PCI DSSなどのセキュリティ基準を用いてクラウドセキュリティの現状把握や対策立案を支援

パブリッククラウド環境でITシステムをセキュアに構成するためには現状把握が欠かせない。代表的なクラウドサービスであるAWS（Amazon Web Services）環境に対するクレジットカード業界のセキュリティ基準であるPCI DSSを活用したアセスメントサービスを紹介する。

クラウド環境で守るべき情報と保護領域、セグメンテーション方法を確認

クラウド環境でシステムを構築する際のセキュリティ要件として何を拠り所にすれば良いか。多様な基準やガイドが存在するが、その解決策の1つとしてクレジットカード業界のセキュリティ基準であるPCI DSSを用いたアセスメントサービスをお薦めしたい。PCI DSSはクレジットカード情報を保護するための対策が具体的かつ体系的にまとめられ、カード情報を扱うシステムに限らず様々なシステムの現状把握に最適だ。ここでは代表的なパブリッククラウドサービスであるAWS上でのアセスメント観点についてPCI DSSの要件概要と共に説明する。

PCI DSSでは、守るべき情報の流れを識別し、重要な保護領域を特定することをスコーピングと呼ぶ。また、保護領域に対して範囲外の環境からアクセスできないように制限することをセグメンテーションといい、AWSでは3つの手段で実現される。1つ目は課金管理の単位でもあるAWSアカウント分割により、明示的に指定しない限り他のリソースから論理的に分離できる（図1-①）。2つ目はAmazon Virtual Private Cloud（VPC）の機能であるセキュリティグループによりポート、送信元および宛先アドレスに基づいたネットワーク制御が可能である（図1-②）。3つ目はAmazon Simple Storage Service（S3）などのAWSサービスに対するアクセス制御であ

NTTデータ先端技術株式会社
セキュリティ事業本部
セキュリティコンサルティング事業部
チーフコンサルタント　**堀 茂人**氏

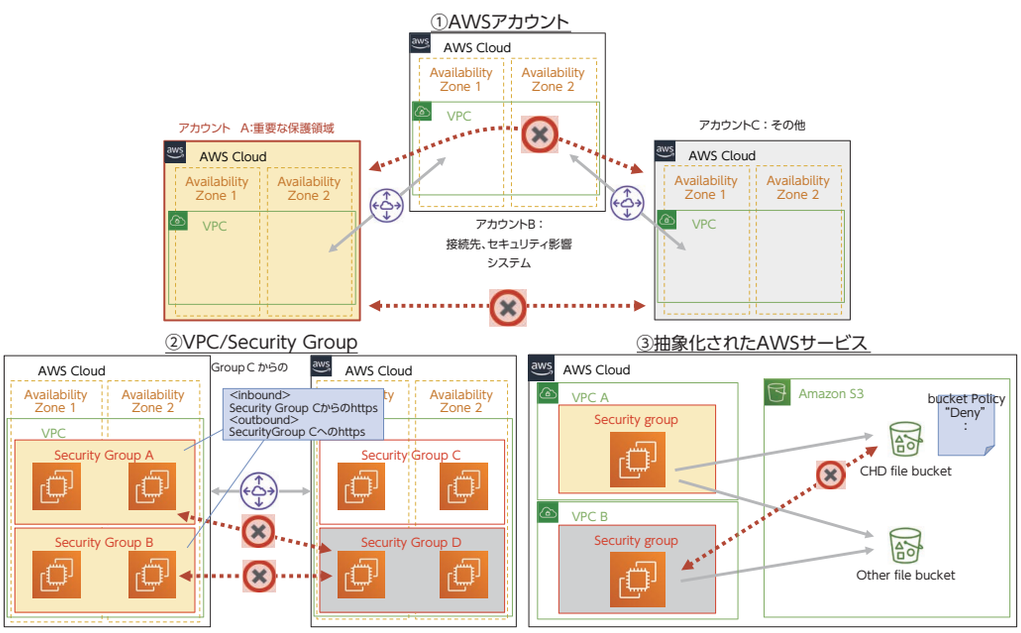

図1　AWSのセグメンテーション設計

る。データ保護やアクセス権設定などの対策は利用者が責任を負うため、提供されるコントロールを用いたアクセス制御が欠かせない（図1-③）。

重要な情報が置かれる内部ネットワークへの直接アクセスを禁止

スコーピングとセグメンテーション状況の確認後、PCI DSS レベルの対策が講じられているか 12 の要件に沿って確認する。要件 1 はファイアウォールを適切に構成して業務上必要な通信に制限することが求められる。セキュリティグループを適用して Public subnet を介さないと Private subnet にアクセスできないよう制限、また S3 のバケットポリシー設定などにより VPC エンドポイント経由でのプライベート接続のみ可能な構成とするなど、重要な情報が置かれるネットワークへのインターネットからの直接アクセスの禁止が必要である（図 2）。要件 2 は、業界で認知されているシステム強化基準（米国の Center for Internet Security が発行する CIS Benchmark など）を用いてシステムをセキュアに構成することが求められる。IaaS サービスである EC2 を用いて構成したインスタンスだけでなく、S3 などの AWS サービスも対象となる。

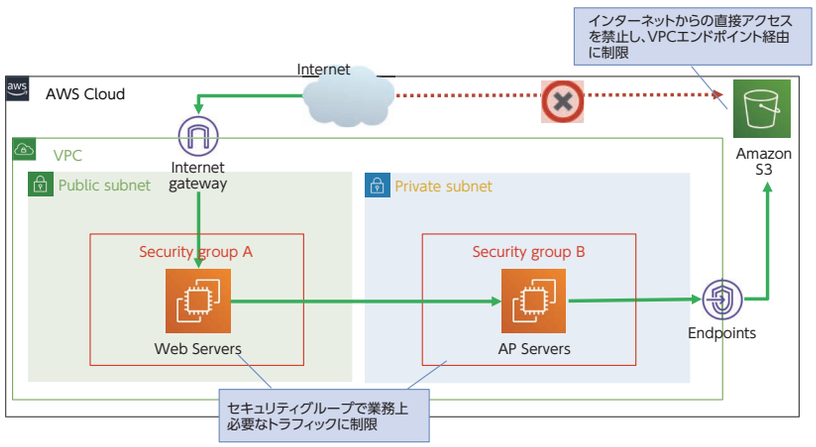

図 2　VPC ネットワークの構成例

重要な情報は暗号化して、厳格な鍵管理プロセスを構築

要件 3 では、守るべき情報は必要最小限とし、暗号化などで保護することが求められる。暗号化の鍵自体を厳格に管理することも求められるが、AWS Key Management Service（KMS）という鍵管理サービスの利用により AWS のセキュアなハードウェア上に保存可能である。ただし、アクセス制御や鍵管理ポリシーの実装は利用者責任であり、鍵管理作業は暗号鍵管理者のみ、暗号化や復号処理はアプリケーションのみとし、他のアクセスは拒否するなど KMS のキーポリシー設定を用いた制限が必要となる（図 3）。要件 4 では、インターネットなどを介して伝送する場合に強力な暗号化方式を用いて保護することが求められる。例えば、Amazon Elastic Load Balancing などで https を構成する場合、tls1.2 などセキュアな設定のみが許可されたポリシーの選択が必要となる。要件 5 では、マルウェアの影響を受けやすいすべてのシステムに対する対策ソフトウェアの導入および適切な管理が求められる。EC2 を用いて構成したインスタンスでは利用者側で適切なソフトウェアの選定が必要となる。要件 6 では、脆弱性管理やセキュアなアプリケーション開発などの対策が求められる。Amazon Inspector による脆弱性の識別、AWS WAF による Web ベースの攻撃からの保護など AWS サービスの活用や、個別に選定した製品を導入し、自分たちで安全なシステムを開発し、保守することが必要となる。

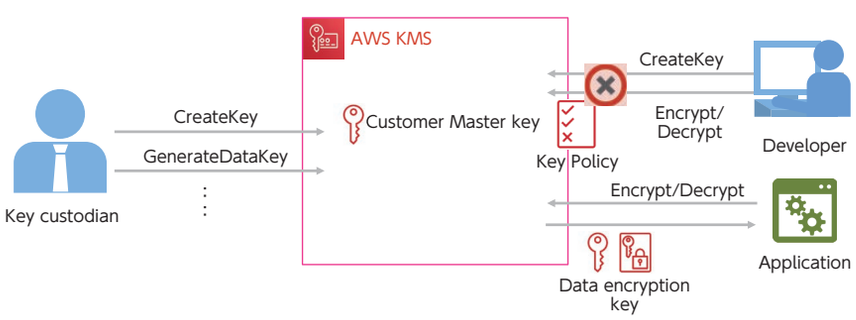

図 3　暗号鍵アクセスの制限

業務に必要な最小権限の割当て、多要素認証など要件に沿った認証ポリシーの構成

要件 7 は職種と職務に基づいた最小限のアクセス権の割当て、要件 8 は一意のアカウントの払出し、パスワードの複雑性などの認証ポリシー構成、

多要素認証の実装などが求められる。AWSではIdentity and Access Management（IAM）によってユーザー・ユーザーグループ・ロールに対して許可または拒否されるアクションやリソースなどのポリシーを設定可能であるが、マネジメントコンソールによるAWSへのアクセス、EC2インスタンスへのログイン手段、AWSサービスやデータベースへのプログラムからの接続方法など各レイヤーで考慮が必要である（図4）。要件9は物理的なセキュリティ対策であり、データセンターのセキュリティなど基本的にはAWSが責任を担うが、AWSに接続される環境の物理セキュリティは利用者側で対策が必要となる。要件10では、各種ログの有効化、要件に沿った適切な保存および監視が求められる。AWSサービスでのアクションを記録するAWS CloudTrail、ネットワークログであるVPCフローログなどのログの洗出し、有効化を行うとともに、ログをS3に集約して保全、Amazon CloudWatch EventsとAWS Lambdaなどを活用した監視ポリシーに基づいた通知や自動復旧の仕組みの実装なども必要となる。要件11では、定期的なセキュリティ診断の実施、侵入検知システムや変更検出メカニズムによる監視などが求められる。AWSから提供される各種サービスや個別に選定した製品により実現する。なお、セキュリティ診断は「侵入テストのAWSカスタマーサポートポリシー」に従って禁止行為などに留意して実施する必要がある。要件12では、AWSを利用する組織の情報セキュリティポリシーの確立と維持が求められる。AWSから提供されるガイダンスなども考慮し、例えばインシデント発生時のAWSからの情報入手手段などを確認しておく必要がある。

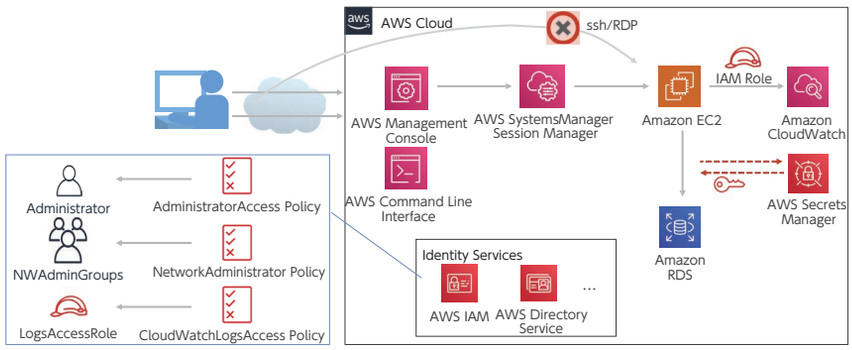

図4　AWSアクセスの構成例

アセスメントや設定診断サービスを活用してクラウドセキュリティの現状把握を

クラウドサービスでは、S3のようなAWSマネージドのサービスであってもアクセス制御などの責任は利用者側にあり、利用者が講ずべきセキュリティ対策の範囲を正確に把握しないと漏れが生じてしまう恐れがある。そこで、今回紹介したPCI DSSなどの基準に基づいたクラウドセキュリティアセスメントサービスにより対象となるクラウド環境のPCI DSSレベルの対策状況についての現状把握が可能である。また当社では、IAMやS3のようなAWSの各サービスの設定について、業界のベストプラクティスがまとめられているCIS Benchmarkを活用して検証するクラウド設定診断サービスを提供している（図5）。本サービスではCIS Benchmarkに基づいて機械的にチェックするだけでなく、CIS Benchmarkの推奨項目でも当該設定が本当に必要かどうかを診断員の眼で分析・提言している。これらのサービスを組み合わせて活用することでクラウド環境の対策状況の見える化を進め、緊急度に応じて段階的に対策を講じていくことをお薦めしたい。

	クラウド設定診断	AWS環境におけるクラウドセキュリティアセスメント
目的	クラウド基盤の基本的なセキュリティ設定状況の確認	セキュリティ基準に基づいた網羅的かつPCI DSSレベルの対策状況確認
基準	CIS（Center for Internet Security）Benchmark	PCI DSS（Payment Card Industry Data Security Standard）
対象	主要なAWSサービス ・IAM ・Storage（S3,EBS）、 ・Logging（CloudTrailなど） ・Monitoring（CloudWatchなど） ・Network（VPC,EC2）	守るべき情報の流れを識別し、対象となる領域（AWSアカウント、VPC、AWSサービス）をスコーピングにより決定
確認方法	CIS Benchmarkから選定した確認項目に基づいてクラウド環境の設定値を検査、セキュリティ上推奨されない問題点を洗出し	PCI DSSに基づいたインタビュー、設計書や設定値の確認により、要件ギャップや追加対策案を抽出

図5　クラウド設定診断とアセスメントサービス