カンテレのクラウドセキュリティ第一歩

関西テレビ放送株式会社
DX推進局 DX戦略部　主事　石井克典

2025/12/17

自己紹介

関西テレビ放送株式会社
DX推進局 DX戦略部　主事
石井 克典 （いしい かつのり）

配属部署：マスター(10年)→DX戦略部（6年目）
主な担務：情報システム、SaaSサービス、クラウド

好きなAWSサービス：
AWS Control Tower、AWS Security Hub CSPM

突然ですが、皆さん

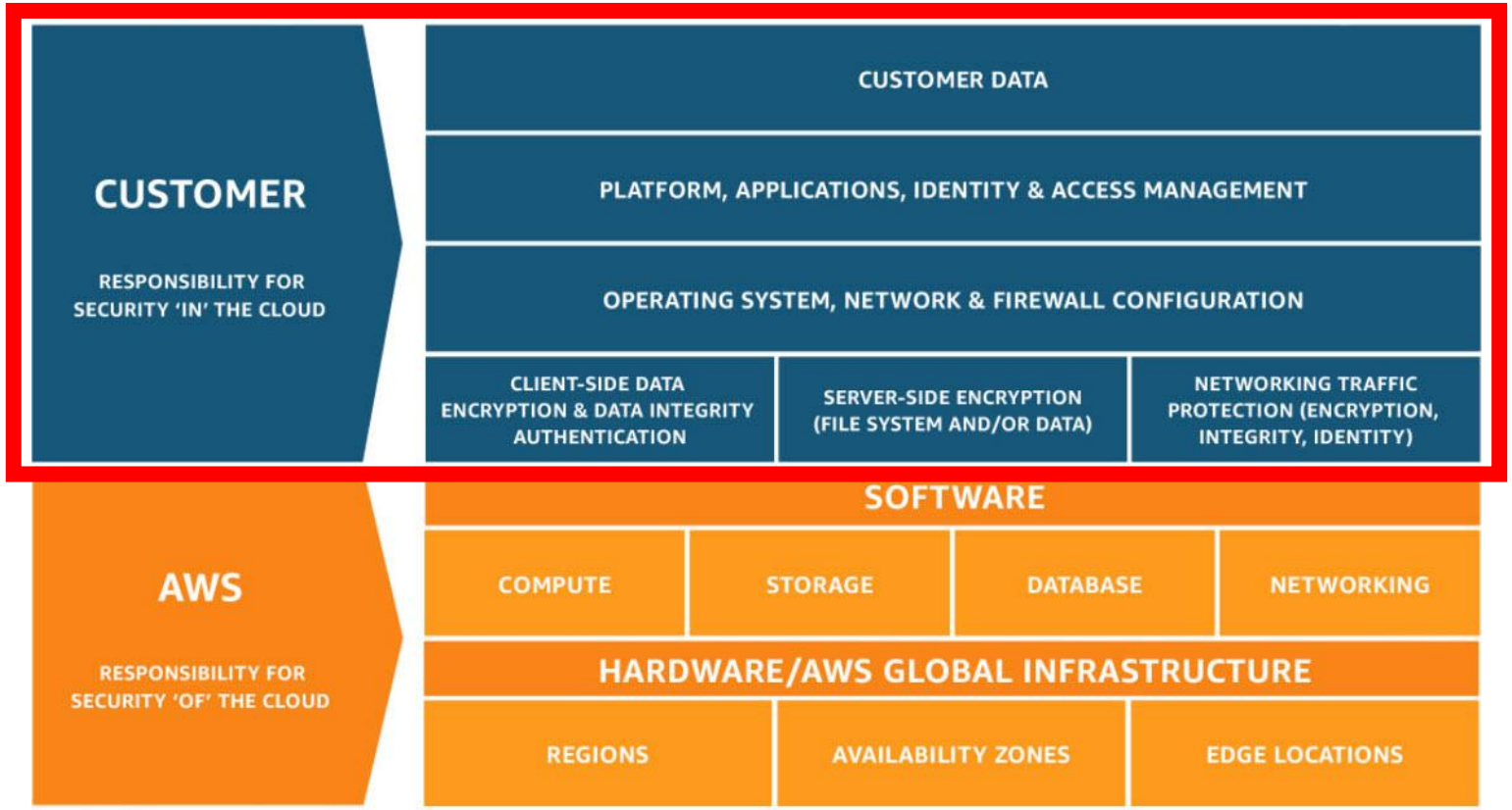
AWSの「セキュリティ」 意識してますか？

AWS責任共有モデル

AWSならセキュリティ完璧
顧客は何もしなくてもOK！！

・・・というわけではない！！

・IDやパスワードの管理
・OSのアップデート
・適切なネットワーク設計
など、すべて「顧客の責任」



責任共有モデル – Amazon Web Services (AWS)
https://aws.amazon.com/jp/compliance/shared-responsibility-model/

AWSでやりがちな「セキュリティの落とし穴」

- すべてのIAMユーザーにAdmin権限付与

  → 社員全員に会社のマスター鍵を配布する

- Amazon S3の公開設定ミス

  → 社外秘の書類を会社の前に貼り出す

- 監査ログを残していない

  → 防犯カメラを設置していない

なぜセキュリティを意識するようになったか

- ✓ AWS様からセキュリティ対策のススメ
- ✓ 2025年8月からAWS環境で会計システム本稼働
- ✓ 非開発者の石井が業務時間中にAWSを触りたかった

設計のコンセプト

- ✓ AWSのベストプラクティスに従う

  AWS セキュリティリファレンスアーキテクチャ

  https://docs.aws.amazon.com/ja_jp/prescriptive-guidance/latest/security-reference-architecture/architecture.html

- ✓ ルールはとにかくシンプル

- ✓ コードはできるだけ書かない

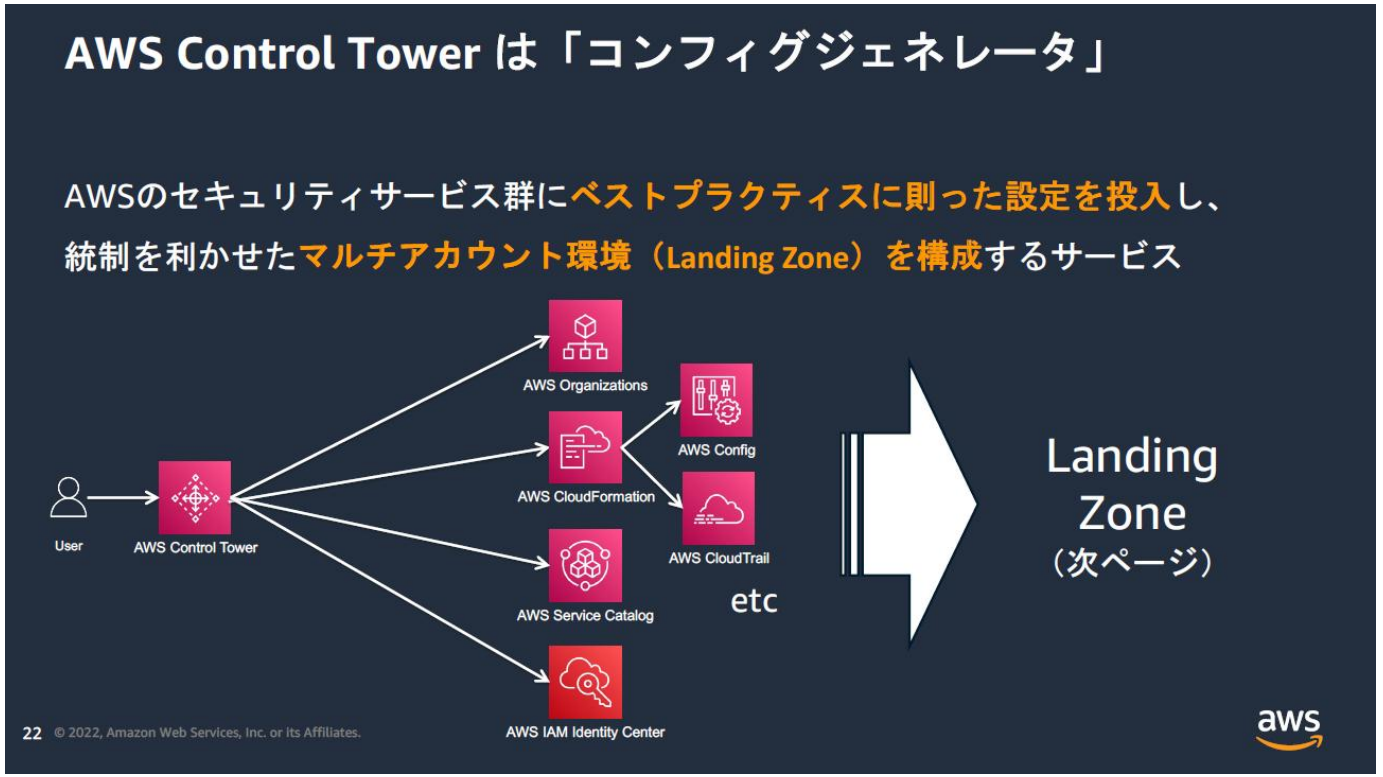
  →AWSマネジメントコンソールを使う

- ✓ 自分以外が担当になっても回るように

一番はじめにやったこと

AWS Control Towerの有効化

複数のAWSアカウントを「安全に」「一貫したルールで」「自動的に」管理するためのサービス。



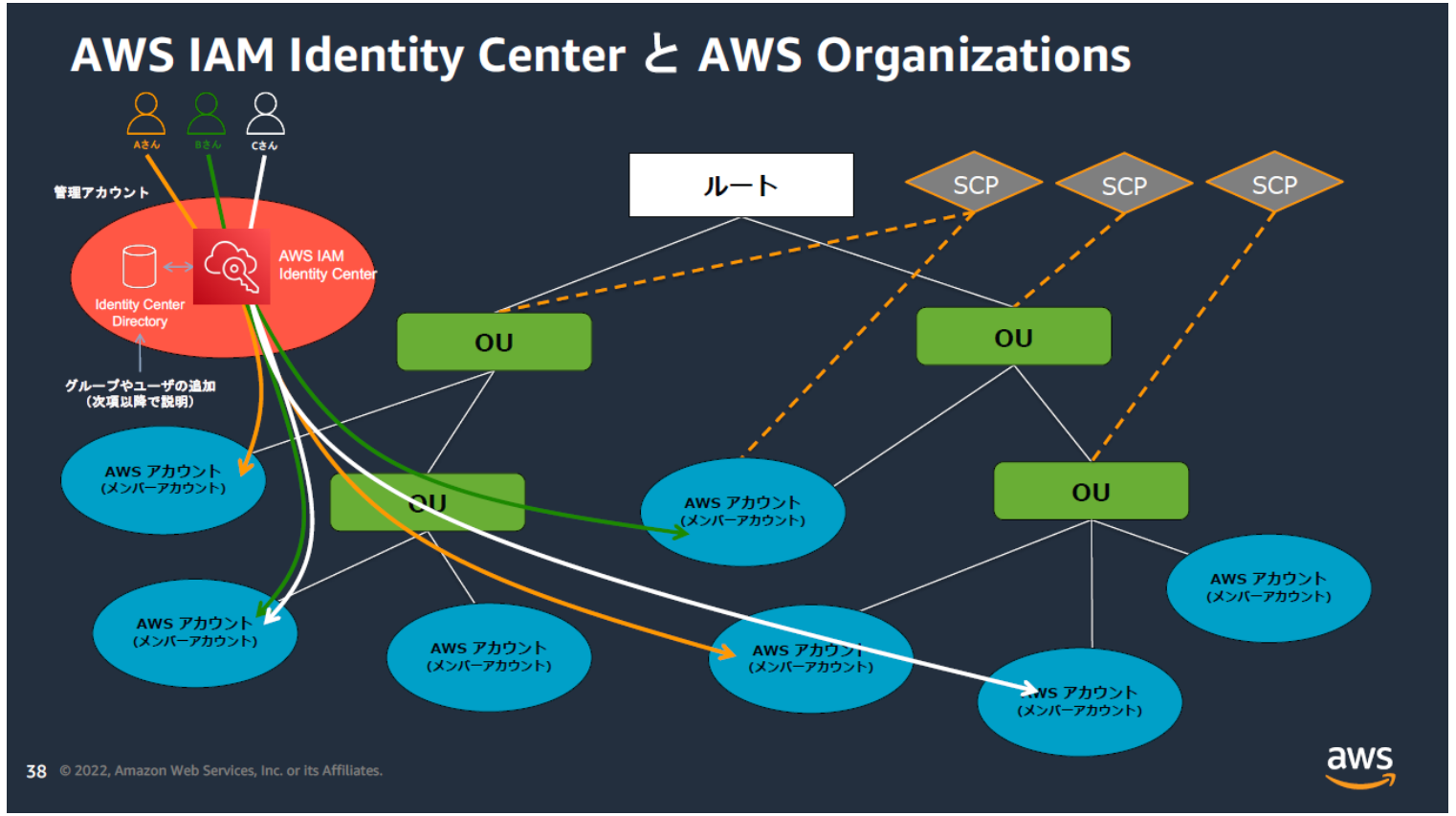
AWS Organizationsや
AWS IAM Identity Centerなど
これまではサービス個別で
設定しなければならなかったが、
AWS Control Towerなら数クリックで
マルチアカウント環境を整えられる！！

AWS Control Towerによる複数アカウントの一元管理

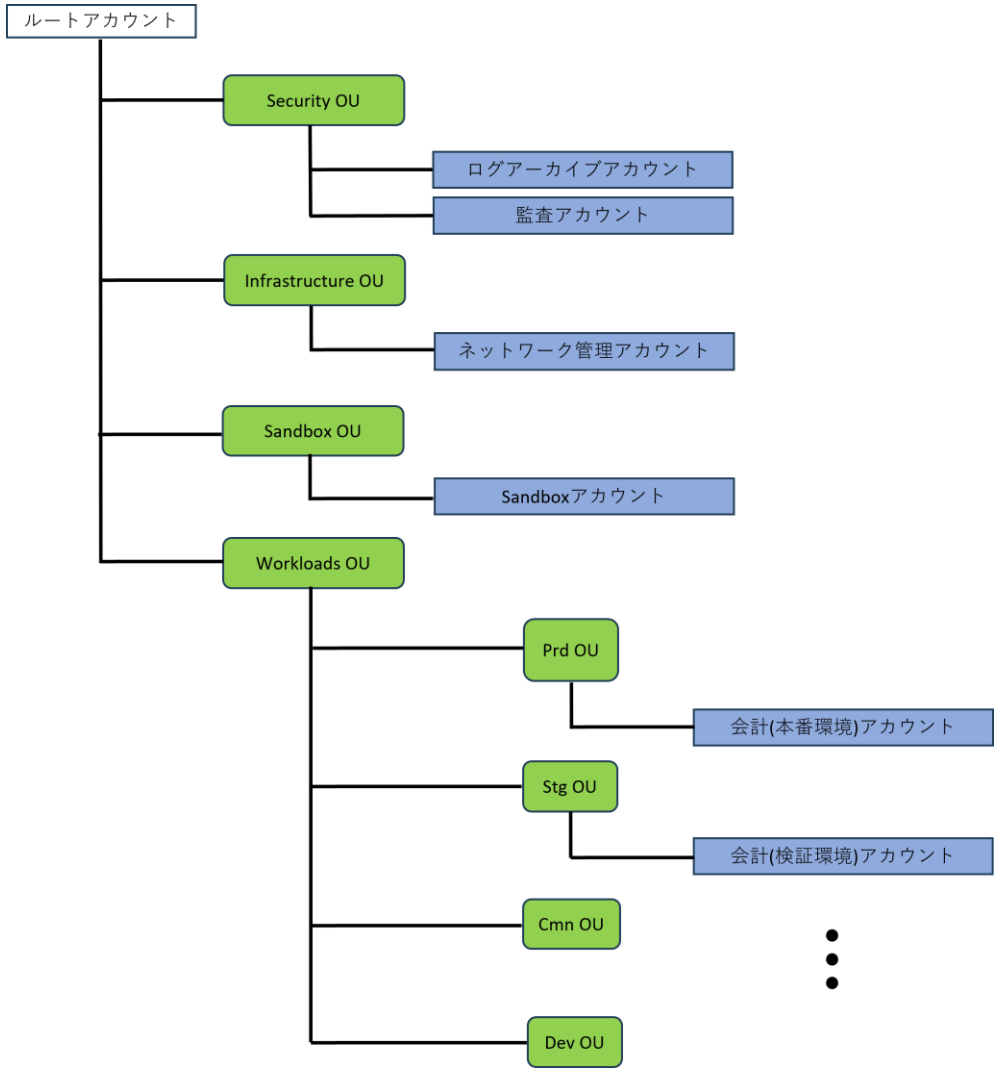
システム/用途ごとに
アカウントを分けることが重要

- セキュリティ対策の統一化
- 最小権限付与によるオペレーションミスの防止

- 請求の一元管理
- システム単位のコスト可視化



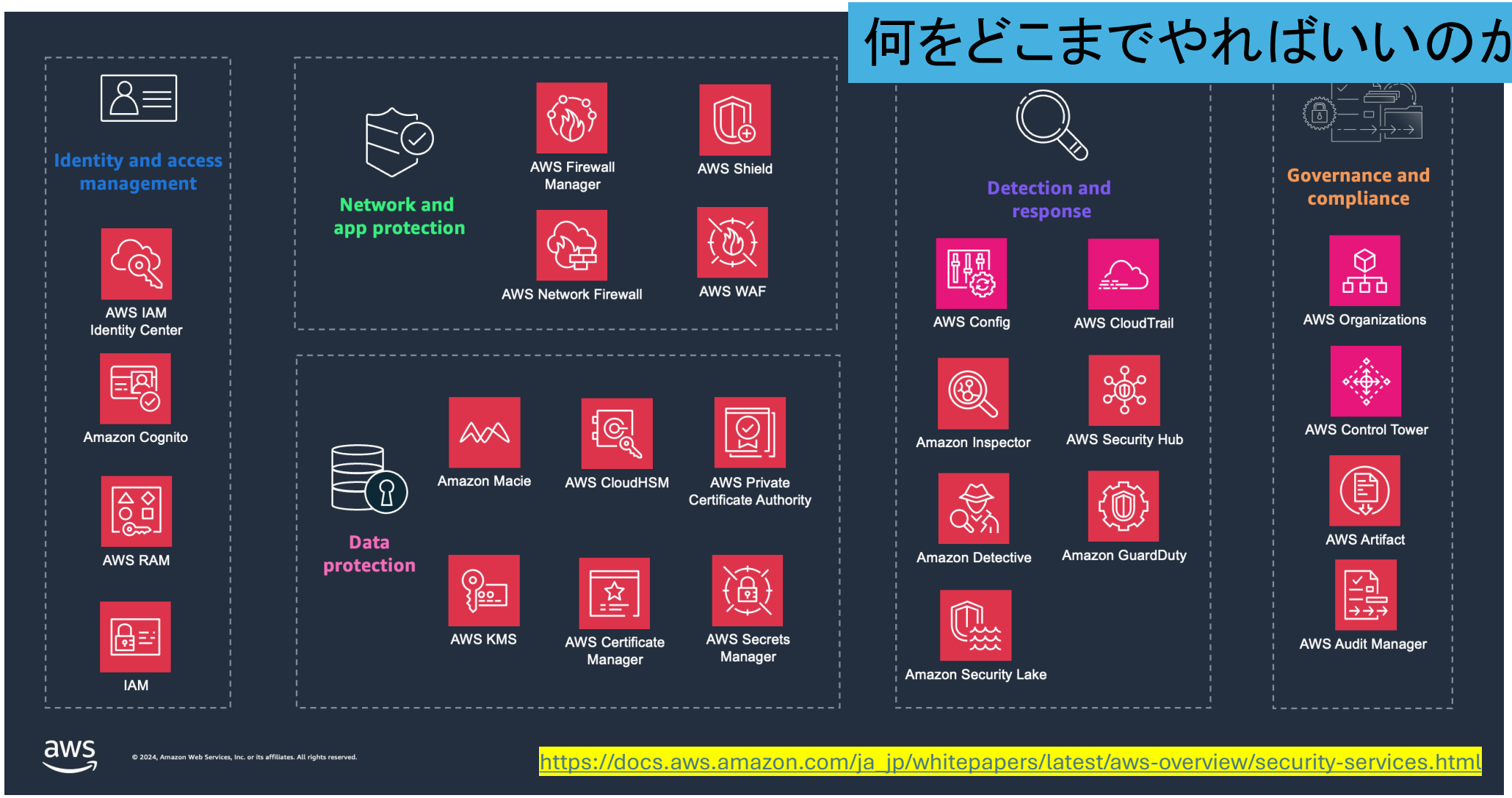
OUの設計例（カンテレの場合）



- AWSのベストプラクティスに従う
- 深いOU構造は避ける
- ルートアカウントは管理機能のみ
- メンバーアカウントはシステム/用途別
- 本番環境と非本番環境を分ける

セキュリティ関連サービス多すぎ問題

何をどこまでやればいいのか・・・



https://docs.aws.amazon.com/ja_jp/whitepapers/latest/aws-overview/security-services.html

どのように検討・構築したか

- 在阪5局共通セキュリティガイドライン策定
- アカウントSA様、サポートチームによる技術支援
- 会計システムSIerの(株)JSOL様による技術支援
- mini Security−JAWSコミュニティでの意見交換

在阪5局共通セキュリティガイドライン策定

AWS メディア業界向け勉強会 #6（2024 年 12 月 13 日開催）

【開催報告＆資料公開】AWS メディア業界向け勉強会開催報告 | Amazon Web Services ブログ

「在阪局で一緒に取り組めることを考えてみた」

在阪局共通のセキュリティガイドラインについて、参考資料となる
「AWS利用ガイドライン整備のためのセキュリティリファレンス」が完成。

→ カンテレの基本方針はこれに沿う形で検討

アカウントSA様、サポートチームによる技術支援

AWS Control Towerは構築できました。次は何から手をつければ良いでしょうか？

AWS様

Amazon GuardDutyを有効化することが最優先です。

AWS様

AWS Security Hub CSPMに「統合」という機能があり、Amazon GuardDutyやAWS Configなどの結果をアカウントをまたいで一か所に集約することができます。

管理が楽になりますね。一か所に集約する方向で進めます。

AWS様

AWS IAM Access Analyzerの設定をおすすめします。
組織内のリソースに対して、外部からアクセスが可能であるかを検出します。

意図しない外部アクセスに対処することができますね。有効化したいと思います。

会計システムSIerの(株)JSOL様による技術支援

JSOL様

AWS Organizations を使用するお客様のためのルートアクセスの一元管理 | Amazon Web Services ブログ

新しい機能がリリースされるようです。

セキュリティ関連のサービスを順次有効にしていきたいのですが、
一般的な企業の対策として漏れがあればアドバイスいただけないでしょうか？

JSOL様

主要なサービスは網羅できているかと思います。
あとはAWS Trusted Advisorのチェック項目をどこまで考慮するかによりますね。

Amazon Macieを有効にしましたが、会計システムが利用している特定のS3バケットのみ
チェックできていないようです。対応可能でしょうか？

JSOL様

S3バケットがKMSで暗号化されているためです。
KMSのキーポリシーで復号化を許可する設定を行いました。

mini Security−JAWSコミュニティでの意見交換

コミュニティ有志

自分に出来ないことはやらないほうが良いです。責任が取れないのであれば、やれる人にやってもらう。
例えば、マルウェアの調査は自社でやらず、外部の専門業者にまかせるなど。

ログの保存期間をどう決めるか悩んでいます。

コミュニティ有志

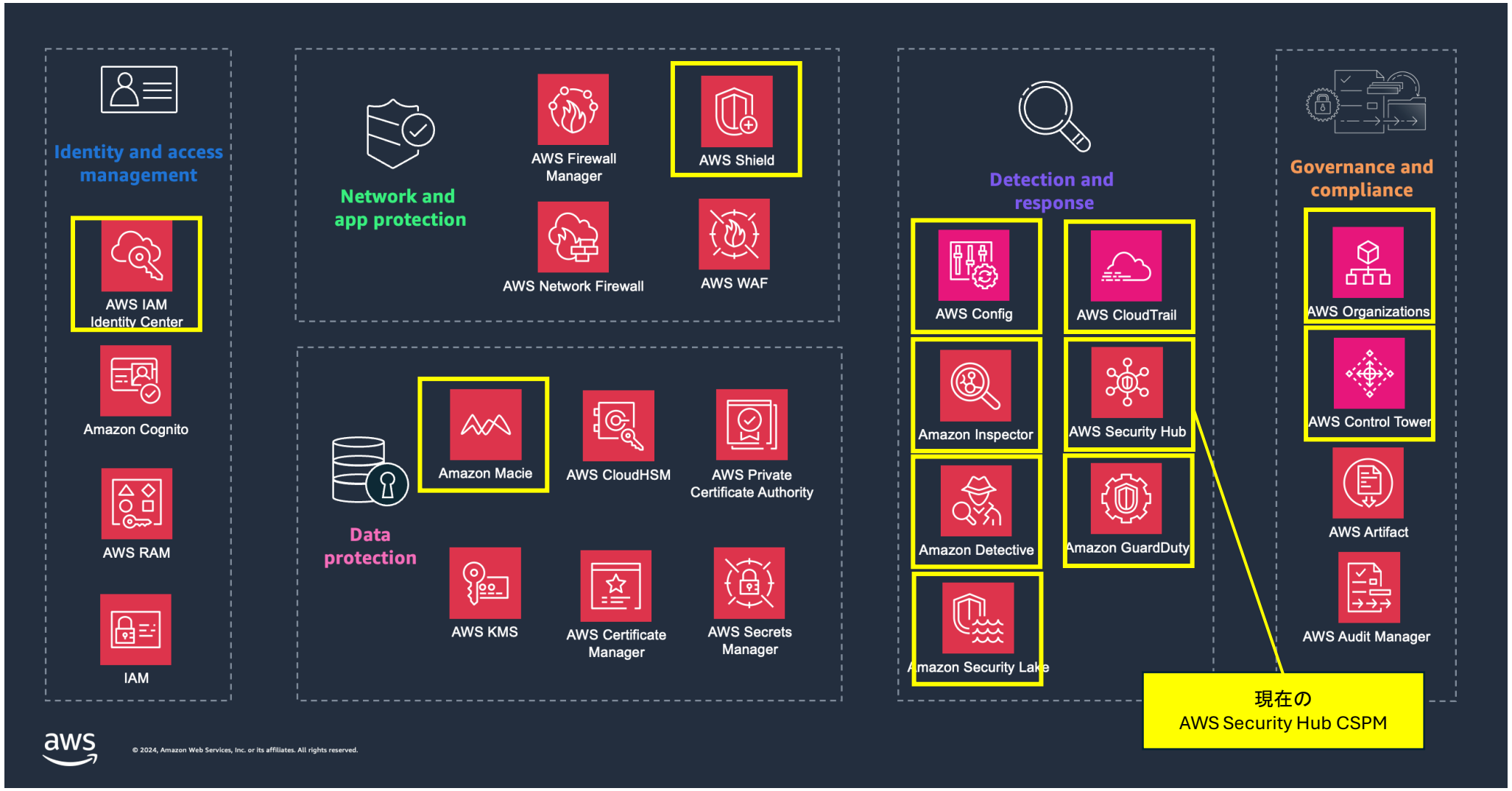
不正アクセス禁止法違反の時効（3年）、電子計算機使用詐欺罪の時効（7年）など、法律を参考に。
コストが把握できるかどうかが重要。最後は決めの問題ですね。

できるだけ多くのログを長い期間保持するように進めていますが、次はログをどのように可視化しますか？
セキュリティ事故が起きた場合、ログ調査は外部のSoCサービスに依頼しても良いでしょうか。

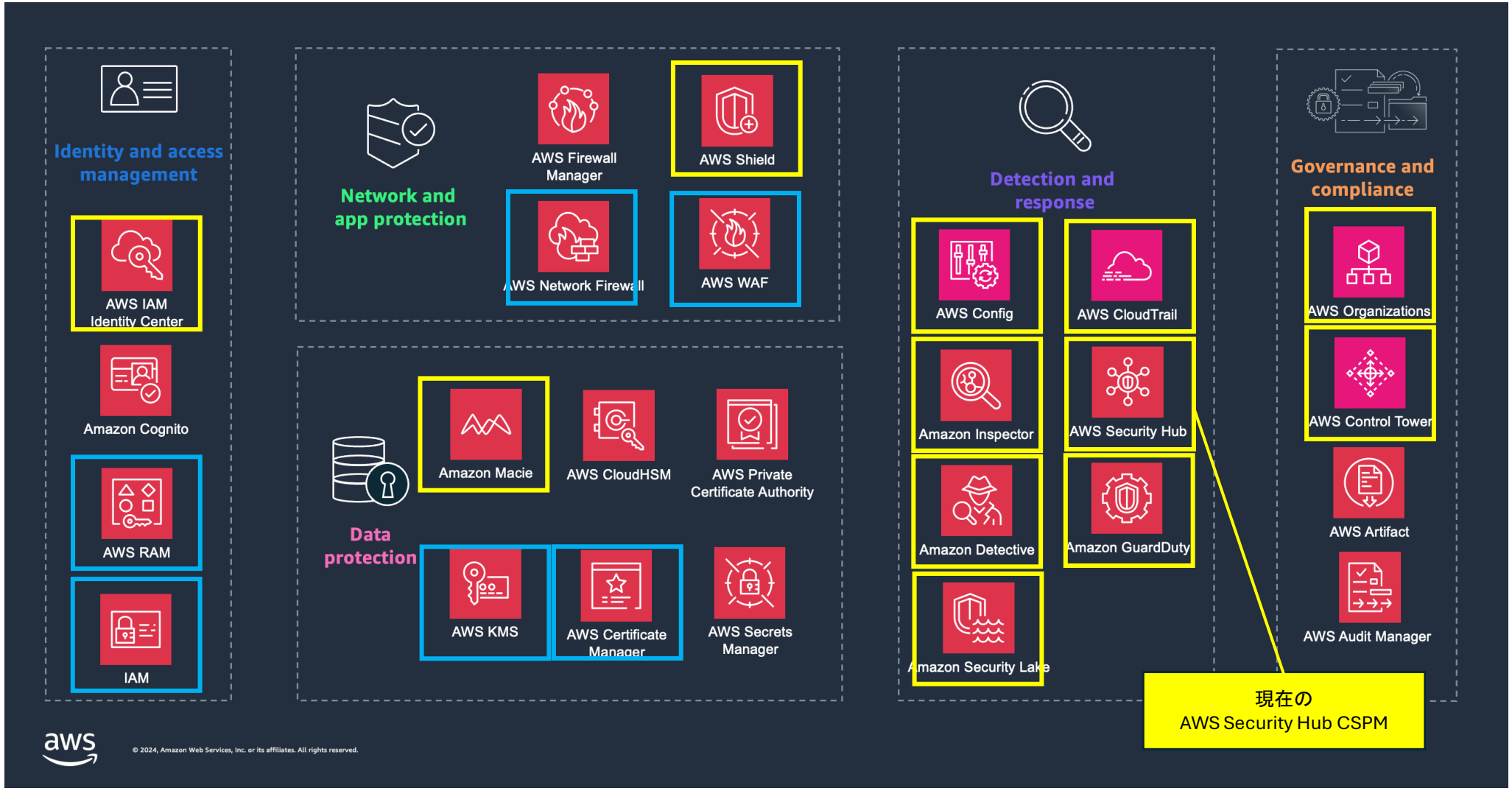
コミュニティ有志

ログの調査は自社でやらなくて良いです。むやみに可視化する必要はありません。
Amazon GuardDutyとAWS Security Hub CSPMに任せてください。使いこなせるようになってから
ログの可視化、SIEMの仕組みを入れてください。自分たちで活用するのはかなり進んだ段階です。

現在有効にしているサービス（各アカウント共通のみ記載）



【参考】会計システムアカウント



AWS Control Towerのリージョン拒否コントロール

指定したリージョン以外のリージョンへアクセスできなくなる機能。
セキュリティ向上や予期せぬ課金防止に有効。

カンテレでアクセス可能なリージョンは以下5リージョンのみ。

us-east-1（バージニア北部）、us-west-2（オレゴン）、eu-west-1（アイルランド）、ap-northeast-1（東京）、ap-northeast-3（大阪）

※自社で設定される場合は影響範囲に注意してください。

AWSにおけるセキュリティの適正なコストとは？

IT予算のうち、セキュリティ関連費用は5～15%の企業が多い

AWS全体の利用料のうち、現在10%以内に収まっている

何から手をつければいいかわからない方へ

「AWSセキュリティ成熟度モデル」に当てはめてチェック可能。

レベル1．クイックウィン
レベル2．基礎
レベル3．効率化
レベル4．最適化

レベル2．基礎 までできたら安心

ホーム :: AWS セキュリティ成熟度モデル　https://maturitymodel.security.aws.dev/ja/

まず以下をやる！！

- 「AWSセキュリティ成熟度モデル」のレベル1．クイックウィン
- 「AWS利用ガイドライン整備のためのセキュリティリファレンス」の必須事項

それでも難しい方へ

- 複数アカウントの一元管理を検討
- AWS Control Towerを有効化、リージョン拒否設定
- Amazon GuardDutyを有効化
- AWS Security Hub CSPMを有効化、「CRITICAL」判定を対処

今後の課題と展望

- 各種ログをいつまで残すかの検討
- カンテレ個社のセキュリティガイドライン策定
- AWSセキュリティ成熟度モデルのチェック
- 他部署が保有するAWSアカウントの巻き取り
- AWSを運用するための持続的な体制作り（現在３名）
- セキュリティ運用の自動化（いかに少ない人数で回せるか）
- AWS人材育成
- マルチクラウド戦略

AWS様への要望

- サービスごとにアカウントを分けているため、有償サポートの費用がかさみます。Enterpriseプランは高すぎます・・・

  Amazon Security Lakeはログアーカイブアカウントに集約、
  AWS Security Hub CSPMは監査アカウントに集約、など。

- AWS Control Tower配下でメンバーアカウントを新規作成したとき、デフォルトから変更する作業があります。
  「AWS CloudFormationを使ってください」ということになりますが、
  テンプレートをメンテナンスする人員を維持するのが難しいです。

- Amazon Detectiveの大阪リージョン対応

まとめ

- セキュリティの脅威は日進月歩。単一のセキュリティ対策を入れて終わりではなく、常に回し続けなければならない。
- セキュリティは「競争領域」ではなく「協調領域」。
  業界全体で高めあっていきたい！
- 社外のコミュニティ活動にも積極的に参加するべし。

Security-JAWS激しくおススメ

Security-JAWS – connpass　https://s-jaws.connpass.com/

mini Security-JAWS Docs　https://mini-study.security.jaws-ug.jp/