

# "売れば売るほど大変" を防ぐ! 「IoT デバイス初期設定の工数削減」手法

---

株式会社ソラコム テクノロジー・エバンジェリスト  
松下 享平 (ma2shita@soracom.jp / Max)

2018/11/22

# 自己紹介

株式会社ソラコム / テクノロジー・エバンジェリスト

## 松下 享平 (まつした こうへい) “Max”

静岡県民 ▲ 新幹線通勤族 🚄

経歴: 東証二部ハードウェア・メーカーで  
情シス, EC 事業, 調達部門長, IoT 事業開発 → 現職

登壇数 190以上、保有スライド枚数 7500枚以上

好きなソラコムサービス

- SORACOM Air メタデータサービス
- SORACOM Funnel
- soracom-cli

Facebook, Twitter: [ma2shita](#)



# カリフォルニア州でデバイスのデフォルトパスワードを禁ずる法律が成立

セキュリティ向上のため

良いニュースだ!

California州が2020年から、すべての新しい消費者電子製品に、"admin", "123456", あるいは古くからお馴染みの"password"といった、デフォルトのパスワードを設けることを禁ずる法律を成立させた。

良い事じゃん!

生産や物流の現場で  
一か月働きなさい

生産や出荷の現場  
オタ \ (^o^) / オタ  
どうしよう...

あなたが正解

そんなの関係ねえ

次は  
法廷で会いましょう

<https://aws.amazon.com/jp/blogs/news/aws-iot-core-ats-endpoints/>

Amazon Web Services ブログ

## AWS IoT Core がお客様に提供する Symantec の認証局無効化の対応方法

by AWS Japan Staff | on 30 AUG 2018 | in AWS IoT Platform, Internet Of Things | Permalink | [Share](#)

エンドポイント URL を変更(必須)し  
新しい CA ファイルを(追加で)インストールしなければならない

だからクラウドは (略

あなたのサーバや  
謎クラウドも  
対象ですよ

もう売っちゃったよ  
オタ \ (^o^ ) / オタ  
どうしよう...

あなたは正しい

そんなの関係ねえ

また  
法廷で会いましょう

# デバイス「売れば売るほど大変」



売る前

個体毎の設定、顧客毎や出荷先の設定

売った後

サーバとの接続設定変更



クラウドと連携するデバイスって  
売れば売るほど大変

# IoT デバイスは 「クラウドファースト デバイス」



# お客様事例: チカク様



## スマホで撮った 子どもの写真・動画を 実家のテレビへ配信

お年寄りをターゲット。テレビにつなぐ  
だけ。難しい通信設定は不要で不具合  
時も電源の入れなおし。

# トラディショナル デバイスと クラウドファースト デバイス

## トラディショナル デバイス

出荷時が**最高**の状態  
ハードウェア体験が主体

時間と共に**劣化**  
ソフトウェア更新は**無い**

買い替え理由は  
「新しいソフトウェアでないと**困る**」



## クラウドファースト デバイス

出荷時は**最低**の状態  
ソフトウェア体験が主体

時間と共に**成長**  
ソフトウェア更新は**前提**

買い替え理由は  
「新しいハードウェアによる**新たな体験**」



# クラウドファースト デバイスの特徴と課題



# 主な初期設定 — トラディショナル デバイス

## ソフトウェアやコンテンツ

- 公式カスタマイズの他、顧客指定の追加ソフトウェア

## 周辺機器の動作設定

- 標準搭載の I/O や、顧客指定の追加設定

収益になるので  
対応しても OK

## デバイス固有設定

- デバイス ID、デバイス管理用ログイン情報

純粋なコスト

出荷後の事は、考えなくて良かった

# 主な初期設定 – クラウドファースト デバイス

## ソフトウェアやコンテンツ

- 公式カスタマイズその他、顧客指定の追加ソフトウェア  
**クラウド連携用 SDK や実装**

## 周辺機器の動作設定

- 標準搭載の I/O や、顧客指定の追加設定  
**通信機器の設定 (有線、Wi-Fi、BLE、セルラー 等)**

## デバイス固有設定

- デバイス ID、デバイス管理用ログイン情報  
**アクセスキー、接続先設定**

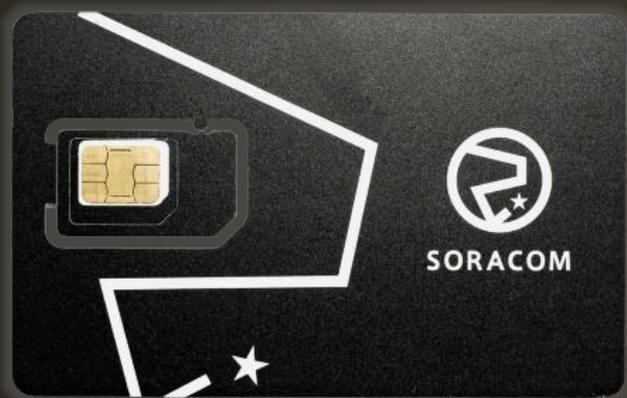
**純粋なコスト**

# 世界でも SORACOM



## SORACOM Air for セルラー

100 を超える国と地域で



カード型 SIM



チップ型 SIM  
(eSIM)



APN 名 "soracom.io"

# お客様事例:ソースネクスト様



POCKETALK



74以上の言語で双方向の  
コミュニケーションを  
実現、クラウド型通訳機

グローバル向け Air SIM  
eSIM内蔵で  
世界105カ国で使える

plan01s eSIM



# 主な初期設定 – クラウドファースト デバイス

## ソフトウェアやコンテンツ

- 公式カスタマイズその他、顧客指定の追加ソフトウェア  
**クラウド連携用 SDK や実装**

## 周辺機器の動作設定

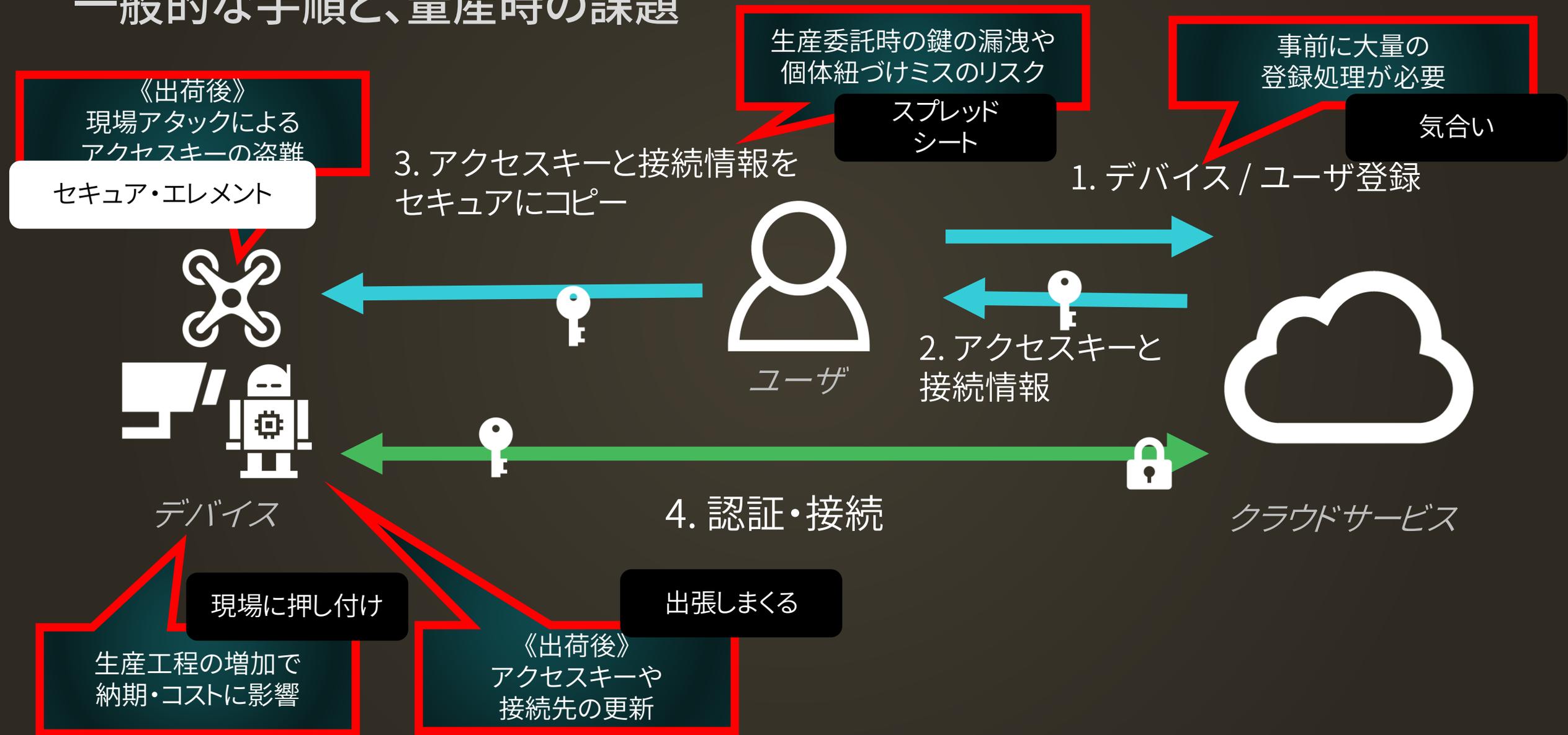
- 標準搭載の I/O や、顧客指定の追加設定  
**通信機器の設定** →

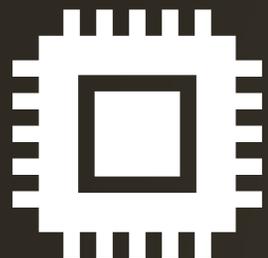
IoT 向けデータ通信サービス  
SORACOM Air

## デバイス固有設定

- デバイス ID、デバイス管理用ログイン情報  
**アクセスキー、接続先設定**

# デバイスをクラウドサービスに接続する 一般的な手順と、量産時の課題





情報を安全に格納するメモリや、暗号化を補助するロジックや乱数生成が実行可能なモジュール

ハードウェア的な特性《耐タンパー性》

- 物理的な破壊によって内部情報が消滅

ソフトウェア的な特性《厳重なアクセス制御》

- 決められた手続きでのみ内部情報にアクセス可能

読み書きや複製が  
極めて困難

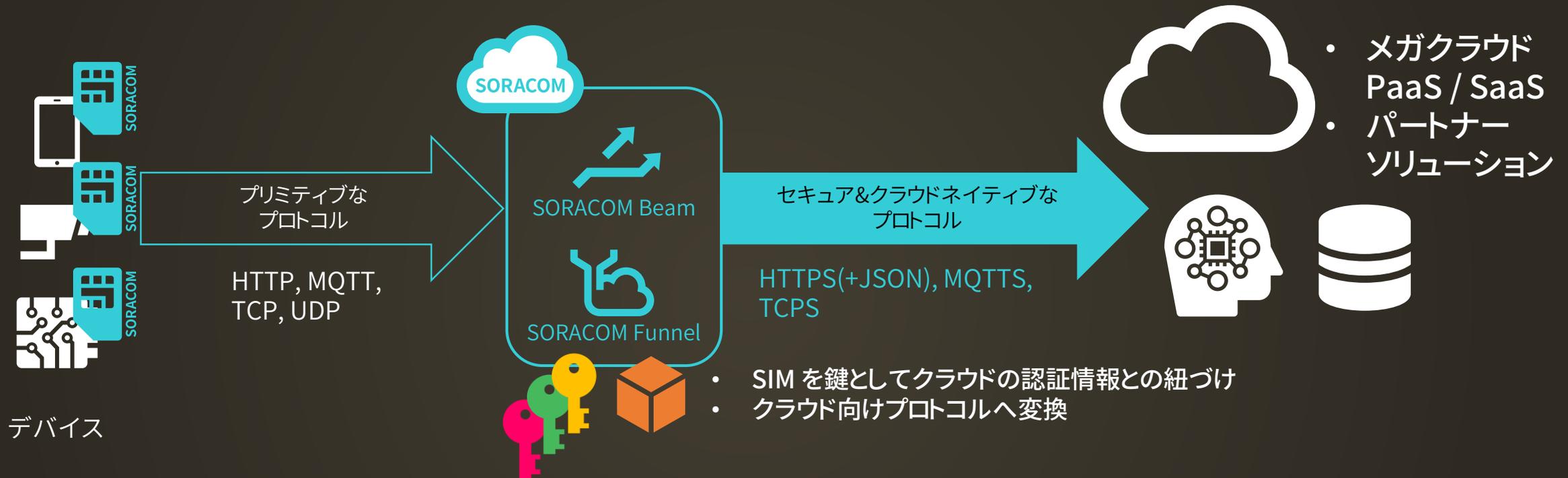


SIM もセキュア・エレメント



SIM を「鍵」として  
活用できる

# SORACOM Beam / Funnel による デバイス開発の工数削減



SDK やアクセスキー、接続情報を  
デバイスから取り除ける

# 主な初期設定 – クラウドファースト デバイス

## ソフトウェアやコンテンツ

- 公式カスタマイズその他、顧客指定の追加ソフトウェア  
**クラウド連携用 SDK や実装** →

データ転送サービス  
SORACOM Beam  
クラウド・アダプタ  
SORACOM Funnel

## 周辺機器の動作設定

- 標準搭載の I/O や、顧客指定の追加周辺機器の設定  
**通信機器の設定** →

IoT 向けデータ通信サービス  
SORACOM Air

## デバイス固有設定

- デバイス ID、デバイス管理用ログイン情報  
**アクセスキー、接続先設定** →

データ転送サービス  
SORACOM Beam  
クラウド・アダプタ  
SORACOM Funnel

# 主な初期設定 – クラウドファースト デバイス

## ソフトウェアやコンテンツ

- 公式カスタマイズその他、顧客指定の追加ソフトウェア  
**クラウド連携用 SDK や実装**

データ転送サービス  
SORACOM Beam  
クラウド・アダプタ  
SORACOM Funnel

## 周辺機器の動作設定

- 標準搭載の I/O や、顧客指定の追加周辺機器の設定  
**通信機器の設定**

IoT 向けデータ通信サービス  
SORACOM Air

## デバイス固有設定

- デバイス ID、デバイス管理用ログイン情報  
**アクセスキー、接続先設定**

データ転送サービス  
SORACOM Beam  
クラウド・アダプタ  
SORACOM Funnel

# SORACOM Air メタデータサービス

メタデータとは

通信を行っている SIM 自身の情報



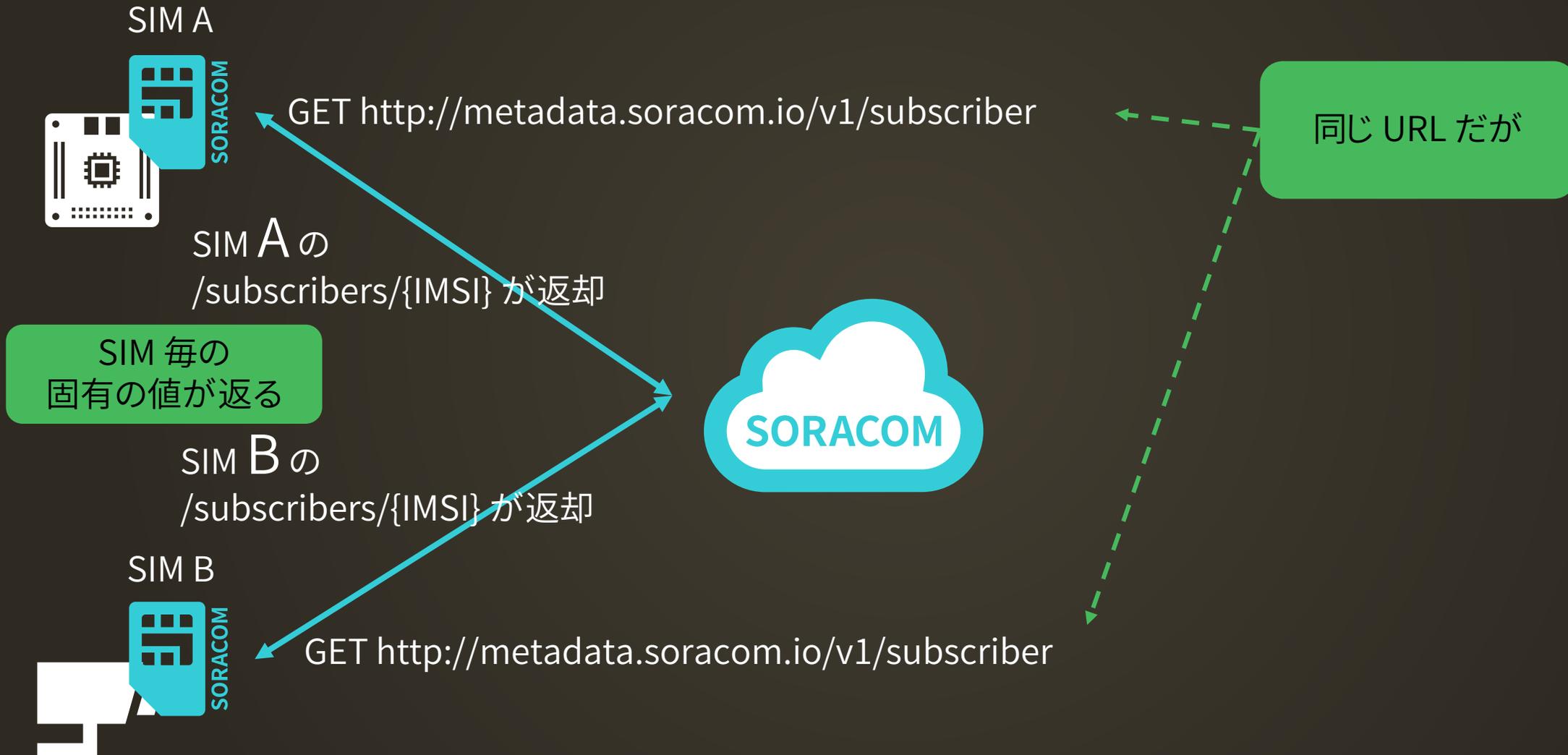
メタデータサービスを使うと、

自身の情報だけは**認証なし**で取得・更新可能

詳しくは開発者サイトにて「SORACOM Air メタデータサービス機能を使用する」をご参照ください

<https://dev.soracom.io/jp/start/metadata/>

# メタデータサービスの認証



# SORACOM Air メタデータサービスで 取得可能なデータ

## タグ

SIM 毎に設定

例)

- ハードウェアに依存しないID  
割り当て
- 動作パラメータ

## ユーザーデータ

グループ毎に設定

例)

- SSH公開鍵
- 暗号化fs復号用鍵
- Bootstrap 用スクリプト

# curl でメタデータを取得する

注意: 単数形

GET metadata.soracom.io/v1/subscriber ←

GET metadata.soracom.io/v1/subscriber.tags

→ application/json で返却される

GET metadata.soracom.io/v1/subscriber.tags.NAME

→ text/plain で返却される ※LF付き

GET metadata.soracom.io/v1/userdata

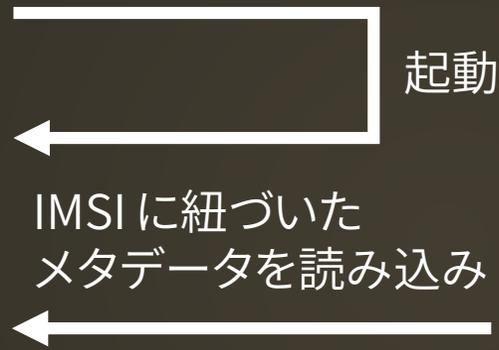
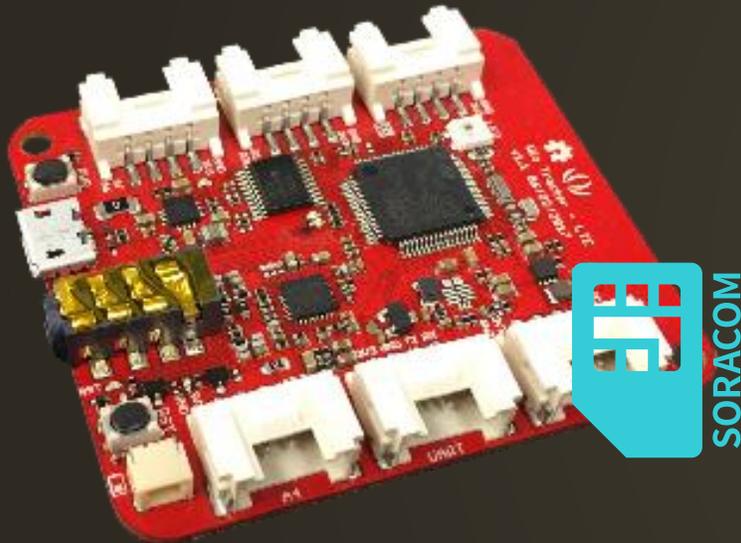
→ グループ共通での値が返却される

# DEMO 1

— SORACOM Air メタデータサービス —

# SORACOM Air メタデータサービス

## — 例) DI パターン



デバイスの初期設定を  
動的にできる

## SORACOM Air メタデータサービス

SIM 詳細

IMSI [REDACTED]

名前 Customer A 

グループ

詳細情報 通信量履歴 タグ 監視 セッション詳細

| タグ名称     | 値                  |
|----------|--------------------|
| DEBUG    | 1                  |
| INTERVAL | 5000               |
| HOST     | harvest.soracom.io |
| PORT     | 8514               |

# メタデータの値で JSON 文字列の活用

```
#include <ArduinoJson.h>

// パラメータをグローバル変数としておき、いろいろな関数から参照できるようにしておく
const char *endpoint_host;
int endpoint_port = 0;
bool debug_flag = false;

void set_params()
{
    /* 例として "conf" というタグに下記JSON文字列を設定
    {"endpoint_host": "harvest.soracom.io", "endpoint_port": 8514, "debug_flag": true}
    */
    char conf_str[2048];
    Wio.HttpGet("http://metadata.soracom.io/v1/subscriber.tags.conf", conf_str, sizeof(conf_str));
    StaticJsonBuffer<2048> jsonBuffer;
    JsonObject &json_root = jsonBuffer.parseObject(conf_str); // 文字列をparse
    // グローバル変数へパラメータを設定する
    endpoint_host = json_root["endpoint_host"]; // テキストはそのままcharで
    endpoint_port = json_root["endpoint_port"].as<int>(); // intとして読み込む
    debug_flag = json_root["debug_flag"].as<bool>(); // boolも可能
}
```

# 主な初期設定 – クラウドファースト デバイス

## ソフトウェアやコンテンツ

- 公式カスタマイズその他、顧客指定の追加ソフトウェア  
**クラウド連携用 SDK や実装** →

データ転送サービス  
SORACOM Beam  
クラウド・アダプタ  
SORACOM Funnel

## 周辺機器の動作設定

- 標準搭載の I/O や、顧客指定の追加周辺機器の設定  
**通信機器の設定** →

IoT 向けデータ通信サービス  
SORACOM Air

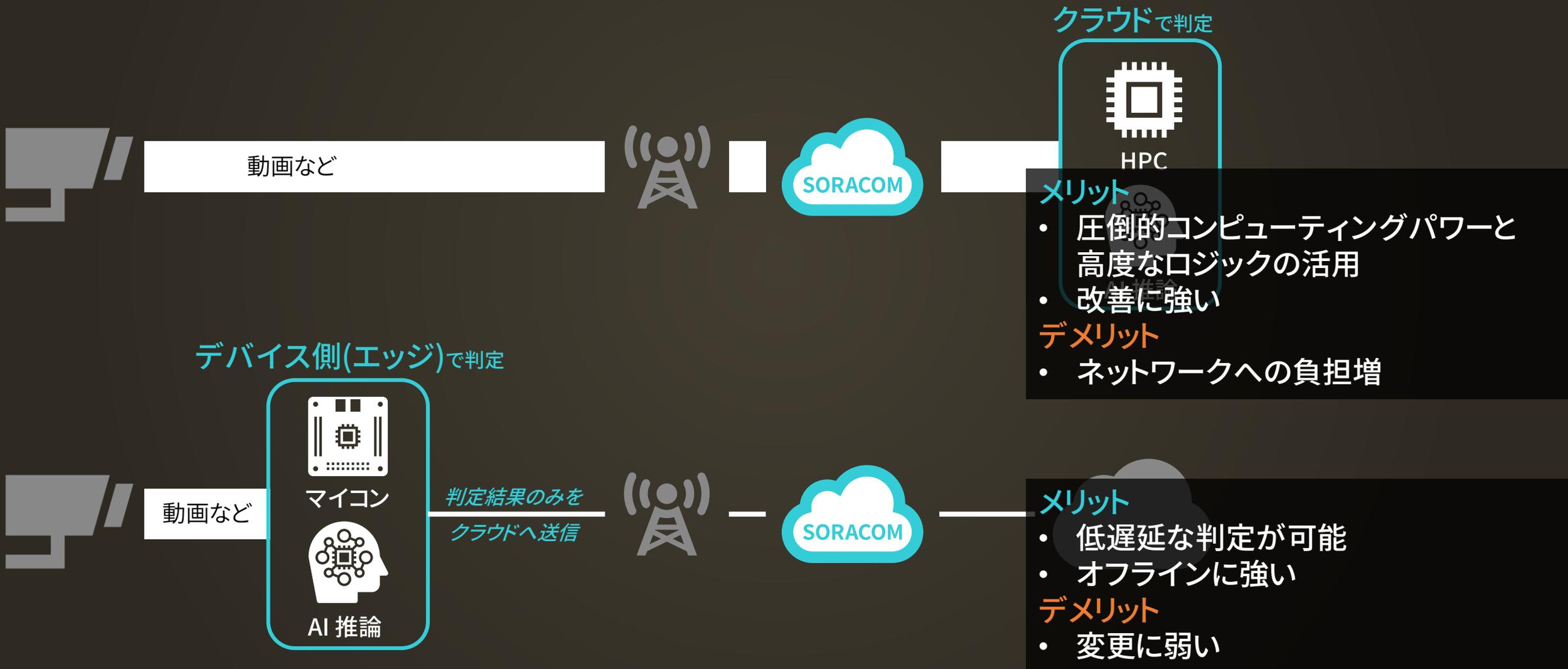
## デバイス固有設定

- デバイス ID、デバイス管理用ログイン情報  
**アクセスキー、接続先設定** →

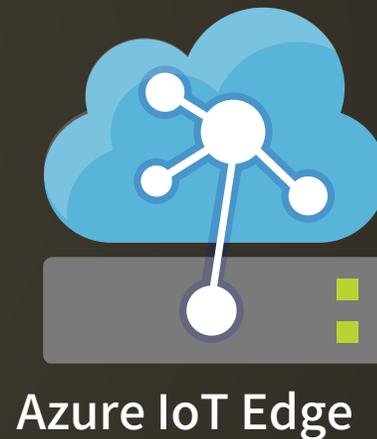
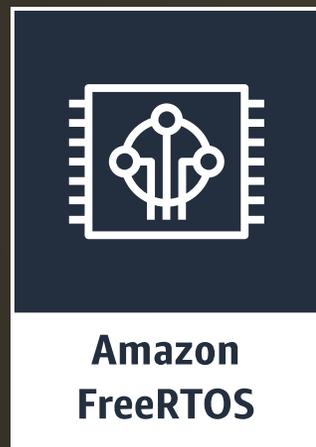
データ転送サービス  
SORACOM Beam  
クラウド・アダプタ  
SORACOM Funnel

# エッジ・コンピューティング

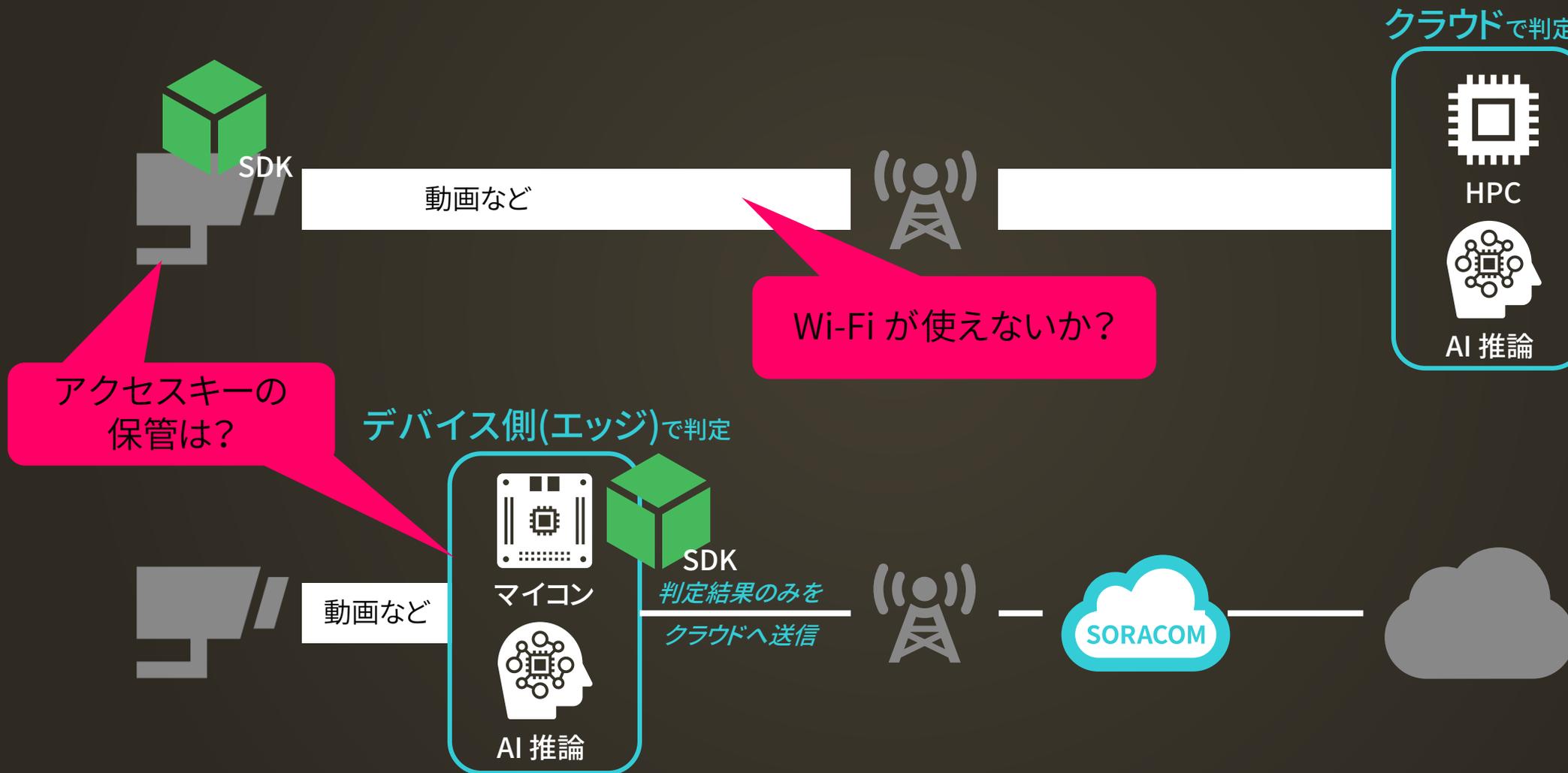
# クラウドコンピューティングと エッジ・コンピューティング



# エッジ・コンピューティングを実現する ミドルウェア

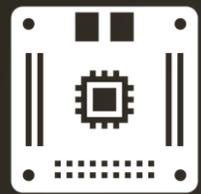


# クラウドコンピューティングと エッジ・コンピューティング



# DEMO 2-1 — 人手による作業

エッジ・コンピューティング  
デバイス



頑張ってコピー



X.509 証明書と  
エンドポイント URL

管理コンソールで作業



X.509 証明書と  
エンドポイント URL

デバイスに接続して、デバイス証明書、プライベートキー、およびルート CA 証明書をコピーする場合は、デバイスのドキュメントを参照してください。

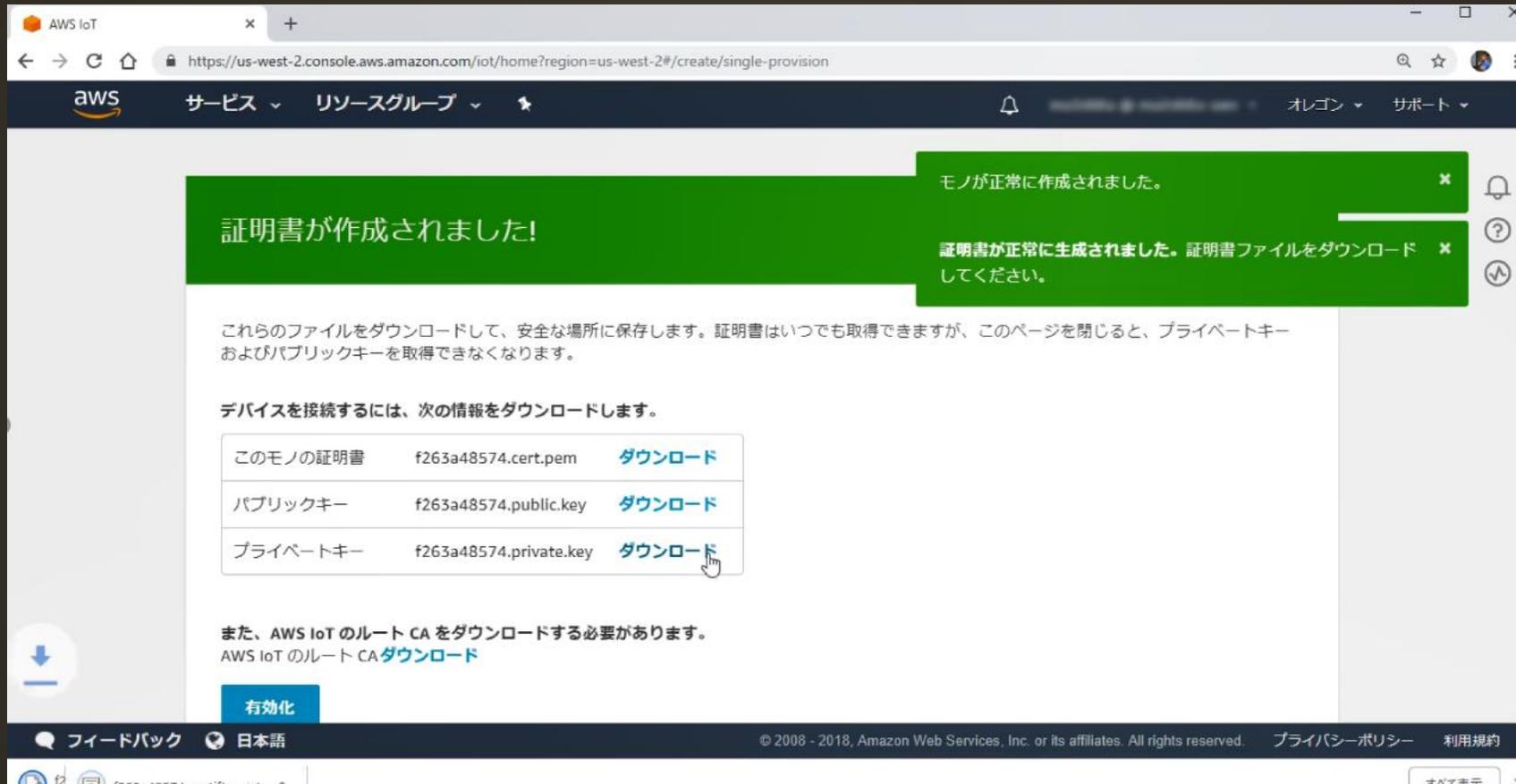
[https://docs.aws.amazon.com/ja\\_jp/iot/latest/developerguide/configure-iot.html](https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/configure-iot.html)

Wi-Fi で AWS IoT Core に接続



AWS IoT Core  
トピック

# AWS IoT Core を手動で設定する (動画)



The screenshot shows the AWS IoT console interface. At the top, there's a navigation bar with the AWS logo and menu items like 'サービス' and 'リソースグループ'. The main content area features a large green confirmation banner that reads '証明書が作成されました!' (Certificate created successfully!). Below this, there's a table with three rows, each representing a certificate file to be downloaded: 'このモノの証明書' (Device certificate), 'パブリックキー' (Public key), and 'プライベートキー' (Private key). Each row includes the filename and a 'ダウンロード' (Download) button. A mouse cursor is pointing at the 'ダウンロード' button for the private key. Below the table, there's a note about downloading the root CA and a '有効化' (Activate) button. The footer contains copyright information and links for 'フィードバック' and '日本語'.

| ファイル名                           | ダウンロード |
|---------------------------------|--------|
| このモノの証明書 f263a48574.cert.pem    | ダウンロード |
| パブリックキー f263a48574.public.key   | ダウンロード |
| プライベートキー f263a48574.private.key | ダウンロード |

<https://youtu.be/Gz1DWqDLaiQ>



# SORACOM Krypton

— SIMで認証、接続情報をセキュアにプロビジョニング

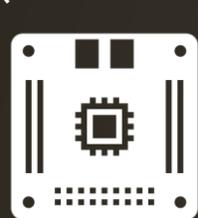


認証には強化された SORACOM Endorse を活用した2つの方法

- Option 1: セルラー回線経由で専用エンドポイントに接続
- Option 2: Wi-Fi, 有線を含む任意のアクセス回線上で SIM AKA 認証 (plan01s のみ)

# DEMO 2-2 — SORACOM Krypton

エッジ・コンピューティング  
デバイス



POST [krypton.soracom.io](https://krypton.soracom.io)



SORACOM Krypton が  
代理で発行依頼



AWS IoT Core



X.509 証明書と  
エンドポイント URL が  
JSON で返却



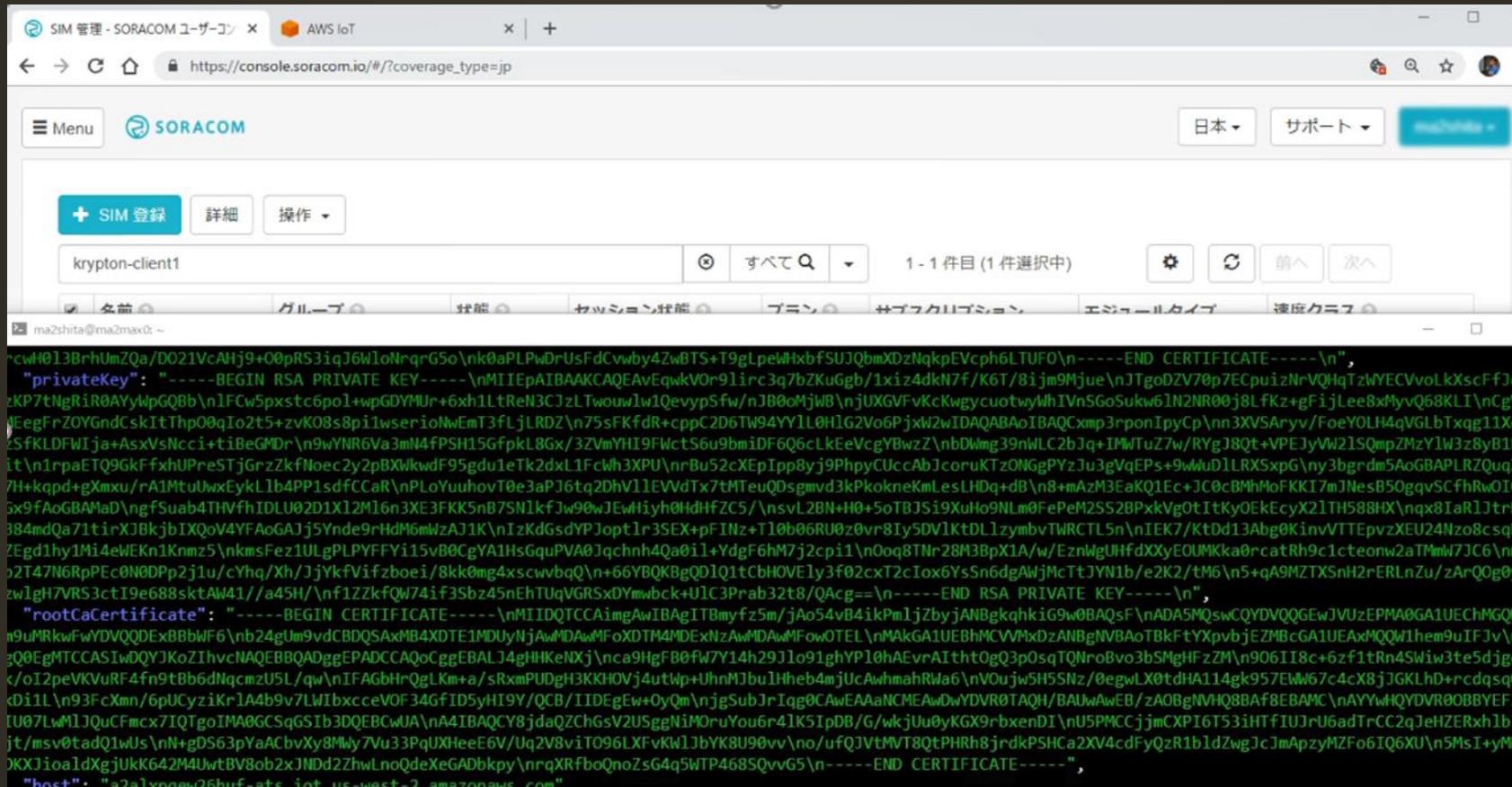
X.509 証明書

Wi-Fi で AWS IoT Core に接続



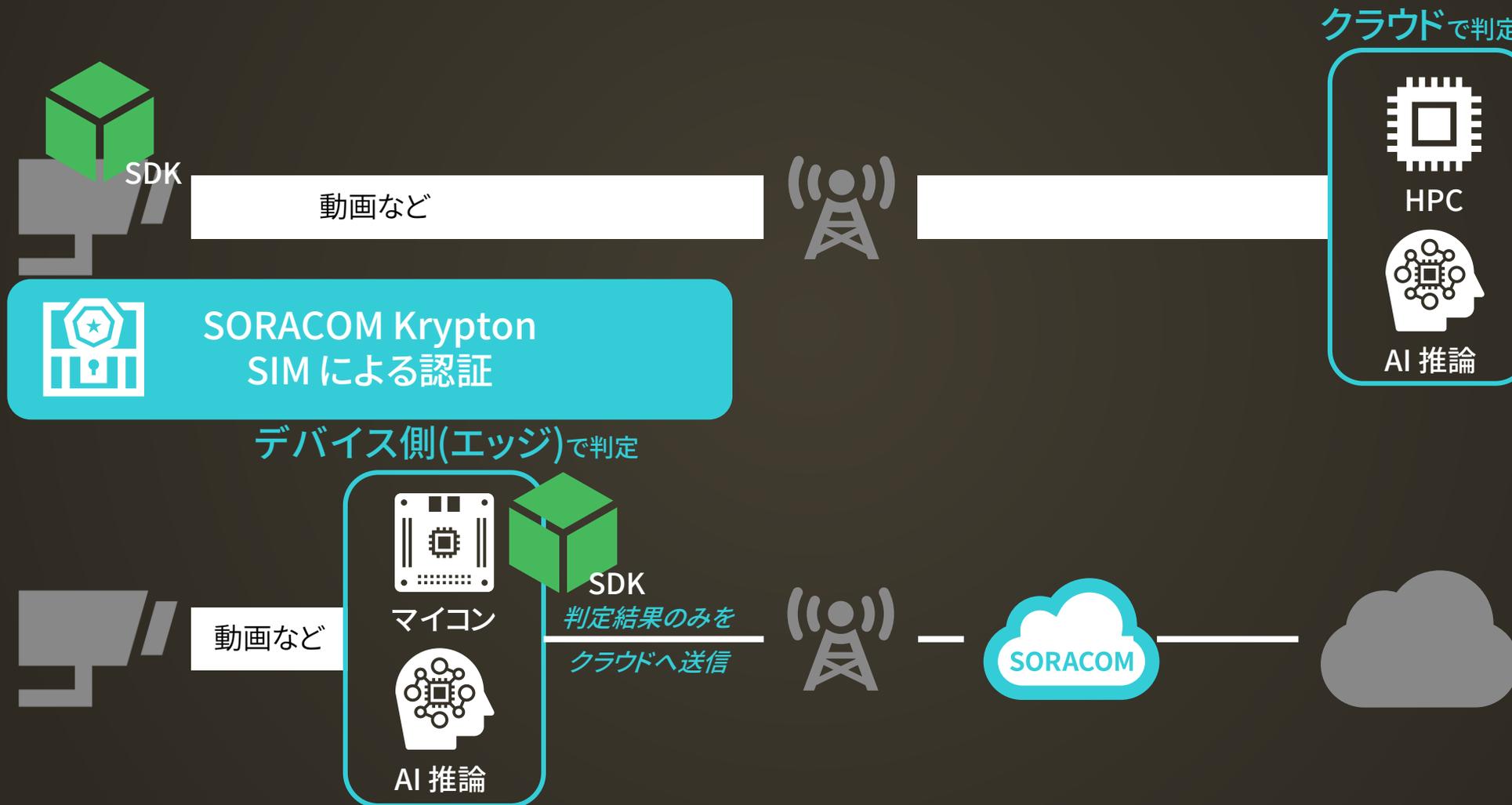
AWS IoT Core  
トピック

# SORACOM Krypton 経由で AWS IoT Core の設定と証明書を得る (動画)



<https://youtu.be/JSTS0xbWAFc>

# SORACOM Krypton で エッジ・コンピューティングもサポート



# 設定情報やファームウェア配布にも SORACOM Krypton

SORACOM Krypton サポート済み認証プロバイダ

AWS IoT Core, Amazon Cognito, SORACOM Inventory  
例)

Amazon Cognito から得た一時アクセスキー (STS) で  
Amazon S3 に認証された状態でアクセスし  
個別設定やファイルダウンロード

SORACOM Air メタデータサービスとの組み合わせも可能

# 主な初期設定 – クラウドファースト デバイス

## ソフトウェアやコンテンツ

- 公式カスタマイズその他、顧客指定の追加ソフトウェア  
**クラウド連携用 SDK や実装** →

データ転送サービス  
SORACOM Beam  
クラウド・アダプタ  
SORACOM Funnel

## 周辺機器の動作設定

- 標準搭載の I/O や、顧客指定の追加周辺機器の設定  
**通信機器の設定** →

IoT 向けデータ通信サービス  
SORACOM Air

## デバイス固有設定

- デバイス ID、デバイス管理用ログイン情報  
**アクセスキー、接続先設定** →

データ転送サービス  
SORACOM Beam  
クラウド・アダプタ  
SORACOM Funnel

セキュア・  
プロビジョニング  
SORACOM  
Krypton

# デバイス「売れば売るほど大変」



売る前

個体毎の設定、顧客毎や出荷先の設定

売った後

サーバとの接続設定変更



クラウドと連携するデバイスって  
売れば売るほど大変

たくさん売っても楽な仕組みへ



売る前

個体毎の設定、顧客毎や出荷先の設定

売った後

サーバとの接続設定変更



企画段階から SORACOM を練りこむ  
デバイスも「DevOps」はできる!

# 開発者サイト・ブログのご紹介

## 開発者サイト



<https://dev.soracom.io/jp/>

各サービスのGetting Startedを用意しています

## SORACOM ブログ



<https://blog.soracom.jp/>

最新の技術情報アップデートをいち早くお届けします

# Try! SORACOM チャレンジキャンペーン



～記事を書いてノベルティをゲットしよう～

期間:11月22日～12月25日

対象:企業・個人問わずどなたでもご参加いただけます

内容:SORACOM を使った電子工作やDeep Diveな記事を書いてくださった方に素敵なノベルティをプレゼントします



クラウド ⇒ 多くのビジネス、Webサービス

SORACOM ⇒ 多くのIoTビジネス、システム

たくさんの  
IoTプレイヤーが生まれますように

世界中のヒトとモノをつなげ  
共鳴する社会へ



SORACOM