



Amazon Web Services: セキュリティプロセスの概要

2009 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 (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。また顧客に、様々な種類のアプリケーションを構築することのできる柔軟性を提供します。当社の顧客システムやデータの機密性、完全性、可用性を保証することは、AWS にとって、信頼性を維持することと同様に最大の重要事項です。本ドキュメントは、例えば「私のデータの安全性を、AWS はどのように確保しているのか」といった疑問に答えることを目的としています。特に、AWS が管理するネットワークとインフラ、及び各サービス固有のセキュリティ実装について、物理的、または運用上のようなセキュリティプロセスが存在するかについて記述しています。

本ドキュメントは、AWS に関連する以下の領域について、セキュリティの概要を提供します。

認証と認定

セキュリティ設計の原則

物理的セキュリティ

バックアップ

ネットワークセキュリティ

- Amazon Virtual Private Cloud (Amazon VPC)

AWS のセキュリティ

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

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

- Amazon SimpleDB のセキュリティ

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

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

- Amazon CloudFront のセキュリティ

- Amazon Elastic MapReduce のセキュリティ

- Amazon アカウント セキュリティ証明書

認証と認定

Amazon Web Services は、Auditing Standards No.70(SAS70) Type II の監査を取得しています。またその独立監査人から、公正かつ高い評価を得ています。SAS70 は、サービスプロバイダー等の組織が持つ(コントロールオブジェクトやコントロールアクティビティなどの)内部統制に関して、入念な監査を行なったことを証明するものです。AWS の場合、これはサービス遂行方法や顧客データを守るためのセキュリティに関連しています。AWS は安全で、ワールドクラスのクラウドコンピューティング環境を提供するというそのコミットメントを実証するために、最も厳格な産業認証を取得する

努力を続けています。

さらに、AWS プラットフォームが提供する柔軟性と顧客によるコントロールによって、ある産業特有の認証要件に適合するソリューションを構築することができます。例えば、HIPAA に準拠する医療用アプリケーションを、AWS 上で構築されたお客様がいらっしゃいます。

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います。これには、当社内部の AWS セキュリティチームによる公式設計レビュー、脅威モデリング、リスク査定の実行、静的コード分析、さらに厳選された業界専門家により何度も繰り返される侵入テストなどが含まれています。当社のセキュリティリスク査定の実行は、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続きます。

物理的セキュリティ

AWS 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による手段を用いて、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。権限のあるスタッフでも、データセンターのフロアへのアクセスには2要素認証を最低2回行う必要があります。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せん。

AWS だけが、業務上このような特権を必要とする従業員や契約業者に対して、データセンターへのアクセスや情報を提供できます。従業員がこれらの特権を必要とする作業を完了したら、たとえ彼らが引き続き 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。

AWS は、顧客データにアクセスする可能性のあるスタッフに、その肩書きやデータへのアクセスレベルに応じて、(法律の許す範囲で)綿密な身元調査を実施しています。AWS は、あなたの機密性のあるデータのセキュリティとプライバシーが、あなたにとって最も重要な関心事であることを理解しています。

バックアップ

Amazon S3、Amazon SimpleDB、または Amazon Elastic Block Store に保存されるデータは、冗長化のため自動的に複数の物理的ロケーションで保存されます。これによる追加費用はかかりません。Amazon S3 および Amazon SimpleDB は、最初の書き込み時に複数のデータセンターで複数回オブジェクトを保存し、記憶デバイスが利用不能になる際、またはビット崩壊時にさらに複製を行なうことによって、オブジェクトの堅牢性を保証しています。Amazon EBS の複製は、同一の Availability Zone 内に保存され、複数のゾーンにまたがって保存されることはありません。その

ため、更に長期的なデータ堅牢性を保証するために、Amazon S3 へ定期的にスナップショットを作成することを強く推奨します。Amazon EBS のスナップショットは、ファイルシステムを停止することなく取得可能です。これは Amazon EBS でデータベースを利用している人々にとっては重要な機能です。尚、Amazon EC2 で実行中のインスタンスの仮想ディスク上で管理されるデータのバックアップを、お客様が知らないところで AWS が実行することはありません。

ネットワークセキュリティ

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提供しており、お客様はさらに堅牢な保護を行なうことができます。以下はいくつかの例です：

分散サービス妨害(DDoS)攻撃： Amazon のアプリケーション プログラミング インターフェース(API)エンドポイントは、大規模、インターネットスケール、ワールドクラスのインフラストラクチャであり、Amazon を世界最大のオンライン小売業者としたエンジニアリング技術と、同じエンジニアリング技術を利用することが出来ます。特許取得済みの、DDoS 緩和技術も適用されています。さらに、AWS のネットワークは、複数のプロバイダにまたがるマルチなアクセス環境を構成しており、多様なインターネットアクセスに対応しています。

中間者 (MITM) 攻撃： 全ての AWS API は、サーバー認証による SSL 保護されたエンドポイント経由で利用する事ができます。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。その後顧客は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、最初にインスタンスにログインする前にホスト証明書へアクセスすることができます。顧客は、AWS とのやりとりすべてにおいて SSL を使用することを推奨されています。

IP スプーフィング： Amazon EC2 インスタンスは、偽装されたネットワークトラフィックを送信できません。AWS の管理してい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は、それ自身以外のソース IP または MAC アドレスを有するトラフィックの送信をインスタンスに許可しません。

ポートスキャンング： Amazon EC2 の顧客による許可のないポートスキャンは、Amazon EC2 が許可する利用ポリシー(AUP)に違反します。AUP の違反は深刻に受け止められ、報告されたあらゆる違反は調査されます。違反の疑いを発見した場合、以下の URL から報告を行なうことができます。

<http://aws.amazon.com/contact-us/report-abuse/>

許可のないポートスキャンングが検出された場合、それは停止されてブロックされます。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。なぜなら、Amazon EC2 インスタンスの全入力ポートはデフォルトで閉じられており、顧客のみが開くことができるからです。

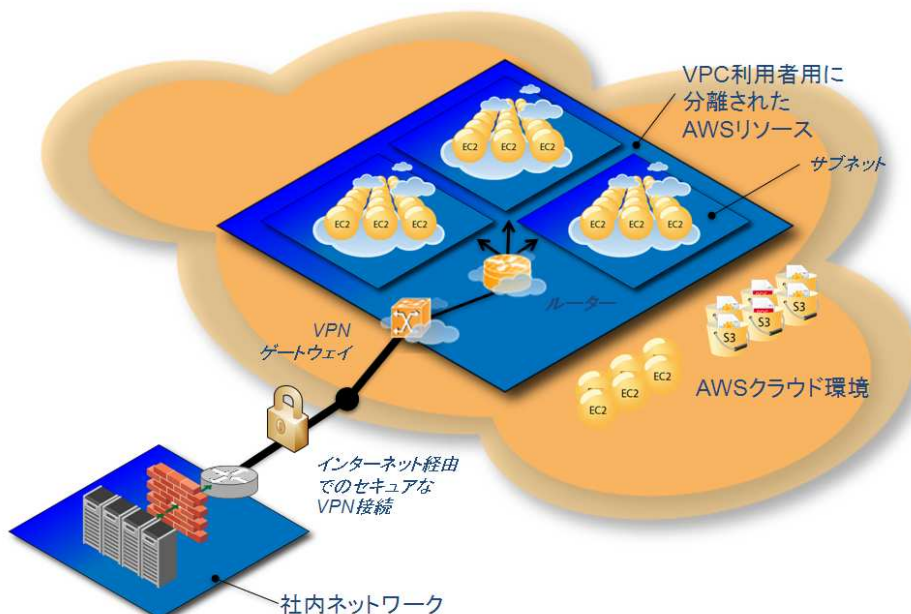
顧客がセキュリティグループを厳格に管理することによって、ポートスキャンの脅威をさらに緩和することができます。顧客が外部から特定のポートへのトラフィックを許可するようにセキュリティグループを設定した場合、その特定のポ

ートは、ポートスキャンに対して脆弱になります。これらの場合、顧客は適切なセキュリティ手段を講じて、アプリケーションにとって重要なリスニングサービスを、未許可のポートスキャンに発見されることから保護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を保証する責任を有しています。

第三者によるパケットスニффイング: 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したり「傍受」することは不可能です。顧客が自らのインターフェースを無差別モードにすることはできますが、ハイパーバイザーが宛先でないインスタンスにトラフィックを伝送することはありません。物理的に同一のホスト上に位置する、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 cache poisoning のような攻撃は、Amazon EC2 内では機能しません。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。

Amazon Virtual Private Cloud (Amazon VPC)

Amazon Virtual Private Cloud (Amazon VPC) は、企業の既存の IT インフラと AWS クラウドをつなぐ、安全かつシームレスなブリッジです。Amazon VPC では、企業の既存インフラを、AWS 内の特別なエリアのコンピュータリソースに Virtual Private Network (VPN) 接続経由で接続し、企業が持つセキュリティサービス、ファイアウォール、侵入検知システムなどの既存の管理機能を AWS リソースにまで拡張します。Amazon VPC では現在 Amazon EC2 が統合されています。将来的には、その他の AWS サービスとも統合される予定です。



顧客が持つ IP アドレスを適用し、業界標準の暗号化された IPsec VPN を使い、全ネットワークトラフィックのルーティングを行なうことによって、Amazon VPC と顧客のデータセンター間でのエンド・ツー・エンドでの (外部とは) 隔離された接続を提供します。これによって、顧客は既存のセキュリティインフラストラクチャを活用することができます。Amazon VPC についての詳細は、AWS ウェブサイト (<http://aws.amazon.com/vpc/>) でご確認ください。

設定管理

既存の AWS インフラストラクチャに対する緊急、非定期的、その他の設定の変更は、こうしたシステムで適用される業界基準に従って、認定、記録、テスト、承認を経て、文書化されます。AWS のインフラストラクチャに対する更新は、このように顧客や彼らのサービスの利用に影響を与えない方法で実施されます。サービスに影響がでる可能性がある場合は、E メールまたは AWS Service Health Dashboard (<http://status.aws.amazon.com/>) によって、AWS が顧客に通知します。

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

Amazon EC2 のセキュリティは次のような複数のレベルで提供されます: ホストシステムのオペレーティングシステム (OS)、仮想インスタンス オペレーティングシステムまたはゲスト OS、ファイヤウォール、署名された API 呼び出し等。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、安全であるようにすることです。

複数のセキュリティレベル

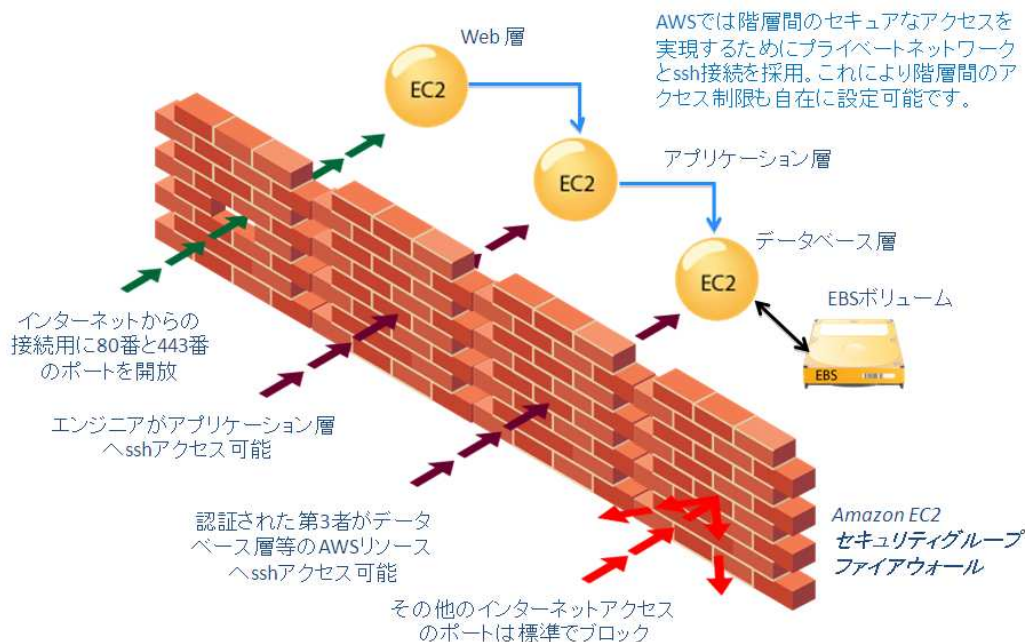
ホストオペレーティングシステム: 管理レベルにアクセスする必要がある作業を担当する管理者は、Multi-Factor Authentication (多要素認証) を使用して専用の管理ホストにアクセスする必要があります。これらの管理ホストは、特別に設計、構築、設定されており、クラウドの管理レベル保護機能を強化したシステムです。これらのアクセスは全て記録され、監査されます。管理レベルにアクセスする必要がある作業を従業員が完了すると、これらのホストと関連するシステムへの特権とアクセス権は取り消されます。

ゲストオペレーティングシステム: 仮想インスタンスは、顧客によって完全に管理されます。顧客は、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有しています。AWS は、顧客インスタンスに対するアクセス権を有しておらず、ゲスト OS にログインすることはできません。AWS はセキュリティのベストプラクティスの基本セットを推奨しており、これには次のものがあります: 顧客は自分のホストに対するパスワードを用いたアクセスを無効にすべきです。また、multi-factor authentication (多要素認証) のいくつかの方法を使って、自分のインスタンスにアクセスすべきです。(または少なくとも証明書ベースの SSH バージョン 2 アクセス)。さらに、顧客は、各ユーザー毎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べきです。例えば、ゲスト OS が Linux の場合、それらのインスタンスをさらに堅牢化した後、証明書ベースの SSHv2 を使用して、仮想インスタンスにアクセスし、リモートル

ートログインを無効にし、コマンドラインのロギングを使用し、特権をエスカレーションするために「sudo」を使用すべきです。それらが一意であり、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、顧客は彼ら自身のキーペアを生成すべきです。

ファイヤウォール: Amazon EC2 は、完全なファイヤウォール ソリューションを提供します。この強制インバウンド (mandatory inbound) ファイヤウォールは、デフォルトでは拒否モードに設定されているため、Amazon EC2 の顧客が、インバウンドトラフィックの受け入れに必要な全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、またソース IP アドレス (1つの IP アドレスまたはネットワーク IP レンジ (CIDR ブロック) 指定) 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、異なる規則を適用できるよう、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のみに対して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:



ゲスト OS では、ファイヤウォールはコントロールできません。変更を許可してセキュリティの特別層を追加するには、顧客の X.509 証明書およびキーが必要になります。AWS は、インスタンスとファイヤウォール上の様々な管理機能に対して、詳細なアクセス権を付与する能力をサポートしています。そのため顧客は、職務の分離を通じて、更なるセキュリティ

ィを実施することができます。ファイアウォールによって提供されるセキュリティレベルは、顧客によって、どれだけの期間、どのような目的でポートが開かれるかによって異なります。デフォルトでは、全インバウンドトラフィックを拒絶するモードです。顧客は彼らが何を開き、彼らのアプリケーションをいつ構築してセキュリティで保護するのか、注意深く計画すべきです。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、インスタンス毎に必要です。

AWS はさらに、IPtable または Windows Firewall と IPsec などの、ホストベースのファイアウォールを有する、インスタンス毎のその他のフィルタを顧客が採用することを推奨しています。これにより、各インスタンスについて、インバウンドおよびアウトバウンドトラフィックの両方を制限することができます。

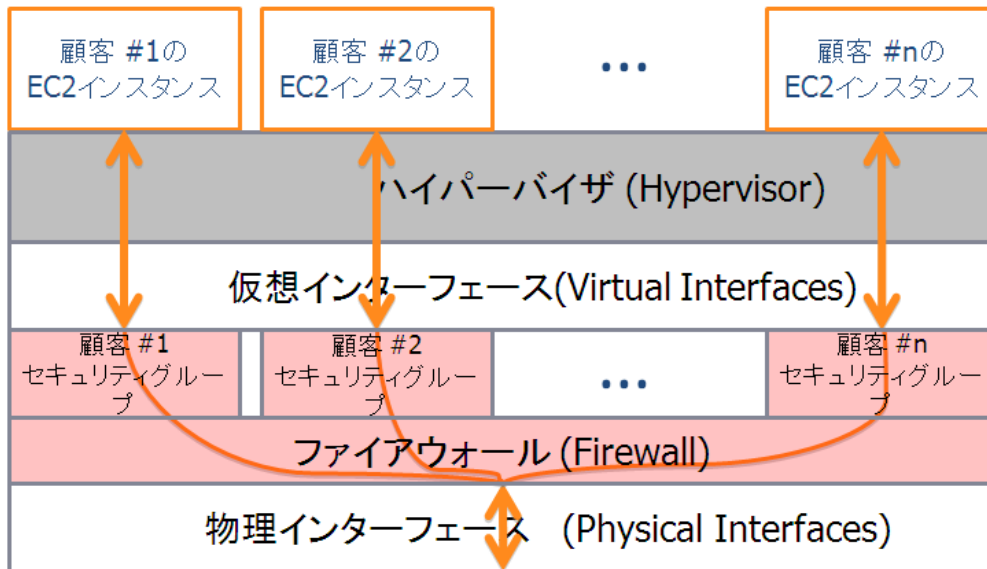
API: インスタンスの起動と終了、ファイアウォールパラメータの変更、その他の機能の実行のための呼び出しは、すべて X.509 証明書または顧客の Amazon 秘密アクセスキーによって署名します。顧客の秘密アクセスキーまたは X.509 証明書へアクセスしない場合、Amazon EC2 API 呼び出しをその目的のために行なうことはできません。さらに、API 呼び出しは、SSL で暗号化して、機密性を維持することができます。Amazon は、常に SSL で保護された API エンドポイントを使用することを推奨しています。

ハイパーバイザー

Amazon EC2 は現在、(Linux ゲストの場合)準仮想化(paravirtualized)の利点を生かすため、Xen ハイパーバイザーの極めてカスタマイズされたバージョンを活用しています。準仮想化されたゲストが、特権的なアクセスを必要とするオペレーションへ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もちません。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 を実行します。しかし、ほとんどのオペレーティングシステムが行なうようにリング 0 で実行するのではなく、ゲスト OS は、より権限の少ないリング 1 で実行を行い、アプリケーションは最も権限の少ないリング 3 で実行を行ないます。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

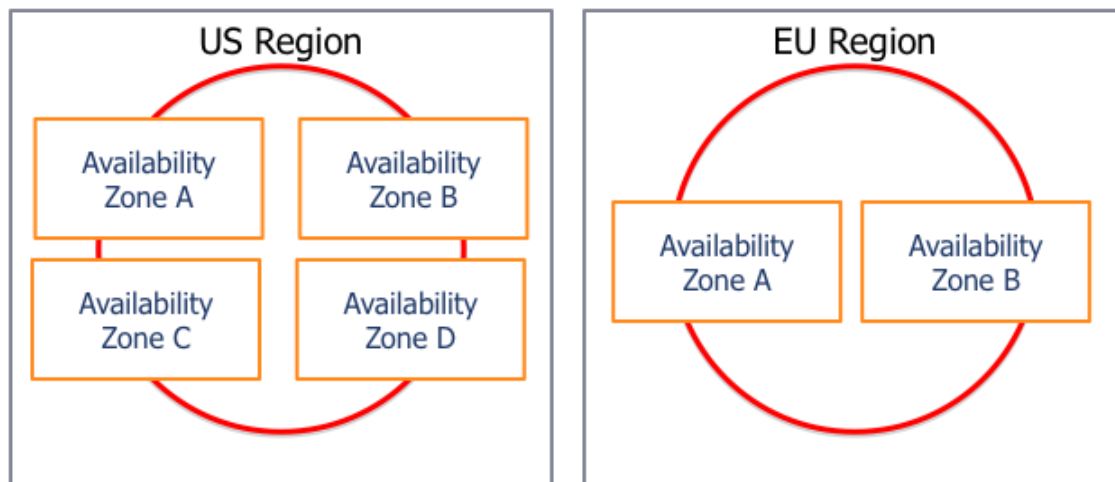
同一の物理マシン上で実行中の異なるインスタンスは、Xen ハイパーバイザーを経由して互いに分離されます。Amazon は、Xen コミュニティで積極的に活動しており、これによって最新の開発事項にいち早く対応することができます。さらに、AWS ファイアウォールは、物理的ネットワークインターフェイスとインスタンスの仮想インターフェイスの間にある、ハイパーバイザー層の中に存在しています。全パケットはこの層を通過しなければなりません。こうして、インスタンス同士が、インターネット上の他のホスト以上に互いにアクセス権を有することはなく、それらがあたかも物理的に分離したホスト上に存在しているかのように扱うことができます。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。特許取得済みの AWS のディスク仮想層は、顧客に使用されるストレージの各ブロックを自動的にリセットします。これによって、1人の顧客のデータが、誤って他者の目に曝されることがないようにになっています。AWS は、顧客が適切な手段をもちいて、彼らの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。

障害分離

Amazon EC2 は、顧客に、インスタンスを複数のアベイラビリティゾーン (Availability Zone) だけでなく、複数の地理的に離れたリージョン (Region) に配置できる柔軟性を提供しています。各アベイラビリティゾーンは、障害分離が可能なようデザインされています。つまり、個々のアベイラビリティゾーンは、一般的な都市地域内で物理的に分離されており、地震や洪水での影響が同時に及ばないような場所が考慮されています。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、さらに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なっています。これらはすべて、冗長的に、複数の Tier-1 プロバイダに接続されています。



同一リージョン内における、アベイラビリティゾーン間のプライベートネットワークでのトラフィックは、AWS が管理するインフラストラクチャを経由しますが、リージョン間の全通信は一般的なインターネットインフラストラクチャを経由するため、重要なデータは適切な暗号化手段を使用して保護すべきであるにご注意ください。また、顧客によって積極的にそのようになされない限り、データは地域間で複製されません。

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

共有されたストレージシステムにおいて、よく見られるセキュリティに関する質問は、未許可のユーザーが意図的に、または誤って情報にアクセスすることができるかということです。AWS 内に格納されている情報をどのように、いつ、誰に対して開示するか決定する柔軟性を顧客が有することができるようにするために、Amazon S3 API は、バケットおよびオブジェクトの両方のレベルのアクセスコントロールを提供します。これらはデフォルトでは、バケットおよび/またはオブジェクトの作成者によって権限を付与されたアクセスのみを許可するよう設定されています。顧客が彼らのデータに対して匿名のアクセス権を付与しない限り、ユーザーがデータにアクセスできるようになるための最初のステップは、ユーザーのプライベートキーを使用して、リクエストの HMAC-SHA1 署名を利用する認証を行なうことです。認証されたユーザーは、アクセスコントロールリスト (ACL) でオブジェクトレベルの読み取り権限を付与された場合に限り、オブジェクトの読み取りを行なうことができます。認証されたユーザーは、ACL でバケットレベルの読み取りと書き込み権限を付与された場合に限り、キーをリストアップし、バケットのオブジェクトを作成または上書きすることができます。バケットおよびオブジェクトレベル ACL は独立しています。オブジェクトはそのバケットから ACL を継承しません。バケットまたはオブジェクト ACL の読み込みまたは修正に対する許可は、既定で作成者のみのアクセス権が設定されている ACL によってコントロールされます。そのため、顧客は彼らのデータに誰がアクセスするのかについて完全なコントロールを維持します。AWS アカウント ID、Eメール、または DevPay 商品 ID を使用して、顧客は彼らの Amazon S3 データに対するアクセス権を、他の AWS ユーザーに付与することができます。顧客はまた、彼らの Amazon S3 データに対するアクセス権を、全 AWS ユーザーまたは(匿名アクセスを有効にしている)すべての人に付与することができます。

データ管理

セキュリティを最大化するために、SSL エンドポイント経由で Amazon S3 にアクセスすることができます。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。これによって、AWS の内部と外部とのやりとりの双方で、データを安全に転送することができるようになっています。

データを保護するほかの方法には、物理的セキュリティやデータの暗号化があります。『物理的セキュリティ』の項で詳細に説明されているように、Amazon は複数層の物理的セキュリティ手段を採用して、顧客データを安全に保ちます。例えば、Amazon S3 データセンターに対する物理的アクセスは、監査リストに記載された Amazon の担当者に制限されています。重要なデータの暗号化は一般的に、セキュリティ上の優れた手法です。Amazon は、ユーザーが重要なデータを Amazon S3 にアップロードする前に、それらを暗号化することを推奨しています。

オブジェクトが Amazon S3 から削除される場合、オブジェクトに対するパブリック名からのマッピング削除は直ちに行なわれます。また一般的には、数秒以内に分散システムで処理されます。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。

ストレージデバイスの廃棄

ストレージデバイスが製品寿命に達した場合、AWS の処理手順には、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 Sanitation”: 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手法をもちいて、廃棄プロセスの一環としてデータを破棄します。

Amazon SimpleDB セキュリティ

Amazon SimpleDB API は、ドメインコントローラによって認証されたアクセスのみを許可する、ドメインレベルのコントロールを提供します。これによって顧客は、自分のデータにアクセスする者に対して完全なコントロールを維持することができます。

Amazon SimpleDB へのアクセス権は、AWS アカウント ID に基づいて付与することができます。認証されると、利用者は全ユーザーオペレーションに対して完全なアクセス権をもちます。独立した各ドメインに対するアクセスは、認証済みユーザーを彼らが所有するドメインにマッピングする、独立したアクセスコントロールリスト(ACL)によってコントロールされます。

Amazon SimpleDB は、SSL 暗号化されたエンドポイント経由でアクセス可能です。暗号化されたエンドポイントは、インタ

一ネットと Amazon EC2 内の両方からアクセス可能です。Amazon SimpleDB 内に保管されたデータは、AWS によって暗号化されません。しかし顧客はデータを Amazon SimpleDB にアップロードする前に、それらを暗号化することができます。暗号化された属性は、Get オペレーションの一部としてのみ、取得可能です。クエリフィルタリングの条件の一部として、それらを使用することはできません。Amazon SimpleDB へ送信する前に暗号化することによって、AWS を含む第三者が、顧客の重要なデータにアクセスできないようになります。

Amazon SimpleDB データ管理

ドメインが Amazon SimpleDB から削除される場合、ドメインマッピングの削除は直ちに開始されます。そして、一般的には数秒以内に分散システムで処理されます。マッピングが削除されると、削除されたドメインに対するリモートアクセスは存在しなくなります。

ドメイン内でアイテムと属性データが削除されると、ドメイン内のマッピング削除は直ちに開始され、一般的には数秒以内に完了します。マッピングが削除されると、削除されたデータに対するリモートアクセスは存在しなくなります。ストレージ領域はその後、書き込みオペレーションのみが可能となり、データは新規に保存されるデータによって上書きされます。

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ー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、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って、あなたのためにデータベースインスタンスを管理します。

Amazon RDS DB インスタンスへのアクセスは、Amazon EC2 セキュリティグループと同種のデータベースセキュリティグループ経由で、顧客により管理されます。データセキュリティグループはデフォルトで[すべて拒絶]のアクセスモードに設定されており、顧客はネットワークへのアクセスを個々に承認する必要があります。これを行なうには2つの方法があります - ネットワーク IP レンジの許可、または既存の Amazon EC2 セキュリティグループの許可です。データベース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することなく更新できるので、顧客が彼らのデータベースへのアクセスを、シームレスに制御することができます。

Amazon RDS DB インスタンス 削除 API (DeleteDBInstance)が実行されると、DB インスタンスには、削除のマークがつけます。インスタンスが「削除中」ステータスを示さなくなると、それは削除されていることを意味します。この時点では、インスタンスにアクセスすることはできません。最終スナップショットのコピーを作成しなかった場合、復元することはできません。またツールや API でリストアップされることもありません。

Amazon Simple Queue Service (Amazon SQS) 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。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なうことができます。

Amazon SQS へのアクセスは、AWS アカウント ID に基づいて付与されます。一旦権限を付与されると、ユーザーはすべてのユーザーオペレーションに対して完全なアクセス権をもちます。デフォルトでは、各個別キューに対するアクセスは、それを作成した AWS アカウント ID 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、顧客がキューに対して他者にアクセス権を付与することができます。

Amazon SQS は、SSL 暗号化されたエンドポイント経由でアクセス可能です。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。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。しかし、ユーザーは、データを Amazon SQS にアップロードする前に、それらを暗号化することができます。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それを復号する手段を有していることが条件となります。Amazon SQS へ送信する前に暗号化することによって、AWS を含む第三者が、顧客の重要なデータにアクセスできないようになります。

Amazon CloudFront のセキュリティ

Amazon CloudFront は、そのコントロール API になされる各リクエストが、認証されることを要求します。これによって、認証されたユーザーだけが、彼ら自身の Amazon CloudFront ディストリビューションを作成、修正または削除できるようになります。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 は、SSL 暗号化されたエンドポイント経由でのみアクセスすることができます。

Amazon CloudFront は現在、アクセス制限されていないファイルを伝送するようデザインされています。Amazon CloudFront 経由で伝送されるオブジェクトは、一般的な読み取りアクセスを許可する ACL ポリシーを有する、Amazon S3 に保管される必要があります。同様に、Amazon CloudFront のエッジロケーションには、アクセスコントロールまたは他の認証機能はありません。

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場合があります。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 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。これには例えば、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、あなたの Amazon CloudFront で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するだけです。

Amazon Elastic MapReduce のセキュリティ

Amazon Elastic MapReduce は、その API になされるあらゆるリクエストが認証されることを必要とします。これによって、認証されたユーザーのみが、彼らのジョブフローを作成、検索、終了することができるようになります。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。Amazon Elastic MapReduce は、そのウェブサービス API とコンソールに対するアクセスのために SSL エンドポイントを提供します。

顧客のためにジョブフローを起動する場合、Amazon Elastic MapReduce は、マスターノードの Amazon EC2 セキュリティグループをセットアップして、SSH を経由する外部アクセスのみが可能のようにします。当サービスは、外部アクセスを許可しない、独立したスレーブのセキュリティグループを作成します。顧客の入力および出力データセットを保護するために、Amazon Elastic MapReduce は SSL をもちいて、データを S3 とやりとりします。

Amazon アカウント セキュリティ証明書

AWS は、あなたが自身の ID を確認し、アカウントに安全にアクセスできるよう、様々な方法を提供しています。AWS によってサポートされる証明書の完全なリストは、[Your Account(あなたのアカウント)]の下にある、[Security Credentials (セキュリティ証明書)]のページにあります。AWS はまた、お客様がさらにアカウントを保護してアクセスをコントロールすることができる、その他の2つのセキュリティオプション: Multi-Factor Authentication (多要素認証)とキーローテーションも提供します。

AWS Multi-Factor Authentication (多要素認証)(AWS MFA)

AWS Multi-Factor Authentication (多要素認証)(AWS MFA)は、AWS アカウント設定に拡張されたコントロールを提供する補助的なセキュリティレイヤーです。オプトイン アカウント機能を有効にすると、AWS アカウント設定にアクセスが許可される前に、標準 AWS アカウント証明書に加えて、6桁のワンタイム・コードを提供する必要があります。顧客は彼らの物理的に所有す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。顧客のアカウントへアクセス権が与えられる前に2つの要素が確認されるため、これは Multi-Factor Authentication (多要素認証)と呼ばれています。Amazon E メール ID とパスワード(あなたのご存知の最初の「要素」)および彼らの認証デバイスからの正確なコード(あなたが保有する2番目の「要素」)の両方を提供する必要があります。

サードパーティのプロバイダから認証デバイスを取得し、AWS ウェブサイト経由で使用のためのセットアップを行なうことは簡単です。Multi-Factor Authentication (多要素認証) についての詳細は、AWS のウェブサイト <http://aws.amazon.com/mfa/> でご確認いただけます。

キーローテーション

パスワードを頻繁に変更することが重要であるのと同じ理由で、AWS は、アクセスキーと証明書を定期的にローテーションさせることを推奨しています。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を行なえるよう、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、アプリケーションのダウンタイムなく、定期的にオペレーションの内外でキーと証明書をローテーション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、その情報を漏洩したりするリスクを軽減できます。

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

© 2008–2009, Amazon.com, Inc. およびその関係者本ホワイトペーパーは、情報提供の目的のみのために提供されるものです。Amazon Web Services LLC は、本ホワイトペーパー内で提供される情報に関連するいかなる損害に対しても責任を負うものではなく、これらの情報は明示的、暗示的、または法律上いかなる保証も伴うことなく、「現状のまま」提供されるものです。本ホワイトペーパー内のいかなるものも、Amazon Web Services LLC、その関係者、サプライヤ、またはライセンサーからの保証を行なう、またはそれらを代表するものとはなりません。本ホワイトペーパーは、Amazon Web Services ウェブサイトなど、Amazon Web Services の技術の利用を規定する、適切な利用規約を修正す

るものではありません。本ホワイトペーパーは、本文書の発行日時点での、Amazon Web Services の提供商品を紹介するものであり、これらは事前の通知なく変更される場合があります。