アマゾン ウェブ サービス: セキュリティプロセスの概要

2014 年 11 月

（本書の最新版については、http://aws.amazon.com/security/ を参照してください）

amazon
web services

目次

はじめに

アマゾン ウェブ サービス（AWS）は可用性、信頼性、そして拡張性が高いクラウドコンピューティングプラットフォームを提供します。また、さまざまな種類のアプリケーションを実行できるツールをお客様に提供します。当社の顧客システムやデータの機密性、完全性、可用性を保護することは、AWS にとって、顧客からの信頼を維持することと同様に最大の重要事項です。このドキュメントは、たとえば「AWS がどのようにしてデータの保護を支援するのか」といった疑問に答えることを目的としています。特に、AWS の管理下にあるネットワークとサーバーのインフラストラクチャ、およびサービス特有のセキュリティの導入に関する AWS の物理的な運用上のセキュリティプロセスについて説明します。

共有セキュリティ責任モデル

AWS がリソースのセキュリティをどのように確保するかを詳しく説明する前に、クラウドのセキュリティがオンプレミスデータセンターのセキュリティとは少し異なるということを説明する必要があります。コンピュータシステムとデータをクラウドに移行する場合、セキュリティについてはお客様とクラウドサービスプロバイダーが共同で責任を負います。この場合、クラウドをサポートする基盤インフラストラクチャのセキュリティ保護は AWS が担い、クラウドに置かれるリソースやクラウドに接続する手段についてはお客様が責任を負います。このセキュリティ責任分担モデルにより、多くの面でお客様の運用の負担が軽減されるだけでなく、追加の対策を行わなくても現状のセキュリティ体制を強化できる場合さえあります。

図 1: AWS 共有セキュリティ責任モデル

お客様が行う必要のあるセキュリティ設定作業の量は、選択するサービスおよびデータの機密性によって異なります。ただし、一部のセキュリティ機能（個々のユーザーアカウントおよび認証情報、データ転送における SSL/TLS、ユーザーアクティビティのログ記録など）については、利用する AWS サービスにかかわらず設定が必要です。これらのセキュリティ機能の詳細については、以下の「AWS アカウントのセキュリティ機能」セクションを参照してください。

セキュリティに関する AWS の責任

アマゾン ウェブ サービスは、AWS クラウドで提供されるすべてのサービスを実行するグローバルインフラストラクチャの保護を担います。このインフラストラクチャは、AWS サービスを実行するハードウェア、ソフトウェア、ネットワーキング、および施設で構成されます。このインフラストラクチャの保護は AWS の最優先事項です。お客様は当社のデータセンターやオフィスを訪れてこの保護を直接確認することができない代わりに、サードパーティの監査人による複数のレポートを受け取ることができます。監査人は、当社がコンピュータセキュリティに関するさまざまな基準や規制に準拠していることを証明しています（詳細については、aws.amazon.com/compliance を参照してください）。

このグローバルインフラストラクチャの保護に加え、AWS はマネージドサービスとみなされる AWS 製品のセキュリティ設定についても責任を負います。このタイプのサービスには、Amazon DynamoDB、Amazon RDS、Amazon Redshift、Amazon Elastic MapReduce、Amazon WorkSpaces などがあります。これらのサービスには、クラウドベースリソースの拡張性と柔軟性だけでなく、マネージドサービスとしての利点もあります。これらのサービスについては、ゲストオペレーティングシステム（OS）やデータベースのパッチ適用、ファイアウォールの設定、災害対策などのセキュリティタスクを AWS が行います。ほとんどの場合、これらのマネージドサービスでお客様が行う作業は、リソースの論理アクセスコントロールを設定してアカウントの認証情報を保護することだけです。一部のサービスでは、データベースユーザーアカウントの設定などの追加タスクが必要になる場合がありますが、全般的なセキュリティ設定作業はサービスに含まれています。

セキュリティに関するお客様の責任

AWS クラウドでは、通常なら数週間かかる仮想サーバー、ストレージ、データベース、およびデスクトップのプロビジョニングを数分で完了できます。また、必要に応じてクラウドベースの分析やワークフローツールを使用してデータを処理し、そのデータを独自のデータセンターやクラウドに保存することもできます。お客様の責任で行う設定作業の量は、どの AWS サービスを使用するかによって決まります。

IaaS（Infrastructure as a Service）の上級者向けカテゴリに属する AWS 製品（Amazon EC2、Amazon VPC、Amazon S3 など）の場合、管理は完全にお客様の責任となり、必要なセキュリティ設定と管理タスクもすべてお客様自身で行う必要があります。たとえば、EC2 インスタンスの場合、ゲスト OS の管理（アップデートやセキュリティパッチの適用を含む）、各インスタンスにインストールしたアプリケーションソフトウェアやユーティリティ、AWS が提供する各インスタンスのファイアウォール（セキュリティグループ）の設定は、お客様がその責任を負います。サーバーの設置場所が異なるだけで、これらはお客様が慣れ親しんだセキュリティタスクと基本的には同じです。

Amazon RDS や Amazon Redshift といった AWS マネージドサービスには特定のタスクの実行に必要なすべてのリソースが含まれており、それらに伴う設定作業も必要ありません。マネージドサービスでは、インスタンスの起動や管理、ゲスト OS やデータベースのパッチ適用、データベースのレプリケートなどに頭を悩ませる必要はありません。お客様に代わって AWS がこれらを行います。ただし、ユーザーに個々の認証情報を付与して役割分担を行えるように、Amazon Identity and Access Management（IAM）による AWS アカウント認証情報の保護と個々のユーザーアカウントの設定は、他のサービス同様お客様自身で行う必要があります。また、AWS では各アカウントに多要素認証（MFA）を使用し、AWS リソースへのアクセスに SSL/TLS の使用を義務付け、AWS CloudTrail で API/ユーザーアクティビティのログを記録するように設定することを推奨しています。追加で行える対策の詳細については、AWS セキュリティのベストプラクティスに関するホワイトペーパーおよび AWS セキュリティリソースウェブページの推奨する参照情報を参照してください。

AWS グローバルインフラストラクチャのセキュリティ

AWS は、処理やストレージなどさまざま基本コンピューティングリソースをプロビジョニングするために使用するグローバルなクラウドインフラストラクチャを運用します。AWS グローバルインフラストラクチャには、施設、ネットワーク、ハードウェア、およびこれらのリソースのプロビジョニングと使用をサポートする運用ソフトウェア（ホスト OS、仮想化ソフトウェアなど）が含まれます。AWS グローバルインフラストラクチャは、さまざまなセキュリティのコンプライアンス基準だけでなく、セキュリティのベストプラクティスに準じて、設計され、管理されています。AWS のお客様として、確実に世界で最も安全なコンピューティングインフラストラクチャにウェブアーキテクチャーを構築できます。

AWS コンプライアンスプログラム

AWS コンプライアンスプログラムにより、強力なセキュリティを適切に理解し、セキュリティおよびデータ保護に関する業界および政府の要件に合理的に準拠できます。AWS がお客様に提供する IT インフラストラクチャは、次のようなセキュリティのベストプラクティス、および各種 IT セキュリティ基準に合わせて設計、管理されています。

- SOC 1/SSAE 16/ISAE 3402（旧称 SAS70）
- SOC 2
- SOC 3
- FISMA、DIACAP、FedRAMP
- DoD CSM レベル 1～5
- PCI DSS レベル 1
- ISO 27001
- ITAR
- FIPS 140-2
- MTCS レベル 3

さらに、AWS プラットフォームが提供する柔軟性と制御により、お客様は以下のような業界特有の標準を満たすソリューションをデプロイすることができます。

- HIPAA
- クラウドセキュリティアライアンス（CSA）
- アメリカ映画協会（MPAA）

AWS は、ホワイトペーパー、レポート、認定、認証評価、およびその他のサードパーティによる証明を通して、当社の IT 統制環境に関するさまざまな情報をお客様に提供しています。詳細については、ウェブサイト（http://aws.amazon.com/compliance/）で入手可能な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。

物理的および環境のセキュリティ

Amazon のデータセンターは最新式で、革新的で建築的かつ工学的アプローチを採用しています。Amazon は大規模データセンターの設計、構築、運用において、長年の経験を有しています。この経験は、AWS プラットフォームとインフラストラクチャに活かされています。AWS のデータセンターは、外部からはそれとはわからないようになっています。ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。

AWS は、そのような権限に対して正規のビジネスニーズがある従業員や業者に対してのみデータセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、たとえかれらが引き続き Amazon または Amazon Web Services の従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。

火災検出と鎮火

自動火災検出および鎮火装置が取り付けられ、リスクを軽減しています。この火災検出システムは、全データセンター環境、機械的及び電気的インフラストラクチャースペース、冷却室および発電機設備室において、煙検出センサーを使用しています。これらのエリアは、充水型、二重連結予作動式、またはガス式スプリンクラーシステムによって守られています。

電力

データセンターの電力システムは、完全に冗長性をもち、運用に影響を与えることなく管理が可能となっています。1 日 24 時間体制で、年中無休で稼動しています。施設内で重要かつ不可欠な負荷に対応するために、電力障害時には無停電電源装置（UPS）がバックアップ電力を供給しています。データセンターは、発電機を使用して施設全体のバックアップ電力を供給しています。

空調と温度

サーバーその他のハードウェアの運用温度を一定に保つために、空調制御が必要です。これによって過熱を防ぎ、サーバー停止の可能性を減らすことができます。データセンターは、大気の状態を最適なレベルに保つように設定されています。作業員とシステムが、温度と湿度を適切なレベルになるよう監視してコントロールしています。

管理

AWS は、問題が速やかに特定されるように、電気、機械、ライフサポートシステムおよび設備を監視しています。予防的メンテナンスが実行され、設備を継続的な運用性が保たれています。

ストレージデバイスの廃棄

AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は、DoD 5220.22-M（「National Industrial Security Program Operating Manual（国立産業セキュリティプログラム作業マニュアル）」）または NIST 800-88（「Guidelines for Media Sanitization（メディア衛生のためのガイドライン）」）に詳細が記載されている技術を用いて、廃棄プロセスの一環としてデータを破棄します。廃棄された磁気ストレージデバイスはすべて業界標準の方法に従って消磁され、物理的に破壊されます。

事業継続性管理

Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを配備する機能を顧客に提供します。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。また、AWS におけるデータセンターの事業の継続性は、Amazon Infrastructure Group の指示に従って管理されます。

可用性

世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

AWS を使用すると、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。

AWS の使用量は、複数のリージョンやアベイラビリティーゾーンを利用できるように設計することをお勧めします。複数のアベイラビリティゾーンにアプリケーションを配置すると、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つことができます。

インシデントへの対応

Amazon のインシデント管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制でインシデントを検出し、影響と解決方法を管理します。

役員による全社的検査

Amazon の内部監査グループは、最近になって AWS サービスの復元プランを検査しました。このプランは、上級役員管理チームと取締役の監査委員会のメンバーによっても定期的に検査されています。

コミュニケーション

AWS は、様々な方法でグローバルレベルの内部コミュニケーションを実施することで、従業員が各自の役割と責任を理解することを手助けし、重要なイベントについて適時伝達しています。これらの方法には、新入社員向けのオリエンテーションとトレーニングプログラム、業績その他についてアップデートを行う定例のマネジメント会議、ビデオ会議、電子メールメッセージ、Amazon イントラネットでの情報の投稿などの電子的手段があります。

AWS はまた、様々な手段の外部コミュニケーションを実施して、その顧客ベースとコミュニティをサポートしてきました。カスタマーエクスペリエンスに影響を与える運用上の問題についてカスタマーサポートチームが通知受けることができるようにするためのメカニズムが配備されています。[Service Health Dashboard] が、顧客サポートチームによって管理運営されており、大きな影響を与える可能性のある問題について顧客に警告を発することができます。「AWS セキュリティセンター」は、AWS に関するセキュリティとコンプライアンスの詳細情報を提供しています。カスタマーサポートチームと直接連絡を取ったり、お客様に影響を与えるあらゆる問題に対する警告を事前に受け取ることができる AWS サポートに申し込みをすることもできます。

ネットワークセキュリティ

AWS ネットワークは作業負荷に応じてセキュリティと弾力性のレベルを選択できるように設計されています。クラウドリソースで地理的に分散した、フォールトトレラントなウェブアーキテクチャーを構築できるように、AWS ではワールドクラスのネットワークインフラストラクチャを実装し、慎重に監視と管理を行っています。

安全なネットワークアーキテクチャ

ファイアウォールや他の境界デバイスなどのネットワークデバイスは、ネットワークの外部境界およびネットワーク内の主要な内部境界で通信を監視および制御するために用意されています。これらの境界デバイスでは、ルールセット、アクセスコントロールリスト（ACL）、および設定が採用され、強制的に特定の情報システムサービスに情報が流れます。

ACL、つまりトラフィックフローのポリシーは、各マネージドインターフェイスに設定され、トラフィックの流れを監視して流します。ACL ポリシーは Amazon 情報セキュリティによって承認されます。これらのポリシーは、AWS の ACL 管理ツールを使用して自動的にプッシュされ、確実にマネージドインターフェイスで最新の ACL が実行されます。

安全なアクセスポイント

AWS では、インバウンドとアウトバウンドの通信およびネットワークトラフィックをより包括的に監視することを考え、限られた数のクラウドへのアクセスポイントを戦略的に設置しました。このようなお客様のアクセスポイントは API エンドポイントと呼ばれ、安全な HTTP アクセス（HTTPS）を許可します。これにより、ご利用のストレージまたは AWS 内のコンピューティングインスタンスとの安全な通信セッションを確立できます。FIPS 暗号要件への準拠を必要とするお客様をサポートするために、AWS GovCloud（米国）内の SSL 終端ロードバランサーは、FIPS 140-2 に準拠しています。

さらに、AWS は、インターネットサービスプロバイダ（ISP）とのインターフェイス通信を管理するためのネットワークデバイスを実装しました。AWS ネットワークのインターネット側のそれぞれの境界では、複数の通信サービスへの重複する接続を採用しています。これらの接続にはそれぞれ、専用ネットワークデバイスがあります。

送信の保護

HTTP または Secure Sockets Layer（SSL）を使用した HTTPS を介して AWS のアクセスポイントに接続できます。SSL は、傍受、改ざん、およびメッセージの偽造から保護するように設計された暗号プロトコルです。

ネットワークセキュリティの追加レイヤーが必要なお客様のために、AWS では Amazon Virtual Private Cloud（VPC）を提供しています。これにより、AWS クラウド内にプライベートサブネットが提供され、Amazon VPC とデータセンターの間に暗号化されたトンネルを提供する IPsec 仮想プライベートネットワーク（VPN）のデバイスを使用できるようになります。VPC の設定オプションの詳細については、後の「Amazon Virtual Private Cloud（Amazon VPC）のセキュリティ」のセクションをご覧ください。

Amazon 社からの分離

論理的に、AWS 本稼働環境のネットワークは、ネットワークセキュリティ/分離デバイスの複雑な組み合わせによって、Amazon 社内ネットワークから分離しています。AWS クラウドのコンポーネントを維持するためにアクセスする必要がある社内ネットワーク上の AWS 開発者と管理者は AWS 発券システムを通して明示的にアクセスをリクエストしなければなりません。すべてのリクエストは、該当するサービスの所有者によって確認および承認されます。

承認された AWS 担当者は、ネットワーク デバイスやその他のクラウドコンポーネントへのアクセスを制限する拠点ホストを介して AWS ネットワークに接続します。このとき、すべてのアクティビティはセキュリティレビューのために記録されます。拠点ホストへのアクセスには、ホスト上のすべてのユーザーアカウントに対して SSH 公開鍵認証が必要です。AWS 開発者および管理者の論理的アクセスの詳細については、後の「AWS アクセス」をご覧ください。

フォールトトレラントな設計

Amazon のインフラストラクチャは高いレベルの可用性を備え、回復機能を持つ IT アーキテクチャを展開できます。AWS のシステムは、お客様への影響を最小限に抑えながらシステムまたはハードウェア障害に耐えられるように設計されています。

データセンターは、世界のさまざまなリージョンにクラスター化されて構築されています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。

AWS を使用すると、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理上のリージョン内に、柔軟にインスタンスを配置してデータを保管できます。各アベイラビリティーゾーンは、障害が発生しても他のゾーンに影響を与えないように設計されています。つまり、アベイラビリティゾーンは、代表的な都市のリージョン内で物理的に区切られており、低リスクの氾濫原にあります（具体的な洪水帯の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップジェネレータの利用に加え、単一点障害の発生をさらに減らすため、それぞれ別々の電力供給施設から異なる配管網を経由して電力供給を受けています。アベイラビリティゾーンはすべて、複数の Tier-1 トランジットプロバイダに重複して接続しています。

AWS の使用量は、複数のリージョンやアベイラビリティーゾーンを利用できるように設計することをお勧めします。複数のアベイラビリティゾーンにアプリケーションを配置すると、自然災害やシステム障害を含むほとんどの障害が発生したときに、回復力を持った状態を保つことができます。ただし、EU データ保護指令のようなロケーションに依存するプライバシーおよびコンプライアンスの要件に注意する必要があります。お客様が積極的に行わなければ、リージョン間でデータは複製されません。従って、このような種類のデータの配置およびプライバシーの要件を持つお客様が、規格に準拠した環境を構築できます。リージョン間の通信はすべて、パブリックなインターネットインフラストラクチャを介して行われることに注意してください。このため、適切な暗号方式を使用して機密データを保護することをお勧めします。

本文書の執筆時点では、リージョンは 11 あります。米国東部（バージニア北部）、米国西部（オレゴン）、米国西部（北カリフォルニア）、AWS GovCloud（米国）、欧州（アイルランド）、欧州（フランクフルト）、アジアパシフィック（シンガポール）、アジアパシフィック（東京）、アジアパシフィック（シドニー）、南米（サンパウロ）、中国（北京）です。

AWS GovCloud（米国）は、特定の規制およびコンプライアンス要件への準拠をサポートすることで、米国政府関連機関や顧客がワークロードをクラウドに移行できるように設計された、分離された AWS リージョンです。AWS GovCloud（米国）のフレームワークでは、米国政府関連機関およびその請負業者が米国武器規制国際交渉規則（U.S. International Traffic in Arms Regulations/ITAR）および Federal Risk and Authorization Management Program（FedRAMP）の各種要件に対応できます。AWS GovCloud（米国）は、FedRAMP が認定する第三者評価組織（3PAO）を利用し、いくつかの AWS サービスについて米国保健福祉省（HHS）から Agency Authority to Operate（ATO）を取得しました。

AWS GovCloud（米国）リージョンは、2 つのアベイラビリティーゾーンを利用して、他のリージョンと同様に耐障害性に優れた設計を提供します。さらに、AWS GovCloud（米国）リージョンは、AWS クラウド内に独立した部分を作成し、プライベート（RFC 1918）アドレスを持つ Amazon EC2 インスタンスを起動するための、デフォルトでは必須の AWS Virtual Private Cloud（VPC）サービスです。GovCloud の詳細については、AWS のウェブサイト（http://aws.amazon.com/govcloud-us/）をご覧ください

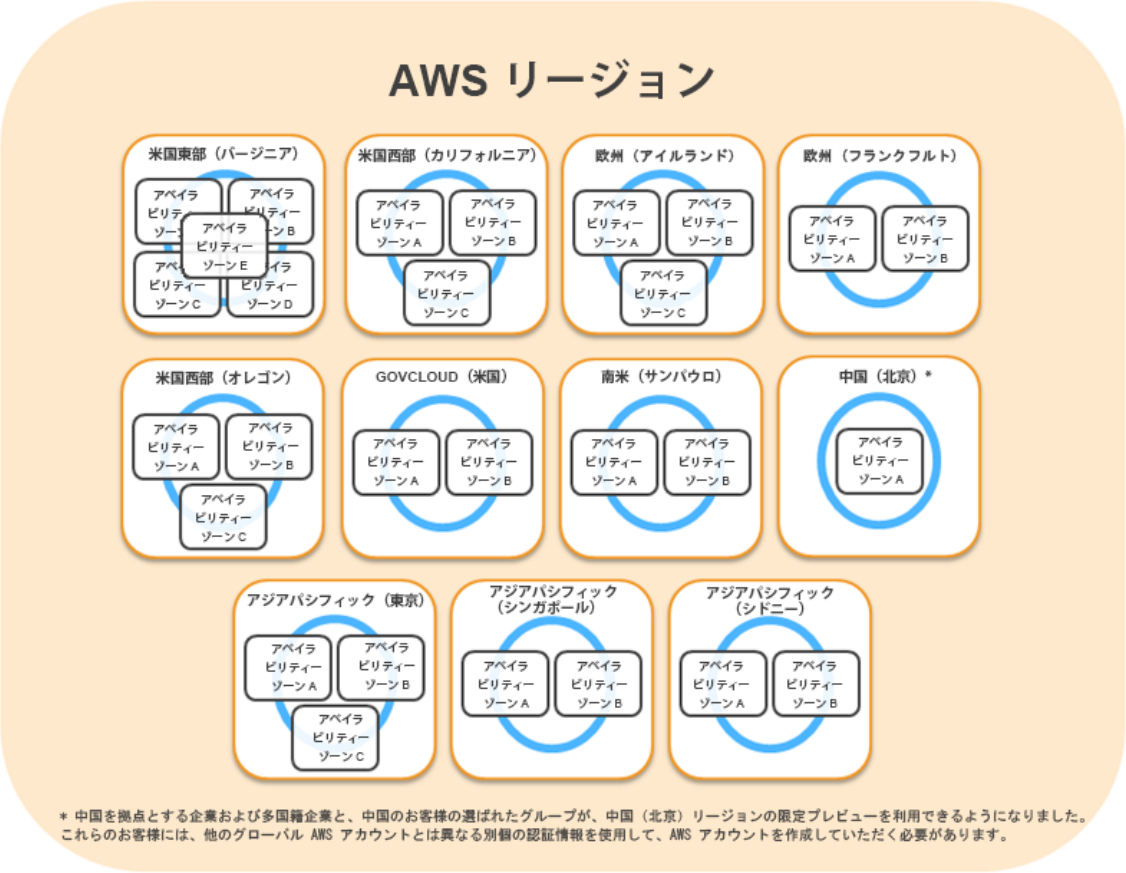


図 2: リージョンとアベイラビリティーゾーン

アベイラビリティゾーンの数は、変更されることがあります。

ネットワークの監視と保護

AWS は、様々な自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。AWS モニタリングツールは、異常な、または不正なアクティビティと条件を通信の出入り口で検出するように設計されています。これらのツールは、サーバーおよびネットワークの利用状況、ポートスキャニングアクティビティ、アプリケーションの利用状況、および許可されていない侵入の試みをモニタリングします。このツールを使用して、異常なアクティビティに対して独自に性能測定基準のしきい値を設定することができます。

AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。主要なオペレーションメトリックが早期警告しきい値を超えた場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュール(常時待機体制)が採用されているので、担当者が運用上の問題にいつでも対応することができます。ポケットベルシステムがサポートされ、アラームが迅速かつ確実に運用担当者に届きます。

インシデントや問題の処理時には、運用担当者を支援して情報を提供するための文書が保持されます。問題の解決のために協力体制が必要な場合は、情報伝達と記録機能をサポートする会議システムが使用されます。協力体制を必要とする運用上の問題の処理にあたっては、訓練を受けた通話リーダーが、コミュニケーションと進捗を支援します。深刻な運用上の問題が発生した後には、外部的な影響の有無に関わらず、事後分析会議が開かれます。そしてエラーの原因(COE)に関する文書が起草され、根本的な原因が捕捉されて、今後のために予防措置が取られるようにします。予防措置の実施は、週に一度開かれる運用会議において追跡されます。

AWS のセキュリティモニタリングツールは、分散型のフラッディング攻撃、およびソフトウェア/ロジックによる攻撃を含む、数種類のサービス妨害(DoS)攻撃の特定に役立ちます。DoS 攻撃が確認されると、AWS のインシデントレスポンスプロセスが開始されます。DoS 予防ツールに加えて、各リージョンの豊富な通信プロバイダや容量の増設により DoS 攻撃を予防します。

AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、さらに堅牢な保護を実装することができます。以下にいくつかの例を示します:

- **分散型サービス妨害(DDoS)攻撃。**Amazon API エンドポイントは、Amazon を世界最大のインターネットショッピング業者にしたエンジニアリングの専門知識を参考にして、大規模で、インターネット規模の、ワールドクラスのインフラストラクチャにホストされています。専属的な DDoS 緩和技術が使用されています。さらに、AWS ネットワークは、複数のプロバイダによるマルチホーム構成になっていて、インターネットアクセスの多様化を実現しています。
- **中間者(MITM)攻撃。**すべての AWS API は、サーバー認証を提供する、SSL で保護されたエンドポイント経由で利用可能です。Amazon EC2 AMI は新しい SSH ホスト証明書を、最初のブート時に自動的に生成し、それらをインスタンスのコンソールに記録します。その後、セキュリティで保護された API を使用してコンソールを呼び出し、ホスト証明書にアクセスしてから、初めてインスタンスにログインできます。AWS とのやり取りにはすべて SSL を使用することをお勧めします。
- **IP スプーフィング。**Amazon EC2 インスタンスは、なりすましたネットワークトラフィックを送信できません。AWS によって管理される、ホストベースのファイアウォールインフラストラクチャでは、インスタンスは、ソース IP または MAC アドレスがインスタンス自身のものでないトラフィックを送信できません。

- **ポートスキャン**。Amazon EC2 の顧客による許可のないポートスキャンは、AWS の適正利用規約に違反します。AWS の使用許可ポリシーの違反は深刻に受け止められ、報告された違反はすべて調査されます。不正利用の疑いは、ウェブサイト（http://aws.amazon.com/contact-us/report-abuse/）に示されている連絡先から報告することができます。不正なポートスキャンが AWS によって検出された場合、停止およびブロックされます。Amazon EC2 インスタンスのインバウンドポートはすべてデフォルトで閉じられており、お客様によってのみ開かれるため、Amazon EC2 インスタンスのポートスキャンは、一般的には効果がありません。セキュリティグループを厳格に管理することによって、ポートスキャンの脅威をより軽減できます。任意のソースから特定のポートへのトラフィックを許可するようにセキュリティグループを設定した場合、そのポートは、ポートスキャンに対して脆弱になります。この場合、適切なセキュリティ対策をして、アプリケーションに必要不可欠な可能性のあるリスニングサービスが、未許可のポートスキャンによって検出されないようにする必要があります。例えば、ウェブサーバーは、外部に対してポート 80（HTTP）を開く必要があります。また、このサーバーの管理者は、Apache のような HTTP サーバーソフトウェアのセキュリティに対して責任を有しています。特定のコンプライアンス要件を満たすために、必要に応じて脆弱性のスキャンを行う許可をリクエストできます。これらのスキャンは自身のインスタンスに限定する必要があり、AWS の利用規定に違反することはできません。このタイプのスキャンの事前承認は、ウェブサイト（https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest）からリクエストを送信することで開始できます。
- **第三者によるパケットスニッフィング。**無差別モード（プロミスキャスモード）で実行中の仮想インスタンスが、異なる仮想インスタンス向けのトラフィックを受信または "傍受" することはできません。インターフェイスをプロミスキャスモードにすることはできますが、ハイパーバイザーは宛先に指定されていないインターフェイスにトラフィックを伝送しません。物理的に同一のホスト上に配置された、同一の顧客によって保有される 2 つの仮想インスタンスであっても、互いのトラフィックを傍受することはできません。ARP キャッシュポイズニングなどの攻撃は、Amazon EC2 および Amazon VPC では機能しません。Amazon EC2 は、意図せず、または悪意をもって他者のデータを閲覧しようとする利用者に対して、豊富な防止対策を提供していますが、一般的にはお客様は重要なトラフィックを暗号化すべきです。

モニタリングに加えて、AWS 環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースで様々なツールを使用した脆弱性のスキャンが定期的に実行されます。また、AWS セキュリティチームは、該当するベンダーの不具合に関するニュースフィードを購読し、積極的にベンダーのウェブサイトやその他の関連する販売経路を監視し、新しいパッチがないかどうかの確認を行っています。さらに、AWS のお客様から各種問題を AWS にご報告いただけるようにしています。AWS 脆弱性レポートのウェブサイト（http://aws.amazon.com/security/vulnerability-reporting/）をご利用ください

AWS アクセス

AWS 本稼働環境のネットワークは、Amazon 社内ネットワークから分離されており、論理的アクセスのために個別の認証情報が必要です。Amazon 社内ネットワークは、ユーザー ID、パスワード、Kerberos に依存しています。一方、AWS 本稼働環境のネットワークは拠点ホストを介した SSH 公開キー認証が必要となります。

AWS クラウドのコンポーネントにアクセスする必要がある Amazon 社内ネットワーク上の AWS 開発者と管理者は、AWS アクセス管理システムを通して明示的にアクセスをリクエストしなければなりません。すべてのリクエストは、適切な所有者または管理者によって確認および承認されます。

アカウントの確認および監査

アカウントは 90 日ごとにレビューされます。明示的な再承認が必要となり、これを行わない場合は、リソースに対するアクセス権が自動的に取り消されます。従業員の記録が Amazon のヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。Windows および UNIX のアカウントは無効となり、Amazon の権限管理システムは全システムからそのユーザーを削除します。

アクセスに関する変更リクエストは、Amazon 権限管理ツールの監査ログに記録されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。承認しない場合、アクセス権は自動的に取り消されます。

経歴確認

AWS は、正式なポリシーと手順を確立し、AWS プラットフォームとインフラストラクチャホストに対する論理的アクセスの、最低限の基準を定めてきました。AWS は従業員に対し、その従業員の役職やアクセスレベルに応じて、適用法令が認める範囲で、雇用前審査の一環として犯罪歴の確認を行います。ポリシーはまた、論理的アクセスとセキュリティの管理のために、役割上の責任を特定しています。

認証情報のポリシー

AWS セキュリティは、必要な設定と有効期限の間隔が含まれる認証情報のポリシーを作成しました。パスワードは複雑である必要があり、90 日おきに変更されます。

セキュリティ設計の原則

AWS の開発プロセスは、安全なソフトウェア開発のベストプラクティスに従っており、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスクアセスメントの完遂などが含まれています。静的コード分析ツールは、標準ビルドプロセスの一環として実行され、配備される全ソフトウェアは、注意深く選択された業界の専門家によって実行される反復侵入テストを受けます。当社のセキュリティリスク査定のレビューは、設計段階に開始され、この作業はソフトウェアの立ち上げ後まで継続します。

変更管理

既存の AWS インフラストラクチャに対する定期的な変更、緊急の変更、および設定の変更は、類似するシステムの業界基準に従って、許可、記録、テスト、承認、および文書化されます。AWS インフラストラクチャを更新するにあたり、お客様とお客様によるサービスの使用に対する影響は最小限に抑えられます。サービスが悪影響を受ける可能性がある場合、AWS は E メールまたは AWS Service Health Dashboard（http://status.aws.amazon.com/）を通じて顧客に通知します。

ソフトウェア

AWS は、変更の管理にシステム的なアプローチを採用しています。そのためお客様に影響を与えるサービスの変更は、徹底的に検証、テスト、承認され、充分な情報が提供されます。AWS の変更管理プロセスは、意図しないサービス障害を防ぎ、お客様に対するサービスの完全性を維持することを目的としています。実稼働環境にデプロイされる変更には、以下の対応が行われます:

- 検証: 変更の技術的側面について専門家による検証が必要です。

- テスト: 適用されている変更は、予想どおりに動作し、パフォーマンスに悪影響を与えないことを確認するためにテストされます。
- 承認: すべての変更は、ビジネスへの影響を適切に監視し、それらの影響についての情報を提供するために、承認される必要があります。

変更の実稼動環境への投入は通常、最も影響の小さいエリアへの段階的配備から開始されます。デプロイは単一のシステムでテストされ、影響が評価できるよう綿密にモニタリングされます。サービスの所有者は、数多くの設定可能な評価指標を保有しています。これは、そのサービスの上流工程に対する依存関係の健全度を評価するものです。3つの測定値が、閾値と設定中のアラームとともに注意深くモニタリングされます。ロールバック手順は、変更管理(CM)チケットで文書化されています。

可能な場合、変更は通常の変更時間帯に予定されます。標準の変更管理手順と異なる手順を必要とする実稼動システムに対する緊急の変更は、インシデントと関連付けられており、必要に応じて記録され、承認されます。

AWS は、重要なサービスの変更に対する自己監査を定期的に行っており、品質をモニタリングしながら高い基準を維持することによって、変更管理プロセスの継続的な改善に貢献しています。例外は分析され、根本的な原因が決定されて適切な措置が取られます。変更はコンプライアンスに従うようにされるか、または必要に応じてロールバックされます。その後プロセスまたは人的問題を解決して修正するための措置が取られます。

インフラ

Amazon の法人アプリケーションチームは、ソフトウェアの開発と管理を行って、サードパーティのソフトウェア配布、内部開発ソフトウェアと設定管理の領域で、UNIX/Linux ホストの IT プロセスを自動化します。インフラストラクチャチームは、UNIX/Linux 設定管理フレームワークを運用して、ハードウェアの拡張性、可用性、監査、セキュリティ管理を解決します。変更管理の自動プロセスを使用した集中管理ホストにより、当社は、高可用性、再現性、拡張性、セキュリティおよび障害復旧という目標を達成することが可能となります。システムおよびネットワークエンジニアは、これらの自動ツールのステータスを日常的にモニタリングしており、レポートを検証して、設定やソフトウェアの取得または更新に失敗するホストへの対応を行っています。

新しいハードウェアがプロビジョニングされると、内部開発された設定管理ソフトウェアがインストールされます。これらのツールは UNIX ホスト上で稼動し、ホストが設定されていること、またホストに割り当てられた役割によって決定された基準に従ってソフトウェアがインストールされていることを確認します。この設定管理ソフトウェアは、ホストにインストールされているパッケージを定期的に更新するときにも役立ちます。パーミッションサービスによって許可された作業員だけが、集中設定管理サーバーにログインすることができます。

AWS アカウントのセキュリティ機能

AWS は、AWS アカウントやリソースを不正使用から保護するためのさまざまなツールや機能を提供します。これには、アクセスコントロールのための認証情報、暗号化されたデータ転送のための HTTPS エンドポイント、個別の IAM ユーザーアカウントの作成、セキュリティモニタリングのためのユーザーアクティビティのログ記録、および Trusted Advisor セキュリティチェックが含まれます。どの AWS サービスを選択するかにかかわらず、これらすべてのセキュリティツールを利用できます。

AWS 認証情報

承認されたユーザーおよびプロセスだけが AWS アカウントおよびリソースにアクセスできるように、AWS は数種類の認証情報を使用して認証を行います。これには、パスワード、暗号キー、デジタル署名、および証明書が含まれます。AWS アカウントまたは IAM ユーザーアカウントへのログインに多要素認証(MFA)を要求するオプションもあります。次の表に、さまざまな AWS 認証情報とその用途を示します。

認証情報の種類	使用アイテム	説明
パスワード	AWS マネジメントコンソールへの AWS ルートアカウントまたは IAM ユーザーアカウントのログイン	AWS アカウントまたは IAM アカウントへのログインに使用する文字列です。AWS パスワードの最小文字数は 6 文字、最大文字数は 128 文字です。
Multi-Factor Authentication(MFA)	AWS マネジメントコンソールへの AWS ルートアカウントまたは IAM ユーザーアカウントのログイン	AWS アカウントまたは IAM ユーザーアカウントにログインする際に、パスワードに加えて要求される 6 桁のワンタイムコードです。
アクセスキー	AWS API へのデジタル署名付きリクエスト(AWS SDK、CLI、または REST/クエリ API を使用)	アクセスキー ID とシークレットアクセスキーが含まれます。アクセスキーを使用して、AWS へのプログラムによるリクエストにデジタル署名します。
キーペア	• EC2 インスタンスへの SSH ログイン • CloudFront の署名付き URL	キーペアは、パブリック AMI から起動された EC2 インスタンスに接続するときに必要になります。Amazon EC2 が使用するキーは、1024-bit SSH-2 RSA キーです。キーペアは、インスタンスの起動時に自動的に生成することも、手動でアップロードすることもできます。
X.509 証明書	• AWS API へのデジタル署名付き SOAP リクエスト • HTTPS 用の SSL サーバー証明書	X.509 証明書は、SOAP ベースのリクエストに署名するときにのみ使用されます(現在は Amazon S3 でのみ使用されています)。AWS ではダウンロード可能な X.509 証明書とプライベートキーを作成できます。また、[Security Credentials] ページを使用して、独自の証明書をアップロードすることもできます。

アカウントの認証情報レポートは、[Security Credentials] ページからいつでもダウンロードできます。このレポートには、アカウントのすべてのユーザーとユーザーの認証情報のステータスが表示されます。ステータスには、パスワードを使用しているかどうか、パスワードの期限切れにより定期的な変更が必要かどうか、パスワードを最後に変更した日時、アクセスキーを最後に更新した日時、MFA が有効になっているかどうかが含まれます。

セキュリティ上の理由から、認証情報を紛失したり忘れたりすると、復元や再ダウンロードを行うことはできません。ただし、新しい認証情報を作成し、古い認証情報のセットを無効化または削除することができます。

さらに、AWS ではアクセスキーと証明書を定期的に変更(更新)することをお勧めしています。アプリケーションの可用性に影響を与えることなくこれらを更新できるように、AWS は複数の並列アクセスキーと証明書をサポートしています。この機能を用いて、アプリケーションを止める必要もなく、定期的にオペレーションの内外でキーと証明書を循環させることができます。これによってアクセスキーまたは証明書を紛失したり、その情報が漏洩したりするリスクを軽減できます。AWS IAM API を使用すると、AWS アカウントのアクセスキーのほか、IAM ユーザーアカウントのアクセスキーを更新できます。

パスワード

AWS アカウント、個々の IAM ユーザーアカウント、AWS フォーラム、および AWS サポートセンターにアクセスするにはパスワードが必要です。パスワードはアカウントの初回作成時に指定しますが、[Security Credentials] ページにアクセスすればいつでも変更できます。AWS パスワードは特殊文字を含めて最大 128 文字まで指定できますので、簡単に推測できない強力なパスワードを作成することをお勧めします。

使用されるパスワードの強度を確保し、パスワードが頻繁に変更されるように、IAM ユーザーアカウントのパスワードポリシーを設定できます。パスワードポリシーは、IAM ユーザーが設定できるパスワードの種類を定義するルールのセットです。パスワードポリシーの詳細については、「IAM の使用」の「パスワードの管理」を参照してください。

AWS Multi-Factor Authentication（AWS MFA）

AWS の Multi-Factor Authentication (AWS MFA) は、AWS サービスにアクセスするための追加のセキュリティのレイヤーです。この任意の機能を有効にした場合、標準ユーザー名とパスワードの認証情報に加えて 6 桁のワンタイムコードを提供するまで、AWS アカウント設定または AWS サービスとリソースにアクセスできません。物理的所有物の中に保存されている認証デバイスから、このワンタイムコードを取得します。アクセスが許可される前に、パスワード（ユーザーが知っているもの）と認証デバイスからの正確なコード（ユーザーが持っているもの）という複数の認証要素が確認されるため、これは多要素認証と呼ばれます。AWS アカウントおよび AWS IAM を使用して、AWS アカウントの下に作成したユーザーの MFA デバイスを有効にできます。さらに、ある AWS アカウントで作成したユーザーが IAM ロールを使用して別の AWS アカウントのリソースにアクセスできるようにする場合は、複数の AWS アカウントをまたぐアクセスに MFA 保護を追加します。追加のセキュリティレイヤーとしてのロールを引き受ける前に、MFA を使用するようにユーザーに要求できます。

AWS MFA は、ハードウェアトークンの使用と仮想 MFA デバイスの使用をサポートします。仮想 MFA デバイスは、物理 MFA のデバイスと同じプロトコルを使用しますが、スマートフォンを含む任意のハードウェアデバイスで動作します。仮想 MFA デバイスとは、6 桁の認証コードを作成するソフトウェアアプリケーションで、RFC 6238 にある Time-Based One-Time Password（TOTP）標準に準拠しています。また、ほとんどの仮想 MFA アプリケーションでは、複数の仮想 MFA デバイスを有効にすることができるので、ハードウェア MFA デバイスよりも便利に利用できます。しかしながら、仮想 MFA が稼働するデバイスはスマートフォンのような安全性の低く、またハードウェア MFA デバイスが提供するようなレベルのセキュリティを実装していない点に留意する必要があります。

Amazon EC2 インスタンスの終了や、Amazon S3 に格納されている重要なデータの読み取りなど、強力なアクションおよび特権アクションに対する追加の保護レイヤーを提供するために、AWS サービス API に MFA 認証を適用することもできます。このためには、IAM ポリシーに MFA 認証の要件を追加します。これらのアクセス ポリシーを IAM ユーザー、IAM グループ、または Amazon S3 のバケット、SQS キュー、および SNS トピックのようなアクセスコントロールリスト（ALC）をサポートするリソースにアタッチできます。

参加するサードパーティのプロバイダーからハードウェア トークン、または AppStore から仮想 MFA アプリケーションを取得し、AWS ウェブサイトで使用するために設定するのは簡単です。AWS MFA の詳細については、AWS のウェブサイト（http://aws.amazon.com/mfa/）をご覧ください。

アクセスキー

AWS では、すべての API リクエストに署名が必要です。つまり、AWS がリクエスタの ID を確認するためのデジタル署名を含める必要があります。デジタル署名は暗号化ハッシュ関数を使用して計算します。この場合、ハッシュ関数に渡される入力データとしては、リクエストのテキスト、およびシークレットアクセスキーが該当します。AWS SDK を使用してリクエストを生成すると、デジタル署名の計算が行われます。AWS SDK を使用しない場合は、ドキュメント [LINK] の指示に従うと、アプリケーションによって計算を行い、生成されたデジタル署名を REST または Query リクエストに含めることができます。

署名プロセスは送信中のリクエストの改ざんを防ぐことでメッセージの整合性を保護するだけでなく、潜在的なリプレイ攻撃の防止にも役立ちます。リクエストは、リクエストのタイムスタンプの 15 分以内に AWS に到達する必要があります。その条件を満たさない場合、AWS はリクエストを拒否します。

デジタル署名計算プロセスの最新バージョンは、HMAC-SHA256 プロトコルを使用して署名を計算する署名バージョン 4 です。バージョン 4 では、シークレットアクセスキー自体を使用するのではなく、シークレットアクセスキーから取得されたキーを使用してメッセージに署名するよう要求することで、以前のバージョンよりも保護がさらに強化されます。また、署名キーの暗号化分離を促進する認証情報スコープに基づいて署名キーを取得します。

アクセスキーが悪意のある第三者の手に渡ると悪用される恐れがあるため、アクセスキーは安全な場所に保管して、コードには埋め込まないようにしてください。頻繁に拡大縮小される大量の EC2 インスタンスを抱えるお客様の場合、IAM ロールを使用すると、アクセスキーの配布をより安全かつ便利に管理できるようになります。IAM ロールは、ターゲットインスタンスに自動的にロードされるだけでなく、1 日に複数回自動的に更新される一時的な認証情報を提供します。

キーペア

パブリック AMI から作成される Amazon EC2 インスタンスは、Secure Shell（SSH）を介してサインインする際に、パスワードではなくパブリック/プライベートのキーペアを使用します。パブリックキーはインスタンスに埋め込まれているため、プライベートキーを使用して、パスワードなしで安全にログインできます。独自 AMI の作成後は、新しいインスタンスに安全にログインするための他のメカニズムを選択できます。

キーペアは、インスタンスの起動時に自動的に生成することも、手動でアップロードすることもできます。プライベートキーをお使いのシステムの安全な場所に保存し、保存した場所を記録します。

Amazon CloudFront では、他のユーザーが料金を支払った制限されたコンテンツを配信する場合など、プライベートコンテンツの署名付き URL を作成するためにキーペアを使用します。[Security Credentials] ページを使用して Amazon CloudFront キーペアを作成します。CloudFront キーペアは、ルートアカウントのみが作成でき、IAM ユーザーが作成することはできません。

X.509 証明書

X.509 証明書は、SOAP ベースのリクエストに署名する際に使用されます。X.509 証明書にはパブリックキーと追加のメタデータ（証明書をアップロードする際に AWS が検証する有効期限など）が含まれ、各証明書はプライベートキーに関連付けられています。リクエストを作成する場合、プライベートキーにデジタル署名を作成してから、その署名を証明書と共にリクエストに含めます。AWS は、証明書のパブリックキーの署名を復号化することで、送信者であることを確認します。AWS は、送信した証明書が AWS にアップロードした証明書と一致することも確認します。

AWS アカウントについては、ダウンロード可能な X.509 証明書とプライベートキーを AWS で作成できます。[Security Credentials] ページを使用して、独自の証明書をアップロードすることもできます。IAM ユーザーについては、サードパーティソフトウェアを使用して X.509 証明書(署名証明書)を作成する必要があります。ルートアカウント認証情報とは異なり、AWS では IAM ユーザーの X.509 証明書を作成することはできません。証明書を作成したら、IAM を使用してその証明書を IAM ユーザーにアタッチします。

SOAP リクエストに加え、X.509 証明書は HTTPS を使用してデータ転送を暗号化する場合の SSL/TLS サーバー証明書としても使用されます。X.509 証明書を HTTPS で使用するには、OpenSSL などのオープンソースツールを使用して独自のプライベートキーを作成します。サーバー証明書を取得する際に認証機関(CA)に送信する証明書署名要求(CSR)を作成するには、プライベートキーが必要になります。その後、AWS CLI を使用して、証明書、プライベートキー、および証明書チェーンを IAM にアップロードします。

また、EC2 インスタンス用にカスタマイズした Linux AMI を作成する際も X.509 証明書が必要です。この証明書が必要なのは、Instance-Backed AMI を作成する場合のみです(EBS-Backed AMI の作成には必要ありません)。AWS ではダウンロード可能な X.509 証明書とプライベートキーを作成できます。また、[Security Credentials] ページを使用して、独自の証明書をアップロードすることもできます。

個々のユーザーアカウント

AWS が提供するのは、AWS アカウント内で個々のユーザーを作成および管理するための、AWS Identity and Access Management (IAM) と呼ばれる一元化されたメカニズムです。ユーザーに指定できるのは、個人やシステム、あるいはアプリケーションです。アプリケーションは、プログラムを使用するか AWS マネジメントコンソールや AWS コマンドラインインターフェイス(CLI)を介して AWS とやり取りします。各ユーザーには、AWS アカウント内で一意の名前が付いており、一意のセキュリティ認証情報セットは、他のユーザーと共有しません。AWS IAM を利用すると、パスワードやアクセスキーを共有する必要がなくなり、AWS アカウント認証情報の使用を最小限に抑えることができます。

IAM では、ユーザーがアクセスできる AWS サービスと、それらのサービスでユーザーが実行できる操作を制御するポリシーを定義します。ユーザーがジョブを実行するのに必要な最小限の権限のみを付与できます。詳細については、以下の「AWS Identity and Access Management(AWS IAM)」のセクションを参照してください。

安全な HTTPS アクセスポイント

AWS リソースにアクセスする際の通信セキュリティを高めるには、データ転送に HTTP ではなく HTTPS を使用します。HTTPS では、傍受、改ざん、偽造の防止にパブリックキー暗号を使用する SSL/TLS プロトコルを使用します。すべての AWS サービスは安全なカスタマアクセスポイント(API エンドポイント)を提供しているため、安全な HTTPS 通信セッションを確立できます。

現在では、Elliptic Curve Diffie-Hellman Ephemeral(ECDHE)プロトコルを使用する、より高度な暗号スイートを提供するサービスもあります。ECDHE を利用すれば、SSL/TLS クライアントで、どの場所にも保存されない一時セッションキーを使用する Perfect Forward Secrecy を利用できます。そのため、長期間使用するシークレットキー自体が漏洩した場合でも、権限のない第三者によるキャプチャされたデータのデコードを防ぐことができます。

セキュリティログ

セキュリティの問題を回避するために認証情報と暗号化されたエンドポイントが重要なのと同じように、問題が発生した後のイベントを理解するためにはログが欠かせません。またセキュリティツールとして有効に活用するために、ログは問題の内容と発生日時のリストを表示するだけでなく、送信元も特定できなければなりません。事後調査およびほぼリアルタイムの侵入検出に役立てるため、AWS CloudTrail はアカウント内の AWS リソースに対するすべてのリクエストのログに対応します。イベントごとに、アクセスされたサービス、実行されたアクション、およびリクエストを確認できます。CloudTrail は、使用するすべての AWS リソースへのすべての API 呼び出し(サインインイベントを含む)に関する情報をキャプチャします。

CloudTrail を有効にすると、5 分間隔でイベントログが送信されます。CloudTrail は、複数のリージョンからのログファイルを 1 つの Amazon S3 バケットに集約するように設定できます。こうすると、使い慣れたログ管理および分析ソリューションにログファイルをアップロードし、セキュリティ分析を実行して、ユーザーの行動パターンを検出できます。デフォルトでは、ログファイルは Amazon S3 に安全に保存されますが、監査やコンプライアンスの要件に合わせてログファイルを Amazon Glacier にアーカイブすることもできます。

CloudTrail のユーザーアクティビティログに加えて、Amazon CloudWatch Logs で、EC2 インスタンスやその他のソースからほぼリアルタイムにシステム、アプリケーション、およびカスタムログファイルの収集とモニタリングを利用できます。たとえば、お客様のウェブサーバーのログファイルに無効なユーザーメッセージがあるかどうかをモニタリングして、お客様のゲスト OS への不正ログインの試みを検出したりできます。

AWS Trusted Advisor セキュリティチェック

AWS Trusted Advisor のカスタマーサポートサービスは、クラウドのパフォーマンスと弾力性だけではなく、クラウドのセキュリティも監視します。このサービスでは、お客様の AWS 環境を検査し、コスト削減、システムパフォーマンス向上、セキュリティギャップの封鎖につながる推奨事項をお知らせします。この機能は、一部のポートが開いたままであるためハッキングや不正アクセスを受けやすい状態や、内部ユーザー用に IAM アカウントを作成していない場合、Amazon S3 バケットへのパブリックアクセスを許可していることや、ユーザーアクティビティログの記録をオンにしていない(AWS CloudTrail)、ルート AWS アカウントで MFA を使用していないなど、起こりうる最も一般的なセキュリティ設定ミスについて警告します。また、Trusted Advisor のセキュリティチェックにおける最新のステータスが記載された E メールが、週に 1 度、組織のセキュリティに関する連絡先に自動的に届くようにすることもできます。

AWS Trusted Advisor サービスでは、すべてのユーザーが追加料金なしで 4 つのチェックを利用できますが、制限されていない特定のポート、IAM の使用、およびルートアカウントの MFA という重要な 3 つのセキュリティチェックが含まれています。また、ビジネスレベルあるいはエンタープライズレベルの AWS サポートを契約すると、Trusted Advisor のすべてのチェックを利用できます。

AWS サービス固有のセキュリティ

セキュリティは、AWS のインフラストラクチャのすべての層だけではなく、そのインフラストラクチャで利用できるすべてのサービスにも組み込まれています。AWS サービスのアーキテクチャは、すべての AWS ネットワークおよびプラットフォームと効率的かつ安全に連動するように設計されています。各サービスに豊富なセキュリティ機能が用意されており、これらを活用して機密データおよびアプリケーションを保護できます。

コンピューティングサービス

アマゾン ウェブ サービスは、お使いのアプリケーションまたは企業のニーズに応じてその規模を自動的にスケールアップまたはスケールダウンできる多彩なコンピューティングインスタンスを含む、クラウドベースのさまざまなコンピューティングサービスを提供します。

Amazon Elastic Compute Cloud(Amazon EC2)のセキュリティ

Amazon Elastic Compute Cloud(EC2)は Amazon の IaaS(Infrastructure as a Service)の重要なコンポーネントであり、AWS のデータセンター内のサーバーインスタンスを使用することにより、規模を自在に変更できる処理能力を提供します。Amazon EC2 は、お客様が最小限の操作で処理能力を取得し、設定できるようにすることで、容易にウェブ規模のコンピューティングを実現できるよう設計されています。お客様がプラットフォームハードウェアとソフトウェアの集合であるインスタンスを作成して起動します。

複数のセキュリティレベル

Amazon EC2 のセキュリティは、ホストプラットフォームのオペレーティングシステム(OS)、仮想インスタンス OS、ゲスト OS、ファイアウォール、署名された API 呼び出しなど、複数のレベルで提供されます。これら各アイテムは、他の機能に追加される形で構築されます。この目的は、Amazon EC2 内に含まれるデータが、未許可のシステムまたはユーザーによって傍受されないようにすると同時に、顧客によるシステム設定の柔軟性を犠牲にすることなく、Amazon EC2 インスタンスそのものが、できるだけ安全であるようにすることです。

ハイパーバイザー

Amazon EC2 は現在、準仮想化を利用して、Xen ハイパーバイザーの高度にカスタマイズされたバージョンを活用しています(Linux ゲストの場合)。準仮想化されたゲストは、特権的なアクセスを必要とする操作のサポートをハイパーバイザーに依存しているため、ゲスト OS は CPU に対して高度なアクセスを持ちません。CPU は、リングと呼ばれる、4 つの独立した特権モード: 0～3 を提供します。リング 0 は、最も権限があり、3 は最も権限がありません。ホスト OS は、リング 0 で実行されます。ほとんどのオペレーティングシステムがリング 0 で実行されますが、ゲスト OS は、リング 0 ではなく、権限の低いリング 1 で実行されます。

また、アプリケーションは最も権限の低いリング 3 で実行されます。物理的リソースに対するこのような明示的仮想化は、ゲストとハイパーバイザーの間に明確な分離をもたらし、結果的に両者の間にセキュリティ上有効な分離を追加することになります。

インスタンスの分離

同一の物理マシン上で実行中の様々なインスタンスが、Xen ハイパーバイザーを経由して互いに分離されます。Amazon は、Xen コミュニティでアクティブに活動しており、これによって最新の開発事項にいち早く対応することができます。さらに、AWS ファイヤウォールは、物理的ネットワークインターフェイスとインスタンスの仮想インターフェイスの間にある、ハイパーバイザー層の中に存在しています。全パケットはこの層を通過しなければなりません。こうして、インスタンス同士が、インターネット上の他のホスト以上に互いにアクセス権を有することはなく、それらがあたかも物理的に分離したホスト上に存在しているかのように扱うことができます。同様のメカニズムをもちいることにより、物理的 RAM も分離しています。

顧客のインスタンスは、ディスクデバイスに対して直接アクセス権をもちませんが、代わりに仮想化されたディスク上に表示されます。AWS 独自のディスク仮想化レイヤーでは、お客様が使用しているストレージのすべてのブロックが自動的にリセットされます。これにより、お客様のデータが他のお客様に意図せずに見えてしまうということがありません。さらに、ゲストに割り当てられたメモリは、ゲストへの割り当てが解除されるとハイパーバイザーによって完全消去（ゼロに設定）されます。メモリは、メモリの完全消去が完了するまで、新しい割り当てに使用可能な空きメモリのプールに返されません。

AWS は、顧客が適切な手段によってデータをさらに保護することを推奨しています。一般的解決方法の 1 つは、仮想化されたディスクデバイス上で、暗号化されたファイルシステムを実行する方法です。

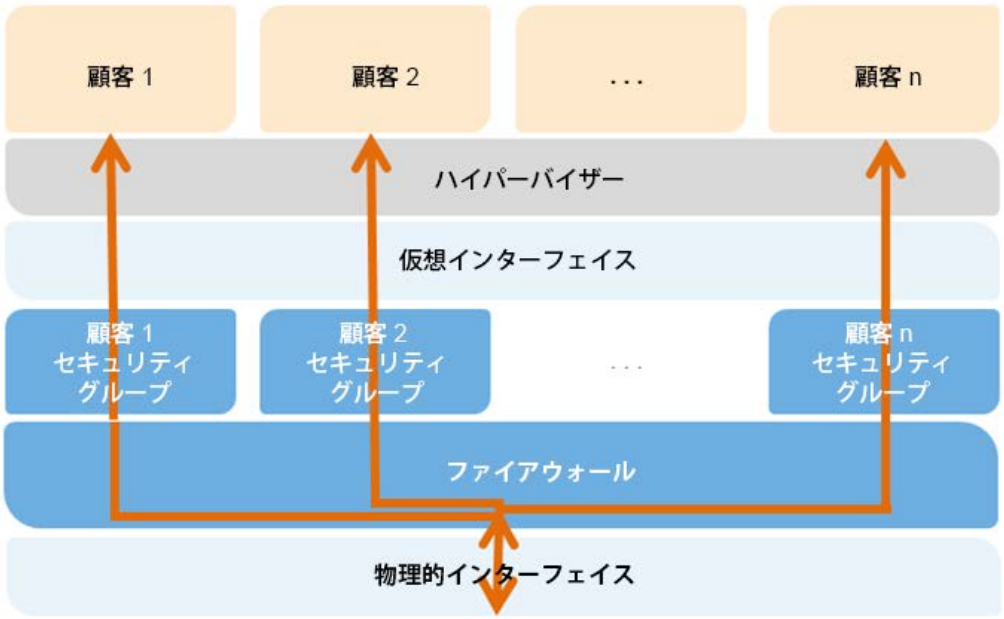


図 3: Amazon EC2 の多重セキュリティレイヤー

ホストオペレーティングシステム: 管理プレーンにアクセスする必要のある作業を担当する管理者は、多要素認証を使用して専用の管理ホストにアクセスする必要があります。これらの管理ホストは、特別に設計、構築、設定されており、クラウドの管理プレーン保護機能を強化したシステムです。これらのアクセスは全て記録され、監査されます。管理プレーンにアクセスする必要のある作業を従業員が完了すると、これらのホストと関連するシステムへの特権とアクセス権を取り消すことができます。

ゲストオペレーティングシステム: 仮想インスタンスは、お客様が管理します。お客様は、アカウント、サービス、およびアプリケーションに対して、完全なルートアクセス権または管理コントロールを持っています。AWS には、お客様のインスタンスまたはゲスト OS に対するアクセス権はありません。セキュリティに関する基本的なベストプラクティスとして、お客様のゲストにパスワードのみでアクセスできないようにすることと、お客様のインスタンスへのアクセスに一定の形式の多要素認証を使用すること（または最低でも証明書ベースの SSH バージョン 2 によるアクセス）を盛り込むことが推奨されます。さらに、お客様は、ユーザーごとに記録される特権エスカレーションメカニズムを採用する必要があります。たとえば、ゲスト OS が Linux の場合、お客様はインスタンスを堅牢化した後、仮想インスタンスにアクセスする、リモート ルートログインを無効にする、コマンドラインのログ機能を使用する、および特権をエスカレーションするための「sudo」を使用するには、証明書ベースの SSHv2 を使用する必要があります。お客様は、キーペアが一意であり、他の顧客または AWS と共有されないことを保証するために、独自のキーペアを生成する必要があります。

AWS は、Secure Shell（SSH）ネットワークプロトコルの使用をサポートしています。これにより、お客様はお客様の UNIX/Linux EC2 インスタンスに安全にログインできます。AWS と併用される SSH の認証は、インスタンスに対する不正アクセスのリスクを軽減するため、パブリックキーとプライベートキーのペアを使用して行われます。お客様のインスタンスに対して生成された Remote Desktop Protocol（RDP）証明書を使用して RDP を利用することによって Windows インスタンスにリモートで接続することもできます。

また、お客様がゲスト OS のセキュリティ更新を含む更新およびパッチ適用を制御します。アマゾンが提供する Windows および Linux ベースの AMI は最新のパッチによって定期的に更新されますので、実行中の Amazon AMI インスタンスでデータまたはカスタム設定を保存する必要がない場合は、最新の更新された AMI で新しいインスタンスを再作成できます。さらに、Amazon Linux AMI の更新は、Amazon Linux yum リポジトリを通して提供されます。

ファイアウォール: Amazon EC2 は、完全なファイアウォールソリューションを提供します。この強制着信ファイアウォールは、デフォルトではすべて拒否するモードに設定されているため、Amazon EC2 の顧客は、着信トラフィックの受け入れに必要なポートを明示的に開く必要があります。トラフィックは、プロトコル、サービスポート、ソース IP アドレス（個別 IP またはクラスなしドメイン間ルーティング（CIDR）ブロック）によって制限される場合があります。

ファイヤウォールは、異なるルールを適用できるよう、インスタンスの異なるクラスを許可するグループ内で設定することができます。例えば、これまでの 3 層ウェブアプリケーションの場合を考えてみてください。ウェブサービスのグループは、インターネットに対してポート 80（HTTP）および／またはポート 443（HTTPS）を開いていることでしょう。アプリケーションサーバーのグループは、（アプリケーションに固有の）ポート 8000 を、ウェブ サーバー グループに対してのみアクセス可能にしているでしょう。データベースサーバーのグループは、ポート 3306（MySQL）を、アプリケーション サーバー グループに対してのみ開いているでしょう。全 3 グループは、ポート 22（SSH）への管理アクセスを許可するでしょう。しかし、これは顧客の企業ネットワークからのみ許可されます。このメカニズムを使用して、極めてセキュリティ能力の高いアプリケーションを配置することができます。以下の図を参照してください：

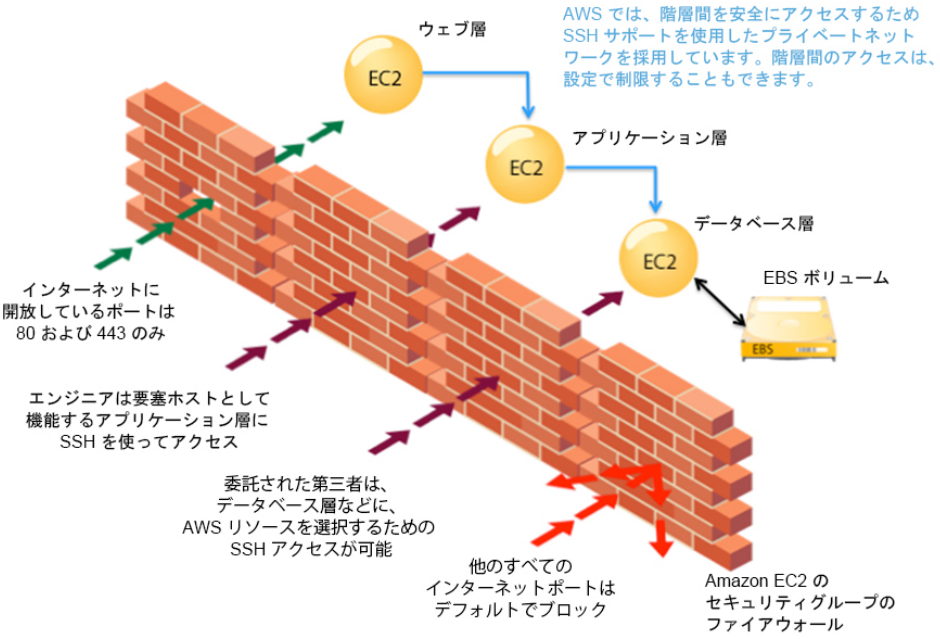


図 4: Amazon EC2 のセキュリティグループのファイアウォール

ファイアウォールはゲスト OS では制御できません。変更を許可してセキュリティレイヤーを追加するには、お客様の X.509 証明書およびキーが必要になります。AWS では、インスタンスおよびファイアウォールのさまざまな管理機能に対して詳細なアクセス権を付与できます。そのため、お客様は職務の分離を通じて追加のセキュリティを実装できます。ファイアウォールによって提供されるセキュリティのレベルは、お客様がどのポートを、どれだけの期間、どのような目的で開くかによって異なります。デフォルトでは、すべての着信トラフィックを拒否するモードになっています。アプリケーションの構築およびセキュリティ設計の際に、どのポートを開くのかを慎重に検討してください。引き続き、インスタンスごとに、十分な情報に基づくトラフィック管理とセキュリティ設計が必要です。さらに、IPtable、Windows Firewall、VPN などのホストベースのファイアウォールを使用して、追加のインスタンス別のフィルタを適用することが推奨されます。これによってインバウンドトラフィックとアウトバウンドトラフィックの両方を制限できます。

API アクセス: インスタンスの起動および終了、ファイアウォールパラメータの変更、およびその他の機能を実行するための API 呼び出しはすべて、お客様の Amazon シークレットアクセスキーによって署名されます。このシークレットアクセスキーは、AWS アカウントのシークレットアクセスキー、または AWS IAM で作成されたユーザーのシークレットアクセスキーのいずれかです。お客様のシークレットアクセスキーにアクセスできなければ、Amazon EC2 API 呼び出しは実行されません。さらに、API 呼び出しは、SSL で暗号化して、機密性を維持することができます。Amazon は、常に SSL で保護された API エンドポイントを使用することを推奨しています。

アクセス権限: AWS IAM では、AWS IAM を使用してユーザーが作成した API のうち、どの API に呼び出し権限を付与するかを制御することもできます。

Elastic Block Storage (Amazon EBS) セキュリティ

Amazon Elastic Block Storage（EBS）では、Amazon EC2 インスタンスによってデバイスとしてマウントできる 1 GB ～ 1 TB のストレージボリュームを作成できます。ストレージボリュームは、未フォーマットの raw ブロックデバイスのように動作し、ユーザーが指定したデバイス名と、ブロックデバイスインターフェイスを持ちます。Amazon EBS ボリュームの上にファイルシステムを構築したり、ブロックデバイスを使用する別の方法（ハードドライブとして使用など）で使用できます。Amazon EBS ボリューム アクセスは、ボリュームを作成した AWS アカウントに限定されます。また、EBS 操作に対するアクセスがユーザーに付与されている場合は、AWS IAM で作成された AWS アカウントのユーザーに限定されます。したがって、その他の AWS アカウントおよびユーザーについては、ボリュームを表示する、またはボリュームにアクセスする権限は付与されません。

Amazon EBS ボリュームに保存されるデータは、これらのサービスの通常オペレーションの一部として、複数の物理的ロケーションで冗長的に保存され、追加費用はかかりません。ただし、Amazon EBS のレプリケーションは、複数のアベイラビリティゾーンに分散されるのではなく、同一のアベイラビリティゾーン内に保存されます。そのため、長期的なデータ堅牢性を考えて、定期的に Amazon S3 にスナップショットを作成することを強くお勧めします。EBS で複合トランザクションデータベースを構築しているお客様には、データベース管理システムを使って Amazon S3 にバックアップを行い、分散トランザクションやログがチェックポイントを使用できるようにしておくことをお勧めします。Amazon EC2 で実行中のインスタンスにアタッチされた仮想ディスクが保持するデータについては、AWS ではバックアップを行いません。

Amazon EBS ボリュームのスナップショットを公開し、それをベースに他の AWS アカウントが自分のボリュームを作成できるようにすることも可能です。Amazon EBS ボリュームのスナップショットを共有しても、他の AWS アカウントにオリジナルスナップショットを変更または削除する権限を与えることにはなりません。その権限はボリュームを作成した AWS アカウントが明示的に保持します。EBS スナップショットは、EBS ボリューム全体に対するブロックレベルのビューです。EBS スナップショットには、削除されたファイルなど、ボリュームのファイルシステムでは見えないデータが含まれる場合があります。共有スナップショットを作成する際は慎重に行ってください。ボリュームが重要なデータを保持している、またはファイルがそのボリュームから削除された場合は、新しい EBS ボリュームを作成します。共有スナップショットに含まれるデータは、新しいボリュームや、新しいボリュームから作成されたスナップショットにコピーします。

Amazon EBS ボリュームは、ワイプ処理を行った後、未フォーマットのローブロックデバイスとしてお客様に提供されます。ワイプは再使用の直前に実施されるため、お客様に提供された時点でワイプ処理は完了しています。業務手順上、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」)や NIST 800-88(「媒体のサニタイズに関するガイドライン」)が指定するような、特定の方法で全データをワイプする必要がある場合、お客様自身で Amazon EBS のワイプ作業を行うこともできます。お客様がしかるべき手順でワイプを実施してからボリュームを削除することで、コンプライアンスの要件を満たすようにします。

機密データの暗号化は、一般的なセキュリティのベストプラクティスです。AWS には、EBS ボリュームとスナップショットを AES-256 で暗号化する機能があります。EC2 インスタンスをホストするサーバーで暗号化が行われるため、EC2 インスタンスと EBS ストレージとの間を移動するデータが暗号化されます。この処理が効率的に低レイテンシーで行われるようにするために、EBS 暗号化機能は EC2 の強力なインスタンスタイプ(たとえば、M3、C3、R3、G2)だけで使用できます。

Auto Scaling のセキュリティ

Auto Scaling を使用すると、お客様が定義した条件に従って Amazon EC2 容量が自動的に拡大または縮小するよう指定できます。したがって、使用される Amazon EC2 インスタンスの数は、需要が急激に増える時間帯はパフォーマンスを維持するためにシームレスに増え、需要が少ないときはコストを最小限に抑えるために自動的に少なくなります。

他の AWS サービスと同様に、Auto Scaling のコントロール API に対するすべてのリクエストが認証される必要があります。これにより、許可されたユーザーのみが Auto Scaling にアクセスし、管理することができます。リクエストには、リクエストとユーザーの秘密鍵から生成された HMAC-SHA1 署名が添付されます。ただし、Auto Scaling で起動される新しい EC2 インスタンスに認証情報を提供することは、インスタンス群が大規模であったり柔軟に拡大縮小したりする場合には、困難な場合があります。このプロセスを簡素化するには、IAM 内でロールを使用します。ロールを使用して起動された新しいインスタンスには、自動的に認証情報が提供されます。IAM ロールを使用して EC2 インスタンスを起動すると、ロールが指定するアクセス許可を持つ一時的な AWS セキュリティ認証情報が安全にプロビジョニングされ、Amazon EC2 インスタンスのメタデータサービスを通してアプリケーションで使用できるようになります。メタデータサービスは、現在のアクティブな認証情報の有効期限が切れる前に新しい一時的なセキュリティ認証情報を使用できるようにするので、インスタンスには常に有効な認証情報があります。さらに、一時的なセキュリティ認証情報は 1 日に複数回、自動的に変更されるため、より高いセキュリティが確保されます。AWS IAM を使用してお客様の AWS アカウントでユーザーを作成し、これらのユーザーがどの Auto Scaling API に対して呼び出し権限を持つかを制御することによって、Auto Scaling へのアクセスをさらに細かく制御できます。インスタンスを起動する際のロールの使用の詳細については、AWS ウェブサイトの Amazon EC2 ユーザーガイド(http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM)をご覧ください。

ネットワークサービス

アマゾン ウェブ サービスは幅広いネットワーキングサービスを提供しており、論理的に分離されたネットワークを作成して定義し、AWS クラウドに対するプライベートネットワーク接続を確立し、高い可用性でスケーラブルな DNS サービスを使用して、低レイテンシーで高速なデータ転送のコンテンツ配信ウェブサービスをエンドユーザーに提供できます。

Amazon Elastic Load Balancing のセキュリティ

Amazon Elastic Load Balancing は、Amazon EC2 インスタンス群のトラフィック管理に使用され、インスタンスへのトラフィックをリージョン内のすべての Availability Zone に分散します。Elastic Load Balancing にはオンプレミスのロードバランサーという利点のほかに、以下のようなセキュリティ面でのメリットがあります。

- Amazon EC2 インスタンスから暗号化および復号化の作業を引き継いで、ロードバランサーで集中管理します。

- クライアントにとって単一の通信先となるだけでなく、ネットワークへの攻撃に対する最前線の防御機能も持ちます。
- Amazon VPC で使用する際は、追加のネットワークおよびセキュリティオプションを提供するために、Elastic Load Balancing に関連付けられているセキュリティグループを作成および管理できます。
- 安全な HTTP(HTTPS)接続を使用しているネットワークで、TLS(以前の SSL)を使用したエンドツーエンドのトラフィック暗号化がサポートされます。TLS を使用する場合は、クライアント接続の終了に使用する TLS サーバー証明書を、個々のインスタンスではなく、ロードバランサーで集中管理できます。

HTTPS/TLS は、ロングタームシークレットキーを使用して、サーバーとブラウザの間で使用されるショートタームセッションキーを生成し、暗号化されたメッセージを作成します。Amazon Elastic Load Balancing は、クライアントとロードバランサーの間で接続が確立されるときに TLS ネゴシエーションに使用される事前定義された暗号セットと連動するようにロードバランサーを設定します。事前定義された暗号セットは幅広いクライアントと互換性があり、強力な暗号アルゴリズムを採用しています。ただし、一部のお客様ではセキュリティの基準を確実に満たすために、クライアントからの特定の暗号とプロトコル(PCI、SOX など)のみを許可するための要件がある場合があります。このような場合、Amazon Elastic Load Balancing は、TLS プロトコルと暗号に異なる設定を選択するためのオプションを提供します。お客様固有の要件に従って、暗号を有効または無効にすることが可能です。

安全な接続を確立するときに新しい強力な暗号スイートが確実に使用されるようにするため、クライアント/サーバーネゴシエーション中にロードバランサーが暗号スイートの選択を最終決定するように設定できます。[Server Order Preference] オプションを選択すると、ロードバランサーはクライアントではなくサーバーの暗号スイート優先順位に基づいて暗号スイートを選択します。これにより、クライアントがロードバランサーへの接続に使用するセキュリティレベルを細かく制御できるようになります。

通信のプライバシーをさらに高めるため、Amazon Elastic Load Balancing では、どこにも保存されないエフェメラルなセッションキーを使用する Perfect Forward Secrecy を使用できます。そのため、長期間使用するシークレットキー自体が漏洩した場合でも、キャプチャされたデータのデコードを防ぐことができます。

Amazon Elastic Load Balancing を使用すると、HTTPS または TCP どちらの負荷分散を使用していても、サーバーに接続している接続元 IP アドレスを特定できます。通常、リクエストがロードバランサーを通じてプロキシされると、IP アドレスやポートなどのクライアント接続情報が失われます。これは、ロードバランサーがクライアントの代わりにサーバーにリクエストを送信するため、ロードバランサーが要求元のクライアントであるかのように見えるからです。接続統計の収集、トラフィックログの分析、または IP アドレスのホワイトリストの管理を行うために、アプリケーションへのアクセス元に関する詳しい情報が必要な場合は、発生元クライアントの IP アドレスがわかっていると便利です。

Amazon Elastic Load Balancing アクセスログには、ロードバランサーにより処理される各 HTTP および TCP リクエストに関する情報が含まれています。これには、クライアントの IP アドレスとポート、要求を処理したインスタンスのバックエンド IP アドレス、リクエストおよび応答のサイズ、クライアントからの実際の応答メッセージ(例: GET http://www.example.com: 80/HTTP/1.1)が含まれています。バックエンドのインスタンスに到達しなかったリクエストを含め、ロードバランサーに送信されたすべてのリクエストが記録されます。

Amazon Virtual Private Cloud（Amazon VPC）のセキュリティ

通常、起動する Amazon EC2 インスタンスごとに Amazon EC2 アドレス空間内のパブリック IP アドレスがランダムに割り当てられます。Amazon VPC を使用すると、AWS クラウド内に独立した部分を作成して、特定の範囲内（例: 10.0.0.0/16）のプライベート（RFC 1918）アドレスを持つ Amazon EC2 インスタンスを起動することができます。VPC 内で IP アドレス範囲に基づいて同種のインスタンスをグループ化するサブネットを定義して、インスタンスおよびサブネットに出入りするトラフィックの流れを制御するルーティングとセキュリティを設定することができます。

AWS では各種 VPC アーキテクチャテンプレートを使用でき、これらを使用してさまざまなレベルのパブリックアクセスを提供できます。

- **1 つのパブリックサブネットのみを持つ VPC。**インスタンスは、インターネットに直接アクセスできる AWS クラウドの独立したプライベートセクションで実行されます。インスタンスのインバウンドおよびアウトバウンドネットワークトラフィックを厳重に管理するには、ネットワーク ACL とセキュリティグループを使用します。
- **パブリックサブネットとプライベートサブネットを持つ VPC。**この設定は、パブリックサブネットに加えて、インターネットからアドレスを指定できないインスタンスを持つプライベートサブネットを追加します。プライベートサブネットのインスタンスは、ネットワークアドレス変換（NAT）を使用してパブリックサブネットを介してインターネットへのアウトバウンド接続を確立できます。
- **パブリックサブネット、プライベートサブネット、およびハードウェア VPN アクセスを持つ VPC。**この設定は、Amazon VPC とデータセンターの間に IPsec VPN 接続を追加して、実質的にデータセンターをクラウドに拡張すると同時に、Amazon VPC のパブリックサブネットのインスタンスがインターネットに直接アクセスできるようにします。この構成では、自社データセンター側に VPN アプライアンスを追加します。
- **プライベートサブネットのみとハードウェア VPN アクセスを持つ VPC。**インスタンスは、インターネットからアドレスを指定できないインスタンスを持つプライベートサブネットが含まれる AWS クラウドの独立したプライベートセクションで実行されます。このプライベートサブネットは、IPsec VPN トンネルを介して自社データセンターに接続できます。

プライベート IP アドレスを使用して 2 つの VPC を接続して、2 つの VPC 内のインスタンスが同じネットワークにあるかのように相互に通信できるようにすることもできます。VPC ピア接続は、自分の VPC 間、または 1 つのリージョン内の他の AWS アカウントにある VPC との間に作成できます。

Amazon VPC 内のセキュリティ機能には、セキュリティグループ、ネットワーク ACL、ルーティングテーブル、外部ゲートウェイなどがあります。この各アイテムは補完的なもので、インターネットへの直接アクセス有効にするか、他のネットワークにプライベート接続するかを選択することで拡張できる、安全で独立したネットワークを提供します。Amazon VPC 内で実行される Amazon EC2 インスタンスは、以下に説明する、ゲスト OS およびパケット盗聴に対する保護に関連するすべての利点を継承します。ただし、Amazon VPC 専用のセキュリティグループを作成する必要があります。お客様が作成した Amazon EC2 のセキュリティグループは、Amazon VPC 内では正常に機能しません。また、Amazon VPC のセキュリティグループには、Amazon EC2 のセキュリティグループにない追加の機能があります。たとえば、インスタンスが起動された後にセキュリティグループを変更したり、標準のプロトコル番号を持つ任意のプロトコル（TCP、UDP、または ICMP だけではなく）を指定したりできます。

各 Amazon VPC は、クラウド内の独立したネットワークです。各 Amazon VPC 内のネットワークトラフィックは、他のすべての Amazon VPC から独立しています。各 Amazon VPC の IP アドレス範囲は作成時に選択します。インターネットゲートウェイ、仮想プライベートゲートウェイ、またはその両方を作成し、接続して、外部接続を確立します。これは以下のコントロールの影響を受けます。

API アクセス: Amazon VPC の作成と削除、ルーティングの変更、セキュリティグループの変更、ネットワーク ACL パラメータの変更、およびその他の機能を実行するための呼び出しは、お客様の Amazon シークレットアクセスキーによって署名されます。このシークレットアクセスキーは、AWS アカウントのシークレットアクセスキー、または AWS IAM で作成されたユーザーのシークレットアクセスキーのいずれかです。お客様のシークレットアクセスキーにアクセスできなければ、Amazon VPC API 呼び出しは実行されません。さらに、API 呼び出しは、SSL で暗号化して、機密性を維持することができます。Amazon は、SSL で保護された API エンドポイントを常に使用することを推奨しています。AWS IAM を使用すると、どの API に対して、新しく作成されたユーザーが呼び出し権限を持つようにするかを詳細にコントロールできます。

サブネットおよびルートテーブル: お客様は、各 Amazon VPC 内に 1 つ以上のサブネットを作成します。Amazon VPC で起動された各インスタンスは、1 つのサブネットに接続されます。MAC スプーフィング、ARP スプーフィングなど、従来のレイヤー2 セキュリティ攻撃がブロックされます。

Amazon VPC 内の各サブネットはルーティングテーブルに関連付けられています。サブネットからのネットワークトラフィックはすべてルーティングテーブルによって処理され、その宛先が判断されます。

ファイアウォール(セキュリティグループ): Amazon EC2 のように、Amazon VPC は完全なファイアウォールソリューションをサポートしているため、インスタンスのインバウンドトラフィックとアウトバウンドトラフィックの両方をフィルタできます。デフォルトのグループでは、同じグループ内の他のメンバーからの着信通信、および任意の宛先への発信通信が有効になっています。トラフィックは、IP プロトコル、サービスポート、ソース／宛先 IP アドレス(個別 IP またはクラスなしドメイン間ルーティング(CIDR)ブロック)で制限できます。

ファイアウォールは、ゲスト OS では制御されず、Amazon VPC API を起動することでのみ変更できます。AWS では、インスタンスおよびファイアウォールのさまざまな管理機能に対して詳細なアクセス権を付与できます。そのため、お客様は職務の分離を通じて追加のセキュリティを実装できます。ファイアウォールによって提供されるセキュリティのレベルは、お客様がどのポートを、どれだけの期間、どのような目的で開くかによって異なります。引き続き、インスタンスごとに、十分な情報に基づくトラフィック管理とセキュリティ設計が必要です。さらに、IPtable や Windows Firewall などのホストベースのファイアウォールを使用して、追加のインスタンス別のフィルタを適用することが推奨されます。

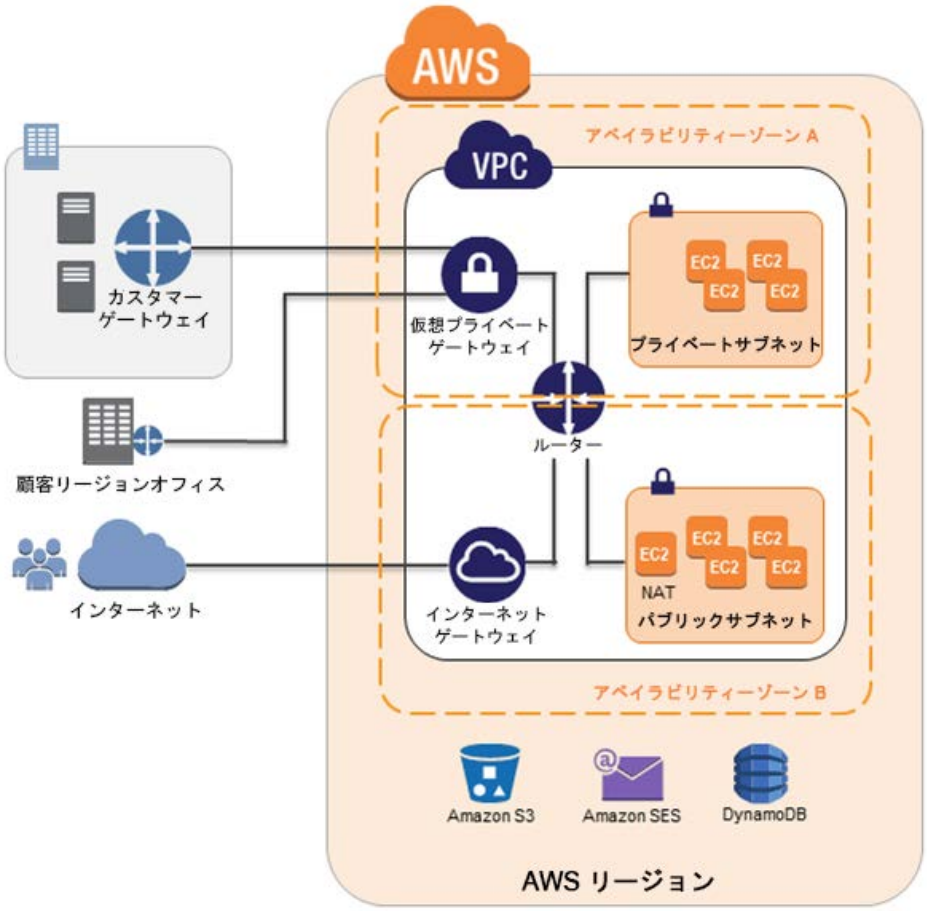


図 5: Amazon VPC のネットワークアーキテクチャ

ネットワークアクセスコントロールリスト: Amazon VPC 内にさらにセキュリティレイヤーを追加するには、ネットワーク ACL を設定します。これらは、Amazon VPC 内のサブネットのすべてのインバウンドトラフィックおよびアウトバウンドトラフィックに適用されるステートレスのトラフィックフィルタです。ACL には順序付けされたルールが含まれており、IP プロトコル、サービスポート、ソース／宛先 IP アドレスに基づいてトラフィックを許可または拒否できます。

セキュリティグループと同様、ネットワーク ACL は Amazon VPC API で管理され、保護レイヤーを追加したり、職務の分離によって追加セキュリティを有効にしたりします。以下の図は、上記のセキュリティコントロールがどのように関連し合い、柔軟なネットワークトポロジを実現しながら、ネットワーク トラフィック フローを完全にコントロールするかを示しています。

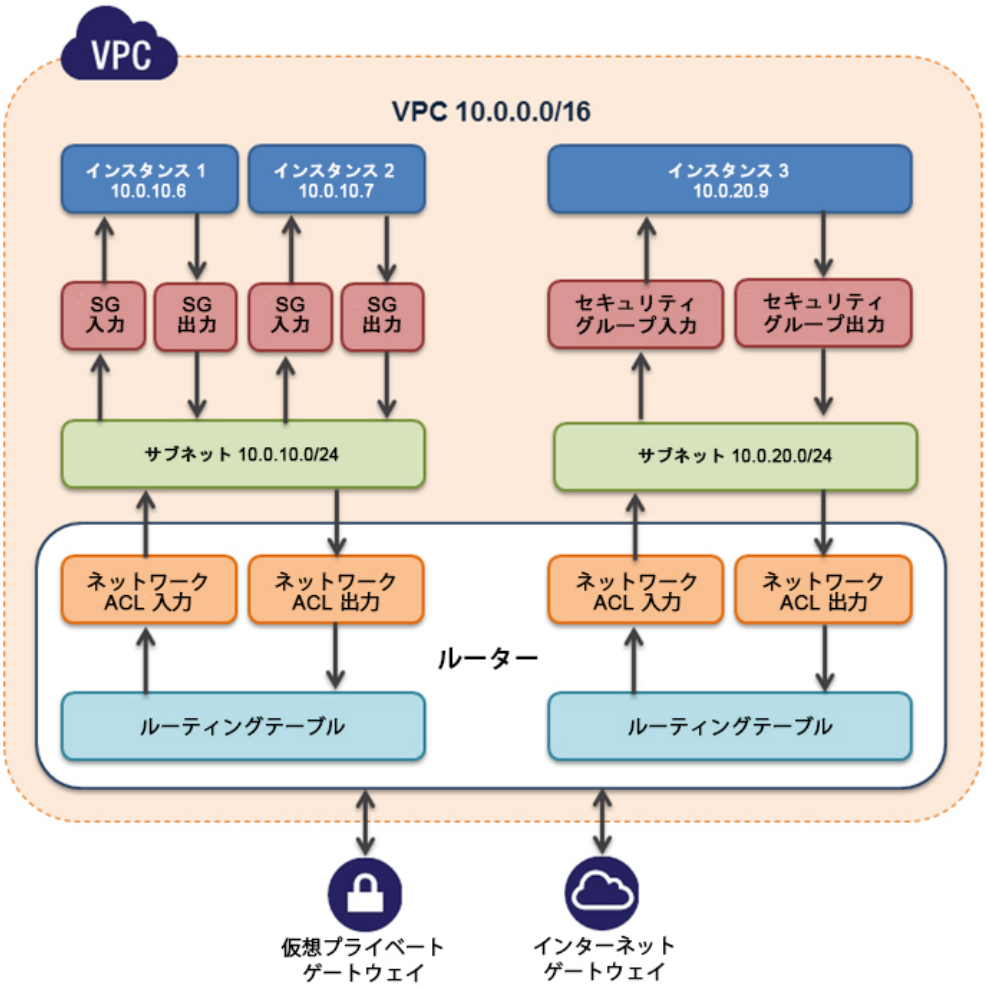


図 6: 柔軟なネットワークトポロジ

仮想プライベートゲートウェイ: 仮想プライベートゲートウェイを使用すると、Amazon VPC と別のネットワークのプライベート接続が可能です。各プライベートゲートウェイ内のネットワークトラフィックは、他のすべてのプライベートゲートウェイ内のネットワークトラフィックから切り離されています。オンプレミスのゲートウェイのデバイスから仮想プライベートゲートウェイへの VPN 接続を確立できます。各接続は、事前に共有されたキーと、顧客のゲートウェイデバイスの IP アドレスの組み合わせによって保護されます。

インターネットゲートウェイ: インターネットゲートウェイを Amazon VPC に接続することにより、Amazon S3、その他の AWS サービス、およびインターネットへの直接接続が可能です。このアクセスを必要とする各インスタンスには、そのインスタンスに関連付けられた Elastic IP または NAT インスタンスを介したルートトラフィックが必要です。さらに、ネットワークルートは、トラフィックがインターネットゲートウェイに向かうように設定されています(上を参照)。AWS では、参照 NAT AMI を拡張して、ネットワークロギング、詳細なパケット検査、アプリケーション層フィルタリング、またはその他のセキュリティ制御を実行できます。

このアクセスは、Amazon VPC API を起動することでのみ変更できます。AWS では、インスタンスおよびインターネットゲートウェイのさまざまな管理機能に対して詳細なアクセス権を付与できます。そのため、お客様は職務の分離を通じて追加のセキュリティを実装できます。

ハードウェア専有インスタンス: VPC では、ホストのハードウェアレベルで物理的に分離された Amazon EC2 インスタンスを起動できます(これらは単一テナントハードウェアで実行されます)。Amazon VPC は "専有" テナンシーを使用して作成できるため、Amazon VPC で起動されたすべてのインスタンスがこの機能を利用できます。または、"デフォルト" テナンシーを使用して Amazon VPC を作成することもできますが、その場合は、そこで起動した特定のインスタンスに対して専有テナンシーを指定できます。

Elastic Network Interface: 各 Amazon EC2 インスタンスにはデフォルトのネットワークインターフェイスがあり、これには Amazon VPC ネットワークのプライベート IP アドレスが割り当てられています。Amazon VPC 内の Amazon EC2 インスタンスには、Elastic Network Interface(ENI)と呼ばれるネットワークインターフェイスを追加で作成してアタッチすることができ、インスタンスあたり合計 2 つのネットワークインターフェイスを使用することができます。インスタンスに複数のネットワークインターフェイスをアタッチできることは、管理ネットワークを作成する、Amazon VPC でネットワークおよびセキュリティアプライアンスを使用する、または別のサブネットの作業負荷/ロールを使用してデュアルホーム接続インスタンスを作成する際に便利です。プライベート IP アドレス、Elastic IP アドレス、および MAC アドレスなどの ENI 属性は、インスタンスとのアタッチやデタッチ、別のインスタンスとの再アタッチを行っても ENI で維持されます。Amazon VPC の詳細については、AWS のウェブサイト(http://aws.amazon.com/vpc/)をご覧ください。

EC2-VPC での追加のネットワークアクセスコントロール

AWS が新しい EC2-VPC 機能(デフォルトの VPC とも呼ばれる)を起動する前にはインスタンスがなかったリージョンでインスタンスを起動すると、すべてのインスタンスが、すぐに利用できるデフォルトの VPC で自動的にプロビジョニングされます。追加の VPC を作成することも、EC2-VPC を起動する前にインスタンスがあったリージョンのインスタンス用の VPC を作成することもできます。

通常の VPC を使用して後で VPC を作成する場合は、CIDR ブロックを指定し、サブネットを作成して、これらのサブネットのルーティングとセキュリティを入力します。サブネットのいずれかがインターネットにアクセスできるようにする場合は、インターネットゲートウェイまたは NAT インスタンスをプロビジョニングします。EC2-VPC で EC2 インスタンスを起動すると、この作業のほとんどが自動的に行われます。EC2-VPC を使用してデフォルトの VPC でインスタンスを起動する場合は、以下の処理が自動的に行われてインスタンスが設定されます。

- 各 Availability Zone にデフォルトのサブネットを作成する
- インターネットゲートウェイを作成してデフォルトの VPC に接続する
- インターネットに向かうすべてのトラフィックをインターネットゲートウェイに送信するルールを持つデフォルトの VPC のメインルートテーブルを作成する
- デフォルトのセキュリティグループを作成してデフォルトの VPC に関連付ける
- デフォルトのネットワークアクセスコントロールリスト(ACL)を作成してデフォルトの VPC に関連付ける
- AWS アカウントのデフォルトの DHCP オプションセットをデフォルトの VPC に関連付ける

デフォルト VPC には独自のプライベート IP 範囲があるだけではなく、デフォルトの VPC で起動された EC2 インスタンスにはパブリック IP を割り当てることもできます。

次の表は、EC2-Classic で起動したインスタンス、デフォルトの VPC で起動したインスタンス、およびデフォルトの VPC 以外で起動したインスタンスの違いをまとめたものです。

特徴	EC2-Classic	EC2-VPC（デフォルト VPC）	通常の VPC
パブリック IP アドレス	インスタンスはパブリック IP アドレスを受け取ります。	デフォルトサブネットで起動したインスタンスは、パブリック IP アドレスをデフォルトで受け取ります。ただし、起動時に別のアドレスを指定した場合を除きます。	インスタンスは、起動時に別のアドレスを指定した場合を除き、パブリック IP アドレスをデフォルトで受け取りません。
プライベート IP アドレス	インスタンスは、起動するたびに、EC2-Classic の範囲に含まれるプライベート IP アドレスを受け取ります。	インスタンスはデフォルト VPC のアドレス範囲から静的プライベート IP アドレスを受け取ります。	インスタンスは VPC のアドレス範囲から静的プライベート IP アドレスを受け取ります。
複数のプライベート IP アドレス	インスタンスに対して 1 つの IP アドレスを選択します。複数の IP アドレスはサポートされていません。	複数のプライベート IP アドレスを 1 つのインスタンスに割り当てることができます。	複数のプライベート IP アドレスを 1 つのインスタンスに割り当てることができます。
Elastic IP アドレス	停止すると、EIP とインスタンスの関連付けが解除されます。	停止しても、EIP とインスタンスの関連付けが維持されます。	停止しても、EIP とインスタンスの関連付けが維持されます。
DNS ホスト名	DNS ホスト名はデフォルトで有効化されています。	DNS ホスト名はデフォルトで有効化されています。	DNS ホスト名はデフォルトで無効化されています。
セキュリティグループ	セキュリティグループは、その他の AWS アカウントに属するセキュリティグループを参照できます。	セキュリティグループは、VPC のみのセキュリティグループを参照できます。	セキュリティグループは、VPC のみのセキュリティグループを参照できます。
セキュリティグループの関連付け	インスタンスを強制終了し、そのセキュリティグループを変更する必要があります。	実行中のインスタンスのセキュリティグループを変更できます。	実行中のインスタンスのセキュリティグループを変更できます。
セキュリティグループのルール	インバウンドトラフィックのみにルールを追加できます。	インバウンドトラフィックとアウトバウンドトラフィックのルールを追加できます。	インバウンドトラフィックとアウトバウンドトラフィックのルールを追加できます。
テナンシー	インスタンスは共有ハードウェアで実行されます。シングルテナントハードウェアでインスタンスを実行することはできません。	共有ハードウェアまたはシングルテナントハードウェアでインスタンスを実行できます。	共有ハードウェアまたはシングルテナントハードウェアでインスタンスを実行できます。

EC2-Classic のインスタンスのセキュリティグループは、EC2-VPC のインスタンスのセキュリティグループとは若干異なります。たとえば、EC2-Classic ではインバウンドトラフィックのルールを追加できますが、EC2-VPC ではインバウンドトラフィックとアウトバウンドトラフィックの両方のルールを追加できます。EC2-Classic ではインスタンスを起動した後にインスタンスに割り当てたセキュリティグループを変更できませんが、EC2-VPC ではインスタンスを起動した後にインスタンスに割り当てたセキュリティグループを変更できます。さらに、EC2-Classic で使用するために作成したセキュリティグループを VPC のインスタンスで使用することはできません。VPC のインスタンスで使用するためのセキュリティグループを特別に作成する必要があります。VPC のセキュリティグループで使用するために作成したルールは、EC2-Classic のセキュリティグループを参照できません。その逆も同様です。

Amazon Route 53 のセキュリティ

Amazon Route 53 は、可用性が高いスケーラブルなドメインネームシステム (DNS) サービスであり、コンピュータが相互に通信できるようにするため、DNS クエリに応答してドメイン名を IP アドレスに変換します。Route 53 は、Amazon EC2 インスタンスや Amazon S3 バケットなどの AWS で実行するインフラストラクチャ、または AWS 外のインフラストラクチャにユーザーリクエストを接続するために使用できます。

Amazon Route 53 によって、ドメイン名に対してリストされる IP アドレス（レコード）を管理でき、また特定のドメイン名を対応する IP アドレスに変換するリクエスト（クエリ）に応答します。ドメインに対するクエリは、レイテンシーを可能な限り最も小さくするために、エニーキャストを使用して近隣の DNS サーバーに自動的にルーティングされます。Route 53 では、レイテンシーベースルーティング (LBR)、Geo DNS、加重ラウンドロビン (WRR) など、さまざまなルーティングタイプを通じてトラフィックをグローバルに管理できます。これらすべては、DNS フェイルオーバーと組み合わせて、各種の低レイテンシー、フォルトトレラントアーキテクチャを実現できます。Amazon Route 53 に実装されたフェイルオーバーアルゴリズムは、正常なエンドポイントにトラフィックをルーティングするだけでなく、ヘルスチェックやアプリケーションの設定ミス、エンドポイントの過負荷、分断障害などに起因する最悪のシナリオを回避するように設計されています。

また、Route 53 ではドメイン名登録も提供します。example.com のようなドメイン名を購入および管理でき、Route 53 でお客様のドメインのデフォルト DNS 設定が自動的に構成されます。ドメインは、さまざまな汎用および国別の最上位ドメイン (TLD) の中から購入、管理、譲渡（転入または転出）できます。登録手続きの際に、ドメインのプライバシー保護を有効にするオプションがあります。このオプションを選択すると、スクラップやスパムを防止するため、公開 Whois データベースにほとんどの個人情報が登録されません。

Amazon Route 53 は、AWS の高い可用性と信頼性を備えるインフラストラクチャを使用して構築されています。AWS DNS サーバーの分散性により、エンドユーザーを確実にアプリケーションにルーティングします。Route 53 は、ヘルスチェックや DNS フェイルオーバー機能を提供することで、ウェブサイトの可用性を確保します。ウェブサイトの状態を定期的に確認し（SSL 経由でのみ利用できる安全なウェブサイトでも）、プライマリウェブサイトが応答しない場合にバックアップサイトに切り替えられるよう、Route 53 を簡単に設定することができます。

Amazon Route 53 では、すべての AWS サービスと同様に、サービスのコントロール API に対する全リクエストに認証が必要です。したがって、許可されたユーザーのみが、Route 53 にアクセスし、管理することができます。API リクエストは、リクエストから生成された HMAC-SHA1 または HMAC-SHA256 署名と、ユーザーの AWS シークレットアクセスキーによって署名されます。さらに、Amazon Route 53 コントロール API には、SSL により暗号化されたエンドポイント経由でのみアクセスできます。また、IPv4 と IPv6 の両ルーティングがサポートされます。

AWS IAM を使用して AWS アカウントに紐づくユーザーを作成し、Amazon Route53 へのアクセスを制御でき、Route 53 の実行権限を持つユーザーの管理ができます。

Amazon CloudFront のセキュリティ

Amazon CloudFront によってお客様は、短いレイテンシーと高いデータ転送速度で、エンドユーザーにコンテンツを簡単に配信できます。Amazon CloudFront は、エッジロケーションのグローバルなネットワークを利用して、動的、静的、ストリーミングのコンテンツを配信します。お客様のオブジェクトのリクエストは、最寄りのエッジロケーションに自動的にルーティングされます。そのためコンテンツは、可能な限り最良のパフォーマンスで配信されます。Amazon CloudFront は、Amazon S3、Amazon EC2、Amazon Elastic Load Balancing、Amazon Route 53 など、他の AWS サービスとの処理のために最適化されています。また、オリジナルの最終ファイルが格納されている AWS 以外のオリジンサーバーともシームレスに連携します。

Amazon CloudFront では、サービスのコントロール API に対する全リクエストに認証が必要です。したがって、許可されたユーザーのみが、そのユーザーの Amazon CloudFront の配信物を作成、変更、または削除できます。リクエストには、リクエストとユーザーの秘密鍵から生成された HMAC-SHA1 署名が添付されます。さらに、Amazon CloudFront コントロール API には、SSL が有効なエンドポイント経由でのみアクセスできます。

Amazon CloudFront エッジロケーション内で保有されるデータの堅牢性は保証されません。これらのオブジェクトが頻繁にリクエストされない場合、当サービスがエッジロケーションからオブジェクトを削除することがあります。堅牢性は、Amazon S3 によって提供されます。Amazon S3 は、Amazon CloudFront のオリジンサーバーとして機能し、Amazon CloudFront が提供するオブジェクトの、オリジナルかつ最新版が格納されます。

Amazon CloudFront からコンテンツを誰がダウンロードできるのか管理したい場合、サービスのプライベートコンテンツ機能を有効にすることができます。この機能には、次の 2 つのコンポーネントがあります。1 つ目は、Amazon CloudFront エッジロケーションから、インターネット上の閲覧者にコンテンツが配信される方法を制御するものです。2 つ目は、Amazon S3 内で、オブジェクトに対して、Amazon CloudFront エッジロケーションがアクセスする方法を制御するものです。CloudFront では、閲覧者の地理的場所に基づいてコンテンツへのアクセスを制限する地域制限がサポートされます。

Amazon S3 内でオブジェクトのオリジナルコピーに対するアクセスを制御するために、Amazon CloudFront は、1 つ以上の [オリジンアクセス識別子] を作成して、これらをお客様の配信物と関連付けます。オリジンアクセス識別子が Amazon CloudFront の配信物と関連づけられる場合、配信物はこの識別子を使って Amazon S3 からオブジェクトを取得します。そして、Amazon S3 の ACL 機能を利用できます。これはオブジェクトのオリジナルコピーが公開されないように、オリジンアクセス識別子へのアクセスを制限します。

Amazon CloudFront エッジロケーションからオブジェクトをダウンロードできるユーザーを制御するために、このサービスは署名付きの URL 認証システムを使用します。このシステムを使用するには、最初に公開鍵と秘密鍵のペアを作成し、AWS マネジメントコンソールを通じてアカウントに公開鍵をアップロードします。次に、Amazon CloudFront の配信物を設定し、リクエストに署名する権限を付与したいアカウントを指定します。リクエストに署名できるアカウントとして、信頼できる AWS アカウントを 5 つまで指定できます。そして、コンテンツにサービスを提供する Amazon CloudFront の条件を指定するポリシー文書を作成します。これらのポリシー文書では、リクエストされたオブジェクト名、リクエストの日付と時刻、リクエストを行なった顧客のソース IP (または CIDR レンジ) を指定できます。その後、ポリシー文書の SHA1 ハッシュを計算し、秘密鍵をもちいてこれに署名します。最後に、お客様がオブジェクトを参照する場合、暗号化されたポリシー文書と署名の両方を、クエリ文字列パラメータとして含めます。Amazon CloudFront がリクエストを受け取ると、お客様の公開鍵を用いて署名を復号します。Amazon CloudFront は、有効なポリシー文書と一致する署名をもつリクエストに対してのみサービスを提供します。

プライベートコンテンツはオプション機能であり、CloudFront 配信の設定時に有効にする必要があります。この機能を有効にしない場合、配信されるコンテンツは、一般に公開されます。

Amazon CloudFront には、暗号化された接続(HTTPS)を通じてコンテンツを転送するオプションが用意されています。デフォルトでは、CloudFront は HTTP および HTTPS プロトコルの両方でリクエストを受け付けます。ただし、すべてのリクエストに HTTPS を必須にしたり、CloudFront が HTTP リクエストを HTTPS にリダイレクトするように CloudFront を設定することもできます。一部のオブジェクトで HTTP を許可するが、他のオブジェクトでは HTTPS を必須にするように、CloudFront ディストリビューションを設定することもできます。

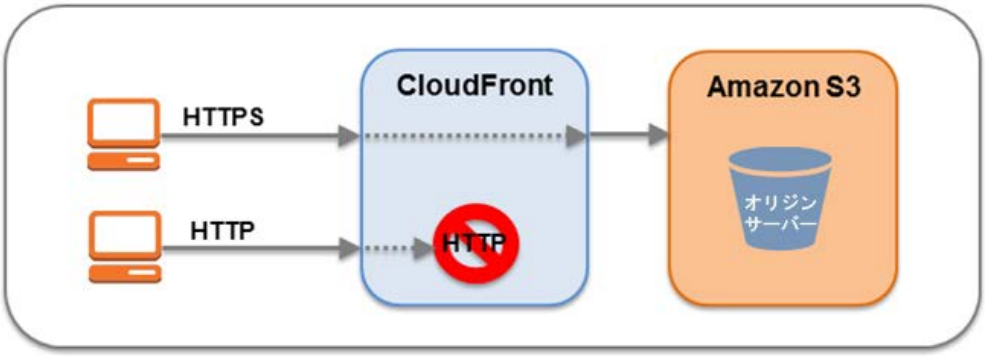


図 7: Amazon CloudFront で暗号化された送信

ビューアがオブジェクトの要求で使用したプロトコルを、CloudFront がオリジンからのオブジェクトのフェッチで使用するように、1 つ以上の CloudFront オリジンを設定できます。たとえば、この CloudFront 設定を使用した場合、ビューアが HTTPS を使用して CloudFront にオブジェクトを要求すると、CloudFront も HTTPS を使用してリクエストをオリジンに転送します。

Amazon CloudFront は、ビューアへの接続とオリジンへの接続の両方で、SSLv3 または TLSv1 プロトコルと、Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) プロトコルを含む一連の暗号スイートを使用します。ECDHE を利用すれば、SSL/TLS クライアントで、どの場所にも保存されない一時セッションキーを使用する Perfect Forward Secrecy を利用できます。そのため、長期間使用するシークレットキー自体が漏洩した場合でも、権限のない第三者によるキャプチャされたデータのデコードを防ぐことができます。

独自のサーバーをオリジンとして使用しており、ビューアと CloudFront 間および CloudFront とオリジン間の両方で HTTPS を使用する場合、たとえば、VeriSign、DigiCert のようなサードパーティ認証局で署名された有効な SSL 証明書を HTTP サーバーにインストールする必要があります。

デフォルトでは、URL に CloudFront ディストリビューションドメイン名を使用して、コンテンツを HTTPS 接続でビューアに配信できます(例: https://dxxxxx.cloudfront.net/image.jpg)。独自のドメイン名と独自の SSL 証明書を使用して HTTPS 接続でコンテンツを配信する場合は、SNI カスタム SSL または専用 IP カスタム SSL を使用できます。Server Name Identification(SNI)カスタム SSL を使用した場合、CloudFront は、ほとんどの最新ウェブブラウザでサポートされている TLS プロトコルの SNI 拡張に依存します。ただし、ユーザーによっては、SNI をサポートしない古いブラウザを使用しているためコンテンツにアクセスできないことがあります(サポートされるブラウザの一覧については、http://aws.amazon.com/cloudfront/faqs/ を参照してください)。専用 IP カスタム SSL を使用した場合、CloudFront が受信リクエストを適切な SSL 証明書に関連付けることができるように、CloudFront は各 CloudFront エッジロケーションで SSL 証明書に専用の IP アドレスを使用します。

Amazon CloudFront のアクセスログには、コンテンツのリクエストに関する包括的な情報セットが含まれています。これにはたとえば、リクエストされたオブジェクト、リクエストの日付と時刻、リクエストを処理するエッジロケーション、クライアント IP アドレス、参照者、ユーザーエージェントなどがあります。アクセスログを有効にするには、Amazon CloudFront のディストリビューションを設定する際に、Amazon S3 バケットの名前を指定して、ログイン情報を保存します。

AWS Direct Connect のセキュリティ

AWS Direct Connect を使用すると、内部ネットワークと AWS リージョン間において、高スループットかつ専用接続で、直接接続を実現できます。これは、ネットワークコストの削減、スループットの向上、安定したネットワーク接続の実現に役立ちます。この専用接続があれば、AWS クラウド(たとえば、Amazon EC2 および Amazon S3)および Amazon VPC への仮想インターフェイスを直接作成することができます。

Direct Connect では、ネットワークパス内のインターネットサービスプロバイダーを迂回します。お客様は、AWS Direct Connect ロケーションがある施設内にラックスペースを調達し、近くに機器を配置することができます。配置後は、クロスコネクトを使用して、この機器を AWS Direct Connect に接続することができます。各 AWS Direct Connect ロケーションでは、地理的に最も近い AWS リージェントへの接続と米国の他のリージョンへのアクセスが有効になります。たとえば、米国内の任意の AWS Direct Connect ロケーションに 1 つ接続し、それを使用して、すべての米国リージョンおよび AWS GovCloud(米国)内の公共の AWS サービスにアクセスできます。

業界標準の 802.1q VLAN を使用して、専用接続を複数の仮想インターフェースに分割することができます。このようにすると、同じ接続を使用して、パブリックリソース(たとえば Amazon S3 に格納されたオブジェクト)にはパブリック IP アドレススペースを使用してアクセスし、プライベートリソース(たとえば Amazon VPC 内で実行されている Amazon EC2 インスタンス)にはプライベート IP スペースを使用してアクセスすることができるので、パブリック環境とプライベート環境の間でネットワークを分離できます。

Amazon Direct Connect では、ボーダーゲートウェイプロトコル(BGP)と自律システム番号(ASN)を使用する必要があります。仮想インターフェイスを作成するには、メッセージの認証に MD5 暗号キーを使用します。MD5 により、シークレットキーを使用してキー付きハッシュが作成されます。AWS が BGP MD5 キーを自動的に生成するようにするか、独自のキーを提供することができます。

ストレージサービス

アマゾン ウェブ サービスは、堅牢性と可用性を備えた低コストのデータストレージを提供しています。AWS は、ブロックストレージおよびオブジェクトストレージであり、バックアップ、アーカイブ、災害対策用にストレージを提供しています。

Amazon Simple Storage Service(Amazon S3)のセキュリティ

Amazon Simple Storage Service (S3) を使用すれば、ウェブ上の任意の場所からいつでも、データをアップロードし、取り出すことができます。Amazon S3 は、オブジェクトとしてデータをバケットに保管します。オブジェクトは、テキストファイル、写真、ビデオなど、どのような種類のファイルでもかまいません。Amazon S3 にファイルを追加する際、ファイルと共にメタデータを含める、およびファイルへのアクセスをコントロールする権限を設定するオプションがあります。それぞれのバケットにおいて、バケットへのアクセスをコントロール (誰がバケットのオブジェクトを作成、削除、リストできるか)、バケットとそのオブジェクトのアクセスログを表示、Amazon S3 がバケットとそのコンテンツを保管する地域を選択することができます。

データアクセス

Amazon S3 に格納されているデータへのアクセスは、デフォルトで制限されます。バケットおよびオブジェクトの所有者のみが、作成した Amazon S3 リソースにアクセスできます (バケット/オブジェクトの所有者は AWS アカウント所有者であり、バケット/オブジェクトを作成したユーザーではないことに注意してください)。バケットとオブジェクトへのアクセスを管理するには、いくつか方法があります。

- **IAM (Identity and Access Management) ポリシー。**AWS IAM により、多数の従業員がいる組織が単一の AWS アカウントの下で複数のユーザーを作成および管理することができます。IAM ポリシーはユーザーにアタッチされるため、AWS アカウント内のユーザーがバケットまたはオブジェクトにアクセスするためのアクセス権限を一元管理できます。IAM ポリシーでは、AWS アカウント内のユーザーにのみ、Amazon S3 リソースへのアクセスを許可できます。
- **アクセスコントロールリスト(ACL)。**Amazon S3 では、バケットまたはオブジェクトへの読み込みアクセスまたは書き込みアクセスをユーザーグループに許可するために ACL を使用できます。ACL では、(特定のユーザーではなく) 他の AWS アカウントにのみ、Amazon S3 リソースへのアクセスを許可できます。
- **バケットポリシー。**Amazon S3 のバケットポリシーは、単一のバケット内のオブジェクトの一部またはすべてにわたってアクセス許可を追加および拒否するのに使用することができます。ポリシーは、ユーザー、グループ、または Amazon S3 バケットにアタッチでき、権限の中央集中管理が可能になります。バケットポリシーを使用すると、AWS アカウントのユーザーに、または他の AWS アカウントに S3 リソースへのアクセスを許可できます。

アクセスコントロールのタイプ	AWS アカウントレベルの制御	ユーザーレベルの制御
IAM ポリシー	いいえ	はい
ACL	はい	いいえ
バケットポリシー	はい	はい

また、特定の条件に基づいて、特定のリソースへのアクセスをさらに制限できます。たとえば、リクエストが SSL (ブール条件)、リクエスタの IP アドレス (IP アドレス条件)、リクエスタのクライアントアプリケーション (文字列条件) のいずれを使用して送信されたかによって、リクエストの時間 (日付条件) に基づいてアクセスを制限できます。これらの条件を特定するには、ポリシーキーを使用します。Amazon S3 で利用可能なオペレーション固有のポリシーキーに関する詳細については、「Amazon Simple Storage Service 開発者ガイド」をご覧ください。

Amazon S3 では開発者は、事前定義された 期間有効な URL を通して Amazon S3 オブジェクトを共有できるクエリ文字列認証を使用できます。クエリ文字列認証は、通常は認証を必要とするリソースに対する HTTP またはブラウザアクセスを提供するのに役立ちます。クエリ文字列の署名は、リクエストをセキュリティ保護します。

データ転送

セキュリティを最大限に高めるために、SSL で暗号化されたエンドポイント経由で Amazon S3 に安全にデータをアップロード/ダウンロードできます。暗号化されたエンドポイントは、インターネットと Amazon EC2 内の両方からアクセス可能です。これにより、AWS 内と、AWS の外部ソースとのやり取りの両方で、データが安全に転送されます。

データストレージ

Amazon S3 ではまた、保管時のデータの暗号化用に複数のオプションを用意しています。お客様が独自の暗号化キーを管理したい場合は、Amazon S3 の暗号化クライアントのようなクライアント暗号化ライブラリを使用して、Amazon S3 にアップロードする前にデータを暗号化することができます。また、Amazon S3 で暗号化プロセスの管理を行いたい場合は、Amazon S3 のサーバーサイド暗号化(SSE)を使用できます。データは、要件に応じて、AWS により生成されたキーまたは指定したキーを使用して暗号化されます。Amazon S3 の SSE により、オブジェクトを書き込む際に追加のリクエストヘッダーを単純に追加するだけで、アップロード時にデータを暗号化することができます。データが取得された時に、自動的に復号化が行われます。

オブジェクトに含めることができるメタデータは暗号化されないことに注意してください。これらによって、AWS では、Amazon S3 メタデータに機密情報を含めないことをお勧めします。

Amazon S3 SSE では、ブロック暗号の中で最も強力である 256 ビット Advanced Encryption Standard(AES-256)が使用されます。Amazon S3 SSE で、すべての保護されたオブジェクトは一意のキーで暗号化されます。このオブジェクトキー自体が定期的に更新されるマスターキーによって暗号化されます。Amazon S3 SSE では、暗号化されたデータと暗号キーを異なるホストに保存することにより、セキュリティを高めます。また Amazon S3 SSE により、暗号化要件を強制できます。たとえば、暗号化されたデータのみをバケットにアップロードできるよう要求するバケットポリシーを作成し、適用できます。

長期保管用として、Glacier という AWS のアーカイブサービスに Amazon S3 バケットのコンテンツを自動的にアーカイブできます。どのオブジェクトをいつ Glacier にアーカイブするかを記述するライフサイクルルールを Amazon S3 内に作成することによって、指定された間隔で Glacier にデータを転送できます。データ管理戦略の一部として、オブジェクトを Amazon S3 に格納した後、オブジェクトを削除するまで Amazon S3 が待機する時間を指定できます。

オブジェクトが Amazon S3 から削除されると、オブジェクトに対するパブリック名からのマッピングの削除が直ちに開始されます。この処理は、一般的に、数秒以内に分散システムで実行されます。マッピングが削除されると、削除されたオブジェクトに対するリモートアクセスは存在しなくなります。基本的なストレージ領域は、その後システムが使用するために再生されます。

データの堅牢性と信頼性

Amazon S3 は、任意の 1 年間について 99.999999999% のオブジェクト堅牢性を提供するよう設計されています。オブジェクトは、Amazon S3 のリージョン内の複数の施設の複数のデバイスで冗長的に格納されます。堅牢性を高めるため、Amazon S3 PUT および COPY 操作は、複数の施設で同期をとりながらデータを保存し、その後 SUCCESS を返します。いったん保存されると、Amazon S3 は、冗長性の喪失をすばやく検出して修復することによって、オブジェクトの堅牢性を維持します。Amazon S3 は、チェックサムを用いて、格納されているデータの完全性を定期的に検証しています。破損が検出されると、冗長データを使用して修復されます。さらに Amazon S3 は、ネットワークの全トラフィックに対してチェックサムを計算し、データの格納または取得時のデータパケットの損傷を検出しています。

Amazon S3 はバージョニングを通じて、さらなる保護能力提供しています。バージョニングを使用して、Amazon S3 バケットに格納されたあらゆるオブジェクトのあらゆるバージョンを、格納、取得、復元することができます。バージョニングを使用すれば、意図せぬユーザーアクションとアプリケーション障害の両方から、簡単に回復することができます。デフォルトでは、リクエストは最も新しく書き込まれたバージョンを取得するようになっています。リクエストでバージョンを指定することによって、オブジェクトの旧バージョンを取得することができます。Amazon S3 バージョニングの MFA 削除機能を使用して、バージョンをさらに保護できます。これを Amazon S3 バケットに対して有効にした場合、バージョン削除リクエストに多要素認証デバイスの 6 桁のコードとシリアルナンバーが含まれている必要があります。

アクセスログ

Amazon S3 バケットを設定して、バケットとそのバケットに含まれるオブジェクトに対するアクセスを記録できます。アクセスログには、リクエストタイプ、リクエストされたリソース、リクエストした者の IP、リクエストの日時など、各アクセスリクエストの詳細が含まれています。ロギングがバケットに対して有効になると、ログ記録は定期的にログファイルに収集され、指定された Amazon S3 バケットに配信されます。

Cross-Origin Resource Sharing (CORS)

静的なウェブページをホストしたり、他のウェブページで使用されるオブジェクトを保存したりするために Amazon S3 を使用する AWS のお客様は、明示的にクロスオリジンのリクエストを有効にするように Amazon S3 バケットを設定することで、コンテンツを安全にロードすることができます。最新のブラウザでは同一オリジンポリシーを使用して、(クロスサイトスクリプト攻撃時など)悪意のあるコンテンツを低い信頼性のソースからロードされないようにする方法として、別のサイトまたはドメインからコンテンツをロードするためのリクエストの許可を JavaScript または HTML5 でできないようにします。Cross-Origin Resource Sharing (CORS) ポリシーが有効である場合、Amazon S3 バケットに保存されたウェブのフォントやイメージなどの資産は、外部ウェブページ、スタイルシート、HTML5 アプリケーションから安全に参照できます。

AWS Glacier セキュリティ

Amazon S3 と同様に、Amazon Glacier サービスは低コストで安全かつ堅牢なストレージを提供します。ただし、Amazon S3 が迅速な検索用に設計されている Glacier では、それほど頻繁にアクセスされず、数時間の取得時間が適切であるデータのアーカイブサービスとしての使用が想定されています。

Amazon Glacier は、ボールト内にアーカイブとしてファイルを保存します。アーカイブは写真、動画、ドキュメントなどのデータであり、1 個または複数のファイルを含めることができます。単一のボールトに無制限の数のアーカイブを格納し、またリージョンごとに最大 1,000 個のボールトを作成できます。各オブジェクトに最大 40 TB のデータを格納できます。

データのアップロード

Amazon Glacier のボールトにデータを転送するために、1 回のアップロード操作またはマルチパート操作でアーカイブをアップロードできます。1 回のアップロード操作では、最大 4 GB のアーカイブをアップロードできます。ただし、100 MB より大きいアーカイブをアップロードする場合には、マルチパートアップロード API を使用することでより適切な結果が得られます。マルチパートアップロード API を使用することで、最大約 40,000 GB の大きなアーカイブをアップロードすることができます。マルチパートアップロード API の呼び出しでは、大きなアーカイブのアップロードを効率よく実行できるように設計されています。これによって、パートアップロードを個別に、または任意の順序で、あるいは並行して行うことができます。マルチパートアップロードが失敗した場合、アーカイブ全体ではなく、失敗したパートのみを再度アップロードするだけで済みます。

Glacier にデータをアップロードする場合は、木構造ハッシュを計算および指定する必要があります。Glacier は、データに対してハッシュをチェックし、途中で変化していないことを確認します。木構造ハッシュは、メガバイトサイズごとのデータセグメントについてハッシュを計算することによって生成されるもので、常に拡大するデータの隣接セグメントを表すために木形式のハッシュを結合します。

Amazon Glacier に対して大きなアップロードを行うお客様は、マルチパートアップロード機能の使用に代わる方法として、データを転送するのではなく、AWS Import/Export サービスの使用を検討できます。AWS Import/Export では、転送用のポータブル記憶装置を用いて AWS に対する大容量データの転送を支援します。AWS は、Amazon の高速内部ネットワークを駆使し、インターネットを使うことなく、データを直接ストレージデバイスから転送します。

また、特定の間隔で Glacier にデータを転送するように Amazon S3 をセットアップできます。どのオブジェクトをいつ Glacier にアーカイブするかを記述するライフサイクルルールを Amazon S3 に作成できます。また、オブジェクトを Amazon S3 に格納した後、オブジェクトを削除するまで Amazon S3 が待機する時間を指定できます。

セキュリティをさらに高めるために、SSL で暗号化されたエンドポイント経由で Amazon Glacier に安全にデータをアップロード/ダウンロードできます。暗号化されたエンドポイントは、インターネットと Amazon EC2 内の両方からアクセス可能です。これにより、AWS 内と、AWS の外部ソースとのやり取りの両方で、データが安全に転送されます。

データの取得

Amazon Glacier からアーカイブを取得するには、一般的に完了までに 3～5 時間かかる取得ジョブを開始する必要があります。その後、HTTP GET リクエストにより、データにアクセスできます。このデータは、24 時間、使用できます。

アーカイブ全体またはアーカイブから任意のファイルを取得できます。アーカイブのサブセットのみ取得する場合、1 つの取得リクエストを使用して、対象のファイルを含むアーカイブの範囲を指定するか、それぞれ 1 つ以上のファイルの範囲を含む複数の取得リクエストを開始できます。アーカイブの作成日範囲でフィルタリングするか、最大項目数制限を設定することによって、取得されるボールトインベントリの項目数を制限することもできます。アーカイブの一部を取り出す場合、どの方法を選択したとしても、取得する範囲がアーカイブ全体のツリーハッシュと整合性がとれていれば、提供されるチェックサムを利用してファイルの整合性を確認することができます。

データストレージ

Amazon Glacier は AES-256 を使用して自動的にデータを暗号化し、変更不可能な形式で永続的に格納します。Amazon Glacier は、アーカイブの平均年間耐久性が 99.999999999% となるように設計されています。複数の施設および複数のデバイスに各アーカイブを格納します。従来型のシステムでは、データの検証と修復にかなりの人的作業が必要になることもありますが、対照的に Glacier では、体系的なデータ完全性チェックが定期的に実施されるほか、自己修復を自動的に行うように設計されています。

データアクセス

自身のアカウントでのみ Amazon Glacier の自身のデータにアクセスできます。Amazon Glacier のデータへのアクセスを管理するために、AWS IAM を使用して、アカウント内のどのユーザーに該当ボールトでの操作の権利を与えるかを指定できます。

AWS Storage Gateway のセキュリティ

AWS Storage Gateway サービスは、オンプレミスのソフトウェアアプライアンスをクラウドベースのストレージと接続することで、IT 環境と AWS のストレージインフラストラクチャ間でシームレスかつセキュアな統合を実現します。このサービスを利用すれば、コスト効率の高いバックアップと迅速な災害復旧のために、スケーラブルで信頼性が高くセキュアな Amazon S3 ストレージサービスにデータを安全にアップロードできます。

AWS Storage Gateway は、データを Amazon EBS スナップショット形式でオフサイトの Amazon S3 に透過的にバックアップします。Amazon S3 は複数の施設全体にある複数デバイス上のスナップショットを冗長に保存し、冗長性が失われれば検出し、修正します。Amazon EBS スナップショットは、オンプレミスで復元可能な、または新しい Amazon EBS ボリュームでインスタンス化するために使用するポイントインタイムバックアップを提供します。データは、指定する単一のリージョン内に保存されます。

AWS Storage Gateway は次の 3 つの方式を提供しています。

- **ゲートウェイ保管型ボリューム(クラウドがバックアップ)**。この方式では、ボリュームデータはローカルに保存された後、冗長化、かつ、暗号化された形式で Amazon S3 にコピーされ、Elastic Block Storage (EBS) スナップショットの形式で使用可能になります。このモデルを使用する場合、オンプレミスのストレージがプライマリであり、データセット全体に対する低レイテンシー アクセスを提供します。また、クラウド ストレージはバックアップになります。
- **ゲートウェイキャッシュ型ボリューム(クラウドがプライマリ)**。このオプションでは、ボリュームデータは Amazon S3 で暗号化および保存され、iSCSI インターフェイスによってエンタープライズネットワーク内に表示されるようになります。最近アクセスされたデータは、オンプレミスでキャッシュされるので、低レイテンシーのローカルアクセスが可能です。このモデルを使用する場合、クラウドストレージがプライマリですが、オンプレミスのキャッシュされたボリューム内のアクティブワーキングセットに対する低レイテンシー アクセスが得られます。
- **ゲートウェイ仮想テープライブラリ(VTL)。**この方式では、ゲートウェイあたり最大 10 個の仮想テープドライブ、メディアチェンジャー 1 個、最大 1500 個の仮想テープカートリッジを使用してゲートウェイ VTL を設定できます。各仮想テープドライブは SCSI コマンドセットに応答するため、既存のオンプレミスバックアップアプリケーション(ディスクからテープ、またはディスクからディスクを経由してテープ)を修正する必要はありません。

どのオプションを選択しても、データはオンプレミスのストレージハードウェアから SSL 経由で AWS に非同期に転送されます。データは、Advanced Encryption Standard(AES)256(256 ビットの暗号化キーを使用した対称鍵暗号標準)を使用して、Amazon S3 で暗号化され、保存されます。AWS Storage Gateway は、インターネットで送信されるデータ量を最小に抑えるために、変更されたデータのみをアップロードします。

AWS Storage Gateway は、VMware ESXi Hypervisor v 4.1 または v 5、あるいは Microsoft Hyper-V を実行しているデータセンターのホストにデプロイする仮想マシン (VM) として実行します (設定プロセス中に、VMware ソフトウェアをダウンロードします)。ゲートウェイ AMI を使用して EC2 内で実行することもできます。インストールおよび設定プロセスで、ゲートウェイあたり最大 12 個の保管型ボリューム、20 個のキャッシュ型ボリューム、または 1,500 個の仮想テープカートリッジを作成できます。インストールされると、各ゲートウェイはアップデートやパッチを自動的にダウンロード、インストール、デプロイします。このアクティビティは、ゲートウェイごとに設定できるメンテナンスウィンドウ期間中に行われます。

iSCSI プロトコルは、CHAP(チャレンジハンドシェイクオーセンティケーションプロトコル)経由でゲートウェイとイニシエータの間の認証をサポートします。CHAP は、ストレージボリュームターゲットへのアクセスの認証時に、iSCSI イニシエータのアイデンティティを定期的に確認することにより、中間者攻撃やプレイバック攻撃から保護します。CHAP を設定するには、AWS Storage Gateway コンソールと、ターゲットへの接続に使用される iSCSI イニシエータソフトウェアの両方で設定する必要があります。

AWS Storage Gateway VM のデプロイ後、AWS Storage Gateway コンソールを使用してゲートウェイをアクティベートする必要があります。アクティブ化を行うと、ゲートウェイが AWS アカウントに関連付けられます。この接続の確立後は、ゲートウェイのほぼすべての属性をコンソールから管理することができます。アクティベーションプロセスでは、ゲートウェイの IP アドレスを指定し、ゲートウェイに名前を付け、スナップショットのバックアップを保存する AWS リージョンを識別して、ゲートウェイのタイムゾーンを指定します。

AWS Import/Export

AWS Import/Export は、Amazon S3、EBS、または Glacier ストレージに大量のデータを物理的に転送するためのシンプルで安全な方法です。このサービスは一般的に、100 GB を超えるデータを持つか、インターネット経由で非常に低速の転送レートになる接続速度のお客様によって使用されます。AWS Import/Export では、安全な AWS 施設に送付するためのポータブル ストレージ デバイスを用意します。AWS は、Amazon の高速内部ネットワークを駆使し、したがってインターネットを使うことなく、データを直接ストレージデバイスから転送します。また逆に、AWS からポータブル ストレージデバイスにデータをエクスポートできます。

他のすべての AWS サービスと同様に、AWS Import/Export サービスではストレージ デバイスを安全に確認および認証する必要があります。この場合、Amazon S3 バケット、Amazon EBS リージョン、AWS アクセスキー ID、および返送先住所を含むジョブリクエストを AWS に送信します。それに対して、固有のジョブ識別子、デバイスを認証するためのデジタル署名、およびストレージデバイスを発送するための AWS 住所が返信されます。Amazon S3 の場合は、デバイスのルートディレクトリに署名ファイルを格納します。Amazon EBS の場合は、署名バーコードをデバイスの外側にテープで貼ります。署名ファイルは認証でのみ使用され、Amazon S3 または EBS にはアップロードされません。

Amazon S3 への転送では、データのロード先となる特定のバケットを指定し、ロードを実行するアカウントが該当バケットに対して書き込みアクセス許可を持つことを確認します。また、Amazon S3 にロードされる各オブジェクトに適用するアクセス制御リストを指定する必要があります。

EBS への転送では、EBS のインポート操作のために、ターゲット リージョンを指定します。ストレージデバイスが最大 1 TB のボリュームサイズ以下であれば、そのコンテンツは Amazon EBS のスナップショットに直接読み込まれます。ストレージデバイスの容量が 1 TB を超える場合は、デバイスのイメージは指定された S3 のログバケット内に格納されます。その後、論理ボリュームマネージャなどのソフトウェアを使用して EBS ボリュームの RAID を作成し、Amazon S3 からこの新しいボリュームにイメージをコピーすることができます。

保護を強化するため、AWS に送付する前にデバイス上のデータを暗号化できます。Amazon S3 データの場合、AWS に送付する前に、PIN コードデバイスを利用したハードウェア暗号化または TrueCrypt ソフトウェアを使用してデータを暗号化できます。EBS や Glacier のデータの場合、PIN コードデバイスを含む、どの暗号化方法でも使用できます。AWS は、インポート前に、PIN コードや、インポートマニフェストで指定した TrueCrypt パスワードを使用して、Amazon S3 データを復号化します。AWS は、お客様の PIN を使用して PIN コードデバイスにアクセスしますが、Amazon EBS または Amazon Glacier にインポートするためにソフトウェアで暗号化されたデータを復号化しません。次の表は、インポート/エクスポートジョブの各タイプの暗号化オプションをまとめたものです。

Amazon S3 へのインポート		
ソース	ターゲット	結果
• デバイスのファイルシステム上のファイル • PIN コードデバイスや TrueCrypt を使用してデータを復号化	• 既存の Amazon S3 バケット内のオブジェクト • AWS がインポートの実行前にデータを復号化	• ファイルごとに 1 つのオブジェクト • AWS はすべてのジョブが完了した後、返送前にデバイスを消去

Amazon S3 からのエクスポート		
ソース	ターゲット	結果
• 1 つ以上の Amazon S3 バケット内のオブジェクト • AWS がデータの暗号化に使用する PIN コードやパスワードを指定	• ストレージデバイス上のファイル • AWS がデバイスをフォーマット • AWS がデバイス上の暗号化ファイルコンテナにデータをコピー	• オブジェクトごとに 1 つのファイル • 返送前に AWS がデータを暗号化 • PIN コードデバイスや TrueCrypt を使用してデータを復号化
Amazon Glacier へのインポート		
ソース	ターゲット	結果
• デバイス全体 • 送付する前に選択した暗号化方法を使用してデータを暗号化	• 既存の Amazon Glacier ボールト内にアーカイブ 1 つ • AWS はデバイスを復号化しない	• 単一のアーカイブとして保存されたデバイスイメージ • 送付前にインポートジョブが実行されるたびに AWS がデバイスを消去する
Amazon EBS にインポート（デバイス容量が 1 TB 未満）		
ソース	ターゲット	結果
• デバイス全体 • 送付する前に選択した暗号化方法を使用してデータを暗号化する	• 1 つの Amazon EB スナップショット • AWS はデバイスを復号化しない	• デバイスイメージは単一のスナップショットとして保存される • デバイスが暗号化されていた場合、イメージも暗号化される • 送付前にインポートジョブが実行されるたびに AWS がデバイスを消去する
Amazon EBS にインポート（デバイス容量 1 TB 超）		
ソース	ターゲット	結果
• デバイス全体 • 送付する前に選択した暗号化方法を使用してデータを暗号化する	• 既存の Amazon S3 バケット内の複数のオブジェクト • AWS はデバイスを復号化しない	• デバイスイメージは一連の 1 TB 毎のスナップショットのチャンクに分割されマニフェストファイルに指定された Amazon S3 バケット上のオブジェクトとして保存される • デバイスが暗号化された場合、イメージが暗号化される • 送付前にインポートジョブが実行されるたびに AWS がデバイスを消去する

インポートが完了すると、AWS Import/Export はストレージデバイスのコンテンツを消去し、返送中のデータを保護します。AWS は、ストレージ デバイスのすべての書き込み可能なブロックをゼロで上書きします。このため、デバイスの再パーティション化とフォーマットを行う必要があります。AWS がデバイス上のデータを消去できない場合、破棄がスケジュールされ、AWS のサポートチームがデバイスとともに送付されたマニフェストファイルで指定された E メールアドレスに連絡します。

デバイスを国外に送付する場合、AWS に送信するマニフェストファイルにはカスタムオプション、および特定の必須サブフィールドが必要です。AWS Import/Export は、届いた送付品を検証し、送付に関するカスタム書類を準備するためにこれらの値を使用します。これらのオプションのうちの 2 つは、デバイス上のデータが暗号化されているかどうかと、暗号化アプリケーションの分類です。暗号化されたデータの送付先または送付元が米国である場合、暗号化アプリケーションは米国輸出規制の 5D992 に分類されることが必要です。

データベースサービス

アマゾン ウェブ サービスは、マネージド型のリレーショナルおよび NoSQL データベースサービスから、サービスとしてのインメモリキャッシュ、ペタバイト規模のデータウェアハウスサービスまで、開発者および企業向けの多くのデータベースソリューションを提供しています。

Amazon DynamoDB のセキュリティ

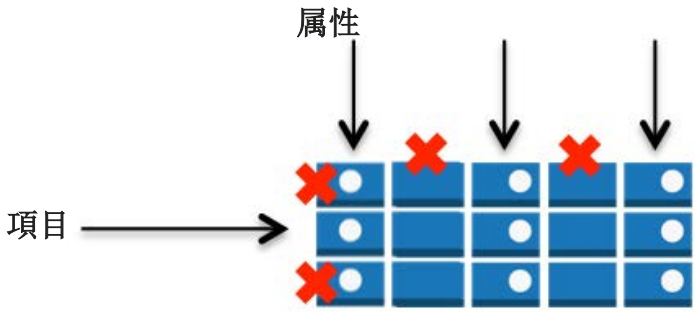
Amazon DynamoDB は、マネージド型の NoSQL データベースサービスで、高速で予測可能なパフォーマンスとシームレスなスケーラビリティを備えています。Amazon DynamoDB を使用すると、分散データベースの運用と AWS に拡張するための管理負荷を軽減できます。お客様はハードウェアのプロビジョニング、設定、構成、レプリケーション、ソフトウェア修正プログラムの適用、クラスター拡張などについて心配する必要がありません。

任意の量のデータを格納および取得できるデータベーステーブルを作成し、任意のレベルのリクエストトラフィックを処理できます。DynamoDB によって自動的に、そのテーブルのデータとトラフィックが多数のサーバーに分散されます。サーバーの数は、指定されたリクエスト容量と保存されているデータを処理するのに十分であるように選択されます。このような分散処理の間も、パフォーマンスは一定で、高速です。また、すべてのデータ項目を SSD (Solid State Drive) に格納し、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レプリケートするので、高い可用性とデータ堅牢性を実現します。

DynamoDB テーブルをコピーするためだけに作成された AWS Data Pipeline 内の特別なテンプレートを使用して、自動バックアップを設定できます。同じリージョンまたは異なるリージョン内のテーブルに対する完全バックアップまたは増分バックアップを選択できます。コード内のエラーにより元のテーブルが破損した場合、またはリージョン間で DynamoDB データを連携してマルチリージョンアプリケーションをサポートするために、災害対策（DR）用途としてこのコピーを使用できます。

DynamoDB リソースと API を使用可能なユーザーを制御するため、AWS IAM でアクセス権限を設定します。IAM では、リソースレベルでのアクセスを制御することに加えて、データベースレベルでのアクセスも制御できます。アプリケーションの必要に基づいて、項目（行）および属性（列）へのアクセスを許可または拒否するデータベースレベルのアクセス権限を作成できます。これらのデータベースレベルのアクセス権限は、きめ細やかなアクセス制御と呼ばれ、

ユーザーまたはアプリケーションが DynamoDB テーブルにアクセス可能な状況を指定する IAM ポリシーを使用して作成できます。IAM ポリシーによって、テーブルの個別の項目へのアクセス、その項目の属性へのアクセス、またはその両方へのアクセスを同時に制御できます。



必要に応じて、Login with Amazon、Facebook、または Google によって認証されたアプリケーションユーザーによるアクセスを制御するため、ウェブアイデンティティフェデレーションを使用できます。ウェブアイデンティティフェデレーションを使用すると、個々の IAM ユーザーを作成する必要がなくなります。その代わりに、ユーザーはアイデンティティプロバイダーにサインインして、AWS Security Token Service (AWS STS) から一時的なセキュリティ認証情報を取得できます。AWS STS は、一時的な AWS 認証情報をアプリケーションに返し、特定の DynamoDB テーブルへのアクセスを許可します。

データベースとユーザーのアクセス権限が必要なだけでなく、DynamoDB サービスに対する各リクエストには、有効な HMAC-SHA256 署名を含める必要があります。これを含めない場合、リクエストは拒否されます。AWS SDK はリクエストに自動的に署名を行います。独自に HTTP POST リクエストを作成したい場合は、Amazon DynamoDB に対するリクエストのヘッダーに署名を含める必要があります。署名を計算するには、AWS Security Token Service から一時的なセキュリティ認証情報をリクエストする必要があります。次に、一時的なセキュリティ認証情報を使用して、Amazon DynamoDB に対するリクエストに署名します。

Amazon DynamoDB は SSL で暗号化されたエンドポイント経由で使用できます。暗号化されたエンドポイントには、インターネットと Amazon EC2 内の両方からアクセスできます。

Amazon Relational Database Service（Amazon RDS）のセキュリティ

Amazon RDS を使用すれば、リレーショナルデータベースのインスタンスを素早く作成し、関連するコンピュータリソースやストレージ能力を柔軟に拡張して、アプリケーションの需要に適合させることができます。Amazon RDS は、バックアップおよびフェールオーバー処理を実行し、データベースソフトウェアを維持管理することにより、ユーザーに代わってデータベースインスタンスを管理します。現在、Amazon RDS では、MySQL、Oracle、Microsoft SQL Server、PostgreSQL データベースエンジンを使用できます。

Amazon RDS には、DB セキュリティグループ、アクセス許可、SSL 接続、自動バックアップ、DB スナップショット、マルチ AZ 配置など、重要な生産データベースの信頼性を強化する機能があります。DB インスタンスは、ネットワークの分離性を高めるために Amazon VPC でデプロイすることができます。

アクセスコントロール

最初に Amazon RDS 内に DB インスタンスを作成した場合は、DB インスタンスへのアクセスをコントロールするために、Amazon RDS のコンテキスト内でのみ使用されるマスターユーザーアカウントを作成します。マスターユーザーアカウントは、すべてのデータベース特権を持ち、DB インスタンスにログオンできるネイティブなデータベース ユーザー アカウントです。DB インスタンスの作成時に、各 DB インスタンスと関連付けたいマスターユーザー名とパスワードを指定することができます。一旦 DB インスタンスを作成すると、マスターユーザー証明書を使用してデータベースへ接続することができます。後で、追加のユーザー アカウントを作成できるので、DB インスタンスへアクセスできる人を制限することができます。

Amazon EC2 のセキュリティグループに類似していますが、交換可能ではない DB セキュリティグループによって Amazon RDS DB インスタンスアクセスをコントロールできます。DB セキュリティグループは、DB インスタンスに対するネットワークアクセスをコントロールするファイアウォールのように動作します。データベースセキュリティグループはデフォルトでは「deny all」アクセスモードになっており、ネットワークへの着信はお客様が明示的に許可する必要があります。そのためには、次の 2 つの方法があります。ネットワーク IP 範囲を許可する方法と、既存の Amazon EC2 セキュリティグループを許可する方法です。DB セキュリティ グループは、データベース サーバー ポートへのアクセスのみを許可します（他はすべてブロックされます）。また Amazon RDS DB インスタンスを再起動せずに更新できるので、お客様は自身のデータベースへのアクセスを、シームレスに制御できます。AWS IAM を使用して、さらに RDS DB インスタンスへのアクセスを制御できます。たとえば、AWS IAM により、どの RDS 操作に対して、各 AWS IAM ユーザーが呼び出し権限を持つようにするかを制御できます。

ネットワークの隔離

ネットワークアクセス制御を高めるために、Amazon VPC で DB インスタンスを実行できます。使用する IP アドレス範囲をお客様が指定して、DB インスタンスを隔離することができます。既存の IT インフラストラクチャとの接続には業界標準の IPSec VPN が使えます。VPC で Amazon RDS を実行すると、プライベートサブネット内に DB インスタンスを置くことができます。また、社内ネットワークを VPC に拡張する仮想プライベートゲートウェイを設定して、その VPC 内で RDS DB インスタンスへのアクセスを許可する方法もあります。詳細については、Amazon VPC ユーザーガイドを参照してください。

Multi-AZ 配置の場合、リージョン内のすべてのアベイラビリティーゾーン用にサブネットを定義すると、必要に応じて Amazon RDS で別のアベイラビリティーゾーンに新しいスタンバイを作成できるようになります。VPC 内の RDS DB インスタンス用に指定するサブネットのコレクションである DB サブネットグループを作成できます。各 DB サブネットグループには、特定のリージョン内のアベイラビリティーゾーンごとに 1 つ以上のサブネットを指定する必要があります。この場合、VPC 内に DB インスタンスを作成するときに、DB サブネットグループを選択します。これによって Amazon RDS では、サブネットとそのサブネット内の IP アドレスを選択するために、DB サブネットグループと優先アベイラビリティーゾーンを使用します。Amazon RDS によって Elastic Network Interface が作成され、その IP アドレスを持つ DB インスタンスに関連付けられます。

Amazon VPC 内に展開した DB インスタンスには、インターネットからアクセスできるだけでなく、VPN またはパブリックサブネットで起動できる拠点ホストを介して VPC 以外にある Amazon EC2 インスタンスからもアクセスできます。踏み台ホストを使用するには、SSH の踏み台として動作する EC2 インスタンスを使用してパブリックサブネットを設定する必要があります。このパブリックサブネットには、SSH ホストを介してトラフィックを制御できるインターネットゲートウェイまたはルーティングルールが必要です。また、その SSH ホストから Amazon RDS DB インスタンスのプライベート IP アドレスに要求を転送できる必要があります。

DB セキュリティグループを使用すると、Amazon VPC 内の DB インスタンスを保護できます。また、各サブネットに出入りするネットワークトラフィックは、ネットワーク ACL を介して許可または拒否することができます。IPsec VPN 接続を介する Amazon VPC へのすべてのネットワークトラフィックの出入りは、ネットワークファイアウォール、侵入検知システムなど、オンプレミス側のセキュリティインフラストラクチャによって監視することができます。

暗号化

SSL を使用して、アプリケーションと DB インスタンス間の接続を暗号化できます。MySQL および SQL Server では、RDS は SSL 証明書を作成し、インスタンスがプロビジョニングされるとき、DB インスタンスにその証明書をインストールします。MySQL の場合は、接続の暗号化のためにパブリックキーを参照する ssl_ca パラメータを使用して、mysql クライアントを起動します。SQL Server では、パブリックキーをダウンロードして、Windows オペレーティングシステムに証明書をインポートします。Oracle RDS は、DB インスタンスに Oracle ネイティブネットワークの暗号化を使用します。オプショングループにネイティブネットワークの暗号化オプションをそのまま追加し、そのオプショングループを DB インスタンスに関連付けます。暗号化された接続が確立されたら、DB インスタンスとお客様のアプリケーション間で転送されるデータは、転送中に暗号化されるようになります。また、DB インスタンスに対して、暗号化された接続のみを受け付けるよう要求できます。

Amazon RDS は、SQL Server(SQL Server Enterprise Edition)および Oracle(Oracle Enterprise Edition)で使用できる Oracle Advanced Security Option の一部)の Transparent Data Encryption(TDE)をサポートします。TDE 機能は、ストレージへの書き込み前に自動的にデータを暗号化し、ストレージからの読み取り時に自動的にデータを復号化します。MySQL で、データベースへの保存時にデータを暗号化する必要がある場合、アプリケーションでデータの暗号化と復号化を管理しなければなりません。

また、Amazon RDS 内での SSL サポートは、アプリケーションと DB インスタンス間での接続暗号化のためにあることにご注意ください。これは DB インスタンスそのものの認証には使用しないでください。

SSL がセキュリティ上の利点を提供する一方で、SSL 暗号化がかなりの計算処理を必要とするオペレーションであり、お客様のデータベース接続の待ち時間を増加させることにご注意ください。SSL と MySQL の連携方法の詳細については、ここにある MySQL の文書を直接ご参照ください。SQL Server に対する SSL の動作の詳細については、「RDS ユーザーガイド」を参照してください。

自動バックアップと DB スナップショット

Amazon RDS は、DB インスタンスのバックアップと復旧を行うための 2 つの方法、つまり自動化バックアップとデータベース スナップショット(DB Snapshots)を提供しています。

既定でオンになっている Amazon RDS の自動バックアップ機能により、DB インスタンスのポイントインタイムリカバリが可能です。Amazon RDS は、お客様のデータベースとトランザクションログをバックアップし、これらをユーザーが指定した保持期間格納します。これによって、最大 5 分前まで、保持期間内の任意の時点に DB インスタンスを復元させることができます。自動バックアップの保持期間は、最大 35 日間まで設定できます。

バックアップ ウィンドウ期間で、データのバックアップ中にはストレージ I/O は一時停止する場合があります。この I/O 中断は通常で数分間継続します。この I/O 中断はマルチ AZ DB 配置では避けることができます。なぜならバックアップがスタンバイから取得されるからです。

DB スナップショットは、DB インスタンスのユーザー始動型バックアップです。これらの完全なバックアップは、お客様が明示的にそれらを削除するまで、Amazon RDS によって保存されます。任意のサイズの DB スナップショットをコピーして AWS のパブリックリージョン間で移動したり、同じスナップショットを複数のリージョンに同時にコピーしたりすることができます。いつでも必要なときに DB スナップショットから新しい DB インスタンスを作成することができます。

DB インスタンスのレプリケーション

Amazon クラウドコンピューティングリソースは、世界のさまざまなリージョンの可用性の高いデータセンター施設に収容されており、各リージョンにはアベイラビリティーゾーンと呼ばれる複数のそれぞれ独立した場所が含まれています。各アベイラビリティーゾーンは、他のアベイラビリティーゾーンにおける障害の影響は受けず、同じリージョン内の他のアベイラビリティーゾーンに対して、低コスト、低レイテンシーでネットワーク接続できるように設計されています。

Oracle、PostgreSQL、または MySQL データベースの高可用性を設計する場合、マルチ AZ 配置と呼ばれるオプションにより、RDS DB インスタンスを複数のアベイラビリティーゾーンで実行できます。このオプションを選択すると、Amazon は自動的に異なるアベイラビリティーゾーンに DB インスタンスの同期スタンバイレプリカをプロビジョニングし、維持します。プライマリ DB インスタンスは、アベイラビリティーゾーンを跨いでスタンバイレプリカに対して同期的にレプリケートされます。DB インスタンスまたはアベイラビリティーゾーンの障害時、Amazon RDS は自動的にスタンバイに対してフェイルオーバーを行います。これによりデータベースの稼働を手動の管理介入なく速やかに再開できます。

MySQL を使用しており、読み込み負荷の高いデータベースワークロードに対応するため単一 DB インスタンスの能力を超えて拡張する必要があるお客様のために、Amazon RDS にはリードレプリカオプションが用意されています。リードレプリカを作成すると、MySQL の非同期レプリケーション機能を使って、ソース DB インスタンスのデータベース更新がリードレプリカに複製されます。1 つのソース DB インスタンスに対して複数のリードレプリカを作成して、アプリケーションの読み込みトラフィックをこれらのレプリカに分散させることができます。リードレプリカをマルチ AZ 配置と併せて作成することにより、マルチ AZ 配置が提供するデータの書き込み可用性と耐久性に加えて、読み込み性能を拡大することができます。

ソフトウェアの自動パッチ適用

Amazon RDS により、デプロイメントを駆動しているリレーショナルデータベースソフトウェアは、確実に最新のパッチで常に最新化されます。必要であれば、制御可能なメンテナンス時間中にパッチが適用されます。リクエストされた、または必要なイベントにおいて、DB インスタンスの修正（DB インスタンスクラスの拡張など）やソフトウェアのパッチが発生する場合、コントロールを行う機会として、Amazon RDS メンテナンスウィンドウを利用できます。「メンテナンス」イベントが特定の週に予定されている場合、識別する 30 分のメンテナンス時間中の一定の時点で開始され、完了します。

お客様の DB インスタンスをオフラインにする Amazon RDS を必要とする唯一のメンテナンスイベントは、スケール計算オペレーション（これは通常開始から終了まで数分のみを要します）。または要求されたソフトウェアパッチです。要求されたパッチに対しては、安全で堅牢かつ関連性のあるパッチのみが自動的にスケジューリングされます。このようなパッチは頻繁に発生するものではありません（通常数ヵ月ごとに一度です）。またお客様のメンテナンスウィンドウのごく一部以外を使用する必要があることは稀なはずです。DB インスタンスの作成時点で、希望する週間メンテナンス時間が指定されていない場合は、30 分のデフォルト値が割り当てられます。メンテナンスがお客様のために実行される際に修正を行いたい場合、AWS マネジメントコンソールで DB インスタンスを修正する、または ModifyDBInstance API を使用することでそれを行うことができます。お客様の各 DB インスタンスは、個々に異なるメンテナンス ウィンドウを選択することができます。

DB インスタンスをマルチ AZ 配置として実行すると、メンテナンスイベントの影響をさらに抑えることができますが、これは Amazon RDS が以下の手順でメンテナンスを実行するためです。1）スタンバイでメンテナンスを実行する、2）スタンバイをプライマリに昇格させる、3）古いプライマリでメンテナンスを実行し、これが新しいスタンバイになる。

Amazon RDS DB インスタンスの削除 API (DeleteDBInstance) が実行されると、DB インスタンスは削除用にマークされます。インスタンスに「削除中」ステータスが表示されない場合、削除済みです。この時点でインスタンスにアクセスできなくなります。また、最終スナップショットのコピーを作成しなかった場合は、復元できません。また、ツールや API でリストアップされることもなくなります。

イベント通知

インスタンスがシャットダウンされているか、バックアップが開始されているか、フェイルオーバーが発生しているか、セキュリティグループが変更されているか、またはストレージ容量が低下しているかどうかなど、RDS インスタンスに発生する可能性があるさまざまな重要なイベントの通知を受け取ることができます。そのカテゴリのイベントが発生したときに通知を受けることができるように、Amazon RDS サービスは、サブスクライブ可能なカテゴリにイベントをグループ分けします。DB インスタンス、DB スナップショット、DB セキュリティグループ、または DB パラメータグループのイベントのカテゴリーをサブスクライブできます。RDS のイベントは、AWS SNS 経由で公開され、お客様に電子メールまたはテキストメッセージとして送信されます。RDS の通知イベントのカテゴリーに関する詳細については、RDS のユーザーガイドを参照してください。

Amazon Redshift のセキュリティ

Amazon Redshift は、高度に最適化され、管理された AWS のコンピューティングおよびストレージ リソースで実行される、ペタバイト規模の SQL データウェアハウス サービスです。このサービスは、迅速に拡張または縮小できるだけでなく、極めて大規模なデータセットに対して実行する場合にもクエリのスピードを大幅に向上するように設計されています。パフォーマンスを向上させるために Redshift は、列形式のストレージ、データ圧縮、ゾーンのマッピングなどの手法を使用して、クエリを実行するために必要な IO の量を削減します。Amazon Redshift には超並列処理（MPP）アーキテクチャーが採用されており、SQL 操作の並列化と分散化によって、すべてのリソースがフルに活用されます。

Redshift データウェアハウスを作成するとき、クラスターを構成するノードのタイプおよび数を指定して、単一ノードまたは複数ノードのクラスターをプロビジョニングします。ノードのタイプによって、各ノードのストレージ サイズ、メモリおよび CPU が決まります。各複数ノードクラスターには、リーダーノードおよび 2 つ以上のコンピューティングノードが含まれます。リーダーノードは接続の管理、クエリの解析、実行計画の構築のほか、コンピューティングノードでのクエリの実行を管理します。コンピューティングノードは、データの格納、計算の実行のほか、リーダーノードの指示に従ってクエリを実行します。各クラスターのリーダーノード

は、標準の PostgreSQL ドライバを使用して ODBC と JDBC のエンドポイントとしてアクセス可能です。コンピューティングノードは、別個の分離されたネットワーク上で実行され、直接アクセスされることはありません。

クラスターをプロビジョニングした後は、データセットをアップロードし、一般的な SQL ベースのツールおよびビジネスインテリジェンスアプリケーションを使用してデータ分析クエリを実行できます。

クラスターのアクセス

デフォルトで、作成するクラスターは誰もアクセスできません。Amazon Redshift を使用すると、データウェアハウスクラスターへのネットワークアクセスをコントロールするためのファイアウォールルールを設定できます。Redshift を Amazon VPC の中で実行することもでき、このようにするとデータウェアハウスクラスターはお客様専用の仮想ネットワーク内に隔離されます。このクラスターを既存の IT インフラストラクチャに接続するには、業界標準の暗号化 IPsec VPN を使用します。

クラスターを作成する AWS アカウントには、クラスターへのフルアクセス権が付与されています。AWS アカウント内で、AWS IAM を使用して、ユーザーアカウントを作成し、それらのアカウントのアクセス権を管理できます。IAM を使用し、さまざまなユーザーにその職務に必要なクラスター操作のみを実行する権限を与えることができます。

すべてのデータベースと同様にリソースレベルでアクセスを付与することに加えて、データベースレベルで Redshift 内でアクセス許可を付与する必要があります。データベースユーザーには、データベースに接続できるユーザーアカウント名が与えられており、Amazon Redshift へのログイン時に認証されます。Redshift では、テーブルごとではなく、クラスターごとにデータベースユーザーのアクセス許可を付与します。ただし、ユーザーは、自身のアクティビティによって生成されたテーブルの行にのみデータを表示できます。他のユーザーによって生成された行は表示されません。

データベースのオブジェクトを作成したユーザーがその所有者です。デフォルトでは、スーパーユーザーまたはオブジェクトの所有者のみが、オブジェクトに対するクエリの実行、変更、アクセス権の付与が可能です。ユーザーがオブジェクトを使用するには、そのユーザー、またはそのユーザーが属するグループに、必要なアクセス権を付与する必要があります。さらに、オブジェクトの所有者のみが、それを変更または削除できます。

データバックアップ

Amazon Redshift は、クラスター内のすべてのコンピューティングノードにわたってデータを分散します。2 つ以上のコンピューティングノードを持つクラスターを実行する場合は、各ノードのデータが常に別のノードのディスクにミラーリングされ、データ損失が発生するリスクが減少します。さらに、クラスター内でノードに書き込まれたすべてのデータは、スナップショットを使用して Amazon S3 に継続的にバックアップされます。スナップショットの保持期間は、1 日以上 35 日以下の範囲内で指定できます。すべての既存システムのスナップショットを活用していつでも独自のスナップショットを取得することもでき、明示的に削除されるまでは保持できます。

クラスターの状態は常時モニタリングされており、障害があるドライブから自動的にデータを再度複製し、必要に応じてノードの交換が行われます。これらはすべて、お客様が何も作業しなくても実行されますが、再レプリケーション処理中パフォーマンスが多少低下する可能性があります。

システムのスナップショットまたはユーザーのスナップショットを使用し、AWS マネジメントコンソールまたは Amazon Redshift API からクラスターを復元できます。システムのメタデータが復元されるとすぐにクラスターを利用できるようになり、データがバックグラウンドでスプールされている間にクエリの実行を開始できます。

データの暗号化

クラスター作成時に、保存データの保護を強化するために暗号化を選択できます。クラスターで暗号化を有効にすると、Amazon Redshift は、ユーザーが作成したテーブルにすべてのデータをハードウェアアクセラレーションを利用した AES-256 ブロック暗号化キーを使用した暗号化形式で保存します。これには、ディスクに書き込まれたすべてのデータに加えて、すべてのバックアップが含まれます。

Amazon Redshift は、4 層のキーベースの暗号化アーキテクチャを使用します。これらのキーは、データ暗号化キー、データベースキー、クラスターキー、マスターキーから構成されます。

- データ暗号化キーは、クラスター内のデータブロックを暗号化します。各データブロックに、ランダムに生成された AES-256 キーが割り当てられます。これらのキーは、クラスターのデータベースキーを使用して暗号化されます。

- データベースキーは、クラスターのデータ暗号化キーを暗号化します。データベースキーは、ランダムに生成された AES-256 キーです。これは、Amazon Redshift クラスターとは別のネットワーク上にあるディスクに保存され、マスターキーで暗号化されます。Amazon Redshift は、セキュリティで保護されたチャネルを通じてデータベースキーを受け渡し、クラスターのメモリに保持します。
- クラスターキーは、Amazon Redshift クラスターのデータベースキーを暗号化します。クラスターキーを保管するには、AWS Key Management Service (AWS KMS) またはハードウェアセキュリティモジュール(HSM)を使用できます。HSM は、キーの生成と管理に関する直接的な制御を提供し、キー管理をアプリケーションおよびデータベースから分離します。
- マスターキーは、クラスターキーが AWS に保管されている場合はクラスターキーを暗号化します。クラスターキーが HSM に保管されている場合は、マスターキーはクラスターキーで暗号化されたデータベースキーを暗号化します。

Redshift では暗号化されたクラスターに対して、いつでも暗号化キーのローテーションを行うことができます。ローテーションプロセスの一部として、対象クラスターのすべての自動および手動スナップショットのキーも更新されます。

クラスターで暗号化を有効にすると、ハードウェアで加速されるものの、パフォーマンスに影響を与えることに注意してください。暗号化はバックアップにも適用されます。暗号化されたスナップショットから復元すると、新しいクラスターも暗号化されます。

テーブルロードデータファイルを Amazon S3 にアップロードするときに暗号化するには、Amazon S3 クライアント側の暗号化を使用します。Amazon S3 からデータをロードすると、テーブルのロード時に COPY コマンドによってデータが復号化されます。

データベース監査ロギング

Amazon Redshift はデータベースに対する接続試行、クエリ、変更を含むすべての SQL 操作をログに記録します。このログにアクセスするには、システムテーブルに対する SQL クエリを使用するか、Amazon S3 バケット上の安全な場所にログをダウンロードします。それらの監査ログをセキュリティおよびトラブルシューティングの目的でクラスターをモニターするために利用できます。

ソフトウェアの自動パッチ適用

Amazon Redshift は、容量のプロビジョニング、クラスターの監視、Amazon Redshift エンジンのパッチとアップグレードの適用など、設定、運用、データウェアハウスの拡張に関するあらゆる作業を管理します。パッチは、指定されたメンテナンスの時間枠にのみ適用されます。

SSL 接続

AWS クラウド内で送信中のデータを保護するために、Amazon Redshift はハードウェアアクセラレーション SSL を使用して Amazon S3 または Amazon DynamoDB と通信し、コピー、アンロード、バックアップ、復旧操作を実行します。クラスターに関連付けられたパラメータグループ内で SSL を指定することで、クライアントとクラスター間の接続を暗号化できます。クライアントに Redshift サーバーを認証させるには、SSL 証明書のパブリックキー(.pem ファイル)をクライアントにインストールし、このキーを使ってクラスターに接続します。

Amazon Redshift は、Elliptic Curve Diffie-Hellman Ephemeral プロトコルを使用する、より新しい強力な暗号スイートを提供しています。ECDHE を使用すると、SSL クライアントに対して、クライアントおよび Redshift クラスター間における Perfect Forward Secrecy を提供できます。Perfect Forward Secrecy は、どこにも保存されないエフェメラルなセッションキーを使用します。このキーを使用すると、長期間使用するシークレットキー自体が漏洩した場合でも、権限のない第三者によるキャプチャされたデータのデコードを防ぐことができます。ECDHE を有効にするために、Amazon Redshift で設定を行う必要はありません。ECDHE を使用してクライアント/サーバー間の通信を暗号化する SQL クライアントツールから接続する場合、Amazon Redshift は提供された暗号リストを使用して適切な接続を行います。

Amazon ElastiCache のセキュリティ

Amazon ElastiCache は、クラウドでのメモリ内分散キャッシュ環境のセットアップ、管理、およびスケーリングを容易に行えるようにするウェブサービスです。このサービスは、低速のディスクベースのデータベースに完全に頼る代わりに、高速の管理されたインメモリキャッシングシステムから情報を取得できるようにすることで、ウェブアプリケーションのパフォーマンスを向上させます。これは、多数の読み取り操作の多いアプリケーションの作業負荷(ソーシャルネットワーキング、ゲーム、メディア共有、Q&A ポータルなど)、または計算集約的な作業負荷(レコメンデーションエンジンなど)のレイテンシーおよびスループットを大幅に改善するために使用できます。キャッシングは、アクセスの待ち時間を短くするためにメモリ内にデータの重要な部分を格納することにより、アプリケーションのパフォーマンスを向上させます。キャッシュされた情報には、I/O 集中型データベースのクエリ結果や計算集中的な計算結果が含まれます。

Amazon ElastiCache サービスにより、パッチ管理、障害検出、および復旧など、インメモリキャッシュ環境の時間のかかる管理タスクが自動化されます。これは、安全で高パフォーマンスの管理されたインメモリキャッシュを提供するために、(Amazon EC2、Amazon CloudWatch、Amazon SNS などの)その他のアマゾン ウェブ サービス (AWS)クラウドと連携して動作します。たとえば、Amazon EC2 で実行中のアプリケーションは、同じリージョンの Amazon ElastiCache クラスターに非常に低いレイテンシーで安全にアクセスできます。

お客様は、Amazon ElastiCache サービスを使用してキャッシュクラスターを作成します。キャッシュクラスターは、1 つ以上のキャッシュノードの集合で、それぞれ Memcached サービスのインスタンスを実行します。キャッシュノードは、安全なネットワークに接続された RAM の固定サイズの断片です。各キャッシュノードは、Memcached サービスのインスタンスを実行し、それ自身の DNS 名とポートを持っています。それぞれ関連付けられている異なるメモリ量で、複数のタイプのキャッシュノードがサポートされています。キャッシュクラスターは、キャッシュノードの特定の数、および各キャッシュノードのプロパティをコントロールするキャッシュプロパティグループを使用して設定できます。キャッシュクラスター内のすべてのキャッシュノードは、同じノードタイプで、同一のパラメータ設定およびセキュリティグループ設定となるように設計されています。

Amazon ElastiCache を使用すると、キャッシュセキュリティグループを使用して、キャッシュクラスターへのアクセスをコントロールすることができます。キャッシュセキュリティグループは、キャッシュクラスタへのネットワークアクセスをコントロールするファイアウォールのように動作します。デフォルトでは、キャッシュクラスタへのネットワークアクセスは無効になっています。アプリケーションにキャッシュクラスタにアクセスさせる場合は、特定の EC2 セキュリティグループ内のホストからのアクセスを明示的に有効にする必要があります。入口ルールが設定されると、同じルールがそのキャッシュセキュリティグループに関連するすべてのキャッシュクラスターに適用されます。

キャッシュクラスターへのネットワークアクセスを許可するには、キャッシュセキュリティグループを作成し、Authorize Cache Security Group Ingress API または CLI コマンドを使用して、必要な EC2 セキュリティグループ を認証します(その結果として、許可されている EC2 インスタンスを指定します。)IP レンジベースのアクセスコントロールは現在、キャッシュクラスターでは有効になっていません。キャッシュクラスターへのすべてのクライアントは、EC2 ネットワーク内にある必要があり、キャッシュセキュリティグループを介して認可されていなければなりません。

ElastiCache for Redis には、バックアップと復元の機能が備わっています。この機能を使用すると、Redis クラスター全体のスナップショットを、特定の時点で存在していた状態で作成できます。定期的な日々の自動スナップショットをスケジュールできます。または、いつでも手動スナップショットを作成できます。自動スナップショットの場合、保持期間を指定できます。手動スナップショットはユーザーが削除するまで保持されます。スナップショットは、耐久性の高い Amazon S3 に保存され、ウォームスタート、バックアップ、アーカイブに使用できます。

アプリケーションサービス

アマゾン ウェブ サービスは、アプリケーションストリーミング、キュー、プッシュ通知、E メール配信、検索、トランスコーディングを提供するサービスなど、アプリケーションに使用できるさまざまなマネージドサービスを提供しています。

Amazon CloudSearch のセキュリティ

Amazon CloudSearch はクラウドにおけるマネージドサービスであり、ウェブサイト向けの検索ソリューションを容易に設定、管理、スケールできます。Amazon CloudSearch は、ウェブページ、ドキュメントファイル、フォーラムの投稿、製品情報など大規模なデータコレクションを検索できるようにします。ウェブサイトに検索機能を迅速に追加できます。検索の高度な知識を習得したり、ハードウェアの準備、設定、およびメンテナンスについて考える必要はありません。データやトラフィックの変動に伴い、Amazon CloudSearch はニーズに合わせて自動的に縮小または拡張します。

Amazon CloudSearch ドメインは、検索するデータコレクション、検索リクエストを処理する検索インスタンスに加えて、データにどのようにインデックスを作成し、データを検索するかを制御する設定をカプセル化します。検索可能にするデータの各コレクションについて、個別の検索ドメインを作成します。各ドメインに対して、インデックスに含めるフィールドを記述するインデックスオプション、ドメイン固有のストップワード、語幹、シノニムを定義するテキストオプション、検索結果のランク付け方法をカスタマイズするランク式、ドメインのドキュメントおよび検索エンドポイントへのアクセスを制御するアクセスポリシーを設定します。

承認されたホストのみがドキュメントを提出し、検索リクエストを送信できるように、検索ドメインのエンドポイントへのアクセス IP アドレスによって制限します。IP アドレスの承認は、ドキュメントおよび検索エンドポイントへのアクセスを制御するためにのみ使用します。すべての Amazon CloudSearch 設定リクエストは、標準の AWS 認証を使用して認証する必要があります。

Amazon CloudSearch は設定、検索、ドキュメントサービスにアクセスするための個別のエンドポイントを提供します。

- 構成サービスには、一般的なエンドポイント（cloudsearch.us-east-1.amazonaws.com）を通じてアクセスします
- ドキュメントサービスエンドポイントは、インデックス作成のためにドキュメントをドメインに送信するために使用され、ドメイン固有のエンドポイント（http://doc-domainname-domainid.us-east-1.cloudsearch.amazonaws.com）を通じてアクセスされます。
- 検索エンドポイントは、ドメインへの検索リクエストの送信に使用され、ドメイン固有のエンドポイント（http://search-domainname-domainid.us-east-1.cloudsearch.amazonaws.com）を通じてアクセスされます。

静的 IP アドレスを持たない場合は、IP アドレスが変更されるたびにコンピュータを再承認する必要があることに注意してください。IP アドレスを動的に割り当てる場合は、おそらくネットワーク上の他のコンピュータとそのアドレスを共有することになります。つまり、IP アドレスを許可する場合、その IP アドレスを共有するすべてのコンピュータが検索ドメインのドキュメントサービスエンドポイントにアクセスできます。

Amazon CloudSearch では、すべての AWS サービスと同様に、サービスのコントロール API に対する全リクエストに認証が必要です。したがって、許可されたユーザーのみが、CloudSearch ドメインにアクセスし、管理することができます。API リクエストは、リクエストから生成された HMAC-SHA1 または HMAC-SHA256 署名と、ユーザーの AWS シークレットアクセスキーによって署名されます。さらに、Amazon CloudSearch コントロール API には、SSL により暗号化されたエンドポイント経由でアクセスできます。AWS IAM を使用して AWS アカウントでユーザーを作成し、該当ユーザーが実行アクセス許可を持つ CloudSearch オペレーションを制御することによって、Amazon CloudSearch 管理機能へのアクセスを管理できます。

Amazon Simple Queue Service（Amazon SQS）のセキュリティ

Amazon SQS は、信頼性が高く、拡張可能なメッセージキューサービスであり、アプリケーションの分散コンポーネント間で、非同期のメッセージベースの通信を可能にします。コンポーネントは、コンピュータまたは Amazon EC2 インスタンス、または両方の組み合わせである場合があります。Amazon SQS を使用すれば、任意の数のメッセージを、任意のタイミングで、任意のコンポーネントから、Amazon SQS キューに送信することができます。メッセージは直ちに、または後で（4 日以内）、同一または異なるコンポーネントから取得可能です。メッセージは極めて堅牢です。各メッセージは可用性や信頼性が高いキュー内で、持続的に保管されます。複数のプロセスは、互いに干渉することなく、Amazon SQS キューに対して同時に読み書きを行うことができます。

Amazon SQS アクセス権は、AWS アカウント、または AWS IAM で作成されたユーザーに基づいて付与されます。認証されると、AWS アカウントはすべてのユーザー操作に対して完全なアクセス権を持ちます。ただし、AWS IAM ユーザーは、ポリシー経由でアクセス権が付与された操作とキューにしかアクセスできません。デフォルトでは、各個別キューに対するアクセスは、そのキューを作成した AWS アカウントに制限されています。ただし、SQS が生成したポリシーまたはユーザーが記述したポリシーを使用して、キューに対するその他のアクセスを許可することもできます。

Amazon SQS には、SSL 暗号化されたエンドポイント経由でアクセスできます。暗号化されたエンドポイントには、インターネットと Amazon EC2 内の両方からアクセスできます。Amazon SQS 内に保管されたデータは、AWS によっては暗号化されませんが、ユーザーは、Amazon SQS にアップロードする前にデータを暗号化できます。ただし、キューを使用するアプリケーションが、メッセージの取得時に暗号を解除する手段を備えていることが条件となります。Amazon SQS にメッセージを送信する前に暗号化すると、許可されていない人によるアクセスから重要な顧客データを保護するのに役立ちます。

Amazon Simple Notification Service（Amazon SNS）のセキュリティ

Amazon Simple Notification Service（Amazon SNS）は、クラウドからのメッセージ通知のセットアップ、作業、送信を簡単にするウェブサービスです。拡張性が高く、柔軟で、費用対効果の高い機能を開発者に提供し、アプリケーションからメッセージを発行し、利用者または他のアプリケーションに迅速に配信します。

Amazon SNS はシンプルなウェブ サービス インターフェイスを提供します。このインターフェイスを使用して、お客様がアプリケーション(または人)に通知したいトピックを作成したり、クライアントをそのトピックに登録したりできます。また、メッセージを発行し、そのメッセージをクライアントが選択したプロトコル(HTTP/HTTPS、電子メールなど)に配信することもできます。Amazon SNS は、「プッシュ」メカニズムを用いてクライアントに通知を行います。これは新しい情報や更新の定期的な確認または「調査」を必要としません。Amazon SNS は、信頼性が高く、イベント駆動型のワークフローやメッセージングアプリケーションを構築するために利用できます。複雑なミドルウェアやアプリケーション管理は必要ありません。その他、Amazon SNS の利用が考えられるものには、アプリケーション、ワークフローシステム、タイミングが鍵となる情報の更新、モバイルアプリケーション等のモニタリングへの適用があります。Amazon SNS はアクセス コントロール メカニズムを提供し、トピックとメッセージが、許可のないアクセスから保護されるようにします。トピックの所有者はトピック用のポリシーを設定して、トピックの発行者または受信者を制限できます。さらに、トピックの所有者は、配信メカニズムが HTTPS であることを指定することにより、送信を暗号化できます。

Amazon SNS アクセス権は、AWS アカウント、または AWS IAM で作成されたユーザーに基づいて付与されます。認証されると、AWS アカウントはすべてのユーザー操作に対して完全なアクセス権を持ちます。ただし、AWS IAM ユーザーは、ポリシー経由でアクセス権が付与された操作とトピックにしかアクセスできません。デフォルトでは、各個別トピックに対するアクセスは、そのトピックを作成した AWS アカウントに制限されています。ただし、SNS が生成したポリシーまたはユーザーが記述したポリシーを使用して、SNS に対するその他のアクセスを許可することもできます。

Amazon Simple Workflow Service(Amazon SWF)のセキュリティ

Amazon Simple Workflow Service(SWF)を使用すると、分散されたコンポーネント全体にわたって作業を調整するアプリケーションを簡単に構築できます。Amazon SWF を使用すれば、1 つのアプリケーション内のさまざまな処理ステップを分散アプリケーションで「タスク」として構成できます。Amazon SWF はこれらのタスクを確実にスケーラブルな方法で調整します。Amazon SWF は、タスク実行の従属関係、スケジューリング、および同時実行の管理を、開発者のアプリケーションロジックに従って行います。このサービスはタスクを保管し、アプリケーションコンポーネントにタスクを割り当ててその進行状況をトラッキングし、最新の状態情報を保持します。

Amazon SWF はシンプルな API 呼び出し機能を備えており、任意の言語のコードから実行できます。このコードは EC2 インスタンス上で実行することも、インターネットにアクセス可能な任意の場所のマシンで実行することもできます。Amazon SWF は、コーディネーションハブとして、お客様のアプリケーションホストと相互作用します。お客様は、タスクを組み合わせてワークフローを作成し、適用する条件ロジックがある場合は指定して、Amazon SWF に保管します。

Amazon SWF アクセス権は、AWS アカウントまたは AWS IAM で作成されたユーザーに基づいて付与されます。ワークフローの実行に参加するすべてのアクター(決定者、アクティビティワーカー、ワークフロー管理者)は、Amazon SWF リソースを所有する AWS アカウントの下で IAM ユーザー管理者である必要があります。その他の AWS アカウントに関連付けられているユーザーに、Amazon SWF ワークフローへのアクセス権を付与できません。ただし、AWS IAM ユーザーは、ポリシー経由でアクセス権が付与されたワークフローとリソースにしかアクセスできません。

Amazon Simple Email Service(Amazon SES)のセキュリティ

Amazon Simple Email Service (SES) は、Amazon の高信頼でスケーラブルなインフラストラクチャに構築された外部配信専用の E メール送信サービスです。Amazon SES を使用すると、E メールの配信可能性を最大限に高め、E メールの配信ステータスを常に把握することができます。Amazon SES はその他の AWS サービスと統合されているため、Amazon EC2 のようなサービスでホストされているアプリケーションから簡単に電子メールを送信することができます。

残念ながら、他の E メールシステムを使用すると、スパムの発信者が、E メールヘッダーを改ざんし、元のメールアドレスを偽装して、E メールが別の送信元から送られたように見せかけることができます。これらの問題を軽減するために、Amazon SES は、ユーザーの電子メールアドレスまたはドメインを確認することを要求しています。これにより、ユーザーが電子メールアドレスまたはドメインを所有していることを確認し、別のユーザーがそれを使用できないようにします。ドメインを検証するため、Amazon SES は、ドメインを管理していることの証明として Amazon SES が指定する DNS レコードを送信者がパブリッシュすることを要求します。Amazon SES は定期的にドメインの検証ステータスを見直し、有効でなくなっている場合には検証を取り消します。

Amazon SES では問題あるコンテンツが送られないよう積極的に取り組んでおり、ISP がアマゾンのドメインから受け取るメールは常に高品質です。それゆえに信頼できるメールサービスの発信元として受け取られます。すべての送信における配信性能と信頼性を最大化するために、次の機能があります。

- Amazon SES で使用されているコンテンツフィルタリングテクノロジーは、ウイルスやマルウェアが含まれるメッセージを検出してブロックし、これらが送信されることを未然に防ぎます。
- Amazon SES は、大手 ISP からのフィードバックループを維持しています。苦情フィードバックループにより、受信者がスパムとしてマークしたメールが分かります。Amazon SES では、お客様自身がこれらの配信メトリックスにアクセスすることができるので、送信戦略の方向付けに役立ちます。
- Amazon SES は、さまざまな手法を使用して各ユーザーの送信品質を測定します。これらのメカニズムは、Amazon SES を迷惑メール送信のために使用する試みの特定および無効化に役立ち、ISP、メールボックスプロバイダー、アンチスパムサービスによる Amazon SES のレピュテーションを傷つける他の送信パターンを検出します。
- Amazon SES は、Sender Policy Framework（SPF）やドメインキーアイデンティファイドメール（DKIM）などの認証メカニズムをサポートしています。E メールを認証するときに、ドメインを所有する ISP に証拠を提供します。Amazon SES により、メールの認証が簡単になります。Easy DKIM を使用するようアカウントを設定すると、お客様の代わりに Amazon SES がメールに DKIM 署名を付加するので、お客様はメール送信戦略の他の面に集中することができます。配信可能性を最大限確保するために、E メールを認証することをお勧めします。

他の AWS サービスと同様に、セキュリティ認証情報を使用して、お客様の身元と、お客様に Amazon SES を操作するためのアクセス権限があることを示します。どの認証情報を使用するかについては、「Amazon SES での認証情報の使用」を参照してください。Amazon SES は AWS IAM とも統合されているため、ユーザーが実行できる Amazon SES API アクションを指定することができます。

Amazon SES の SMTP インターフェイスを使用して Amazon SES と通信する場合は、TLS を使用して接続を暗号化する必要があります。Amazon SES は、STARTTLS および TLS ラッパーという、TLS で暗号化された接続を確立するための 2 つのメカニズムをサポートしています。HTTP 経由で Amazon SES と通信する場合は、すべての通信が Amazon SES の HTTPS エンドポイントを介して TLS によって保護される必要があります。Amazon SES は、E メールを最終送信先に送信する際、その E メールのコンテンツを便宜的な TLS で暗号化します（受信者がサポートしている場合）。

Amazon Elastic Transcoder サービス セキュリティ

Amazon Elastic Transcoder サービスは、1 つの形式、サイズ、品質から、別の形式、サイズ、品質にメディアファイルを変換するという、通常複雑なプロセスを簡素化します。Elastic Transcoder サービスは、オーディオファイルに加えて、標準解像度(SD)または高解像度(HD)のビデオファイルを変換します。これは Amazon S3 バケットから入力を読み取って変換し、それによって生成されたファイルを別の Amazon S3 バケットに書き込みます。同じバケットを入力と出力に使用でき、バケットは任意の AWS リージョンに配置できます。Elastic Transcoder は、さまざまな種類のウェブ、消費者、およびプロフェッショナル形式の入力ファイルを受け入れます。出力ファイルのタイプには、MP3、MP4、OGG、TS、WebM、MPEG-2 を使用する HLS、fmp4 コンテナを使用する Smooth Streaming などがあります(H.264 動画、VP8 動画、AAC 音声、MP3 音声、Vorbis 音声を保存)。

1 つ以上の入力ファイルから開始して、ファイルごとにトランスコーディングパイプラインというワークフローのタイプで変換ジョブを作成します。パイプラインの作成時に、IAM ロールとともに入力および出力バケットを指定します。各ジョブは、トランスコーディングプリセットいうメディア変換テンプレートを参照する必要があり、最終的に 1 つ以上の出力ファイルが生成されます。プリセットは、特定の入力ファイルを処理する際に使用する必要がある設定を Elastic Transcoder に指示します。プリセットの作成時に、サンプル レート、ビット レート、解像度(出力の高さと幅)、参照の数、およびキーフレーム、ビデオビットレート、サムネイル作成オプションなど、多数の設定を指定できます。

ベストエフォート型であり、送信順にジョブが開始されますが、ジョブは並行して処理され、また複雑さが異なるために、これは強い保証ではなく、通常は順序が入れ替わって完了します。必要に応じてパイプラインを停止し、再起動できます。

Elastic Transcoder は、各ジョブを開始および終了するとき、エラーまたは警告の状態を検出した旨を通知する必要があるときに、SNS 通知の使用をサポートします。SNS 通知のパラメータは、各パイプラインに関連付けられます。また、ステータスごとのジョブリスト機能を使用して特定ステータス (「Completed」など) のすべてのジョブを検索するか、ジョブの読み取り機能を使用して特定のジョブに関する詳細情報を取得できます。

他のすべての AWS サービスと同様に、Elastic Transcoder は、AWS Identity および Access Management (IAM) と統合し、このサービスへのアクセスに加えて、Amazon S3 バケット、Amazon SNS トピックなどの Elastic Transcoder に必要な他の AWS リソースへのアクセスを制御できます。デフォルトでは、IAM ユーザーは Elastic Transcoder またはそれが使用するリソースにアクセスできません。IAM ユーザーに Elastic Transcoder での作業を許可する場合、明示的にアクセス許可を付与する必要があります。

Amazon Elastic Transcoder では、そのコントロール API に対する全リクエストを認証する必要があります。したがって、認証されたプロセスまたはユーザーのみが独自の Amazon Transcoder のパイプラインおよびプリセットを変更、作成、または削除できます。リクエストは、リクエストから生成された HMAC-SHA256 署名と、ユーザーの秘密鍵から得られたキーによって署名されます。さらに、Amazon Elastic Transcoder API は、SSL によって暗号化されたエンドポイント経由でのみアクセスできます。

耐久性は、メディアファイルが Amazon S3 のリージョンの複数の施設にまたがる複数のデバイスに冗長的に格納される Amazon S3 によって提供されます。ユーザーが誤ってメディアファイルを削除した場合の保護を強化するには、Amazon S3 のバージョニング機能を使用できます。これにより、Amazon S3 バケットに保存されているすべてのオブジェクトのすべてのバージョンを保存、取得、復元できます。Amazon S3 バージョニングの MFA 削除機能を使用して、バージョンをさらに保護できます。これを Amazon S3 バケットに対して有効にした場合、バージョン削除リクエストに多要素認証デバイスの 6 桁のコードとシリアルナンバーが含まれている必要があります。

Amazon AppStream のセキュリティ

Amazon AppStream サービスは、ストリーミングアプリケーションを実行するためのフレームワークとして機能します。これは、特に、モバイルデバイスを実行している軽量クライアントを必要とするアプリケーションを対象としています。これを使用すると、クラウド内の強力な並列処理 GPU でアプリケーションを保存し、実行して、入出力を任意のクライアントデバイスにストリーミングできます。Amazon AppStream と連動するように既存のアプリケーションを変更することも、このサービスと連動する新しいアプリケーションを設計することもできます。

Amazon AppStream SDK によって、インタラクティブなストリーミングアプリケーションやクライアントアプリケーションの開発が簡単になります。SDK には、お客様の顧客のデバイスをお客様のアプリケーションに直接接続する、音声と動画をキャプチャしエンコードする、インターネットを介してほぼリアルタイムでコンテンツをストリーミングする、クライアントデバイスでコンテンツをデコードする、ユーザー入力をアプリケーションに返す、といった処理を行う API が用意されています。お客様のアプリケーションの処理はクラウド内で行われるため、これは膨大なコンピューティング負荷を処理するためにスケールできます。

Amazon AppStream は Amazon EC2 にストリーミングアプリケーションをデプロイします。AWS マネジメントコンソールを使用してストリーミングアプリケーションを追加すると、お客様のアプリケーションをホストするために必要な AMI が作成され、アプリケーションをストリーミングクライアントで使用できるようになります。需要に合わせて設定した容量制限内で、必要に応じてアプリケーションがスケーリングされます。Amazon AppStream SDK を使用するクライアントはストリーミングされるアプリケーションに自動的に接続されます。

一般的に、クライアントを実行しているユーザーが、セッション ID を取得する前に、お客様のアプリケーションを使用することを承認されているかどうかを確認する必要があります。クライアントを認証し、クライアントがお客様のアプリケーションに接続することを承認する使用権限管理サービスを利用することをお勧めします。この場合、使用権限管理サービスは、クライアントの新しいストリーミングセッションを作成するために、Amazon AppStream REST API も呼び出します。使用権限管理サービスは、新しいセッションを作成したら、承認したクライアントにワンタイム使用権限 URL としてセッション識別子を返します。クライアントは、使用権限 URL を使用してアプリケーションに接続します。使用権限管理サービスは、Amazon EC2 インスタンスまたは AWS Elastic Beanstalk でホストできます。

Amazon AppStream では、GPU EC2 インスタンスをデプロイするプロセスを自動化する AWS CloudFormation テンプレートが使用されています。このインスタンスは、AppStream Windows アプリケーションと Windows クライアント SDK ライブラリがインストールされています。また、このサービスは SSH、RDC、または VPN アクセスに対応するように設定されており、これには Elastic IP アドレスが割り当てられています。このテンプレートを使用してスタンドアロンストリーミングサーバーをデプロイすることにより、必要な作業はお客様のアプリケーションをサーバーにアップロードし、それを起動するコマンドを実行するだけになります。その後、Amazon AppStream サービスシミュレーターツールを使用して、アプリケーションを本稼動環境にデプロイする前にスタンドアロンモードでテストできます。

Amazon AppStream では、お客様のアプリケーションを AWS からローカルデバイスにストリーミングする処理を管理するために STX プロトコルも使用されています。Amazon AppStream の STX プロトコルは、独自のプロトコルであり、高品質アプリケーション動画をさまざまなネットワーク条件でストリーミングするために使用されます。これは、ネットワーク条件をモニタリングし、動画ストリームを自動的に適応させるため、動画視聴時のレイテンシーは低くなり、解像度は高くなります。音声と動画を同期したり、視聴者からの入力をキャプチャして AWS で実行中のアプリケーションに送り返したりする間に発生するレイテンシーは最小限に抑えられます。

分析サービス

アマゾン ウェブ サービスは、大量のデータも処理および分析できるクラウドベースの分析サービスを提供しており、マネージド Hadoop クラスター、リアルタイムストリーミングデータ、ペタバイト規模のデータウェアハウス、オーケストレーションといったさまざまなニーズに対応できます。

Amazon Elastic MapReduce（Amazon EMR）のセキュリティ

Amazon Elastic MapReduce（Amazon EMR）は、作業とデータを複数のサーバーに分散させることによって大量のデータを処理する Hadoop クラスターを使用できるマネージドウェブサービスです。このサービスでは、Amazon EC2 および Amazon S3 のウェブスケールのインフラストラクチャで実行されている Apache Hadoop フレームワークの強化バージョンが活用されています。入力データとデータ処理アプリケーションを Amazon S3 にアップロードするだけで、Amazon EMR が指定されている数の Amazon EC2 インスタンスを起動します。Amazon S3 から入力データを起動した Amazon EC2 インスタンスに投入する間に、サービスがジョブフローの実行を開始します。ジョブフローが終了すると、Amazon EMR は出力データを Amazon S3 に転送します。これにより、Amazon S3 でその出力データを取得したり、別のジョブフローの入力として使用したりできます。

お客様のためにジョブフローを起動すると、Amazon Elastic MapReduce は、マスターノード用およびスレーブ用の 2 つの Amazon EC2 セキュリティグループをセットアップします。マスターセキュリティグループには通信用に開いたポートがあり、これを使ってサービスを行っています。また SSH ポートが開いており、起動時に指定されたキーを使用して、SSH をインスタンスに対して許可することができます。スレーブは別のセキュリティグループで開始します。これらはマスターのインスタンスとのやりとりのみを許可します。デフォルトでは、どちらのセキュリティグループも、外部ソース（他のユーザーに属する Amazon EC2 インスタンスなど）からのアクセスを許可しないように設定されています。お客様のアカウント内にセキュリティグループが存在するため、標準 EC2 ツールまたはダッシュボードを使用して、それらの再設定を行うことができます。Amazon EMR は、視聴者の入力および出力データセットを保護するため、SSL を使用して Amazon S3 との間でデータを送受信します。

Amazon EMR では、いくつかの方法でクラスターのリソースへのアクセスを制御できます。AWS IAM を使用して、ユーザーアカウントとロールを作成し、それらがどの AWS 機能にアクセスできるかを制御するアクセス権限を設定できます。クラスターを起動するとき、Amazon EC2 キーペアをクラスターに関連付けることができます。これにより、SSH を使用してクラスターに接続できるようになります。また、デフォルトの Hadoop ユーザー以外のユーザーがジョブをクラスターに送信する許可を設定することもできます。

デフォルトでは、IAM ユーザーが起動したクラスターは、その AWS アカウントの他の IAM ユーザーからは見えません。このフィルタリングは、すべての Amazon EMR インターフェイス（コンソール、CLI、API、SDK）で行われ、IAM ユーザーが他の IAM ユーザーの作成したクラスターにアクセスしたり、不注意で変更したりすることを防止するために役立ちます。これは、1 人の IAM ユーザーとメインの AWS アカウントだけが見ることのできるクラスターを使用する場合に便利です。クラスターを 1 つの AWS アカウントに属するすべての IAM ユーザーに表示し、アクセスできるようにするオプションもあります。

保護をさらに強化するため、EMR クラスターの EC2 インスタンスを、プライベートサブネットで起動するように、Amazon VPC 内で起動できます。これにより、サブネットワーク全体へのアクセスを制御できます。クラスターを VPC 内で起動し、クラスターが VPN 接続を使用してお客様の内部ネットワーク上のリソースにアクセスできるように設定することもできます。入力データを Amazon S3 にアップロードする前に、一般的なデータ暗号化ツールを使用して入力データを暗号化できます。アップロードの前にデータを暗号化した場合、Amazon Elastic MapReduce が Amazon S3 からデータを取得したときに、ジョブフローの先頭に復号化ステップを追加する必要があります。

Amazon Kinesis のセキュリティ

Amazon Kinesis は、ビッグデータのリアルタイムストリーミングを処理することを目的としたマネージドサービスです。これは必要に応じてスケーリングできるため、多数のソースからの大量のデータにも対応できます。Kinesis は、サーバーログ、ソーシャルメディアやマーケットデータフィード、ウェブクリックストリームデータなどの大規模なリアルタイムデータ取り込みおよび処理が必要とされる状況で活用できます。

アプリケーションは、Amazon Kinesis との間でデータレコードを読み書きするために、ストリームを使用します。データをキャプチャ、保存、送信するために必要な数だけの Kinesis ストリームを作成できます。Amazon Kinesis は、ストリーミングアプリケーションが必要とするレベルのスループットでデータを収集および処理するために必要なインフラストラクチャ、ストレージ、ネットワーキング、設定を自動的に管理します。大規模データのリアルタイムキャプチャとストレージを可能にするためのハードウェア、ソフトウェア、またはその他のサービスのプロビジョニング、デプロイ、継続的保守を行う必要はありません。さらに、Amazon Kinesis は、同じ AWS リージョン内の 3 つの施設間でデータを同期的にレプリケートするので、高い可用性とデータ耐久性を提供します。

Amazon Kinesis のデータレコードには、シーケンス番号、パーティションキー、データ BLOB（解釈されない変更不可のバイトシーケンス）が含まれています。Amazon Kinesis サービスが BLOB 内のデータを検査、解釈、変更することはありません。データレコードは、Amazon Kinesis ストリームに追加されてから 24 時間のみアクセス可能で、24 時間が経過すると自動的に破棄されます。

お客様のアプリケーションは、一般的に複数の Amazon EC2 インスタンスで実行される Amazon Kinesis ストリームのコンシューマーです。Kinesis アプリケーションは、Amazon Kinesis クライアントライブラリを使用して、Amazon Kinesis ストリームからデータを読み取ります。Kinesis クライアントライブラリは、お客様に代わってフェイルオーバー、復旧、負荷分散などのさまざまな詳細を処理するため、お客様のアプリケーションは使用可能になったデータの処理に集中できます。レコードの処理が終了すると、お客様のコンシューマーコードがレコードを別の Kinesis ストリームに渡したり、Amazon S3 バケット、Redshift データウェアハウス、または DynamoDB テーブルに書き込んだり、単に破棄したりできるようになります。Kinesis を他の AWS サービス（DynamoDB、Redshift、Amazon S3 など）や Apache Storm などのサードパーティ製品と統合するには、コネクターライブラリを使用できます。

AWS IAM を使用してお客様の AWS アカウントでユーザーを作成し、作成したユーザーが実行できる Kinesis オペレーションを制御することによって、Kinesis のリソースおよび管理機能への論理アクセスを制御できます。Amazon EC2 インスタンスでのプロデューサーまたはコンシューマーアプリケーションの実行を容易にするため、IAM ロールを使用してそのインスタンスを設定できます。これにより、そのインスタンスのアプリケーションが、IAM ロールに関連付けられているアクセス権限を反映する AWS 認証情報を利用できるようになるため、有効期間の長い AWS セキュリティ認証情報を使用する必要がありません。ロールには、短期間で失効する一時的な認証情報を提供するという利点もあり、それによって保護がさらに強化されます。IAM ロールの詳細については、「IAM の使用」ガイドを参照してください。

Amazon Kinesis API は、SSL で暗号化されたエンドポイント（kinesis.us-east-1.amazonaws.com）を介してのみアクセスできるため、データを AWS に安全に送信するために役立ちます。Kinesis にアクセスするには、そのエンドポイントに接続する必要がありますが、接続した後は、API を使用して AWS リージョンにスタックを作成するように AWS Kinesis に指示できます。

AWS Data Pipeline のセキュリティ

AWS Data Pipeline サービスでは、データ駆動型ワークフローおよび組み込みの依存関係チェックを使用して、指定された間隔でさまざまなデータソース間でのデータの処理/移動を行うことができます。パイプラインを作成する場合と、データソース、前提条件、宛先、処理ステップ、運用スケジュールを定義します。パイプラインを定義してアクティブ化したら、指定したスケジュールに従って自動的に実行します。

AWS Data Pipeline では、リソースの可用性の保証、タスク間の依存関係の管理、タスクごとの一時的な失敗による再試行やタイムアウト、失敗通知システムの作成などについて心配する必要はありません。AWS Data Pipeline は、パイプラインでデータを処理し (Amazon EC2 や EMR など)、ストレージ (Amazon S3、RDS、DynamoDB、EMR など) に処理結果を転送するために必要になる AWS サービスとリソースを起動します。

このコンソールを使用する場合、AWS Data Pipeline は信頼されたエンティティ リストを含めて、必要な IAM ロールとポリシーを作成します。IAM ロールによって、パイプラインでアクセスできる対象と実行できるアクションが決定します。さらに、パイプラインがリソース (EC2 インスタンスなど) を作成する場合、IAM ロールによって EC2 インスタンスで許可されるリソースとアクションが決定します。パイプラインの作成時に、パイプラインを管理する 1 つの IAM ロールと、パイプライン リソースを管理するもう 1 つの IAM ロール (「リソースロール」と呼ばれます) を指定します。両者が同じロールであっても構いません。最小特権のセキュリティのベストプラクティスの一部として、パイプラインで作業を実行し、それに応じて IAM ロールを定義するために必要な最小限のアクセス許可を使用することをお勧めします。

ほとんどの AWS サービスと同様に、AWS Data Pipeline は SSL を介したアクセスのための安全な (HTTPS) エンドポイントオプションを提供します。

デプロイ & マネジメントサービス

アマゾン ウェブ サービスでは、お客様のアプリケーションのデプロイと管理に役立つ各種ツールを利用できます。一部のサービスでは、AWS サービスにアクセスするための認証情報を使用して個々のユーザーアカウントを作成できます。また、AWS リソースのスタックを作成および更新するためのサービス、これらのリソースにアプリケーションをデプロイするためのサービス、およびこれらのリソースの状態をモニタリングするためのサービスもあります。さらに、ハードウェアセキュリティモジュール（HSM）を使用して暗号キーを管理するためのツールや、セキュリティとコンプライアンスを確保するために AWS API アクティビティをログに記録するためのツールもあります。

AWS Identity and Access Management（AWS IAM）

AWS IAM により、複数のユーザーを作成し、AWS アカウント内でこれらのユーザーごとにアクセス許可を管理することができます。ユーザーは、AWS サービスへのアクセスに使うことができる独特なセキュリティ認証情報を持つ（AWS アカウント内の）アイデンティティです。AWS IAM を利用すると、パスワードやアクセスキーを共有する必要がなくなり、必要に応じてユーザのアクセスを簡単に有効化または無効化することができます。

AWS IAM を使用すると、「最小権限」などのセキュリティのベストプラクティスを実装できます。この最小権限では、AWS アカウント内のすべてのユーザーに独自の認証情報を割り当てて、ユーザーがジョブを実行するのに必要な AWS サービスおよびリソースのみへのアクセスを許可します。AWS IAM はデフォルトで安全です。新しいユーザーは、アクセス許可が明示的に付与されるまで、AWS へアクセスすることはできません。

マーケットプレイスで提供されるソフトウェアとサービスをサブスクライブできる組織内のユーザーをコントロールできるように、AWS IAM は、AWS Marketplace とも統合されます。マーケットプレイス内の特定のソフトウェアをサブスクライブすると、ソフトウェアを実行するための EC2 インスタンスが起動されます。これは、重要なアクセスコントロール機能です。

AWS IAM を使用して AWS マーケットプレイスへのアクセスをコントロールすると、AWS アカウント所有者は、使用状況やソフトウェアのコストを細かく制御することも可能になります。

AWS IAM を使用すると、AWS アカウント認証情報の使用を最小限に抑えることができます。AWS IAM ユーザーアカウントを作成すると、AWS サービスおよびリソースとのやり取りはすべて、AWS IAM ユーザーのセキュリティ認証情報を使用して実行される必要があります。AWS IAM の詳細については、AWS のウェブサイト（http://aws.amazon.com/iam/）をご覧ください。

ロール

IAM ロールは、一時的なセキュリティ認証情報を使用して、お客様の AWS リソースに通常はアクセスできないユーザーまたはサービスにアクセスを委任できるようにします。ロールは、特定の AWS リソースにアクセスするための一連のアクセス権限ですが、これらのアクセス権限は、特定の IAM ユーザーまたはグループに関連付けられていません。承認されたエンティティ（モバイルユーザー、EC2 インスタンスなど）は、ロールを引き受け、ロールで定義されているリソースにアクセスするための認証に必要な一時的なセキュリティ認証情報を受け取ります。一時的なセキュリティ認証情報は、存続期間が短く（デフォルトの有効期間は 12 時間）、失効すると再利用できないため、セキュリティを強化するために効果的です。これは、特定の状況で、制限のあるコントロールされたアクセスを提供する際に特に役立つ場合があります。

- **フェデレーティッド (AWS 以外の) ユーザーアクセス。**フェデレーティッドユーザーは、AWS アカウントがないユーザー（またはアプリケーション）です。ロールを使用すると、お客様の AWS リソースへのアクセスを一定期間のみにわたって許可できます。これは、Microsoft の Active Directory、LDAP、Kerberos などの外部サービスを使用して認証できる AWS 以外のユーザーがある場合に役立ちます。ロールとともに一時的な AWS 認証情報を使用すると、お客様の組織の ID および承認システム内の AWS ユーザーと AWS ユーザー以外との間で ID フェデレーションが生成されます。
- お客様の組織が SAML 2.0（Security Assertion Markup Language 2.0）をサポートしている場合、ID プロバイダー（IdP）としてのお客様の組織とサービスプロバイダーとしての他の組織との間に信頼を作成できます。AWS では、AWS をサービスプロバイダーとして設定し、SAML を使用して AWS マネジメントコンソールへのフェデレーションシングルサインオン（SOO）をお客様のユーザーに提供したり、フェデレーションアクセスを取得して AWS API を呼び出したりできます。
- ロールは、AWS リソースにアクセスするモバイルまたはウェブベースのアプリケーションを作成する場合にも便利です。AWS リソースは、プログラムによるリクエストに対してセキュリティ認証情報を要求しますが、有効期間の長いセキュリティ認証情報をお客様のアプリケーションに埋め込むことはお勧めしません。アプリケーションのユーザーがその認証情報にアクセスでき、またローテーションが困難になる可能性があるからです。代わりに、ユーザーが Amazon、Facebook、または Google でのログインを使用してお客様のアプリケーションにサインインし、ユーザーの認証情報を使用してロールを引き受け、一時的なセキュリティ認証情報を取得できるようにできます。
- **クロスアカウントアクセス。**複数の AWS アカウントを使用してリソースを管理している場合、あるアカウントでアクセス権限を持っているユーザーが別のアカウントのリソースにアクセスできるようにロールをセットアップできます。別のアカウントのリソースにまれにしかアクセスする必要のないユーザーがいる場合、ロールを使用することで、その認証情報が必要なときにのみ一時的に提供されるようにできます。

- **AWS リソースにアクセスする必要のある EC2 インスタンスで実行されているアプリケーション。**アプリケーションが Amazon EC2 インスタンスで実行されており、Amazon S3 バケットや DynamoDB テーブルなどの AWS リソースをリクエストする必要がある場合、そのセキュリティ認証情報が必要になります。各インスタンスの各アプリケーションの IAM アカウントを個別に作成する代わりに、ロールを使用すると、多数のインスタンスを管理する顧客、または AWS の Auto Scaling を使用して柔軟にスケーリングするフリートを管理する顧客は、時間を大幅に節約できます。

一時認証情報には、セキュリティトークン、アクセスキー ID、およびシークレットアクセスキーが含まれます。特定のリソースにアクセスを付与するには、一時アクセスを付与するユーザーに一時的なセキュリティ認証情報を分散します。ユーザーがリソースを呼び出すとき、ユーザーは、トークンとアクセスキー ID を渡し、シークレットアクセスキーでリクエストに署名します。トークンは、異なるアクセスキーでは機能しません。ユーザーがトークンを渡す方法は、ユーザーが呼び出す API および AWS 製品のバージョンによって異なります。一時的なセキュリティ認証情報についての詳細は、AWS ウェブサイト（http://docs.amazonwebservices.com/STS）にあります。

一時ユーザーに対して長期の認証情報を管理または分散する必要はないため、一時認証情報を使用することは、追加の保護が提供されることを意味します。さらに、一時認証情報はターゲットインスタンスに自動的にロードされるため、コードのように安全でない場所に認証情報を埋め込む必要はありません。一時認証情報は、ユーザーが何もしなくても 1 日に複数回自動的に更新または変更され、デフォルトで安全に保存されます。

IAM ロールを使用して、EC2 インスタンスのアクセスキーを自動プロビジョニングする方法の詳細については、AWS ウェブサイトの IAM の使用ガイド（http://docs.amazonwebservices.com/IAM）を参照してください。

Amazon CloudWatch のセキュリティ

Amazon CloudWatch は、Amazon EC2 で起動し、AWS クラウドリソースのモニタリングを提供するウェブサービスです。CPU 使用状況、ディスク読み込みや書き込み、ネットワークトラフィックなどの測定指標など、これはリソースの使用状況に対する視認性、運用上のパフォーマンス、そして全体的な需要パターンを顧客に提供します。特定のしきい値を超過したときに通知を送ったり、その他の自動アクション（Auto Scaling が有効である場合に EC2 インスタンスを追加または削除するなど）を実行したりするように CloudWatch アラームをセットアップできます。

CloudWatch は、AWS リソースの使用状況メトリックスをネイティブにキャプチャして要約します。また、他のログを CloudWatch に送信し、そこでモニタリングされるようにすることもできます。お客様のゲスト OS、アプリケーション、EC2 インスタンスにインストールされているソフトウェアのカスタムログファイルを CloudWatch にルーティングし、そこで永続的に保存されるようにできます。CloudWatch が受信したログエントリに特定のシンボルまたはメッセージがあるかどうかをモニタリングし、結果を CloudWatch のメトリックスとして視覚化するように設定できます。たとえば、お客様のウェブサーバーのログファイルに 404 エラーがあるかどうかをモニタリングして無効なインバウンドリンクを検出したり、無効なユーザーメッセージがあるかどうかをモニタリングしてお客様のゲスト OS への不正ログインの試みを検出したりできます。

Amazon CloudWatch では、すべての AWS サービスと同様に、サービスのコントロール API に対する全リクエストに認証が必要です。したがって、許可されたユーザーのみが、CloudWatch にアクセスし、管理することができます。リクエストには、リクエストとユーザーの秘密鍵から生成された HMAC-SHA1 署名が添付されます。さらに、Amazon CloudWatch コントロール API には、SSL 暗号化されたエンドポイント経由でのみアクセスできます。

AWS IAM を使用して AWS アカウントでユーザーを作成し、そのユーザーがどの CloudWatch 操作に対して呼び出し権限を持つかを制御することにより、Amazon CloudWatch へのアクセスをさらに細かく管理できます。

AWS CloudHSM のセキュリティ

AWS CloudHSM サービスを利用すると、侵入防止や改ざん検知機能を持つデバイスで安全な暗号キーのストレージと運用を提供するように設計されたハードウェアセキュリティモジュール（HSM）アプライアンスにアクセスできます。データ暗号化に使用する暗号キーを、お客様しかアクセスできないように生成、保存、管理できます。AWS CloudHSM アプライアンスは、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、さまざまな用途に使用する暗号キーマテリアルを保存および処理するよう設計されています。また、AES、RSA、ECC、およびその他の使用可能な強力な暗号アルゴリズムをサポートしています。

AWS CloudHSM サービスは、Amazon EC2 や VPC と組み合わせて使用して、プライベートサブネット内でアプライアンスに独自のプライベート IP を提供するように設計されています。EC2 サーバーから CloudHSM アプライアンスへの接続には、双方向のデジタル証明書による認証と 256 ビットの暗号化を使用して安全な通信チャネルを提供する SSL/TLS を使用します。

EC2 インスタンスと同じリージョンにある CloudHSM サービスを選択すると、ネットワークのレイテンシーが小さくなり、アプリケーションのパフォーマンスが向上します。EC2 インスタンスにクライアントを設定して、アプリケーションで PKCS#11、MS CAPI、Java JCA/JCE（Java Cryptography Architecture/Java Cryptography Extensions）などの HSM から提供される API を利用することができます。

HSM の使用を開始する前に、アプライアンスにパーティションを 1 つ以上設定する必要があります。暗号パーティションは論理的かつ物理的なセキュリティの境界で、ユーザーのキーへのアクセスを制限します。そのため、ユーザーのキーおよび HSM が実行する操作は、ユーザーにしか制御できません。AWS にはアプライアンスに対する管理用の認証情報がありますが、この認証情報はアプライアンスの管理にのみ使用され、アプライアンスの HSM パーティションには使用されません。AWS はこの認証情報をアプライアンスの状態および可用性の監視/保守のために使用します。AWS ではユーザーのキーの抽出や、キーを使用したアプライアンスでの暗号化操作を実行することはできません。

HSM アプライアンスは物理的および論理的両方の改ざん検出および対応メカニズムであり、改ざんが検出された場合には暗号キーマテリアルを消去してイベントログを生成します。HSM は、HSM アプライアンスの物理的な防壁が突破された場合、不正使用を検出するように設計されています。さらに、HSM 管理者認証情報を使用した HSM パーティションへのアクセスが 3 回失敗すると、HSM アプライアンスはその HSM パーティションを削除します。

CloudHSM のサブスクリプションが終了し、HSM のコンテンツが不要であることを確認したら、各パーティションとそのコンテンツ、およびログを削除する必要があります。廃棄プロセスの一環として、AWS はアプライアンスをゼロにし、すべてのキーマテリアルを永久に無効にします。

AWS CloudTrail のセキュリティ

AWS CloudTrail は、お客様のアカウント内における AWS リソースのリクエストをすべて記録したログを提供します。記録されているイベントごとに、アクセスされたサービス、実行されたアクション、そのアクションのパラメータ、リクエストを確認できます。AWS サービスでアクションを実行したユーザーまたはサービスを確認できるだけではなく、それが AWS ルートアカウントユーザーであったか IAM ユーザーであったか、またはロールの一時的な認証情報が使用されたかフェデレーションユーザーの一時的な認証情報が使用されたかも確認できます。

CloudTrail は、基本的に、AWS マネジメントコンソール、CLI、または SDK から行われたかにかかわらず、AWS リソースに対するすべての API 呼び出しに関する情報をキャプチャします。API リクエストがエラーを返した場合、CloudTrail は、承認に失敗したことを示すメッセージとともに、そのエラーの説明を提供します。また、AWS マネジメントコンソールのサインインイベントもキャプチャし、AWS アカウント所有者、フェデレーションユーザー、または IAM ユーザーがコンソールにサインインするたびにログレコードを作成します。

CloudTrail を有効にすると、お客様が指定した Amazon S3 バケットに 5 分間隔でイベントログが送信されます。ログファイルは、AWS アカウント ID、リージョン、サービス名、日付、時刻に基づいて整理されます。CloudTrail は、複数のリージョンからのログファイルを 1 つの Amazon S3 バケットに集約するように設定できます。こうすると、使い慣れたログ管理および分析ソリューションにログファイルをアップロードし、セキュリティ分析を実行して、ユーザーの行動パターンを検出できます。

デフォルトでは、ログファイルは永続的に保存されます。ログファイルは、Amazon S3 のサーバー側の暗号化を使用して自動的に暗号化され、削除またはアーカイブするまでバケット内に残ります。Amazon S3 のライフサイクル設定ルールを使用して、自動的に古いログファイルが削除されるようにしたり、低コストでより長い期間にわたってログファイルを使用できるよう Amazon Glacier にアーカイブしたりできます。

他の AWS サービスと同様に、特定のユーザーしか CloudTrail にアクセスできないように制限できます。IAM を使用すると、どの AWS ユーザーが AWS CloudTrail の証跡を削除、設定、削除できるかを制御できるだけではなく、どのユーザーがログ記録を開始および終了できるかも制御できます。IAM または Amazon S3 バケットのポリシーを適用することによって、ログファイルへのアクセスを制御できます。Amazon S3 バケットで MFA Delete を有効にすることによって、セキュリティをさらに強化することもできます。

モバイルサービス

AWS モバイルサービスを使用すると、クラウド駆動のモバイルデバイス用アプリケーションをより簡単に構築、配信、実行、モニタリング、最適化、スケールできます。また、お客様のモバイルアプリケーションのユーザーの認証、データの同期、アプリケーションの使用状況データの収集と分析を行うこともできます。

Amazon Cognito

Amazon Cognito は、モバイルおよびウェブベースのアプリケーションを対象とした ID および同期サービスです。これにより、ユーザーの認証、および複数のデバイス、プラットフォーム、アプリケーションにわたるデータの保存、管理、同期が簡素化されます。これは、認証されているユーザーと認証されていないユーザーの両方に、権限が制限されている一時的な認証情報を提供します。お客様はバックエンドインフラストラクチャを管理する必要がありません。

Cognito は、Google、Facebook、Amazon などの広く利用されているアイデンティティプロバイダーと連動して、お客様のモバイルおよびウェブアプリケーションのエンドユーザーを認証します。お客様独自の ID および承認機能を構築し、維持する代わりに、これらのサービスによって提供される ID および承認機能を利用できます。お客様のアプリケーションは、これらのアイデンティティプロバイダーのいずれかと連動して、プロバイダーの SDK を使用して認証を行います。エンドユーザーがプロバイダーによって認証されると、プロバイダーから返される OAuth または OpenID Connect のトークンがお客様のアプリケーションによって Cognito に渡され、ユーザーの新しい Cognito ID と、権限が制限されている一時的な AWS 認証情報が Amazon Cognito から返されます。

Amazon Cognito の使用を開始するには、Amazon Cognito コンソールを使用してアイデンティティプールを作成します。アイデンティティプールとは、お客様の AWS アカウントに固有のユーザー ID 情報のストアです。アイデンティティプールの作成中、お客様のエンドユーザーに対して新しい IAM ロールを作成するか、既存のロールを選択するかを確認するメッセージが表示されます。IAM ロールは、特定の AWS リソースにアクセスするための一連のアクセス権限ですが、これらのアクセス権限は、特定の IAM ユーザーまたはグループに関連付けられていません。承認されたエンティティ（モバイルユーザー、EC2 インスタンスなど）は、ロールを引き受け、ロールで定義されている AWS リソースにアクセスするための認証に必要な一時的なセキュリティ認証情報を受け取ります。一時的なセキュリティ認証情報は、存続期間が短く（デフォルトの有効期間は 12 時間）、失効すると再利用できないため、セキュリティを強化するために効果的です。

選択するロールによって、お客様のエンドユーザーが一時的な認証情報を使用してアクセスできる AWS サービスが決定されます。デフォルトでは、Amazon Cognito はアクセス権限が制限されている新しいロールを作成するので、エンドユーザーがアクセスできるのは Cognito Sync サービスと Amazon Mobile Analytics のみです。お客様のアプリケーションが Amazon S3 や DynamoDB などの他の AWS リソースにアクセスする必要がある場合は、IAM マネジメントコンソールから直接ロールを変更できます。

Amazon Cognito を使用すると、お客様の AWS リソースにアクセスする必要のあるウェブまたはモバイルアプリのすべてのエンドユーザーのために AWS アカウントまたは IAM アカウントを個別に作成する必要がありません。IAM ロールとともに使用することにより、モバイルユーザーはアカウントを作成したりログインしたりすることなく AWS リソースとアプリケーション機能に安全にアクセスでき、AWS クラウドにデータを保存することもできます。ただし、ユーザーがこれを後で行うことにした場合、Cognito はデータと識別情報をマージします。

Amazon Cognito はデータをサービスの中に保存するだけでなく、ローカルにも保存するため、お客様のエンドユーザーはオフラインになった後も引き続きデータを操作できます。ユーザーのオフラインデータが古くなる場合もありますが、データセットに保存されているデータは、オンラインであるかどうかにかかわらず、すぐに取得できます。クライアント SDK は、アプリケーションが接続されていないときでも動作できるようにローカル SQLite ストアを管理します。SQLite ストアはキャッシュとして機能し、すべての読み書きオペレーションがこれに対して行われます。Cognito の同期機能は、ローカルバージョンのデータをクラウド上のバージョンと比較し、必要に応じて差分をプッシュアップまたはプルダウンします。複数のデバイスにわたってデータを同期するには、アイデンティティプールが、認証されているアイデンティティに対応している必要があります。認証されていないアイデンティティはデバイスに関連付けられているため、エンドユーザーが認証されていなければ、データを複数のデバイスにわたって同期できません。

Cognito を使用すると、お客様のアプリケーションは、サポートされているパブリックアイデンティティプロバイダー（Amazon、Facebook、または Google）と直接通信してユーザーを認証します。Amazon Cognito は、ユーザーの認証情報を受け取ったり保存したりせず、アイデンティティプロバイダーから OAuth または OpenID Connect トークンを受け取るのみです。Cognito は、トークンを受け取ると、ユーザーの新しい Cognito ID と、権限が制限されている一時的な AWS 認証情報を返します。

Cognito ID は、同期ストア内の独自のデータにのみアクセスでき、このデータは保存時に暗号化されます。さらに、アイデンティティデータはすべて HTTPS 経由で送信されます。デバイス上の一意の Amazon Cognito 識別子は、適切で安全な場所に保存されます。たとえば、iOS では、Cognito 識別子は iOS キーチェインに保存されます。ユーザーデータは、アプリケーションのサンドボックス内にあるローカルの SQLite データベースにキャッシュされます。セキュリティをさらに強化する必要がある場合は、お客様のアプリケーションに暗号化を実装することによって、このローカルキャッシュ内の ID データを暗号化できます。

Amazon Mobile Analytics

Amazon Mobile Analytics は、モバイルアプリケーションの使用状況データを収集、視覚化、把握するためのサービスです。これを使用すると、顧客の行動を追跡したり、メトリックスを集計したりできるほか、お客様のモバイルアプリケーションにおける特徴的なパターンを特定できます。Amazon Mobile Analytics は、お客様のアプリを実行しているクライアントデバイスからデータを受信すると、使用状況のメトリックスを自動的に計算し、更新して、コンソールにデータを表示します。

お客様のアプリケーションを Amazon Mobile Analytics と統合しても、アイデンティティプロバイダー（Google、Facbook、または Amazon）を使用してお客様のアプリケーションのユーザーを認証する必要はありません。Mobile Analytics は、このような認証されていないユーザーには、Amazon Cognito と連動して、権限が制限されている一時的な認証情報を提供します。これを行うには、まず Cognito でアイデンティティプールを作成します。アイデンティティプールは、特定の IAM リソースへのアクセスを許可する、特定の IAM ユーザーまたはグループに関連付けられてない一連のアクセス権限である IAM ロールを使用します。このエンティティは、ロールを引き受け、ロールで定義されている AWS リソースにアクセスするための認証に必要な一時的なセキュリティ認証情報を受け取ります。デフォルトでは、Amazon Cognito はアクセス権限が制限されている新しいロールを作成するので、エンドユーザーがアクセスできるのは Cognito Sync サービスと Amazon Mobile Analytics のみです。お客様のアプリケーションが Amazon S3 や DynamoDB などの他の AWS リソースにアクセスする必要がある場合は、IAM マネジメントコンソールから直接ロールを変更できます。

AWS Mobile SDK for Android または iOS をお客様のアプリケーションに統合することも、Amazon Mobile Analytics REST API を使用して接続されているデバイスまたはサービスからのイベントを送信し、レポートでデータを視覚化することもできます。Amazon Mobile Analytics API は、SSL で暗号化されているエンドポイント（https://mobileanalytics.us-east-1.amazonaws.com）を介してのみアクセスできます。

アプリケーション

AWS アプリケーションは、お客様のユーザーにクラウド内の安全な一元管理型ストレージと作業領域を提供できるようにするマネージドサービスです。

Amazon WorkSpaces

Amazon WorkSpaces は、お客様のユーザーのためにクラウドベースのデスクトップを迅速にプロビジョニングできるようにするマネージドデスクトップサービスです。お客様のユーザーのニーズに最適な Windows 7 バンドルと、起動する WorkSpaces の数を選択するだけで、WorkSpaces が使用できるようになると、ユーザーは関連クライアントをダウンロードできる場所とユーザーの WorkSpace にログインできる場所を通知する E メールを受け取ります。これで、ユーザーは、PC、ノート PC、モバイルデバイスなどのさまざまなエンドポイントデバイスからクラウドベースのデスクトップにアクセスできるようになります。お客様の組織のデータがエンドユーザーのデバイスに送信されたり保存されたりすることはありません。Amazon WorkSpaces は、実際のデータを送信することなくインタラクティブ動画ストリームを提供する PC-over-IP（PCoIP）を使用しているからです。PCoIP プロトコルは、ユーザーのデスクトップにおけるコンピューティングアクティビティを圧縮、暗号化、エンコードし、"ピクセルのみ" を標準の IP ネットワーク経由でエンドユーザーのデバイスに送信します。

ユーザーが WorkSpace にアクセスするには、一意の認証情報のセットまたは通常使用する Active Directory 認証情報を使用してサインインする必要があります。Amazon WorkSpaces をお客様の組織の Active Directory と統合すると、WorkSpace はお客様の Active Directory ドメインに含められ、組織内の他のデスクトップとまったく同様に管理できます。つまり、Active Directory のグループポリシーを使用して、お客様のユーザーの WorkSpaces を管理し、デスクトップを制御する設定オプションを指定できます。お客様のユーザーの WorkSpaces を管理するために Active Directory またはその他のタイプのオンプレミスディレクトリを使用しない場合は、管理用のプライベートクラウドディレクトリを Amazon WorkSpaces 内に作成できます。

セキュリティをさらに強化するため、サインイン時にハードウェアまたはソフトウェアトークンの形式で多要素認証の利用を要求することもできます。Amazon WorkSpaces は、オンプレミスの Remote Authentication Dial In User Service（RADIUS）サーバー、または RADIUS 認証をサポートするセキュリティプロバイダーを使用する多要素認証をサポートしています。現時点では、RADIUS プロキシに加えて、PAP、CHAP、MS-CHAP1、MS-CHAP2 プロトコルがサポートされています。

WorkSpace は、VPC 内の独自の EC2 インスタンスに配置されています。既に所有している VPC 内に WorkSpaces を作成することも、WorkSpaces のクイックスタートオプションを使用して WorkSpaces サービスが自動的に WorkSpaces を作成するように設定することもできます。クイックスタートオプションを使用する場合、WorkSpaces は VPC を作成するだけではなく、たとえば、VPC のインターネットゲートウェイを作成する、ユーザー情報と WorkSpaces 情報を保存するために使用されるディレクトリを VPC 内にセットアップする、ディレクトリ管理者アカウントを作成する、特定のユーザーアカウントを作成してディレクトリに追加する、WorkSpace インスタンスを作成するなどのその他のプロビジョニングおよび設定タスクも実行します。また、既存のオンプレミスの Active Directory と他のイントラネットのリソースにアクセスできるように、安全な VPN 接続を使用して VPC をオンプレミスネットワークに接続することができます。Amazon VPC 内に作成したセキュリティグループを、ディレクトリに属するすべての WorkSpaces に追加することができます。これにより、Amazon VPC 内の Amazon WorkSpaces から VPC 内のその他のリソースおよびオンプレミスネットワークへのネットワークアクセスを制御できます。

WorkSpaces の永続的ストレージは、Amazon EBS によって提供され、1 日に 2 回 Amazon S3 に自動的にバックアップされます。WorkSpaces Sync が WorkSpace で有効になっている場合、ユーザーが同期を選択したフォルダーは継続的にバックアップされ、Amazon S3 に保存されます。WorkSpaces Sync を Mac または PC で使用して、WorkSpace との間でドキュメントを同期することもできます。これにより、使用するデスクトップコンピューターに関係なく、常にデータにアクセスできます。

これはマネージドサービスであるため、AWS が日次バックアップやパッチ適用などのいくつかのセキュリティおよび保守タスクを行います。更新は週次の保守管理時間枠の間に WorkSpaces に自動的に配信されます。ユーザーの WorkSpace のパッチ適用を設定する方法を制御できます。デフォルトでは、Windows Update はオンになっていますが、その設定をカスタマイズしたり、必要であれば、パッチ管理に代替手法を利用したりできます。ベースとなる OS については、WorkSpaces では Windows Update がデフォルトで有効になっており、更新を週に 1 回インストールするように設定されています。代替のパッチ適用方法を使用することも、お客様にとって適切な時間帯に Windows Update が更新を実行するように設定することもできます。

IAM を使用して、チームのどのメンバーが管理機能（WorkSpaces の作成や削除、ユーザーのディレクトリのセットアップなど）を実行できるかを制御できます。また、ディレクトリ管理用の WorkSpace をセットアップしたり、使い慣れた Active Directory 管理ツールをインストールしたりできるほか、すべての WorkSpaces ユーザーがより簡単に Active Directory の変更を適用できるように組織単位とグループポリシーを作成することもできます。

Amazon Zocalo

Amazon Zocalo は、ユーザーのコラボレーションに役立つフィードバック機能を備えたマネージドエンタープライズストレージおよび共有サービスです。ユーザーは、さまざまなタイプのファイルを Zocalo フォルダーに保存でき、他のユーザーがこれらのファイルを表示したりダウンロードしたりすることを許可できます。コメント機能と注釈機能は、MS Word などの特定のファイルタイプで動作し、ファイルを作成するために使用されたアプリケーションを必要としません。Zocalo は、レビューアクティビティと期限を寄稿者に E メールで通知し、Zocalo Sync アプリケーションを使用して同期しているファイルのバージョニングを行います。

ユーザー情報は、Active Directory と互換性のあるネットワークディレクトリに保存されます。クラウドに新しいディレクトリを作成するか、オンプレミスディレクトリに Amazon Zocalo を接続することができます。Zocalo のクイックスタートセットアップを使用してクラウドディレクトリを作成すると、管理者の E メールをユーザー名とするディレクトリ管理者アカウントも作成されます。登録を完了する手順が記載された E メールが管理者に送信されます。管理者は、このアカウントを使用してディレクトリを管理します。

Zocalo のクイックスタートセットアップを使用してクラウドディレクトリを作成すると、そのディレクトリで使用する VPC も作成および設定されます。ディレクトリ設定を詳細に制御する必要がある場合、標準セットアップを選択できます。標準セットアップでは、独自のディレクトリドメイン名のほか、ディレクトリで使用する既存の VPC の 1 つを指定できます。既存の VPC を使用する場合は、その VPC にインターネットゲートウェイと少なくとも 2 つのサブネットがある必要があります。各サブネットはそれぞれ異なるアベイラビリティーゾーンにある必要があります。

Amazon Zocalo マネジメントコンソールを使用すると、管理者は、時間、IP アドレス、デバイスごとに、ファイルとユーザーの活動を追跡する監査ログを表示したり、ユーザーが組織外の他者とファイルを共有することを許可するかどうかを選択したりできます。これにより、ユーザーは誰がどのファイルにアクセスできるかを制御したり、共有しているファイルのダウンロードを無効にしたりできます。

通信中のデータは、すべて業界標準の SSL で暗号化されます。Zocalo のウェブおよびモバイルアプリケーションとデスクトップ同期クライアントは、SSL を使用して Amazon Zocalo に直接ファイルを送信します。Zocalo ユーザーは、所属する組織が RADIUS サーバーをデプロイしていれば、多要素認証（MFA）を使用することもできます。MFA では、ユーザー名、パスワード、RADIUS サーバーによってサポートされている方法が使用されます。サポートされているプロトコルは、PAP、CHAP、MS-CHAPv1、MS-CHAPv2 です。

Zocalo サイトのファイルが保存されている AWS リージョンを選択します。現在、Amazon Zocalo は、米国東部（バージニア）、米国西部（オレゴン）、および欧州（アイルランド）の各 AWS リージョンのリソースで利用可能です。Zocalo に保存されているファイル、コメント、注釈はすべて AES-256 暗号化で自動的に暗号化されます。

付録 – 用語集

AMI: Amazon マシンイメージ（AMI）は、暗号化されたマシンイメージであり、Amazon S3 に格納されています。ここにはあなたのソフトウェアのインスタンスを起動するのに必要なすべての情報が含まれています。

API: アプリケーションプログラミングインターフェイス (API) は、コンピューターサイエンスにおけるインターフェイスで、アプリケーションプログラムがライブラリおよび／またはオペレーティングシステムにサービスをリクエストすることのできる方法を定義します。

Auto Scaling: ユーザーが定義した条件に従って Amazon EC2 のキャパシティーを自動的に拡張または縮小できするようにする AWS サービス。

CIDR ブロック: IP アドレスのクラスなしドメイン間ルーティングブロック。

CloudFormation: ユーザーがアプリケーションを実行するために必要な AWS リソースの基本設定を記録して、規則的かつ予測可能な方法でそれらをプロビジョニングおよび更新できるようにするプロビジョニングツール。

Cognito: **ユーザーの認証、および複数のデバイス、プラットフォーム、アプリケーションにわたるデータの保存、管理、同期を簡素化する** AWS サービスです。これは複数の既存のアイデンティティプロバイダーと連動し、認証されていないゲストユーザーに対応しています。

DynamoDB サービス: AWS マネージド NoSQL データベースサービス。高速で予測可能なパフォーマンスとシームレスなスケーラビリティが特長です。

EBS: Amazon Elastic Block Store (EBS) は、Amazon EC2 インスタンスで使用するためのブロックレベルのストレージボリュームです。Amazon EBS ボリュームは、EC2 インスタンスのライフサイクルから独立して存続するストレージです。

ElastiCache: AWS ウェブサービスの 1 つで、これを使用するとクラウドで分散型インメモリキャッシュ環境を設定、管理、および拡大縮小できます。このサービスは、低速のディスクベースのデータベースに完全に頼る代わりに、高速の管理されたインメモリキャッシングシステムから情報を取得できるようにすることで、ウェブアプリケーションのパフォーマンスを向上させます。

Elastic Beanstalk: 容量のプロビジョニング、負荷の分散、および顧客のアプリケーションの拡大縮小を自動化する AWS 配置および管理ツール。

Elastic IP アドレス: Amazon VPC のすべてのインスタンスに割り当てることができる静的なパブリック IP アドレス。これを割り当てられたインスタンスはパブリックインスタンスになります。Elastic IP アドレスを使用すると、あるインスタンスで障害が発生した場合に、速やかに VPC の別のインスタンスにパブリック IP アドレスを再マッピングすることによって、障害を隠すこともできます。

Elastic Load Balancing: Amazon EC2 インスタンス群のトラフィック管理に使用され、インスタンスへのトラフィックをリージョン内のすべてのアベイラビリティーゾーンに分散します。Elastic Load Balancing にはオンプレミスのロードバランサーという利点のほかに、セキュリティ面でのメリットがいくつかあります。たとえば、EC2 インスタンスから暗号化/復号化の作業を引き継いだり、それをロードバランサーで集中管理したりできます。

Elastic MapReduce（EMR）サービス: Amazon EC2 と Amazon S3 のウェブスケールのインフラストラクチャで実行されているホスト型 Hadoop フレームワークを活用する AWS サービス。Elastic MapReduce では、膨大な量のデータ（ビッグデータ）を簡単に、高いコストパフォーマンスで処理できます。

Elastic Network Interface: Amazon VPC 内では、Elastic Network Interface は、EC2 インスタンスに任意でアタッチできる第 2 のネットワークインターフェイスです。Elastic Network Interface は、管理ネットワークを作成するときや、Amazon VPC でネットワークまたはセキュリティアプライアンスを使用する場合に便利です。これは、簡単にインスタンスからデタッチして別のインスタンスに再アタッチできます。

HMAC-SHA1/HMAC-SHA256: 暗号学では、鍵付きハッシュメッセージ認証コード（HMAC または KHMAC）は、メッセージ認証コード（MAC）の一種であり、暗号化ハッシュ関数とシークレットキーを組み合わせる特定のアルゴリズムを使用して計算されます。他の MAC と同様に、データの完全性とメッセージの信憑性両方を同時に検証するために使用できます。SHA-1 または SHA-256 といった反復暗号化ハッシュ関数は、HMAC の計算に使用される場合があります。結果的に生じた MAC アルゴリズムは、状況に応じて HMAC-SHA1 または HMAC-SHA256 と呼ばれます。HMAC の暗号強度は、ベースとなるハッシュ関数、キーのサイズと質、ハッシュ出力ビット長のサイズによって異なります。

IP アドレス: インターネットプロトコル（IP）アドレスは、ノード間の通信にインターネットプロトコルを使用するコンピュータネットワークに参加するデバイスに割り当てられる、数字で構成されるラベルです。

IP スプーフィング: 偽のソース IP アドレスを使用して IP パケットを作成することをスプーフィング（なりすまし）と呼びます。送信者の身元を隠す、または別のコンピューティングシステムになりすますことを目的としています。

Identity and Access Management（IAM）: AWS IAM を使用すると、お客様の AWS アカウント内に複数のユーザーを作成し、ユーザーごとにアクセス許可を管理することができます。

Import/Export サービス: ポータブルストレージデバイスを安全な AWS ファシリティに物理的に発送することによって AWS S3 または EBS ストレージに大量のデータを転送するための AWS サービス。

Mobile Analytics: モバイルアプリケーションの使用状況データを収集、視覚化、把握するための AWS サービス。これを使用すると、顧客の行動を追跡したり、メトリックスを集計したりできるほか、お客様のモバイルアプリケーションにおける特徴的なパターンを特定できます。

Multi-Factor Authentication (MFA): 複数の認証要素の使用。認証要素には、お客様が知っているもの（パスワードなど）とお客様が持っているもの（ランダムに番号を生成するトークンなど）があります。AWS IAM では、ユーザー名やパスワードといった認証情報に加えて 6 桁のワンタイムコードを使用できます。このワンタイムコードは、物理的に所有している認証デバイス（物理的なトークンデバイスまたはスマートフォンからの仮想トークン）から取得します。

Relational Database Service (RDS): この AWS サービスを使用すると、リレーショナルデータベース（DB）のインスタンスを作成し、関連付けられているコンピューティングリソースとストレージ容量がアプリケーションの要求に応じて柔軟に拡大縮小されるように設定できます。Amazon RDS は、MySQL、Oracle、または Microsoft SQL Server データベースエンジンに使用できます。

Route 53: 開発者がパブリック DNS 名を管理するために使用できる更新メカニズムを提供する「権威ある（authoritative）DNS」システム。コンピュータが相互に通信できるようにするため、DNS クエリに応答し、ドメイン名を IP アドレスに変換します。

Secure Sockets Layer (SSL): アプリケーション層でインターネット経由の通信に対してセキュリティを提供する暗号プロトコル。TLS 1.0 プロトコル仕様も SSL 3.0 プロトコル仕様も、暗号メカニズムを使用して、セキュリティで保護された TCP/IP 接続を確立および維持するセキュリティサービスを実装します。接続をセキュリティで保護すると、傍受、改ざん、またはメッセージの偽造を防ぐことができます。AWS エンドポイントには HTTP または SSL を使用する HTTP（HTTPS）を介して接続できます。

Security Token Service (STS): AWS STS API は、セキュリティトークン、アクセスキー ID、およびシークレットアクセスキーで構成される一時的なセキュリティ認証情報を返します。STS を使用して、一時的にお客様のリソースにアクセスする必要のあるユーザーにセキュリティ認証情報を発行できます。このようなユーザーの例としては、既存の IAM ユーザー、AWS を利用していないユーザー（フェデレーティッドアイデンティティ）、システム、またはお客様の AWS リソースにアクセスする必要のあるアプリケーションなどがあります。

Simple Data Base (SimpleDB): AWS ユーザーがウェブサービスリクエストを通してデータアイテムを保存およびクエリできる非リレーショナル型のデータストア。Amazon SimpleDB は、地理的に分散した場所でデータの複数のレプリカを自動的に作成、管理し、高可用性とデータの堅牢性を可能にしています。

Simple Email Service (SES): ビジネスおよび開発者を対象としたスケーラブルな一括および取引電子メール送信サービスを提供する AWS サービス。送信者の電子メールの配信可能性と信頼性を最大限に高めるため、Amazon SES は疑わしいコンテンツが送信されるのを防止する予防措置を講じます。これにより、ISP はこのサービスを信頼できる電子メールの送信元とみなします。

Simple Mail Transfer Protocol (SMTP): IP ネットワークを介して電子メールを転送するためのインターネット標準。Amazon Simple Email Service では SMTP が使用されています。Amazon SES を使用するユーザーは SMTP インターフェイスを使用して電子メールを送信できますが、TLS を介して SMTP エンドポイントに接続する必要があります。

Simple Notification Service (SNS): クラウドからの通知の設定、操作、および送信を簡単にするウェブサービス。Amazon SNS には、開発者がアプリケーションからメッセージを発行し、すぐに加入者または他のアプリケーションに配信できる機能があります。

Simple Queue Service (SQS): AWS のスケーラブルなメッセージキュー管理サービス。これを使用すると、分散しているアプリケーションコンポーネント間のメッセージベースの非同期通信が可能です。コンポーネントは、コンピューターまたは Amazon EC2 インスタンスまたは両者の組み合わせである場合があります。

Simple Storage Service (Amazon S3): この AWS サービスを使用すると、オブジェクトファイルを安全に保存できます。オブジェクトへのアクセスをファイルレベルまたはバケットレベルで制御でき、リクエスト IP ソースやリクエスト時間などの追加の条件を設定してアクセスをさらに制限できます。AES-256 暗号化を使用してファイルを自動的に暗号化することもできます。

Simple Workflow Service (SWF): 分散しているコンポーネント間で作業を調整するアプリケーションを構築することができる AWS サービス。Amazon SWF を使用すると、開発者はさまざまな処理ステップを 1 つのアプリケーションに「タスク」として組み込むことができ、各タスクは分散アプリケーションとして動作します。Amazon SWF は、開発者のアプリケーションロジックに従ってタスク実行の従属関係、スケジューリング、および同時実行を管理することで、これらのタスクを調整します。

Storage Gateway: VMware ESXi Hypervisor を実行しているデータセンター内のホストにデプロイしている VM を使用して、お客様の業務用のソフトウェア機器を Amazon S3 ストレージに安全に接続する AWS サービス。データはお客様の業務用ストレージのハードウェアから AWS に SSL 経由で非同期的に転送され、Amazon S3 に AES-256 を使用して暗号化されて保管されます。

Transcoder: メディアファイル(音声または動画)を別の形式、サイズ、または品質にトランスコード(変換)するシステム。Amazon Elastic Transcoder は、動画ファイルのトランスコードを容易にする、スケーラブルでコスト効果に優れたサービスです。

Transport Layer Security (TLS): アプリケーション層でインターネット経由の通信に対してセキュリティを提供する暗号プロトコル。Amazon Simple Email Service(SES)を使用していたお客様は、SMTP エンドポイントに TLS 経由で接続する必要があります。

Virtual Private Cloud (VPC): 独自の IP アドレス範囲の選択、サブネットの定義、およびルーティングテーブルやネットワークゲートウェイの設定など、AWS クラウドの独立したセクションをプロビジョニングできるようにする AWS サービス。

WorkSpaces: お客様のユーザーのためにクラウドベースのデスクトップをプロビジョニングするための、AWS マネージドデスクトップサービス。ユーザーは、一連の一意の認証情報または通常使用する Active Directory 認証情報を使用してサインインできます。

X.509: X.509 は、暗号化におけるシングルサインオンおよび権限管理基盤(PMI)のための公開鍵基盤(PKI)の規格です。X.509 では、公開鍵証明書、証明書失効リスト、属性証明書、および認証パス検証アルゴリズムの標準形式が規定されています。AWS 製品には、特定のインターフェイスにアクセスするため、シークレットアクセスキーの代わりに X.509 証明書を使用するものもあります。例えば、Amazon EC2 はクエリインターフェイスにアクセスするためにシークレットアクセスキーを使いますが、SOAP インターフェイスやコマンドラインインターフェイスにアクセスする場合には、署名証明書を使います。

Zocalo: ユーザーのコラボレーションに役立つフィードバック機能を備えた、AWS マネージドエンタープライズストレージおよび共有サービス。

アーカイブ: Amazon Glacier 内のアーカイブは、お客様が保存しておきたいファイルであり、Amazon Glacier 内のストレージの基本単位です。写真、動画、ドキュメントなどのあらゆるデータをアーカイブにすることができます。各アーカイブには一意の ID が割り当てられており、必要に応じて説明が付けられています。

アイデンティティプール: Amazon Cognito 内にある、お客様の AWS アカウントに固有のユーザーアイデンティティ情報のストア。アイデンティティプールは IAM ロールを使用します。IAM ロールとは、特定の IAM ユーザーまたはグループに関連付けられていない、ロールで定義されている AWS リソースにアクセスするための認証に必要な一時的なセキュリティ認証情報を使用するアクセス権限です。

アイデンティティプロバイダー: サービスまたは他の連動するサービスの利用を希望するユーザーの識別情報を発行するオンラインサービス。主なアイデンティティプロバイダーには、Facebook、Google、Amazon などがあります。

アクセスキー ID: AWS の各ユーザーを識別するために AWS が配布する文字列。これは英数字のトークンで、各ユーザーのシークレットアクセスキーに関連付けられます。

アクセスコントロールリスト(ACL): オブジェクトやネットワークリソースにアクセスするためのアクセス許可や規則のリスト。Amazon EC2 では、インスタンスのレベルではセキュリティグループが ACL として機能し、特定のインスタンスにアクセスするためのユーザーのアクセス許可を制御します。Amazon S3 では、ACL を使用してバケットまたはオブジェクトへの読み込みアクセスまたは書き込みアクセスをユーザーグループに許可することができます。Amazon VPC では、ACL はネットワークのファイアウォールのように機能し、サブネットレベルでアクセスを制御します。

アベイラビリティーゾーン: Amazon EC2 の場所は、リージョンとアベイラビリティーゾーンから構成されます。アベイラビリティーゾーンとは、それぞれ独立したロケーションであり、他のアベイラビリティーゾーンで発生した障害の影響を受けないように設計されています。同一リージョン内の他のアベイラビリティーゾーンへは、低コスト、低遅延でネットワーク接続できるようになっています。

インスタンス: インスタンスとは仮想化されたサーバーのことであり、仮想マシン(VM)とも呼ばれ、独自のハードウェアリソースとゲスト OS を使用します。EC2 では、インスタンスとは 1 つの実行中の Amazon Machine Image(AMI)のコピーを意味します。

エンドポイント: AWS サービスのエントリポイントである URL です。アプリケーションのデータレイテンシーを減らすために、ほとんどの AWS サービスでリージョンのエンドポイントを選択してリクエストを行うことができます。一部のウェブサービスではリージョンを指定しない一般的なエンドポイントを使用できますが、そのような一般的なエンドポイントはサービスの us-east-1 エンドポイントに解決されます。AWS エンドポイントには HTTP または SSL を使用する HTTP(HTTPS)を介して接続できます。

オブジェクト: Amazon S3 に格納される基本的なエンティティです。オブジェクトは、オブジェクトデータとメタデータで構成されます。データ部分を、Amazon S3 から見ることはできません。メタデータは、オブジェクトを表現する名前と値のペアのセットです。これらには、

キー: 暗号学では、キーとは暗号アルゴリズム(ハッシュアルゴリズム)の出力を決定するパラメータです。キーペアとは、身分を電子的に証明するために使用される 1 組のセキュリティ認証情報であり、パブリックキーとプライベートキーで構成されます。

キー更新: データの暗号化またはリクエストのデジタル署名に使用される暗号キーを定期的に変更するプロセス。パスワードの変更と同じように、キーを更新することにより、何らかの手段で有効なキーを取得した攻撃者が不正にアクセスするリスクが最小限に抑えられます。AWS では、同時に複数のアクセスキーおよび証明書を使用できるため、アプリケーションのダウンタイムを発生させることなく定期的にキーおよび証明書を有効または無効にできます。

クライアント側暗号化: データを Amazon S3 にアップロードする前にクライアント側で行うデータの暗号化。

ゲスト OS: 仮想マシン環境では、単一のハードウェアで複数のオペレーティングシステムを実行できます。これらのインスタンスはそれぞれ、ホストのハードウェアでは 1 つのゲストとみなされ、独自の OS を使用します。

サーバー側の暗号化(SSE): 保管時のデータを自動的に暗号化するための S3 ストレージのオプション。Amazon S3 SSE を使用すると、オブジェクトを書き込む際に追加のリクエストヘッダーを追加するだけで、更新時にデータを暗号化することができます。データが取得されると自動的に復号化が行われます。

サービス: ネットワークを通じて提供されるソフトウェアまたはコンピューティング機能(例: Amazon EC2、Amazon S3)。

シークレットアクセスキー: お客様が AWS アカウントにサインアップするときに AWS がお客様に割り当てるキー。AWS ユーザーが API 呼び出しを行ったりコマンドラインインターフェイスを操作したりするには、それぞれのシークレットアクセスキーとアクセスキー ID を使用する必要があります。ユーザーはシークレットアクセスキーを使用して各リクエストに署名し、それにアクセスキー ID を含めます。お客様の AWS アカウントのセキュリティを確保するため、シークレットアクセスキーにアクセスできるのはキーおよびユーザーの作成時のみです。再度アクセスする必要がある場合に備えて、キーを保存しておいてください(安全な方法で保存しているテキストファイル内など)。

シャード: Amazon Kinesis ストリーム内のデータレコードのグループ。これらは一意に識別されます。Kinesis ストリームは複数のシャードで構成され、各シャードが容量の 1 単位になります。

シングルサインオン: 1 回ログインするだけで複数のアプリケーションおよびシステムにアクセスできる機能。安全なシングルサインオン機能は、一時的なセキュリティ認証情報を AWS マネジメントコンソールに渡す URL を作成することによって、フェデレーティッドユーザー(AWS ユーザーと AWS を利用していないユーザー)に提供できます。

ステートフルファイアウォール: コンピューターの世界では、ステートフルファイアウォール(ステートフルパケットインスペクション(SPI)またはステートフルインスペクションを実行する任意のファイアウォール)とは、それを通過する(TCP ストリーム、UDP 接続などの)ネットワーク接続の状態を記録するファイアウォールのことです。

スナップショット: Amazon S3 に保存されている EBS ボリュームの顧客主導型バックアップ、または Amazon RDS に保存されている RDS データベースの顧客主導型バックアップ。スナップショットは、新しい EBS ボリュームまたは Amazon RDS データベースの開始点として使用できるほか、データを長期保存および復旧用として保護するためにも使用できます。

セキュリティグループ: セキュリティグループを使用して、お客様の Amazon EC2 インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲を制御できます。つまり、これはお客様のインスタンスのファイアウォールルールを定義するものです。これらのルールは、どのインバウンドネットワークトラフィックがお客様のインスタンスに配信されるべきかを指定します(例: ポート 80 のウェブトラフィックを受け入れる)。

デジタル署名: デジタルメッセージまたはドキュメントの信憑性を示すための暗号方法。有効なデジタル署名は、そのメッセージが認可された送信者によって作成されたものであり、転送中に改変されていないこと確信するための理由を受信者に示します。デジタル署名は認証プロセスの一部として、AWS API へのリクエストに署名する目的でユーザーが使用します。

ネットワーク ACL: Amazon VPC 内のサブネットのすべてのインバウンドトラフィックおよびアウトバウンドトラフィックに適用されるステートレスのトラフィックフィルタ。ネットワーク ACL には順序付けされたルールが含まれており、これらのルールを使用して IP プロトコル、サービスポート、および送信元/送信先 IP アドレスに基づいてトラフィックを許可または拒否できます。

ハードウェアセキュリティモジュール(HSM): HSM は、不正使用防止策の施されたハードウェアデバイスで安全に暗号キーを保存および操作できるようにするアプライアンスです。HSM は暗号キーデータを安全に保存し、アプライアンスの暗号境界の外側からは見えないようにキーデータを使用できるように設計されています。AWS CloudHSM サービスを使用すると、HSM アプライアンスへの専有の、シングルテナントアクセスを利用できます。

ハードウェア専有インスタンス: ホストのハードウェアレベルで物理的に切り離されている Amazon EC2 インスタンス。たとえば、シングルテナントのハードウェアで実行されます。

ハイパーバイザ: 仮想マシンモニター（VMM）とも呼ばれるハイパーバイザは、コンピュータソフトウェア/ハードウェアプラットフォーム仮想化ソフトウェアであり、1 台のホストコンピュータ上で、複数のオペレーティングシステムを同時に稼動させることができるようにするものです。

ハッシュ: AWS API へのリクエストに署名するためのデジタル署名を計算するには、暗号ハッシュ関数が使用されます。暗号ハッシュは、入力に基づいて一意のハッシュ値を返す一方向関数です。ハッシュ関数に渡される入力データとしては、リクエストのテキスト、およびシークレットアクセスキーが該当します。ハッシュ関数から返されるハッシュ値をリクエストに署名として含めます。

バージョニング: Amazon S3 の各オブジェクトにはキーとバージョン ID があります。同じキーのオブジェクトは、バージョン ID が異なっていても、同じバケットに格納できます。バージョニングは、バケット層で有効で、PUT Bucket のバージョニングを使用します。

バケット: Amazon S3 に格納されるオブジェクトのコンテナ。すべてのオブジェクトはバケット内に格納されます。たとえば、photos/puppy.jpg という名前のオブジェクトが johnsmith バケットに格納される場合、URL http://johnsmith.s3.amazonaws.com/photos/puppy.jpg を使ってアドレス解決することができます。

ピア接続: VPC ピア接続は、プライベート IP アドレスを使用して 2 つの VPC 間でトラフィックをルーティングすることを可能にするネットワーク接続です。どちらの VPC のインスタンスも、同じネットワーク内に存在しているかのように、相互に通信できます。

ファイアウォール: 特定のルールに従って入力/出力ネットワークトラフィックを制御するハードウェアまたはソフトウェアコンポーネント。Amazon EC2 のファイアウォールルールを使用して、インスタンスにアクセスするためのプロトコル、ポート、およびソース IP アドレス範囲を指定します。これらのルールは、どの着信ネットワークトラフィックがインスタンスに配信されるべきかを指定します（例：ポート 80 のウェブトラフィックを受け入れる）。Amazon VPC は完全なファイアウォールソリューションをサポートしているため、インスタンスのインバウンドトラフィックとアウトバウンドトラフィックの両方をフィルタできます。デフォルトのグループでは、同じグループ内の他のメンバーからの着信通信、および任意の宛先への発信通信が有効になっています。トラフィックは、IP プロトコル、サービスポート、ソース／宛先 IP アドレス（個別 IP またはクラスなしドメイン間ルーティング（CIDR）ブロック）で制限できます。

フェデレーションユーザー: 現在、お客様の AWS サービスにアクセスする権限はないが、お客様が一時的にアクセス権を付与するユーザー、システム、またはアプリケーション。このアクセスは、AWS Security Token Service（STS）の API を使用して提供されます。

ボールト: Amazon Glacier では、ボールトはアーカイブを保存するためのコンテナです。ボールトを作成する際には、名前を指定し、ボールトの作成先となる AWS リージョンを選択します。ボールトリソースには、それぞれ一意のアドレスが割り当てられています。

ポートスキャニング: コンピュータネットワークサービスはそれぞれ「よく知られている」ポート番号に関連付けられており、ポートスキャンとは、コンピュータが提供しているコンピュータネットワークサービスを特定するためにコンピュータへの侵入を試みる攻撃者が一連のメッセージを送信することです。

リージョン: 同じ地域にある AWS リソースのうち、指定されたもの。各リージョンには少なくとも 2 つの Availability Zone があります。

レプリケーション: データベースの第 2 バージョンを維持するためにデータベースからデータを継続的にコピーすること。その主な目的は、障害復旧対策です。複数の AZ を使用して Amazon RDS データベースレプリケーションを行うことができます。MySQL を使用している場合は、リードレプリカを使用できます。

ロール: 別のエンティティに割り当てることができる一連のアクセス許可を持つ AWS IAM のエンティティ。IAM ロールを用いることにより、Amazon EC2 インスタンスで作動しているアプリケーションが、お客様の AWS リソースに安全にアクセスできるようになります。ロールに特定のアクセス許可を付与し、ロールを使用して Amazon EC2 インスタンスを起動します。Amazon EC2 で実行されているアプリケーションの AWS 認証情報管理は EC2 が自動的に処理するように設定します。

一時的なセキュリティ認証情報: AWS サービスへの一時的なアクセスを提供する AWS の認証情報。一時的なセキュリティ認証情報は、AWS サービスと、自身の ID および承認システムの非 AWS ユーザーの間の ID フェデレーションを提供するために使用できます。一時的なセキュリティ認証情報は、セキュリティトークン、アクセスキー ID、およびシークレットアクセスキーから成ってます。

仮想 MFA: トークン/fob からではなく、スマートフォンから 6 桁のワンタイム MFA コードを取得する機能。MFA では、ユーザー名とパスワードと共に追加要素(ワンタイムコード)を認証に使用します。

仮想インスタンス: AMI が起動されると、結果的に生じる実行システムがインスタンスとして参照されます。同一の AMI を基にするすべてのインスタンスは、完全に同じものとして開始しますが、インスタンスが終了または失敗する場合、それらに関する情報は失われます。

仮想プライベートネットワーク (VPN): インターネットなどのパブリックネットワーク上の 2 か所の間にプライベートのセキュリティで保護されたネットワークを作成する機能。AWS のユーザーは、Amazon VPC とデータセンター間の IPsec VPN 接続を追加することができ、実質的にデータセンターがクラウドに拡張されると同時に、Amazon VPC のパブリックサブネットのインスタンスがインターネットに直接アクセスできるようになります。この構成では、自社のデータセンター側に VPN アプライアンスを追加します。

拠点ホスト: 攻撃に持ちこたえられるよう特別に設定されているコンピュータ。通常は非武装地帯(DMZ)の外側(パブリック側)あるいはファイアウォールの外側に配置します。Amazon EC2 インスタンスは、Amazon VPC の一部としてパブリックサブネットを設定することで SSH 拠点としてセットアップできます。

最終更新日などのデフォルトのメタデータや、Content-Type などの標準 HTTP メタデータが含まれます。開発者が、オブジェクトの格納時にカスタムメタデータを指定することもできます。

準仮想化: コンピューターの世界では、準仮想化とは仮想化技術の 1 つであり、ベースとするハードウェアのソフトウェアインターフェイスに近いが、全く同一ではない、仮想マシンに対するソフトウェアインターフェイスを表わしています。

署名: デジタル署名のこと。デジタルメッセージの正統性を確認するための数学的な手段です。AWS は、暗号アルゴリズムで計算された署名とお客様のプライベートキーを使用して、お客様が Amazon のウェブサービスに送信したリクエストを認証します。

証明書: 一部の AWS 製品で、AWS アカウントおよびユーザーの認証に使用する認証情報。X.509 証明書とも呼ばれます。証明書はプライベートキーと組み合わせられます。

直接接続サービス: 高スループットの専用接続を使用して、内部ネットワークと AWS リージョンとの間の直接接続をプロビジョニングできるようにする Amazon サービス。この専用接続があれば、ネットワークパスのインターネットサービスプロバイダをバイパスして、AWS クラウド（たとえば Amazon EC2 や Amazon S3）への論理接続を直接確立することができます。

認証: 認証とは、誰か、または何かが、実際に申告された通りのものであるかどうか決定するプロセスのことです。認証を受ける必要があるのはユーザーだけではなく、AWS API で公開されている機能を呼び出すプログラムもすべて認証を受ける必要があります。AWS では、すべてのリクエストを暗号ハッシュ関数を使用してデジタル署名することで認証する必要があります。

認証情報: ユーザーまたはプロセスが、サービスへのアクセスを認可されるための認証プロセスで、AWS サービスに確認するために所有する必要のある項目。AWS 認証情報には、パスワード、シークレットアクセスキー、X.509 証明書、多要素トークンなどがあります。

木構造ハッシュ: 木構造ハッシュは、メガバイトサイズごとのデータセグメントについてハッシュを計算することによって生成されるもので、常に拡大するデータの隣接セグメントを表すために木形式のハッシュを結合します。Glacier は、ハッシュをデータと照らし合わせてチェックし、途中で変更されていないことを確認します。

最終版（2014 年 6 月）からの変更

- セキュリティ責任分担モデルの更新
- AWS アカウントのセキュリティ機能の更新
- サービスのカテゴリに基づく再編成
- 新機能によるサービスの更新: CloudWatch、CloudTrail、CloudFront、EBS、ElastiCache、Redshift、Route 53、S3、Trusted Advisor、WorkSpaces
- Cognito のセキュリティの強化
- Mobile Analytics のセキュリティの強化
- Zocalo のセキュリティの強化

最終版（2013 年 11 月）からの変更

- リージョンの更新
- 新機能によるサービスの更新: CloudFront、DirectConnect、DynamoDB、EBS、ELB、EMR、Glacier、IAM、OpsWorks、RDS、Redshift、Route 53、Storage Gateway、VPC
- AppStream のセキュリティの強化
- CloudTrail のセキュリティの強化
- Kinesis のセキュリティの強化
- WorkSpaces のセキュリティの強化

最終版（2013 年 5 月/6 月）からの変更

- IAM にロールと API アクセスを組み込むために更新
- API アクセスの MFA をユーザー指定の特権アクションに対応するように更新
- SQL Server 2012 にイベントの通知、マルチ AZ、SSL を追加するために RDS を更新
- デフォルトで複数の IP アドレス、静的ルーティング VPN、VPC を追加するように VPC を更新
- その他のサービスを次の新しい機能で更新: CloudFront、CloudWatch、EBS、ElastiCache、Elastic Beanstalk、Route 53、S3、Storage Gateway
- Glacier セキュリティを追加
- Redshift のセキュリティの強化
- Data Pipeline セキュリティを追加
- Transcoder セキュリティを追加
- Trusted Advisor セキュリティを追加
- OpsWorks セキュリティを追加
- CloudHSM セキュリティを追加

最終版（2011 年 5 月）からの変更

- サービス固有のセキュリティに対するインフラストラクチャをよりよく識別するために再編
- 統制環境の概要を AWS コンプライアンスプログラムに変更
- 情報通信を管理と通信に変更
- 従業員ライフサイクルを論理的アクセスに変更
- 構成管理を変更管理に変更
- 環境保全セクションと物理的セキュリティセクションを統合
- バックアップセクションの情報を、S3、SimpleDB、および EBS セクションに組み込み

- SAS70 の SSAE 16 への名前変更、および FedRAMP の追加を反映するために証明書を更新
- 安全なネットワークアーキテクチャー、およびネットワークの監視と保護を追加するために、ネットワークセキュリティセクションを更新
- ロール/キーのプロビジョニング、仮想 MFA、一時的なセキュリティ認証情報、シングルサインオンを組み込むために IAM を更新
- リージョンに新しいリージョンと GovCloud の説明を盛り込むために更新
- サービスとセキュリティの説明を明確にするために EBS、S3、SimpleDB、RDS、および EMR を更新
- 設定オプション、VPN、Elastic Network Interface 追加するために VPC を更新
- Amazon Direct Connect のセキュリティセクションの追加
- Amazon Elastic Load Balancing のセキュリティの追加
- AWS Storage Gateway のセキュリティの追加
- AWS Import/Export のセキュリティの追加
- Auto Scaling のセキュリティの追加
- Amazon DynamoDB のセキュリティの追加
- Amazon ElastiCache のセキュリティの追加
- Amazon Simple Workflow Service（Amazon SWS）のセキュリティの追加
- Amazon Simple Email Service（Amazon SES）のセキュリティの追加
- Amazon Route 53 のセキュリティの追加
- Amazon CloudSearch のセキュリティの追加
- AWS Elastic Beanstalk のセキュリティの追加
- AWS CloudFormation のセキュリティの追加
- 用語集の更新

最終版（2010 年 8 月）からの変更

- AWS Identity and Access Management（AWS IAM）の追加
- Amazon Simple Notification Service（SNS）のセキュリティの追加
- Amazon CloudWatch のセキュリティの追加
- Auto Scaling のセキュリティの追加
- Amazon Virtual Private Cloud（Amazon VPC）の更新
- コントロール環境の更新
- リスク管理の削除（別のホワイトペーパーで詳述）

最終版（2009 年 6 月）からの変更

- 主な改訂

最終版（2009 年 6 月）からの変更

- SAS70 を反映する、『証明書と認定』の項に対する変更
- Amazon Virtual Private Cloud (Amazon VPC) の追加
- 『セキュリティ証明書』の項に追加を行い、AWS 多要素認証とキーローテーションについて説明
- Amazon Relational Database Service (Amazon RDS) のセキュリティを追加

最終版（2008 年 9 月）以降の変更

- セキュリティ設計の原則の追加
- 物理的セキュリティ情報の更新と、身元調査の追加
- Amazon EBS に関連する内容を明確化するため、『バックアップ』の項を更新
- 『Amazon EC2 のセキュリティ』の項を更新して以下を追加：
- 証明書ベースの SSHv2
- 複数層のセキュリティグループと図
- ハイパーバイザーの説明とインスタンス分離の図
- 障害分離
- 設定管理の追加
- 『Amazon S3』の項を更新し、内容をさらに詳しく明確化
- 『ストレージデバイスの廃棄』を追加
- 『Amazon SQS のセキュリティ』を追加
- 『Amazon CloudFront のセキュリティ』を追加
- 『Amazon Elastic MapReduce のセキュリティ』を追加

通知