AWS IoT Device Defender

AWS Black Belt Online Seminar

戸塚 智哉
Solutions Architect
2022/05

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が主催するオンラインセミナーシリーズです
- AWS の技術担当者が、AWS の各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

- 本資料では2022年04月時点のサービス内容および価格についてご説明しています。
  最新の情報は AWS 公式ウェブサイト(http://aws.amazon.com)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。
  日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

自己紹介

戸塚　智哉

アマゾンウェブサービスジャパン合同会社
ソリューションアーキテクト

経歴：　AI / IoT に関わる新規ソリューション開発に従事
　　基幹系システム開発に従事

好きな AWS サービス：

AWS IoT Core

AWS IoT Device Defender

本セミナーの対象者

- AWS IoT サービスをこれからご利用予定の方
- AWS IoT Core をすでにご利用の方で、よりデバイスのセキュリティに関する理解を深めたい技術者の方

アジェンダ

- IoT におけるセキュリティ
- AWS IoT Device Defender とは
- AWS IoT Device Defender の機能詳細
- AWS IoT Device Defender の料金
- まとめ

アジェンダ

- IoT におけるセキュリティ
- AWS IoT Device Defender とは
- AWS IoT Device Defender の機能詳細
- AWS IoT Device Defender の料金
- まとめ

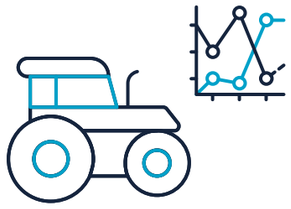
AWS IoTを利用してお客様が実現していること

生産性と
プロセスの最適化

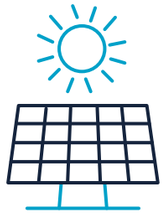
リモートで患者の健康と
状態をモニター

在庫の可視化と
倉庫業務の最適化

家庭、建物、都市のスマート化
及びより良い体験の構築



効率的に良品の
作物を育てる



エネルギー資源を
効率的に管理

コネクテッドカー、
自動運転で輸送の変革

家庭、オフィス、工場
の安全性向上

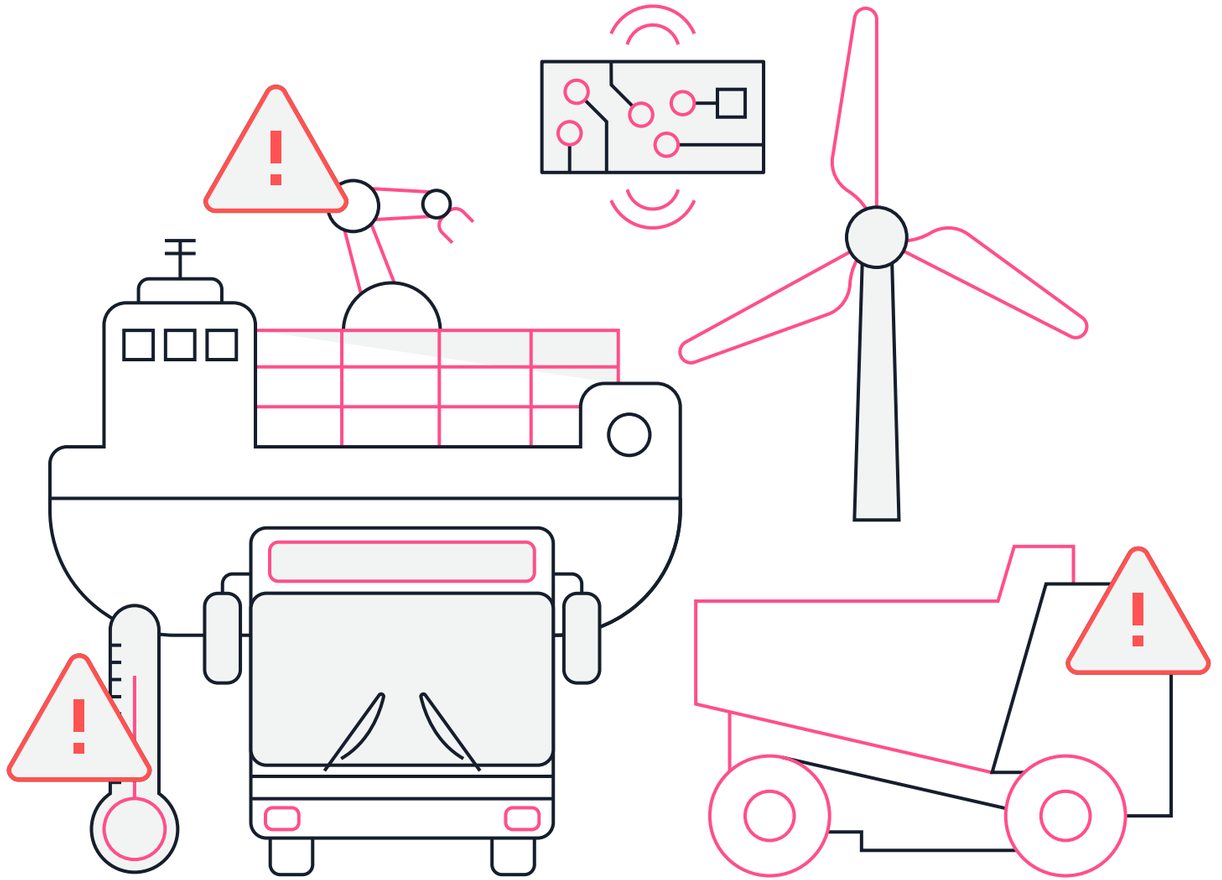
IoT におけるセキュリティの課題

- 今日デバイスが安全な状態であっても、明日も安全な状態とは限らない

- どうすれば IoT デバイスの安全を維持できるのか

- 安全でなくなった状態を**検出**し、運用者に**通知**を行い、
- 進化を続ける脅威に対応すべく IoT デバイスも**進化**する

接続されたデバイスを
セキュアに保つ方法は？



IoT セキュリティの脅威 – クラウド側

知的財産の窃盗

違法コピー、デバイスや証明書の盗難

データの不正な取り出し

認証されていないデータ転送、データ盗難

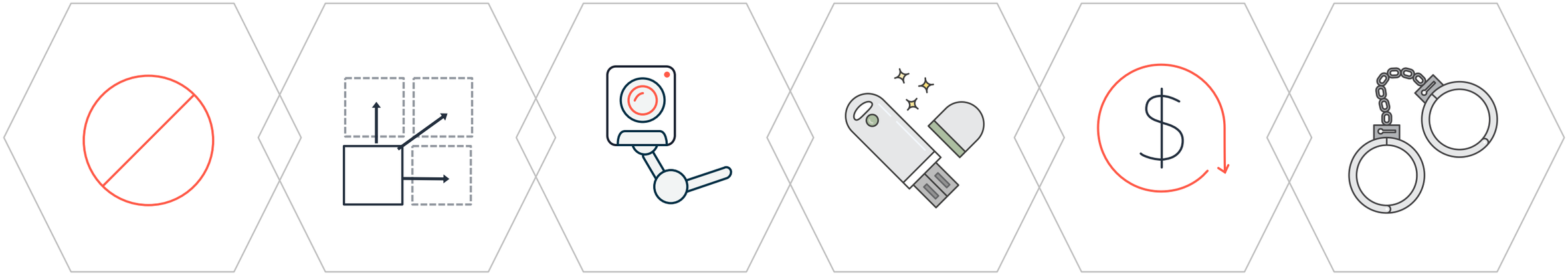
なりすまし

信頼されたデバイスの認証情報を利用したなりすまし

クラウドインフラの不正利用

AWS IoT に対する不正利用による大量のメッセージの送受信

IoT セキュリティの脅威 – デバイス側



DoS 攻撃

外部ホストに対するDoS攻撃にデバイスが利用される

踏み台攻撃

ネットワークへ侵入し権限を拡大しながら脅威が拡大

監視

悪意あるコードによってユーザの行動を監視し認証情報を取得

サボタージュ攻撃

マルウェアに感染したデバイスが被害を受け停止

暗号通貨のマイニング

感染したデバイスが暗号通貨のマイニングに利用される

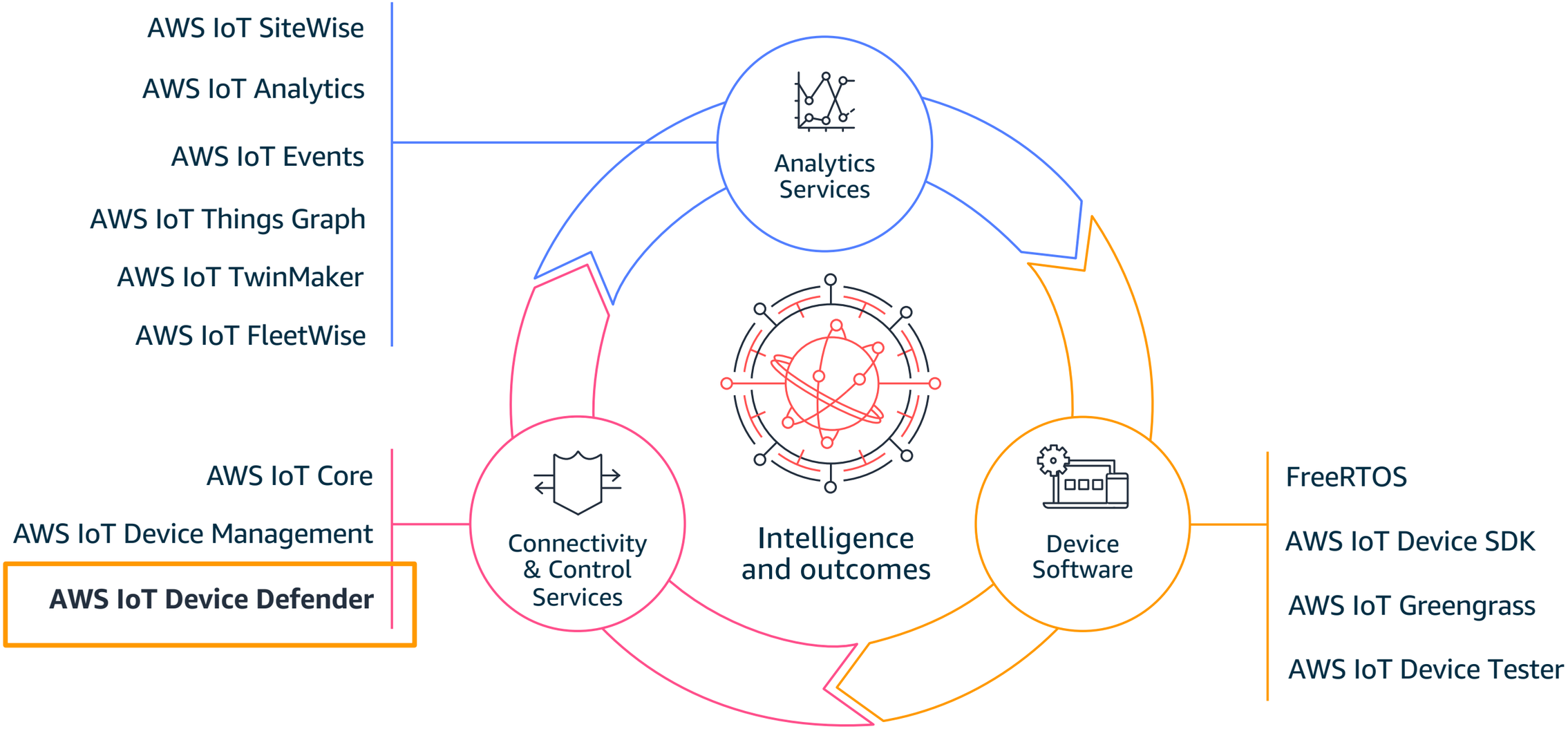
ランサムウェア

ランサムウェアによる暗号化によってデバイスへのアクセスが失われる

アジェンダ

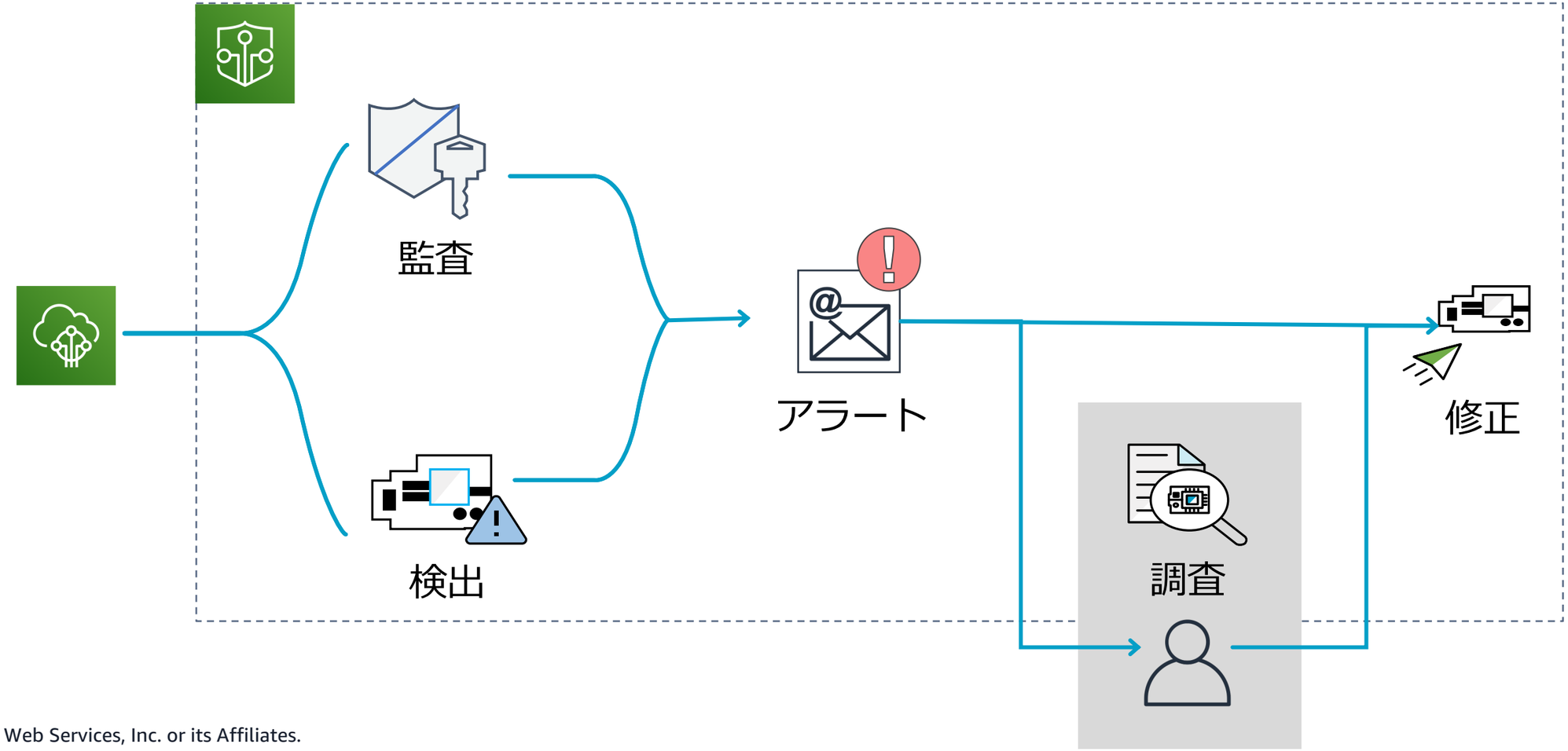
- IoT におけるセキュリティ
- **AWS IoT Device Defender とは**
- AWS IoT Device Defender の機能詳細
- AWS IoT Device Defender の料金
- まとめ

IoT の好循環なサイクル



AWS IoT Device Defender

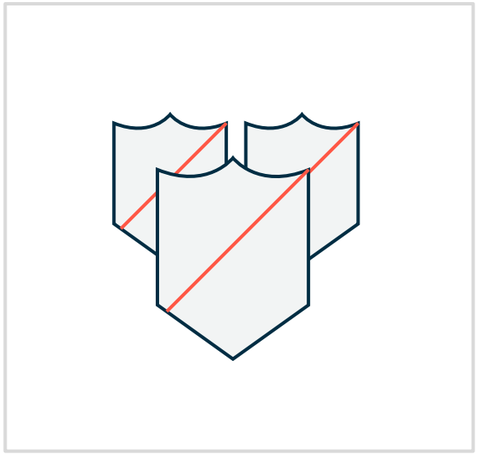
AWS IoT Device Defender は、フル・マネージドの IoT セキュリティ
サービスであり、接続されたデバイス群を継続的に保護することができます



アジェンダ

- IoT におけるセキュリティ
- AWS IoT Device Defender とは
- **AWS IoT Device Defender の機能詳細**
- AWS IoT Device Defender の料金
- まとめ

AWS IoT のビルトインセキュリティ



相互認証

AWS IoT Core はデバイス向けに X.509 のクライアント証明書、モバイルアプリ向けに Amazon Cognito、デスクトップアプリ向けに AWS Identity and AccessManagement (IAM) を利用した相互認証を必須としている

詳細な認可

AWS IoT はそのまま利用できる IAM のマネージドポリシーやカスタムポリシーを提供。アクセス権限やデータ操作権限の設定に利用可能。

暗号化

各デバイスはAWS IoT Core への接続時にサーバ証明書を取得。有効期限などの情報が含まれたX.509 形式のTLS 証明書を利用。

監査

IoT の設定がセキュアであることを数クリックで検証

一連の組み込みの IoT セキュリティベストプラクティスに対して準拠しているか IoT リソースを監査

様々な IoT リソースに対して標準的な監査を実施

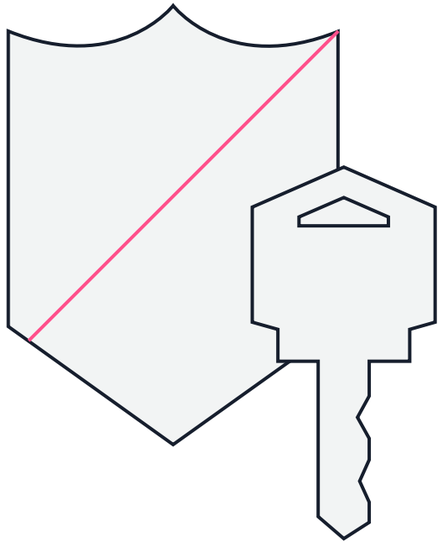
証明書 (例: 失効や無効化)

ポリシー (例: 過度な権限)

MQTT クライアント ID (例: 競合)

アカウント設定 (例: ログ)

定期的な監査(日次、週次)もしくは、修正を検証するためのアドホックな監査



Scheduled

Ad-hoc

AWS IoT Device Defender 監査 チェック項目

○ 認証

- デバイス証明書の共有
- デバイス証明書のキー品質
- デバイス証明書の有効期限

- CA 証明書のキー品質
- CA 証明書は取り消されたが、デバイス証明書が有効
- CA 証明書の有効期限切れ

- 失効したデバイス証明書がアクティブ
- MQTT のクライアント ID の競合

認可

- 認証されていない Cognito ロールが過度に許容
- 認証された Cognito ロールが過度に許容

- IoT ポリシーが過度に許容

- ロールエイリアスが過度に許容
- ロールエイリアスが未使用のサービスへのアクセスを許可

ロギング

- AWS IoT のログ記録が無効

監査内容

- **REVOKED_CA_CERT_CHECK**
  CA 証明書が取り消されたが、デバイス証明書が有効になっている
- **DEVICE_CERTIFICATE_SHARED_CHECK**
  複数の同時接続が同じ X.509 証明書を使用して AWS IoT サービスに対して認証されている
- **DEVICE_CERTIFICATE_KEY_QUALITY_CHECK**
  登録されている証明書が求めているキーの品質を確認
- **CA_CERTIFICATE_KEY_QUALITY_CHECK**
  登録されている CA の証明書が求めているキーの品質を確認
- **UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK**
  Cognito 未認証ユーザーの権限が推奨されている以上の権限が付与されているかを確認
- **AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK**
  Cognito 認証ユーザーの権限が推奨されている以上の権限が付与されているかを確認
- **IOT_POLICY_OVERLY_PERMISSIVE_CHECK**
  IoT Policy にワイルドカードのような広域な権限が付与されているかを確認

* 詳細なチェック内容はこちらを参照ください
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/device-defender-audit-checks.html

監査内容

- **IOT_ROLE_ALIAS_OVERLY_PERMISSIVE_CHECK**
  Role Alias で許可されいてるサービスで "*” が指定されているものを確認
- **IOT_ROLE_ALIAS_ALLOWS_ACCESS_TO_UNUSED_SERVICES_CHECK**
  Role Alias で使われていないサービス権限が着いているかをチェック
- **CA_CERT_APPROACHING_EXPIRATION_CHECK**
  CA 証明書が 30 日以内に有効期限が切れるか、既に切れているかをチェック
- **CONFLICTING_CLIENT_IDS_CHECK**
  複数のデバイスが同じクライアント ID を使用して接続しているかをチェック
- **DEVICE_CERT_APPROACHING_EXPIRATION_CHECK**
  デバイス証明書が 30 日以内に有効期限が切れるか、既に切れているかをチェック
- **REVOKED_DEVICE_CERT_CHECK**
  取り消されたデバイス証明書がアクティブになっているかをチェック
- **LOGGING_DISABLED_CHECK**
  AWS IoT のログ設定が有効になっているかをチェック

* 詳細なチェック内容はこちらを参照ください
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/device-defender-audit-checks.html

監査結果

監査の結果はレポートとして出力される

監査の実行

- 実行頻度を指定できます
    - 今すぐ監査を実行(1回)
    - 毎日
    - 毎週(曜日を指定)
    - 隔週(曜日を指定)
    - 毎月(1日、月末、特定の日)

監査結果の抑制

- 指定されたリソースで監査結果を抑制すると、指定された監査チェックのリソースに関連する結果は、非準拠としてフラグ付け
- 適合カテゴリと不適合カテゴリとは別に、抑制された所見として分類される

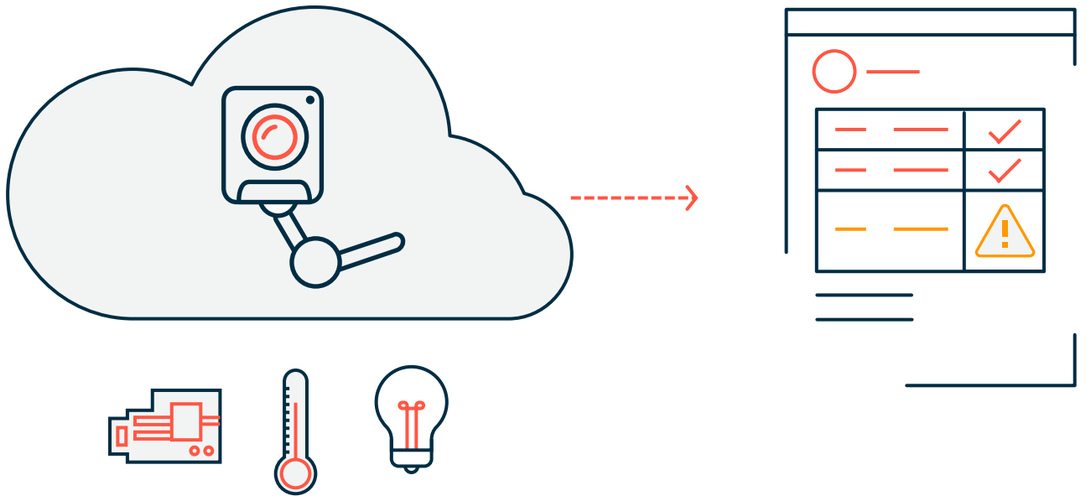
  - 設定項目
    - 監査チェック
    - リソース
    - 抑制期間
    - 説明(オプション)

異常の検出

デバイス動作の異常を検出

アカウント内のすべてのデバイスまたは類似した動作特性を持つデバイスのグループに対してセキュリティプロファイルを作成

接続済デバイスと AWS IoT Core のセキュリティプロファイルからセキュリティメトリクスおよびデータに対するルールベースの動作を定義



セキュリティプロファイルとは

- メトリクスと正常(または異常)と判断する条件を定義する
- 複数の条件が指定可能
- 以下の Thing グループに対して設定することで、対象となる Thing に対してチェックされる
  - すべての Thing
  - IoT レジストリに登録されていない Thing
  - 登録されている Thing
  - 任意のグループ
- アラートの通知先(SNS)を指定

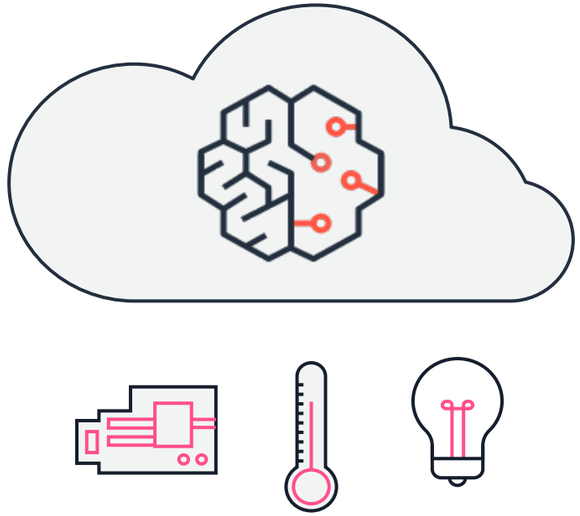
異常検出は2種類あり、組み合わせが可能

組み合わせることでよりセキュリティを強固にできる

ルール検出

予期されるデバイス動作の定義

ML 検出



デバイス履歴データに基づいてモデルを自動的に作成

アラート

いつ・何がおきたかを知る

発見された異常や監査結果に基づいてアラートを生成

AWS IoT コンソール, AWS IoT Device Defender API, Amazon CloudWatch, Amazon SNS にアラートを送信

非準拠の監査やデバイスの異常に対して、デバイスやリソースレベルで履歴やコンテキスト情報を確認

AWS IoT Device Defender のメトリクス

標準メトリクス

クラウド側

- 認証エラー
- 接続試行
- 切断

- メッセージサイズ
- 受信したメッセージ
- 送信したメッセージ

- 送信元 IP

デバイス側

- 受信バイト数
- 送信バイト数
- 入力パケット
- 出力パケット

- TCP 接続確立数
- リッスン TCP ポート
- TCP ポートのリッスン回数
- リッスン UDP ポート
- UDP ポートのリッスン回数

- 送信先 IP

カスタムメトリクス

- デバイス特有のメトリクスを定義して監視 (例: バッテリー残量、パワーサイクル、プロセス数)

- 事前定義したルールや統計ベースから外れた以上の発生時にアラームを受信

- カスタムメトリクスをデバイスからクラウドへ送信するリファレンス実装を利用可能

デバイス側でメトリクスを取得するには

- AWS IoT Device Defender Agent SDK サンプル
  - Python 版　https://github.com/aws-samples/aws-iot-device-defender-agent-sdk-python
  - C 版　https://github.com/aws-samples/aws-iot-device-defender-agent-c
- FreeRTOS ライブラリ
  - https://docs.aws.amazon.com/ja_jp/freertos/latest/userguide/afr-device-defender-library.html
  - 注）一部のメトリクスのみ対応
- AWS IoT Device Client
  - https://github.com/awslabs/aws-iot-device-client/blob/main/source/devicedefender/README.md

検出のメトリクス組み合わせ例

Denial of Service	他へ接続	情報漏えい	覗き見	外部からの攻撃	コインの採掘	ランサムウエア	外部攻撃	クラウドへの攻撃
PacketsOut BytesOut DestIP Port	PacketsOut BytesOut DestIP Auth Fail	PacketsOut BytesOut DestIP	PacketsIn BytesOut DestIP	PacketsIn BytesIn DestIP	Dest IP Port	DestIP Port	DestIP Port	Msg rate Msg size Source IP

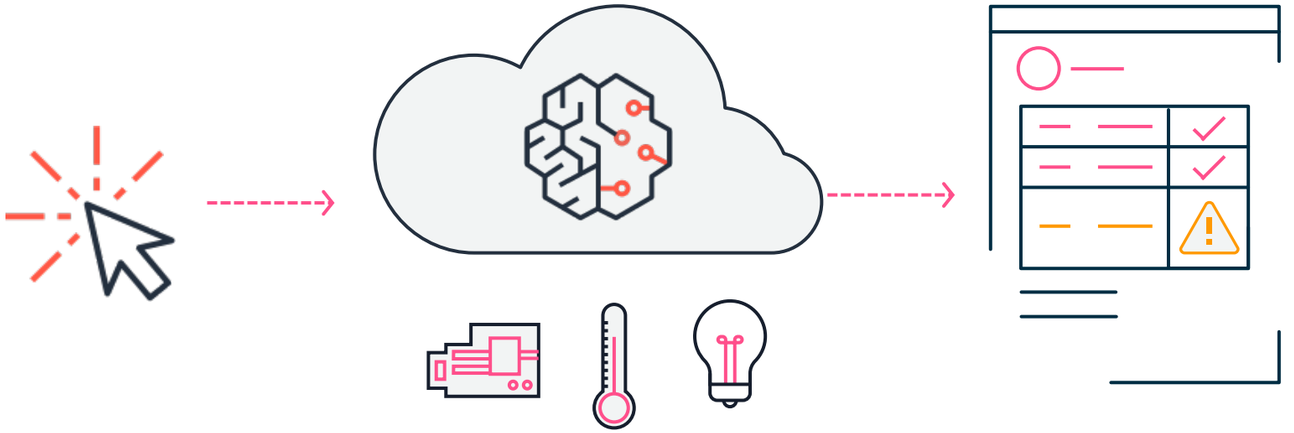
ML 検出

機械学習によってデバイスの挙動の異常を検出

セキュリティプロファイルを作成して
デバイスに関する事前の知識不要で運用
とセキュリティのメトリクスを監視

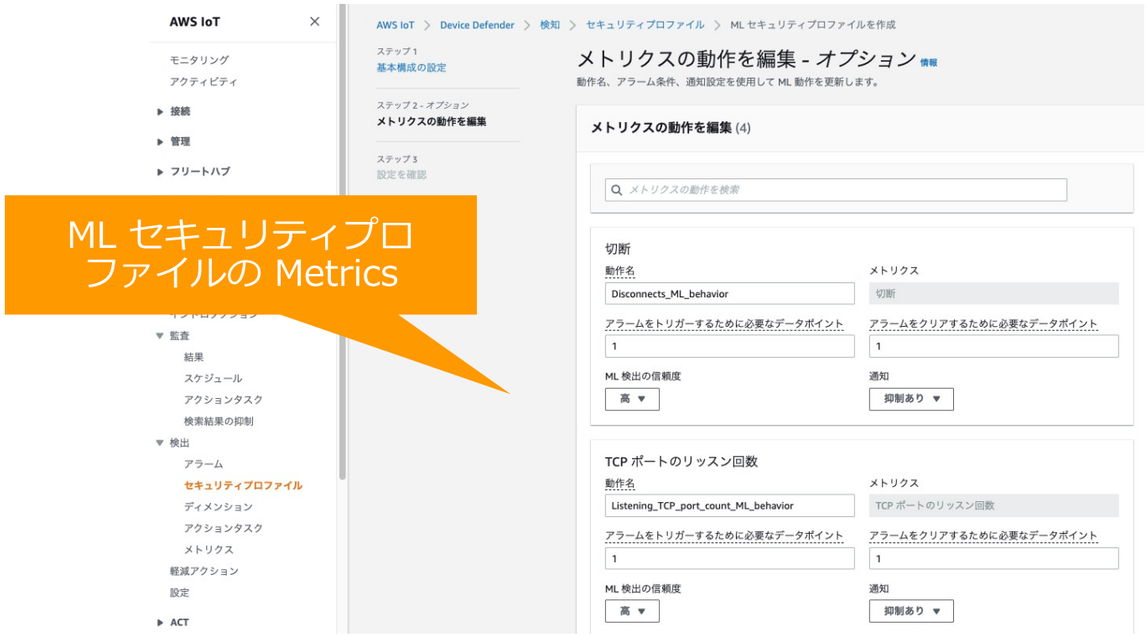
デバイス全体に対して運用上やセキュリ
ティの異常を各デバイスレベルで自動的
に検出

新しいデータのトレンドから想定される
デバイスの挙動を継続的にアップデート



機械学習による脅威の検出機能

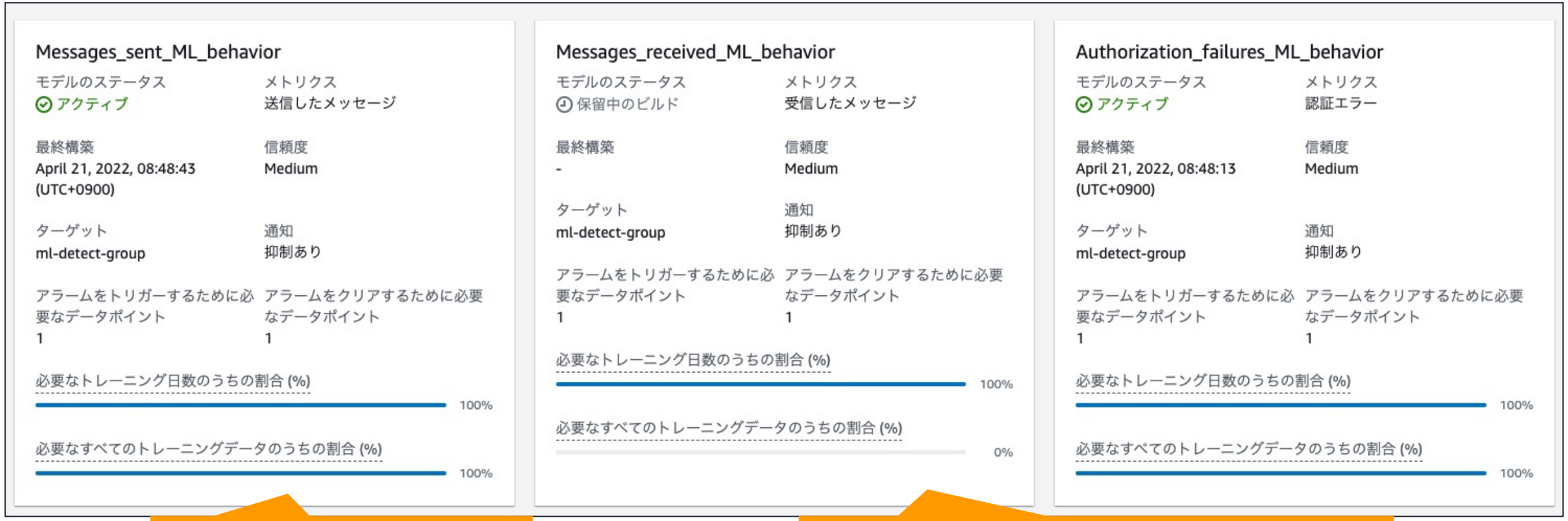
- AWS IoT Device Defender のセキュリティプロファイル（脅威検出設定）に機械学習タイプが登場（ 2021 年 3 月）
- デバイスの挙動を機械学習し異常を判定
  - 例）デバイスからのメッセージ通知頻度を学習し
  - 正常状態と異なるパターンを検出



ML セキュリティプロファイルの Metrics

ML モデルのトレーニングレポート
トレーニングの進み具合を表示

モデルのトレーニング状態の確認



日数・データポイント数ともに十分

データポイント数が不足しているためモデルが作成されていない

違反状態の確認

過去の違反イベントの履歴

ML 検出注意点

- 学習に最低でも 14 日分、25,000 ポイントのデータが必要
- 初期モデルが作成されると、ML モデルは毎日更新
- セキュリティプロファイルのターゲットのモノのグループにモノが含まれている必要あり

台数とデータポイント間隔の組み合わせ例

- 60 台のデバイスが AWS IoT 上で 45 分間隔で接続しアクティビティを実行
- 40 台のデバイスによる 30 分間隔での接続と実行
- 15 台のデバイスによる 10 分間隔での接続と実行
- 7 台のデバイスによる 5 分間隔での接続と実行

サポートされるメトリクス

クラウド側

- 認可の失敗
- 接続試行
- 切断
- メッセージサイズ
- 送信されたメッセージ
- 受信したメッセージ

デバイス側

- 出力バイト数
- 入力バイト数
- リスニング TCP ポート数
- リスニング UDP ポート数
- 出力パケット
- 入力パケット
- 確率された TCP 接続数

https://docs.aws.amazon.com/iot/latest/developerguide/dd-detect-ml.html

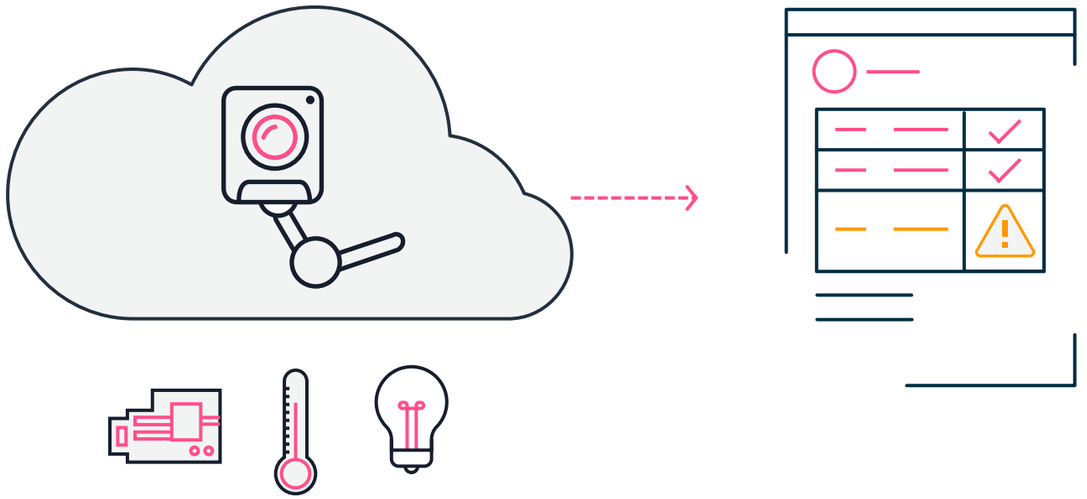
ルール検出

手動で設定した閾値に基づいて デバイスの挙動の異常を検出

類似した挙動をするアカウント内の全デバイスやデバイス群に対してセキュリティプロファイルを作成

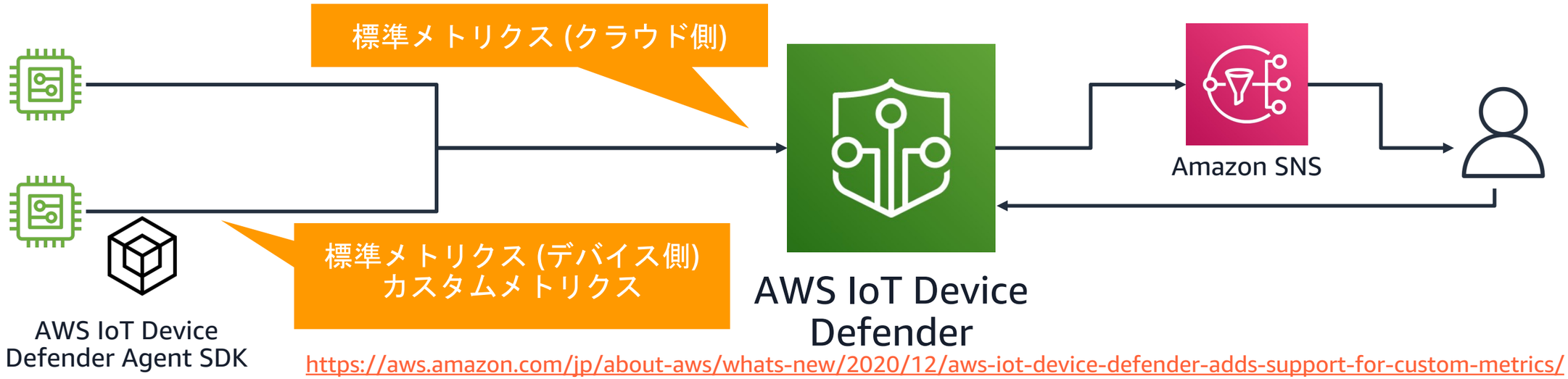
接続されたデバイスや AWS IoT Core の運用上もしくはセキュリティのメトリクスに対して、ルールもしくは統計ベースの挙動を定義

定義された挙動に基づいて運用上やセキュリティの異常を各デバイスレベルで検出



AWS IoT Device Defender カスタムメトリクス

- AWS IoT Device Defender で独自のメトリクスを定義して、監視やアラームに利用することが可能に
  - 例: CPU 負荷が一定の値域や統計的閾値を超えた場合に、管理者にアラームを送信
- GitHub でデバイス向けのエージェントのサンプルコードを提供



https://aws.amazon.com/jp/about-aws/whats-new/2020/12/aws-iot-device-defender-adds-support-for-custom-metrics/
https://github.com/aws-samples/aws-iot-device-defender-agent-sdk-python

セキュリティ問題を軽減

検出された問題へ対応

軽減アクションを実施して非準拠の監査項目の修正や検出アラームへ対応。事前構築されたアクションやカスタムアクションを利用可能

モノをグループに追加 (pre-built)

IoT ロギングの有効化 (pre-built)

結果をSNSに通知 (pre-built)

デフォルトのポリシーバージョンの置き換え (pre-built)

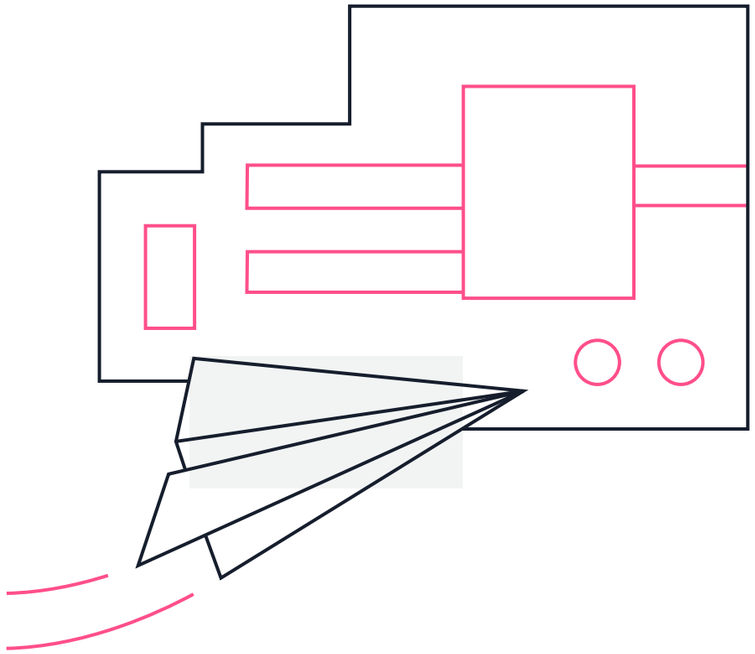
CA 証明書の更新 (pre-built)

デバイス証明書の更新 (pre-built)

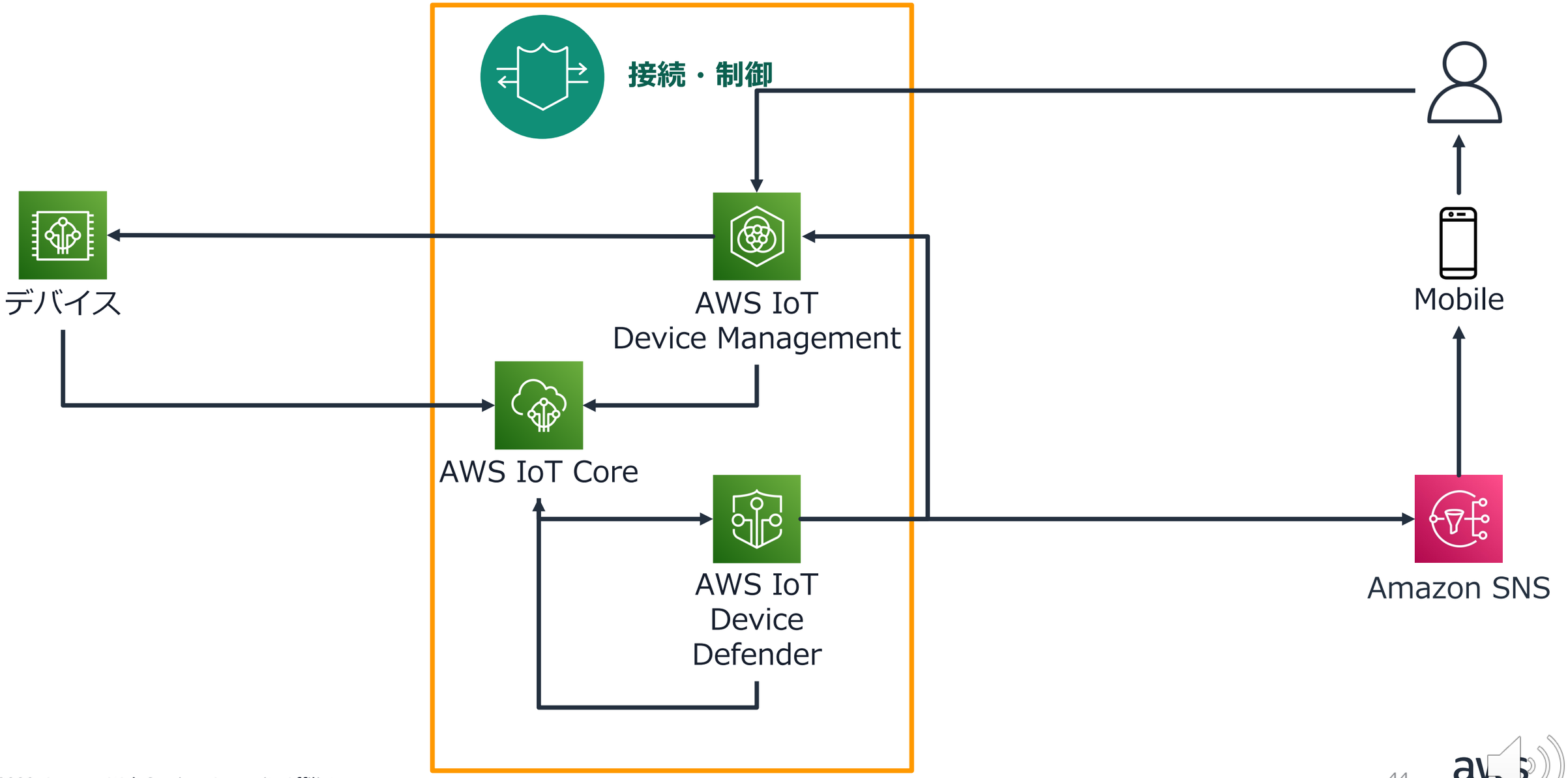
デバイスの再起動

セキュリティ更新の配信

AWS SNS でカスタムアクションを自動化

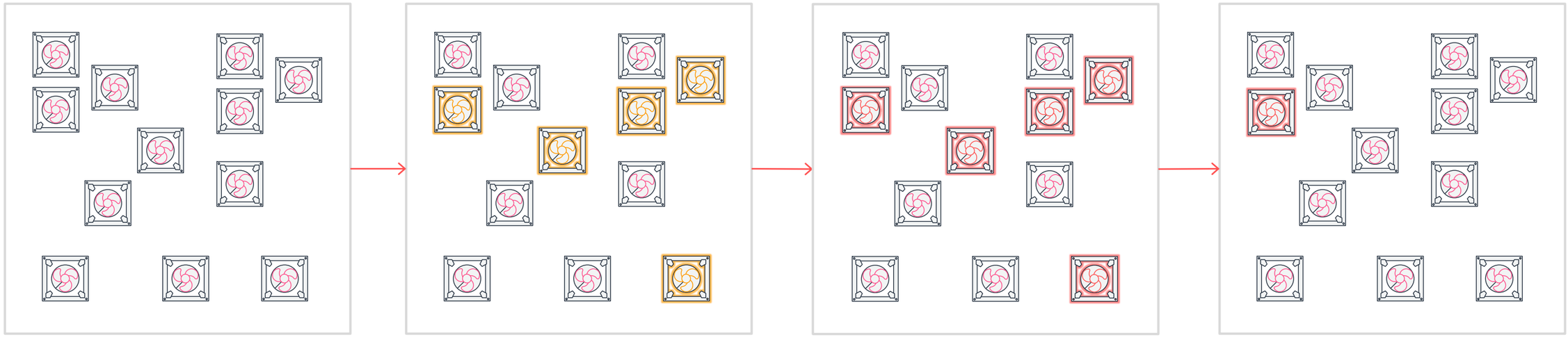


デバイスの監視・監査を実現する構成



AWS IoT Device Management

AWS IoT Device Management は、増加するデバイスの導入、整理、監視、リモート管理を支援します



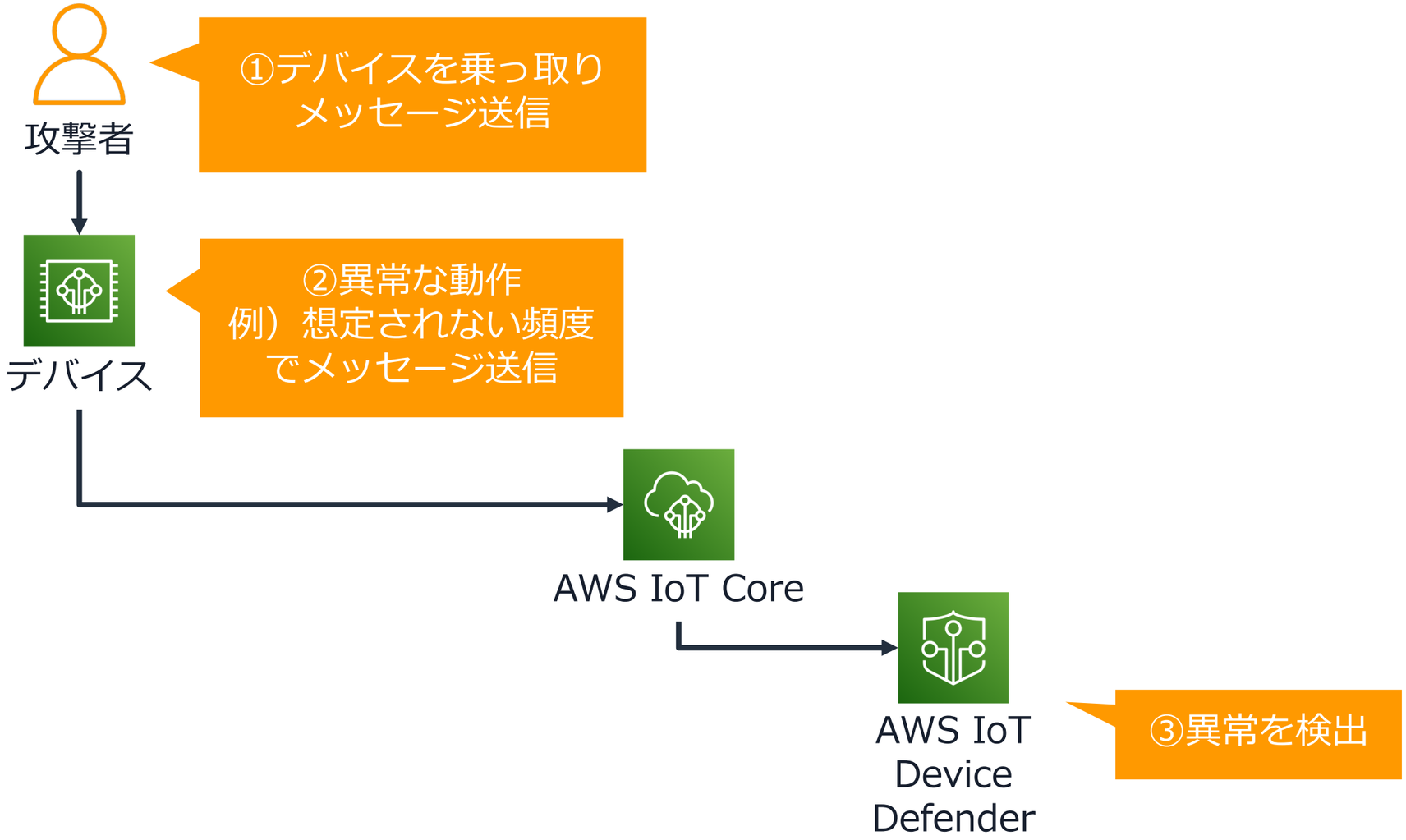
迅速でスケーラブルなデバイスの導入

リアルタイムなデバイスのインデックス化と検索

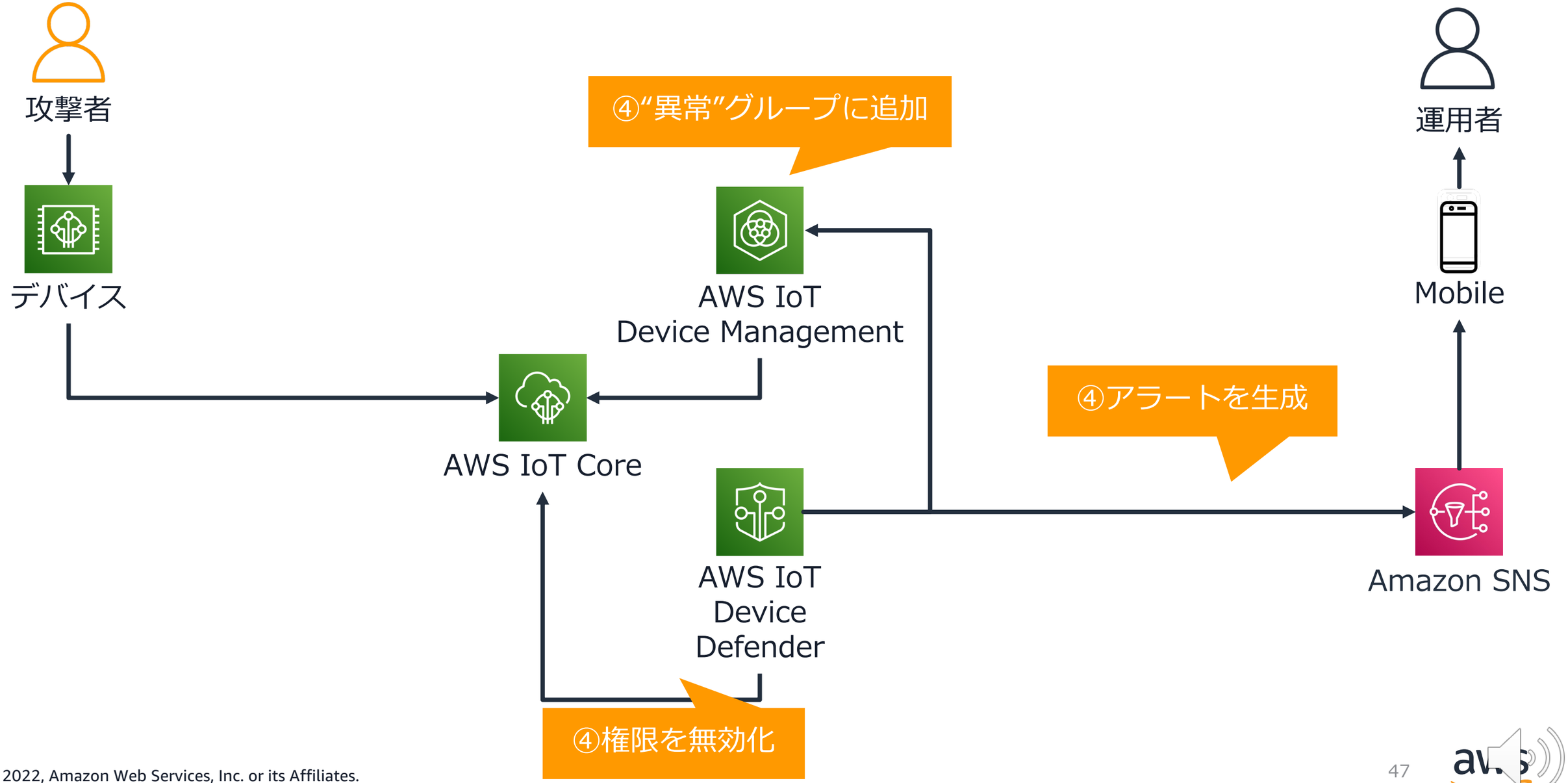
モニタリングとデバイスのアップデート

個別のデバイスへセキュアなアクセス

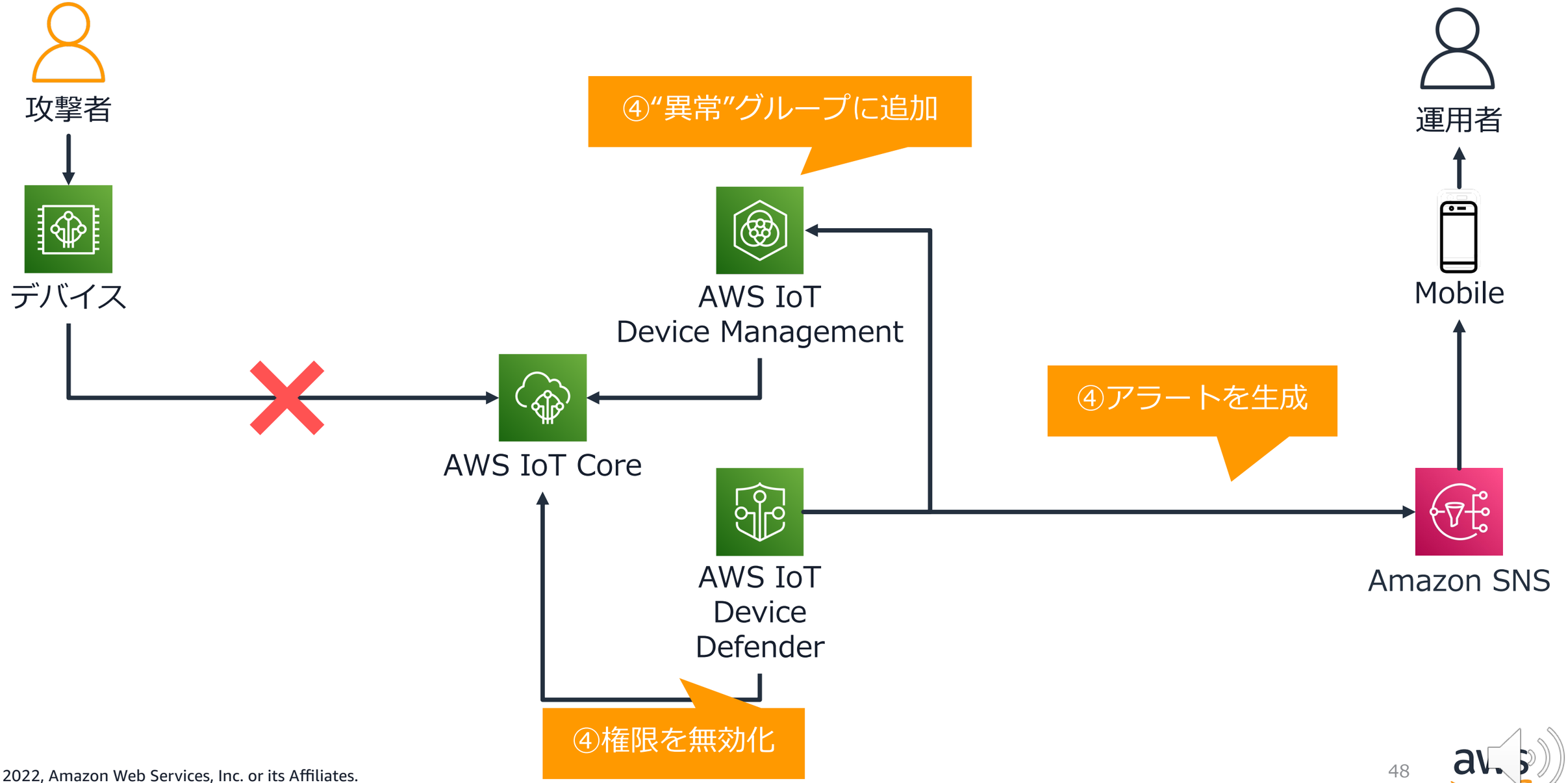
デバイス攻撃の影響を最小にしたい (1/3)



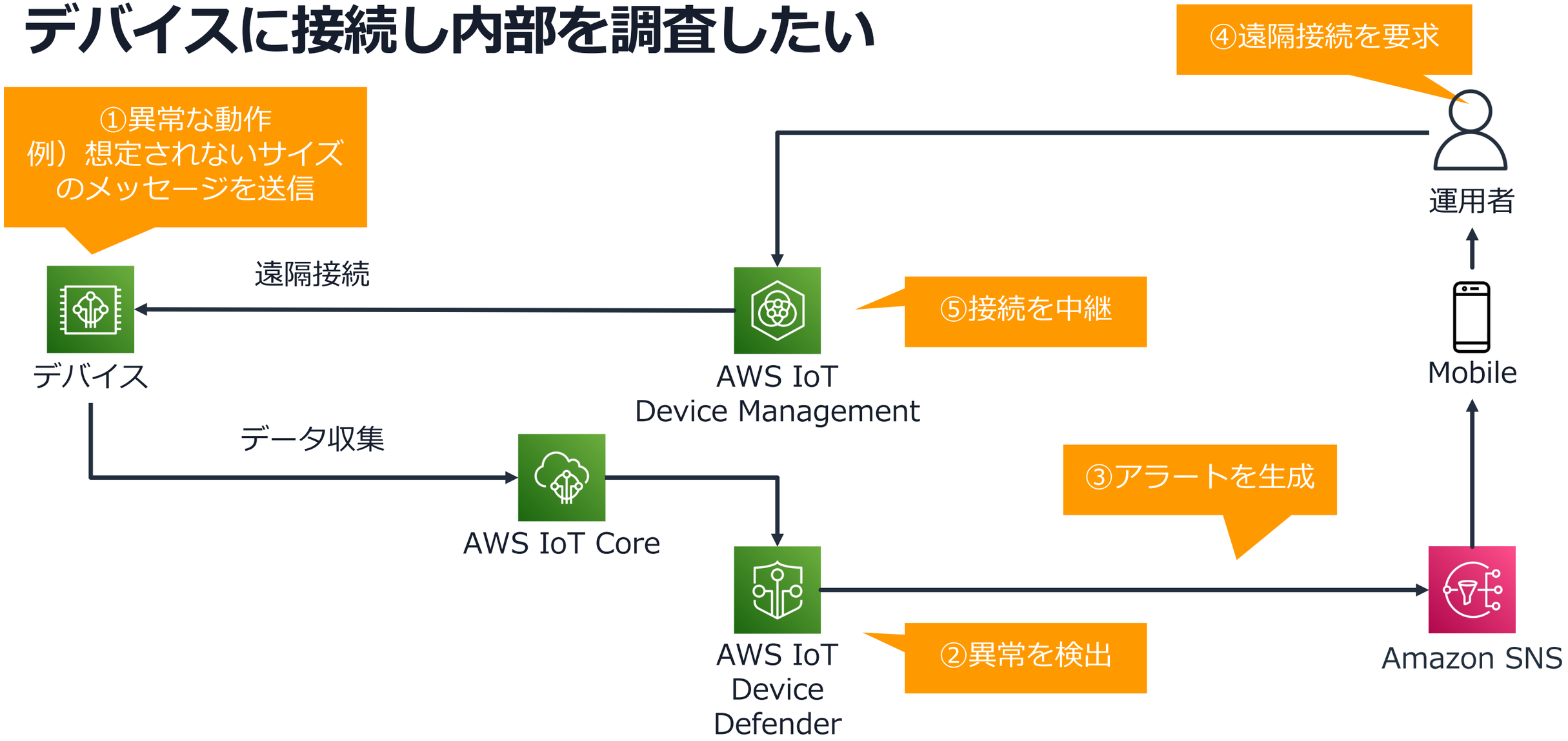
デバイス攻撃の影響を最小にしたい (2/3)



デバイス攻撃の影響を最小にしたい (3/3)



デバイスに接続し内部を調査したい



アジェンダ

- IoT におけるセキュリティ
- AWS IoT Device Defender とは
- AWS IoT Device Defender の機能詳細
- **AWS IoT Device Defender の料金**
- まとめ

Device Defender の料金の考え方

- **監査の料金**
  - AWS IoT Core に接続のあったデバイスの数に基づく料金
- **ルール検出の料金**
  - 送信されたモニタリングのためのデータポイントの件数に基づく料金
- **ML 検出の料金**
  - 送信されたモニタリングのためのデータポイントの件数に基づく料金

この例は、2022/4月時点での東京リージョーンの計算です。最新の情報は以下の料金サイトを参照してください

- **監査の料金**
  - 料金 = 100 台のデバイス x デバイスあたりの月額 0.00149 USD = 0.15 USD/月
- **ルール検出の料金**
  - 100 台のデバイス、1 時間あたり 2 データポイントの割合で 4 つのメトリックを報告しています。
  - 月間のメトリクス データポイントの件数 = 100 台のデバイス x 4 件のメトリクス x 2 件のデータポイント/時間 x 24 時間 x 30 日/月 = 576,000件
  - 料金 = 576,000 メトリクスデータポイント x 0.034 USD/100,000 件のメトリクスデータポイント = 0.20 USD/月
- **ML 検出の料金**
  - 100 台のデバイスがあり、ML 検出をオンにすると、1 時間あたり 2 データポイントの割合で 6 つのメトリックが報告されます
  - 月間のメトリックデータポイントの件数 = 100 台のデバイス x 6 件のメトリック x 2 件のデータポイント/時間 x 24 時間 x 30 日/月 = 864,000件
  - 料金 = 300,000 メトリックデータポイント x 100,000 メトリックデータポイントあたり 2.70 USD + (864,000 - 300,000) メトリックデータポイント x 100,000 メトリックデータポイントあたり 1.00 USD = 1 か月あたり 13.74 USD

- **合計月額料金** = 監査コスト 0.15 USD + ルール検出コスト 0.20 USD + ML 検出コスト 13.74 USD (100 台のデバイスが 6 つのメトリックを報告する場合) = 14.09 USD

https://aws.amazon.com/jp/iot-device-defender/pricing/

AWS IoT Device Defender を学びたい

https://aws.amazon.com/jp/blogs/news/aws-iot-device-defender-workshop/

AWS IOT DEVICE DEFENDERハンズオン

はじめに

Note

このハンズオンではAWS IoT Device Defenderを利用してIoTをデバイスの監査を行う方法について学びます。AWS IoTサービス全般の利用方法や説明はこのハンズオンで扱っておりません。 記載内容は2020年3月末現在のテスト実行結果に基づいていますが、その後、AWSコンソール画面やメッセージなど変更されている可能性がある点をご了承ください。

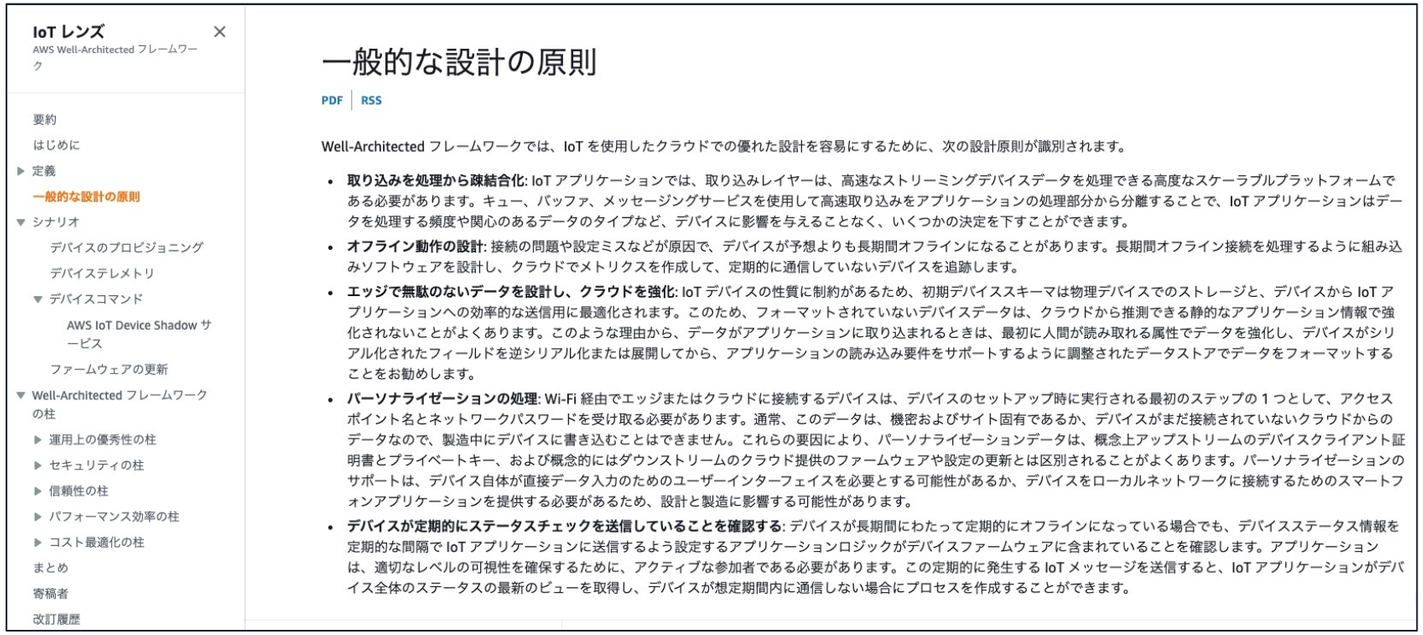
AWS IoT Device Defender を始めるには

1. 監査の機能を有効にして、現状を確認
    - https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/device-defender-audit.html
    - スケジュールによる監査を設定
        - https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/AuditCommands.html#dd-api-iot-CreateScheduledAudit

2. 検出機能で、デバイスの異常動作を確認
    - https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/device-defender-detect.html

IoT レンズ – AWS Well-Architected フレームワーク

Well-Architected IoT アプリケーションを実装するには、接続された物理的アセット (モノ) の調達から、安全で信頼性の高い自動化された方法でそれらの同じアセットを最終的に廃棄することまで、Well-Architected 原則に従う必要がある



https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/iot-lens/welcome.html

まとめ

- AWS IoT Device Defender を利用することで、デバイスをセキュアに保ち続けるために、セキュリティ上の問題やデバイスの異常な挙動を検出し、通知を受け、対応することができる

- サーバ側の監査、検出は数クリックで利用可能。デバイスに SDK を組み込めば、より多角的に異常な振る舞いを検出できる

- AWS IoT Device Management と組み合わせて、過剰な権限付与がされているような問題を Job の実行により、適切なアクセス範囲となるように設定反映させることで複雑な対応も自動化が可能に

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しましては、有料のAWSサポート窓口へ
  お問い合わせください
  - https://aws.amazon.com/jp/premiumsupport/
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
  お問い合わせください（マネジメントコンソールへのログインが必要です）
  - https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service
- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS のハンズオン資料の場所「AWS ハンズオン」で検索

AWS 初心者向けハンズオン

AWS 初心者向けに「AWS Hands-on for Beginners」と題し、初めて AWS を利用する方や、初めて対象のサービスを触る方向けに、操作手順の解説動画を見ながら自分のペースで進められるハンズオンをテーマごとにご用意しています。

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS 個別相談会

- 毎週「AWS 個別相談会」を実施中
  - AWS のソリューションアーキテクト（SA）に対策などを相談することも可能
- 申込みは下記の URL から
  - https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html

AWS 個別相談会 で[検索]

ご視聴ありがとうございました