

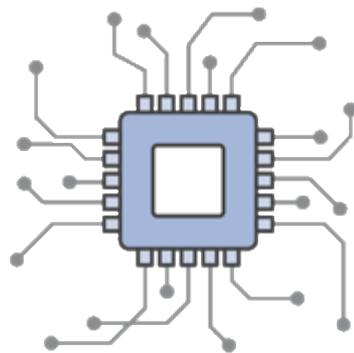
Amazon Web Servicesが開く 新しい可能性 AWS IoT

2016/3/1

アマゾン ウェブ サービス ジャパン株式会社
吉荒 祐一

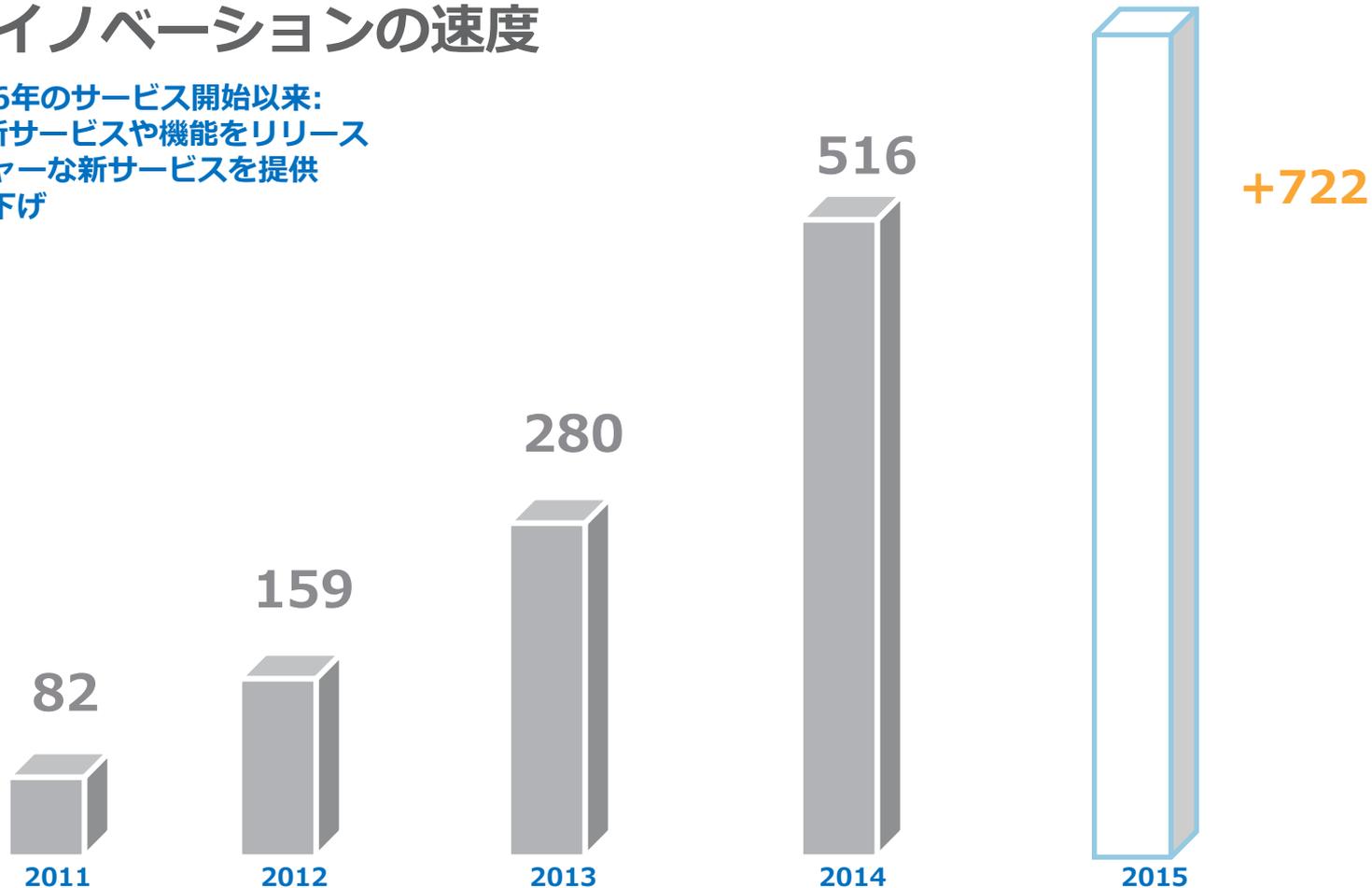
アジェンダ

- 📦 Amazon Web Services(AWS)最新情報
- 📦 AWS IoT
- 📦 まとめ



AWSのイノベーションの速度

AWSは、2006年のサービス開始以来:
1,896以上の新サービスや機能をリリース
60以上のメジャーな新サービスを提供
51回の料金値下げ



AWSの特長：グローバルインフラストラクチャ



190か国以上で、100万を超えるお客様がご利用中

12のリージョン(地域)：日本国内は東京リージョン、データやシステムはお客様が選択したリージョンに配置

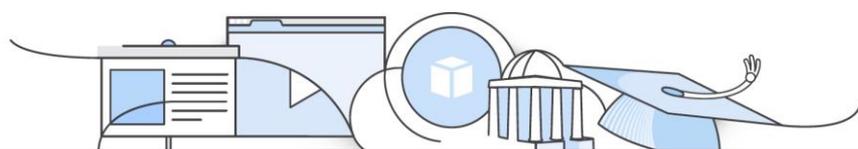
32のアベイラビリティゾーン：東京リージョンには二つのアベイラビリティゾーン

(同一災害で同時に被災しないよう配置したデータセンターのクラスター)

AWS 研究助成



- AWS 研究助成プログラムは、以下のような目標を持つ研究者をサポートします。
 - 今後の自らの研究および研究者のコミュニティによる研究に役立てるため、クラウドをホストとして一般公開される "サービスとしてのサイエンス" アプリケーションを構築する。
 - コンセプトの実証やベンチマークテストの実施により、科学方面のワークロードやオープンデータセットをクラウドに移行することの有効性を評価する。
 - 研究方面のワークロードに対するクラウド利用について、ワークショップやチュートリアルを通じ、より幅広いコミュニティを訓練する。



FREE

AWS Educateは、 クラウドのトレーニングと リソースを提供します

AWS Educateは、次世代のITプロフェッショナル、クラウドプロフェッショナルに向け教育機関に開かれた登竜門です。アマゾンのグローバルなイニシアティブにより、学生や教師がクラウドに関連する学習を加速し、明日の起業家・技術者・研究者を強力に支援するために必要なクラウドのリソースを提供します。

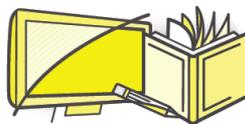
認定による特典は www.awseducate.com までお申込みください



AWSの
テクノロジーと
サービスの
無料利用枠



クラウド
コンピューティングと
AWSに関する
ラボ、チュートリアル、
トレーニング



専門家、
プロフェッショナル、
AWSが提供する
オープンソースの
講座コンテンツ



ベストプラクティスを
共有する
ヴァーチャル・
対面両方の
コミュニティ

AWS Educateの特典

特典	教員	生徒
AWS無料利用枠	\$200/教員あたり：加盟教育機関の場合 \$75/教員あたり：非加盟教育機関の場合	\$100/生徒あたり：加盟教育機関の場合 \$35/生徒あたり：非加盟教育機関の場合
AWSトレーニング	セルフペースラボの無料利用 AWS Essential e-Learningの無料受講 インストラクターによる講習、資格試験 の50%割引	セルフペースラボの無料利用
コンテンツ	AWS提供コンテンツへの無料アクセス 最先端の教育者提供コンテンツへの無料 アクセス	課題、演習、自習用のAWS提供コンテン ツへの無料アクセス
コラボレーションツール	Educator Collaboration Portal（教員コ ラボレーションポータル）へのアクセス 仮想・有人のイベント コンテンツの提供と評価 公開・非公開のディスカッションフォー ラム AWS Educateへのフィードバック	Student Portal（生徒ポータル）へのア クセス 情報収集・ベストプラクティスの共有・ ネットワーキングのための仮想・有人の イベント AWS Educateへのフィードバック

Global Data Egress Waiver for Research

研究分野データ転送料金軽減プログラム

Scientific Computing

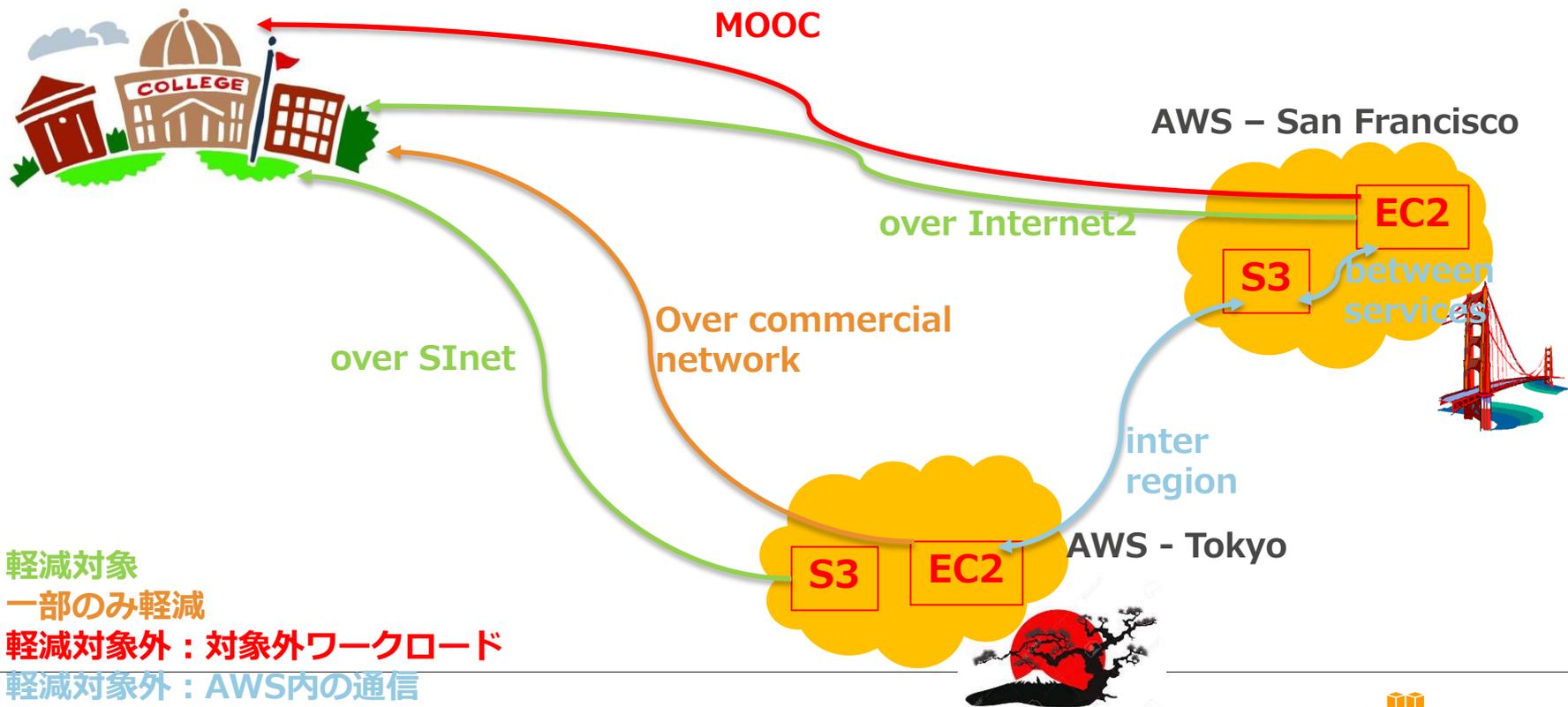


AWSは全世界の科学計算マーケットをサポートします。

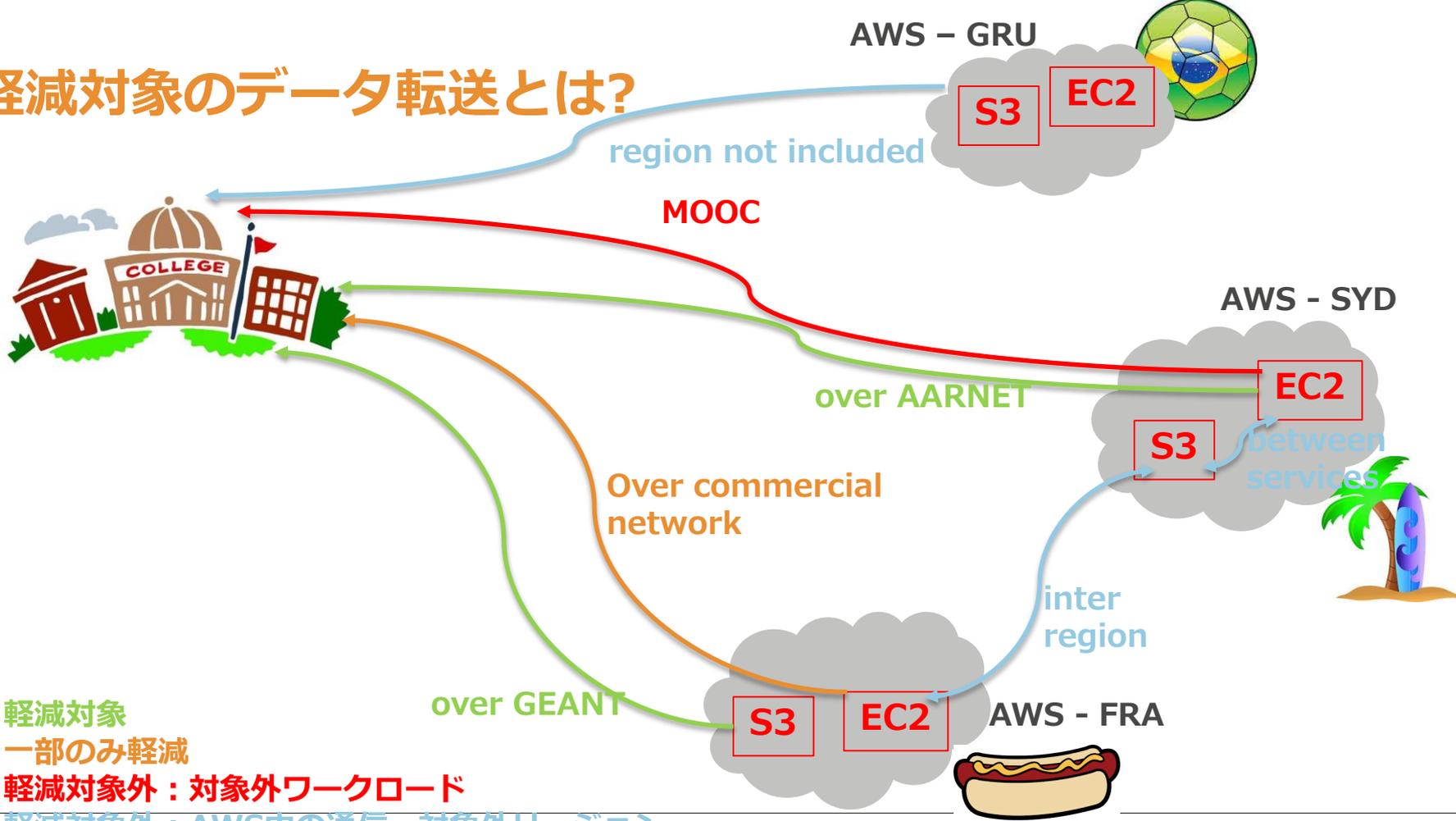
Why?

科学は計算を最も大規模に行うエリアであり、また、コストとグローバルなアクセスにおける民主化・大衆化から最も大きな恩恵を受けるものでもあります。Amazonはそこに参加することで、**巨大で、不連続な変化をもたらすインパクト**を世界にもたらすことが出来ると考えています。それは私たちが**企業として目指す最も根源的な事**なのです。

軽減対象のデータ転送とは?



軽減対象のデータ転送とは?



- 軽減対象
- 一部のみ軽減
- 軽減対象外：対象外ワークロード
- 軽減対象外：AWS内の通信、対象外リージョン

研究分野データ転送料金軽減プログラム

Why

- 研究分野においては予測・固定可能な費用が求められるため

Who

- 公共機関の研究者においてご利用可能です
- 永続的な制度です
- 北米、欧州、アジア太平洋、GovCloudリージョンが対象
(南米、中東、中国、インド、アフリカは含みません)

What

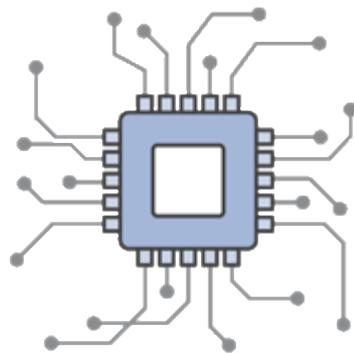
- 認定されたアカウントの対象データ転送料金を免除します
- 請求金額の15%までの免除を上限とします
- MOOCsや他の外部にサービスを提供する場合は除外します
- 相互接続している学術研究ネットワーク (例SINET)の使用が必要です

How

- Contract addendum (契約書別紙) の締結が必要です
- お客様はリセラー経由での購入も可能です (例：米国のDLT)

アジェンダ

- 📦 Amazon Web Services(AWS)最新情報
- 📦 AWS IoT
- 📦 まとめ



クラウドとモノをつなげるときに、 様々な要件がある



たくさんの
SDKやツール



クラウドへの接続



スケーラビリティ



セキュリティ



クラウドに適した
アプリケーション
実装



ビッグデータ
分析



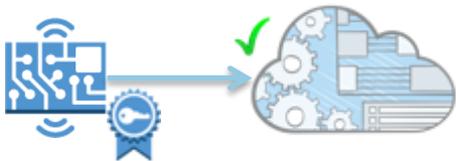
予測

AWS IoT

さまざまなデバイスとAWSをセキュアに接続し、デバイスデータに対する処理やアクションを実行したり、デバイスをリモートで制御・管理することが可能

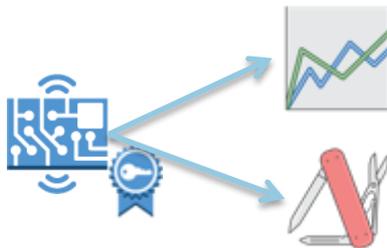
1

セキュアでスケーラブルな
デバイスとクラウドの
双方向接続



2

デバイスデータに対する
いろいろなアクション

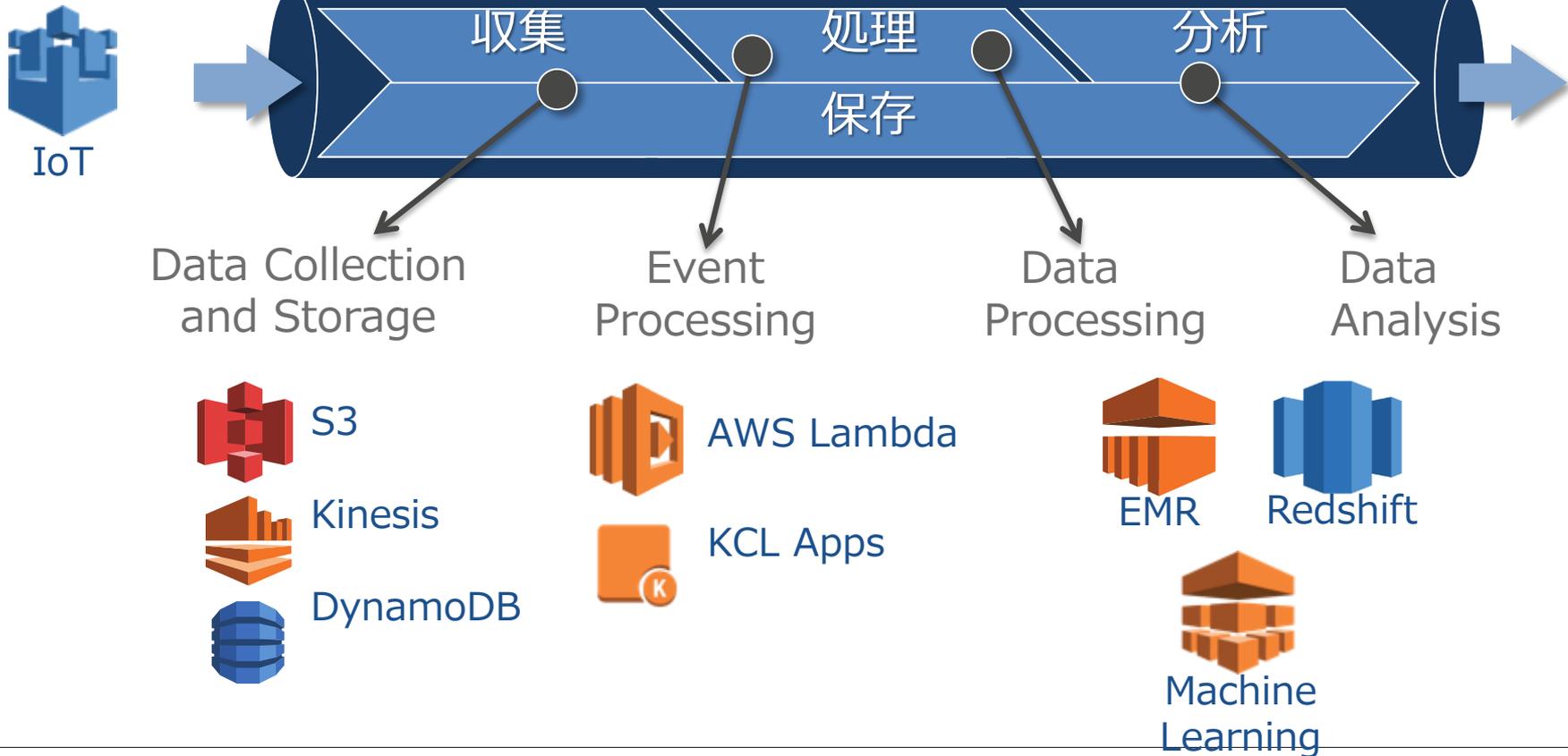


3

誰でも簡単に
はじめられる



データフローとAWSサービスのマッピング



AWS IoT: デバイスとセキュアに接続

Multi-protocol Message Gateway

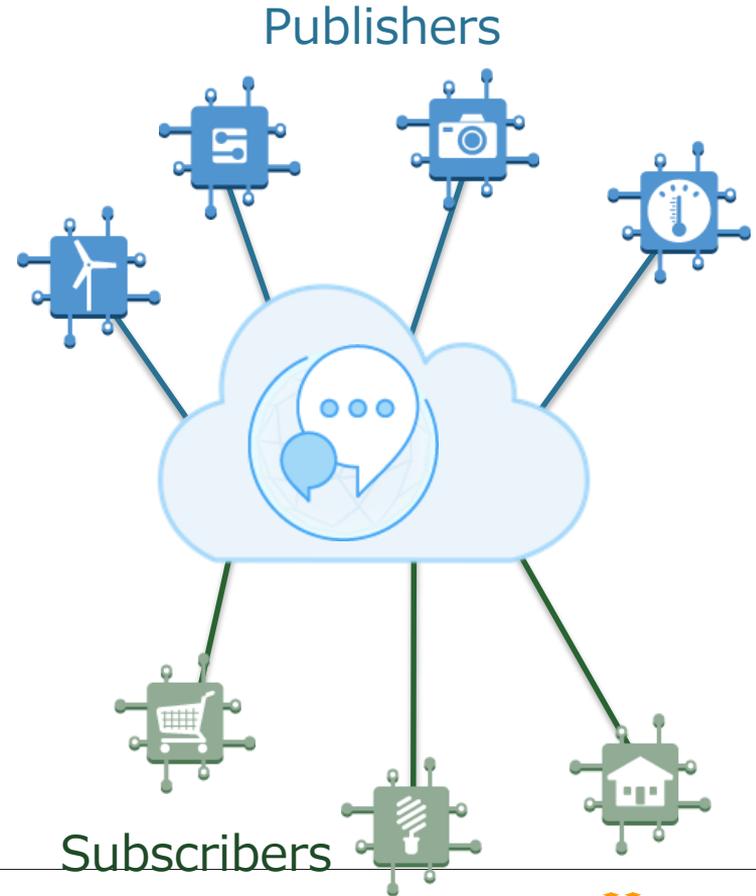
Millions of devices and apps can connect over MQTT or HTTP.

Elastic Pub Sub Broker

Go from 1 to 1-billion long-lived connections with zero provisioning

Secure by Default

Connect securely via X509 Certs and TLS v1.2 Client Mutual Auth



AWS IoT: AWSへの玄関

Registry

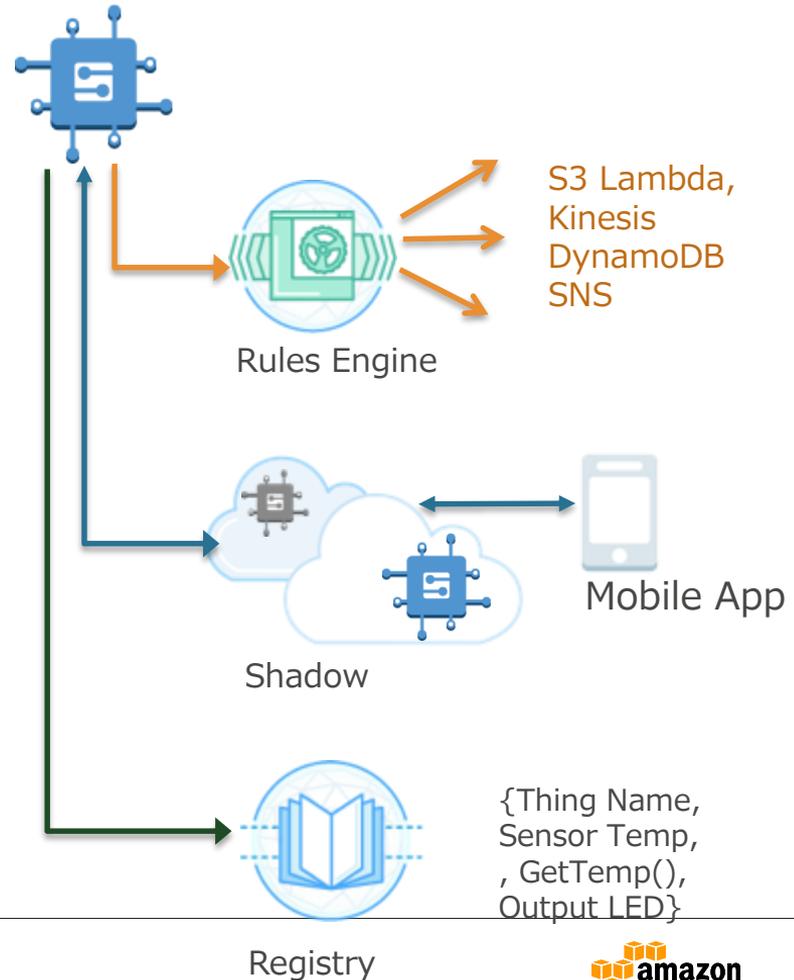
Establishes an identity for devices and manages metadata such as the devices' attributes and capabilities

Shadows

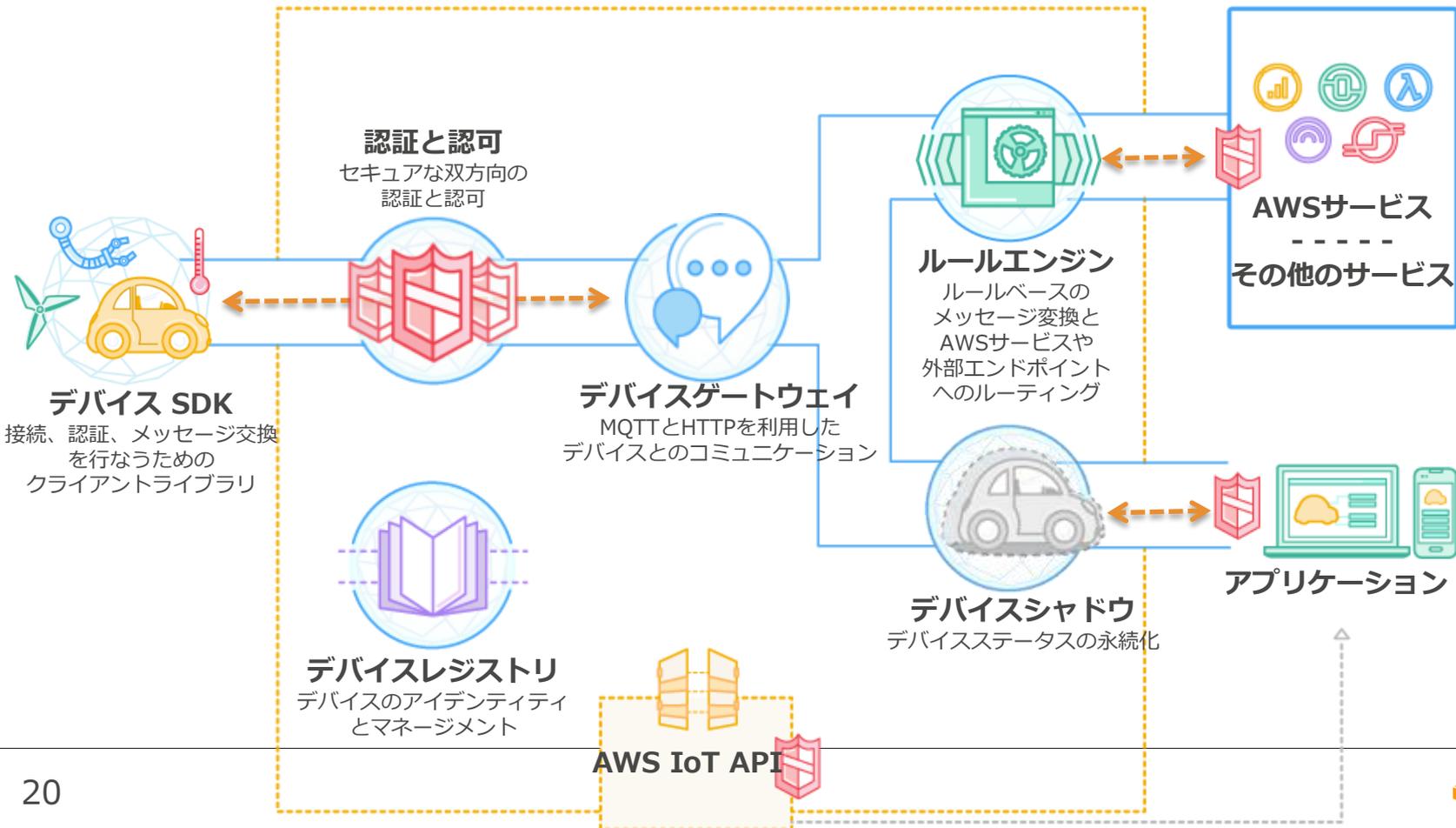
Apps and devices can access "RESTful" Shadow (Thing's State) that is in sync with the device

Rules and Actions

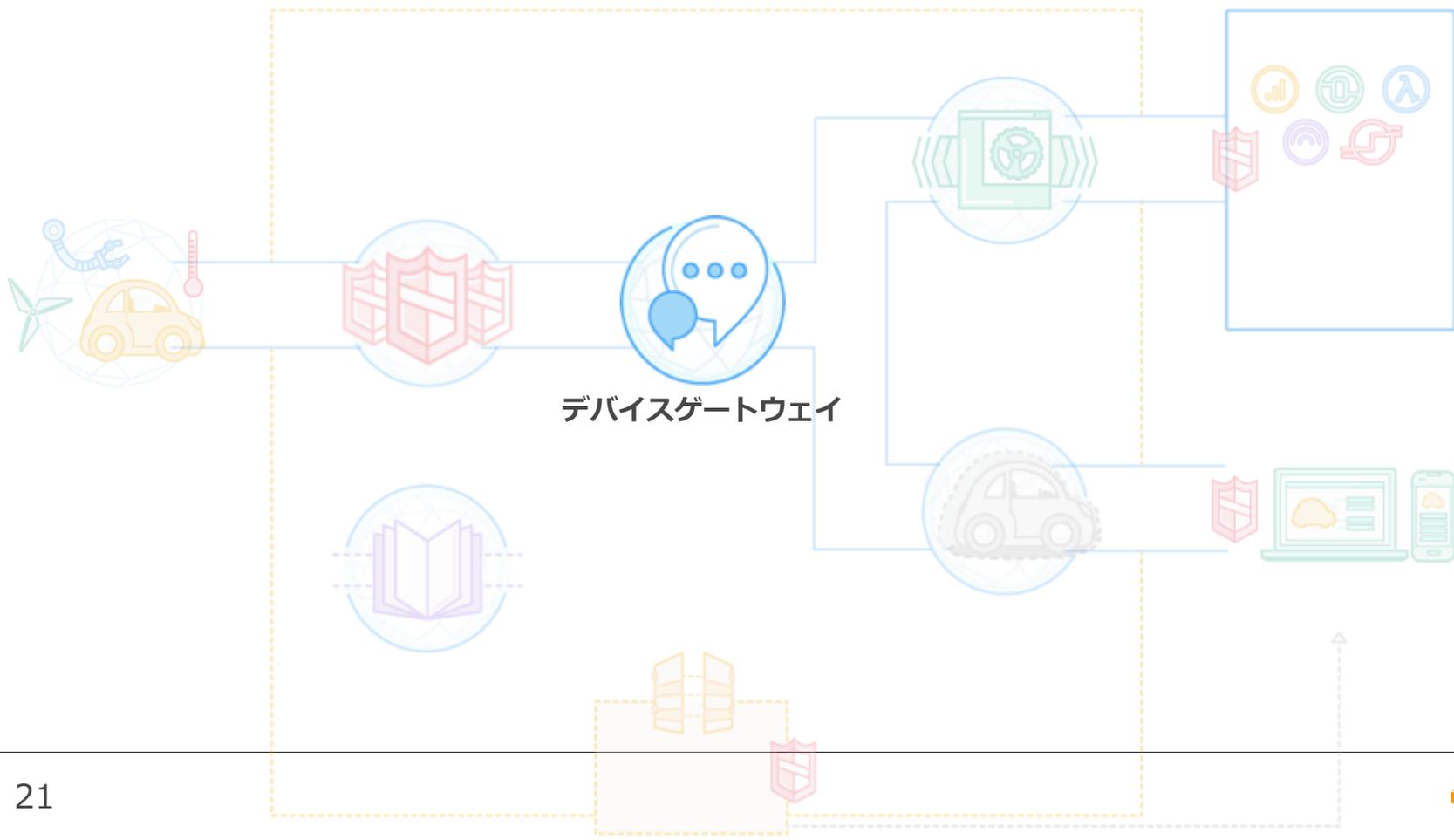
Match patterns and take actions to send data to other AWS services or republish



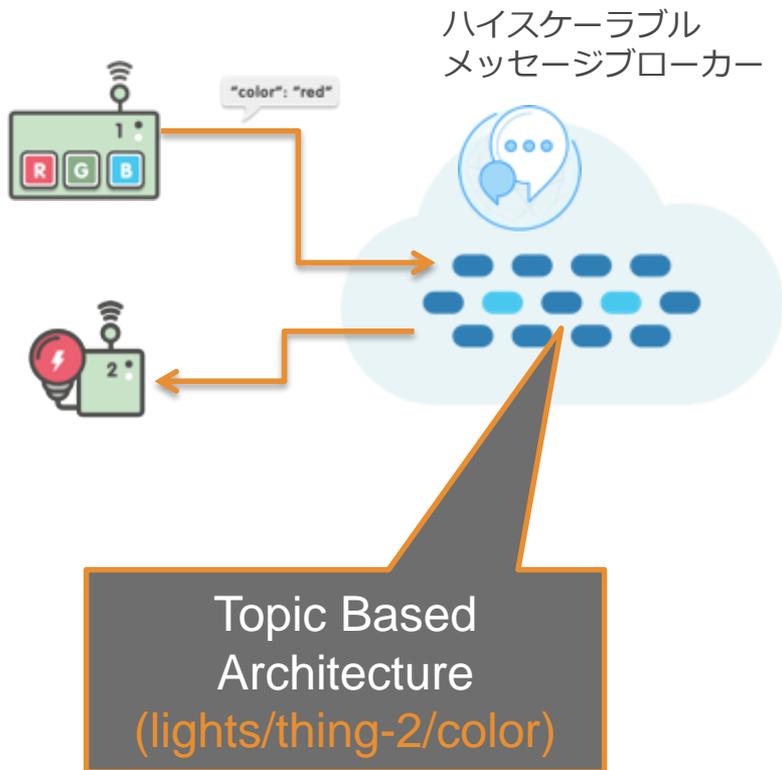
AWS IoT 全体構成



デバイスゲートウェイ



デバイスゲートウェイ



スタンダードプロトコル (no lock-in)

数百万デバイスやアプリをMQTTやHTTP1.1プロトコルを使って通信ができる。

SDK以外にも汎用ライブラリが利用可能。

長期間のセッション保持によるクラウドを介したメッセージ送受信

クライアント（デバイスやアプリ）は制御信号やコマンドなどをクラウドから受信することができる

デフォルトのセキュリティ

X509証明書とTLS1.2を使った相互認証

MQTTプロトコルとは



- M2M/IoTで利用されるコミュニケーションプロトコル
- OASIS スタンダードプロトコル(v3.1.1)
- ライトウェイト
- Pub-Sub メッセージ交換モデル
- リソースや回線帯域が限られているデバイスで利用

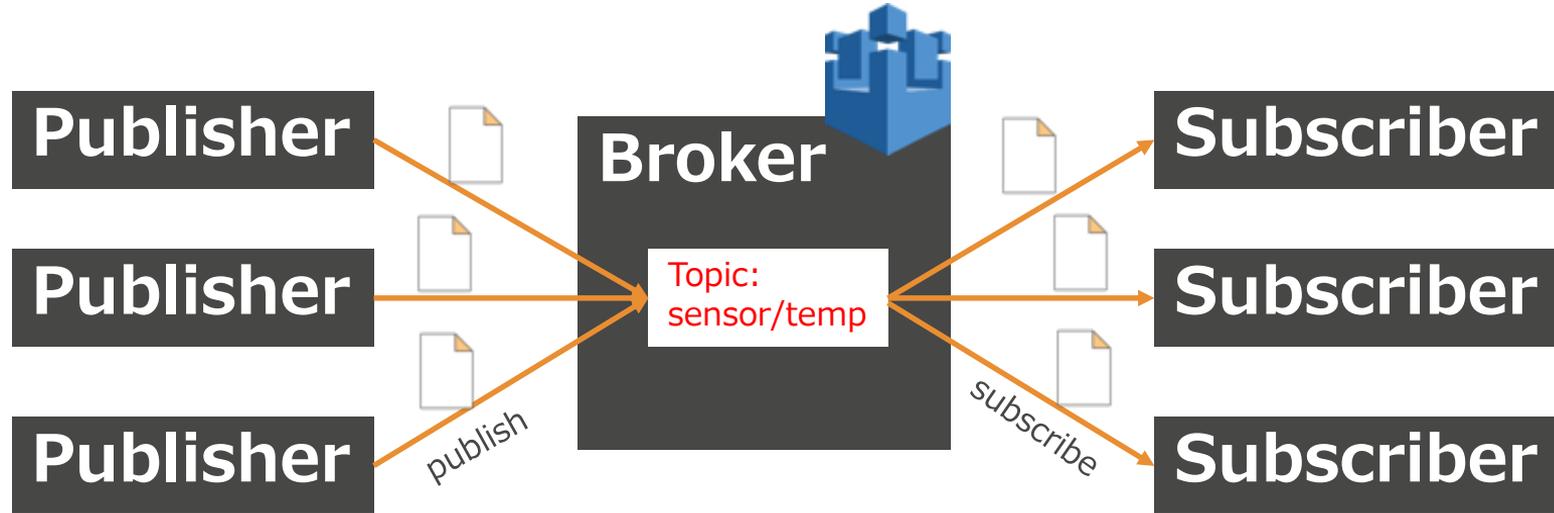
MQTT vs HTTPS

MQTTを利用することで・・・

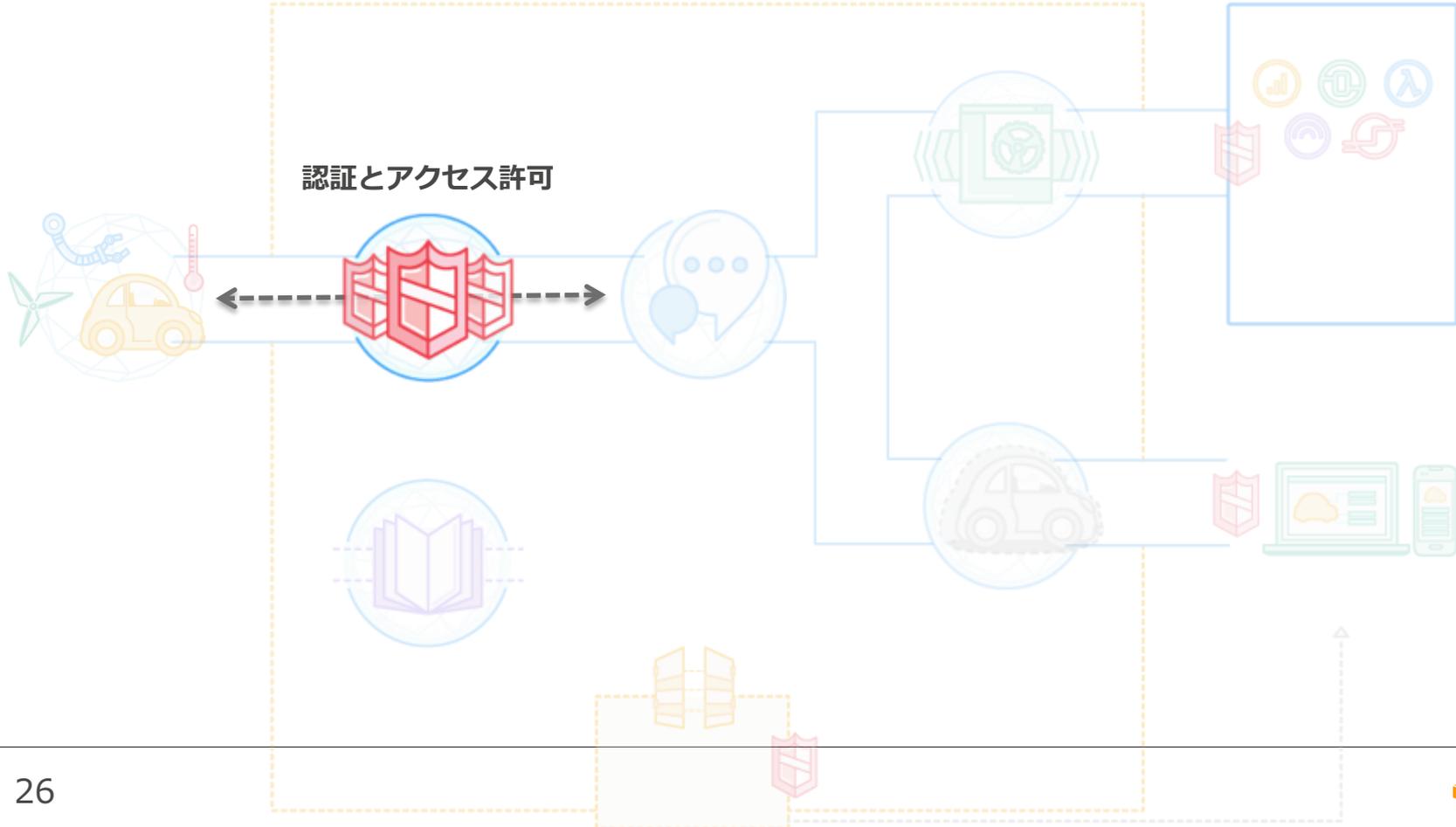
- スループットが93倍あがる
- メッセージ送信において1/12の消費電力
- メッセージ受信において1/180の消費電力
- コネクション維持において1/2の消費電力
- ネットワークオーバーヘッドの8倍削減

Source: <http://stephendnicholas.com/archives/1217>

MQTT Publish/Subscribe



認証とアクセス許可



AWS IoTが対応する2つのプロトコル

	NEW MQTT + TLS相互認証	従来のAWSプロトコル AWS認証 + HTTPS
サーバ認証	TLS + Cert	TLS + Cert
クライアント認証	TLS + Cert	AWS API Keys
Confidentiality	TLS	TLS
プロトコル	MQTT	HTTP
識別	AWS ARNs	AWS ARNs
認可	AWS Policy	AWS Policy

AWS IoTポリシー

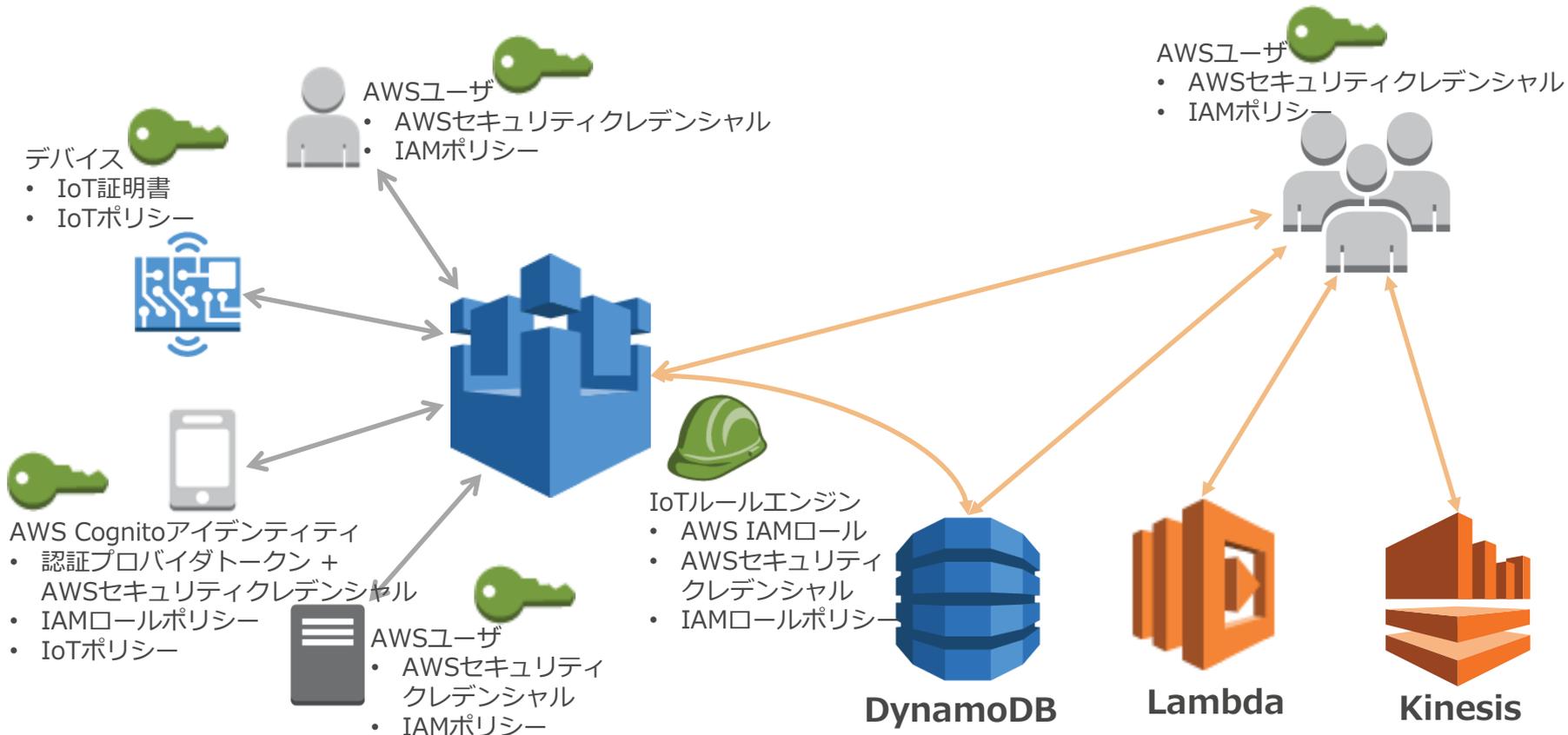
デバイスに対してAWS IoTのどのリソース（トピックなど）に対し、どのような権限を与えるか、きめ細かい権限設定が可能



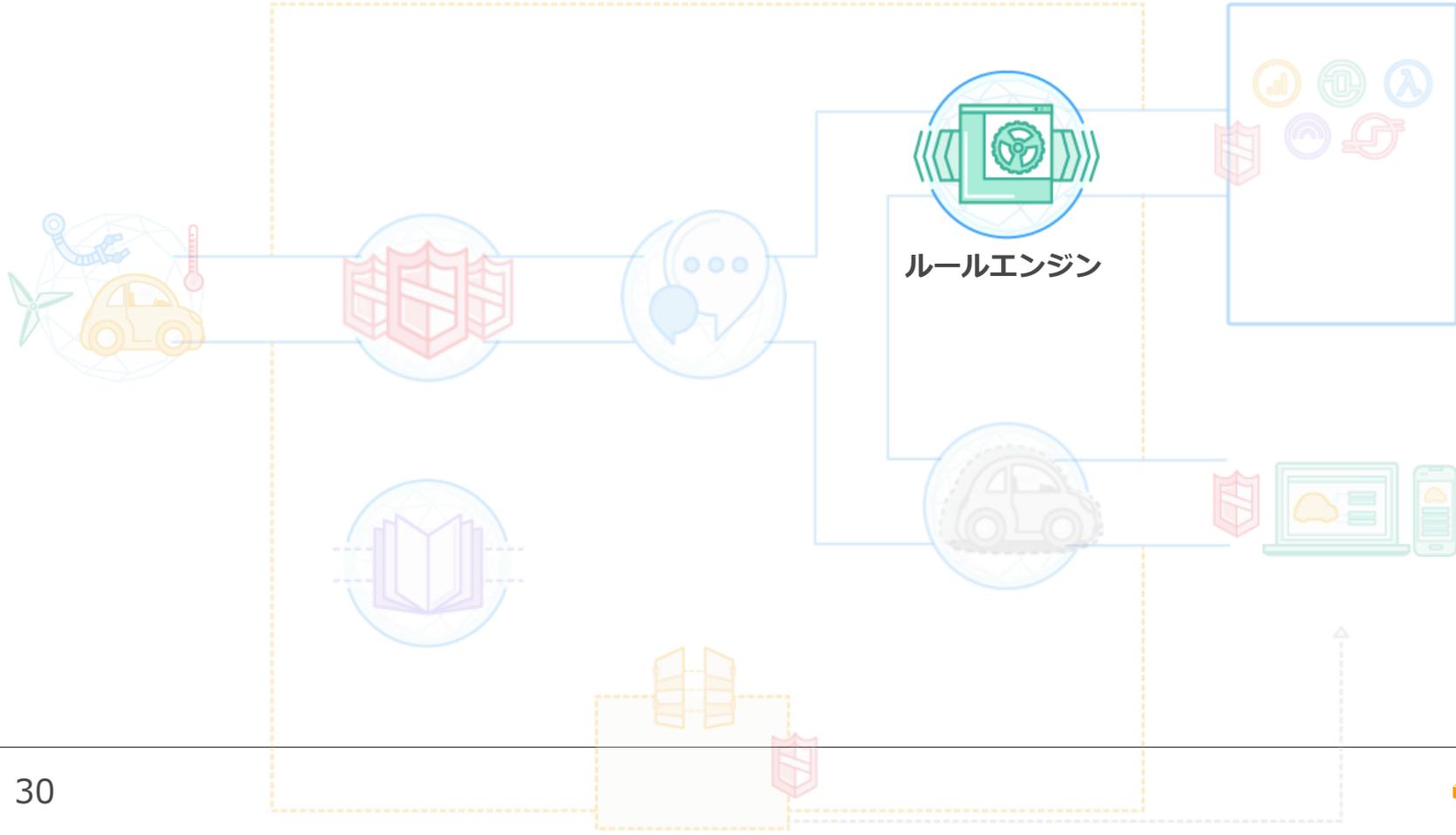
証明書にアタッチ

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iot:Publish"],
    "Resource": ["arn:aws:iot:ap-northeast-1-1:123456789012:topic/foo/bar"]
  }, {
    "Effect": "Allow",
    "Action": ["iot:Connect"],
    "Resource": ["*"]
  }
]
```

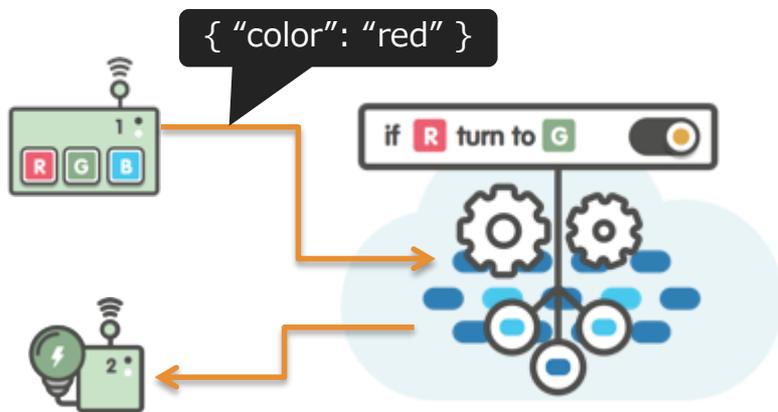
AWS IoT全体のセキュリティ



ルールエンジン



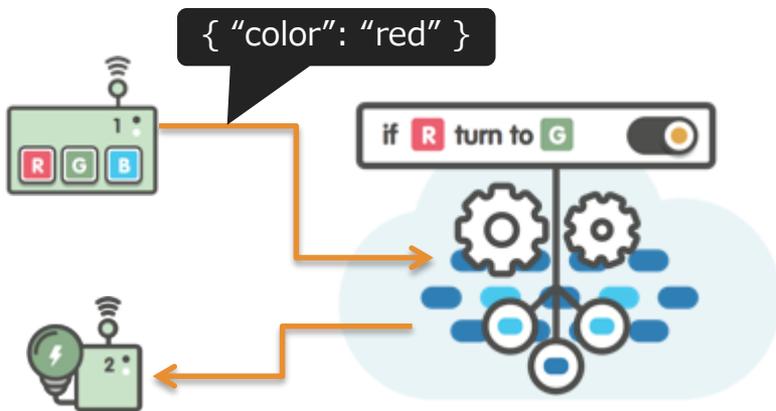
ルールエンジン



- シンプル&慣れた構文
 - ・ SQL文を使ったトピックのフィルタ
 - ・ オプションのWHERE句で条件を記述することが可能
 - ・ JSONサポート
- メッセージ変換機能
 - ・ 文字列操作 (正規表現サポート)
 - ・ 算術計算
 - ・ コンテキストベースのヘルパー
 - ・ 暗号
 - ・ UUID, Timestamp, 乱数など。

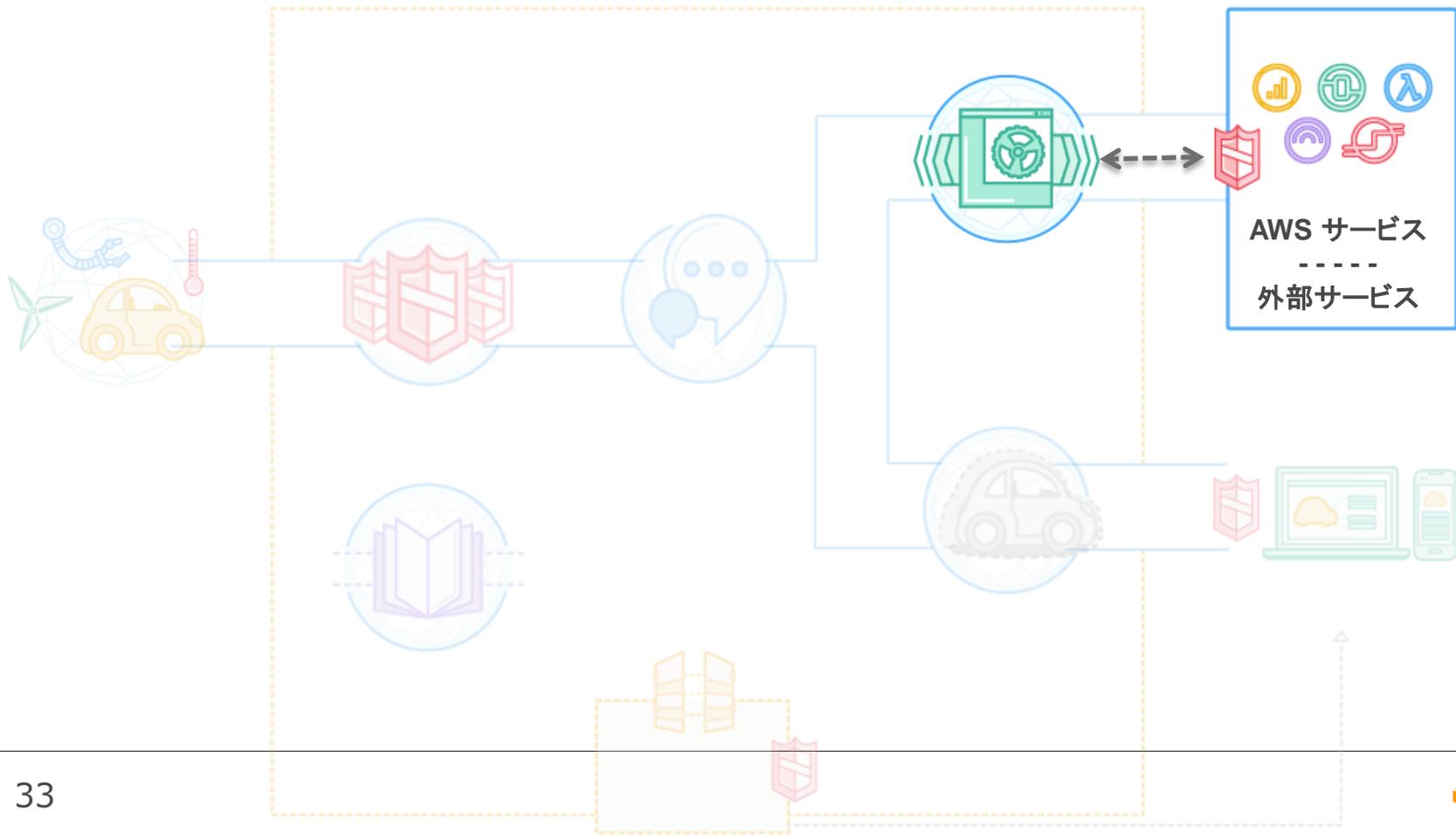
```
SELECT * FROM 'things/thing-2/color'  
WHERE color = 'red'
```

ルールエンジン



```
SELECT *, clientId() as MQTTClientId
FROM 'one/rule'
WHERE
startsWith(topic(2), 'Vac123') AND
(state = 'SWEEP' OR bin.size < 30)",
"actions":
[
  {
    "republish": {
      "topic":
        "controllers/${substring(topic(3),
          3, 5)}",
    }
  }
]
```

ルールエンジンのアクション



ルールエンジンのアクション

AWS IoTからAWSサービス/
外部のエンドポイントの
呼び出しを行なう

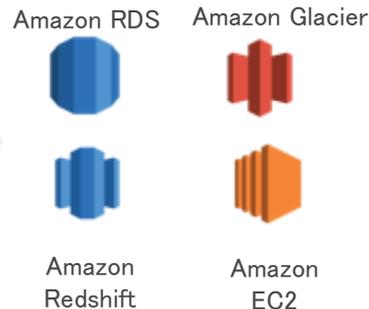


アクション

1. AWS サービス (直接連携可能)



2. その他のAWS (Amazon Kinesis, AWS Lambda, Amazon S3などのサービスを経由)



3. 外部のエンドポイント (Lambda and SNSを経由)

直接連携できるAWSのサービス



ルールエンジンは、AWS IoTにPublishされたメッセージを評価し、メッセージの変換後にルールに基づいて適切なエンドポイントにメッセージを配信

外部のエンドポイント呼び出しはLambdaかSNSを利用



アクション



Lambda functionの呼び出し



S3 bucketへのデータ格納



DynamoDBテーブルへの挿入、更新と読み出し



SNS Topicまたは、Endpointに対するパブリッシュ



Kinesis streamへのパブリッシュ

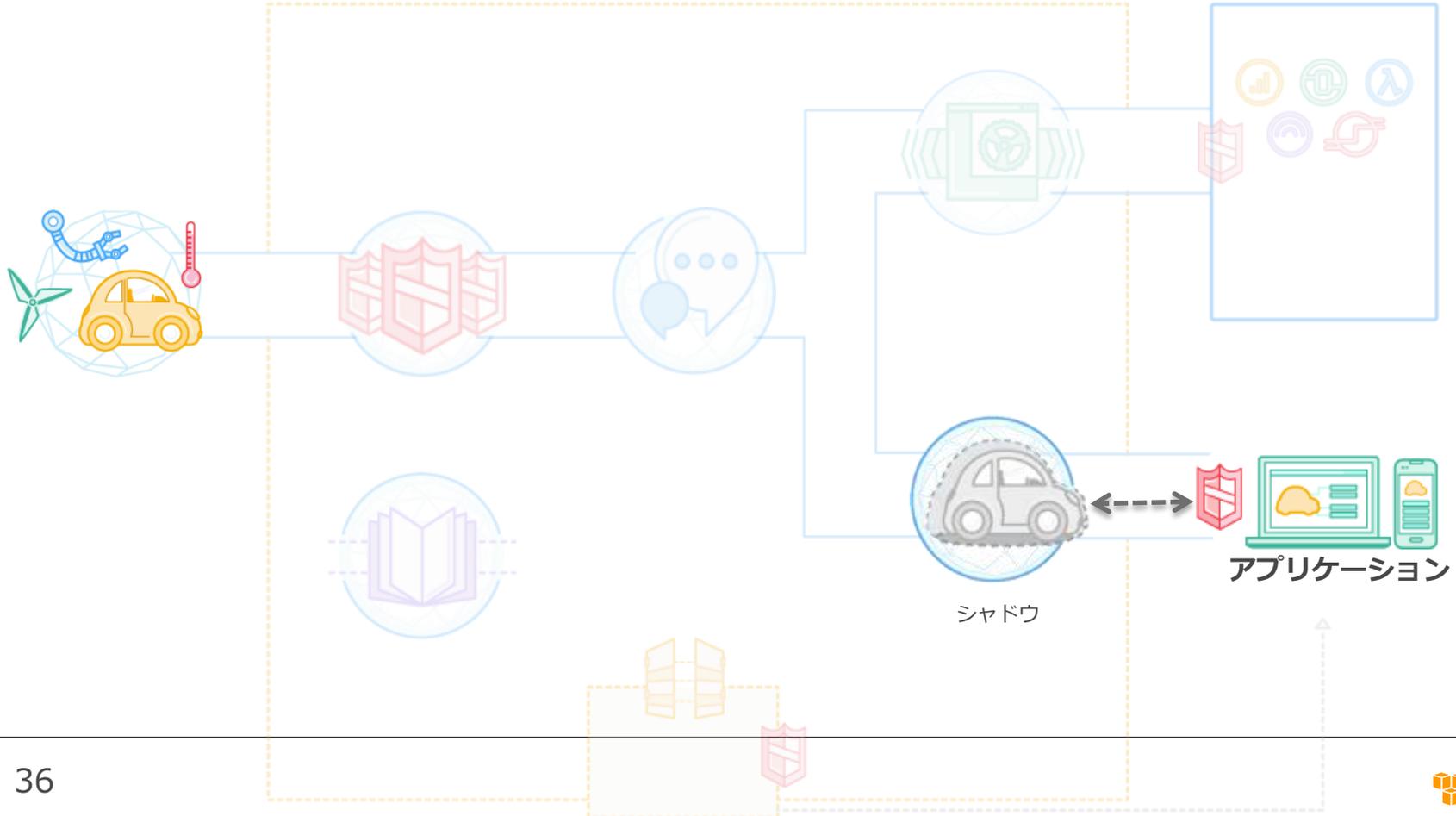


Amazon Firehoseへのパブリッシュ



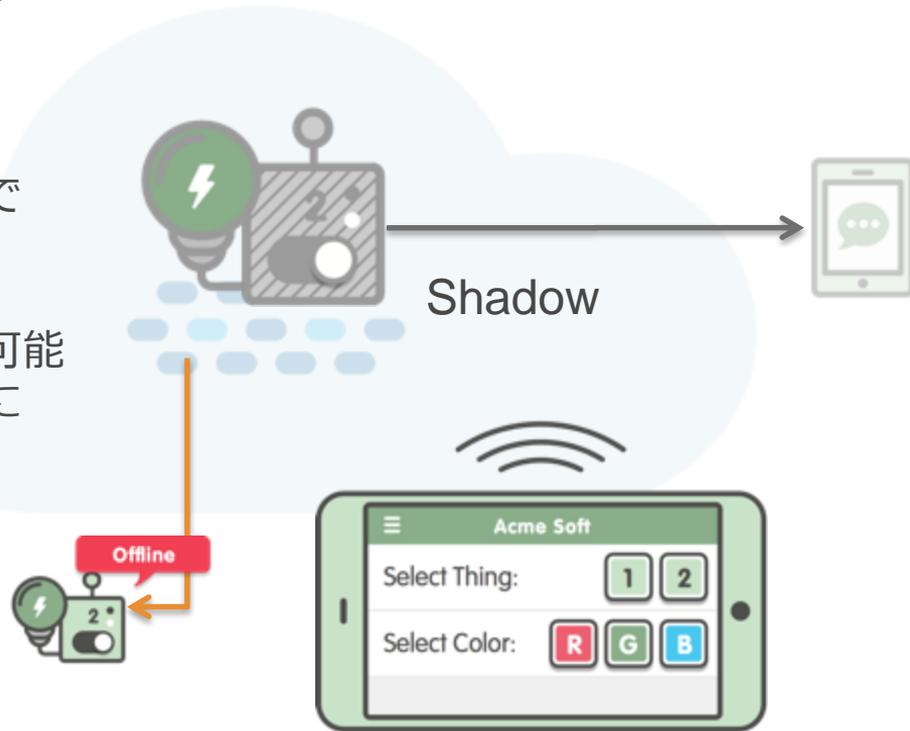
AWS IoTへのリパブリッシュ

デバイス シャドウ



デバイス シャドウ

- デバイスの現在のステータス、アプリケーションから要求されたステータスを管理するJSONドキュメント
- デバイスの影（シャドウ）として振る舞うことでクラウド上で仮想デバイス
- アプリケーションからの要求をデバイスに通知可能（デバイスがオフラインでも次回オンライン時にデバイスに通知）
- ドキュメントはAWS IoT上で管理され、APIやSDKで操作可能



AWS IoT Device Shadows



Read Last
Reported State

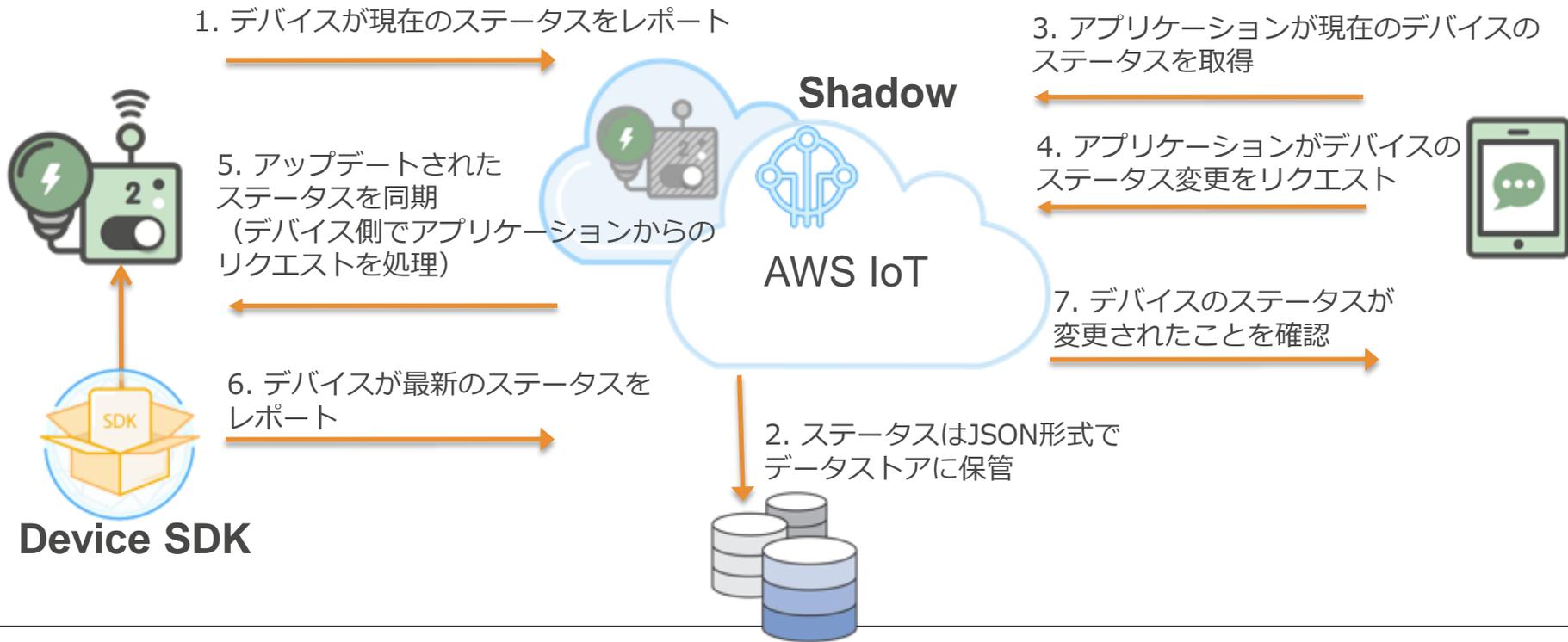


Set Desired
Future State

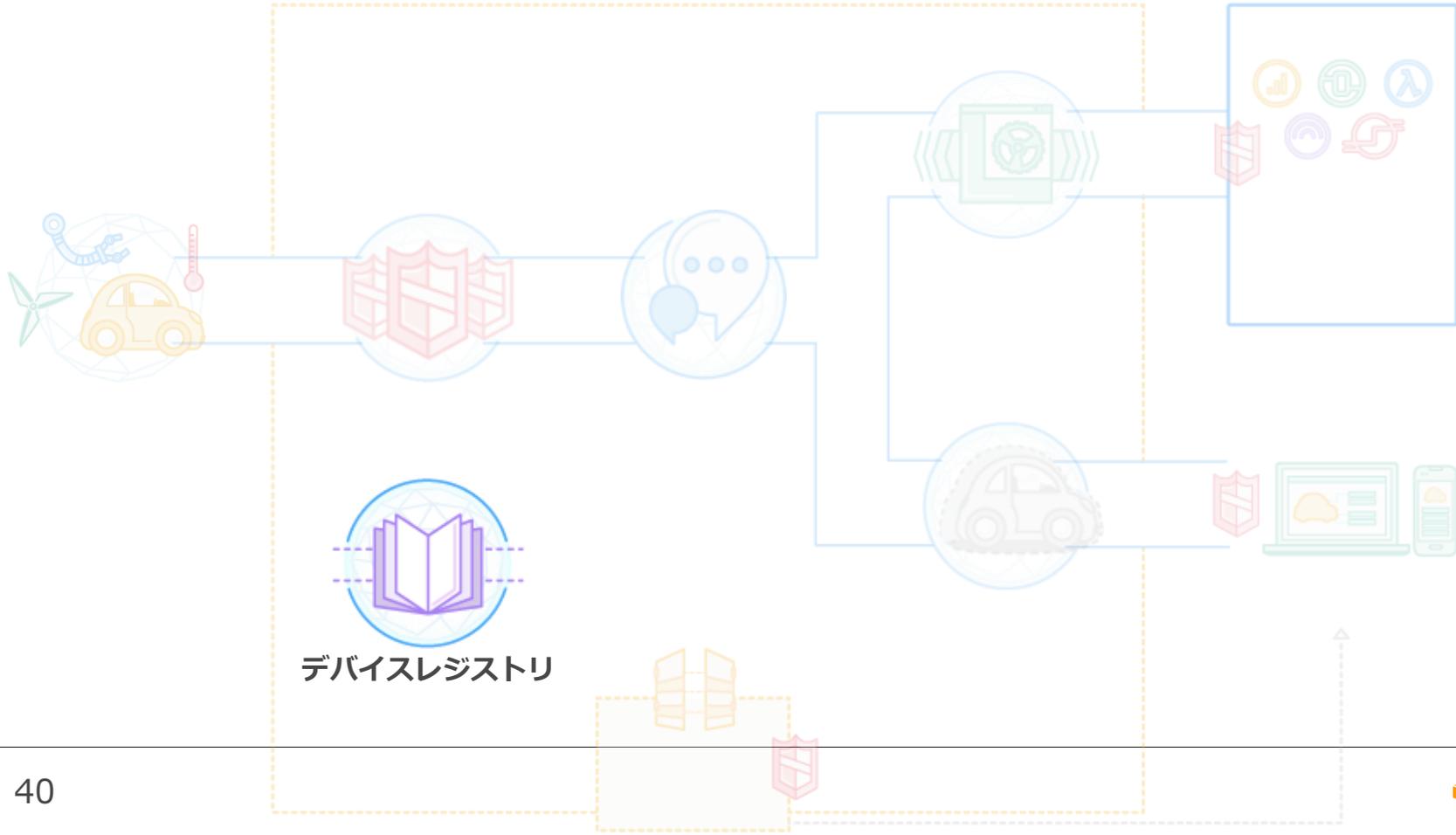


Via RESTful
API

デバイス シャドウの動作フロー



デバイスレジストリ

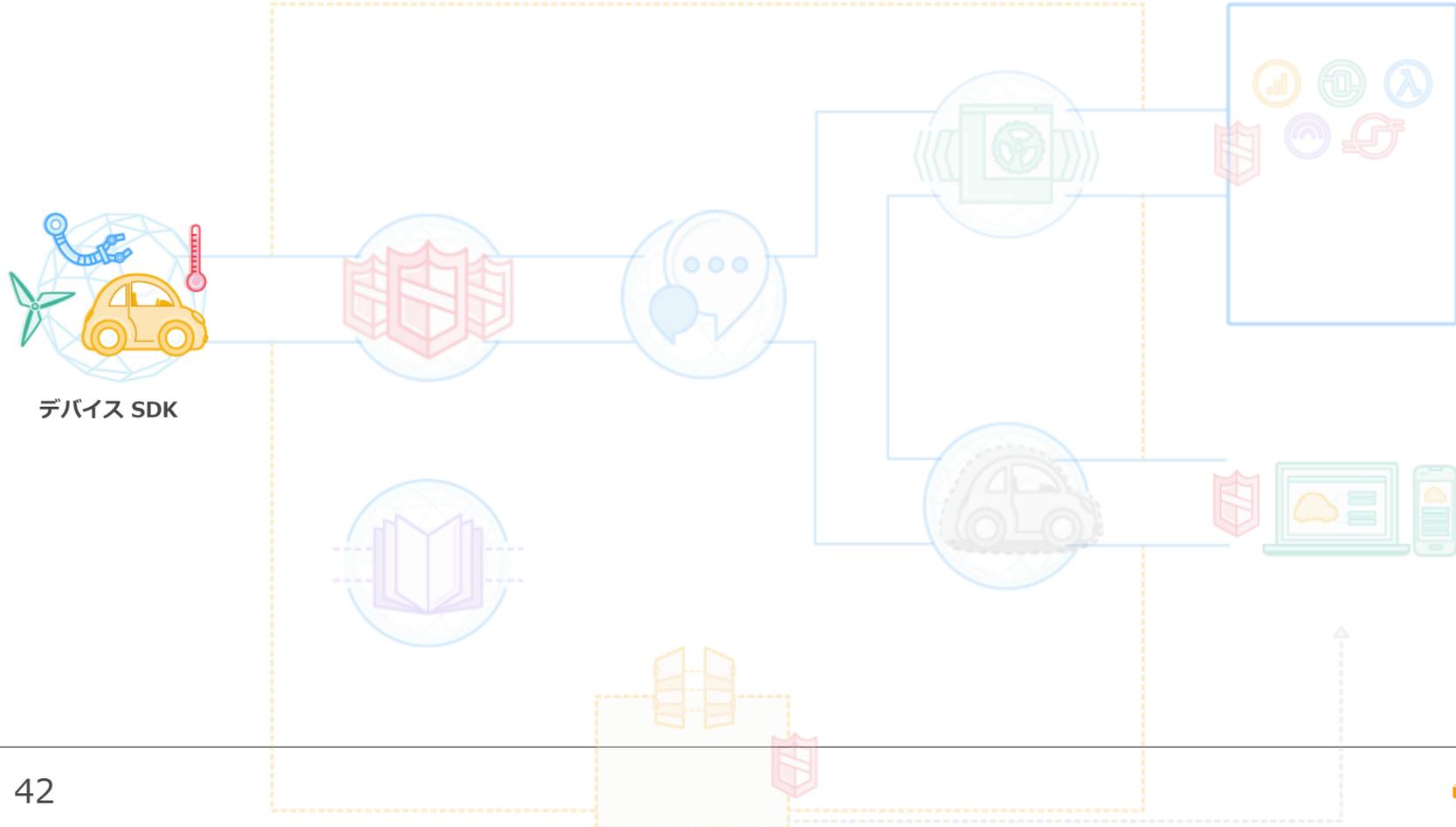


デバイスレジストリ



- key: value
 - ファームバージョンやシリアル番号など
- サポートやメンテナンス目的で利用
 - マニュアルのURLやリファレンス番号
- 外部システム連携でも利用可能

デバイスSDK



AWS IoT デバイスSDK

- AWS IoTが提供しているデバイス向けのSDK
- C/Arduino Yun/Javascript(node.js)に対応
- AWS IoTを利用するための以下の機能を提供
 - メッセージブローカーとの双方向接続のためのTLS1.2セキュリティクレデンシャルの設定
 - MQTTコネクションの管理
 - 汎用MQTTクライアントライブラリのラップ (Publish/Subscribe)
 - デバイスシャドウの各種オペレーション



C-SDK

(Ideal for embedded OS)



JS-SDK

(Ideal for Embedded Linux Platforms)



Arduino Library

(Arduino Yun)

http://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/iot-device-sdk.html

AWS IoT Hardware Program

AWS IoT Hardware Programは、AWSユーザーがハードウェアプラットフォームを使ってコネクテッドプロダクトを作るときに役立ちます。

IoT Hardware パートナーは、AWSに必要なツールやSDKなどを提供することで、エンドユーザー様の時間を削減でき、結果として顧客満足度をあげることができます。

このProgramは、ハードウェア(semiconductors, connectivity modules, sensors, actuators)を提供しているパートナー様向けに設計されております。

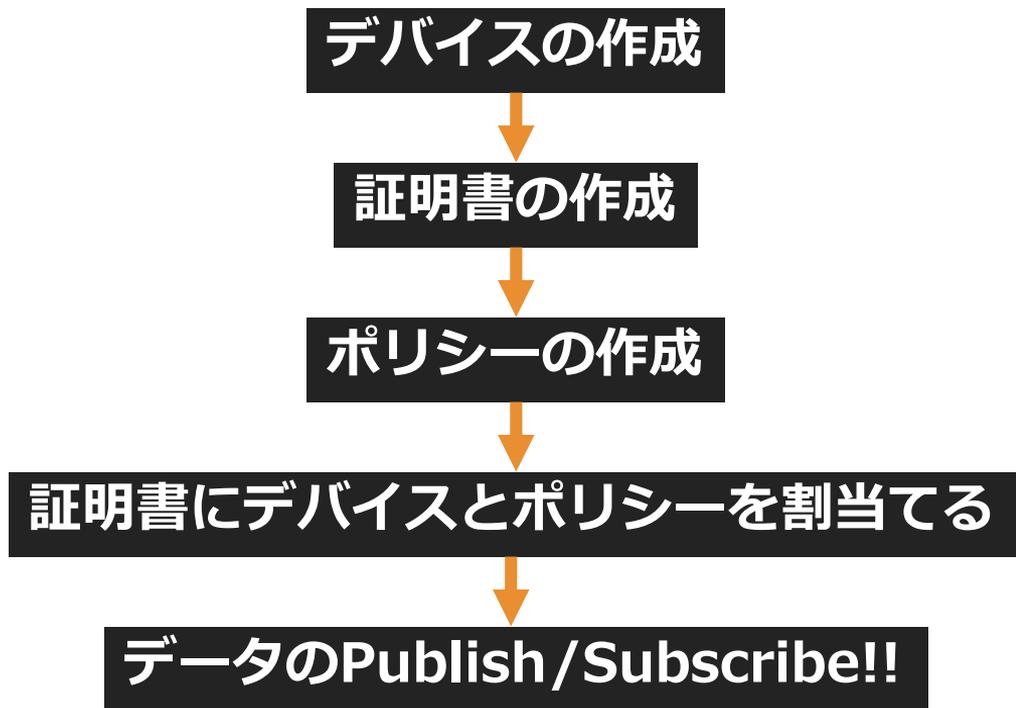


Login to the APN Portal

Apply for IoT Hardware Partner Program

Find AWS IoT Hardware Partners

AWS IoTを使うための手順



AWS IoTをクリック

Amazon Web Services

Compute

-  **EC2**
Virtual Servers in the Cloud
-  **EC2 Container Service**
Run and Manage Docker Containers
-  **Elastic Beanstalk**
Run and Manage Web Apps
-  **Lambda**
Run Code in Response to Events

Developer Tools

-  **CodeCommit**
Store Code in Private Git Repositories
-  **CodeDeploy**
Automate Code Deployments
-  **CodePipeline**
Release Software using Continuous Delivery

Management Tools

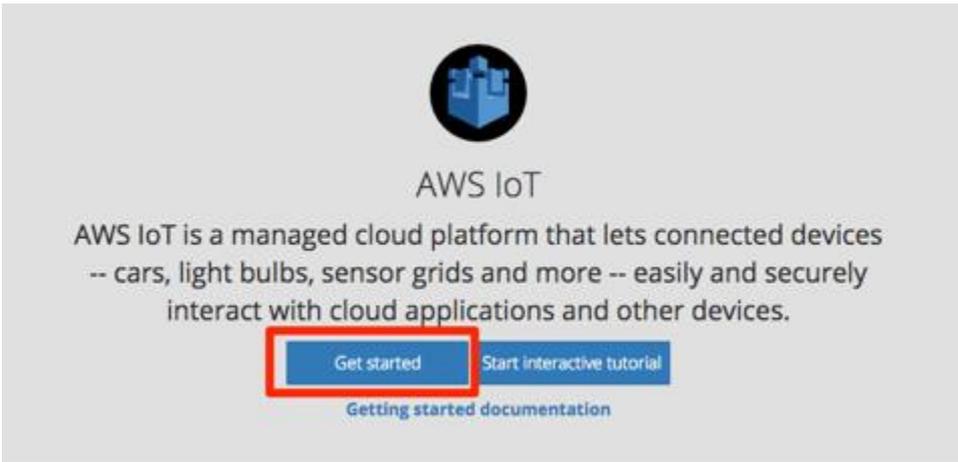
 **CloudWatch**

Internet of Things

-  **AWS IoT** BETA
Connect Devices to the cloud

Mobile Services

-  **Mobile Hub** BETA
Build, Test, and Monitor Mobile apps
-  **Cognito**
User Identity and App Data Synchronization
-  **Device Farm**



The image shows a landing page for AWS IoT. At the top center is the AWS IoT logo, which consists of a blue cube icon inside a black circle. Below the logo, the text "AWS IoT" is displayed in a large, dark font. Underneath, a paragraph reads: "AWS IoT is a managed cloud platform that lets connected devices -- cars, light bulbs, sensor grids and more -- easily and securely interact with cloud applications and other devices." At the bottom of the page, there are two blue buttons: "Get started" and "Start interactive tutorial". The "Get started" button is highlighted with a red rectangular border. Below the buttons, the text "Getting started documentation" is visible in a smaller, lighter font.

デバイスを作成

AWS IoT

Resources | Tutorial

Resources

Create a thing

Create a thing to represent your device in the cloud. This step creates an entry in the thing registry and also a thing shadow for your device.

Name

Attributes

Next (optional), you can use thing attributes to describe the identity and capabilities of your device. Each attribute is a key-value pair.

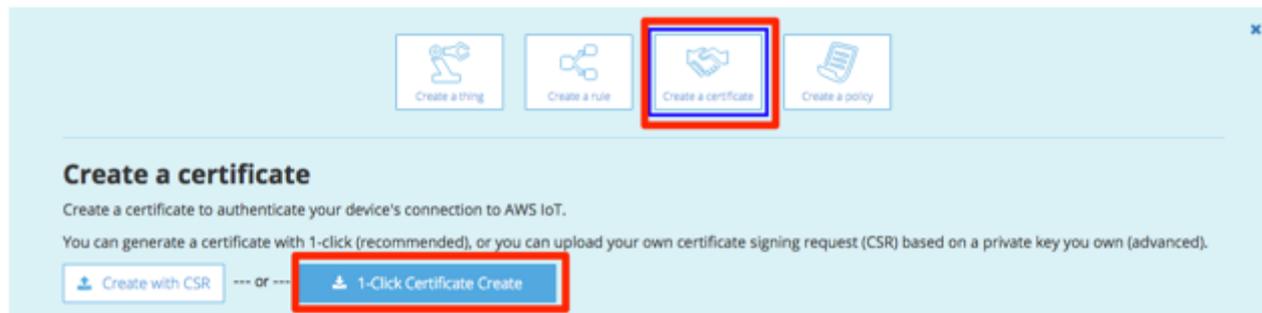
Attribute Key Value



証明書を作成（1クリック）

Resources

✕ Close create panel



Create a thing Create a rule **Create a certificate** Create a policy

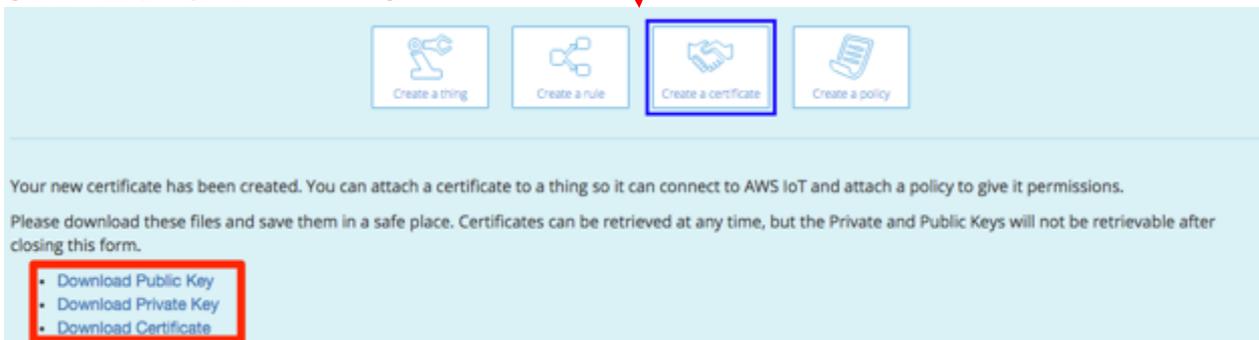
Create a certificate

Create a certificate to authenticate your device's connection to AWS IoT.

You can generate a certificate with 1-click (recommended), or you can upload your own certificate signing request (CSR) based on a private key you own (advanced).

[Create with CSR](#) --- or --- **[1-Click Certificate Create](#)**

3つのファイルをダウンロード



Create a thing Create a rule **Create a certificate** Create a policy

Your new certificate has been created. You can attach a certificate to a thing so it can connect to AWS IoT and attach a policy to give it permissions.

Please download these files and save them in a safe place. Certificates can be retrieved at any time, but the Private and Public Keys will not be retrievable after closing this form.

- [Download Public Key](#)**
- [Download Private Key](#)**
- [Download Certificate](#)**

証明書の作成(自前のCSR)

```
$ openssl genrsa -out privatekey.pem 2048
```

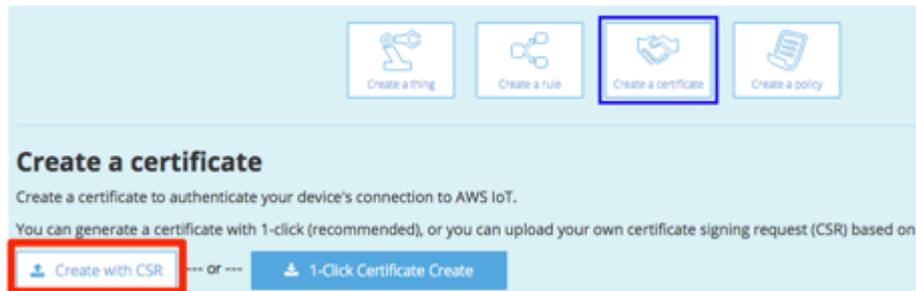
```
$ openssl req -new ¥
```

```
-subj "/C=JP/ST=Tokyo/L=Meguro/O=Amazon Web Services Japan K.K./CN=AWS IoT Certificate" \
```

```
-key privatekey.pem ¥
```

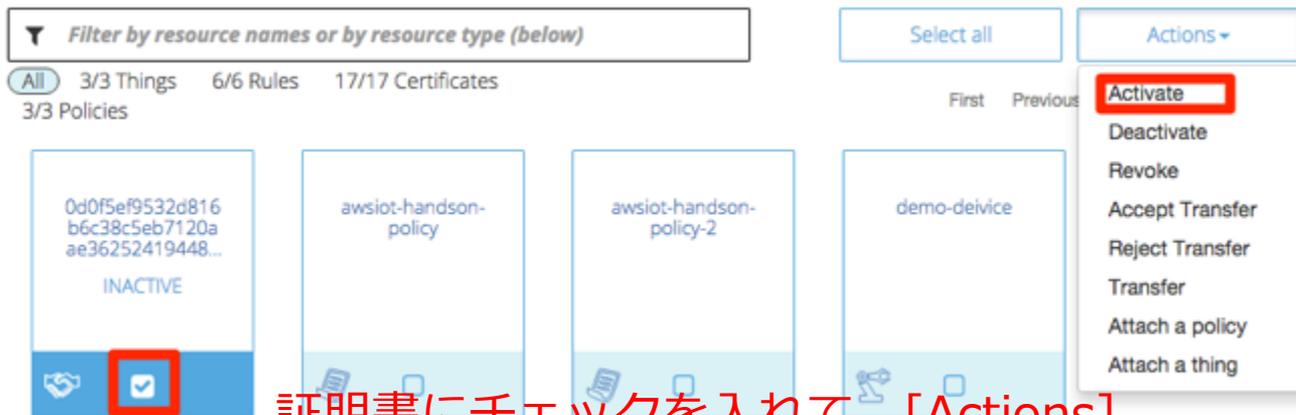
```
-out cert.csr
```

プライベートキーとCSRを作成



CSRをアップロード

証明書の有効化とルート証明書のダウンロード



証明書にチェックを入れて、[Actions] から[Activate]をクリック

以下のリンクからルート証明書をダウンロード。

<https://www.symantec.com/content/en/us/enterprise/verisign/roots/VeriSign-Class%203-Public-Primary-Certification-Authority-G5.pem>

ポリシーの作成

Create a policy

Name: awsiot-handson-policy

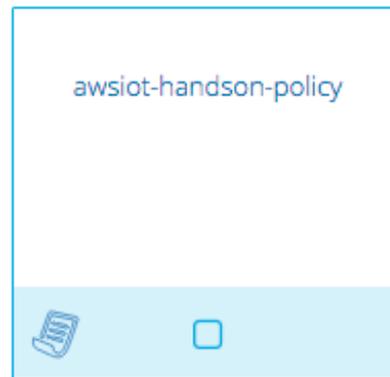
Action: iot:*

Resource: *

Allow Deny

Add Statement

Create



デバイスに与える権限を記述

証明書にポリシーを割り当てる

The screenshot shows the AWS IAM console interface. At the top, there is a filter bar with the text "Filter by resource names or by resource type (below)". Below the filter bar, there are tabs for "All", "1/1 Things", "0/0 Rules", "1/1 Certificates", and "1/1 Policies". The "Certificates" tab is selected. Below the tabs, there are three certificate cards. The middle card, with ID "b879c586ab31eb3763800454d1afe15e89d183bc2647bb...", is selected and has a red box around its bottom-right corner where a checkmark icon is located. To the right of the certificates, there is a "Select all" button and an "Actions" dropdown menu. The "Attach a policy" option in the dropdown menu is highlighted with a red box. A red arrow points from the "Attach a policy" option down to the "Attach policy to the following certificates:" section below.

証明書にチェックを入れて、[Actions]
から[Attach a policy]をクリック

Attach policy to the following certificates:
• b879c586ab31eb3763800454d1afe15e89d183bc2647bb568a0a74ff56dfe583

Policy Name

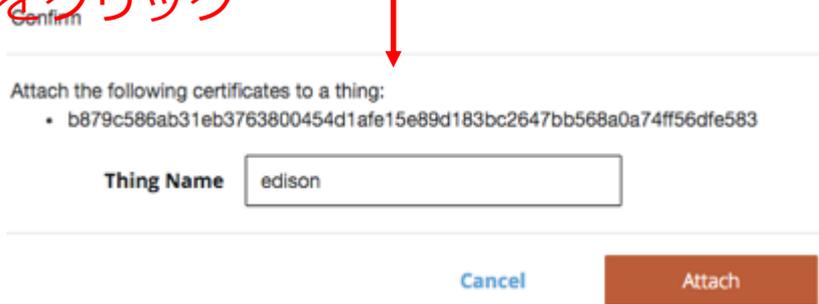
Cancel

Attach

証明書にデバイスを割り当てる



証明書にチェックを入れて、[Actions] から[Attach a thing]をクリック



データをPublish/Subscribeしてみる (mosquittoクライアント)

privatekey.pem: プライベートキー
cert.pem: 証明書
rootca.pem: ルート証明書

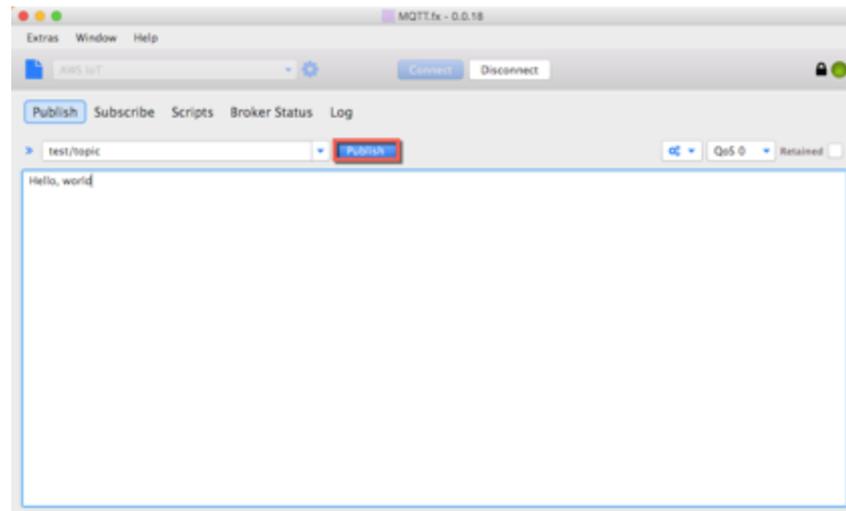
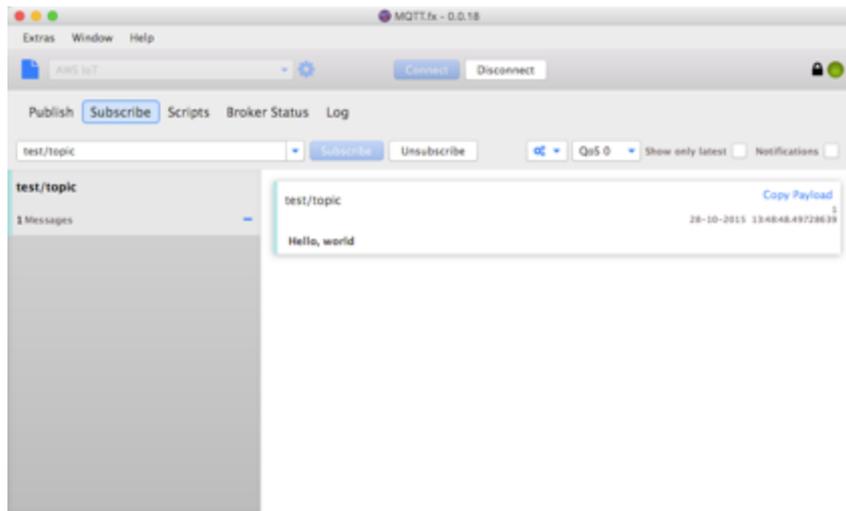
Subscribe

```
$ mosquitto_sub --cafile "rootca.pem" --cert "cert.pem" --key "privatekey.pem" ¥  
-h "data.iot.ap-northeast-1.amazonaws.com" -p 8883 -q 1 -d -t 'test/topic'
```

Publish

```
$ mosquitto_pub --cafile "rootca.pem" --cert "cert.pem" --key "privatekey.pem" ¥  
-h "data.iot.ap-northeast-1.amazonaws.com" -p 8883 -q 1 -d -t 'test/topic' ¥  
-m 'hogehoge'
```

データをPublish/Subscribeしてみる(MQTT.fx)



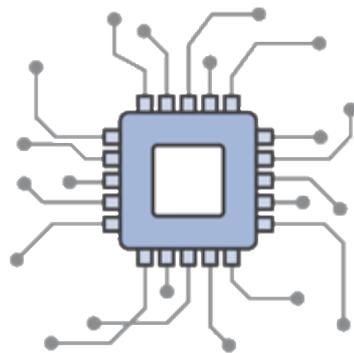
http://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/verify-pub-sub.htm

アジェンダ

📦 Amazon Web Services(AWS)最新情報

📦 AWS IoT

📦 まとめ



まとめ

- AWSの助成制度を有効活用しよう
- AWSのデータ転送料金を軽減するにはSINETクラウドサービスがお得

まとめ

- AWS IoTで、IoTに必要な機能を簡単に安全に利用することが可能
- AWSの他のサービスや外部サービスとのシームレスな連携で、分析や制御など様々な処理を組み合わせることが可能
- すぐに簡単にお試し可能

2016年AWSイベントカレンダー お待ちしております！

- **AWS Summit Tokyo**

- Day1 6月1日
- Day2,3 6月2日-3日 一般セッション

- AWS Public Sector Summit

- 6月20日、Washington DC

- AWS Public Sector Summit

- 8月3日、Canberra

2016年も開催します！

re:Invent 2016

2016年11月29日~12月2日

ベネチアンホテル@ラスベガス



參考資料 – re:Invent 2015(初級)

(MBL203)From Drones to Cars

<http://www.slideshare.net/AmazonWebServices/mb1203-drones-to-cars-connecting-the-devices-in-motion-to-the-cloud>

<https://www.youtube.com/watch?v=o1cN0KDaOf4>

(MBL204)Connecting the Unconnected

<http://www.slideshare.net/AmazonWebServices/mb1204-state-of-the-union-iot-powered-by-aws>

<https://www.youtube.com/watch?v=0WDiSLVEkYQ>

(MBL205)Everything You Want to Know About AWS IoT

<http://www.slideshare.net/AmazonWebServices/mb1205-new-everything-you-want-to-know-about-aws-iot>

<https://www.youtube.com/watch?v=OvoIh9ENxdM>

參考資料 – re:Invent 2015(中級)

(MBL302)Build Scalable, Serverless Mobile & IoT Back Ends with AWS Lambda

<http://www.slideshare.net/AmazonWebServices/mb1302-scalable-serverless-mobile-iot-backendsporate-it-into-a-consumerfacing-device>
<https://www.youtube.com/watch?v=GnaO-LwdSuU>

(MBL303)Build Mobile Apps for IoT Devices and IoT Apps for Mobile Devices

<http://www.slideshare.net/AmazonWebServices/mb1303-build-mobile-apps-for-iot-devices-and-iot-apps-for-devices>
<https://www.youtube.com/watch?v=IUXFVJbDtUY>

(MBL305)You Have the Data from Your Devices – Now What?

<http://www.slideshare.net/AmazonWebServices/mb1305-you-have-data-from-the-devices-now-what-getting-the-value-of-the-iot>
<https://www.youtube.com/watch?v=2LHsfmfKLL0>

(MBL311)Securely Thinging Across the Internet With AWS

<http://www.slideshare.net/AmazonWebServices/mb1311-new-aws-iot-securely-building-provisioning-using-things>
https://www.youtube.com/watch?v=G-kJxzd_NA8

(MBL312)AWS IoT Deep Dive – Programming the Physical World with Shadows and Rules

<http://www.slideshare.net/AmazonWebServices/mb1312-new-aws-iot-programming-a-physical-world-w-shadows-rules>

(MBL313)Understanding Hardware Platforms, Devices SDKs and Protocols

<http://www.slideshare.net/AmazonWebServices/mb1313-new-aws-iot-understanding-hardware-kits-sdks-protocols>
<https://www.youtube.com/watch?v=rMiplPiU2nI>