PCI DSSから考える、
AWSセキュリティのあれこれ

伊藤忠テクノソリューションズ株式会社

金融技術第４部

大友　勝明

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

はじめに

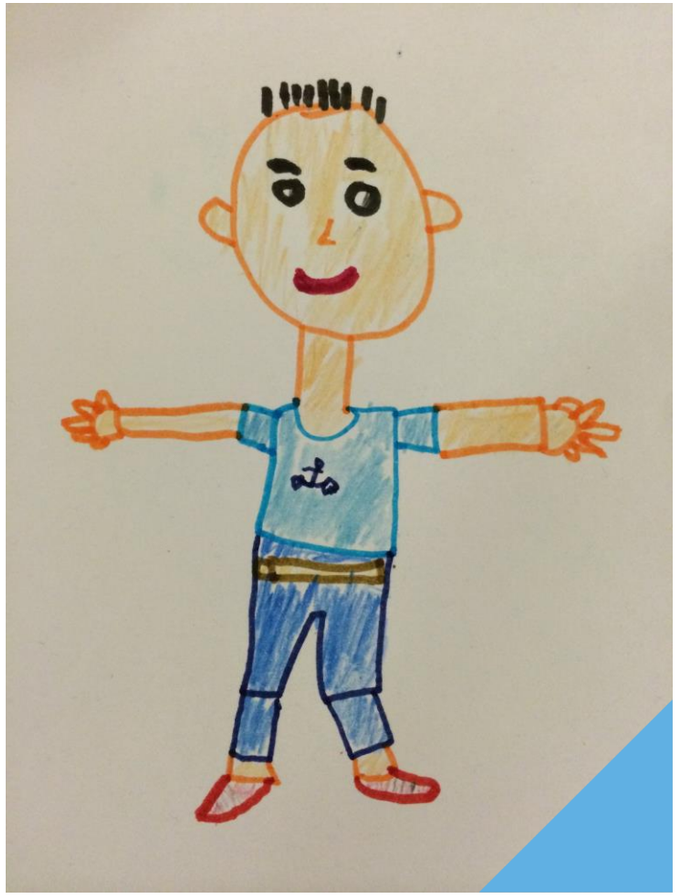
はなすひとの紹介、はなすこと、はなさないこと

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

はなすひとの紹介

- 名前：大友 勝明
- 所属：伊藤忠テクノソリューションズ株式会社 金融技術第４部
- 生年月日：1971年10月23日
- 好きなひと：妻と子供（高2男子）
- 好きなSF作家：テッド・チャン
- 好きな犬種：シーズー
- 好きな空手家：渡口 政吉



無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

はなすこと

- クラウドでのセキュリティの考え方について
- AWSのセキュリティサービスの紹介
- AWSのセキュリティサービスについてのちょっとしたポイント

「どんな時にどのサービスが利用できるのか」がわかります

はなさないこと

- PCI DSSの要件についての網羅的な対応策
- AWSの特定のサービスの設計や設定についての詳細

「これだけでPCI DSS対応もバッチリ！」とはなりません

クラウドとセキュリティのはなし

クラウドについての簡単な説明とクラウドでのセキュリティの考え方の簡単な説明

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

クラウドってなぁに？

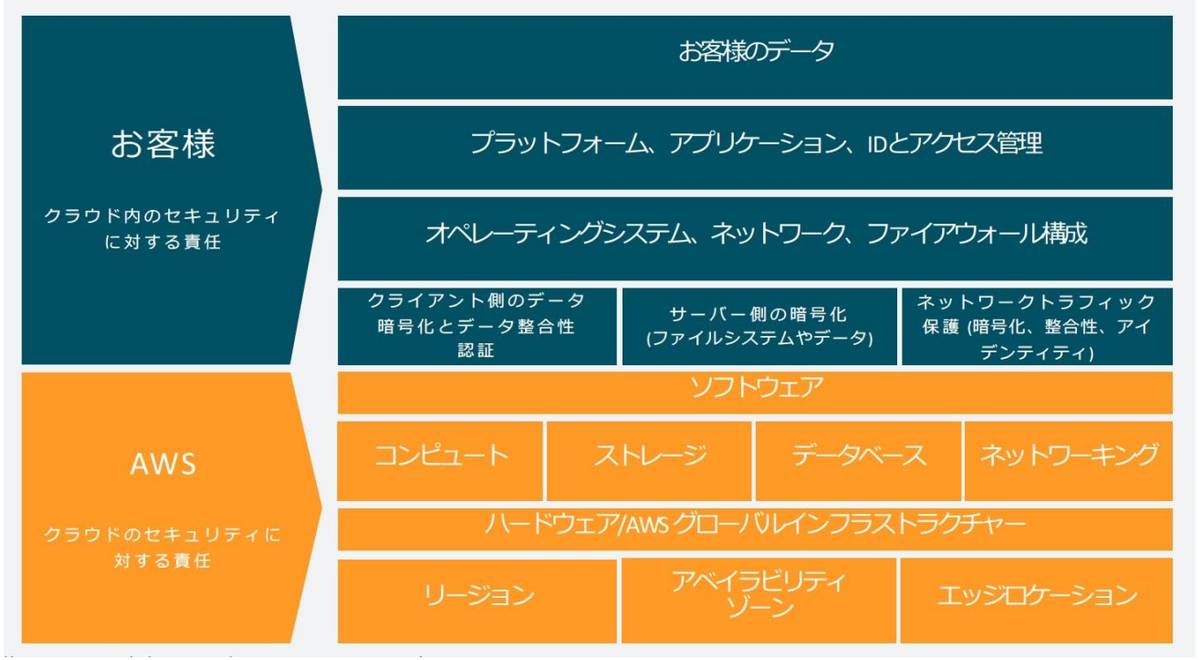
クラウドコンピューティングとは…

- オンデマンド・セルフサービス
- 幅広いネットワークアクセス
- リソースの共用
- スピーディな拡張性
- サービスが測定可能であること

※NIST SP 800-145（日本語）

クラウドでのセキュリティの考え方、責任共有モデル

- **AWS の “クラウドのセキュリティ” 責任**— AWS 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インフラストラクチャの保護について責任を負います。このインフラストラクチャはハードウェア、ソフトウェア、ネットワーキング、AWS クラウドのサービスを実行する施設で構成されます。
- **お客様の “クラウドにおけるセキュリティ” 責任** —お客様の責任は、選択した AWS クラウドのサービスに応じて異なります。選択によって、セキュリティに関する責任の一環としてお客様が実行する構成作業の量が決定されます。たとえば、Amazon Elastic Compute Cloud (Amazon EC2) などのサービスは Infrastructure as a Service (IaaS) に分類されているため、必要なすべてのセキュリティ構成および管理のタスクをお客様が実行する必要があります。お客様が Amazon EC2 インスタンスをデプロイした場合、お客様は、ゲストオペレーティングシステムの管理 (更新やセキュリティパッチなど)、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またはユーティリティの管理、AWS より各インスタンスに提供されるファイアウォール (セキュリティグループと呼ばれる) の構成に責任を負います。 Amazon S3 や Amazon DynamoDB などの抽象化されたサービスの場合、AWS はインフラストラクチャレイヤー、オペレーティングシステム、およびプラットフォームを運用し、お客様はエンドポイントにアクセスしてデータを保存および取得します。お客様は、データの管理 (暗号化オプションを含む)、アセットの分類、IAM ツールでの適切な権限の適用について責任を負います。



※AWS「責任共有モデル」

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

セキュリティ強化のための設計原則

- **強力なアイデンティティ基盤を実装する：** 最小特権の原則を実装し、 AWS リソースとのやり取りごとに適切な認可を得て職務の分離を適用します。アイデンティティ管理を一元化し、長期的な静的認証情報への依存を排除することを目指します。
- **トレーサビリティの維持:** 環境に対して、リアルタイムでモニタリング、アラート、監査のアクションと変更を行います。ログとメトリクスの収集をシステムと統合して、自動的に調査してアクションを実行します。
- **すべての層にセキュリティを適用する:** 複数のセキュリティコントロールを使用して、詳細な防御アプローチを適用します。すべてのレイヤー (ネットワークのエッジ、、VPCロードバランシング、すべてのインスタンスとコンピューティングサービス、オペレーティングシステム、アプリケーション、コードなど) に適用します。
- **セキュリティのベストプラクティスの自動化:** 自動化されたソフトウェアベースのセキュリティメカニズムにより、迅速かつコスト効果に優れた方法で安全にスケールできます。バージョン管理されたテンプレートのコードとして定義および管理されるコントロールの実装を含む、安全なアーキテクチャを作成します。
- **転送中のデータおよび保管中のデータの保護**: データを機密レベルに分類し、必要に応じて暗号化、トークン化、アクセス制御などのメカニズムを使用します。
- **人をデータから遠ざける:** メカニズムとツールを使用して、データに直接アクセスしたり、手動でデータを処理したりする必要性を軽減または排除します。これにより、機密データを扱う際の誤処理や変更、人的ミスのリスクが軽減されます。
- **セキュリティイベントの準備:** 組織の要件に合わせたインシデント管理および調査のポリシーとプロセスを導入し、インシデントに備えます。インシデント対応シミュレーションを実行し、ツールと自動化により、検出、調査、復旧のスピードを上げます。

※AWS「セキュリティ基盤 - 設計原則」

PCI DSSのはなし

PCI DSSについての簡単な説明

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

PCI DSSってなぁに？

PCI DSSとは…

Payment Card Industry Data Security Standardの略。

クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準のこと。

カード情報を「保存、処理、または伝送する」企業であるカード加盟店、銀行、決済代行など行うサービス・プロバイダーが、年間のカード取引量に応じて、PCI DSS 準拠する必要がある。

※日本カード情報セキュリティ協議会「PCI DSSとは」

PCI DSSの要件

安全なネットワークとシステムの構築と維持	1. ネットワークのセキュリティコントロールを導入し、維持します。 2. すべてのシステムコンポーネントに安全な設定を適用します。
アカウントデータの保護	3. 保存されたアカウントデータを保護します。 4. オープンな公共ネットワークでカード会員データを伝送する場合、強力な暗号化技術でカード会員データを保護します。
脆弱性管理プログラムの維持	5. すべてのシステムとネットワークを悪意のあるソフトウェアから保護します。 6. 安全性の高いシステムおよびソフトウェアを開発し、保守します。
強固なアクセス制御手法の導入	7. システムコンポーネントおよびカード会員データへのアクセスを、業務上必要な適用範囲に制限します。 8. ユーザを識別し、システムコンポーネントへのアクセスを認証します。 9. カード会員データへの物理的なアクセスを制限します。
ネットワークの定期的な監視およびテスト	10. システムコンポーネントおよびカード会員データへのすべてのアクセスを記録し、監視します。 11. システムおよびネットワークのセキュリティを定期的にテストします。
情報セキュリティポリシーの維持	12. 事業体のポリシーとプログラムにより、情報セキュリティを維持します。

AWSにおけるセキュリティサービスのはなし

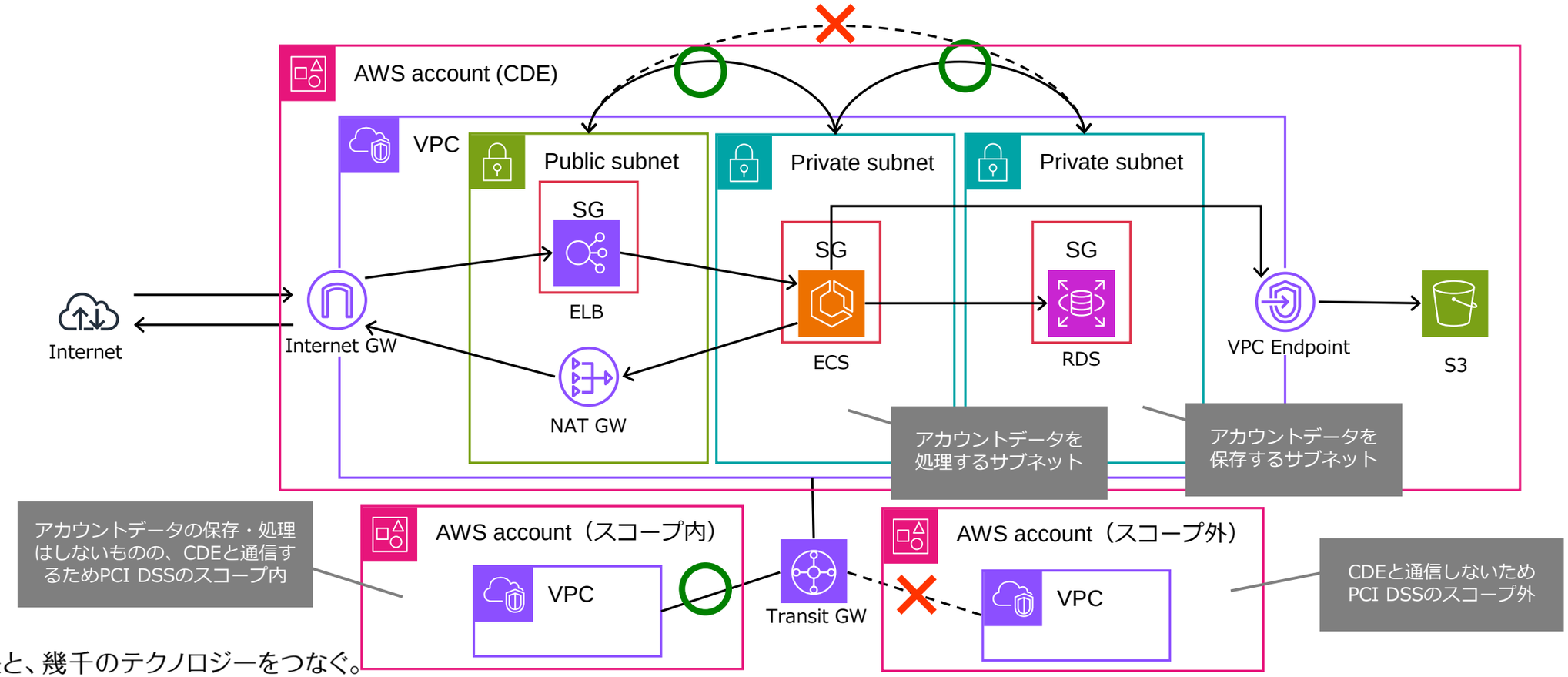
AWSのセキュリティサービスの紹介とちょっとしたポイント

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

安全なネットワークとシステムの構築と維持

- アカウントデータを保存・処理するコンポーネントと伝送する経路を明確にすること
- CDE（Card Data Environment）、スコープ内、スコープ外を明確にすること

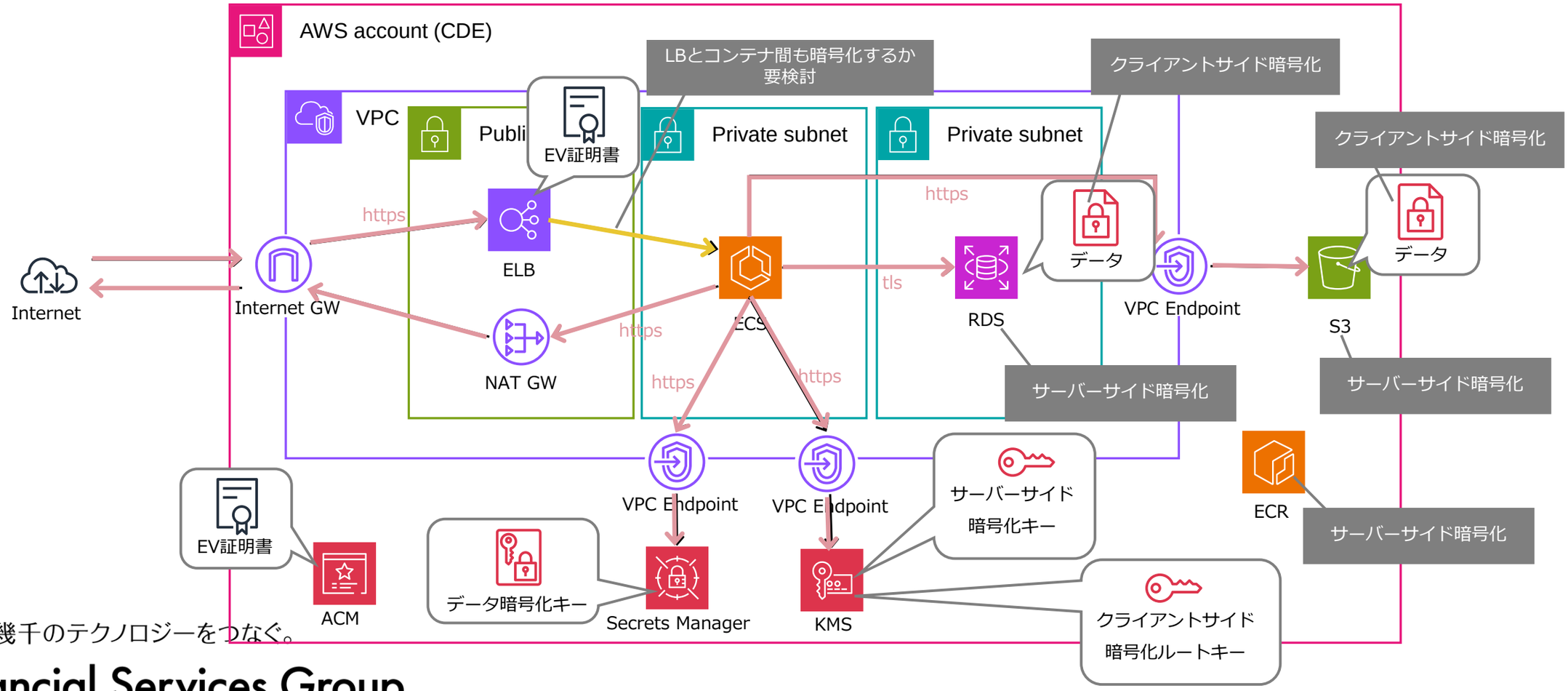


無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

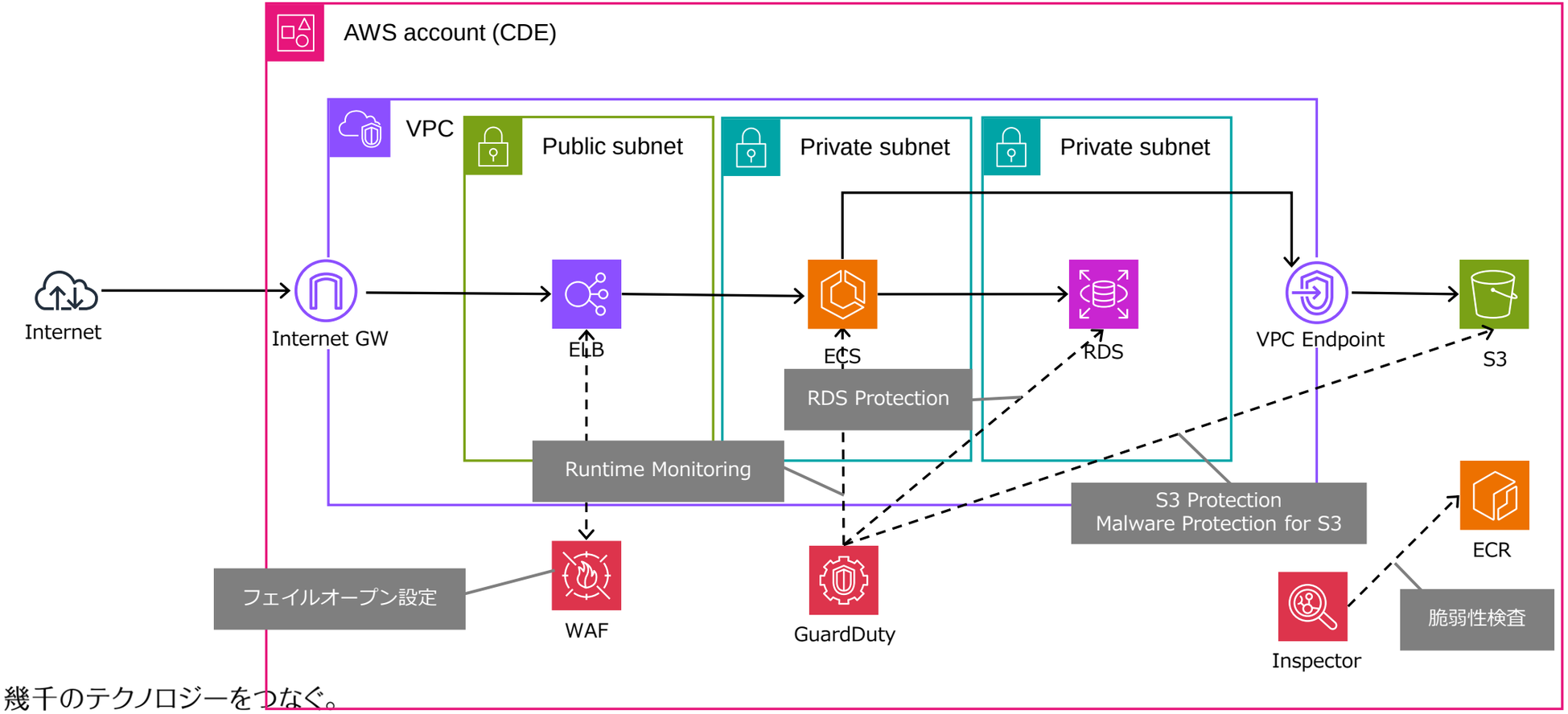
アカウントデータの保護

- 保管時のデータの暗号化と転送時のデータの暗号化をそれぞれ意識すること
- TLSの終端についても考慮すること



脆弱性管理プログラムの維持

- 可能な限りAWSのサービスを利用すること
- マルウエア対策など、必要に応じてサードパーティーのソフトウェア導入も検討すること

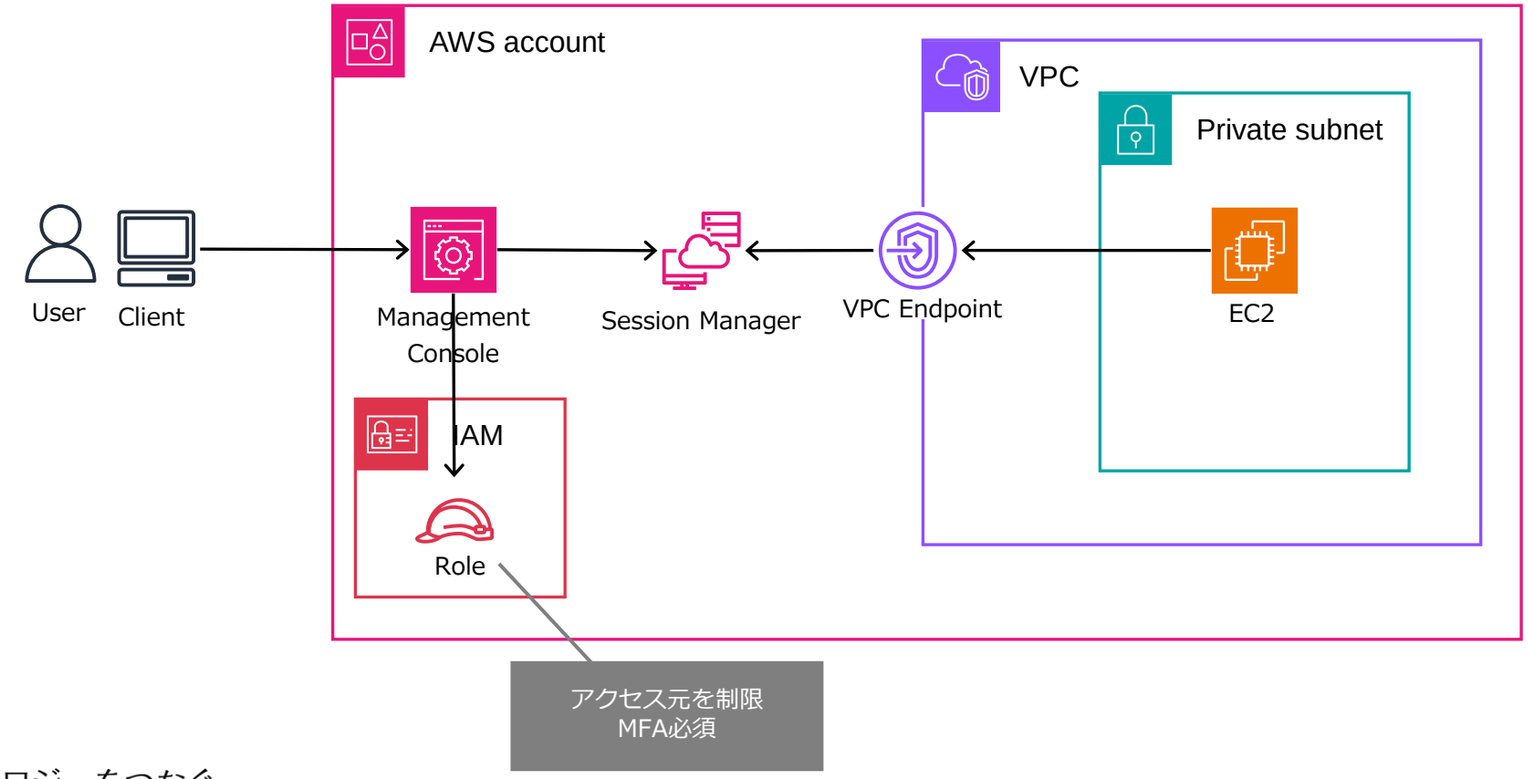


無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

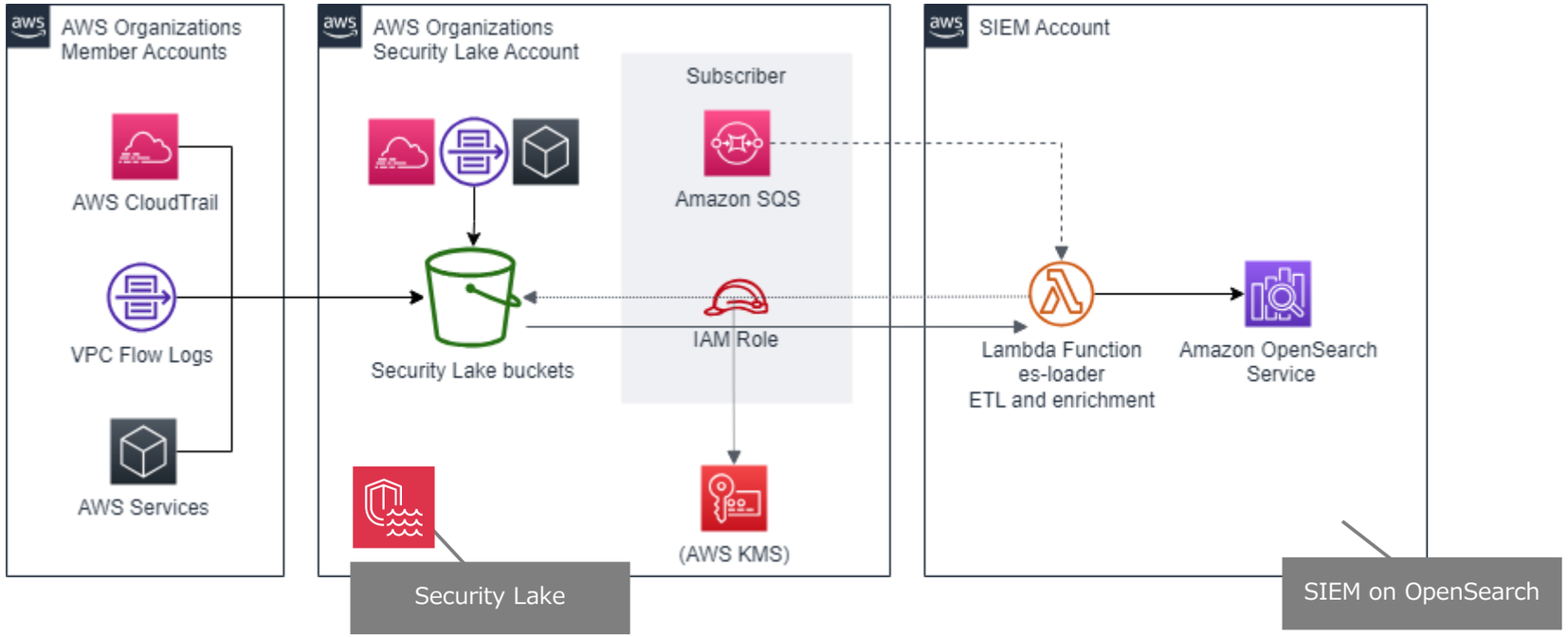
強固なアクセス制御手法の導入

- ロールとポリシーの設計をしっかりおこなうこと（最小権限の原則）
- コントロールプレーンとデータプレーンのそれぞれのアクセス制御をすること



ネットワークの定期的な監視およびテスト

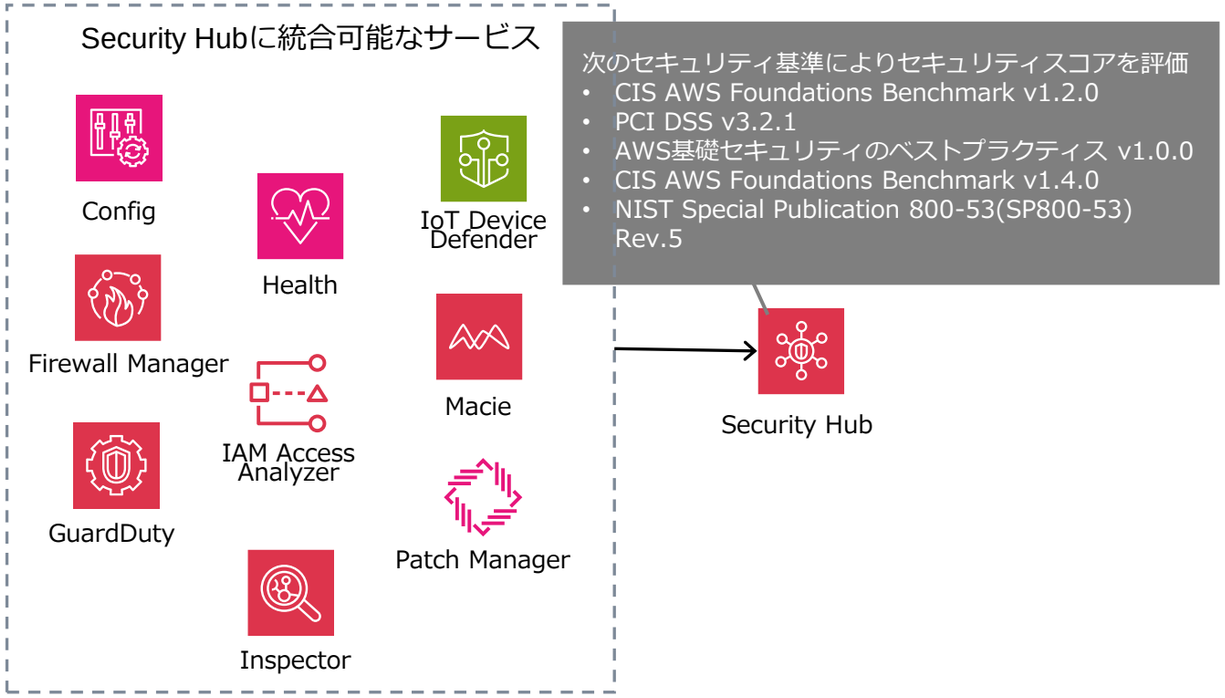
- すべてのアクセスの記録、監視ができるように抜け漏れなくログの設定をおこなうこと
- ログを集約させること



※https://github.com/aws-samples/siem-on-amazon-opensearch-service/blob/main/docs/securitylake_ja.md

情報セキュリティポリシーの維持

- 継続的に監視をすること
- 新しい脅威について情報収集すること
- 新しいサービスの利用を検討すること



※Security Bulletin (セキュリティ速報)

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

さいごに

今日おぼえて帰って欲しいこと

無限の未来と、幾千のテクノロジーをつなぐ。

CTC Financial Services Group

このはなしの教訓

- セキュリティは継続的な取り組み

  技術は日進月歩。小さな改善の積み重ねが大事。

- 守るものを明確にすることが大事

  それぞれの対策によって何を（保護対象）何から（脅威）守るのかを常に意識する。

- リスクを評価して柔軟に対応することも大事

  いろいろなトレードオフがある。リスクに応じて適切なセキュリティ対策をとることが大事。

  マネージドサービスを利用することでクラウド利用者としての責任を減らすことも考える。

無限の未来と、
幾千のテクノロジーをつなぐ。

CTC Financial Services Group

CTC
Challenging Tomorrow's Changes