aws INNOVATE
ONLINE CONFERENCE

IoTにおけるセキュリティ考慮事項とAWSを活用した対策のご紹介

飯塚 将太
Amazon Web Services Japan
IoT Solution Architect

Twitterハッシュタグ #AWSInnovate

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

お伝えしたいこと

IoT環境では、**物理**や**デバイス**のレイヤまで含めてセキュリティを考慮する必要がある

IoTデバイス**特有の特徴や制約**から、IoT特有のセキュリティ要件が生まれる

AWS IoTを用いることで、IoT特有の**セキュリティ要件を解決**できる

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

取り扱う内容

1. IoTにおけるセキュリティ考慮事項

2.IoTデバイス特有の要件

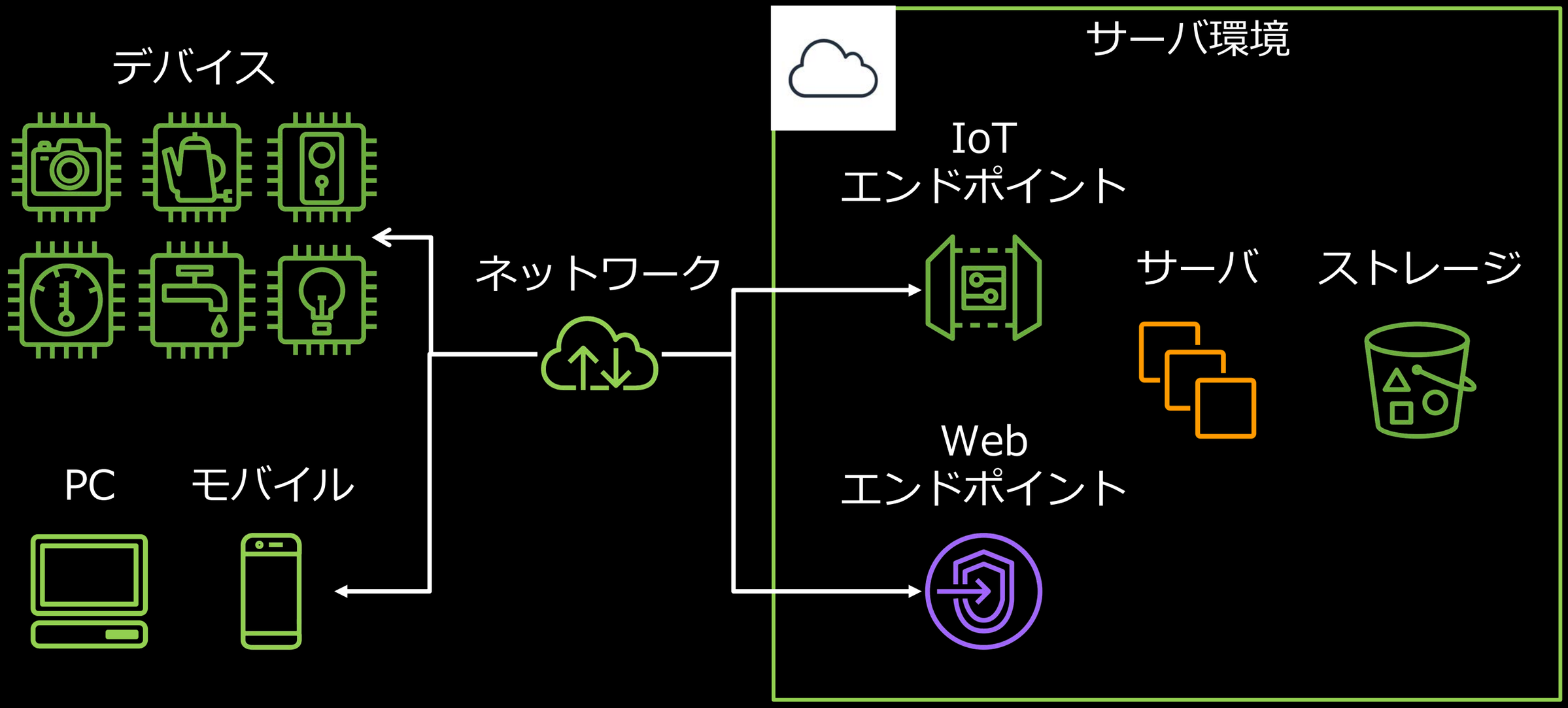
3.AWSを活用したセキュリティ対策

4.クイズ

本セッション内容について確認するためのクイズおよび
簡単なアンケートがセッションの最後にあります
なおクイズの回答はアンケートとあわせて表示されます

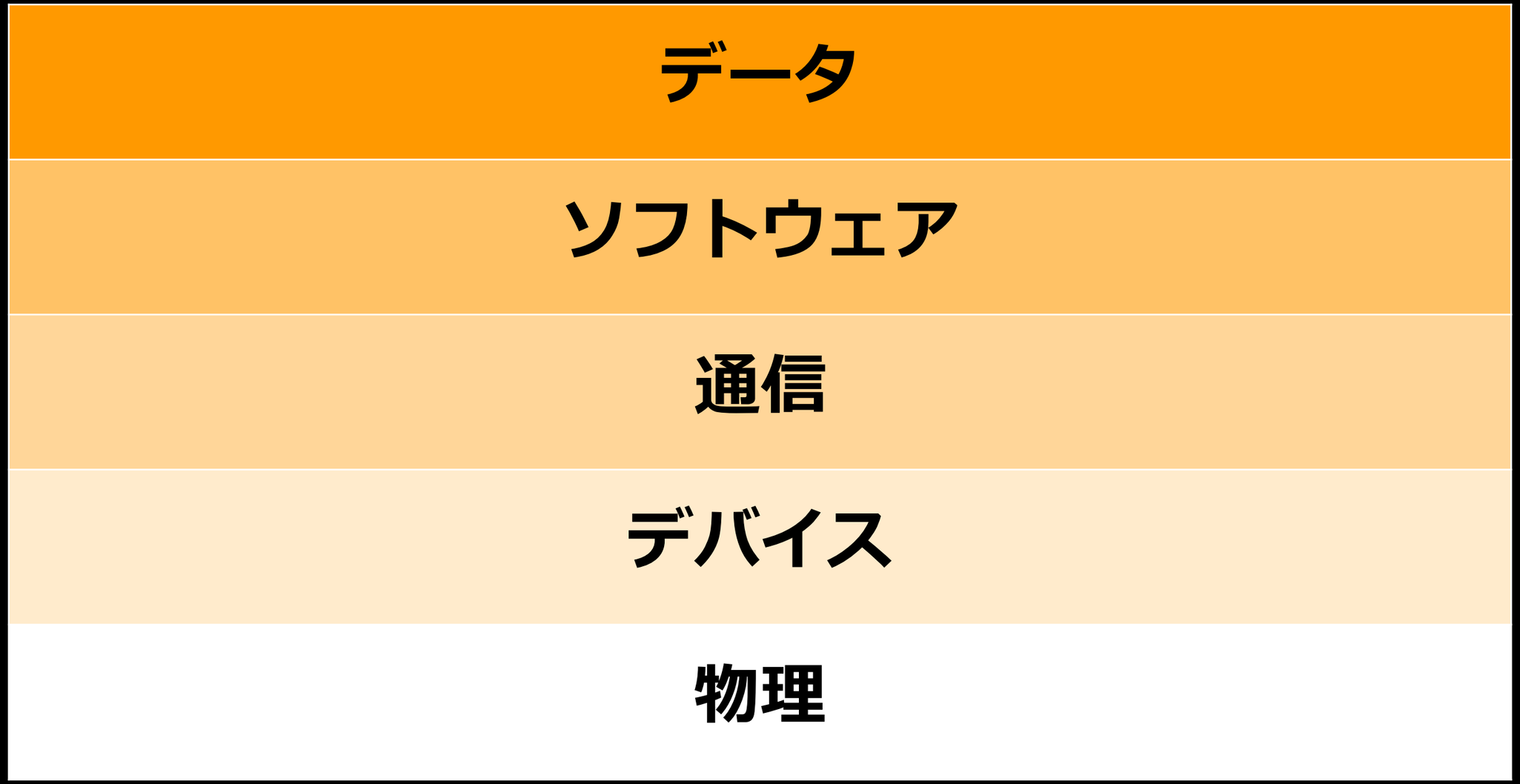
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTシステムの全体イメージ



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTで考慮すべきセキュリティのレイヤ



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTにおけるセキュリティ考慮事項

データ
データの保護

ソフトウェア
デバイスソフトウェア更新

通信
データの保護

デバイス
デバイスの安全な認証・認可
デバイスの監視・監査

物理
ハードウェアの保護

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTにおけるセキュリティ考慮事項

データ
データの保護

ソフトウェア
デバイスソフトウェア更新

どれか一つに留意すれば良いというわけではなく、
これら**全てのレイヤ**について考慮し検討する必要がある

デバイス
デバイスの安全な認証・認可
デバイスの監視・監査

物理
ハードウェアの保護

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTにおけるセキュリティ考慮事項

認証・認可

データの保護

監視・監査

ソフトウェア更新

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTにおけるセキュリティ考慮事項

認証・認可

データの保護

監視・監査

ソフトウェア更新

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

認証における要件

特徴/制約

- 必ずしも**ユーザ**が介在するとは限らない
- デバイスに対し、**物理攻撃**や**ネットワーク攻撃**のリスクが生じる

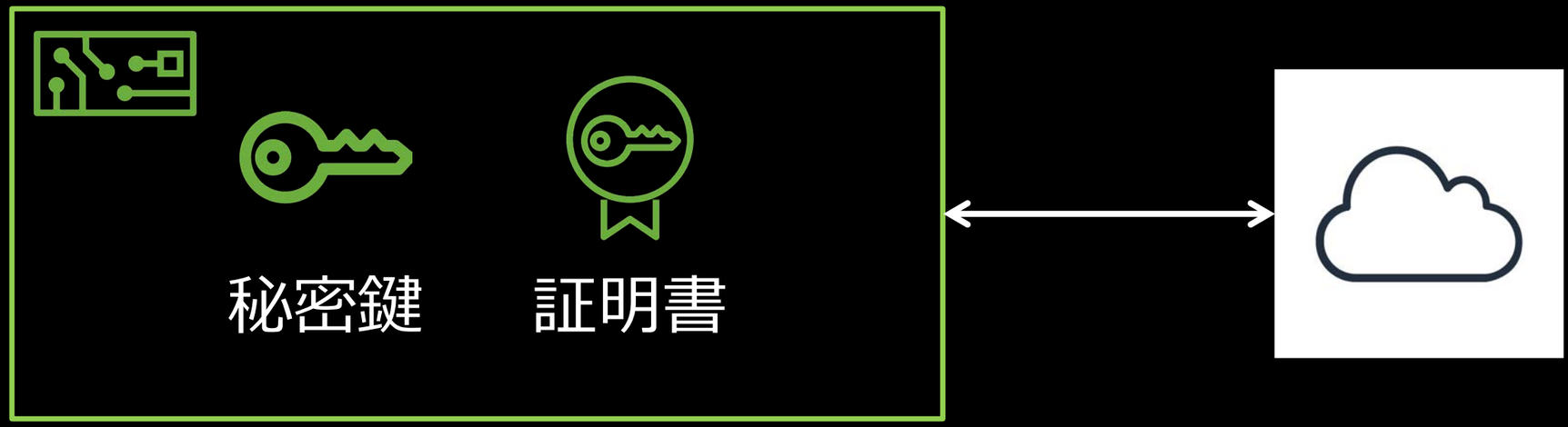
要件

サーバとデバイス単体で安全に認証したい

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

サーバとデバイス単体で安全に認証したい

個別のデバイス証明書を用いて認証する



考慮ポイント

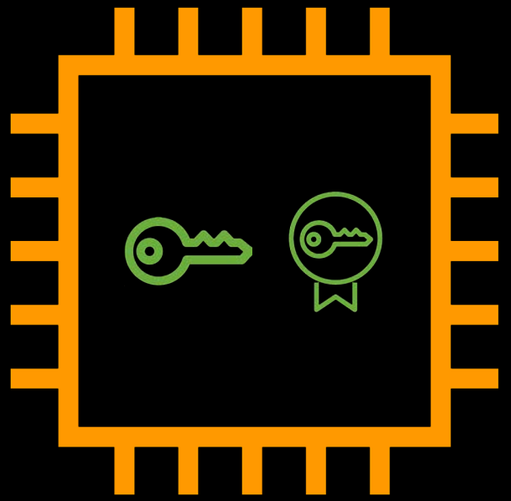
1. **認証情報を不正に取得されないよう保存する**
2. **認証情報が漏れた場合のリスクを最小化する**

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

認証情報を不正に取得されないよう保存する

認証情報をセキュア領域に保存する

認証情報の保存および認証操作に、

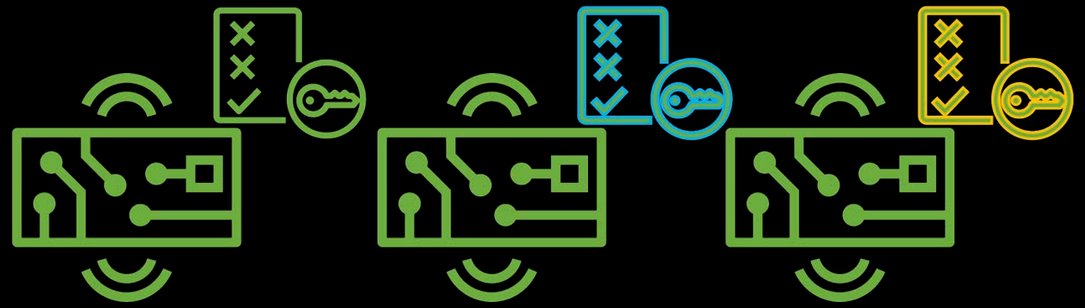


- **T**rusted **P**latform **M**odule
- **H**ardware **S**ecurity **M**odule

などのハードウェア保護モジュールを使用する

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

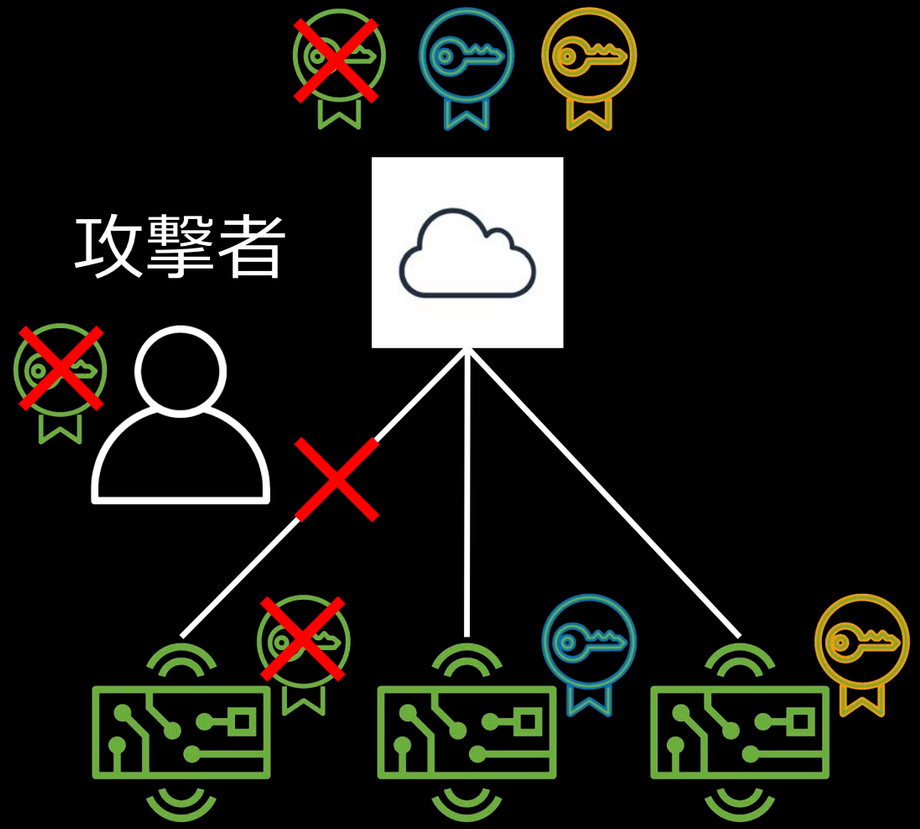
認証情報が漏れた場合のリスクを最小化する



1. デバイス証明書を**個別に無効化**できるようにする
2. デバイス毎に**最小権限**のみを与える

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

デバイス証明書を個別に無効化できるようにする



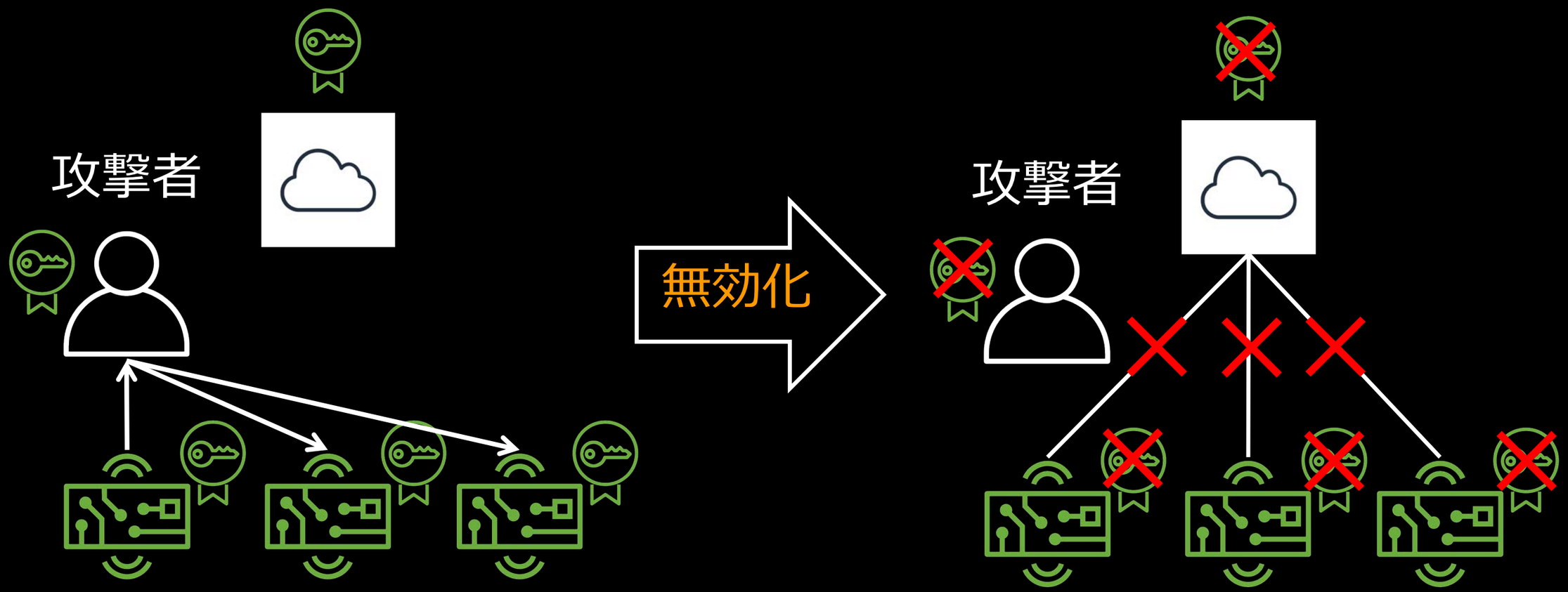
対象デバイスの認証情報を**無効化**

影響

対象デバイスのみがクラウドへ接続不能に

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

仮に共通の秘密鍵を使用して漏洩が起きると・・？

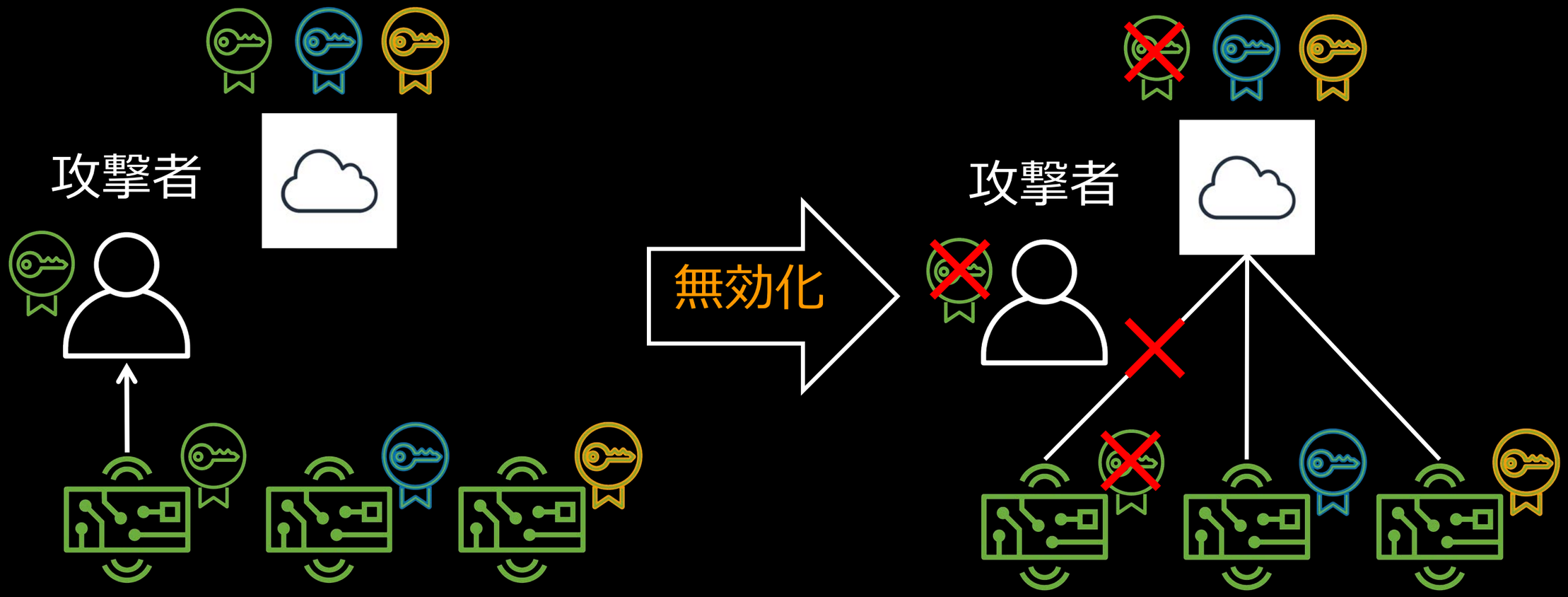


全デバイスが不正利用されるリスクがある

無効化時の影響範囲も**全デバイス**に及ぶ

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

個別の秘密鍵を使用することによるリスクの最小化

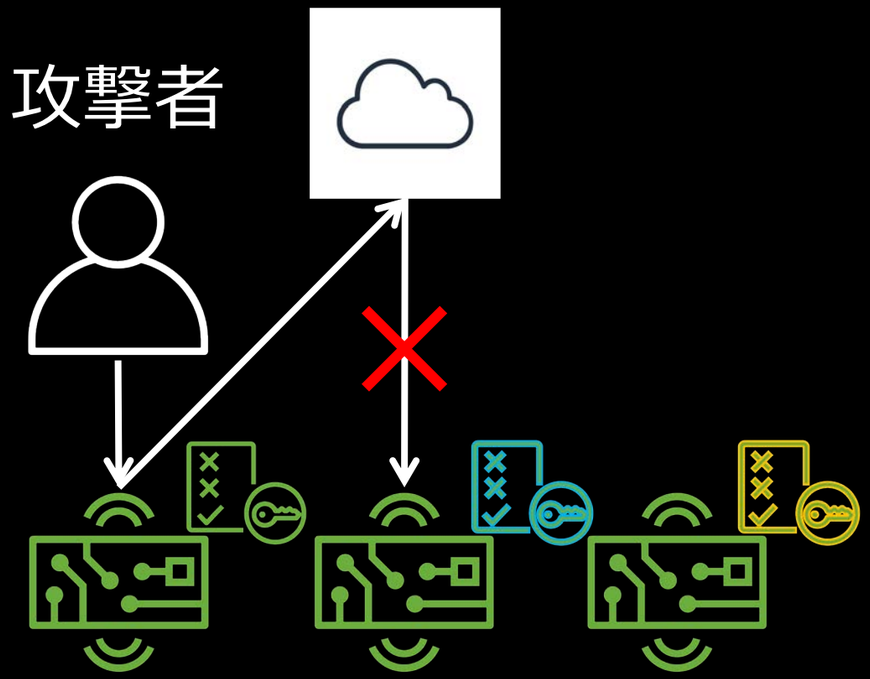


対象デバイスのみが不正利用されるリスクがある

無効化時**対象デバイスのみ**がクラウドへ接続不能に

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

デバイス毎に最小権限のみを与える

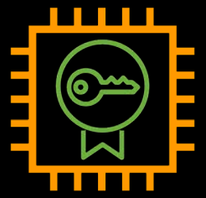


認証情報が漏洩しても、クラウドや他デバイスに対しての操作が**制限**され、リスクを**最小化**できる

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

認証・認可におけるベストプラクティス

デバイスに**個別の認証情報**を割り当てる



認証情報を**セキュア領域**に保存する

認証情報の**生成**、**配布**、**無効化**を行う仕組みを導入する

デバイス毎に**最小権限**のみ与える

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

デバイスに個別の認証情報を割り当てる

AWS IoT Coreはデバイス証明書による相互認証をサポート

- デバイス証明書を**無制限**に発行・登録が可能
- デバイス毎に個別の証明書を発行・登録可能

AWS IoT Coreにおけるデバイス証明書
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/x509-client-certs.html

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

認証情報の生成、配布、無効化を行う仕組みを導入する

AWS IoT Coreはデバイス証明書の管理をサポート

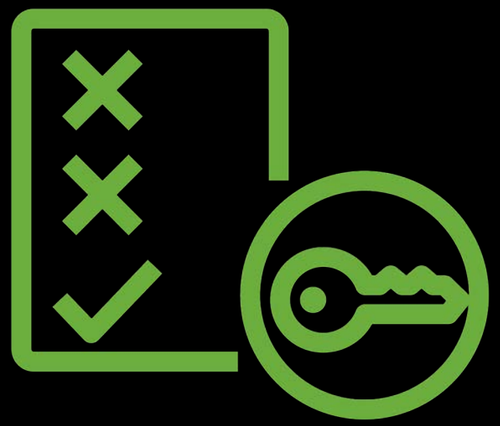
- クラウドから証明書を**無効化可能**

AWS IoT Coreでのデバイス証明書の発行および登録方法
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/device-certs-create.html

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

デバイス毎に最小権限のみ与える

AWS IoTポリシーで権限制御が可能



- AWS IAMポリシーと同様の記述方式
- AWS IoT Coreに対する**アクションやリソースの制御**が可能
- 例）接続、受信、送信
- デバイス証明書にアタッチして使用

AWS IoTポリシー
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/client-authentication.html

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTにおけるセキュリティ考慮事項

認証・認可

データの保護

監視・監査

ソフトウェア更新

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

データ保護における要件

特徴/制約

- クラウドとの通信や同一ローカルネットワーク内のゲートウェイを介した通信もある
- デバイスに対し、**物理攻撃**や**ネットワーク攻撃**のリスクが生じる

要件

通信を暗号化したい

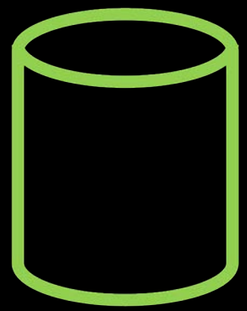
データを安全にデバイス上に保存したい

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

データ保護におけるベストプラクティス

転送時の暗号化

暗号化されたネットワークプロトコルをクラウドとの通信やローカルネットワークでの通信に用いる



保存時の暗号化

デバイス内の鍵を用いてIoTデバイスやゲートウェイ内に一時的に保存されるデータを**非対称暗号化**する

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

通信を暗号化したい

AWS IoT Coreはデフォルトで通信の暗号化をサポート

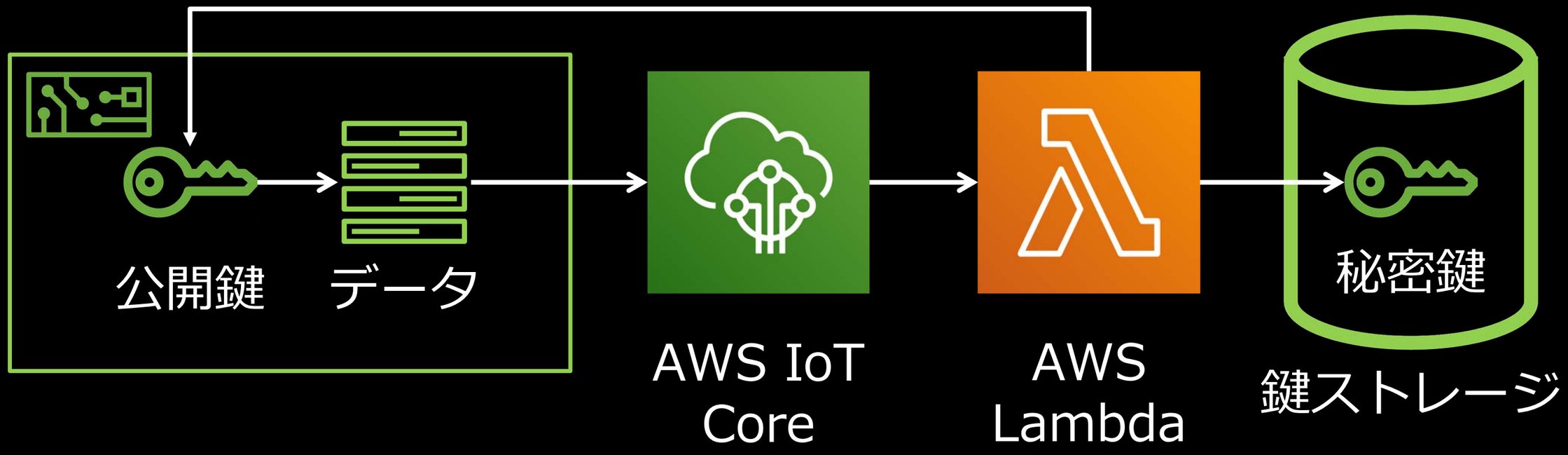
- **MQTTS**と**HTTPS**に対応
- フルマネージドサービス
- サーバーの運用・管理不要
- スケーリングの考慮も不要

AWS IoTメッセージブローカー
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/iot-message-broker.html

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

データを安全にデバイス上に保存したい

クラウド上で非対称暗号鍵を発行し、デバイスに埋め込んだ公開鍵でデータを暗号化し保存する



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTにおけるセキュリティ考慮事項

認証・認可

データの保護

監視・監査

ソフトウェア更新

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

監視・監査における要件

特徴/制約

- 一定の動作を繰り返すことが多い
- デバイスに対し、**物理攻撃**や**ネットワーク攻撃**のリスクが生じる

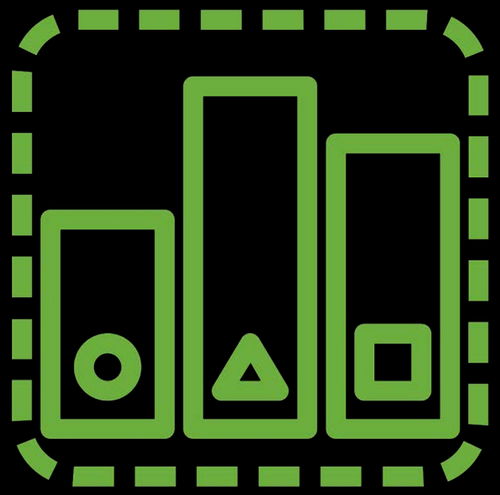
異常動作の検出ができる

要件

不適切なデバイス設定や異常動作を自動的に検出したい

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

監視・監査におけるベストプラクティス



セキュリティリスクを事前に**評価**する

IoT環境全体からメトリクスとログを継続的に収集およびレポートする監視・監査の**仕組み**を用意する

監視と監査を**自動化**する

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

不適切なデバイス設定や異常動作を自動的に検出したい

AWS IoT Device Defenderを用いてデバイスを監査・監視する

デバイス設定の監査、異常動作の検出
を行うセキュリティサービス

- クラウドメトリクスをすぐに監視・監査可能
- エージェントをデバイスにインストールすることで、デバイスメトリクスを監視・監査可能

AWS IoT Device Defender
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/device-defender.html

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IoTにおけるセキュリティ考慮事項

認証・認可

データの保護

監視・監査

ソフトウェア更新

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ソフトウェア更新における要件

特徴/制約

- ネットワークに繋ぐデバイスでは更新が必須
- 遠隔地に配置されているため直接更新できない

Over-The-Airによって更新しなければならない

要件

OTA更新を管理したい

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ソフトウェア更新におけるベストプラクティス

暗号化プロトコルを用いて更新パッケージを転送する

デジタル署名を用いて更新パッケージを**検証**する

配布システムで**認証**と**アクセス制御**を行う

バージョンやパッチの状態を**管理**する

更新状態を監視し、失敗・停止した更新を**調査**する

更新できない場合は、関係者に**通知**する

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

OTA更新を管理したい

AWS IoTのジョブ機能を用いてOTA更新を配布する

AWS IoT
Device Management

AWS IoTに接続されたデバイスに任意のジョブを配布可能

任意のOTA更新が可能

AWS IoTジョブ
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/iot-jobs.html

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

まとめ

IoT環境では、**物理**や**デバイス**のレイヤまで含めてセキュリティを考慮する必要がある

IoTデバイス**特有の特徴や制約**から、IoT特有のセキュリティ要件が生まれる

AWS IoTを用いることで、IoT特有の**セキュリティ要件を解決**できる

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

参考資料

[Presentation] IoTにおけるセキュリティ

[Training] AWS IoT Security Primer

[Blog] IoTソリューションにおける10のゴールデンルール

[Presentation] IoT Well Architected

[Presentation] 【初級】AWS で始める IoT 入門

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

クイズ

Q1
AWS IoT Coreに接続するため、デバイス証明書を使用して認証することにしました。各デバイスへ**個別の証明書をプロビジョニング**するためにはどのような手段があるでしょうか？

Q2
AWS IoT Coreに送信されたデータをクラウド上に**暗号化**して**S3**に保存したいです。どのようなアーキテクチャで実現できるでしょうか？

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Shota Iizuka

aws INNOVATE
ONLINE CONFERENCE

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.