

PCI DSS スコーピングおよび AWS 上でのセグメンテーション のためのアーキテクチャの設計

適切なセグメンテーションコントロールを使用した
適用範囲の特定および最小化

2019年 5月



注意

お客様は、本文書に記載されている情報について、ご自身の評価に基づき判断する責任を負います。本文書は、(a) 情報提供のみを目的としており、(b) 予告なしに変更される可能性のある AWS の現時点での製品と対応を説明するものであり、(c) AWS およびその関連会社、サプライヤー、ライセンサーからの確約や保証を意味するものではありません。AWS の製品やサービスは、明示または黙示を問わずいかなる種類の保証、表明、条件も伴うことなく、「現状のまま」提供されます。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間のいかなる契約の一部も構成するものではなく、また、当該契約が本文書によって変更されることもありません。

目次

要約.....	4
はじめに.....	1
AWS での PCI DSS スコーピングプロセス.....	1
セキュリティ統制.....	2
ソリューションに関する AWS クラウドプラットフォームの考慮事項	3
決定フロー - PCI DSS の適用範囲の識別.....	7
手順 1: CHD フローを識別する	8
手順 2: 環境内にある適用範囲内のリソースをすべて識別する	8
手順 3: システムを分類する	8
手順 4: セグメンテーション境界を設計する	9
クラウドのセグメンテーションの設計.....	10
AWS アカウントレイヤー	10
ネットワーク層 (OSI 第 3~4 層).....	14
アプリケーション層 (OSI 第 7 層)	15
Docker コンテナを活用したワークロードのスコーピングおよびセグメンテーション.....	17
ハイブリッド環境のためのスコーピングガイダンス.....	19
スコーピングおよびセグメンテーションの検証.....	21
予防的な統制.....	22
フィードバックループ	23
まとめ.....	24
執筆者.....	24
詳細情報.....	25
文書改訂.....	25
注記.....	26

要約

本書では、AWS クラウドプラットフォームで動作する PCI (Payment Card Industry) DSS (Data Security Standard) ワークロードの適用範囲を適切に定義する方法と、クラウドネイティブのアマゾン ウェブ サービス (AWS) のサービスを使用して適用範囲内のリソースと適用範囲外のリソースの間にセグメンテーション境界を定義する方法について説明します。

また、PCI DSS v3.2.1¹ の PCI DSS 要件 11.3.4 で規定されている、導入済みのセグメンテーションコントロールを検証する方法についても説明します。本書は、PCI SSC (PCI Security Standards Council) が発行した [Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation](#) に基づいています。

本書はエンジニアやソリューションビルダーを対象としています。また、QSA (Qualified Security Assessor) や ISA (Internal Security Assessor) 向けのガイドとしても利用可能で、AWS プラットフォーム内で利用可能なさまざまなセグメンテーションコントロールや関連するスコーピングの考慮事項をよりよく理解する際に役立ちます。

はじめに

AWS 上のソフトウェアで定義されたネットワーク(SDN)では、アプリケーションのスコーピングプロセスがオンプレミス環境と比較して異なります。AWS で利用可能な追加のセグメンテーションコントロールは、単なるネットワークセグメンテーションにとどまりません。必要なコントロールを実装するためにアプリケーションを慎重に設計し、セキュリティに影響を与えるサービスを選択することで、カード所有者のデータ環境 (CDE) 内のシステムとサービスの数を大幅に削減できます。接続されているシステムやサービスを厳格に制限したり排除したりするには、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを利用して Amazon Virtual Private Cloud (VPC) Security Groups とファイアウォールを組み込んだウェブサービスインターフェイスを適切な粒度で定義します。

AWS での PCI DSS スコーピングプロセス

従来のスコーピングプロセスと同様に、AWS アプリケーションのスコーピングプロセスはカード所有者のデータ (CHD) フローから始まります。²ただし、CHD 向けの多くの通過点が [Amazon API Gateway](#) や [AWS WAF](#) のような特定の目的に特化したサービスであることが、直接的に違います。このようなサービスは明確に定義された接続構成を備え、[AWS PCI DSS レベル 1 サービスプロバイダー評価](#)の一部として評価されています。さらに、このような AWS エンドポイントは、ファイアウォール機能 (AWSのPCI DSS の適用範囲の一部) によって保護された RESTful ウェブサービスインターフェイスであり、CHD を受信しないサービスのセグメンテーション境界として機能します。

一般的な Amazon Elastic Compute Cloud (Amazon EC2) インスタンスには、オンプレミスサーバーよりもはるかに明確に定義されたネットワーク接続があります。EC2 インスタンスは、ルーターやネットワークゲートウェイとしてではなく、スタンドアロンネットワークホストとして扱われます。セキュリティグループは、サブネット間だけでなく、各インスタンスインターフェイスでも動作し、粒度がサブネットレベルである従来のネットワークファイアウォールアプライアンスとは対照的に、粒度がインターフェイスレベルのネットワークルールを提供します。セキュリティグループを使用するネットワーク設定では、インスタンスのネットワーク構成では回避できない粒度の高いネットワークアクセス制御を実施できます。

PCI DSS の適用範囲が AWS プラットフォーム内でどのように展開されるかについては、使用されている AWS のサービスの性質によって異なります。

AWS のサービスは、以下の大きなグループに分類されます。³

- Amazon EC2 インスタンスなどのインフラストラクチャサービス
- Amazon Relational Database Service (Amazon RDS) などのコンテナサービス
- Amazon Simple Storage Service (Amazon S3) などの抽象化されたサービス

最小限の PCI DSS の適用範囲を確立するための戦略は、上記のように 3 つの大きなグループに分類された AWS のサービスをすべて対象としています。また、適用範囲内の PCI DSS ワークロードがオンプレミスのデータセンターと AWS クラウドに分散するハイブリッド環境向けのスコーピングとセグメンテーションの考慮事項にも対応しています。

セキュリティ統制

カード所有者のデータ (CHD) を保存、処理、転送する組織はすべて、通常、アクワイアラー契約により、PCI DSS 要件を満たし、遵守状況を証明する必要があります。サービスプロバイダーの場合、これはお客様の要件である場合があります。

PCI Security Standards Council が管理するこのグローバルセキュリティ標準には、機密性の高いクレジットカード情報を保護するための規範的な IT セキュリティ要件 (コントロールとも呼ばれます) が含まれています。組織は、カード所有者のデータ環境 (CDE) を正しく特定および定義する責任を負います。これは、PCI DSS 評価の適用範囲とも呼ばれます。CDE は、CHD を処理するか、またはセキュリティに影響を与えるため PCI の適用範囲となるような人、プロセス、および技術で構成されていますが、ここでは、CDE の技術的側面の適用範囲のみに焦点を当てます。

セグメンテーション

セグメンテーションは、一般的には *PCI DSS Requirement 0* と呼ばれます。つまり、セグメンテーションは、他の PCI DSS 要件に対処する前に、支払いフローにとって重要なシステムに適用範囲を制限するために最初に使用されます。従来、組織では、PCI DSS の適用範囲の環境を制限し、これを自らの IT インフラストラクチャの他の部分から保護するために、ネットワークのセグメンテーションを重要なコントロール手段として使用していました。このアプローチでは、組織が適用範囲外のインフラストラクチャを保護する必要はないということを意味するものではありません。むしろ、適用範囲外のインフラストラクチャに対するさまざまな検証要件だけでなく、セキュリティ統制の選択においても柔軟性を持たせることが可能です。

[Guidance for PCI DSS Scoping and Network Segmentation](#) では、PCI DSS の適用範囲に関して、IT インフラストラクチャとリソースを以下のセグメントに分類しています。

- **CDE システム:** このようなシステムコンポーネントは、CHD または機密性の高い認証データ (SAD) を格納、処理、または送信します。これらは PCI DSS の適用範囲内にあって、他のリソースに適用範囲を広げる傾向があります (つまり、該当の CDE システムと通信するすべてのリソースも適用範囲内のシステムになります)。
- **接続先システムやセキュリティに影響を与えるシステム:** このようなシステムコンポーネントは、CDE システムに対し、制限付きで直接的または間接的に接続し、CDE システムにある種の管理サービスおよびセキュリティサービスを提供します。これらは、1 つ以上の PCI DSS 要件を満たしたり、セグメンテーション境界を確立したりする際にも役立ちます。このようなシステムは適用範囲内にありますが、接続の観点のみから言うと他のリソースに適用範囲を広げることはありません。
- **適用範囲外のシステム:** このようなシステムコンポーネントは上記の基準を満たしておらず、CDE システムのセキュリティまたは設定には影響を与えません。また、適用範囲に含まれることもありません。

ソリューションに関する AWS クラウドプラットフォームの考慮事項

AWS クラウドプラットフォームには、スケーラビリティ、使い捨て可能なリソース、トレーサビリティ、セキュリティ統制の自動化、継続的な検証やテストといった、一定の特性があります。これらの独自の特性に加えて、Operating Expenditure (OPEX) モデルなどのさまざまなビジネス上の利点があるため、ほとんどの組織でクラウドの採用が有益なものとなります。⁴ クラウドのメリットは、このようなクラウド固有の特性を利用して決済アプリケーションのインフラストラクチャを設計することで実現されます。

責任共有モデル

セキュリティとコンプライアンスは AWS とお客様の間で責任を共有します。この責任共有モデルでは、ホストオペレーティングシステムや仮想化レイヤーからサービスが動作する施設の物理的セキュリティに至るまで、AWS がコンポーネントを運用、管理、制御するので、お客様の運用上の負担を軽減できます。主に、AWS はクラウドのセキュリティに責任を持ち、お客様はクラウド内のデータの機密性、完全性、可用性を保護し、情報保護に関する特定のビジネス要件を満たす責任を負います。

コンプライアンスを推進する前に、[責任共有モデル](#)を理解しておく必要があります。共有される責任は、特定の AWS のサービスに関して組み込まれた抽象化の状況によって異なります。サービスの抽象化は、ユーザーの責任に反比例します。自らの環境で使用されているすべてのサービスを必ず評価して、サービスの使用による PCI DSS の適用範囲全体に及ぶ影響を理解してください。このアプローチは、コンプライアンス上の義務を果たすために何をすべきかを正確に理解する際に役立ちます。AWS では、Service Adoption Framework (SAF) を採用して AWS の各サービスを正式に評価し、組織のセキュリティ要件やコンプライアンス要件に従って、決定プロセスや必要なコントロールを文書化することを推奨しています。

従来のネットワーク管理の仮想化

レイヤー 2 ネットワークはエンドユーザーに対して透過的であるため、AWS では VLAN のような従来のオンプレミスネットワーク管理が異なる方法で実装されています。AWS のネットワークは、従来のネットワーク構造を模倣した Software Defined Network (SDN) です。

AWS プラットフォーム内では、Amazon Virtual Private Cloud (Amazon VPC) は AWS クラウドの論理的に隔離されたセクションを表し、仮想ネットワーク内でリソースを起動することができます。さらに、類似した機能を提供するリソース、または類似した適用範囲にあるリソースが、冗長性を提供する異なるアベイラビリティゾーンを横断する複数のサブネットに広がっていることも一般的です。したがって、VPC とサブネットは、セグメンテーションコントロールというよりもグループ化の構成要素になります。

伸縮性

コンピューティングやストレージなどのアプリケーションに割り当てられた AWS リソースは、要求に応じて水平方向に拡張できます。[AWS Auto Scaling](#) はアプリケーションを監視し、計算能力を自動的に調整して、安定した予測可能なパフォーマンスを可能な限り低いコストで維持します。このような AWS リソースは一時的なもので、短期間で終了するものです。AWS Lambda や Application Load Balancer (ALB) のような他の AWS マネージドサービスは、リソース要件に合わせて垂直方向に拡張されます。設計するセグメンテーションコントロールは、クラウド環境の弾力的で一時的な性質に対応できなければなりません。このようなコントロールは、インフラストラクチャの変更時にも適切な状態を維持できるように設計します。そうしないと、適用範囲の定義が適切でなくなる可能性があります。

抽象化されたサービスと API ベースのインフラストラクチャ

多くの AWS 製品はマネージドサービスとして提供されます。つまり、AWS がインフラストラクチャを管理します。このようなサービスのうち、抽象化された AWS のサービスはウェブサービス API 呼び出しを介してのみ通信します。

ウェブサービス API は、認証、承認、データの整合性などの他のコントロールに加えて、固有のネットワークセグメンテーションコントロールを使用します。これにより、許可されたエンティティからのデータのみが呼び出し側システムとサービスとの間で確実に交換されます。設計上、このような抽象化されたサービスは、明示的に許可されない限り、サービスの異なるインスタンス間でデータを共有できないように保護されています。このようなサービスは、アクセス制御された API を介して、同種のサービスやその他のサービスと通信します。この構成はサービスの一部として提供され、ファイアウォールによって実現されるレイヤー 3~4 ネットワーク制御に適合します。全体的な責任共有モデルの一部として、アプリケーション層ベースのセグメンテーションおよびトラフィックフィルタリング制御を設計する必要があります。

可能であれば、アプリケーションの機能と制御にはウェブ API または疎結合なサービスを使用します。例えば、オープンな TCP/IP 接続を維持するエージェントではなく、ログデータを転送するためにウェブ API 呼び出しを行う、[Amazon CloudWatch](#) のようなログ統合サービスを選択します。

自動化

自動化を使用すると、ほとんどのインフラストラクチャとアプリケーションの変更を手動の作業なしで実装できます。これにより、俊敏性が提供され、変更管理プロセスが分散化され、デプロイメントプロセスが迅速化されます。インフラストラクチャおよびアプリケーション変更管理とともにセグメンテーションコントロールが適用されるように、可能な限りこのセグメンテーションコントロールを自動化する必要があります。そのような方法では、適切な適用範囲の境界が維持されます。自動化は、手動チェックを排除することにより、セグメンテーションコントロールが変更されたとき、およびコントロールを強化したり、変更の原因と結果を分析するためにほぼリアルタイムで誰かに警告するなど、適切な修正手順を実装できるタイミングを検出するのにも役立ちます。

ハイブリッドインフラストラクチャ

組織が AWS クラウドプラットフォームにワークロードを移行する際には、一定期間ハイブリッドインフラストラクチャを稼働させる場合があります。つまり、オンプレミスのデータセンターと AWS クラウドプラットフォームの両方でワークロードが実行されている可能性があります。セグメンテーションコントロールでは、このハイブリッドインフラストラクチャ、およびオンプレミスと AWS クラウドプラットフォーム間の通信を考慮する必要があります。

決定フロー - PCI DSS の適用範囲の識別

決定フローは、組織内の PCI DSS の適用範囲を正しく識別する際に役立ちます。このプロセスは、組織環境内の CHD のフローを正しく識別することから始まります。

CHD フローを正しく識別したら、次の手順は、環境内にある適用範囲内のリソースをすべて識別することです。

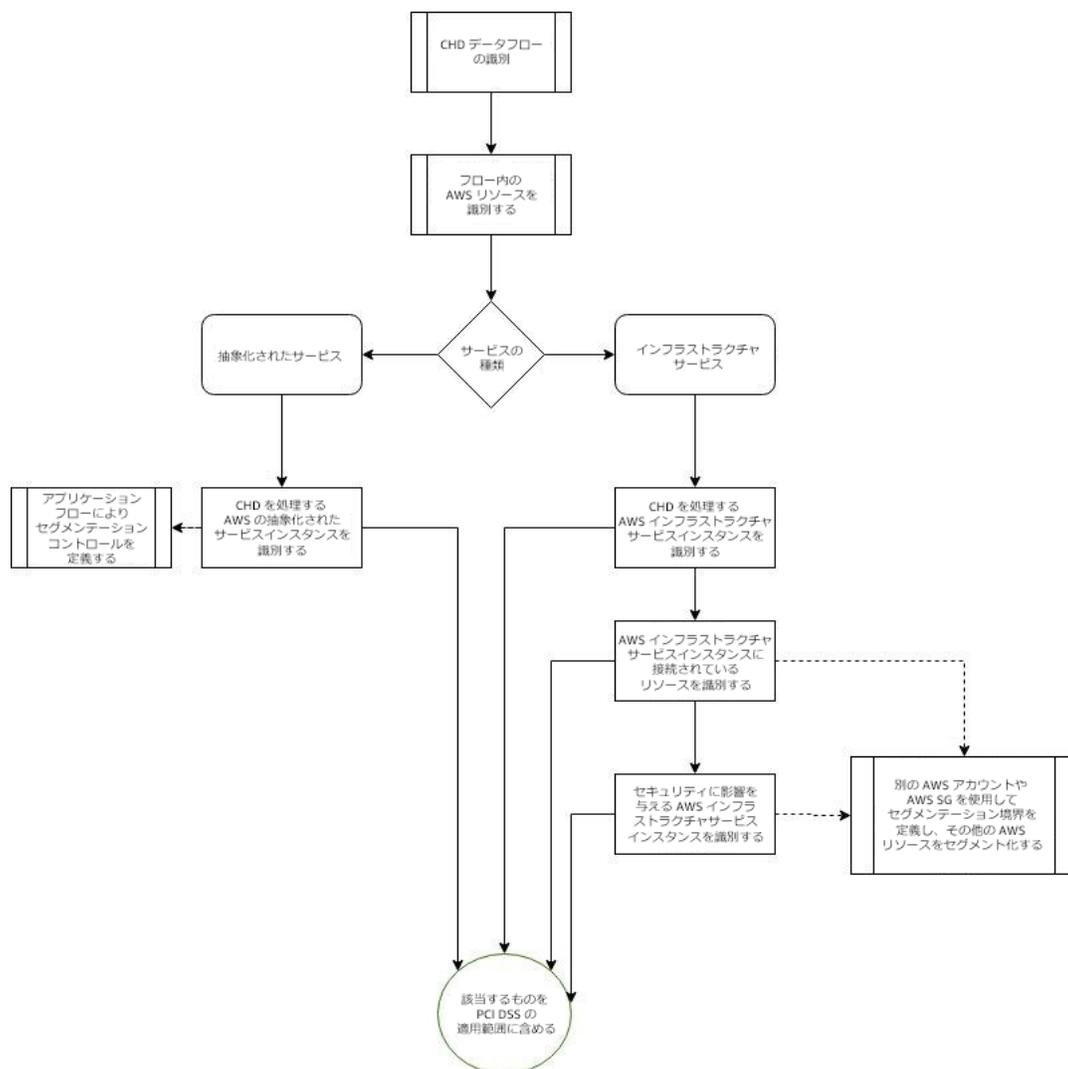


図 1: PCI DSS の適用範囲と関連するセグメンテーション境界を正しく識別するための決定フロー

上の図は、PCI DSS の適用範囲を正しく識別するために従う必要がある決定フローを示しています。また、他の AWS リソースを適用範囲内のリソースから分離し、PCI DSS の適用範囲を最小限に抑えるため

に、フローのさまざまな段階でセグメンテーション境界を正しく定義する際にも役立ちます。

手順 1: CHD フローを識別する

PCI DSS の適用範囲やセグメンテーション境界を設計するプロセスを開始する前に、組織内の CHD フローを正確に理解しておく必要があります。CHD フローを正しく識別するには、組織内で CHD のライフサイクル全体を識別して定義する必要があります。これには、環境内での CHD の利用または入力の経路、その後の CHD の処理および保管、そして最終的には環境からの CHD の安全な破棄、無価値化、または移動までが含まれます。

手順 2: 環境内にある適用範囲内のリソースをすべて識別する

CHD フローを構成するさまざまな種類の AWS リソースを識別します。このようなリソースは、CHD を受信、処理、保存、または送信するためのリソースです。ISA と QSA が監査を行う際に、どのようなサービスに評価を制限すべきかを明確に理解できるようにするためには、分析の一環として、何が適用範囲内で何が適用範囲外かを定義することが重要です。

手順 3: システムを分類する

この手順では、抽象化されたサービスとインフラストラクチャサービスにシステムを分類します。このようなリソースの適用範囲の識別とセグメンテーションは、さまざまな種類の接続に基づいて行われます。インフラストラクチャサービスは主にネットワーク (OSI 第 3~4 層) 接続を介して相互に通信しますが、抽象化されたサービスの唯一の通信形式は、何らかの形式の API (OSI 第 7 層) を介して確立されたデータ接続です。

このような異なる種類の AWS リソースを識別した後で、PCI DSS の正確な適用範囲を識別することができます。

抽象化されたサービス

AWS の抽象化されたサービスの場合、適用範囲内のリソースは、サービスへのアクセスに使用される AWS のサービスのエンドポイントではありません。適用範囲内の唯一のリソースは、CHD を処理する AWS のサービスの特定のインスタンス化です。例えば、組織で多数の Amazon DynamoDB テーブルをプロビジョニングしている場合、テーブルのサブセットのみが CHD の保存/処理に使用されます。この場

合、CHD を格納するために使用されている RDS テーブルのみが組織の PCI DSS の適用範囲に入ります。

コンテナ化されたサービス

抽象化されたサービスと同様に、コンテナ化されたサービスのエンドポイントは PCI DSS の適用範囲に含まれません。CHD を処理するサービスのインスタンス化は適用範囲内に含まれます。ただし、インスタンス化は追加のレイヤーを含めることができます。例えば、RDS インスタンスに複数のテーブルがあり、その一部のみが CHD を処理する場合があります。このようなテーブルは、テーブルが存在する RDS スキーマの適用範囲内にあります。これは、抽象化されたサービスの場合、プラットフォーム (この場合は RDS インスタンスのデータベースプラットフォーム) のセキュリティはお客様が責任を負うためです。

インフラストラクチャサービス

インフラストラクチャサービスの場合、適用範囲の識別プロセスには追加の手順が含まれます。CHD を処理する AWS リソースを識別するだけでなく、接続先と、セキュリティに影響を与える AWS リソースも識別する必要があります。例えば、CHD を処理するウェブサービスを実行している EC2 インスタンスは、明らかに適用範囲内にあります。ただし、このインスタンスによって、CHD 以外のデータレポートを取得するためのネットワーク接続を持つレポートサーバーなど、他の接続先リソースが適用範囲に含まれる場合があります。また、セキュリティに影響を与える他の AWS リソースも適用範囲に含めることができます。これには、認証および認可サービスを提供するディレクトリリソースが含まれる可能性があります。

手順 4: セグメンテーション境界を設計する

適用範囲内の AWS リソースがすべて識別されたら、その他の AWS リソースがすべて適切にセグメント化され、PCI DSS スコープから除外されるように、セグメンテーション境界を設計します。AWS の抽象化されたサービスの場合、このセグメンテーションは主に、CHD のフローを制御するアプリケーションや関連するアプリケーションコードによって制御されます。アプリケーションレベルのセグメンテーションと連携するインフラストラクチャベースのリソースの場合は、ネットワークレベルのセグメンテーションも設計する必要があります。

クラウドのセグメンテーションの設計

このセクションでは、クラウド機能を使用してクラウドサービスを保護し、徹底した防御を実現するという原則に基づいて設計可能な各種のセグメンテーション境界について説明します。このような境界を AWS プラットフォームのさまざまなレイヤーで実現し、それぞれを互いに組み合わせることによって、セキュアで機能的な CDE に必要な PCI DSS の適用範囲内のシステムを最小限の規模で実現できます。

セグメンテーションは PCI DSS の要件ではありませんが、セグメンテーションを使用すると、PCI の適用範囲をできるだけ少ないリソースに制限できます。PCI DSS の適用範囲内のリソースを特定した後にセグメンテーション境界を設計し、PCI DSS の適用範囲外のシステムが正しく分離されるようにします。

AWS アカウントレイヤー

個々の AWS アカウントは、AWS プラットフォームで実現可能な最上位レベルのセグメンテーション境界を提供します。設計上、AWS アカウント内でプロビジョニングされたすべてのリソースは、他の AWS アカウントでプロビジョニングされたリソース (お客様自身の [AWS Organizations](#) 内リソースも含む) から論理的に隔離されます。PCI ワークロード用に隔離したアカウントを使用することは、AWS で動作する PCI アプリケーションを設計する際の最も重要なベストプラクティスであり、オンプレミスでの実装では達成できない高いレベルのセキュリティを実現します。

適用範囲内のリソースと適用範囲外のリソースを複数の AWS アカウントに分割することで、PCI DSS の範囲を縮小できます。これにより、論理アカウントレベルの隔離は別々の AWS アカウントのリソース間に明示的な通信チャネルを確立することによってのみ変更できるため、偶発的な適用範囲の変更が発生するのを防ぐことができます。また、このアプローチは、適用範囲外の AWS アカウントのアーキテクチャやコントロールに対する変更が他の AWS アカウントの適用範囲内リソースのセキュリティに悪影響を与えないようにすることにより、影響を軽減する際にも役立ちます。以下の図は、PCI DSS の適用範囲の設計に関する AWS マルチアカウントアーキテクチャとして提案可能な一例を示しています。

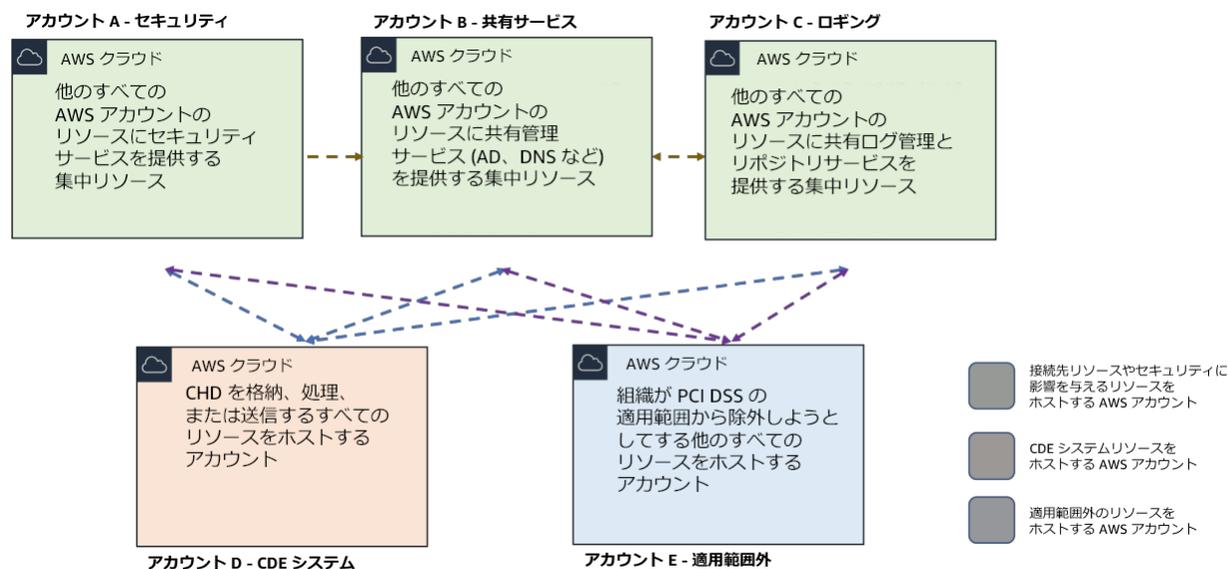


図 2: PCI DSS の適用範囲を制限するためのマルチアカウントアーキテクチャ

マルチアカウントアーキテクチャのコンポーネント

図 2 は、AWS のベストプラクティスに従って設計されたマルチアカウントアーキテクチャを示しており、AWS の [ランディングゾーンアーキテクチャ](#) を通じて公開されています。ここでは、同様の機能を提供するリソースが AWS アカウント内にまとめられています。このグループ化により、範囲内の AWS リソースと範囲外の AWS リソースの間でセキュリティと管理を提供するリソースを共有しながら、PCI DSS の適用範囲を制限できます。このシナリオでは、リソースの PCI DSS の適用範囲、CDE システム、接続先システムやセキュリティに影響を与えるシステム、および適用範囲外のシステムに基づいてアカウントがグループ化されます。

CDE システムアカウント (図 2 のアカウント D)

1 つ以上の専用 AWS アカウントで CHD を処理する IT インフラストラクチャをプロビジョニングします。このアカウントを他の IT リソースのプロビジョニングに使用しないでください。

CDE システムアカウントが含むリソースの例を以下に示します。

- 外部エンティティとの間で CHD を受信または送信するコンピューティングリソースおよびネットワークリソース
- CHD を処理するコンピューティングリソース
- 保管時の CHD を保存するストレージリソース

CDE システムアカウントは、PCI DSS インフラストラクチャの最も機密性の高い部分とと考えてください。このアカウントのシステムコンポーネントは、適用範囲を他のリソースへと広げる傾向があります。つまり、通信に関連する機能やデータに関係なく、接続先のシステムコンポーネントも PCI の適用範囲にあるとみなされます。このアカウント以外での通信は、システム管理やビジネス要件の目的のために、他の AWS アカウントの必要なリソースのみに厳しく制限する必要があります (ポートとプロトコルの制限)。厳格な変更管理プロセスを実装して、このアカウントの変更がセグメンテーション境界や組織の PCI DSS 全体に悪影響を及ぼさないようにします。AWS Config を使用すると、特定の AWS リソースに対するすべての変更を追跡できます。これにより、AWS Lambda 機能でアラートを生成したり、セキュリティコントロールの逸脱を自動修正したり、変更コントロールプロセスを実装するためのさまざまな手順を調整したりすることができます。

接続先のシステムアカウントやセキュリティに影響を与えるシステムアカウント (図 2 のアカウント B および C)

別の AWS アカウントを使用して、CDE システムの管理や CDE システムへのセキュリティ機能の提供に必要な他のシステムコンポーネントをプロビジョニングします。

セキュリティに影響を与えるシステムアカウントが含むリソースの例を以下に示します。

- ジャンプサーバーまたは要塞ホスト
- ディレクトリサービス
- ウイルス対策およびマルウェア対策サービス
- 脆弱性スキャンサービス
- CDE システムの管理を支援する、または 1 つ以上の PCI DSS 要件を満たすために必要なその他のサービス

接続先システムアカウントが含むリソースの例を以下に示します。

- CHD 以外のデータを抽出するビジネスインテリジェンスアプリケーションなどのビジネス目的を達成するために、CDE システムからデータを抽出するアプリケーションまたはサービス。
- 接続先システムやセキュリティに影響を与えるシステムのプロビジョニングに使用されるアカウント。
- 集中セキュリティアカウントと共有サービスアカウント

これらのアカウントのリソースは、組織の CDE 以外の AWS リソースから隔離する必要はありません。ここで提供されるサービスは、PCI の適用範囲に属さない他の AWS リソースで利用できます。このように強化されたセキュリティ統制では、セキュリティサービスと制御が一元化され、すべてのワークロードで同じベースラインを維持できるようになります。

AWS が公開している[ランディングゾーンアーキテクチャ](#)によると、セキュリティアカウントや共有サービスアカウントとは別に、集中型ロギング専用の AWS アカウントを用意する必要があります。このアカウントは、すべての AWS アカウントから、すべてのシステムとアプリケーションのあらゆる種類のログを収集する必要があります。これにより、集中管理が可能になり、セキュリティログを含むすべてのログデータへのアクセスも制限可能になります。[図 2](#) のアカウント C - ロギングアカウントは、集中ログ管理 AWS アカウントを表します。ログ管理の一部であり、PCI DSS 要件 10.3 を満たすために使用されるこのアカウントのシステムのみが、PCI DSS の対象となります。

適用範囲外のシステムアカウント (図 2 のアカウント E)

別の AWS アカウントを使用して、CDE システムに対していかなる形式の接続も必要とせず、サービスを提供しない IT インフラストラクチャをプロビジョニングします。これにより、AWS アカウントに備わる隔離機能を活用して、そのようなインフラストラクチャが PCI の適用範囲内のシステムから適切かつ意図的に隔離されます。

CDE システムと接続先システムとの間の通信は許可されますが、そのようなチャネルを CHD が流れないようにする必要があります。そうしないと、接続先システムを CDE システムに再分類する必要があります。このシナリオでは、適用範囲の変更が連鎖的に発生する可能性があります。また、監視することにより、悪意のある者が侵入先の CDE システムからデータを流出させる目的で接続先システムを使用することを容易に防止できるようになります。

マルチアカウントアーキテクチャは、類似のアカウントに標準のセキュリティ管理を横断的に実装するために AWS アカウントをグループ化する際にも役立ちます。このようなアカウントをまとめて、[AWS Organizations](#) およびポリシーベースのアカウント管理の一部として個々の組織単位 (OU) を形成することができます。複数の AWS アカウントにわたる AWS のサービスの使用を集中的に制御する OU にサービスコントロールポリシー (SCP) を適用できます。SCP によって、[AWS Identity and Access Management \(IAM\)](#) ポリシーがアカウント内のエンティティ (IAM ユーザーやロールなど) に付与できる権限が制限されます。例えば、SCP を使用して、適用範囲内のシステムアカウント内で PCI DSS に準拠していない AWS のサービスのプロビジョニングを禁止することができます。

ネットワーク層 (OSI 第 3~4 層)

セキュリティグループは、明示的な拒否の原則に基づいて動作するステートフルなネットワーク層トラフィックフィルタリングを提供する Amazon Virtual Private Cloud (VPC) の機能です。セキュリティグループはホストベースのファイアウォールに相当し、EC2 インスタンスのネットワークインターフェイスに関連付けられます。セキュリティグループはネットワーク層におけるセグメンテーション境界であり、PCI DSS スコープ戦略はセキュリティグループを中心としてネットワーク層で設計されている必要があります。さらに、セキュリティグループを使用して、インスタンス間のトラフィックフローを制限し、PCI DSS v3.2.1 の要件 1.2⁵ および 1.3⁶ を満たすことができます。

セキュリティグループを使用して、CDE システムを他の接続先システムからセグメント化するのに必要なポート、送信元、および宛先アドレスに基づいてネットワーク通信を制限します。

セキュリティグループを Auto Scaling グループに参加させると、そのグループがスケールアウトおよびスケールインするときに、グループ内のインスタンスに適用したり、グループ内のインスタンスから削除したりすることができます。2 つのピアリングされた VPC 間でセキュリティグループを連結することにより、1 つのセキュリティグループでハードコードされた IP アドレスを参照する代わりに、もう 1 つのセキュリティグループを発信元または宛先として参照するようになります。この設計によって、セキュリティグループアーキテクチャの自動化が容易になります。また、CIDR 範囲ではなくセキュリティグループメンバシップを通じてピアトラフィックを制御することにより、スケーラビリティも提供されます。

デフォルトでは、セキュリティグループはすべてのアウトバウンドトラフィックを許可するため、PCI DSS 要件 1.2.x を満たしていません。セキュリティグループのデフォルトを設定して、インバウンドとアウトバウンドのトラフィックを必要なトラフィックのみに制限し、その他のトラフィックはすべて拒否するようにします。

PCI DSS の適用範囲全体に影響を与えることなく、適用範囲外の AWS アカウントの EC2 インスタンス間の接続を接続先システムアカウントを使用して有効にすることができます。さらに、VPC ピアリング接続は推移的ではないので、CDE システムアカウントと適用範囲外システムアカウントとの間にピアリング接続が設定されていない限り、CDE システムアカウントと接続先システムアカウントとの間のピアリング接続が適用範囲外システムアカウントへ拡張されるということはありません。

以下の図は、セキュリティグループを使用してセグメンテーションを行う方法を示しています。図のように、セキュリティグループは、主に、VPC やネットワークセグメントなどの他のネットワーク構成とは無関係に、ネットワークセグメントを定義します。

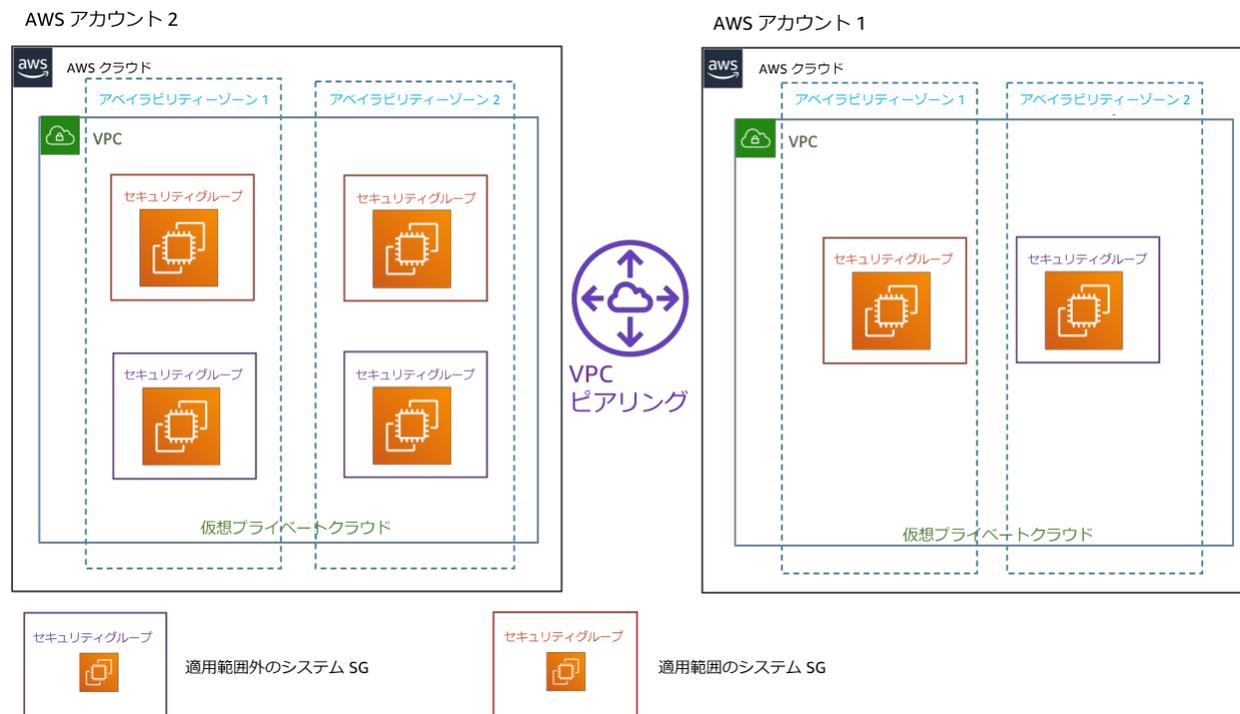


図 3: セキュリティグループを使用したネットワークセグメンテーション

アプリケーション層 (OSI 第 7 層)

この層では、CHD を処理するアプリケーションが CHD フローを管理し、セグメンテーション境界を定義する必要があります。AWS では、AWS Lambda、Amazon S3、Amazon DynamoDB など、ウェブ API ベースの抽象化されたサービスを数多く提供しています。お客様の組織では、このようなサービスを利用することで、

サーバーや EC2 インスタンスの管理を気にせずにビジネス機能を実現できます。このような抽象化されたサービスの唯一可能な通信形式は、エンドポイントに対するウェブサービス API 呼び出しです。API 呼び出しは、アプリケーション層 (OSI 第 7 層) を介して行われます。

抽象化された AWS のサービスのセグメンテーション

抽象化されたサービスには、意図的にネットワークの隔離機能が実装されています。このようなサービス間の接続は、ネットワーク接続ではなくデータ接続です。スコーピングでは、接続を通過するデータの種類に焦点が当てられます。

抽象化されたサービスで CHD が処理されない場合は、コンテンツに基づいた制御を使用して、CHD が CDE からそのような抽象化されたサービスに到達できないことを十分に示し、そのようなサービスを PCI の適用範囲から除外できます。

データのフィルタリングや監視など、適切なアーキテクチャ設計を採用して、そのようなサービスが CHD を保存、処理、または送信しないようにし、確実に PCI の適用範囲外とみなすことができるようにします。

Amazon API Gateway によるセグメンテーション

お客様が定義するウェブ API ベースのサービス (サーバーレスのアプリケーションなど) では、[Amazon API Gateway](#) を使用して、CDE リソース/サービスと他のウェブベースのサービスとの間の接続を仲介することができます。Amazon API Gateway は、バックエンドサービスのデータやビジネスロジック、機能にアクセスするアプリケーションに対して「フロントドア」として機能します。そのようなアプリケーションには、[Amazon Elastic Compute Cloud \(Amazon EC2\)](#) で動作するワークロード、[AWS Lambda](#) で実行されるコード、その他のサポートされた AWS のサービス、またはウェブ/モバイルアプリケーションなどが含まれます。API Gateway を使用して、AWS でホストされている CDE システムおよびサービスからの通信に対してフロントエンド処理を行うことができます。この場合、CDE システムおよびサービスからの接続に対する終端が API Gateway に置かれ、API Gateway から宛先システムまたはサービスに対して新しい接続が確立されます。

その結果、API Gateway を介して CDE システムと通信する AWS 外部のウェブ API ベースのリソースは、そのリソースが CHD を処理したり、CDE システムにセキュリティサービスを提供したりしない限り、お客様の PCI DSS の適用範囲から除外できます。API Gateway サービスのインスタンスは、接続されたシステムとして PCI DSS の適用範囲内にあります。これは PCI DSS の検証済みサービスであるため、PCI DSS 用のサービスの保守と検証について心配する必要はありません。API Gateway はセキュアな、アクセス制御されたウェブサービス API メカニズムを提供しますが、CDE からの予期しない CHD の監視などの着信データの検証は、アプリケーション側の責任範囲です。

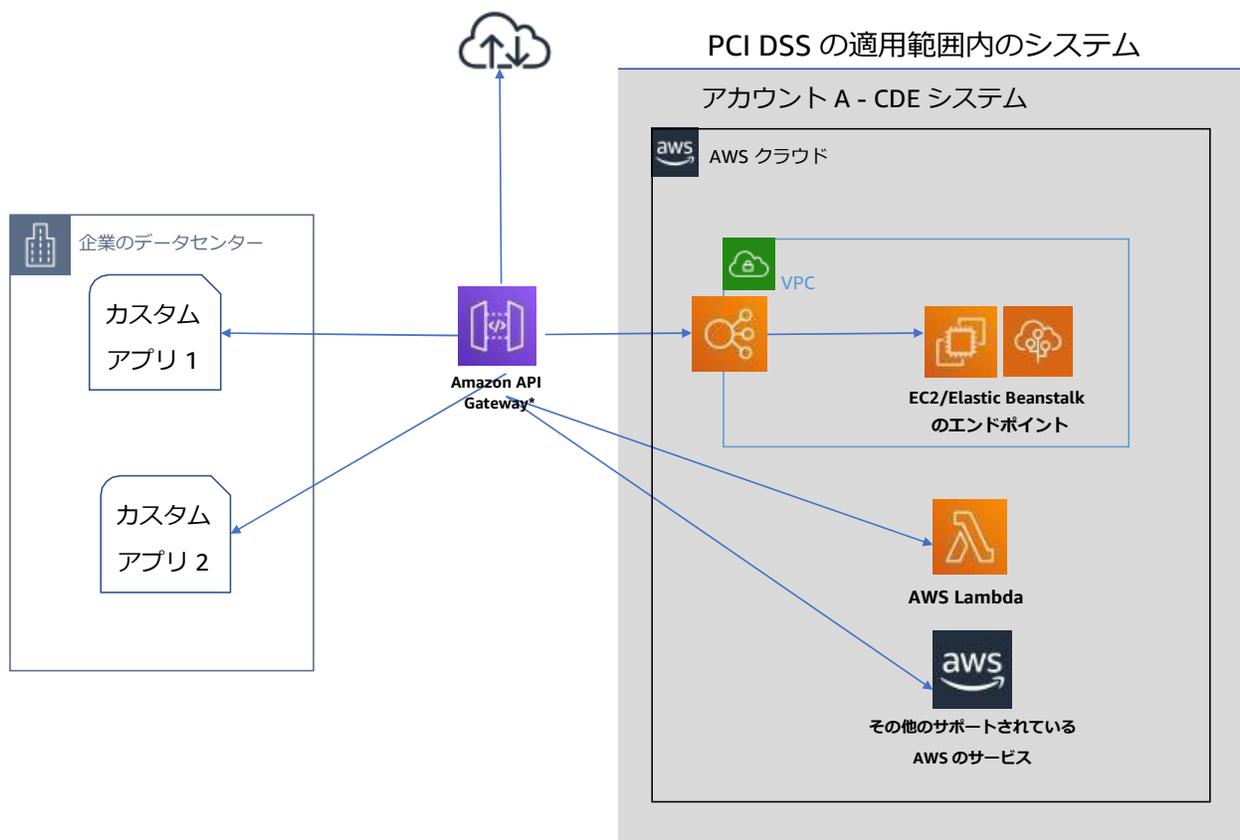


図 4: 抽象化されたサービスに Amazon API Gateway を使用したセグメンテーション

Docker コンテナを活用したワークロードのスコーピング およびセグメンテーション

組織で透過的なアプリケーションを迅速、確実、一貫性のある方法でデプロイメント環境に導入するためにコンテナが使用されています。コンテナを使用すると、アプリケーションのコード、構成、依存関係を簡単にパッケージ化して、環境の一貫性、運用効率、開発者の生産性、バージョン管理を実現するビルディングブロックにまとめることができます。[Amazon Elastic Container Service \(Amazon ECS\)](#) は、Docker コンテナをサポートし、AWS でコンテナ化されたアプリケーションを簡単に実行および拡張できるようにする、拡張性とパフォーマンスに優れたコンテナオーケストレーションサービスです。コンテナ化された PCI の適用範囲内のアプリケーションを実行している、または実行するように設計している場合は、適切なスコーピングおよびセグメンテーションが行われるようにする必要があります。

タスクとは、実行中のコンテナの論理グループです。Amazon ECS タスクは、以下の 2 つのタスク起動タイプをサポートしています。

- Amazon EC2 インスタンスタイプ: このタイプを使用すると、管理対象の Amazon EC2 インスタンスのクラスタでコンテナ化されたアプリケーションを実行できます。
- [AWS Fargate](#) タイプ: このタイプを使用すると、バックエンドインフラストラクチャのプロビジョニングや管理を行うことなく、コンテナ化されたアプリケーションを実行できます。

コンテナのスコーピング

タスク定義とタスク起動タイプの組み合わせによって、コンテナの適用範囲が決まります。理想的には、PCI の適用範囲内のコンテナと適用範囲外のコンテナをグループ化する、個別のタスクを作成します。EC2 インスタンス起動タイプの場合は、そのようなタスクを別々のクラスタに割り当てます。この割り当てにより、PCI の適用範囲内のコンテナタスクを実行しているクラスタ内のすべての EC2 インスタンスが PCI の適用範囲内にのみ含まれるようになります。セキュリティグループを ECS クラスタに割り当て、セキュリティグループの ACL を設計することで、ネットワーク通信を適用範囲内のその他のシステムとの間のみで制限したり、適用範囲外のシステムコンポーネントからクラスタを隔離したりできます。クラスタを隔離したら、タスクレベルの隔離またはセグメンテーションを設計します。ECS は[タスクネットワーク](#)をサポートしています。タスクネットワークを使用すると、コンテナタスクを独自のネットワークインターフェイスに隔離することで、個々のタスクのセキュリティグループルールを定義できます。

awsipc モードを使用してタスク定義を作成する方法の詳細については、[タスクネットワーク](#)に関する AWS のドキュメントを参照してください。

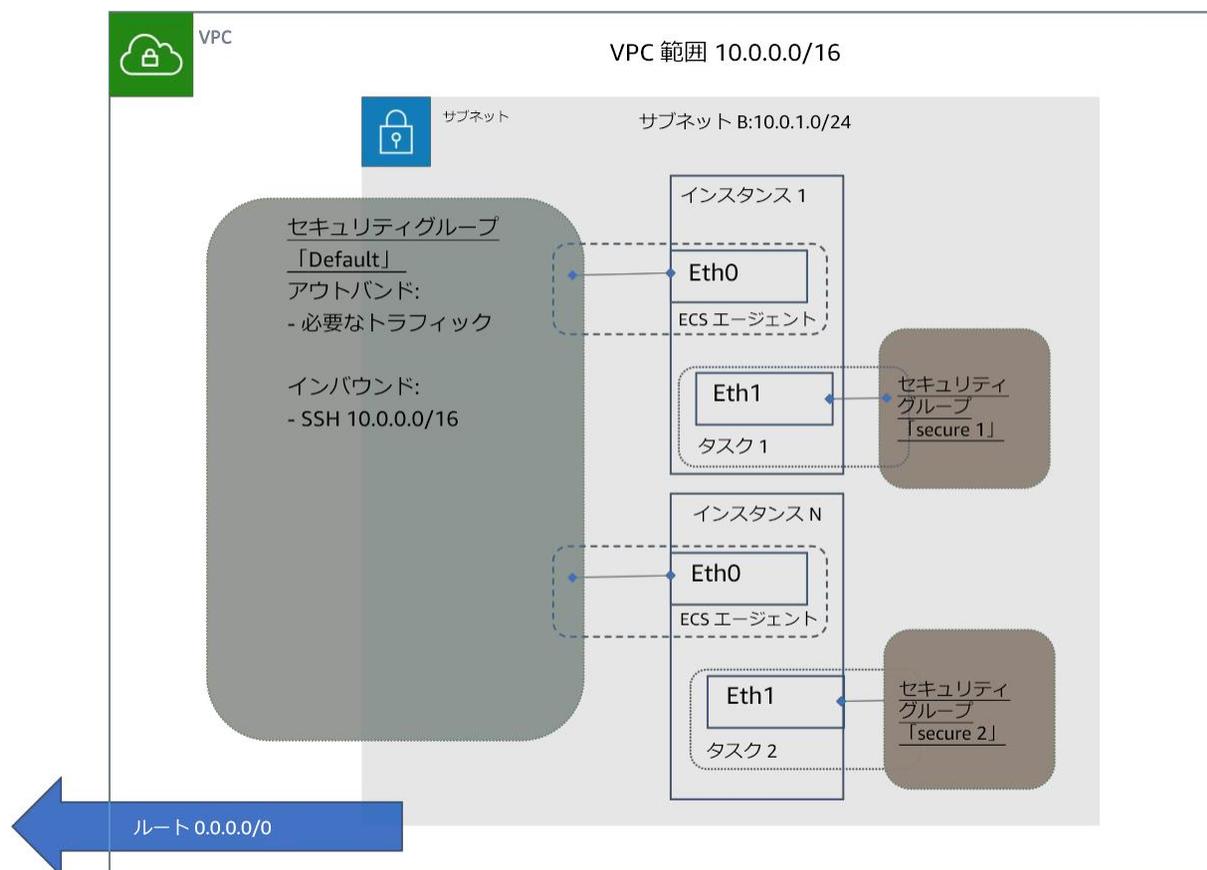


図 5: ECS タスクレベルのセグメンテーション

ネットワークセグメンテーションはタスク内で実現できますが、適用範囲内アプリケーションと適用範囲外アプリケーションの両方を 1 つの ECS タスクの一部として実行することは避けてください。両方を実行してしまうと、適切な適用範囲境界の定義にオーバーヘッドが生じる可能性があります。

AWS Fargate タスク起動タイプでは、タスクは最下位の構成要素であるため、クラスタの割り当てや適用範囲について気にする必要はありません。適用範囲内コンテナを実行するタスクをグループ化し、awsipc ネットワークモードをセキュリティグループルールと組み合わせて使用して、適用範囲内タスクと適用範囲外タスク間の通信をセグメント化または制限します (あるいはその両方)。

ハイブリッド環境のためのスコーピングガイダンス

ハイブリッドアーキテクチャ (AWS プラットフォームとオンプレミスのデータセンターの両方で実行されるワークロード) を実行する組織は、オンプレミスシステムコンポーネントと AWS CDE リソースとの接続を考慮する必要があります。

以下のシナリオを考慮してください。

シナリオ 1: AWS でホストされている PCI リソースが、オンプレミスのデータセンターのリソースにネットワーク接続されている。

シナリオ 2: オンプレミスデータセンターでホストされている PCI リソースが、AWS のリソースにネットワーク接続されている。

シナリオ 3: PCI リソースが、オンプレミスのデータセンターと AWS の両方でホストされている。

シナリオ 1 および 2 では、CDE 以外のリソースの適用範囲は、そのリソースがホストされている場所に関係なく、CDE 以外のリソースと適用範囲内システムとの接続のタイプによって決まります。

- CDE 以外のリソースが CDE リソースに直接接続されている場合、そのようなオンプレミスまたは AWS のリソースは PCI DSS の適用範囲内となります。
- CDE 以外のリソースが接続先システムに接続されている場合、そのようなオンプレミスまたは AWS のリソースは、CDE システムにセキュリティまたは管理サービスを提供していない限り、PCI DSS の対象外とみなすことができます。さらに、このような適用範囲外のシステムが侵害された場合でも、そのシステムを使用して CDE を侵害することはできません。例えば、AWS Systems Manager はオンプレミスサーバーと適用範囲内の EC2 インスタンスの両方を管理できます。このシナリオでは、オンプレミスサーバーが CHD とやり取りをしていないか、CDE に対して他の接続がない限り、適用範囲外です。

適用範囲を制限する場合、以下のガイドラインを考慮してください。

- オンプレミスネットワークからのネットワーク接続は、CDE 以外のリソースへ接続のみに制限します。
- CDE リソースに接続する必要がある場合、適切なセキュリティ統制と設計を実装して、不要なネットワークコンポーネントやシステムコンポーネントにまで適用範囲の対象を広げてしまう可能性がある推移的なネットワーク接続を防止します。

- 適用範囲の境界が誤って変更されないように、複数のセグメンテーションコントロールを実装してください。このようなコントロールは、オンプレミスのステートフルファイアウォールテクノロジーとセキュリティグループを使用して定義および実装され、徹底的な防御を実現するためにネットワークアクセスコントロールリスト (ネットワーク ACL) によって支援されたアクセスコントロールルールの組み合わせによって実装できます。

シナリオ 3 では、適用範囲を簡単に決定できるように、CDE リソースをオンプレミスまたは AWS にグループ化します。このグループ化ができない場合は、すべての CDE と接続先システムがオンプレミスと AWS の両方で識別され、そのようなシステムへの接続が正しく識別されていることを慎重に確認します。

スコーピングおよびセグメンテーションの検証

PCI DSS 要件 11.3.4⁷ によると、ネットワークおよびアプリケーション層のテストを実行する必要があります。この手順は、NIST SP 800-37 で概説されているセキュリティとプライバシーのためのシステムライフサイクルアプローチの「コントロールの評価と承認」フェーズに対応します。

PCI DSS が公開した [Information Supplement: Penetration Testing Guidance](#) によると、侵入テストの適用範囲には CDE の境界全体と重要なシステムが含まれます。⁸ これは、CDE の外部境界 (公開された状態の攻撃断面) と内部境界 (LANからLANへの攻撃断面) の両方に適用されます。さらに、AWS でホストされている CDE への VPN 接続など、すべてのリモートアクセスベクターが含まれます。

このようなセグメンテーション境界を検証する侵入テストは、CDE が EC2 インスタンスなどのインフラストラクチャサービスで構成されている場合にのみ必要です。抽象化されたサービスでは、AWS のサービスとエンドポイントのスキャンと侵入テストは、AWS の PCI DSS サービスプロバイダー評価に含まれています。

EC2 インスタンスなどのインフラストラクチャサービスでは、セキュリティグループが基本的なセグメンテーション境界を形成します。セキュリティグループの設定が信頼できるものである限り、セキュリティグループのセグメンテーションを検証するために侵入テストを実施しても意味がありません。セキュリティグループがセグメンテーション境界を定義し、EC2 インスタンスのネットワークインターフェイスに関連付けられるので、侵入境界を検証するには、適用範囲外の EC2 インスタンスから適用範囲内の EC2 インスタンスに侵入する方法をお勧めします。

ハイブリッド環境では、侵入テストのソースは物理的なオンプレミスネットワークの適用範囲外のネットワークセグメントで、ターゲットは適用範囲内の EC2 インスタンスです。

適用範囲内の AWS の抽象化されたサービスでは、CHD フローとセグメンテーション境界はアプリケーションとアプリケーションコードによって制御されます。したがって、アプリケーション内に組み込まれた設計に基づいて、セグメンテーション境界を検証するアプリケーションテストに集中する必要があります。そうすることで、CHD フローと PCI DSS 適用範囲が、CHD フロー図に示されているようにアプリケーションによって維持されます。

PCI 準拠の抽象化された AWS のサービスの API には、侵入テストは必要ありません。
AWS エンドポイントの侵入テストは AWS 側の責任範囲です。

AWS クラウドプラットフォームで侵入テストを準備する際には、AWS 利用規約を必ず理解しておいてください。AWS は、侵入テストベンダーやサードパーティの候補を調査し、そのようなベンダーが有する AWS プラットフォームやテクノロジーに関するクラウド全体の経験と侵入テストの経験について判断することをお勧めします。AWS リソースを使用して脆弱性の評価や侵入テストを実施する方法の詳細については、[脆弱性テストと侵入テスト](#)を参照してください。

予防的な統制

PCI DSS で義務付けられている定期的な侵入テストに加えて、セグメンテーションコントロールの不正な変更を防ぐために、予防的なセキュリティ統制が必要です。

このセクションでは、実装されたセグメンテーションコントロールのステータスの監視について説明します。この監視によって、定義されている PCI DSS の適用範囲が意図的または誤って侵害されないようにすることができます。違反があった場合には、それぞれの利害関係者にできるだけ早く通知し、直ちに是正措置を講じることができるように、予防的な統制を設計しなければなりません。セキュリティ体制が十分に整ったら、対応の大部分を自動化し、人間の介入なしにほぼリアルタイムで逸脱を修正できるようにします。以下に、セグメンテーション境界を監視する方法をいくつか示します。

- すべてのセキュリティグループルールを、計画されている CDE の適用範囲に対して定期的に検証します。
- 変更管理プロセスですべてのセキュリティグループとネットワーク設定を管理します。
- CDE システムアカウントのすべてのセキュリティグループルールの変更を監視します。
- CDE システムアカウントへのすべての VPC ピアリング接続を監視します。

- 適用範囲内の API Gateway に対するすべての設定変更を監視します。
- CHD の漏洩を防止し、適用範囲の境界を検証するために、すべての接続先システムにデータ損失に対する予防的な統制を実装します。

[AWS Config](#) を使用して対応を自動化できます。AWS Config は、ガバナンスとセキュリティを実現する際に役立つ、リソース設定履歴や設定変更通知を提供します。

カスタム AWS Config ルールを作成すると、セキュリティグループ、VPC ピアリング接続、API Gateway、およびセグメンテーション境界を強制する AWS 内のその他のリソースに対するすべての変更を監視できます。AWS Config ルールを適切な AWS Lambda レスポンダに適用して逸脱を評価し、定義された PCI DSS セグメンテーション境界に違反した変更を自動修正します。

AWS CloudTrail を使用すると、AWS リソースのすべての設定変更を監視することができます。さらに、Amazon CloudWatch Events を設定し、Lambda レスポンダが修正アクションを実行するようにもできます。この例は、CDE のセキュリティ統制を設計して自動化するのに使用できるさまざまな AWS のサービスを示しています。

フィードバックループ

ビジネスは絶えず変化しており、その結果、PCI の適用範囲内のアプリケーションの設計と機能、および関連する AWS のサービスの選択肢は、時間の経過とともに変化します。ビジネス要件の変化は別にしても、AWS インフラストラクチャをさらに安全かつ効率的で管理しやすいインフラストラクチャに進化させることとなります。この絶え間ない変化の中では、セキュリティとセグメンテーションコントロールの設計プロセスでフィードバックループを確立することが不可欠となります。前のフェーズや同業者からのフィードバックを収集するチャネルを確立し、そのフィードバックを使用して現在のプロセスを改善し、より安全にできます。フィードバックループとそれに関連する変更によって、PCI DSS の適用範囲を定義するために実装された現在のセグメンテーションコントロールの再評価が必要になる場合があります。この再評価は、組織の CHD フローの変更によっても発生する場合があります。既存の確立された PCI DSS の適用範囲を検証して必要に応じて適用範囲内のシステムを再分類するプロセスが、理由の有無にかかわらず少なくとも年 1 回は必要です。

まとめ

本書では、さまざまなアーキテクチャパターンを取り上げました。そのようなアーキテクチャパターンは、適切なセグメンテーション境界を設計する際に採用可能です。また、AWS プラットフォームでホストされる CDE リソースを安全に機能させるために必要なシステムコンポーネントに PCI DSS の適用範囲を制限する際も役立ちます。セグメンテーション境界の設計に使用されるサービスや機能には、AWS アカウントとセキュリティグループが含まれます。どちらもクラウドネイティブであるため、本質的に復元力が高く、弾力性があります。インフラストラクチャをソフトウェアコードとして実装し、既存の CI/CD パイプラインを通じて自動化することで、継続的なコンプライアンスを実現できます。

PCI DSS で定義されたセグメンテーションの概念である隔離と制限された通信という考え方は AWS プラットフォームのリソース全体で統一されています。異なる部分はコントロールの実現方法であり、これは AWS クラウドプラットフォーム特有のものであります。また、責任共有モデルの一環として、PCI DSS 検証済みの AWS のサービスを使用すること自体がお客様の環境における PCI DSS への準拠を示すわけではありません。それらのサービスは、PCI DSS に準拠した方法で使用および設計してください。

適用範囲の設計と決定は常にお客様の組織の責任範囲ですが、AWS では、よりアジャイルに設計を実施できます。

執筆者

本書の執筆者は以下のとおりです。

- Avik Mukherjee、セキュリティアーキテクト、AWS
- Balaji Palanisamy、シニアコンサルタント、AWS
- Tim Winston、シニアアシュアランスコンサルタント、AWS Security Assurance Services LLC

詳細情報

詳細については、以下を参照してください。

- [PCI Compliance in AWS Technical Workbook](#)
- [AWS ホワイトペーパー](#)
- [SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#)
- [PCI Security Standards Council Penetration Testing Guidance](#)
- [Architecting for the Cloud: AWS Best Practices Whitepaper](#)
- [Introducing Cloud Native Networking for Amazon ECS Containers](#)
- [AWS Multiple Account Security Strategy](#)
- [PCI SSC Cloud Computing Guidelines](#)
- [PCI Security Standards Council Penetration Testing Guidance](#)
- [PCI DSS Virtualization Guidelines](#)

文書改訂

日付	説明
2019 年 5 月	初版

注記

- 1 PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1 (https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf) の「Requirement 11: Regularly test security systems and processes」を参照してください。
- 2 カード所有者のデータ (CHD): カード所有者のデータは最低でも完全な PAN で構成されます。これは、完全な PAN に、カード所有者名、有効期限、およびサービスコードのいずれかを加えた形式で表すこともできます。支払い取引の一環として転送または処理される可能性のある (ただし、保存はされない) 追加のデータ要素については、機密性の高い認証データを参照してください。
- 3 さまざまなタイプの AWS のサービスと関連する責任共有モデルの詳細については、ホワイトペーパーの [AWS Security Best Practices](#) を参照してください。
- 4 クラウドの利点の詳細な分析については、ホワイトペーパーの [Architecting for the Cloud: AWS Best Practices](#) および [Overview of Amazon Web Services](#) を参照してください。
- 5 PCI DSS v3.2.1 要件 1.2 - 1.2 カード所有者のデータ環境において、信頼されていないネットワークとシステムコンポーネント間の接続を制限するファイアウォールとルーター構成を構築します。
- 6 PCI DSS v3.2.1 要件 1.3.5 - 1.3.5 ネットワークに対し、「確立された」接続のみを許可します。
- 7 PCI DSS 要件 11.3.4 - 他のネットワークから CDE を隔離するためにセグメンテーションを使用する場合は、侵入テストを少なくとも年に 1 回実施します。さらに、追加でセグメンテーションコントロール/方法を変更した後に実施し、セグメンテーション方法が運用可能かつ効果的であることを確認してすべての適用範囲外のシステムを CDE 内のシステムから隔離します。
- 8 PCI DSS 要件 10 - ネットワークリソースとカード所有者のデータへのすべてのアクセスを管理/監視します。
ロギングメカニズムとユーザーアクティビティを追跡する機能は、データ侵害の影響を防止、検出、または最小化するために重要です。すべての環境にログが存在することにより、何か問題が発生した場合に、完全な追跡、アラート通知、分析を行うことができます。システムアクティビティログがないと、侵害の原因を特定するのは困難です。