



購入者ガイド

AWS Marketplace



AWS Marketplace: 購入者ガイド

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有しない他の商標はすべてそれぞれの所有者に帰属します。所有者は必ずしも Amazon との提携や関連があるわけではありません。また、Amazon の支援を受けているとはかぎりません。

Table of Contents

とは AWS Marketplace	1
の契約構造 AWS Marketplace	2
EULA の更新	3
AWS Marketplaceの標準契約	5
購入者 AWS Marketplace としての の使用	5
AWS Marketplace でのソフトウェアとサービス	6
AWS Marketplace と Amazon の違い DevPay	8
購入者としての開始方法	9
製品の購入	9
ソフトウェアの起動	10
チュートリアル: AMI ベースのソフトウェア製品の購入	11
ステップ 1: を作成する AWS アカウント	11
ステップ 2: ソフトウェアを選択する	11
ステップ 3: ソフトウェアを設定する	13
ステップ 4: Amazon EC2 でソフトウェアを起動する	14
ステップ 5: ソフトウェアを管理する	15
ステップ 6: インスタンスを終了する	15
詳細情報	16
サポートされるリージョン	17
[製品カテゴリ]	19
インフラストラクチャソフトウェア	19
DevOps	20
ビジネスアプリケーション	21
機械学習	22
IoT	23
プロフェッショナルサービス	24
デスクトップアプリケーション	24
データ製品	25
業界	26
製品のタイプ	27
AMI ベースの製品	27
AWS CloudFormation テンプレート	28
AMI サブスクリプション	29
契約料金による AMI 製品	32

計測対応 AMI 製品	37
AMI 製品のコスト配分タグ	37
AMI エイリアスを使用する	40
コンテナ製品	42
有料コンテナ製品の料金モデル	42
コンテナと Kubernetes の概要	43
コンテナ製品の検索とサブスクリプション	43
契約料金によるコンテナ製品	48
コンテナソフトウェアの起動	53
Machine Learning 製品	58
Amazon SageMaker モデルパッケージ	59
Amazon SageMaker アルゴリズム	60
検索、サブスクリプション、デプロイ	61
プロフェッショナルサービス製品	63
プロフェッショナルサービスの購入	64
SaaS 製品	64
料金モデル	65
クイック起動	68
データ製品	70
製品への支払い	71
発注書	72
AWS Marketplace のトランザクションに発注書を使用する	72
一括使用発注書を使用する	73
発注書に関するトラブルシューティング	74
返金に関する情報	76
製品のサブスクリプションをキャンセルする	77
SaaS サブスクリプションのキャンセル	77
機械学習のサブスクリプションをキャンセルする	77
AMI サブスクリプションのキャンセル	78
SaaS 契約サブスクリプションの自動更新をキャンセルする	79
支払い方法	79
支払いエラー	79
サポートされている通貨	79
指定通貨の変更	81
送金手順の更新	81
コスト配分タグ	83

ベンダー計測タグ	83
関連トピック	40
プライベートマーケットプレイス	85
製品の詳細ページの表示	86
プライベートマーケットプレイスの製品へのサブスクライブ	86
プライベートマーケットプレイスで製品をサブスクライブする	86
プライベートマーケットプレイスへの製品の追加をリクエストする	87
プライベートマーケットプレイスの作成と管理	87
プライベートマーケットプレイスの開始方法	87
プライベートマーケットプレイスの管理	88
プライベートマーケットプレイスエクスペリエンスの作成	90
プライベートマーケットプレイスエクスペリエンスへの製品の追加	90
プライベートマーケットプレイスエクスペリエンスでの製品の確認	91
プライベートマーケットプレイスエクスペリエンスのカスタマイズ	91
対象者の管理	92
プライベートマーケットプレイスの設定	92
プライベート製品の使用	93
ユーザーリクエストの管理	93
プライベートマーケットプレイスエクスペリエンスのアーカイブと再有効化	94
プライベートオファー	96
プライベートオファーに適した製品のタイプ	98
プライベートオファーの受け入れ準備	101
AWS Billing and Cost Management 設定の確認	101
支払い方法の確認	101
課税設定の確認	101
プライベートオファーの表示とサブスクライブ	102
プライベートオファーのリストからのプライベートオファーの表示とサブスクリプション	102
販売者が提供したリンクからプライベートオファーを表示してサブスクライブする	102
製品ページからのプライベートオファーの表示とサブスクリプション	103
プライベートオファーのトラブルシューティング	104
プライベートオファーを表示するために [オファー ID] をクリックすると、[ページが見つかりません] (404) エラーが表示されます。	104
どの提案でも機能しない場合	105
のプライベートオファーページ AWS Marketplace	105
プライベートオファーページについて理解する	105

プライベートオファーページの閲覧に必要なアクセス許可	106
SaaS プライベートオファーへのサブスクライブ	107
AMI プライベートオファーへのサブスクライブ	110
Flexible Payment Schedule で年間 AMI プライベートオファーをサブスクライブする	112
Flexible Payment Schedule なしで年間 AMI プライベートオファーをサブスクライブする	113
プライベートオファーの変更またはサブスクライブ解除	114
パブリックオファーからプライベートオファーへの料金設定の変更	115
SaaS 契約の変更 - アップグレードと更新	115
SaaS サブスクリプションから SaaS 契約に変更する	116
AMI 契約から新しい契約に変更する	116
時間単位の AMI から年単位の AMI に変更する	116
年単位の AMI から時間単位の AMI に変更する	116
将来の日付の契約の使用	117
将来の日付の契約の作成	118
将来の日付の契約での Flexible Payment Scheduler の使用	118
将来の日付の契約の修正	119
将来の日付の契約の通知を受け取る	119
組織内でのサブスクリプションの共有	120
ライセンス共有の前提条件	120
ライセンスの表示	121
ライセンスの共有	122
ライセンスの使用状況の追跡	122
通知	124
E メール通知	124
Amazon EventBridge 通知	124
AWS Marketplace Discovery API Amazon EventBridge イベント	125
調達システムの統合	127
調達統合の仕組み	127
調達システム統合の設定	129
IAM 許可の設定	130
Coupa と統合 AWS Marketplace するための の設定	130
SAP Ariba と統合 AWS Marketplace するための の設定	132
AWS Marketplaceが使用する UNSPSC コード	134
調達システムの統合の無効化	134
無料トライアル	135
ソフトウェアとインフラストラクチャの料金	135

AMI ベースの製品の無料トライアル	135
コンテナベースの製品の無料トライアル	136
機械学習製品の無料トライアル	136
SaaS 製品の無料トライアル	137
AWS Marketplace での AWS 無料利用枠の使用	138
AWS Service Catalog への AWS Marketplace のサブスクリプションの追加	139
製品レビュー	140
ガイドライン	140
制限事項	140
タイミングと心構え	141
サポート情報	142
AWS Marketplace Vendor Insights	143
購入者としての開始方法	144
AWS Marketplace Vendor Insights で製品を検索する	144
サブスクライブして、評価データへのアクセスをリクエストしてください。	145
評価データのサブスクリプションを解除する	145
製品のセキュリティプロファイルの表示	146
AWS Marketplace Vendor Insights のダッシュボード	146
SaaS 製品のセキュリティプロファイルを表示する	146
コントロールカテゴリを理解する	147
のスナップショットをエクスポートする	194
スナップショットをエクスポートする	144
.....	145
アクセスの制御	195
AWS Marketplace Vendor Insights 購入者のアクセス許可	196
GetProfileAccessTerms	196
ListEntitledSecurityProfiles	196
ListEntitledSecurityProfileSnapshots	196
GetEntitledSecurityProfileSnapshot	197
のセキュリティ AWS Marketplace	198
販売者と共有されるサブスクライバー情報	198
IAM ポリシーを IPv6 にアップグレードする	198
IPv4 から IPv6 に移行する際、影響を受けるお客様	199
IPv6 とは	199
IPv6 用の IAM ポリシーを更新する	199
IPv4 から IPv6 に更新した後のネットワークのテスト	201

AWS Marketplace サブスクリプションへのアクセスのコントロール	202
AWS Marketplace アクセスの IAM ロールの作成	203
AWS の マネージドポリシー AWS Marketplace	204
License Manager で使用するアクセス許可	204
追加リソース	205
AWS マネージドポリシー	205
AWSMarketplaceDeploymentServiceRolePolicy	206
AWSMarketplaceFullAccess	206
AWSMarketplaceLicenseManagementServiceRolePolicy	210
AWSMarketplaceManageSubscriptions	211
AWSMarketplaceProcurementSystemAdminFullAccess	212
AWSMarketplaceReadのみ	212
AWSPrivateMarketplaceAdminFullAccess	214
AWSPrivateMarketplaceRequests	215
AWS マネージドポリシー: AWSServiceRoleForPrivateMarketplaceAdminPolicy	216
AWSVendorInsightsAssessorFullAccess	216
AWSVendorInsightsAssessorReadOnly	217
AWS マネージドポリシーに関するAWS Marketplace の更新	218
カスタマーサポートの AWS アカウント 電話番号の検索	221
サービスリンクロールの使用	221
使用権限を共有するロール	222
発注書のロール	225
AWS Marketplace 製品を設定および起動するためのロール	228
Private Marketplace を設定するためのロール	232
プライベートマーケットプレイスの管理者の作成	236
プライベートマーケットプレイス管理者向けのカスタムポリシーの作成	237
ドキュメント履歴	241
AWS 用語集	253
.....	ccliv

とは AWS Marketplace

AWS Marketplace は、ソリューションの構築とビジネスの実行に必要なサードパーティーのソフトウェア、データ、サービスを検索、購入、デプロイ、管理するために使用できる厳選されたデジタルカタログです。には、セキュリティ、ネットワーク、ストレージ、機械学習、IoT、ビジネスインテリジェンス、データベース、などの一般的なカテゴリからの数千のソフトウェアリスト AWS Marketplace が含まれています DevOps。 AWS Marketplace また、柔軟な料金オプションと複数のデプロイ方法を使用して、ソフトウェアのライセンスと調達を簡素化します。さらに、AWS Data Exchange から利用可能なデータ製品 AWS Marketplace も含まれます。

数回クリックするだけで事前設定されたソフトウェアをすばやく起動し、ソフトウェアソリューションを Amazon マシンイメージ (AMI) 形式、SaaS (Software-as-a-Service) 形式、その他の形式で選択できます。さらに、データ製品を参照してサブスクライブすることもできます。柔軟な料金オプションには、無料トライアル、時間単位、月単位、年単位、複数年、Bring-Your-Own-License (BYOL) モデルなどがあります。これらの料金オプションはすべて 1 つの source. AWS handles から請求され、請求には料金が表示されます AWS 。

購入者 (サブスクライバー) AWS Marketplace または販売者 (プロバイダー) として、あるいはその両方として 使用できます。を持つユーザーは誰でもコンシューマー AWS Marketplace として AWS アカウント を使用し、 を販売者に登録できます。販売者は、独立系ソフトウェアベンダー (ISV)、付加価値リセラー、または AWS 製品やサービスと連携する何かを提供する個人です。

Note

データ製品プロバイダーは、AWS Data Exchange の資格要件を満たす必要があります。詳細については、「AWS Data Exchange ユーザーガイド」の「[AWS Data Exchange でのデータ製品の提供](#)」を参照してください。

のすべてのソフトウェア製品はキュレーションプロセスを経て AWS Marketplace います。製品ページで、製品に対して 1 つ以上のサービスがあります。販売者が で製品を送信すると AWS Marketplace、製品の価格と利用規約が定義されます。購入者は、価格設定およびオファーに設定された利用規約に同意します。

では AWS Marketplace、製品は無料で使用でき、関連する料金が発生する可能性があります。料金は AWS 請求書の一部となり、支払い後に が販売者に AWS Marketplace 支払います。

Note

米国以外の販売者から購入した場合は、販売者から税金請求書も送信される場合があります。詳細については、「[アマゾン ウェブ サービス 税務ヘルプ](#)」の「[AWS Marketplace 出品者](#)」を参照してください。

製品はたくさんの形式を持つことができます。例えば、製品は、AWS アカウントを使用してインスタンス化された Amazon マシンイメージ (AMI) として提供できます。また、コンシューマーへの配信に AWS CloudFormation テンプレートを使用するように製品を設定することもできます。製品は、ISV の SaaS (Software-as-a-Service) サービス、ウェブ ACL、ルールセット、または AWS WAF の条件である場合もあります。

ソフトウェア製品は、ISV の標準エンドユーザー使用許諾契約 (EULA) に基づく出品料金で購入したり、カスタムの料金と EULA に基づくプライベートオファーで購入したりできます。また、期間や使用の範囲が指定された[標準契約](#)に基づいて製品を購入することもできます。

製品のサブスクリプションが完了したら、AWS Service Catalog を使用して製品をコピーし、組織内で製品がどのようにアクセスおよび使用されるかを管理できます。詳細については、「AWS Service Catalog 管理者ガイド」の「[ポートフォリオへの AWS Marketplace 製品の追加](#)」を参照してください。

の契約構造 AWS Marketplace

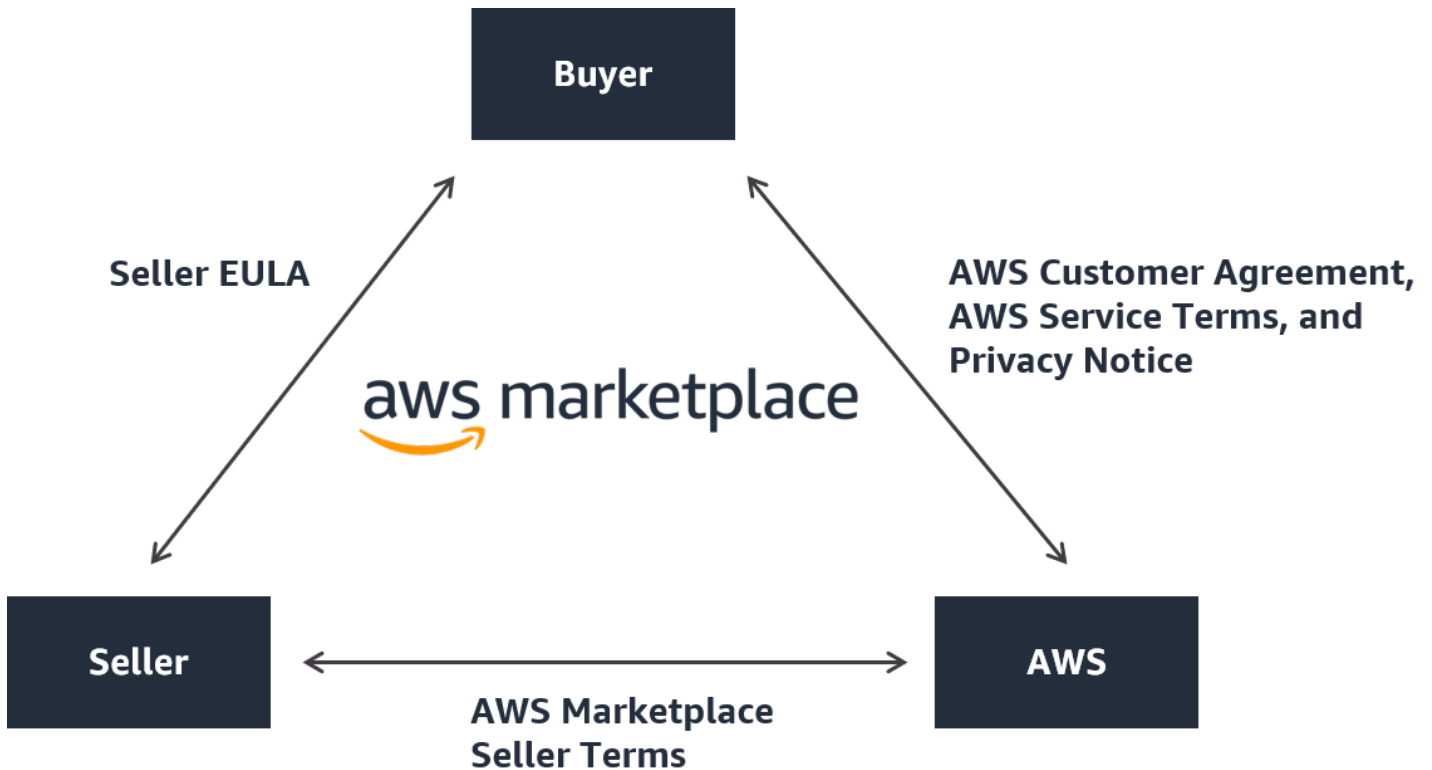
で販売されるソフトウェア、サービス、およびデータ製品の使用は、購入者と販売者の間の契約 AWS Marketplace に準拠します。AWS は、これらの契約の当事者ではありません。

購入者としての の使用 AWS Marketplace には、[AWS サービス条件](#)、[AWS カスタマーアグリーメント](#)、および[プライバシー通知](#)が適用されます。

販売者契約には以下が含まれます。

- 販売者の EULA は、AWS Marketplace に公開されているソフトウェアリストの製品リストページに記載されています。多くの販売者は、[AWS Marketplace 標準契約 \(SCMP\)](#) をデフォルトの EULA として使用しています。SCMP をプライベートオファーの交渉のベースとして使用したり、修正テンプレートを使用して SCMP を変更したりすることもできます。プライベートオファーには、当事者間で交渉したカスタム契約条件を含めることもできます。
- [AWS Marketplace での販売者のアクティビティ](#)には、[AWS Marketplace 販売者規約](#)が適用されます。

次の図は、の契約構造を示しています AWS Marketplace。



EULA の更新

販売者は、それぞれの製品の EULA を更新できます。更新の発効日は、EULA、オファータイプ、および料金モデルによって異なります。

次の表は、新しい EULA が有効になる時期に関する情報を示しています。

Note

お客様と販売者がカスタム契約を結んでいる場合、以下は適用されない場合があります。

オファーのタイプ	料金モデル	更新時に EULA が有効になります
Public	使用方法	サブスクリプションをキャンセルし、再サブスクライブを行います。

オファ어의タイプ	料金モデル	更新時に EULA が有効になります
Public	Contract	現在の契約は終了し、新しいパブリックオファー契約に更新されます。
Public	消費量での契約	現在の契約は終了し、新しいパブリックオファー契約に更新されます。
プライベート	使用方法	現在のプライベートオファーは期限切れになり、新しいパブリックオファー契約に自動更新されます。プライベートオファーの更新は、特定のプライベートオファーによって異なります。
プライベート	Contract	現在のプライベートオファーの有効期限が切れ、パブリックオファーまたは新しいプライベートオファーに再サブスクライブします。プライベートオファーの更新は、特定のプライベートオファーによって異なります。
プライベート	消費量での契約	現在のプライベートオファーの有効期限が切れ、パブリックオファーまたは新しいプライベートオファーに再サブスクライブします。プライベートオファーの更新は、特定のプライベートオファーによって異なります。

AWS Marketplaceの標準契約

製品を購入する準備をするときは、関連する EULA または標準化された契約を確認してください。多くの販売者は、出品時に同じ標準化された契約である「[標準契約 AWS Marketplace \(SCMP\)](#)」を提供しています。は、購入者および販売者コミュニティと協力して SCMP AWS Marketplace を開発し、デジタルソリューションの使用を管理し、購入者および販売者の義務を定義しました。デジタルソリューションの例としては、サーバーソフトウェア、Software as a Service (SaaS)、人工知能と機械学習 (AI/ML) アルゴリズムなどがあります。

購入ごとにカスタム EULA を確認する代わりに、SCMP を一度確認するだけで済みます。[契約条件](#)は、SCMP を使用するすべての製品に共通です。

販売者は、SCMP に付随する以下の補遺を使用することもできます。

- [セキュリティ強化補遺](#) - データセキュリティ要件が厳しい取引をサポートします。
- [HIPAA ビジネスアソシエイト補遺](#) - HIPAA (Health Insurance Portability and Accountability Act of 1996: 医療保険の携行性と責任に関する法律) に準拠している取引をサポートします。

標準化されたライセンス条項を提供している出品を検索するには、製品の検索時に [標準契約] フィルターを使用します。プライベートオファナーの場合は、販売者に EULA を SCMP に置き換え、取引固有の要件に対応するために必要に応じて合意された修正を適用できるかどうかを問い合わせてください。

詳細については、「[の標準化契約 AWS Marketplace](#)」を参照してください。

購入者 AWS Marketplace としての の使用

購入者は、[AWS Marketplace](#) に移動して、Amazon Web Services で実行される製品を検索、フィルタリング、および参照します。

ソフトウェア製品を選択すると、製品のページに移動します。ページには、製品に関する情報、料金、使用状況、サポート、および製品レビューがあります。ソフトウェア製品をサブスクライブするには、にサインイン AWS アカウントし、EULA、利用規約、サブスクリプションのカスタマイズに使用できるオプションを含むサブスクリプションページに移動します。

AWS Marketplace 欧州、中東、アフリカ (トルコと南アフリカを除く) を拠点とする アカウントが EMEA の対象となる販売者から購入すると、Amazon Web Services EMEA SARL によって促進されます。

特定の国の顧客の場合、Amazon Web Services EMEA SARL は AWS Marketplace 、購入に対して現地の付加価値税 (VAT) を請求します。税金の詳細については、[AWS Marketplace Buyers Tax ヘルプページ](#)を参照してください。

Amazon Web Services EMEA SARL の詳細については、「[Amazon Web Services EMEA SARL FAQs](#)」を参照してください。

EMEA の対象となる販売者と取引を行うお客様には、Amazon Web Services EMEA SARL から請求書が届きます。他のすべてのトランザクションは、引き続き AWS Inc を通過します。詳細については、「[製品の支払い](#)」を参照してください。

サブスクリプションが処理されたら、フルフィルメントオプション、ソフトウェアバージョン、製品を使用する AWS リージョン 場所を設定し、ソフトウェア製品を起動できます。製品を検索または起動するには、AWS Marketplace ウェブサイトの [Marketplace ソフトウェア](#) にアクセスするか、AWS Marketplace または Amazon Elastic Compute Cloud (Amazon EC2) コンソールから、または Service Catalog からアクセスします。

で利用可能な製品カテゴリの詳細については AWS Marketplace、「」を参照してください [製品カテゴリ](#)。

のソフトウェア製品の配信方法の詳細については AWS Marketplace、以下を参照してください。

- [AMI ベースの製品](#)
- [コンテナ製品](#)
- [Machine Learning 製品](#)
- [プロフェッショナルサービス製品](#)
- [SaaS 製品](#)
- データ製品 - AWS Data Exchange ユーザーガイドで「[AWS Data Exchange とは](#)」を参照してください。

AWS Marketplace でのソフトウェアとサービス

AWS Marketplace には、データベース、アプリケーションサーバー、テストツール、モニタリングツール、コンテンツ管理、ビジネスインテリジェンスなど、多くのソフトウェアカテゴリがあります。よく知られている販売者が提供する商用ソフトウェアとともに、多くの広く使用されているオープンソースソフトウェアを選択できます。必要な製品が見つかったら、1-Click でそのソフトウェアを購入し、独自の Amazon EC2 インスタンスにデプロイできます。AWS CloudFormation を使用して製品のトポロジをデプロイすることもできます。

どの AWS お客様も でショッピングできます AWS Marketplace。ソフトウェア価格とインフラストラクチャの見積もり価格はウェブサイトに表示されます。で既にファイルされている支払い手段を使用して、ほとんどのソフトウェアをすぐに購入できます AWS。ソフトウェア料金は AWS インフラストラクチャ料金と同じ月次請求書に表示されます。

メモ

- Software as a Service (SaaS) とサーバーベースの製品の両方を含む AWS Marketplace、多くのビジネス製品が で利用できます。サーバーベースの製品には、技術知識やセットアップと管理の IT サポートが必要な場合があります。
- 「[チュートリアル: Amazon EC2 Linux インスタンスの開始方法](#)」の情報とチュートリアルは、Amazon EC2 の基本について学習するのに役立ちます。
- を通じて AWS Marketplace 製品の複雑なトポロジを起動する予定の場合 AWS CloudFormation、[AWS の開始方法 CloudFormation](#)を参考にして、AWS CloudFormation の基本について学習してください。

AWS Marketplace には、次のカテゴリのソフトウェアが含まれています。

- インフラストラクチャソフトウェア
- デベロッパーツール
- ビジネスソフトウェア
- 機械学習
- IoT
- プロフェッショナルサービス
- デスクトップアプリケーション
- データ製品

詳細については、「[製品カテゴリ](#)」を参照してください。

主要なソフトウェアカテゴリのそれぞれに、より具体的なサブカテゴリがあります。例えば、インフラストラクチャソフトウェアのカテゴリには、[アプリケーション開発]、[データベースとキャッシュ]、[オペレーティングシステム]などのサブカテゴリがあります。ソフトウェアは、Amazon マシンイメージ (AMI) や Software as a Service (SaaS) など、7 種類の製品タイプから選べます。各種ソフトウェアについては、「[製品のタイプ](#)」を参照してください。

必要なソフトウェアの選択に役立つように、では以下の情報 AWS Marketplace を提供しています。

- 販売者の詳細
- ソフトウェアのバージョン
- ソフトウェアのタイプ (AMI または SaaS)、および AMI に関する情報 (該当する場合)
- 購入者の評価
- 価格
- 製品情報

AWS Marketplace と Amazon の違い DevPay

AWS Marketplace と Amazon には大きな違いがあります DevPay。どちらも、で実行されるソフトウェアを購入するのに役立ちますが AWS、Amazon よりも包括的なエクスペリエンス AWS Marketplace を提供します DevPay。ソフトウェア購入者にとって、主な相違点は以下のとおりです。

- AWS Marketplace は、Amazon.com のようなショッピングエクスペリエンスを提供し、利用可能なソフトウェアの検出を簡素化します。
- AWS Marketplace 製品は、Virtual Private Cloud (VPC) などの他の AWS 機能と連携し、オンデマンドインスタンスに加えて、Amazon Elastic Compute Cloud (Amazon EC2) リザーブドインスタンスおよびスポットインスタンスで実行できます。
- AWS Marketplace は、Amazon Elastic Block Store (Amazon EBS) によってバックアップされたソフトウェアをサポートしていますが、Amazon DevPay はサポートしていません。

さらに、ソフトウェア販売者には、マーケティングアウトリーチおよび AWS Marketplace の検出のしやすさというメリットがあります。

購入者としての開始方法

次のトピックでは、AWS Marketplace 購入者としてソフトウェア製品の使用を開始するプロセスの概要を示します。

トピック

- [製品の購入](#)
- [ソフトウェアの起動](#)
- [チュートリアル: AMI ベースのソフトウェア製品の購入](#)
- [詳細情報](#)

データ製品の使用開始方法の詳細については、「AWS Data Exchange ユーザーガイド」の「[AWS Data Exchange でのデータ製品のサブスクリプション](#)」を参照してください。

製品の購入

で製品を購入すると AWS Marketplace、製品の詳細ページに表示されている製品の条件に同意したことになります。これには、価格条件と販売者のエンドユーザーライセンス契約 (EULA) が含まれています。お客様は [AWS カスタマーアグリーメント](#) に従ってこれらの製品を使用することに同意します。で承諾されたオファー AWS アカウント について、に関連付けられた E メールアドレスに E メール通知が送信されます AWS Marketplace。

Note

AWS では、で特定の製品のガイド付きデモンストレーション AWS Marketplace を無料でリクエストできます。ガイド付きデモンストレーションが利用可能な場合、製品詳細ページにデモのリクエストボタンが表示されます。デモをリクエストするには、ボタンを選択し、リクエストの詳細を指定します。リクエストをまとめた確認メールが届き、担当者から AWS 連絡があります。

月額料金がある製品や、サブスクリプション契約で購入した製品は、サブスクリプション時に料金が発生します。サブスクリプションは、当月の残り期間に応じて日割り計算されます。次のアクションの 1 つを実行するまで、その他の請求は発生しません。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを Amazon マシンイメージ (AMI) で起動する。
- AWS CloudFormation テンプレートを使用して製品をデプロイします。
- 販売者のウェブサイトにて製品を登録する。

製品に年間サブスクリプションのオプションがある場合、サブスクリプションの年間料金がすべて課金されます。この料金は、製品の使用状況ベースで適用され、当初のサブスクリプションを行った日の1年後にサブスクリプションが更新されます。年間サブスクリプション期間の終了時にサブスクリプションを更新しない場合、サブスクリプションは最新の時間単位に基づいた時間別のサブスクリプションに切り替わります。

データ製品のサブスクリプションの詳細については、「AWS Data Exchange ユーザーガイド」の「[AWS Data Exchange でのデータ製品のサブスクリプション](#)」を参照してください。

ソフトウェアの起動

ソフトウェア購入後は、AWS Marketplaceの [1-Click で起動] ビューを使用して、そのソフトウェアを含む Amazon マシンイメージ (AMI) を起動できます。Amazon Elastic Compute Cloud (Amazon EC2 AWS) コンソール、Amazon EC2 APIs AWS Management Console、AWS CloudFormation コンソールなど、Amazon EC2 Web Services () 管理ツールを使用して起動することもできます。

[1-Click で起動] ビューを使用すると、ソフトウェア販売者が推奨する設定で、ソフトウェアの単一インスタンスをすばやく確認、変更、起動できます。Launch with EC2 Console ビューでは、Amazon EC2 APIs、またはその他の管理ツールを使用して AWS Management Console、AMI の起動に必要な AMI 識別番号やその他の関連情報を簡単に見つけることができます。また、[EC2 コンソールで起動] ビューには、インスタンスのタグ付けなど、AWS Management Consoleから起動するよりも多くの設定オプションが用意されています。

Note

インスタンスタイプまたは にアクセスできない場合は AWS リージョン、プライベートオファァーが送信された時点でサポートされていない可能性があります。詳細については、契約の詳細を確認してください。インスタンスまたはリージョンへのアクセスを取得するには、販売者に連絡し、更新されたプライベートオファァーをリクエストします。新しいオファァーを承諾すると、新しく追加されたインスタンスまたはリージョンにアクセスできます。

複雑なトポロジを持つ AWS Marketplace 製品の場合、カスタム起動ビューには、適切な AWS CloudFormation テンプレートを使用して CloudFormation 製品をコンソールにロードするコンソールで起動オプションが表示されます。AWS CloudFormation その後、AWS CloudFormation コンソールウィザードの手順に従って、その製品の AMIs および関連 AWS リソースのクラスターを作成できます。

チュートリアル: AMI ベースのソフトウェア製品の購入

次のチュートリアルでは、AWS Marketplace で Amazon マシンイメージ (AMI) 製品を購入する方法について説明します。

ステップ

- [ステップ 1: を作成する AWS アカウント](#)
- [ステップ 2: ソフトウェアを選択する](#)
- [ステップ 3: ソフトウェアを設定する](#)
- [ステップ 4: Amazon EC2 でソフトウェアを起動する](#)
- [ステップ 5: ソフトウェアを管理する](#)
- [ステップ 6: インスタンスを終了する](#)

ステップ 1: を作成する AWS アカウント

にサインインしなくても、AWS Marketplace ウェブサイト (<https://aws.amazon.com/marketplace>) を参照できます AWS アカウント。ただし、製品のサブスクリプションや起動には、サインインする必要があります。

AWS Marketplace コンソールにアクセスするには AWS アカウント、にサインインする必要があります。の作成方法については AWS アカウント、「AWS Account Management リファレンスガイド」の「[AWS アカウントの作成](#)」を参照してください。

ステップ 2: ソフトウェアを選択する

ソフトウェアを選択するには

1. [AWS Marketplace ウェブサイト](#) に移動します。

Note

新しいインスタンスは、パブリック AWS Marketplace ウェブサイト、<https://aws.amazon.com/marketplace>、または AWS Marketplace の から購入、サブスクライブ AWS Management Console、起動できます <https://console.aws.amazon.com/marketplace/home#/subscriptions>。

この2つの場所でのエクスペリエンスは似ています。この手順では AWS Marketplace ウェブサイトを使用しますが、コンソールを使用する場合の主な相違点を説明します。

- [Shop All Categories (すべてのカテゴリ)] ペインに、選択できるカテゴリの一覧が表示されています。中央のペインで紹介されているソフトウェアを選択することもできます。このチュートリアルでは、[すべてのカテゴリ] ペインで [コンテンツ管理] を選択します。
- コンテンツ管理リストから、WordPressBitnami と Automattic によって認定された を選択します。
- 製品の詳細ページで製品情報を確認します。製品詳細ページには以下のような追加情報も記載されています。
 - 購入者の評価
 - サポート
 - [ハイライト]
 - 製品の詳細な説明
 - 各 のインスタンスタイプの料金詳細 AWS リージョン (AMIs の場合)
 - 使用開始に役立つその他のリソース
- [サブスクリプションを続行する] を選択します。
- AWS Marketplaceにまだサインインしていない場合は、サインインするように求められます。を既にお持ちの場合は AWS アカウント、そのアカウントを使用してサインインできます。をまだお持ちでない場合は AWS アカウント、「」を参照してください [ステップ 1: を作成する AWS アカウント](#)。
- Bitnami の提供条件を読み、[契約に同意する] を選択してサブスクリプションの提供に同意します。
- サブスクリプションアクションが完了するまでに時間がかかることがあります。完了すると、サブスクリプション条件に関する E メールメッセージが届き、続行できます。[設定に進む] を選択して、ソフトウェアを設定して起動します。

製品をサブスクライブすると、その製品の利用規約に同意したことになります。その製品に月額料金がある場合は、サブスクリプション時に料金が請求され、契約月の残り期間に応じて日割り計算されます。選択した AMI で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを起動するまで、その他の料金は発生しません。

Note

製品のサブスクライバーは、サブスクライブしているソフトウェアの新しいバージョンが公開されると、アカウントに E メールメッセージが届きます。

ステップ 3: ソフトウェアを設定する

ソフトウェアを AMI として選択したため、次のステップでは、配信方法、バージョン、ソフトウェアを使用する AWS リージョン 場所の選択など、ソフトウェアを設定します。

ソフトウェアを設定するには

1. [このソフトウェアを設定する] ページで、[配信方法] に [64 ビット (x86) Amazon マシンイメージ (AMI)] を選択します。
2. [ソフトウェアのバージョン] には、使用可能な最新バージョンを選択してください。
3. 製品を起動する [リージョン] (例えば 米国東部 (バージニア北部) など) を選択します。

Note

設定を変更すると、画面下部の [Ami ID] が更新されたことに気付くかもしれません。AMI ID は `ami-<identifier>` の形式で、例えば `ami-123example456` などです。AMI は、リージョン、製品、製品バージョンによって異なります。この AMI ID により、製品の起動時に使用する正しい AMI を指定できます。AMI エイリアスは似たような ID で、自動化ではより簡単に使用できます。AMI エイリアスの詳細については、「[AMI エイリアスを使用する](#)」を参照してください。

4. [続行して起動する] を選択します。

ステップ 4: Amazon EC2 でソフトウェアを起動する

Amazon EC2 インスタンスを起動する前に、1-Click 起動を使用して起動するかどうか、または Amazon EC2 コンソールを使用して起動するかどうかを決めておく必要があります。1-Click 起動を使用すると、セキュリティグループやインスタンスタイプなどの推奨されるデフォルトのオプションを使用してすばやく起動できます。1-Click 起動を使用すると、推定月額料金を確認することもできます。Amazon Virtual Private Cloud (Amazon VPC) 内での起動やスポットインスタンスの使用など、他のオプションを使用する場合は、Amazon EC2 コンソールを使用して起動する必要があります。以下では、製品をサブスクライブし、1-Click 起動または Amazon EC2 コンソールを使用して EC2 インスタンスを起動する手順について説明します。

1-Click 起動を使用して Amazon EC2 で起動する

1-Click 起動を使用して Amazon EC2 で起動するには

1. [このソフトウェアを起動] ページで、[アクションを選択] ドロップダウンから [ウェブサイトから起動] を選択し、デフォルト設定を確認します。設定を変更するには以下を実行します。
 - [EC2 インスタンスタイプ] ドロップダウンリストから、インスタンスタイプを選択します。
 - [VPC の設定] と [サブネットの設定] ドロップダウンリストで、使用するネットワーク設定を選択します。
 - [セキュリティグループの設定] で、既存のセキュリティグループを選択するか、[販売者の設定に基づいて新規クリックする] を選択してデフォルト設定を受け入れます。セキュリティグループの詳細については、[Amazon EC2 ユーザーガイド](#)の「Linux インスタンス用の Amazon EC2 セキュリティグループ Amazon EC2」を参照してください。
 - [キーペア] を展開し、キーペアがある場合は既存のキーペアを選択します。キーペアがない場合は、キーペアを作成するように求められます。Amazon EC2 のキーペアの詳細については、「[Amazon EC2 のキーペア](#)」を参照してください。
2. 設定が完了したら、[起動] を選択します。

新しいインスタンスは、WordPress Bitnami によって認定され、それで実行されている Automattic ソフトウェアを使用して起動されます。ここから、インスタンスの詳細の表示、別のインスタンスの作成、ソフトウェアのすべてのインスタンスの表示を行うことができます。

EC2 コンソールによる起動を使用して Amazon EC2 で起動する

EC2 コンソールによる起動を使用して Amazon EC2 で起動するには

1. [EC2 で起動] ページで、[EC2 コンソールで起動] ビューを選択し、[バージョンを選択] の一覧から AMI バージョンを選択します。
2. [Firewall Settings (ファイアウォールの設定)]、[Installation Instructions (インストール手順)]、および [Release Notes (リリースノート)] の内容を確認してから、[Launch with EC2 Console (EC2 コンソールによる起動)] を選択します。
3. EC2 コンソールで、リクエストインスタンスウィザードを使用して AMI を起動します。
「[Amazon EC2 Linux インスタンスの開始方法](#)」の手順に従って、ウィザードを操作します。

ステップ 5: ソフトウェアを管理する

[AWS Marketplace コンソール](#) の「サブスクリプションの管理」ページ AWS Marketplace を使用して、いつでもソフトウェアサブスクリプションを管理できます。

ソフトウェアを管理するには

1. [AWS Marketplace コンソール](#) に移動し、[サブスクリプションの管理] を選択します。
2. [サブスクリプションの管理] ページでは、以下の内容を確認できます。
 - 製品別のインスタンスのステータスの確認
 - 当月の月額料金の確認
 - 新しいインスタンスの実行
 - インスタンスの販売者のプロフィールの確認
 - インスタンスの管理
 - ソフトウェアを設定するための Amazon EC2 インスタンスへの直接リンク

ステップ 6: インスタンスを終了する

インスタンスがなくなったら、そのインスタンスを終了できます。

Note

終了したインスタンスを再起動することはできません。ただし、同じ AMI から別のインスタンスを起動できます。

インスタンスを終了するには

1. [AWS Marketplace コンソール](#)に移動し、[サブスクリプションの管理] を選択します。
2. [サブスクリプションの管理] ページで、インスタンスを終了するソフトウェアのサブスクリプションを選択し、[管理] を選択します。
3. 特定のサブスクリプションページで、[アクション] ドロップダウンリストから [インスタンスの表示] を選択します。
4. 終了するインスタンスがある [リージョン] を選択します。これにより Amazon EC2 コンソールが開き、そのリージョンのインスタンスが新しいタブに表示されます。必要に応じて、このタブに戻って、終了するインスタンスのインスタンス ID を確認できます。
5. Amazon EC2 コンソールで、[インスタンス ID] を選択し、[インスタンスの詳細ページ] を開きます。
6. [インスタンスの状態] ドロップダウンリストから [インスタンスを終了] を選択します。
7. 確認を求めるメッセージが表示されたら、[Terminate (終了)] を選択します。

終了するまでに数分かかります。

詳細情報

製品カテゴリとタイプの詳細については、「[\[製品カテゴリ\]](#)」および「[製品のタイプ](#)」を参照してください。

Amazon EC2 の詳細については、[Amazon Elastic Compute Cloud ドキュメント](#)でサービスのドキュメントを参照してください。

の詳細については AWS、<https://aws.amazon.com/> を参照してください。

AWS リージョン でサポートされる AWS Marketplace

ソフトウェア製品の場合、販売者はソフトウェア AWS リージョン をどの で利用できるか、およびインスタンスタイプを選択します。利用可能なすべてのリージョンおよび有効なすべてのインスタンスタイプで製品を利用可能にすることをお勧めします。AWS Marketplace ウェブサイトは世界中で利用でき、以下のリージョンをサポートしています。

- 北米
 - 米国東部 (オハイオ)
 - 米国東部 (バージニア北部)
 - 米国西部 (北カリフォルニア)
 - 米国西部 (オレゴン)
 - AWS GovCloud (米国東部)
 - AWS GovCloud (米国西部)
 - カナダ (中部)
 - カナダ西部 (カルガリー)
- アフリカ
 - アフリカ (ケープタウン)
- 南米
 - 南米 (サンパウロ)
- ヨーロッパ、中東、およびアフリカ
 - 欧州 (フランクフルト)
 - 欧州 (アイルランド)
 - 欧州 (ロンドン)
 - 欧州 (ミラノ)
 - 欧州 (パリ)
 - 欧州 (スペイン)
 - 欧州 (ストックホルム)
 - 欧州 (チューリッヒ)

- アジアパシフィック
 - アジアパシフィック (香港)
 - アジアパシフィック (ハイデラバード)
 - アジアパシフィック (ジャカルタ)
 - アジアパシフィック (メルボルン)
 - アジアパシフィック (ムンバイ)
 - アジアパシフィック (大阪)
 - アジアパシフィック (ソウル)
 - アジアパシフィック (シンガポール)
 - アジアパシフィック (シドニー)
 - アジアパシフィック (東京)

- 中東
 - イスラエル (テルアビブ)
 - 中東 (バーレーン)
 - 中東 (アラブ首長国連邦)

データ製品についてサポートされているリージョンの詳細は、「AWS 全般のリファレンス」の「[AWS Data Exchange エンドポイントとクォータ](#)」を参照してください。

[製品カテゴリ]

[AWS Marketplace](#) ウェブサイトは、それぞれにサブカテゴリを持つ主要なカテゴリで構成されています。このカテゴリとサブカテゴリに基づいて、検索とフィルタリングを行えます。

トピック

- [インフラストラクチャソフトウェア](#)
- [DevOps](#)
- [ビジネスアプリケーション](#)
- [機械学習](#)
- [IoT](#)
- [プロフェッショナルサービス](#)
- [デスクトップアプリケーション](#)
- [データ製品](#)
- [業界](#)

インフラストラクチャソフトウェア

このカテゴリの製品は、インフラストラクチャ関連のソリューションを提供します。

バックアップおよび復旧

ストレージおよびバックアップソリューションに使用する製品。

データ分析

データ分析に使用される製品。

ハイパフォーマンスコンピューティング

ハイパフォーマンスコンピューティング製品。

移行

移行プロジェクトに使用する製品。

ネットワークインフラストラクチャ

ネットワークソリューションの作成に使用する製品。

オペレーティングシステム

パッケージ化された Linux および Windows オペレーティングシステム。

セキュリティ

インフラストラクチャのセキュリティ製品。

[Storage (ストレージ)]

ストレージに関わるジョブロールに重点を置いたアプリケーション。

DevOps

このカテゴリの製品は、開発者および開発者チーム向けのツールを提供します。

アジャイルなライフサイクル管理

アジャイルな SDLM に使用される製品。

アプリケーション開発

アプリケーション開発に使用する製品。

アプリケーションサーバー

アプリケーション開発に使用するサーバー。

アプリケーションスタック

アプリケーション開発に使用するスタック。

継続的インテグレーションと継続的デリバリー

CI/CD に使用される製品。

Infrastructure as Code

インフラストラクチャに使用される製品。

問題およびバグの記録

開発者チームがソフトウェアのバグの追跡と管理に使用する製品。

モニタリング

オペレーティングソフトウェアの監視に使用する製品。

ログ分析

ログの記録と分析に使用する製品。

ソースコントロール

ソースコントロールの管理と維持に使用する製品。

テスト

ソフトウェア製品の自動テストに使用する製品。

ビジネスアプリケーション

このカテゴリの製品はビジネスの運用に役立ちます。

ブロックチェーン

ブロックチェーンに使用される製品。

コラボレーションおよび生産性

ビジネスにおけるコラボレーションを実現するために使用する製品。

コンタクトセンター

組織内のコンタクトセンターを有効活用するために使用される製品。

コンテンツ管理

コンテンツ管理に重点を置いた製品。

CRM

顧客関係管理に重点を置いたツール。

eコマース

eコマースソリューションを提供する製品。

eラーニング

eラーニングソリューションを提供する製品。

人事

組織内の人事部門を有効活用するために使用される製品。

IT ビジネスマネジメント

組織の IT ビジネスマネジメントを有効活用できるようにするために使用する製品。

ビジネスインテリジェンス

組織のビジネスインテリジェンスを有効活用できるようにするために使用する製品。

プロジェクト管理

プロジェクト管理用のツール。

機械学習

このカテゴリの製品は、Amazon で動作する機械学習アルゴリズムとモデルパッケージを提供します SageMaker。

ML ソリューション

機械学習ソリューション。

データラベリングサービス

データラベリング機能を提供する製品。

コンピュータビジョン

コンピュータビジョン機能を使用できるようにする製品。

自然言語処理

自然言語処理機能を使用できるようにする製品。

音声認識

音声認識機能を使用できるようにする製品。

[Text] (テキスト)

テキスト学習機能を使用できるようにする製品。例としては、分類、クラスタリング、編集/処理、埋め込み、生成、文法/解析、識別、名前とエンティティ認識、感情分析、要約 text-to-speech、翻訳などがあります。

イメージ

画像分析機能を使用できるようにする製品。3D、キャプション、分類、編集/処理、組み込み/機能抽出、生成、文法/解析、手書き文字認識、人/顔、物体検出、セグメント化/ピクセルラベリング、テキスト/OCR などが含まれます。

動画

ビデオ分析機能を使用できるようにする製品。分類、物体検出、編集/処理、異常検出、話者識別、モーション、再識別、要約、テキスト/キャプション、トラッキングなどが含まれます。

Audio

音声分析機能を使用できるようにする製品。例としては、話者識別 speech-to-text、分類、曲識別、セグメンテーションなどがあります。

構造化

構造化分析機能を使用できるようにする製品。分類、クラスタリング、次元削減、因数分解モデル、機能エンジニアリング、ランク付け、回帰、時系列予測などが含まれます。

IoT

IoT 関連ソリューションの作成に使用する製品。

分析

IoT ソリューション用の分析製品。

アプリケーション

IoT ソリューションスペース用のアプリケーション製品。

デバイスの接続

デバイスの接続の管理に使用する製品。

デバイスの管理

デバイスの管理に使用する製品。

デバイスのセキュリティ

IoT デバイスのセキュリティの管理に使用する製品。

産業における IoT

産業関連の IoT ソリューションの提供に重点を置いた製品。

スマートホームおよびスマートシティ

スマートホームおよびスマートシティソリューションを有効活用できるようにするために使用する製品。

プロフェッショナルサービス

このカテゴリの製品は、AWS Marketplace 製品に関連するコンサルティングサービスを提供します。

評価

組織に最適なソリューションを見つけるために、現在の運用環境を評価します。

実装

サードパーティー製ソフトウェアの設定、セットアップ、デプロイを支援します。

マネージドサービス

ユーザーに代わって End-to-end 環境管理を行います。

Premium Support

お客様のニーズに合わせて設計された、エキスパートによるガイダンスやサポートを受けることができます。

トレーニング

従業員がベストプラクティスを学ぶのに役立つ、エキスパートによるカスタマイズされたワークショップ、プログラム、教育ツールを提供します。

デスクトップアプリケーション

このカテゴリの製品は、インフラストラクチャ関連のソリューションを提供します。

デスクトップアプリケーション

全般的な生産性を向上させたり特定のジョブロールを有効にしたりするためのデスクトップアプリケーションおよびユーティリティ。

AP および請求

アカウントの支払いと請求に重点を置いたジョブロールで使用するアプリケーション。

アプリケーションとウェブ

汎用およびウェブ環境アプリケーション。

開発

開発に使用するアプリケーション。

ビジネスインテリジェンス

ビジネスインテリジェンスの管理に重点を置いたジョブロールで使用するアプリケーション。

CAD および CAM

コンピュータ支援設計および製造に重点を置いたジョブロールで使用するアプリケーション。

GIS とマッピング

GIS とマッピングに重点を置いたジョブロールで使用するアプリケーション。

イラストレーションおよびデザイン

イラストレーションとデザインに重点を置いたジョブロールで使用するアプリケーション。

メディアおよびエンコード

メディアとエンコードに関わるジョブロールで使用するアプリケーション。

生産性およびコラボレーション

生産性の向上とコラボレーションの実現に重点を置いたアプリケーション。

プロジェクト管理

プロジェクトマネージャーのジョブロールで使用するアプリケーション。

セキュリティ、ストレージ、およびアーカイブ

セキュリティ、ストレージ、およびデータアーカイブに関わるジョブロールに重点を置いたアプリケーション。

ユーティリティ

さまざまなジョブロールで使用するユーティリティに重点を置いたアプリケーション。

データ製品

このカテゴリの製品は、ファイルベースのデータのセットです。詳細については、「[AWS Data Exchange ユーザーガイド](#)」を参照してください。

業界

教育および研究

教育および研究ソリューションを提供することを目的とする製品。

金融サービス

組織で金融サービスを利用できるようにする製品。

ヘルスケアおよびライフサイエンス

ヘルスケアおよびライフサイエンス業界で使用する製品。

メディアおよびエンターテインメント

メディア関連の製品とソリューション。

工業用

工業関連の製品およびソリューション。

エネルギー

エネルギー関連の製品およびソリューション。

製品のタイプ

AWS Marketplace には、人気のあるオープンソースおよび商用ソフトウェアに加えて、無料および有料のデータ製品が含まれています。これらの製品は、個別の Amazon マシンイメージ (AMIs AWS CloudFormation テンプレートを通じてデプロイされた AMIs のクラスター、Software as a Service (SaaS)、プロフェッショナルサービス、AWS Data Exchange データ製品など、さまざまな方法で利用できます。

これらの製品タイプの詳細については、次のトピックを参照してください。

- [AMI ベースの製品](#) (AMI とプライベートイメージ製品を含む)
- [コンテナ製品](#)
- [Machine Learning 製品](#)
- [プロフェッショナルサービス製品](#)
- [SaaS 製品](#)
- [データ製品](#)

AMI ベースの製品

Amazon マシンイメージ (AMI) は、オペレーティングシステム、および多くの場合に AWS で動作する追加のソフトウェアを含むサーバーのイメージです。

に記載されているソフトウェア AWS Marketplace は、Amazon Elastic Compute Cloud (Amazon EC2) でのみ実行できます。ダウンロードすることはできません。

では AWS Marketplace、AMIs の検索 (検索提案を含む)、他のお客様から送信された製品レビューの表示、AMIs サブスクリプションと起動、サブスクリプションの管理を行うことができます。すべての AWS Marketplace 製品は品質が検証され、Amazon Web Services (AWS) インフラストラクチャの 1-Click 起動機能用に事前設定されています。

AMI 製品と Software as a Service (SaaS) 製品の出品は、どちらも信頼できる販売者から提供されます。AMI 製品は、お客様の AWS アカウントで実行されます。ソフトウェア設定とソフトウェアで動作するサーバーをより詳細に制御できますが、サーバーの設定とメンテナンスに関する責任も大きくなります。

AWS Marketplace カタログには、有名販売者の厳選されたオープンソースおよび商用ソフトウェアが含まれています。の多くの製品は、1 時間で購入 AWS Marketplace できます。

AMI カタログは、ユーザーや開発チームがコストのかかる調査を行うことなく開発中のソフトウェアやプロジェクトを表示および交換できるコミュニティリソースです。コミュニティの AMI カタログに表示される製品は、有名な販売者が提供するものである場合とそうでない場合があります、一般的には詳しい調査を行っていません。

AWS Marketplace 製品には、製品が利用可能な各 AWS リージョン 1 つの AMI が含まれています。これらの AMI は、場所を除いて同じです。また、販売者が最新のパッチと更新プログラムで製品を更新するときに、製品に別の AMI セットを追加することがあります。

テンプレートを使用してクラスターとしてデプロイされるため、AWS Marketplace 製品によっては AMI の複数のインスタンスを起動する場合があります AWS CloudFormation。このインスタンスのクラスターは、CloudFormation テンプレートによって設定された追加の AWS インフラストラクチャサービスとともに、単一の製品のデプロイとして機能します。

AWS CloudFormation テンプレート

Important

AWS Marketplace は、2024 年 8 月に AWS CloudFormation テンプレートを使用して、複数の Amazon マシンイメージ (AMI) 製品の配信方法を中止します。を使用した単一の AMI など CloudFormation、を使用する他の AWS Marketplace 製品は影響を受け CloudFormation ません。

2024 年 8 月まで、既存のサブスクリイパーは、の CloudFormation テンプレートを使用して複数の AMI 製品の新しいインスタンスを起動できます AWS Marketplace。廃止後は、新しいインスタンスを起動できません。Amazon Elastic Compute Cloud (Amazon EC2) で以前に起動および実行されていた既存のインスタンスは影響を受けず、引き続き実行されます。質問がある場合は、[AWS サポート](#)に連絡してください。

AWS CloudFormation は、AWS リソースのモデル化とセットアップに役立つサービスです。これにより、これらのリソースの管理に費やす時間を減らし、で実行されるアプリケーションに集中する時間を増やすことができます AWS。CloudFormation テンプレートは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスや Amazon Relational Database Service (Amazon RDS) データベースインスタンスなど、必要なさまざまな AWS リソースを記述します。CloudFormation は、これらのリソースのプロビジョニングと設定を行います。詳細については、「[AWS の開始方法 CloudFormation](#)」を参照してください。

AWS CloudFormation テンプレートの使用

ソフトウェア販売者は、複数の AMI インスタンスやその他の AWS リソースで構成される優先デプロイトポロジを定義する CloudFormation テンプレートを提供する場合があります。製品で CloudFormation テンプレートが使用可能な場合、製品リストページにデプロイオプションとして一覧表示されます。

AMI では単一の Amazon EC2 インスタンスをデプロイできます。CloudFormation テンプレートを使用して、クラスターとして機能する AMI の複数のインスタンスを、Amazon RDS、Amazon Simple Storage Service (Amazon S3)、またはその他の AWS サービスなどの AWS リソースとともに、単一のソリューションとしてデプロイできます。

トピック

- [の AMI サブスクリプション AWS Marketplace](#)
- [契約料金による AMI 製品](#)
- [計測対応 AMI 製品](#)
- [AMI 製品のコスト配分タグ](#)
- [AMI エイリアスを使用する](#)

の AMI サブスクリプション AWS Marketplace

では AWS Marketplace、一部の Amazon マシンイメージ (AMI) ベースのソフトウェア製品で年間サブスクリプション料金モデルを提供しています。この料金モデルは一括前払いで、以降の 12 か月間は時間単位の使用料金はかかりません。1 つの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに対して、AWS Marketplace のソフトウェア製品の 1 つの年間サブスクリプションを適用できます。

Note

年間料金による時間単位の AMI の場合、年間サブスクリプションは購入時に指定したインスタンスタイプのみを対象としています。例えば t3.medium です。他のインスタンスタイプを起動すると、アクティブなサブスクリプションに基づいて、そのインスタンスタイプの時間単位の料金が発生します。

時間単位の料金を使用して AWS Marketplace、ソフトウェア製品の起動と実行を続行することもできます。から Amazon EC2 およびその他のサービスを使用する際の料金は、AWS Marketplace ソフトウェア製品の購入に対して支払う料金とは AWS 別に発生します。

Amazon EC2 インスタンスタイプを時間単位で使用するように変更した場合、Amazon EC2 インフラストラクチャは契約した Savings Plans に従って請求されます。ただし、からの AMI ライセンス AWS Marketplace は自動的に時間単位の料金に変更されます。

時間単位の AMI 製品が年間料金をサポートしていない場合、購入者は年間サブスクリプションを購入できません。AMI 時間単位の製品が年間料金をサポートしている場合、購入者は の製品ページにアクセスして年間契約 AWS Marketplace を購入できます。各年間契約では、購入者は時間単位の料金を請求されることなく 1 つのインスタンスを実行できます。契約は、インスタンスタイプによって異なります。

年間契約の修正

1 時間ごとの年間 (年間) 計画の修正では、 から直接計画を修正できます AWS Marketplace 管理ポータル。修正は、より多くの vCPUs を持つ Amazon Elastic Compute Cloud (Amazon EC2) インスタンスタイプで実行するように AMI を切り替える必要がある場合や、より最新の世代の CPU アーキテクチャに移行する必要がある場合に使用できます。修正により、既存の年間プランに次の変更を加えることができます。

- Amazon EC2 インスタンスタイプファミリーの切り替え
- Amazon EC2 インスタンスタイプサイズを切り替える
- 新しいインスタンスタイプを追加する
- 契約内の既存のインスタンスタイプの数量を増やす

契約で追加または切り替えた新しい Amazon EC2 インスタンスタイプは、プランの現在の終了日に共同契約され、契約内のすべてのインスタンスタイプが同時に更新されます。

変更の日割りコストが 0 より大きい限り、変更を行うことができます。新しく追加された Amazon EC2 インスタンスの日割り計算されたコストは、契約の残りの期間に合わせて調整されたインスタンスタイプの年間コストに基づきます。インスタンスタイプを切り替える場合、削除された Amazon EC2 インスタンスタイプの日割りコストは、新しく追加された Amazon EC2 インスタンスタイプの日割りコストから差し引かれます。

Note

修正は、パブリックオファーから行われたすべての契約と、分割プランのないプライベートオファーからの契約でサポートされます。

年間契約修正の例

年間契約の修正に関する以下の例を検討してください。次の例では、お客様は 2024 年 1 月 1 日に m5.large インスタンスタイプの 2 ユニット (4000 USD/年) の契約に署名しました。販売者には、出品手数料を引いた 8,000 USD が支払われています。

Example 1: 等しい値のインスタンスタイプへの切り替え

年半ばに、お客様は m5.large インスタンスタイプの 1 つのユニットを r5.large インスタンスタイプの 1 つのユニットに切り替えることを希望しています。切り替えの日割りコストは、追加されたインスタンスの日割りコスト (r5.large の 6 か月 - 2000 USD) から、削除されたインスタンスの日割りコスト (m5.large の 6 か月 - 2000 USD) を差し引いて計算されます。正味コストは 0 USD であるため、修正が発生する可能性があります。

Example 2: より高い価格のインスタンスタイプへの切り替え

年半ばに、お客様は m5.large インスタンスタイプの 1 つのユニットを m5.2xlarge インスタンスタイプの 1 つのユニットに切り替えることを希望しています。スイッチの日割りコストは、追加されたインスタンスの日割りコスト (6 か月分の m5.large - 2000 USD) から、削除されたインスタンスの日割りコスト (6 か月分の m5.2xlarge - 3000 USD) を差し引いて計算されます。正味コストは 1,000 USD であるため、修正が発生する可能性があります。

Example 3: 低価格のインスタンスタイプの単一ユニットへの切り替え

年半ばに、お客様は m5.large インスタンスタイプの 1 つのユニットを c5.large インスタンスタイプの 1 つのユニットに切り替えることを希望しています。スイッチの日割りコストは、追加されたインスタンスの日割りコスト (6 か月の m5.large - 2,000 USD) から、削除されたインスタンスの日割りコスト (6 か月の c5.large - 1,500 USD) を差し引いて計算されます。正味コストは -500 USD (0 USD 未満) であるため、修正を行うことはできません。

Example 4: 低価格のインスタンスタイプの複数ユニットへの切り替え

年半ばに、お客様は m5.large インスタンスタイプの 1 つのユニットを c5.large インスタンスタイプの 2 つのユニットに切り替えることを希望しています。スイッチの日割りコストは、追加されたインスタンスの日割りコスト (6 か月の m5.large - 2,000 USD) から、削除されたインスタンスの日割りコスト (6 か月の 2 つの c5.large - 3,000 USD) を差し引いて計算されます。正味コストは 1,000 USD であるため、修正が発生する可能性があります。

Example 5: 新しいインスタンスタイプを追加する

年半ばに、顧客は m5.large インスタンスタイプの単位を契約に追加したいと考えています。この変更の按分コストは、追加されたインスタンスの按分コストとして計算されます (6 か月分の m5.large - 2,000 USD)。正味コストは 2,000 USD であるため、修正が発生する可能性があります。

Example 6: インスタンスタイプの削除

年半ばに、顧客は m5.large インスタンスタイプの 1 つのユニットを削除したいと考えています。この変更の按分コストは、削除されたインスタンスの按分コストとして計算されます (6 か月分の m5.large - 2,000 USD)。正味コストは -2,000 USD (0 USD 未満) であるため、修正を行うことはできません。

契約料金による AMI 製品

一部の販売者は、Amazon マシンイメージ (AMI) ベースのソフトウェア製品を契約料金モデルで販売しています。このモデルでは、選択した期間、ソフトウェア製品にアクセスするための個別のライセンスについて、一括で前払いすることに同意したものとみなされます。を通じて事前に請求されます AWS アカウント。例えば、1 年間に 10 件のユーザーアクセスライセンスと 5 件の管理ライセンスを購入するとします。ライセンスを自動的に更新するように選択できます。

さらに、一部の企業では、契約料金モデルでプライベート AMI ベースのソフトウェア製品を提供しています。通常、プライベートオファーは期間が決まっており、変更できません。

AMI ベースのソフトウェア製品の契約は、AWS Marketplace の [製品の詳細] ページから購入できます。このオプションが利用可能な場合、商品の詳細ページの [配信方法] に、[契約料金による AMI] が表示されます。製品を購入すると、アカウントのセットアップと設定を行うために、製品のウェブサイトが表示されます。その後、使用料は通常の AWS アカウント 請求レポートに表示されます。

契約料金のパブリックオファーによる AMI 製品のサブスクリプション

契約料金モデルによるパブリックオファーの AMI ベースの製品をサブスクライブするには

1. にサインイン AWS Marketplace し、契約料金モデルを使用してコンテナベースのソフトウェア製品を検索します。
2. [調達] ページで、[料金情報] を表示します。
各期間 (月単位) の [単位] と料金を確認できます。
3. [サブスクライブを続ける] を選択して、サブスクリプションを開始します。
サブスクライブせずにこの製品を保存するには、[リストに保存する] を選択します。
4. 料金情報を確認し、ソフトウェア製品の条件を設定して契約を作成します。
 - a. [1 か月]、[12 か月]、[24 か月]、[36 か月] の中から契約期間を選択します
 - b. [更新設定] で、契約を自動的に更新するかどうかを選択します。
 - c. [契約オプション] で、各単位の数量を選択します。

契約料金の合計は、[料金の詳細] に表示されます。

5. すべての選択を完了したら、[Create Contract (契約の作成)] を選択します。

合計契約料金が に請求されます AWS アカウント。ライセンスは で生成されます AWS License Manager。

Note

サブスクリプションが処理され、ソフトウェア製品のライセンスが AWS License Manager アカウントで生成されるまでに最大 10 分かかる場合があります。

契約料金のプライベートオファーによる AMI 製品のサブスクリプション

契約料金モデルによるプライベートオファーの AMI ベースの製品をサブスクライブするには

1. 購入者アカウント AWS Marketplace で にサインインします。
2. プライベートオファーが表示されます。
3. [調達] ページで、[料金情報] を表示します。

各期間 (月単位) の [単位] と料金を確認できます。

4. [サブスクライブを続ける] を選択して、サブスクリプションを開始します。
5. 料金情報を確認し、ソフトウェア製品の条件を設定して契約を作成します。

契約期間は既に販売者が設定しており、変更できません。

6. [契約オプション] で、各単位の数量を選択します。
7. [料金の詳細] で契約料金の合計を表示します。

また、パブリックオファーは、[ご利用いただけるその他のオファー] の [オファーを表示] を選択して確認できます。

8. すべての選択を完了したら、[Create Contract (契約の作成)] を選択します。

Note


サブスクリプションが処理され、ソフトウェア製品のライセンスが AWS License Manager アカウントで生成されるまでに最大 10 分かかる場合があります。

ソフトウェアへのアクセス

AMI ベースのソフトウェア製品にアクセスするには

1. AWS Marketplace コンソールで、「サブスクリプションを表示」に移動し、ソフトウェア製品のライセンスを表示します。
2. [調達] ページで、次の手順を実行します。
 - a. ライセンスの管理 を選択して、 で使用権限の表示、アクセス許可の付与、使用状況の追跡を行います AWS License Manager。
 - b. [Continue to Configuration (設定に進む)] を選択します。
3. [起動] ページの設定を確認し、[アクションを選択] でソフトウェアの起動方法を選択します。
4. [インスタンスタイプを選択] で、Amazon Elastic Compute Cloud (Amazon EC2) を選択し、次に [次の手順: インスタンスの詳細の設定] を選択します。
5. インスタンスの詳細の設定 ページの IAM ロールで、 から既存の AWS Identity and Access Management (IAM) ロールを選択します AWS アカウント。

IAM ロールがない場合は、[新しい IAM ロールを手動で作成] リンクを選択し、その手順に従ってください。

 Note

契約料金で製品を購入すると、AWS Marketplace によってライセンスが作成され AWS アカウント、ソフトウェアは License Manager API を使用して確認できます。AMI ベースの製品のインスタンスを作成するには、IAM ロールが必要です。
IAM ポリシーでは、次の IAM アクセス許可が必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "license-manager:CheckoutLicense",
        "license-manager:GetLicense",
        "license-manager:CheckInLicense",
        "license-manager:ExtendLicenseConsumption",
        "license-manager:ListReceivedLicenses"
      ],
      "Resource": "*"
    }
  ]
}
```

6. インスタンスの詳細を設定したら、[確認と作成] を選択します。
7. [インスタンス作成の確認] ページで、既存のキーペアを選択するか、新しいキーペアを作成し、[インスタンスの作成] を選択します。

[インスタンスの作成を開始する] 進行状況ウィンドウが表示されます。

8. インスタンスが開始されたら、EC2 ダッシュボードに移動し、[インスタンス] の下の [インスタンスの状態] に [実行中] と表示されていることを確認します。

生成されたライセンスを表示する

生成されたライセンスを表示するには

1. AWS License Manager でサインインします AWS アカウント。
2. [付与されたライセンス] には、付与されたライセンスがすべて表示されます。
3. [検索] バーに、製品 SKU、受取人、または状態を入力してライセンスを検索します。
4. [ライセンス ID] を選択すると、[ライセンスの詳細] が表示されます。
5. [発行者] (AWS/Marketplace) および [使用権限] (ライセンスによってアプリケーションやリソースの使用、アクセス、消費する権限を与える単位) を表示できます。

既存の契約を変更する

AMI 製品に対して既存の前払い契約がある場合、AWS Marketplace 購入者は契約の一部を変更できません。AMI 契約は、時間単位または年単位の Flexible Consumption Pricing (FCP) オファーではなく、契約条件ベースのオファーによってサポートされています。この機能は、と統合されているアプリケーションでのみ使用できます AWS License Manager。購入者は、現在の契約と同一オファーの使用権限の範囲内で、追加ライセンスを購入できます。ただし、購入者は契約で購入した使用権限の数を減らすことはできません。また、販売者がオプションを有効にしている場合、購入者はサブスクリプションの自動更新をキャンセルできます。

Note

Flexible Payment Schedule (FPS) 契約のオファーは変更できません。FPS で購入した契約では、購入者が使用権限を変更することはできません。使用権限とは、アプリケーションやリソースを使用、アクセス、消費する権利のことです。FPS オファーは変更できません。

サブスクリプションを管理する

1. AWS Marketplace コンソールで、「サブスクリプションを表示」に移動し、ソフトウェア製品のライセンスを表示します。
2. [調達] ページで [ライセンスを管理] を選択します。
3. リストから [条件を表示] を選択します。
4. [契約オプション] セクションで、矢印を使って使用権限を増やします。使用権限の数は、購入した使用権限の数よりも減らすことはできません。

5. 契約の詳細と合計金額は [料金の詳細] セクションに表示されます。

サブスクリプションの自動更新をキャンセルするには

1. AWS Marketplace コンソールで、「サブスクリプションを表示」に移動し、ソフトウェア製品のライセンスを表示します。
2. [調達] ページで [ライセンスを管理] を選択します。
3. [サブスクリプション] ページで、[更新設定] セクションを見つけます。
4. キャンセルに関する利用規約を必ずご確認ください。
5. チェックボックスをオンにすると、自動更新がキャンセルされます。

計測対応 AMI 製品

にリストされている一部の製品は AWS Marketplace、ソフトウェアアプリケーションによって測定された使用量に基づいて請求されます。計測された使用状況ディメンションの例として、ホスト/エージェントの使用状況や帯域幅の使用状況などがあります。これらの製品が正しく機能するには追加の設定が必要です。使用量を計測するアクセス許可を持つ IAM ロールは、起動時に AWS Marketplace Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに関連付ける必要があります。Amazon EC2 の IAM ロールの詳細については、「[Amazon EC2 の IAM ロール](#)」を参照してください。

AMI 製品のコスト配分タグ

AWS Marketplace は、Amazon マシンイメージ (AMI) ベースのソフトウェア製品のコスト配分タグ付けをサポートします。新規および既存の Amazon Elastic Compute Cloud (Amazon EC2) インスタスタグは、対応する AWS Marketplace AMI の使用に対して自動的に入力されます。アクティブ化されたコスト配分タグを使用して、AWS コストと使用状況レポート AWS Cost Explorer、AWS 予算、またはその他のクラウド支出分析ツールを通じて AMI の使用状況を特定および追跡できます。

AMI を提供したベンダーでは、製品固有の情報に基づいて、AMI ベースの製品の計測に他のカスタムタグを記録する場合があります。詳細については、「[コスト配分タグ](#)」を参照してください。

タグを使用してリソースを整理し、コスト配分タグを使用して AWS のコストを詳細レベルで追跡できます。コスト配分タグを有効にすると、はコスト配分タグ AWS を使用してコスト配分レポートでリソースコストを整理し、AWS コストの分類と追跡を容易にします。

コスト配分タグは、タグが Billing and Cost Management コンソールでアクティブ化された時点からのコストのみを追跡します。アカウントの請求情報とコスト管理コンソールにアクセスできるのは、AWS アカウント 所有者、AWS Organizations 管理アカウントの所有者、および適切なアクセス許可を持つユーザーのみです。コスト配分タグを使用するかどうかにかかわらず、請求額に変更はありません。コスト配分タグを使用するかどうかは、AMI ベースのソフトウェア製品の機能には影響しません。

複数のインスタンス間での 1 つの AMI のコスト配分タグの追跡

AWS Marketplace AMI サブスクリプション用に起動された各 Amazon EC2 インスタンスには、AWS Marketplace AWS コストと使用状況レポートに対応するソフトウェア使用状況行項目があります。AWS Marketplace 使用状況には、対応する Amazon EC2 インスタンスに適用された特定のタグが常に反映されます。これにより、割り当てられたさまざまなタグ値に基づいて、インスタンスレベルで AWS Marketplace 使用コストを区別できます。

また、タグベースの使用コストを合計して、Cost Explorer または Cost and Usage レポートで請求書に反映されている AMI AWS ソフトウェアの使用料金と等しくなるようにすることもできます。

コスト配分タグ付きインスタンスを使用した予算の検索

Billing and Cost Management コンソールで、複数の Amazon EC2 インスタンスのコスト配分タグでフィルタリング済みの有効な予算が既にある場合、それらすべてを見つけるのは難しい場合があります。次の Python スクリプトは、現在の AWS リージョンの AWS Marketplace からの Amazon EC2 インスタンスを含む予算のリストを返します。

このスクリプトを使用して、予算への潜在的な影響、およびこの変更によってオーバーランが発生する可能性がある場所を認識することができます。請求額は変更されませんが、コスト配分はより正確に反映され、これが予算に影響する可能性があることに注意してください。

```
#!/usr/bin/python

import boto3

session = boto3.Session()
b3account=boto3.client('sts').get_caller_identity()['Account']
print("using account {} in region {}".format(b3account,session.region_name))

def getBudgetFilters(filtertype):
    ...
    Returns budgets nested within the filter values [filter value][budeget name].
```

```

The filtertype is the CostFilter Key such as Region, Service, TagKeyValue.
'''
budget_client = session.client('budgets')
budgets_paginator = budget_client.get_paginator('describe_budgets')
budget_result = budgets_paginator.paginate(
    AccountId=b3account
).build_full_result()
returnval = {}
if 'Budgets' in budget_result:
    for budget in budget_result['Budgets']:
        for cftype in budget['CostFilters']:
            if filtertype == cftype:
                for cfval in budget['CostFilters'][cftype]:
                    if cfval in returnval:
                        if not budget['BudgetName'] in returnval[cfval]:
                            returnval[cfval].append(budget['BudgetName'])
                    else:
                        returnval[cfval] = [ budget['BudgetName'] ]
return returnval

def getMarketplaceInstances():
    '''
    Get all the AWS EC2 instances which originated with AWS Marketplace.
    '''
    ec2_client = session.client('ec2')
    paginator = ec2_client.get_paginator('describe_instances')
    returnval = paginator.paginate(
        Filters=[{
            'Name': 'product-code.type',
            'Values': ['marketplace']
        }]
    ).build_full_result()
    return returnval

def getInstances():
    mp_instances = getMarketplaceInstances()
    budget_tags = getBudgetFilters("TagKeyValue")
    cost_instance_budgets = []
    for instance in [inst for resrv in mp_instances['Reservations'] for inst in
resrv['Instances'] if 'Tags' in inst.keys()]:
        for tag in instance['Tags']:
            # combine the tag and value to get the budget filter string
            str_full = "user:{{}}${{}}".format(tag['Key'], tag['Value'])

```

```
    if str_full in budget_tags:
        for budget in budget_tags[str_full]:
            if not budget in cost_instance_budgets:
                cost_instance_budgets.append(budget)
print("\r\nBudgets containing tagged Marketplace EC2 instances:")
print( '\r\n'.join([budgetname for budgetname in cost_instance_budgets]) )

if __name__ == "__main__":
    getInstances()
```

出力例

```
Using account 123456789012 in region us-east-2
```

```
Budgets containing tagged Marketplace EC2 instances:
EC2 simple
MP-test-2
```

関連トピック

詳細については、次のトピックを参照してください。

- 「AWS Billing ユーザーガイド」の「[コスト配分タグの使用](#)」。
- 「AWS Billing ユーザーガイド」の「[AWS 生成コスト配分タグの有効化](#)」。
- [Amazon EC2 ユーザーガイド](#)の「[Amazon EC2 リソースのタグ付け](#)」。 Amazon EC2

AMI エイリアスを使用する

Amazon マシンイメージ (AMI) は、AMI ID で識別されます。AMI ID を使用して、製品を起動する際に使用する AMI を指定できます。AMI ID は `ami-<identifier>` の形式で、例えば `ami-123example456` などです。AMI (AMI ID) は、AWS リージョン、製品、製品バージョンによって異なります。

から製品を起動すると AWS Marketplace、 が自動的に入力AMI IDされます。を用意しておくAMI IDと、AWS Command Line Interface (AWS CLI) からの製品の起動を自動化する場合や、Amazon Elastic Compute Cloud (Amazon EC2) を使用する場合に便利です。AMI ID は、起動時にソフトウェアを設定すると確認できます。詳細については、「[ステップ 3: ソフトウェアを設定する](#)」を参照してください。

ソフトウェアの設定時には、Ami Alias も AMI ID と同じ場所にあります。Ami Alias は AMI ID と似たような ID ですが、その方が自動化で簡単に使用できます。AMI alias は `aws/service/marketplace/prod-<identifier>/<version>` の形式で、例えば `aws/service/marketplace/prod-1234example5678/12.2` などです。この Ami Alias ID はどのリージョンでも使用でき、 によって自動的に正しいリージョン にマッピング AWS されますAMI ID。

製品の最新バージョンを使用する場合は、「」のバージョン `latest` の代わりに という用語を使用します。AMI alias これにより、 は など、製品の最新バージョン AWS を選択します `aws/service/marketplace/prod-1234example5678/latest`。

Warning

`latest` オプションを使用すると、ソフトウェアの最新リリースバージョンが表示されます。ただし、この機能を使用するには注意する必要があります。例えば、ある製品にバージョン 1.x と 2.x がある場合、2.x を使用している可能性があります。ここで、製品の最新リリースバージョンは 1.x のバグ修正である場合があります。

AMI エイリアスの使用例

AMI エイリアスは自動化に役立ちます。これらは、AWS CLI または テンプレートで AWS CloudFormation 使用できます。

次の例では、AWS CLIを使用することにより、AMI エイリアスを使用してインスタンスエイリアスを起動しています。

```
aws ec2 run-instances
--image-id resolve:ssm:/aws/service/marketplace/<identifier>/version-7.1
--instance-type m5.xlarge
--key-name MyKeyPair
```

次の例は、インスタンスを作成するための入力パラメータとして AMI エイリアスを受け入れる CloudFormation テンプレートを示しています。

```
AWSTemplateFormatVersion: 2010-09-09

Parameters:
  AmiAlias:
    Description: AMI alias
    Type: 'String'
```

```
Resources:
  MyEC2Instance:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Sub "resolve:ssm:${AmiAlias}"
      InstanceType: "g4dn.xlarge"
      Tags:
        -Key: "Created from"
          Value: !Ref AmiAlias
```

コンテナ製品

コンテナ製品は、コンテナイメージとして提供されるスタンドアロン製品です。コンテナ製品は無料の場合もありますが、販売者が提供する料金オプションによって支払いが必要な場合もあります。コンテナ製品は、[Amazon Elastic Container Service](#) (Amazon ECS)、[Amazon Elastic Kubernetes Service](#) (Amazon EKS)、さらに独自のインフラストラクチャ上で実行されるサービスなど、複数のコンテナランタイムやサービスで使用できます。サポートされているランタイムとサービスのすべてのリストと、それぞれの詳細については、「[コンテナ製品向けのサポート対象のサービス](#)」を参照してください。

コンテナ製品は、AWS Marketplace ウェブサイトまたは Amazon ECS コンソールで検出、サブスクライブ、デプロイできます。タスク定義や Helm チャートなど、販売者が提供するデプロイテンプレートを使用して、Amazon ECS や Amazon EKS に多くの製品をデプロイできます。また、製品にサブスクライブした後に、プライベート [Amazon Elastic Container Registry](#) (Amazon ECR) リポジトリからコンテナイメージに直接アクセスできます。

製品で が有効になっている場合は QuickLaunch、数ステップで Amazon EKS クラスターでコンテナ製品をすばやくテストできます。QuickLaunch は AWS CloudFormation を使用して Amazon EKS クラスターを作成し、コンテナソフトウェアを起動します。での起動の詳細については QuickLaunch、「」を参照してください [QuickLaunch の AWS Marketplace](#)。

このセクションでは、AWS Marketplaceでのコンテナ製品の検索、サブスクリプション、起動について説明しています。

有料コンテナ製品の料金モデル

有料コンテナ製品には、1 つ以上の料金モデルが必要です。の他の有料製品と同様に AWS Marketplace、有料コンテナ製品には料金モデル AWS に従って によって課金されます。料金モデル

には、固定月額料金と時間単位の料金があります。時間単位の料金は秒単位でモニタリングして日割り計算されます。料金の詳細は、製品登録時に詳細ページに表示されます。

でサポートされているコンテナ製品の料金モデル AWS Marketplace は次のとおりです。

- 無制限の使用を提供する固定月額料金。
- 長期契約期間中の製品使用に対する前払い料金。
- 製品の使用状況に基づく pay-as-you-go モデル (通常は時間単位)。
- 契約料金の pay-up-front モデル。

各モデルの詳細については、「AWS Marketplace 販売者ガイド」の「[コンテナ製品料金表](#)」を参照してください。

コンテナと Kubernetes の概要

[Docker](#) コンテナなどのコンテナは、仮想化されたオペレーティングシステム (Linux や Windows Server など) に対して抽象化と自動化の追加レイヤーを提供する、オープンソースのソフトウェアテクノロジーです。仮想マシンがサーバーイメージのインスタンスであるのと同様に、コンテナは Docker コンテナイメージのインスタンスです。コンテナでは、サーバーアプリケーションソフトウェアが、その実行に必要なあらゆるもの (コード、ランタイム、システムツール、システムライブラリなど) が含まれているファイルシステムでラップされます。コンテナを使用することにより、ソフトウェアは環境に関係なく常に同じように動作します。

Java 仮想マシンと同様に、コンテナでは、変換レイヤーとオーケストレーションレイヤーを提供し、オペレーティングシステムとコンテナ間および各コンテナ間を分離するための、基盤となるプラットフォームが必要です。Docker コンテナで使用できるさまざまな Docker 互換ランタイムおよびオーケストレーションサービスがあります。Amazon ECS は、用の非常にスケーラブルで高性能なオーケストレーションサービスです。AWS Amazon EKS は、オープンソースの管理およびオーケストレーションサービスである [Kubernetes](#) を使用してコンテナ化されたアプリケーションのデプロイ、管理、スケーリングを容易にします。

コンテナ製品の検索とサブスクリプション

コンテナ製品は、コンテナイメージで起動 AWS Marketplace できる 内の製品です。コンテナ製品には AWS Marketplace、販売者がコンテナイメージ、Helm チャート、または Amazon EKS のアドオン配信方法を使用してフルフィルメントオプションを提供した の製品が含まれます。コンテナ製品の配信方法の詳細については、「[コンテナ製品の配信方法](#)」を参照してください。

コンテナ製品のフルフィルメントオプションには、サポート対象のサービスとも呼ばれる多くの起動環境が用意されています。起動環境には Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS) などのサービスや、独自のセルフマネージド型インフラストラクチャが含まれます。使用可能なコンテナ製品の起動環境の詳細なリストについては、「[コンテナ製品向けのサポート対象のサービス](#)」を参照してください。

AWS Marketplace ウェブサイトでコンテナ製品を閲覧する

[AWS Marketplace ウェブサイト](#)でコンテナ製品を閲覧できます。

AWS Marketplace ウェブサイトを使用してコンテナ製品を参照するには

1. [\[AWS Marketplace 検索ページ\]](#) に移動します。
2. コンテナイメージまたは Helm チャートで、配信方法をフィルタリングします。
3. (オプション) サポート対象のサービスをフィルタリングして、製品を起動できるサービスで検索結果を絞り込みます。

関心のある製品が見つかったら、タイトルを選択して [\[製品の詳細\]](#) ページに移動します。

[\[コンテナ製品の詳細\]](#) ページ

の製品の詳細ページには AWS Marketplace、以下の情報を含む製品の詳細が表示されます。

- [\[製品概要\]](#) - 概要には、製品の説明と次の情報が含まれます。
 - 表示されている製品のバージョン。
 - 販売者のプロフィールへのリンク。
 - この製品が属する製品カテゴリ。
 - このソフトウェアを実行するためにサポートされているオペレーティングシステム。
 - ソフトウェアの起動に使用できる配信方法。
 - この製品を起動できるサポート対象のサービス。
- [\[料金情報\]](#) - 製品には、無料利用枠、Bring Your Own License (BYOL)、pay-up-front 契約料金、固定月額料金、年間料金、時間料金 pay-as-you-go のいずれかが適用されます。料金モデルの詳細については、「[コンテナ製品料金表](#)」を参照してください。
- [\[使用状況情報\]](#) - 販売者が提供するフルフィルメントオプションと、ソフトウェアの起動と実行の手順が記載されています。各製品には少なくとも1つのフルフィルメントオプションが必要で、最大5つまで指定できます。各フルフィルメントオプションには、配信方法と、ソフトウェアの起動と実行の手順が記載されています。

- [サポート情報] - このセクションには、製品のサポートを受ける方法と返金ポリシーに関する詳細が含まれています。
- [カスタマーレビュー] - 他のユーザーからの製品レビューを検索したり、自分でレビューを書いたりできます。

製品をサブスクライブするには、[製品の詳細] ページで [サブスクライブを続ける] を選択します。製品のサブスクリプションの詳細については、「[AWS Marketplaceで製品をサブスクライブする](#)」を参照してください。

AWS Marketplaceで製品をサブスクライブする

製品を使用するには、まずその製品をサブスクライブする必要があります。サブスクリプションページでは、有料製品の料金情報を確認でき、ソフトウェアのエンドユーザー使用許諾契約 (EULA) にアクセスできます。

コンテナ契約料金の製品の場合は、契約料金を選択し、[契約に同意する] を選択して続行します。製品のサブスクリプションが作成され、その製品を使用するための使用権限が提供されます。サブスクリプションが完了するまでに 1~2 分程度かかります。有料製品の使用権限を受け取った後、その製品の使用を開始すると課金されます。そのソフトウェアの実行中のインスタンスを 1 つでも削除せずにサブスクリプションをキャンセルした場合、ソフトウェアの使用状況に対する課金は継続されます。また、その製品の使用に関連するインフラストラクチャの料金が発生する場合があります。たとえば、ソフトウェア製品をホストするために新規 Amazon EKS クラスターを作成した場合は、そのサービスに対して課金されます。

Note

コンテナベースの製品をサブスクライブしてデプロイする方法については、次の動画も参照してください。

- [Amazon ECS クラスターへの AWS Marketplace コンテナのデプロイ \(3:34\)](#)
- [Amazon ECS Anywhere を使用して AWS Marketplace コンテナベースの製品をデプロイする \(5:07\)](#)
- [Amazon EKS アドオンの管理](#)

コンテナ製品の配信方法

の製品は、販売者がコンテナイメージ、Helm チャート、または Amazon EKS 用アドオンのいずれかの配信方法を使用して少なくとも 1 つのフルフィルメントオプションを提供している場合、コンテナ製品 AWS Marketplace と見なされます。

コンテナイメージの配信方法

コンテナイメージの配信方法を使用するフルフィルメントオプションについては、販売者が提供した手順に従って製品を販売します。これは、Amazon Elastic Container Registry の AWS Marketplace レジストリから Docker イメージを直接プルすることによって行われます。この配信方法による起動の詳細については、「[コンテナイメージのフルフィルメントオプションで起動する](#)」を参照してください。

Helm チャートの配信方法

Helm チャートの配信方法を使用するフルフィルメントオプションについては、販売者が提供した手順またはデプロイテンプレートに従って製品を販売します。これを行うには、Helm CLI を使用して Helm チャートをインストールします。アプリケーションは、既存の Amazon EKS クラスター、EKS Anywhere のセルフマネージド型クラスター、Amazon Elastic Compute Cloud (Amazon EC2)、またはオンプレミスで起動できます。この配信方法による起動の詳細については、「[Helm フルフィルメントオプションで起動する](#)」を参照してください。

Amazon EKS アドオンの配信方法

Amazon EKS アドオンの配信方法を使用したフルフィルメントオプションの場合、Amazon EKS コンソールまたは Amazon EKS CLI を使用して製品を起動します。Amazon EKS アドオンの詳細については、「[Amazon EKS アドオン](#)」を参照してください。

コンテナ製品向けのサポート対象のサービス

次のリストには、AWS Marketplace のコンテナ製品でサポート対象のすべてのサービスが含まれています。サポート対象のサービスとは、製品を起動できるコンテナサービスまたは環境です。コンテナ製品には、1 つ以上の環境への起動手順が記載された配信方法を含むフルフィルメントオプションが少なくとも 1 つ含まれている必要があります。

Amazon ECS

Amazon Elastic Container Service (Amazon ECS) は、スケーラビリティの高い、高速のコンテナ管理サービスで、クラスターでコンテナの実行、停止、管理に使用できます。コンテナは、個々の

タスクやサービス内のタスクを実行するために使用するタスク定義で定義されます。ここでのサービスとは、クラスター内で指定された数のタスクを同時に実行および維持する構成のことです。タスクとサービスは、によって管理されるサーバーレスインフラストラクチャで実行できます AWS Fargate。または、インフラストラクチャをより詳細に制御するために、管理する Amazon EC2 インスタンスのクラスターでタスクとサービスを実行できます。

Amazon ECS の詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「[Amazon Elastic Container Service とは](#)」を参照してください。

Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) は、AWS で Kubernetes を簡単に実行できるようにするマネージド型サービスです。独自の Kubernetes コントロールプレーンまたはノードをインストール、操作、維持する必要はありません。Kubernetes は、コンテナ化されたアプリケーションのデプロイ、スケーリング、および管理を自動化するためのオープンソースシステムです。

Amazon EKS コンソールを使用して、サードパーティーの Kubernetes ソフトウェアを検索、サブスクライブ、デプロイできます。詳細については、「Amazon EKS ユーザーガイド」の「[Amazon EKS アドオンの管理](#)」を参照してください。

セルフマネージド型 Kubernetes

コンテナ製品は、EKS Anywhere で実行中のセルフマネージド型 Kubernetes クラスター、Amazon ECS Anywhere、Amazon EC2、またはオンプレミスのインフラストラクチャで起動できます。

Amazon ECS Anywhere は Amazon ECS の機能の 1 つで、顧客が管理するインフラストラクチャ上でコンテナワークロードを実行および管理するために使用できます。Amazon ECS Anywhere は Amazon ECS を基盤としており、コンテナベースのアプリケーション全体で整合性のあるツールと API エクスperiエンスを提供します。

詳細については、「[Amazon ECS Anywhere](#)」を参照してください。

EKS Anywhere は、顧客が管理するインフラストラクチャに Amazon EKS クラスターを作成するために使用できるサービスです。EKS Anywhere は、サポートされていないローカル環境としてデプロイすることも、サポート対象のオンプレミスの Kubernetes プラットフォームとして使用できる本番環境としてデプロイすることもできます。

EKS Anywhere の詳細については、[EKS Anywhere ドキュメント](#)を参照してください。

Amazon ECS コンソールを使用してコンテナ製品を閲覧する

Amazon ECS コンソールでコンテナ製品を見つけることもできます。ナビゲーションペインには、からの新製品を検出 AWS Marketplace したり、既存のサブスクリプションを表示したりするためのリンクがあります。

サブスクリプションのキャンセル

製品のサブスクリプションをキャンセルするには [Your Software (ソフトウェア)] ページを使用します。

契約料金によるコンテナ製品

一部の販売者は、契約料金モデルでパブリックコンテナベースのソフトウェア製品を提供しています。このモデルでは、選択した期間において、ソフトウェア製品にアクセスするための個別のライセンス数量に対して一括前払いすることに同意することになり、お客様の AWS アカウントを通じて事前に請求されます。

Example 異なるライセンスを異なる数量で購入する例

例えば、1 年間に 10 件のユーザーアクセスライセンスと 5 件の管理ライセンスを購入するとします。ライセンスを自動的に更新するように選択できます。

さらに、一部の企業では、契約料金モデルでプライベートコンテナベースのソフトウェア製品を提供しています。通常、プライベートオファーは期間が決まっており、変更できません。

コンテナベースのソフトウェア製品の契約は、AWS Marketplace の [製品の詳細] ページから購入できます。このオプションが利用可能な場合、商品の詳細ページの [配信方法] に、[契約料金による AMI] が表示されます。製品を購入すると、アカウントのセットアップと設定を行うために、製品のウェブサイトが表示されます。その後、使用料は通常の AWS アカウント 請求レポートに表示されます。

で契約料金のパブリックオファーを使用してコンテナ製品をサブスクライブする AWS Marketplace

契約料金モデルによるパブリックオファーのコンテナベースの製品をサブスクライブするには

Note

Amazon EKS を使用してサブスクライブする方法の詳細については、「[Amazon EKS アドオンの管理](#)」を参照してください。

1. にサインイン AWS Marketplace し、契約料金モデルを使用してコンテナベースのソフトウェア製品を検索します。

2. [調達] ページで、[料金情報] を表示します。

各期間 (月単位) に対する [単位] と料金を確認できます。

3. サブスクリプションを開始するには、[サブスクライブを続ける] を選択します。

サブスクライブせずにこの製品を保存するには、[リストに保存する] を選択します。

4. 料金情報を確認し、ソフトウェア製品の条件を設定して契約を作成します。

a. [1 か月]、[12 か月]、[24 か月]、[36 か月] の中から契約期間を選択します。

b. [更新設定] で、契約を自動的に更新するかどうかを選択します。

c. [契約オプション] で、各単位の数量を選択します。

契約料金の合計は、[料金の詳細] に表示されます。

5. すべての選択を完了したら、[契約書を作成] を選択します。

合計契約料金が^g に請求 AWS アカウント され、ライセンスが^g で生成されます AWS License Manager。

Note

サブスクリプションを処理し、ソフトウェア製品のライセンスが License Manager アカウントに生成されるまで、最大 10 分かかる場合があります。

で契約料金のプライベートオファーを使用してコンテナ製品をサブスクライブする AWS Marketplace

契約料金モデルによるプライベートオファーのコンテナベースの製品をサブスクライブするには

Note

Amazon EKS を使用してサブスクライブする方法の詳細については、「[Amazon EKS アドオンの管理](#)」を参照してください。

1. 購入者アカウント AWS Marketplace でサインインします。
2. プライベートオファーが表示されます。
3. [調達] ページで、[料金情報] を表示します。

各期間 (月単位) の [単位] と料金を確認できます。

4. [サブスクライブを続ける] を選択して、サブスクリプションを開始します。
5. 料金情報を確認し、ソフトウェア製品の条件を設定して契約を作成します。

契約期間は既に販売者が設定しており、変更できません。

6. [契約オプション] で、各単位の数量を選択します。
7. [料金の詳細] で契約料金の合計を表示します。

また、パブリックオファーは、[ご利用いただけるその他のオファー] の [オファーを表示] を選択して確認できます。

8. すべての選択を完了したら、[契約書を作成] を選択します。

Note

サブスクリプションを処理し、ソフトウェア製品のライセンスが License Manager アカウントに生成されるまで、最大 10 分かかる場合があります。

ソフトウェアへのアクセス

コンテナベースのソフトウェア製品にアクセスするには

1. AWS Marketplace コンソールで、「サブスクリプションを表示」に移動し、ソフトウェア製品のライセンスを表示します。
2. [調達] ページで、次の手順を実行します。
 - a. ライセンスの管理 を選択して、 で使用権限の表示、アクセス許可の付与、使用状況の追跡を行います AWS License Manager。
 - b. [Continue to Configuration (設定に進む)] を選択します。
3. [起動] ページで、コンテナイメージの詳細を確認し、表示される手順に従います。

Amazon Elastic Container Service (Amazon ECS) クラスターを作成する場合、IAM ポリシーに次の AWS Identity and Access Management (IAM) アクセス許可を追加する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "license-manager:CheckoutLicense",
        "license-manager:GetLicense",
        "license-manager:CheckInLicense",
        "license-manager:ExtendLicenseConsumption",
        "license-manager:ListReceivedLicenses"
      ],
      "Resource": "*"
    }
  ]
}
```

生成されたライセンスを表示する

生成されたライセンスを表示するには

1. AWS License Manager で にサインインします AWS アカウント。

2. [付与されたライセンス] には、付与されたライセンスがすべて表示されます。
3. [検索] バーに、製品 SKU、受取人、または状態を入力してライセンスを検索します。
4. [ライセンス ID] を選択すると、[ライセンスの詳細] が表示されます。
5. [発行者] (AWS/Marketplace) および [使用権限] (ライセンスによってアプリケーションやリソースの使用、アクセス、消費する権限を与える単位) を表示できます。

既存の契約を変更する

コンテナ製品に対する既存の前払いコミットメントがある場合、AWS Marketplace 購入者は契約の一部を変更できます。コンテナ契約は、時間単位または年単位の Flexible Consumption Pricing (FCP) オファーではなく、契約条件ベースのオファーによってサポートされています。この機能は、と統合されているアプリケーションでのみ使用できます AWS License Manager。購入者は、現在の契約と同一オファーの使用権限の範囲内で、追加ライセンスを購入できます。ただし、購入者は契約で購入した使用権限の数を減らすことはできません。また、販売者がオプションを有効にしている場合、購入者はサブスクリプションの自動更新をキャンセルできます。

Note

Flexible Payment Schedule (FPS) 契約のオファーは変更できません。FPS で購入した契約では、購入者が使用権限を変更することはできません。使用権限とは、アプリケーションやリソースを使用、アクセス、消費する権利のことです。FPS オファーは変更できません。

サブスクリプションを管理する

1. AWS Marketplace コンソールで、「サブスクリプションを表示」に移動し、ソフトウェア製品のライセンスを表示します。
2. [調達] ページで [ライセンスを管理] を選択します。
3. リストから [条件を表示] を選択します。
4. [契約オプション] セクションで、矢印を使って使用権限を増やします。使用権限の数は、購入した使用権限の数よりも減らすことはできません。
5. 契約の詳細と合計金額は [料金の詳細] セクションに表示されます。

サブスクリプションの自動更新をキャンセルするには

1. AWS Marketplace コンソールで、「サブスクリプションを表示」に移動し、ソフトウェア製品のライセンスを表示します。
2. [調達] ページで [ライセンスを管理] を選択します。
3. [サブスクリプション] ページで、[更新設定] セクションを見つけます。
4. キャンセルに関する利用規約を必ずご確認ください。
5. チェックボックスをオンにすると、自動更新オプションがキャンセルされます。

AWS Marketplaceからのコンテナソフトウェアの起動

でコンテナ製品へのアクティブなサブスクリプションを取得したら AWS Marketplace、次のステップはソフトウェアを起動することです。ソフトウェアを起動するには、販売者が提供する配信オプションのいずれかに記載されている指示に従ってください。では AWS Marketplace、フルフィルメントオプションは、環境で製品を起動するための、販売者が用意したオプションの手順です。コンテナ製品の場合、販売者は最大 4 つのフルフィルメントオプションを提供でき、それぞれ異なる配信方法を使用したり、異なるソフトウェアの構成を示したりすることができます。例えば、販売者は製品のテストに使用するフルフィルメントオプションと、企業内で大規模にデプロイするフルフィルメントオプションを作成する場合があります。

どのフルフィルメントオプションがあるかは、AWS Marketplaceの [製品の詳細] ページの [使用情報] セクションで確認できます。各フルフィルメントオプションには、サポートされているサービスに関する情報と、ソフトウェアバージョンの詳細が含まれています。サービスの例には、Amazon Elastic Container Service (Amazon ECS) および Amazon Elastic Kubernetes Service (Amazon EKS) が含まれます。[使用手順] を選択すると、製品の使用方法 (ウェブサーバーへのサインイン方法や起動後の設定方法など) に関する販売者からのドキュメントを参照できます。

Note

コンテナベースの製品をサブスクライブしてデプロイする方法については、次の動画も参照してください。

- [Amazon ECS クラスターへの AWS Marketplace コンテナのデプロイ \(3:34\)](#)
- [Amazon ECS Anywhere を使用して AWS Marketplace コンテナベースの製品をデプロイする \(5:07\)](#)

[ECS Anywhere を使用して AWS Marketplace のコンテナベースの製品をデプロイする](#)

からコンテナソフトウェアを起動する AWS Marketplace

からコンテナソフトウェアを起動するには AWS Marketplace

1. [AWS Marketplace](#) にサインインします。
2. を参照して AWS Marketplace、起動するソフトウェアを含む製品を見つけます。ソフトウェアを起動するには、製品のサブスクリプションが必要です。でコンテナ製品を検索してサブスクライブする方法については AWS Marketplace、「」を参照してください [コンテナ製品の検索とサブスクライブ](#)。
3. [製品の詳細] ページで [サブスクライブを続ける] を選択します。
4. [Continue to Configuration (設定に進む)] を選択します。ボタンが表示されない場合は、最初の利用規約に同意する必要があるか、製品のサブスクリプションがない可能性があります。
5. [フルフィルメントオプション] で、販売者が提供したオプションのリストからフルフィルメントオプションを選択します。フルフィルメントオプションを選択すると、[サポート対象のサービス] で開始できるサービスが表示されます。フルフィルメントオプションの詳細については、「[コンテナ製品のフルフィルメントオプション](#)」を参照してください。
6. [Continue to Launch] (続行して起動する) を選択します。
7. 販売者が提供する手順に従って製品を起動します。手順は、フルフィルメントオプションによって異なります。詳細については、[コンテナイメージのフルフィルメントオプションで起動する](#) または [Helm フルフィルメントオプションで起動する](#) を参照してください。
8. オプション - [使用手順] を選択すると、起動後の製品の設定方法や使用方法について、販売者からのドキュメントが表示されます。

コンテナ製品のフルフィルメントオプション

利用可能なフルフィルメントオプションは、[製品の詳細] ページの [使用情報] セクションで確認できます。販売者が提供するフルフィルメントオプションに加えて、には、Amazon Elastic Container Registry (Amazon ECR) から直接 Docker イメージをプルする手順 AWS Marketplace が含まれています。

フルフィルメントオプションは販売者によって提供されるため、それらの名前とコンテンツはの製品ごとに異なります AWS Marketplace。配信方法は製品や販売者によって異なりますが、各フルフィルメントオプションには配信方法が必要です。配信方法は、フルフィルメントオプションの種類

と考えることができます。コンテナ製品には、コンテナイメージ、Helm チャート、Amazon EKS アドオンの 3 つの配信方法があります。

コンテナイメージのフルフィルメントオプションで起動する

コンテナイメージの配信方法を使用するフルフィルメントオプションについては、販売者が提供した手順に従って製品を販売します。これは、Amazon ECR から Docker イメージを直接プルすることによって行われます。製品を起動する一般的なステップは次のとおりです。

1. AWS Command Line Interface (AWS CLI) と Docker の最新バージョンがインストールされていることを確認します。詳細については、「Amazon Elastic Container Registry ユーザーガイド」の「[AWS CLIで Amazon ECR を使用する](#)」を参照してください。
2. Amazon ECR レジストリに対し、Docker クライアントを認証します。これを行うステップは、オペレーティングシステムによって異なります。
3. 提供された Amazon ECR イメージの Amazon リソースネーム (ARN) を使用して、すべての Docker イメージをプルします。詳細については、「Amazon Elastic Container Registry ユーザーガイド」の「[イメージのプル](#)」を参照してください。
4. 製品の使用方法については、販売者から提供されている使用手順や外部リンクを確認してください。

Helm フルフィルメントオプションで起動する

Helm の配信方法を使用するフルフィルメントオプションについては、販売者が提供した手順に従って製品を販売します。これを行うには、Helm CLI を使用して Helm チャートをインストールします。アプリケーションは、既存の Amazon EKS クラスタ、EKS Anywhere のセルフマネージド型クラスタ、Amazon Elastic Compute Cloud (Amazon EC2)、またはオンプレミスで起動できます。

Note

起動環境には、Helm CLI バージョン 3.7.1 を使用する必要があります。Helm バージョンのリストについては、「」の「[Helm リリース GitHub](#)」を参照してください。

販売者が を有効にしている場合は QuickLaunch、それを使用してアプリケーションを起動できます。QuickLaunch は、 を使用して Amazon EKS クラスタ AWS CloudFormation を作成し、そのクラスタでアプリケーションを起動 AWS Marketplace する の機能です。の詳細については、QuickLaunch 「」を参照してください[QuickLaunch の AWS Marketplace](#)。

手順は販売者が提供するもので、販売者や製品ごとに異なります。Helm フルフィルメントオプションによる製品を起動する一般的な手順は次のとおりです。

Helm フルフィルメントオプションによる製品を起動するには


1. [からコンテナソフトウェアを起動する AWS Marketplace](#) のステップ 1~6 に従い、Helm チャートの配信方法を含むフルフィルメントオプションを選択します。
2. [起動ターゲット] で、デプロイする環境を選択します。
 - [Amazon マネージド型 Kubernetes] を選択し、Amazon EKS でアプリケーションをデプロイします。販売者が を有効にしている場合は QuickLaunch、それを使用して新しい Amazon EKS クラスターを作成し、起動できます。
 - [セルフマネージド型 Kubernetes] を選択すると、[EKS Anywhere](#)、Amazon EC2 またはオンプレミスで実行中の任意の Kubernetes クラスターにアプリケーションをデプロイできます。
3. Amazon マネージド型 Kubernetes クラスターで起動する場合:
 - a. Amazon EKS の既存のクラスターで起動するには、[起動方法] で [既存のクラスターで起動する] を選択し、[起動手順] に従います。手順には、AWS Identity and Access Management (IAM) ロールの作成とアプリケーションの起動が含まれます。Helm CLI バージョン 3.7.1 を使用していることを確認します。
 - b. QuickLaunch を使用して新しい Amazon EKS クラスターを作成して起動するには、起動方法で、 を使用して新しい EKS クラスターで起動 QuickLaunchを選択します。コンソールでスタックを作成するためにリダイレクトする起動を選択します AWS CloudFormation 。このスタックによって Amazon EKS クラスターを作成し、販売者が提供した Helm チャートをインストールしてアプリケーションをデプロイします。
 - c. [スタックのクイック作成] ページの [スタック名] に、このスタックの名前を入力します。
 - d. [パラメータ] タイルの情報を確認し、必要な情報を入力します。[機能] に表示される確認事項を確認して選択し、[スタックを作成] を選択します。

Note

AWS CloudFormation、スタック QuickLaunch、作成された Amazon EKS クラスターなど、の詳細については、「」を参照してください [QuickLaunch の AWS Marketplace](#)。

4. セルフマネージド型 Kubernetes クラスターで起動する場合:

- a. Helm CLI バージョン 3.7.1 を使用していることを確認します。
- b. [トークンを作成] を選択して、ライセンストークンと IAM ロールを生成します。このトークンとロールは、と通信 AWS License Manager して製品の使用権限を検証するために使用されます。

 Note

アカウントのライセンストークンの最大数は 10 です。

- c. [CSV 形式でダウンロード] を選択して、生成されたトークン情報を含む .csv のファイルをダウンロードします。すべてのシークレットやパスワードと同様に、.csv ファイルは安全な場所に保存します。
- d. [Kubernetes シークレットとして保存] のコマンドを実行して、ライセンストークンと IAM ロールを Kubernetes クラスターのシークレットとして保存します。このシークレットは、Helm チャートをインストールしてアプリケーションを起動するときに使用されます。AWS Marketplace はシークレットを使用して、この製品の使用権限を検証します。
- e. [トークンを使用してアプリケーションを起動する] のコマンドを実行して、アプリケーションをクラスターにデプロイする Helm チャートをインストールします。
- f. [使用手順] を選択すると、起動後の製品の設定方法や使用方法について、販売者からのドキュメントが表示されます。
- g. オプション - [[オプション] アーティファクトをダウンロード] に記載されているコマンドを使用して、製品のコンテナイメージと Helm チャートをローカルにダウンロードします。

Amazon EKS フルフィルメントオプションで起動する

Amazon EKS アドオンの配信方法を使用したフルフィルメントオプションの場合、Amazon EKS コンソールを使用して、Amazon EKS クラスターにソフトウェアをデプロイします。製品を起動する一般的なステップは次のとおりです。

Amazon EKS フルフィルメントオプションによる製品を起動するには

1. 製品をサブスクライブしたら、[設定] ページに移動し、[Amazon EKS コンソールに進む] を選択して Amazon EKS コンソールにアクセスします。
2. Amazon EKS コンソールから、クラスター AWS リージョン がデプロイされている を選択します。ソフトウェアをデプロイするクラスターを選択します。
3. [アドオン] タブを選択します。

4. [アドオンをさらに追加] を選択し、スクロールしてデプロイするアドオンを検索し、[次へ] を選択します。
5. デプロイするバージョンを選択し、[次へ] を選択します。Amazon EKS のデプロイの詳細については、「[EKS アドオン](#)」を参照してください。
6. 場所を確認して [作成] を選択します。

QuickLaunch の AWS Marketplace

販売者がフルフィルメントオプション QuickLaunch で を有効にしている場合は、それを使用して Amazon EKS クラスターを作成し、コンテナアプリケーションをデプロイできます。では QuickLaunch、AWS CloudFormation を使用して Amazon EKS クラスターを設定および作成し、そのクラスターでコンテナアプリケーションを起動します。を使用すると QuickLaunch、テスト目的でコンテナアプリケーションを起動できます。を使用するには QuickLaunch、「」のステップに従います[Helm フルフィルメントオプションで起動する](#)。

アプリケーションをデプロイできる Amazon EKS クラスターを作成するには、スタックを作成します CloudFormation。スタックは、単一のユニットとして管理できる AWS リソースのコレクションです。スタック内のすべてのリソースは、スタックの CloudFormation テンプレートによって定義されます。では QuickLaunch、スタックのリソースには、Amazon EKS クラスターを作成してアプリケーションを起動するために必要な情報が含まれています。のスタックの詳細については AWS CloudFormation、「AWS CloudFormation ユーザーガイド」の「[スタックの使用](#)」を参照してください。

クラスターが作成されると、 は、販売者提供の Helm チャートをクラスターにインストールして、そのクラスターでアプリケーション QuickLaunch を起動します。QuickLaunch は、Amazon EKS クラスターも作成するスタック作成の一環としてこれを処理します。

Machine Learning 製品

AWS Marketplace には、 を通じてサブスクライブできる機械学習製品のカテゴリがあります AWS Marketplace。その製品カテゴリは [Machine Learning] です。このカテゴリの製品には、機械学習 (ML) モデルパッケージとアルゴリズムがあります。

さまざまなサブカテゴリ (コンピュータビジョン、自然言語処理、音声認識、テキスト、データ、音声、イメージ、動画分析、不正検出、予測分析など) で、何百もの ML モデルパッケージとアルゴリズムを参照および検索できます。

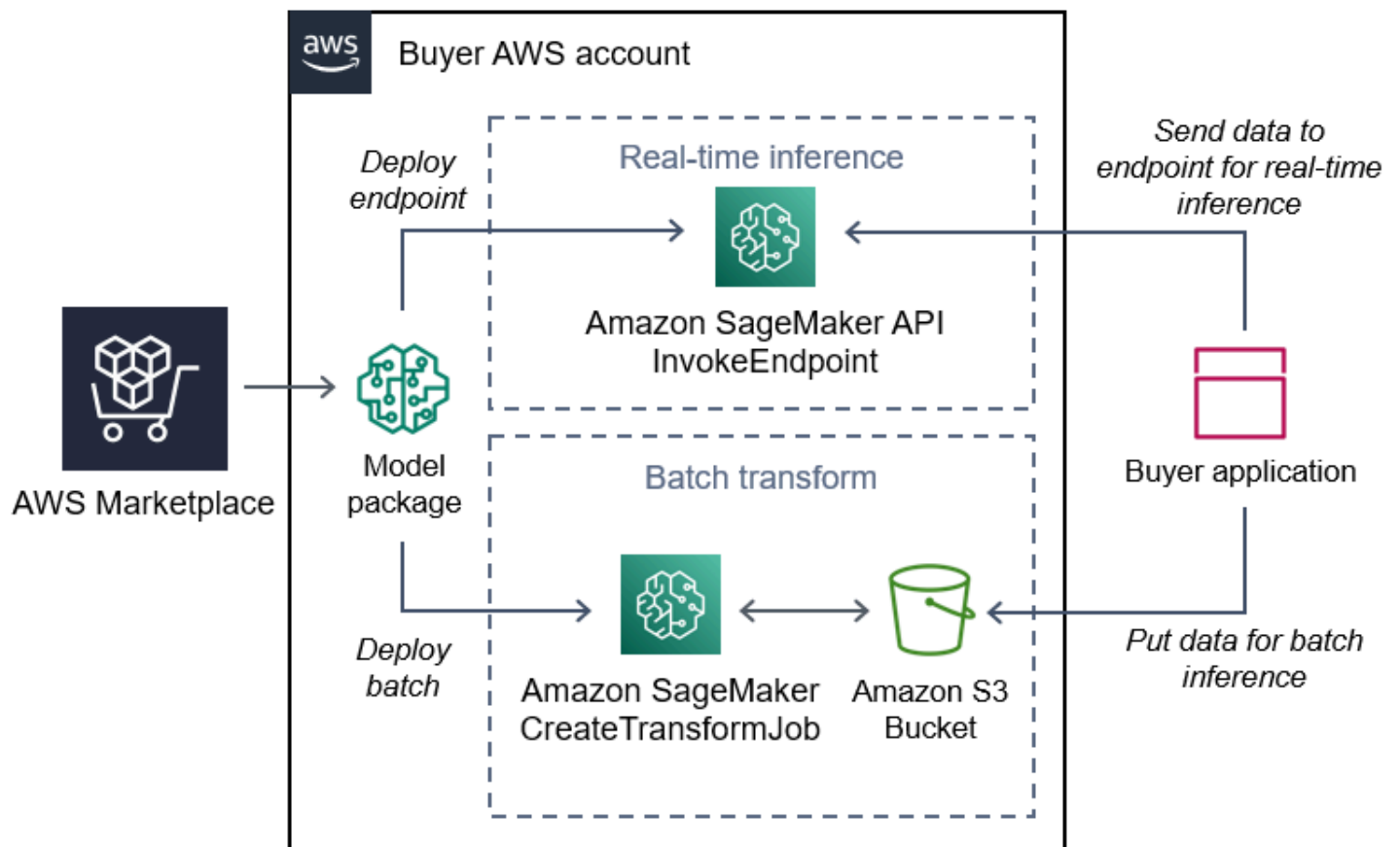
モデルの品質や適合性を評価するために、製品説明、使用手順、お客様のレビュー、サンプルの [Jupyter ノートブック](#)、料金情報、およびサポート情報を確認できます。Amazon SageMaker コンソールから直接、Jupyter Notebook を介して、Amazon SageMaker SDK を使用して、または を使用してモデルをデプロイします AWS Command Line Interface AWS CLI。Amazon SageMaker は、すべてのマーケットプレイス製品に対して静的スキャンを実行することで、トレーニングジョブと推論ジョブを実行するための安全な環境を提供します。

Amazon SageMaker モデルパッケージ

Amazon SageMaker モデルパッケージは、Amazon の Amazon リソースネーム (ARN) によって識別される一意の事前トレーニング済み ML モデルです SageMaker。お客様はモデルパッケージを使用して Amazon でモデルを作成します SageMaker。次に、モデルをホスティングサービスで使用してリアルタイム推論を実行するか、バッチ変換で Amazon でバッチ推論を実行できます SageMaker。

次の図は、モデルパッケージ製品を使用するワークフローを示しています。

1. で AWS Marketplace、モデルパッケージ製品を見つけてサブスクライブします。
2. 製品の推論コンポーネントを にデプロイ SageMaker して、リアルタイムまたはバッチで推論 (または予測) を実行します。



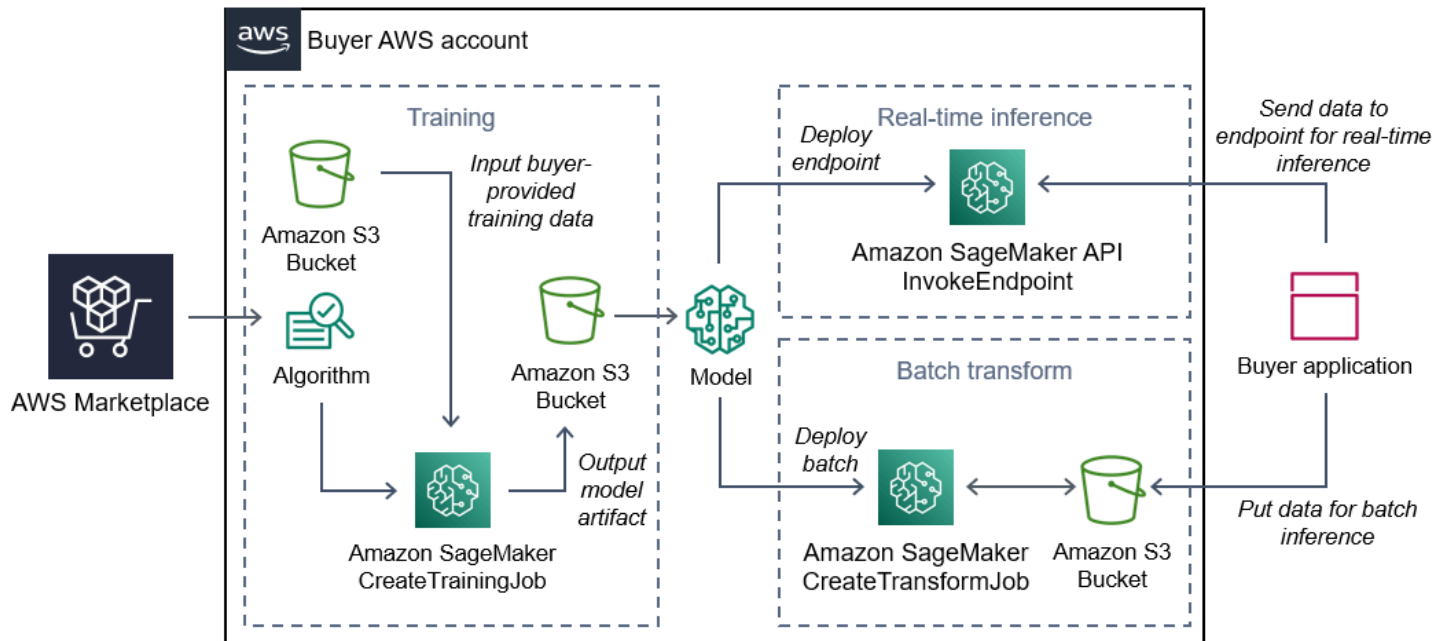
Amazon SageMaker アルゴリズム

Amazon SageMaker アルゴリズムは、ARN によって識別される一意の Amazon SageMaker エンティティです。アルゴリズムには、トレーニングと推論という 2 つの論理コンポーネントがあります。

次の図は、アルゴリズム製品を使用するワークフローを示しています。

1. で AWS Marketplace、アルゴリズム製品を見つけてサブスクライブします。
2. 製品のトレーニングコンポーネントを使用して、Amazon の入力データセットを使用して機械学習モデル SageMaker を構築するトレーニングジョブまたはチューニングジョブを作成します。
3. 製品のトレーニングコンポーネントが完了すると、機械学習モデルのアーティファクトが生成されます。
4. SageMaker は、モデルアーティファクトを Amazon Simple Storage Service (Amazon S3) バケットに保存します。

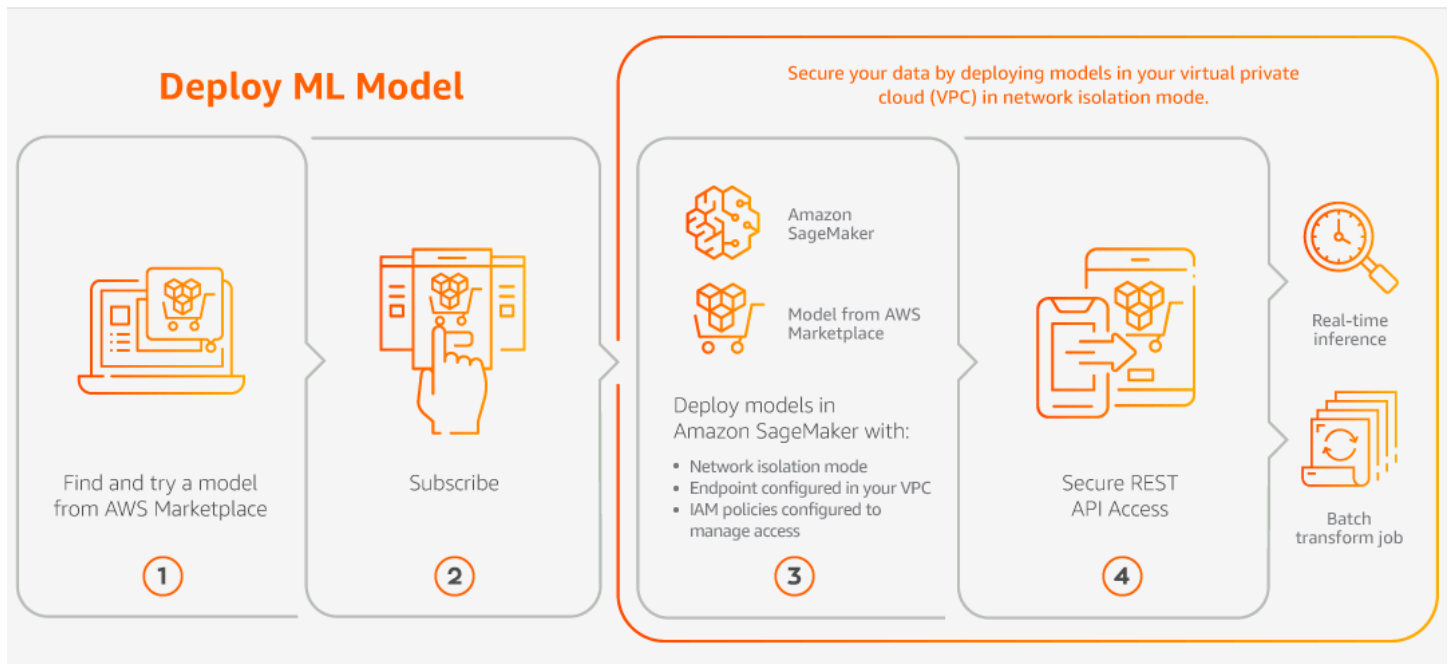
5. では SageMaker、生成されたモデルアーティファクトを使用して製品の推論コンポーネントをデプロイし、リアルタイムまたはバッチで推論 (または予測) を実行できます。



検索、サブスクリプション、デプロイ

次の図は、Amazon で機械学習製品を検索、サブスクリプション、デプロイするプロセスの概要を示しています SageMaker。

1. からモデルを検索して試す AWS Marketplace
2. ML 製品をサブスクリプションする
3. Amazon にモデルをデプロイする SageMaker
4. 安全な REST API を使用する
5. 実行
 - リアルタイム推論
 - バッチ変換ジョブ



最低料金や前払いのコミットメントなしで、使用量に対してのみお支払いいただきます。AWS Marketplace は、アルゴリズムとモデルパッケージ、および AWS インフラストラクチャ使用料金の一括請求を提供します。

次のセクションでは、ML 製品の検索、サブスクライブ、デプロイする方法について説明します。

トピック

- [機械学習製品の検索](#)
- [機械学習製品をサブスクライブする](#)
- [機械学習製品をデプロイする](#)

機械学習製品の検索

Amazon SageMaker モデルパッケージとアルゴリズムを検索するには

1. [AWS Marketplace ウェブサイト](#) にサインインします。
2. 「ニーズを満たす AWS Marketplace 製品を検索する」で、カテゴリドロップダウンメニューを使用して、関心のある Machine Learning のサブカテゴリを見つけます。
3. リソースタイプ、カテゴリ、および料金プランのフィルターを適用して検索結果を絞り込むことができます。
4. 検索結果から、[製品の詳細] ページにアクセスします。

5. 製品の説明、使用方法、カスタマーレビュー、データ要件、サンプル Jupyter Notebook、料金とサポート情報を確認してください。

機械学習製品をサブスクライブする

Amazon SageMaker モデルパッケージとアルゴリズムをサブスクライブするには

1. [製品の詳細] ページで [サブスクライブを続ける] を選択します。
2. 調達ページで、製品の料金情報とエンドユーザー使用許諾契約 (EULA) を確認します。
3. [サブスクリプションを続行する] を選択します。

機械学習製品をデプロイする

Amazon SageMaker モデルパッケージとアルゴリズムをデプロイするには

1. [\[Marketplace ソフトウェア\]](#) に移動して、有効なアルゴリズムまたはモデルパッケージのサブスクリプションがあることを確認します。
2. AWS Marketplace ウェブサイトで製品を設定します (特定のバージョンやデプロイリージョンを選択するなど)。

モデルパッケージ製品またはアルゴリズム製品をサブスクライブすると、SageMaker コンソールの製品リストに追加されます。AWS SDKs、AWS Command Line Interface (AWS CLI)、または SageMaker コンソールを使用して、フルマネージド REST 推論エンドポイントを作成したり、データのバッチに対して推論を実行したりすることもできます。

3. Amazon で表示 を選択して、Amazon SageMaker SageMaker 製品の詳細ページを表示します。
4. Amazon SageMaker コンソールから、Amazon コンソール、Jupyter Notebook SageMaker、Amazon SageMaker CLI コマンド、または API オペレーションを使用してモデルパッケージとアルゴリズムをデプロイできます。

Amazon でのデプロイの詳細については SageMaker、[「の開始方法」](#) を参照してください。

プロフェッショナルサービス製品

AWS Marketplace には、AWS Marketplace 販売者からのプロフェッショナルサービスである製品が含まれています。これらの製品は、AWS Marketplace の [プロフェッショナルサービス] カテゴリで検索すると見つかります。これらの製品を [を通じて](#) サブスクライブして購入しますが AWS

Marketplace、販売者と協力して、ニーズを満たすプロフェッショナルサービスをセットアップします。

プロフェッショナルサービスの購入

AWS Marketplaceの [プロフェッショナルサービス] カテゴリを使用してプロフェッショナルサービスを検索できます。関心のある製品が見つかったら、販売者にオファーをリクエストしてください。通常、プロフェッショナルサービスでは連携が必要なため、購入を完了するには販売者に追加情報を提供する必要があります。また、この機会を利用して、料金や解決が必要なその他のサービスの詳細について交渉できます。製品のプライベートオファーが届きます。詳細については、「[プライベートオファー](#)」を参照してください。

プロフェッショナルサービス製品を購入するには

1. [AWS Marketplace](#) にアクセスして AWS アカウントにサインインし、購入するプロフェッショナルサービス製品を検索して検索します。
2. その製品の [製品の詳細] ページで、[続行] を選択します。
3. [サービスのリクエスト] ページで、販売者がオファーを作成するのに必要な追加情報を追加します。これには、名前、E メールアドレス、会社名その他、ビジネスニーズ、タイムライン、契約要件など、販売者に有益な追加情報が含まれます。
4. 販売者は、提供された E メールアドレスを使用してお客様に連絡し、オファーの詳細を検討します。同意すると、販売者は のオファーへのリンクを送信します AWS Marketplace。ブラウザでリンクを開き、AWS アカウントにサインインします。
5. 販売者によって開かれた [調達] ページで、オファーの詳細を確認します。そのオファーが、期待したサービスと料金に合っていることを確認してください。一括払いなのか、分割払いなのかといった条件も確認してください。オファーが正しければ、続行します。それ以外の場合は、販売者に連絡して変更を加えます。
6. [契約を設定] で、契約に使用する設定を選択します。例えば、サポート契約を購入する場合、Silver、Gold、Platinum のオプションがあり、それぞれ料金が異なります。
7. [契約書を作成] を選択してサービスを購入します。2 営業日以内に、販売者からサービスの使用方法を連絡します。

SaaS 製品

Software as a Service (SaaS) 製品の場合、 を通じて製品をサブスクライブしますが AWS Marketplace、ソフトウェア販売者の環境で製品にアクセスします。

トピック

- [料金モデル](#)
- [クイック起動](#)

料金モデル

AWS Marketplace では、以下の料金モデルを提供しています。

SaaS 使用量ベースのサブスクリプション

SaaS 使用量ベースのサブスクリプションでは、ソフトウェア販売者が使用量を追跡し、ユーザーは使用した分の料金だけを支払います。この pay-as-you-go 料金モデルは、多くの の料金モデルと似ています AWS のサービス。SaaS 製品の使用量に対する請求は、AWS の請求書で管理されます。

SaaS 使用量ベースサブスクリプションを使用してサブスクライブするには

1. 製品詳細ページで [購入オプションを表示] を選択し、サブスクリプションプロセスを開始します。
2. サブスクリプション内容を確認し、サブスクリプションページで [サブスクライブ] を選択します。

Note

一部の製品には、ソフトウェアの設定、デプロイ、起動に必要な時間とリソースを削減できるクイック起動デプロイオプションが用意されています。これらの製品はクイック起動バッジで識別されます。詳細については、「[the section called “クイック起動”](#)」を参照してください。

SaaS の前払いのコミットメント

一部の企業では、を通じて SaaS 契約を事前に購入できます AWS Marketplace。このオプションでは、これらの製品のライセンスまたはデータインジェストを個別に購入できます。その後、を通じてこれらの製品を事前に請求できます AWS アカウント。たとえば、1年間のユーザーアクセスライセンスを 10 個購入したり、1日に 10 GB のデータを取り込める 1年間のサービスを購入したりできます。

製品を購入すると、クイック起動が有効になっていない場合にはアカウントのセットアップと設定を行う製品のウェブサイトに移動します。その後、使用料は通常の AWS アカウント 請求レポートに表示されます。

Note

クイック起動エクスペリエンスについて詳しくは、「[the section called “クイック起動”](#)」を参照してください。

SaaS 契約でサブスクライブするには

1. 製品詳細ページで [購入オプションを表示] を選択し、サブスクリプションプロセスを開始します。必要な量かユニット、サブスクリプションの期間 (複数のオプションを使用できる場合)、および自動更新を選択できます。
2. すべての選択を完了したら、[Create Contract (契約の作成)] を選択します。
3. [Set Up Your Account (アカウントのセットアップ)] を選択すると、製品を提供する会社のウェブサイトに移動します。アカウントが設定されていて、支払いが検証されている間、製品 AWS Marketplace の詳細ページに契約が保留されていることが表示されます。

Note

一部の製品には、ソフトウェアの設定、デプロイ、起動に必要な時間とリソースを削減できるクイック起動デプロイオプションが用意されています。これらの製品はクイック起動バッジで識別されます。詳細については、「[the section called “クイック起動”](#)」を参照してください。

設定が完了すると、製品ページにアカウントを設定するためのリンクが表示されます。AWS Marketplace ソフトウェアは、アカウントにサインインすると Marketplace ソフトウェアの下に表示されます。これでソフトウェアの使用を開始できます。アカウントのセットアッププロセスを完了しない場合は、AWS Marketplace でその製品を保持するときにセットアップを完了するように求められます。

ソフトウェア会社のウェブサイトで作成したアカウントを使用して、その会社のウェブサイトからソフトウェアサブスクリプションにアクセスします。AWS Marketplace アカウントにサインインしたときに Marketplace Software AWS Marketplace で購入したソフトウェアサブスクリプションのウェブサイトリンクも参照できます。

SaaS 無料トライアル

一部のベンダーでは、AWS Marketplace 評価目的でを通じて SaaS 製品の無料トライアルを提供しています。で SaaS 製品を検索 AWS Marketplace し、結果をフィルタリングして、無料トライアルがある製品のみを表示できます。検索結果には、どの製品が無料トライアルを提供しているかがわかります。すべての無料トライアル製品には、製品ロゴの横に [無料トライアル] バッジが表示されます。製品調達ページでは、無料試用期間と試用版に含まれる無料ソフトウェアの使用量を確認できます。

無料トライアル中、または無料トライアルの有効期限が切れた後は、プライベートオファーを交渉するか、パブリックオファーに登録することにより、購入を決定できます。SaaS の無料トライアルは、自動的に有料契約に切り替わりません。無料トライアルが不要になった場合は、期限切れにできません。

AWS Marketplace コンソールからサブスクリプションの管理を選択すると、サブスクリプションを表示できます。

Note

各 AWS アカウント は、製品ごとに 1 つの無料トライアルのみの対象となります。

SaaS 契約無料トライアルオファーのサブスクリプション

SaaS 契約無料トライアルオファーをサブスクライブするには

1. AWS Marketplace コンソールにサインインし、AWS Marketplace メニューから製品の検出を選択します。
2. [結果の絞り込み] パネルで [無料トライアル] に移動し、[無料トライアル] を選択します。
3. [配信方法] には [SaaS] を選択します。
4. [料金モデル] で [前払いのコミットメント] を選択すると、無料トライアルを提供するすべての製品が表示されます。対象となるすべての製品には、[無料トライアル] バッジが表示されます。
5. 必要な SaaS 製品を選択します。
6. [製品の詳細] ページから [無料で試す] を選択します。
7. [オファータイプ] には、[無料トライアル] オプションを選択します。
8. [購入] では、[契約書を作成] を選択し、[契約に同意する] を選択します。
9. [アカウントのセットアップ] を選択して登録を完了し、ソフトウェアの使用を開始します。

SaaS サブスクリプション無料トライアルオファ어의サブスクリプション

SaaS サブスクリプション無料トライアルオファ어를サブスクライブするには

1. AWS Marketplace コンソールにサインインし、AWS Marketplace メニューから製品の検出を選択します。
2. [結果の絞り込み] パネルで [無料トライアル] に移動し、[無料トライアル] を選択します。
3. [配信方法] には [SaaS] を選択します。
4. [料金モデル] で [使用量ベース] を選択すると、無料トライアルを提供するすべての製品が表示されます。対象となるすべての製品には、[無料トライアル] バッジが表示されます。
5. 必要な SaaS 製品を選択します。
6. [製品の詳細] ページから [無料で試す] を選択します。
7. [オファertype] には、[無料トライアル] オプションを選択します。
8. [購入] には [サブスクライブ] を選択します。

クイック起動

クイック起動は、クイック起動が有効になっている SaaS 製品で使用できる AWS Marketplace デプロイオプションです。これにより、ソフトウェアの設定、デプロイ、起動に必要な時間、リソース、手順が削減されます。この機能を提供する製品では、クイック起動を使用するか、リソースを手動で設定するかを選択できます。

クイック起動エクスペリエンスを使用して SaaS 製品を検索、サブスクライブ、起動するには

1. [\[AWS Marketplace 検索ページ\]](#) に移動します。
2. を参照して AWS Marketplace、起動するソフトウェアを含む製品を見つけます。クイック起動エクスペリエンスを提供する製品には、製品説明にクイック起動バッジが付いています。

Tip

クイック起動エクスペリエンスが有効になっている製品を検索するには、結果の絞り込みペインで SaaS フィルターと CloudFormation テンプレートフィルターを使用します。

3. 製品をサブスクライブしたら、[アカウントの設定] ボタンを選択して [設定と起動] ページに移動します。

4. **ステップ 1: 必要なアクセス許可があることを確認する** の設定と起動ページで、**クイック起動エクスペリエンス**を使用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。AWS AWS 管理者に連絡してアクセス許可をリクエストしてください。

クイック起動エクスペリエンスをフル活用するには、次のアクセス許可が必要です。

- `CreateServiceLinkedRole` – `AWSServiceRoleForMarketplaceDeployment` サービスにリンクされたロールを作成 AWS Marketplace できるようにします。このサービスにリンクされたロールにより、 は AWS Marketplace 、ユーザーに代わって にシークレットとして保存されるデプロイ関連のパラメータを管理 AWS Secrets Manager できます。
 - `DescribeSecrets` — 販売者が渡したデプロイパラメータに関する情報の取得 AWS Marketplace を許可します。
 - `GetRole` — AWS Marketplace サービスにリンクされたロールがアカウントで作成されたかどうかを が判断できるようにします。
 - `ListSecrets` – AWS Marketplace デプロイパラメータのステータスの取得を許可します。
 - `ListRegions` – 現在のアカウント AWS Marketplace でオプトインされている AWS リージョン の取得を許可します。
 - `ReplicateSecrets` — ソフトウェアをデプロイする選択したリージョンへのシークレットのレプリケーションを開始 AWS Marketplace できるようにします。
5. 「**ステップ 2: 既存または新規のベンダーアカウントにログインする**」で、**[ログインまたはアカウントを作成]** ボタンを選択します。販売者のサイトが新しいタブで開き、そこでログインするか、新しいアカウントを作成できます。完了したら、**[設定と起動]** ページに戻ります。
 6. **ステップ 3: ソフトウェアと AWS 統合 を設定する** で、製品の**設定方法**を選択します。
 - `AWS CloudFormation` – **起動テンプレート** ボタンを選択して、事前定義された `CloudFormation` テンプレートをデプロイし、製品を設定します。 `CloudFormation` を使用してテンプレートパラメータを確認し、追加の必須フィールドを入力します。完了したら、**[設定と起動]** ページに戻り、ソフトウェアを起動します。
 - **手動** — 販売者が提供する指示に従ってソフトウェアを設定します。
 7. 「**ステップ 4: ソフトウェアを起動する**」で、**[ソフトウェアを起動]** ボタンを選択してソフトウェアを起動します。

データ製品

を使用して AWS Marketplace、AWS Data Exchange で利用可能なデータ製品を検索してサブスクライブできます。詳細については、「AWS Data Exchange ユーザーガイド」の「[AWS Data Exchange でのデータ製品のサブスクライブ](#)」を参照してください。

製品への支払い

月初めに、Amazon Web Services (AWS) から AWS Marketplace 料金の請求書が届きます。ソフトウェア製品の場合、請求書には、ソフトウェアの時間単位料金に、このソフトウェアの Amazon マシンイメージ (AMI) インスタンスの実行時間数を掛けた計算結果が示されます。また、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Simple Storage Service (Amazon S3)、Amazon Elastic Block Store (Amazon EBS)、帯域幅などの AWS インフラストラクチャサービスの使用料金も請求されます。

AWS アカウントがトルコと南アフリカを除く欧州、中東、アフリカ (EMEA) を拠点とし、EMEA の対象となる販売者からの購入である場合、Amazon Web Services EMEA SARL () から請求書を受け取ります AWS Europe。AWS アカウントがオーストラリアに拠点を置く場合は、Amazon Web Services Australia Pty Ltd () から請求書を受け取ります AWS Australia。AWS アカウントが日本に拠点を置く場合は、Amazon Web Services Japan G.K (AWS Japan) から請求書を受け取ります。それ以外の場合は、AWS Inc. から請求書を受け取ります。

Note

AMI の年間購入および契約購入の場合、サブスクリプション料金の請求書は、一括月額請求ではなく、サブスクリプション時に発生します。AMI の年間購入では、サブスクリプション中に購入したすべてのインスタンスタイプを対象とする契約全体に対して 1 つの請求書が生成されます。契約の Flexible Payment は、予定されている支払い時に請求されます。使用量コンポーネント (pay-as-you-go モデルなど) を含む契約の場合、使用量は一括月額請求に表示されます。

AWS Marketplace 複雑なトポロジを使用する製品では、提供された AWS CloudFormation テンプレートによって起動された AMIs やその他の AWS インフラストラクチャサービスのクラスターに対して料金が発生する場合があります。

たとえば、EC2 スモールインスタンスタイプでソフトウェアを 720 時間実行したとします。ソフトウェア使用に対する販売者の料金は 0.12 USD/時間であり、EC2 料金は 0.085 USD/時間です。この場合、月末の請求額は 147.60 USD になります。

データ製品のサブスクリプションの詳細については、「AWS Data Exchange ユーザーガイド」の「[AWS Data Exchange でのデータ製品のサブスクリプション](#)」を参照してください。

AWS 請求書の支払いの詳細については、[AWS Billing 「ユーザーガイド」](#)を参照してください。

Amazon Web Services EMEA SARL (AWS Europe) での支払い管理の詳細については、「AWS Billing ユーザーガイド」の「[AWS Europe での支払いの管理](#)」を参照してください。

トピック

- [発注書](#)
- [返金に関する情報](#)
- [製品のサブスクリプションをキャンセルする](#)
- [支払い方法](#)
- [サポートされている通貨](#)
- [指定通貨の変更](#)
- [送金手順の更新](#)

発注書

AWS Marketplace および AWS Billing コンソールで発注書を使用すると、お客様が定義した発注書番号 AWS を含む請求書が から届きます。この方法により、支払い処理とコスト配分が簡単になります。out-of-cycle では AWS Marketplace、請求書には、即時に請求されるか、プライベートオファーでスケジュールされた定義済みの支払いに従って請求される購入が含まれます。通常、pay-as-you-go 料金は AWS Marketplace 一括月次使用請求書に表示されます。

AWS Marketplace のトランザクションに発注書を使用する

トランザクション時に発注書を追加できます。これは、そのトランザクションに関連する後続のすべての out-of-cycle 請求書に適用されます。

次の製品は、発注書をサポートしています。

- Software as a Service (SaaS) 契約
- プロフェッショナルサービス製品
- サーバー製品 (AMI インスタンス、コンテナ、AWS CloudFormation テンプレート、年間料金モデルまたは契約料金モデルを含む Helm チャートを含む)

Note

年間料金モデルの発注書サポートは、Flexible Payment Schedule によるプライベートオファーでのみ利用可能です。

年間料金モデルの発注書は、Flexible Payment Schedule によるプライベートオファーでのみサポートされます。指定した発注書は、一括の AWS Marketplace 月別 pay-as-you-go 請求料金には適用されません。

Note

で発注書を使用するには AWS Marketplace、AWS 組織内の管理アカウントで AWS Billing 統合を有効にする必要があります。この 1 回限りの設定タスクにより、サービスにリンクされたロールが作成されます。このロールによって、組織内のアカウントに発注書の仕様をサブスクライブするアクセス許可を与えます。統合を有効にしないと、組織内のアカウントは調達中に発注書を追加できません。統合の詳細については、「[AWS Marketplaceのサービスにリンクされたロールの作成](#)」を参照してください。

で発注書を指定するには AWS Marketplace

1. から[サポートされている製品](#)を見つけて購入する準備をします AWS Marketplace。
2. 購入プロセス中に、[ソフトウェアサブスクリプションの設定] ページ (SaaS) の [発注書] で [発注書番号を追加] を選択します。
3. [発注書番号] フィールドに発注書番号を入力します。

発注書番号は、システム内で注文を追跡するために使用する番号またはテキストです。通常、社内システムまたはプロセスによって発行されます。最大 200 文字を使用できます。

AWS Marketplace トランザクション中に提供された発注書を含む発注書の詳細については、[AWS Billing コンソールの発注書ダッシュボード](#) を使用してください。

一括使用発注書を使用する

他の発注書から AWS Marketplace 請求を分離するには、AWS Billing コンソールで AWS Marketplace 一括使用明細項目を使用して発注書を作成できます。AWS Marketplace 請求書トランザクションには、特定の条件とパラメータが一致する場合に指定する一括使用発注書 (請求エンティティなど) が含まれます。例外は、AWS Marketplace トランザクション発注書を指定した請求書です out-of-cycle。詳細については、「AWS Billing and Cost Management ユーザーガイド」の「[発注書の管理](#)」を参照してください。

発注書に関するトラブルシューティング

次の表の情報は、発注書の問題のトラブルシューティングや、さまざまなシナリオで何が起こるかを理解するのに役立ちます。

シナリオ	詳細
アクセス権限の不足	aws-marketplace:Subscribe のアクセス許可がない場合は、[発注書エントリ] フィールドの近くに注意が表示されます。管理アカウントも AWS Billing 統合を有効にする必要があります。統合の有効化の詳細については、「 AWS Marketplaceのサービスにリンクされたロールの作成 」を参照してください。
発注書がない	AWS Marketplace は新しい発注書を作成します。新しい発注書にはデフォルトの情報が記載されており、連絡先の情報はありません。
発注書の通知が届かない	連絡先情報のない発注書 (によって作成された発注書を含む AWS Marketplace) は、Eメール通知を受信しません。 Billing and Cost Management コンソールの発注書ダッシュボード で、発注書に連絡先情報を追加できます。
誤った発注書番号が追加された	誤った注文番号を入力したために、更新する必要がある場合は、AWS Support に連絡して注文番号を更新するように依頼してください。
サブスクリプションアカウントが別の組織に移動した	発注書を新しい組織で機能させるには、新しい組織で統合を完了する必要があります。統合が完了し、発注書サポートが新しい組織で機能している場合、サブスクリプションアカウントが組織間を移動すると、新しい請求書には新しい組織の発注書番号が表示されます (必要に応じて新しい発注書が作成されます)。

シナリオ	詳細
チェックアウト時に発注書オプションが使用できない	この AWS Billing 統合は、SaaS 契約、プロフェッショナルサービス製品、契約料金のサーバー製品、および柔軟な支払いスケジュールのプライベートオファターの年間料金のサーバー製品でのみ使用できます。
この契約 pay-as-you-go	<p>契約に対する請求書には発注書番号が表示されますが、消費 (従量制料金) の請求書には発注書番号は表示されません。この pay-as-you-go モデルは、発注書番号の追加をサポートしていません。</p> <p>AWS Billing コンソールで、AWS Marketplace 一括使用明細項目 を含む発注書を追加することを検討してください。</p>
発注書の中断	発注書番号が指定され、Billing and Cost Management コンソールの発注書ダッシュボードで、発注書が中断としてマークされている場合、新しい明細目は発注書に追加されませんが、請求書には発注書は含まれません。の請求管理者は、発注書をアクティブにし、AWS Support に連絡してアクティブな発注書で請求書を再生成 AWS アカウント する必要があります。
発注書の有効期限切れ	発注書番号が指定され、発注書の有効期限が切れた場合、新しい明細項目が作成され、発注書が有効とマークされます。明細項目の終了日は、新しい発注書の有効期限として使用されません。
残高の追跡	残高追跡は AWS Marketplace 明細項目に対して有効になっていません。
調達システムの統合	統合調達システムによって提供された発注書は、請求書に表示されます。

シナリオ	詳細
Flexible Payment Schedule - 初回購入	請求日が決まっている契約 (Flexible Payment Schedule) では、発注書の最初の項目は 0 USD で生成されます。各請求書には、該当する料金の明細項目が作成されます。
Flexible Payment Schedule - 複数の発注書	フレキシブル支払いスケジュールの個別の支払いに異なる発注書を表示する必要がある場合は、AWS Support に連絡して、今後の請求書の発注書番号を変更してください。

返金に関する情報

お客様は AWS Marketplace、製品のさまざまなタイプの返金をリクエストできます。で販売されている AWS Marketplace 製品については AWS、返金ポリシーページを参照し、を使用して問い合わせサポートフォームを送信してください AWS Support Center Console。サードパーティーによって製品が販売された場合は、[製品の詳細] ページの返金ポリシーを確認してください。AWS Marketplace サブスクリプションのソフトウェア料金は製品の販売者に支払い、返金は販売者から直接リクエストする必要があります。各 AWS Marketplace 販売者は、AWS Marketplace ページに返金ポリシーを含める必要があります。

購入に関連する返金の詳細については AWS Marketplace、AWS Marketplace 販売者ガイドの以下のトピックを参照してください。

- [返金](#)
- [製品の料金](#)

Note

プライベートオファーに関連するすべての返金については、販売者にお問い合わせください。

製品のサブスクリプションをキャンセルする

AWS Marketplaceの製品のサブスクリプションまたは自動更新をキャンセルできます。次の手順では、AWS Marketplaceの Software as a Service (SaaS)、機械学習 (ML)、および Amazon マシンイメージ (AMI) 製品について説明しています。

トピック

- [SaaS サブスクリプションのキャンセル](#)
- [機械学習のサブスクリプションをキャンセルする](#)
- [AMI サブスクリプションのキャンセル](#)
- [SaaS 契約サブスクリプションの自動更新をキャンセルする](#)

SaaS サブスクリプションのキャンセル

1. にサインイン AWS Management Console し、[AWS Marketplace コンソール](#) を開きます。
2. [\[サブスクリプションの管理\]](#) ページに移動します。
3. 配信方法には、ドロップダウンリストから [SaaS] を選択します。
4. キャンセルする製品のサブスクリプションを選択します。
5. [Cancel subscription] を選択します。

機械学習のサブスクリプションをキャンセルする

機械学習のサブスクリプションをキャンセルする前に、次のアクションを実行してください。

- ML アルゴリズムの場合 – にサインイン AWS Management Console し、[Amazon SageMaker](#) コンソールを開きます。アルゴリズムに対して実行中のトレーニングジョブをすべて終了します。アルゴリズムからモデルパッケージを作成した場合は、機械学習のサブスクリプションがキャンセルされた後は、リアルタイムエンドポイントを起動したり、バッチ推論ジョブを作成したりすることはできません。
- アルゴリズムから作成された ML モデルパッケージまたはモデルの場合 – にサインイン AWS Management Console し、[Amazon SageMaker](#) コンソールを開きます。実行中のモデルのリアルタイムエンドポイントをすべて終了するか、実行中のバッチ推論ジョブをすべて終了します。

Note

終了していない既存のジョブやエンドポイントは実行が継続され、終了するまで課金されます。

機械学習のサブスクリプションをキャンセルするには

1. にサインイン AWS Management Console し、[AWS Marketplace コンソール](#) を開きます。
2. [\[マイサブスクリプション\]](#) ページに移動します。
3. キャンセルする製品のサブスクリプションを選択します。
4. [\[Cancel subscription\]](#) を選択します。サブスクリプションをキャンセルすると、アルゴリズムやモデルを起動できなくなります。

AMI サブスクリプションのキャンセル

1. にサインイン AWS Management Console し、[AWS Marketplace コンソール](#) を開きます。
2. [\[サブスクリプションの管理\]](#) ページに移動します。
3. 配信方法には、ドロップダウンリストから [\[Amazon マシンイメージ\]](#) を選択します。
4. キャンセルする製品のサブスクリプションを選択します。
5. [\[アクション\]](#) ドロップダウンリストから [\[サブスクリプションをキャンセル\]](#) を選択します。
6. 表示された「実行中のインスタンスがアカウントで課金されることを了解する」という情報を読み、チェックボックスをオンにします。 [\[Yes, cancel subscription\]](#) (はい、サブスクリプションをキャンセルします) を選択します。
7. 新しいタブで AWS コンソールで [管理](#) を開きます。
8. Amazon EC2 コンソールで実行中のインスタンスを終了します。複数のインスタンスを実行している場合は、すべてのインスタンスを終了する必要があります。また、該当する場合は AWS CloudFormation スタックを削除する必要があります。
9. [\[サブスクリプションの管理\]](#) タブに戻り、[\[はい、サブスクリプションをキャンセルします\]](#) を選択します。サブスクリプションをキャンセルすると、ソフトウェアにアクセスできなくなります。また、料金は請求されなくなります。

SaaS 契約サブスクリプションの自動更新をキャンセルする

1. にサインイン AWS Management Console し、[AWS Marketplace コンソール](#) を開きます。
2. [製品の詳細] ページに異動します。
3. [続行] を選択して [注文] ページに移動します。
4. [更新の変更] タブを選択し、[更新をキャンセル] を選択します。

支払い方法

を初めて作成するときは AWS アカウント、そのアカウントの支払い方法を設定します。[AWS Billing and Cost Management コンソール](#) を使用して、支払い方法を管理できます。手順については、「AWS Billing ユーザーガイド」の「[支払いの管理](#)」を参照してください。

支払いエラー

支払者アカウントでの支払い処理中にエラーが発生した場合は、支払い方法を更新してもう一度試してください。このエラーは、次の理由で発生する可能性があります。

- 支払い方法が見つからない、無効、またはサポートされていない。
- 支払いが拒否された。
- Amazon Internet Services Private Limited (AISPL) アカウントでは、契約料金モデルによる新規購入の際、デビットカードまたはクレジットカードの使用が制限されています。AISPL アカウントをお持ちの場合は、[AWS カスタマーサービス](#) に連絡して、デフォルトの支払い方法を更新してください。詳細については、AWS Marketplace ブログウェブサイトの「[を使用する AISPL のお客様向けのクレジットカードおよびデビットカードの購入の制限 AWS Marketplace](#)」を参照してください。
- プライベートオファーには、支払いスケジュールが含まれます。ただし、デフォルトの支払い方法は請求書発行条件に設定されていません。

更新された支払い方法が新規購入で利用できるようになるまで、最大 7 日間かかる場合があります。トラブルシューティングについては、[AWS Support](#) にお問い合わせください。

サポートされている通貨

次のリストには、Amazon Web Services EMEA SARL AWS、Amazon Web Services Australia、および Amazon Web Services Japan G.K でサポートされている既存の通貨がすべて含まれています。

Note

Amazon Internet Services Private Limited (AISPL) は、現在 AWS Marketplace でサポートされていないため、インドルピー (INR) はサポートされていない通貨です。詳細については、「[AWS アカウント と AISPL アカウントの違いは何ですか](#)」を参照してください。

Amazon Web Services でサポートされている通貨は次のとおりです。

- オーストラリアドル (AUD)
- 英国ポンド (GBP)
- カナダドル (CAD)
- デンマーククローネ (DKK)
- ユーロ (EUR)
- 香港ドル (HKD)
- 日本円 (JPY)
- ニュージーランドドル (NZD)
- ノルウェークローネ (NOK)
- シンガポールドル (SGD)
- 南アフリカランド (ZAR)
- スウェーデンクローナ (SEK)
- スイスフラン (CHF)
- 米ドル (USD)

Amazon Web Services EMEA SARL でサポートされている通貨は次のとおりです。

- 英国ポンド (GBP)
- デンマーククローネ (DKK)
- ユーロ (EUR)
- ノルウェークローネ (NOK)
- 南アフリカランド (ZAR)
- スウェーデンクローナ (SEK)

- スイスフラン (CHF)
- 米ドル (USD)

Amazon Web Services Australia でサポートされている通貨は次のとおりです。

- オーストラリアドル (AUD)
- 米ドル (USD)

Amazon Web Services Japan G.K. でサポートされている通貨は次のとおりです。

- 日本円 (JPY)
- 米ドル (USD)

指定通貨の変更

AWS Marketplace 購入は、 に指定した通貨で表示されます AWS アカウント。 [AWS Billing and Cost Management コンソール](#) で、アカウントに指定されている通貨を変更できます。手順については、「AWS Billing ユーザーガイド」の「[請求の支払いに使用する通貨の変更](#)」を参照してください。

Note

希望通貨を変更すると、送金手順が変更されます。更新された送金手順を表示するには、AWS Marketplace 請求書を参照するか、[AWS Billing and Cost Management コンソール](#) のアカウント設定ページを参照してください。

送金手順の更新

欧州、中東、アフリカ (EMEA) を AWS アカウント 拠点とする のお客様。ただし、トルコと南アフリカを除き、EMEA の対象となる販売者からソフトウェア製品を購入した場合は、Amazon Web Services EMEA SARL から請求書を受け取ります。Amazon Web Services EMEA SARL (AWS Europe) の請求書には AWS、Inc. とは異なる送金指示書があります。 [AWS Billing and Cost Management コンソール](#) にサインインすると、請求書に送金情報が表示されます。請求書の送金情報部分に記載されている銀行口座は、Amazon Web Services EMEA SARL を通じて購入した AWS クラウド サービスとは異なります。Amazon Web Services EMEA SARL は、ルクセンブルクの認可された電子金融機関である Amazon Payments Europe, S.C.A. を AWS Marketplace 請求書の支払い

プロセッサとして使用します。すべての請求は、全額決済される必要があります。請求金額の全額に満たない支払いは、お客様の銀行口座に返金されます。

次の表は、取引の種類、取引主体、対応する送金手順 (請求書の「電子送金詳細」に記載されているアカウント名) の概要を示しています。

取引の種類	取引主体	送金手順
AWS クラウド サービスの購入	Amazon Web Services EMEA SARL	Amazon Web Services EMEA SARL
対象となる AWS Marketplace 販売者	Amazon Web Services EMEA SARL	Amazon Payments Europe, S.C.A.
対象外 AWS Marketplace の販売者	AWS 株式会社	AWS

送金手順のために残高証明書を請求するには、請求またはアカウントのサポートを選択し、[\[AWSへのお問い合わせ\]](#) でアカウントおよび請求サポートケースを作成するか、<awslux-receivables-support@email.amazon.com> まで E メールメッセージを送信してください。

通貨設定をサポート対象通貨に変更する方法の詳細については、「AWS Billing ユーザーガイド」の[「請求書の支払いに使用する通貨の変更」](#)を参照してください。

Amazon Web Services EMEA SARL は、MasterCardVISA、および American Express クレジットカードによる電子送金による支払いを受け入れます。Diners Club または Discover のクレジットカードはご利用いただけません。

詳細については、「[AWS Marketplace 購入者の税務ヘルプ](#)」を参照してください。

コスト配分タグ

AWS Marketplace は、購入するソフトウェア製品のコスト配分タグ付けをサポートします。アクティブ化されたコスト配分タグを使用して、AWS コストと使用状況レポート AWS Cost Explorer、AWS 予算、またはその他のクラウドコスト分析ツールを通じて AWS Marketplace リソースの使用状況を特定および追跡できます。AWS Marketplace コストの分類と追跡を容易にするために、コスト配分タグを使用してコスト配分レポートでリソースコストを整理できます。

のコスト配分タグ AWS Marketplace は、次の 2 つのソースから取得されます。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに関連付けられる Amazon マシンイメージ (AMI) ソフトウェア製品のコストは、同じタグを継承します。これらのタグは、アカウントの AWS Billing and Cost Management コンソールでコスト配分タグとしてアクティブ化できます。AMI 製品でのコスト配分タグの使用の詳細については、「[AMI 製品のコスト配分タグ](#)」を参照してください。
- AMI、コンテナ、Software as a Service (SaaS) 製品には、ベンダーが提供するタグが付いている場合があります。例えば、ユーザー数で請求する SaaS 製品では、タグを使用して部門ごとの使用状況を識別できます。これらのタグの使用の詳細については、「[ベンダー計測タグ](#)」を参照してください。

コスト配分タグは、タグが Billing and Cost Management コンソールでアクティブ化された時点からのコストのみを追跡します。アカウントの請求情報とコスト管理コンソールにアクセスできるのは、AWS アカウント 所有者、AWS Organizations 管理アカウントの所有者、および適切なアクセス許可を持つユーザーのみです。コスト配分タグを使用するかどうかにかかわらず、請求額に変更はありません。コスト配分タグを使用するかどうかは、AWS Marketplace のソフトウェア製品の機能には影響しません。

EMEA 対象販売者からのサブスクリプションの場合、コストと使用状況レポートには AWS、契約当事者 (Amazon Web Services EMEA SARL) の列が含まれます。

ベンダー計測タグ

AWS Marketplace ベンダー計測を使用する 製品 (AMI、コンテナ、SaaS 製品を含む) には、ソフトウェアベンダーが顧客に追加サービスとして提供するタグがあります。これらのタグは、ベンダーが提供するメトリクス全体での AWS Marketplace リソースの使用状況を理解するのに役立つコスト配分タグです。これらのタグを使用して、AWS Cost Explorer Service、AWS Cost and

Usage Report AWS Budgets、またはその他のクラウドコスト分析ツールを通じてリソースの使用状況を特定および追跡 AWS Marketplace できます。

タグは、AWS Marketplace 製品の使用を開始し、ベンダーが計測レコードを に送信した後、AWS Billing コンソールに表示されます AWS Marketplace。前払いのコミットメントに基づいて製品を使用している場合は、その製品の使用量の計測を受け取ることはできません。そのため、AWS Billing コンソールにベンダー計測タグはありません。リンクされたアカウントを管理する場合は、 でタグを表示およびアクティブ化するための ModifyBillingと の両方のViewBillingアクセス許可が必要です AWS Billing。詳細については、「AWS 請求ユーザーガイド」の「[AWS Billing アクションポリシー](#)」を参照してください。

Note

ベンダー計測タグを有効にすると、コストと使用状況レポートのサイズが大きくなる場合があります。コストと使用状況レポートは Amazon S3 に保存されます。そのため、Amazon S3 のコストも増加する可能性があります。

すべての対象 AWS Marketplace 製品のベンダー計測タグを有効にするには

1. にサインイン AWS Management Console し、[AWS Billing コンソール](#) を開きます。次に、左側のナビゲーションペインで、[コスト配分タグ] を選択します。
2. [AWS生成のコスト配分タグ] タブを選択します。
3. `aws:marketplace:isv:` を検索して、ベンダー計測タグによるタグ付けをサポートするすべての製品のタグを見つけます。
4. すべてのタグのチェックボックスをオンにして、[有効化] を選択します。ベンダー計測タグは、24 時間以内に有効になります。

関連トピック

詳細については、次のトピックを参照してください。

- 「AWS Billing ユーザーガイド」の「[コスト配分タグの使用](#)」
- 「AWS Billing ユーザーガイド」の「[AWS 生成コスト配分タグの有効化](#)」

プライベートマーケットプレイス

プライベートマーケットプレイスは AWS アカウント、ビジネスユーザーやエンジニアリングチームなど、 のユーザーが から調達できる製品を制御します AWS Marketplace。上に構築されており AWS Marketplace、管理者は承認された独立系ソフトウェアベンダー (ISVs) と社内ポリシーに準拠した製品の厳選されたデジタルカタログを作成およびカスタマイズできます。のユーザーは、プライベートマーケットプレイスから承認済み製品 AWS アカウント を検索、購入、デプロイし、利用可能なすべての製品が組織のポリシーと標準に準拠していることを確認できます。

プライベートマーケットプレイスでは、 で利用可能な製品の幅広いカタログと AWS Marketplace、それらの製品のきめ細かな制御が可能です。を使用すると [AWS Organizations](#)、すべてのアカウントの管理を一元化し、アカウントを組織単位 (OUsにグループ化し、各 OU に異なるアクセスポリシーをアタッチできます。組織全体、1 つ以上の OUs、または組織内の 1 つ以上のアカウントに関連付けられた複数のプライベートマーケットプレイスエクスペリエンスを作成し、それぞれに独自の承認済み製品のセットを作成できます。AWS 管理者は、会社またはチームのロゴ、メッセージング、およびカラースキームに関する各プライベートマーケットプレイスエクスペリエンスに会社のブランドを適用することもできます。

このセクションでは、プライベートマーケットプレイスを購入者として使用方法について説明します。プライベートマーケットプレイスを管理者として管理する方法については、[プライベートマーケットプレイスの作成と管理](#) を参照してください。

メモ

- ([プライベートオファー](#)を通じて) シェアされたプライベート製品をプライベートマーケットプレイスに追加できます。詳細については、「[プライベートマーケットプレイスで製品をサブスクライブする](#)」を参照してください。
- プライベートマーケットプレイスでは、EULA EULAs がカスタマーアグリーメントまたは AWS の使用を管理する とのその他の契約に準拠するすべての製品に対する権利が AWS、自動的に付与されます AWS のサービス。顧客にはデフォルトで既にこれらの製品を利用する資格があるため、プライベートマーケットプレイスで承認した製品のリストには含まれません。お客様は Service Catalog を使用してこれらの製品のデプロイを管理できます。

製品の詳細ページの表示

ユーザーは、アカウントを管理するプライベートマーケットプレイスで許可されている製品のみをサブスクライブできます。製品の詳細ページを閲覧したり表示したりすることはできますが、サブスクリプションが有効になっているのは、プライベートマーケットプレイスに追加した製品のみです。製品がプライベートマーケットプレイスに含まれていない場合は、ページ上部に赤色のバナーが表示され、製品が AWS Marketplaceでの調達が承認されていないことを示します。

ソフトウェアリクエストが有効な場合、ユーザーは製品詳細ページで [リクエストを作成] を選択できます。ユーザーが [リクエストを作成] を選択すると、製品をプライベートマーケットプレイスで入手可能にするためのリクエストが管理者に送信されます。この機能の詳細については、「[ユーザーリクエストの管理](#)」を参照してください。

プライベートマーケットプレイスの製品へのサブスクライブ

ユーザーとしてプライベートマーケットプレイスで製品をサブスクライブするには、製品の詳細ページに移動し、[続行] を選択します。これにより、製品のサブスクリプションページにリダイレクトされます。サブスクリプションページで、設定を選択してから、[サブスクライブ] を選択できます。

プライベートマーケットプレイスで製品が承認されていない場合、[Subscribe (サブスクライブ)] は使用できません。現時点で製品の調達承認されていないことを示す赤色のバナーがページ上部に表示されます。ソフトウェアリクエストが有効な場合は、[Create request (リクエストの作成)] を選択して、プライベートマーケットプレイスに製品を追加するよう管理者にリクエストを送信できます。

プライベートマーケットプレイスで製品をサブスクライブする

一部の製品は、参照するために公開されていません AWS Marketplace。これらの製品は、販売者からプライベートオファーを受けた場合にのみ表示されます。ただし、プライベートマーケットプレイスの管理者が最初にプライベートマーケットプレイスに製品を追加した場合にのみ、サブスクライブできます。このため、プライベートオファーは、AWS アカウントと組織のプライベートマーケットプレイス管理者を含むアカウントの両方に拡張する必要があります。プライベートオファーがユーザーと管理者の両方に拡大されたら、プライベートマーケットプレイスの管理者はプライベートマーケットプレイスに製品を追加できます。製品が承認されると、他のプライベートオファーと同様に製品をサブスクライブできます。

プライベートマーケットプレイスへの製品の追加をリクエストする

ユーザーは、管理者にプライベートマーケットプレイスにない製品の追加をリクエストできます。リクエストを行うには、製品の詳細ページに移動して [Create request (リクエストの作成)] を選択し、製品をプライベートマーケットプレイスに追加するためのリクエストを管理者宛てに入力して、送信します。リクエストのステータスを追跡するには、左側のドロップダウンメニューで [Your Private Marketplace Requests (プライベートマーケットプレイスのリクエスト)] を選択します。

プライベートマーケットプレイスの作成と管理

プライベートマーケットプレイスを作成および管理するには、プライベートマーケットプレイスの管理アカウントまたは委任された管理者アカウントにサインインする必要があります。IAM ポリシーには AWS Identity and Access Management (IAM) `AWSPprivateMarketplaceAdminFullAccess` アクセス許可も必要です。このポリシーをユーザー、グループ、およびロールに適用するための詳細については、「[the section called “プライベートマーケットプレイスの管理者の作成”](#)」を参照してください。

Note

プライベートマーケットプレイスと AWS Organizations の統合がない現在のプライベートマーケットプレイスのお客様は、IAM `AWSPprivateMarketplaceAdminFullAccess` ポリシーを持つ組織内の任意のアカウントからプライベートマーケットプレイスを作成および管理できます。

このセクションでは、AWS Marketplace ウェブサイトを通じてプライベートマーケットプレイス管理者として実行できるタスクについて説明します。AWS Marketplace Catalog APIを使用してプライベートマーケットプレイスを管理することもできます。詳細については、「AWS Marketplace Catalog API リファレンス」の「[Working with a private marketplace](#)」を参照してください。

プライベートマーケットプレイスの開始方法

プライベートマーケットプレイスの使用を開始するには、AWS 管理アカウントにサインインし、[Private Marketplace](#) に移動して、次の前提条件を有効にします。

- 信頼されたアクセス – の信頼されたアクセスを有効にする必要があります。これにより AWS Organizations、組織の管理アカウントは、AWS サービスの AWS Organizations データへのアクセスを許可または取り消すことができます。信頼されたアクセスを有効にすることは、プライベ

トマーケットプレイスがと統合 AWS Organizations し、プライベートマーケットプレイスを組織内の信頼されたサービスとして指定するために不可欠です。

- サービスにリンクされたロール – プライベートマーケットプレイスのサービスにリンクされたロールを有効にする必要があります。このロールは管理アカウントにあり、プライベートマーケットプレイスがユーザーに代わってプライベートマーケットプレイスリソースを記述 AWS Organizations および更新するために必要なすべてのアクセス許可が含まれています。サービスにリンクされたロールの詳細については、「」の「[ロールを使用した Private Marketplace の設定 AWS Marketplace](#)」を参照してください。

Note

現在のプライベートマーケットプレイスのお客様は、Private Marketplace 管理者のページに移動し、設定を選択することで、プライベートマーケットプレイスの設定を有効にできます。の信頼されたアクセスを有効に AWS Organizations し、サービスにリンクされたロールを作成することで、OUs をプライベートマーケットプレイスエクスペリエンスに関連付ける、委任された管理者を登録するなどの機能を利用できます。有効にすると、管理アカウントと委任された管理者アカウントのみがマーケットプレイスエクスペリエンスを作成および管理でき、既存のリソースは管理アカウントに転送され、委任された管理者のみと共有されます。信頼されたアクセスを無効にすると、組織のプライベートマーケットプレイスガバナンスが削除されます。プライベートマーケットプレイスにはアカウントグループが表示されません。組織のガバナンスをさまざまなレベルで表示するには、組織構造ページを使用します。ご質問やサポートについては、[にお問い合わせください](#)。

プライベートマーケットプレイスの管理

プライベートマーケットプレイスは、左側のペインの設定の Private Marketplace 管理者のページから管理できます。管理アカウント管理者と委任管理者は、このページを使用して、デフォルトのプライベートマーケットプレイスやライブエクスペリエンスの数など、プライベートマーケットプレイスの詳細を表示できます。

管理アカウント管理者は、このページを使用して以下の設定を管理することもできます。

委任された管理者

管理アカウント管理者は、プライベートマーケットプレイスの管理権限を、委任管理者と呼ばれる指定されたメンバーアカウントに委任できます。アカウントをプライベートマーケットプレイスの委任

管理者として登録するには、管理アカウント管理者が信頼されたアクセスとサービスにリンクされたロールが有効になっていることを確認し、新しい管理者の登録を選択し、12桁のAWSアカウント番号を指定して、送信を選択する必要があります。

管理アカウントと委任された管理者アカウントは、エクスペリエンスの作成、ブランド設定の更新、対象者の関連付けまたは関連付け解除、製品の追加または削除、保留中のリクエストの承認または拒否など、プライベートマーケットプレイスの管理タスクを実行できます。

信頼されたアクセスとサービスにリンクされたロール

管理アカウント管理者は、プライベートマーケットプレイスで次の機能を有効にできます。

Note

現在のプライベートマーケットプレイスのお客様は、Private Marketplace 管理者のページに移動し、設定を選択することで、プライベートマーケットプレイスの設定を有効にできます。の信頼されたアクセスを有効に AWS Organizations し、サービスにリンクされたロールを作成することで、OUs をプライベートマーケットプレイスエクスペリエンスに関連付ける、委任された管理者を登録するなどの機能を利用できます。有効にすると、管理アカウントと委任された管理者アカウントのみがマーケットプレイスエクスペリエンスを作成および管理でき、既存のリソースは管理アカウントに転送され、委任された管理者のみと共有されます。信頼されたアクセスを無効にすると、組織のプライベートマーケットプレイスガバナンスが削除されます。プライベートマーケットプレイスにはアカウントグループが表示されません。組織のガバナンスをさまざまなレベルで表示するには、組織構造ページを使用します。ご質問やサポートについては、[にお問い合わせください](#)。

- 信頼されたアクセス – の信頼されたアクセスを有効にする必要があります。これにより AWS Organizations、組織の管理アカウントは、AWS サービスの AWS Organizations データへのアクセスを許可または取り消すことができます。信頼されたアクセスを有効にすることは、プライベートマーケットプレイスがと統合 AWS Organizations し、プライベートマーケットプレイスを組織内の信頼されたサービスとして指定するために不可欠です。
- サービスにリンクされたロール – プライベートマーケットプレイスのサービスにリンクされたロールを有効にする必要があります。このロールは管理アカウントにあり、プライベートマーケットプレイスがユーザーに代わってプライベートマーケットプレイスリソースを記述 AWS Organizations および更新するために必要なすべてのアクセス許可が含まれています。サービスにリンクされたロールの詳細については、「」の「[ロールを使用した Private Marketplace の設定 AWS Marketplace](#)」を参照してください。

プライベートマーケットプレイスエクスペリエンスの作成

プライベートマーケットプレイスは 1 つ以上のプライベートマーケットプレイスエクスペリエンスで構成されます。エクスペリエンスは、組織全体、1 つ以上の OUs、または組織内の 1 つ以上のアカウントに関連付けることができます。AWS アカウント が組織のメンバーでない場合は、1 つのアカウントに関連付けられた 1 つのプライベートマーケットプレイスエクスペリエンスがあります。プライベートマーケットプレイスを作成するには、[プライベートマーケットプレイス](#)に移動し、左側の [エクスペリエンス] ページを選択して、[エクスペリエンスを作成] を選択します。

Note

でプライベートマーケットプレイスを使用するには AWS Organizations、組織のすべての機能を有効にする必要があります。詳細については、「AWS Organizations ユーザーガイド」の「[組織内のすべての機能の有効化](#)」を参照してください。
AWS アカウント が組織のメンバーでない場合は、プライベートマーケットプレイスを使用するための前提条件となる手順は必要ありません。

プライベートマーケットプレイスエクスペリエンスは、承認された商品やブランド要素なしで作成され、組織内のアカウントにも関連付けられていません。デフォルトでは有効になっていません。以下のトピックでは、プライベートマーケットプレイスエクスペリエンスを使用する方法について説明します。

プライベートマーケットプレイスエクスペリエンスへの製品の追加

プライベートマーケットプレイスエクスペリエンスに製品を追加するには

1. [プライベートマーケットプレイス] 管理者ページから、左側のナビゲーションペインで [エクスペリエンス] を選択します。次に、「製品」タブで、「すべての AWS Marketplace 製品」を選択します。製品名または販売者名で検索できます。
2. プライベートマーケットプレイスに追加する各製品の横にあるチェックボックスを選択してから、[Add to Private Marketplace] を選択します。

Note

赤いバナーの [プライベートマーケットプレイスに追加] ボタンを選択して、商品詳細ページから直接商品を追加することもできます。赤いバナーが製品ページに表示されていない場合、その商品は既にプライベートマーケットプレイスにあります。

左側のナビゲーションペインで [製品を一括追加/削除] を選択すれば、複数の製品を複数のエクスペリエンスに一度に追加することもできます。

プライベートマーケットプレイスエクスペリエンスでの製品の確認

プライベートマーケットプレイスエクスペリエンスで製品が承認されていることを確認するには

1. [プライベートマーケットプレイス] 管理者ページから、左側のナビゲーションペインで [エクスペリエンス] を選択します。
2. [承認された製品] を選択します。承認された製品はすべて承認済みリストに表示されます。

Note

編集中のエクスペリエンスに関連付けられているアカウントを使用していて、そのエクスペリエンスが有効になっている場合は、AWS Marketplace コンソール (<https://console.aws.amazon.com/marketplace>) で製品を直接表示することもできます。プライベートマーケットプレイスの一部であれば、検索結果のすべての製品に [調達の承認済み] のバッジが表示されます。

プライベートマーケットプレイスエクスペリエンスのカスタマイズ

エクスペリエンスは、1人以上のオーディエンスに関連付けることができる製品のサブセットおよび関連するブランドです。エクスペリエンスが組織に関連付けられている場合、または組織内の1つ以上のアカウントや組織単位を管理している場合、単一のプライベートマーケットプレイスエクスペリエンスで組織全体を管理できます。

エクスペリエンス設定は、左側のペインの「エクスペリエンス」の Private Marketplace 管理者のページから管理できます。このページを使用して、すべてのアクティブエクスペリエンスとアーカイブエクスペリエンスを表示および管理し、プライベートマーケットプレイスの新しいエクスペリエン

スを作成します。エクスペリエンスごとに、ロゴの追加、タイトルの追加、組織のカラースキームを使用するようにユーザーインターフェイスをカスタマイズできます。

対象者の管理

対象者とは、プライベートマーケットプレイスエクスペリエンスに関連付けることができる組織または組織単位のグループ (OUsまたはアカウントです。オーディエンスは、Private Marketplace 管理者のページ左側のペインの Experiences で作成できます。

1つ以上の対象者を エクスペリエンスに関連付けることができます。対象者の関連付けまたは関連付け解除を行うと、子 OUs とアカウントの管理エクスペリエンスが変わる可能性があります。組織構造ページを使用して、関連付けの影響を受けるアカウントと OUsを表示します。信頼されたアクセスを無効にすると、対象者の関連付けが解除され、すべてのガバナンスが削除されます。

Note

プライベートマーケットプレイスから組織の AWS Organizations 階層を表示し、ガバナンスを管理できます。プライベートマーケットプレイスを組織単位レベルで管理し、委任された管理者を登録するには、設定ページから信頼されたアクセスとサービスにリンクされたロールを有効にします。ご質問やサポートについては、[にお問い合わせください](#)。

プライベートマーケットプレイスの設定

エクスペリエンスの製品リスト、マーケットプレイスのブランド設定、関連するアカウントグループに問題がなければ、プライベートマーケットプレイスを公開できます。AWS Private Marketplace 管理者のページから、左側のナビゲーションペインでエクスペリエンスを選択し、有効にするエクスペリエンスを選択します。[設定] タブでは、プライベートマーケットプレイスのステータスを [ライブ] (有効) と [非ライブ] (無効) に変更できます。

[ソフトウェアリクエスト] を使用して、ユーザーがソフトウェアリクエストを送信できるように選択することもできます。ソフトウェアリクエストが [オン] (有効) の場合、エンドユーザーは製品詳細ページで [リクエストを作成] を選択し、プライベートマーケットプレイスで製品を利用できるようにするリクエストを管理者に送信できます。ソフトウェアリクエストはデフォルトで有効になっており、プライベートマーケットプレイスが有効になっている間のみ設定を変更できます。

プライベートマーケットプレイスがライブの場合、エンドユーザーは承認した製品のみを購入できます。プライベートマーケットプレイスを無効にした場合は、製品のリストが保持されます。ただし、プライベートマーケットプレイス無効にすると、AWS Organizations 組織のユーザーに対

する制限が解除されます。その結果、パブリック内の任意の製品をサブスクライブできます AWS Marketplace。

プライベートマーケットプレイスをライブ化しても、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで実行されているアクティブな Amazon マシンイメージ (AMI) が中断されることはありません。ベストプラクティスとして、組織全体で現在使用されているすべての AWS Marketplace 製品がプライベートマーケットプレイスに含まれていることを確認してください。また、プライベートマーケットプレイスをライブにする前に、未承認製品の使用を中止する計画を立てておくのもベストプラクティスです。プライベートマーケットプレイスの開始後は、すべての新規購読または更新は、プライベートマーケットプレイスのカタログで承認された製品によって管理されます。

プライベート製品の使用

一部の製品は、で参照するために公開されていません AWS Marketplace。これらの製品は、販売者からプライベートオファーを受けた場合にのみ表示されます。販売者からのプライベートオファーには、製品へのリンクが含まれています。ページ上部のバナーから、プライベートマーケットプレイスに製品を追加できます。

Note

組織内の別のアカウントからプライベート製品をサブスクライブする場合、販売者は AWS アカウント プライベートオファーに (製品をプライベートマーケットプレイスに追加するため) とユーザーのアカウント (製品をサブスクライブするため) の両方を含める必要があります。

プライベートマーケットプレイスからプライベート製品を削除するには、[AWS Marketplace サポートに連絡する](#)必要があります。

ユーザーリクエストの管理

ソフトウェアリクエスト機能を使用して、自分の Private Marketplace カタログに製品を追加するリクエストをユーザーが送信できるようにできます。そのためには、プライベートマーケットプレイスの管理者ページに移動し、左側のナビゲーションペインで [エクスペリエンス] を選択し、管理するエクスペリエンスを選択します。[製品] タブから [保留中のリクエスト] を選択します。ここから、ユーザーが自分の Private Marketplace カタログに追加した製品のリクエストを確認できます。

このページから、リクエストされた製品をいくつでも追加できます。追加するには、リクエストされた各製品の名前の横にあるチェックボックスをオンにし、[Add to Private Marketplace (プライベート

マーケットプレイスに追加)] を選択します。同様に、[拒否] を選択して、1 つまたは複数の選択したリクエストを拒否することもできます。製品 (またはそのソフトウェアリクエスト) に関する詳細情報を表示するには、そのリクエストの [詳細] 列で [詳細を表示] を選択します。

製品リクエストを拒否する場合は、その理由を追加して、今後この製品がリクエストされないように (ブロック) できます。製品のブロックにより、プライベートマーケットプレイスに製品を追加できなくなることはありませんが、ユーザーは製品をリクエストできなくなります。

プライベートマーケットプレイスエクスペリエンスのアーカイブと再有効化

プライベートマーケットプレイスエクスペリエンスはアーカイブして削除できます。アーカイブされたエクスペリエンスは更新したり、組織内のアカウントを管理したりするために使用できません。アーカイブされたエクスペリエンスにオーディエンスが関連付けられている場合は、別のエクスペリエンスに関連付けることができます。後でエクスペリエンスを使用する場合は、いつでも再有効化できます。管理アカウント管理者または委任された管理者は、エクスペリエンスをアーカイブして再有効化するアクセス許可を持っています。

Note

エクスペリエンスをアーカイブする前に、そのエクスペリエンスを無効にする必要があります。エクスペリエンスの無効化については、「[Configuring your private marketplace](#)」を参照してください。

プライベートマーケットプレイスと AWS Organizations の統合がない現在のプライベートマーケットプレイスのお客様の場合、エクスペリエンスを作成したアカウントの管理者は、エクスペリエンスをアーカイブして再アクティブ化するアクセス許可を持っています。

1 つ以上のプライベートマーケットプレイスエクスペリエンスをアーカイブするには

1. [プライベートマーケットプレイス] 管理者ページから、左側のナビゲーションペインで [エクスペリエンス] を選択します。
2. [アクティブエクスペリエンス] タブで、1 つ以上のエクスペリエンスを選択します。
3. [エクスペリエンスをアーカイブ] を選択します。

Note

1つ以上のエクスペリエンスのステータスが「ライブ」になっている場合は、[エクスペリエンスをオフラインにする]を選択してオフラインにする必要があります。

4. エクスペリエンスをアーカイブするかどうかを確認するには、テキストボックスに **confirm** (すべて小文字) と入力します。
5. [Archive] (アーカイブ) を選択します。

Note

エクスペリエンスを選択し、[設定] タブの [管理者] モードで [エクスペリエンスをアーカイブ] を選択し、[保存] を選択してもエクスペリエンスをアーカイブできます。

1つ以上のプライベートマーケットプレイスエクスペリエンスを再有効化するには

1. [プライベートマーケットプレイス] 管理者ページから、左側のナビゲーションペインで [エクスペリエンス] を選択します。
2. [アーカイブされたエクスペリエンス] タブで、1つ以上のエクスペリエンスを選択します。
3. [再有効化] を選択します。
4. エクスペリエンスを再有効化するかどうかを確認するには、テキストボックスに **confirm** と入力します。
5. [再有効化] を選択します。

Note

エクスペリエンスを選択し、[設定] タブの [管理者] モードで [エクスペリエンスを再有効化] を選択し、[保存] を選択してもエクスペリエンスを再有効化できます。

プライベートオファー

AWS Marketplace 販売者のプライベートオファー機能を使用すると、公開されていない販売者から製品の料金と EULA 条件を受け取ることができます。販売者と料金と条件を交渉すると、販売者は指定した AWS アカウントのプライベートオファーを作成します。プライベートオファーを受け入れ、交渉価格と利用規約の受信を開始します。

各プライベートオファーには、お客様のアカウントに特別に提供される価格設定およびライセンス条件があります。製品の販売者がプライベートオファーを拡張し、そしてオファーには設定された有効期限があります。有効期限内にプライベートオファーを受け入れない場合は、プライベートオファーの対象となる製品の種類によっては、自動的に製品のパブリックオファーに移動するか、製品をサブスクライブしなくなります。

一括請求機能を使用している場合は AWS Organizations、組織の管理アカウントまたはメンバーアカウントからプライベートオファーを受け入れることができます。管理アカウントから承諾すると、プライベートオファーを組織内のすべてのメンバーアカウントと共有できます。以前この製品をサブスクライブしていたメンバーアカウントも、価格設定のメリットを受けるためには、新しいプライベートオファーを受け入れる必要があります。また、AMI およびコンテナ製品の場合は、AWS License Manager を使用して管理アカウントからのライセンスをメンバーアカウントと共有できます。製品をサブスクライブしていないメンバーアカウントは、製品をデプロイするためにプライベートオファーを受け入れる必要があります。

一括請求の詳細については、AWS Billing ユーザーガイドの[組織の一括請求](#)を参照してください。以下は、プライベートオファーを使い始める際に留意すべき重要なポイントです。

- AWS Marketplace 購入者は、プライベートオファーのためにサードパーティーの資金調達サービスにアクセスできます。詳細については、[「カスタマーローン」が利用可能になりました AWS Marketplace](#)」を参照してください。
- プライベートオファーを使用して購入するソフトウェア製品に違いはありません。プライベートオファーを使用して購入したソフトウェアは、プライベートオファーを使用せずにソフトウェアを購入した場合と同じように動作します。
- プライベートオファーで購入した製品サブスクリプションは、その他すべての AWS Marketplace 製品と同じように毎月の請求書に記載されています。詳細請求を使用して、AWS Marketplace が購入した各製品の使用状況を表示できます。各プライベートオファーは、内訳別に明細項目が表示されます。
- プライベートオファーをサブスクライブするのに、ソフトウェアの新しいインスタンスを起動する必要はありません。プライベートオファーを承諾すると、料金がプライベートオファーの料金に

対応したものに更新されます。製品に 1-Click 起動機能がある場合は、ソフトウェアの新しいインスタンスをデプロイできます。製品の 1-Click 起動機能がデフォルトになっている場合は、新しいインスタンスを起動せずにプライベートオファーを承諾できます。新しいインスタンスをデプロイせずに起動するには、受理ページで [Manual Launch (手動起動)] を選択します。Amazon Elastic Compute Cloud コンソールを使用して、他の AWS Marketplace 製品と同様に、追加のインスタンスをデプロイできます。

- 販売者がプライベートオファーを行うと、販売者がプライベートオファーに含めたアカウントに対して確認メッセージが送信されます。プライベートオファーは、表示されている特定のソフトウェア購入者のアカウントに連結されています。ソフトウェア販売者は、指定されたアカウントのプライベートオファーを作成します。各プライベートオファーは、最大 25 個のアカウントに対して作成できます。
- プライベートオファーを承諾すると、それは販売者との契約になります (コントラクトまたはサブスクリプションとも呼ばれます)。
- 販売者は、購入済みの SaaS 契約製品または従量課金制の SaaS 契約製品に対するアップグレードや更新を提供する場合があります。たとえば、販売者は新しいプライベートオファーを作成することで、新しい権利の付与、料金割引の提供、支払いスケジュールの調整、またはエンドユーザーライセンス契約 (EULA) の変更を行い、[標準化されたライセンス条項](#)を使用できます。

これらの更新やアップグレードは、承諾済みの元のプライベートオファーに対する変更であり、この変更を承諾するには同じプロセスを使用します。新しいアップグレードや更新のプライベートオファーを承諾すると、新しい契約条項が即座に発効し、ソフトウェアサービスが中断されることはありません。以前の条項または残りの支払予定はキャンセルされ、この新しい契約の条項に置き換えられます。

- 年間ソフトウェアサブスクリプションはすべて、ソフトウェア AWS Marketplace ので確認できます。一括請求の AWS Organizations を使用して 1 つのアカウントで年間サブスクリプションを購入した場合、連結アカウントファミリー全体で共有されます。サブスクリプションを購入したアカウントに実行中のインスタンスがない場合、年間サブスクリプションは、そのソフトウェアを実行する別の連結アカウントの使用量としてカウントされます。年間サブスクリプションの詳細については、「[the section called “AMI サブスクリプション”](#)」を参照してください。
- プライベートオファーの有効期限が切れると、サブスクライブすることはできません。ただし、販売者に問い合わせることもできます。販売者に、現在のオファーの有効期限を将来の日付に変更してもらおうか、新しいプライベートオファーを作成してもらってください。

プライベートオファーに適した製品のタイプ

次の製品タイプのプライベートオファーを取得できます。

オファーのタイプ	説明
データ製品	詳細については、「AWS Data Exchange ユーザーガイド」の「 プライベートオファーの承諾 」を参照してください。
SaaS 契約	<p>SaaS (Software-as-a-Service) 契約では、SaaS 製品の予想使用量に対する前払い金をコミットするか、販売者と Flexible Payment Schedule を交渉できます。契約期間は 1 か月、1 年、2 年、3 年、または月単位で最長 60 か月までのカスタム期間を選択できます。前払い料金をお支払いいただく場合は、製品ソフトウェアを使用する前に前払い料金が請求されます。</p> <p>販売者が Flexible Payment Schedule を提供する場合、プライベートオファーに記載されている金額で、支払いスケジュールの日付に従って請求されます。</p> <p>販売者は、契約した使用量を超える使用量の交渉済み pay-as-you-go 料金を含めることもできます。</p>
SaaS サブスクリプション	SaaS サブスクリプションを使用すると、製品の使用に対する価格に同意したことになります。販売者は使用状況を追跡してに報告し AWS Marketplace、使用した分に対して課金されます。
時間単位の AMI	時間単位の Amazon Machine Image (AMI) では、AMI を使用するための時間あたりの料金を交渉して、最も近い時間に四捨五入します。

オファーのタイプ	説明
年間料金による時間単位の AMI	<p>年間料金による時間単位の AMI では、インスタンスタイプごとに時間単位と長期料金を交渉します。長期料金は、プライベートオファーの期間 (1 日から 3 年間) を対象としています。販売者が Flexible Payment Schedule なしでプライベートオファーを作成した場合、プライベートオファーで決定された時間単位の料金で Amazon EC2 インスタンスを実行し、オプションでプライベートオファーに設定された長期料金で契約期間中の前払いのコミットメントを購入できます。販売者が Flexible Payment Schedule を設定したプライベートオファーを作成した場合、利用状況にかかわらず、プライベートオファーに記載されている金額で、支払いスケジュールの日付に従って請求されます。このタイプのプライベートオファーでは、販売者は、時間単位の料金の請求なしで実行できるインスタンスタイプごとに Amazon EC2 インスタンスの数を含めることができます。使用量がこの料金に含まれるものを超え得た場合、プライベートオファーで設定された時間単位の料金で請求されます。</p>

オファーのタイプ	説明
AMI 契約	AMI 契約では、契約料金と契約期間 (1 ~ 60 か月) を交渉します。販売者が Flexible Payment Schedule なしでプライベートオファーを作成した場合、承諾時にプライベートオファーに設定されている料金とオプションに従って契約を設定できます。販売者が Flexible Payment Schedule を設定したプライベートオファーを作成した場合、プライベートオファーに記載されている金額で、支払いスケジュールの日付に従って請求されます。このタイプのプライベートオファーでは、販売者はプライベートオファーで契約を設定しますが、承諾時には設定できません。
コンテナ製品	コンテナ製品では、購入する製品に合わせて、ポッド、タスク、カスタム単位で、使用するコンテナ製品の時間単位または年間料金を交渉します。コンテナ製品のプライベートオファーは、AMI 製品のプライベートオファーと一致します。
Machine Learning 製品	プライベートオファーは、指定された日数の固定前払い料金が適用される契約にできます。契約の終了時に、継続して実行するすべてのインスタンスには、販売者がプライベートオファーで設定した時間単位の料金で請求されます。
プロフェッショナルサービス	プロフェッショナルサービスのオファーは、すべてプライベートオファーです。プライベートオファーを作成するには、購入者と協力する必要があります。詳細については、「 プロフェッショナルサービス製品 」を参照してください。

プライベートオファーの受け入れ準備

一般的なプライベートオファーを交渉する場合、サードパーティーの資金調達を利用している場合を除き、オファーを承諾した時点でオファーの全額を支払います。サードパーティーの資金調達では、金融機関がお客様に代わって契約料金を支払い、合意された支払いスケジュールに基づいて請求書を発行します。プライベートオファーを承諾する前に、会社の請求構造、AWS 請求の支払い方法、税金設定を確認してください。

Note

一部の販売者は、で製品のプライベートオファーをリクエストするオプションを提供しています AWS Marketplace。参加している販売者の場合、プライベートオファーのリクエストボタンが製品詳細ページに表示されます。プライベートオファーをリクエストするには、ボタンを選択し、リクエストの詳細を指定します。リクエストをまとめた確認メールが届き、担当者から AWS 連絡があります。

AWS Billing and Cost Management 設定の確認

請求情報とコスト管理は、AWS 請求の支払い、使用状況のモニタリング、コストの予算作成に使用するサービスです。の統合請求機能を使用して AWS Organizations、複数のアカウントまたは複数の Amazon Internet Services Pvt の請求と支払いを統合することができます。株式会社 (AISPL) アカウント。のすべての組織 AWS Organizations には、すべてのメンバーアカウントの料金を支払う管理アカウントがあります。管理アカウントは支払者アカウントと呼ばれ、メンバーアカウントは連結アカウントと呼ばれます。プライベートオファーをネゴシエートする前に、会社が AWS 請求の支払い方法と、プライベートオファーが行われた AWS アカウントを確認します。

支払い方法の確認

プライベートオファーを受け入れる前に、支払い方法でプライベートオファーの全額の支払いがサポートされていることを確認してください。支払い方法を確認するには、Billing and Cost Management コンソール (<https://console.aws.amazon.com/billing/>) を開きます。

課税設定の確認

ユーザーの会社が免税を受ける資格がある場合は、課税設定を確認してください。税金設定を表示または変更するには、にサインイン AWS Management Console し、アカウント設定で税金設定を表

示します。税登録の詳細については、「[AWS アカウントに関する納税者登録番号または事業法人所在地を追加または更新する方法を教えてください](#)」を参照してください。

プライベートオファーの表示とサブスクライブ

プライベートオファーは、次のいずれかの方法で表示できます。

トピック

- [プライベートオファーのリストからのプライベートオファーの表示とサブスクリプション](#)
- [販売者が提供したリンクからプライベートオファーを表示してサブスクライブする](#)
- [製品ページからのプライベートオファーの表示とサブスクリプション](#)

プライベートオファーのリストからのプライベートオファーの表示とサブスクリプション

に拡張されたプライベートオファーのリストからプライベートオファーを表示してサブスクライブするには AWS アカウント

1. [AWS Marketplace](#) コンソールにサインインします。
2. [\[プライベートオファー\] ページ](#)に移動します。
3. [プライベートオファー] ページの [利用可能なオファー] タブで、関心のあるオファーの [オファー ID] を選択します。
4. プライベートオファーを表示して、サブスクライブします。

販売者が提供したリンクからプライベートオファーを表示してサブスクライブする

販売者から送られたリンクからプライベートオファーを表示してサブスクライブするには

1. [AWS Marketplace](#) コンソールにサインインします。
2. 販売者から送られたリンクに従って、プライベートオファーに直接アクセスします。

Note

正しいアカウントにログインする前にこのリンクをクリックすると、[ページが見つかりません] (404) というエラーが表示されます。

詳細については、「[プライベートオファーを表示するために \[オファー ID\] をクリックすると、\[ページが見つかりません\] \(404\) エラーが表示されます。](#)」を参照してください。

3. プライベートオファーを表示して、サブスクライブします。

製品ページからのプライベートオファーの表示とサブスクリプション

製品ページからプライベートオファーを表示してサブスクライブするには

1. [AWS Marketplace](#) コンソールにサインインします。
2. その製品の製品ページに移動します。
3. ページの上部のバナーで、プライベートオファー、オファー ID、およびオファーの有効期限を確認します。

Note

将来の日付のプライベートオファーは早期更新として表示されます。詳細については、「[the section called “将来の日付の契約の使用”](#)」を参照してください。

4. [オファー ID] を選択します。
5. プライベートオファーを表示して、サブスクライブします。

Note

その製品に対して複数のプライベートオファーがある場合、各オファーは [オファー名] の下に表示されます。現在契約中の製品がある場合は、そのオファーの横に [使用中] アイコンが表示されます。

プライベートオファ어의トラブルシューティング

でプライベートオファ어を使用する際に HTTP ステータスコード 404 (Not Found) の問題や同様の問題が発生した場合は AWS Marketplace、このセクションのトピックを参照してください。

問題

- [プライベートオファ어を表示するために \[オファ어 ID\] をクリックすると、\[ページが見つかりません\] \(404\) エラーが表示されます。](#)
- [どの提案でも機能しない場合](#)

プライベートオファ어を表示するために [オファ어 ID] をクリックすると、[ページが見つかりません] (404) エラーが表示されます。

- 正しい AWS アカウントにサインインしていることを確認します。販売者はプライベートオファ어를特定の AWS アカウント IDs。
- オファ어가 AWS Marketplace コンソールの[プライベートオファ어](#)に存在するかどうかを確認します。[プライベートオファ어] にオファ어가見つからない場合は、販売者が別の AWS アカウント ID に対してオファ어를延長したことが原因である可能性があります。販売者に問い合わせ、オファ어가延長された AWS アカウント ID を確認します。
- AWS Marketplace コンソールの「プライベートオファ어」の「承諾済みオファ어と期限切れオファ어」タブを表示して、[プライベートオファ어](#)の有効期限が切れていないことを確認します。オファ어의有効期限が切れている場合は、販売者と協力してオファ어의有効期限を変更するか、お客様のアカウントに対して新しいオファ어를延長してください。
- アカウント ID がプライベートオファ어의表示を許可していることを確認します。ISV によっては、限定出品を使用する場合があります。ISV に、お客様のアカウントが製品の表示を許可しているかどうかを問い合わせてください。AMI 製品の限定出品には許可リストが必要です。AWS 組織に属していて、販売者が管理アカウントにオファ어를延長している場合、連結アカウントにはサブスクライブするには許可リストが必要です。そうしないと、許可リストにない購入者の連結アカウントがオファ어를表示しようとしたときに「ページが見つかりません (404)」というエラーが表示されます。
- オファ어를表示する必要がある場合は、AWS 管理者に問い合わせ、aws-marketplace:ViewSubscriptions IAM アクセス許可があることを確認してください。AWS Marketplace セキュリティの詳細については、「」を参照してくださいの[セキュリティ AWS Marketplace](#)。
- プライベートマーケットプレイスを利用しているかどうかを確認してください。

- 製品がプライベートマーケットプレイス (該当する場合) の許可リストに掲載されていることを確認し、製品を購入できることを確認します。不明な場合は、システム管理者に問い合わせを確認してください。

どの提案でも機能しない場合

どの提案でも HTTP ステータスコード 404 (Not Found) エラーが解決されない場合は、ブラウザで次の操作を試してください。

- キャッシュをクリアします。
- Cookie を削除します。
- サインアウトし、サインインし直します。
- シークレットモードまたはプライベートブラウジングモードを使用します。
- 別のブラウザを試します。Internet Explorer を使用することは推奨しません。

トラブルシューティングの提案をすべて完了しても「ページが見つかりません」というエラーが引き続き表示される場合は、<mpcustdesk@amazon.com> に E メールを送信してサポートを受けてください。

のプライベートオファーページ AWS Marketplace

では AWS Marketplace、プライベートオファーページには、プライベート製品とパブリック製品 AWS アカウント の両方でに拡張されたすべてのプライベートオファーが一覧表示されます。利用できるすべてのオファーは、製品ごとに表示されます。各製品につき 1 つのオファーを受け入れることができます。

プライベートオファーページについて理解する

[プライベートオファー] ページを表示するには、AWS Marketplace コンソールにサインインして [プライベートオファー] に移動します。に拡張されたプライベートオファー AWS アカウント は、オファー ID、製品、登録販売者 (ISV またはチャネルパートナー)、パブリッシャー、有効な契約 (該当する場合)、オファーの有効期限など、「プライベートオファー」に記載されています。関心のあるオファーの [オファー ID] を選択してオファーの詳細を確認したり、プライベートオファーをサブスクライブしたりできます。

プライベートオファーページには以下の情報が含まれます。

- [ご利用いただけるオファー] タブには、ご利用のアカウントに適用されたプライベートオファーのうち、受け付け可能なプライベートオファーが一覧表示されます。このタブの [オファー ID] リンクは、プライベートオファーの詳細にアクセスするために販売者が提供しているリンクと同じです。
- [受け入れたオファーと期限切れのオファー] タブには、お客様が承諾し、契約が作成されたオファーが一覧表示されます。また、販売者が設定したオファーの有効期限に達したオファーも一覧表示されます。このタブは、販売者との契約を更新するときに、以前のオファー ID と契約 ID (ある場合) を取得するのに便利です。オファーによって契約が成立し、契約がアクティブな場合は、契約を選択してサブスクリプションの詳細ページを表示できます。

Note

将来の日付のプライベートオファーは早期更新として表示されます。詳細については、[「the section called “将来の日付の契約の使用”」](#)を参照してください。

プライベートオファーの変更、アップグレード、更新について詳しくは、[「プライベートオファーの変更またはサブスクリプション解除」](#)を参照してください。

プライベートオファーページの閲覧に必要なアクセス許可

AWS Marketplace コンソールでプライベートオファーページを表示するには、次のアクセス許可が必要です。

- AWS マネージドポリシーを使用する場合: `AWSMarketplaceReadOnly`、`AWSMarketplaceManageSubscriptions`、または `AWSMarketplaceFullAccess`
- AWS マネージドポリシーを使用していない場合: IAM アクション `aws-marketplace:ListPrivateListings` と `aws-marketplace:ViewSubscriptions`

プライベートオファーページを表示できない場合は、管理者に連絡して正しい AWS Identity and Access Management (IAM) アクセス許可を設定してください。に必要な IAM アクセス許可の詳細については、AWS Marketplace 「」を参照してください [AWS 購入者向けの AWS Marketplace マネージドポリシー](#)。

SaaS プライベートオファーへのサブスクライブ

Software as a Service (SaaS) のプライベートオファーで利用できる設定オプションは、販売者と交渉する可能性のある契約によって異なります。

次の図に示すように、[プライベートオファー] ページには次のセクションがあります。

- [オファー名] - これは、作成時に販売者がプライベートオファーに提供した名前です。
- 一括請求情報 - この通知は、で一括請求を使用している場合に表示されます AWS アカウント。
- [契約の仕様と期間] - このペインには、オファーの期間とオファーを定義する範囲が表示されます。ディメンションは、使用状況の測定方法と交渉された料金設定が有効になっている期間を表します。たとえば、12 か月間 5 GB/日、または 1 時間にユーザーあたり 0.01 USD など。プライベートオファーが契約の場合は、契約期間にわたって合意された使用量に対して支払います。プライベートオファーがサブスクリプションの場合、合意されたレートで測定された使用法に対して支払います。

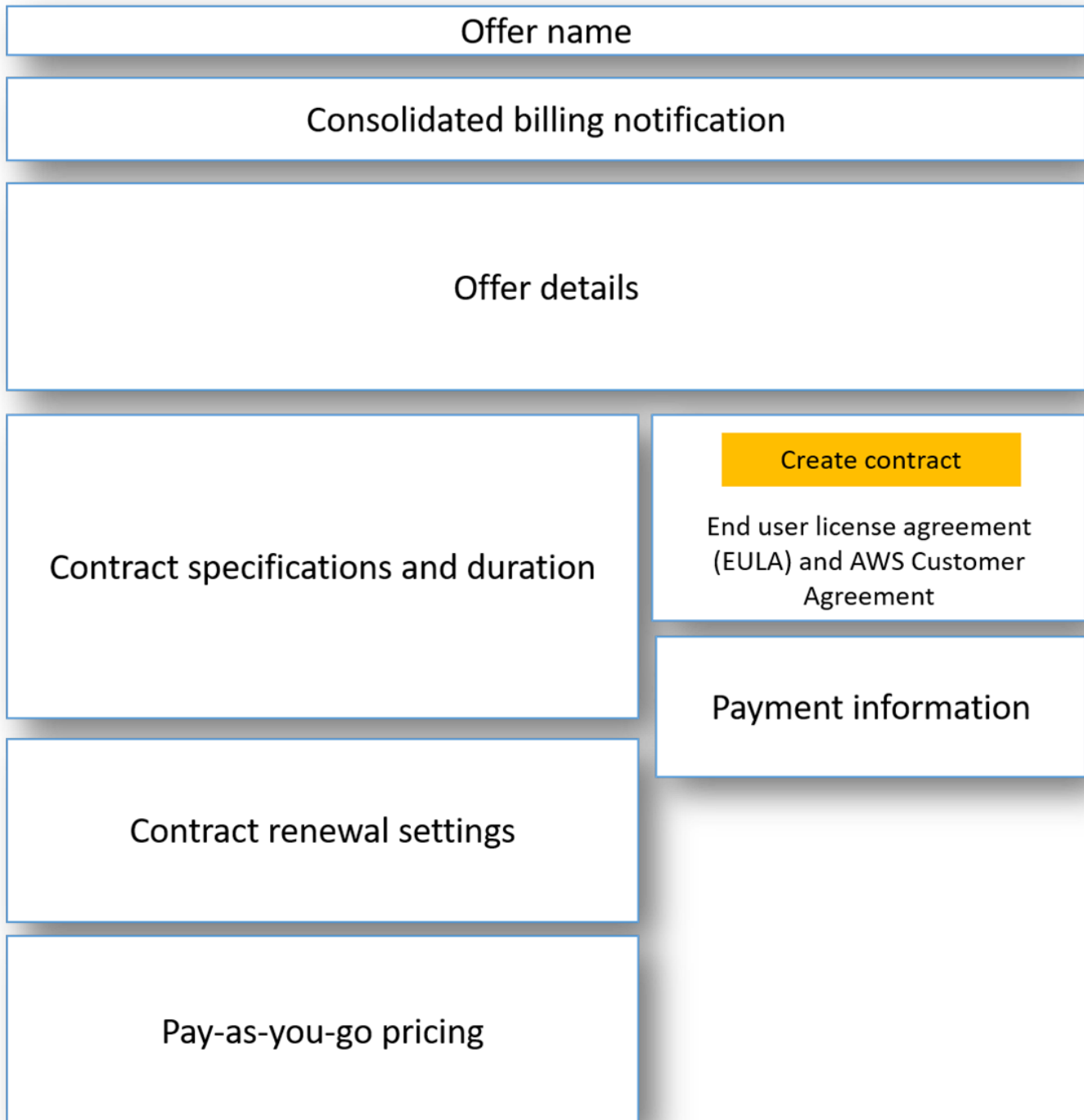
Note

将来の日付のプライベートオファーは早期更新として表示されます。詳細については、[「the section called “将来の日付の契約の使用”](#)」を参照してください。

- [契約更新設定] - プライベートオファーを自動的に更新するように設定することはできません。SaaS 製品のプライベートオファーの場合、このペインには常にこのオファーの更新がないことが示されます。
- Pay-as-you-go 料金 - プライベートオファーで定義されている料金を超える製品使用量の料金を交渉すると、追加使用コストの仕様がここに表示されます。たとえば、12 か月間 5 GB/日のデータストレージに関する SaaS 契約に同意し、10 GB/日を使用する場合、最初の 5 GBがその契約に該当します。追加の 5 GB/日には料金がかかります pay-as-you-go。SaaS サブスクリプションでは、契約期間中に使用した金額の大部分について合意したレートがあります。
- [エンドユーザーライセンス契約 (EULA) と契約作成ボタン] - ここでは、販売者がこのプライベートオファー向けにアップロードしたライセンス契約を参照できます。これは、すべてのプライベートオファーの仕様を確認し、契約を締結する準備ができた後に契約を承諾する場所でもあります。
- [支払い情報] - このペインには、支払いの期限、および支払いスケジュールを交渉した場合は支払いの期限の日時が表示されます。

⚠ Important

[プライベートオファー] ページに表示されないセクションは、プライベートオファーの交渉対象ではありません。



SaaS プライベートオファーをサブスクライブするには

1. 「[プライベートオファーの表示とサブスクライブ](#)」の手順を実行します。

2. オファーの詳細ペインで、適切なプライベートオファーを選択していることを確認します。製品に対して複数のオファーがある可能性があります。
3. 契約の仕様と期間のペインで、契約期間と契約の詳細が交渉したものであることを確認します。そうでない場合は、適切なプライベートオファーを選択したことを確認するか、オファーを作成した販売者にお問い合わせください。

Note

将来の日付のプライベートオファーは早期更新として表示されます。詳細については、[「the section called “将来の日付の契約の使用”」](#)を参照してください。

4. pay-as-you-go 価格を交渉した場合は、交渉した条件を説明する情報を含むペインがあるはずで、情報を確認するか、(あるはずの)情報が欠落している場合は、販売者にお問い合わせください。
5. 支払い情報ペインで、支払い情報を確認します。Flexible Payment Schedule について交渉した場合は、支払い日と金額が一覧表示されます。層ではない場合は、オファーを承諾する際に、契約の合計金額が請求されます。
6. EULA と契約の作成ペインで、EULA が販売者と交渉したものであることを確認します。契約のすべての利用規約を確認したら、[Create contract (契約の作成)] を選択してオファーを承諾します。

オファーを承諾すると、[確認] ページが開き、製品を正常にサブスクライブしたことを示します。販売者のページにリダイレクトされたら、[Set Up Your Account] を選択して、販売者のウェブサイトでのアカウントの設定を完了します。

AMI プライベートオファーへのサブスクライブ

Amazon マシンイメージ (AMI) のプライベートオファーに使用できるセクションと設定オプションは、製品ベンダーと交渉した契約によって異なります。次の図は、AWS Marketplace ウェブサイトの AMI プライベートオファーページのレイアウトを示しています。

次の図に示すように、[プライベートオファー] ページには次のセクションがあります。

- [ベンダー名と製品] - これは、プライベートオファーの対象となるベンダーおよび製品の名前です。右側には製品の設定ボタンがあります。
- [ページのガイダンス] - この領域には、このページのタスクを完了してプライベートオファーを受け入れるためのガイダンスがあります。

- [利用規約] - このセクションには、次の情報が含まれます。
 - 左上には、プライベートオファーの名前と、これがプライベートオファーであることを示すラベルがあります。
 - プライベートオファー名セクションの下には、契約受諾の通知があります。[契約に同意する] ボタンを使用すると、プライベートオファーを承諾できます。
 - 通知セクションの下には、契約期間、契約に含まれるコンポーネント、交渉済みのインスタンス料金に関するセクションの他、EULA を確認またはダウンロードする別の機会が表示されます。
- [契約期間] - このセクションには、契約日数と契約終了日が表示されます。
- [その他のオファー情報] - 右側には、契約金額の合計、次回の支払い予定、現在の条件、その他のプライベートオファーやパブリックオファーのサムネイルイメージが表示されます。

Note

インスタンスタイプ または にアクセスできない場合は AWS リージョン、プライベートオファーが送信された時点でサポートされていない可能性があります。詳細については、契約の詳細を確認してください。インスタンスまたはリージョンへのアクセスを取得するには、販売者に連絡し、更新されたプライベートオファーをリクエストします。新しいオファーを承諾すると、新しく追加されたインスタンスまたはリージョンにアクセスできます。

Vendor name and product		Continue to Configuration button
Page guidance		Additional offer information
Terms and Conditions		Contract pricing
Private offer name	Private Offer	Scheduled payments
Notification for accepting the private offer contract		Accept Contract button
Contract duration		Other Available Offers
Components included in the contract		
Additional usage costs		
Terms duration		


Flexible Payment Schedule で年間 AMI プライベートオファーをサブスクライブする

AMI のプライベートオファーをサブスクライブするには、AWS Marketplace ウェブサイトでプライベートオファーを受け入れる必要があります。AWS Marketplace コンソールまたは Amazon Elastic Compute Cloud (Amazon EC2) コンソールでは、プライベートオファーを承諾できません。販売者が Flexible Payment Schedule を設定したプライベートオファーを作成した場合、プライベートオファーに記載されている金額で、支払いスケジュールの日付に従って請求されます。Flexible Payment Schedule で AMI プライベートオファーを受け入れるには、次の手順に従ってください。

Flexible Payment Schedule で AMI プライベートオファーを受け入れるには

1. 「[プライベートオファーの表示とサブスクライブ](#)」の手順を実行します。

2. 適切なプライベートオファーを表示していることを確認します。ベンダーは、その製品に対して複数のプライベートオファーを作成できます。その他のプライベートオファーは [ご利用いただけるその他のオファー] セクションに表示されます。
3. オファーの有効期限と料金設定情報が、プライベートオファーについて交渉したものであることを確認してください。そうでない場合は、適切なプライベートオファーを表示していることを確認します。
4. EULA をダウンロードして、それがプライベートオファーについて交渉したものであることを確認してください。
5. [契約期間] セクションで、プライベートオファーの条件が交渉したものであることを確認します。
6. プライベートオファーの詳細を確認したら、[利用規約] セクションで [条件に同意する] を選択します。
7. 条件を確認し、同意する場合は [確認] を選択します。

 Important

システムが契約のリクエストを処理している間は、ブラウザを更新しないでください。

AMI を設定する準備が整ったら、[Continue to Configuration (設定を続行)] を選択します。製品を使用するたびにサブスクリプションプロセスを完了する必要があります。

Flexible Payment Schedule なしで年間 AMI プライベートオファーをサブスクライブする

AMI のプライベートオファーをサブスクライブするには、AWS Marketplace ウェブサイトでプライベートオファーを受け入れる必要があります。AWS Marketplace コンソールまたは Amazon EC2 コンソールでは承諾できません。販売者が Flexible Payment Schedule なしでプライベートオファーを作成した場合、承諾時にプライベートオファーに設定されている料金とオプションに従って契約を設定できます。Flexible Payment Schedule なしで AMI プライベートオファーを受け入れるには、次の手順に従ってください。

Flexible Payment Schedule なしで AMI プライベートオファーを受け入れるには

1. 適切なプライベートオファーを表示していることを確認します。ベンダーは、その製品に対して複数のプライベートオファーを作成できます。追加のプライベートオファーが追加のプライベ

トオファーペインに表示されます。承諾するオファーが、[このオファーを表示しています] と表示されていることを確認します。

Note

多くの場合、支払いアカウントは製品を使用するアカウントではありません。支払いアカウントを使用してオファーを承諾する場合は、ワンクリックオプションを選択するのではなく、手動で製品を起動することをお勧めします。

2. オファーの有効期限と料金設定情報が、プライベートオファーについて交渉したものであることを確認してください。そうでない場合は、適切なプライベートオファーを表示していることを確認します。
3. EULA をダウンロードして、それがプライベートオファーについて交渉したものであることを確認してください。
4. 契約条件ペインで、プライベートオファーの条件が交渉したものであることを確認します。
5. オファーの詳細がプライベートオファーについて交渉した内容であることを確認し、[Accept Terms (条件に同意する)] を選択します。そうでない場合は、適切なプライベートオファーを表示していることを確認します。
6. [このソフトウェアをサブスクライブする] の [インスタンスタイプ] を、利用可能なインスタンスタイプのリストから選択します。[数量] で、ライセンスの数を選択します。
7. 選択を確認します。選択内容を確認して問題がなければ、[契約の作成] を選択し、次に [確認] を選択します。

AMI を設定する準備が整ったら、[Continue to Configuration (設定を続行)] を選択します。製品を使用するたびにサブスクリプションプロセスを完了する必要があります。

プライベートオファーの変更またはサブスクライブ解除

標準サブスクリプションからプライベートオファーに更新したり、AWS Marketplaceの既存の特定のプライベートオファーを変更したりすることもできます。プロセスは、定められた契約によって異なります。

多くのサブスクリプションでは、パブリックプライシングからプライベートオファーに移行する際に、ISV またはチャネルパートナーとオファーについて交渉します。プライベートオファーを承諾すると、関連する既存の1つまたは複数のサブスクリプションが自動的にプライベートオファー料金

モデルに移行します。これにはユーザー側のアクションは一切必要ありません。以下のガイダンスを使用して、プライベートオファーの料金設定を受けるシナリオとステップを確認してください。

パブリックオファーからプライベートオファーへの料金設定の変更

プライベートオファーを承諾すると、そのオファーを承諾したユーザーに対してそれ以上のアクションは必要ありません。これらは、プライベートオファーで定義されている料金設定、契約条件に切り替えられます。プライベートオファーの料金、契約条件に切り替えるには、製品を使用している連結済みの各ユーザーがプライベートオファーを承諾する必要があります。製品の使用を開始するユーザーも、プライベートオファーで定義されている料金設定、および契約条件を取得するために、プライベートオファーを受け入れる必要があります。

SaaS 契約の変更 - アップグレードと更新

このセクションは、Software as a Service (SaaS) 契約と従量課金制の製品の SaaS 契約に適用されます。以前のプライベートオファーで有効な契約があり、同じ製品の新しいプライベートオファーを受け入れる場合、販売者は既存の契約をアップグレードまたは更新して、条件、価格、期間を変更したり、既存の契約を終了前に更新したりすることができます。これにより、既存の契約を先にキャンセルしなくても、新しいプライベートオファーを受け入れることができます。

Note

将来の日付のプライベートオファーは早期更新として表示されます。詳細については、「[the section called “将来の日付の契約の使用”](#)」を参照してください。

アップグレードまたは更新を受け入れるには、請求書の発行条件を満たしている必要があります。現在、請求書発行の条件を満たしていない場合は、[AWS カスタマーサービス](#)にチケットを送信して、支払い方法を請求書発行に変更してください。

請求書発行に切り替えない場合は、次のいずれかのアクションを取ることができます。

- 製品ベンダーおよび AWS Marketplace カスタマーサポートチームと協力して、その製品の新しいプライベートオファーを受け入れる前に現在の契約をキャンセルします。
- 別の AWS アカウントでオファーを受け入れます。

SaaS サブスクリプションから SaaS 契約に変更する

SaaS サブスクリプションから SaaS 契約に変更するには、まず SaaS サブスクリプションを解除する必要があります。その後、SaaS 契約のプライベートオファーを承諾します。既存の SaaS サブスクリプションを表示するには、AWS Marketplace コンソールの右上隅にある Marketplace ソフトウェアを選択します。

AMI 契約から新しい契約に変更する

以前のプライベートオファーから Amazon マシンイメージ (AMI) 契約を結んでいて、同じ製品に対して新しいプライベートオファーを受け入れる場合は、次のいずれかを実行する必要があります。

- 新しい AMI 契約を受け入れる前に、現在の AMI 契約が終了するのを待つ。
- 製品ベンダーと AWS Marketplace カスタマーサポートチームと協力して、現在の契約を終了します。
- 契約しているもの AWS アカウント とは異なる を使用してプライベートオファーを受け入れる

時間単位の AMI から年単位の AMI に変更する

時間単位の AMI サブスクリプションから年単位の AMI サブスクリプションに移行すると、そのサブスクリプションはバウチャーシステムと同様に機能します。時間単位の各 AMI の使用量は、年単位の AMI サブスクリプションの 1 単位で相殺されます。年間サブスクリプションを購入すると、関連付けられているすべてのプライベートオファーを介して製品にサブスクライブしているアカウントは、自動的にプライベートオファーで交渉された料金に変更されます。プライベートオファーが設定された後にサブスクリプションを開始する連結済みのアカウントは、サブスクライブ時にプライベートオファーをサブスクライブする必要があります。

Note

古いオファーの年間ライセンスは、新しいオファーの条項に同意するとすぐに無効化されます。ISV と協力して、古いライセンスの補償と新しいオファーを続行する方法について検討します。

年単位の AMI から時間単位の AMI に変更する

年単位のサブスクリプションの有効期限が終了すると、製品にサブスクライブしている連結済みアカウントは自動的に 時間単位の AMI 料金に切り替わります。年単位のサブスクリプションが設定され

ている場合は、連結済みアカウントはそのサブスクリプションをキャンセルせずにその製品の時間単位のサブスクリプションに切り替えることはできません。

将来の日付の契約やプライベートオファ어의使用

で将来の日付の契約 (FDA) を使用すると AWS Marketplace、将来の日付で製品の使用が開始される製品をサブスクライブできます。支払い時期や使用時期とは独立して製品を購入する時期を管理できます。

FDA は、AWS Marketplaceで購入者が以下の取引について独立して以下のアクションを実行できるようサポートします。

- オファーを受け入れ、製品を調達するか、取引を予約する。
- 製品の使用 (ライセンス/権利のアクティベーション) を開始する。
- 購入代金を支払う (請求書の生成)。

FDAは、Software as a Service (SaaS) 製品契約や、Flexible Payment Schedule の有無にかかわらず、使用料金付きの契約 (CCP) を作成するプライベートオファーでサポートされています。

将来の日付の契約を使用する場合は、以下の日付に注意します。

契約署名日

オファーを承諾した日付と、契約が作成された日付。この日付は契約 ID が作成された日です。

契約開始日

製品の使用が開始される日付。これは将来の日付または将来の開始日です。これはライセンス/権利が有効になる日付です。

契約終了日

契約が終了する日付。契約とライセンス/権利はこの日付で失効します。

FDA の使用の詳細については、以下のトピックを参照してください。

トピック

- [将来の日付の契約の作成](#)
- [将来の日付の契約での Flexible Payment Scheduler の使用](#)

- [将来の日付の契約の修正](#)
- [将来の日付の契約の通知を受け取る](#)

将来の日付の契約の作成

SaaS 契約や、Flexible Payment Schedule の有無にかかわらず、使用料金付き契約の場合、販売者はプライベートオファーの作成の一環として契約開始日を設定します。購入者は販売者と協力して、開始日が要件を満たしていることを確認する必要があります。

将来の日付の契約を作成するには、次の手順に従います。将来の日付の契約は、AWS Marketplace コンソールの「サブスクリプションの管理」ページで確認できます。

将来の日付の契約を作成するには

1. 「[プライベートオファーの表示とサブスクライブ](#)」の手順を実行します。
2. オファーの詳細ペインで、正しいプライベートオファーを選択したことで、契約開始日が正しいことを確認します。将来の日付のオファーは、[オファー] ドロップダウンメニューに [早期更新] と表示されます。

Note

SaaS 製品の場合は、契約開始日に、必ず ISV のアカウント設定を完了する必要があります。契約開始日より前にこのステップを完了することはできません。詳細については、「[the section called “SaaS プライベートオファーへのサブスクライブ”](#)」を参照してください。

将来の日付の契約での Flexible Payment Scheduler の使用

Flexible Payment Scheduler は、将来の日付の契約に使用できます。購入代金の支払い時期は、契約署名日と契約終了日の間の時期を選択して設定できます。このアプローチには、契約開始日の前後の支払いが含まれます。

プライベートオファーを作成した記録上の販売者が支払い日と金額を選択します。詳細については、「[Flexible Payment Scheduler](#)」を参照してください。

将来の日付の契約の修正

契約開始日の前後に、FDA で特定のディメンションの購入数量を増やすことができます。このオプションは、契約に Flexible Payment Schedule がない場合に可能です。詳細については、「[Flexible Payment Scheduler](#)」を参照してください。

修正が完了すると、契約開始日に日割り計算された金額が請求されます。開始日が過去の場合は、すぐに請求されます。

将来の日付の契約の通知を受け取る

将来の日付の契約に対して実行された次のアクションについて、指定されたルートアカウントに送信される電子メール通知が届きます。

- オファアの承認/契約の作成 (契約署名日)
- ライセンスまたは権利のアクティベーション時 (契約開始日)
- 30 日後、60 日後、または 90 日後に失効する契約に関する事前のリマインダー
- 契約失効日 (契約終了日)
- 契約の修正または置き換え時

組織内でのサブスクリプションの共有

で製品をサブスクライブすると AWS Marketplace、それらの製品を使用するライセンスを付与する契約が作成されます。AWS アカウント が組織のメンバーである場合は、Amazon マシンイメージ (AMI)、コンテナ、機械学習、データ製品のライセンスを、その組織内の他のアカウントと共有できます。でライセンスサポートを設定し AWS Marketplace、内から共有する必要があります AWS License Manager。

Note

の詳細については AWS Organizations、[「AWS Organizations ユーザーガイド」](#)を参照してください。

で組織とライセンスを共有する方法の詳細については AWS License Manager、[「AWS License Manager ユーザーガイド」](#)の[「付与されたライセンス」](#)を参照してください。

次の動画では、ライセンス共有について簡単に紹介します。

[AWS Marketplace ライセンス使用権限の配布 \(3:56\)](#)

以下のトピックで、アカウント間でライセンスを表示、共有、追跡するプロセスの概要を説明します。

トピック

- [ライセンス共有の前提条件](#)
- [ライセンスの表示](#)
- [ライセンスの共有](#)
- [ライセンスの使用状況の追跡](#)

ライセンス共有の前提条件

でライセンスを共有する前に、組織のライセンス共有を設定 AWS Marketplace する必要があります。以下のタスクを完了して、組織のライセンス共有をセットアップしてください。

- ライセンスを購入または共有するときに、関連するライセンス付与を作成できるように、ユーザーに代わってライセンスを管理する AWS Marketplace アクセス許可を付与します。詳細については、[「ロールを使用した の使用権限の共有 AWS Marketplace」](#)を参照してください。

- 初回使用 AWS License Manager のために をセットアップします。詳細については、「AWS License Manager ユーザーガイド」の「[AWS License Managerの使用開始](#)」を参照してください。

ライセンスの表示

AWS Marketplace は、AMI、コンテナ、機械学習、Software as a Service (SaaS)、および購入したデータ製品のライセンスを自動的に作成します。それらのライセンスを組織内の他のアカウントと共有できます。

Note

ライセンスは SaaS 製品用に作成されますが、SaaS ライセンスの共有は現在サポートされていません。

を使用してライセンスを管理および共有します AWS License Manager。ただし、AWS Marketplace を使用して、内から購入した製品のライセンスを表示できます AWS Marketplace。

でサブスクライブした製品のライセンスを表示するには AWS Marketplace

1. [AWS Marketplace](#) でサインインして [サブスクリプションを管理する] を選択します。
2. すべてのライセンスを表示することも、特定のサブスクリプションのライセンスを表示することもできます。
 - すべてのライセンスを表示するには
 - アクションメニューからライセンスを表示 を選択して、License Manager コンソールですべての AWS Marketplace マネージドライセンスを表示します。
 - 単一のサブスクリプションのライセンスを表示するには
 - a. 表示する製品のカードを選択すると、製品の詳細ページに移動します。
 - b. [アクション] メニューから [ライセンスの表示] を選択し、その製品のライセンスを License Manager コンソールに表示します。

Note

組織内のすべてのアカウントから集計された、付与されたライセンスを表示することもできます。詳細については、[AWS License Manager ユーザーガイド](#)の付与されたライセンスを参照してください。

ライセンスの共有

共有できるライセンスがあるのは、AMI、コンテナ、機械学習、データ製品だけです。

のサブスクリプション AWS Marketplace には、製品の詳細に表示されるアクセスレベルがありません。

- [契約] レベルのある製品には、組織内の他のアカウントで使用したり共有したりできるライセンスがあります。
- [使用権限] レベルのある製品は、アカウントと共有されているライセンスです。これらの製品を使用することはできますが、共有することはできません。

AWS Marketplace は、ライセンスの使用を、AWS Organizations、AWS アカウントまたはを使用する組織単位と直接共有する許可をサポートします AWS License Manager。許可のアクティベーションプロセスには、から取得した同じ製品に対してアクティブ化された許可を置き換える追加オプションが含まれるようになりました AWS Marketplace。詳細については、[AWS License Manager ユーザーガイド](#)の付与されたライセンスを参照してください。

Note

特定の に制限されている製品の場合 AWS リージョン、ライセンスを共有するアカウントは、アカウントが許可されたリージョン内にある場合にのみライセンスをアクティブ化できます。

ライセンスの使用状況の追跡

各ライセンスの使用状況ダッシュボードタブ AWS License Manager を選択すると、で AMI 製品の
使用状況ベースのライセンスメトリクスを追跡できます。

License Manager を使用してライセンスの使用状況を追跡する方法については、「AWS License Manager ユーザーガイド」の「[付与されたライセンス](#)」を参照してください。

AWS Marketplace イベントの購入者通知

AWS Marketplace は、E メール、Amazon EventBridge イベント、Amazon Simple Notification Service (Amazon SNS) トピックを通じてタイムリーな通知を提供します。

トピック

- [AWS Marketplace イベントの E メール通知](#)
- [AWS Marketplace イベントの Amazon EventBridge 通知](#)

AWS Marketplace イベントの E メール通知

の購入者は AWS Marketplace、次のいずれかが発生した場合に E メール通知を受け取ります。

- オファーを承諾します。
- 販売者は、以前に受け入れたプライベートオファーに関連する新しいプライベートオファーを公開するか、または以前に受諾したオファーのアップデートを公開します。

Note

通知は、購入者 AWS アカウント ID に関連付けられた E メールアドレスに送信されます。特定の E メールプロバイダー (Google や Yahoo など) は、AWS Marketplace の通知 E メールを除外する場合があります。から通知を受信していない場合 AWS Marketplace、またはスパムフォルダに表示されている場合は、E メール設定を調整します。例えば、[「Google グループの手順」](#)または[「Yahoo の手順」](#)を参照してください。

AWS Marketplace イベントの Amazon EventBridge 通知

AWS Marketplace は EventBridge、以前は Amazon CloudWatch Events と呼ばれていた Amazon と統合されています。EventBridge は、アプリケーションをさまざまなソースのデータに接続するために使用できるイベントバスサービスです。詳細については、[「Amazon ユーザーガイド EventBridge」](#)を参照してください。

購入者は、販売者がオファーを作成して購入できるようにする AWS Marketplace たびに、からイベントを受け取ります。イベントには、ID、有効期限、製品の詳細、販売者の名前などの詳細が含まれます。

トピック

- [AWS Marketplace Discovery API Amazon EventBridge イベント](#)


AWS Marketplace Discovery API Amazon EventBridge イベント

このトピックでは、次の表に示す各イベントに関する詳細情報を提供します。

販売者によるアクション	購入者が受信したイベント	関連トピック
オファーを作成して購入できるようにします。	Listing Available	the section called “新規出品のイベント”

新規出品のイベント

販売者がオファーを作成して購入できるようになると、購入者は Listing Available の詳細タイプのイベントを受け取ります。

 Note

EventBridge ルールの作成については、[「Amazon ユーザーガイド」の「Amazon EventBridge ルール」](#)を参照してください。 EventBridge

次の例は、Listing Available イベント本文のエントリです。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "Listing Available",
  "source": "aws.discovery-marketplace",
  "account": "123456789012",
  "time": "2023-08-26T00:00:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "requestId": "3d4c9f9b-b809-4f5e-9fac-a9ae98b05cbb",
    "catalog": "AWSMarketplace",
    "offer": {
```

```
    "id": "offer-1234567890123",
    "expirationDate": "2025-08-26T00:00:00Z"
  },
  "product": {
    "id": "bbbbaaaa-abcd-1111-abcd-666666666666",
    "title": "Product Title"
  },
  "sellerOfRecord": {
    "name": "Seller Name"
  }
}
```

AWS Marketplace 調達システムとの統合

AWS Marketplace と Coupa または SAP Ariba 調達ソフトウェアの統合を設定できます。設定を完了すると、組織内のユーザーは調達ソフトウェアを使用して AWS Marketplace 製品を検索し、製品のサブスクリプションをリクエストできます。サブスクリプションリクエストが承認されると、取引が完了し、ユーザーにソフトウェアのサブスクリプションが利用可能であることが通知されます。ユーザーがサインインすると AWS Marketplace、ソフトウェア製品は購入したサブスクリプションとしてリストされ、使用できます。調達システムとの統合により、AWS Marketplace 請求書を発注書システムと統合することもできます。

調達統合の仕組み

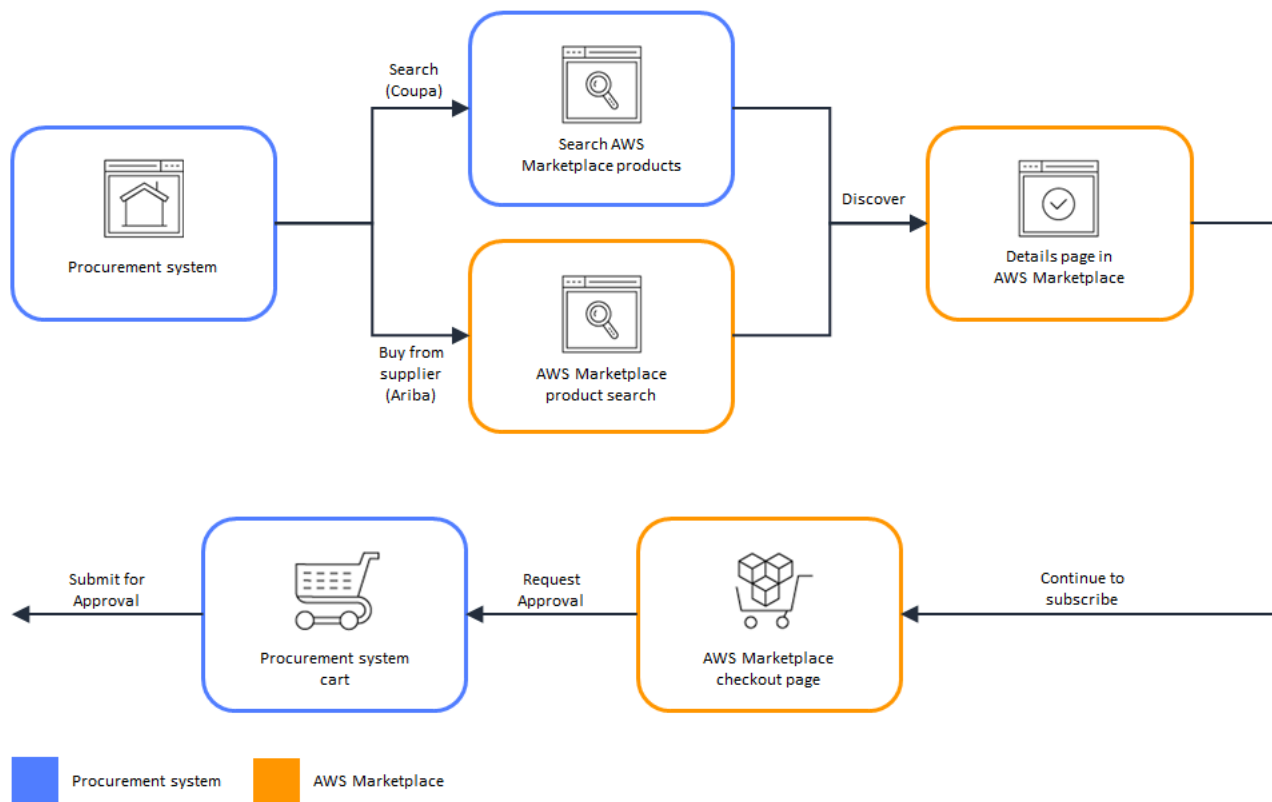
コマース拡張マークアップ言語 (cXML) プロトコル AWS Marketplace に従って と統合するように調達ソフトウェアを設定できます。この統合は、サードパーティーのカタログにパンチアウトとも呼ばれるアクセスポイントを作成します。

統合は、調達システムによってわずかに異なります。

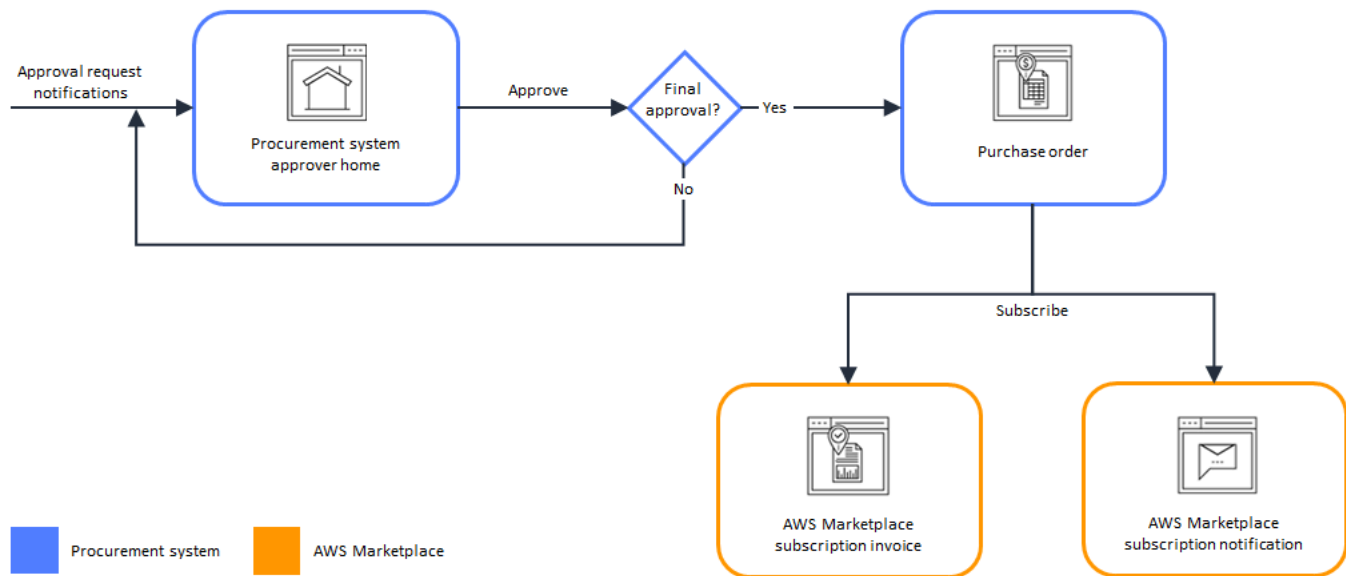
- Coupa – Coupa Open Buy 機能を使用して、Coupa 内 AWS Marketplace から検索できます。Coupa は検索結果を表示し、ユーザーが製品を選択すると、AWS Marketplace にリダイレクトされて詳細が表示されます。または、Coupa の調達ソフトウェアのユーザーは、ホームページのオンラインショッピングセクションで AWS Marketplace カタログにアクセスできます。ユーザーは、で直接開始 AWS Marketplace して製品を参照することもできます。
- SAP Ariba – Ariba はユーザーを AWS Marketplace にリダイレクトしてソフトウェアを検索し、製品の詳細を取得します。管理者がパンチアウト統合を設定すると、Ariba の調達ソフトウェアのユーザーは Catalog タブを選択し、カタログを選択して AWS Marketplace ソフトウェアを検索できます AWS Marketplace 。これにより、関心のある製品を見つける AWS Marketplace ために にリダイレクトされます。

Ariba ユーザーは AWS Marketplaceではなく、Ariba 内から購入を開始する必要があります。

ユーザーがで閲覧しているサブスクリプションを購入すると AWS Marketplace、内でサブスクリプションリクエストが作成されます AWS Marketplace。製品のサブスクリプションページでは、購入を完了する代わりに、ユーザーは承認をリクエストします。承認プロセスを完了するために、リクエストは調達システムのショッピングカートに返送されます。次の図は、調達システムサブスクリプションリクエストのプロセスを示しています。



調達システムが リクエストを受信すると AWS Marketplace、調達システムはワークフローを開始して承認プロセスを完了します。リクエストが承認されると、調達システムの発注書システムは AWS Marketplace の取引を自動的に完了し、ユーザーにサブスクリプションのデプロイ準備ができたことを通知します。リクエストは、購入を完了するために AWS Marketplace に戻る必要はありません。ただし、購入した製品の使用方法 AWS Marketplace については、「」に戻りたい場合があります。AWS Marketplace は、へのアクセスに使用した AWS アカウントに E メールメッセージを送信します AWS Marketplace。E メールメッセージは、サブスクリプションが成功し、ソフトウェアが から利用可能であることを受信者に通知します AWS Marketplace。次の図は、調達システムサブスクリプションリクエストの承認プロセスを示しています。



調達システムとの統合に関するその他の注意事項は次のとおりです。

- 無料試用版には料金がかからないため、調達システムでは請求書は生成されません。
- 料金に加えて 1 回限りの料金が pay-as-you-go かかる契約には、2 セットの承認が必要になる場合があります。1 つの承認は契約 (または年間) 料金で、もう 1 つは時間単位またはユニット単位の料金 () です pay-as-you-go。
- PSI (調達システム統合) を利用しているお客様は、無料製品と BYOL 製品の事前承認を有効にできます。無料版と BYOL 版の 2 つの設定があります。設定を有効にすると、注文は で事前に承認されるため AWS Marketplace、顧客は承認のために調達システムに注文を送信する必要はありません。この設定が無効になっている場合、顧客は [リクエスト承認] ボタンを使用して調達システムに承認を送信します。無料製品と BYOL 製品の事前承認設定を無効にすると、顧客の調達システムで 0.00 USD の注文が生成されます。調達システム統合の詳細については、「<https://aws.amazon.com/marketplace/features/procurementsystem>」を参照してください。

調達システム統合の設定

AWS Marketplace と調達システムの統合を設定するには、 でプロセスを開始し AWS Marketplace、調達システムでプロセスを完了します。AWS Marketplace で生成された情報を使用して、調達システムパンチアウトを設定します。設定を完了するには、使用するアカウントが以下の要件を満たしている必要があります。

- AWS Marketplace 設定を完了する AWS アカウント ために使用される は、管理アカウントであり、AWSMarketplaceProcurementSystemAdminFullAccess 管理ポリシーで定義されている AWS Identity and Access Management (IAM) アクセス許可を持っている必要があります。
- 設定の完了に使用される調達システムアカウントは、調達システムに契約、サプライヤー、パンチアウトカタログを設定するための管理アクセスを持つ必要があります。

IAM 許可の設定

次の IAM アクセス許可は [AWS 管理ポリシー](#) :

[AWSMarketplaceProcurementSystemAdminFullAccess](#) 管理ポリシーにあり、AWS Marketplace と調達システムの統合を設定するために必要です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

アクセス許可を手動で設定するのではなく、IAM マネージドアクセス許可を使用することをお勧めします。この方法を使用すると、ヒューマンエラーが発生しにくくなり、アクセス許可が変更された場合に、管理ポリシーが更新されます。AWS Marketplaceでの IAM の設定と使用の詳細については、「[のセキュリティ AWS Marketplace](#)」を参照してください。


Coupa と統合 AWS Marketplace するための の設定

IAM アクセス許可を設定したら、Coupa と AWS Marketplace の統合を設定する準備が整います。[調達の管理] に移動します。[調達システムの管理] ペインで、パンチアウトの名前と説明を入力

します。統合をテストモードに切り替えて、準備ができるまで製品サブスクリプションを作成せずに統合をテストすることもできます。統合の AWS Marketplace 部分を設定するには、次の手順を実行します。

Coupa と統合 AWS Marketplace するように を設定するには

1. [AWS Marketplace Manage Procurement Systems](#) の [Procurement systems (調達システム)] で、[Set up Coupa integration (Coupa 統合の設定)] を選択します。
2. [Manage Coupa integration (Coupa 統合の管理)] ページの [Account information (アカウント情報)] で、統合の名前と説明を入力します。


 Note

Software as a Service (SaaS) 契約製品のサブスクライブに使用されるコマース拡張マークアップ言語 (cXML) 発注書を AWS Billing コンソールで参照できます。その場合は、AWS Marketplace 設定でサービスにリンクされたロールを使用して請求統合を有効にできます。

3. リダイレクトを有効にするとテストモード の設定をオンまたはオフにし、保存 を選択して AWS Marketplace システム内の統合を完了できます。

で統合が完了したら AWS Marketplace、Coupa で統合をセットアップする必要があります。このページで生成された情報を使用して、Coupa システムのパンチアウトを設定します。

AWS Marketplace 設定はデフォルトでテストモードが有効になります。テストモードでは、サブスクリプションリクエストは Coupa バックエンドに送られるため、フロー全体を確認できますが、最終的な請求書は作成されません。これは、設定を完了してから計画的にパンチアウトを有効するのに役立ちます。

 Note

必要に応じてテストモードをオンまたはオフに切り替えることができます。統合が完了したら、テストモードをオフにすることを忘れないでください。そうしない場合、システム内のユーザーがリクエストを作成しているように見えますが、ソフトウェアは購入されません。

Coupa の設定

Coupa システムでとの統合を設定するには、「」の AWS Marketplace 「Coupa 統合の管理」ページの「購入情報」ペインから情報をコピーします AWS Marketplace。この情報を使用して以下のリンクのステップを完了し、ガイドに従って Coupa 調達システムを設定します。

- [Coupa パンチアウト設定](#)
- [cXML 発注書用のサプライヤーの設定](#)

Note

で使用される UNSPSC コードについては AWS Marketplace、[AWS Marketplaceが使用する UNSPSC コード](#)「」を参照してください。

SAP Ariba と統合 AWS Marketplace するための の設定

を Ariba と統合 AWS Marketplace するように設定するには、AWS Marketplace 運用チームと協力してレベル 1 のパンチアウトを作成する必要があります。SAP Ariba のパンチアウトの詳細については、SAP コミュニティウェブサイト [の「SAP Ariba の概要 PunchOut」](#)を参照してください。

セットアップを設定する準備として、以下の情報を収集してください。

- AWS アカウント ID。が AWS 組織の一部である場合 AWS アカウント は、管理アカウント ID も必要です。
- SAP Ariba システムの Ariba ネットワーク ID (ANID)。

Note

Ariba の ANID に関する情報、および Ariba に関するその他の質問への回答については、SAP Ariba ウェブサイトの「[サプライヤー向け Ariba ネットワーク:よくある質問](#)」ページを参照してください。

を Ariba と統合 AWS Marketplace するように設定するには

1. [AWS Marketplace Manage Procurement Systems](#) の [調達システム] で、[Ariba 統合の設定] を選択します。

2. [SAP Ariba 統合の管理] ページの [アカウント情報] で、統合の名前と説明、Ariba システムの [SAP Ariba ネットワーク ID] (ANID) を入力します。

Note

SaaS 契約製品のサブスクライブに使用される cXML 発注書を AWS Billing コンソールで参照できます。その場合は、AWS Marketplace 設定でサービスにリンクされたロールを使用して請求統合を有効にできます。

3. テストモードが有効になっていることを確認し、保存を選択して AWS Marketplace 統合設定を保存します。
4. SAP Ariba 統合の作成プロセスを開始するには、[お問い合わせください](#)。上記の情報を含めてください。AWS Marketplace から Ariba 統合の設定とテストの手順をお送りします。

Note

とのサプライヤー関係を作成するには、SAP Ariba システムへの管理者アクセス権が必要です AWS Marketplace。

AWS Marketplace チームの指示と設定に従って、SAP Ariba テスト環境で統合を作成し、テストモードで AWS Marketplace を実行します。テスト環境では、サブスクリプションリクエストは Ariba バックエンドに送られるため、サブスクリプションを作成しなくても、承認を含む完全なフローを確認でき AWS Marketplace、請求書は生成されません。この方法では、本番環境でパンチアウトを有効にする前に設定をテストできます。テストが完了し、本番環境に移行する準備ができたなら、[当社に連絡して](#)実稼働環境でアカウントを設定してください。


Note

統合のテストが終わったら、忘れずに本番環境に移行してください。そうしない場合、システム内のユーザーは自分がリクエストを作成していると思っても、ソフトウェアは購入されません。

テストが完了し、AWS Marketplace チームと協力してテストモードをオフにすると、統合は完了です。

SAP Ariba の設定の詳細については、SAP Ariba の以下のトピックを参照してください。

- [SAP Ariba PunchOut](#) ウェブサイトの SAP Ariba
- [SAP Community](#) ウェブサイトの SAP Ariba の概要 PunchOut

 Note

で使用される UNSPSC コードについては AWS Marketplace、「」を参照してください [AWS Marketplaceが使用する UNSPSC コード](#)。

AWS Marketplaceが使用する UNSPSC コード

AWS Marketplace は、調達カートに返送されるソフトウェアリストに、以下の国際連合標準製品およびサービスコード (UNSPSC) を使用します: 43232701

調達システムの統合の無効化

Coupa または SAP Ariba との統合を無効にするには、調達システム内からパンチアウト統合を削除する必要があります。これを行うには、Coupa または Ariba 内 AWS Marketplace からの自動リダイレクト機能を無効にします。これにより統合は無効になりますが、設定は維持され、簡単に再有効化できます。

AWS Marketplace 側の統合設定を完全に削除する必要がある場合は、[にお問い合わせください](#)。

無料トライアル

に記載されている一部の製品では AWS Marketplace、無料トライアルを提供しています。無料トライアルでは、購入前にソフトウェアを試用できます。無料トライアルは、一定の無料使用量または期間に制限されています。無料トライアル期間を開始すると一時停止できません。

ソフトウェアとインフラストラクチャの料金

販売者が提供する無料トライアルは、に記載されている製品のソフトウェア料金にのみ適用されます AWS Marketplace。購入者は、ソフトウェアの料金に無料トライアルが含まれているかどうか AWS Marketplace にかかわらず、から販売者の製品を使用する際のすべてのインフラストラクチャコストを負担する責任があります。これらのインフラストラクチャコストはによって設定 AWS され、それぞれの料金ページで利用できます。例えば、無料トライアルがある Amazon マシンイメージ (AMI) 製品をサブスクライブする場合、無料トライアル中の AMI の使用に対しては課金されません。ただし、AMI 製品を実行する Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに対して課金される場合があります。

Note

製品によっては、実行するために追加の AWS インフラストラクチャが必要になる場合があります。例えば、販売者は、ロードバランサー、ストレージ、データベース、またはその他のを AWS のサービスにデプロイするデプロイ手順またはテンプレートを提供する場合があります AWS アカウント。販売 AWS のサービス 者が製品に何を必要としているかを理解するには、「」に記載されている製品の詳細ページを確認してください AWS Marketplace。次に、該当する AWS のサービスの料金ページを確認します。

AMI ベースの製品の無料トライアル

の年間料金で時間単位または時間単位の AMI 製品には、無料トライアル AWS Marketplace があります。無料トライアルにサブスクライブすると、販売者が設定した期間中、AMI 製品の Amazon EC2 インスタンスを 1 つ、時間単位のソフトウェア料金なしで実行できます。インフラストラクチャの料金は、ユーザーの負担となります。追加の Amazon EC2 インスタンスを起動するには、インスタンスごとに時間単位のソフトウェア料金が発生します。無料トライアルは、有効期限が切れると自動的に有料サブスクリプションに切り替わります。

無料トライアルの終了前に Amazon EC2 インスタンスを終了しないと、無料トライアルが終了した時点から時間単位のソフトウェア料金が発生します。無料トライアルのサブスクリプションを解除しても、Amazon EC2 インスタンスは自動的に終了せず、継続して使用するとソフトウェア料金が発生します。インフラストラクチャの料金の詳細については、「[Amazon EC2 料金表](#)」を参照してください。

コンテナベースの製品の無料トライアル

で時間単位または時間単位の長期料金を使用する一部のコンテナ製品 AWS Marketplace には、無料トライアルがあります。無料トライアルにサブスクライブすると、複数の Amazon Elastic Container Service (Amazon ECS) タスクまたは Amazon Elastic Kubernetes Service (Amazon EKS) ポッドを時間単位のソフトウェア料金なしで一定期間実行できます。含まれるタスクまたはポッドの数、無料トライアルの期間は、販売者が設定します。インフラストラクチャの料金は、ユーザーの負担となります。無料トライアルに含まれる数を超過して追加のタスクまたはポッドを起動すると、タスクまたはポッドごとに時間単位のソフトウェア料金が発生します。無料トライアルは、有効期限が切れると自動的に有料サブスクリプションに切り替わります。

無料トライアルの終了前にタスクやポッドを終了しないと、無料トライアルが終了した時点から時間単位のソフトウェア料金が発生します。無料トライアルのサブスクリプションを解除しても、タスクやポッドは自動的に終了せず、継続して使用するとソフトウェア料金が発生します。これらの料金の詳細については、「[Amazon ECS 料金表](#)」と「[Amazon EKS 料金表](#)」を参照してください。

機械学習製品の無料トライアル

で時間単位の料金を使用する一部の機械学習製品 AWS Marketplace には、無料トライアルがあります。無料トライアルにサブスクライブすると、時間単位のソフトウェア料金を発生させることなく、販売者が設定した期間、Amazon SageMaker エンドポイント、バッチ変換ジョブ、またはトレーニングジョブを実行できます。インフラストラクチャの料金は、ユーザーの負担となります。無料トライアルは、有効期限が切れると自動的に有料サブスクリプションに切り替わります。

無料トライアルが終了する前に Amazon SageMaker エンドポイント、バッチ変換ジョブ、またはトレーニングジョブを終了しない場合、無料トライアルが終了すると時間単位のソフトウェア料金が発生します。無料トライアルのサブスクリプションを解除しても、Amazon SageMaker エンドポイント、バッチ変換ジョブ、またはトレーニングジョブは自動的に終了せず、引き続き使用するとソフトウェア料金が発生します。インフラストラクチャ料金の詳細については、「[Amazon SageMaker 料金表](#)」を参照してください。

SaaS 製品の無料トライアル

の Software as a Service (SaaS) 製品 AWS Marketplace には無料トライアルがあります。SaaS の無料トライアルは、自動的に有料契約に切り替わりません。無料トライアルが不要になった場合は、期限切れにできます。詳細については、「[SaaS 無料トライアル](#)」を参照してください。

AWS Marketplace での AWS 無料利用枠の使用

Amazon Web Services (AWS) の新規のお客様がクラウドを使い始められるように、AWS では無料利用枠を導入しています。無料利用枠は、新しいアプリケーションの起動、クラウド上での既存アプリケーションのテスト、AWS の体験利用のみなど、クラウド上で実行するあらゆるものにご使用いただけます。無料利用期間が終了した場合 (またはアプリケーションの使用が無料利用枠の制限を超えた場合)、標準の pay-as-you-go サービス料金をお支払いいただきます。詳細については、「[AWS無料利用枠](#)」を参照してください。

AWS 無料利用枠の対象のお客様は、無料の AWS Marketplace ソフトウェアを 1 年間、毎月最大 750 時間まで Amazon Elastic Compute Cloud (Amazon EC2) をご利用いただけます。使用開始するには、[AWS Marketplace](#) を参照してください。

AWS Service Catalog への AWS Marketplace のサブスクリプションの追加

Service Catalog では、Amazon Web Services (AWS) での使用が承認された IT サービスのカタログを作成および管理できます。この IT サービスには、仮想マシンイメージ、サーバー、ソフトウェア、データベースから包括的な多層アプリケーションアーキテクチャまで、あらゆるものが含まれます。Service Catalog では、一般的にデプロイされる IT サービスを一元管理できます。Service Catalog により、一貫性のあるガバナンスを実現してコンプライアンス要件を満たし、ユーザーは必要な承認されたサービスのみをすばやくデプロイできるようになります。

詳細については、「Service Catalog [管理者ガイド](#)」の「[ポートフォリオへの AWS Marketplace 製品の追加](#)」を参照してください。

製品レビュー

AWS Marketplace は、購入者が賢明な購入選択を行うために必要な情報を取得したいと考えています。AWS のお客様は、AWS Marketplace に表示されるアイテムのレビューコメントを送信できます。好意的な意見と否定的な意見のどちらもお寄せください。

Note

データ製品は、製品レビューをサポートしていません。

ガイドライン

製品に AWS Marketplace サブスクリプションしているユーザーは誰でもそのレビューを作成できます。製品レビューを書く際には、以下のガイドラインに従ってください。

- 理由を記載する - レビューには製品の好き嫌いだけでなく、その理由も書かれていると大変参考になります。関連する製品についての意見やそれらの製品との比較結果を書いてもかまいません。
- 具体的に記載する - レビューでは、製品の具体的な機能やエクスペリエンスに焦点を当てます。ビデオレビューの場合は、簡単な紹介を書きます。
- 簡潔にする - レビューコメントは 20~5,000 語でお願いいたします。理想的な長さは 75~500 語です。
- 正直に記載する - 肯定的か否定的かを問わず、製品に関する正直な意見をお聞かせください。それらの意見は顧客による購入の決定に役立つと考えています。
- 透明性を保つ - レビューを行うことを条件に無料の製品を受け取った場合は、その旨を明確かつわかりやすい形で開示してください。

制限事項

AWS は、次のいずれかのコンテンツを含むレビューを削除する権利を有します。

- 以下を含む不快な資料:
 - ひわいな内容や不快な内容
 - 不敬な意見や悪意のある意見
 - 違法行為や不道德な行為を促す内容

- 以下を含む販促コンテンツ:
 - 広告、販促資料、または同じ主張を繰り返す投稿
 - 個人や会社による、または個人や会社のための、製品や直接競合する製品の金銭的利益につながる意見 (作成者、公開者、製造者、または製品を販売するサードパーティーの業者によるレビューなど)
 - 製品の無料コピー以外の対価を受けることを目的としたレビューコメント (有料の宣伝パッケージに含まれるレビューなど)
 - 製品への検証可能なサブスクリプションのない顧客のレビューコメント
- 以下を含む不適切なコンテンツ:
 - 他者からコピーされたコンテンツ (過度の引用など)
 - Amazon.com 以外の連絡先または URL
 - 在庫や別の注文/発送の詳細
 - ウォーターマークを含む動画
 - ページで閲覧できる他のレビューに対するコメント (ページの表示が予告なく変更されることがあるため)
 - 外国語の内容 (製品と明らかに関係がある場合を除く)
 - 形式に問題があるテキスト
- 以下を含む主題から外れた情報:
 - 販売者や配送に関するフィードバック
 - カタログや製品説明の誤植や間違いに関するフィードバック (これについては、製品ページの下にあるフィードバックフォームを使用)

カスタマーレビューに関するご質問は、[お問い合わせ](#)までご連絡ください。

タイミングと心構え

当社では、製品レビューをできるだけ迅速に処理するよう努めています。ただし、AWS Marketplace チームはレビューワーと販売者の両方と通信して、フィードバックが当社のおよび [the section called “ガイドライン”](#) と有効であることを確認する必要があります [the section called “制限事項”](#)。プロセスの完了にかかる時間については、「AWS Marketplace 販売者ガイド」に記載されているものと同じ「[タイミングと心構え](#)」のガイダンスに従います。

サポート情報

一般的な AWS Marketplace 問題については、[にお問い合わせください](#)。を通じて購入したソフトウェアに関するご質問は AWS Marketplace、ソフトウェア販売者にお問い合わせください。

AWS Marketplace Vendor Insights

AWS Marketplace Vendor Insights は、信頼でき、業界標準を満たすソフトウェアの調達を支援することで、ソフトウェアリスク評価を簡素化します。AWS Marketplace Vendor Insights を使用すると、単一のユーザーインターフェイスから製品のセキュリティプロファイルをほぼリアルタイムでモニタリングできます。ソフトウェア製品のセキュリティ情報をダッシュボードに表示することにより、評価にかかる労力を低減できます。ダッシュボードを使用して、データプライバシー、アプリケーションセキュリティ、アクセスコントロールなどの情報を表示および評価できます。

AWS Marketplace Vendor Insights は、業界標準を継続的に満たす信頼できるソフトウェアを調達することで、販売者からセキュリティデータを収集し、購入者をサポートします。と統合することで AWS Audit Manager、AWS Marketplace Vendor Insights は 内の Software as a Service (SaaS) 製品の up-to-date セキュリティ情報を自動的に取得できます AWS Marketplace。AWS Marketplace Vendor Insights は AWS Artifact サードパーティーのレポートと統合されるため、のレポートとともに、ベンダーソフトウェアのオンデマンドコンプライアンスレポートにアクセスできます AWS のサービス。

AWS Marketplace Vendor Insights は、10 のコントロールカテゴリと複数のコントロールからの証拠ベースの情報を提供します。次の 3 つのソースから、証拠に基づいた情報を収集します。

- ベンダーの本番環境アカウント - 複数のコントロールのうちの 25 のコントロールが、ベンダーの本番環境アカウントからのライブエビデンスの収集をサポートしています。各コントロールのライブ証拠は、販売者の AWS リソースの設定を評価する 1 つ以上の AWS Config ルールによって生成されます。ライブエビデンスは、複数のソースからのデータを一貫して更新して最新の情報を表示する方法です。は証拠を AWS Audit Manager キャプチャし、AWS Marketplace Vendor Insights ダッシュボードに配信します。
- Vendor ISO 27001 および SOC 2 Type II レポート - コントロールカテゴリは、国際標準化機構 (ISO) レポートおよび Service Organization Controls (SOC) 2 レポートのコントロールにマッピングされています。販売者がこれらのレポートを AWS Marketplace Vendor Insights と共有すると、サービスは関連するデータを抽出し、ダッシュボードに表示します。
- Vendor 自己評価 - 販売者によって自己評価を行います。また、AWS Marketplace Vendor Insights のセキュリティ自己評価や CAIQ (Consensus Assessment Initiative Questionnaire) など、他の自己評価を作成してアップロードできます。

次の動画では、AWS Marketplace Vendor Insights を使用して、SaaS リスク評価を簡素化する方法を示しています。

Vendor AWS Marketplace Insights を購入者として開始する

AWS Marketplace Vendor Insights は、 で利用可能なソフトウェア製品のセキュリティ情報を提供します AWS Marketplace。AWS Marketplace Vendor Insights を使用すると、AWS Marketplaceの製品のセキュリティプロファイルを表示できます。

AWS Marketplace Vendor Insights ダッシュボードには、AWS Marketplace Vendor Insights を使用して製品を評価するソフトウェア製品のコンプライアンスアーティファクトとセキュリティコントロール情報が表示されます。AWS Marketplace Vendor Insights は、ダッシュボードに表示される複数のセキュリティコントロールに関する証拠ベースの情報を収集します。

AWS Marketplace Vendor Insights を使用して製品のセキュリティおよびコンプライアンス情報にアクセスする場合、料金はかかりません。

AWS Marketplace Vendor Insights で製品を検索する

Vendor AWS Marketplace Insights ダッシュボードで製品のプロファイルと概要情報を表示したり、カテゴリコントロールを選択して、製品で収集されたデータの詳細を確認したりできます。AWS Marketplace Vendor Insights AWS Marketplace を使用して で製品を検索するには、次の手順を使用します。

AWS Marketplace Vendor Insights で製品を検索するには

1. にサインイン AWS Management Console し、 [AWS Marketplace コンソール](#) を開きます。
2. [すべての製品を表示] を選択します。
3. [Vendor Insights] タグが付いた製品を表示します。
4. [ベンダーインサイトの検索結果を絞り込む] で、[セキュリティプロファイル] を選択します。
5. [製品の詳細] ページの [製品概要] から、[ベンダーインサイト] セクションを選択します。
6. [この製品のすべてのプロファイルを表示] を選択します。
7. [概要] では、製品に関する詳細と、受け取ったセキュリティ証明書の一覧を表示できます。
8. [アクセスをリクエスト] を選択します。
9. Vendor Insights データへのアクセスをリクエストページで情報を入力し、アクセスをリクエストを選択します。

この製品の AWS Marketplace Vendor Insights データへのアクセスのリクエストが成功したことを示すメッセージが表示されます。

サブスクライブして、評価データへのアクセスをリクエストしてください。

AWS Marketplace Vendor Insights を使用すると、ベンダーソフトウェアのセキュリティプロファイルを継続的にモニタリングできます。まず、モニタリングする製品のベンダー評価データをサブスクライブするか、アクセスをリクエストします。製品の評価データをモニタリングする必要がなくなった場合、その製品の評価データの配信を停止できます。AWS Marketplace Vendor Insights を使用して製品のセキュリティおよびコンプライアンス情報にアクセスする場合、料金はかかりません。料金の詳細については、「[AWS Marketplace Vendor Insights 料金表](#)」を参照してください。

特定のベンダー製品のすべての評価データにアクセスするには、その製品の評価データをサブスクライブする必要があります。

製品の AWS Marketplace Vendor Insights 評価データをサブスクライブするには

1. にサインイン AWS Management Console し、[AWS Marketplace コンソール](#) を開きます。
2. [ベンダーインサイト] を選択します。
3. [ベンダーインサイト] から製品を選択します。
4. [概要] タブを選択します。
5. [アクセスをリクエスト] を選択します。
6. 指定されたフィールドに、お客様の情報を入力します。
7. 完了したら、[アクセスをリクエスト] を選択します。

この製品のすべてのベンダー評価データへのアクセスをリクエストしたことを示す成功メッセージが表示されます。

評価データのサブスクリプションを解除する

そのベンダーの製品の評価データにアクセスする必要がなくなった場合、その製品の評価データの配信を停止できます。

製品の AWS Marketplace Vendor Insights 評価データのサブスクリプションを解除するには

1. にサインイン AWS Management Console し、[AWS Marketplace コンソール](#) を開きます。
2. [ベンダーインサイト] を選択します。
3. [製品の詳細] ページで製品を選択し、[サブスクリプション解除] を選択します。

4. AWS Marketplace Vendor Insights データのサブスクリプション解除に記載されている用語をお読みください。
5. テキスト入力フィールドに **Unsubscribe** を入力し、[サブスクリプション解除] を選択します。

Vendor AWS Marketplace Insights データのサブスクリプションを解除し、アクセスに対して課金されなくなることを示す成功メッセージが表示されます。

AWS Marketplace Vendor Insights による製品のセキュリティプロファイルの表示

AWS Marketplace Vendor Insights は、販売者からセキュリティデータを収集します。製品のセキュリティプロファイルには、製品のセキュリティ、回復力、コンプライアンス、その他の評価に必要な要素に関する最新情報が表示されます。この情報は、常に業界標準に適合し、信頼できるソフトウェアの調達を支援することにより、お客様をはじめとする購入者をサポートします。評価対象の Software as a Service (SaaS) 製品ごとに、AWS Marketplace Vendor Insights は複数のセキュリティコントロールに関する証拠ベースの情報を収集します。

トピック

- [AWS Marketplace Vendor Insights のダッシュボード](#)
- [SaaS 製品のセキュリティプロファイルを表示する](#)
- [コントロールカテゴリを理解する](#)

AWS Marketplace Vendor Insights のダッシュボード

ダッシュボードには、AWS Marketplace Vendor Insights によって収集されたソフトウェア製品のコンプライアンスアーティファクトとセキュリティコントロール情報が表示されます。すべてのセキュリティ [コントロールカテゴリ](#) について、データレジデンシーの変更や認証の期限切れなど、証拠に基づく情報を提供します。統合ダッシュボードには、コンプライアンス情報の変更が表示されません。AWS Marketplace Vendor Insights を使用すると、追加のアンケートを作成し、リスク評価ソフトウェアを使用する必要がなくなります。ダッシュボードは常に更新および検証されているため、調達後もソフトウェアのセキュリティコントロールを継続的にモニタリングできます。

SaaS 製品のセキュリティプロファイルを表示する

AWS Marketplace Vendor Insights は、販売者のソフトウェアに関する意思決定に役立ちます。AWS Marketplace Vendor Insights は、10 のコントロールカテゴリと複数のコントロールにわたる販

売者の証拠ベースの情報からデータを抽出します。ダッシュボードで SaaS 製品のプロフィールと概要情報を表示したり、コントロールカテゴリを選択して、収集したデータの詳細を確認したりすることができます。プロフィールを通じてコンプライアンス情報を表示するには、製品をサブスクライブし、アクセス許可を付与されている必要があります。

1. にサインイン AWS Management Console し、[AWS Marketplace コンソール](#) を開きます。
2. [ベンダーインサイト] を選択します。
3. [ベンダーインサイト] から製品を選択します。
4. [プロフィールの詳細] ページで、[セキュリティとコンプライアンス] タブを選択します。

Note

赤丸の中の数字は、非準拠のコントロールの数を示しています。

5. [コントロールカテゴリ] では、一覧表示されたカテゴリの下のテキストを選択すると、詳細情報が表示されます。
 - 最初の [コントロール名] (適用される法律、規制、契約上の要求事項を確実に遵守するためのポリシー/手順がありますか?) を選択します。
 - 表示された情報を読んでください。また、AWS Artifact サードパーティーのレポートからレポートを表示したり、監査人からの例外を表示したりすることもできます。
 - 上のナビゲーションで製品名を選択すると、[製品の詳細] ページに戻ります。

コントロールカテゴリを理解する

AWS Marketplace Vendor Insights は、10 のコントロールカテゴリ内の複数のコントロールから証拠ベースの情報を提供します。AWS Marketplace Vendor Insights は、ベンダーの本番稼働用アカウント、ベンダーの自己評価、ベンダーの ISO 27001 および SOC 2 Type II レポートの 3 つのソースから情報を収集します。これらのソースの詳細については、「[AWS Marketplace Vendor Insights](#)」を参照してください。

次のリストは、各コントロールカテゴリの説明です。

アクセス管理

システムまたはアプリケーションへのアクセスを識別、追跡、管理、コントロールします。

アプリケーションセキュリティ

アプリケーションの設計、開発、テストを行う際に、アプリケーションにセキュリティが組み込まれているかどうかを検証します。

監査、コンプライアンス、セキュリティポリシー

組織の規制要件の遵守状況を評価します。

ビジネスの回復力と継続性

事業の継続性を維持しながら、迅速に混乱に適応する組織の能力を評価します。

データセキュリティ

データと資産を保護します。

エンドユーザーデバイスのセキュリティ

エンドユーザーのポータブルデバイスと、それらが接続されているネットワークを脅威や脆弱性から保護します。

人事

従業員の雇用、給与支払い、退職などのプロセスにおける機密データの取り扱いについて、従業員関連部門を評価します。

インフラストラクチャセキュリティ

重要な資産を脅威や脆弱性から保護します。

リスク管理とインシデント対応

許容可能と判断したリスクのレベルと、リスクや攻撃に対応するために講じられた措置を評価します。

セキュリティと設定に関するポリシー

組織の資産を保護するセキュリティポリシーとセキュリティ設定を評価します。

コントロールカテゴリセット

次の表は、各カテゴリの詳細情報と、収集された各カテゴリの値に関する情報を示しています。次の表は、表の各列に含まれる情報の種類を示しています。

- **コントロールセット** - コントロールはコントロールセットに割り当てられ、各コントロールにはそのカテゴリのセキュリティ機能を反映します。各カテゴリには、複数のコントロールセットがあります。
- **コントロール名** - ポリシーまたはプロシージャの名前。「手動による認証が必要」とは、ポリシーまたは手順の書面による確認または文書化が必要であることを意味します。
- **コントロールの説明** - このポリシーまたは手続きに関して必要な質問、情報、または文書。
- **証拠抽出の詳細** - このカテゴリに必要なデータを追加で取得するために必要な、コントロールに関する情報と背景情報。
- **サンプル値** - このカテゴリのコンプライアンス値が規制基準に準拠していることを示すガイダンスのために示した例。

トピック

- [アクセス管理コントロール](#)
- [アプリケーションのセキュリティコントロール](#)
- [監査とコンプライアンスのコントロール](#)
- [ビジネスの回復力のコントロール](#)
- [データセキュリティコントロール](#)
- [エンドユーザーデバイスのセキュリティコントロール](#)
- [人事コントロール](#)
- [インフラストラクチャのセキュリティ](#)
- [リスク管理とインシデント対応のコントロール](#)
- [セキュリティと設定に関するポリシーコントロール](#)

アクセス管理コントロール

アクセス管理コントロールは、システムまたはアプリケーションへのアクセスを識別、追跡、管理、制御します。この表は、アクセス管理コントロールの値と説明をまとめたものです。

コントロールセット	コントロールタイトル	コントロールの記述
安全な認証	アクセス管理 3.1.1 - 安全な認証 - の UserId 個人データ (手動による認証が必要)	ユーザー ID に個人情報 (名前や E 外) が必要ですか?

コントロールセット	コントロールタイトル	コントロールの記述
	アクセス管理 3.1.2 - 安全な認証 - アプリケーションが 2 要素認証をサポート (手動による認証が必要)	アプリケーションは 2 要素認証を すか?
	アクセス管理 3.1.3 - 安全な認証 - アカ ウントロックアウト (手動による認証が 必要)	ログインに複数回失敗した場合、 はロックされますか?
認証情報管理	アクセス管理 3.2.1 - 認証情報管理 - パ スワードポリシー	アプリケーションには、強力なパ がありますか?
	アクセス管理 3.2.2 - 認証情報管理 - パ スワード暗号化	パスワードポリシーは、サインイン ワードとユーザー ID) を転送時に暗 ソルトでハッシュ化することを要
	アクセス管理 3.2.3 - 認証情報管理 - シークレット管理	シークレット管理サービスを使用
	アクセス管理 3.2.4 - 認証情報管理 - コード内の認証情報 (手動による認証が 必要)	コードに認証情報が含まれていま
本番環境へのアクセス	アクセス管理 3.3.1 - 本番環境へのアク セス - シングルサインオン (手動による 認証が必要)	SSO は本番環境にアクセスできる すか?

コントロールセット	コントロールタイトル	コントロールの記述
	アクセス管理 3.3.2 - 本番環境へのアクセス - 2 要素認証	本番環境またはホスト環境にアクセス認証が必要ですか？
	アクセス管理 3.3.3 - 本番環境へのアクセス - ルートユーザー (手動による認証が必要)	ルートユーザーは例外的に本番環境のみ使用されますか？
	アクセス管理 3.3.4 - 本番環境へのアクセス - ルートユーザー MFA	ルートユーザーには多要素認証 (MFA) が必要ですか？
	アクセス管理 3.3.5 - 本番環境へのアクセス - リモートアクセス	本番環境へのリモートアクセスは、チャネルやキーベースの認証などを使用して保護されていますか？
アクセスコントロールポリシー	アクセス管理 3.4.1 - アクセスコントロールポリシー - 最小特権アクセス	ユーザーが本番環境にアクセスする際に、アクセスポリシーに従っていますか？
	アクセス管理 3.4.2 - アクセスコントロールポリシー - アクセスポリシーのレビュー	本番環境のすべてのアクセスポリシーは、定期的にレビューされていますか？
	アクセス管理 3.4.3 - アクセスコントロールポリシー - ユーザーとセキュリティポリシーの設定 (手動による認証が必要)	このアプリケーションは、ユーザーとユーザーとその権限を設定できるように設計されていますか？

コントロールセット	コントロールタイトル	コントロールの記述
	アクセス管理 3.4.4 - アクセスコントロールポリシー - 論理セグメンテーション (手動による認証が必要)	アプリケーションユーザーには論理セグメンテーションがありますか?
	アクセス管理 3.4.5 - アクセスコントロールポリシー - 終了時のアクセスのレビュー	従業員の退職時または職務変更時のアクセスポリシーが更新されていますか?
アクセスログ	アクセス管理 3.5.1 - アクセスログ	本番環境で個々のユーザーが実行されているすべてのログを記録していますか?

アプリケーションのセキュリティコントロール

アプリケーションのセキュリティコントロールは、アプリケーションの設計、開発、テストを行う際に、アプリケーションにセキュリティが組み込まれているかどうかを検証します。この表は、アプリケーションのセキュリティポリシーコントロールの値と説明をまとめたものです。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
安全なソフトウェア開発ライフサイクル	アプリケーションセキュリティ 4.1.1 - 安全なソフトウェア開発ライフサイクル - 個別の環境	開発環境、テスト環境、ステージング環境は本番環境から分離されていますか?	開発環境、テスト環境、ステージング環境が本番環境から分離されているかどうかを記載します。	はい
	アプリケーションセキュリティ 4.1.2 - 安全なソフトウェア開発ライフサイクル - 個別の環境	セキュリティエンジニアは、デベロッパーと協働して、アプリケーションのセキュリティを確保していますか?	デベロッパーとセキュリティエンジニアが、アプリケーションのセキュリティを確保していますか?	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	ソフトウェア開発 ライフサイクル - 安全なコーディ ング対策	カしてセキュリ ティ対策に取り 組んでいますか？	全なコーディ ング対策について 協力しているか どうかを記載し ます。	
	アプリケーション セキュリティ 4.1.3 - 安全なソ フトウェア開発 ライフサイクル - テスト環境での 顧客データの使 用 (手動による認 証が必要)	顧客データは、 テスト、開発、 または QA 環境 で使用されたこ とはありますか？	顧客データは、 テスト、開発、 または QA 環境 で使用されたこ とはありますか？ その場合、どの ようなデータ が、何のために 使用されていま すか？	いいえ
	アプリケーション セキュリティ 4.1.4 - 安全なソ フトウェア開発 ライフサイクル - 安全な接続	SSL/TLS は、 顧客データを使 用するすべて のウェブページ と通信で有効に なっていますか？	顧客データを使 用するすべての 通信に安全な接 続 (SSL/TLS な ど) を使用するか どうかを記載し ます。	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	アプリケーションセキュリティ 4.1.5 - 安全なソフトウェア開発 ライフサイクル - イメージのバックアップ	アプリケーションイメージのスナップショットはバックアップされていますか？	イメージスナップショット (アプリケーションをサポートするシステムや顧客データをホストするシステムなど) をバックアップするかどうかを記載します。 「はい」の場合、対象範囲内のデータを含むイメージスナップショットがスナップされる前に、承認されていることを確認するプロセスはありますか？ イメージスナップショットへのアクセスコントロールは実装されていますか？	はい。イメージは、顧客と経営層の承認を得てバックアップされます。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
アプリケーションセキュリティレビュー	アプリケーションセキュリティ 4.2.1 - アプリケーションセキュリティレビュー - セキュアコードのレビュー	セキュアコードのレビューは各リリースの前に行われますか？	セキュアコードのレビューは各リリースの前に行われるかどうかを記載します。	はい
	アプリケーションセキュリティ 4.2.2 - アプリケーションセキュリティレビュー - ペネトレーションテスト	ペネトレーションテストは実施されていますか？ペネトレーションテストのレポートを提示していただけますか？	アプリケーションでペネトレーションテストを実施するかどうかを記載します。「はい」の場合、直近の3件のレポートを手動による証拠として提示していただけますか？	はい
	アプリケーションセキュリティ 4.2.3 - アプリケーションセキュリティレビュー - セキュリティパッチ	入手可能なリスクの高いセキュリティパッチはすべて適用され、定期的に検証されていますか？	リスクの高いセキュリティパッチを定期的に適用するかどうかを記載します。「はい」の場合、どのくらいの頻度で適用されていますか？	はい。セキュリティパッチは毎月適用されます。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	アプリケーション セキュリティ 4.2.4 - アプリ ケーションセ キュリティレ ビュー - アプリ ケーションの脆 弱性スキャン	インターネット に接続している すべてのアプリ ケーションに 対して、定期的 または大幅な変 更が行われた後 で、脆弱性ス キャンを実施し ていますか？	インターネット に接続している すべてのアプリ ケーションに 対して脆弱性ス キャンを実行す るかどうかを記 載します。「は い」の場合、脆 弱性スキャンは どのくらいの頻 度で行われてい ますか？レポー トのコピーを提 出していただけ ますか？	はい。脆弱性ス キャンを毎月実 行しています。
	アプリケーション セキュリティ 4.2.5 - アプリ ケーションセ キュリティレ ビュー - 脅威と 脆弱性の管理	脅威および脆弱 性の評価ツール と、それらが収 集するデータを 管理するプロセ スはありますか？	脅威および脆弱 性の評価ツール と、その検出結 果を管理するプ ロセスがあるか どうかを記載し ます。脅威と脆 弱性の管理方法 について、詳細 を記載してくだ さい。	はい。さまざま なソースからの すべての脅威と 脆弱性が 1 つの ポータルに集約 されます。それ らは重大度別に 管理されていま す。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	アプリケーションセキュリティ 4.2.6 - アプリケーションセキュリティレビュー - マルウェア対策スキャン	アプリケーションをホストするネットワークやシステムに対して、定期的にマルウェア対策スキャンを実施していますか？	アプリケーションをホストするネットワークやシステムに対して、マルウェア対策スキャンを実施するかどうかを記載します。「はい」の場合、どのくらいの頻度で行われていますか？レポートを提出していただけますか？	はい。マルウェア対策スキャンを毎月実行しています。
アプリケーションログ	アプリケーションセキュリティ 4.3.1 - アプリケーションログ - アプリケーションログ	アプリケーションログを収集し、それを確認していますか？	アプリケーションログを収集し、それを確認しているかどうかを記載します。「はい」の場合、ログはどのくらいの期間保持されますか？	はい。ログは 1 年間保持されます。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
	アプリケーションセキュリティ 4.3.2 - アプリケーションログ - ログへのアクセス	オペレーティングシステムとアプリケーションのログは、変更、削除、不適切なアクセスから保護されていますか？	オペレーティングシステムとアプリケーションのログが、変更、削除、不適切なアクセスから保護されているかどうかを記載します。侵害やインシデントが発生した場合、アプリケーションログの消失を検知するプロセスを導入していますか？	はい
	アプリケーションセキュリティ 4.3.3 - アプリケーションログ - ログに保存されたデータ (手動による認証が必要)	顧客の個人を特定できる情報 (PII) をログに保存していますか？	顧客の個人を特定できる情報 (PII) をログに保存しているかどうかを記載します。	いいえ。PII データはログに保存されません。
変更管理ポリシー	アプリケーションセキュリティ 4.4.1 - 変更管理ポリシー - 機能テストと耐障害性テスト	変更をリリースする前に、機能テストと耐障害性テストを実施していますか？	新規リリースの前に、アプリケーションの機能テストと耐障害性テストを実施するかどうかを記載します。	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	アプリケーションセキュリティ 4.4.2 - 変更管理 ポリシー - 変更 管理手順	変更管理手順 は、本番環境に 対するすべての 変更に必要なで すか？	本番環境で行わ れたすべての変 更に変更管理手 順が適用されて いるかどうかを 記載します。	はい
	アプリケーションセキュリティ 4.4.3 - 変更管理 ポリシー - 本番 環境における人 為的ミス/リスク の回避	ヒューマンエ ラーやリスクが 本番環境に影響 を与えないこと を検証するプロ セスは整ってい ますか？	ヒューマンエ ラーやリスクが 本番環境に影響 を与えないこと を検証するプロ セスがあること を記載します。	はい
	アプリケーションセキュリティ 4.4.4 - 変更管 理ポリシー - ド キュメントとロ グの変更	サービスに影響 を与える可能性 のある変更を文 書化してログを 記録しています か？	サービスに影響 を与える変更を 文書化して記録 するかどうか を記載します。 「はい」の場 合、ログはどの くらいの期間保 持されますか？	はい

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
	アプリケーションセキュリティ 4.4.5 - 変更管理ポリシー - 購入者への変更通知 (手動による認証が必要)	サービスに影響を与える可能性のある変更が加えられる前に、顧客に確実に通知するための正式なプロセスはありますか？	サービスに影響を与える可能性のある変更を行う前に、顧客に通知するかどうかを記載します。「はい」の場合、影響のある変更について、顧客に通知するための SLA はどのようなものですか？	はい。影響がある変更の 90 日前にお客様に通知します。

監査とコンプライアンスのコントロール

監査とコンプライアンスのコントロールでは、組織の規制要件の遵守状況を評価します。この表は、監査コントロールとコンプライアンスコントロールの値と説明を一覧にしたものです。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
認証完了	監査とコンプライアンス 1.1.1 - 認証完了 (手動による認証が必要)	保有している認証を一覧表示します。	持っている認証の名称を記載します。	SOC2、ISO/IEC 27001
認証中	監査とコンプライアンス 1.2.1 - 認証中 (手動による認証が必要)	現在進行中の認証を追加で記載します。	現在監査または審査中の追加の認証と、完了予定日を記載します。	はい。PCI の認証が進行中です (2022 年第 2 四半期に完了予定)。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
コンプライアンス確保の手順	監査とコンプライアンス 1.3.1 - コンプライアンス確保の手順 - コンプライアンス確保の手順	適用される法律、規制、契約上の要求事項を確実に遵守するための方針または手順がありますか？	適用される法律、規制、契約上の要求事項を確実に遵守するための方針または手順があるかどうかを指定します。「はい」の場合は、手順の詳細を記載し、手動による証拠をアップロードします。	はい。SOC2、ISO/IEC 27001などのドキュメントをアップロードしました。
	監査とコンプライアンス 1.3.2 - コンプライアンス確保の手順 - 未完了の要件を追跡する監査	未完了の規制要件やコンプライアンス要件を追跡する監査は完了していますか？	未完了の要件を追跡する監査を実施するかどうかを記載します。「はい」の場合は、詳細を記載します。	はい、未完了の要件を追跡する監査を毎月実施しています。
	監査とコンプライアンス 1.3.3 - コンプライアンス確保の手順 - 逸脱と例外 (手動による認証が必要)	コンプライアンス要件からの逸脱や例外を処理するプロセスがありますか？	例外やコンプライアンス要件からの逸脱を処理するプロセスがあるかどうかを記載します。「はい」の場合は、詳細を記載します。	はい。逸脱のログとレポートツールを用意しています。例外や逸脱をすべて調査して、今後発生しないように予防します。

ビジネスの回復力のコントロール

ビジネスの回復力のコントロールでは、事業の継続性を維持しながら、迅速に混乱に適応する組織の能力を評価します。この表は、ビジネスの回復力のポリシーコントロールの値と説明をまとめたものです。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
ビジネスの回復力	ビジネスの回復力と継続性 6.1.1 - ビジネスの回復力 - フェイルオーバーテスト (手動による認証が必要)	サイトのフェイルオーバーテストは、少なくとも年に 1 回実施されていますか？	フェイルオーバーテストを毎年実施するかどうかを記載します。実施していない場合は、どのくらいの頻度で実施しますか？	はい
	ビジネスの回復力と継続性 6.1.2 - ビジネスの回復力 - ビジネスインパクト分析 (手動による認証が必要)	ビジネスインパクト分析は実施されていますか？	ビジネスインパクト分析を実施したかどうかを記載します。「はい」の場合、最後に実施したのはいつですか？ 実施した分析の詳細を記載します。	はい。ビジネスインパクト分析は 6 か月前に実施しました。
	ビジネスの回復力と継続性 6.1.3 - ビジネスの回復力 - サードパーティーベンダーへの依存 (手動による認証が必要)	重要なサードパーティーサービスプロバイダー (クラウドサービスプロバイダー以外) への依存関係はありますか？	(クラウドサービスプロバイダー以外の) サードパーティーベンダーへの依存関係があるかどうかを記載します。「はい」の場合、ベンダー	いいえ

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
			の詳細を記載し てください。	
	ビジネスの回復 力と継続性 6.1.4 - ビジネスの回復 力 - サードパー ティーの継続性 と回復力テスト (手動による認証 が必要)	サードパー ティーベンダー に独自のデザ スタリカバリプ ロセスと演習を 要求しています か？	サードパー ティーベンダー が独自のデザ スタリカバリの プロセスと演習 を行う必要があ るかどうかを記 載します。	このサンプルは 該当しません。
	ビジネスの回復 力と継続性 6.1.5 - ビジネスの回復 力 - サードパー ティーベンダー の契約違反 (手動 による認証が必 要)	重要なサー ビスプロバイ ダーとの契約 には、Amazon が販売、出荷 (SSA) する可用 性と継続性の違 反に対する罰則 や是正条項が含 まれていますか？	サードパー ティーベンダー との契約には、 可用性と継続性 の違反に対する 罰則や是正条項 は含まれていま すか？	このサンプルは 該当しません。
	ビジネスの回復 力と継続性 6.1.6 - ビジネスの回復 力 - システムの 健全性	システムの健全 性を把握するた めのモニタやア ラートはありま すか？	システムの健全 性を把握するた めのモニタやア ラートがあるか どうかを記載し ます。	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
ビジネス継続性	ビジネスの回復 力と継続性 6.2.1 - ビジネス継続性 - ビジネス継続性 ポリシー/手順	正式なビジネス 継続性手順が策 定され、文書化 されていますか？	ビジネス継続性 の正式な手順が 策定され、維持 されているかど うかを記載しま す。「はい」の 場合は、手順の 詳細を記載しま す。	はい
	ビジネスの回復 力と継続性 6.2.2 - ビジネス継続性 - 対応と復旧の戦 略	優先順位の高い 活動に対して、 具体的な対応と 復旧の戦略が定 められています か？	復旧と対応の戦 略が顧客の活動 とサービスを対 象として策定 されているかど うかを記載しま す。	はい
	ビジネスの回復 力と継続性 6.2.3 - ビジネス継続性 - ビジネス継続性 テスト	ビジネス継続性 を確実にするた め、復旧テスト を実施していま すか？	障害発生時のビ ジネス継続性を 確保するために 復旧テストを実 施するかどうか を記載します。	はい。障害が発 生した場合、ビ ジネス継続性続 のためのシステ ムが 2 時間以内 に有効になりま す。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	事業回復力と継続性 6.2.4 - ビジネス継続性 - マルチテナンシー環境における可用性への影響 (手動による認証が必要)	購入者によって、システムの他のユーザーの可用性に影響を与える可能性のある負荷を与えることを制限していますか？	ある購入者の負荷が他の購入者の可用性に影響を与える可能性があるかどうかを記載します。「はい」の場合、影響がなくなるまでのしきい値はどれくらいですか？「いいえ」の場合、使用のピークを越えた時間帯にサービスが影響を受けないようにする方法について、詳細を記載してください。	はい。このサンプルにはしきい値はありません。
アプリケーションの可用性	ビジネスの回復力と継続性 6.3.1 - アプリケーションの可用性 - 可用性の記録 (手動による認証が必要)	昨年、信頼性や可用性に関して重大な問題がありましたか？	過去 1 年間で信頼性や可用性に関する重大な問題があったかどうかを記載します。	いいえ

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	ビジネスの回復 力と継続性 6.3.2 - アプリケーショ ンの可用性 - 提 起メンテナンス 期間 (手動による 認証が必要)	定期メンテナ ス中はダウン タイムが予想さ れますか？	定期メンテナ ス期間中にサー ビスが停止する 可能性がある かどうかを指定 してください。 「はい」の場 合、ダウンタイ ムはどのくらい ですか？	いいえ
	ビジネスの回復 力と継続性 6.3.3 - アプリケーショ ンの可用性 - オ ンラインインシ デントポータル (手動による認証 が必要)	計画的な停止と 予期しない停止 の概要を示すオ ンラインのイン シデント対応ス テータスポータ ルはありますか？	計画的な停止と 予期しない停止 の概要を示すイ ンシデントス テータスポータ ルがあるかど うかを記載しま す。「はい」の 場合は、顧客が アクセスする方 法の詳細を記載 します。サービ ス停止後、どの くらいでポータ ルが更新されま すか？	はい。お客様は example.com か ら詳細情報に アクセスできま す。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
	ビジネスの回復力と継続性 6.3.4 - アプリケーションの可用性 - 目標復旧時間 (手動による認証が必要)	具体的な目標復旧時間 (RTO) がありますか?	目標復旧時間 (RTO) があるかどうかを記載します。「はい」の場合、RTO を記載してください。	はい、RTO は 2 時間です。
	ビジネスの回復力と継続性 6.3.5 - アプリケーションの可用性 - 目標復旧時点 (手動による認証が必要)	具体的な目標復旧時点 (RPO) がありますか?	目標復旧時点 (RPO) があるかどうかを記載します。「はい」の場合、RPO を記載してください。	はい、RPO は 1 週間です。

データセキュリティコントロール

データセキュリティコントロールでは、データと資産を保護します。この表は、データセキュリティコントロールの値と説明をまとめたものです。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
顧客データインジェスト	データセキュリティ 2.1.1 - 顧客データインジェスト (手動による認証が必要)	製品機能のために顧客に必要なデータのリストを作成します。	顧客で消費されるすべてのデータを記載します。機密データや秘密データが消費されるかどうかを記載します。	機密データや秘密データは消費されません。この製品は、アプリケーション、インフラストラクチャ、AWS のサービスからのログなど、機密ではない情報

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
				のみを消費し ます。(AWS CloudTrai l、 AWS Config、 VPC フ ローログ)
データストレ ージの場所	データセキュリ ティ 2.2.1 - デ ータストレージの 場所 (手動による 認証が必要)	お客様のデータ はどこに保存さ れますか? デ ータが保存され ている国やリー ジョンを一覧に します。	データが保存さ れている国と地 域のリストを記 載します。	オハイオ (米 国)、オレゴン (米国)、アイルラ ンド (EU)
アクセスコント ロール	データセキュリ ティ 2.3.1 - アク セスコントロー ル - 従業員のア クセス (手動によ る認証が必要)	従業員は暗号化 されていない顧 客データにアク セスできますか?	従業員が暗号化 されていない顧 客データにアク セスできるか どうかを記載し ます。「はい」 の場合は、アク セスが必要な理 由を簡単に記載 してください。 「いいえ」の場 合は、アクセス コントロールの 方法を簡単に 記載してくださ い。	いいえ。すべて のデータは保存 時に暗号化され ます。従業員 は顧客データに はアクセスでき ず、使用状況に 関するデータに のみアクセスで きます。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	データセキュリティ 2.3.2 - アクセスコントロール - モバイルアプリケーション (手動による認証が必要)	顧客はモバイルアプリケーションからデータにアクセスできますか？	顧客がモバイルアプリケーションからデータにアクセスできるかどうかを記載します。「はい」の場合は、詳細を記載します。顧客はどのようにサインインしますか？認証情報はアプリケーションによってキャッシュされますか？トークンはどのくらいの頻度で更新されますか？	いいえ。モバイルアプリケーションを使用してサービスにアクセスすることはできません。
	データセキュリティ 2.3.3 - アクセスコントロール - データの送信先の国 (手動による認証が必要)	顧客データは送信元以外の国にも送信されますか？	顧客データは送信元以外の国にも送信されますか？「はい」の場合は、顧客データが送受信される国のリストを記載します。	いいえ

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	データセキュリティ 2.3.4 - アクセスコントロール - データはサードパーティーベンダーと共有されるか (手動による認証が必要)	顧客データはサードパーティーベンダー (クラウドサービスプロバイダー以外) と共有されていますか？	顧客データはサードパーティーベンダーと共有されていますか？ 「はい」の場合は、顧客データを提供するサードパーティーベンダーとその国または地域のリストを記載します。	いいえ
	データセキュリティ 2.3.5 - アクセスコントロール - サードパーティーベンダーに関連するセキュリティポリシー	サードパーティーベンダーが顧客データの機密性、可用性、完全性を維持することを保証するためのポリシーや手順がありますか？	サードパーティーベンダーが顧客データの機密性、可用性、完全性を維持することを保証するためのポリシーや手順があるかどうかを記載します。「はい」の場合は、ポリシーまたは手順のマニュアルまたは文書をアップロードしてください。	このサンプルは該当しません。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
データの暗号化	データセキュリティ 2.4.1 - データ暗号化 - 保管時のデータ暗号化	すべてのデータは保管時に暗号化されますか？	すべてのデータが保管時に暗号化されるかどうかを記載します。	はい
	データセキュリティ 2.4.2 - データ暗号化 - 転送中のデータ暗号化	すべてのデータは転送時に暗号化されますか？	すべてのデータが転送時に暗号化されるかどうかを記載します。	はい
	データセキュリティ 2.4.3 - データ暗号化 - 強力なアルゴリズム (手動による認証が必要)	強力な暗号化アルゴリズムを使用していますか？	強力な暗号化アルゴリズムを使用していますか？「はい」の場合は、使用する暗号化アルゴリズム (RSA、AES 256 など) を記載してください。	はい。データの暗号化に AES 256 を使用しています。
	データセキュリティ 2.4.4 - データ暗号化 - 固有の暗号化キー (手動による認証が必要)	顧客には固有の暗号キーを生成する機能がありますか？	顧客は独自の暗号キーを提供または生成できますか？「はい」の場合は、詳細を記載し、証拠をアップロードしてください。	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	データセキュリティ 2.4.5 - データ暗号化 - 暗号化キーへのアクセス (手動による認証が必要)	従業員は顧客の暗号キーにアクセスできないようになっていますか？	従業員が顧客の暗号キーにアクセスできないようになっているかどうかを記載します。「いいえ」の場合は、従業員が顧客のキーにアクセスする理由を記載してください。「はい」の場合は、アクセスコントロールの方法を記載してください。	はい。暗号キーは安全に保管され、定期的にローテーションされます。従業員はこれらのキーにアクセスできません。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
データストレージと分類	データセキュリティ 2.5.1 - データストレージと分類 - データのバックアップ	顧客データをバックアップしていますか？	顧客データをバックアップするかどうかを記載します。「はい」の場合は、バックアップポリシー (バックアップの実行頻度、保存場所、暗号化、冗長性に関する詳細を含む) を記載します。	はい、バックアップは3か月ごとに行われます。バックアップは暗号化され、顧客データと同じリージョンに保存されます。顧客のサポートエンジニアにはバックアップを復元するためのアクセス許可がありますが、バックアップ内のデータにはアクセスできません。
	データセキュリティ 2.5.2 - データストレージと分類 - データアクセスコントロールポリシー	保存されている顧客データに対して適切なアクセスコントロールを実施していますか？ アクセスコントロールポリシーを記載します。	保存されている顧客データに適切なアクセスコントロール (RBAC など) を実装するかどうかを記載します。データアクセスのコントロール方法について、より詳細な情報と手動による証拠を提供してください。	はい。顧客データへのアクセスを制限するために、最小特権のアクセスコントロールが実装されています。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	データセキュリティ 2.5.3 - データストレージと分類 - トランザクションデータ (手動による認証が必要)	顧客のトランザクション詳細 (支払いカード情報やトランザクションを行うグループに関する情報など) は境界ゾーンに保存されていますか?	顧客のトランザクション詳細 (支払いカード情報やトランザクションを行うグループに関する情報など) が境界ゾーンに保存されているかどうかを記載します。「はい」の場合は、それを境界ゾーンに保存する必要がある理由を記載してください。	いいえ
	データセキュリティ 2.5.4 - データストレージと分類 - 情報の分類	顧客データは、法的または規制の要件、ビジネス価値、不正な開示や変更に対する機密性に従って分類されていますか?	顧客データを機密性によって分類するかどうかを記載します。「はい」の場合は、この分類に関する手動による証拠をアップロードしてください。	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	データセキュリティ 2.5.5 - データストレージと分類 - データのセグメンテーション (手動による認証が必要)	顧客間のデータセグメンテーションと分離機能は提供されていますか？	異なる顧客のデータをセグメンテーションするかどうかを記載します。「いいえ」の場合は、データを交差汚染から保護するためのメカニズムを記載してください。	はい
データ保持期間	データセキュリティ 2.6.1 - データ保持 (手動による認証が必要)	データの保持期間はどのくらいですか？	データ保持期間を記載します。保持期間がデータの分類と機密性によって異なる場合、それぞれの保持期間の詳細を記載してください。	6 か月間
購入者がサブスクリプションを解除した後のデータ保持	データセキュリティ 2.6.2 - クライアントがサブスクリプションを解除した後のデータ保持 (手動による認証が必要)	購入者がサブスクリプションを解除した後は、どのくらいの期間データを保持しますか？	顧客がサブスクリプションを解除した後のデータ保持期間を記載します。	3 か月間

エンドユーザーデバイスのセキュリティコントロール

エンドユーザーデバイスのセキュリティコントロールでは、ポータブルエンドユーザーデバイスと、それらが接続されるネットワークを脅威や脆弱性から保護します。この表は、エンドユーザーデバイスのセキュリティポリシーコントロールの値と説明をまとめたものです。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
資産/ソフトウェアインベントリ	エンドユーザーデバイスセキュリティ 7.1.1 - 資産/ソフトウェアインベントリ - 資産インベントリ	資産インベントリリストは定期的に更新されていますか？	資産インベントリを管理しているかどうかを記載します。「はい」の場合、どのくらいの頻度で更新していますか？	はい。インベントリは毎週更新しています。
	エンドユーザーデバイスセキュリティ 7.1.2 - 資産/ソフトウェアインベントリ - ソフトウェアおよびアプリケーションインベントリ	対象範囲のシステムにインストールされているすべてのソフトウェアプラットフォームとアプリケーションがインベントリ化されていますか？	インストールされているすべてのソフトウェアとアプリケーションのインベントリが維持されているかどうかを記載します。「はい」の場合、どのくらいの頻度で更新していますか？	はい。インベントリは毎週更新しています。
資産のセキュリティ	エンドユーザーデバイスセキュリティ 7.2.1 - 資産のセキュリティ - セキュリティバッチ	すべてのエンドユーザーデバイスに、利用可能なリスクの高いすべてのセキュリティバッチが適用され、少な	リスクの高いすべてのセキュリティバッチを少なくとも毎月適用するかどうかを記載します。「いいえ」の	はい。セキュリティチームによって、このプロセスを隔週で実行しています。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
		くとも毎月検証 されていますか？	場合、どのくら いの頻度で適用 していますか？ パッチの管理方 法について、詳 細を記載してく ださい。	
	エンドユーザー デバイスセキュ リティ 7.2.2 - 資産のセキュ リティ - エンド ポイントのセキュ リティ	エンドポイント のセキュリティ はありますか？	エンドポイント のセキュリティ がすべてのデバ イスにインス トールされてい るかどうかを記 載します。「は い」の場合、 ツールとその保 守方法について 詳細を記載して ください。	はい。当社のセ キュリティチー ムでは、社内 ツールを使用し て、これを隔週 で処理していま す。
	エンドユーザー デバイスセキュ リティ 7.2.3 - 資 産セキュリティ - 資産のメンテナ ンスと修復 (手動 による認証が必 要)	組織の資産のメ ンテナンスと修 復は、承認およ び管理されてい るツールを使用 して実施し、記 録されています か？	資産のメンテナ ンスと修復を管 理対象ツールで 実施し、記録さ れちるかどうか を記載します。 「はい」の場 合、その管理方 法について詳細 を記載してくだ さい。	はい。デバイ スのメンテナ ンスは、すべて記録 されています。 このメンテナ ンスによってダウ ンタイムが発生 することはない ません。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	エンドユーザー デバイスセキュ リティ 7.2.4 - 資 産セキュリティ - デバイスのアク セスコントロー ル	デバイスのアク セスコントロー ルは有効になっ ていますか？	デバイスのアク セスコントロー ル (RBAC など) が有効になって いるかどうかを 記載します。	はい。最小特権 アクセスがすべ てのデバイスに 実装されていま す。
デバイスログ	エンドユーザー デバイスセキュ リティ 7.3.1 - デ バイスログ - 十 分な詳細をログ に記載 (手動によ る認証が必要)	インシデントの 調査をサポート するため、オペ レーティングシ ステムやデバイ スのログには十 分な詳細が記録 されていますか？	インシデントの 調査をサポート するために、ロ グに十分な詳細 (ログイン試行の 成功と失敗、機 密設定やファイ ルへの変更など) が含まれている かどうかを記載 します。「いい え」の場合は、 インシデントの 調査方法の詳細 を記載してくだ さい。	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	エンドユーザー デバイスセキュ リティ 7.3.2 - デ バイスログ - デ バイスログへの アクセス	デバイスログ は、変更、削 除、不適切なア クセスから保護 されていますか？	デバイスログ は、変更、削 除、不適切な アクセスから保 護されているか どうかを記載し ます。「はい」 の場合、その実 施方法の詳細を 記載してくださ い。	はい。ログの変 更はアクセスコ ントロールによっ て実施されま す。ログに加え られた変更は、 すべてアラート につながりま す。
	エンドユーザー デバイスセキュ リティ 7.3.3 - デ バイスログ - ロ グの保持 (手動に よる認証が必要)	ログは、攻撃を 調査するのに十 分な期間保持さ れていますか？	ログはどのくら いの期間保持さ れますか？	はい、1 年間で す。
モバイルデバイ ス管理	エンドユーザー デバイスセキュ リティ 7.4.1 - モ バイルデバイス 管理 - モバイル デバイス管理プ ログラム	モバイルデバイ ス管理プログラ ムはありますか？	モバイルデバイ ス管理プログラ ムがあるかどう かを記載しま す。「はい」の 場合は、モバイル デバイス管理に 使用している ツールを記載し てください。	はい。社内ツ ールを使用してい ます。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	エンドユーザー デバイスセキュ リティ 7.4.2 - モバイルデバイ ス管理 - プライ ベートモバイル デバイスから本 番環境へのアク セス (手動による 認証が必要)	管理されていな いプライベート モバイルデバイ スを使用して、 スタッフが本番 環境にアクセス することは禁止 されていますか？	管理されていな いプライベート モバイルデバイ スを使用して、 スタッフが本番 環境にアクセス することが禁止 されているかど うかを記載しま す。「いいえ」 の場合、このコ ントロールを実 施する方法を 記載してくださ い。	はい
	エンドユーザー デバイスセキュ リティ 7.4.3 - モ バイルデバイス 管理 - モバイル デバイスから顧 客データへのア クセス (手動によ る認証が必要)	従業員は、管理 されていないプ ライベートモバ イルデバイス を使用して、顧客 データを閲覧ま たは処理するこ とを禁止されて いますか？	従業員は、管理 されていないプ ライベートモバ イルデバイス を使用して、顧 客データにアク セスすることが 禁止されている かどうかを記載 します。「いい え」の場合、ア クセスを許可す るユースケース は何ですか？ど のようにアクセ スをモニタリン グしていますか？	はい

人事コントロール

人事コントロールでは、従業員の雇用、給与支払い、退職などのプロセスにおける機密データの取り扱いについて、従業員関連部門を評価します。この表は、人事ポリシーコントロールの値と説明をまとめたものです。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
人事ポリシー	人事 9.1.1 - 人事ポリシー - 従業員の身元調査	雇用前に身元調査は行われますか？	雇用前に全従業員の身元調査を実施するかどうかを記載します。	はい
	人事 9.1.2 - 人事ポリシー - 雇用契約	雇用契約は雇用前に締結されていますか？	雇用前に雇用契約が締結されているかどうかを記載します。	はい
	人事 9.1.3 - 人事ポリシー - 従業員向けセキュリティ研修	全従業員は、定期的にセキュリティ意識向上トレーニングを受けていますか？	従業員が定期的にセキュリティトレーニングを受けているかどうかを記載します。「はい」の場合、どのくらいの頻度でセキュリティトレーニングを受けていますか？	はい。毎年セキュリティトレーニングを受けています。
	人事 9.1.4 - 人事ポリシー - ポリシー違反の懲戒処分	人事ポリシーに違反した場合の懲戒処分はありますか？	人事ポリシーの違反に対する懲戒処分の有無を記載します。	はい

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
	人事 9.1.5 - 人事ポリシー - 請負業者/下請業者の身元調査 (手動による認証が必要)	サードパーティーベンダー、請負業者、下請業者の身元調査は行われていますか？	サードパーティーベンダー、請負業者、下請業者に対して身元調査を実施しているかどうかを記載します。「はい」の場合、身元調査は定期的に行われていますか？	はい。身元調査は毎年行われます。
	人事 9.1.6 - 人事ポリシー - 退職時の資産返還	退職時に貸与した資産の返還を確認するプロセスはありますか？	従業員の退職時に貸与した資産の返還を検証するプロセスがあるかどうかを記載します。	はい

インフラストラクチャのセキュリティ

インフラストラクチャのセキュリティコントロールでは、重要な資産を脅威や脆弱性から保護します。この表は、インフラストラクチャのセキュリティポリシーコントロールの値と説明をまとめたものです。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
物理的なセキュリティ	インフラストラクチャのセキュリティ 8.1.1 - 物理的なセキュリティ	資産 (建物、車両、ハードウェアなど) に直接アクセスする必要がある個人は、	資産 (建物、車両、ハードウェアなど) に直接アクセスする必要がある個人に対	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	<p>テイ - 施設への物理的アクセス</p>	<p>ID と必要な認証情報を提供する必要がありますか？</p>	<p>し、ID と必要な認証情報を提供する必要があるかどうかを記載します。</p>	
	<p>インフラストラクチャのセキュリティ 8.1.2 - 物理的なセキュリティ - 物理的なセキュリティと環境管理の実施</p>	<p>データセンターやオフィスビルでは、物理的なセキュリティと環境管理が実施されていますか？</p>	<p>すべての施設で物理的なセキュリティと環境管理が実施されているかどうかを記載します。</p>	<p>はい</p>
	<p>インフラストラクチャのセキュリティ 8.1.3 - 物理的なセキュリティ - 訪問者のアクセス (手動による認証が必要)</p>	<p>訪問者のアクセスを記録していますか？</p>	<p>訪問者が施設に入ることを許可されている場合、訪問者のアクセスログは保存されていますか？「はい」の場合、ログはどのくらいの期間保持されますか？</p>	<p>はい。ログは 1 年間保持されます。</p>
<p>ネットワークセキュリティ</p>	<p>インフラストラクチャのセキュリティ 8.2.1 - ネットワークセキュリティ - 未使用のポートとサービスの無効化 (手動による認証が必要)</p>	<p>未使用のポートとサービスは、すべて本番環境とシステムで無効になっていますか？</p>	<p>未使用のポートとサービスが、すべて本番環境とシステムで無効になっているかどうかを記載します。</p>	<p>はい</p>

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	インフラストラ クチャのセキュ リティ 8.2.2 - ネットワーク セキュリティ - ファイアウォー ルの使用	ファイアウォー ルを使用して、 重要で機密性の 高いシステム を、機密性の低 いシステムにあ るネットワーク セグメントとは 別のネットワー クセグメントに 分離しています か？	ファイアウォー ルを使用して、 重要で機密性の 高いシステム を、機密性の低 いシステムにあ るネットワーク セグメントとは 別のネットワー クセグメントに 分離しているか どうかを記載し ます。	はい
	インフラストラ クチャのセキュ リティ 8.2.3 - ネットワーク セキュリティ - ファイアウォー ルルールのレ ビュー	ファイアウォー ルのルールはす べて定期的にし レビューし、更新 されていますか？	ファイアウォー ルのルールはど のくらいの頻度 で定期的にし レビューし、更新 されていますか？	はい。ファイア ウォールのルー ルは 3 か月ごと に更新されてい ます。
	インフラストラ クチャのセキュ リティ 8.2.4 - ネットワークセ キュリティ - 侵 入検知/防止シス テム	機密性の高いす べてのネット ワークゾーンと ファイアウォー ルが有効な場所 に、侵入検知/防 止システムが設 置されています か？	機密性の高いす べてのネット ワークゾーンで 侵入検知および 防止システムが 有効になっている かどうかを記 載します。	はい

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
	インフラストラクチャのセキュリティ 8.2.5 - ネットワークセキュリティ - セキュリティ基準と強化基準	ネットワークデバイスのセキュリティ基準と強化基準は定められていますか？	ネットワークデバイスのセキュリティ基準と強化基準を定めているかどうかを記載します。「はい」の場合、詳細(これらの基準が実装および更新される頻度に関する詳細を含む)を記載してください。	はい。セキュリティ基準と強化基準は、毎月ネットワークデバイスに実装されています。
クラウドサービス	インフラストラクチャのセキュリティ 8.3.1 - クラウドサービス - アプリケーションのホストに使用されるプラットフォーム(手動による認証が必要)	アプリケーションのホストに使用するクラウドプラットフォームを一覧にしてください。	アプリケーションのホストに使用するクラウドプラットフォームを記載してください。	AWS

リスク管理とインシデント対応のコントロール

リスク管理とインシデント対応のコントロールでは、許容可能と判断したリスクのレベルと、リスクや攻撃に対応するために講じられた措置を評価します。この表は、リスク管理とインシデント対応のコントロールの値と説明をまとめたものです。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
リスク評価	リスク管理/インシデント対応 5.1.1 - リスク評価 - リスクの対応と特定	組織に対する破壊的インシデントのリスクを特定し、対処することに焦点を当てた正式なプロセスはありますか？	組織に破壊的なインシデントを引き起こすリスクを特定し、対処するプロセスがあるかどうかを記載します。	はい
	リスク管理/インシデント対応 5.1.2 - リスク評価 - リスク管理プロセス	評価中に特定されたリスクの処理を管理するプログラムまたはプロセスはありますか？	リスクとその軽減策を管理するためのプログラムまたはプロセスがあるかどうかを記載します。「はい」の場合、リスク管理プロセスについて詳細を記載してください。	<p>はい。不適合に対処するため、問題を定期的に見直し、修正しています。環境に影響を与えるすべての問題について、次の情報が特定されます。</p> <ul style="list-style-type: none"> • 特定された問題の詳細 • 根本原因 • 補償コントロール • 重要度 • 所有者 • 短期的な方向性 • 長期的な方向性

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	リスク管理/イ ンシデント対応 5.1.3 - リスク評 価 - リスク評価	リスク評価は頻 繁に行われてい ますか？	リスク評価は頻 繁に行われて いますか？「は い」の場合は、 リスク評価の頻 度を記載してく ださい。	はい。リスク評 価は 6 か月ご とに実施してい ます。
	リスク管理/イ ンシデント対応 5.1.4 - リスク評 価 - サードパー ティーベンダー のリスク評価	リスク評価は、 すべてのサード パーティーベン ダーを対象に実 施されています か？	リスク評価は、 すべてのサード パーティーベン ダーに対して実 施されているか どうかを記載し ます。「はい」 の場合は、どの くらいの頻度で 実施されていま すか？	このサンプルは 該当しません。
	リスク管理/イ ンシデント対応 5.1.5 - リスク評 価 - 契約変更時 のリスク再評価	サービス提供や 契約変更が行わ れたときに、リ スク評価が実施 されていますか？	サービス提供や 契約変更が行わ れるたびに、リ スク評価を実施 するかどうかを 記載します。	このサンプルは 該当しません。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	リスク管理/インシデント対応 5.1.6 - リスク評価 - リスクの受け入れ (手動による認証が必要)	経営陣がリスクを承知の上で客観的に受け入れ、アクションプランを承認するプロセスがありますか？	経営陣がリスクを理解した上で受け入れ、リスクに関連する問題を解決するためのアクションプランとタイムラインを承認するプロセスがあるかどうかを記載します。そのプロセスには、各リスクの背後にあるメトリクスの詳細を経営陣に提供することが含まれていますか？	はい。リスクの重大度と、リスクが軽減されない場合に発生する可能性のある問題に関する詳細が、リスクを承認する前に経営陣に提供されます。
	リスク管理/インシデント対応 5.1.7 - リスク評価 - リスクメトリクス (手動による認証が必要)	リスクメトリクスを定義、監視、報告するための対策は整っていますか？	リスクメトリクスを定義、監視、報告するプロセスがあるかどうかを記載します。	はい
インシデント管理	リスク管理/インシデント対応 5.2.1 - インシデント管理 - インシデント対応計画	正式なインシデント対応計画はありますか？	正式なインシデント対応計画があるかどうかを記載します。	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	リスク管理/インシデント対応 5.2.2 - インシデント管理 - セキュリティインシデントの報告 窓口 (手動による 認証が必要)	顧客がセキュリティインシデントを報告するプロセスはありますか？	顧客がセキュリティインシデントを報告するプロセスがあるかどうかを記載します。「はい」の場合、顧客がセキュリティインシデントを報告する方法を記載してください。	はい。お客様は example.com でインシデントを報告できます。
	リスク管理/インシデント対応 5.2.3 - インシデント管理 - インシデントの報告/ 主要な活動	主要な活動を報告していますか？	主要な活動を報告していますか？ 主要な活動を報告するための SLA はどのようなものですか？	はい。主要な活動はすべて 1 週間以内に報告されます。
	リスク管理/インシデント対応 5.2.4 - インシデント管理 - インシデントのリカバリ	ディザスタリカバリ計画はありますか？	インシデント発生後のリカバリ計画があるかどうかを記載します。「はい」の場合、リカバリ計画の詳細を記載してください。	はい。インシデントの発生後、24 時間以内にリカバリが行われます。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	リスク管理/インシデント対応 5.2.5 - インシデント管理 - 攻撃発生時に購入者が利用できるログ (手動による認証が必要)	攻撃を受けた場合、顧客は関連するリソース (ログ、インシデントレポート、データなど) を利用できますか?	攻撃やインシデントが発生した場合、顧客はその使用に関連するリソース (ログ、インシデントレポート、データなど) を利用できますか?	はい
	リスク管理/インシデント対応 5.2.6 - インシデント管理 - セキュリティ情報 (手動による認証が必要)	アプリケーションに影響を及ぼす最新の攻撃や脆弱性をまとめたセキュリティ情報はありますか?	アプリケーションに影響を及ぼす最新の攻撃や脆弱性をまとめたセキュリティ情報があるかどうかを記載します。「はい」の場合、詳細を記載してください。	はい。お客様は example.com でインシデントを報告できます。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
インシデント検 知	リスク管理/イ ンシデント対応 5.3.1 - インシデ ント検知 - 包括 的なログ記録	インシデントの 特定と軽減に役 立つ包括的なロ グ記録はありま すか？	包括的なログ記 録が有効になっ ているかどうか を記載します。 システムがログ に記録できるイ ベントのタイプ を特定します。 ログはどのくら いの期間保持さ れますか？	はい。次のイ ベントがログ に記録されま す: アプリケー ション、デバ イス、および AWS のサービス AWS CloudTrai l、AWS Config、VPC フ ローログ。ログ は 1 年間保持さ れます。
	リスク管理/イ ンシデント対応 5.3.2 - インシデ ント検知 - ログ のモニタリング	ログのモニタリ ングなどの検知 メカニズムを使 用してて、異常 な活動や不審な 活動をモニタリ ングし、警告し ていますか？	セキュリティの モニタリングと 警告を定期的に 実施するかど うかを記載しま す。「はい」の 場合、異常な動 作や不審な動作 のログのモニタ リングも含まれ ていますか？	はい。すべての ログは、複数の ログイン失敗、 通常とは異なる 位置情報から のログイン、そ の他の不審なア ラートなどの異 常な動作がない かモニタリング されます。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
	リスク管理/インシデント対応 5.3.3 - インシデント検知 - サードパーティーのデータ侵害	下請業者のセキュリティ、プライバシー、データ侵害の問題を特定、検出、ログ記録するプロセスはありますか？	データ侵害、セキュリティ問題、プライバシー問題について、サードパーティーベンダーや下請業者を特定して検出するプロセスがあるかどうかを記載します。	はい
インシデント通知の SLA	リスク管理/インシデント対応 5.4.1 - インシデント通知の SLA (手動による認証が必要)	インシデントや違反に関する通知を送信するための SLA はどのようなものですか？	インシデントや違反に関する通知を送信するための SLA はどのようなものですか？	7 日間

セキュリティと設定に関するポリシーコントロール

セキュリティと設定に関するポリシーコントロールは、組織の資産を保護するセキュリティポリシーとセキュリティ設定を評価します。この表は、セキュリティと設定に関するポリシーコントロールの値と説明をまとめたものです。

コントロールセット	コントロールタイトル	コントロールの記述	証拠収集の詳細	サンプル値
情報セキュリティに関するポリシー	セキュリティと設定に関するポリシー 10.1.1 - 情報セキュリティに関するポリシー - 情報セ	セキュリティチームが所有し、維持する情報セキュリティポリシーはありますか？	情報セキュリティポリシーがあるかどうかを記載します。「はい」の場合は、手動による	はい。NIST フレームワークに基づいてセキュリティポリシーを構築します。

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	セキュリティポリ シー		証拠を共有また はアップロード してください。	
	セキュリティと 設定に関するポ リシー 10.1.2 - 情報セキュリ ティに関する ポリシー - ポリ シーのレビュー	すべてのセキュ リティポリシー は、毎年レ ビューされてい ますか？	セキュリティポ リシーを毎年レ ビューするかど うかを記載し ます。「いい え」の場合、ポ リシーはどのく らいの頻度でレ ビューされます か？	はい。毎年レ ビューされま す。
セキュリティ設 定に関するポリ シー	セキュリティと 設定に関するポ リシー 10.2.1 - セキュリティ設 定に関するポリ シー - セキュリ ティ設定 (手動に よる認証が必要)	セキュリティ設 定の標準は維持 され、文書化さ れていますか？	すべてのセキュ リティ設定の標 準が維持され、 文書化されてい るかどうかを記 載します。「は い」の場合は、 手動による証拠 を共有またはア ップロードして ください。	はい

コントロール セット	コントロールタ イトル	コントロールの 記述	証拠収集の詳細	サンプル値
	セキュリティと 設定に関するポ リシー 10.2.2 - セキュリティ 設定に関するポ リシー - セキュ リティ設定のレ ビュー (手動によ る認証が必要)	セキュリティ設 定は少なくと も年に 1 回レ ビューされてい ますか?	セキュリティ設 定を少なくとも 年 1 回レビュー するかどうかを 記載します。 「いいえ」の場 合は、レビュー の頻度を記載し てください。	はい。3 か月ご とにレビューさ れます。
	セキュリティと 設定に関するポ リシー 10.2.3 - セキュリティ設 定に関するポリ シー - 設定の変 更	設定の変更は記 録されますか?	設定の変更を記 録するかどうか を指定してくだ さい。「はい」 の場合、ログは どのくらいの期 間保持されます か?	はい。設定の変 更はすべてモニ タリングされ、 記録されます。 設定が変更され るとアラートが 生成されます。 ログは 6 か月間 保持されます。

AWS Marketplace Vendor Insights を使用して購入者としてスナッ プショットをエクスポートする

スナップショットは、セキュリティプロファイルの point-in-time 体制です。スナップショットをエクスポートすることにより、データをダウンロードしてオフラインでの確認、証拠データの確認、製品の比較を行うことができます。

スナップショットをエクスポートする

JSON 形式または CSV 形式にエクスポートできます。スナップショットをエクスポートするには、次の手順を実行します。

1. にサインイン AWS Management Console し、[AWS Marketplace コンソール](#) を開きます。

2. [ベンダーインサイト] を選択します。
3. [ベンダーインサイト] から製品を選択します。
4. [セキュリティとコンプライアンス] タブから [概要] セクションに移動し、[エクスポート] を選択します。
5. ドロップダウンリストから [ダウンロード (JSON)] または [ダウンロード (CSV)] を選択します。

AWS Marketplace Vendor Insights でのアクセスの制御

AWS Identity and Access Management (IAM) は AWS のサービス、AWS リソースへのアクセスを制御するのに役立ちます。IAM は、追加料金なしで AWS のサービスを使用できます。管理者は、誰を認証 (サインイン) し、誰に AWS Marketplace リソースの使用を承認する (アクセス許可を付与する) かを制御します。AWS Marketplace Vendor Insights は IAM を使用して、販売者のデータ、評価、販売者の自己認証、および業界標準の監査レポートへのアクセスを制御します。

で誰が何をできるかを制御するための推奨方法は AWS Marketplace 管理ポータル、IAM を使用してユーザーとグループを作成することです。次に、そのユーザーをグループに追加してグループを管理します。読み取り専用のアクセス許可を付与するポリシーまたはアクセス許可をグループに割り当てます。読み取り専用アクセスが必要なユーザーが他にもいる場合は、アクセス許可を AWS アカウントに許可するのではなく、作成したグループにそれらのユーザーを追加します。

ポリシーは、ユーザー、グループ、またはロールに適用されるアクセス許可を定義したドキュメントです。AWSでユーザーができることを決定するアクセス許可。ポリシーでは通常、特定のアクションへのアクセスを許可し、オプションで、それらのアクションを Amazon EC2 インスタンスや Amazon S3 バケットなどの特定のリソースで実行することを許可することができます。また、ポリシーにより、アクセスを明示的に拒否することもできます。アクセス許可は、特定のリソースへのアクセスを許可または拒否するポリシー内のステートメントです。

Important

作成したすべてのユーザーは、自分の認証情報を使用して認証します。ただし、同じ AWS アカウントを使用します。ユーザーが行った変更はアカウント全体に影響を及ぼす可能性があります。

AWS Marketplace には、それらのアクセス許可を持つユーザーがで実行できるアクションを制御するためのアクセス許可が定義されています AWS Marketplace 管理ポータル。また、複

数のアクセス許可を組み合わせるが AWS Marketplace 作成および管理するポリシーもあります。AWSMarketplaceSellerProductsFullAccess ポリシーでは、ユーザーに AWS Marketplace 管理ポータル製品へのフルアクセスを許可します。

使用可能なアクション、リソース、および条件キーの詳細については、「サービス認証リファレンス」の [AWS Marketplace 「Vendor Insights 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。

AWS Marketplace Vendor Insights 購入者のアクセス許可

AWS Marketplace Vendor Insights の IAM ポリシーでは、次のアクセス許可を使用できます。アクセス許可を 1 つの IAM ポリシーにまとめて、必要なアクセス許可を付与できます。

GetProfileAccessTerms

GetProfileAccessTerms では、ユーザーは Vendor Insights AWS Marketplace プロファイルを確認、承諾、およびアクセスするために必要な条件を取得できます。

アクショングループ: 読み取り専用、読み取り/書き込み。

必要なリソース: SecurityProfile。

ListEntitledSecurityProfiles

ListEntitledSecurityProfiles では、ユーザーは有効な読み取り権限を持つすべてのセキュリティプロファイルを一覧表示できます。

アクショングループ: 読み取り専用、リスト専用、読み取り/書き込み。

必要なリソース: なし

ListEntitledSecurityProfileSnapshots

ListEntitledSecurityProfileSnapshots では、ユーザーは有効な SecurityProfile の読み取り権限を持つセキュリティプロファイルのセキュリティプロファイルスナップショットを一覧表示できます。

アクショングループ: 読み取り専用、リスト専用、読み取り/書き込み。

必要なリソース: SecurityProfile

GetEntitledSecurityProfileSnapshot

GetEntitledSecurityProfileSnapshot では、ユーザーは有効な読み取り権限を持つセキュリティプロファイルのセキュリティプロファイルスナップショットを一覧表示できます。

アクショングループ: 読み取り専用、読み取り/書き込み。

必要なリソース: SecurityProfile

のセキュリティ AWS Marketplace

高品質の販売者のソフトウェアをリストアップし、選択の品質の維持に積極的に取り組みます。すべての顧客は異なるため、顧客が適切な購入決定を下 AWS Marketplace せるように、にリストされている製品に関する十分な情報を提供することが目標です。

Note

AWS Data Exchange のデータ製品のセキュリティについては、「AWS Data Exchange ユーザーガイド」の「[セキュリティ](#)」を参照してください。

の販売者のセキュリティの詳細については AWS Marketplace、「販売者ガイド」の[AWS Marketplace 「セキュリティ」](#)を参照してください。AWS Marketplace

販売者と共有されるサブスクリイバー情報

当社は、以下の理由により、販売者の連絡先情報を当社の販売者と共有することがあります。

- カスタマーレーニングとテクニカルサポートを提供する必要がある場合。
- ソフトウェアのアクティベーション、設定、およびコンテンツのカスタマイズに使用する場合。
- 販売チームに社内で補償する場合。

さらに、販売者が販売チームに報酬を支払うために、会社名、住所、使用料などの情報を販売者と共有することがあります。また、ベンダーがマーケティングキャンペーンの有効性を評価できるように、当社が特定の情報を販売者と共有することもあります。販売者は、この情報をすでに所有している情報と共に使用して、販売チームに対する報酬や特定の購入者の使用法を決定することができます。

そうでない場合は、当社では通常、購入者の情報を販売者と共有することはなく、共有する情報は個人を特定できる情報ではありません。ただし、購入者が個人情報を共有することを当社に許可している場合、もしくは法律や規制に準拠するためにその情報を販売者に提供することが必要であると当社が認めた場合を除きます。

IAM ポリシーを IPv6 にアップグレードする

AWS Marketplace のお客様は、IAM ポリシーを使用して IP アドレスの許容範囲を設定し、設定された範囲外の IP アドレスが AWS Marketplace リソースにアクセスできないようにします。

AWS Marketplace ウェブサイトドメインは IPv6 プロトコルにアップグレード中です。

IPv6 アドレスを処理するように更新されていない IP アドレスフィルタリングポリシーは、クライアントが AWS Marketplace ウェブサイト上のリソースにアクセスできなくなる可能性があります。

IPv4 から IPv6 に移行する際、影響を受けるお客様

デュアルアドレス指定を使用しているお客様は、このアップグレードの影響を受けます。デュアルアドレス指定とは、ネットワークが IPv4 と IPv6 の両方をサポートすることを意味します。

デュアルアドレス指定を使用している場合は、現在 IPv4 形式のアドレスで構成されている IAM ポリシーを、IPv6 形式のアドレスを含むように更新する必要があります。

アクセスに関する問題については、[AWS Support](#) にお問い合わせください。

Note

次のお客様は、アップグレードの影響を受けません。

- IPv4 ネットワークのみを利用しているお客様。
- IPv6 ネットワークのみを利用しているお客様。

IPv6 とは

IPv6 は、最終的に IPv4 を IPv6 に置き換えることを意図した次世代の IP 規格です。以前のバージョンの IPv4 は、32 ビットのアドレス指定方式を使用して 43 億台のデバイスをサポートしていました。IPv6 は代わりに 128 ビットのアドレス指定を使用して、約 340 兆 x1 兆倍 x1 兆倍 (つまり 2 の 128 乗) のデバイスをサポートします。

```
2001:cdba:0000:0000:0000:0000:3257:9652
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

IPv6 用の IAM ポリシーを更新する

現在、IAM ポリシーは、aws:SourceIp フィルターを使用して IP アドレスの許容範囲を設定するために使用されています。

デュアルアドレス指定では、IPv4 と IPv6 の両方のトラフィックをサポートしています。ネットワークでデュアルアドレス指定を使用している場合、IP アドレスフィルタリングに使用されている IAM ポリシーが、IPv6 のアドレス範囲を含むように更新されていることを確認する必要があります。

例えば、この Amazon S3 バケットポリシーは、Condition 要素で許可された IPv4 アドレス範囲の 192.0.2.0.* と 203.0.113.0.* を識別します。

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NotIpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24",
          "203.0.113.0/24"
        ]
      },
      "Bool": {
        "aws:ViaAWSService": "false"
      }
    }
  }
}
```

このポリシーを更新するには、Condition 要素を IPv6 アドレス範囲の 2001:DB8:1234:5678::/64 と 2001:cdba:3257:8593::/64 を含むように更新します。

Note

既存の IPv4 アドレスは下位互換性のために必要なため、削除しないでください。

```
"Condition": {
  "NotIpAddress": {
    "aws:SourceIp": [
      "192.0.2.0/24", <<DO NOT remove existing IPv4 address>>
    ]
  }
}
```

```
        "*203.0.113.0/24*", <<DO NOT remove existing IPv4 address>>
        "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
        "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
    ]
},
"Bool": {
    "aws:ViaAWSService": "false"
}
}
```

IAM によるアクセス許可の管理の詳細については、「AWS Identity and Access Management 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](#)」を参照してください。

IPv4 から IPv6 に更新した後のネットワークのテスト

IAM ポリシーを IPv6 形式に更新した後、ネットワークが IPv6 エンドポイントと AWS Marketplace ウェブサイト機能にアクセスしているかどうかをテストできます。

トピック

- [Linux/UNIX または Mac OS X を使用したネットワークのテスト](#)
- [Windows 7 または Windows 10 でネットワークをテストする](#)
- [AWS Marketplace ウェブサイトのテスト](#)

Linux/UNIX または Mac OS X を使用したネットワークのテスト

Linux/Unix または Mac OS X を使用している場合、次の curl コマンドを使用して、ネットワークが IPv6 エンドポイントにアクセスしているかどうかをテストできます。

```
curl -v -s -o /dev/null http://ipv6.ec2-reachability.amazonaws.com/
```

例えば、IPv6 で接続している場合、接続されている IP アドレスには、次の情報が表示されます。

```
* About to connect() to aws.amazon.com port 443 (#0)
* Trying IPv6 address... connected
* Connected to aws.amazon.com (IPv6 address) port 443 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.18.1 (x86_64-unknown-linux-gnu) libcurl/7.18.1 OpenSSL/1.0.1t
zlib/1.2.3
> Host: aws.amazon.com
```

Windows 7 または Windows 10 でネットワークをテストする

Windows 7 または Windows 10 を使用している場合、ネットワークが IPv6 または IPv4 でデュアルスタックのエンドポイントにアクセスできるかどうかをテストできます。次の例に示すように ping コマンドを使用します。

```
ping aws.amazon.com
```

IPv6 経由でエンドポイントにアクセスしている場合、このコマンドは IPv6 アドレスを返します。

AWS Marketplace ウェブサイトのテスト

更新後の AWS Marketplace ウェブサイト機能のテストは、主にポリシーの記述方法と使用目的によって異なります。一般的には、ポリシーで指定されている機能が意図したとおりに動作することを確認する必要があります。

以下のシナリオは、AWS Marketplace ウェブサイト機能のテストを開始するのに役立ちます。

AWS Marketplace ウェブサイトの購入者として、次のタスクを実行できるかどうかをテストします。

- AWS Marketplace 製品をサブスクライブします。
- AWS Marketplace 製品を設定します。
- AWS Marketplace 製品を起動または実行します。

AWS Marketplace ウェブサイトの販売者として、次のタスクを実行できるかどうかをテストします。

- 既存の AWS Marketplace 製品を管理します。
- AWS Marketplace 製品を作成します。

AWS Marketplace サブスクリプションへのアクセスのコントロール

AWS IAM Identity Center は、ワークフォース ID を安全に作成または接続し、AWS アカウント およびアプリケーション間で一元的にアクセスを管理するのに役立ちます。IAM Identity Center は、あらゆる規模とタイプの組織に、ワークフォースの認証と認可 AWS を行う際に推奨されるアプロー

手です。その他の設定ガイダンスについては、「[AWS セキュリティリファレンスアーキテクチャ](#)」を参照してください。

IAM Identity Center には、ユーザーが自分に割り当てられている AWS アカウント、ロール、クラウドアプリケーション、カスタムアプリケーションを一元的に検索してアクセスできるユーザーポータルが含まれます。IAM Identity Center は、接続先ディレクトリのユーザーとグループにシングルサインオンアクセスを割り当て、ユーザーはアクセス権許可セットを使用してアクセスレベルを決定します。これにより、一時的なセキュリティ認証情報を有効にします。AWS 組織全体の AWS Marketplace サブスクリプションの管理を委任 AWS Marketplace するためのアクセスに特定の AWS マネージドロールを割り当てることで、アクセスのレベルを定義できます。

例えば、顧客 A は、そのロールにアタッチされた ManagedMarketplace_ViewOnly ポリシーとのフェデレーションによってロールを引き受けます。つまり、顧客 A は AWS Marketplace のサブスクリプションのみを表示できるということになります。サブスクリプションを閲覧するアクセス許可を持つ IAM ロールを作成し、顧客 A に[このロールを引き受ける](#)権限を付与できます。

AWS Marketplace アクセスの IAM ロールの作成

IAM ロールを使用して、AWS リソースへのアクセスを委任できます。

アクセス AWS Marketplace 許可を割り当てる IAM ロールを作成するには

1. [IAM コンソール](#)を開きます。
2. 左側のナビゲーションペインから、[Roles] (ロール) を選択してから、[Create role] (ロールの作成) をクリックします。
3. を選択します AWS アカウント。
4. [アクセス許可を追加] から、次のポリシーのいずれかを選択します。
 - サブスクリプションを表示するのみ (変更はできない) のアクセス許可を付与するには、[AWSMarketplaceRead-only] を選択します。
 - サブスクリプションやサブスクリプション解除のアクセス許可を付与するには、[AWSMarketplaceManageSubscriptions] を選択します。
 - サブスクリプションの完全な統制を許可するには、[AWSMarketplaceFullAccess] を選択します。
5. [次へ] をクリックします。
6. [ロール名] に、ロールの名前を入力します。例えば、*MarketplaceReadOnly* または *MarketplaceFullAccess*。次に、[Create role (ロールの作成)] を選択します。詳細については、「[IAM ロールの作成](#)」を参照してください。

Note

指定したアカウントの管理者は、そのアカウントのすべてのユーザーに、このロールを引き受けるアクセス許可を付与できます。

前述のステップを繰り返し、異なるアクセス許可セットを持つロールを追加で作成し、各ユーザーのペルソナが、カスタマイズされたアクセス許可を持つ IAM ロールを使用できるようにします。

ここで説明する AWS マネージドポリシーのアクセス許可に限定されません。IAM を使用して、カスタムアクセス許可を持つポリシーを作成し、そのポリシーを IAM ロールに追加できます。詳細については、「[IAM ポリシーの管理](#)」および「[IAM アイデンティティアクセス許可の追加](#)」を参照してください。

AWS の マネージドポリシー AWS Marketplace

AWS 管理ポリシーを使用して、基本的な AWS Marketplace アクセス許可を付与できます。次に、任意のシナリオで独自のポリシーを作成し、シナリオ用の特定の要件を持つロールに適用できます。次の基本的な AWS Marketplace 管理ポリシーを使用して、どのアクセス許可を持つかを制御できます。

- `AWSMarketplaceRead-only`
- `AWSMarketplaceManageSubscriptions`
- `AWSPrivateMarketplaceRequests`
- `AWSPrivateMarketplaceAdminFullAccess`
- `AWSMarketplaceFullAccess`

AWS Marketplace は、特定のシナリオに特化した マネージドポリシーも提供します。AWS Marketplace 購入者向けの AWS 管理ポリシーの完全なリストと、それらが提供するアクセス許可の説明については、「」を参照してください。[AWS 購入者向けの AWS Marketplace マネージドポリシー](#)。

License Manager で使用するアクセス許可

AWS Marketplace は と統合して、組織内のアカウント間でサブスクライブする製品のライセンス AWS License Manager を管理および共有します。でサブスクリプションの詳細をすべて表示する

には AWS Marketplace、ユーザーが からライセンス情報を一覧表示できる必要があります AWS License Manager。

ユーザーが AWS Marketplace 製品とサブスクリプションに関するすべてのデータを表示するために必要なアクセス許可を持っていることを確認するには、次のアクセス許可を追加します。

- `license-manager:ListReceivedLicenses`

アクセス許可の設定の詳細については、「[IAM ユーザーガイド](#)」の「IAM ポリシーの管理」を参照してください。

追加リソース

IAM ロールの詳細については、「IAM ユーザーガイド」の「[IAM アイデンティティ \(ユーザー、ユーザーグループ、ロール\)](#)」を参照してください。

IAM アクセス許可とポリシーの管理の詳細については、IAM ユーザーガイドの「[ポリシーを使用した AWS リソースへのアクセスの制御](#)」を参照してください。

AWS Data Exchange のデータ製品の IAM アクセス許可とポリシーの管理の詳細については、「AWS Data Exchange ユーザーガイド」の「[AWS Data Exchange でのアイデンティティとアクセス管理](#)」を参照してください。

AWS 購入者向けの AWS Marketplace マネージドポリシー

AWS 管理ポリシーは、によって作成および管理されるスタンドアロンポリシーです AWS。AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、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注意してください。ユースケース別に[カスタマー マネージドポリシー](#)を定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、その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 ID (ユーザー、グループ、ロール) に影響します。は、新しい AWS のサービスが起動されるか、既存のサービスで新しい API AWS オペレーションが使用可能になると、AWS 管理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 マネージドポリシー](#)」を参照してください。

このセクションには、購入者の AWS Marketplace へのアクセスを管理するために使用される各ポリシーが記載されています。販売者ポリシーの詳細については、「[AWS Marketplace 販売者ガイド](#)」の「[販売者向けの管理ポリシー](#)」を参照してください。AWS Marketplace

トピック

- [AWS マネージドポリシー: AWSMarketplaceDeploymentServiceRolePolicy](#)
- [AWS マネージドポリシー: AWSMarketplaceFullAccess](#)
- [AWS マネージドポリシー: AWSMarketplaceLicenseManagementServiceRolePolicy](#)
- [AWS 管理ポリシー: AWSMarketplaceManageSubscriptions](#)
- [AWS 管理ポリシー: AWSMarketplaceProcurementSystemAdminFullAccess](#)
- [AWS 管理ポリシー: AWSMarketplaceReadのみ](#)
- [AWS マネージドポリシー: AWSPrivateMarketplaceAdminFullAccess](#)
- [AWS マネージドポリシー: AWSPrivateMarketplaceRequests](#)
- [AWS マネージドポリシー: AWSServiceRoleForPrivateMarketplaceAdminPolicy](#)
- [AWS マネージドポリシー: AWSVendorInsightsAssessorFullAccess](#)
- [AWS 管理ポリシー: AWSVendorInsightsAssessorReadOnly](#)
- [AWS マネージドポリシーに関するAWS Marketplace の更新](#)

AWS マネージドポリシー: AWSMarketplaceDeploymentServiceRolePolicy

IAM エンティティに AWSMarketplaceDeploymentServiceRolePolicy をアタッチすることはできません。このポリシーは、がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロール AWS Marketplace にアタッチされます。詳細については、「[AWS Marketplace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。

このポリシーは、がユーザーに代わって AWS Marketplace にシークレットとして保存されるデプロイ関連のパラメータを管理できるようにする寄稿者アクセス許可を付与[AWS Secrets Manager](#)します。

AWS マネージドポリシー: AWSMarketplaceFullAccess

AWSMarketplaceFullAccess ポリシーは IAM ID にアタッチできます。

このポリシーは、購入者および販売者として、AWS Marketplace および関連サービスへのフルアクセスを許可する管理権限を付与します。これらのアクセス許可には、AWS Marketplace ソフトウェアのサブスクリプションとサブスクリプション解除、からの AWS Marketplace ソフトウェアインスタンスの

管理 AWS Marketplace、アカウントでのプライベートマーケットプレイスの作成と管理、Amazon EC2 AWS CloudFormation、および Amazon EC2 Systems Manager へのアクセスが含まれます。

許可の詳細

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
```



```

        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:StartAutomationExecution"
    ],
    "Resource": [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "s3:ListBucket",
        "s3:GetObject"
    ],
    "Resource": [
        "arn:aws:s3::*image-build*"
    ]
},
{
    "Effect": "Allow",

```

```

    "Action": [
      "sns:Publish",
      "sns:setTopicAttributes"
    ],
    "Resource": "arn:aws:sns:*:*:*image-build*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringLike": {
        "iam:PassedToService": [
          "ec2.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringLike": {
        "iam:PassedToService": [
          "ssm.amazonaws.com"
        ],
        "iam:AssociatedResourceARN": [
          "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
          "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
          "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
          "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
          "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
          "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
          "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
          "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
        ]
      }
    }
  }
}

```

```

    ]
  }
}
]
}

```

AWS マネージドポリシー :

AWSMarketplaceLicenseManagementServiceRolePolicy

IAM エンティティ `AWSMarketplaceLicenseManagementServiceRolePolicy` に をアタッチすることはできません。このポリシーは、 がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロール `AWS Marketplace` にアタッチされます。詳細については、「[AWS Marketplace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。

このポリシーは、 がユーザーに代わってライセンスを管理できるようにする権限 `AWS Marketplace` を寄稿者に付与します。

許可の詳細

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLicenseManagerActions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "license-manager:ListReceivedGrants",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager>DeleteGrant",
        "license-manager:AcceptGrant"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

AWS 管理ポリシー : AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions ポリシーは IAM ID にアタッチできます。

このポリシーは、寄稿者に AWS Marketplace 製品のサブスクリプションとサブスクリプション解除を許可するアクセス許可を付与します。

許可の詳細

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Resource": "*",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ListPrivateListings"
      ]
    }
  ]
}
```

AWS 管理ポリシー : AWSMarketplaceProcurementSystemAdminFullAccess

AWSMarketplaceProcurementSystemAdminFullAccess ポリシーは IAM ID にアタッチできません。

このポリシーは、組織内のアカウントの一覧表示など、AWS Marketplace eProcurement の統合のあらゆる側面を管理できる管理者権限を付与します。eProcurement 統合の詳細については、「[AWS Marketplace 調達システムとの統合](#)」を参照してください。

許可の詳細

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS 管理ポリシー: AWSMarketplaceReadのみ

AWSMarketplaceRead-only ポリシーは IAM ID にアタッチできます。

このポリシーは、でのアカウントの製品、プライベートオファー、サブスクリプションの表示 AWS Marketplace、およびアカウントの Amazon EC2 AWS Identity and Access Management、および Amazon SNS リソースの表示を許可する読み取り専用アクセス許可を付与します。

許可の詳細

```
{
  "Version": "2012-10-17",
```

```
"Statement": [
  {
    "Resource": "*",
    "Action": [
      "aws-marketplace:ViewSubscriptions",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAddresses",
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs"
    ],
    "Effect": "Allow"
  },
  {
    "Resource": "*",
    "Effect": "Allow",
    "Action": [
      "aws-marketplace:ListBuilds",
      "aws-marketplace:DescribeBuilds",
      "iam:ListRoles",
      "iam:ListInstanceProfiles",
      "sns:GetTopicAttributes",
      "sns:ListTopics"
    ]
  },
  {
    "Resource": "*",
    "Effect": "Allow",
    "Action": [
      "aws-marketplace:ListPrivateMarketplaceRequests",
      "aws-marketplace:DescribePrivateMarketplaceRequests"
    ]
  },
  {
    "Resource": "*",
    "Effect": "Allow",
    "Action": [
      "aws-marketplace:ListPrivateListings"
    ]
  }
]
```

```
}
```

AWS マネージドポリシー : AWSPrivateMarketplaceAdminFullAccess

AWSPrivateMarketplaceAdminFullAccess ポリシーは IAM ID にアタッチできます。

このポリシーは、アカウント (または組織) 内のプライベートマーケットプレイスを管理するためのフルアクセスを許可する管理者権限を付与します。複数の管理者を使用する方法の詳細については、「[the section called “プライベートマーケットプレイス管理者向けのカスタムポリシーの作成”](#)」を参照してください。

許可の詳細

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PrivateMarketplaceRequestPermissions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "PrivateMarketplaceCatalogAPIPermissions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    "Sid": "PrivateMarketplaceCatalogTaggingPermissions",
    "Effect": "Allow",
    "Action": [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
    ],
    "Resource": "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
},
{
    "Sid": "PrivateMarketplaceOrganizationPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*"
}
]
}

```

AWS マネージドポリシー : AWSPrivateMarketplaceRequests

AWSPrivateMarketplaceRequests ポリシーは IAM ID にアタッチできます。

このポリシーでは、プライベートマーケットプレイスへの製品の追加をリクエストしたり、それらのリクエストを閲覧したりするためのアクセス許可を寄稿者に付与します。これらのリクエストは、プライベートマーケットプレイスの管理者によって承認または拒否される必要があります。

許可の詳細

```

{
    "Version": "2012-10-17",
    "Statement": [
        {

```



```
    "Effect": "Allow",
    "Action": [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
    ],
    "Resource": "*"
}
]
```

AWS マネージドポリシー:

AWSServiceRoleForPrivateMarketplaceAdminPolicy

IAM エンティティに `AWSServiceRoleForPrivateMarketplaceAdminPolicy` 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 AWS Marketplace 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、「[AWS Marketplace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。

このポリシーは、が Private Marketplace リソースを記述および更新し、AWS Marketplace を記述できるようにする寄稿者アクセス許可を付与します AWS Organizations。

AWS マネージドポリシー: AWSVendorInsightsAssessorFullAccess

`AWSVendorInsightsAssessorFullAccess` ポリシーは IAM ID にアタッチできます。

このポリシーは、権限を持つ AWS Marketplace Vendor Insights リソースを表示し、Vendor Insights AWS Marketplace サブスクリプションを管理するためのフルアクセスを付与します。これらのリクエストは、管理者によって承認または拒否される必要があります。これにより、サードパーティーのレポートへの読み取り専用アクセスが許可され AWS Artifact ます。

AWS Marketplace Vendor Insights は、評価者が購入者と等しく、ベンダーが販売者と等しいことを示します。

許可の詳細

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Action": [
      "vendor-insights:GetProfileAccessTerms",
      "vendor-insights:ListEntitledSecurityProfiles",
      "vendor-insights:GetEntitledSecurityProfileSnapshot",
      "vendor-insights:ListEntitledSecurityProfileSnapshots"
    ],
    "Resource": "*"
  },
  {
    "Action": [
      "aws-marketplace:CreateAgreementRequest",
      "aws-marketplace:GetAgreementRequest",
      "aws-marketplace:AcceptAgreementRequest",
      "aws-marketplace:CancelAgreementRequest",
      "aws-marketplace:ListAgreementRequests",
      "aws-marketplace:SearchAgreements",
      "aws-marketplace:CancelAgreement"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws-marketplace:AgreementType": "VendorInsightsAgreement"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "artifact:GetReport",
      "artifact:GetReportMetadata",
      "artifact:GetTermForReport",
      "artifact:ListReports"
    ],
    "Resource": "arn:aws:artifact:*::report/*"
  }
]
}

```

AWS 管理ポリシー: AWSVendorInsightsAssessorReadOnly

AWSVendorInsightsAssessorReadOnly ポリシーは IAM ID にアタッチできます。

このポリシーは、権限を持つ AWS Marketplace Vendor Insights リソースを表示するための読み取り専用アクセスを許可します。これらのリクエストは、管理者によって承認または拒否される必要があります。これにより、 のレポートへの読み取り専用アクセスが許可されます AWS Artifact。

リクエストは、管理者によって承認または拒否される必要があります。これにより、サードパーティーのレポートへの読み取り専用アクセスが許可され AWS Artifact ます。

AWS Marketplace Vendor Insights は、このガイドの目的上、評価者を購入者として識別し、ベンダーが販売者と同等であると判断します。

許可の詳細

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "arn:aws:artifact:*::report/*"
    }
  ]
}
```

AWS マネージドポリシーに関するAWS Marketplace の更新

このサービスがこれらの変更の追跡を開始した AWS Marketplace 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、AWS Marketplace [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。

変更	説明	日付
レガシーAWSMarketplaceImageBuildFullAccess AWS Marketplace ポリシーを削除しました	AWS Marketplace はプライベートイメージビルドの配信方法を停止したため、AWSMarketplaceImageBuildFullAccess ポリシーも廃止されました。	2024 年 5 月 8 日
AWSServiceRoleForPrivateMarketplaceAdminPolicy – で新機能のポリシーを追加 AWS Marketplace	AWS Marketplace は、Private Marketplace リソースの管理との説明をサポートする新しいポリシーを追加しました AWS Organizations。	2024 年 2 月 16 日
AWSPrivateMarketplaceAdminFullAccess – 既存のポリシーの更新	AWS Marketplace は、データの読み取り AWS Organizations をサポートするようにポリシーを更新しました。	2024 年 2 月 16 日
AWSMarketplaceDeploymentServiceRolePolicy – で新機能のポリシーを追加 AWS Marketplace	AWS Marketplace は、デプロイ関連のパラメータの管理をサポートする新しいポリシーを追加しました。	2023 年 11 月 29 日
AWSMarketplaceReadのみ および AWSMarketplaceManageSubscriptions – 既存のポリシーの更新	AWS Marketplace は、プライベートオフページへのアクセスを許可するように既存のポリシーを更新しました。	2023 年 1 月 19 日
AWSPrivateMarketplaceAdminFullAccess – 既存のポリシーの更新	AWS Marketplace は、新しいタグベースの認証機能のポリシーを更新しました。	2022 年 12 月 9 日
AWSVendorInsightsAssessorReadOnly AWS Marketplace 更新済み	AWS Marketplace が更新されAWSVendorInsightsAssessorReadOnly 、AWS Artifact サードパー	2022 年 11 月 30 日

変更	説明	日付
AWSVendorInsightsAssessorReadOnly	ティーレポート (プレビュー) のレポートへの読み取り専用アクセスが追加されました。	
AWSVendorInsightsAssessorFullAccess AWS Marketplace 更新済み AWSVendorInsightsAssessorFullAccess	AWS Marketplace は AWSVendorInsightsAssessorFullAccess し、AWS Artifact サードパーティーレポート (プレビュー) への契約検索と読み取り専用アクセスを追加しました。	2022 年 11 月 30 日
AWSVendorInsightsAssessorFullAccess および AWSVendorInsightsAssessorReadOnly - の新機能に関するポリシーを追加 AWS Marketplace	AWS Marketplace AWS Marketplace Vendor Insights の新機能である AWSVendorInsightsAssessorFullAccess および AWSVendorInsightsAssessorReadOnly のポリシーを追加しました。	2022 年 7 月 26 日
AWSMarketplaceFullAccess および AWSMarketplaceImageBuildFullAccess - 既存のポリシーの更新	AWS Marketplace は、セキュリティを強化するために不要になったアクセス許可を削除しました。	2022 年 3 月 4 日
AWSPrivateMarketplaceAdminFullAccess - 既存ポリシーへの更新。	AWS Marketplace は、 AWSPrivateMarketplaceAdminFullAccess ポリシー内の未使用のアクセス許可を削除しました。	2021 年 8 月 27 日

変更	説明	日付
AWSMarketplaceFullAccess - 既存ポリシーへの更新。	AWS Marketplace がAWSMarketplaceFull Access ポリシーから重複するec2:DescribeAccountAttributes アクセス許可を削除しました。	2021 年 7 月 20 日
AWS Marketplace が変更の追跡を開始しました	AWS Marketplace が 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 20 日

カスタマーサポートの AWS アカウント 電話番号の検索

ユーザーまたはユーザーが に連絡する必要がある場合は AWS Support、AWS アカウント 番号が必要です。

AWS アカウント 番号を検索するには

1. ユーザー名で [AWS Management Console](#) にサインインします。
2. 上部のナビゲーションバーで、[サポート]、[サポートセンター] の順に選択します。

AWS アカウント ID (アカウント番号) が上部のナビゲーションバーの下に表示されます。

AWS Marketplaceのサービスにリンクされたロールの使用

AWS Marketplace は 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。サービスにリンクされたロールは、 に直接リンクされた一意のタイプの IAM ロールです AWS Marketplace。サービスリンクロールは、AWS Marketplace による事前定義済みのロールであり、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可を備えています。

トピック

- [ロールを使用した の使用権限の共有 AWS Marketplace](#)
- [でロールを使用して発注書进行操作する AWS Marketplace](#)

- [ロールを使用して製品を設定および起動する AWS Marketplace](#)
- [でロールを使用して Private Marketplace を設定する AWS Marketplace](#)

ロールを使用した の使用権限の共有 AWS Marketplace

AWS Marketplace は 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。サービスにリンクされたロールは、に直接リンクされた一意のタイプの IAM ロールです AWS Marketplace。サービスにリンクされたロールは、によって事前定義 AWS Marketplace されており、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、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、の設定 AWS Marketplace が簡単になります。は、サービスにリンクされたロールのアクセス許可 AWS Marketplace を定義し、特に定義されている場合を除き、のみがそのロールを引き受け AWS Marketplace 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ます。こ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。

AWS Marketplace サブスクリプションを AWS 組織内の他のアカウントと共有するには AWS License Manager、共有するアカウントごとにアクセス AWS Marketplace 許可を付与する必要があります。これを行うには、[AWSServiceRoleForMarketplaceLicenseManagement](#) ロールを使用します。詳細については、「[のサービスにリンクされたロールの作成 AWS Marketplace](#)」を参照してください。

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 と連動するAWS 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探してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] を選択します。

のサービスにリンクされたロールのアクセス許可 AWS Marketplace

AWS Marketplace は、という名前のサービスにリンクされたロールを使用します [AWSServiceRoleForMarketplaceLicenseManagement](#)。このロールは AWS Marketplace、でサブスクライブする製品のライセンス AWS License Manager を で作成および管理するためのアクセス許可を に付与します AWS Marketplace。

[AWSServiceRoleForMarketplaceLicenseManagement](#) サービスにリンクされたロールは、ユーザーに代わって License Manager でアクションを実行するために、次のサービスを信頼します。

- `license-management.marketplace.amazonaws.com`

という名前のロールアクセス許可ポリ

シーAWSMarketplaceLicenseManagementServiceRolePolicyは AWS Marketplace、 が指定されたりソースに対して次のアクションを実行できるようにします。

- アクション:
 - "organizations:DescribeOrganization"
 - "license-manager:ListReceivedGrants"
 - "license-manager:ListDistributedGrants"
 - "license-manager:GetGrant"
 - "license-manager:CreateGrant"
 - "license-manager:CreateGrantVersion"
 - "license-manager>DeleteGrant"
 - "license-manager:AcceptGrant"
- リソース:
 - すべてのリソース ("*")

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、グループ、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「[サービスリンクされたロールのアクセス許可](#)」を参照してください。

のサービスにリンクされたロールの作成 AWS Marketplace

AWS Marketplace との統合を設定すると、 によってサービスにリンクされたロールが作成されます AWS License Manager。

組織内のすべてのアカウントに対してサービスにリンクされたロールを一度に AWS Marketplace 作成するように指定することも、1つのアカウントにサービスにリンクされたロールを一度に作成することもできます。すべてのアカウントでサービスにリンクされたロールを作成するオプションは、組織で [すべての機能] が有効になっている場合にのみ使用できます。詳細については、「AWS Organizations ユーザーガイド」の「[組織内のすべての機能の有効化](#)」を参照してください。

すべてのアカウントでサービスにリンクされたロールを作成するには

1. [AWS Marketplace コンソール](#)でサインインし、[設定] を選択します。
2. [AWS Organizations 統合] セクションで、[統合を作成] を選択します。

3. AWS Organizations 「統合の作成」 ページで、「組織全体で信頼されたアクセスを有効にする」を選択し、「統合の作成」を選択します。

Note

この設定により、内の信頼が有効になります AWS Organizations。その結果、現在のアクションに加えて、今後組織に追加されるアカウントには、サービスにリンクされたロールが自動的に追加されます。

現在のアカウントにサービスにリンクされたロールを作成するには

1. [AWS Marketplace コンソール](#) でサインインし、[設定] を選択します。
2. [AWS Organizations 統合] セクションで、[統合を構成する] を選択します。
3. AWS Organizations 「統合の作成」 ページで、AWS Marketplace このアカウント のライセンス管理サービスにリンクされたロールを選択し、「統合の作成」を選択します。

Important

現在のアカウントに対してのみサービスにリンクされたロールを作成することを選択した場合、組織全体で信頼されたアクセスを有効にすることはできません。でライセンスを共有 (付与または受領) するアカウントごとに、これらのステップを繰り返す必要があります AWS Marketplace。これには、組織に今後追加されるアカウントも含まれます。

のサービスにリンクされたロールの編集 AWS Marketplace

AWS Marketplace では、サービスにリンクされた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を作成した後は、多くのエンティティによって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 を使用したロールの説明の編集はできます。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。

のサービスにリンクされたロールの削除 AWS Marketplace

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエン

ティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

Note

リソースを削除しようとしたときに AWS Marketplace サービスがロールを使用している場合、削除が失敗する可能性があります。その場合は、数分待ってからオペレーションを再試行してください。

IAM を使用してサービスリンクロールを手動で削除するには

IAM コンソール、または AWS API を使用して AWS CLI、`AWSServiceRoleForMarketplaceLicenseManagement` サービスにリンクされたロールを削除します。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削除](#)」を参照してください。

AWS Marketplace のサービスにリンクされたロールをサポートするリージョン

AWS Marketplace は、サービスが利用可能なすべての AWS リージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「[AWS Marketplace リージョンとエンドポイント](#)」を参照してください。

でロールを使用して発注書进行操作する AWS Marketplace

AWS Marketplace は 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。サービスにリンクされたロールは、に直接リンクされた一意のタイプの IAM ロールです AWS Marketplace。サービスリンクロールは、AWS Marketplace による事前定義済みのロールであり、ユーザーに代わってサービスから他の AWS のサービス呼び出すために必要なすべてのアクセス許可を備えています。

サービスにリンクされたロールを使用すると、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、の設定 AWS Marketplace が簡単になります。は、サービスにリンクされたロールのアクセス許可 AWS Marketplace を定義し、特に定義されている場合を除き、のみがそのロールを引き受け AWS Marketplace することができます。定義したアクセス許可には、信頼ポリシーと許可ポリシーが含まれます。こ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は、まずその関連リソースを削除しなければ削除できません。これにより、AWS Marketplace リソースにアクセスするためのアクセス許可を誤って削除することがないため、リソースが保護されます。

サービスリンクロールをサポートする他のサービスについては、「[IAM と連動するAWS のサービス](#)」を参照し、[Service-linked role (サービスリンクロール)] の列内で [Yes (はい)] と表記されたサービスを確認してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

のサービスにリンクされたロールのアクセス許可 AWS Marketplace

AWS Marketplace は、 という名前のサービスにリンクされたロールを使用します `AWSServiceRoleForMarketplacePurchaseOrders`。このロールは、 の AWS Marketplace サブスクリプションに発注書番号をアタッチする AWS Marketplace アクセス許可を提供します AWS Billing and Cost Management。

`AWSServiceRoleForMarketplacePurchaseOrders` サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `purchase-orders.marketplace.amazonaws.com`

という名前のロールアクセス許可ポリシー `AWSMarketplacePurchaseOrdersServiceRolePolicy` は AWS Marketplace、 が指定されたリソースに対して次のアクションを実行できるようにします。

- アクション: "*" 上で `"purchase-orders:ViewPurchaseOrders"`, `"purchase-orders:ModifyPurchaseOrders"`

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、権限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「[サービスにリンクされたロールのアクセス許可](#)」を参照してください。

のサービスにリンクされたロールの作成 AWS Marketplace

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。との統合を設定すると AWS Billing and Cost Management、 によってサービスにリンクされたロールが自動的に AWS Marketplace 作成されます。

Note

内では AWS Organizations、この設定は管理アカウントでのみ機能します。この手順は管理アカウントから実行する必要があります。これにより、組織内のすべてのアカウントのサービスにリンクされたロールと発注書サポートが設定されます。

サービスにリンクされたロールを作成するには

1. [AWS Marketplace コンソール](#)で管理アカウントにサインインし、[設定] を選択します。
2. [AWS 請求インテグレーション] セクションで、[統合を構成する] を選択します。
3. AWS 「請求統合の作成AWS Marketplace」 ページで、組織の請求管理サービスにリンクされたロールを選択し、「統合の作成」を選択します。

このサービスリンクロールを削除した後に再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。この統合を設定すると AWS Billing and Cost Management、によってサービスにリンクされたロールが再度 AWS Marketplace 作成されます。

のサービスにリンクされたロールの編集 AWS Marketplace

AWS Marketplace では、AWSServiceRoleForMarketplacePurchaseOrdersサービスにリンクされた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を作成した後は、多くのエンティティによって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 を使用したロールの説明の編集はできます。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。

のサービスにリンクされたロールの削除 AWS Marketplace

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスにリンクされたロールを手動で削除する

IAM コンソール、または AWS API を使用して AWS CLI、AWSServiceRoleForMarketplacePurchaseOrdersサービスにリンクされたロールを削除します。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削除](#)」を参照してください。

AWS Marketplace のサービスにリンクされたロールをサポートするリージョン

AWS Marketplace は、サービスが利用可能なすべての AWS リージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「[AWS Marketplace リージョンとエンドポイント](#)」を参照してください。

ロールを使用して製品を設定および起動する AWS Marketplace

AWS Marketplace は 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。サービスにリンクされたロールは、に直接リンクされた一意のタイプの IAM ロールです AWS Marketplace。サービスリンクロールは、AWS Marketplace による事前定義済みのロールであり、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可を備えています。

サービスにリンクされたロールを使用すると、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、の設定 AWS Marketplace が簡単になります。は、サービスにリンクされたロールのアクセス許可 AWS Marketplace を定義し、特に定義されている場合を除き、のみがそのロールを引き受け AWS Marketplace することができます。定義したアクセス許可には、信頼ポリシーと許可ポリシーが含まれます。こ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をサポートする他のサービスについては、「[IAM と連動するAWS のサービス](#)」を参照し、[Service-linked role (サービスリンクロール)] の列内で [Yes (はい)] と表記されたサービスを確認してください。そのサービスに関するサービスリンクロールのドキュメントを表示するには、リンクが設定されている [Yes (はい)] を選択します。

AWS Marketplaceのサービスリンクロールのアクセス許可

AWS Marketplace は、という名前のサービスにリンクされたロールを使用して、[AWS Secrets Manager](#) AWS Marketplace がユーザーに代わってにシークレットとして保存されるデプロイ関連のパラメータを管理AWSServiceRoleForMarketplaceDeploymentできるようにします。これらのシークレットは、AWS CloudFormation テンプレートで販売者が参照できます。テンプレートは、でクイック起動が有効になっている製品を設定するときに起動できます AWS Marketplace。

AWSServiceRoleForMarketplaceDeployment サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `deployment.marketplace.amazonaws.com`

という名前のロールアクセス許可ポリシーを使用し、`AWSServiceRoleForMarketplaceDeploymentServiceRolePolicy`、AWS Marketplace がリソースに対するアクションを完了できるようにします。

Note

AWS Marketplace 管理ポリシーの詳細については、[AWS Marketplace 「購入者向けの AWS 管理ポリシー」](#) を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageMarketplaceDeploymentSecrets",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager>DeleteSecret",
        "secretsmanager:RemoveRegionsFromReplication"
      ],
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ListSecrets",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:ListSecrets"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "TagMarketplaceDeploymentSecrets",
      "Effect": "Allow",
      "Action": [
```

```
"secretsmanager:TagResource"
],
"Resource": "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
"Condition": {
  "Null": {
    "aws:RequestTag/expirationDate": "false"
  },
  "ForAllValues:StringEquals": {
    "aws:TagKeys": [
      "expirationDate"
    ]
  },
  "StringEquals": {
    "aws:ResourceAccount": "${aws:PrincipalAccount}"
  }
}
}
]
}
```

ユーザー、グループ、ロールなどがサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限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権限」を参照してください。

AWS Marketplaceのサービスリンクロールの作成

サービスにリンクされたロールの設定は、そのロールが存在する限りで、クイック起動が有効になっているすべての製品にアクセス許可が付与される 1 回限りのアクションです。

クイック起動が有効になっている製品を設定すると、AWS Marketplace はアカウントに必要なサービスにリンクされたロールが作成されているかどうかを検出します。ロールがない場合、AWS Marketplace デプロイパラメータの統合を有効にするプロンプトが表示されます。これには統合を有効にするボタンが含まれます。このボタンを選択すると、[AWS Marketplace](#) が作成されます。

Important

このサービスにリンクされたロールは、クイック起動が有効になっている製品を以前に設定している場合に、アカウントに表示されます。詳細については、[「に新しいロールが表示されました AWS アカウント」](#)を参照してください。

サービスにリンクされたこのロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。クイック起動が有効になっている製品の [設定] ページを開くと、[統合を有効にする] ボタンが表示されます。このボタンをもう一度選択すると、サービスにリンクされたロールを再作成できます。

また、AWS Marketplace - デプロイ管理ユースケースでサービスにリンクされたロールを作成するには、IAM コンソールを使用します。AWS CLI または AWS API で、サービス名を使用して `deployment.marketplace.amazonaws.com` サービスにリンクされたロールを作成します。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作成](#)」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

のサービスにリンクされたロールの編集 AWS Marketplace

AWS Marketplace では、サービスにリンクされた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を作成した後は、多くのエンティティによって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 を使用したロールの説明の編集はできます。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。

AWS Marketplaceのサービスリンクロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

Note

リソースを削除する際に、サービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

`deployment.marketplace.amazonaws.com` サービスで使用されている AWS Marketplace リソースを削除するには、 から Marketplace デプロイ関連のシークレットをすべて削除する必要があります SecretsManager。関連するシークレットは次の方法で検索できます。

- `marketplace-deployment` によって管理されているシークレットを検索する。
- タグキー `aws:secretsmanager:owningService` と値 `marketplace-deployment` を使用してシークレットを検索する。

- シークレット名にプレフィックス `marketplace-deployment!` があるシークレットを検索する。

IAM を使用して、サービスにリンクされたロールを削除するには

IAM コンソール、または AWS API を使用して AWS

CLI、`AWSServiceRoleForMarketplaceDeployment` サービスにリンクされたロールを削除します。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削除](#)」を参照してください。

AWS Marketplace サービスにリンクされたロールでサポートされているリージョン

AWS Marketplace は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「[AWS Marketplace のリージョンとエンドポイント](#)」を参照してください。

でロールを使用して Private Marketplace を設定する AWS Marketplace

AWS Marketplace は 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。サービスにリンクされたロールは、に直接リンクされた一意のタイプの IAM ロールです AWS Marketplace。サービスリンクロールは、AWS Marketplace による事前定義済みのロールであり、ユーザーに代わってサービスから他の AWS のサービスを呼び出すために必要なすべてのアクセス許可を備えています。

サービスにリンクされたロールを使用すると、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、の設定 AWS Marketplace が簡単になります。は、サービスにリンクされたロールのアクセス許可 AWS Marketplace を定義し、特に定義されている場合を除き、のみがそのロールを引き受け AWS Marketplace することができます。定義したアクセス許可には、信頼ポリシーと許可ポリシーが含まれます。こ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をサポートする他のサービスについては、「[IAM と連動するAWS のサービス](#)」を参照し、[Service-linked role (サービスリンクロール)] の列内で [Yes (はい)] と表記されたサービスを確認してください。そのサービスに関するサービスリンクロールのドキュメントを表示するには、リンクが設定されている [Yes (はい)] を選択します。

AWS Marketplaceのサービスリンクロールのアクセス許可

AWS Marketplace は、という名前のサービスにリンクされたロー

ル `AWSServiceRoleForPrivateMarketplaceAdmin` を使用して Private Marketplace リソースを記述および更新し、を記述します AWS Organizations。

AWSServiceRoleForPrivateMarketplaceAdmin サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- private-marketplace.marketplace.amazonaws.com

という名前のロール許可ポリシーを使用してAWSServiceRoleForPrivateMarketplaceAdminPolicy、が指定されたリソースに対して次のアクションを実行 AWS Marketplace できるようにします。

Note

AWS Marketplace 管理ポリシーの詳細については、[AWS Marketplace 「購入者向けの AWS 管理ポリシー」](#)を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PrivateMarketplaceCatalogDescribePermissions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource": [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
      ]
    },
    {
      "Sid": "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource": "*"
    },
    {
      "Sid": "PrivateMarketplaceCatalogListPermissions",
      "Effect": "Allow",
```

```

    "Action": [
      "aws-marketplace:ListEntities",
      "aws-marketplace:ListChangeSets"
    ],
    "Resource": "*"
  },
  {
    "Sid": "PrivateMarketplaceStartChangeSetPermissions",
    "Effect": "Allow",
    "Action": [
      "aws-marketplace:StartChangeSet"
    ],
    "Condition": {
      "StringEquals": {
        "catalog:ChangeType": [
          "AssociateAudience",
          "DisassociateAudience"
        ]
      }
    },
    "Resource": [
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
      "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    ]
  },
  {
    "Sid": "PrivateMarketplaceOrganizationPermissions",
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeAccount",
      "organizations:DescribeOrganizationalUnit",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListChildren"
    ],
    "Resource": [
      "*"
    ]
  }
]
}

```

ユーザー、グループ、ロールなどがサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限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権限」を参照してください。

AWS Marketplaceのサービスリンクロールの作成

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。組織の Private Marketplace を有効にすると、によってサービスにリンクされたロール AWS Marketplace が自動的に作成されます。

Note

このロールは の管理アカウントでのみ必要 AWS Organizations で、管理アカウントでのみ作成されます。

サービスにリンクされたロールを作成するには

1. Private Marketplace の開始方法ページで、組織全体で信頼されたアクセスを有効にするオプションを選択し、Private Marketplace サービスにリンクされたロールを作成します。これらのオプションは、管理アカウントでのみ使用できます。
2. Private Marketplace を有効にする を選択します。

既存の Private Marketplace のお客様の場合、組織全体で信頼されたアクセスを有効にし、Private Marketplace のサービスにリンクされたロールを有効にするオプションは、プライベートマーケットプレイス管理ダッシュボードの設定ページで利用できます。

サービスにリンクされたこのロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。

のサービスにリンクされたロールの編集 AWS Marketplace

AWS Marketplace では、サービスにリンクされた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を作成すると、多くのエンティティによって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。

AWS Marketplaceのサービスリンクロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

サービスにリンクされたロールを削除する前に、以下を実行する必要があります。

- 組織全体の信頼されたアクセスを無効にします。
- すべてのプライベートマーケットプレイスエクスペリエンスの関連付けを解除します。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、または AWS API を使用して AWS CLI、`AWSServiceRoleForPrivateMarketplaceAdmin` サービスにリンクされたロールを削除します。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削除](#)」を参照してください。

AWS Marketplace サービスにリンクされたロールでサポートされているリージョン

AWS Marketplace は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「[AWS Marketplace のリージョンとエンドポイント](#)」を参照してください。

プライベートマーケットプレイスの管理者の作成

会社の[プライベートマーケットプレイス](#)設定を管理するために、IT 管理者グループを作成できます。組織でプライベートマーケットプレイスを有効にすると、プライベートマーケットプレイスの管理者は次のような多くのタスクを実行できます。

- エクスペリエンスとオーディエンスを表示して作成します。
- プライベートマーケットプレイスエクスペリエンスに製品を追加します。
- プライベートマーケットプレイスエクスペリエンスから製品を削除します。
- プライベートマーケットプレイスエクスペリエンスのユーザーインターフェイスを設定します。
- プライベートマーケットプレイスエクスペリエンスを有効または無効にします。
- を呼び出し AWS Marketplace Catalog API で、プライベートマーケットプレイスエクスペリエンスをプログラムで管理します。

組織では、各管理者がタスクのサブセットに限定されている複数のプライベートマーケットプレイス管理者を作成するには、[the section called “プライベートマーケットプレイス管理者向けのカスタムポリシーの作成”](#) を参照してください。

Note

プライベートマーケットプレイスの有効化は、管理アカウントから実行する必要がある 1 回限りのアクションです。詳細については、[「プライベートマーケットプレイスの開始方法」](#) を参照してください。

ユーザー、グループ、またはロールに [the section called “AWSPrivateMarketplaceAdminFullAccess”](#) をアタッチすることで、プライベートマーケットプレイスを管理するための AWS Identity and Access Management (IAM) アクセス許可を付与します。グループまたはロールを使用することをお勧めします。ポリシーのアタッチについては、「IAM ユーザーガイド」の [「Attaching a policy to a user group」](#) を参照してください。

AWSPrivateMarketplaceAdminFullAccess ポリシーのアクセス許可の詳細については、「[the section called “AWSPrivateMarketplaceAdminFullAccess”](#)」を参照してください。で使用するその他のポリシーについては AWS Marketplace、にサインインし AWS Management Console、[IAM ポリシーページ](#) を参照してください。検索ボックスに「**Marketplace**」と入力して、AWS Marketplaceに関連するすべてのポリシーを検索します。

プライベートマーケットプレイス管理者向けのカスタムポリシーの作成

組織では、各管理者によってタスクのサブセットに限定された複数のプライベートマーケットプレイス管理者を作成できます。AWS Identity and Access Management (IAM) ポリシーを調整して、Catalog のアクション、リソース、および条件キーにリストされている AWS Marketplace Catalog API アクションの条件キーとリソースを指定できます。[AWS Marketplace](#) AWS Marketplace Catalog API 変更タイプとリソースを使用して IAM ポリシーを調整する一般的なメカニズムについては、[AWS Marketplace Catalog API ガイド](#) を参照してください。プライベートで使用できるすべての変更タイプのリストについては AWS Marketplace、「[プライベートマーケットプレイスの使用](#)」を参照してください。

カスタマー管理ポリシーの作成方法については、「[IAM ポリシーの作成](#)」を参照してください。次の例は、プライベートマーケットプレイスから商品を追加または削除することのみが可能な管理者を作成するために使用できるポリシー JSON です。

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "aws-marketplace:AssociateProductsWithPrivateMarketplace",
      "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
      "aws-marketplace:ListPrivateMarketplaceRequests",
      "aws-marketplace:DescribePrivateMarketplaceRequests"
    ],
    "Resource": [
      "*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "aws-marketplace:DescribeEntity",
      "aws-marketplace:ListEntities",
      "aws-marketplace:ListChangeSets",
      "aws-marketplace:DescribeChangeSet",
      "aws-marketplace:CancelChangeSet"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "aws-marketplace:StartChangeSet"
    ],
    "Condition": {
      "StringEquals": {
        "catalog:ChangeType": [
          "AllowProductProcurement",
          "DenyProductProcurement"
        ]
      }
    },
    "Resource": "*"
  }
]
```

ポリシーをプライベートマーケットプレイスのリソースの一部だけを管理するように制限することもできます。次の例は、特定のプライベートマーケットプレイスエクスペリエンスのみを管理できる管理者を作成するために使用できるポリシー JSON です。この例では、Experience 識別子として exp-1234example のリソース文字列を使用しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource": [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/exp-1234example"
      ]
    }
  ]
}
```


エンティティ識別子の取得方法とプライベートマーケットプレイスのリソースセットの表示方法について詳しくは、「[プライベートマーケットプレイスの操作](#)」を参照してください。

ドキュメント履歴

以下の表は、本リリースのAWS Marketplace 購入者ガイドのドキュメントを説明するものです。

このドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

変更	説明	日付
Amazon マシンイメージ (AMI) の年間契約修正オプションを更新	購入者はサブスクリプションを修正して AMI インスタンスタイプを追加または切り替えることができるようになりました。	2024 年 5 月 8 日
AWSMarketplaceImag eBuildFullAccess ポリシーを削除しました	AWS Marketplace はプライベートイメージビルドの配信方法を停止したため、AWSMarketplaceImag eBuildFullAcces ポリシーも廃止されました。	2024 年 5 月 8 日
の新しいデモとプライベート オファ어의オプション AWS Marketplace	AWS Marketplace では、一部の製品の製品詳細ページで デモ および プライベートオファ어 のリクエストオプションがサポートされるようになりました。	2024 年 4 月 1 日
AWS Organizations サポートのポリシーを更新しました	AWS Organizations データの読み取りアクセスを許可するように マネージドポリシーを更新AWSPrivateMarketpl aceAdminFullAccess し ました。	2024 年 2 月 16 日
での製品の新しいサービス にリンクされたロール AWS Marketplace	AWS Marketplace は、Private Marketplace リソースを記述 および更新し、 を記述する	2024 年 2 月 16 日

サービスにリンクされたロールを提供するようになりました AWS Organizations。

[での新しいプライベートマーケットプレイスエクスペリエンス AWS Marketplace](#)

AWS Marketplace は、この統合 AWS Organizations と、プライベートマーケットプレイスエクスペリエンスを管理するための委任管理者の登録機能をサポートするようになりました。

2024 年 2 月 16 日

[での将来の日付の契約の一般提供 AWS Marketplace](#)

すべての SaaS ISVs とチャネルパートナーの将来の日付の契約機能が一般公開されました AWS Marketplace。お客様は、将来の日付の契約を使用して、同じ製品出品で既存の製品を購入した場合に、取引を事前に予約したり、更新を設定したりできるため、運用上の労力を軽減できます。

2024 年 1 月 16 日

[カナダ西部 \(カルガリー\) リージョンでのサポート](#)

AWS Marketplace では、AWS リージョンカナダ西部 (カルガリー) の がサポートされるようになりました。

2023 年 12 月 20 日

[での製品の新しいサービスにリンクされたロール AWS Marketplace](#)

AWS Marketplace は、購入者 AWS Secrets Manager に代わって シークレットとして保存されるデプロイ関連のパラメータを管理するためのサービスにリンクされたロールを提供するようになりました。

2023 年 11 月 29 日

購入者向けの新しいクイック起動デプロイオプション	購入者は、AWS Marketplace での、該当する Software as a Service (SaaS) 製品の設定、展開、および発売に必要な時間、リソース、手順を削減できるようになりました。	2023 年 11 月 29 日
プライベートオファー用の Flexible Payment Schedule が利用可能に	プライベートオファー用の Flexible Payment Schedule (FPS) が AWS Marketplace のすべてのお客様に利用可能になりました。	2023 年 11 月 17 日
Amazon EKS のサードパーティーアドオン	お客様は、Amazon EKS コンソールからサードパーティー製アドオンを AWS Marketplace にリダイレクトされずにサブスクライブできるようになりました。	2023 年 10 月 18 日
Amazon のサポート EventBridge	AWS Marketplace は EventBridge、以前は Amazon CloudWatch Events と呼ばれていた Amazon と統合されました。	2023 年 9 月 6 日
イスラエル (テルアビブ) リージョンのサポート	AWS Marketplace は、AWS リージョンイスラエル (テルアビブ) の をサポートするようになりました。	2023 年 8 月 1 日
AMI 年間契約の発注書サポート	AWS Marketplace は、Amazon マシンイメージ (AMI) 年間契約の発注書機能をサポートするようになりました。	2023 年 6 月 29 日

[AWS Billing コンソールでの発注書の可用性](#)

購入者は AWS Billing 、コンソールですべての発注書を管理し、 out-of-cycle SaaS 契約 PDF 請求書に対応する発注書と簡単に照合できるようになりました。

2023 年 2 月 3 日

[アジアパシフィック \(メルボルン\) リージョンのサポート](#)

AWS Marketplace では、AWS リージョンアジアパシフィック (メルボルン) のがサポートされるようになりました。

2023 年 1 月 24 日

[プライベートオファーページのポリシーを更新しました](#)

[プライベートオファー] ページへのアクセスを許可するようにマネージドポリシー `AWSMarketplaceRead-only` と `AWSMarketplaceManageSubscriptions` を更新しました。

2023 年 1 月 19 日

[プライベートオファーページ](#)

認証された購入者は、AWS Marketplace プライベートオファーページでに拡張 AWS アカウントされたプライベートオファーを表示できるようになりました。

2023 年 1 月 19 日

[購入者へのメール通知が更新されました](#)

プライベートオファーが公開されると購入者に通知されるようになりました。

2022 年 12 月 22 日

[AWS Marketplaceの購入者は、サブスクリプションの SaaS 無料トライアルを利用できるようになりました](#)

購入者は、サブスクリプション SaaS 製品の無料トライアルにサブスクライブできるようになりました。

2022 年 12 月 16 日

[購入者は SaaS プライベート
オファー、アップグレード、
または更新を受け入れること
ができます](#)

販売者が以前の SaaS プライ
ベートオファーをアップグ
レードまたは更新した場合、
購入者は既存の契約をキャン
セルしなくても新しいプライ
ベートオファーを受け入れる
ことができます。

2022 年 12 月 13 日

[AWS Marketplace がプライ
ベートマーケットプレイスエ
クスペリエンスのアーカイブ
をサポート](#)

購入者はプライベートマー
ケットプレイス体験を AWS
Marketplace でアーカイブして
再アクティブ化できるよう
になりました。

2022 年 12 月 12 日

[AWS Marketplace タグベース
の認証機能のポリシーを更新](#)

AWS Marketplace でタグベ
ースの認証をサポートするよ
うに AWSPrivateMarketpl
aceAdminFullAccess
ポリシーを更新しました。

2022 年 12 月 9 日

[サブスクリプションのキャン
セル方法に関する情報を提供
する新しいトピックを追加し
ました](#)

AWS Marketplace で
AMI、ML、SaaS 製品のサブ
スクリプションをキャンセル
する方法についての情報を追
加しました。また、SaaS 契約
の自動更新のキャンセルに関
する情報を追加しました。

2022 年 12 月 8 日

[AWS Marketplace Vendor
Insights で購入者向けのポリ
シーを更新](#)

AWS Marketplace Vendor
Insights 購入者AWSVendor
InsightsAssessorRe
adOnly 向けの 管理ポリ
シーAWSVendorInsightsA
ssessorFullAccess とを
更新しました。

2022 年 11 月 30 日

AWS Marketplace Vendor Insights で購入者のアクセスを制御する	AWS Marketplace Vendor Insights に新しいトピックを追加し、購入者が利用できるアクションとアクセス許可について説明しました。	2022 年 11 月 30 日
アジアパシフィック (ハイデラバード) リージョンのサポート	AWS Marketplace では、AWS リージョンアジアパシフィック (ハイデラバード) のがサポートされるようになりました。	2022 年 11 月 22 日
欧州 (スペイン) リージョンのサポート	AWS Marketplace では、欧州 AWS リージョン (スペイン) のがサポートされるようになりました。	2022 年 11 月 16 日
欧州 (チューリッヒ) リージョンのサポート	AWS Marketplace では、AWS リージョン欧州 (チューリッヒ) のがサポートされるようになりました。	2022 年 11 月 9 日
AWS Marketplace 2022 年 12 月までの IPv6 へのウェブサイトのアップグレード	現在 IAM ポリシーで IPv4 形式のアドレスを使用している購入者は、2022 年 12 月 15 日の前に IAM ポリシーを IPv6 形式のアドレスに更新することをお勧めします。	2022 年 9 月 29 日
AWS Marketplace プライベートマーケットプレイスの詳細なアクセス許可	購入者は、プライベートマーケットプレイスのエクスペリエンスを管理するためのより詳細なアクセス許可を持つようになりました。	2022 年 9 月 8 日

AWS Marketplace Vendor Insights に 2 つのポリシーを追加しました。	Vendor Insights AWSVendor InsightsAssessorReadOnly にソフトウェアリスク評価を提供する機能である 2 AWS Marketplace のポリシーAWSVendorInsightsAssessorFullAccess とを追加しました。	2022 年 7 月 26 日
AWS Marketplace Vendor Insights	AWS Marketplace Vendor Insights は、ソフトウェアリスク評価を提供する機能です。	2022 年 7 月 26 日
支払い方法の更新	AWS 請求コンソールでの支払い方法の変更方法を明確にするためのドキュメントのみの更新。	2022 年 6 月 1 日
契約用の SaaS 無料トライアル	購入者は、SaaS 無料トライアルに登録して、有料トライアルに移行する前に製品を確認できるようになりました。	2022 年 5 月 31 日
AMI、コンテナ、SaaS 製品にベンダー計測タグが追加されました	ベンダーが提供するメトリクス全体で AWS Marketplace のリソースの使用状況を顧客が理解できるようにタグを提供する新機能。	2022 年 5 月 27 日
購入者の取引にメール通知が追加されました	購入者にメールで通知し、AWS Marketplaceで作成される契約書を確認する新機能。	2022 年 5 月 23 日
eProcurement のお客様向けの無料/BYOL 製品の自動承認が有効になりました	eProcurement のお客様向けの無料/BYOL 製品の新しい自動承認により、お客様は製品をすぐに使用できます。	2022 年 5 月 2 日

[AMI およびコンテナ製品契約の購入者の契約変更が可能になりました](#)

AMI およびコンテナ製品契約を変更して、追加のエンタイトルメントを購入したり、サブスクリプションの自動更新オプションを有効にしたりできます。

2022 年 4 月 6 日

[ライセンス使用状況を追跡する機能](#)

購入者は、を使用して AMI および SaaS 製品の使用状況ベースのライセンスメトリクスを追跡できるようになりました AWS License Manager。

2022 年 3 月 28 日

[Helm CLI バージョンへの更新](#)

Helm CLI バージョンが 3.7.0 から 3.7.1 に変更されたことに関してコンテナ製品のドキュメントを更新しました。現時点で互換性のあるバージョンは、このバージョンだけです。

2022 年 3 月 8 日

[既存のマネージドポリシーの更新](#)

不要になったアクセス許可は、次のポリシー、AWSMarketplaceFullAccess と AWSMarketplaceImageBuildFullAccess から削除されました。

2022 年 3 月 4 日

[EMEA に拠点を置く購入者が Amazon Web Services EMEA SARL を通じて製品を購入できます](#)

AWS Marketplace トルコと南アフリカを除く欧州、中東、アフリカ (EMEA) の国と地域に拠点を置く 購入者 AWS アカウント は、EMEA の対象となる販売者からの購入について、Amazon Web Services EMEA SARL を通じて AWS Marketplace 請求書を受け取ることができるようになりました。

2022 年 1 月 7 日

[アジアパシフィック \(ジャカルタ\) リージョンのサポート](#)

AWS Marketplace では、AWS リージョンアジアパシフィック (ジャカルタ) の がサポートされるようになりました。

2021 年 12 月 13 日

[コンテナベースの製品の Helm チャート配送方法](#)

購入者は起動環境に Helm チャートをインストールすることにより、コンテナベースの製品を起動できるようになりました。

2021 年 11 月 29 日

[コンテナベースの製品ドキュメントの全般的な更新と再編成](#)

コンテナベースの製品ドキュメントを更新し、コンテナベースの製品の検出結果、購読、発売に関する情報を増やし、わかりやすくしました。

2021 年 11 月 29 日

[のドキュメントを追加
QuickLaunch](#)

購入者は、Helm チャート配信方法でコンテナベースの製品を起動 QuickLaunch するときに使用できるようになりました。QuickLaunch は、を活用して新しい Amazon EKS クラスター AWS CloudFormation をすばやく作成し、そのクラスターでコンテナベースのアプリケーションを起動 AWS Marketplace するの機能です。

2021 年 11 月 29 日

[AMI ベースの製品およびコンテナベースの製品の契約料金](#)

購入者は AMI ベースの製品またはコンテナベースの製品を前払い価格で購入できるようになりました。

2021 年 11 月 17 日

[SaaS 製品の注文書のサポート](#)

AWS Marketplace では、Software as a Service (SaaS) 契約の購入に発注書番号を追加することができます。

2021 年 10 月 28 日

[SAP Ariba 統合のサポート](#)

AWS Marketplace は、SAP Ariba 調達システムとの統合をサポートしています。

2021 年 10 月 13 日

[AMI エイリアスのサポート](#)

AWS Marketplace は、リージョン間で使用できる AMI IDs エイリアスの使用をサポートしています。

2021 年 9 月 8 日

管理ポリシーから未使用のアクセス許可を削除しました	AWSPrivateMarketplaceAdminFullAccess AWS 管理ポリシーから未使用のアクセス許可が削除されました。	2021 年 8 月 27 日
によるライセンス共有のサポート AWS License Manager	AWS 組織内の他のアカウントと購入した製品にライセンスを共有できます。	2020年12月3日
AWS Marketplace がプロフェッショナルサービスをサポート	AWS Marketplace でプロフェッショナルサービスの購入がサポートされるようになりました。	2020年12月3日
希望通貨のサポート	ご希望の通貨を使用して AWS Marketplace 購入に対してお支払いいただけます。	2020 年 7 月 27 日
プライベートオファ어의アップグレードや更新を確認して承諾できます	販売者は、SaaS 契約製品および従量課金制の SaaS 契約製品のアップグレードや更新のプライベートオファ어를提供する場合があります、これを既存の契約中に確認して承諾できます。	2020 年 5 月 28 日
AWS Marketplace が AWS Data Exchange を通じてデータ製品をサポート	AWS Marketplaceで AWS Data Exchange データ製品にサブスクライブできるようになりました。	2019 年 11 月 13 日
AWS Marketplace が有料の時間単位コンテナをサポート	AWS Marketplace は、Amazon Elastic Kubernetes Service (Amazon EKS) で実行されている有料の時間単位コンテナをサポートするようになりました。	2019 年 9 月 25 日

でのプライベートオファアの更新 AWS Marketplace	さまざまなタイプのプライベートオファアの受け入れに関する詳細を提供するためにコンテンツを更新しました。	2019 年 3 月 29 日
のセキュリティの更新 AWS Marketplace	IAM ポリシー情報を更新し、読みやすくするためにセクションを再構成しました。	2019 年 3 月 25 日
プライベートマーケットプレイス機能に関するコンテンツを追加しました。	プライベートマーケットプレイスのリリースをサポートするコンテンツを追加しました。	2018 年 11 月 27 日
購入者向けユーザーガイドの初回リリース。	AWS Marketplace 購入者ガイドの初回リリース。	2018 年 11 月 16 日

AWS 用語集

最新の AWS 用語については、「AWS の用語集 リファレンス」の[AWS 「用語集」](#)を参照してください。

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。