明日から簡単に始められる！

AWSセキュリティ対策

自己紹介

JIG-SAW株式会社

事業推進室 マネージャー

池川　健太郎

担当業務

自社開発のクラウドセキュリティSaaSの事業推進

本セッションのゴール

AWS環境でよくある脅威を事例ベースで知り
対策するためのＡＷＳセキュリティサービスを理解する

AWSのセキュリティ対策で多くの方が抱える課題感

- 社内や顧客からセキュリティの対策を求められるが
  具体的に何をすればいいか分からない
- AWSのセキュリティサービスが多すぎて、選び方がわからない
- セキュリティサービスを有効化しただけで活用できていない
- セキュリティインシデントが発生しても気づける仕組みや体制がない

AWSセキュリティ対策の流れ

1. セキュリティインシデント発生時のリスクを把握する
2. 対策したいセキュリティ課題を把握する
3. 現在のセキュリティサービスの設定と活用状況を把握
4. 最適なサービスの選定、運用方法の決定
5. セキュリティサービスの導入・運用の改善

AWSのセキュリティサービスMAP

ID/アクセス管理

ユーザーアクセス管理

AWS IAM

マルチアカウント管理

AWS Organizations

AWS IAM Identity Center

AWS Control Tower

検出/モニタリング

設定監査

AWS Security Hub

AWS Config

不正アクセス検出

Amazon GuardDuty

Amazon Detective

OS脆弱性検出

Amazon Inspector

情報漏洩対策

Amazon Macie

セキュリティログモニタリング

AWS CloudTrail

Amazon CloudWatch

アプリケーションセキュリティ

Webセキュリティ対策

AWS WAF

データセキュリティ

データ保護対策

AWS Backup

DR対策

AWS Backup

AWS Elastic Disaster Recovery (AWS DRS)

ネットワークセキュリティ

不正アクセス対策

AWS Network Firewall

Amazon Route 53

運用管理

パッチ適用自動化

AWS Systems Manager

AWSのセキュリティサービスMAP

本資料ではID/アクセス管理と
検出/モニタリングを紹介

ID/アクセス管理

ユーザーアクセス管理

AWS IAM

マルチアカウント管理

AWS Organizations

AWS IAM Identity Center

AWS Control Tower

検出/モニタリング

設定監査

AWS Security Hub

AWS Config

不正アクセス検出

Amazon GuardDuty

Amazon Detective

OS脆弱性検出

Amazon Inspector

情報漏洩対策

Amazon Macie

セキュリティログモニタリング

AWS CloudTrail

Amazon CloudWatch

アプリケーションセキュリティ

Webセキュリティ対策

AWS WAF

データセキュリティ

データ保護対策

AWS Backup

DR対策

AWS Backup

AWS Elastic Disaster Recovery (AWS DRS)

ネットワークセキュリティ

不正アクセス対策

AWS Network Firewall

Amazon Route 53

運用管理

パッチ適用自動化

AWS Systems Manager

セキュリティ
インシデント例

I

ストレージが公開され情報漏洩

事　象

- Amazon S3の閲覧制限が不必要に付与されていたことで、個人情報の漏洩につながった

原　因

- Amazon S3の誤った公開設定
  - 読み取りアクセスの公開設定
  - 書き込みアクセスの公開設定

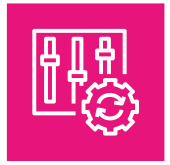
対　策

- 公開されているS3バケットを検出し、誤った公開設定を修復する
- 誤った公開設定ができない仕組みを設定する

利用するAWSセキュリティサービス

AWS Security Hub

- AWS のセキュリティチェックの自動化とセキュリティアラートの一元化をする機能
- パブリックアクセスが可能なS3バケットを検出するため、設定ミスが発生しているS3バケットを検出できる



AWS Config

- リソースの構成を監査、評価する機能
- 公開設定のバケットをリストアップ
- 公開設定としてしまった場合の自動修復設定

セキュリティ
インシデント例

Ⅱ

OS/ミドルウェアの脆弱性を突かれてウイルス感染

事　象

- 古いOSやミドルウェアの脆弱性が、ウイルス/マルウェアの感染経路となる

原　因

- 最新のOS/ミドルウェアにアップデートが行われていないため重大な脆弱性がある
- 脆弱性を検出し、脅威、影響度合いを把握する仕組みがない

対　策

- 定期的なOS/ミドルウェアの診断をし、脆弱性を発見する
- 発見した脆弱性に対するアップデートを適用する

CVE(共通脆弱性識別子）とは

- 「Common Vulnerabilities and Exposures 」の略称
- 日本語では「共通脆弱性識別子」
- 米国政府の支援を受けた非営利団体のMITRE社によって一般公開されている
  情報セキュリティの欠陥（脆弱性）をデータベース化したもの
- それぞれ固有の名前やID番号が付けられている
- 脆弱性検査ツールや脆弱性対策情報提供サービスの多くがCVEを利用している

利用するAWSセキュリティサービス

Amazon Inspector

- Amazon EC2 インスタンス、コンテナ、Lambda 関数などのワークロードを自動的に検出し、ソフトウェアの脆弱性や意図しないネットワークの露出がないかをスキャン
- CVE情報を元にリスクスコアを作成

AWS Systems Manager

Patch Manager

- Patch Manager はAWS Systems Manager の一機能
- OSやミドルウェアのアップデートを自動化

セキュリティインシデント例

III

暗号資産(仮想通貨)の不正マイニングにリソースが使われた

事　象

- 仮想通貨マイニングのために不正にリソースを使用される

原　因

- Amazon EC2やAmazon ECSでホストされるOSやコンテナの脆弱性を突いたマルウェア感染
- IAMユーザーやアクセスキーが乗っ取られ不正にマイニング用インスタンスが立ち上げられる

対　策

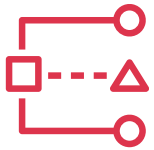
- アンチマルウェアソフトを導入する
- IAMユーザーにMFAを設定する
- 不正なアクティビティやマルウェア感染を検出する仕組みを設定する

利用するAWSセキュリティサービス

Amazon GuardDuty

- 人による作業やサードパーティーのツールを必要とすることなく、AWS アカウントの脅威検出が可能
- 不正なアクティビティやマルウェアの感染を自動で検知

AWS IAM



IAM Access Analyzer

- IAM Access AnalyzerはAWS IAMの一機能
- AWSリソースに紐づいているポリシーを検査し、管理者として意図せぬ公開設定がされていないかを検出

本日のゴール（再掲）

AWS環境でよくある脅威を事例ベースで知り
対策するためのＡＷＳセキュリティサービスを理解する

セキュリティの知識

- 専門性、スキルをもった人材がいない
- セキュリティ対策の方法がわからない
- インシデントの検知基盤を構築したい

AWSの知識

- AWSのセキュリティに詳しいエンジニアがいない
- AWSのセキュリティ対策が可能なエンジニアがいない
- AWSのベストプラクティスに沿った最適化を行いたい

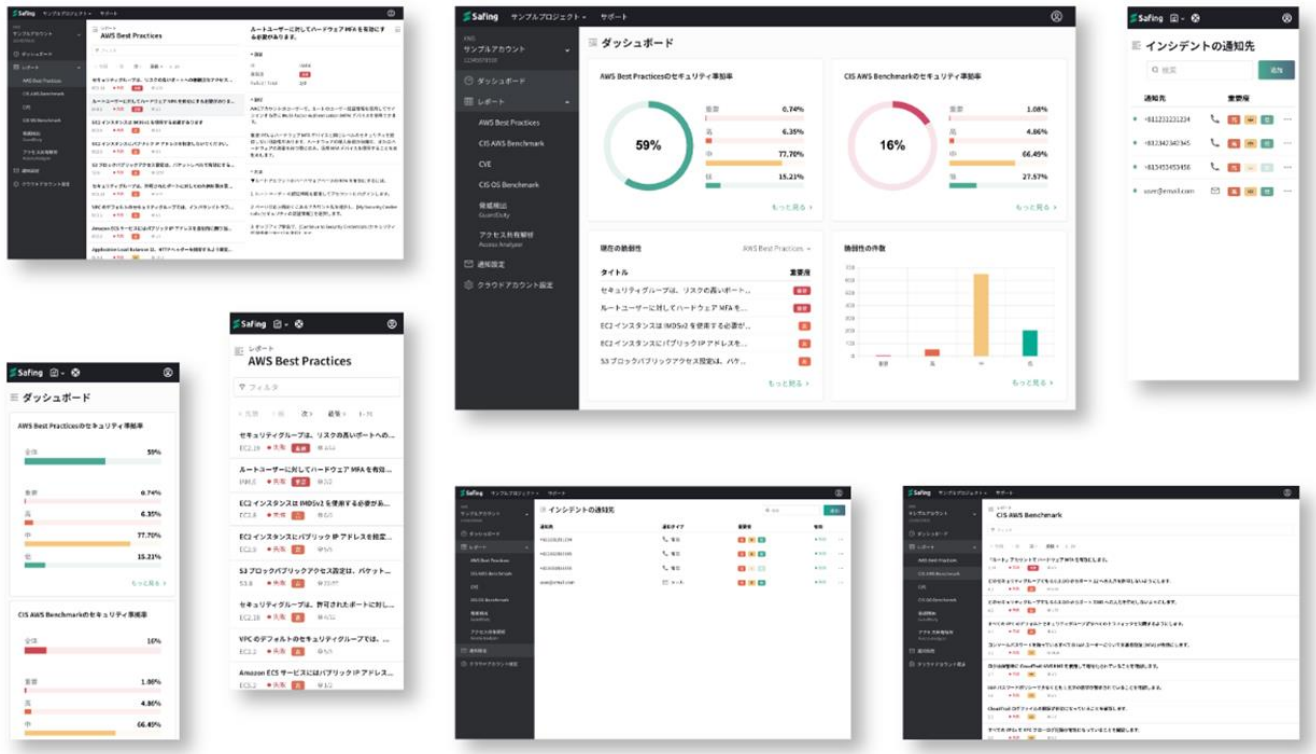
人員・体制

- 調査や対応検討の為の工数確保が難しい
- 24時間365日のセキュリティ検知の体制がない
- 新しい脆弱性を追従する為の体制がない

Safing(セーフィング)で
クラウドセキュリティを一元管理

Safingは、AWSを安全に利用し続けるために、クラウドセキュリティをまとめて管理できるサービスです。

Safing



Safingをご利用いただくことで、
AWS Security HubやAmazon Inspectorによる
脆弱性情報や、Amazon GuardDutyや
IAM Access Analyzerが検出する脅威通知を
まとめて管理できます。
サービスの詳細情報はこちら

無償トライアル実施中

詳細は次のページ

AWS Summit Japan限定 Safingクーポン

Safing

AWS Summit Japan 2024

来場者特典

最大3カ月無料
トライアルクーポン

お問合せフォームにキーワードを入力いただき申請いただくと
ご利用開始当月+2カ月間、Safingビジネスプランを無償でご利用いただけます。

こちらから申請!

キーワード：ASJ2024

有効期限：2024/12/15
裏面の申請方法をご参照の上、
お問合せフォームより申請ください。

https://safing.com/ja/

JIG-SAW

JIG-SAW株式会社
〒100-0005 東京都千代田区丸の内1丁目4-1丸の内永楽ビルディング23F
03-6269-9810 （受付時間 平日9:30−18:30）

申請方法

STEP 01 https://safing.com/ja/ へアクセスし「導入前のお問合せ」をクリック

STEP 02 「お問い合わせ内容」に表面のキーワードを入入力し「送信」

STEP 03 お問合せ時に入力いただいたメールアドレスに
プロモーションコードと開始手順をご案内いたします。