AWS セキュリティのベストプラクティス

2016 年 8 月

(このホワイトペーパーの最新バージョンは、
http://aws.amazon.com/security
を参照してください)

注意

本書は情報提供のみを目的としています。本書の発行時点における AWS の現行製品と慣行を表したものであり、そ予告なく変更されることがあります。お客様は本書の情報、および AWS 製品またはサービスの利用について、独自の評価に基づき判断する責任を負います。いずれの AWS 製品またはサービスも、明示または黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されます。本書のいかなる内容も、AWS、その関係者、サプライヤ、またはライセンサーからの保証、表明、契約的責任、条件や確約を意味するものではありません。
The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

目次

要約

このホワイトペーパーは、アマゾン ウェブ サービス (AWS) で実行するアプリケーションのセキュリティインフラストラクチャおよび設定を現在設計している、または今後設計することをお考えのお客様を対象としています。このホワイトペーパーでは、AWS クラウド内のデータと資産を保護できるように Information Security Management System (ISMS) を定義し、各組織用の一連のセキュリティポリシーとプロセスを作成するのに役立つセキュリティのベストプラクティスについて説明します。また、AWS での資産の識別と分類と保護、アカウント、ユーザー、グループを使用した AWS リソースへのアクセスの管理、また、クラウド内のデータ、オペレーティングシステム、アプリケーション、およびインフラストラクチャ全体を保護するために推奨される方法など、セキュリティに関するさまざまなトピックの概要についても説明します。

本書の対象者は IT に関する意思決定者およびセキュリティ担当者であり、ネットワーキング、オペレーティングシステム、データ暗号化、運用管理の分野におけるセキュリティの基本的な概念を理解していることを前提として書かれています。

概要

アマゾン ウェブ サービス (AWS) のお客様にとって最も重要なことは、情報のセキュリティです。セキュリティは、偶発的または意図的な盗難、漏洩、不整合、削除からミッションクリティカルな情報を保護する機能要件の中核部分です。

AWS は責任分担モデルにおいて、グローバルで安全なインフラストラクチャと、コンピューティング、ストレージ、ネットワーキング、データベースの基盤サービスおよびそれより上位のサービスを提供します。AWS が提供する広範なセキュリティサービスと機能を使用して、AWS のお客様は資産を保護できます。お客様は、クラウド内にあるデータの機密性、整合性、可用性を保護し、情報保護のための特定のビジネス要件を満たす責任を持ちます。AWS のセキュリティ機能の詳細については、「セキュリティプロセスの概要」 ホワイトペーパーをお読みください。

このホワイトペーパーでは、Information Security Management System (ISMS)、つまり AWS 上にある組織の資産に対する情報セキュリティのポリシーとプロセスのコレクションを作成および定義するために活用できるベストプラクティスについて説明します。ISMS の詳細については、http://www.27000.org/iso-27001.htm にある ISO 27001 を参照してください。ISMS を作成せずに AWS を使用できますが、広く採用されているグローバルセキュリティアプローチの基本構成要素を基盤として構築された情報セキュリティを管理するための体系的なアプローチは、組織の全体的なセキュリティ体制の向上に役立つものと考えられます。

次のトピックについて説明します。

- AWS とお客様との間でセキュリティ上の責任を共有する方法
- 資産を定義および分類する方法
- 特権アカウントとグループを使用してデータへのユーザーアクセスを管理する方法
- データ、オペレーティングシステム、ネットワークの保護に関するベストプラクティス
- セキュリティ上の目標の達成におけるモニタリングとアラートの重要性

このホワイトペーパーでは、これらの分野のセキュリティに関するベストプラクティスについて詳しく説明します。（設定する「方法」に関するガイダンスは含みません。設定ガイダンスについては、http://aws.amazon.com/documentation にある AWS ドキュメントを参照してください)。

AWS 責任共有モデルの概要

アマゾン ウェブ サービスは、クラウドにおいて安全なグローバルインフラストラクチャおよびサービスを提供します。AWS を基盤としてシステムを構築し、AWS の機能を利用する ISMS を設計できます。

AWS において ISMS を設計するには、最初に AWS 責任共有モデルについて理解しておく必要があります。責任共有モデルでは、セキュリティ上の目標に向けて AWS とお客様が連携する必要があります。

AWS が安全なインフラストラクチャとサービスを提供する一方で、お客様は安全なオペレーティングシステム、プラットフォーム、データを用意する責任を持ちます。安全なグローバルインフラストラクチャを確保するため、AWS では、インフラストラクチャコンポーネントを構成し、お客様がセキュリティの強化に利用できるサービスと機能を提供します。たとえば、その 1 つである Identity and Access Management (IAM) サービスを使用すると、AWS のサービスのサブセットにおいてユーザーとユーザーアクセス権限を管理できます。サービスを安全なものにするため、AWS では提供するサービスの種類ごとに責任共有モデルが用意されています。

- インフラストラクチャサービス
- コンテナサービス
- 抽象化サービス

たとえば、Amazon Elastic Compute Cloud (Amazon EC2) などのインフラストラクチャサービスの責任共有モデルでは、AWS が次の資産のセキュリティを管理することが指定されています。

- 設備
- ハードウェアの物理的セキュリティ
- ネットワークインフラストラクチャ
- 仮想化インフラストラクチャ

ISMS アセットの定義においては、AWS がこれらのアセットの所有者であると考えます。これらの AWS 統制を活用して、ISMS に組み込みます。

この Amazon EC2 の例では、お客様は次のアセットのセキュリティの責任を負います。

- Amazon マシンイメージ（AMI）
- オペレーティングシステム
- アプリケーション
- 送信中のデータ
- 保管中のデータ
- データストア
- 認証情報
- ポリシーと設定

個々のサービスでは、お客様と AWS の間での責任の共有がさらに明確に規定されています。詳細については、http://aws.amazon.com/compliance/#third-party を参照してください。

AWS の安全なグローバルインフラストラクチャについて

AWS の安全なグローバルインフラストラクチャおよびサービスは AWS によって管理され、エンタープライズシステムおよび個々のアプリケーションのための信頼性の高い基盤を提供します。アプリケーション。AWS では、クラウド内の情報セキュリティに関して高い水準が確立されており、ソフトウェア調達および開発による物理的なセキュリティから従業員のライフサイクル管理およびセキュリティ組織まで、包括的かつ総合的な一連の統制目標が用意されています。AWS の安全なグローバルインフラストラクチャおよびサービスは、定期的に第三者によるコンプライアンス監査を受けます。詳細については、「アマゾン ウェブ サービスのリスクとコンプライアンス」ホワイトペーパー を参照してください。(「参考資料と参考文献」を参照)。

IAM サービスの使用

IAM サービスは、本書で説明する AWS の安全なグローバルインフラストラクチャのコンポーネントの 1 つです。IAM を使用すると、ユーザー、パスワードやアクセスキーなどのセキュリティ認証情報、およびユーザーがアクセスできる AWS のサービスとリソースを制御するアクセス権限ポリシーを集中管理できます。

AWS にサインアップする際に AWS アカウントを作成し、ユーザー名 (E メールアドレス) とパスワードを設定します。ユーザー名とパスワードを使用して AWS マネジメントコンソールにログインすると、ブラウザベースのインターフェイスを使用して AWS のリソースを管理できます。また、アクセスキー (アクセスキー ID とシークレットアクセスキーで構成されます) を作成し、コマンドラインインターフェイス (CLI)、AWS SDK、または API 呼び出しを使用して AWS のプログラムによる呼び出しを行うときに使用できます。

IAM を使用すると、AWS アカウント内に個々のユーザーを作成し、個別にユーザー名、パスワード、アクセスキーを設定できます。その後、個々のユーザーは、アカウントに固有の URL を使用してコンソールにログインできます。また、プログラムで呼び出しを行って AWS リソースにアクセスできるように、個々のユーザー用のアクセスキーを作成することもできます。IAM ユーザーによって実行されたアクティビティに関するすべての料金は、AWS アカウントに対して請求されます。ベストプラクティスとして、自身用であっても IAM ユーザーを作成し、日常的な AWS へのアクセスには AWS アカウントの認証情報を使用しないことをお勧めします。詳細については、「IAM のベストプラクティス」を参照してください。

リージョン、アベイラビリティーゾーン、エンドポイント

AWS の安全なグローバルインフラストラクチャのコンポーネントであるリージョン、アベイラビリティーゾーン、エンドポイントについても理解しておく必要があります。

AWS リージョンを使用して、ネットワークレイテンシーおよび規制コンプライアンスを管理します。特定のリージョンに保存されたデータは、そのリージョンの外部にはレプリケートされません。ビジネス上のニーズによりデータを異なるリージョンにレプリケートする必要がある場合は、お客様の責任において行います。AWS は、各リージョンが存在する国および州 (該当する場合) に関する情報を提供します。お客様は、コンプライアンスおよびネットワークレイテンシーの要件を考慮して、データを保存するリージョンを選択する必要があります。

リージョンは可用性を考慮して設計されており、少なくとも 2 つ (通常はそれより多く) のアベイラビリティーゾーンで構成されます。アベイラビリティーゾーンは、障害の分離を目的として設計されています。各アベイラビリティーゾーンは複数のインターネットサービスプロバイダー (ISP) およびさまざまな電力グリッドに接続されています。アベイラビリティーゾーン間は高速リンクを使用して相互接続されているため、アプリケーションは同じリージョン内のアベイラビリティーゾーン間の通信にローカルエリアネットワーク (LAN) 接続を利用できます。お客様は、システムを配置するアベイラビリティーゾーンを慎重に選択する必要があります。システムは複数のアベイラビリティーゾーンにまたがることができるため、災害時のアベイラビリティーゾーンの一時的または長時間の障害に対応できるようにシステムを設計することをお勧めします。

AWS では、AWS マネジメントコンソールを使用したサービスへのウェブアクセスが可能です。サービスごとに個別のコンソールで利用できます。また、アプリケーションプログラミングインターフェイス (API) およびコマンドラインインターフェイス (CLI) を使用して、プログラムからサービスにアクセスすることもできます。AWS によって管理されるサービスエンドポイントは、管理 (「バックプレーン」) アクセスを提供します。

AWS サービスのセキュリティ上の責任共有

AWS では、さまざまなインフラストラクチャサービスおよびプラットフォームサービスが提供されます。このような AWS のサービスのセキュリティおよび責任共有モデルを理解するため、サービスを 3 つの主要なカテゴリに分類します。それは、インフラストラクチャサービス、コンテナサービス、抽象化サービスです。各カテゴリのセキュリティ所有権モデルは、機能の操作方法およびアクセス方法に基づいて少しずつ異なります。

- **インフラストラクチャサービス:** このカテゴリには、Amazon EC2 などのコンピューティングサービスと、Amazon Elastic Block Store (Amazon EBS)、Auto Scaling、Amazon Virtual Private Cloud (Amazon VPC) などの関連サービスが含まれます。 これらのサービスを利用すると、オンプレミスソリューションと類似しているとともに幅広く互換性があるテクノロジーを使用して、クラウドインフラストラクチャを設計および構築できます。オペレーティングシステムを管理し、仮想化スタックのユーザー層へのアクセスが可能なあらゆる認証管理システムを設定して運用できます。
- **コンテナサービス:** 通常、このカテゴリのサービスは独立した Amazon EC2 または他のインフラストラクチャインスタンスで実行されますが、お客様はそのオペレーティングシステムまたはプラットフォーム層を管理しない場合があります。AWS では、こうしたアプリケーション「コンテナ」に対してマネージド型サービス提供します。お客様は、ファイアウォールルールなどのネットワーク制御のセットアップと管理、および IAM とは別にプラットフォームレベルの ID とアクセス管理を担当します。コンテナサービスの例としては、Amazon Relational Database Services (Amazon RDS)、Amazon Elastic Map Reduce (Amazon EMR)、AWS Elastic Beanstalk などがあります。

- **抽象化サービス:** このカテゴリには、高レベルのストレージ、データベース、メッセージングの各サービスが含まれます。Amazon Simple Storage Service (Amazon S3)、Amazon Glacier、Amazon DynamoDB、Amazon Simple Queuing Service (Amazon SQS)、Amazon Simple Email Service (Amazon SES) などです。これらのサービスは、お客様がクラウドアプリケーションを構築して運用できるプラットフォーム層または管理層を抽象化します。お客様は AWS API を使用してこれらの抽象化サービスのエンドポイントにアクセスし、AWS は基盤のサービスコンポーネントまたはそれらが存在するオペレーティングシステムを管理します。お客様は基盤のインフラストラクチャを共有し、抽象化サービスではデータを安全に分離して IAM との強力な統合を実現するマルチテナントプラットフォームを提供します。

各サービスタイプの責任共有モデルについてもう少し詳しく説明します。

インフラストラクチャサービスの責任共有モデル

Amazon EC2、Amazon EBS、Amazon VPC などのインフラストラクチャサービスは、AWS グローバルインフラストラクチャを基盤として実行されます。可用性と耐久性の目標はサービスごとに異なりますが、これらのサービスは起動された特定のリージョン内で常に動作します。複数のアベイラビリティーゾーンにまたがって耐障害性を持つコンポーネントを利用することにより、AWS の個別のサービスの可用性の目標を超える可用性の目標を満たすシステムを構築できます。

図 1 では、インフラストラクチャサービスの責任共有モデルの構成要素を示します。

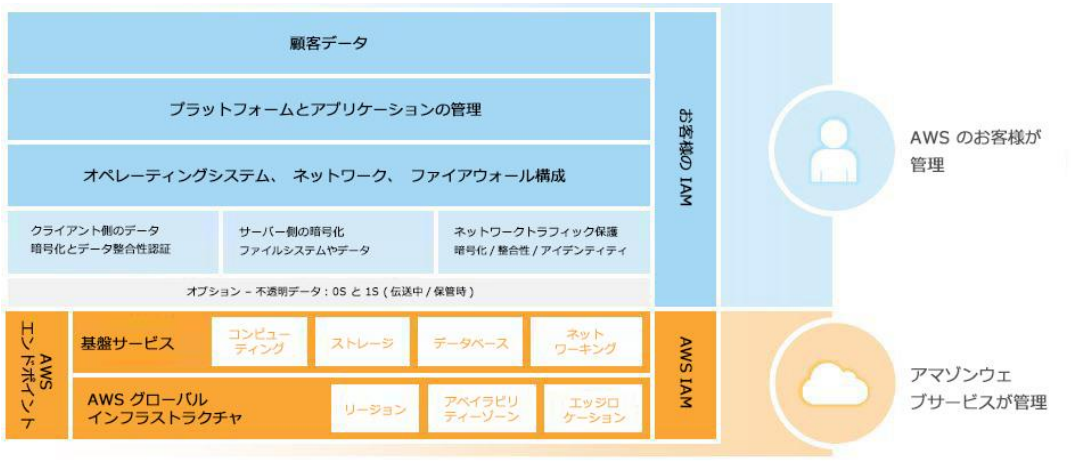

図 1: インフラストラクチャサービスの責任共有モデル

オンプレミスの独自のデータセンターと同じように、AWS の安全なグローバルインフラストラクチャの基盤上で、AWS クラウドにオペレーティングシステムとプラットフォームをインストールして設定します。その後、プラットフォームにアプリケーションをインストールします。最終的に、データはお客様独自のアプリケーション内で保存および管理されます。より厳格なビジネス要件またはコンプライアンス要件がない場合、AWS の安全なグローバルインフラストラクチャによって提供されるもの以外の保護レイヤーを追加導入する必要はありません。

コンプライアンスの要件によっては、AWS のサービスと、アプリケーションおよびデータが存在するお客様のオペレーティングシステムおよびプラットフォームの間に、保護レイヤーを追加することが必要になる場合があります。保管中のデータの保護、送信中のデータの保護、AWS のサービスとお客様のプラットフォームの間への不可視レイヤーの導入など、追加の管理を組み込むことができます。不可視レイヤーには、データ暗号化、データ整合性認証、ソフトウェア署名およびデータ署名、安全なタイムスタンプなどを含めることができます。

AWS が提供するテクノロジーを実装することにより、保管中および送信中のデータを保護できます。詳細については、このホワイトペーパーの「Amazon EC2 インスタンスへの OS レベルのアクセスの管理」および「データの保護」のセクションを参照してください。または、独自のデータ保護ツールを導入したり、AWS のパートナーが提供するサービスを利用したりすることもできます。

前のセクションでは、AWS のサービスへの認証を必要とするリソースへのアクセスを管理する方法について説明しました。しかし、EC2 インスタンス上のオペレーティングシステムにアクセスするには、異なる認証情報のセットが必要です。責任共有モデルでは、お客様がオペレーティングシステムの認証情報を所有しますが、AWS はオペレーティングシステムへの初期アクセスのブートストラップを補助します。

標準の AMI から新しい Amazon EC2 インスタンスを起動するとき、お客様は Secure Shell (SSH) や Windows リモートデスクトッププロトコル (RDP) などの安全なリモートシステムアクセスプロトコルを使用してそのインスタンスにアクセスできます。Amazon EC2 インスタンスにアクセスし、要件に合わせて設定するには、オペレーティングシステムレベルの認証に成功している必要があります。認証を受けて Amazon EC2 インスタンスにリモートアクセスした後は、適切なオペレーティングシステム認証メカニズムを設定できます。
X.509 証明書認証、Microsoft Active Directory、またはローカルのオペレーティングシステムアカウント。

EC2 インスタンスへの認証を有効にするため、AWS では Amazon EC2 キーペアと呼ばれる非対称キーペアが提供されます。このキーペアは業界標準の RSA キーペアです。各ユーザーは、複数の Amazon EC2 キーペアの使用が可能であり、異なるキーペアを使用して新しいインスタンスを起動できます。EC2 キーペアは、これまでに説明した AWS アカウントまたは IAM ユーザー認証情報とは関係ありません。これらの認証情報は AWS の他のサービスへのアクセスを制御します。EC2 キーペアは、特定のインスタンスへのアクセスのみを制御します。

OpenSSL などの業界標準ツールを使用して、独自の Amazon EC2 キーペアを生成することもできます。キーペアの生成は信頼できる安全な環境で行い、キーペアのパブリックキーのみを AWS にインポートします。プライベートキーは安全に保存します。この方法を使用する場合は、高品質の乱数ジェネレーターを使用することをお勧めします。

AWS で生成された Amazon EC2 キーペアを使用することもできます。その場合は、インスタンスを初めて作成するときに、RSA キーペアのプライベートキーとパブリックキーの両方がお客様に提供されます。お客様は、Amazon EC2 キーペアのプライベートキーをダウンロードして安全に保存する必要があります。AWS ではプライベートキーを保存しません。プライベートキーをなくした場合は、新しいキーペアを生成する必要があります。

cloud-init サービスを使用する Amazon EC2 Linux インスタンスの場合、標準 AWS AMI から新しいインスタンスが起動されるときに、Amazon EC2 キーペアのパブリックキーが初期オペレーティングシステムユーザーの ~/.ssh/authorized_keys ファイルに追加されます。

~/.ssh/authorized_keys ファイル。その後、そのユーザーは、正しい Amazon EC2 インスタンスユーザーの名前を ID として使用するようにクライアントを設定し (ec2-user など)、ユーザー認証用にプライベートキーファイルを提供することによって、SSH クライアントを使用して Amazon EC2 Linux インスタンスに接続できます。

ec2config サービスを使用する Amazon EC2 Windows インスタンスの場合、標準の AWS AMI から新しいインスタンスを起動すると、**ec2config** サービスによって、そのインスタンス用に新しいランダムな管理者パスワードが設定され、Amazon EC2 キーペアの対応するパブリックキーで暗号化されます。ユーザーは、AWS マネジメントコンソールまたはコマンドラインツールを使用して、パスワードを復号するための対応する Amazon EC2 プライベートキーを指定することで、Windows インスタンスのパスワードを取得できます。このパスワードと Amazon EC2 インスタンスのデフォルトの管理アカウントを使用して、Windows インスタンスに対する認証を行うことができます。

AWS では、Amazon EC2 のキーを管理したり、新たに起動した Amazon EC2 インスタンスに業界標準の認証を適用したりするのに役立つ、柔軟で実用的な一連のツールを用意しています。より高いセキュリティが必要な場合は、LDAP や Active Directory などの別の認証メカニズムを実装し、Amazon EC2 キーペア認証を無効にすることもできます。

コンテナサービスの責任共有モデル

AWS の責任共有モデルは、Amazon RDS や Amazon EMR など、コンテナサービスにも適用されます。これらのサービスの基盤となるインフラストラクチャ、基盤サービス、オペレーティングシステム、アプリケーションプラットフォームについては、AWS が管理します。たとえば、Amazon RDS for Oracle はマネージド型のデータベースサービスであり、Oracle データベースプラットフォームまでを含むコンテナのすべてのレイヤーが AWS で管理されます。AWS プラットフォームには、Amazon RDS などのサービス用に、データバックアップ復旧ツールが用意されています。ただし、事業継続および災害対策 (BC/DR) ポリシーに関連するツールについては、ユーザー側で用意する必要があります。

AWS のコンテナサービスを利用する場合、データの管理やコンテナサービスにアクセスするためのファイアウォールルールの管理についてはユーザーが行う必要があります。たとえば、Amazon RDS では RDS セキュリティグループを利用できるほか、Amazon EMR では Amazon EMR インスタンスの Amazon EC2 セキュリティグループを通じてファイアウォールルールを管理できます。

図 2 では、コンテナサービスの責任分担モデルを示します。

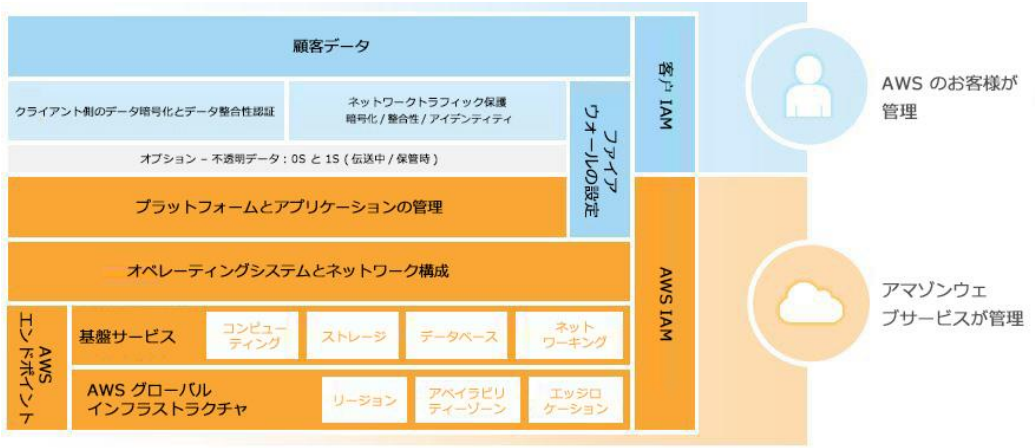

図 2: コンテナサービスの責任共有モデル

抽象化されたサービスの責任共有モデル

Amazon S3 や Amazon DynamoDB などの抽象化されたサービスについては、インフラストラクチャレイヤー、オペレーティングシステム、プラットフォームの運用を AWS が行い、ユーザーはエンドポイントにアクセスしてデータを保存、取得します。Amazon S3 と DynamoDB は IAM に緊密に統合されています。データの管理 (アセットの分類を含む) はユーザーが行う必要があり、IAM ツールを使用してプラットフォームレベルで個々のリソースに ACL タイプのアクセス権限を適用したり、IAM ユーザー/グループレベルでユーザーの ID または責任に基づいてアクセス権限を適用したりできます。また、Amazon S3 などの一部のサービスでは、保管されているデータをプラットフォームの暗号化機能を使用して保護したり、サービスとの間で送信されるデータをプラットフォームのペイロードの HTTPS カプセル化機能を使用して保護したりできます。

図 3 では、AWS の抽象化されたサービスの責任分担モデルの概略を示します。

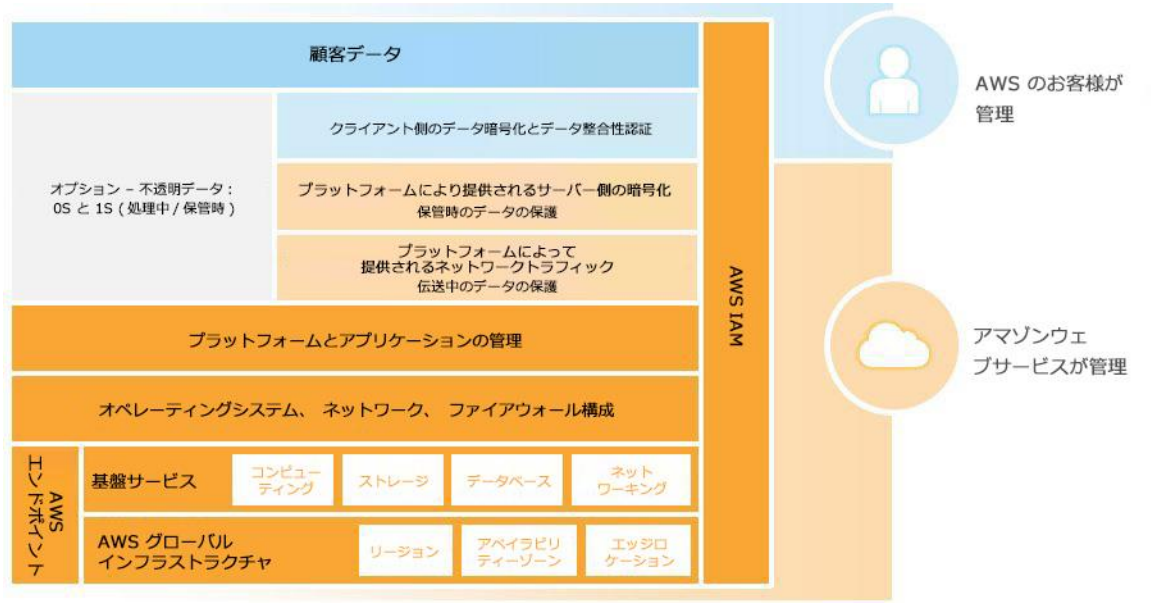

図 3: 抽象化されたサービスの責任共有モデル

Trusted Advisor ツールの使用

AWS プレミアムサポートの一部のプランでは、Trusted Advisor ツールを利用できます。これは、サービスの状況をひと目で確認できるツールで、一般的なセキュリティ設定ミス、システムパフォーマンスの向上に関する提案、使用率の低いリソースを特定するのに役立ちます。このホワイトペーパーでは、Amazon EC2 に関連する Trusted Advisor のセキュリティの側面について説明します。

Trusted Advisor では、次のセキュリティの推奨事項に準拠しているかどうかがチェックされます。

- 一般的な管理ポートへのアクセスが一部のアドレスのみに制限されているかどうか。対象となるポートは、22 (SSH)、23 (Telnet) 3389 (RDP)、5500 (VNC) などです。
- 一般的なデータベースポートへのアクセスが制限されているかどうか。対象となるポートは、1433 (MSSQL Server)、1434 (MSSQL Monitor)、3306 (MySQL)、Oracle (1521)、5432 (PostgreSQL) などです。
- AWS リソースへのアクセスを安全にコントロールできるように IAM が設定されているかどうか。
- ルート AWS アカウントの 2 要素認証に対応できるように Multi-Factor Authentication (MFA) トークンが有効化されているかどうか。

AWS でのアセットの定義と分類

ISMS の設計を開始する前に、保護する必要があるすべての情報アセットを特定し、それらを保護するための実現可能なソリューションを技術面とコスト面の両方から検討します。それぞれのアセットのコストを量的に数値化することが難しい場合は、質的なメトリック (無視できるほど低い/低い/中/高い/非常に高いなど) で分類すると効果的なことがあります。

アセットは 2 つのカテゴリに分類されます。

- 本質的要素 (業務の情報、プロセス、活動など)
- 本質的要素をサポートする構成要素 (ハードウェア、ソフトウェア、人員、サイト、パートナー組織など)

表 1 に、アセットのマトリックスのサンプルを示します。

アセット名	アセットの所有者	アセットカテゴリ	依存関係	コスト
顧客向けウェブサイトアプリケーション	e コマースチーム	必須	EC2、Elastic Load Balancing、RDS、開発	
顧客のクレジットカードデータ	e コマースチーム	必須	PCI カード所有者の環境、暗号化、AWS PCI サービス	
人事データ	最高執行責任者 (COO)	必須	Amazon RDS、暗号化プロバイダー、開発運用 IT、サード	
データアーカイブ	最高執行責任者 (COO)	必須	S3、Glacier、開発運用 IT	
HR 管理システム	HR	必須	EC2、S3、RDS、開発運用 IT、サードパーティ	
AWS Direct Connect インフラストラクチャ	最高情報責任者 (CIO)	ネットワーク	ネットワーク運用、通信事業者、AWS Direct Connect	
ビジネスインテリジェンスインフラストラクチャ	BI チーム	ソフトウェア	EMR、Redshift、Dynamo DB、S3、開発運用	
ビジネスインテリジェンスサービス	最高執行責任者 (COO)	必須	BI インフラストラクチャチーム、BI 分析チーム	
LDAP ディレクトリ	IT セキュリティチーム	セキュリティ	EC2、IAM、カスタムソフトウェア開発運用	
Windows AMI	サーバーチーム	ソフトウェア	EC2、パッチ管理ソフトウェア、開発運用	
顧客認証情報	コンプライアンスチーム	セキュリティ	毎日の更新、アーカイブインフラストラクチャ	

デプロイ、交換、メンテナンス、コスト/損失の結果

表 1: アセットのマトリックスのサンプル

AWS でアセットを保護するための ISMS の設計

アセット、カテゴリ、コストを特定したら、AWS での情報セキュリティマネージメントシステム (ISMS) の実装、運用、モニタリング、確認、保守、改良に関する基準を定めます。セキュリティ要件は組織ごとに異なります。影響する要因としては次のものがあります。

- ビジネスのニーズや目標
- 採用しているプロセス
- 組織の規模や構造

これらの要因はいずれも時間とともに変わる可能性があるため、すべての情報を管理できるように循環的なプロセスを構築することが重要です。

表 2 に、AWS で ISMS を設計および構築するための段階的アプローチを示します。ISMS の設計や実装には、ISO 27001 などの標準的なフレームワークが役立つ場合があります。

段階	タイトル	説明
1	**スコープと境界の定義**	「スコープ」に含めるリージョン、アベイラビリティーゾーン、インスタンス、AWS リソースを定義します。いずれかのコンポーネントを対象から除外する場合 (設備の管理は AWS が行うため、独自の管理システムで管理する必要がない場合など)、そのコンポーネントと除外理由を記述します。

段階	タイトル	説明
2	**ISMS ポリシーの定義**	次の情報を含めます。 • 情報セキュリティに関するアクションの方向性と指針 • 法律、契約、規制による要件 • 組織のリスク管理の目標 • リスクの評価方法 • マネジメントによる計画の承認方法
3	**リスク評価方法の選択**	組織のグループから次の要因に関する情報を収集し、それに基づいてリスク評価方法を選択します。 • ビジネスニーズ • 情報セキュリティ要件 • IT 機能とその用途 • 法的な要件 • 規制による責任 パブリッククラウドインフラストラクチャの運用方法は既存の環境と異なるため、リスクを受け入れる基準やリスクの許容レベル (リスク許容度) を識別する基準を定めることが重要です。 最初にリスク評価を行い、可能な範囲内で自動化を利用することをお勧めします。AWS のリスク管理の自動化を利用すると、リスク管理に必要なリソースの範囲を絞り込むことができます。 リスク評価方法には、OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)、ISO 31000:2009 Risk Management、ENISA (European Network and Information Security Agency)、IRAM (Information Risk Analysis Methodology)、NIST (National Institute of Standards & Technology) Special Publication (SP) 800-30 rev.1 Risk Management Guide などがあります。
4	**リスクの特定**	すべての資産を脅威にマッピングしてリスク登録簿を作成してから、脆弱性評価および影響分析の結果に基づいて、それぞれの AWS 環境に応じた新しいリスクマトリックスを作成することをお勧めします。 こちら’でリスク登録簿に含める情報の例を示します。 • アセット • アセットに対する脅威

段階	タイトル	説明
		• 脅威によって悪用される可能性がある脆弱性 • 脆弱性が悪用された場合の結果
5	**リスクの分析と評価**	リスクの分析と評価を行い、ビジネスへの影響、可能性、リスクレベルを試算します。
6	**リスクへの対処**	リスクに対処する方法を選択します。セキュリティコントロールを適用する、リスクを受け入れる、リスクを回避する、リスクを移転するなどの対処方法があります。
7	**セキュリティコントロールフレームワークの選択**	セキュリティコントロールを選択するときは、ISO 27002、NIST SP 800-53、COBIT (Control Objectives for Information and related Technology)、CSA-CCM (Cloud Security Alliance-Cloud Control Matrix) などのフレームワークを使用します。これらのフレームワークは、再利用可能な一連のベストプラクティスで構成され、関連するコントロールを選択するのに役立ちます。
8	**マネジメントによる承認の取得**	あらゆるコントロールを実装しても、リスクを完全に取り除くことはできません。すべての残留リスクをマネジメントに報告し、ISMS の実装および運用についての承認を得ることをお勧めします。
9	**適用宣言書**	次の情報を含む適用宣言書を作成します。 • 選択したコントロールと選択理由 • 導入済みのコントロール • 導入予定のコントロール • 除外したコントロールと除外理由

表 2: ISMS の構築までの段階

AWS アカウント、IAM ユーザー、グループ、ロールの管理

ISMS の設計においては、ユーザーが必要とするリソースのみに限定して、それらのリソースにアクセスするための最低限のアクセス権限をユーザーに割り当てることが重要です。これには IAM が役立ちます。AWS アカウントで *IAM* ユーザーを作成してから、ユーザーにアクセス権限を直接割り当てるか、ユーザーをグループに割り当ててそのグループにアクセス権限を割り当てます。AWS アカウントと IAM ユーザーのもう少し詳しい定義を次に示します。

- **AWS アカウント。**AWS に最初にサインアップしたときに作成するアカウントです。AWS アカウントは、AWS ユーザーと AWS の間のビジネス上の関係を表したものです。ユーザーが AWS のリソースやサービスを管理するときに使用します。AWS アカウントは、AWS のすべてのリソースとサービスにアクセス可能なルートアクセス権限を持つ非常に強力なアカウントです。このルートアカウントの認証情報は、AWS との日常的なやり取りには使用しないでください。組織によっては、主要な部門ごとに 1 つずつというように複数の AWS アカウントを使用し、それぞれの AWS アカウントで人やリソースに応じて IAM ユーザーを作成している場合があります。

- **IAM ユーザー。**IAM では、複数のユーザーを作成して各ユーザーに個別のセキュリティ認証情報を割り当て、それらのすべてのユーザーを単一の AWS アカウントで管理することができます。IAM ユーザーは、AWS リソースにマネジメントコンソールや CLI、あるいは API から直接アクセスする必要がある人、サービス、またはアプリケーションを表します。ベストプラクティスは、AWS アカウントのサービスやリソースにアクセスする必要があるユーザーごとに、個別に IAM ユーザーを作成することです。AWS アカウントでリソースへのきめ細かなアクセス権限を作成し、グループを作成してそのアクセス権限を適用し、それらのグループにユーザーを割り当てることができます。このベストプラクティスに従うと、タスクに必要な最小限のアクセス権限がユーザーに割り当てられます。

複数の AWS アカウントを使用する場合の戦略

AWS アカウントの戦略を練るときは、セキュリティを最大限に高めるとともに、ビジネスやガバナンスの要件を満たすように設計することが重要です。表 3 に、戦略の例を示します。

ビジネス要件	設計例	コメント
セキュリティを一元的に管理	単一の AWS アカウント	情報セキュリティの管理を一元化し、オーバーヘッドを最小限に抑えます。
本番環境、開発環境、テスト環境を分離	3 つの AWS アカウント	本番サービス用、開発用、テスト用に AWS アカウントを 1 つずつ作成します。
独立した複数の部門	複数の AWS アカウント	組織の独立部門ごとに AWS アカウントを個別に作成します。アカウントごとにアクセス権限やポリシーを割り当てることができます。

ビジネス要件	設計例	コメント
独立した複数のプロジェクトでセキュリティを一元的に管理	複数の AWS アカウント	共通のプロジェクトリソース (DNS サービス、Active Directory など) 用に AWS アカウントを 1 つ作成し、さらにプロジェクトごとに個別の AWS アカウントを作成します。プロジェクト用のアカウントごとにアクセス権限やポリシーを割り当て、アカウント全体に対してリソースへのアクセスを許可できます。

表 3: AWS アカウントの戦略

複数のアカウントについて一括請求関係を設定すると、アカウント別に請求を管理する複雑さを軽減し、スケールメリットを活用することができます。一括請求を使用する場合、アカウント間でリソースや認証情報は共有されません。

IAM ユーザーの管理

新しい IAM ユーザーの作成、および既存のユーザーの管理や削除は、適切なレベルのアクセス権限を持つ IAM ユーザーのみが実行できます。高い権限が与えられたこの IAM ユーザーは、AWS の設定を管理したり AWS リソースに直接アクセスしたりする組織内の人、サービス、またはアプリケーションのそれぞれに対して個別に IAM ユーザーを作成できます。複数のエンティティで同じ認証情報を共有する共有ユーザー ID は、使用しないことを強くお勧めします。

IAM グループの管理

IAM グループは、1 つの AWS アカウントの複数の IAM ユーザーの集合です。IAM グループは、職務、部門、または地域単位で作成したり、プロジェクト別に作成したりするなど、ジョブを実行するために同様の AWS リソースにアクセスする必要がある IAM ユーザーを任意の基準でまとめて作成できます。それぞれの IAM グループに、1 つまたは複数の IAM ポリシーを割り当てて、AWS リソースにアクセスするためのアクセス権限を付与できます。IAM グループに割り当てられたポリシーは、そのグループに属する IAM ユーザーにすべて継承されます。

たとえば、組織でバックアップ作業を担当している John という IAM ユーザーが、`Archives` という Amazon S3 バケットのオブジェクトにアクセスする必要があるとします。この場合、John にアクセス権限を直接付与すれば、`Archives` バケットへのアクセスを許可することができます。次に、John と同じチームに Sally と Betty も配属するとします。この場合は、`Archives` バケットにアクセスするためのアクセス権限を John、Sally、Betty の 3 人に個別に付与することもできますが、グループにアクセス権限を割り当ててそのグループに John、Sally、Betty の 3 人を加えた方が管理やメンテナンスが簡単になります。同じアクセス権限が必要なユーザーがほかにもいる場合は、そのユーザーを同じグループに追加することでアクセス権限を付与できます。また、ユーザーがリソースにアクセスする必要がなくなった場合は、そのリソースへのアクセスを提供するグループからそのユーザーを削除できます。

IAM グループは、AWS リソースへのアクセスを管理する強力なツールです。特定のリソースにアクセスする必要があるユーザーが 1 人しかいない場合でも、ベストプラクティスとして、そのアクセス用に新しい AWS グループを用意し、グループメンバーシップおよびグループレベルで割り当てられたアクセス権限とポリシーを通じてユーザーのアクセスをプロビジョニングすることをお勧めします。

AWS 認証情報の管理

AWS アカウントと IAM ユーザーはそれぞれ一意の ID であり、固有の長期的な認証情報が設定されます。これらの ID に関連付けられる認証情報は 2 種類あり、1 つは AWS マネジメントコンソールおよび AWS ポータルページへのサインインに使用され、もう 1 つはプログラムによる AWS API へのアクセスに使用されます。

表 4 に、これらの 2 種類のサインイン認証情報を示します。

サインイン認証情報の種類	詳細
ユーザー名/パスワード	AWS アカウントのユーザー名は常に E メールアドレスになります。IAM ユーザーのユーザー名は柔軟に設定できます。AWS アカウントのパスワードは任意に定義できます。IAM ユーザーのパスワードには、ポリシーを定義して要件として設定できます (パスワードの最小文字数を指定したり、英数字以外の文字を必ず含めるように設定したりできます)。
多要素認証（MFA）	AWS Multi-Factor Authentication (MFA) を使用すると、サインイン認証情報のセキュリティを強化できます。MFA が有効な場合、ユーザーが AWS ウェブサイトにサインインすると、ユーザー名とパスワード (第 1 の要素 – ユーザーが知っている情報)、および MFA デバイスからの認証コード (第 2 の要素 – ユーザーが所有している情報) を求められます。MFA は、ユーザーが S3 オブジェクトを削除する際にも要求することができます。AWS 環境への不正アクセスを防止するために、AWS アカウントと IAM ユーザーの両方に対して MFA を有効にすることをお勧めします。現在のところ、AWS では、Gemalto のハードウェア MFA デバイスおよび仮想 MFA デバイスをスマートフォンアプリケーションの形でサポートしています。

表 4:サインイン認証情報

表 5 に、プログラムから API にアクセスする際に使用する認証情報の種類を示します。

アクセス認証情報の種類	詳細
アクセスキー	アクセスキーは、AWS サービスの API 呼び出しへのデジタル署名に使用されます。アクセスキーの認証情報は、アクセスキー ID とシークレットキーで構成されます。シークレットキーの部分は、AWS アカウントの所有者または AWS アカウントを割り当てられた IAM ユーザーが安全に管理する必要があります。 ユーザーは、アクティブなアクセスキーのセットを同時に 2 つまで所有できます。ベストプラクティスとして、アクセスキーは定期的に更新することをお勧めします。
API 呼び出しに対する MFA	Multi-Factor Authentication (MFA) で保護された API にアクセスする場合、IAM ユーザーは、API の特定の関数を使用する前に有効な MFA コードの入力が求められます。どの API で MFA が求められるかは、IAM で作成したポリシーで決まります。AWS サービス API の呼び出しは AWS マネジメントコンソールで行われるため、コンソールと API のどちらからアクセスされるかに応じて API に MFA を適用することができます。

表 5:プログラムによるアクセスの認証情報

IAM ロールと一時的なセキュリティ認証情報を使用した委任について

シナリオによっては、通常は AWS リソースにアクセスできないユーザーやサービスにアクセスを委任する場合があります。表 6 に、そのようなアクセスを委任する場合の一般的なユースケースの概要を示します。

ユースケース	説明
Amazon EC2 インスタンスで実行されるアプリケーションからの AWS リソースへのアクセス	Amazon EC2 インスタンスで実行されるアプリケーションで、Amazon S3 バケットや Amazon DynamoDB テーブルなどの AWS リソースにアクセスする必要がある場合、AWS へのリクエストをプログラムで行うためにセキュリティ認証情報が必要になります。このような場合、各インスタンスに開発者の認証情報を配布すれば、アプリケーションでそれらの認証情報を使用してリソースにアクセスできるようになります。ただし、長期的な認証情報を各インスタンスに配布すると、管理が困難になり、セキュリティのリスクとなる可能性もあります。
クロスアカウント アクセス	開発環境を本稼働環境から分離するなど、リソースへのアクセスを管理するためには、複数の AWS アカウントを持つ必要があります。ただし、一方のアカウントのユーザーが、もう一方のアカウントのリソースへのアクセスを必要とすることもあります。たとえば、開発環境から本稼働環境に更新を移す場合などです。両方のアカウントで作業するユーザーがそれぞれの ID を保持することも可能ですが、複数のアカウントに対して複数の認証情報を管理することになると、ID 管理が困難になります。
ID フェデレーション	社内のディレクトリなど、AWS 以外の ID をユーザーがすでに持っているとします。ただし、それらのユーザーが AWS リソースを使用する (または、それらのリソースにアクセスするアプリケーションを使用する) 必要がある場合もあります。その場合、それらのユーザーには、AWS へのリクエストを行うために AWS のセキュリティ認証情報も必要になります。

表 6:委任の一般的なユースケース

これらのユースケースには、IAM ロールと一時的なセキュリティ認証情報を使用して対応できます。IAM ロールを使用することでユーザーまたはサービスが必要とするリソースにアクセスするための一連のアクセス権限を定義することができますが、このアクセス権限は特定の IAM ユーザーまたはグループに付与するものではありません。IAM ユーザー、モバイルアプリケーションや EC2 ベースのアプリケーション、または AWS サービス (Amazon EC2 など) に対してロールを適用できます。ロールを適用すると、プログラムによる AWS へのリクエストにユーザーまたはアプリケーションが使用できる一時的なセキュリティ認証情報が返されます。これらの一時的なセキュリティ認証情報は、有効期限の設定が可能で、自動的に更新されます。IAM ロールと一時的なセキュリティ認証情報を使用することで、リソースにアクセスする必要があるエンティティごとに長期的なセキュリティ認証情報や IAM ユーザーを常時管理する必要がなくなります。

Amazon EC2 の IAM ロール

Amazon EC2 の IAM ロールは、表 6 の 1 つ目のユースケースに対応する IAM ロールの具体的な実装です。次の図では、開発者は Amazon EC2 インスタンスでアプリケーションを実行しており、`photos` という名前の Amazon S3 バケットにアクセスする必要があります。管理者が作成した `Get-pics` ロールには、バケットの読み取りと、開発者がロールを Amazon EC2 インスタンスで起動することを許可するポリシーが含まれています。アプリケーションをインスタンスで実行すると、ロールの一時的な認証情報を使用して `photos` バケットにアクセスすることができます。管理者は開発者に `photos` バケットにアクセスする権限を与える必要はなく、開発者が認証情報を共有する必要もありません。

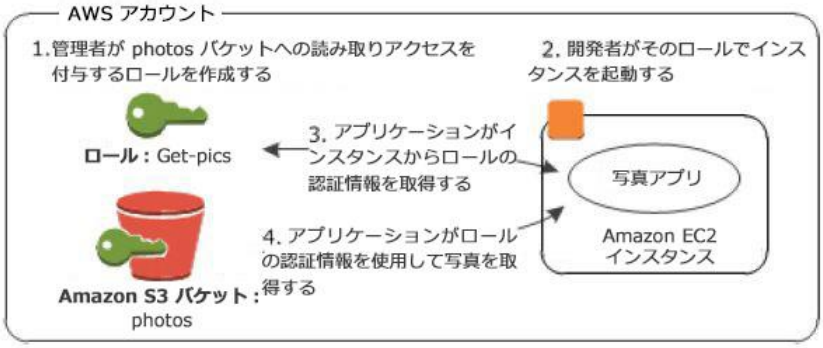

図 4:EC2 のロールの仕組み

1 管理者は、IAM を使用して `Get-pics` ロールを作成します。このロール内で、管理者はポリシーを使用して、Amazon EC2 インスタンスだけがこのロールを取得できることを指定し、`photos` バケットに対する読み取り専用のアクセス権限を指定します。

2 開発者は Amazon EC2 インスタンスを起動し、`Get- pics` ロールをそのインスタンスに関連付けます。

3 アプリケーションを実行すると、Amazon EC2 インスタンスのインスタンスメタデータから認証情報が取得されます。

4 アプリケーションは、ロールの認証情報を使用して、読み取り専用のアクセス権限で `photo` バケットにアクセスします。

クロスアカウントアクセス

表 6 の 2 つ目のユースケースには、IAM ロールを使用して、AWS アカウント内のリソースへのアクセスを別の AWS アカウントの IAM ユーザーに許可することで対応できます。このプロセスのことをクロスアカウントアクセスと呼びます。クロスアカウントアクセスでは、リソースへのアクセスを他の AWS アカウントのユーザーと共有できます。

クロスアカウントアクセスを確立するには、信頼する側のアカウント (アカウント A) で、信頼される側のアカウント (アカウント B) に特定のリソースへのアクセスを許可する IAM ポリシーを作成します。これにより、アカウント B で、そのアカウントの IAM ユーザーにこのアクセスを委任できるようになります。アカウント B の IAM ユーザーに、アカウント A から付与されたアクセス権限の範囲を超えるアクセスを委任することはできません。

ID フェデレーション

表 6 の 3 つ目のユースケースには、IAM ロールを使用して、企業ユーザーと AWS リソースの間に認証と認可のプロセスを管理する ID ブローカーを作成することで対応できます。すべてのユーザーを AWS で IAM ユーザーとして作成し直す必要はありません。

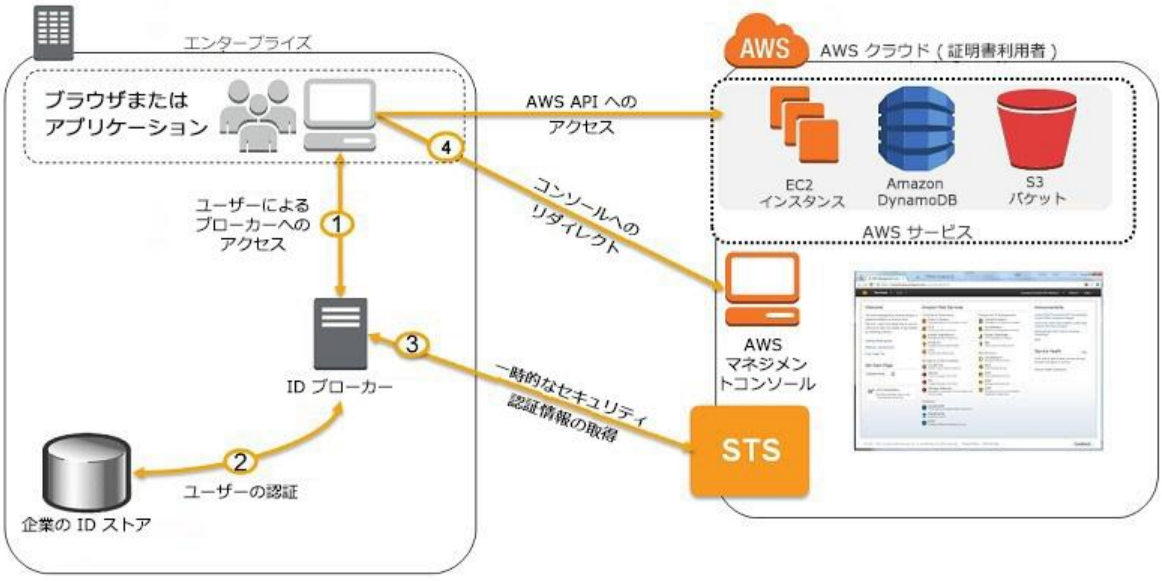

図 5:一時的なセキュリティ認証情報を使用した AWS ID フェデレーション

1. 企業ユーザーが ID ブローカーアプリケーションにアクセスします。
2. ID ブローカーアプリケーションで企業の ID ストアが照合され、ユーザーが認証されます。
3. ID ブローカーアプリケーションには、一時的なセキュリティ認証情報をリクエストするために AWS Security Token Service (STS) にアクセスする権限があります。
4. 企業ユーザーは、AWS API または AWS マネジメントコンソールにアクセスするための一時的な URL を入手できます。AWS では、Microsoft Active Directory で使用できるサンプルの ID ブローカーアプリケーションを提供しています。

Amazon EC2 インスタンスへの OS レベルのアクセスの管理

前のセクションでは、AWS のサービスへの認証を必要とするリソースへのアクセスを管理する方法について説明しました。しかし、EC2 インスタンス上のオペレーティングシステムにアクセスするには、異なる認証情報のセットが必要です。責任共有モデルでは、お客様がオペレーティングシステムの認証情報を所有しますが、AWS はオペレーティングシステムへの初期アクセスのブートストラップを補助します。

標準の AMI から新しい Amazon EC2 インスタンスを起動するとき、お客様は Secure Shell (SSH) や Windows リモートデスクトッププロトコル (RDP) などの安全なリモートシステムアクセスプロトコルを使用してそのインスタンスにアクセスできます。Amazon EC2 インスタンスにアクセスし、要件に合わせて設定するには、オペレーティングシステムレベルの認証に成功している必要があります。認証を受けて Amazon EC2 インスタンスにリモートアクセスした後は、適切なオペレーティングシステム認証メカニズムを設定できます。
X.509 証明書認証、Microsoft Active Directory、またはローカルのオペレーティングシステムアカウント。

EC2 インスタンスへの認証を有効にするため、AWS では Amazon EC2 キーペアと呼ばれる非対称キーペアが提供されます。このキーペアは業界標準の RSA キーペアです。各ユーザーは、複数の Amazon EC2 キーペアの使用が可能であり、異なるキーペアを使用して新しいインスタンスを起動できます。EC2 キーペアは、これまでに説明した AWS アカウントまたは IAM ユーザー認証情報とは関係ありません。これらの認証情報は AWS の他のサービスへのアクセスを制御します。EC2 キーペアは、特定のインスタンスへのアクセスのみを制御します。

OpenSSL などの業界標準ツールを使用して、独自の Amazon EC2 キーペアを生成することもできます。キーペアの生成は信頼できる安全な環境で行い、キーペアのパブリックキーのみを AWS にインポートします。プライベートキーは安全に保存します。この方法を使用する場合は、高品質の乱数ジェネレーターを使用することをお勧めします。

AWS で生成された Amazon EC2 キーペアを使用することもできます。その場合は、インスタンスを初めて作成するときに、RSA キーペアのプライベートキーとパブリックキーの両方がお客様に提供されます。お客様は、Amazon EC2 キーペアのプライベートキーをダウンロードして安全に保管する必要があります。AWS ではプライベートキーを保存しません。プライベートキーをなくした場合は、新しいキーペアを生成する必要があります。

cloud-init サービスを使用する Amazon EC2 Linux インスタンスの場合、標準 AWS AMI から新しいインスタンスが起動されるときに、Amazon EC2 キーペアのパブリックキーが初期オペレーティングシステムユーザーの ~/.ssh/authorized_keys ファイルに追加されます。**~/.ssh/authorized_keys** ファイル。その後、そのユーザーは、正しい Amazon EC2 インスタンスユーザーの名前を ID として使用するようにクライアントを設定し (ec2-user など)、ユーザー認証用にプライベートキーファイルを提供することによって、SSH クライアントを使用して Amazon EC2 Linux インスタンスに接続できます。

ec2config サービスを使用する Amazon EC2 Windows インスタンスの場合、標準の AWS AMI から新しいインスタンスを起動すると、**ec2config** サービスによって、そのインスタンス用に新しいランダムな管理者パスワードが設定され、Amazon EC2 キーペアの対応するパブリックキーで暗号化されます。ユーザーは、AWS マネジメントコンソールまたはコマンドラインツールを使用して、パスワードを復号するための対応する Amazon EC2 プライベートキーを指定することで、Windows インスタンスのパスワードを取得できます。このパスワードと Amazon EC2 インスタンスのデフォルトの管理アカウントを使用して、Windows インスタンスに対する認証を行うことができます。

AWS では、Amazon EC2 のキーを管理したり、新たに起動した Amazon EC2 インスタンスに業界標準の認証を適用したりするのに役立つ、柔軟で実用的な一連のツールを用意しています。より高いセキュリティが必要な場合は、LDAP や Active Directory などの別の認証メカニズムを実装し、Amazon EC2 キーペア認証を無効にすることもできます。

データの保護

このセクションでは、AWS プラットフォームにおける保管時と転送時のデータの保護について説明します。ここでは、資産の特定と分類が完了し、それらの保護目標がリスクプロファイルに基づいて設定されていることを前提としています。

リソースへのアクセスの承認

ユーザーまたは IAM ロールが認証されると、承認されたリソースへのアクセスが許可されます。リソースの承認には、リソースの制御をユーザーが行えるようにするか、あるいはポリシーの設定を各ユーザーの設定よりも優先して適用するかに応じて、リソースポリシーまたは機能ポリシーのどちらかを使用します。

- **リソースポリシー**は、ユーザーがリソースを作成し、それらのリソースへのアクセスを他のユーザーに許可する場合に適したポリシーです。このモデルでは、ポリシーをリソースに直接アタッチし、そのリソースを使用できるユーザーと実行できる操作を定義します。リソースの制御はユーザーが行います。この方法により、IAM ユーザーにリソースへの明示的なアクセスを提供できます。ルート AWS アカウントは、そのアカウントで作成されたすべてのリソースの所有者となり、常にリソースポリシーを管理するためのアクセスが付与されます。また、リソースに対するアクセス権限を管理するための明示的なアクセスをユーザーに付与することもできます。
- **機能ポリシー** (IAM のドキュメントでは「ユーザーベースアクセス権限」と呼んでいます) は、企業全体のアクセスポリシーを適用する場合によく使用されます。機能ポリシーは、IAM ユーザーに直接割り当てられる場合と、IAM グループを使用して間接的に割り当てられる場合があります。また、実行時に適用されるロールに割り当てることもできます。機能ポリシーでは、ユーザーによる実行を許可または禁止する機能 (アクション) を定義します。リソースベースのポリシーのアクセス権限を明示的に否定することで、それらよりも優先して適用できます。

- IAM ポリシーは、特定のソースの IP アドレス範囲、または特定の日や時間など、何らかの条件に基づいてアクセスを制限する場合に使用できます。
- リソースポリシーと機能ポリシーは、実際は組み合わせて使用されます。各ユーザーに実際に適用されるアクセス権限は、リソースポリシーと直接またはグループメンバーシップを通じて付与された機能ポリシーのアクセス権限を組み合わせたものになります。

クラウドでの暗号化キーの保管と管理

暗号化を使用するセキュリティ対策にはキーが必要です。オンプレミスのシステムと同じように、クラウドでもキーを安全に保管することが不可欠です。

既存のプロセスを使用してクラウドで暗号化キーを管理できるほか、サーバー側の暗号化と AWS のキー管理および保管機能を利用することもできます。

独自のキー管理プロセスを使用する場合、さまざまな方法でキーマテリアルを保管および保護することができます。キーの保管には、ハードウェアセキュリティモジュールなど、不正操作を防止できるストレージを使用することを強くお勧めします。アマゾンウェブサービスでは、AWS CloudHSM という HSM サービスをクラウドで提供しています。また、オンプレミスにキーを保管する HSM を使用して、Amazon VPC への IPSec 仮想プライベートネットワーク (VPN) 接続や IPSec を使用した AWS Direct Connect など、安全なリンクを介してそれらのキーにアクセスする方法もあります。

オンプレミスの HSM または CloudHSM を使用して、データベースの暗号化、デジタル著作権管理 (DRM)、公開鍵基盤 (PKI)、認証と認可、ドキュメントの署名、トランザクション処理など、さまざまなユースケースや用途に対応できます。CloudHSM では、現在、SafeNet の Luna SA HSM を使用しています。Luna SA は、Federal Information Processing Standard (FIPS) 140-2 および Common Criteria EAL4+ の規格に準拠するように設計されており、業界標準の各種の暗号化アルゴリズムをサポートしています。

CloudHSM にサインアップすると、CloudHSM アプライアンスに対する専用のシングルテナントアクセスが提供されます。各アプライアンスは Amazon VPC でリソースとして表示されます。AWS ではなくお客様自身が CloudHSM の暗号ドメインを初期化し、管理してください。暗号ドメインは論理的かつ物理的なセキュリティの境界で、キーに対するアクセスを制限します。お客様のキーおよび CloudHSM で実行される操作を管理できるのは、お客様のみです。AWS の管理者は CloudHSM アプライアンスの状態を管理、保守、モニタリングしますが、暗号ドメインへのアクセス権はありません。暗号ドメインを初期化したら、CloudHSM が提供する API をアプリケーションが使用できるように、EC2 インスタンス上のクライアントを設定できます。

アプリケーションで、PKCS#11、MS CAPI、Java JCA/JCE (Java Cryptography Architecture/Java Cryptography Extensions) など、CloudHSM でサポートされる標準の API を利用することができます。CloudHSM クライアントでは、相互に認証される SSL 接続を使用して CloudHSM アプライアンスに接続することで、アプリケーションに API を提供し、それぞれの API 呼び出しを実装します。

CloudHSM を複数のアベイラビリティーゾーンに実装し、それらの間でレプリケーションを設定することで、可用性やストレージの耐障害性を高めることができます。

保管時のデータの保護

規制またはビジネス要件に従って、AWS の Amazon S3、Amazon EBS、Amazon RDS などのサービスで保管しているデータの保護を強化しなければならない場合があります。

表 7 に、AWS で保管時のデータの保護を実装する際の注意事項を示します。

課題	推奨される保護方法	戦略
偶発的な情報の開示	データを機密情報として扱い、アクセスできるユーザーを制限します。Amazon S3 などのサービスについては、AWS のアクセス権限を使用してリソースへのアクセスを管理します。Amazon EBS や Amazon RDS では、暗号化を使用して機密データを保護します。	アクセス権限 ファイル、パーティション、ボリューム、またはアプリケーションの各レベルでの暗号化
データの不整合	偶発的または意図的な変更によってデータの整合性が損なわれないようにするには、リソースアクセス権限を使用して、データを変更できるユーザーの範囲を制限します。リソースアクセス権限を使用した場合でも、権限があるユーザーによって誤って削除される可能性は残るため (権限があるユーザーの認証情報を使用したトロイの木馬による潜在的な攻撃も含む)、最小限の権限だけを付与するという原則に従うことが重要になります。メッセージ認証コード (SHA-1/SHA-2)、ハッシュメッセージ認証コード (HMAC)、デジタル署名、認証されている暗号化 (AES-GCM) などのデータ整合性チェックを実行して、データの整合性が損なわれないように保護します。データの不整合が見つかった場合は、バックアップまたはオブジェクトの以前のバージョン (Amazon S3 の場合) からデータを復元します。	アクセス権限 データ整合性チェック (MAC/HMAC/デジタル署名/認証されている暗号化) バックアップ バージョニング (Amazon S3)

過失による削除	正しいアクセス権限と最小特権のルールを使用することは、過失による削除や悪意のある削除に対する最善の防御策となります。Amazon S3 などのサービスでは、オブジェクトの削除に多要素認証を要求する MFA Delete を使用することによって、Amazon S3 オブジェクトへのアクセスを特権ユーザーのみに制限できます。データの不整合が見つかった場合は、バックアップまたはオブジェクトの以前のバージョン (Amazon S3 の場合) からデータを復元します。	アクセス許可バックアップのバージョニング (Amazon S3) MFA Delete (Amazon S3)
システム、インフラストラクチャ、ハードウェア、ソフトウェアの可用性	システム障害や自然災害が発生した場合は、バックアップやレプリカからデータを復元します。Amazon S3、Amazon DynamoDB などの一部のサービスでは、リージョン内の複数のアベイラビリティーゾーン間で自動的にデータのレプリケーションが実行されます。その他のサービスでは、レプリケーションやバックアップを設定する必要があります。	バックアップレプリケーション

表 7: 保管時のデータに対する脅威

お客様を取り巻く脅威の状況を分析し、表 1 で説明されている関連する防御手段を講じてください。資産マトリックスのサンプル資産保護のための ISMS 設計セクション

以下のセクションでは、AWS のさまざまなサービスで保管時のデータを保護するための設定方法について説明します。

Amazon S3 での保管時のデータの保護

Amazon S3 には、保管時のデータを保護するための数多くのセキュリティ機能が用意されています。これらの機能は、脅威の分析結果に応じて、使用するかどうかを決定できます。表 8 にこれらの機能の概要を示します。

Amazon S3 の機能	説明
アクセス権限	バケットレベルまたはオブジェクトレベルのアクセス権限を IAM ポリシーとともに使用することによって、不正アクセスからリソースを保護したり、情報開示、データの不整合や削除を防止したりすることができます。
バージョニング	Amazon S3 では、オブジェクトのバージョニングをサポートしています。バージョニングはデフォルトで無効になっています。バージョニングを有効にすると、オブジェクトを変更または削除するたびに新しいバージョンが保存され、必要に応じて、脅威にさらされたオブジェクトをそこから復元できます。
レプリケーション	Amazon S3 では、それぞれのリージョンにあるすべてのアベイラビリティーゾーンで各オブジェクトがレプリケートされます。レプリケーションでは、システム障害が発生した場合のデータやサービスの可用性を提供することはできますが、過失による削除やデータの不整合に対する保護は提供されません。–コピーが保存されているすべてのアベイラビリティーゾーンに、変更内容がレプリケートされます。Amazon S3 には、標準の冗長化オプションと低冗長化オプションが用意されています。これらは耐久性と価格が異なります。
バックアップ	Amazon S3 では、自動バックアップの代わりに、データのレプリケーションとバージョニングをサポートしています。ただし、アプリケーションレベルのテクノロジーを使用して、Amazon S3 に保存されているデータを、他の AWS リージョンやオンプレミスバックアップシステムにバックアップすることができます。
暗号化–サーバー側	Amazon S3 では、ユーザーデータのサーバー側での暗号化をサポートしています。サーバー側の暗号化はエンドユーザーに対して透過的です。AWS によって、各オブジェクトについて一意の暗号化キーが生成され、AES-256 を使用してオブジェクトが暗号化されます。次に、暗号化キー自体が、AES-256 を使用して、安全な場所に保存されているマスターキーによって暗号化されます。マスターキーは定期的にローテーションされます。

暗号化–クライアント側	クライアント側の暗号化では、お客様が独自の暗号化キーを作成して管理します。お客様が作成したキーは、クリアテキストで AWS にエクスポートされることはありません。アプリケーションは、Amazon S3 に送信する前にデータを暗号化し、Amazon S3 から受信した後にデータを復号化します。データは、お客様のみが知っているキーとアルゴリズムを使用して暗号化された形式で保存されます。データの暗号化には任意の暗号化アルゴリズムを使用でき、また対称キーと非対称キーのいずれも使用できますが、AWS が提供する Java SDK には Amazon S3 のクライアント側暗号化機能が含まれています。「参考資料と参考文献」 を参照して詳細を確認してください。

表 8: 保管時のデータを保護するための Amazon S3 の機能

Amazon EBS での保管時のデータの保護

Amazon EBS は、AWS の抽象ブロックストレージサービスです。Amazon EBS ボリュームはそれぞれ、新品のハードディスクのように、未フォーマットの raw モードで提供されます。お客様は、Amazon EBS ボリュームの分割、ソフトウェア RAID アレイの作成、選択したファイルシステムでのパーティションのフォーマットを行うことができ、最終的には Amazon EBS ボリューム上のデータを保護することができます。Amazon EBS ボリュームに対するこれらの決定やオペレーションはすべて、AWS オペレーションからは見えません。

Amazon EBS ボリュームは、Amazon EC2 インスタンスにアタッチできます。

表 9 は、Amazon EC2 インスタンスで実行しているオペレーティングシステムを使用して、保管時に Amazon EBS データを保護するための機能をまとめたものです。

Amazon EBS の機能	説明
レプリケーション	各 Amazon EBS ボリュームはファイルとして保存され、AWS によって冗長化のために EBS ボリュームの 2 つのコピーが作成されます。ただし、両方のコピーは同じアベイラビリティーゾーンに存在するため、Amazon EBS のレプリケーションはハードウェア障害には対応できますが、長時間の停電や災害対策を目的とした可用性ツールとしては適していません。アプリケーションレベルでデータをレプリケートするか、バックアップを作成すること (またはその両方) をお勧めします。
バックアップ	Amazon EBS は、特定の時点で Amazon EBS ボリュームに保存されているデータをキャプチャした、スナップショットを提供します。ボリュームが (システム障害などによって) 破損した場合や、ボリュームからデータが削除された場合に、スナップショットからボリュームを復元できます。 Amazon EBS スナップショットは AWS オブジェクトであり、IAM ユーザー、グループ、ロールに対してこのオブジェクトへのアクセス権限を割り当てることができます。これにより、承認されたユーザーのみが Amazon EBS バックアップにアクセスできます。
暗号化: Microsoft Windows EFS	AWS で Microsoft Windows Server を実行しており、さらに高いレベルのデータの機密性が必要である場合、暗号化ファイルシステム (EFS) を実装することによって、システムまたはデータパーティションに保存された機密データの保護を強化できます。EFS は NTFS ファイルシステムの拡張機能であり、ファイルやフォルダの透過的な暗号化を実現するとともに、Windows や Active Directory のキー管理機能と PKI を統合します。EFS で独自のキーを管理できます。
暗号化: Microsoft	Windows BitLocker は、Windows Server 2008 以降のオペレーティングシステムに含まれている、ボリューム (単一ドライブの場合はパーティション) 暗号化ソリューションです。BitLocker では以下を使用します。
Windows Bitlocker	AES 128 ビットおよび 256 ビット暗号化 デフォルトでは、BitLocker はキーを保存するためにトラステッドプラットフォームモジュール (TPM) を必要としますが、これは Amazon EC2 ではサポートされていません。ただし、パスワードを使用するように設定すると、BitLocker を使用して EBS ボリュームを保護できます。詳細については、次のホワイトペーパーを参照してください。「Amazon の 法人 IT チームが SharePoint 2010 をアマゾン ウェブサービスクラウドにデプロイ」

Amazon EBS の機能	説明
暗号化: Linux dm-crypt	カーネルバージョン 2.6 以降を実行している Linux インスタンスでは、dm-crypt を使用して、Amazon EBS ボリュームおよびスワップ空間で透過的なデータ暗号化を設定できます。キー管理には、さまざまな暗号や Linux Unified Key Setup (LUKS) を使用できます。
暗号化: TrueCrypt	TrueCrypt は、Amazon EBS ボリューム上で保管時のデータの透過的な暗号化を提供するサードパーティ製のツールです。TrueCrypt は、Microsoft Windows と Linux の両方のオペレーティングシステムをサポートしています。
暗号化と整合性認証: SafeNet ProtectV	SafeNet ProtectV は、Amazon EBS ボリュームのディスク全体の暗号化と AMI のプリブート認証を実現するサードパーティ製の製品です。SafeNet ProtectV は、データと基になるオペレーティングシステムのデータの機密性やデータ整合性認証を提供します。

表 9: 保管時のデータを保護するための Amazon EBS の機能

Amazon RDS での保管時のデータの保護

Amazon RDS は、Amazon EC2 と同様の安全なインフラストラクチャを活用します。Amazon RDS サービスを保護を追加せずに使用することはできますが、コンプライアンスやその他の目的で、保管時のデータの暗号化やデータ整合性認証が必要な場合は、アプリケーションレイヤーで保護を追加することも、SQL の暗号化関数を使用してプラットフォームレイヤーで保護を追加することもできます。

たとえば、アプリケーションレイヤーで保護を追加するには、機密性の高いデータベースフィールドをすべて暗号化する組み込みの暗号化関数を使用する方法や、データベースに保存する前にアプリケーションキーを使用する方法があります。アプリケーションでは、PKI インフラストラクチャによる対称暗号化や、マスター暗号化キーを提供するその他の非対称キーによる手法を使用してキーを管理できます。

プラットフォームで保護を追加するには、MySQL の暗号化関数を使用します。暗号化関数は、次のようにステートメントの形式で使用できます。

```
INSERT INTO Customers (CustomerFirstName,CustomerLastName) VALUES
(AES_ENCRYPT('John',@key), AES_ENCRYPT('Smith',@key);
```

プラットフォームレベルの暗号化キーは、アプリケーションレベルの暗号化キーと同様に、アプリケーションレベルで管理されます。表 10 に、Amazon RDS のプラットフォームレベルの保護オプションを示します。

Amazon RDS プラットフォーム	コメント
MySQL	MySQL の暗号化関数には、暗号化、ハッシュ、圧縮の機能が含まれます。詳細については、「https://dev.mysql.com/doc/refman/5.5/en/encryption-functions.html.」を参照してください。
Oracle	Oracle Transparent Data Encryption は、Amazon RDS for Oracle Enterprise Edition の、自分のライセンス使用 (BYOL) モデルでサポートされています。
Microsoft SQL	Microsoft Transact-SQL のデータ保護機能には、暗号化、署名、ハッシュが含まれます。詳細については、「http://msdn.microsoft.com/en- us/library/ms173744.」を参照してください。

表 10: Amazon RDS プラットフォームレベルでの保管時のデータの保護

SQL の範囲のクエリは、データの暗号化された部分には適用されないことに注意してください。たとえば、`CustomerFirstName` 列の内容がアプリケーションレイヤーまたはプラットフォームレイヤーで暗号化されている場合、このクエリでは「John」、「Jonathan」、「Joan」など、結果として予想される名前が返されません。

```
SELECT CustomerFirstName, CustomerLastName from Customers WHERE
CustomerName LIKE 'Jo%';”
```

次のような直接比較の場合は、`CustomerFirstName` が正確に「John」と一致するすべてのフィールドについて、適切に動作して予想される結果が返されます。

```
SELECT CustomerFirstName, CustomerLastName FROM Customers WHERE
CustomerFirstName = AES_ENCRYPT('John', @key);
```

範囲クエリは暗号化されていないフィールドに対しても機能します。たとえば、テーブル内の日付フィールドを暗号化しないことによって、範囲クエリで使用することができます。

一方向関数は、社会保障番号や一意の識別子として使用される類似の個人 ID などの個人識別情報を難読化するのに適切な方法です。個人識別情報の暗号化および復号を、それらを使用する前にアプリケーションまたはプラットフォームレイヤーで行えますが、キー付き HMAC-SHA1 などの一方向関数を使用して、個人識別情報を固定長のハッシュ値に変換する方が便利です。商用 HMAC での衝突は非常にまれであるため、個人識別情報の一意性は維持されます。ただし、HMAC を元の個人識別情報に戻すことはできないため、元の個人 ID が分かっており、同じキー付き HMAC 関数で処理する場合を除き、このデータから元の個人を特定することはできません。

すべてのリージョンで、Amazon RDS は透過的なデータ暗号化とネイティブネットワーク暗号化をサポートしています。これらはいずれも、Oracle Database 11g Enterprise Edition の Advanced Security オプションのコンポーネントです。Oracle Database 11g Enterprise Edition は、Amazon RDS for Oracle の、自分のライセンス使用 (BYOL) モデルで利用できます。これらの機能は追加料金なしで使用できます。

Oracle Transparent Data Encryption は、ストレージへの書き込み前にデータを暗号化し、ストレージからの読み取り時にデータを復号します。Oracle Transparent Data Encryption によって、Advanced Encryption Standard (AES) や Data Encryption Standard (Triple DES) などの業界標準の暗号化アルゴリズムを使用して、テーブルスペースや特定のテーブル列を暗号化できます。

Amazon Glacier での保管時のデータの保護

Amazon Glacier に保存されるすべてのデータは、サーバー側の暗号化を使用して保護されます。AWS では、Amazon Glacier の各アーカイブについて個別に一意の暗号化キーを生成し、AES-256 を使用してアーカイブを暗号化します。暗号化キー自体が暗号化されますが、これは、AES-256 を使用して、安全な場所に保存されているマスターキーによって行われます。マスターキーは定期的にローテーションされます。保管時の情報の保護をさらに強化する必要がある場合は、データを暗号化してから Amazon Glacier にアップロードすることができます。

Amazon DynamoDB での保管時のデータの保護

Amazon DynamoDB は AWS の共有サービスです。DynamoDB は保護を追加せずに使用できますが、標準 DynamoDB サービスに加えてデータ暗号化レイヤーを実装することもできます。範囲クエリへの影響などを含む、アプリケーションレイヤーでのデータの保護に関する考慮事項については、前のセクションを参照してください。

DynamoDB は数値、文字列、raw バイナリデータ型のフォーマットをサポートします。DynamoDB に暗号化されたフィールドを保存する場合のベストプラクティスは、raw バイナリフィールドまたは Base64 でエンコードされた文字列フィールドを使用することです。

Amazon EMR での保管時のデータの保護

Amazon EMR は、クラウドでのマネージド型サービスです。AWS では、Amazon EMR を実行するために必要な AMI が提供されます。カスタム AMI や独自の EBS ボリュームを使用することはできません。デフォルトでは、Amazon EMR インスタンスは保管時のデータを暗号化しません。

Amazon EMR クラスターでは、Amazon S3 と DynamoDB のいずれかを永続的なデータストアとして使用することがよくあります。Amazon EMR クラスターが起動すると、操作に必要なデータを永続的なストアから HDFS にコピーできます。また、Amazon S3 や DynamoDB から直接データを使用することもできます。

保管時のデータの機密性と整合性のレベルを向上させるには、表 11 に示されているような、いくつかの手法を使用できます。

要件	説明
Amazon S3 のサーバー側の暗号化–HDFS にコピーしない場合	データは Amazon S3 にのみ永続的に保存され、HDFS にはまったくコピーされません。Hadoop は Amazon S3 からデータをフェッチし、永続的なローカルコピーを作成せずに、データをローカルで処理します。 「Amazon S3 での保管時のデータの保護」 セクションで、Amazon S3 サーバー側暗号化に関する詳細について参照してください。
Amazon S3 のクライアント側の暗号化	データは Amazon S3 にのみ永続的に保存され、HDFS にはまったくコピーされません。Hadoop は Amazon S3 からデータをフェッチし、永続的なローカルコピーを作成せずに、データをローカルで処理します。クライアント側の復号を適用するには、カスタムシリアライザー/デシリアライザー (SerDe) を、Hive などの製品、または、Java Map Reduce ジョブ用の InputFormat とともに使用することができます。ファイルを分割できるようにするには、個々の行またはレコードごとに暗号化を適用します。 「Amazon S3 での保管時のデータの保護」 セクションで、Amazon S3 クライアント側暗号化に関する詳細について参照してください。

要件	説明
アプリケーションレベルの暗号化–ファイル全体を暗号化	データを Amazon S3 または DynamoDB に保存する際に、アプリケーションレベルで (たとえば、HMAC-SHA1 を使用して) データの暗号化、またはデータの整合性の保護が行えます。 データを復号するには、カスタム SerDe と Hive を使用するか、スクリプトやブートストラップアクションを使用して Amazon S3 からデータをフェッチして復号し、HDFS にロードしてから処理します。ファイル全体が暗号化されているため、マスターノードなど、単一ノードでこのアクションを実行する必要があります。S3Distcp などのツールを、特殊なコーデックとともに使用できます。
アプリケーションレベルの暗号化–個々のフィールドの暗号化/構造の維持	Hadoop では、JSON など、標準 SerDe を使用できます。データの復号は、Hadoop ジョブの Map ステージ中に実行でき、ストリーミングジョブ用のカスタム復号ツールによって標準入力/出力のリダイレクトを使用できます。
ハイブリッド	Amazon S3 のサーバー側の暗号化とクライアント側の暗号化、およびアプリケーションレベルの暗号化を組み合わせて使用することもできます。

表 11: Amazon EMR での保管時のデータの保護

Amazon ソフトウェアパートナー (Gazzang など) が、Amazon EMR で保管時と伝送中のデータを保護するための特別なソリューションを提供しています。

データとメディアの安全な廃棄

クラウドと従来のオンプレミス環境では、データを廃棄する方法が異なります。

AWS にクラウド内のデータの削除を依頼した場合、AWS は基になる物理メディアを廃棄しません。代わりに、ストレージブロックが未割り当てとしてマークされます。AWS は安全なメカニズムを使って、ブロックを他に再度割り当てます。ブロックストレージをプロビジョニングする場合、ハイパーバイザーまたは Virtual Machine Manager (VMM) によって、インスタンスの書き込み先のブロックが追跡されます。インスタンスがストレージのブロックに書き込むときに、前のブロックがゼロ設定された後、データのブロックで上書きされます。インスタンスが以前に書き込んだブロックからの読み取りを試行した場合、以前に保存したデータが返されます。インスタンスが以前に書き込んでいないブロックからの読み取りを試行すると、ハイパーバイザーはディスクにある以前のデータをゼロで埋めて、インスタンスにゼロを返します。

メディアが製品寿命に達したと AWS が判断した場合や、ハードウェア障害が発生した場合は、AWS は国防省 (DoD) 5220.22-M (『国家産業セキュリティプログラム運営マニュアル』) または NIST SP 800-88 (『媒体のサニタイズに関するガイドライン』) に詳述された技術を用い、廃棄プロセスの一環としてデータを破棄します。

クラウド内のデータの削除の詳細については、「AWS セキュリティプロセス」ホワイトペーパーを参照してください。(「参考資料と参考文献」を参照してください)。

法規制またはビジネス上の理由から安全なデータの廃棄をさらに厳格に管理する必要がある場合は、クラウドに保存されないカスタマー管理型のキーを使用して、保管時のデータの暗号化を実装できます。次に、前のプロセスに加えて、廃棄したデータの保護に使用していたキーを削除して、データを回復できないようにします。

伝送中のデータの保護

クラウドアプリケーションは、通常、インターネットなどのパブリックリンクで通信するため、クラウドでアプリケーションを実行する場合は伝送中のデータを保護することが重要になります。これには、クライアントとサーバーの間のネットワークトラフィックやサーバー間のネットワークトラフィックの保護が含まれます。

表 12 に、インターネットなどのパブリックリンクでの通信に関連する、一般的な懸念事項のリストを示します。

懸念事項	コメント	推奨される保護
偶発的な情報の開示	機密データへのアクセスは制限する必要があります。データがパブリックネットワークを経由する場合は、データが開示されないように暗号化によって保護する必要があります。	IPSec ESP や SSL/TLS (またはその両方) を使用して、伝送中のデータを暗号化します。
データの不整合	データが機密データであるかどうかに関係なく、意図的または偶発的な変更によってデータの整合性が損なわれていないことを確認できます。	IPSec ESP/AH や SSL/TLS (またはその両方) を使用してデータの整合性を認証します。

懸念事項	コメント	推奨される保護
ピアアイデンティティの漏洩/なりすまし/中間者	暗号化とデータ整合性認証は通信チャネルを保護するために重要です。接続のリモートエンドの ID を認証することも同じく重要です。リモートエンドがたまたま攻撃者または替え玉であり、対象の受信者への接続を中継している場合、チャネルを暗号化しても意味がありません。	IKE による IPSec を事前共有キーや X.509 証明書とともに使用して、リモートエンドを認証します。または、サーバーの共通名 (CN) や代替名 (AN/SAN) に基づくサーバー証明書認証とともに SSL/TLS を使用します。

表 12: 伝送中のデータに対する脅威

AWS のサービスでは、伝送中のデータを保護するために、IPSec と SSL/TLS の両方のサポートを提供しています。IPSec は、通常、ネットワークインフラストラクチャで、IP プロトコルスタックを拡張するプロトコルです。これにより、上位レイヤーのアプリケーションは、変更しなくても安全に通信を行うことができます。一方、SSL/TLS は、セッションレイヤーで動作します。サードパーティ製の SSL/TLS ラッパーもありますが、通常、アプリケーションレイヤーでのサポートも必要です。

以下のセクションでは、伝送中のデータの保護に関する詳細を説明します。

アプリケーションの管理と AWS パブリッククラウドサービスへの管理アクセス

AWS パブリッククラウドで実行中のアプリケーションにアクセスする場合、接続はインターネットを経由します。多くの場合、セキュリティポリシーでは、インターネットは安全ではない通信メディアと見なされ、伝送中のアプリケーションデータの保護が必要になります。

表 13 に、パブリッククラウドサービスにアクセスするときに伝送中のデータを保護するためのアプローチの概要を示します。

プロトコル/シナリオ	説明	推奨される保護方法
HTTP/HTTPS トラフィック (ウェブアプリケーション)	デフォルトでは、HTTP トラフィックは保護されていません。SSL/TLS による HTTP トラフィックの保護は、HTTPS としても知られている業界標準であり、ウェブサーバーやブラウザで広くサポートされています。 HTTP トラフィックには、ウェブページへのクライアントアクセスだけではなく、ウェブサービス (REST ベースのアクセス) も含まれていることがあります。	HTTPS (HTTP over SSL/TLS) をサーバー証明書認証とともに使用します。
HTTPS のオフロード (ウェブアプリケーション)	通常、特に機密データを扱う場合には、HTTPS の使用が推奨されますが、SSL/TLS の処理には、ウェブサーバーとクライアントの両方からの追加の CPU およびメモリリソースが必要になります。これにより、数千の SSL/TLS セッションを処理するために、ウェブサーバーに相当な負荷がかかる可能性があります。クライアントに対する影響はこれよりも小さく、限られた数の SSL/TLS 接続が終了するだけです。	Elastic Load Balancing で HTTPS の処理をオフロードすることによって、伝送中のデータを保護しながら、ウェブサーバーへの影響を最小限に抑えることができます。HTTP over SSL などのアプリケーションプロトコルを使用して、インスタンスへのバックエンド接続をさらに保護できます。

Remote Desktop Protocol (RDP) のトラフィック	パブリッククラウド内の Windows Terminal Services にアクセスするユーザーは、通常、Microsoft Remote Desktop Protocol (RDP) を使用します。 デフォルトでは、RDP 接続は基になる SSL/TLS 接続を確立します。	最適な保護を実現するには、なりすましや中間者攻撃を防ぐために、アクセス対象の Windows Server に対して、信頼された X.509 証明書が発行されている必要があります。デフォルトでは、Windows RDP サーバーは自己署名証明書を使用しますが、この証明書は信頼されていないため使用しないでください。
Secure Shell (SSH) トラフィック	SSH は、以下を確立するのに適したアプローチです。 Linux サーバーに対しての管理用の接続 SSH SSL と同様に、クライアントとサーバーの間に安全な通信チャネルを提供するプロトコルです。加えて、SSH はトンネリングもサポートしています。トンネリングは、SSH 上で X-Windows などのアプリケーションを実行しながら、伝送中のアプリケーションセッションを保護するために使用します。	特権を持たないユーザーアカウントを使用して SSH バージョン 2 を使用します。
データベースサーバーのトラフィック	クライアントやサーバーがクラウド内のデータベースにアクセスする必要がある場合、インターネットを経由することが必要になる可能性もあります。	最近のデータベースの多くは、ネイティブデータベースプロトコル用の SSL/TLS ラッパーをサポートしています。Amazon EC2 でデータベースサーバーを実行している場合は、このアプローチで伝送中のデータを保護することをお勧めします。Amazon RDS では、SSL/TLS のサポートを提供している場合があります。 「Amazon RDS に伝送中のデータの保護」セクションで、詳細について参照してください。

表 13: パブリッククラウドにアクセスする際の伝送中のアプリケーションデータの保護

AWS サービスを管理する際の伝送中のデータの保護

AWS マネジメントコンソールや AWS API を使用して、Amazon EC2 や Amazon S3 などの AWS のサービスを管理できます。サービス管理トラフィックの例としては、新しい Amazon EC2 インスタンスの起動、Amazon S3 バケットへのオブジェクトの保存、Amazon VPC でのセキュリティグループの修正などが挙げられます。

AWS マネジメントコンソールでは、AWS サービス管理トラフィックを保護するために、クライアントブラウザとコンソールサービスエンドポイントの間で SSL/TLS を使用します。トラフィックが暗号化され、データ整合性が認証されるとともに、クライアントブラウザは X.509 証明書を使用して、コンソールサービスエンドポイントの ID を認証します。SSL/TLS セッションがクライアントブラウザとコンソールサービスエンドポイントの間で確立されると、それ以降のすべての HTTP トラフィックは、SSL/TLS セッション内で保護されます。

代わりに、AWS API を使用すると、アプリケーションやサードパーティ製のツールから直接、または SDK や AWS コマンドラインツールを使用して、AWS のサービスを管理できます。AWS API は HTTPS 上のウェブサービス (REST) です。クライアントと特定の AWS サービスエンドポイントの間に SSL/TLS セッションが確立されると、使用される API によって、REST エンベロープやユーザーペイロードを含め、それ以降のすべてのトラフィックは SSL/TLS セッション内で保護されます。

Amazon S3 に伝送中のデータの保護

AWS サービス管理トラフィックと同様に、Amazon S3 へのアクセスは HTTPS を通じて行われます。これには、すべての Amazon S3 サービス管理リクエストおよびユーザーペイロード (Amazon S3 で保存/取得するオブジェクトの内容など) や関連するメタデータが含まれます。

AWS サービスコンソールを使用して Amazon S3 を管理する場合、クライアントブラウザとサービスコンソールエンドポイントの間に SSL/TLS による安全な接続が確立されます。それ以降のすべてのトラフィックはこの接続内で保護されます。

Amazon S3 API を直接的または間接的に使用する場合、クライアントと Amazon S3 エンドポイントの間に SSL/TLS 接続が確立され、それ以降のすべての HTTP およびユーザーペイロードのトラフィックは保護されたセッション内でカプセル化されます。

Amazon RDS に伝送中のデータの保護

Amazon EC2 インスタンスから同じリージョン内の Amazon RDS に接続している場合、AWS ネットワークのセキュリティを利用できますが、インターネットから接続している場合は、SSL/TLS を使用して保護を追加する必要があります。

SSL/TLS によって、サーバーの X.509 証明書によるピア認証、データ整合性認証、およびクライアントサーバー接続のデータ暗号化が提供されます。

SSL/TLS は、現在、Amazon RDS MySQL インスタンスおよび Microsoft SQL インスタンスへの接続でサポートされています。どちらの製品についても、アマゾンウェブサービスは MySQL または Microsoft SQL リスナーに関連付けられた単一の自己署名証明書を提供します。この自己署名証明書をダウンロードし、信頼された証明書として指定できます。これによって、ピア ID 認証が提供され、サーバー側での中間者攻撃やなりすまし攻撃を防止できます。SSL/TLS によって、クライアントとサーバーの間の通信チャネルのネイティブ暗号化とデータ整合性認証が提供されます。AWS 上のすべての Amazon RDS MySQL インスタンスで同じ自己署名証明書が使用され、AWS 上のすべての Amazon RDS Microsoft SQL インターフェイスで別の単一の自己署名証明書が使用されるため、ピア ID 認証では、個々のインスタンスの認証は提供されません。SSL/TLS による個々のサーバーの認証が必要な場合は、Amazon EC2 とセルフマネージド型リレーショナルデータベースサービスを活用する必要があります。

Oracle Native Network Encryption 用の Amazon RDS では、データベースのデータの入出力時にデータが暗号化されます。Oracle Native Network Encryption によって、AES や Triple DES などの業界標準の暗号化アルゴリズムを使用して、Oracle Net Services で伝送されるネットワークトラフィックを暗号化できます。

Amazon DynamoDB に伝送中のデータの保護

同じリージョン内の他の AWS サービスから DynamoDB に接続している場合、AWS ネットワークのセキュリティを利用できますが、インターネット経由で DynamoDB に接続している場合は、HTTP over SSL/TLS (HTTPS) を使用して DynamoDB サービスエンドポイントに接続する必要があります。DynamoDB へのアクセスおよびインターネット経由でのすべての接続において、HTTP を使用しないでください。

Amazon EMR に伝送中のデータの保護

Amazon EMR には多くのアプリケーション通信パスが含まれており、それぞれの通信パスについて、伝送中のデータの保護メカニズムが個別に必要です。表 14 では、通信パスと推奨される保護のアプローチの概要を示します。

Amazon EMR のトラフィックのタイプ	**説明**	**推奨される保護方法**
Hadoop ノード間	Hadoop マスター、ワーカー、およびコアノードはすべて、独自のプレーン TCP 接続を使用して相互に通信します。ただし、Amazon EMR 上のすべての Hadoop ノードは同じアベイラビリティーゾーン内に存在し、物理的レイヤーやインフラストラクチャレイヤーでセキュリティ標準によって保護されます。	すべてのノードが同じ施設内に存在しているため–通常、追加の保護は必要ありません。
Hadoop クラスターと Amazon S3 の間	Amazon EMR では、DynamoDB と Amazon EC2 の間で HTTPS を使用してデータを送信します。詳細については、「Amazon S3 に伝送中のデータの保護」セクションを参照してください。	デフォルトでは、HTTPS が使用されます。
Hadoop クラスターと Amazon DynamoDB 間	Amazon EMR では、Amazon S3 と Amazon EC2 の間で HTTPS を使用してデータを送信します。詳細については、「Amazon DynamoDB に伝送中のデータの保護」セクションを参照してください。	デフォルトでは、HTTPS が使用されます。

Amazon EMR のトラフィックのタイプ	説明	推奨される保護方法
Hadoop クラスターへのユーザーまたはアプリケーションのアクセス	オンプレミスのクライアントまたはアプリケーションは、スクリプトを使用して、インターネット経由で Amazon EMR クラスターにアクセスできます。(SSH ベースのアクセス)、REST、Thrift や Avro などのプロトコル。	アプリケーションへのインタラクティブなアクセスや、SSH 内での他のプロトコルのトンネリングには、SSH を使用します。 Thrift、REST、または Avro が使用されている場合は、SSL/TLS を使用します。
Hadoop クラスターへの管理アクセ	Amazon EMR クラスター管理者は、通常、SSH を使用してクラス	Amazon EMR マスターノードに対して SSH を使用します。

表 14: Amazon EMR に伝送中のデータの保護

オペレーティングシステムとアプリケーションのセキュリティによる保護

AWS 責任分担モデルによって、オペレーティングシステムとアプリケーションのセキュリティを管理します。Amazon EC2 は、真に仮想的なコンピューティング環境を提供します。これにより、ウェブサービスインターフェイスを使用して、さまざまなオペレーティングシステムのインスタンスを、事前にロードされたカスタムアプリケーションとともに起動できます。オペレーティングシステムやアプリケーションのビルドを標準化し、単一の安全なビルドリポジトリでオペレーティングシステムやアプリケーションのセキュリティを一元管理できます。セキュリティの要件に合わせて、事前に設定した AMI をビルドしてテストできます。

推奨事項には以下が含まれます。

- ルート API アクセスキーとシークレットキーを無効にする
- セキュリティグループを使用して、制限された IP 範囲からのインスタンスへのアクセスを制限する
- ユーザーマシンの .pem ファイルをパスワードで保護
- 誰かが退職したり、アクセスの必要がなくなった場合に、インスタンス上の承認されたキーファイルからのキーを削除する
- 認証情報 (DB、アクセスキー) を更新する
- IAM ユーザーのアクセスアドバイザー、または、IAM ユーザーが前回使用したアクセスキーを使用して、最小特権チェックを定期的に実行する
- 拠点ホストを使用して、制御と可視性を強化する

このセクションは、AMI のセキュリティ強化標準の包括的なリストを示すことを目的としていません。業界で受け入れられている、システムのセキュリティ強化標準のソースには、次のようなものがあります (ただし、これらに限定されません)。

- Center for Internet Security (CIS)
- 国際標準化機構 (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- 米国国立標準技術研究所 (NIST)

すべてのシステムコンポーネントの設定標準を作成することをお勧めします。これらの標準によって、既知のセキュリティの脆弱性がすべて解決され、業界で受け入れられたシステムのセキュリティ強化標準との一貫性が維持されていることを確認します。

公開された AMI がベストプラクティスに違反していることが分かった場合、または AMI を実行しているお客様に重大なリスクを生じさせた場合、AWS はパブリックカタログから AMI を削除し、発行者と AMI を実行しているお客様に調査の結果を通知するための手段を講じる権利を留保します。

カスタム AMI の作成

組織の特定の要件を満たす独自の AMI を作成し、内部 (プライベート) または外部 (パブリック) で使用できるように公開できます。AMI の発行者は、本稼働環境で使用するマシンイメージの初期のセキュリティ体制に対する責任を負います。AMI に対して適用するセキュリティコントロールは特定の時点で有効であり、動的なものではありません。プライベート AMI はお客様のビジネスのニーズに合わせてどのようにでも設定でき、AWS の適正利用規約の違反にはなりません。詳細については、「アマゾン ウェブサービスの適正利用規約 – http://*aws.amazon.com/aup/*.」を参照してください。

ただし、AMI から起動するユーザーがセキュリティの専門家ではない場合があるため、一定の最小限セキュリティ標準を満たしておくことをお勧めします。

AMI を公開する前に、公開するソフトウェアが関連するセキュリティパッチを適用した最新の状態であることを確認し、表 15 に示されているクリーンアップとセキュリティ強化のタスクを実行します。

エリア	推奨されるタスク
安全でないアプリケーションの無効化	ネットワーク上でクリアテキストでユーザーを認証するサービスやプロトコル、およびその他の安全でないサービスやプロトコルを無効にします。
公開範囲の最小化	起動時に必要不可欠ではないネットワークサービスを無効にします。管理サービス (SSH/RDP) および不可欠なアプリケーションで必要なサービスのみを開始する必要があります。

エリア	推奨されるタスク
認証情報の保護	すべての AWS の認証情報をディスクや設定ファイルから安全に削除します。
認証情報の保護	任意のサードパーティの認証情報をディスクや設定ファイルから安全に削除します。
認証情報の保護	すべての追加の証明書やキーマテリアルをシステムから安全に削除します。
認証情報の保護	インストールされているソフトウェアがデフォルトの内部アカウントやパスワードを使用していないことを確認します。
良好なガバナンスの使用	システムがアマゾンウェブサービスの適正利用規約に違反していないことを確認します。違反の例としては、SMTP オープンリレーやプロキシサーバーなどがあります。詳細については、「アマゾンウェブサービス の適正利用規約– http://*aws.amazon.com/aup/*.」を参照してください。

表 15: AMI を公開する前のクリーンアップタスク

表 16 および 17 に、追加のオペレーティングシステム固有のクリーンアップタスクを示します。表 16 に、Linux AMI をセキュリティで保護するためのステップを示します。

エリア	セキュリティ強化アクティビティ
安全なサービス	パブリックキー認証のみを許可するように sshd を設定します。**[PubkeyAuthentication]** を **[Yes]** に、**[PasswordAuthentication]** を **[No]** に **sshd_config** で設定します。
安全なサービス	インスタンス作成時に一意の SSH ホストキーを生成します。AMI が **cloud-init** を使用する場合、AMI によってこれが自動的に処理されます。
認証情報の保護	すべてのユーザーアカウント用のパスワードを、ログインに使用できないようにし、デフォルトのパスワードを持たないようにするために、削除して無効にします。各アカウントについて、**passwd -l <USERNAME>** を実行します。
認証情報の保護	すべてのユーザーの SSH パブリックキーとプライベートキーのペアを安全に削除します。
データの保護	機密データを含んでいるすべてのシェル履歴およびシステムログファイルを安全に削除します。

表 16: Linux/UNIX AMI の保護

表 17 に、Windows AMI をセキュリティで保護するためのステップを示します。

エリア	セキュリティ強化アクティビティ
認証情報の保護	インスタンスの作成時に、有効なすべてのユーザーアカウントに対して新しくランダムに生成されたパスワードが設定されるようにします。ブート時に管理者アカウントについてこれを実行するように EC2 Config サービスを設定できますが、イメージをバンドルする前に明示的にこの作業を行う必要があります。
認証情報の保護	ゲストアカウントが無効であることを確認します。
データの保護	Windows のイベントログを消去します。
認証情報の保護	AMI が Windows ドメインの一部でないことを確認します。
公開範囲の最小化	ファイル共有、印刷スプーラー、RPC など、必須ではないのにデフォルトで有効になっている Windows サービスを有効にしないでください。

表 17: Windows AMI の保護

ブートストラッピング

強化した AMI をインスタンス化した後も、ブートストラップアプリケーションを使用してセキュリティコントロールを修正し更新することができます。一般的なブートストラップアプリケーションとしては、Puppet、Chef、Capistrano、Cloud-Init、Cfn-Init などがあります。また、サードパーティ製のツールを使用しないで、ブートストラップ用のカスタム Bash スクリプトまたは Microsoft Windows PowerShell スクリプトを実行することもできます。

検討対象となるブートストラップアクションを以下にいくつか挙げます。

- セキュリティソフトウェア更新プログラムで、AMI のパッチレベルを超えた最新のパッチ、サービスパック、重要な更新プログラムをインストールします。

- 初期アプリケーションパッチで、AMI でキャプチャされた現在のアプリケーションレベルビルドを超えたアプリケーションレベルの更新プログラムをインストールします。
- コンテキスト依存データと設定により、本稼働用、テスト用、DMZ/インターネット用など、起動環境に固有の設定をインスタンスに適用できます。
- リモートセキュリティモニタリングシステムと管理システムにインスタンスを登録します。

パッチの管理

AMI およびライブインスタンスのパッチ管理は、お客様が行う必要があります。パッチ管理を制度として導入し、手続きを文書化して整備することをお勧めします。

オペレーティングシステムと主要アプリケーション向けにサードパーティ製パッチ管理システムを利用することもできますが、すべてのソフトウェアとシステムコンポーネントについて在庫目録を作成し、各システムにインストールされたセキュリティパッチの一覧を最新のベンダーセキュリティパッチ一覧と比較して、最新のベンダーパッチがインストールされていることを確認することをお勧めします。

新しいセキュリティ上の脆弱性を特定して、その脆弱性のリスクをランク付けするプロセスを導入します。最低でも、最も重大で最もリスクが高い脆弱性は「高」とランク付けします。

パブリック AMI のセキュリティ管理

パブリックに共有する場合は、AMI に重要な認証情報を残さないよう注意します。詳しくは、パブリック AMI を安全に共有し利用する方法に関するこのチュートリアルを参照してください。
http://aws.amazon.com/articles/0155828273219400

マルウェアからのシステムの保護

ウィルス、ワーム、トロイの木馬、ルートキット、ボットネット、スパムなどの脅威から従来のインフラストラクチャを保護する場合と同様に、クラウドのシステムも保護します。

個々のインスタンスにマルウェアが感染した場合と、クラウドシステム全体に感染した場合の影響を理解することが大切です。ユーザーが、故意または無意識に、Linux または Windows システム上でプログラムを実行すると、その実行プログラムはそのユーザーの権限を入手します (場合によっては、別のユーザーの権限を借用します)。コードは、コードを起動したユーザーが権限を持つ任意のアクションを実行できます。ユーザーは信頼できるコードだけを実行するように注意する必要があります。

信頼できないコードをシステムで実行すると、そのシステムはもはや自分のシステムではなく、他人のシステムになります。管理権限を持つスーパーユーザーまたはユーザーが、信頼できないプログラムを実行すると、そのプログラムが実行されたシステムはもはや信頼することができなくなります。悪意のあるコードによってオペレーティングシステムの一部が変更されたり、ルートキットがインストールされたり、システムにアクセスするためのバックドアが仕込まれたりする可能性があります。悪意のあるコードは、データを削除したり、データの整合性を損ねたり、サービスの可用性を脅かしたり、秘かにまたはあからさまな方法で第三者に情報を開示したりするかもしれません。

感染したコードがインスタンスで実行されたと考えてみましょう。感染したインスタンスがシングルサインオン環境の一部である場合、または、インスタンス間でのアクセスについて暗黙的な信頼モデルが存在している場合、感染は個々のインスタンスを超えて、急速にシステム全体とその外部に広まります。感染がこの規模になると、たちまちデータ漏洩、データやサービスの障害につながり、会社の評判を損なうことになります。たとえば、第三者に対するサービスに障害が発生したり、クラウドリソースを過剰に消費したりした場合は、直接の金銭的な被害が生じることもあり得ます。お客様がマルウェアの脅威を管理しなくてはいけません。

表 18 は、マルウェア対策の一般的な手法をいくつかまとめたものです。

Factor	一般的な手法
信頼できない AMI	信頼できる AMI からのみインスタンスを起動します。信頼できる AMI としては、AWS が提供する標準の Windows および Linux AMI と、信頼できるサードパーティ製 AMI があります。標準の信頼できる AMI から独自のカスタム AMI を派生させる場合は、すべての追加ソフトウェアとそれに適用する設定もまた信頼できる必要があります。 信頼できないサードパーティ製 AMI を起動すると、クラウド環境全体が危険にさらされ汚染される可能性があります。
信頼できないソフトウェア	信頼できるソフトウェア業者の信頼できるソフトウェアだけをインストールして実行します。信頼できるソフトウェア業者とは、業界で評判が良く、責任を持てる安全な方法でソフトウェアを開発しており、悪意のあるコードがソフトウェアパッケージに混入することを許さない業者です。オープンソースソフトウェアも信頼できるソフトウェアになり得ますが、自前で実行可能ファイルをコンパイルできる必要があります。ソースコードに悪意がないことを確認するために、入念なコードレビューを実施することを強くお勧めします。 信頼できるソフトウェア業者は、多くの場合、コード署名用の証明書を使ってソフトウェアに署名するか、製品の MD5 または SHA-1 署名を提示して、ダウンロードしたソフトウェアの健全性を確認できるようにしています。

Factor	一般的な手法
信頼できないソフトウェアリポジトリ	信頼できる場所から信頼できるソフトウェアをダウンロードします。インターネットやネットワーク上にあるさまざまなソフトウェアサイトでは、実際には、評判の良い正当なソフトウェアパッケージの内部にマルウェアを埋め込んで配布していることがあります。そのような信頼できないサイトでも、マルウェアを含む派生パッケージの MD5 または SHA-1 署名を提示していることがありますが、そのような署名は信頼できません。 ユーザーが信頼できるソフトウェアをインストールして利用できるように、独自の内部ソフトウェアリポジトリをセットアップすることをお勧めします。インターネットのさまざまな場所からソフトウェアをダウンロードしてインストールするという危険な行為はしないよう、ユーザーに強く要請します。
最小権限の原則	ユーザーに付与する権限は、ユーザーがタスクを実行するのに必要な最小限の権限とします。そうすることで、感染した実行ファイルをユーザーが誤って起動した場合でも、インスタンスとクラウドシステム全体に対する影響を最小限に抑えることができます。
パッチ適用	外部向けのシステムと内部システムに最新のセキュリティレベルのパッチを適用します。ワームは、多くの場合、ネットワークのパッチが適用されていないシステムを介して広がります。
ボットネット	従来のウィルスであれ、トロイの木馬であれ、ワームであれ、個々のインスタンスを超えて感染が広まり、多数のインスタンスに感染する場合は、ボットネットを構築する悪意のあるコードが含まれている可能性があります。ボットネットとは、攻撃者がリモートでコントロールできる感染したホストのネットワークです。ボットネットの感染を防ぐには、ここまでの推奨事項をすべて実行します。
スパム	感染したシステムを利用して、攻撃者は大量の迷惑メール (スパム) を送信することができます。AWS には、Amazon EC2 インスタンスが送信できる E メー
	SMTP オープンリレーは避けてください。この機能は、スパムを広めるために利用でき、AWS の適正利用規約違反になる可能性もあります。詳細については、「アマゾン ウェブ サービスの利用規定 http://aws.amazon.com/aup/」を参照してください。
ウィルス/スパム対策ソフトウェア	使用中のシステムで評判の良い最新のウィルスおよびスパム対策ソリューションを必ず利用します。

Factor	一般的な手法
ホスト方式の IDS ソフトウェア	多くの AWS 利用者は、オープンソース製品の OSSEC のような、ファイル整合性チェック機能やルートキット検出ソフトウェアを含む、ホスト方式の IDS ソフトウェアをインストールしています。このような製品を使用して、重要なシステムファイルやフォルダを分析し、信頼性を示すチェックサムを計算し、これらのファイルが変更されていないか定期的にチェックして、変更された場合はシステム管理者に警告します。

表 18: マルウェア対策の手法

インスタンスが感染した場合、ウィルス対策ソフトウェアが感染を検出して、ウィルスを除去できることがあります。その場合は、最も安全で広く推奨されている手法をお勧めします。それは、システムデータをすべて保存し、システム、プラットフォーム、アプリケーションの実行可能ファイルをすべて信頼できるソースから再インストールして、データはバックアップからのみ復元するという方法です。

侵害と迷惑行為の軽減

AWS は、お客様がソリューションを構築するグローバルインフラストラクチャを提供します。ソリューションの多くはインターネットにつながっています。お客様のソリューションは、残りのインターネットコミュニティに害をなさないような方法で動作する必要があります。つまり、迷惑行為を避ける必要があります。

迷惑行為とは、AWS のお客様のインスタンスまたはその他のリソースの外部で観察される、悪意のある行動、有害な行動、違法な行動、他のインターネットサイトに害をなす可能性のある行動です。

AWS はお客様と協力して、AWS リソースからの疑わしい悪意のある活動を検出して対処します。リソースからの想定外の行動または疑わしい行動は、AWS リソースが侵害された可能性があることを示し、これはお客様の業務に対する潜在的なリスクとなります。

AWS は以下のメカニズムを利用して、お客様のリソースからの迷惑行為を検出します。

- AWS 内部イベントモニタリング
- AWS ネットワーク空間に対する外部セキュリティインテリジェンス
- AWS リソースに対するインターネット迷惑行為に関する苦情

AWS の迷惑行為対応チームは、AWS で実行されている悪意のある迷惑プログラムまたは詐欺プログラムを積極的にモニターしシャットダウンしていますが、迷惑行為に関する苦情の大多数は AWS で正当な業務を行っているお客様に対するものです。意図しない迷惑行為の一般的な原因を以下に挙げます。

- **侵害されたリソース。**たとえば、パッチが適用されていない Amazon EC2 インスタンスがウィルスに感染してボットネットエージェントになることがあります。
- **意図しない迷惑行為。**たとえば、あまりに精力的なウェブクローラーを DOS 攻撃とみなすインターネットサイトがあります。
- **二次的な迷惑行為。**たとえば、AWS のお客様の提供するサービスのエンドユーザーが Amazon S3 のパブリックバケットにマルウェアファイルを投稿する可能性があります。
- **間違った苦情。**インターネットユーザーが正当な活動を迷惑行為と誤解することがあります。

AWS は AWS のお客様と協力して、迷惑行為の防止、検出、軽減と、将来の再発防止に取り組むことをお約束いたします。お客様が AWS から迷惑行為の警告を受け取った場合、お客様のセキュリティスタッフと運用スタッフはただちに問題を調査する必要があります。対応が遅れると、他のインターネットサイトに被害が広がり、お客様の評判が低下し、法的な責任を負うこともあり得ます。さらに重要なことは、関係する迷惑リソースが悪意のあるユーザーによって侵害されており、その状態を無視することによりお客様の業務に対する被害が拡大する可能性があるという点です。

AWS リソースを使用した悪意のある活動、違法な活動、有害な活動は、AWS の適正利用規約に違反し、アカウントが停止されることがあります。詳細については、「アマゾンウェブサービスの利用規定 http://*aws.amazon.com/aup/*」を参照してください。インターネットコミュニティによって正常と評価されるサービスを維持することは、お客様の責任です。報告された迷惑行為に AWS のお客様が対処できない場合、AWS はその AWS アカウントを停止して、AWS プラットフォームとインターネットコミュニティの健全性を守ります。

表 19 に、迷惑行為に対応する際に役立つベストプラクティスを示します。

ベストプラクティス	説明
AWS からの迷惑行為の連絡を無視しません。	迷惑行為が申し立てられると、AWS はただちに E メール通知を'お客様の登録 E メールアドレスに送信します。迷惑行為警告 E メールに返信して、AWS の迷惑行為対応チームと簡単に情報交換することができます。通信内容はすべて、将来参照できるように AWS の迷惑行為追跡システムに保存されます。 AWS の迷惑行為対応チームは、苦情の内容をお客様が理解できるよう支援いたします。AWS はお客様に協力して、迷惑行為を軽減し防止します。アカウントの停止は、迷惑行為を止めるために AWS の迷惑行為対応チームがとる最後の手段です。 AWS は、問題を緩和し懲罰的な対応を回避するためにお客様と協力します。しかし、お客様は、迷惑行為の警告に対応し、悪意のある活動を止めるために対策をとり、将来の再発を防ぐ必要があります。インスタンスとアカウントがブロックされる主な理由は、お客様の対応がないことです。
セキュリティのベストプラクティスに従います。	リソース侵害に対する最高の防止策は、本文書で概要を示したセキュリティのベストプラクティスに従うことです。AWS にはクラウド環境の強力な防御策を構築するのに役立つセキュリティツールが用意されていますが、自前のデータセンター内のサーバーと同様に、セキュリティのベストプラクティスに従う必要があります。最新のソフトウェアパッチの適用、ファイアウォールまたは Amazon EC2 セキュリティグループによるネットワークトラフィックの制限、ユーザーに対する最小限のアクセス権限の付与など、シンプルな防御慣行を一貫して採用してください。

ベストプラクティス	説明
侵害を軽減します。	コンピューティング環境が侵害されている場合、または感染している場合は、以下の手順に従って安全な状態を回復することをお勧めします。 • 既知の侵害された Amazon EC2 インスタンスまたは AWS リソースは安全でないと考えてください。Amazon EC2 インスタンスが、アプリケーションの利用法では説明できないトラフィックを生み出している場合、そのインスタンスはおそらく悪意のあるソフトウェアに侵害されているか感染しています。そのインスタンスをシャットダウンし完全にリビルドして、安全な状態に戻します。物理世界では完全な新規再起動は大変ですが、クラウド環境ではこれが最初のリスク緩和手法です。 • 根本原因を探るには、侵害されたインスタンスに対するフォレンジック分析が必要になることがあります。このような調査は、よく訓練されたセキュリティ専門家のみが実施します。また、感染したインスタンスは隔離して、調査中に被害と感染が広がるのを防ぎます。 Amazon EC2 インスタンスを隔離して調査するために、非常に制限の強いセキュリティグループをセットアップすることができます。たとえば、ある単一 IP アドレスからの SSH または RDP インバウンドトラフィックを許可する以外はすべてのポートを閉じると、そのアドレスからフォレンジック調査者が安全にインスタンスを調査できます。 また、感染したインスタンスの Amazon EBS オフラインスナップショットを作成して、そのオフラインスナップショットをフォレンジック調査に回して深く分析することもできます。 AWS は、インスタンスやその他のリソース内のプライベート情報にアクセスすることはできません。そのため、アプリケーションアカウントの乗っ取りのような、ゲストオペレーティングシステムやアプリケーションレベルのセキュリティ侵害は検出できません。お客様が自前のツールを使って情報 (アクセスログ、IP トラフィックログ、その他の属性など) を記録していない場合、AWS はそのような情報を過去にさかのぼって提供することはできません。非常に詳細なインシデント調査とリスク緩和の作業は、お客様の責任です。 侵害された Amazon EC2 インスタンスを回復するために行う必要のある最後の手順は、主要な業務データのバックアップ、感染したインスタンスの完全終了、そして完全に新しいリソースとしての再起動です。 将来の侵害を防ぐために、新たに起動したインスタンスのセキュリティ管理環境を見直すことをお勧めします。最新のソフトウェアパッチの適用やファイアウォールによる制限など、シンプルな対策が大いに役立ちます。

ベストプラクティス	説明
セキュリティ用の連絡 E メールアドレスを設定します。	AWS の迷惑行為対応チームは、E メールを使用して迷惑行為の警告を通知します。デフォルトで、この E メールは登録された E メールアドレスに送信されますが、大企業の場合、対応専用の E メールアドレスを作成した方が便利なことがあります。追加の E メールアドレスはお客様の [**Personal Information**] ページの [**Configure Additional Contacts**] で設定できます。

表 19: 迷惑行為軽減のベストプラクティス

その他のアプリケーションセキュリティ慣行の採用

以下に、オペレーティングシステムとアプリケーション向けに、セキュリティに関する追加の一般的なベストプラクティスをいくつか示します。

- 新しい AMI を作成する前、または、新しいアプリケーションをデプロイする前に、パスワード、SNMP コミュニティ文字列、セキュリティ設定などのベンダー指定のデフォルト値を必ず変更します。
- 不要なユーザーアカウントを削除するか無効にします。
- Amazon EC2 インスタンスごとに導入する主要機能は 1 つだけにして、異なるセキュリティレベルを必要とする機能が、同じサーバーに混在しないようにします。たとえば、ウェブサーバー、データベースサーバー、DNS はそれぞれ別のサーバーに導入します。
- システムが機能するために必要となる、必須で安全なサービス、プロトコル、デーモンなどのみを有効にします。インスタンスとシステム全体のセキュリティリスクが増大するため、不可欠ではないサービスはすべて無効にします。

- スクリプト、ドライバー、フィーチャー、サブシステム、EBS ボリュームなどの不要な機能と不要なウェブサーバーはすべて無効にするか削除します。

セキュリティのベストプラクティスを念頭に置いてすべてのサービスを設定します。必要なサービス、プロトコル、デーモンのセキュリティ機能を有効にします。Telnet のように比較的安全性の低いサービスよりも、ユーザー/ピア認証、暗号化、データ整合性認証のためのセキュリティ機構を内蔵した SSH のようなサービスを選択します。ファイル転送には、FTP のように安全でないプロトコルではなく、SSH を使用します。安全性の低いプロトコルやサービスを使用せざるを得ない場合は、ネットワーク層で通信チャネルを保護する IPSec やその他の仮想プライベートネットワーク (VPN) 技術、または、アプリケーション層でネットワークを保護する GSS-API、Kerberos、SSL、TLS などによって、追加のセキュリティ層を導入します。

どの組織でもセキュリティガバナンスは重要ですが、セキュリティポリシーの適用がベストプラクティスです。可能な限り、セキュリティポリシーとガイドラインを遵守するようにシステムセキュリティパラメータを設定して、乱用を防止します。

管理者がシステムとアプリケーションにアクセスする場合は、強力な暗号化のメカニズムを使ってコンソール以外の管理者アクセスを暗号化します。SSH、ユーザーおよびサイト間 IPSec VPN、SSL/TLS のような技術を利用して、リモートシステム管理をさらに安全にします。

インフラストラクチャの保護

このセクションでは、AWS プラットフォームでインフラストラクチャサービスを保護するための推奨事項を示します。

Amazon Virtual Private Cloud (VPC) の使用

Amazon Virtual Private Cloud (VPC) を使うと、AWS パブリッククラウド内にプライベートクラウドを作成できます。

お客様の Amazon VPC はそれぞれお客様が割り当てた IP アドレス空間を使用します。Amazon VPC では (RFC 1918 の推奨に従って) プライベート IP アドレスを使用して、インターネットに直接ルーティングできないプライベートクラウドと関連ネットワークをクラウドに構築することができます。

Amazon VPC では、プライベートクラウドを他のお客様から分離できるだけでなく、インターネットからレイヤー 3 (ネットワーク層の IP ルーティング) を分離することもできます。表 20 は Amazon VPC でアプリケーションを保護するオプションを示しています。

課題	説明	推奨される保護方法
インターネットのみ	Amazon VPC は、オンプレミスまたはそれ以外のインフラストラクチャのどれにも接続されていません。オンプレミスまたはそれ以外に追加インフラストラクチャが存在する場合も存在しない場合もあります。 インターネットユーザーからの接続を許可する必要がある場合は、インバウンドアクセスを必要とする Amazon VPC インスタンスのみに Elastic IP アドレス (EIP) を割り当てることで、インバウンドアクセスを許可することができます。セキュリティグループまたは NACL を使用することで、特定のポートと送信元 IP アドレス範囲のみにインバウンド接続をさらに制限することもできます。 インターネットからのインバウンドトラフィックの負荷を分散できる場合、EIP は必要ありません。インスタンスは Elastic Load Balancing の背後に配置できます。 インターネットに対するアウトバウンドアクセスの場合、たとえば、ソフトウェアの更新を取得したり、Amazon S3 などの AWS パブリックサービスのデータにアクセスする場合、NAT インスタンスを使用して送信接続のマスカレード機能を実現できます。EIP は必要ありません。	SSL/TLS を使用してアプリケーショントラフィックと管理トラフィックを暗号化するか、カスタムユーザー VPN ソリューションを構築します。 パブリックおよびプライベートサブネットでのルーティングとサーバー配置を慎重に計画します。 セキュリティグループと NACL を使用します。

課題	説明	推奨される保護方法
インターネット経由の IPSec	AWS には、VPC 向けに業界標準の障害に強い IPSec ターミネーションインフラストラクチャが用意されています。お客様は、オンプレミスまたは他の VPN インフラストラクチャから Amazon VPC への IPSec トンネルを確立できます。 IPSec トンネルは AWS とお客様のインフラストラクチャエンドポイントとの間に確立されます。クラウドまたはオンプレミスで実行されるアプリケーションに修正はまったく必要なく、ただちに IPSec による伝送中のデータ保護の恩恵を受けることができます。	IKEv1 を使用してプライベート IPSec 接続を確立し、標準の AWS VPN 機能 (Amazon VPC VPN ゲートウェイ、カスタマーゲートウェイ、VPN 接続) を使用して IPSec を確立します。 別の方法として、顧客専用の VPN ソフトウェアインフラストラクチャをクラウドとオンプレミスに確立します。
IPSec を使わない AWS Direct Connect	AWS Direct Connect を使うと、専用リンクを経由した AWS とのプライベートピアリングにより、インターネットを使わないで Amazon VPC に対する接続を確立できます。この場合、データ保護要件に応じて、IPSec を使用しないこともできます。	データ保護要件によっては、プライベートピアリング経由の追加の保護が必要ない場合もあります。
IPSec を使用した AWS Direct Connect	AWS Direct Connect リンク経由の IPSec を使用してエンドツーエンドの保護を追加することができます。	上記の「インターネット経由の IPSec」を参照してください。
ハイブリッド	これらの方法を組み合わせて利用することを検討します。使用する接続方法ごとに適切な保護の仕組みを採用します。	

表 20: Amazon VPC でのリソースアクセス

Amazon VPC-IPSec または VPC-AWS Direct Connect を活用すると、オンプレミスまたは他のホスト型インフラストラクチャを安全な方法で Amazon VPC リソースとシームレスに統合できます。どちらの方法でも、IPSec 接続により伝送中のデータが保護される一方で、IPSec または AWS Direct Connect リンク上の BGP は Amazon VPC およびオンプレミスルーティングドメインと統合されます。ネイティブのネットワークセキュリティメカニズムをサポートしないアプリケーションを含む任意のアプリケーションで、透過的な統合が実現されます。

VPC-IPSec はアプリケーションを業界標準の方法で透過的に保護しますが、VPC-IPSec リンク経由の SSL/TLS のような追加の保護メカニズムレベルを使用する必要のある場合があります。

詳細については、Amazon VPC 接続オプションのホワイトペーパーを参照してください。

セキュリティゾーニングとネットワークセグメンテーションの使用

セキュリティ要件が異なると、必要なセキュリティ管理も異なります。インフラストラクチャを、類似したセキュリティ管理を適用するゾーンに分割することが、セキュリティのベストプラクティスです。

AWS の土台となるインフラストラクチャの大半は AWS の運用チームとセキュリティチームによって管理されていますが、お客様は独自のオーバーレイインフラストラクチャコンポーネントを構築することができます。Amazon VPC、サブネット、ルーティングテーブル、セグメント化/ゾーン化されたアプリケーション、および、カスタムサービスインスタンス (ユーザーリポジトリ、DNS、時刻サーバーなど) が、AWS の管理するクラウドインフラストラクチャを補完しています。

通常、ネットワークエンジニアリングチームはセグメンテーションを別のインフラストラクチャ設計コンポーネントと解釈して、ネットワーク中心のアクセスコントロールとファイアウォールルールを適用してアクセスを管理します。しかし、セキュリティゾーニングとネットワークセグメンテーションは、2 つの異なる概念です。ネットワークセグメントは、単純に 1 つのネットワークを別のネットワークから分離します。一方、セキュリティゾーンは、共通のコントロールを使うセキュリティレベルが類似したシステムコンポーネントのグループを作成します。

AWS では、以下のアクセスコントロール方法を使ってネットワークセグメントを構築できます。

- **Amazon VPC** を使って、ワークロードまたは組織エンティティごとに、分離したネットワークを定義します。
- **セキュリティグループ**を使って、機能とセキュリティ要件が類似したインスタンスに対するアクセスを管理します。セキュリティグループとは、許可され確立されたあらゆる TCP セッションまたは UDP 通信チャネルで、双方向のファイアウォールルールを有効にするステートフルファイアウォールです。
- **ネットワークアクセスコントロールリスト** (NACL) を使うと、IP トラフィックのステートレス管理が可能になります。NACL は TCP および UDP セッションに制約されませんが、IP プロトコル (たとえば GRE、IPSec ESP、ICMP) をきめ細かく制御でき、送信元/送信先 IP アドレスおよび TCP と UDP のポート単位で制御することもできます。NACL はセキュリティグループと連携して動作し、トラフィックがセキュリティグループに到達する前でもトラフィックを許可または拒否できます。

- **ホストベースのファイアウォール**を使って、各インスタンスに対するアクセスを制御します。
- **脅威保護レイヤー**をトラフィックフローに作成して、すべてのトラフィックがゾーンを経由するようにします。
- **他のレイヤーにアクセスコントロール**を適用します (たとえば、アプリケーションレイヤーやサービスレイヤー)。

従来の環境で、ファイアウォールのような中央セキュリティ実施システムを介してトラフィックをルーティングするには、別個のブロードキャストエンティティを表す別個のネットワークセグメントが必要です。AWS クラウドのセキュリティグループという概念では、この要件が時代遅れになります。セキュリティグループはインスタンスの論理的なグループ分けであり、インスタンスが存在するサブネットにかかわらず、インスタンスにインバウンドおよびアウトバウンドトラフィックルールを適用することもできます。

セキュリティゾーンを作成するには、ネットワークセグメントごとに追加のコントロールが必要であり、多くの場合、以下のようなコントロールを含みます。

- **共有アクセスコントロール** – 中央の Identity and Access Management (IDAM) システム。フェデレーションも可能ですが、これは多くの場合、IAM から分離されることに注意してください。
- **共有監査ログ記録** – 共有ログ記録は、イベント分析と相関、およびセキュリティイベントの追跡に必要です。
- **共有データ分類** – 詳しくは、「表 1: 資産のマトリックスのサンプル」資産を保護するための ISMS の設計セクションを参照してください。

- **共有管理インフラストラクチャ** – ウィルス/スパム対策システム、パッチ適用システム、パフォーマンスモニタリングシステムなど、多様なコンポーネント。
- **共有セキュリティ (機密性/整合性) 要件** – 多くの場合、データ分類と組み合わせて検討されます。

ネットワークセグメンテーションとセキュリティゾーニングの要件を評価するには、以下の質問に答えてください。

- ゾーン間通信を制御しますか ?ネットワークセグメンテーションツールを使ってセキュリティゾーン A と B の間の通信を管理できますか ?通常、セキュリティグループ、ACL、ネットワークファイアウォールのようなアクセスコントロール要素は、セキュリティゾーン間に壁を構築する必要があります。Amazon VPC はデフォルトでゾーン間の分離壁を構築します。
- 業務要件に応じて IDS/IPS/DLP/SIEM/NBAD システムを使って、ゾーン間通信をモニタリングできますか ?アクセスのブロックとアクセスの管理は、異なる用語です。セキュリティゾーン間の通信には穴があるため、ゾーン間には洗練されたセキュリティモニタリングツールが必要になります。AWS インスタンスは水平方向に拡張できるため、各インスタンスをオペレーティングシステムレベルでゾーニングして、ホストベースのセキュリティモニタリングエージェントを活用することができます。
- ゾーンごとにアクセスコントロール権限を適用できますか ?ゾーニングの利点の 1 つは、送信アクセスを制御できる点です。技術的には、Amazon S3 や Amazon SMS のリソースポリシーのように、リソース別にアクセスを制御できます。

- 専用の管理チャネル/ロールを使用して各ゾーンを管理できますか ？ 特権アクセスのためのロールベースアクセスコントロールは、一般的な要件です。IAM を使用して、グループとロールを AWS に作成し、さまざまな特権レベルを作成することができます。また、アプリケーションユーザーとシステムユーザーについても類似の方法を使用することができます。Amazon VPC に基づくネットワークの新しい主要機能の 1 つは、複数の Elastic Network Interface のサポートです。セキュリティエンジニアは、デュアルホームインスタンスを使用して管理用オーバーレイネットワークを作成できます。
- ゾーンごとに機密性ルールと整合性ルールを適用できますか ?ゾーンごとの暗号化、データ分類、DRM は、単に全体的なセキュリティ体制を強化します。セキュリティ要件がセキュリティゾーンごとに異なる場合は、データセキュリティ要件も異なるはずです。また、各セキュリティゾーンで、キーを更新する異なる暗号化オプションを使用することは、常に優れたポリシーと言えます。

AWS には柔軟なセキュリティーゾーニングオプションが用意されています。セキュリティエンジニアとアーキテクトは、以下の AWS 機能を活用して、Amazon VPC アクセスコントロールに従って、分離したセキュリティゾーン/セグメントを AWS に構築できます。

- サブネット単位のアクセスコントロール
- セキュリティグループ単位のアクセスコントロール
- インスタンス単位のアクセスコントロール (ホストベース)
- Amazon VPC 単位のルーティングブロック
- リソース単位のポリシー (S3/SNS/SMS)
- ゾーン単位の IAM ポリシー

- ゾーン単位のログ管理
- ゾーン単位の IAM ユーザー、管理ユーザー
- ゾーン単位のログフィード
- ゾーン単位の管理チャネル (ロール、インターフェイス、マネジメントコンソール)
- ゾーン単位の AMI
- ゾーン単位のデータストレージリソース (Amazon S3 バケットまたは Glacier アーカイブ)
- ゾーン単位のユーザーディレクトリ
- ゾーン単位のアプリケーション/アプリケーションコントロール

伸縮自在のクラウドインフラストラクチャと自動デプロイを利用すると、すべての AWS リージョンに対して同じセキュリティコントロールを適用できます。反復可能で均質なデプロイによりセキュリティ体制全体が改善されます。

ネットワークセキュリティの強化

責任共有モデルに従って、AWS は、データセンターネットワーク、ルーター、スイッチ、ファイアウォールのようなインフラストラクチャコンポーネントを安全な方法で設定します。クラウドでシステムに対するアクセスを制御する責任、Amazon VPC 内のネットワークセキュリティおよび安全なインバウンド/アウトバウンドネットワークトラフィックを設定する責任はお客様にあります。

リソースへのアクセスにユーザー認証とアクセス権限を適用することは不可欠ですが、これだけでは、攻撃者がネットワークレベルのアクセスを取得して、正規ユーザーを偽装しようとする試みは防げません。ユーザーのネットワーク上の場所に基づいてアプリケーションとサービスに対するアクセスを制御すると、セキュリティレイヤーが追加されます。
たとえば、強力なユーザー認証機能を備えたウェブベースのアプリケーションは、ソーストラフィックを特定の範囲の IP アドレスに限定する IP アドレスベースのファイアウォールや、セキュリティ上の暴露リスクを制限しアプリケーションの潜在的な攻撃対象領域を最小限に抑える侵入防止システムの恩恵も受けることができます。

AWS クラウドにおけるネットワークセキュリティのベストプラクティスを以下に挙げます。

- 常にセキュリティグループを使用します。セキュリティグループは、ハイパーバイザーレベルで動作する Amazon EC2 インスタンスのステートフルファイアウォールです。複数のセキュリティグループを 1 つのインスタンスと 1 つの ENI に適用することができます。
- ネットワーク ACL を使ってセキュリティグループを強化します。ネットワーク ACL はステートレスですが、高速かつ効率的にアクセスを制御できます。ネットワーク ACL はインスタンス特有ではないため、セキュリティグループに加えて、コントロールレイヤーを増やすことができます。ACL 管理とセキュリティグループ管理には職掌分散を適用することができます。
- 他のサイトに対する信頼できる接続のために、IPSec または AWS Direct Connect を使用します。Amazon VPC に基づくリソースがリモートネットワーク接続を必要とする場合は、仮想ゲートウェイ (VGW) を使用します。

- データの機密性と整合性、および通信している当事者の身元を保証するために、伝送中のデータを保護します。
- 大規模なデプロイの場合、ネットワークセキュリティをレイヤーに分けて設計します。ネットワークセキュリティを保護する単一のレイヤーを作成する代わりに、外部、DMZ、内部の各レイヤーにセキュリティネットワークを適用します。
- VPC フローログでは、VPC のネットワークインターフェイス間を行き来する IP トラフィックに関する情報をキャプチャできるようになるため、さらに可視性が向上します。

お客様がやり取りする AWS のサービスエンドポイントの多くは、ネイティブのファイアウォール機能またはアクセスコントロールリストを備えていません。AWS では、最先端のネットワークレベルおよびアプリケーションレベルの管理システムを使用して、このようなエンドポイントを監視し保護します。IAM ポリシーを使用すると、リクエストの送信元 IP アドレスに基づいて、リソースへのアクセスを制限することができます。

周辺システムの保護：ユーザーリポジトリ、DNS、NTP

オーバーレイセキュリティ管理は、安全なインフラストラクチャを土台としている場合にのみ効果があります。DNS クエリトラフィックはこの種の管理を示す良い例です。DNS システムが適切に保護されていない場合、DNS クライアントのトラフィックが傍受され、クエリおよび応答の DNS 名がなりすまされる可能性があります。なりすましは、基本的な管理がなされていないインフラストラクチャに対する単純ですが効率的な攻撃です。SSL/TLS は保護機能を強化できます。

一部の AWS のお客様は、安全な DNS サービスである Amazon Route 53 を利用しています。内部 DNS が必要な場合は、カスタム DNS ソリューションを Amazon EC2 インスタンスに導入することができます。DNS は、ソリューションインフラストラクチャに不可欠な要素であり、そのためセキュリティ管理計画でも重要な要素になります。すべての DNS システムは、その他の重要なカスタムインフラストラクチャコンポーネントと同様に、以下の管理を適用する必要があります。

一般的な管理	説明
管理レベルアクセスの分離	ロールの分離とアクセスコントロールを導入して、サービスへのアクセスを制限します。多くの場合、アプリケーションアクセス、または、インフラストラクチャの他の部分に対するアクセスに必要なアクセスコントロールから分離します。
モニタリング、アラート、監査証跡	正規の活動と不正な活動のログを記録し監視します。
ネットワークレイヤーアクセスコントロール	ネットワークアクセスを、それを必要とするシステムのみに制限します。可能な場合は、すべてのネットワークレベルのアクセス試行に対してプロトコルを強制的に適用します (つまり、NTP および DNS にカスタム RFC 標準を強制的に適用します)。
セキュリティパッチが適用された最新の安定したソフトウェア	ソフトウェアにパッチが適用されており、既知の脆弱性などのリスクにさらされていないことを確認します。
継続的なセキュリティテスト (評価)	インフラストラクチャが定期的にテストされていることを確認します。
他のあらゆるセキュリティ管理プロセスの導入	周辺システムが、サービス固有のカスタムセキュリティ管理に加えて、情報セキュリティ管理システム (ISMS) のベストプラクティスに従っていることを確認します。

表 21: 周辺システムの管理

DNS に加えて、他のインフラストラクチャサービスも特定の管理を必要とする場合があります。

集中管理されたアクセスコントロールは、リスク管理に不可欠です。IAM サービスは、AWS 向けにロールベースのアイデンティティおよびアクセス管理機能を提供しますが、AWS には、オペレーティングシステムとアプリケーション向けに Active Directory や LDAP、RADIUS のようなエンドユーザーリポジトリが用意されていません。その代わり、お客様は、Authentication Authorization Accounting (AAA) サーバーまたは時には周辺データベーステーブルとともに、ユーザーの識別と認証のシステムを確立します。ユーザープラットフォームとアプリケーションを対象としたすべてのアイデンティティおよびアクセス管理サーバーは、セキュリティ上、重要であり、特別な注意が必要です。

時刻サーバーも重要なカスタムサービスです。ログのタイムスタンプや証明書の検証など、多くのセキュリティ関連トランザクションに欠かすことができません。中央管理された時刻サーバーを利用して、すべてのシステムを同じ時刻サーバーに同期することが重要です。Payment Card Industry (PCI) Data Security Standard (DSS) では時刻同期に関する優れた方法が提案されています。

- 時刻同期技術が実装され最新状態であることを確認します。
- 正しい時刻を組織内で入手、配布、保管するプロセスを見直し、システムコンポーネントのサンプルについて時刻関連のシステムパラメータ設定を確認します。
- 指定された中央時刻サーバーのみが外部ソースから時刻信号を受け取り、外部ソースからの時刻信号は国際原子時または協定世界時 (UTC) に基づいていることを確認します。

- 指定された中央時刻サーバーが互いにピア接続して正確な時刻を保持し、他の内部サーバーは中央時刻サーバーからのみ時刻を受け取ることを確認します。
- システム設定と時刻同期設定をレビューして、時刻データにアクセスするビジネス上の必要性が認められているユーザーにのみ時刻データへのアクセスが制限されていることを確認する。
- システム設定と時刻同期設定およびプロセスをレビューして、重要なシステムの時刻設定への変更がログ記録、モニタリング、およびレビューされていることを確認する。
- 業界が認定している特定の外部ソースからの時刻の更新をタイムサーバーに適用できることを確認する。(これにより、悪意のある個人がクロックを変更することを防止できます)。(対称キーで暗号化された更新を受け取るように設定することも、更新されるクライアントマシンの IP アドレスを指定するアクセスコントロールリストを作成することもできます。これにより、内部タイムサーバーの不正使用が防止されます)。

カスタムインフラストラクチャのセキュリティの検証は、クラウドにおけるセキュリティの管理に不可欠な要素です。

脅威保護レイヤーの構築

多層セキュリティがネットワークインフラストラクチャを保護するためのベストプラクティスであると多くの組織が考えています。クラウドでは、Amazon VPC、ハイパーバイザーレイヤーにおける暗黙的ファイアウォールルール、ネットワークアクセスコントロールリスト、セキュリティグループ、ホストベースのファイアウォール、および IDS/IPS システムを組み合わせて、ネットワークセキュリティを確保するための階層型ソリューションを構築できます。

セキュリティグループ、NACL、およびホストベースのファイアウォールは多くの顧客のニーズには対応できますが、徹底した防御が必要な場合は、ネットワークレベルのセキュリティコントロールアプライアンスをデプロイする必要があります。これはインラインで行う必要があり、これによりトラフィックがアプリケーションサーバーなどの最終送信先に転送される前に遮断され、分析されます。

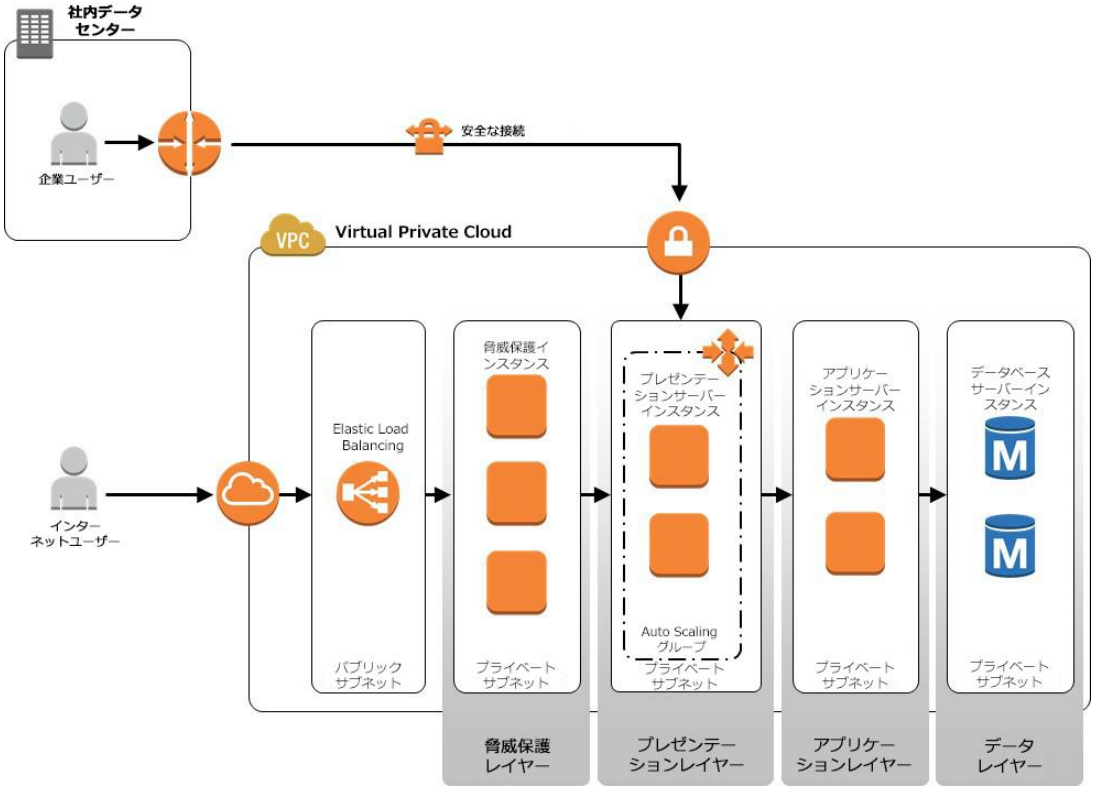

図 6: クラウドにおける階層型ネットワーク防御

インライン脅威保護テクノロジーの例としては以下のようなものがあります。

- Amazon EC2 インスタンスにインストールされたサードパーティーのファイアウォールデバイス (別名ソフトブレード)
- 統合脅威管理 (UTM) ゲートウェイ

- 侵入防止システム
- データ損失管理ゲートウェイ
- 異常検出ゲートウェイ
- 持続的標的型攻撃検出ゲートウェイ

Amazon VPC インフラストラクチャの以下の主要な機能が脅威保護レイヤーテクノロジーのデプロイをサポートしています。

- **多重ロードバランサーレイヤーのサポート:** 脅威保護ゲートウェイを使用してウェブサーバー、アプリケーションサーバー、またはその他の重要なサーバーのクラスターのセキュリティを確保する場合、スケーラビリティが重要な課題となります。AWS リファレンスアーキテクチャーでは、脅威管理と内部サーバーの負荷分散および高可用性のために外部および内部ロードバランサーをデプロイすることが重要視されています。Elastic Load Balancing または独自のカスタムロードバランサーインスタンスを多層設計に活用できます。ステートフルなゲートウェイのデプロイを実行するには、ロードバランサーレベルでセッションの永続性を管理する必要があります。
- **複数の IP アドレスのサポート:** いくつかのインスタンス (たとえばウェブサーバー、メールサーバー、アプリケーションサーバー) で構成されるプレゼンテーションレイヤーを脅威保護ゲートウェイが保護する場合、これらの複数のインスタンスは 1 つのセキュリティゲートウェイを多対 1 の関係で使用する必要があります。AWS は、単一のネットワークインターフェイスでの複数の IP アドレスの使用をサポートしています。

- **複数の Elastic Network Interface (ENI) のサポート:** 脅威保護ゲートウェイはデュアルホーム接続である必要があり、多くの場合、ネットワークの複雑さに応じて複数のインターフェイスを必要とします。ENI の概念に基づいて、AWS では複数の異なるインスタンスタイプでの複数のネットワークインターフェイスをサポートしているため、マルチゾーンセキュリティ機能のデプロイができます。

レイテンシーや複雑さなどのアーキテクチャー上の制約によってインライン脅威管理レイヤーの実装ができない場合は、以下のいずれかの代替案を選択できます。

- **分散型脅威保護ソリューション:** このアプローチでは、脅威保護エージェントをクラウドの個々のインスタンスにインストールします。中央脅威管理サーバーは、ログ収集、分析、相関、アクティブな脅威応答のためにすべてのホストベースの脅威管理エージェントと通信します。
- **オーバーレイネットワーク脅威保護ソリューション:** GRE トンネルや vtun インターフェイスなどのテクノロジーを使用する Amazon VPC を基盤として、または一元管理されているネットワークトラフィック分析と侵入検知システムに別の ENI のトラフィックを転送することによって、オーバーレイネットワークを構築します。これにより、アクティブまたはパッシブな脅威応答が可能になります。

セキュリティのテスト

すべての ISMS では、セキュリティコントロールとポリシーの有効性を定期的にレビューする必要があります。新しい脅威および脆弱性に対するコントロールの効率性を保証するには、インフラストラクチャが攻撃から保護されていることをお客様が確認する必要があります。

既存のコントロールを検証するには、テストを行う必要があります。AWS のお客様は、さまざまなテストアプローチに取り組む必要があります。

- **外部脆弱性評価:** インフラストラクチャとそのコンポーネントに関する知識がほとんどあるいはまったくないサードパーティがシステムの脆弱性を評価します。
- **外部侵入テスト:** システムに関する知識がほとんどあるいはまったくないサードパーティがコントロールされた環境でアクティブに侵入を試みます。
- **アプリケーションとプラットフォームの内部グレー/ホワイトボックスレビュー:** システムに関する知識を部分的または十分に持っているテスターが、配備されているコントロールの効率性を検証したり、アプリケーションとプラットフォームに既知の脆弱性があるかどうかを評価したりします。

AWS 適正利用規約では、AWS クラウドで許可または禁止されている行動を規定し、セキュリティの侵害とネットワークの不正使用について定義しています。AWS ではクラウドにおけるインバウンドとアウトバウンドの侵入テストの両方がサポートされていますが、侵入テストを実施するにはアクセス権限をリクエストする必要があります。詳細については、「アマゾンウェブ サービスの適正利用規約 – http://*aws.amazon.com/aup/*」を参照してください。

リソースの侵入テストをリクエストするには、AWS 脆弱性侵入テストリクエストフォームを提出します。テストするインスタンスに関連付けられている認証情報を使用して AWS マネジメントコンソールにログインしている必要があります。ログインしていない場合、フォームに情報が正しく入力されません。サードパーティの侵入テストの場合は、ユーザーがフォームに入力し、AWS が承認した後、サードパーティに通知する必要があります。

フォームには、テストするインスタンスに関する情報や予想されるテストの開始日時と終了日時を入力し、侵入テストおよびテストに適切なツールの使用に関する諸条件に同意する必要があります。AWS ポリシーでは、m1.small または t1.micro のテストは許可されていません。インスタンスタイプフォームを提出すると、リクエストの受領を確認する通知が 1 営業日以内に送信されます。

追加のテストを行うためにさらに時間が必要な場合は、承認メールに返信する形でテスト期間の延長を申請できます。リクエストごとに個別の承認プロセスが行われます。

メトリクスの管理と向上

コントロールの有効性の測定は、それぞれの ISMS に不可欠なプロセスです。メトリクスでは、コントロールによって環境がどれほど効果的に保護されているかを確認できます。通常、リスク管理は定性的および定量的なメトリクスに基づいて行われます。表 22 は、測定および向上のためのベストプラクティスをまとめたものです。

ベストプラクティス	改善
手順とその他のコントロールのモニタリングおよびレビュー	• 処理の結果でエラーを迅速に検出する • 試行および実行されたセキュリティ侵害やインシデントを迅速に特定する • 管理を有効にして、ユーザーに委任された、または情報テクノロジーによって実装されたセキュリティアクティビティが想定どおりに実行されているかどうかを判断する • セキュリティイベントを検出して、指標の使用によってセキュリティインシデントを防止するのに役立つ • セキュリティ侵害を解決するために取られた措置が効果的であったかどうかを判断する
ISMS の有効性の定期的なレビュー	• セキュリティ監査、インシデント、有効性測定の結果だけではなく、あらゆる関係者からの提案およびフィードバックを考慮する • ISMS がポリシーと目的に適合していることを確認する • セキュリティコントロールをレビューする
コントロールの有効性の測定	• セキュリティ要件が満たされていることを確認する
定期的なリスク評価レビュー	• 以下を考慮して残留リスクと特定された許容可能なレベルのリスクをレビューする • 組織、テクノロジー、ビジネス目標とプロセス、特定された脅威の変更 • 実装されたコントロールの有効性 • 法的または規制環境の変更、変更された契約上の義務、社会的風土の変更などの外部イベント
内部 ISMS 監査	• 第一者監査 (内部監査) は、社内の目的のために組織自体によって、または組織に代わって行われます。
定期的な管理レビュー	• スコープが適切なままであることを確認する • ISMS プロセスにおける改善点を特定する
セキュリティ計画の更新	• モニタリングとレビューのアクティビティで判明したことを考慮する • ISMS の有効性またはパフォーマンスに影響を与える可能性のあるアクションとイベントを記録する

表 22: メトリクスの測定および向上

DoS & DDoS 攻撃の緩和と保護

インターネットアプリケーションを実行している組織は、競合他社、活動家、または個人によるサービス妨害 (DoS) 攻撃または分散サービス妨害 (DDoS) 攻撃の標的となるリスクを認識しています。リスクプロファイルは、ビジネスの性質、最新のイベント、政治情勢、テクノロジーの公開によって異なります。緩和および保護の技術は、オンプレミスで使用されているものと似ています。

DoS/DDoS 攻撃の保護と緩和について懸念がある場合は、AWS プレミアムサポートサービスに登録することを強くお勧めします。これにより、AWS の環境における攻撃の緩和または進行中のインシデントを阻止するプロセスで AWS サポートサービスが事前および事後にサポートを提供するようにできます。

Amazon S3 などの一部のサービスでは共有インフラストラクチャを使用します。これは、複数の AWS アカウントが Amazon S3 インフラストラクチャコンポーネントの同じセットでデータにアクセスし、データを保存するということです。この場合、抽象化されたサービスへの DoS/DDoS 攻撃が、複数のお客様に影響する可能性があります。AWS では、AWS から抽象化されたサービスへの DoS/DDoS 攻撃に対する緩和コントロールと保護コントロールの両方を提供し、そのような攻撃が発生した場合のお客様への影響を最小限に抑えます。そのようなサービスに対する追加の DoS/DDoS 保護を用意する必要はありませんが、このホワイトペーパーに記載されているベストプラクティスに従うことをお勧めします。

Amazon EC2 などのその他のサービスは共有物理インフラストラクチャを使用しますが、ユーザーはオペレーティングシステム、プラットフォーム、および顧客データを管理することが期待されます。このようなサービスの場合、連携して効果的な DDoS の緩和と保護を提供する必要があります。

AWS では AWS プラットフォームに対する DoS/DDoS 攻撃を緩和および阻止するために独自の技術が使用されています。ただし、実際のユーザートラフィックへの干渉を回避するため、責任共有モデルに従って、AWS では緩和を提供せず、また個々の Amazon EC2 インスタンスに影響を与えるネットワークトラフィックをアクティブにブロックしません。過剰なトラフィックが予想され、それが無害なものか、DoS/DDoS 攻撃の一部であるかどうかを判断できるのはユーザーのみです。

クラウドにおける DoS/DDoS 攻撃を緩和するために使用できる技術は多数ありますが、通常の状況でシステムパラメータを取り込むセキュリティとパフォーマンスのベースラインを確立することを強くお勧めします。この際、1 日に 1 回、1 週間に 1 回、1 年に 1 回といったビジネスに適用できるパターンを検討することもできます。統計モデルや行動モデルなどの一部の DoS/DDoS 保護技術では、特定のベースラインの通常のオペレーションパターンと比較することによって異常を検出できます。たとえば、1 日の特定の時刻におけるウェブサイトへの同時セッションの数が通常は 2,000 である場合、現在の同時セッションの数がその 2 倍 (4,000) を超えると Amazon CloudWatch と Amazon SNS を使用してアラームがトリガーされるように設定できます。

クラウドにおいてセキュリティを確立するときも、オンプレミスのデプロイに適用されるものと同じ要素を考慮します。

表 23 は、クラウドにおける DoS/DDoS 攻撃の緩和と保護のための一般的なアプローチをまとめたものです。

手法	説明	DoS/DDoS 攻撃からの保護
ファイアウォール: セキュリティグループ、ネットワークアクセスコントロールリスト、ホストベースのファイアウォール	従来のファイアウォール技術は、潜在的な攻撃者にとっての攻撃対象領域を制限し、攻撃元と攻撃先の間のトラフィックを拒否します。	• 許可されている接続先のサーバーおよびサービスのリストを管理する (IP アドレスと TCP/UDP ポート) • 許可されているトラフィックプロトコルのソースのリストを管理する • 一時的または永久に特定の IP アドレスからのアクセスを明示的に拒否する • 許可されているリストを管理する
ウェブアプリケーションファイアウォール (WAF)	ウェブアプリケーションファイアウォールでは、ウェブトラフィックのディープパケットインスペクションができます。	• プラットフォーム固有およびアプリケーション固有の攻撃 • プロトコル健全性攻撃 • 不正ユーザーアクセス
ホストベースまたはインラインの IDS/IPS システム	IDS/IPS システムは、統計/行動や署名ベースのアルゴリズムを使用してネットワーク攻撃とトロイの木馬を検出および阻止できます。	• すべてのタイプの攻撃
トラフィック形成/レート制限	多くの場合、DoS/DDoS 攻撃はネットワークとシステムのリソースを消費します。レート制限は希少なリソースを過剰消費から保護するための効果的な手法です。	• ICMP フラッディング • アプリケーションリクエストフラッディング
未発達セッション制限	TCP SYN フラッディング攻撃には簡略型と分散型があります。どちらの場合でも、システムのベースラインがある場合は、半分開いている (未発達の) TCP セッションの数が正常なときとは著しく異なることを検出して、それ以降の特定のソースからの TCP SYN パケットを遮断できます。	• TCP SYN フラッディング

表 23: DoS/DDoS 攻撃の緩和と保護の技術

従来の DoS/DDoS 攻撃の緩和と保護のアプローチに加えて、AWS クラウドではその伸縮性に基づく機能が提供されています。

DoS/DDoS 攻撃は、限りあるコンピューティング、メモリ、ディスク、またはネットワークリソースを使い果たす試みであり、多くの場合、オンプレミスインフラストラクチャが被害を受けます。しかし、AWS クラウドは本質的に伸縮自在で、必要な場合に新しいリソースをオンデマンドで使用できます。たとえば、ウェブサーバーに対する正常なユーザーリクエストと区別がつかないリクエストを 1 秒間に何十万も生成するボットネットから DDoS 攻撃があったとします。従来の阻止技術を使用する場合、攻撃者のみが存在し、有効な顧客は存在しないと想定して、まず特定のソース (多くの場合、地理単位全体) からのトラフィックを拒否します。しかし、このような想定とアクションは、顧客に対してサービスを拒否することになります。

クラウド上で、このような攻撃を吸収するオプションを選択できます。Elastic Load Balancing や Auto Scaling などの AWS テクノロジーを使用すると、ウェブサーバーが攻撃時には (負荷に基づいて) スケールアウトし、攻撃終了後には元に戻るように設定できます。激しい攻撃を受けても、ウェブサーバーはクラウドの伸縮性を活用してスケールし、最適なユーザーエクスペリエンスを提供できます。攻撃を吸収することで、追加の AWS のサービスコストが発生する可能性がありますが、このような攻撃を持続させることは攻撃者にとって多大な経済的負担となるため、吸収された攻撃が永続する可能性が低くなります。

また、Amazon CloudFront を使用して DoS/DDoS フラッディング攻撃を吸収することもできます。AWS WAF は、AWS CloudFront と統合されており、アプリケーションの可用性に影響を与え、セキュリティを侵害し、過度にリソースを消費する可能性のある一般的なウェブの弱点からウェブアプリケーションを保護するのに役立ちます。CloudFront のコンテンツに対する攻撃を試みる潜在的な攻撃者は、ほとんどまたはすべてのリクエストを CloudFront のエッジロケーションに送る可能性が高く、そこでは AWS インフラストラクチャがバックエンドの顧客ウェブサーバーへの影響を最小限またはゼロに抑えながら過剰なリクエストを吸収します。この場合も攻撃を吸収するために追加の AWS のサービス料金が発生しますが、攻撃者が攻撃を継続するために発生するコストを考慮すると、金額に見合う効果があります。

DoS/DDoS 攻撃に対する露出を効果的に緩和、阻止、管理するには、このドキュメント全体で言及されているレイヤー防御モデルを構築する必要があります。

セキュリティモニタリング、アラート、監査証跡、インシデント対応の管理

責任共有モデルでは、オペレーティングシステムおよびそれより高いレイヤーで環境をモニタリングおよび管理する必要があります。これをオンプレミスまたはその他の環境ですでに実装している場合は、既存のプロセス、ツール、方法をクラウドで応用して使用できます。

セキュリティモニタリングの詳細については、「ENISA 安全調達」ホワイトペーパーを参照してください。これにはクラウドにおける継続的なセキュリティモニタリングの概念がまとめられています (参考資料と参考文献を参照)。

セキュリティモニタリングを開始する前に、以下の要素を考慮する必要があります。

- 測定するパラメータ
- これらを測定する方法
- これらのパラメータのしきい値
- エスカレーションプロセス
- データを保存する場所

多くの場合、最も重要なのは、ログ記録を行うには何が必要であるかを確認することです。ログ記録と分析を行うには、以下を設定することをお勧めします。

- ルートまたは管理者権限のあるユーザーが実行するアクション
- すべての監査証跡へのアクセス
- 無効な論理的アクセスの試み
- 識別と認証のメカニズムの使用
- 監査ログの初期化
- システムレベルのオブジェクトの作成と削除

ログファイルを設計するときは、表 24 の考慮事項に留意してください。

エリア	考慮事項
ログ収集	ログファイルが収集される方法に注意します。多くの場合、オペレーティングシステム、アプリケーション、またはサードパーティ/ミドルウェアエージェントがログファイル情報を収集します。
ログトランスポート	ログファイルを一元管理する場合は、ログファイルを一元管理場所に安全、確実、タイムリーに転送します。
ログストレージ	複数のインスタンスのログファイルを一元管理して、リテンションポリシーと分析および相関を容易にします。
ログ分類	複数のログファイルカテゴリを分析に適した形式で提供します。
ログ分析/相関	ログファイルを分析してログファイル内のイベントを相互に関連付けることで、セキュリティインテリジェンスが得られます。ログはリアルタイムまたは予定された間隔で分析できます。
ログの保護/セキュリティ	ログファイルには機密情報が含まれています。ネットワークコントロール、Identity and Access Management、暗号化、データ整合性の認証、および改ざんが不可能なタイムスタンプでログファイルを保護します。

表 24: ログファイルに関する考慮事項

セキュリティログのソースが複数ある場合があります。ファイアウォール、IDP、DLP、AV システム、オペレーティングシステム、プラットフォーム、アプリケーションなどのさまざまなネットワークコンポーネントがログファイルを生成します。その多くがセキュリティに関連しており、ログファイル戦略に組み込まれる必要があります。その他はセキュリティに関連しておらず、戦略には組み込まないほうが賢明です。ログにはユーザーのアクティビティ、例外、セキュリティイベントが含まれている必要があり、ログは将来の調査で使用できるように特定の期間にわたって保存しておく必要があります。

どのログファイルを含めるかを判断するには、以下の点を考慮してください。

- クラウドシステムのユーザー。どのように登録するか、どのように認証するか、リソースにアクセスする権限をどのように受けるか。
- クラウドシステムにアクセスするアプリケーション。どのように認証情報を取得するか、どのように認証するか、そのようなアクセスのための権限をどのように受けるか。
- AWS インフラストラクチャ、オペレーティングシステム、アプリケーションへの特権アクセス (管理者レベルのアクセス) を持っているユーザー。どのように認証するか、そのようなアクセスのための権限をどのように受けるか。

多くのサービスにアクセスコントロール監査証跡が組み込まれていますが (たとえば、Amazon S3 と Amazon EMR にはそのようなログが用意されています)、ログ記録のためのビジネス要件がネイティブサービスログから入手できるものよりも高い場合があります。このような場合は、特権エスカレーションゲートウェイを使用してアクセスコントロールログと認証を管理することを検討してください。

特権エスカレーションゲートウェイを使用する場合、システムへのすべてのアクセスを単一の (クラスター化された) ゲートウェイで一元管理します。AWS インフラストラクチャ、オペレーティングシステム、またはアプリケーションを直接呼び出す代わりに、インフラストラクチャへの信頼済みの中間証明書として機能するプロキシシステムによってすべてのリクエストが処理されます。通常、このようなシステムは以下を提供または実行する必要があります。

- 特権アクセスのための**自動パスワード管理**: 特権アクセスコントロールシステムは、Microsoft Active Directory、UNIX、LDAP、MYSQL などの組み込みのコネクタを自動的に使用して、所定のポリシーに基づいてパスワードと認証情報のローテーションを行うことができます。

- AWS IAM ユーザーのアクセスアドバイザーと AWS IAM ユーザーが前回使用したアクセスキーを使用して**最小権限チェックを定期的に実行する**
- フロントエンドにおける**ユーザー認証**とバックエンドにおける AWS のサービスへの委任アクセス: 通常、すべてのユーザーがシングルサインオンでウェブサイトにアクセスできます。ユーザーには認証プロファイルに基づいてアクセス権限が割り当てられます。一般的なアプローチでは、ウェブサイトに対してはトークンベースの認証を使用し、ユーザーのプロファイルで許可されている他のシステムへはクリックスルーでアクセスします。
- すべての重要なアクティビティの**改ざんが不可能な監査証跡**。
- **共有アカウントの複数のサインオン認証情報:** 複数のユーザーが同じパスワードを共有する必要のある場合があります。特権エスカレーションゲートウェイにより、共有アカウントを開示することなくリモートアクセスを行うことができます。
- ターゲットシステムへのアクセスのみを許可することによる**リープフロッギングまたはリモートデスクトップホッピングの制限**。
- セッション中に使用できるコマンドの管理。SSH 管理、アプライアンス管理、AWS CLI などのインタラクティブセッションの場合、このようなソリューションが使用可能なコマンドおよびアクションの範囲を制限することによってポリシーを適用します。
- コンプライアンスおよびセキュリティ確保のための**ターミナル用監査証跡および GUI ベースセッション**の提供。
- ポリシーの特定のしきい値に基づくすべてのログ記録とアラート。

変更管理ログの使用

セキュリティログを管理することで、変更を追跡することもできます。これには組織の変更管理プロセス (MACD-Move/Add/Change/Delete とも呼ばれる) の一部である計画されていた変更、臨時の変更、インシデントなどの予期しない変更が含まれます。変更はシステムのインフラストラクチャ側で発生する場合もあれば、コードリポジトリの変更、ゴールドイメージ/アプリケーションインベントリの変更、プロセスとポリシーの変更、ドキュメントの変更などの他のカテゴリに関連するものである場合もあります。ベストプラクティスとして、上記のすべてのカテゴリの変更に、不正操作が不可能なログリポジトリを使用することをお勧めします。変更管理システムとログ管理システムを相互に関連付け、接続します。

変更ログを削除または変更する特権を持つ専用ユーザーが必要です。ほとんどのシステム、デバイス、アプリケーションにおいて、変更ログは改ざんが不可能である必要があり、標準ユーザーにログを管理する特権が与えられてはなりません。通常のユーザーが変更ログから証拠を消去できる状態であってはなりません。AWS のお客様は、ログに対してファイル整合性モニタリングまたは変更検出ソフトウェアを使用する場合があります。これにより、既存のログデータが変更されたときにはアラートが生成され、新しいエントリが追加されたときにはアラートが生成されません。

システムコンポーネントのすべてのログを少なくとも 1 日に 1 回はレビューする必要があります。ログレビューには、侵入検出システム (IDS) や認証、許可、およびアカウンティングプロトコル (AAA) サーバー (たとえば RADIUS) などのセキュリティ機能を実行するサーバーが含まれている必要があります。このプロセスを容易にするためにログ収集、解析、アラートツールを使用できます。

重要なトランザクションのログの管理

重要なアプリケーションの場合、すべての Add、Change/Modify、Delete アクティビティまたはトランザクションがログエントリを生成する必要があります。各ログエントリには以下の情報が含まれている必要があります。

- ユーザー識別情報
- イベントのタイプ
- 日付とタイムスタンプ
- 成否
- イベントの原因
- 影響を受けたデータ、システムコンポーネント、またはリソースの ID または名前

ログ情報の保護

ログ記録設備とログ情報は改ざんおよび不正アクセスから保護されている必要があります。管理者ログと運営者ログはアクティビティの追跡情報を消去する攻撃の標的になりがちです。

ログ情報を保護するために行われている一般的なコントロールには以下のようなものがあります。

- 監査証跡がシステムコンポーネントで有効になっており、アクティブであることを確認する

- 職務上の必要性が認められる個人のみが監査証跡ファイルを閲覧できることを確認する
- アクセスコントロールメカニズム、物理的な分離、またはネットワークの分離によって現在の監査証跡ファイルが不正な変更から保護されていることを確認する
- 変更が困難な一元管理ログサーバーまたはメディアに現在の監査証跡ファイルが迅速にバックアップされていることを確認する
- 一元管理されている安全な内部ログサーバーまたはメディアに外部向けのテクノロジー (ワイヤレス、ファイアウォール、DNS、メールなど) のログがオフロードまたはコピーされていることを確認する
- システム設定、モニタリングされているファイル、モニタリングアクティビティの結果を検証することによって、ログに対してファイル整合性モニタリングまたは変更検出ソフトウェアを使用する
- セキュリティポリシーおよび手順を取得し、検証することによって、少なくとも 1 日に 1 回はセキュリティログをレビューする手順がそれらに含まれており、例外のフォローアップが必要であることを確認する
- 定期的なログレビューがすべてのシステムコンポーネントで実行されていることを確認する
- セキュリティポリシーおよび手順に監査ログリテンションポリシーが含まれており、ビジネス要件とコンプライアンス要件によって定義された所定の期間にわたる監査ログリテンションが必要であることを確認する

障害のログ記録

MACD イベントのモニタリングに加えて、ソフトウェアまたはコンポーネントの障害をモニタリングします。障害はハードウェアまたはソフトウェアの障害の結果として発生することがあり、サービスおよびデータの可用性が関連している場合もあれば、セキュリティインシデントとは無関係である場合もあります。また、サービス障害は、サービス妨害攻撃などの悪意のある意図的なアクティビティの結果である可能性もあります。どの場合でも、障害によってアラートが生成されるため、イベント分析および相互関連手法を使用して、なぜ障害が発生したか、それによってセキュリティ対応がトリガーされる必要があるかどうかを判断する必要があります。

まとめ

AWS クラウドプラットフォームでは、柔軟性、伸縮性、ユーティリティの請求、市場投入までの時間の短縮など、重要な利点を最先端企業に提供します。AWS では、広範なセキュリティサービスと機能を利用して資産とデータのセキュリティを管理できます。AWS ではインフラストラクチャまたはプラットフォームサービスにおいて優れたサービス管理レイヤーを提供しますが、クラウド内のデータの機密性、整合性、可用性を保護し、企業固有の情報保護のためのビジネス要件を満たす責任は企業にあります。

従来のセキュリティとコンプライアンスの概念はクラウドでも適用されます。このホワイトペーパーで説明したさまざまなベストプラクティスを使用して、独自のセキュリティポリシーおよびプロセスを構築することをお勧めします。これにより、アプリケーションとデータを迅速かつ安全にデプロイできます。

寄稿者

- Dob Todorov
- Yinal Ozkan

参考資料と参考文献

- アマゾン ウェブ サービス: セキュリティプロセスの概要 – http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
- 『アマゾン ウェブ サービスのリスクとコンプライアンス』ホワイトペーパー – http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
- アマゾン ウェブ サービスによる災害復旧 – http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
- Amazon VPC ネットワーク接続オプション – http://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf
- Active Directory ユースケースのための ID フェデレーションのサンプルアプリケーション – http://aws.amazon.com/code/1288653099190193
- Amazon EC2 .NET アプリケーションへの Windows ADFS でのシングルサインオン – http://aws.amazon.com/articles/3698?_encoding=UTF8&queryArg=searchQuery&x=20&y=25&fromSearch=1&searchPath=all&searchQuery=identity%20federation
- Token Vending Machine を使用して AWS モバイルアプリケーションのユーザー認証を行う – http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
- AWS SDK for Java と Amazon S3 でのクライアント側データ暗号化 – http://aws.amazon.com/articles/2850096021478074

- Amazon の法人 IT チームが SharePoint 2010 をアマゾン ウェブ サービスクラウドにデプロイ –
  http://media.amazonwebservices.com/AWS_Amazon_SharePoint_Deployment.pdf
- アマゾン ウェブ サービスの適正利用規約 –
  http://aws.amazon.com/aup/
- ENISA 安全調達: クラウド契約におけるセキュリティサービスレベルのモニタリングに関するガイド –
  http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to- monitoring-of- security-service-levels-in-cloud-contracts
- PCI のデータセキュリティ標準 –
  https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2- 0#pci_dss_v2-0
- ISO/IEC 27001:2005 –
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103
- AWS を使用するためのセキュリティチェックリストの監査 –
  http://media.amazonwebservices.com/AWS_Auditing_Security_Checklist.pdf