AWS SECURITY

AWS クラウド環境をランサムウェアから保護する

目次

ランサムウェア : 恐るべき脅威 3

セキュリティを念頭に構築された AWS 6

ランサムウェアに攻撃される前に : ネットワークの要塞化と保護 8

インシデント発生時 : 早期検知と自動対応 14

ランサムウェアからの復旧 : 根本原因と教訓 17

まとめ 19

リソース 19

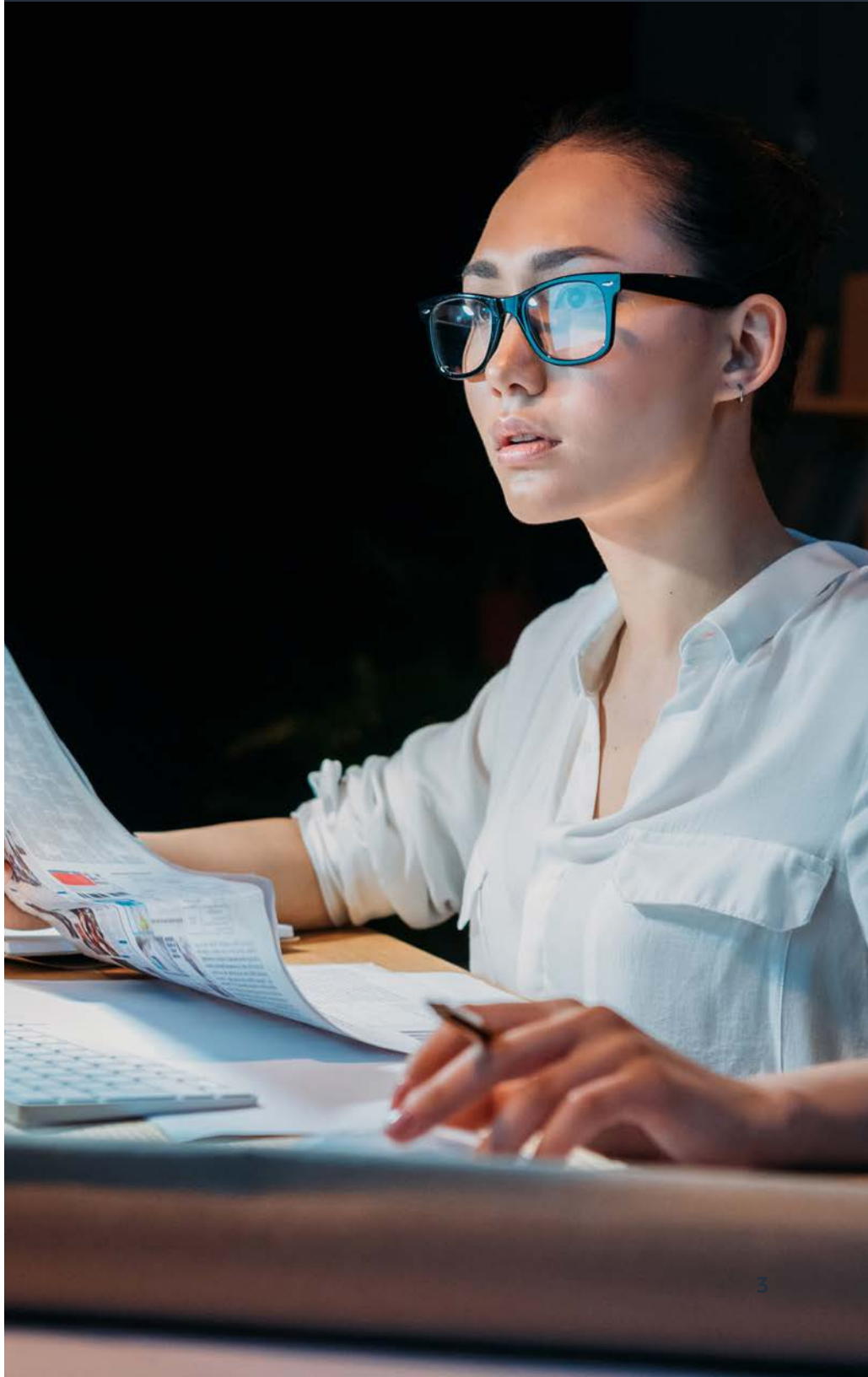
注記

ランサムウェア：恐るべき脅威

ランサムウェアは、1989 年に PC Cyborg という最初のランサムウェア攻撃が記録されて以来、漫画の題材となるような危険性を持つ突出したサイバー脅威として世界的に注目され続けています (CryptoLocker [2014]、Petya [2016]、WannaCry [2017]、NotPetya [2017]、Ryuk [2019])。

ランサムウェア攻撃は**政府、非営利団体、企業に何十億ドルもの負担を強い**、業務を中断させます。海運業の大企業 Maersk は、NotPetya の攻撃で、「深刻な事業の中断」が発生したため 3 億 USD をかけ 4,000 台のサーバーと 45,000 台の PC の再インストールを余儀なくされました。バルチモア市に対するランサムウェア攻撃では 1,800 万 USD を超える被害が発生しました。フロリダ州のリビエラビーチおよびレイクシティの地方行政機関は、システムとデータを取り戻そうと、総額 100 万 USD をハッカーに支払いました。

未報告のインシデントや攻撃が阻止した件数は未知数であるため、ランサムウェア攻撃の頻度を推定することは困難ですが、米国連邦捜査局 (FBI) は、この脅威が、あまり遠くない未来に、**より対象を絞り、洗練され、被害額が大きい**ものになると予想しています。このような警告は米国外にも広がっており、Europol もまた、ランサムウェアを「**サイバー攻撃の中で最も広く使用され、最も金銭的ダメージが大きい形態**」と呼んでいます。



ランサムウェアとは？

ランサムウェアは、システムやデータへのアクセスを不正に取得し、そのデータを暗号化して正当なユーザーによるアクセスをブロックするように、サイバー犯罪者によって設計された悪意のあるコードです。ランサムウェアがユーザーをシステムから締め出し、機密データを暗号化すると、サイバー犯罪者は、ブロックされたシステムを解除しデータを復号する復号キーと引き換えに、身代金を要求します。建て前では、期限内に身代金が支払われた場合、システムとデータは復号されて再度利用できるようになり、通常の業務を継続できます。ただし、身代金が不十分だった場合、組織は攻撃者の思うがままに、データを完全に破壊される、公共の場へデータを漏えいされるなどのリスクにさらされることになります。

ランサムウェアは無差別

ほとんどのランサムウェアは、その特性上、手当たり次第に攻撃します。つまり、人やマシンベクターを介してアクセス可能なネットワークを無差別に荒らします。業界や地理的位置は関係ありません。ランサムウェアの事例は、事実上、世界中のあらゆる業界で発生しています。しかしながら、不正行為者の間では、侵入に成功する確率が高く、身代金の支払いに応じる可能性が高い特定の業界をターゲットにする傾向が強まっています。教育機関、州や地方の行政機関、ヘルスケア組織のセキュリティチームは、**ランサムウェア攻撃の増加から**自分たちのデータを安全に保つ手段を強化しています。

不正行為者は、業種の弱点を特定する方法を把握しています。例えば、教育機関や行政機関の多くは、予算の縮小、セキュリティリソースにおける認識のずれ、脆弱性にパッチが適用されていないレガシー IT システムが組み合わさり、攻撃に対して脆弱になっています。同様にランサムウェアは、支払いに応じる可能性が高くなることを狙って、病院のようにダウンタイムを許容できない業界をターゲットにすることもあります。

ビットコインは人気の暗号通貨ですが、監督する統治機関もなく取引は匿名で行われるため、身代金の支払いに理想的な手段となっています。

なぜランサムウェアが効果的なのか？

- 従業員の間でセキュリティの認識が低い
- 組織がデータをバックアップしていない
- 攻撃にはほとんどスキルが必要ないが、多額の金銭を獲得できる
- 重大な脆弱性 (Common Vulnerabilities and Exposures) に組織がパッチを適用するのに数週間かかる
- 多忙な技術スタッフはすべてのセキュリティ上のギャップを対処または予想できない
- 1 つの攻撃で複数のベクターまたはチャネルが使用されている

支払うべきか支払わざるべきか？

身代金を支払うか拒否するかの判断については、サイバーセキュリティの専門家たちの間で活発に議論が交わされています。FBI を含む多くの専門家は、**組織には身代金を支払わないようアドバイス**しています。支払いに応じても、ロックされたシステムやデータが再び使用できるようになる保証はなく、サイバー犯罪者が悪質な犯罪行為を続ける動機付けにしかならないという主張です。

身代金を支払った後のシステムやデータに対するアクセスが保証されないとしても、いち早く通常の業務を再開できることを願い、リスクを承知で支払う組織もあります。そうすることで、生産性のロスや時間に伴う収益の減少、機密データ[1] の露出、風評被害など、攻撃に付随する潜在的なコストが軽減されることを望んでいるのです。

ランサムウェアの脅威は深刻ですが、賢く備えて継続的に警戒すれば、ランサムウェアに効果的に対抗できます。データセキュリティの完全防御には、人的要素と技術的要素の両方が含まれますが、AWS クラウドの機能はランサムウェア攻撃を軽減するのに役立ちます。

AWS は、高可用性、優れたセキュリティ、高レジリエンスを備え、インターネットでの不正行為者に対抗できるツール、ベストプラクティス、サービスを提供することをお約束します。

[1] 個人を特定できる情報 (PII) および保護対象医療情報 (PHI) を含む。

サイバー犯罪者がランサムウェアで利益を得る方法を見つけ続ける限り、多くの組織のリーダーはこう言います。

「攻撃されるかどうかではなく、いつ攻撃されるかが問題である」

セキュリティを念頭に構築された AWS

AWS は、さまざまなユースケースを持つ多種多様な業界を代表する、数百万のアクティブなお客様を世界中で保護しています。これには、大企業、スタートアップ企業、教育機関、政府組織などが含まれます。このようなお客様のさまざまな規模やグローバル展開により、AWS はクラウドのセキュリティに関する広い視野と深い視点を得ることができ、それらを迅速に AWS のインフラストラクチャやサービスに再投資しています。AWS におけるセキュリティは、中核となるインフラストラクチャから始まります。このインフラストラクチャは、クラウド向けに特別に構築され、かつ世界で最も厳しいセキュリティおよび規制要件を満たすように設計されています。

IT インフラストラクチャの物理的、環境的、およびセキュリティの統制を継承する

AWS クラウドに移行する前のお客様は、お客様がセキュリティコンプライアンスおよび監査プログラムに規定された統制全体の責任を負っていたかもしれません。AWS に移行すると、AWS コンプライアンスプログラムから統制を継承できます。これにより、クラウドに置いたワークロードやデータの保護に集中できます。AWS では、ホストオペレーティングシステムおよび仮想化レイヤーからサービスが運用されている施設の物理的なセキュリティに至るまでの要素を、AWS が運用、管理、および制御するため、お客様の運用上の負担を軽減できます。

AWS でのシステムやデータの保護は責任共有

お客様が AWS クラウドにシステムをデプロイする際、AWS はセキュリティに関する責任をお客様と共有することで支援します。AWS は安全な設計原則を使用して基盤となるクラウドインフラストラクチャを設計し、お客様は AWS にデプロイするワークロードに独自のセキュリティアーキテクチャを実装できます。

AWS は、AWS クラウドで提供されるすべてのサービスを実行するインフラストラクチャの保護について責任を負います。このインフラストラクチャは、AWS クラウドサービスを実行するハードウェア、ソフトウェア、ネットワーク、および施設で構成されています。

お客様の責任は、選択した AWS クラウドのサービスに応じて異なります。これにより、お客様がセキュリティの責任の一部として実行する必要がある設定作業の量が決まります。お客様は、データの管理 (暗号化オプションを含む)、アセットの分類、および AWS Identity and Access Management (IAM) を使用した適切なアクセス許可の適用について責任を負います。

お客様

クラウド「における」セキュリティに対する責任

- お客様のデータ
- プラットフォーム、アプリケーション、アイデンティティとアクセスの管理
- オペレーティングシステム、ネットワーク、ファイアウォール構成
- クライアント側のデータ暗号化とデータ整合性認証
- ネットワークトラフィックの保護 (暗号化、整合性、アイデンティティ)
- サーバー側の暗号化 (ファイルシステムやデータ)

AWS

クラウド「の」セキュリティに対する責任

- ソフトウェア
- コンピューティング　ストレージ
  データベース　ネットワーキング
- ハードウェア/AWS グローバルインフラストラクチャ
- リージョン　アベイラビリティーゾーン
  エッジロケーション

ランサムウェアに攻撃される前

ネットワークの要塞化と保護

セキュリティフレームワークを採用する

米国国立標準技術研究所 (NIST) サイバーセキュリティフレームワーク (CSF) のようなセキュリティフレームワークを実装することで、組織のサイバーセキュリティのリスクの管理と削減における標準を設定できます。これは自発的、リスクベース、結果重視のフレームワークであり、5 つの機能 (識別、防御、検知、対応、復旧) を中心としたセキュリティ活動の基盤を築き、セキュリティ、リスク管理、組織のレジリエンスを向上できるように設計されています。

CSF は本来、重要なインフラストラクチャ分野向けのものでしたが、業種や規模を問わずあらゆる組織で推奨される指針として、世界中の政府機関や産業界から支持されています。ヘルスケア、金融サービス、製造業などさまざまな分野で NIST CSF が使用されており、世界的には日本、イスラエル、英国、ウルグアイなどがいち早く採用しています。

フレームワークに準拠する

ガイド「**NIST Cybersecurity Framework (CSF): Aligning to the NIST CSF in the AWS Cloud**」(NIST サイバーセキュリティフレームワーク (CSF): AWS クラウドにおける NIST CSF への準拠) は、世界中のあらゆる規模の民間企業や公的機関が、AWS のサービスやリソースを使用して CSF へ準拠できるように作られています。

安全でコンプライアンスに準拠した AWS インフラストラクチャをデプロイする

NIST の National Cybersecurity Center of Excellence (NCCoE) は、ランサムウェアや他の破壊的なイベントによって引き起こされるデータの整合性に関する課題に対処するために、組織がどのようにセキュリティコントロールを開発、実装するべきかを示すプラクティスガイドを発行しています。これらの詳細について、またその他の予防的セキュリティ機能および手段については、AWS のホワイトペーパー「**Ransomware Risk Management on AWS Using the NIST Cyber Security Framework (CSF)**」(NIST サイバーセキュリティフレームワーク (CSF) を使用した AWS でのランサムウェアリスク管理) をご覧ください。

NIST サイバーセキュリティフレームワーク

識別

- 資産管理
- ビジネス環境
- ガバナンス
- リスク評価
- リスク評価戦略
- サプライチェーンリスク管理

保護

- アクセス制御
- 意識向上およびトレーニング
- データセキュリティ
- 情報を保護するためのプロセスおよび手順
- 保守
- 保護技術

検知

- 異常とイベント
- セキュリティの継続的なモニタリング
- 検知プロセス

対応

- 対応計画
- コミュニケーション
- 低減
- 改善

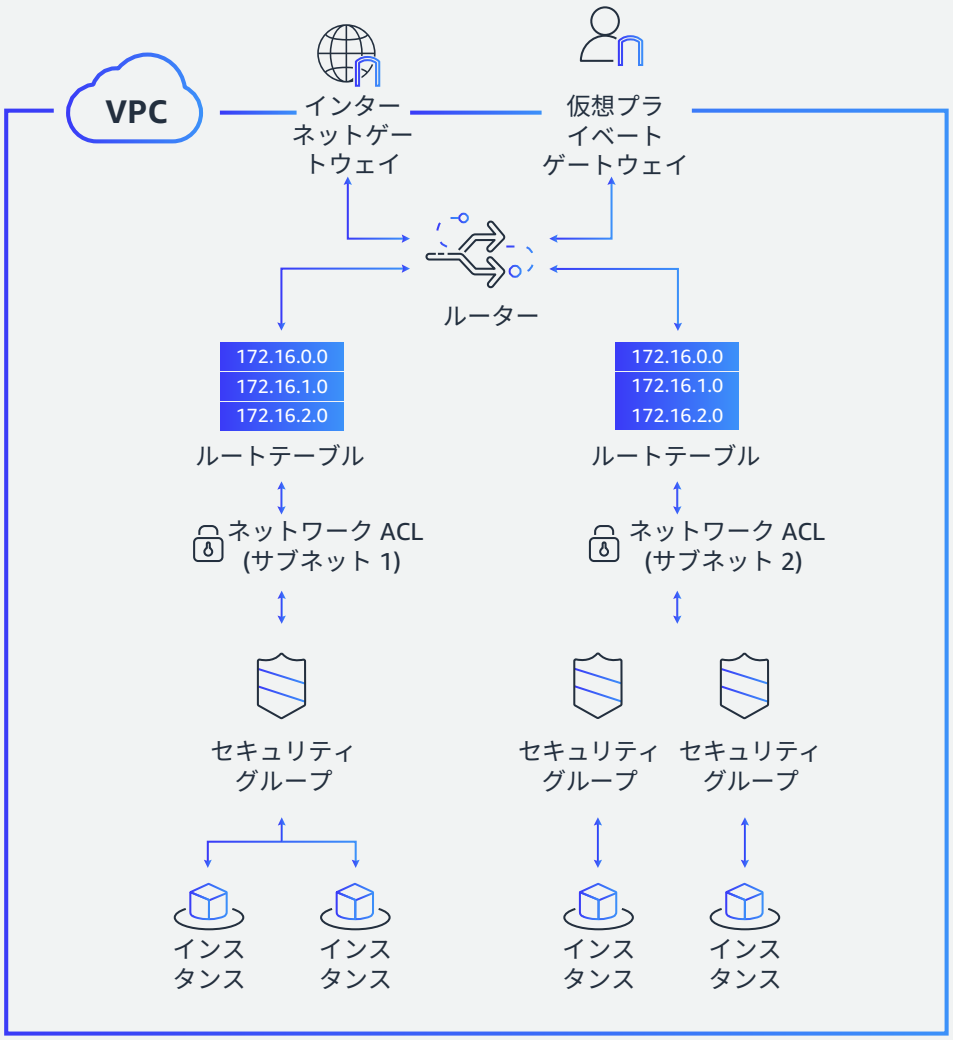
復旧

- 復旧計画
- 改善
- コミュニケーション

Amazon Virtual Private Cloud (VPC) をセグメント化する

ネットワークのセグメント化により、ローカルトラフィックの輻輳が軽減されます。また、ユーザー固有のリソースのみを割り当てることでセキュリティを向上できます。これにより、攻撃者がネットワーク内を横方向に移動する手段を大幅に減らすことができます。

AWS クラウドの一部を論理的に隔離してプロビジョニングできます。ここでは、お客様が定義する仮想ネットワーク内で AWS リソースを起動できます。Amazon VPC は、セキュリティグループやネットワークアクセスコントロールリスト (ACL) を使って、隔離したコンポーネントにセグメント化することで、必要なトラフィックのみを許可し、無差別に拡散するというランサムウェアの能力を AWS 環境全体で低減させることができます。



重要なシステムやデータへのユーザーのアクセスを管理する

個別のユーザーやユーザーのグループが使用できるシステムやデータ、またそのデータにアクセスできる条件を決定する強力な IAM ポリシーを設定することで、ランサムウェアがアクセスできる環境の範囲を制限できます。

ユーザーレベルでは、AWS では、ユーザーやロールがアクセスできる特定のシステムやデータを定義することで、きめ細かいアクセスコントロールの条件を定義できます。これらのコントロールは、AWS の特定のリソースで実行できるアクションを決定するもので、業務上の必要性や職務上の責務に応じて、「知る必要性」をベースにユーザーへ権限を与えます。

AWS IAM を使用すると、AWS のサービスとリソースへのアクセスを安全に管理できます。また、AWS のユーザーとグループを作成および管理し、アクセス権により AWS リソースへのアクセス許可や拒否ができます。

AWS では、社内外のネットワークユーザーに対しては、最小特権の原則に従うことをベストプラクティスとして推奨しています。例えば、ランサムウェアの中には、システム管理者のアカウントを使用してオペレーションを実行するように設計されているものがあります。このタイプのランサムウェアに対しては、ユーザーアカウントの特権を減らし、デフォルトのシステム管理者アカウントをすべて停止することで、セキュリティ上の防壁を追加できます。

データのバックアップと復旧計画を定義、テスト、実行する

ランサムウェアが組織に与え得る影響を軽減するために、バックアップは極めて重要です。ランサムウェアに対する最も効果的な抑止対策は、定期的なバックアップとシステムの検証です。データのバックアップと復旧の戦略を明確にし、バックアップに保存されたデータを本稼働環境ですぐに使用できるように備えておくことで、ランサムウェアの攻撃によるデータの削除や破壊から防御することができます。定義したバックアップと復旧計画をゲームデーのシナリオで定期的にテストすることで、対応を改善し、方法が効果的であることを確認できます。

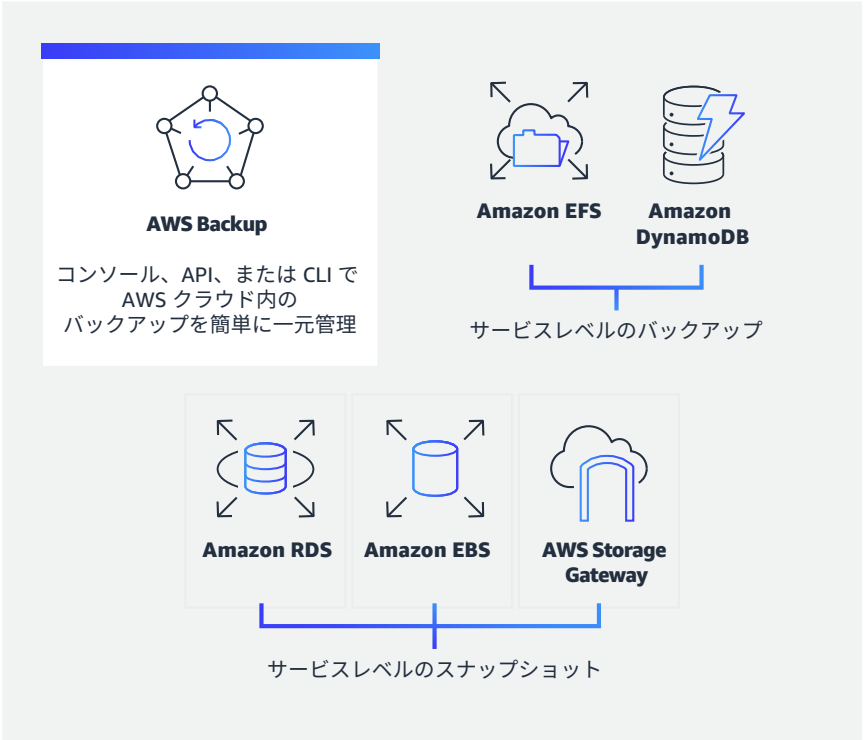
お客様は、**AWS Backup** や **CloudEndure Disaster Recovery** などのサービスを使用して、可用性が高く回復力のあるアプリケーションを構築およびデプロイできます。AWS Backup を使用すると、Amazon Elastic Block Store (Amazon EBS) ボリューム、Amazon Relational Database Service (Amazon RDS) データベース、Amazon DynamoDB テーブル、Amazon Elastic File System (Amazon EFS)、AWS Storage Gateway ボリュームなどの AWS リソースのバックアップアクティビティを監視し、バックアップポリシーを一元的に構成できます。ランサムウェアの攻撃を受けた場合、CloudEndure Disaster Recovery によって数クリックで最新バージョンのマシンがスピンアップされ、システムを復旧し、ユーザーが再びデータを利用できるようにします。

データバックアップの保存における考慮事項

ある時点のデータのバックアップと本稼働環境への迅速な復元を効果的に行うことができる組織は、ランサムウェアの影響を大幅に軽減できます。

より賢くなった新しいランサムウェアの亜種では、保存されたバックアップを検索し、それらを暗号化または削除して復旧作業を妨害するように設計されているものもあります。バックアップには複数のコピーを用意し、それらを隔離されたオフラインの場所に保存する必要があります。

- **目標復旧時点 (RPO)** を含めることで、データをアクティブな本稼働環境に戻したときに実用に耐える最新のデータを得るために、バックアップをどの程度の頻度で実行するかを決定できます。
- 同様に、復旧計画には、バックアップされた情報が取得され本稼働環境に配置されて通常のオペレーションを再開できるまでの時間を確立する、**目標復旧時間 (RTO)** を含める必要があります。AWS の環境、リソース、データベース、コード、その他データソースには、組織の運用における優先順位と重要性に基づいて、異なる RPO と RTO が設定されるでしょう。



AWS ワークロード内の脆弱性を検出してパッチを適用する

パッチが適用されていない脆弱性は、ランサムウェアが組織の環境に侵入する最も一般的な原因のひとつです。脆弱性を迅速に特定しパッチを適用すれば、組織は侵入経路を制限することでランサムウェアの脅威に晒されるリスクを減らすことができます。

Amazon Inspector を使用すれば、AWS 環境で CVE を検索し、インスタンスをセキュリティベンチマークで評価して、検出結果があった場合のセキュリティおよび IT エンジニアへの通知を完全自動化できます。脆弱性が特定された場合、**AWS Systems Manager Patch Manager** などのパッチ適用ツールは、大規模なインスタンスグループ全体にオペレーティングシステムやソフトウェアのパッチを自動的にデプロイし、脆弱性への対応に役立ちます。

インシデント発生時

早期検知と自動対応

セキュリティインシデントの検知とアラートを自動化する

サイバーインシデントに対応するには、何よりもまず脅威の存在を検知できる必要があります。身代金の要求がコンピュータ画面にポップアップ表示されて初めてランサムウェアに気付くのでは、遅すぎます。異常なユーザーの動作やネットワークアクティビティの早期検知が、ランサムウェアの脅威を阻止しインシデント対応プロセスを開始するための鍵です。AWS 環境における「正常」がどのようなものか把握することで、悪意のある動作や不正な動作が存在した場合に、セキュリティアラートを自動的に設定し、通知を送信することができます。

このような脅威を特定するために、脅威検知サービスである Amazon GuardDuty では AWS 環境内のアクティビティを継続的にモニタリングし関連付けて、悪意のある動作や不正な動作から AWS のアカウントとワークロードを保護します。このサービスは、機械学習、異常検出、統合された脅威インテリジェンスを使用して、潜在的な脅威を特定し、優先順位を付けます。

インシデント対応計画を実践する

AWS がポリシー駆動型の方式でポリシーや手順を自動化し、検出時間の改善、応答時間の短縮、アタックサーフェスの削減を可能にする機能を提供する一方、サイバーインシデントに対応するポリシーや手順の策定はお客様の責任となります。

インシデント対応チームは、インシデント発生時に、インシデントに関わる環境やリソースにアクセスする必要があります。AWS のアカウント戦略やクラウドアイデンティティ戦略を見極め、組織のクラウドアーキテクトと話し合って、どのような認証および認可方法が設定されているか理解します。

実際に攻撃される前にインシデント対応シナリオをシミュレートすることで、設定したコントロールやプロセスが期待どおりに動作するかを検証できます。この方法を取ることで、インシデント発生時に効果的に復旧および対応できるか判断できます。

ランサムウェアを関係機関に報告する

FBI では、ランサムウェアインシデントを法執行機関に報告することを組織に奨励しています。Internet Crime Complaint Center (IC3) は、実際の被害者または被害者以外の第三者からの**インターネット犯罪に対する苦情をオンライン** (米国のみ) で受け付けており、彼らと連携してその後に打つべき最良の手段を判断します。

日本国内でランサムウェアの被害に遭った場合は各都道府県警察の**サイバー犯罪相談窓口**に通報してください。

Nomoreransom.org にアクセスする

Nomoreransom.org は、法執行機関、IT セキュリティ企業、世界中の政府機関が連携協力し、ランサムウェアの被害者が身代金を払うことなく暗号化されたデータを取り戻すための支援を目的としています。

システムが影響を受けてから脅威に対処するよりも、脅威を回避する方がはるかに容易であるため、このプロジェクトでは、ランサムウェアの仕組みや侵入を効果的に防ぐための対策についてユーザーに周知することも目的としています。他の公的機関および民間組織もこの取り組みに参加することが可能です。

準備すべき共有する情報：

- 被害者の名前、住所、電話番号、E メール
- 金融取引情報 (口座情報、取引日および金額、受取人の詳細)
- 被疑者の名前、住所、電話番号、E メール、ウェブサイト、IP アドレス
- 被害状況の具体的な詳細
- E メールヘッダー
- 苦情内容を補完するために必要と思われるその他関連情報

ランサムウェアからの復旧

根本原因と教訓

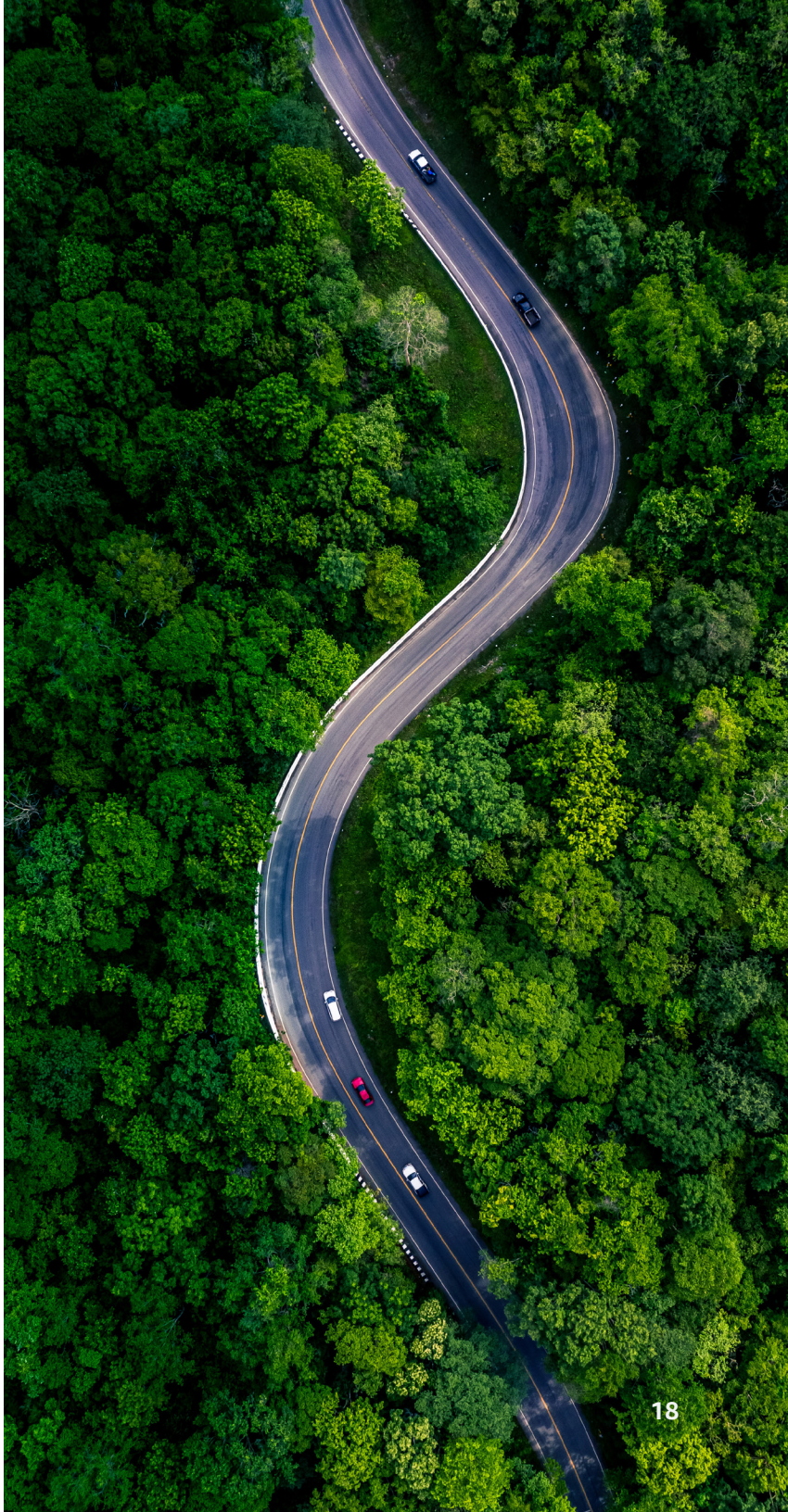
根本原因の分析を行う

お客様が使用しているフォレンジックツールは、ほとんどの場合、AWS 環境でも動作します。フォレンジックチームは、ツールの AWS リージョン全体への自動デプロイや、業務に不可欠なアプリケーションが構築されているのと同じ堅牢でスケーラブルなサービスを使用した低負荷で迅速な大容量データの収集機能によるメリットを得ることができます。

Amazon Detective は、潜在的なセキュリティの問題点や疑わしいアクティビティを容易に分析、調査し、根本原因を迅速に特定します。当サービスは、AWS リソースからログデータを自動的に収集し、機械学習、統計分析、グラフ理論を使用して、リンクされたデータセットを構築します。これにより、より迅速で効率的なセキュリティ調査を実行できます。

教訓を活かしセキュリティプログラムを更新する

シミュレーションや実際のインシデント中に得た教訓を文書化し、「ニューノーマル」のプロセスと手順に循環させることで、組織は違反が発生した際の状況をよりよく理解できます。例えば、どの箇所が脆弱だったか、どの箇所のオートメーションが失敗したのか、どの箇所の可視性が欠けていたのか、またセキュリティ体制全体を強化する機会も把握できます。



まとめ

ランサムウェアは進化を続けていますが、お客様のセキュリティの認識や準備態勢も進化できます。世界中の政府機関、非営利団体や企業が AWS を信頼し、インフラストラクチャを強化してシステムとデータの安全を確保しています。AWS のサービスと、このガイドブックのベストプラクティスを使用することで、プロアクティブな対策を講じ、AWS 環境内でのランサムウェアによる被害の可能性と影響を削減できます。

AWS リソース

AWS クラウドセキュリティリソースハブ

AWS クラウドにおける NIST CSF への準拠

Security Pillar - AWS Well-Architected Framework (セキュリティの柱 - AWS Well-Architected フレームワーク)

Building a Threat Detection Strategy in AWS (AWS での脅威検出戦略の策定)

AWS Security Incident Response Guide (AWS セキュリティインシデント対応ガイド)

AWS コンプライアンス

日本国内の公的な連絡先

情報セキュリティ安心相談窓口 (IPA)

AWS の使用を開始する

AWS の基礎を学び、AWS コミュニティとつながり、認定で知識を向上しましょう。無料アカウントに今すぐご登録ください。

サインアップ ›

ご質問がある場合やサポートが必要な場合

クラウド移行のどの段階であっても、AWS に関するあらゆる質問に、回答いたします。

お問い合わせ ›