aws

ユーザーガイド

Amazon Macie

Amazon Macie: ユーザーガイド

Table of Contents

Amazon Macie とは

Amazon Macie は、機械学習とパターンマッチングを使用して機密データを検出し、データセキュリティリスクを可視化し、それらのリスクに対する自動保護を可能にするデータセキュリティサービスです。

組織の Amazon Simple Storage Service (Amazon S3) データ資産のセキュリティ体制を管理するために、Macie は S3 汎用バケットのインベントリを提供し、セキュリティとアクセスコントロールのためにバケットを自動的に評価およびモニタリングします。Macie は、バケットがパブリックアクセス可能になっているなど、データのセキュリティまたはプライバシーに関する潜在的な問題を検出した場合、必要に応じて確認および修正するための検出結果を生成します。

Macieはまた機密データの検出とレポートを自動化するので、組織が Amazon S3 に保存しているデータをより詳細に把握できるようになります。機密データを検出するには、Macie が提供する組み込み型の基準と手法、ユーザーが定義するカスタム基準、またはこの 2 つの組み合わせを使用できます。Macie が S3 オブジェクト内の機密データを検出すると、Macie は検出結果を生成して、検出した機密データを通知します。

検出結果に加えて、Macie は Amazon S3 データのセキュリティ体制と機密データがデータ資産内に存在する可能性のある場所に関するインサイトを提供する統計と情報を提供します。統計と情報は、特定の S3 バケットとオブジェクトのより深い調査を実行する決定をガイドできます。Amazon Macie コンソールまたは Amazon Macie Amazon Macie API を使用して、結果、統計、その他の情報を確認および分析できます。また、Macie と Amazon EventBridge および の統合を活用して、他のサービス、アプリケーション、システムを使用して検出結果を AWS Security Hub モニタリング、処理、修正することもできます。

トピック

Amazon Macie の機能

Amazon Macie を使用して Amazon S3 で機密データを検出、監視、保護するための主要な方法をいくつか紹介します。

機密データの検出を自動化する

Macie を使って、以下 2 つの方法で機密データの検出とレポートを自動化できます。機密データ検出を自動化するよう Macie を設定する方法と、機密データ検出ジョブを作成し実行する方法です。S3 オブジェクト内の機密データを検出すると、Macie は機密データの検出結果を作成します。検出結果は、Macie が検出した機密データの詳細なレポートを提供します。

機密データの自動検出により、Amazon S3 データエステート内の機密データがどこに存在するかに幅広い可視性を提供しています。このオプションでは、Macie は S3 バケットインベントリを継続的に評価し、サンプリング技術によりバケットから代表的な S3 オブジェクトを識別して選択します。その後、Macie は選択したオブジェクトを取得して分析し、機密データがないか検査します。

機密データ検出ジョブでは、より詳細で対象を絞った分析が可能になります。このオプションを使用し、分析の幅と深さ、つまり、分析する S3 バケット、サンプリング深度、S3 オブジェクトのプロパティから派生するカスタム基準を定義します。ジョブは、オンデマンドの分析と評価用には 1 回のみ、定期的な分析、評価、監視用には継続的に実行するよう設定できます。

どちらのオプションでも、組織が Amazon S3 に保存するデータと、そのデータのセキュリティやコンプライアンスリスクに関する包括的なビューを構築して維持できます。

さまざまな機密データタイプを発見する

Macie で機密データ検出を検出するために、S3 バケット内のオブジェクトを分析するよう組み込まれた基準と手法 (機械学習やパターンマッチングなど) を使用することができます。これらの基準と手法は、マネージドデータ識別子と呼ばれ、複数タイプの個人を特定できる情報 (PII)、財務情報、認証情報データなど、多くの国や地域で増加している大規模な機密データタイプのリストを検出できます。

また、カスタムデータ識別子を使用することもできます。カスタムデータ識別子は、機密データを検出するために定義する基準のセットです。これらの基準は、一致するテキストパターンを定義し、オプションで文字シーケンス、結果を絞り込む近接ルールを定義する正規表現 (正規表現) で設定されます。このタイプの識別子を使用すれば、お客様の特定のシナリオ、知的財産、または専有データを反映する機密データを検出できます。Macie が提供するマネージドデータ識別子を補足できます。

分析を微調整するのに許可リストも使えます。許可リストは、Macie に S3 オブジェクトで無視させたい特定のテキストやテキストパターンを定義します。これらは通常、特定のシナリオや環境における機密データの例外です。例えば、組織の代表者氏名、組織の代表電話番号、組織がテストに使用するサンプルデータなどです。

セキュリティとアクセスコントロールについてデータを評価してモニタリングする

Macie を有効にすると、Macie は S3 汎用バケットの完全なインベントリを自動的に生成し、維持を開始します。また、Macie はセキュリティとアクセスコントロールのためバケットの評価と監視を開始します。Macie がバケットのセキュリティまたはプライバシーに関する潜在的な問題を検出すると、ユーザー用に ポリシーの調査結果を作成します。

特定の検出結果に加えて、ダッシュボードでは Amazon S3 データの集約統計スナップショットを提供します。これには、パブリックにアクセス可能または他の と共有されているバケットの数など、主要なメトリクスの統計が含まれます AWS アカウント。各統計をドリルダウンして、そのサポートデータを確認できます

Macie はインベントリ内の個別のバケット詳細情報と統計も提供します。データには、バケットのパブリックアクセスと暗号化設定の内訳、およびバケット内の機密データを検出するために Macie が分析できるオブジェクトのサイズと数が含まれます。特定のフィールドで インベントリの参照、またはインベントリの並べ替えおよびフィルタリングを行うことができます。

調査結果を確認して分析する

Macie では、検出結果は、Macie が S3 オブジェクトで検出した機密データの詳細なレポート、または S3 汎用バケットのセキュリティまたはプライバシーに関する潜在的な問題です。各検出結果には、重要度評価、影響を受けるリソースに関する情報、Macie がデータや問題をいつどのように検出したかなどの追加の詳細が表示されます。

調査結果の確認、分析、管理を行うには、Amazon Macie コンソールの 調査結果ページを使用できます。これらのページでは、調査結果をリスト化し、個別の調査結果の詳細を提供します。また、調査結果のグループ化、フィルタリング、並べ替え、および抑制のための複数のオプションも提供します。また、Amazon Macie API を使用して、調査結果をクエリ、取得、および抑制することもできます。API を使用する場合、データを別のアプリケーション、サービス、またはシステムに渡して、より詳細な分析、長期保存、またはレポートの作成を行うことができます。

他のサービスおよびシステムを用いた調査結果のモニタリングと処理

他の のサービスやシステムとの統合をサポートするために、Macie は検出結果を検出結果イベントとして Amazon に発行します EventBridge。 EventBridge は、検出結果を AWS Lambda 関数や Amazon Simple Notification Service (Amazon SNS) トピックなどのターゲットにルーティングできるサーバーレスイベントバスサービスです。を使用すると EventBridge、既存のセキュリティおよびコンプライアンスワークフローの一部として、結果をほぼリアルタイムでモニタリングおよび処理できます。

調査結果を AWS Security Hubに発行するように Macie を設定することもできます。Security Hub は、 AWS 環境全体のセキュリティ体制を包括的に把握し、セキュリティ業界標準とベストプラクティスに照らして環境をチェックするのに役立つサービスです。Security Hub を使用すると、AWS内の組織のセキュリティ体制の広範な分析の一部として、検出結果をより簡単にモニタリングおよび処理できます。また、複数の から結果を集約し AWS リージョン、1 つのリージョンから集約された結果データをモニタリングして処理することもできます。

複数の Macie アカウントを集中管理する

AWS 環境に複数のアカウントがある場合は、環境内のアカウントの Macie を一元管理できます。これは、Macie を と統合するか、Macie でメンバーシップの招待を送信および承諾 AWS Organizations することで、2 つの方法で行うことができます。

複数アカウント設定では、指定された Macie 管理者が特定のタスクを実行し、同じ組織のメンバーであるアカウントの特定の Macie 設定、データ、およびリソースにアクセスできます。タスクには、メンバーアカウントが所有する S3 バケットに関する情報の確認、それらのバケットのポリシー検出結果の確認、機密データのためのバケット検査が含まれます。アカウントが を通じて関連付けられている場合 AWS Organizations、Macie 管理者は組織内のメンバーアカウントに対して Macie を有効にすることもできます。

リソースをプログラムで開発して管理する

Amazon Macie コンソールに加えて、Amazon Macie API を使用してMacie を操作することができます。Amazon Macie API は、Macie アカウント設定、データ、リソースへの包括的なプログラムによるアクセスを提供します。

Macie とプログラムでやり取りするには、HTTPS リクエストを Macie に直接送信するか、最新バージョンの AWS コマンドラインツールまたは AWS SDK を使用できます。 AWS は PowerShell、、、Java、Go、Python、C++、.NET などのさまざまな言語とプラットフォーム用のライブラリとサンプルコードで構成されるツールと SDKs を提供します。

Amazon Macie にアクセスする

Amazon Macie はほとんどの で利用可能です AWS リージョン。Macieが現在利用可能なリージョンのリストについては、AWS 全般のリファレンスのAmazon Macieエンドポイントとクォータを参照してください。の 管理 AWS リージョン の詳細については AWS アカウント、「 AWS Account Management リファレンスガイド」の AWS リージョン 「アカウントで使用できる の指定」を参照してください。

各リージョンで、次のいずれかの方法で Macie を使用できます。

AWS Management Console

AWS Management Console は、 リソースの作成と管理 AWS に使用できるブラウザベースのインターフェイスです。そのコンソールの一部として、Amazon Macie コンソールは Macie アカウント、データ、リソースへのアクセスを提供します。Macie コンソールを使えば、S3 バケットに関する統計やその他情報の確認、機密データ検出ジョブの実行、検出結果の確認と分析など多くのタスクを実行することができます。

AWS コマンドラインツール

AWS コマンドラインツールを使用すると、システムのコマンドラインでコマンドを発行して、Macie タスクと AWS タスクを実行できます。コマンドラインを使用すると、コンソールを使用するよりも高速で便利になります。コマンドラインツールは、タスクを実行するスクリプトを作成する場合にも便利です。

AWS には、 AWS Command Line Interface （ AWS CLI) と の 2 セットのコマンドラインツールが用意されています AWS Tools for PowerShell。のインストールと使用については AWS CLI、「AWS Command Line Interface ユーザーガイド」を参照してください。Tools for のインストールと使用については PowerShell、「 AWS Tools for PowerShell ユーザーガイド」を参照してください。

AWS SDK

AWS はSDKs を提供します。SDKs、Macie やその他の への便利なプログラムによるアクセスを提供します AWS のサービス。SDK は、暗号署名によるリクエスト、エラーの管理、リクエストの自動再試行などのタスクも処理します。 AWS SDKsで構築するツール AWS」を参照してください。

Amazon Macie REST API

Amazon Macie REST API は、Macie アカウント、データ、リソースへの包括的なプログラムによるアクセスを提供します。この API を使用すると、HTTPS リクエストを Macie に直接送信できます。ただし、 AWS コマンドラインツールや SDKsを使用するには、アプリケーションがリクエストに署名するためのハッシュの生成など、低レベルの詳細を処理する必要があります。この API の詳細については、Amazon Macie API リファレンスを参照してください。

Amazon Macie の料金

他の AWS 製品と同様に、Amazon Macie を使用するための契約や最低契約金はありません。

Macie の料金は、セキュリティとアクセスコントロール用 S3 バケット評価と監視、機密データ自動検出用 S3 オブジェクト監視、オブジェクト内機密データの検出と報告用 S3 オブジェクト分析、といったいくつかの体系に基づいて設定されています。詳細については、Amazon Macie 料金表を参照してください。

Macie の使用コストを理解して予測するために、Macie はアカウントの推定使用コストを提供します。Amazon Macie コンソールでこれらの見積もりを確認して、Amazon Macie API でそれらにアクセスできます。サービスの使用方法によっては、Amazon S3 からバケットデータを取得したり、カスタマーマネージド を使用して分析のためにオブジェクトを復号化したりするなど、他の を特定の Macie 機能 AWS のサービス と組み合わせて使用すると、追加料金が発生する場合があります。AWS KMS keys

Macie を初めて有効にすると、 AWS アカウント は Macie の 30 日間の無料トライアルに自動的に登録されます。これには、 AWS Organizationsで組織の一部として有効化されている個別のアカウントが含まれます。無料トライアル期間中は、該当する で Macie を使用して S3 バケットのセキュリティとアクセスコントロールを評価およびモニタリング AWS リージョン するための料金はかかりません。アカウントの設定によっては、無料トライアルに Amazon S3 データの機密データ自動検出実行が含まれる場合もあります。無料トライアルには、S3 オブジェクト内機密データ検出とレポートのための機密データ検出ジョブ実行は含まれません。

無料トライアル終了後の Macie の使用コストを理解して予測できるように、Macie はトライアルの間の Macie の使用状況に基づく推定使用コストを提供します。使用状況データには、無料トライアルが終了するまでの残り時間も示されます。Amazon Macie コンソールでこのデータを表示して、Amazon Macie API でそのデータにアクセスできます。

関連サービス

のデータ、ワークロード、アプリケーションをさらに保護するには AWS、以下を Amazon Macie AWS のサービス と組み合わせて使用することを検討してください。

AWS Security Hub

> AWS Security Hub は、 AWS リソースのセキュリティ状態を包括的に把握し、セキュリティ業界標準とベストプラクティスに照らして AWS 環境をチェックするのに役立ちます。これは、複数の AWS のサービス (Macie を含む) およびサポートされている AWS パートナーネットワーク (APN) 製品からセキュリティ検出結果を消費、集約、整理、優先順位付けすることによって部分的に行われます。Security Hub は、セキュリティの傾向を分析し、 AWS 環境全体で最も優先度の高いセキュリティ問題を特定するのに役立ちます。

Security Hub の詳細については、AWS Security Hub ユーザーガイドを参照してください。Macie と Security Hub を一緒に使用する方法については、Amazon Macie の AWS Security Hub との統合を参照してください。

Amazon GuardDuty

Amazon GuardDuty は、Amazon S3 AWS CloudTrail のデータイベント AWS ログや CloudTrail 管理イベントログなど、特定のタイプのログを分析および処理するセキュリティモニタリングサービスです。悪意のある IP アドレスやドメインのリストなどの脅威インテリジェンスフィードや機械学習を使用して、 AWS 環境内の予期しないアクティビティや、潜在的に不正なアクティビティや悪意のあるアクティビティを特定します。

の詳細については GuardDuty、「Amazon ユーザーガイド GuardDuty 」を参照してください。

その他の AWS セキュリティサービスの詳細については、「 のセキュリティ、アイデンティティ、コンプライアンス AWS」を参照してください。

Amazon Macie の開始方法

このチュートリアルでは、Amazon Macie の概要を説明します。 AWS アカウントで Macie を有効化する方法について説明します。また、Amazon Simple Storage Service (Amazon S3) のセキュリティ体制を評価し、S3 バケット内の機密データを検出してレポートするためのキー設定とリソースを設定する方法についても説明します。

タスク

開始する前に

Amazon Web Services AWSにサインアップすると、Amazon Macie を含むすべての AWS のサービスに、アカウントが自動的にサインアップされます。ただし、Macie を有効化して使用するには、まず Amazon Macie コンソールと API オペレーションへのアクセスを許可するアクセス許可を設定する必要があります。これを行う AWS には、 AWS Identity and Access Management (IAM) を使用して、 という名前 AWS の管理ポリシーを IAM ID `AmazonMacieFullAccess`にアタッチします。詳細については、Amazon Macie の AWS マネージドポリシーを参照してください。

ステップ 1: Amazon Macie を有効化する

必要なアクセス許可を設定した後、 AWS アカウントで Amazon Macie を有効化することができます。次のステップに従ってアカウントで Macieを有効化します。

Macie を有効化するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、Macie を有効にして使用するリージョンを選択します。
3. Amazon Macie ページで、開始方法を選択します。

4. (オプション) Macie を有効にする AWS のサービス と、Macie はユーザーに代わって他の を呼び出して AWS リソースをモニタリングするために必要なアクセス許可を Macie に付与するサービスにリンクされたロールを自動的に作成します。このロールのアクセスポリシーを確認するには、コンソールで View role permissions (ロールのアクセス許可の表示) を選択します。このロールの詳細については、Amazon Macie のサービスにリンクされたロールを参照してください。
5. Macie を有効化 を選択します。

Macie は数分以内に、現在のリージョンで S3 汎用バケットの完全なインベントリを自動的に生成し、維持を開始します。また、Macie は、セキュリティとアクセスコントロールについてバケットのモニタリングと評価を開始します。詳細については、Macie が Amazon S3 データセキュリティをモニタリングする方法を参照してください。

アカウントの設定によっては、Macie は S3 バケットの機密データの自動検出も開始します。Macie はバケット内の代表的なオブジェクトを継続的に識別、選択、分析し始め、オブジェクトに機密データがないか検査します。分析が進むにつれて、Macie は通常、アカウントで Macie を有効にしてから 48 時間以内に統計やその他の結果を提供し、確認することができます。アカウントの機密データ自動検出設定を設定することで、分析をカスタマイズできます。詳細については、機密データの自動検出の仕組みを参照してください。

Amazon S3 データの集計統計を確認するには、コンソールのナビゲーションペインで概要を選択します。インベントリ内の個々の S3 バケットの詳細を確認するには、ナビゲーションペインで S3 バケットを選択します。バケットの詳細を表示するには、バケットを選択します。詳細パネルには、バケットのデータのセキュリティ、プライバシー、機密性に関する洞察を提供する統計およびその他の情報が表示されます。これらの詳細については、S3 バケットインベントリを確認するを参照してください。

ステップ 2: 機密データの検出結果のリポジトリを設定する

Amazon Macie では、S3 バケット内の機密データを検出するには、Macie が自動的に機密データ検出を実行するように設定するか、機密データ検出ジョブを実行するという2つの方法があります。機密データ検出ジョブは、S3 バケット内のオブジェクトを分析して、オブジェクトに機密データが含まれているかどうかを判断するために作成したジョブです。

Macie は、機密データ検出ジョブを実行するとき、または機密データ自動検出を実行するときに分析する S3 オブジェクトごとにレコードを作成します。これらのレコードは 機密データの検出結果 と呼ばれ、個々のオブジェクトの分析に関する詳細を記録します。Macie は、エラーや問題が原因で分

析できないオブジェクトの機密データ検出結果も作成します。機密データの検出結果から、データプライバシーと保護の監査や調査に役立つ分析レコードが得られます。

Macie は機密データの検出結果を 90 日間だけ保存します。結果にアクセスし、それらの長期保存と保持を有効化するには、結果を S3 バケットに保存するように Macie を設定します。これは Macie を有効化してから 30 日以内に行う必要があります。この後、バケットは、機密データ検出結果のすべての最終的で長期的なリポジトリとして機能します

このリポジトリを設定する方法については、機密データ検出結果の保存と保持を参照してください。

ステップ 3: 検出結果のサンプルを調べる

Amazon Macie には、ポリシー検出結果と機密データ検出結果の 2 つのカテゴリがあります。 Macie は、S3 汎用バケットのポリシーまたは設定が、バケットとバケットのオブジェクトのセキュリティまたはプライバシーを低下させる方法で変更されたときにポリシー検出結果を作成します。Macie が S3 オブジェクト内の機密データを検出すると、Macie は機密データの調査結果を作成します。各カテゴリには、複数のタイプの調査結果があります。

Macie が提供するさまざまなカテゴリとタイプの調査結果を探索して学ぶために、必要に応じて検出結果のサンプルを作成して確認します。検出結果のサンプルでは、データ例とプレースホルダー値を使用して、Macie がそれぞれのタイプの調査結果に含める可能性があるさまざまな種類の情報が示されます。

検出結果のサンプルを作成して確認するには、以下のステップに従います。

検出結果のサンプルを作成して確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定 を選択します。
3. 検出結果のサンプル で、検出結果のサンプルの生成 を選択します。Macie がサポートする調査結果のタイプごとに 1 つの検出結果のサンプルを Macie が生成します。
4. ナビゲーションペインで 結果 を選択します。調査結果ページには、現在の AWS リージョンでのアカウントの現在の調査結果が表示されます。これには、前のステップで作成した検出結果のサンプルも含まれます。
5. 調査結果ページで、タイプが SAMPLE で始まる調査結果を見つけます。
6. 特定のサンプル結果の詳細を確認するには、調査結果を選択します。詳細パネルに、結果の詳細が表示されます。

調査結果の各タイプの詳細については、調査結果のタイプを参照してください。検出結果のサンプルの作成と確認の詳細については、検出結果のサンプルの使用を参照してください。

ステップ 4: 機密データを検出するジョブを作成する

S3 バケット内の機密データの検出およびレポートするには、機密データ検出ジョブを実行します。機密データ検出ジョブは、S3 バケット内のオブジェクトを分析して、オブジェクトに機密データが含まれているかどうかを判断します。機密データの自動検出とは異なり、分析の幅と深さを定義します。また、 1 回、またはスケジュールベースで定期的に実行するか、その頻度を指定します。

デフォルト設定を使用するジョブを作成し、それを作成した直後に 1 回実行するには、次のステップに従います。定期的に実行されるジョブまたはカスタム設定を使用するジョブを作成する方法については、機密データ検出ジョブの作成を参照してください。

機密データ検出ジョブを作成するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブを選択します。
3. ジョブの作成を選択します。
4. S3 バケットを選択するステップでは、特定のバケットを選択するを選択します。次に、テーブルで、ジョブで分析する各 S3 バケットのチェックボックスをオンにします。

   この表は、現在の の S3 汎用バケットの完全なインベントリを示しています AWS リージョン。特定のバケットをより簡単に検索するには、テーブルの上にあるフィルターボックスにフィルター基準を入力します。テーブルで列見出しを選択して、テーブルを並べ替えることもできます。
5. バケットの選択が終了したら、次へを選択します。
6. S3 バケットを確認する ステップで、バケットの選択を確認して検証します。
7. 範囲を絞り込むステップで、1 回限りのジョブを選択し、次に 次へ を選択します。
8. マネージドデータ識別子の選択ステップでは、推奨 を選択します。必要に応じて、ジョブに推奨するマネージドデータ識別子のテーブルを確認し、次へ を選択します。

   マネージドデータ識別子は、クレジットカード番号、 AWS シークレットアクセスキー、特定の国や地域のパスポート番号など、特定のタイプの機密データを検出するように設計された一連の組み込み基準と手法です。詳細については、マネージドデータ識別子の使用を参照してください。
9. カスタムデータ識別子を選択するステップで、次へを選択します。

カスタムデータ識別子は、機密データを検出するために定義する基準のセットです。これらの基準は、一致するテキストパターンを定義し、オプションで文字シーケンス、結果を絞り込む近接ルールを定義する正規表現 (正規表現) で設定されます。詳細については、カスタムデータ識別子の構築を参照してください。

10. 許可リストの選択ステップでは、次へを選択します。

    Macieでは、許可リストは、Macieが機密データのためにS3オブジェクトを検査するときに無視したいテキストまたはテキストパターンを指定します。これらは通常、特定のシナリオや環境における機密データの例外です。詳細については、許可リストでの機密データの例外の定義を参照してください。

11. 名前と説明を入力するステップで、名前を入力し、必要に応じてジョブの説明を入力します。続いて、次へを選択します。

12. 確認して作成するステップでは、ジョブの設定設定を確認し、それらが正しいことを検証します。

    ジョブを実行した場合の合計推定コスト (米ドル単位) も確認できます。見積もりは、ジョブを保存する前にジョブの設定を調整するかどうかを判断するのに役立ちます。詳細については、機密データ検出ジョブのコスト予測を参照してください。

13. ジョブの設定の確認と検証が終了したら、送信を選択します。

Macie は直ちにジョブの実行を開始します。ジョブをモニタリングする方法については、機密データ検出ジョブのステータスをチェックするを参照してください。

ステップ 5: 調査結果を確認する

Amazon Macie は S3 汎用バケットのセキュリティとアクセスコントロールを自動的にモニタリングし、バケットのセキュリティまたはプライバシーに関する潜在的な問題を報告するためのポリシー検出結果を作成します。機密データ検出ジョブを実行するか、機密データ自動検出を実行するように Macie を設定すると、Macie は機密データ検出結果を作成して、S3 オブジェクトで検出された機密データを報告します。調査結果の詳細については、調査結果を分析するを参照してください。

調査結果を確認するには、以下のステップを実行します。

調査結果を確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。

2. ナビゲーションペインで 調査結果 を選択します。調査結果ページには、現在の AWS リージョンでのアカウントの現在の調査結果が表示されます。
3. (オプション) 特定の基準で調査結果をフィルタリングするには、テーブルの上にあるフィルターボックスに基準を入力します。
4. 特定の調査結果の詳細を確認するには、調査結果を選択します。詳細パネルに、結果の詳細が表示されます。

検出結果をグループ化してフィルタリングする方法など、詳細については、調査結果を確認する を参照してください。

Amazon Macie の概念と用語

Amazon Macie では、一般的な AWS 概念と用語に基づいて構築し、これらの追加用語を使用します。

アカウント

AWS リソースと、それらのリソースにアクセスできる ID AWS アカウント を含む標準。

Macie を使用するには、 AWS アカウント 認証情報 AWS を使用して にサインインし、Macie AWS リージョン を使用する を選択し、そのリージョン AWS アカウント で に対して Macie を有効にします。詳細については、「Amazon Macie の開始方法」を参照してください。

Macie には次の 3 タイプのアカウントがあります。

- 管理者アカウント — このタイプのアカウントは、組織の Macie アカウントを管理します。組織は、関連するアカウントのグループとして集中管理されるアカウントのセットです。
- メンバーアカウント — このタイプのアカウントは、組織の Macie 管理者アカウントに関連付けられ、管理されます。
- スタンドアロンアカウント — このタイプのアカウントは、管理者アカウントでもメンバーアカウントでもありません。組織の一部ではありません。

Macie アカウントを組織に追加するには 2 つの方法があります。1 つは Macie を AWS Organizations に統合する方法と、Macie メンバーシップの招待を送信および受け入れる方法です。詳細については、複数のアカウントの管理を参照してください。

管理者アカウント

Macie では、組織の Macie アカウントを管理するアカウントです。Macie では、組織は、関連するアカウントのグループとして集中管理されるアカウントのセットです。

Macie 管理者アカウントのユーザーは、Amazon Simple Storage Service (Amazon S3) のインベントリデータ、ポリシーの検出結果、および組織内のすべてのアカウントの特定の Macie 設定とリソースにアクセスできます。また、自動機密データ検出を実行し、機密データ検出ジョブを実行し、アカウントが所有する S3 バケット内の機密データを検出することもできます。アカウントがどのように

管理者アカウントとして指定されるかによっては、組織内の他のアカウントに対して追加のタスクを実行できる場合もあります。

詳細については、複数のアカウントの管理を参照してください。

許可リスト

Macie では、許可リストによって、Macie が機密データの S3 オブジェクトを検査する際に無視するテキストまたはテキストパターンを特定します。

Macie では、無視する特定の単語やその他のタイプの文字シーケンスをリストするプレーンテキストファイルと、無視するテキストパターンを定義する正規表現(正規表現)の 2 つのタイプの許可リストを作成できます。オブジェクトに許可リストのエントリまたはパターンに一致するテキストが含まれている場合、Macie は、テキストがマネージドデータ識別子またはカスタムデータ識別子の基準に一致していてもMacie はそのテキストの出現を機密データ検出結果や統計、その他のタイプの結果に報告しません。

詳細については、許可リストでの機密データの例外の定義を参照してください。

機密データの自動検出

Macie が継続的に実行する一連の自動分析アクティビティで、S3 バケットから代表的なオブジェクトを特定して選択し、選択したオブジェクトに機密データがないかを検査します。

各ジョブは、その検出された機密データと実行された分析のレコード (機密データの調査結果と 機密データの検出結果) を作成します。Macie は、Amazon S3 データに関して提供する統計やその他の情報も更新します。

詳細については、「機密データ自動検出を実行する」を参照してください。

AWS Security Finding 形式 (ASFF)

に発行または によって生成された検出結果の内容の標準化された JSON 形式 AWS Security Hub。ASFF には、セキュリティ問題のソース、影響を受けるリソース、および調査結果のステータスに関する詳細が含まれます。

詳細については、AWS Security Hub ユーザーガイドの AWS Security Finding 形式 (ASFF)を参照してください。Security Hub への Macie の調査結果の公開の詳細については、Amazon Macie の AWS Security Hub との統合を参照してください。

分類可能なバイト数またはサイズ

Macie が提供する S3 バケット統計では、S3 バケット内のすべての分類可能なオブジェクトの合計ストレージサイズ。

バケットでバージョニングが有効化されている場合、この値は、バケット内の分類可能な各オブジェクトの最新バージョンのストレージサイズに基づきます。オブジェクトが圧縮ファイルの場合、この値はファイル解凍後のファイルの内容の実際のサイズを反映しません。

詳細については、「S3 バケットインベントリを確認する」および「Amazon S3 のセキュリティ体制を評価する」を参照してください。

分類可能なオブジェクト

Macie が分析して機密データを検出できる S3 オブジェクト。

S3 バケット統計を計算する際、Macie はオブジェクトのストレージクラスとファイル名拡張子に基づいてオブジェクトを分類可能と判断します。前のデータでは、オブジェクトがサポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を持っている場合、オブジェクトは 分類可能です。

詳細については、「S3 バケットインベントリを確認する」および「Amazon S3 のセキュリティ体制を評価する」を参照してください。

機密データを検出する場合、Macie はオブジェクトのストレージクラス、ファイル名拡張子、内容に基づいてオブジェクトを分類可能と判断します。オブジェクトが分類可能であるのは:サポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を持っていて、Macie がオブジェクトからデータを抽出および分析できる場合。

詳細については、「機密データの検出」および「コストの予測とモニタリング」を参照してください。

カスタムデータ識別子

機密データを検出するために定義する基準のセット。

基準は、一致するテキストパターン、オプションで文字シーケンス、結果を絞り込む近接ルールを定義する正規表現 (正規表現) から設定されています。文字シーケンスは次のようになります。

- 正規表現に一致するテキストに近接している必要がある単語またはフレーズであるキーワード、または
- 単語を無視は、結果から除外する単語またはフレーズです。

検出基準に加えて、カスタムデータ識別子が生成する機密データ結果のカスタム重要度設定を定義できます。

詳細については、カスタムデータ識別子の構築を参照してください。

フィルタールール

Amazon Macie コンソールで検出結果を分析するために作成して保存する属性ベースのフィルタ条件のセット。フィルタールールは、特定のタイプの機密データを報告する重要度の高い検出結果など、特定の特性を持つ検出結果の一貫した分析を実行するのに役立ちます。

詳細については、調査結果のフィルタールールの作成と管理を参照してください。

検出結果

Macie が S3 オブジェクトで検出した機密データ、または S3 汎用バケットのセキュリティまたはプライバシーに関する潜在的な問題の詳細なレポート。各結果では、重要度評価、影響を受けたリソースに関する情報、Macie がデータや問題を見つけたタイミングなどの詳細が示されます。

Macie は 2 つのカテゴリの結果を生成します。1 つは 機密データの調査結果 (Macie が S3 オブジェクトで検出した機密データ)で、もう 1 つは ポリシーの検出結果(Macie が S3 バケットのセキュリティとアクセス制御の設定で検出した潜在的な問題に関するポリシー結果) です。各カテゴリには、特定のタイプの調査結果があります。

詳細については、Amazon Macie の調査結果のタイプを参照してください。

イベントの

機密データの検出結果またはポリシーの検出結果の詳細を含む Amazon EventBridge イベント。

Macie は、機密データの検出結果とポリシーの検出結果をイベント として Amazon EventBridge に自動的に発行します。 イベントは、イベントの EventBridge スキーマに準拠する JSON オブジェクトです AWS 。これらのイベントを使用して、他のアプリケーション、サービス、およびシステムを使用して、検出結果をモニタリングし、処理し、アクションを取ることができます。

詳細については、「Amazon Macie の Amazon EventBridge との統合」および「Amazon Macie の調査結果の Amazon EventBridge イベントスキーマ」を参照してください。

ジョブ

機密データ検出ジョブを参照してください。

マネージドデータ識別子

特定のタイプの機密データを検出するように設計された、組み込み型の基準と手法のセットです。機密データの例としては、クレジットカード番号、 AWS シークレットアクセスキー、特定の国または地域のパスポート番号などがあります。これらの識別子は、多くの国や地域の機密データタイプの大規模かつ増加しているリストを検出できます。

詳細については、マネージドデータ識別子の使用を参照してください。

メンバーアカウント

組織の指定された Macie 管理者アカウントによって管理される Macie アカウント。組織は、相互に関連付けられ、特定の の関連アカウントのグループとして一元管理される Macie アカウントのセットです AWS リージョン。

アカウントは、Macie を のアカウントの組織と統合するか、Macie メンバーシップの招待を受け入れる AWS Organizations という 2 つの方法でメンバーアカウントになることができます。

メンバーアカウントをお持ちの場合、Macie 管理者はメンバーアカウントの Amazon S3 インベントリデータ、ポリシーの検出結果、特定の Macie 設定とリソースにアクセスできます。管理者は、自動機密データ検出を実行し、機密データ検出ジョブを実行し、S3 バケット内の機密データを検出することもできます。また、アカウントがメンバーアカウントになった経緯によっては、アカウントに対し追加のタスクを実行できる場合もあります。

詳細については、複数のアカウントの管理を参照してください。

組織

相互に関連付けられ、特定の 内の関連アカウントのグループとして一元管理される一連の Macie アカウント AWS リージョン。

各組織は、指定された Macie 管理者アカウントと 1 つ以上の関連付けられたメンバーアカウントで設定されています。管理者アカウントは、メンバーアカウントの特定の Macie 設定、データ、およびリソースにアクセスできます。組織を作成するには、Macie を AWS Organizations と統合する方法と、Macie 内でメンバーシップ招待を送信および受け入れる方法の 2 つの方法があります。

詳細については、複数のアカウントの管理を参照してください。

ポリシーの検出結果

S3 汎用バケットのセキュリティおよびアクセスコントロール設定に関する潜在的なポリシー違反または問題の詳細なレポート。詳細には、重要度評価、影響を受けたリソースに関する情報、いつ Macie が問題を見つけたかが含まれます。

Macie は、S3 汎用バケットのポリシーまたは設定が、バケットとバケットのオブジェクトのセキュリティまたはプライバシーを低下させる方法で変更されたときにポリシーの検出結果を生成します。Macie は、Amazon S3 データの継続的なモニタリングアクティビティの一部としてこれらの結果を生成します。Macie はいくつかのタイプのポリシー結果を生成できます。

詳細については、「Amazon Macie の調査結果のタイプ」および「データのセキュリティとプライバシーのモニタリング」を参照してください。

サンプルの検出結果

検出結果のサンプルでは、データ例とプレースホルダー値を使用して、各タイプの調査結果に含まれる可能性のある情報の種類を示します。

詳細については、検出結果のサンプルの使用を参照してください。

機密データの調査結果

Macie が S3 オブジェクトで検出した機密データの詳細なレポート。詳細には、重要度評価、影響を受けたリソースに関する情報、Macie が見つけた機密データのタイプと出現回数、およびいつ Macie が機密データを検出したかが含まれます。

Macie は、機密データ検出ジョブを実行したり、自動機密データ検出を実行したりするときに分析する S3 オブジェクト内に機密データを検出した場合に、機密データの検出結果を生成します。Macie は、いくつかのタイプの機密データの検出結果を生成することができます。

詳細については、「Amazon Macie の調査結果のタイプ」および「機密データの検出」を参照してください。

機密データ検出ジョブ

ジョブとも呼ばれ、Macie が S3 オブジェクト内の機密データを検出して報告するために実行する一連の自動処理および分析タスクです。ジョブを作成するときは、ジョブを実行する頻度を指定し、ジョブの分析の範囲と性質を定義します。

各ジョブは、その検出された機密データと実行された分析のレコード (機密データの調査結果と 機密データの検出結果) を作成します。Macie はログデータを Amazon CloudWatch Logs に発行します。

詳細については、「機密データ検出ジョブの実行」を参照してください。

機密データの検出結果

Macie が S3 オブジェクトに対して実行した分析の詳細を記録して、オブジェクトに機密データが含まれているかどうかを判断するレコード。Macie はこれらのレコードを生成して JSON Lines (.jsonl) ファイルに書き込み、暗号化して指定した S3 バケットに保存します。レコードは標準化されたスキーマに準拠しています。

機密データ検出ジョブを実行するか、Macie が 自動機密データ検出を実行すると、Macie は分析の範囲に含まれるオブジェクトごとに機密データ検出結果を作成します。これには、以下が含まれます。

- Macie が機密データを検出し、したがって機密データの検出結果を生成するオブジェクト。
- Macie が機密データを検出せず、したがって機密データの検出結果を生成しないオブジェクト。
- アクセス許可の設定や、サポートされていないファイルまたはストレージ形式の使用などのエラーまたは問題により、Macie が分析できないオブジェクト。

詳細については、機密データ検出結果の保存と保持を参照してください。

スタンドアロンアカウント

組織の管理者でもメンバーアカウントでもない Macie アカウント。アカウントは組織の一部ではありません。

抑制された検出結果

抑制ルールによって自動的にアーカイブされた検出結果。つまり、Macie が検出結果を生成したときにその検出結果が抑制ルールの条件と一致したため、Macie は検出結果ステータスを自動的に アーカイブ済みに変更しました。

詳細については、調査結果を抑制するを参照してください。

抑制ルール

検出結果を自動的にアーカイブ (抑制する) ために作成・保存する属性ベースのフィルター条件一式。抑制ルールは、調査結果のクラスを確認した後、それらの調査結果を再度通知してほしくない場合に役立ちます。

抑制ルールを使用して検出結果を抑制する場合、Macie はルールの基準に一致する検出結果を生成し続けます。ただし、Macie は調査結果のステータスを自動的に アーカイブ済みに変更します。これは、検出結果がデフォルトで Amazon Macie コンソールに表示されず、Macie がそれらを他の AWS のサービスに公開しないことを意味します。

詳細については、調査結果を抑制するを参照してください。

分類不可能なバイト数またはサイズ

Macie が提供する S3 バケット統計では、S3 バケット内のすべての分類不可能なオブジェクトの合計ストレージサイズ。

バケットでバージョニングが有効化されている場合、この値は、バケット内の分類不可能各オブジェクトの最新バージョンのストレージサイズに基づきます。オブジェクトが圧縮ファイルの場合、この値はファイル解凍後のファイルの内容の実際のサイズを反映しません。

詳細については、「S3 バケットインベントリを確認する」および「Amazon S3 のセキュリティ体制を評価する」を参照してください。

分類不可能オブジェクト

Macie が機密データを検出するために分析できない S3 オブジェクト。

S3 バケット統計を計算する際、Macie はオブジェクトのストレージクラスとファイル名拡張子に基づいてオブジェクトが分類不可と判断します。分類不可能オブジェクトは、サポートされている

Amazon S3 ストレージクラスを使用しないか、サポートされているファイルまたはストレージ形式のファイル名拡張子を持たないオブジェクトです。

詳細については、「S3 バケットインベントリを確認する」および「Amazon S3 のセキュリティ体制を評価する」を参照してください。

機密データを検出する場合、Macie はオブジェクトのストレージクラス、ファイル名拡張子、および内容に基づいてオブジェクトを分類不可と判断します。オブジェクトが分類不可であるのは: サポートされている Amazon S3 ストレージクラスを使用しないか、サポートされているファイルまたはストレージ形式のファイル名拡張子を持たないか、Macie がオブジェクトからデータを抽出および分析できなかった場合。たとえば、オブジェクトの形式が不正なファイルです。

詳細については、「機密データの検出」および「コストの予測とモニタリング」を参照してください。

Amazon Macie によるデータセキュリティとプライバシーのモニタリング

で Amazon Macie を有効にすると AWS アカウント、Macie は現在の で Amazon Simple Storage Service (Amazon S3) 汎用バケットの完全なインベントリを自動的に生成し、維持を開始します AWS リージョン。また、Macie は、セキュリティとアクセスコントロールについてバケットの評価とモニタリングを開始します。Macie がバケットのセキュリティまたはプライバシーを低下させるイベントを検出すると、Macie は必要に応じてレビューおよび修正するためのポリシー検出結果を作成します。

また、機密データの存在について S3 バケットを評価およびモニタリングするには、機密データ検出ジョブを作成して実行できます。機密データ検出ジョブでは、毎日、毎週、または毎月ベースでバケットオブジェクトの増分分析を実行できます。Macie が S3 オブジェクト内の機密データを検出すると、Macie は機密データの検出結果を作成して、検出した機密データを通知します。アカウント設定に応じて、機密データの自動検出を実行するように Macie を設定することもできます。機密データの自動検出では、サンプリング技術を使用してバケット内の代表的なオブジェクトを継続的に特定、選択、分析します。両方のオプションの詳細については、「」を参照してください機密データの検出。

Macie は、Amazon S3 データのセキュリティとプライバシーを継続的に可視化することもできます。データのセキュリティ体制を評価し、どこでアクションを実行するかを判断するには、コンソールの 概要ダッシュボードを使用できます。ダッシュボードには、Amazon S3 データの集約された統計のスナップショットが表示されます。統計には、パブリックにアクセス可能である、または他の と共有されている汎用バケットの数など、主要なセキュリティメトリクスのデータが含まれます AWS アカウント。ダッシュボードには、アカウントの集約された調査結果データのグループ (たとえば、過去 7 日間の最も多い調査結果を持つ 1～5 個のバケットの名前) も表示されます。各統計をドリルダウンして、そのサポートデータを確認できます。プログラムで統計をクエリするには、Amazon Macie API の GetBucketStatisticsオペレーションを使用します。

より詳細な分析と評価のために、Macie はインベントリ内の個々の S3 バケットの詳細情報と統計を提供します。これには、各バケットのパブリックアクセスと暗号化設定の内訳、およびバケット内の機密データを検出するために Macie が分析できるオブジェクトのサイズと数が含まれます。インベントリは、バケット内のオブジェクトを分析するために機密データ検出ジョブまたは機密データ自動検出を設定しているかどうかも示します。ある場合は、その分析が最後に発生した日時を示します。Amazon Macie コンソールまたは Amazon Macie Amazon Macie API の DescribeBucketsオペレーションを使用して、インベントリを参照、ソート、フィルタリングできます。

ユーザーが組織の Macie 管理者である場合、メンバーアカウントが所有する S3 バケットに関する統計およびその他のデータにアクセスできます。Macie がバケットに対して生成するポリシーの検出結果にアクセスし、バケットに機密データがないか調べることもできます。つまり、Macie を使用して、組織の Amazon S3 データ資産の全体的なセキュリティ体制を評価およびモニタリングできます。詳細については、「複数のアカウントの管理」を参照してください。

トピック

- Amazon Macie がAmazon S3 データセキュリティをモニタリングする方法
- Amazon Macie で Amazon S3 のセキュリティ体制を評価する
- Amazon Macie で Amazon S3 のセキュリティ体制を分析する
- Amazon Macie が S3 バケットおよびオブジェクトにアクセスすることを許可する

Amazon Macie がAmazon S3 データセキュリティをモニタリングする方法

で Amazon Macie を有効にすると AWS アカウント、Macie は現在の でアカウントの AWS Identity and Access Management (IAM) サービスにリンクされたロールを作成します AWS リージョン。このロールのアクセス許可ポリシーにより、Macie はユーザーに代わって他の を呼び出し AWS のサービス 、 AWS リソースをモニタリングできます。このロールを使用することで、Macie は リージョン内の Amazon Simple Storage Service (Amazon S3) 汎用バケットの完全なインベントリを生成し、維持します。Macie は、セキュリティとアクセスコントロールについてバケットをモニタリングおよび評価します。

ユーザーが組織の Macie 管理者である場合、インベントリには、組織内のアカウントとメンバーアカウントの S3 バケットに関する統計およびその他のデータが含まれます。このデータを使用すると、Macie を使用して Amazon S3 データ資産全体の組織のセキュリティ体制をモニタリングおよび評価できます。詳細については、「複数のアカウントの管理」を参照してください。

トピック

- 主要コンポーネント
- データの更新
- 追加の考慮事項

主要コンポーネント

Amazon Macie は、機能と手法を組み合わせて、S3 汎用バケットに関するインベントリデータを提供および維持し、セキュリティとアクセスコントロールのためにバケットをモニタリングおよび評価します。

メタデータの収集と統計の計算

バケットインベントリのメタデータと統計を生成および維持するために、Macie は Amazon S3 からバケットとオブジェクトメタデータを直接取得します。バケットごとに、メタデータには次のものが含まれます。

- バケットの名前、Amazon リソースネーム (ARN)、作成日、暗号化設定、タグ、バケットを所有 AWS アカウント する のアカウント ID など、バケットに関する一般的な情報。
- バケットに適用されるアカウントレベルのアクセス許可設定 (アカウントのブロックパブリックアクセス設定など)。
- バケットのブロックパブリックアクセス設定や、バケットポリシーまたはアクセスコントロールリスト (ACL) から派生する設定など、バケットのバケットレベルのアクセス許可設定。
- バケットデータが組織の一部 AWS アカウント ではない にレプリケートされるか、 と共有されるかなど、バケットの共有アクセスとレプリケーション設定。
- バケット内のオブジェクト数や、暗号化タイプ、ファイルタイプ、ストレージクラス別のオブジェクト数の内訳など、バケット内のオブジェクトのオブジェクト数と設定。

Macie は、この情報を直接ユーザーに提供します。また、Macie はこの情報を使用して統計を計算し、バケットインベントリ全体およびインベントリ内の個別のバケットのセキュリティとプライバシーに関する評価を提供します。たとえば、インベントリ内の合計ストレージサイズとバケットの数、それらのバケット内の合計ストレージサイズとオブジェクトの数、およびバケット内の機密データを検出するために Macie が分析できる合計のストレージサイズとオブジェクトの数を確認できます。

デフォルトでは、メタデータと統計には、マルチパートアップロードが不完全だったために存在するすべてのオブジェクトパーツのデータが含まれます。特定のバケットのオブジェクトメタデータを手動で更新すると、Macie はバケットとバケットインベントリ全体の統計を再計算し、オブジェクトパーツのデータを再計算された値から除外します。Macie が毎日の更新サイクルの一部として Amazon S3 からバケットとオブジェクトメタデータを次回、Macie が取得したときに、Macie はインベントリデータを更新し、オブジェクトパーツのデータを再度含めます。Macie がバケットとオブジェクトのメタデータを取得するタイミングについては、データの更新 を参照してください。

Macie はオブジェクトパーツを分析して機密データを検出することはできないことに注意してください。Amazon S3 はまず、Macie が分析できるように、パーツを 1 つ以上のオブジェクトに組み立てる必要があります。ライフサイクルルールでパーツを自動的に削除する方法など、マルチパートアップロードとオブジェクトパーツについては、Amazon Simple Storage Service ユーザーガイドのマルチパートアップロードを使用したオブジェクトのアップロードとコピーを参照してください。オブジェクトパーツを含むバケットを特定するには、Amazon S3 ストレージレンズの不完全なマルチパートアップロードメトリクスを参照してください。詳細については、Amazon Simple Storage Service ユーザーガイドのストレージのアクティビティと使用状況の評価を参照してください。

バケットのセキュリティとプライバシーのモニタリング

インベントリ内のバケットレベルのデータの精度を確保するために、Macie は、Amazon S3 データで発生する可能性のある特定の AWS CloudTrail イベントをモニタリングして分析します。関連するイベントが発生すると、Macie は適切なインベントリデータを更新します。

例えば、バケットのパブリックアクセスブロック設定を有効にすると、Macie はバケットのパブリックアクセス設定に関するすべてのデータを更新します。同様に、バケットにバケットポリシーを追加したり、バケットのバケットポリシーを更新したりすると、Macie はポリシーを分析し、インベントリ内の関連データを更新します。

Macie は、以下の CloudTrail イベントについてデータをモニタリングおよび分析します。

- アカウントレベルのイベント – DeletePublicAccessBlock および PutPublicAccessBlock
- バケットレベルのイベント – CreateBucket、 DeleteAccountPublicAccessBlock DeleteBucket、DeleteBucketEncryption、 DeleteBucketPolicy、DeleteBucketPublicAccessBlock、DeleteBucketReplication、 DeleteBucketTagging、PutAccountPublicAccessBlock、PutBucketAcl、 PutBucketEncryption PutBucketPolicy、PutBucketPublicAccessBlock PutBucketReplication、 PutBucketTagging、、および PutBucketVersioning

追加の CloudTrail イベントのモニタリングを有効にしたり、前述のイベントのモニタリングを無効にしたりすることはできません。前のイベントの対応するオペレーションの詳細については、Amazon Simple Storage Service API リファレンスを参照してください。

> **Tip**
>
> オブジェクトレベルのイベントをモニタリングするには、Amazon の Amazon S3 保護機能を使用することをお勧めします GuardDuty。この機能は、オブジェクトレベルの Amazon S3 データイベントをモニタリングし、悪意のあるアクティビティや疑わしいア

クティビティについてそれらを分析します。詳細については、「Amazon ユーザーガイド」の「Amazon での Amazon S3 保護 GuardDuty GuardDuty 」を参照してください。

バケットセキュリティとアクセスコントロールの評価

バケットレベルのセキュリティとアクセスコントロールを評価するために、Macie は自動化された論理ベースの推論を使用して、バケットに適用されるリソースベースのポリシーを分析します。Macie は、バケットに適用されるアカウントレベルおよびバケットレベルのアクセス許可設定も分析します。この分析では、アカウントとバケットに対するバケットポリシー、バケットレベル ACL、およびブロックパブリックアクセス設定を考慮します。

リソースベースのポリシーでは 、Macie はZelkova を使用します。Zelkova は、 AWS Identity and Access Management (IAM) ポリシーを論理ステートメントに変換し、決定問題に対して汎用および特殊な論理ソルバー (充足可能性モジュロ理論) のスイートを実行する自動推論エンジンです。Macie は、ポリシーが許可する動作のクラスの特徴を明確にするためのより具体的なクエリを使用して、Zelkova を繰り返しポリシーに適用します。Zelkova が使用するソルバーの性質の詳細については、充足可能性モジュロ理論を参照してください。

Important

バケットに対して前述のタスクを実行するには、バケットが S3 汎用バケットである必要があります。Macie は S3 ディレクトリバケットをモニタリングまたは分析しません。
さらに、Macie はバケットへのアクセスを許可されている必要があります。バケットのアクセス許可設定により、Macie がバケットまたはバケットのオブジェクトのメタデータを取得するのを妨げるようにしている場合、Macie はバケットの名前や作成日など、バケットに関する情報のサブセットのみを提供できます。Macie はバケットに対して追加のタスクを実行できません。詳細については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。

データの更新

で Amazon Macie を有効にすると AWS アカウント、Macie は S3 汎用バケットとオブジェクトのメタデータを Amazon S3 から直接取得します。その後、Macie は毎日の更新サイクルの一環として、バケットとオブジェクトのメタデータを Amazon S3 から直接毎日自動的に取得します。

また、次のいずれかが発生したときに、Macie は Amazon S3 から直接バケットメタデータも取得します。

- インベントリデータを更新するには、Amazon Macie コンソールの更新  を選択します。データは最短で 5 分ごとに更新できます。
- Amazon Macie API にDescribeBucketsリクエストをプログラムで送信し、過去 5 分以内にDescribeBucketsリクエストを送信していない。
- Macie は関連する AWS CloudTrail イベントを検出します。

特定のバケットの最新のオブジェクトメタデータを手動で更新することを選択した場合、Macie はそのデータも取得できます。これは、バケットを最近作成したり、過去 24 時間にバケットのオブジェクトに重要な変更を行った場合に役立ちます。バケットのオブジェクトメタデータを手動で更新するには、コンソールのS3バケットのバケット詳細パネルのオブジェクト統計セクションで更新()を選択します。この機能は、30,000 個以下のオブジェクトを保存するバケットで使用できます。

Macie がバケットまたはオブジェクトメタデータを取得するたびに、Macie はインベントリ内の関連データをすべて自動的に更新します。Macie がバケットのセキュリティやプライバシーに影響を与える違いを検出すると、Macie は直ちに変更の評価と分析を開始します。分析が完了すると、Macie はインベントリ内の関連データを更新します。違いによってバケットのセキュリティやプライバシーが低下した場合、Macie は適切な ポリシーの調査結果を作成して、必要に応じて確認および修正を行います。

Macie が毎日の更新サイクルの一部として、アカウントのバケットとオブジェクトメタデータの両方を最後に取得したタイミングを判断するには、コンソールの 最終更新 フィールドを参照できます。このフィールドは、概要ダッシュボード、S3 バケットページ、および S3 バケットページのバケット詳細パネルに表示されます。(Amazon Macie API を使用してインベントリデータをクエリする場合、`lastUpdated` フィールドに、この情報が表示されます。) ユーザーが組織の Macie 管理者である場合、最終更新 フィールドには、Macie が組織内のアカウントのデータを取得した最も早い日時が示されます。

まれに、特定の条件下で、レイテンシーやその他の問題により、Macie がバケットとオブジェクトメタデータを取得するのを妨げることがあります。また、バケットインベントリへの変更または個別のバケットのアクセス許可設定とポリシーについて Macie が受け取る通知を遅らせる可能性があります。例えば、 CloudTrail イベントで配信の問題が発生すると、遅延が発生する可能性があります。

このような場合、Macie は、次回 (24 時間以内) 毎日の更新を実行するときに、新しいデータと更新されたデータを分析します。

追加の考慮事項

Amazon Macie を使用して Amazon S3 データのセキュリティ体制をモニタリングおよび評価する場合は、次の点に注意してください。

- インベントリデータは、現在の の S3 汎用バケットにのみ適用されます AWS リージョン。追加のリージョンのデータにアクセスするには、追加の各リージョンで Macie を有効化して使用します。
- ユーザーが組織の Macie 管理者である場合は、現在のリージョンでそのアカウントで Macie が有効になっている場合にのみ、メンバーアカウントのインベントリデータにアクセスできます。
- バケットのアクセス許可設定により、Macie がバケットまたはバケットのオブジェクトに関する情報を取得することを妨げた場合、Macie はバケットのデータのセキュリティとプライバシーを評価およびモニタリングしたり、バケットに関する詳細情報を提供したりできません。

  この場合、バケットを特定しやすくするために、Macie は次の処理を行います。

  - バケットインベントリに、Macie はバケットの警告アイコン⚠
    を表示します。バケットの詳細について、Macie はフィールドとデータのサブセットのみを表示します。バケットを所有 AWS アカウント する のアカウント ID、バケットの名前、Amazon リソースネーム (ARN)、作成日、リージョン、および毎日の更新サイクルの一部として Macie がバケットとオブジェクトの両方のメタデータを最後に取得した日時です。Amazon Macie API を使用してインベントリデータをクエリする場合、Macie はバケットのエラーコードとメッセージを提供し、バケットのほとんどのプロパティの値が null になります。
  - 概要ダッシュボードで、バケットはパブリックアクセス、暗号化 、および 共有 統計で 不明の値を持ちます。(Amazon Macie API を使用して統計のクエリを行う場合、バケットはこれらの統計で unknown の値を持ちます。) さらに、Macie は、ストレージ および オブジェクト 統計でのデータの計算時にそのバケットを除外します。

  問題を調査するには、Amazon S3 内のバケットのポリシーとアクセス許可の設定を確認します。たとえば、バケットには制限があるバケットポリシーが設定されている場合があります。詳細については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。
- アクセス権とアクセス許可に関するデータは、アカウントレベルおよびバケットレベルの設定に限定されます。バケット内の特定のオブジェクトへのアクセス権を判断するオブジェクトレベルの設

定は反映されません。たとえば、バケット内の特定のオブジェクトに対してパブリックアクセスが有効になっている場合、Macie はバケットまたはバケットのオブジェクトがパブリックアクセス可能であることをレポートしません。

オブジェクトレベルのオペレーションをモニタリングし、潜在的なセキュリティリスクを特定するには、Amazon の Amazon S3 保護機能を使用することをお勧めします GuardDuty。この機能は、オブジェクトレベルの Amazon S3 データイベントをモニタリングし、悪意のあるアクティビティや疑わしいアクティビティについてそれらを分析します。詳細については、「Amazon ユーザーガイド」の「Amazon での Amazon S3 保護 GuardDuty GuardDuty 」を参照してください。

- 特定のバケットのオブジェクトメタデータを手動で更新すると、Macie は、オブジェクトに適用される暗号化統計で一時的に 不明をレポートします。Macie が次回 (24 時間以内) 毎日のデータ更新を実行するときに、Macie はオブジェクトの暗号化メタデータを再評価し、統計の定量データを再度レポートします。
- 特定のバケットのオブジェクトメタデータを手動で更新すると、Macie はマルチパートアップロードが不完全であるためにバケットに含まれるオブジェクトパーツのデータを一時的に除外します。Macie が次回 (24 時間以内) 毎日のデータ更新を実行するときに、Macie はバケットオブジェクトの数とストレージサイズの値を再計算し、パーツのデータをそれらの計算に含めます。
- まれに、Macie がバケットがパブリックアクセス可能かどうか、共有されているかどうか、または新しいオブジェクトのサーバー側の暗号化が必要であるかどうかを判断できない場合があります。たとえば、一時的な問題により、Macie が必要なデータを取得して分析することを妨げる可能性があります。あるいは、Macie は 1 つ以上のポリシーステートメントが外部エンティティへのアクセスを許可するかどうかを完全には判断できない場合があります。これらのケースでは、Macie はインベントリ内の関連する統計とフィールドで 不明をレポートします これらのケースを調査するには、Amazon S3 内のバケットのポリシーとアクセス許可の設定を確認します。

また、アカウントで Macie を有効にした後にバケットのセキュリティまたはプライバシーが低下した場合にのみ、Macie はポリシーの調査結果を生成することに注意してください。例えば、Macie を有効にした後にバケットのブロックパブリックアクセス設定を無効にすると、Macie はバケットの Policy:IAMUser /S3 BlockPublicAccessDisabled検出結果を生成します。ただし、Macie を有効にしたときにバケットのパブリックアクセスブロック設定が無効になっても無効のままである場合、Macie はバケットの Policy:IAMUser /S3 BlockPublicAccessDisabled検出結果を生成しません。

さらに、Macie がバケットのセキュリティとプライバシーを評価するときに、アクセスログを調べたり、アカウントのユーザー、ロール、その他の関連する設定を分析したりすることはありません。代わりに、Macie は、potential (潜在的な) セキュリティリスクを示す主要な設定についてデータを分析してレポートします。たとえば、ポリシーの調査結果が、バケットがパブリックアクセス可能である

ことを示している場合、それは必ずしも外部エンティティがバケットにアクセスしたことを意味するわけではありません。同様に、ポリシーの検出結果でバケットが組織 AWS アカウント 外の と共有されていることが示された場合、Macie はこのアクセスが意図的で安全かどうかを判断しようとしません。代わりに、これらの調査結果は、外部エンティティがバケットのデータにアクセスできる可能性があることを示しており、意図しないセキュリティリスクになる可能性があります。

Amazon Macie で Amazon S3 のセキュリティ体制を評価する

Amazon Simple Storage Service (Amazon S3) データの全体的なセキュリティ体制を評価し、どこでアクションを実行するかを判断するには、Amazon Macie コンソールの 概要 ダッシュボードを使用できます。

概要 ダッシュボードには、現在の AWS リージョンでの Amazon S3 データの集約された統計のスナップショットが表示されます。統計には、パブリックにアクセス可能である、または他の と共有されている汎用バケットの数など、主要なセキュリティメトリクスのデータが含まれます AWS アカウント。ダッシュボードには、アカウントの集約された調査結果データのグループ (例えば、過去 7 日間の出現の数が最も多い調査結果のタイプ) も表示されます。ユーザーが組織の Macie 管理者である場合、ダッシュボードには、組織内のすべてのアカウントの集約された統計とデータが提供されます。オプションで、アカウント別にデータをフィルタリングすることができます。

詳細な分析を実行するために、ダッシュボード上の個別の項目のサポートデータをドリルダウンして確認できます。Amazon Macie コンソールを使用して S3 バケットインベントリを確認および分析したり、Amazon Macie API の DescribeBucketsオペレーションを使用してインベントリデータをプログラムでクエリおよび分析したりすることもできます。

トピック

- 概要ダッシュボードを表示する
- 概要ダッシュボードのコンポーネントを理解する
- 概要ダッシュボードのデータセキュリティ統計を理解する

概要ダッシュボードを表示する

Amazon Macie コンソールで、概要ダッシュボードには、現在の AWS リージョンでの Amazon S3 データの集約された統計と調査結果データのスナップショットが表示されます。プログラムで統計をクエリする場合は、Amazon Macie API の GetBucketStatisticsオペレーションを使用できます。

サマリーダッシュボードを表示するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 概要を選択します。Macie は 概要ダッシュボードを表示します。
3. Macie がアカウントのバケットとオブジェクトメタデータの両方を最後に取得したタイミングを判断するには、ダッシュボードの上部にある 最終更新 フィールドを参照してください。詳細については、データの更新を参照してください。
4. ダッシュボードで項目のサポートデータをドリルダウンして確認するには、項目を選択します。

ユーザーが組織の Macie 管理者である場合、ダッシュボードには、自分のアカウントと組織内のメンバーアカウントの集約された統計とデータが表示されます。ダッシュボードをフィルタリングし、特定のアカウントのデータのみを表示するには、ダッシュボードの上の Account (アカウント) ボックスにアカウント ID を入力します。

概要ダッシュボードのコンポーネントを理解する

概要ダッシュボードでは、統計とデータがいくつかのセクションに分かれています。ダッシュボードのトップには、Amazon S3 に保存するデータの量と、Amazon Macie が機密データを検出するために分析できるデータの量を示す集約された統計が表示されます。最終更新日フィールドを参照して、Macie がアカウントの Amazon S3 からバケットまたはオブジェクトメタデータを最近取得したタイミングを確認することもできます。その他のセクションでは、現在の AWS リージョンの Amazon S3 データのセキュリティ、プライバシー、機密性を評価するのに役立つ統計と最近の検出結果データを提供します。

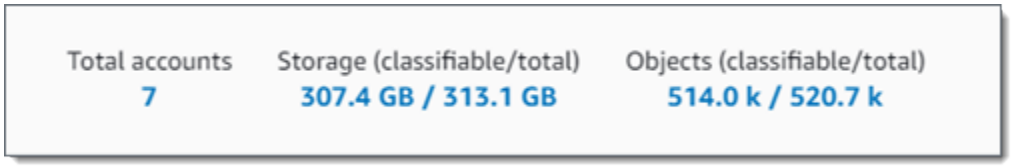
統計とデータは以下のセクションに分かれています。

ストレージと機密データの検出 | 自動検出とカバレッジ問題 | データセキュリティ | トップの S3 バケット | トップの検出結果タイプ | ポリシー検出結果

各セクションを確認するときに、オプションで項目を選択してドリルダウンし、サポートデータを確認します。また、ダッシュボードには S3 ディレクトリバケットのデータが含まれず、汎用バケットのみが含まれることに注意してください。Macie はディレクトリバケットをモニタリングまたは分析しません。

ストレージと機密データ検出

ダッシュボードの上部にある統計は、Amazon S3に保存しているデータの量と、機密データを検出するためにMacieが分析できるデータの量を示しています。例:



このセクションの内容:

- 合計アカウント — このフィールドは、組織の Macie 管理者であるか、スタンドアロンの Macie アカウントを持っている場合に表示されます。これは、バケットインベントリ内のバケットを所有 AWS アカウント する の合計数を示します。Macie 管理者の場合、これは組織で管理している Macie アカウントの総数です。スタンドアロンの Macie アカウントをお持ちの場合、この値は 1 です。

  S3 バケットの合計 — このフィールドは、Macie アカウントが組織のメンバーである場合に表示されます。オブジェクトを保存しないバケットを含め、インベントリ内の汎用バケットの合計数を示します。

- ストレージ — これらのメトリクスは、バケットインベントリ内のオブジェクトのストレージサイズに関する情報を提供します。
  - 分類可能 – バケット内で Macie が分析できるすべてのオブジェクトの合計ストレージサイズ。
  - 合計— Macie が分析できないオブジェクトを含む、バケット内のすべてのオブジェクトの合計ストレージサイズ。

  いずれかのオブジェクトが圧縮ファイルである場合、これらの値は解凍後のファイルの実際のサイズを反映しません。いずれかのバケットでバージョニングが有効化されている場合、これらの値は、それらのバケット内の各オブジェクトの最新バージョンのストレージサイズに基づきます。

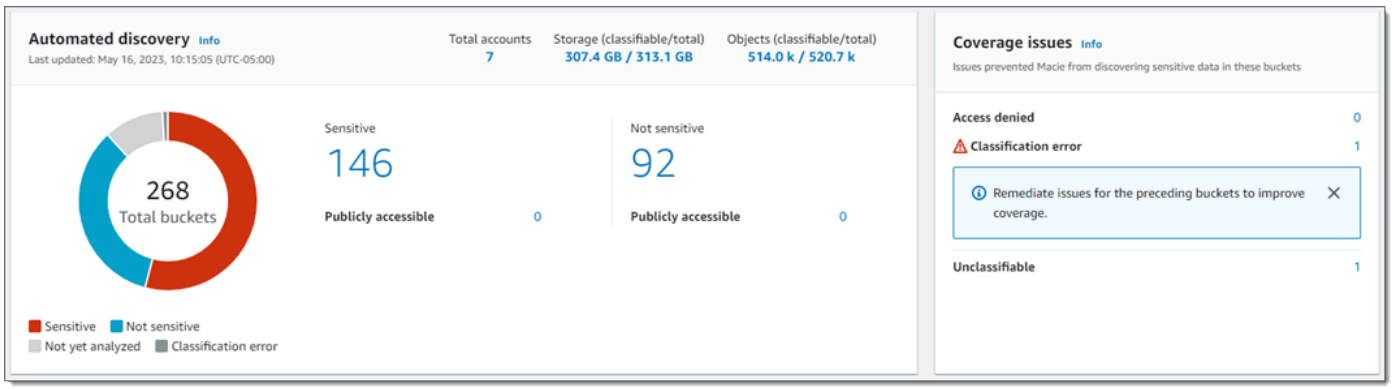
- オブジェクト — これらのメトリクスは、バケットインベントリ内のオブジェクト数に関する情報を提供します。
  - 分類可能 - バケット内で Macie が分析できるオブジェクトの合計数。
  - 合計— Macie が分析できないオブジェクトを含む、バケット内のオブジェクトの総数。

前述の統計では、データとオブジェクトは、サポートされているAmazon S3ストレージクラスを使用し、サポートされているファイルまたはストレージフォーマットのファイル名拡張子を持っている場合、分類可能です。Macie を使用して、オブジェクト内の機密データを検出できます。詳細については、サポートされているストレージクラスとフォーマットを参照してください。

ストレージ と オブジェクト の統計には、Macie がアクセスするのを許可されていないバケット内のオブジェクトに関するデータは含まれないことに注意してください。例えば、制限の厳しいバケットポリシーが適用されているバケット内のオブジェクトなどです。これが当てはまるバケットを特定するには、(バケットインベントリを確認できます。警告アイコン⚠
がインベントリ内のバケット名の横に表示される場合、Macie はバケットへのアクセスが許可されていません。

自動検出 と カバレッジ問題

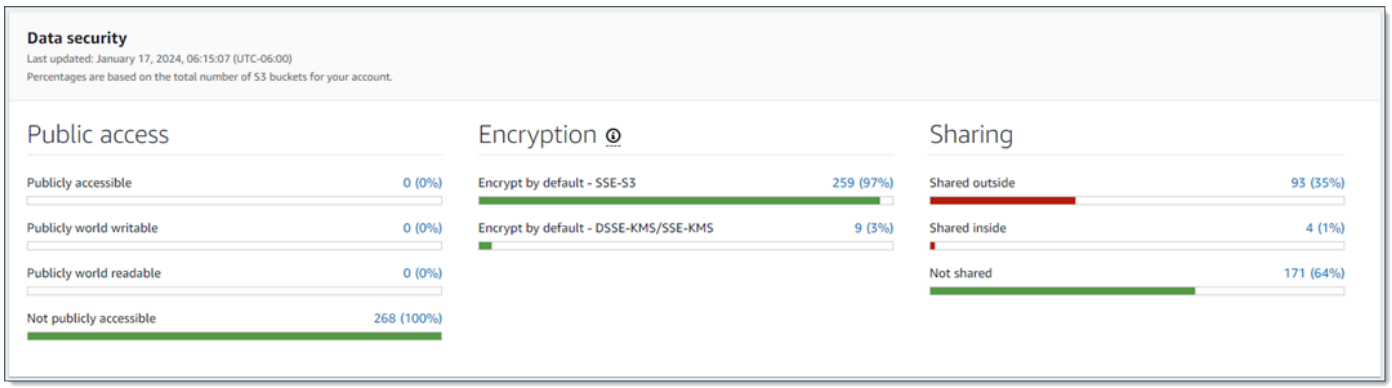
機密データの自動検出が有効になっている場合、これらのセクションはダッシュボードに表示されます。これらのセクションの統計には、Macie がこれまで Amazon S3 データに対して実行した機密データ自動検出アクティビティのステータスと結果がキャプチャされます。例:



これらの統計の詳細については、[概要ダッシュボードの集約されたデータ機密性統計を確認する]を参照してください。

データセキュリティ

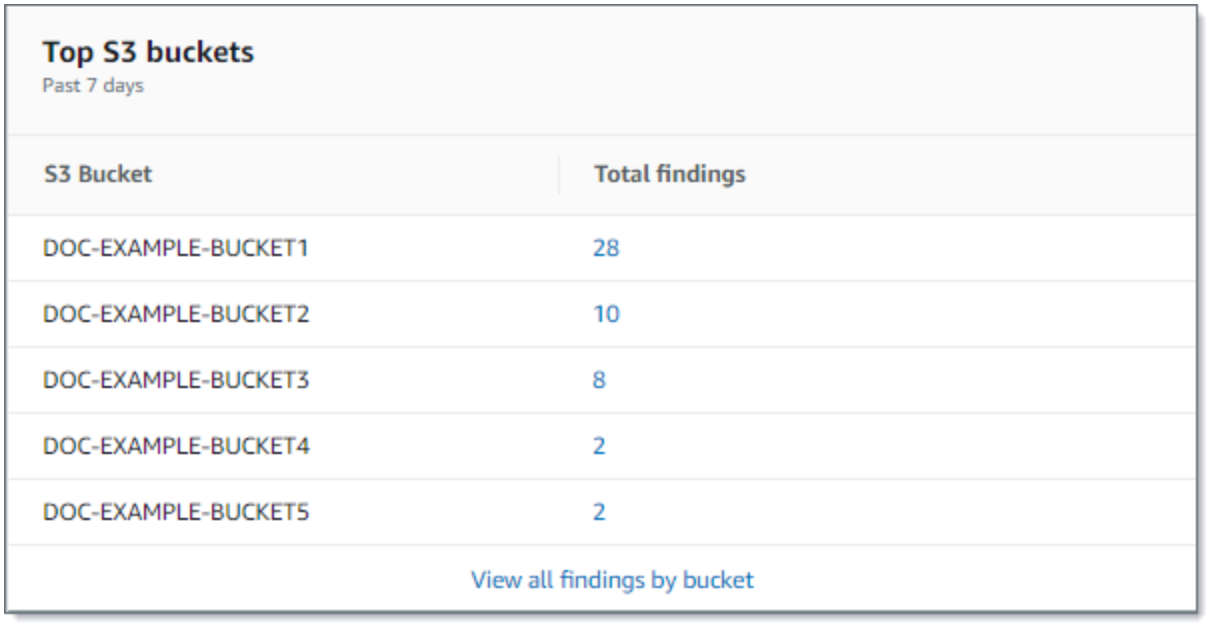
このセクションでは、Amazon S3 データの潜在的なセキュリティおよびプライバシーリスクを示す統計も提供します。例:



これらの統計の詳細については、概要ダッシュボードのデータセキュリティ統計を理解するを参照してください。

トップの S3 バケット

このセクションでは、過去 7 日間に任意のタイプの最も多くの調査結果を生成した S3 バケットを、最大 5 つのバケットについてリスト化します。また、Macie がバケットごとに作成した調査結果の数も示します。例:

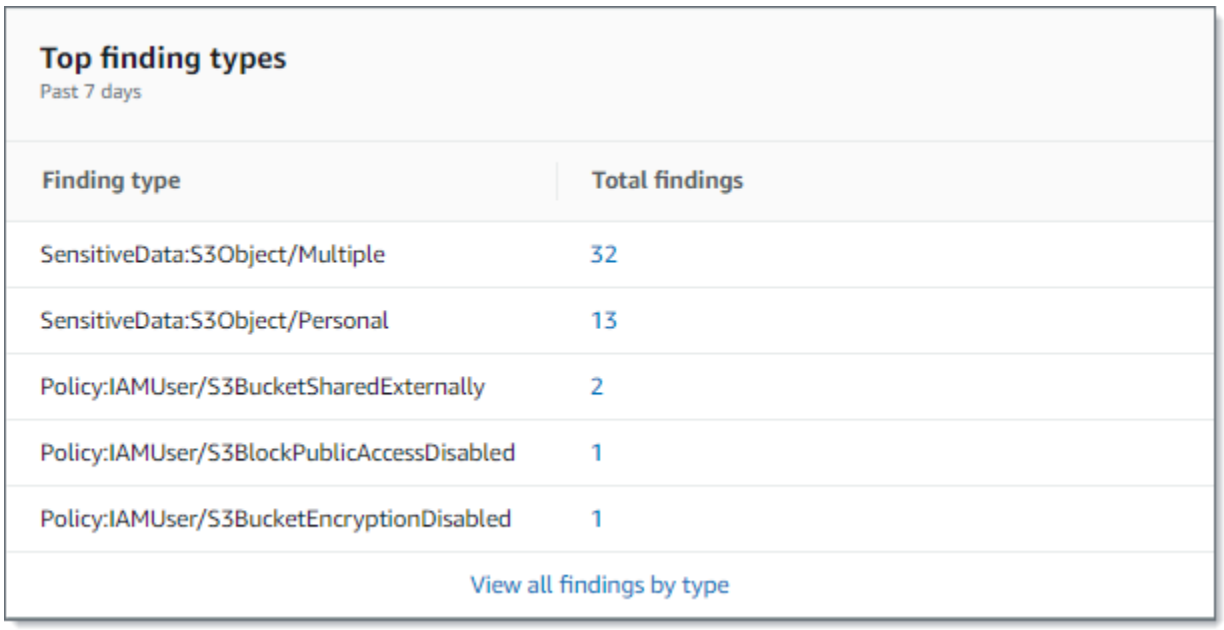


過去 7 日間のバケットのすべての調査結果を表示し、オプションでドリルダウンするには、合計調査結果 フィールドの値を選択します。バケットごとにグループ化された、すべてのバケットの現在の調査結果をすべて表示するには、バケットごとにすべての調査結果を表示 を選択します。

Macie が過去 7 日間に調査結果を作成しなかった場合、このセクションは空になります。または、過去 7 日間に作成されたすべての検出結果が、抑制ルールによって非表示にされました。

トップの調査結果タイプ

このセクションでは、過去 7 日間に最も多くの出現の数があった 調査結果のタイプ を、最大 5 つの調査結果のタイプについてリスト化します。また、Macie がタイプごとに作成した調査結果の数も示します。例:



過去 7 日間の特定のタイプのすべての調査結果を表示し、オプションでドリルダウンするには、合計調査結果 フィールドの値を選択します。調査結果タイプごとにグループ化された、現在の調査結果をすべて表示するには、タイプごとにすべての調査結果を表示 を選択します。

Macie が過去 7 日間に調査結果を作成しなかった場合、このセクションは空になります。または、過去 7 日間に作成されたすべての検出結果が、抑制ルールによって非表示にされました。

ポリシーの調査結果

このセクションでは、Macie が最後に作成または更新した ポリシーの調査結果 を、最大 10 件の調査結果についてリスト化します。例:

特定の調査結果の詳細を表示するには、調査結果を選択します。

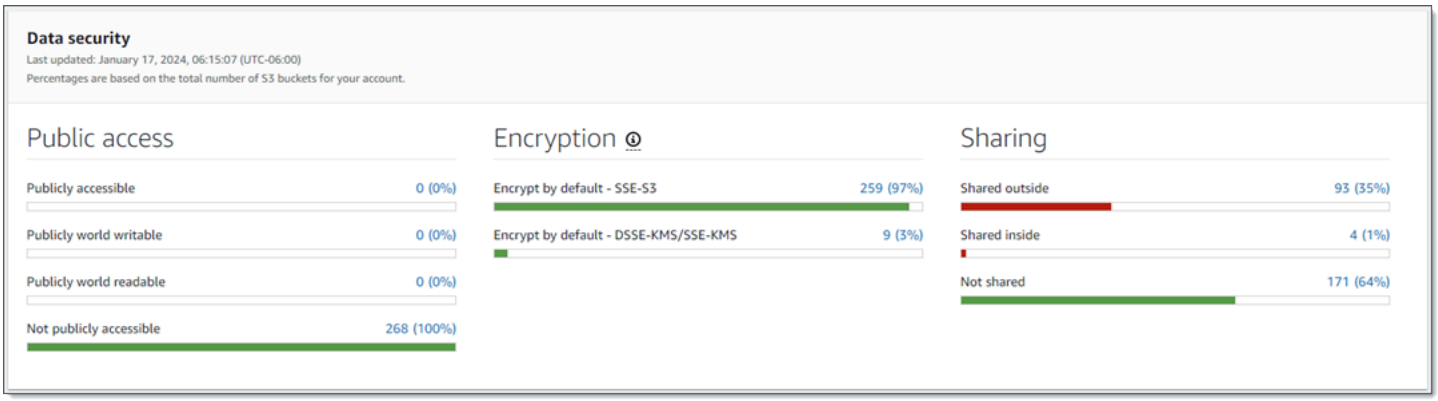
Macie が過去 7 日間にポリシーの調査結果を作成または更新しなかった場合、このセクションは空になります。または、過去 7 日間に作成または更新されたすべてのポリシー検出結果が、抑制ルールによって非表示にされました。

概要ダッシュボードのデータセキュリティ統計を理解する

概要 ダッシュボードの [データセキュリティ] セクションには、現在の AWS リージョンの Amazon S3 データの潜在的なセキュリティリスクとプライバシーリスクを特定して調査するのに役立つ統計情報が提供されます。例えば、このデータを使用して、パブリックにアクセス可能である、または他の と共有されている汎用バケットを識別できます AWS アカウント。

Macie アカウントが組織のメンバーである場合、このセクションの上部にあるストレージと機密データ検出の統計に、Amazon S3 に保存するデータの量と、Macie が機密データを検出するために分析できるデータの量が表示されます。

Macie アカウントのタイプを問わず、以下のイメージで示すように、追加の統計は 3 つの領域に整理されています。



各領域を確認するときは、必要に応じて項目を選択してドリルダウンし、サポートデータを確認します。また、統計には S3 ディレクトリバケットのデータが含まれず、汎用バケットのみが含まれることに注意してください。Macie はディレクトリバケットをモニタリングまたは分析しません。

各エリアの個別の統計は以下のとおりです。

パブリックアクセス

これらの統計では、パブリックアクセス可能、または可能でない S3 バケットの数を示します。

- パブリックアクセス可能 — 一般ユーザーがバケットへの読み取りまたは書き込みアクセス権を持つことを許可するバケットの数とパーセンテージ。
- パブリックワールド書き込み可能 — 一般ユーザーがバケットへの書き込みアクセス権を持つことを許可するバケットの数とパーセンテージ。
- パブリックワールド読み取り可能 — 一般ユーザーがバケットへの読み取りアクセス権を持つことを許可するバケットの数とパーセンテージ。

- パブリックアクセス可能でない — 一般ユーザーがバケットへの読み取りまたは書き込みアクセス権を持つことを許可しないバケットの数とパーセンテージ。

各パーセンテージを計算するために、Macie は該当するバケットの数をバケットインベントリ内のバケットの総数で割ります。

このセクションの値を決定するために、Macie は各バケットのアカウントレベルとバケットレベルの設定、アカウントのブロックパブリックアクセスの設定、バケットのブロックパブリックアクセスの設定、バケットのバケットポリシー、およびバケットのアクセスコントロールリスト (ACL) の組み合わせを分析します。これらの設定の詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 での Identity and access managementとAmazon S3 ストレージへのパブリックアクセスのブロックを参照してください。

場合によっては、パブリックアクセスセクションにも不明の値が表示されます。これらの値が表示された場合、Macie は指定されたバケットの数とパーセンテージについて、パブリックアクセス設定を評価できませんでした。例えば、一時的な問題やバケットのアクセス許可設定により、Macie は必要なデータの取得を妨げられました。あるいは、Macie は 1 つ以上のポリシーステートメントが外部エンティティのバケットへのアクセスを許可するかどうかを完全には判断できませんでした。

暗号化

これらの統計は、バケットに追加されたオブジェクトに特定のタイプのサーバー側暗号化を適用するように設定されている S3 バケットの数を示しています。

- デフォルトで暗号化 — SSE-S3 — Amazon S3 マネージドキーを使用して新しいオブジェクトを暗号化するようにデフォルトの暗号化設定が設定されているバケットの数と割合。これらのバケットでは、新しいオブジェクトは SSE-S3 暗号化を使用して自動的に暗号化されます。
- デフォルトで暗号化 – DSSE-KMS/SSE-KMS – デフォルトの暗号化設定が AWS マネージドキー またはカスタマーマネージドキー AWS KMS keyを使用して新しいオブジェクトを暗号化するように設定されたバケットの数と割合。これらのバケットでは、新しいオブジェクトは DSSE-KMS または SSE-KMS 暗号化を使用して自動的に暗号化されます。

各パーセンテージを計算するために、Macie は該当するバケットの数をバケットインベントリ内のバケットの総数で割ります。

このセクションの値を決定するために、Macie は各バケットのデフォルトの暗号化設定を分析します。2023 年 1 月 5 日以降、Amazon S3 はバケットに追加されるオブジェクトに対して、基本レベルの暗号化として Amazon S3 管理キー (SSE-S3) によるサーバーサイド暗号化を自動的に適用します。オプションで、 キーによるサーバー側の暗号化 (SSE-KMS) または AWS KMS

キーによる二層式サーバー側の暗号化 AWS KMS (DSSE-KMS) を使用するようにバケットのデフォルトの暗号化設定を設定できます。デフォルトの暗号化設定とオプションの詳細については、Amazon Simple Storage Service ユーザーガイドのS3 バケットのデフォルトのサーバー側の暗号化動作の設定を参照してください。

場合によっては、このセクションには不明の値も表示されます。これらの値が表示された場合、Macie は指定されたバケットの数とパーセンテージについて、デフォルトの暗号化設定を評価できませんでした。例えば、一時的な問題やバケットのアクセス許可設定により、Macie は必要なデータの取得を妨げられました。

共有中

これらの統計は、他の 、Amazon CloudFront オリジンアクセスアイデンティティ (OAI) AWS アカウント、またはオリジンアクセスコントロール (OACs) と共有されている、または CloudFront 共有されていない S3 バケットの数を示します。 OAIs

- 外部で共有 — OAI、 CloudFront OAC、 CloudFrontまたは同じ組織外のアカウントのいずれかまたは組み合わせで共有されているバケットの数と割合。
- 内部で共有 — 同じ組織内のアカウントと共有されているバケットの数とパーセンテージ。これらのバケットは CloudFront OAIs または OACs と共有されません。
- Not shared – 他のアカウント、 CloudFront OAIs、または CloudFront OACs と共有されていないバケットの数と割合。

各パーセンテージを計算するために、Macie は該当するバケットの数をバケットインベントリ内のバケットの総数で割ります。

バケットが他の と共有されているかどうかを判断するために AWS アカウント、Macie は各バケットのバケットポリシーと ACL を分析します。さらに、組織は、 を通じて、 AWS Organizations または Macie の招待によって関連アカウントのグループとして一元管理される一連の Macie アカウントとして定義されます。Amazon S3 のバケット共有のオプションの詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 での Identity and Access Managementを参照してください。

> **Note**
>
> 場合によっては、同じ組織に所属していない AWS アカウント とバケットが共有されていると Macie が誤って報告することがあります。これは、Macie がバケットポリシー内の `Principal` 要素と、ポリシーの `Condition` 要素内の特定のAWS グローバル条件コンテキストキーまたは Amazon S3 条件キーとの関係を完全に評価できない場合に発生する可能性があります。適用可能な条件キー

はaws:PrincipalAccount、、aws:PrincipalArn、aws:PrincipalOrgID、aws:Princip
および aws:SourceVpce aws:useridですs3:DataAccessPointArn。
個々のバケットに当てはまるかどうかを判断するには、ダッシュボードの 外部共有 統計を選択します。テーブルには、各バケットの名前を書き留めることが表示されます。次に、Amazon S3 を使用して各バケットのポリシーを確認し、共有アクセス設定が意図的で安全かどうかを判断します。

バケットが CloudFront OAIs または OACs、Macie は各バケットのバケットポリシーを分析します。 CloudFront OAI または OAC を使用すると、ユーザーは 1 つ以上の指定された CloudFront ディストリビューションを介してバケットのオブジェクトにアクセスできます。 CloudFront OAIs と OACs」を参照してください。 Amazon S3 CloudFront

場合によっては、このセクションには不明の値も表示されます。これらの値が表示される場合、Macie は指定されたバケットの数と割合が他のアカウント、 CloudFront OAIs、または CloudFront OACs と共有されているかどうかを判断できませんでした。例えば、一時的な問題やバケットのアクセス許可設定により、Macie は必要なデータの取得を妨げられました。あるいは、Macie はバケットのポリシーまたは ACL を完全に評価できませんでした。

Amazon Macie で Amazon S3 のセキュリティ体制を分析する

Amazon Simple Storage Service (Amazon S3) データの詳細な分析とセキュリティ体制の評価に役立つように、Amazon Macie は Macie AWS リージョン を使用する各 で S3 汎用バケットの完全なインベントリを保持します。Macie がこのインベントリを維持する方法については、Macie が Amazon S3 データセキュリティをモニタリングする方法を参照してください。ユーザーが組織の Macie 管理者である場合、インベントリには、メンバーアカウントが所有する S3 バケットのデータが含まれます。

このインベントリを使用すると、Amazon S3 のデータ資産を確認し、個別の S3 バケットに適用される主要なセキュリティ設定とメトリクスの詳細と統計を調べることができます。たとえば、各バケットのパブリックアクセスと暗号化設定の内訳、および各バケット内の機密データを検出するために Macie が分析できるオブジェクトのサイズと数にアクセスできます。また、バケット内のオブジェクトを分析するために機密データ検出ジョブまたは機密データ自動検出を設定しているかどうかも判断できます。存在する場合、インベントリデータは、その分析が最後に発生した日時を示します。機密データの自動検出が有効になっている場合は、インベントリを使用して、Macie がこれまで Amazon S3 データに対して実行した機密データ自動検出アクティビティの結果を確認することもできます。詳細については、「機密データの検出」を参照してください。

Amazon Macie コンソールの S3 バケットページを使用して、インベントリデータを参照、並べ替え、フィルタリングできます。Amazon Macie API の DescribeBucketsオペレーションを使用して、インベントリデータにプログラムでアクセスすることもできます。

トピック

- Amazon Macie で S3 バケットインベントリを確認する
- Amazon Macie で S3 バケットインベントリをフィルタリングする

Amazon Macie で S3 バケットインベントリを確認する

Amazon MacieコンソールのS3バケットページでは、現在の AWS リージョンのAmazon Simple Storage Service (Amazon S3)データのセキュリティとプライバシーに関する詳細な洞察を提供します。このページでは、リージョン内の S3 汎用バケットの完全なインベントリを確認および分析し、個々のバケットの詳細情報と統計を確認できます。ユーザーが組織の Macie 管理者である場合、インベントリには、メンバーアカウントが所有する S3 バケットの詳細と統計が含まれます。

S3 バケットページには、Macie が毎日の更新サイクルの一部として、アカウントのバケットとオブジェクトメタデータの両方を最後に取得したタイミングも示されます。この情報は、ページの上部の 最終更新フィールドにあります。ユーザーが組織の Macie 管理者である場合、最終更新フィールドには、Macie が組織内のアカウントのデータを取得した最も早い日時が示されます。詳細については、「データの更新」を参照してください。

インベントリデータと統計には、S3 ディレクトリバケットに関するデータはなく、汎用バケットのみが含まれることに注意してください。Macie はディレクトリバケットをモニタリングまたは分析しません。さらに、ほとんどのインベントリデータは、Macie がアカウントに対してアクセスを許可されているバケットに限定されます。バケットのアクセス許可設定により、Macie がバケットまたはバケットのオブジェクトに関する情報を取得するのを妨げるようにしている場合、Macie はバケットに関する情報のサブセットのみを提供できます。これが特定のバケットに当てはまる場合、Macie はバケットインベントリに警告アイコン⚠ とメッセージを表示します。バケットの詳細では、Macie は以下のフィールドとデータのサブセットのみを表示します: バケットを所有する AWS アカウント のアカウント ID、バケットの名前、Amazon リソースネーム (ARN)、作成日、リージョン、および毎日の更新サイクルの一部として Macie がバケットとオブジェクトメタデータの両方を最後に取得したタイミング。問題を調査するには、Amazon S3 内のバケットのポリシーとアクセス許可の設定を確認します。例えば、バケットには制限があるバケットポリシーが設定されている場合があります。詳細については、「Macie が S3 バケットおよびオブジェクトにアクセスすることを許可する」を参照してください。

プログラムでインベントリデータにアクセスしてクエリを実行する場合は、Amazon Macie API の DescribeBuckets オペレーションを使用できます。

トピック

- S3 バケットインベントリを確認する
- S3 バケットの詳細を確認する

S3 バケットインベントリを確認する

Amazon Macie コンソールの S3 バケットページには、現在の の S3 汎用バケットに関する情報が表示されます AWS リージョン。このページでは、インベントリ内の各バケットの概要情報がテーブルに表示されます。ビューをカスタマイズするには、テーブルを並べ替えてフィルタリングします。テーブルでバケットを選択すると、詳細パネルにバケットに関する追加情報が表示されます。これには、バケットのデータのセキュリティとプライバシーに関する洞察を提供する設定とメトリクスの詳細と統計が含まれます。オプションで、データをテーブルからカンマ区切り値 (CSV) ファイルにエクスポートできます。

機密データの自動検出が有効になっている場合は、インタラクティブなヒートマップを使用してインベントリを確認するオプションもあります。このマップは、Amazon S3 データ資産全体のデータ機密性を視覚的に表しています。Macie がこれまでに実行した機密データ自動検出アクティビティの結果をキャプチャします。このマップの詳細については、S3 バケットマップによるデータ機密性の視覚化を参照してください。

S3 バケットインベントリを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで、S3 バケットを選択します。S3 バケットページにはバケットインベントリが表示されます。ページにインベントリのインタラクティブマップが表示されている場合は、ページの上部にあるテーブル () を選択します。S3 バケットページが開き、インベントリ内のバケットの数とバケットのテーブルが表示されます。

   自動機密データ検出が有効になっている場合、デフォルトビューには、現在自動検出から除外されているバケットのデータが表示されません。このデータを表示するには、フィルターボックスの下にある自動検出フィルタートークンによってモニタリングされている で X を選択します。

3. ページの上部で、必要に応じて、更新

を選択して、Amazon S3 から最新のバケットメタデータを取得します。

情報アイコン が バケット名の横に表示された場合、これを行うことをお勧めします。このアイコンは、Macie が毎日の更新サイクルの一部として Amazon S3 からバケットとオブジェクトメタデータをおそらく最後に取得した後の過去 24 時間にバケットが作成されたことを示します。

4. S3 バケットページで、テーブルを使用して、インベントリ内の各バケットに関する情報のサブセットを確認します。

- 機密性 — バケットの現在の機密性スコア。この列は、機密データの自動検出が有効になっている場合にのみ表示されます。Macie が定義する機密性スコアの範囲については、S3 バケットの機密スコアを参照してください。
- バケット — バケットの名前。
- アカウント— バケットを所有している AWS アカウント のアカウント ID。
- 分類可能なオブジェクト– バケット内の機密データを検出するために Macie が分析できるオブジェクトの総数。
- 分類可能なサイズ– バケット内の機密データを検出するために Macie が分析できるすべてのオブジェクトの合計ストレージサイズ。

  この値は、圧縮解除後の圧縮オブジェクトの実際のサイズを反映していないことに注意してください。また、バケットでバージョニングが有効化されている場合、この値は、バケット内の各オブジェクトの最新バージョンのストレージサイズに基づきます。
- ジョブによるモニタリング- 機密データ検出ジョブがバケット内のオブジェクトを毎日、毎週、または毎月ベースで定期的に分析するように設定されているかどうか。

  このフィールドの値が はいの場合、バケットが定期的なジョブに明示的に含まれるか、バケットが過去 24 時間以内の定期的なジョブの基準に一致したことになります。さらに、それらのジョブの少なくとも 1 つのステータスは キャンセルされません。Macie は毎日ベースでこのデータを更新します。
- 最新のジョブ実行 — バケット内のオブジェクトを分析するように 1 回限りまたは定期的な機密データ検出ジョブが設定されている場合、このフィールドには、それらのジョブのいずれかの実行が開始された最新の日時が表示されます。それ以外の場合は、このフィールドにダッシュ (–) が表示されます。

前述のデータでは、オブジェクトは、サポートされているAmazon S3のストレージクラスを使用し、サポートされているファイルまたはストレージフォーマットのファイル名拡張子を持っていれば、分類可能です。Macie を使用して、オブジェクト内の機密データを検出できます。詳細については、サポートされているストレージクラスとフォーマットを参照してください。

5. テーブルを使用してインベントリを分析するには、次のいずれかの操作を行います。

   - 特定のフィールドでテーブルをソートするには、フィールドの列見出しを選択します。ソート順序を変更するには、列見出しを再度選択します。
   - テーブルをフィルタリングし、フィールドに対して特定の値を持つバケットのみを表示するには、フィルターボックスにカーソルを置き、フィールドでフィルター条件を追加します。結果をさらに絞り込むには、追加のフィールドでフィルター条件を追加します。詳細については、S3 バケットインベントリをフィルタリングするを参照してください。

6. 特定のバケットの詳細と統計を確認するには、テーブルでバケットの名前を選択し、詳細パネルを参照します。

   > **Tip**
   >
   > バケット詳細パネルでは、多くのフィールドをピボットしてドリルダウンできます。フィールドに対して同じ値を持つバケットを表示するには、フィールドで
   >
   > を選択します。フィールドに対して他の値を持つバケットを表示するには、フィールドで
   >
   > を選択します。

7. テーブルから CSV ファイルにデータをエクスポートするには、エクスポートする各行のチェックボックスを選択するか、選択列見出しのチェックボックスを選択してすべての行を選択します。次に、ページ上部の CSV にエクスポートを選択します。テーブルから最大 50,000 行をエクスポートできます。

S3 バケットの詳細を確認する

Amazon Macie コンソールでは、S3 バケットページの詳細パネルを使用して、S3 バケットS3インベントリ内の各汎用バケットに関する統計やその他の情報を確認できます。これには、バケットの

データのセキュリティとプライバシーに関する洞察を提供する設定とメトリクスの詳細と統計が含まれます。

たとえば、S3 バケットのパブリックアクセス設定の内訳を確認し、バケットがオブジェクトをレプリケートするように設定されているか、他の AWS アカウントと共有するかを判断できます。また、機密データ検出ジョブがバケット内の機密データを検査するように設定されているかどうかを判断することもできます。存在する場合は、最後に実行されたジョブに関する詳細にアクセスし、必要に応じてジョブが生成した調査結果を表示できます。

機密データの自動検出が有効になっている場合は、詳細パネルを使用して、機密データ検出統計や個々の S3 バケットに関するその他の情報を確認することもできます。このパネルには、Macie がこれまでにバケットに対して行った機密データ自動検出アクティビティの結果がキャプチャされます。これらの詳細については、個々の S3 バケットのデータ機密情報の確認を参照してください。

S3 バケットの詳細を確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで、S3 バケットを選択します。S3 バケットページにはバケットインベントリが表示されます。

   自動機密データ検出が有効になっている場合、デフォルトビューには、現在自動検出から除外されているバケットのデータが表示されません。このデータを表示するには、フィルターボックスの下にある自動検出フィルタートークンによってモニタリングされている で X を選択します。
3. ページの上部で、必要に応じて、更新 
   を選択して、Amazon S3 から最新のバケットメタデータを取得します。
4. 詳細を確認するバケットを選択します。詳細パネルには、バケットに関する統計およびその他の情報が表示されます。

詳細パネルでは、統計と情報が次の主要セクションにまとめられています。

概要| オブジェクト統計| サーバー側の暗号化| 機密データ検出| パブリックアクセス| レプリケーション| タグ

各セクションの情報を確認するときに、必要に応じて特定のフィールドをピボットしてドリルダウンできます。フィールドに対して同じ値を持つバケットを表示するには、フィールドで 

を選択します。フィールドに対して他の値を持つバケットを表示するには、フィールドで

を選択します。

概要

このセクションでは、バケットの名前、バケットの作成日時、バケットを所有 AWS アカウント する のアカウント ID など、バケットに関する一般的な情報を提供します。特に、最終更新フィールドは、Macie がバケットまたはバケットのオブジェクトのメタデータを Amazon S3 から取得した日時を示します。

共有アクセスフィールドは、バケットが別の 、Amazon CloudFront オリジンアクセスアイデンティティ (OAI) AWS アカウント、または CloudFront オリジンアクセスコントロール (OAC) と共有されているかどうかを示します。

- 外部 – バケットは、OAI、 CloudFront OCloudFront AC、または組織の外部 (一部ではない) アカウントのいずれかまたは組み合わせと共有されます。
- 内部 — バケットは組織の内部にある (一部である) 1 つ以上のアカウントと共有されます。CloudFront OAI または OAC と共有されません。
- 共有なし — バケットは別のアカウント、 CloudFront OAI、または CloudFront OAC と共有されません。
- 不明— Macie はバケットの共有アクセス設定を評価できませんでした。

バケットが別の と共有されているかどうかを判断するために AWS アカウント、Macie はバケットのバケットポリシーとアクセスコントロールリスト (ACL) を分析します。分析はバケットレベルの設定に制限されます。特定のオブジェクトをバケット内で共有するためのオブジェクトレベルの設定は反映されません。さらに、組織は、 を通じて、 AWS Organizations または Macie の招待によって関連アカウントのグループとして一元管理される一連の Macie アカウントとして定義されます。バケット共有の Amazon S3 オプションの詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 での Identity and Access Managementを参照してください。

> **Note**
>
> 場合によっては、Macie はバケットが組織の外部 (一部ではない) AWS アカウント と共有されていると誤って指摘することがあります。これは、Macie がバケットポリシー内の `Principal` 要素と、ポリシーの `Condition` 要素内の特定のAWS グローバル条件コンテキストキーまたは Amazon S3 条件キーとの関係

を完全に評価できない場合に発生する可能性があります。適用可能な条件キーはaws:PrincipalAccount、、aws:PrincipalArn、aws:PrincipalOrgID、aws:PrincipalOおよび ですs3:DataAccessPointArn。バケットポリシーを確認して、このアクセスが安全かつ意図されたものか判断することをお勧めします。

バケットが CloudFront OAI または OAC と共有されているかどうかを判断するために、Macie はバケットのバケットポリシーを分析します。 CloudFront OAI または OAC を使用すると、ユーザーは 1 つ以上の指定された CloudFront ディストリビューションを介してバケットのオブジェクトにアクセスできます。 CloudFront OAIs と OACs」を参照してください。 Amazon S3 CloudFront

概要セクションには、最新の自動検出実行フィールドも含まれています。このフィールドは、Macie が機密データの自動検出を実行中にバケット内のオブジェクトを最後に分析した日時を示します。この分析が行われていない場合は、このフィールドにダッシュ (–) が表示されます。

オブジェクト統計

このセクションではバケット内のオブジェクトに関する情報を提供し、それはバケット内のオブジェクトの総数 (合計数)、それらのすべてのオブジェクトの合計ストレージサイズ (合計ストレージサイズ)、および圧縮されたすべてのオブジェクト (.gz、.gzip、または.zip) の合計ストレージサイズ (合計圧縮サイズ) から始まります。このセクションの追加統計は、Macie がバケット内の機密データを検出するために分析できるデータの量を評価するのに役立ちます。

最近バケットを作成した場合、または過去 24 時間の間にバケットのオブジェクトに大きな変更を加えた場合は、必要に応じて更新 を選択して、バケットのオブジェクトの最新のメタデータを取得します。Macie は、これが当てはまるかどうかを判断するのに役立つように、情報アイコン を表示します。更新オプションは、バケットが 30,000 個以下のオブジェクトを保存する場合に使用できます。

このセクションの統計を確認する際には、以下の点に注意してください。

- バケットでバージョニングが有効化されている場合、サイズ値はバケット内の各オブジェクトの最新バージョンのストレージサイズに基づきます。
- バケットに圧縮オブジェクトが保存されている場合、サイズ値は解凍後のオブジェクトの実際のサイズを反映しません。

- バケットのオブジェクトメタデータを更新すると、Macie は、オブジェクトに適用される暗号化統計で一時的に 不明をレポートします。Macie はバケットとオブジェクトメタデータの次回 (24 時間以内) の毎日の更新を実行するときに、これらの統計のデータを再評価して更新します。
- デフォルトでは、オブジェクト数とサイズの値には、マルチパートアップロードが不完全だったためにバケットに含まれるすべてのオブジェクトパーツのデータが含まれます。バケットのオブジェクトメタデータを更新すると、Macie はオブジェクトパーツのデータを再計算された値から除外します。Macie が次の毎日のバケットとオブジェクトメタデータの更新を行うと (24 時間以内)、Macie はこれらの統計の値を再計算して更新し、オブジェクトパーツのデータを値に再び含めます。

  Macie はオブジェクトパーツを分析して機密データを検出することはできないことに注意してください。Amazon S3 はまず、Macie が分析できるように、パーツを 1 つ以上のオブジェクトに組み立てる必要があります。ライフサイクルルールでパーツを自動的に削除する方法など、マルチパートアップロードとオブジェクトパーツについては、Amazon Simple Storage Service ユーザーガイドのマルチパートアップロードを使用したオブジェクトのアップロードとコピーを参照してください。オブジェクトパーツを含むバケットを特定するには、Amazon S3 ストレージレンズの不完全なマルチパートアップロードメトリクスを参照してください。詳細については、Amazon Simple Storage Service ユーザーガイドのストレージのアクティビティと使用状況の評価を参照してください。

オブジェクト統計は次のように設定されています。

分類可能なオブジェクト

このセクションは、Macie が機密データを検出するために分析できるオブジェクトの総数と、それらのオブジェクトの合計ストレージサイズを示します。前のデータでは、オブジェクトがサポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を持っている場合、オブジェクトは 分類可能です。Macie を使用して、オブジェクト内の機密データを検出できます。詳細については、サポートされているストレージクラスとフォーマットを参照してください。

分類不可能オブジェクト

このセクションは、Macie が機密データを検出するために分析できないオブジェクトの総数と、それらのオブジェクトの合計ストレージサイズを示します。これらのオブジェクトは、サポートされている Amazon S3 ストレージクラスを使用せず、サポートされているファイルまたはストレージ形式のファイル名拡張子も持っていません。

分類不可能オブジェクト: ストレージクラス

このセクションでは、オブジェクトがサポートされている Amazon S3 ストレージクラスを使用しないため、Macie が分析できないオブジェクトの数とストレージサイズの内訳を示します。

分類不可能オブジェクト: ファイルタイプ

このセクションでは、オブジェクトがサポートされているファイルまたはストレージ形式のファイル名拡張子を持っていないため、Macie が分析できないオブジェクトの数とストレージサイズの内訳を示します。

暗号化タイプ別のオブジェクト

このセクションでは、Amazon S3 がサポートする各タイプの暗号化を使用するオブジェクトの数の内訳を示します。

- 顧客提供 – 顧客提供のキーで暗号化されたオブジェクトの数。これらのオブジェクトは SSE-C 暗号化を使用します。
- AWS KMS マネージド – AWS マネージドキー またはカスタマーマネージドキー AWS KMS keyのいずれかで暗号化されたオブジェクトの数。これらのオブジェクトは DSSE-KMS または SSE-KMS 暗号化を使用します。
- Amazon S3 マネージド – Amazon S3 マネージドキーで暗号化されたオブジェクトの数。これらのオブジェクトは SSE-S3 暗号化を使用します。
- 暗号化なし— 暗号化されていない、またはクライアント側の暗号化を使用するオブジェクトの数。(オブジェクトがクライアント側の暗号化を使用して暗号化されている場合、Macie はそのオブジェクトの暗号化データにアクセスしてレポートできません)。
- 不明— Macie が現在の暗号化メタデータを持たないオブジェクトの数。これは通常、バケットのオブジェクトのメタデータを手動で更新することを最近選択した場合に発生します。Macie はバケットとオブジェクトメタデータの次回 (24 時間以内) の毎日の更新を実行するときに、暗号化統計を更新します。

サポートされている各暗号化タイプの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「暗号化によるデータの保護」を参照してください。

サーバー側の暗号化

このセクションでは、バケットのサーバー側の暗号化設定に関する洞察を提供します。

バケットポリシーで必要とされる暗号化フィールドは、オブジェクトをバケットにアップロードするときに、バケットのポリシーではオブジェクトのサーバー側の暗号化を必要とするかどうかを示します。

- いいえ— バケットにバケットポリシーがないか、バケットのポリシーでは新しいオブジェクトのサーバー側の暗号化を必要としません。バケットポリシーが存在する場合、有効なサーバー側の暗号化ヘッダーを含めるPutObjectリクエストは必要ありません。
- はい— バケットのポリシーでは、新しいオブジェクトのサーバー側の暗号化が必要です。PutObject は、バケットに有効なサーバー側の暗号化ヘッダーを含めることを必要としています。アクセス許可がない場合、Amazon S3 はリクエストを拒否します。
- 不明— Macie は、バケットポリシーを評価して、それが新しいオブジェクトのサーバー側の暗号化を必要とするかどうかを判断できませんでした。

この評価で有効なサーバー側の暗号化ヘッダーは、`x-amz-server-side-encryption` (値は `AES256` または `aws:kms`)、および `x-amz-server-side-encryption-customer-algorithm` (値は `AES256`)。バケットポリシーを使用して新しいオブジェクトのサーバー側の暗号化を要求する方法については、「Amazon Simple Storage Service ユーザーガイド」の「サーバー側の暗号化によるデータの保護」を参照してください。

デフォルトの暗号化フィールドは、バケットに追加されたオブジェクトにバケットがデフォルトで適用されるように設定されたサーバー側の暗号化アルゴリズムを示します。

- AES256 — バケットのデフォルトの暗号化設定は、Amazon S3 マネージドキーを使用して新しいオブジェクトを暗号化するように設定されています。新しいオブジェクトは SSE-S3 暗号化を使用して自動的に暗号化されます。
- aws:kms – バケットのデフォルトの暗号化設定は AWS KMS key、 AWS マネージドキー または カスタマーマネージドキーのいずれかの で新しいオブジェクトを暗号化するように設定されています。新しいオブジェクトは SSE-KMS 暗号化を使用して自動的に暗号化されます。AWS KMS key フィールドには、使用されているキーの Amazon リソースネーム (ARN) または一意の識別子 (キー ID) が表示されます。
- aws:kms:dsse – バケットのデフォルトの暗号化設定は AWS KMS key、 AWS マネージドキー または カスタマーマネージドキーのいずれかの で新しいオブジェクトを暗号化するように設定されています。新しいオブジェクトは、DSSE-KMS 暗号化を使用して自動的に暗号化されます。AWS KMS key フィールドには、使用されているキーの ARN またはキー ID が表示されます。
- なし— バケットのデフォルトの暗号化設定では、新しいオブジェクトに対するサーバー側の暗号化動作は指定されていません。

2023 年 1 月 5 日以降、Amazon S3 はバケットに追加されるオブジェクトに対して、基本レベルの暗号化として Amazon S3 管理キー (SSE-S3) によるサーバーサイド暗号化を自動的に適用します。オプションで、 キーによるサーバー側の暗号化 (SSE-KMS) または AWS KMS キーによる二層式

サーバー側の暗号化 AWS KMS (DSSE-KMS) を使用するようにバケットのデフォルトの暗号化設定を設定できます。デフォルトの暗号化設定とオプションの詳細については、Amazon Simple Storage Service ユーザーガイドのS3 バケットのデフォルトのサーバー側の暗号化動作の設定を参照してください。

機密データ検出

このセクションでは、機密データ検出ジョブがバケット内のオブジェクトを毎日、毎週、または毎月ベースで定期的に分析するように設定されているかどうかを示します。ジョブによって積極的にモニタリングされているフィールドの値が はいの場合、バケットが定期的なジョブに明示的に含まれるか、バケットが過去 24 時間以内の定期的なジョブの基準に一致したことになります。さらに、それらのジョブの少なくとも 1 つのステータスは キャンセルされません。Macie は毎日ベースでこのデータを更新します。

バケットを検査するように任意のタイプの機密データ検出ジョブ (定期的なジョブまたは 1 回限りのジョブ) が設定されている場合、最新のジョブフィールドには、最後に実行を開始したジョブの一意の識別子が表示されます。最新のジョブ実行フィールドは、そのジョブの実行が開始されたタイミングを示します。

> **Tip**
>
> ジョブが生成した機密データの調査結果をすべて表示するには、最新のジョブ実行フィールドのリンクを選択します。表示されるジョブ詳細パネルで、パネルの上部の 結果を表示するを選択し、次に 調査結果を表示するを選択します。

パブリックアクセス

このセクションでは、バケットがパブリックアクセス可能かどうかを示します。また、これが当てはまるかどうかを判断するさまざまなアカウントレベルおよびバケットレベルの設定の詳細を示します。有効なアクセス許可フィールドは、次の設定の累積結果を示します。

- パブリックではない– バケットはパブリックアクセス可能ではありません。
- パブリック– バケットはパブリックアクセス可能です。
- 不明— Macie は、バケットのパブリックアクセス設定のすべては評価できませんでした。

このデータは、アカウントレベルおよびバケットレベルの設定に制限されることに注意してください。バケット内の特定のオブジェクトへのパブリックアクセスを有効化するオブジェクトレベルの設定は反映されません。

バケットおよびバケットデータへのパブリックアクセスを管理するための Amazon S3 設定の詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 での Identity and Access Managementと Amazon S3 ストレージへのパブリックアクセスのブロックを参照してください。

レプリケーション

このセクションでは、レプリケートされたフィールドは、バケットが他のバケットにオブジェクトをレプリケートするように設定されているかどうかを示します。このフィールドの値が はいの場合、バケットに 1 つ以上のレプリケーションルールが設定され、有効になっています。次に、このセクションには、レプリケート先バケットを所有 AWS アカウント する各 のアカウント ID も一覧表示されます。

レプリケート外部フィールドは、バケットが組織の外部 (一部ではない) のバケットにオブジェクトをレプリケート AWS アカウント するように設定されているかどうかを示します。組織は、Macie の招待を通じて、 AWS Organizations または Macie の招待によって、関連アカウントのグループとして一元管理される Macie アカウントのセットです。このフィールドの値がはい の場合、レプリケーションルールがバケットに対して設定および有効になり、外部 が所有するバケットにオブジェクトをレプリケートするようにルールが設定されます AWS アカウント。

> **Note**
>
> 特定の条件下では、Macie は、バケットが外部 が所有するバケットにオブジェクトをレプリケートするように設定されていることを誤って示す可能性があります AWS アカウント。これは、毎日の更新サイクルの一環として Macie が Amazon S3 からバケットとオブジェクトメタデータを取得した後、過去 24 時間以内に宛先バケットが別の AWS リージョン に作成された場合に発生する可能性があります。
> Macie を使用して問題を調査するには、更新  を選択して Amazon S3 から最新のバケットメタデータを取得します。次に、このセクションのアカウント ID のリストを確認してください。より詳細な調査を行うには、Amazon S3 を使用してバケットのレプリケーションルールを確認してください。

バケットオブジェクトをレプリケートするための Amazon S3 オプションと設定の詳細については、Amazon Simple Storage Service ユーザーガイドのオブジェクトのレプリケーションを参照してください。

タグ

バケットにタグが関連付けられている場合は、このセクションがパネルに表示され、それらのタグがリスト化されます。タグは,定義して、S3 バケットを含む、 AWS リソースの特定のタイプに関連付けることができるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。

バケットのタグ付けの詳細については、Amazon Simple Storage Service ユーザーガイドのコスト配分 S3 バケットタグの使用を参照してください。

Amazon Macie で S3 バケットインベントリをフィルタリングする

特定の特性を持つバケットを特定し、それに焦点を絞るには、Amazon Macie コンソールで、および Amazon Macie API を使用してプログラムで送信するクエリで S3 バケットインベントリをフィルタリングできます。フィルターを作成するときは、特定のバケット属性を使用して、ビューまたはクエリ結果からバケットを含めるか除外するための基準を定義します。バケット属性は、バケットの特定のメタデータを保存するフィールドです。

Macie では、フィルターは 1 つ以上の条件で設定されます。各条件は、基準とも呼ばれ、3 つの部分で設定されています。

- バケット名、タグキー、または ジョブで定義されているなどの、属性ベースのフィールド。
- 演算子 (等しい や 等しくない など)。
- 1 つまたは複数の値。値のタイプと数は、選択するフィールドと演算子によって異なります。

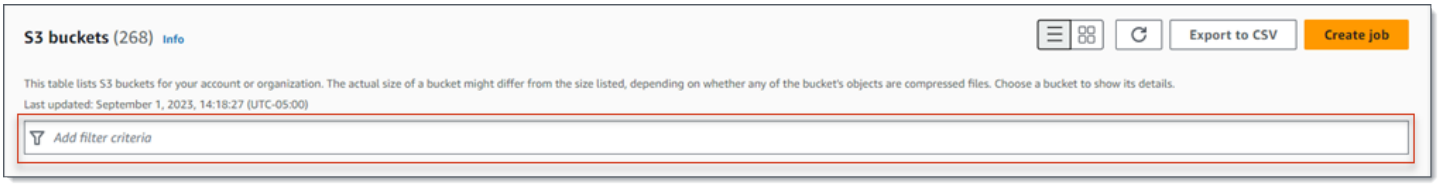
フィルター条件の定義および適用方法は、Amazon Macie コンソールと Amazon Macie API のどちらを使用するかによって異なります。

トピック

- Amazon Macie コンソールでインベントリをフィルタリングする
- Amazon Macie API を用いてインベントリをプログラムでフィルタリングする

Amazon Macie コンソールでインベントリをフィルタリングする

Amazon Macie コンソールを使用して S3 バケットインベントリをフィルタリングする場合、Macie は個別の条件のフィールド、演算子、値を選択するのに役立つオプションを提供します。これらのオプションにアクセスするには、次のイメージに示すように、S3 バケットページのフィルターバーを使用します。

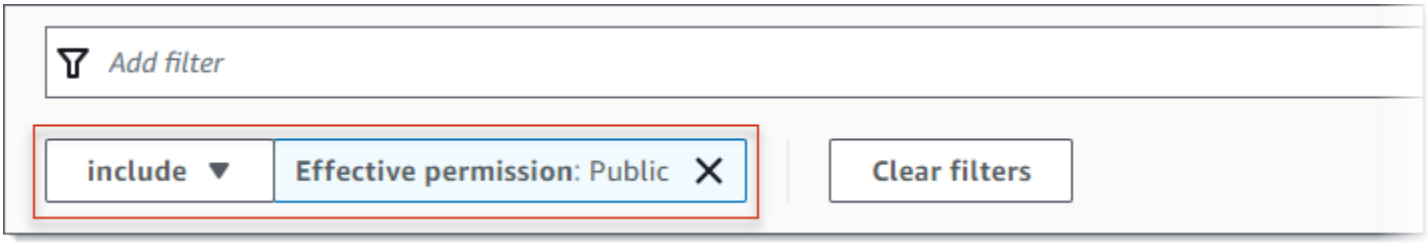


フィルターボックスにカーソルを置くと、Macie はフィルター条件で使用できるフィールドのリストを表示します。フィールドは論理カテゴリ別に整理されています。たとえば、共通のフィールドカテゴリには S3 バケットに関する一般的な情報を格納するフィールドが含まれます。パブリックアクセスカテゴリには、バケットに適用できるさまざまなタイプのパブリックアクセス設定に関するデータを保存するフィールドが含まれます。フィールドは、各カテゴリ内でアルファベット順に並べ替えられます。

条件を追加するには、まずリストからフィールドを選択します。フィールドを見つけるには、完全なリストを参照するか、フィールド名の一部を入力してフィールドのリストを絞り込みます。

選択したフィールドに応じて、Macie は異なるオプションを表示します。オプションには、選択したフィールドのタイプと性質が反映されます。たとえば、ジョブで定義されているフィールドを選択した場合、Macie は選択する値のリストを表示します。バケット名フィールドを選択した場合、Macie は、バケット名を入力できるテキストボックスを表示します。どのフィールドを選択しても、Macie はフィールドに必要な設定を含む条件を追加するステップを順を追ってガイドします。

条件を追加すると、次の図に示すように、Macie はその条件の基準を適用し、フィルターボックスの下のフィルタートークンに条件を表示します。



この例では、パブリックアクセス可能なすべてのバケットが含まれ、他のすべてのバケットを除外するように条件が設定されています。有効なアクセス許可フィールドの値 と等しい パブリックの場合、バケットが返されます。

条件を追加すると、Macie はその基準を適用し、それらをフィルターボックスの下に表示します。複数の条件を追加する場合、Macie は AND ロジックを使用して条件を結合し、フィルター基準を評価します。これは、バケットは、すべてのフィルター内の条件に一致した場合にのみ、フィルター基準を満たすことを意味します。フィルターボックスの下の領域をいつでも参照して、適用した基準を確認できます。

コンソールを使用してインベントリをフィルタリングするには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで、S3 バケットを選択します。S3 バケットページにはバケットインベントリが表示されます。

   自動機密データ検出が有効になっている場合、デフォルトビューには、現在自動検出から除外されているバケットのデータが表示されません。ユーザーが組織の Macie 管理者である場合、自動検出が現在無効になっているアカウントのデータも表示されません。このデータを表示するには、フィルターボックスの下にある自動検出フィルタートークンによってモニタリングされるで X を選択します。
3. ページの上部で、必要に応じて、更新
   を選択して、Amazon S3 から最新のバケットメタデータを取得します。
4. フィルターボックスにカーソルを置き、条件に使用するフィールドを選択します。
5. 次のヒントを念頭に置いて、フィールドに適切な値のタイプを選択または入力します。

   日付、時刻、および時間範囲

   日付と時刻では、From および To ボックスを使用して、包括的な時間範囲を定義します。

   - 固定時間範囲を定義するには、From および To ボックスを使用して、範囲内の最初の日時と最後の日時をそれぞれ指定します。
   - 特定の日時に開始し、現在の時刻で終了する相対時間範囲を定義するには、開始日時を From ボックスに入力し、To ボックス内のテキストを削除します。
   - 特定の日時に終了する相対時間範囲を定義するには、終了日時を To ボックスに入力し、From ボックス内のテキストを削除します。

   時間値は 24 時間表記を使用することに注意してください。日付ピッカーを使用して日付を選択する場合は、テキストをFrom および To ボックスに直接入力して、値を絞り込むことができます。

   数値および数値範囲

   数値では、From と To ボックスを使用して、包括的な数値範囲を定義する整数を入力します。

   - 固定数値範囲を定義するには、From と To ボックスを使用して、範囲内の最小と最大の数値をそれぞれ指定します。

- 1 つの特定の値に制限される固定数値範囲を定義するには、From と To 両方のボックスに値を入力します。例えば、厳密に 15 個のオブジェクトを保存する S3 バケットのみを含めるには、**15**From および To ボックスに と入力します。
- 特定の数値で始まる相対数値範囲を定義するには、From ボックスに数値を入力し、To ボックスにテキストは入力しないでください。
- 特定の数値で終わる相対数値範囲を定義するには、To ボックスに数値を入力し、From ボックスにテキストは入力しないでください。

テキスト (文字列) 値

このタイプの値では、フィールドに完全で有効な値を入力します。値は大文字と小文字が区別されます。

このタイプの値では、部分的な値またはワイルドカード文字を使用することはできないことに注意してください。唯一の例外は バケット名フィールドです。そのフィールドでは、完全なバケット名の代わりにプレフィックスを指定できます。たとえば、名前が my-S3 で始まるすべての S3 バケットを見つけるには、バケット名 フィールドのフィルター値として **my-S3** と入力します。**My-s3** や **my*** などの他の値を入力した場合、Macie はバケットを返しません。

6. フィールドの値の追加が終了したら、適用を選択します。Macie はフィルター基準を適用し、フィルターボックスの下のフィルタートークンに条件を表示します。
7. 追加する追加の条件ごとに、ステップ 4～6 を繰り返します。
8. 条件を削除するには、条件のフィルタートークンの X を選択します。
9. 条件を変更するには、条件のフィルタートークンの X を選択して条件を削除します。次に、ステップ 4～6 を繰り返して、正しい設定を持つ条件を追加します。

Amazon Macie API を用いてインベントリをプログラムでフィルタリングする

S3 バケットインベントリをプログラムでフィルタリングするには、Amazon Macie API の DescribeBucketsオペレーションを使用して送信するクエリでフィルター条件を指定します。このオペレーションは、オブジェクトの配列を返します。各オブジェクトには、フィルター基準と一致するバケットに関する統計データおよびその他の情報が含まれます。

クエリでフィルター基準を指定するには、リクエストにフィルター基準のマップを含めます。条件ごとに、フィールド、演算子、およびフィールドの 1 つ以上の値を指定します。値のタイプと数は、選択するフィールドと演算子によって異なります。条件で使用できるフィールド、演算子、および値

のタイプについては、Amazon Macie API リファレンスのAmazon S3 データソースを参照してください。

次の例は、AWS Command Line InterfaceAWS CLI を使用して送信するクエリでフィルター基準を指定する方法を示しています。これを行うには、別の AWS コマンドラインツールまたは AWS SDK の最新バージョンを使用するか、HTTPS リクエストを Macie に直接送信します。 AWS ツールと SDKsで構築するツール AWS」を参照してください。

例

- 例 1: バケット名でバケットを見つける
- 例 2: パブリックアクセス可能なバケットを見つける
- 例 3: 暗号化されていないオブジェクトを保存するバケットを検索する
- 例 4: ジョブによってモニタリングされていないバケットを見つける
- 例 5: 外部アカウントにデータをレプリケートするバケットを見つける
- 例 6: 複数の基準に基づいてバケットを見つける

この例では、describe-buckets コマンドを使用します。例が正常に実行されると、Macie は buckets 配列を返します。配列には、現在の にあり AWS リージョン 、フィルター条件に一致する各バケットのオブジェクトが含まれます。この出力の例では、以下のセクションを展開します。

buckets 配列の例

この例では、buckets 配列は、クエリで指定されたフィルター基準と一致する 2 つのバケットの詳細を提供します。

```
{
    "buckets": [
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "FALSE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "bucketCreatedAt": "2020-05-18T19:54:00+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET1",
            "classifiableObjectCount": 13,
            "classifiableSizeInBytes": 1592088,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "TRUE",
```

```
            "lastJobId": "08c81dc4a2f3377fae45c9ddaexample",
            "lastJobRunTime": "2024-05-26T14:55:30.270000+00:00"
        },
        "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
        "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
        "objectCount": 13,
        "objectCountByEncryptionType": {
            "customerManaged": 0,
            "kmsManaged": 2,
            "s3Managed": 7,
            "unencrypted": 4,
            "unknown": 0
        },
        "publicAccess": {
            "effectivePermission": "NOT_PUBLIC",
            "permissionConfiguration": {
                "accountLevelPermissions": {
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    }
                },
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            }
        },
        "region": "us-east-1",
        "replicationDetails": {
```

```
            "replicated": false,
            "replicatedExternally": false,
            "replicationAccounts": []
        },
        "sensitivityScore": 78,
        "serverSideEncryption": {
            "kmsMasterKeyId": null,
            "type": "NONE"
        },
        "sharedAccess": "NOT_SHARED",
        "sizeInBytes": 4549746,
        "sizeInBytesCompressed": 0,
        "tags": [
            {
                "key": "Division",
                "value": "HR"
            },
            {
                "key": "Team",
                "value": "Recruiting"
            }
        ],
        "unclassifiableObjectCount": {
            "fileType": 0,
            "storageClass": 0,
            "total": 0
        },
        "unclassifiableObjectSizeInBytes": {
            "fileType": 0,
            "storageClass": 0,
            "total": 0
        },
        "versioning": true
    },
    {
        "accountId": "123456789012",
        "allowsUnencryptedObjectUploads": "TRUE",
        "automatedDiscoveryMonitoringStatus": "MONITORED",
        "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
        "bucketCreatedAt": "2020-11-25T18:24:38+00:00",
        "bucketName": "DOC-EXAMPLE-BUCKET2",
        "classifiableObjectCount": 8,
        "classifiableSizeInBytes": 133810,
        "jobDetails": {
```

```
            "isDefinedInJob": "TRUE",
            "isMonitoredByJob": "FALSE",
            "lastJobId": "188d4f6044d621771ef7d65f2example",
            "lastJobRunTime": "2024-04-09T19:37:11.511000+00:00"
        },
        "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
        "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
        "objectCount": 8,
        "objectCountByEncryptionType": {
            "customerManaged": 0,
            "kmsManaged": 0,
            "s3Managed": 8,
            "unencrypted": 0,
            "unknown": 0
        },
        "publicAccess": {
            "effectivePermission": "NOT_PUBLIC",
            "permissionConfiguration": {
                "accountLevelPermissions": {
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    }
                },
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            }
        },
```

```
            "region": "us-east-1",
            "replicationDetails": {
                "replicated": false,
                "replicatedExternally": false,
                "replicationAccounts": []
            },
            "sensitivityScore": 95,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
                "type": "AES256"
            },
            "sharedAccess": "EXTERNAL",
            "sizeInBytes": 175978,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
            ],
            "unclassifiableObjectCount": {
                "fileType": 3,
                "storageClass": 0,
                "total": 3
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 2999826,
                "storageClass": 0,
                "total": 2999826
            },
            "versioning": true
        }
    ]
}
```


フィルター基準と一致するバケットがない場合、Macie は空の buckets 配列を返します。


```
{
    "buckets": []
```

```
}
```

例 1: バケット名でバケットを見つける

この例では、describe-buckets コマンドを使用して、名前が my-S3で始まり、現在の にあるすべてのバケットのメタデータをクエリします AWS リージョン。

Linux、macOS、Unix の場合:

```
$ aws macie2 describe-buckets --criteria '{"bucketName":{"prefix":"my-S3"}}'
```

Microsoft Windows の場合:

```
C:\> aws macie2 describe-buckets --criteria={\"bucketName\":{\"prefix\":\"my-S3\"}}
```

コードの説明は以下のとおりです。

- *bucketName* は バケット名フィールドの JSON 名を指定します。
- *prefix* は prefix 演算子を指定します。
- *my-S3* は バケット名 (バケット名) フィールドの値です。

例 2: パブリックアクセス可能なバケットを見つける

この例では、describe-buckets コマンドを使用して、現在の にあり AWS リージョン 、アクセス許可設定の組み合わせに基づいてパブリックにアクセス可能なバケットのメタデータをクエリします。

Linux、macOS、Unix の場合:

```
$ aws macie2 describe-buckets --criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]}}'
```

Microsoft Windows の場合:

```
C:\> aws macie2 describe-buckets --criteria={\"publicAccess.effectivePermission\":
{\"eq\":[\"PUBLIC\"]}}
```

コードの説明は以下のとおりです。

- *publicAccess.effectivePermission* は 有効なアクセス許可フィールドの JSON 名を指定します。
- *eq*は、等しい 演算子を指定します。
- *PUBLIC* は 有効なアクセス許可フィールドの列挙値です。

例 3: 暗号化されていないオブジェクトを保存するバケットを検索する

この例では、describe-buckets コマンドを使用して、現在の にあるバケットのメタデータをクエリ AWS リージョン し、暗号化されていないオブジェクトを保存します。

Linux、macOS、Unix の場合:

```
$ aws macie2 describe-buckets --criteria '{"objectCountByEncryptionType.unencrypted":
{"gte":1}}'
```

Microsoft Windows の場合:

```
C:\> aws macie2 describe-buckets --
criteria={\"objectCountByEncryptionType.unencrypted\":{\"gte\":1}}
```

コードの説明は以下のとおりです。

- *objectCountByEncryptionType.unencrypted* は、暗号化なしフィールドの JSON 名を指定します。
- *gte*は、 ~ 以上演算子を指定します。
- *1* は、暗号化なしフィールドの包括的で相対的な数値範囲内の最小値です。

例 4: ジョブによってモニタリングされていないバケットを見つける

この例では、describe-buckets コマンドを使用して、現在の にあり AWS リージョン 、定期的な機密データ検出ジョブに関連付けられていないバケットのメタデータをクエリします。

Linux、macOS、Unix の場合:

```
$ aws macie2 describe-buckets --criteria '{"jobDetails.isMonitoredByJob":{"eq":
["FALSE"]}}'
```

Microsoft Windows の場合:

```
C:\> aws macie2 describe-buckets --criteria={\"jobDetails.isMonitoredByJob\":{\"eq\":
[\"FALSE\"]}}
```

コードの説明は以下のとおりです。

- *jobDetails .isMonitoredByJob* は、ジョブによってアクティブにモニタリングされるフィールドの JSON 名を指定します。
- *eq*は、と等しい 演算子を指定します。
- *FALSE* は ジョブによって積極的にモニタリングされているフィールドの列挙値です。

例 5: 外部アカウントにデータをレプリケートするバケットを見つける

この例では、describe-buckets コマンドを使用して、現在の にあり AWS リージョン 、組織の一部 AWS アカウント ではない にオブジェクトをレプリケートするように設定されているバケットのメタデータをクエリします。

Linux、macOS、Unix の場合:

```
$ aws macie2 describe-buckets --criteria '{"replicationDetails.replicatedExternally":
{"eq":["true"]}}'
```

Microsoft Windows の場合:

```
C:\> aws macie2 describe-buckets --
criteria={\"replicationDetails.replicatedExternally\":{\"eq\":[\"true\"]}}
```

コードの説明は以下のとおりです。

- *replicationDetails.replicatedExternally* は Replicated externally (外部でレプリケートされた) フィールドの JSON 名を指定します。
- *eq*は、と等しい 演算子を指定します。
- *true* は 外部でレプリケートされたフィールドのブール値を指定します。

例 6: 複数の基準に基づいてバケットを見つける

この例では、describe-buckets コマンドを使用して、現在の にあり AWS リージョン 、次の条件に一致するバケットのメタデータをクエリします。 は、アクセス許可設定の組み合わせに基づいてパ

ブリックにアクセス可能、暗号化されていないオブジェクトを保存、定期的な機密データ検出ジョブに関連付けられていません。

Linux、macOS、または Unix の場合、読みやすさを向上させるためにバックスラッシュ (\) の行連結文字を使用します。

```
$ aws macie2 describe-buckets \
--criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]},"objectCountByEncryptionType.unencrypted":
{"gte":1},"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Microsoft Windows の場合、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

```
C:\> aws macie2 describe-buckets ^
--criteria={\"publicAccess.effectivePermission\":{\"eq\":
[\"PUBLIC\"]},\"objectCountByEncryptionType.unencrypted\":{\"gte\":1},
\"jobDetails.isMonitoredByJob\":{\"eq\":[\"FALSE\"]}}
```

ここで、

- *publicAccess.effectivePermission* は 有効なアクセス許可フィールドの JSON 名を指定し、
  - *eq*は、と等しい 演算子を指定します。
  - *PUBLIC* は 有効なアクセス許可フィールドの列挙値です。
- *objectCountByEncryptionType.unencrypted* は、暗号化なしフィールドの JSON 名を指定します。
  - *gte*は、 ~ 以上演算子を指定します。
  - *1* は、暗号化なしフィールドの包括的で相対的な数値範囲内の最小値です。
- *jobDetails .isMonitoredByJob* は、ジョブによってアクティブにモニタリングされるフィールドの JSON 名を指定します。
  - *eq*は、と等しい 演算子を指定します。
  - *FALSE* は ジョブによって積極的にモニタリングされているフィールドの列挙値です。

Amazon Macie が S3 バケットおよびオブジェクトにアクセスすることを許可する

で Amazon Macie を有効にすると AWS アカウント、Macie はユーザーに代わって Amazon Simple Storage Service (Amazon S3) およびその他の を呼び出すために必要なアクセス許可を Macie に付与するサービスにリンクされたロールを作成します。Amazon S3 AWS のサービス サービスにリンクされたロールは、ユーザーに代わってアクションを実行するためにサービスに手動でアクセス許可を追加する必要がない AWS のサービス ため、 のセットアッププロセスを簡素化します。このタイプのロールの詳細については、AWS Identity and Access Management ユーザーガイドのサービスにリンクされたロールの使用を参照してください。

Macie のサービスにリンクされたロール`AWSServiceRoleForAmazonMacie` のアクセス許可ポリシーにより、Macie が S3 バケットとオブジェクトに関する情報の取得およびバケット内のオブジェクトからの取得を含むアクションを実行することを許可します。ユーザーが組織の Macie 管理者である場合、ポリシーにより Macie が組織のメンバーアカウントに対してユーザーの代わりにこれらのアクションを実行することも許可します。

Macie は、次のようなタスクを実行するためにこれらの許可を使用します。

- S3 汎用バケットのインベントリを生成して維持する
- バケットおよびバケット内のオブジェクトに関する統計およびその他のデータを提供する
- バケットのセキュリティとアクセスコントロールをモニタリングして評価する
- バケット内のオブジェクトを分析して機密データを検出する

ほとんどの場合、Macie はこれらのタスクを実行するために必要なアクセス許可を持っています。ただし、S3 バケットが制限付きバケットポリシーを持つ場合、ポリシーにより Macie がこれらのタスクの一部またはすべてを実行することを妨げる場合があります。

バケットポリシーは、プリンシパル AWS Identity and Access Management（ユーザー、アカウント、サービス、またはその他のエンティティ) が S3 バケットに対して実行できるアクションと、プリンシパルがそれらのアクションを実行できる条件を指定するリソースベースの (IAM) ポリシーです。アクションと条件は、バケットに関する情報の取得などのバケットレベルのオペレーションや、バケットからのオブジェクトの取得などのオブジェクトレベルのオペレーションに適用できます。

バケットポリシーは通常、明示的な `Allow` または `Deny` ステートメントと条件を使用してアクセス権を付与または制限します。たとえば、バケットポリシーには、特定のソース IP アドレス、Amazon Virtual Private Cloud (Amazon VPC) エンドポイント、または VPC がバケットにアクセ

スするために使用されていない限り、バケットへのアクセスを拒否する Allow または Denyステートメントが含まれる場合があります。バケットポリシーを使用してバケットにアクセス権を付与または制限する方法の詳細については、Amazon Simple Storage Service ユーザーガイドのバケットポリシーとユーザーポリシーとAmazon S3 がリクエストを許可する方法を参照してください。

バケットポリシーが明示的な Allow ステートメントを使用する場合、ポリシーは、Macie がバケットとバケットのオブジェクトに関する情報を取得したり、バケットからオブジェクトを取得したりすることを妨げません。これは、Macie のサービスにリンクされたロールのアクセス許可ポリシーの Allow ステートメントが、これらのアクセス許可を付与するからです。

ただし、バケットポリシーが 1 つ以上の条件を持つ明示的な Deny ステートメントを使用する場合、Macie はバケットまたはバケットのオブジェクトに関する情報を取得したり、バケットのオブジェクトを取得したりすることを許可されない場合があります。たとえば、バケットポリシーが特定の IP アドレスを除くすべてのソースからのアクセスを明示的に拒否した場合、Macie は機密データ検出ジョブを実行するときにバケットのオブジェクトを分析することを許可されなくなります。これは、制限付きバケットポリシーが、Macie のサービスにリンクされたロールのアクセス許可ポリシーの Allow ステートメントより優先されるからです。

Macie が制限付きバケットポリシーを持つバケットにアクセスすることを許可するために、Macie のサービスにリンクされたロール AWSServiceRoleForAmazonMacie の条件をバケットポリシーに追加できます。その条件により、Macie のサービスにリンクされたロールをポリシーの Deny 制限との一致から除外できます。これは、aws:PrincipalArn グローバル条件キー および Macie のサービスにリンクされたロールの Amazon リソースネーム (ARN) を使用して行うことができます。

次の手順では、このプロセスについて説明し、例を示します。

Macie のサービスにリンクされたロールをバケットポリシーに追加するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. ナビゲーションペインで、バケットを選択します。
3. Macie がアクセスすることを許可する S3 バケットを選択します。
4. アクセス許可タブの バケットポリシーで 編集をクリックします。
5. バケットポリシーエディタで、アクセスを制限し、Macie がバケットまたはバケットのオブジェクトにアクセスすることを妨げるそれぞれの Deny ステートメントを特定します。
6. それぞれの Deny ステートメントで、aws:PrincipalArn グローバル条件コンテキストキーを使用する条件を追加し、 AWS アカウントの Macie のサービスにリンクされたロールの ARN を指定します。

条件キーの値は arn:aws:iam::*123456789012*:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie である必要があります。ここで、 AWS アカウントのアカウント ID は *123456789012* です。

これをバケットポリシーのどこに追加するかは、ポリシーに現在含まれている構造、要素、および条件によって異なります。サポートされている構造と要素の詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 のポリシーとアクセス許可を参照してください。

DOC-EXAMPLE-BUCKETという名前の S3 バケットへのアクセスを制限するための明示的な Deny ステートメントを使用するバケットポリシーの例を次に示します。現在のポリシーでは、バケットには ID が vpce-1a2b3c4d である VPC エンドポイントからのみアクセスできます。 AWS Management Console および Macie からのアクセスを含め、他のすべての VPC エンドポイントからのアクセスは拒否されます。

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115example",
   "Statement": [
      {
         "Sid": "Access from specific VPCE only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            }
         }
      }
   ]
}
```

このポリシーを変更し、Macie がバケットとバケットのオブジェクトにアクセスすることを許可するには、StringNotLike 条件演算子 とaws:PrincipalArn グローバル条件キー を使用する条件を

追加できます。この追加の条件により、Macie のサービスにリンクされたロールを Deny 制限との一致から除外します。

```
{
   "Version": "2012-10-17",
   "Id":" Policy1415115example ",
   "Statement": [
      {
         "Sid": "Access from specific VPCE and Macie only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            },
            "StringNotLike": {
               "aws:PrincipalArn": "arn:aws:iam::123456789012:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
            }
         }
      }
   ]
}
```

前の例では、StringNotLike 条件演算子は、aws:PrincipalArn 条件コンテキストキーを使用して、Macie のサービスにリンクされたロールの ARN を指定します。

- 123456789012 は、Macie を使用してバケットとバケットのオブジェクトに関する情報を取得し、バケットからオブジェクトを取得することを許可 AWS アカウント されている のアカウント ID です。
- macie.amazonaws.com は、Macie サービスプリンシパルの識別子です。
- AWSServiceRoleForAmazonMacie は、Macie のサービスにリンクされたロールの名前です。

ポリシーが StringNotEquals 演算子をすでに使用しているため、StringNotLike 演算子が使用されました。ポリシーでは、StringNotEquals 演算子は一度だけ使用できます。

Amazon S3 リソースへのアクセスの管理に関する追加のポリシー例および詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 での Identity and Access Managementを参照してください。

Amazon Macie で機密データを検出する

Amazon Macie を使用すると、Amazon Simple Storage Service (Amazon S3) データ資産内の機密データの検出、ログ記録、レポート作成を自動化できます。これは、Macie が機密データの自動検出を実行するように設定する方法と、機密データ検出ジョブを作成して実行する方法の 2 つの方法で行うことができます。

機密データの自動検出

機密データの自動検出により、Amazon S3 データエステート内の機密データがどこに存在するかに幅広い可視性を提供しています。このオプションでは、Macie は S3 バケットインベントリを毎日評価し、サンプリング技術を使用してバケットから代表的な S3 オブジェクトを識別して選択します。その後、Macie は選択したオブジェクトを取得して分析し、機密データがないか検査します。詳細については、機密データ自動検出を実行するを参照してください。

機密データ検出ジョブ

機密データ検出ジョブでは、より詳細で対象を絞った分析が可能になります。このオプションでは、選択する特定の S3 バケット、または特定の条件に一致するバケットなど、分析の範囲と深さを定義します。S3 オブジェクトのプロパティから派生するカスタム基準などのオプションを選択して、その分析の範囲を絞り込むこともできます。また、ジョブは、オンデマンドの分析および評価では 1 回のみ、または定期的な分析、評価、およびモニタリングでは繰り返しベースで実行するように設定できます。詳細については、機密データ検出ジョブの実行を参照してください。

機密データの自動検出と機密データ検出ジョブのいずれの場合も、各機密データ検出ジョブは、Macie が提供したマネージドデータ識別子、お客様が定義したカスタムデータ識別子、または 2 つの組み合わせを使用して、S3 オブジェクトを分析できます。許可リストを使用して分析を微調整することもできます。

マネージドデータ識別子

マネージドデータ識別子 は、特定の種類の機密データ (たとえば、クレジットカード番号、 AWS シークレットアクセスキー、または特定の国または地域のパスポート番号) を検出するように設計された組み込み型の基準と手法のセットです。これらは、複数のタイプの認証情報データ、財務情報、個人を特定できる情報 (PII) など、多くの国や地域の機密データタイプの大規模かつ増加しているリストを検出できます。詳細については、マネージドデータ識別子の使用を参照してください。

カスタムデータ識別子

カスタムデータ識別子は、機密データを検出するためのカスタム条件を定義します。基準は、一致するテキストパターン、オプションで文字シーケンス、結果を絞り込む近接ルールを定義する正規表現 (正規表現)から設定されています。それらを使用して、従業員 ID、顧客アカウント番号、内部データの分類など、特定のシナリオ、知的財産、または専有データを反映する機密データを検出できます。詳細については、カスタムデータ識別子の構築を参照してください。

許可リスト

Macie では、許可リストは S3 オブジェクトで無視するテキストとテキストパターンを指定します。これは通常、特定のシナリオや環境における機密データの例外 (組織の公開名や電話番号、組織がテストに使用するサンプルデータなど) です。Macie が許可リストのエントリまたはパターンと一致するテキストを見つけた場合、そのテキストがマネージドデータ識別子またはカスタムデータ識別子の基準に一致していても、Macie はそのテキストの出現を報告しません。詳細については、許可リストでの機密データの例外の定義を参照してください。

Macie が S3 オブジェクトを分析すると、Macie は Amazon S3 からオブジェクトの最新バージョンを取得し、オブジェクトの内容に機密データがないか検査します。以下が当てはまる場合、Macie はオブジェクトを分析できます。

- オブジェクトはサポートされているファイルまたはストレージ形式を使用し、サポートされているストレージクラスを使用して S3 汎用バケットに保存されます。詳細については、「サポートされているストレージクラスとフォーマット」を参照してください。
- オブジェクトが暗号化されている場合、Macie がアクセス可能で使用を許可されているキーを用いて暗号化されます。詳細については、暗号化された S3 オブジェクトの分析を参照してください。
- 制限バケットポリシーがあるバケットにオブジェクトが保存されている場合、ポリシーにより、Macie はバケット内のオブジェクトへのアクセスが許可されます。詳細については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。

Macieは、お客様がデータセキュリティおよびプライバシーに関する要件を満たし、コンプライアンスを維持できるよう、機密データを発見し、分析を実行した記録機密データの検出および機密データの検出結果を作成します。機密データの調査結果は、Macie がオブジェクトで検出した機密データの詳細なレポートです。機密データの検出結果は、オブジェクトの分析に関する詳細を記録するレコードです。各タイプのレコードは、標準化されたスキーマに従っており、必要に応じて他のアプリケーション、サービス、システムを使用して、そのクエリ、モニタリング、および処理に役立ちます。

> **Tip**
>
> Macie は Amazon S3 向けに最適化されていますが、現在別の場所に保存されているリソース内の機密データを検出するために使用できます。これを行うには、データを Amazon S3 に一時的または永続的に移動します。たとえば、Amazon Relational Database Service または Amazon Aurora のスナップショットを Apache Parquet 形式で Amazon S3 にエクスポートします。あるいは、Amazon DynamoDB テーブルを Amazon S3 にエクスポートします。その後、ジョブを作成して Amazon S3 内のデータを分析できます。

トピック

Amazon Macie でのマネージドデータ識別子の使用

Amazon Macie は、機械学習やパターンマッチングなどの基準と手法の組み合わせを使用して、Amazon Simple Storage Service (Amazon S3) オブジェクトの機密データを検出します。これらの基準と手法は、総称してマネージドデータ識別子と呼ばれ、複数のタイプの財務データ、個人健康情報 (PHI)、個人を特定できる情報 (PII) など、多くの国またはリージョンの機密データタイプの大規模かつ増加しているリストを検出できます。各マネージドデータ識別子は、特定の種類の機密データ (たとえば、AWS シークレットアクセスキー、クレジットカード番号、または特定の国またはリージョンのパスポート番号) を検出するように設計されています。

Macie は、マネージドデータ識別子を使用して、次のカテゴリの機密データを検出できます。

- プライベートキーや AWS シークレットアクセスキーなどの認証情報データに関する認証情報。
- クレジットカード番号や銀行口座番号などの財務データに関する財務情報。

- 医療保険や医療識別番号などの PHI、および運転免許証識別番号やパスポート番号などの PII に関する個人情報。

各カテゴリ内で、Macie は複数のタイプの機密データを検出できます。このセクションのトピックでは、各タイプとその検出に関連する要件をリスト化して説明します。各タイプでは、データを検出するように設計されたマネージドデータ識別子の一意の識別子 (ID) も示します。機密データ検出ジョブを作成する、または機密データの自動検出の設定を設定するとき、これらの ID を使用して、S3 オブジェクトを分析するときに Macie がどのマネージドデータ識別子を使用するかを指定できます。

ジョブに推奨されるマネージドデータ識別子のリストは 機密データ検出ジョブに推奨されるマネージドデータ識別子 を参照してください。機密データの自動検出に推奨され、デフォルトで使用されるマネージドデータ識別子のリストについては、機密データの自動検出のデフォルト設定を参照してください。

トピック

- Amazon Macie マネージドデータ識別子のキーワード要件
- クイックリファレンス: Amazon Macie マネージドデータ識別子
- 詳細リファレンス:Amazon Macie マネージドデータ識別子

Amazon Macie マネージドデータ識別子のキーワード要件

マネージドデータ識別子を使用して特定のタイプの機密データを検出するには、Amazon Macie ではデータの近くにあるキーワードが必要です。特定のタイプのデータに当てはまる場合、このセクションのその後のトピックでは、そのデータのキーワード要件を示します。

キーワードが特定のタイプのデータの近くにある必要がある場合は、通常、キーワードはデータから 30 文字以内 (包括的) になければなりません。追加の近接要件は、Amazon Simple Storage Service (Amazon S3) オブジェクトのファイルタイプまたはストレージ形式によって異なります。

Structured, columnar data (構造化された列指向データ)

列指向データでは、キーワードは同じ値の一部であるか、値を格納する列またはフィールドの名前内にある必要があります。これは、Microsoft Excel ワークブック、CSV ファイル、および TSV ファイルに当てはまります。

たとえば、フィールドの値に SSN と米国社会保障番号 (SSN) の構文を使用する 9 桁の番号の両方が含まれている場合、Macie はフィールド内の SSN を検出できます。同様に、列の名前に

SSN が含まれている場合、Macie は列内の各 SSN を検出できます。Macie は、その列内の値を、キーワード SSN の近くにあるものとして扱います。

Structured, record-based data (構造化されたレコードベースのデータ)

レコードベースのデータでは、キーワードは同じ値の一部であるか、値を格納するフィールドまたは配列へのパス内の要素の名前内にある必要があります。これは Apache Avro オブジェクトコンテナ、Apache Parquet ファイル、JSON ファイル、および JSON Lines ファイルに当てはまります。

たとえば、フィールドの値に credentials (認証情報) と AWS シークレットアクセスキーの構文を使用する文字シーケンスの両方が含まれている場合、Macie はフィールド内のキーを検出できます。同様に、フィールドへのパスが `$.credentials.aws.key` である場合、Macie はフィールド内の AWS シークレットアクセスキーを検出できます。Macie は、そのフィールド内の値を、キーワード credentials (認証情報) の近くにあるものとして扱います。

Unstructured data (非構造化データ)

Adobe Portable Document Format ファイル、Microsoft Word ドキュメント、E メールメッセージ、および CSV、JSON、JSON Lines、および TSV ファイル以外の非バイナリテキストファイルでは、追加の近接要件はありません。通常、キーワードはデータから 30 文字以内 (包括的) になければなりません。これには、これらのタイプのファイルに含まれるテーブルなどの構造化データが含まれます。

キーワードでは大文字と小文字が区別されません。さらに、キーワードにスペースが含まれている場合、Macie は、スペースを含まないキーワードのバリエーションや、スペースではなくアンダースコア (_) またはハイフン (-) を含むキーワードのバリエーションを自動的に照合します。場合によっては、Macie はキーワードの一般的なバリエーションに対処するためにキーワードを拡張または短縮します。

キーワードがコンテキストを提供し、Macie が特定のタイプの機密データを検出するのにどのように役立つかについては、次の動画をご覧ください。Amazon Macie がキーワードを使用して機密データを検出する方法。

クイックリファレンス: Amazon Macie マネージドデータ識別子

Amazon Macie のマネージドデータ識別子は、特定の種類の機密データ (特定の国または地域のクレジットカード番号、 AWS シークレットアクセスキー、パスポート番号など) を検出するように設計

された一連の組み込みの基準と手法です。これらの識別子は、複数のタイプの認証情報データ、財務情報、個人健康情報 (PHI)、個人を特定できる情報 (PII) など、多くの国や地域の機密データタイプの大規模かつ増加しているリストを検出できます。

次の表は、Macie が現在提供しているすべてのマネージドデータ識別子を機密データタイプ別にまとめたものです。それぞれのタイプについて、以下の情報を提供している：

- 機密データカテゴリ — 機密データの一般的なカテゴリを指定します。そのタイプには、シークレットキーなどの認証情報データの場合は認証情報、クレジットカード番号や銀行口座番号などの財務データの場合は財務情報、健康保険や医療識別番号などの個人の健康情報の場合は個人情報: PHI、および運転免許証の識別番号やパスポート番号などの個人を特定できる情報の場合は個人情報: PIIなどがあります。
- マネージドデータ識別子 ID — データを検出するように設計された 1 つ以上のマネージドデータ識別子の一意の識別子 (ID) を指定します。機密データ検出ジョブを作成したり、機密データの自動検出設定を設定したりする場合、これらの ID を使用して Macie がデータを分析するときに使用するマネージドデータ ID を指定できます。ジョブに推奨されるマネージドデータ識別子のリストは機密データ検出ジョブに推奨されるマネージドデータ識別子 を参照してください。機密データの自動検出に推奨されるマネージドデータ識別子のリストは 機密データの自動検出のデフォルト設定 を参照してください。
- キーワードが必要 — 検出には、キーワードがデータの近くにある必要があるかどうかを指定します。Macie がデータを分析する際にどのようにキーワードを使用するかについては、キーワード要件 を参照してください。
- 国と地域 — 該当するマネージドデータ ID がどの国または地域を対象に設計されているかを指定します。マネージドデータ識別子が特定の国や地域向けに設計されていない場合、この値はいずれかになります。

特定のタイプの機密データのマネージドデータ識別子に関する詳細情報を確認するには、そのタイプを選択します。

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
AWS シークレットアクセスキー	認証情報	AWS_CREDENTIALS	はい	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
銀行口座番号	財務情報	BANK_ACCOUNT_NUMBER(カナダと米国の場合)、	はい	カナダ、米国
基本銀行口座番号 (BBAN)	財務情報	国またはリージョンによって異なります。 FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	はい	フランス、ドイツ、イタリア、スペイン、英国
生年月日	個人情報: PHI	DATE_OF_BIRTH	はい	すべて
クレジットカードの有効期限	財務情報	CREDIT_CARD_EXPIRATION	はい	すべて
クレジットカードの磁気ストライプデータ	財務情報	CREDIT_CARD_MAGNETIC_STRIPE	はい	すべて
クレジットカード番号	財務情報	CREDIT_CARD_NUMBER (キーワードに近いクレジットカード番号の場合) と CREDIT_CARD_NUMBER_(NO_KEYWORD) (キーワードに近くないクレジットカード番号の場合)	可変	すべて
クレジットカード認証コード	財務情報	CREDIT_CARD_SECURITY_CODE	はい	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
運転免許証識別番号	個人情報: PII	国またはリージョンによって異なります。 AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	はい	オーストラリア、オーストリア、ベルギー、ブルガリア、カナダ、クロアチア、キプロス、チェコ共和国、デンマーク、エストニア、フィンランド、フランス、ドイツ、ギリシャ、ハンガリー、インド、アイルランド、イタリア、ラトビア、リトアニア、ルクセンブルク、マルタ、オランダ、ポーランド、ポルトガル、ルーマニア、スロバキア、スロベ

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		ニア、スペイン、スウェーデン、英国、米国
麻薬取締局 (DEA) 登録番号	個人情報: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	はい	米国
選挙人名簿番号	個人情報: PII	UK_ELECTORAL_ROLL_NUMBER	はい	UK
フルネーム	個人情報: PII	NAME	いいえ	すべて (名前にラテン文字セットが使用されている場合)
全地球測位システム (GPS) 座標	個人情報: PII	LATITUDE_LONGITUDE	はい	すべて (座標が英語のキーワードの近くにある場合)
Google Cloud API キー	認証情報	GCP_API_KEY	はい	すべて
健康保険請求番号 (HICN)	個人情報: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	はい	米国

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
健康保険または医療識別番号	個人情報: PHI	国またはリージョンによって異なります。 CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	はい	カナダ、EU、フィンランド、フランス、英国、米国
ヘルスケア共通手順コーディングシステム (HCPCS) コード	個人情報: PHI	USA_HEALTHCARE_PROCEDURE_CODE	はい	米国
HTTP 基本認証ヘッダー	認証情報	HTTP_BASIC_AUTH_HEADER	いいえ	すべて
HTTP クッキー	個人情報: PII	HTTP_COOKIE	いいえ	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
国際銀行口座番号 (IBAN)	財務情報	国またはリージョンによって異なります。 ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER	いいえ	アルバニア、アンドラ、ボスニア・ヘルツェゴビナ、ブラジル、ブルガリア、コスタリカ、クロアチア、キプロス、チェコ共和国、デンマーク、ドミニカ共和国、エジプト、エストニア、フェロー諸島、フィンランド、フランス、ジョージア、ドイツ、ギリシャ、グリーンランド、ハンガリー、アイスランド、アイルランド、イタリア、ヨルダン、コ

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
		, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER		ソボ、リヒテンシュタイン、リトアニア、マルタ、モーリタニア、モーリシャス、モナコ、モンテネグロ、オランダ、北マケドニア、ポーランド、ポルトガル、サンマリノ、セネガル、セルビア、スロバキア、スロベニア、スペイン、スウェーデン、スイス、東ティモール、チュニジア、トルコ、英国、ウクライナ、アラブ首長国連邦、バージ

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
		, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (イギリス領バージン諸島用)		ン諸島 (英国)
JSON ウェブトークン (JWT)	認証情報	JSON_WEB_TOKEN	いいえ	すべて
郵送先住所	個人情報: PII	ADDRESS、BRAZIL_CEP_CODE (ブラジルの Código de Endereçamento Postal の場合)	可変	オーストラリア、ブラジル、カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国
全米医薬品コード (NDC)	個人情報: PHI	USA_NATIONAL_DRUG_CODE	はい	米国
国民識別番号	個人情報: PII	国またはリージョンによって異なります。 BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	はい	ブラジル、フランス、ドイツ、インド、イタリア、スペイン

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
国民保険番号 (NINO)	個人情報: PII	UK_NATIONAL_INSURANCE_NUMBER	はい	UK
国家プロバイダー識別子 (NPI)	個人情報: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	はい	米国
OpenSSH プライベートキー	認証情報	OPENSSH_PRIVATE_KEY	いいえ	すべて
パスポート番号	個人情報: PII	国またはリージョンによって異なります。 CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	はい	カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国
本籍地	個人情報: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	はい	カナダ
PGP プライベートキー	認証情報	PGP_PRIVATE_KEY	いいえ	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
電話番号	個人情報: PII	国またはリージョンによって異なります。 BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	可変	ブラジル、カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国
公開鍵暗号標準 (PKCS) プライベートキー	認証情報	PKCS	いいえ	すべて
PuTTY プライベートキー	認証情報	PUTTY_PRIVATE_KEY	いいえ	すべて
社会保険番号 (SIN)	個人情報: PII	CANADA_SOCIAL_INSURANCE_NUMBER	はい	カナダ
社会保障番号 (SSN)	個人情報: PII	国またはリージョンによって異なります: SPAIN_SOCIAL_SECURITY_NUMBER、USA_SOCIAL_SECURITY_NUMBER	はい	スペイン、米国
the section called “ストライプ API キー”	認証情報	STRIPE_CREDENTIALS	いいえ	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
納税者識別番号または参照番号	個人情報: PII	国またはリージョンによって異なります。 AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	はい	オーストラリア、ブラジル、フランス、ドイツ、インド、イタリア、スペイン、英国、米国
機器固有識別子 (UDI)	個人情報: PHI	MEDICAL_DEVICE_UDI	はい	米国

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
車両識別番号 (VIN)	個人情報: PII	VEHICLE_IDENTIFICATION_NUMBER	はい	すべて (VIN が英語、フランス語、ドイツ語、リトアニア語、ポーランド語、ポルトガル語、ルーマニア語、またはスペイン語のいずれかの言語でキーワードの近くにある場合)

詳細リファレンス:Amazon Macie マネージドデータ識別子

Amazon Macieでは、管理されたデータ識別子は、特定のタイプの機密データを検出するために設計された組み込みの基準とテクニックです。これらは、複数タイプの認証情報データ、財務情報、個人情報など、多くの国や地域で増加している大規模な機密データのリストを検出できます。各マネージドデータ識別子は、特定の種類の機密データ (AWS シークレットアクセスキー、クレジットカード番号、特定の国や地域のパスポート番号など) を検出するように設計されています。

Macie は、マネージドデータ識別子を使用して、いくつかのカテゴリの機密データを検出できます。各カテゴリ内で、Macie は複数のタイプの機密データを検出できます。このセクションのトピックでは、各タイプとデータ検出に関連する要件をリスト化して説明します。特定のタイプの機密データのマネージドデータ識別子に関する詳細については、カテゴリ別にトピックを参照してください。

- 認証情報 — AWS 秘密鍵や秘密アクセスキーなどの認証情報データ用。
- 財務情報— クレジットカード番号や銀行口座番号などの財務データ関連

- 個人情報:PHI— 健康保険や医療識別番号などの個人健康情報 (PHI) 関連
- 個人情報:PII — 運転免許証の識別番号やパスポート番号など個人を特定できる情報 (PII) 関連

また、次の表から特定のタイプの機密データを選択することもできます。この表には、Macie が現在提供しているすべてのマネージドデータ識別子が機密データタイプ別にまとめられています。この表には、各タイプの検出に関連する要件もまとめられています。

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
AWS シークレットアクセスキー	認証情報	AWS_CREDENTIALS	はい	すべて
銀行口座番号	財務情報	BANK_ACCOUNT_NUMBER(カナダと米国の場合)、	はい	カナダ、米国
基本銀行口座番号 (BBAN)	財務情報	国またはリージョンによって異なります。 FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	はい	フランス、ドイツ、イタリア、スペイン、英国
生年月日	個人情報: PHI	DATE_OF_BIRTH	はい	すべて
クレジットカードの有効期限	財務情報	CREDIT_CARD_EXPIRATION	はい	すべて
クレジットカードの磁気ストライプデータ	財務情報	CREDIT_CARD_MAGNETIC_STRIPE	はい	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
クレジットカード番号	財務情報	CREDIT_CARD_NUMBER (キーワードに近いクレジットカード番号の場合) と CREDIT_CARD_NUMBER_(NO_KEYWORD) (キーワードに近くないクレジットカード番号の場合)	可変	すべて
クレジットカード認証コード	財務情報	CREDIT_CARD_SECURITY_CODE	はい	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
運転免許証識別番号	個人情報: PII	国またはリージョンによって異なります。 AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	はい	オーストラリア、オーストリア、ベルギー、ブルガリア、カナダ、クロアチア、キプロス、チェコ共和国、デンマーク、エストニア、フィンランド、フランス、ドイツ、ギリシャ、ハンガリー、インド、アイルランド、イタリア、ラトビア、リトアニア、ルクセンブルク、マルタ、オランダ、ポーランド、ポルトガル、ルーマニア、スロバキア、スロベ

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		ニア、スペイン、スウェーデン、英国、米国
麻薬取締局 (DEA) 登録番号	個人情報: PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	はい	米国
選挙人名簿番号	個人情報: PII	UK_ELECTORAL_ROLL_NUMBER	はい	UK
フルネーム	個人情報: PII	NAME	いいえ	すべて (名前にラテン文字セットが使用されている場合)
全地球測位システム (GPS) 座標	個人情報: PII	LATITUDE_LONGITUDE	はい	すべて (座標が英語のキーワードの近くにある場合)
Google Cloud API キー	認証情報	GCP_API_KEY	はい	すべて
健康保険請求番号 (HICN)	個人情報: PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	はい	米国

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
健康保険または医療識別番号	個人情報: PHI	国またはリージョンによって異なります。 CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	はい	カナダ、EU、フィンランド、フランス、英国、米国
ヘルスケア共通手順コーディングシステム (HCPCS) コード	個人情報: PHI	USA_HEALTHCARE_PROCEDURE_CODE	はい	米国
HTTP 基本認証ヘッダー	認証情報	HTTP_BASIC_AUTH_HEADER	いいえ	すべて
HTTP クッキー	個人情報: PII	HTTP_COOKIE	いいえ	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
国際銀行口座番号 (IBAN)	財務情報	国またはリージョンによって異なります。 ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER	いいえ	アルバニア、アンドラ、ボスニア・ヘルツェゴビナ、ブラジル、ブルガリア、コスタリカ、クロアチア、キプロス、チェコ共和国、デンマーク、ドミニカ共和国、エジプト、エストニア、フェロー諸島、フィンランド、フランス、ジョージア、ドイツ、ギリシャ、グリーンランド、ハンガリー、アイスランド、アイルランド、イタリア、ヨルダン、コ

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
		, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER		ソボ、リヒテンシュタイン、リトアニア、マルタ、モーリタニア、モーリシャス、モナコ、モンテネグロ、オランダ、北マケドニア、ポーランド、ポルトガル、サンマリノ、セネガル、セルビア、スロバキア、スロベニア、スペイン、スウェーデン、スイス、東ティモール、チュニジア、トルコ、英国、ウクライナ、アラブ首長国連邦、バージ

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
		, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (イギリス領バージン諸島用)		ン諸島 (英国)
JSON ウェブトークン (JWT)	認証情報	JSON_WEB_TOKEN	いいえ	すべて
郵送先住所	個人情報: PII	ADDRESS、BRAZIL_CEP_CODE (ブラジルの Código de Endereçamento Postal の場合)	可変	オーストラリア、ブラジル、カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国
全米医薬品コード (NDC)	個人情報: PHI	USA_NATIONAL_DRUG_CODE	はい	米国
国民識別番号	個人情報: PII	国またはリージョンによって異なります。 BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	はい	ブラジル、フランス、ドイツ、インド、イタリア、スペイン

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
国民保険番号 (NINO)	個人情報: PII	UK_NATIONAL_INSURANCE_NUMBER	はい	UK
国家プロバイダー識別子 (NPI)	個人情報: PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	はい	米国
OpenSSH プライベートキー	認証情報	OPENSSH_PRIVATE_KEY	いいえ	すべて
パスポート番号	個人情報: PII	国またはリージョンによって異なります。 CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	はい	カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国
本籍地	個人情報: PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	はい	カナダ
PGP プライベートキー	認証情報	PGP_PRIVATE_KEY	いいえ	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
電話番号	個人情報: PII	国またはリージョンによって異なります。 BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	可変	ブラジル、カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国
公開鍵暗号標準 (PKCS) プライベートキー	認証情報	PKCS	いいえ	すべて
PuTTY プライベートキー	認証情報	PUTTY_PRIVATE_KEY	いいえ	すべて
社会保険番号 (SIN)	個人情報: PII	CANADA_SOCIAL_INSURANCE_NUMBER	はい	カナダ
社会保障番号 (SSN)	個人情報: PII	国またはリージョンによって異なります: SPAIN_SOCIAL_SECURITY_NUMBER、USA_SOCIAL_SECURITY_NUMBER	はい	スペイン、米国
the section called “ストライプ API キー”	認証情報	STRIPE_CREDENTIALS	いいえ	すべて

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
納税者識別番号または参照番号	個人情報: PII	国またはリージョンによって異なります。 AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	はい	オーストラリア、ブラジル、フランス、ドイツ、インド、イタリア、スペイン、英国、米国
機器固有識別子 (UDI)	個人情報: PHI	MEDICAL_DEVICE_UDI	はい	米国

機密データタイプ	機密データのカテゴリ	マネージドデータ識別子 ID	キーワードが必須	国とリージョン
車両識別番号 (VIN)	個人情報: PII	VEHICLE_IDENTIFICATION_NUMBER	はい	すべて (VIN が英語、フランス語、ドイツ語、リトアニア語、ポーランド語、ポルトガル語、ルーマニア語、またはスペイン語のいずれかの言語でキーワードの近くにある場合)

認証情報データのマネージドデータ識別子

Amazon Macie は、マネージドデータ識別子を使用して、複数のタイプの機密認証情報データを検出できます。このページのトピックでは、各タイプを指定し、データを検出するように設計されたマネージドデータ識別子に関する情報を提供します。このトピックでは、以下に関する情報を提供します。

- マネージドデータ識別子 ID — データを検出するように設計されたマネージドデータ識別子の一意の識別子 (ID) を指定します。機密データ検出ジョブを作成したり、機密データの自動検出設定を設定したりする場合、これらの ID を使用して Macie がデータを分析するときに使用するマネージドデータ ID を指定できます。
- サポートされている国と地域 — 該当するマネージドデータ識別子がどの国または地域を対象に設計されているかを示します。マネージドデータ識別子が特定の国または地域向けに設計されていない場合、この値は Any になります。

- キーワードが必要 — 検出には、キーワードがデータの近くにある必要があるかどうかを指定します。キーワードが必要な場合、トピックには必要なキーワードの例も記載されています。Macie がデータを分析する際にどのようにキーワードを使用するかについては、キーワード要件 を参照してください。
- コメント — マネージドデータ識別子の選択や、報告された機密データの出現状況に関する調査に影響する可能性のある関連情報を提供します。詳細には、サポートされている標準、構文要件、例外などの情報が含まれます。

トピックは機密データタイプのアルファベット順にリストされています。

機密データタイプ

- AWS シークレットアクセスキー
- Google Cloud API キー
- HTTP 基本認証ヘッダー
- JSON ウェブトークン (JWT)
- OpenSSH プライベートキー
- PGP プライベートキー
- 公開鍵暗号標準 (PKCS) プライベートキー
- PuTTY プライベートキー
- ストライプ API キー

AWS シークレットアクセスキー

マネージドデータ識別子 ID: AWS_CREDENTIALS

サポートされている国と地域: すべて

キーワードが必須: はい。キーワードには: aws_secret_access_key, credentials, secret access key, secret key, set-awscredentialが含まれます。

コメント: Macie は、架空の例としてよく使われる次の文字シーケンスの出現をレポートしません。`je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY` および `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Google Cloud API キー

マネージドデータ識別子 ID: GCP_API_KEY

サポートされている国と地域: すべて

キーワードが必須: はい。キーワードには: G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-keyが含まれます。

コメント: Macie は Google Cloud API キーの文字列 `keyString` コンポーネントのみを検出できます。Support には、Google Cloud API キーの ID または表示名コンポーネントの検出は含まれていません。

HTTP 基本認証ヘッダー

マネージドデータ識別子 ID: HTTP_BASIC_AUTH_HEADER

サポートされている国と地域: すべて

キーワードが必須: いいえ

コメント: 検出には、RFC 7617 で指定されているように、フィールド名と認証スキームディレクティブを含む完全なヘッダーが必要です。例: `Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==` および `Proxy-Authorization: Basic dGVzdDoxMjPCow==`。

JSON ウェブトークン (JWT)

マネージドデータ識別子 ID: JSON_WEB_TOKEN

サポートされている国と地域: すべて

キーワードが必須: いいえ

コメント: Macie は、JSON ウェブ署名 (JWS) 構造に関する RFC 7519 で規定されている要件に準拠する JSON ウェブトークン (JWT) を検出できます。トークンは署名付きでも署名なしでもかまいません。

OpenSSH プライベートキー

マネージドデータ識別子 ID: OPENSSH_PRIVATE_KEY

サポートされている国と地域: すべて

キーワードが必須: いいえ

コメント: なし

PGP プライベートキー

マネージドデータ識別子 ID: PGP_PRIVATE_KEY

サポートされている国と地域: すべて

キーワードが必須: いいえ

コメント: なし

公開鍵暗号標準 (PKCS) プライベートキー

マネージドデータ識別子 ID: PKCS

サポートされている国と地域: すべて

キーワードが必須: いいえ

コメント: なし

PuTTY プライベートキー

マネージドデータ識別子 ID: PUTTY_PRIVATE_KEY

サポートされている国と地域: すべて

キーワードが必須: いいえ

コメント： Macie は、、PuTTY-User-Key-File、、Encryption、、Private-Linesおよび の標準ヘッダーとヘッダーシーケンスを使用する PuTTY Comment Public-Linesプライベートキーを検出できますPrivate-MAC。ヘッダー値には、英数字、ハイフン (-) 、改行文字 (\n または) を含めることができます\r。 Public-Linesおよび Private-Linesの値には、スラッシュ ()、プラス記号 (/) 、等号 (+) を含めることもできます=。 Private-MACの値にはプラス記号 () を含めることもできます+。サポートには、スペースやアンダースコア () など、他の文字を含むヘッダー値を持つプライベートキーの検出は含まれません_。サポートには、カスタムヘッダーを含むプライベートキーの検出は含まれません。

ストライプ API キー

マネージドデータ識別子 ID: STRIPE_CREDENTIALS

サポートされている国と地域: すべて

キーワードが必須: いいえ

コメント: Macie は、Stripe のコード例でよく使われる、次の文字シーケンスの出現を報告していません。`sk_test_4eC39HqLyjWDarjtT1zdp7dc` および `pk_test_TYooMQauvdEDq54NiTphI7jx`

財務情報のマネージドデータ識別子

Amazon Macie がマネージドデータ識別子を使用して検出できる財務情報の種類について説明します。このページのトピックでは、それぞれのタイプを一覧表示し、データを検出するために設計されたマネージドデータ識別子に関する情報を提供しています。このトピックでは、以下に関する情報を提供します。

- マネージドデータ識別子 ID — データを検出するように設計された 1 つ以上のマネージドデータ識別子の一意の識別子 (ID) を指定します。機密データ検出ジョブを作成したり、機密データの自動検出設定を設定したりする場合、これらの ID を使用して Macie がデータを分析するときに使用するマネージドデータ ID を指定できます。
- サポートされている国と地域 — 該当するマネージドデータ識別子がどの国または地域を対象に設計されているかを示します。マネージドデータ識別子が特定の国や地域向けに設計されていない場合、この値はいずれかになります。
- キーワードが必要 — 検出には、キーワードがデータの近くにある必要があるかどうかを指定します。キーワードが必要な場合、トピックには必要なキーワードの例も記載されています。Macie がデータを分析する際にどのようにキーワードを使用するかについては、キーワード要件 を参照してください。
- コメント — マネージドデータ識別子の選択や、報告された機密データの出現状況に関する調査に影響する可能性のある関連情報を提供します。詳細には、サポートされている標準、構文要件、例外などの情報が含まれます。

トピックは機密データタイプのアルファベット順にリストされています。

機密データタイプ

- 銀行口座番号
- 基本銀行口座番号 (BBAN)
- クレジットカードの有効期限
- クレジットカードの磁気ストライプデータ

- クレジットカード番号
- クレジットカード認証コード
- 国際銀行口座番号 (IBAN)

銀行口座番号

Macie では、9 ~ 17 桁のシーケンスで設定され、スペースが含まれないカナダおよび米国の銀行口座番号を検出できます。

マネージドデータ識別子 ID: BANK_ACCOUNT_NUMBER

サポートされている国と地域: カナダ、米国

キーワードが必須: はい。キーワードには: bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct が含まれます。

コメント: このマネージドデータ識別子は、カナダと米国の銀行口座番号を検出するために特別に設計されています。これらの国では、ISO 13616 の規定による銀行口座の番号付けのための ISO 国際規格で定義されている基本銀行口座番号 (BBAN) または国際銀行口座番号 (IBAN) 形式を使用していません。他の国や地域の銀行口座番号を検出するには、その形式用に設計されたマネージドデータ識別子を使用してください。詳細については、「基本銀行口座番号 (BBAN)」および「国際銀行口座番号 (IBAN)」を参照してください。

基本銀行口座番号 (BBAN)

Macie は、ISO 13616 の規定による銀行口座の番号付けのための ISO 国際標準で定義されている BBAN 構造に準拠する基本銀行口座番号 (BBAN) を検出できます。これには、スペースを含まない BBAN が含まれるか、`NWBK60161331926819`、`NWBK 6016 1331 9268 19`、および `NWBK-6016-1331-9268-19` などのスペースやハイフンの区切り文字を使用します。

マネージドデータ識別子 ID: 国やリージョンによっては、FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

サポートされている国と地域: フランス、ドイツ、イタリア、スペイン、英国

キーワードが必須: はい。次のテーブルに、Macie が特定の国およびリージョンについて認識するキーワードのリストを示します。

国またはリージョン	キーワード
フランス	account code, account number, accountno#, accountnumber#, bban, code bancaire, compte bancaire, customer account id, customer account number, customer bank account id, iban, numéro de compte
ドイツ	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzahl, iban, kartennummer, kontonummer, kreditkartennummer, sepa
イタリア	account code, account number, accountno #, accountnumber#, bban, codice bancario, conto bancario, customer account id, customer account number, customer bank account id, iban, numero di conto
スペイン	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account number, customer bank account id, iban, número cuenta bancaria cliente, número cuenta cliente
英国	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

コメント: これらのマネージドデータ識別子は、ISO 13616 規格に準拠する国際銀行口座番号 (IBAN) も検出できます。詳細については、国際銀行口座番号 (IBAN) を参照してください。英国のマネー

ジドデータ識別子 UK_BANK_ACCOUNT_NUMBER は、たとえば 60-16-13 31926819 など英国の国内銀行口座番号も検出できます。

クレジットカードの有効期限

マネージドデータ識別子 ID: CREDIT_CARD_EXPIRATION

サポートされている国と地域: すべて

キーワードが必須: はい。キーワードには: exp d, exp m, exp y, expiration, expiryが含まれます。

Comments (コメント): Support には、すべての数字や数字と月の名前の組み合わせなど、ほとんどの日付形式が含まれます。日付コンポーネントは、スラッシュ (/)、ハイフン (-)、または該当するキーワードで区切ることができます。たとえば、Macie は02/26、02/2026、Feb 2026、26-Feb、および expY=2026, expM=02 などの日付を検出できます。

クレジットカードの磁気ストライプデータ

マネージドデータ識別子 ID: CREDIT_CARD_MAGNETIC_STRIPE

サポートされている国と地域: すべて

キーワードが必須: はい。キーワードには: card data, iso7813, mag, magstripe, stripe, swipeが含まれます。

コメント: Supportにはトラック 1 と 2 が含まれます。

クレジットカード番号

マネージドデータ識別子 ID: キーワードに近いクレジットカード番号の場合は CREDIT_CARD_NUMBER、キーワードに近くないクレジットカード番号の場合は CREDIT_CARD_NUMBER_(NO_KEYWORD)

サポートされている国と地域: すべて

必須キーワード: 不定です。キーワードは、CREDIT_CARD_NUMBERマネージドデータ識別子で必要です。キーワードには: account number, american express, amex, bank card, c card, card, cc #, ccn, check card, cred card, credit, credit card, credit cards, credit no, credit num, dankort, debit, debit card, debit no, debit num, diners club, discover, electron, japanese card bureau, jcb, mastercard, mc, pan, payment account number, payment card number, pcn, pmnt #, pmnt card, pmnt no, pmnt number, union pay, visaが含まれます。CREDIT_CARD_NUMBER_(NO_KEYWORD) マネージドデータ識別子にはキーワードは必要ありません。

コメント： 検出では、データは Luhn チェック式に準拠する 13 ~ 19 桁のシーケンスである必要があります。また、American Express、Dankort、Diner's Club、Discover、Electron、日本語カード局 (JCB)、Mastercard UnionPay、Visa のいずれかのタイプのクレジットカードに標準のカード番号プレフィックスを使用します。

Macie、クレジットカード発行会社が公開テスト用に予約している以下のシーケンスの発生を報告していない：122000000000003, 2222405343248877, 2222990905257051, 2223007648726984, 2223577120017656, 30569309025904, 34343434343434, 3528000700000000, 3530111333300000, 3566002020360505, 36148900647913, 36700102000000, 371449635398431, 378282246310005, 378734493671000, 38520000023237, 4012888888881881, 4111111111111111, 4222222222222, 4444333322221111, 4462030000000000, 4484070000000000, 4911830000000, 4917300800000000, 4917610000000000, 49176100000000000003, 5019717010103742, 5105105105105100, 5111010030175156, 5185540810000019, 5200828282828210, 5204230080000017, 5204740009900014, 5420923878724339, 5454545454545454, 5455330760000018, 5506900490000436, 5506900490000444, 5506900510000234, 5506920809243667, 5506922400634930, 5506927427317625, 5553042241984105, 5555553753048194, 5555555555554444, 5610591081018250, 6011000990139424, 6011000400000000, 6011111111111117, 63049001774029244l, 63049506000000000, 6331101999990016, 6759649826438453, 6799990100000000019, と76009244561.

クレジットカード認証コード

マネージドデータ識別子 ID CREDIT_CARD_SECURITY_CODE

サポートされている国と地域: すべて

キーワードが必須: はい。キーワードには: card id, card identification code, card identification number, card security code, card validation code, card validation number, card verification data, card verification value, cvc, cvc2, cvv, cvv2, elo verification codeが含まれます。

コメント: なし

国際銀行口座番号（IBAN）

Macieは、国コードなどの要素を含む最大34文字の英数字で設定される国際銀行口座番号（IBAN）を検出することができます。具体的には、Macie は ISO 13616 の規定による銀行口座の番号付けのための ISO 国際標準に準拠する IBAN を検出できます。これには、スペースを含まない IBAN が含まれるか、GB29NWBK60161331926819、GB29 NWBK 6016 1331 9268 19、および GB29-

NWBK-6016-1331-9268-19 などのスペースやハイフンの区切り文字を使用します。検出には、Modulus 97 スキームに基づく検証チェックが含まれます。

マネージドデータ識別子 ID: 国やリージョンによっては、ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (イギリス領バージン諸島の場合)

サポートされている国と地域: アルバニア、アンドラ、ボスニア・ヘルツェゴビナ、ブラジル、ブルガリア、コスタリカ、クロアチア、キプロス、チェコ共和国、デンマーク、ドミニカ共和国、エジプト、エストニア、フェロー諸島、フィンランド、フランス、ジョージア、ドイツ、ギリシャ、グリーンランド、ハンガリー、アイスランド、アイルランド、イタリア、ヨルダン、コソボ、リヒテンシュ

タイン、リトアニア、マルタ、モーリタニア、モーリシャス、モナコ、モンテネグロ、オランダ、北マケドニア、ポーランド、ポルトガル、サンマリノ、セネガル、セルビア、スロバキア、スロベニア、スペイン、スウェーデン、スイス、東ティモール、チュニジア、トルコ、英国、ウクライナ、アラブ首長国連邦エミレーツ、バージン諸島 (英国)

キーワードが必須: いいえ

コメント: フランス、ドイツ、イタリア、スペイン、英国のマネージドデータ識別子では、ISO 13616 規格で定義されている BBAN 構造に準拠する基本銀行口座番号 (BBAN) も検出できます (文字列がキーワードに近い場合)。詳細については、基本銀行口座番号 (BBAN)を参照してください。

個人健康情報 (PHI) のマネージドデータ識別子

Amazon Macie では、マネージドデータ識別子を使用して複数のタイプの機密の個人健康情報 (PHI) を検出できます。このページのトピックでは、各タイプを指定し、データを検出するように設計されたマネージドデータ識別子に関する情報を提供します。このトピックでは、以下に関する情報を提供します。

- マネージドデータ識別子 ID — データを検出するように設計されたマネージドデータ識別子の一意の識別子 (ID) を指定します。機密データ検出ジョブを作成したり、機密データの自動検出設定を設定したりする場合、これらの ID を使用して Macie がデータを分析するときに使用するマネージドデータ ID を指定できます。
- サポートされている国と地域 — 該当するマネージドデータ識別子がどの国または地域を対象に設計されているかを示します。マネージドデータ識別子が特定の国または地域向けに設計されていない場合、この値は Any になります。
- キーワードが必要 — 検出には、キーワードがデータの近くにある必要があるかどうかを指定します。キーワードが必要な場合、トピックには必要なキーワードの例も記載されています。Macie がデータを分析する際にどのようにキーワードを使用するかについては、キーワード要件 を参照してください。
- コメント — マネージドデータ識別子の選択や、報告された機密データの出現状況に関する調査に影響する可能性のある関連情報を提供します。詳細には、サポートされている標準、構文要件、例外などの情報が含まれます。

トピックは機密データタイプのアルファベット順にリストされています。

機密データタイプ

- 麻薬取締局 (DEA) 登録番号

- 健康保険請求番号 (HICN)
- 健康保険または医療識別番号
- ヘルスケア共通手順コーディングシステム (HCPCS) コード
- 全米医薬品コード (NDC)
- 国家プロバイダー識別子 (NPI)
- 機器固有識別子 (UDI)

麻薬取締局 (DEA) 登録番号

マネージドデータ識別子 ID: US_DRUG_ENFORCEMENT_AGENCY_NUMBER

サポートされている国と地域: 米国

キーワードが必須: はい。キーワードには: dea number, dea registrationが含まれます。

コメント: なし

健康保険請求番号 (HICN)

マネージドデータ識別子 ID: USA_HEALTH_INSURANCE_CLAIM_NUMBER

サポートされている国と地域

キーワードが必須: はい。キーワードには: health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#が含まれます。

コメント: なし

健康保険または医療識別番号

EUとフィンランドの欧州健康保険証番号、フランスの健康保険番号、米国のメディケア受給者番号、英国のNHS番号、カナダのパーソナル・ヘルス・ナンバーをサポートしています。

マネージドデータ識別子 ID: 国やリージョンによっては、CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

サポートされている国と地域: カナダ、EU、フィンランド、フランス、英国、米国

キーワードが必須: はい。次のテーブルに、Macie が特定の国およびリージョンについて認識するキーワードのリストを示します。

国またはリージョン	キーワード
カナダ	canada healthcare number, msp number, personal healthcare number, phn, soins de santé
EU	assicurazione sanitaria numero, carta assicurazione numero, carte d’assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d’assurance maladie, numéro de carte d’assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausvakuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicherungsnummer
フィンランド	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskort, hälsokort, health card, health card number, health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin, sairausvakuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskor

国またはリージョン	キーワード
	t, suomen sairausvakuutuskortti, suomi ehic-numero, terveyskortti
フランス	carte d'assuré social, carte vitale, insurance card
英国	national health service, NHS
US	mbi, medicare beneficiary

コメント: なし

ヘルスケア共通手順コーディングシステム (HCPCS) コード

マネージドデータ識別子 ID: USA_HEALTHCARE_PROCEDURE_CODE

サポートされている国と地域: 米国

キーワードが必須: はい。キーワードには: current procedural terminology, hcpcs, healthcare common procedure coding systemが含まれます。

コメント: なし

全米医薬品コード (NDC)

マネージドデータ識別子 ID: USA_NATIONAL_DRUG_CODE

サポートされている国と地域: 米国

キーワードが必須: はい。キーワードには: national drug code, ndcが含まれます。

コメント: なし

国家プロバイダー識別子 (NPI)

マネージドデータ識別子 ID: USA_NATIONAL_PROVIDER_IDENTIFIER

サポートされている国と地域: 米国

キーワードが必須: はい。キーワードには: hipaa, n.p.i, national provider, npiが含まれます。

コメント: なし

機器固有識別子 (UDI)

マネージドデータ識別子 ID: MEDICAL_DEVICE_UDI

サポートされている国と地域: 米国

キーワードが必須: はい。キーワードには: blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifierが含まれます。

コメント: Macie は、米国食品医薬品局が承認した形式に準拠する一意のデバイス識別子 (UDI) を検出できます。これには GS1、HIBCC、および ICCBBA で定義されている標準フォーマットが含まれます。ICCBA は ISBT 標準をサポートしています。

個人を特定できる情報 (PII) のマネージドデータ識別子

Amazon Macie は、マネージドデータ識別子を使用して、複数のタイプの個人を特定できる情報 (PII) 機密データを検出できます。このページのトピックでは、それぞれのタイプを一覧表示し、データを検出するために設計されたマネージドデータ識別子に関する情報を提供しています。各トピックは以下の情報を提供します。

- マネージドデータ識別子 ID — データを検出するように設計された 1 つ以上のマネージドデータ識別子の一意の識別子 (ID) を指定します。機密データ検出ジョブを作成したり、機密データの自動検出設定を設定したりする場合、これらの ID を使用して Macie がデータを分析するときに使用するマネージドデータ ID を指定できます。
- サポートされている国と地域 — 該当するマネージドデータ識別子がどの国または地域を対象に設計されているかを示します。マネージドデータ識別子が特定の国や地域向けに設計されていない場合、この値はいずれかになります。
- キーワードが必要 — 検出には、キーワードがデータの近くにある必要があるかどうかを指定します。キーワードが必要な場合、トピックには必要なキーワードの例も記載されています。Macie がデータを分析する際にどのようにキーワードを使用するかについては、キーワード要件 を参照してください。
- コメント — マネージドデータ識別子の選択や、報告された機密データの出現状況に関する調査に影響する可能性のある関連情報を提供します。詳細には、サポートされている標準、構文要件、例外などの情報が含まれます。

トピックは機密データタイプのアルファベット順にリストされています。

機密データタイプ

- 生年月日

- 運転免許証識別番号
- 選挙人名簿番号
- フルネーム
- 全地球測位システム (GPS) 座標
- HTTP クッキー
- 郵送先住所
- 国民識別番号
- 国民保険番号 (NINO)
- パスポート番号
- 本籍地
- 電話番号
- 社会保険番号 (SIN)
- 社会保障番号 (SSN)
- 納税者識別番号または参照番号
- 車両識別番号 (VIN)

生年月日

マネージドデータ識別子 ID: DATE_OF_BIRTH

サポートされている国と地域: すべて

キーワードが必須: はい。キーワードには: bday, b-day, birth date, birthday, date of birth, dobが含まれます。

Comments (コメント): Support には、すべての数字や数字と月の名前の組み合わせなど、ほとんどの日付形式が含まれます。日付コンポーネントは、スペース、スラッシュ (/)、またはハイフン (-) で区切ることができます。

運転免許証識別番号

マネージドデータ識別子 ID: 国や地域によっては、AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE,

FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE

サポートされている国と地域: オーストラリア、オーストリア、ベルギー、ブルガリア、カナダ、クロアチア、キプロス、チェコ共和国、デンマーク、エストニア、フィンランド、フランス、ドイツ、ギリシャ、ハンガリー、インド、アイルランド、イタリア、ラトビア、リトアニア、ルクセンブルク、マルタ、オランダ、ポーランド、ポルトガル、ルーマニア、スロバキア、スロベニア、スペイン、スウェーデン、英国、米国

キーワードが必須: はい。次のテーブルに、Macie が特定の国およびリージョンについて認識するキーワードのリストを示します。

国またはリージョン	キーワード
オーストラリア	dl#, dl:, dlno#, driver licence, driver license, driver permit, drivers lic., drivers licence, driver's licence, drivers license, driver's license, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
オーストリア	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
ベルギー	fuehrerschein, fuehrerschein- nr, fuehrerschheinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrerschheinnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer

国またはリージョン	キーワード
ブルガリア	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка
カナダ	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit, permis de conduire
クロアチア	vozačka dozvola
キプロス	άδεια οδήγησης
チェコ共和国	číslo licence, číslo licence řidiče, číslo řidičského průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský prúkaz, řidičský průkaz
デンマーク	kørekort, kørekortnummer
エストニア	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
フィンランド	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire
フランス	permis de conduire

国またはリージョン	キーワード
ドイツ	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer
ギリシャ	δεια οδήγησης, adeia odigisis
ハンガリー	illesztőprogramok lic, jogosítvány, jogsi, licencszám, vezető engedély, vezetői engedély
インド	driver licence, driver licences, driver license, driver licenses, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, driving licence, driving license
アイルランド	ceadúnas tiomána
イタリア	patente di guida, patente di guida numero, patente guida, patente guida numero
ラトビア	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
リトアニア	vairuotojo pažymėjimas
ルクセンブルグ	fahrerlaubnis, führerschäin
マルタ	liċenzja tas-sewqan
オランダ	permis de conduire, rijbewijs, rijbewijsnummer
ポーランド	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie

国またはリージョン	キーワード
ポルトガル	carta de condução, carteira de habilitação, carteira de motorist, carteira habilitação, carteira motorist, licença condução, licença de condução, número de licença, número licença, permissão condução, permissão de condução
ルーマニア	numărul permisului de conducere, permis de conducere
スロバキア	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
スロベニア	vozniško dovoljenje
スペイン	carnet conducer, el carnet de conducer, licencia conducer, licencia de manejo, número carnet conducer, número de carnet de conducer, número de permiso conducer, número de permiso de conducer, número licencia conducer, número permiso conducer, permiso conducción, permiso conducer, permiso de conducción
スウェーデン	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsn ummer, kuljettajat lic.

国またはリージョン	キーワード
英国	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
米国	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

コメント: なし

選挙人名簿番号

マネージドデータ識別子 ID: UK_ELECTORAL_ROLL_NUMBER

サポートされている国と地域: 英国

キーワードが必須: はい。キーワードには: electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollnoが含まれます。

コメント: なし

フルネーム

マネージドデータ識別子 ID: NAME

サポートされている国と地域: すべて

キーワードが必須: いいえ

Comments (コメント): Macie はフルネームのみを検出できます。Support はラテン文字セットに限定されます。

全地球測位システム (GPS) 座標

マネージドデータ識別子 ID: LATITUDE_LONGITUDE

サポートされる国と地域: 座標が英語のキーワードに近い場合は任意。

キーワードが必須: はい。キーワードには: coordinate, coordinates, lat long, latitude longitude, positionが含まれます。

Comments (コメント): Macie は、緯度と経度の座標がペアとして保存され、それらが10 進度 (DD) 形式の場合、GPS 座標を検出できます (たとえば、`41.948614,-87.655311`)。Support には、たとえば、度 10 進分 (DDM) 形式 (たとえば、`41°56.9168'N 87°39.3187'W`)、または、度、分、秒 (DMS) 形式 (たとえば、`41°56'55.0104"N 87°39'19.1196"W`) の座標の検出は含まれません。

HTTP クッキー

マネージドデータ識別子 ID: HTTP_COOKIE

サポートされている国と地域: すべて

キーワードが必須: いいえ

コメント: 検出には完全な `Cookie` または `Set-Cookie` ヘッダーが必要です。ヘッダーには、名前と値のペアを 1 つ以上含めることができます。例えば、`Set-Cookie: id=TWlrZQ` と `Cookie: session=3948; lang=en`。

郵送先住所

管理データ識別子 ID: ADDRESS (オーストラリア、カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国向け)、BRAZIL_CEP_CODE (ブラジルの郵便局コード)

サポートされている国と地域:オーストラリア、ブラジル、カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国

必須キーワード: 不定です。管理データ識別子にはキーワードは必要ありません。ADDRESSBRAZIL_CEP_CODE管理データ識別子にはキーワードが必要です。キーワードには: cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postalが含まれます。

コメント:ADDRESSマネージドデータ ID ではキーワードは必須ではありませんが、検出には都市名または場所名と、サポートされている国または地域の対応する ZIP コードまたは郵便番号を含む住所が必要です。BRAZIL_CEP_CODEマネージドデータ識別子は、住所の郵便番号 (CEP) 部分のみを検出できます。

国民識別番号

サポートには、インドの Aadhaar 番号、イタリアの Codice Fiscale 番号、スペインの Documento Nacional de Identidad (DNI) 識別子、フランス国立統計経済研究所 (INSEE) コード、ドイツの国民 ID カード番号、ブラジルの Registro Geral (RG) 番号が含まれます。

マネージドデータ識別子 ID: 国や地域によっては、BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

サポートされている国と地域: ブラジル、フランス、ドイツ、インド、イタリア、スペイン

キーワードが必須: はい。次のテーブルに、Macie が特定の国およびリージョンについて認識するキーワードのリストを示します。

国またはリージョン	キーワード
ブラジル	registro geral, rg
フランス	assurance sociale, carte nationale d’identité, cni, code sécurité sociale, French social security number, fssn#, insee, insurance number, national id number, nationalid#, numéro d'assurance, sécurité sociale, sécurité sociale non., sécurité sociale numéro, social, social security, social security number, socialsecuritynumber, ss#, ssn, ssn#
ドイツ	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
インド	aadhaar, aadhar, adhaar, uidai

国またはリージョン	キーワード
イタリア	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
スペイン	dni, dni#, dninúmero#, documento nacional de identidad, identidad único, identidadúnico#, insurance number, national identification number, national identity, nationalid#, nationali dno#, número nacional identidad, personal identification number, personal identity no, unique identity number, uniqueid#

コメント: なし

国民保険番号 (NINO)

マネージドデータ識別子 ID: UK_NATIONAL_INSURANCE_NUMBER

サポートされている国と地域: 英国

キーワードが必須: はい。キーワードには: insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, ninoが含まれます。

コメント: なし

パスポート番号

マネージドデータ識別子 ID: 国や地域によっては、CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

サポートされている国と地域: カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国

キーワードが必須: はい。次のテーブルに、Macie が特定の国およびリージョンについて認識するキーワードのリストを示します。

国またはリージョン	キーワード
カナダ	passeport, passeport#, passport, passport#, passportno, passportno#
フランス	numéro de passeport, passeport, passeport #, passeport n °, passeport non
ドイツ	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass–nr, reisepassnummer
イタリア	italian passport number, numéro passeport, numéro passeport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
スペイン	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport
英国	passeport #, passeport n °, passeport non, passeportn °, passport #, passport no, passport number, passport#, passportid
米国	passport, travel document

コメント: なし

本籍地

マネージドデータ識別子 ID: CANADA_NATIONAL_IDENTIFICATION_NUMBER

サポートされている国と地域:カナダ

キーワードが必須: はい。キーワードには: carte résident permanent, numéro carte résident permanent, numéro résident permanent, permanent resident card, permanent resident card number,

permanent resident no, permanent resident no., permanent resident number, pr no, pr no., pr non, pr number, résident permanent no., résident permanent nonが含まれます。

コメント: なし

電話番号

マネージドデータ識別子 ID: 国や地域によっては、BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER

サポートされている国と地域: ブラジル、カナダ、フランス、ドイツ、イタリア、スペイン、英国、米国

必須キーワード: 不定です。キーワードがデータの近くにある場合、番号に国コードを含める必要はありません。キーワードには: cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone numberが含まれます。ブラジル: キーワードにはcel, celular, fone, móvel, número residencial, numero residencial, telefone.も含まれます。キーワードがデータの近くにない場合は、番号に国コードを含める必要があります。

コメント: 米国では、サポートには通話料無料の番号が含まれます。

社会保険番号 (SIN)

マネージドデータ識別子 ID: CANADA_SOCIAL_INSURANCE_NUMBER

サポートされている国と地域:カナダ

キーワードが必須: はい。キーワードには: canadian id, numéro d'assurance sociale, sin, social insurance numberが含まれます。

コメント: なし

社会保障番号 (SSN)

マネージドデータ識別子 ID: 国や地域によっては、SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

サポートされている国と地域:スペイン、米国

キーワードが必須: はい。スペインの場合、キーワードにはnúmero de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#が含まれます。米国の場合、キーワードにはsocial security, ss#, ssnが含まれます。

コメント: なし

納税者識別番号または参照番号

サポートには、スペインの CIF、NIE、NIF 番号、ブラジルの CNPJ および CPF 番号、イタリアの Codice Fiscale 番号、米国の ITIN、インドの PAN、ドイツの SteueridentifikationsNummer 番号、オーストラリアの TFN 番号、フランスの TIN、英国の TRN および UTR 番号が含まれます。

マネージドデータ識別子 ID: 国や地域によっては、AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

サポートされている国と地域: オーストラリア、ブラジル、フランス、ドイツ、インド、イタリア、スペイン、英国、米国

キーワードが必須: はい。次のテーブルに、Macie が特定の国およびリージョンについて認識するキーワードのリストを示します。

国またはリージョン	キーワード
オーストラリア	tax file number, tfn
ブラジル	cadastro de pessoa física, cadastro de pessoa fisica, cadastro de pessoas físicas, cadastro de pessoas fisicas, cadastro nacional da pessoa jurídica, cadastro nacional da pessoa juridica, cnpj, cpf
フランス	numéro d'identification fiscal, tax id, tax identification number, tax number, tin, tin#
ドイツ	identifikationsnummer, steuer id, steueridentifikationsnummer, steuernummer, tax id, tax identification number, tax number
インド	e-pan, pan card, pan number, permanent account number

国またはリージョン	キーワード
イタリア	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
スペイン	cif, cif número, cifnúmero#, nie, nif, número de contribuyente, número de identidad de extranjero, número de identificación fiscal, número de impuesto corporativo, personal tax number, tax id, tax identification number, tax number, tin, tin#
英国	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
米国	i.t.i.n.、個別の納税者識別番号、itin

コメント: なし

車両識別番号 (VIN)

マネージドデータ識別子 ID: VEHICLE_IDENTIFICATION_NUMBER

サポートされている国と地域: すべて (VIN が英語、フランス語、ドイツ語、リトアニア語、ポーランド語、ポルトガル語、ルーマニア語、またはスペイン語のいずれかの言語でキーワードの近くにある場合)。

キーワードが必須: はい。キーワードには: Fahrgestellnummer, niv, numarul de identificare, numarul seriei de sasiu, numer VIN, Número de Identificação do Veículo, Número de Identificación de Automóviles, numéro d'identification du véhicule, vehicle identification number, vin, VIN numerisが含まれます。

コメント: Macieは、17文字のシーケンスで設定され、ISO 3779および3780規格に準拠したVINを検出することができます。これらの規格は、世界中で使用するために設計されています。

Amazon Macie でのカスタムデータ識別子の構築

カスタムデータ識別子は、機密データを検出するために定義する基準のセットです。基準は、一致するテキストパターン、オプションで文字シーケンス、結果を絞り込む近接ルールを定義する正規表現 (正規表現) から設定されています。

カスタムデータ識別子を使用すると、従業員 ID、顧客アカウント番号、内部データの分類など、組織の特定のシナリオ、知的財産、または独自のデータを反映する検出基準を定義できます。機密データ検出ジョブまたは機密データ自動検出をこれらの識別子を使用するように設定すると、Amazon Macie が提供しているマネージドデータ識別子を補足する方法で S3 オブジェクトを分析できます。

検出基準に加えて、カスタムデータ識別子が生成する機密データ結果のカスタム重要度設定を定義できます。デフォルトでは、Macie はカスタムデータ識別子が生成するすべての結果に中重要度を自動的に割り当てます。カスタムデータ識別子の検出基準に一致するテキストの出現回数に基づいて重要度が変化することはありません。カスタム重要度設定を定義することにより、基準に一致するテキストの出現回数に基づいて、割り当てる重要度を指定できます。

トピック

- カスタムデータ識別子の検出基準の定義
- カスタムデータ識別子の結果の重要度設定の定義
- カスタムデータ識別子の作成
- カスタムデータ識別子での正規表現のサポート

カスタムデータ識別子の検出基準の定義

各カスタムデータ識別子を作成するときに、S3 オブジェクト内で一致するテキストパターンを定義する正規表現 (正規表現) を指定します。Macie は、Perl 互換正規表現 (PCRE) ライブラリによって提供される正規表現パターン構文のサブセットをサポートしています。詳細については、このセクションで後述する正規表現のサポートを参照してください。

また、単語やフレーズなどの文字シーケンス、および結果を絞り込む近接ルールを指定することもできます。

キーワード

> これらは、正規表現パターンに一致するテキストの近接内にある必要がある文字シーケンスです。近接要件は、S3 オブジェクトのストレージ形式またはファイルタイプによって異なります。

- 構造化列データでは、テキストが正規表現パターンに一致し、キーワードがテキストを保存するフィールドまたは列の名前に含まれている場合、またはテキストの前にキーワードがあり、かつテキストが同じフィールドまたはセル値内のキーワードの最大一致距離内にある場合に、Macie は結果をレポートします。これは、Microsoft Excel ワークブック、CSV ファイル、および TSV ファイルに当てはまります。
- 構造化レコードベースデータでは、テキストが正規表現パターンに一致し、テキストがキーワードの最大一致距離内にある場合、Macie は結果を含めます。キーワードは、テキストを保存するフィールドまたは配列へのパス内の要素の名前に含めるか、またはテキストを保存するフィールドまたは配列内の同じ値の前にくるかその一部にすることができます。これは Apache Avro オブジェクトコンテナ、Apache Parquet ファイル、JSON ファイル、および JSON Lines ファイルに当てはまります。
- 非構造化データでは、テキストが正規表現パターンに一致し、テキストの前にキーワードがあり、かつテキストがキーワードの最大一致距離内にある場合、Macie は結果をレポートします。これは、Adobe ポータブルドキュメント形式ファイル、Microsoft Word ドキュメント、E メールメッセージ、および CSV、JSON、JSON Lines、および TSV ファイル以外の非バイナリテキストファイルに当てはまります。これには、これらのタイプのファイルに含まれるテーブルなどの構造化データが含まれます。

最大 50 個のキーワードを指定できます。各キーワードには、3～90 の UTF-8 文字を含めることができます。キーワードでは、大文字と小文字が区別されません。

Maximum match distance (最大一致距離)

これは文字ベースのキーワードの近接ルールです。Macie はこの設定を使用して、キーワードが正規表現パターンに一致するテキストの前に置かれているかどうかを判断します。この設定は、キーワード全体の終わりと正規表現パターンに一致するテキストの終わりの間に存在できる最大文字数を定義します。テキストが正規表現パターンに一致し、少なくとも 1 つのキーワードが完了した後に出現し、キーワードから指定された距離内にある場合、Macie はそのテキストを結果に含めます。それ以外の場合、Macie はそのテキストを結果から除外します。

1～300 文字の距離を指定できます。デフォルトの距離は 50 文字です。最良の結果を得るには、この距離が正規表現が検出するように設計されているテキストの最小文字数よりも大きくなければなりません。テキストの一部だけがキーワードの最大一致距離内にある場合、Macie はそのテキストを結果に含めません。

無視する単語

これらは、結果から除外する文字シーケンスです。テキストが正規表現パターンと一致しても、無視する単語が含まれている場合、Macie はそのテキストを結果に含めません。

無視する単語を 10 個まで指定できます。無視する単語には、4～90 の UTF-8 文字を含めることができます。無視する単語では、大文字と小文字が区別されます。

たとえば、多くの企業は、従業員 ID の特定の構文を持っています。そのような構文の 1 つは、従業員がフルタイム (F) またはパートタイム (P) の従業員であるかを示す大文字で、その後にハイフン (-)、その後に従業員を識別する 8 桁のシーケンスが続きます。例としては、正社員の場合は F-12345678、パートタイムの従業員の場合は P-87654321です。

この構文を使用する従業員 ID を検出するためのカスタムデータ識別子を作成する場合は、次の正規表現を使用できます: `[A-Z]-\d{8}`。分析を絞り込み、誤検出を回避するために、カスタムデータ識別子を設定して、キーワード従業員と 従業員 ID の最大一致距離を 20 文字にすることもできます。これらの基準では、テキストが従業員 ID または従業員 ID というキーワードの後にあり、すべてのテキストがいずれかのキーワードから 20 文字以内の場合にのみ、正規表現に一致するテキストが結果に含まれます。

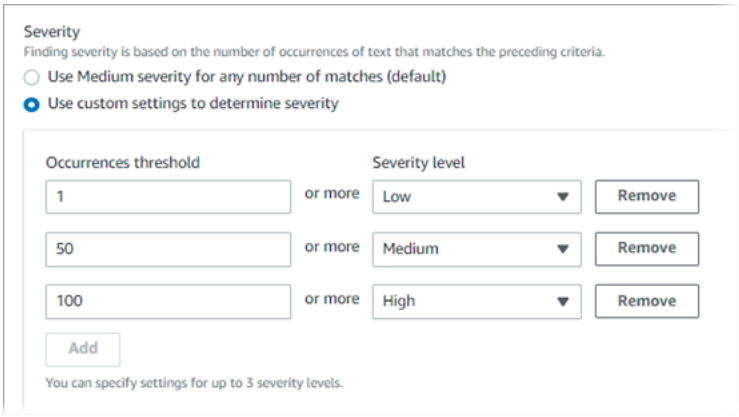
キーワードが機密データの検索や誤検出の回避にどのように役立つかについては、次の動画をご覧ください。Amazon Macie がキーワードを使用して機密データを検出する方法。

カスタムデータ識別子の結果の重要度設定の定義

カスタムデータ識別子を作成するときに、識別子が生成する機密データの結果のカスタム重要度設定を定義することもできます。デフォルトでは、Macie はカスタムデータ識別子が生成するすべての結果に中重要度を割り当てます。S3 オブジェクトに、カスタムデータ識別子の検出基準に一致するテキストが少なくとも 1 つ含まれている場合、Macie は結果を作成し、結果に中重要度を自動的に割り当てます。

カスタム重要度設定を使用すると、カスタムデータ識別子の検出基準に一致するテキストの出現回数に基づいて、割り当てる重要度を指定できます。これを行うには、以下の最大 3 つの重要度レベルで 頻度しきい値を定義します: 低 (最小重要度)、中および 高 (最大重要度)。頻度しきい値は、指定された重要度で結果を生成するために S3 オブジェクトに存在する必要がある一致の最小数です。しきい値を超える値を指定する場合、しきい値は重要度で昇順 (低 から 高 に移動) である必要があります。

たとえば、次の図は 3 つの頻度しきい値を指定するカスタムデータ識別子の重要度設定 (Macie がサポートする重要度レベルごとに 1 つ) を示しています。



次のテーブルに、カスタムデータ識別子が生成する結果の重要度を示します。

頻度しきい値	重要度レベル	結果
1	低	S3 オブジェクトに、検出基準に一致するテキストの出現が 1～49 回含まれている場合、Macie はオブジェクトで低重要度の結果を作成します。
50	中	S3 オブジェクトに、検出基準に一致するテキストの出現が 50～99 回含まれている場合、Macie はオブジェクトで中重要度の結果を作成します。
100	高	S3 オブジェクトに、検出基準に一致するテキストの出現が 100 回以上含まれている場合、Macie はオブジェクトで高重要度の結果を作成します。

重要度設定を使用して、結果を作成するかどうかを指定することもできます。S3 オブジェクトに含まれる出現の回数が最小頻度しきい値よりも少ない場合、Macie は結果を作成しません。

カスタムデータ識別子の作成

Amazon Macie コンソールを使用してカスタムデータ識別子を作成するには、次のステップに従います。カスタムデータ識別子をプログラムで作成するには、Amazon Macie APIの CreateCustomDataIdentifier オペレーションを使用します。

カスタムデータ識別子を作成するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインの 設定 の下で、カスタムデータ識別子 を選択します。
3. 作成 を選択します。
4. 名前 では、カスタムデータ識別子の名前を入力します。名前には最大 128 文字を含めることができます。

   名前に機密データを含めないようにしてください。Macie で実行できるアクションによっては、アカウントの他のユーザーが名前を確認できる場合があります。
5. 説明 では、カスタムデータ識別子の簡単な説明を入力します。説明には最大 512 文字を含めることができます。

   説明に機密データを含めないようにしてください。Amazon Macie で実行できるアクションによっては、アカウントの他のユーザーが説明を確認できる場合があります。
6. 正規表現 では、一致するテキストパターンを定義する正規表現 (正規表現) を入力します。正規表現には最大 512 文字を含めることができます。サポートされている構文と制約の詳細については、このセクションで後ほど説明される正規表現のサポートを参照してください。
7. (オプショナル) キーワード では、一致する特定のテキストを定義する 50 文字のシーケンス (カンマ区切り) を入力します。各キーワードには、3～90 の UTF-8 文字を含めることができます。キーワードでは、大文字と小文字が区別されません。

   Macie は、前のトピック で説明されているとおり、テキストが正規表現パターンに一致し、これらのキーワードの 1 つの最大一致距離内にある場合に出現を含めます。
8. (オプショナル) 無視する単語 では、結果から除外する特定のテキストを定義する最大 10 文字シーケンス (カンマ区切り) を入力します。無視する単語には、4～90 の UTF-8 文字を含めることができます。無視する単語では、大文字と小文字が区別されます。

   Macie は、テキストが正規表現パターンと一致しても、これらの無視する単語のいずれかが含まれている出現を結果から除外します。

9. 最大一致距離は、正規表現に一致するテキストとキーワードの間に存在できる文字の最大数です。距離は 1〜300 文字です。デフォルトの距離は 50 文字です。

   Macie は、前のトピック で説明されているとおり、テキストが正規表現パターンに一致し、キーワードのこの距離内にある場合にのみ出現を含めます。

10. 重要度 の下で、Macie が、カスタムデータ識別子が生成する機密データの調査結果に重要度を割り当てる方法を選択します。

    - 中重要度をすべての結果に自動的に割り当てるには、任意の数の一致に対して中重要度を使用する (デフォルト) を選択します。このオプションでは、影響を受ける S3 オブジェクトに検出基準と一致するテキストが 1 つ以上含まれている場合、Macie は検出結果に自動的に重大度中を割り当てます。
    - 指定したカスタム頻度しきい値に基づいて重要度を割り当てるには、カスタム設定を使用して重要度を判断する を選択します。次に、頻度しきい値 および 重要度レベル オプションを使用して、選択した重要度で結果を生成するために S3 オブジェクトに存在する必要がある一致の最小数を指定します。

      たとえば、 高 重要度を、識別子の検出基準に一致するテキストの 100 回以上の出現をレポートしている結果に割り当てるには、**`100`** を 頻度しきい値 ボックスに入力し、重要度 リストから 高 を選択します。

      Macie がサポートする重大度レベルごとに 1 つずつ、最大 3 つの頻度しきい値を指定できます: Low (低) (最小の重要度の場合)、中 または 高 (最大の重要度の場合)。1 を超える値を指定する場合、しきい値は重要度で昇順 (低 から 高 に移動) である必要があります。S3 オブジェクトに含まれる出現の回数が最小指定しきい値よりも少ない場合、Macie は結果を作成しません。

11. (オプショナル) タグ で タグを追加 を選択し、カスタムデータ識別子に割り当てるタグを 50 個まで入力します。

    タグは、ユーザーが定義して特定のタイプの AWS リソースに割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを特定、分類および管理できます。詳細については、Amazon Macie リソースへのタグ付けを参照してください。

12. (オプショナル) 評価 では、サンプルデータ ボックスに最大 1,000 文字を入力し、テスト を選択して検出条件をテストします。Macie はサンプルデータを評価し、基準に一致するテキストの出現回数をレポートします。基準を調整して最適化するために、このステップを何回でも繰り返すことができます。

> **Note**
>
> カスタムデータ識別子を保存する前に、検出基準をテストして調整することを強くお勧めします。カスタムデータ識別子は、機密データ検出ジョブで使用されるため、カスタムデータ識別子は保存後に編集することはできません。これにより、実施するデータプライバシーと保護の監査または調査に関する機密データの調査結果と検出結果のイミュータブルな履歴を確実に保持できます。

13. 完了したら、送信 を選択します。

Macie は設定をテストし、正規表現をコンパイルできることを確認します。設定や正規表現のいずれかに問題があると、エラーが発生し、問題の性質が示されます。問題を解決したら、カスタムデータ識別子を保存できます。

カスタムデータ識別子での正規表現のサポート

Macie は、Perl 互換正規表現 (PCRE) ライブラリによって提供される正規表現パターン構文のサブセットをサポートしています。PCRE ライブラリによって提供される設定のうち、Macie は次のパターン要素をサポートしていません。

- バックリファレンス
- キャプチャグループ
- 条件付きパターン
- 埋め込みコード
- グローバルパターンフラグ (`/i`、`/m`、および `/x` など)
- 再帰的なパターン
- 正と負のルックビハインドおよびルックアヘッドのゼロ幅アサーション (?=、?!、?<=、および ?<! など)。

カスタムデータ識別子の効果的な正規表現パターンを作成するには、以下のヒントとレコメンデーションにも注意してください。

- アンカー — 行の先頭または末尾ではなく、ファイルの先頭または末尾にパターンが表示されることを想定している場合にのみ、アンカー (^ または $) を使用します。

- 有界リピート — パフォーマンス上の理由から、Macie は有界リピートグループのサイズを制限します。たとえば、`\d{100,1000}` は Macie ではコンパイルしません。この機能に近づくには、`\d{100,}` のようなオープンエンドリピートを使用できます。
- 大文字と小文字を区別しない — パターンの一部で大文字と小文字を区別しないようにするには、`/i` フラグの代わりに `(?i)` 設定を使用します。
- パフォーマンス — プレフィックスや交代を手動で最適化する必要はありません。たとえば、`/hello|hi|hey/` から `/h(?:ello|i|ey)/` に変更してもパフォーマンスは向上しません。
- ワイルドカード — パフォーマンス上の理由から、Macie はワイルドカードの繰り返し数を制限します。たとえば、`a*b*a*` は Macie ではコンパイルしません。

不正な形式または長時間実行される式から保護するために、Macie はサンプルテキストのコレクションに対して正規表現パターンを自動的にテストします。

Amazon Macie の許可リストでの機密データの例外の定義

Amazon Macie の許可リストでは、Macie が Amazon Simple Storage Service (Amazon S3) オブジェクトの機密データを検査するときに無視する特定のテキストとテキストパターンを定義できます。これらは通常、特定のシナリオや環境における機密データの例外です。データが許可リストのテキストまたはテキストパターンと一致する場合、データがマネージドデータ識別子またはカスタムデータ識別子の基準に一致していても、Macie はデータを報告しません。許可リストを使用することで、Amazon S3 データの分析を改善し、ノイズを減らすことができます。

Macie では、次の 2 タイプの許可リストを作成して使用できます。

- 定義済みテキスト— このタイプのリストでは、無視する特定の文字シーケンスを指定します。たとえば、組織の公的担当者の名前、特定の電話番号、組織がテストに使用する特定のサンプルデータなどです。このタイプのリストを使用する場合、Macie はリスト内のエントリに完全に一致するテキストを無視します。

  このタイプのリストには、通常、機密性が低く、変更される可能性が低く、必ずしも共通のパターンに従っているとは限らない特定の単語、フレーズ、その他の種類の文字列が含まれています。
- 正規表現 — このタイプのリストでは、無視するテキストパターンを定義する正規表現 (正規表現) を指定します。例としては、組織の公開電話番号、組織のドメインのメールアドレス、組織がテストに使用するパターン化されたサンプルデータなどがあります。このタイプのリストを使用する場合、Amazon Macie はリストで定義されたパターンに完全に一致するテキストを無視します。

このタイプの許可リストは、共通のパターンに準拠させつつ、機密性はないが変更する、または変更される可能性が高いテキストを指定したい場合に役立ちます。

許可リストを作成したら、それを使用するために機密データ検出ジョブを作成して設定したり、機密データ自動検出設定にそれを追加したりできます。その後、Macie はそのリストを使用してデータを分析します。Macie が許可リストのエントリまたはパターンに一致するテキストを見つけても、機密データの検出結果、統計、その他のタイプの結果にそのテキストの出現は報告しません。

アジアパシフィック (大阪) リージョンを除く、Macie が現在利用可能なすべての AWS リージョンで許可リストを作成して使用できます。

トピック

- Amazon Macie での許可リストのオプションと要件
- Amazon Macie での許可リストの作成と管理

Amazon Macie での許可リストのオプションと要件

Amazon Macie では、Amazon Simple Storage Service (Amazon S3) オブジェクトに機密データがあるか検査するときに無視すべきテキストまたはテキストパターンを、許可リストを使用して指定できます。Macie には、定義済みのテキストと正規表現の 2 タイプの許可リストのオプションが用意されています。

定義済みテキストのリストは、機密性があると見なさない特定の単語、フレーズ、その他のタイプの文字列を無視させたい場合に役立ちます。例としては、組織の公的担当者の名前、特定の電話番号、組織がテストに使用する特定のサンプルデータなどがあります。Macie がマネージドデータ識別子またはカスタムデータ識別子の基準に一致するテキストを検出し、そのテキストが許可リストのエントリにも一致する場合、Macie は機密データの検出結果、統計、およびその他のタイプの結果におけるテキストの出現を報告しません。

正規表現 (正規表現) は、共通のパターンに準拠させつつ、変更する、または変更される可能性が高いテキストを Macie に無視するようにしたい場合に役立ちます。regex は、無視するテキストパターンを指定します。例としては、組織の公開電話番号、組織のドメインのメールアドレス、組織がテストに使用するパターン化されたサンプルデータなどがあります。Macie がマネージドデータ識別子またはカスタムデータ識別子の基準に一致するテキストを見つけ、そのテキストが許可リストの正規表現パターンにも一致する場合、Macie は機密データの検出結果、統計、およびその他のタイプの結果におけるテキストの出現を報告しません。

アジアパシフィック (大阪) リージョンを除く AWS リージョン Macie が現在利用可能なすべてので、両方のタイプの許可リストを作成して使用できます。許可リストを作成および管理する際には、次のオプションと要件を念頭に置いてください。また、郵送先住所の許可リストエントリと regex パターンはサポートされていないことにも注意してください。

トピック

定義済みテキストのリストのオプションと要件

このタイプの許可リストでは、無視する特定の文字シーケンスを列挙した行区切りのプレーンテキストファイルを用意します。このタイプのリストには、通常、機密性が低く、変更される可能性が低く、必ずしも共通のパターンに従っているとは限らない特定の単語、フレーズ、その他の種類の文字列が含まれています。このタイプのリストを使用する場合、Amazon Macie はリスト内のエントリと完全に一致するテキストの出現を報告しません。Macie は、各リストエントリを文字列リテラル値として扱います。

このタイプの許可リストを使用するには、まずテキストエディターでリストを作成し、プレーンテキストファイルとして保存します。次に、リストを S3 汎用バケットにアップロードします。また、バケットとオブジェクトのストレージと暗号化の設定で、Macie がリストを取得および復号化できることを確認します。次に、Macie でリストを作成して設定を行います。

Macie で設定を設定したら、アカウントまたは組織の代表的な小さなデータセットを使用して許可リストをテストすることをお勧めします。リストをテストするには、1 回限りのジョブを作成して、データ分析に通常使用するマネージドデータ識別子とカスタムデータ識別子に加えてそのリストを使用するようにジョブを設定できます。その後、ジョブの結果 (機密データの検出結果、機密データの検出結果、あるいはその両方) を確認できます。ジョブの結果が予想と異なる場合は、期待どおりの結果になるまでリストを変更してテストできます。

許可リストの設定とテストが完了したら、そのリストを使用する追加のジョブを作成・設定したり、アカウントの機密データ自動検出設定に追加したりできます。これらのジョブの実行が開始されるか、次の自動検出分析サイクルが開始されると、Macie は Amazon S3 から最新バージョンのリストを取得し、一時メモリに保存します。その後、Macie は S3 オブジェクトに機密データがないか検査するときに、リストの一時的なコピーを使用します。ジョブの実行が終了するか、分析サイクルが完了すると、Macie はリストのコピーをメモリから完全に削除します。このリストは Macie では保持されません。Macie ではリストの設定のみが保持されます。

> **Important**
>
> Macie では定義済みのテキストのリストは保持されないため、許可リストのステータスを定期的に確認することが重要です。ジョブまたは自動検出で使用するように設定したリストを Macie が取得または解析できない場合、Macie はそのリストを使用しません。これにより、リストに指定したテキストの機密データが見つかるなど、予期しない検出結果が生じる可能性があります。

トピック

- 構文要件
- ストレージの要件
- 暗号化/復号化の要件
- 設計上の考慮事項と推奨事項

構文要件

このタイプの許可リストを作成するときは、リストのファイルに関する次の要件に注意してください。

- リストは、.txt、.text、.plain ファイルなどのプレーンテキスト `text/plain` ファイルとして保存する必要があります。
- リストでは、個々のエントリを改行して区切る必要があります。例:

```
Akua Mansa
John Doe
Martha Rivera
425-555-0100
425-555-0101
```

```
425-555-0102
```

Macie は各行をリスト内の 1 つの個別のエントリとして扱います。ファイルには読みやすくするために空白行を含めることもできます。Macie はファイルを解析する際に空白行をスキップします。

- 各エントリには、1～90 の UTF-8 文字を含めることができます。
- テキストの完全一致が無視されるようにするためには、各エントリが完全である必要があります。Macie はエントリのワイルドカード文字または部分的な値の使用をサポートしていません。Macie は、各エントリを文字列リテラル値として扱います。一致では大文字と小文字は区別されません。
- このファイルには 1 ～ 100,000 個のエントリを含めることができます。
- 添付されたファイルの合計サイズが 35 MB を超えることはできません。

ストレージの要件

Amazon S3 で許可リストを追加および管理するときは、以下のストレージ要件と推奨事項に注意してください。

- リージョンサポート – 許可リストは、Macie アカウント AWS リージョン と同じ にあるバケットに保存する必要があります。Macie は、許可リストが別のリージョンに保存されている場合、その許可リストにアクセスできません。
- バケットの所有権 – 許可リストは、 が所有するバケットに保存する必要があります AWS アカウント。他のアカウントに同じ許可リストを使用させたい場合は、Amazon S3 レプリケーションルールを作成して、それらのアカウントが所有するバケットにリストを複製することを検討してください。S3オブジェクトのレプリケーションについては、Amazon Simple Storage Service ユーザーガイドのオブジェクトのレプリケートを参照してください。

  さらに、 AWS Identity and Access Management (IAM) ID には、リストを保存するバケットとオブジェクトへの読み取りアクセス権が必要です。そうしないと、Macie を使用してリストの設定を作成または更新したり、リストのステータスを確認したりできなくなります。
- ストレージタイプとクラス – 許可リストは、ディレクトリバケットではなく汎用バケットに保存する必要があります。さらに、低冗長化 (RRS)、S3 Glacier Instant Retrieval、S3 Intelligent-Tiering、S3S3 One Zone-IA、S3 Standard、または S3 Standard-IA のいずれかのストレージクラスを使用して保存する必要があります。
- バケットポリシー - 制限付きのバケットポリシーを持つバケットに許可リストを保存する場合は、ポリシーで Macie がリストを取得できることを確認してください。これを行うには、Macie

のサービスにリンクされたロールの条件をバケットポリシーに追加できます。詳細については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。

また、ポリシーが、IAM アイデンティティがバケットへの読み取りアクセス権を持つことを許可していることを確認してください。そうしないと、Macie を使用してリストの設定を作成または更新したり、リストのステータスを確認したりできなくなります。

- オブジェクトパス — Amazon S3 に複数の許可リストを保存する場合、各リストのオブジェクトパスは一意である必要があります。つまり、各許可リストはそれぞれ独自の S3 オブジェクトとして個別に保存する必要があります。
- バージョニング – バケットに許可リストを追加するときは、バケットのバージョニングも有効にすることをお勧めします。その後、日付と時刻の値を使用して、リストのバージョンと、そのリストを使用する機密データ検出ジョブの結果や機密データ自動検出サイクルの結果を関連付けることができます。これは、実施するデータプライバシーと保護の監査または調査に役立ちます。
- オブジェクトロック — 許可リストが一定期間または無期限に削除または上書きされないようにするには、リストを保存するバケットのオブジェクトロックを有効にします。この設定を有効にしても Macie がリストにアクセスできなくなるわけではありません。詳細については、Amazon Simple Storage Service ユーザーガイドのS3 オブジェクトロックの使用を参照してください。

暗号化/復号化の要件

Amazon S3 で許可リストを暗号化する場合、通常、Macie のサービスにリンクされたロールのアクセス許可ポリシーは、リストの復号化に必要なアクセス許可をMacie に付与します。ただし、これは使用された暗号化のタイプによって異なります。

- リストが Amazon S3 マネージドキー (SSE-S3) によるサーバー側の暗号化を使用して暗号化されている場合、Macie はリストを復号できます。Macie アカウントのサービスにリンクされたロールは、Macie に必要なアクセス許可を付与します。
- AWS マネージド AWS KMS key (DSSE-KMS または SSE-KMS) によるサーバー側の暗号化を使用してリストが暗号化されている場合、Macie はリストを復号できます。Macie アカウントのサービスにリンクされたロールは、Macie に必要なアクセス許可を付与します。
- リストがカスタマー管理 AWS KMS key (DSSE-KMS または SSE-KMS) によるサーバー側の暗号化を使用して暗号化されている場合、Macie は Macie にキーの使用を許可した場合にのみリストを復号できます。これを行う方法については、Macie にカスタマーマネージド の使用を許可する AWS KMS keyを参照してください。

> **Note**
>
> リストは、外部キーストアでカスタマー管理 AWS KMS key で暗号化できます。ただし、そのキーは、完全に AWS KMS内で管理されるキーよりも遅く、信頼性が低くなる可能性があります。レイテンシーや可用性の問題により Macie がリストを復号化できない場合、Macie は S3 オブジェクトの分析にリストを使用しません。これにより、リストに指定したテキストの機密データが見つかるなど、予期しない検出結果が生じる可能性があります。このリスクを軽減するには、そのキーを S3 バケットキーとして使用するように設定された S3 バケットにリストを保存することを検討してください。
>
> 外部キーストアで KMS キーを使用する方法については、AWS Key Management Service デベロッパーガイドの外部キーストアを参照してください。S3 バケットキー使用の詳細については、Amazon Simple Storage Service ユーザーガイドの、Amazon S3 バケットキーを使用した SSE-KMS のコストの削減を参照してください。

- 顧客提供キーを使用したサーバー側の暗号化 (SSE-C)、またはクライアント側の暗号化を使用してリストが暗号化されている場合、Macie はリストを復号化できません。代わりに、SSE-S3、DSSE-KMS、または SSE-KMS 暗号化の使用を検討してください。

リストが AWS マネージド KMS キーまたはカスタマーマネージド KMS キーで暗号化されている場合、 AWS Identity and Access Management (IAM) ID にもキーの使用を許可する必要があります。そうしないと、Macie を使用してリストの設定を作成または更新したり、リストのステータスを確認したりできなくなります。KMS キーのアクセス許可を確認または変更する方法については、AWS Key Management Service デベロッパーガイドのキーポリシー AWS KMSを参照してください。

Amazon S3 データの暗号化オプションの詳細については、「Amazon Simple Storage Service ユーザーガイド」の「暗号化によるデータの保護」を参照してください。

設計上の考慮事項と推奨事項

一般的に、Macieは許可リストの各エントリーを文字列リテラル値として扱います。つまり、Macieは許可リストのエントリ全体と完全に一致するテキストの出現をすべて無視します。一致では大文字と小文字は区別されません。

ただし、Macie はそれらのエントリをより大規模なデータ抽出および分析フレームワークの一部として使用します。このフレームワークには、文法や構文のバリエーション、そして多くの場合はキーワードの近接性などの次元を考慮に入れる機械学習とパターンマッチング機能が含まれています。このフレームワークは、S3 オブジェクトのファイルタイプまたはストレージ形式も考慮します。その

ため、許可リストにエントリを追加して管理する際には、次の考慮事項と推奨事項に留意してください。

さまざまなファイルタイプや保存形式に備える

Adobe Portable Document Format (.pdf) ファイル内のテキストなどの非構造化データでは、Macie は許可リストのエントリ全体と完全に一致するテキスト (複数行またはページにまたがるテキストを含む) を無視します。

CSV ファイルの列データや JSON ファイルのレコードベースのデータなどの構造化データでは、すべてのテキストが 1 つのフィールド、セル、または配列に格納されている場合、Macie は許可リストのエントリ全体と完全に一致するテキストを無視します。この要件は、.pdf ファイル内のテーブルなど、非構造であるファイルに格納されている構造化データには適用されません。

例えば、CSV ファイル内の次の内容を考えてください。

```
Name,Account ID
Akua Mansa,111111111111
John Doe,222222222222
```

`Akua Mansa` と `John Doe` が許可リストに登録されている場合、Macie は CSV ファイル内のそれらの名前を無視します。各リストエントリの全テキストは 1 つの `Name` フィールドに保存されます。

逆に、以下の列とフィールドを含む CSV ファイルを考えてみましょう。

```
First Name,Last Name,Account ID
Akua,Mansa,111111111111
John,Doe,222222222222
```

`Akua Mansa` と `John Doe` が許可リストに登録されている場合、Macie は CSV ファイル内のそれらの名前を無視しません。CSV ファイルのどのフィールドにも、許可リストのエントリの全テキストは含まれていません。

一般的なバリエーションを含める

数値データ、固有名詞、用語、および英数字の文字列の一般的なバリエーションのエントリを追加します。たとえば、単語間にスペースが 1 つしかない名前やフレーズを追加する場合は、単語の間にスペースを 2 つ含むバリエーションも追加します。同様に、特殊文字を含む単語と含まない単語やフレーズを追加し、一般的な構文や意味のバリエーションを含めることを検討してください。

たとえば、米国の電話番号425-555-0100の場合は、次のエントリを許可リストに追加するとよいでしょう。

```
425-555-0100
425.555.0100
(425) 555-0100
+1-425-555-0100
```

多国籍の文脈における日付2022 年 2 月 1 日には、特殊文字を含むバリエーションと含まないバリエーションを含む、英語とフランス語の一般的な構文バリエーションを含むエントリを追加します。

```
February 1, 2022
1 février 2022
1 fevrier 2022
Feb 01, 2022
1 fév 2022
1 fev 2022
02/01/2022
01/02/2022
```

人物の名前には、機密ではないと思われるさまざまな形式の名前のエントリを含めてください。たとえば、名前の後に姓、姓の後に名前、名前と姓を 1 スペースで区切る、名前と姓を 2 つのスペースで区切る、ニックネームなどを含めます。

たとえばMartha Riveraという名前には、次のように追加します。

```
Martha Rivera
Martha  Rivera
Rivera, Martha
Rivera,  Martha
Rivera Martha
Rivera  Martha
```

多くの部分を含む特定の名前のバリエーションを無視したい場合は、代わりに正規表現を使用する許可リストを作成します。たとえば、Dr. Martha Lyda Rivera, PhDという名前には、次の正規表現を使用します。`^(Dr. )?Martha\s(Lyda|L\.)?\s?Rivera,?( PhD)?$`

許可リスト内の正規表現のオプションと要件

このタイプの許可リストでは、無視するテキストパターンを定義する正規表現 (正規表現) を指定します。たとえば、組織の公開電話番号、組織のドメインのメールアドレス、組織がテストに使用するパターン化されたサンプルデータなどです。regex は、機密と見なされない特定のタイプのデータに共通のパターンを定義します。このタイプの許可リストを使用する場合、Amazon Macie は指定されたパターンに完全に一致するテキストの出現を報告しません。無視する定義済みのテキストを指定する許可リストとは異なり、正規表現と他のすべてのリスト設定を Macie に作成して保存します。

このタイプの許可リストを作成または更新すると、リストを保存する前にサンプルデータを使用してリストの regex をテストできます。これは、複数のサンプルデータセットで行うことをお勧めします。あまりにも一般的な regex を作成すると、Macie は機密と見なされるテキストの出現を無視する可能性があります。regex が具体的すぎると、Macie は機密と見なされないテキストの出現を無視しない可能性があります。不正な形式または長時間実行される表現から保護するために、Macie はサンプルテキストのコレクションに対して正規表現 regex を自動的にコンパイルしてテストし、対処すべき問題を通知します。

さらにテストを行うには、アカウントまたは組織の代表的な小さなデータセットを使用してリストの regex をテストすることもお勧めします。そのためには、1 回限りのジョブを作成して、データ分析に通常使用するマネージドデータ識別子とカスタムデータ識別子に加えて、リストを使用するようにジョブを設定できます。その後、ジョブの結果 (機密データの検出結果、機密データの検出結果、あるいはその両方) を確認できます。ジョブの結果が予想と異なる場合は、期待どおりの結果になるまで regex を変更してテストできます。

許可リストを設定してテストしたら、それを使用する追加のジョブを作成して設定したり、アカウントの機密データ自動検出設定に追加したりできます。これらのジョブが実行されるか、Macie がアカウントの自動検出を実行すると、Macie はリストの regex の最新バージョンを使用してデータを分析します。

トピック

- 構文サポートと推奨事項
- 例

構文サポートと推奨事項

許可リストでは、512 文字までの正規表現 (正規表現) を指定できます。Macie は、Perl 互換正規表現 (PCRE) ライブラリによって提供される正規表現パターン構文のサブセットをサポートしていま

す。PCRE ライブラリによって提供される設定のうち、Macie は次のパターン要素をサポートしていません。

- バックリファレンス
- キャプチャグループ
- 条件付きパターン
- 埋め込みコード
- グローバルパターンフラグ (/i、/m、および /x など)
- 再帰的なパターン
- 正と負のルックビハインドおよびルックアヘッドのゼロ幅アサーション (?=、?!、?<=、および ?<! など)。

許可リストの効果的な regex パターンを作成するには、次のヒントと推奨事項にも注意してください。

- アンカー — 行の先頭または末尾ではなく、ファイルの先頭または末尾にパターンが表示されることを想定している場合にのみ、アンカー (^ または $) を使用します。
- 有界リピート — パフォーマンス上の理由から、Macie は有界リピートグループのサイズを制限します。たとえば、\d{100,1000} は Macie ではコンパイルしません。この機能に近づくには、\d{100,} のようなオープンエンドリピートを使用できます。
- 大文字と小文字を区別しない — パターンの一部で大文字と小文字を区別しないようにするには、/i フラグの代わりに (?i) 設定を使用します。
- パフォーマンス — プレフィックスや交代を手動で最適化する必要はありません。たとえば、/hello|hi|hey/ から /h(?:ello|i|ey)/ に変更してもパフォーマンスは向上しません。
- ワイルドカード — パフォーマンス上の理由から、Macie はワイルドカードの繰り返し数を制限します。たとえば、a*b*a* は Macie ではコンパイルしません。
- 代替 — 1 つの許可リストに複数のパターンを指定するには、代替演算子 | を使用してパターンを連結できます。これを行うと、Macie は OR ロジックを使用してパターンを結合し、新しいパターンを形成します。たとえば、(apple|orange)を指定すると、Macie は appleとorangeの両方を一致するものとして認識し、両方の単語の出現を無視します。パターンを連結する場合は、連結する式全体の長さを必ず 512 文字以下に制限してください。

最後に、regex を開発するときは、さまざまなファイルタイプとストレージ形式に対応するように設計してください。Macie は regex をより大規模なデータ抽出および分析フレームワークの一部と

して使用しています。フレームワークは、S3 オブジェクトのファイルタイプまたはストレージ形式を考慮します。CSV ファイルの列指向データや JSON ファイルのレコードベースのデータなどの構造化データでは、すべてのテキストが 1 つのフィールド、セル、または配列に格納されている場合のみ、Macie はパターンに完全に一致するテキストを無視します。この要件は、Adobe Portable Document Format (.pdf) ファイル内のテーブルなど、非構造であるファイルに格納されている構造化データには適用されません。.pdf ファイル内のテキストなどの非構造化データでは、Macie はパターンに完全に一致するテキスト (複数行またはページにまたがるテキストを含む) を無視します。

例

以下の例は、いくつかの一般的なシナリオで有効な regex パターンを示しています。

E メールアドレス

カスタムデータ識別子を使用してE メールアドレスを検出する場合、組織の電子メールアドレスなど、機密と見なされない電子メールアドレスは無視できます。

特定のセカンドレベルドメインとトップレベルドメインのメールアドレスを無視するには、次のパターンを使用できます。

```
[a-zA-Z0-9_.+\\-]+@example\.com
```

ここで、*example* は第 2 レベルドメインの名前で、*com* は最上位ドメインです。この場合、Macie は johndoe@example.com や john.doe@example.com などのアドレスを一致させ無視します。

.com や .gov などの汎用トップレベルドメイン (gTLD) の特定のドメインのメールアドレスを無視するには、次のパターンを使用できます。

```
[a-zA-Z0-9_.+\\-]+@example\.[a-zA-Z]{2,}
```

ここで、*example* はドメインの名前です。この場合、Macie は johndoe@example.com や john.doe@example.com などのアドレスを一致させ無視します。

カナダの .ca、オーストラリアの .au など、単一国コード最上位ドメイン (ccTLD) 内の特定のドメインのメールアドレスを無視するには、次のパターンを使用できます。

```
[a-zA-Z0-9_.+\\-]+@example\.(ca|au)
```

ここで、*example* はドメインの名前で、*ca* および *au* は無視すべき特定のccTLDs です。この場合、Macie は johndoe@example.com や john.doe@example.com などのアドレスを一致させ無視します。

特定のドメインと gTLD 用で、第 3 レベルと第 4 レベルのドメインを含むメールアドレスを無視するには、次のパターンを使用できます。

```
[a-zA-Z0-9_.+\\-]+@([a-zA-Z0-9-]+\.)?[a-zA-Z0-9-]+\.example\.com
```

ここで、*example* はドメインの名前で、*com* はgTLD です。この場合、Macie は johndoe@example.com や john.doe@example.com などのアドレスを一致させ無視します。

電話番号

Macie は、複数の国や地域の電話番号を検出できるマネージドデータ識別子を提供しています。組織のフリーダイヤル番号や公開電話番号など、特定の電話番号を無視するには、次のようなパターンを使用できます。

800 の市外局番を使用し、(800) ###-#### という形式のフリーダイヤルの米国の電話番号を無視するには:

```
^\(?800\)?[ -]?\d{3}[ -]?\d{4}$
```

888 の市外局番を使用し、(888) ###-#### という形式のフリーダイヤルの米国の電話番号を無視するには:

```
^\(?888\)?[ -]?\d{3}[ -]?\d{4}$
```

33 の国コードを含み、+33 ## ## ## ## ##という形式の 10 桁のフランスの電話番号を無視するには:

```
^\+33 \d( \d\d){4}$
```

特定の市外局番と交換コードを使用し、国コードが含まれず、(###) ###-####という形式の米国およびカナダの電話番号を無視するには:

```
^\(?123\)?[ -]?555[ -]?\d{4}$
```

123 はエリアコード、*555* は交換コードです。

特定の市外局番と交換コードを使用し、国コードが含まれ、+1 (###) ##-##### という形式の米国およびカナダの電話番号を無視するには:

```
^\+1\(?123\)?[ -]?555[ -]?\d{4}$
```

123 はエリアコード、*555* は交換コードです。

Amazon Macie での許可リストの作成と管理

Amazon Macie では、許可リストによって、Macie が機密データの Amazon Simple Storage Service (Amazon S3) オブジェクトを検査する際に無視する特定のテキストまたはテキストパターンを定義します。データが許可リストのテキストまたはテキストパターンと一致する場合、データがカスタムデータ識別子またはマネージドデータ識別子 の基準に一致していても、Macie は機密データ結果または機密データ検出結果のデータを報告しません。

Macie では次のタイプの許可リストを作成および管理できます。

定義済みのテキスト

このタイプのリストには、通常、機密性が低く、変更される可能性が低く、必ずしも共通のパターンに従っているとは限らない特定の単語、フレーズ、その他の種類の文字列が含まれています。例としては、組織の公的担当者の名前、特定の電話番号、組織がテストに使用する特定のサンプルデータなどがあります。このタイプのリストを使用する場合、Macie はリスト内のエントリに完全に一致するテキストを無視します。

このタイプのリストでは、無視する特定のテキストを列挙した行区切りのプレーンテキストファイルを作成します。次に、S3 バケットにファイルを保存し、バケット内のリストにアクセスするための Macie の設定を設定します。その後、そのリストを使用するように機密データ検出ジョブを作成して設定したり、アカウントの機密データ自動検出設定にリストを追加したりできます。各ジョブの実行が開始されるか、次の自動検出分析サイクルが開始されると、Macie は Amazon S3 から最新バージョンのリストを取得します。その後、Macie はそのバージョンのリストを使用して S3 オブジェクトに機密データがないか検査します。Macie がリスト内のエントリに完全に一致するテキストを見つけた場合、Macie はテキストの出現を機密データとして報告しません。

正規表現

無視するテキスト・パターンを定義する正規表現 (正規表現)を指定するには、このタイプのリストを使う。例としては、組織の公開電話番号、組織のドメインのメールアドレス、組織がテストに使用するパターン化されたサンプルデータなどがあります。このタイプのリストを使用する場合、Macie はリストで定義された正規表現パターンに完全に一致するテキストを無視します。

このタイプのリストでは、機密性はないが変更する、または変更される可能性が高いテキストの共通のパターンを定義する正規表現を作成します。定義済みテキストのリストとは異なり、正規表現と他のすべてのリスト設定を作成して Macie に保存します。その後、そのリストを使用するように機密データ検出ジョブを作成して設定したり、アカウントの機密データ自動検出設定にリストを追加したりできます。これらのジョブが実行されるか、Macie がアカウントの自動検出を

実行すると、Macie はリストの regex の最新バージョンを使用してデータを分析します。Macie がリストで定義されたパターンに完全に一致するテキストを見つけた場合、Macie はテキストの出現を機密データとして報告しません。

詳細な要件、推奨事項、および各タイプのリストの例については、許可リストのオプションと要件を参照してください。サポートされている各 で、アカウントに最大 10 個の許可リストを作成できます。事前定義されたテキストを指定する許可リストは AWS リージョン最大 5 つ、正規表現を指定する許可リストは最大 5 つまで作成できます。アジアパシフィック (大阪) リージョンを除く AWS リージョン Macie が現在利用可能なすべての で許可リストを作成して使用できます。

許可リストを作成および管理するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。次のトピックでは、その方法を説明します。API について、トピックでは、AWS Command Line InterfaceAWS CLI を用いてこれらのタスクを実行する方法を説明します。これらのタスクは、別の AWS コマンドラインツールまたは AWS SDK の最新バージョンを使用するか、HTTPS リクエストを Macie に直接送信することで実行することもできます。 AWS ツールと SDKsで構築するツール AWS」を参照してください。

トピック

- 許可リストの作成
- 許可リストのステータスをチェックする
- 許可リストの変更
- 許可リストを削除する

許可リストの作成

Amazon Macie で許可リストを作成する方法は、作成するリストのタイプによって異なります。許可リストは、無視する定義済みのテキストをリストしたファイルでも、無視するテキストパターンを定義する正規表現 (正規表現) でもかまいません。作成するリストのタイプに対応するセクションを選択します。

定義済みのテキスト

Macie でこのタイプの許可リストを作成する前に、次の手順を実行します。

1. テキストエディタを使用して、無視する特定のテキスト (.txt、.text、.plain ファイルなど) をリストした行区切りのプレーンテキストファイルを作成します。詳細については、「定義済みテキストのリストの構文要件」を参照してください。

2. ファイルを S3 汎用バケットにアップロードし、バケットの名前とオブジェクトを書き留めます。Macie で設定を設定するときに、これらの名前を入力する必要があります。
3. S3 バケットとオブジェクトの設定で、あなたと Macie がバケットからリストを取得できることを確認してください。詳細については、定義済みテキストのリストのストレージ要件を参照してください。
4. S3 オブジェクトを暗号化した場合、ユーザーと Macie が使用を許可されているキーを用いて暗号化されていることも確認してください。詳細については、定義済みテキストのリストの暗号化/復号化要件を参照してください。

これらの手順を実行すると、Macie でリストの設定を行う準備が整います。Amazon Macie コンソールまたは Amazon Macie API を使用して、設定を定義できます。

Console

Amazon Macie コンソールを使用して許可リストの設定を定義するには、次のステップに従います。

Macie で許可リスト設定を設定するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定 の リスト を選択します。
3. 許可リストページで、作成を選択します。
4. リストのタイプの選択 で 定義済みテキスト を選択します。
5. リスト設定 で、以下のオプションを使用して許可リストの追加設定を入力します。

   - リスト名 で、リストの名前を入力します。名前には最大 128 文字を含めることができます。
   - 説明に、任意に 簡単な説明を入力します。説明には最大 512 文字を含めることができます。
   - S3 バケット名 には、リストを保存するバケットの名前を入力します。

     Amazon S3 では、この値はバケットのプロパティの 名前 フィールドにあります。この値では、大文字と小文字が区別されます。また、ワイルドカード文字を使用したり、名前に部分的な値を指定したりしないでください。
   - S3 オブジェクト名 には、リストを保存する S3 オブジェクトの名前を入力します。

Amazon S3 では、この値はオブジェクトのプロパティの キーフィールドにあります。名前にパスが含まれる場合は、名前を入力するときにたとえば **allowlists/macie/mylist.txt** のように、完全なパスを含めます。この値では、大文字と小文字が区別されます。また、ワイルドカード文字を使用したり、名前に部分的な値を指定したりしないでください。

6. (オプション) タグ で タグを追加 を選択し、許可リストに割り当てるタグを 50 個まで入力します。

   タグは、特定のタイプの AWS リソースを定義して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを分類および管理できます。詳細については、Amazon Macie リソースへのタグ付けを参照してください。

7. 完了したら、作成 を選択します。

Macie はリストの設定をテストします。Macie は、Amazon S3 からリストを取得し、リストのコンテンツを解析できることも確認します。エラーが発生した場合、Macie はエラーを説明するメッセージを表示します。エラーのトラブルシューティングに役立つ詳細情報は定義済みテキストのリストのオプションと要件を参照してください。エラーを解決したら、リストの設定を保存できます。

API

許可リスト設定をプログラムで設定するには、Amazon Macie API の CreateAllowListオペレーションを使用して、必要なパラメータに適切な値を指定します。

`criteria` パラメータには、`s3WordsList` オブジェクトを使用して S3 バケットの名前 `bucketName` と、リストを保存する S3 オブジェクト `objectKey` の名前を指定します。バケット名を確認するには、Amazon S3 の `Name` フィールドを参照してください。オブジェクト名を確認するには、Amazon S3 の `Key` フィールドを参照してください。値 では、大文字と小文字が区別されることに注意してください。また、これらの名前を指定するとき、ワイルドカード文字や部分的な値を使用しないでください。

を使用して設定を構成するには AWS CLI、 create-allow-list コマンドを実行し、必要なパラメータに適切な値を指定します。以下の例は、*`DOC-EXAMPLE-BUCKET`* という名前の S3 バケットに保存されている許可リストの設定方法を示しています。リストを保存する S3 オブジェクトの名前は *`allowlists/macie/mylist.txt`* です。

この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws macie2 create-allow-list \
--criteria '{"s3WordsList":{"bucketName":"DOC-EXAMPLE-
BUCKET","objectKey":"allowlists/macie/mylist.txt"}}' \
--name my_allow_list \
--description "Lists public phone numbers and names for Example Corp."
```

この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行継続文字を使用しています。

```
C:\> aws macie2 create-allow-list ^
--criteria={\"s3WordsList\":{\"bucketName\":\"DOC-EXAMPLE-BUCKET\",\"objectKey\":
\"allowlists/macie/mylist.txt\"}} ^
--name my_allow_list ^
--description "Lists public phone numbers and names for Example Corp."
```

リクエストを送信すると、Macie はリストの設定をテストします。Macie は、Amazon S3 からリストを取得し、リストのコンテンツを解析できることも確認します。エラーが発生した場合、リクエストは失敗し、Macie はエラーを説明するメッセージを返します。エラーのトラブルシューティングに役立つ詳細情報は定義済みテキストのリストのオプションと要件を参照してください。

Macie がリストを取得して解析できた場合、リクエストは成功し、以下に類似した出力が表示されます。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
nkr81bmtu2542yyexample",
    "id": "nkr81bmtu2542yyexample"
}
```

ここで、`arn` は、作成された許可リストの Amazon リソースネーム (ARN)で、`id` は、リストの一意の識別子です。

リストの設定を保存したら、そのリストを使用するために機密データ検出ジョブを作成して設定したり、機密データ自動検出設定にリストを追加したりできます。これらのジョブの実行が開始される

か、自動検出分析サイクルが開始されるたびに、Macie は Amazon S3 から最新バージョンのリストを取得します。その後、Macie はそのバージョンのリストを使用してデータを分析します。

正規表現

正規表現 (正規表現) を指定する許可リストを作成する場合、その正規表現とその他のリスト設定はすべて Macie で直接定義します。Macie は、Perl 互換正規表現 (PCRE) ライブラリによって提供される正規表現パターン構文のサブセットをサポートしています。詳細については、構文サポートと推奨事項を参照してください。

Amazon Macie コンソールまたは Amazon Macie API を使用して、このタイプのリストを作成できます。

Console

Amazon Macie コンソールを使用して許可リストを作成するには、次のステップに従います。

許可リストを作成するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定 の リスト を選択します。
3. 許可リスト ページで、作成を選択します。
4. リストのタイプの選択 で 正規表現 を選択します。
5. リスト設定 で、以下のオプションを使用して許可リストの追加設定を入力します。
   - リスト名 で、リストの名前を入力します。名前には最大 128 文字を含めることができます。
   - 説明に、任意に 簡単な説明を入力します。説明には最大 512 文字を含めることができます。
   - 正規表現には、無視するテキスト· パターンを定義する正規表現を入力する。正規表現には512文字まで含めることができる。
6. (オプション) 評価 では、サンプルデータ ボックスに 1,000 文字まで入力し、テスト を選択して regex をテストします。Macie はサンプルデータを評価し、正規表現に一致するテキストの出現回数をレポートします。正規表現を調整して最適化するために、このステップを何回でも繰り返すことができます。

> **Note**
>
> regex は、複数のサンプルデータセットでテストして調整することをお勧めします。あまりにも一般的な regex を作成すると、Macie は機密と見なされるテキストの出現を無視する可能性があります。regex が具体的すぎると、Macie は機密と見なされないテキストの出現を無視しない可能性があります。

7. (オプション) タグ で タグを追加 を選択し、許可リストに割り当てるタグを 50 個まで入力します。

   タグは、特定のタイプの AWS リソースを定義して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを分類および管理できます。詳細については、Amazon Macie リソースへのタグ付けを参照してください。
8. 完了したら、作成 を選択します。

Macie はリストの設定をテストします。Macie は regex をテストして表現をコンパイルできるかどうかも確認します。エラーが発生した場合は、エラーを説明するメッセージ。エラーのトラブルシューティングに役立つ詳細情報は許可リスト内の正規表現のオプションと要件を参照してください。エラーに対処したら、許可リストを保存できます。

API

Macie でこのタイプの許可リストを作成する前に、複数のサンプルデータを使用して正規表現をテストし、調整することをお勧めします。あまりにも一般的な regex を作成すると、Macie は機密と見なされるテキストの出現を無視する可能性があります。regex が具体的すぎると、Macie は機密と見なされないテキストの出現を無視しない可能性があります。

Macie で式をテストするには、Amazon Macie API の TestCustomDataIdentifierオペレーションを使用するか、 で test-custom-data-identifier コマンド AWS CLIを実行します。Macie は同じ基本コードを使用して、許可リストとカスタムデータ識別子の表現をコンパイルします。この方法で式をテストする場合は、必ず `regex` と `sampleText` パラメータの値のみを指定してください。これを実行しない場合は、不正確な結果が表示されます。

このタイプの許可リストを作成する準備ができたら、Amazon Macie API の CreateAllowListオペレーションを使用して、必要なパラメータに適切な値を指定します。`criteria`パラメータでは、`regex` フィールドを使用して、無視するテキストパターンを定義する正規表現を指定します。式には最大 512 文字を含めることができます。

を使用してこのタイプのリストを作成するには AWS CLI、 create-allow-list コマンドを実行し、必要なパラメータに適切な値を指定します。次の例では、*my_allow_list* という名前の許可リストを作成します。regex は、カスタムデータ識別子が検出した可能性がある example.com ドメインのすべての電子メールアドレスを無視するように設計されています。

この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws macie2 create-allow-list \
--criteria '{"regex":"[a-z]@example.com"}' \
--name my_allow_list \
--description "Ignores all email addresses for Example Corp."
```

この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行継続文字を使用しています。

```
C:\> aws macie2 create-allow-list ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--name my_allow_list ^
--description "Ignores all email addresses for Example Corp."
```

リクエストを送信すると、Macie はリストの設定をテストします。Macie は regex をテストして表現をコンパイルできるかどうかも確認します。エラーが発生した場合、リクエストは失敗し、Macie はエラーを説明するメッセージを返します。エラーのトラブルシューティングに役立つ詳細情報は許可リスト内の正規表現のオプションと要件を参照してください。

Macie が表現をコンパイルできた場合、リクエストは成功し、次のような出力が表示されます。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

ここで、arn は、作成されたフィルタールールの Amazon リソースネーム (ARN)で、id は、ルールの一意の識別子です。

リストを保存したら、それを使用するために機密データ検出ジョブを作成して設定したり、機密データ自動検出設定にそれを追加したりできます。これらのジョブが実行されるか、Macie がアカウント

の自動検出を実行すると、Macie はリストの regex の最新バージョンを使用してデータを分析します。

許可リストのステータスをチェックする

許可リストのステータスを定期的に確認することが重要です。そうしないと、エラーが原因で Amazon Macie が予期しない分析結果 (許可リストで指定したテキストの機密データ検出結果など) を生成する可能性があります。

機密データ検出ジョブを許可リストを使用するように設定し、ジョブの実行開始時に Macie がそのリストにアクセスできない、または使用できない場合、ジョブは引き続き実行されます。ただし、Macie は S3 オブジェクトを分析するときにはリストを使用しません。同様に、機密データを自動検出する分析サイクルが開始され、Macie が指定された許可リストにアクセスできない、または使用できない場合、分析は続行されますが、Macie はそのリストを使用しません。

正規表現 (正規表現) を指定する許可リストでは、エラーが発生する可能性はほとんどありません。これは、リストの設定を作成または更新すると、Macie が自動的に regex をテストすることが一因です。さらに、regex と他のすべてのリスト設定を Macie に保存します。

ただし、Macie ではなく Amazon S3 にリストを保存すると、定義済みのテキストを指定する許可リストでエラーが発生する可能性があります。一般的なエラーの原因は次のとおりです。

- S3 バケットまたはオブジェクトが削除されている。
- S3 バケットまたはオブジェクトの名前が変更されたが、Macie のリストの設定には新しい名前が指定されていない。
- S3 バケットのアクセス許可設定が変更され、Macie はバケットとオブジェクトにアクセスできない。
- S3 バケットの暗号化設定が変更され、Macie はリストを保存するオブジェクトを復号化できない。
- 暗号化キーのポリシーが変更され、Macie はキーにアクセスできない。Macie はリストを保存する S3 オブジェクトを復号化できない。

> **Important**
>
> これらのエラーは分析結果に影響するため、許可リストのステータスを定期的に確認することをお勧めします。許可リストを保存する S3 バケットの許可または暗号化設定を変更す

る場合、またはリストの暗号化に使用される AWS Key Management Service（ AWS KMS) キーのポリシーを変更する場合にも、これを行うことをお勧めします。

Amazon Macie コンソールまたは Amazon Macie API を使用して、許可リストのステータスを確認できます。発生したエラーのトラブルシューティングに役立つ詳細情報は[定義済みテキストのリストのオプションと要件]を参照してください。

Console

Amazon Macie コンソールを使用して許可リストのステータスを確認するには、次のステップに従います。

許可リストのステータスを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定 の リスト を選択します。
3. 許可リスト ページで 更新 を選択します。Macie はすべての許可リストの設定をテストし、ステータス フィールドを更新して各リストの現在のステータスを示します。

   リストに正規表現が指定されている場合、そのステータスは通常 OK です。つまり、Macie は式をコンパイルできます。リストに定義済みのテキストが指定されている場合、そのステータスは次の値のいずれかになります。

   OK

   Macie はリストのコンテンツを取得して解析できます。

   アクセスが拒否されました

   Macie はリストが保存されている S3 オブジェクトにアクセスすることが許可されていません。Amazon S3 はオブジェクトを取得するリクエストを拒否しました。オブジェクトが Macie AWS KMS key が使用を許可されていないカスタマー管理の で暗号化されている場合、リストにこのステータスになることもあります。

   このエラーに対処するには、バケットとオブジェクトのバケットポリシーとその他のアクセス許可設定を確認します。Macie がオブジェクトへのアクセスと取得を許可されている

ことを確認してください。オブジェクトがカスタマーマネージド AWS KMS キーで暗号化されている場合、キーポリシーも確認して Macie がキーの使用が許可されていることを確認してください。

エラー

Macie がリストの内容を取得または解析しようとしたときに、一時的なエラーまたは内部エラーが発生しました。許可リストが Amazon S3 と Macie がアクセスまたは使用できない暗号化キーで暗号化されている場合も、このステータスになる可能性があります。

このエラーを解決するには、数分間待ってから更新  を再試行してください。ステータスが エラー のままの場合は、S3 オブジェクトの暗号化設定を確認してください。オブジェクトが Amazon S3 と Macie がアクセスして使用できるキーで暗号化されていることを確認してください。

オブジェクトは空です

Macie は Amazon S3 からリストを取得できますが、リストにはコンテンツが含まれていません。

このエラーに対処するには、Amazon S3 からオブジェクトをダウンロードし、正しいエントリが含まれていることを確認します。エントリが正しければ、Macie のリストの設定を確認してください。指定したバケット名とオブジェクト名が正しいことを確認してください。

オブジェクトが見つかりません。

リストは Amazon S3 に存在しません。

このエラーを解決するには、Macie のリストの設定を確認してください。指定したバケット名とオブジェクト名が正しいことを確認してください。

リソースクォータ

Macie は Amazon S3 のリストにアクセスできます。ただし、リストのエントリ数またはリストのストレージサイズが、許可リストのクォータを超えています。

このエラーに対処するには、リストを複数のファイルに分割してください。各ファイルに含まれるエントリが 100,000 件未満であることを確認してください。また、各ファイルのサイズが 35 MB 未満であることを確認してください。次に、各ファイルを Amazon S3 にアップロードします。完了したら、Macie でファイルごとに許可リスト設定を設定しま

す。サポートされている各 AWS リージョンで最大 5 つの定義済みテキストのリストを含めることができます。

スロットル済み

Amazon S3 はリストを取得するリクエストを抑制しました。

このエラーを解決するには、数分間待ってから更新
を再試行してください。

ユーザーアクセスが拒否されました

Amazon S3 はオブジェクトを取得するリクエストを拒否しました。指定されたオブジェクトが存在する場合、そのオブジェクトへのアクセスは許可されていないか、使用が許可されていない AWS KMS キーで暗号化されています。

このエラーに対処するには、 AWS 管理者と協力して、リストの設定で正しいバケット名とオブジェクト名が指定され、バケットとオブジェクトへの読み取りアクセス権があることを確認します。オブジェクトが暗号化されている場合、使用を許可されているキーを用いて暗号化されていることも確認してください。

4. 特定のリストの設定とステータスを確認するには、リストの名前を選択します。

API

プログラムで許可リストのステータスを確認するには、Amazon Macie API の GetAllowListオペレーションを使用するか、 の場合は get-allow-list コマンド AWS CLIを実行します。

`id` パラメータでは、ステータスを確認する許可リストの一意の識別子を指定します。この識別子を取得するには、 ListAllowListsオペレーションを使用できます。ListAllowLists のオペレーションでは、アカウントのすべての許可リストに関する情報を取得します。を使用している場合は AWS CLI、 list-allow-lists コマンドを実行してこの情報を取得できます。

GetAllowList リクエストを送信すると、Macie は許可リストのすべての設定をテストします。設定で正規表現(正規表現)が指定されている場合、Macie は表現をコンパイルできることを確認します。設定で定義済みテキストのリストが指定されている場合、Macie はリストを取得して解析できることを確認します。

次に Macie は許可リストの詳細を提供する `GetAllowListResponse` オブジェクトを返します。`GetAllowListResponse` オブジェクトで、`status` のオブジェクトは、リストの現在のス

テータス、つまりステータスコード code と、ステータスコードによってはリストのステータスの簡単な説明 description を示します。

許可リストに regex が指定されている場合、ステータスコードは通常OKで、関連する説明はありません。これは Macie が表現を正常にコンパイルしたことを意味します。

許可リストに定義済みのテキストが指定されている場合、ステータスコードはテスト結果によって異なります。

- Macie がリストの取得と解析に成功した場合、ステータスコードは OK で、関連する説明はありません。
- エラーが原因で Macie がリストを取得または解析できなかった場合は、ステータスコードと説明は発生したエラーの性質を示します。

可能なステータスコードのリストとそれぞれの説明については、Amazon Macie API リファレンスのAllowListStatus「」を参照してください。

許可リストの変更

許可リストを作成したら、Amazon Macie のリスト設定のほとんどを変更できます。たとえば、リストの名前と説明を変更したり、リストのタグを追加したり編集したりできます。変更できない設定はリストのタイプだけです。たとえば、既存の許可リストで正規表現が指定されている場合、そのタイプを事前定義済みのテキストに変更することはできません。

許可リストに定義済みのテキストが指定されている場合は、リスト内のエントリを変更することもできます。これを行うには、エントリを含むファイルを更新し、新しいバージョンのファイルを Amazon S3 にアップロードします。Macie が次にリストを使用する準備をするときに、Macie は Amazon S3 からファイルの最新バージョンを取得します。新しいファイルをアップロードするときは、必ず同じ S3 バケットとオブジェクトに保存してください。または、バケットまたはオブジェクトの名前を変更した場合は、必ず Macie のリストの設定を更新してください。

Amazon Macie コンソールまたは Amazon Macie API を使用して、許可リストの設定を変更できます。

Console

Amazon Macie コンソールを使用して許可リストの設定を変更するには、次のステップに従います。

許可リストを変更するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定 の リスト を選択します。
3. 許可リスト ページで、変更する許可リストの名前を選択します。許可リストページが開き、リストの現在の設定が表示されます。
4. 許可リストのタグを割り当てまたは編集するには、タグ セクションで、タグの管理 を選択します。次に、必要に応じてタグを変更します。終了したら、保存 を選択します。
5. 許可リストの他の設定を変更するには、リスト設定セクションで 編集を選択します。次に、必要に応じて設定を変更してください。

   - 名前 — リストの新しい名前を入力します。名前には最大 128 文字を含めることができます。
   - 説明 — リストの新しい説明を入力します。説明には最大 512 文字を含めることができます。
   - 許可リストに定義済みのテキストが指定されている場合:
     - S3 バケット名 – 現在リストを保存しているバケットの名前を入力します。

       Amazon S3 では、この値はバケットのプロパティの 名前 フィールドにあります。この値では、大文字と小文字が区別されます。また、ワイルドカード文字を使用したり、名前に部分的な値を指定したりしないでください。
     - S3 オブジェクト名 – 現在リストを保存している S3 オブジェクトの名前を入力します。

       Amazon S3 では、この値はオブジェクトのプロパティの キーフィールドにあります。名前にパスが含まれる場合は、名前を入力するときにたとえば **`allowlists/macie/mylist.txt`** のように、完全なパスを含めます。この値では、大文字と小文字が区別されます。また、ワイルドカード文字を使用したり、名前に部分的な値を指定したりしないでください。
   - 許可リストに正規表現(正規表現)が指定されている場合は、正規表現 ボックスに新しい正規表現を入力します。正規表現には最大 512 文字を含めることができます。

     新しい regex を入力したら、必要に応じてテストします。これを行うには、最大 1,000 文字のテキストを サンプルデータ ボックスに入力し、次に 送信 を選択します。Macie はサンプルデータを評価し、検出基準に一致するテキストの出現回数をレポートします。正規表現を調整して最適化してから変更を保存するために、このステップを何回でも繰り返すことができます。

設定の入力が完了したら、保存を選択します。

Macie はリストの設定をテストします。定義済みのテキストのリストについては、Macie は Amazon S3 からリストを取得してリストの内容を解析できるかどうかも確認します。regex の場合、Macie は表現をコンパイルできるかどうかも確認します。エラーが発生した場合は、エラーを説明するメッセージ。エラーのトラブルシューティングに役立つ詳細情報は許可リストのオプションと要件を参照してください。エラーを解決したら、変更を保存できます。

API

プログラムで許可リストを変更するには、Amazon Macie API の UpdateAllowListオペレーションを使用するか、 の場合は update-allow-list コマンド AWS CLIを実行します。リクエストでは、サポートされているパラメータを使用して、変更する設定ごとに新しい値を指定します。`criteria`、`id`、および `name` パラメータが必要なことに注意してください。必須パラメータの値を変更したくない場合は、パラメータの現在の値を指定します。

たとえば、次のコマンドでは、既存の許可リストの名前と説明を変更します。この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

```
C:\> aws macie2 update-allow-list ^
--id km2d4y22hp6rv05example ^
--name my_allow_list-email ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--description "Ignores all email addresses for the example.com domain"
```

コードの説明は以下のとおりです。

- *km2d4y22hp6rv05example* はリストの一意の識別子です。
- *my_allow_list-email* はリストの新しい名前です。
- *a-z@example .com* はリストの基準、正規表現です。
- リストの新しい説明である *example.com ####################*。

リクエストを送信すると、Macie はリストの設定をテストします。リストに定義済みのテキストが指定されている場合、これには Macie が Amazon S3 からリストを取得し、リストのコンテンツを解析できるかどうかの検証も含まれます。リストに regex が指定されている場合は、Macie が表現をコンパイルできるかどうかの検証も含まれます。

Macie が設定をテストしたときにエラーが発生した場合、リクエストは失敗し、Macie はエラーを説明するメッセージを返します。エラーのトラブルシューティングに役立つ詳細情報は許可リストのオプションと要件を参照してください。別の理由でリクエストが失敗した場合、Macie は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

リクエストが成功すると、Macie はリストの設定を更新し、次のような出力を受け取ります。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

ここで、arn は、更新された許可リストの Amazon リソースネーム (ARN)で、id は、リストの一意の識別子です

許可リストを削除する

Amazon Macie で許可リストを削除すると、リストのすべての設定が完全に削除されます。これらの設定は、削除後は復元できません。設定で Amazon S3 に保存する定義済みテキストのリストが指定されている場合、Macie はそのリストを保存する S3 オブジェクトを削除しません。Macie の設定のみが削除されます。

機密データ検出ジョブを許可リストを使用するように設定し、後でそのリストを削除すると、ジョブはスケジュールどおりに実行されます。ただし、機密データ検出結果と機密データ検出結果の両方で、以前に許可リストに指定したテキストがジョブの結果から報告されることがあります。同様に、リストを使用するように自動機密データ検出を設定し、その後そのリストを削除すると、毎日の分析サイクルが続行されます。ただし、機密データの検出結果、統計、またはその他のタイプの結果では、以前に許可リストに指定したテキストが報告される場合があります。

許可リストを削除する前に、ジョブインベントリを確認して、そのリストを使用するジョブで、将来に実行が予定されているジョブを特定することをお勧めします。インベントリの詳細パネルには、ジョブが許可リストを使用するように設定されているかどうか、設定されている場合はどの許可リストを使用するかが示されます。さらに、機密データの自動検出設定も確認してください。リストを削除するよりも変更する方が良いと判断するかもしれません。

追加の安全対策として、許可リストを削除しようとすると、Macie はすべてのジョブの設定をチェックします。リストを使用するようにジョブを設定していて、それらのジョブのいずれかのステータス

が 完了 または キャンセル以外の場合、ユーザーが追加の確認を行わない限り、Macie はリストを削除しません。

Amazon Macie コンソールまたは Amazon Macie API を使用して、許可リストを削除できます。

Console

Amazon Macie コンソールを使用して許可リストを削除するには、次のステップに従います。

許可リストを削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定の リストを選択します。
3. 許可リストページで、削除する許可リストのチェックボックスをオンにします。
4. Actions メニューで、Delete を選択します。
5. 確認を求められたら、**delete**と入力してから、Delete (削除) を選択します。

API

プログラムで許可リストを削除するには、Amazon Macie API の DeleteAllowListオペレーションを使用します。`id` パラメータでは、削除する許可リストの一意の識別子を指定します。この識別子は、 ListAllowListsオペレーションを使用して取得できます。ListAllowLists のオペレーションでは、アカウントのすべての許可リストに関する情報を取得します。を使用している場合は AWS CLI、 list-allow-lists コマンドを実行してこの情報を取得できます。

機密データ検出ジョブがリストを使用するように設定されている場合でも、`ignoreJobChecks` パラメータにはリストを強制的に削除するかどうかを指定します。

- `false` を指定した場合、Macie は `COMPLETE` または `CANCELLED` 以外のステータスのすべてのジョブの設定をチェックします。どのジョブもリストを使用するように設定されていない場合、Macie はそのリストを完全に削除します。これらのジョブのいずれかがリストを使用するように設定されている場合、Macie はリクエストを拒否し、HTTP 400 `ValidationException` エラーを返します。エラーメッセージには、最大 200 件のジョブに適用可能なジョブの数が表示されます。
- `true` を指定した場合、Macie はジョブの設定を確認せずにリストを完全に削除します。

を使用して許可リストを削除するには AWS CLI、 delete-allow-list コマンドを実行します。例:

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks
 false
```

ここで、*nkr81bmtu2542yyexample* は削除する許可リストの一意の識別子です。

リクエストが成功すると、Macie は空の HTTP 200 レスポンスを返します。それ以外の場合、Macie は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

許可リストに定義済みのテキストが指定されている場合は、リストを格納する S3 オブジェクトをオプションで削除できます。ただし、このオブジェクトを保持すると、データプライバシーと保護の監査または調査に関する機密データの調査結果と検出結果のイミュータブルな履歴を確実に保持できます。

Amazon Macie で機密データ自動検出を実行する

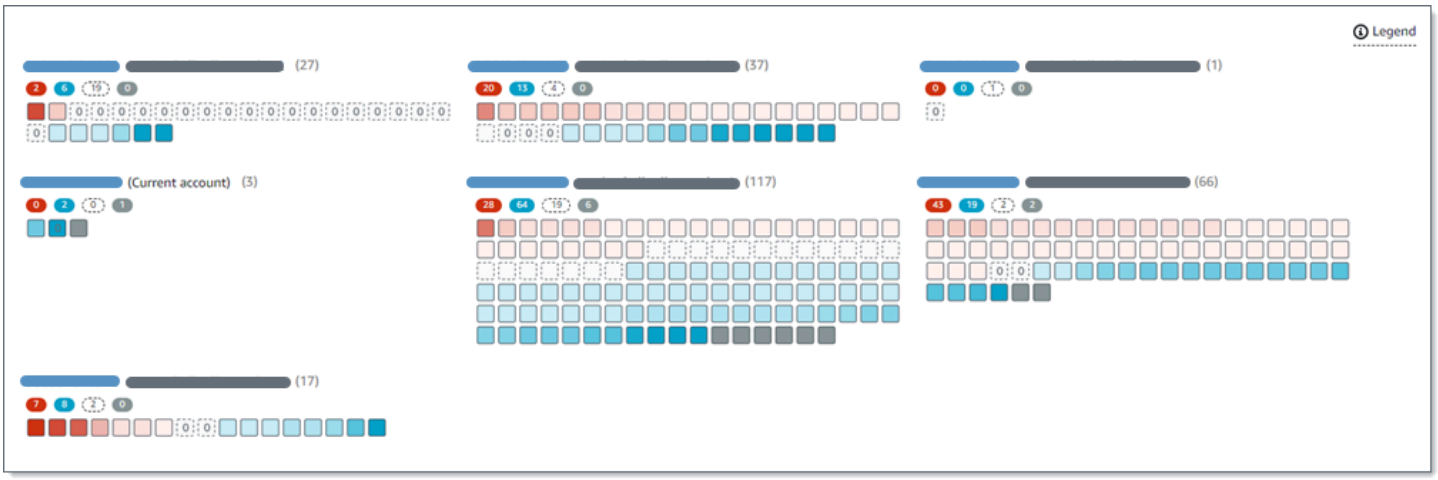
Amazon Simple Storage Service (Amazon S3) のデータ資産内の機密データがどこにあるかを広く把握するには、アカウントまたは組織の機密データを自動検出するように Amazon Macie を設定します。機密データ自動検出により、Macie は S3 バケットインベントリを継続的に評価し、サンプリング技術を使用してバケット内の代表的な S3 オブジェクトを識別して選択します。その後、Macie は選択したオブジェクトを取得して分析し、機密データがないか検査します。

デフォルトでは、Macie はすべての S3 汎用バケットからオブジェクトを選択して分析します。ユーザーが組織の Macie 管理者である場合、これにはメンバーアカウントが所有するバケット内のオブジェクトが含まれます。通常は AWS ログデータを保存するバケットなど、特定のバケットを除外して分析の範囲を調整できます。Macie 管理者の場合は、組織内の個々のアカウント case-by-case に対して機密データの自動検出を有効または無効にするオプションが追加されています。

特定の種類の機密データに焦点を当てるように分析を調整できます。デフォルトでは、Macie は機密データ自動検出に推奨するマネージドデータ識別子のセットを使用して S3 オブジェクトを分析します。分析を調整するには、Macie が提供する特定のマネージドデータ識別子、定義したカスタムデータ識別子、または 2 つの組み合わせを使用するように Macie を設定します。指定した許可リストを使用するように Macie を設定して、分析を絞り込むこともできます。

分析が毎日進行するにつれて、Macie は検出した機密データと実行した分析のレコードを生成します。機密データの検出結果は、Macie が個々の S3 オブジェクトで検出した機密データを報告し、機密データの検出結果は、個々の S3 オブジェクトの分析に関する詳細を口グに記録します。Macie は、Amazon S3 データに関して提供する統計、インベントリデータ、およびその他の情報も更新し

ます。例えば、コンソールのインタラクティブなヒートマップでは、データ資産全体のデータ機密性が視覚的に表示されます。



これらの機能は、Amazon S3 データ資産全体のデータ機密性を評価し、ドリルダウンして個々のアカウント、バケット、オブジェクトを調査して評価するのに役立つように設計されています。また、機密データ検出ジョブを実行することで、より詳細で即時に分析を行うべき箇所を判断するのにも役立ちます。Macie が提供する Amazon S3 データのセキュリティとプライバシーに関する情報と組み合わせることで、これらの機能を使用して、即時の修正が必要なケース (Macie が機密データを検出した一般にアクセス可能なバケットなど) を特定することもできます。

機密データの自動検出を設定および管理するには、 アカウントが組織の Macie 管理者アカウントまたはスタンドアロン Macie アカウントである必要があります。

トピック

- 機密データの自動検出の仕組み
- 機密データ自動検出の設定
- 個々の S3 バケットの機密データ自動検出の管理
- 機密データ自動検出カバレッジの評価
- 機密データの自動検出の統計と結果の確認
- S3 バケットの機密スコア
- 機密データの自動検出のデフォルト設定

機密データの自動検出の仕組み

で Amazon Macie を有効にすると AWS アカウント、Macie は現在の でアカウントの AWS Identity and Access Management (IAM) サービスにリンクされたロールを作成します AWS リージョン。

このロールのアクセス許可ポリシーにより、Macie はユーザーに代わって他の を呼び出し AWS のサービス 、 AWS リソースをモニタリングできます。このロールを使用することで、Macie はリージョン内の Amazon Simple Storage Service (Amazon S3) 汎用バケットの完全なインベントリを生成し、維持します。インベントリには、バケット内の各 S3 バケットとオブジェクトに関する情報が含まれます。ユーザーが組織の Macie 管理者である場合、インベントリにはメンバーアカウントが所有するバケットに関する情報が含まれます。詳細については、「複数のアカウントの管理」を参照してください。

機密データの自動検出を有効にすると、Macie はインベントリデータを毎日評価して、自動検出の対象となる S3 オブジェクトを特定します。評価の一環として、Macie は代表的なオブジェクトのサンプルを選択して分析します。その後、Macie は選択した各オブジェクトの最新バージョンを取得して分析し、機密データがないか検査します。

分析が毎日進むにつれて、Macie は Amazon S3 データについて提供する統計、インベントリデータ、およびその他の情報を更新します。Macie は、検出した機密データや実行した分析の記録も作成します。結果として得られるデータは、Macie が Amazon S3 データ資産内の機密データを検出した場所に関するインサイトを提供します。これは、Macie がアカウントのためにモニタリングおよび分析するすべての S3 汎用バケットにまたがる可能性があります。このデータは、Amazon S3 データのセキュリティとプライバシーを評価し、より詳細な調査を行う場所を決定し、修復が必要なケースを特定するのに役立ちます。

機密データの自動検出の仕組みの簡単なデモンストレーションについては、次の動画をご覧ください。Amazon Macie 自動データ検出の概要

機密データの自動検出を設定および管理するには、 アカウントが組織の Macie 管理者アカウントまたはスタンドアロン Macie アカウントである必要があります。アカウントが組織の一部である場合、組織の Macie 管理者のみが組織内のアカウントの機密データ自動検出を有効または無効にできます。さらに、Macie 管理者のみがアカウントの機密データ自動検出設定を構成および管理できます。

トピック

- 主要コンポーネント
- 考慮事項

主要コンポーネント

Amazon Macie は、機能と手法を組み合わせて機密データの自動検出を実行します。これらは、Macie が提供する機能と連動して、Amazon S3 データのセキュリティとアクセスコントロールのモニタリングを支援します。

分析する S3 オブジェクトの選択

Macie は毎日 Amazon S3 インベントリデータを評価して、機密データ自動検出による分析の対象となる S3 オブジェクトを識別します。ユーザーが組織の Macie 管理者である場合、デフォルトでは、評価にはメンバーアカウントが所有する S3 バケットのデータが含まれます。

評価の一環として、Macie はサンプリング技術を使用して、分析する代表的な S3 オブジェクトを選択します。この手法は、メタデータが類似していて内容が類似している可能性が高いオブジェクトのグループを定義します。グループは、バケット名、プレフィックス、ストレージクラス、ファイル名拡張子、最終更新日などのディメンションに基づいています。次に、Macie は各グループから代表的なサンプルセットを選択し、選択した各オブジェクトの最新バージョンを Amazon S3 から取得し、選択した各オブジェクトを分析して、オブジェクトに機密データが含まれているかどうかを判断します。分析が完了すると、Macie はオブジェクトのコピーを破棄します。

サンプリング戦略では、分散分析が優先されます。一般的に、Amazon S3 のデータエステートは幅優先のアプローチを採用しています。毎日、S3 オブジェクトの代表的なセットは、Amazon S3 データエステート内のすべての分類可能なオブジェクトの合計ストレージサイズに基づいて、可能な限り多くの汎用バケットから選択されます。例えば、Macie が 1 つのバケット内のオブジェクトの機密データをすでに分析して検出し、別のバケット内のオブジェクトをまだ分析していない場合、後者のバケットは分析の優先度が高くなります。このアプローチにより、Amazon S3 データの機密性に関する幅広い洞察をより迅速に得ることができます。データ資産のサイズによっては、分析結果が 48 時間以内に表示され始める場合があります。

また、サンプリング戦略では、さまざまなタイプの S3 オブジェクトや、最近作成または変更されたオブジェクトの分析も優先されます。単一のオブジェクトサンプルが決定的であるとは限りません。したがって、さまざまなオブジェクトのセットを分析することで、S3 バケットに含まれる機密データのタイプと量をよりよく理解できます。さらに、新しいオブジェクトまたは最近変更されたオブジェクトに優先順位を付けると、バケットインベントリへの変更に分析を適応させるのに役立ちます。例えば、前回の分析の後にオブジェクトが作成または変更された場合、それらのオブジェクトはその後の分析で優先度が高くなります。逆に、オブジェクトが以前に分析され、その分析以降に変更されていない場合、Macie はそのオブジェクトを再度分析しません。このアプローチは、個々の S3 バケットの感度ベースラインを確立するのに役立ちます。その後、

アカウントの継続的な段階的な分析が進むにつれて、個々のバケットの感度評価が予測可能な速度でますます深く、詳細になります。

分析範囲の定義

デフォルトでは、Macie はインベントリデータを評価し、分析する S3 オブジェクトを選択するときに、アカウントのためにモニタリングおよび分析するすべての S3 汎用バケットを含めます。お客様が組織の Macie 管理者である場合、これには、お客さまのメンバーアカウントが所有するバケットが含まれます。

特定の S3 バケットを除外することで、分析の範囲を調整できます。例えば、イベントログなどの AWS AWS CloudTrail ログデータを保存するバケットを除外できます。バケットを除外するには、アカウントまたはバケットの機密データ自動検出設定を変更できます。これを行うと、Macie は次の日次評価および分析サイクルが始まるときにバケットの除外を開始します。最大 1,000 個のバケットを分析から除外できます。S3 バケットを除外すると、後で再度含めることができます。これを行うには、アカウントまたはバケットの設定を再度変更します。Macie は、次の日次評価と分析のサイクルが始まるとバケットの検出を開始します。

ユーザーが組織の Macie 管理者である場合は、組織内の個々のアカウントの機密データ自動検出を有効または無効にすることもできます。アカウントの自動検出を無効にすると、Macie はアカウントが所有するすべての S3 バケットを除外します。その後、アカウントの自動検出を再度有効にすると、Macie はバケットを再度含め始めます。

検出して報告する機密データのタイプを決定する

デフォルトでは、Macie は機密データの自動検出に推奨されるマネージドデータ識別子のセットを使用して S3 オブジェクトを検査します。これらのマネージドデータ識別子のリストについては、機密データの自動検出のデフォルト設定 を参照してください。

特定の種類の機密データに焦点を当てるように分析を調整できます。そのためには、アカウントの機密データ自動検出設定を以下のいずれかの方法で変更します。

- マネージドデータ識別子の追加または削除 – マネージドデータ識別子は、クレジットカード番号、 AWS シークレットアクセスキー、特定の国または地域のパスポート番号など、特定のタイプの機密データを検出するように設計された一連の組み込み基準と手法です。詳細については、「マネージドデータ識別子の使用」を参照してください。
- カスタムデータ識別子の追加または削除 – カスタムデータ識別子は、機密データを検出するために定義する一連の基準です。カスタムデータ識別子を使用すると、従業員 ID、顧客アカウント番号、内部データの分類など、組織の特定のシナリオ、知的財産、または専有データを反映する機密データを検出できます。詳細については、「カスタムデータ識別子の構築」を参照してください。

- 許可リストの追加または削除 – Macie では、許可リストは、Macie が S3 オブジェクトで無視するテキストまたはテキストパターンを指定します。これらは通常、組織のパブリックネームや電話番号、組織がテストに使用するサンプルデータなど、特定のシナリオや環境の機密データの例外です。詳細については、「許可リストでの機密データの例外の定義」を参照してください。

設定を変更した場合、Macie は次の日次分析サイクルの開始時に変更を適用します。ユーザーが組織の Macie 管理者である場合、Macie は組織内の他のアカウントの S3 オブジェクトを分析するときに、アカウントの設定を使用します。

バケットレベルの設定を調整して、特定のタイプの機密データをバケットの機密性の評価に含めるかどうかを決定することもできます。この方法の詳細は、個々の S3 バケットの機密データ自動検出の管理を参照してください。

機密スコアの計算

デフォルトでは、Macie はアカウントのモニタリングと分析を行う S3 汎用バケットごとに機密スコアを自動的に計算します。お客様が組織の Macie 管理者である場合、これには、お客さまのメンバーアカウントが所有するバケットが含まれます。

Macie では、機密スコアは、Macie がバケット内で検出した機密データの量と Macie がバケット内で分析したデータの量という 2 つの主要なディメンションの共通集合を定量的に測定したものです。バケットの機密スコアによって、Macie がバケットに割り当てる機密ラベルが決まります。機密ラベルは、バケットの機密スコアを定性的に表したものです。例えば、機密、非機密、分析が未完了などです。Macie が定義する機密性スコアとラベルの範囲の詳細については、S3 バケットの機密スコア を参照してください。

> **Important**
>
> S3 バケットの機密スコアとラベルは、バケットまたはバケットのオブジェクトが組織に対して緊急性または重要性を意味する、または示すものではありません。代わりに、潜在的なセキュリティリスクの特定とモニタリングに役立つ参照ポイントを提供することを目的としています。

機密データの自動検出を最初に有効にすると、Macie は機密スコア 50 と未分析ラベルを各 S3 バケットに自動的に割り当てます。ただし、空のバケットは例外です。空のバケットは、オブジェクトを保存しないバケット、またはバケットのすべてのオブジェクトにゼロ (0) バイトのデータが含まれているバケットです。バケットの場合、Macie はバケットに1のスコアを割り当て、バケットには非機密ラベルを割り当てます。

機密データの自動検出が進むにつれて、Macie は分析の結果を反映するように機密スコアとラベルを更新します。例:

- Macie がオブジェクト内の機密データを検出しない場合、必要に応じてMacie はバケットの機密スコアを下げ、バケットの機密ラベルを更新します。
- Macie がオブジェクト内の機密データを検出すると、必要に応じて Macie はバケットの機密スコアを上げ、バケットの機密ラベルを更新します。
- その後変更されたオブジェクト内で機密データが検出された場合、Macie は必要に応じてそのオブジェクトの機密データ検出をバケットの機密スコアから削除し、バケットの機密ラベルを更新します。
- その後削除されたオブジェクト内で機密データが検出された場合、Macie は必要に応じてそのオブジェクトの機密データをバケットの機密スコアから削除し、バケットの機密ラベルを更新します。

特定のタイプの機密データをバケットのスコアに含めたり除外したりすることで、個々の S3 バケットの感度スコアリング設定を調整できます。最大スコア(100) をバケットに手動で割り当てることで、バケットの計算スコアを上書きすることもできます。最大スコアを割り当てると、バケットには機密というラベルが付けられます。詳細については、個々の S3 バケットの自動検出の管理を参照してください。

メタデータ、統計、結果の生成

機密データの自動検出を有効にすると、Macie はアカウントでモニタリングおよび分析する S3 汎用バケットに関する追加のインベントリデータ、統計、およびその他の情報を生成して維持し始めます。ユーザーが組織の Macie 管理者である場合、デフォルトでは、メンバーアカウントが所有するバケットが含まれます。

追加情報は、Macie がこれまでに実行した機密データ自動検出アクティビティの結果をキャプチャします。また、個々のバケットのパブリックアクセスや共有アクセス設定など、Macie が提供する Amazon S3 データに関するその他の情報を補足するものでもあります。追加情報には以下が含まれます。

- Macie が機密データを検出したバケットの総数や、それらのバケットのうちパブリックにアクセスできるバケットの数など、集約されたデータ機密性統計。
- Amazon S3 データ工ステート全体のデータ機密性をインタラクティブかつ視覚的に表現します。
- 分析の現在のステータスを示すバケットレベルの詳細。例えば、Macie がバケット内で分析したオブジェクトのリスト、Macie がバケット内で検出した機密データのタイプ、Macie が検出した各タイプの機密データの出現回数などです。

この情報には、Amazon S3 データのカバレッジを評価およびモニタリングするのに役立つ統計と詳細も含まれています。データエステート全体とバケットインベントリ内の個々の S3 バケットの分析ステータスを確認できます。Macie が特定バケット内のオブジェクトを分析できなかった問題を特定することもできます。問題を修正すれば、その後の分析サイクルで Amazon S3 データのカバレッジを拡大できます。詳細については、「機密データ自動検出カバレッジの評価」を参照してください。

Macie は、機密データの自動検出を実行している間、この情報を自動的に再計算して更新します。例えば、Macie が S3 オブジェクトで機密データを見つけ、その後変更または削除された場合、Macie は該当するバケットのメタデータを更新します。分析されたオブジェクトのリストからオブジェクトを削除します。Macie がオブジェクト内で見つけた機密データの出現を削除します。スコアが自動的に計算された場合、機密性スコアを再計算します。また、必要に応じて機密ラベルを更新して新しいスコアを反映します。

メタデータと統計に加えて、Macie は検出した機密データと実行した分析のレコードを生成します。機密データの検出結果は、Macie が個々の S3 オブジェクトで検出した機密データをレポートし、機密データの検出結果は、個々の S3 オブジェクトの分析に関する詳細をログに記録します。

詳細については、「機密データの自動検出の統計と結果の確認」を参照してください。

考慮事項

Amazon Macie を設定して使用して Amazon S3 データの自動機密データ検出を実行するときは、次の点に注意してください。

- 自動検出設定は、現在の にのみ適用されます AWS リージョン。したがって、結果の分析とデータは、現在のリージョンの S3 汎用バケットとオブジェクトにのみ適用されます。追加のリージョンの自動検出を実行し、結果データにアクセスするには、追加の各リージョンで自動検出を有効化して設定します。
- ユーザーが組織の Macie 管理者である場合:
  - 現在のリージョンのアカウントで Macie が有効になっている場合にのみ、メンバーアカウントの自動検出を実行できます。さらに、そのリージョンのアカウントの自動検出を有効にする必要があります。メンバーは、自分のアカウントで自動検出を有効にすることはできません。
  - メンバーアカウントの自動検出を有効にすると、Macie はメンバーアカウントのデータを分析する際に、管理者アカウントの自動検出設定を使用します。適用可能な設定は、分析から除外する S3 バケットのリスト、マネージドデータ識別子、カスタムデータ識別子、S3 オブジェクトの分

析時に使用できる許可リストです。メンバーは、自分のアカウントに対してこれらの設定を構成することはできません。

  - メンバーは S3 バケットの自動検出設定にアクセスできません。例えば、メンバーが所有しているバケットの機密スコアリング設定を調整することはできません。Macie 管理者だけがこれらの設定にアクセスできます。
  - メンバーは、Macie が S3 バケットに直接提供する機密データ検出統計やその他の結果にアクセスできません。例えば、メンバーは Macie を使用して S3 バケットの機密スコアを確認したり、自動検出が S3 オブジェクトに対して生成する検出結果にアクセスしたりすることはできません。Macie を使用してこのデータにアクセスできるのは、Macie 管理者のみです。

- S3 バケットのアクセス許可設定により、Macie がバケットまたはバケットのオブジェクトに関する情報を取得する、またはバケットのオブジェクトにアクセスするのを妨げるようにしている場合、Macie はバケットの自動検出を実行できません。Macie は、バケットを所有する AWS アカウント のアカウント ID、バケットの名前、および毎日の更新サイクルの一部として Macie がバケットとオブジェクトのメタデータを最後に取得した日時。バケットインベントリでは、これらのバケットの機密スコアは50で、その機密ラベルの分析が未完了です。

  このような状況にある S3 バケットをすばやく特定するには、自動検出力バレッジデータを参照してください。詳細については、機密データ自動検出力バレッジの評価を参照してください。特定のバケットの問題を調査するには、Amazon S3 内のバケットのポリシーとアクセス許可の設定を確認します。例えば、バケットには制限があるバケットポリシーが設定されている場合があります。詳細については、「Macie が S3 バケットおよびオブジェクトにアクセスすることを許可する」を参照してください。

- 選択と分析の対象となるには、S3 オブジェクトを汎用バケットに保存し、分類可能な である必要があります。分類可能なオブジェクトは、サポートされているAmazon S3ストレージクラスを使用し、サポートされているファイルまたはストレージフォーマットのファイル名拡張子を持っています。詳細については、サポートされているストレージクラスとフォーマットを参照してください。

- S3 オブジェクトが暗号化されている場合、Macie がそれを分析できるのは Macie がアクセス可能で使用を許可されているキーを用いて暗号化されている場合のみです。詳細については、暗号化された S3 オブジェクトの分析を参照してください。暗号化設定により Macie がバケット内の 1 つ以上のオブジェクトを分析できなかったケースを特定するには、自動検出力バレッジデータを参照してください。詳細については、機密データ自動検出力バレッジの評価を参照してください。

機密データ自動検出の設定

機密データの自動検出により、Amazon Macie は Amazon Simple Storage Service (Amazon S3) 汎用バケットからサンプルオブジェクトを継続的に選択し、オブジェクトを分析して機密データが含まれているかどうかを判断します。ユーザーが組織の Macie 管理者である場合、デフォルトでは、メンバーアカウントが所有する S3 バケット内のオブジェクトが含まれます。分析が進むにつれて、Macie は Amazon S3 データについて提供する統計、インベントリデータ、およびその他の情報を更新します。Macie は、検出した機密データや実行した分析の記録も作成します。

機密データの自動検出を設定および管理するには、 アカウントが組織の Macie 管理者アカウントまたはスタンドアロン Macie アカウントである必要があります。アカウントが組織の一部である場合、組織の Macie 管理者のみが組織内のアカウントの機密データ自動検出を有効または無効にできます。さらに、Macie 管理者のみがアカウントの機密データ自動検出設定を行うことができます。メンバーアカウントがあり、Macie に S3 バケットの機密データ自動検出を実行させたい場合は、Macie 管理者にお問い合わせください。

トピック

自動機密データ検出を有効、設定、または無効にすると、変更は現在の にのみ適用されます AWS リージョン。追加のリージョンで同じ変更を行うには、追加のリージョンごとに該当するステップを繰り返します。

開始する前に

機密データの自動検出を有効化または設定する前に、以下のタスクを完了して、必要なリソースとアクセス許可があることを確認してください。

タスク

これらのタスクは、機密データの自動検出を既に有効化および設定していて、設定を変更または無効化するだけの場合はオプションです。

機密データ検出結果のリポジトリを設定する

Amazon Macie が機密データの自動検出を実行すると、分析用に選択した各 Amazon Simple Storage Service (Amazon S3) オブジェクトの分析レコードが作成されます。これらのレコードは、機密データ検出結果 と呼ばれ、個々の S3 オブジェクトの分析に関する詳細を口グに記録します。これには、Macie が機密データを見つけられないオブジェクト、およびアクセス許可設定などのエラーや問題のために Macie が分析できないオブジェクトが含まれます。Macie がオブジェクト内で機密データを検出した場合、機密データ検出結果には Macie が検出した機密データに関する情報が含まれます。機密データの検出結果から、データプライバシーと保護の監査や調査に役立つ分析レコードが得られます。

Macie は機密データの検出結果を 90 日間だけ保存します。結果にアクセスし、それらの長期保存と保持を有効化するには、結果を S3 バケットに保存するように Macie を設定します。バケットは、機密データの検出結果のすべての最終的で長期的なリポジトリとして機能します。

このリポジトリを設定したことを確認するには、Amazon Macie コンソールのナビゲーションペインで検出結果を選択します。プログラムでこれを行う場合は、Amazon Macie API の GetClassificationExportConfigurationオペレーションを使用します。機密データ検出の結果とこのリポジトリの設定方法の詳細については、「機密データ検出結果の保存と保持」を参照してください。

リポジトリを設定した場合、Macie は機密データの自動検出を初めて有効にすると、リポジトリ`automated-sensitive-data-discovery`に という名前のフォルダを作成します。このフォルダには、アカウントまたは組織の自動検出の実行中に Macie が作成した機密データ検出結果が保存されます。

アクセス許可を確認する

アクセス許可を確認するには、 AWS Identity and Access Management (IAM) を使用して、IAM ID にアタッチされている IAM ポリシーを確認します。次にこれらのポリシー内の情報を、実行が許可される必要がある次のアクションのリストと比較します。

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`
- `macie2:ListClassificationScopes`
- `macie2:UpdateClassificationScope`
- `macie2:ListSensitivityInspectionTemplates`

- macie2:UpdateSensitivityInspectionTemplate

最初のアクションでは、Amazon Macie アカウントにアクセスできます。2 番目のアクションでは、アカウントまたは組織の機密データ自動検出を有効または無効にできます。組織の場合、組織内のアカウントの機密データ自動検出を自動的に有効にすることもできます。残りのアクションでは、設定を識別して変更できます。

Amazon Macie コンソールを使用して構成設定を確認または変更する場合は、次のアクションの実行も許可されていることを確認します。

- macie2:GetAutomatedDiscoveryConfiguration
- macie2:GetClassificationScope
- macie2:GetSensitivityInspectionTemplate

これらのアクションにより、アカウントまたは組織の現在の設定と機密データ自動検出のステータスを取得できます。構成設定をプログラムで変更する場合は、これらのアクションを実行するアクセス許可はオプションです。

ユーザーが組織の Macie 管理者である場合は、次のアクションの実行も許可されている必要があります。

- macie2:ListAutomatedDiscoveryAccounts
- macie2:BatchUpdateAutomatedDiscoveryAccounts

最初のアクションでは、組織内の個々のアカウントの機密データ自動検出のステータスを取得できます。2 番目のアクションでは、組織内の個々のアカウントの機密データ自動検出を有効または無効にできます。

必要なアクションを実行することが許可されていない場合は、 AWS 管理者にサポートを依頼してください。

組織の設定オプション

アカウントが複数の Amazon Macie アカウントを一元管理する組織の一部である場合、組織の Macie 管理者は組織内のアカウントの機密データ自動検出を設定および管理します。これには、Macie がアカウントに対して実行する分析の範囲と性質を定義する設定が含まれます。メンバーは、自分のアカウントのこれらの設定にアクセスできません。

ユーザーが組織の Macie 管理者である場合は、いくつかの方法で分析の範囲を定義できます。

- アカウントの機密データ自動検出を自動的に有効にする – 機密データ自動検出を有効にする場合、既存のすべてのアカウントと新しいメンバーアカウントに対して自動的に有効にするか、新しいメンバーアカウントに対してのみ有効にするか、アカウントなしで有効にするかを指定します。新しいメンバーアカウントで自動的に有効にすると、その後 Macie で組織に参加するすべてのアカウントで有効になります。アカウントで有効になっている場合、Macie にはアカウントが所有する S3 バケットが含まれます。アカウントに対して無効になっている場合、Macie はアカウントが所有するバケットを除外します。
- アカウントの機密データ自動検出を選択的に有効にする – このオプションでは、個々のアカウントの機密データ自動検出を case-by-case ベースで有効または無効にします。アカウントに対して有効にすると、Macie にはアカウントが所有する S3 バケットが含まれます。有効にしない場合、またはアカウントに対して無効にした場合、Macie はアカウントが所有するバケットを除外します。
- 機密データの自動検出から特定の S3 バケットを除外する – 1 つ以上のアカウントで機密データの自動検出を有効にすると、アカウントが所有する特定の S3 バケットを除外できます。その後、Macie は組織の自動検出を実行するときにバケットをスキップします。特定のバケットを除外するには、管理者アカウントの設定でバケット除外リストに追加します。組織に対して最大 1,000 個のバケットを除外できます。

デフォルトでは、組織内のすべての新規および既存のアカウントに対して機密データの自動検出が自動的に有効になります。さらに、Macie にはアカウントが所有するすべての S3 バケットが含まれます。デフォルト設定のままにしておくと、Macie は管理者アカウントのためにモニタリングおよび分析するすべてのバケットの自動検出を実行します。これには、メンバーアカウントが所有するすべてのバケットが含まれます。

Macie 管理者は、Macie が組織に対して実行する分析の性質も定義します。これを行うには、管理データ識別子、カスタムデータ識別子、および Macie が S3 オブジェクトを分析するときに使用するリストなど、管理者アカウントの追加設定を行います。Macie は、組織内の他のアカウントの S3 オブジェクトを分析するときに、管理者アカウントの設定を使用します。

機密データ自動検出の有効化

機密データ自動検出を有効にすると、Amazon Macie は Amazon S3 インベントリデータの評価と、現在の でアカウントのその他の自動検出アクティビティの実行を開始します AWS リージョン。ユーザーが組織の Macie 管理者である場合、デフォルトでは、メンバーアカウントが所有する S3 バ

ケットが含まれます。Amazon S3 データ資産のサイズによっては、機密データ検出統計やその他の結果が 48 時間以内に表示され始める場合があります。

アカウントまたは組織の機密データの自動検出を有効にするには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。コンソールを使用して有効にするには、次の手順に従います。プログラムで有効にするには、Amazon Macie API の次のオペレーションを使用します。、組織内の個々のアカウントBatchUpdateAutomatedDiscoveryAccountsの場合は 、、組織UpdateAutomatedDiscoveryConfigurationの場合は 、Macie 管理者アカウント、スタンドアロン Macie アカウント。

機密データの自動検出を有効にするには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、機密データの自動検出を有効にするリージョンを選択します。
3. ナビゲーションペインの設定 で、機密データの自動検出 を選択します。
4. スタンドアロン Macie アカウントをお持ちの場合は、ステータスセクションで有効化を選択します。
5. ユーザーが組織の Macie 管理者である場合は、ステータスセクションでオプションを選択して、機密データの自動検出を有効にするアカウントを指定します。

   - 組織内のすべてのアカウントで有効にするには、 を有効にする を選択します。表示されるダイアログボックスで、組織 を選択します。後で組織に参加するアカウントでも自動的に有効にするには、新しいアカウントで自動的に有効にする を選択します。完了したら、 を有効にする を選択します。
   - 特定のメンバーアカウントでのみ有効にするには、アカウントを管理する を選択します。次に、「アカウント」ページの表で、有効にする各アカウントのチェックボックスをオンにします。完了したら、アクションメニューで機密データの自動検出を有効にするを選択します。
   - Macie 管理者アカウントでのみ有効にするには、 を有効にするを選択します。表示されるダイアログボックスで、マイアカウント を選択し、新しいアカウント に対して自動的に有効にする を選択します。完了したら、 を有効にする を選択します。

   その後、組織内の個々のアカウントの機密データ自動検出のステータスを確認または変更するには、ナビゲーションペインのアカウントを選択します。アカウントページで、テーブルの機密データ自動検出フィールドは、アカウントの自動検出の現在のステータスを示します。アカウン

トのステータスを変更するには、アカウントを選択し、アクションメニューを使用して を有効にし、アカウントの自動検出を無効にします。

機密データの自動検出を有効にしたら、設定を確認して設定し、Macie が実行する分析を絞り込みます。

機密データ自動検出の設定

アカウントまたは組織の機密データ自動検出を有効にすると、自動検出の設定を調整して、Amazon Macie が実行する分析を絞り込むことができます。これらの設定では、分析から除外する S3 バケットを指定します。また、マネージドデータ識別子、カスタムデータ識別子、S3 オブジェクトの分析時に使用できるリストなど、検出してレポートする機密データのタイプと出現も指定します。

デフォルトでは、Macie はアカウントのモニタリングと分析を行うすべての S3 汎用バケットに対して機密データの自動検出を実行します。お客様が組織の Macie 管理者である場合、これには、お客さまのメンバーアカウントが所有するバケットが含まれます。特定のバケットを分析から除外できます。例えば、 AWS CloudTrail イベントログなどの AWS ログデータを保存するバケットを除外できます。バケットを除外した場合、そのバケットを後で再び含めることができます。

さらに、Macie は、機密データ自動検出に推奨されるマネージドデータ識別子のセットのみを使用して S3 オブジェクトを分析します。Macie はカスタムデータ識別子やユーザーが定義した許可リストを使用しません。分析をカスタマイズするには、特定のマネージドデータ識別子、カスタムデータ識別子、許可リストを使用するように Macie を設定します。

以下のセクションでは、各タイプの設定に関する追加情報を提供します。また、Amazon Macie コンソールを使用して設定を変更する方法についても説明します。詳細については、セクションを選択してください。設定をプログラムで確認または変更するには、Amazon Macie API の次のオペレーションを使用できます。UpdateClassificationScope、分析から除外する S3 バケットを指定する、およびUpdateSensitivityInspectionTemplate、どのマネージドデータ識別子、カスタムデータ識別子、および許可リストを使用するかを指定します。

設定を変更した場合、Macie は、機密データ自動検出のための次の評価および分析サイクルが開始されたときに（通常は 24 時間以内）、変更を適用します。

S3 バケットを除外または含める

デフォルトでは、Macie はアカウントのモニタリングと分析を行うすべての S3 汎用バケットに対して機密データの自動検出を実行します。お客様が組織の Macie 管理者である場合、これには、お客さまのメンバーアカウントが所有するバケットが含まれます。

スコープを絞り込むには、分析から最大 1,000 個の S3 バケットを除外できます。バケットを除外すると、Macie は機密データの自動検出を実行するときに、バケット内のオブジェクトの選択と分析を停止します。バケットの既存の機密データ検出統計と詳細は保持されます。例えば、バケットの現在の機密スコアは変わりません。バケットを除外した後、そのバケットを再度含めることができます。

特定の S3 バケットを除外または含めるには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、自動検出分析で特定の S3 バケットを除外または含めるリージョンを選択します。
3. ナビゲーションペインの設定 で、機密データの自動検出 を選択します。

   機密データ自動検出 ページが表示され、現在の設定が表示されます。そのページの [S3 バケット] セクションには、現在除外されている S3 バケットが一覧表示されているか、現在すべてのバケットが含まれていることが示されます。
4. S3 バケット セクションで、編集 を選択します。
5. 次のいずれかを行います。

   - 1 つ以上の S3 バケットを除外するには、[除外リストにバケットを追加] を選択します。次に、[S3 バケット] テーブルで、除外する各バケットのチェックボックスをオンにします。この表には、現在のリージョンのアカウントまたは組織のすべての汎用バケットが一覧表示されます。
   - 以前に除外した 1 つ以上の S3 バケットを含めるには、[除外リストからバケットを削除する] を選択します。次に、[S3 バケット] テーブルで、含める各バケットのチェックボックスをオンにします。この表には、現在自動検出分析から除外されているすべてのバケットが一覧表示されています。

   特定のバケットをより簡単に検索するには、テーブルの上にある検索ボックスに検索条件を入力します。列見出しを選択して、テーブルを並べ替えることもできます。
6. バケットを選択し終えたら、前のステップで選択したオプションに応じて [追加] または [削除] を選択します。

マネージドデータ識別子の追加または削除

マネージドデータ識別子は、クレジットカード番号、 AWS シークレットアクセスキー、特定の国や地域のパスポート番号など、特定のタイプの機密データを検出するように設計された一連の組み込み

基準と手法です。デフォルトでは、Macie は機密データ自動検出に推奨するマネージドデータ識別子のセットを使用して S3 オブジェクトを分析します。これらの識別子のリストを確認するには、「」を参照してください機密データの自動検出のデフォルト設定。

分析を調整して、特定のタイプの機密データに焦点を当てることができます。

- Macie が検出およびレポートする機密データのタイプにマネージドデータ識別子を追加します。
- Macie が検出して報告したくない機密データのタイプに関するマネージドデータ識別子を削除します。

マネージドデータ識別子を削除しても、S3 バケットの既存の機密データ検出統計や詳細には影響しません。例えば、シークレットアクセスキーの AWS マネージドデータ識別子を削除し、Macie がバケット内のそのタイプのデータを以前に検出した場合、Macie は引き続きバケットの検出を報告します。

> **Tip**
>
> すべての S3 バケットの後続の分析に影響するマネージドデータ識別子を削除する代わりに、その検出を特定のバケットの機密スコアから除外できます。詳細については、「個々の S3 バケットの機密データ自動検出の管理」を参照してください。

マネージドデータ識別子を追加または削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、自動検出分析でマネージドデータ識別子を追加または削除するリージョンを選択します。
3. ナビゲーションペインの設定 で、機密データの自動検出 を選択します。

   機密データ自動検出 ページが表示され、現在の設定が表示されます このページの「マネージドデータ識別子」セクションには、現在の設定が 2 つのタブに整理されて表示されます。

   - デフォルトに追加 – このタブには、追加したマネージドデータ識別子が一覧表示されます。Macie は、デフォルトセットに含まれていて、削除されていない識別子に加えて、これらの識別子を使用します。
   - デフォルトから削除 – このタブには、削除したマネージドデータ識別子が一覧表示されます。Macie はこれらの識別子を使用しません。
4. [マネージドデータ識別子] セクションで [編集] を選択します。

5. 次のいずれかを実行します。

   - 1 つ以上のマネージドデータ識別子を追加するには、[デフォルトに追加] タブを選択します。次に、テーブルで、追加する各マネージドデータ識別子のチェックボックスをオンにします。チェックボックスが既にオンになっている場合は、その識別子を既に追加しています。
   - 1 つ以上のマネージドデータ識別子を削除するには、[デフォルトから削除] タブを選択します。次に、テーブルで、削除する各マネージドデータ識別子のチェックボックスをオンにします。チェックボックスが既にオンになっている場合は、その識別子を既に削除しています。

   各タブには、Macie が現在提供しているすべてのマネージドデータ識別子のリストがテーブルに表示されます。表の最初の列では、各マネージドデータ識別子の ID を指定します。ID は、識別子が検出するように設計された機密データのタイプを記述します。例えば、米国のパスポート番号の場合は USA_PASSPORT_NUMBER です。特定のマネージドデータ識別子をより簡単に検索するには、テーブルの上にある検索ボックスに検索条件を入力します。列見出しを選択して、テーブルを並べ替えることもできます。各識別子の詳細については、マネージドデータ識別子の使用 を参照してください。

6. 完了したら、保存 を選択します。

カスタムデータ識別子の追加または削除

カスタムデータ識別子は、機密データを検出するために定義する基準のセットです。基準は、一致するテキストパターン、オプションで文字シーケンス、結果を絞り込む近接ルールを定義する正規表現 (正規表現) から設定されています。詳細については、カスタムデータ識別子の構築を参照してください。

デフォルトでは、Amazon Macie は機密データ自動検出を実行する際にカスタムデータ識別子を使用しません。Macie に特定のカスタムデータ識別子を使用させたい場合は、それらを分析に追加できます。次に、Macie は、Macie が使用するように設定したマネージドデータ識別子に加えて、カスタムデータ識別子を使用します。

カスタムデータ識別子を追加すると、後で削除できます。変更は、S3 バケットの既存の機密データ検出統計や詳細には影響しません。つまり、以前にバケットの検出を生成したカスタムデータ識別子を削除した場合、Macie はバケットの検出を引き続き報告します。ただし、すべてのバケットの後続の分析に影響する識別子を削除する代わりに、特定のバケットのみの機密スコアからその検出を除外することを検討してください。詳細については、「個々の S3 バケットの機密データ自動検出の管理」を参照してください。

カスタムデータ識別子を追加または削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、自動検出分析でカスタムデータ識別子を追加または削除するリージョンを選択します。
3. ナビゲーションペインの設定 で、機密データの自動検出 を選択します。

   機密データ自動検出 ページが表示され、現在の設定が表示されます このページの「カスタムデータ識別子」セクションには、追加したカスタムデータ識別子が一覧表示されるか、カスタムデータ識別子が選択されていないことを示します。
4. [カスタムデータ識別子] セクションで [編集] を選択します。
5. 次のいずれかを実行します。

   - 1 つ以上のカスタムデータ識別子を追加するには、追加するカスタムデータ識別子ごとにチェックボックスをオンにします。チェックボックスが既にオンになっている場合は、その識別子を既に追加しています。
   - 1 つ以上のカスタムデータ識別子を削除するには、削除するカスタムデータ識別子ごとにチェックボックスをオフにします。チェックボックスが既にオフになっている場合、Macie は現在その識別子を使用しません。

   > **Tip**
   >
   > カスタムデータ識別子を選択する前にその識別子を確認またはテストするには、識別子の名前の横にあるリンクアイコン
   > を選択します。Macie は、識別子の設定を表示するページを開きます。サンプルデータを使用して識別子をテストするには、そのページのサンプルデータボックスに最大 1,000 文字のテキストを入力します。次に、テスト を選択します。Macie はサンプルデータを評価し、一致の数を報告します。
6. 完了したら、保存 を選択します。

許可リストを追加または削除する

Amazon Macie では、許可リストによって、Macie が機密データの S3 オブジェクトを検査する際に無視する特定のテキストまたはテキストパターンを定義します。テキストが許可リストのエントリ

またはパターンと一致する場合、Macie はテキストを報告しません。これは、テキストがマネージドデータ識別子またはカスタムデータ識別子の基準と一致していても当てはまります。詳細については、許可リストでの機密データの例外の定義を参照してください。

デフォルトでは、Macie は機密データ自動検出を実行する際に許可リストを使用しません。Macie に特定の許可リストを使用させたい場合は、それらを分析に追加できます。許可リストを追加すると、後で削除できます。

許可リストを追加または削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、自動検出分析で許可リストを追加または削除するリージョンを選択します。
3. ナビゲーションペインの設定 で、機密データの自動検出 を選択します。

   機密データ自動検出 ページが表示され、現在の設定が表示されます そのページで、許可リストセクションで、既に追加した許可リストを指定するか、許可リストを選択していないことを示します。
4. ストレージ セクションで、編集 を選択します。
5. 次のいずれかを実行します。

   - 1 つ以上の許可リストを追加するには、追加する許可リストごとにチェックボックスをオンにします。チェックボックスが既に選択されている場合は、そのリストを既に追加しています。
   - 1 つ以上の許可リストを削除するには、削除する許可リストごとにチェックボックスをオフにします。チェックボックスが既にオフになっている場合、Macie は現在そのリストを使用しません。

> **Tip**
>
> 許可リストを追加または削除する前にその設定を確認するには、リスト名の横にあるリンクアイコン
> を選択します。Macie は、リストの設定を表示するページを開きます。リストで正規表現 (正規表現)を指定する場合は、このページを使用してサンプルデータでその正規表現を確認することもできます。これを行うには、テキスト (最大 1,000 文字) を サンプル

データ ボックスに入力し、次に テスト を選択します。Macie はサンプルデータを評価し、一致の数を報告します。

6. 完了したら、保存 を選択します。

機密データ自動検出の無効化

アカウントまたは組織の機密データ自動検出はいつでも無効にできます。これを行うと、Macie は後続の評価と分析サイクルを開始する前に、通常 48 時間以内にアカウントまたは組織のすべての自動検出アクティビティの実行を停止します。その他の効果はさまざまです。

- 組織内のアカウントに対して無効にした場合、アカウントの自動検出の実行中に Macie が生成および直接提供したすべての統計データ、インベントリデータ、およびその他の情報に引き続きアクセスできます。アカウントの自動検出を再度有効にすることもできます。その後、Macie はアカウントのすべての自動検出アクティビティを再開します。
- 組織またはスタンドアロン Macie アカウントで無効にすると、組織またはアカウントの自動検出の実行中に Macie が生成および直接提供したすべての統計データ、インベントリデータ、その他の情報にアクセスできなくなります。例えば、S3 バケットインベントリに機密性の視覚化や統計分析が含まれなくなりました。その後、再度有効にすることができます。その後、Macie は組織またはアカウントのすべての自動検出アクティビティを再開します。30 日以内に再度有効にすると、Macie が自動検出の実行中に以前に生成して直接提供したすべてのデータと情報へのアクセスが回復します。30 日以内に再度有効にしないと、Macie はこのデータと情報を完全に削除します。

Macie が組織またはアカウントに対して機密データの自動検出を実行している間に生成した機密データの検出結果に引き続きアクセスできます。Macie は 90 日間調査結果を保存します。さらに、他のに保存または公開したデータはそのまま AWS のサービス 残り、Amazon S3 での機密データの検出結果や Amazon でのイベントの検出結果など、影響を受けません EventBridge。

機密データの自動検出を無効にするには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。コンソールを使用して無効にするには、次の手順に従います。プログラムで無効にするには、Amazon Macie API の次のオペレーションを使用します。、組織内の個々のアカウントBatchUpdateAutomatedDiscoveryAccountsの場合は 、組織UpdateAutomatedDiscoveryConfigurationの場合は 、Macie 管理者アカウント、またはスタンドアロン Macie アカウント。

機密データの自動検出を無効にするには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、機密データの自動検出を無効にするリージョンを選択します。
3. ナビゲーションペインの設定 で、機密データの自動検出 を選択します。
4. ユーザーが組織の Macie 管理者である場合は、ステータスセクションでオプションを選択して、機密データの自動検出を無効にするアカウントを指定します。

   - 特定のメンバーアカウントでのみ無効にするには、アカウントを管理する を選択します。次に、「アカウント」ページの表で、無効にするアカウントごとにチェックボックスをオンにします。完了したら、アクションメニューで機密データの自動検出を無効にするを選択します。
   - Macie 管理者アカウントでのみ無効にするには、 の無効化を選択します。表示されるダイアログボックスで、マイアカウント を選択し、 を無効化 を選択します。
   - 組織内のすべてのアカウントと組織全体で無効にするには、 の無効化を選択します。表示されるダイアログボックスで、組織 を選択し、 を無効化 を選択します。
5. スタンドアロン Macie アカウントをお持ちの場合は、ステータスセクションで Disable を選択します。

個々の S3 バケットの機密データ自動検出の管理

機密データ自動検出の統計と結果を確認して評価すると、個々の Amazon Simple Storage Service (Amazon S3) バケットの機密スコアリングやその他の設定を調整できます。これらの設定を調整することで、Amazon S3 データ資産全体とデータ資産内の特定のバケットの機密性評価を微調整できます。また、特定のバケットに対して実施した調査の結果をキャプチャすることもできます。

S3 バケットの機密データ自動検出設定は、次の方法で調整できます。

機密スコアを割り当てる

デフォルトでは、Amazon Macie はバケットの機密スコアを自動的に計算します。スコアは主に Macie がバケット内で検出した機密データ量、およびバケット内で分析したデータ量に基づいています。詳細については、S3 バケットの機密スコアを参照してください。

バケットの計算スコアを上書きし、手動で最大スコア(100)を割り当てることができます。これにより、バケットに機密ラベルも適用されます。これを行うと、Macie はバケットに対して引き続

き自動検出を実行します。ただし、その後の分析はバケットのスコアには影響しません。スコアを再度自動的に計算するには、設定をもう一度変更してください。

特定の機密データタイプを機密スコアから除外または含める

自動計算の場合、バケットの機密スコアは部分的に、Macie がバケット内で検出した機密データ量に基づいて算出されます。これは主に、Macie がバケット内で検出した機密データタイプの性質と数、および各タイプの出現数から導き出されます。デフォルトでは、Macie はバケットの機密スコアを計算するときに、あらゆるタイプの機密データの出現回数を含めます。

特定のタイプの機密データをバケットのスコアから除外したり含めたりすることで、計算を調整できます。例えば、Macie がバケット内の郵送先住所を検出し、それが問題ないと判断した場合、そのバケットのスコアからすべての郵送先住所を除外できます。ある機密データタイプを除外した場合、Macie は引き続きバケットにそのタイプのデータがないか調べ、検出したデータの出現を報告します。ただし、これらの出現はバケットの計算スコアには影響しません。計算スコアに機密データタイプを再度含めるには、設定を再度変更してください。

対象のバケットを今後の分析に除外または含める

デフォルトでは、Macie はアカウントのモニタリングと分析を行うすべての汎用バケットの自動検出を実行します。ユーザーが組織の Macie 管理者である場合、デフォルト設定にはメンバーアカウントが所有するバケットが含まれます。分析から特定のバケットを除外できます。例えば、AWS CloudTrail イベントログなどの AWS ログデータを保存するバケットを除外できます。

バケットを除外しても、そのバケットに関する既存の機密データ検出統計と詳細はそのまま残ります。例えば、バケットの現在の機密スコアは変わりません。ただし、Macie は自動検出を実行するとバケット内のオブジェクトの分析を停止します。バケットを除外した後、そのバケットを再度含めることができます。

S3 バケットの機密スコアに影響する設定を変更すると、Macie は直ちに Amazon S3 データに関して提供する関連する統計と情報の再計算と更新を開始します。例えば、バケットに最大スコアを割り当てると、Macie はアカウントまたは組織の集計統計で機密バケットの数を増やします。

Amazon Macie コンソールを使用して設定を変更するには、次のステップに従います。設定をプログラムで変更するには、Amazon Macie API の次のオペレーションを使用できます。UpdateResourceProfile、バケットに機密性スコアを割り当てる、UpdateResourceProfileDetections、バケットのスコアに機密データタイプを除外またはその後含める、および後続の分析にバケットUpdateClassificationScopeを除外または含める。

S3 バケットの機密データ自動検出設定を変更する

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで、S3 バケットを選択します。S3 バケットページにはバケットインベントリが表示されます。

   デフォルトでは、このページには、現在分析から除外されているバケットのデータが表示されません。ユーザーが組織の Macie 管理者である場合、機密データの自動検出が現在無効になっているアカウントのデータも表示されません。このデータを表示するには、フィルターボックスの下にある自動検出フィルタートークンによってモニタリングされる で X を選択します。
3. 設定を変更する S3 バケットを選択します。テーブルビュー
   ( )
   またはインタラクティブマップ () を使用してバケットを選択できます 。
4. 詳細パネルで、次のいずれかの操作を実行します。

   - 計算されたスコアを上書きしてバケットに機密スコアを手動で割り当てるには、[最大スコアの割り当
     て]
     をオンにします。これによりバケットのスコアが 100 に変更され、機密ラベルがバケットに適用されます。

     Macie が自動的に計算するスコアを割り当てるには、[最大スコアの割り当
     て]
     をオフにします。
   - バケットを以降の分析から除外するには、[自動検出から除
     外]
     をオンにします。

     以前にバケットを分析から除外していた場合は、[自動検出から除
     外]
     をオフにして再度分析対象に含めます。
   - 特定の種類の機密データをバケットの機密スコアから除外または含めるには、[機密性] タブを選択します。[検出] テーブルで、除外または含める機密データタイプのチェックボックスを選択します。次に、[アクション] メニューで [スコアから除外] を選択してタイプを除外するか、[スコアに含める] を選択してタイプを含めます。

表の 機密データタイプ フィールドには、データを検出したマネージドデータ識別子の固有識別子 (ID)、またはデータを検出したカスタムデータ識別子の名前を指定します。マネージドデータ識別子の ID は、識別子が検出する機密データのタイプを表します。例えば、米国のパスポート番号の場合は USA_PASSPORT_NUMBER などです。各マネージドデータ識別子の詳細については、マネージドデータ識別子の使用を参照してください。

S3 バケットの機密スコアに影響する設定を変更した場合、Macie は直ちに関連する機密データ検出統計およびバケットに関するその他の情報の再計算と更新を開始します。

機密データ自動検出カバレッジの評価

アカウントまたは組織の機密データの自動検出が進むにつれて、Amazon Macie は、Amazon Simple Storage Service (Amazon S3) データ資産のカバレッジを評価およびモニタリングするのに役立つ統計と詳細を提供します。このデータを使用して、データ資産全体およびバケットインベントリ内の個々の S3 バケットについて、機密データ自動検出のステータスを確認できます。Macie が特定バケット内のオブジェクトを分析できなかった問題を特定することもできます。問題を修正すれば、その後の分析サイクルで Amazon S3 データのカバレッジを拡大できます。

カバレッジデータは、現在の の S3 汎用バケットの機密データ自動検出の現在のステータスのスナップショットを提供します AWS リージョン。お客様が組織の Macie 管理者である場合、これには、お客さまのメンバーアカウントが所有するバケットが含まれます。各バケットのデータには、Macie がバケット内のオブジェクトを分析しようとしたときに問題が発生したかどうかが示されます。問題が発生した場合、データには各問題の性質が示され、発生回数が示されるケースもあります。データは、機密データの自動検出が毎日進行するにつれて更新されます。Macie が毎日の分析サイクル中にバケット内の 1 つ以上のオブジェクトを分析または分析を試みる場合に、Macie はカバレッジやその他のデータを更新して結果を反映します。

特定のタイプの問題については、すべての S3 汎用バケットのデータを集約して確認し、オプションでドリルダウンして各バケットに関する追加の詳細を確認できます。例えば、カバレッジデータを使用すると、Macie がアカウントに対してアクセスすることを許可されていないバケットを迅速に特定できます。カバレッジデータには、発生したオブジェクトレベルの問題も報告されます。分類エラーと呼ばれるこれらの問題により、Macie はバケット内の特定のオブジェクトを分析できませんでした。例えば、オブジェクトが使用できなくなった AWS Key Management Service （ AWS KMS) キーで暗号化されているために、Macie がバケット内で分析できなかったオブジェクトの数を判断できます。

Amazon Macie コンソールを使用してカバレッジデータを確認する場合、データビューには各タイプの問題を修正するためのガイダンスも含まれます。このセクションの以降のトピックでは、各タイプの修正ガイダンスも提供します。

トピック

機密データ自動検出のカバレッジデータを確認

機密データ自動検出カバレッジを確認および評価するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。コンソールと API の両方が、現在の の Amazon Simple Storage Service (Amazon S3) 汎用バケットの分析の現在のステータスを示すデータを提供します AWS リージョン。データには、分析に差異が生じる問題に関する情報が含まれています。

- Macie がアクセスを許可されていないバケット。バケットの権限設定により Macie がバケットとバケットのオブジェクトにアクセスできないため、Macie はこれらのバケット内のオブジェクトを分析できません。
- 分類可能なオブジェクトを保存しないバケット。すべてのオブジェクトが Macie がサポートしていない Amazon S3 ストレージクラスを使用しているか、Macie がサポートしていないファイルまたはストレージ形式のファイル名拡張子が付いているため、Macie はこれらのバケット内のオブジェクトを分析できません。
- オブジェクトレベルの分類エラーが原因で Macie がまだ分析できなかったバケット。Macie は、これらのバケット内の 1 つ以上のオブジェクトを分析しようとしました。しかし、オブジェクトレベルのアクセス許可設定、オブジェクトコンテンツ、またはクォータに問題があったため、Macie はそのオブジェクトを分析できませんでした。

カバレッジデータは、機密データの自動検出が毎日進行するにつれて更新されます。ユーザーが組織の Macie 管理者である場合、データには、組織のメンバーアカウントによって所有されている S3 バケットの情報が含まれます。

> **Note**
>
> カバレッジデータには、作成して実行した機密データ検出ジョブの結果は明示的に含まれていません。ただし、機密データ自動検出結果に影響するカバレッジの問題を修正すると、その後に実行する機密データ検出ジョブのカバレッジも拡大する可能性があります。ジョブのカバレッジを評価するには、ジョブの統計と結果を確認。ジョブのログイベントやその他の結果がカバレッジ問題を示す場合は、このセクションの後半にある修正ガイダンスがいくつかの問題に対処するのに役立ちます。

機密データ自動検出のカバレッジデータを確認するには

アカウントまたは組織のカバレッジデータを確認するには、Amazon Macie コンソールまたは Amazon Macie API を使用します。コンソールでは、単一ページに、各バケットで最近発生した問題のロールアップなど、すべての S3 汎用バケットのカバレッジデータを統合して表示できます。このページには、問題タイプ別にデータグループを確認するオプションもあります。特定のバケットの問題調査を追跡するために、そのページからデータをカンマ区切り値 (CSV) ファイルにエクスポートできます。

Console

Amazon Macie コンソールを使用して機密データ自動検出カバレッジデータを確認するには、次のステップに従います。

カバレッジデータを確認する

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで **リソースカバレッジ** を選択します。
3. **リソースカバレッジ** ページで、確認したいカバレッジデータのタイプに対応するタブを選択します。
   - **すべて** — Macie がアカウントについてモニタリングおよび分析するすべてのバケットを一覧表示します。

各バケットの [問題] フィールドには、問題によって Macie がバケット内のオブジェクトを分析できなかったかどうかが示されます。このフィールドの値が なし の場合、Macie はバケットのオブジェクトを少なくとも 1 つ分析したか、または Macie がバケットのオブジェクト分析を試みていないことを意味します。問題がある場合、このフィールドに問題の性質と修正方法が表示されます。オブジェクトレベル分類エラーの場合、エラーの発生回数が (括弧内に) 表示されるケースもあります。

- アクセス拒否 — Macie がアクセスを許可されていないバケットを一覧表示します。これらのバケットの権限設定により、Macie はバケットとバケットのオブジェクトにアクセスできなくなります。そのため、Macie はこれらのバケット内のオブジェクトを分析できません。
- 分類エラー — オブジェクトレベルの分類エラーが原因で Macie がまだ分析していないバケットを一覧表示します。オブジェクトレベルのアクセス許可設定、オブジェクトコンテンツ、またはクォータに関する問題です。

  各バケットの [問題] フィールドには、発生して Macie がバケット内のオブジェクトを分析できなかった各タイプのエラーの性質が表示されます。また、各種エラーの修正方法も示します。エラーによっては、エラーの発生回数が (括弧内に) 表示される場合もあります。
- 分類不可 — 分類可能なオブジェクトを保存しないため Macie が分析できないバケットを一覧表示します。これらのバケット内のすべてのオブジェクトは、サポートされていない Amazon S3 ストレージクラスを使用しているか、サポートされていないファイルまたはストレージ形式のファイル名拡張子が付いています。そのため、Macie はこれらのバケット内のオブジェクトを分析できません。

4. バケットのサポートデータをドリルダウンして確認するには、バケットの名前を選択します。次に、バケットに関する統計およびその他の情報については、バケット詳細パネルを参照してください。
5. テーブルを CSV ファイルにエクスポートするには、ページ上部の [CSV にエクスポート] を選択します。結果の CSV ファイルには、最大 50,000 個のバケットについて、テーブル内の各バケットのメタデータのサブセットが含まれます。このファイルには [カバレッジ問題] フィールドが含まれています。このフィールドの値は、問題によって Macie がバケット内のオブジェクトを分析できなかったかどうか、もしできなかった場合は、その問題の性質を示します。

API

プログラムでカバレッジデータを確認するには、Amazon Macie API の DescribeBucketsオペレーションを使用して送信するクエリでフィルター条件を指定します。このオペレーションは、オブジェクトの配列を返します。各オブジェクトには、フィルター条件に一致する S3 汎用バケットに関する統計データとその他の情報が含まれています。

フィルター条件には、確認したいカバレッジデータのタイプに関する条件を含めます。

- バケットの権限設定により Macie がアクセスできないバケットを特定するには、`errorCode` のフィールドの値が `ACCESS_DENIED` に等しいという条件を含めます。
- Macie がアクセスを許可されていてまだ分析されていないバケットを特定するには、`sensitivityScore` のフィールドの値が `50` に等しく、`errorCode` のフィールドの値が `ACCESS_DENIED` に等しくないという条件を含めます。
- すべてのバケットのオブジェクトがサポートされていないストレージクラスまたは形式を使用しているために Macie が分析できないバケットを特定するには、`classifiableSizeInBytes` のフィールドの値が `0` に等しく、`sizeInBytes` のフィールドの値が `0` より大きいという条件を含めます。
- Macie が 1 つ以上のオブジェクトを分析したバケットを特定するには、`sensitivityScore` フィールドの値が 1 ~ 99 の範囲内にあるが、`50` に等しくないという条件を含めます。手動で最大スコアを割り当てたバケットも含めるには、範囲を 1 ~ 100 にする必要があります。
- オブジェクトレベルの分類エラーが原因で Macie がまだ分析していないバケットを特定するには、`sensitivityScore` のフィールドの値が `-1` に等しいという条件を含めます。次に、特定のバケットで発生したエラーのタイプと数の内訳を確認するには、 GetResourceProfileオペレーションを使用します。

AWS Command Line Interface (AWS CLI) を使用している場合は、describe-bucketsコマンドを実行して送信するクエリにフィルター条件を指定します。特定の S3 バケットで発生したエラーのタイプと数の内訳を確認するには、 get-resource-profile コマンドを実行します。

例えば、次の AWS CLI コマンドはフィルター条件を使用して、バケットのアクセス許可設定のために Macie がアクセスを許可されていないすべての S3 バケットの詳細を取得します。

この例は Linux、macOS、または Unix 用にフォーマットされています。

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

この例は Microsoft Windows 用にフォーマットされています。

```
C:\> aws macie2 describe-buckets --criteria={\"errorCode\":{\"eq\":[\"ACCESS_DENIED
\"]}}
```

リクエストが成功すると、Macie は buckets 配列を返します 配列には、現在の にあり AWS リージョン 、フィルター条件に一致する各 S3 バケットのオブジェクトが含まれます。

フィルター基準を満たす S3 バケットがない場合、Macie は空の buckets の配列を返します。

```
{
    "buckets": []
}
```

一般的な条件の例も含め、クエリでフィルター基準を指定する詳細については、S3 バケットインベントリをフィルタリングする を参照してください。

機密データ自動検出のカバレッジ問題を修正する

Amazon Macie は、Amazon Simple Storage Service (Amazon S3) データの機密データ自動検出カバレッジを低下させる問題のタイプをいくつか報告します。以下の情報は、これらの問題を調査して修正するのに役立ちます。

問題のタイプと詳細

- アクセスが拒否されました
- 分類エラー:コンテンツが無効です
- 分類エラー:暗号化が無効です
- 分類エラー:KMS キーが無効です
- 分類エラー:権限が拒否されました
- 分類不可

> **Tip**
>
> S3 バケットのオブジェクトレベル分類エラーを調査するには、まずバケットのオブジェクトサンプルリストを確認します。このリストには、Macie がバケット内で分析、または分析を試みたオブジェクト (最大 100 個) が表示されます。
> Amazon Macie コンソールでリストを確認するには、S3バケット ページでバケットを選択し、バケット詳細パネルの オブジェクトのサンプル タブを選択します。プログラムでリス

トを確認するには、Amazon Macie API の ListResourceProfileArtifacts オペレーションを使用します。オブジェクトの分析ステータスが SKIPPED スキップ済みの場合、そのオブジェクトがエラーの原因となっている可能性があります。

アクセスが拒否されました

この問題は、S3 バケットのアクセス許可設定により、Macie がバケットとバケットのオブジェクトにアクセスできなかったことを示します。Macie はバケット内のオブジェクトを取得、分析することはできません。

詳細

このタイプの問題の最も一般的な原因は、制限の厳しいバケットポリシーです。バケットポリシーは、プリンシパル AWS Identity and Access Management（ユーザー、アカウント、サービス、またはその他のエンティティ）が S3 バケットに対して実行できるアクションと、プリンシパルがそれらのアクションを実行できる条件を指定するリソースベースの (IAM) ポリシーです。制限付きバケットポリシーでは、特定の条件に基づいてバケットデータへのアクセスを許可または制限する明示的な `Allow` または `Deny` のステートメントを使用します。例えば、バケットポリシーには、特定のソース IP アドレスがバケットにアクセスするために使用されていない限り、バケットへのアクセスを拒否する `Allow` または `Deny` のステートメントが含まれる場合があります。

S3 バケットのバケットポリシーに 1 つ以上の条件を持つ明示的な `Deny` のステートメントがある場合、Macie は機密データ検出のためバケットオブジェクトを取得、分析することを許可されない場合があります。Macie は、バケット名や作成日など、バケットに関する情報のサブセットのみを提供できます。

修正ガイダンス

この問題を修正するには、S3 バケットのバケットポリシーを更新します。Macie がバケットとバケットのオブジェクトにアクセスすることをポリシーで許可されているか確認してください。このアクセスを許可するには、Macie サービスリンクロール`AWSServiceRoleForAmazonMacie`の条件をポリシーに追加します。その条件により、Macie サービスリンクロールがポリシーの `Deny` 制限と一致することを除外できます。これは、`aws:PrincipalArn` グローバル条件コンテキストキー および ユーザーアカウントの Macie サービスリンクロールの Amazon リソースネーム (ARN) を使用して行うことができます。

バケットポリシーを更新し、Macie が S3 バケットにアクセスできるようになると、Macie は変更を検出します。この場合、Macie は Amazon S3 データに関して提供する統計、インベントリ

データ、およびその他の情報を更新します。さらに、その後の分析サイクルでは、バケットのオブジェクトがより優先的に分析されます。

追加の参考資料

Macie がバケットにアクセスできるように S3 バケットポリシーを更新する詳細については、Amazon Macie が S3 バケットおよびオブジェクトにアクセスすることを許可する を参照してください。バケットポリシーを使用してバケットへのアクセス権を制御する詳細については、Amazon Simple Storage Service ユーザーガイドのバケットポリシーとユーザーポリシーとAmazon S3 がリクエストを許可する仕組みを参照してください。

分類エラー:コンテンツが無効です

このタイプの分類エラーは、Macie が S3 バケット内のオブジェクトを分析しようとして、そのオブジェクトの形式に誤りがあるか、オブジェクトに機密データ検出クォータを超えるコンテンツが含まれている場合に発生します。Macie はオブジェクトを分析できません。

詳細

このエラーは通常、S3 オブジェクトが誤った形式であるか、破損したファイルであることが原因で発生します。そのため、Macie はファイル内のすべてのデータを解析して分析することができません。

このエラーは、S3 オブジェクトの分析が個々のファイルの機密データ検出クォータを超える場合にも発生する可能性があります。例えば、オブジェクトのストレージサイズが、そのタイプのファイルのサイズクォータを超えている場合などです。

いずれの場合も、Macie は S3 オブジェクトの分析を完了できず、オブジェクトの分析ステータスは スキップ済みSKIPPEDになります。

修正ガイダンス

このエラーを調べるには、S3 オブジェクトをダウンロードし、ファイルの形式とコンテンツを確認します。また、ファイルのコンテンツを Macie の機密データ検出のクォータと比較して評価してください。

このエラーを修正しないと、Macie は S3 バケット内の他のオブジェクトの分析を試みようとします。Macie が別のオブジェクトを正常に分析すると、Macie はカバレッジデータやバケットに関して提供されるその他の情報を更新します。

追加の参考資料

特定のタイプのファイルに対するクォータを含む機密データ検出クォータのリストについては、Amazon Macie クォータ を参照してください。Macie が S3 バケットに関して提供される機密スコアやその他の情報を更新する方法については、機密データの自動検出の仕組み を参照してください。

分類エラー:暗号化が無効です

このタイプの分類エラーは、Macie が S3 バケット内のオブジェクトを分析しようとして、そのオブジェクトはお客様が用意したキーで暗号化されている場合に発生します。オブジェクトが SSE-C 暗号を使用しているため、Macie はそのオブジェクトを取得、分析することができません。

詳細

Amazon S3 は S3 オブジェクトの複数の暗号化オプションをサポートしています。これらのオプションのほとんどで、Macie は、ユーザーアカウントの Macie サービスリンクロールを使用してオブジェクトを復号化できます。ただし、これは使用された暗号化のタイプによって異なります。

Macie が S3 オブジェクトを復号化するには、Macie がアクセスして使用を許可されているキーを用いてオブジェクトが暗号化されている必要があります。お客様が用意したキーによりオブジェクトが暗号化されている場合、Macie は Amazon S3 からオブジェクトを取得するのに必要なキーマテリアルを提供できません。その結果、Macie はオブジェクトを分析できず、オブジェクトの分析ステータスはスキップ済みSKIPPEDになります。

修正ガイダンス

このエラーを修正するには、Amazon S3 マネージドキーまたは AWS Key Management Service (AWS KMS) キーを使用して S3 オブジェクトを暗号化します。 Amazon S3 AWS KMS キーを使用する場合は、キーは AWS マネージド KMS キー、または Macie が使用できるカスタマーマネージド KMS キーにすることができます。

Macie がアクセスして使用できるキーで既存の S3 オブジェクトを暗号化するには、オブジェクトの暗号化設定を変更します。Macie がアクセスして使用できるキーを使用して新しいオブジェクトを暗号化するには、S3 バケットのデフォルトの暗号化設定を変更します。また、バケットのポリシーで、新しいオブジェクトはお客様が用意したキーで暗号化するよう要求されていないことも確認してください。

このエラーを修正しないと、Macie は S3 バケット内の他のオブジェクトの分析を試みようとします。Macie が別のオブジェクトを正常に分析すると、Macie はカバレッジデータやバケットに関して提供されるその他の情報を更新します。

追加の参考資料

Macie を使用して暗号化された S3 オブジェクトを分析するための要件とオプションについては、を参照してくださいAmazon Macie を用いた暗号化された Amazon S3 オブジェクトの分析。デフォルトの暗号化設定の詳細については、Amazon Simple Storage Service ユーザーガイドの暗号化を使用したデータの保護およびS3 バケット向けのサーバー側のデフォルトの暗号化動作の設定を参照してください。

分類エラー:KMS キーが無効です

このタイプの分類エラーは、Macie が S3 バケット内のオブジェクトの分析を試み、そのオブジェクトが使用できなくなった AWS Key Management Service （ AWS KMS) キーで暗号化されている場合に発生します。Macie はオブジェクトを取得、分析することができません。

詳細

AWS KMS には、カスタマー管理の を無効化および削除するオプションが用意されています AWS KMS keys。S3 オブジェクトが無効、削除予定、または削除済みの KMS キーで暗号化されている場合、Macie はそのオブジェクトを取得および復号化できません。その結果、Macie はオブジェクトを分析できず、オブジェクトの分析ステータスはスキップ済みSKIPPEDになります。Macie が暗号化されたオブジェクトを分析するには、Macie がアクセスして使用を許可されているキーを用いてオブジェクトが暗号化されている必要があります。

修正ガイダンス

このエラーを修正するには、キーの最新ステータスに応じて該当する AWS KMS keyの予定削除を再度有効にするか、またはキャンセルします。該当するキーが既に削除されている場合、このエラーは修正できません。

どの AWS KMS key が S3 オブジェクトの暗号化に使用されたかを判断するには、まず Macie を使用して S3 バケットのサーバー側の暗号化設定を確認します。バケットのデフォルトの暗号化設定で KMS キーを使用するように設定されている場合は、バケット詳細に使用されているキーが表示されます。さらに、そのキーのステータスを確認できます。または、Amazon S3 を使用して、バケットとバケット内の個々のオブジェクトの暗号化設定を確認することもできます。

このエラーを修正しないと、Macie は S3 バケット内の他のオブジェクトの分析を試みようとします。Macie が別のオブジェクトを正常に分析すると、Macie はカバレッジデータやバケットに関して提供されるその他の情報を更新します。

追加の参考資料

Macie を使用して S3 バケットのサーバー側の暗号化設定を確認する詳細については、S3 バケットの詳細を確認する を参照してください。のスケジュールされた削除の再有効化またはキャンセルについては AWS KMS key、「 AWS Key Management Service デベロッパーガイド」の「キーの有効化と無効化」および「キーの削除のスケジュールとキャンセル」を参照してください。

分類エラー:権限が拒否されました

このタイプの分類エラーは、Macie が S3 バケット内のオブジェクトを分析しようとして、オブジェクトの権限設定またはオブジェクトの暗号化に使用されたキーの権限設定が原因でオブジェクトを取得または復号化できない場合に発生します。Macie はオブジェクトを取得、分析することができません。

詳細

このエラーは通常、S3 オブジェクトが Macie が使用を許可されていないカスタマーマネージド AWS Key Management Service AWS KMSキーで暗号化されていることが原因で発生します。オブジェクトがカスタマー管理の で暗号化されている場合 AWS KMS key、キーのポリシーは Macie がキーを使用してデータを復号することを許可する必要があります。

このエラーは、Amazon S3 のアクセス許可設定によって Macie が S3 オブジェクトを取得できない場合にも発生する可能性があります。S3 バケットポリシーでは、特定のバケットオブジェクトへのアクセスを制限したり、特定のプリンシパル (ユーザー、アカウント、サービス、またはその他のエンティティ) にのみオブジェクトへのアクセスを許可したりする場合があります。または、オブジェクトのアクセスコントロールリスト (ACL) により、オブジェクトへのアクセスが制限される場合があります。その結果、Macie はオブジェクトにアクセスできない場合があります。

上記のいずれの場合も、Macie はオブジェクトを取得、分析できず、オブジェクトの分析ステータスは スキップ済みSKIPPEDになります。

修正ガイダンス

このエラーを修正するには、S3 オブジェクトがカスタマーマネージド AWS KMS keyで暗号化されているかどうかを確認します。お客様が用意したもので暗号化されている場合は、キーポリ

シーで Macie サービスリンクロールAWSServiceRoleForAmazonMacieがそのキーを使用してデータを復号化することを許可していることを確認します。このアクセスを許可する方法は、 を所有するアカウントが、オブジェクトを保存する S3 バケット AWS KMS key も所有しているかどうかによって異なります。同じアカウントが KMS キーとバケットを所有している場合、アカウントのユーザーはキーのポリシーを更新する必要があります。1 つのアカウントが KMS キーを所有し、別のアカウントがバケットを所有している場合、そのキーを所有するアカウントのユーザーはキーへのクロスアカウントアクセスを許可する必要があります。

> **Tip**
>
> Macie AWS KMS keys がアカウントの S3 バケット内のオブジェクトを分析するためにアクセスする必要があるすべてのカスタマーマネージド のリストを自動的に生成できます。これを行うには、 の Amazon Macie Scripts リポジトリから入手できる AWS KMS Permission Analyzer スクリプトを実行します GitHub。 Amazon Macie このスクリプトは、 AWS Command Line Interface （ AWS CLI) コマンドの追加スクリプトを生成することもできます。必要に応じてこれらのコマンドを実行し、指定した KMS キーに必要な設定設定とポリシーを更新できます。

Macie が既に該当する の使用を許可されている場合、 AWS KMS key または S3 オブジェクトがカスタマーマネージド KMS キーで暗号化されていない場合は、バケットのポリシーで Macie がオブジェクトにアクセスすることを許可していることを確認してください。また、オブジェクトの ACL が Macie にオブジェクトのデータおよびメタデータの読み取りを許可していることも確認してください。

バケットポリシーでは、Macie のサービスリンクロールの条件をポリシーに追加することで、このアクセスを許可できます。その条件により、Macie サービスリンクロールがポリシーの Deny 制限と一致することを除外できます。これは、aws:PrincipalArn グローバル条件コンテキストキー および ユーザーアカウントの Macie サービスリンクロールの Amazon リソースネーム (ARN) を使用して行うことができます。

オブジェクト ACL の場合、オブジェクト所有者と協力して、オブジェクトに対するREADアクセス許可を持つ被付与者として を追加することで AWS アカウント 、このアクセスを許可できます。その後、Macie はアカウントのサービスリンクロールを使用してオブジェクトを取得、分析できます。また、バケットのオブジェクト所有権設定を変更することも検討してください。これらの設定により、バケット内のすべてのオブジェクトの ACL を無効にし、バケットを所有するアカウントに所有権の許可を与えることができます。

このエラーを修正しないと、Macie は S3 バケット内の他のオブジェクトの分析を試みようとします。Macie が別のオブジェクトを正常に分析すると、Macie はカバレッジデータやバケットに関して提供されるその他の情報を更新します。

追加の参考資料

Macie がカスタマーマネージド AWS KMS keyを使ってデータ復号化をできるようにする詳細については、Amazon Macie にカスタマーマネージド の使用を許可する AWS KMS key を参照してください。Macie がバケットにアクセスできるよう S3 バケットポリシーを更新する詳細については、Amazon Macie が S3 バケットおよびオブジェクトにアクセスすることを許可する を参照してください。

キーポリシー更新の詳細については、AWS Key Management Service デベロッパーガイドのキーポリシーの変更を参照してください。カスタマー管理の を使用して S3 オブジェクト AWS KMS keys を暗号化する方法については、「Amazon Simple Storage Service ユーザーガイド」の AWS KMS 「キーによるサーバー側の暗号化の使用」を参照してください。

バケットポリシーを使用して S3 バケットにアクセス権を制御する詳細については、Amazon Simple Storage Service ユーザーガイドのバケットポリシーとユーザーポリシーおよびAmazon S3 がリクエストを許可する仕組みを参照してください。ACL またはオブジェクト所有権設定を使用して S3 オブジェクトへのアクセスを制御する方法については、Amazon Simple Storage Service ユーザーガイドのACL によるアクセス管理およびオブジェクトの所有権の制御とバケットの ACL の無効化を参照してください。

分類不可

この問題は、S3 バケット内のすべてのオブジェクトが、サポートされていない Amazon S3 ストレージクラスまたはサポートされていないファイルまたはストレージ形式を使用して保存されていることを示しています。Macie はバケット内のどのオブジェクトも分析できません。

詳細

選択と分析の対象となるには、S3 オブジェクトが Macie がサポートする Amazon S3 ストレージクラスを使用する必要があります。オブジェクトには、Macie がサポートするファイルまたはストレージ形式のファイル名拡張子もまた必要です。オブジェクトがこれらの基準を満たさない場合、そのオブジェクトは分類不可能なオブジェクトとして扱われます。Macie は分類不可のオブジェクト内データに対して取得、分析の試みをしません。

S3 バケット内のオブジェクトがすべて分類不可の場合、そのバケット全体が分類できないバケットになります。Macie はバケットの機密データ自動検出を実行できません。

修正ガイダンス

この問題に対処するには、S3 バケットにオブジェクトを保存するためにどのストレージクラスを使用するかを決定するライフサイクル設定ルールやその他の設定を確認してください。Macie がサポートするストレージクラスを使用するようにこれらの設定を調整することを検討してください。バケット内の既存のオブジェクトのストレージクラスを変更することもできます。

S3 バケット内の既存のオブジェクトのファイルフォーマットとストレージフォーマットも評価します。オブジェクトを分析するため、サポートされている形式を使用する新しいオブジェクトに、一時的または永続的にデータを移植することを検討してください。

S3 バケットに追加されたオブジェクトが、サポートされているストレージクラスとフォーマットを使用している場合、Macie は次回バケットインベントリ評価時にオブジェクトを検出します。その場合、Macie は Amazon S3 データに関して提供する統計、カバレッジデータ、その他の情報において、バケットが分類不可という報告を停止します。さらに、次の分析サイクルで、新しいオブジェクトは分析優先度が高くなります。

追加の参考資料

Macie がサポートする Amazon S3 ストレージクラス、ファイル、ストレージ形式については、Amazon Macie でサポートされているストレージのクラスと形式 を参照してください。Amazon S3 が提供するライフサイクル設定ルールとストレージクラスオプションについては、Amazon Simple Storage Service ユーザーガイドのストレージライフサイクルの管理とAmazon S3 ストレージクラスの使用を参照してください。

機密データの自動検出の統計と結果の確認

機密データの自動検出が有効になっている場合、Amazon Macie は、アカウントでモニタリングおよび分析する Amazon Simple Storage Service (Amazon S3) 汎用バケットに関する追加のインベントリデータ、統計、およびその他の情報を自動的に生成して維持します。ユーザーが組織の Macie 管理者である場合、デフォルトでは、メンバーアカウントが所有する S3 バケットが含まれます。

追加情報は、Macie がこれまでに実行した機密データ自動検出アクティビティの結果をキャプチャします。また、Macie が提供する Amazon S3 データに関するその他の情報 (パブリックアクセスや個々の S3 バケットの暗号化設定など) を補足するものでもあります。メタデータと統計に加えて、Macie は検出した機密データと、機密データの検出結果 という機密データの検出結果である、実行した分析のレコードを生成します。

機密データの自動検出が毎日進行するにつれて、以下の機能とデータが結果の確認と評価に役立ちます。

- 概要ダッシュボード - Amazon S3データエステートの集計された統計情報を提供します。統計には、Macie が機密データを検出したバケットの総数や、それらのうちパブリックアクセスが可能であるものの数など、主要なメトリクスのデータが含まれます。また、Amazon S3 データのカバレッジに影響する問題も報告します。
- S3 バケットヒートマップ — データ資産全体のデータ機密性を AWS アカウントによりグループ化してインタラクティブに視覚的に表します。マップにはアカウントごとに集約された機密性統計が含まれ、アカウントが所有する各バケットの現在の機密性スコアが色で示されています。また、マップではシンボルを使用して、一般にアクセス可能なバケット、Macie では分析できないバケットなどを識別できます。
- S3 バケットテーブル — インベントリ内の各 S3 バケットの概要情報を提供します。テーブルには、バケットごとに、バケットの現在の機密性スコア、Macie がバケット内で分析できるオブジェクトの数、バケット内のオブジェクトを定期的に分析するように機密データ検出ジョブを設定しているかどうかなどのデータが含まれます。テーブルからカンマ区切り値 (CSV) ファイルにデータをエクスポートできます。
- 詳細パネル — ヒートマップまたはテーブルで選択した S3 バケットの詳細と統計が表示されます。詳細には、Macie がバケット内で分析したオブジェクトのリスト、Macie がバケット内で検出した機密データのタイプと出現回数の内訳が含まれます。パネルを使用して、バケットの自動検出設定を管理することもできます。
- 機密データ調査結果 — Macie が個々の S3 オブジェクト内で検出した機密データの詳細なレポートを提供します。詳細には、Macie が機密データをいつ見つけたか、また Macie が見つけた機密データのタイプと出現回数が含まれます。詳細には、バケットのパブリックアクセス設定やオブジェクトの最新の変更日など、影響を受けた S3 バケットとオブジェクトに関する情報も含まれます。
- 機密データの検出結果 – Macie が個々の S3 オブジェクトに対して実行した分析の記録を提供します。これには、Macie が機密データを見つけられないオブジェクトや、問題や エラーのために Macie が分析できないオブジェクトが含まれます。Macie がオブジェクト内で機密データを検出すると、機密データの検出結果は Macie が検出した機密データに関する情報を提供します。

このデータを使用して、Amazon S3 データ資産全体のデータ機密性を評価し、ドリルダウンして個々の S3 バケットとオブジェクトを評価および調査できます。Macie が提供する Amazon S3 データのセキュリティとプライバシーに関する情報と組み合わせることで、即時の修復が必要なケースを特定することもできます。たとえば、Macie が機密データを発見したパブリックにアクセス可能なバケットなどです。

追加データは、Amazon S3 データ資産のカバレッジの評価とモニタリングに役立ちます。カバレッジデータを使用すると、データ資産全体とバケットインベントリ内の個々の S3 バケットの分析ス

テータスを確認できます。Macie が特定バケット内のオブジェクトを分析できなかった問題を特定することもできます。問題を修正すれば、その後の分析サイクルで Amazon S3 データのカバレッジを拡大できます。詳細については、機密データ自動検出カバレッジの評価を参照してください。

トピック

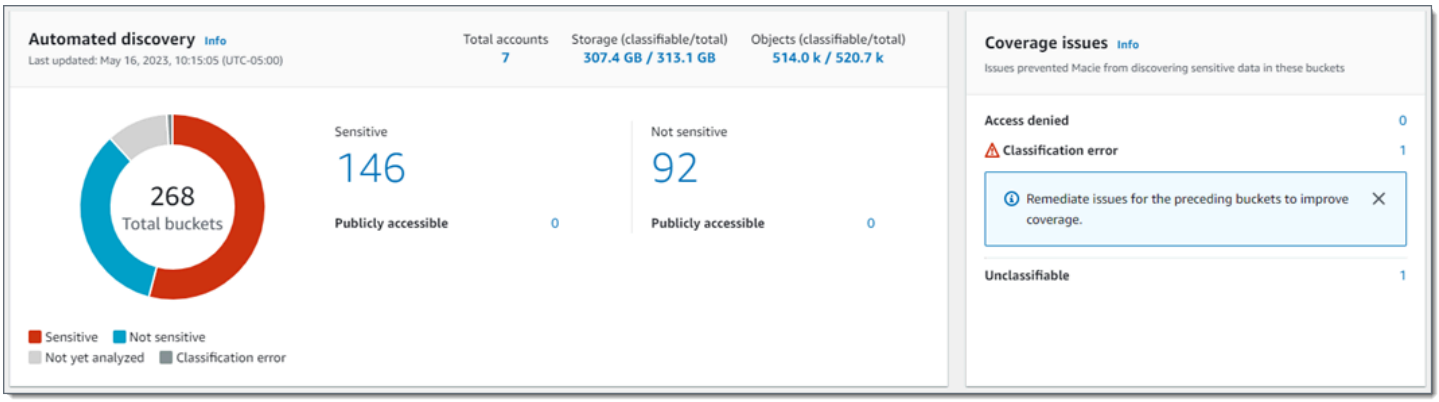
- 概要ダッシュボードの集約されたデータ機密性統計を確認する
- S3 バケットマップによるデータ機密性の視覚化
- S3 バケットテーブルによるデータ機密性の評価
- 個々の S3 バケットのデータ機密情報の確認
- 自動検出によって生成された機密データ調査結果の分析
- 自動検出によって生成された機密データの検出結果へのアクセス

概要ダッシュボードの集約されたデータ機密性統計を確認する

Amazon Macie コンソールで、概要ダッシュボードには、現在の AWS リージョンでの Amazon S3 データの集約された統計と調査結果データのスナップショットが表示されます。Amazon S3 データの全体的なセキュリティ体制を評価するのに役立つように設計されています。

ダッシュボード統計には、パブリックにアクセス可能または他の と共有されている S3 汎用バケットの数など、主要なセキュリティメトリクスのデータが含まれます AWS アカウント。ダッシュボードには、過去 7 日間に最も多くの検出結果を生成したバケットなど、アカウントの集計された検出結果データのグループも表示されます。ユーザーが組織の Macie 管理者である場合、ダッシュボードには、組織内のすべてのアカウントの集約された統計とデータが提供されます。オプションで、アカウント別にデータをフィルタリングすることができます。

機密データの自動検出が有効になっている場合、概要ダッシュボードには自動検出統計が含まれます。統計には、Macie がこれまで Amazon S3 データに対して実行した機密データ自動検出アクティビティのステータスと結果が記録されます。例:



「自動検出」セクションの統計は、機密データ自動検出アクティビティの現在のステータスと結果のスナップショットを提供します。データには、作成して実行した機密データ検出ジョブの結果は含まれません。

[カバレッジ問題]セクションの統計は、問題によって Macie が個々の S3 バケット内のオブジェクトを分析できなくなるかどうかを示しています。これらの統計には、作成して実行した機密データ検出ジョブのデータが明示的に含まれていません。ただし、機密データの自動検出結果に影響するカバレッジの問題を修正すると、後で実行するジョブのカバレッジも向上する可能性があります。

トピック

- 概要ダッシュボードを表示する
- 概要ダッシュボードの自動機密データ検出統計について

概要ダッシュボードを表示する

Amazon Macie コンソールに[概要] ダッシュボードを表示するには、次のステップに従います。プログラムで統計をクエリする場合は、Amazon Macie API の GetBucketStatisticsオペレーションを使用できます。

サマリーダッシュボードを表示するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 概要を選択します。Macie は 概要ダッシュボードを表示します。
3. ダッシュボードの項目をドリルダウンして、その項目のサポートデータを確認するには、その項目を選択します。

ユーザーが組織の Macie 管理者である場合、ダッシュボードには、自分のアカウントと組織内のメンバーアカウントの集約された統計とデータが表示されます。ダッシュボードをフィルタリングし、特定のアカウントのデータのみを表示するには、ダッシュボードの上の アカウントボックスにアカウント ID を入力します。

概要ダッシュボードの自動機密データ検出統計について

Amazon Macie コンソールの [概要]ダッシュボードには、Amazon S3 データの機密データの自動検出をモニタリングするのに役立つ集計統計が含まれています。現在の の Amazon S3 データの現在のステータスと分析結果のスナップショットを提供します AWS リージョン。

たとえば、ダッシュボードの統計情報を使用して、Amazon Macie が機密データを見つけた S3 バケットの数や、それらのうちパブリックアクセスが可能であるものの数をすばやく判断できます。Amazon S3 データのカバレッジを評価し、Macie が個々の S3 バケット内のオブジェクトを分析できない問題を特定することもできます。

ダッシュボードでは、機密データの自動検出統計は主に以下のセクションに分かれています。

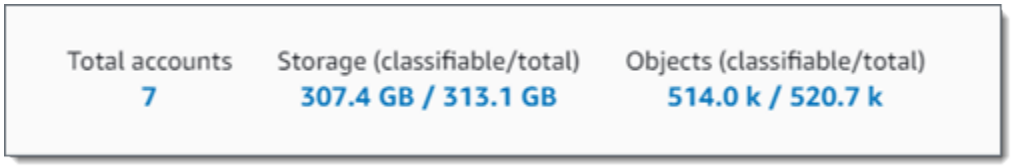
- ストレージと機密データ検出
- 自動検出
- カバレッジ問題

各セクションを確認するときに、オプションで項目を選択してドリルダウンし、サポートデータを確認します。また、ダッシュボードには S3 ディレクトリバケットのデータが含まれず、汎用バケットのみが含まれることに注意してください。Macie はディレクトリバケットをモニタリングまたは分析しません。

各セクションの個別統計は以下の通りです。[概要]ダッシュボードの他のセクションの統計情報については、概要ダッシュボードのコンポーネントを理解する を参照してください。

ストレージと機密データ検出

Automated discoveryセクションの上部には、Amazon S3に保存しているデータの量と、Macieが機密データを検出するために分析できるデータの量を示す統計が表示されます。例:



このセクションの内容:

- アカウントの合計 — バケットインベントリ内のバケットを所有 AWS アカウント する の合計数。ユーザーが組織の Macie 管理者である場合、これはそのユーザーが組織のために管理している Macie アカウントの総数です。スタンドアロンの Macie アカウントをお持ちの場合、この値は 1 です。
- ストレージ — これらのメトリクスは、バケットインベントリ内のオブジェクトのストレージサイズに関する情報を提供します。
  - 分類可能 – バケット内で Macie が分析できるすべてのオブジェクトの合計ストレージサイズ。

- 合計— Macie が分析できないオブジェクトを含む、バケット内のすべてのオブジェクトの合計ストレージサイズ。

いずれかのオブジェクトが圧縮ファイルである場合、これらの値は解凍後のファイルの実際のサイズを反映しません。いずれかのバケットでバージョニングが有効化されている場合、これらの値は、それらのバケット内の各オブジェクトの最新バージョンのストレージサイズに基づきます。

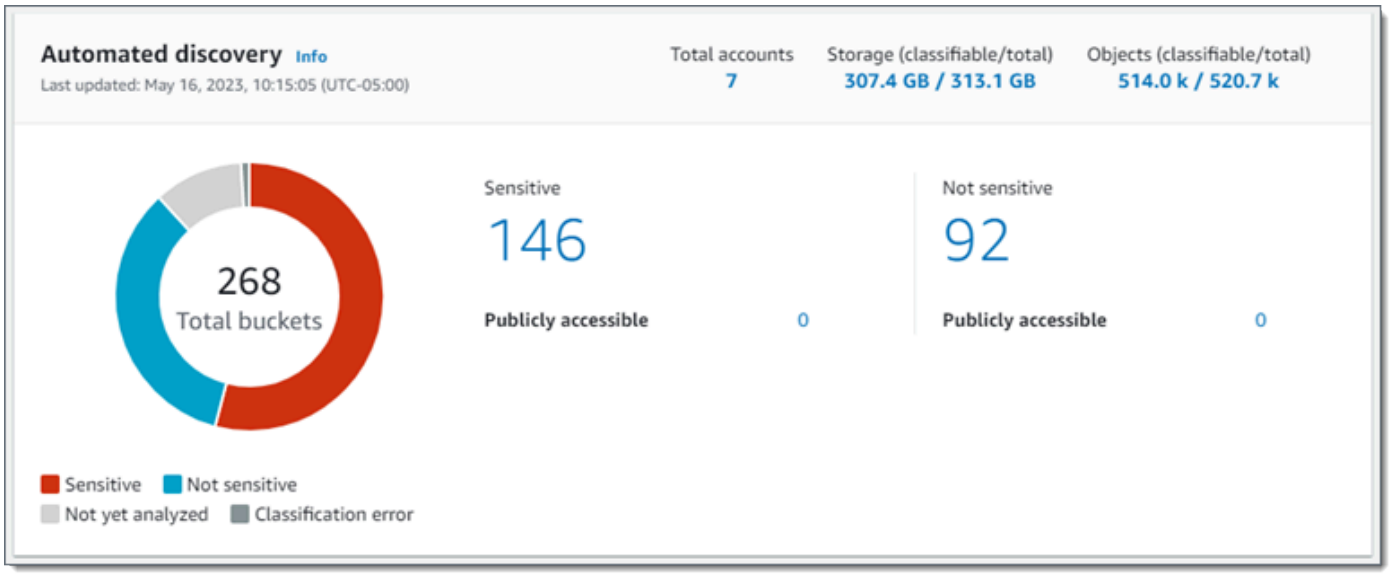
- オブジェクト — これらのメトリクスは、バケットインベントリ内のオブジェクト数に関する情報を提供します。
  - 分類可能 - バケット内で Macie が分析できるオブジェクトの合計数。
  - 合計— Macie が分析できないオブジェクトを含む、バケット内のオブジェクトの総数。

前述の統計では、データとオブジェクトは、サポートされているAmazon S3ストレージクラスを使用し、サポートされているファイルまたはストレージフォーマットのファイル名拡張子を持っている場合、分類可能です。Macie を使用して、オブジェクト内の機密データを検出できます。詳細については、サポートされているストレージクラスとフォーマットを参照してください。

ストレージ と オブジェクト の統計には、Macie がアクセスするのを許可されていないバケット内のオブジェクトに関するデータは含まれないことに注意してください。このようなケースを特定するには、ダッシュボードの [カバレッジ問題] セクションにある [アクセス拒否] 統計を選択します。

自動検出

これらの統計は主に、Macie がこれまで Amazon S3 データに対して実行した自動機密データ検出アクティビティのステータスと結果をキャプチャします。例:



このセクションの個々の統計は以下のとおりです。

バケットの総数

ドーナツグラフは、バケットインベントリ内のバケットの総数を示します。このグラフは、各バケットの現在の機密性スコアに基づいてバケットをカテゴリ別に次のようにグループ化します。

- 高機密性 (赤) — 機密性スコアが51～100の範囲にあるバケットの総数。
- 低機密性 (青) — 機密性スコアが1～49の範囲にあるバケットの総数。
- 分析が未完了 (ライトグレー) — 機密性スコアが50のバケットの総数。
- 分類エラー (濃い灰色) — 機密性スコアが-1のバケットの総数

Macie が定義する機密性スコアとラベルの範囲の詳細については、S3 バケットの機密スコアを参照してください。

グループのその他の統計情報を確認するには、そのグループにカーソルを合わせます。

- バケット — アカウント内のバケットの総数。
- パブリックアクセス可能 — 一般ユーザーがバケットへの読み取りまたは書き込みアクセス権を持つことを許可するバケットの数とパーセンテージ。
- 分類可能 – バケット内で Macie が分析できるすべてのオブジェクトの合計ストレージサイズ。これらのオブジェクトは、サポートされているAmazon S3ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を持っています。詳細については、サポートされているストレージクラスとフォーマットを参照してください。
- 合計バイト数 — すべてのバケットの合計ストレージサイズ。

前述の統計では、ストレージサイズの値は、バケット内の各オブジェクトの最新バージョンのストレージサイズに基づきます。いずれかのオブジェクトが圧縮ファイルである場合、これらの値は解凍後のファイルの実際のサイズを反映しません。

機密性

この領域は、現在機密性スコアが 51～100 の範囲にあるバケットの総数を示します。このグループ内の パブリックアクセス可能は、一般ユーザーもバケットへの読み取りまたは書き込みアクセス権を持つことが許可されるバケットの総数を示します。

非機密

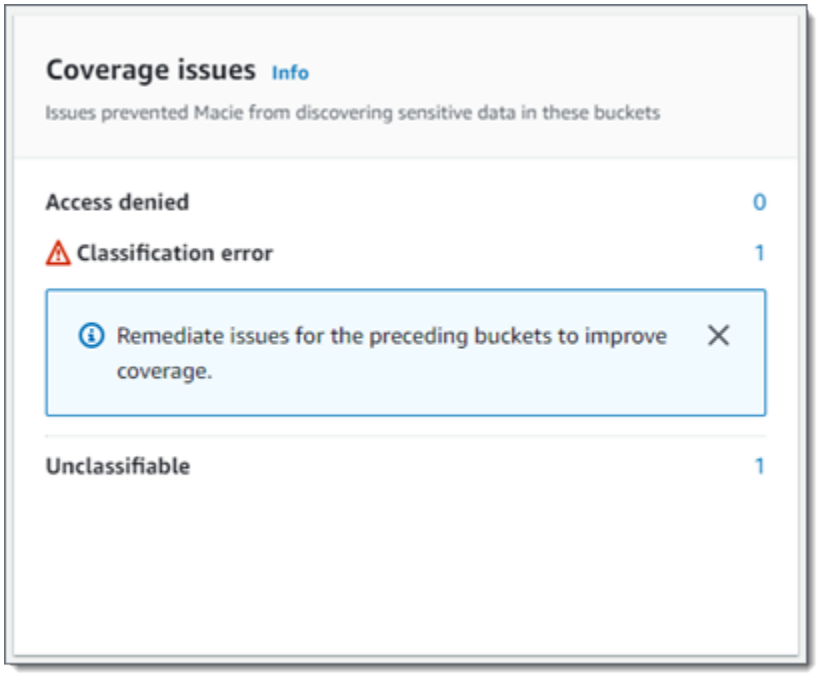
この領域は、現在機密性スコアが 1～49 の範囲にあるバケットの総数を示します。このグループ内の [パブリックアクセス可能]は、一般ユーザーもバケットへの読み取りまたは書き込みアクセス権を持つことが許可されるバケットの総数を示します。

[パブリックアクセス可能]統計の値を決定および計算するために、Macie はアカウントとバケットのパブリックアクセスをブロックする設定や、バケットのバケットポリシーなど、各バケットのアカウントレベルとバケットレベルの設定を組み合わせて分析します。詳細については、「Macie が Amazon S3 データセキュリティをモニタリングする方法」を参照してください。

自動検出セクションの統計には、作成して実行した機密データ検出ジョブの結果が含まれないことに注意してください。

カバレッジ問題

これらの統計は、特定のタイプの問題によって Macie が個々の S3 バケット内のオブジェクトを分析できなくなるかどうかを示しています。例:



このセクションの内容:

- アクセス拒否 — Macie がアクセスを許可されていないバケットの総数。Macie はこれらのバケット内のオブジェクトを一切分析できません。バケットのアクセス許可設定により、Macie はバケットとバケットのオブジェクトにアクセスできなくなります。
- 分類エラー — オブジェクトレベルの分類エラーにより Macie がまだ分析していないバケットの総数。Macie は、これらのバケット内の 1 つ以上のオブジェクトを分析しようとしました。

しかし、オブジェクトレベルのアクセス許可設定、オブジェクトコンテンツ、またはクォータに問題があったため、Macie はそのオブジェクトを分析できませんでした。

- 分類不可 — 分類可能なオブジェクトを一切保存していないバケットの総数です。Macie はこれらのバケット内のオブジェクトを一切分析できません。すべてのオブジェクトは、Macie がサポートしていない Amazon S3 ストレージクラスを使用しているか、Macie がサポートしていないファイルまたはストレージ形式のファイル名拡張子が付いています。

統計の値を選択すると、追加の詳細と、該当する場合修復ガイダンスが表示されます。アクセスの問題や分類エラーを修正すれば、その後の分析サイクルで Amazon S3 データのカバレッジを拡大できます。詳細については、「機密データ自動検出カバレッジの評価」を参照してください。

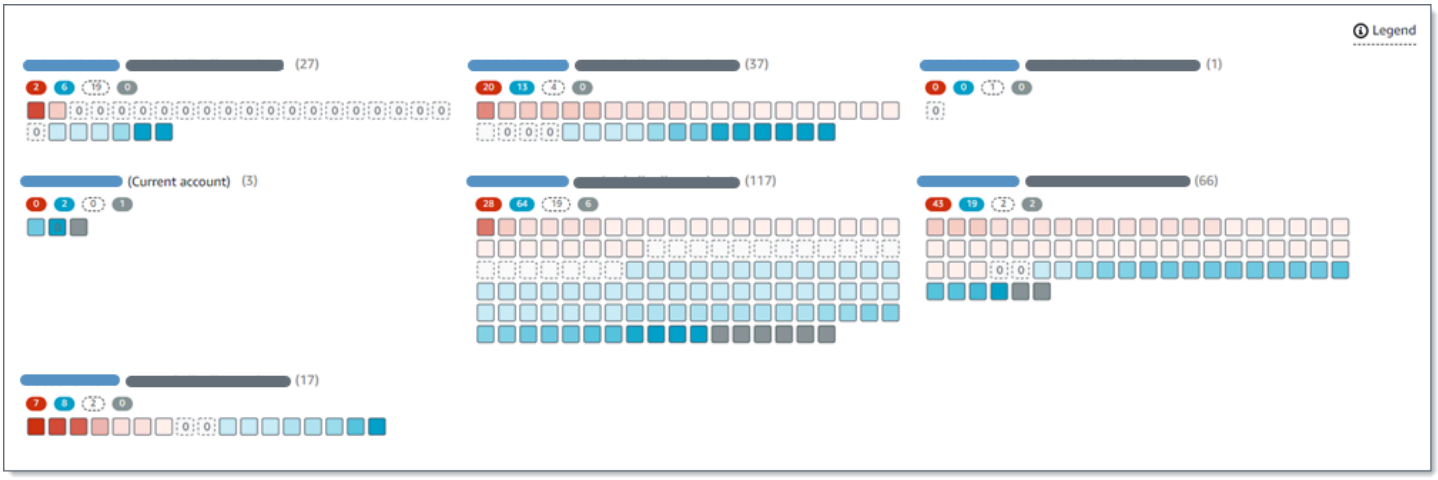
カバレッジ問題セクションの統計には、作成して実行した機密データ検出ジョブのデータが明示的に含まれていないことに注意してください。ただし、機密データの自動検出結果に影響するカバレッジの問題を修正すると、後で実行するジョブのカバレッジも向上する可能性があります。

[概要] ダッシュボードの他のセクションについては、概要ダッシュボードのコンポーネントを理解する を参照してください。

S3 バケットマップによるデータ機密性の視覚化

Amazon Macie コンソールでは、S3 バケットのヒートマップにより、Amazon Simple Storage Service (Amazon S3) データ資産全体のデータ機密性をインタラクティブに視覚的に表現できます。Macie が現在の の Amazon S3 データに対してこれまでに実行した機密データ自動検出アクティビティの結果をキャプチャします AWS リージョン。

ユーザーが組織の Macie 管理者である場合、マップにはメンバーアカウントが所有する S3 バケットの結果が含まれます。データは でグループ化され AWS アカウント 、アカウント ID でソートされます。例:



マップの各ページには、組織または Amazon S3 のデータ資産の規模に応じて、最大 99 のアカウントまたは 1,000 のバケットのデータが表示されます。

コンソールの左側のナビゲーションペインで、S3 バケット を選択します。ページの上部で、名前の変更を選択します。マップは、アカウントまたは組織で機密データの自動検出が現在有効になっている場合にのみ使用できます。作成して実行した機密データ検出ジョブの結果は含まれません。

トピック

- S3 バケットマップ内のデータの解釈
- S3 バケットマップを操作する

S3 バケットマップ内のデータの解釈

S3 バケットマップでは、各四角形はバケットインベントリ内の S3 汎用バケットを表します。四角の色はバケットの現在の機密性スコアを表します。これは、Macie がバケット内で見つけた機密データの量と Macie がバケット内で分析したデータの量という 2 つの主要な指標の共通点を測定します。色相の濃さは、次の図に示すように、バケットのスコアがデータ機密性値の範囲内のどの部分に当てはまるかを表しています。

一般に、色と色相の濃さは次のように解釈できます。

- 青 — バケットの現在の機密性スコアが 1 ~ 49 の範囲であれば、バケットの四角形は青で、バケットの機密性ラベルは [低機密性] です。青の色相の濃さは、バケット内の一意のオブジェクトの総数に関連して、Macie がバケット内で分析した一意のオブジェクトの数を反映しています。色相が濃いほど、機密性スコアが低くなります。
- 色なし — バケットの現在の機密性スコアが 50 の場合、バケットの四角形は色付けされず、バケットの機密性ラベルは分析が未完了 です。さらに、四角形には破線が付いています。
- 赤 — バケットの現在の機密性スコアが51 ~ 100の場合、バケットの四角形は赤で、バケットの機密性ラベルは[高機密性] です。赤の色相の濃さは、Macie がバケット内で検出した機密データの量を反映しています。色相が暗いほど、機密性スコアが高いことを示します。
- グレー — バケットの現在の機密性スコアが -1 の場合、バケットの四角形は濃い灰色で、バケットの機密性ラベルは [分類エラー] です。色相の濃さは変化しません。

Macie が定義する機密性スコアとラベルの範囲の詳細については、S3 バケットの機密スコア を参照してください。

マップでは、S3 バケットの四角形にはシンボルも含まれている場合があります。このシンボルはエラー、問題、またはバケットの機密性の評価に影響する可能性のあるその他の考慮事項を示しています。シンボルは、バケットがパブリックアクセス可能であるといった、バケットのセキュリティに関する潜在的な問題を示す場合もあります。次の表は、Macie がこれらのケースを通知するために使用する記号の一覧です。

記号	定義	説明
	アクセスが拒否されました	Macie はバケットやバケットのオブジェクトにアクセスすることが許可されていません。そのため、Macie はバケット内のオブジェクトを分析できません。 この問題は通常、バケットに制限があるバケットポリシーが設定されているために発生します。この問題の対処方法については、Macie が S3 バケットおよびオブジェクトに

記号	定義	説明
		アクセスすることを許可する を参照してください。
	パブリックアクセス可能	一般ユーザーは、バケットへの読み取りまたは書き込みのアクセス権を持っています。 この決定を行うために、Macie はアカウントとバケットのパブリックアクセスをブロックする設定や、バケットのバケットポリシーなど、各バケットのアカウントレベルとバケットレベルの設定を組み合わせて分析します。詳細については、「Macie が Amazon S3 データセキュリティをモニタリングする方法」を参照してください。

記号	定義	説明
?	分類不可	Macie はバケット内のどのオブジェクトも分析できません。バケットのすべてのオブジェクトには、Macie がサポートしていない Amazon S3 ストレージクラスが使用されているか、Macie がサポートしていないファイルまたはストレージ形式のファイル名拡張子が付いています。 Macie がオブジェクトを分析するには、オブジェクトはサポートされているストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を有している必要があります。詳細については、「サポートされているストレージクラスとフォーマット」を参照してください。
0	0 バイト	バケットには、Macie が分析するオブジェクトは保存されません。バケットが空か、バケット内のすべてのオブジェクトにゼロ (0) バイトのデータが含まれています。

S3 バケットマップを操作する

S3 バケット マップを確認すると、さまざまな方法でマップを操作して、個々のアカウントやバケットの追加データや詳細を確認したり評価したりできます。Amazon Macie コンソールにマップを表示し、そのマップが提供するさまざまな機能を使用するには、次の手順に従います。

S3 バケットマップを操作するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで、S3 バケットを選択します。S3 バケットには、バケットインベントリのマップが表示されます。ページにインベントリが表形式で表示されている場合は、ページ上部の map  を選択します。

   デフォルトでは、マップには、現在機密データの自動検出から除外されているバケットのデータが表示されません。ユーザーが組織の Macie 管理者である場合、機密データの自動検出が現在無効になっているアカウントのデータも表示されません。このデータを表示するには、フィルターボックスの下にある自動検出フィルタートークンによってモニタリングされる で X を選択します。
3. ページの上部で、必要に応じて、更新  を選択して、Amazon S3 から最新のバケットメタデータを取得します。
4. S3 バケット マップで、次のいずれかを実行します。

   - 特定の機密ラベルを持つバケットの数を確認するには、 AWS アカウント ID のすぐ下にある色付きのバッジを参照してください。バッジには、機密性ラベル別に分類された集計されたバケット数が表示されます。

     たとえば、赤のバッジは、アカウントが所有しており[高機密性] ラベルが付いているバケットの総数を示しています。これらのバケットの機密性スコアは 51 ~ 100 の範囲です。青のバッジは、そのアカウントが所有していて、低機密性 というラベルが付いたバケットの総数を示しています。これらのバケットの機密性スコアは 1 ~ 49 の範囲です。
   - バケットに関する情報のサブセットを確認するには、バケットの四角形にカーソルを合わせます。ポップオーバーにはバケットの名前と現在の機密性スコアが表示されます。

     ポップオーバーには、Macie がバケット内で分析できるオブジェクトの総数と、それらのオブジェクトの最新バージョンの合計ストレージサイズも表示されます。これらのオブジェクトは分類可能です。サポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子が付いています。詳細については、サポートされているストレージクラスとフォーマットを参照してください。
   - マップをフィルタリングし、フィールドに対して特定の値を持つバケットのみを表示するには、フィルターボックスにカーソルを置き、フィールドでフィルター条件を追加しま

す。Macie は条件の基準を適用し、フィルターボックスの下に条件を表示します。結果をさらに絞り込むには、追加のフィールドでフィルター条件を追加します。詳細については、S3 バケットインベントリをフィルタリングするを参照してください。

- 特定のアカウントが所有するバケットだけをドリルダウンして表示するには、そのアカウントのアカウント ID を選択します。Macie は、そのアカウントのみのデータをフィルタリングして表示する新しいタブを開きます。

5. 特定のバケットのすべての機密データ検出統計およびその他の情報を確認するには、バケットの四角形を選択し、詳細パネルを参照してください。その詳細については、「個々の S3 バケットのデータ機密情報の確認」を参照してください。

> **Tip**
>
> 詳細パネルでは、多くのフィールドをピボットしてドリルダウンできます。フィールドに対して同じ値を持つバケットを表示するには、フィールドで
>
> 
>
> を選択します。フィールドに対して他の値を持つバケットを表示するには、フィールドで
>
> 
>
> を選択します。

S3 バケットテーブルによるデータ機密性の評価

Amazon Macie コンソールでは、S3 バケットテーブルに、現在の の各 Amazon Simple Storage Service (Amazon S3) 汎用バケットに関する概要情報が表示されます AWS リージョン。ユーザーが組織の Macie 管理者である場合、これにはメンバーアカウントが所有するバケットに関する情報が含まれます。プログラムでデータにアクセスする場合は、Amazon Macie API の DescribeBucketsオペレーションを使用できます。

コンソールで、テーブルを並べ替えてフィルタリングし、てビューをカスタマイズできます。テーブルからカンマ区切り値 (CSV) ファイルにデータを エクスポートすることもできます。テーブルで S3 バケットを選択すると、詳細パネルにバケットに関する追加情報が表示されます。これには、バケットのデータのセキュリティとプライバシーに関する洞察を提供する設定とメトリクスの詳細と統計が含まれます。自動機密データ検出が有効になっている場合、Macie がこれまでにバケットに対して実行した自動検出アクティビティの結果をキャプチャするデータも含まれます。これらの詳細を確認するだけでなく、パネルを使用してバケットの自動検出設定を調整できます。この方法の詳細は、個々の S3 バケットの機密データ自動検出の管理を参照してください。

S3 バケットテーブルを使用してデータの機密性を評価するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで、S3 バケットを選択します。S3 バケットページにはバケットインベントリが表示されます。

   デフォルトでは、このページには、現在機密データの自動検出から除外されているバケットのデータが表示されません。ユーザーが組織の Macie 管理者である場合、機密データの自動検出が現在無効になっているアカウントのデータも表示されません。このデータを表示するには、フィルターボックスの下にある自動検出フィルタートークンによってモニタリングされる で X を選択します。
3. ページの上部にあるテーブル
   ()
   を選択します。S3 バケットページが開き、インベントリ内のバケットの数とバケットのテーブルが表示されます。
4. Amazon S3 から最新のバケットメタデータを取得するには、ページの上部の [refresh] (更新)
   ()
   を選択します。

   情報アイコン  が
   バケット名の横に表示された場合、これを行うことをお勧めします。このアイコンは、Macie が毎日の更新サイクル の一部として Amazon S3 からバケットとオブジェクトメタデータをおそらく最後に取得した後の過去 24 時間にバケットが作成されたことを示します。
5. S3 バケット ページで、テーブルを使用して、インベントリ内の各バケットに関する情報のサブセットを確認します。

   - 機密性 — バケットの現在の機密性スコア。Macie が定義する機密性スコアの範囲については、S3 バケットの機密スコアを参照してください。
   - バケット — バケットの名前。
   - Account – バケットを所有 AWS アカウント する のアカウント ID。
   - 分類可能なオブジェクト– バケット内の機密データを検出するために Macie が分析できるオブジェクトの総数。
   - 分類可能なサイズ – バケット内の機密データを検出するために Macie が分析できるすべてのオブジェクトの合計ストレージサイズ。

この値は、圧縮解除後の圧縮オブジェクトの実際のサイズを反映していません。また、バケットでバージョニングが有効化されている場合、この値は、バケット内の各オブジェクトの最新バージョンのストレージサイズに基づきます。

- ジョブによるモニタリング- 機密データ検出ジョブがバケット内のオブジェクトを毎日、毎週、または毎月ベースで定期的に分析するように設定されているかどうか。

  このフィールドの値が はいの場合、バケットが定期的なジョブに明示的に含まれるか、バケットが過去 24 時間以内の定期的なジョブの基準に一致したことになります。さらに、それらのジョブの少なくとも 1 つのステータスは キャンセルされません。Macie は毎日ベースでこのデータを更新します。

- 最新のジョブ実行 — バケット内のオブジェクトを分析するように 1 回限りまたは定期的な機密データ検出ジョブが設定されている場合、このフィールドには、それらのジョブのいずれかの実行が開始された最新の日時が表示されます。それ以外の場合は、このフィールドにダッシュ (–) が表示されます。

前述のデータでは、オブジェクトは、サポートされているAmazon S3のストレージクラスを使用し、サポートされているファイルまたはストレージフォーマットのファイル名拡張子を持っていれば、分類可能です。Macie を使用して、オブジェクト内の機密データを検出できます。詳細については、サポートされているストレージクラスとフォーマットを参照してください。

6. テーブルを使用してインベントリを分析するには、次のいずれかの操作を行います。

- 特定のフィールドでテーブルをソートするには、フィールドの列見出しを選択します。ソート順序を変更するには、列見出しを再度選択します。
- テーブルをフィルタリングし、フィールドに対して特定の値を持つバケットのみを表示するには、フィルターバーにカーソルを置き、フィールドでフィルター条件を追加します。Macie は条件の基準を適用し、フィルターボックスの下に条件を表示します。結果をさらに絞り込むには、追加のフィールドでフィルター条件を追加します。詳細については、「S3 バケットインベントリをフィルタリングする」を参照してください。
- 特定のバケットの機密データ検出統計やその他の情報を確認するには、テーブルでバケットの名前を選択し、詳細パネルを参照します。その詳細については、「S3 バケットの詳細の確認」を参照してください。

> **Tip**
>
> 詳細パネルでは、多くのフィールドをピボットしてドリルダウンできます。フィールドに対して同じ値を持つバケットを表示するには、フィールドで


を選択します。フィールドに対して他の値を持つバケットを表示するには、フィールドで

を選択します。

7. テーブルから CSV ファイルにデータをエクスポートするには、エクスポートする各行のチェックボックスを選択するか、選択列見出しのチェックボックスを選択してすべての行を選択します。次に、ページ上部の CSV にエクスポートを選択します。テーブルから最大 50,000 行をエクスポートできます。
8. 1 つ以上のバケット内のオブジェクトをより詳細かつ迅速に分析するには、各バケットのチェックボックスを選択し、[ジョブを作成] を選択します。詳細については、機密データ検出ジョブの作成を参照してください。

個々の S3 バケットのデータ機密情報の確認

Amazon Macie コンソールでは、S3 バケットページの詳細パネルを使用して、Macie がアカウントでモニタリングおよび分析する各 Amazon Simple Storage Service (Amazon S3) 汎用バケットに関する統計情報やその他の情報を確認できます。お客様が組織の Macie 管理者である場合、これには、お客さまのメンバーアカウントが所有するバケットが含まれます。

統計およびその他の情報には、S3 バケットのデータのセキュリティとプライバシーに関する洞察を提供する詳細が含まれます。機密データの自動検出が有効になっている場合、Macie がこれまでにバケットに対して実行した自動検出アクティビティの結果もキャプチャされます。たとえば、Macie がバケット内で分析したオブジェクトのリストや、Macie がバケット内で見つけた機密データのタイプと出現回数の内訳を検索できます。データには、作成して実行した機密データ検出ジョブの結果は含まれていないことに注意してください。

Macie は、機密データの自動検出を実行している間、これらの統計と詳細を自動的に再計算して更新します。例:

- Macie が S3 オブジェクト内に機密データを見つけられない場合、Macie はバケットの機密性スコアを下げ、必要に応じてバケットの機密ラベルを更新します。Macie はまた、バケット内で分析したオブジェクトのリストにオブジェクトを追加します。
- Macie が S3 オブジェクトで機密データを見つけると、Macie はそれらの出現を Macie がバケット内で見つけた機密データタイプの内訳に追加します。また、Macie は必要に応じてバケットの機密性スコアを上げ、バケットの機密ラベルを更新します。さらに、Macie はバケット内で分析したオ

ブジェクトのリストにオブジェクトを追加します。これらのタスクは、オブジェクトについて機密データの結果を作成する以外にも行われます。

- Macie が S3 オブジェクト内の機密データを発見し、そのデータがその後変更または削除された場合、Macie はバケットの機密データタイプの分類からそのオブジェクトにおける機密データの出現を削除します。また、Macie は必要に応じてバケットの機密性スコアを下げ、バケットの機密ラベルを更新します。さらに、Macie はバケット内で分析したオブジェクトのリストからオブジェクトを削除します。
- Macie が S3 オブジェクトを分析しようとしても、問題または エラーによりが分析できない場合、Macie はバケットで分析したオブジェクトのリストにそのオブジェクトを追加し、そのオブジェクトを分析できなかったことを通知します。

このパネルでは、統計と詳細を確認できるだけでなく、S3 バケットの機密データ自動検出の設定を調整できます。たとえば、特定のタイプの機密データをバケットのスコアに含めたり除外したりできます。詳細については、個々の S3 バケットの自動検出の管理を参照してください。

S3 バケットのデータ機密性の詳細を確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで、S3 バケットを選択します。S3 バケットページには、バケットインベントリのインタラクティブマップが表示されます。オプションで、ページの上部にあるテーブル

   を選択すると、インベントリが表形式で表示されます。

   デフォルトでは、このページには、現在機密データの自動検出から除外されているバケットのデータが表示されません。ユーザーが組織の Macie 管理者である場合、機密データの自動検出が現在無効になっているアカウントのデータも表示されません。このデータを表示するには、フィルターボックスの下にある自動検出フィルタートークンによってモニタリングされているで X を選択します。
3. S3 バケットマップまたはテーブルで、詳細を確認する S3 バケットを選択します。詳細パネルには、バケットに関する統計およびその他の情報が表示されます。

パネルの上部には、バケットの名前と、バケットを所有 AWS アカウント する のアカウント ID など、バケットに関する一般的な情報が表示されます。また、バケットの[特定の機密データ自動検出設定を変更する]オプションもあります。バケットに関するその他の設定や情報は、以下のタブにまとめられています。

- 感性
- バケットの詳細
- オブジェクトのサンプル
- 機密データ検出

各タブの個別の設定と情報は次のとおりです。

感性

このタブには、バケットの現在の機密性スコアが -1 から 100 の範囲で表示されます。Macie が定義する機密性スコアの範囲については、S3 バケットの機密スコアを参照してください。

このタブには、Macie がバケットのオブジェクト内で見つけた機密データのタイプと、各タイプの出現回数も表示されます。

- 機密データタイプ — データを検出したマネージドデータ識別子の一意の識別子 (ID)、またはデータを検出したカスタムデータ識別子の名前。

  マネージドデータ識別子の ID は、識別子が検出する機密データのタイプを表します。たとえば、米国のパスポート番号の場合は USA_PASSPORT_NUMBER などです。各マネージドデータ識別子の詳細については、マネージドデータ識別子の使用を参照してください。
- カウント — マネージドデータ識別子またはカスタムデータ識別子が検出したデータの出現数の合計。
- スコアリングステータス — データの出現回数をバケットの機密性スコアに含めるか除外するかを指定します。

  バケットのスコアを自動的に計算するように Macie を設定した場合は、特定のタイプの機密データをバケットのスコアに含めたり除外したりして計算を調整できます。含めたり除外したりするデータ識別子のチェックボックスを選択し、[アクション] メニューで必要なオプションを選択します。詳細については、個々の S3 バケットの自動検出の管理を参照してください。

Macie が現在バケットに保存されているオブジェクトに機密データを見つけられない場合、このセクションには [検出が見つかりません] というメッセージが表示されます。

機密性 タブには、Macie が分析し、その後変更または削除されたオブジェクトのデータは含まれないことに注意してください。Macie が分析した後でオブジェクトが変更されたり、バケットから削除されたりした場合、Macie は該当する統計とデータを自動的に再計算して更新し、オブジェクトを除外します。

バケットの詳細

このタブには、データセキュリティやプライバシー設定など、バケットの設定に関する詳細が表示されます。たとえば、バケットのパブリックアクセス設定の内訳を確認し、バケットがオブジェクトをレプリケートするか、他の AWS アカウントと共有するかを判断できます。

最終更新フィールドは、毎日の更新サイクルの一部として、Macie がバケットとバケットのオブジェクトの両方について Amazon S3 からメタデータを最後に取得した日時を示します。。最新の自動検出実行 には、Macie が自動検出を実行中にバケット内のオブジェクトを最後に分析した日時が表示されます。この分析が行われていない場合は、このフィールドにダッシュ (–) が表示されます。

タブは、Macie がバケット内で分析できるデータの量を評価するのに役立つオブジェクトレベルの統計も示します。また、機密データ検出ジョブがバケット内のオブジェクトを分析するように設定されているかどうかも示します。存在する場合は、最後に実行されたジョブに関する詳細にアクセスし、必要に応じてジョブが生成した調査結果を表示できます。

このタブの情報の詳細については、S3 バケットの詳細を確認するを参照してください。

オブジェクトのサンプル

このタブには、Macie がバケットの自動機密データ検出を実行中に分析対象として選択したオブジェクトが一覧表示されます。オプションでオブジェクトの名前を選択すると、Amazon S3 コンソールが開き、オブジェクトのプロパティが表示されます。

リストには最大 100 のオブジェクトのデータが含まれます。このリストは、[オブジェクト機密性] フィールド、[機密性]、その次に [低機密性] 、その次に Macie が分析できなかったオブジェクトの値に基づいて入力されます。

リストの [オブジェクト機密性] フィールドには、Macie がオブジェクト内に次の機密データを見つけたかどうかが示されます。

- 機密性 — Macie はオブジェクト内に少なくとも 1 つの機密データを検出しました。
- 低機密性 — Macie はオブジェクト内に機密データを検出しませんでした。
- — (ダッシュ) — 問題または エラーのため、Macie はオブジェクトの分析を完了できませんでした。

分類結果 フィールドには、Macie がオブジェクトを分析できたかどうかが表示されます。

- Complete (完了) — Macie はオブジェクトの分析を完了しました。

- 部分的 — Macie は問題またはエラーのため、オブジェクト内のデータのサブセットのみを分析しました。例えば、オブジェクトはサポートされていない形式のファイルを含むアーカイブファイルです。
- スキップ — 問題またはエラーのため、Macie はオブジェクト内のデータを分析できませんでした。たとえば、オブジェクトは Macie が使用を許可されていないキーを用いて暗号化されます。

Macie が分析または分析を試みた後に変更または削除されたオブジェクトは、リストに含まれていないことに注意してください。Macie は、オブジェクトが後で変更または削除された場合、そのオブジェクトをリストから自動的に削除します。

機密データ検出

このタブには、バケットの集計機密データの自動検出統計が表示されます。

- 分析されたバイト数 — Macie がバケット内で分析したデータの総量 (バイト単位)。
- 分類可能 – バケット内で Macie が分析できるすべてのオブジェクトの合計ストレージサイズ。前のデータでは、オブジェクトがサポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を持っている場合、オブジェクトは 分類可能です。詳細については、サポートされているストレージクラスとフォーマットを参照してください。
- 検出数の合計 — Macie がバケット内で検出した機密データの出現数の合計。これには、バケットの機密性スコアリング設定によって現在抑制されているデータが含まれます。

分析されたオブジェクト チャートには、Macie がバケット内で分析したオブジェクトの総数が表示されます。また、Macie が機密データを見つけた、または見つけなかったオブジェクトの数も視覚的に表示されます。グラフの下の凡例には、これらの結果の内訳が示されています。

- 機密性オブジェクト (赤) — Macie が機密データの出現を少なくとも 1 回検出したオブジェクトの総数。
- 低機密性 オブジェクト (青) — Macie が機密データを検出しなかったオブジェクトの総数。
- スキップされたオブジェクト (濃い灰色) — 問題またはエラーが原因で Macie が分析できなかったオブジェクトの総数。

グラフの凡例の下の領域は、特定のタイプのアクセス許可の問題または暗号化エラーが発生したために Macie がオブジェクトを分析できなかったケースの内訳を示しています。

- スキップ: 無効な暗号化 — お客様が用意したキーで暗号化されたオブジェクトの総数。Macie はこれらのキーにアクセスできません。

- スキップ: 無効な KMS – 使用できなくなった AWS Key Management Service （ AWS KMS) キーで暗号化されたオブジェクトの総数。これらのオブジェクトは、無効 AWS KMS keys になっている、削除がスケジュールされている、または削除された で暗号化されます。Macie はこれらのキーを使用できません。
- スキップ: アクセス許可拒否 – オブジェクトのアクセス許可設定、またはオブジェクトの暗号化に使用されたキーのアクセス許可設定が原因で Macie がアクセスを許可されていないオブジェクトの合計数。

これらの問題、および発生する可能性のあるその他のタイプの問題や エラーの詳細については、「」を参照してください機密データ自動検出のカバレッジ問題を修正する。問題と エラーを修正すると、後続の分析サイクル中にバケットのデータのカバレッジを増やすことができます。

機密データ検出 タブの統計には、Macie が分析または分析を試みた後に変更または削除されたオブジェクトのデータは含まれていません。Macie が分析または分析を試みた後にオブジェクトが変更されたり、バケットから削除されたりした場合、Macie はこれらの統計を自動的に再計算してオブジェクトを除外します。

自動検出によって生成された機密データ調査結果の分析

Amazon Macie は、機密データの自動検出を実行している間に、機密データを検出する各 Amazon Simple Storage Service (Amazon S3) オブジェクトの機密データ検出結果を作成します。機密データの調査結果は、Macie がオブジェクトで検出した機密データの詳細なレポートです。各機密データの調査結果には、重要度評価と次のような詳細が示されます。

- Macie が機密データを検出した日時。
- Macie が検出した機密データのカテゴリとタイプ。
- Macie が検出した機密データのタイプごとの出現回数。
- Macie が機密データ、機密データの自動検出、または機密データ検出ジョブを検出した方法。
- 影響を受けた S3 バケットおよびオブジェクトに関する名前、パブリックアクセス設定、暗号化タイプ、およびその他の情報。

影響を受けた S3 オブジェクトのファイルタイプまたはストレージ形式によっては、Macie が見つけた機密データの最大 15 までの出現の場所も詳細に含まれます。機密データの調査結果には、Macie が検出した機密データは含まれません。代わりに、必要に応じてさらなる調査と修復に使用できる情報が提供されます。

Macie は機密データの調査結果を 90 日間保存します。Amazon Macie コンソールまたは Amazon Macie API を使用してそれらにアクセスできます。また、他のアプリケーション、サービス、およびシステムを使用して、調査結果をモニタリングおよび処理することもできます。詳細については、調査結果を分析するを参照してください。

機密データの自動検出によって得られた結果を分析するには

Macie が機密データの自動検出の実行中に作成した検出結果を特定して分析するには、検出結果をフィルタリングできます。フィルターを使用すると、検出結果の特定の属性を使用して、検出結果のカスタムビューとクエリを構築します。Amazon Macie コンソールを使用して調査結果をフィルタリングするか、Amazon Macie API を使用してプログラムでクエリを送信できます。

Console

Amazon Macie コンソールを使用してサンプル検出結果を作成するには、次のステップに従います。

自動検出によって生成された結果を分析するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 結果 を選択します。
3. (オプション) 抑制ルールによって抑制された所見を表示するには、検出結果スタタス設定を変更する。次に アーカイブ済み を選択して、抑制された調査結果のみを表示するか、すべて を選択して、現在の調査結果と抑制された調査結果の両方を表示します。非表示にした結果を再度非表示にするには、[現在]を選択します。
4. [フィルター条件] ボックスにカーソルを置きます。表示されるフィールドのリストで、サンプル を選択します。

   このフィールドには、Macie が検出結果、機密データの自動検出、または機密データ検出ジョブの原因となった機密データをどのように見つけたかを指定します。フィルタフィールドのリスト内でこのフィールドを見つけるには、完全なリストを参照するか、フィールド名の一部を入力してフィールドのリストを絞り込みます。
5. フィールドの値として AUTOMATED_SENSITIVE_DATA_DISCOVERY を選択し、次に 適用 を選択します。Macie はフィルター基準を適用し、フィルター条件ボックスのフィルタートークンに条件を追加します。
6. (オプション) 結果を絞り込むには、追加のフィールドにフィルター条件を追加します。たとえば、検出果が作成された時間範囲には 作成日時 、影響を受けたバケットの名前には S3 バケット名 、検出され犬種結果を生成した機密データのタイプには 機密データ検出タイプ な

どのフィルター条件を追加します。詳細については、調査結果のフィルタリングを参照してください。

後でこの条件のセットを再度使用する場合は、フィルタールールとして保存できます。これを行うには、フィルターバーの ルールを保存する を選択します。次に、ルールの名前を入力し、オプションで説明を入力します。終了したら、保存 を選択します。

API

プログラムで結果を特定して分析するには、Amazon Macie API の ListFindingsまたは GetFindingStatisticsオペレーションを使用して送信するクエリでフィルター条件を指定します。ListFindings オペレーションは、フィルター基準と一致する結果ごとの 1 つの ID である、検索条件 ID の配列を返します。その後、それらの ID を使用して各検出結果の詳細を取得できます。GetFindingStatistics オペレーションは、リクエストで指定したフィールド別にグループ化された、フィルター基準と一致するすべての調査結果に関する集計統計データを返します。プログラムによる結果のフィルタリングの詳細については、「」を参照してください調査結果のフィルタリング。

フィルター条件には、`originType` フィールドの条件を含めてください。このフィールドには、Macie が検出結果、機密データの自動検出、または機密データ検出ジョブの原因となった機密データをどのように見つけたかを指定します。このフィールドの値は、自動検出の実行中に検出結果が見つかった場合 `AUTOMATED_SENSITIVE_DATA_DISCOVERY` となります。

AWS Command Line Interface （ AWS CLI ） を使用して検出結果を特定して分析するには、list-findings または get-finding-statistics コマンドを実行します。以下の例では、list-findings コマンドを使用して、現在の AWS リージョンにおける機密データの自動検出によって生成された重要度の高いすべての検出結果の結果 ID を取得しています。

Linux、macOS、または Unix の場合、読みやすさを向上させるためにバックスラッシュ (\) の行連結文字を使用します。

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

Microsoft Windows の場合、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

```
C:\> aws macie2 list-findings ^
```

```
--finding-criteria={\"criterion\":{\"classificationDetails.originType\":{\"eq
\":[\"AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},\"severity.description\":{\"eq\":
[\"High\"]}}}
```

ここで、

- classificationDetails.originType は、[オリジンタイプ] フィールドの JSON 名を指定し、
  - eqは、equals演算子を指定します。
  - AUTOMATED_SENSITIVE_DATA_DISCOVERY はフィールドの列挙値です。
- *severity.description* は[重要度] フィールドの JSON 名を指定し、
  - eqは、equals 演算子を指定します*eq* 。
  - *High* はフィールドの列挙値です。

コマンドが正常に実行された場合、Macie は、findingIds 配列を返します。配列には、次の例に示すように、フィルター基準と一致する各調査結果の一意の識別子がリスト化されます。

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

フィルター基準と一致する調査結果がない場合、Macie は空の findingIds 配列を返します。

```
{
    "findingIds": []
}
```

自動検出によって生成された機密データの検出結果へのアクセス

Amazon Macie は、機密データの自動検出の実行中に分析用に選択する各 Amazon Simple Storage Service (Amazon S3) オブジェクトの分析レコードを作成します。これらのレコードは機密データの検出結果と呼ばれ、Macie が個々の S3 オブジェクトに対して実行した分析の詳細を記録します。こ

れには、Macie が機密データを見つけられないオブジェクト、およびアクセス許可の設定やサポートされていないファイルやストレージ形式の使用などのエラーや問題のために Macie が分析できないオブジェクトが含まれます。

Macie が S3 オブジェクトで機密データを検出すると、機密データの検出結果は Macie が検出した機密データに関する情報を提供します。この情報には、機密データの検出結果が提供するのと同じタイプの詳細が含まれます。Macie が検出した各タイプの機密データの最大 1,000 件の出現の場所など、追加情報も提供します。例:

- Microsoft Excel ワークブック、CSV ファイル、または TSV ファイル内のセルまたはフィールドの列番号と行番号
- JSON または JSON Lines ファイル内のフィールドまたは配列へのパス
- CSV、JSON、JSON Lines、または TSV ファイル以外の非バイナリテキストファイル (HTML、TXT、XML ファイルなど) 内の行の行番号
- Adobe Portable Document Format (PDF) ファイル内のページのページ番号
- Apache Avro オブジェクトコンテナまたは Apache Parquet ファイル内のレコードのレコードインデックスとフィールドへのパス

影響を受ける S3 オブジェクトが .tar ファイルや .zip ファイルなどのアーカイブファイルである場合、機密データの検出結果には、Macie がアーカイブから抽出した個々のファイル内の機密データの出現に関する詳細な位置データも表示されます。Macie は、アーカイブファイルの機密データの調査結果にこの情報を含めません。位置データを報告するために、機密データ検出結果は標準化された JSON スキーマを使用します。

機密データの検出結果には、Macie が検出した機密データは含まれません。代わりに、データのプライバシーと保護の監査や調査に役立つ分析レコードが提供されます。

Macie は機密データの検出結果を 90 日間保存します。Amazon Macie コンソールまたは Amazon Macie API からそれらに直接アクセスすることはできません。代わりに、それを暗号化して S3 バケットに保存するように Macie を設定します。バケットは、機密データの検出結果のすべての最終的で長期的なリポジトリとして機能します。次に、オプションで、そのリポジトリ内の結果にアクセスしてクエリを実行できます。

アカウントのこのリポジトリの場所を確認するには、Amazon Macie コンソールのナビゲーションペインで [検出結果] を選択します。プログラムでこれを行うには、Amazon Macie API の GetClassificationExportConfiguration オペレーションを使用します。アカウントにこのリポジトリを設定していない場合は、機密データ検出結果の保存と保持 でその方法を確認してください。

機密データの検出結果を S3 バケットに保存するように Macie を設定した後、Macie は JSON Lines (.jsonl) ファイルに結果を書き込み、それらのファイルを暗号化し GNU Zip (.gz) ファイルとしてバケットに追加します。Macie は、機密データの自動検出のために、バケット内の という名前のフォルダ`automated-sensitive-data-discovery`にファイルを追加します。

機密データ検出結果の場合と同様に、機密データ検出の結果は標準化されたスキーマに従います。これは、オプションで、他のアプリケーション、サービス、およびシステムを使用して、それらをクエリ、モニタリング、および処理するのに役立ちます。

> **Tip**
>
> 機密データ検出結果をクエリして使用して潜在的なデータセキュリティリスクを分析およびレポートする方法の詳細な説明例については、 セキュリティブログのAmazon Athena と Amazon で Macie 機密データ検出結果をクエリおよび視覚化する方法 QuickSightAWS 」ブログ記事を参照してください。
> 機密データ検出結果の分析に使用できる Athena クエリのサンプルについては、 の Amazon Macie 結果分析リポジトリを参照してください GitHub。このリポジトリでは、結果を取得および復号化するように Athena を設定する手順と、結果のテーブルを作成するためのスクリプトも提供します。

S3 バケットの機密スコア

機密データの自動検出が有効になっている場合、Amazon Macie はアカウントまたは組織のモニタリングと分析を行う各 Amazon Simple Storage Service (Amazon S3) 汎用バケットに対して機密スコアを自動的に計算して割り当てます。機密スコアは、S3 バケットに含まれる可能性のある機密データの量を定量的に表したものです。そのスコアに基づいて、Macie は各バケットに機密ラベルも割り当てます。機密ラベルは、バケットの機密スコアを定性的に表したものです。これらの値は、Amazon S3 データ資産内の機密データがどこにあるかを判断し、そのデータの潜在的なセキュリティリスクを特定して監視するための参照ポイントとして役立ちます。

デフォルトでは、S3 バケットの機密スコアとラベルには、Macie がそれまでにバケットに対して実行した機密データ自動検出活動の結果が反映されています。作成、実行した機密データ検出ジョブの結果は反映されません。さらに、スコアもラベルも、バケットやバケットのオブジェクトが組織にもたらす緊急性や重要度を暗示したり、提示したりするものではありません。ただし、バケットに手動で最大スコア(100)を割り当てることでバケットの計算スコアを上書きできます。これにより、バケットに機密ラベルも割り当てられます。

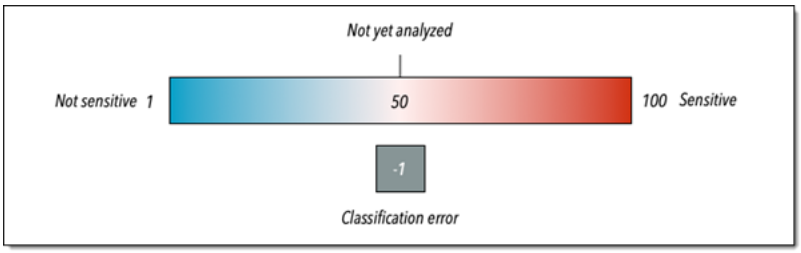
トピック

機密スコアリングの寸法と範囲

Amazon Macie の計算上、S3 バケットの機密スコアは 2 つの主要な寸法の交差点を定量的に測定したものです。

- Macie がバケット内で検出した機密データ量 これは主に、Macie がバケット内で検出した機密データタイプの性質と数、および各タイプの出現数から導き出されます。
- Macie がバケット内で分析したデータ量 これは主に、Macie がバケット内で分析したユニークオブジェクトの数と、バケット内の固有オブジェクトの総数との比較から算出されます。

S3 バケットの機密スコアによって、Macie がバケットに割り当てる機密ラベルも決まります。機密ラベルは、スコアを機密または非機密など定性的に表したものです。Amazon Macie コンソールでは、バケットの機密スコアによって、次の図に示すように Macie ユーザーがデータ視覚化でバケットを表すために使う色も決まります。



機密スコアの範囲は-1から100す（次の表を参照）。S3 バケットのスコアへの入力を評価するには、Macie がバケットに関して提供する機密データ検出統計やその他詳細情報を参照します。

機密スコア	機密ラベル	追加情報
-1	分類エラー	Macie は、オブジェクトレベルの分類エラー、つまりオブジェクトレベルのアクセス許可設定、オブジェクトコンテンツ、またはクォータの問題により、バケットのオブジェ

機密スコア	機密ラベル	追加情報
		クトをまだ正常に分析していません。 Macie がバケット内の 1 つ以上のオブジェクトを分析しようとしたときに、エラーが発生しました。例えば、オブジェクトが不正な形式のファイルであったり、Macie がアクセスできない、あるいは使用を許可されていないキーでオブジェクトが暗号化されている場合などです。バケットのカバレッジデータは、エラーの調査と修正に役立ちます。詳細については、機密データ自動検出カバレッジの評価を参照してください。 Macie はバケット内のオブジェクトの分析を引き続き試みます。Macie がオブジェクトを正常に分析すると、Macie はバケットの機密スコアとラベルを更新して、分析結果を反映します。

機密スコア	機密ラベル	追加情報
1 ～ 49	非機密	この範囲で 49のような高いスコアは、Macie がバケット内で分析したオブジェクトが比較的少ないことを示します。1のような低いスコアは、Macie がバケット内の多数のオブジェクト (バケット内のオブジェクト総数に対して) を分析し、それらのオブジェクトに含まれる機密データのタイプと出現が比較的少ないことを示します。 スコア 1 は、バケットにオブジェクトが保存されていないか、バケット内のすべてのオブジェクトにゼロ (0) バイトのデータが含まれていることを示すこともできます。バケットの詳細にあるオブジェクトの統計は、それに該当するか判断するのに役立ちます。詳細については、S3 バケットの詳細の確認を参照してください。

機密スコア	機密ラベル	追加情報
50	分析が未完了	Macie はまだバケットのオブジェクトを分析していない、または分析を試みていません。 Macie は、自動検出が最初に有効になったとき、またはバケットがアカウントのバケットインベントリに追加されると、このスコアを自動的に割り当てます。組織では、バケットを所有するアカウントで自動検出が有効になっていない場合、バケットにこのスコアを付けることもできます。 スコアが50の場合、バケットのアクセス許可設定により、Macie がバケットまたはバケットのオブジェクトにアクセスできなくなっている可能性もあります。これは通常、制限の厳しいバケットポリシーが原因です。Macie はバケットに関するサブセットのみの情報を提供できるので、バケットの詳細がそれに該当するか判断するのに役立ちます。この問題の対処方法については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。

機密スコア	機密ラベル	追加情報
51 ～ 99	機密	この範囲で、99のような高いスコアは、Macie がバケット内の多数のオブジェクト (バケット内のオブジェクトの総数に対して) を分析し、それらのオブジェクトに含まれる機密データの多くのタイプと出現を検出したことを示します。51のような低めのスコアは、Macie がバケット内で中程度の数のオブジェクト (バケット内のオブジェクトの総数と比較して) を分析し、それらのオブジェクト内の機密データのタイプと出現を少なくとも数種類検出したことを示します。
100	機密	スコアは手動でバケットに割り当てられ、計算されたスコアは上書きされました。Macie はこのスコアをバケットに割り当てません。

機密スコアの監視

アカウントで機密データの自動検出が最初に有効になると、Amazon Macie はアカウントが所有する各 S3 バケットに 50 の機密スコアを自動的に割り当てます。Macie は、バケットがアカウントのバケットインベントリに追加されると、このスコアをバケットにも割り当てます。そのスコアに基づいて、各バケットの機密ラベルは分析が未完了です。例外は空のバケットです。これは、オブジェクトを保存しないか、バケット内のすべてのオブジェクトにゼロ (0) バイトのデータが含まれているバケットです。その場合、Macie はバケットに1のスコアを割り当て、バケットの機密ラベルは非機密とします。

機密データの自動検出が毎日進行するにつれて、Macie は分析の結果を反映するために S3 バケットの機密スコアとラベルを更新します。例:

- Macie がオブジェクト内の機密データを検出しない場合、必要に応じてMacie はバケットの機密スコアを下げ、バケットの機密ラベルを更新します。
- Macie がオブジェクト内の機密データを検出すると、必要に応じて Macie はバケットの機密スコアを上げ、バケットの機密ラベルを更新します。
- その後変更されたオブジェクト内で機密データが検出された場合、Macie は必要に応じてそのオブジェクトの機密データ検出をバケットの機密スコアから削除し、バケットの機密ラベルを更新します。
- その後削除されたオブジェクト内で機密データが検出された場合、Macie は必要に応じてそのオブジェクトの機密データをバケットの機密スコアから削除し、バケットの機密ラベルを更新します。
- 以前は空だったバケットにオブジェクトが追加され、Macie がそのオブジェクトに機密データを検出した場合、必要に応じて Macie はバケットの機密スコアを上げ、バケットの機密ラベルを更新します。
- バケットの権限設定により、Macie がバケットまたはバケットのオブジェクトに関する情報を取得またはアクセスができなくなっている場合、Macie はバケットの機密スコアを50に変更し、バケットの機密ラベルを分析が未完了に変更します。

分析結果は、アカウントの機密データ自動検出を有効にしてから 48 時間以内に表示され始めることができます。

お客様が組織の Macie 管理者である場合、またはスタンドアロン Macie アカウントをお持ちの場合は、組織またはアカウントの機密スコアリング設定を調整できます。

- すべての S3 バケットの後続の分析の設定を調整するには、アカウントの機密データ自動検出設定を変更します。特定のマネージドデータ識別子、カスタムデータ識別子、または許可リストの包含または除外を開始できます。特定のバケットを除外することもできます。詳細については、「自動検出の設定」を参照してください。
- 個々の S3 バケットの設定を調整するには、各バケットの自動機密データ検出設定を変更します。バケットのスコアには、特定のタイプの機密データを含めることも除外することもできます。自動的に計算されたスコアをバケットに割り当てるかどうかを指定することもできます。詳細については、「個々の S3 バケットの自動検出の管理」を参照してください。

機密データの自動検出を無効にすると、既存の機密スコアとラベルへの影響は異なります。組織内のメンバーアカウントに対して無効にすると、アカウントが所有する S3 バケットに対して既存のスコ

アとラベルが保持されます。組織全体またはスタンドアロン Macie アカウントで無効にした場合、既存のスコアとラベルは 30 日間だけ保持されます。30 日後、Macie は組織またはアカウントが所有するすべてのバケットのスコアとラベルをリセットします。バケットにオブジェクトが保存されている場合、Macie はスコアを 50 に変更し、未分析のラベルをバケットに割り当てます。バケットが空の場合、Macie はスコアを 1 に変更し、機密性のないラベルをバケットに割り当てます。このリセット後、組織またはアカウントの機密データ自動検出を再度有効にしない限り、Macie はバケットの機密スコアとラベルの更新を停止します。

機密データの自動検出のデフォルト設定

機密データの自動検出が有効になっている場合、Amazon Macie は、アカウントでモニタリングおよび分析するすべての Amazon Simple Storage Service (Amazon S3) 汎用バケットからサンプルオブジェクトを自動的に選択して分析します。ユーザーが組織の Macie 管理者である場合、デフォルトでは、メンバーアカウントが所有する S3 バケットが含まれます。

分析の範囲を絞り込むには、特定の S3 バケットを機密データの自動検出から除外できます。これを行うには、アカウントの設定を変更する方法と、個々のバケットの設定を変更する方法の 2 つの方法があります。Macie 管理者の場合は、組織内の個々のアカウントの機密データ自動検出を有効または無効にすることもできます。詳細については、「機密データ自動検出の設定」を参照してください。

デフォルトでは、Macie は機密データ自動検出に推奨するマネージドデータ識別子のセットのみを使用して S3 オブジェクトを分析します。Macie は、ユーザーが定義したカスタムデータ識別子や許可リストを使用しません。分析をカスタマイズするには、特定のマネージドデータ識別子、カスタムデータ識別子、許可リストを使用するように Macie を設定します。これを行うには、アカウントの設定を変更します。詳細については、「機密データ自動検出の設定」を参照してください。

トピック

- 機密データ自動検出のためのデフォルトのマネージドデータ識別子
- 機密データ自動検出用にデフォルト設定へ更新

機密データ自動検出のためのデフォルトのマネージドデータ識別子

デフォルトでは、Amazon Macie は、機密データ自動検出に推奨するマネージドデータ識別子のセットのみを使用して S3 オブジェクトを分析します。このデフォルトのマネージドデータ識別子セットは、一般的なカテゴリやタイプの機密データを検出するように設計されています。当社の研究に基づいて、一般的なカテゴリやタイプの機密データを検出できると同時に、ノイズを減らすことで自動検出結果を最適化できます。

デフォルトセットは動的です。新しいマネージドデータ識別子をリリースするにあたり、機密データの自動検出結果をさらに最適化できる可能性がある場合は、それらをデフォルトセットに追加します。別途、既存のマネージドデータ識別子を追加したり、セットから削除したりする可能性もあります。マネージドデータ識別子を削除しても、S3 バケットの既存の機密データ検出統計や詳細には影響しません。例えば、以前 Macie によってバケット内で検出されあるタイプの機密データのマネージドデータ識別子を削除しても、Macie は引き続きそのバケットの検出結果を報告します。マネージドデータ識別子をデフォルトセットに追加または削除すると、このページが更新され、変更の性質とタイミングが示されます。これらの変更に関する自動アラートについては、Macie ドキュメント履歴ページの RSS フィードをサブスクライブしてください。

以下のトピックでは、現在デフォルトセットに含まれているマネージドデータ識別子を機密データのカテゴリとタイプ別に一覧表示しています。セット内の各マネージドデータ識別子の一意の識別子 (ID) を指定します。この ID は、PGP_PRIVATE_KEY PGP プライベートキーや米国パスポート番号の USA_PASSPORT_NUMBER など、マネージドデータ識別子が検出するに設計された機密データのタイプを表します。アカウントの機密データ自動検出設定を変更する場合、この ID を使用して、以降の分析でマネージドデータ識別子を明示的に除外できます。

トピック

- 認証情報
- 財務情報
- 個人を特定できる情報 (PII)

特定のマネージドデータ識別子、または Macie が現在提供しているマネージドデータ識別子の全リストについては、マネージドデータ識別子の使用　を参照してください。

認証情報

Macie では、S3 オブジェクトでの認証情報データの出現を検知するために、次のマネージドデータ識別子を使用します。

機密データタイプ	マネージドデータ識別子 ID
AWS シークレットアクセスキー	AWS_CREDENTIALS
HTTP 基本認証ヘッダー	HTTP_BASIC_AUTH_HEADER
OpenSSH プライベートキー	OPENSSH_PRIVATE_KEY

機密データタイプ	マネージドデータ識別子 ID
PGP プライベートキー	PGP_PRIVATE_KEY
公開鍵暗号標準 (PKCS) プライベートキー	PKCS
PuTTY プライベートキー	PUTTY_PRIVATE_KEY

財務情報

Macie では、S3 オブジェクトでの財務情報の出現を検知するために、次のマネージドデータ識別子を使用します。

機密データタイプ	マネージドデータ識別子 ID
クレジットカードの磁気ストライプデータ	CREDIT_CARD_MAGNETIC_STRIPE
クレジットカード番号	CREDIT_CARD_NUMBER (キーワードに近いクレジットカード番号の場合)

個人を特定できる情報 (PII)

S3 オブジェクトで個人を特定できる情報 (PII) の出現を検知するために、Macie はデフォルトで次のマネージドデータ識別子を使用します。

機密データタイプ	マネージドデータ識別子 ID
運転免許証識別番号	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (米国の場合)、 UK_DRIVERS_LICENSE
選挙人名簿番号	UK_ELECTORAL_ROLL_NUMBER
国民識別番号	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NAT

機密データタイプ	マネージドデータ識別子 ID
	IONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
国民保険番号 (NINO)	UK_NATIONAL_INSURANCE_NUMBER
パスポート番号	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
社会保険番号 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
社会保障番号 (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
納税者識別番号または参照番号	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

機密データ自動検出用にデフォルト設定へ更新

次の表は、Amazon Macie が機密データの自動検出用にデフォルトで使用する設定の変更を示しています。これらの変更に関する自動アラートについては、Macie ドキュメント履歴ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
デフォルトマネージドデータ識別子の新しい動的セットを実装	新しい機密データ自動検出設定は、動的なマネージドデータ識別子のデフォルトセットをベースにするようになりました。この日以降に初めて機密データ自動検出を有効にした場合、設定は動的セットに基づいて行われます。 この日より以前に初めて機密データ自動検出を有効にした場合、設定は別のマネージドデータ識別子のセットに基づいています。詳細については、この表の後にある注を参照してください。	2023 年 8 月 2 日
一般提供	機密データ自動検出の初回リリース。	2022 年 11 月 28 日

2023 年 8 月 2 日より前に機密データの自動検出を最初に有効にした場合、設定はデフォルトのマネージドデータ識別子の動的セットに基づいていません。代わりに、以下の表に示すように、機密データ自動検出の初回リリース用に定義したマネージドデータ識別子の静的なセットに基づいています。

機密データ自動検出を最初に有効にした日時を確認するには、Amazon Macie コンソールのナビゲーションペインで機密データ自動検出を選択し、ステータスセクションで有効になった日付を参照します。これをプログラムで実行するには、Amazon Macie API の GetAutomatedDiscoveryConfigurationオペレーションを使用し、 `firstEnabledAt`フィールドの値を参照します。日付が 2023 年 8 月 2 日より前で、デフォルトのマネージドデータ識別子の動的セットの使用を開始する場合は、 AWS Support にお問い合わせください。

次の表には、静的セットのマネージドデータ識別子がすべて示されています。この表は、まず機密データカテゴリ別に、次に機密データタイプ別にソートされています。特定のマネージドデータ識別子の詳細については、マネージドデータ識別子の使用 を参照してください。

機密データのカテゴリ	機密データタイプ	マネージドデータ識別子 ID
認証情報	AWS シークレットアクセスキー	AWS_CREDENTIALS
認証情報	HTTP 基本認証ヘッダー	HTTP_BASIC_AUTH_HEADER
認証情報	OpenSSH プライベートキー	OPENSSH_PRIVATE_KEY
認証情報	PGP プライベートキー	PGP_PRIVATE_KEY
認証情報	公開鍵暗号標準 (PKCS) プライベートキー	PKCS
認証情報	PuTTY プライベートキー	PUTTY_PRIVATE_KEY
財務情報	銀行口座番号	BANK_ACCOUNT_NUMBER (カナダおよび米国の銀行口座番号の場合)、FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
財務情報	クレジットカードの有効期限	CREDIT_CARD_EXPIRATION
財務情報	クレジットカードの磁気ストライプデータ	CREDIT_CARD_MAGNETIC_STRIPE
財務情報	クレジットカード番号	CREDIT_CARD_NUMBER (キーワードに近いクレジットカード番号の場合)

機密データのカテゴリ	機密データタイプ	マネージドデータ識別子 ID
財務情報	クレジットカード認証コード	CREDIT_CARD_SECURITY_CODE
個人情報: 個人の健康情報 (PHI)	麻薬取締局 (DEA) 登録番号	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
個人情報: PHI	健康保険請求番号 (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
個人情報: PHI	健康保険または医療識別番号	CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER
個人情報: PHI	ヘルスケア共通手順コーディングシステム (HCPCS) コード	USA_HEALTHCARE_PROCEDURE_CODE
個人情報: PHI	全米医薬品コード (NDC)	USA_NATIONAL_DRUG_CODE
個人情報: PHI	国家プロバイダー識別子 (NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
個人情報: PHI	機器固有識別子 (UDI)	MEDICAL_DEVICE_UDI
個人情報: 個人を特定できる情報 (PII)	生年月日	DATE_OF_BIRTH

機密データのカテゴリ	機密データタイプ	マネージドデータ識別子 ID
個人情報: PII	運転免許証識別番号	AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (米国の場合)、ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLAN

機密データのカテゴリ	機密データタイプ	マネージドデータ識別子 ID
		DS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
個人情報: PII	選挙人名簿番号	UK_ELECTORAL_ROLL_NUMBER
個人情報: PII	フルネーム	NAME
個人情報: PII	全地球測位システム (GPS) 座標	LATITUDE_LONGITUDE
個人情報: PII	郵送先住所	ADDRESS, BRAZIL_CEP_CODE
個人情報: PII	国民識別番号	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

機密データのカテゴリ	機密データタイプ	マネージドデータ識別子 ID
個人情報: PII	国民保険番号 (NINO)	UK_NATIONAL_INSURANCE_NUMBER
個人情報: PII	パスポート番号	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
個人情報: PII	本籍地	CANADA_NATIONAL_IDENTIFICATION_NUMBER
個人情報: PII	電話番号	BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (カナダと米国の場合)、SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
個人情報: PII	社会保険番号 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
個人情報: PII	社会保障番号 (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

機密データのカテゴリ	機密データタイプ	マネージドデータ識別子 ID
個人情報: PII	納税者識別番号または参照番号	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER
個人情報: PII	車両識別番号 (VIN)	VEHICLE_IDENTIFICATION_NUMBER

Amazon Macie で機密データ検出ジョブを実行する

Amazon Macie を使用すると、機密データ検出ジョブを作成して実行し、Amazon Simple Storage Service (Amazon S3) 汎用バケット内の機密データの検出、ログ記録、レポートを自動化できます。機密データ検出ジョブは、Amazon S3 オブジェクト内の機密データを検出して報告するために Macie が実行する一連の自動処理および分析タスクです。各ジョブでは、Macie が検出した機密データと Macie が実行する分析に関する詳細なレポートが提供されます。ジョブを作成して実行すると、組織が Amazon S3 に保存するデータと、そのデータのセキュリティまたはコンプライアンスのリスクに関する包括的なビューを構築して維持できます。

データセキュリティおよびプライバシーの要件を満たし、それへの準拠を維持するために、Macie はジョブの範囲のスケジュールおよび定義のためのいくつかのオプションを提供しています。ジョブは、オンデマンドの分析および評価では 1 回のみ、または定期的な分析、評価、およびモニタリングでは繰り返しベースで実行するように設定できます。ジョブの分析の幅と深さ、つまり、選択する

特定の S3 バケット、または特定の条件に一致するバケットも定義します。追加のオプションを選択して、オプションとして分析の範囲を絞り込むことができます。オプションには、タグやプレフィックスなどの S3 オブジェクトのプロパティから派生するカスタム基準やオブジェクト最終更新日時があります。

それぞれのジョブで、Macie が検出してレポートする機密データのタイプも指定します。各ジョブは、Macie が提供した マネージドデータ識別子、お客様が定義した カスタムデータ識別子、またはこの 2 つの組み合わせを使用して、オブジェクトを分析できます。ジョブに対して特定のマネージドデータ識別子とカスタムデータ識別子を選択することで、特定のタイプの機密データに焦点を絞るように分析を調整できます。分析を微調整するために、定義した 許可リストを使用するようにジョブを設定することもできます。許可リストで、Macie に無視させたいテキストとテキストパターンを指定します。通常、組織の特定のシナリオや環境における機密データの例外です。

各ジョブは、その検出された機密データと実行された分析のレコード (機密データの調査結果 (機密データの調査結果) と 機密データの検出結果) を作成します。機密データの調査結果は、Macie がS3 オブジェクトで検出した機密データの詳細なレポートです。機密データの検出結果は、オブジェクトの分析に関する詳細を記録するレコードです。Macie は、分析するジョブを設定するオブジェクトごとに、機密データの検出結果を作成します。これには、Macie が機密データを見つけられないために機密データの検出結果を生成しないオブジェクト、およびエラーや問題のために Macie が分析できないオブジェクトが含まれます。各タイプのレコードは、標準化されたスキーマに従っており、セキュリティおよびコンプライアンスの要件を満たすために、レコードのクエリ、モニタリング、および処理に役立ちます。

トピック

- 機密データ検出ジョブの範囲のオプション
- 機密データ検出ジョブの作成
- 機密データ検出ジョブの統計と結果の確認
- Amazon CloudWatch Logs を用いた機密データ検出ジョブのモニタリング
- 機密データ検出ジョブの管理
- 機密データ検出ジョブのコストの予測とモニタリング
- 機密データ検出ジョブに推奨されるマネージドデータ識別子

機密データ検出ジョブの範囲のオプション

機密データ検出ジョブでは、Amazon Macie が機密データを検出してレポート作成する Amazon Macie が分析する Amazon Simple Storage Service (Amazon S3) データの範囲を定義します。これを

行うために、Macie では、ジョブを作成および設定するときに選択できるジョブ固有のオプションがいくつか用意されています。

範囲オプション

- S3 バケット
- 初回実行: 既存の S3 オブジェクト
- サンプリング深度
- S3 オブジェクト基準

S3 バケット

機密データ検出ジョブを作成するときは、ジョブの実行時に Macie が分析するオブジェクトを保存する S3 バケットを指定します。これは、バケットインベントリから特定の S3 バケットを選択する方法と、S3 バケットのプロパティから派生するカスタム条件を指定する方法の S3 つの方法で実行できます。

特定の S3 バケットを選択する

このオプションでは、分析する各 S3 バケットを明示的に選択します。次に、ジョブが実行されると、選択したバケット内のオブジェクトのみが分析されます。毎日、毎週、または毎月ベースで定期的に実行するようにジョブを設定すると、ジョブは実行されるたびに同じバケット内のオブジェクトを分析します。

この設定は、特定のデータセットのターゲットを絞った分析を実行する場合に役立ちます。これにより、ジョブが分析するバケットの正確かつ予測可能な制御が可能になります。

S3 バケット条件を指定する

このオプションでは、分析する S3 バケットを決定するランタイム基準を定義します。基準は、パブリックアクセス設定やタグなど、バケットプロパティから派生する 1 つ以上の条件で設定されます。ジョブが実行されると、基準に一致するバケットが識別され、次にそれらのバケット内のオブジェクトが分析されます。ジョブを定期的に実行するように設定した場合、ジョブは実行されるたびにこれを実行します。その結果、ジョブは、バケットインベントリへの変更および定義した基準に応じて、実行されるたびに異なるバケット内のオブジェクトを分析することがあります。

この設定は、分析の範囲をバケットインベントリの変更に動的に適応させたい場合に役立ちます。バケット基準を使用して定期的に実行するようにジョブを設定すると、ジョブは基準に一致する新しいバケットを自動的に識別し、機密データについてそれらのバケットを検査します。

このセクションのトピックでは、各オプションに関する追加の詳細を提供します。

トピック

- 特定のバケットを選択する
- S3 バケット基準の指定

特定のバケットを選択する

ジョブで分析する各 S3 バケットを明示的に選択すると、Macie は現在の の汎用バケットの完全なインベントリを提供します AWS リージョン。次に、インベントリを確認し、必要なバケットを選択できます。Macie がこのインベントリを生成して維持する方法については、Macie が Amazon S3 データセキュリティをモニタリングする方法を参照してください。

お客様が組織の Macie 管理者である場合、インベントリには、組織のメンバーアカウントによって所有されているバケットが含まれます。これらのバケットは最大 1,000 個まで選択でき、最大 1,000 個のアカウントで設定されます。

バケットの選択を支援するために、インベントリは各バケットの詳細と統計を提供します。これには、ジョブが各バケットで分析できるデータの量が含まれます。分類可能なオブジェクトは、サポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子 を持つオブジェクトです。インベントリは、バケット内のオブジェクトを分析するように既存のジョブが設定されているかどうかも示します。これらの詳細は、ジョブの幅を推定し、バケットの選択を絞り込むのに役立ちます。

インベントリテーブルには、以下があります。

- 機密性 — 自動機密データ検出が有効になっている場合のバケットの現在の機密性スコアを示します。
- 分類可能なオブジェクト– このフィールド は、ジョブがバケット内で分析できるオブジェクトの合計数を示します。
- 分類可能なサイズ – このフィールドは、ジョブがバケット内で分析できるすべてのオブジェクトの合計ストレージサイズを示します。

  バケットに圧縮オブジェクトが保存されている場合、この値は解凍後のオブジェクトの実際のサイズを反映しません。バケットでバージョニングが有効化されている場合、この値は、バケット内の各オブジェクトの最新バージョンのストレージサイズに基づきます。
- モニタリングされている- のフィールドは、バケット内のオブジェクトを毎日、毎週、または毎月ベースで定期的に分析するように既存のジョブが設定されているかどうかを示します。

このフィールドの値が はいの場合、バケットが定期的なジョブに明示的に含まれるか、バケットが過去 24 時間以内の定期的なジョブの基準に一致したことになります。さらに、それらのジョブの少なくとも 1 つのステータスは キャンセルされません。Macie は毎日ベースでこのデータを更新します。

- 最新のジョブの実行— バケット内のオブジェクトを分析するように既存の定期ジョブまたは 1 回限りのジョブが設定されている場合、このフィールドは、これらのジョブの実行が開始された最新の時刻を示します。それ以外の場合は、このフィールドにダッシュ (–) が表示されます。

情報アイコン が テーブル内の任意のバケット名の横に表示される場合、Amazon S3 から最新のバケットメタデータを取得することをお勧めします。これを行うには、テーブルの上の更新 ( ) を選択します。情報アイコンは、Macie が毎日の更新サイクルの一部として Amazon S3 からバケットとオブジェクトのメタデータをおそらく最後に取得した後の過去 24 時間にバケットが作成されたことを示します。詳細については、データの更新を参照してください。

警告アイコン が テーブルのバケットの名前の横に表示される場合、Macie はバケットまたはバケットのオブジェクトへのアクセスが許可されません。これは、ジョブがバケット内のオブジェクトを分析できなくなることを意味します。問題を調査するには、Amazon S3 内のバケットのポリシーとアクセス許可の設定を確認します。例えば、バケットには制限があるバケットポリシーが設定されている場合があります。詳細については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。

インベントリビューをカスタマイズし、特定のバケットをより簡単に検索するには、フィルターボックスにフィルター基準を入力してテーブルをフィルタリングできます。例をいくつか、次のテーブルに示します。

...のすべてのバケットを表示するには	...でこのフィルターを適用
特定のアカウントによって所有されている	アカウント ID= *the 12-digit ID for the account* (アカウントの 12 桁の ID)
パブリックアクセス可能である	有効なアクセス許可 = パブリック

...のすべてのバケットを表示するには	...でこのフィルターを適用
定期的なジョブには含まれない	ジョブによって積極的にモニタリングされる= False
定期的または 1 回限りのジョブに含まれない	ジョブで定義されている= (False)
特定のタグキーを持っている*	タグキー= ######
特定のタグ値を持っている*	タグ値= #####
暗号化されていないオブジェクト (またはクライアント側の暗号化を使用するオブジェクト) を保存する	暗号化によるオブジェクトカウントは、暗号化なしおよび From = 1

* タグのキーと値は大文字と小文字が区別されます。また、フィルターでこれらのフィールドに完全で有効な値を指定する必要があります。部分的な値を指定したり、ワイルドカード文字を使用したりすることはできません。

バケットの詳細を表示するには、バケットの名前を選択し、詳細パネルを参照します。そこから、次のこともできます。

- フィールドの拡大鏡を選択して、特定のフィールドでピボットしてドリルダウンします。
  を選択して同じ値を持つバケットを表示するか、
  を選択して他の値を持つバケットを表示します。
- バケット内のオブジェクトの最新のメタデータを取得します。これは、バケットを最近作成したり、過去 24 時間にバケットのオブジェクトに重要な変更を行った場合に役立ちます。データを取得するには、パネルの オブジェクト統計セクションで更新 を選択します。このオプションは、30,000 個以下のオブジェクトを保存するバケットで使用できます。

S3 バケット基準の指定

ジョブのバケット基準を指定することを選択した場合、Macie は基準を定義およびテストするためのオプションを提供します。これらは、分析するオブジェクトを保存する S3 バケットを決定するランタイム基準です。ジョブが実行されるたびに、条件に一致する汎用バケットを識別し、適切なバケット内のオブジェクトを分析します。お客様が組織の Macie 管理者である場合、これには、組織のメンバーアカウントによって所有されているバケットが含まれます。

バケット基準の定義

バケット基準は、S3 バケットのプロパティから派生する 1 つ以上の基準で設定されます。各条件は、基準とも呼ばれ、以下の設定要素があります。

- アカウント IDまたは 有効なアクセス許可 などの、プロパティベースのフィールド。
- 演算子で、と等しいeqまたは 等しくないneqのいずれか。
- 1 つまたは複数の値。
- 条件に一致するバケットを分析する (を含む) かスキップする (を除く) かを示す include または exclude ステートメント。

フィールドに複数の値を指定した場合、Macie は OR ロジックを使用して値を結合します。基準に複数の条件を指定した場合、Macie は AND ロジックを使用して条件を結合します。また、除外条件は含む条件よりも優先されます。たとえば、パブリックアクセス可能なバケットを含めて、特定のタグを持つバケットを除外する場合、ジョブは、バケットに指定されたタグのいずれかがない限り、パブリックアクセス可能なバケット内のオブジェクトを分析します。

S3 バケットの次のプロパティベースのフィールドのいずれかから派生する条件を定義できます。

アカウント ID

バケットを所有 AWS アカウント する の一意の識別子 (ID)。このフィールドに複数の値を指定するには、各アカウントの ID を入力し、各エントリをカンマで区切ります。

また、Macie はこのフィールドのワイルドカード文字または部分的な値の使用をサポートしていないことに注意してください

バケット名

バケットの名前。このフィールドは、Amazon S3 内の、Amazon Resource Name (ARN) (Amazon リソースネーム (ARN)) フィールドではなく、名前フィールドに関連します。この

フィールドに複数の値を指定するには、各バケットの名前を入力し、各エントリをカンマで区切ります。

values (値) では、大文字と小文字が区別されることに注意してください。また、Macie はこのフィールドのワイルドカード文字または部分的な値の使用をサポートしていません。

有効なアクセス許可

バケットがパブリックアクセス可能かどうかを指定します。このフィールドには、次の値を 1 つ以上選択できます。

- パブリックではない— 一般ユーザーは、バケットへの読み取りまたは書き込みのアクセス権を持っていません。
- パブリック— 一般ユーザーは、バケットへの読み取りまたは書き込みのアクセス権を持っています。
- 不明— Macie はバケットのパブリックアクセス設定を評価できませんでした。

バケットのこの値を決定するために、Macie はバケットのアカウントレベルとバケットレベルの設定、アカウントのブロックパブリックアクセスの設定、バケットのブロックパブリックアクセスの設定、バケットのバケットポリシー、およびバケットのアクセスコントロールリスト (ACL) の組み合わせを分析します。

共有アクセス

バケットを別の 、Amazon CloudFront オリジンアクセスアイデンティティ (OAI) AWS アカウント、または CloudFront オリジンアクセスコントロール (OAC) と共有するかどうかを指定します。このフィールドには、次の値を 1 つ以上選択できます。

- 外部 – バケットは、OAI、 CloudFront OCloudFront AC、または組織の外部 (一部ではない) アカウントのいずれかまたは組み合わせと共有されます。
- 内部 — バケットは組織の内部にある (一部である) 1 つ以上のアカウントと共有されます。CloudFront OAI または OAC と共有されません。
- 共有なし — バケットは別のアカウント、 CloudFront OAI、または CloudFront OAC と共有されません。
- 不明— Macie はバケットの共有アクセス設定を評価できませんでした。

バケットが別の と共有されているかどうかを判断するために AWS アカウント、Macie はバケットのバケットポリシーと ACL を分析します。さらに、組織は、 を通じて、 AWS Organizations または Macie の招待によって関連アカウントのグループとして一元管理される一連の Macie

アカウントとして定義されます。Amazon S3 のバケット共有のオプションの詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 での Identity and Access Managementを参照してください。

バケットが CloudFront OAI または OAC と共有されているかどうかを判断するために、Macie はバケットのバケットポリシーを分析します。 CloudFront OAI または OAC を使用すると、ユーザーは 1 つ以上の指定された CloudFrontディストリビューションを介してバケットのオブジェクトにアクセスできます。 CloudFront OAIs と OACs」を参照してください。 Amazon S3 CloudFront

タグ

バケットに関連付けられているタグ。タグは、S3 バケットを含む特定のタイプの AWS リソースを定義して割り当てることができるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。S3 バケットのタグ付けの詳細については、Amazon Simple Storage Service ユーザーガイドのコスト配分 S3 バケットタグの使用を参照してください。

機密データ検出ジョブの場合、このタイプの条件を使用して、特定のタグキー、特定のタグ値、または特定のタグキーとタグ値 (ペアとして) を持つバケットを含めるか除外できます。例:

- タグキーとして **`Project`** を指定し、条件でタグ値を指定しない場合、プロジェクトタグキーを持つバケットは、そのタグキーに関連付けられているタグ値に関係なく、条件の基準を満たします。
- **`Development`** と **`Test`** をタグ値として指定し、条件でタグキーを指定しない場合、**`Development`** または **`Test`** のタグ値を持つバケットは、それらのタグ値に関連付けられているタグキーに関係なく、条件の基準と一致します。

条件で複数のタグキーを指定するには、各タグキーを キーフィールドに入力し、各エントリをカンマで区切ります。条件で複数のタグ値を指定するには、各タグ値を 値フィールドに入力し、各エントリをカンマで区切ります。

タグのキーと値は大文字と小文字が区別されることに注意してください。また、Macie はタグ条件でのワイルドカード文字または部分的な値の使用をサポートしていません。

バケット基準のテスト

バケット基準を定義している間、結果をプレビューして基準をテストおよび絞り込むことができます。これを行うには、コンソールの条件の下に表示される 基準の結果のプレビューセクションを展開します。このセクションでは、現在条件に一致する S3 汎用バケットの表を表示します。

この表はまた、ジョブが各バケットで分析できるデータ量についての洞察を提供します。分類可能なオブジェクトとは、サポートされているAmazon S3ストレージクラスを使用し、サポートされているファイルまたはストレージフォーマットのファイル名拡張子を持つオブジェクトです。テーブルは、バケット内のオブジェクトを定期的に分析するように既存のジョブが設定されているかどうかも示します。

このテーブルの説明を以下に示します。

- 機密性 – 自動機密データ検出が有効になっている場合のバケットの現在の機密性スコアを示します。
- 分類可能なオブジェクト– このフィールド は、ジョブがバケット内で分析できるオブジェクトの合計数を示します。
- 分類可能なサイズ – このフィールドは、ジョブがバケット内で分析できるすべてのオブジェクトの合計ストレージサイズを示します。

  バケットに圧縮オブジェクトが保存されている場合、この値は解凍後のオブジェクトの実際のサイズを反映しません。バケットでバージョニングが有効化されている場合、この値は、バケット内の各オブジェクトの最新バージョンのストレージサイズに基づきます。
- モニタリングされている- のフィールドは、バケット内のオブジェクトを毎日、毎週、または毎月ベースで定期的に分析するように既存のジョブが設定されているかどうかを示します。

  このフィールドの値が はいの場合、バケットが定期的なジョブに明示的に含まれるか、バケットが過去 24 時間以内の定期的なジョブの基準に一致したことになります。さらに、それらのジョブの少なくとも 1 つのステータスは キャンセルされません。Macie は毎日ベースでこのデータを更新します。

警告アイコン⚠ が バケットの名前の横に表示される場合、Macie はバケットまたはバケットのオブジェクトへのアクセスが許可されません。これは、ジョブがバケット内のオブジェクトを分析できなくなることを意味します。問題を調査するには、Amazon S3 内のバケットのポリシーとアクセス許可の設定を確認します。例えば、バケットには制限があるバケットポリシーが設定されている場合があります。詳細については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。

ジョブのバケット基準を絞り込むには、フィルターオプションを使用して、基準の条件を追加、変更、または削除します。Macie は、変更を反映するようにテーブルを更新します。

初回実行: 既存の S3 オブジェクト

機密データ検出ジョブを使用して、S3 バケット内のオブジェクトの継続的な増分分析を実行できます。ジョブを定期的に実行するように設定した場合、Macie はこれを自動的に実行します。各実行は、前の実行後に作成または変更されたオブジェクトのみを分析します。既存のオブジェクトを含めるオプションでは、最初の増分の開始点を選択します。

- ジョブの作成終了直後に、既存のオブジェクトをすべて分析するには、このオプションのチェックボックスをオンにします。
- ジョブを作成した後、最初の実行前に作成または変更されたオブジェクトのみを分析するには、このオプションのチェックボックスをオフにします。

  このチェックボックスをオフにすると、データをすでに分析し、定期的に分析を続ける場合に役立ちます。たとえば、以前は別のサービスやアプリケーションを使用してデータを分類していたが、最近Macieを使用し始めた場合、このオプションを使用することで、不必要なコストや分類データの重複を発生させることなく、データの検出と分類を継続できるようになります。

定期ジョブの後続の実行ごとに、前の実行後に作成または変更されたオブジェクトのみが自動的に分析されます。

定期的なジョブと 1 回限りのジョブの両方について、特定の時間の前後または特定の時間範囲の間に作成または変更されたオブジェクトのみを分析するためのジョブを設定することもできます。これを行うには、オブジェクトの最終更新日を使用する object criteria (オブジェクト基準) を追加します。

サンプリング深度

このオプションでは、機密データ検出ジョブで分析する適格な S3 オブジェクトのパーセンテージを指定します。適格なオブジェクトとは、サポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を持つオブジェクトを有し、ジョブに指定するその他の条件を満たすオブジェクトです。

この値が 100% 未満の場合、Macie は、分析する適格なオブジェクトをランダムに選択し、指定されたパーセンテージまで、それらのオブジェクトのすべてのデータを分析します。例えば、10,000 個のオブジェクトを分析するようにジョブを設定し、サンプリング深度を 20% に指定した場合、Macie はジョブの実行時にランダムに選択された対象オブジェクトを約 2,000 個分析します。

ジョブのサンプリング深度を下げると、コストを削減し、ジョブの所要時間を短縮できます。これは、オブジェクト内のデータに高い一貫性があり、各オブジェクトではなく S3 バケットに機密データを保存するかどうかを判断する場合に便利です。

このオプションは、分析される バイトのパーセンテージではなく、分析される オブジェクトのパーセンテージを制御することに注意してください。100% 未満のサンプリング深度を入力すると、Macie は選択した各オブジェクトのデータのパーセンテージではなく、選択した各オブジェクトのすべてのデータを分析します。

S3 オブジェクト基準

機密データ検出ジョブの範囲を微調整するために、Macieがジョブの分析からどのS3オブジェクトを含むか、または除外するかを決定するカスタム基準を定義することもできます。これらの基準は、S3 オブジェクトのプロパティから派生する 1 つ以上の条件で設定されます。条件は、分析するジョブを設定するすべての S3 バケットのオブジェクトに適用されます。バケットにオブジェクトの複数のバージョンが保存されている場合、条件はオブジェクトの最新バージョンに適用されます。

複数の条件をオブジェクト基準として定義する場合、Macie は AND ロジックを使用して条件を結合します。また、除外条件は 含む条件よりも優先されます。たとえば、.pdf ファイル名拡張子を持つオブジェクトを含めて、5 MB を超えるオブジェクトを除外すると、オブジェクトが 5 MB を超えない限り、ジョブは .pdf ファイル名拡張子を持つ任意のオブジェクトを分析します。

S3 オブジェクトの次のプロパティのいずれかから派生する条件を定義できます。

ファイル名拡張子

これは S3 オブジェクトのファイル名拡張子に関連します。このタイプの条件を使用して、ファイルタイプに基づいてオブジェクトを含めるか除外することができます。複数のタイプのファイルに対してこれを行うには、各タイプのファイル名拡張子を入力し、各エントリをカンマで区切ります。次に例を示します: **`docx,pdf,xlsx`**。条件の値として複数のファイル名拡張子を入力すると、Macie は OR ロジックを使用して値を結合します。

values (値) では、大文字と小文字が区別されることに注意してください。また、Macie はこのタイプの条件での部分的な値またはワイルドカード文字の使用をサポートしていません。

Macie が分析できるファイルのタイプの詳細については、サポートされているファイルおよびストレージ形式を参照してください。

最終更新日時

これは、Amazon S3 の 最終更新日時フィールドに関連します。Amazon S3 では、このフィールドには S3 オブジェクトが作成された日時、または最後に変更された日時のいずれか最新の日時が保存されます。

機密データ検出ジョブでは、この条件には、特定の日付、特定の日時、または唯一の時間範囲を指定できます。

- 特定の日付または日時の後に最後に変更されたオブジェクトを分析するには、From フィールドに値を入力します。
- 特定の日付または日時より前に最後に変更されたオブジェクトを分析するには、To フィールドに値を入力します。
- 特定の時間範囲の間に最後に変更されたオブジェクトを分析するには、From フィールドを使用して、時間範囲内の最初の日付または日時の値を入力します。To フィールドを使用して、時間範囲内の最後の日付または日時の値を入力します。
- 特定の 1 日の任意の時刻で最後に変更されたオブジェクトを分析するには、From フィールドに日付を入力します。To フィールドに次の日の日付を入力します 次に、両方の時間フィールドが空白であることを確認します。(Macie は空白の時間フィールドを `00:00:00` として扱います。) 例えば、2023 年 8 月 9 日に変更されたオブジェクトを分析するには、**`2023/08/09`**From date フィールドに を入力し、To date **`2023/08/10`** フィールドに を入力し、どちらの時間フィールドにも値を入力しないでください。

協定世界時 (UTC) に任意の時間値を入力し、24 時間表記を使用します。

プレフィックス

これは、Amazon S3 の キーフィールドに関連します。Amazon S3 では、このフィールドには、オブジェクトのプレフィックスを含む S3 オブジェクトの名前が保存されます。プレフィックスは、バケット内のディレクトリパスと類似しています。これにより、類似ファイルをファイルシステム上のフォルダにまとめて保存する場合と同様に、バケット内の類似オブジェクトをまとめてグループ化できます。Amazon S3 のオブジェクトのプレフィックスとフォルダの詳細については、Amazon Simple Storage Service ユーザーガイドのフォルダを使用して Amazon S3 コンソールでオブジェクトを整理するを参照してください。

このタイプの条件を使用して、キー (名前) が特定の値で始まるオブジェクトを含めるか除外することができます。例えば、キーが で始まるすべてのオブジェクトを除外するにはAWSLogs、プレフィックス条件の値**`AWSLogs`**として を入力し、 を除外を選択します。

条件の値として複数のプレフィックスを入力すると、Macie は OR ロジックを使用して値を結合します。例えば、条件の値**AWSLogs2**として **AWSLogs1**と を入力すると、キーが AWSLogs1 または AWSLogs2 で始まるオブジェクトは条件の基準と一致します。

プレフィックス条件で値を入力するときは、以下の点に注意してください。

- 値は大文字と小文字が区別されます。
- Macie は、これらの値でのワイルドカード文字の使用をサポートしていません。
- Amazon S3 では、オブジェクトのキーには、オブジェクトを保存するバケットの名前は含まれません。このため、これらの値にはバケット名を指定しないでください。
- プレフィックスに区切り文字が含まれている場合は、値に区切り文字を含めます。例えば、キーが /eventlogs で始まるすべてのオブジェクトの条件を定義する**AWSLogs/eventlogs**には、 と入力します。 AWSLogsMacie は、スラッシュ (/) であるデフォルトの Amazon S3 区切り文字とカスタム区切り文字をサポートしています。

また、オブジェクトが条件の条件に一致するのは、オブジェクトのキーの最初の文字から入力した値と完全に一致する場合だけであることに注意してください。また、Macieは、オブジェクトのファイル名を含め、オブジェクトの完全な キー値に条件を適用します。

例えば、オブジェクトのキーが AWSLogs/eventlogs/testlog.csv で、条件に次のいずれかの値を入力すると、オブジェクトは条件の基準に一致します。

- **AWSLogs**
- **AWSLogs/event**
- **AWSLogs/eventlogs/**
- **AWSLogs/eventlogs/testlog**
- **AWSLogs/eventlogs/testlog.csv**

ただし、 と入力すると**eventlogs**、オブジェクトは条件と一致しません。条件の値にはキー AWSLogs/ の最初の部分は含まれません。同様に、 **awslogs**を入力しても、大文字と小文字の違いにより、オブジェクトは条件に一致しない。

ストレージサイズ

これは、Amazon S3 の サイズフィールドに関連します。Amazon S3 では、このフィールドは S3 オブジェクトの合計ストレージサイズを示します。オブジェクトが圧縮ファイルの場合、この値は解凍後のファイルの実際のサイズを反映しません。

このタイプの条件を使用して、特定のサイズより小さい、特定のサイズより大きい、または特定のサイズ範囲内にあるオブジェクトを含めるか除外することができます。Macie は、圧縮ファイ

ルやアーカイブファイル、およびそれらに含まれるファイルなど、すべてのタイプのオブジェクトにこの条件を適用します。サポートされている各フォーマットのサイズベースの制限については、Amazon Macie クォータを参照してください。

タグ

S3オブジェクトに関連付けられたタグ。タグは、S3 オブジェクトを含む特定のタイプの AWS リソースを定義して割り当てることができるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。S3 オブジェクトのタグ付けの詳細については、Amazon Simple Storage Service ユーザーガイドのタグを使用してストレージを分類するを参照してください。

機密データ検出ジョブの場合、このタイプの条件を使用して、特定のタグを持つオブジェクトを含めるか除外できます。これは、特定のタグキー、または特定のタグキーとタグ値 (ペア) です。条件の値として複数のタグを指定すると、Macie は OR ロジックを使用して値を結合します。例えば、ある条件のタグキーとして、**`Project1`** と **`Project2`** を指定した場合、Project1またはProject2のタグキーを持つオブジェクトが、条件と一致します。

タグのキーと値は大文字と小文字が区別されることに注意してください。また、Macie はこのタイプの条件での部分的な値またはワイルドカード文字の使用をサポートしていません。

機密データ検出ジョブの作成

Amazon Macie を使用すると、機密データ検出ジョブを作成して実行し、Amazon Simple Storage Service (Amazon S3) 汎用バケット内の機密データの検出、ログ記録、およびレポートを自動化できます。機密データ検出ジョブは、Amazon S3 オブジェクト内の機密データを検出して報告するために Macie が実行する一連の自動処理および分析タスクです。分析が進むにつれて、Macie は検出した機密データと実行した分析に関する詳細なレポートを作成します。機密データ検出結果では、Macie が個々の S3 オブジェクト内で検出した機密データを報告し、機密データ検出結果では、個々の S3 オブジェクトの分析に関するログ詳細を記録します。詳細については、「ジョブの統計と結果の確認」を参照してください。

ジョブを作成するときは、まず、ジョブの実行時に Macie が分析するオブジェクトを保存する S3 バケットを指定します。これは、選択した特定のバケット、または特定の条件に一致するバケットです。次に、ジョブを 1 回実行するか、毎日、毎週、または毎月ベースで実行するか、その頻度を指定します。また、オプションを選択して、ジョブの分析範囲を絞り込むこともできます。オプションには、タグやプレフィックスなどの S3 オブジェクトのプロパティから派生するカスタム基準やオブジェクト最終更新日時があります。

ジョブのスケジュールと範囲を定義したら、使用するマネージドデータ識別子とカスタムデータ識別子を指定します。

- マネージドデータ識別子は、クレジットカード番号、 AWS シークレットアクセスキー、特定の国や地域のパスポート番号など、特定のタイプの機密データを検出するように設計された一連の組み込み基準と手法です。これらの識別子は、複数タイプの認証情報データ、財務情報、個人健康情報 (PHI)、個人を特定できる情報 (PII) など、多くの国や地域で増加している大規模な機密データタイプのリストを検出できます。詳細については、マネージドデータ識別子の使用を参照してください。
- カスタムデータ識別子は、機密データを検出するために定義する基準のセットです。カスタムデータ識別子を使用すると、従業員 ID、顧客アカウント番号、内部データの分類など、組織の特定のシナリオ、知的財産、または専有データを反映する機密データを検出できます。Macie が提供するマネージドデータ識別子を補足できます。詳細については、「カスタムデータ識別子の構築」を参照してください。

次に、オプションで、使用する許可リストを選択します。許可リストは、Macie に無視させたいテキストまたはテキストパターン (通常、特定のシナリオや環境における機密データの例外 — 例えば、公開されている組織の代表者名や電話番号、または組織がテストに使用するサンプルデータなど) を指定します。詳細については、許可リストでの機密データの例外の定義を参照してください。

これらのオプションの選択が完了したら、ジョブの名前やジョブの詳細など、ジョブの一般的な設定を入力できます。その後、ジョブを確認して保存します。

タスク

- 開始する前に
- ステップ 1: S3 バケットを選択する
- ステップ 2: S3 バケットの選択または基準を確認する
- ステップ 3: スケジュールを定義し、範囲を絞り込む
- ステップ 4: マネージドデータ識別子を選択する
- ステップ 5: カスタムデータ識別子を選択する
- ステップ 6: 許可リストの選択
- ステップ 7: 全般設定を入力
- ステップ 8: 確認して作成

開始する前に

ジョブを作成する前に、次のステップを実行することをお勧めします。

- 機密データ検出の結果用のリポジトリを設定していることを確認します。これを行うには、Amazon Macie コンソールのナビゲーションペインで 検出結果 を選択します。これらの設定の詳細については、機密データ検出結果の保存と保持を参照してください。
- ジョブで使用するカスタムデータ識別子を作成します。この方法の詳細は、カスタムデータ識別子の構築を参照してください。
- ジョブで使用する許可リストを作成します。この方法の詳細は、許可リストの作成と管理を参照してください。
- 暗号化された S3 オブジェクトを分析する場合は、Macie が正しい暗号化キーにアクセスして使用できることを確認してください。詳細については、暗号化された S3 オブジェクトの分析を参照してください。
- 制限があるバケットポリシーを持つ S3 バケット内のオブジェクトを分析する場合は、Macie がオブジェクトにアクセス許可されているか確認してください。詳細については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。

ジョブ作成の前にこれらの処理を行えば、ジョブ作成が効率化され、確実にジョブが対象データを分析できるようになります。

ステップ 1: S3 バケットを選択する

ジョブを作成するときの最初のステップは、ジョブの実行時に Macie が分析するオブジェクトを保存する S3 バケットを指定することです。このステップでは、2 つのオプションがあります。

- 特定のバケットを選択する – このオプションでは、分析する各 S3 バケットを明示的に選択します。次に、ジョブが実行されると、選択したバケット内のオブジェクトのみが分析されます。
- バケット条件を指定する – このオプションでは、分析する S3 バケットを決定するランタイム条件を定義します。基準は、バケットプロパティから派生する 1 つ以上の条件で設定されます。次に、ジョブが実行されると、基準に一致するバケットが識別され、それらのバケット内のオブジェクトが分析されます。

これらのオプションの詳細な情報については、ジョブの範囲のオプションを参照してください。

以下のセクションでは、各オプションの選択および設定の手順について説明します。目的のオプションのセクションを選択します。

特定のバケットを選択する

分析する各 S3 バケットを明示的に選択することを選択した場合、Macie は現在の の汎用バケットの完全なインベントリを提供します AWS リージョン。その後、このインベントリを使用して、ジョブの 1 つ以上のバケットを選択できます。このインベントリの詳細については、特定のバケットを選択するを参照してください。

お客様が組織の Macie 管理者である場合、インベントリには、組織のメンバーアカウントによって所有されているバケットが含まれます。これらのバケットは最大 1,000 個まで選択でき、最大 1,000 個のアカウントで設定されます。

ジョブの特定の S3 バケットを選択するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブを選択します。
3. ジョブの作成を選択します。
4. S3 バケットを選択するページで、特定のバケットを選択する を選択します。Macie は、現在のリージョンのアカウントのすべての汎用バケットのテーブルを表示します。
5. S3 バケットを選択 のセクションで、必要に応じてリフレッシュ を選択して、Amazon S3 から最新バケットメタデータを取得します。

   情報アイコン が バケット名の横に表示された場合、これを行うことをお勧めします。このアイコンは、Macie が daily refresh cycle (毎日の更新サイクル) の一部として Amazon S3 からバケットとオブジェクトメタデータをおそらく最後に取得した後の過去 24 時間にバケットが作成されたことを示します。
6. テーブルで、ジョブで分析する各バケットのチェックボックスをオンにします。

> **Tip**
>
> - 特定のバケットをより簡単に検索するには、テーブルの上にあるフィルターボックスにフィルター条件を入力します。列見出しを選択して、テーブルを並べ替えることもできます。
> - バケット内のオブジェクトを定期的に分析するジョブを既に設定したかを判断するには、ジョブによるモニタリング フィールドを参照します。はい がフィールドに表示

される場合、バケットは定期的なジョブに明示的に含まれるか、あるいは、バケットが過去 24 時間以内の定期的なジョブの条件に一致したことになります。さらに、それらのジョブの少なくとも 1 つのステータスは キャンセルされません。Macie は毎日ベースでこのデータを更新します。

- 既存の定期的な設定か、あるいは、直近の 1 回限りのバケット内オブジェクト分析ジョブになっているかを判断するには、最新のジョブ実行 フィールドを参照します。そのジョブの追加の情報については、バケットの詳細を参照してください。
- バケットの詳細を表示するには、バケットの名前を選択します。ジョブ関連情報に加えて、詳細パネルには、バケットのパブリックアクセス設定など、バケットに関する統計やその他の情報が表示されます。このデータの詳細については、S3 バケットインベントリを確認するを参照してください。

7. バケットの選択が終了したら、次へを選択します。

次のステップでは、選択内容を確認します。

バケット基準を指定する

分析する S3 バケットを決定するランタイム条件を指定することを選択した場合、Macie は条件内の個々の条件のフィールド、演算子、値を選択するのに役立つオプションを提供します。これらのオプションの詳細については、S3 バケット基準の指定を参照してください。

ジョブの S3 バケット条件を指定するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブを選択します。
3. ジョブの作成を選択します。
4. S3 バケットを選択するページで、バケット基準を指定する を選択します。
5. バケット基準を指定する の下で、以下を実行して、条件を基準に追加します。

   a. フィルターボックスにカーソルを置き、条件に使用するバケットプロパティを選択します。
   b. 最初のボックスで、条件の演算子 (等しい または 等しくない を選択します。
   c. 次のボックスに、プロパティの値を 1 つ以上入力します。

      バケットプロパティのタイプと性質に応じて、Macie は値を入力するためのさまざまなオプションを表示します。たとえば、有効なアクセス許可 プロパティを選択した場合、Macie は選択する値のリストを表示します。アカウント ID プロパティを選択した場合、Macie

は、1 つ以上の AWS アカウント ID を入力できるテキストボックスを表示します。テキストボックスに複数の値を入力するには、各値を入力し、各エントリをカンマで区切ります。

d. 適用 を選択します。Macie は条件を追加し、フィルターボックスの下に表示します。

デフォルトでは、Macie は include ステートメントで条件を追加します。これは、ジョブが条件に一致するバケット内のオブジェクトを分析する含めるように設定されていることを意味します 。条件に一致するバケットをスキップする (除外する) には、条件で含める を選択し、次に 除外する を選択します。

e. 基準に追加する追加の条件ごとに、上記のステップを繰り返します。

6. 基準をテストするには、条件の結果をプレビューするセクションを展開します。このセクションでは、現在条件に一致する汎用バケットの表を表示します。
7. 基準を絞り込むには、以下のいずれかを行ってください。

- 条件を削除するには、条件で X を選択します。
- 条件を変更するには、条件で X を選択してその条件を削除します。次に、正しい設定を持つ条件を追加します。
- すべての条件を削除するには、フィルターをクリアを選択します。

Macie は、基準の結果のテーブルを更新して、変更を反映します。

8. バケット基準の指定が終了したら、次へを選択します。

次のステップでは、基準を確認します。

ステップ 2: S3 バケットの選択または基準を確認する

このステップでは、前のステップで正しい設定を選択したことを検証します。

- バケット選択の確認 ジョブに特定の S3 バケットを選択した場合は、バケットのテーブルを確認し、必要に応じてバケットの選択を変更します。このテーブルは、ジョブの分析の予測範囲とコストに関する洞察を提供します。データは、バケットに現在保存されているオブジェクトのサイズとタイプに基づいています。

  推定コスト フィールドは、S3 バケット内のオブジェクトを分析するための合計推定コスト (米ドル単位) を示します。各見積もりは、ジョブがバケット内で分析する非圧縮データの予測量を反映します。オブジェクトが圧縮ファイルまたはアーカイブファイルである場合、見積もりではファイルが 3:1 の圧縮率を使用し、ジョブはすべての抽出されたファイルを分析できると仮定します。詳細については、ジョブのコストの予測とモニタリングを参照してください。

- バケット条件を確認 ジョブのバケット条件を指定した場合は、それぞれの条件がその条件になっているか確認します。基準を変更するには、前へ を選択し、前のステップのフィルターオプションを使用して正しい条件を入力します。終了したら、次へを選択します。

設定の確認と検証が終了したら、次へ を選択します。

ステップ 3: スケジュールを定義し、範囲を絞り込む

このステップでは、ジョブを 1 回実行するか、毎日、毎週、または毎月ベースで実行するか、その頻度を指定します。また、さまざまなオプションを選択して、ジョブの分析範囲を絞り込みます。これらのオプションについては、ジョブの範囲のオプションを参照してください。

スケジュールを定義し、ジョブの範囲を絞り込むには

1. 範囲を絞り込む ページで、ジョブを実行する頻度を選択します。
   - ジョブを 1 回だけ実行するには、作成終了直後に、1 回限りのジョブを選択します。
   - ジョブを繰り返しベースで定期的に実行するには、スケジュールされたジョブを選択します。更新頻度では、ジョブを毎日、毎週、または毎月実行するかを選択します。次に、既存のオブジェクトを含めるオプションを使用して、ジョブの初回実行の範囲を定義します。
     - ジョブの終了直後に、既存のすべてのオブジェクトを分析するには、このチェックボックスをオンにします。後続の実行ごとに、前の実行後に作成または変更されたオブジェクトのみが分析されます。
     - このチェックボックスをオフにすると、既存のすべてのオブジェクトの分析がスキップされます。ジョブの最初の実行では、ジョブの作成終了後で最初の実行開始前に作成または変更されたオブジェクトのみが分析されます。後続の実行ごとに、前の実行後に作成または変更されたオブジェクトのみが分析されます。

       このチェックボックスをオフにすると、データをすでに分析し、定期的に分析を続ける場合に役立ちます。例えば、以前他のサービスまたはアプリケーションを使ってデータを分類し、最近 Macie を使用し始めた場合は、このオプションを使用すると、不要なコストや重複した分類データを発生させずにデータの検出と分類を継続することができます。
2. (オプショナル) ジョブで分析するオブジェクトのパーセンテージを指定するには、サンプリング深度ボックスにパーセンテージを入力します。

   この値が 100% 未満の場合、Macie は、分析するオブジェクトをランダムに選択し、指定されたパーセンテージまで、それらのオブジェクトのすべてのデータを分析します。デフォルト値は 100% です。

3. (オプショナル) ジョブの分析に含めるか除外する S3 オブジェクトを決定する特定の基準を追加するには、追加の設定セクションを展開し、次に基準を入力します。これらの条件は、オブジェクトのプロパティから派生する個別の条件で設定されます。

   - 分析するため特定の条件を満たすオブジェクトを含め 、条件のタイプと値を入力し、次に 含めるを選択します。
   - 特定の条件を満たすオブジェクトをスキップする (除外する) には、条件のタイプと値を入力し、次に 除外するを選択します。

   必要な 含めるまたは 除外する条件ごとに、このステップを繰り返します。

   複数の条件を入力した場合、すべての除外条件は、適用する条件より優先されます。たとえば、.pdf ファイル名拡張子を持つオブジェクトを含めて、5 MB を超えるオブジェクトを除外すると、オブジェクトが 5 MB を超えない限り、ジョブは .pdf ファイル名拡張子を持つ任意のオブジェクトを分析します。

4. 終了したら、次へ を選択します。

ステップ 4: マネージドデータ識別子を選択する

このステップでは、S3 オブジェクトを分析するときにジョブで使用するマネージドデータ識別子を指定します。これには 2 つのオプションがあります。

- 推奨設定を使用 このオプションでは、ジョブに推奨するマネージドデータ識別子のセットを使用して、ジョブにより S3 オブジェクトが分析されます。このセットは、一般的なカテゴリとタイプの機密データを検出するように設計されています。現在セット内にあるマネージドデータ識別子の詳細なリストを確認するには、ジョブに推奨されるマネージドデータ識別子 を参照してください。マネージドデータ識別子がセットに追加または削除されるたびに、そのリストは更新されます。
- カスタム設定を使用 このオプションでは、選択したマネージドデータ識別子を使用して、ジョブにより S3 オブジェクトが分析されます。これは、現在利用可能なマネージドデータ識別子のすべてまたは一部のみとなる可能性があります。また、マネージドデータ識別子を使用しないようジョブを設定することもできます。代わりに、次のステップで選択するカスタムデータ識別子をジョブに使用します。現在利用可能なマネージドデータ識別子の一覧を確認するには、クイックリファレンス: Amazon Macie マネージドデータ識別子 を参照してください。新しいマネージドデータ識別子がリリースされるたびに、そのリストが更新されます。

いずれかのオプションを選択すると、Macie はマネージドデータ識別子のテーブルを表示します。テーブルの 機密データのタイプ フィールドで、マネージドデータ識別子に一意の識別子 (ID) を指定します。この ID は、マネージドデータ識別子によって検出される機密データのタイプを示します。例えば、米国のパスポート番号は USA_PASSPORT_NUMBER、クレジットカード番号は CREDIT_CARD_NUMBER、PGP プライベートキーは PGP_PRIVATE_KEY です。特定の識別子をよりすばやく検索するには、機密データのカテゴリまたはタイプでテーブルを並べ替えたり、フィルタリングします。

ジョブのマネージドデータ ID を選択するには

1. マネージドデータ識別子を選択する ページの マネージドデータ識別子のオプション のところで、次のいずれかを実行します。

   - ジョブに推奨するマネージドデータ識別子のセットを使用するには、お勧め を選択します。

     このオプションを選択し、ジョブを複数回実行するように設定した場合、各実行では、実行の開始時に推奨セットにあるすべてのマネージドデータ識別子が自動的に使用されます。これには、セットに追加した新しいマネージドデータ識別子も含まれます。セットから削除し、ジョブに推奨しなくなったマネージドデータ識別子は含まれません。

   - 選択した特定のマネージドデータ識別子のみを使用するには、カスタム を選択してから 特定のマネージドデータ識別子を使用するを選択します。次にテーブルで、ジョブに使用するマネージドデータ識別子のチェックボックスをオンにします。

     このオプションを選択し、ジョブを複数回実行するように設定した場合、各実行では選択したマネージドデータ識別子のみを使用します。つまり、ジョブは実行のたびにこれらの同じマネージドデータ識別子を使用します。

   - Macie が現在提供しているマネージドデータ識別子をすべて使用するには、カスタム を選択してから 特定のマネージドデータ識別子を使用するを選択します。次にテーブルで、選択列の見出しにあるチェックボックスをオンにして、すべての行を選択します。

     このオプションを選択し、ジョブを複数回実行するように設定した場合、各実行では選択したマネージドデータ識別子のみを使用します。つまり、ジョブは実行のたびにこれらの同じマネージドデータ識別子を使用します。

   - マネージドデータ識別子を一切使用せず、カスタムデータ識別子のみを使用するには、カスタム を選択してから マネージドデータ識別子を一切使用しないを選択します。それから次のステップで、使用するカスタムデータ識別子を選択します。

2. 終了したら、次へ を選択します。

ステップ 5: カスタムデータ識別子を選択する

このステップでは、S3 オブジェクトを分析するときにジョブで使用する カスタムデータ識別子を選択します。ジョブでは、ジョブで使用するために設定したマネージドデータ識別子に加えて、選択された識別子が使用されます。カスタムデータ識別子の詳細については、カスタムデータ識別子の構築を参照してください。

ジョブのカスタムデータ識別子を選択するには

1. カスタムデータ識別子を選択するページで、ジョブで使用するカスタムデータ識別子ごとに、チェックボックスをオンにします。カスタムデータ識別子は最大 30 個まで選択できます。

   > **Tip**
   >
   > カスタムデータ識別子を選択する前にその識別子を確認ま
   > たはテストするには、識別子の名前の横にあるリンクアイコ
   > ン
   > を
   > 選択します。Macie は、識別子の設定を表示するページを開きます。
   > このページを使用して、サンプルデータを用いて識別子をテストすることもできます。
   > これを行うには、最大 1,000 文字のテキストを サンプルデータ ボックスに入力し、次
   > に Submit (送信) を選択します。Macie は識別子を使用してサンプルデータを評価し、
   > 一致の数をレポートします。

2. カスタムデータ識別子の選択が終了したら、次へ を選択します。

ステップ 6: 許可リストの選択

このステップでは、S3 オブジェクトを分析するときにジョブで使用する許可リストを選択します。許可リストの詳細については、許可リストでの機密データの例外の定義 を参照してください。

ジョブの許可リストを選択する

1. 許可リストの選択 ページで、ジョブで使用する許可リストのチェックボックスをオンにします。リストは 10 個まで選択できます。

   > **Tip**
   >
   > 許可リストを選択する前にそのリストを確認するには、リスト名の横にあるリンクアイコ

ン を選択します。Macie は、リストの設定を表示するページを開きます。
リストで正規表現 (正規表現)を指定する場合は、このページを使用してサンプルデータでその正規表現を確認することもできます。これを行うには、テキスト (最大 1,000 文字) を サンプルデータ ボックスに入力し、次に テスト を選択します。Macie は正規表現を使用してサンプルデータを評価し、一致の数をレポートします。

2. 許可リストの選択が完了したら、次へ を選択します。

ステップ 7: 全般設定を入力

このステップでは、ジョブの名前と、必要に応じてジョブの詳細を入れます。ジョブにタグを割り当てることもできます。タグは、特定のタイプの AWS リソースを定義して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを分類および管理できます。詳細については、Amazon Macie リソースへのタグ付けを参照してください。

ジョブの全般設定を入力する

1. 名前と説明を入力 ページで、ジョブの名前を ジョブ名 ボックスに入力します。名前には最大 500 文字を含めることができます。
2. (オプショナル) ジョブの説明では、ジョブの簡単な説明を入力します。説明には最大 200 文字を含めることができます。
3. (オプショナル) タグ で タグを追加 を選択し、ジョブに割り当てるタグを 50 個まで入力できます。
4. 終了したら、次へ を選択します。

ステップ 8: 確認して作成

この最後のステップでは、ジョブの設定設定を確認し、その設定が正しいことを検証します。これは重要なステップです。ジョブ作成後は、これらの設定を変更することはできません。これにより、実施するデータプライバシーと保護の監査または調査に関する機密データの調査結果と検出結果のイミュータブルな履歴を確実に保持できます。

ジョブの設定に応じて、ジョブを 1 回実行した場合の推定コスト (米ドル単位) も確認できます。ジョブで特定の S3 バケットを選択した場合、見積もりは、選択したバケット内のオブジェクトのサイズとタイプ、およびジョブが分析できるデータの量に基づきます。ジョブのバケット基準を指定し

た場合、見積もりは、現在基準に一致する最大 500 個までのバケット内のオブジェクトのサイズとタイプ、およびジョブが分析できるデータの量に基づきます。この見積もりの詳細については、ジョブのコストの予測とモニタリングを参照してください。

ジョブを確認して作成するには

1. 確認して作成するページで、各設定を確認し、それが正しいことを検証します。設定を変更するには、設定が含まれるセクションで Edit (編集) を選択し、次に正しい設定を入力します。ナビゲーションタブを使用して、設定が含まれるページに移動することもできます。
2. 設定の確認が完了したら、提出を選択して、ジョブを作成して保存します。Macie は設定を確認し、対処すべき問題があれば通知します。

   > **Note**
   >
   > 機密データの検出結果のリポジトリを設定していない場合、Macie は警告を表示し、ジョブを保存しません。この問題に対処するには、機密データの検出結果のリポジトリセクションで 設定を選択します。次に、リポジトリの設定設定を入力します。この方法の詳細は、機密データ検出結果の保存と保持を参照してください。設定を入力したら、確認して作成 ページに戻り、そのページの 機密データ検出結果のリポジトリセクションでリフレッシュ  を選択します。
   > それは推奨されませんが、リポジトリ要件を一時的に上書きしてジョブを保存することができます。これを行うと、ジョブの検出結果を失うリスクがあります。Macie は 90 日間だけ結果を保持します。要件を一時的に上書きするには、上書きオプションのチェックボックスをオンにします。

3. Macie が対処すべき課題を通知した場合は、問題に対処し、もう一度 提出を選択して、ジョブを作成して保存します。

ジョブの実行頻度を 1 回限りまたは毎日ベースに設定しているか、週の現在の曜日または月の現在の日付に設定している場合、Macie はジョブを保存した直後にジョブの実行を開始します。それ以外の場合、Macie は週の指定された曜日または月の指定された日付にジョブを実行する準備をします。ジョブをモニタリングするには、ジョブのステータスをチェックできます。

機密データ検出ジョブの統計と結果の確認

機密データ検出ジョブを実行すると、Amazon Macie はそのジョブの特定の統計データを自動的に計算してレポートします。たとえば、Macie は、ジョブが実行された回数、および現在の実行中にジョブがまだ処理をしていない Amazon Simple Storage Service (Amazon S3) オブジェクトのおおよその数をレポートします。Macie は、ログイベント、機密データの調査結果、機密データの検出結果など、ジョブのいくつかのタイプの結果も生成します。

トピック

機密データ検出ジョブの結果のタイプ

機密データ検出ジョブの進行に伴い、Amazon Macie はそのジョブの次のタイプの結果を生成します。

ログイベント

これは、ジョブの実行中に発生したイベントのレコードです。Macie は、特定のイベントのデータを自動的にログに記録し、Amazon CloudWatch Logs に発行します。これらのログのデータは、ジョブの実行を開始または停止した正確な日時など、ジョブの進行状況またはステータスに対する変更のレコードを提供します。データは、ジョブの実行中に発生したアカウントレベルまたはバケットレベルのエラーに関する詳細も提供します。

ログイベントは、ジョブをモニタリングして、ジョブが目的のデータを分析するのを妨げた問題に対処するのに役立ちます。ジョブがランタイム基準を使用して、分析する S3 バケットを決定する場合、ログイベントは、ジョブの実行時に条件に S3 バケットが一致したかどうか、およびどの S3 バケットが一致したかを判断するのに役立ちます。

Amazon CloudWatch コンソールまたは Amazon CloudWatch Logs API を使用して、ログイベントにアクセスできます。ジョブのログイベントに移動しやすくするために、Amazon Macie コンソールはログイベントへのリンクを提供しています。詳細については、ジョブのモニタリングを参照してください。

機密データの調査結果

これは Macie が S3 オブジェクトで検出した機密データのレポートです。各調査結果には、重要度評価と次のような詳細が示されます。

- Macie が機密データを検出した日時。
- Macie が検出した機密データのカテゴリとタイプ。
- Macie が検出した機密データのタイプごとの出現回数。
- 調査結果を生成したジョブの一意の識別子。
- 影響を受けた S3 バケットおよびオブジェクトに関する名前、パブリックアクセス設定、暗号化タイプ、およびその他の情報。

影響を受けた S3 オブジェクトのファイルタイプまたはストレージ形式によっては、Macie が見つけた機密データの最大 15 までの出現の場所も詳細に含まれます。位置データを報告するために、機密データの検出結果は、標準化された JSON スキーマを使用します。

機密データの調査結果には、Macie が検出した機密データは含まれません。代わりに、必要に応じてさらなる調査と修復に使用できる情報が提供されます。

Macie は機密データの調査結果を 90 日間保存します。Amazon Macie コンソールまたは Amazon Macie API を使用してそれらにアクセスできます。また、他のアプリケーション、サービス、およびシステムを使用して、それらをモニタリングおよび処理することもできます。詳細については、調査結果を分析するを参照してください。

機密データの検出結果

これは、S3 オブジェクトの分析に関する詳細のログを記録するレコードです。Macie は、分析するジョブを設定するオブジェクトごとに、機密データの検出結果を自動的に作成します。これには、Macie が機密データを見つけられないために機密データの検出結果を生成しないオブジェクト、およびアクセス許可設定やサポートされていないファイルまたはストレージ形式の使用などのエラーや問題のために Macie が分析できないオブジェクトが含まれます。

Macie が S3 オブジェクト内の機密データを見つけると、、機密データの検出結果には、対応する機密データの調査結果のデータが含まれます。また、Macie がオブジェクト内で検出した機密データのタイプごとに最大 1,000 個までの出現の場所などの追加情報も提供します。例:

- Microsoft Excel ワークブック、CSV ファイル、または TSV ファイル内のセルまたはフィールドの列番号と行番号
- JSON または JSON Lines ファイル内のフィールドまたは配列へのパス
- CSV、JSON、JSON Lines、または TSV ファイル以外の非バイナリテキストファイル (HTML、TXT、XML ファイルなど) 内の行の行番号
- Adobe Portable Document Format (PDF) ファイル内のページのページ番号

- Apache Avro オブジェクトコンテナまたは Apache Parquet ファイル内のレコードのレコードインデックスとフィールドへのパス

影響を受ける S3 オブジェクトが .tar ファイルや .zip ファイルなどのアーカイブファイルである場合、機密データの検出結果には、Macie がアーカイブから抽出した個々のファイル内の機密データの出現に関する詳細な位置データも表示されます。Macie は、アーカイブファイルの機密データの調査結果にこの情報を含めません。位置データを報告するために、機密データ検出結果は標準化された JSON スキーマを使用します。

機密データの検出結果には、Macie が検出した機密データは含まれません。代わりに、データのプライバシーと保護の監査や調査に役立つ分析レコードが提供されます。

Macie は機密データの検出結果を 90 日間保存します。Amazon Macie コンソールまたは Amazon Macie API からそれらに直接アクセスすることはできません。代わりに、それを暗号化して S3 バケットに保存するように Macie を設定します。バケットは、機密データの検出結果のすべての最終的で長期的なリポジトリとして機能します。次に、オプションで、そのリポジトリ内の結果にアクセスしてクエリを実行できます。これらの設定を行う方法については、機密データ検出結果の保存と保持を参照してください。

設定を設定したら、Macie は機密データの検出結果を JSON Lines (.jsonl) ファイルに書き込み、それらのファイルを暗号化し GNU Zip (.gz) ファイルとして S3 バケットに追加します。結果に移動しやすくするために、Amazon Macie コンソールは結果へのリンクを提供しています。

機密データの調査結果と機密データの検出結果は、どちらも標準化されたスキーマに準拠しています。これは、オプションで、他のアプリケーション、サービス、およびシステムを使用して、それらをクエリ、モニタリング、および処理するのに役立ちます。

> **Tip**
>
> 機密データ検出結果をクエリして使用して潜在的なデータセキュリティリスクを分析およびレポートする方法の詳細な説明例については、 セキュリティブログのAmazon Athena と Amazon で Macie 機密データ検出結果をクエリおよび視覚化する方法 QuickSightAWS 」ブログ記事を参照してください。
> 機密データ検出結果の分析に使用できる Amazon Athena クエリのサンプルについては、 の Amazon Macie 結果分析リポジトリを参照してください GitHub。このリポジトリでは、結果を取得および復号化するように Athena を設定する手順と、結果のテーブルを作成するためのスクリプトも提供します。

機密データ検出ジョブの統計と結果の確認

個々の機密データ検出ジョブの処理統計と結果を確認するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。コンソールを使用してジョブの統計と結果を確認するには、次のステップに従います。

ジョブの処理統計にプログラムでアクセスするには、Amazon Macie API の DescribeClassificationJobオペレーションを使用します。ジョブが生成した検出結果にプログラムでアクセスするには、Amazon Macie API の ListFindingsオペレーションを使用して、`classificationDetails.jobId` フィールドのフィルター条件でジョブの一意の識別子を指定します。この方法の詳細は、フィルターの作成と調査結果への適用を参照してください。その後、GetFindingsオペレーションを使用して検出結果の詳細を取得できます。

ジョブの統計と結果を確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブ を選択します。
3. ジョブ ページで、ユーザーが確認する統計と結果を持つジョブの名前を選択します。詳細パネルには、ジョブに関する統計、設定、およびその他の情報が表示されます。
4. 詳細パネルで、次のいずれかの操作を実行します。

   - ジョブの処理統計を確認するには、パネルの 統計セクションを参照してください。このセクションには、ジョブが実行された回数や、現在の実行中にジョブがまだ処理をしていないオブジェクトのおおよその数などの統計が表示されます。
   - ジョブのログイベントを確認するには、パネルの上部にある結果を表示を選択し、ログを表示 CloudWatch を選択します。Macie は Amazon CloudWatch コンソールを開き、Macie がジョブに対して公開したログイベントのテーブルを表示します。
   - ジョブが生成したすべての機密データの調査結果を確認するには、パネルの上部で、結果を表示するを選択し、次に 調査結果を表示するを選択します。Macie は 調査結果ページを開き、ジョブのすべての結果を表示します。特定の調査結果の詳細を確認するには、調査結果を選択し、次に詳細パネルを参照します。

     > **Tip**
     >
     > 調査結果の詳細 パネルで、詳細な結果の場所フィールド内のリンクを使用して、Amazon S3 内の調査結果に対応する機密データの検出結果に移動します。

- 大きなアーカイブまたは圧縮ファイルに調査結果が適用される場合、リンクには、ファイルの検出結果を含むフォルダが表示されます。アーカイブまたは圧縮ファイルが 100 個を超える検出結果を生成する場合、それは 大きい になります。
- 小さなアーカイブまたは圧縮ファイルに調査結果が適用される場合、リンクには、ファイルの検出結果を含むファイルが表示されます。アーカイブまたは圧縮ファイルが 100 個以下の検出結果を生成する場合、それは 小さい になります。
- 別のタイプのファイルに調査結果が適用される場合、リンクには、ファイルの検出結果を含むファイルが表示されます。

- ジョブが生成したすべての機密データの検出結果を確認するには、パネルの上部で、結果を表示するを選択し、次に 分類を表示するを選択します。Macie は Amazon S3 コンソールを開き、ジョブのすべての検出結果を含むフォルダを表示します。このオプションは、Macie を S3 バケットで 機密データの検出結果を保存するように設定した後にのみ使用できます。

Amazon CloudWatch Logs を用いた機密データ検出ジョブのモニタリング

また、機密データ検出ジョブの 全体的なステータスのモニタリング に加え、ジョブの進行に伴って発生する特定のイベントをモニタリングして分析できます。これを行うには、Amazon Macie が自動的に Amazon CloudWatch Logs に発行するほぼリアルタイムのログ記録データを使用します。これらのログのデータは、ジョブの実行開始、一時停止、実行終了の正確な日時など、ジョブの進行状況またはステータスに対する変更のレコードを提供します。

ログデータは、ジョブの実行中に発生したアカウントレベルまたはバケットレベルのエラーに関する詳細も提供します。たとえば、S3 バケットのアクセス許可設定により、ジョブがバケット内のオブジェクトを分析するのを防ぐようにすると、Macie はイベントをログに記録します。イベントはいつエラーが発生したかを示し、影響を受けたバケットとバケットを所有するアカウントの両方を識別します。これらのタイプのイベントのデータは、Macie が目的のデータを分析するのを妨げたエラーの特定、調査、対処に役立ちます。

Amazon CloudWatch Logs を使用すると、複数のシステム、アプリケーション、および Macie を含むAWS のサービス からログファイルのモニタリング、保存、およびアクセスを行えます。ログデータのクエリと分析を行い、特定のイベントが発生した場合やしきい値に達したときに通知するように CloudWatch Logs を設定することもできます。また、CloudWatch Logs は、ログデータをアーカイブし、データを Amazon S3 にエクスポートする機能も提供します。CloudWatch Logs の詳細については、Amazon CloudWatch Logs ユーザーガイドを参照してください。

トピック

- 機密データ検出ジョブでのログ記録の仕組み
- 機密データ検出ジョブのログの確認
- 機密データ検出ジョブのログイベントスキーマ
- 機密データ検出ジョブのログイベントのタイプ

機密データ検出ジョブでのログ記録の仕組み

機密データ検出ジョブの実行を開始すると、Macie は Amazon CloudWatch Logs で適切なリソースを自動的に作成し、現在の AWS リージョン 内のジョブのすべてのイベントをログに記録するように設定します。Macie は、ジョブの実行時にイベントデータをこれらのリソースに自動的に発行します。アカウントの Macie サービスにリンクされたロール のアクセス許可ポリシーは、Macie がお客様に代わってこれらのタスクを実行することを許可します。CloudWatch Logs でリソースを作成または設定したり、ジョブのイベントデータをログに記録したりするために、ステップのいずれかを実行する必要はありません。

CloudWatch Logs では、ログは ロググループ に整理されます。各ロググループには ログストリーム が含まれます。各ログストリームには ログイベント が含まれます。これらの各リソースの一般的な目的は次のとおりです。

- ロググループ は、保持、モニタリング、アクセス制御について同じ設定を共有するログストリームのコレクションです。たとえば、すべての機密データ検出ジョブのログのコレクションなどです。
- ログストリーム は、同じソースを共有する一連のログイベントです。たとえば、個別の機密データ検出ジョブなどです。
- ログイベント は、アプリケーションまたはリソースによって記録されたアクティビティのレコードです。たとえば、Macie が特定の機密データ検出ジョブについて記録および発行した個別のイベントなどです。

Macie は、すべての機密データ検出ジョブのイベントを 1 つのロググループに発行し、各ジョブは、そのロググループ内に一意のログストリームがあります。ロググループには、次のプレフィックスと名前があります。

```
/aws/macie/classificationjobs
```

このロググループが既に存在する場合、Macie はそれを使用してジョブのログイベントを保存します。これは、組織で AWS CloudFormation のような自動設定を使用して、ジョブイベントに対して

事前定義された保持期間、暗号化設定、タグ、メトリクスフィルターなどのロググループを作成する場合に便利です。

このロググループが存在しない場合、Macie は新しいロググループで CloudWatch Logs が使用するデフォルト設定を用いてグループを作成します。設定には、期限切れにならない のログ保持期間が含まれます。つまり、CloudWatch Logs はログを無期限に保存します。ロググループの保持期間を変更するには、Amazon CloudWatch コンソールまたは Amazon CloudWatch Logs API を使用します。詳細については、Amazon CloudWatch Logs ユーザーガイドのロググループとログストリームの操作を参照してください。

このロググループ内で、Macie はジョブを初めて実行するときに、実行するジョブごとに一意のログストリームを作成します。ログストリームの名前は、`85a55dc0fa6ed0be5939d0408example` のようなジョブの一意の識別子であり、以下の形式になります。

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

各ログストリームには、Macie が、対応するジョブについて記録および発行したすべてのログイベントが含まれます。定期的なジョブの場合、これにはすべてのジョブの実行のイベントが含まれます。定期的なジョブのログストリームを削除すると、次回ジョブが実行されたときに Macie によってストリームが再度作成されます。1 回限りのジョブのログストリームを削除すると、復元できません。

すべてのジョブのログ記録はデフォルトで有効化されていることに注意してください。これを無効にしたり、Macie が CloudWatch Logs にジョブイベントを発行するのを防いだりすることはできません。ログを保存したくない場合は、ロググループの保持期間を 1 日のみに短縮できます。保持期間の終了時に、CloudWatch Logs はロググループから期限切れのイベントデータを自動的に削除します。

機密データ検出ジョブのログの確認

Amazon CloudWatch コンソールまたは Amazon CloudWatch Logs API を使用して、機密データ検出ジョブのログを確認できます。コンソールと API の両方は、ログデータの確認と分析に役立つように設計された機能を提供します。CloudWatch Logs の他のタイプのログデータを操作する場合と同様に、これらの機能を使用して、ジョブのログストリームとイベントを操作できます。

たとえば、集計データを検索およびフィルタリングして、特定の時間範囲の間にすべてのジョブで発生した特定のタイプのイベントを識別できます。あるいは、特定のジョブで発生したすべてのイベントのターゲットを絞ったレビューを実行することもできます。CloudWatch Logs には、ログデータのモニタリング、メトリクスフィルターの定義、カスタムアラームの作成などのオプションも用意されています。

> **Tip**
>
> Amazon Macie コンソールを使用して特定のジョブのログイベントに移動するには、次の操作を行います: Jobs (ジョブ) ページで、ジョブの名前を選択します。詳細パネルの上部で、結果を表示する を選択し、次に CloudWatch ログを表示する を選択します。Macie は Amazon CloudWatch コンソールを開き、ジョブのログイベントのテーブルを表示します。

ジョブのログを確認するには (Amazon CloudWatch コンソール)

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ページの右上の AWS リージョン セレクターを使用して、ログを確認するジョブを実行したリージョンを選択します。
3. ナビゲーションペインで、ログ、ロググループ の順に選択します。
4. ロググループ ページで、/aws/macie/classificationjobs ロググループを選択します。CloudWatch Logs には、実行したジョブのログストリームのテーブルが表示されます。ジョブごとに一意のストリームが 1 つあります。各ストリームの名前は、ジョブの一意の識別子に関連します。
5. ログストリーム の下で、次のいずれかを実行します。
   - 特定のジョブのログイベントを確認するには、ジョブのログストリームを選択します。ストリームをより簡単に検索するには、テーブルの上にあるフィルターボックスにジョブの一意の識別子を入力します。ログストリームを選択すると、CloudWatch Logs にはジョブのログイベントのテーブルが表示されます。
   - すべてのジョブのログイベントを確認するには、すべてのログストリームを検索 を選択します。CloudWatch Logs には、すべてのジョブのログイベントのテーブルが表示されます。
6. (オプション) テーブルの上にあるフィルターボックスで、確認する特定のイベントの特性を指定する用語、語句、または値を入力します。詳細については、Amazon CloudWatch Logs ユーザーガイドのフィルターパターンを使用したログデータの検索を参照してください。
7. 特定のログイベントの詳細を確認するには、イベントの行にある右矢印▶ を選択します。CloudWatch Logs には、イベントの詳細が JSON 形式で表示されます。

ログイベントのデータに習熟すると、ログデータを数値の CloudWatch メトリックスに変換する メトリクスフィルターの作成や、特定のログイベントを識別して応答することを容易にする カスタム

アラームの作成などのタスクを実行することもできます。詳細については、Amazon CloudWatch Logs ユーザーガイドを参照してください。

機密データ検出ジョブのログイベントスキーマ

機密データ検出ジョブの各ログイベントは、Amazon CloudWatch Logs イベントスキーマに準拠する JSON オブジェクトであり、標準のフィールドセットが含まれています。一部のイベントのタイプでは、そのタイプのイベントに特に役立つ情報を提供する追加のフィールドがあります。たとえば、アカウントレベルのエラーのイベントには、影響を受けた AWS アカウント のアカウント ID が含まれます。バケットレベルのエラーのイベントには、影響を受けた S3 バケットの名前が含まれます。Macie が CloudWatch Logs に発行するジョブイベントの詳細なリストについては、ジョブのログイベントのタイプを参照してください。

次の例は、機密データ検出ジョブのログイベントスキーマを示します。この例では、Amazon S3 がバケットへのアクセスを拒否したため、Macie が S3 バケット内のオブジェクトを分析できなかったことがイベントによってレポートされます。

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:08:30.345809Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

前の例では、Macie は、Amazon S3 API の ListObjectsV2 オペレーションを使用してバケット内のオブジェクトをリスト化しようとしました。Macie が Amazon S3 にリクエストを送信すると、Amazon S3 はバケットへのアクセスを拒否しました。

機密データ検出ジョブのすべてのログイベントに共通するフィールドは、次のとおりです。

- `adminAccountId` – ジョブを作成したAWS アカウントの一意の識別子。
- `jobId` — ジョブの一意の識別子。

- eventType発生したイベントのタイプ。使用可能な値の完全なリストと各値の説明については、ジョブのログイベントのタイプを参照してください。
- occurredAtoccurredAt – イベントが発生した日時 (協定世界時 (UTC) および拡張 ISO 8601 形式)。
- descriptionイベントに関する簡単な説明です。
- jobName – ジョブのカスタム名。

イベントのタイプと性質に応じて、ログイベントには次のフィールドを含めることもできます。

- affectedAccount – 影響を受けたリソースを所有している AWS アカウント の一意の識別子。
- affectedResourceaffectedResource – 影響を受けたリソースに関する詳細を提供するオブジェクト。オブジェクトでは、type フィールドは、リソースに関するメタデータを保存するフィールドを指定します。value フィールドは、フィールドの値を指定しますtype。
- operation– Macie が実行しようとし、エラーの原因となったオペレーション。
- runDate– 該当するジョブまたはジョブ実行が開始された日時 (協定世界時 (UTC) および拡張 ISO 8601 形式)。

機密データ検出ジョブのログイベントのタイプ

Macie は、次の 3 つのカテゴリのイベントのログイベントを発行します。

- ジョブステータスイベント: ジョブまたはジョブ実行のステータスまたは進行状況への変更を記録します。
- アカウントレベルのエラーイベント: Macie が特定の AWS アカウント の Amazon S3 データを分析するのを妨げたエラーを記録します。
- バケットレベルのエラーイベント: Macie が特定の S3 バケット内のデータを分析するのを妨げたエラーを記録します。

このセクションのトピックでは、Macie がカテゴリごとに発行するイベントの種類をリスト化して説明します。

トピック

- ジョブステータスイベント
- アカウントレベルのエラーイベント

- バケットレベルのエラーイベント

ジョブステータスイベント

ジョブステータスイベントは、ジョブまたはジョブ実行のステータスや進行状況への変更を記録します。定期的なジョブの場合、Macie はジョブ全体と個別のジョブ実行の両方について、これらのイベントをログに記録して発行します。全体的なジョブのステータスの判断に関する詳細については、機密データ検出ジョブのステータスをチェックするを参照してください。

次の例では、サンプルデータを使用して、ジョブステータスイベント内のフィールドの構造と性質を示します。この例では、SCHEDULED_RUN_COMPLETED イベントは、定期的なジョブのスケジュールされた実行が終了したことを示します。runDate フィールドに示されているとおり、実行は 2021 年 4 月 14 日 17:09:30 UTC に開始しました。occurredAt フィールドに示されているとおり、実行は 2021 年 4 月 14 日 17:16:30 UTC に終了しました。

```
{
    "adminAccountId": "123456789012",
    "jobId": "ffad0e71455f38a4c7c220f3cexample",
    "eventType": "SCHEDULED_RUN_COMPLETED",
    "occurredAt": "2021-04-14T17:16:30.574809Z",
    "description": "The scheduled job run finished running.",
    "jobName": "My_Daily_Macie_Job",
    "runDate": "2021-04-14T17:09:30.574809Z"
}
```

次のテーブルは、Macie がログに記録し、CloudWatch Logs に発行するジョブステータスイベントのタイプをリスト化して説明します。イベントタイプ列には、イベントの eventType フィールドに表示されるとおり、各イベントの名前が示されます。説明列には、イベントの description フィールドに表示されるとおり、イベントの簡単な説明が表示されます。追加情報には、イベントが適用されるジョブのタイプに関する情報が表示されます。テーブルは、最初にイベントが発生する可能性のある一般的な時系列順で並べ替えられ、次にイベントタイプ別のアルファベット順に並べ替えられます。

イベントタイプ	説明	追加情報
JOB_CREATED	ジョブが作成されました。	1 回限りのジョブと定期的なジョブに適用されます。

イベントタイプ	説明	追加情報
ONE_TIME_JOB_STARTED	ジョブが実行を開始しました。	1 回限りのジョブにのみ適用されます。
SCHEDULED_RUN_STARTED	スケジュールされたジョブが実行を開始しました。	定期的なジョブにのみ適用されます。1 回限りのジョブの開始を口グに記録するために、Macie はこのタイプのイベントではなく ONE_TIME_JOB_STARTED イベントを発行します。
BUCKET_MATCHED_THE_CRITERIA	影響を受けたバケットは、ジョブで指定されたバケット基準に一致しました。	ランタイムバケット基準を使用して、分析する S3 バケットを決定する 1 回限りのジョブと定期的なジョブに適用されます。 `affectedResource` オブジェクトは、基準に一致し、ジョブの分析に含まれていたバケットの名前を指定します。
NO_BUCKETS_MATCHED_THE_CRITERIA	ジョブの実行が開始されましたが、現在ジョブで指定されたバケット基準に一致するバケットはありません。ジョブはデータを分析しませんでした。	ランタイムバケット基準を使用して、分析する S3 バケットを決定する 1 回限りのジョブと定期的なジョブに適用されます。

イベントタイプ	説明	追加情報
SCHEDULED_RUN_COMPLETED	スケジュールされたジョブの実行が終了しました。	定期的なジョブにのみ適用されます。1 回限りのジョブの完了を口グに記録するために、Macie はこのタイプのイベントではなく JOB_COMPLETED イベントを発行します。
JOB_PAUSED_BY_USER	ジョブがユーザーによって一時停止されました。	ユーザーが一時的に停止した (一時停止した) 1 回限りのジョブと定期的なジョブに適用されます。
JOB_RESUMED_BY_USER	ジョブはユーザーによって再開されました。	ユーザーが一時的に停止して (一時停止して) その後再開した 1 回限りのジョブと定期的なジョブに適用されます。
JOB_PAUSED_BY_MACIE_SERVICE_QUOTA_MET	ジョブが Macie によって一時停止されました。ジョブの完了は、影響を受けたアカウントの毎月のクォータを超えます。	Macie が一時的に停止した (一時停止した) 1 回限りのジョブと定期的なジョブに適用されます。 Macie は、ジョブの完了またはジョブの実行が、ジョブがデータを分析するアカウントの毎月の 機密データ検出クォータを超える場合、ジョブを自動的に一時停止します。この問題を避けるには、影響を受けたアカウントのクォータを増やすことを検討してください。

イベントタイプ	説明	追加情報
JOB_RESUMED_BY_MACIE_SERVICE_QUOTA_LIFTED	ジョブが Macie によって再開されました。影響を受けたアカウントの毎月のサービスクォータが解除されました。	Macie が一時的に停止して (一時停止して) その後再開した 1 回限りのジョブと定期的なジョブに適用されます。 Macie が 1 回限りのジョブを自動的に一時停止した場合、Macie は、次の月が始まるとき、または影響を受けたすべてのアカウントの月次の機密データの検出クォータが増加したときのどちらか早い方で、自動的にジョブを再開します。Macie が定期的なジョブを自動的に一時停止した場合、Macie は、次の実行が開始される予定になったとき、または翌月が始まるときのどちらか早い方で、自動的にジョブを再開します。

イベントタイプ	説明	追加情報
JOB_CANCELLED	ジョブがキャンセルされました。	恒久的に停止した (キャンセルした) 1 回限りのジョブと定期的なジョブに、または 1 回限りのジョブの場合は一時停止して30 日以内に再開しなかったジョブに適用されます。 Macie を停止または無効にした場合、このタイプのイベントは、Macie を停止または無効にしたときにアクティブだったか一時停止されたジョブにも適用されます。リージョンで Macie を停止または無効にした場合、Macie は AWS リージョン 内のジョブを自動的にキャンセルします。
JOB_COMPLETED	ジョブの実行が終了しました。	1 回限りのジョブにのみ適用されます。定期的なジョブについてジョブの実行の完了を口グに記録するために、Macie はこのタイプのイベントではなく SCHEDULED_RUN_COMPLETED イベントを発行します。

アカウントレベルのエラーイベント

アカウントレベルのエラーイベントは、Macie が特定の AWS アカウント によって所有されている S3 バケット内のオブジェクトを分析するのを妨げたエラーを記録します。各イベント内の `affectedAccount` フィールドは、そのアカウントのアカウント ID を指定します。

次の例では、サンプルデータを使用して、アカウントレベルのエラーイベント内のフィールドの構造と性質を示します。この例では、ACCOUNT_ACCESS_DENIED イベントは、Macie がアカウント 444455556666 によって所有されている S3 バケット内のオブジェクトを分析できなかったことを示します。

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "ACCOUNT_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:08:30.585709Z",
    "description": "Macie doesn't have permission to access S3 bucket data for the
 affected account.",
    "jobName": "My_Macie_Job",
    "operation": "ListBuckets",
    "runDate": "2021-04-14T17:05:27.574809Z",
    "affectedAccount": "444455556666"
}
```

次のテーブルは、Macie がログに記録し、CloudWatch Logs に発行するアカウントレベルのエラーイベントのタイプをリスト化して説明します。イベントタイプ列には、イベントの eventType フィールドに表示されるとおり、各イベントの名前が示されます。説明列には、イベントの description フィールドに表示されるとおり、イベントの簡単な説明が表示されます。追加情報列には、発生したエラーの調査または対処を行うための適切なヒントが表示されます。テーブルは、イベントタイプ別にアルファベット順に昇順に並べ替えられます。

イベントタイプ	説明	追加情報
ACCOUNT_ACCESS_DENIED	Macie には、影響を受けたアカウントの S3 バケットデータにアクセスする許可がありません。	これは、通常、アカウントが所有するバケットに制限があるバケットポリシーがあるために発生します。この問題の対処方法については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。

イベントタイプ	説明	追加情報
		イベント内の `operation` フィールドの値は、Macie がアカウントの S3 データにアクセスするのを防いだアクセス許可設定を特定するのに役立ちます。このフィールドは、エラーが発生したときに Macie が実行しようとした Amazon S3 オペレーションを示します。
ACCOUNT_DISABLED	ジョブは、影響を受けたアカウントが所有するリソースをスキップしました。Macie はアカウントに対して無効になりました。	この問題に対処するには、同じ AWS リージョン アカウントで Macie を再度有効化します。
ACCOUNT_DISASSATED	ジョブは、影響を受けたアカウントが所有するリソースをスキップしました。アカウントは、もうメンバーアカウントとして Macie 管理者アカウントに関連付けられていません。	これは、お客様が、組織の Macie 管理者として、関連付けられたメンバーアカウントのデータを分析するジョブを設定し、その後メンバーアカウントが組織から削除された場合に発生します。 この問題に対処するには、影響を受けたアカウントをメンバーアカウントとして Macie 管理者アカウントに再度関連付けます。詳細については、複数のアカウントの管理を参照してください。

イベントタイプ	説明	追加情報
ACCOUNT_ISOLATED	ジョブは、影響を受けたアカウントが所有するリソースをスキップしました。AWS アカウント は分離されました。	–
ACCOUNT_REGION_DISABLED	ジョブは、影響を受けたアカウントが所有するリソースをスキップしました。AWS アカウント は、現在 AWS リージョン 内でアクティブではありません。	–
ACCOUNT_SUSPENDED	ジョブはキャンセルされたか、影響を受けたアカウントが所有するリソースをスキップしました。Macie はアカウントで停止されました。	指定したアカウントが自分のアカウントである場合、同じリージョンで Macie を停止したときに、Macie は自動的にジョブをキャンセルしました。この問題に対処するには、リージョンで Macie を再度有効化します。 指定したアカウントがメンバーアカウントである場合は、同じリージョンでそのアカウントの Macie を再度有効化します。
ACCOUNT_TERMINATED	ジョブは、影響を受けたアカウントが所有するリソースをスキップしました。AWS アカウント は終了しました。	–

バケットレベルのエラーイベント

バケットレベルのエラーイベントは、Macie が特定の S3 バケット内のオブジェクトを分析するのを妨げたエラーを記録します。各イベント内の `affectedAccount` フィールドは、バケットを所有している AWS アカウント のアカウント ID を指定します。各イベントの `affectedResource` オブジェクトは、バケットの名前を指定します。

次の例では、サンプルデータを使用して、バケットレベルのエラーイベント内のフィールドの構造と性質を示します。この例では、`BUCKET_ACCESS_DENIED` イベントは、Macie が `DOC-EXAMPLE-BUCKET` という名前の S3 バケット内のオブジェクトを分析できなかったことを示します。Macie が Amazon S3 API の ListObjectsV2 オペレーションを使用してバケット内のオブジェクトをリスト化しようとしたときに、Amazon S3 はバケットへのアクセスを拒否しました。

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:09:30.685209Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

次のテーブルは、Macie がログに記録し、CloudWatch Logs に発行するバケットレベルのエラーイベントのタイプをリスト化して説明します。イベントタイプ列には、イベントの `eventType` フィールドに表示されるとおり、各イベントの名前が示されます。説明列には、イベントの `description` フィールドに表示されるとおり、イベントの簡単な説明が表示されます。追加情報 列には、発生したエラーの調査または対処を行うための適切なヒントが表示されます。テーブルは、イベントタイプ別にアルファベット順に昇順に並べ替えられます。

イベントタイプ	説明	追加情報
BUCKET_ACCESS_DENIED		

イベントタイプ	説明	追加情報
	Macie には、影響を受けた S3 バケットにアクセスする許可がありません。	これは通常、バケットには制限があるバケットポリシーが設定されているために発生します。この問題の対処方法については、Macie が S3 バケットおよびオブジェクトにアクセスすることを許可するを参照してください。 イベント内の `operation` フィールドの値は、Macie がバケットにアクセスするのを防いだアクセス許可設定を特定するのに役立ちます。このフィールドは、エラーが発生したときに Macie が実行しようとした Amazon S3 オペレーションを示します。

イベントタイプ	説明	追加情報
BUCKET_DETAILS_UNAVAILABLE	一時的な問題により、Macie がバケットとバケットのオブジェクトに関する詳細を取得するのを妨げられました。	これは、一時的な問題により、Macie がバケットのオブジェクトを分析するのに必要なバケットとオブジェクトのメタデータを取得するのを妨げられた場合に発生します。たとえば、Macie がバケットへのアクセスを許可されていることを確認しようとしたときに Amazon S3 例外が発生しました。 1 回限りのジョブの問題に対処するには、バケット内のオブジェクトを分析する新しい 1 回限りのジョブを作成して実行することを検討してください。スケジュールされたジョブの場合、Macie は次のジョブ実行時にメタデータの取得を再度試みます。
BUCKET_DOES_NOT_EXIST	影響を受けた S3 バケットはもう存在しません。	これは通常、バケットが削除されたために発生します。
BUCKET_IN_DIFFERENT_REGION	影響を受けた S3 バケットは別の AWS リージョン に移動されました。	–

イベントタイプ	説明	追加情報
BUCKET_OWNER_CHANGED	影響を受けた S3 バケットの所有者が変更されました。Macie には、もうバケットにアクセスする許可がありません。	これは通常、バケットの所有権が組織の一部ではない AWS アカウント に移転された場合に発生します。イベント内の `affectedAccount` フィールドは、以前にバケットを所有していたアカウントのアカウント ID を示します。

機密データ検出ジョブの管理

機密データ検出ジョブの管理に役立つように、Amazon Macie は各 のジョブの完全なインベントリを提供します AWS リージョン。このインベントリを使用すると、ジョブを単一のコレクションとして管理し、個々のジョブの設定設定、ステータス、および処理統計にアクセスできます。また、各ジョブが生成した 機密データの調査結果およびその他の結果にもアクセスできます。

これらのタスクに加えて、個別のジョブのカスタムバリエーションを作成できます。既存のジョブをコピーし、コピーの設定を調整し、コピーを新しいジョブとして保存します。これは、異なるデータセットを同じ方法で分析する場合や、異なる方法で同じデータセットを分析する場合に役立ちます。あるいは、既存のジョブの設定設定を調整します。既存のジョブをキャンセルしてコピーし、新しいジョブとしてコピーを調整して保存します。

トピック

- 機密データ検出ジョブのインベントリの確認
- 機密データ検出ジョブの設定設定の確認
- 機密データ検出ジョブのステータスをチェックする
- 機密データ検出ジョブの一時停止、再開、またはキャンセル
- 機密データ検出ジョブをコピーする

機密データ検出ジョブのインベントリの確認

Amazon Macie コンソールの ジョブ ページには、現在の AWS リージョン内のアカウントのすべての機密データ検出ジョブに関する情報が表示されます。各ジョブについて、テーブルには、ジョブの

現在のステータス、スケジュールされた定期的ベースでジョブが実行されるかどうか、ジョブが特定の数の S3 バケットを分析するかどうか、ランタイム基準に一致する S3 バケットを分析するかどうかなどの概要情報が表示されます。テーブルでジョブを選択すると、詳細パネルにジョブに関する設定設定およびその他の情報が表示されます。

ジョブインベントリを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブを選択します。ジョブ ページが開き、インベントリ内のジョブの数とそれらのジョブのテーブルが表示されます。
3. 特定のジョブをよりすばやく検索するには、次のいずれかの操作を行います。

   - 特定のフィールドでテーブルをソートするには、フィールドの列見出しを選択します。ソート順序を変更するには、列見出しを再度選択します。
   - フィールドで特定の値を持つジョブのみを表示するには、フィルターボックスにカーソルを置きます。表示されるメニューで、フィルターに使用するフィールドを選択し、フィルターの値を入力します。次に、適用を選択します。
   - フィールドで特定の値を持つジョブを非表示にするには、フィルターボックスにカーソルを置きます。表示されるメニューで、フィルターに使用するフィールドを選択し、フィルターの値を入力します。次に、適用を選択します。フィルターバーで、フィルターボックスと等しいアイコン
     
     を選択します。これにより、フィルターの演算子が 等しい から 等しくない
     
     に変わります。
   - フィルターを削除するには、削除するフィルターのフィルターボックス内のフィルターを削除アイコン
     
     を選択します。
4. 特定のジョブの設定設定やその他の詳細を確認するには、テーブルでジョブの名前を選択し、次に詳細パネルを参照します。

機密データ検出ジョブの設定設定の確認

Amazon Macie コンソールで、ジョブページの詳細パネルを使用して、個別の機密データ検出ジョブに関する設定設定およびその他の情報を確認します。たとえば、ジョブが分析するように設定されて

いる S3 バケットのリストと、それらのバケット内のオブジェクトの分析のためにジョブが使用するマネージドデータ識別子を確認できます。

> **Note**
>
> 既存のジョブの設定設定は変更できません。これにより、実施するデータプライバシーと保護の監査または調査に関する機密データの調査結果と検出結果のイミュータブルな履歴を確実に保持できます。既存のジョブを変更する場合は、ジョブをキャンセル します。その後 ジョブをコピーする で、目的の設定を使用するようにコピーを設定し、コピーを新しいジョブとして保存します。
> この場合、新しいジョブが既存のデータを同じ方法で再度分析しないようにするためのステップも実行する必要があります。これを行うには、既存のジョブをキャンセルした日時をメモします。次に、元のジョブをキャンセルした後に作成または変更されたオブジェクトのみを含めるように新しいジョブの範囲を設定します。たとえば、オブジェクト基準を使用して、元のジョブをキャンセルした日時を指定する 最終更新日時 exclude 条件を追加します。

ジョブの設定設定を確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブ を選択します。
3. ジョブ ページで、ユーザーが確認する設定を持つジョブの名前を選択します。詳細パネルには、ジョブに関する設定などの情報が表示されます。ジョブの設定に応じて、パネルには次のセクションがあります。

   一般情報

   一般情報 — このセクションはジョブの現在のステータスを示し、ジョブに関する一般的な情報を提供します。たとえば、ジョブの Amazon リソースネーム (ARN)、ジョブの実行が開始された最新の日時などです。ジョブを一時停止した場合、このセクションは、ジョブを一時停止した日時と、ジョブまたは最後のジョブの実行が期限切れになった日時または再開されない場合に期限切れになる日時も示します。

   統計

   統計- このセクションには、ジョブの処理統計が表示されます。たとえば、ジョブが実行された回数や、現在の実行中にジョブがまだ処理をしていないオブジェクトのおおよその数などです。

スコープ

範囲 — このセクションは、ジョブの実行頻度を示します。また、ジョブの範囲を調整する設定も表示されます。たとえば、サンプリング深度や、ジョブの分析で S3 オブジェクトを含めるか除外する任意の オブジェクト基準などです。

S3 バケット

S3 バケット — このセクションは、ジョブを作成したときに明示的に選択したバケットをジョブが分析するように設定されている場合、パネルに表示されます。これは、ジョブ AWS アカウント がデータを分析するように設定されている の数を示します。また、ジョブが分析するように設定されているバケットの数と、それらのバケットの名前 (アカウント別にグループ化) も示します。

アカウントとバケットの完全なリストを JSON 形式で表示するには、合計バケットフィールド内の数を選択します。

S3 バケット基準

このセクションは、ジョブがどのバケツを分析するかを決定するために実行時の基準を使用する場合にパネルに表示されます。ここには、ジョブが使用するように設定されている基準がリスト化されています。

JSON 形式で基準を確認するには、詳細を選択し、次に表示されたウィンドウの 基準タブを選択します。

現在条件に一致するバケットのテーブルを確認するには、詳細を選択し、次に表示されたウィンドウの 一致するバケットタブを選択します。必要に応じて更新 を選択して、最新のデータを取得します。

> **Tip**
>
> ジョブがすでに実行されている場合は、ジョブの実行時に基準に一致したバケットがあるかどうか、および該当する場合は、それらのバケットの名前は何かを判断することもできます。これを行うには、ジョブのログイベントを確認します。パネルの上部にある結果を表示を選択し、 CloudWatch ログを表示を選択します。Macie は Amazon CloudWatch コンソールを開き、ジョブのログイベントのテーブルを表示します。イベントには、基準に一致し、ジョブの分析に含まれていた各バケットの

BUCKET_MATCHED_THE_CRITERIA イベントが含まれます。詳細については、ジョブのモニタリングを参照してください。

カスタムデータ識別子

このセクションは、ジョブが 1 つ以上のカスタムデータ識別子 を使用するように設定されている場合にパネルに表示されます。これらのカスタムデータ識別子の名前が指定されます。

許可リスト

このセクションは、ジョブが 1 つ以上の 許可リストを使用するように設定されている場合にパネルに表示されます。これらのリストの名前を指定します。リストの設定とステータスを確認するには、リスト名の横にあるリンクアイコン

を選択します。

マネージドデータ識別子

このセクションには、ジョブが使用するように設定されているマネージドデータ識別子 が表示されます。これは、ジョブのマネージドデータ識別子の選択タイプによって決まります。

- 推奨— ジョブの実行時には、推奨セットに含まれるマネージドデータ識別子を使用してください。
- 選択したものを含める— 選択セクションにリスト化されているマネージドデータ識別子のみを使用します。
- すべて含める– ジョブの実行時に使用可能なすべてのマネージドデータ識別子を使用します。
- 選択されたものを除外する— 選択セクションにリスト化されたものを除き、ジョブの実行時に使用可能なすべてのマネージドデータ識別子を使用します。
- すべて除外する— マネージドデータ識別子を使用しません。指定したカスタムデータ識別子のみを使用してください。

これらの設定を JSON 形式で確認するには、詳細を選択します。

タグ

このセクションは、タグがジョブに関連付けられている場合にパネルに表示されます。これらのタグが一覧表示されます。

タグは、特定のタイプの AWS リソースを定義して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを分類および管理できます。詳細については、Amazon Macie リソースへのタグ付けを参照してください。

4. (オプション) ジョブの設定を JSON 形式で確認して保存するには、パネルの上部で、ジョブの一意の識別子 (ジョブ IDを選択し、次に ダウンロードを選択します。

機密データ検出ジョブのステータスをチェックする

機密データ検出ジョブを作成すると、ジョブのタイプとスケジュールに応じて、最初のステータスが アクティブ (実行中または アクティブ (アイドル)になります。次に、ジョブは追加の状態をパススルーし、ジョブの進行に合わせてそれをモニタリングできます。

> **Tip**
>
> 全体的なジョブのステータスのモニタリングに加え、ジョブの進行に伴って発生する特定のイベントをモニタリングできます。これを行うには、Macie が自動的に Amazon CloudWatch Logs に発行するログデータを使用します。これらのログのデータは、ジョブのステータスに対する変更のレコードと、ジョブの実行中に発生したアカウントレベルまたはバケットレベルのエラーに関する詳細を提供します。詳細については、ジョブのモニタリングを参照してください。

ジョブのステータスを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブを選択します。
3. ジョブページで、ユーザーがチェックするステータスを持つジョブを見つけます。ステータスフィールドは、ジョブの現在のステータスを示します。

   アクティブ (アイドル)

   アクティブ (アイドル)— 定期的なジョブでは、前の実行が完了し、次のスケジュールされた実行は保留中です。この値は 1 回限りのジョブには適用されません。

アクティブ (実行中)

アクティブ (実行中)— 1 回限りのジョブでは、ジョブが現在進行中です。定期的なジョブでは、スケジュールされた実行が進行中です。

キャンセル

どのタイプのジョブでも、ジョブは永久に停止 (キャンセル) された。

ジョブを明示的にキャンセルした場合、またはそれが 1 回限りのジョブであり、ジョブを一時停止し、30 日以内に再開しなかった場合、ジョブはこのステータスになります。現在の AWS リージョンリージョンで Macie を停止した場合も、ジョブはこのステータスになります。

完了

1 回限りのジョブの場合、ジョブは正常に実行され、完了しました。この値は定期的なジョブには適用されません。代わりに、定期的なジョブのステータスは、各実行が正常に完了したときに アクティブ (アイドル)に変わります。

一時停止 (Macie により)

どのタイプのジョブでも、Macie によって一時的に停止された。

ジョブの完了またはジョブの実行が、ジョブがデータを分析するユーザーのアカウントまたはメンバーアカウントの毎月の 機密データ検出クォータを超える場合、ジョブはこのステータスになります。この場合、Macie は自動的にジョブを一時停止します。Macie は、次の暦月が始まる (アカウントの毎月の割り当てがリセットされる) か、アカウントの割り当てを増やすと、自動的にジョブを再開します。

組織の Macie 管理者で、メンバーアカウントのデータを分析するようにジョブを設定した場合、そのジョブは、ジョブまたはジョブ実行の完了がメンバーアカウントの毎月の機密データ検出クォータを超えたとしても、このステータスになります。

ジョブが実行中で、適格なオブジェクトの分析がメンバーアカウントのこのクォータに達すると、ジョブはアカウントが所有するオブジェクトの分析を停止します。ジョブが、クォータを満たしていない他のすべてのアカウントのオブジェクトの分析を終了すると、Macie は自動的にジョブを一時停止します。1 回限りのジョブの場合、Macie は次の暦月が始まったとき、または影響を受けたすべてのアカウントのクォータが増加したときのどちらか早い方で、自動的にジョブを再開します。定期的なジョブの場合は、次の実行が開始予定になるか、または次の暦月が始まるときのいずれか早いタイミングで、Macie はジョブを自動的

に再開します。スケジュールされた実行が次の暦月が始まる前に開始された場合、または影響を受けるアカウントのクォータが増加した場合、ジョブはそのアカウントが所有するオブジェクトを分析しません。

ユーザーにより一時停止

どのタイプのジョブでも、ジョブはお客様によって一時的に停止されました。

1 回限りのジョブを一時停止し、30 日以内に再開しないと、ジョブは期限切れになり、Macie はそれをキャンセルします。定期的なジョブがアクティブに実行されているときに一時停止し、30 日以内に再開しないと、ジョブの実行は期限切れになり、Macie は実行をキャンセルします。一時停止中のジョブまたはジョブ実行の有効期限を確認するには、テーブルでジョブの名前を選択し、次に詳細パネルの Status details (ステータスの詳細) セクションの Expires (有効期限) フィールドを参照します。

ジョブがキャンセルまたは一時停止された場合、ジョブの詳細を参照して、ジョブの実行が開始されたかどうか、または定期的なジョブでは、キャンセルまたは一時停止の前に少なくとも 1 回実行されたかを確認できます。これを行うには、テーブルでジョブの名前を選択し、次に詳細パネルを参照します。パネルの 実行の数 フィールドは、ジョブが実行された回数を示します。最終ランタイム フィールドは、ジョブの実行が開始された最新の日時を示します。

ジョブの現在のステータスに応じて、必要に応じてジョブを一時停止、再開、またはキャンセルできます。

機密データ検出ジョブの一時停止、再開、またはキャンセル

機密データ検出ジョブを作成した後、一時的に一時停止するか、永続的にキャンセルできます。アクティブに実行されているジョブを一時停止すると、Macie はそのジョブのすべての処理タスクの一時停止を直ちに開始します。アクティブに実行されているジョブをキャンセルすると、Macie はそのジョブのすべての処理タスクの停止を直ちに開始します。ジョブがキャンセルされた後は、ジョブを再開または再起動することはできません。

1 回限りのジョブを一時停止した場合は、30 日以内にそれを再開できます。ジョブを再開すると、Macie はジョブを一時停止した時点から直ちに処理を再開します。Macie はジョブを最初から再開することはありません。1 回限りのジョブを一時停止してから 30 日以内に再開しないと、ジョブは期限切れになり、Macie はそれをキャンセルします。

定期的なジョブを一時停止した場合は、いつでもそれを再開できます。定期的なジョブを再開し、ジョブを一時停止したときにアイドル状態だった場合、Macie はジョブを作成したときに選択したス

ケジュールおよびその他の設定設定に従ってジョブを再開します。定期的なジョブを再開し、ジョブを一時停止したときにそれがアクティブに実行されていた場合、Macie がジョブを再開する方法はジョブを再開するタイミングによって異なります。

- ジョブを一時停止してから 30 日以内に再開すると、Macie はジョブを一時停止した時点から最新のスケジュールされた実行を直ちに再開します。Macie は実行を最初から再開することはありません。
- ジョブを一時停止してから 30 日以内に再開しないと、最新のスケジュールされた実行が期限切れになり、Macie はその実行の残りの処理タスクをすべてキャンセルします。その後ジョブを再開すると、Macie はジョブを作成したときに選択したスケジュールおよびその他の設定設定に従って、ジョブを再開します。

一時停止したジョブまたはジョブの実行がいつ期限切れになるかを判断しやすくするために、Macie はジョブの一時停止中にジョブの詳細に有効期限を追加します。この日付を確認するには、ジョブページのテーブルでジョブの名前を選択し、次に詳細パネルの ステータスの詳細 セクションの 有効期限 フィールドを参照します。さらに、ジョブまたはジョブの実行の有効期限が切れる約 7 日前に通知されます。ジョブまたはジョブの実行の有効期限が切れてキャンセルされると、再度通知されます。通知するために、ユーザーの AWS アカウントに関連付けられているアドレスに E メールが送信されます。また、 アカウントの AWS Health イベントと Amazon CloudWatch Events も作成します。

ジョブを一時停止、再開、またはキャンセルするには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブを選択します。
3. ジョブ (ジョブ) ページで、一時停止、再開、またはキャンセルするジョブのチェックボックスをオンにし、Actions (アクション) メニューで以下のいずれかを実行します。
   - ジョブを一時的に一時停止するには、一時停止を選択します。このオプションは、ジョブの現在のステータスが アクティブ (アイドル)、 アクティブ (実行中)、または 一時停止 (Macie により)の場合にのみ使用できます。
   - ジョブを再開するには、再開を選択します。このオプションは、ジョブの現在のステータスが一時停止 (ユーザーにより)の場合にのみ使用できます。
   - ジョブを完全にキャンセルするには、キャンセルを選択します。このオプションを選択すると、後でジョブを再開または再起動することはできません。

機密データ検出ジョブをコピーする

既存のジョブと類似している新しい機密データ検出ジョブをすばやく作成するには、ジョブのコピーを作成し、コピーの設定を編集して、コピーを新しいジョブとして保存します。これは、既存のジョブのカスタムバリエーションを作成する場合に役立ちます。あるいは、ジョブをキャンセルしてコピーし、次に新しいジョブとして設定をコピー、変更、および保存することで既存のジョブの設定設定を調整します。

ジョブをコピーするには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで ジョブを選択します。
3. コピーするジョブのチェックボックスをオンにします。
4. アクション メニューで 新規にコピーを選択します。
5. コンソールのステップを完了して、ジョブのコピーの設定を確認および調整します。スコープを絞り込むステップでは、ジョブが既存のデータを再度同じ方法で分析することを防ぐオプションを選択することを検討する：

   - 1 回限りのジョブでは、object criteria (オブジェクト基準) を使用して、特定の時刻の後に作成または変更されたオブジェクトのみを含めます。たとえば、キャンセルしたジョブのコピーを作成する場合は、既存のジョブをキャンセルした日時を指定する 最終更新日時条件を追加します。
   - 定期的なジョブにでは、既存のオブジェクトを含めるチェックボックスをオフにします。これを行う場合、ジョブの最初の実行では、ジョブを作成した後でジョブの最初の実行前に作成または変更されたオブジェクトのみが分析されます。また、オブジェクト基準を使用して、特定の日時より前に最後に変更されたオブジェクトを除外することもできます。

   この手順やその他の手順の詳細については、機密データ検出ジョブの作成 を参照してください。
6. 終了したら、送信を選択して、コピーを新しいジョブとして保存します。

機密データ検出ジョブのコストの予測とモニタリング

Amazon Macie の料金は、機密データ検出ジョブを実行して分析するデータの量に部分的に基づいています。機密データ検出ジョブを実行する際の推定コストを予測およびモニタリングするには、ジョブの作成時およびジョブの実行開始後に Macie が提供するコストの見積もりを確認できます。

実際のコストを確認および監視するには、AWS Billing and Cost Management を使用します。AWS Billing and Cost Management には、AWS のサービス サービスのコストを追跡、分析できるように設計された機能が用意されており、アカウントまたは組織の予算を管理できます。また、履歴データに基づいて使用コストを予測するのに役立つ機能も提供します。詳細については、AWS Billing ユーザーガイドを参照してください。

Macie の料金の詳細については、Amazon Macie 料金表を参照してください。

トピック

- 機密データ検出ジョブのコスト予測
- 機密データ検出ジョブの推定コストのモニタリング

機密データ検出ジョブのコスト予測

機密データ検出ジョブを作成すると、ジョブ作成プロセスの主要な 2 ステップ中に、Amazon Macie は推定コストを計算して表示します。ジョブで選択した S3 バケットのテーブルを確認するステップ (ステップ 2) と、ジョブですべての設定を確認するステップ (ステップ 8) です。これらの見積もりは、ジョブを保存する前にジョブの設定を調整するかどうかを判断するのに役立ちます。見積りの可用性と性質は、ジョブに対して選択した設定によって異なります。

Reviewing estimated costs for individual buckets (step 2) (個別のバケットの推定コストの確認 (ステップ 2

分析するジョブに対して個別のバケットを明示的に選択した場合、それらの各バケット内のオブジェクトを分析するための推定コストを確認できます。Macie は、バケットの選択を確認するときに、ジョブ作成プロセスのステップ 2 の間にこれらの見積もりを表示します。このステップのテーブルで、推定コスト フィールドは、バケット内オブジェクトを分析するためにジョブを 1 回実行した場合の合計推定コスト (米ドル単位) を示します。

各見積もりは、バケットに現在保存されているオブジェクトのサイズとタイプに基づいて、ジョブがバケット内で分析する非圧縮データの予測量を反映します。見積もりには、現在の AWS リージョン の Macie 料金も反映されています。

バケットのコスト見積もりには、分類可能なオブジェクトのみが含まれます。分類可能オブジェクトは、サポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を持つ S3 オブジェクトです。分類可能なオブジェクトが圧縮ファイルまたはアーカイブファイルである場合、見積もりではファイルが 3:1 の圧縮率を使用し、ジョブはすべての抽出されたファイルを分析できると仮定します。

ジョブの合計推定コストの確認 (ステップ 8)

1 回限りのジョブを作成する場合、または既存の S3 オブジェクトを含めるように定期的なジョブを作成して設定する場合、Macie はジョブ作成プロセスの最終ステップ中にジョブの合計推定コストを計算して表示します。この見積もりは、ジョブに対して選択したすべての設定を確認して検証する間に確認できます。

この見積もりは、現在のリージョンでジョブを 1 回実行した場合の合計予測コスト (米ドル単位) を示します。見積もりは、ジョブが分析する非圧縮データの予測量を反映します。これは、ジョブに対して明示的に選択したバケットに現在保存されているオブジェクトのサイズとタイプ、またはジョブの設定に応じて、ジョブで指定したバケット基準に現在一致する最大 500 個のバケットに基づきます。

この見積もりには、ジョブの範囲を調整して縮小するために選択したオプション (より低いサンプリング深度や、ジョブから特定の S3 オブジェクトを除外する条件など) は反映されていないことに注意してください。また、毎月の sensitive data discovery quota (機密データ検出クォータ) を反映していません。これにより、ジョブの分析の範囲とコスト、またはアカウントに適用される可能性のある割引が制限される場合があります。

ジョブの合計推定コストに加えて、見積もりは、ジョブの予測範囲とコストに関する洞察を提供する集計データを提供します。

- Size (サイズ) 値は、ジョブで分析できるオブジェクトと分析できないオブジェクトの合計ストレージサイズを示します。
- Object count (オブジェクトカウント) 値は、ジョブが分析できないオブジェクトの合計数を示します。

これらの値で 分類可能 オブジェクトは、サポートされている Amazon S3 ストレージクラスを使用し、サポートされているファイルまたはストレージ形式のファイル名拡張子を持つ S3 オブジェクトです。コスト見積もりには、分類可能なオブジェクトのみが含まれます。分類不可 オブジェクトは、サポートされているストレージクラスを使用していないか、サポートされているファイルまたはストレージ形式のファイル名拡張子を持たないオブジェクトです。これらのオブジェクトは、コスト見積もりには含まれません。

この見積もりは、圧縮ファイルまたはアーカイブファイルである S3 オブジェクトの追加の集計データを提供します。Compressed (圧縮) 値は、サポートされている Amazon S3 ストレージクラスを使用して、サポートされているタイプの圧縮ファイルまたはアーカイブファイルのファイル名拡張子を持つオブジェクトの合計ストレージサイズを示します。非圧縮 値は、指定された圧縮率に基づいて、これらのオブジェクトが解凍された場合のおおよそのサイズを示しま

す。Macie が圧縮ファイルとアーカイブファイルを分析する方法のため、このデータは関連しています。

Macie が圧縮ファイルまたはアーカイブファイルを分析すると、完全なファイルとファイルの内容の両方が検査されます。ファイルの内容を検査するために、Macie はファイルを解凍し、次にサポートされている形式を使用する各抽出ファイルを検査します。したがって、ジョブが分析する実際のデータの量は以下によって異なります。

- ファイルが圧縮を使用するかどうか、および該当する場合は、使用する圧縮率を使用するかどうか。
- 抽出されたファイルの数、サイズ、および形式。

デフォルトでは、Macie はジョブのコスト見積りを計算するときに次のことを想定しています。

- すべての圧縮ファイルとアーカイブファイルは 3:1 の圧縮率を使用します。
- すべての抽出されたファイルは、サポートされているファイルまたはストレージ形式を使用します。

これらの仮定により、ジョブが分析するデータの範囲のサイズ見積もりが大きくなり、その結果、ジョブのコスト見積もりが大きくなります。

異なる圧縮率に基づいて、ジョブの合計推定コストを再計算できます。これを行うには、推定コストセクションの 推定圧縮率を選択するリストから率を選択します。次に Macie は、選択に一致するように見積もりを更新します。

Macie が推定コストを計算する方法の詳細については、推定使用コストの計算方法を理解するを参照してください。

機密データ検出ジョブの推定コストのモニタリング

機密データ検出ジョブをすでに実行している場合、Amazon Macie コンソールの 使用状況ページは、これらのジョブの推定コストのモニタリングに役立ちます。このページには、現在の暦月の間に AWS リージョン で Macie を使用するための推定コスト (米ドル単位) が表示されています。Macie がこれらの見積もりを計算する方法については、推定使用コストの計算方法を理解するを参照してください。

実行中のジョブの推定コストを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。

2. ページの右上の AWS リージョン セレクターを使用して、推定コストを確認するリージョンを選択します。
3. ナビゲーションペインで 使用状況を選択します。
4. 使用状況 ページで、アカウントの推定コスト内訳を参照します。機密データ検出ジョブ 項目は、現在のリージョンで当月に実行したジョブの合計推定コストをレポートします。

   お客様が組織の Macie 管理者である場合、Estimated costs (推定コスト) セクションには、現在のリージョンでの当月の組織全体の推定コストが表示されます。特定のアカウントで実行されたジョブの合計推定コストを表示するには、テーブル内のアカウントを選択します。推定コスト セクションには、実行されたジョブの推定コストを含む、アカウントの推定コストの内訳が表示されます。別のアカウントに関するこのデータを表示するには、テーブルでアカウントを選択します。アカウントの選択を解除するには、パネルのアカウント ID の横にある X を選択します。

実際のコストを確認および監視するには、AWS Billing and Cost Management を使用します。

機密データ検出ジョブに推奨されるマネージドデータ識別子

機密データ検出ジョブの結果を最適化するために、ジョブに推奨するマネージドデータ識別子のセットを自動的に使用するように個々のジョブを設定できます。マネージドデータ識別子は、特定の種類の機密データ (たとえば、クレジットカード番号、AWS シークレットアクセスキー、または特定の国または地域のパスポート番号) を検出するように設計された組み込み型の基準と手法のセットです。

推奨されるマネージドデータ識別子のセットは、機密データの一般的なカテゴリとタイプを検出するように設計されています。当社の調査に基づいて、機密データの一般的なカテゴリやタイプを検出できると同時に、ノイズを減らすことで業務結果を最適化できます。新しいマネージドデータ識別子をリリースする際、それがジョブ結果をさらに最適化できると思われる場合は、このセットに追加します。別途、既存のマネージドデータ識別子を追加したり、セットから削除したりする可能性もあります。推奨セットからマネージドデータ識別子を追加または削除すると、このページを更新し、変更の性質と時期がわかるようにします。これらの変更に関する自動通知については、Macie ドキュメント履歴 ページの RSS フィードをサブスクライブしてください。

機密データ検出ジョブを作成するときに、ジョブがAmazon Simple Storage Service (Amazon S3) バケットでオブジェクトを分析するときにどのマネージドデータ識別子を使用するかを指定します。推奨マネージドデータ識別子のセットを使用するようにジョブを設定するには、ジョブの作成時に推奨オプションを選択します。そうすると、ジョブの実行開始時に、推奨セットに含まれるすべてのマネージドデータ識別子が自動的に使用されます。ジョブを複数回実行するように設定した場合、各実行では、実行の開始時に推奨セットにあるマネージドデータ識別子をすべて自動的に使用します。

以下のトピックでは、現在推奨セットに含まれているマネージドデータ識別子を機密データのカテゴリとタイプ別に一覧表示しています。セット内の各マネージドデータ識別子の一意の識別子 (ID) を指定します。この ID は、PGP_PRIVATE_KEY PGP プライベートキーや米国パスポート番号の USA_PASSPORT_NUMBER など、マネージドデータ識別子が検出するに設計された機密データのタイプを表します。

トピック

特定のマネージドデータ識別子、または Macie が現在提供しているマネージドデータ識別子の全リストについては、マネージドデータ識別子の使用　を参照してください。

認証情報

S3 オブジェクトでの認証情報データの出現を検知するために、推奨セットでは次のマネージドデータ識別子を使用します。

機密データタイプ	マネージドデータ識別子 ID
AWS シークレットアクセスキー	AWS_CREDENTIALS
HTTP 基本認証ヘッダー	HTTP_BASIC_AUTH_HEADER
OpenSSH プライベートキー	OPENSSH_PRIVATE_KEY
PGP プライベートキー	PGP_PRIVATE_KEY
公開鍵暗号標準 (PKCS) プライベートキー	PKCS
PuTTY プライベートキー	PUTTY_PRIVATE_KEY

財務情報

S3 オブジェクトでの財務情報の出現を検知するために、推奨セットでは次のマネージドデータ識別子を使用します。

機密データタイプ	マネージドデータ識別子 ID
クレジットカードの磁気ストライプデータ	CREDIT_CARD_MAGNETIC_STRIPE
クレジットカード番号	CREDIT_CARD_NUMBER (キーワードに近いクレジットカード番号の場合)

個人を特定できる情報 (PII)

S3 オブジェクトでの個人を特定できる情報 (PII) の出現を検知するために、推奨セットでは次のマネージドデータ識別子を使用します。

機密データタイプ	マネージドデータ識別子 ID
運転免許証識別番号	CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE (米国の場合)、UK_DRIVERS_LICENSE
選挙人名簿番号	UK_ELECTORAL_ROLL_NUMBER
国民識別番号	FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
国民保険番号 (NINO)	UK_NATIONAL_INSURANCE_NUMBER
パスポート番号	CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
社会保険番号 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER

機密データタイプ	マネージドデータ識別子 ID
社会保障番号 (SSN)	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
納税者識別番号または参照番号	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

推奨セットの更新

次の表は、機密データ検出ジョブに推奨するマネージドデータ識別子セットの変更点をまとめたものです。これらの変更に関する自動通知については、Macie ドキュメント履歴 ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
一般提供	推奨セットの初回リリース。	2023 年 6 月 27 日

Amazon Macie を用いた暗号化された Amazon S3 オブジェクトの分析

で Amazon Macie を有効にすると AWS アカウント、Macie はユーザーに代わって Amazon Simple Storage Service (Amazon S3) およびその他の を呼び出すために必要なアクセス許可を Macie に付与するサービスにリンクされたロールを作成します。Amazon S3 AWS のサービス サービスにリンクされたロールは、ユーザーに代わってアクションを実行するためにサービスに手動でアクセス許可を追加する必要がない AWS のサービス ため、 のセットアッププロセスを簡素化します。このタイプのロールの詳細については、AWS Identity and Access Management ユーザーガイドのサービスにリンクされたロールの使用を参照してください。

Macie のサービスリンクロールAWSServiceRoleForAmazonMacieのアクセス許可ポリシーにより、Macie は S3 バケットとオブジェクトに関する情報の取得および S3 バケット内のオブジェクトの取得、分析などのアクションを実行することが許可されます。ユーザーのアカウントが組織の Macie 管理者アカウントである場合、ポリシーにより Macie が組織のメンバーアカウントに対してユーザーに代わってこれらのアクションを実行することも許可されます。

S3 オブジェクトが暗号化されている場合、Macie サービスリンクロールのアクセス許可ポリシーは通常、オブジェクトの復号化に必要なアクセス許可を Macie に付与します。ただし、これは使用された暗号化のタイプによって異なります。それは、Macie が適切な暗号化キーの使用を許可されているかどうかによっても異なる可能性があります。

トピック

- Amazon S3 オブジェクトの暗号化オプション
- Amazon Macie にカスタマーマネージド の使用を許可する AWS KMS key

Amazon S3 オブジェクトの暗号化オプション

Amazon S3 は S3 オブジェクトの複数の暗号化オプションをサポートしています。これらのオプションのほとんどで、Amazon Macie は、ユーザーアカウントの Macie サービスリンクロールを使用してオブジェクトを復号化できます。ただし、これはオブジェクトの暗号化に使用された暗号化のタイプによって異なります。

Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)

Amazon S3 マネージドキー (SSE-S3) によるサーバー側の暗号化を使用してオブジェクトが暗号化されている場合、Macie はオブジェクトを復号できます。

このタイプの暗号化の詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 マネージドキーを用いたサーバー側の暗号化を使用を参照してください。

AWS KMS keys (DSSE-KMS および SSE-KMS) によるサーバー側の暗号化

AWS マネージド AWS KMS key (DSSE-KMS または SSE-KMS) による二層式サーバー側の暗号化またはサーバー側の暗号化を使用してオブジェクトが暗号化されている場合、Macie はオブジェクトを復号できます。

オブジェクトが、二層式サーバー側の暗号化またはカスタマー管理のサーバー側の暗号化 AWS KMS key (DSSE-KMS または SSE-KMS) を使用して暗号化されている場合、Macie はキー の使用を Macie に許可する場合にのみオブジェクトを復号できます。これは、 内で完全に管理される KMS キー AWS KMS と外部キーストア内の KMS キーで暗号化されたオブジェクトの場合に当て

はまります。Macie が該当の KMS キー使用を許可されていない場合、Macie はオブジェクトのメタデータの保存およびレポートのみできます。

これらのタイプの暗号化の詳細については、Amazon Simple Storage Service ユーザーガイドの「 での二層式サーバー側の暗号化 AWS KMS keysの使用」および「 でのサーバー側の暗号化 AWS KMS keysの使用」を参照してください。

> **Tip**
>
> Macie AWS KMS keys がアカウントの S3 バケット内のオブジェクトを分析するためにアクセスする必要があるすべてのカスタマーマネージド のリストを自動的に生成できます。これを行うには、 の Amazon Macie Scripts リポジトリから入手できる AWS KMS Permission Analyzer スクリプトを実行します GitHub。 Amazon Macie このスクリプトは、 AWS Command Line Interface （ AWS CLI) コマンドの追加スクリプトを生成することもできます。必要に応じてこれらのコマンドを実行し、指定した KMS キーに必要な設定設定とポリシーを更新できます。

顧客提供のキーを用いたサーバー側の暗号化 (SSE-C)。

お客様が用意したキーによるサーバー側の暗号化 (SSE-C) を使用してオブジェクトが暗号化されている場合、Macie はオブジェクトを復号できません。Macie はオブジェクトのメタデータのみを保存およびレポートできます。

このタイプの暗号化の詳細については、Amazon Simple Storage Service ユーザーガイドのお客様が用意したキーによるサーバー側の暗号化の使用を参照してください。

クライアント側の暗号化

クライアント側の暗号化を使用してオブジェクトが暗号化されている場合、Macie はオブジェクトを復号化できません。Macie はオブジェクトのメタデータのみを保存およびレポートできます。たとえば、Macie はオブジェクトに関連付けられているオブジェクトとタグのサイズをレポートできます。

Amazon S3 のコンテキストでのこのタイプの暗号化詳細については、Amazon Simple Storage Service ユーザーガイドのクライアント側の暗号化を使用したデータの保護を参照してください。

Macie でバケットインベントリをフィルタリングして、特定のタイプの暗号化を使用するオブジェクトを保存する S3 バケットを判別できます。また、新しいオブジェクトを保存するときに、デフォル

トで特定のタイプのサーバー側の暗号化を使用するバケットを判別することもできます。次の表は、この情報を検索するためにバケットインベントリに適用できるフィルターの例を示しています。

...のバケットを表示するには	...でこのフィルターを適用
SSE-C 暗号化を使用するオブジェクトを保存する	暗号化によるオブジェクト数はお客様提供、From = 1
DSSE-KMS または SSE-KMS 暗号化を使用するオブジェクトを保存する	暗号化によるオブジェクト数はAWS KMS 管理され、From = 1
SSE-S3 暗号化を使用するオブジェクトを保存する	暗号化によるオブジェクト数は Amazon S3 が管理し、From = 1 です。
クライアント側の暗号化を使用するオブジェクトを保存する (または暗号化されていない)	暗号化によるオブジェクトカウントは、暗号化なしおよび From = 1
DSSE-KMS 暗号化を使用してデフォルトで新しいオブジェクトを暗号化する	デフォルトの暗号化 = aws:kms:dsse
SSE-KMS 暗号化を使用してデフォルトで新しいオブジェクトを暗号化する	デフォルトの暗号化= aws:kms
SSE-S3 暗号化を使用してデフォルトで新しいオブジェクトを暗号化する	デフォルトの暗号化= AES256

バケットが DSSE-KMS または SSE-KMS 暗号化を使用してデフォルトで新しいオブジェクトを暗号化するように設定されている場合 AWS KMS key は、どのオブジェクトが使用されているかも判断できます。これを行うには、S3バケット ページでバケットを選択します。バケットの詳細パネルのサーバー側の暗号化 で、 AWS KMS keyフィールドを参照してください。このフィールドには、Amazon リソースネーム (ARN) またはキーの一意の識別子 (キー ID) が表示されます。

Amazon Macie にカスタマーマネージド の使用を許可する AWS KMS key

Amazon S3 オブジェクトが、二層式サーバー側の暗号化またはカスタマー管理のサーバー側の暗号化 AWS KMS key (DSSE-KMS または SSE-KMS) を使用して暗号化されている場合、Amazon Macie はキーの使用が許可されている場合にのみオブジェクトを復号できます。このアクセスを提供する方

法は、キーを所有するアカウントがオブジェクトを保存する S3 バケットも所有しているかどうかによって異なります。

- 同じアカウントが AWS KMS key とバケットを所有している場合、アカウントのユーザーはキーのポリシーを更新する必要があります。
- あるアカウントが を所有 AWS KMS key し、別のアカウントがバケットを所有している場合、キーを所有するアカウントのユーザーは、キーへのクロスアカウントアクセスを許可する必要があります。

このトピックでは、これらのタスクの実行方法を説明し、両方のシナリオの例を示します。カスタマー管理の へのアクセスを許可する方法の詳細については AWS KMS keys、「 AWS Key Management Service デベロッパーガイド」の「 の認証とアクセスコントロール AWS KMS」を参照してください。

カスタマーマネージドキーへの同じアカウントのアクセスを許可する

同じアカウントが AWS KMS key と S3 バケットの両方を所有している場合、アカウントのユーザーはキーのポリシーにステートメントを追加する必要があります。追加のステートメントでは、アカウントの Macie サービスリンクロールがキーを使用してデータを復号することを許可する必要があります。キーポリシーの更新の詳細な情報については、AWS Key Management Service デベロッパーガイドのキーポリシーの変更を参照してください。

ステートメントにおいて:

- `Principal` 要素は、 AWS KMS key と S3 バケットを所有するアカウントの Macie サービスにリンクされたロールの Amazon リソースネーム (ARN) を指定する必要があります。

  アカウントがオプトイン にある場合 AWS リージョン、ARN にはリージョンに適したリージョンコードも含める必要があります。たとえば、アカウントが、リージョンコード me-south-1 が設定されている中東 (バーレーン) リージョン内にある場合、`Principal` 要素は `arn:aws:iam::`*`123456789012`*`:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie` を指定する必要があります。ここで、*`123456789012`*は、アカウントのアカウント ID です。Macie が現在利用可能なリージョンのリージョンコードのリストについては、「AWS 全般のリファレンス」の「Amazon Macie エンドポイントとクォータ」を参照してください。
- `Action` 配列は、`kms:Decrypt` アクションを指定する必要があります。これは、キーで暗号化された S3 オブジェクトを復号するために Macie が実行することを許可される必要がある唯一の AWS KMS アクションです。

AWS KMS keyのポリシーに追加するステートメントの例を次に示します。

```
{
    "Sid": "Allow the Macie service-linked role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

前の例では、以下のようになっています。

- `Principal` 要素 の `AWS` フィールドは、アカウントの Macie サービスリンクロールAWSServiceRoleForAmazonMacieのARNを指定します。これにより、Macie サービスにリンクされたロールがポリシーステートメントで指定されたアクションを実行することを許可します。*123456789012* はアカウント ID の例です。この値をKMS キーと S3 バケットを所有するアカウントのアカウント ID に置き換えます。
- `Action` 配列は、Macie サービスリンクロールが KMS キーを使用して実行することを許可されたアクション (キーで暗号化される暗号文を復号) を指定します。

このステートメントをキーポリシーのどこに追加するかは、ポリシーに現在含まれている構造と要素によって異なります。ステートメントをポリシーに追加するときに、構文が有効であることを確認します。キーポリシーは JSON 形式を使用します。これは、ステートメントをポリシーのどこに追加するかに応じて、ステートメントの前後にカンマを追加する必要があることも意味します。

カスタマーマネージドキーへのクロスアカウントアクセスを許可する

あるアカウントが を所有し AWS KMS key （ キー所有者 ）、別のアカウントが S3 バケットを所有している場合 (バケット所有者)、キー所有者はバケット所有者に KMS キーへのクロスアカウントアクセスを提供する必要があります。これを行うには、キー所有者はまず、キーのポリシーにより、バケット所有者がキーの使用とキーの付与の作成の両方を行うことを許可することを確認します。次に、バケット所有者はキーの付与を作成します。付与 は、ポリシーツールであり、付与によって指定された条件が満たされている場合、 AWS プリンシパルに暗号化オペレーションで (KMS キー) の

使用を許可します。この場合、許可は、関連する許可をバケット所有者のアカウントの Macie サービスリンクロールに委任します。

キーポリシーの更新の詳細な情報については、AWS Key Management Service デベロッパーガイドのキーポリシーの変更を参照してください。付与の詳細については、AWS Key Management Service デベロッパーガイドのAWS KMSでの付与を参照してください。

ステップ 1: キーポリシーを変更する

キーポリシーでは、キー所有者は、ポリシーに 2 つのステートメントが含まれていることを確認する必要があります:

- 最初のステートメントは、バケット所有者がキーを使用してデータを復号することを許可します。
- 2 番目のステートメントは、バケット所有者が自らの (当該バケット所有者の) アカウントの Macie サービスリンクロールの許可を作成することを許可します。

最初のステートメントでは、`Principal` 要素は、バケット所有者のアカウントの ARN を指定する必要があります。`Action` 配列は、`kms:Decrypt` アクションを指定する必要があります。これは、キーで暗号化されたオブジェクトを復号するために Macie が実行することを許可される必要がある唯一の AWS KMS アクションです。 AWS KMS keyのポリシーのこのステートメントの例を次に示します。

```
{
    "Sid": "Allow account 111122223333 to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

前の例では、以下のようになっています。

- `Principal` 要素の `AWS` フィールドは、バケット所有者のアカウントの ARN を指定します (*111122223333*)。これにより、バケット所有者がポリシーステートメントで指定されたアクションを実行することを許可します。*111122223333* はアカウント ID の例です。この値をバケット所有者のアカウントのアカウント ID に置き換えます。

- Action 配列は、バケット所有者が KMS キーを使用して実行することを許可されたアクション (キーで暗号化される暗号文を復号) を指定します。

キーポリシーの 2 番目のステートメントは、バケット所有者が自分のアカウントの Macie サービスにリンクされたロールの付与を作成することを許可します。このステートメントでは、Principal 要素は、バケットの所有者のアカウントの ARN を指定する必要があります。Action 配列は、kms:CreateGrant アクションを指定する必要があります。Condition 要素は、ステートメントで指定された kms:CreateGrant アクションへのアクセスをフィルタリングできます。 AWS KMS keyのポリシーのこのステートメントの例を次に示します。

```
{
    "Sid": "Allow account 111122223333 to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
        }
    }
}
```

前の例では、以下のようになっています。

- Principal 要素の AWS フィールドは、バケット所有者のアカウントの ARN を指定します (*111122223333*)。これにより、バケット所有者がポリシーステートメントで指定されたアクションを実行することを許可します。*111122223333* はアカウント ID の例です。この値をバケット所有者のアカウントのアカウント ID に置き換えます。
- Action 配列は、バケット所有者が KMS キーを使用して実行することを許可されたアクションを指定します (キーの付与を作成)。
- Condition 要素は、StringEquals 条件演算子と kms:GranteePrincipal 条件キーを使用して、ポリシーステートメントで指定されたアクションへのアクセスをフィルタリングします。この場合、バケット所有者は指定された GranteePrincipal のためのみ許可を作成できます。これ

は、これらのバケット所有者のアカウントの Macie サービスリンクロールの ARN です。そのARN では、*111122223333* はアカウント ID の例です。この値をバケット所有者のアカウントのアカウント ID に置き換えます。

バケット所有者のアカウントがオプトイン にある場合は AWS リージョン、Macie サービスにリンクされたロールの ARN に適切なリージョンコードも含めます。たとえば、アカウントが、リージョンコード me-south-1 が設定されている中東 (バーレーン) リージョンにある場合は、ARN で `macie.amazonaws.com` を `macie.me-south-1.amazonaws.com` と置き換えます。Macie が現在利用可能なリージョンのリージョンコードのリストについては、「AWS 全般のリファレンス」の「Amazon Macie エンドポイントとクォータ」を参照してください。

キー所有者がこれらのステートメントをキーポリシーのどこに追加するかは、ポリシーに現在含まれている構造と要素によって異なります。キー所有者がステートメントを追加するときは、構文が有効であることを確認する必要があります。キーポリシーは JSON 形式を使用します。これは、ステートメントをポリシーのどこに追加するかに応じて、キー所有者は各ステートメントの前後にカンマを追加する必要があることも意味します。

ステップ 2: 許可を作成する

キー所有者が必要に応じてキーポリシーを更新した後、バケット所有者はキーの付与を作成する必要があります。この付与は、関連するアクセス許可を (バケット所有者の) アカウントの Macie サービスにリンクされたロールに委任します。バケット所有者が付与を作成する前に、バケット所有者はアカウントの `kms:CreateGrant` アクションの実施が許可されていることを確認する必要があります。このアクションにより、ロール所有者が既存のカスタマーマネージド AWS KMS keyに許可を追加することが許可されます。

許可を作成するには、バケット所有者は AWS Key Management Service API の CreateGrantオペレーションを使用できます。バケット所有者が付与を作成するときに、必要なパラメータに次の値を指定する必要があります。

- `KeyId` – KMS キーの ARN。KMS キーへのクロスアカウントアクセスでは、この値は ARN である必要があります。キー ID にすることはできません。
- `GranteePrincipal` – アカウントの Macie サービスリンクロール (`AWSServiceRoleForAmazonMacie`) の ARN この値は `arn:aws:iam::`*111122223333*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie` である必要があります。ここで、*111122223333* は、バケット所有者のアカウントのアカウント ID です。

アカウントがオプトインリージョン内にある場合、ARN には適切なリージョンコードを含める必要があります。例えば、アカウントが、リージョンコード me-south-1 が設定されている中東 (バーレーン) リージョン内にある場合、ARN は `arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie` である必要があります。ここで、*111122223333* は、バケット所有者のアカウント ID です。

- `Operations` – 復 AWS KMS 号アクション (`Decrypt`) 。これは、KMS キーで暗号化されたオブジェクトを復号するために Macie が実行することを許可される必要がある唯一の AWS KMS アクションです。

AWS Command Line Interface （ AWS CLI) を使用してカスタマーマネージド KMS キーの許可を作成するには、create-grant コマンドを実行します。以下の例のように指定します。この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie ^
--operations "Decrypt"
```

コードの説明は以下のとおりです。

- `key-id` は、付与を適用する KMS キーの ARN を指定します。
- `grantee-principal` は、許可によって指定されたアクションの実行を許可されたアカウントの Macie サービスリンクロールの ARN を指定します。この値は、キーポリシーの 2 番目のステートメントの `kms:GranteePrincipal` 条件によって指定された ARN と一致する必要があります。
- `operations` は、許可が、指定されたプリンシパルが実行することを許可するアクション (KMS キーで暗号化される暗号文の復号) を指定します。

コマンドが正常に実行された場合は、以下のような出力が表示されます。

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

ここで、GrantToken は、作成された付与を表す、一意で、非シークレットで、可変長の base64 でエンコードされた文字列であり、GrantIdは、付与の一意の識別子です。

Amazon Macie での機密データ検出結果の保存と保持

機密データ検出ジョブを実行するか、Amazon Macie が機密データ自動検出を実行すると、Macie は分析のスコープに含まれる各 Amazon Simple Storage Service (Amazon S3) オブジェクトの分析レコードを作成します。これらのレコードは機密データ検出結果と呼ばれ、Macie が個々の S3 オブジェクトに対して実行した分析の詳細を記録します。これには、Macie が機密データを検出しないために検出結果を生成しないオブジェクト、およびエラーや問題のために Macie が分析できないオブジェクトが含まれます。Macie がオブジェクト内の機密データを検出すると、レコードには対応する検出結果のデータと追加情報が含まれます。機密データの検出結果から、データプライバシーと保護の監査や調査に役立つ分析レコードが得られます。

Macie は機密データの検出結果を 90 日間だけ保存します。機密データの検出結果にアクセスし、それらの長期保存と保持を有効化するには、結果を S3 バケットに保存し、 AWS Key Management Service AWS KMSキーを用いて暗号化するように Macie を設定します。バケットは、機密データの検出結果のすべての最終的で長期的なリポジトリとして機能します。次に、オプションで、そのリポジトリ内の結果にアクセスしてクエリを実行できます。

このトピックでは、 を使用して機密データ検出結果のリポジトリ AWS Management Console を設定するプロセスについて説明します。設定は、結果を暗号化する 、結果を保存する S3 汎用バケット、および使用するキーとバケットを示す Macie 設定の組み合わせ AWS KMS key です。Macie 設定をプログラムで設定する場合は、Amazon Macie API の PutClassificationExportConfigurationオペレーションを使用できます。

Macie で設定を設定すると、選択は現在の AWS リージョンにのみ適用されます。お客様が組織の Macie 管理者である場合、選択はお客様のアカウントにのみ適用されます。選択は、関連付けられたメンバーアカウントには適用されません。

複数の で Macie を使用する場合は AWS リージョン、Macie を使用するリージョンごとにリポジトリ設定を構成します。オプションで、複数のリージョンの機密データ検出結果を同じ S3 バケットに保存できます。ただし、次の要件に注意してください。

- 米国東部 (バージニア北部) リージョンなど AWS アカウント、 で をデフォルトで AWS 有効にするリージョンの結果を保存するには、デフォルトで有効になっているリージョンのバケットを選択する必要があります。結果は、オプトインリージョン (デフォルトで無効になっているリージョン) のバケットに保存できません。

- 中東 (バーレーン) リージョンなど、オプトインリージョンの結果を保存するには、同じリージョンまたはデフォルトで有効になっているリージョンのバケットを選択する必要があります。別のオプトインリージョンのバケットに結果を保存することはできません。

リージョンがデフォルトで有効になっているかを確認するには、「AWS Identity and Access Management ユーザーガイド」の「リージョンとエンドポイント」を参照してください。上記の要件に加えて、Macie が個々の検出結果で報告する機密データのサンプルを取得するかどうかも検討してください。影響を受ける S3 オブジェクトから機密データのサンプルを取得するには、影響を受けるオブジェクト、該当する検出結果、対応する機密データ検出結果のリソースとデータを同じリージョンに保存する必要があります。

タスク

概要

Amazon Macie は、機密データ検出ジョブを実行するとき、または機密データ自動検出を実行するときに分析または分析を試みる Amazon S3 オブジェクトごとに機密データ検出結果を自動的に作成します。これには、以下が含まれます。

- Macie が機密データを検出したオブジェクトなので、機密データの検出結果も生成されます。
- Macie が機密データを検出しないため、機密データの検出結果も生成されないオブジェクト。
- アクセス許可設定やサポートされていないファイルやストレージ形式の使用などのエラーや問題のため Macie が分析できないオブジェクト。

Macie が S3 オブジェクト内の機密データを検出すると、機密データの検出結果には、対応する機密データの調査結果のデータが含まれます。また、Macie がオブジェクト内で検出した機密データのタイプごとに最大 1,000 個までの出現の場所などの追加情報も提供します。例:

- Microsoft Excel ワークブック、CSV ファイル、または TSV ファイル内のセルまたはフィールドの列番号と行番号
- JSON または JSON Lines ファイル内のフィールドまたは配列へのパス

- CSV、JSON、JSON Lines、または TSV ファイル以外の非バイナリテキストファイル (HTML、TXT、XML ファイルなど) 内の行の行番号
- Adobe Portable Document Format (PDF) ファイル内のページのページ番号
- Apache Avro オブジェクトコンテナまたは Apache Parquet ファイル内のレコードのレコードインデックスとフィールドへのパス

影響を受ける S3 オブジェクトが .tar ファイルや .zip ファイルなどのアーカイブファイルである場合、機密データの検出結果には、Macie がアーカイブから抽出した個々のファイル内の機密データの出現に関する詳細な位置データも表示されます。Macie は、アーカイブファイルの機密データの調査結果にこの情報を含めません。位置データを報告するために、機密データ検出結果は標準化された JSON スキーマを使用します。

機密データの検出結果には、Macie が検出した機密データは含まれません。代わりに、監査や調査に役立つ分析レコードが提供されます。

Macie は機密データの検出結果を 90 日間保存します。Amazon Macie コンソールまたは Amazon Macie API からそれらに直接アクセスすることはできません。代わりに、このトピックの手順に従って、指定した で結果を暗号化し、 AWS KMS key 指定した S3 汎用バケットに結果を保存するように Macie を設定します。その後、Macie は結果を JSON Lines (.jsonl) ファイルに書き込み、そのファイルを GNU Zip (.gz) ファイルとしてバケットに追加し、SSE-KMS 暗号化を使用してデータを暗号化します。2023 年 11 月 8 日現在、Macie は結果の S3 オブジェクトにハッシュベースのメッセージ認証コード (HMAC) で署名します AWS KMS key。

機密データ検出の結果を S3 バケットに保存するように Macie を設定すると、バケットは、結果の最終的な長期リポジトリとして機能します。次に、オプションで、そのリポジトリ内の結果にアクセスしてクエリを実行できます。

> **Tip**
>
> 機密データ検出結果をクエリして使用して潜在的なデータセキュリティリスクを分析およびレポートする方法の詳細な説明例については、 セキュリティブログのAmazon Athena と Amazon で Macie 機密データ検出結果をクエリおよび視覚化する方法 QuickSightAWS 」ブログ記事を参照してください。
>
> 機密データ検出結果の分析に使用できる Amazon Athena クエリのサンプルについては、 の Amazon Macie 結果分析リポジトリを参照してください GitHub。このリポジトリでは、結果を取得および復号化するように Athena を設定する手順と、結果のテーブルを作成するためのスクリプトも提供します。

ステップ 1: アクセス許可を確認する

機密データの検出結果のリポジトリを設定する前に、結果を暗号化して保存するために必要なアクセス許可があることを確認します。アクセス許可を確認するには、 AWS Identity and Access Management (IAM) を使用して、IAM ID にアタッチされている IAM ポリシーを確認します。次にこれらのポリシー内の情報を、リポジトリを設定するために実行が許可される必要がある次のアクションのリストと比較します。

Amazon Macie

Macie の場合、次のアクションの実行が許可されていることを確認します。

`macie2:PutClassificationExportConfiguration`

このアクションにより、Macie のリポジトリ設定の追加または変更が許可されます。

Amazon S3

Amazon S3 の場合、次のアクションの実行が許可されていることを確認します。

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

これらのアクションにより、リポジトリとして機能する S3 汎用バケットにアクセスして設定できます。

AWS KMS

Amazon Macie コンソールを使用してリポジトリ設定を追加または変更するには、次の AWS KMS アクションの実行が許可されていることを確認します。

- `kms:DescribeKey`
- `kms:ListAliases`

これらのアクションにより、アカウントの AWS KMS keys に関する情報を取得して表示することが許可されます。その後、これらのキーのいずれかを選択して、機密データの検出結果を暗号化できます。

データを暗号化 AWS KMS key するために新しい を作成する場合は、`kms:CreateKey`、、`kms:GetKeyPolicy`および のアクションを実行することも許可する必要がありま`kms:PutKeyPolicy`す。

必要なアクションを実行することが許可されていない場合は、次のステップに進む前に AWS 管理者にサポートを依頼してください。

ステップ 2: AWS KMS keyを設定する

アクセス許可を確認したら、Macie AWS KMS key が機密データ検出結果を暗号化するために使用するものを決定します。キーは、結果を保存する S3 バケット AWS リージョン と同じ で有効になっている、カスタマー管理の対称暗号化 KMS キーである必要があります。

キーは、自分のアカウント AWS KMS key から既存の でも、 AWS KMS key 別のアカウントが所有する既存の でもかまいません。新しい KMS キーを使用する場合は、先に進む前にキーを作成します。別のアカウントが所有する既存のキーを使用する場合、キーの Amazon リソースネーム (ARN) を取得します。Macie でリポジトリ設定を設定するときに、この ARN を入力する必要があります。KMS キーの作成と設定の見直しについては、AWS Key Management Service デベロッパーガイドのキーの管理を参照してください。

> **Note**
>
> キーは、外部キーストア AWS KMS key の にすることができます。ただし、そのキーは、完全に AWS KMS内で管理されるキーよりも遅く、信頼性が低くなる可能性があります。機密データの検出結果を S3 バケットキーとして使用するように設定された S3 バケットに保存することで、このリスクを軽減できます。そうすることで、機密データディスカバリーの結果を暗号化するために行う必要のある AWS KMS リクエストの数が減ります。
> 外部キーストアで KMS キーを使用する方法については、AWS Key Management Service デベロッパーガイドの外部キーストアを参照してください。S3 バケットキー使用の詳細については、Amazon Simple Storage Service ユーザーガイドの、Amazon S3 バケットキーを使用した SSE-KMS のコストの削減を参照してください。

Macie が使用する KMS キーを決定した後、Macie にそのキーを使用するアクセス許可を付与します。そうしないと、Macie はリポジトリで結果を暗号化したり保存したりすることができなくなります。Macie にキーを使用するアクセス許可を付与するには、キーのポリシーを更新します。キーポリシーと KMS キーへのアクセス管理の詳細については、AWS Key Management Service デベロッパーガイドの AWS KMSのキーポリシーを参照してください。

キーポリシーを更新するには

1. https://console.aws.amazon.com/kms で AWS KMS コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。
3. 機密データ検出の結果を暗号化するために Macie に使用させるキーを選択します。
4. アクセスポリシー タブで 編集 を選択します。
5. 次のステートメントをクリップボードにコピーし、ポリシーに追加します。

```
{
    "Sid": "Allow Macie to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "macie.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
         },
         "ArnLike": {
             "aws:SourceArn": [
                 "arn:aws:macie2:Region:111122223333:export-configuration:*",
                 "arn:aws:macie2:Region:111122223333:classification-job/*"
             ]
         }
    }
}
```

> **Note**
>
> ステートメントをポリシーに追加するときは、構文が有効であることを確認します。ポリシーは JSON 形式を使用します。またこれは、ステートメントをポリシーに追加する場所に応じて、ステートメントの前後にカンマを追加する必要があることを意味します。ステートメントを最後のステートメントとして追加する場合は、前のステートメン

トの中括弧の後にカンマを追加します。最初のステートメントとして追加するか、既存の 2 つのステートメントの間に追加する場合は、中括弧の後にカンマを追加します。

6. ステートメントを環境に対して正しい値で更新します。

- Condition フィールドで、プレースホルダーの値を置き換えます。ここで、
  - *111122223333* は、お客様の AWS アカウントのアカウント ID です。
  - *#####*は、Macie AWS リージョン を使用していて、Macie にキーの使用を許可する です。

    複数のリージョンで Macie を使用していて、追加のリージョンでの Macie のキーの使用を許可する場合は、追加のリージョンごとに aws:SourceArn 条件を追加します。例:

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
    "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]
```

    代わりに、all (すべての) リージョンで Macie のキーの使用を許可することもできます。これを行うには、プレースホルダーの値をワイルドカード文字 (*) に置き換えます。例:

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- オプトインリージョンで Macie を使用している場合は、適切なリージョンコードを Service フィールドの値に追加します。例えば、リージョンコード me-south-1 が設定されている中東 (バーレーン) リージョンで Macie を使用している場合は、macie.amazonaws.com を macie.me-south-1.amazonaws.com と置き換えます。Macieが現在利用可能なリージョンのリストと、それぞれのリージョンコードについては、AWS 全般のリファレンスの Amazon Macieのエンドポイントとクォータを参照してください。

Condition フィールドでは、2 つの IAM グローバル条件キーを使用することに注意してください。。

- aws:SourceAccount – この条件により、Macie はお客様のアカウントに対してのみ指定されたアクションを実行できます。具体的には、aws:SourceArn 条件で指定されたリソースおよびアクションに対して、指定されたアクションを実行できるアカウントを決定します。

  Macie が追加のアカウントに対して指定されたアクションを実行することを許可するには、追加の各アカウントのアカウント ID をこの条件に追加します。例:

  ```
  "aws:SourceAccount": [111122223333,444455556666]
  ```

- aws:SourceArn – この条件は、他の AWS のサービス が指定されたアクションを実行できないようにします。また、Macie がお客様のアカウントで他のアクションを実行中にキーを使用するのを防ぐこともできます。つまり、オブジェクトが機密データ検出結果であり、結果が指定されたリージョンの指定されたアカウントによって作成された機密データ自動検出ジョブまたは機密データ検出ジョブの場合にのみ、Macie が キーを使用して S3 オブジェクトを暗号化できるようにします。

  Macie が追加のアカウントで指定したアクションを実行することを許可するには、追加のアカウントごとに ARN をこの条件に追加します。例:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
      "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
      "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
      "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
  ]
  ```

  aws:SourceAccount と aws:SourceArn の条件によって指定されたアカウントは、一致する必要があります。

  これらの条件は、 とのトランザクション中に Macie が混乱した代理として使用されるのを防ぐのに役立ちます AWS KMS。お勧めしませんが、ステートメントからこれらの条件を削除できます。

7. ステートメントの追加と更新が完了したら、変更を保存する を選択します。

ステップ 3: S3 バケットを選択する

アクセス許可を確認して を設定したら AWS KMS key、機密データ検出結果のリポジトリとして使用する S3 バケットを指定する準備が整います。これには 2 つのオプションがあります。

- Macie が作成する新しい S3 バケットを使用する – このオプションを選択すると、Macie は検出結果 AWS リージョン 用に現在の に新しい S3 汎用バケットを自動的に作成します。また、Macie はバケットにバケットポリシーを適用します。このポリシーでは、Macie がバケットにオブジェクトを追加することを許可します。また、SSE-KMS 暗号化を使用して、指定した AWS KMS key でオブジェクトを暗号化する必要もあります。ポリシーを確認するには、バケットの名前と使用する KMS キーを指定した後、Amazon Macie コンソールで [ポリシーを表示] を選択します。
- 作成した既存の S3 バケットを使用する — 特定の S3 バケットに検出結果を保存する場合は、続行する前にバケットを作成します。バケットは汎用バケットである必要があります。さらに、バケットの設定とポリシーは、Macie がバケットにオブジェクトを追加することを許可する必要があります。このトピックでは、チェックする設定はどれか、およびポリシーの更新方法について説明します。また、ポリシーに追加するステートメントの例も示します。

以下のセクションでは、各オプションの手順について説明します。目的のオプションのセクションを選択します。

Macie が作成した新しい S3 バケットを使用します。

Macie が作成した新しい S3 バケットを使用する場合は、プロセスの最後のステップは、Macie でリポジトリ設定を設定することです。

Macie でリポジトリ設定を設定するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインの 設定 の下で、検出結果 を選択します。
3. 機密データの検出結果のリポジトリ の下で、バケットを作成する を選択します。
4. バケットを作成する ボックスで、バケットの名前を入力します。

   名前はすべての S3 バケットで一意である必要があります。また、名前は、小文字、数字、ドット (.)、およびハイフン (-) のみで設定できます。追加の命名要件については、Amazon Simple Storage Service ユーザーガイドのバケットの名前付けルールを参照してください。
5. 詳細設定 セクションを展開します。

6. (オプショナル) バケット内の場所へのパスに使用するプレフィックスを指定するには、データ検出結果のプレフィックス ボックスにプレフィックスを入力します。

   値を入力すると、Macie はボックスの下の例を更新して、検出結果を保存するバケットの場所へのパスを表示します。

7. すべてのパブリックアクセスをブロックするではいを選ぶと、バケツに対するすべての公開ブロック設定が有効になります。

   これらの設定の詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 ストレージへのパブリックアクセスのブロックを参照してください。

8. [暗号化設定] で、結果を暗号化するために Macie に使用させる AWS KMS key を指定します。

   - 自分のアカウントにキーを使用するには、アカウントからキーを選択する を選択します。そして、AWS KMS keyリストからユーザー名を選択します。リストには、お客様のアカウントの、お客様が管理する対称暗号化 KMS キーが表示されます。
   - 別のアカウントが所有し、使用が許可されているキーを使用するには、別のアカウントのキーの ARN を入力する を選択します。次に、AWS KMS key ARN ボックスに、使用するキーの Amazon リソースネーム (ARN) を入力します。例えば、**`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**

9. 設定の入力が完了したら、保存 を選択します。

   Macie は設定をテストして、それらが正しいことを確認します。正しくない設定がある場合、Macie は問題への対処に役立つエラーメッセージを表示します。

リポジトリ設定を保存した後、Macie は過去 90 日間の既存の検出結果をリポジトリに追加します。また、Macie は、新しい検出結果をリポジトリに追加し始めます。

作成した既存の S3 バケットを使用します。

機密データの検出結果を作成した特定の S3 バケットに保存する場合は、Macie で設定を構成する前にバケットを作成して設定します。バケットを作成する際は、次の各要件に注意してください。

- バケットは汎用バケットである必要があります。ディレクトリバケットにすることはできません。
- バケットのObject Lockを有効化する場合は、その機能のデフォルトの保持設定を無効にする必要があります。そうしないと、Macie は検出結果をバケットに追加できません。詳細については、Amazon Simple Storage Service ユーザーガイドの「S3 Object Lock の使用」を参照してください。

- 米国東部 (バージニア北部) リージョンなど AWS アカウント、 でデフォルトで有効になっているリージョンの検出結果を保存するには、バケットがデフォルトで有効になっているリージョンにある必要があります。結果は、オプトインリージョン (デフォルトで無効になっているリージョン) のバケットに保存できません。
- 中東 (バーレーン) リージョンなど、オプトインリージョンについての検出の結果を保存するには、バケットは、同じリージョンまたはデフォルトで有効になっているリージョンに存在している必要があります。別のオプトインリージョンのバケットに結果を保存することはできません。

リージョンがデフォルトで有効になっているかを確認するには、「AWS Identity and Access Management ユーザーガイド」の「リージョンとエンドポイント」を参照してください。

バケットを作成したら、バケットのポリシーを更新して、Macie がバケットに関する情報を取得し、バケットにオブジェクトを追加することを許可します。その後、Macie で設定を構成できます。

バケットのバケットポリシーを更新するには

1. https://console.aws.amazon.com/s3/でAmazon S3 コンソールを開きます。
2. 検出結果を保存するバケットを選択します。
3. アクセス許可 タブを選択します。
4. バケットポリシー セクションで、編集 を選択します。
5. 次のポリシー例をクリップボードにコピーします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Macie to use the GetBucketLocation operation",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
```

```
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Allow Macie to add objects to the bucket",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption headers. This is optional",
```

```
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:Region:111122223333:key/KMSKeyId"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::myBucketName/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

6. ポリシー例をAmazon S3 コンソールの バケットポリシー エディタに貼り付けます。
7. ポリシー例を環境に対して正しい値で更新します。

   - 不正な暗号化ヘッダーを拒否するオプションのステートメントでは、以下を行います。
     - をバケットの名前*myBucketName*に置き換えます。
     - StringNotEquals 条件では、*arn:aws:kms:Region:111122223333:key/KMSKeyId* を、検出結果の暗号化 AWS KMS key に使用する の Amazon リソースネーム (ARN) に置き換えます。
   - 他のすべてのステートメントでは、プレースホルダーの値を置き換えます。ここで、
     - *myBucketName* はバケットの名前です。
     - *111122223333* は、お客様の AWS アカウントのアカウント ID です。

- ##### は、お客様が Macie を使用していて、Macie が検出結果をバケットに追加することを許可する AWS リージョン です。

  複数のリージョンで Macie を使用していて、追加のリージョンで Macie が結果をバケットに追加することを許可する場合は、追加のリージョンごとに aws:SourceArn 条件を追加します。例:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
      "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
      "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
      "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
  ]
  ```

  代わりに、all (すべての) リージョンで Macie が結果をバケットに追加することを許可することもできます。これを行うには、プレースホルダーの値をワイルドカード文字 (*) に置き換えます。例:

  ```
  "aws:SourceArn": [
      "arn:aws:macie2:*:111122223333:export-configuration:*",
      "arn:aws:macie2:*:111122223333:classification-job/*"
  ]
  ```

- オプトインリージョンで Macie を利用している場合は、Macie サービスプリンシパルを指定するステートメントごとに、適切なリージョンコードを Service フィールドの値に追加します。例えば、リージョンコード me-south-1 が設定されている中東 (バーレーン) リージョンで Macie を使用している場合は、該当するステートメントごとに、macie.amazonaws.com を macie.me-south-1.amazonaws.com と置き換えます。Macieが現在利用可能なリージョンのリストと、それぞれのリージョンコードについては、AWS 全般のリファレンスの Amazon Macieのエンドポイントとクォータを参照してください。

ポリシー例には、Macie がバケットが存在するリージョン (GetBucketLocation) を判断したり、オブジェクトをバケット (PutObject) に追加したりすることを許可するステートメントが含まれていることに留意してください。これらのステートメントは、2 つの IAM グローバル条件キーを使用する条件を定義します。

- aws:SourceAccount – この条件により、Macie はユーザーのアカウントに対してのみ機密データ検出結果をバケットに追加できます。これにより、Macie が他のアカウントの検出結果をバ

ケットに追加するのを防ぎます。具体的には、条件は、aws:SourceArn 条件で指定されたリソースおよびアクションに対して、バケットを使用できるアカウントを指定します。

バケット内の追加アカウントの結果を保存するには、追加のアカウントごとにアカウント ID をこの条件に追加します。例:

```
"aws:SourceAccount": [111122223333,444455556666]
```

- aws:SourceArn – この条件は、バケットに追加されるオブジェクトのソースに基づいてバケットへのアクセスを制限します。これにより、他の AWS のサービス がバケットにオブジェクトを追加できなくなります。また、Macie がお客様のアカウントで他のアクションを実行中にオブジェクトをバケットに追加するのを防ぐこともできます より具体的には、この条件により、オブジェクトが機密データ検出結果であり、結果が指定されたリージョンの指定されたアカウントによって作成された機密データ自動検出ジョブまたは機密データ検出ジョブの場合にのみ、Macie がバケットにオブジェクトを追加できるようになります。

  Macie が追加のアカウントで指定したアクションを実行することを許可するには、追加のアカウントごとに ARN をこの条件に追加します。例:

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
    "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
]
```

aws:SourceAccount と aws:SourceArn の条件によって指定されたアカウントは、一致する必要があります。

どちらの条件も、Macie が Amazon S3 とのトランザクション中に confused deputy (混乱した代理) として使用されるのを防ぐのに役立ちます。お勧めしませんが、バケットポリシーからこれらの条件を削除できます。

8. バケットポリシーの更新が完了したら、変更を保存する を選択します。

Macie でリポジトリ設定を設定できるようになりました。

Macie でリポジトリ設定を設定するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインの 設定 の下で、検出結果 を選択します。
3. 機密データの検出結果のリポジトリ の下で、既存のバケット を選択します。
4. バケットを選択する で、検出結果を保存するバケットを選択します。
5. (オプショナル) バケット内の場所へのパスに使用するパスプレフィックスを指定するには、詳細設定 セクションを展開します。次に、データ検出結果プレフィックス で、使用するパスのプレフィクスを入力します。

   値を入力すると、Macie はボックスの下の例を更新して、検出結果を保存するバケットの場所へのパスを表示します。
6. [暗号化設定] で、結果を暗号化するために Macie に使用させる AWS KMS key を指定します。

   - 自分のアカウントにキーを使用するには、アカウントからキーを選択する を選択します。そして、AWS KMS keyリストからユーザー名を選択します。リストには、お客様のアカウントの、お客様が管理する対称暗号化 KMS キーが表示されます。
   - 別のアカウントが所有し、使用が許可されているキーを使用するには、別のアカウントのキーの ARN を入力する を選択します。次に、AWS KMS key ARN ボックスに、使用するキーの ARN を入力します。例えば、**`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**
7. 設定の入力が完了したら、保存 を選択します。

   Macie は設定をテストして、それらが正しいことを確認します。正しくない設定がある場合、Macie は問題への対処に役立つエラーメッセージを表示します。

リポジトリ設定を保存した後、Macie は過去 90 日間の既存の検出結果をリポジトリに追加します。また、Macie は、新しい検出結果をリポジトリに追加し始めます。

> **Note**
>
> その後に [データ検出の結果のプレフィックス] の設定を変更する場合は、Amazon S3 のバケットポリシーも更新します。以前のパスを指定するポリシーステートメントでは、新しいパスを指定する必要があります。指定しない場合、Macie は検出の結果をバケットに追加することが許可されません。

> **Tip**
>
> サーバー側の暗号化コストを削減するには、S3 バケットキーを使用するように S3 バケットを設定し、機密データ検出結果の暗号化用に AWS KMS key 設定した も指定します。S3 バケットキーを使用すると、 への呼び出し回数が減り AWS KMS、 AWS KMS リクエストコストを削減できます。KMS キーが外部キーストアにある場合は、S3 バケットキーを使用することでキーの使用によるパフォーマンスへの影響を最小限に抑えることができます。詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 バケットキーを使用した SSE-KMS のコストの削減を参照してください。

Amazon Macie でサポートされているストレージのクラスと形式

Amazon Simple Storage Service (Amazon S3) データエステート内の機密データを検出できるように、Amazon Macie は、ほとんどの Amazon S3 ストレージクラスと、さまざまなファイルおよびストレージ形式をサポートします。このサポートは、S3 オブジェクトを分析するためのマネージドデータ識別子およびカスタムデータ識別子の使用に適用されます。

Macie が S3 オブジェクトを分析するには、サポートされているストレージクラスを使用してオブジェクトを Amazon S3 の汎用バケットに保存する必要があります。オブジェクトは、サポートされているファイルまたはストレージ形式を使用する必要があります。このセクションのトピックでは、Macie が現在サポートしているストレージクラス、ファイルおよびストレージ形式を一覧表示しています。

> **Tip**
>
> Macie は Amazon S3 向けに最適化されていますが、現在別の場所に保存されているリソース内の機密データを検出するために使用できます。これを行うには、データを Amazon S3 に一時的または永続的に移動します。たとえば、Amazon Relational Database Service または Amazon Aurora のスナップショットを Apache Parquet 形式で Amazon S3 にエクスポートします。あるいは、Amazon DynamoDB テーブルを Amazon S3 にエクスポートします。その後、機密データ検出ジョブを作成して Amazon S3 内のデータを分析できます。

トピック

- サポートされている Amazon S3 ストレージクラス
- サポートされているファイルおよびストレージ形式

サポートされている Amazon S3 ストレージクラス

機密データを検出するために、Amazon Macie は次の Amazon S3 ストレージクラスをサポートしています。

- 低冗長化 (RRS)
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering
- S3 1 ゾーン - 低頻度アクセス (S3 1 ゾーン -IA)
- S3 Standard
- S3 標準 - 低頻度アクセス (S3 標準 IA)

Macie は、S3 Glacier Deep Archive や S3 Express One Zone など、他の Amazon S3 ストレージクラスを使用する S3 オブジェクトを分析しません。さらに、Macie は S3 ディレクトリバケットに保存されているオブジェクトを分析しません。

サポートされている Amazon S3 ストレージクラスを使用しない S3 オブジェクトを分析する機密データ検出ジョブを設定する場合、Macie はジョブの実行時にそれらのオブジェクトをスキップします。Macie はオブジェクト内のデータを取得または分析しようとはしません。オブジェクトは分類できないオブジェクトとして扱われます。分類できないオブジェクトとは、サポートされているストレージクラスと、サポートされているファイルまたはストレージ形式を使用していないオブジェクトです。Macie は、サポートされているストレージクラスと、サポートされているファイルまたはストレージ形式を使用するオブジェクトのみを分析します。

同様に、機密データの自動検出を実行するように Macie を設定した場合、分類できないオブジェクトは選択と分析の対象にはなりません。Macie は、サポートされている Amazon S3 ストレージクラスと、サポートされているファイルまたはストレージ形式を使用するオブジェクトのみを選択します。

分類できないオブジェクトを保存する S3 バケットを識別するには、S3 バケットインベントリ をフィルタリングします。インベントリ内の各バケットには、バケット内の分類できないオブジェクトの数と合計ストレージサイズを報告するフィールドがあります。

Amazon S3 が提供するストレージクラスの詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 ストレージクラスの使用を参照してください。

サポートされているファイルおよびストレージ形式

Amazon Macie が S3 オブジェクトを分析すると、Macie は Amazon S3 からオブジェクトの最新バージョンを取得し、オブジェクトのコンテンツを詳細に検査します。この検査では、データのファイルまたはストレージ形式が考慮されます。Macie は、一般的に使用される圧縮形式やアーカイブ形式など、さまざまな形式でデータを分析できます。

Macie が圧縮ファイルまたはアーカイブファイル内のデータを分析するとき、Macie は完全なファイルとファイルの内容の両方を検査します。ファイルの内容を検査するために、Macie はファイルを解凍し、次にサポートされている形式を使用する各抽出ファイルを検査します。Macie は、最大 1,000,000 個までのファイルに対して、最大 10 レベルのネストされた深さまでこれを行うことができます。機密データ検出に適用される追加のクォータの詳細については、Amazon Macie クォータを参照してください。

次のテーブルでは、Macie が機密データを検出するために分析できるファイルおよびストレージ形式のタイプをリスト化して説明します。サポートされているタイプごとに、表には該当するファイル名拡張子もリスト化されています。

ファイルまたはストレージタイプ	説明	ファイル名拡張子
ビッグデータ	Apache Avro オブジェクトコンテナおよび Apache Parquet ファイル	.avro、.parquet
圧縮またはアーカイブ	GNU Zip 圧縮アーカイブ、TAR アーカイブ、および ZIP 圧縮アーカイブ	.gz、.gzip、.tar、.zip
ドキュメント	Adobe Portable Document Format ファイル、Microsoft Excel ワークブック、および Microsoft Word ドキュメント	.doc、.docx、.pdf、.xls、.xlsx
E メールメッセージ	内容が IETF RFC で指定された電子メールメッセージに関する要件 (RFC 2822など) に準拠する電子メールファイル	.eml

ファイルまたはストレージタイプ	説明	ファイル名拡張子
Text (テキスト)	カンマ区切り値 (CSV) ファイル、ハイパーテキストマークアップ言語 (HTML) ファイル、 JavaScript オブジェクト表記 (JSON) ファイル、JSON Lines ファイル、プレーンテキストドキュメント、タブ区切り値 (TSV) ファイル、拡張マークアップ言語 (XML) ファイルなどの非バイナリテキストファイル	.csv、.htm、.html、.json、.jsonl、.tsv、.txt、.xml、その他 (非バイナリテキストファイルのタイプに応じて)

Macie は、画像または音声、動画、その他のマルチメディアコンテンツのデータを分析しません。

機密データ検出ジョブを設定して、サポートされているファイルまたはストレージ形式を使用しない S3 オブジェクトを分析すると、Macie はジョブの実行時にそれらのオブジェクトをスキップします。Macie はオブジェクト内のデータを取得または分析しようとはしません。オブジェクトは分類できないオブジェクトとして扱われます。分類不可能オブジェクトは、サポートされている Amazon S3 ストレージクラスを使用しないか、サポートされているファイルまたはストレージ形式のファイル名拡張子を持たないオブジェクトです。Macie は、サポートされているストレージクラスと、サポートされているファイルまたはストレージ形式を使用するオブジェクトのみを分析します。

同様に、機密データの自動検出を実行するように Macie を設定した場合、分類できないオブジェクトは選択と分析の対象にはなりません。Macie は、サポートされている Amazon S3 ストレージクラスと、サポートされているファイルまたはストレージ形式を使用するオブジェクトのみを選択します。

分類できないオブジェクトを保存する S3 バケットを識別するには、S3 バケットインベントリ をフィルタリングします。インベントリ内の各バケットには、バケット内の分類できないオブジェクトの数と合計ストレージサイズを報告するフィールドがあります。

Amazon Macie の調査結果を分析する

Amazon Macie は、Amazon Simple Storage Service (Amazon S3) の汎用バケットのセキュリティまたはプライバシーに関する潜在的なポリシー違反や問題を検出したとき、または S3 オブジェクト内の機密データを検出したときに検出結果を生成します。検出結果とは、Macie が検出した潜在的問題や機密データの詳細レポートです。各検出結果では、重要度評価、影響するリソースに関する情報、およびMacie が問題やデータを検出したタイミングや方法などの追加の詳細が示されます。Macie は、ポリシーと機密データの調査結果を 90 日間保存します。

調査結果は、次の方法で確認、分析、および管理できます。

Amazon Macie コンソール

Amazon Macie コンソールの 調査結果ページでは、調査結果をリスト化し、個別の調査結果の詳細な情報を提供します。これらのページでは、調査結果のグループ化、フィルタリング、並べ替え、および抑制ルール() の作成および管理のためのオプションも用意されています。抑制ルールは、調査結果の分析を合理化するのに役立ちます。

Amazon Macie API

Amazon Macie API では、 AWS コマンドラインツールまたは AWS SDK を使用するか、HTTPS リクエストを Macie に直接送信することで、検出結果データをクエリおよび取得できます。データのクエリを行うには、Amazon Macie API にリクエストを送信し、サポートされているパラメータを使用して、取得する検出結果を指定します。リクエストを送信すると、Macie が結果を JSON レスポンスで返します。その後、調査結果を別のサービスまたはアプリケーションに渡して、より詳細な分析、長期保存、またはレポートの作成を行うことができます。詳細については、Amazon Macie API リファレンスを参照してください。

Amazon EventBridge

モニタリングやイベント管理システムなどの他の のサービスやシステムとの統合をさらにサポートするために、Macie は調査結果をイベント EventBridge として Amazon に公開します。以前の Amazon CloudWatch Events は、独自のアプリケーション EventBridge、Software as a Service (SaaS) アプリケーション、および Macie AWS のサービス などのリアルタイムデータのストリームを配信できるサーバーレスイベントバスサービスです。そのデータを AWS Lambda 関数、Amazon Simple Notification Service トピック、Amazon Kinesis ストリームなどのターゲットにルーティングして、追加の自動処理を行うことができます。 EventBridge また、 を使用すると、検出結果データの長期的な保持を確保できます。の詳細については EventBridge、「Amazon EventBridge ユーザーガイド」を参照してください。

Macie は、新しい検出結果 EventBridge のイベントを に自動的に発行します。また、Macie は既存のポリシーの調査結果のその後の出現でもイベントを自動的に発行します。検出結果データは EventBridge イベントとして構成されているため、他の サービスやツールを使用して、検出結果をより簡単にモニタリング、分析、対応できます。例えば、 EventBridge を使用して、特定のタイプの新しい検出結果を AWS Lambda 関数に自動的に送信し、次にデータを処理してセキュリティインシデントおよびイベント管理 (SIEM) システムに送信できます。AWS User Notifications を Macie と統合すると、イベントを使用して、指定した配信チャネルを通じて検出結果を自動的に通知することもできます。 EventBridge イベントを使用して検出結果をモニタリングおよび処理する方法については、「」を参照してくださいAmazon Macie の Amazon EventBridge との統合。

AWS Security Hub

組織のセキュリティ体制をさらに広く詳細に分析するには、検出結果を AWS Security Hubに出力することもできます。Security Hub は、 AWS のサービス およびサポートされているセキュリティソリューションから AWS Partner Network セキュリティデータを収集し、 AWS 環境全体のセキュリティ状態を包括的に把握できるようにするサービスです。Security Hub はまた、お客様の環境をセキュリティ業界の標準とベストプラクティスに照らしてチェックすることにも役立ちます。Security Hub の詳細については、AWS Security Hub ユーザーガイドを参照してください。Security Hub を使用した調査結果のモニタリングと処理の詳細については、Amazon Macie の AWS Security Hub との統合を参照してください。

検出結果に加えて、Macie は、機密データ検出を分析するよう S3 オブジェクトに対する機密データ検出結果を作成します。機密データの検出結果は、オブジェクトの分析に関する詳細を記録するレコードです。これには、Macie が機密データを見つけられないために検出結果を生成しないオブジェクト、およびエラーや問題のために Macie が分析できないオブジェクトが含まれます。機密データの検出結果から、データプライバシーと保護の監査や調査に役立つ分析レコードが得られます。Amazon Macie コンソールまたは Amazon Macie API を使って機密データの検出結果に直接アクセスすることはできません。代わりに、結果を S3 バケットに保存するように Macie を設定します。次に、オプションで、そのバケット内の結果にアクセスしてクエリを実行できます。結果を保存するように Macie を設定する方法については、機密データ検出結果の保存と保持を参照してください。

トピック

- Amazon Macie の調査結果のタイプ
- Amazon Macie での検出結果のサンプルの使用
- Amazon Macie コンソールで調査結果を確認する
- Amazon Macie の調査結果のフィルタリング

- Amazon Macieの検出結果による機密データの調査
- Amazon Macie の調査結果を抑制する
- Amazon Macie 調査結果の重要度スコアリング

Amazon Macie の調査結果のタイプ

Amazon Macie は、2 つのカテゴリの調査結果を生成します: ポリシーの調査結果と機密データの調査結果。ポリシーの検出結果は、Amazon Simple Storage Service (Amazon S3) 汎用バケットのセキュリティまたはプライバシーに関する潜在的なポリシー違反または問題の詳細なレポートです。Macie は、セキュリティとアクセスコントロールについて汎用バケットを評価およびモニタリングするための継続的な活動の一環として、ポリシーの検出結果を生成します。機密データの検出結果は、Macie が S3 オブジェクトで検出した機密データの詳細レポートです。Macie は、機密データ検出ジョブを実行したり、機密データ自動検出を実行したりすると、機密データ検出を実行するアクティビティの一部として機密データの検出結果を生成します。

各カテゴリには特定のタイプがあります。検出結果のタイプによって、Macie が検出した問題の性質や機密データに対する洞察が得られます。検出結果の詳細では、重要度評価、影響を受けたリソースに関する情報、および Macie が問題や機密データを検出したタイミングと方法などの追加情報が示されます。各検出結果の重要度と詳細は、その検出結果のタイプと性質によって異なります。

トピック

- ポリシー検出結果のタイプ
- 機密データ検出結果のタイプ

> **Tip**
>
> Macie が生成できるさまざまなカテゴリとタイプの調査結果を探索して学ぶために、検出結果のサンプルを作成 。検出結果のサンプルでは、データ例とプレースホルダー値を使用して、各タイプの調査結果に含まれる可能性のある情報の種類を示します。

ポリシー検出結果のタイプ

Amazon Macie は、S3 汎用バケットのポリシーまたは設定が、バケットとバケットのオブジェクトのセキュリティまたはプライバシーを低下させる方法で変更されたときにポリシー検出結果を生成し

ます。Macie がこれらの変更を検出する詳細については、Macie が Amazon S3 データセキュリティをモニタリングする方法 を参照してください。

Macie は、 AWS アカウントに対して Macie を有効にした後に変更が生じた場合にのみ、ポリシーの検出結果を生成します。例えば、Macie を有効にした後に S3 バケットのブロックパブリックアクセス設定が無効になっている場合、Macie はバケットの Policy:IAMUser /S3 BlockPublicAccessDisabled検出結果を生成します。Macie を有効にしたときにバケットのパブリックアクセスブロック設定が無効になっても無効のままである場合、Macie はバケットの Policy:IAMUser /S3 BlockPublicAccessDisabled検出結果を生成しません。

既存のポリシー検出結果にその後の出現を検出すると、Macie はその後の出現に関する詳細を追加し、出現カウント数を加えて検出結果を更新します。Macie は 90 日間検出結果を保存します。

Macie は、S3 汎用バケットに対して次のタイプのポリシー検出結果を生成できます。

Policy:IAMUser/S3BlockPublicAccessDisabled

バケットレベルのパブリックアクセスブロック設定がバケットに対し無効になりました。バケットへのアクセスは、アカウントのパブリックアクセスブロック設定、アクセスコントロールリスト (ACL)、およびバケットポリシーによって制御されます。

S3 バケットのブロックパブリックアクセス設定の詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 ストレージへのパブリックアクセスのブロックを参照してください。

Policy:IAMUser/S3BucketEncryptionDisabled

バケットのデフォルトの暗号化設定は、Amazon S3 マネージドキーを使用して新しいオブジェクトを自動的に暗号化するデフォルトの Amazon S3 暗号化動作にリセットされました。

2023 年 1 月 5 日以降、Amazon S3 はバケットに追加されるオブジェクトに対して、基本レベルの暗号化として Amazon S3 管理キー (SSE-S3) によるサーバーサイド暗号化を自動的に適用します。オプションで、 キーによるサーバー側の暗号化 (SSE-KMS) または AWS KMS キーによる二層式サーバー側の暗号化 AWS KMS (DSSE-KMS) を使用するようにバケットのデフォルトの暗号化設定を設定できます。S3 バケットのデフォルト暗号化設定とオプションについては、Amazon Simple Storage Service ユーザーガイドのS3 バケットのデフォルトのサーバー側の暗号化動作の設定を参照してください。

Macie が 2023 年 1 月 5 日より前にこのタイプの検出結果を生成した場合、その検出結果では、デフォルトの暗号化設定が影響するバケットでは無効になっていたことが示されます。つまり、バケットの設定では、新しいオブジェクトに対するデフォルトのサーバー側の暗号化動作

が指定されていなかったということです。バケットのデフォルトの暗号化設定を無効にする機能は、Amazon S3 ではサポートされなくなりました。

Policy:IAMUser/S3BucketPublic

匿名ユーザーまたはすべての認証済み AWS Identity and Access Management (IAM) ID によるアクセスを許可するように、バケットの ACL またはバケットポリシーが変更されました。

S3 バケットの ACL およびバケットポリシーの詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 での Identity and Access Managementを参照してください。

Policy:IAMUser/S3BucketReplicatedExternally

レプリケーションが有効になっており、組織の外部 (一部ではない) AWS アカウント にある のバケットにオブジェクトをレプリケートするように設定されています。組織は、Macie の招待を通じて、 AWS Organizations または Macie の招待によって、関連するアカウントのグループとして一元管理される一連の Macie アカウントです。

特定の条件下では、Macie は、外部 のバケットにオブジェクトをレプリケートするように設定されていないバケットに対して、このタイプの検出結果を生成することがあります AWS アカウント。これは、Macie が毎日の更新サイクル の一部として Amazon S3 からバケットとオブジェクトのメタデータを取得した後、過去 24 AWS リージョン 時間以内にレプリケート先バケットが別の に作成された場合に発生する可能性があります。この検出結果を調べるには、まずインベントリデータを更新することから始めてください。その後、バケットの詳細を確認します。詳細には、そのバケットが他のバケットにオブジェクトをレプリケートするよう設定されているかどうかが示されます。バケットがそのように設定されている場合、詳細には宛先バケットを所有する各アカウントのアカウント ID が表示されます。

S3 バケットのレプリケーション設定の詳細については、Amazon Simple Storage Service ユーザーガイドのオブジェクトのレプリケーションを参照してください。

Policy:IAMUser/S3BucketSharedExternally

バケットの ACL またはバケットポリシーが変更され、組織の外部 (一部ではない) AWS アカウント の とバケットを共有できるようになりました。組織は、Macie の招待を通じて、 AWS Organizations または Macie の招待によって、関連アカウントのグループとして一元管理される一連の Macie アカウントです。

場合によっては、Macie は外部 AWS アカウントと共有されていないバケットに対してこのタイプの検出結果を生成することがあります。これは、Macie がバケットポリシー内の `Principal` 要素と、ポリシーの `Condition` 要素内の特定

のAWS グローバル条件コンテキストキーまたは Amazon S3 条件キーとの関係を完全に評価できない場合に発生する可能性があります。適用可能な条件キーはaws:PrincipalAccount、、aws:PrincipalArn、aws:PrincipalOrgID、aws:PrincipalOrおよび ですs3:DataAccessPointArn。バケットポリシーを確認して、このアクセスが安全かつ意図されたものか判断することをお勧めします。

S3 バケットの ACL およびバケットポリシーの詳細については、Amazon Simple Storage Service ユーザーガイドのAmazon S3 での Identity and Access Managementを参照してください。

Policy:IAMUser/S3BucketSharedWithCloudFront

バケットのバケットポリシーが変更され、バケットを Amazon CloudFront オリジンアクセスアイデンティティ (OAI)、 CloudFront オリジンアクセスコントロール (OAC)、または CloudFront OAI と CloudFront OAC の両方と共有できるようになりました。 CloudFront OAI または OAC を使用すると、ユーザーは 1 つ以上の指定された CloudFrontディストリビューションを介してバケットのオブジェクトにアクセスできます。

CloudFront OAIs と OACs」を参照してください。 Amazon S3 CloudFront

> **Note**
>
> 場合によっては、Macie はバケットの Policy:IAMUser /S3 BucketSharedExternallyの検出結果の代わりに Policy:IAMUser /S3BucketSharedWithCloudFront の検出結果を生成します。そのケースは以下のとおりです。
>
> - バケットは、 CloudFront OAI または AWS アカウント OAC に加えて、組織の外部にあると共有されます。
> - バケットのポリシーは、 CloudFront OAI の Amazon リソースネーム (ARN) の代わりに正規ユーザー ID を指定します。
>
> これにより、バケットのポリシー検出結果はより重要度の高いものを生成します。

機密データ検出結果のタイプ

Macie は、機密データを検出するために分析する S3 オブジェクト内で機密データを検出するときに、機密データ検出結果を生成します。これには、機密データ検出ジョブを実行したとき、または機密データ自動検出を実行したときに Macie が実行する分析が含まれます。

例えば、機密データ検出ジョブを作成して実行し、Macie が S3 オブジェクト内の銀行口座番号を検出すると、Macie はオブジェクトの SensitiveData:S3Object /Financial 検出結果を生成します。同様に、Macie が機密データの自動検出サイクル中に分析する S3 オブジェクト内の銀行口座番号を検出すると、Macie はオブジェクトの SensitiveData:S3Object /Financial 検出結果を生成します。

Macie がその後のジョブ実行中または機密データ自動検出サイクル中に同じ S3 オブジェクト内で機密データを検出すると、Macie はそのオブジェクトに対して新しい機密データ検出結果を生成します。ポリシー検出結果とは異なり、機密データ検捨結果はすべて、新規 (一意) として処理されます。Macie は機密データの調査結果を 90 日間保存します。

Macie は、S3 オブジェクトに対して次のタイプの機密データ検出結果を生成することができます。

SensitiveData:S3Object/Credentials

オブジェクトには、 AWS シークレットアクセスキーやプライベートキーなどの機密認証情報データが含まれています。

SensitiveData:S3Object/CustomIdentifier

オブジェクトには、1 つ以上のカスタムデータ識別子の検出基準に一致するテキストが含まれています。オブジェクトには、複数のタイプの機密データが含まれている場合があります。

SensitiveData:S3Object/Financial

オブジェクトには、銀行口座番号やクレジットカード番号など機密性の高い財務情報が含まれます。

SensitiveData:S3Object/Multiple

オブジェクトには、1 つ以上のカテゴリの機密データ (1 つ以上のカスタムデータ識別子の検出基準に一致する認証情報データ、財務情報、個人情報、またはテキストの任意の組み合わせ) が含まれます。

SensitiveData:S3Object/Personal

オブジェクトには、パスポート番号や運転免許証識別番号などの個人を特定できる情報 (PII)、健康保険や医療識別番号などの個人の健康情報 (PHI)、または PII と PHI の組み合わせのような機密性の高い個人情報が含まれます。

Macie が組み込まれた基準と技術で検出できる機密データのタイプの詳細については、マネージドデータ識別子の使用 を参照してください。Macie が分析できる S3 オブジェクトのタイプの詳細については、サポートされているストレージクラスとフォーマットを参照してください。

Amazon Macie での検出結果のサンプルの使用

Amazon Macie が生成できるさまざまな types of findings (調査結果のタイプ) を探索して学ぶために、検出結果のサンプルを作成できます。検出結果のサンプルでは、データ例とプレースホルダー値を使用して、各タイプの調査結果に含まれる可能性のある情報の種類を示します。

たとえば、Policy:IAMUser/S3BucketPublic 検出結果のサンプルには、架空の Amazon Simple Storage Service (Amazon S3) バケットの詳細が含まれています。調査結果の詳細には、バケットのアクセスコントロールリスト (ACL) を変更し、バケットをパブリックにアクセスできるようにしたアクターとアクションに関するデータ例が含まれます。同様に、SensitiveData:S3Object/Multiple サンプル検出結果には、架空の Microsoft Excel スプレッドシートに関する詳細が含まれています。検出結果の詳細には、スプレッドシート内の機密データのタイプと場所に関するデータ例が含まれます。

さまざまなタイプの調査結果に含まれる可能性のある情報に習熟するのに加え、検出結果のサンプルを使用して、他のアプリケーション、サービス、およびシステムとの統合をテストできます。アカウントの suppression rules (抑制ルール) に応じて、Macie は検出結果のサンプルを Amazon EventBridge にイベントとして発行できます。検出結果のサンプルのデータ例を使用することで、これらのイベントをモニタリングおよび処理するための自動ソリューションを開発およびテストできます。アカウントで選択した 発行設定に応じて、Macie は AWS Security Hub にその検出結果のサンプルを発行することもできます。これは、検出結果のサンプルを使用して、Security Hub で Macie の調査結果をモニタリングおよび処理するためのソリューションを開発およびテストできることも意味します。調査結果をこれらのサービスに発行する方法については、調査結果のモニタリングと処理を参照してください。

トピック

- 検出結果のサンプルの作成
- 検出結果のサンプルを確認する
- 検出結果のサンプルの抑制

検出結果のサンプルの作成

Amazon Macie コンソールまたは Amazon Macie API を使用して、検出結果のサンプルを作成できます。コンソールを使用する場合、Macie がサポートする調査結果のタイプごとに 1 つの検出結果のサンプルを Macie が自動的に生成します。API を使用する場合、各タイプに対してサンプルを作成することも、指定した特定のタイプのみにサンプルを作成することもできます。

Console

Amazon Macie コンソールを使用して検出結果のサンプルを作成するには、次のステップに従います。

調査結果サンプルを作成するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定 を選択します。
3. 検出結果のサンプル で、検出結果サンプルの生成 を選択します。

API

検出結果のサンプルをプログラムで作成するには、Amazon Macie APIの CreateSampleFindings オペレーションを使用できます。リクエストを送信するときは、オプションで `findingTypes` パラメータを使用して、作成する特定のタイプの検出結果のサンプルのみを指定します。すべてのタイプのサンプルを自動的に作成するには、このパラメータをリクエストに含めないでください。

AWS Command Line InterfaceAWS CLIを使用して検出結果のサンプルを作成するには、create-sample-findings コマンドを実行します。すべてのタイプの調査結果のサンプルを自動的に作成するには、`finding-types` パラメータを含めないでください。特定のタイプの調査結果のみのサンプルを作成するには、このパラメータを含めて、作成する検出結果のサンプルのタイプを指定します。例:

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

ここで、*SensitiveData:S3Object/Multiple* は、作成する機密データの調査結果のタイプで、*SensitiveData:S3Object/Multiple* は、作成するポリシーの調査結果のタイプです。

コマンドが正常に実行されると、Macie は空のレスポンスを返します。

検出結果のサンプルを確認する

作成した検出結果のサンプルを特定しやすくするために、Macie は各検出結果のサンプルの Sample (サンプル) フィールドの値を True に設定しています。さらに、影響を受けた S3 バケットの名前

は、すべての検出結果のサンプルで同じです (macie-sample-finding-bucket)。Amazon Macie コンソールの 検出結果ページを使用してサンプル検出結果を確認する場合、Macie は各サンプルの 検出結果タイプの SAMPLE プレフィックスも表示します。

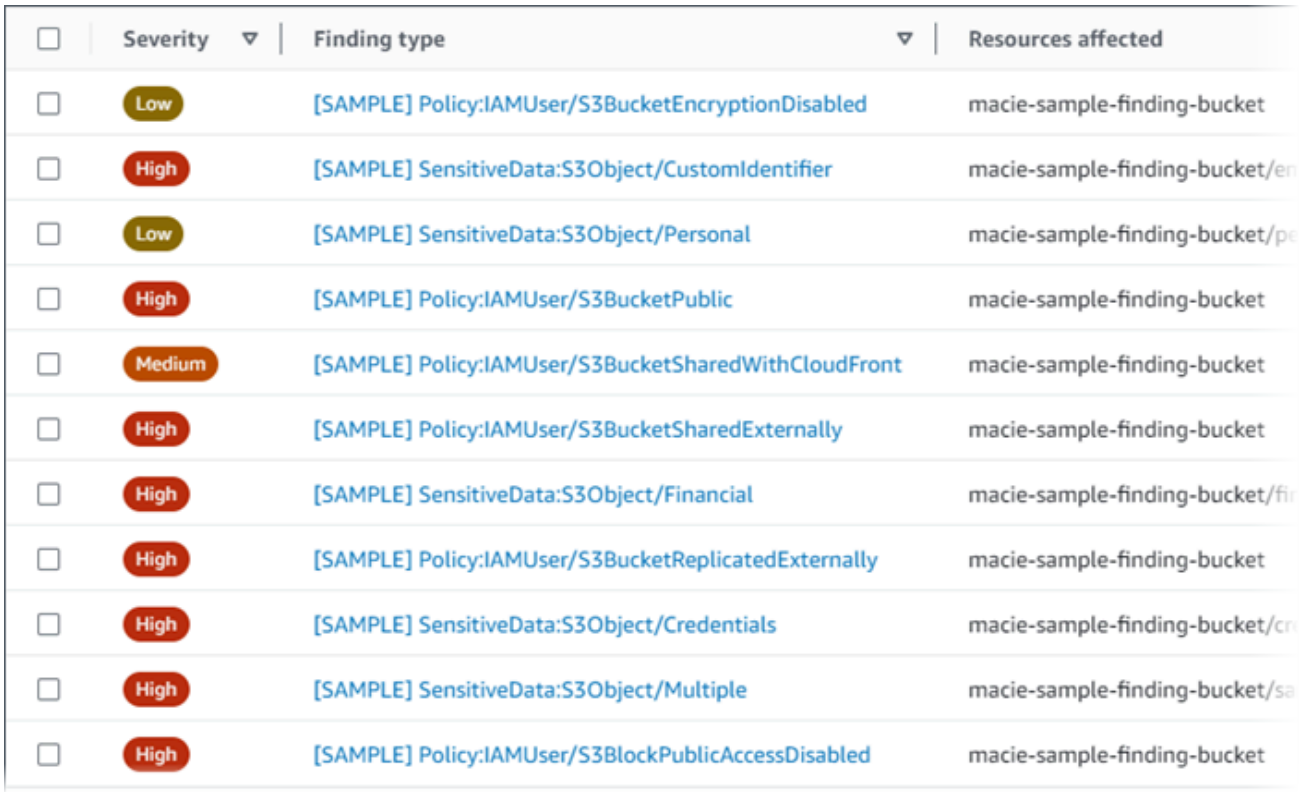
Console

Amazon Macie コンソールを使用して検出結果のサンプルを確認するには、次のステップに従います。

検出結果のサンプルを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果を選択します。
3. 調査結果ページで、次のいずれかの操作を行います。

   - 調査結果タイプ列で、次のイメージに示すように、タイプが サンプル で始まる調査結果を見つけます。



   - テーブルの上にある フィルタ条件 ボックスを使用して、テーブルをサンプル検出結果のみにフィルタリングします。これを行うには、ボックスにカーソルを合わせます。表示されるフィールドのリストで、サンプルを選択します。True を選択し、次に 適用を選択します。これにより、次のフィルター条件がテーブルに追加されます。

4. 特定のサンプル検出結果の詳細を確認するには、検出結果を選択します。詳細パネルに、調査結果の情報が表示されます。

1 つ以上の検出結果のサンプルの詳細を JSON ファイルとしてダウンロードして保存することもできます。これを行うには、ダウンロードして保存する各検出結果のサンプルのチェックボックスをオンにします。次に、調査結果 ページ上部にある アクション メニューで (JSON)をエクスポート を選択します。表示されたウィンドウで、ダウンロードを選択します。検出結果に含めることができる JSON フィールドの詳細については、Amazon Macie API リファレンスの検出結果を参照してください。

API

検出結果のサンプルをプログラムで確認するには、まず Amazon Macie API の ListFindings オペレーションを使用して、作成した各検出結果のサンプルの一意の識別子`findingId`を取得します。次に、GetFindings オペレーションを使用して、それらの調査結果の詳細を取得します。

ListFindings リクエストを送信するときに、結果に検出結果のサンプルのみを含めるようにフィルター基準を指定できます。これを行うには、`sample` フィールドの値が `true` であるフィルター条件を追加します。AWS CLI を使用している場合、list-findings コマンドを実行し、`finding-criteria` パラメータを使用して、フィルター条件を指定します。例:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"sample\":{\"eq\":[\"true\"]}}}
```

リクエストが成功すると、Macie は `findingIds` 配列を返します この配列には、現在の AWS リージョン 内のアカウントの検出結果のサンプルごとに一意の識別子がリスト化されています。

次に、検出結果のサンプルの詳細を取得するには、GetFindings リクエスト内のこれらの一意の識別子を指定するか、AWS CLI では、get-findings コマンドを実行しているときに行います。

検出結果のサンプルの抑制

他の調査結果と同様に、Macie は検出結果のサンプルを 90 日間保存します。サンプルの確認と実験が終了したら、必要に応じて 抑制ルールの作成 を行い、サンプルをアーカイブできます。これを行うと、検出結果のサンプルがデフォルトでコンソールに表示されなくなるため、それらのステータスが archived (アーカイブ済み) に変わります。

Amazon Macie コンソールを使用してサンプル結果をアーカイブするには、サンプル フィールドの値が True である場合、調査結果をアーカイブするようにルールを設定します。Amazon Macie API を使用してサンプル結果をアーカイブするには、`sample` フィールドの値が `true` である場合、調査結果をアーカイブするようにルールを設定します。

Amazon Macie コンソールで調査結果を確認する

Amazon Macie は、Amazon Simple Storage Service (Amazon S3) 汎用バケットのセキュリティまたはプライバシーに関する潜在的なポリシー違反または問題を検出すると、 AWS 環境を監視し、ポリシーの検出結果を生成します。Macie は、S3 オブジェクト内の機密データを検出するときに、機密データの検出結果を生成します。Macie は、ポリシーと機密データの調査結果を 90 日間保存します。

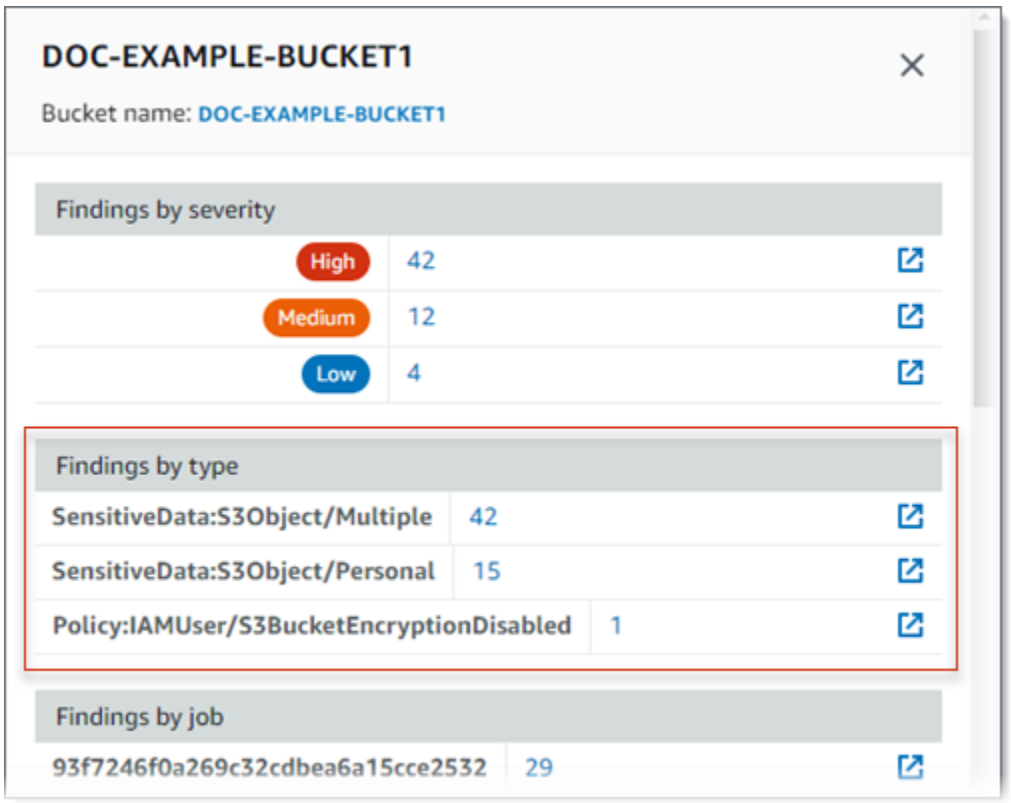
検出結果ごとに、検出結果タイプと重要度のランク付けが指定されます。追加の詳細には、影響を受けるリソースに関する情報、および Macie が問題を検出した時期と方法、または検出結果により報告された機密データが含まれます。各検出結果の重要度と詳細は、その検出結果のタイプと性質によって異なります。

Amazon Macie コンソールを使用して、調査結果を確認して分析し、個別の調査結果の詳細にアクセスできます。1 つ以上の検出結果を JSON ファイルにエクスポートすることもできます。分析を合理化するために、コンソールには、調査結果のカスタムビューを構築するためのいくつかのオプションが用意されています。

事前定義されたグループを使用する

特定のページを使用して、影響を受けた S3 バケット、調査結果タイプ、機密データ検出ジョブなどの基準別にグループ化された結果を確認します。これらのページでは、重要度別の調査結果の数など、各グループの集計された統計を確認できます。ドリルダウンして、グループ内の個別の調査結果の詳細を確認したり、フィルターを適用して分析を絞り込んだりすることもできます。

例えば、すべての検出結果を S3 バケット別にグループ化し、特定のバケットにポリシー違反があることに注目した場合、バケットに機密データもまた含まれているかどうかをすばやく判断できます。これを行うには、ナビゲーションペイン (調査結果の下) の バケット別を選択し、バケットを選択します。表示される詳細パネルでは、タイプ別の検出結果 セクションには、バケットに適用される検出結果のタイプが、次の図のように一覧になっています。

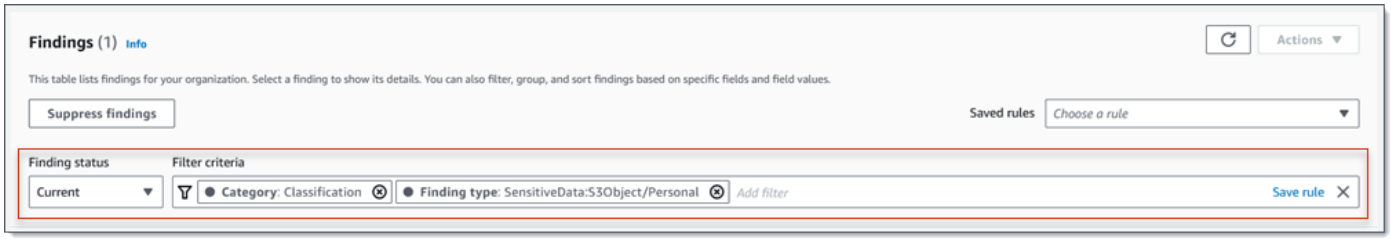


特定のタイプを調べるには、そのタイプの番号を選択します。Macie は、選択したタイプに一致し、S3 バケットに適用されるすべての検出結果のテーブルを表示します。調査結果を絞り込むには、テーブルをフィルタリングします。

フィルターを作成して適用

特定の調査結果属性を使用して、特定の調査結果を 調査結果テーブルに含めるか除外します。検出結果の属性とは、検出結果タイプ、重要度、影響する S3 バケットの名前など、検出結果用に特定データを保存するフィールドです。テーブルをフィルタリングすると、特定の特性を持つ調査結果をより簡単に特定できます。次に、ドリルダウンして、それらの調査結果の詳細を確認できます。

例えば、ポリシーの検出結果をすべて確認するには、カテゴリ フィールドでフィルター条件を追加します。結果を絞り込み、特定タイプのポリシーの機密データ検出結果のみ含めるには、検出結果タイプ フィールドでフィルター条件を追加します。例:



特定の調査結果の詳細を確認するには、調査結果を選択します。詳細パネルに、調査結果の情報が表示されます。

特定のフィールドで、調査結果を昇順または降順で並べ替えることもできます。これを行うには、フィールドの列見出しを選択します。ソート順序を変更するには、列見出しを再度選択します。

コンソールで調査結果を確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果を選択します。検出結果ページには、Macie が AWS リージョン 過去 90 日間に現在の でアカウントに対して作成または更新された検出結果が表示されます。デフォルトでは、これには 抑制ルールで抑制された調査結果は含まれません。
3. 事前定義の論理グループで検出結果をピボットして確認するには、ナビゲーションペイン (検出結果 の下) の バケット別 、タイプ別、または ジョブ別 を選択します。次に、テーブル内の項目を選択します。詳細パネルで、ピボットするフィールドのリンクを選択します。
4. (任意) 特定の条件で検出結果をフィルターするには、テーブル上のにフィルターオプションを使用します。

   - 抑制ルールによって抑制された検出結果を表示するには、 検出結果ステータス メニューを使用します。すべて を選択して、抑制または非抑制の検出結果の両方を表示するか、アーカイブ済み を選択して、抑制された検出結果のみを表示します。非表示にした結果を再度非表示にするには、[現在]を選択します。
   - 特定の属性を持つ検出結果のみを表示するには、[フィルター条件] ボックスを使用します。ボックスにカーソルを置き、属性のフィルター条件を追加します。調査結果をさらに絞り込むには、追加の属性で条件を追加します。条件を削除するには、削除する条件の条件アイコン ⊗ を選択します。

   検出結果フィルターの詳細については、フィルターの作成と調査結果への適用 を参照してください。
5. 結果を特定のフィールドでソートするには、フィールドの列見出しを選択します。ソート順序を変更するには、列見出しを再度選択します。
6. 特定の検出結果の詳細を確認するには、検出結果を選択します。詳細パネルに、調査結果の情報が表示されます。

> **Tip**
>
> 詳細パネルを使用して、特定のフィールドをピボットおよびドリルダウンすることもできます。フィールドに対して同じ値を持つ調査結果を表示するには、フィールドで
>
> 
>
> を選択します。または
>
> 
>
> を選択して、フィールドの他の値を持つ調査結果を表示します。
> 機密データの検出結果では、Macie が影響する S3 オブジェクトで見つけた機密データを調査する詳細パネルを使用することもできます。
>
> - 特定タイプの機密データの出現を見つけるには、そのタイプのデータのフィールドで数値リンクを選択します。Macie は Macie がデータを見つけた場所に関する情報を (JSON 形式で) 表示します。詳細については、機密データを見つけるを参照してください。
> - Macie が検出した機密データのサンプルを取得するには、[サンプルを公開] フィールドで [確認] を選択します。詳細については、機密データのサンプルの取得を参照してください。
> - 対応する機密データの検出結果に移動するには、Detailed result location (詳細な調査結果の場所) フィールドのリンクを選択します。Macie は Amazon S3 コンソールを開き、検出結果を含むファイルまたはフォルダーを表示します。詳細については、機密データ検出結果の保存と保持を参照してください。

1 つ以上の調査結果の詳細を JSON ファイルとしてダウンロードして保存することもできます。これを行うには、ダウンロードして保存する各調査結果のチェックボックスをオンにします。次に、検出結果 ページの上部にある アクション メニューで エクスポート (JSON) を選択します。表示されたウィンドウで、ダウンロードを選択します。検出結果に含めることができる JSON フィールドの詳細については、Amazon Macie API リファレンスの検出結果を参照してください。

Amazon Macie の調査結果のフィルタリング

ターゲット分析を実行し、調査結果をより効率的に分析するために、Amazon Macie の調査結果をフィルタリングできます。フィルターを使用すると、調査結果のカスタムビューとクエリを構築します。これは特定の特性を持つ調査結果を特定して、それに焦点を絞るのに役立ちます。Amazon

Macie コンソールを使用して調査結果をフィルタリングするか、Amazon Macie API を使用してプログラムでクエリを送信します。

フィルターを作成するときは、調査結果の特定の属性を使用して、ビューまたはクエリ結果から結果を含めるか除外するための基準を定義できます。調査結果の属性は、調査結果が適用される S3 バケットの重要度、タイプ、名前などの特定のデータを保存するフィールドです。

Macie では、フィルターは 1 つ以上の条件で設定されます。各条件は、基準とも呼ばれ、3 つの部分で設定されています。

- 属性ベースのフィールド (重要度や 調査結果タイプなど)。
- 演算子 (と等しい や 等しくない など)。
- 1 つまたは複数の値。値のタイプと数は、選択するフィールドと演算子によって異なります。

再度使用するフィルターを作成する場合は、それを フィルタールール (フィルタールール) として保存できます。フィルタールールは、Amazon Macie コンソールで調査結果を表示するときに再度適用するために作成および保存するフィルター基準のセットです。

また、フィルターを 抑制ルールとして保存することもできます。抑制ルールは、ルールの基準を満たす調査結果を自動的にアーカイブするために作成および保存するフィルター基準のセットです。抑制ルールの詳細については、調査結果を抑制するを参照してください。

トピック

- 調査結果のフィルタリングの基礎
- フィルターの作成と調査結果への適用
- 調査結果のフィルタールールの作成と管理
- 調査結果をフィルタリングするためのフィールド

調査結果のフィルタリングの基礎

フィルターを作成する場合は、次の特徴とガイドラインに留意してください。また、フィルタリングされた結果は、過去 90 日間と現在の AWS リージョン に限定されることにも注意してください。Amazon Macie は、調査結果をそれぞれの AWS リージョン で90日間だけ保存します。

トピック

- フィルターで複数の条件を使用する
- フィールドの値を指定する

- 1 つのフィールドに複数の値を指定する
- 条件での演算子の使用

フィルターで複数の条件を使用する

フィルターには、1 つ以上の条件を含めることができます。各条件は、criterion (基準) とも呼ばれ、3 つの部分で設定されています。

- 属性ベースのフィールド (Severity (重要度) や Finding type (調査結果タイプ) など)。使用できるフィールドのリストについては、調査結果をフィルタリングするためのフィールドを参照してください。
- 演算子 (equals や not equals など)。使用できる演算子のリストについては、条件での演算子の使用を参照してください。
- 1 つまたは複数の値。値のタイプと数は、選択するフィールドと演算子によって異なります。

フィルターに複数の条件が含まれている場合、Macie は AND ロジックを使用して条件を結合し、フィルター基準を評価します。これは、調査結果は、すべて のフィルター内の条件に一致した場合にのみ、フィルター基準を満たすことを意味します。

たとえば、重要度の高い調査結果のみを含めるように条件を追加し、機密データの調査結果のみを含めるように別の条件を追加した場合、Macie は高い重要度の機密データの調査結果をすべて返します。つまり、Macie は、すべてのポリシーの調査結果と、中程度の重要度および低い重要度の機密データの調査結果をすべて除外します。

フィルターでは、フィールドを 1 回だけ使用できます。ただし、多くのフィールドに複数の値を指定することができます。

たとえば、高い重要度の調査結果のみを含めるように条件で Severity (重要度) フィールドを使用する場合は、中程度の重要度または低い重要度の調査結果を含めるように別の条件で Severity (重要度) フィールドを使用することはできません。代わりに、既存の条件に複数の値を指定するか、既存の条件に別の演算子を使用します。たとえば、中程度の重要度と高い重要度の調査結果をすべて含めるには、Severity (重要度) equals Medium, High (中、高) 条件を追加するか、Severity (重要度) not equals Low (低) 条件を追加します。

フィールドの値を指定する

フィールドの値を指定する場合、値はフィールドの基盤となるデータタイプに準拠する必要があります。フィールドに応じて、次のいずれかのタイプの値を指定できます。

テキスト (文字列) の配列

フィールドのテキスト (文字列) 値のリストを指定します。各文字列は、フィールドの事前定義された値または既存の値と相関します。たとえば、重要度フィールドでは 高、調査結果タイプフィールドでは SensitiveData:S3Object/Financial、または S3 バケット名 フィールドでは S3 バケットの名前です。

配列を使用する場合は、次の点に注意してください。

- 値は大文字と小文字が区別されます。
- 部分的な値を指定したり、値にワイルドカード文字を使用したりすることはできません。フィールドに完全で有効な値を指定する必要があります。

たとえば、my-S3-bucket という名前の S3 バケットの調査結果をフィルタリングするには、S3 バケット名 フィールドの値として **`my-S3-bucket`** と入力します。**`my-s3-bucket`** や **`my-S3`** などの他の値を入力した場合、Macie はバケットの調査結果を返しません。

各フィールドの有効な値のリストについては、調査結果をフィルタリングするためのフィールドを参照してください。

配列には、最大 50 個までの値を指定できます。値の指定方法は、1 つのフィールドに複数の値を指定するで説明されているように、Amazon Macie コンソールと Amazon Macie API のどちらを使用するかによって異なります。

ブール値

フィールドの 2 つの相互に排他的な値のうちの 1 つを指定します。

Amazon Macie コンソールを使用してこのタイプの値を指定する場合、コンソールには選択可能な値のリストが表示されます。Amazon Macie API を使用する場合は、値で `true` または `false` を指定します。

日付/時刻 (および時間範囲)

フィールドで絶対的な日付と時刻を指定します。このタイプの値を指定する場合は、日付と時刻の両方を指定する必要があります。

Amazon Macie コンソールでは、日付と時刻の値はお客様のローカルタイムゾーンにあり、24 時間表記を使用します。その他のすべてのコンテキストでは、これらの値は協定世界時 (UTC) 形式および拡張 ISO 8601 形式になります。たとえば、2:31:13 PM UTC September 1, 2020 では、`2020-09-01T14:31:13Z`。

フィールドに日付/時刻値が保存されている場合、フィールドを使用して固定時間範囲または相対時間範囲を定義できます。たとえば、2 つの特定の日時の間に作成された調査結果のみ、または特定の日時の前後に作成された調査結果のみを含めることができます。時間範囲の定義方法は、Amazon Macie コンソールと Amazon Macie API のどちらを使用するかによって異なります。

- コンソールで、日付ピッカーを使用するか、テキストを From および To ボックスに直接入力します。
- API を使用して、範囲内の最初の日付と時刻を指定する条件を追加して固定時間範囲を定義し、範囲内の最後の日付と時刻を指定する別の条件を追加します。これを行うと、Macie は AND ロジックを使用して条件を結合します。相対時間範囲を定義するには、範囲内の最初または最後の日付と時刻を指定する条件を 1 つ追加します。値を Unix のタイムスタンプとしてミリ秒単位で指定します。たとえば、22:49:32 UTC November 5, 2020 では、`1604616572653`。

コンソールでは、時間範囲は包括的です。API を使用すると、選択した演算子に応じて、時間範囲を包括的または排他的にすることができます。)

数値 (および数値範囲

フィールドで長い整数を指定します。

フィールドに数値が保存されている場合、フィールドを使用して固定または相対数値範囲を定義できます。たとえば、S3 オブジェクトでは、50 ~ 90 回の機密データの出現をレポートする結果のみを含めることができます。数値範囲の定義方法は、Amazon Macie コンソールと Amazon Macie API のどちらを使用するかによって異なります。

- コンソールで、From および To ボックスを使用して、範囲内の最小および最大の数値をそれぞれ入力します。
- API を使用して、範囲内の最小の数値を指定する条件を追加して固定数値範囲を定義し、範囲内の最大の数値を指定する別の条件を追加します。これを行うと、Macie は AND ロジックを使用して条件を結合します。相対数値範囲を定義するには、範囲内の最小または最大の数値を指定する条件を 1 つ追加します。

コンソールでは、数値範囲は包括的です。API を使用すると、選択した演算子に応じて、数値範囲を包括的または排他的にすることができます。

テキスト (文字列)。

フィールドの単一のテキスト (文字列) 値を指定します。各文字列は、フィールドの事前定義された値または既存の値と相関します。たとえば、重要度フィールドでは 高、S3 バケット名 フィー

ルドでは S3 バケットの名前、または ジョブ ID フィールドでは機密データ検出ジョブの一意の識別子です。

単一のテキスト文字列を指定する場合は、次の点に注意してください。

- 値は大文字と小文字が区別されます。
- 部分的な値を使用したり、値にワイルドカード文字を使用したりすることはできません。フィールドに完全で有効な値を指定する必要があります。

たとえば、my-S3-bucket という名前の S3 バケットの調査結果をフィルタリングするには、S3 バケット名 フィールドの値として **my-S3-bucket** と入力します。**my-s3-bucket** や **my-S3** などの他の値を入力した場合、Macie はバケットの調査結果を返しません。

各フィールドの有効な値のリストについては、調査結果をフィルタリングするためのフィールドを参照してください。

1 つのフィールドに複数の値を指定する

特定のフィールドと演算子では、フィールドに複数の値を指定できます。これを行うと、Macie は OR ロジックを使用して値を結合し、フィルター基準条件を評価します。これは、調査結果は、フィールドの値の いずれか を持つ場合に、基準を満たすことを意味します。

たとえば、調査結果タイプ の値がSensitiveData:S3Object/Financial, SensitiveData:S3Object/Personalと等しい調査結果を含めるように条件を追加した場合、Macie は財務データのみを含む S3 オブジェクトと、個人情報のみを含む S3 オブジェクトの機密データの調査結果を返します。つまり、Macie はすべてのポリシーの調査結果を除外します。Macie は、他のタイプの機密データまたは複数のタイプの機密データを含むオブジェクトに関するすべての機密データの調査結果を除外します。

例外は、eqExactMatch 演算子を使用する条件です。この演算子では、Macie は AND ロジックを使用して値を結合し、フィルター基準を評価します。これは、調査結果は、フィールドの値の すべて およびフィールドのそれらの値 のみ を持つ場合のみ、基準を満たすことを意味します。この演算子の詳細については、条件での演算子の使用を参照してください。

フィールドに複数の値を指定する方法は、Amazon Macie API と Amazon Macie コンソールのどちらを使用するかによって異なります。API では、値をリスト化する配列を使用します。

コンソールでは通常、リストから値を選択します。ただし、一部のフィールドでは、値ごとに異なる条件を追加する必要があります。たとえば、Macie が特定のカスタムデータ識別子を使用して検出したデータの調査結果を含めるには、以下を行います。

1. フィルター条件 ボックスにカーソルを置き、カスタムデータ識別子名 フィールドを選択します。カスタムデータ識別子の名前を入力し、適用 を選択します。
2. フィルターで指定する追加のカスタムデータ ID ごとに、上記のステップを繰り返します。

これを行う必要があるフィールドのリストについては、調査結果をフィルタリングするためのフィールドを参照してください。

条件での演算子の使用

個別の条件で、次のタイプの演算子を使用できます。

等しいeq

フィールドで指定された値に一致します (=)。次のタイプの値を持つ equals 演算子を使用できます: テキスト (文字列) の配列、ブール値、日付/時刻、数値、テキスト (文字列)。

多くのフィールドでは、この演算子を使用して、フィールドの値を最大 50 個まで指定できます。これを行うと、Macie は OR ロジックを使用して値を結合します。これは、調査結果は、フィールドの指定された値のいずれかを持つ場合に、基準を満たすことを意味します。

例:

- 財務情報、個人情報、または財務情報と個人情報両方の出現をレポートする調査結果を含めるには、機密データのカテゴリ フィールドとこの演算子を使用する条件を追加し、財務情報と個人情報 をフィールドの値として指定します。
- クレジットカード番号、郵送先住所、またはクレジットカード番号と郵送先住所の両方の出現を報告する調査結果を含めるには、機密データ検出タイプフィールドに条件を追加し、この演算子を使用し、フィールドの値として CREDIT_CARD_NUMBERとADDRESS を指定します。

Amazon Macie API を使用して日付/時刻値でこの演算子を使用する条件を定義する場合は、その値を Unix タイムスタンプとしてミリ秒単位で指定します。たとえば、22:49:32 UTC November 5, 2020 では、`1604616572653`。

完全一致eqExactMatch

フィールドに指定されたすべての値に排他的に一致します。フィールドの選択セットを持つ equals exact match (完全一致と等しい) 演算子を使用できます。

この演算子を使用してフィールドに複数の値を指定すると、Macie は AND ロジックを使用して値を結合します。これは、調査結果は、フィールドの指定された値の すべて およびフィールド

のそれらの値 のみ を持つ場合のみ、基準を満たすことを意味します。フィールドには、最大 50 個までの値を指定できます。

例:

- クレジットカード番号の発生を報告し、他のタイプの機密データを報告しない調査結果を含めるには、機密データ検出タイプフィールドに条件を追加し、この演算子を使用し、フィールドの唯一の値としてCREDIT_CARD_NUMBERを指定します。
- クレジットカード番号と郵送先住所の両方の発生を報告する調査結果を含めるには (他のタイプの機密データは含まず)、機密データ検出タイプフィールドに条件を追加し、この演算子を使用し、フィールドの値として CREDIT_CARD_NUMBER とADDRESSを指定します。

Macie は AND ロジックを使用してフィールドの値を結合するため、同じフィールドの他の演算子と組み合わせてこの演算子を使用することはできません。つまり、1 つの条件でフィールドの完全一致と等しい 演算子を使用する場合、同じフィールドを使用する他のすべての条件でそれを使用する必要があります。

他の演算子と同様に、フィルター内の複数の条件で 完全一致と等しい 演算子を使用できます。これを行うと、Macie は AND ロジックを使用して条件を結合し、フィルターを評価します。これは、調査結果は、フィルター内の すべて の条件によって指定された すべて の値を持つ場合のみ、フィルター基準を満たすことを意味します。

たとえば、特定の時間後に作成された結果を含めるようにし、クレジットカード番号の出現をレポートし、他のタイプの機密データをレポートしない場合は、以下を行います。

1. 作成日時 フィールドを使用し、以上演算子を使用し、フィルターの開始日時を指定する条件を追加します。
2. 機密データ検出タイプフィールドを使用し、完全一致と等しい演算子を使用し、フィールドの唯一の値としてCREDIT_CARD_NUMBERを指定する別の条件を追加する。

次のフィールドを持つ 完全一致と等しい 演算子を使用できます。

- カスタムデータ識別子`customDataIdentifiers.detections.arn`
- カスタムデータ識別子`customDataIdentifiers.detections.name`
- S3 バケットタグキー`resourcesAffected.s3Bucket.tags.key`
- S3 バケットタグ値`resourcesAffected.s3Bucket.tags.value`
- S3 オブジェクトタグキー`resourcesAffected.s3Object.tags.key`
- S3 オブジェクトタグ値`resourcesAffected.s3Object.tags.value`
- 機密データの検出タイプ`sensitiveData.detections.type`

- 機密データのカテゴリsensitiveData.category

前のリストでは、括弧内の名前は、調査結果と Amazon Macie API の JSON 表現内のフィールドの名前を示すために、ドット表記を使用しています。

gtより大きい

フィールドに指定された値より大きい (>)。数値と日付/時刻の値を持つ greater than (~ より大きい) 演算子を使用できます。

たとえば、S3 オブジェクトで 90 件を超える機密データの出現をレポートする調査結果のみを含めるには、Sensitive data total count (機密データの合計カウント) フィールドとこの演算子を使用する条件を追加し、フィールドの値として 90 を指定します。Amazon Macie コンソールでこれを行うには、From ボックスに **91** と入力し、To ボックスには値を入力せず、次に Apply (適用) を選択します。コンソールでは、数値と時間ベースの比較は包括的です。

Amazon Macie API を使用してこの演算子を使用する時間範囲を定義する場合は、日付/時刻の値を Unix タイムスタンプとしてミリ秒単位で指定する必要があります。たとえば、22:49:32 UTC November 5, 2020では、1604616572653。

gteより大きいか等しい

この値は、フィールドで指定した値以上 (>=) にする必要があります。数値と日付/時刻の値を持つ greater than or equal to (~ 以上) 演算子を使用できます。

たとえば、S3 オブジェクトで 90 件以上の機密データの出現をレポートする調査結果のみを含めるには、Sensitive data total count (機密データの合計カウント) フィールドとこの演算子を使用する条件を追加し、フィールドの値として 90 を指定します。Amazon Macie コンソールでこれを行うには、From ボックスに **90** と入力し、To ボックスには値を入力せず、次に 適用 を選択します。

Amazon Macie API を使用してこの演算子を使用する時間範囲を定義する場合は、日付/時刻の値を Unix タイムスタンプとしてミリ秒単位で指定する必要があります。たとえば、22:49:32 UTC November 5, 2020では、1604616572653。

lt未満

フィールドに指定された値より小さい (<)。数値と日付/時刻の値を持つ Less than (lt) (~ より小さい (lt)) 演算子を使用できます。

たとえば、S3 オブジェクトで 90 件未満の機密データの出現をレポートする調査結果のみを含めるには、Sensitive data total count (機密データの合計カウント) フィールドとこの演算子を使用する条件を追加し、フィールドの値として 90 を指定します。Amazon Macie コンソールでこれを

行うには、To ボックスに **89** と入力し、From ボックスには値を入力せず、次に 適用 を選択します。コンソールでは、数値と時間ベースの比較は包括的です。

Amazon Macie API を使用してこの演算子を使用する時間範囲を定義する場合は、日付/時刻の値を Unix タイムスタンプとしてミリ秒単位で指定する必要があります。たとえば、22:49:32 UTC November 5, 2020では、`1604616572653`。

lte以下

この値は、フィールドで指定した値以下 (<=) にする必要があります。数値と日付/時刻の値を持つ ~以下 演算子を使用できます。

たとえば、S3 オブジェクトで 90 件以下の機密データの出現をレポートする調査結果のみを含めるには、Sensitive data total count (機密データの合計カウント) フィールドとこの演算子を使用する条件を追加し、フィールドの値として 90 を指定します。Amazon Macie コンソールでこれを行うには、To ボックスに **`90`** と入力し、From ボックスには値を入力せず、次に 適用 を選択します。

Amazon Macie API を使用してこの演算子を使用する時間範囲を定義する場合は、日付/時刻の値を Unix タイムスタンプとしてミリ秒単位で指定する必要があります。たとえば、22:49:32 UTC November 5, 2020では、`1604616572653`。

neq等しくない

フィールドで指定された値に一致しません (≠)。次のタイプの値を持つ not equals 演算子を使用できます: テキスト (文字列) の配列、ブール値、日付/時刻、数値、テキスト (文字列)。

多くのフィールドでは、この演算子を使用して、フィールドの値を最大 50 個まで指定できます。これを行うと、Macie は OR ロジックを使用して値を結合します。これは、調査結果は、フィールドの指定された値の いずれか を持たない場合に、基準を満たすことを意味します。

例:

- 財務情報、個人情報、または財務情報と個人情報両方の出現をレポートする調査結果を除外するには、機密データのカテゴリ フィールドとこの演算子を使用する条件を追加し、財務情報 と 個人情報 をフィールドの値として指定します。
- クレジットカード番号の出現を報告する調査結果を除外するには、機密データ検出タイプフィールドに条件を追加し、この演算子を使用し、フィールドの値として CREDIT_CARD_NUMBER を指定します。
- クレジットカード番号、郵送先住所、またはクレジットカード番号と郵送先住所の両方の出現を報告する調査結果を除外するには、機密データ検出タイプフィールドに条件を追加し、こ

の演算子を使用し、フィールドの値としてCREDIT_CARD_NUMBER とADDRESSを指定します。

Amazon Macie API を使用して日付/時刻値でこの演算子を使用する条件を定義する場合は、その値を Unix タイムスタンプとしてミリ秒単位で指定します。たとえば、22:49:32 UTC November 5, 2020 では、1604616572653。

フィルターの作成と調査結果への適用

特定の特性を持つ調査結果を特定し、それに焦点を絞るには、Amazon Macie コンソールで、および Amazon Macie API を使用してプログラムで送信するクエリで調査結果をフィルタリングできます。フィルターを作成するときは、調査結果の特定の属性を使用して、ビューまたはクエリ結果から結果を含めるか除外するための基準を定義できます。調査結果の属性は、調査結果が適用される S3 バケットの重要度、タイプ、名前などの特定のデータを保存するフィールドです。

Macie では、フィルターは 1 つ以上の条件で設定されます。各条件は、基準とも呼ばれ、3 つの部分で設定されています。

- 属性ベースのフィールド (重要度や 調査結果タイプなど)。
- 演算子 (と等しい や 等しくない など)。
- 1 つまたは複数の値。値のタイプと数は、選択するフィールドと演算子によって異なります。

フィルター条件の定義および適用方法は、Amazon Macie コンソールと Amazon Macie API のどちらを使用するかによって異なります。

トピック

- Amazon Macie コンソールでの調査結果のフィルタリング
- Amazon Macie API を用いて調査結果をプログラムでフィルタリングする

Amazon Macie コンソールでの調査結果のフィルタリング

Amazon Macie コンソールを使用して調査結果をフィルタリングする場合、Macie は個別の条件のフィールド、演算子、値を選択するのに役立つオプションを提供します。これらのオプションにアクセスするには、次の画像に示すように、調査結果ページのフィルターバーを使用します。

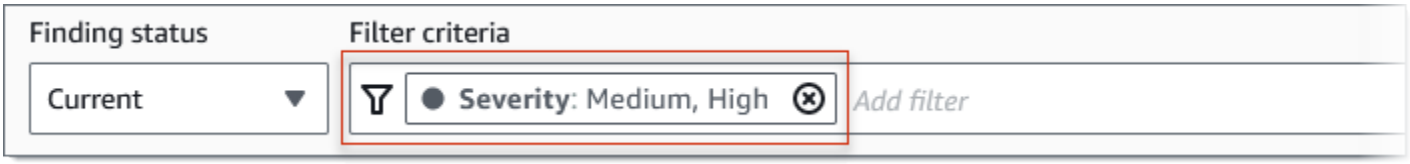
検出結果のステータスメニューを使用して、抑制ルールによって抑制 (自動的にアーカイブ) された結果を含めるかどうかを指定できます。フィルター条件ボックスを使用すると、フィルター条件を入力できます。

フィルター条件ボックスにカーソルを置くと、Macie はフィルター条件で使用できるフィールドのリストを表示します。フィールドは論理カテゴリ別に整理されています。たとえば、一般的なフィールドカテゴリには、任意のタイプの調査結果に適用されるフィールドが含まれ、分類フィールドカテゴリには、機密データの調査結果にのみ適用されるフィールドが含まれます。フィールドは、各カテゴリ内でアルファベット順に並べ替えられます。

条件を追加するには、まずリストからフィールドを選択します。フィールドを見つけるには、完全なリストを参照するか、フィールド名の一部を入力してフィールドのリストを絞り込みます。

選択したフィールドに応じて、Macie は異なるオプションを表示します。オプションには、選択したフィールドのタイプと性質が反映されます。たとえば、重要度フィールドを選択した場合、Macie は選択する値のリストを表示します (低、中、および高)。S3 バケット名フィールドを選択した場合、Macie は、バケット名を入力できるテキストボックスを表示します。どのフィールドを選択しても、Macie はフィールドに必要な設定を含む条件を追加するステップを順を追ってガイドします。

条件を追加すると、次の図に示すように、Macie はその条件の基準を適用し、フィルター条件ボックスのフィルタートークンに条件を追加します。



この例では、中程度の重要度および高い重要度の調査結果をすべて含め、低い重要度の調査結果をすべて除外するように条件が設定されています。これは、重要度フィールドの値 と等しい 中 または 高 の場合に調査結果を返します。

> **Tip**
>
> 多くのフィールドでは、条件のフィルタートークンの等しいアイコン
> ●
> を選択して、条件の演算子を equalsと等しいから等しくないに変更できます。これを行うと、Macie は演算子を等しくないに変更し、トークンに 等しくない アイコン
> ⦸
> を表示します。再度 と等しい 演算子に切り替えるには、等しくない アイコンを選択します。

条件を追加すると、Macie はその基準を適用し、それらをフィルター条件ボックスのトークンに追加します。フィルターボックスをいつでも参照して、適用した基準を確認できます。条件を削除するには、条件のトークンで 条件の削除アイコン
⊗
を選択します。

コンソールを使用して調査結果をフィルタリングするには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 結果 を選択します。
3. (オプション) 事前定義された論理グループで調査結果をピボットして確認するには、ナビゲーションペイン (調査結果の下) の バケット別、タイプ別、または ジョブ別を選択し、次にテーブル内で項目を選択します。次に、テーブル内の項目を選択します。詳細パネルで、ピボットするフィールドのリンクを選択します。
4. (オプション) 抑制ルールによって抑制された調査結果を表示するには、フィルターバーの 現在を選択します。次に アーカイブ済みを選択して、抑制された調査結果のみを表示するか、すべてを選択して、現在の調査結果と抑制された調査結果の両方を表示します。非表示になっている検出結果を非表示にするには、 現在を選択します。
5. フィルタ条件を追加するには:

   a. フィルター条件ボックスにカーソルを置き、条件に使用するフィールドを選択します。使用可能なフィールドの詳細については、調査結果をフィルタリングするためのフィールドを参照してください。

   b. フィールドに適切なタイプの値を入力します。さまざまなタイプの値の詳細については、フィールドの値を指定するを参照してください。

テキスト (文字列) の配列

このタイプの値では、Macie は多くの場合、選択する値のリストを提供します。この場合、条件で使用するそれぞれの値を選択します。

Macie が値のリストを提供しない場合は、フィールドに完全で有効な値を入力します。フィールドに追加の値を指定するには、適用を選択し、次に追加の値ごとに別の条件を追加します。

値では、大文字と小文字が区別されることに注意してください。また、値には部分的な値やワイルドカード文字を使用することはできません。たとえば、my-S3-bucket という名前の S3 バケットの調査結果をフィルタリングするには、S3 バケット名フィールドの値として **my-S3-bucket** と入力します。**my-s3-bucket** や **my-S3** などの他の値を入力した場合、Macie はバケットの調査結果を返しません。

ブール値

このタイプの値について、Macie は選択する値のリストを提供します。条件で使用する値を選択します。

日付/時刻 (時間範囲

このタイプの値には、From および To ボックスを使用して、包括的な時間範囲を定義します。

- 固定時間範囲を定義するには、From および To ボックスを使用して、範囲内の最初の日時と最後の日時をそれぞれ指定します。
- 特定の日時に開始し、現在の時刻で終了する相対時間範囲を定義するには、開始日時を From ボックスに入力し、To ボックス内のテキストを削除します。
- 特定の日時に終了する相対時間範囲を定義するには、終了日時を To ボックスに入力し、From ボックス内のテキストを削除します。

時間値は 24 時間表記を使用することに注意してください。日付ピッカーを使用して日付を選択する場合は、テキストをFrom および To ボックスに直接入力して、値を絞り込むことができます。

数値 (数値範囲

このタイプの値では、From および To ボックスを使用して、包括的、固定、または相対の数値範囲を定義する 1 つ以上の整数を入力します。

テキスト (文字列) 値

このタイプの値では、フィールドに完全で有効な値を入力します。

値では、大文字と小文字が区別されることに注意してください。また、値には部分的な値やワイルドカード文字を使用することはできません。たとえば、my-S3-bucket という名前の S3 バケットの調査結果をフィルタリングするには、S3 バケット名フィールドの値として **my-S3-bucket** と入力します。**my-s3-bucket** や **my-S3** などの他の値を入力した場合、Macie はバケットの調査結果を返しません。

c. フィールドの値の追加が終了したら、適用を選択します。Macie はフィルター基準を適用し、フィルター条件ボックスのフィルタートークンに条件を追加します。

6. 追加する追加の条件ごとに、ステップ 5 を繰り返します。
7. 条件を削除するには、条件のフィルタートークンで条件の削除アイコン

   を選択します。
8. 条件を変更するには、条件のフィルタートークンで条件の削除アイコン

   を選択して、条件を削除します。次に、ステップ 5 を繰り返して、正しい設定を持つ条件を追加します。

後でこの条件のセットを再度使用する場合は、セットをフィルタールールとして保存できます。これを行うには、フィルター条件ボックスのルールを保存するを選択します。次に、ルールの名前を入力し、オプションで説明を入力します。終了したら、保存を選択します。

Amazon Macie API を用いて調査結果をプログラムでフィルタリングする

調査結果をプログラムでフィルタリングするには、Amazon Macie APIの ListFindings または GetFindingStatistics オペレーションを使用して送信するクエリでフィルター基準を指定します。ListFindings オペレーションは、フィルター基準を満たす結果ごとの 1 つの ID である、検索条件 ID の配列を返します。GetFindingStatistics オペレーションは、リクエストで指定したフィールド別にグループ化された、フィルター基準を満たすすべての調査結果に関する集計統計データを返します。

以下の点に注意してください。ListFindings および GetFindingStatistics オペレーションは、結果を抑制するために使用するオペレーションとは異なることに注意してください フィルター基準も指定する抑制オペレーションとは異なり、ListFindings および GetFindingStatistics オペレーションは、

調査結果データのみをクエリします。それらは、フィルター基準と一致する検出結果に対するアクションは実行しません。検出結果を非表示にするには、Amazon Macie APIの CreateFindingsFilter オペレーションを使用します。

クエリでフィルター基準を指定するには、リクエストにフィルター基準のマップを含めます。条件ごとに、フィールド、演算子、およびフィールドの 1 つ以上の値を指定します。値のタイプと数は、選択するフィールドと演算子によって異なります。条件で使用できるフィールド、演算子、および値のタイプについては、調査結果をフィルタリングするためのフィールド、条件での演算子の使用、およびフィールドの値を指定するを参照してください。

次の例は、AWS Command Line InterfaceAWS CLI を使用して送信するクエリでフィルター基準を指定する方法を示しています。現在のバージョンの別の AWS コマンドラインツールまたは AWS SDKを使用するか、HTTPS リクエストを Macie に直接送信してこれを行うこともできます。AWS のツールと SDK に関する詳細については、AWS での構築ツールを参照してください。

例

- 例 1: 重要度に基づいて調査結果をフィルタリングする
- 例 2: 機密データのカテゴリに基づいて調査結果をフィルタリングする
- 例 3: 固定時間範囲に基づいて結果をフィルタリングする
- 例 4: 抑制ステータスに基づいて調査結果をフィルタリングする
- 例 5: 複数のフィールドと値のタイプに基づいて調査結果をフィルタリングする

この例では list-findings コマンドを使用します。例が正常に実行されると、Macie は `findingIds` 配列を返します。配列には、次の例に示すように、フィルター基準を満たす各調査結果の一意の識別子がリスト化されます。

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

フィルター基準を満たす調査結果がない場合、Macie は空の `findingIds` 配列を返します。

```
{
    "findingIds": []
}
```

例 1: 重要度に基づいて調査結果をフィルタリングする

この例では list-findings コマンドを使用して、現在の AWS リージョン 内の高い重要度および中程度の重要度のすべての調査結果の調査結果 ID を取得します。

Linux、macOS、Unix の場合:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

Microsoft Windows の場合:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":
{\"severity.description\":{\"eq\":[\"High\",\"Medium\"]}}}
```

ここで、

- *severity.description* は 重要度フィールドの JSON 名を指定します。
- *eq*は、等しい 演算子を指定します。
- *#*および *#* は、重要度フィールドの列挙値の配列です。

例 2: 機密データのカテゴリに基づいて調査結果をフィルタリングする

この例では list-findings コマンドを使用して、現在のリージョン内にある機密データの調査結果の調査結果 ID を取得し、S3 オブジェクト内の財務情報 (他のカテゴリの機密データは含まない) の出現をレポートします。

Linux、macOS、または Unix の場合、読みやすさを向上させるためにバックスラッシュ (\) の行連結文字を使用します。

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

Microsoft Windows の場合、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"FINANCIAL_INFORMATION\"]}}}
```

ここで、

- *classificationDetails.result.sensitiveData.category* は、機密データのカテゴリフィールドの JSON 名を指定します。
- *eqexactMatch* は、完全一致と等しい演算子を指定します。
- *FINANCIAL_INFORMATION* は、機密データのカテゴリフィールドの列挙値です。

例 3: 固定時間範囲に基づいて結果をフィルタリングする

この例では list-findings コマンドを使用して、現在のリージョン内にあり、07:00 UTC October 5, 2020 から 07:00 UTC November 5, 2020 の間に作成されたすべての調査結果の調査結果 ID を取得します (包括的)。

Linux、macOS、Unix の場合:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":
{"gte":1601881200000,"lte":1604559600000}}}'
```

Microsoft Windows の場合:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"createdAt\":
{\"gte\":1601881200000,\"lte\":1604559600000}}}
```

ここで、

- *createdAt*は、Created at (作成日時) フィールドの JSON 名を指定します。
- *gte*は、greater than or equal to (~ 以上) 演算子を指定します。
- *1601881200000* は、時間範囲内の最初の日付と時刻です (ミリ秒単位での Unix のタイムスタンプとして)。
- *lte* は、 ~ 以下演算子を指定します。

- *1604559600000* は、時間範囲内の最後の日付と時刻です (ミリ秒単位での Unix のタイムスタンプとして)。

例 4: 抑制ステータスに基づいて調査結果をフィルタリングする

この例では list-findings コマンドを使用して、現在のリージョン内にあり、抑制ルールによって抑制された (自動的にアーカイブされた) すべての調査結果の調査結果 ID を取得します)。

Linux、macOS、Unix の場合:

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":
["true"]}}}'
```

Microsoft Windows の場合:

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"archived\":{\"eq\":
[\"true\"]}}}
```

ここで、

- *#######* は、アーカイブ済みフィールドの JSON 名を指定します。
- *eq*は、と等しい 演算子を指定します。
- *true*は、アーカイブ済みフィールドのブール値です。

例 5: 複数のフィールドと値のタイプに基づいて調査結果をフィルタリングする

この例では list-findings コマンドを使用して、現在のリージョン内にあり、以下の基準に一致するすべての調査結果の調査結果 ID を取得します: 07:00 UTC October 5, 2020 から 07:00 UTC November 5, 2020 の間に作成された (排他的); S3 オブジェクト内の財務データ (他のカテゴリの機密データは含まない) の出現をレポートする; 抑制ルールによって抑制 (自動的にアーカイブ) されていない。

Linux、macOS、または Unix の場合、読みやすさを向上させるためにバックスラッシュ (\) の行連結文字を使用します。

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":1601881200000,"lt":1604559600000},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

Microsoft Windows の場合、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

ここで、

- *createdAt*は、作成日時フィールドの JSON 名を指定し、
  - *gt*は、 ~ 以上演算子を指定します。
  - *1601881200000* は、時間範囲内の最初の日付と時刻です (ミリ秒単位での Unix のタイムスタンプとして)。
  - *lt* は、 ~ 以下演算子を指定します。
  - *1604559600000* は、時間範囲内の最後の日付と時刻です (ミリ秒単位での Unix のタイムスタンプとして)。
- *classificationDetails.result.sensitiveData.category* は、Sensitive data category (機密データのカテゴリ) フィールドの JSON 名を指定し、
  - *eqexactMatch* は、完全一致と等しい演算子を指定します。
  - *FINANCIAL_INFORMATION* は、フィールドの列挙値です。
- archived は、*#######*フィールドの JSON 名を指定し、
  - *eq*は、等しい 演算子を指定します。
  - *false* は、フィールドのブール値です。

調査結果のフィルタールールの作成と管理

フィルタールールは、Amazon Macie コンソールで調査結果を表示するときに再度使用するために作成および保存するフィルター基準のセットです。フィルタールールは、特定の特性を持つ調査結果の一貫した分析を実行するのに役立ちます。たとえば、暗号化されていないオブジェクトを含む S3 バケットの高い重要度のポリシーの調査結果をすべて分析するための 1 つのフィルタールールと、特定の種類の機密データをレポートする高い重要度の機密データの調査結果をすべて分析するためのもう 1 つのフィルタールールを作成できます。

フィルタールールは、抑制ルールとは異なることに注意してください。抑制ルールは、ルールの基準を満たす調査結果を自動的にアーカイブするために作成および保存するフィルター基準のセット

です。どちらのタイプのルールもフィルター基準を保存および適用しますが、フィルタールールは、ルールの基準と一致する調査結果に対してアクションを実行しません。代わりに、フィルタールールは、ルールを適用した後にコンソールに表示される調査結果の決定のみを行います。抑制ルールの詳細については、調査結果を抑制するを参照してください。

フィルタールールを作成および管理するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。次のトピックでは、その方法を説明します。API について、トピックでは、AWS Command Line InterfaceAWS CLI を用いてこれらのタスクを実行する方法を説明します。HTTPS リクエストを Macie に直接送信するか、現在のバージョンの別の AWS コマンドラインツールまたは AWS SDKを使用してこれらのタスクを実行することもできます。AWS のツールと SDK に関する詳細については、AWS での構築ツールを参照してください。

トピック

- フィルタールールの作成
- フィルタールールの適用
- フィルタールールの変更
- フィルタールールの削除

フィルタールールの作成

フィルタールールを作成するときは、フィルター基準、名前、および必要に応じてルールの説明を指定します。フィルタールールは、Amazon Macie コンソールまたは Amazon Macie API を使用して作成できます。

Console

Amazon Macie コンソールを使用してフィルタールールを作成するには、次のステップに従います。

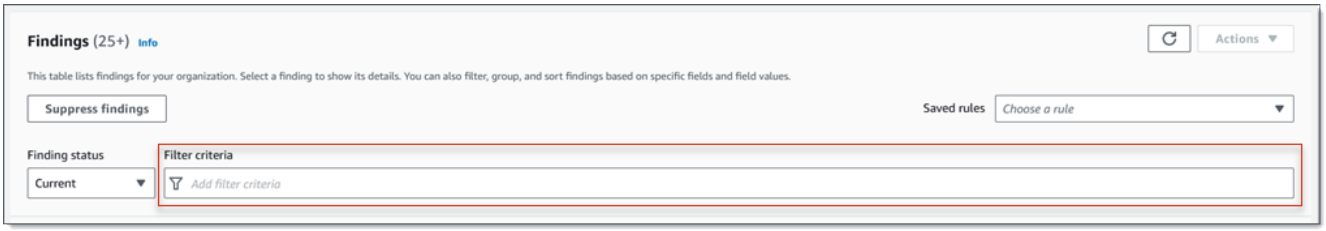
フィルタールールを作成するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果 を選択します。

> **Tip**
>
> 既存のフィルタールールを開始点として使用するには、保存されたルールのリストからルールを選択します。

また、事前定義された論理グループによる調査結果を最初にピボットしてドリルダウンすることで、ルールの作成を合理化することもできます。これを行うと、Macie は適切なフィルター条件を自動的に作成して適用します。これは、ルールを作成するために役立つ開始点となる場合があります。これを行うには、ナビゲーションペイン (調査結果の下の バケット別、タイプ別、または ジョブ別を選択し、次にテーブル内で項目を選択します。詳細パネルで、ピボットするフィールドのリンクを選択します。

3. フィルター条件ボックスで、ルールのフィルター基準を定義する条件を追加します。



フィルター条件を追加する方法については、フィルターの作成と調査結果への適用を参照してください。

4. ルールのフィルター基準の定義が終了したら、フィルターバーのルールを保存するを選択します。

5. フィルタールールの下で、ルールの名前を入力し、必要に応じて説明を入力します。
6. 保存 を選択します。

API

プログラムでフィルタールールを作成するには、Amazon Macie API の CreateFindingsFilter オペレーションを使用して、必要なパラメータに適切な値を指定します。

- `action` パラメータでは、`NOOP` を指定して、Macie がルールの基準と一致する調査結果を抑制 (自動的にアーカイブ) しないようにします。
- `criterion` パラメータでは、ルールのフィルター基準を定義する条件のマップを指定します。

マップでは、条件ごとに、フィールド、演算子、およびフィールドの 1 つ以上の値を指定する必要があります。値のタイプと数は、選択するフィールドと演算子によって異なります。条件で使用できるフィールド、演算子、および値のタイプについては、調査結果をフィルタリングするためのフィールド、条件での演算子の使用、およびフィールドの値を指定するを参照してください。

AWS CLI を使用してフィルタールールを作成するには、create-findings-filter コマンドを実行し、必要なパラメータに適切な値を指定します。次の例では、現在の AWS リージョン 内にあり、S3 オブジェクト内の個人情報 (他のカテゴリの機密データは含まない) の出現をレポートするすべての機密データの調査結果を返すフィルタールールを作成します。

この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws macie2 create-findings-filter \
--action NOOP \
--name my_filter_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行継続文字を使用しています。

```
C:\> aws macie2 create-findings-filter ^
--action NOOP ^
--name my_filter_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"PERSONAL_INFORMATION\"]}}}
```

ここで、

- *my_filter_rule* は、ルールのカスタム名です。
- criterion は、ルールのフィルター条件のマップです。
  - *classificationDetails.result.sensitiveData.category* は、機密データのカテゴリフィールドの JSON 名です。
  - *eqexactMatch* は、完全一致と等しい演算子を指定します。

- *PERSONAL_INFORMATION* は、機密データのカテゴリフィールドの列挙値です。

コマンドが正常に実行された場合は、以下のような出力が表示されます。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

ここで、arn は、作成されたフィルタールールの Amazon リソースネーム (ARN)で、id は、ルールの一意の識別子です。

フィルター基準のその他の例については、Amazon Macie API を用いて調査結果をプログラムでフィルタリングするを参照してください。

フィルタールールの適用

フィルタールールを適用すると、Amazon Macie はルールの基準を使用して、コンソール上の調査結果の表示に含めるか除外する調査結果を決定します。Macie は条件も表示するため、どの条件を適用したかを判断しやすくなります。

フィルタールールは Amazon Macie コンソールで使用するために設計されていることに注意してください。Amazon Macie API を使用してプログラムで送信するクエリでそれらを直接使用することはできません。ただし、API を使用して調査結果をクエリする場合は、GetFindingsFilter オペレーションを使用してルールのフィルター基準を取得します。その後、その条件をクエリに追加できます。クエリでフィルター基準を指定する方法については、フィルターの作成と調査結果への適用を参照してください。

フィルタールールを適用して、コンソールで調査結果をフィルタリングするには、次のステップに従います。

フィルタールールを適用するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 結果 を選択します。
3. Saved rules (保存されたルール) のリストで、適用するフィルタールールを選択します。Macie は、ルールの基準を適用し、フィルター条件ボックスに基準を表示します。

4. (オプション) 基準を絞り込むには、フィルター条件を使用してフィルター条件を追加または削除します。これを行っても、変更はルールの設定に影響しません。Macie は、明示的に新しいルールとして保存しない限り、変更を保存しません。
5. 別のフィルタールールを適用するには、ステップ 3 を繰り返します。

フィルタールールを適用した後、フィルター条件ボックスの X を選択して、フィルター基準のすべてをビューからすみやかに削除することができます。

フィルタールールの変更

フィルタールールの設定は、Amazon Macie コンソールまたは Amazon Macie API を使用していつでも変更できます。ルールにタグを割り当てて管理することもできます。

タグは、ユーザーが定義して特定のタイプの AWS リソースに割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを分類および管理できます。詳細については、Amazon Macie リソースへのタグ付けを参照してください。

Console

Amazon Macie コンソールを使用して既存のフィルタールールの設定を変更するには、次のステップに従います。

フィルタールールを変更するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 結果 を選択します。
3. 保存されたルールのリストで、変更するフィルタールールの隣にある編集アイコン
   を
   選択します。
4. 次のいずれかを実行します。
   - ルールのフィルター基準を変更するには、フィルター条件ボックスを使用して、目的の基準の条件を入力します。この方法の詳細は、フィルターの作成と調査結果への適用を参照してください。
   - ルールの名前を変更するには、新しい名前を フィルタールールの下の 名前ボックスに入力します。

- ルールの説明を変更するには、新しい説明を フィルタールールの下の 説明ボックスに入力します。
- ルールのタグを割り当て、確認、または編集するには、フィルタールールの タグの管理を選択します。必要に応じてタグを確認および変更します。ルールには、最大 50 個のタグを含めることができます。

5. 変更が完了したら、保存 を選択します。

API

フィルタールールをプログラムで変更するには、Amazon Macie API の UpdateFindingsFilter オペレーションを使用します。リクエストを送信するときは、サポートされているパラメータを使用して、変更する設定ごとに新しい値を指定します。

id パラメータでは、変更するルールの一意の識別子を指定します。ListFindingsFilter オペレーションを使用して、アカウントのフィルタールールと抑制ルールのリストを取得することで、この識別子が得られます。AWS CLI を使用している場合は、list-findings-filters コマンドを実行してこのリストを取得してください。

AWS CLI を使用してフィルタールールを変更するには、update-findings-filter コマンドを実行し、サポートされているパラメータを使用して、変更する設定ごとに新しい値を指定します。たとえば、次のコマンドでは、既存のフィルタールールの名前を変更します。

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --
name personal_information_only
```

ここで、

- *9b2b4508-aa2f-4940-b347-d1451example* は、ルールの一意の識別子です。
- *personal_information_only* は、ルールの新しい名前です。

コマンドが正常に実行された場合は、以下のような出力が表示されます。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

ここで、arn は、変更されたルールの Amazon リソースネーム (ARN)で、id は、ルールの一意の識別子です

同様に、次の例では、action パラメータの値を ARCHIVE から NOOP に変更することで、抑制ルールをフィルタールールに変換します。

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action NOOP
```

ここで、

- *8a1c3508-aa2f-4940-b347-d1451example* は、ルールの一意の識別子です。
- *NOOP* は、ルールの基準と一致する調査結果に対して Macie が実行する新しいアクションです (アクションは実行しません (調査結果を抑制しません))。

コマンドが正常に実行された場合は、次のような出力が表示されます。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

ここで、arn は、変更されたルールの Amazon リソースネーム (ARN)で、id は、ルールの一意の識別子です

フィルタールールの削除

フィルタールールは、Amazon Macie コンソールまたは Amazon Macie API を使用していつでも削除できます。

Console

Amazon Macie コンソールを使用してフィルタールールを削除するには、次のステップに従います。

フィルタールールを削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。

2. ナビゲーションペインで 結果 を選択します。
3. 保存されたルールのリストで、削除するフィルタールールの隣にある編集アイコン
   を
   選択します。
4. フィルタールール の下で、削除を選択します。

API

フィルタールールをプログラムで削除するには、Amazon Macie API の DeleteFindingsFilter オペレーションを使用します。id パラメータでは、削除するフィルタールールの一意の識別子を指定します。list-findings-filters コマンドを実行して、アカウントの抑制ルールとフィルタールールのリストを取得することで、この識別子が得られます。AWS CLI を使用している場合は、list-findings-filters コマンドを実行してこのリストを取得してください。

AWS CLI を使用してフィルタールールを削除するには、delete-findings-filter コマンドを実行します。例:

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

9b2b4508-aa2f-4940-b347-d1451example は、ルールの一意の識別子です。

コマンドが正常に実行されると、Macie は空の HTTP 200 レスポンスを返します。それ以外の場合、Macie は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

調査結果をフィルタリングするためのフィールド

調査結果をより効率的に分析できるようにするために、Amazon Macie コンソールと Amazon Macie API では、結果をフィルタリングするためのいくつかのフィールドセットにアクセスできます。

- 一般的なフィールド -これらのフィールドには、あらゆるタイプの調査結果に適用されるデータが保存されます。これらのフィールドは、重要度、調査結果タイプ、調査結果 IDなど、調査結果の一般的な属性に関連しています。
- 影響を受けたリソースフィールド — これらのフィールドには、影響を受けた S3 バケットまたはオブジェクトの名前、パブリックアクセス設定、暗号化設定など、調査結果が適用されるリソースに関するデータが保存されます。

- ポリシーフィールド — これらのフィールドには、調査結果を生成したアクション、アクションを実行したエンティティなど、ポリシーの調査結果に固有のデータが保存されます。
- 機密データ分類フィールド — これらのフィールドには、Macie が影響を受ける S3 オブジェクトで見つけた機密データのカテゴリやタイプなど、機密データの検出結果固有のデータが格納されます。

フィルターは、上記のいずれかのセットのフィールドの組み合わせを使用できます。

このセクションのトピックでは、調査結果をフィルタリングするために使用できる個別のフィールドをリスト化し、説明します。フィールド間の関係など、これらのフィールドの詳細については、Amazon Macie API リファレンスの調査結果を参照してください。

トピック

一般的なフィールド

次のテーブルでは、一般的な調査結果の属性に基づいて調査結果をフィルタリングするために使用できるフィールドのリストと説明を示します。これらのフィールドには、あらゆるタイプの調査結果に適用されるデータが保存されます。

テーブルでは、フィールド 列は Amazon Macie コンソールのフィールドの名前を示します。JSON フィールド 列はドット表記を使用して、調査結果と Amazon Macie API の JSON 表現でフィールドの名前を示します。説明列はフィールドに保存されるデータの簡単な説明と、フィルター値の要件を示します。テーブルは、フィールドごとにアルファベット順に昇順で並べ替えられ、次に JSON フィールド別に並べ替えられます。

フィールド	JSON フィールド	説明
アカウント ID*	`accountId`	調査結果が適用される AWS アカウント アカウントの一意の識別子。これは通常、影響

フィールド	JSON フィールド	説明
		を受けたリソースを所有するアカウントです。
—	`archived`	調査結果が抑制ルールによって抑制された (自動的にアーカイブされた) かどうかを指定するブール値。 このフィールドをコンソールのフィルタに使用するには、検索ステータス メニューのオプションとして アーカイブ済み 抑制済みのみ、現在抑制解除のみ、または すべて抑制済みと抑制解除の両方を選択します。
カテゴリ	`category`	検出結果のカテゴリ。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API では、有効な値は次のとおりです: 機密データの調査結果では、`CLASSIFICATION` 、および、ポリシーの調査結果では、`POLICY`。

フィールド	JSON フィールド	説明
—	`count`	調査結果の合計出現数。機密データの調査結果では、この値は常に 1 です。機密データの検出結果はすべて一意とみなされます。 このフィールドは、コンソールではフィルターオプションとして使用できません。API を使用すると、このフィールドを使用してフィルターの数値範囲を定義できます。
作成日時	`createdAt`	Macie が調査結果を作成した日時。 このフィールドを使用して、フィルターの時間範囲を定義できます。
調査結果 ID*	`id`	フィルターの一意の識別子。これは、調査結果を作成したときに、Macie が生成して調査結果に割り当てるランダムな文字列です。

フィールド	JSON フィールド	説明
調査結果タイプ*	`type`	調査結果のタイプ。たとえば、`SensitiveData:S3Object/Personal` または `Policy:IAMUser/S3BucketPublic` 。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API の有効な値のリストについては、「Amazon Macie API リファレンスFindingType」の「」を参照してください。
リージョン	`region`	Macie が調査結果を作成した AWS リージョン。たとえば、`us-east-1` または `ca-central-1` 。
サンプル	`sample`	調査結果が検出結果のサンプルかどうかを指定するブール値。sample finding (検出結果のサンプル) は、何が調査結果に含まれる可能があるかを示すために、データ例とプレースホルダー値を使用する調査結果です。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。

フィールド	JSON フィールド	説明
緊急度	`severity.description`	調査結果の重要度の定性的表現。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API では、有効な値は `Low`、`Medium`、および `High` です。
更新時刻	`updatedAt`	調査結果が最終更新された日時。機密データの調査結果では、この値は 作成日時 フィールドの値と同じです。機密データの検出結果は、新規 (一意) とみなされます。 このフィールドを使用して、フィルターの時間範囲を定義できます。

* コンソールでこのフィールドに複数の値を指定するには、フィールドを使用してフィルターに個別の値を指定する条件を追加し、次に追加の値ごとにそのステップを繰り返します。API でこれを行うには、フィルターに使用する値をリスト化する配列を使用します。

影響を受けたリソースフィールド

次のトピックでは、調査結果が適用されるリソースに基づいて結果をフィルタリングするために使用できるフィールドのリストと説明を示します。トピックは、リソースタイプごとに整理されます。

トピック

- S3 バケット
- S3 オブジェクト

S3 バケット

次のテーブルでは、調査結果が適用される S3 バケットの特性に基づいて結果をフィルタリングするために使用できるフィールドのリストと説明を示します。

テーブルでは、フィールド 列は Amazon Macie コンソールのフィールドの名前を示します。JSON フィールド 列はドット表記を使用して、調査結果と Amazon Macie API の JSON 表現でフィールドの名前を示します。(長い JSON フィールド名は、読みやすさを向上させるために改行文字シーケンス (\n) を使用します。) 説明列はフィールドに保存されるデータの簡単な説明と、フィルター値の要件を示します。テーブルは、フィールドごとにアルファベット順に昇順で並べ替えられ、次に JSON フィールド別に並べ替えられます。

フィールド	JSON フィールド	説明
—	`resourcesAffected.s3Bucket.createdAt`	影響を受けるバケットが作成された日時、またはバケットのポリシーの編集などの変更が影響を受けたバケットに最近加えられた日付と時刻。 このフィールドは、コンソールではフィルターオプションとして使用できません。API では、このフィールドを使用してフィルターの時間範囲を定義できます。
S3 バケットのデフォルトの暗号化	`resourcesAffected.s3Bucket.defaultServerSideEncryption.encryptionType`	影響を受けたバケットに追加されるオブジェクトを暗号化するためにデフォルトで使用されるサーバー側の暗号化アルゴリズム。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API の

フィールド	JSON フィールド	説明
		有効な値のリストについては、「Amazon Macie API リファレンスEncryptionType」の「」を参照してください。
S3 バケット暗号化 KMS キー ID*	`resourcesAffected.s3Bucket.defaultServerSideEncryption.kmsMasterKeyId`	Amazon リソースネーム (ARN) または影響を受けたバケットに追加されたオブジェクトを暗号化するためにデフォルトで使用される AWS KMS key の一意の識別子 (キー ID)。
バケットポリシーで必要な S3 バケットの暗号化	`resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads`	オブジェクトがバケットに追加されるときに、影響を受けたバケットのバケットポリシーで、オブジェクトのサーバー側の暗号化が必要かどうかを指定します。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API の有効な値のリストについては、Amazon Macie API リファレンスのS3Bucketを参照してください。
S3 バケット名*	`resourcesAffected.s3Bucket.name`	影響を受けたバケットの完全な名前。

フィールド	JSON フィールド	説明
S3 バケット所有者の表示名*	`resourcesAffected.s3Bucket.owner.displayName`	影響を受けたバケットを所有する AWS ユーザーの表示名。
S3 バケットのパブリックアクセス許可	`resourcesAffected.s3Bucket.publicAccess.effectivePermission`	バケットに適用されるアクセス許可設定の組み合わせに基づいて、影響を受けたバケットがパブリックにアクセス可能かどうかを指定します。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API の有効な値のリストについては、「Amazon Macie API リファレンスBucketPublicAccess」の「」を参照してください。

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicAcls`
		影響を受けたバケットとバケット内のオブジェクトのパブリックアクセスコントロールリスト (ACL) が、Amazon S3 によってブロックされるかどうかを指定するブール値。これは、バケットのアカウントレベルのブロックパブリックアクセス設定です。
		
		このフィールドは、コンソールではフィルターオプションとして使用できません。

フィールド	JSON フィールド	説明
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.blockPublicPolicy	影響を受けたバケットのパブリックバケットポリシーを Amazon S3 がブロックするかどうかを指定するブール値。これは、バケットのアカウントレベルのブロックパブリックアクセス設定です。 このフィールドは、コンソールではフィルターオプションとして使用できません。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.ignorePublicAcls	影響を受けたバケットおよびバケット内のオブジェクトのパブリック ACL を Amazon S3 が無視するかどうかを指定するブール値。これは、バケットのアカウントレベルのブロックパブリックアクセス設定です。 このフィールドは、コンソールではフィルターオプションとして使用できません。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.restrictPublicBuckets	影響を受けたバケットのパブリックバケットポリシーを Amazon S3 が制限するかどうかを指定するブール値。これは、バケットのアカウントレベルのブロックパブリックアクセス設定です。 このフィールドは、コンソールではフィルターオプションとして使用できません。

フィールド	JSON フィールド	説明
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicReadAccess`	影響を受けたバケットのバケットレベルの ACL が、一般ユーザーにバケットの読み取りアクセス許可を付与するかどうかを指定するブール値。 このフィールドは、コンソールではフィルターオプションとして使用できません。
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicWriteAccess`	影響を受けたバケットのバケットレベルの ACL が、一般ユーザーにバケットの書き込みアクセス許可を付与するかどうかを指定するブール値。 このフィールドは、コンソールではフィルターオプションとして使用できません。
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicAcls`	影響を受けたバケットおよびバケット内のオブジェクトのパブリック ACL を Amazon S3 がブロックするかどうかを指定するブール値。これは、バケットのバケットレベルのブロックパブリックアクセス設定です。 このフィールドは、コンソールではフィルターオプションとして使用できません。

フィールド	JSON フィールド	説明
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.blockPublicPolicy	影響を受けたバケットのパブリックバケットポリシーを Amazon S3 がブロックするかどうかを指定するブール値。これは、バケットのバケットレベルのブロックパブリックアクセス設定です。 このフィールドは、コンソールではフィルターオプションとして使用できません。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.ignorePublicAcls	影響を受けたバケットおよびバケット内のオブジェクトのパブリック ACL を Amazon S3 が無視するかどうかを指定するブール値。これは、バケットのバケットレベルのブロックパブリックアクセス設定です。 このフィールドは、コンソールではフィルターオプションとして使用できません。
—	resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets	影響を受けたバケットのパブリックバケットポリシーを Amazon S3 が制限するかどうかを指定するブール値。これは、バケットのバケットレベルのブロックパブリックアクセス設定です。 このフィールドは、コンソールではフィルターオプションとして使用できません。

フィールド	JSON フィールド	説明
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess`	影響を受けたバケットのポリシーが、一般ユーザーがバケットへの読み取りアクセス権を持つことを許可するかどうかを指定するブール値。 このフィールドは、コンソールではフィルターオプションとして使用できません。
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess`	影響を受けたバケットのポリシーが、一般ユーザーがバケットへの書き込みアクセス権を持つことを許可するかどうかを指定するブール値。 このフィールドは、コンソールではフィルターオプションとして使用できません。
S3 バケットタグキー*	`resourcesAffected.s3Bucket.tags.key`	影響を受けたバケットに関連付けられたタグキー。
S3 バケットタグ値*	`resourcesAffected.s3Bucket.tags.value`	影響を受けたバケットに関連付けられたタグ値。

* コンソールでこのフィールドに複数の値を指定するには、フィールドを使用してフィルターに個別の値を指定する条件を追加し、次に追加の値ごとにそのステップを繰り返します。API でこれを行うには、フィルターに使用する値をリスト化する配列を使用します。

S3 オブジェクト

次のテーブルでは、調査結果が適用される S3 オブジェクトの特性に基づいて結果をフィルタリングするために使用できるフィールドのリストと説明を示します。

テーブルでは、フィールド 列は Amazon Macie コンソールのフィールドの名前を示します。JSON フィールド 列はドット表記を使用して、調査結果と Amazon Macie API の JSON 表現でフィールドの名前を示します。説明列はフィールドに保存されるデータの簡単な説明と、フィルター値の要件を示します。テーブルは、フィールドごとにアルファベット順に昇順で並べ替えられ、次に JSON フィールド別に並べ替えられます。

フィールド	JSON フィールド	説明
S3 オブジェクトの暗号化 KMS キー ID*	`resourcesAffected.s3Object.serverSideEncryption.kmsMasterKeyId`	Amazon リソースネーム (ARN) または影響を受けたオブジェクトを暗号化するために使用された AWS KMS key の一意の識別子 (キー ID) です。
S3 オブジェクトの暗号化タイプ	`resourcesAffected.s3Object.serverSideEncryption.encryptionType`	影響を受けたオブジェクトの暗号化に使用されたサーバー側の暗号化アルゴリズム。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API の有効な値のリストについては、「Amazon Macie API リファレンスEncryptionType」の「」を参照してください。
—	`resourcesAffected.s3Object.extension`	影響を受けたオブジェクトのファイル名拡張子。ファイル名拡張子のないオブジェクトでは、フィルターの値として "" を指定します。

フィールド	JSON フィールド	説明
		このフィールドは、コンソールではフィルターオプションとして使用できません。
—	`resourcesAffected.s3Object.lastModified`	影響を受けたオブジェクトが作成された日時、または最後に変更された日時 (いずれか最新の日時)。 このフィールドは、コンソールではフィルターオプションとして使用できません。API では、このフィールドを使用してフィルターの時間範囲を定義できます。
S3 オブジェクトキー*	`resourcesAffected.s3Object.key`	影響を受けるオブジェクトのフルネーム (キー)。該当する場合は、オブジェクトのプレフィックスを含みます。
—	`resourcesAffected.s3Object.path`	影響を受けるバケットの名前とオブジェクトの名前 (キー) を含む、影響を受けるオブジェクトへのフルパス。 このフィールドは、コンソールではフィルターオプションとして使用できません。

フィールド	JSON フィールド	説明
S3 オブジェクトのパブリックアクセス	`resourcesAffected.s3Object.publicAccess`	オブジェクトに適用されるアクセス許可設定の組み合わせに基づいて、影響を受けたオブジェクトがパブリックにアクセス可能かどうかを指定するブール値。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。
S3 オブジェクトタグキー*	`resourcesAffected.s3Object.tags.key`	影響を受けたオブジェクトに関連付けられたタグキー。
S3 オブジェクトタグ値*	`resourcesAffected.s3Object.tags.value`	影響を受けたオブジェクトに関連付けらたタグ値。

* コンソールでこのフィールドに複数の値を指定するには、フィールドを使用してフィルターに個別の値を指定する条件を追加し、次に追加の値ごとにそのステップを繰り返します。API でこれを行うには、フィルターに使用する値をリスト化する配列を使用します。

ポリシーフィールド

次のテーブルでは、ポリシーの調査結果をフィルタリングするために使用できるフィールドのリストと説明を示します。これらのフィールドは、ポリシーの調査結果に固有のデータを保存します。

テーブルでは、フィールド 列は Amazon Macie コンソールのフィールドの名前を示します。JSON フィールド 列はドット表記を使用して、調査結果と Amazon Macie API の JSON 表現でフィールドの名前を示します。(長い JSON フィールド名は、読みやすさを向上させるために改行文字シーケンス (\n) を使用します。) 説明列はフィールドに保存されるデータの簡単な説明と、フィルター値の要件を示します。テーブルは、フィールドごとにアルファベット順に昇順で並べ替えられ、次に JSON フィールド別に並べ替えられます。

フィールド	JSON フィールド	説明
アクションタイプ	policyDetails.action.actionType	結果を生成したアクションのタイプ。このフィールドで唯一の有効な値は AWS_API_CALL です。
API コール名*	policyDetails.action.apiCallDetails.api	最後に呼び出され、調査結果を生成したオペレーションの名前。たとえば、PutBucketPublicAccessBlock 。
API サービス名*	policyDetails.action.apiCallDetails.apiServiceName	呼び出され、調査結果を生成したオペレーションを提供する AWS のサービス の URL。たとえば、s3.amazonaws.com 。
—	policyDetails.action.apiCallDetails.firstSeen	いずれかのオペレーションが呼び出され、調査結果を生成した最初の日付と時刻。 このフィールドは、コンソールではフィルターオプションとして使用できません。API では、このフィールドを使用してフィルターの時間範囲を定義できます。
—	policyDetails.action.apiCallDetails.lastSeen	指定されたオペレーション (API コール名 または api) が呼び出され、調査結果が生成された最新の日時。 このフィールドは、コンソールではフィルターオプションとして使用できません。API では、このフィールドを使用

フィールド	JSON フィールド	説明
		してフィルターの時間範囲を定義できます。
—	`policyDetails.actor.domainDetails.domainName`	アクションの実行に使用されたデバイスのドメイン名。 このフィールドは、コンソールではフィルターオプションとして使用できません。
IP 都市*	`policyDetails.actor.ipAddressDetails.ipCity.name`	アクションの実行に使用されたデバイスの IP アドレスの発信元の都市の名前。
IP 国*	`policyDetails.actor.ipAddressDetails.ipCountry.name`	アクションの実行に使用されたデバイスの IP アドレスの発信元の国の名前。たとえば、`United States`。
—	`policyDetails.actor.ipAddressDetails.ipOwner.asn`	アクションの実行に使用されたデバイスの IP アドレスを含む自律システムの自律システム番号 (ASN)。 このフィールドは、コンソールではフィルターオプションとして使用できません。
IP 所有者 ASN 組織*	`policyDetails.actor.ipAddressDetails.ipOwner.asnOrg`	アクションの実行に使用されたデバイスの IP アドレスを含む、自律システムの ASN に関連付けられた組織 ID。

フィールド	JSON フィールド	説明
IP 所有者 ISP*	`policyDetails.actor.ipAddressDetails.ipOwner.isp`	アクションの実行に使用されたデバイスの IP アドレスを所有していたインターネットサービスプロバイダー (ISP) の名前。
IP V4 アドレス*	`policyDetails.actor.ipAddressDetails.ipAddressV4`	アクションの実行に使用されたデバイスのインターネットプロトコルバージョン 4 (IPv4) のアドレス。
—	`policyDetails.actor.userIdentity.assumedRole.accessKeyId`	AWS STS APIの `AssumeRole` オペレーションを使用して取得された一時的なセキュリティ認証情報で実行したアクションでは、認証情報を識別する AWS アクセスキー ID。 このフィールドは、コンソールではフィルターオプションとして使用できません。
ユーザー ID が引き受けたロールアカウント ID*	`policyDetails.actor.userIdentity.assumedRole.accountId`	AWS STS APIの `AssumeRole` オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、認証情報を取得するために使用されたエンティティを所有する AWS アカウント の一意の識別子。

フィールド	JSON フィールド	説明
ユーザー ID が引き受けたロールプリンシパル ID*	`policyDetails.actor.userIdentity.assumedRole.principalId`	AWS STS APIの `AssumeRole` オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、認証情報を取得するために使用されたエンティティの一意の識別子。
ユーザー ID が引き受けたロールセッション ARN*	`policyDetails.actor.userIdentity.assumedRole.arn`	AWS STS APIの `AssumeRole` オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、認証情報を取得するために使用されたソースアカウント、IAM ユーザー、またはロールの Amazon リソースネーム (ARN)。

—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n`
	
	`sessionIssuer.type`
		AWS STS APIの `AssumeRole` オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、一時的セキュリティ認証情報のソース。たとえば、`Root`、`IAMUser`、または `Role`。
		
		このフィールドは、コンソールではフィルターオプションとして使用できません。

フィールド	JSON フィールド	説明
—	policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.userName	AWS STS APIの AssumeRole オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、セッションを発行したユーザーまたはロールの名前またはエイリアス エイリアスを持たないルートアカウントから認証情報が取得された場合、この値は null になることに注意してください。 このフィールドは、コンソールではフィルターオプションとして使用できません。
ユーザー ID AWS アカウントのアカウント ID*	policyDetails.actor.userIdentity.awsAccount.accountId	別の AWS アカウント の認証情報を使用して実行されたアクションでは、アカウントの一意の識別子。
ユーザー ID AWS アカウントのプリンシパル ID*	policyDetails.actor.userIdentity.awsAccount.principalId	別の AWS アカウント の認証情報を使用して実行されたアクションでは、アクションを実行したエンティティの一意の識別子。
呼び出されたユーザー ID AWS サービス	policyDetails.actor.userIdentity.awsService.invokedBy	AWS のサービス に属するアカウントによって実行されたアクションでは、サービスの名前。

フィールド	JSON フィールド	説明
—	`policyDetails.actor.userIdentity.federatedUser.accessKeyId`	AWS STS APIの `GetFederationToken` オペレーションを使用して取得された一時的なセキュリティ認証情報で実行したアクションでは、認証情報を識別する AWS アクセスキー ID。 このフィールドは、コンソールではフィルターオプションとして使用できません。
ユーザー ID フェデレーティッドセッション ARN*	`policyDetails.actor.userIdentity.federatedUser.arn`	AWS STS APIの `GetFederationToken` オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、認証情報を取得するために使用されたエンティティの ARN。
ユーザー ID フェデレーテッドユーザーアカウント ID*	`policyDetails.actor.userIdentity.federatedUser.accountId`	AWS STS APIの `GetFederationToken` オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、認証情報を取得するために使用されたエンティティを所有する AWS アカウント の一意の識別子。

フィールド	JSON フィールド	説明
ユーザー ID フェデレーティッドユーザープリンシパル ID*	`policyDetails.actor.userIdentity.federatedUser.principalId`	AWS STS APIの `GetFederationToken` オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、認証情報を取得するために使用されたエンティティの一意の識別子。
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n  sessionIssuer.type`	AWS STS APIの `GetFederationToken` オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、一時的セキュリティ認証情報のソース。たとえば、`Root`、`IAMUser`、または `Role`。 このフィールドは、コンソールではフィルターオプションとして使用できません。

フィールド	JSON フィールド	説明
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName`	AWS STS APIの GetFederationToken オペレーションを使用して取得された一時的セキュリティ認証情報で実行されたアクションでは、セッションを発行したユーザーまたはロールの名前またはエイリアス エイリアスを持たないルートアカウントから認証情報が取得された場合、この値は null になることに注意してください。 このフィールドは、コンソールではフィルターオプションとして使用できません。
ユーザー ID IAM アカウント ID*	`policyDetails.actor.userIdentity.iamUser.accountId`	IAM ユーザーの認証情報を使用して実行されたアクションでは、アクションを実行した IAM ユーザーに関連付けられた AWS アカウント の一意の識別子。
ユーザー ID IAM プリンシパル ID*	`policyDetails.actor.userIdentity.iamUser.principalId`	IAM ユーザーの認証情報を使用して実行されたアクションでは、アクションを実行した IAM ユーザーの一意の識別子。
ユーザー ID IAM ユーザー名*	`policyDetails.actor.userIdentity.iamUser.userName`	IAM ユーザーの認証情報を使用して実行されたアクションでは、アクションを実行した IAM ユーザーのユーザー名。

フィールド	JSON フィールド	説明
ユーザー ID ルートアカウント ID*	`policyDetails.actor.userIdentity.root.accountId`	ユーザーの AWS アカウントの認証情報を使用して実行されたアクションでは、アカウントの一意の識別子。
ユーザー ID ルートプリンシパル ID*	`policyDetails.actor.userIdentity.root.principalId`	ユーザーの AWS アカウントの認証情報を使用して実行されたアクションでは、アクションを実行したエンティティの一意の識別子。
ユーザー ID タイプ	`policyDetails.actor.userIdentity.type`	調査結果を生成したアクションを実行したエンティティのタイプ。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API の有効な値のリストについては、「Amazon Macie API リファレンスUserIdentityType」の「」を参照してください。

* コンソールでこのフィールドに複数の値を指定するには、フィールドを使用してフィルターに個別の値を指定する条件を追加し、次に追加の値ごとにそのステップを繰り返します。API でこれを行うには、フィルターに使用する値をリスト化する配列を使用します。

機密データの分類フィールド

次のテーブルでは、機密データの調査結果をフィルタリングするために使用できるフィールドのリストと説明を示します。これらのフィールドは、機密データの調査結果に固有のデータを保存します。

テーブルでは、フィールド 列は Amazon Macie コンソールのフィールドの名前を示します。JSON フィールド 列はドット表記を使用して、調査結果と Amazon Macie API の JSON 表現でフィールドの名前を示します。説明列はフィールドに保存されるデータの簡単な説明と、フィルター値の要件

を示します。テーブルは、フィールドごとにアルファベット順に昇順で並べ替えられ、次に JSON フィールド別に並べ替えられます。

フィールド	JSON フィールド	説明
カスタムデータ識別子 ID*	`classificationDetails.result.customDataIdentifiers.detections.arn`	データを検出して結果を生成したカスタムデータ識別子の一意の識別子。
カスタムデータ識別子名*	`classificationDetails.result.customDataIdentifiers.detections.name`	データを検出して結果を生成したカスタムデータ識別子の名前。
カスタムデータ識別子の合計カウント	`classificationDetails.result.customDataIdentifiers.detections.count`	カスタムデータ識別子によって検出され、調査結果を生成したデータの合計出現数。 このフィールドを使用して、フィルターの数値範囲を定義できます。
ジョブ ID*	`classificationDetails.jobId`	調査結果を生成した機密データ検出ジョブの一意の識別子。
オリジンのタイプ	`classificationDetails.originType`	Macie が検出結果の原因となった機密データをどのように見つけたか: `AUTOMATED_SENSITIVE_DATA_DISCOVERY` または `SENSITIVE_DATA_DISCOVERY_JOB` 。
—	`classificationDetails.result.mimeType`	調査結果が適用される MIME タイプなどのコンテンツのタイプ。たとえば、CSV ファイ

フィールド	JSON フィールド	説明
		ルでは、text/csv、Adobe Portable Document Format ファイルでは、application/pdf 。 このフィールドは、コンソールではフィルターオプションとして使用できません。
—	classificationDetails.result.sizeClassified	調査結果が適用される S3 オブジェクトの合計ストレージサイズ (バイト単位)。 このフィールドは、コンソールではフィルターオプションとして使用できません。API を使用すると、このフィールドを使用してフィルターの数値範囲を定義できます。

フィールド	JSON フィールド	説明
結果ステータスコード*	`classificationDetails.result.status.code`	調査結果のステータス。有効な値は次のとおりです。 • COMPLETE — Macie はオブジェクトの分析を完了しました。 • PARTIAL — Macie はオブジェクト内のデータのサブセットのみを分析しました。たとえば、オブジェクトはサポートされていない形式のファイルを含むアーカイブファイルです。 • SKIPPED — Macie はオブジェクトを分析できませんでした。たとえば、オブジェクトの形式が不正なファイルです。
機密データのカテゴリ	`classificationDetails.result.sensitiveData.category`	検出され、調査結果を生成した機密データのカテゴリ。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。API では、有効な値は `CREDENTIALS` 、`FINANCIAL_INFORMATION` 、および `PERSONAL_INFORMATION` です。

フィールド	JSON フィールド	説明
機密データの検出タイプ	`classificationDetails.result.sensitiveData.detections.type`	検出され、結果を生成した機密データのタイプ。 コンソールには、このフィールドをフィルターに追加するときに選択する値のリストが表示されます。コンソールと API の両方に有効な値のリストについては、機密データの検出タイプ を参照してください。
機密データの合計カウント	`classificationDetails.result.sensitiveData.detections.count`	検出され、結果を生成した機密データの出現の合計数。 このフィールドを使用して、フィルターの数値範囲を定義できます。

* コンソールでこのフィールドに複数の値を指定するには、フィールドを使用してフィルターに個別の値を指定する条件を追加し、次に追加の値ごとにそのステップを繰り返します。API でこれを行うには、フィルターに使用する値をリスト化する配列を使用します。

機密データの検出タイプ

次のトピックでは、フィルター内の 機密データの検出タイプ に対して指定できる値のリストを示します。(このフィールドの JSON 名は `classificationDetails.result.sensitiveData.detections.type` です。) トピックは、Macie がマネージドデータ識別子を使用して検出できる機密データのカテゴリ別に整理されています。

カテゴリ

- 認証情報
- 財務情報
- 個人情報: 個人の健康情報 (PHI)

- 個人情報: 個人を特定できる情報 (PII)

特定のタイプの機密データのマネージドデータ識別子の詳細については、詳細リファレンス:Amazon Macie マネージドデータ識別子 を参照してください。

認証情報

次の値を指定して、S3 オブジェクトでの認証情報データの出現をレポートする調査結果をフィルタリングできます。

機密データタイプ	フィルターの値
AWS シークレットアクセスキー	AWS_CREDENTIALS
Google Cloud API キー	GCP_API_KEY
HTTP 基本認証ヘッダー	HTTP_BASIC_AUTH_HEADER
JSON ウェブトークン (JWT)	JSON_WEB_TOKEN
OpenSSH プライベートキー	OPENSSH_PRIVATE_KEY
PGP プライベートキー	PGP_PRIVATE_KEY
公開鍵暗号標準 (PKCS) プライベートキー	PKCS
PuTTY プライベートキー	PUTTY_PRIVATE_KEY
ストライプ API キー	STRIPE_CREDENTIALS

財務情報

次の値を指定して、S3 オブジェクトでの財務情報の出現をレポートする調査結果をフィルタリングできます。

機密データタイプ	フィルターの値
銀行口座番号	BANK_ACCOUNT_NUMBER (カナダと米国の場合)

機密データタイプ	フィルターの値
基本銀行口座番号 (BBAN)	国またはリージョンによって異なります: FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER
クレジットカードの有効期限	CREDIT_CARD_EXPIRATION
クレジットカードの磁気ストライプデータ	CREDIT_CARD_MAGNETIC_STRIPE
クレジットカード番号	CREDIT_CARD_NUMBER (キーワードに近いクレジットカード番号の場合) と CREDIT_CARD_NUMBER_(NO_KEYWORD) (キーワードに近くないクレジットカード番号の場合)
クレジットカード認証コード	CREDIT_CARD_SECURITY_CODE

機密データタイプ	フィルターの値
銀行口座の支店コード (IBAN)	国または地域による：ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER,

機密データタイプ	フィルターの値
	MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (イギリス領バージン諸島の場合)

個人情報: 個人の健康情報 (PHI)

次の値を指定して、S3 オブジェクトでの個人ヘルス情報 (PHI) の出現をレポートする結果をフィルタリングできます。

機密データタイプ	フィルターの値
麻薬取締局 (DEA) 登録番号	US_DRUG_ENFORCEMENT_AGENCY_NUMBER
健康保険請求番号 (HICN)	USA_HEALTH_INSURANCE_CLAIM_NUMBER
健康保険または医療識別番号	国またはリージョンによって異なります: CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER
ヘルスケア共通手順コーディングシステム (HCPCS) コード	USA_HEALTHCARE_PROCEDURE_CODE
全米医薬品コード (NDC)	USA_NATIONAL_DRUG_CODE
国家プロバイダー識別子 (NPI)	USA_NATIONAL_PROVIDER_IDENTIFIER
機器固有識別子 (UDI)	MEDICAL_DEVICE_UDI

個人情報: 個人を特定できる情報 (PII)

次の値を指定して、S3 オブジェクトでの個人識別情報 (PII) の出現をレポートする結果をフィルタリングできます。

機密データタイプ	フィルターの値
生年月日	DATE_OF_BIRTH
運転免許証識別番号	国またはリージョンによって異なります: AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE,

機密データタイプ	フィルターの値
	BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (米国の場合)、ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
選挙人名簿番号	UK_ELECTORAL_ROLL_NUMBER
フルネーム	NAME
全地球測位システム (GPS) 座標	LATITUDE_LONGITUDE
HTTP クッキー	HTTP_COOKIE

機密データタイプ	フィルターの値
郵送先住所	ADDRESS, BRAZIL_CEP_CODE
国民識別番号	国またはリージョンによって異なります: BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER
国民保険番号 (NINO)	UK_NATIONAL_INSURANCE_NUMBER
パスポート番号	国またはリージョンによって異なります: CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
本籍地	CANADA_NATIONAL_IDENTIFICATION_NUMBER
電話番号	国または地域による：BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (カナダと米国の場合)、SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER
社会保険番号 (SIN)	CANADA_SOCIAL_INSURANCE_NUMBER
社会保障番号 (SSN)	国またはリージョンによって異なります: SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

機密データタイプ	フィルターの値
納税者識別番号または参照番号	国またはリージョンによって異なります: AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER
車両識別番号 (VIN)	VEHICLE_IDENTIFICATION_NUMBER

Amazon Macieの検出結果による機密データの調査

機密データ検出結果ジョブを実行するか、Amazon Macieが自動化された機密データ検出結果を実行すると、MacieはAmazon Simple Storage Service (Amazon S3)オブジェクトで見つけた機密データの各オカレンスの場所に関する詳細をキャプチャします。これには、マネージドデータ識別子を使用してMacieが検出した機密データや、ジョブまたはMacieが使用するように設定したカスタムデータ識別子の条件に一致するデータが含まれます。

機密データの検出結果では、Macieが個々のS3オブジェクトで検出結果した15件もの機密データについて、これらの詳細を確認することができます。詳細は、特定のS3バケットとオブジェクトが含む可能性のある機密データのカテゴリとタイプの広さについての洞察を提供します。オブジェクトに含まれるセンシティブなデータの個々の出現箇所を特定し、特定のバケットやオブジェクトについてより詳細な調査を行うかどうかを判断するのに役立ちます。

さらに詳しい情報を得るために、Macie が個別の検出結果で報告する機密データのサンプルを取得するように設定して使用することもできます。サンプルは、Macie が検出した機密データの性質を確認するのに役立ちます。また、対象の S3 バケットとオブジェクトの調査をカスタマイズするのにも役立ちます。検出結果のために機密データのサンプルを取得することを選択した場合、Macie は検出結果のデータを使用して、検出結果によって報告された各タイプの機密データが 1 ~ 10 件見つかった

箇所を特定します。次に、Macie は影響を受けたオブジェクトから機密データのそれらの出現を抽出し、データを表示して確認できるようにします。

S3 オブジェクトに多くの機密データの出現が含まれている場合は、検出結果を使用して、その検出結果の対応する機密データの検出結果に移動することもできます。機密データの検出結果とは異なり、機密データの検出結果は、Macie がオブジェクト内で検出した各タイプの機密データの最大 1,000 件までの出現の詳細な場所データを提供します。Macie は、機密データの調査結果と機密データの検出結果の場所データに同じスキーマを使用します。機密データの検出結果の詳細については、機密データ検出結果の保存と保持を参照してください。

このセクションのトピックでは、機密データの検出結果によって報告されたセンシティブ・データの出現箇所を検索し、オプションで取得する方法を説明する。また、Macie が見つけた機密データの個別の出現の場所をレポートするために Macie が使用するスキーマについても説明します。

トピック

- Amazon Macie の調査結果を用いて機密データを見つける
- Amazon Macie の検出結果を用いて機密データのサンプルを取得する
- 機密データの場所の JSON スキーマ

Amazon Macie の調査結果を用いて機密データを見つける

機密データ検出ジョブを実行するか、Amazon Macie が機密データ自動検出を実行すると、Macie は分析する各 Amazon Simple Storage Service (Amazon S3) オブジェクトの最新バージョンの詳細な検査を実行します。Macie は、深さ優先検索アルゴリズムも使用して、Macie が検出した機密データの 1～15 件の出現の場所に関する詳細をジョブの調査結果に入力します。これらの出現は、影響を受けた S3 バケットおよびオブジェクトに含まれる可能性のある機密データのカテゴリとタイプに関する洞察を提供します。また、この詳細によって、オブジェクト内の機密データの個別の出現を見つけ、特定のバケットやオブジェクトの詳細な調査を行うかどうかを判断することもできます。

機密データの検出結果を使用すると、Macie が影響を受けた S3 オブジェクトで見つけた機密データのうち最大 15 件までの出現の場所を特定できます。これには、Macie が マネージドデータ識別子を使用して検出した機密データ、および使用するジョブを設定している任意の カスタムデータ識別子の基準に一致するデータが含まれます。

機密データの検出結果は次のような詳細を提供できます。

- Microsoft Excel ワークブック、CSV ファイル、または TSV ファイルのセルまたはフィールドの列番号と行番号。

- JSON または JSON Lines ファイル内のフィールドまたは配列へのパス。
- CSV、JSON、JSON Lines、または TSV ファイル以外の非バイナリテキストファイル (HTML、TXT、XML ファイルなど) 内の行の行番号。
- Adobe Portable Document Format (PDF) ファイル内のページのページ番号。
- Apache Avro オブジェクトコンテナまたは Apache Parquet ファイル内のレコードのレコードインデックスとフィールドへのパス。

Amazon Macie コンソールまたは Amazon Macie API を使用してこれらの詳細にアクセスできます。また、Macie が他の AWS のサービス (Amazon EventBridge と AWS Security Hub の両方) に発行した調査結果でのこれらの詳細にもアクセスできます。Macie がこれらの詳細情報を報告するために使用する JSON 構造については、機密データの場所の JSON スキーマを参照してください。Macie が他の AWS のサービス に発行した調査結果の詳細にアクセスする方法については、調査結果のモニタリングと処理を参照してください。

S3 オブジェクトに多くの機密データの出現が含まれている場合は、検出結果を使用して、その検出結果の対応する機密データの検出結果に移動することもできます。機密データの検出結果とは異なり、機密データの検出結果は、Macie がオブジェクト内で検出した各タイプの機密データの最大 1,000 件までの出現の詳細な場所データを提供します。S3 オブジェクトが.tar ファイルや.zip ファイルなどのアーカイブファイルの場合、Macie がアーカイブから抽出した個々のファイルに含まれる機密データも含まれます。(Macie は、機密データの調査結果にこの情報を含めません。) 機密データの検出結果の詳細については、機密データ検出結果の保存と保持を参照してください。Macie は、機密データの調査結果と機密データの検出結果の場所データに同じスキーマを使用します。

機密データの出現を見つける

機密データの出現を見つけるには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。次の手順では、コンソールを使用して機密データを見つける方法を示しています。

機密データをプログラムで特定するには、Amazon Macie API の検出結果を取得オペレーションを使用します。特定タイプの機密データが 1 回以上出現した場所に関する詳細が検出結果に含まれている場合、その検出結果に含まれる `occurrences` オブジェクトがその詳細を提供します。詳細については、機密データの場所の JSON スキーマを参照してください。

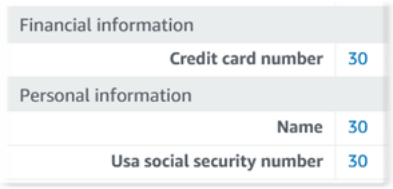
機密データの出現を見つけるには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果 を選択します。

> **Tip**
>
> また、ジョブ ページを使用して、特定のジョブのすべての調査結果を表示することもできます。これを行うには、ナビゲーションペインで ジョブ を選択し、次にジョブの名前を選択します。詳細パネルの上部で、結果を表示する を選択し、次に 調査結果を表示する を選択します。

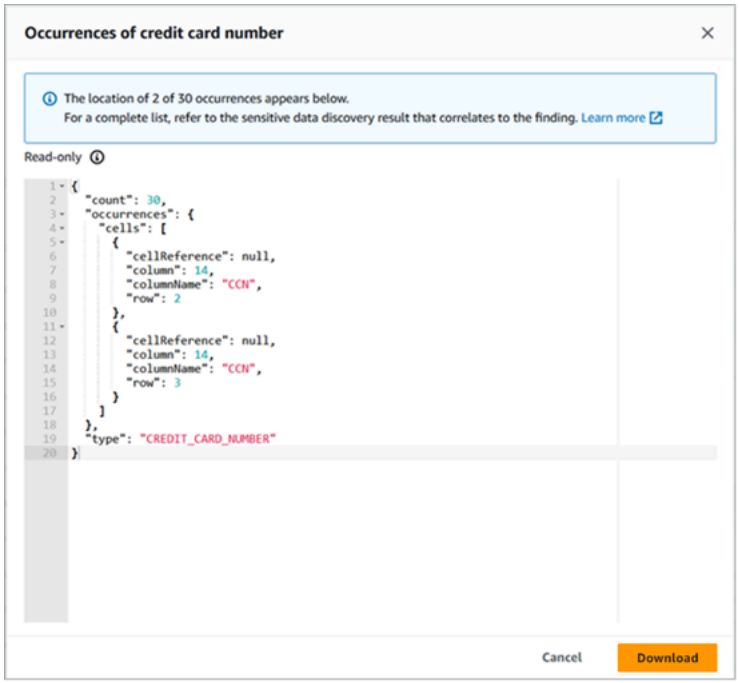
3. 調査結果 ページで、見つけたい機密データの調査結果を選択します。詳細パネルに、調査結果の情報が表示されます。
4. 詳細パネルで、詳細 セクションにスクロールします。このセクションでは、Macie が影響を受けた S3 オブジェクトで見つけた機密データのカテゴリとタイプに関する情報を提供します。Macie が検出した機密データのタイプごとの出現回数も示します。

   たとえば、以下の画像は、クレジットカード番号が 30 件、名前が 30 件、米国社会保障番号が 30 件発生したことを報告した検出結果の詳細を示しています。



   検出結果に、特定のタイプの機密データのうち 1 つ以上の出現の場所に関する詳細が含まれている場合、出現の数がリンクになります。リンクを選択すると、詳細が表示されます。Macie は新しいウィンドウを開き、詳細を JSON 形式で表示します。

   たとえば、次の図は、影響を受ける S3 オブジェクト内のクレジットカード番号が 2 つ出現する場所を示しています。



詳細を JSON ファイルとして保存するには、ダウンロード を選択し、次にファイルの名前と場所を指定します。

5. (オプション) すべての調査結果の詳細を JSON ファイルとして保存するには、詳細パネルの上部にある調査結果の識別子 (調査結果 ID) を選択します。Macie は新しいウィンドウを開き、すべての詳細を JSON 形式で表示します。ダウンロード を選択し、次にファイルの名前と場所を指定します。

影響を受けたオブジェクト内の各タイプの機密データの最大 1,000 件までの出現の場所に関する詳細にアクセスするには、その検出結果に対して対応する機密データの検出結果を参照します。そのためには、パネルの 詳細 セクションの先頭までスクロールします。次に、詳細結果の場所 フィールドでリンクを選択します。Macie は Amazon S3 コンソールを開き、対応する検出結果を含むファイルまたはフォルダーを表示します。

Amazon Macie の検出結果を用いて機密データのサンプルを取得する

Amazon Macie が検出結果で報告する機密データの性質を検証するために、必要に応じ、Macie を設定して使用し、個々の検出結果によって報告された機密データのサンプルを取得して公開することができます。これには、Macie が マネージドデータ識別子 を使用して検出した機密データ、および使用するジョブを設定している任意の カスタムデータ識別子 の基準に一致するデータが含まれます。サンプルは、対象の Amazon Simple Storage Service (Amazon S3) オブジェクトとバケットの調査をカスタマイズするのに役立ちます。

検出結果についての機密データのサンプルを取得して公開する場合、Macie は次の一般的なタスクを実行します。

1. 検出結果によって、機密データの個別の出現場所と、対応する機密データ検出の結果の場所が指定されていることを確認します。
2. 対応する機密データ検出の結果を評価し、対象の S3 オブジェクトのメタデータ、およびオブジェクトにおいて機密データが出現した場所のデータの有効性を確認します。
3. 機密データ検出結果のデータを使用して、検出結果によって報告された機密データの最初の 1 ~ 10 件を特定し、該当する S3 オブジェクトから各出現箇所の最初の 1 ~ 128 文字を抽出します。検出結果から複数タイプの機密データが報告された場合、Macie は最大 100 種類の機密データを検出します。
4. 抽出されたデータは、指定の AWS Key Management ServiceAWS KMSキーを使用して暗号化されます。
5. 暗号化されたデータを一時的にキャッシュに保存し、確認できるようにデータを表示します。データは、転送時および保管時のいずれも常に暗号化されます。
6. 運用上の問題を解決するために一時的に追加の保存が必要になった場合を除き、データは抽出、暗号化の後すぐにキャッシュから完全に削除されます。

検出結果についての機密データのサンプルを再度取得して公開することを選択した場合、Macie はこれらのタスクを繰り返して、サンプルを検索、抽出、暗号化、保存し、最終的には削除します。

Macie はこれらのタスクを実行するのに、アカウントの Macie サービスにリンクされたロールを使用しません。代わりに、AWS Identity and Access Management (IAM) ID を使用するか、または Macie がアカウント内で IAM ロールを引き受けることを許可します。ユーザーまたはロールが必要なリソースとデータにアクセスし、必要なアクションを実行することを許可されている場合は、検出結果についての機密データのサンプルを取得して公開することができます。必要なアクションはすべて AWS CloudTrail に口グで記録されます。

> **Important**
>
> カスタム IAM ポリシーを使用して、この機能へのアクセスを制限することをお勧めします。アクセス制御を強化するために、取得する機密データサンプルの暗号化専用 AWS KMS key を作成し、機密データサンプルの取得と開示を許可する必要があるプリンシパルのみにキーの使用を制限することをお勧めします。

この機能へのアクセスを制御するために使用できる推奨事項とポリシーの例については、AWSセキュリティブログのAmazon Macie を使用して S3 バケット内の機密データをプレビューする方法ブログ投稿を参照してください。

このセクションのトピックでは、Macie を設定および使用して、検出結果の機密データのサンプルを取得および開示する方法について説明します。アジアパシフィック (大阪) およびイスラエル (テルアビブ)リージョンを除く、Macie が現在利用可能なすべての AWS リージョン でこれらのタスクを実行できます。

トピック

- 検出結果についての機密データのサンプルを取得するための設定オプションと要件
- 検出結果についての機密データのサンプルを取得して公開するように Amazon Macie を設定する
- 検出結果についての機密データのサンプルの取得と公開

検出結果についての機密データのサンプルを取得するための設定オプションと要件

オプションで Amazon Macie を設定して使用し、Macie が個々の検出結果で報告する機密データのサンプルを取得して公開することができます。検出結果についての機密データのサンプルを取得して公開する場合、Macie は対応する機密データ検出の結果のデータを使用して、対象の Amazon Simple Storage Service (Amazon S3) オブジェクト内の機密データの出現を見つけます。次に、Macie は該当オブジェクトからそれらの出現のサンプルを抽出します。Macie は、抽出したデータを指定した AWS Key Management ServiceAWS KMS キーで暗号化し、暗号化されたデータを一時的にキャッシュに保存し、結果にそのデータを結果として返します。Macie は、運用上の問題を解決するために一時的に追加の保存が必要になった場合を除き、抽出と暗号化の直後に、データをキャッシュから完全に削除します。

Macie は、対象の S3 オブジェクトについての機密データのサンプルを検索、取得、暗号化、公開することを目的として、アカウントのために Macie サービスリンクロールを使用することはありません。代わりに、Macie はアカウントのために構成した設定とリソースを使用します。Macie で設定を構成する際には、対象の S3 オブジェクトに対するアクセスメソッドを指定します。また、サンプルを暗号化するために使用する AWS KMS key も指定します。アジアパシフィック (大阪) およびイスラエル (テルアビブ) リージョンを除く、Macie が現在利用可能なすべての AWS リージョン で設定を構成できます。

対象の S3 オブジェクトにアクセスし、そこから機密データのサンプルを取得するには、2 つのオプションがあります。AWS Identity and Access Management (IAM) ユーザー認証情報を使用するか、または IAM ロールを引き受けるように Macie を設定できます:

- IAM ユーザー認証情報を使用する – このオプションを使用すると、アカウントの各ユーザーは、個別の IAM ID を使用して、サンプルを検索、取得、暗号化、公開します。これは、ユーザーまたはロールが必要なリソースとデータにアクセスし、必要なアクションを実行することを許可されている場合は、検出結果についての機密データのサンプルを取得して公開することができることを意味します。
- IAM ロールを引き受ける – このオプションを使用すると、Macie にアクセスを委任する IAM ロールを作成します。また、ロールの信頼ポリシーと許可ポリシーが、Macie がロールを引き受けるためのすべての要件を満たしているようにしてください。その後、アカウントのユーザーが、検出結果についての機密データのサンプルを検索、取得、暗号化、公開することを選択すると、Macie がそのロールを引き受けます。

いずれの設定も、組織のために委任された Macie 管理者アカウント、組織内の Macie メンバーアカウント、スタンドアロン Macie アカウントなど、あらゆるタイプの Macie アカウントで使用できます。

次のトピックでは、アカウントのための設定とリソースを構成する方法を決定するのに役立つオプション、要件、考慮事項について説明します。これには、IAM ロールにアタッチする信頼ポリシーと許可ポリシーが含まれます。機密データのサンプルを取得して公開するために使用できる追加のレコメンデーションとポリシーの例については、AWS セキュリティブログのブログ記事「Amazon Macie を利用して S3 バケットの機密データをプレビューする方法」を参照してください。

トピック

使用するアクセスメソッドの決定

AWS 環境に最適な設定を決定する場合、重要な考慮事項は、組織として一元的に管理されている複数の Amazon Macie アカウントが環境に含まれているかどうかです。自分が組織の委任された

Macie の管理者である場合、IAM ロールを引き受けるように Macie を設定すると、組織内のアカウントのために、対象の S3 オブジェクトからの機密データのサンプルの取得を効率化できます。このアプローチでは、管理者アカウントに IAM ロールを作成します。また、該当の各メンバーアカウントにも IAM ロールを作成します。管理者アカウントのロールは、Macie に対するアクセスを委任します。メンバーアカウントのロールは、管理者アカウントのロールに対するクロスアカウントアクセスを委任します。その後、実装されている場合は、メンバーアカウントのために、ロールの連鎖を使用して対象の S3 オブジェクトにアクセスできます。

また、デフォルトで個々の検出結果に直接アクセスできるようにするユーザーについても検討します。検出結果についての機密データのサンプルを取得して公開するには、ユーザーはまず、検出結果にアクセスできる必要があります。

- 機密データ検出ジョブ – ジョブを作成するアカウントのみが、ジョブが生成する検出結果にアクセスできます。Macie の管理者アカウントがある場合は、組織内の任意のアカウントのために、S3 バケット内のオブジェクトを分析するジョブを設定できます。そのため、ジョブは、メンバーアカウントが所有するバケット内のオブジェクトについての検出結果を生成できます。メンバーアカウントまたはスタンドアロン Macie アカウントがある場合は、アカウントが所有するバケット内のオブジェクトのみを分析するようにジョブを設定できます。
- 機密データの自動検出 – Macie の管理者アカウントのみが、組織内のアカウントのために、自動検出によって生成された検出結果にアクセスできます。メンバーアカウントはこれらの検出結果にアクセスできません。スタンドアロン Macie アカウントがある場合は、自分のアカウントのためにのみ、自動検出によって生成された検出結果にアクセスできます。

IAM ロールを使用して対象の S3 オブジェクトにアクセスする予定がある場合は、次の点も考慮してください:

- オブジェクトにおける機密データの出現を特定するには、検出結果についての対応する機密データ検出の結果が、Macie が Hash-based Message Authentication Code (HMAC) AWS KMS key で署名した S3 オブジェクトに保存されている必要があります。Macie は、機密データ検出の結果の完全性と信頼性を検証できる必要があります。検証できない場合、Macie は、機密データのサンプルを取得するための IAM ロールを引き受けません。これは、アカウントのために、S3 オブジェクト内のデータに対するアクセスを制限することを目的とした追加のガードレールです。
- カスタマーマネージド AWS KMS key を使用して暗号化されたオブジェクトから機密データのサンプルを取得するには、IAM ロールがキーを使用してデータを復号することを許可する必要があります。より具体的には、キーのポリシーで、ロールによる `kms:Decrypt` アクションの実行が許可されている必要があります。他のタイプのサーバー側の暗号化の場合、対象のオブジェクトを

復号するために追加の許可やリソースは必要ありません。詳細については、「対象の S3 オブジェクトの復号」を参照してください。

- 別のアカウントのためにオブジェクトから機密データのサンプルを取得するには、現在、該当の AWS リージョン のアカウントのために委任された Macie の管理者である必要があります。加えて:
  - 現在、該当のリージョンのメンバーアカウントのために Macie が有効になっている必要があります。
  - メンバーアカウントには、Macie の管理者アカウントの IAM ロールに対するクロスアカウントアクセスを委任する IAM ロールが必要です。ロールの名前は、Macie の管理者アカウントとメンバーアカウントで同じである必要があります。
  - メンバーアカウントの IAM ロールの信頼ポリシーには、設定のために正しい外部 ID を指定する条件が含まれている必要があります。この ID は、Macie の管理者アカウントのために設定を構成した後に Macie が自動的に生成する一意の英数字の文字列です。信頼ポリシーにおける外部 ID の使用の詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS リソースに対するアクセス権を第三者に付与するときに外部 ID を使用する方法」を参照してください。
  - メンバーアカウントの IAM ロールが Macie のすべての要件を満たしている場合、メンバーアカウントは、自らのアカウントのためにオブジェクトから機密データのサンプルを取得することを目的として、Macie の設定を構成して有効にする必要はありません。Macie は、Macie の管理者アカウントの設定と IAM ロール、およびメンバーアカウントの IAM ロールのみを使用します。

> **Tip**
>
> アカウントが大規模な組織に属している場合は、AWS CloudFormation テンプレートとスタックセットを使用して、組織内のメンバーアカウントのために IAM ロールをプロビジョニングおよび管理することを検討してください。テンプレートとスタックセットの作成と使用については、「AWS CloudFormation ユーザーガイド」を参照してください。
>
> 開始点として機能する CloudFormation テンプレートを確認し、必要に応じてダウンロードするには、Amazon Macie コンソールを使用できます。コンソールのナビゲーションペインの [設定] で、[サンプルを公開] を選択します。[編集] を選択し、[メンバーロールの許可と CloudFormation テンプレートを表示] を選択します。

このセクションの後続のトピックでは、各タイプの設定に関する追加の詳細と考慮事項を説明します。IAM ロールの場合、これには、ロールにアタッチする信頼ポリシーと許可ポリシーが含まれま

す。どのタイプの設定が環境に最適であるかが不明な場合は、AWS の管理者に問い合わせてください。

IAM ユーザー認証情報を使用した、対象の S3 オブジェクトに対するアクセス

IAM ユーザー認証情報を使用して機密データのサンプルを取得するように Amazon Macie を設定すると、Macie アカウントの各ユーザーは自らの IAM ID を使用して、個々の検出結果についてのサンプルを検索、取得、暗号化、公開します。これは、ユーザーの IAM ID が必要なリソースとデータにアクセスし、必要なアクションを実行することを許可されている場合は、検出結果についての機密データのサンプルを取得して公開することができることを意味します。必要なアクションはすべて AWS CloudTrail にログで記録されます。

特定の検出結果について機密データのサンプルを取得して公開するには、ユーザーによる次のデータおよびリソースに対するアクセスが許可されている必要があります: 検出結果、対応する機密データ検出の結果、対象の S3 バケット、および対象の S3 オブジェクト。また、対象のオブジェクトの暗号化に使用した AWS KMS key (該当する場合)、および機密データのサンプルの暗号化に使用するように Macie を設定した AWS KMS key の使用も許可されている必要があります。IAM ポリシー、リソースポリシー、または他の許可設定で必要なアクセスが拒否されている場合、ユーザーは、検出結果のサンプルを取得して公開することができません。

このような構成を設定するには、次の一般的なタスクを実行します。

1. 機密データ検出の結果用のリポジトリを設定していることを確認します。
2. 機密データのサンプルの暗号化に使用するための AWS KMS key を設定します。
3. Macie で設定を構成するための許可を確認します。
4. Macie で設定を構成して有効にします。

これらのタスクの実行の詳細については、「検出結果についての機密データのサンプルを取得して公開するように Amazon Macie を設定する」を参照してください。

対象の S3 オブジェクトにアクセスするための IAM ロールの引き受け

IAM ロールを引き受けることで機密データのサンプルを取得するように Amazon Macie を設定するには、まず Macie にアクセスを委任する IAM ロールを作成します。ロールの信頼ポリシーと許可ポリシーが、Macie がロールを引き受けるためのすべての要件を満たしているようにしてください。Macie アカウントのユーザーが検出結果についての機密データのサンプルを取得して公開することを選択すると、Macie は、対象の S3 オブジェクトからサンプルを取得するためのロールを引き受けます。Macie は、ユーザーが検出結果についてのサンプルを取得して公開することを選択した場合にのみ、ロールを引き受けます。ロールを引き受けるために、Macie は AWS Security Token

Service (AWS STS) API の AssumeRole オペレーションを使用します。必要なアクションはすべて AWS CloudTrail にログで記録されます。

特定の検出結果についての機密データのサンプルを取得して公開するには、その検出結果、対応する機密データ検出の結果、および機密データのサンプルを暗号化するために使用するように Macie を設定する AWS KMS key に対するユーザーによるアクセスが許可されている必要があります。IAM ロールは、Macie が対象の S3 バケットおよび対象の S3 オブジェクトにアクセスするのを許可する必要があります。また、該当する場合、ロールは、対象のオブジェクトの暗号化に使用された AWS KMS key を使用することを許可されている必要があります。IAM ポリシー、リソースポリシー、または他の許可設定で必要なアクセスが拒否されている場合、ユーザーは、検出結果のサンプルを取得して公開することができません。

このような構成を設定するには、次の一般的なタスクを実行します。組織内にメンバーアカウントがある場合は、Macie の管理者と協力して、アカウントのために設定およびリソースを構成するかどうか、およびその方法を決定します。

1. 次を定義します:
   - Macie に引き受けさせる IAM ロールの名前。アカウントが組織に属している場合、この名前は、委任された Macie の管理者アカウントと、組織内の該当の各メンバーアカウントで同じである必要があります。この名前が異なる場合、Macie の管理者は、該当のメンバーアカウントのために、対象の S3 オブジェクトにアクセスできません。
   - IAM ロールにアタッチする IAM 許可ポリシーの名前。アカウントが組織に属している場合は、組織内の該当の各メンバーアカウントで同じポリシー名を使用することをお勧めします。これにより、メンバーアカウントでのロールのプロビジョニングおよび管理を合理化できます。
2. 機密データ検出の結果用のリポジトリを設定していることを確認します。
3. 機密データのサンプルの暗号化に使用するための AWS KMS key を設定します。
4. IAM ロールを作成し、Macie で設定を構成するための許可を確認します。
5. 自分が組織の委任された Macie の管理者である場合、またはスタンドアロン Macie アカウントがある場合:
   a. アカウントのために、IAM ロールを作成して設定します。ロールの信頼ポリシーと許可ポリシーが、Macie がロールを引き受けるためのすべての要件を満たしているようにしてください。これらの要件の詳細については、次のトピックを参照してください。
   b. Macie で設定を構成して有効にします。その後、Macie は設定の外部 ID を生成します。ユーザーが組織の Macie 管理者である場合は、この ID を書き留めます。該当の各メンバーアカウントの IAM ロールの信頼ポリシーでは、この ID が指定される必要があります。
6. 組織にメンバーアカウントがある場合:

a. アカウントの IAM ロールの信頼ポリシーで指定する外部 ID については、Macie の管理者に問い合わせてください。また、作成する IAM ロールと許可ポリシーの名前も確認します。

b. アカウントのために、IAM ロールを作成して設定します。ロールの信頼ポリシーと許可ポリシーが、Macie の管理者がロールを引き受けるためのすべての要件を満たしているようにしてください。これらの要件の詳細については、次のトピックを参照してください。

c. (オプション) 自分のアカウントのために、対象の S3 オブジェクトから機密データのサンプルを取得して公開する場合は、Macie で設定を構成して有効にします。サンプルを取得するための IAM ロールを Macie に引き受けさせる場合は、まずアカウントに追加の IAM ロールを作成して設定します。この追加ロールの信頼ポリシーと許可ポリシーが、Macie がロールを引き受けるためのすべての要件を満たしているようにしてください。その後、Macie で設定を構成し、この追加ロールの名前を指定します。ロールのポリシー要件の詳細については、次のトピックを参照してください。

これらのタスクの実行の詳細については、「検出結果についての機密データのサンプルを取得して公開するように Amazon Macie を設定する」を参照してください。

対象の S3 オブジェクトにアクセスするための IAM ロールの設定

IAM ロールを使用して対象の S3 オブジェクトにアクセスするには、まず Amazon Macie にアクセスを委任するロールを作成して設定します。ロールの信頼ポリシーと許可ポリシーが、Macie がロールを引き受けるためのすべての要件を満たしているようにしてください。これを行う方法は、保有している Macie アカウントのタイプによって異なります。

次のセクションでは、Macie アカウントのタイプごとに、IAM ロールにアタッチする信頼ポリシーと許可ポリシーについて詳しく説明します。保有しているアカウントのタイプに応じたセクションを選択してください。

> **Note**
>
> 組織にメンバーアカウントがある場合は、アカウントのために 2 つの IAM ロールを作成して設定する必要がある場合があります。
>
> - Macie の管理者が、アカウントのために、対象の S3 オブジェクトから機密データのサンプルを取得して公開するのを許可するには、管理者のアカウントが引き受けることができるロールを作成して設定します。これらの詳細については、Macie メンバーアカウントのセクションを選択します。

- 自分のアカウントのために、対象の S3 オブジェクトから機密データのサンプルを取得して公開するには、Macie が引き受けることができるロールを作成して設定します。これらの詳細については、スタンドアロン Macie アカウントのセクションを選択します。

いずれかの IAM ロールを作成して設定する前に、Macie の管理者と協力してアカウントのために適切な設定を決定します。

IAM を使用したロールの作成の詳細については、「AWS Identity and Access Management ユーザーガイド」の「カスタム信頼ポリシーを使用したロールの作成」を参照してください。

Macie 管理者アカウント

自分が組織の委任された Macie の管理者である場合は、まず IAM ポリシーエディタを使用して IAM ロールの許可ポリシーを作成します。ポリシーは次のとおりである必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "AssumeMacieRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::*:role/IAMRoleName"
        }
    ]
}
```

IAMRoleName は、組織のアカウントのために、対象の S3 オブジェクトから機密データのサンプルを取得する際に Macie が引き受ける IAM ロールの名前です。この値を、アカウントのために作成しようとしているロールの名前、および組織内の該当のメンバーアカウントのために作成する予定のロールの名前に置き換えます。この名前は、Macie の管理者アカウントと、該当の各メンバーアカウントで同じである必要があります。

> **Note**
>
> 前述の許可ポリシーでは、最初のステートメントの Resource 要素で、ワイルドカード文字 (*) が使用されています。これにより、アタッチされた IAM エンティティは、組織が所有するすべての S3 バケットからオブジェクトを取得できるようになります。特定のバケットについてのみ、このアクセスを許可するには、ワイルドカード文字を各バケットの Amazon リソースネーム (ARN) に置き換えます。例えば、DOC-EXAMPLE-BUCKET という名前のバケット内のオブジェクトに対するアクセスのみを許可するには、要素を次のように変更します:
>
> `"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"`
>
> 個々のアカウントのために、特定の S3 バケット内のオブジェクトに対するアクセスを制限することもできます。これを行うには、該当の各アカウントの IAM ロールの許可ポリシーの Resource 要素でバケット ARN を指定します。詳細と例については、「AWS Identity and Access Management ユーザーガイド」の「IAM JSON ポリシー要素: Resource」を参照してください。

IAM ロールの許可ポリシーを作成した後、ロールを作成して設定します。IAM コンソールを使用してこれを行う場合は、ロールの [信頼されたエンティティタイプ] として [カスタム信頼ポリシー] を選択します。ロールの信頼されたエンティティを定義する信頼ポリシーについては、次のように指定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

accountID はお客様の AWS アカウント のアカウント ID です。この値を自分の 12 桁のアカウント ID に置き換えます。

前述の信頼ポリシーでは次のようになります:

- `Principal` 要素は、対象の S3 オブジェクト `reveal-samples.macie.amazonaws.com` から機密データのサンプルを取得する際に Macie が使用するサービスプリンシパルを指定します。
- `Action` 要素は、サービスプリンシパルによる実行が許可されているアクション (AWS Security Token Service (AWS STS) API の AssumeRole オペレーション) を指定します。
- `Condition` 要素は、aws:SourceAccount グローバル条件コンテキストキーを使用する条件を定義します。この条件により、指定されたアクションを実行できるアカウントが決まります。この場合、Macie は指定されたアカウント(*accountID*) のためにのみ、ロールを引き受けることができます。この条件は、Macieが AWS STS とのトランザクション中に混乱した使節として使用されるのを防ぐのに役立ちます。

IAM ロールの信頼ポリシーを定義した後、許可ポリシーをロールにアタッチします。これは、ロールの作成を開始する前に作成した許可ポリシーである必要があります。その後、IAM の残りのステップを完了して、ロールの作成と設定を完了します。完了したら、Macie で設定を構成して有効にします。

Macie メンバーアカウント

Macie メンバーアカウントがあり、アカウントのために、対象の S3 オブジェクトから機密データのサンプルを取得して公開することを Macie の管理者に許可したい場合は、まず Macie の管理者に次の情報を問い合わせてください。

- 作成する IAM ロールの名前。この名前は、自分のアカウントと、組織の Macie の管理者アカウントで同じである必要があります。
- ロールにアタッチする IAM 許可ポリシーの名前。
- ロールの信頼ポリシーで指定する外部 ID。この ID は、Macie の管理者の設定用に Macie が生成した外部 ID である必要があります。

この情報を受け取ったら、IAM ポリシーエディタを使用して、ロールの許可ポリシーを作成します。ポリシーは次のとおりである必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

前述の許可ポリシーにより、アタッチされた IAM エンティティが、アカウントのために、すべての S3 バケットからオブジェクトを取得できるようになります。これは、ポリシー内の Resource 要素でワイルドカード文字 (*) が使用されているためです。特定のバケットについてのみ、このアクセスを許可するには、ワイルドカード文字を各バケットの Amazon リソースネーム (ARN) に置き換えます。例えば、DOC-EXAMPLE-BUCKET2 という名前のバケット内のオブジェクトに対するアクセスのみを許可するには、要素を次のように変更します:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

詳細と例については、「AWS Identity and Access Management ユーザーガイド」の「IAM JSON ポリシー要素: Resource」を参照してください。

IAM ロールの許可ポリシーを作成した後、ロールを作成します。IAM コンソールを使用してロールを作成する場合は、ロールの [信頼されたエンティティタイプ] として [カスタム信頼ポリシー] を選択します。ロールの信頼されたエンティティを定義する信頼ポリシーについては、次のように指定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieAdminRevealRoleForCrossAccountAccess",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::administratorAccountID:role/IAMRoleName"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "externalID",
                    "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
                }
            }
        }
    ]
}
```

前述のポリシーで、プレースホルダーの値を AWS 環境の正しい値に置き換えます。ここでは次のとおりです:

- *administratorAccountID* は、Macie の管理者アカウントの 12 桁のアカウント ID です。
- *IAMRoleName* は、Macie の管理者のアカウントの IAM ロールの名前です。これは、Macie の管理者から受け取った名前である必要があります。
- *externalID* は、Macie の管理者から受け取った外部 ID です。

一般に、信頼ポリシーにより、Macie の管理者は、アカウントのために、対象の S3 オブジェクトから機密データのサンプルを取得して公開するためのロールを引き受けることができます。`Principal` 要素は、Macie の管理者のアカウントにおける IAM ロールの ARN を指定します。これは、Macie の管理者が、組織のアカウントのために、機密データのサンプルを取得して公開するために使用するロールです。`Condition` ブロックは、そのロールを引き受けることができるユーザーをさらに決定する 2 つの条件を定義します。

- 1 つ目の条件は、組織の設定に固有の外部 ID を指定します。外部 ID の詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS リソースへのアクセス権を第三者に付与するときに外部 ID を使用する方法」を参照してください。
- 2 つ目の条件は、aws:PrincipalOrgID グローバル条件コンテキストキーを使用します。キーの値は、AWS Organizations (`${aws:ResourceOrgID}`) 内の組織の一意の識別子を表す動的変数です。この条件により、AWS Organizations の同じ組織に属しているアカウントのみにアクセスが制限されます。Macie で招待を承諾して組織に参加した場合は、この条件をポリシーから削除します。

IAM ロールの信頼ポリシーを定義した後、許可ポリシーをロールにアタッチします。これは、ロールの作成を開始する前に作成した許可ポリシーである必要があります。その後、IAM の残りのステップを完了して、ロールの作成と設定を完了します。Macie でロールの設定を構成および入力しないでください。

スタンドアロン Macie アカウント

スタンドアロン Macie アカウントまたは Macie メンバーアカウントがあり、自分のアカウントのために、対象の S3 オブジェクトから機密データのサンプルを取得して公開する場合は、まず IAM ポリシーエディタを使用して IAM ロールの許可ポリシーを作成します。ポリシーは次のとおりである必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

前述の許可ポリシーでは、Resource 要素で、ワイルドカード文字 (*) が使用されています。これにより、アタッチされた IAM エンティティは、アカウントのために、すべての S3 バケットからオブジェクトを取得できるようになります。特定のバケットについてのみ、このアクセスを許可するには、ワイルドカード文字を各バケットの Amazon リソースネーム (ARN) に置き換えます。例えば、DOC-EXAMPLE-BUCKET3 という名前のバケット内のオブジェクトに対するアクセスのみを許可するには、要素を次のように変更します:

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

詳細と例については、「AWS Identity and Access Management ユーザーガイド」の「IAM JSON ポリシー要素: Resource」を参照してください。

IAM ロールの許可ポリシーを作成した後、ロールを作成します。IAM コンソールを使用してロールを作成する場合は、ロールの [信頼されたエンティティタイプ] として [カスタム信頼ポリシー] を選択します。ロールの信頼されたエンティティを定義する信頼ポリシーについては、次のように指定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

accountID はお客様の AWS アカウント のアカウント ID です。この値を自分の 12 桁のアカウント ID に置き換えます。

前述の信頼ポリシーでは次のようになります:

- Principal 要素は、対象の S3 オブジェクト reveal-samples.macie.amazonaws.com から機密データのサンプルを取得して公開する際に Macie が使用するサービスプリンシパルを指定します。
- Action 要素は、サービスプリンシパルによる実行が許可されているアクション (AWS Security Token Service (AWS STS) API の AssumeRole オペレーション) を指定します。
- Condition 要素は、aws:SourceAccount グローバル条件コンテキストキーを使用する条件を定義します。この条件により、指定されたアクションを実行できるアカウントが決まります。Macie は指定されたアカウント(*accountID*) のためにのみ、ロールを引き受けることができます。この条件は、Macieが AWS STS とのトランザクション中に混乱した使節として使用されるのを防ぐのに役立ちます。

IAM ロールの信頼ポリシーを定義した後、許可ポリシーをロールにアタッチします。これは、ロールの作成を開始する前に作成した許可ポリシーである必要があります。その後、IAM の残りのステップを完了して、ロールの作成と設定を完了します。完了したら、Macie で設定を構成して有効にします。

対象の S3 オブジェクトの復号

Amazon S3 は S3 オブジェクトの複数の暗号化オプションをサポートしています。これらのオプションのほとんどでは、IAM ユーザーまたはロールが対象のオブジェクトから機密データのサンプルを復号して取得するために追加のリソースや許可は必要ありません。これは、Amazon S3 マネージドキーまたは AWS マネージド AWS KMS key を使用したサーバー側の暗号化を使用して暗号化されたオブジェクトの場合に当てはまります。

ただし、S3 オブジェクトがカスタマーマネージド AWS KMS key で暗号化されている場合、オブジェクトから機密データのサンプルを復号して取得するには追加の許可が必要です。より具体的には、KMS キーのキーポリシーでは、IAM ユーザーまたはロールによる `kms:Decrypt` アクションの実行が許可されている必要があります。許可されていない場合、エラーが発生し、Macie はオブジェクトからサンプルを取得しません。IAM ユーザーのためにこのアクセスを提供する方法については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS の認証とアクセスコントロール」を参照してください。

IAM ロールのためにこのアクセスを提供する方法は、AWS KMS key を所有するアカウントがそのロールも所有しているかどうかによって異なります。

- 同じアカウントが KMS キーとロールを所有している場合、アカウントのユーザーはキーのポリシーを更新する必要があります。
- 1 つのアカウントが KMS キーを所有し、別のアカウントがロールを所有している場合、そのキーを所有するアカウントのユーザーはキーに対するクロスアカウントアクセスを許可する必要があります。

このトピックでは、S3 オブジェクトから機密データのサンプルを取得するために作成した IAM ロールのためにこれらのタスクを実行する方法について説明します。両方のシナリオの例も示します。他のシナリオでカスタマーマネージド AWS KMS keys に対するアクセスを許可する方法については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS の認証とアクセスコントロール」を参照してください。

カスタマーマネージドキーへの同じアカウントのアクセスを許可する

同じアカウントが AWS KMS key と IAM ロールの両方を所有している場合、アカウントのユーザーはキーのポリシーにステートメントを追加する必要があります。追加のステートメントでは、IAM ロールによるキーを使用したデータの復号が許可されている必要があります。キーポリシーの更新の詳細な情報については、AWS Key Management Serviceデベロッパーガイドのキーポリシーの変更を参照してください。

ステートメントにおいて:

- `Principal` 要素は、IAM ロールの Amazon リソースネーム (ARN) を指定するものである必要があります。
- `Action` 配列は、`kms:Decrypt` アクションを指定する必要があります。これは、キーで暗号化されるオブジェクトを復号するために IAM ロールが実行することを許可される必要がある唯一の AWS KMS アクションです。

以下は、KMS キーのポリシーに追加するステートメントの例です。

```
{
    "Sid": "Allow the Macie reveal role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

前の例では、以下のようになっています。

- `Principal` 要素の `AWS` フィールドは、アカウントの IAM ロールの ARN を指定します。これにより、ロールがポリシーステートメントで指定されたアクションを実行することを許可します。*123456789012* はアカウント ID の例です。この値をロールと KMS キーを所有するアカウントのアカウント ID に置き換えます。*IAMRoleName* は名前の例です。この値をアカウントの IAM ロールの名前に置き換えます。
- `Action` 配列は、IAM ロールが KMS キーを使用して実行することを許可されたアクション (キーで暗号化される暗号文を復号) を指定します。

このステートメントをキーポリシーのどこに追加するかは、ポリシーに現在含まれている構造と要素によって異なります。ステートメントをポリシーに追加するときに、構文が有効であることを確認します。キーポリシーは JSON 形式を使用します。これは、ステートメントをポリシーのどこに追加するかに応じて、ステートメントの前後にカンマを追加する必要があることも意味します。

カスタマーマネージドキーへのクロスアカウントアクセスを許可する

1 つのアカウントが AWS KMS key を所有 (キー所有者) し、別のアカウントが IAM ロールを所有 (ロール所有者) している場合、キー所有者は、キーに対するクロスアカウントアクセスをロール所有者に提供する必要があります。これを実現する方法の 1 つは許可を使用することです。付与 は、ポリシーツールであり、付与によって指定された条件が満たされている場合、AWS プリンシパルに暗号化オペレーションで (KMS キー) の使用を許可します。付与の詳細については、AWS Key Management Service デベロッパーガイドのAWS KMS での付与を参照してください。

このアプローチでは、キー所有者はまず、キーのポリシーで、ロール所有者によるキーの許可の作成が許可されているようにします。その後、ロール所有者はキーの許可を作成します。この許可は、関連する許可をロール所有者のアカウントの IAM ロールに委任します。これにより、ロールは、キーを使用して暗号化された S3 オブジェクトを復号できるようになります。

ステップ 1: キーポリシーを変更する

キー所有者は、ロール所有者が自ら (ロール所有者) のアカウントの IAM ロールのために許可を作成することを許可するステートメントが、キーポリシーに含まれているようにする必要があります。このステートメントでは、Principal 要素は、ロールの所有者のアカウントの ARN を指定する必要があります。Action 配列は、kms:CreateGrant アクションを指定する必要があります。Condition ブロックは、指定されたアクションに対するアクセスをフィルタリングできます。以下は、KMS キーのポリシーのこのステートメントの例です。

```
{
    "Sid": "Allow a role in an account to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/IAMRoleName"
```

```
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": "Decrypt"
        }
    }
}
```

前の例では、以下のようになっています。

- `Principal` 要素の `AWS` フィールドは、ロール所有者のアカウントの ARN を指定します。これにより、アカウントがポリシーステートメントで指定されたアクションを実行することを許可します。*111122223333* はアカウント ID の例です。この値をロール所有者のアカウントのアカウント ID に置き換えます。
- `Action` 配列は、ロール所有者が KMS キーを使用して実行することを許可されたアクションを指定します (キーの許可を作成)。
- `Condition` ブロックは、条件演算子と次の条件キーを使用して、ロール所有者が KMS キーに対して実行することを許可されているアクションに対するアクセスをフィルタリングします。
  - kms:GranteePrincipal – この条件は、ロール所有者が、アカウント内の IAM ロールの ARN である、指定された許可付与対象プリンシパルのためにのみ、許可を作成することを許可します。そのARNでは、*111122223333* はアカウント ID の例です。この値をロール所有者のアカウントのアカウント ID に置き換えます。*IAMRoleName* は名前の例です。この値をロール所有者のアカウントの IAM ロールの名前に置き換えます。
  - kms:GrantOperations – この条件は、ロール所有者が、AWS KMS `Decrypt` アクション (キーを使用して暗号化された暗号文の復号) を実行するための許可を委任するためだけに許可を作成することを許可します。これにより、ロール所有者は、KMS キーに対して他のアクションを実行するための許可を委任する許可を作成できなくなります。`Decrypt` アクションは、キーで暗号化されるオブジェクトを復号するために IAM ロールが実行することを許可される必要がある唯一の AWS KMS アクションです。

キー所有者がこのステートメントをキーポリシーのどこに追加するかは、ポリシーに現在含まれている構造と要素によって異なります。キー所有者がステートメントを追加するときは、構文が有効であることを確認する必要があります。キーポリシーは JSON 形式を使用します。これは、ステートメントをポリシーのどこに追加するかに応じて、キー所有者はステートメントの前後にカンマを追加する必要があることも意味します。キーポリシーの更新の詳細な情報については、AWS Key Management Service デベロッパーガイドのキーポリシーの変更を参照してください。

ステップ 2: 許可を作成する

キー所有者が必要に応じてキーポリシーを更新した後、ロール所有者はキーの許可を作成します。この許可は、関連する許可を (ロール所有者の) アカウントの IAM ロールに委任します。ロール所有者が許可を作成する前に、ロール所有者は、`kms:CreateGrant` アクションの実施が許可されていることを確認する必要があります。このアクションにより、ロール所有者が既存のカスタマーマネージド AWS KMS key に許可を追加することが許可されます。

許可を作成するには、ロール所有者は AWS Key Management Service APIの CreateGrant オペレーションを使用できます。ロール所有者が許可を作成するときに、必要なパラメータに次の値を指定する必要があります。

- `KeyId` – KMS キーの ARN。KMS キーへのクロスアカウントアクセスでは、この値は ARN である必要があります。キー ID にすることはできません。
- `GranteePrincipal` – アカウント内の IAM ロールの ARN。この値は `arn:aws:iam::`*`111122223333`*`:role/`*`IAMRoleName`* である必要があります。ここで、*`111122223333`* はロール所有者のアカウントのアカウント ID であり、*`IAMRoleName`* はロールの名前です。
- `Operations` – AWS KMS 復号アクション (`Decrypt`)。これは、KMS キーで暗号化されるオブジェクトを復号するために IAM ロールが実行することを許可される必要がある唯一の AWS KMS アクションです。

ロール所有者が AWS Command Line Interface (AWS CLI) を使用している場合は、create-grant コマンドを実行して許可を作成できます。以下の例のように指定します。この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/IAMRoleName ^
--operations "Decrypt"
```

実行する条件は以下のとおりです。

- `key-id` は、付与を適用する KMS キーの ARN を指定します。
- `grantee-principal` は、許可によって指定されたアクションの実行を許可された IAM ロールの ARN を指定します。この値は、キーポリシーの `kms:GranteePrincipal` 条件によって指定された ARN と一致する必要があります。

- operations は、許可が、指定されたプリンシパルが実行することを許可するアクション (キーで暗号化される暗号文の復号) を指定します。

コマンドが正常に実行された場合は、以下のような出力が表示されます。

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

ここで、GrantToken は、作成された付与を表す、一意で、非シークレットで、可変長の base64 でエンコードされた文字列であり、GrantIdは、付与の一意の識別子です。

検出結果についての機密データのサンプルを取得して公開するように Amazon Macie を設定する

オプションで Amazon Macie を設定して使用し、Macie が個々の機密データ検出結果で報告する機密データのサンプルを取得して公開することができます。サンプルは、Macie が検出した機密データの性質を確認するのに役立ちます。また、影響を受ける Amazon Simple Storage Service (Amazon S3) オブジェクトとバケットの調査を調整するのにも役立ちます。アジアパシフィック (大阪) リージョンとイスラエル (テルアビブ) リージョンを除く、Macie が現在利用可能なすべての AWS リージョン で、機密データの取得と公開を行うことができます。

検出結果の機密データのサンプルを取得して公開すると、Macie は対応する機密データの検出結果のデータを使用して、影響を受ける S3 オブジェクト内の機密データの出現を見つけます。次に、Macie は該当オブジェクトからそれらの出現のサンプルを抽出します。Macie は、抽出したデータを指定した AWS Key Management ServiceAWS KMS キーで暗号化し、暗号化されたデータを一時的にキャッシュに保存し、結果にそのデータを結果として返します。Macie は、運用上の問題を解決するために一時的に追加の保存が必要になった場合を除き、抽出と暗号化の直後に、データをキャッシュから完全に削除します。

検出結果についての機密データのサンプルを取得して公開するには、まず Macie アカウントの設定を構成し、有効にする必要があります。また、アカウントのためにサポートリソースと許可を設定する必要があります。このセクションのトピックでは、機密データのサンプルを取得して公開するように Macie を設定し、アカウントの設定ステータスを管理するプロセスについて説明します。

トピック

- 開始する前に

- Amazon Macie の設定の構成と有効化
- Amazon Macie の設定の無効化

> **Tip**
>
> この機能へのアクセスを制御するために使用できる推奨事項とポリシーの例については、AWSセキュリティブログのAmazon Macie を使用して S3 バケット内の機密データをプレビューする方法ブログ投稿を参照してください。

開始する前に

検出結果についての機密データのサンプルを取得して公開するように Amazon Macie を設定する前に、必要なリソースと許可を確実に備えているようにするために次のタスクを完了します。

タスク

- ステップ 1: 機密データ検出の結果のリポジトリを設定する
- ステップ 2: 対象の S3 オブジェクトにアクセスする方法を決定する
- ステップ 3: AWS KMS key を設定する
- ステップ 4: 許可を確認する

機密データのサンプルを取得して公開するように Macie を既に設定しており、構成設定のみを変更したい場合、これらのタスクはオプションです。

ステップ 1: 機密データ検出の結果のリポジトリを設定する

検出結果の機密データのサンプルを取得して公開すると、Macie は対応する機密データの検出結果のデータを使用して、影響を受ける S3 オブジェクト内の機密データの出現を見つけます。そのため、機密データ検出の結果用のリポジトリを設定していることを確認することが重要です。そうしないと、Macie は、取得して公開したい機密データのサンプルを見つけることができません。

アカウントのためにこのリポジトリを設定済みであるかどうかを確認するには、Amazon Macie コンソールを使用します。ナビゲーションペインで [検出の結果] ([設定] の下にあります) を選択します。Amazon Macie APIの GetClassificationExportConfiguration オペレーションを使用して、プログラムでこのデータにアクセスすることもできます。機密データ検出の結果とこのリポジトリの設定方法の詳細については、「機密データ検出結果の保存と保持」を参照してください。

ステップ 2: 対象の S3 オブジェクトにアクセスする方法を決定する

対象の S3 オブジェクトにアクセスし、そこから機密データのサンプルを取得するには、2 つのオプションがあります。AWS Identity and Access Management (IAM) ユーザー認証情報を使用するように Macie を設定できます。あるいは、Macie にアクセスを委任する IAM ロールを引き受けるように Macie を設定することもできます。いずれの設定も、組織のために委任された Macie 管理者アカウント、組織内の Macie メンバーアカウント、スタンドアロン Macie アカウントなど、あらゆるタイプの Macie アカウントで使用できます。Macie で設定を構成する前に、使用するアクセスメソッドを決定します。各メソッドのオプションと要件の詳細については、「検出結果についての機密データのサンプルを取得するための設定オプションと要件」を参照してください。

IAM ロールを使用する予定がある場合は、Macie で設定を構成する前にロールを作成して設定します。また、ロールの信頼ポリシーと許可ポリシーが、Macie がロールを引き受けるためのすべての要件を満たしているようにしてください。アカウントが複数の Macie アカウントを一元的に管理する組織に属している場合は、まず Macie 管理者と協力して、アカウントのためにロールを設定するかどうか、またその設定方法を決定します。

ステップ 3: AWS KMS key を設定する

検出結果についての機密データのサンプルを取得して公開すると、Macie は、指定された AWS Key Management Service (AWS KMS) キーを使用してサンプルを暗号化します。そのため、サンプルを暗号化するために使用する AWS KMS key を決定する必要があります。キーは、自分のアカウントの既存の KMS キーでも、別のアカウントが所有する既存の KMS キーでもかまいません。別のアカウントが所有するキーを使用する場合、キーの Amazon リソースネーム (ARN) を取得します。Macie で設定設定を入力するときに、この ARN を指定する必要があります。

KMS キーは、カスタマーマネージドキーで、対称暗号化キーである必要があります。また、Macie アカウントと同じ AWS リージョン で有効になっている単一リージョンのキーである必要があります。KMS キーは、外部キーストアに格納できます。ただし、そのキーは、完全に AWS KMS 内で管理されるキーよりも遅く、信頼性が低くなる可能性があります。レイテンシーまたは可用性の問題により、取得して公開したい機密データサンプルを Macie が暗号化できない場合、エラーが発生し、Macie は検出結果のサンプルを返しません。

さらに、キーのキーポリシーでは、適切なプリンシパル (IAM ロール、IAM ユーザー、または AWS アカウント) が次のアクションを実行できるようにする必要があります。

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

> **Important**
>
> アクセスコントロールをさらに強化するために、取得する機密データサンプルを暗号化するための専用の KMS キーを作成し、そのキーの使用を、機密データサンプルの取得と開示を許可する必要があるプリンシパルのみに制限することをお勧めします。ユーザーがキーのために前述のアクションを実行することを許可されていない場合、Macie は、機密データのサンプルを取得して公開するという当該ユーザーのリクエストを拒否します。Macie は、検出結果についてのサンプルを返しません。

KMS キーの作成と設定については、「AWS Key Management Service デベロッパーガイド」の「キーの管理」を参照してください。KMS キーに対するアクセスを管理するためのキーポリシーの使用については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS のキーポリシー」を参照してください。

ステップ 4: 許可を確認する

Macie で設定を構成する前に、必要な許可が付与されていることも確認してください。アクセス許可を確認するには、AWS Identity and Access Management (IAM) を使用して IAM ID に添付されている IAM ポリシーを確認してください。次にこれらのポリシー内の情報を、実行が許可される必要がある次のアクションのリストと比較します。

Amazon Macie

Macie の場合、次のアクションの実行が許可されていることを確認します。

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

1 つ目のアクションでは、Macie アカウントにアクセスできます。2 つ目のアクションでは、機密データのサンプルを取得して公開するための設定を変更できます。これには、アカウントの設定の有効化と無効化が含まれます。

オプションで、`macie2:GetRevealConfiguration` アクションの実行も許可されていることを確認します。このアクションにより、アカウントの現在の設定設定と設定の現在の状態を取得できます。

AWS KMS

Amazon Macie コンソールを使用して設定を入力する予定がある場合は、次の AWS Key Management Service (AWS KMS) アクションを実行できることも確認してください。

- `kms:DescribeKey`
- `kms:ListAliases`

これらのアクションにより、アカウントの AWS KMS keys に関する情報を取得できます。その後、設定を入力するときに、これらのキーのいずれかを選択できます。

IAM

機密データのサンプルを取得して公開するための IAM ロールを引き受けるように Macie を設定する予定がある場合は、次の IAM アクションの実行が許可されていることも確認してください: `iam:PassRole`。このアクションにより、ロールを Macie に渡すことができ、Macie がそのロールを引き受けることができるようになります。アカウントのために構成設定を入力すると、Macie はそのロールがアカウントに存在し、正しく設定されていることを検証することもできます。

必要なアクションの実行が許可されていない場合は、AWS 管理者にサポートを依頼してください。

Amazon Macie の設定の構成と有効化

必要なリソースと許可があることを確認したら、Amazon Macie で設定を構成し、アカウントのために設定を有効にすることができます。

アカウントが複数の Macie アカウントを一元的に管理する組織に属している場合は、アカウントのために設定を構成する前、または後にその設定を変更する前に、次の点に留意してください。

- メンバーアカウントがある場合は、Macie の管理者と協力して、アカウントのために設定を構成するかどうか、およびその方法を決定します。Macie の管理者は、アカウントのために正しい構成設定を決定するのをサポートできます。
- Macie の管理者アカウントがあり、対象の S3 オブジェクトにアクセスするための設定を変更すると、その変更によって、組織の他のアカウントやリソースに影響が及ぶ可能性があります。これは、Macie が機密データのサンプルを取得する AWS Identity and Access Management (IAM) ロールを引き受けるように現在設定されているかどうかによって異なります。そのように設定されており、IAM ユーザー認証情報を使用するように Macie を再設定すると、Macie は IAM ロールの既存の設定 (ロールの名前と設定の外部 ID) を完全に削除します。その後、組織が IAM ロールを再度使用することを選択した場合は、該当の各メンバーアカウントのロールの信頼ポリシーで新しい外部 ID を指定する必要があります。

各タイプのアカウントの設定オプションの詳細については、「検出結果についての機密データのサンプルを取得するための設定オプションと要件」を参照してください。

Macie で設定を構成し、アカウント用に設定を有効にするために、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用して設定を構成し、有効にするには、次のステップに従います。

Macie 設定を構成して有効にするには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上にある AWS リージョン セレクターを使用して、機密データのサンプルを取得したり、公開したりするように Macie を設定して有効にするリージョンを選択します。
3. ナビゲーションペインの 設定 で、イベントの流れ を選択します。
4. 設定 セクションで、編集 を選択します。
5. ステータス で、有効 を選択します。
6. [アクセス] で、対象の S3 オブジェクトから機密データのサンプルを取得する際に使用するアクセスメソッドと設定を指定します。

   - Macie にアクセスを委任する IAM ロールを使用するには、[IAM ロールを引き受ける] を選択します。このオプションを選択すると、Macie は、AWS アカウント で作成および設定した IAM ロールを引き受けてサンプルを取得します。[ロール名] ボックスで、ロールの名前を入力します。
   - サンプルをリクエストする IAM ユーザーの認証情報を使用するには、[IAM ユーザー認証情報を使用] を選択します。このオプションを選択した場合、アカウントの各ユーザーは、個別の IAM ID を使用してサンプルを取得します。
7. [暗号化] で、取得される機密データのサンプルを暗号化するために使用する AWS KMS key を指定します。

   - 自分のアカウントに KMS キーを使用するには、[アカウントからキーを選択] を選択します。そして、AWS KMS key リストからユーザー名を選択します。リストには、アカウントの既存の対称暗号化 KMS キーが表示されます。
   - 別のアカウントが所有し、使用が許可されている KMS キーを使用するには、[別のアカウントのキーの ARN を入力] を選択します。次に、AWS KMS key ARN ボックスに、使用するキーの Amazon リソースネーム (ARN) を入力します。例えば、**`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**
8. 設定の入力が完了したら、Save (保存) を選択します。

Macie は設定をテストして、それらが正しいことを検証します。Macie が IAM ロールを引き受けるように設定した場合、Macie は、そのロールがアカウントに存在し、信頼ポリシーと許可ポリシーが正しく設定されていることも検証します。問題がある場合、Macie は、問題を説明するメッセージを表示します。

AWS KMS key の問題に対処するには、前述のトピックの要件を参照し、要件を満たす KMS キーを指定します。IAM ロールの問題に対処するには、まず、正しいロール名を入力したことを確認します。名前が正しい場合は、Macie がそのロールを引き受けるためのすべての要件を、そのロールのポリシーが満たしていることを確認します。これらの詳細については、「対象の S3 オブジェクトにアクセスするための IAM ロールの設定」を参照してください。問題に対処したら、設定を保存して有効にすることができます。

> **Note**
>
> 自分が組織の Macie の管理者で、IAM ロールを引き受けるように Macie を設定した場合、アカウントのための設定を保存した後、Macie は外部 ID を生成して表示します。この ID を書き留めます。該当の各メンバーアカウントの IAM ロールの信頼ポリシーでは、この ID が指定される必要があります。指定されていない場合、アカウントが所有する S3 オブジェクトから機密データのサンプルを取得できません。

API

設定をプログラムで構成して、有効にするには、Amazon Macie API の UpdateRevealConfiguration オペレーションを使用します。リクエストでは、サポートされているパラメータの適切な値を指定します。

- `retrievalConfiguration` パラメータで、対象の S3 オブジェクトから機密データのサンプルを取得する際に使用するアクセスメソッドと設定を指定します。
  - Macie にアクセスを委任する IAM ロールを引き受けるには、`retrievalMode` パラメータに `ASSUME_ROLE` を指定し、`roleName` パラメータにロールの名前を指定します。これらの設定を指定すると、Macie は、AWS アカウント で作成および設定した IAM ロールを引き受けてサンプルを取得します。
  - サンプルをリクエストする IAM ユーザーの認証情報を使用するには、`retrievalMode` パラメータに `CALLER_CREDENTIALS` を指定します。この設定を指定すると、アカウントの各ユーザーは、個別の IAM ID を使用してサンプルを取得します。

> **Important**
>
> これらのパラメータの値を指定しない場合、Macie はアクセスメソッド (`retrievalMode`) を `CALLER_CREDENTIALS` に設定します。また、Macie が現在 IAM ロールを使用してサンプルを取得するように設定されている場合、Macie は現在のロール名と設定の外部 ID を完全に削除します。既存の設定のためにこれらの設定を維持するには、リクエストに `retrievalConfiguration` パラメータを含めて、それらのパラメータのために現在の設定を指定します。現在の設定を取得するには、GetRevealConfiguration オペレーションを使用するか、または AWS Command Line Interface (AWS CLI) を使用している場合は get-reveal-configuration コマンドを使用します。

- `kmsKeyId` パラメータには、取得される機密データのサンプルを暗号化するために使用する AWS KMS key を指定します。
  - 自分のアカウントから KMS キーを使用するには、キーの Amazon リソースネーム (ARN)、ID、またはエイリアスを指定します。エイリアスを指定する場合は、`alias/` プレフィックスを含めてください。例えば、`alias/ExampleAlias`
  - 別のアカウントが所有する KMS キーを使用するには、キーの ARN を指定します。例えば、`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`または、キーのエイリアスの ARN を指定します。例えば、`arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`
- `status` パラメータには、Macie `ENABLED` アカウントの設定を有効にするように指定します。

また、リクエストでは、設定を有効にして使用する AWS リージョン を必ず指定してください。

AWS CLI を使用して設定を構成し、有効にするには、update-reveal-configuration コマンドを実行し、サポートされているパラメータに適切な値を指定します。例えば、Microsoft Windows で AWS CLI を使用する場合は、次のコマンドを実行します:

```
C:\> aws macie2 update-reveal-configuration ^
--region us-east-1 ^
--configuration={\"kmsKeyId\":\"arn:aws:kms:us-east-1:111122223333:alias/
ExampleAlias\",\"status\":\"ENABLED\"} ^
--retrievalConfiguration={\"retrievalMode\":\"ASSUME_ROLE\",\"roleName\":
\"MacieRevealRole\"}
```

実行する条件は以下のとおりです。

- *us-east-1* は、設定を有効にして使用するリージョンです。この例では、米国東部 (バージニア北部) リージョンです。
- *arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias* は、使用する AWS KMS key のエイリアスの ARN です。この例では、キーは別のアカウントが所有しています。
- 設定のステータスは ENABLED です。
- *ASSUME_ROLE* は、使用するアクセスメソッドです。この例では、指定された IAM ロールを引き受けます。
- *MacieRevealRole* は、機密データのサンプルを取得する際に Macie が引き受ける IAM ロールの名前です。

前述の例は、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

リクエストを送信すると、Macie は設定をテストします。Macie が IAM ロールを引き受けるように設定した場合、Macie は、そのロールがアカウントに存在し、信頼ポリシーと許可ポリシーが正しく設定されていることも検証します。問題がある場合、リクエストは失敗し、Macie は問題を説明するメッセージを返します。AWS KMS key の問題に対処するには、前述のトピックの要件を参照し、要件を満たす KMS キーを指定します。IAM ロールの問題に対処するには、まず、正しいロール名を指定したことを確認します。名前が正しい場合は、Macie がそのロールを引き受けるためのすべての要件を、そのロールのポリシーが満たしていることを確認します。これらの詳細については、「対象の S3 オブジェクトにアクセスするための IAM ロールの設定」を参照してください。問題に対処した後、リクエストを再度送信します。

リクエストが成功すると、Macie は指定されたリージョンのアカウント設定を有効にし、次のような出力を受け取ります。

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

ここで、kmsKeyId は、取得される機密データのサンプルの暗号化に使用する AWS KMS key を指定し、status は Macie アカウントの設定のステータスを指定します。retrievalConfiguration の値は、サンプルを取得する際に使用するアクセスメソッドと設定を指定します。

> **Note**
>
> 自分が組織の Macie の管理者で、Macie が IAM ロールを引き受けるように設定した場合は、応答内の外部 ID (externalId) を書き留めます。該当の各メンバーアカウントの IAM ロールの信頼ポリシーでは、この ID が指定される必要があります。指定されていない場合、アカウントが所有する対象の S3 オブジェクトから機密データのサンプルを取得できません。

アカウントの設定や設定の状態を後で確認するには、GetRevealConfigurationオペレーションを使用するか、AWS CLI の場合はget-reveal-configurationコマンドを実行します。

Amazon Macie の設定の無効化

Amazon Macie アカウントの構成設定はいつでも無効にできます。設定を無効にしても、Macie は、取得した機密データのサンプルの暗号化に使用する AWS KMS key を指定する設定を保持します。Macie は、構成についての Amazon S3 のアクセス設定を完全に削除します。

> **Warning**
>
> Macie アカウントのために構成設定を無効にすると、対象の S3 オブジェクトに対するアクセスメソッドを指定する現在の設定も完全に削除されます。Macie が現在 AWS Identity and Access Management (IAM) ロールを引き受けることによって、対象のオブジェクトにアクセスするように設定されている場合、これには、ロールの名前と、Macie が設定用に生成した外部 ID が含まれます。これらの設定は、削除後は復元できません。

Macie アカウントのために構成設定を無効にするには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用して、アカウントのために構成設定を無効にするには、次のステップに従います。

Macie の設定を無効にするには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上にある AWS リージョン セレクターを使用して、Macie アカウントのために構成設定を無効にするリージョンを選択します。
3. ナビゲーションペインの 設定 で、イベントの流れ を選択します。
4. 設定 セクションで、編集 を選択します。
5. [ステータス] で、[無効] を選択します。
6. [Save (保存)] を選択します。

API

構成設定をプログラムで無効にするには、Amazon Macie API の UpdateRevealConfiguration オペレーションを使用します。リクエストでは、設定を無効にする AWS リージョン を必ず指定してください。`status` パラメータでは、`DISABLED` を指定します。

AWS Command Line Interface (AWS CLI) を使用して構成設定を無効にするには、update-reveal-configuration コマンドを実行します。設定を無効にするリージョンを指定するには `region` パラメータを使用します。`status` パラメータでは、`DISABLED` を指定します。例えば、Microsoft Windows で AWS CLI を使用する場合は、次のコマンドを実行します:

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --
configuration={\"status\":\"DISABLED\"}
```

実行する条件は以下のとおりです。

- *`us-east-1`* は、設定を無効にするリージョンです。この例では、米国東部 (バージニア北部) リージョンです。
- `DISABLED` は、設定の新しいステータスです。

リクエストが成功すると、Macie は指定されたリージョンのアカウント設定を無効にし、次のような出力を受け取ります。

```
{
    "configuration": {
        "status": "DISABLED"
```

```
    }
}
```

`status` は Macie アカウントの設定の新しいステータスです。

Macie が機密データのサンプルを取得する IAM ロールを引き受けるように設定されている場合は、オプションでロールとロールの許可ポリシーを削除できます。アカウントのために構成設定を無効にしても、Macie はこれらのリソースを削除しません。さらに、Macie は、これらのリソースを使用してアカウントの他のタスクを実行することはありません。ロールとその許可ポリシーを削除するために、IAM コンソールまたは IAM API を使用できます。詳細については、「AWS Identity and Access Management ユーザーガイド」の「ロールの削除」を参照してください。

検出結果についての機密データのサンプルの取得と公開

Amazon Macie を使用すると、Macie が個々の機密データの検出結果で報告する機密データのサンプルを取得して公開できます。これには、Macie が マネージドデータ識別子 を使用して検出した機密データ、および使用するジョブを設定している任意の カスタムデータ識別子 の基準に一致するデータが含まれます。サンプルは、Macie が検出した機密データの性質を確認するのに役立ちます。また、影響を受ける Amazon Simple Storage Service (Amazon S3) オブジェクトとバケットの調査を調整するのにも役立ちます。アジアパシフィック (大阪) とイスラエル (テルアビブ) リージョンを除き、Macie が現在利用可能なすべての地域で機密データサンプルを取得して公開できます。 AWS リージョン

調査結果の機密データサンプルを取得して公開すると、Macie は対応する機密データ検出結果のデータを使用して、調査結果によって報告された機密データのうち、最初の 1 ~ 10 件を特定します。次に、Macie は該当する S3 オブジェクトから各出現の最初の 1 ~ 128 文字を抽出します。検出結果から複数のタイプの機密データが報告された場合、Macie はその結果によって報告された最大 100 タイプの機密データに対して抽出を行います。

Macie が影響を受ける S3 オブジェクトから機密データを抽出すると、Macie は指定した AWS Key Management Service (AWS KMS) キーでデータを暗号化し、暗号化されたデータを一時的にキャッシュに保存し、検出結果のデータを結果に返します。Macie は、運用上の問題を解決するために一時的に追加の保存が必要になった場合を除き、抽出と暗号化の直後に、データをキャッシュから完全に削除します。

機密データのサンプルを再度取得して公開することを選択した場合、Macie はサンプルの検索、抽出、暗号化、保存、そして最終的には削除のプロセスを繰り返します。

Amazon Macie コンソールを使用して機密データサンプルを取得して公開する方法のデモンストレーションについては、次のビデオをご覧ください。Amazon Macie による機密データサンプルの取得と表示。

トピック

- 開始する前に
- 検出結果についての機密データのサンプルが使用できるかどうかの判断
- 検出結果についての機密データのサンプルの取得と公開

開始する前に

検出結果についての機密データのサンプルを取得して公開する前に、Amazon Macie アカウントの設定を構成し、有効にする必要があります。また、 AWS 管理者と協力して、必要な権限とリソースがあることを確認する必要があります。

検出結果についての機密データのサンプルを取得して公開すると、Macie は、サンプルを検索、取得、暗号化、公開する一連のタスクを実行します。Macie はこれらのタスクを実行するのに、アカウントの Macie サービスにリンクされたロールを使用しません。代わりに、 AWS Identity and Access Management (IAM) ID を使用するか、Macie にアカウント内の IAM ロールを引き受けることを許可してください。

検出結果の機密データサンプルを取得して公開するには、検出結果、対応する機密データ検出結果、および機密データサンプルの暗号化に使用する Macie AWS KMS key を設定した情報にアクセスできる必要があります。さらに、ユーザーまたは IAM ロールは、対象の S3 バケットおよび対象の S3 オブジェクトにアクセスすることが許可されている必要があります。該当する場合は、該当オブジェクトの暗号化に使用されたものの使用を、 AWS KMS key ユーザーまたはロールが許可されている必要もあります。IAM ポリシー、リソースポリシー、または他の許可の設定によって必要なアクセスが拒否された場合、エラーが発生し、Macie は検出結果についてのサンプルを返しません。

また、次の Macie アクションの実行が許可される必要があります。

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

最初の 3 つのアクションでは、Macie アカウントにアクセスして検出結果の詳細を取得できます。最後のアクションでは、検出結果についての機密データのサンプルを取得して公開できます。

Amazon Macie コンソールを使用して機密データのサンプルを取得して公開するには、次のアクションの実行も許可されている必要があります: `macie2:GetSensitiveDataOccurrencesAvailability`。このアクションにより、個々の検出結果にサンプルがあるかどうかを判断できます。このアクションを実行しても、サンプルをプログラムで取得して公開するアクセス許可は必要ありません。ただし、このアクセス許可があると、サンプルの検索を効率化できます。

自分が組織の委任された Macie の管理者であり、機密データのサンプルを取得するための IAM ロールを引き受けるように Macie を設定した場合は、次のアクションの実行も許可されている必要があります: `macie2:GetMember`。このアクションにより、自分のアカウントと対象のアカウントとの関連付けに関する情報を取得できます。これにより、対象のアカウントについてユーザーが現在 Macie の管理者であることを Macie が検証できます。

必要なアクションを実行したり、必要なデータやリソースにアクセスしたりすることが許可されていない場合は、 AWS 管理者に支援を依頼してください。

検出結果についての機密データのサンプルが使用できるかどうかの判断

検出結果に必要な機密データのサンプルを取得して明らかにするためには、その検出結果が一定の基準を満たす必要があります。特定の機密データが見つかった場合の位置データを含める必要があります。さらに、対応する有効な機密データ検出結果の場所を指定する必要があります。機密データの検出結果は、 AWS リージョン 検出結果と同じ場所に保存する必要があります。 AWS Identity and Access Management (IAM) ロールを引き受け、影響を受ける S3 オブジェクトにアクセスするように Amazon Macie を設定した場合、機密データの検出結果は、Macie がハッシュベースのメッセージ認証コード (HMAC) で署名した S3 オブジェクトにも保存する必要があります。 AWS KMS key

影響を受ける S3 オブジェクトも一定の基準を満たす必要があります。オブジェクトの MIME タイプは、次のいずれかである必要があります。

- application/avro は、Apache Avro オブジェクトコンテナ (.avro) ファイルの場合
- application/gzip は、GNU Zip 圧縮アーカイブ (.gz または.gzip) ファイルの場合
- application/json、JSON または JSON ライン (.json または.jsonl) ファイルの場合
- application/parquet、Apache Parquet (.parquet) ファイル
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet、Microsoft Excel ワークブック (.xlsx) ファイルのサイズ

- application/zip は、ZIP 圧縮アーカイブファイル (.zip) の場合
- text/csv 、CSV (.csv) ファイルの場合
- text/plain 、CSV、JSON、JSON ライン、または TSV ファイル以外の非バイナリテキストファイルの場合
- text/tab-separated-values 、TSV (.tsv) ファイルの場合

さらに、S3 オブジェクトの内容は検出結果が作成されたときと同じである必要があります。Macie はオブジェクトのエンティティタグ (ETag) をチェックして、検出結果で指定された ETag と一致するかどうかを判断します。また、オブジェクトのストレージサイズは、機密データサンプルの取得と公開に適用されるサイズクォータを超えることはできません。適用可能なクォータのリストについては、Amazon Macie クォータを参照してください。

結果と影響を受ける S3 オブジェクトが前述の基準を満たす場合は、その検出結果に機密データのサンプルを使用できます。検出結果のサンプルを取得して公開する前に、特定の検出結果に当てはまるかどうかを任意で判断できます。

センシティブデータのサンプルが検出結果に利用できるかどうかを判断するには

Amazon Macie コンソールまたは Amazon Macie API を使用して、機密データのサンプルが検出結果に使用できるかどうかを判断できます。

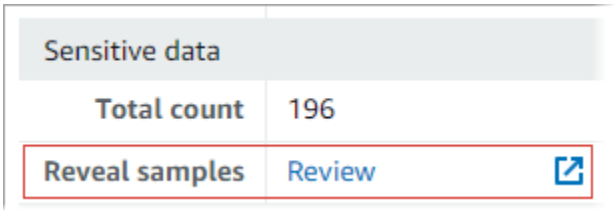
Console

Amazon Macie コンソールの次の手順に従って、機密データのサンプルが検出結果に利用できるかどうかを判断します。

検出結果にサンプルが使用できるかどうかを判断するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果 を選択します。
3. GuardDuty の 検出結果 のページで、検出結果を選択します。詳細パネルに、調査結果の情報が表示されます。
4. 詳細パネルで、詳細 セクションにスクロールします。次に、サンプルを公開 フィールドを参照してください。

   検出結果に機密データのサンプルがある場合は、次の図に示すように レビュー リンクがフィールドに表示されます。



検出結果に用いる機密データサンプルがない場合、サンプルを公開 フィールドには理由を示すテキストが表示されます。

- [アカウントが組織に含まれていません] – Macie を使用して、対象の S3 オブジェクトにアクセスすることは許可されていません。対象のアカウントは現在、組織に属していません。あるいは、アカウントは組織に属していますが、現在の AWS リージョンのアカウントのために Macie が有効になっていません。
- [分類の結果が無効です] – 検出結果についての機密データ検出の結果はありません。または、対応する機密データ検出結果が現在 AWS リージョンのデータにはない、形式に誤りがある、破損している、またはサポートされていない保存形式が使用されています。Macie は、取得する機密データの場所を検証できません。
- [結果の署名が無効です] – 対応する機密データ検出の結果は、Macie によって署名されていない S3 オブジェクトに保存されています。Macie は、機密データ検出の結果の完全性と信頼性を検証できません。そのため、Macie は取得する機密データの場所を検証できません。
- [メンバーロールの許可範囲が広すぎます] - 対象のメンバーアカウントの IAM ロールの信頼または許可ポリシーが、ロールに対するアクセスの制限に関する Macie の要件を満たしていません。あるいは、ロールの信頼ポリシーで組織の正しい外部 ID が指定されていません。Macie は、機密データを取得するためのロールを引き受けることができません。
- GetMember 権限がない — 自分のアカウントと影響を受けるアカウントとの関連付けに関する情報を取得することはできません。Macie は、対象のアカウントについての委任された Macie の管理者として、対象の S3 オブジェクトにアクセスすることが許可されているかどうかを判断できません。
- [オブジェクトがサイズクォータを超えています] – 対象の S3 オブジェクトのストレージサイズが、そのタイプのファイルから機密データのサンプルを取得して公開するためのサイズクォータを超えています。
- [オブジェクトを使用できません] – 対象の S3 オブジェクトは使用できません。Macie が検出結果を作成した後に、オブジェクトの名前が変更されたり、移動されたり、削除されたり、その内容が変更されたりしました。あるいは、オブジェクトは現在無効になっている AWS KMS key で暗号化されています。

- [結果が署名されていません] – 対応する機密データ検出の結果は、署名されていない S3 オブジェクトに保存されています。Macie は、機密データ検出の結果の完全性と信頼性を検証できません。そのため、Macie は取得する機密データの場所を検証できません。
- [ロールの許可範囲が広すぎます] - アカウントは、ロールに対するアクセスの制限に関する Macie 要件を満たしていない信頼または許可ポリシーを持つ IAM ロールを使用して、機密データの出現を取得するように設定されています。Macie は、機密データを取得するためのロールを引き受けることができません。
- [サポートされていないオブジェクトタイプ] – 対象の S3 オブジェクトは、Macie が機密データのサンプルの取得と公開をサポートしていないファイルまたはストレージ形式を使用しています。対象の S3 オブジェクトの MIME タイプが前述のリストの値に含まれていません。

検出結果についての機密データ検出の結果に問題がある場合は、検出結果の [詳細な結果の場所] フィールドの情報が問題の調査に役立ちます。このフィールドは、Amazon S3 の結果への元のパスを指定します。IAM ロールの問題を調査するには、Macie がロールを引き受けるためのすべての要件を、ロールのポリシーが満たしているようにしてください。これらの詳細については、「対象の S3 オブジェクトにアクセスするための IAM ロールの設定」を参照してください。

API

機密データのサンプルが検索に使用できるかどうかをプログラムで判断するには、Amazon Macie API GetSensitiveDataOccurrencesAvailabilityのオペレーションを使用します。リクエストを送信するときは、`findingId` パラメータを使用して、検出結果の一意の識別子を指定します。この ID を取得するには、オペレーションを使用できます。ListFindings

AWS Command Line Interface (AWS CLI) を使用している場合は、get-sensitive-data-occurrences-availabilityコマンドを実行し、`finding-id`パラメーターを使用して結果の一意の識別子を指定します。この識別子を取得するには、list-findingsコマンドを実行します。

リクエストが成功し、検出結果のサンプルが入手された場合は、お客様は次のような出力を受け取ります。

```
{
    "code": "AVAILABLE",
    "reasons": []
}
```

リクエストが成功しても結果にサンプルがない場合、code フィールドの値は UNAVAILABLE で、reasons 配列には理由が示されます。例:

```
{
    "code": "UNAVAILABLE",
    "reasons": [
        "UNSUPPORTED_OBJECT_TYPE"
    ]
}
```

検出結果についての機密データ検出の結果に問題がある場合は、検出結果の [classificationDetails.detailedResultsLocation] フィールドの情報が問題の調査に役立ちます。このフィールドは、Amazon S3 の結果への元のパスを指定します。IAM ロールの問題を調査するには、Macie がロールを引き受けるためのすべての要件を、ロールのポリシーが満たしているようにしてください。これらの詳細については、「対象の S3 オブジェクトにアクセスするための IAM ロールの設定」を参照してください。

検出結果についての機密データのサンプルの取得と公開

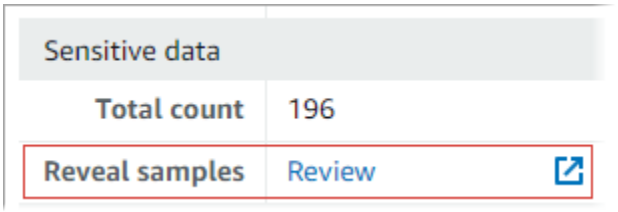
検出結果に含まれる機密データのサンプルを取得して公開するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用して、検出結果の機密データのサンプルを取得して表示するには、次のステップに従います。

検出結果の機密データサンプルを取得して公開するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果 を選択します。
3. GuardDuty の 検出結果 のページで、検出結果を選択します。詳細パネルに、調査結果の情報が表示されます。
4. 詳細パネルで、詳細 セクションにスクロールします。次に、サンプルを公開 フィールドで 確認 を選択します。

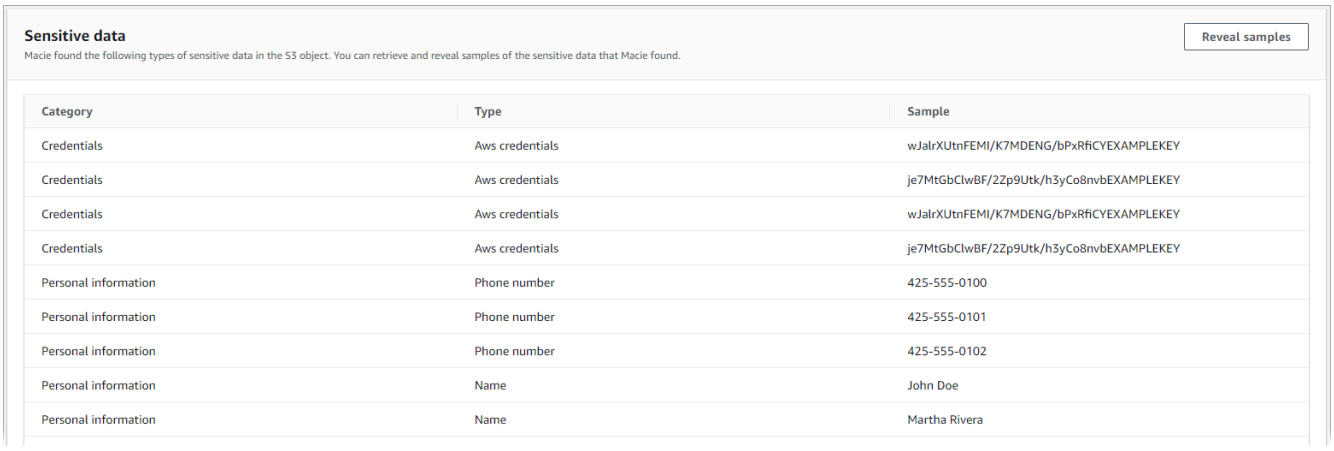


> **Note**
>
> サンプルを公開 フィールドに 確認 リンクが表示されない場合、機密データのサンプルは結果に使用できません。これに関する詳細については、前のセクション を参照してください。

レビュー を選択すると、Macie は検出結果の主要な詳細を要約したページを表示します。詳細には、Macie が影響を受けた S3 オブジェクトで見つけた機密データのカテゴリ、タイプ、出現の数が含まれます。

5. ページの 機密データ セクションで、サンプルを公開 を選択します。その後、Macie は、検出結果によって報告された機密データのうち、最初の 1～10 件の機密データの出現のサンプルを取得して公開します。各サンプルには、機密データの最初の 1 ～ 128 文字が含まれます。サンプルを取得して公開するまでに数分かかる場合があります。

   結果から複数のタイプの機密データが報告された場合、Macie は最大 100 タイプのサンプルを取得して表示します。たとえば、以下の画像は、AWS 認証情報、米国の電話番号、個人の名前など、複数のカテゴリと種類の機密データを対象としたサンプルを示しています。



   サンプルは最初にセンシティブデータカテゴリ別に整理され、次にセンシティブデータタイプ別に整理されています。

API

検出結果の機密データサンプルをプログラムで取得して表示するには、Amazon Macie GetSensitiveDataOccurrencesAPI のオペレーションを使用します。リクエストを送信するときは、findingId パラメータを使用して、検出結果の一意の識別子を指定します。この ID を取得するには、オペレーションを使用できます。ListFindings

AWS Command Line Interface (AWS CLI) を使用して機密データサンプルを取得して表示するには、get-sensitive-data-occurrencesコマンドを実行し、finding-idパラメーターを使用して検出結果の一意の識別子を指定します。例:

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
 "1f1c2d74db5d8caa76859ec52example"
```

ここで、*1f1c2d74db5d8caa76859ec52example* は検出結果を表す一意の識別子です。を使用してこの ID を取得するには AWS CLI、list-findings コマンドを実行します。

リクエストが成功すると、Macie がリクエストの処理を開始し、お客様は次のような出力を受け取ります。

```
{
    "status": "PROCESSING"
}
```

がスタックを作成するのに、数分かかります。数分以内にリクエストを再度送信してください。

Macie が機密データサンプルを検索、取得、暗号化できる場合、Macie はサンプルを sensitiveDataOccurrences マップに返します。マップには、検出結果によって報告された機密データが 1 ~ 100 タイプ指定され、タイプごとに 1 ~ 10 個のサンプルが指定されています。各サンプルには、検出結果によって報告された機密データの最初の 1 ~ 128 文字が含まれています。

マップ内の各キーは、機密データを検出したマネージドデータ識別子の ID、または機密データを検出したカスタムデータ識別子の名前と一意の識別子です。値は、指定されたマネージドデータ識別子またはカスタムデータ識別子のサンプルです。たとえば、次のレスポンスでは、マネージドデータ識別子によって検出されたユーザー名のサンプルが 3 つAWS_CREDENTIALS、 AWS シークレットアクセスキーのサンプルが 2 つ (NAMEそれぞれ) 返されます。

```
{
```

```
    "sensitiveDataOccurrences": {
        "NAME": [
            {
                "value": "Akua Mansa"
            },
            {
                "value": "John Doe"
            },
            {
                "value": "Martha Rivera"
            }
        ],
        "AWS_CREDENTIALS": [
            {
                "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
            },
            {
                "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
            }
        ]
    },
    "status": "SUCCESS"
}
```


リクエストが成功しても、その検出結果に含まれる機密データのサンプルが見つからない場合は、サンプルが入手できない理由を示す UnprocessableEntityException メッセージが表示されます。例:


```
{
    "message": "An error occurred (UnprocessableEntityException) when calling the
 GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```


前述の例では、Macie は対象の S3 オブジェクトからサンプルを取得しようとしましたが、そのオブジェクトは使用不可になっています。Macie が検出結果を作成した後でオブジェクトの内容が変更されたこともあります。

リクエストが成功しても、別のタイプのエラーで、Macie が検出結果の機密データのサンプルを取得して表示できなかった場合は、お客様は次のような出力が表示されます。


```
{
```

```
    "error": "Macie can't retrieve the samples. You're not allowed to access the
 affected S3 object or the object is encrypted with a key that you're not allowed to
 use.",
    "status": "ERROR"
}
```

ERROR フィールドの値はで、status と error フィールドには発生したエラーが説明されています。前述のトピックの情報は、エラーを調査するのに役立ちます。

機密データの場所の JSON スキーマ

Amazon Macie は、標準化された JSON 構造を使用して、Amazon Simple Storage Service (Amazon S3) オブジェクト内の機密データを検出した場所に関する情報を保存します。その構造は、機密データの検出結果で使用されます。機密データの検出結果では、構造は検出結果の JSON スキーマの一部です。検出結果の完全な JSON スキーマを確認するには、Amazon Macie API リファレンスの検出結果を参照してください。機密データの検出結果の詳細については、機密データ検出結果の保存と保持を参照してください。

トピック

- 機密データの場所の JSON スキーマ概要
- 機密データの場所に関する JSON スキーマの詳細と例

機密データの場所の JSON スキーマ概要

Amazon Macie が対象の S3 オブジェクト内で検出した機密データの場所を報告するために、機密データ検出結果の JSON スキーマには 1 つの customDataIdentifiers オブジェクトと 1 つの sensitiveData オブジェクトが含まれます。customDataIdentifiers オブジェクトは、Macie が カスタムデータ識別子を使用して検出したデータの詳細を提供します。sensitiveData オブジェクトは、Macie がマネージドデータ識別子を使用して検出した機密データの詳細を提供します。

それぞれの customDataIdentifiers と sensitiveData オブジェクトには、1 つ以上の detections 配列が含まれます。

- customDataIdentifiers オブジェクトでは、detections 配列は、データを検出して結果を生成したカスタムデータ識別子を示します。各カスタムデータ識別子について、配列は識別子が検出したデータの出現の数も示します。また、識別子が検出したデータの場所を示すこともできます。

- sensitiveData オブジェクトでは、detections 配列 は、Macie がマネージドデータ識別子を使用して検出した機密データのタイプを示します。機密データのタイプごとに、配列はデータの出現の数も示し、またデータの場所を示すことができます。

機密データの調査結果では、detections 配列には 1～15 個の occurrences オブジェクトを含めることができます。それぞれの occurrences オブジェクトは、Macie が特定のタイプの機密データの個別の出現を検出した場所を指定します。

例えば、次の detections 配列は、Macie が CSV ファイルで機密データ (米国社会保障番号) の 3 箇所の出現場所を示します。

```
"sensitiveData": [
     {
       "category": "PERSONAL_INFORMATION",
       "detections": [
          {
             "count": 30,
             "occurrences": {
                "cells": [
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 2
                   },
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 3
                   },
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 4
                   }
                ]
             },
             "type": "USA_SOCIAL_SECURITY_NUMBER"
          }
```

detections 配列内の occurrences オブジェクトの場所と数は、機密データ自動検出の分析サイクルまたは機密データ検出ジョブの実行中に Macie が検出する機密データのカテゴリ、タイプ、および発生数によって異なります。分析サイクルまたはジョブ実行のたびに、Macie は深さ優先検索アルゴリズムを使用して、S3 オブジェクト内で検出した出現 1 ~ 15 件の機密データの位置データを検出結果に取り込みます。これらの出現は、影響を受ける S3 バケットおよびオブジェクトに含まれる機密データのカテゴリとタイプを示すものです。

occurrences オブジェクトには、影響を受ける S3 オブジェクトのファイルタイプまたはストレージ形式に応じて、次の構造を含めることができます。

- cells 配列 — この配列は Microsoft Excel ワークブック、CSV ファイル、および TSV ファイルに適用されます。この配列内のオブジェクトは、Macie が機密データの出現を検出したセルまたはフィールドを指定します。
- lineRanges 配列 — この配列は、Eメールメッセージ (EML) ファイル、非バイナリテキストファイル (CSV、JSON、JSON Lines、TSV ファイル以外 — 例えば HTML、TXT、XML ファイルなど) に適用されます。この配列内のオブジェクトは、Macie が機密データの出現を検出した 1 つの行または包括的な範囲、および指定された行 (1 つまたは複数) のデータの位置を指定します。

  場合によっては、lineRanges 配列内のオブジェクトは、別のタイプの配列でサポートされているファイルタイプまたはストレージ形式で、機密データ検出の場所を指定します。そのような場合とは、ファイル内のコメントなど、構造化されたファイルの非構造化セクションでの検出、Macie がプレーンテキストとして分析する不正な形式のファイルの検出、Macie が機密データを検出した 1 つ以上の列名を持つ CSV または TSV ファイルなどです。
- offsetRanges 配列 – この配列は、将来の利用のために予約されています。この配列が存在する場合、その配列の値は null です。
- pages 配列 — この配列は Adobe Portable Document Format (PDF) ファイルに適用されます。この配列内のオブジェクトは、Macie が機密データの出現を検出したページを指定します。
- records 配列 — この配列は Apache Avro オブジェクトコンテナ、Apache Parquet ファイル、JSON ファイル、および JSON Lines ファイルに適用されます。Avro オブジェクトコンテナおよび Parquet ファイルでは、この配列内のオブジェクトは、Macie が機密データの出現を検出したレコードインデックスおよびレコード内のフィールドへのパスを指定します。JSON および JSON Lines ファイルでは、この配列内のオブジェクトは、Macie が機密データの出現を検出したフィールドまたは配列へのパスを指定します。JSON Lines ファイルでは、データを含む行のインデックスも指定します。

これらの配列の内容は、影響を受けた S3 オブジェクトのファイルタイプまたはストレージ形式、およびその内容によって異なります。

機密データの場所に関する JSON スキーマの詳細と例

Amazon Macie は、特定のタイプのファイルやコンテンツ内の機密データを検出した場所を示すために使用する JSON 構造のコンテンツをカスタマイズします。次のトピックでは、これらの構造について説明し、例を示します。

トピック

機密データの検出結果に含めることができる JSON 構造の完全なリストについては、Amazon Macie API リファレンスの検出結果を参照してください。

セルの配列

Microsoft Excel ワークブック、CSV ファイル、および TSV ファイルに適用先

`cells` 配列内で、`Cell` オブジェクトは、Macie が機密データの出現を検出したセルまたはフィールドを指定します。以下のテーブルでは、`Cell` オブジェクト内の各フィールドの目的について説明しています。

フィールド	タイプ	説明
`cellReference`	文字列	出現を含む絶対セル参照としてのセルの場所 このフィールドは、Excel ワークブックにのみ適用されます。CSV ファイルおよび TSV ファイルでは、この値は null です。
`column`	整数	出現を含む列の列番号 Excel ワークブックでは、この値は

フィールド	タイプ	説明
		列識別子のアルファベット文字に関連します。たとえば、列 A では、1、列 B では、2 など。
columnName	文字列	出現を含む列の名前 (可能な場合)
row	整数	出現を含む行の行番号

次の例では、Macie が CSV ファイル内で検出した機密データの出現場所を指定する Cell オブジェクトの構造を示します。

```
"cells": [
   {
      "cellReference": null,
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

前の例では、検出結果は Macie がファイルの 3 番目の列の 5 行目のフィールド (SSN) に機密データを検出したことを示しています。

次の例では、Macie が Excel ワークブック内で検出した機密データの出現場所を指定する Cell オブジェクトの構造を示します。

```
"cells": [
   {
      "cellReference": "Sheet2!C5",
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

前の例では、検出結果は Macie がワークブックの Sheet2 という名前のワークシートで機密データを検出したことを示しています。そのワークシートで Macie は 3 列目の 5 行目 (列 C、SSN) のセルに機密データを検出しました。

LineRanges 配列

適用先: Eメールメッセージ (EML) ファイル、非バイナリテキストファイル (CSV、JSON、JSON Lines、TSV ファイル以外 — 例えば HTML、TXT、XML ファイルなど

`lineRanges` 配列内で、Range オブジェクトは、Macie が機密データの出現を検出した 1 つの行または複数の行の包括的な範囲、および指定された行 (1 つまたは複数) のデータの位置を指定します。

このオブジェクトは、`occurrences` オブジェクトの他のタイプの配列でサポートされているファイルタイプでは空であることがしばしばあります。例外は次のとおりです。

- 構造化されたファイルの構造化されていないセクション内のデータ。
- Macie がプレーンテキストとして分析する不正な形式のファイル内のデータ。
- Macie が機密データを検出した 1 つ以上の列名を持つ CSV ファイルまたは TSV ファイル

以下のテーブルでは、`lineRanges` 配列の Range オブジェクト内の各フィールドの目的について説明しています。

フィールド	タイプ	説明
`end`	整数	ファイルの先頭から出現の末尾までの行数
`start`	整数	ファイルの先頭から出現の先頭までの行数
`startColumn`	整数	出現`start`を含む最初の行の先頭から出現の先頭までの、1 から始まるスペースを含めた文字数

次の例では、Macie が TXTファイル内の 1 行に検出した機密データの出現場所を指定する Range オブジェクトの構造を示します。

```
"lineRanges": [
   {
      "end": 1,
      "start": 1,
      "startColumn": 119
   }
]
```

前の例では、検出結果は Macie がファイルの最初の行に機密データ (郵送先住所) の完全な出現を検出したことを示しています。出現での最初の文字は、その行の先頭から 119 番目の文字 (スペースを含む) です。

次の例では、TXT ファイル内の複数行にまたがる機密データの出現場所を指定する Range オブジェクトの構造を示します。

```
"lineRanges": [
   {
      "end": 54,
      "start": 51,
      "startColumn": 1
   }
]
```

前の例では、検出結果は Macie がファイルの 51 行目から 54 行目に機密データ (郵送先住所) の出現を検出したことを示しています。出現での最初の文字は、ファイルの 51 行目の最初の文字です。

ページ配列

Adobe Portable Document Format (PDF) ファイルに適用先

pages 配列内で、Page オブジェクトは、Macie が機密データの出現を検出したページを指定します。オブジェクトには pageNumber フィールドが含まれます。pageNumber フィールドは、出現を含むページ番号を指定する整数を格納します。

次の例では、Macie が PDF ファイル内で検出した機密データの出現場所を指定する Page オブジェクトの構造を示します。

```
"pages": [
   {
      "pageNumber": 10
```

```
    }
]
```

前の例では、検出結果はファイルの 10 ページに出現が含まれていることを示しています。

レコード配列

Apache Avro オブジェクトコンテナ、Apache Parquet ファイル、JSON ファイル、および JSON Lines ファイルに適用先

Avro オブジェクトコンテナまたは Parquet ファイルでは、`records` 配列内の `Record` オブジェクトは、Macie が機密データの出現を検出したレコードインデックスおよびレコード内のフィールドへのパスを指定します。JSON および JSON Lines ファイルでは、`Record` オブジェクトは、Macie が機密データの出現を検出したフィールドまたは配列へのパスを指定します。JSON Lines ファイルでは、出現を含む行のインデックスも指定します。

以下のテーブルでは、`Record` オブジェクト内の各フィールドの目的について説明しています。

フィールド	タイプ	説明
`jsonPath`	文字列	JSONPath 式としての出現へのパス Avro オブジェクトコンテナまたは Parquet ファイルでは、これは出現を含むレコード`recordIndex` 内のフィールドへのパスです。JSON または JSON Lines ファイルでは、これは出現を含むフィールドまたは配列へのパスです。データが配列内の値である場合、パスは出現を含む値も示します。 Macie がパス内の任意の要素の名前で機密データを検出した場合、Macie は `Record` オ

フィールド	タイプ	説明
		ブジェクトから jsonPath フィールドを省略します。パス要素の名前が 240 文字を超える場合、Macie は名前の先頭から文字を削除して名前を切り捨てます。結果としてフルパスが 250 文字を超える場合、Macie はパスに含まれる文字が 250 文字以下になるまで、パスの最初の要素から開始してパスを切り捨てます。
recordIndex	整数	Avro オブジェクトコンテナまたは Parquet ファイルでは、出現を含むレコードの 0 から始まるレコードインデックス JSON Lines ファイルでは、出現を含む行の 0 から始まる行インデックス この値は、JSON ファイルでは常に 0 です。

次の例では、Macie が Parquet ファイル内で検出した機密データの出現場所を指定する Record オブジェクトの構造を示します。

```
"records": [
   {
      "jsonPath": "$['abcdefghijklmnopqrstuvwxyz']",
      "recordIndex": 7663
   }
]
```

前の例では、検出結果は、インデックス 7663 (レコード番号 7664) のレコードで Macie が機密データを検出したことを示しています。そのレコードで、Macie は abcdefghijklmnopqrstuvwxyz という名前のフィールドで機密データを検出しました。レコード内のフィールドへの完全な JSON

パスは $.abcdefghijklmnopqrstuvwxyz です。このフィールドはルート (外部レベル) オブジェクトの直系の子孫です。

次の例では、Macie が Parquet ファイル内で検出した機密データの出現の Record オブジェクトの構造も示します。この例では、名前が文字数の制限を超えているため、Macie は出現を含むフィールドの名前を切り捨てました。

```
"records": [
   {
      "jsonPath":
 "$['...uvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabc
      "recordIndex": 7663
   }
]
```

前の例では、フィールドはルート (外部レベル) オブジェクトの直系の子孫です。

次の例でも、Macie が Parquet ファイル内で検出した機密データの出現に対し、Macie はその出現を含むフィールドへのフルパスを切り捨てました。フルパスが文字制限を超えています。

```
"records": [
   {
      "jsonPath":
 "$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
      "recordIndex": 2335
   }
]
```

前の例では、検出結果は、インデックス 2335 (レコード番号 2336) のレコードで Macie が機密データを検出したことを示しています。そのレコードで、Macie は abcdefghijklmnopqrstuvwxyz という名前のフィールドで機密データを検出しました。レコード内のフィールドへの完全な JSON パスは以下です。

```
$['1234567890']ussn1.ussn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

次の例では、Macie が JSON ファイル内で検出した機密データの出現場所を指定する Record オブジェクトの構造を示します。この例では、出現は配列内の特定の値です。

```
"records": [
   {
      "jsonPath": "$.access.key[2]",
```

```
      "recordIndex": 0
   }
]
```

前の例では、検出結果は、key という名前の配列の 2 番目の値に Macie が機密データを検出したことを示しています。配列は、access という名前のオブジェクトの子です。

次の例では、Macie が JSON Lines ファイル内で検出した機密データの出現場所を指定する Record オブジェクトの構造を示します。

```
"records": [
   {
      "jsonPath": "$.access.key",
      "recordIndex": 3
   }
]
```

前の例では、検出結果は、ファイル内の 3 番目の値 (行) で Macie が機密データを検出したことを示しています。その行では、出現は key という名前のフィールドにあり、それは access という名前のオブジェクトの子です。

Amazon Macie の調査結果を抑制する

調査結果の分析を合理化するために、抑制ルール を作成して使用できます。suppression rules (抑制ルール) は、Amazon Macie が調査結果を自動的にアーカイブするケースを定義する属性ベースのフィルター条件のセットです。抑制ルールは、調査結果のクラスを確認した後、それらの調査結果を再度通知してほしくない場合に役立ちます。

例えば、バケットがパブリックアクセスを許可せず、自動的に特定の AWS KMS key で新しいオブジェクトを暗号化する場合に、S3 バケットが郵送先住所を含める許可を決定することがあります。この場合は、フィールドのフィルター基準を指定する以下の抑制ルールを作成します: 機密データ検出タイプ、S3 バケットパブリックアクセス許可、および S3 バケットの暗号化 KMS キー ID このルールは、フィルター基準を満たす今後の検出結果を制限します。

抑制ルールを使用して検出結果を抑制する場合、Macie は、ルールの基準を満たす機密データおよび潜在的なポリシー違反の今後の発生について検出結果を生成し続けます。ただし、Macie は調査結果のステータスを自動的に archived (アーカイブ済み) に変更します。これは、調査結果がデフォルトで Amazon Macie コンソールに表示されないけれども、有効期限が切れるまで Macie には保持されることを意味します。Macie は 90 日間調査結果を保存します。

さらに、Macie は抑制した検出結果をイベントとしての Amazon EventBridge または AWS Security Hub に出力しません。ただし、Macie は、抑制した機密データの調査結果に関連している sensitive data discovery results (機密データの検出結果) を引き続き作成して保存します。これにより、実施するデータプライバシーと保護の監査または調査に関する機密データの調査結果のイミュータブルな履歴を確実に保持できます。

> **Note**
>
> アカウントが複数の Macie アカウントを集中管理する組織に含まれる場合は、アカウントによって抑制ルールの動作が異なる場合があります。これは、制限したい結果のカテゴリと、Macie 管理者アカウントまたはメンバーアカウントのどちらを使用しているかによって異なります。
>
> - ポリシー検出結果 — 組織のアカウントに関するポリシー検出結果を制限できるのは Macie 管理者のみです。
>
> Macie 管理者アカウントを持ち、抑制ルールを作成する場合、特定のアカウントを除外するようにルールを設定しない限り、Macie は組織内のすべてのアカウントのポリシー検出結果にルールを適用します。Macie メンバーアカウントを持ち、そのアカウントのポリシー検出結果を制限したい場合は、Macie 管理者に連絡してください。
> - 機密データ検出結果 — Macie 管理者と個々のメンバーは、機密データ検出ジョブで生成された機密データ検出結果を制限することができます。Macie 管理者は、組織の機密データ自動検出を実行している間に、Macie が生成する検出結果を制限することもできます。
>
> 機密データ検出ジョブを作成するアカウントのみ、そのジョブの生成する機密データの検出結果を制限、または検出結果にアクセスできます。組織の Macie 管理者アカウントのみが、機密データ自動検出によって組織内のアカウント用に生成された検出結果を制限、または検出結果にアクセスできます。
>
> 管理者とメンバーが実行できるタスクの詳細については、Amazon Macie 管理者とメンバーアカウントの関係について理解する を参照してください。

抑制ルールを作成および管理するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。次のトピックでは、その方法を説明します。API に向けたトピックでは、AWS Command Line InterfaceAWS CLIを用いてこれらのタスクを実行する方法を説明します。現在のバージョンの別の AWS コマンドラインツールまたは AWS SDKを使用するか、HTTPS リクエスト

を Macie に直接送信してこれらのタスクを実行することもできます。AWS のツールと SDK に関する詳細については、AWS での構築ツールを参照してください。

トピック

- 抑制ルールを作成する
- 抑制された検出結果を確認する
- 抑制ルールを変更する
- 抑制ルールを削除する

抑制ルールを作成する

抑制ルールを作成する前に、抑制ルールを使用して抑制した調査結果を復元 (アーカイブ解除) できないことに注意してください。ただし、Amazon Macie コンソールで 抑制された検出結果を表示し、Amazon Macie API を用いて抑制された検出結果にアクセスできます。

抑制ルールを作成するときは、フィルター基準と名前、必要に応じてルールの詳細を指定します。抑制ルールは、Amazon Macie コンソールまたは Amazon Macie API を使用して作成できます。

Console

Amazon Macie コンソールを使用して抑制ルールを作成するには、次のステップに従います。

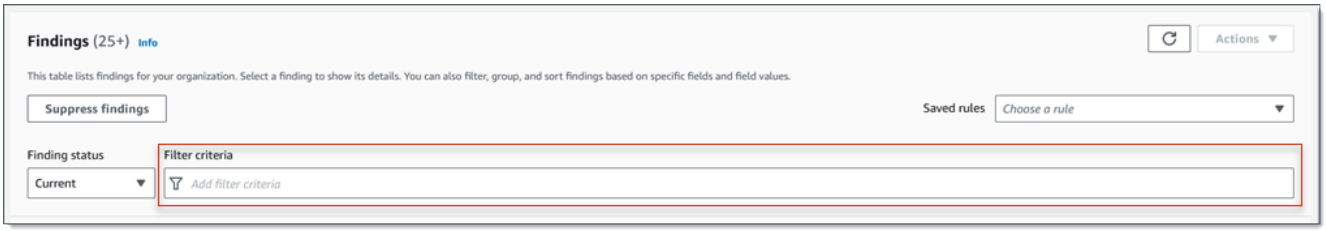
抑制ルールを作成するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果を選択します。

> **Tip**
>
> 既存の抑制ルールまたはフィルタールールを開始点として使用するには、Saved rules (保存されたルール) のリストからルールを選択します。
> また、事前定義された論理グループによる調査結果を最初にピボットしてドリルダウンすることで、ルールの作成を合理化することもできます。これを行うと、Macie は適切なフィルター条件を自動的に作成して適用します。これは、ルールを作成するために役立つ開始点となる場合があります。これを行うには、ナビゲーションペイン (調査結果 の下) の バケット別、タイプ別、または ジョブ別を選択し、次にテーブル

内で項目を選択します。詳細パネルで、ピボットするフィールドのリンクを選択します。

3. フィルタ条件ボックスで、ルールで抑制する検出結果の属性を指定するフィルター条件を追加します。



フィルター条件を追加する方法については、フィルターの作成と調査結果への適用を参照してください。

4. ルールのフィルター条件の追加が完了したら、フィルターバーの上にある 検出結果を抑制する を選択します。
5. 抑制ルール の下で、ルールの名前を入力し、必要に応じて説明を入力します。
6. 保存 を選択します。

API

プログラムで抑制ルールを作成するには、Amazon Macie API の CreateFindingsFilter オペレーションを使用して、必要なパラメータに適切な値を指定します。

- `action` パラメータでは、`ARCHIVE` を指定して、Macie がルールの基準を満たす検出結果を制限するようにします。
- `criterion` パラメータでは、ルールのフィルター基準を定義する条件のマップを指定します。

  マップでは、条件ごとに、フィールド、演算子、およびフィールドの 1 つ以上の値を指定する必要があります。値のタイプと数は、選択するフィールドと演算子によって異なります。条件で使用できるフィールド、演算子、および値のタイプについては、調査結果をフィルタリングするためのフィールド、条件での演算子の使用、およびフィールドの値を指定するを参照してください。

AWS CLI を使用して抑制ルールを作成するには、create-findings-filter コマンドを実行し、必要なパラメータに適切な値を指定します。次の例では、現在の AWS リージョン 内にあり、S3 オブ

ジェクト内の郵送先住所 (他のタイプの機密データは含まない) の出現をレポートするすべての機密データの検出結果を返す抑制ルールを作成します。

この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行継続文字を使用しています。

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.detections.type\":{\"eqExactMatch\":
[\"ADDRESS\"]}}}
```

実行する条件は以下のとおりです。

- *my_suppression_rule* は、ルールのカスタム名です。
- criterion は、ルールのフィルター条件のマップです。
  - *classificationDetails.result.sensitiveData.detections.type* は、機密データの検出タイプ フィールドの JSON 名です。
  - *eqexactMatch* は、完全一致と等しい 演算子を指定します。
  - *ADDRESS* は、機密データ検出タイプ フィールドの列挙値です。

コマンドが正常に実行された場合は、以下のような出力が表示されます。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
```

```
}
```

ここで、arn は、作成された抑制ルールの Amazon リソースネーム (ARN)で、id は、ルールの一意の識別子です。

フィルター基準のその他の例については、Amazon Macie API を用いて調査結果をプログラムでフィルタリングするを参照してください。

抑制された検出結果を確認する

デフォルトでは、Macie は Amazon Macie コンソールに抑制された調査結果を表示しません。フィルター設定を変更することにより、コンソールでこれらの検出結果を確認できます。

抑制された検出結果をコンソールで確認する

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果を選択します。この 検出結果 ページには、Macie が過去 90 日間に現在の AWS リージョン でアカウントに対し作成または更新した検出結果が表示されます。デフォルトでは、これには抑制ルール で抑制された調査結果は含まれません。
3. ステータスを検索 で、以下のいずれかを実行します。

   - 抑制された検出結果のみを表示するには、アーカイブ済み を選択します。
   - 抑制された検出結果と抑制されていない検出結果の両方を表示するには、すべてを選択します。
   - 抑制された検出結果を再度非表示にするには、現在 を選択します。

Amazon Macie API を使用して、抑制された結果にアクセスすることもできます。抑制された調査結果のリストを取得するには、ListFindings オペレーションを使用し、archived フィールドに true を指定するフィルター条件を含めます。AWS CLI を使用してこれを行う方法の例については、調査結果をプログラムでフィルタリングするにはを参照してください。1 つ以上の抑制された検出結果の詳細を取得するには、GetFindingsオペレーションを使用し、取得する各検出結果に一意の識別子を指定します。

抑制ルールを変更する

抑制ルールの設定は、Amazon Macie コンソールまたは Amazon Macie API を使用していつでも変更できます。ルールにタグを割り当てて管理することもできます。

タグは、ユーザーが定義して特定のタイプの AWS リソースに割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを特定、分類および管理できます。詳細については、Amazon Macie リソースへのタグ付けを参照してください。

Console

Amazon Macie コンソールを使用して既存の抑制ルールの設定を変更するには、次のステップに従います。

抑制ルールを変更するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果を選択します。
3. Saved rules (保存されたルール) のリストで、変更する抑制ルールの隣にある edit (編集) アイコン を選択します。
4. 次のいずれかを実行します。
   - ルールのフィルター基準を変更するには、フィルタ条件ボックスを使用してルールで抑制する検出結果の属性を指定するフィルター条件を追加します。この方法の詳細は、フィルターの作成と調査結果への適用を参照してください。
   - ルールの名前を変更するには、新しい名前を 抑制ルールの下の 名前ボックスに入力します。
   - ルールの説明を変更するには、新しい説明を 抑制ルールの下の 説明ボックスに入力します。
   - ルールのタグを割り当て、確認、または編集するには、抑制ルールのタグを管理 を選択します。必要に応じてタグを確認および変更します。ルールには、最大 50 個のタグを含めることができます。
5. 変更が完了したら、Save を選択します。

API

プログラムで抑制ルールを変更するには、Amazon Macie API のUpdateFindingsFilterオペレーションを使用します。リクエストを送信するときは、サポートされているパラメータを使用して、変更する設定ごとに新しい値を指定します。

id パラメータでは、変更するルールの一意の識別子を指定します。ListFindingsFilterオペレーションを実行して、アカウントの抑制ルールとフィルタールールのリストを取得することで、この識別子が得られます。AWS CLI を使用している場合は、list-findings-filters コマンドを実行してこのリストを取得してください。

AWS CLI を使用して抑制ルールを変更するには、update-findings-filter コマンドを実行し、サポートされているパラメータを使用して、変更する設定ごとに新しい値を指定します。次の例では、既存の抑制ルールの名前を変更します。

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --
name mailing_addresses_only
```

実行する条件は以下のとおりです。

- *8a3c5608-aa2f-4940-b347-d1451example* は、ルールの一意の識別子です。
- *mailing_addresses_only* は、ルールの新しい名前です。

コマンドが正常に実行された場合は、以下のような出力が表示されます。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

ここで、arn は、変更されたルールの Amazon リソースネーム (ARN)で、id は、ルールの一意の識別子です

同様に、次の例では、action パラメータの値を NOOP から ARCHIVE に変更することで、フィルタールールを抑制ルールに変換します。

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action ARCHIVE
```

実行する条件は以下のとおりです。

- *8a1c3508-aa2f-4940-b347-d1451example* は、ルールの一意の識別子です。
- ***#####*** は、ルールの基準を満たす検出結果に対して Macie が実行する新しいアクションです (検出結果を制限します)。

コマンドが正常に実行された場合は、次のような出力が表示されます。

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

ここで、arn は、変更されたルールの Amazon リソースネーム (ARN)で、id は、ルールの一意の識別子です

抑制ルールを削除する

抑制ルールは、Amazon Macie コンソールまたは Amazon Macie API を使用していつでも削除できます。抑制ルールを削除すると、Macie は、ルールの基準を満たし、他のルールに抑制されない検出結果の新規およびその後の出現の抑制を停止します。ただし、Macie は、現在処理中であり、ルールの基準を満たす検出結果を引き続き制限する可能性があることに注意してください。

抑制ルールを削除した後、ルールの基準を満たす検出結果の新規およびその後の出現は、現在のステータス (アーカイブ済みにならない) となります。これは、それらが Amazon Macie コンソールにデフォルトで表示されることを意味します。さらに、Macie はこれらの検出結果を Amazon EventBridge イベントとして発行します。アカウントで選択した出力設定に応じて、Macie は AWS Security Hub にそのサンプル検出結果を発行することもできます。

Console

Amazon Macie コンソールを使用して抑制ルールを削除するには、次のステップに従います。

抑制ルールを削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 調査結果を選択します。
3. Saved rules (保存されたルール) のリストで、削除する抑制ルールの隣にある編集アイコン
   を選択します。
4. 抑制ルールの下で、削除を選択します。

API

プログラムで抑制ルールを削除するには、Amazon Macie API の DeleteFindingsFilter オペレーションを使用します。id パラメータでは、削除する抑制ルールの一意の識別子を指定します。ListFindingsFilterオペレーションを実行して、アカウントの抑制ルールとフィルタールールのリストを取得することで、この識別子が得られます。AWS CLI を使用している場合は、list-findings-filters コマンドを実行してこのリストを取得してください。

AWS CLI を使用して抑制ルールを削除するには、delete-findings-filter コマンドを実行します。例:

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

ここで *8a3c5608-aa2f-4940-b347-d1451example* は、削除する抑制ルールの一意の識別子です。

コマンドが正常に実行されると、Macie は空の HTTP 200 レスポンスを返します。それ以外の場合、Macie は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

Amazon Macie 調査結果の重要度スコアリング

Amazon Macie がポリシーまたは機密データの調査結果を生成すると、その調査結果に重要度が自動的に割り当てられます。調査結果の重要度は、調査結果の主要な特性を反映し、調査結果の評価と優先順位付けに役立ちます。調査結果の重要度は、影響を受けたリソースが組織に対して緊急性または重要性を意味する、または示すものではありません。

ポリシーの検出結果の場合、重要度は Amazon Simple Storage Service (Amazon S3) 汎用バケットのセキュリティまたはプライバシーに関する潜在的な問題の性質に基づいています。機密データの調査結果では、重要度は、Macie が S3 オブジェクトで見つけた機密データの性質と出現の数に基づいています。

Macie では、調査結果の重要度は 2 つの方法で表されます。

重要度レベル

これは重要度の定性的表現です。重要度の範囲は、最も低い重要度での Low から、最も高い重要度での High までです。

重要度レベルは Amazon Macie コンソールに直接表示されます。またそれらは、Macie コンソールで、Amazon Macie API から、および機密データの調査結果に関連する機密データ検出結果では、JSON 表現で利用できます。重要度レベルは、Macie が Amazon に発行する検出結果イベント EventBridge や、Macie が に発行する検出結果にも含まれます AWS Security Hub。

重要度スコア

これは重要度の数値表現です。重要度スコアの範囲は、1 から 3で、重要度レベルに直接マッピングされます。

重要度スコア	重要度レベル
1	低
2	中
3	高

重要度スコアは Amazon Macie コンソールに直接表示されません。ただし、それらは、Macie コンソールで、Amazon Macie API から、および機密データの調査結果に関連する機密データ検出結果では、JSON 表現で利用できます。重要度スコアは、Macie が Amazon に発行する検出結果イベントにも含まれます EventBridge。Macie が に発行する検出結果には含まれません AWS Security Hub。

このセクションのトピックでは、Macie がポリシーの調査結果および機密データの調査結果の重要度をどのように判断するかを示します。

トピック

- ポリシーの調査結果の重要度スコアリング
- 機密データの調査結果の重要度スコア

ポリシーの調査結果の重要度スコアリング

ポリシー検出結果の重要度は、S3 汎用バケットのセキュリティまたはプライバシーに関する潜在的な問題の性質に基づいています。次のテーブルに、Macie がポリシーの調査結果の各タイプに割り当てる重要度レベルをリスト化します。各タイプの説明については、調査結果のタイプを参照してください。

調査結果タイプ	重要度レベル
Policy:IAMUser/S3BlockPublicAccessDisabled	高い
Policy:IAMUser/S3BucketEncryptionDisabled	低
Policy:IAMUser/S3BucketPublic	高い
Policy:IAMUser/S3BucketReplicatedExternally	高い
Policy:IAMUser/S3BucketSharedExternally	高
Policy:IAMUser/S3BucketSharedWithCloudFront	中程度

ポリシーの調査結果の重要度は、調査結果の出現の数によって変化しません。

機密データの調査結果の重要度スコア

機密データの調査結果の重要度は、Macie が S3 オブジェクトで見つけた機密データの性質と出現の数に基づいています。次のトピックでは、Macie が各タイプの機密データの調査結果の重要度をどのように判断するかを示します。

- SensitiveData:S3Object/Credentials
- SensitiveData:S3Object/CustomIdentifier
- SensitiveData:S3Object/Financial
- SensitiveData:S3Object/Personal
- SensitiveData:S3Object/Multiple

Macie が機密データの調査結果で検出およびレポートできる機密データのタイプの詳細な情報については、マネージドデータ識別子の使用 と カスタムデータ識別子の構築 を参照してください。

SensitiveData:S3Object/Credentials

SensitiveData:S3Object /Credentials の検出結果は、S3 オブジェクトに機密認証情報データが含まれていることを示します。このタイプの調査結果では、Macie がオブジェクトで見つけた認証情報データのタイプと出現の数に基づいて、Macie が重要度を判断します。

次のテーブルに、S3 オブジェクト内の認証情報データの出現をレポートする調査結果に Macie が割り当てる重要度レベルを示します。

機密データタイプ	出現 1 回	出現 2～99 回	出現 100 回以上
AWS シークレットアクセスキー	高い	高い	高い
Google Cloud API キー	高い	高い	高い
HTTP 基本認証ヘッダー	高い	高い	高い
JSON ウェブトークン (JWT)	高い	高い	高い
OpenSSH プライベートキー	高い	高い	高い
PGP プライベートキー	高い	高い	高い
公開鍵暗号標準 (PKCS) プライベートキー	高い	高い	高い
PuTTY プライベートキー	高い	高い	高い
ストライプ API キー	高い	高い	高い

SensitiveData:S3Object/CustomIdentifier

SensitiveData:S3Object/CustomIdentifier検出結果は、S3 オブジェクトに 1 つ以上のカスタムデータ識別子の検出基準に一致するテキストが含まれていることを示します。オブジェクトには、複数のタイプの機密データが含まれている場合があります。

デフォルトでは、Macie はこのタイプの調査結果に 中重要度レベルを割り当てます。S3 オブジェクトに、少なくとも 1 つのカスタムデータ識別子の検出基準に一致するテキストの少なくとも 1 つの出現が含まれている場合、Macie は調査結果に中重要度レベルを自動的に割り当てます。検出結果の重要度は、カスタムデータ識別子の基準に一致するテキストの出現の数によって変化しません。

ただし、調査結果を生成したカスタムデータ識別子のカスタム重要度設定を定義した場合、このタイプの調査結果の重要度は異なる場合があります。この場合、Macie は重要度を次のように判断します。

- S3 オブジェクトに 1 つのみのカスタムデータ識別子の検出基準に一致するテキストが含まれている場合、Macie はその識別子の重要度設定に基づいて調査結果の重要度を判断します。
- S3 オブジェクトに複数のカスタムデータ識別子の検出基準に一致するテキストが含まれている場合、Macie は各カスタムデータ識別子の重要度設定を評価し、それらの設定のうちどれが最も高い重要度を生成するかを判断し、次にその最も高い重要度を調査結果に割り当てることで調査結果の重要度を判断します。

カスタムデータ識別子の重要度の設定を確認するには、Amazon Macie コンソールのナビゲーションペインで カスタムデータ識別子を選択します。次に、カスタムデータ識別子の名前を選択します。重要度セクションには、設定が表示されます。詳細については、「カスタムデータ識別子の結果の重要度設定の定義」を参照してください。

SensitiveData:S3Object/Financial

SensitiveData:S3Object /Financial の検出結果は、S3 オブジェクトに機密性の高い財務情報が含まれていることを示します。このタイプの調査結果では、Macie がオブジェクトで見つけた財務情報のタイプと出現の数に基づいて、Macie が重要度を判断します。

次のテーブルに、S3 オブジェクト内の財務情報の出現をレポートする調査結果に Macie が割り当てる重要度レベルを示します。

機密データタイプ	出現 1 回	出現 2～99 回	出現 100 回以上
銀行口座番号 [1]	高い	高い	高い
クレジットカードの有効期限	低	中程度	高い

機密データタイプ	出現 1 回	出現 2～99 回	出現 100 回以上
クレジットカードの磁気ストライプデータ	高い	高い	高い
クレジットカード番号 [2]	高い	高い	高い
クレジットカード認証コード	中程度	高い	高い

1. 重要度レベルは、基本銀行口座番号 (BBAN)、国際銀行口座番号 (IBAN)、カナダまたは米国の銀行口座番号など、どのタイプの銀行口座番号でも同じです。
2. 重要度レベルは、キーワードの近くにある、またはないクレジットカード番号で同じです。

調査結果がオブジェクト内の複数のタイプの財務情報をレポートする場合、Macie が見つけた財務情報のタイプごとに重要度を計算し、どのタイプが最も高い重要度を生成するタイプを判断し、その最も高い重要度を調査結果に割り当てることで、Macie が重要度を判断します。たとえば、Macie がオブジェクト内で 10 件のクレジットカードの有効期限 (中重要度レベル) と 10 件のクレジットカード番号 (高重要度レベルを検出した場合、Macie は高重要度レベルを調査結果に割り当てます。

SensitiveData:S3Object/Personal

SensitiveData:S3Object /Personal の検出結果は、S3 オブジェクトに個人健康情報 (PHI)、個人を特定できる情報 (PII)、またはこれら 2 つの組み合わせなどの機密性の高い個人情報が含まれていることを示します。このタイプの調査結果では、Macie がオブジェクトで見つけた個人情報のタイプと出現の数に基づいて、Macie が重要度を判断します。

次のテーブルに、S3 オブジェクト内の PHI の出現をレポートする機密データの調査結果に Macie が割り当てる重要度レベルを示します。

機密データタイプ	出現 1 回	出現 2～99 回	出現 100 回以上
	高い	高い	高い

機密データタイプ	出現 1 回	出現 2～99 回	出現 100 回以上
麻薬取締局 (DEA) 登録番号			
健康保険請求番号 (HICN)	高い	高い	高い
健康保険または医療識別番号	高い	高い	高い
ヘルスケア共通手順コーディングシステム (HCPCS) コード	高い	高い	高い
全米医薬品コード (NDC)	高い	高い	高い
国家プロバイダー識別子 (NPI)	高い	高い	高い
機器固有識別子 (UDI)	低	中程度	高い

次のテーブルに、S3 オブジェクト内の PII の出現をレポートする機密データの調査結果に Macie が割り当てる重要度レベルを示します。

機密データタイプ	出現 1 回	出現 2～99 回	出現 100 回以上
生年月日	低	中程度	高い
運転免許証識別番号	低	中程度	高い
選挙人名簿番号	高い	高い	高い
フルネーム	低	中程度	高い
全地球測位システム (GPS) 座標	低	中程度	中程度

機密データタイプ	出現 1 回	出現 2～99 回	出現 100 回以上
HTTP クッキー	低	中程度	高い
郵送先住所	低	中程度	高い
国民識別番号	高い	高い	高い
国民保険番号 (NINO)	高い	高い	高い
パスポート番号	中程度	高い	高い
本籍地	高い	高い	高い
電話番号	低	中程度	高い
社会保険番号 (SIN)	高い	高い	高い
社会保障番号 (SSN)	高い	高い	高い
納税者識別番号または参照番号	高い	高い	高い
車両識別番号 (VIN)	低	低	中程度

検出結果がオブジェクト内の複数のタイプの PHI、PII、または PHI と PII 両方をレポートする場合、Macie がタイプごとに重要度を計算し、どのタイプが最も高い重要度を生成するタイプを判断し、その最も高い重要度を検出結果に割り当てることでその重要度を判断します。

たとえば、Macie がオブジェクト内で 10 件のフルネーム (中重要度レベル) と 5 件のパスポート番号 (高重要度レベル) を検出した場合、Macie は高重要度レベルを調査結果に割り当てます。同様に、Macie がオブジェクト内で 10 件のフルネーム (中重要度レベル) と 10 件の健康保険識別番号 (高重要度レベル) を検出した場合、Macie は 高重要度レベルを調査結果に割り当てます。

SensitiveData:S3Object/Multiple

SensitiveData:S3Object /Multiple の検出結果は、S3 オブジェクトに、認証情報データ、財務情報、個人情報、または 1 つ以上のカスタムデータ識別子の検出基準に一致するテキストの組み合わせなど、複数の機密データカテゴリにまたがるデータが含まれていることを示します。

このタイプの調査結果では、(前のトピックで示したように) Macie が見つけた機密データのタイプごとに重要度を計算し、どのタイプが最も高い重要度を生成するタイプを判断し、その最も高い重要度を調査結果に割り当てることで、Macie が重要度を判断します。

例えば、Macie がオブジェクト内で 10 個のフルネーム (Medium 重要度レベル) と 10 AWS 個のシークレットアクセスキー (High 重要度レベル) を検出すると、Macie は検出結果に High 重要度レベルを割り当てます。

Amazon Macie の調査結果のモニタリングと処理

モニタリングシステムやイベント管理システムなど、他のアプリケーション、サービス、およびシステムとの統合をサポートするために、Amazon Macie はポリシーと機密データの調査結果をイベントとして Amazon EventBridge に自動的に発行します。追加のサポートと組織のセキュリティ体制の広範な分析については、ポリシーと機密データの調査結果も AWS Security Hub に発行するように Macie を設定できます。

Amazon EventBridge

以前の Amazon CloudWatch Events である Amazon EventBridge は、アプリケーションやサービスからのリアルタイムのデータのストリーミングを配信し、そのデータを AWS Lambda 関数、Amazon Simple Notification Service のトピック、および Amazon Kinesis ストリームなどのターゲットにルーティングするサーバーレスイベントバスサービスです。EventBridge を使用すると、Macie が調査結果について発行するイベントなど、特定のタイプのイベントのモニタリングと処理を自動化できます。EventBridge の詳細については、Amazon EventBridge ユーザーガイドを参照してください。

AWS User Notificationsを Macie と統合すると、EventBridge イベントを使用して、Macie が検出結果のために公開するイベントに関する通知を自動的に生成することもできます。ユーザー通知では、関心のあるEventBridge に関する通知を受信するためのカスタムルールを作成し、配信チャネルを設定します。配信チャネルには、E メール、AWS Chatbot チャット通知、AWS Console Mobile Application プッシュ通知が含まれます。通知は、AWS Management Console の一元された場所で確認することもできます。ユーザー通知の詳細については、AWS User Notifications ユーザーガイドを参照してください。

AWS Security Hub

AWS Security Hub は、AWS 環境全体のセキュリティ状態を包括的に把握するセキュリティサービスです。AWS のサービス およびサポートされている AWS Partner Network セキュリティソリューションからセキュリティデータを収集し、セキュリティ業界標準およびベストプラクティスに照らして環境をチェックするのに役立ちます。また、セキュリティの傾向を分析し、特に優先度の高いセキュリティ問題を特定するのにも役立ちます。Security Hub を使用すると、組織のセキュリティ体制の広範な分析の一部として、Macie の調査結果を確認できます。また、複数の AWS リージョン からの検出結果を集約したり、1 つのリージョンから集計した検出結果データをモニタリングおよび処理することもできます。Security Hub の詳細については、AWS Security Hub ユーザーガイドを参照してください。

Macie が調査結果を作成すると、その調査結果を新しいイベントとして EventBridge に自動的に発行します。アカウントで選択した発行設定に応じて、Macie は Security Hub にその調査結果を発行することもできます。Macie は、調査結果の処理が終了した直後に、新しい調査結果をそれぞれ発行します。Macie は、既存のポリシーの調査結果のその後の出現を検出すると、その調査結果の既存の EventBridge イベントに更新を発行します。発行設定に応じて、Macie は Security Hub にその更新を発行することもできます。Macie は、アカウントの発行設定で指定した発行頻度を使用して、これらの更新を定期的に発行します。

トピック

Amazon Macie 調査結果の発行設定を設定する

他のアプリケーション、サービス、およびシステムとの統合をサポートするために、Amazon Macie はポリシーの調査結果と機密データの調査結果の両方をイベント EventBridge として Amazon に自動的に発行します。 EventBridge を使用して検出結果のモニタリングと処理を行う方法については、「」を参照してくださいAmazon Macie の Amazon EventBridge との統合。

アカウントの発行設定で指定した送信先オプションを使用して AWS Security Hub 、調査結果を自動的に に発行するように Macie を設定できます。これらのオプションを使用すると、ポリシーの調査結果のみ、機密データの調査結果のみ、またはポリシーと機密データの調査結果の両方を Security Hub に発行するように Macie を設定できます。また、Security Hub への調査結果の発行を停止するように Macie を設定することもできます。Security Hub を使用して調査結果のモニタリングと処理を行う方法の詳細については、Amazon Macie の AWS Security Hub との統合を参照してください。

ポリシーの調査結果では、Macie が別の AWS のサービス に調査結果を発行するタイミングは、調査結果が新規であるかどうか、およびアカウントに指定する発行頻度によって異なります。機密データの調査結果では、タイミングは常に即時です。Macie は、調査結果の処理が終了した直後に機密データの調査結果を発行します。ポリシーの検出結果とは異なり、すべての機密データの検出結果はすべて (一意) として処理されます。

Macie は、suppression rule (抑制ルール) によって自動的にアーカイブされるポリシーや機密データの調査結果を発行しないことに注意してください。つまり、Macie は抑制された調査結果を他の AWS のサービスに発行しません。

トピック

- 調査結果の発行先を選択する
- 調査結果の発行頻度を決定する
- 調査結果の発行頻度を変更する

調査結果の発行先を選択する

Amazon Macie は、Amazon AWS Security Hub に加えて、ポリシーと機密データの検出結果を に自動的に発行するように設定できます EventBridge。デフォルトでは、Macie は新規および更新されたポリシーの調査結果のみを Security Hub に発行します。デフォルトの設定を変更または拡張するには、アカウントの発行先の設定を調整します。

送信先設定を調整するときは、Macie が Security Hub に発行する調査結果のカテゴリを選択します。ポリシーの調査結果のみ、機密データの調査結果のみ、またはポリシーと機密データの調査結果の両方を選択します。調査結果のカテゴリの Security Hub への発行を停止することもできます。

発行先の設定を変更した場合、変更は現在の AWS リージョンにのみ適用されます。ユーザーが組織の Macie 管理者である場合、変更は自分のアカウントにのみ適用されます。関連付けられているメンバーアカウントには適用されません。詳細については、複数のアカウントの管理を参照してください。

調査結果の発行先を選択するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定 を選択します。
3. Publication of findings (調査結果の発行) セクションの Destinations (発行先) の下で、次のオプションから選択します。

    - Security Hub へのポリシーの調査結果の発行 – このチェックボックスをオンにすると、新規および更新されたポリシーの調査結果を Security Hub に自動的に発行できるようになります。Security Hub への新規および更新されたポリシーの調査結果の発行を停止するには、このチェックボックスをオフにします。

このチェックボックスをオンにして既存のポリシーの調査結果がある場合、Macie はそれらを Security Hub に自動的に公開しません。代わりに、Macie は変更を保存した後に作成または更新したポリシーの調査結果のみを公開します。

- 機密データの調査結果を Security Hub に公開する — このチェックボックスをオンにすると、新しい機密データの検出結果を Security Hub に自動的に公開し始めます。Security Hub への新しい機密データの検出結果の発行を停止するには、このチェックボックスをオフにします。

  このチェックボックスをオンにして、既存の機密データの検出結果がある場合、Macie はそれらを Security Hub に自動的に公開しません。代わりに、Macie は変更を保存した後に作成した機密データの調査結果のみを公開します。

4. [保存] を選択します。

Security Hub に任意のカテゴリの結果を発行することを選択した場合は、現在のリージョンで Security Hub も有効にし、Macie からの結果を受け入れるように設定してください。そうしないと、Security Hub の調査結果にアクセスできなくなります。Security Hub で調査結果を受け入れる方法については、AWS Security Hub ユーザーガイドの製品統合の管理を参照してください。

調査結果の発行頻度を決定する

Amazon Macie では、各調査結果に一意の識別子があります。Macie はこの識別子を使用して、別の AWS のサービスに調査結果をいつ公開するかを決定します。

- New findings (新しい調査結果) — Macie が新しいポリシーまたは機密データの調査結果を作成すると、調査結果の処理の一部として一意の識別子が調査結果に割り当てられます。Macie が検出結果の処理を完了するとすぐに、検出結果を新しい Amazon EventBridge イベントとして公開します。アカウントの発行設定に応じて、Macie はその調査結果を新しい調査結果として AWS Security Hubでも発行します。
- 更新された調査結果 – Macie は、既存のポリシーの調査結果のその後の出現を検出すると、その後の出現に関する詳細を追加し、出現の数を増加させて、既存の調査結果を更新します。Macie はこれらの更新を既存の EventBridgeイベントに発行し、アカウントの発行設定に応じて、既存の Security Hub の検出結果にも発行します。Macie は、ポリシーの調査結果についてのみこれを行います。機密データの検出結果は、ポリシーの検出結果とは異なり、すべて新規 (一意) として処理されます。

  デフォルトでは、Macie は定期的な発行サイクルの一部として 15 分ごとに更新された調査結果を発行します。これは、最新の発行サイクル後に更新されたポリシーの調査結果はすべて保持され、

必要に応じて再度更新され、次の発行サイクル (約 15 分後) に含まれることを意味します。このスケジュールを変更するには、別の発行頻度を選択します。たとえば、Macie が 1 時間ごとに更新された結果を発行するように設定し、発行が 12:00 に発生した場合は、12:00 以降に発生するすべての更新は 13:00 に発行されます。

これらのケースはいずれも、抑制ルール によって自動的にアーカイブされる調査結果には適用されないことに注意してください。Macie は抑制された検出結果を他の に公開しません AWS のサービス。

調査結果の発行頻度を変更する

Amazon Macie が他の の既存のポリシーの調査結果に更新を発行するために使用するスケジュールを変更できます AWS のサービス。デフォルトでは、Macie は 15 分ごとに更新された調査結果を発行します。このスケジュールを変更した場合、変更は現在の AWS リージョンにのみ適用されます。ユーザーが組織の Macie 管理者である場合、変更はリージョン内のすべての関連付けられたメンバーアカウントにも適用されます。詳細については、複数のアカウントの管理を参照してください。

更新された調査結果の発行頻度を変更するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ナビゲーションペインで 設定 を選択します。
3. 調査結果の発行 セクションの ポリシーの調査結果の更新頻度 の下で、Macie が更新されたポリシーの調査結果を他の AWS のサービスに発行する頻度を選択します。
4. 保存 を選択します。

Amazon Macie の Amazon EventBridge との統合

以前の Amazon CloudWatch Events である Amazon EventBridge は、サーバーレスイベントバスサービスです。EventBridge は、アプリケーションとサービスからリアルタイムデータのストリームを配信し、そのデータを、AWS Lambda 関数、Amazon Simple Notification Service (Amazon SNS) のトピック、および Amazon Kinesis ストリームなどのターゲットにルーティングします。EventBridge の詳細については、Amazon EventBridge ユーザーガイドを参照してください。

EventBridge を使用すると、特定のタイプのイベントのモニタリングと処理を自動化できます。これには、新しいポリシーの調査結果と機密データの調査結果について Amazon Macie が自動的に発行するイベントが含まれます。これには、Macie が既存のポリシーの調査結果のその後の出現で自動的

に発行するイベントも含まれます。Macie がこれらのイベントを発行する方法とタイミングの詳細については、調査結果の発行設定を設定するを参照してください。

EventBridge と、Macie が調査結果について発行するイベントを使用することで、ほぼリアルタイムで調査結果をモニタリングおよび処理できます。次に、他のアプリケーションやサービスを使用して、調査結果に対してアクションを取ることができます。たとえば、EventBridge を使用して、特定のタイプの新しい調査結果を AWS Lambda 関数に送信することができます。次に、Lambda 関数は、データを処理し、セキュリティインシデントおよびイベント管理 (SIEM) システムに送信する場合があります。AWS User Notifications を Macie と統合すると、イベントを使用して、指定した配信チャネルを通じて検出結果を自動的に通知することもできます。

自動化されたモニタリングと処理に加えて、EventBridge を使用すると、調査結果データの長期保存が可能になります。Macie は 90 日間調査結果を保存します。EventBridge を使用すると、調査結果データを好みのストレージプラットフォームに送信し、データをいつまででも保存できます。

> **Note**
>
> 長期の保持では、機密データの検出結果を S3 バケットに保存するように Macie を設定してください。機密データの検出結果は、Macie が S3 オブジェクトに対して実行した分析に関する詳細を記録するレコードです。詳細については、機密データ検出結果の保存と保持を参照してください。

トピック

- Amazon EventBridge スキーマの使用
- 調査結果用の Amazon EventBridge ルールの作成

Amazon EventBridge スキーマの使用

Amazon EventBridge では、モニタリングするイベントを指定し、それらのイベントに対して自動アクションを実行するターゲットを指定するルールを作成します。ターゲット は、EventBridge がイベントを送信する送信先です。

調査結果のモニタリングと処理タスクを自動化するには、Amazon Macie 調査結果イベントを自動的に検出し、それらのイベントを処理またはその他のアクションのために別のアプリケーションまたはサービスに送信する EventBridge ルールを作成できます。特定の基準を満たすイベントのみを送信するようにルールを調整できます。そのためには、調査結果の EventBridge イベントスキーマから導き出される基準を指定します。

たとえば、特定のタイプの新しい調査結果を AWS Lambda 関数に送信するルールを作成できます。次に、Lambda 関数は、データを処理して SIEM システムへ送信する、S3 オブジェクトに自動的に特定のタイプのサーバー側の暗号化を適用する、オブジェクトのアクセスコントロールリスト (ACL) を変更して S3 オブジェクトへのアクセスを制限するなどのタスクを実行できます。あるいは、新しい高い重要度の調査結果を Amazon SNS トピックに自動的に送信するルールを作成します。これにより、インシデント対応チームに結果を通知することができます。

Lambda 関数の呼び出しと Amazon SNS トピックの通知に加えて、EventBridge は、Amazon Kinesis Streamsへのイベントの中継、AWS Step Functions ステートマシンを起動、AWS Systems Manager実行コマンドを呼び出しなど、他のタイプのターゲットやアクションもサポートしています。詳細については、Amazon EventBridge ユーザーガイド の Amazon EventBridge ターゲット を参照してください 。

調査結果用の Amazon EventBridge ルールの作成

次の手順では、Amazon EventBridge コンソールと AWS Command Line InterfaceAWS CLI を使用して、Macie の調査結果の EventBridge ルールを作成する方法について説明します。ルールは、Macie 調査結果のイベントスキーマとパターンを使用する EventBridge イベントを検出し、それらのイベントを処理のために AWS Lambda 関数に送信します。

AWS Lambda はサーバーをプロビジョニングしたり管理しなくてもコードを実行するために使用できるコンピューティングサービスです。コードをパッケージ化し、Lambda 関数 としてAWS Lambdaにアップロードします。関数が呼び出されるとAWS Lambdaは関数を実行します。関数は、ユーザーが手動で呼び出したり、イベントに応答して自動的に呼び出したり、またはアプリケーションやサービスからのリクエストに応答したりすることができます。Lambda 関数の作成および呼び出しについては、 AWS Lambda 開発者ガイドを参照してください。

Console

この手順では、Amazon EventBridge コンソールを使用して、すべての Macie 調査結果イベントを処理のために Lambda 関数に自動的に送信するルールを作成する方法について説明します。このルールは、特定のイベントを受信したときに実行されるルールのデフォルト設定を使用します。ルール設定の詳細や、カスタム設定を使用するルールの作成方法については、Amazon EventBridge ユーザーガイドのイベントに反応するルールの作成を参照してください。

> **Tip**
>
> カスタムパターンを使用して、Macie 調査結果イベントのサブセットのみを検出して処理するルールを作成することもできます。このサブセットは、Macie が調査結果イベントに

含める特定のフィールドに基づいて作成できます。使用可能なフィールドについては、調査結果の EventBridge イベントスキーマを参照してください。このタイプのルールの作成方法については、Amazon EventBridge ユーザーガイドのイベントパターンのコンテンツフィルタリングを参照してください。

このルールを作成する前に、Lambda 関数を作成して、ルールがターゲットとして使用されるようにします。ルールを作成するときは、この関数をルールのターゲットとして指定する必要があります。

コンソールを使用してイベントのルールを作成するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインの イベント で、ルール を選択します。
3. セクションで、ルールの作成 を選択します。
4. 詳細のルール定義 で、次の操作を行います。
   - 名前 にルールの名前を入力します。
   - 説明 に、認可ルールの簡単な説明を入力します。
   - イベントバスを選択 の下で、 デフォルトのイベントバスが選択され、選択したイベントバスのルールを有効にするがオンになっていることを確認します。
   - ルールタイプ では、イベントパターンを持つルール を選択します。
5. 終了したら、次へ を選択します。
6. イベントパターンの作成 で、次の操作を行います。
   - イベントソース で、AWSイベントまたは EventBridge パートナーイベント ( ) を選択します。
   - (オプショナル) サンプルイベント については、Macie 用のサンプル検索イベントを確認して、イベントに含まれる可能性がある内容を確認してください。そのためには、AWS イベント を選択します。次に、サンプルイベント で Macie 検出結果 を選択します。
   - イベントパターン で、イベントパターンフォーム を選択します。次に、以下の設定を入力します。
     - イベントソース で AWS のサービス を選択します。
     - AWS のサービス にはMacie と入力します。
     - イベントタイプ では、Macie の調査結果 を選択します。

7. 終了したら、次へ を選択します。
8. ターゲットを選択 ページで、次の操作を行います。
   - ターゲットタイプ には、AWS のサービス を選択します。
   - ターゲットを選択) では、(Lambda 関数) を選択します。次に、関数で、結果イベントの送信先となる Lambda 関数を選択します。
   - (オプショナル) バージョン/エイリアスを設定 で、ターゲットの Lambda 関数のバージョンとエイリアスの設定を入力します。
   - (オプショナル) 追加設定 で、Lambda 関数に送信するイベントデータを指定します。関数に正常に配信されないイベントを処理する方法を指定することもできます。
9. 終了したら、次へ を選択します。
10. タグの設定 ページで、ルールに割り当てる 1 つ以上のタグをオプションで入力します。続いて、次へ を選択します。
11. 確認して作成するステップでは、ジョブの設定設定を確認し、それらが正しいことを検証します。

    設定を変更するには、設定が含まれるセクションで 編集を選択し、次に正しい設定を入力します。ナビゲーションタブを使用して、設定が含まれるページに移動することもできます。
12. 設定の確認が完了したら Create rule (ルールの作成) を選択します。

AWS CLI

この手順では、AWS CLI を使用して、すべての Macie 調査結果イベントを処理のために Lambda 関数に送信する EventBridge ルールを作成する方法について説明します。このルールは、特定のイベントを受信したときに実行されるルールのデフォルト設定を使用します。手順では、Microsoft Windows 用にコマンドがフォーマットされています。Linux、macOS、または Unix では、キャレット (^) 行連結文字をバックスラッシュ (\) に置き換えます。

このルールを作成する前に、Lambda 関数を作成して、ルールがターゲットとして使用されるようにします。関数を作成するときは、関数の Amazon リソースネーム (ARN) を書き留めておきます。ルールのターゲットを指定するときに、この ARN を入力する必要があります。

AWS CLI を使用してイベントルールを作成するには

1. Macie が EventBridge に公開するすべての調査結果のイベントを検出するルールを作成します。これを行うには、EventBridge のput-ruleコマンドを使用してください。例:

```
C:\> aws events put-rule ^
--name MacieFindings ^
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

ここで、*Macie ####*はルールに必要な名前です。

コマンドが正常に実行された場合は、ルールの ARN を使用して EventBridge が応答します。この ARN をメモします。それをステップ 3 で入力する必要があります。

> **Tip**
>
> カスタムパターンを使用して、Macie 調査結果イベントのサブセットのみを検出して処理するルールを作成することもできます。このサブセットは、Macie が調査結果イベントに含める特定のフィールドに基づいて作成できます。使用可能なフィールドについては、調査結果の EventBridge イベントスキーマを参照してください。このタイプのルールの作成方法については、Amazon EventBridge ユーザーガイドのイベントパターンのコンテンツフィルタリングを参照してください。

2. ルールのターゲットとして使用する Lambda 関数を指定します。これを行うには、EventBridge のput-targetsコマンドを使用してください。例:

```
C:\> aws events put-targets ^
--rule MacieFindings ^
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-
findings-function
```

ここで、*MacieFindings* は、ステップ 1 でルールに指定した名前で、`Arn` パラメータの値は、ルールでターゲットとして使用する関数の ARN です。

3. ルールがターゲット Lambda 関数を呼び出すことを許可する権限を追加します。これを行うには、Lambdaadd-permissionコマンドを使用します。例:

```
C:\> aws lambda add-permission ^
--function-name my-findings-function ^
--statement-id Sid ^
--action lambda:InvokeFunction ^
--principal events.amazonaws.com ^
--source-arn arn:aws:events:regionalEndpoint:accountId:rule:MacieFindings
```

実行する条件は以下のとおりです。

- *my-findings-function* は、ルールがターゲットとして使用する Lambda 関数の名前です。
- *Sid* は、Lambda 関数ポリシーでステートメントを記述するために定義するステートメント識別子です。
- source-arnは EventBridge ルールの ARN です。

コマンドが正常に実行された場合は、次のような出力が表示されます。

```
{
  "Statement": "{\"Sid\":\"sid\",
    \"Effect\":\"Allow\",
    \"Principal\":{\"Service\":\"events.amazonaws.com\"},
    \"Action\":\"lambda:InvokeFunction\",
    \"Resource\":\"arn:aws:lambda:us-east-1:111122223333:function:my-findings-
function\",
    \"Condition\":
      {\"ArnLike\":
        {\"AWS:SourceArn\":
         \"arn:aws:events:us-east-1:111122223333:rule/MacieFindings\"}}}"
}
```

Statement 値は、Lambda 関数ポリシーに追加されたステートメントの JSON 文字列バージョンです。

Amazon Macie の AWS Security Hub との統合

AWS Security Hub は、AWS 環境全体のセキュリティ体制を包括的に把握し、セキュリティ業界標準およびベストプラクティスに照らして環境をチェックするのに役立つサービスです。これは、複数の AWS のサービス とサポート対象の AWS Partner Network セキュリティソリューションからの検出結果を消費、集約、整理、および優先順位付けすることによって部分的に行われます。Security Hub は、セキュリティの傾向を分析し、特に優先度の高いセキュリティ問題を特定するのに役立ちます。また、Security Hub で複数の AWS リージョン からの検出結果を集約したり、1 つのリージョンから集計した検出結果データをモニタリングおよび処理することもできます。Security Hub の詳細については、AWS Security Hub ユーザーガイドを参照してください。

Amazon Macie は Security Hub と統合します。つまり、Macie から Security Hub に結果を自動的に発行できます。Security Hub では、このような検出結果をセキュリティ体制の分析に含めることができます。さらに、Security Hub を使用して、AWS環境の大規模で集約された検出結果データのセットの一部として、ポリシーと機密データの検出結果をモニタリングおよび処理できます。つまり、組織のセキュリティ体制の広範な分析を実行しながら Macie の検出結果を分析し、必要に応じて検出結果を修正できます。Security Hub は、複数のプロバイダーからの大量の調査結果に対処することの複雑さを低減します。さらに、これは Macie からの検出結果を含むすべての検出結果に標準形式を使用します。この形式、すなわち AWS Security Finding 形式を使用すると、時間のかかるデータ変換作業を実行する必要性を排除します。

トピック

Amazon Macie が検出結果を AWS Security Hub に出力する方法

AWS Security Hub では、セキュリティの問題が検出結果として追跡されます。検出結果の中には、Amazon Macie などの AWS のサービス またはサポート対象の AWS Partner Network セキュリティソリューションによって検出された問題に由来するものがあります。Security Hub には、セキュリティの問題を検出し、検出結果を生成するために使用する一連のルールもあります。

Security Hub には、これらすべてのソースからの調査結果を管理するためのツールが用意されています。検出結果のリストを確認およびフィルタリングして、個々の検出結果の詳細をレビューできます。この方法については、AWS Security Hub ユーザーガイドの検出結果リストと詳細の表示を参照してください。調査結果の調査状況を追跡することもできます この方法については、AWS Security Hub ユーザーガイドの調査結果に対するアクションの実行を参照してください。

Security Hub のすべての調査結果で、AWS Security Finding 形式 (ASFF) と呼ばれる標準の JSON 形式が使用されます。ASFF には、問題のソース、影響を受けるリソース、および調査結果の現在のステータスに関する詳細が含まれます。詳細については、AWS Security Hub ユーザーガイドの AWS Security Finding 形式 (ASFF)を参照してください。

Macie が発行する調査結果のタイプ

Macie アカウント用に選択した発行設定に応じて、Macie は機密データの調査結果とポリシーの調査結果の両方で作成されるすべての調査結果を Security Hub に発行できます。これらの設定とそ

れらの変更方法については、調査結果の発行設定を設定するを参照してください。デフォルトでは、Macie は新規および更新されたポリシーの調査結果のみを Security Hub に発行します。Macie は機密データの調査結果を Security Hub に発行しません。

機密データの調査結果

Macie が 機密データの調査結果を Security Hub に発行するように設定した場合、Macie はアカウントに対して作成された各機密データの調査結果を自動的に発行し、調査結果の処理が終了した直後にそれを行います。Macie は、抑制ルールによって自動的にアーカイブされないすべての機密データの調査結果に対してこれを行います。

ユーザーが組織の Macie 管理者である場合、出力は、Macie の所属組織の機密データ検出活動をユーザーが実行および自動化する機密データ検出ジョブからの検出結果に限定されます。ジョブを作成するアカウントのみが、ジョブが生成する機密データの結果を発行できます。Macie 管理者アカウントのみが、機密データ自動検出によって所属組織用に生成された機密データ検出結果を出力できます。

Macie が機密データの調査結果をSecurity Hub に発行するときに、Security Hub のすべての調査結果に対する標準的な形式である AWS セキュリティ調査結果形式を使用します。ASFF では、Types フィールドは調査結果のタイプを示します。このフィールドでは、Macie での調査結果タイプの分類とは若干異なる分類を使用します。

次のテーブルに、Macie が作成できる機密データの調査結果の各タイプの ASFF 調査結果タイプを示します。

Macie 調査結果タイプ	ASFF 調査結果タイプ
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	Sensitive Data Identifications/PII/SensitiveData:S3Object-CustomIdentifier
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	

Macie 調査結果タイプ	ASFF 調査結果タイプ
	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

ポリシーの調査結果

Macie が ポリシーの調査結果を Security Hub に発行するように設定した場合、Macie は作成した新しい各ポリシーの調査結果を自動的に発行し、調査結果の処理が終了した直後にそれを行います。Macie が既存のポリシーの調査結果のその後の出現を検出した場合、アカウントに指定した発行頻度を使用して、Security Hub の既存の調査結果への更新を自動的に発行します。Macie は、抑制ルールによって自動的にアーカイブされないすべてのポリシーの調査結果に対してこれらのタスクを実行します。

ユーザーが組織の Macie 管理者である場合、出力は、ユーザーのアカウントが直接所有する S3 バケットのポリシー検出結果に制限されます。Macie は、組織内のメンバーアカウントに対して作成または更新したポリシーの調査結果を発行しません。これにより、Security Hub には重複した調査結果データがないことが保証されます。

機密データの調査結果の場合と同様に、Macie は、Security Hub に新規および更新されたポリシーの調査結果を発行するときに、AWS Security Finding Format (ASFF) を使用します。ASFF では、Types フィールドは、Macie での調査結果タイプの分類とは若干異なる分類を使用します。

次のテーブルに、Macie が作成できるポリシーの調査結果の各タイプについて ASFF 調査結果タイプを示します。Macie が 2021 年 1 月 28 日以降に Security Hub でポリシーの調査結果を作成または更新した場合、その調査結果は Security Hub の ASFF Types フィールドに対して次のいずれかの値になります。

Macie 調査結果タイプ	ASFF 調査結果タイプ
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled

Macie 調査結果タイプ	ASFF 調査結果タイプ
Policy:IAMUser/S3BucketEncryptionDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketEncryptionDisabled
Policy:IAMUser/S3BucketPublic	Effects/Data Exposure/Policy:IAMUser-S3BucketPublic
Policy:IAMUser/S3BucketReplicatedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketReplicatedExternally
Policy:IAMUser/S3BucketSharedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedExternally
Policy:IAMUser/S3BucketSharedWithCloudFront	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedWithCloudFront

Macie が 2021 年 1 月 28 日より前にポリシーの調査結果を作成または更新した場合、その調査結果は Security Hub の ASFF Types フィールド に対して次のいずれかの値になります。

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

前のリストの値は、Macieの 調査結果タイプ(type) フィールドの値に直接マッピングされます。

> **Note**
>
> Security Hub でポリシーの調査結果を確認して処理するときは、次の例外に注意してください。
>
> - 特定の AWS リージョン で、早くも 2021 年 1 月 25 日に Macie は新規および更新された検出結果用の ASFF 検出結果タイプを使用開始しました。
> - Macie がユーザーの AWS リージョン で ASFF 検出結果タイプの使用を開始する前に、ユーザーが Security Hub でポリシーの検出結果を処理した場合、その ASFF Types フィールドの値は、前のリストの Macie 検出結果タイプのいずれかになります。それは、前のテーブルの ASFF 調査結果タイプのいずれかにはなりません。これは、AWS Security Hub コンソールまたは AWS Security Hub APIの BatchUpdateFindings オペレーションを使用して処理したポリシーの調査結果に当てはまります。

調査結果のレイテンシー

Macie が新しいポリシーまたは機密データの調査結果を作成するときに、調査結果の処理が終了した直後に Security Hub にその調査結果を発行します。

Macie が既存のポリシー結果のその後の出現を検出したときに、既存の Security Hub の調査結果への更新を発行します。更新のタイミングは、Macie アカウントで選択した発行頻度によって異なります。デフォルトでは、Macie は 15 分ごとに更新を発行します。アカウントの設定を変更する方法など、詳細については、調査結果の発行設定を設定するを参照してください。

Security Hub が使用できないときに発行を再試行する

Security Hub が使用できない場合、Macie は Security Hub によって受信されていない調査結果のキューを作成します。システムが復元されると、Macie は結果が Security Hub によって受信されるまで、発行を再試行します。

Security Hub の既存の調査結果を更新する

Macie がポリシーの調査結果を Security Hub に発行した後、Macie は調査結果を更新して、調査結果または調査結果アクティビティの追加の出現を反映します。Macie は、ポリシーの調査結果についてのみこれを行います。機密データの検出結果は、ポリシーの検出結果とは異なり、すべて新規 (一意) として処理されます。

Macie がポリシー結果への更新を発行するときに、Macie は、調査結果の 更新時刻UpdatedAtのフィールド値を更新します。この値を使用して、検出結果を生成した潜在的なポリシー違反または問題のその後の出現を Macie が最後に検出したタイミングを判断できます。

Macie は、フィールドの既存の値が ASFF 調査結果タイプではない場合、調査結果の タイプTypesフィールドの値も更新する場合があります。これは、Security Hub での調査結果に基づいて処理したかどうかによって異なります。調査結果を処理していない場合、Macie はフィールドの値を適切な ASFF 調査結果タイプに変更します。AWS Security Hub コンソールまたは AWS Security Hub APIの BatchUpdateFindings オペレーションのいずれかを使用して、調査結果の処理をした場合、Macie はフィールドの値を変更しません。

AWS Security Hub での Amazon Macie の検出結果の例

Amazon Macie が検出結果を AWS Security Hub に出力するときは、AWS Security Finding Format (ASFF) を使用します。これは、Security Hub のすべての調査結果に対する標準形式です。次の例では、サンプルデータを使用して、Macie がこの形式で Security Hub に発行する調査結果データの構造と性質を示します。

- 機密データの調査結果の例
- ポリシーの調査結果の例

Security Hub での機密データの調査の例

以下に、Macie が ASFF を使用してSecurity Hub に発行した機密データの調査結果の例を示します。

```
{
    "SchemaVersion": "2018-10-08",
    "Id": "5be50fce24526e670df77bc00example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types":[
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
    ],
    "CreatedAt": "2022-05-11T10:23:49.667Z",
    "UpdatedAt": "2022-05-11T10:23:49.667Z",
```

```
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "The S3 object contains personal information.",
    "Description": "The object contains personal information such as first or last
 names, addresses, or identification numbers.",
    "ProductFields": {
        "JobArn": "arn:aws:macie2:us-east-1:111122223333:classification-
job/698e99c283a255bb2c992feceexample",
        "S3Object.Path": "DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
        "S3Object.Extension": "tsv",
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "OriginType": "SENSITIVE_DATA_DISCOVERY_JOB",
        "S3Object.PublicAccess": "false",
        "S3Object.Size": "14",
        "S3Object.StorageClass": "STANDARD",
        "S3Bucket.allowsUnencryptedObjectUploads": "TRUE",
        "JobId": "698e99c283a255bb2c992feceexample",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/5be50fce24526e670df77bc00example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
            "Type": "AwsS3Bucket",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "Partition": "aws",
            "Region": "us-east-1",
            "Details": {
                "AwsS3Bucket": {
                    "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
                    "OwnerName": "johndoe",
                    "OwnerAccountId": "444455556666",
                    "CreatedAt": "2020-12-30T18:16:25.000Z",
                    "ServerSideEncryptionConfiguration": {
                        "Rules": [
                            {
                                "ApplyServerSideEncryptionByDefault": {
                                    "SSEAlgorithm": "aws:kms",
                                    "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
```

```
                                }
                            }
                        ]
                    },
                    "PublicAccessBlockConfiguration": {
                        "BlockPublicAcls": true,
                        "BlockPublicPolicy": true,
                        "IgnorePublicAcls": true,
                        "RestrictPublicBuckets": true
                    }
                }
            }
        },
        {
            "Type": "AwsS3Object",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
            "Partition": "aws",
            "Region": "us-east-1",
            "DataClassification": {
                "DetailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/111122223333/Macie/us-east-1/
                698e99c283a255bb2c992feceexample/111122223333/32b8485d-4f3a-3aa1-be33-
aa3f0example.jsonl.gz",
                "Result":{
                    "MimeType": "text/tsv",
                    "SizeClassified": 14,
                    "AdditionalOccurrences": false,
                    "Status": {
                        "Code": "COMPLETE"
                    },
                    "SensitiveData": [
                        {
                            "Category": "PERSONAL_INFORMATION",
                            "Detections": [
                                {
                                    "Count": 1,
                                    "Type": "USA_SOCIAL_SECURITY_NUMBER",
                                    "Occurrences": {
                                        "Cells": [
                                            {
                                                "Column": 10,
                                                "Row": 1,
                                                "ColumnName": "Other"
                                            }
```

```
                                    ]
                                }
                            }
                        ],
                        "TotalCount": 1
                    }
                ],
                "CustomDataIdentifiers": {
                    "Detections": [
                    ],
                    "TotalCount": 0
                }
            }
        },
        "Details": {
            "AwsS3Object": {
                "LastModified": "2022-04-22T18:16:46.000Z",
                "ETag": "ebe1ca03ee8d006d457444445example",
                "VersionId": "SlBC72z5hArgexOJifxw_IN57example",
                "ServerSideEncryption": "aws:kms",
                "SSEKMSKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            }
        }
    }
],
"WorkflowState": "NEW",
"Workflow": {
    "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
    "Severity": {
        "Label": "HIGH"
    },
    "Types": [
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
    ]
},
"Sample": false,
"ProcessedAt": "2022-05-11T10:23:49.667Z"
}
```

Security Hub でのポリシーの調査結果の例

以下に、Macie が ASFF で Security Hub に発行した新しいポリシーの調査結果の例を示します。


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "36ca8ba0-caf1-4fee-875c-37760example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-
S3BlockPublicAccessDisabled"
    ],
    "CreatedAt": "2022-04-24T09:27:43.313Z",
    "UpdatedAt": "2022-04-24T09:27:43.313Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "Block Public Access settings are disabled for the S3 bucket",
    "Description": "All Amazon S3 block public access settings are disabled for the
 Amazon S3 bucket. Access to the bucket is
      controlled only by access control lists (ACLs) or bucket policies.",
    "ProductFields": {
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "S3Bucket.allowsUnencryptedObjectUploads": "FALSE",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/36ca8ba0-caf1-4fee-875c-37760example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
        "Type": "AwsS3Bucket",
        "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
        "Partition": "aws",
        "Region": "us-east-1",
        "Tags": {
            "Team": "Recruiting",
            "Division": "HR"
```

```
        },
        "Details": {
            "AwsS3Bucket": {
              "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
              "OwnerName": "johndoe",
              "OwnerAccountId": "444455556666",
              "CreatedAt": "2020-11-25T18:24:38.000Z",
              "ServerSideEncryptionConfiguration": {
                "Rules": [
                    {
                    "ApplyServerSideEncryptionByDefault": {
                        "SSEAlgorithm": "aws:kms",
                        "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                    }
                  }
                ]
              },
              "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": false,
                "BlockPublicPolicy": false,
                "IgnorePublicAcls": false,
                "RestrictPublicBuckets": false
               }
            }
         }
      }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Software and Configuration Checks/AWS Security Best Practices/
Policy:IAMUser-S3BlockPublicAccessDisabled"
        ]
    },
    "Sample": false
```

```
}
```

AWS Security Hub 統合の有効化と設定

Amazon Macie を と統合するにはAWS Security Hub、 の Security Hub を有効にしますAWS アカウント。この方法については、「 ユーザーガイド」の「Security Hub の有効化AWS Security Hub」を参照してください。

Macie と Security Hub の両方を有効化すると、統合は自動的に有効化されます。デフォルトでは、Macie は新規および更新されたポリシーの調査結果を Security Hub に自動的に発行し始めます。統合を設定するために追加の手順を実行する必要はありません。統合が有効になっているときに既存のポリシーの調査結果がある場合、Macie はそれらを Security Hub に公開しません。代わりに、Macie は統合が有効になった後に作成または更新したポリシーの調査結果のみを公開します。

必要に応じて、Macie が Security Hub でポリシーの調査結果に対する更新を発行する頻度を選択して、設定をカスタマイズできます。機密データの検出結果を Security Hub に発行することもできます。この方法の詳細は、調査結果の発行設定を設定するを参照してください。

AWS Security Hub への検出結果出力の停止

AWS Security Hub への検出結果の出力を停止するには、Amazon Macie アカウントの出力設定を変更します。この方法の詳細は、調査結果の発行先を選択するを参照してください。これは、Security Hub コンソールまたはSecurity Hub API を使用しても実行できます。詳細については、統合からの調査結果のフローの無効化と有効化 (コンソール)または AWS Security Hub ユーザーガイドの統合からの調査結果のフローの無効化 (Security Hub API、AWS CLI)を参照してください 。

Amazon Macie の AWS User Notifications との統合

AWS User Notifications は、AWS Management Console での AWS 通知を一元的に管理するサービスです。これには、Amazon CloudWatch のアラーム、AWS Support ケース、他のユーザーからの通信などの通知が含まれます。AWS のサービスユーザー通知では、特定の種類の Amazon EventBridge イベントに関する通知を受信するためのカスタムルールと配信チャネルを設定できます。配信チャネルには、E メール、AWS Chatbot チャット通知、AWS Console Mobile Application プッシュ通知が含まれます。AWS User Notifications コンソールで通知を確認することもできます。ユーザー通知の詳細については、AWS User Notifications ユーザーガイドを参照してください。

Macie は AWS User Notifications と統合されているため、ポリシーや機密データの検出結果について Macie が EventBridge に公開するイベントを通知するようにユーザー通知を設定できます。検索イベントが指定した条件に一致すると、ユーザー通知によって通知が生成されます。通知には、検出

結果のタイプや重要度、影響を受けるリソースの名前など、関連する結果の重要な詳細が含まれます。ユーザー通知は、指定した 1 つ以上の配信チャネルに通知を送信することもできます。セキュリティとコンプライアンスのワークフローに合わせて、選択した配信チャネルを調整できます。

たとえば、特定のタイプの新しい重要度の高い検出結果に関する通知を生成するようにユーザー通知を設定できます。また、これらの通知の配信チャネルとして AWS Chatbot を指定することもできます。次に、ユーザー通知は結果の EventBridge イベントを検出し、結果からのデータを含む通知を生成し、通知を AWS Chatbot に送信します。その後、AWS Chatbot は通知を Slack チャネルまたは Amazon Chime チャットルームに転送して、インシデント対応チームに通知します。

トピック

AWS User Notifications の使用

AWS User Notifications では、モニタリングし、通知を受信する Amazon EventBridge イベントのタイプを指定するルールを作成します。ルールは、通知を生成するために EventBridge イベントが一致しなければならない条件を定義します。ルールには 1 つ以上の配信チャネルを選択することもできます。配信チャネルでは、ルールの条件に一致するイベントの通知を受信する場所を指定します。

ユーザー通知がルールの条件に一致する EventBridge イベントを検出すると、次の一般的なタスクが実行されます。

1. イベントからデータのサブネットを抽出します。
2. 抽出されたデータを含む通知を生成します。
3. そのタイプのイベント用に指定した配信チャネルに通知を送信します。

通知のデザインと構造は、送信先の配信チャネルごとに最適化されます。

受信する通知の頻度や数を制御するには、ルールの集計設定を設定できます。これらの設定を有効にすると、ユーザー通知は複数のイベントのデータを 1 つの通知にまとめます。集約されたイベント通知を迅速かつ頻繁に送信するように選択できます。これは、重要度の高いイベントを検索する場合に便利です。または、送信頻度を減らして受け取る通知の数を減らすこともできます。これは、重要

度が低い検出イベントに対して行うとよいでしょう。イベントデータを組み合わせると、AWS User Notifications コンソールを使用して集計された各イベントの詳細をドリルダウンして確認できます。そこから、Amazon Macie コンソール上の関連する検出結果に移動することもできます。

Amazon Macie に関する AWS User Notifications の有効化と設定に関する検出結果

AWS User Notifications で Amazon Macie の検出結果に関する通知を生成できるようにするには、ユーザー通知で Macie の通知設定を作成します。通知設定はルールの基準を指定します。また、ルールの条件に一致する Amazon EventBridge イベントを監視して通知を送信するための配信チャネルやその他の設定も指定します。通知設定の作成の詳細については、AWS User Notifications ユーザーガイドの AWS User Notifications の使用開始を参照してください。

Macie の結果の通知設定を作成するには、イベントルールで以下のオプションを選択します。

- AWS のサービスサービス名 では Macie を選択します。
- イベントタイプ では、Macie の調査結果 を選択します。
- リージョン では、Macie を使用していて、結果の通知を受け取りたい地域をそれぞれ AWS リージョン を選択します。

この設定では、ユーザー通知は AWS アカウント の EventBridge イベントを監視し、選択したリージョン内のすべての Macie Finding イベントに関する通知を生成します。イベントは、以下の条件に一致します。

- `source`が`aws.macie`
- `detail-type`が`Macie Finding`

イベントルールの基になる JSON パターンは次のとおりです。

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"]
}
```

ルールを絞り込み、結果のサブセットのみの通知を生成するには、ルールの JSON パターンをカスタマイズできます。これを行うには、 Macie の調査結果の EventBridge イベントスキーマ から派生する基準を指定します。

カスタム JSON パターンを使用するルールを作成すると、Macie の結果に対して複数の通知設定を作成できます。その後、特定のタイプの調査結果のセキュリティとコンプライアンスのワークフローに合わせて、設定ごとに配信チャネルやその他の設定を調整できます。

たとえば、Macie がPolicy:IAMUser/S3BucketPublic検出結果を生成または更新した場合に通知する 1 つのルールを作成できます。この場合、ルールのパターンは次のようになります。

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": ["Policy:IAMUser/S3BucketPublic"]
    }
}
```

また、Macie がパブリックにアクセス可能な S3 バケットの機密データ検出結果を生成した場合に通知する別のルールを作成することもできます。この場合、ルールのパターンは次のようになります。

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": [ { "prefix": "SensitiveData" } ],
        "resourcesAffected": {
            "effectivePermission": ["PUBLIC"]
        }
    }
}
```

Macie の結果に対して複数の通知設定を作成する場合は、各設定のルールが固有であることを確認するとよいでしょう。それ以外の場合は、個別の検出結果の通知が重複する場合があります。

ルールのイベントパターンのカスタマイズについて詳しくは、User Notifications ユーザーガイドのカスタマイズされた JSON イベントパターンの使用を参照してください。

AWS User Notifications フィールドを Amazon Macie の検索フィールドにマッピングする

AWS User Notifications が Amazon Macie の検出結果に関する通知を生成すると、対応する Amazon EventBridge イベントのフィールドのサブセットからのデータが通知に入力されます。これらの

フィールドには、結果のタイプや重大度、影響を受けるリソースの名前など、関連する結果の重要な詳細が表示されます。

AWS User Notifications コンソールで通知を確認すると、通知にはこのフィールドのサブセットのすべてのデータが含まれます。Amazon Macie コンソール内の関連する調査結果へのリンクも提供します。他の配信チャネルの通知を確認すると、その通知には一部のフィールドのデータしか含まれていない可能性があります。これは、ユーザー通知は、サポートする各タイプの配信チャネルに合わせて通知のデザインと構造を調整するためです。

以下のテーブルには、結果の通知に含まれる可能性のあるフィールドが一覧表示されます。このテーブルには、通知フィールド 列には、通知に含まれるフィールドの説明 (イタリック体) または名前を示しています。調査結果イベントフィールド の列は、EventBridge イベント内の対応する JSON フィールドの名前を示すために、ドット表記を使用します。説明列には、フィールドに保存されているデータが説明されています。

通知フィールド	イベントフィールドの検索	説明
メッセージヘッドライン	`detail.type`	結果のタイプ。 たとえば、`Policy:IAMUser/S3BucketPublic` 、`Sensitive Data:S3Object/Financial` などです。
概要	`detail.title`	検出結果の簡単な説明。 例: `The S3 object contains financial information.`
説明	`detail.description`	結果の詳細な説明 例: `The S3 object contains financial information such as bank account numbers or credit card numbers.`

通知フィールド	イベントフィールドの検索	説明
緊急度	detail.severity.description	調査結果の重要度の定性的表現: Low、MediumまたはHigh。
検出結果 ID	detail.id	フィルターの一意の識別子。
作成	detail.createdAt	Macie が調査結果を作成した日時。
更新	detail.updatedAt	Macie が検出結果を直近に更新した日時。 機密データの調査結果では、この値は作成detail.createdAt 日時フィールドの値と同じです。機密データの検出結果は、新規 (一意) とみなされます。
影響を受ける S3 バケット	detail.resourcesAffected.s3Bucket.arn	影響を受ける S3 バケットの Amazon リソースネーム (ARN)。
影響を受ける S3 オブジェクト	detail.resourcesAffected.s3Object.path	オブジェクトを格納するバケットの名前と、該当する場合はオブジェクトのプレフィックスが含む、影響を受けた S3 オブジェクトの名前キー。 このフィールドはポリシー検出結果の通知には含まれません。

通知フィールド	イベントフィールドの検索	説明

機密データの検出	`detail.classificationDetails.result.sensitiveData.detections...`
	
	And/Or
	
	`detail.classificationDetails.result.customDataIdentifiers.detections...`
		これは、機密データが見つかった場合のイベント内の複数のフィールドを連結したものです。このフィールドはポリシー検出結果の通知には含まれません。
		
		マネージドデータ識別子が機密データを検出した場合、このフィールドには検出された機密データのカテゴリ、タイプ、および出現回数count を指定します。例: `PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences` 。
		
		カスタムデータ識別子が機密データを検出した場合、このフィールドにはカスタムデータ識別子の名前と検出された機密データの出現回数count を指定します。例: `Employee ID 20 occurrences` 。
		
		結果から複数のタイプの機密データが報告される場合、通知には最大 4 種類のデータが含まれます。データは最初に該当するカスタムデータ識別子によって入力され、次に該当するマネージドデータ識別子によって入力されます。

Amazon Macie の検出結果に対する AWS User Notifications の設定を変更する

Amazon Macie 検出結果の AWS User Notifications 設定は、いつでも変更できます。そのためには、ユーザー通知設定を編集します。方法については、AWS User Notifications ユーザーガイドの通知設定の管理を参照してください。

Macie の検出結果に対して複数の通知設定がある場合、1 つの設定を変更しても他の設定の設定には影響しません。すべての設定を編集することも、一部の設定のみを編集することもできます。

Amazon Macie 検出結果に対する AWS User Notifications を無効化する

Amazon Macie の AWS User Notifications の検出結果からの通知の生成と受信を停止するには、ユーザー通知の通知設定を削除します。方法については、AWS User Notifications ユーザーガイドの通知設定の管理を参照してください。

Macie の結果に対して複数の通知設定がある場合、1 つの設定を削除しても他の設定には影響しません。すべての設定を削除することも、一部の設定のみを削除することもできます。

Amazon Macie の調査結果の Amazon EventBridge イベントスキーマ

モニタリングやイベント管理システムなど、他のアプリケーション、サービス、およびシステムとの統合をサポートするために、Amazon Macie は調査結果をイベントとして Amazon EventBridge に自動的に発行します。以前の Amazon CloudWatch Events である Amazon EventBridge は、アプリケーションや他の AWS のサービス からのリアルタイムのデータのストリーミングを AWS Lambda 関数、Amazon Simple Notification Service のトピック、および Amazon Kinesis ストリームなどのターゲットに配信するサーバーレスイベントバスサービスです。EventBridge の詳細については、Amazon EventBridge ユーザーガイドを参照してください。

> **Note**
>
> CloudWatch Events を現在使用している場合は、EventBridge イベントと CloudWatch イベントは同じ基盤となるサービスと API であることに注意してください。ただし、EventBridge には、SaaS (software as a service) アプリケーションやユーザー独自のアプリケーションからイベントを受け取ることができる追加機能が含まれています。基盤となるサービスと API が同じであるため、Macie の調査結果のイベントスキーマも同じです。

Macie は、新しい検出結果およびその後の既存のポリシーの検出結果に関するイベントを発行しますが、抑制ルールを使用して自動的にアーカイブする検出結果を除きます。イベントは、AWS イベントの EventBridge スキーマに準拠する JSON オブジェクトです。各イベントには、特定の検出結果の JSON 表現が含まれます。データは EventBridge イベントとして設定されているため、他のアプリケーション、サービス、およびツールを使用して、より簡単に検出結果をモニタリングおよび処理し、その検出結果に基づいて対応できます。Macie が検出結果についてのイベントを発行する方法とタイミングの詳細については、「調査結果の発行設定を設定する」を参照してください。

トピック

イベントスキーマ

次の例は、Amazon Macie の検出結果についての Amazon EventBridge イベントのスキーマを示しています。調査結果イベントに含めることができるフィールドの詳細な説明については、Amazon Macie API リファレンスの調査結果を参照してください。調査結果イベントの構造とフィールドは、Amazon Macie API の調査結果オブジェクトの近くにマッピングされます。

```
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "AWS ##### ID (string)",
    "time": "event timestamp (string)",
    "region": "AWS ##### (string)",
    "resources": [
        <-- ARNs of the resources involved in the event -->
    ],
    "detail": {
        <-- Details of a policy or sensitive data finding -->
    },
    "policyDetails": null, <-- Additional details of a policy finding or null for a
 sensitive data finding -->
    "sample": Boolean,
    "archived": Boolean
}
```

ポリシーの調査結果のイベント例

次の例では、サンプルデータを使用して、ポリシーの調査結果の Amazon EventBridge イベント内のオブジェクトとフィールドの構造と性質を示します。

この例では、イベントは既存のポリシーのその後の出現をレポートします。S3 バケットのパブリックアクセスブロック設定が無効になっています。次のフィールドと値は、これが当てはまるかどうかを判断するのに役立ちます。

- type フィールドは Policy:IAMUser/S3BlockPublicAccessDisabled に設定されます。
- createdAt と updatedAt フィールドは異なる値を持ちます。これは、イベントが既存のポリシーの調査結果のその後の出現をレポートする指標の 1 つです。イベントで新しい調査結果がレポートされた場合、これらのフィールドの値は同じになります。
- count フィールドは 2 に設定されます。これは、それが調査結果の 2 回目の出現であることを示しています。
- category フィールドは POLICY に設定されます。
- classificationDetails フィールドの値は null です。これは、ポリシーの調査結果のこのイベントと、機密データの調査結果のイベントを区別するのに役立ちます。機密データの調査結果では、この値は、機密データを見つけた方法と種類に関する情報を提供するオブジェクトとフィールドのセットになります。

sample フィールドの値は true であることにも注意してください。この値は、これがドキュメントで使用するイベント例であることを強調しています。

```
{
    "version": "0",
    "id": "0948ba87-d3b8-c6d4-f2da-732a1example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2021-04-30T23:12:15Z",
    "region":"us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "64b917aa-3843-014c-91d8-937ffexample",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
```

```
        "type": "Policy:IAMUser/S3BlockPublicAccessDisabled",
        "title": "Block public access settings are disabled for the S3 bucket",
        "description": "All bucket-level block public access settings were disabled for
 the S3 bucket. Access to the bucket is controlled by account-level block public access
 settings, access control lists (ACLs), and the bucket's bucket policy.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2021-04-29T15:46:02Z",
        "updatedAt": "2021-04-30T23:12:15Z",
        "count": 2,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
                "name": "DOC-EXAMPLE-BUCKET1",
                "createdAt": "2020-04-03T20:46:56.000Z",
                "owner":{
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags": [
                    {
                        "key": "Division",
                        "value": "HR"
                    },
                    {
                        "key": "Team",
                        "value": "Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
```

```
                        "bucketPolicy": {
                            "allowsPublicReadAccess": false,
                            "allowsPublicWriteAccess": false
                        },
                        "blockPublicAccess": {
                            "ignorePublicAcls": false,
                            "restrictPublicBuckets": false,
                            "blockPublicAcls": false,
                            "blockPublicPolicy": false
                        }
                    },
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "ignorePublicAcls": true,
                            "restrictPublicBuckets": true,
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true
                        }
                    }
                },
                "effectivePermission": "NOT_PUBLIC"
            },
            "allowsUnencryptedObjectUploads": "FALSE"
        },
        "s3Object": null
    },
    "category": "POLICY",
    "classificationDetails": null,
    "policyDetails": {
        "action": {
            "actionType": "AWS_API_CALL",
            "apiCallDetails": {
                "api": "PutBucketPublicAccessBlock",
                "apiServiceName": "s3.amazonaws.com",
                "firstSeen": "2021-04-29T15:46:02.401Z",
                "lastSeen": "2021-04-30T23:12:15.401Z"
            }
        },
        "actor": {
            "userIdentity": {
                "type": "AssumedRole",
                "assumedRole": {
                    "principalId": "AROA1234567890EXAMPLE:AssumedRoleSessionName",
```

```
                        "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
                        "accountId": "111122223333",
                        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                        "sessionContext": {
                            "attributes": {
                                "mfaAuthenticated": false,
                                "creationDate": "2021-04-29T10:25:43.511Z"
                            },
                            "sessionIssuer": {
                                "type": "Role",
                                "principalId": "AROA1234567890EXAMPLE",
                                "arn": "arn:aws:iam::123456789012:role/
RoleToBeAssumed",
                                "accountId": "123456789012",
                                "userName": "RoleToBeAssumed"
                            }
                        }
                    },
                    "root": null,
                    "iamUser": null,
                    "federatedUser": null,
                    "awsAccount": null,
                    "awsService": null
                },
                "ipAddressDetails":{
                    "ipAddressV4": "192.0.2.0",
                    "ipOwner": {
                        "asn": "-1",
                        "asnOrg": "ExampleFindingASNOrg",
                        "isp": "ExampleFindingISP",
                        "org": "ExampleFindingORG"
                    },
                    "ipCountry": {
                        "code": "US",
                        "name": "United States"
                    },
                    "ipCity": {
                        "name": "Ashburn"
                    },
                    "ipGeoLocation": {
                        "lat": 39.0481,
                        "lon": -77.4728
                    }
```

```
                },
                "domainDetails": null
            }
        },
        "sample": true,
        "archived": false
    }
}
```

機密データの調査結果のイベント例

次の例では、サンプルデータを使用して、機密データの調査結果の Amazon EventBridge イベント内のオブジェクトとフィールドの構造と性質を示します。

この例では、イベントは新しい機密データの調査結果をレポートします。Amazon Macieは、S3 オブジェクト内で複数のカテゴリの機密データを見つけました。次のフィールドと値は、これが当てはまるかどうかを判断するのに役立ちます。

- type フィールドは SensitiveData:S3Object/Multiple に設定されます。
- createdAt と updatedAt フィールドは同じ値を持ちます。ポリシーの調査結果とは異なり、機密データの調査結果では常にこれが当てはまります。すべての機密データの検出結果は、新規とみなされます。
- count フィールドは 1 に設定されます。これは、それが新しい調査結果であることを示しています。ポリシーの調査結果とは異なり、機密データの調査結果では常にこれが当てはまります。すべての機密データの検出結果は、一意 (新規) とみなされます。
- category フィールドは CLASSIFICATION に設定されます。
- policyDetails フィールドの値は null です。これは、機密データの調査結果のこのイベントと、ポリシーの調査結果のイベントを区別するのに役立ちます。ポリシーの調査結果では、この値は、S3 バケットのセキュリティまたはプライバシーに関するポリシー違反やポリシーの問題の可能性に関する情報を提供するオブジェクトとフィールドのセットになります。

sample フィールドの値は true であることにも注意してください。この値は、これがドキュメントで使用するイベント例であることを強調しています。

```
{
    "version": "0",
    "id": "14ddd0b1-7c90-b9e3-8a68-6a408example",
    "detail-type": "Macie Finding",
```

```
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2022-04-20T08:19:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "4ed45d06-c9b9-4506-ab7f-18a57example",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "SensitiveData:S3Object/Multiple",
        "title": "The S3 object contains multiple categories of sensitive data",
        "description": "The S3 object contains more than one category of sensitive
data.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2022-04-20T18:19:10Z",
        "updatedAt": "2022-04-20T18:19:10Z",
        "count": 1,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "name": "DOC-EXAMPLE-BUCKET2",
                "createdAt": "2020-05-15T20:46:56.000Z",
                "owner": {
                    "displayName": "johndoe",
                    "id":
"7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
```

```
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy":{
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "TRUE"
            },
            "s3Object":{
                "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "key": "2022 Sourcing.csv",
                "path": "DOC-EXAMPLE-BUCKET2/2022 Sourcing.csv",
                "extension": "csv",
                "lastModified": "2022-04-19T22:08:25.000Z",
                "versionId": "",
                "serverSideEncryption": {
                    "encryptionType": "aws:kms",
```

```
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "size": 4750,
                "storageClass": "STANDARD",
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "publicAccess": false,
                "etag": "6bb7fd4fa9d36d6b8fb8882caexample"
            }
        },
        "category": "CLASSIFICATION",
        "classificationDetails": {
            "jobArn": "arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample",
            "jobId": "3ce05dbb7ec5505def334104bexample",
            "result": {
                "status": {
                    "code": "COMPLETE",
                    "reason": null
                },
                "sizeClassified": 4750,
                "mimeType": "text/csv",
                "additionalOccurrences": true,
                "sensitiveData": [
                    {
                        "category": "PERSONAL_INFORMATION",
                        "totalCount": 65,
                        "detections": [
                            {
                                "type": "USA_SOCIAL_SECURITY_NUMBER",
                                "count": 30,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
                                    "pages": null,
```

```
                "records": null,
                "cells": [
                    {
                        "row": 2,
                        "column": 1,
                        "columnName": "SSN",
                        "cellReference": null
                    },
                    {
                        "row": 3,
                        "column": 1,
                        "columnName": "SSN",
                        "cellReference": null
                    },
                    {
                        "row": 4,
                        "column": 1,
                        "columnName": "SSN",
                        "cellReference": null
                    }
                ]
            }
        },
        {
            "type": "NAME",
            "count": 35,
            "occurrences": {
                "lineRanges": null,
                "offsetRanges": null,
                "pages": null,
                "records": null,
                "cells": [
                    {
                        "row": 2,
                        "column": 3,
                        "columnName": "Name",
                        "cellReference": null
                    },
                    {
                        "row": 3,
                        "column": 3,
                        "columnName": "Name",
                        "cellReference": null
                    }
```

```
                                ]
                            }
                        }
                    ]
                },
                {
                    "category": "FINANCIAL_INFORMATION",
                    "totalCount": 30,
                    "detections": [
                        {
                            "type": "CREDIT_CARD_NUMBER",
                            "count": 30,
                            "occurrences": {
                                "lineRanges": null,
                                "offsetRanges": null,
                                "pages": null,
                                "records": null,
                                "cells": [
                                    {
                                        "row": 2,
                                        "column": 14,
                                        "columnName": "CCN",
                                        "cellReference": null
                                    },
                                    {
                                        "row": 3,
                                        "column": 14,
                                        "columnName": "CCN",
                                        "cellReference": null
                                    }
                                ]
                            }
                        }
                    ]
                }
            ],
            "customDataIdentifiers": {
                "totalCount": 0,
                "detections": []
            }
        },
        "detailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/123456789012/Macie/us-east-1/3ce05dbb7ec5505def334104bexample/
d48bf16d-0deb-3e49-9d8c-d407cexample.jsonl.gz",
```

```
            "originType": "SENSITIVE_DATA_DISCOVERY_JOB"
        },
        "policyDetails": null,
        "sample": true,
        "archived": false
    }
}
```

Amazon Macie のコストの予測とモニタリング

Amazon Macie の使用にかかるコストを予測およびモニタリングするために、Macie はアカウントの推定使用コストを計算して提供します。このデータを使用して、サービスの使用量またはアカウントクォータを調整するかどうかを判断できます。現在 Macie 30 日間無料トライアルに参加している場合は、このデータを使用して、無料トライアル終了後に Macie 使用コストを見積もることができます。トライアルのステータスを確認することもできます。

Amazon Macie コンソールで推定使用コストを確認し、Amazon Macie API を使用してプログラムでアクセスできます。お客様が組織の Macie 管理者である場合は、組織の集計データと組織内のアカウントのデータの内訳の両方を確認してアクセスできます。

Macie が提供する推定使用コストに加えて、 を使用して実際のコストを確認およびモニタリングできます AWS Billing and Cost Management。 のコストを追跡および分析し AWS のサービス、アカウントまたは組織の予算を管理するのに役立つ機能 AWS Billing and Cost Management を提供します。また、履歴データに基づいて使用コストを予測するのに役立つ機能も提供します。詳細については、AWS Billing ユーザーガイドを参照してください。

トピック

- Amazon Macie の推定使用コスト計算方法を理解する
- Amazon Macie で推定使用コストを確認する
- Amazon Macie 無料トライアルに参加する

Amazon Macie の推定使用コスト計算方法を理解する

Amazon Macie の料金は、以下の体系に基づいています。

予防的制御のモニタリング

これらのコストは、Amazon Simple Storage Service (Amazon S3) 汎用バケットのインベントリを維持し、セキュリティとアクセスコントロールのためにバケットを評価およびモニタリングすることから発生します。詳細については、「Macie が Amazon S3 データセキュリティをモニタリングする方法」を参照してください。

Macie がアカウントでモニタリングする S3 汎用バケットの合計数に基づいて課金されます。料金は 1 日あたりの日割り計算です。

機密データを自動検出するためのオブジェクト監視

これらのコストは、S3 バケットインベントリを監視および評価して、機密データ自動検出による分析の対象となる S3 オブジェクトを特定することから発生します。詳細については、「機密データの自動検出の仕組み」を参照してください。

Macie がアカウントでモニタリングする汎用バケット内の S3 オブジェクトの合計数に基づいて課金されます。料金は 1 日あたりの日割り計算です。

機密データ検出ジョブと機密データ自動検出によるオブジェクト分析

これらのコストは、S3 オブジェクトを分析し、Macie がオブジェクト内で検出する機密データを報告することで発生します。これには、機密データ検出ジョブと機密データ自動検出による分析および報告が含まれます。詳細については、「機密データの検出」を参照してください。

Macie が S3 オブジェクト内で分析する非圧縮データの量に基づいて課金されます。サポートされていない Amazon S3 ストレージクラスの使用、サポートされていないファイルまたはストレージ形式の使用、アクセス許可の設定などの理由により、Macie が分析できないオブジェクトには課金されません。さらに、これらのコストは、ジョブや機密データ自動検出によって生成された機密データ検出結果の数によって変化しません。

機密データの自動検出のコストを管理するには、分析から個々の S3 バケットを除外できます。例えば、組織のセキュリティやコンプライアンス要件を満たすことがわかっているバケットを除外できる可能性があります。アカウントが複数の Macie アカウントを一元管理する組織の一部である場合、追加のオプションとして、組織内の個々のアカウントの機密データ自動検出を選択的に有効または無効にすることができます。詳細については、「機密データ自動検出の設定」を参照してください。

機密データ検出ジョブのコストは、アカウントの毎月の機密データ検出クォータによって制限されます。(デフォルトのクォータは 5 TB のデータ)。ジョブが実行されていて、対象となるオブジェクトの分析がこのクォータに達すると、Macie は翌月が始まり、アカウントの月間クォータがリセットされるまで、またはアカウントのクォータを引き上げるまでジョブを自動的に一時停止します。

ユーザーが組織の Macie 管理者の場合、機密データ検出ジョブのコストは、データを分析する各アカウントの月別機密データ検出クォータによって制限されます。メンバーアカウントのクォータは、暦月中にユーザー自身のジョブとメンバーアカウントのジョブがそのアカウントで分析できる最大データ量を定義します。ジョブが実行されていて、対象となるオブジェクトの分析がメンバーアカウントのこのクォータに達すると、Macie はアカウントが所有するバケット内のオブジェクトの分析を停止します。Macie がクォータを満たしていない他のすべてのアカウ

ントのオブジェクトの分析を終了すると、Macie は自動的にジョブを一時停止します。1 回限りのジョブの場合、Macie は次の暦月が始まったとき、または影響を受けたすべてのアカウントのクォータが増加したときのどちらか早い方で、自動的にジョブを再開します。定期的なジョブの場合は、次の実行が開始予定になるか、または次の暦月が始まるときのいずれか早いタイミングで、Macie はジョブを自動的に再開します。スケジュールされた実行が次の暦月が始まる前に開始された場合、または影響を受けるアカウントのクォータが増加した場合、Macie はアカウントが所有するバケット内のオブジェクトを分析しません。

> **Tip**
>
> 機密データの検出コストを管理または削減するための役立つヒントについては、AWS セキュリティブログのAmazon Macie を使用して機密データ検出コストを削減する方法ブログ投稿を参照してください。

使用コストの詳細と例については、Amazon Macie の料金を参照してください。

Macie を使用して推定使用コストを確認するときは、コストの見積もりがどのように計算されるかを理解することが重要です。以下の点を考慮します。

- 見積もりは米ドルで報告され、現時点の AWS リージョン にのみ有効です。Macie を複数のリージョンで使用する場合、データは Macie を使用するすべてのリージョンで集計されません。
- コンソールでは、当月の月初から現在までの見積もりが含まれます。Amazon Macie API を使用してプログラムでデータをクエリする場合、見積もりに含める時間範囲を選択できます。これは、過去 30 日間のローリング時間枠、または当月の月初から現在までにすることができます。
- 見積もりには、アカウントに適用される可能性のあるすべての割引が反映されるわけではありません。例外は、Amazon Macie の料金で説明されているように、リージョンの従量料金階層から導出される割引です。アカウントがこのタイプの割引の対象となる場合、見積もりにはその割引が反映されます。
- お客様が組織の Macie 管理者である場合、見積もりには組織の統合使用量での従量制割引は反映されません。これらの割引については、AWS Billing ユーザーガイドの従量制割引を参照してください。
- 予防的制御のモニタリングの場合、見積もりは該当する時間範囲の 1 日の平均コストに基づきます。コストは 1 日あたりの日割り計算です。
- 機密データ自動検出の場合、全体的な見積もりは、Macie がこれまで該当する期間内で分析した非圧縮データの量とオブジェクト監視の 1 日の平均コスト (1 日あたりの比例配分) に基づきます。ユーザーが組織の Macie 管理者であり、メンバーアカウントの機密データ自動検出を有効にして

いる場合、それらのアクティビティの推定コストは、該当する各メンバーアカウントの見積もりに含まれます。

- 機密データ検出ジョブの場合、見積もりは該当する時間範囲の間にジョブがこれまでに分析した非圧縮データの量に基づきます。ユーザーが組織の Macie 管理者であり、メンバーアカウントのデータを分析するジョブを実行する場合、それらのジョブの推定コストは、該当する各メンバーアカウントの見積もりに含まれます。
- アカウントが組織のメンバーアカウントであり、Macie 管理者が機密データの自動検出を実行したり、機密データ検出ジョブを実行してデータを分析したりすると、それらのアクティビティの推定コストがアカウントの見積もりに含まれます。
- 見積もりには、特定の Macie 機能がある他の AWS のサービス の使用で発生するコストは含まれません。例えば、カスタマーマネージド AWS KMS keys を使用して、機密データを検査する S3 オブジェクトを復号化する場合です。

また、Macie は、機密データ検出ジョブと機密データ自動検出による S3 オブジェクトの分析に、月間無料利用枠を提供することにも注意してください。毎月、S3 オブジェクトの機密データを検出して報告するために最大 1 GB のデータまで分析に料金は課せられません。1 か月のデータ分析が 1 GB を超える場合、最初の 1 GB のデータ以降、ユーザーアカウントに対して機密データ検出料金が発生し始めます。1 か月のデータ分析が 1 GB 未満でも、残りの割り当ては翌月に移管されません。ユーザーのアカウントが一括請求を行っている組織の一部である場合は、組織で分析されたデータの合計量に無料利用枠が適用されます。つまり、組織内のすべてのアカウントに対して、毎月最大 1 GB のデータまでは分析での料金は発生しません。

Amazon Macie で推定使用コストを確認する

最新の Amazon Macie 推定使用コストを確認するには、Amazon Macie コンソールまたは Amazon Macie API を使用します。コンソールと API の両方で、Macie 料金体系の見積もりコストが提供されます。現在 30 日間の無料トライアルに参加している場合は、このデータを使用して、無料トライアル終了後に Macie 使用コストを見積もることができます。Macie の料金体系と考慮事項については、推定使用コストの計算方法を理解する を参照してください。使用コストの詳細と例については、Amazon Macie の料金を参照してください。

Macie では、推定使用コストは米ドルで報告され、現時点の AWS リージョンにのみ適用されます。コンソールを使用してデータを確認する場合、コストの見積もりは当月の月初から現在までのもの (包括的) です。Amazon Macie API を使用してプログラムでデータをクエリする場合は、過去 30 日間のローリング時間枠、または当月の月初から現在までを指定できます。

トピック

Amazon Macie コンソールで推定使用コストを確認する

Amazon Macie コンソールでは、コスト見積もりは次のように設定されています:

- 予防的コントロールのモニタリング – これは、Amazon Simple Storage Service (Amazon S3) 汎用バケットのインベントリを維持し、セキュリティとアクセスコントロールのためにバケットを評価およびモニタリングするための推定コストです。
- 機密データ検出ジョブ — 実行した機密データ検出ジョブの推定コストです。
- 機密データ自動検出 — 機密データ自動検出を実行する推定コストです。これには、S3 バケットインベントリの監視と評価を行い、分析の対象となる S3 オブジェクトを特定することが含まれます。また、対象オブジェクトの分析や、機密データの統計、検出結果、およびその他タイプの結果の報告も含まれます。これらの見積りを確認するには、アカウントが組織の Macie 管理者アカウントであるか、スタンドアロン Macie アカウントである必要があります。

Amazon Macie コンソールで推定使用コストを確認するには、次の手順に従います。

コンソールで推定使用コストを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、推定コストを確認するリージョンを選択します。
3. ナビゲーションペインで 使用状況を選択します。

スタンドアロンの Macie アカウントを持っている場合や、お客様のアカウントが組織のメンバーアカウントの場合は、使用状況ページには、アカウントの推定使用コストの内訳が表示されます。

ユーザーが組織の Macie 管理者である場合、使用状況ページには組織内のアカウントが一覧表示されます。このテーブルの説明を以下に示します。

- サービスクォータ – ジョブ – これは、アカウントが所有するバケット内の S3 オブジェクトを分析するために機密データ検出ジョブを実行するための現在の月次クォータです。

- 無料トライアル – これらのフィールドは、アカウントが現在、予防的コントロールのモニタリングまたは機密データの自動検出の無料トライアルに参加しているかどうかを示します。該当の無料トライアルがアカウントに対して終了した場合、[無料トライアル] フィールドは空になります。
- 合計 — アカウントの合計推定コストです。

推定コスト セクションには、組織の推定コストの合計と、それらのコストの内訳が表示されます。組織内の特定のアカウントの推定コストの内訳を確認するには、テーブルでアカウントを選択します。推定コストセクションには、この内訳が表示されます。別のアカウントに関するこのデータを表示するには、テーブルでアカウントを選択します。アカウントの選択を解除するには、パネルのアカウント ID の横にある X を選択します。

Amazon Macie API を使用して推定使用コストをクエリする

推定使用コストをプログラムでクエリするには、Amazon Macie API の以下のオペレーションを使用できます。

- GetUsageTotals — このオペレーションは、使用メトリクス別にグループ化されたアカウントの推定使用コストの合計を返します。お客様が組織の Macie 管理者である場合、このオペレーションは、組織内のすべてのアカウントの集計コスト見積もりを返します。このオペレーションの詳細については、Amazon Macie API リファレンスの使用合計を参照してください。
- GetUsageStatistics — このオペレーションは、アカウントごとにグループ化され、次に使用メトリクス別にグループ化されたアカウントの使用統計と関連データを返します。データには、合計推定使用コストと現在のアカウントクォータが含まれます。該当する場合は、Macie および機密データ自動検出の 30 日間無料トライアルがいつ開始したかも表示されます。お客様が組織の Macie 管理者である場合、このオペレーションは組織内のすべてのアカウントのデータの内訳を返します。クエリ結果をソートしてフィルタリングすることで、クエリをカスタマイズできます。このオペレーションの詳細については、Amazon Macie API リファレンスの使用統計を参照してください。

どちらのオペレーションを使用する場合でも、オプションでデータの包括的な時間範囲を指定できます。この時間範囲は、過去 30 日間のローリング時間枠`PAST_30_DAYS`、または当月の月初から現在まで`MONTH_TO_DATE`にすることができます。時間範囲を指定しない場合、Macie は過去 30 日間のデータを返します。

次の例では、AWS Command Line InterfaceAWS CLI を使用して、推定使用コストと統計をクエリする方法を説明します。別の AWS コマンドラインツールまたは AWS SDK の最新バージョンを使用するか、HTTPS リクエストを Macie に直接送信して、データをクエリすることもできます。 AWS ツールと SDKsで構築するツール AWS」を参照してください。

例

- 例 1: 合計推定使用コストのクエリ
- 例 2: 使用統計のクエリ

例 1: 合計推定使用コストのクエリ

を使用して推定使用コストの合計をクエリするには AWS CLI、 get-usage-totals コマンドを実行し、オプションでデータの時間範囲を指定します。例:

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

ここで、*MONTH_TO_DATE* はデータの時間範囲として当月の月初から現在までを指定します。

コマンドが正常に実行された場合は、以下のような出力が表示されます。

```
{
    "timeRange": "MONTH_TO_DATE",
    "usageTotals": [
        {
            "currency": "USD",
            "estimatedCost": "153.45",
            "type": "SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "65.18",
            "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "1.51",
            "type": "DATA_INVENTORY_EVALUATION"
        },
        {
            "currency": "USD",
            "estimatedCost": "0.98",
            "type": "AUTOMATED_OBJECT_MONITORING"
        }
    ]
}
```

estimatedCost 関連使用指標 (type) の推定使用コストの合計は、以下のとおりです。

- SENSITIVE_DATA_DISCOVERY、機密データ検出ジョブを使った S3 オブジェクトの分析用。
- AUTOMATED_SENSITIVE_DATA_DISCOVERY、機密データ自動検出を使った S3 オブジェクトの分析用。
- DATA_INVENTORY_EVALUATION、セキュリティとアクセスコントロールのための S3 汎用バケットのモニタリングと評価用。
- AUTOMATED_OBJECT_MONITORING、S3 バケットインベントリの評価および監視用に、機密データ自動検出による分析の対象となる S3 オブジェクトを特定するものです。

例 2: 使用統計のクエリ

を使用して使用状況統計をクエリするには AWS CLI、 get-usage-statistics コマンドを実行します。必要に応じて、クエリ結果の時間範囲の並べ替え、フィルタリング、および指定を行えます。次の例では、過去 30 日間の Macie 管理者アカウントの使用統計を取得します。結果は AWS アカウント ID で昇順にソートされます。

Linux、macOS、または Unix の場合、読みやすさを向上させるためにバックスラッシュ (\) の行連結文字を使用します。

```
$ aws macie2 get-usage-statistics \
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

Microsoft Windows の場合、読みやすさを向上させるためにキャレット (^) の行連結文字を使用します。

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={\"key\":\"accountId\",\"orderBy\":\"ASC\"} ^
--time-range PAST_30_DAYS
```

ここで、

- *accountId* は、フィードを指定して結果をソートするために使用します。
- *ASC* は、指定されたフィールド (*accountId*) の値に基づいて結果に適用されるソートオーダーです。
- *PAST_30_DAYS* は、データの期間範囲として過去 30 日間を指定します。

コマンドが正常に実行された場合、Macie は、records 配列を返します。配列には、クエリ結果に含まれる各アカウントのオブジェクトが含まれます。例:


```
{
    "records": [
        {
            "accountId": "111122223333",
            "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-20T12:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.51",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "65.18",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "153.45",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "0.98",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        },
        {
            "accountId": "444455556666",
            "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-18T16:26:36.917000+00:00",
            "usage": [
                {
```

```
                    "currency": "USD",
                    "estimatedCost": "1.58",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "63.13",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "145.12",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "1.02",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        }
    ],
    "timeRange": "PAST_30_DAYS"
}
```

estimatedCost アカウントの関連する使用指標typeの推定使用コストの合計は、以下のとおりです。

- DATA_INVENTORY_EVALUATION、セキュリティとアクセスコントロールのための S3 汎用バケットのモニタリングと評価用。
- AUTOMATED_SENSITIVE_DATA_DISCOVERY、機密データ自動検出を使った S3 オブジェクトの分析用。
- SENSITIVE_DATA_DISCOVERY、機密データ検出ジョブを使った S3 オブジェクトの分析用。
- AUTOMATED_OBJECT_MONITORING、アカウントの S3 バケットインベントリを評価および監視して、機密データ自動検出による分析の対象となる S3 オブジェクトを特定するためのものです。

Amazon Macie 無料トライアルに参加する

Amazon Macie を初めて有効にすると、 AWS アカウント は Macie の 30 日間の無料トライアルに自動的に登録されます。これには、 AWS Organizations 組織内の個々のメンバーアカウントが含まれます。

無料トライアル期間中は、特定の で Macie を使用するために料金はかかりません AWS リージョン 。

- 予防的コントロールモニタリングの実行 — これには、リージョン内の Amazon Simple Storage Service (Amazon S3) 汎用バケットのインベントリの生成と維持が含まれます。また、セキュリティおよびアクセスコントロールのためのバケット監視および評価も含まれます。

  詳細については、Macie が Amazon S3 データセキュリティをモニタリングする方法を参照してください。
- 機密データの自動検出を実行 — リージョン内の S3 バケットインベントリの監視と評価を行い、分析の対象となる S3 オブジェクトを特定することが含まれます。また、対象オブジェクトの分析や、機密データの統計、検出結果、およびその他タイプの結果の報告も含まれます。この機能を設定および管理するには、 アカウントが組織の Macie 管理者アカウントであるか、スタンドアロン Macie アカウントである必要があります。ユーザーが組織の Macie 管理者である場合、この機能を使用して、メンバーアカウントが所有する S3 バケット内のオブジェクトを分析できます。

  詳細については、「機密データの自動検出の仕組み」を参照してください。

Macie が現在利用可能なリージョンの一覧については、AWS 全般のリファレンスのAmazon Macie エンドポイントとクォータを参照してください。

無料トライアルは 30 日間連続でご利用いただけます。開始後に一時停止することはできません。無料トライアル期間が終了すると、予防的統制モニタリングを実行するための料金が発生し始めます。機密データの自動検出を実行する場合にも料金が発生し始めます。ユーザーが組織の Macie 管理者である場合、組織内のアカウントごとに料金が発生します。Macie を使用して、組織内の個々のアカウントの推定使用コストの内訳を確認できます。

> **メモ**
>
> 無料トライアル中は、特定の Macie 機能 AWS のサービス で使用する他の に対して料金が発生する場合があります。例えば、カスタマー管理 AWS KMS keys の を使用して、機密データを検査する S3 オブジェクトを復号化する場合などです。

無料トライアルに、機密データ検出ジョブによる S3 オブジェクト分析は含まれません。無料トライアル中に 1 GB を超える非圧縮データを分析する機密データ検出ジョブを作成して実行すると、料金が発生します。(Macie は機密データ検出用に月間無料利用枠を提供しています。 毎月、S3 オブジェクトで最大 1 GB の非圧縮データまでは分析での料金は発生しません。最初の 1 GB を超えるとコストが発生します。)

無料トライアルの間は、トライアルのステータスをチェックし、アカウントの推定使用コストを確認できます。コストの見積もりは、無料トライアル期間中の Macie の使用に基づいています。それらは、トライアル終了後の使用コストの一部を理解するのに役立ちます。Macie がこれらの値を計算する方法の詳細については、推定使用コストの計算方法を理解するを参照してください。

無料トライアル中にステータスと推定コストを確認するには

Amazon Macie コンソールを使用してトライアルのステータスを確認し、推定使用コストを確認するには、次の手順に従います。Amazon Macie API の GetUsageStatisticsオペレーションを使用して、このデータにプログラムでアクセスすることもできます。

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、無料トライアルのステータスと推定使用コストを確認するリージョンを選択します。
3. ナビゲーションペインで 使用状況を選択します。

使用状況ページには、無料トライアルの残り日数が表示されます。また、米ドルでの推定使用コストの内訳も表示されます。

- 予防的コントロールのモニタリング — S3 汎用バケットのインベントリを維持し、無料トライアル終了後にバケットのセキュリティとアクセスコントロールを評価およびモニタリングするための総予測コストです。
- 機密データ検出ジョブ — 実行した機密データ検出ジョブの合計推定コストです。機密データ検出ジョブは無料トライアルに含まれません。
- 機密データ自動検出 — 無料トライアルの終了後に機密データ自動検出を実行する合計推定コストで、料金体系 (オブジェクト監視とオブジェクト分析) ごとに分類されます。これらの見積りを確認するには、アカウントが組織の Macie 管理者アカウントであるか、スタンドアロン Macie アカウントである必要があります。

ユーザーが組織の Macie 管理者である場合、使用状況ページには組織内の Macie アカウントに関する詳細が表示されます。このテーブルの説明を以下に示します。

- サービスクォータ – ジョブ – これは、アカウントが所有するバケット内の S3 オブジェクトを分析するために機密データ検出ジョブを実行するための現在の月次クォータです。
- 無料トライアル – これらのフィールドは、アカウントが現在、予防的コントロールのモニタリングまたは機密データの自動検出の無料トライアルに参加しているかどうかを示します。該当の無料トライアルがアカウントに対して終了した場合、[無料トライアル] フィールドは空になります。
- 合計 — アカウントの合計推定コストです。

推定コストセクションには、組織全体の推定コストが表示されます。組織内の特定のアカウントの推定コストの内訳を確認するには、テーブルでアカウントを選択します。推定コストセクションには、この内訳が表示されます。別のアカウントに関するこのデータを表示するには、テーブルでアカウントを選択します。アカウントの選択を解除するには、パネルのアカウント ID の横にある X を選択します。

> **メモ**
>
> アカウントが Amazon S3 に 150 TB を超えるデータを保存している場合、機密データ自動検出にかかるアカウントの推定コストと実際のコストは、Macie が 30 日間の無料トライアル中に提示するコスト予測よりも高くなる可能性があります。これは、無料トライアルに登録されているアカウントの 150 GB の非圧縮データが分析されると、機密データ自動検出によるオブジェクト分析が一時停止されるためです。アカウントのオブジェクト分析は、無料トライアルの終了後に再開します。Amazon S3 に 150 TB を超えるデータを保存するアカウントのコストを予測する方法については、 AWS Supportにお問い合わせください。
>
> 無料トライアル終了後に機密データの自動検出のコストを管理するには、個々の S3 バケットを後続の分析から除外できます。お客様が組織の Macie 管理者である場合、追加のオプションとして、組織内の個々のアカウントの機密データ自動検出を選択的に有効または無効にすることができます。これらのオプションについては、「機密データ自動検出の設定」を参照してください。

複数の Amazon Macie アカウントの管理

AWS 環境に複数のアカウントがある場合、環境内で Amazon Macie アカウントを関連付けて、Macie 内で組織としてそれらを集中管理できます。この設定により、指定 Macie 管理者は、組織の Amazon Simple Storage Service (Amazon S3) のデータ資産の全体的なセキュリティ体制を評価およびモニタリングし、組織の S3 バケット内の機密データを検出できます。管理者は、推定使用コストのモニタリングやアカウントクォータの評価など、さまざまなアカウント管理および管理タスクも大規模に実行できます。

Macie では、組織は、指定 Macie 管理者アカウントと 1 つ以上の関連付けられたメンバーアカウントで設定されています。Macie を AWS Organizations と統合する、または Macie でメンバーシップの招待を送信および受け入れるという 2 つの方法で、アカウントを関連付けることができます。Macie を AWS Organizations と統合することをお勧めします。

AWS Organizations はグローバルアカウント管理サービスであり、AWS 管理者は複数の AWS アカウント を統合して集中管理することが可能になります。予算、セキュリティ、コンプライアンスのニーズをサポートするように設計されたアカウント管理および一括請求 (コンソリデーティッドビリング) 機能が備わっています。追加料金なしで提供され、Macie、AWS Security Hub、Amazon GuardDuty を含む、複数の AWS のサービス と統合されています。詳細については、AWS Organizations ユーザーガイドを参照してください。

AWS Organizations を使用せずに複数の Macie アカウントを集中管理したい場合は、代わりにメンバーシップの招待を使用できます。招待を送信し、別のアカウントによって受け入れられた場合、お客様のアカウントは別のアカウントの Macie 管理者アカウントになります。招待を受け取って受け入れると、お客様のアカウントは Macie メンバーアカウントになり、Macie 管理者アカウントは Macie アカウントの特定の設定、データ、およびリソースにアクセスして管理できるようになります。

トピック

- Amazon Macie 管理者とメンバーアカウントの関係について理解する
- AWS Organizations を用いた Amazon Macie アカウントの管理
- 招待による Amazon Macie アカウントの管理

Amazon Macie 管理者とメンバーアカウントの関係について理解する

複数の Amazon Macie アカウントを組織として集中管理する場合、Macie 管理者は Amazon Simple Storage Service (Amazon S3) のインベントリデータ、ポリシーの結果、関連するメンバーアカウントの特定の Macie 設定とリソースにアクセスできます。管理者は、機密データの自動検出を有効にし、機密データ検出ジョブを実行して、メンバーアカウントが所有する S3 バケット内の機密データを検出することもできます。特定のタスクのサポートは、Macie 管理者アカウントが を通じて、AWS Organizations または招待によってメンバーアカウントに関連付けられているかどうかによって異なります。

以下のテーブルでは、Macie 管理者アカウントとメンバーアカウントの関係の詳細を示しています。これは、各タイプのアカウントに対するデフォルトのアクセス許可を示します。Macie の機能へのアクセスやオペレーションをさらに制限するには、カスタム AWS Identity and Access Management (IAM) ポリシーを使用できます。

このテーブルの説明を以下に示します。

- セルフ は、関連付けられたアカウントに対してそのアカウントがアクションを実行できないことを示します。
- いずれか は、アカウントが個別の関連付けられたアカウントに対してアクションを実行できることを示します。
- すべて は、アカウントがアクションを実行でき、アクションがすべての関連付けられたアカウントに適用されることを示します。

ダッシュ (–) は、アカウントがタスクを実行できないことを示します。

タスク	経由 AWS Organizations		招待により	
	管理者	メンバー	管理者	メンバー
Macie を有効化する	任意	–	自分	自分
組織のアカウントインベントリを確認する[1]	すべて	–	すべて	–

メンバーアカウントを追加する	すべて	–	すべて	–
S3 バケットの統計とメタデータを確認する	すべて	自分	すべて	自分
ポリシーの検出結果を確認する	すべて	自分	すべて	自分
(アーカイブ) ポリシーの検出結果を非表示にする[2]	すべて	–	すべて	–
ポリシーの結果を発行する [3]	自分	自分	自分	自分
機密データ検出結果のリポジトリを設定する[4]	自分	自分	自分	自分
許可リストを作成して使用する	自分	自分	自分	自分
カスタムデータ識別子を作成して使用する	自分	自分	自分	自分
機密データ自動検出設定を構成する	すべて	–	すべて	–
機密データの自動検出を有効または無効にする	すべて	–	すべて	–

機密データ自動検出の統計、データ、結果を確認する	すべて	–	すべて	–
機密データ検出ジョブの作成と実行[5]	すべて	Self	すべて	Self
機密データ検出ジョブの詳細を確認する[6]	自分	自分	自分	自分
機密データの検出結果を確認する[7]	自分	自分	自分	自分
機密データの検出結果を抑制(アーカイブ) する[7]	自分	自分	自分	自分
機密データの結果を発行する[7]	自分	自分	自分	自分
検出結果の機密データサンプルを取得するように Macie を設定する	自分	自分	自分	自分
検出結果の機密データのサンプルを取得する[8]	自分	自分	自分	自分
結果の公開先を設定する	自分	自分	自分	自分

結果の公開頻度を設定する	すべて	自分	すべて	自分
サンプルの結果を生成する	自分	自分	自分	自分
アカウントクォータと推定使用コストを確認する	すべて	自分	すべて	自分
Macie[9] を一時停止する	すべて	–	すべて	Self
Macie[10] を無効にする	自分	自分	自分	自分
メンバーアカウントを削除する(関連付けを解除する)	すべて	–	すべて	–
管理者アカウントとの関連付けを解除する	–	–	–	自分
別のアカウントとの関連付けを削除する[11]	すべて	–	すべて	Self

1. の組織の管理者は AWS Organizations 、Macie を有効にしていないアカウントを含め、組織内のすべてのアカウントを確認できます。招待ベースの組織の管理者は、インベントリに追加したアカウントのみを確認できます。
2. ポリシー検出結果を非表示にできるのは管理者だけです。管理者が抑制ルールを作成すると、Macie は特定のアカウントを除外するようにルールが設定されていない限り、組織内のすべ

てのアカウントのポリシー検出結果にルールを適用します。メンバーが抑制ルールを作成しても、Macie はそのメンバーのアカウントのポリシー検出結果にルールを適用しません。

3. 影響を受けるリソースを所有するアカウントのみが、リソースのポリシー結果を に発行できます AWS Security Hub。管理者アカウントとメンバーアカウントの両方が、影響を受けるリソースのポリシー検出結果を自動的に Amazon に発行します EventBridge。

4. 管理者が機密データの自動検出を有効にするか、メンバーアカウントが所有する S3 バケット内のオブジェクトを分析するようにジョブを設定すると、Macie は機密データの検出結果を管理者アカウントのリポジトリに保存します。

5. メンバーは、アカウントが所有する S3 バケット内のオブジェクトのみを分析するためのジョブを設定できます。管理者は、アカウントとメンバーアカウントが所有するバケット内のオブジェクトを分析するためのジョブを設定できます。複数アカウントのジョブにおけるクォータの適用方法とコストの計算方法については、以下を参照してください推定使用コストの計算方法を理解する。

6. ジョブを作成したアカウントのみが、ジョブの詳細にアクセスできます。これには、S3 バケットのインベントリ内のジョブ関連の詳細が含まれます。

7. ジョブを作成するアカウントのみが、ジョブが生成する機密データの結果にアクセスし、それを抑制、発行できます。機密データ自動検出で生成された機密データ検出結果にアクセスしたり、非表示、公開したりできるのは管理者だけです。

8. 機密データの検出結果がメンバーアカウント所有の S3 オブジェクトに適用される場合、管理者は、検出結果によって報告された機密データのサンプルを取得できる可能性があります。これは、検出結果のソース、および管理者アカウントとメンバーアカウントの構成設定とリソースによって異なります。詳細については、「機密データのサンプルを取得するための設定オプションと要件」を参照してください。

9. 管理者が自身のアカウントの メイシーを一時停止には、まず管理者がすべてのメンバーアカウントから自分のアカウントの関連付けを解除する必要があります。

10. 管理者が自分のアカウントの Macie を無効化するには、まず管理者がすべてのメンバーアカウントから自分のアカウントの関連付けを解除し、そのアカウントとそれらのすべてのアカウント間の関連付けを削除する必要があります。の組織の管理者は AWS Organizations 、組織の管理アカウントと協力して別のアカウントを管理者アカウントとして指定することで、これを行うことができます。

AWS Organizations 組織のメンバーで Macie を無効にするには、管理者はまずメンバーのアカウントの管理者アカウントとの関連付けを解除する必要があります。招待制の組織では、メンバーは自分のアカウントと管理者アカウントの関連付けを解除し、Macie を無効にすることもできます。

11. の組織の管理者は、アカウントと管理者アカウントの関連付けを解除した後、メンバーアカウントとの関連付けを削除 AWS Organizations できます。アカウントは引き続き管理者のアカウントインベントリに表示されますが、ステータスはメンバーアカウントではないことを示しています。招待制の組織では、管理者とメンバーは、自分のアカウントと別のアカウントの関連付けを解除した後に、別のアカウントとの関連付けを削除できます。その後、他のアカウントはアカウントインベントリに表示されなくなります。

AWS Organizations を用いた Amazon Macie アカウントの管理

AWS Organizations を使用して複数の AWS アカウント を集中管理する場合、Amazon MacieをAWS Organizations と統合し、次に組織内のアカウントの Macie を集中管理することができます。この設定では、指定 Macie 管理者が 10,000 個ものアカウントの Macie を有効化および管理できます。管理者は、Amazon Simple Storage Service (Amazon S3) のインベントリデータにアクセスし、アカウントが所有する S3 バケット内の機密データを検出することもできます。管理者が実行できるタスクの詳細については、Amazon Macie 管理者とメンバーアカウントの関係について理解するを参照してください。

Macie を AWS Organizations と統合するには、まずアカウントを組織の委任 Macie 管理者アカウントとして指定します。次に Macie 管理者は、組織内の他のアカウントで Macie を有効化し、それらのアカウントを Macie メンバーアカウントとして追加し、そのアカウントの Macie 設定とリソースを設定します。

> **Tip**
>
> 招待を使用して Macie 管理者アカウントをメンバーアカウントにすでに関連付けている場合は、そのアカウントを AWS Organizations 内で組織の委任 Macie 管理者アカウントとして指定できます。これを行うと、現在関連付けられているすべてのメンバーアカウントがメンバーとして残り、AWS Organizations を使用してアカウントを管理する利点を最大限に活用できます。詳細については、招待ベースの組織からの移行を参照してください。

このセクションのトピックでは、Macie を AWS Organizations と統合する方法、および組織内のアカウントの Macie を管理および管理する方法について説明します。

トピック

で Amazon Macie を使用する際の考慮事項と推奨事項 AWS Organizations

Amazon Macie を と統合 AWS Organizations し、Macie で組織を設定する前に、次の要件と推奨事項を検討してください。また、Macie 管理者アカウントとメンバーアカウントの関係を理解してください。

トピック

Macie 管理者アカウントの指定

組織の委任 Macie 管理者アカウントにする必要があるアカウントを決定する際には、次の点に注意してください。

- 組織は、委任 Macie 管理者アカウントを 1 つだけ持つことができます。
- アカウントを Macie 管理者とメンバーアカウントに同時に設定することはできません。
- 組織の委任 Macie 管理者アカウントを指定できるのは、組織の AWS Organizations 管理アカウントのみです。その後、その指定を変更または削除できるのは管理アカウントのみです。
- 組織の AWS Organizations 管理アカウントは、組織の委任 Macie 管理者アカウントにもできます。ただし、 AWS セキュリティのベストプラクティスと最小特権の原則に基づいてこの設定を推

奨しません。請求の目的で管理アカウントにアクセスできるユーザーは、情報セキュリティの目的で Macie にアクセスする必要があるユーザーとは異なる可能性があります。

この設定を希望する場合は、アカウントを委任 Macie 管理者アカウントとして指定する AWS リージョン 前に、少なくとも 1 つの で組織の管理アカウントに対して Macie を有効にする必要があります。そうしないと、アカウントはメンバーアカウントの Macie 設定とリソースへのアクセスおよび管理ができなくなります。

- とは異なり AWS Organizations、Macie はリージョンサービスです。これは、Macie 管理者アカウントの指定がリージョンでの指定であることを意味します。それは、Macie 管理者とメンバーアカウントの間の関連付けはリージョンでのものであることも意味します。たとえば、管理アカウントが米国東部 (バージニア北部) リージョンの Macie 管理者アカウントを指定している場合、Macie 管理者はそのリージョンのメンバーアカウントの Macie のみを管理できます。

  複数の で Macie アカウントを一元管理するには AWS リージョン、管理アカウントが現在 Macie を使用している、または今後使用する各リージョンにサインインし、それらの各リージョンで Macie 管理者アカウントを指定する必要があります。次に Macie 管理者は、それらの各リージョンで組織を設定できます。Macie が現在利用可能なリージョンの一覧については、AWS 全般のリファレンスのAmazon Macie エンドポイントとクォータを参照してください。
- アカウントは、一度に 1 つの Macie 管理者アカウントのみと関連付けることができます。組織が複数のリージョンで Macie を使用している場合、指定 Macie 管理者アカウントは、それらのすべてのリージョンで同じである必要があります。ただし、組織の管理アカウントは、各リージョンで管理者アカウントを個別に指定する必要があります。
- アカウントは、一度に 1 つの組織のみの委任 Macie 管理者アカウントにすることができます。で複数の組織を管理する場合は AWS Organizations、組織ごとに異なる Macie 管理者アカウントを指定する必要があります。これは要件 AWS Organizations によるものです。アカウントは一度に 1 つの組織のメンバーにしかなれません。

Macie 管理者の AWS アカウント が一時停止、分離、または閉鎖されている場合、関連するすべての Macie メンバーアカウントは Macie メンバーアカウントとして自動的に削除されますが、Macie はアカウントに対して引き続き有効になります。1 つ以上のメンバーアカウントで機密データの自動検出が有効になっている場合、アカウントでは無効になります。これにより、アカウントの自動検出の実行中に Macie が生成して直接提供した統計データ、インベントリデータ、その他の情報へのアクセスも無効になります。このデータへのアクセスを復元するには、30 日以内に以下を実行する必要があります。

1. Macie 管理者の AWS アカウント が復元されます。

2. AWS Organizations 管理アカウントは、アカウントを Macie 管理者アカウントとして再度指定します。
3. Macie 管理者は組織を設定し、適切なアカウントの自動検出を再度有効にします。

30 日後、Macie は、該当するアカウントの自動検出を実行している間に、以前に生成して直接提供したデータを完全に削除します。

Macie 管理者アカウントの指定の変更または削除

組織の委任 Macie 管理者アカウントの指定を変更または削除できるのは、組織の AWS Organizations 管理アカウントのみです。

管理アカウントが指定を変更または削除した場合：

- 関連付けられたすべてのメンバーアカウントは Macie メンバーアカウントとして削除されますが、Macie は引き続きアカウントに対して有効になります。アカウントはスタンドアロン Macie アカウントになります。Macie の使用を一時停止または停止するには、メンバーアカウントのユーザーがアカウントの Macie を停止 (一時停止) または無効化 (停止) する必要があります。
- 機密データの自動検出は、有効化されたアカウントごとに無効になります。これにより、Macie が各アカウントの自動検出を実行している間に生成して直接提供した統計データ、インベントリデータ、その他の情報へのアクセスも無効になります。このデータへのアクセスを復元するには、管理アカウントが 30 日以内に同じ Macie 管理者アカウントを再度指定する必要があります。さらに、Macie 管理者は組織を再度設定し、30 日以内に各アカウントの自動検出を再度有効にする必要があります。30 日後、データは期限切れになり、Macie はそのデータを完全に削除します。

Macie メンバーアカウントの追加と削除

組織のメンバーアカウントを追加、削除、または管理する場合は、次の点に注意してください。

- Macie 管理者アカウントは、各 AWS リージョン内では、わずか 10,000 個のアクティブな (有効な) Macie メンバーアカウントにしか関連付けることができません。組織がこのクォータを超える場合、Macie 管理者は、リージョン内の必要な数の既存のメンバーアカウントを削除するまで、メンバーアカウントを追加できなくなります。組織がこのクォータを満たすと、アカウントの AWS Health および Amazon CloudWatch イベントを作成して Macie 管理者に通知します。また、E メールが彼らのアカウントに関連付けられているアドレスに送信されます。

  ユーザーが組織の Macie 管理者である場合は、Amazon Macie コンソールのアカウントページまたは Amazon Macie Amazon Macie API の ListMembersオペレーションを使用して、現在アカウン

トに関連付けられているアクティブなメンバーアカウントの数を判断できます。詳細については、「組織の Amazon Macie アカウントの確認」を参照してください。

- アカウントは、一度に 1 つの Macie 管理者アカウントのみと関連付けることができます。これは、アカウントが AWS Organizations内で組織の Macie 管理者アカウントにすでに関連付けられている場合、別のアカウントからの Macie の招待は受け入れられないことを意味します。

  同様に、アカウントが既に招待を承諾している場合、 の組織の Macie AWS Organizations 管理者はアカウントを Macie メンバーアカウントとして追加できません。そのアカウントは、まず現在の招待ベースの管理者アカウントから関連付けを解除する必要があります。

- AWS Organizations 管理アカウントを Macie メンバーアカウントとして追加するには、まず管理アカウントのユーザーがアカウントの Macie を有効にする必要があります。Macie 管理者は、管理アカウントで Macie を有効化することはできません。

- Macie 管理者が Macie メンバーアカウントを削除した場合：

  - Macie は引き続きそのアカウントに対して有効化されています。アカウントはスタンドアロン Macie アカウントになります。Macie の使用を一時停止または停止するには、アカウントのユーザーがアカウントの Macie を停止 (一時停止) または無効化 (停止) する必要があります。

  - アカウントで機密データの自動検出が有効になっている場合、そのアカウントでは機密データの自動検出は無効になります。これにより、アカウントの自動検出の実行中に Macie が生成して直接提供した統計データ、インベントリデータ、その他の情報へのアクセスも無効になります。

- メンバーアカウントは Macie 管理者アカウントから関連付けを解除できません。Macie 管理者のみが Macie メンバーアカウントとしてアカウントを削除できます。

招待ベースの組織からの移行

Macie メンバーシップの招待を使用して Macie 管理者アカウントをメンバーアカウントにすでに関連付けている場合は、そのアカウントを AWS Organizations内で組織の委任 Macie 管理者アカウントとして指定することをお勧めします。これにより、招待ベースの組織からの移行が簡素化されます。

これを行うと、現在関連付けられているすべてのメンバーアカウントが引き続きメンバーになります。メンバーアカウントが の組織の一部である場合 AWS Organizations、アカウントの関連付けは Macie の Via への招待によって自動的に変更されます。 AWS Organizationsメンバーアカウントが AWS Organizations内で組織の一部ではない場合、アカウントの関連付けは引き続き 招待によりになります。どちらの場合も、アカウントは引き続きメンバーアカウントとして委任 Macie 管理者アカウントに関連付けられます。

1 つのアカウントを複数の Macie 管理者アカウントに同時に関連付けることができないため、この方法をお勧めします。で別のアカウントを組織の Macie 管理者アカウントとして指定すると AWS Organizations、指定された管理者は、招待によって別の Macie 管理者アカウントに既に関連付けられているアカウントを管理できなくなります。各メンバーアカウントは、まず現在の招待ベースの管理者アカウントから関連付けを解除する必要があります。次に、 AWS Organizations 内で組織の Macie 管理者アカウントはそのアカウントを Macie メンバーアカウントとして追加し、アカウントの管理を開始できます。

Macie を と統合 AWS Organizations し、Macie で組織を設定したら、必要に応じて組織の別の Macie 管理者アカウントを指定できます。招待を引き続き使用して、 AWS Organizations内で組織の一部ではないメンバーアカウントを関連付けて管理することもできます。

Amazon Macie 内で組織を統合および設定する

で Amazon Macie の使用を開始するには AWS Organizations、組織の AWS Organizations 管理アカウントが、そのアカウントの委任 Macie 管理者アカウントとして指定します。これにより、Macie は の信頼されたサービスとして有効になります AWS Organizations。それにより、Macie が指定管理者アカウントとして現在の AWS リージョン でも有効化され、指定管理者アカウントはそのリージョン内で組織内の他のアカウントの Macie を有効化および管理できるようになります。これらのアクセス許可の付与方法については、 ユーザーガイドの「他の AWS Organizations で AWS のサービスを使用するAWS Organizations 」を参照してください。

委任 Macie 管理者は、主に組織のアカウントをリージョン内の Macie メンバーアカウントとして追加することで、Macie 内で組織を設定します。その後、管理者は、そのリージョン内のアカウントの特定の Macie 設定、データ、およびリソースにアクセスできます。また、機密データの自動検出を実行し、機密データ検出ジョブを実行して、アカウントが所有する Amazon Simple Storage Service (Amazon S3) バケット内の機密データを検出することもできます。

このトピックでは、組織の委任 Macie 管理者を指定する方法と、組織のアカウントを Macie メンバーアカウントとして追加する方法について説明します。これらのタスクを実行する前に、管理者アカウントとメンバーアカウントの関係を理解してください。また、 で Macie を使用する際の考慮事項と推奨事項を確認することをお勧めします AWS Organizations。

タスク

- ステップ 1: アクセス許可を確認する
- ステップ 2: 組織の委任 Macie 管理者アカウントを指定する
- ステップ 3: 新しい組織のメンバーアカウントを Macie メンバーアカウントとして自動的に有効化して追加する

- ステップ 4: 既存の組織アカウントを Macie メンバーアカウントとして有効化して追加する

組織を複数のリージョンに統合して設定するには、 AWS Organizations 管理アカウントと委任 Macie 管理者が追加のリージョンごとにこれらのステップを繰り返します。

ステップ 1: アクセス許可を確認する

組織の委任 Macie 管理者アカウントを指定する前に、自分 (AWS Organizations 管理アカウントのユーザー) が Macie アクション の実行を許可されていることを確認しますmacie2:EnableOrganizationAdminAccount。この操作により、Macie を使用して組織の委任 Macie 管理者アカウントを指定できます。

また、次のアクションを実行できることを確認します AWS Organizations 。

- organizations:DescribeOrganization
- organizations:EnableAWSServiceAccess
- organizations:ListAWSServiceAccessForOrganization
- organizations:RegisterDelegatedAdministrator

これらのアクションにより、組織に関する情報の取得、Macie と の統合 AWS Organizations、 AWS のサービス との統合先に関する情報の取得、 AWS Organizations組織の委任 Macie 管理者アカウントの指定を行うことができます。

これらのアクセス許可を付与するには、アカウントの AWS Identity and Access Management (IAM) ポリシーに次のステートメントを含めます。

```
{
   "Sid": "Grant permissions to designate a delegated Macie administrator",
   "Effect": "Allow",
   "Action": [
      "macie2:EnableOrganizationAdminAccount",
      "organizations:DescribeOrganization",
      "organizations:EnableAWSServiceAccess",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:RegisterDelegatedAdministrator"
   ],
   "Resource": "*"
}
```

AWS Organizations 管理アカウントを組織の委任 Macie 管理者アカウントとして指定する場合、アカウントには次の IAM アクションを実行するアクセス許可も必要です: `CreateServiceLinkedRole`。このアクションにより、管理アカウントで Macie を有効化することが許可されます。ただし、 AWS セキュリティのベストプラクティスと最小特権の原則に基づいて、これを行うことはお勧めしません。

このアクセス許可を付与する場合は、 AWS Organizations 管理アカウントの IAM ポリシーに次のステートメントを追加します。

```
{
   "Sid": "Grant permissions to enable Macie",
   "Effect": "Allow",
   "Action": [
      "iam:CreateServiceLinkedRole"
   ],
   "Resource": "arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
   "Condition": {
      "StringLike": {
         "iam:AWSServiceName": "macie.amazonaws.com"
      }
   }
}
```

ステートメントで、*111122223333* を管理アカウントのアカウント ID と置き換えます。

オプトイン AWS リージョン (デフォルトで無効になっているリージョン) で Macie を管理する場合は、 `Resource`要素と `iam:AWSServiceName`条件の Macie サービスプリンシパルの値も更新します。値には、リージョンのリージョンコードを指定する必要があります。たとえば、リージョンコード me-south-1 を持つ中東 (バーレーン) リージョンで Macie を管理するには、以下を行います。

- `Resource` 要素で、次を置き換えます:

  `arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`

  with

  `arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`

ここで、*111122223333* は管理アカウントのアカウント ID を指定し、*me-south-1* はリージョンのリージョンコードを指定します。

- `iam:AWSServiceName` 条件では、`macie.amazonaws.com` を `macie.`*me-south-1*`.amazonaws.com` に置き換えます。ここで、*me-south-1* はリージョンのリージョンコードを指定します。

Macieが現在利用可能なリージョンのリストと、それぞれのリージョンコードについては、AWS 全般のリファレンスの Amazon Macieのエンドポイントとクォータを参照してください。オプトインリージョンについては、「AWS Account Management リファレンスガイド」の「アカウントがで使用できる AWS リージョン を指定する」を参照してください。

ステップ 2: 組織の委任 Macie 管理者アカウントを指定する

アクセス許可を確認したら、(AWS Organizations 管理アカウントのユーザーとして) 組織の委任 Macie 管理者アカウントを指定できます。

組織の委任 Macie 管理者アカウントを指定するには

組織の委任 Macie 管理者アカウントを指定するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。 AWS Organizations 管理アカウントのユーザーのみがこのタスクを実行できます。

Console

以下のステップに従って、Amazon Macie コンソールを使用して委任 Macie 管理者アカウントを指定します。

委任 Macie 管理者アカウントを指定するには

1. AWS Organizations 管理アカウント AWS Management Console を使用して にサインインします。
2. ページの右上隅にある AWS リージョン セレクターを使用して、組織の委任 Macie 管理者アカウントを指定するリージョンを選択します。
3. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
4. Macie が現在のリージョンで管理アカウントに対して有効化されているかどうかに応じて、次のいずれかを実行します。

- Macie が有効化されていない場合は、Welcome Page (ようこそページ) の Get started (開始方法) を選択します。
- Macie が有効化されている場合は、ナビゲーションペインの Settings (設定) を選択します。

5. 委任管理者 で、Macie 管理者アカウントとして AWS アカウント 指定する の 12 桁のアカウント ID を入力します。
6. Delegate (委任) を選択します。

組織を Macie と統合する追加のリージョンごとに、前述のステップを繰り返します。それらの各リージョンで同じ Macie 管理者アカウントを指定する必要があります。

API

委任 Macie 管理者アカウントをプログラムで指定するには、Amazon Macie API の EnableOrganizationAdminAccountオペレーションを使用します。複数のリージョンでアカウントを指定するには、組織を Macie と統合するリージョンごとに指定を送信します。それらの各リージョンで同じ Macie 管理者アカウントを指定する必要があります。

指定を送信するときは、必須adminAccountIdパラメータを使用して、組織の Macie 管理者アカウントとして AWS アカウント 指定する の 12 桁のアカウント ID を指定します。また、指定が適用されるリージョンも必ず指定してください。

AWS Command Line Interface （ AWS CLI ） を使用して Macie 管理者アカウントを指定するには、 enable-organization-admin-account コマンドを実行します。admin-account-id パラメータには、 AWS アカウント 指定する の 12 桁のアカウント ID を指定します。region パラメータを使用して、指定が適用されるリージョンを指定します。例:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333
```

ここで、*us-east-1* は指定が適用されるリージョン (米国東部 (バージニア北部) リージョン) であり、*111122223333* は指定するアカウントのアカウント ID です。

組織の Macie 管理者アカウントを指定した後、Macie 管理者は Macie 内で組織の設定を開始できます。

ステップ 3: 新しい組織のメンバーアカウントを Macie メンバーアカウントとして自動的に有効化して追加する

デフォルトでは、アカウントが AWS Organizations内で組織に追加されたときに、Macie は新しいアカウントに対して自動的に有効化されません。また、アカウントは Macie メンバーアカウントとして自動的に追加されません。アカウントは Macie 管理者のアカウントインベントリに表示されます。ただし、Macie がアカウントに対して必ずしも有効化されているわけではなく、Macie 管理者はアカウントの Macie 設定、データ、およびリソースに必ずしもアクセスできるわけではありません。

お客様が組織の委任 Macie 管理者である場合は、この設定を変更できます。組織の自動有効化を有効にできます。これを行うと、アカウントが で組織に追加されると、Macie は新しいアカウントに対して自動的に有効になり AWS Organizations、アカウントはメンバーアカウントとして Macie 管理者アカウントに自動的に関連付けられます。この設定を有効にしても、組織の既存のアカウントには影響しません。既存のアカウントで Macie を有効化して管理するには、アカウントを Macie メンバーアカウントとして手動で追加する必要があります。次のステップでは、これを行う方法を説明します。

> **メモ**
>
> 自動有効化を有効にする場合は、次の例外に注意してください。
>
> - 新しいアカウントがすでに別の Macie 管理者アカウントに関連付けられている場合、Macie は組織内のメンバーアカウントとしてアカウントを自動的に追加しません。
>
> そのアカウントは、Macie 内で組織の一部になる前に、現在の Macie 管理者アカウントから関連付けを解除する必要があります。その後、アカウントを手動で追加できます。これが当てはまるアカウントを特定するには、組織のアカウントインベントリを確認することができます。
> - 組織が 内の 10,000 個の Macie メンバーアカウントのクォータに達すると AWS リージョン、Macie はリージョンでこの設定を自動的にオフにします。
>
> この場合、Macie 管理者アカウントの AWS Health および Amazon CloudWatch イベントを作成して通知します。また、E メールがそのアカウントに関連付けられているアドレスに送信されます。その後、アカウントの総数が10,000アカウント未満に減少した場合、Macieは自動的に設定を再度オンにします。

新しい組織アカウントを Macie メンバーアカウントとして自動的に有効化して追加するには

新しいアカウントを Macie メンバーアカウントとして自動的に有効化して追加するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。組織の委任 Macie 管理者のみが、このタスクを実行できます。

Console

コンソールを使用してこのタスクを実行するには、 の AWS Organizations アクションを実行できる必要がありますorganizations:ListAccounts。このアクションにより、組織内のアカウントに関する情報を取得して表示することが許可されます。これらのアクセス許可を持っている場合は、次のステップに従って、新しい組織アカウントを Macie メンバーアカウントとして自動的に有効化して追加します。

新しい組織アカウントを自動的に有効化して追加するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、Macie メンバーアカウントとして新しいアカウントを自動的に有効化して追加するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
4. アカウント ページの新規アカウント セクションで、編集 を選択します。
5. 「新しいアカウントの設定の編集」ダイアログボックスで、「Macie を有効にする」を選択します。

   新しいメンバーアカウントで機密データ自動検出も有効にするには、機密データ自動検出を有効にする を選択します。アカウントに対してこの機能を有効にすると、Macie はアカウントの S3 バケットからサンプルオブジェクトを継続的に選択し、オブジェクトを分析して機密データが含まれているかどうかを判断します。詳細については、「機密データ自動検出を実行する」を参照してください
6. 保存を選択します。

Macie 内で組織を設定する追加のリージョンごとに、前述のステップを繰り返します。

これらの設定を後で変更するには、前の手順を繰り返し、各設定のチェックボックスをオフにします。

API

プログラムで新しい Macie メンバーアカウントを自動的に有効化して追加するには、Amazon Macie API の UpdateOrganizationConfigurationオペレーションを使用します。リクエストを送信するときは、autoEnable パラメータの値を true に設定します。(デフォルト値は false です。) また、リクエストが適用されるリージョンを必ず指定してください。追加のリージョンで新しいアカウントを自動的に有効化して追加するには、追加のリージョンごとにリクエストを送信します。

を使用してリクエスト AWS CLI を送信する場合は、 update-organization-configuration コマンドを実行し、 auto-enableパラメータを指定して新しいアカウントを自動的に有効化および追加します。例:

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

ここで、*us-east-1* は、新しいアカウントを自動的に有効化して追加するリージョン (米国東部 (バージニア北部) リージョン) です。

後でこの設定を変更し、新しいアカウントの自動的な有効化と追加を停止するには、同じコマンドを再度実行して、該当するリージョンごとに、auto-enable パラメータではなく、no-auto-enable パラメータを使用します。

新しいメンバーアカウントで機密データの自動検出を自動的に有効にすることもできます。アカウントに対してこの機能を有効にすると、Macie はアカウントの S3 バケットからサンプルオブジェクトを継続的に選択し、オブジェクトを分析して機密データが含まれているかどうかを判断します。詳細については、「機密データ自動検出を実行する」を参照してください。メンバーアカウントでこの機能を自動的に有効にするには、 UpdateAutomatedDiscoveryConfigurationオペレーションを使用するか、 を使用している場合は update-automated-discovery-configuration コマンド AWS CLIを実行します。

ステップ 4: 既存の組織アカウントを Macie メンバーアカウントとして有効化して追加する

Macie を と統合すると AWS Organizations、組織内のすべての既存のアカウントで Macie が自動的に有効になるわけではありません。また、アカウントは委任 Macie 管理者アカウントに Macie メンバーアカウントとして自動的に関連付けられません。したがって、Macie 内で組織を統合して設定する最後のステップは、既存の組織アカウントを Macie メンバーアカウントとして追加することです。既存のアカウントを Macie メンバーアカウントとして追加すると、そのアカウントに対して

Macie が自動的に有効化され、お客様は (委任 Macie 管理者として) アカウントの特定の Macie 設定、データ、およびリソースにアクセスできるようになります。

別の Macie 管理者アカウントに現在関連付けられているアカウントを追加することはできないことに注意してください。アカウントを追加するには、アカウント所有者と協力して、まずアカウントを現在の管理者アカウントから関連付けを解除します。また、Macie が現在そのアカウントで停止されている場合、既存のアカウントを追加することはできません。アカウント所有者は、まずアカウントの Macie を再度有効化する必要があります。最後に、 AWS Organizations 管理アカウントをメンバーアカウントとして追加したい場合、そのアカウントのユーザーは、まずアカウントの Macie を有効化する必要があります。

既存の組織アカウントを Macie メンバーアカウントとして有効化して追加するには

既存の組織アカウントを Macie メンバーアカウントとして有効化して追加するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。組織の委任 Macie 管理者のみが、このタスクを実行できます。

Console

コンソールを使用してこのタスクを実行するには、 の AWS Organizations アクションを実行できる必要がありますorganizations:ListAccounts。このアクションにより、組織内のアカウントに関する情報を取得して表示することが許可されます。これらのアクセス許可を持っている場合は、次のステップに従って、既存のアカウントを Macie メンバーアカウントとして有効化して追加します。

既存の組織アカウントを有効化して追加するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、既存のアカウントを有効にして Macie メンバーアカウントとして追加するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

   Accounts (アカウント) ページが開き、Macie アカウントに関連付けられているアカウントのテーブルが表示されます。アカウントが の組織の一部である場合 AWS Organizations、そのタイプは 経由です AWS Organizations。アカウントが既に Macie メンバーアカウントである場合、そのステータスは有効になります。
4. Accounts (アカウント) テーブルで、Macie メンバーアカウントとして追加する各アカウントのチェックボックスをオンにします。
5. Actions (アクション) メニューで、Add member (メンバーを追加) を選択します。

6. 選択したアカウントをメンバーアカウントとして追加することを確認します。

選択したアカウントの追加を確認すると、アカウントのステータスが処理中の有効化 に変わり、次に有効化 に変わります。メンバーアカウントを追加したら、アカウントの機密データ自動検出を有効にすることもできます。アカウント テーブルで、有効にする各アカウントのチェックボックスを選択し、アクション メニューで機密データ自動検出を有効にするを選択します。アカウントに対してこの機能を有効にすると、Macie はアカウントの S3 バケットからサンプルオブジェクトを継続的に選択し、オブジェクトを分析して機密データが含まれているかどうかを判断します。詳細については、「機密データ自動検出を実行する」を参照してください。

Macie 内で組織を設定する追加のリージョンごとに、前述のステップを繰り返します。

API

プログラムで 1 つ以上の既存のアカウントを Macie メンバーアカウントとして有効にして追加するには、Amazon Macie API の CreateMemberオペレーションを使用します。リクエストを送信するときは、サポートされているパラメータを使用して、有効化および追加 AWS アカウント する各 の 12 桁のアカウント ID と E メールアドレスを指定します。また、リクエストが適用されるリージョンも指定します。追加のリージョンで既存のアカウントを有効化して追加するには、追加のリージョンごとにリクエストを送信します。

を有効にして追加 AWS アカウント する のアカウント ID と E メールアドレスを取得するには、オプションで Amazon Macie API の ListMembersオペレーションを使用できます。このオペレーションは、Macie メンバーアカウントではないアカウントを含む、Macie アカウントに関連付けられているアカウントの詳細を提供します。アカウントの `relationshipStatus` プロパティの値が `Enabled` ではない場合、アカウントは Macie メンバーアカウントではありません。

を使用して 1 つ以上の既存のアカウントを有効にして追加するには AWS CLI、create-member コマンドを実行します。`region` パラメータを使用して、アカウントを有効化して追加するリージョンを指定します。`account` パラメータを使用して、追加する各 のアカウント ID AWS アカウント と E メールアドレスを指定します。例:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

ここで、*us-east-1* は、アカウントを Macie メンバーアカウントとして有効化して追加するリージョン (米国東部 (バージニア北部) リージョン) であり、`account` パラメータはそのアカウントのアカウント ID (*123456789012*) と E メールアドレス (*janedoe@example.com*) を指定します。

リクエストが成功すると、指定されたアカウントのステータス `relationshipStatus` がアカウントのインベントリの `Enabled` に変わります。

また、1 つ以上のアカウントの機密データ自動検出を有効にするには、BatchUpdateAutomatedDiscoveryAccountsオペレーションを使用するか、 を使用している場合は batch-update-automated-discovery-accounts コマンド AWS CLIを実行します。アカウントに対してこの機能を有効にすると、Macie はアカウントの S3 バケットからサンプルオブジェクトを継続的に選択し、オブジェクトを分析して機密データが含まれているかどうかを判断します。詳細については、「機密データ自動検出を実行する」を参照してください。

組織の Amazon Macie アカウントの確認

AWS Organizations 組織が Amazon Macie で統合および設定されると、委任 Macie 管理者は Macie 内の組織のアカウントのインベントリにアクセスできます。 Amazon Macie 組織の Macie 管理者として、このインベントリを使用して、 AWS リージョン内で組織の Macie アカウントの統計と詳細を確認できます。これを使用して、アカウントの特定の管理タスクを実行することもできます。

組織の Macie アカウントを確認するには

組織のアカウントを確認するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。コンソールを使用する場合は、 の AWS Organizations アクションを実行できる必要がありますorganizations:ListAccounts。このアクションにより、 AWS Organizations内で組織の一部であるアカウントに関する情報を取得して表示することが許可されます。

Console

Amazon Macie コンソールを使用して組織の Macie アカウントを確認するには、次のステップに従います。

組織のアカウントを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、組織のアカウントを確認するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

アカウントページが開き、現在の AWS リージョン内で Macie アカウントに関連付けられている集約された統計とアカウントのテーブルが表示されます。

アカウントページの先頭に、次の集約された統計が表示されます。

経由 AWS Organizations

アクティブ は、 を通じてアカウントに関連付けられ、現在組織内の Macie メンバーアカウント AWS Organizations であるアカウントの総数を報告します。Macie はこれらのアカウントに対して有効化されており、お客様はアカウントの Macie 管理者です。

すべての は、現在 Macie メンバーアカウントではないアカウントを含め AWS Organizations、 を通じてアカウントに関連付けられているアカウントの総数を報告します。

招待により

アクティブにより、Macie の招待によってお客様のアカウントに関連付けられていて、現在 Macie メンバーアカウントであるアカウントの総数が報告されます。これらのアカウントは、を通じてアカウントに関連付けられません AWS Organizations。Macie はアカウントに対して有効化されており、お客様から Macie メンバーシップへの招待を受け入れたため、お客様はアカウントの Macie 管理者です。

すべてにより、お客様からの招待に応答していないアカウントを含む、Macie の招待によってお客様のアカウントに関連付けられているアカウントの総数が報告されます。

アクティブ/すべて

Active は、 を通じて、 AWS Organizations または Macie の招待によって、現在 Macie メンバーアカウントであるアカウントの総数を報告します。Macie はこれらのアカウントに対して有効化されており、お客様はアカウントの Macie 管理者です。

すべての は、 を通じて、 AWS Organizations または Macie の招待によって、アカウントに関連付けられているアカウントの総数を報告します。これには、 の組織の一部であり、現在 Macie AWS Organizations メンバーアカウントではないアカウント、および Macie メンバーシップの招待に応答していないアカウントが含まれます。

テーブルには、現在のリージョン内の各アカウントの詳細が表示されます。テーブルには、AWS Organizations または Macie の招待によって Macie アカウントに関連付けられているすべてのアカウントが含まれます。

アカウント ID

AWS アカウントのアカウント ID と E メールアドレス。

名前

AWS アカウントのアカウント名。この値は通常、Macie の招待によってお客様のアカウントに関連付けられているアカウントの場合、該当なし になります。

タイプ

AWS Organizations を通じて、または Macie の招待によって、そのアカウントがお客様のアカウントに関連付けられる方法。

ステータス

お客様のアカウントとそのアカウントの関係のステータス。 AWS Organizations 組織内のアカウント (タイプは 経由) AWS Organizationsの場合、指定できる値は次のとおりです。

- アカウントが停止— AWS アカウント が停止されています。
- 作成済み/有効化中— Macie は、アカウントを Macie メンバーアカウントとして有効化して追加するためのリクエストを処理しています。
- 有効化— アカウントは Macie メンバーアカウントです。Macie はアカウントに対して有効化されており、お客様はそのアカウントの Macie 管理者です。
- メンバーではない – アカウントは の組織の一部 AWS Organizations ですが、Macie メンバーアカウントではありません。
- 一時停止 (停止)— アカウントは Macie メンバーアカウントですが、現在 Macie はアカウントを停止しています。
- リージョンが無効 – アカウントは の組織の一部 AWS Organizations ですが、現在のリージョンは に対して無効になっています AWS アカウント。
- 削除 (関連付け解除— アカウントは以前は Macie メンバーアカウントでしたが、その後メンバーアカウントとして削除されました。(Macie 管理者アカウントからそのアカウントを解除しました。) Macie は引き続きそのアカウントに対して有効化されています。

最終ステータス更新

お客様または関連するアカウントが、お客様のアカウント間の関係に影響を与えたアクションを最後に実行したとき。

機密データの自動検出

アカウントで機密データの自動検出が現在有効または無効になっているかどうか。

特定のフィールドでテーブルをソートするには、フィールドの列見出しを選択します。ソート順序を変更するには、列見出しを再度選択します。テーブルをフィルタリングするには、フィル

ターボックスにカーソルを置き、フィールドのフィルター条件を追加します。結果をさらに絞り込むには、追加のフィールドでフィルター条件を追加します。

API

組織のアカウントをプログラムで確認するには、Amazon Macie API の ListMembersオペレーションを使用して、リクエストが適用されるリージョンを指定します。追加のリージョン内のアカウントを確認するには、追加のリージョンごとにリクエストを送信します。

リクエストを送信するときは、onlyAssociated パラメータを使用して、レスポンスに含めるアカウントを指定します。デフォルトでは、Macie は、 を通じて、 AWS Organizations または Macie の招待によって、指定されたリージョン内の Macie メンバーアカウントであるアカウントのみに関する詳細を返します。メンバーアカウントではないアカウントを含む、Macie アカウントに関連付けられているすべてのアカウントについて、これらの詳細を取得するには、リクエストに onlyAssociated パラメータを含め、パラメータの値を false に設定します。

AWS Command Line InterfaceAWS CLIを使用して組織のアカウントを確認するには、list-members コマンドを実行します。only-associated パラメータでは、関連するすべてのアカウントを含めるか、Macie メンバーアカウントのみを含めるかを指定します。メンバーアカウントのみを含めるには、このパラメータを省略するか、パラメータの値を true に設定します。すべてのアカウントを含めるには、この値を false に設定します。例:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

ここで、*us-east-1* は、リクエストが適用されるリージョン (米国東部 (バージニア北部) リージョン) です。

リクエストが成功すると、Macie は members 配列を返します 配列には、リクエストで指定された基準を満たす各アカウントの member オブジェクトが含まれます。そのオブジェクトでは、relationshipStatus フィールドは、指定されたリージョン内のお客様のアカウントと他方のアカウント間の関係の現在のステータスを示します。 AWS Organizations 組織内のアカウントの場合、指定できる値は次のとおりです。

- AccountSuspended – AWS アカウント は中断されます。
- Created — Macie は、アカウントを Macie メンバーアカウントとして有効化して追加するためのリクエストを処理しています。
- Enabled — アカウントは Macie メンバーアカウントです。Macie はアカウントに対して有効化されており、お客様はそのアカウントの Macie 管理者です。

- `Paused` — アカウントは Macie メンバーアカウントですが、Macie は現在アカウントが停止 (一時停止) されています。
- `RegionDisabled` – アカウントは の組織の一部 AWS Organizations ですが、現在のリージョンは に対して無効になっています AWS アカウント。
- `Removed`— アカウントは以前は Macie メンバーアカウントでしたが、その後メンバーアカウントとして削除されました。(Macie 管理者アカウントからそのアカウントの関連付けを解除しました。) Macie は引き続きそのアカウントに対して有効化されています。

`member` オブジェクト内の他のフィールドの詳細については、Amazon Macie API リファレンスのメンバーを参照してください。

組織の Amazon Macie メンバーアカウントの管理

AWS Organizations 組織が Amazon Macie で統合および設定されると、組織の委任 Macie 管理者はメンバーアカウントの特定の Macie 設定、データ、リソースにアクセスできます。 Amazon Macie

組織の Macie 管理者として、Macie 内の特定のアカウント管理および管理タスクを一元的に実行することもできます。例:

- Macie メンバーアカウントを追加および削除
- アカウントの Macie 有効化または停止など個別アカウントの Macie ステータスを管理
- 個別アカウントおよび組織全体の Macie クォータと推定使用コストを監視

また、Macie メンバーアカウントの Amazon Simple Storage Service (Amazon S3) のインベントリデータとポリシー結果を確認することもできます。また、アカウントが所有する S3 バケット内の機密データを検出できます。実行できるタスクの詳細なリストについては、Amazon Macie 管理者とメンバーアカウントの関係について理解するを参照してください。

デフォルトでは、Macie は、組織内のすべての Macie メンバーアカウントの関連データとリソースを可視化します。ドリルダウンして、個々のアカウントのデータとリソースを確認することもできます。例えば、概要ダッシュボードを使用して、組織の Amazon S3 セキュリティ体制を評価する場合は、アカウントごとにデータをフィルタリングできます。同様に、推定使用量のコストをモニタリングする場合は、個々のメンバーアカウントの推定コストの内訳にアクセスできます。

管理者およびメンバーアカウントに共通するタスクに加えて、組織のさまざまな管理タスクを実行できます。

タスク

- Amazon Macie メンバーアカウントを組織に追加する
- 組織内のメンバーアカウントの Amazon メイシーを一時停止
- 組織からの Amazon Macie メンバーアカウントの削除

組織の Macie 管理者は、Amazon Macie コンソールまたは Amazon Macie API を使用してこれらのタスクを実行できます。コンソールを使用する場合は、 の AWS Organizations アクションを実行できる必要がありますorganizations:ListAccounts。このアクションにより、 AWS Organizations内で組織の一部であるアカウントに関する情報を取得して表示することが許可されます。

Amazon Macie メンバーアカウントを組織に追加する

場合によっては、アカウントを Macie メンバーアカウントとして手動で追加する必要があります。これは、以前にメンバーアカウントとして削除 (関連付け解除) したアカウントの場合です。これは、アカウントが で組織に追加されるときに、新しいメンバーアカウントを自動的に有効化して追加するように Macie を設定していない場合にも当てはまります AWS Organizations。

Macie メンバーアカウントとしてアカウントを追加する場合：

- Macie は、リージョンでまだ有効になっていない場合 AWS リージョン、現在の でアカウントに対して有効になっています。
- アカウントは、リージョンのメンバーアカウントとして Macie 管理者アカウントに関連付けられます。メンバーアカウントは、招待またはお客様のアカウント間にこの関係を確立したというその他の通知を受け取りません。
- リージョンのアカウントで機密データの自動検出が有効になっている場合があります。これは、組織に指定した構成設定によって異なります。詳細については、「機密データ自動検出の設定」を参照してください。

すでに関連付けられているアカウントは別の Macie 管理者アカウントに追加できないことに注意してください。アカウントは、まず現在の管理者アカウントから関連付けを解除する必要があります。さらに、Macie がアカウントに対して既に有効になっていない限り、 AWS Organizations 管理アカウントをメンバーアカウントとして追加することはできません。追加の要件については、で Amazon Macie を使用する際の考慮事項と推奨事項 AWS Organizationsを参照してください。

組織に Macie メンバーアカウントを追加するには

1 つ以上の Macie メンバーアカウントを組織に追加するには、Amazon Macie コンソールまたは Amazon Macie API を使用することができます。

Console

Amazon Macie コンソールを使用して 1 つ以上の Macie メンバーアカウントを追加するには、次のステップに従います。

Macie メンバーアカウントを追加するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、メンバーアカウントを追加するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウント ページが開き、お客様のアカウントに関連付けられているアカウントのテーブルが表示されます。
4. (オプション) で組織の一部であり AWS Organizations 、Macie メンバーアカウントではないアカウントをより簡単に識別するには、Accounts テーブルの上にあるフィルターボックスを使用して、次のフィルター条件を追加します。

   - タイプ = 組織
   - ステータス = メンバーではない

   また、以前に削除したがメンバーアカウントとして追加する可能性のあるアカウントを表示するには、ステータス = 削除済み (関連付け解除済み)も追加します。
5. アカウントテーブルで、メンバーアカウントとして追加する各アカウントのチェックボックスをオンにします。
6. Actions (アクション) メニューで、Add member (メンバーを追加) を選択します。
7. 選択したアカウントをメンバーアカウントとして追加することを確認します。

選択を確認すると、選択したアカウントのステータスが処理中の有効化 に変わり、アカウントインベントリで有効化 に変わります。

メンバーアカウントを追加する追加のリージョンごとに、前述のステップを繰り返します。

API

プログラムで 1 つ以上の Macie メンバーアカウントを追加するには、Amazon Macie API の CreateMemberオペレーションを使用します。

リクエストを送信するときは、サポートされているパラメータを使用して、追加 AWS アカウント する各 の 12 桁のアカウント ID と E メールアドレスを指定します。また、リクエストが適用されるリージョンも指定します。追加のリージョンでアカウントを追加するには、追加のリージョンごとにリクエストを送信します。

追加するアカウントのアカウント ID と E メールアドレスを取得するには、 AWS Organizations API の ListAccountsオペレーションと Amazon Macie API の ListMembersオペレーションの出力を関連付けることができます。Macie API の ListMembers オペレーションでは、リクエストに `onlyAssociated` パラメータを含め、パラメータの値を `false` に設定します。オペレーションが成功すると、Macie は、指定されたリージョンの Macie 管理者アカウントに関連付けられているすべてのアカウント (現在メンバーアカウントではないアカウントを含む) の詳細を提供する `members` 配列を返します。配列では次の点に注意してください。

- アカウントの `relationshipStatus` プロパティの値が `Enabled` ではない場合、そのアカウントはお客様のアカウントに関連付けられていますが、Macie メンバーアカウントではありません。
- アカウントが配列に含まれていないが、 AWS Organizations API の ListAccounts オペレーションの出力に含まれている場合、そのアカウントは AWS Organizations 内で組織の一部となりますが、お客様のアカウントに関連付けられていないため、Macie メンバーアカウントではありません。

を使用してメンバーアカウントを追加するには AWS CLI、create-member コマンドを実行します。`region` パラメータを使用して、アカウントを追加するリージョンを指定します。`account` パラメータを使用して、追加する各アカウントのアカウント ID とメールアドレスを指定します。例:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

ここで *us-east-1* は、メンバーアカウントとしてアカウントを追加するリージョン (米国東部 (バージニア北部) リージョン) であり、`account` パラメータは、アカウントのアカウント ID (*123456789012*) とメールアドレス (*janedoe@example.com*) を指定します。

リクエストが成功すると、その指定されたアカウントのステータス`relationshipStatus`がアカウントインベントリの `Enabled` に変わります。

組織内のメンバーアカウントの Amazon メイシーを一時停止

内の組織の Macie 管理者として AWS Organizations、組織内のメンバーアカウントの Macie を停止できます。これを行うと、後でアカウントの Macie を再度有効化することもできます。

メンバーアカウントの メイシーを一時停止と、次のようになります。

- Macie は、現在の AWS リージョン内のアカウントの Amazon S3 データに関するメタデータへのアクセスを失い、提供を停止します。
- Macie は、リージョン内のアカウントのすべてのアクティビティの実行を停止します。これには、セキュリティとアクセスコントロールのための S3 バケットのモニタリング、機密データの自動検出、および現在進行中の機密データ検出ジョブの実行などが含まれます。
- Macie は、リージョン内のアカウントによって作成された機密データ検出ジョブをすべてキャンセルします。ジョブがキャンセルされた後は、ジョブを再開したり再起動したりすることはできません。メンバーアカウントが所有するデータを分析するためのジョブを作成した場合、Macie はジョブをキャンセルしません。代わりに、ジョブはアカウントが所有するリソースをスキップします。

アカウントが停止されている間、Macie は該当するリージョン内のアカウントの Macie セッション識別子、設定、およびリソースを保持します。例えば、アカウントの調査結果はそのまま残り、最大 90 日間は影響を受けません。そのリージョン内のアカウントで Macie が停止されている間、該当するリージョン内のアカウントに対する Macie の請求は組織に発生しません。

組織内のメンバーアカウントの メイシーを一時停止には

組織内のメンバーアカウントの メイシーを一時停止には、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用してメンバーアカウントの メイシーを一時停止には、次のステップに従います。

メンバーアカウントの メイシーを一時停止には

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、メンバーアカウントの Macie を停止するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウント ページが開き、お客様のアカウントに関連付けられているアカウントのテーブルが表示されます。

4. アカウント テーブルで、停止するアカウントのチェックボックスをオンにします。
5. アクションメニューで、メイシーを一時停止を選択します。
6. アカウントの メイシーを一時停止ことを確認します。

停止を確認すると、アカウントのステータスがインベントリで 一時停止 (停止)に変わります。

アカウントのメイシーを一時停止したい追加リージョンごとに、前述の手順を繰り返します。

API

メンバーアカウントの Macie をプログラムで停止するには、Amazon Macie API の UpdateMemberSessionオペレーションを使用します。

リクエストを送信するときは、 idパラメータを使用して、Macie を停止 AWS アカウント するの 12 桁のアカウント ID を指定します。status パラメータでは、Macie アカウントの新しいステータスとして PAUSED を指定します。また、リクエストが適用されるリージョンも指定します。追加のリージョンでアカウントを停止するには、追加のリージョンごとにリクエストを送信します。

停止するアカウントのアカウント ID を取得するには、Amazon Macie API の ListMembersオペレーションを使用できます。これを実行する場合は、リクエストに onlyAssociated パラメータを含めることで結果をフィルタリングすることを検討してください。このパラメータの値を true に設定した場合、Macie は現在メンバーアカウントであるアカウントのみの詳細を提供する members 配列を返します。

を使用してメンバーアカウントの Macie を停止するには AWS CLI、 update-member-session コマンドを実行します。region パラメータを使用して Macie を停止するリージョンを指定し、 idパラメータを使用して Macie を停止 AWS アカウント する のアカウント ID を指定します。status パラメータでは、PAUSED を指定します。例:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

ここで、*us-east-1* は メイシーを一時停止リージョン (米国東部 (バージニア北部) リージョン)であり、*123456789012* は メイシーを一時停止アカウントのアカウント ID であり、PAUSED はそのアカウントの Macie の新しいステータスです。

リクエストが成功すると、Macie は空のレスポンスを返し、指定されたアカウントのステータスはアカウントのインベントリの Paused に変わります。

組織からの Amazon Macie メンバーアカウントの削除

メンバーアカウントの Macie 設定、データ、およびリソースへのアクセスを停止したい場合、お客様は Macie メンバーアカウントとしてアカウントを削除できます。これを行うには、Macie 管理者アカウントからそのアカウントの関連付けを解除します。ご自身でのみ、メンバーアカウントに対してこれを実行できることに注意してください。 AWS Organizations メンバーアカウントは Macie 管理者アカウントとの関連付けを解除できません。

Macie メンバーアカウントを削除しても、Macie は現在の AWS リージョン内のアカウントに対して有効化されたままとなります。ただし、アカウントは Macie 管理者アカウントから関連付けが解除され、スタンドアロンの Macie アカウントになります。これは、アカウントの Amazon S3 データのメタデータやポリシーの結果など、アカウントのすべての Macie 設定、データ、およびリソースにアクセスできなくなることを意味します。これは、アカウントが所有する S3 バケット内の機密データ検出で Macie を使用できなくなることも意味します。これを実行する機密データ検出ジョブを既に作成している場合、ジョブはアカウントが所有するバケットをスキップします。アカウントの機密データ自動検出を有効にした場合、ユーザーとメンバーアカウントの両方が、アカウントの自動検出の実行中に Macie が生成して直接提供した統計データ、インベントリデータ、およびその他の情報にアクセスできなくなります。

Macie メンバーアカウントを削除しても、アカウントは引き続きアカウントのインベントリに表示されます。Macie は、お客様がアカウントを削除したことをアカウントの所有者に通知しません。アカウントは後で組織に追加できます。アカウントを追加して 30 日以内にそのアカウントの自動機密データ検出を有効にすると、アカウントの自動検出の実行中に Macie が以前に生成して直接提供したデータや情報へのアクセスも回復します。

組織から Macie メンバーアカウントを削除するには

組織から Macie メンバーアカウントを削除するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用して Macie メンバーアカウントを削除するには、次のステップに従います。

Macie メンバーアカウントを削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、メンバーアカウントを削除するリージョンを選択します。

3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウント ページが開き、お客様のアカウントに関連付けられているアカウントのテーブルが表示されます。
4. Accounts (アカウント) テーブルで、メンバーアカウントとして削除するアカウントのチェックボックスをオンにします。
5. アクションメニューで、アカウントを解除するを選択します。
6. 選択されたアカウントをメンバーアカウントとして削除することを確認します。

選択を確認すると、アカウントのステータスが、アカウントのインベントリで Removed (disassociated) (削除 (関連付け解除)) に変わります。

メンバーアカウントを削除する追加のリージョンごとに、前述のステップを繰り返します。

API

Macie メンバーアカウントをプログラムで削除するには、Amazon Macie API の DisassociateMemberオペレーションを使用します。

リクエストを送信するときは、 `id`パラメータを使用して、削除するメンバーアカウントの 12 桁の AWS アカウント ID を指定します。また、リクエストが適用されるリージョンも指定します。追加のリージョン内のアカウントを削除するには、追加のリージョンごとにリクエストを送信します。

削除するメンバーアカウントのアカウント ID を取得するには、Amazon Macie API の ListMembersオペレーションを使用できます。これを実行する場合は、リクエストに `onlyAssociated` パラメータを含めることで結果をフィルタリングすることを検討してください。このパラメータの値を `true` に設定した場合、Macie は現在 Macie メンバーアカウントであるアカウントのみの詳細を提供する `members` 配列を返します。

を使用して Macie メンバーアカウントを削除するには AWS CLI、disassociate-member コマンドを実行します。`region` パラメータを使用して、アカウントを削除するリージョンを指定します。`id` パラメータを使用して、削除するメンバーアカウントのアカウント ID を指定します。例:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

ここで、*`us-east-1`* は、アカウントを削除するリージョン (米国東部 (バージニア北部) リージョン) であり、*`123456789012`* は削除するアカウントのアカウント ID です。

リクエストが成功すると、Macie は空のレスポンスを返し、指定されたアカウントのステータスはアカウントのインベントリの `Removed` に変わります。

組織の別の Amazon Macie 管理者アカウントの指定

AWS Organizations 組織が Amazon Macie に統合され、設定されると、 AWS Organizations 管理アカウントは別のアカウントを組織の委任 Macie 管理者アカウントとして指定できます。 Amazon Macie

組織の AWS Organizations 管理アカウントのユーザーとして、組織の別の Macie 管理者アカウントを指定する前に、次のアクセス許可要件を満たしていることを確認します。

- 組織の Macie 管理者アカウントを最初に指定するために必要であったものと同じアクセス許可を持つ必要があります。また、次の AWS Organizations アクションの実行も許可されている必要があります: `organizations:DeregisterDelegatedAdministrator`。この追加アクションにより、現在の指定の削除が許可されます。
- お客様のアカウントが Macie メンバーアカウントとなっている場合は、現時点の Macie 管理者が、Macie メンバーアカウントとしてのお客様のアカウントを削除する必要があります。そうしないと、別の管理者アカウントを指定する Macie オペレーションにはアクセスできません。お客様が新しい管理者アカウントを指定すると、新しい Macie 管理者がお客様のアカウントを Macie メンバーアカウントとして再度追加できます。

組織が複数の で Macie を使用している場合は AWS リージョン、組織が Macie を使用する各リージョンで委任 Macie 管理者アカウントも変更してください。委任 Macie 管理者アカウントは、これらのすべてのリージョンで同じである必要があります。で複数の組織を管理する場合 AWS Organizations、アカウントは一度に 1 つの組織の委任 Macie 管理者アカウントになることができることに注意してください。追加の要件については、で Amazon Macie を使用する際の考慮事項と推奨事項 AWS Organizationsを参照してください。

> **Note**
>
> 組織の別の Macie 管理者アカウントを指定すると、組織内のアカウントの機密データ自動検出を実行している間に Macie が生成して直接提供した既存の統計データ、インベントリデータ、その他の情報へのアクセスも無効にします。新しい Macie 管理者アカウントは、既存のデータにアクセスできません。指定を変更し、新しい Macie 管理者がアカウントの自動検出を有効にすると、Macie はアカウントの自動検出を実行するときに新しいデータを生成して維持します。

組織の別の Macie 管理者アカウントを指定するには

組織の別の Macie 管理者アカウントを指定するには、Amazon Macie コンソールを使用するか、Amazon Macie と AWS Organizations APIsの組み合わせを使用できます。組織の指定を変更できるのは、 AWS Organizations 管理アカウントのユーザーのみです。

Console

Amazon Macie コンソールを使用して指定を変更するには、次のステップに従います。

別の Macie 管理アカウントを指定するには

1. AWS Organizations 管理アカウント AWS Management Console を使用して にサインインします。
2. ページの右上隅にある AWS リージョン セレクターを使用して、指定を変更するリージョンを選択します。
3. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
4. Macie が現在のリージョンで管理アカウントに対して有効化されているかどうかに応じて、次のいずれかを実行します。
   - Macie が有効化されていない場合は、Welcome Page (ようこそページ) の Get started (開始方法) を選択します。
   - Macie が有効化されている場合は、ナビゲーションペインの Settings (設定) を選択します。
5. Delegated administrator (委任管理者) の下で、Remove (削除) を選択します。指定を変更するには、まず現在の指定を削除する必要があります。
6. 現在の指定を削除することを確認します。
7. 委任管理者 で、組織の新しい Macie 管理者アカウントとして AWS アカウント 指定する の 12 桁のアカウント ID を入力します。
8. [委任] を選択します。

Macie を AWS Organizationsと統合する追加のリージョンごとに、前述のステップを繰り返します。

API

プログラムで指定を変更するには、Amazon Macie API の 2 つのオペレーションと API の 1 つのオペレーションを使用します AWS Organizations 。これは、新しい指定を送信する AWS Organizations 前に、Macie と の両方で現在の指定を削除する必要があるためです。

現在の指定を削除するには、以下を実行します。

1. Macie API の DisableOrganizationAdminAccountオペレーションを使用します。必須adminAccountIdパラメータには、組織の Macie 管理者アカウントとして現在指定されている の 12 AWS アカウント 桁のアカウント ID を指定します。
2. API の DeregisterDelegatedAdministrator AWS Organizations オペレーションを使用します。AccountId パラメータでは、組織の Macie 管理者アカウントとして現在指定されているアカウントの 12 桁のアカウント ID を指定します。この値は、前の Macie リクエストで指定したアカウント ID と一致する必要があります。ServicePrincipal パラメータでは、Macie サービスプリンシパルmacie.amazonaws.comを指定します。

現在の指定を削除したら、Macie API の EnableOrganizationAdminAccountオペレーションを使用して新しい指定を送信します。必須adminAccountIdパラメータには、組織の新しい Macie 管理者アカウントとして AWS アカウント 指定する の 12 桁のアカウント ID を指定します。

を使用して指定を変更するにはAWS CLI、Macie API の disable-organization-admin-account コマンドと AWS Organizations API の deregister-delegated-administrator コマンドを実行します。これらのコマンドは AWS Organizations、Macie と の現在の指定をそれぞれ削除します。admin-account-id および account-idパラメータには、削除する の 12 桁のアカウント ID AWS アカウント を現在の Macie 管理者アカウントとして指定します。region パラメータを使用して、削除が適用されるリージョンを指定します。例:

```
C:\> aws macie2 disable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333 && aws organizations deregister-delegated-administrator --
region us-east-1 --account-id 111122223333 --service-principal macie.amazonaws.com
```

ここで、

- *us-east-1*は、削除が適用されるリージョン (米国東部 (バージニア北部) リージョン) です。
- *111122223333*は、Macie 管理者アカウントとして削除するアカウントのアカウント ID です。
- macie.amazonaws.com は、Macie サービスプリンシパルです。

現在の指定を削除したら、Macie API の enable-organization-admin-account コマンドを実行して新しい指定を送信します。admin-account-id パラメータには、組織の新しい Macie 管理者アカウントとして AWS アカウント 指定する の 12 桁のアカウント ID を指定します。region パラメータを使用して、指定が適用されるリージョンを指定します。例:

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 444455556666
```

ここで、*us-east-1* は指定が適用されるリージョン (米国東部 (バージニア北部) リージョン) であり、*444455556666* は新しい Macie 管理者アカウントとして指定するアカウントのアカウント ID です。

Amazon Macie の AWS Organizationsとの統合の無効化

AWS Organizations 組織が Amazon Macie と統合されると、 AWS Organizations 管理アカウントはその後統合を無効にすることができます。 AWS Organizations 管理アカウントのユーザーは、 で Macie の信頼されたサービスアクセスを無効にすることでこれを行うことができます AWS Organizations。

Macie の信頼されたサービスアクセスを無効化すると、以下が起こります。

- Macie は、 で信頼されたサービスとしてのステータスを失います AWS Organizations。
- 組織の Macie 管理者アカウントは、すべての AWS リージョンの Macie メンバーアカウントのすべての Macie 設定、データ、およびリソースへのアクセスを失います。
- Macie メンバーアカウントはすべてスタンドアロンの Macie アカウントになります。Macie が 1 つ以上のリージョン内のメンバーアカウントに対して有効化されている場合、Macie はそのリージョン内のアカウントに対して有効化された状態が継続します。ただし、そのアカウントはどのリージョンの Macie 管理者アカウントとも関連付けられなくなります。さらに、アカウントは、Macie がアカウントの機密データ自動検出を実行している間に生成して直接提供した統計データ、インベントリデータ、およびその他の情報にアクセスできなくなります。

信頼されたサービスアクセスを無効にする結果の詳細については、 ユーザーガイドの「他の AWS Organizations で AWS のサービスを使用するAWS Organizations 」を参照してください。

Macie の信頼されたサービスのアクセスを無効にするには

信頼されたサービスアクセスを無効にするには、 AWS Organizations コンソールまたは AWS Organizations API を使用できます。Macie の信頼されたサービスアクセスを無効にすることができるのは、 AWS Organizations 管理アカウントのユーザーのみです。必要なアクセス許可に関する詳細は、AWS Organizations ユーザーガイドの信頼できるアクセスを無効にするために必要なアクセス許可を参照してください。

信頼されたサービスアクセスを無効にする前に、必要に応じて組織の委任された Macie 管理者に連絡して、メンバーアカウントの Macie を停止または無効にし、それらのアカウントの Macie リソースをクリーンアップしてください。

Console

AWS Organizations コンソールを使用して信頼されたサービスアクセスを無効にするには、次の手順に従います。

信頼されたサービスのアクセスを無効にするには

1. AWS Organizations 管理アカウント AWS Management Console を使用して にサインインします。
2. https://console.aws.amazon.com/organizations/ で AWS Organizations コンソールを開きます。
3. ナビゲーションペインで Services (サービス) を選択します。
4. 統合サービス で Amazon Macie を選択します。
5. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
6. 信頼されたアクセスを無効化することを確認します。

API

信頼できるサービスアクセスをプログラムで無効にするには、 AWS Organizations API の DisableAWSServiceAccess オペレーションを使用します。`ServicePrincipal` パラメータでは、Macie サービスプリンシパル `macie.amazonaws.com` を指定します。

AWS Command Line Interface （ AWS CLI ） を使用して信頼されたサービスアクセスを無効にするには、 AWS Organizations API の disable-aws-service-access コマンドを実行します。`service-principal` パラメータでは、Macie サービスプリンシパル `macie.amazonaws.com` を指定します。例:

```
C:\> aws organizations disable-aws-service-access --service-principal
 macie.amazonaws.com
```

招待による Amazon Macie アカウントの管理

複数の Amazon Macie アカウントを、次の 2 つの方法で集中管理できます: Macie を AWS Organizations と統合する、またはメンバーシップの招待を使用する。メンバーシップの招待を使用する場合、指定 Macie 管理者は最大 1,000 アカウントの Macie を管理できます。管理者は、Amazon Simple Storage Service (Amazon S3) のインベントリデータにアクセスし、アカウントが所有する S3 バケット内の機密データを検出することもできます。管理者が実行できるタスクの詳細については、Amazon Macie 管理者とメンバーアカウントの関係について理解するを参照してください。

招待ベースの組織では、Macie でメンバーシップ招待を送信および受け入れることで、Macie アカウントを相互に関連付けます。招待を送信し、別のアカウントによって受け入れられた場合、お客様は他のアカウントの Macie 管理者になり、他方のアカウントは組織のメンバーアカウントになります。招待を受け取って受け入れると、お客様のアカウントはメンバーアカウントになり、Macie 管理者はアカウントの特定の Macie 設定、データ、およびリソースにアクセスできるようになります。

> **Tip**
>
> Macie で招待ベースの組織を作成する場合は、後で代わりに AWS Organizations の使用に移行します。両方の方法を同時に使用して、複数の Macie アカウントを管理することもできます。たとえば、AWS 環境にテストアカウントが含まれている場合、AWS Organizations 内の組織からアカウントを除外し、招待によりそれらを個別に管理します。

このセクションのトピックでは、招待ベースの組織を作成して参加する方法、および組織のさまざまな管理タスクを実行する方法について説明します。

トピック

- Amazon Macie 内の招待ベースの組織に関する考慮事項とレコメンデーション
- Amazon Macie での招待ベースの組織の作成と管理
- 招待ベースの組織の Amazon Macie アカウントの確認
- 招待ベースの組織の別の Amazon Macie 管理者アカウントの指定
- Amazon Macie で招待ベースの組織内のメンバーシップを管理する

Amazon Macie 内の招待ベースの組織に関する考慮事項とレコメンデーション

Amazon Macie で招待ベースの組織を作成または管理する前に、次の要件とレコメンデーションを検討してください。また、Macie 管理者アカウントとメンバーアカウントの関係を理解してください。

トピック

Macie 管理者アカウントの選択

組織の Macie 管理者アカウントにするアカウントを決定する際には、次の点に注意してください。

- 組織が持つことができる Macie 管理者アカウントは 1 つのみです。
- アカウントを Macie 管理者とメンバーアカウントに同時に設定することはできません。
- Macie はリージョンでのサービスです。つまり、Macie 管理者アカウントとメンバーアカウント間の関連付けはリージョン別です。関連付けは AWS リージョン 、招待の送信元および承諾元のにのみ存在します。例えば、Macie 管理者が米国東部 (バージニア北部) リージョンで招待を送信し、それらの招待が受け入れられる場合、Macie 管理者はそのリージョン内のメンバーアカウントのみを管理できます。
- Macie アカウントを複数の で一元管理するには AWS リージョン、Macie 管理者は、組織が現在 Macie を使用している、または使用する予定の各リージョンにサインインし、それらの各リージョンの適切なアカウントに招待を送信する必要があります。Macieが現在利用可能なリージョンのリストについては、AWS 全般のリファレンスのAmazon Macieエンドポイントとクォータを参照してください。
- メンバーアカウントは、一度に 1 つの Macie 管理者アカウントのみと関連付けることができます。組織が複数のリージョンで Macie を使用している場合、これは Macie 管理者アカウントがそれらのすべてのリージョンで同じである必要があることを意味します。ただし、管理者アカウントとメンバーアカウントは、各リージョンで個別に招待を送信および受け入れる必要があります。

Macie 管理者の AWS アカウント が停止、分離、または閉鎖されている場合、関連するすべてのメンバーアカウントはメンバーアカウントとして自動的に削除されますが、Macie は引き続きアカウン

トに対して有効になります。アカウントはスタンドアロン Macie アカウントになります。メンバーアカウントで機密データの自動検出が有効になっている場合、そのアカウントでは無効になります。これにより、アカウントの自動検出の実行中に Macie が生成して直接提供した統計データ、インベントリデータ、その他の情報へのアクセスも無効になります。30 日後、このデータは期限切れになり、Macie はそのデータを完全に削除します。有効期限が切れる前にデータへのアクセスを復元するには、Macie 管理者の を復元し AWS アカウント、そのアカウントを使用して組織を再度作成して設定します。

招待の送信と Macie メンバーアカウントの管理

招待ベースの組織の Macie 管理者として、招待を送信し、組織内のアカウントを管理するときは、次の点に注意してください。

- 招待を送信すると、関連するデータが 間で転送される場合があります AWS リージョン。これは、Macie が 米国東部 (バージニア北部) リージョンでのみ動作する E メール検証サービスを使用して、受信アカウントの E メールアドレスを検証するためです。
- Macie を有効にしていないアカウントを含め AWS アカウント、アクティブな に招待を送信できます。ただし、招待を受け入れまたは拒否するには、受信アカウントは招待の送信元のリージョンで Macie を有効化する必要があります。
- Macie 管理者アカウントは、各 AWS リージョン内では、わずか 1,000 個のアカウントにしか関連付けることができません。これには、まだ招待に応答していないアカウントも含まれます。アカウントがこのクォータを満たしている場合、必要な数の関連付けられたアカウントを削除するか、必要な数の拒否された招待を受け取る、またはその 2 つの組み合わせを受け取るまで、追加のアカウントを追加または招待することはできません。

  現在アカウントに関連付けられているアカウントの数を確認するには、Amazon Macie コンソールのアカウントページまたは Amazon Macie API の ListMembersオペレーションを使用できます。詳細については、「招待ベースの組織の Amazon Macie アカウントの確認」を参照してください。
- アカウントは、一度に 1 つの Macie 管理者アカウントのみと関連付けることができます。これは、アカウントが別の Macie 管理者アカウントに既に関連付けられている場合、お客様の招待は受け入れられないことを意味します。アカウントは、まず現在の Macie 管理者アカウントから関連付けを解除する必要があります。
- 招待ベースの組織では、メンバーアカウントはいつでも Macie 管理者アカウントから関連付けを解除できます。この場合、Macie はアカウントに対して引き続き有効になりますが、そのアカウントはスタンドアロン Macie アカウントになります。Macie は、メンバーアカウントが管理者アカ

ウントから関連付けを解除してもお客様に通知しません。ただし、アカウントは引き続きアカウントのインベントリに表示され、メンバー退会済み ステータスとなります。

- 組織からメンバーアカウントを削除すると、Macie はそのアカウントに対して引き続き有効になります。アカウントはスタンドアロン Macie アカウントになります。

メンバーシップの招待への応答と管理

招待の受信者または招待ベースの組織のメンバーとして、受け取った招待に応答して管理するときは、次の点に注意してください。

- 招待を受け入れる前に、Macie 管理者アカウントとメンバーアカウントの関係を理解してください。
- アカウントは、一度に 1 つの Macie 管理者アカウントのみと関連付けることができます。招待を承諾し、その後に別の組織に (招待または を通じて AWS Organizations) 参加する場合は、まず現在の Macie 管理者アカウントからアカウントの関連付けを解除する必要があります。その後、他の組織に参加できます。
- 招待を受け入れまたは拒否するには、招待の送信元の AWS リージョン 内の Macie を有効化する必要があります。招待を送信したアカウントは、そのリージョンで Macie を有効化することはできません。招待の拒否はオプションです。招待を拒否した場合、招待を拒否した後に、必要に応じて該当するリージョンで Macie を無効にできます。
- Macie 管理者の場合、メンバーアカウントになるための招待を受け入れることはできません。アカウントを Macie 管理者とメンバーアカウントに同時に設定することはできません。メンバーアカウントになるには、まず現在の組織からすべてのメンバーアカウントを削除して、すべてのメンバーアカウントからアカウントの関連付けを解除する必要があります。
- Macie はリージョンでのサービスです。招待を受け入れると、アカウントと Macie 管理者アカウントとの関連付けはリージョン別になります。関連付けは、 AWS リージョン 招待の送信元と承諾元の にのみ存在します。
- Macie を複数のリージョンで使用する場合、アカウントの Macie 管理者アカウントは、それらのすべてのリージョンで同じである必要があります。ただし、Macie 管理者は各リージョンで個別に招待を送信する必要があり、お客様は各リージョンで個別に招待を受け入れる必要があります。
- Macie 管理者アカウントからいつでもお客様のアカウントの関連付けを解除できます。同様に、Macie 管理者はいつでも組織からアカウントを削除できます。どちらかが発生した場合 :
  - Macie は引き続きアカウントで有効になります。アカウントがスタンドアロン Macie アカウントになります。

- アカウントで機密データの自動検出が有効になっている場合、その検出は無効になります。これにより、アカウントの自動検出の実行中に Macie が生成して直接提供した既存の統計データ、インベントリデータ、その他の情報へのアクセスも無効になります。アカウントの自動検出を再度有効にできます。ただし、既存のデータへのアクセスは復元されません。代わりに、Macie はアカウントの自動検出を実行しながら、新しいデータを生成して維持します。

AWS Organizationsへの移行

Macie で招待ベースの組織を作成したら、 AWS Organizations 代わりに の使用に移行できます。移行を簡素化するために、 AWS Organizations内で組織の Macie 管理者アカウントとして、既存の招待ベースの管理者アカウントを指定することをお勧めします。

これを行うと、現在関連付けられているすべてのメンバーアカウントが引き続きメンバーになります。メンバーアカウントが の組織の一部である場合 AWS Organizations、アカウントの関連付けは Macie の Via への招待によって自動的に変更されます。 AWS Organizationsメンバーアカウントが AWS Organizations内で組織の一部ではない場合、アカウントの関連付けは引き続き 招待による になります。どちらの場合も、アカウントは引き続きメンバーアカウントとして Macie 管理者アカウントに関連付けられます。

メンバーアカウントは一度に 1 つの Macie 管理者アカウントのみと関連付けることができるため、この方法をお勧めします。で組織の Macie 管理者アカウントとして別のアカウントを指定した場合 AWS Organizations、指定された管理者は、招待によって別の Macie 管理者アカウントに既に関連付けられているアカウントを管理できません。各メンバーアカウントは、まず現在の招待ベースの管理者アカウントから関連付けを解除する必要があります。その場合にのみ、 AWS Organizations 組織の Macie 管理者はメンバーアカウントを組織に追加し、アカウントの Macie の管理を開始できます。

Macie を と統合 AWS Organizations し、Macie で組織を設定したら、必要に応じて組織の別の Macie 管理者アカウントを指定できます。招待を引き続き使用して、 AWS Organizations内で組織の一部ではないメンバーアカウントを関連付けて管理することもできます。

Macie を と統合する方法については AWS Organizations、「」を参照してくださいAWS Organizations を用いた Amazon Macie アカウントの管理。

Amazon Macie での招待ベースの組織の作成と管理

Amazon Macie で招待ベースの組織を作成するには、まず、組織の Macie 管理者アカウントにするアカウントを決定します。次に、そのアカウントを使用してメンバーアカウントを追加します。他のにメンバーシップの招待を送信し AWS アカウント、そのアカウントを現在の の Macie メンバーア

カウントとして組織に招待します AWS リージョン。複数のリージョンに組織を作成するには、他のアカウントが現在 Macie を使用している、または使用する予定の各リージョンからメンバーシップの招待を送信します。

アカウントが招待を受け入れると、そのアカウントは該当するリージョンの Macie 管理者アカウントに関連付けられた Macie メンバーアカウントになります。その後、Macie 管理者アカウントは、そのリージョン内のメンバーアカウントの特定の Macie 設定、データ、およびリソースにアクセスできます。

招待ベースの組織の Macie 管理者として、お客様は Amazon Simple Storage Service (Amazon S3) のインベントリデータとメンバーアカウントのポリシー結果を確認できます。また、機密データの自動検出を有効にし、機密データ検出ジョブを実行して、メンバーアカウントが所有する S3 バケット内の機密データを検出することもできます。実行できるタスクの詳細なリストについては、Amazon Macie 管理者とメンバーアカウントの関係について理解するを参照してください。

デフォルトでは、Macie は、組織全体の関連データとリソースを可視化します。ドリルダウンして、組織内の個々のアカウントのデータとリソースを確認することもできます。たとえば、概要ダッシュボードを使用して、組織の Amazon S3 セキュリティ体制を評価する場合は、アカウントごとにデータをフィルタリングできます。同様に、推定使用量のコストをモニタリングする場合は、個々のメンバーアカウントの推定コストの内訳にアクセスできます。

管理者およびメンバーアカウントに共通するタスクに加えて、組織のさまざまな管理タスクを一元的に実行できます。これらのタスクを実行する前に、Macie で招待ベースの組織を管理するために、考慮事項とレコメンデーションを確認することをお勧めします。

タスク

- Amazon Macie メンバーアカウントを招待ベースの組織に追加する
- 招待ベースの組織内のメンバーアカウントの Amazon メイシーを一時停止
- 招待ベースの組織からの Amazon Macie メンバーアカウントの削除
- 他のアカウントとの関連付けを削除する

Amazon Macie メンバーアカウントを招待ベースの組織に追加する

招待ベースの組織の Macie 管理者として、お客様は 2 つの主なステップを実行して、組織にメンバーアカウントを追加します。

1. Macie のアカウントインベントリにお客様のアカウントを追加します。これによりそのアカウントをお客様のアカウントに関連付けます。

2. メンバーシップの招待をアカウントに送信します。

アカウントがお客様の招待を受け入れると、それは組織のメンバーアカウントになります。

ステップ 1: アカウントを追加する

1 つ以上のアカウントをアカウントインベントリに追加するには、Amazon Macie コンソールまたは Amazon Macie API を使用することができます。

Console

Amazon Macie コンソールでは、一度に 1 つのアカウントを追加したり、カンマ区切り値 (CSV) ファイルをアップロードして複数のアカウントを同時に追加したりできます。コンソールを使用して 1 つ以上のアカウントを追加するには、次のステップに従います。

1 つのアカウントを追加するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、アカウントを追加するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウントページが開き、現在アカウントに関連付けられているアカウントのテーブルが表示されます。
4. アカウントの追加を選択します。
5. 「アカウントの詳細を入力」セクションで、「アカウントを追加」を選択します。次に、以下の操作を実行します。
   - アカウント ID には、追加 AWS アカウント する の 12 桁のアカウント ID を入力します。
   - E メールアドレス には、追加 AWS アカウント する の E メールアドレスを入力します。
6. 追加を選択します。
7. ページの最下部にある [Next] (次へ) を選択します。

Macie はアカウントインベントリにアカウントを追加します。アカウントのタイプは 招待により で、そのステータスは 作成済み です。アカウントを追加する追加のリージョンごとに、前述のステップを繰り返します。

複数のアカウントを追加するには

1. テキストエディタを使用して、次のように CSV ファイルを作成します。

a. ファイルの最初の行として、次のヘッダーを追加します: `Account ID,Email`

b. アカウントごとに、 AWS アカウント 追加する の 12 桁のアカウント ID とアカウントの E メールアドレスを含む新しい行を作成します。エントリをカンマで区切ります。例: `111111111111,janedoe@example.com`

E メールアドレスは、 AWS アカウントと関連付けられた E メールアドレスと一致する必要があります。

c. ファイルの内容が、次の例に示すようにフォーマットされていることを確認します。これには、3 つのアカウントの必須ヘッダーと情報が含まれています。

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

d. ファイルをコンピュータに保存します。

2. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
3. ページの右上隅にある AWS リージョン セレクターを使用して、アカウントを追加するリージョンを選択します。
4. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウントページが開き、現在アカウントに関連付けられているアカウントのテーブルが表示されます。
5. アカウントの追加を選択します。
6. 「アカウントの詳細を入力」セクションで、「リストをアップロード (CSV)」を選択します。
7. 参照を選択し、ステップ 1 で作成した CSV ファイルを選択します。
8. アカウントの追加を選択します。
9. ページの最下部にある [Next] (次へ) を選択します。

Macie はアカウントインベントリにそれらのアカウントを追加します。それらのタイプは 招待によりで、それらのステータスは 作成済みです。アカウントを追加する追加のリージョンごとにステップ 3～8 を繰り返します。

API

プログラムで 1 つ以上のアカウントを追加するには、Amazon Macie API の CreateMemberオペレーションを使用します。リクエストを送信するときは、サポートされているパラメータを使

用して、追加 AWS アカウント する各 の 12 桁のアカウント ID と E メールアドレスを指定します。また、リクエストが適用されるリージョンも指定します。追加のリージョンでアカウントを追加するには、追加のリージョンごとにリクエストを送信します。

AWS Command Line InterfaceAWS CLIを使用してアカウントを追加するには、create-member コマンドを実行します。region パラメータを使用して、アカウントを追加するリージョンを指定します。account パラメータを使用して、追加する各 AWS アカウント についてアカウント ID と E メールアドレスを指定します。例:

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"111111111111\",\"email\":\"janedoe@example.com\"}
```

ここで、*us-east-1* は、アカウントを追加するリージョン (米国東部 (バージニア北部) リージョン) であり、account パラメータは、追加するアカウントのアカウント ID (*111111111111*) とそのアカウントの E メールアドレス (*janedoe@example.com*) を指定します。

リクエストが成功すると、Macie は Created のステータスでアカウントのインベントリに各アカウントを追加し、お客様は次のような出力を受け取ります。

```
{
    "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"
}
```

ここで、arn は、お客様のアカウントと追加したアカウントとの関連付けのために作成されたリソースの Amazon リソースネーム (ARN) です。この例では、123456789012 は関連付けを作成したアカウントのアカウント IDで、111111111111 は追加されたアカウントのアカウント ID です。

ステップ 2: アカウントへメンバーシップの招待を送信する

アカウントインベントリにアカウントを追加した後、そのアカウントを招待して Macie メンバーアカウントとして組織に参加させることができます。これを行うには、アカウントにメンバーシップの招待を送信します。招待を送信すると、アカウントで Macie が有効化されている場合、受信者のアカウントの Amazon Macie コンソールに アカウント バッジと通知が表示されます。Macie はアカウントの AWS Health イベントも作成します。

Amazon Macie コンソールまたは API を使用して招待を送信するかどうかに応じて、Macie は、アカウントを追加したときに受信者のアカウントで指定した E メールアドレスにも招待を送信します。E

メールメッセージは、お客様が彼らのアカウントの Macie 管理者になりたいことを示し、それにはお客様の AWS アカウント のアカウント ID と受信者の AWS アカウントが含まれています。メッセージは、招待へのアクセス方法も説明しています。オプションで、メッセージにカスタムテキストを追加できます。

1 つ以上のアカウントにメンバーシップの招待を送信するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用してメンバーシップの招待を送信するには、次のステップに従います。

メンバーシップの招待を送信するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、招待を送信するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウントページが開き、現在アカウントに関連付けられているアカウントのテーブルが表示されます。
4. アカウントテーブルで、招待の送信先の各アカウントのチェックボックスをオンにします。

   > **Tip**
   >
   > 追加したアカウントや、招待をまだ送信していないアカウントをより簡単に識別するには、テーブルをフィルタリングします。これを行うには、テーブルの上にあるフィルターボックスにカーソルを置き、[ステータス] を選択します。次に [ステータス = 作成済み]を選択します。

5. アクションメニューで、招待を選択します。
6. (オプション) メッセージボックスに、招待を含む E メールメッセージに含めるカスタムテキストを入力します。テキストには最大 80 文字の英数字を含めることができます。
7. 招待を選択します。

追加の で招待を送信するには AWS リージョン、追加のリージョンごとに前述の手順を繰り返します。

招待を送信すると、受信者アカウントのステータスがアカウントのインベントリで E メール認証中に変わります。Macie がアカウントの E メールアドレスを確認できる場合、その後アカウントのステータスは 招待済みに変わります。Macie がアドレスを確認できない場合、アカウントのステータスは E メール認証に失敗しましたに変わります。このような場合は、アカウントの所有者と協力して、正しい E メールアドレスを取得してください。次に、アカウント間の関連付けを削除し、もう一度アカウントを追加し、再度招待を送信します。

受信者が招待を受け入れると、受信者のアカウントのステータスはアカウントのインベントリで Enabled (有効) に変わります 。受信者が招待を拒否すると、お客様のアカウントから受信者のアカウントの関連付けが解除され、お客様のアカウントのインベントリから削除されます。

API

プログラムで招待を送信するには、Amazon Macie API の CreateInvitationsオペレーションを使用します。リクエストを送信するときは、サポートされているパラメータを使用して、招待 AWS アカウント を送信する各 の 12 桁のアカウント ID を指定します。アカウント ID は、アカウントのインベントリ内のアカウントのアカウント ID と一致する必要があります。それ以外の場合は、エラーが発生します。招待の送信元のリージョンも指定します。追加のリージョンから招待を送信するには、追加のリージョンごとにリクエストを送信します。

リクエストでは、招待を E メールメッセージとして送信するかどうか、およびそのメッセージにカスタムテキストを含めるかどうかを指定することもできます。E メールメッセージを送信することを選択した場合、Macie は、アカウントのインベントリにアカウントを追加したときにアカウントで指定した E メールアドレスに招待を送信します。招待を E メールメッセージとして送信するには、disableEmailNotification パラメータを省略するか、パラメータの値を false に設定します。。(デフォルト値はfalseです。) メッセージにカスタムテキストを追加するには、message パラメータを使用して、追加するテキストを指定します。テキストには最大 80 文字の英数字を含めることができます。

を使用して招待を送信するには AWS CLI、create-invitations コマンドを実行します。region パラメータを使用して、招待の送信元のリージョンを指定します。account-ids パラメータを使用して、招待の送信先の各 AWS アカウント のアカウント ID を指定します。例:

```
C:\> aws macie2 create-invitations --region us-east-1 --account-
ids=[\"111111111111\",\"222222222222\",\"333333333333\"]
```

ここで、*us-east-1* は招待の送信元のリージョン (米国東部 (バージニア北部) リージョン) で、account-ids パラメータは、招待の送信先の 3 つのアカウントのアカウント ID を指定します。招待を E メールメッセージとして送信する場合も、no-disable-email-

notification パラメータも含め、オプションで message パラメータを含めて、メッセージに追加するカスタムテキストを指定します。

招待を送信すると、各受信者アカウントのステータスが EmailVerificationInProgress に変わります。Macie がアカウントの E メールアドレスを確認できる場合、その後アカウントのステータスは Invited に変わります。Macie がアドレスを確認できない場合、アカウントのステータスは EmailVerificationFailed に変わります。このような場合は、アカウントの所有者と協力して正しいアドレスを取得してください。次に、アカウント間の関連付けを削除し、もう一度アカウントを追加し、再度招待を送信します。

受信者が招待を受け入れると、受信者のアカウントのステータスはアカウントのインベントリで Enabled に変わります 。受信者が招待を拒否すると、お客様のアカウントから受信者のアカウントの関連付けが解除され、お客様のアカウントのインベントリから削除されます。

招待ベースの組織内のメンバーアカウントの Amazon メイシーを一時停止

組織の Macie 管理者として、組織内の個々のメンバーアカウント AWS リージョン について、特定の で Macie を停止できます。ただし、停止した後、メンバーアカウントで Macie を再度有効化できないことに注意してください。その後、アカウントのユーザーのみがアカウントの Macie を再度有効化できます。

メンバーアカウントの メイシーを一時停止と、次のようになります。

- Macie は、リージョン内のアカウントの Amazon S3 データに関するメタデータへのアクセスを失い、提供を停止します。
- Macie は、リージョン内のアカウントのすべてのアクティビティの実行を停止します。これには、セキュリティとアクセスコントロールのための S3 バケットのモニタリング、機密データの自動検出、および現在進行中の機密データ検出ジョブの実行などが含まれます。
- Macie は、リージョン内のアカウントによって作成された機密データ検出ジョブをすべてキャンセルします。ジョブがキャンセルされた後は、ジョブを再開したり再起動したりすることはできません。メンバーアカウントが所有するデータを分析するためのジョブを作成した場合、Macie はそれらのジョブをキャンセルしません。代わりに、ジョブはアカウントが所有するリソースをスキップします。

アカウントが停止されている間、Macie は該当するリージョン内のアカウントの Macie セッション識別子、設定、およびリソースを保持します。たとえば、アカウントの調査結果はそのまま残り、最

大 90 日間は影響を受けません。そのリージョン内のアカウントで Macie が停止されている間、アカウントは該当するリージョン内での Macie の使用に対して請求されません。

招待ベースの組織内のメンバーアカウントの メイシーを一時停止には

招待ベースの組織内のメンバーアカウントの メイシーを一時停止には、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用してメンバーアカウントの メイシーを一時停止には、次のステップに従います。

メンバーアカウントの メイシーを一時停止には

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、メンバーアカウントの Macie を停止するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウントページが開き、現在アカウントに関連付けられているアカウントのテーブルが表示されます。
4. アカウント テーブルで、停止するアカウントのチェックボックスをオンにします。
5. アクション (アクション)メニューで、メイシーを一時停止 を選択します。
6. 選択したアカウントの メイシーを一時停止ことを確認します。

停止を確認すると、アカウントのステータスがインベントリで 一時停止 (停止) に変わります。

アカウントのメイシーを一時停止したい追加リージョンごとに、前述の手順を繰り返します。

API

メンバーアカウントの Macie をプログラムで停止するには、Amazon Macie API の UpdateMemberSessionオペレーションを使用します。リクエストを送信するときは、 `id`パラメータを使用して、Macie を停止 AWS アカウント する の 12 桁のアカウント ID を指定します。`status` パラメータでは、Macie アカウントの新しいステータスとして `PAUSED` を指定します。また、リクエストが適用されるリージョンも指定します。追加のリージョンでメイシーを一時停止には、追加のリージョンごとにリクエストを送信します。

メンバーアカウントのアカウント ID を取得するには、Amazon Macie API の ListMembersオペレーションを使用できます。これを実行する場合は、リクエストに `onlyAssociated` パラメータを含めることで結果をフィルタリングすることを検討してください。このパラメータの値を

`true` に設定した場合、Macie は現在管理者アカウントのメンバーアカウントであるアカウントのみの詳細を提供する `members` 配列を返します。

を使用してメンバーアカウントの Macie を停止するには AWS CLI、 update-member-session コマンドを実行します。`region` パラメータを使用して、メイシーを一時停止リージョンを指定し、`id` パラメータを使用して、メイシーを一時停止アカウントのアカウント ID を指定します。`status` パラメータでは、PAUSED を指定します。例:

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

ここで、*us-east-1* は メイシーを一時停止リージョン (米国東部 (バージニア北部) リージョン) であり、*123456789012* は メイシーを一時停止アカウントのアカウント ID であり、PAUSED はそのアカウントの Macie の新しいステータスです。

リクエストが成功すると、Macie は空のレスポンスを返し、指定されたアカウントのステータスはアカウントのインベントリの `Paused` に変わります。

招待ベースの組織からの Amazon Macie メンバーアカウントの削除

Macie 管理者として、お客様は組織からメンバーアカウントを削除できます。これを行うには、Macie 管理者アカウントからそのアカウントの関連付けを解除します。

メンバーアカウントを削除しても、Macie はそのアカウントに対して引き続き有効化され、アカウントは引き続きアカウントのインベントリに表示されます。ただし、そのアカウントがスタンドアロンの Macie アカウントになります。Macie は、お客様がアカウントを削除しても、アカウントの所有者に通知しません。したがって、アカウント所有者に連絡して、アカウントの設定とリソースの管理を開始してもらうことを検討してください。

メンバーアカウントを削除すると、アカウントのすべての Macie 設定、リソース、およびデータへのアクセスが失われます。これには、そのアカウントが所有するS3バケットのポリシー所見とメタデータが含まれます。さらに、アカウントが所有するS3バケット内の機密データを発見するためにMacieを使用することはできなくなりました。このために機密データ検出ジョブを作成済みの場合、ジョブはアカウントが所有するバケットをスキップします。アカウントの機密データ自動検出を有効にした場合、ユーザーとアカウントの両方が、アカウントの自動検出の実行中に Macie が生成して直接提供した統計データ、インベントリデータ、およびその他の情報にアクセスできなくなります。

メンバーアカウントを削除した後、アカウントに新しい招待を送信して、組織にアカウントを再度追加できます。アカウントが新しい招待を受け入れ、30 日以内にアカウントの機密データ自動検出を

有効にした場合、アカウントの自動検出の実行中に Macie が以前に生成して直接提供したデータや情報へのアクセスも回復します。

メンバーアカウントを削除し、再度追加する予定がない場合は、アカウントインベントリから完全に削除できます。この方法の詳細は、他のアカウントとの関連付けを削除するを参照してください。

招待ベースの組織からメンバーアカウントを削除するには

組織からメンバーアカウントを削除するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用してメンバーアカウントを削除するには、次のステップに従います。

メンバーアカウントを削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、メンバーアカウントを削除するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウントページが開き、現在アカウントに関連付けられているアカウントのテーブルが表示されます。
4. アカウント テーブルで、削除するアカウントのチェックボックスをオンにします。
5. アクション メニューで、Disassociate account (アカウントの関連付けを解除する) を選択します。
6. 選択されたアカウントをメンバーアカウントとして削除することを確認します。

選択を確認すると、アカウントのステータスが、アカウントのインベントリで Removed (disassociated) (削除 (関連付け解除)) に変わります。

メンバーアカウントを削除する追加のリージョンごとに、前述のステップを繰り返します。

API

プログラムでメンバーアカウントを削除するには、Amazon Macie API の DisassociateMemberオペレーションを使用します。リクエストを送信するときは、 `id`パラメータを使用して、削除するメンバーアカウントの 12 桁の AWS アカウント ID を指定します。また、リクエストが適用され

るリージョンも指定します。追加のリージョン内のアカウントを削除するには、追加のリージョンごとにリクエストを送信します。

削除するアカウントのアカウント ID を取得するには、Amazon Macie API の ListMembersオペレーションを使用できます。これを実行する場合は、リクエストに `onlyAssociated` パラメータを含めることで結果をフィルタリングすることを検討してください。このパラメータの値を `true` に設定した場合、Macie は現在お客様のアカウントのメンバーアカウントであるアカウントのみの詳細を提供する `members` 配列を返します。

を使用してメンバーアカウントを削除するには AWS CLI、disassociate-member コマンドを実行します。`region` パラメータを使用して、アカウントを削除するリージョンを指定します。`id` パラメータを使用して、削除するアカウントのアカウント ID を指定します。例:

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

ここで、*`us-east-1`* は、アカウントを削除するリージョン (米国東部 (バージニア北部) リージョン) であり、*`123456789012`* は削除するアカウントのアカウント ID です。

リクエストが成功すると、Macie は空のレスポンスを返し、指定されたアカウントのステータスはアカウントのインベントリの `Removed` に変わります。

他のアカウントとの関連付けを削除する

アカウントのインベントリにアカウントを追加した後、お客様のアカウントと他のアカウント間の関連付けを削除できます。この操作は、インベント内の任意のアカウントで実行できますが、以下を除きます。

- AWS Organizations内の組織の一部であるアカウント このタイプの関連付けは、Macie AWS Organizations ではなく によって制御されます。
- 組織に参加するための Macie メンバーシップの招待を受け入れたメンバーアカウント。このような場合は、関連付けを削除する前にメンバーアカウントを削除する必要があります。

関連付けを削除すると、Macie はアカウントのインベントリからアカウントを削除します。後で関連付けを復元する場合は、完全に新しいアカウントであるかのようにアカウントを再度追加する必要があります。

別のアカウントとの関連付けを削除するには

お客様のアカウントと他のアカウント間の関連付けを削除するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用して別のアカウントとの関連付けを削除するには、次のステップに従います。

関連付けを削除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、関連付けを削除するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウントページが開き、現在アカウントに関連付けられているアカウントのテーブルが表示されます。
4. アカウント テーブルで、関連付けを削除するアカウントのチェックボックスをオンにします。
5. Actions メニューで、Delete を選択します。
6. 選択した関連付けを削除することを確認します。

関連付けを削除する追加のリージョンごとに、前述のステップを繰り返します。

API

別のアカウントとの関連付けをプログラムで削除するには、Amazon Macie API の DeleteMemberオペレーションを使用します。リクエストを送信するときは、 `id`パラメータを使用して、関連付け AWS アカウント を削除する の 12 桁のアカウント ID を指定します。また、リクエストが適用されるリージョンも指定します。追加のリージョンで関連付けを削除するには、追加のリージョンごとにリクエストを送信します。

アカウントのアカウント ID を取得するには、Amazon Macie API の ListMembersオペレーションを使用できます。これを行う場合は、リクエストに `onlyAssociated` パラメータを含め、パラメータの値を `false` に設定します。オペレーションが成功すると、Macie は、お客様のアカウントに関連付けられているすべてのアカウント (現在メンバーアカウントではないアカウントを含む) の詳細を提供する `members` 配列を返します。

を使用して別のアカウントとの関連付けを削除するには AWS CLI、delete-member コマンドを実行します。`region` パラメータを使用して、関連付けを削除するリージョンを指定し、`id` パラメータを使用して、そのアカウントのアカウント ID を指定します。例:

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

ここで、*us-east-1* は、他のアカウントとの関連付けを削除するリージョン (米国東部 (バージニア北部) リージョン) であり、*123456789012* はそのアカウントのアカウント ID です。

リクエストが成功すると、Macie は空の応答を返し、お客様のアカウントと他のアカウント間の関連付けは削除されます。以前に関連付けられたアカウントがアカウントのインベントリから削除されます。

招待ベースの組織の Amazon Macie アカウントの確認

組織内のアカウントを管理しやすくするために、Amazon Macie は Macie AWS リージョン を使用する各 で Macie アカウントに関連付けられているアカウントのインベントリを提供します。組織の Macie 管理者として、このインベントリを使用して、組織のアカウント統計と詳細を確認できます。これを使用して、メンバーアカウントの特定の管理タスクを実行し、アカウントと他のアカウントとの関係のステータスを管理することもできます。

招待ベースの組織のアカウントを確認するには

組織内のアカウントを確認するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用して組織のアカウントを確認するには、次のステップに従います。

組織のアカウントを確認するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、組織のアカウントを確認するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。

アカウントページが開き、現在の AWS リージョン内で Macie アカウントに関連付けられている集約された統計とアカウントのテーブルが表示されます。

アカウントページの先頭に、次の集約された統計が表示されます。

経由 AWS Organizations

の組織の Macie 管理者である場合 AWS Organizations、Active は、 を通じてアカウントに関連付けられ、現在組織内の Macie メンバーアカウント AWS Organizations であるアカウントの総数を報告します。Macie はこれらのアカウントに対して有効化されており、お客様はアカウントの Macie 管理者です。

すべての は、現在 Macie メンバーアカウントではないアカウントを含め AWS Organizations、 を通じてアカウントに関連付けられているアカウントの総数を報告します。

招待により

Active (アクティブ) により、招待ベースの組織内で現在 Macie メンバーアカウントであるアカウントの総数が報告されます。Macie はこれらのアカウントに対して有効化されており、お客様からメンバーシップへの招待を受け入れたため、お客様はアカウントの Macie 管理者です。

すべて により、お客様からの招待に応答していないアカウントを含む、Macie の招待によってお客様のアカウントに関連付けられているアカウントの総数が報告されます。

アクティブ/すべて

アクティブ は、 を通じて、 AWS Organizations または招待によって、現在 Macie メンバーアカウントであるアカウントの総数を報告します。Macie はこれらのアカウントに対して有効化されており、お客様はアカウントの Macie 管理者です。

すべての は、 を通じて、 AWS Organizations または招待によって、アカウントに関連付けられているアカウントの総数を報告します。これには、お客様からの Macie メンバーシップ招待を受け入れていないアカウントも含まれます。また、 を通じてアカウントに関連付けられ AWS Organizations 、現在 Macie メンバーアカウントではないアカウントも含まれます。

テーブルには、現在のリージョン内の各アカウントの詳細が表示されます。テーブルには、Macie の招待または によって Macie アカウントに関連付けられているすべてのアカウントが含まれます AWS Organizations。

アカウント ID

AWS アカウントのアカウント ID と E メールアドレス。

名前

AWS アカウントのアカウント名。この値は通常、招待によってお客様のアカウントに関連付けられているアカウントの場合、N/A (該当なし) になります。

タイプ

Macie の招待によって、または AWS Organizationsを通じてそのアカウントがお客様のアカウントに関連付けられる方法。

ステータス

お客様のアカウントとそのアカウントの関係のステータス。招待ベースの組織のアカウントの場合 (タイプ は (招待により) です)、指定できる値は以下のとおりです。

- アカウントが停止 — AWS アカウント が停止されています。
- 作成済み (招待)— アカウントを追加しましたが、メンバーシップの招待をそれに送信していません。
- E メール認証に失敗しました — アカウントにメンバーシップの招待を送信しようとしましたが、指定された E メールアドレスがアカウントに対して有効ではありません。
- E メール認証中 — アカウントにメンバーシップの招待を送信済みで、Macie がリクエストを処理しています。
- 有効 — アカウントはメンバーアカウントです。Macie はアカウントに対して有効化されており、お客様はそのアカウントの Macie 管理者です。
- 招待済み — アカウントにメンバーシップの招待を送信しましたが、アカウントが招待に応答していません。
- メンバー退会済み— アカウントは以前メンバーアカウントでした。ただし、アカウントとの関連付けを解除して、アカウントが組織から脱退しました。
- 一時停止 (停止) — アカウントはメンバーアカウントですが、現在 Macie はアカウントを停止しています。
- リージョンが無効— 現在のリージョンは AWS アカウントで無効です。
- 削除 (関連付け解除) — アカウントは以前メンバーアカウントでした。ただし、アカウントから関連付けを解除して、メンバーアカウントとしてそれを削除しました。

最終ステータス更新

お客様または関連するアカウントが、お客様のアカウント間の関係に影響を与えたアクションを最後に実行したとき。

機密データの自動検出

アカウントで機密データの自動検出が現在有効または無効になっているかどうか。

特定のフィールドでテーブルをソートするには、フィールドの列見出しを選択します。ソート順序を変更するには、列見出しを再度選択します。テーブルをフィルタリングするには、フィルターボックスにカーソルを置き、フィールドのフィルター条件を追加します。結果をさらに絞り込むには、追加のフィールドでフィルター条件を追加します。

API

組織のアカウントをプログラムで確認するには、Amazon Macie API の ListMembersオペレーションを使用して、リクエストが適用されるリージョンを指定します。追加のリージョン内の詳細を確認するには、追加のリージョンごとにリクエストを送信します。

リクエストを送信するときは、onlyAssociated パラメータを使用して、レスポンスに含めるアカウントを指定します。デフォルトでは、Macie は指定されたリージョンのメンバーアカウントであるアカウントに関する詳細のみを招待または を通じて返します AWS Organizations。メンバーアカウントではないアカウントを含む、すべてのアカウントの詳細を取得するには、リクエストに onlyAssociated パラメータを含め、パラメータの値を false に設定します。

AWS Command Line InterfaceAWS CLIを使用して組織のアカウントを確認するには、list-members コマンドを実行します。only-associated パラメータでは、関連するすべてのアカウントを含めるか、メンバーアカウントのみを含めるかを指定します。メンバーアカウントのみを含めるには、このパラメータを省略するか、パラメータの値を true に設定します。すべてのアカウントを含めるには、この値を false に設定します。例:

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

ここで、*us-east-1* は、リクエストが適用されるリージョン (米国東部 (バージニア北部) リージョン) です。

リクエストが成功すると、Macie は members 配列を返します 配列には、リクエストで指定された基準を満たす各アカウントの member オブジェクトが含まれます。そのオブジェクトでは、relationshipStatus フィールドは、指定されたリージョン内のお客様のアカウントと他方のアカウント間の関連付けの現在のステータスを示します。招待ベースの組織のアカウントの場合、指定できる値は以下のとおりです。

- AccountSuspended – AWS アカウント は中断されます。
- Created — アカウントを追加しましたが、メンバーシップの招待をそれに送信していません。
- EmailVerificationFailed — アカウントにメンバーシップの招待を送信しようとしましたが、指定された E メールアドレスがアカウントに対して有効ではありません。

- `EmailVerificationInProgress` — アカウントにメンバーシップの招待を送信済みで、Macie がリクエストを処理しています。
- `Enabled` — アカウントはメンバーアカウントです。Macie はアカウントに対して有効化されており、お客様はそのアカウントの Macie 管理者です。
- `Invited` — アカウントにメンバーシップの招待を送信しましたが、アカウントが招待に応答していません。
- `Paused` — アカウントはメンバーアカウントですが、Macie は現在アカウントが停止 (一時停止) されています。
- `RegionDisabled` — 現在のリージョンは AWS アカウントで無効です。
- `Removed` — アカウントは以前メンバーアカウントでした。ただし、アカウントから関連付けを解除して、メンバーアカウントとしてそれを削除しました。
- `Resigned` — アカウントは以前メンバーアカウントでした。ただし、アカウントとの関連付けを解除して、アカウントが組織から脱退しました。

`member` オブジェクト内の他のフィールドの詳細については、Amazon Macie API リファレンスのメンバーを参照してください。

招待ベースの組織の別の Amazon Macie 管理者アカウントの指定

招待ベースの組織を作成して確立した後、その組織の Amazon Macie 管理者アカウントを変更できます。これを行うには、組織の管理者とメンバーは次のステップに従う必要があります。

1. 現在の Macie 管理者は、必要に応じて、組織のアクティブなメンバーアカウントの現在のインベントリをエクスポートします。これにより、引き続き組織の一部となるメンバーアカウントを識別できるようにして、移行が簡素化されます。
2. 現在の Macie 管理者は、現在の組織からすべてのメンバーアカウントを削除します。これにより、現在の管理者アカウントからアカウントの関連付けが解除されます。Macie は引き続きアカウントに対して有効になっていますが、アカウントはスタンドアロン Macie アカウントになります。

> **Note**
>
> 現在の Macie 管理者がメンバーアカウントを削除すると、Macie はアカウントの機密データ自動検出を自動的に無効にします。これにより、アカウントの自動検出の実行中に Macie が生成して直接提供した統計データ、インベントリデータ、その他の情報へのアク

セスも無効になります。新しい組織への移行が完了すると、新しい Macie 管理者はこのデータにアクセスできなくなります。

3. 新しい Macie 管理者は、新しい組織に前のメンバーアカウントを追加します。これにより、アカウントが新しい管理者アカウントに関連付けられます。
4. 各メンバーアカウントは、新しい組織に参加するための招待を受け入れます。アカウントが招待を受け入れると、そのアカウントは新しい組織のアクティブなメンバーアカウントになります。新しい Macie 管理者は、アカウントの Macie 設定、データ、およびリソースにアクセスできます。アカウントで機密データの自動検出が以前に有効になっていた場合、アカウントの自動検出の実行中に Macie が以前に生成して直接提供したデータは含まれません。代わりに、新しい Macie 管理者がアカウントの自動検出を有効にしている場合、Macie はアカウントの新しいデータを生成して維持します。

組織が複数の で Macie を使用している場合は AWS リージョン、それらの各リージョンで前述のステップを実行します。

アクティブなメンバーアカウントの現在のインベントリをエクスポートするには、現在の Macie 管理者は Amazon Macie コンソールまたは Amazon Macie API を使用できます。コンソールを使用すると、現在の管理者は、データをカンマ区切り値 (CSV) ファイルにエクスポートできます。その後、新しい管理者は、コンソールを使用して CSV ファイルをアップロードし、すべてのアカウントを (一括で) 新しい組織に追加できます。

コンソールを使用してメンバーアカウントのデータを エクスポートするには

1. 現在の Macie 管理者アカウント AWS Management Console を使用して にサインインします。
2. ページの右上隅にある AWS リージョン セレクターを使用して、データを エクスポートするリージョンを選択します。
3. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
4. ナビゲーションペインで、[Accounts] (アカウント) を選択します。アカウントページが開き、現在の Macie 管理者アカウントに関連付けられているアカウントのテーブルが表示されます。
5. (オプション) アカウント テーブルをフィルタリングし、組織内で現在アクティブな Macie メンバーアカウントであるアカウントのみを表示するには、フィルターバーを使用して次のフィルター条件を追加します。
   - タイプ は 招待 です。
   - ステータス は 有効 です。

6. アカウント テーブルで、エクスポートされたデータに含める各メンバーアカウントのチェックボックスをオンにします。
7. Export CSV (CSV のエクスポート) を選択します。
8. ファイルの場所とファイル名を指定します。

Amazon Macie API を使用すると、現在の Macie 管理者は JSON 形式でデータを取得できます。その後、新しい Macie 管理者は、そのデータを使用して、新しい組織に追加および招待するアカウントのアカウント ID と E メールアドレスのリストを生成できます。JSON 形式でデータを取得するには、Amazon Macie API の ListMembersオペレーションを使用します。オペレーションが成功すると、Macie は、管理者のアカウントに関連付けられているすべてのアカウントの詳細を提供する `members` 配列を返します。アカウントが現在の招待ベースの組織内のアクティブな Macie メンバーアカウントである場合、アカウントの `relationshipStatus` プロパティの値は `Enabled` であり、`invitedAt` プロパティは日付と時刻を指定します。

Amazon Macie で招待ベースの組織内のメンバーシップを管理する

Amazon Macie で組織への参加を招待されている場合は、必要に応じて招待を受け入れまたは拒否できます。Macie では、組織は、関連するアカウントのグループとして集中管理されるアカウントのセットです。組織は、指定された 1 つの Macie 管理者アカウントと 1 つ以上の関連付けられたメンバーアカウントで設定されています。

招待を受け入れると、お客様のアカウントは組織のメンバーアカウントになります。受け入れると、招待を送信したアカウントがお客様のアカウントの Macie 管理者アカウントになります。お客様のアカウントを他のアカウントに関連付けて、アカウント間の管理者とメンバーの関係を有効化します。その後、Macie 管理者アカウントは、該当する AWS リージョン内のアカウントの特定の Macie 設定、データ、およびリソースにアクセスできます。詳細については、「Amazon Macie 管理者とメンバーアカウントの関係について理解する」を参照してください。

招待を拒否しても、Macie アカウントの現在のステータスと設定は変更されません。

トピック

- 組織のメンバーシップの招待への応答
- Amazon Macie 管理者アカウントから関連付けを解除する

組織のメンバーシップの招待への応答

組織に参加するための招待を受け取ると、Amazon Macie はいくつかの方法でお客様に通知します。デフォルトでは、Macie は招待を E メールメッセージとして送信します。Macie は の AWS Health イベントも作成します AWS アカウント。招待の送信 AWS リージョン 元の で既に Macie を使用している場合、Macie は Macie コンソールにアカウントバッジと通知も表示します。

招待を受け取った後、必要に応じて招待を受け入れまたは拒否できます。応答する前に、次の点に注意してください。

- お客様が組織のメンバーになることができるのは、一度に 1 つのみです。複数の招待を受け取った場合は、1 つのみ受け入れることができます。あるいは、お客様が既に組織のメンバーである場合は、別の組織に参加する前に、現在の Macie 管理者アカウントからお客様のアカウントの関連付けを解除する必要があります。
- Macie を複数のリージョンで使用する場合、お客様のアカウントは、それらのすべてのリージョンで同じ Macie 管理者アカウントを持っている必要があります。Macie 管理者は各リージョンから個別に招待を送信する必要があり、お客様は各リージョンで個別に招待を受け入れる必要があります。
- 招待を受け入れまたは拒否するには、招待の送信元のリージョン内の Macie を有効化する必要があります。招待の拒否はオプションです。招待を拒否するように Macie を有効化した場合、招待を拒否した後に、リージョンで Macie を無効にできます。これにより、リージョンでの Macie の使用で不必要な料金が発生しないようにできます。
- アカウントで機密データの自動検出が有効になっていて招待を承諾すると、Macie がアカウントの自動検出の実行中に生成して直接提供した統計データ、インベントリデータ、その他の情報にアクセスできなくなります。招待を承諾すると、Macie 管理者はアカウントの自動検出を有効にできます。ただし、既存のデータへのアクセスは復元されません。代わりに、Macie はアカウントの自動検出を実行しながら、新しいデータを生成して維持します。

その他の考慮事項については、メンバーシップの招待への応答と管理を参照してください。

組織のメンバーシップの招待に応答するには

メンバーシップの招待に応答するには、Amazon Macie コンソールまたは Amazon Macie API を使用できます。

Console

Amazon Macie コンソールを使用してメンバーシップの招待に応答するには、次のステップに従います。

メンバーシップの招待に応答するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、招待を受け取ったリージョンを選択します。
3. リージョンで Macie を有効化していない場合は、開始方法 を選択し、Macie を有効化する を選択します。招待を受け入れまたは拒否する前に、Macie を有効化する必要があります。
4. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
5. 管理者アカウントで、次のいずれかを実行します。
   - 招待を受け入れるには、招待の横にある 受け入れる( ) をオンにします。次に、以前に別の招待を受け入れたかどうかに応じて、招待を受け入れるまたは 更新を選択します。
   - 招待を拒否するには、招待の横にある 招待を拒否するを選択し、次に招待を拒否することを確認します。

追加のリージョンで招待を受け取って返信する場合は、追加のリージョンごとに前述のステップを繰り返します。

API

プログラムで招待に応答するには、招待を受け入れるか拒否するかに応じて、Amazon Macie API の AcceptInvitationまたは DeclineInvitationsオペレーションを使用します。リクエストを送信するときは、招待の送信元のリージョンを必ず指定してください。追加のリージョンで招待に応答するには、追加のリージョンごとにリクエストを送信します。

`AcceptInvitation` リクエストでは、 `administratorAccountId`パラメータを使用して、招待 AWS アカウント を送信した の 12 桁のアカウント ID を指定します。`invitationId` パラメータを使用して、受け入れる招待の一意の ID を指定します。

`DeclineInvitations` リクエストでは、 `accountIds`パラメータを使用して、拒否の招待 AWS アカウント を送信した の 12 桁のアカウント ID を指定します。

IDs、Amazon Macie API の ListInvitationsオペレーションを使用できます。オペレーションが成功すると、Macie は、各招待を送信したアカウントのアカウント ID および各招待の一意の ID を含む、受け取った招待の詳細を提供する `invitations` 配列を返します。招待の `relationshipStatus` プロパティの値が `Invited` である場合、お客様は招待にまだ応答していません。

AWS Command Line InterfaceAWS CLIを使用して招待に応答するには、招待を受け入れるか拒否するかどうかに応じて、accept-invitation または decline-invitations コマンドを実行します。`region` パラメータを使用して、招待の送信元のリージョンを指定します。例:

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-
id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

ここで、*us-east-1* は、招待の送信元のリージョン (米国東部 (バージニア北部) リージョン) であり、*123456789012* は招待を送信したアカウントのアカウント ID で、*d8bdad0e203fd1242e0a4721bexample* は受け入れる招待の一意の ID です。

招待を受け入れるためのリクエストが成功すると、Macie は空の応答を返します。招待を拒否するためのリクエストが成功すると、Macie は空の `unprocessedAccounts` 配列を返します。

招待を拒否した後も、招待は Macie アカウントのリソースとして保持されます。オプションで、DeleteInvitationsオペレーション、または の場合は delete AWS CLI-invitations コマンドを使用して削除できます。

Amazon Macie 管理者アカウントから関連付けを解除する

Amazon Macie で組織に参加するための招待を受け入れても、その後に既存の Macie 管理者アカウントからお客様のアカウントの関連付けを解除することで、その組織から脱退できます。お客様のアカウントが AWS Organizations 組織のメンバーアカウントである場合は、これを行えないことに注意してください。 AWS Organizations 組織から辞任するには、Macie 管理者と協力して Macie メンバーアカウントとしてアカウントを削除します。

Macie 管理者アカウントからアカウントの関連付けを解除すると、Macie 管理者は Macie アカウントのすべての設定、データ、およびリソースへのアクセスを失います。これには、所有している Amazon S3 データのメタデータとポリシー結果が含まれます。これはまた、管理者がお客様の Amazon S3 データを、機密データ自動検出ジョブの実行や機密データ検出ジョブの実行で、分析できなくなることも意味します。

アカウントの関連付けを解除すると、Macie は該当するリージョンで引き続きアカウントに対して有効化されます。ただし、お客様のアカウントはリージョン内でスタンドアロンの Macie アカウントになります。アカウントのステータスは、管理者のアカウントインベントリで 辞職したメンバー に変わります。

Macie 管理者アカウントから関連付けを解除するには

現在の Macie 管理者アカウントからアカウントの関連付けを解除するには、Amazon Macie コンソールまたは Amazon Macie API を使用します。

Console

Amazon Macie コンソールを使用して、Macie 管理者アカウントからアカウントの関連付けを解除するには、次のステップに従います。

管理者アカウントから関連付けを解除するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、アカウントの管理者アカウントとの関連付けを解除するリージョンを選択します。
3. ナビゲーションペインで、[Accounts] (アカウント) を選択します。
4. 管理者アカウントの下で、招待の横にある 受け入れる( ) をオフにし、次に 更新を選択します。

そのアカウントは、引き続き アカウント ページに表示されます。組織に再参加する場合は、このページを使用して元の招待を再度受け入れることができます。または、招待を拒否、削除もできます。これにより、お客様のアカウントと他のアカウント間の関連付けも削除されます。これを実行するには、[招待を拒否] を選択します。

追加のリージョンで Macie 管理者アカウントからアカウントの関連付けを解除する場合は、追加のリージョンごとに前述のステップを繰り返します。

API

プログラムで Macie 管理者アカウントからアカウントの関連付けを解除するには、Amazon Macie API の DisassociateFromAdministratorAccountオペレーションを使用します。リクエストを送信するときは、リクエストが適用されるリージョンを必ず指定してください。追加のリージョンでアカウントから関連付けを解除するには、追加のリージョンごとにリクエストを送信します。

を使用して Macie 管理者アカウントからアカウントの関連付けを解除するには AWS CLI、disassociate-from-administrator-account コマンドを実行します。`region` パラメータを使用して、アカウントから関連付けを解除するリージョンを指定します。

リクエストが成功すると、Macie は空のレスポンスを返します。

アカウントから関連付けを解除した後、元の招待は、削除しない限り Macie アカウントのリソースとして保持されます。組織に再参加する場合は、このリソースを使用して元の招待を再度受け入れることができます。または、 DeleteInvitationsオペレーション、または の場合は delete-invitations コマンドを使用して AWS CLI招待を削除することもできます。招待を削除すると、お客様のアカウントと他のアカウント間の関連付けも削除されます。

Amazon Macie のセキュリティ

AWS では、クラウドセキュリティを最優先事項としています。AWS のユーザーは、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを利用できます。

セキュリティは、AWS とユーザーの間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — AWS は、AWS クラウド で AWS のサービス を実行するインフラストラクチャを保護する責任を負います。また AWS は、お客様が使用するサービスを安全に提供します。AWS コンプライアンスプログラム の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。Amazon Macie に適用するコンプライアンスプログラムの詳細については、コンプライアンスプログラムによる対象範囲の AWS サービス を参照してください。
- クラウド内のセキュリティ — お客様の責任は、使用する AWS のサービス に応じて異なります。またお客様は、データの機密性、企業要件、適用法令と規制などのその他の要因に対しても責任を担います。

このドキュメントは、Macie を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Macie を設定する方法を示します。また、Macie リソースのモニタリングや保護に役立つ、他の AWS のサービス 使用方法についても説明します。

トピック

Amazon Macie でのデータ保護

AWS 責任共有モデル は、Amazon Macie のデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべてを実行するグローバルインフラストラクチャを保護するがあります。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データを保護するため、AWS アカウント の認証情報を保護し、AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみを各ユーザーに付与できます。また、次の方法でデータを保護することをおすすめします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須です。TLS 1.3 が推奨されます。
- AWS CloudTrail で API とユーザーアクティビティロギングをセットアップします。
- AWS のサービス内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API により AWS にアクセスするときに FIPS 140-2 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの機密情報やセンシティブ情報は、タグや Name フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これには、コンソール、API、AWS CLIまたはAWSSDKを使用してMacieまたは他のAWS のサービス作業を行う場合も含まれます。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

保管中の暗号化

Amazon Macie は、AWS 暗号化ソリューションを使用して、保管中のデータを安全に保存します。Macie は、AWS Key Management Service からの AWS マネージドキー を使用してAWS KMS、結果などのデータを暗号化します。

Macie を無効にすると、機密データ検出ジョブ、カスタムデータ識別子、結果など、お客様のために保存または維持されるすべてのリソースが完全に削除されます。

転送中の暗号化

Macie は AWS のサービス 間の転送中のすべてのデータを暗号化します。

Amazon Macie は Amazon S3 からのデータを分析し、機密データの検出結果を S3 バケットにエクスポートします。Macie が S3 オブジェクトから必要な情報を取得すると、それらは破棄されます。

Macie は、AWS PrivateLink によって駆動する VPC エンドポイントを使用して Amazon S3 にアクセスします。したがって、Macie と Amazon S3 の間のトラフィックは Amazon ネットワーク上に留まり、パブリックインターネットを経由しません。詳細については、AWS PrivateLinkを参照してください。

Amazon Macie の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、Macie リソースを使用するための認証 (サインイン) および許可 (アクセス許可を持たせる) を行うことができる人を制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、Macie で行う作業によって異なります。

サービスユーザー - Macie サービスを使用してジョブを実行する場合は、必要なアクセス許可と認証情報を管理者が用意します。作業を実行するためにさらに多くの Macie の機能を使用するとき、追加の許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Macie の特徴にアクセスできない場合は、Amazon Macie アイデンティティとアクセスのトラブルシューティングを参照してください。

サービス管理者 - 社内の Macie リソースを担当している場合は、通常、Macie へのフルアクセスがあります。サービスのユーザーがどの Macie 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。お客様の会社で Macie を使用して IAM を利用する方法の詳細については、Amazon Macie が と連携する方法 AWS Identity and Access Managementを参照してください。

IAM 管理者 - 管理者は、Macie へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Macie アイデンティティベースのポリシーの例を表示するには、Amazon Macie のアイデンティティベースのポリシー例を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 にサインインする方法 AWS アカウントAWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「Multi-factor authentication」(多要素認証) および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドのルートユーザー認証情報が必要なタスクを参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリ、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がにアクセスすると AWS アカウント、ロールが引き受けられ、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションするを参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdminsという名前のグループを設定して、そのグループにIAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスでき

るものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、IAM ユーザーガイドのAmazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与するを参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、IAM ユーザーガイドの(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) AWS がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドのJSON ポリシー概要を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデ

ンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、IAM ユーザーガイドのマネージドポリシーとインラインポリシーの比較を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、Amazon Simple Storage Service デベロッパーガイドのアクセスコントロールリスト (ACL) の概要を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。

エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、IAM ユーザーガイドのIAM エンティティのアクセス許可の境界を参照してください。

- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、IAM ユーザーガイドのセッションポリシーを参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

Amazon Macie が と連携する方法 AWS Identity and Access Management

AWS Identity and Access Management (IAM) を使用して Amazon Macie へのアクセスを管理する前に、Macie で使用できる IAM 機能を確認してください。

Amazon Macie で使用できる IAM の機能

IAM 機能	Macie サポート
アイデンティティベースのポリシー	あり

IAM 機能	Macie サポート
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	あり
アクセスコントロールリスト (ACL)	なし
属性ベースのアクセス制御 (ABAC) – ポリシー内のタグ	あり
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	いいえ
サービスリンクロール	あり

Macie およびその他の がほとんどの IAM 機能と AWS のサービス 連携する方法の概要については、「IAM ユーザーガイド」のAWS のサービス 「IAM と連携する 」を参照してください。

Amazon Macie のアイデンティティベースの ポリシー

アイデンティティベースポリシーをサポートする	あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、IAM ユーザーガイドのIAM JSON ポリシーの要素のリファレンスを参照してください。

Macie はアイデンティティベースのポリシーをサポートします。例については、Amazon Macie のアイデンティティベースのポリシー例を参照してください。

Amazon Macie 内のリソースベースのポリシー

リソースベースのポリシーのサポート	なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

Macie では、resource-based policies はサポートされていません。つまり、ポリシーを Macie リソースに直接アタッチすることはできません。

Amazon Macie のポリシーアクション

ポリシーアクションに対するサポート	あり

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーのAction要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

Macie のポリシーアクションは、アクションの前に、次のプレフィックスを使用しています。

```
macie2
```

例えば、プロジェクトのすべてのセグメントに関する情報を表示するためのアクセス許可をユーザーに付与するには、ポリシーに macie2:ListManagedDataIdentifiers アクションを含めます (これは、Amazon Macie API の ListManagedDataIdentifiers オペレーションに対応するアクションです)。

```
"Action": "macie2:ListManagedDataIdentifiers"
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。例:

```
"Action": [
      "macie2:ListManagedDataIdentifiers",
      "macie2:ListCustomDataIdentifiers"
]
```

ワイルドカード (*) を使用して複数のアクションを指定することもできます。例えば、List という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "macie2:List*"
```

ただしベストプラクティスとして、最小特権 の原則に準拠したポリシーを作成してください。別の言い方をすると、特定タスクの実行にのみ必要とされる権限のみが含まれたポリシーを作成してください。

Macie アクションのリストを確認するには、サービス認証リファレンスの Amazon Macie で定義されるアクションを参照してください。Macie アクションを指定するポリシーの例については、Amazon Macie のアイデンティティベースのポリシー例を参照してください。

Amazon Macie のポリシーリソース

ポリシーリソースに対するサポート	あり

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

`Resource` JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Macie は以下のリソースタイプを定義しています。

- 許可リスト
- カスタムデータ識別子
- フィルターまたは抑制ルール、検出結果フィルターとも呼ばれる
- メンバーアカウント
- 機密データ検出ジョブ分類ジョブとも呼ばれる

ポリシーでは、次のタイプの リソースに対して ARN を指定できます。

例えば、ジョブ ID が 3ce05dbb7ec5505def334104bexample の機密データ検出ジョブのポリシーを作成するには、次の ARN を使用できます。

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

または、特定のアカウントのすべての機密データ検出ジョブを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

ここで、*123456789012* はジョブを作成した AWS アカウント のアカウント ID です。ただしベストプラクティスとして、最小特権 の原則に準拠したポリシーを作成してください。別の言い方をすると、特定のリソースで特定タスクの実行にのみ必要とされる権限のみが含まれたポリシーを作成してください。

Macie アクションの中には、複数のリソースに適用できるものもあります。例えば、macie2:BatchGetCustomDataIdentifiers アクションは複数のカスタムデータ識別子の詳細を取得できます。このような場合、プリンシパルにはアクションが適用されるすべてのリソースにアクセスする権限が必要です。単一のステートメントで複数のリソースを指定するには、ARN 間をカンマで区切ります。

```
"Resource": [
 "arn:aws:macie2:*:*:custom-data-identifier/12g4aff9-8e22-4f2b-b3fd-3063eexample",
 "arn:aws:macie2:*:*:custom-data-identifier/2d12c96a-8e78-4ca6-b1dc-8fd65example",
 "arn:aws:macie2:*:*:custom-data-identifier/4383a69d-4a1e-4a07-8715-208ddexample"
]
```

Macieリソースタイプのリストとそれぞれの ARN 構文については、サービス認証リファレンスのResource types defined by Amazon Macieを参照してください。各リソースタイプで指定できるアクションについては、サービス認証リファレンスのAmazon Macie によって定義されるアクションを参照してください。リソースを指定するポリシーの例については、Amazon Macie のアイデンティティベースのポリシー例を参照してください。

Amazon Macie のポリシー条件キー

サービス固有のポリシー条件キーのサポート	あり

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、IAM ユーザーガイドのIAM ポリシーの要素: 変数およびタグを参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

Macie での条件キーの一覧については、サービス認証リファレンスのAmazon Macie の条件キーを参照してください。どのアクションおよびリソースと条件キーを使用できるかについては、Amazon Macie で定義されるアクションを参照してください。条件キーを使用するポリシーの例については、Amazon Macie のアイデンティティベースのポリシー例を参照してください。

Amazon Macie のアクセスコントロールリスト (ACL)

ACL のサポート	なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon Simple Storage Service (Amazon S3) は、ACL AWS のサービス をサポートする の例です。 ACLs ACL の詳細については、Amazon Simple Storage Service デベロッパーガイドのアクセスコントロールリスト (ACL) の概要を参照してください。

Macie では、ACL はサポートされません。つまり、Macie リソースに ACL をアタッチすることはできません。

Amazon Macie での属性ベースのアクセス制御 (ABAC)

ABAC のサポート (ポリシー内のタグ)	はい

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義するアクセス許可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/`*`key-name`*、`aws:RequestTag/`*`key-name`*、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、IAM ユーザーガイドのABAC とは?を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、IAM ユーザーガイドの属性に基づくアクセスコントロール (ABAC) を使用するを参照してください。

Macie リソース (許可リスト、カスタムデータ識別子、フィルタールールと抑制ルール、メンバーアカウント、機密データ検出ジョブ) にはタグを添付できます。ポリシーの `Condition` 要素にタグ情報を指定することで、これらのタイプのリソースへのアクセスを制御することもできます。Macie リソースのタグ付けについては、Amazon Macie リソースへのタグ付けを参照してください。タグに基づいてリソースへのアクセスを制御するアイデンティティベースのポリシーの例については、Amazon Macie のアイデンティティベースのポリシー例をご参照ください。

Amazon Macie での一時的な認証情報の使用

一時的な認証情報のサポート	あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、IAM ユーザーガイドのロールへの切り替え (コンソール)を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、IAM の一時的セキュリティ認証情報を参照してください。

Macie は、一時的な認証情報の使用をサポートしています。

Amazon Macie のフォワードアクセスセッション

転送アクセスセッション (FAS) をサポート	あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Macie は、次のタスクを実行する AWS のサービス ときに FAS リクエストをダウンストリームに送信します。

- S3 バケットに保存されている許可リストの Macie の設定を作成または更新します。
- S3 バケットに保存されている許可リストのステータスをチェックします。
- IAM ユーザー認証情報を使用して、対象の S3 オブジェクトから機密データのサンプルを取得します。

- IAM ユーザー認証情報または IAM ロールを使用して取得した機密データのサンプルを暗号化します。
- Macie が と統合できるようにします AWS Organizations。
- AWS Organizationsで組織のために委任された Macie 管理者アカウントを指定します。

他のタスクでは、Macie は、サービスリンクロールを使用して、ユーザーに代わってアクションを実行します。このロールの詳細については、Amazon Macie のサービスにリンクされたロールを参照してください。

Amazon Macie のサービスロール

サービスロールのサポート	いいえ

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドのAWS のサービスにアクセス許可を委任するロールの作成を参照してください。

Macie はサービスロールを引き受けたり使用したりしません。ユーザーに代わってアクションを実行するには、Macie は主にサービスリンクロールを使用します。このロールの詳細については、Amazon Macie のサービスにリンクされたロールを参照してください。

Amazon Macie のサービスにリンクされたロール

サービスリンクロールのサポート	あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

Macie は、サービスにリンクされたロールを使用して、ユーザーに代わってアクションを実行します。このロールの詳細については、Amazon Macie のサービスにリンクされたロールを参照してください。

Amazon Macie のアイデンティティベースのポリシー例

デフォルトでは、ユーザーおよびロールには、Macie リソースを作成または変更するアクセス許可はありません。また、AWS Management Console、AWS Command Line InterfaceAWS CLI、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、リソースで必要なアクションを実行するためのアクセス許可をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

Macie が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、サービス認可リファレンスのAmazon Macie のアクション、リソース、および条件キーを参照してください。

ポリシーを作成したら、ポリシーを保存する前に、AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) からのセキュリティ警告、エラー、一般的な警告、および提案を解決してください。IAM Access Analyzer は、IAM ポリシーの文法およびベストプラクティス に対してポリシーチェックを行います。これらのチェックにより、機能的でセキュリティのベストプラクティスに準拠したポリシーを作成するのに、役立つ結果と実行可能なレコメンデーションが示されます。IAM Access Analyzer を使用したポリシーの検証の詳細については、IAM ユーザーガイドのIAM Access Analyzer のポリシーの検証を参照してください。IAM Access Analyzer が返すことのできる警告、エラー、および提案のリストを確認するには、IAM ユーザーガイドの IAM Access Analyzer ポリシーチェックリファレンスを参照してください。

トピック

- ポリシーのベストプラクティス
- Amazon Macie コンソールの使用
- 例 : ユーザーにそれぞれのアクセス権限の確認を許可する
- 例:機密データ検出ジョブの作成をユーザーに許可する
- 例:ユーザーに機密データ検出ジョブを管理するのを許可する
- 例:ユーザーに検出結果を確認するのを許可する
- 例:タグに基づいてユーザーがカスタムデータ識別子を確認するのを許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Macie リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、AWS アカウント に追加料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください。

- AWS マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの許可の付与を開始するには、多くの一般的なユースケースのために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウント で使用できます。ユースケースに応じた AWS カスタマーマネージドポリシーを定義することで、許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイドのAWS マネージドポリシーまたはAWS ジョブ機能の管理ポリシーを参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定するときは、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイドのIAM でのポリシーとアクセス許可を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定することができます。また、AWS のサービス などの特定の AWS CloudFormation を介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、IAM ユーザーガイドのIAM JSON policy elements: Condition (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な許可を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM Access Analyzer は 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーを作成できるようサポートします。詳細については、IAM ユーザーガイドのIAM Access Analyzer ポリシーの検証を参照してください。
- 多要素認証 (MFA) を要求する – AWS アカウント で IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドのMFA 保護 API アクセスの設定を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドのIAM でのセキュリティのベストプラクティスを参照してください。

Amazon Macie コンソールの使用

Amazon Macie コンソールにアクセスするには、許可の最小限のセットが必要です。これらのアクセス許可により、AWS アカウント の Macie リソースの詳細をリストおよび表示できます。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソール許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールに Amazon Macie コンソールを使用できるようにするには、ユーザーにコンソールアクセスを提供する IAM ポリシーを作成します。詳細については、IAM ユーザーガイド の IAM のポリシーとアクセス許可を参照してください。

ユーザーまたはロールに Amazon Macie コンソールの使用を許可するポリシーを作成する場合は、そのポリシーが `macie2:GetMacieSession` アクションを許可することを確認してください。そうしないと、それらのユーザーまたはロールは、コンソール上の Macie リソースやデータにアクセスできなくなります。

また、それらのユーザーまたはロールがコンソール上でアクセスする必要のあるリソースに対して、適切な `macie2:List` アクションがポリシーで許可されていることも確認してください。そうしないと、コンソールにそれらのリソースに移動したり、リソースの詳細を表示したりすることができなくなります。たとえば、機密データ検出ジョブの詳細をコンソールを使用して確認するには、ユーザーにそのジョブの `macie2:DescribeClassificationJob` アクションと `macie2:ListClassificationJobs` アクションの実行を許可する必要があります。ユーザーが `macie2:ListClassificationJobs` アクションの実行を許可されていない場合、ユーザーはコンソールの ジョブ ページにジョブのリストを表示できないため、ジョブを選択して詳細を表示することもできません。ジョブが使用するカスタムデータ識別子に関する情報を詳細に含めるには、そのカスタムデータ識別子の `macie2:BatchGetCustomDataIdentifiers` アクションの実行もユーザーに許可されている必要があります。

例 : ユーザーにそれぞれのアクセス権限の確認を許可する

この例では、ユーザーアイデンティティに添付されたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーを作成する方法を示します。このポリシーには、コンソールで、

または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

例:機密データ検出ジョブの作成をユーザーに許可する

この例では、ユーザーに機密データ検出ジョブを作成するのを許可するポリシーを作成する方法を示します。

この例では、最初のステートメントがユーザーに macie2:CreateClassificationJob アクセス許可を付与しています。これらのアクセス許可により、ユーザーはジョブを作成できます。このス

テートメントは macie2:DescribeClassificationJob アクセス許可も付与します。これらのアクセス許可により、ユーザーは既存のジョブの詳細にアクセスできます。これらのアクセス許可はジョブの作成には必要ありませんが、これらの詳細にアクセスできると、ユーザーが独自の設定設定を持つジョブを作成するのに役立ちます。

この例の 2 番目のステートメントでは、ユーザーは Amazon Macie コンソールを使用してジョブを作成、設定、およびレビューできます。macie2:ListClassificationJobs のアクセス許可により、ユーザーはコンソールの ジョブ ページに既存のジョブを表示できます。ステートメント内の他のすべてのアクセス許可では、ユーザーはコンソールの ジョブを作成 ページを使用してジョブを設定および作成できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndReviewJobs",
            "Effect": "Allow",
            "Action": [
                "macie2:CreateClassificationJob",
                "macie2:DescribeClassificationJob"
            ],
            "Resource": "arn:aws:macie2:*:*:classification-job/*"
        },
        {
            "Sid": "CreateAndReviewJobsOnConsole",
            "Effect": "Allow",
            "Action": [
                "macie2:ListClassificationJobs",
                "macie2:ListAllowLists",
                "macie2:ListCustomDataIdentifiers",
                "macie2:ListManagedDataIdentifiers",
                "macie2:SearchResources",
                "macie2:DescribeBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

例:ユーザーに機密データ検出ジョブを管理するのを許可する

この例では、ユーザーが特定の機密データ検出ジョブ (ID が 3ce05dbb7ec5505def334104bexample のジョブ) の詳細にアクセスするのを許可するポリシーを作成する方法を示します。この例では、ユーザーは必要に応じてジョブのステータスを変更することもできます。

例の最初のステートメントは、ユーザーに macie2:DescribeClassificationJob と macie2:UpdateClassificationJob のアクセス許可を付与します。これらのアクセス許可により、ユーザーはそれぞれジョブの詳細を取得したり、ジョブのステータスを変更したりできます。2 番目のステートメントはユーザーに macie2:ListClassificationJobs アクセス許可を付与します。これにより、ユーザーは Amazon Macie コンソールの ジョブ ページを使用してジョブにアクセスできます。

```
{
   "Version": "2012-10-17",
   "Statement": [
 {
         "Sid": "ManageOneJob",
         "Effect": "Allow",
         "Action": [
            "macie2:DescribeClassificationJob",
            "macie2:UpdateClassificationJob"
         ],
         "Resource": "arn:aws:macie2:*:*:classification-
job/3ce05dbb7ec5505def334104bexample"
 },
 {
         "Sid": "ListJobsOnConsole",
         "Effect": "Allow",
         "Action": "macie2:ListClassificationJobs",
         "Resource": "*"
 }
   ]
}
```

Macie がジョブ用に Amazon CloudWatch Logs に公開するロギングデータ (ログイベント) にユーザーがアクセスできるようにすることもできます。そのためには、ロググループで CloudWatch ログlogs アクションを実行するアクセス権限を付与するステートメントを追加し、ジョブのストリーミングを行うことができます。例:

```
"Statement": [
    {
        "Sid": "AccessLogGroupForMacieJobs",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs"
    },
    {
        "Sid": "AccessLogEventsForOneMacieJob",
        "Effect": "Allow",
        "Action": "logs:GetLogEvents",
        "Resource": [
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs/*",
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs:log-
stream:3ce05dbb7ec5505def334104bexample"
        ]
    }
]
```

CloudWatch Logs のアクセス管理の詳細については、Amazon CloudWatch Logs ユーザーガイドのCloudWatch Logs リソースへの許可の管理の概要を参照してください。

例:ユーザーに検出結果を確認するのを許可する

この例では、ユーザーに結果データへのアクセスを許可するポリシーを作成する方法を示しています。

この例では、`macie2:GetFindings` および `macie2:GetFindingStatistics` アクセス権限により、ユーザーは Amazon Macie API または Amazon Macie コンソールを使用してデータを取得できます。この `macie2:ListFindings` 権限により、ユーザーは Amazon Macie コンソールの 概要 ダッシュボードと 検出結果 ページを使用してデータを取得および確認できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
```

```
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

また、検出結果のフィルタルールと抑制ルールの作成と管理をユーザーに許可することもできます。そのためには、macie2:CreateFindingsFilter、macie2:GetFindingsFilter、macie2:UpdateFindingsFi および macie2:DeleteFindingsFilter などのアクセス許可を付与するステートメントを含めることができます。ユーザーが Amazon Macie コンソールを使用してルールを管理できるようにするには、ポリシーに macie2:ListFindingsFilters アクセス権限も含めてください。例:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageRules",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindingsFilter",
                "macie2:UpdateFindingsFilter",
                "macie2:CreateFindingsFilter",
                "macie2:DeleteFindingsFilter"
            ],
            "Resource": "arn:aws:macie2:*:*:findings-filter/*"
        },
        {
            "Sid": "ListRulesOnConsole",
```

```
            "Effect": "Allow",
            "Action": "macie2:ListFindingsFilters",
            "Resource": "*"
        }
    ]
}
```

例:タグに基づいてユーザーがカスタムデータ識別子を確認するのを許可する

アイデンティティベースのポリシーでは、条件を使用して、タグに基づいて Amazon Macie リソースへのアクセスを制御できます。この例では、ユーザーが Amazon Macie コンソールまたは Amazon Macie API を使用してカスタムデータ識別子を確認するのを許可するポリシーを作成する方法を示します。ただし、アクセス許可は、Owner タグの値がそのユーザーのユーザー名である場合にのみ付与されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewCustomDataIdentifiersIfOwner",
            "Effect": "Allow",
            "Action": "macie2:GetCustomDataIdentifier",
            "Resource": "arn:aws:macie2:*:*:custom-data-identifier/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListCustomDataIdentifiersOnConsoleIfOwner",
            "Effect": "Allow",
            "Action": "macie2:ListCustomDataIdentifiers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

この例では、そのユーザー名 richard-roe を持つユーザーがカスタムデータ識別子の詳細を確認しようとした場合、カスタムデータ識別子には Owner=richard-roe または owner=richard-roe はのタグを付ける必要があります。それ以外の場合、ユーザーはアクセスを拒否されます。条件キー

名では大文字と小文字は区別されないため、条件タグキー Owner は Owner と owner に一致します。詳細については、IAM ユーザーガイドのIAM JSON ポリシー要素: 条件を参照してください。

Amazon Macie のサービスにリンクされたロール

Amazon Macie はという名前の AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。AWSServiceRoleForAmazonMacieこのサービスリンクロールは、Macie に直接リンクされた IAM ロールです。Macie が事前に定義したもので、Macie AWS のサービス がユーザーに代わって他のユーザーを呼び出したり、リソースをモニタリングしたりするのに必要なすべての権限が含まれています。 AWS Macie は、Macie を利用できるすべての AWS リージョン でこのサービスリンクロールを使用します。

サービスにリンクされたロールを使用することで、必要なアクセス許可を手動で追加する必要がなくなるため、Macie の設定が簡単になります。Macie は、このサービスリンクロールのアクセス許可を定義します。特に定義されている場合を除き、Macie のみがそのロールを引き受けることができます。定義された許可には信頼ポリシーと許可ポリシーが含まれ、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザーやロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、IAM ユーザーガイドのサービスリンクロールのアクセス許可を参照してください。サービスリンクロールは、その関連リソースを削除した後にのみ削除できます。これにより、リソースにアクセスするための許可を意図せず削除することが防止され、 リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、IAM と連携するAWS のサービスを参照し、サービスにリンクされたロールの列内ではいと表記されたサービスを確認してください。サービスリンクロールに関するドキュメントをサービスで確認するには、はいリンクを選択します。

トピック

- Amazon Macie 向けのサービスリンクロールのアクセス許可
- Amazon Macie 向けのサービスリンクロールを作成する
- Amazon Macie 向けのサービスリンクロールを編集する
- Amazon Macie 向けのサービスリンクロールを削除する
- Amazon Macie サービスにリンクされたロールでサポートされています AWS リージョン

Amazon Macie 向けのサービスリンクロールのアクセス許可

Amazon Macie では、AWSServiceRoleForAmazonMacie という名称のサービスリンクロールを使用します。このサービスリンクロールは、ロールを引き受ける上で macie.amazonaws.com サービスを信頼します。

AmazonMacieServiceRolePolicy と呼ばれるロールのアクセス許可ポリシーにより、Macie は次のようなタスクを、指定されたリソースで実行することが許可されます:

- Amazon S3 アクションを使用して、S3 バケットとオブジェクトに関する情報を取得します。
- Amazon S3 アクションを使用して、S3 オブジェクトを取得します。
- AWS Organizations アクションを使用して、関連するアカウントに関する情報を取得できます。
- Amazon CloudWatch Logs アクションを使用して、機密データ検出ジョブのイベントを記録します。

このロールは、次のアクセス許可ポリシーを使用して設定されます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
```

```
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

AmazonMacieServiceRolePolicy ポリシーへの更新詳細については、AWS マネージドポリシーへの Amazon Macie の更新 を参照してください。このポリシーの変更に関する自動アラートを受け取るには、Macie ドキュメント履歴ページの RSS フィードを購読してください。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザーやロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、IAM ユーザーガイドのサービスリンクロールのアクセス許可を参照してください。

Amazon Macie 向けのサービスリンクロールを作成する

Amazon Macie 向けに AWSServiceRoleForAmazonMacie サービスリンクロールを手動で作成する必要はありません。Macie を有効にすると AWS アカウント、Macie はサービスにリンクされたロールを自動的に作成します。

この Macie サービスリンクロールを削除した後、また作成が必要になった場合は、同じプロセスでユーザーのアカウントにそのロールを再作成することができます。Macie を再び有効にすると、Macie はユーザー用にサービスリンクロールを再度作成します。

Amazon Macie 向けのサービスリンクロールを編集する

Amazon Macie では、AWSServiceRoleForAmazonMacie のサービスリンクロールを編集することはできません。サービスリンクロールが作成されると、多くのエンティティによってそのロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、IAM ユーザーガイドのサービスにリンクされたロールの編集を参照してください。

Amazon Macie 向けのサービスリンクロールを削除する

Amazon Macie が不要になった場合は、AWSServiceRoleForAmazonMacie のサービスリンクロールを手動で削除することをお勧めします。Macie を無効化しても、Macie はそのロールを削除しません。

ロールを削除する前に、有効にした各 AWS リージョン Macie を無効にする必要があります。また、ロールのリソースは手動でクリーンアップする必要があります。ロールを削除するには、IAM コンソール、 AWS CLI、または API を使用できます。 AWS 詳細については、IAM ユーザーガイドのサービスにリンクされたロールの削除を参照してください。

> **Note**
>
> リソースを削除する際に、AWSServiceRoleForAmazonMacie のロールが使用されている場合、削除が失敗することがあります。その場合は、数分待ってから操作を再試行してください。

AWSServiceRoleForAmazonMacie サービスリンクロールを削除した後、また作成が必要になった場合は、ユーザーのアカウント用の Macie を有効化することで再作成することができます。Macie を再び有効にすると、Macie はユーザー用にサービスリンクロールを再度作成します。

Amazon Macie サービスにリンクされたロールでサポートされています AWS リージョン

Amazon Macie は、Macie AWSServiceRoleForAmazonMacie AWS リージョン が利用可能なすべての場所でサービスにリンクされたロールの使用をサポートしています。Macie が現在利用可能な

リージョンの一覧については、AWS 全般のリファレンス のAmazon Macie エンドポイントとクォータを参照してください。

Amazon Macie の AWS マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。AWS のすべてのお客様が使用できるようになるのを避けるためです。ユースケース別にカスタマー管理ポリシーを定義することで、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義したアクセス権限は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、IAM ユーザーガイドのAWS 管理ポリシーを参照してください。

Amazon Macie には、`AmazonMacieFullAccess` ポリシー、`AmazonMacieReadOnlyAccess` ポリシー、`AmazonMacieServiceRolePolicy` ポリシーという複数の AWS 管理ポリシーが用意されています。

トピック

- AWS マネージドポリシー: AmazonMacieFullAccess
- AWS マネージドポリシー: AmazonMacieReadOnlyAccess
- AWS マネージドポリシー: AmazonMacieServiceRolePolicy
- AWS マネージドポリシーへの Amazon Macie の更新

AWS マネージドポリシー: AmazonMacieFullAccess

IAM エンティティに AmazonMacieFullAccess ポリシーをアタッチできます。

このポリシーは、IAM アイデンティティ (プリンシパル) がAmazon Macie サービスにリンクされたロールを作成し、Amazon Macie のすべての読み取り/書き込みアクションを実行できるようにする完全な管理権限を付与します。アクセス許可には、作成、更新、削除などの変更機能が含まれます。このポリシーがプリンシパルにアタッチされている場合、プリンシパルはアカウントのすべての Macie リソース、データ、設定を作成、取得、その他の方法でアクセスできます。

プリンシパルが自分のアカウントで Macie を有効にする前に、このポリシーをプリンシパルにアタッチする必要があります。プリンシパルが自分のアカウントで Macie を有効にするには、Macie サービスにリンクされたロールの作成を許可されている必要があります。

許可の詳細

このポリシーには、以下の許可が含まれています。

- macie2 — プリンシパルが Amazon Macie のすべての読み取りおよび書き込みアクションを実行できるようにします。
- iam - サービスにリンクされたロールの作成をプリンシパルに許可します。Resource の要素は、Macie のサービスにリンクされたロールを指定します。Condition の要素は iam:AWSServiceName条件キーと条件演算子を使用して、Macie のサービスにリンクされたロールへのアクセス権限を制限します。
- pricing — プリンシパルが AWS Billing and Cost Management から AWS アカウント の価格データを取得できるようにします。Macie は、プリンシパルが機密データ検出ジョブを作成および設定するときに、このデータを使用して推定コストを計算して表示します。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:*"
         ],
         "Resource": "*"
      },
      {
```

```
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "macie.amazonaws.com"
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": "pricing:GetProducts",
         "Resource": "*"
      }
   ]
}
```

AWS マネージドポリシー: AmazonMacieReadOnlyAccess

IAM エンティティに AmazonMacieReadOnlyAccess ポリシーをアタッチできます。

このポリシーは、IAM ID (プリンシパル) が Amazon Macie のすべての読み取りアクションを実行できるようにする読み取り専用のアクセス許可を付与します。アクセス許可には、作成、更新、削除などの変更機能は含まれません。このポリシーがプリンシパルにアタッチされている場合、プリンシパルはアカウントのすべての Macie リソース、データ、設定を取得できますが、それ以外の方法ではアクセスできません。

許可の詳細

このポリシーには、以下の許可が含まれています。

macie2 - プリンシパルにすべての Amazon Macie アクションを実行するためのフルアクセスを許可します。

```
{
   "Version": "2012-10-17",
   "Statement": [
```

```
      {
         "Effect": "Allow",
         "Action": [
            "macie2:Describe*",
            "macie2:Get*",
            "macie2:List*",
            "macie2:BatchGetCustomDataIdentifiers",
            "macie2:SearchResources"
         ],
         "Resource": "*"
      }
   ]
}
```

AWS マネージドポリシー: AmazonMacieServiceRolePolicy

IAM エンティティに AmazonMacieServiceRolePolicy をアタッチすることはできません。このポリシーは、ユーザーに代わって Macie がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、Amazon Macie のサービスにリンクされたロールを参照してください。

AWS マネージドポリシーへの Amazon Macie の更新

Amazon Macie の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について確認します。このページの変更に関する自動通知については、Macie ドキュメント履歴 ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AmazonMacieReadOnlyAccess – は新しいポリシーを追加しました。	Macie は新しいポリシー、AmazonMacieReadOnlyAccess ポリシーを追加しました。このポリシーは、プリンシパルがアカウントのすべての Macie リソース、データ、および設定を取得できる	2023 年 6 月 15 日

変更	説明	日付
	読み取り専用のアクセス許可を付与します。	
AmazonMacieFullAccess – 既存のポリシーの更新	AmazonMacieFullAccess ポリシーには、Macie は、Macie サービスにリンクされたロールaws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie の Amazon リソースネーム (ARN) を更新しました。	2022 年 6 月 30 日
AmazonMacieServiceRolePolicy – 既存のポリシーの更新	Macie は Amazon Macie クラシックのアクションとリソースを AmazonMacieServiceRolePolicy ポリシーから削除しました。Amazon Macie クラシックは廃止され、現在は利用できなくなっています。 具体的には、Macie はすべての AWS CloudTrail アクションを削除しました。Macie は、arn:aws:s3:::awsmacie-* 、arn:aws:s3:::awsmacietrail-* および arn:aws:s3:::*-awsmacietrail-* というリソースの Amazon S3 アクションもすべて削除しました。	2022 年 5 月 20 日

変更	説明	日付
AmazonMacieFullAccess – 既存のポリシーの更新	Macie は AmazonMacieFullAccess ポリシーに AWS Billing and Cost Managementpricing アクションを追加しました。このアクションにより、プリンシパルはアカウントの価格データを取得できます。Macie は、プリンシパルが機密データ検出ジョブを作成および設定するときに、このデータを使用して推定コストを計算して表示します。 また、Macie は AmazonMacieFullAccess ポリシーから Amazon Macie クラシックmacie アクションを削除しました。	2022 年 3 月 7 日
AmazonMacieServiceRolePolicy – 既存のポリシーの更新	Macie は、Amazon CloudWatch Logs のアクションを AmazonMacieServiceRolePolicy ポリシーに追加しました。これらのアクションは、Macie が機密データ検出ジョブのためにログイベントを CloudWatch Logs に発行することを許可します。	2021 年 4 月 13 日
Macie が変更の追跡を開始しました	Macie がその AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 4 月 13 日

Amazon Macie アイデンティティとアクセスのトラブルシューティング

以下の情報は、Amazon Macie と AWS Identity and Access Management (IAM) の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

Amazon Macie でアクションを実行する権限がありません。

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なmacie2:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 macie2:GetWidget on resource: my-example-widget
```

この場合、macie2:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに Amazon Macie リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Macie でこれらの特徴がサポートされるかどうかを確認するには、Amazon Macie が と連携する方法 AWS Identity and Access Managementを参照してください。

- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

Amazon Macie でのログ記録とモニタリング

Amazon Macie は、ユーザー、ロール、または別の AWS のサービス によって Macie で実行されたアクションを記録するサービスである AWS CloudTrail と統合されています。これには、Amazon Macie コンソールからのアクションと Amazon Macie API オペレーションへのプログラムによる呼び出しが含まれます。CloudTrail によって収集された情報を使用して、Macie に対して行われたリクエストを確認できます。リクエストごとに、リクエスト日時、リクエスト元の IP アドレス、作成者、その他の詳細を確認できます。詳細については、AWS CloudTrail を使用した Amazon Macie API コールのログ作成を参照してください。

Amazon Macie のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon Macie の耐障害性

AWS のグローバルインフラストラクチャは AWS リージョン とアベイラビリティーゾーンを中心として構築されます。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン とアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

Amazon Macie のインフラストラクチャセキュリティ

マネージドサービスである Amazon Macie は AWS グローバルネットワークセキュリティで保護されています。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、AWS クラウドセキュリティを参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、セキュリティの柱 - AWS Well-Architected Frameworkのインフラストラクチャ保護を参照してください。

AWS が発行している API コールを使用し、ネットワーク経由で Macie にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS) TLS 1.2 および TLS 1.3 をお勧めします。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートです。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token ServiceAWS STS を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

Amazon Macie とインターフェイス VPC エンドポイントAWS PrivateLink

Amazon Virtual Private Cloud (Amazon VPC) を使用して AWS リソースをホストする場合、VPC と Amazon Macie の間のプライベート接続を確立できます。Amazon VPC は、ユーザー定義の仮想ネットワークで AWS のサービス リソースを起動するために使用できる AWS サービスです。VPC を使用すると、IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどのネットワーク設定を制御できます。

VPC を Macie に接続するには、Macieのインターフェイス VPC エンドポイントを定義します。インターフェイスエンドポイントでは AWS PrivateLink を利用します。このテクノロジーにより、インターネットゲートウェイ、NAT デバイス、VPN 接続、AWS Direct Connect 接続のいずれも必要とせずに、Amazon Macie へのプライベートアクセスが可能になります。VPC のインスタンスは、パブリック IP アドレスがなくても Amazon Macie API と通信できます。VPC と Macie 間のトラフィックは、Amazon ネットワークを離れません。

各インターフェイスエンドポイントは、サブネット内の 1 つ以上の Elastic Network Interface によって表されます。詳細については、Amazon VPC ユーザーガイドのAWS のサービス インターフェイスVPCエンドポイントを使用するのアクセスを参照してください。

トピック

- Amazon Macie VPC エンドポイントに関する考慮事項
- Amazon Macie 用のインターフェイス VPC エンドポイントの作成

Amazon Macie VPC エンドポイントに関する考慮事項

Amazon Macie は、アジアパシフィック (大阪) リージョンとイスラエル (テルアビブ) リージョンを除く、現在利用可能なすべての AWS リージョン リージョンの VPC エンドポイントをサポートしています。Macie が現在利用可能なリージョンの一覧については、AWS 全般のリファレンスのAmazon Macie エンドポイントとクォータを参照してください。また Macie は、API アクションの VPC からの呼び出しをすべてサポートしています。

Macie 用のインターフェイス VPC エンドポイントを作成する場合は、他の AWS のサービス でも VPC サポートを提供し、Amazon EventBridge や AWS Security Hub などの Macie と統合する同じ手順を考慮してください。これで Macie とそれらのサービスは VPC エンドポイントを統合に使用できます。例えば、Macie 用の VPC エンドポイントと Security Hub 用の VPC エンドポイントを作成した場合、Macie は検出結果を Security Hub に発行するときに VPC エンドポイントを使用で

き、Security Hub はその検出結果を受信するときに VPC エンドポイントを使用できます。VPC エンドポイントをサポートするサービスの詳細については、Amazon VPC ユーザーガイドのAWS のサービス と AWS PrivateLink の統合を参照してください。

詳細については、Amazon VPC ユーザーガイドのAWS のサービス インターフェイスVPCエンドポイントを使用するのアクセスを参照してください。

VPC エンドポイントポリシーは Macie ではサポートされません。デフォルトでは、エンドポイント経由のフルアクセスが許可されています。詳細については、Amazon VPC ユーザーガイドのVPC エンドポイントおよび VPC エンドポイントサービスの Identity and Access Management を参照してください。

Amazon Macie 用のインターフェイス VPC エンドポイントの作成

Amazon Macie サービス用のインターフェース VPC エンドポイントは、Amazon VPC コンソールまたは AWS Command Line InterfaceAWS CLIを使用して作成できます。詳細については、Amazon VPC ユーザーガイドのインターフェイス VPC エンドポイントを使用するを参照してください。

Macie 用の VPC エンドポイントを作成するには、次のサービス名を使用します。

- com.amazonaws.*****.macie2

ここで、*****は該当する AWS リージョン のリージョンコードです。

エンドポイントのプライベート DNS を有効にすると、リージョンのデフォルト DNS 名 (例: 米国東部 (バージニア北部)の `macie2.us-east-1.amazonaws.com`) を使用して、 Macie への API リクエストを実行できます。

詳細については、Amazon VPC ユーザーガイドのインタフェース VPC エンドポイントを使用した AWS のサービスへのアクセス を参照してください。

AWS CloudTrail を使用した Amazon Macie API コールのログ作成

Amazon Macie は、ユーザー、ロール、または AWS のサービス によって Macie で実行されたアクションを記録するサービスである AWS CloudTrail と統合されています。CloudTrail は、Macie のすべての API コールをイベントとしてキャプチャします。コールには、Amazon Macie コンソールからの呼び出しと、Amazon Macie API オペレーションに対するプログラムによる呼び出しが含まれます。

証跡を作成する場合は、Macie のイベントなど、Amazon Simple Storage Service (Amazon S3) バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、AWS CloudTrail コンソールの [イベント履歴] を使用して最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Macie に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、『AWS CloudTrail ユーザーガイド』を参照してください。

トピック

- AWS CloudTrail での Amazon Macie 情報
- Amazon Macie ログファイルエントリの概要

AWS CloudTrail での Amazon Macie 情報

AWS CloudTrail は、アカウント作成時に AWS アカウント で有効になります。Amazon Macie でアクティビティが発生すると、そのアクティビティは [イベント履歴] で AWS のその他のサービスのイベントとともに CloudTrail イベントにレコードされます。最近のイベントは、AWS アカウントで確認、検索、ダウンロードできます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。

Macie に関するイベントを含めた AWS アカウント 内でのイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon Simple Storage Service (Amazon S3) バケットに配信できます。デフォルトでは、AWS CloudTrail コンソールを使用して証跡を作成するときに、証跡がすべての AWS リージョン に適用されます。証跡では、AWS パーティションのすべてのリージョンからのイベントがログに記録され、指定した S3 バケットにログファイルが配信されます。さらに、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それ

を基にアクションを取るために他の AWS のサービス を設定できます。次のトピックの詳細については、AWS CloudTrail ユーザーガイドを参照してください。

- AWS アカウント の追跡の作成
- CloudTrail がサポートされているサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- CloudTrail ログファイルの複数のリージョンからの受け取り
- 複数のアカウントから CloudTrail ログファイルを受け取る

すべての Macie アクションは、CloudTrail によってログに記録され、「Amazon Macie API リファレンス」で説明されています。例えば、`CreateClassificationJob`、`DescribeBuckets`、`ListFindings` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するために役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストが、ロールとフェデレーションユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか。
- リクエストが、別の AWS のサービス によって送信されたかどうか。

詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail userIdentity エレメント」を参照してください。

Amazon Macie ログファイルエントリの概要

証跡は、指定した Amazon Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどの情報が含まれます。AWS CloudTrail ログファイルには、イベントの 1 つ以上のログエントリが含まれています。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

以下の例では、Amazon Macie アクションのイベントを示す CloudTrail ログエントリを示しています。ログエントリに含まれる可能性のある情報の詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail ログイベントリファレンス」を参照してください。

例: 検出結果の一覧表示

次の例は、Macie の ListFindings アクションについてのイベントを示す CloudTrail ログエントリを示しています。この例では、ある AWS Identity and Access Management (IAM) ユーザー (Mary_Major) が Amazon Macie コンソールを使用して、自分のアカウントのために、現在のポリシーに関する検出結果についての情報のサブセットを取得しました。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext":{
            "attributes": {
                "creationdate": "2023-11-14T15:49:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-14T16:09:56Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "ListFindings",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "sortCriteria": {
            "attributeName": "updatedAt",
            "orderBy": "DESC"
        },
        "findingCriteria": {
            "criterion": {
                "archived": {
                    "eq": [
```

```
                        "false"
                    ]
                },
                "category": {
                    "eq": [
                        "POLICY"
                    ]
                }
            }
        },
        "maxResults": 25,
        "nextToken": ""
    },
    "responseElements": null,
    "requestID": "d58af6be-1115-4a41-91f8-ace03example",
    "eventID": "ad97fac5-f7cf-4ff9-9cf2-d0676example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

例: 検出結果についての機密データのサンプルの取得

この例は、Macie が検出結果で報告した機密データのサンプルを取得して公開するためのイベントを示す CloudTrail ログエントリを示しています。この例では、ある IAM ユーザー (JohnDoe) が Amazon Macie コンソールを使用して機密データのサンプルを取得して公開しました。ユーザーの Macie アカウントは、機密データのサンプルを取得して公開するための IAM ロール (MacieReveal) を引き受けるように設定されています。

次の口グイベントは、Macie の GetSensitiveDataOccurrences アクションを実行することで機密データのサンプルを取得して公開するというユーザーのリクエストの詳細を示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "UU4MH7OYK5ZCOAEXAMPLE:JohnDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/JohnDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "UU4MH7OYK5ZCOAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-12-12T14:40:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "GetSensitiveDataOccurrences",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "findingId": "3ad9d8cd61c5c390bede45cd2example"
    },
    "responseElements": null,
    "requestID": "c30cb760-5102-47e7-88d8-ff2e8example",
    "eventID": "baf52d92-f9c3-431a-bfe8-71c81example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


次のログイベントは、その後に AWS Security Token Service (AWS STS) AssumeRole アクションを実行することによって、指定された IAM ロール (`MacieReveal`) を引き受ける Macie に関する詳細を示します。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "reveal-samples.macie.amazonaws.com"
```

```
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "reveal-samples.macie.amazonaws.com",
    "userAgent": "reveal-samples.macie.amazonaws.com",
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/MacieReveal",
        "roleSessionName": "RevealCrossAccount"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionToken": "XXYYaz...
EXAMPLE_SESSION_TOKEN
XXyYaZAz",
            "expiration": "Dec 12, 2023, 6:04:47 PM"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROAXOTKAROCSNEXAMPLE:RevealCrossAccount",
            "arn": "arn:aws:sts::111122223333:assumed-role/MacieReveal/
RevealCrossAccount"
        }
    },
    "requestID": "d905cea8-2dcb-44c1-948e-19419example",
    "eventID": "74ee4d0c-932d-3332-87aa-8bcf3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::IAM::Role",
            "ARN": "arn:aws:iam::111122223333:role/MacieReveal"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Amazon Macie リソースへのタグ付け

タグは、特定のタイプの Amazon Macie リソースなど AWS リソースを定義して割り当てることができるオプションのラベルです。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを特定、分類および管理できます。例えば、タグを使用してポリシーを適用したり、コストを割り当てたり、リソースのバージョンを区別したり、特定のコンプライアンス要件やワークフローをサポートするリソースの識別を行うことができます。

許可リスト、カスタムデータ識別子、検出結果のフィルタールールと抑制ルール、機密データ検出ジョブなどのタイプの Macie リソースにタグを割り当てることができます。ユーザーが組織の Macie 管理者である場合、組織のメンバーアカウントにタグを割り当てることもできます。

トピック

タグ付けの基本

リソースには、最大 50 個のタグを含めることができます。タグはそれぞれ、1 つの必須タグキーとオプションの 1 つのタグ値で設定されており、どちらもお客様側が定義します。タグキーは、より具体的なタグ値のカテゴリとして動作する一般的なラベルです。タグ値は、タグキーの記述子として機能します。

例えば、カスタムデータ識別子と機密データ検出ジョブを作成して、ワークフローのさまざまな時点でデータを分析する場合 (ステージングデータ用と本番データ用のセット)、それらのリソースに `Stack` タグキーを割り当てることができます。このタグキーのタグ値は、ステージングされたデータを分析するために設計されたカスタムデータ識別子やジョブ用の `Staging` と、それ他用の `Production` に使用される場合があります。

リソースにタグを定義して割り当てる際、以下の点に注意してください。

- 各リソースには、最大 50 個のタグを設定できます。

- タグキーは、リソースごとにそれぞれ一意である必要があります。また、各タグキーに設定できる値は 1 つのみです。
- タグのキーと値は大文字と小文字が区別されます。タグに大文字を使用する場合の戦略を決定し、その戦略をすべてのリソースにわたって一貫して実装することをベストプラクティスとして推奨します。
- タグキーは最大 128 文字 (UTF-8) です。タグキーは最大 256 文字 (UTF-8) です。文字には、文字、数字、スペース、または記号 (_ . : / = + - @) を使用できます。
- `aws:` プレフィックスは AWS 用に限定されています。定義したどのタグキーやタグ値にも使用できません。さらに、このプレフィックスを使用するタグキーまたは値は変更または削除できません。このプレフィックスを使用するタグは、リソースあたりのタグ数のクォータ (50 個) にはカウントされません。
- 割り当てたタグは、自分の AWS アカウント だけが使用でき、割り当てた AWS リージョン でしか使用できません。
- リソースを削除すると、リソースに関連付けられているすべてのタグも削除されます。

その他の制限事項、ヒント、ベストプラクティスについては、AWS リソースのタグ付けのユーザーガイドを参照してください。

> **Important**
>
> 機密データやその他の重要なデータをタグに保存しないでください。タグは、多くの AWS のサービス から AWS Billing and Cost Management も含めてアクセスできます。プライベートデータや機密データに使用することを意図していません。

Macie リソースのタグを追加、管理するには、Amazon Macie コンソール、Amazon Macie API、AWS Resource Groups コンソールのタグエディター、または AWS Resource Groups タグ付け API を使用します。Macie を使用すると、リソースを作成するとき、リソースにタグを追加できます。また、既存のリソースごとにタグを追加、管理することもできます。リソースグループを使用すると、Macie を含む複数の AWS のサービス にかかる既存リソースに対し、タグを一括で追加、管理できます。詳細については、AWS リソースのタグ付けのユーザーガイドを参照してください。

IAMポリシーでタグを使用する

リソースのタグ付けを開始した後、タグベースのリソースレベルのアクセス許可を AWS Identity and Access Management (IAM) ポリシーで定義できます。このようにタグを使用することで、AWS アカ

ウント のどのユーザーと役割にリソースの作成とタグ付けのアクセス許可があって、どのユーザーと役割にタグの追加、編集、削除のアクセス許可があるかを、広範囲にきめ細かく制御できます。タグに基づいてアクセスを制御するには、IAM ポリシーの条件の要素でタグ関連の条件キーを使用します。

例えば、リソースの Owner タグの値がユーザー名となっているすべての Amazon Macie リソースに対して、ユーザーにフルアクセスを許可するポリシーを作成できます。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "macie2:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

タグをベースにしてリソースレベルでアクセス許可を定義した場合、そのアクセス許可は即座に反映されます。つまり、リソースが作成されるとすぐにリソースの安全性が増し、新しいリソースにタグの使用をすぐに強制できるようになります。リソースレベルのアクセス許可を使用して、新しいリソースと既存のリソースに、どのタグキーと値を関連付けるかを制御することもできます。詳細については、IAM ユーザーガイドのタグを使用したAWSリソースへのアクセスのコントロールを参照してください。

Amazon Macie リソースへのタグの追加

個々の Amazon Macie リソースにタグを追加するには、Amazon Macie コンソールまたは Amazon Macie API を使用します。複数の Macie リソースに同時にタグを追加するには、AWS Resource Groups コンソールのタグエディタを使用するか、AWS Resource Groups タグ付け APIのタグ付けオペレーションを使用します。

> **Important**
>
> リソースにタグを追加すると、リソースへのアクセスに影響を与える可能性があります。リソースにタグを追加する前に、タグを使用してリソースへのアクセスを制御する可能性のある AWS Identity and Access Management IAM ポリシーがあれば、必ず確認してください。

Console

許可リスト、カスタムデータ識別子、または機密データ検出ジョブを作成すると、Amazon Macie コンソールにはリソースにタグを追加するためのオプションが表示されます。リソースを作成するときは、コンソールの指示に従ってこれらのタイプのリソースにタグを追加します。フィルタルール、抑制ルール、または組織のメンバーアカウントにタグを追加するには、タグを追加する前にリソースを作成する必要があります。

Amazon Macie コンソールを使用して既存のリソースに 1 つ以上のタグを追加するには、次のステップに従います。

リソースにタグを追加

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. タグを追加するリソースのタイプに応じて、以下のいずれかを実行します。
   - 許可リストについては、ナビゲーションペインで 許可リスト を選択します。

     次に、テーブル内のリストのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。
   - カスタムデータ識別子の場合は、ナビゲーションペインの カスタムデータ識別子 を選択します。

     次に、テーブル内のカスタムデータ識別子のチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。
   - フィルタまたは抑制ルールについては、ナビゲーションペインで 検出結果 を選択します。

     次に、保存されたルール リストで、ルールの横にある編集アイコン
     を選択します。次に、タグを管理 を選択します。

- 組織のメンバーアカウントについては、ナビゲーションペインで アカウント を選択します。

  次に、テーブル内のアカウントのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。
- 機密データ検出ジョブについては、ナビゲーションペインで ジョブ を選択します。

  次に、テーブル内のジョブのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。

タグを管理 ウィンドウには、現在リソースに割り当てられているタグがすべて一覧表示されます。

3. タグを管理 ウィンドウで タグの編集 を選択します。
4. タグを追加 を選択します。
5. キー ボックスに、リソースに追加するタグ用のタグキーを入力します。次に、値 ボックスに、任意でキーのタグ値を入力します。

   タグキーには最大 128 文字を含めることができます。タグ値は最大 256 文字を含めることができます。文字には、文字、数字、スペース、または記号 (_ . : / = + - @) を使用できます。
6. (オプショナル) 別のタグをリソースに追加するには、タグを追加 をクリックし、前の手順を繰り返します。1 つのリソースに最大 50 個のタグを割り当てることができます。
7. タグの追加を完了したら、保存 を選択します。

API

リソースを作成して 1 つ以上のタグをプログラムで追加するには、作成するリソースのタイプに適した `Create` オペレーションを使用します。

- 許可リスト – CreateAllowListオペレーションを使用するか、AWS Command Line InterfaceAWS CLIを使用している場合はcreate-allow-listコマンドを実行します。
- カスタムデータ識別子 — CreateCustomDataIdentifierオペレーションを使用するか、AWS CLI を使用している場合はcreate-custom-data-identifierコマンドを実行します。
- フィルターまたは抑制ルール —CreateFindingsFilterオペレーションを使用するか、AWS CLI を使用している場合はcreate-findings-filterコマンドを実行します。
- メンバーアカウント —CreateMemberオペレーションを使用するか、AWS CLI を使用している場合はcreate-memberコマンドを実行します。

- 機密データ検出ジョブ — CreateClassificationJobオペレーションを使用するか、AWS CLI を使用している場合はcreate-classification-job コマンドを実行します。

リクエストでは、tags パラメータを使用して、リソースに追加する各タグのタグキーkeyとオプションのタグ値valueを指定します。tags パラメータは、タグキーとそれに関連するタグ値の文字列間マップを指定します。

既存のリソースに 1 つ以上のタグを追加するには、Amazon Macie API の TagResourceオペレーションを使用するか、AWS CLI を使用している場合はtag-resourceコマンドを実行します。リクエストでは、タグを追加するリソースの Amazon リソースネーム (ARN) を指定します。tags パラメータを使用して、リソースに追加する各タグのタグキーkeyとオプションのタグ値valueを指定します。Create オペレーションやコマンドの場合と同様に、tags パラメータはタグキーとそれに関連するタグ値の文字列間マップを指定します。

例えば、以下の AWS CLI コマンドは、Stack タグキーに指定されたジョブへの Production タグ値を追加します。この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行継続文字を使用しています。

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\"}
```

実行する条件は以下のとおりです。

- resource-arn はタグを追加するジョブの ARN を指定します。
- *Stack* はジョブに追加するタグのタグキーです。
- *Production* は指定されたタグキー*Stack*のタグ値です。

次の例では、コマンドはジョブに複数のタグを追加します。

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\",\"CostCenter\":\"12345\",\"Owner\":\"jane-doe\"}
```

tags マップ内の各タグには、key と value の引数の両方が必要です。ただし、value 引数の値は空の文字列とすることができます。タグ値をタグキーに関連付けない場合、value 引数の値

を指定しないでください。例えば、次の AWS CLI コマンドは、タグ値が関連付けられていない Owner タグキーを追加します。

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Owner\":\"\"}
```

タグ付けオペレーションが正常に実行されると、Macie は空の HTTP 204 レスポンスを返します。それ以外の場合、Macie は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

Amazon Macie リソースのタグを確認する

Amazon Macie コンソールまたは Amazon Macie API を使用して、Amazon Macie リソースのタグ (タグキーとタグ値の両方) を確認できます。これを複数の Macie リソースに同時に行いたい場合は、AWS Resource Groups コンソールのタグエディタを使用するか、AWS Resource Groups タグ付け APIのタグ付けオペレーションを使用します。

Console

Amazon Macie コンソールを使用してリソースのタグを確認するには、次のステップに従います。

リソースのタグを確認する

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. タグを確認するリソースのタイプに応じて、次のいずれかの操作を行います。
   - 許可リストについては、ナビゲーションペインで 許可リスト を選択します。

     次に、テーブル内のリストのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。
   - カスタムデータ識別子の場合は、ナビゲーションペインの カスタムデータ識別子 を選択します。

     次に、テーブル内のカスタムデータ識別子のチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。

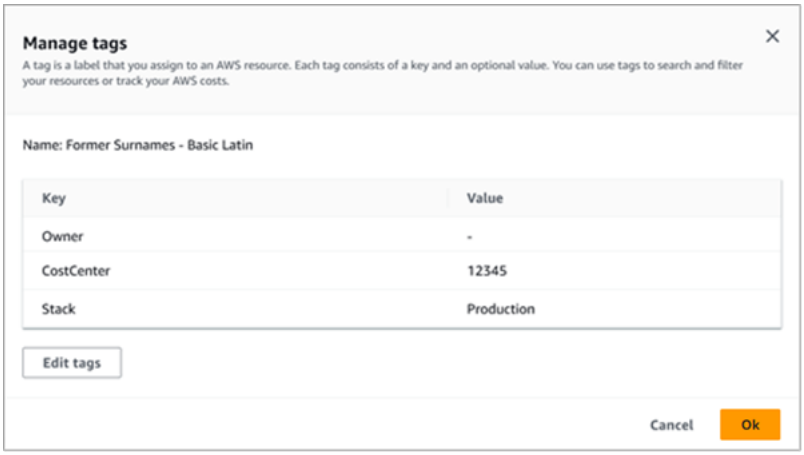
- フィルタまたは抑制ルールについては、ナビゲーションペインで 検出結果 を選択します。

  次に、保存されたルール リストで、ルールの横にある編集アイコン を選択します。次に、タグを管理 を選択します。
- 組織のメンバーアカウントについては、ナビゲーションペインで アカウント を選択します。

  次に、テーブル内のアカウントのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。
- 機密データ検出ジョブについては、ナビゲーションペインで ジョブ を選択します。

  次に、テーブル内のジョブのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。

タグを管理 ウィンドウには、現在リソースに割り当てられているタグがすべて一覧表示されます。例えば、次の図は、カスタムデータ識別子に割り当てられるタグを示しています。



この例では 3 つのタグがカスタムデータ識別子に割り当てられています。タグ値が関連付けられていない オーナー タグキー、関連付けられたタグ値が 12345 の CostCenter タグキー、関連付けられたタグ値が Production の Stack タグキーの 3 つです。

3. タグの確認を完了したら、キャンセル を選択してウィンドウを閉じます。

API

既存のリソースのタグをプログラムで取得、確認するには、タグを確認したいリソースのタイプに適切な Get または Describe オペレーションを使用します。例えば、GetCustomDataIdentifierオペレーションを使用するか、AWS Command Line InterfaceAWS CLIからget-custom-data-identifierコマンドを実行する場合、レスポンスには tags オブジェクトが含まれます。このオブジェクトには、現在リソースに割り当てられているすべてのタグ (タグキーとタグ値の両方) が一覧表示されます。

また、Amazon Macie API のListInvitationsオペレーションを使用することもできます。リクエストでは、resourceArn パラメータを使用して、リソースの Amazon リソースネーム (ARN) を指定します。AWS CLI を使用している場合は、list-tags-for-resourceコマンドを実行し、resource-arn パラメータを使用してリソースの ARN を指定します。例:

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

前の例では、*arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample* は既存の機密データ検出ジョブの ARN です。

オペレーションが正常に実行されると、Macie は現在リソースに割り当てられているすべてのタグ (タグキーとタグ値の両方) を一覧表示する tags オブジェクトを返します。例:

```
{
    "tags": {
        "Stack": "Production",
        "CostCenter": "12345",
        "Owner": ""
    }
}
```

ここで Stack、CostCenter、Owner はリソースに割り当てられるタグキーです。Production は Stack タグキーに関連付けられているタグ値です。12345 は、CostCenter タグキーに関連付けられているタグ値です。Owner タグキーには、関連するタグ値はありません。

タグの付いたすべての Macie リソースと、それらのリソースのそれぞれに関連付けられたすべてのタグのリストを取得するには、AWS Resource Groups タグ付け API の GetResources オペレーションを使用します。リクエストでは、ResourceTypeFilters パラメータの値を macie2 に設定します。AWS CLI を使用してこれを行うには、get-resourcesコマンドを実行し、resource-type-filters パラメータの値を macie2 に設定します。例:

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

オペレーションが正常に実行されると、リソースグループは、タグを持つすべての Macie リソースの ARN と、それらの各リソースに割り当てられているタグキーと値を含む `ResourceTagMappingList` 配列を返します。

Amazon Macie リソースのタグを編集する

Amazon Macie リソースのタグ (タグキーまたはタグ値) を編集するには、Amazon Macie コンソールまたは Amazon Macie API を使用します。これを複数の Macie リソースに同時に行うには、AWS Resource Groups コンソールのタグエディタを使用するか、AWS Resource Groups タグ付け APIのタグ付けオペレーションを使用します。

> **Important**
>
> リソースのタグを編集すると、リソースへのアクセスに影響を与える可能性があります。タグの名前 (キー) や値を編集する前に、タグを使用してリソースへのアクセスを制御する可能性のある AWS Identity and Access Management IAM ポリシーがあれば、必ず確認してください。

Console

Amazon Macie コンソールを使用してリソースのタグを編集するには、次のステップに従います。

リソースのタグを編集する

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. タグを編集するリソースのタイプに応じて、次のいずれかの操作を行います。
   - 許可リストについては、ナビゲーションペインで 許可リスト を選択します。

     次に、テーブル内のリストのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。
   - カスタムデータ識別子の場合は、ナビゲーションペインの カスタムデータ識別子 を選択します。

次に、テーブル内のカスタムデータ識別子のチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。

- フィルタまたは抑制ルールについては、ナビゲーションペインで 検出結果 を選択します。

  次に、保存されたルール リストで、ルールの横にある編集アイコン を選択します。次に、タグを管理 を選択します。

- 組織のメンバーアカウントについては、ナビゲーションペインで アカウント を選択します。

  次に、テーブル内のアカウントのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。

- 機密データ検出ジョブについては、ナビゲーションペインで ジョブ を選択します。

  次に、テーブル内のジョブのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。

タグを管理 ウィンドウには、現在リソースに割り当てられているタグがすべて一覧表示されます。

3. タグを管理 ウィンドウで タグの編集 を選択します。
4. 次のいずれかを実行します。

   - タグキーにタグ値を追加するには、タグキーの横にある 値 ボックスに値を入力します。
   - 既存のタグキーを変更するには、タグの横にある 削除 を選択します。次に、タグを追加 を選択します。表示される キー ボックスに、その新しいタグキーを入力します。値 ボックスに、必要に応じて関連するタグ値を入力します。
   - 既存のタグ値を変更するには、その値を含む 値 ボックスで X を選択します。次に、値 ボックスにその新しいタグの値を入力します。
   - 既存のタグ値を削除するには、その値を含む 値 ボックスで X を選択します。
   - 既存のタグ (タグキーとタグ値の両方) を削除するには、タグの横の 削除 を選択します。

   リソースには、最大 50 個のタグを含めることができます。タグキーには最大 128 文字を含めることができます。タグ値は最大 256 文字を含めることができます。文字には、文字、数字、スペース、または記号 (_ . : / = + - @) を使用できます。

5. タグの編集を完了したら、保存 を選択します。

API

リソースのタグをプログラムで編集すると、既存のタグが新しい値に上書きされます。したがって、タグを編集する最適な方法は、タグキー、タグ値、またはその両方を編集するかどうかによって異なります。タグキーを編集するには、現在のタグを削除して新しいタグを追加します。

タグキーに関連付けられているタグ値のみを編集または削除するには、Amazon Macie API の TagResourceオペレーションを使用するか、AWS Command Line InterfaceAWS CLIを使用している場合はtag-resourceコマンドを実行して、既存の値を上書きします。リクエストでは、タグ値を編集または削除するリソースの Amazon リソースネーム (ARN) を指定します。

タグキーのタグ値を編集するには、tags パラメータを使用してタグ値を変更するタグキーを指定し、そのキーに新しいタグ値を指定します。例えば、次のコマンドは、特定の機密データ検出ジョブに関連付けられている Production タグキーのタグ値を Staging から Stack に変更します。この例は Microsoft Windows 用にフォーマットされており、読みやすさを向上させるためにキャレット (^) の行継続文字を使用しています。

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Staging\"}
```

実行する条件は以下のとおりです。

- resource-arn はジョブの ARN を指定します。
- *Stack* は、変更するタグ値に関連付けられているタグキーです。
- *Staging* は、指定したタグキー*Stack*に使用する新しいタグ値です。

タグキーからタグ値を削除するには、value 引数の値を tags パラメータで指定しないでください。例:

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"\"}
```

オペレーションが正常に実行されると、Macie は空の HTTP 204 レスポンスを返します。それ以外の場合、Macie は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

Amazon Macie リソースからタグを削除する

Amazon Macie リソースからタグを削除するには、Amazon Macie コンソールまたは Amazon Macie API を使用します。これを複数の Macie リソースに同時に行うには、AWS Resource Groups コンソールのタグエディタを使用するか、AWS Resource Groups タグ付け APIのタグ付けオペレーションを使用します。

> **Important**
>
> リソースからタグを削除すると、リソースへのアクセスに影響を与える可能性があります。タグを削除する前に、タグを使用してリソースへのアクセスを制御する可能性のある AWS Identity and Access Management IAM ポリシーがあれば、必ず確認してください。

Console

Amazon Macie コンソールを使用して、リソースから 1 つ以上のタグを削除するには、次のステップに従います。

リソースからタグを削除する

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. タグを削除するリソースのタイプに応じて、以下のいずれかを実行します。
   - 許可リストについては、ナビゲーションペインで 許可リスト を選択します。

     次に、テーブル内のリストのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。
   - カスタムデータ識別子の場合は、ナビゲーションペインの カスタムデータ識別子 を選択します。

     次に、テーブル内のカスタムデータ識別子のチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。

- フィルタまたは抑制ルールについては、ナビゲーションペインで 検出結果 を選択します。

  次に、保存されたルール リストで、ルールの横にある編集アイコン を選択します。次に、タグを管理 を選択します。
- 組織のメンバーアカウントについては、ナビゲーションペインで アカウント を選択します。

  次に、テーブル内のアカウントのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。
- 機密データ検出ジョブについては、ナビゲーションペインで ジョブ を選択します。

  次に、テーブル内のジョブのチェックボックスをオンにします。次に、アクション メニューで タグを管理 を選択します。

タグを管理 ウィンドウには、現在リソースに割り当てられているタグがすべて一覧表示されます。

3. タグを管理 ウィンドウで タグの編集 を選択します。
4. 次のいずれかを実行します。
   - タグに対しタグ値のみを削除するには、削除する値を含む 値 ボックスで X を選択します。
   - タグのタグキーとタグ値の両方を (ペアで) 削除するには、削除するタグの横にある 削除 を選択します。
5. (オプショナル) リソースからさらにタグを削除する場合は、削除する追加タグのそれぞれに対し前の手順を繰り返します。
6. タグの削除を完了したら、保存 を選択します。

API

リソースから 1 つ以上のタグをプログラムで削除するには、Amazon Macie API のUntagResourceオペレーションを使用します。リクエストでは、`resourceArn` パラメータを使用して、タグを削除するリソースの Amazon リソースネーム (ARN) を指定します。`tagKeys` パラメータを使用して、削除するタグのタグキーを指定します。リソースから特定のタグ値 (タグキーではない) のみを削除するには、タグを削除する代わりにタグを編集します。

AWS Command Line InterfaceAWS CLIを使用している場合は、untag-resourceコマンドを実行し、resource-arn パラメータを使用してタグを削除するリソースの ARN を指定します。tag-keys パラメータを使用して、削除するタグのタグキーを指定します。例えば、次のコマンドは、指定した機密データ検出ジョブから Stack タグ (タグキーとタグ値の両方) を削除します。

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack
```

ここで resource-arn はタグを削除するジョブの ARN を指定し、*Stack* は削除するタグのタグキーです。

リソースから複数のタグを削除するには、さらなるタグキーをそれぞれ tag-keys パラメータの引数として追加します。例:

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack Owner
```

ここで resource-arn はタグを削除するジョブの ARN を指定し、*Stack* と *Owner* は削除するタグのタグキーです。

オペレーションが正常に実行されると、Macie は空の HTTP 204 レスポンスを返します。それ以外の場合、Macie は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

AWS CloudFormation で Amazon Macie リソースを作成

Amazon Macie は AWS CloudFormation と統合し、リソースやインフラストラクチャの作成や管理に費やす時間を短縮できるよう、お客様の AWS リソースのモデル化と設定を支援するサービスです。必要なすべての AWS リソース (カスタムデータ識別子など) を記述するテンプレートを作成すれば、AWS CloudFormation がお客様に代わってこれらのリソースのプロビジョニングや設定を処理します。

AWS CloudFormation を使用すると、テンプレートを再利用して Macie リソースをいつでも繰り返しセットアップできます。リソースを一度記述するだけで、同じリソースを複数の AWS アカウントと AWS リージョン で何度でもプロビジョニングできます。

トピック

- Amazon Macie と AWS CloudFormation テンプレート
- AWS CloudFormation の詳細情報

Amazon Macie と AWS CloudFormation テンプレート

Amazon Macie および関連サービスのリソースをプロビジョニングして設定するには、AWS CloudFormation テンプレートを理解しておく必要があります。テンプレートは、JSON または YAML 形式のテキストファイルです。これらのテンプレートには、AWS CloudFormation スタックにプロビジョニングしたいリソースを記述します。

JSON や YAML に詳しくない場合、グラフィックツールである AWS CloudFormation デザイナーを使用すると、AWS CloudFormation テンプレートを作成、変更できます。デザイナーを使用すると、ドラッグアンドドロップインターフェースによりテンプレートリソースを図示し、統合された JSON や YAML エディタ を使用して詳細を編集できます。詳細については、AWS CloudFormation ユーザーガイドのAWS CloudFormation Designer とはを参照してください。

以下のタイプの Macie リソースの AWS CloudFormation テンプレートを作成できます。

- 許可リスト
- カスタムデータ識別子
- 検出結果に関するフィルタールールと抑制ルール検出結果フィルターとも呼ばれています。

これらのタイプのリソース用 JSON テンプレートと YAML テンプレート例を含む詳細については、AWS CloudFormation ユーザーガイドのAmazon Macie リソースタイプのリファレンスを参照してください。

AWS CloudFormation の詳細情報

AWS CloudFormation の詳細については、以下のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- AWS CloudFormation API リファレンス
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

Amazon Macie を停止または無効化する

Amazon Macie コンソールまたは Amazon Macie API を使用して、特定の AWS リージョン で Amazon Macie を停止または無効化できます。Macie は、そのリージョン内のアカウントのすべてのアクティビティの実行を停止します。Macie が停止または無効化されている間は、リージョンでの Macieの使用に対して課金されません。

Macie を停止または無効化すると、後で再度有効化することができます。

トピック

Amazon メイシーを一時停止

Amazon メイシーを一時停止と、Macie は該当する AWS リージョン 内のアカウントのセッション識別子、設定、およびリソースを保持します。たとえば、既存の調査結果はそのまま残り、最大 90 日間保持されます。ただし、メイシーを一時停止と、Macie は現在の該当するリージョン内のアカウントですべてのアクティビティの実行を停止します。これには、Amazon Simple Storage Service (Amazon S3) データのモニタリング、機密データ自動検出の実行、進行中の機密データ検出ジョブの実行が含まれます。また Macie は、リージョン内の機密データ検出ジョブをすべてキャンセルします。

Macie を停止した後、再度有効化することができます。その場合、該当するリージョン内のすべての設定とリソースへのアクセスを回復し、Macie はそのリージョン内のアカウントのアクティビティを再開します。たとえば、アカウントの S3 バケットインベントリの更新が再開され、セキュリティとアクセスコントロールについてバケットのモニタリングが再開されます。これには、機密データ検出ジョブの再開または再起動は含まれません。機密データ検出ジョブは、キャンセル後に再開または再起動できません。

このトピックでは、Amazon Macie コンソールを使用して メイシーを一時停止方法について説明します。プログラムでこの操作を行う場合は、Amazon Macie API の UpdateMacieSession オペレーションを使用できます。

> **Note**
>
> ユーザーが組織の Macie 管理者である場合は、アカウントの メイシーを一時停止前に、アカウントに関連付けられているすべてのメンバーアカウントを削除する必要があります。詳細については、複数のアカウントの管理を参照してください。

メイシーを一時停止には

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、メイシーを一時停止リージョンを選択します。
3. ナビゲーションペインで 設定 を選択します。
4. メイシーを一時停止 を選択します。
5. 確認を求められたら、**Suspend**と入力し、Suspend (停止) を選択します。

追加のリージョンで メイシーを一時停止には、追加のリージョンごとに前のステップを繰り返します。

Amazon Macie を無効化する

Amazon Macie を無効化すると、Macie は該当する AWS リージョン 内のアカウントのすべてのアクティビティの実行を停止します。これには、Amazon Simple Storage Service (Amazon S3) データのモニタリング、機密データ自動検出の実行、進行中の機密データ検出ジョブの実行が含まれます。また、Macie は、調査結果や機密データ検出ジョブを含め、該当するリージョン内のアカウントに保存または維持している既存の設定とリソースをすべて削除します。他の AWS のサービス に保存または出力したデータはそのまま残り、例えば、Amazon S3 での機密データ検出結果や、Amazon EventBridge での検出結果イベントは影響を受けません。

> **Warning**
>
> Macie を無効化すると、既存の調査結果、機密データ検出ジョブ、カスタムデータ識別子、および該当するリージョン内のアカウントに保存または維持しているその他のリソースもすべて完全に削除されます。これらのリソースは、削除後は復元できません。リソースを保持し、Macie の使用のみを一時停止するには、Macie を無効化するのではなく、停止します。

このトピックでは、Amazon Macie コンソールを使用して Macie を無効化する方法について説明します。プログラムでこの操作を行う場合は、Amazon Macie API のDisableMacieオペレーションを使用します。

> **Note**
>
> ユーザーのアカウントが複数の Macie アカウントを集中管理する組織の一部である場合は、Macie を無効化する前に、次の操作を実行する必要があります。
>
> - ユーザーのアカウントが Macie メンバーアカウントである場合は、Macie 管理者に連絡して、メンバーアカウントとしての自身のアカウントを削除します。
> - ユーザーのアカウントが Macie 管理者アカウントである場合は、アカウントに関連付けられているすべてのメンバーアカウントを削除し、自身のアカウントとメンバーアカウント間の関連付けを削除します。
>
> 上記タスクの完了方法は、お使いの Macie アカウントが他のアカウントと AWS Organizations を介しているか、あるいは招待によって関連付けられているかによって異なります。詳細については、複数のアカウントの管理を参照してください。

Macie を無効化するには

1. Amazon Macie コンソール (https://console.aws.amazon.com/macie/) を開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、Macie を無効化するリージョンを選択します。
3. ナビゲーションペインで 設定 を選択します。
4. Disable Macie (Macie を無効化する) を選択します。
5. 確認を求められたら、**`Disable`**と入力し、Disable (無効化) を選択します。

追加のリージョンで Macie を無効化するには、追加のリージョンごとに前のステップを繰り返します。

Amazon Macie クォータ

AWS アカウント には、AWS のサービス ごとに特定のデフォルトのクォータ (以前は 制限 と呼ばれていました) があります。これらのクォータは、アカウントのサービスリソースまたはオペレーションの最大数です。このトピックでは、アカウントの Amazon Macie のリソースとオペレーションに適用されるクォータについて、リストを示して説明します。特に明記されていない限り、クォータはそれぞれの AWS リージョン のアカウントに適用されます。

クォータによっては、引き上げることができないものもあります。クォータの引き上げをリクエストするには、Service Quotas コンソール を使用します。クォータの引き上げをリクエストする方法についての説明は、Service Quotas ユーザーガイド のクォータ引き上げリクエストを参照してください。Service Quotas コンソールでクォータが使用できない場合は、AWS Support Center Console の サービス制限の引き上げフォーム を使用して、クォータの引き上げをリクエストします。

アカウント

- メンバーアカウント数 (招待による): 1,000
- メンバーアカウント数 (AWS Organizations を通じて): 10,000

結果

- アカウントあたりのフィルタールールと抑制ルールの数: 1,000
- 機密データ検出ジョブの実行あたりの検出結果:100,000 + 5% のしきい値の 100,000 + 5% のしきい値に達した後の検出結果

  このクォータは、Amazon Macie コンソールと Amazon Macie API にのみ適用されます。Macie が Amazon EventBridge に発行する検索イベントの数や、Macie がジョブの実行ごとに作成する機密データの検出結果の数にはクォータがありません。
- 機密データの調査結果あたりの検出場所の数: 15
- Amazon S3 オブジェクトからの機密データサンプルの取得と開示のリクエスト:1 日あたり 100 件

  このクォータは 24 時間ごとに 00:00:01 UTC+0 にリセットされます。
- 機密データサンプルを取得して公開する Amazon S3 オブジェクトのサイズ:
  - Apache Avro オブジェクトコンテナ (.avro) ファイル: 70 MB
  - Apache Parquet (.parquet) ファイル: 100 MB
  - CSV (.csv) ファイル:255 MB

- GNU Zip 圧縮アーカイブ (.gz または.gzip) ファイル: 90 MB
- JSON または JSON ライン (.json または.jsonl) ファイル:25 MB
- Microsoft Excel ワークブック (.xlsx) ファイル: 20 MB
- 非バイナリテキストtext/plainファイル: 100 MB
- TSV (.tsv) ファイル:75 MB
- ZIP 圧縮アーカイブ (.zip) ファイル: 355 MB

検索結果が対応する機密データ検出の結果用に複数の.gz ファイルを生成するアーカイブファイルに当てはまる場合、機密データのサンプルをアーカイブファイルから取得したり、公開したりすることはできません。

機密データ検出

- 機密データ検出ジョブによるアカウントあたりの毎月の分析: 5 TB

  このクォータは機密データ検出ジョブにのみ適用されます。クォータを最大 1,000 TB (1 PB) まで引き上げるには、Service Quotas コンソール を使用して、引き上げをリクエストします。1PB以上の増額をご希望の場合は、AWS Support Center Consoleのサービス限度額増額フォーム をご利用ください。
- アカウントあたりのカスタムデータ識別子: 10,000
- アカウントあたりの許可リスト:定義済みのテキストを指定する許可リストは 10 ~ 5 個、正規表現を指定する許可リストは 1 ~ 5 個、正規表現を指定する許可リストは 1 ~ 5 個

  定義済みのテキストを指定する許可リストには、追加のクォータが適用されます。リストには 100,000 件を超えるエントリを含めることはできず、リストのストレージサイズは 35 MB を超えることはできません。
- 機密データ自動検出から除外する S3 バケット数:1,000

  ユーザーが組織の Macie 管理者アカウントである場合、このクォータは組織全体に適用されます。
- 機密データ検出ジョブあたりの S3 バケット: 1,000

  このクォータは、分析するバケットを判断するためにランタイムバケット基準を使用するジョブには適用されません。これは、選択した特定のバケットを分析するようにジョブを設定した場合にのみ、ジョブに適用されます。ユーザーのアカウントが組織の Macie 管理者アカウントである

場合、組織内の最大 1,000 個のアカウントで設定される、最大 1,000 個のバケットを選択できます。

- 機密データ検出ジョブあたりのカスタムデータ識別子の数: 30
- 機密データ検出ジョブ 1 件あたりの許可リスト:定義済みのテキストを指定する許可リストは 10 ~ 5 個、正規表現を指定する許可リストは 1 ~ 5 個、正規表現を指定する許可リストは 1 ~ 5 個
- 分類ジョブの作成オペレーション:1 秒あたり 0.1 リクエスト
- 個々のファイルの分析に要する時間:10 時間
- 分析する個別のファイルのサイズ:
  - Adobe Portable Document Format (.pdf) ファイル: 1,024 MB
  - Apache Avro オブジェクトコンテナ (.avro) ファイル: 8 GB
  - Apache Parquet (.parquet) ファイル: 8 GB
  - メールメッセージ (.eml) ファイル:20 GB
  - GNU Zip 圧縮アーカイブ (.gz または.gzip) ファイル: 8 GB
  - Microsoft Excel ワークブック (.xls または .xlsx) ファイル: 512 MB
  - Microsoft Wordドキュメント (.doc または .docx) ファイル: 512 MB
  - 非バイナリテキストファイル: 20 GB
  - TAR アーカイブ (.tar) アーカイブファイル: 20 GB
  - ZIP 圧縮アーカイブ (.zip) ファイル: 8 GB

  ファイルが該当するクォータより大きい場合、Macie はファイル内のデータを分析しません。
- 圧縮ファイルまたはアーカイブファイル内のデータの抽出と分析:
  - ストレージサイズ (圧縮): GNU Zip 圧縮アーカイブ (.gz または.gzip) ファイルまたは ZIP 圧縮アーカイブ (.zip) ファイルでは 8 GB、TAR アーカイブ (.tar) ファイルでは 20 GB
  - ネストされたアーカイブの深さ: 10 レベル
  - 抽出されたファイルの数: 1,000,000
  - 抽出されたバイト数:全体で 10 GB の非圧縮データ。サポートされているファイルタイプまたはストレージ形式を使用する抽出ファイルごとに 3 GB の非圧縮データ。

  圧縮ファイルまたはアーカイブファイルのメタデータが、ファイルが 10 以上のネストされたレベルを含むか、ストレージサイズまたは抽出されたバイトの適切なクォータを超えていることが示されている場合、Macie はファイル内のデータを抽出または分析しません。Macie が圧縮ファイルまたはアーカイブファイル内のデータの抽出と分析を開始し、その後そのファイルが 1,000,000 個を超えるファイルを含むか、抽出されたバイトのクォータを超えていると判断した場合、Macie は

ファイル内のデータの分析を停止し、処理されたデータのみについて機密データの調査結果と検出結果を作成します。

- 構造化データ内のネストされた要素の分析: ファイルあたり 256 レベル

  このクォータは、JSON (.json) および JSON Lines (.jsonl) ファイルにのみ適用されます。いずれかのタイプのファイルのネストされた深さがこのクォータを超える場合、Macie はファイル内のデータを分析しません。
- 機密データの検出結果あたりの検出場所の数: 機密データ検出タイプあたり 1,000
- フルネームの検出: アーカイブファイルを含め、ファイルあたり 1,000 個

  Macie がファイル内の最初の 1,000 個のフルネームの出現を検出すると、Macie はフルネームのカウントの増加と場所データのレポートを停止します。
- 郵送先住所検出: アーカイブファイルを含め、ファイルあたり 1,000 個。

  Macie がファイル内の最初の 1,000 個の郵送先住所の出現を検出すると、Macie は郵送先住所のカウントの増加と場所データのレポートを停止します。

Amazon Macie ユーザーガイドのドキュメント履歴

次のテーブルに、Amazon Macie の前回のリリース以後に行われたドキュメントの重要な変更を示します。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

ドキュメントの最終更新日： 2024 年 6 月 14 日

変更	説明	日付
新機能	ユーザーが組織の委任 Macie 管理者である場合、組織内の個々のアカウントの機密データ自動検出を有効または無効にできるようになりました。このオプションを追加することで、すべてのアカウントの自動検出を有効にする、特定のアカウントの自動検出を選択的に有効にする、特定の S3 バケットを除外するなど、いくつかの方法で分析の範囲を定義できるようになりました。	2024 年 6 月 14 日
新しい機能	AWS Security Hub は、Macie のステータスとアカウントの機密データ自動検出をチェックするセキュリティコントロールを提供するようになりました。これらのコントロールが有効になっている場合、Security Hub は定期的にセキュリティチェックを実行して、Macie が に対して有効になっているかどうか AWS アカウント（ Macie.1 コント	2024 年 2 月 20 日

	ロール)、および Macie アカウントに対して機密データの自動検出が有効になっているかどうか (Macie.2 コントロール) を判断します。	
新しい機能	Macie は、 (DSSE-KMS) による二層式サーバー側の暗号化を使用して暗号化された Amazon S3 オブジェクトを分析できるようになりました。 AWS KMS keys これらのオブジェクトは、Macie が機密データの自動検出を実行したとき、または機密データ検出ジョブを実行したときに分析の対象になりました。さらに、DSSE-KMS 暗号化を使用する S3 バケットとオブジェクトは、Macie が Amazon S3 データに関して提供する統計とメタデータに含まれるようになりました。	2024 年 1 月 17 日
新機能	Macie が検出結果で報告する機密データのサンプルを取得して公開することを選択した場合に、 AWS Identity and Access Management (IAM) ロールを引き受けるように Macie を設定できるようになりました。このサンプルは、Macie が見つけた機密データの性質を検証し、対象の Amazon S3 オブジェクトおよびバケットの調査をカスタマイズするのに役立ちます。	2023 年 11 月 16 日

新しい機能	Macie は、さらに 47 の国と地域の国際銀行口座番号 (IBAN) を検出するように設計されたマネージドデータ識別子を提供するようになりました。Macie を使用して、50 を超える国と地域の IBAN の発生を検出して報告できるようになりました。	2023 年 11 月 1 日
新しい機能	Macie は現在、Google Cloud API キー、Stripe API キー、Aadhaar 番号、永久口座番号（PAN）、インド向け運転免許証識別番号といった種類の機密データを検出するように設計されたマネージドデータ識別子を提供しています。	2023 年 9 月 25 日
新しい クォータ	検出結果によって報告された機密データの性質を検証しやすくするために、Amazon S3 オブジェクトから機密データサンプルを取得して公開するためのサイズクォータを増やしました。ストレージサイズが 10 MB を超える S3 オブジェクトからサンプルを取得して公開できるようになりました。新しいクォータのリストについては、Amazon Macie クォータを参照してください。	2023 年 9 月 7 日

リージョナルな可用性	Macie がイスラエル (テルアビブ) リージョンで使用可能になりました。Macieが利用可能な AWS リージョン の一覧については、AWS 全般のリファレンスのAmazon Comprehend エンドポイントとクォータを参照してください。	2023 年 8 月 28 日
更新された機能	機密データ自動検出のためのデフォルトマネージドデータ識別子の新しい動的なセットを実装しました。デフォルトセットには、機密データ自動検出に推奨されるマネージドデータ識別子が含まれています。一般的なカテゴリやタイプの機密データを検出すると同時に、機密データの自動検出結果を最適化するように設計されています。	2023 年 8 月 2 日
更新された機能	Macie が機密データ調査結果と機密データ検出結果で報告する機密データの出現箇所を特定しやすいように、`Record` オブジェクト内の JSON パス要素名の文字制限を 20 文字から 240 文字に変更しました。この変更は Apache Avro オブジェクトコンテナ、Apache Parquet ファイル、JSON ファイル、および JSON Lines ファイルの新しい機密データの検出結果に影響します。	2023 年 7 月 24 日

更新された機能	の組織の委任 Macie 管理者である場合は AWS Organizations、組織 内で最大 10,000 個のアカウントの Macie を管理できるようになりました。	2023 年 6 月 30 日
新機能	機密データ検出ジョブを作成および設定して、ジョブに推奨するマネージドデータ識別子のセットを自動的に使用できるようになりました。この推奨されるマネージドデータ識別子セットは、一般的なカテゴリやタイプの機密データを検出すると同時に、ジョブの結果を最適化するように設計されています。	2023 年 6 月 28 日
新しいポリシー	新しいAWS マネージドポリシー、AmazonMacieReadOnlyAccess ポリシーを追加しました。このポリシーは、IAM アイデンティティ（プリンシパル）に、そのアカウントのすべての Macie リソース、データ、および設定を取得することを許可する読み取り専用の権限を付与します。	2023 年 6 月 15 日

新機能	Amazon S3 データの機密データ自動検出カバレッジを評価およびモニタリングしやすくするために、Macie コンソールに リソースカバレッジ ページが追加されました。このページには、各バケットで最近発生した分析上の問題 (ある場合) のロールアップを含め、すべての S3 バケットのカバレッジ統計とデータが統合されて表示されます。問題が発生した場合、このページには修正ガイダンスも提供されます。	2023 年 5 月 15 日
新機能	Macie は と統合 AWS のサービス します。これは AWS User Notifications、 AWS の通知の中心的な場所として機能する新しい です AWS Management Console。を使用すると User Notifications、Macie がポリシーや機密データの検出結果用に公開する Amazon EventBridge イベントに関する通知を生成および送信するためのカスタムルールと配信チャネルを設定できます。	2023 年 5 月 5 日

更新された内容	Macie が提供する S3 バケットのデフォルトの暗号化設定に関する統計とメタデータの説明を更新しました。また、Policy:IAMUser/S3BucketEncryptionDisabled ポリシー検出結果の説明も更新しました。Amazon S3は、新規および既存のバケットに追加されるオブジェクトの暗号化の基本レベルとして、Amazon S3マネージドキー（SSE-S3）によるサーバー側暗号化を自動的に適用するようになりました。Amazon S3 のこの変更の詳細については、Amazon Simple Storage Service ユーザーガイドのS3 バケットのデフォルトのサーバー側の暗号化動作の設定を参照してください。	2023 年 2 月 27 日

新しい機能	Macie は S3 バケットについて追加タイプのポリシー検出結果を生成できるようになりました： `Policy:IAMUser/S3BucketSharedWithCloudFront` このタイプの検出結果は、バケットのポリシーが変更され、バケットを Amazon CloudFront オリジンアクセスアイデンティティ (OAI)、 CloudFront オリジンアクセスコントロール (OAC)、またはその両方と共有できるようにしたことを示します。さらに、CloudFront OAIs または OACs と共有されているバケットは、Macie が Amazon S3 データに関して提供する統計とメタデータで外部で共有されると見なされます。	2023 年 2 月 24 日

新しい機能	Macie は現在、機密データ検出用の Amazon S3 Glacier Instant Retrieval ストレージクラスをサポートしています。Macie が機密データ自動検出を実行したり、ユーザーが機密データ検出ジョブを実行したりすると、このストレージクラスを使用する S3 オブジェクトが分析の対象になります。また、Macie が提供する Amazon S3 データに関する統計やメタデータでも分類可能なオブジェクトと見なされます。	2022 年 12 月 21 日
新機能	アカウントまたは組織に対して、機密データの自動検出を実行するように Macie を設定できるようになりました。機密データ自動検出により、Macie は Amazon S3 データを継続的に評価し、サンプリング技術を使用して S3 バケット内の代表的なオブジェクトを特定、選択、分析し、オブジェクトに機密データがないか検査します。分析の結果は、Macie が提供する Amazon S3 データに関する統計、検出結果、およびその他の情報で評価できます。	2022 年 11 月 28 日

新機能	Macie で Amazon S3 オブジェクトの機密データを検査するときに無視させたいテキストとテキストパターンを許可リストを作成して使用することができるようになりました。許可リストを使用すると、特定のシナリオや環境に合わせて機密データの例外を定義できます。例えば、組織の公的担当者の名前、特定の電話番号、組織がテストに使用するサンプルデータなどです。	2022 年 8 月 30 日
新機能	Macie が S3 オブジェクト内で検出した機密データの性質を確認するために、Macie を設定して使用し、検出結果によって報告された機密データのサンプルを取得することができるようになりました。	2022 年 7 月 26 日
更新された機能	このAmazonMacieFullAccess ポリシーでは、Macie のサービスにリンクされたロールaws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie の Amazon リソースネーム (ARN) を更新しました。	2022 年 6 月 30 日

更新された機能	Macie サービスにリンクされたロールAWSServiceRoleForAmazonMacie にアタッチされているAmazonMacieServiceRolePolicy ポリシーを更新しました。このポリシーでは、Amazon Macie クラシックのアクションとリソースは指定されなくなりました。Amazon Macie クラシックは廃止され、現在は利用できなくなっています。	2022 年 5 月 20 日
新しい機能	Macie は、 に公開する機密データの調査結果に AWS Security HubOriginType フィールドを含めるようになりました。OriginType このフィールドには、Macie が検出結果を生成した機密データをどのように見つけたかを指定します。	2022 年 5 月 11 日
更新された内容	カスタムデータ識別子のキーワードと最大一致距離の設定がどのように動作するのかが明確になりました。	2022 年 4 月 22 日
新しい機能	Macie は、HTTP 基本認証ヘッダー、HTTP クッキー、JSON ウェブトークンを検出するように設計されたマネージドデータ識別子を提供するようになりました。	2022 年 4 月 21 日

新しいコンテンツ	Macie の主要な概念と条件の説明と定義を追加しました。	2022 年 3 月 16 日
新しい機能	機密データ検出ジョブを作成および設定するときに推定コストを計算して表示するために、Macie は AWS アカウント から の料金データを取得するようになりました AWS Billing and Cost Management。この機能をサポートするために、AmazonMacieFullAccess ポリシーに請求およびコスト管理アクションを追加しました。	2022 年 3 月 7 日
新しい機能	Macie は、 に発行する検出結果に AWS Security HubSampleフィールドを含めるようになりました。この Sample フィールドでは、検出結果が検出結果のサンプルであるかどうかを指定します。	2022 年 2 月 24 日
新しいコンテンツ	VPC と Macie とのプライベート接続を確立するため、Amazon Virtual Private Cloud の使用に関する情報が追加されました。	2022 年 1 月 19 日

新しい機能	Amazon Macie コンソールを使用して、カスタムデータ識別子のタグの割り当てと管理、検出結果のフィルタおよび抑制ルール、機密データ検出ジョブ、および組織の Macie 管理者の場合は組織内のメンバーアカウントが可能になりました。タグは、特定のタイプの AWS リソースをオプションで定義および割り当てるラベルです。	2022 年 1 月 12 日
新しいコンテンツ	Macie へのアクセスを管理するためのAWS Identity and Access Managementの使用に関する情報が追加されました。	2021 年 12 月 20 日
新しい特徴	カスタムデータ識別子を作成するときに、識別子が生成する機密データの調査結果の重要度設定を定義できるようになりました。これらの設定を使用すると、カスタムデータ識別子の検出基準に一致するテキストの出現回数に基づいて、調査結果に割り当てる重要度を指定できます。	2021 年 11 月 4 日

新しい機能	Macie が提供するさまざまなタイプの調査結果の詳細を知るには、調査結果サンプルを生成することができます。調査結果サンプルでは、データ例とプレースホルダー値を使用して、Macie がそれぞれのタイプの調査結果に含める可能性があるさまざまな種類の情報が示されます。	2021 年 10 月 28 日
新しい機能	Macie は、 に発行する検出結果に AWS Security Hub`OwnerAccountId` フィールドを含めるようになりました。このフィールドは、影響を受ける S3 バケットを所有 AWS アカウント する のアカウント ID を指定します。	2021 年 10 月 27 日
新しいコンテンツ	複数の Macie アカウントの集中管理に関する情報が追加されました。これは、Macie を と統合するか、Macie からメンバーシップの招待を送信 AWS Organizations することで、2 つの方法で行うことができます。	2021 年 10 月 13 日

新しい機能	バケットのアクセス許可設定により、Macie がバケットまたはバケットのオブジェクトについての情報を取得すること、およびバケットのデータのセキュリティとプライバシーを評価およびモニタリングすることを防ぐようにしたかどうかを、S3 バケットインベントリが示すようになりました。さらに、 AWS KMS keys およびカスタマーマネージドキーへの参照を更新し、現在の用語を反映しました。	2021 年 10 月 5 日
新しい機能	Macie は、ポリシーと機密データの調査結果を 30 日間ではなく 90 日間保存するようになりました。Macie が 2021 年 8 月 31 日以降に調査結果を作成または更新した場合は、Macie コンソールまたは Macie API を使用して最大 90 日間調査結果にアクセスできます。特定の では AWS リージョン、Macie は 2021 年 9 月 27 日に 90 日間の結果の保持を開始しました。	2021 年 10 月 1 日

新機能	機密データ検出ジョブを作成するときに、ジョブが S3 オブジェクトを分析するときにジョブでどのマネージドデータ識別子を使用するかを指定できるようになりました。この特徴により、特定のタイプの機密データに焦点を絞るようにジョブの分析を調整できます。	2021 年 9 月 17 日
新しい機能	機密データの調査結果が、JSON および JSON Lines ファイル内の機密データを見つけるのに役立つ追加情報を提供するようになりました。	2021 年 7 月 6 日
更新された機能	Macie は、 に発行する検出結果で AWS Security HubAwsS3Bucket リソースタイプを使用するようになりました。(Macie は以前にこの値を に設定しましたAWS::S3::Bucket 。) AwsS3Bucket は、 AWS Security Finding 形式 (ASFF) の S3 バケットに使用されるリソースタイプ値です。	2021 年 6 月 28 日

新機能	機密データ検出ジョブを作成するときに、ジョブが分析する S3 バケットを判断するランタイム基準を定義できるようになりました。この特徴により、ジョブの分析の範囲は、バケットインベントリへの変更に動的に適応できるようになります。	2021 年 5 月 15 日
新しい機能	S3 バケットインベントリと概要ダッシュボードは、バケットポリシーに新しいオブジェクトのサーバー側の暗号化が必要かどうかを示す暗号化メタデータと統計を提供するようになりました。さらに、バケットインベントリ内の個別のバケットに対して、オブジェクトメタデータのオンデマンド更新を実行できるようになりました。	2021 年 4 月 30 日
新機能	Amazon CloudWatch Logs を使用して、機密データ検出ジョブの実行時に発生するイベントをモニタリングおよび分析できるようになりました。この機能をサポートするために、Macie サービスにリンクされたロール の マネージドポリシーに CloudWatch Logs アクション AWS を追加しました。	2021 年 4 月 14 日

リージョナルな可用性	Macie が AWS アジアパシフィック (大阪) リージョンで利用可能になりました。	2021 年 4 月 5 日
新機能	機密データの調査結果を AWS Security Hubに発行するように Macie を設定できるようになりました。	2021 年 3 月 22 日
新しいコンテンツ	Macie のコストのモニタリングと予測および無料トライアルへの参加に関する情報が追加されました。	2021 年 2 月 26 日
更新された内容	マスターアカウントという用語を管理者アカウントという用語に置き換えました。管理者アカウントは、複数のアカウントを集中管理するために使用されます。	2021 年 2 月 12 日
新しい機能	機密データ検出ジョブの範囲を、カスタム include および exclude 基準で S3 オブジェクトプレフィックスを使用して絞り込むことができるようになりました。	2021 年 2 月 2 日
更新された内容	Macie は、ポリシーの調査結果を に公開するときに、Security Finding 形式 (ASFF) の検出結果タイプの分類に準拠するようになりました AWS Security Hub。 AWS	2021 年 1 月 28 日

新しいコンテンツ	Amazon S3 データのモニタリングおよびそのデータのセキュリティとプライバシーの評価に関する情報が追加されました	2021 年 1 月 8 日
リージョナルな可用性	Macie が AWS アフリカ (ケープタウン) リージョン、欧州 (ミラノ) AWS リージョン、AWS 中東 (バーレーン) リージョンで利用可能になりました。	2020 年 12 月 21 日
新しい機能	お客様のアカウントが Macie 管理者アカウントである場合、組織内の最大 1,000 個のアカウントで設定される、最大 1,000 個のバケットでデータを分析する機密データ検出ジョブを作成して実行できるようになりました。	2020 年 11 月 25 日
新しい機能	S3 バケットインベントリは、バケット内のデータを分析するために、1 回限りまたは定期的な機密データ検出ジョブを設定しているかどうかを示すようになりました 該当する場合は、最近実行されたジョブに関する詳細も表示されます。	2020 年 11 月 23 日
新しいコンテンツ	調査結果のフィルタリングに関する情報が追加されました。	2020 年 11 月 12 日

新しい機能	機密データの調査結果が、Apache Avro オブジェクトコンテナ、Apache Parquet ファイル、および Microsoft Excel ワークブック内の機密データを見つけるのに役立つ追加情報を提供するようになりました。	2020 年 11 月 9 日
新機能	機密データの調査結果を使用して、S3 オブジェクト内の機密データの個別の出現を見つけることができるようになりました。	2020 年 10 月 22 日
新機能	機密データ検出ジョブの一時停止と再開を行えるようになりました。	2020 年 10 月 16 日
新しいコンテンツ	ポリシーの調査結果と機密データの調査結果の重要度評価システムについての詳細が追加されました。	2020 年 10 月 6 日
新しい特徴	機密データ検出ジョブを実行するときに、Macie が個別の S3 バケットで分析できるデータの量を示す統計を表示できるようになりました。さらに、ジョブを作成するときに、ジョブの推定コストを表示できるようになりました。	2020 年 9 月 3 日
新しいコンテンツ	機密データ検出ジョブの設定、実行、および管理に関する情報が追加されました。	2020 年 8 月 31 日

新しい機能	マネージドデータ識別子は、ブラジルの特定のタイプの個人を特定できる情報を検出できるようになりました。	2020 年 7 月 31 日
更新された内容	カスタムデータ識別子内の正規表現でサポートされている構文に関する情報が追加されました。	2020 年 7 月 30 日
更新された内容	マネージドデータ識別子のキーワード要件が追加され、各機密データ検出ジョブが生成できる調査結果の数のクォータが増加されました。	2020 年 7 月 17 日
新しいコンテンツ	Amazon EventBridge および を使用して検出結果 AWS Security Hub のモニタリングと処理に関する情報を追加しました。 https://docs.aws.amazon.com/macie/latest/user/findings-monitor.htmlこれには、検出結果の EventBridge イベントスキーマと、ポリシーと機密データの検出結果のイベント例が含まれます。	2020年6月22日
新しいコンテンツ	調査結果の分析と抑制に関する情報が追加されました。	2020 年 6 月 17 日
新しいコンテンツ	詳細な検出結果を S3 バケットに保存するように Macie を設定するための手順が追加されました。	2020 年 6 月 2 日

新しいコンテンツ	Macie が検出できる機密データのタイプ、および Amazon S3 オブジェクト内の機密データを検出するための暗号化要件に関する情報が追加されました。	2020 年 5 月 28 日
一般提供	これは、Amazon Macie ユーザーガイドの初回一般リリースです。	2020 年 5 月 13 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。