AWS Black Belt Online Seminar

AWS IoT 活用シリーズ

# 機器の接続と認証・認可

IoT Specialist Solutions Architect

飯塚 将太

# AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供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の各サービスやソリューションについてテーマごとに動画を公開します
- 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
- 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

# 内容についての注意点

- 本資料では 2023 年 6 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(https://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

# Speaker

**IoT Specialist**
**Solutions Architect**

**飯塚 将太**

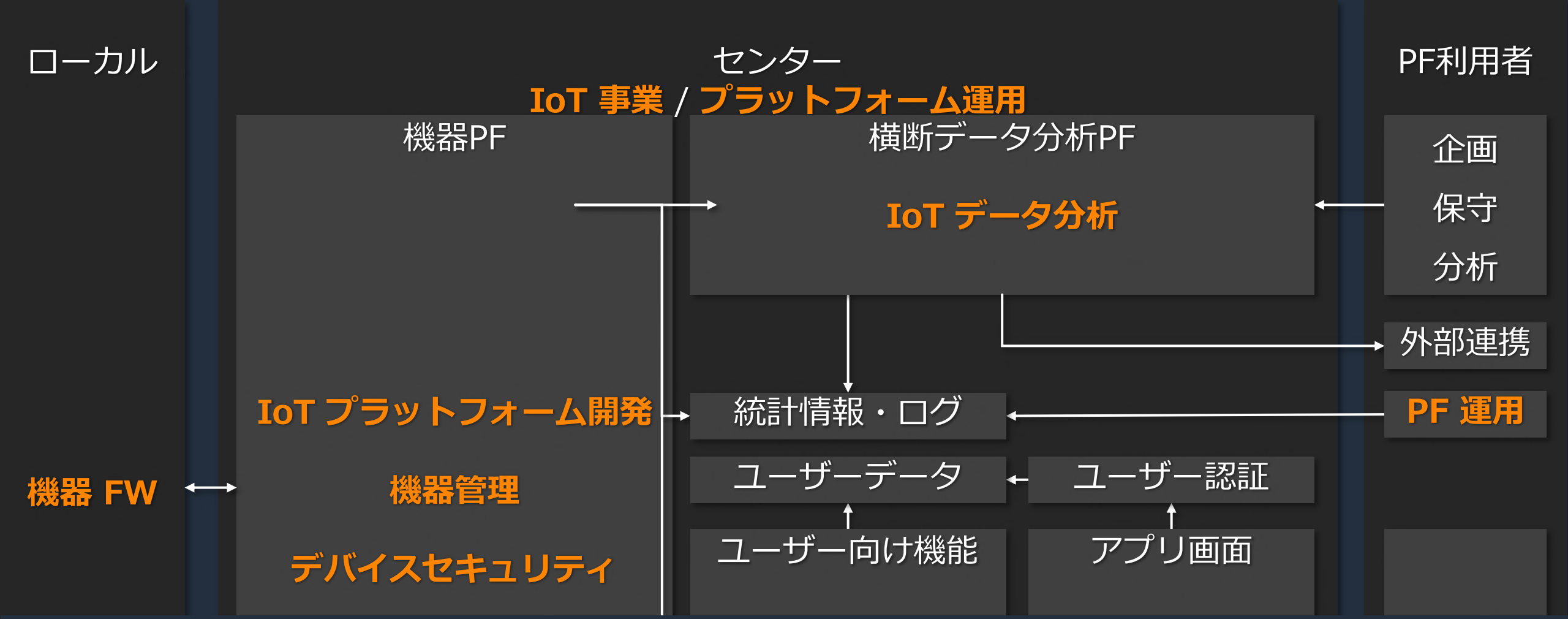
AWS Black Belt Online Seminar

AWS IoT 活用シリーズ　**前回**

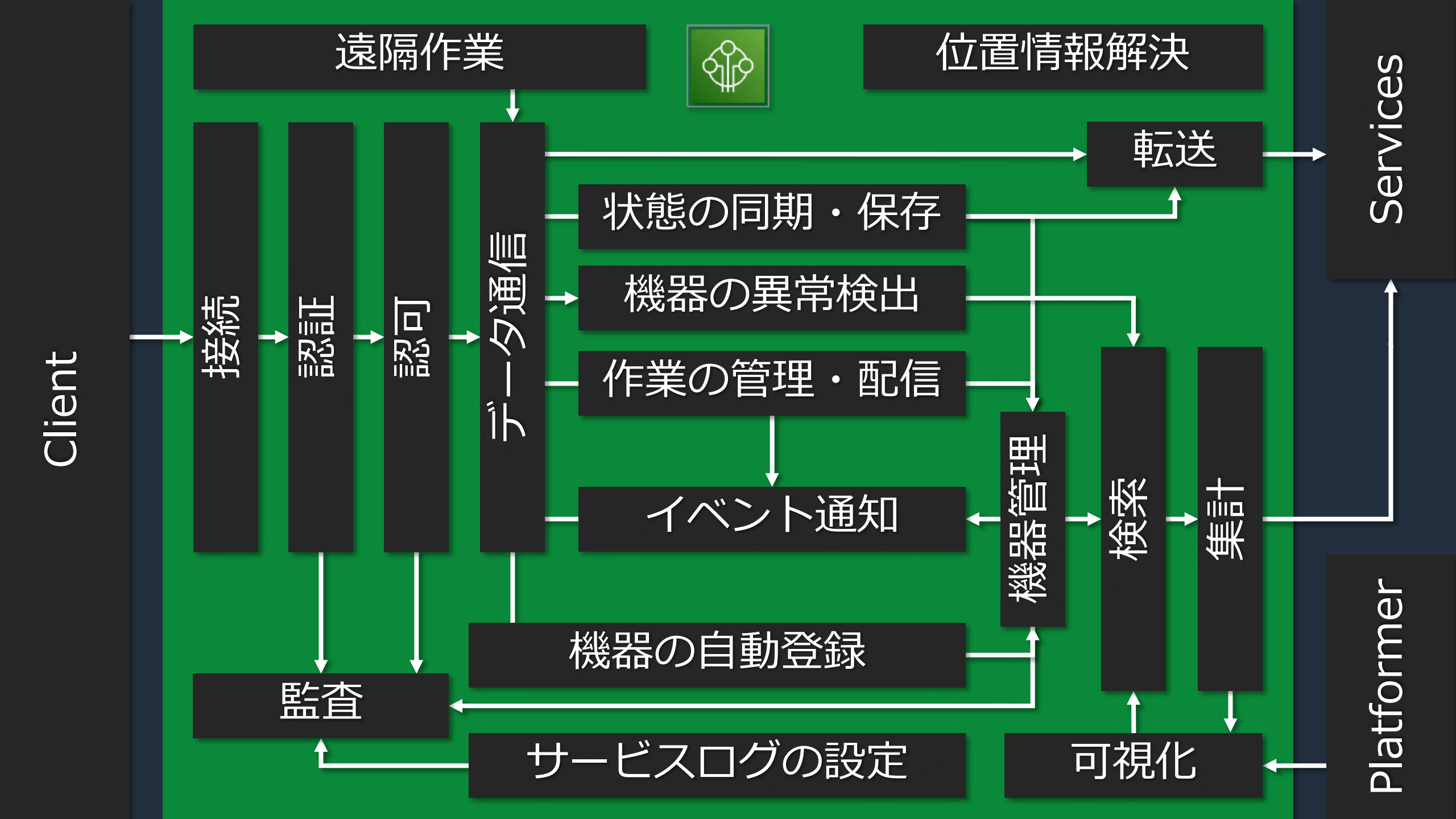
# 各視点別に見た AWS IoT の価値

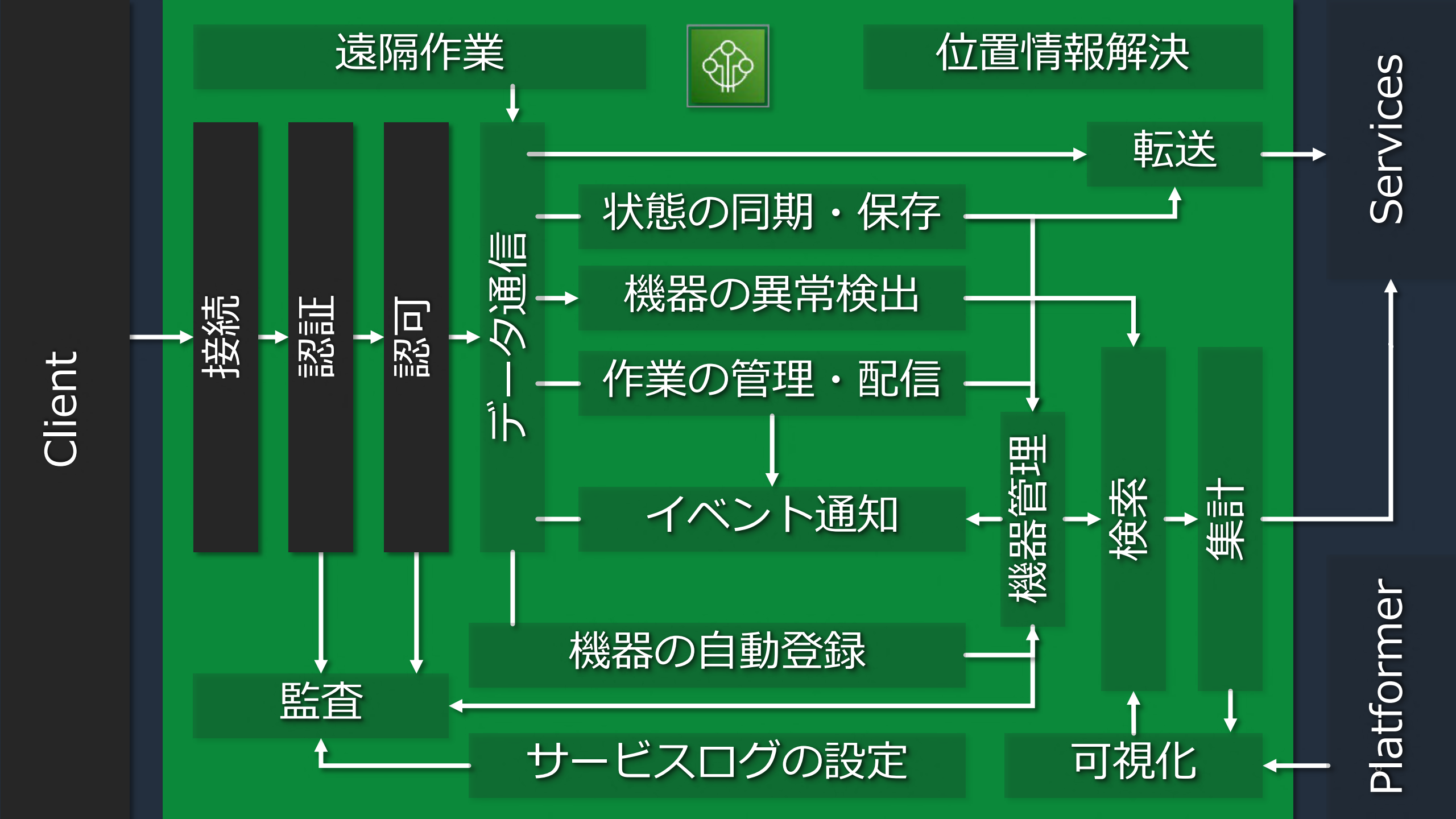
IoT Specialist Solutions Architect

飯塚 将太



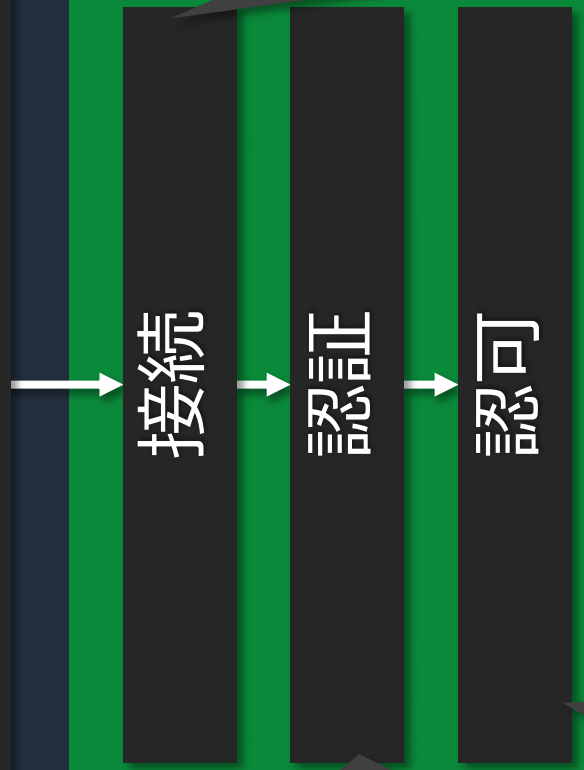

# 各視点別の AWS IoT の価値


Client
遠隔作業
位置情報解決
接続
認証
認可
データ通信
転送
状態の同期・保存
機器の異常検出
作業の管理・配信
イベント通知
機器管理
検索
集計
Services
Platformer
機器の自動登録
監査
サービスログの設定
可視化


遠隔作業
位置情報解決
Client
接続
認証
認可
データ通信
転送
状態の同期・保存
機器の異常検出
作業の管理・配信
イベント通知
機器管理
検索
集計
Services
Platformer
機器の自動登録
監査
サービスログの設定
可視化

どう**接続**したら良い？

Client




**今回のIoT要件**

AWS IoT

柔軟かつ厳密な**権限設定**はどうやる？

**安全**に接続するには？

# どう**接続**したら良い？

Client → 接続 → 認証 → 認可

AWS IoT

どう**接続**したら良い？

Client

Device Gateway

AWS IoT

# AWS IoT

## Device Gateway

**接続プロトコルは？**

AWS IoT

標準プロトコルのため**ロックインしない**

Device Gateway

MQTT over WebSocket

MQTT

HTTP

内部で相互変換

**双方向**通信
- Publish
- Subscribe

**送信**のみ
- Publish

接続対象や目的に
応じて**使い分け**

Device

AWS IoT

SDK不要で
**ロックインしない**

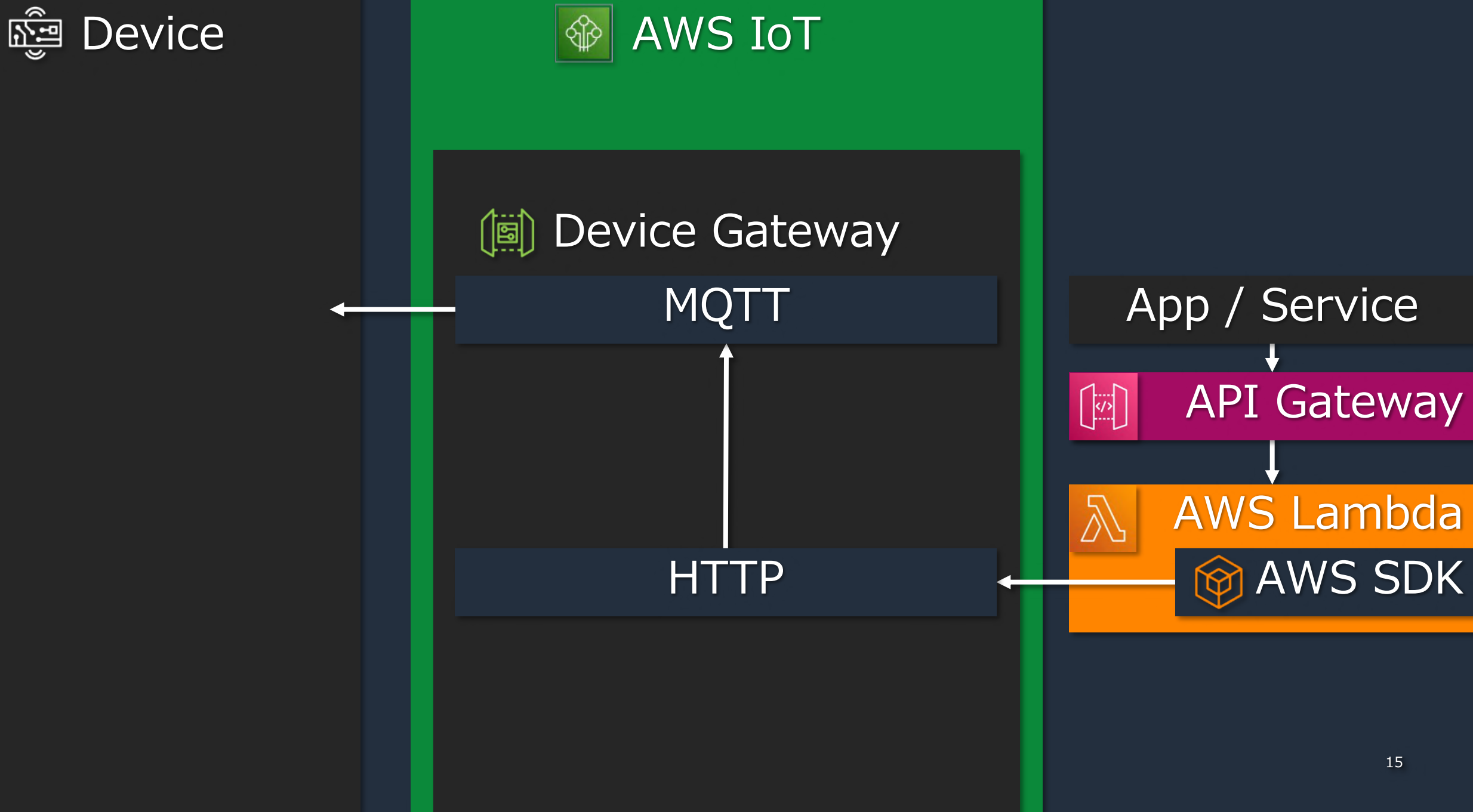
Device Gateway

MQTT Lib.

MQTT

or

AWS IoT
Device SDK


Device
AWS IoT
Device Gateway
MQTT
HTTP
App / Service
API Gateway
AWS Lambda
AWS SDK

Device

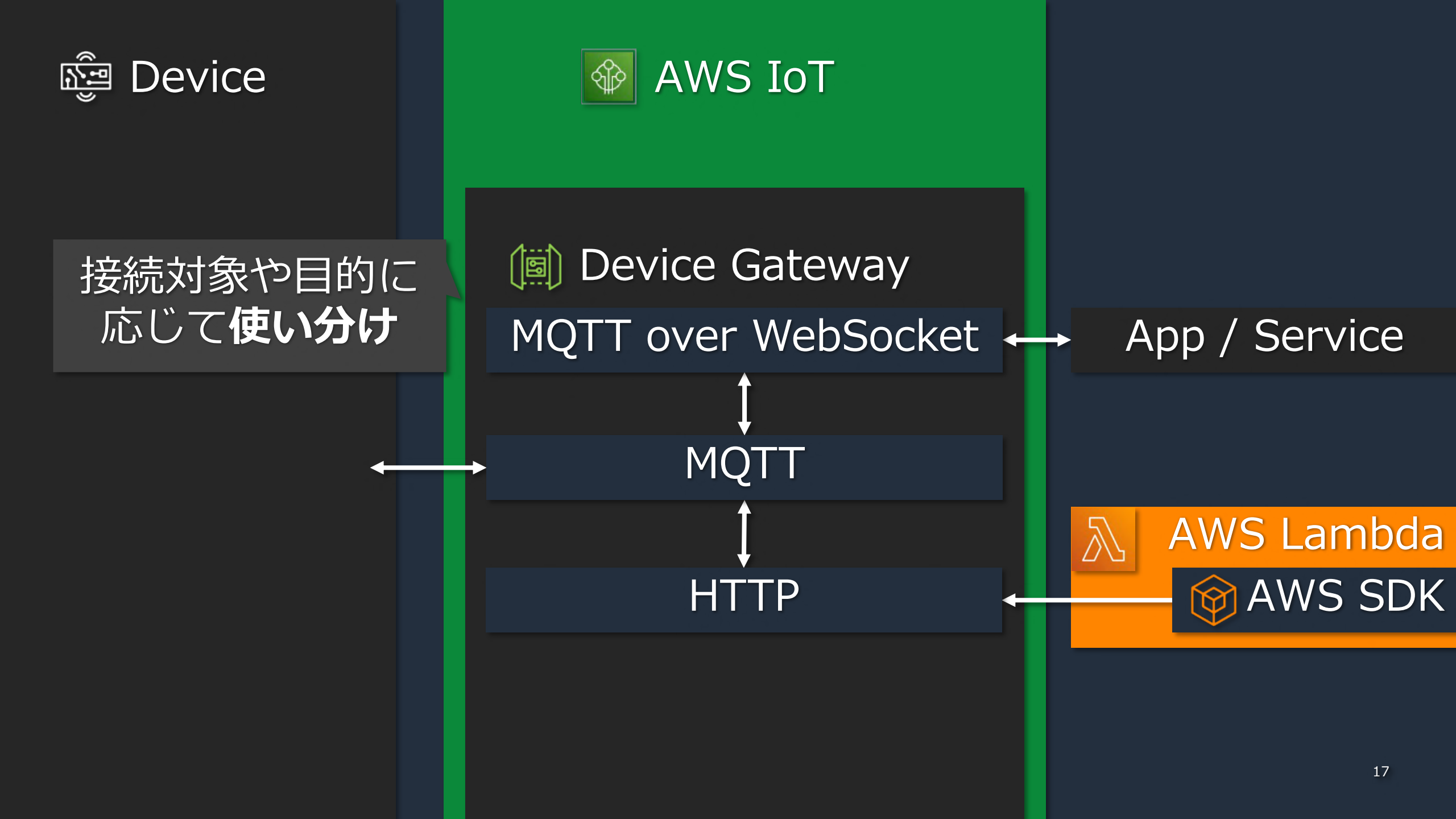
AWS IoT

Device Gateway

MQTT over WebSocket

App / Service

MQTT


Device
AWS IoT
接続対象や目的に
応じて**使い分け**
Device Gateway
MQTT over WebSocket
App / Service
MQTT
HTTP
AWS Lambda
AWS SDK

# AWS IoT

## Device Gateway

接続は全て
**TLS**

経路が**暗号化**

設定可能な TLS ver.

1.3 のみ
1.2 – 1.3
1.2 のみ
1.0 – 1.2

# 高いスケーラビリティ
# **数百万**接続可能

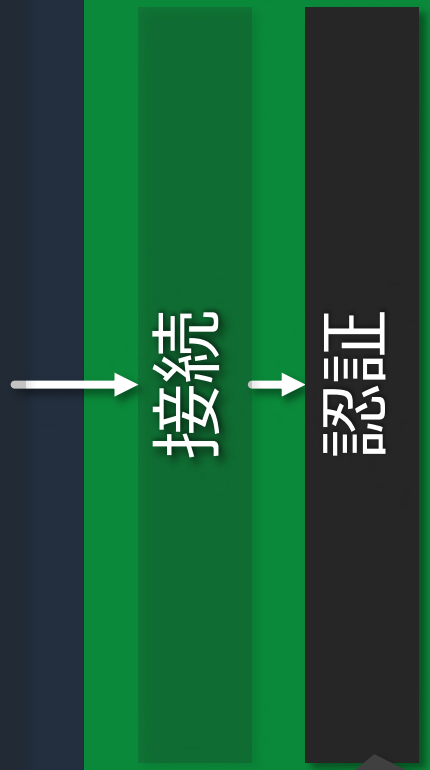
どう**接続**したら良い？

Client

Device Gateway

AWS IoT

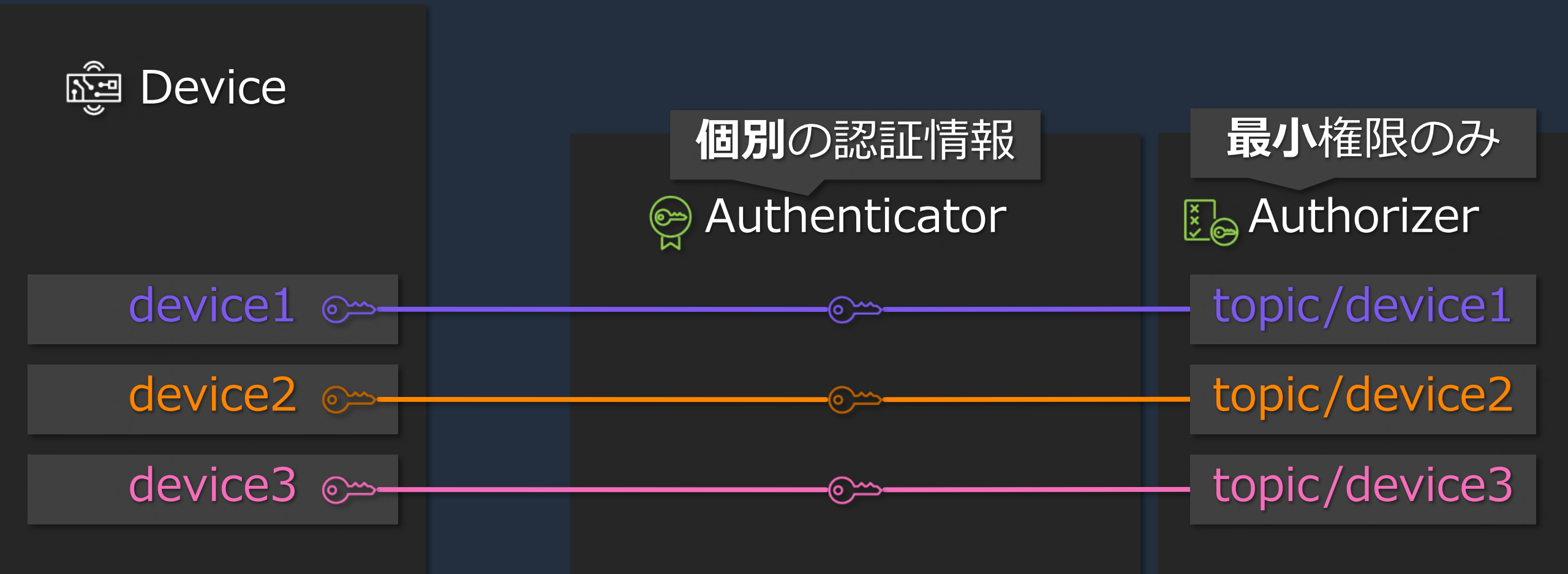
Client

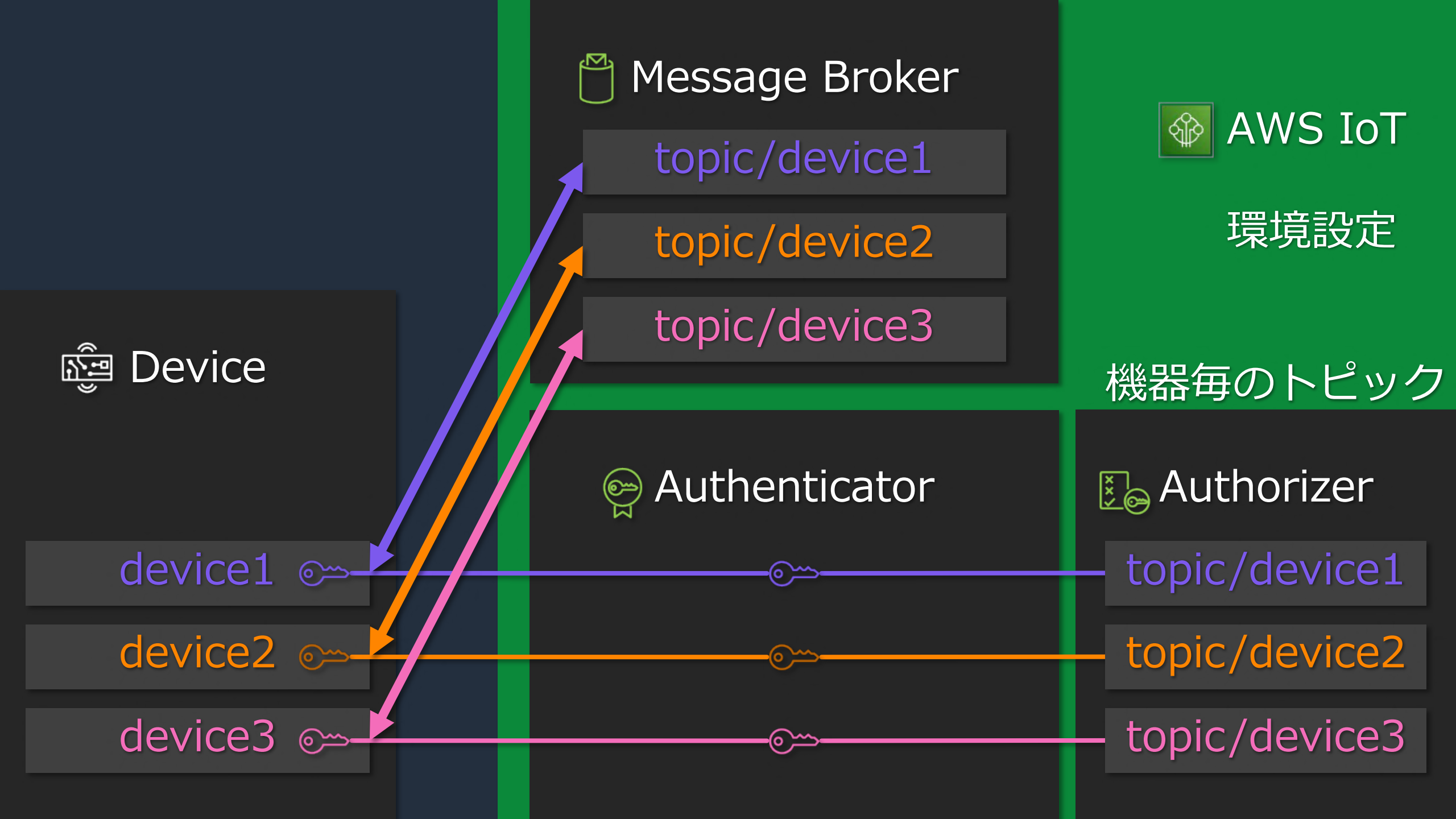


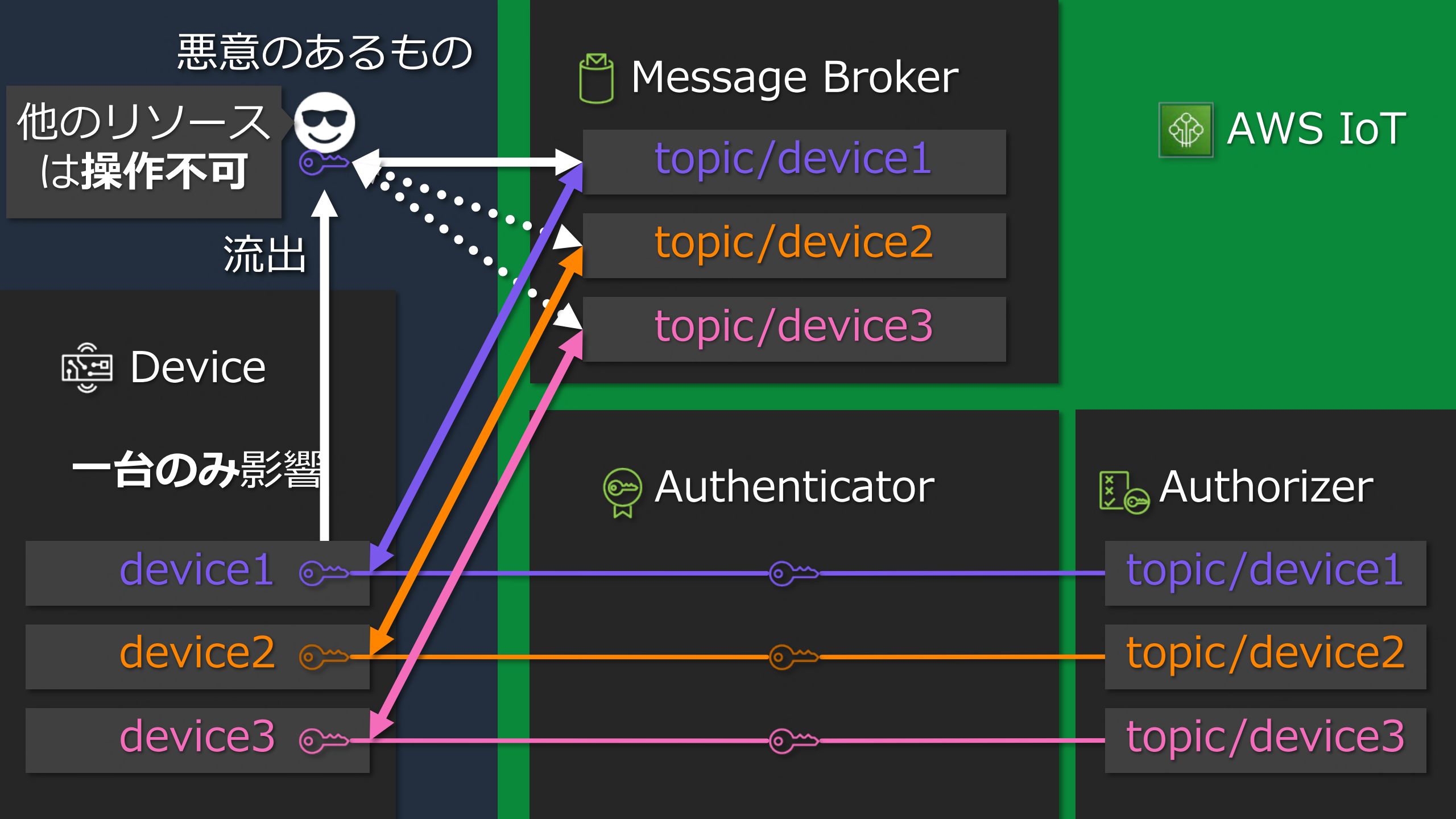

AWS IoT

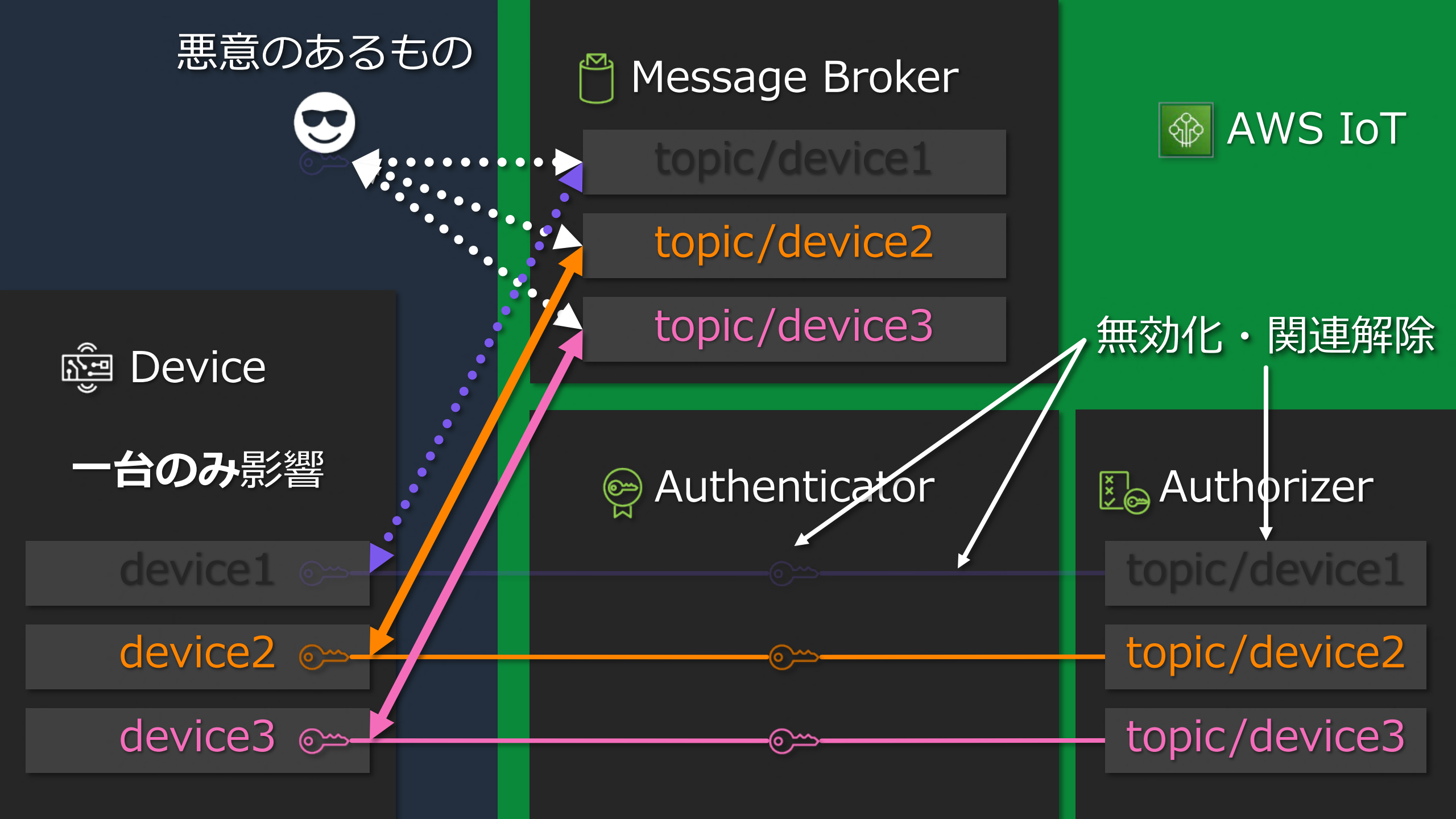
**安全**に接続するには？

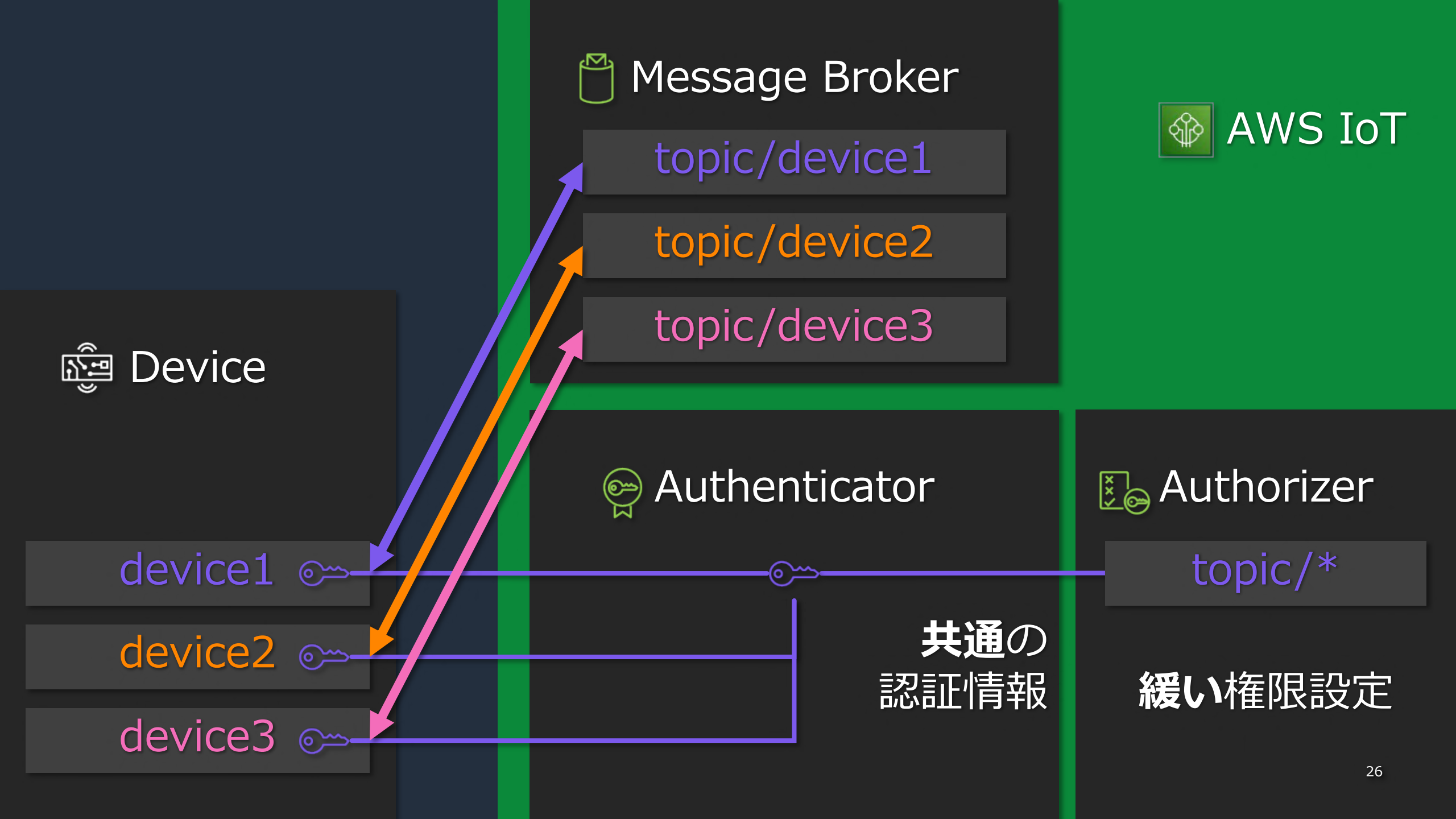
# IoT 機器の認証・認可の**ベストプラクティス**

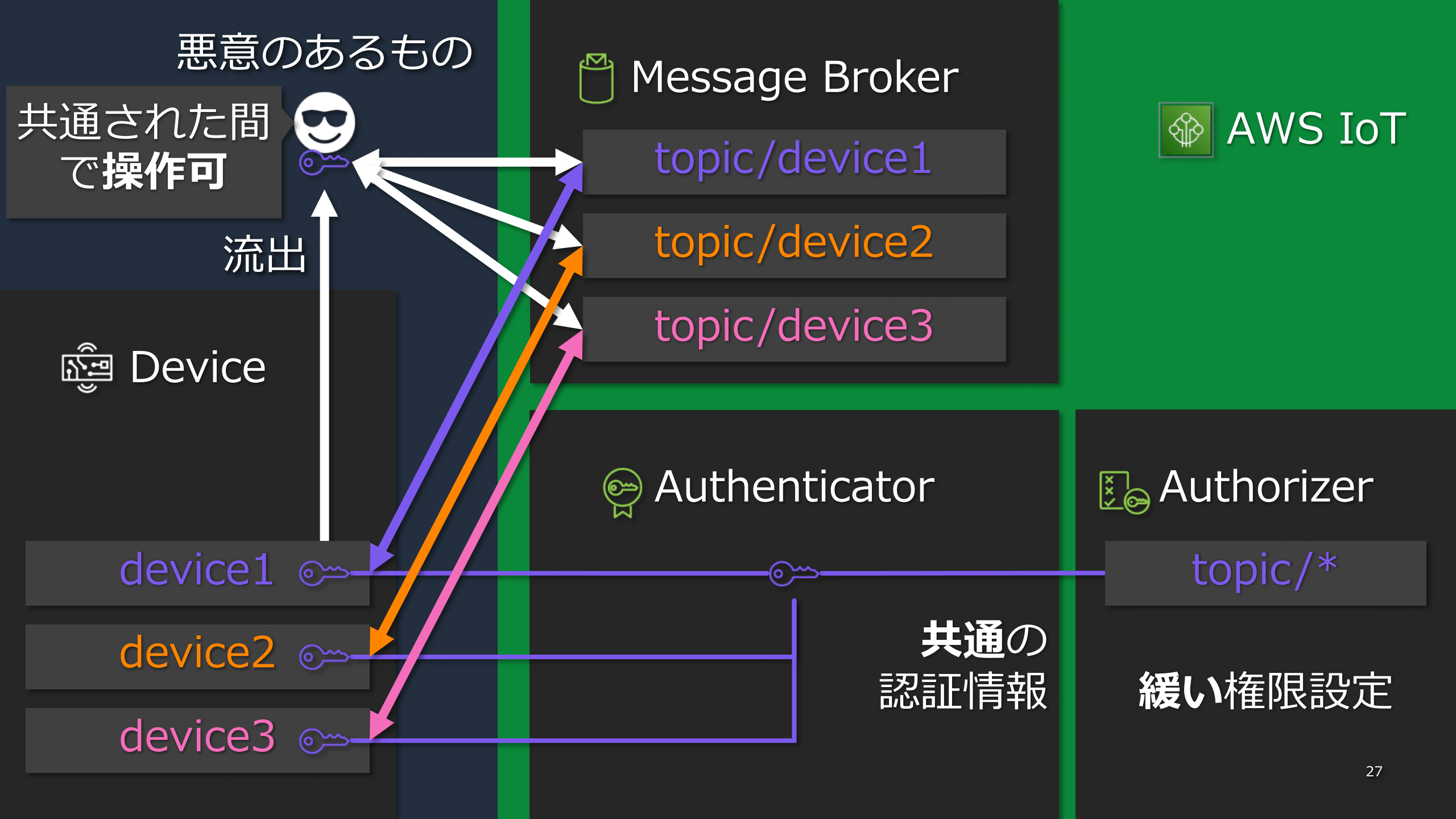


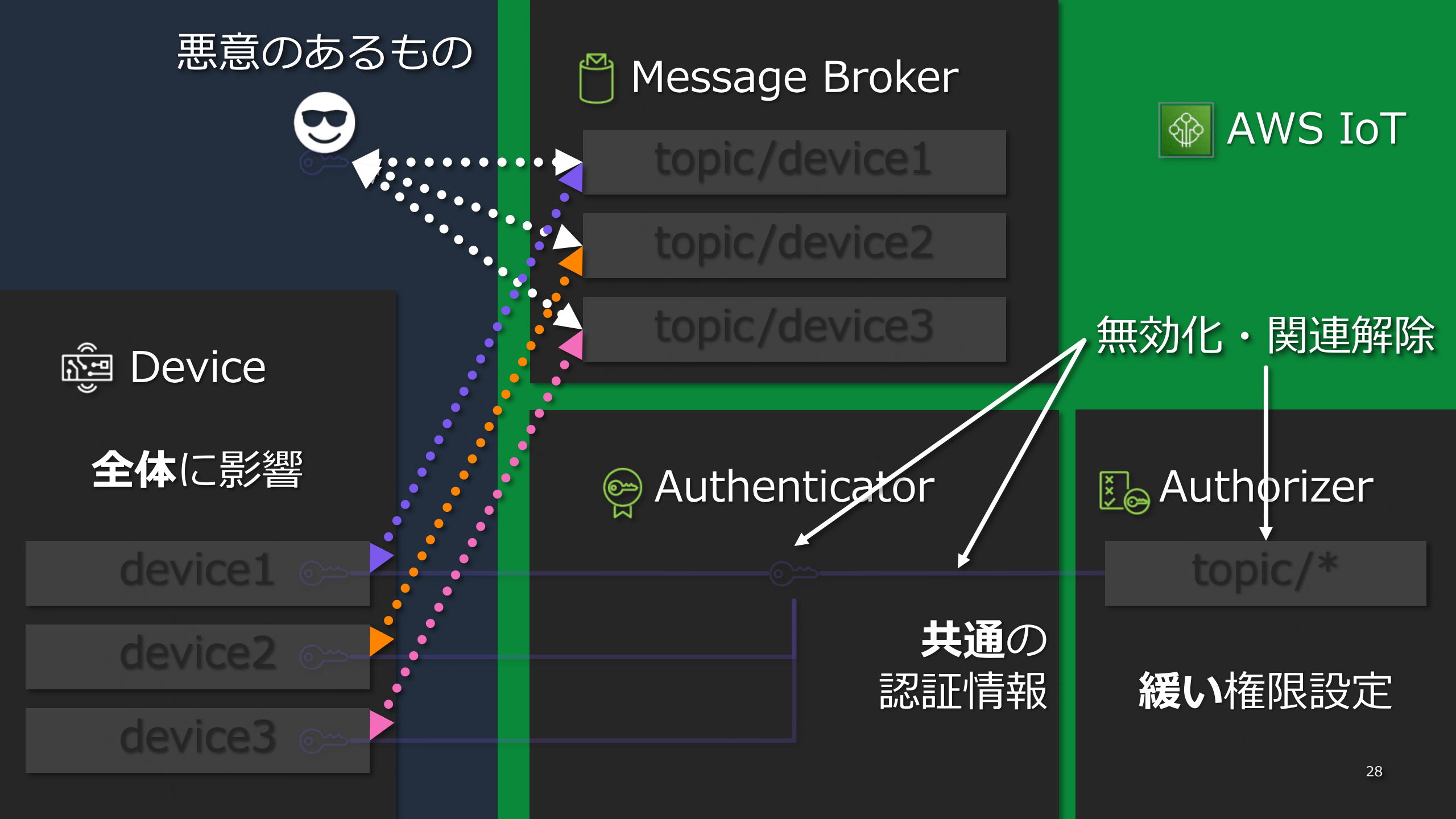

Message Broker
topic/device1
topic/device2
topic/device3
AWS IoT
環境設定
Device
機器毎のトピック
Authenticator
Authorizer
device1
device2
device3
topic/device1
topic/device2
topic/device3


悪意のあるもの
他のリソースは**操作不可**
流出
Device
**一台のみ**影響
Message Broker
topic/device1
topic/device2
topic/device3
AWS IoT
Authenticator
Authorizer
device1
device2
device3
topic/device1
topic/device2
topic/device3


悪意のあるもの
Message Broker
AWS IoT
topic/device1
topic/device2
topic/device3
無効化・関連解除
Device
一台のみ影響
Authenticator
Authorizer
device1
device2
device3
topic/device1
topic/device2
topic/device3


Message Broker
topic/device1
topic/device2
topic/device3
AWS IoT
Device
Authenticator
Authorizer
device1
device2
device3
topic/*
共通の
認証情報
緩い権限設定


悪意のあるもの
共通された間で**操作可**
流出
Device
Message Broker
topic/device1
topic/device2
topic/device3
AWS IoT
Authenticator
Authorizer
device1
device2
device3
topic/*
**共通**の
認証情報
**緩い**権限設定


悪意のあるもの
Message Broker
AWS IoT
topic/device1
topic/device2
topic/device3
無効化・関連解除
Device
全体に影響
Authenticator
Authorizer
device1
device2
device3
topic/*
共通の
認証情報
緩い権限設定

# AWS IoT で使用可能な認証方法 4 つ

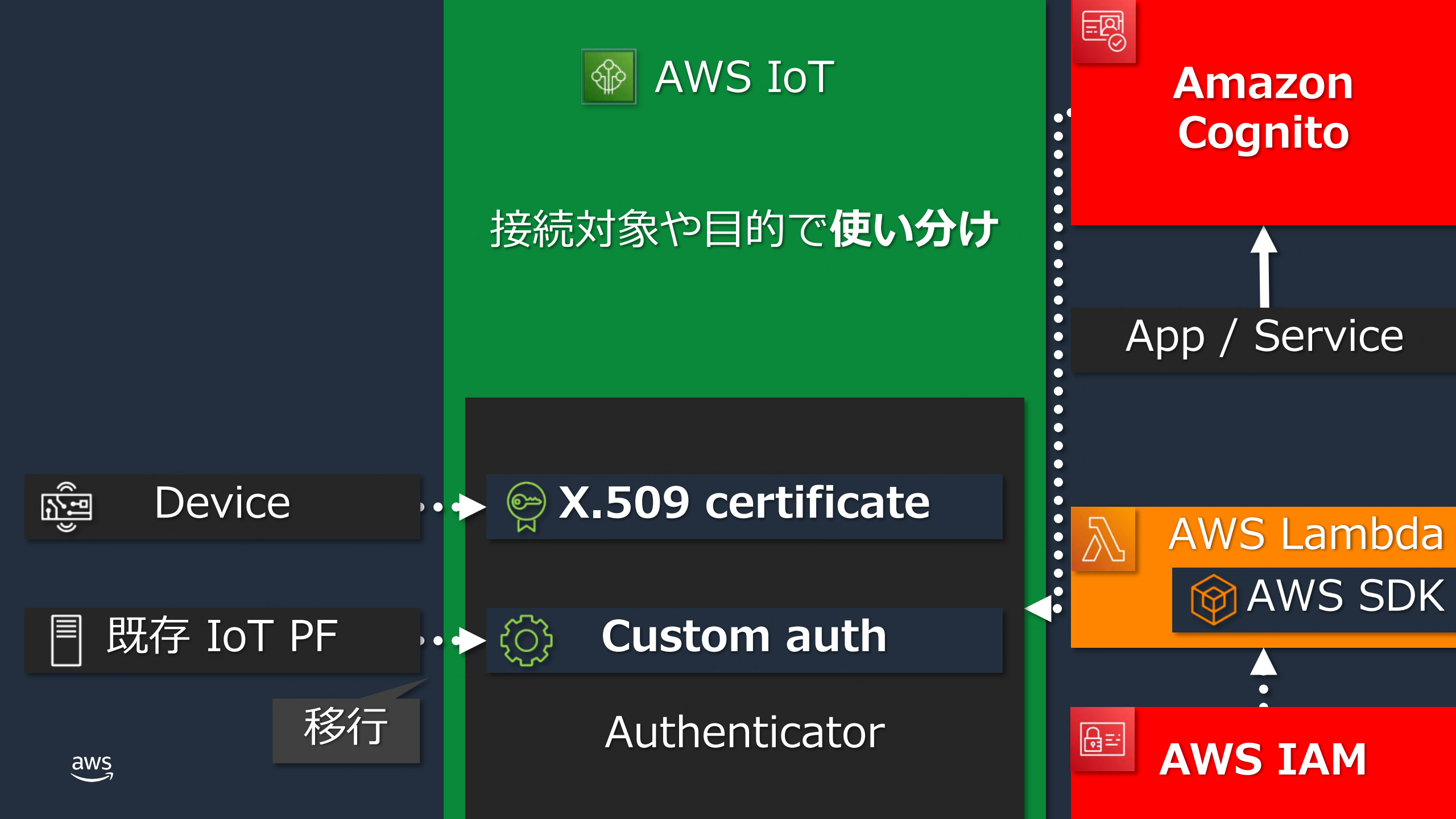
**X.509 certificate**

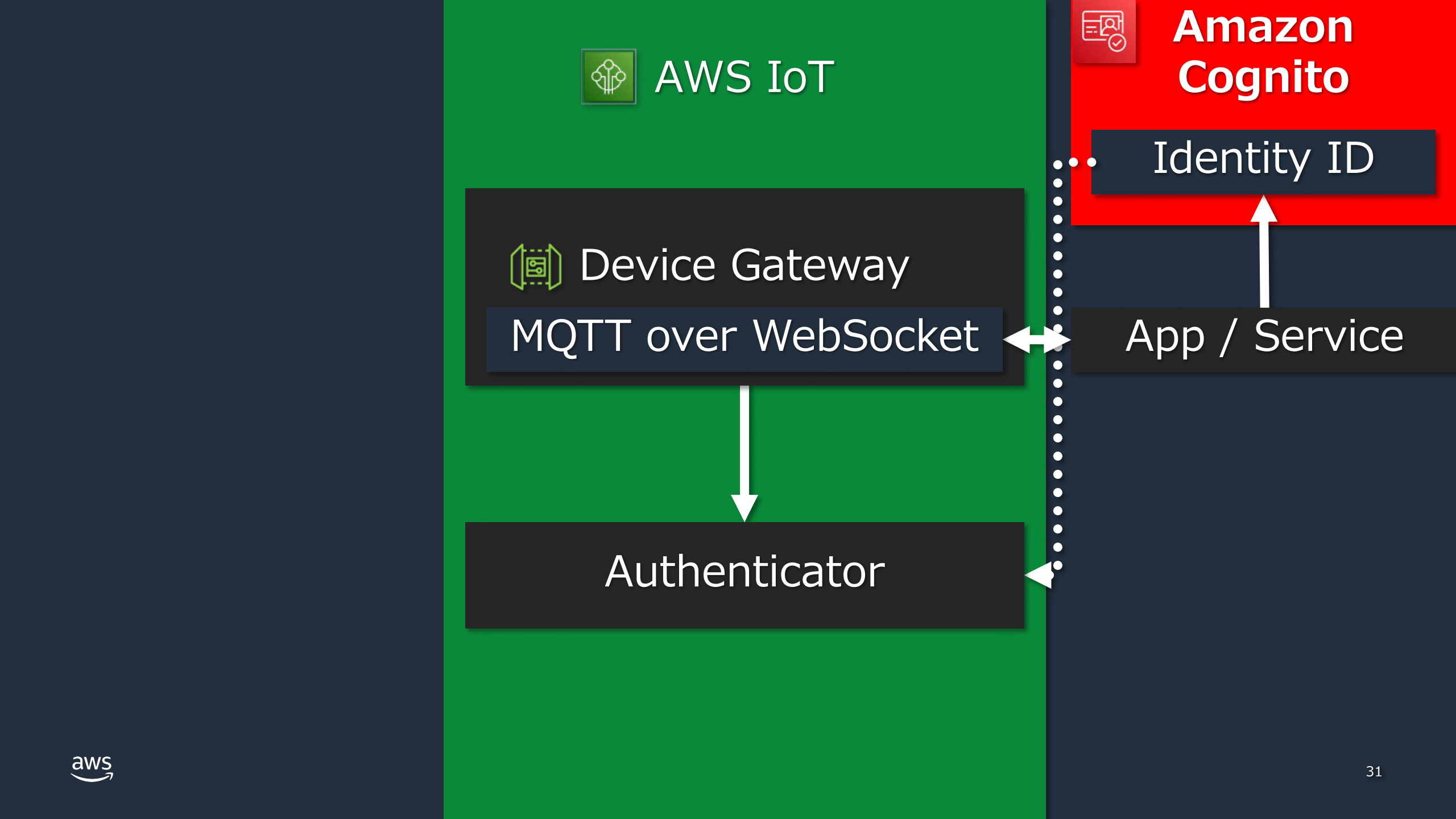
**Custom auth**

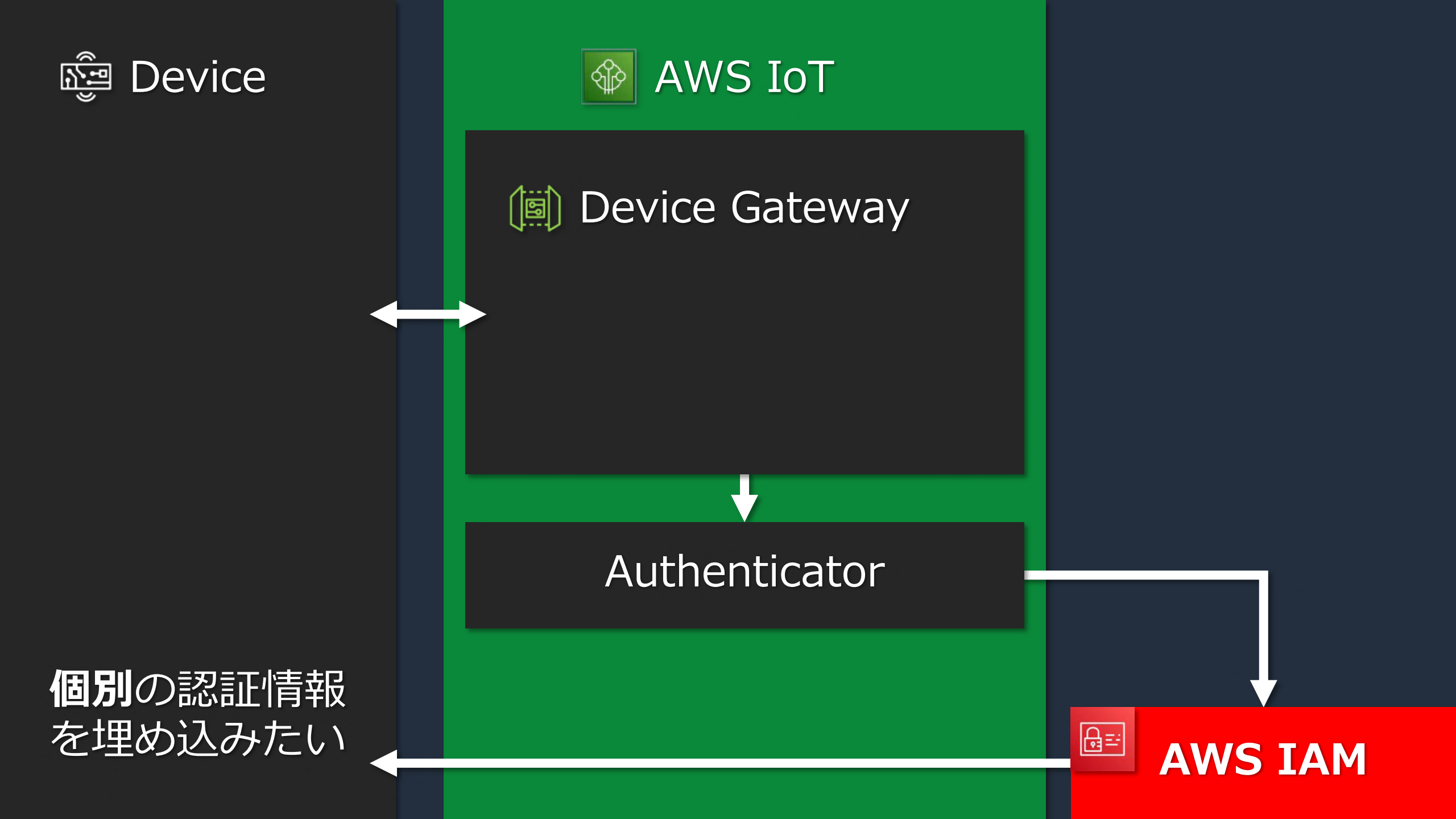
Authenticator

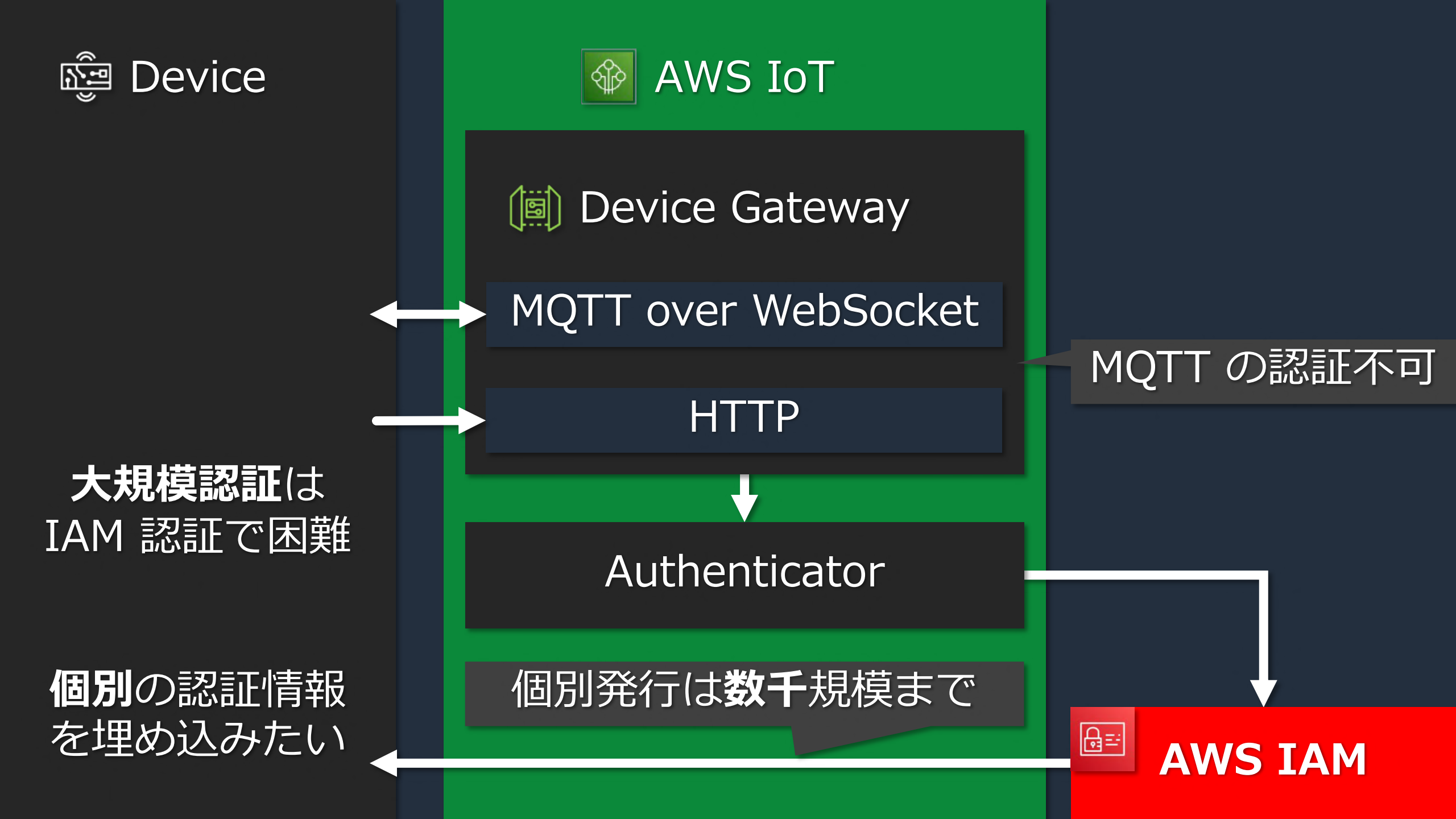
**Amazon Cognito**

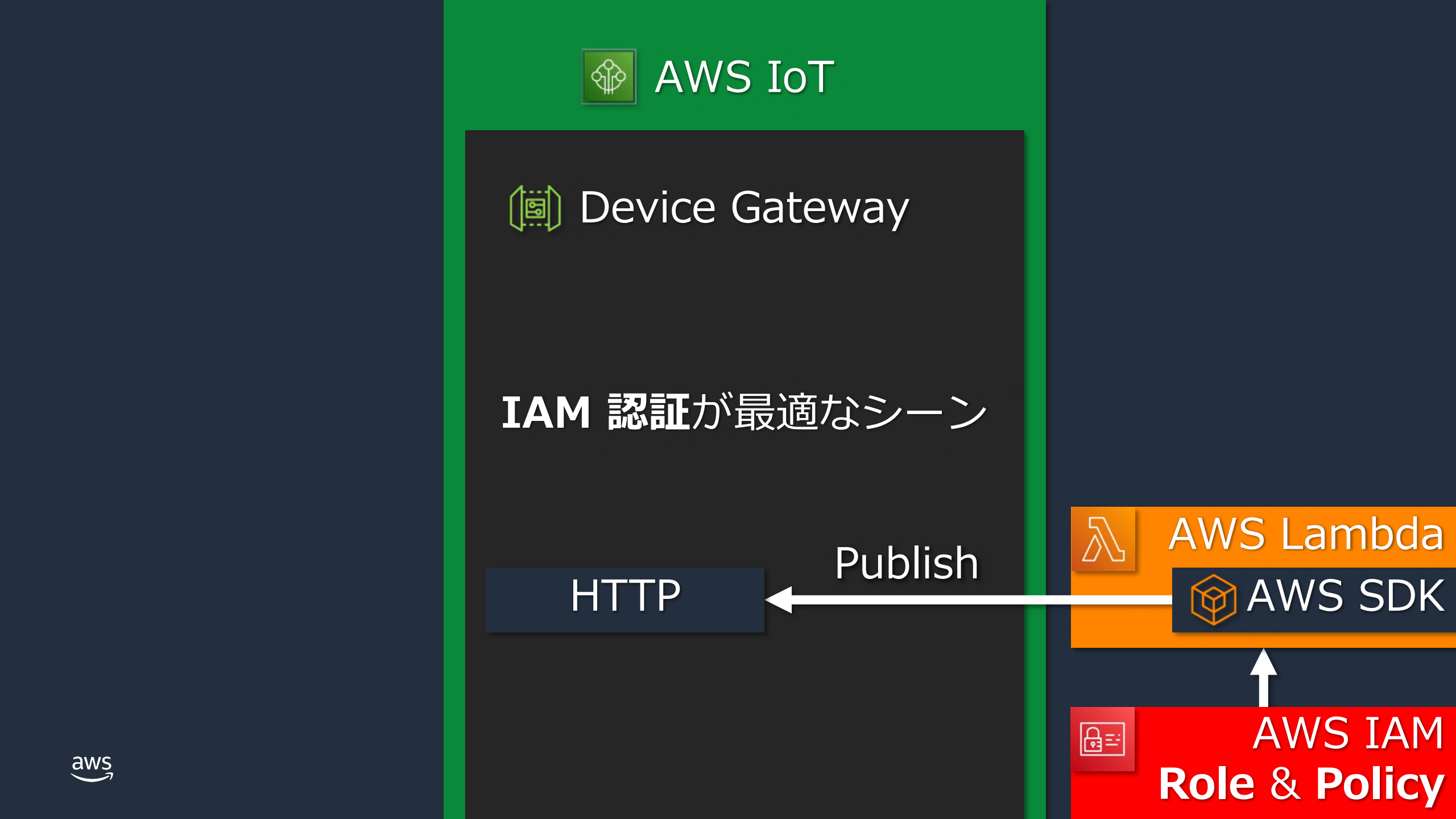
**AWS IAM**


AWS IoT
接続対象や目的で使い分け
Amazon Cognito
App / Service
Device
X.509 certificate
AWS Lambda
AWS SDK
既存 IoT PF
Custom auth
移行
Authenticator
AWS IAM


AWS IoT
Amazon Cognito
Identity ID
Device Gateway
MQTT over WebSocket
App / Service
Authenticator


Device
AWS IoT
Device Gateway
Authenticator
AWS IAM
**個別**の認証情報
を埋め込みたい


Device
AWS IoT
Device Gateway
MQTT over WebSocket
HTTP
MQTT の認証不可
Authenticator
大規模認証は
IAM 認証で困難
個別発行は数千規模まで
個別の認証情報
を埋め込みたい
AWS IAM


AWS IoT
Device Gateway
IAM 認証が最適なシーン
HTTP
Publish
AWS Lambda
AWS SDK
AWS IAM
Role & Policy

AWS IoT

Device Gateway

MQTT

AWS Lambda

```
import AWS IoT Device SDK
connection = Connection(
    client_id = thing_name,
    ca_cert =
    client_cert =
    private_key =
)
connection.connect()
connection.publish(topic, message)
connection.disconnect()
```

要インストール

CA cert.

Client cert.

Private key

要腹持ち

AWS IoT

AWS Lambda

import AWS SDK

インストール不要

```
client = aws_sdk.client('iot-data’)
client.publish(topic, message)
```

セッション不要

Device Gateway

HTTP

Role

AWS IAM

Policy

Connect
Publish

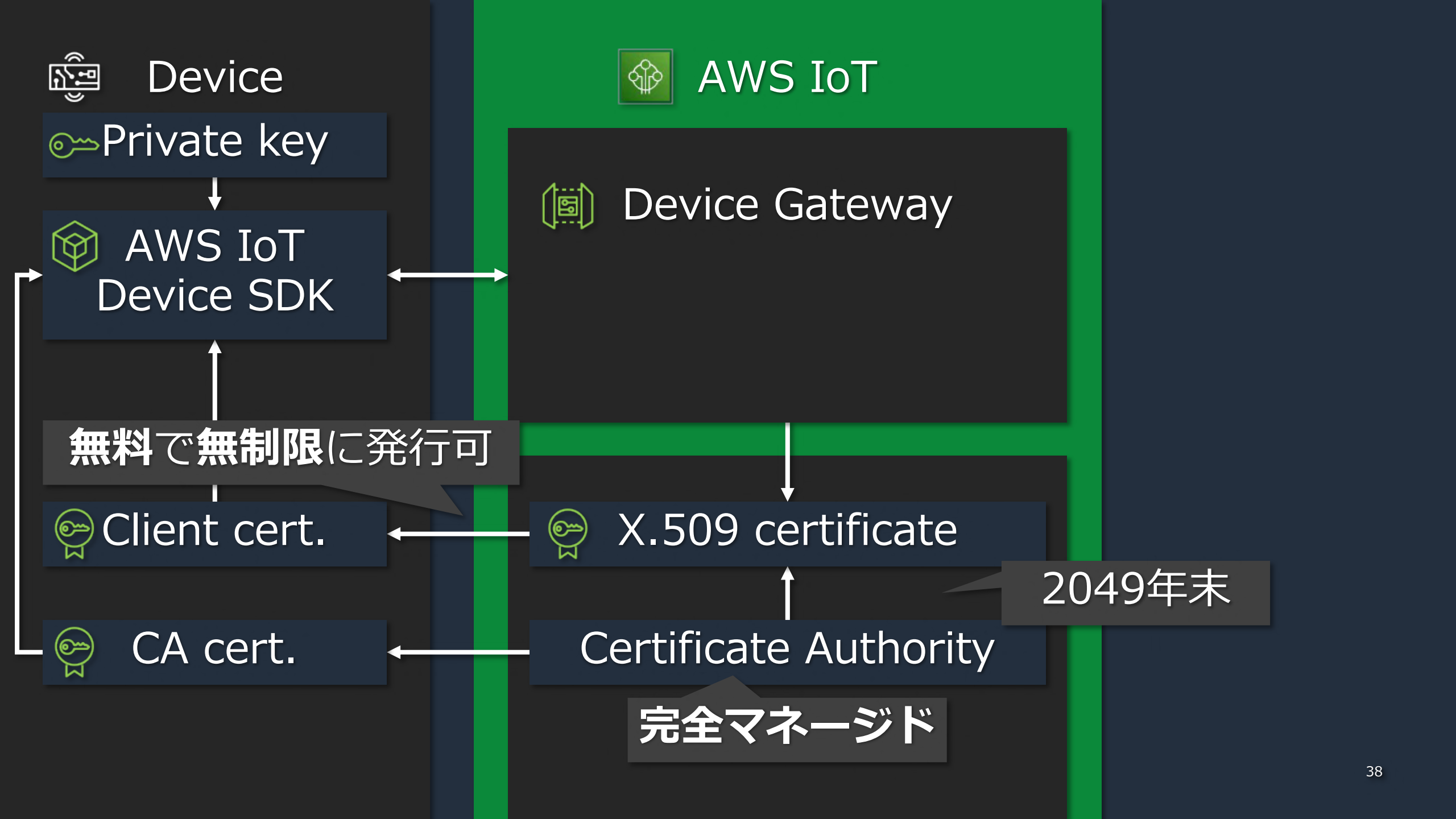
Device
認証の最適解

AWS IoT

Device Gateway



Authenticator


Device
Private key
AWS IoT
Device SDK
AWS IoT
Device Gateway
無料で無制限に発行可
Client cert.
X.509 certificate
2049年末
CA cert.
Certificate Authority
完全マネージド

Device

AWS IoT

**証明書期限を設定したい場合**

Client cert.

CA cert.

X.509 certificate

Certificate Authority

Authenticator

**発行**可

**登録**して
利用可

**3rd Party Certificate Authority**

AWS IoT

**要件に合わせて**
**2 種類の認証局を利用可**

**Certificate Authority**

Authenticator

**登録**して
利用可

**3rd Party Certificate Authority**

Device

Private key

AWS IoT
Device SDK

Client cert.

CA cert.

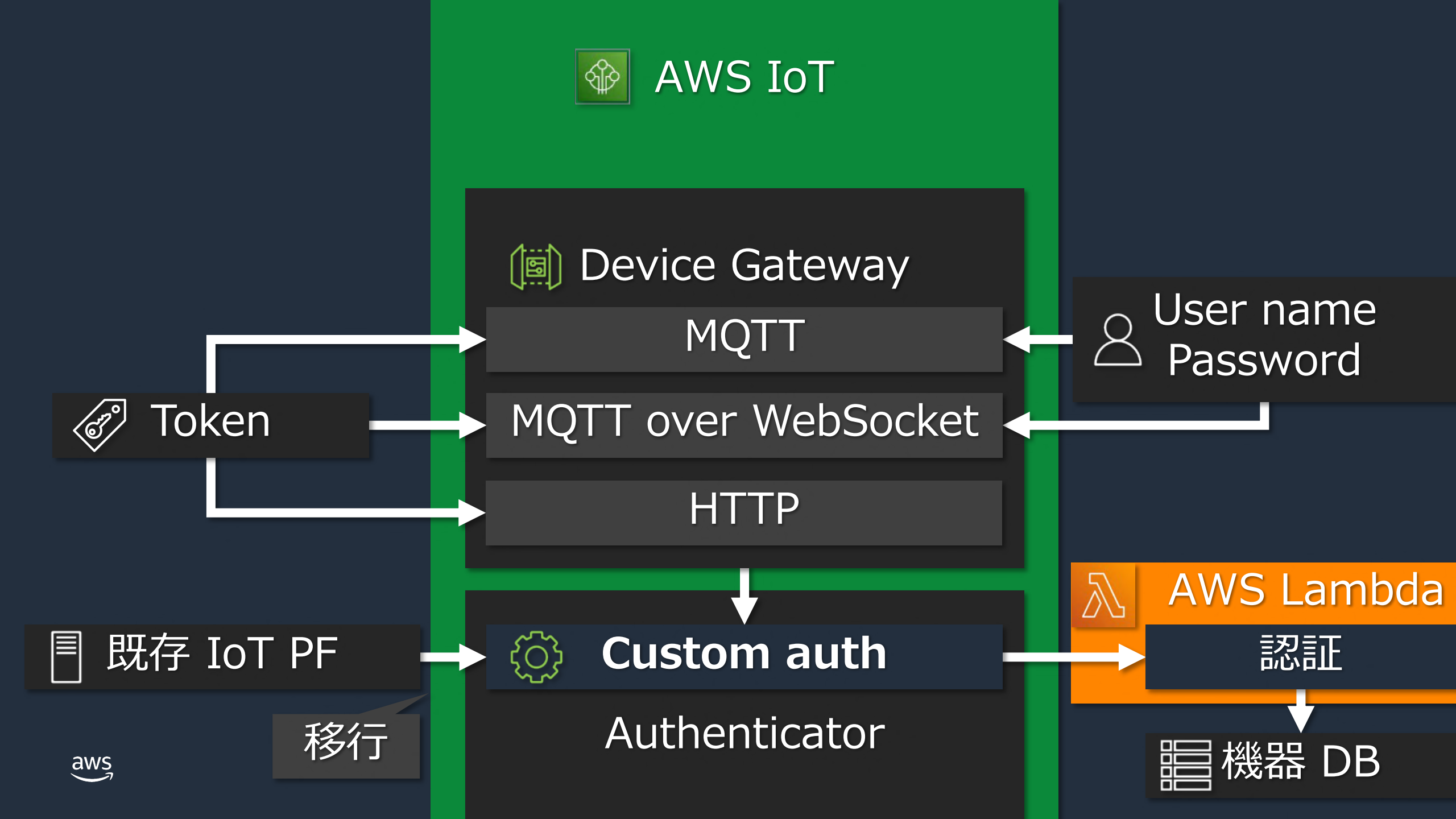
AWS IoT

Device Gateway

MQTT

HTTP

証明書認証では
WebSocket 利用**不可**


AWS IoT
Device Gateway
MQTT
MQTT over WebSocket
HTTP
Token
User name
Password
既存 IoT PF
Custom auth
Authenticator
移行
AWS Lambda
認証
機器 DB
aws

AWS IoT

接続対象や目的で**使い分け**

Amazon Cognito

App / Service

Device

**X.509 certificate**

既存 IoT PF

**Custom auth**

移行

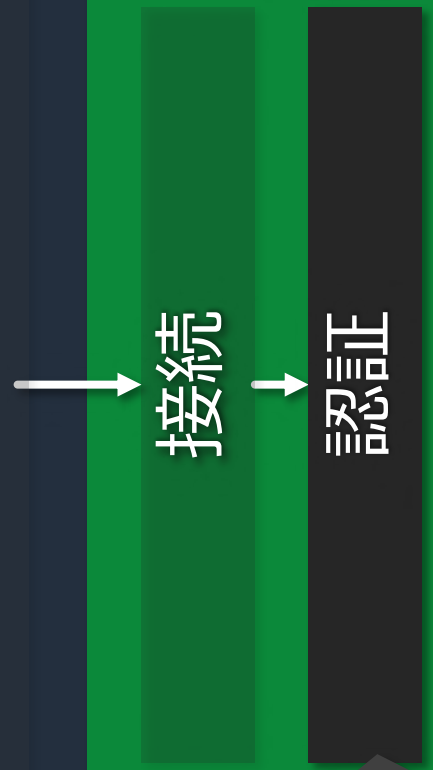
Authenticator

AWS Lambda

AWS SDK

**AWS IAM**

Client



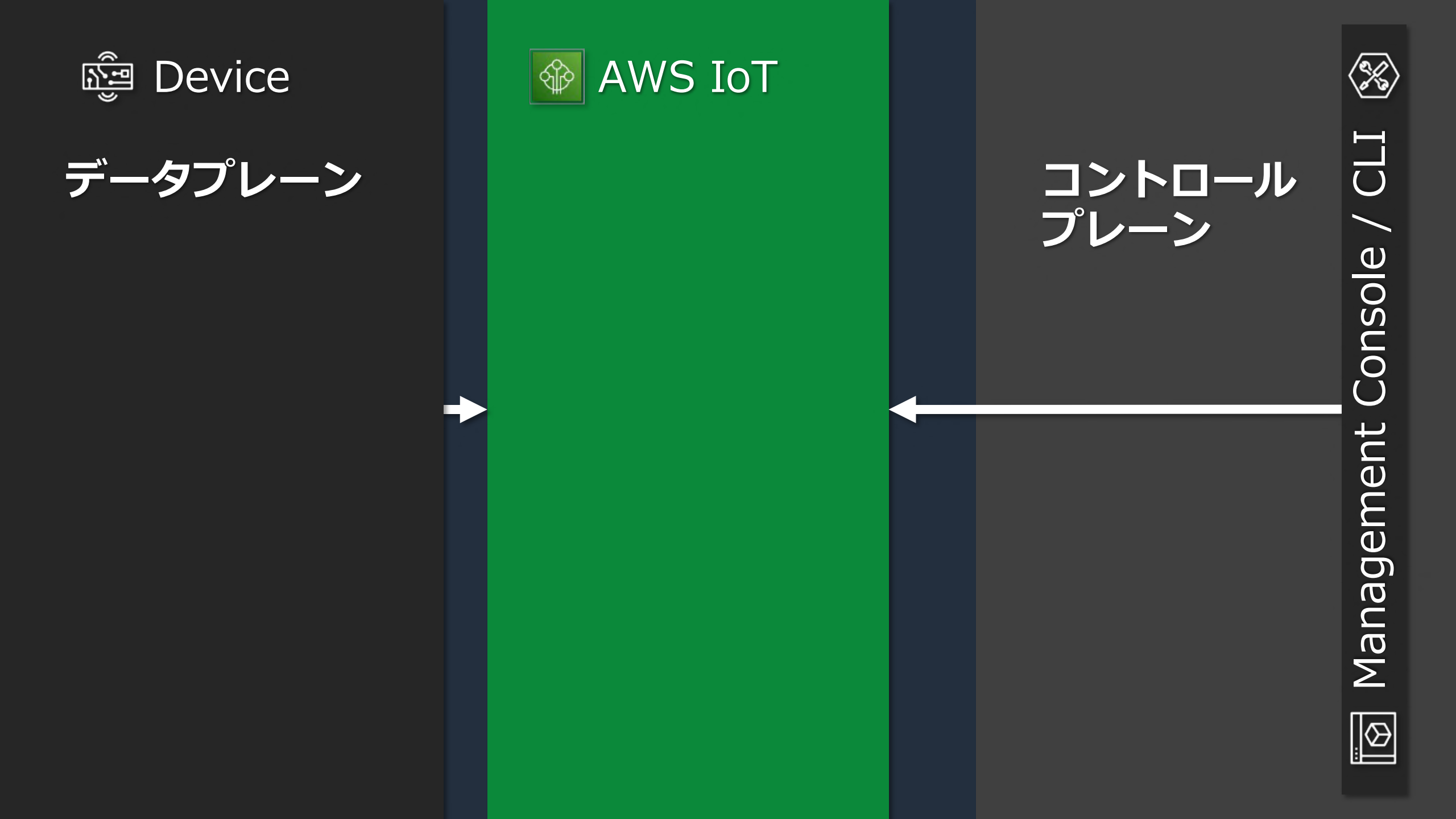

AWS IoT

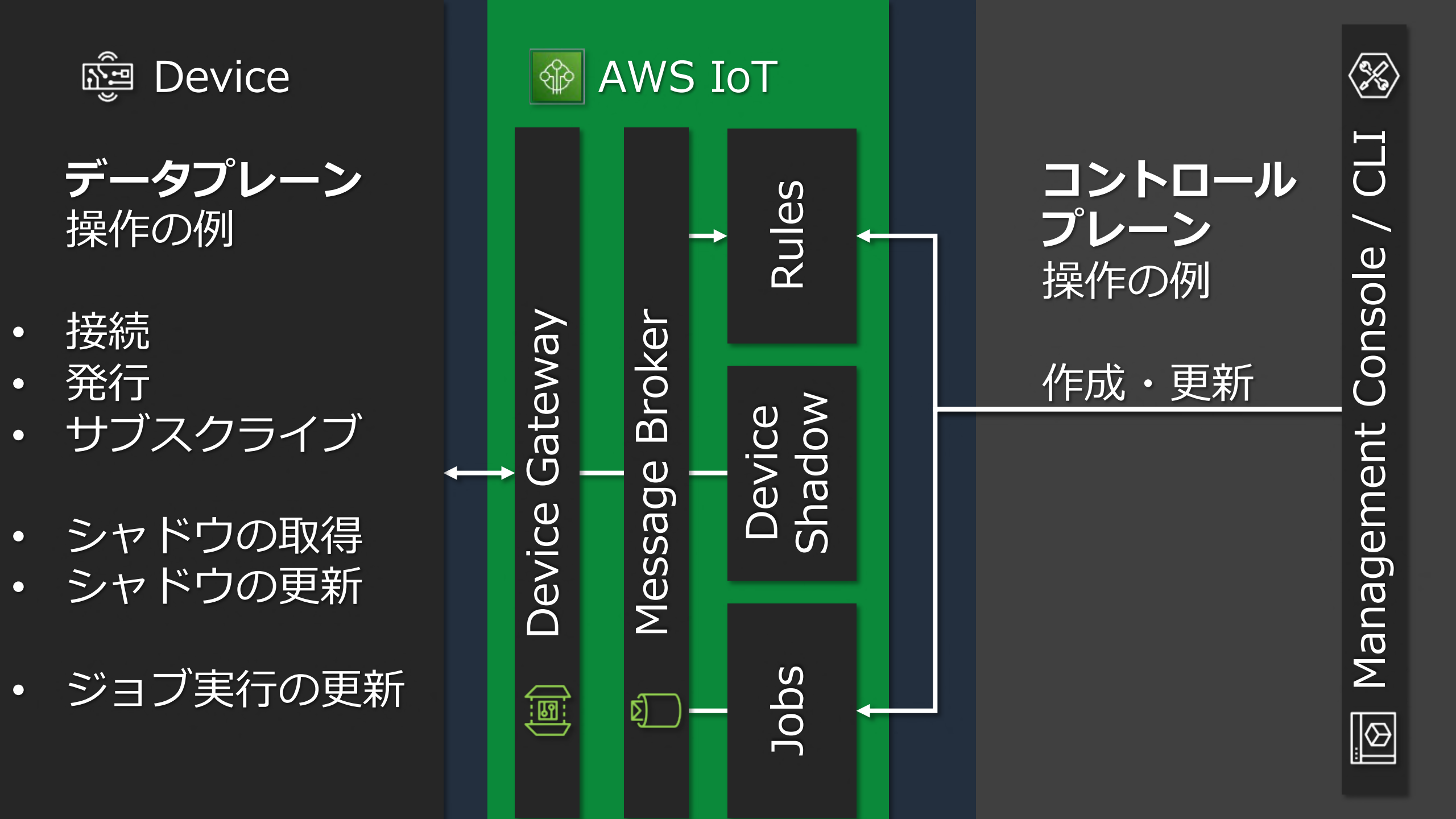
**安全**に接続するには？

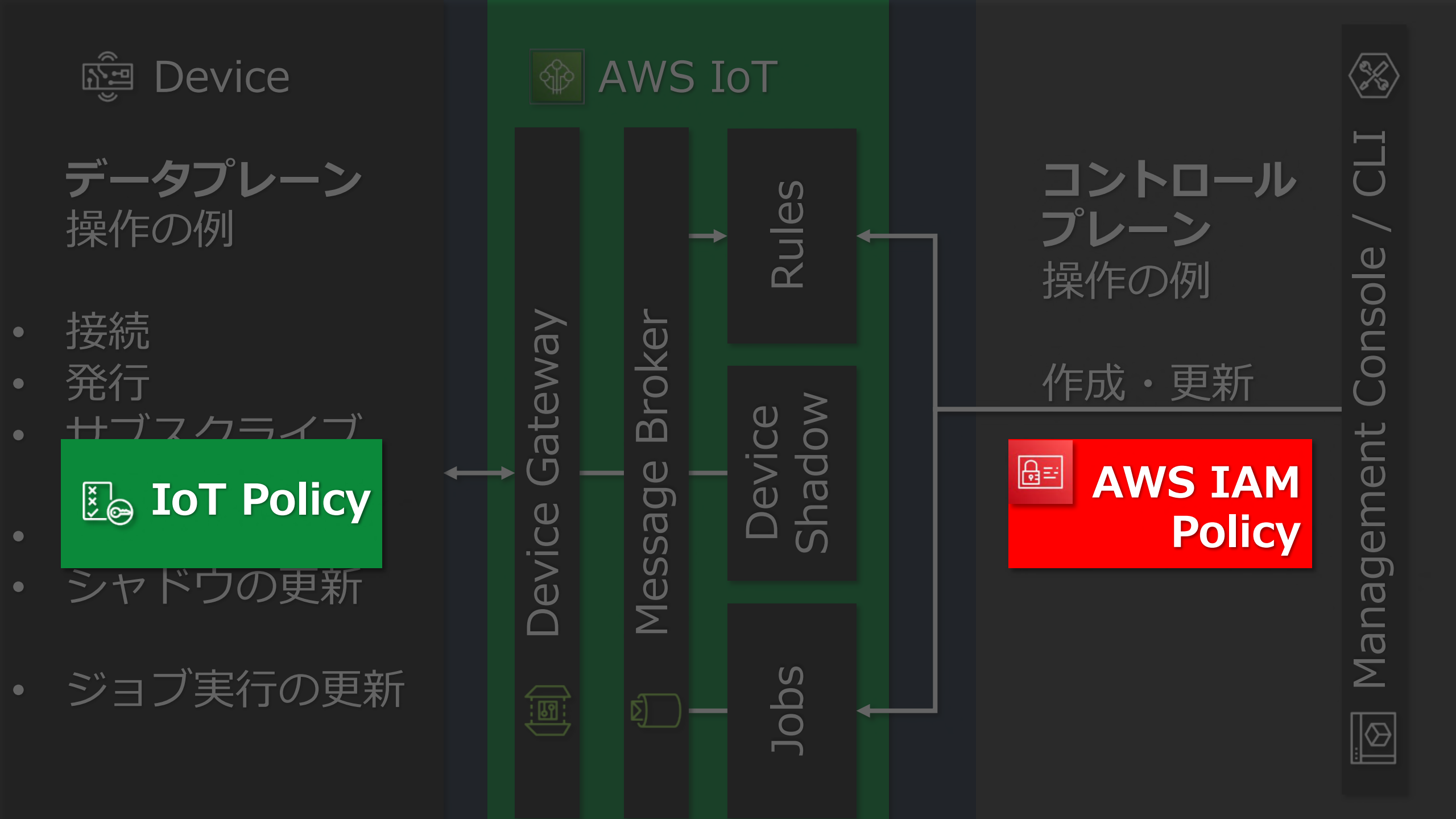
認証 → 認可

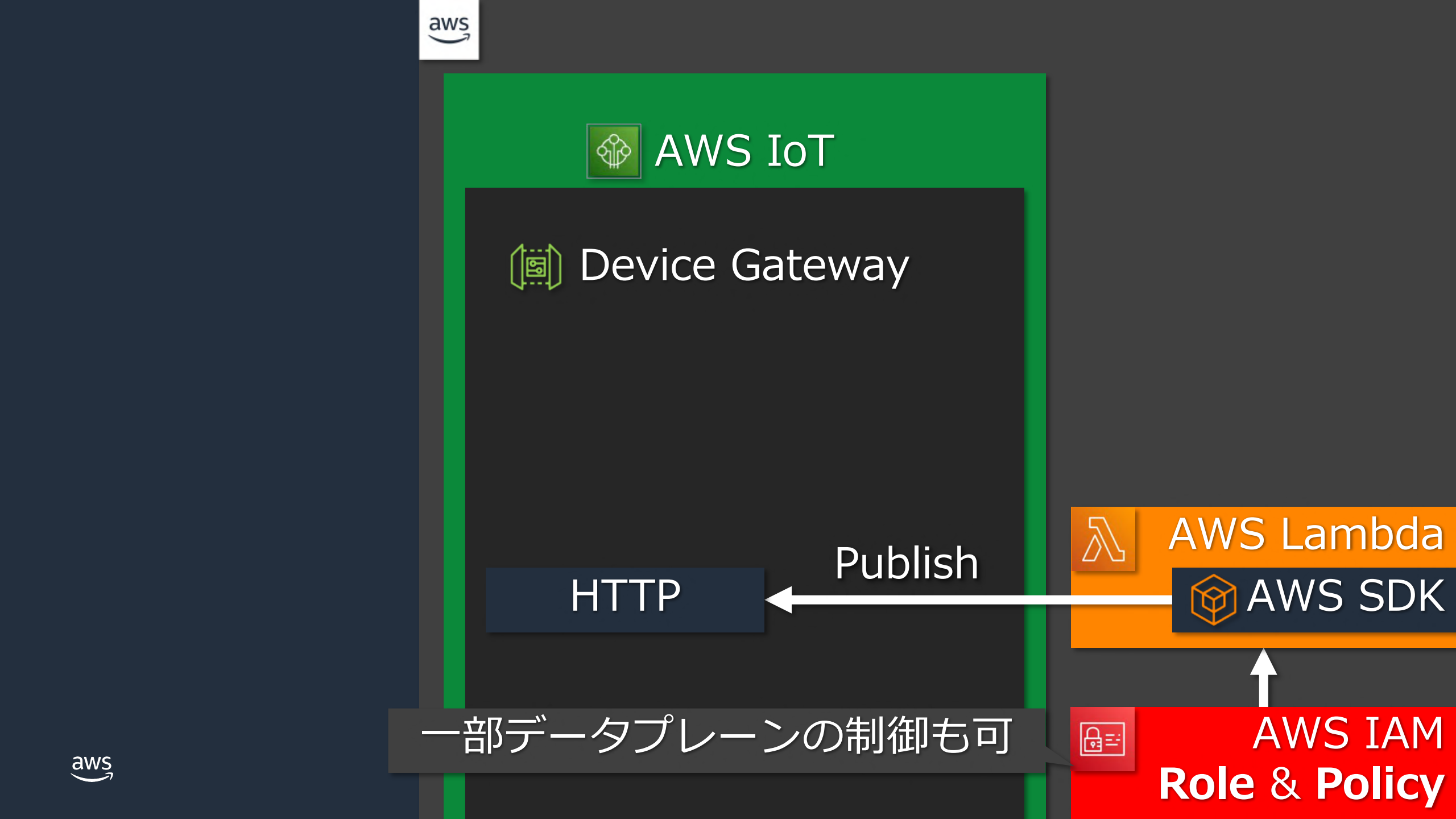
AWS IoT

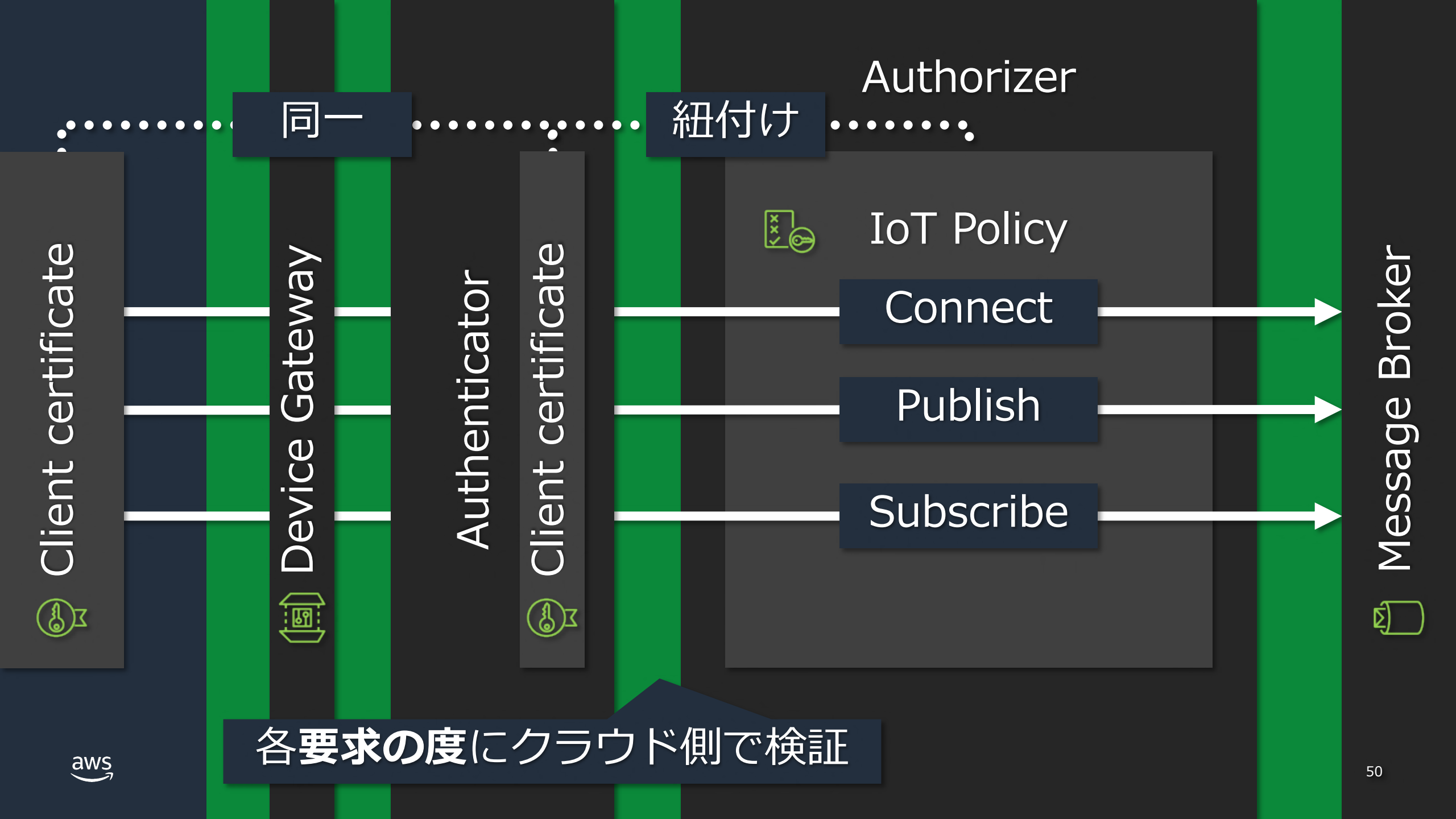
柔軟かつ厳密な**権限設定**はどうやる？

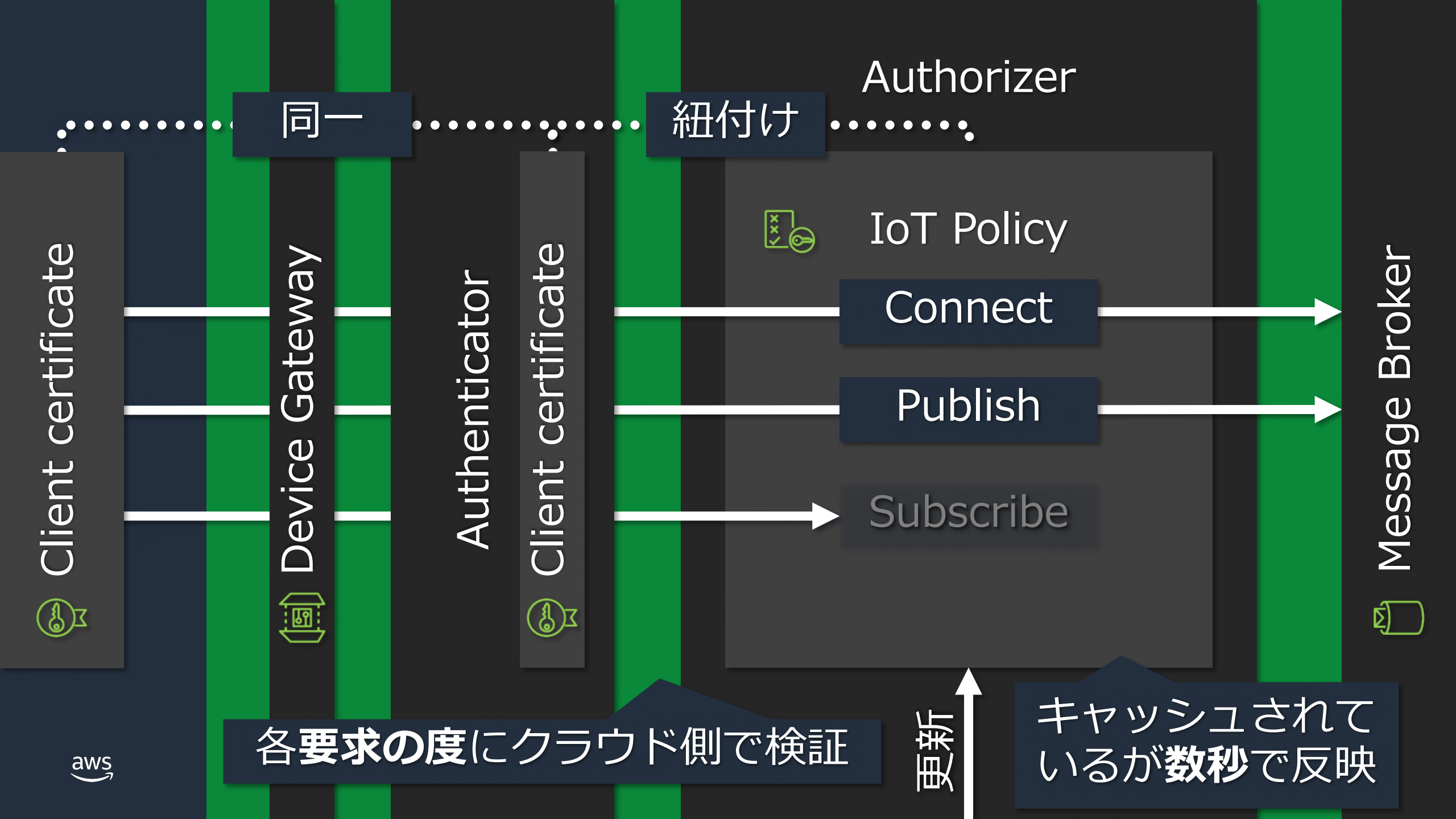

Device
AWS IoT
データプレーン
コントロール
プレーン
Management Console / CLI


Device
AWS IoT
データプレーン
操作の例
• 接続
• 発行
• サブスクライブ
• シャドウの取得
• シャドウの更新
• ジョブ実行の更新
Device Gateway
Message Broker
Rules
Device Shadow
Jobs
コントロールプレーン
操作の例
作成・更新
Management Console / CLI


Device
AWS IoT
データプレーン
操作の例
• 接続
• 発行
• サブスクライブ
IoT Policy
• シャドウの更新
• ジョブ実行の更新
Device Gateway
Message Broker
Rules
Device Shadow
Jobs
コントロール プレーン
操作の例
作成・更新
AWS IAM Policy
Management Console / CLI


aws
AWS IoT
Device Gateway
HTTP
Publish
AWS Lambda
AWS SDK
一部データプレーンの制御も可
AWS IAM
Role & Policy
aws


同一
紐付け
Authorizer
Client certificate
Device Gateway
Authenticator
Client certificate
IoT Policy
Connect
Publish
Subscribe
Message Broker
各**要求の度**にクラウド側で検証


Authorizer
同一
紐付け
Client certificate
Device Gateway
Authenticator
Client certificate
IoT Policy
Connect
Publish
Subscribe
Message Broker
各**要求の度**にクラウド側で検証
更新
キャッシュされているが**数秒**で反映
aws

Authorizer

IoT Policy

Connect

Publish

どのように記述？

Message Broker

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iot:Connect"],
      "Resource": ["arn:aws:iot:REGION:ACCONT_ID:client/CLIENT_ID"]
    }, {
      "Effect": "Allow",
      "Action": ["iot:Publish"],
      "Resource": ["arn:aws:iot:REGION:ACCONT_ID:topic/TOPIC"]
    }
   ]
}
```

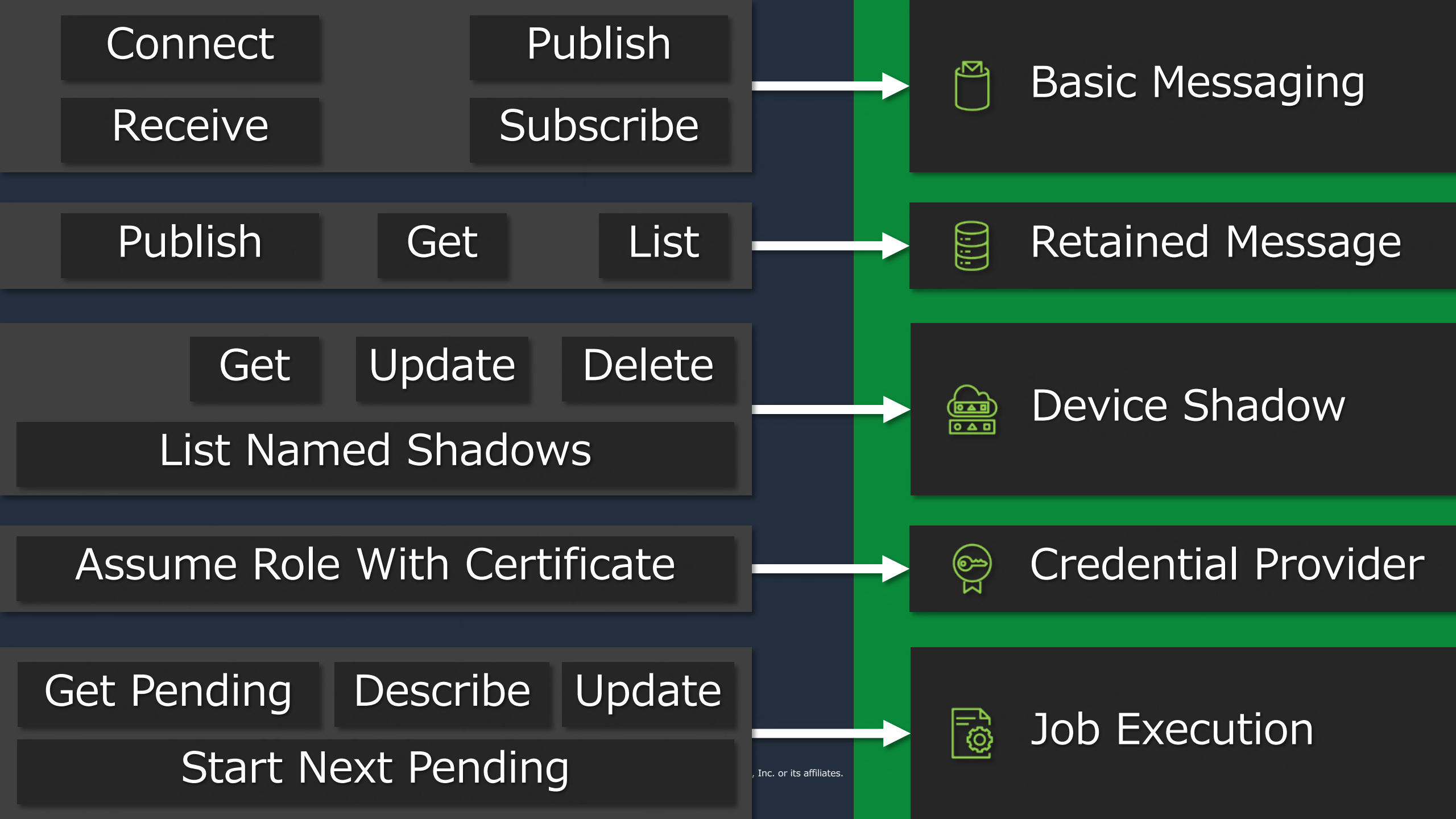
文字は**環境毎**に置き換え

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iot:Connect"],
      "Resource": ["arn:aws:iot:us-east-1:123456789012:client/client1"]
    }, {
      "Effect": "Allow",
      "Action": ["iot:Publish"],
      "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/client1"]
    }
   ]
}
```

置き換えた例

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iot:Connect"],
      "Resource": ["arn:aws:iot:us-east-1:123456789012:client/client1"]
    }, {
      "Effect": "Allow",
      "Action": ["iot:Publish"],
      "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/client1"]
    }
  ]
}
```

IoT ポリシーで許可できる**操作**は？



```
{
   "Version": "2012-10-17",
   "Statement": [
    {
     "Effect": "Allow",
     "Action": ["iot:Connect"],
     "Resource": ["arn:aws:iot:us-east-1:123456789012:client/client1"]
    }, {
     "Effect": "Allow",
     "Action": ["iot:Publish"],
     "Resource": ["arn:aws:iot:us-east-1:123456789012:topic/client1"]
    }
   ]
}
```

Client 毎の最小権限設定には**ベタ書き**？

認証情報と同様に**個別**に用意？

全台数分の作成・管理は**煩雑**に…

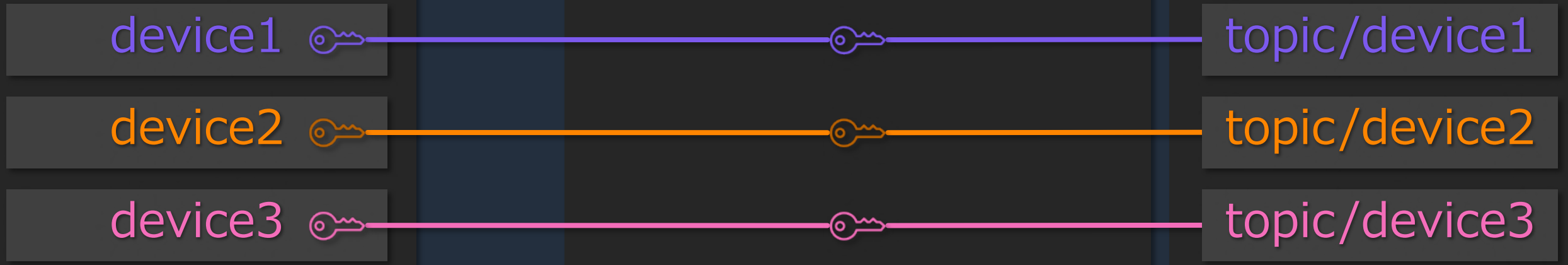
権限は類似のため、**共通化**できないか？

Device

Authenticator

**最小**権限のみ

Authorizer



ポリシー共通化のため、**ポリシー変数**を活用

**${iot:<変数名>}** で利用

定義済変数のみ使用可、自身での**定義は不可**

```
{
  "Version": "2012-10-1
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iot:Connect"],
      “Resource”: [“arn:aws:iot:<略>:client/${iot:ClientId}"]
    }, {
      "Effect": "Allow",
      "Action": ["iot:Publish"],
      “Resource”: [“arn:aws:iot:<略>:topic/${iot:ClientId}"]
    }
  ]
}
```

接続した Client に動的に**限定**

Client ID は Client が**自由に名乗れる**

名乗った ID で変数が置換され、権限付与

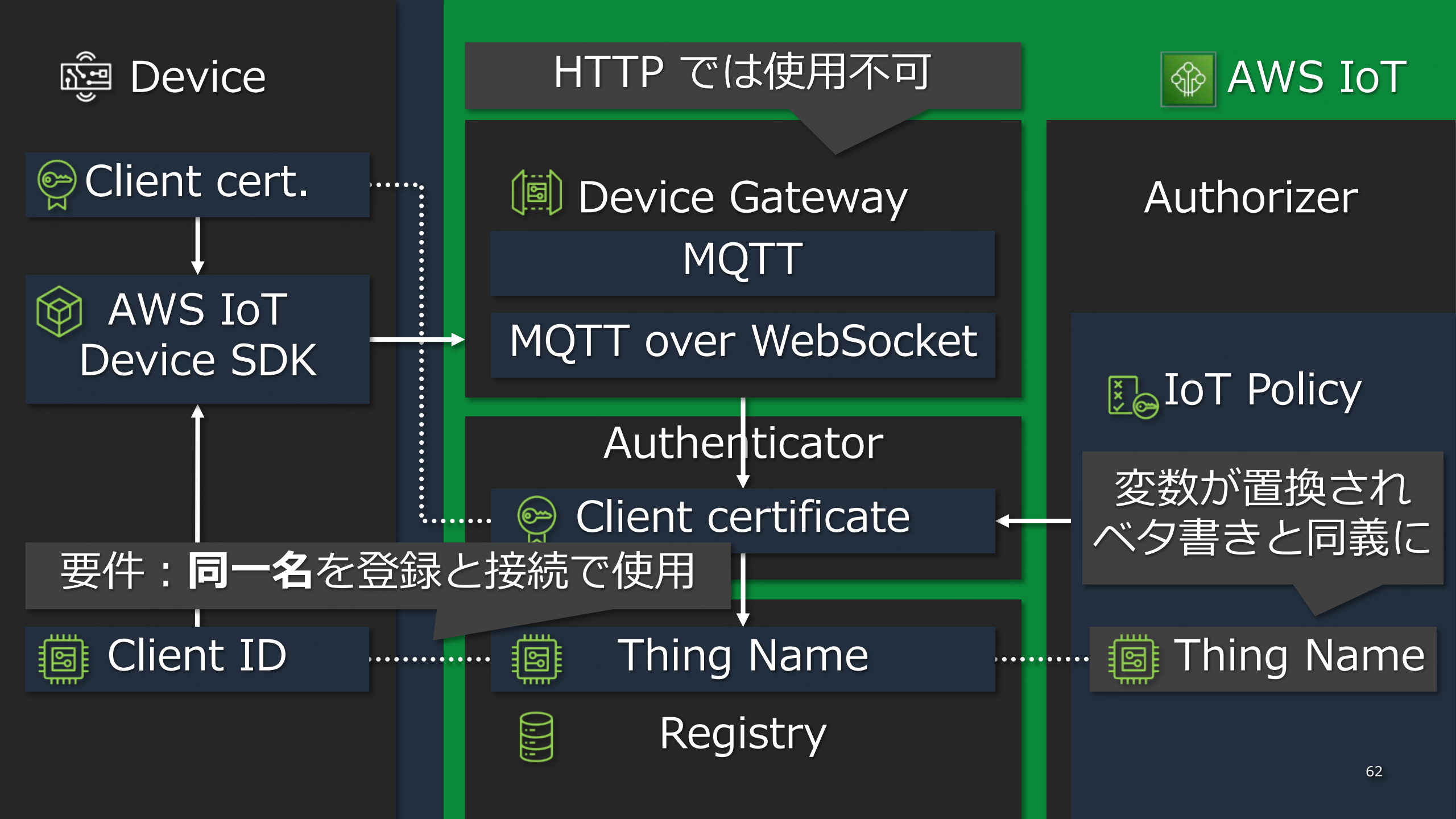
認証情報を持っていれば、**誰でも接続可**

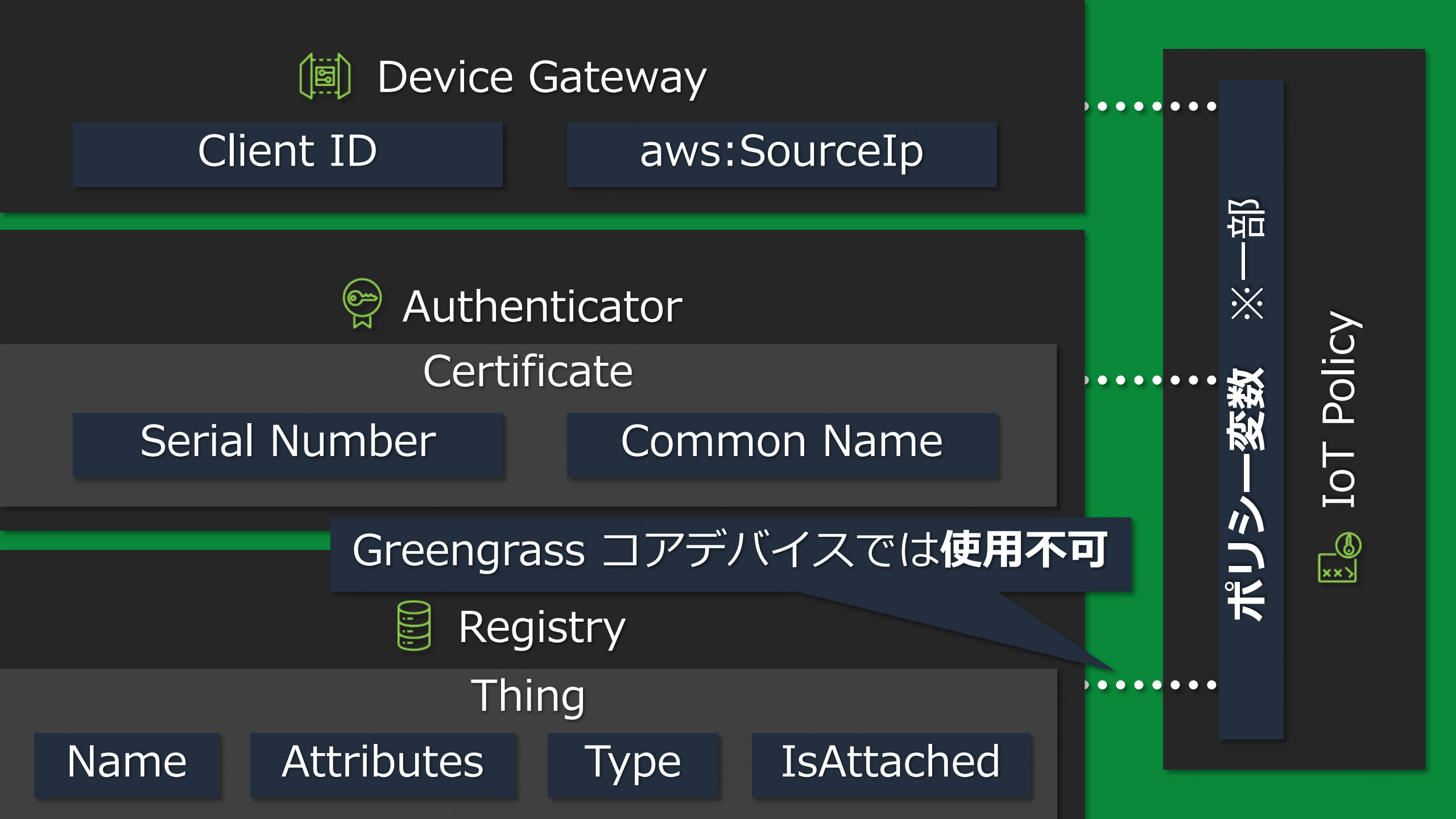
最小権限になっていない！ではどうすれば良い？

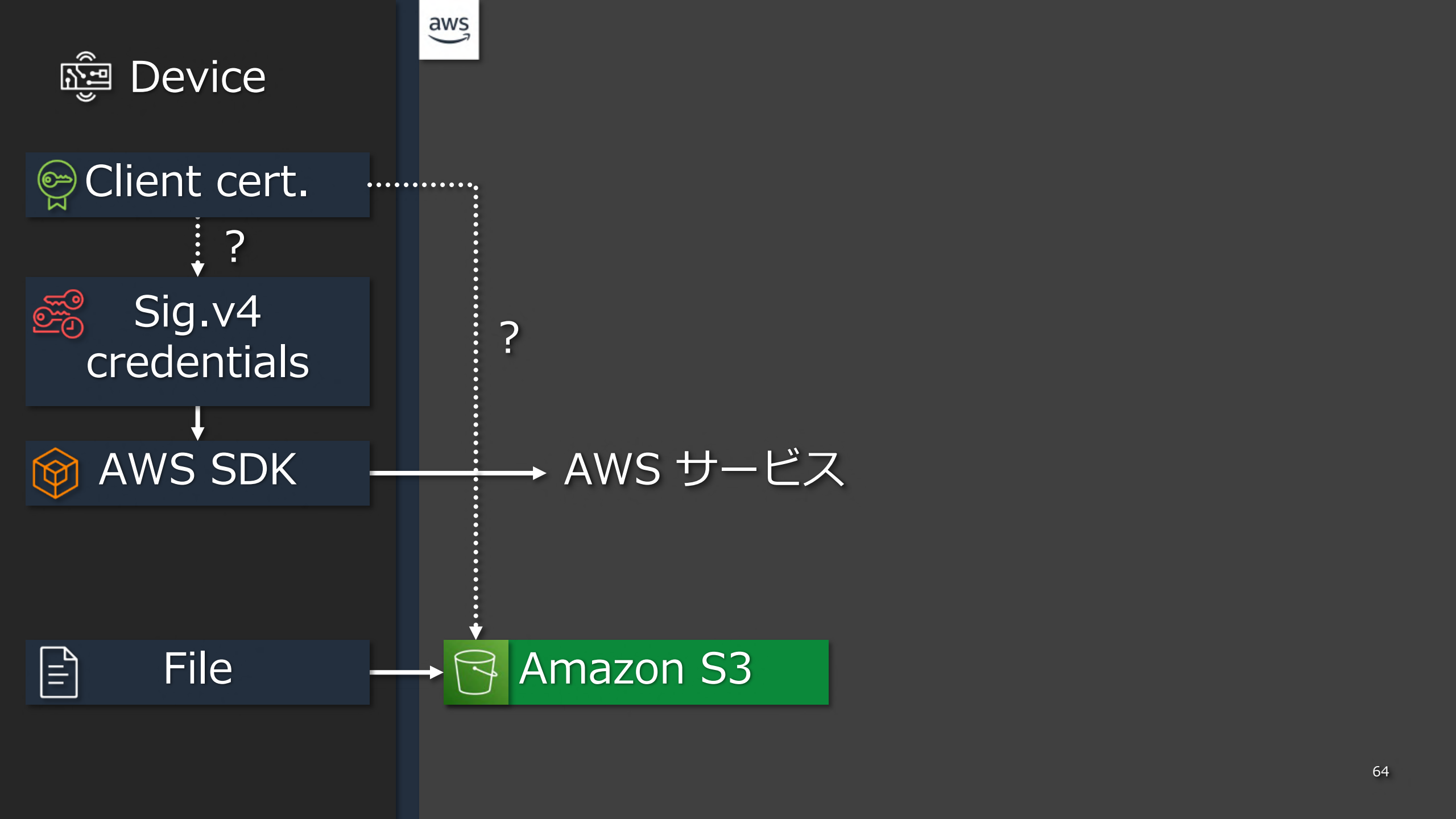
```
{
   "Version": "20
   "Statement": [
     {
       "Effect": "A
       "Action": ["iot:Connect"],
       “Resource”: [“arn:aws:iot:<略>:client/${iot:ClientId}"]
     }, {
       "Effect": "Allow",
       "Action": ["iot:Publish"],
       “Resource”: [“arn:aws:iot:<略>:topic/${iot:ClientId}"]
     }
   ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iot:Connect"],
      “Resource”: [“<略>:client/${iot:Connection.Thing.ThingName}"]
    }, {
      "Effect": "Allow",
      "Action": ["iot:Publish"],
      “Resource”: [“<略>:topic/${iot:Connection.Thing.ThingName}"]
    }
  ]
}
```

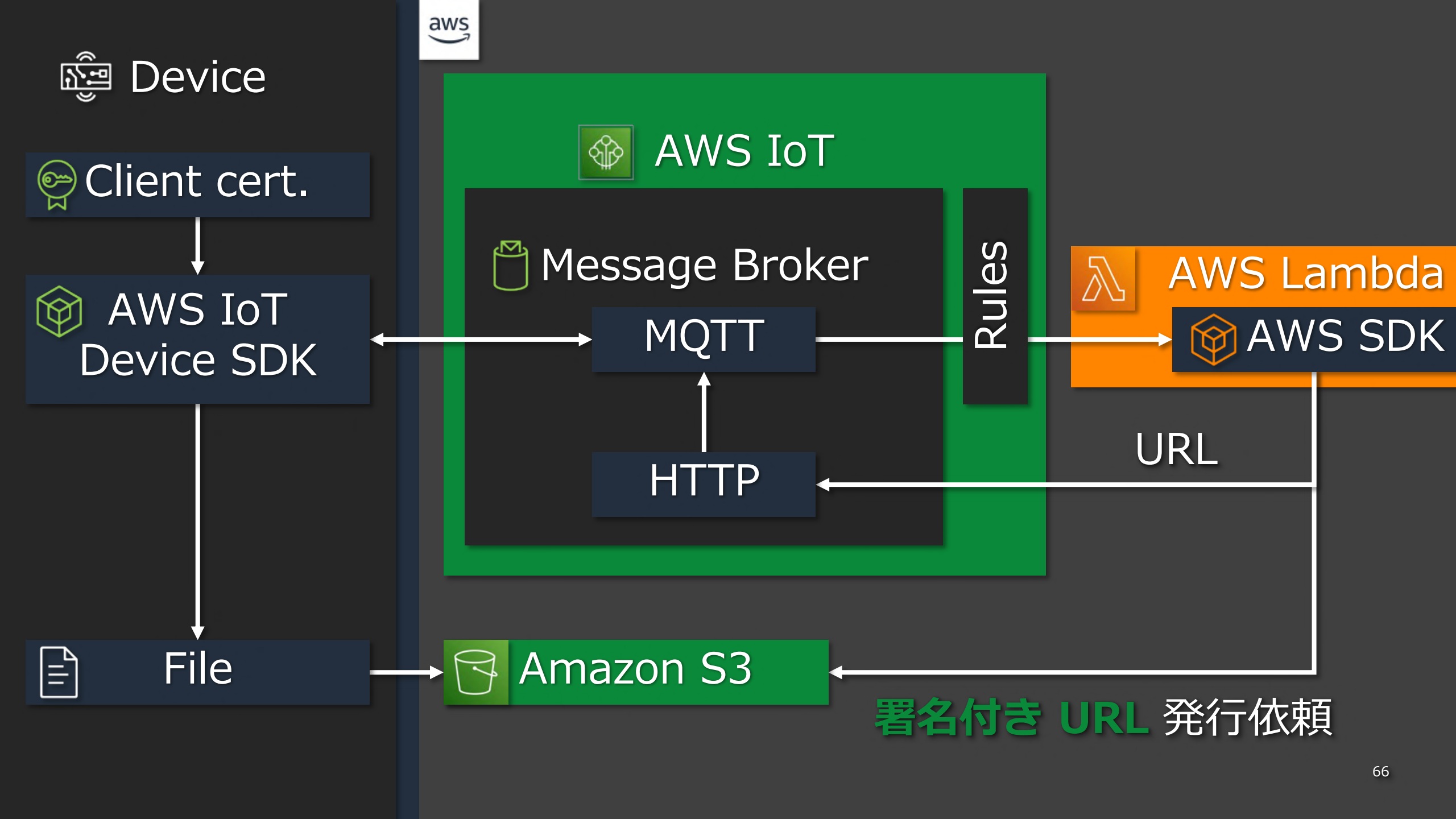
このモノのポリシー変数で解決！

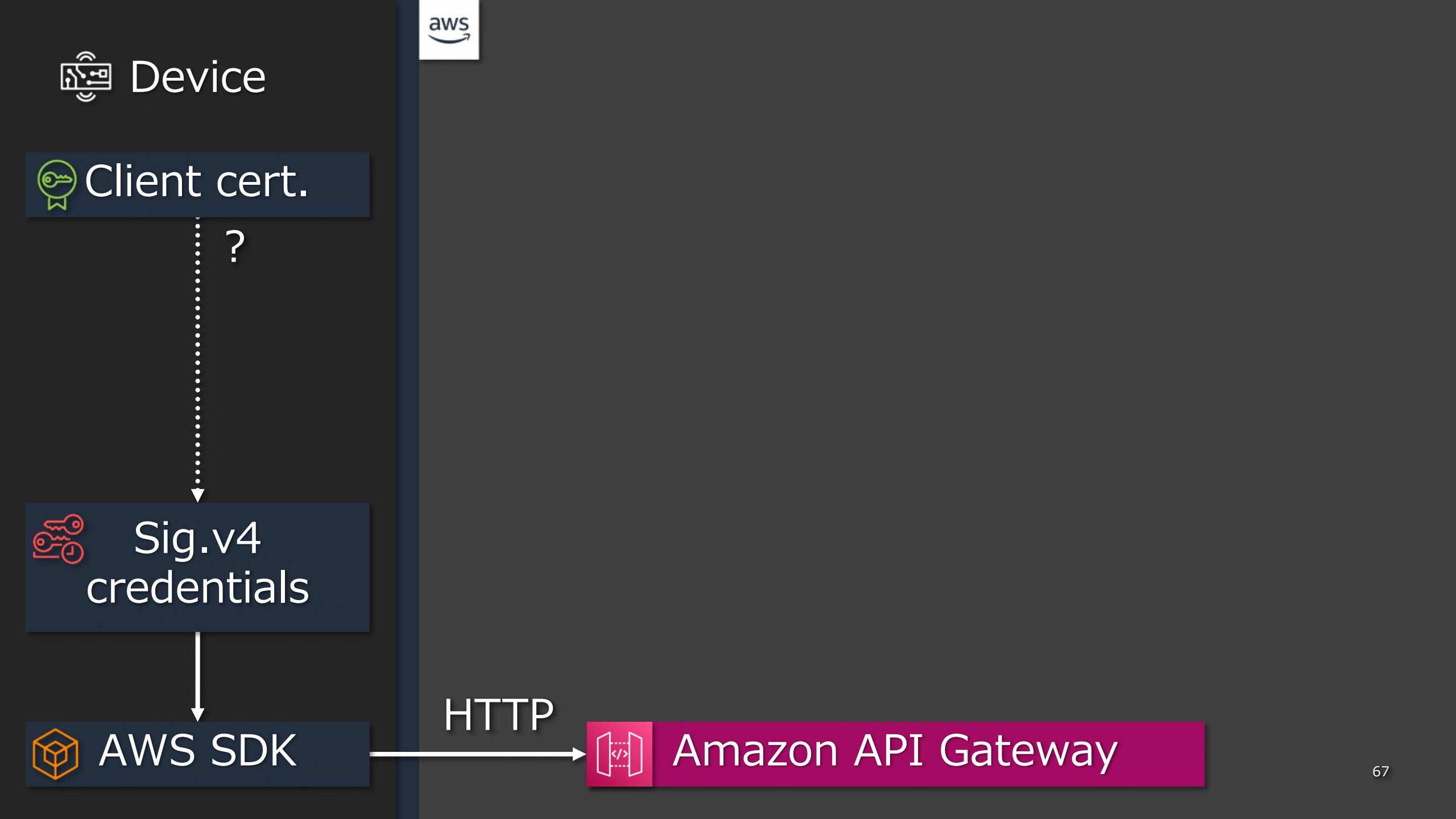

Device
HTTP では使用不可
AWS IoT
Client cert.
Device Gateway
Authorizer
MQTT
AWS IoT
Device SDK
MQTT over WebSocket
IoT Policy
Authenticator
変数が置換され
ベタ書きと同義に
Client certificate
要件：同一名を登録と接続で使用
Client ID
Thing Name
Thing Name
Registry

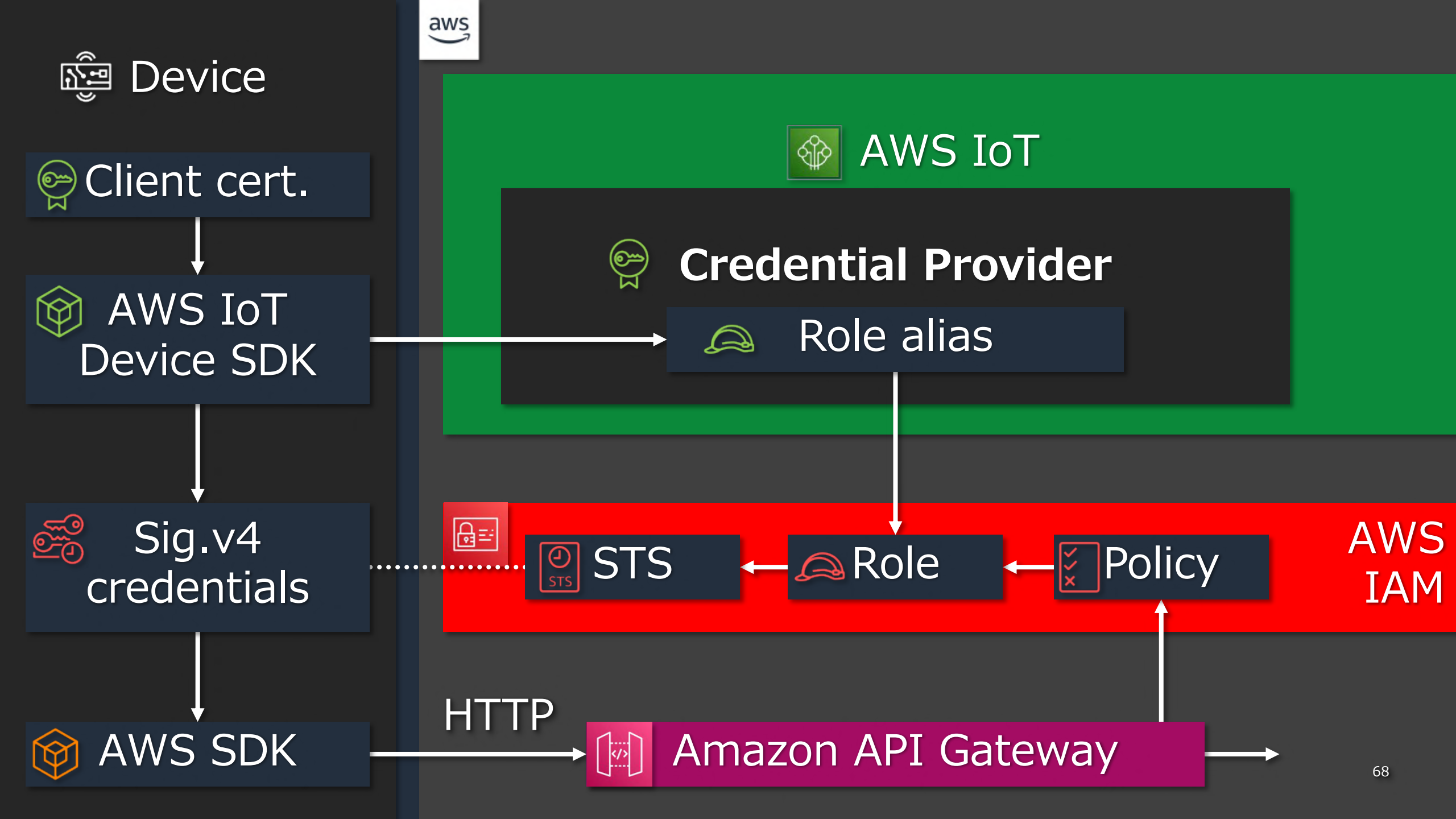

Device Gateway
Client ID
aws:SourceIp
Authenticator
Certificate
Serial Number
Common Name
Greengrass コアデバイスでは使用不可
Registry
Thing
Name
Attributes
Type
IsAttached
IoT Policy
ポリシー変数 ※一部


Device
Client cert.
?
Sig.v4
credentials
AWS SDK
?
AWS サービス
File
Amazon S3


Device
Client cert.
?
署名付き URL
File
Amazon S3


Device
Client cert.
AWS IoT
Device SDK
File
aws
AWS IoT
Message Broker
MQTT
HTTP
Rules
AWS Lambda
AWS SDK
URL
Amazon S3
署名付き URL 発行依頼


Device
Client cert.
?
Sig.v4 credentials
AWS SDK
HTTP
Amazon API Gateway


Device
Client cert.
AWS IoT Device SDK
Sig.v4 credentials
AWS SDK
aws
AWS IoT
Credential Provider
Role alias
STS
Role
Policy
AWS IAM
HTTP
Amazon API Gateway

認証 → 認可

AWS IoT

柔軟かつ厳密な**権限設定**はどうやる？

どう**接続**したら良い？

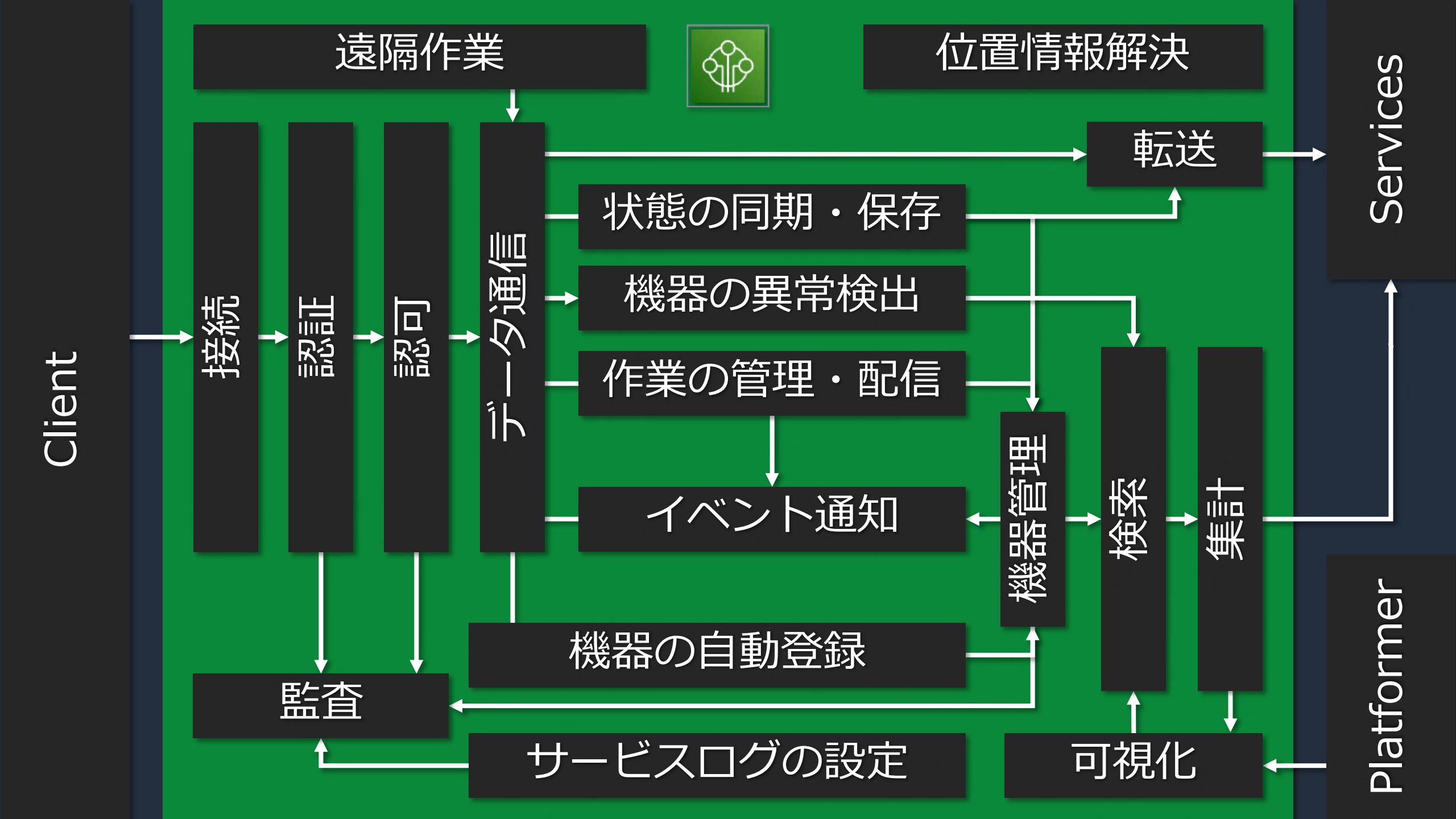
Client → 接続 → 認証 → 認可

**今回のIoT要件**

AWS IoT

柔軟かつ厳密な**権限設定**はどうやる？

**安全**に接続するには？


Client
遠隔作業
位置情報解決
接続
認証
認可
データ通信
転送
状態の同期・保存
機器の異常検出
作業の管理・配信
イベント通知
機器管理
検索
集計
Services
Platformer
機器の自動登録
監査
サービスログの設定
可視化

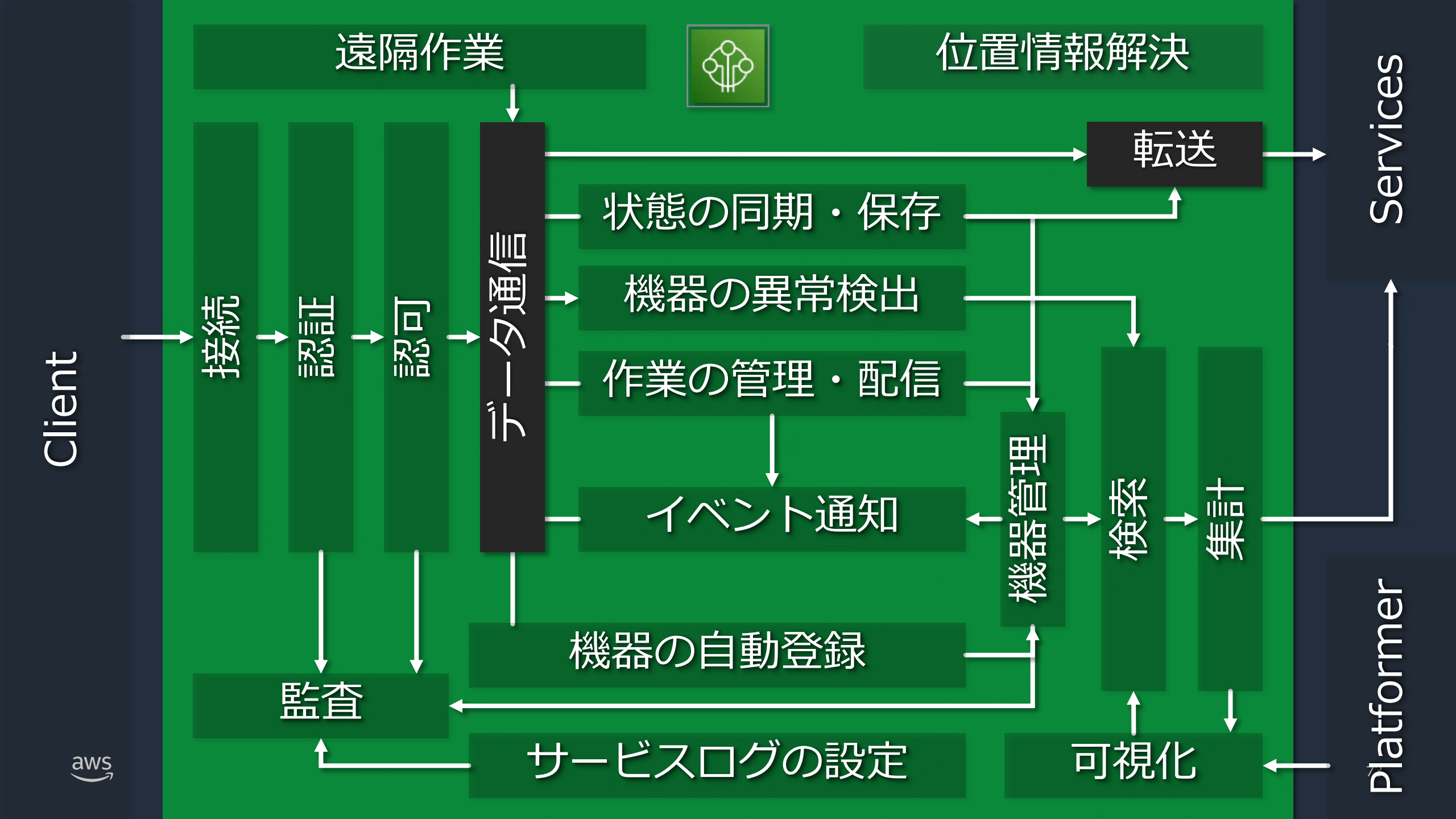
AWS Black Belt Online Seminar

AWS IoT 活用シリーズ **次回**

# データの通信・加工・転送

IoT Specialist Solutions Architect

飯塚 将太


遠隔作業
位置情報解決
Client
接続
認証
認可
データ通信
転送
Services
状態の同期・保存
機器の異常検出
作業の管理・配信
イベント通知
機器管理
検索
集計
機器の自動登録
監査
サービスログの設定
可視化
Platformer
aws

# 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

# その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

https://aws.amazon.com/jp/events/

ハンズオンコンテンツ

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

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html

# Thank you!