



セキュリティにおける

# AWS Well-Architected フレームワークの活用方法

アマゾン ウェブ サービス ジャパン株式会社  
Well-Architected Lead PSA (Japan) 大場 崇令

2020/11/25



AWS Well-Architected

# 本日の対象者

クラウドのセキュリティに悩まれている方

クラウドセキュリティのベストプラクティスを知りたい方



# 今日のゴール

AWS Well-Architected フレームワーク の概要を理解する

セキュリティにおける AWS Well-Architected  
フレームワーク の活用方法を理解する



# Who am I ?



## □ 大場 崇令 (オオバ タカノリ)

- Partner Solutions Architect  
@Amazon Web Services Japan K.K.  
(Joined 2015/12)



## □ Background

- AWS テクニカルトレーナー@AWSJ K.K.
- Web サービスのインフラエンジニア
- 国内クラウドベンダーにてテクニカルサポート

## □ 好きな AWS サービス

- AWS Well-Architected Tool
- AWS Systems Manager
- AWS Service Catalog



Well-Architected Lead

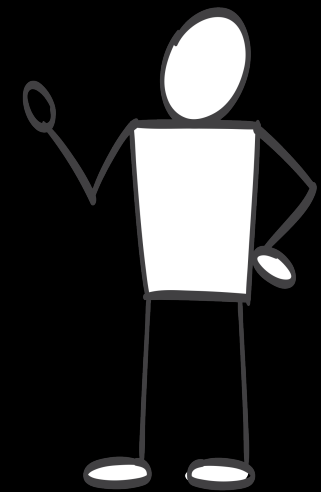
# よくあるクラウド導入の課題と不安



オンプレミスでの経験は豊富だが、  
クラウド最適化のための  
設計・運用のノウハウが無い…

基本的にオンプレミスの経験や知識が  
活用できますので、ご安心ください

+  $\alpha$ として、よりクラウド効率的に  
使うためのノウハウもまとまっています





# AWS Well-Architected フレームワーク

<https://aws.amazon.com/well-architected/>

---

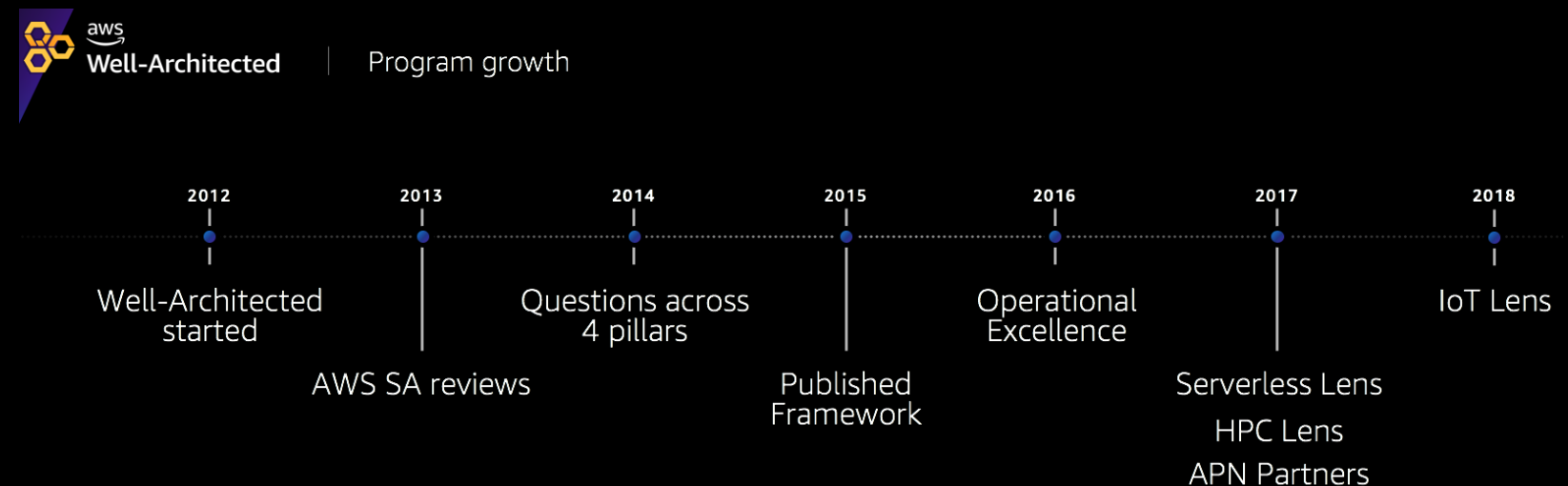
# AWS Well-Architected フレームワーク (W-A) とは?

## システム設計・運用の”大局的な”考え方と ベストプラクティス集

・ AWS のソリューションアーキテクト (SA)、  
パートナー様、お客様の 10 年以上にわたる  
経験から作り上げたもの



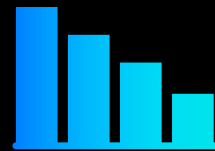
・ AWS とお客様と共に、  
W-A も常に進化し続ける



# Why AWS Well-Architected フレームワーク?



ビルドとデプロイを高速化



リスクを緩和または軽減



データドリブンで決定



AWS のベストプラクティスを学ぶ



# AWS Well-Architected フレームワーク とは？



柱

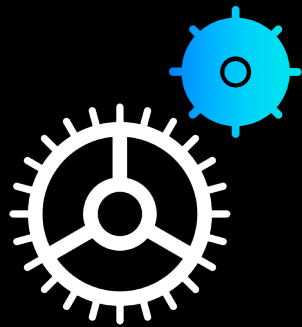


設計原則  
(Design principles)



質問

# AWS Well-Architected フレームワークの 5 本の柱



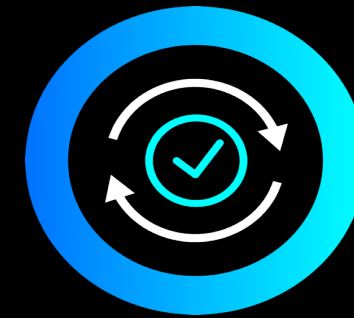
運用の優秀性



セキュリティ



信頼性



パフォーマンス  
効率



コスト最適化

# 設計原則 (Design principles)



一般的な設計原則



柱固有の設計原則

セキュリティイベントへの備え：  
インシデント対応シミュレーションを実行し、自動化されたツールを  
使用して、検出、調査、復旧のスピードを上げる

# W-A における設計原則 (Design Principles)

必要なキャパシティを勘に頼らない

---

本番規模でのシステムテストを行う

---

アーキテクチャ試行の回数を増やすために自動化を取り入れる

---

発展的なアーキテクチャを受け入れる

---

データ計測に基づいてアーキテクチャを決定する

---

本番で想定されるトラブルをあらかじめテストし、対策する

---



# 各柱における設計原則 (Design Principles)

## 運用の優秀性の柱

- コードで運用する
- 定期的に、小規模な、元に戻すことができる変更を適用する
- 運用手順を定期的に改良する
- 障害を予測する
- 運用上のすべての失敗から学ぶ

## セキュリティの柱

- 強力なアイデンティティ基盤を導入する
- 追跡可能性を有効にする
- すべてのレイヤーにセキュリティを適用する
- セキュリティのベストプラクティスを自動化する
- 転送中および保管時のデータを保護する
- 人をデータから遠ざける
- セキュリティイベントに備える

## 信頼性の柱

- 復旧手順をテストする
- 障害からの復旧を自動化する
- システム全体の可用性を向上するために水平方向にスケールする
- キャパシティの判断を感に頼らない
- オートメーションで変更を管理する

## パフォーマンス効率の柱

- 最新のテクノロジーを標準化する
- 数分で世界中にデプロイする
- サーバーレスアーキテクチャを使用する
- 実験の頻度を増やす
- システムを深く理解する

## コスト最適化の柱

- クラウド財務管理の実装
- 消費モデルを導入する
- 全体的な効率を測定する
- データセンター運用への投資をやめる
- 支出を分析し、帰結させる
- 所有コストを低減させるためにマネージドサービスを使用する



# セキュリティの柱における 設計原則

強力なアイデンティティ基盤を導入する

---

追跡可能性を有効にする

---

すべてのレイヤーにセキュリティを適用する

---

セキュリティのベストプラクティスを自動化する

---

転送中および保管時のデータを保護する

---

人をデータから遠ざける

---

セキュリティイベントに備える

---



# 質問と回答形式でのベストプラクティス(例)

## インフラストラクチャ保護

Sec6 コンピューティングリソースをどのように保護していますか?

ワークロード内のコンピューティングリソースを内外の脅威から守るには、複数の防御レイヤーを設ける必要があります。コンピューティングリソースには、EC2 インスタンス、コンテナ、AWS Lambda 関数、データベースサービス、IoT デバイスなどがあります。

- 脆弱性管理を実行する
- 攻撃領域を削減する
- マネージドサービスを活用する
- コンピューティング保護を自動化する
- ユーザーが遠距離でアクションを実行できるようにする
- ソフトウェアの整合性を検証する

柱の分野

質問文

質問のコンテキスト

ベストプラクティス



# セキュリティの柱における 10 の質問

SEC 1. ワークロードを安全に運用するには、どうすればよいですか？

SEC 6. コンピューティングリソースをどのように保護していますか？

SEC 2. ユーザー ID とマシン ID はどのように管理したらよいでしょうか？

SEC 7. どのようにデータを分類していますか？

SEC 3. 人とマシンのアクセス許可はどのように管理すればよいでしょうか？

SEC 8. 保管時のデータをどのように保護していますか？

SEC 4. セキュリティイベントをどのように検出し、調査していますか？

SEC 9. 転送時のデータをどのように保護していますか？

SEC 5. ネットワークリソースをどのように保護しますか？

SEC 10. インシデントの予測、対応、復旧はどのように行いますか？





# 質問と回答形式でのベストプラクティス(例)

## 例：セキュリティの質問(抜粋)

[SEC2] ユーザー ID とマシン ID はどのように管理したらよいでしょうか？

- 強力なサインインメカニズムを使用する
- 一時的な認証情報を使用する
- シークレットを安全に保存して使用する
- 一元化された ID プロバイダーを利用する
- 定期的に認証情報を監査およびローテーションする
- ユーザーグループと属性を活用する



# 質問と回答形式でのベストプラクティス(例)

## 例：セキュリティの質問(抜粋)

[SEC2] ユーザー ID とマシン ID はどのように管理したらよいのでしょうか？

- 強力なサインインメカニズムを使用する
- 一時的な認証情報を使用する
- シークレットを安全に保存して使用する
- 一元化された ID プロバイダーを利用する
- 定期的に認証情報を監査およびローテーションする
- ユーザーグループと属性を活用する



# 質問と回答形式でのベストプラクティス(例)

## 例：セキュリティの質問(抜粋)

[SEC2] ユーザー ID とマシン ID はどのように管理したらよいのでしょうか？

- 強力なサインインメカニズムを使用する
- 一時的な認証情報を使用する
- シークレットを安全に保存して使用する
- 一元化された ID プロバイダーを利用する
- 定期的に認証情報を監査およびローテーションする
- ユーザーグループと属性を活用する



# 質問と回答形式でのベストプラクティス(例)

## 例：セキュリティの質問(抜粋)

全項目ベストプラクティスに  
則っていないとダメなのか？

- 一時的な認証情報を使用する
- シークレットを安全に保存して使用する
- 一元化された ID プロバイダーを利用する
- 定期的に認証情報を監査およびローテーションする
- ユーザーグループと属性を活用する



# 質問と回答形式でのベストプラクティス(例)

例：セキュリティの質問(抜粋)

全項目ベストプラクティスに  
則っていないとダメなのか？

ベストプラクティスを知った上で、  
皆様が「(ビジネス的な)判断をする」ための手法  
→ リスクや改善点の”顕在化”

# 質問と回答形式でのベストプラクティス(例)

例：セキュリティの質問(抜粋)

[SEC2] ユーザー ID とマシン ID はどのように管理したらよいでしょうか？

- 強力なサインインメカニズムを使用する
- **一時的な認証情報を使用する**
- シークレットを安全に保存して使用する
- 一元化された ID プロバイダーを利用する
- 定期的に認証情報を監査およびローテーションする
- ユーザーグループと属性を活用する



# 質問と回答形式でのベストプラクティス(例)

## 例：セキュリティの質問(抜粋)

[SEC2] ユーザー ID とマシン ID はどのように管理したらよいのでしょうか？

- 強力なサインインメカニズムを使用する
- 一時的な認証情報を使用する

たとえば EC2 インスタンスにアクセスキーを組み込んでいると…

- ・ 長期的なアクセスキーが組み込まれることで、他のリソースに対する不正操作のリスクが増大する
- ・ 定期的なキーローテーションを検討する必要がある

複数の AWS アカウントを運用しており、すべての AWS アカウントのアクセスに IAM ユーザーを使用していると…

- ・ 扱うクレデンシャルが増えることで、同時にクレデンシャルの漏洩リスクが増える
- ・ 異動、退職者が出た場合、どうする？



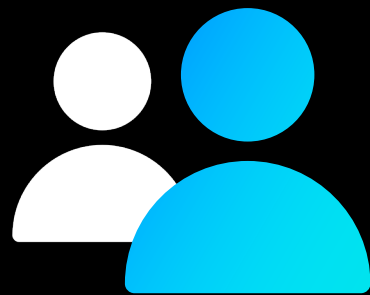
# AWS Well-Architected フレームワーク の活用





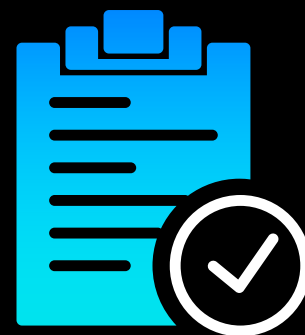
# Well-Architected レビューの意図

監査ではない



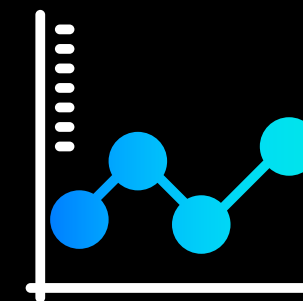
話し合いであり、重大な  
問題や改善可能な領域の  
特定が目的

適切な関係者で  
ディスカッションする



ワークロードの理解と  
適切な改善を検討

1 回限りの  
チェックではない

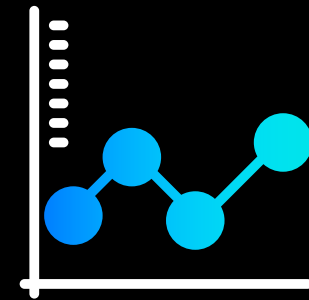


定期的な見直し  
(KAIZEN)

# 1 回限りのチェックではない

- 設計前の段階でホワイトペーパーを読む
  - 質問は必ず読んでおく
- 定期的な見直し (KAIZEN)
  - 設計段階 (もしくはその前の段階)
  - リリース前
  - 運用フェーズ

Not a one-time check



Throughout  
lifecycle



## AWS Well-Architected Tools

<https://aws.amazon.com/well-architected-tool/>



# AWS Well-Architected Tool

## Learn, measure, and build using architectural best practices

The AWS Well-Architected Tool helps you review your workloads against current AWS best practices and provides guidance on how to improve your cloud architectures. This tool is based on the AWS Well-Architected Framework.

### Define a workload

Define a workload based on one of your existing cloud applications.

[Define workload](#)

### Pricing (US)

Any usage

Free

### Getting started

[What is the AWS Well-Architected Tool?](#)

[Getting started video](#)

### More resources

[FAQ](#)

[AWS Well-Architected Partners](#)

## How it works



## Benefits and features

**Get architectural guidance**

Access the knowledge and best

**Enable consistent governance**

Apply a consistent process to help you

**Continuously improve architectures**

Support continuous improvement

# 運用中ワークロードへのW-Aレビュー



## ベストプラクティスを理解した上で、判断する



Your team

TECHNICAL & BUSINESS LEADS



APN Partner



Your team

TECHNICAL & BUSINESS LEADS



APN Partner



Your team

TECHNICAL & BUSINESS LEADS



APN Partner

(前準備)

### セルフチェック

### W-Aレビュー実施

### クラウド最適化

W-Aの質問に答えながら、  
設計中の構成や既に運用し  
ているシステムの現状確認  
(棚卸し)を実施

SAとベストプラクティスとの  
ギャップを把握。様々なリス  
クやクラウドに最適化できる  
ポイントを把握する

ビジネス的な判断や優先度  
づけを実施し、よりクラウ  
ドに最適化していく

AWS Well-Architected Tools へ入力

2~3時間の集中的な打ち合わせ

その後、再度レビュー実施して状況確認

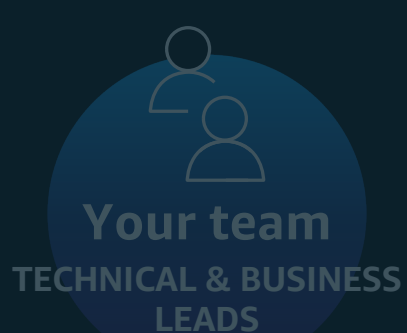


運用開始後も  
**定期的な見直し  
(KAIZEN)が重要**

# 運用中ワークロードへのW-Aレビュー



## 事情により既存ワークロードの改善ができない場合…



Your team

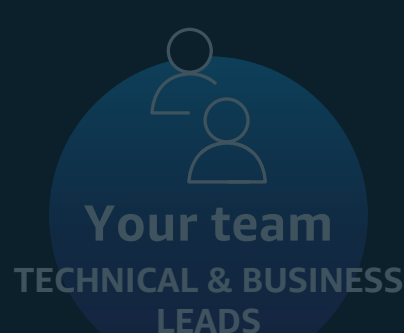
TECHNICAL & BUSINESS LEADS



APN Partner

(前準備)

### セルフチェック



Your team

TECHNICAL & BUSINESS LEADS



APN Partner

### W-Aレビュー実施



Your team

TECHNICAL & BUSINESS LEADS



APN Partner

### 次のワークロードに活かす

W-Aの質問に答えながら、設計中の構成や既に運用しているシステムの現状確認(棚卸し)を実施

AWS Well-Architected Tools へ入力

SAとベストプラクティスとのギャップを把握。様々なリスクやクラウドに最適化できるポイントを把握する

2~3時間の集中的な打ち合わせ

既存ワークロードの改善ができない場合も、次期システム的设计時に活かすことが出来る



# Well-Architected レビューの選択肢

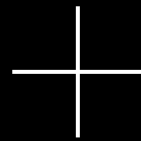
Your team technical  
and business leads

AWS  
WA tool

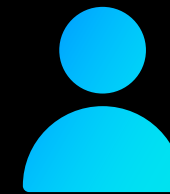
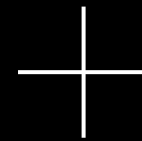
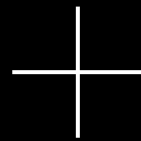
AWS  
APN partner

AWS solutions  
architect

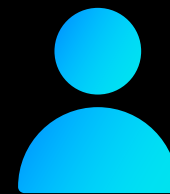
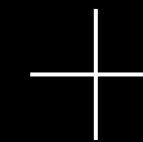
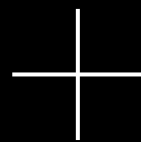
Self-service



Partner



AWS SA



# Well-Architected レビューの選択肢

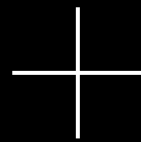
Your team technical  
and business leads

AWS  
WA tool

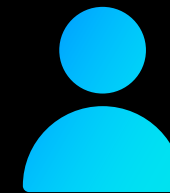
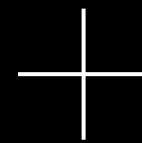
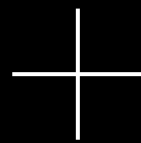
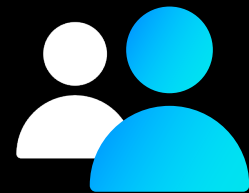
AWS  
APN partner

AWS solutions  
architect

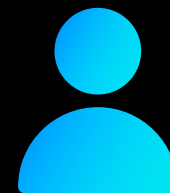
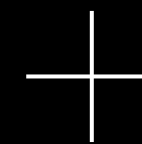
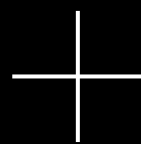
Self-service



Partner



AWS SA





# Well-Architected Partner Program

## Well-Architected パートナープログラム発表 (re:Invent2018)



AWS re:Invent 2018 - Keynote with Werner Vogels



AWS re:Invent 2018 - Global Partner Keynote

# Well-Architected Partners

<https://aws.amazon.com/architecture/well-architected/partners/>



# 日本のWell-Architectedパートナー



# セキュリティの柱におけるベストプラクティス

分野	質問	ベストプラクティス
セキュリティ	SEC 1. ワークロードを安全に運用するには、どうすればよいですか？	アカウントを使用してワークロードを分ける
		AWS アカウントのセキュリティを確保する
		管理目標を特定および検証する
		セキュリティ脅威に関する最新情報を入手する
		情報 セキュリティのレコメンデーションに関する更新情報を入手する
		パイプラインのセキュリティコントロールのテストと検証を自動化する
		脅威モデルを使用してリスクを特定し、優先順位を付ける
Identity and Access Management	SEC 2. ユーザー ID とマシン ID はどのように管理したらよいでしょうか？	強力なサインインメカニズムを使用する
		一時的な認証情報を使用する
		シークレットを安全に保存して使用する
		一元化された ID プロバイダーを利用する
		定期的に認証情報を監査およびローテーションする
	ユーザーグループと属性を活用する	
	SEC 3. 人とマシンのアクセス許可はどのように管理すればよいでしょうか？	アクセス要件を定義する
		最小権限のアクセスを付与する
		緊急アクセスのプロセスを確立する
		アクセス許可を継続的に削減する
組織のアクセス許可ガードレールを定義する		
検出	SEC 4. セキュリティイベントをどのように検出し、調査していますか？	ライフサイクルに基づいてアクセスを管理する
		パブリックおよびクロスアカウントアクセスの分析
		リソースを安全に共有する
		サービスとアプリケーションのログ記録を設定する
		ログ、結果、メトリクスを一元的に分析する
		イベントへの応答を自動化する
		実用的なセキュリティイベントを実装する



# セキュリティの柱におけるベストプラクティス

分野	質問	ベストプラクティス
インフラストラクチャ保護	SEC 5. ネットワークリソースをどのように保護しますか?	<ul style="list-style-type: none"> <li>ネットワークレイヤーを作成する</li> <li>すべてのレイヤーでトラフィックをコントロールする</li> <li>ネットワーク保護を自動化する</li> <li>検査および保護を実装する</li> </ul>
	SEC 6. コンピューティングリソースをどのように保護していますか?	<ul style="list-style-type: none"> <li>脆弱性管理を実行する</li> <li>攻撃領域を削減する</li> <li>マネージドサービスを活用する</li> <li>コンピューティング保護を自動化する</li> <li>ユーザーが遠距離でアクションを実行できるようにする</li> <li>ソフトウェアの整合性を検証する</li> </ul>
データ保護	SEC 7. どのようにデータを分類していますか?	<ul style="list-style-type: none"> <li>ワークロード内のデータを特定する</li> <li>データ保護コントロールを定義する</li> <li>識別および分類を自動化する</li> <li>データのライフサイクル管理を定義する</li> </ul>
	SEC 8. 保管時のデータをどのように保護していますか?	<ul style="list-style-type: none"> <li>安全なキー管理を実装する</li> <li>保管中に暗号化を適用する</li> <li>保管時のデータの保護を自動化する</li> <li>アクセスコントロールを適用する</li> <li>人をデータから遠ざけるメカニズムを使用する</li> </ul>
	SEC 9. 転送時のデータをどのように保護していますか?	<ul style="list-style-type: none"> <li>安全な鍵および証明書管理を実装する</li> <li>伝送中に暗号化を適用する</li> <li>意図しないデータアクセスの検出を自動化する</li> <li>ネットワーク通信を認証する</li> </ul>
インシデント対応	SEC 10. インシデントの予測、対応、復旧はどのように行いますか?	<ul style="list-style-type: none"> <li>重要な人員と外部リソースを特定する</li> <li>インシデント管理計画を作成する</li> <li>フォレンジック機能を備える</li> <li>封じ込め機能を自動化する</li> <li>アクセスを事前プロビジョニングする</li> <li>ツールを事前デプロイする</li> <li>ゲームデーを実施する</li> </ul>



# 最低限おさえたいセキュリティの2項目



これから AWS を使う上で

SEC 1. ワークロードを安全に運用するには、どうすればよいですか？

SEC 4. セキュリティイベントをどのように検出し、調査していますか？

# 最低限おさえたいおきたいセキュリティの2項目



SEC 1. ワークロードを安全に運用するには、どうすればよいですか？

SEC 4. セキュリティイベントをどのように検出し、調査していますか？

# 最低限おさえたいセキュリティの2項目



SEC 1. AWS ルートアカウントには必ず MFA (多要素認証) を  
設定し、最小限の利用に留める(極力使用しない)、  
AWS アカウントの分離を検討する

SEC 4. セキュリティイベントをどのように検出し、調査していますか？



# 1. AWS ルートアカウントには必ず MFA (多要素認証) を設定し、最小限の利用に留める(極力使用しない)

## AWS ルートアカウントとは？

- アカウント作成時のメールアドレスと設定したパスワードでのサインイン
- アカウントの全ての AWS サービスとリソースへの完全なアクセス権限を持つ

## AWS ルートアカウントは MFA を設定し、“極力”利用しない

- 十分に強度の強いパスワードを設定したの上、**多要素認証 (MFA) で保護**し、通常は極力利用しないような運用を推奨
- Security Credential のページから Access Key を削除する  
(ただし Access Key を使用していないか確認が必要)

一部、ルートアカウントが必要となる操作もある

([https://docs.aws.amazon.com/ja\\_jp/general/latest/gr/aws\\_tasks-that-require-root.html](https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws_tasks-that-require-root.html))



# 1. AWS ルートアカウントには必ず MFA (多要素認証) を設定し、最小限の利用に留める(極力使用しない)

## ルートアカウントではなく IAM を利用する



### AWS Identity and Access Management (IAM) とは？

- AWS リソースへのアクセスを安全に制御するためのサービス  
以下の機能を提供

#### ユーザ/認証情報管理

- IAM ユーザ / パスワード
- MFA (多要素認証)
- 認証情報のローテーション

#### AWS リソースへの安全なアクセス

- IAM ロール

#### アクセス権限管理

- IAM グループ
- IAM ポリシー



# 1. AWS アカウントの分離を検討する

## 多数のシステムをどのように管理するか

- AWS で稼働するシステムの増加
  - 単一 ... そのシステムの管理者が AWS 自体の管理も行う
  - 数個 ... 共通基盤チームが AWS 自体の管理と個別システムの監査を行う
  - 多数 ... 仕組みなしにすべてのシステムを管理するのは困難
- 仕組み
  - マルチアカウント化
  - IAM やタグなど権限管理の簡素化、強制化
  - AWS 環境提供の自動化
  - ログの集約や保護の実施
  - 共有サービス利用のためのネットワーク構成



# 1. AWS アカウントの分離を検討する

機能や職務分掌、ビジネスユニット単位で環境を分ける

## 環境

開発、テスト、本番などの環境をセキュリティやガバナンス、規制のために分離できる  
(PCI など)

## 課金

部門単位やシステムの単位でAWSのコストが明確に分離できる

## ビジネス推進

事前定義されたガバナンスフレームワークの中で特定のビジネス部門に対する権限の委譲が行える

## ワークロード

外部向け/社内向けサービスや、リスクやデータ分類、顧客の違いなどに応じてワークロードを分離できる



# 1. AWS アカウントの分離を検討する

AWS がご提供するマルチアカウント管理ソリューション



## AWS Organizations

- アカウント管理サービス
- 複数の AWS アカウントを 1 つの組織に統合できるサービス
- 一括請求 (コンソリデーティッドビルディング) およびアカウント管理機能を使用できるサービス



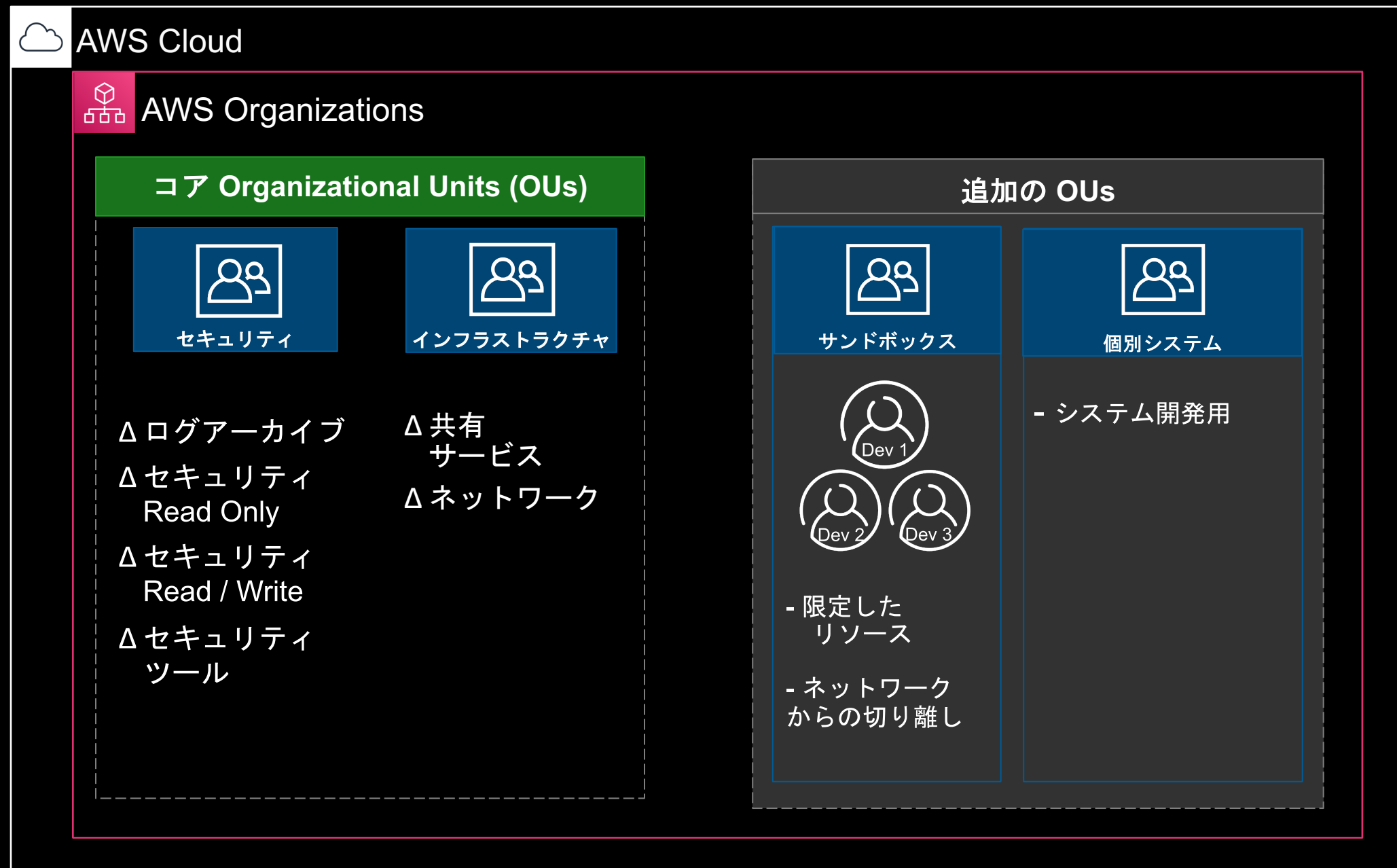
## AWS Control Tower

- マルチアカウント構成の作成
- アカウントの発行
- 監査用ログの集中かつ安全な保存
- ガードレールの設置
  - 実施してはいけない操作の禁止、危険な設定の監視



# 1. AWS アカウントの分離を検討する

## マルチアカウント管理のフレームワーク



# 最低限おさえたいおきたいセキュリティの2項目



SEC 1. ワークロードを安全に運用するには、どうすればよいですか？

SEC 4. セキュリティイベントをどのように検出し、調査していますか？

# 最低限おさえたいおきたいセキュリティの2項目



SEC 1. ワークロードを安全に運用するには、どうすればよいですか?

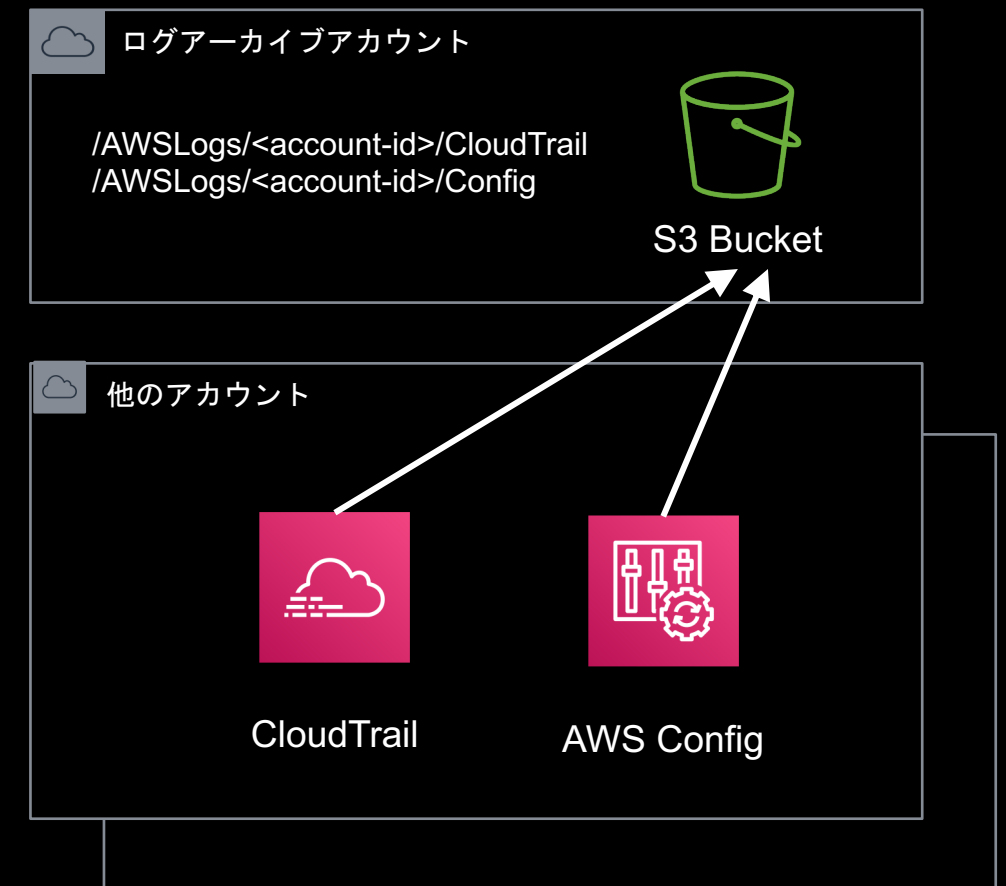
SEC 4. セキュリティ関連のログ取得し、一元的に監視と分析をする



# 4.セキュリティ関連のログ取得し、 一元的に監視と分析をする

## AWS Config や AWS CloudTrail を有効化し、ログを一元的に集約する

- AWS CloudTrail のログとAWS Configのログをログアカウントの Amazon S3バケットに集約
- 保存バケットのバケットポリシーと各サービスの送信先設定だけで実現可能
- ログ集約を停止させないよう AWS Organizations SCP も合わせて利用 する



# 4.セキュリティ関連のログ取得し、 一元的に監視と分析をする

Amazon GuardDuty を使用する



## Amazon GuardDuty とは

- 脅威検出のマネージドサービス
- 既知と未知の振る舞い検知
- 悪意のある IP アドレス、異常検出、機械学習などの統合脅威インテリジェンスを使用して脅威を認識

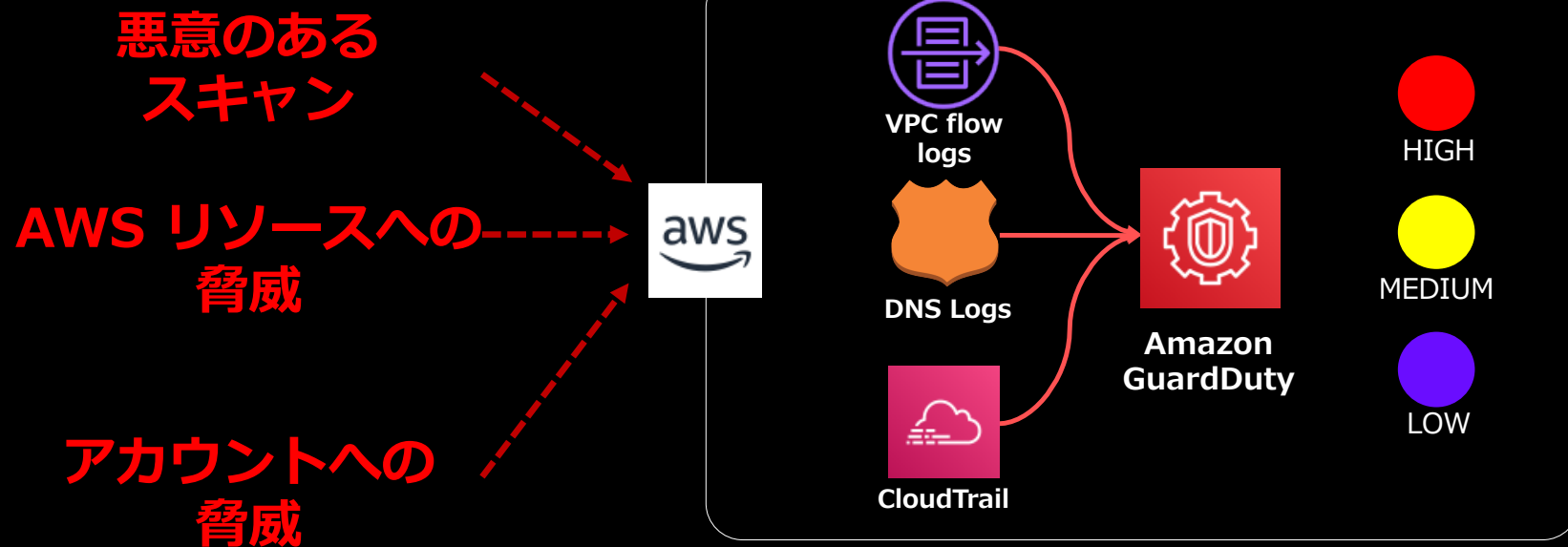
# 4.セキュリティ関連のログ取得し、一元的に監視と分析をする

## Amazon GuardDuty を使用する

脅威の種類

データソース

Findings



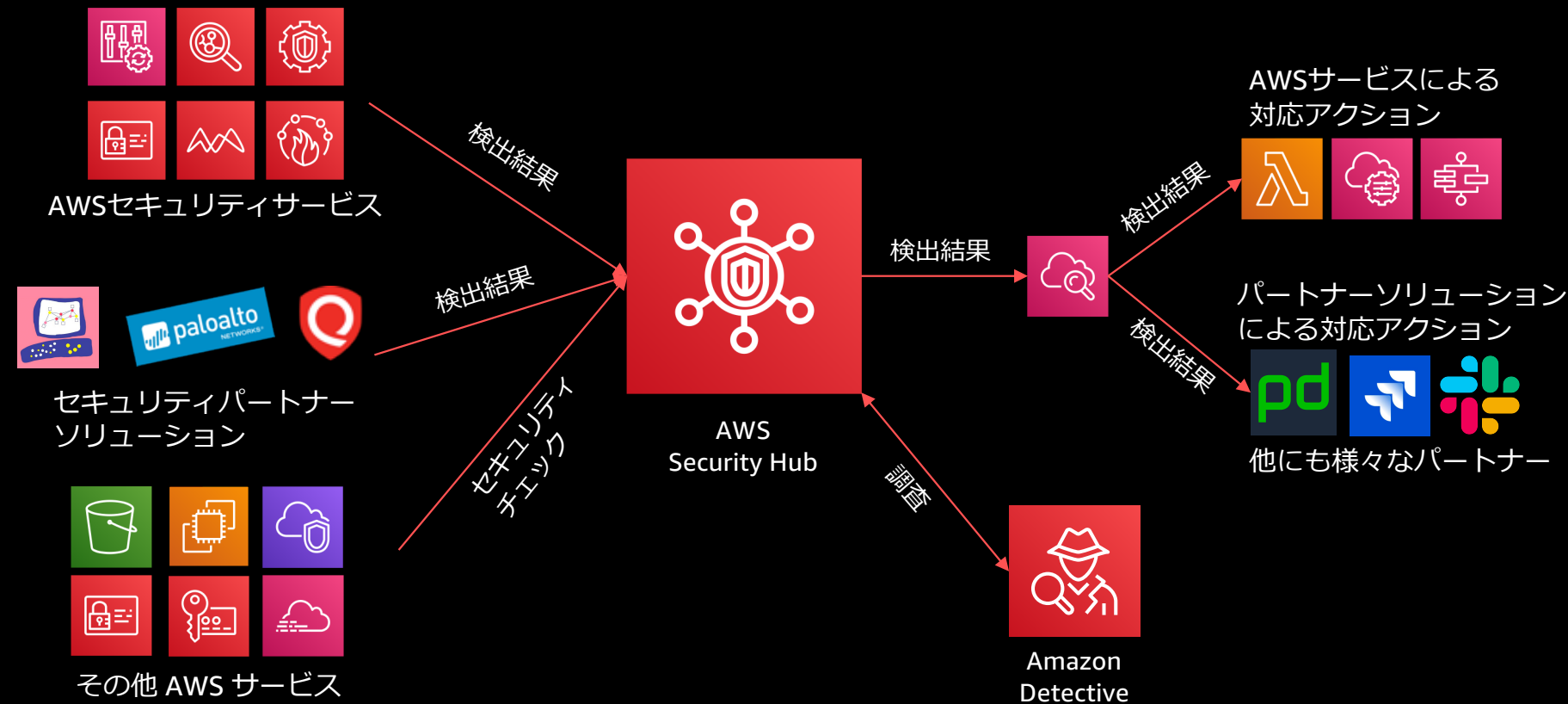
Finding	Last seen	Count
Unprotected port on EC2 Instance	2017-11-27 16:55:46 (an hour ...)	301
188.212.100.78 is performing SSH brute force attacks again...	2017-11-27 16:34:46 (an hour ...)	1
202.107.104.119 is performing SSH brute force attacks agai...	2017-11-26 12:11:00 (a day ago)	1
103.27.239.2 is performing SSH brute force attacks against ...	2017-11-23 19:41:01 (4 days a...)	1
[SAMPLE] Credentials for instance role GeneratedFindingUs...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] Reconnaissance API GeneratedFindingAPIName ...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] Unusually large amount of network traffic from E...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] EC2 instance i-99999999 communicating with kn...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] EC2 instance involved in SSH brute force attacks.	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] Unusual outbound communication seen from EC...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] IAM User GeneratedFindingUserName logged int...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] Drop Point domain name queried by EC2 instanc...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] API GeneratedFindingAPIName was invoked fro...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] Reconnaissance API GeneratedFindingAPIName ...	2017-11-23 19:25:27 (4 days a...)	1
[SAMPLE] Drive-by source domain name queried by EC2 in...	2017-11-23 19:25:27 (4 days a...)	1



# 4.セキュリティ関連のログ取得し、一元的に監視と分析をする

## AWS Security Hub を活用する

- AWS アカウント全体の優先順位が高いセキュリティアラートとコンプライアンス状況を統合ビューで素早くアクセス
- AWS とパートナーのセキュリティサービスで得た知見から今後のトレンドや問題点を抽出
- CIS AWS Foundation Benchmark や PCI DSSなどの業界標準を使用
- 検出結果を調査し、対応や修正アクションを実施する



# AWS Well-Architected フレームワーク の ベストプラクティスを活用するには ①

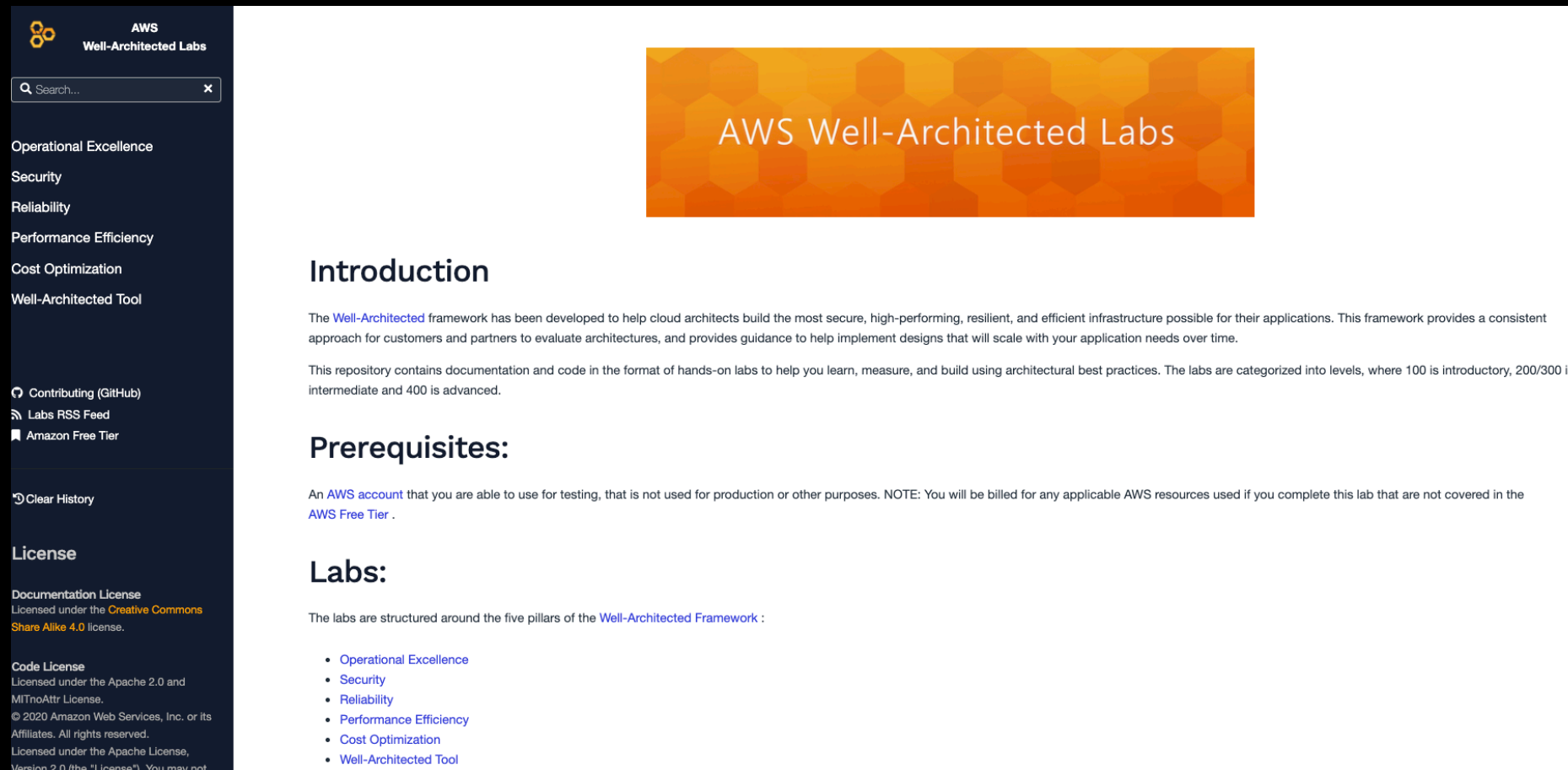
- 始める前にホワイトペーパーを読む
- 質問を通して**反復**する
  - ✓ アクションとバックログを特定する
- リリース前のレビュー
- リリース後も**定期的**にレビュー



# AWS Well-Architected フレームワーク の ベストプラクティスを活用するには ②

## ➤ AWS Well-Architected Labs を活用する

- ハンズオン形式で Well-Architected フレームワーク の  
ベストプラクティスの適用方法を実践的に学ぶことができる



**AWS Well-Architected Labs**

### Introduction

The **Well-Architected** framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help implement designs that will scale with your application needs over time.

This repository contains documentation and code in the format of hands-on labs to help you learn, measure, and build using architectural best practices. The labs are categorized into levels, where 100 is introductory, 200/300 is intermediate and 400 is advanced.

### Prerequisites:

An **AWS account** that you are able to use for testing, that is not used for production or other purposes. NOTE: You will be billed for any applicable AWS resources used if you complete this lab that are not covered in the **AWS Free Tier**.

### Labs:

The labs are structured around the five pillars of the **Well-Architected Framework**:

- [Operational Excellence](#)
- [Security](#)
- [Reliability](#)
- [Performance Efficiency](#)
- [Cost Optimization](#)
- [Well-Architected Tool](#)



# まとめ

AWS Well-Architected

- **AWS Well-Architected フレームワーク とは**
  - 10年以上の経験、数多くのお客様と作りあげたクラウド設計・運用のベストプラクティス集
- **セキュリティの柱におけるベストプラクティスを活用**
  - 10個の質問とベストプラクティスを活用し、現状 (As Is) を理解し、将来あるべき姿 (To Be) を検討
- **AWS Well-Architected フレームワーク のベストプラクティスを学ぶ**
  - ホワイトペーパーを読む
  - AWS Well-Architected Labs 上のハンズオンで実践的に学ぶ



# Well-Architected フレームワーク ホワイトペーパー

## □ W-A ホワイトペーパー(英語版 / 2020年7月更新)

[https://d1.awsstatic.com/whitepapers/architecture/AWS\\_Well-Architected\\_Framework.pdf](https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)

## □ W-A ホワイトペーパー(日本語版 / 2020年7月版の翻訳)

[https://d1.awsstatic.com/whitepapers/ja\\_JP/architecture/AWS\\_Well-Architected\\_Framework.pdf](https://d1.awsstatic.com/whitepapers/ja_JP/architecture/AWS_Well-Architected_Framework.pdf)

→いずれもAppendix(付録)にW-Aツールで扱う  
ベストプラクティスの質問が記載されています

## □ W-A Web サイト



<https://wa.aws.amazon.com/index.ja.html>



AWS Well-Architected



# Thank You!

