IoT ユースケースの具体的パターンから見る AWS IoT の使いどころ

アマゾン ウェブサービス ジャパン合同会社

登壇者紹介

中西 貴大（なかにし たかひろ）

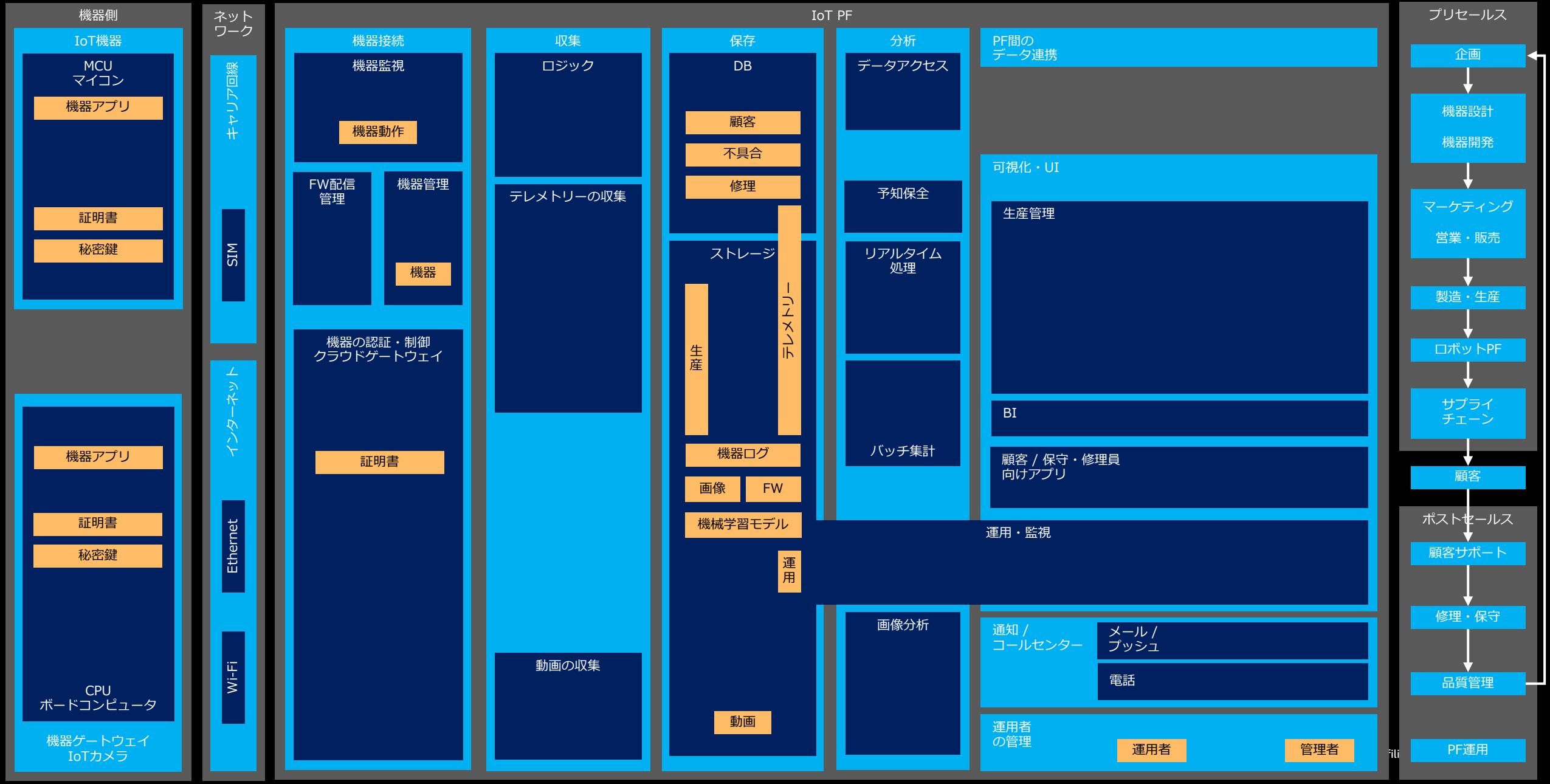
所属：

アマゾン ウェブ サービス ジャパン合同会社
技術統括本部 エンタープライズソリューション本部
ストラテジック製造ビジネス部
ソリューションアーキテクト

aws

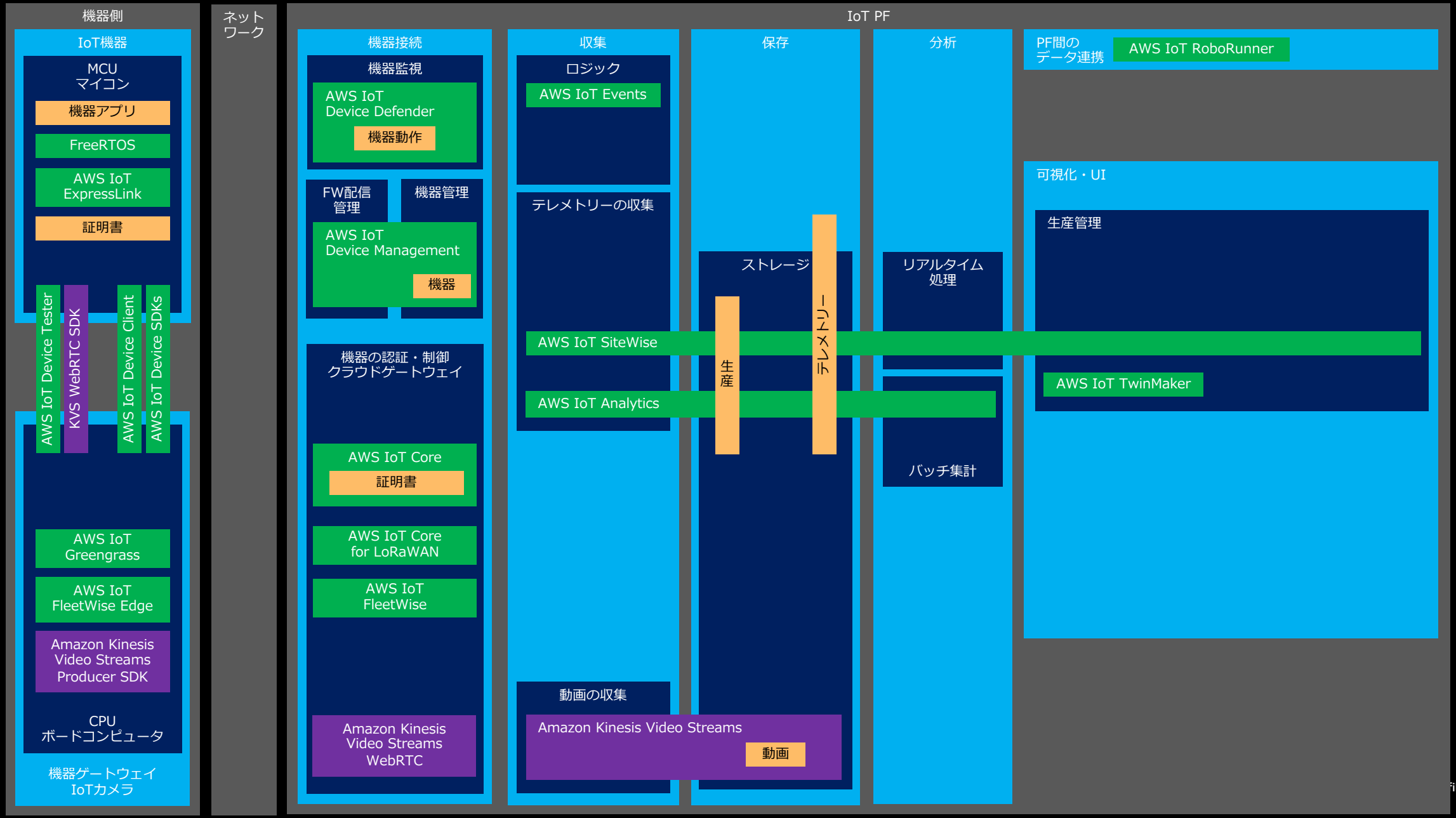
IoT PFに必要な**機能**

AWSセッション①で掲載済み



AWS IoTサービス群

AWSセッション①で掲載済み



アジェンダ

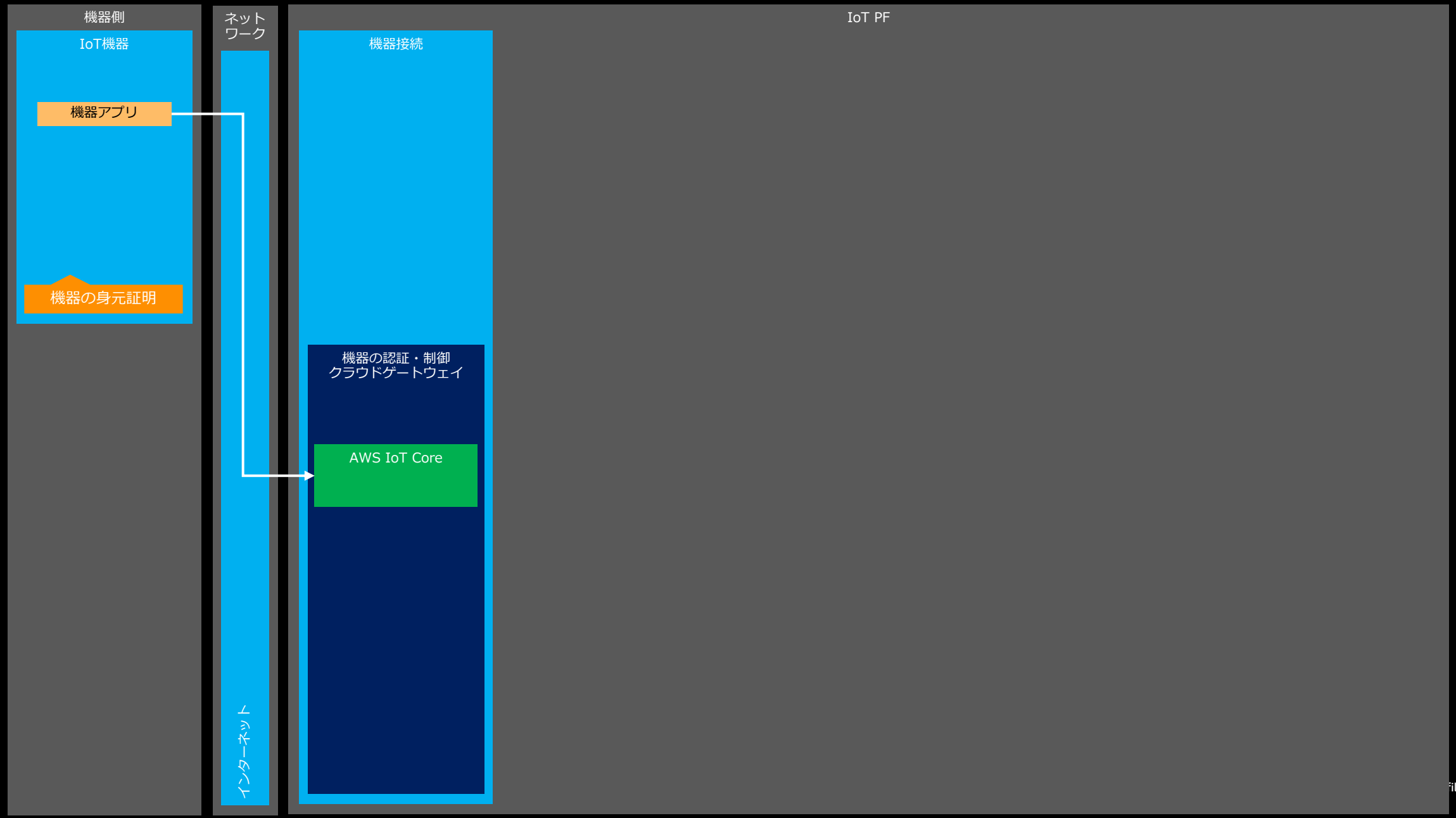
- ユースケースごとの紹介
  - 大量のデバイスの登録
  - 大量のデバイスの管理とその自動化
  - Amazon Kinesis Video Streams: メディア形式とWebRTCの使い分け
- すぐにできるアクション: ハンズオンのご紹介
- まとめ

アジェンダ

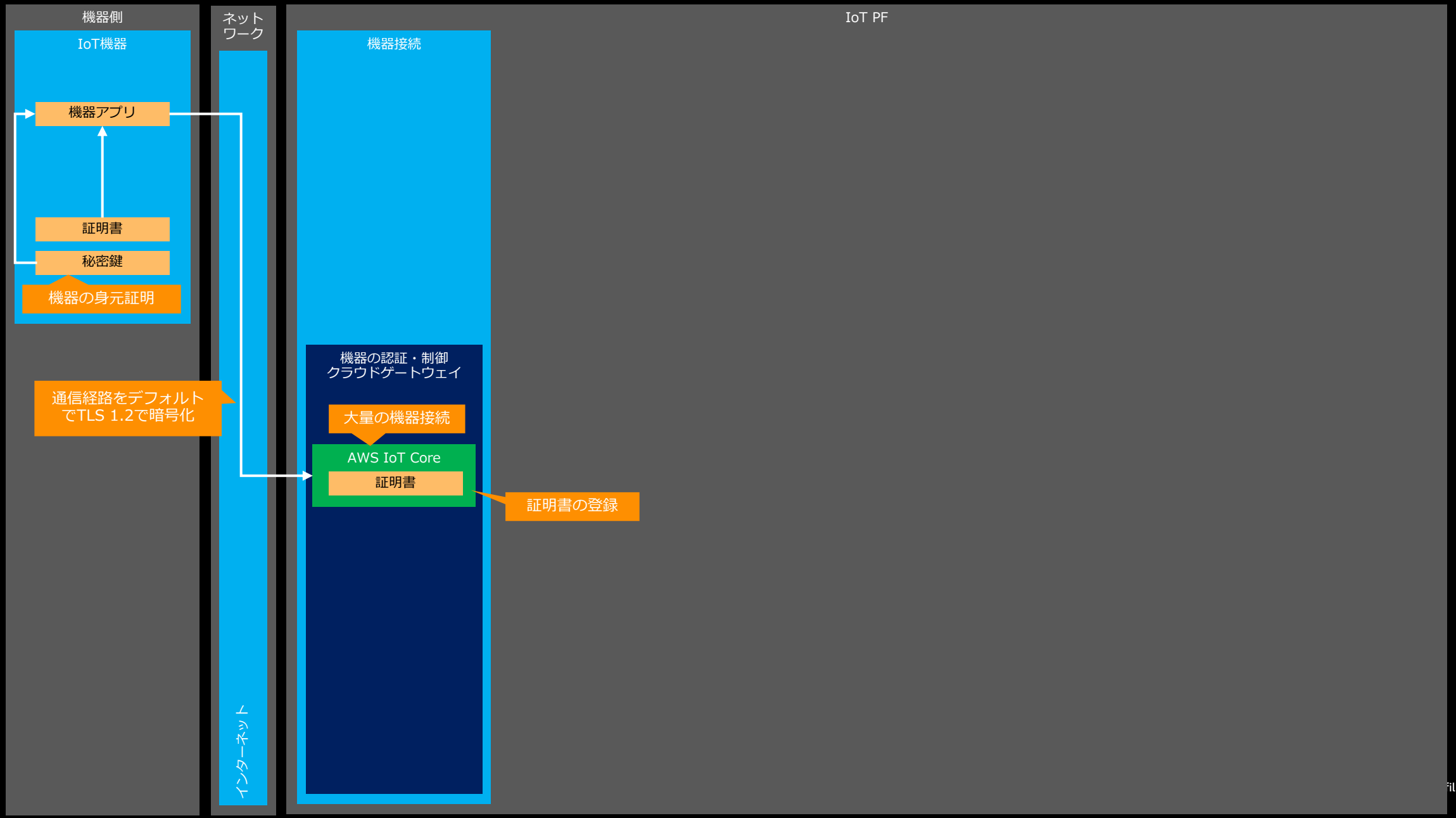
- ユースケースごとの紹介
  - 大量のデバイスの登録
  - 大量のデバイスの管理とその自動化
  - Amazon Kinesis Video Streams: メディア形式とWebRTCの使い分け
- すぐにできるアクション: ハンズオンのご紹介
- まとめ

大量のデバイスの登録

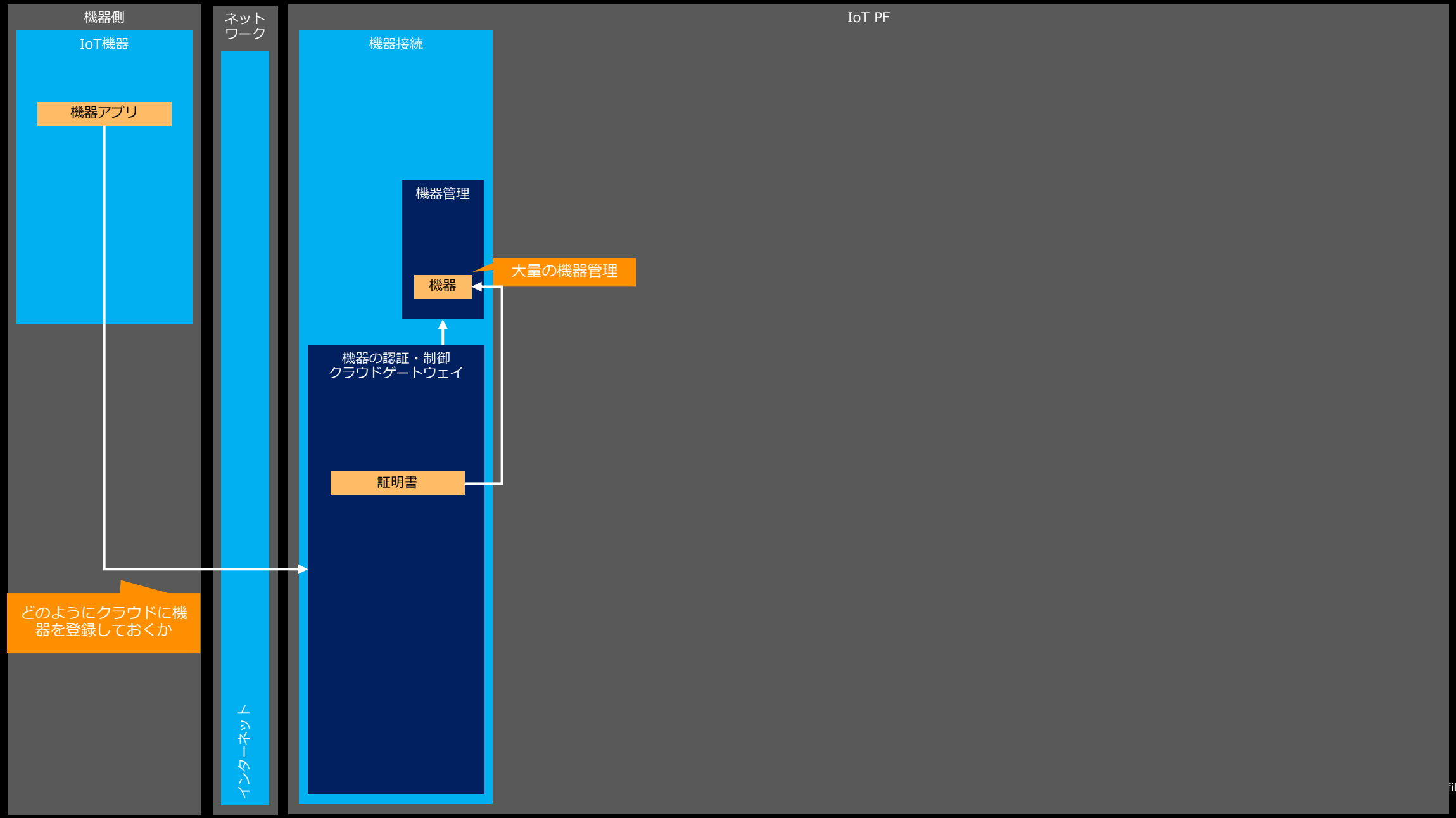
機器の**身元を証明**するには？



機器の身元証明には**デバイス証明書**を用いる



大量の機器を**登録**、証明書を**発行**するには？



AWS IoTにおけるデバイス登録方式

(*1) CSRを用いた場合
(*2) クレデンシャルが必要

どの証明書を用いるか		秘密鍵がインターネットを通るのはNG	製造時に個別証明書を埋め込むのが困難	セキュアチップでベンダCAを利用	複数アカウントで同じ証明書を利用したい
Amazonが管理するCAで証明書を発行 • CAの運用は不要 • 証明書の有効期限は固定	**AWS IoTによる秘密鍵・証明書発行＆事前登録**	No	No	No	No
	AWS IoTによる証明書発行＆事前登録	Yes(*1)	No	No	No
	Fleet Provisioning登録	Yes(*1)	Yes	No	No
Amazon以外のCAで発行した証明書を利用 • 証明書の有効期限を管理可能 • CAの運用が必要	**独自CAによる証明書発行＆AWS IoTへの事前登録**	Yes	No	Yes	Yes
	JITRによる登録	Yes	Yes	No	Yes
	JITPによる登録	Yes	Yes	No	Yes
	CA登録無しの証明書登録（マルチアカウント登録）	Yes	Yes(*2)	Yes	Yes

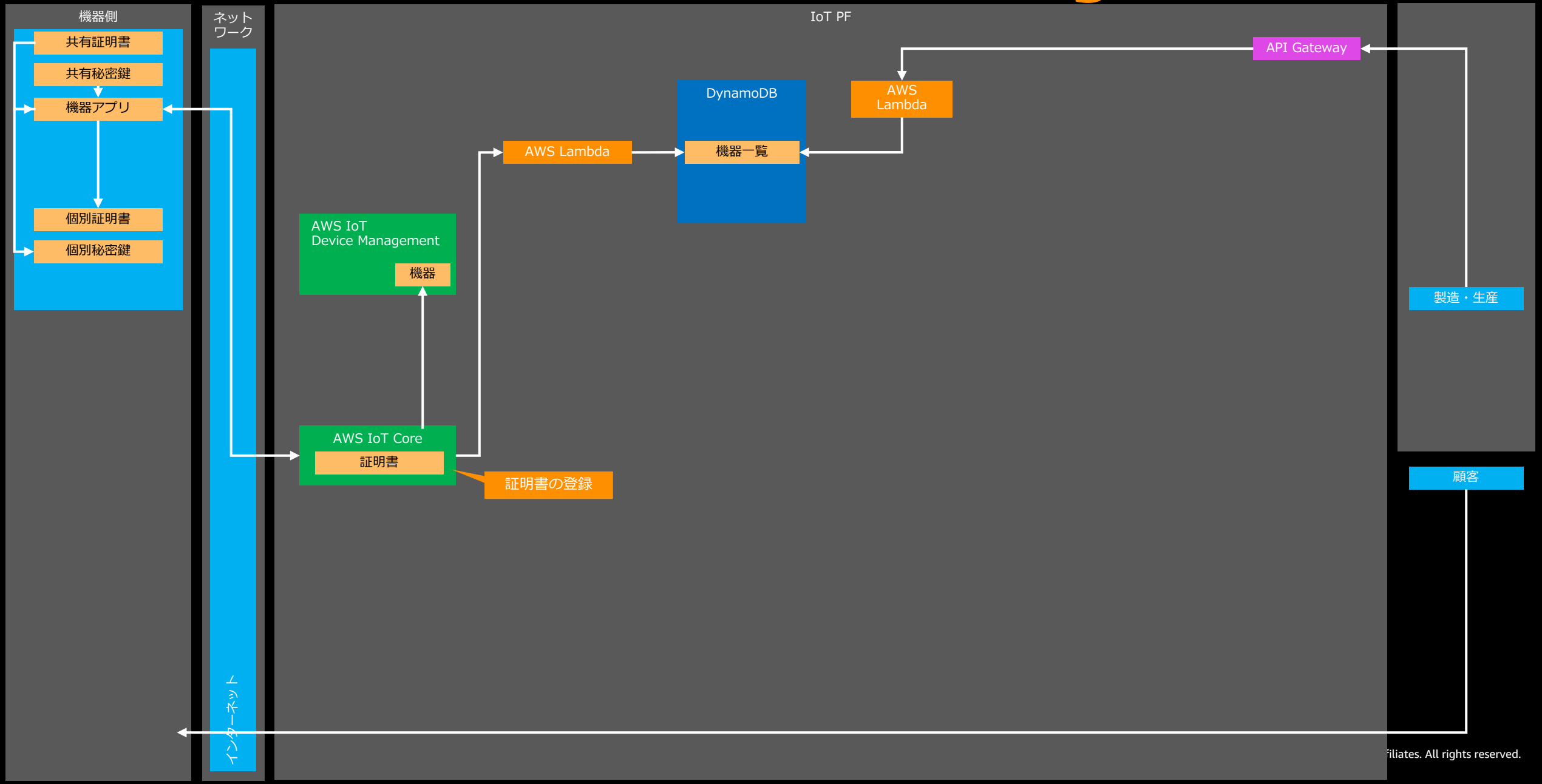
AWS IoTにおけるデバイス登録方式

(*1) CSRを用いた場合
(*2) クレデンシャルが必要

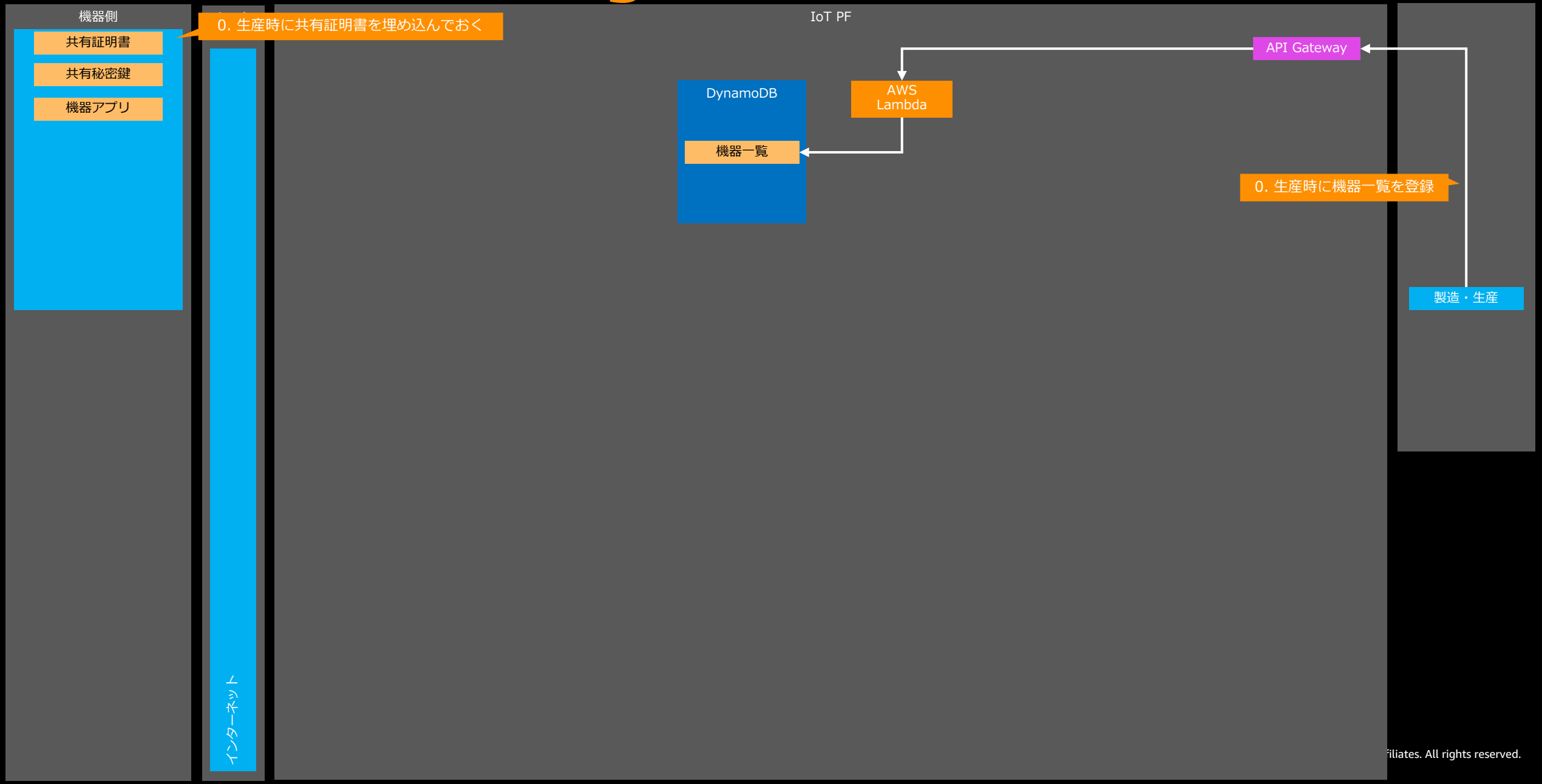
どの証明書を用いるか		秘密鍵がインターネットを通るのはNG	製造時に個別証明書を埋め込むのが困難	セキュアチップでベンダCAを利用	複数アカウントで同じ証明書を利用したい
Amazonが管理するCAで証明書を発行 • CAの運用は不要 • 証明書の有効期限は固定	**AWS IoTによる秘密鍵・証明書発行＆事前登録**	No	No	No	No
	Fleet Provisioning登録	Yes(*1)	Yes	No	No
Amazon以外のCAで発行した証明書を利用 • 証明書の有効期限を管理可能 • CAの運用が必要	**独自CAによる証明書発行＆AWS IoTへの事前登録**	Yes	No	Yes	Yes
	JITRによる登録	Yes	Yes	No	Yes
	JITPによる登録	Yes	Yes	No	Yes
	CA登録無しの証明書登録（マルチアカウント登録）	Yes	Yes(*2)	Yes	Yes

このような場合：
- Amazonが管理するCAで証明書を発行したい
- 製造時に個別証明書を埋め込まない

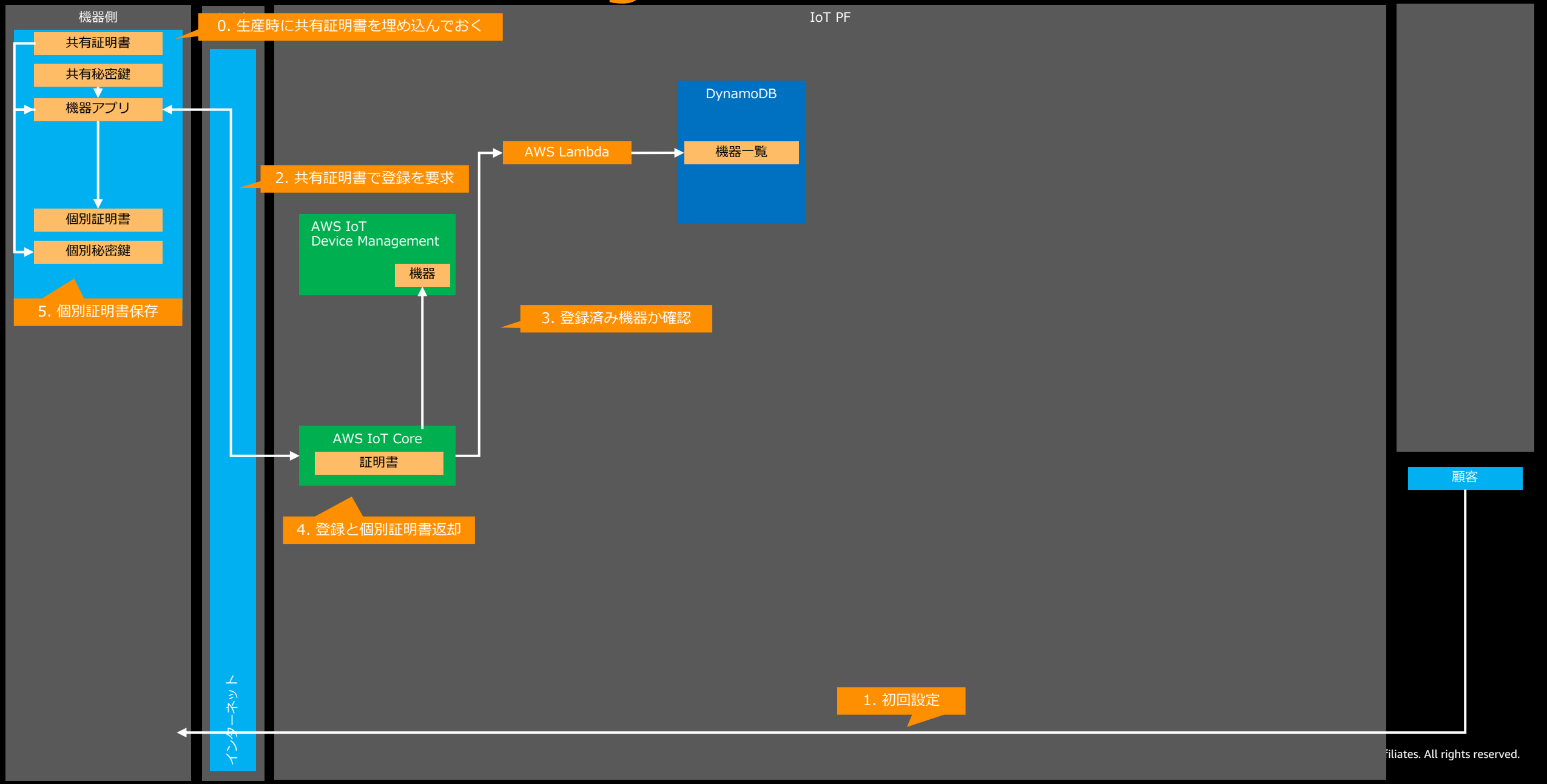
AWS IoT Core: Fleet Provisioning 全体構成



Fleet Provisioningのための事前準備



Fleet Provisioningのデバイス登録フロー



認証情報プロビジョニングの参考資料

aws

AWS IoTにおけるデバイスへの認証情報のプロビジョニング

アマゾン ウェブサービス ジャパン株式会社

AWS IoTにおける証明書発行とデバイス登録の方式

1. AWS IoTによる秘密鍵・証明書発行＆事前登録
   (デバイスキッティング時登録)
2. AWS IoTによる証明書発行＆事前登録
   (デバイスキッティング時登録)
3. Fleet Provisioning登録
4. 独自CAによる証明書発行＆AWS IoTへの事前登録
5. 独自CAによる証明書発行＆JITRによる登録
6. 独自CAによる証明書発行＆JITPによる登録
7. CA登録無しの証明書登録（マルチアカウント登録）

AWS IoTではこのように様々な選択肢を用意

aws

https://pages.awscloud.com/rs/112-TZM-766/images/EV_iot-deepdive-aws2_Sep-2020.pdf

aws

Fleet Provisioningではこんなことに注意

- Fleet Provisioning の MQTT API に関するクォータ

API	デフォルトの最大値	クォータ引き上げ
CreateCertificateFromCsr	100 TPS	可能
CreateKeysAndCertificate	10 TPS	可能
RegisterThing	10 TPS	可能

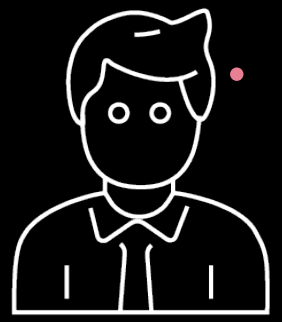
(TPS: 1秒あたりのトランザクション)
2022年10月13日時点

- プロビジョニング用クレーム証明書・秘密鍵を保護すること
  - デバイス上で安全に保存（セキュリティ要件によっては秘密鍵を HSM や TPM に保存）
  - 意図しない利用を監視し、もし検出した場合はクレーム証明書を無効化する（下記が前提）
- デバイス証明書・秘密鍵を入れ替えられる仕組みを構築すること
  - 有効期限切れや不正利用に備え、クラウド側とデバイスFW側の両方で実装が必要

大量のデバイスの管理とその自動化

想定ストーリー

万が一テストで判明しないバグがFWに潜んでいたら？



例えば

デバイスの設置環境によってメッセージの頻度が異常に増加するバグ

- AWS IoTのコストが意図せず増加
- スロットリングが起こり他デバイス利用者にも影響、
  サービス継続性にリスク

コストやクォータの観点でも安全なプラットフォームを構築したい

デバイスの挙動を監視し、管理者への通知やFW更新の判断を自動化できないか？

AWS IoT Device Defender

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

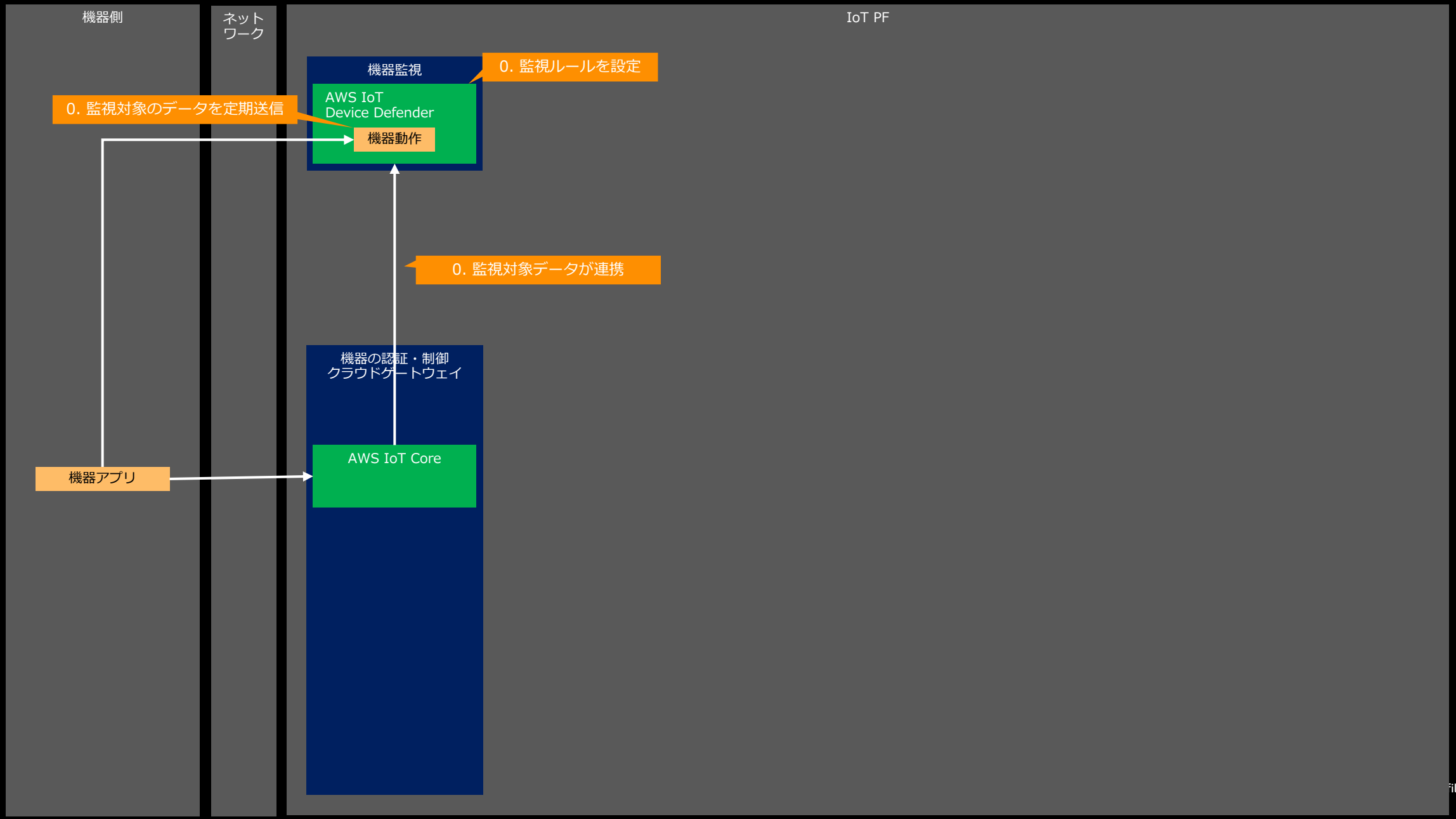
カスタムメトリクス

- 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)

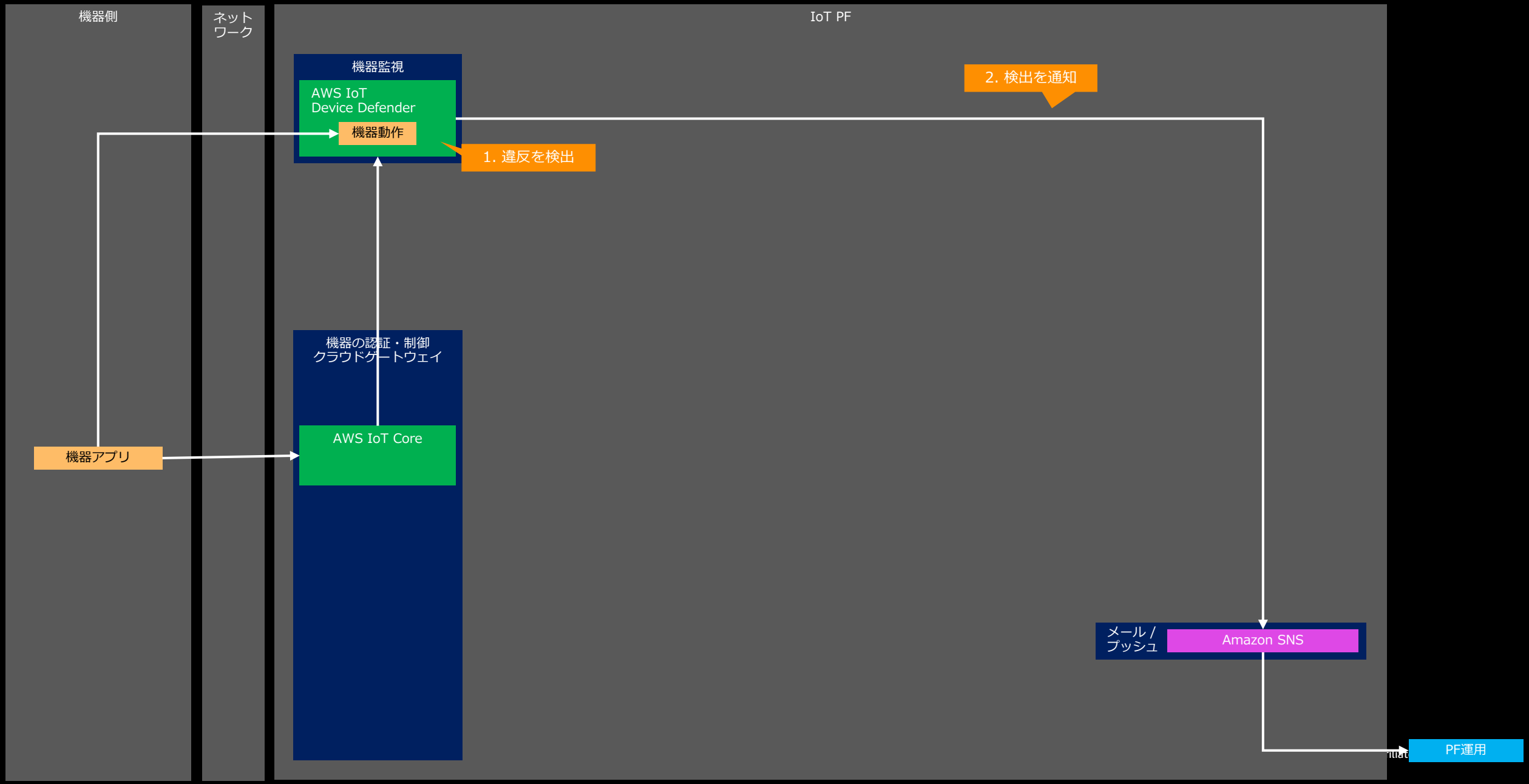
- 事前定義したルールや統計ベースから外れた以上の発生時にアラームを受信

- 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

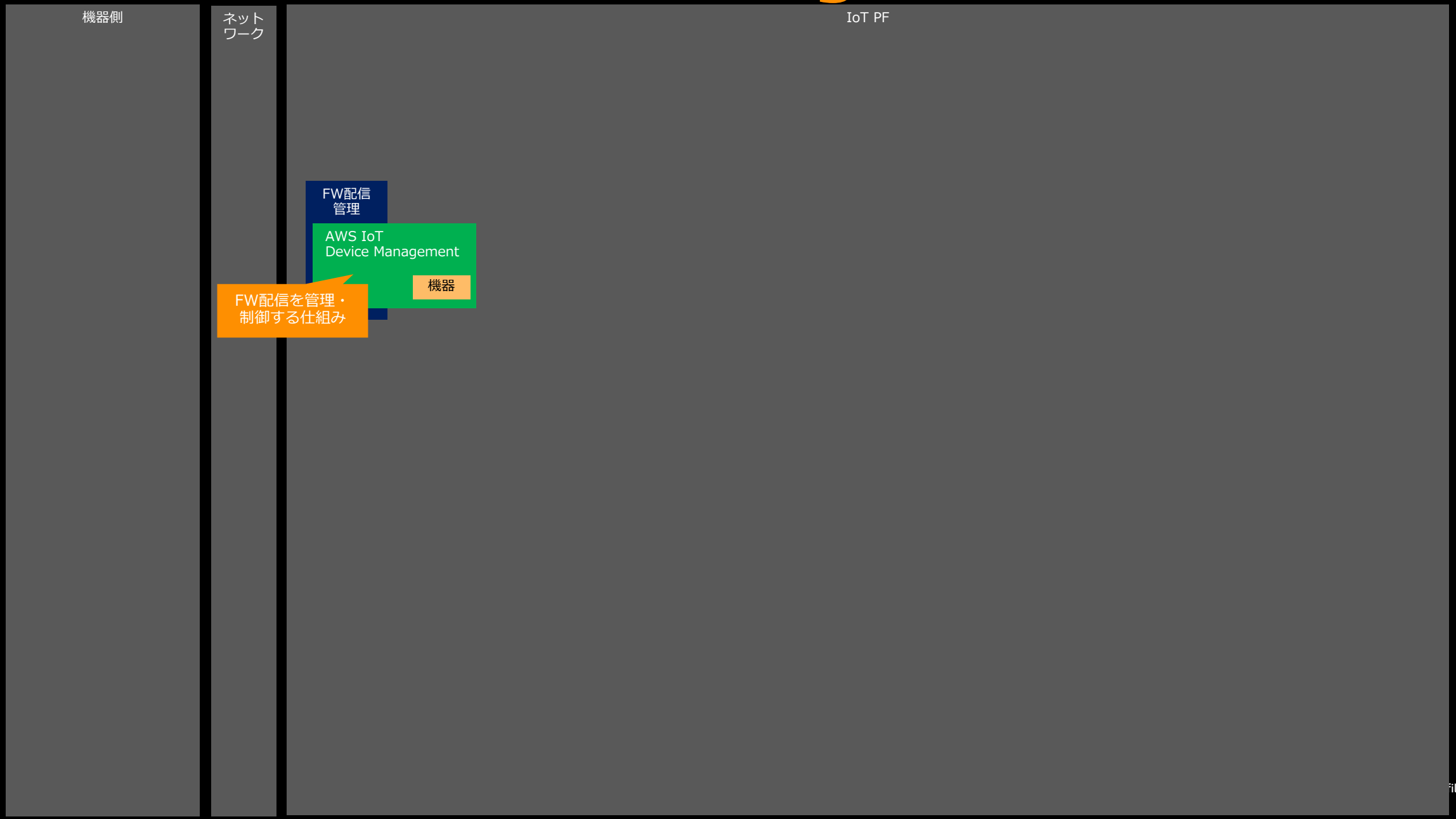
機器を監視



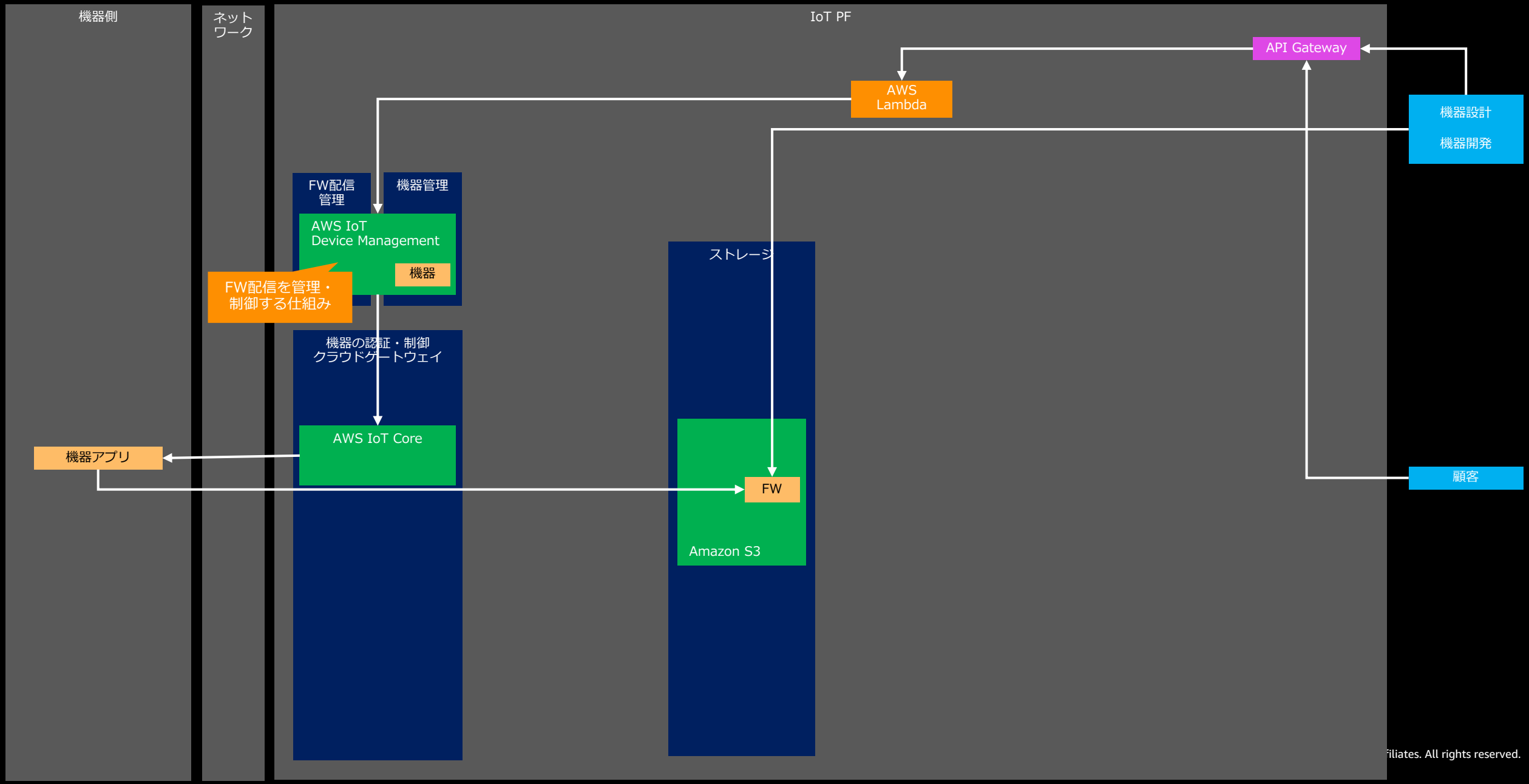
機器を監視


機器側
ネットワーク
IoT PF
機器監視
AWS IoT
Device Defender
機器動作
2. 検出を通知
1. 違反を検出
機器の認証・制御
クラウドゲートウェイ
AWS IoT Core
機器アプリ
メール / プッシュ
Amazon SNS
PF運用

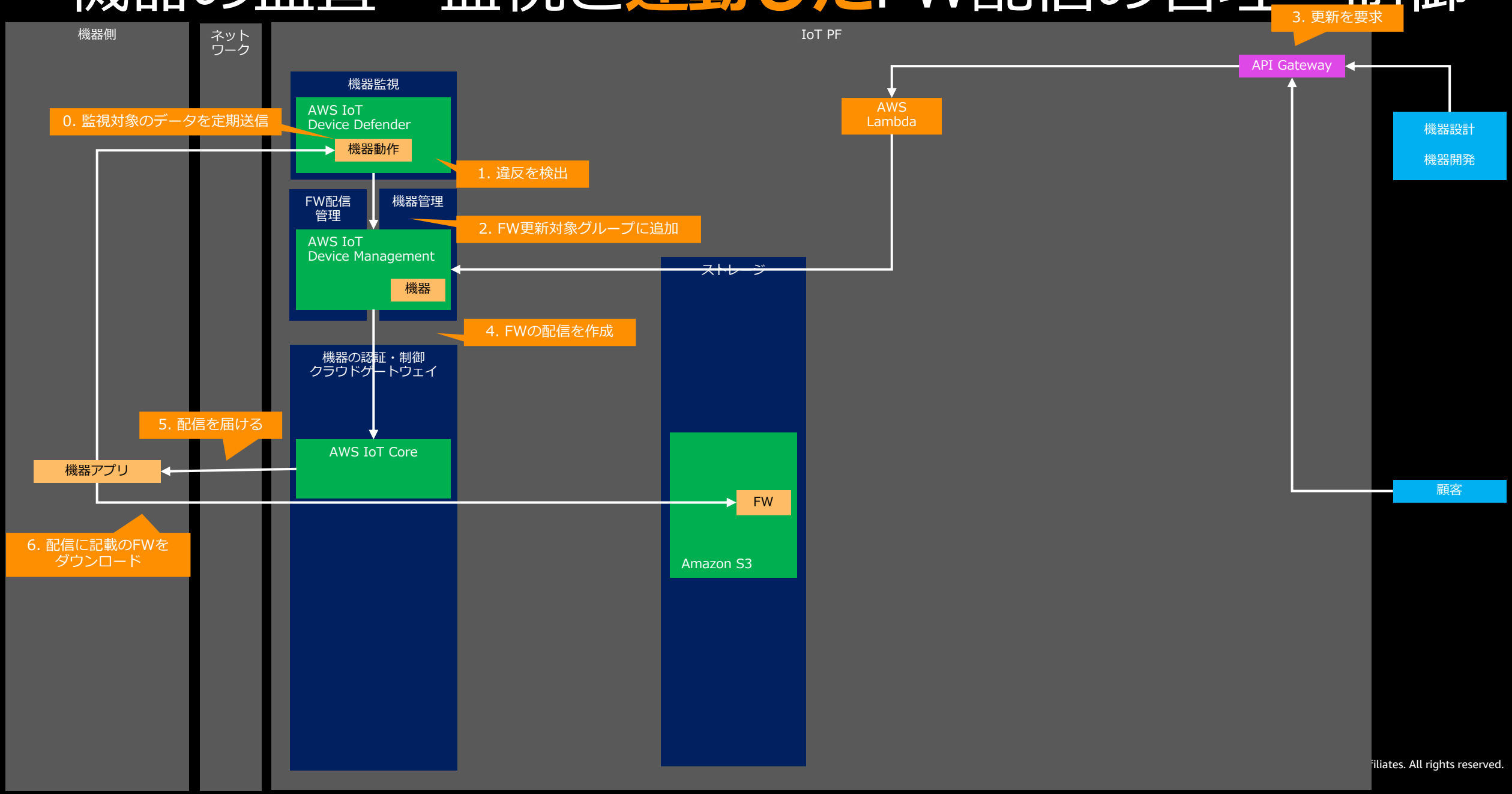
AWS IoT Device Management



大量の機器へのFW配信を管理・制御する

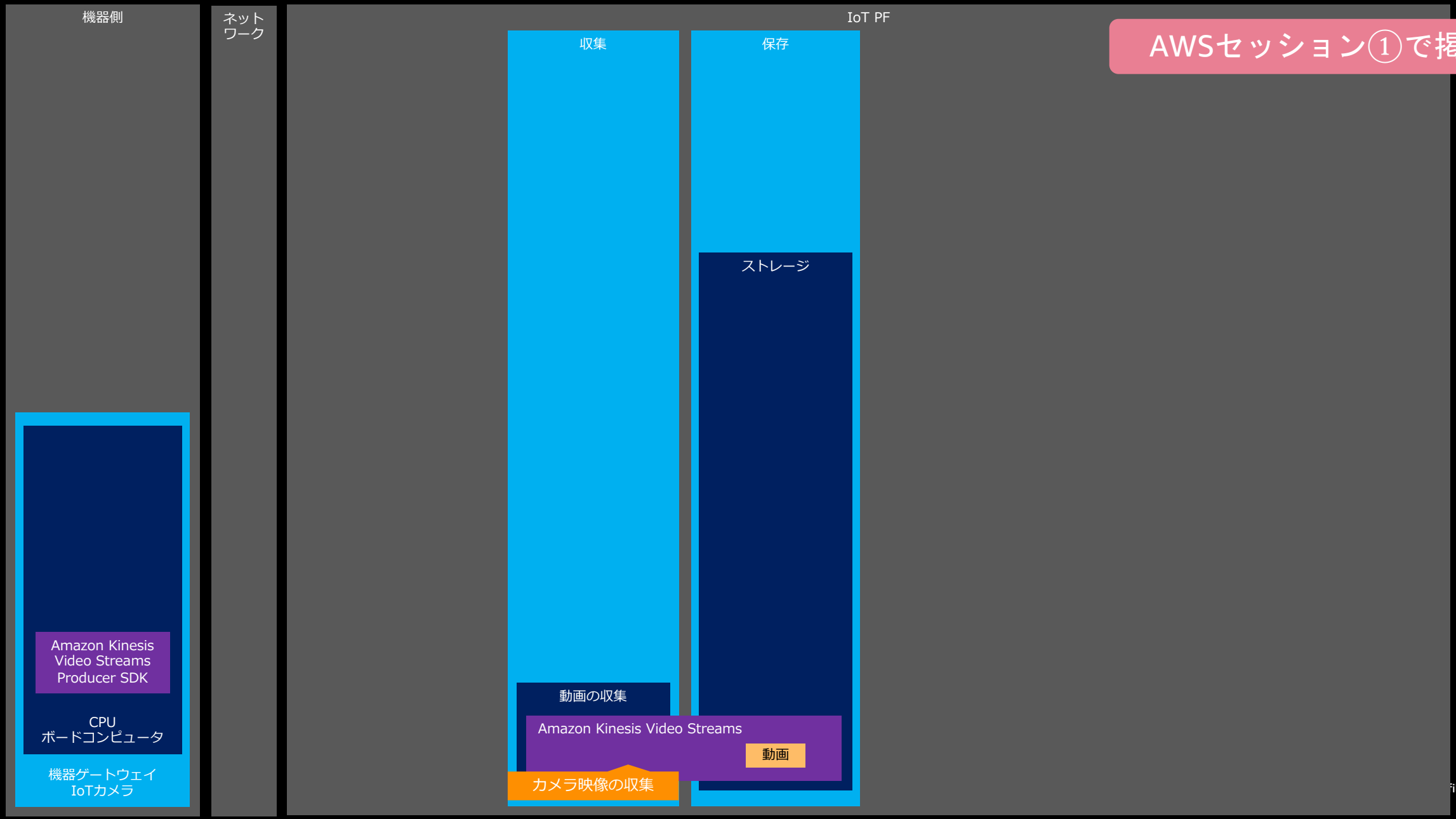


機器の監査・監視と**連動した**FW配信の管理・制御



Amazon Kinesis Video Streams:
メディア形式とWebRTCの使い分け

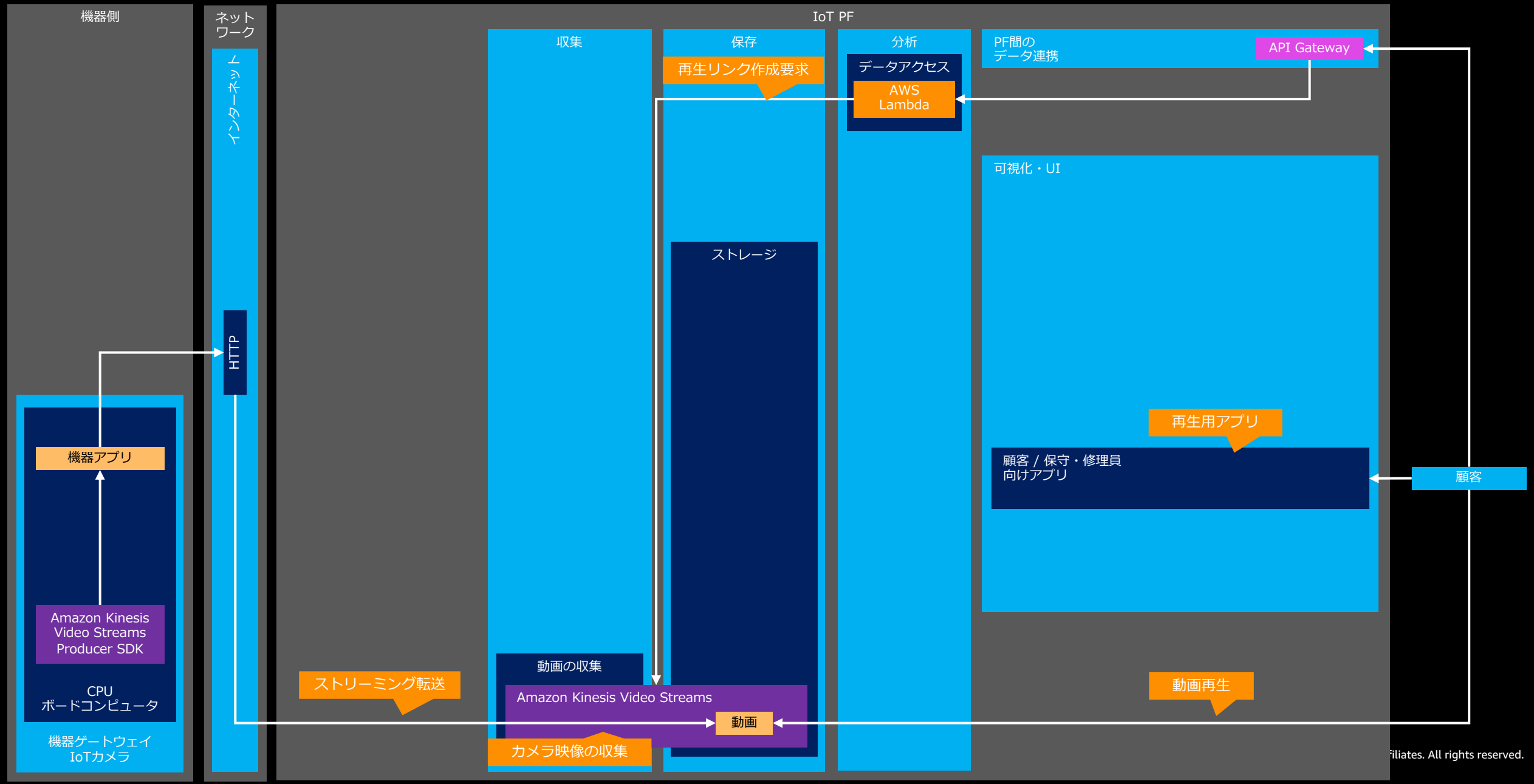
Amazon Kinesis Video Streamsを活用して……



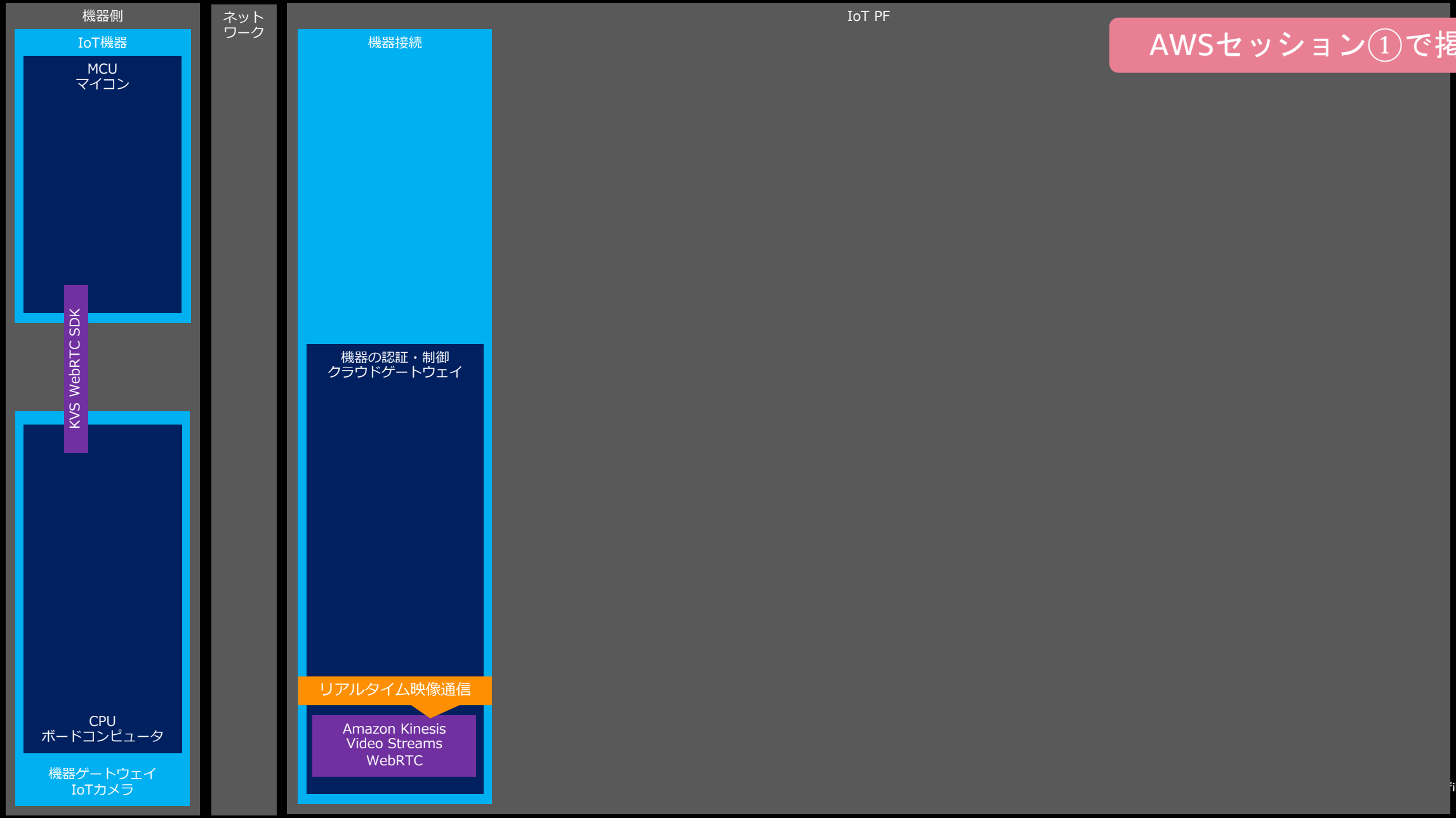
AWSセッション①で掲載済み

ストリーミング映像を保存、再生

AWSセッション①で掲載済み

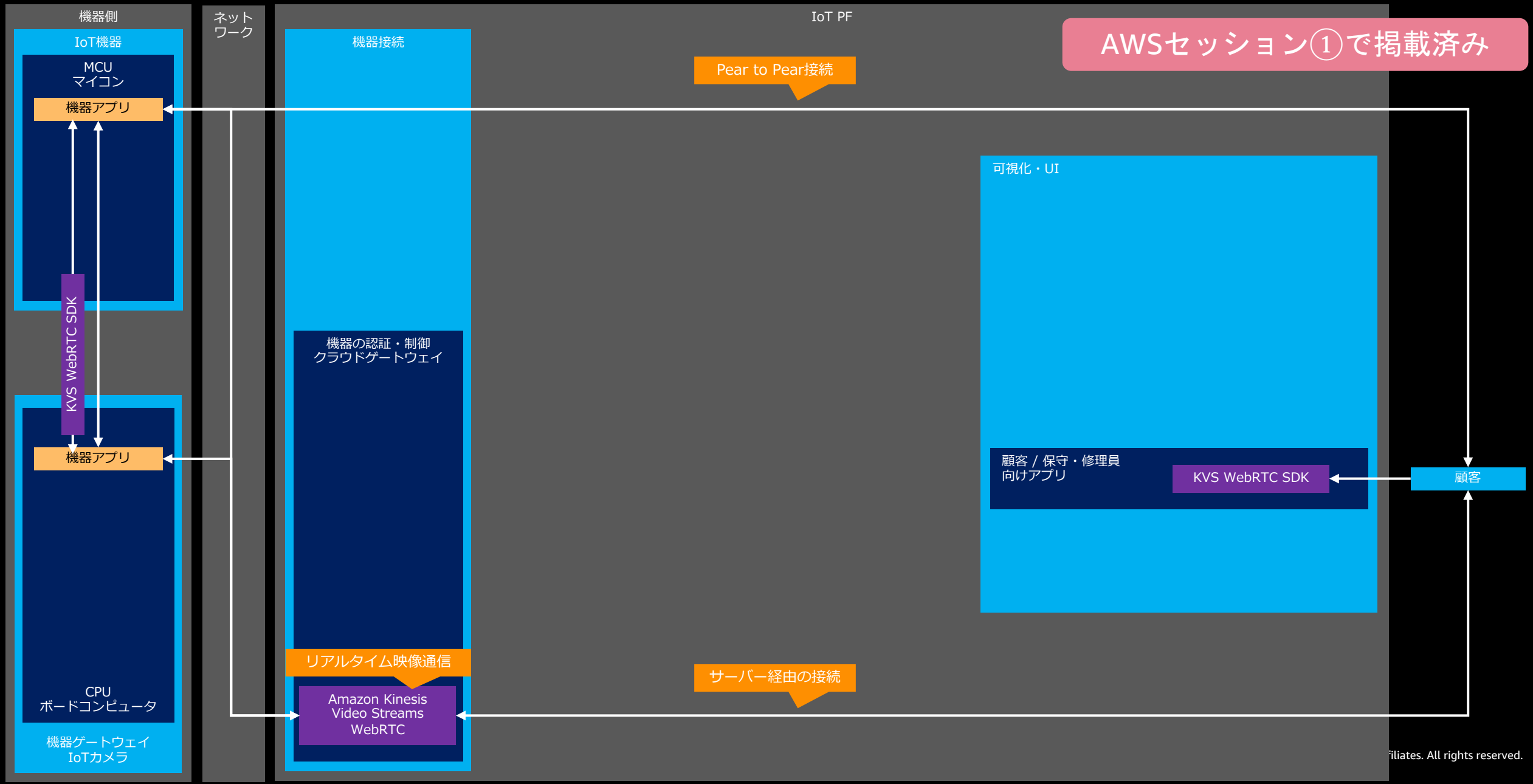


Amazon Kinesis Video Streams WebRTCを活用して……



AWSセッション①で掲載済み

映像をリアルタイムかつ双方向に転送

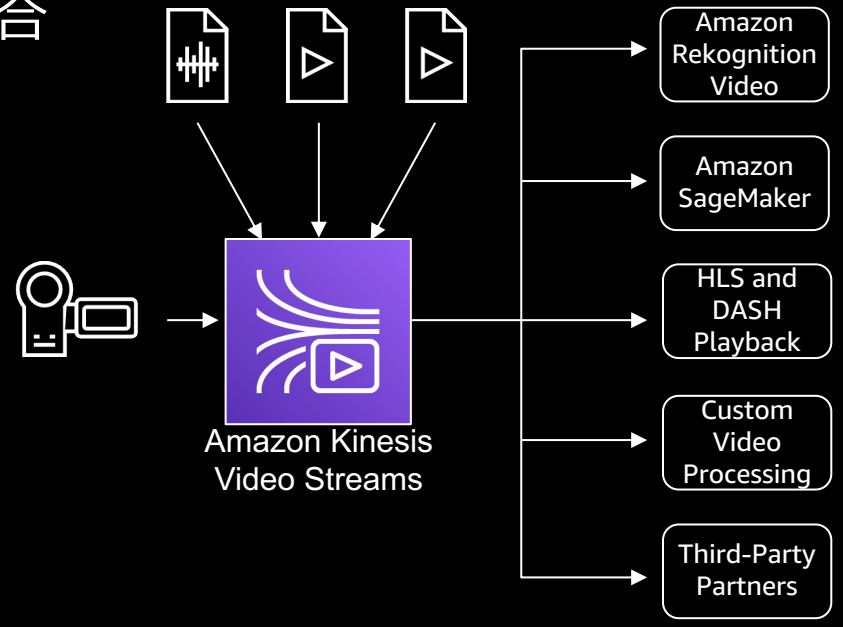


Amazon Kinesis Video Streams - 2種類のストリーミング方法

メディア形式で収集

数百万台規模のデバイスからのセキュアなデータ取り込み

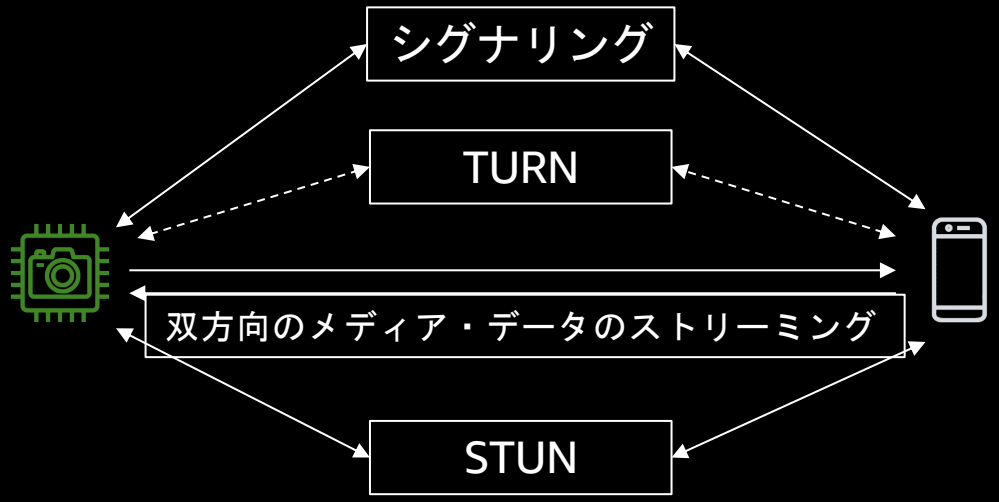
- 時系列でインデックスされたメディアデータの保存とAPI経由での検索
- カメラデバイス向けのSDK
- メディアの再生と機械学習サービスとの統合



WebRTC

WebRTC によるリアルタイムの双方向メディアストリーミング

- シグナリング、STUN、TURN のマネージドサービス
- 組み込みデバイス向けSDK、ウェブ・モバイルアプリ向けのSDK



Amazon Kinesis Video Streams の使い分け

	メディア形式で収集	WebRTC
動画データのクラウド保存 機械学習サービスでの分析	できる	できない
双方向ストリーミング	できない	できる
ライブ再生時のレイテンシ	2秒～	1秒未満
カメラデバイスからの ストリーミングに利用する SDK	Producer SDK	WebRTC SDK

※ レイテンシはデバイス性能、ネットワーク環境、映像のビットレート、フラグメントの設定などによって変化します

レイテンシーの考え方

メディア形式で収集

End-to-End のメディアデータフローにおける、レイテンシーの重要な要因

デバイスのメディアパイプライン	イメージセンサーからのデータ読み取り、(ハードウェア/ソフトウェア)エンコーダーでのメディア変換処理
インターネットのデータ伝送	デバイスからクラウドまでのネットワークスループットやレイテンシ
Amazon Kinesis Video Streams のデータ受信時のレイテンシー	データ保持設定時のデータの暗号化と時間ベースのインデックス生成
Amazon Kinesis Video Streams からコンシューマーの間のレイテンシー	HLS 再生時の動画変換の内部処理、クラウドとコンシューマの間のネットワーク環境、プレイヤーの設定(バッファなど)

タイムスタンプの計測や、プロデューサー・コンシューマーの設定、ネットワーク環境の変更などによってレイテンシーの要因を切り分けることで、レイテンシーを短縮するためのアクションが可能

https://aws.amazon.com/jp/kinesis/video-streams/faqs/

aws

Amazon Kinesis Video StreamsのSDKの比較

メディア形式で収集 **Producer SDK**		WebRTC **WebRTC SDK**
C/C++/Java/Android	言語	C/JavaScript/Android/iOS
Linux, macOS, Windows, Android	デバイス/環境	組み込みカメラ、 ブラウザ、モバイル

Amazon Kinesis Video Streams が 画像抽出のマネージドサポートを発表 (2022/5/4)

サムネイル生成や、MLパイプライン用の画像生成などに利用可能

- オンデマンド画像生成 (GetImages API)
  - StartTimestamp, EndTimestamp, SamplingInterval, …などを指定して画像生成をリクエスト
- 自動画像生成 (S3への配信)
  - Kinesis Video Streamsが自動でリアルタイムに画像生成し、お客様指定のS3バケットに保存

料金

1080p 以下の解像度のストリームから生成された画像	100 万あたり 10USD
1080p を超える解像度のストリームから生成された画像	100 万あたり 18USD

アジェンダ

- ユースケースごとの紹介
  - 大量のデバイスの登録
  - 大量のデバイスの管理とその自動化
  - Amazon Kinesis Video Streams: メディア形式とWebRTCの使い分け
- すぐにできるアクション: ハンズオンのご紹介
- まとめ

ハンズオン集

- AWS IoT Core
  - https://catalog.us-east-1.prod.workshops.aws/workshops/b3e0b830-79b8-4c1d-8a4c-e10406600035/ja-JP
- AWS IoT Device Management
  - https://catalog.us-east-1.prod.workshops.aws/workshops/7c2b04e7-8051-4c71-bc8b-6d2d7ce32727/ja-JP
- AWS IoT Device Defender
  - https://catalog.us-east-1.prod.workshops.aws/workshops/90cbb951-dbf8-4f66-b994-c74072f2232c/ja-JP
- Amazon Kinesis Video Streams
  - https://catalog.us-east-1.prod.workshops.aws/kinesis-video-streams/ja-JP
- Amazon Kinesis Video Streams WebRTC
  - https://catalog.us-east-1.prod.workshops.aws/workshops/a391c4b3-5a5c-4b2a-a92a-681985d108f5/ja-JP

アジェンダ

- ユースケースごとの紹介
  - 大量のデバイスの登録
  - 大量のデバイスの管理とその自動化
  - Amazon Kinesis Video Streams: メディア形式とWebRTCの使い分け
- すぐにできるアクション: ハンズオンのご紹介
- まとめ

まとめ

- AWS IoTでの大量のデバイスの登録
  - 証明書と秘密鍵を安全に扱うための仕組みの考慮が必要
  - Fleet ProvisioningではAPIのクォータに注意（クォータ引き上げ可能）
- AWS IoTでの大量のデバイスの管理
  - 以下サービスを活用し、セキュリティ観点で監視とアクションの自動化
    - AWS IoT Device Defender
    - AWS IoT Device Management
- カメラデバイスに関するユースケースAmazon Kinesis Video Streams
  - メディア形式での収集とWebRTCの違いを理解して選択
    - 動画の保存要件
    - 単方向 or 双方向ストリーミング
    - レイテンシー
    - SDKの言語、動作環境