AWS

SUMMIT

AWSセキュリティ入門

アマゾン ウェブ サービス ジャパン株式会社
セキュリティコンサルタント　松本 照吾

2017/6/2

松本 照吾(Shogo Matsumoto)

AWS Professional Services / Security Consultant

得意分野

・セキュリティポリシー策定支援
・各種コンプライアンス認証への適合支援

好きなAWSサービス

・プロフェッショナルサービス

主な保有資格、活動

・AWS認定資格5資格★★★★★
・ CISA、CISSP、MBA（University of Massachusetts Lowell）
・ 公認情報セキュリティ主任監査人（JASA CAIS-lead auditor）

本日お伝えしたいこと

AWSを知り始めて、セキュリティに不安を覚える皆様に、

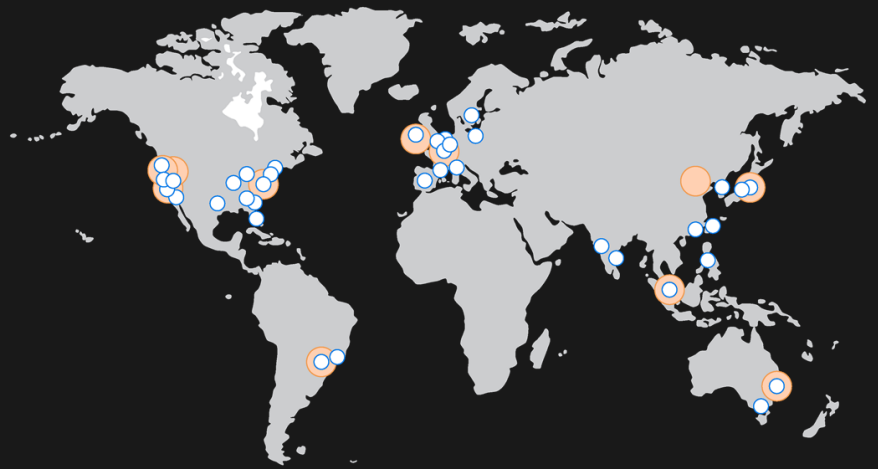
AWS によってセキュア、かつ運用を効率化＝”楽”にするセキュリティを実現する方法をご紹介します。

今回は、その中でも**特に重要な四つのサービス**をご紹介します。

AGENDA

- 本セッションの目的
- クラウドセキュリティの期待と不安
- AWSがセキュリティにもたらしたもの
- AWS Identity and Access Management (IAM)がもたらす
  クラウド時代の認証認可
- AWS Key Management Service (KMS)がもたらす
  暗号鍵管理からの解放
- Amazon Inspectorがもたらすスケーラブルな脆弱性管理
- AWS Certificate Manager（ACM)がもたらす
  “常時SSL”時代の経路暗号化
- まとめにかえて

クラウドセキュリティへの期待と不安



クラウドのセキュリティに不安はありませんか？

- クラウド＝不透明
- クラウド＝規格や法令順守が困難
- クラウド＝セキュリティ管理が複雑

一方で！！！

“金融業界は最悪なサイバー犯罪に狙われている。我々はAWSと綿密に協同したセキュリティモデルを発展させることで、自分たちでデータセンターを所有する以上に安全な運用をすることができるようになる”

Rob Alexander, Capital One's chief information officer
AWS re:Invent 2015 Key Note

組織のクラウド経験によって
大きなギャップが存在する。

そもそも
“良いセキュリティ”とは何か。

セキュリティとは？

アクセスコントロールや
暗号化など

電子署名など

バックアップ、冗長化設計など

Work Factor（労力要因）で考えるセキュリティ

(I) 一般的なセキュリティにおける用法：

一定量の専門能力と資源を使うとき、潜在的な侵入者がシステムに侵入するのに要する、あるいは、特定の対策を突破するのに要すると予想される労力もしくは時間の見積もり

Internet Security Glossary

https://www.ipa.go.jp/security/rfc/RFC2828-03WJA.html

Work Factor＝何かを行う時の面倒くささ

一方で運用、利用する側も。

面倒な運用なら、セキュリティはやりたくない
＝**形骸化、無視**

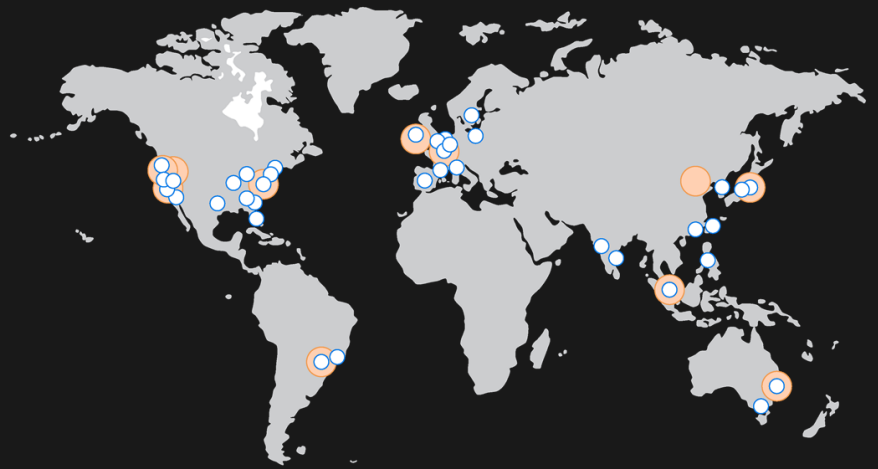
利用/運用側の**Work Factorを軽減すること**
もセキュリティの重要な要素

つまり、“**良い**”セキュリティとは、

本質的にセキュアなことに加えて、
運用/利用側のWork Factorを減らすことで、
本来業務にフォーカスできる、

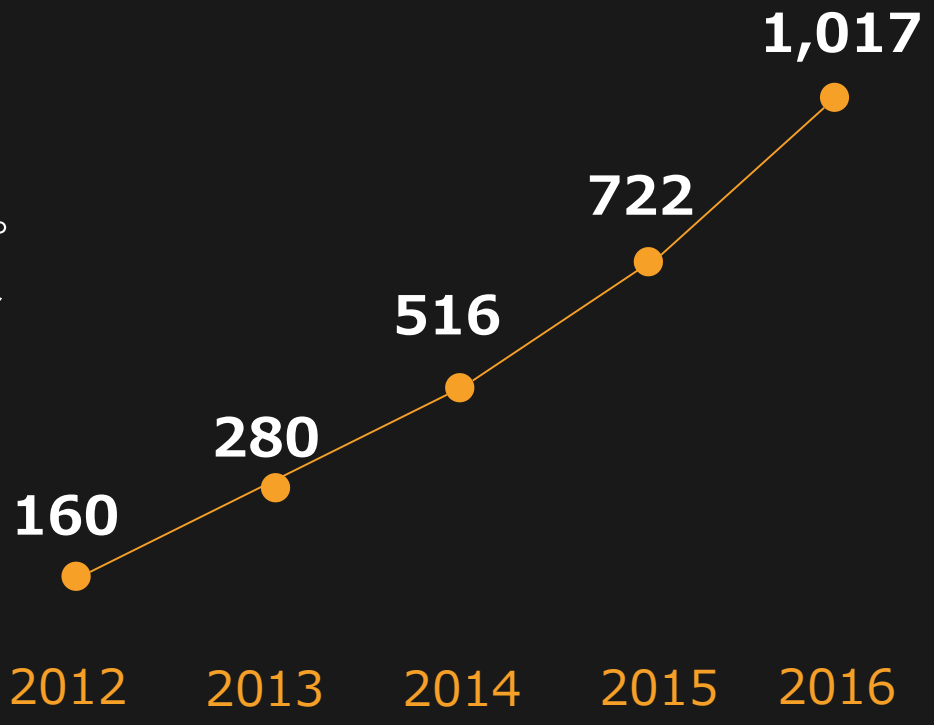
“**楽**”なセキュリティ

AWSがセキュリティにもたらしたもの



規模の経済：AWSの持続的な改善、提供

- スタートアップもエンタープライズも等しくセキュアなインフラを利用可能



すべてをコンプライアンスに準拠したインフラストラクチャで構築

amazon web services

AWS の基盤サービス

コンピューティング | ストレージ | データベース | ネットワーキング

AWS グローバルインフラストラクチャ

アベイラビリティーゾーン

リージョン

エッジロケーション

AWS はクラウドのセキュリティに責任を持つ

お客様に代わって AWS が負担となる作業を実行

AWSが
管理する
セキュリティ

＋

お客様

お客様が
管理する
セキュリティ

＝

求めるべき
セキュリティ
レベル

お客様に代わって AWS が負担となる作業を実行

求めるべき
セキュリティ
レベル

−

AWSが
管理する
セキュリティ

＝

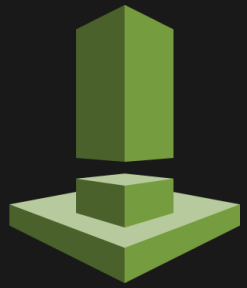
お客様

お客様が
管理する
セキュリティ

セキュリティを分担できることは、
お客様がやるべきことへの集中をもたらす
これがAWSセキュリティ責任共有モデルです。

IAM

AWS
KMS



Amazon
Inspector

ACM

サーバからサービスへ

お客様に代わって AWS が負担となる作業を実行

求めるべき
セキュリティ
レベル

－

amazon web services

AWSが
管理する
セキュリティ

ここを大きくすると

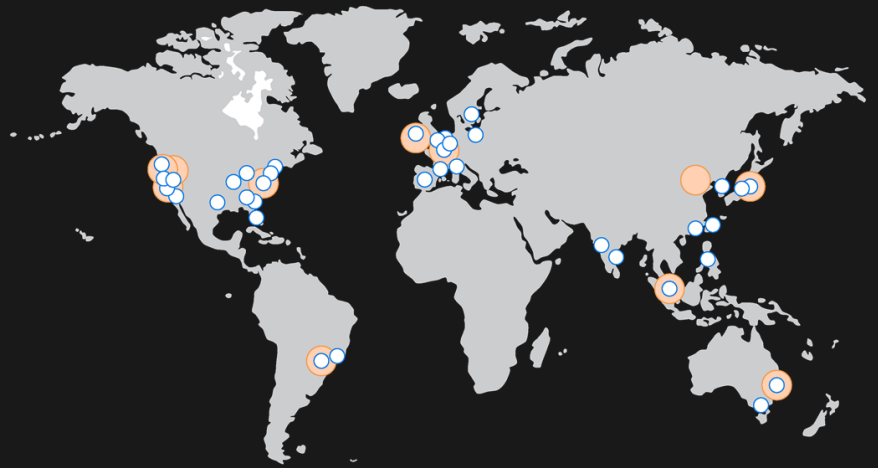
＝

お客様

お客様が
管理する
セキュリティ

ここは小さくなる
→負担が減る！！！

AWS Identity and Access Management (IAM)がもたらすクラウド時代の認証認可



AWS Identity and Access Management (IAM)

AWS操作をよりセキュアに行うための認証・認可の仕組み

AWS利用者の認証と、アクセスポリシーを管理

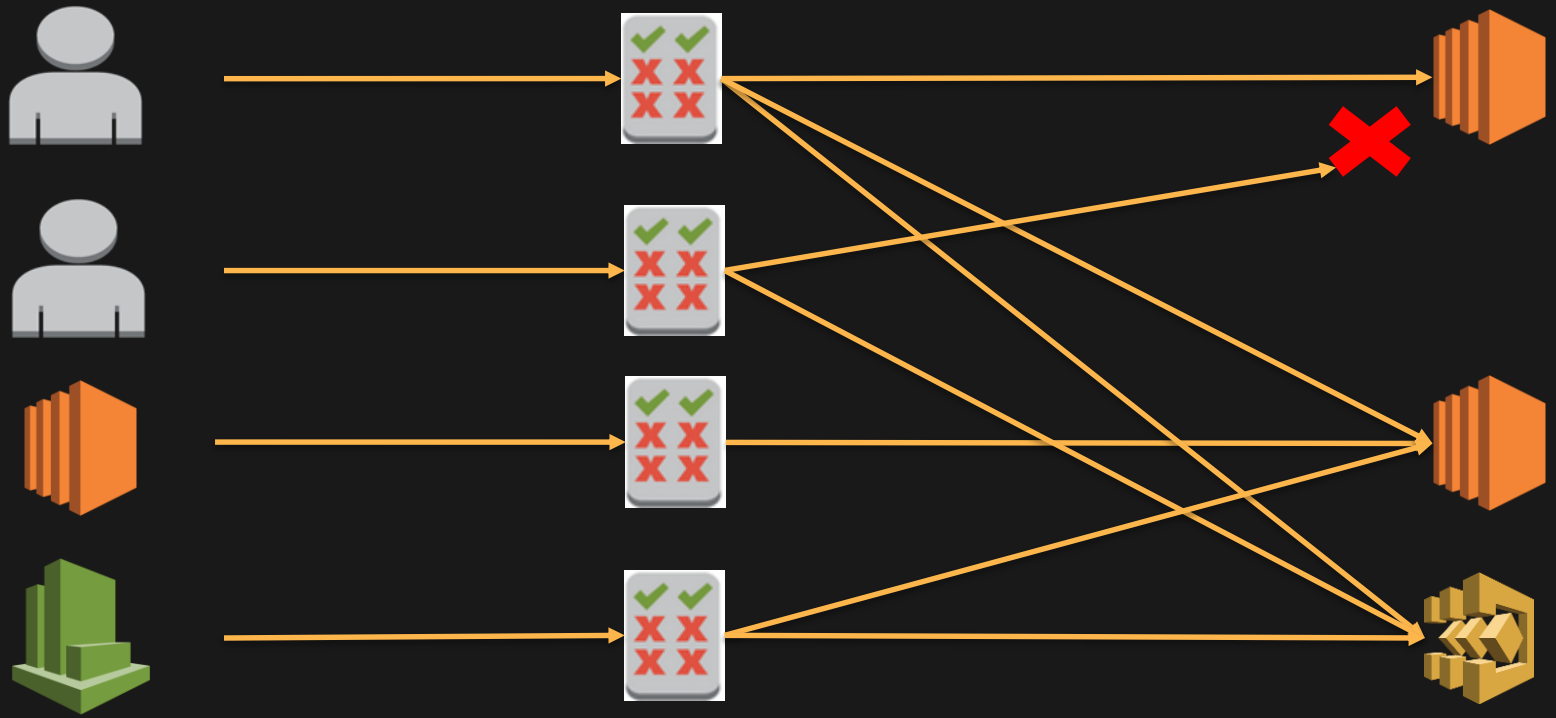
- AWS操作のためのグループ・ユーザー・ロールの作成が可能
- グループ、ユーザーごとに、実行出来る操作を規定できる
- ユーザーごとに認証情報の設定が可能

IAM動作イメージ

アクセスする主体に
対する**認証を提供**

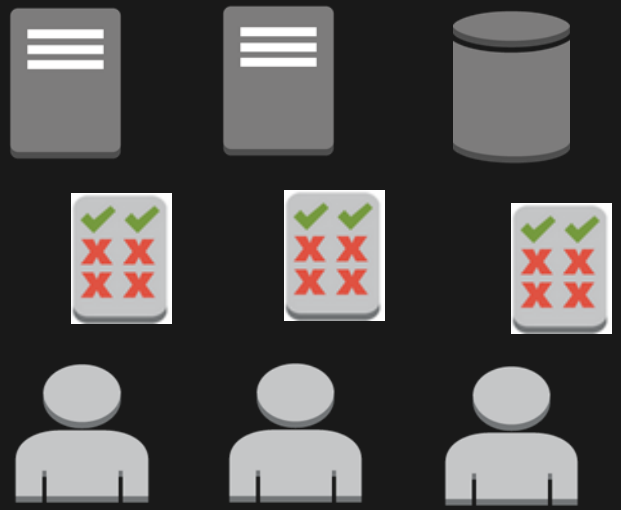
アクセスコントロールを
ポリシーとして定義

AWSの各サービスに
対する**認可を提供**



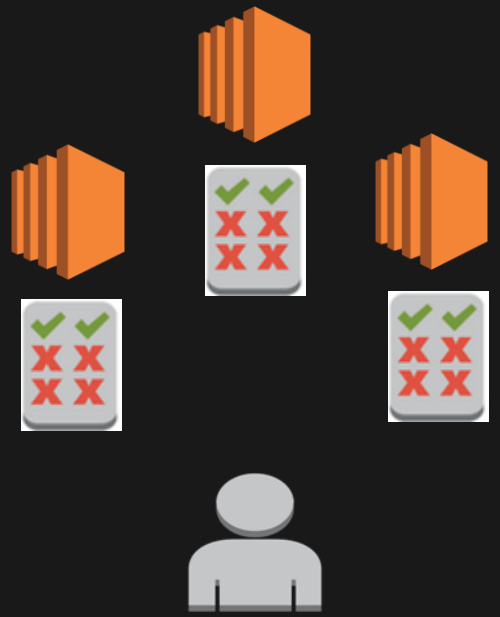
オンプレミスにおける権限管理

オンプレミスの世界



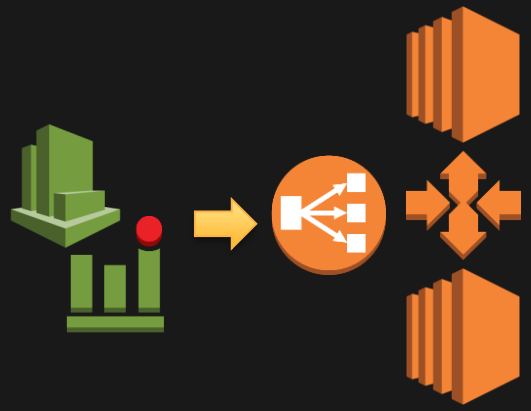
ポリシーは、変更が少なく、単純に管理されることが多かった。

スケールイン/アウトとポリシーの関係



インスタンスに合わせて
ポリシーもそれぞれに
適用される必要がある。

Infrastructure as codeとポリシーの関係



ヒトではないもの
同士がつながる

新しいサービスの追加とポリシーの関係

新しいサービスに対しての
アクセス可否をどこかで
決定しなければならない

IAMがもたらす価値

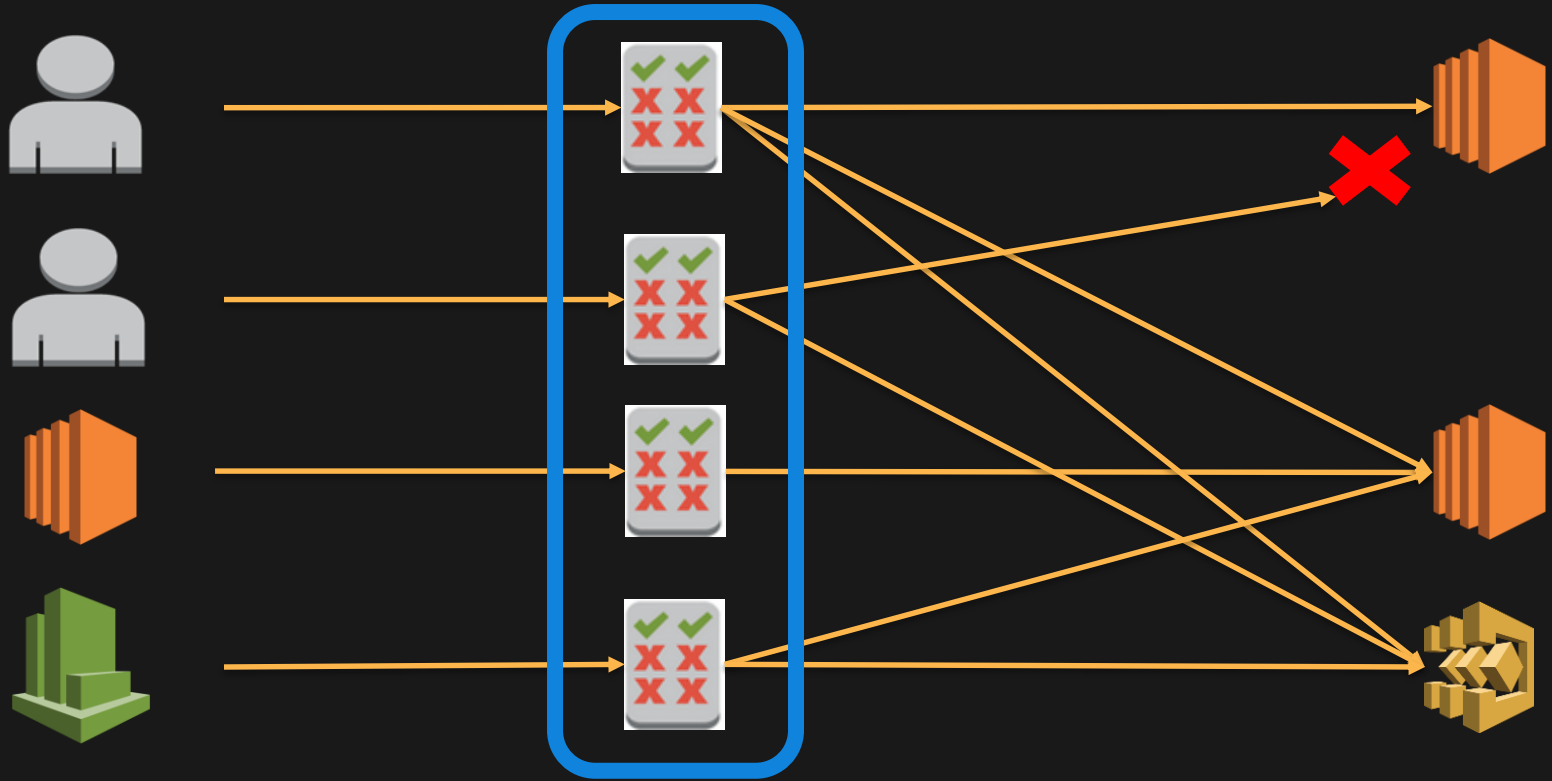
- IAMが利用者にかわって、変更されるポリシーの管理や、異なるサービスに対する共通言語を提供する。
- もちろん、お客様の要望に応じた柔軟なポリシー適用が可能となる。

IAM動作イメージ

アクセスする主体に
対する**認証を提供**

アクセスコントロールを
ポリシーとして定義

AWSの各サービスに
対する**認可を提供**

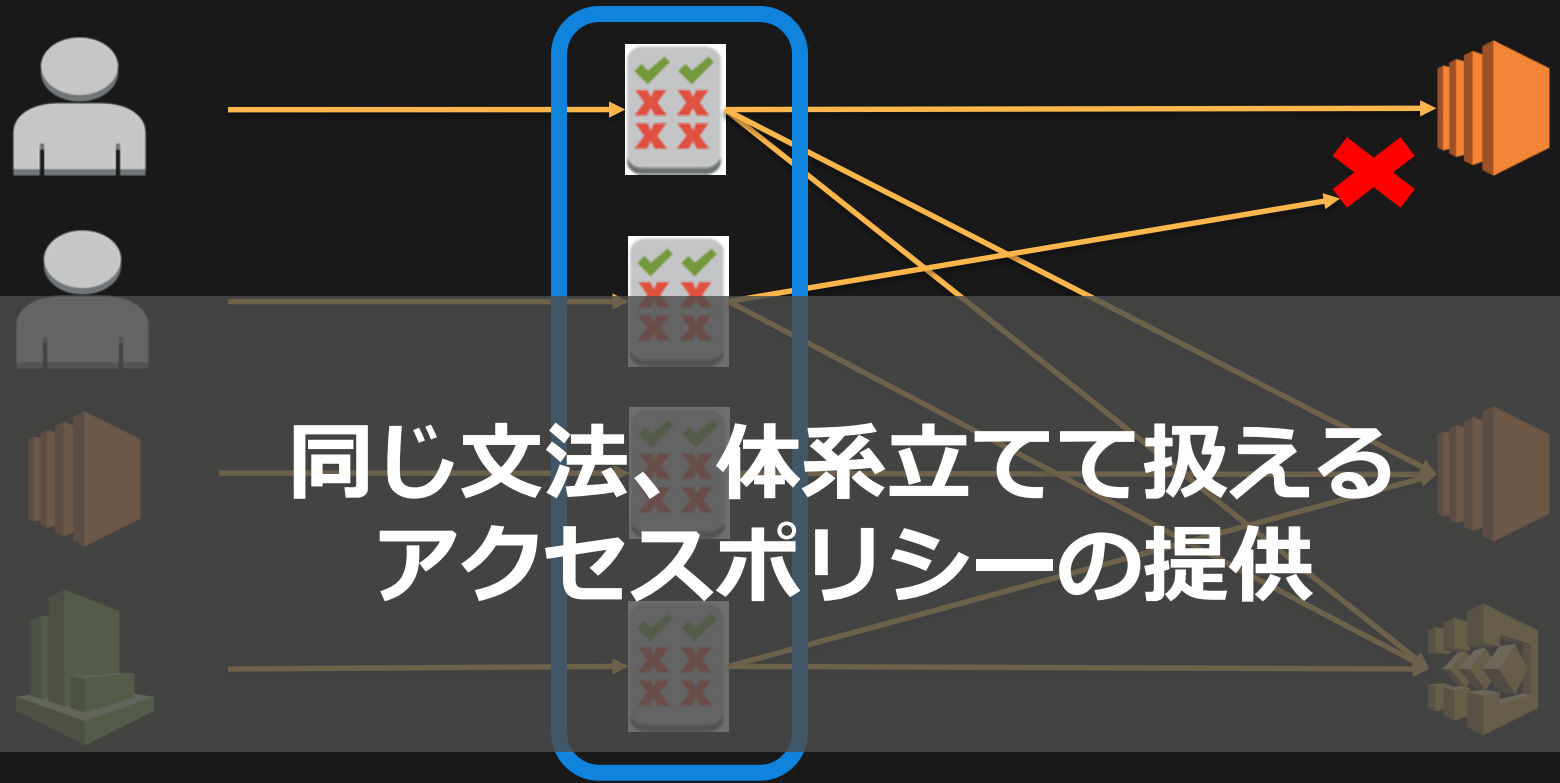


IAM動作イメージ

アクセスする主体に
対する**認証を提供**

アクセスコントロールを
ポリシーとして定義

AWSの各サービスに
対する**認可を提供**



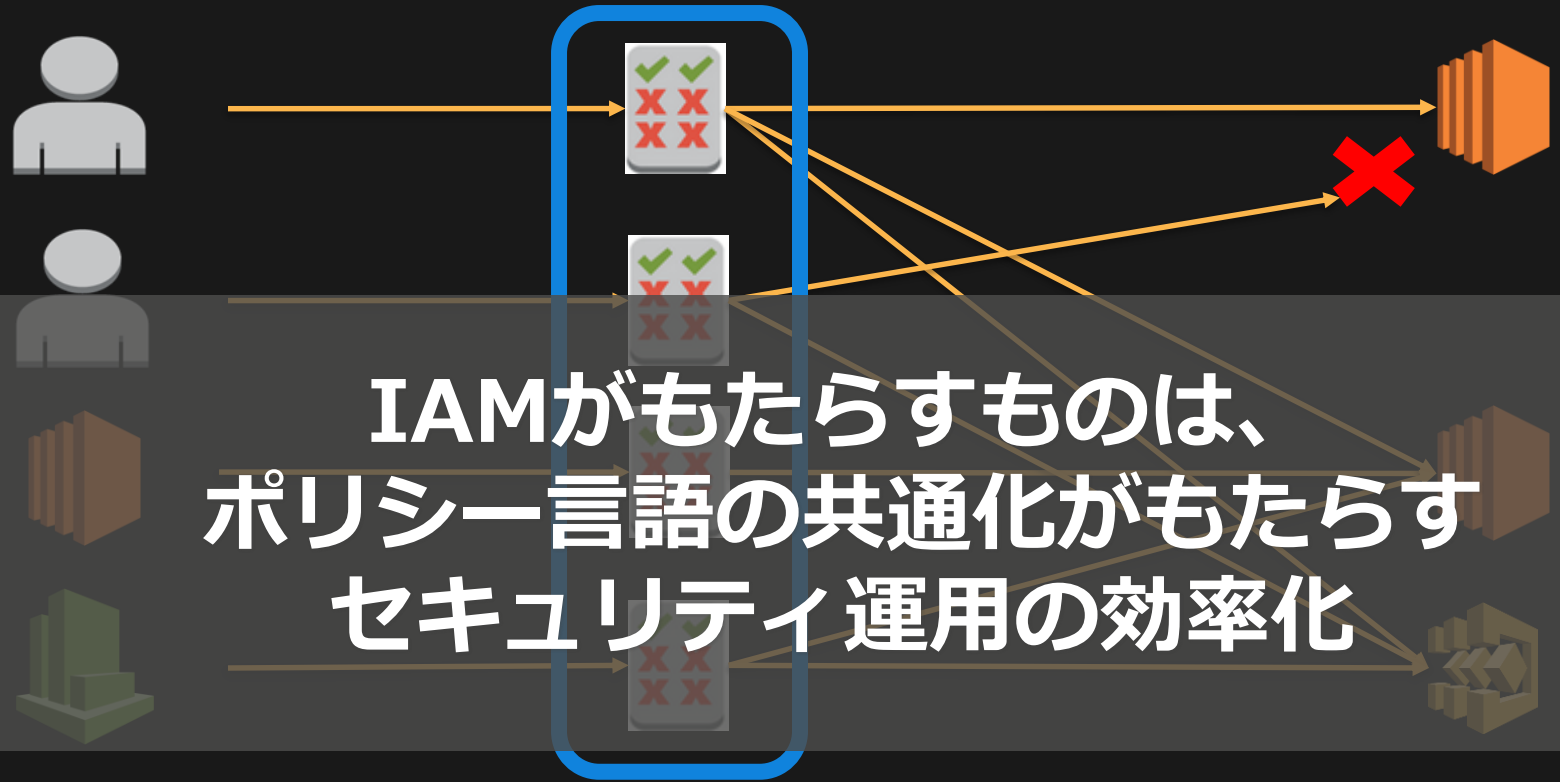
同じ文法、体系立てて扱える
アクセスポリシーの提供

IAM動作イメージ

アクセスする主体に
対する**認証を提供**

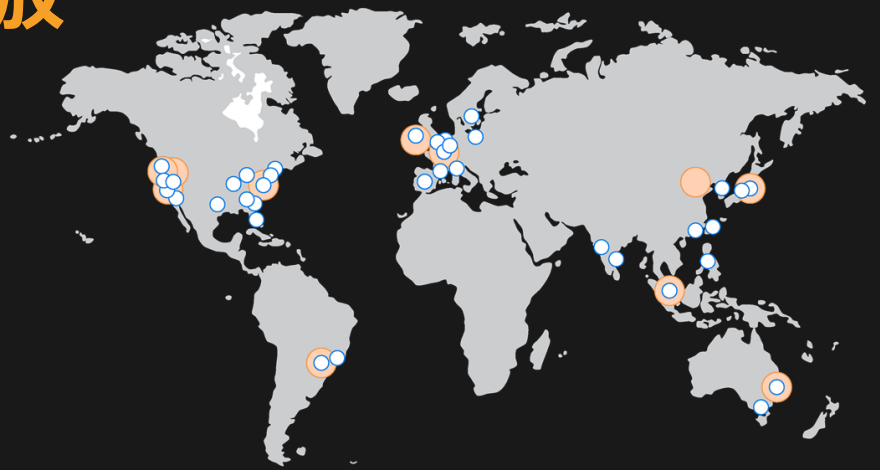
アクセスコントロールを
ポリシーとして定義

AWSの各サービスに
対する**認可を提供**



IAMがもたらすものは、
ポリシー言語の共通化がもたらす
セキュリティ運用の効率化

AWS Key Management Service (KMS)が
もたらす暗号鍵管理からの解放



AWS Key Management Service

暗号鍵の作成、管理、運用サービス

- 暗号鍵の可用性、機密性を確保
- 暗号鍵の有効化・無効化、ローテーション
- AWSサービスにおけるデータを暗号化
- SDKとの連携でお客様の独自アプリケーションデータを暗号化

鍵の管理は**いつも、大変**

セキュアな鍵管理環境の維持

鍵が失われたら、
全ての情報へのアクセスが
失われる。

鍵のライフサイクル管理の維持

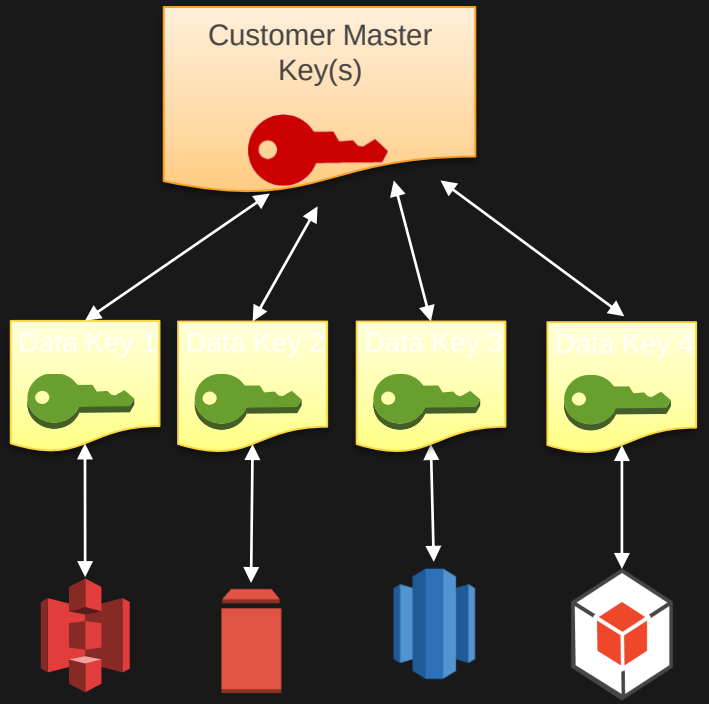
鍵の更新、失効などのライフサイクル管理のための運用が必要となる。

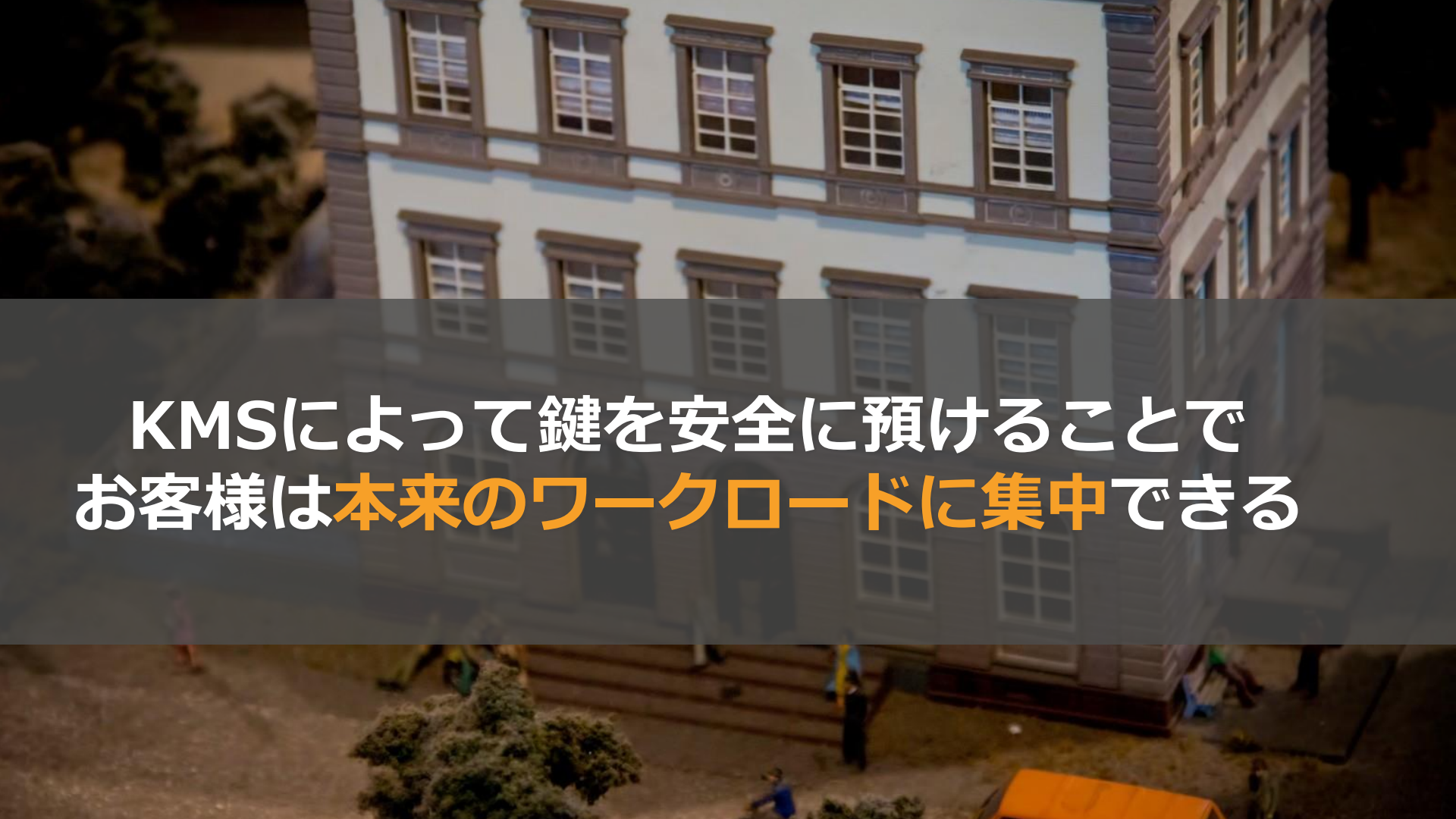
暗号化のサービスへの実装

暗号化を実装として組み込むための開発ワークロードには工数がかかる。

KMSがもたらす価値

- 暗号鍵管理のマネージドサービス（ライフサイクル管理）
- セキュアな鍵管理環境の提供
- AWSサービスとの統合



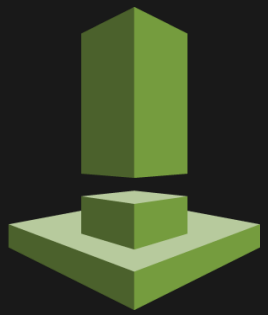


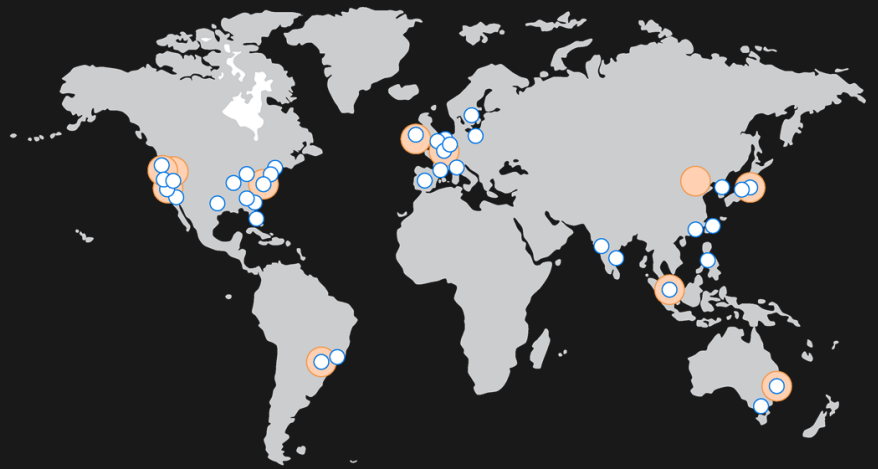
KMSによって鍵を安全に預けることで
お客様は本来のワークロードに集中できる



さらに言えば、AWSがもたらす価値は
暗号化に対するお客様のニーズに沿った
豊富なオプション

Amazon Inspectorがもたらすスケーラブルな脆弱性管理

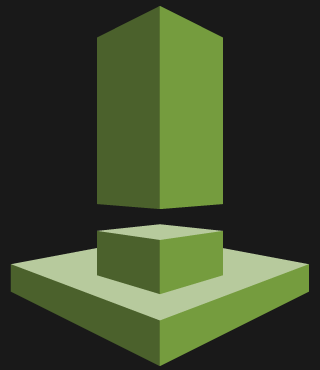




Amazon Inspector

自動化された
セキュリティ評価サービス

- Amazon EC2にエージェントを導入し、セキュリティを評価するホスト型診断
- AWSへの事前申請の必要なし。




サービスインフラは日々、変動する。

評価すべきルールセットの管理

日々、発見されるプラットフォームの脆弱性情報をどのように収集するか。

変動するインフラ

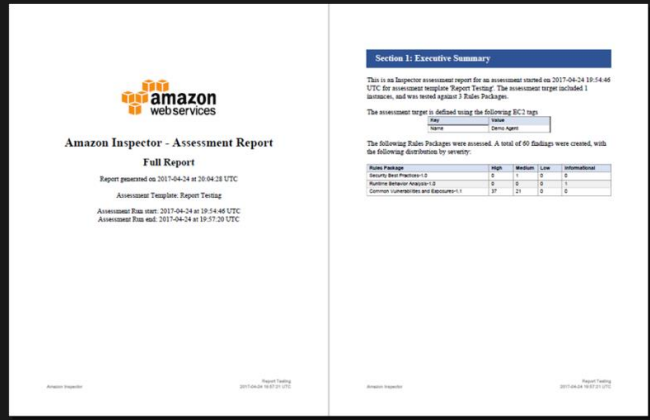
評価すべきサーバインスタンスの状況を可視化することは難しい。

“理解可能”な改善案の提示

発見された脆弱性に対する緊急度、対応の方針はどのように立案できるか。

Inspectorがもたらす価値

- AWSが提供する複数のルールパッケージによる評価
- 評価結果のエグゼクティブサマリ提供
- 自動化によるDevOpsプロセスへの統合



amazon web services

Amazon Inspector - Assessment Report

Full Report

Report generated on 2017-04-24 at 20:04:28 UTC

Assessment Template: Report Testing

Assessment Run start: 2017-04-24 at 19:54:46 UTC
Assessment Run end: 2017-04-24 at 19:57:20 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2017-04-24 19:54:46 UTC for assessment template 'Report Testing'. The assessment target included 1 instances, and was tested against 3 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value
Name	Demo Agent

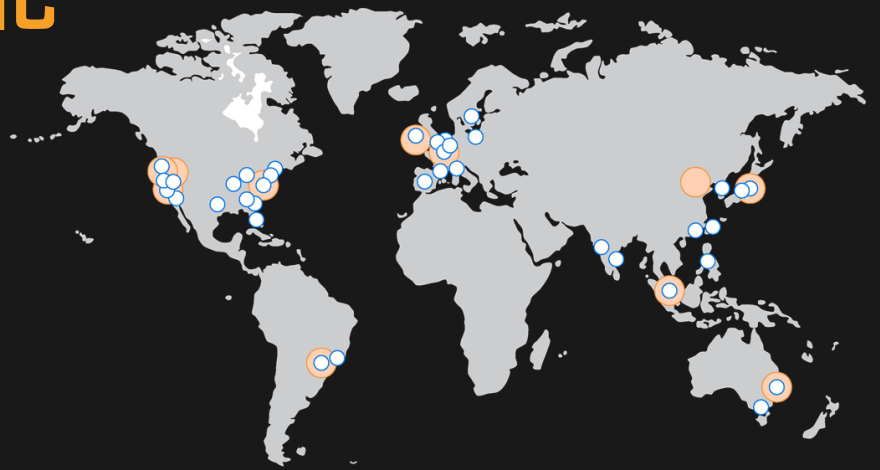
The following Rules Packages were assessed. A total of 60 findings were created, with the following distribution by severity:

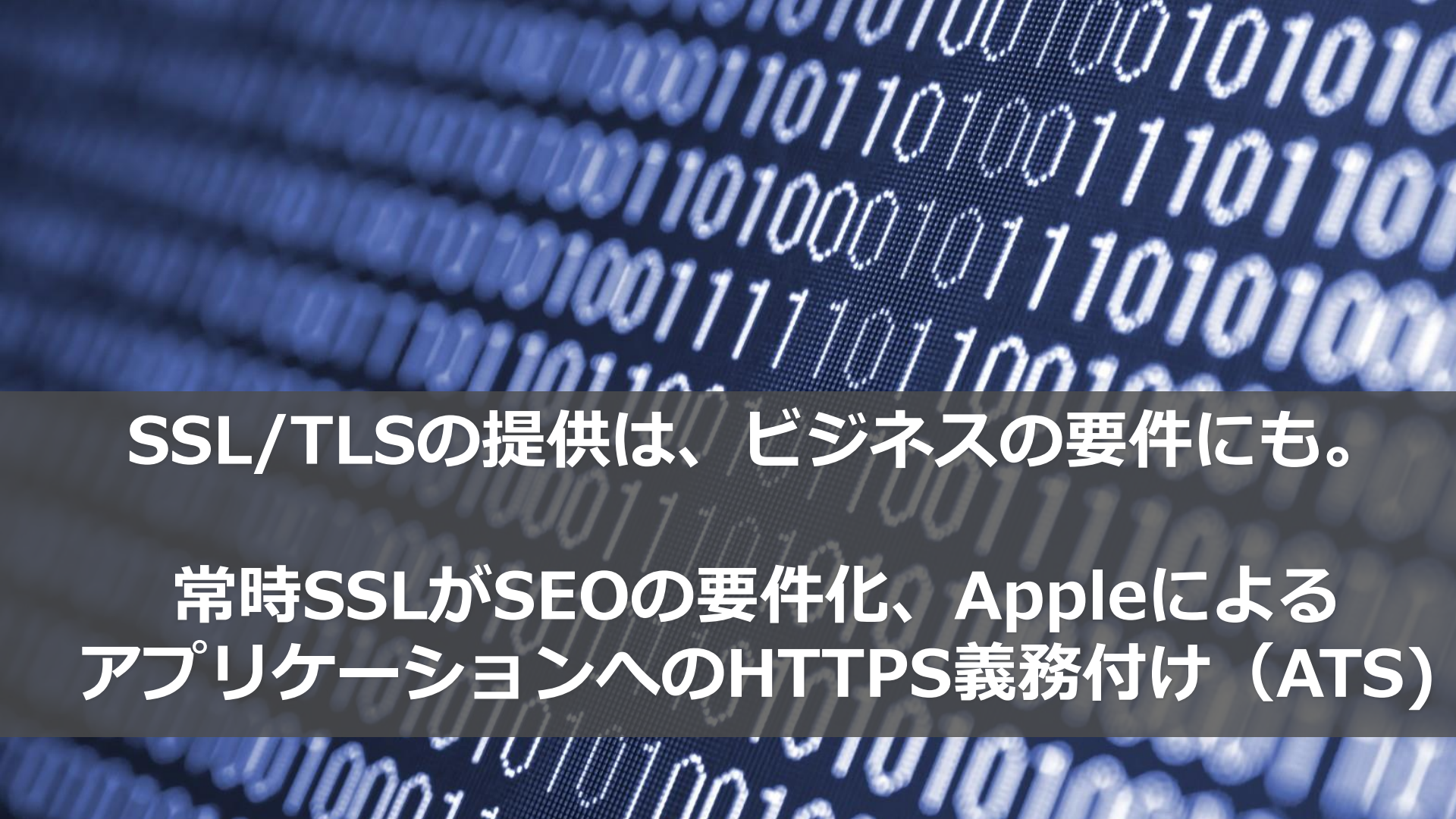
Rules Package	High	Medium	Low	Informational
Security Best Practices-1.0	0	1	0	0
Runtime Behavior Analysis-1.0	0	0	0	1
Common Vulnerabilities and Exposures-1.1	37	23	0	0

評価タイミングのスケジュール化、自動化

DevOpsの一歩先を行く、SecureなCI/CD（DevSecOps）

AWS Certificate Manager（ACM)がもたらす
“常時SSL”時代の経路暗号化



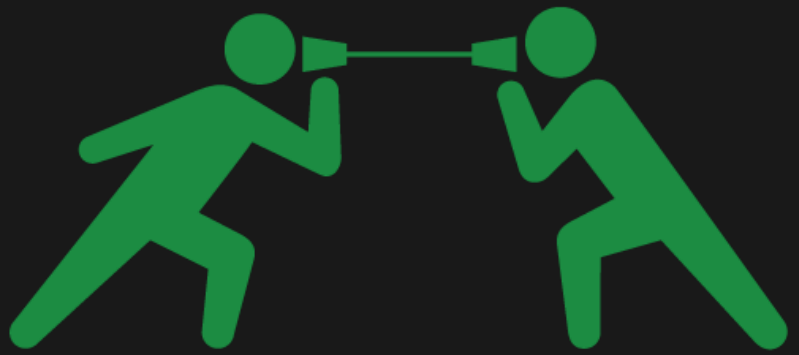


SSL/TLSの提供は、ビジネスの要件にも。

常時SSLがSEOの要件化、Appleによる
アプリケーションへのHTTPS義務付け（ATS）

SSL/TLS証明書の役割

自己の証明
経路の暗号化



AWS Certificate Manager(ACM）

簡単にSSL/TLS証明書を作成・管理・配置

- ドメイン認証（DV）タイプの証明書を無料で提供
- 秘密鍵はAWSサービス内で安全に管理される
- 更新も自動的に行われる

脆弱性が潜在するリスク

古いバージョンを利用し続けることによるセキュリティ侵害の大きなリスク
Ex. Heart breed

失効、更新に対する運用の負荷

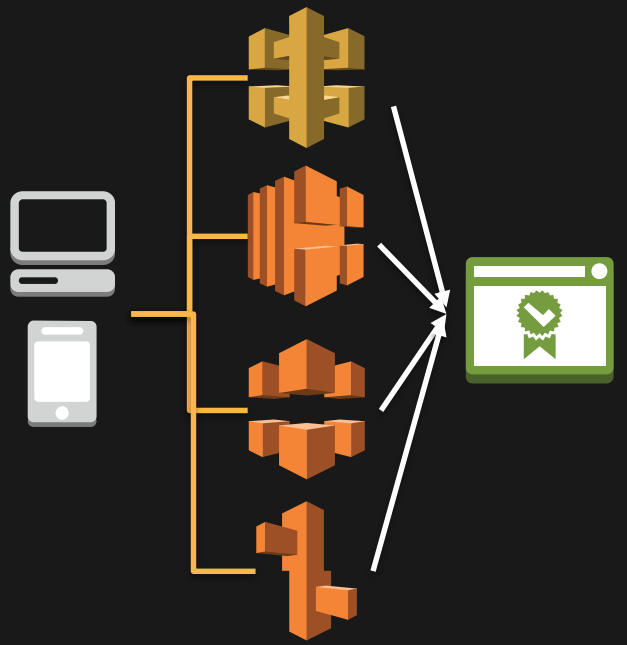
証明書の期限切れは管理の不備をエンドユーザに見せてしまう事態に

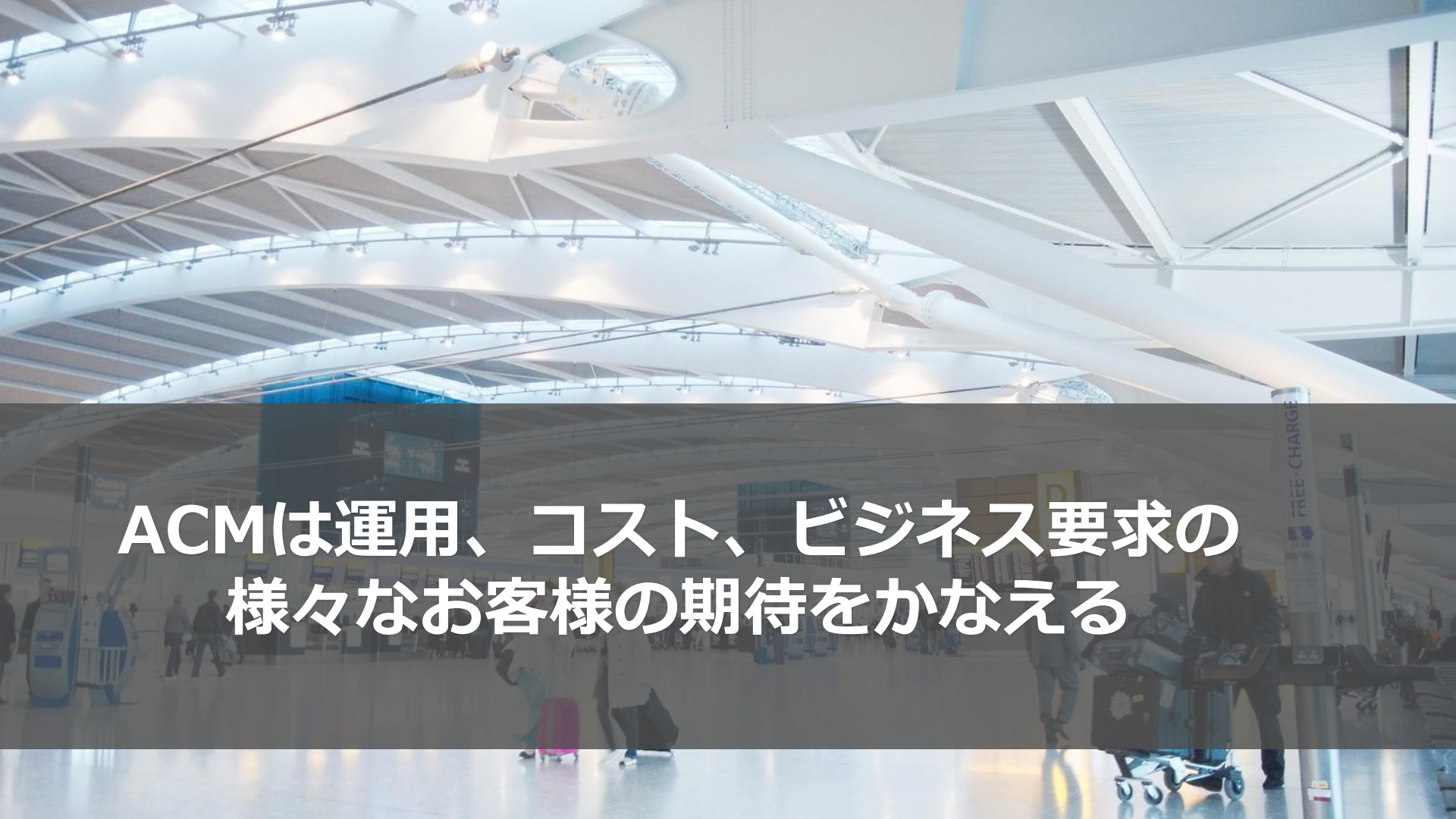
証明書に係るコスト

すべての通信経路を有償の証明書を使って暗号化することは、コストに対するインパクトをもたらす。

ACMがもたらす価値

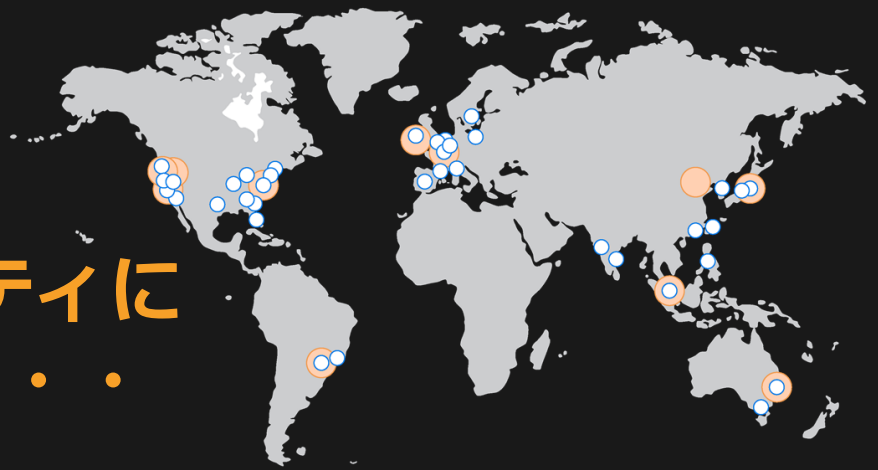
- AWSが更新処理をマネージドサービスとして管理
- CloudFront,ELBなどのAWSサービスへの統合
- 利用は**無料**





ACMは運用、コスト、ビジネス要求の様々なお客様の期待をかなえる

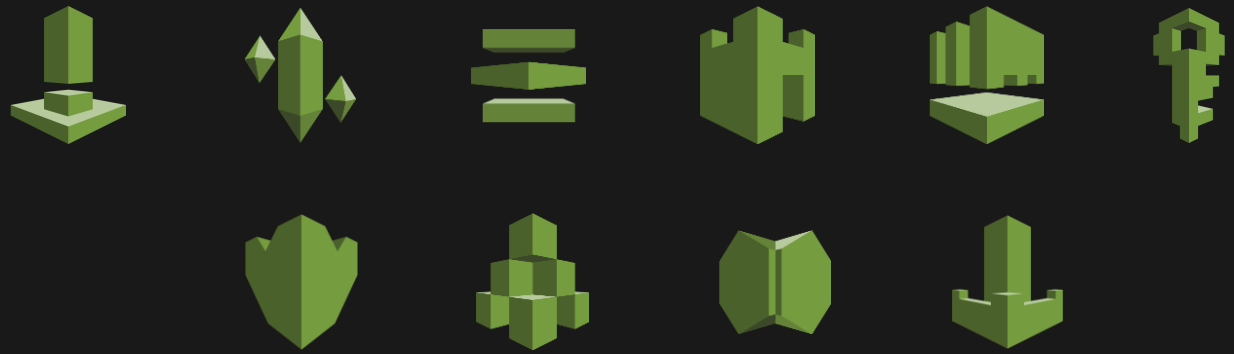
まとめにかえて



つまり、AWSがセキュリティに
もたらしたものは・・・・・・

責任共有モデル、マネージドサービスの活用により、
お客様のWork Factorの軽減をもたらします。
つまり、“**楽に運用**”できるセキュリティを提供します。

そして今日ご紹介したのは、ほんの一部です。



皆様も幅広く、深いAWSセキュリティの世界に触れてみてください。

AWSクラウドサービス活用資料集
セキュリティ & アイデンティティ
https://aws.amazon.com/jp/aws-jp-introduction/

本セッションのFeedbackをお願いします

受付でお配りしたアンケートに本セッションの満足度やご感想などをご記入ください
アンケートをご提出いただきました方には、もれなく素敵なAWSオリジナルグッズを
プレゼントさせていただきます

アンケートは受付、又はパミール3FのEXPO展示会場内にて回収させて頂きます

AWS

SUMMIT

ご清聴、ありがとうございました！

amazon web services