D-01

AWSにおける継続的なセキュリティモニタリングの実践

高田 智己
プラクティス マネージャー
アマゾン ウェブ サービス ジャパン株式会社
プロフェッショナルサービス本部

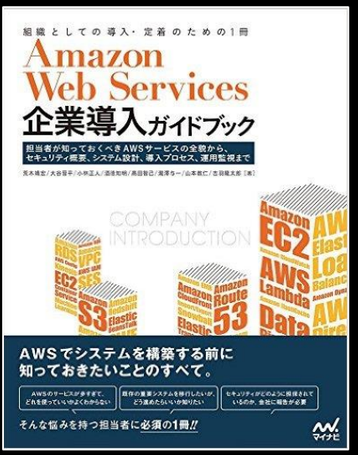
aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

自己紹介

名前
高田 智己（Tomomi Takada）
CISA, CISSP

所属
アマゾン ウェブ サービス ジャパン株式会社
プロフェッショナルサービス本部
プラクティスマネージャー



日本におけるプロフェッショナルサービス立ち上げ期より参画し、エンタープライズのお客様のセキュリティに関する課題解決に従事

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

本セッションについて

目的	AWS利用のメリットを最大限に活かしながら、システムの**コンプライアンスを維持**していくための**アプローチを理解**する
対象者	AWS上のシステムの**セキュリティ設計やその監査**に関わられている方

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

アジェンダ

- セキュリティと監査における現在の課題と継続的コンプライアンス
- 継続的コンプライアンスを導入する5つのステップ
- 継続的コンプライアンスの活用例
- まとめ

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

セキュリティと監査における現在の課題と継続的コンプライアンス

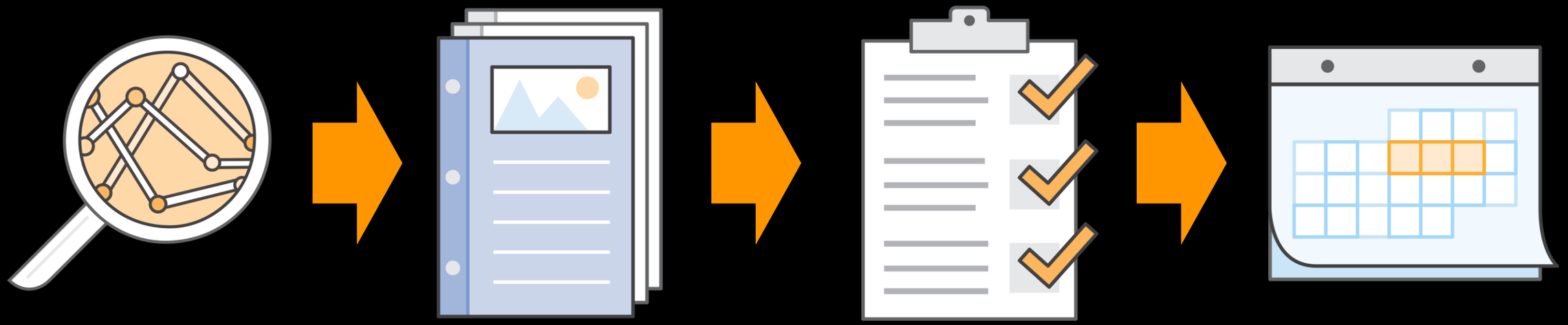
aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Be Compliantな状況とは？

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

セキュリティポリシー準拠への典型的な4ステップ



セキュリティ
要件の分析

統制要件の
定義と文書化

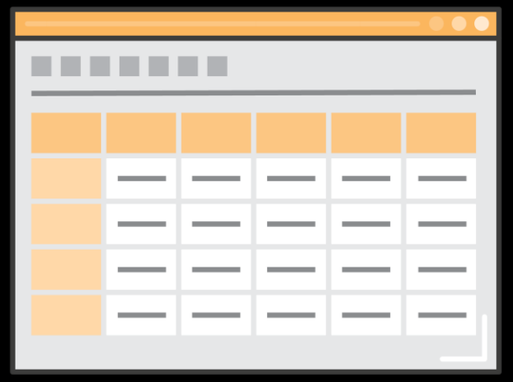
チェックリスト

監査

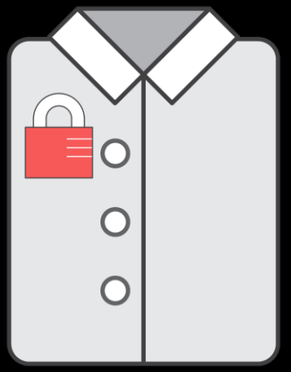
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

準拠に向けてお客様が行う業務の例

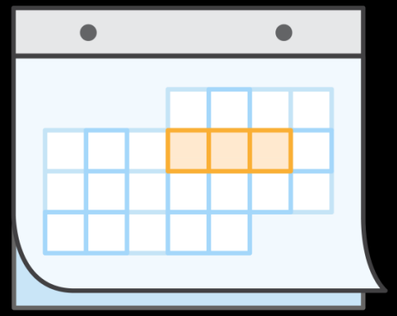
統制要件



チェックリスト

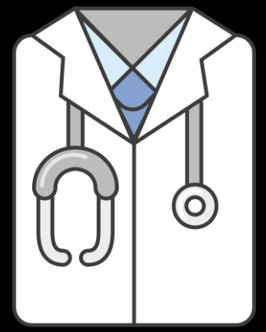


情報セキュリティ部門



監査プロセス

問診/文書
スクリーンショット



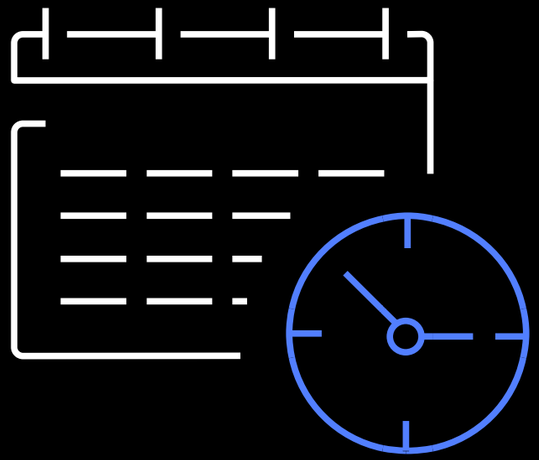
監査人

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

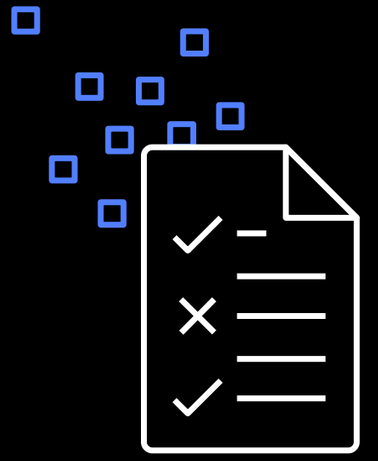
一般的なセキュリティと監査の課題

サンプリング抽出
によるアプローチ



ある時点の状態で
のアセスメント

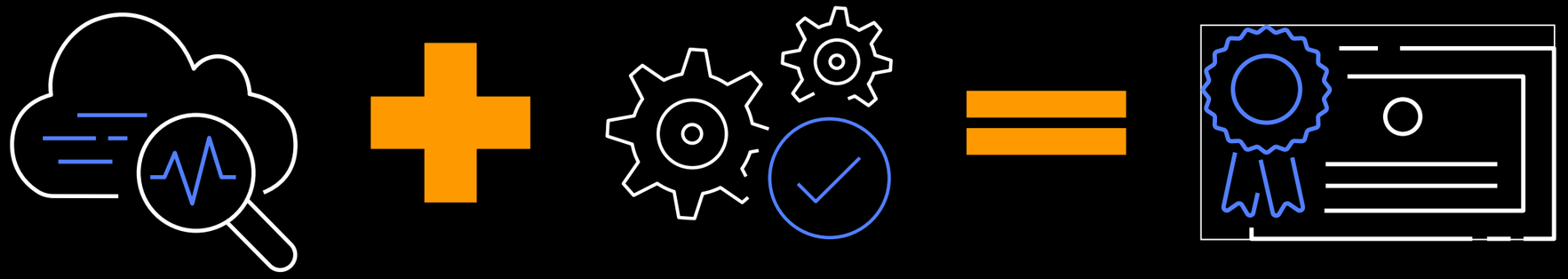
信頼性の低い
証跡と収集手順



人手による
確認作業

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

継続的コンプライアンスとは



継続的モニタリングによる
検知性・可視性の向上

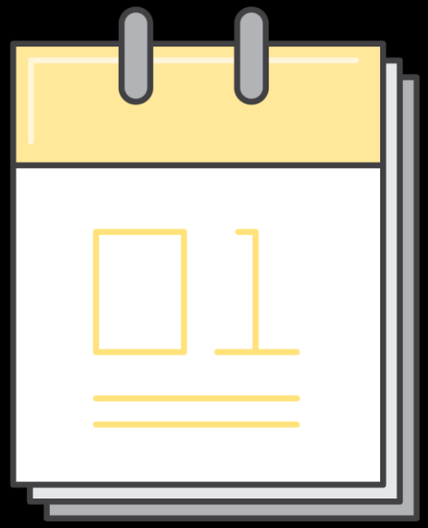
ほぼリアルタイムの
対応自動化

継続的
コンプライアンス

ほぼリアルタイムで**どこから**、**誰が**、**何を**変更したのかというイベントに対して可視性を向上させることにより、お客様環境で発生する誤操作やコンプライアンス要件に沿わない操作の**検知**や、リスクの顕在化を防ぐための迅速な**対応**を可能とする

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

継続的コンプライアンスによる3つのベネフィット



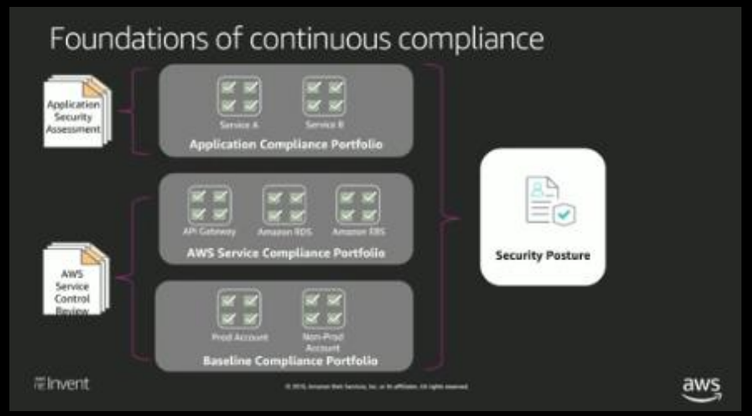
日々の業務への
監査の組み込み

スケールする環境に
対する一貫性のある
監査

付加価値の高い業務
への時間と人的
リソースの集中

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

継続的コンプライアンスに取り組むお客様事例



National Australia Bank

- NABの中で継続的コンプライアンスソリューションを構築している
- AWS上のワークロードのセキュリティコンプライアンスをシステマティックかつ継続的にレビューしている
- セキュリティコントロールの導入にかかる時間を従来の19日間から45秒に短縮

AWS re:Invent 2018: Chart Your Journey with AWS Best Practices (SEC201-R1)
https://www.youtube.com/watch?v=HGkPvP2D45I

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

継続的コンプライアンスを導入する5つのステップ

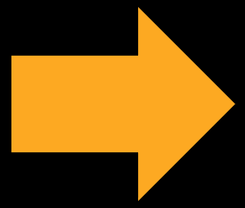
aws SUMMIT

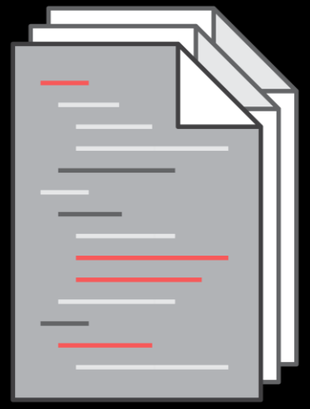
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

継続的コンプライアンスへの2つのアプローチ

1.

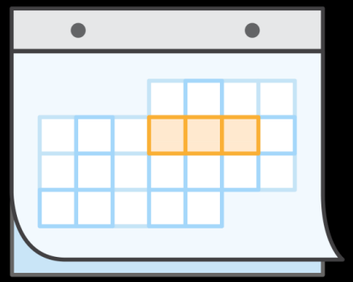
チェックリスト



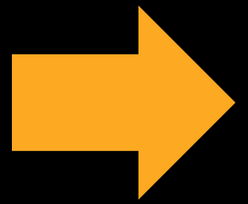


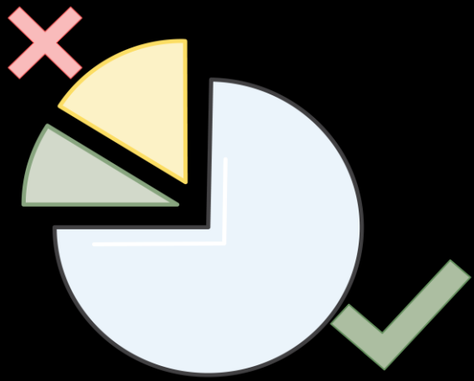
チェック作業
の自動化

2.



監査





継続的な
モニタリング

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

セキュリティポリシー準拠への新しい5ステップ

チェック作業の自動化と**AWS環境にBuilt inされたモニタリング機能**の
活用により、より高度な統制環境の実現をはかる

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.1：セキュリティ要件の分析

分析

お客様環境による統制要件

企業内のポリシー

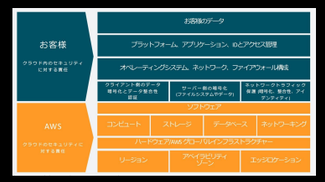
業界の規制

業界標準
(PCI-DSS, NIST)

AWSのセキュリティサービス

予防的統制　発見的統制　訂正的統制

従来の統制目標



AWSの責任共有モデル

AWS コンプライアンスプログラム
(SOC2, ISO27001など)

AWSの統制情報

目的

- セキュリティ要件とAWSの特性の**分析**

進め方

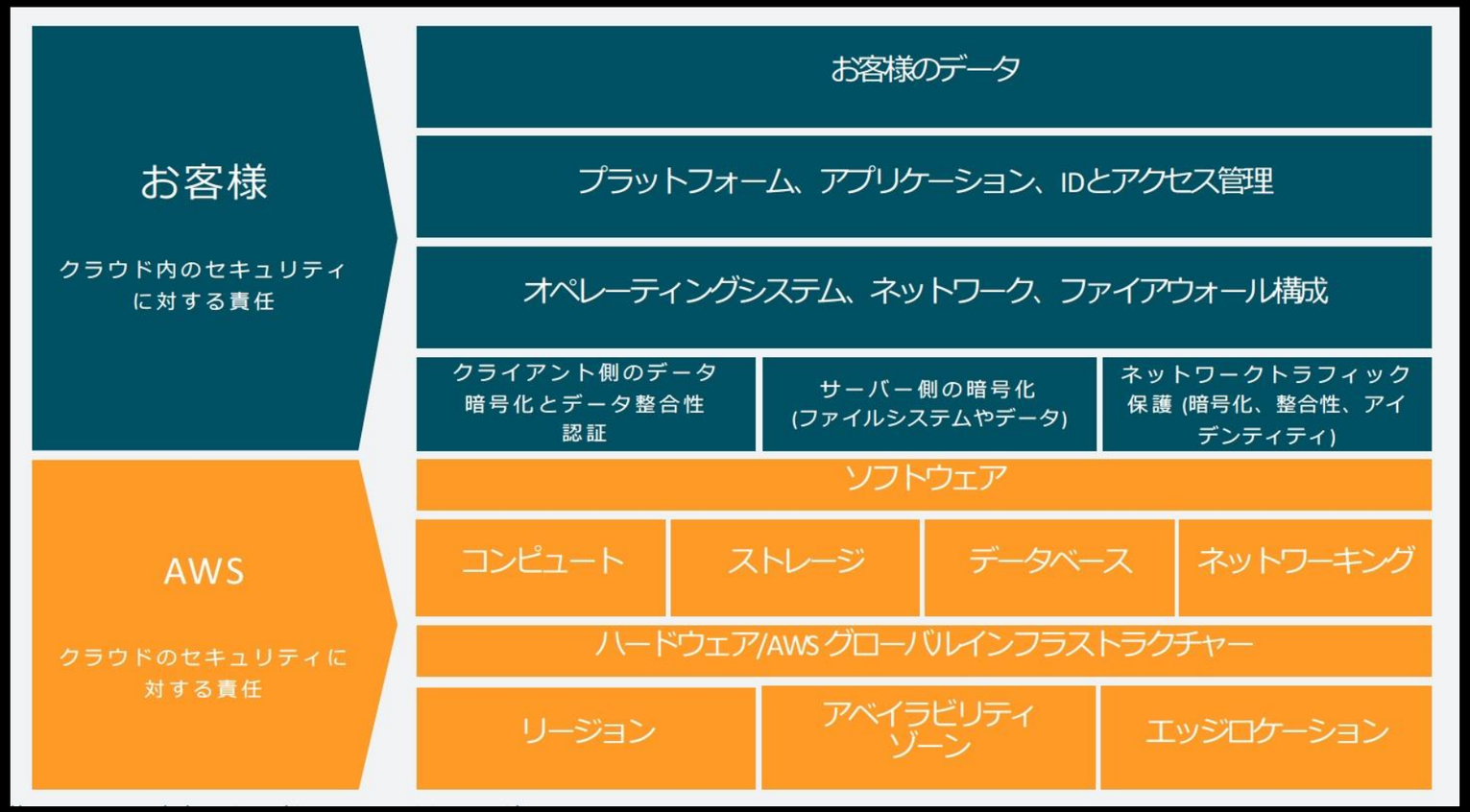
- AWSの**責任共有モデルを念頭**に、利用者の統制要件、AWSの統制情報、AWS及びAPNパートナー様の提供するセキュリティ機能を把握する

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

責任共有モデルの理解

分析



お客様が管理するセキュリティ

aws

AWSが管理するセキュリティ

▶ **従来の統制目標に対して、利用者側が統制すること、AWSが統制することの責任境界の確認をすることがはじめの一歩**

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

責任共有モデル https://aws.amazon.com/jp/compliance/shared-responsibility-model/

AWS Artifactの活用

AWS Artifact

AWSの統制に対する
第三者機関の監査レポートの入手
ポータル

AWS Artifact管理コンソール画面

※入手は各種利用規約に同意が必要

AWSの統制に対する信頼の根拠として第三者機関の各種レポートを取得し、自社の統制目標を満たすことができるか確認する

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWSのセキュリティ関連サービス/機能の把握

IDとアクセス管理	発見的コントロール	インフラセキュリティ	データ保護	インシデントレスポンス
AWS Identity & Access Management (IAM)	AWS CloudTrail	AWS Systems Manager	AWS Key Management Service (KMS)	AWS Config Rules
AWS Directory Service	AWS Config	AWS Shield	AWS CloudHSM	AWS Lambda
AWS Organizations	Amazon CloudWatch	AWS WAF – Web application firewall	Amazon Macie	
AWS Secrets Manager	Amazon GuardDuty	AWS Firewall Manager	AWS Certificate Manager	
AWS Single Sign-On	VPC Flow Logs	Amazon Inspector	Server-Side Encryption	
Amazon Cognito	Security Hub	Amazon Virtual Private Cloud (VPC)		

▶ AWSのセキュリティサービスの機能を把握し、利用者側での統制に活用

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.2：統制要件の定義と文書化

定義と文書化

文書化の例

要件	AWS環境における対応指針	AWS関連サービス・仕様の情報

目的

- セキュリティ要件に対する、**責任分担**と**セキュリティ対策**の定義を行う

進め方

- **各要件に関する対応指針**を責任共有モデルに基づき記載する
  - AWS内の統制状況と根拠
  - 利用者側で行う必要のある対応方針

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.2：統制要件の定義と文書化

定義と文書化

文書化の例

要件	AWS環境における対応指針	AWS関連サービス・仕様の情報

暗号鍵の保護
情報を保護するための暗号による管理策の利用に関する方針を策定、実施する

目的

- セキュリティ要件に対する、**責任分担**と**セキュリティ対策**の定義を行う

進め方

- **各要件に関する対応指針**を責任共有モデルに基づき記載する
  - AWS内の統制状況と根拠
  - 利用者側で行う必要のある対応方針

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.2：統制要件の定義と文書化

文書化の例

要件	AWS環境における対応指針	AWS関連サービス・仕様の情報

暗号鍵の保護

- AWS利用者はAWSが提供するサーバサイド暗号化サービスを利用していない限り、**利用者自身で暗号化に関する管理を行なう**必要がある
- AWSで管理しているキーの管理手順は、**各種規制要件に準拠**している

目的

- セキュリティ要件に対する、**責任分担**と**セキュリティ対策**の定義を行う

進め方

- **各要件に関する対応指針**を責任共有モデルに基づき記載する
  - AWS内の統制状況と根拠
  - 利用者側で行う必要のある対応方針

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.2：統制要件の定義と文書化

文書化の例

要件	AWS環境における対応指針	AWS関連サービス・仕様の情報

暗号鍵の保護

- AWS機能での鍵管理を行う場合、**AWS KMSやAWS CloudHSMを利用**し、利用する暗号鍵を適切に保管する。この時、**暗号鍵に対する適切なアクセス制御**を実施する。

目的

- セキュリティ要件に対する、**責任分担**と**セキュリティ対策**の定義を行う

進め方

- **各要件に関する対応指針**を責任共有モデルに基づき記載する
  - AWS内の統制状況と根拠
  - 利用者側で行う必要のある対応方針

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.2：統制要件の定義と文書化

定義と文書化

文書化の例

要件	AWS環境における対応指針	AWS関連サービス・仕様の情報

暗号鍵の保護

- AWS KMSは暗号化キーを一元管理
- マスターキーは、**HSMで保護**
- **キーの使用ポリシー**で、どのユーザーがキーを使用し、どの条件でデータを暗号化および復号可能かを定義

・・・・・・・・
・・・・・

目的

- セキュリティ要件に対する、**責任分担**と**セキュリティ対策**の定義を行う

進め方

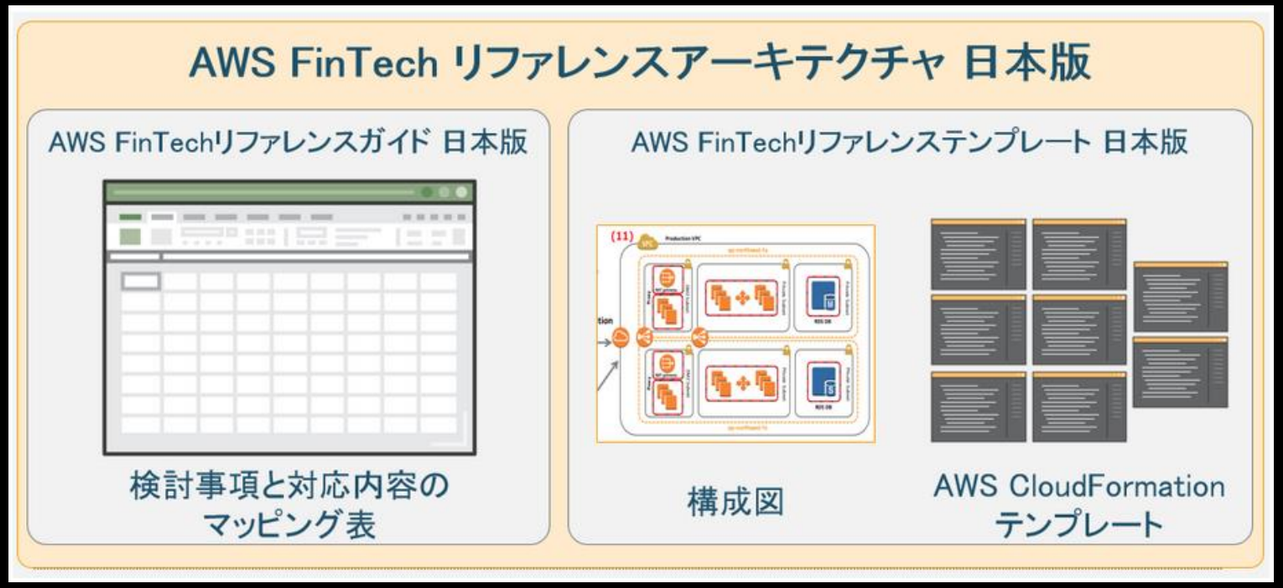
- **各要件に関する対応指針**を責任共有モデルに基づき記載する
  - AWS内の統制状況と根拠
  - 利用者側で行う必要のある対応方針

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

各種リファレンスアーキテクチャーの活用

定義と文書化

要求事項に対する検討事項と対応指針のマッピング資料をまとめたもの



https://aws.amazon.com/jp/blogs/news/aws-fintech-architecture-jp/

様々なリファレンスが入手可能

- AWS FinTech リファレンス・アーキテクチャー
- 医療情報システム向け AWS 利用リファレンス
- NISC 統一基準群（平成 30 年度版）に対応した AWS クラウド利用のセキュリティリファレンス
- 等

各種標準の要件に対して責任共有モデルを前提にした検討事項のマッピングを参考にすることで自社の要件にも活用することが可能

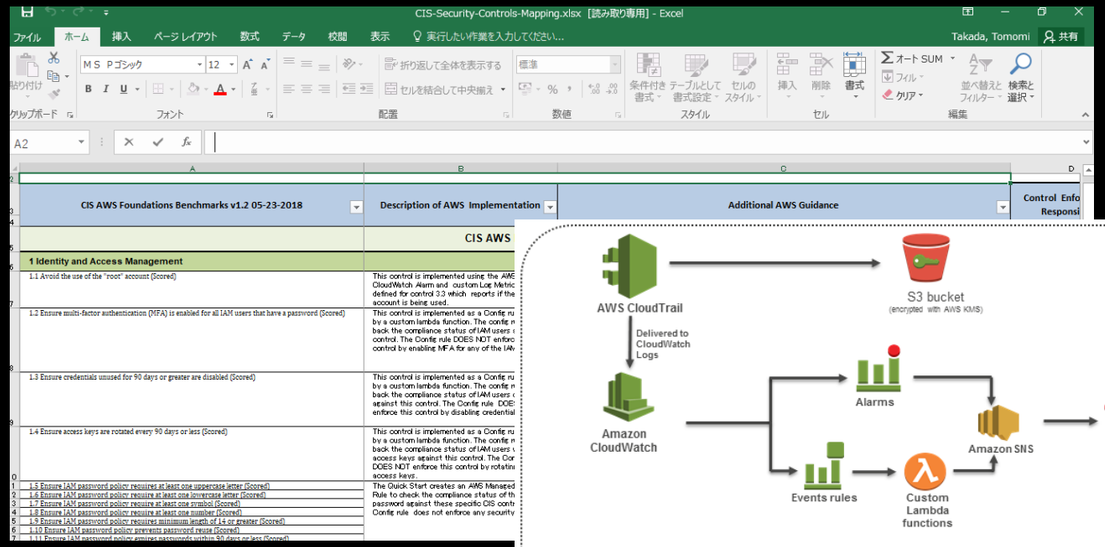
aws SUMMIT

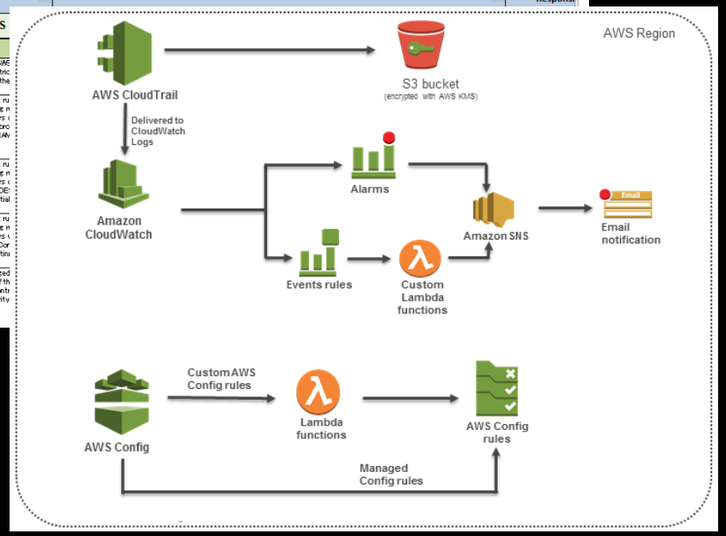
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Quick Starts Security & Compliance

定義と文書化

各種標準に準拠した環境のデプロイ用テンプレートを提供





要求事項に対する検討事項と対応指針のマッピング資料をまとめたマトリックスも付随

様々な内容がリリース済み

- CIS Benchmark
- PCI-DSS
- HIPAA/NIST etc

▶ **Quick Startsでも様々なセキュリティ要件への対応をまとめたマトリックスが提供されており、定義と文書化の作業の参考にすることができる**

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.3：チェックリスト

チェックリスト

1.3 Ensure credentials unused for 90 days or greater are disabled (Scored)

Profile Applicability:

- Level 1

Description:

AWS IAM users can access AWS resources using different types of credentials, such as passwords or access keys. It is recommended that all credentials that have been unused in 90 or greater days be removed or deactivated.

Rationale:

Disabling or removing unnecessary credentials will reduce the window of opportunity for credentials associated with a compromised or abandoned account to be used.

Audit:

Perform the following to determine if unused credentials exist:
Download Credential Report:
Using Management Console:

目的

- 対策状況に関する**確認項目の整理**

進め方

- 対応指針に則っていることを**確認する手段**について各項目についてまとめていく

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.3：チェックリスト

チェックリスト

要件
利用者の活動を記録したイベントログを取得し，保持し，定期的にレビューすること

対応方針
- 管理コンソール、及び、*API*による操作内容のログを収集するために*CloudTrail*を使用する
- ネットワークのアクセスログを収集するために*VPC Flow Logs*を有効化する
- マネージドサービスで取得可能なログについては・・・・・・・

目的
- 対策状況に関する**確認項目の整理**

進め方
- 対応指針に則っていることを**確認する手段**について各項目についてまとめていく

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.3：チェックリスト

チェックリスト

_CloudTrail_に関する確認項目例

- _CloudTrail_が全てのリージョンで有効化されているか
- _CloudTrail_のログファイルの_Validation_機能は有効化されているか
- _CloudTrail_のログを保管するS3のバケットは公開アクセスが禁止されているか
- _CloudTrail_のログは暗号化されて保管されているか

目的

- 対策状況に関する**確認項目の整理**

進め方

- 対応指針に則っていることを**確認する手段**について各項目についてまとめていく

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CIS Benchmark等の活用

チェックリスト

CIS Benchmark は、米国政府、企業、業界、学術機関のエキスパートが開発したコンセンサスベースの設定ガイドライン

CIS Amazon Web Services Foundationsでは以下のカテゴリの設定確認方法がCLIレベルで記載

- Identity And Access Management
- Logging
- Monitoring
- Networking

CIS Benchmarks : https://www.cisecurity.org/cis-benchmarks/

▶ **様々な領域でAWSのセキュリティに関するどのような項目を、どのような手段で確認すればよいかを確認できる**

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

CIS Benchmark等の活用

チェックリスト

確認内容例

確認項目
*Root*アカウントの利用を避ける

監査（確認方法）
本ベンチマークのモニタリングセクションで推奨される監視用フィルターを利用して*Root*アカウント利用時に通知を受けるようにする。
加えて下記のコマンドにより*Root*アカウントが使用された最新の時間を確認する。

```
# aws iam generate-credential-report
# aws iam get-credential-report --query 'Content' --output text | base64 -d | cut -d, -f1,5,11,16 | grep -B1 '<root_account>'
```


© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

チェックリスト作成の流れ

チェックリスト

お客様のデータ
アカウント・権限管理
ミドルウェア・アプリ
ゲストOS

利用者の責任範囲

仮想化レイヤー
コンピュート・ストレージ
ネットワーク・インフラ
物理セキュリティ

AWSの責任範囲
尊守状況が確認できれば今後この部分は**オフロード可能**にも

対応指針の文書化

アプリケーションの設計や運用について確認する項目

AWSサービスの設計や運用について確認する項目

AWSについての統制情報を確認する項目

チェックリスト

遵守状況の確認手段まで整理することで自動化のスコープに結びつける

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.4：チェック作業の自動化

自動化

目的

- **確認作業の自動化**と継続的な監視

進め方

- 具体的な確認手段のうち、AWS ConfigといったAWSのサービスを用いて**自動化できる部分を抽出**し、確認作業の自動化を行う

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Config / Config Rules

自動化

AWS Config

AWS環境の設定にルールを設け、そのルールが守られているかを評価（複数の機能群で構成）

- 標準で提供されているルールの利用と、ルールの作成
- 80を超えるマネージドルール（2019年6月時点）
- 評価結果に応じて各種アクションを定義

ルール項目の例

ルートアカウントのMFA

SSHの制限

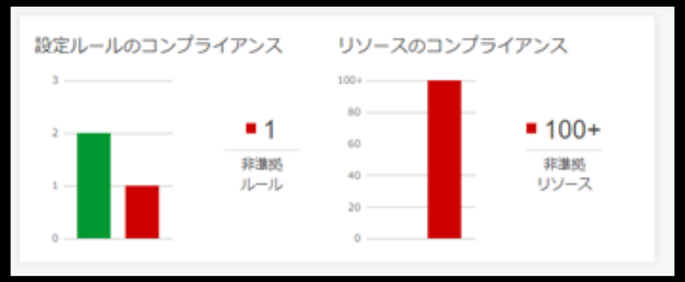
ボリュームの暗号化

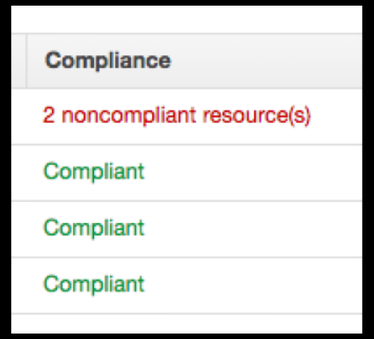
CloudTrailの有効化

タグの付与

ポート設定

評価結果表示画面





aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

80を超えるマネージドルールの活用

自動化

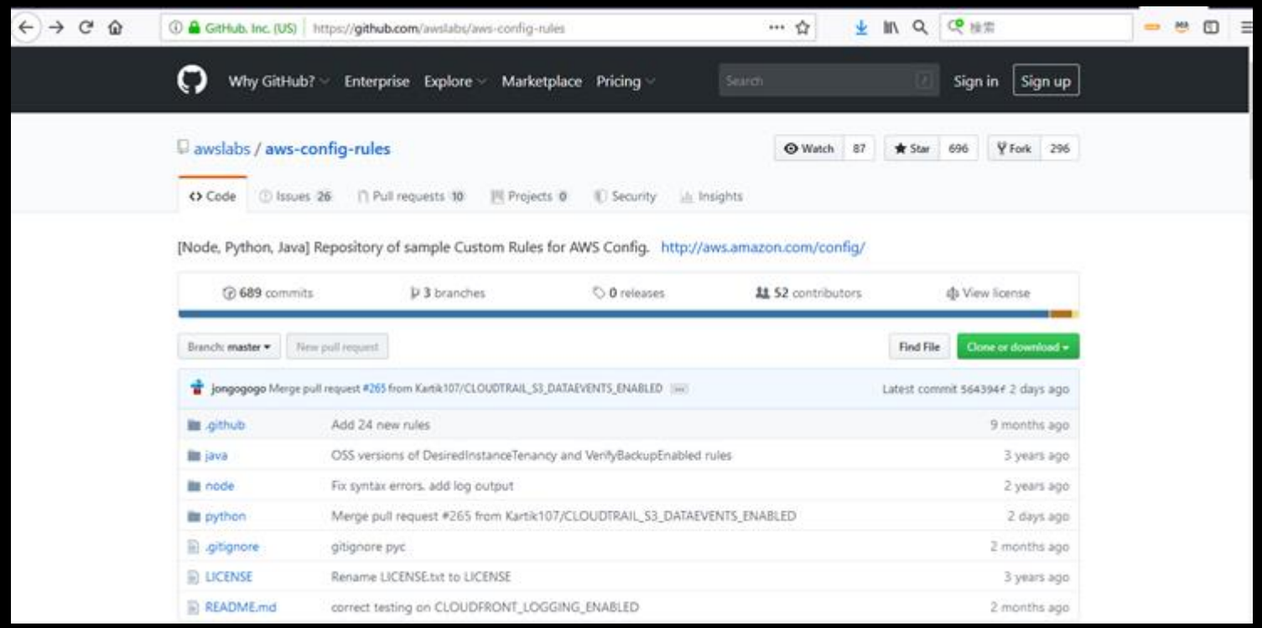
AWSにより用意されている評価ルール例

マネージドルール名	説明（あるべき状態）
s3-bucket-public-read-prohibited	S3バケットでパブリック読み取りアクセスが許可されないこと
elb-logging-enabled	ELBのログ記録が有効になっていること
restricted-ssh	EC2インスタンスのSSH 受信ポートが制限されていること
ec2-instance-managed-by-systems-manager	EC2インスタンスがSSM の管理下に入っていること
cloudtrail-enabled	CloudTrailが有効化されていること
access-keys-rotated	指定した日数以内にアクセスキーがローテートされていること

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Config Rules用のGitHubリポジトリの活用

自動化



https://github.com/awslabs/aws-config-rules

カスタムルール用のサンプル関数の
パブリックレポジトリ

- AWSコミュニティによって作成および提供

カスタムルールを作成するための
RDK (Rule Development Kit)も
AWSから提供

- ローカルでのルールの開発・テスト
- パラメータの設定
- デプロイ
- ログの確認
- マルチアカウント

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

自動化を検討する際の注意点

自動化

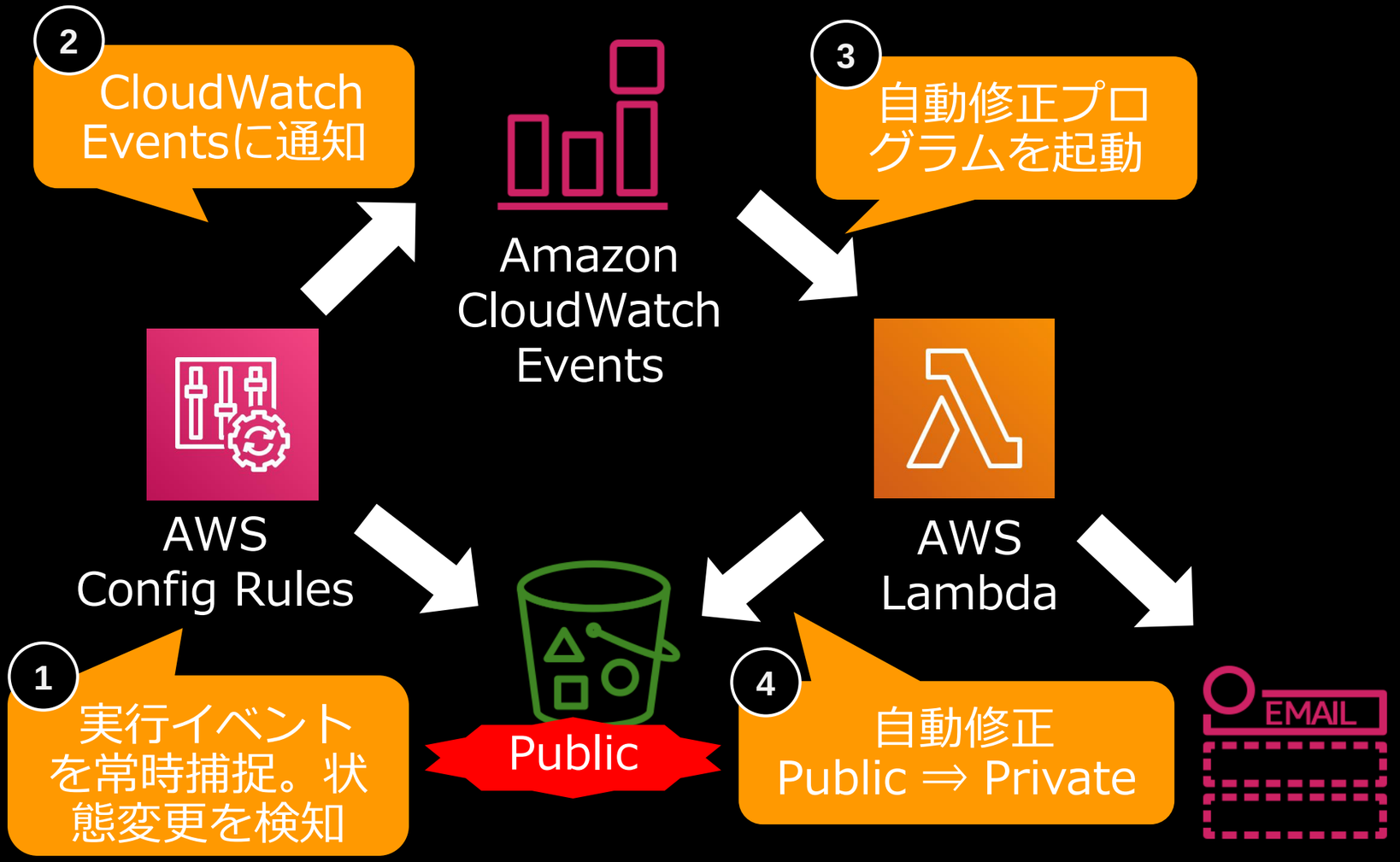
No.	検討が必要な要素	自動化が難しいケース
1	経済合理性があるか	マネージドサービスでのサポートもなく、過度な開発が必要な場合
2	対策状況の確認という目的を果たしているか	一定の自動化はできるが部分的で本来の対策状況の確認ができない場合
3	自動化が目的となっていないか	例外的あるいは特異な確認項目の場合

あらゆる項目の自動化は難しく、また常に適切という訳ではない。リスクや優先度、技術的難易度を鑑み「自動化すべき項目」と「自動化しない項目」を整理することが必要。また自動化すること自体が目的ではない。

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Step.5：継続的なモニタリング

モニタリング



目的

- 一時的な断面での情報ではなく**継続的な統制環境維持**の確認

進め方

- AWSの**イベント検知機能**と**監視機能**とを組み合わせ、継続的な監視状況を作り上げる

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon CloudWatch / Events

モニタリング

Amazon CloudWatch

AWSサービスの各種リソースを監視するマネージドサービス

CloudWatch Eventsは「ルール」を定義し、イベントソースとターゲットを紐付ける

- イベントソースとして各種 AWS サービスを選択可能
- ターゲットは Lambda、SQS、SNS、CodePipeline など

イベントソースの例

EC2のInstance States

スケジュール

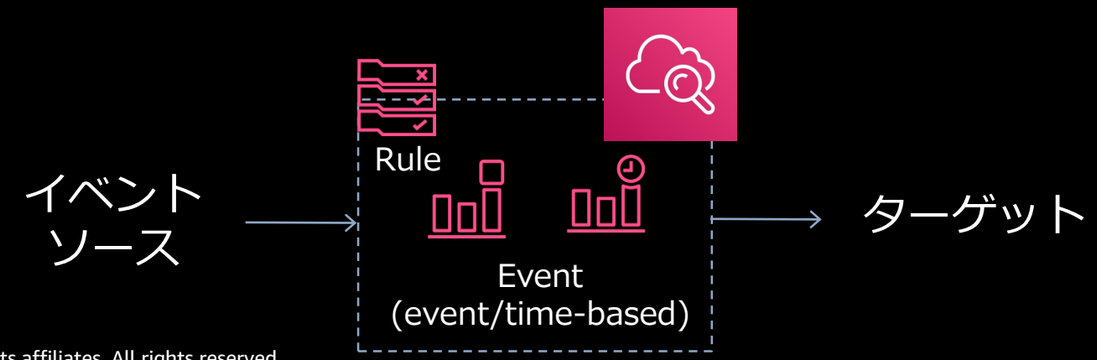
AWS API Call

AWS Console Log-in

AWS Config

Supportのケース作成

CloudWatch Eventsの動作



aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

セキュリティモニタリングを担うサービス

Insights & Standards

- AWS環境におけるセキュリティとコンプライアンス状態を一元表示
- AWSセキュリティサービスやパートナーソリューションで生成された結果を集約
- セキュリティの傾向を分析し重要度の高いセキュリティ課題を特定

AWS Security Hub

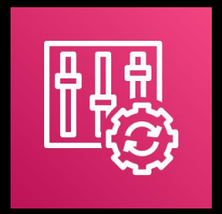
Findings

Security findings providers

Amazon Inspector

Amazon GuardDuty

Amazon Macie



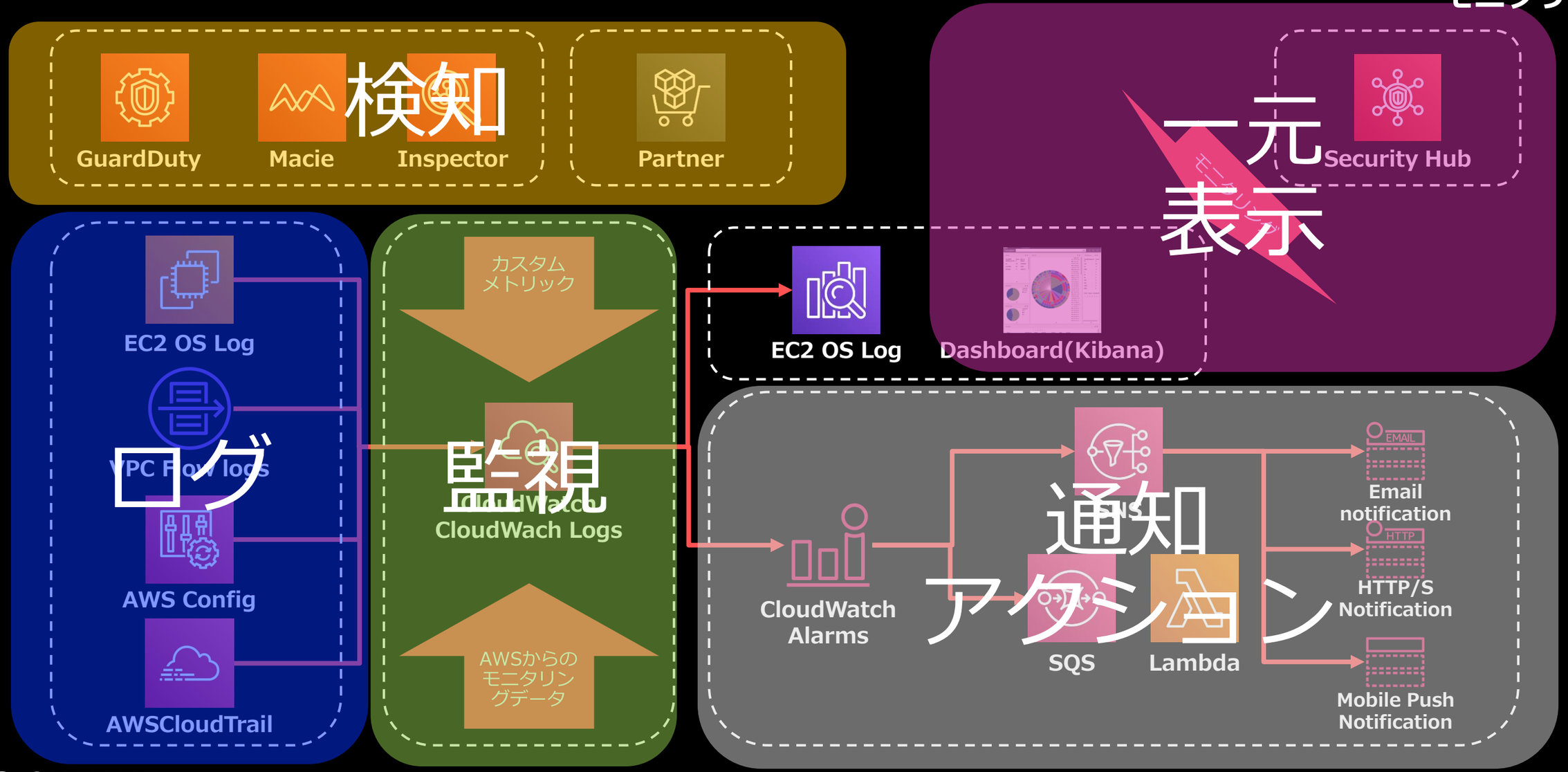
AWS Config

Partner Solutions

Other

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

継続的コンプライアンスを実現するサービス



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

継続的コンプライアンスの活用例

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S3上のデータの漏洩対策についての方針例

クラウド利用の方針
- データ保管にも利用
- 必要な人に対してのみの権限付与
- インターネット上からの許可のないアクセスの禁止
- 設定ミスや1人の内部犯行による漏洩の防止

リスク
- クラウド上にあるデータの漏洩

S3における対策方針例
- S3のバケットポリシー/ACLによる公開アクセス設定の禁止
- IAMによるバケットへの必要のないアクセスの制限
- IAMによるバケットの設定変更権限の制限
- 万が一公開設定が行われた場合の発見・修復措置の実装

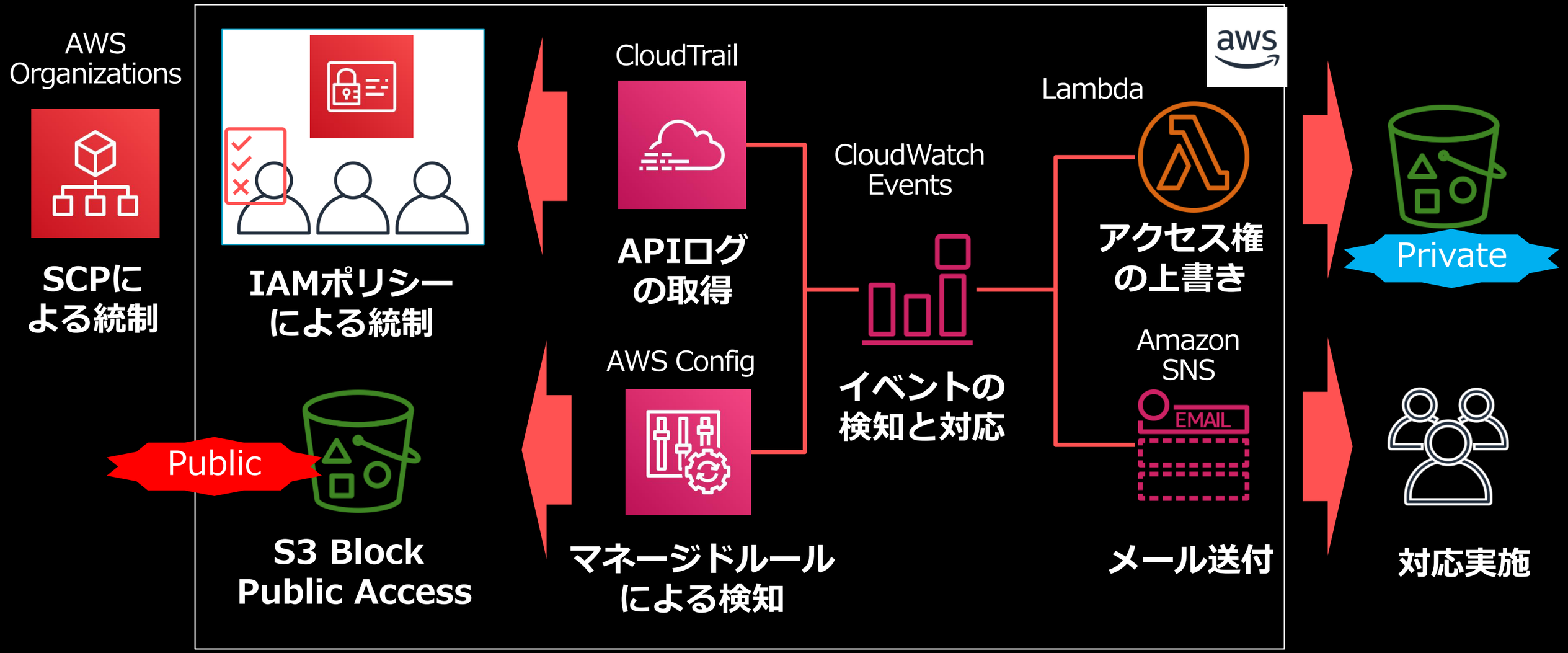
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

確認項目の整理とその自動化の例

No.	セキュリティ要件チェック項目	自動化アプローチ
1	バケットポリシー/ACLの 公開設定がされていないこと	S3 Block Public Access機能の利用
2	バケットへのアクセスに関する IAMポリシーの最小権限設定	IAMポリシー変更の APIログによる検知と通知
3	バケットの設定変更に関するIAMポ リシーの最小権限設定	OrganizationsのSCPによる子アカ ウントにおける設定変更の制限
4	S3 Block Public Accessが 有効化されていること	AWS Configによる設定変更の検知 とAWS Lambdaを用いた自動修復

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

継続的コンプライアンスによる統制例



© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

まとめ

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

本セッションのおさらい

現在のセキュリティ統制と監査における課題

AWSによる継続的コンプライアンスのアプローチの検討を

継続的コンプライアンスの導入に向けた5つのStep

ポイントはチェック作業の自動化と継続的モニタリング

継続的コンプライアンスの一つの活用例

既存の機能やコードを活用して是非はじめの一歩を

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Tomomi Takada
takadat@amazon.co.jp

aws SUMMIT

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.