でバックアップを保護するためのセキュリティのベストプラクティスのトップ 10 AWS

# AWS 規範ガイダンス

# AWS 規範ガイダンス: でバックアップを保護するためのセキュリティのベストプラクティスのトップ 10 AWS

# Table of Contents

# でバックアップを保護するためのセキュリティのベストプラクティスのトップ 10 AWS

Ibukun (IB) Oyewumi (Amazon Web Services (AWS))

2022 年 5 月 (ドキュメント履歴)

セキュリティは、Amazon Web Services (AWS) とお客様の間で責任が共有されます。お客様は、バックアップを保護する方法を求めてきました AWS。セキュリティの慣行 (プラクティス) は、新たに登場したリスクを取り除くために常に進化しているため、リスク評価を定期的に実施し、セキュリティコントロールが適切であるかを見きわめ、複数のコントロール層を導入してデータのリスクを最小限に抑えることが重要になります。

このドキュメントでは、バックアップデータとオペレーションを保護するための上位 10 のセキュリティのベストプラクティスの厳選されたリストについて説明します AWS。AWS Backup サービスを使用した、バックアップデータとオペレーションの保護に焦点をあてていますが、ここで推奨しているセキュリティベストプラクティスは、AWS Marketplace のバックアップツールなど、他のバックアップソリューションと共に使用することが可能です。

# ベストプラクティス

でバックアップを保護する場合は AWS、次の方法を使用することをお勧めします。

トピック



## ステップ 1. バックアップ戦略を実装する

包括的なバックアップ戦略は、セキュリティイベントの発生に起因する影響に耐え、そこから復旧し、影響を最小限に抑えるための、組織のデータ保護計画に欠かせない要素です。バックアップすべきデータ、バックアップの頻度、バックアップと復旧のタスクのモニタリング方法などを規定した、包括的なバックアップ戦略を作成しましょう。

データをバックアップし復元するための包括的な戦略を策定するときは、最初に、起こり得る中断を特定し、それによりビジネスにどのような影響が出る可能性があるかを見きわめるます。

ここでの目標は、許容される目標復旧である目標復旧時間 (RTO) および目標復旧時点 (RPO) までに、ワークロードをバックアップするあるいはダウンタイムを回避する復旧戦略を策定することです。RTO とは、サービスが中断してから復旧するまでに経過した時間 (遅延) の、許容される値のことです。RPO とは、データが最後に復旧した時点を起点とする経過時間の、許容される値のことです。以下のすべてを含む詳細なバックアップ戦略を検討します。

- 継続的なバックアップサイクル
- ポイントインタイムリカバリ (PITR)

- ファイルレベルの復旧
- アプリケーションデータレベルの復旧
- ボリュームレベルの復旧
- インスタンスレベルの復旧

## ランサムウェア

適切に設計されたバックアップ戦略には、ランサムウェアからリソースを保護し復旧するためのアクションが必ず含まれています。これには、アプリケーションやデータの依存関係の詳細な復旧要件も含まれます。例えば、ランサムウェアのリスクを軽減するための予防コントロールと検出コントロールを確立している間は、クロスアカウントAWS リージョン またはクロスアカウントのコピーと復元パターンの適切な詳細レベルも設計して、管理者がセキュリティイベント後に破損したバックアップデータを復元しないようにします。

## 保持要件

業界によっては、バックアップ戦略を策定する際に、データ保持の要件に関する規制も考慮する必要があります。自社のバックアップ戦略が、データの分類レベルやリソースタイプに関する自社の規制ニーズを、十分に満たせる保持要件で設計されていることを確認します。

## コンプライアンス

社内のセキュリティコンプライアンスチームに相談し、バックアップのリソースとオペレーションを会社のコンプライアンスプログラムの範囲に含めるべきか、それとも分離すべきかを確認します。バックアップと復旧を、セキュリティプログラムの重要な要素として組み込めば、データが自社の環境のどこに位置しているのかを理解し、コンプライアンスの範囲を適切に規定することができます。

クラウドで信頼性が高く、安全で、効率的で、費用対効果の高いワークロードを設計および運用するためのアーキテクチャのベストプラクティスについては、「 を使用したバックアップと復旧のアプローチ AWS」および「信頼性の柱 – AWS Well-Architected フレームワーク」を参照してください。

# ステップ 2. バックアップを DR と BCP に組み込む

ディザスタリカバリ (DR) とは、ディザスタ (災害) に備え、対応し、そこから復旧するプロセスのことです。DR プランは回復戦略の重要な要素であり、ディザスタが発生したとき、ワークロードをどのように反応させるか、その方法に関わります。ディザスタには、技術的障害、人の行動、自然災害

などが含まれます。事業継続計画 (BCP) は、予定外の障害が発生したとき、組織が通常の事業活動をどのような方法で継続するのかを概説したものです。

DR プランは会社の BCP に含める必要があります。BCP には AWS Backup 手順も含める必要があります。たとえば、本番データに影響するセキュリティイベントでは、 が別の からのデータのバックアップにフェイルオーバー AWS Backup するために使用する DR プランを呼び出す必要がある場合があります AWS リージョン。災害が発生した場合に組織がサービスの中断をほとんどまたはまったく発生させずに通常の運用を継続できるように、従業員が組織の手順 AWS Backup とともに に精通し、 の使用を実践していることを確認します。の使用の詳細については AWS Backup 、このガイドの他のセクションで説明します。

## ステップ 3. バックアップオペレーションの自動化

組織のバックアッププランとリソースの割り当ては、その組織のデータ保護ポリシーを反映した形で設計する必要があります。バックアップポリシーや組織全体のバックアッププランを自動化してデプロイすれば、バックアップ戦略を標準化してスケールすることができます。AWS Organizations を使用すると、バックアップポリシーを一元的に自動化し、バックアップオペレーションをスケジュールすることで、サポートされている AWS Backup リソースを横断してバックアップアクティビティを実装、設定、管理することができます。

生産性を高め、複数アカウントの環境を横断してインフラストラクチャのオペレーションを管理するために、Infrastructure as Code (IaC) とイベント駆動型アーキテクチャの実装を、デジタルトランスフォーメーションとバックアップ戦略の重要な要素として検討します。バックアップを自動化することには次のような利点があります。

- 時間のかかるバックアップ設定の、手作業によるオーバーヘッドを削減できます。
- エラーが発生するリスクを最小限に抑えられます。
- ドリフトの検出を可視化できます。
- 複数の AWS ワークロードまたはアカウントでバックアップポリシーのコンプライアンスを強化

バックアップポリシーをコードとして実装すると、以下を行ってデータ保護規制を満たすことができます。

- リソースタイプごとに異なる要件を設定する。
- 自社のデータ保護戦略をスケールする。
- ライフサイクルルールを実装して、復旧ポイントが、コールドストレージに移行するか、削除されるまでの時間を指定する。これにより、コストを最適化できます。

バックアップオペレーションを自動化する場合、 AWS タグとリソース IDs を使用して、ビジネスクリティカルなアプリケーションのデータを保存する AWS リソースを自動的に識別し、イミュータブルバックアップを使用してデータを保護することで、リソース割り当てオプションをスケールできます。この方法を使えば、アクセス許可や、バックアッププランまたはバックアップポリシーなどのセキュリティコントロールを優先付けすることができます。

## ステップ 4. アクセスコントロールのメカニズムを実装する

クラウドのセキュリティについて考える上で基本的な戦略となるのは、ユーザーが適切なアクセス許可を使ってデータにアクセスできる、堅牢な ID 基盤です。適切な認証と認可が行われていれば、セキュリティイベントが発生するリスクを抑えられます。責任共有モデルでは、 AWS お客様はアクセスコントロールポリシーを実装する必要があります。アクセスポリシーを大規模に作成して管理するときは、 AWS Identity and Access Management (IAM) を使用します。

アクセスの権限と許可を設定するときは、バックアップデータまたはバックアップボールトにアクセスする各ユーザーまたはシステムに、それぞれの役割を果たすための必要最小限のアクセス許可のみを付与する、最小特権の原則を適用します。 AWS Backup を使用してバックアップボールトにアクセスポリシーを設定し、クラウドワークロードを保護します。

例えば、アクセスコントロールポリシーを実装すると、復旧ポイントを削除する機能を制限したまま、バックアッププランとオンデマンドのバックアップを作成するためのアクセスをユーザーに許可することができます。ボールトアクセスポリシーを使用すると、ビジネスニーズに応じて、送信先バックアップボールトをソース AWS アカウント または IAM ロールと共有できます。また、アクセスポリシーを使用すると、バックアップボールトを 1 つまたは複数のアカウントと、もしくは AWS Organizationsの組織全体と、共有することができます。詳細については、AWS Backup のドキュメントを参照してください。

ワークロードをスケールしたり、 に移行するときに AWS、バックアップボールトとオペレーションへのアクセス許可を一元管理する必要がある場合があります。組織のすべてのアカウントで使用できる最大数のアクセス許可を、一元的に制御するときは、サービスコントロールポリシー (SCP) を使用します。SCP は多重防御を備えており、ユーザーをアクセスコントロールの規定されたガイドライン内に留めておくことができます。詳細については、「Managing access to backups using service control policies with AWS Backup」を参照してください。

バックアップリソースやデータへの意図しないアクセスなどのセキュリティリスクを軽減するには、IAM Access Analyzer を使用して、以下と共有されている IAM AWS Backup ロールを特定します。

- などの外部エンティティ AWS アカウント

- ルートユーザー
- IAM ユーザーまたはロール
- フェデレーションユーザー
- AWS のサービス
- 匿名ユーザー
- フィルタの作成に使用できるその他エンティティ

## ステップ 5. バックアップデータとボールトの暗号化

多くの組織で、データセキュリティ戦略を改善する必要性がますます高まってきています。こうした組織は、クラウドでスケールするときに、データ保護規制の順守を求められる場合があります。暗号化を適切に実装すれば、基本のアクセスコントロールのメカニズムに、もう一段階保護を追加することができます。さらに保護を追加すれば、基本のアクセスコントロールポリシーが万が一失敗した場合でも、その影響を軽減することができます。

例えば、 AWS Backup データに設定しているアクセスコントロールポリシーがそれほど厳格ではない場合、キーの管理システムまたはプロセスを追加すると、セキュリティイベントの最大レベルの影響を軽減することができます。これは、データおよび暗号化キーにアクセスするための認可メカニズムがそれぞれ分離していることによるものです。つまり、バックアップデータは暗号文としてしか表示されません。

AWS クラウド 暗号化を最大限に活用するには、転送中と保管中の両方のデータを暗号化します。転送中のデータを保護するために、 は公開された API コール AWS を使用して、TLS プロトコルを使用してネットワーク AWS Backup 経由で にアクセスし、ユーザー、アプリケーション、および AWS Backup サービス間の暗号化を提供します。保管中のデータを保護するには、 AWS クラウドネイティブ AWS Key Management Service (AWS KMS) または を使用できますAWS CloudHSM。クラウドベースのハードウェアセキュリティモデル (HSM) である AWS CloudHSM は、業界で採用されているデータ暗号化のための強力なアルゴリズム、AES256 (Advanced Encryption Standard のうち 256 ビットの暗号鍵を用いる方式) を使用しています。クラウドデータとバックアップボールトを暗号化するには、自社のデータガバナンスと規制要件を評価して、適切な暗号化サービスを選択します。

暗号化の構成は、リソースのタイプや、アカウント間またはリージョン間のバックアップオペレーションに応じて異なります。特定のリソースタイプでは、ソースリソースの暗号化に使用したキーとは別の暗号化キーでバックアップを暗号化する機能がサポートされています。アクセスコントロールを管理し、 AWS Backup データまたはボールト暗号化キーにアクセスできるユーザーとその条件を決定する責任はユーザーにあるため、 AWS KMS が提供するポリシー言語を使用してキーに対する

アクセスコントロールを定義します。また、バックアップが適切に暗号化されていることを確認するときは AWS Backup Audit Manager も使用できます。詳細については、「Encryption for backups in AWS Backup」を参照してください。

あるリージョンのキーを別のリージョンに複製するときは、AWS KMS のマルチリージョンキーを使用します。マルチリージョンキーは、ディザスタリカバリのため、暗号化されたデータを別のリージョンにコピーする必要があるときに、暗号化の管理を簡素化できるように設計されています。全体的なバックアップ戦略の一環として、マルチリージョン AWS KMS キーを実装する必要があるかどうかを評価します。

## ステップ 6. イミュータブルストレージを使用してバックアップを保護する

イミュータブル (不変) ストレージを使用すると、WORM (Write Once, Read Many) の状態でデータを書き込むことができるようになります。WORM の状態であれば、データを一度書き込めば、記録媒体にコミットした後または書き込まれた後に、必要なだけ何度でも読み取って使用することができます。イミュータブルストレージを使用すると、データの整合性を確実に維持することができます。また、以下からデータを保護することにもつながります。

- 削除
- 上書き
- 不注意によるアクセスや不正なアクセス
- ランサムウェアによるセキュリティ侵害

イミュータブルストレージには、企業活動に影響を及ぼす潜在的なセキュリティイベントに対処するための、効率的なメカニズムが用意されています。

イミュータブルストレージを強固な SCP 制限と組み合わせて使用すれば、ガバナンスをさらに強化できます。また、法令 (リーガルホールドなど) によりイミュータブルデータの利用が要請されている場合は、法令に順守した WORM モードで使用することも可能です。

データの可用性と整合性とを維持するには、AWS Backup ボールトロックを使用してバックアップを保護します。 AWS Backup ボールトロックを使用すると、権限のないエンティティは、必要な保持期間中に顧客またはビジネスデータを消去、変更、または破損することはできません。 AWS Backup ボールトロックは、以下を防ぐことで組織のデータ保護ポリシーを満たすのに役立ちます。

- 特権ユーザー ( AWS アカウント ルートユーザーを含む) による削除

- バックアップのライフサイクル設定の変更
- 規定の保持期間を変更する更新

AWS Backup ボールトロックはイミュータビリティを確保し、バックアップボールトのバックアップ (復旧ポイント) を保護する保護レイヤーを追加します。これは、バックアップとアーカイブの整合性のニーズが厳しい規制の厳しい業界で特に役立ちます。 AWS Backup ボールトロックは、意図しないアクションや悪意のあるアクションが発生した場合に、 から復旧するためのバックアップとともにデータが保持されるようにします。

> **Important**
>
> - AWS Backup ボールトロックは、規制 17 C.F.R. 1.31 (b)-(c) の証券取引委員会 (SEC) ルール 17a-4 (f) および商品取引委員会 (CFTC) への準拠についてまだ評価されていません。
> - AWS Backup ボールトロックはすぐに有効になります。ボールトを恒久的にロックする前に、その設定を削除または更新するため最低 3 日間 (72 時間) のクーリングオフ期間が与えられます。オプションで、このクーリングオフの期間を延長することができます。このクーリングオフ期間を使用して、ワークロードとユースケースに対して AWS Backup ボールトロックをテストします。クーリングオフ期間が終了すると、ボール AWS サポート AWS Backup トロックやロックされたボールトの内容を削除したり変更したりすることはできません。詳細については、「AWS Backup Vault Lock」のドキュメントを参照してください。

## ステップ 7. バックアップのモニタリングとアラートを実装する

バックアップジョブは失敗することがあります。バックアップ、復元、コピータスクなどのジョブが失敗すると、同じプロセス内の後続のステップに影響する恐れがあります。最初のバックアップジョブが失敗すると、後続のその他タスクも失敗する可能性が高くなります。こうしたシナリオでは、モニタリングと通知を使用すれば、一連のイベントを詳細に理解することができます。モニタリングとアラートを使用すると、組織内でバックアップジョブに対する認識を高めることができ、バックアップの失敗に対応できるようになります。

AWS Backup ジョブのモニタリングを有効にし、通知を設定すると、以下のような利点が得られます。

- バックアップのアクティビティに対する認識が向上する。

- 重要なサービスレベルアグリーメント (SLA) を満たすことができる。
- 通常業務のモニタリングを強化できる。
- コンプライアンスの義務を満たすことができる。

AWS Backup 他の AWS のサービス およびチケット発行システムと統合することで、ワークロードのバックアップモニタリングを実装し、自動化された調査およびエスカレーションフローを実行できます。例えば、次のオペレーションを実行できます。

- Amazon CloudWatch を使用して、メトリクスの追跡、アラームの作成、ダッシュボードの表示を行う。
- Amazon EventBridge を使用して、 AWS Backup のプロセスとイベントをモニタリングする。
- AWS CloudTrail を使用して、AWS Backup API 呼び出しを、時間、送信元 IP、ユーザー、呼び出しを行っているアカウントなどの詳細と共にモニタリングする。
- Amazon Simple Notification Service (Amazon SNS) を使用して、バックアップ、復元、コピーイベントなどの AWS Backup 関連トピックをサブスクライブします。

AWS Backup Audit Manager を使用して、各アカウントとリージョンの日次バックアップ監査レポートの証拠を自動的に生成できます。また、一連の自動化テンプレートとダッシュボード (バックアップオブザーバーソリューションと呼ばれる) を使用して、毎日集計されたクロスアカウントマルチリージョン AWS Backup レポートを取得することで、バックアップモニタリングを複数のアカウントにスケールすることもできます。

## ステップ 8. バックアップ設定を監査する

バックアッププログラムが正常に動作していること、およびバックアッププロセスからの異常を特定して修正するには、定義されたバックアップ頻度などの定義されたコントロールに対する AWS Backup ポリシーのコンプライアンスを監査します。ビジネス要件を順守していないバックアップオペレーションやリソースを特定して調査するには、バックアップアクティビティを継続的かつ自動的に追跡し、自動レポートを生成します。

AWS Backup Audit Manager には、ビジネスコンプライアンスと規制要件に沿ったカスタマイズ可能なコンプライアンスコントロールが組み込まれています。組み込みの、カスタマイズ可能なコントロールを監査フレームワークとして使用することで、 AWS Backup の慣行を評価できます。このコントロールには以下が含まれます。

- バックアッププランで保護されているバックアップリソース

- Backup プランの最小頻度および最小保存期間
- Backup 復旧ポイント暗号化
- バックアップのリカバリポイントの手動による削除
- Backup リカバリポイントの最小保存期間
- リージョン間の COPY
- アカウント間のコピー
- バックアップボールトロック

Infrastructure as Code (IaC) オートメーションでは、 で AWS Backup Audit Manager を使用できます AWS CloudFormation。

AWS Security Hub CSPM では、 のセキュリティ状態を包括的に把握できます AWS。また、AWS Foundational Security Best Practices のコントロール など、セキュリティのベストプラクティスや業界標準に照らして、使用している環境をチェックするのにも役立ちます。クラウド環境で Security Hub CSPM を使用する場合は、バックアップの保護に役立つ検出コントロールが含まれているため、 AWS Foundational Security Best Practices 標準を有効にすることをお勧めします AWS。 AWS Backup Audit Manager と Security Hub CSPM の検出コントロールのほとんどは、AWS Config マネージドルールとしても利用できます。

## ステップ 9. データ復旧機能のテスト

バックアップ戦略にはバックアップのテストが含まれていなければなりません。バックアップしたデータを復元できなければ、そのバックアップ戦略は有効ではありません。特定の復旧ポイントを検出して復元する機能を、定期的にテストしましょう。

は保護するリソースから復旧ポイントにタグ AWS Backup を自動的にコピーしますが、タグはデフォルトでは復旧ポイントから対応する復元されたリソースにコピーされません。インベントリ管理をスケールして復旧ポイントを見つけるには、 AWS Backup イベントを使用して、 AWS Backup 復元ジョブによって作成されたリソースでタグレプリケーションプロセスを開始することを検討してください。

データ復旧のワークフローは、データ復旧のパターンを作成することから開始し、これを定期的にテストします。バックアップデータを復元できる確実性を高めるため、データ復旧テストを継続的に実行するための基本的かつ反復可能なプロセスを作成します。例えば、顧客が管理する AWS KMS キーを使って暗号化された、中央の DR バックアップボールトから、顧客が管理する別の AWS KMS

キーを使って暗号化された、ソースアカウントのバックアップボールトへの、クロスアカウント、クロスリージョンの復元オペレーションをテストするパターンなどを作成できます。

このような復元オペレーションを頻繁にテストしない場合、クロスアカウント、クロスリージョンオペレーションの AWS KMS 暗号化に関する前提が正しくない可能性があります。実際に有効な、唯一のバックアップの復元パターンが、頻繁にテストしている経路であるということはよくあります。サポートされているバックアップリソースのタイプを定期的にテストすれば、将来の障害や重要データの損失につながる可能性のある兆候を早期に特定できます。可能であれば、ストレージスペースの浪費を防ぎ、コストを最適化し、時間を節約するために、少数の、しかし現実的な数の復旧経路とパターンを確保しておきます。復旧テストが失敗したときに問題を修正することは、貴重なデータや重要データを失うことに比べれば、はるかに解決が容易です。

## ステップ 10。バックアップをインシデント対応計画に組み込む

セキュリティインシデント対応シミュレーション (SIRS) とは、現実的なシナリオの中でインシデント対応計画と手順とを実行できる、体系的な機会を提供する社内イベントです。クリエイティブな SIRS アクティビティでバックアップデータとオペレーションをテストし、予期せぬ事態に備えて自らをテストできる貴重な機会です。ここでは、組織の準備状況を確認し、滅多に起きない、予期せぬ事態の感覚をつかむことができます。シミュレーションは現実に即したものでなければなりません。また、イベントの発生時に対応を求められる機能横断的な組織チームに、参加する必要があります。

基本のシミュレーション演習から始めて、内容が満載の、複雑なイベントへと進みます。例えば、仮想プライベートクラウド (VPC) と、関連リソースから構成され、不注意による大量の情報漏洩や、ポリシーやアクセスコントロールリストの変更によるデータ侵害の可能性をシミュレートする、現実的なモデルを構築したりします。インシデント対応計画がどの程度有効であるかを評価するために、学んだ教訓を記録して、将来の対応手順に組み込むべき改善点を特定します。

を使用して AWS Backup 、自動インスタンスレベルのバックアップを Amazon マシンイメージ (AMIs) として、ボリュームレベルのバックアップを複数のスナップショットとして設定できます AWS アカウント。これにより、インシデント対応チームは、ランサムウェアなどの潜在的なセキュリティイベントの範囲と影響とを軽減できる復元ポイントを特定し、フォレンジックディスクの自動収集のようなフォレンジックプロセスを強化することができます。

# 次のステップ

このガイドでは、バックアップデータを保護するためのセキュリティのベストプラクティスとコントロールのトップ 10 について説明しました AWS。ビジネスニーズに合わせてスケールでき、ニーズを達成することのできる、複数の管理段階を備えたバックアップと復旧のための戦略およびアーキテクチャを設計し実装する際は、これらのベストプラクティスを活用することが推奨されます。詳細については AWS Backup、 AWS Backup ドキュメントを参照してください。

本ガイドに関してご質問のある方は、AWS Backup のフォーラムに新しいスレッドを作成するか、AWS サポート までお問い合わせください。

# リソース

## AWS 規範ガイダンス

- Backup and recovery approaches on AWS (ガイド)

## AWS ドキュメント

- AWS Backup
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon EventBridge
- IAM
- AWS KMS
- AWS Organizations
- AWS Security Hub CSPM
- Amazon SNS

## ブログ記事

- AWS のサービス を使用して、 全体の大規模な集中バックアップを自動化する AWS Backup
- ディザスタリカバリ (DR) アーキテクチャ AWS、パート I: クラウドでのリカバリの戦略
- 暗号化の重要性と AWS が役立つ方法
- AWS Backup ボールトロックを使用してバックアップのセキュリティ体制を強化する
- AWS Backup Audit Manager によるバックアップコンプライアンスのモニタリング、評価、デモンストレーション
- を使用して、アカウントとリージョン間で暗号化されたバックアップを作成して共有する AWS Backup

- AWS Backup Audit Manager を使用してデータ保護ポリシーの監査を簡素化する
- でサービスコントロールポリシーを使用してバックアップへのアクセスを管理する AWS Backup
- 集計された毎日のクロスアカウントマルチリージョン AWS Backup レポートを取得する

## GitHub リポジトリ

次のコードリポジトリは、複数のアカウントと にまたがる AWS Backup AWS Organizations 組織全体で を使用してバックアップとリカバリを実装するための管理およびデプロイソリューションを提供します AWS リージョン。

- AWS Backup を使用して を実装する AWS
- CI/CD Pipelines AWS Backup を使用して実装する

# ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 初版発行 | — | 2022 年 5 月 13 日 |