

逆引きIoTクラウドデザインパターン

SORACOMサービスとクラウドサービスの組み合わせ/選択肢

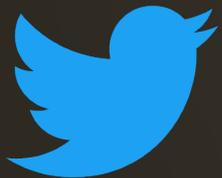
ソリューションアーキテクト 松本悠輔

株式会社ソラコム

2020年2月18日

本日のハッシュタグ

#soracom

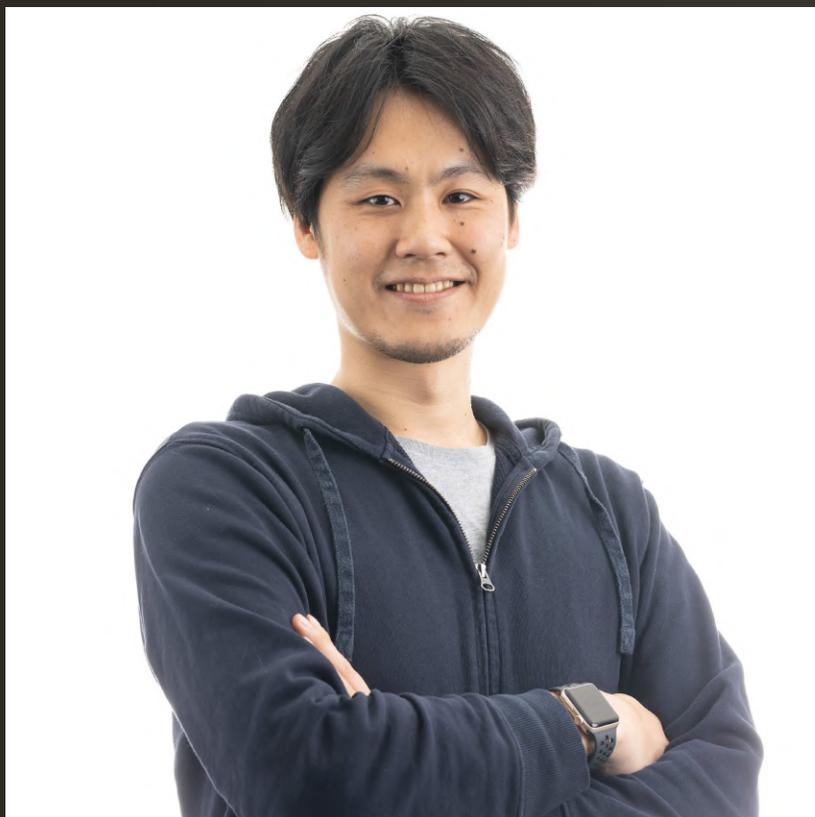


@SORACOM_PR



<https://www.facebook.com/soracom.jp/>

松本悠輔 (Yusuke Matsumoto) ソリューションアーキテクト



SORACOM本の一部執筆を担当しています！

アジェンダ

- IoTプロジェクトの課題認識とアプローチ
- 逆引きIoTクラウドデザインパターン
- まとめ

IoTプロジェクトを取り巻く環境

IoTプロジェクトで必要な技術要素がどんどん進化している

- デバイスの高性能化・安価化
- クラウドサービスの充実
- 通信規格の充実



 lte



 LTE-M



IoTの課題

- 技術的負債が生まれやすい
 - 物理的なモノを後からバージョンアップしづらい
 - ソフトウェアのバージョン管理も重要
 - 特にセキュリティアップデートは重要な課題
- 技術スタックが広い
 - 全て内製だと人的リソースが必要
 - ハードウェア、ソフトウェア、ネットワーク、アプリケーション・・・



コアコンピタンスへの選択と集中が必要

SORACOMの進化

2015年

通信の民主化

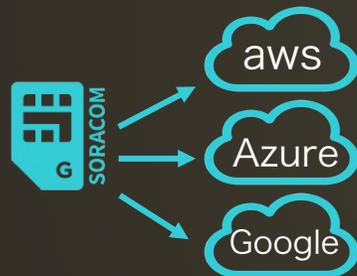
IoT SIM
発売開始



2016年

クラウド連携
閉域対応

IoTクラウド
アダプター



閉域接続
(AWS VPC、
VPN、専用線)



2017年

グローバル
複数無線対応

IoT SIM
グローバル対応



複数無線サポート
(GSM/3G/LTE/LPWA)



2018年

可視化とハード
を簡単に

IoTダッシュボード



IoTネイティブ
デバイス



2019年

エッジ&
サーバレス

エッジ・
コンピューティング



FaaS対応
(Function as a Service)



SORACOM IoT プラットフォーム



インタフェース

Web インターフェース
User Console

API
Web API
Sandbox

アクセス権限管理
SORACOM Access
Management

ライブラリ & SDKs
CLI(Go), Ruby, Swift

開発者サポート
Developer Support

アプリケーション

データ収集・蓄積
SORACOM Harvest

ダッシュボード作成/共有
SORACOM Lagoon

エッジプロセッシング
SORACOM Mosaic

データ転送支援
SORACOM Beam

クラウドアダプタ
SORACOM Funnel

クラウドファンクション
SORACOM Funk

SIM認証・証明
SORACOM Endorse

デバイス管理
SORACOM Inventory

セキュアプロビジョニング
SORACOM Krypton

ネットワーク

デバイスLAN
SORACOM Gate

透過型トラフィック処理
SORACOM Junction

オンデマンドリモートアクセス
SORACOM Napter

プライベート接続
SORACOM Canal

専用線接続
SORACOM Direct

仮想専用線
SORACOM Door

デバイス

USB Dongle / セルラーモジュール / マイコンモジュール / ボタン

コネクティビティ

IoT向けデータ通信
SORACOM Air
for Cellular (2G, 3G, LTE) / LPWA (LoRaWAN, Sigfox, LTE-M)

SORACOM Global Platform

SORACOM IoT プラットフォーム



インタフェース

Web インターフェース
User Console

API
Web API
Sandbox

アクセス権限管理
SORACOM Access
Management

ライブラリ & SDKs
CLI(Go), Ruby, Swift

開発者サポート
Developer Support

アプリケーション

データ収集・蓄積
SORACOM Harvest

ダッシュボード作成/共有
SORACOM Lagoon

エッジプロセッシング
SORACOM Mosaic

データ分析支援
SORACOM Beam

クラウド連携
SORACOM Funnel

クラウド連携
SORACOM Funnel

SIM認証・証明
SORACOM Endorse

デバイス管理
SORACOM Inventory

セキュアプロビジョニング
SORACOM Krypton

ネットワーク

クラウド連携
SORACOM Naper

透過型トランザクティブ処理
SORACOM Juniper

オンデマンドリモートアクセス
SORACOM Napter

プライベート接続
SORACOM Canal

専用線接続
SORACOM Direct

仮想専用線
SORACOM Door

デバイス

USB ドングル / セルラーモジュール / マイコンモジュール / ボタン

コネクティビティ

IoT向けデータ通信
SORACOM Air
for Cellular (2G, 3G, LTE) / LPWA (LoRaWAN, Sigfox, LTE-M)

多くのクラウドとの
連携サービス

SORACOM Global Platform

SORACOMサービスの背景

SORACOMサービスの背景にはIoTの課題が存在する
同様にクラウドサービスも様々な課題解決を目的としている



本セッションのゴール

ユースケースごとの課題を整理する

SORACOMとクラウドの組み合わせを理解する

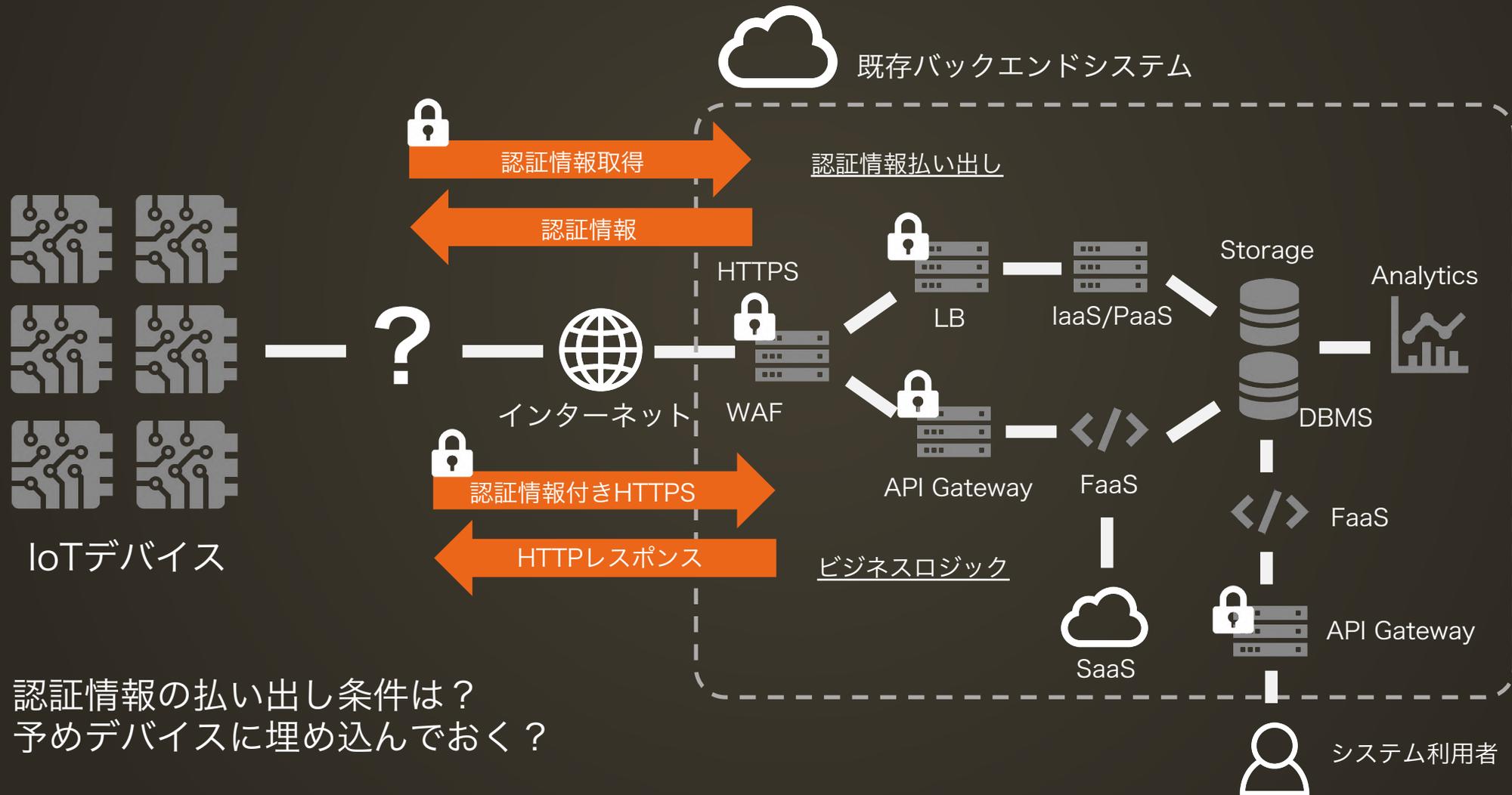
IoTのデザインパターン

1. IoTデバイスを既存のWebシステムと連携する
2. クラウドベースのサーバレスシステムと連携する
3. 現場からの大量データを収集する
4. デバイスとバックエンドを閉域網で接続する
5. 現場のデバイスにセキュアリモートアクセスする

IoTのデザインパターン

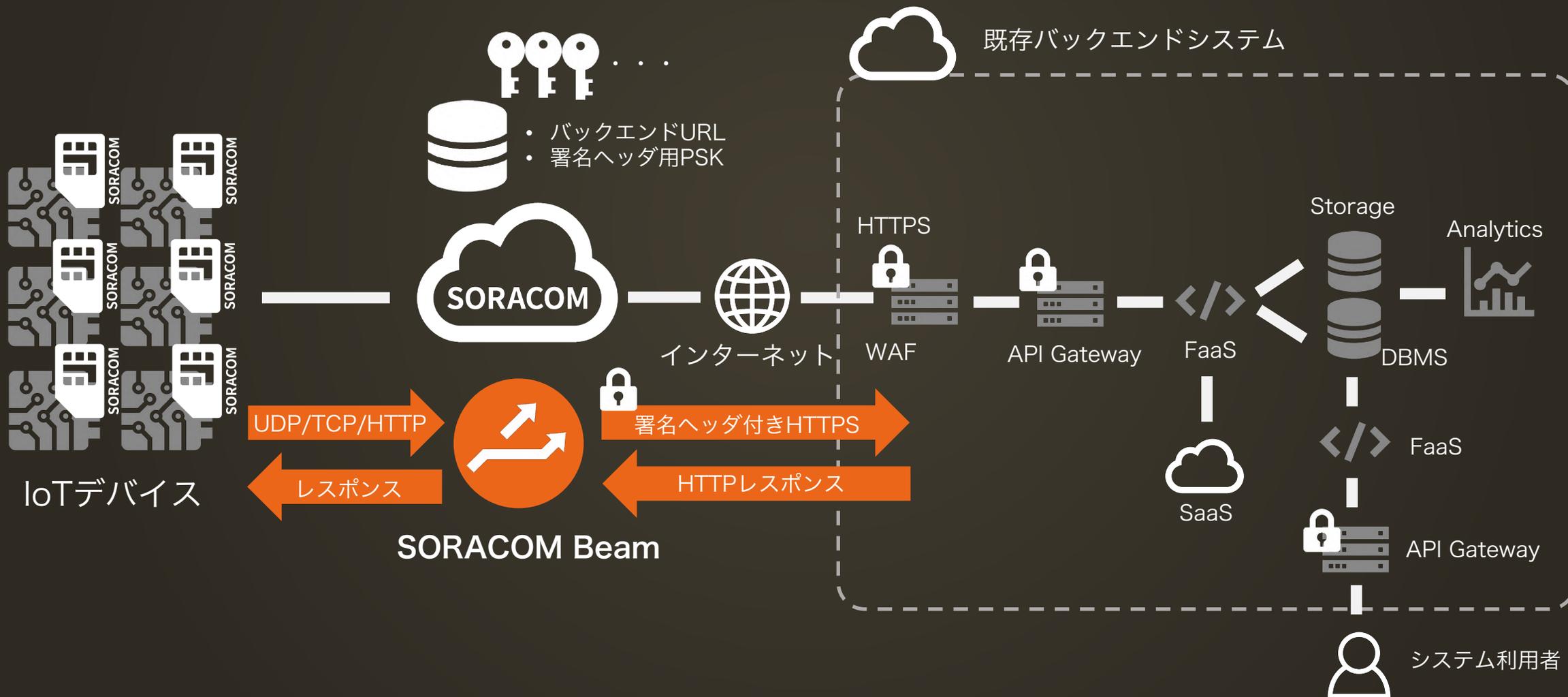
1. IoTデバイスを既存のWebシステムと連携する
2. クラウドベースのサーバレスシステムと連携する
3. 現場からの大量データを収集する
4. デバイスとバックエンドを閉域網で接続する
5. 現場のデバイスにセキュアリモートアクセスする

1. IoTデバイスを既存のWebシステムと連携する(HTTP)

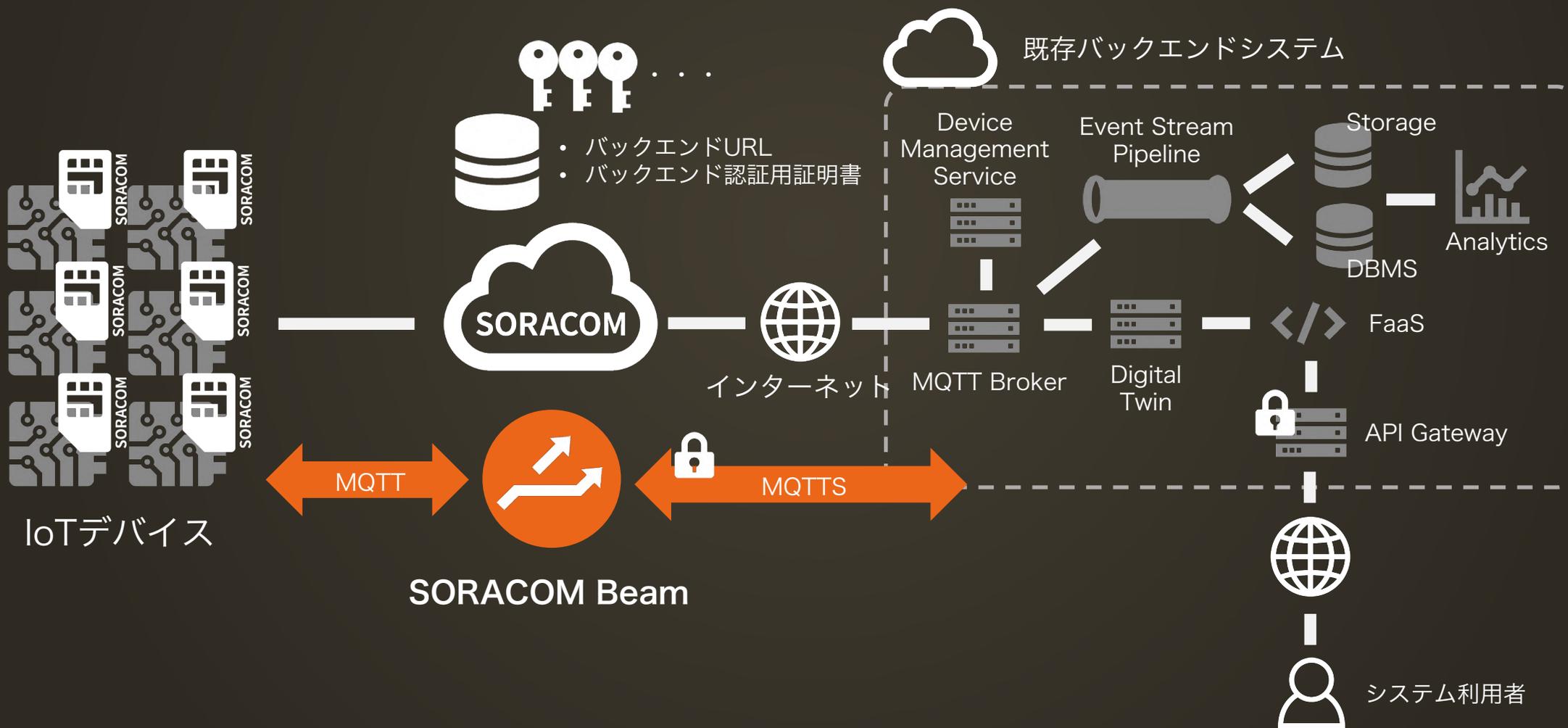


認証情報の払い出し条件は？
予めデバイスに埋め込んでおく？

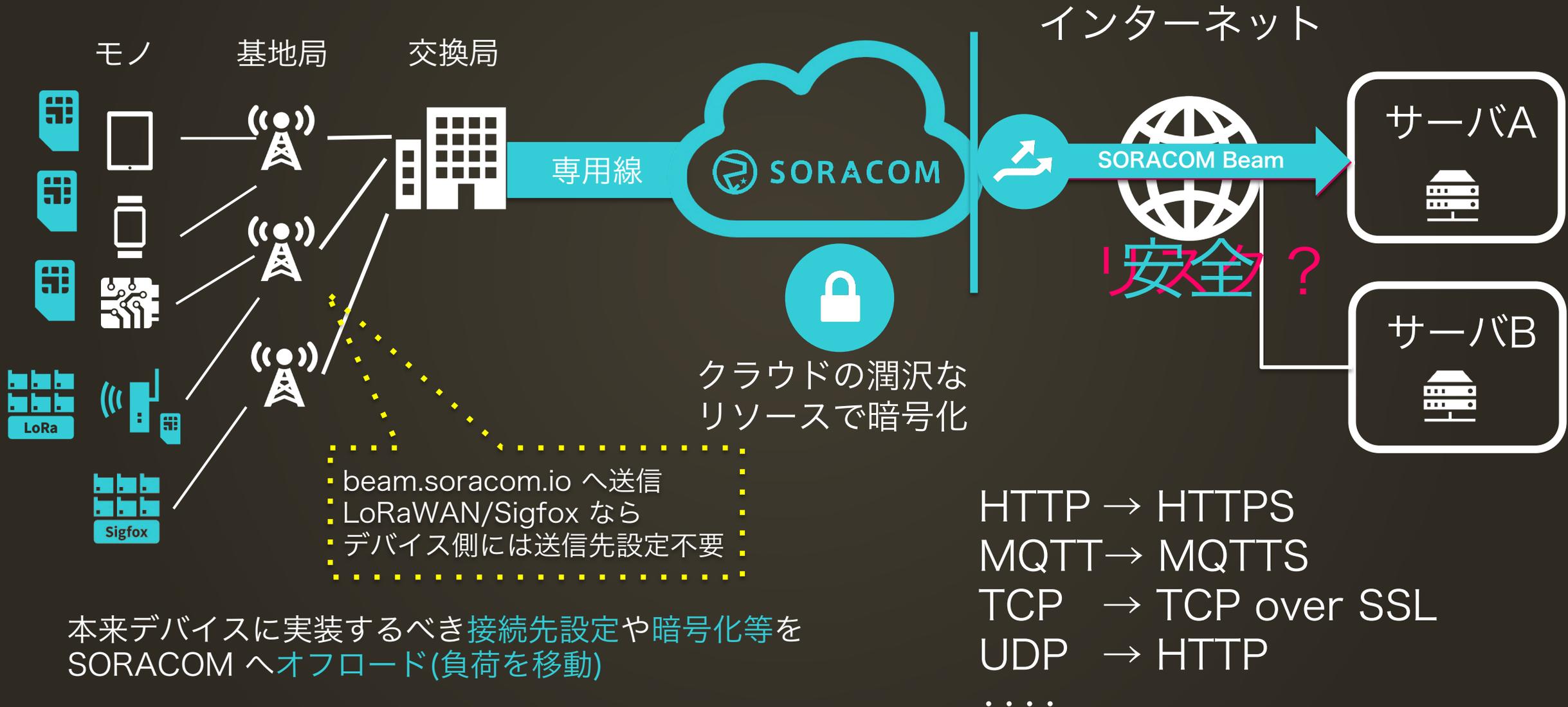
1. IoTデバイスを既存のWebシステムと連携する(HTTP)



1. IoTデバイスを既存の Webシステムと連携する (MQTT)



SORACOM Beamとは？



お客様事例: WHILL様



パーソナル
モビリティに
SORACOM

バッテリーを出来るだけ
使わずに
セキュリティも



天然水を必要な
タイミングにお届け
自動再注文を実現する
IoTウォーターサーバー

SORACOM Beamで
クラウド上のシステムと
セキュアに連携

SORACOM Beamの特徴

- デバイスをシンプルにできる
 - デバイスが利用する通信プロトコルの制約を受けづらい
 - UDP/TCP/HTTP/MQTT等にできる
 - プロトコルオーバーヘッドを小さくして通信量を削減
- セキュリティプロトコルのメリットを受けられる
 - Beamからバックエンドシステムの間はセキュアプロトコル（HTTPS/MQTTs）を利用できる
- バックエンドシステムにデバイス固有の情報を通知できる
 - SORACOM Beamで検証可能な署名を付与、なりすましリスク対策可能
 - SORACOM Air SIMは耐タンパ性が高く複製が困難
- デバイスの通信先変更が容易
 - Beamの通信先はいつでも変更可能
 - デバイスに手を入れずにシステム変更

なぜSSL/TLSをオフロードするのか？(1)

- データ通信量を最適化したい
 - データ通信量を減らすメリットがある
 - 一方でSORACOM Beam利用料金が発生する

例)デバイスから100バイトのデータを送る場合 (※ただしUDPの場合にレスポンスを考慮しない)



SORACOM Air plan-D (s1.minimum利用時)のデータ通信費用
5360バイト \approx 0.001円の削減効果

SORACOM Beamの利用費用
0.0009円 x 2リクエスト = 0.0018円

\Rightarrow 0.0008円/リクエストのコスト増

なぜSSL/TLSをオフロードするのか？(2)

- 暗号化プロトコルを使用しないことで消費電力を抑えられる
 - デバイスによってモチベーションは異なるが、組み込みデバイスの場合やバッテリー駆動デバイスの場合はSSL/TLSのオフロードで消費電力の削減が期待できる
- 消費電力は実行するプログラムのロジックやハードウェアによって異なるので実際に測定することが重要

前ページ例の場合)

SORACOM Air plan-D (s1.minimum利用時)のデータ通信費用
5360バイト \approx 0.001円の削減効果

SORACOM Beamの利用費用
0.0009円 \times 2リクエスト = 0.0018円

\Rightarrow 0.0008円/リクエストで消費電力の削減効果が得られる

参考： Wio LTE消費電力の研究

<https://qiita.com/1stship/items/7b99973b65934696bc91>

なぜSSL/TLSをオフロードするのか？(3)

- SSL/TLSを使っていれば安全？
- 過去のSSL/TLS脆弱性
 - POODLE、BEAST、CRIME/BREACH、etc
- セキュアプロトコルスタックも継続的なアップデートが必要
 - IoTデバイスのクライアント実装はTLSスタックをソフトウェアのアップデートが難しいケースが多い
 - CA Certificationの継続的なメンテナンスも必要
- IoTにおいても継続的にセキュリティプロトコル自体をアップデートする仕組みが望ましい



処理をクラウドにオフロードしておく
クラウドサービス側で対応できる

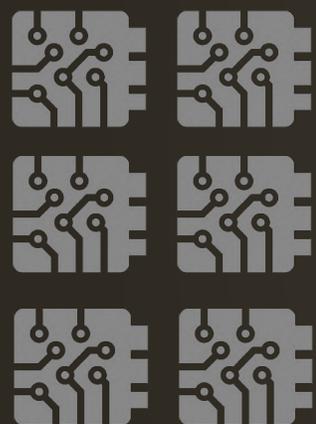
SORACOM Beam利用時のTips

- デバイスでのエラーハンドリング
 - Beam連携先でのエラー、Beamでのエラーいずれもデバイスに返却される
 - エラーハンドリングとリトライは**デバイスの責務**
- さらなる通信量の最適化
 - DNSキャッシュ
 - バイナリパーサー

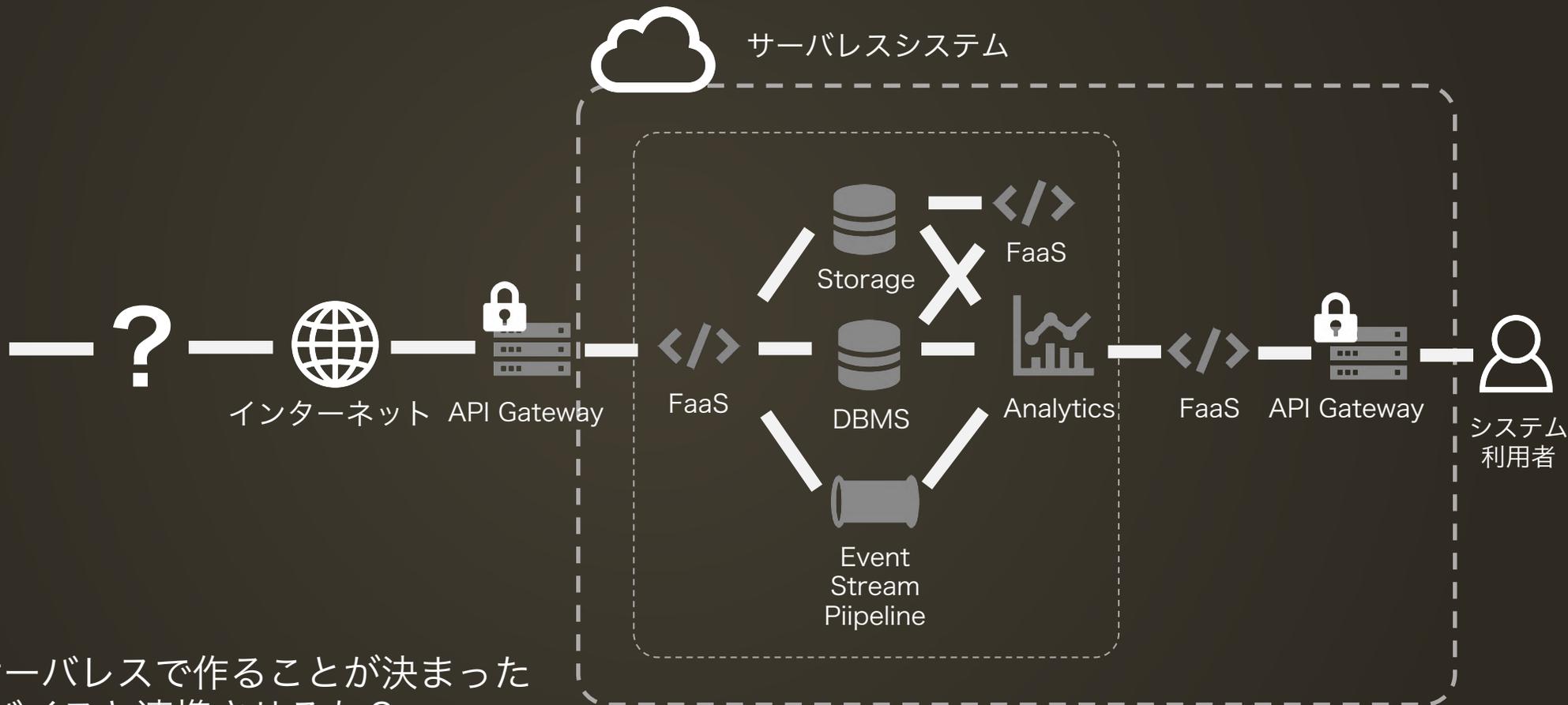
IoTのデザインパターン

1. IoTデバイスを既存のWebシステムと連携する
2. クラウドベースのサーバレスシステムと連携する
3. 現場からの大量データを収集する
4. デバイスとバックエンドを閉域網で接続する
5. 現場のデバイスにセキュアリモートアクセスする

2. クラウドベースの サーバレスシステムと連携する



IoTデバイス

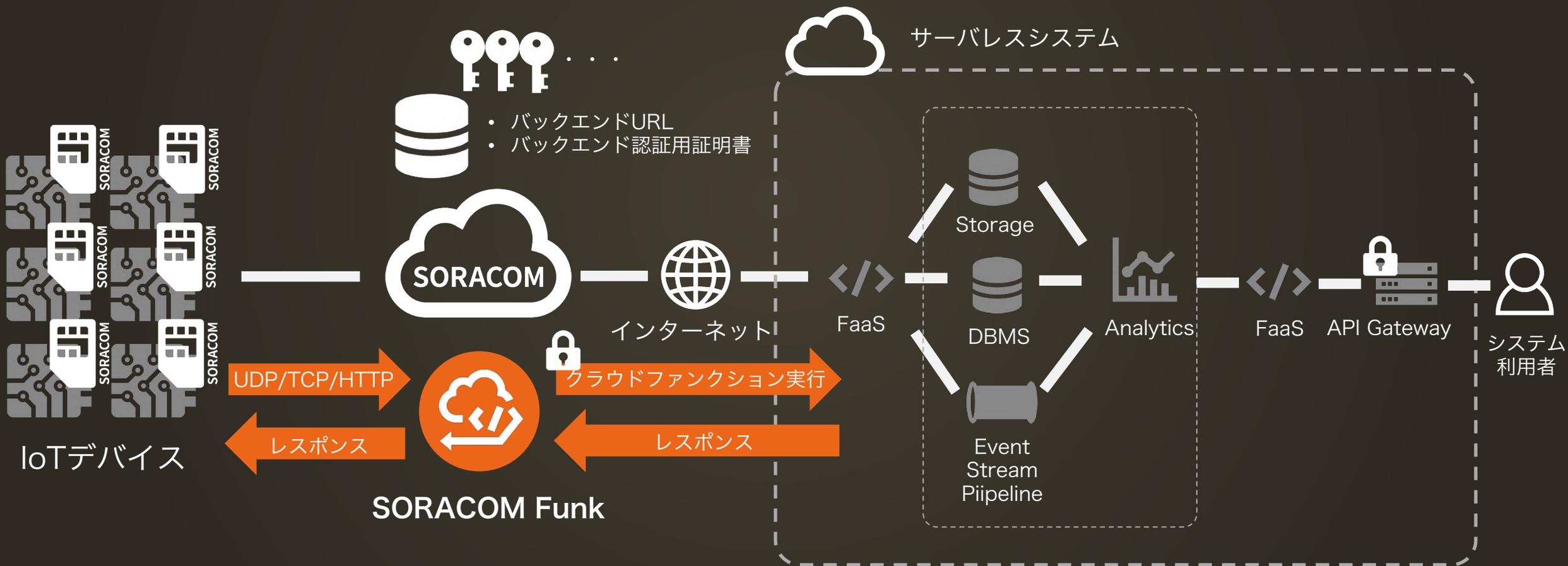


バックエンドはサーバレスで作ることが決まった
どうやってIoTデバイスと連携させるか？

API Gatewayを置く？

個体識別は・・・

2. クラウドベースのサーバレスシステムと連携する



SORACOM Funkとは？

サーバレスでクラウド上のコードを実行
結果を受け取り



デバイス側のロジックを最小限にして
クラウド側にオフロード

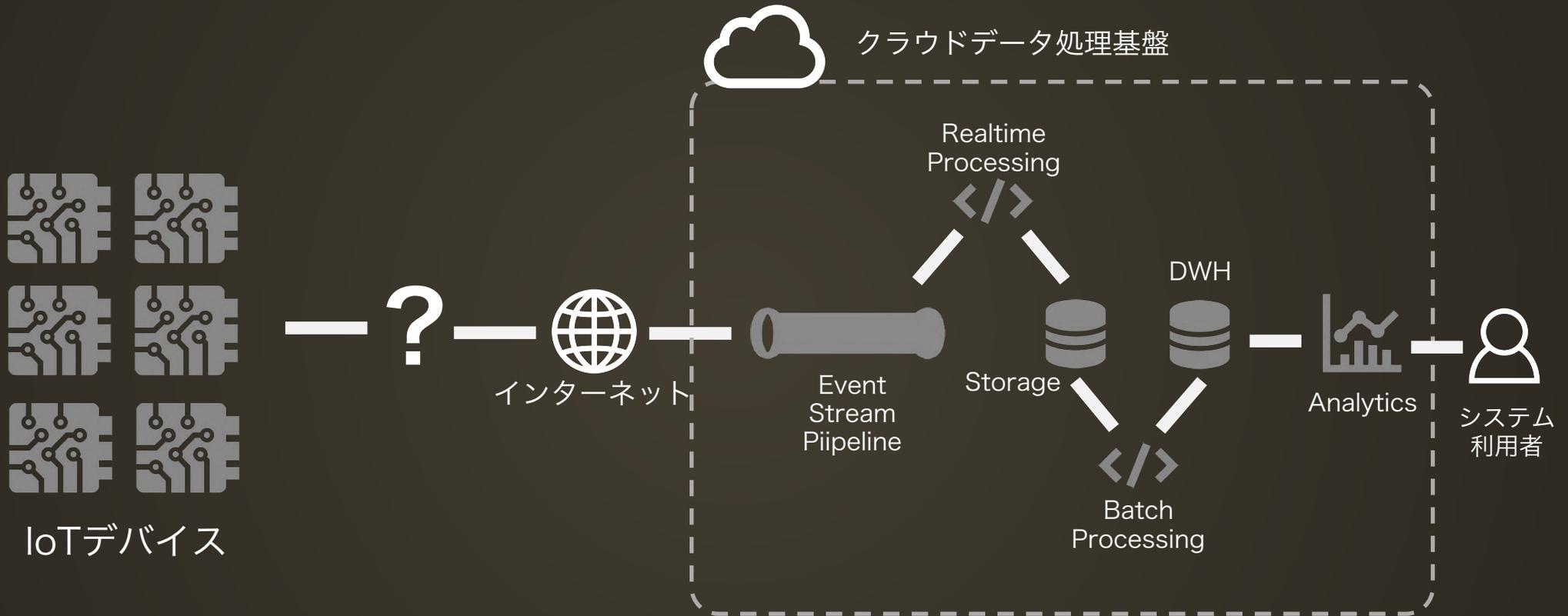
SORACOM Funkの特徴

- デバイスから直接クラウドのFaaSを呼び出し
 - クラウドにデータを投入する前処理が可能
 - バックエンド固有の情報を付与
 - ペイロードを変更
 - デバイスから複数の種類のデータを送信する？
 - 最初に呼び出すファンクションをイベントルータとして活用
- クラウド、Webエンジニアにとって親和性が高い
 - 扱いの慣れているクラウド側にロジックを実装

IoTのデザインパターン

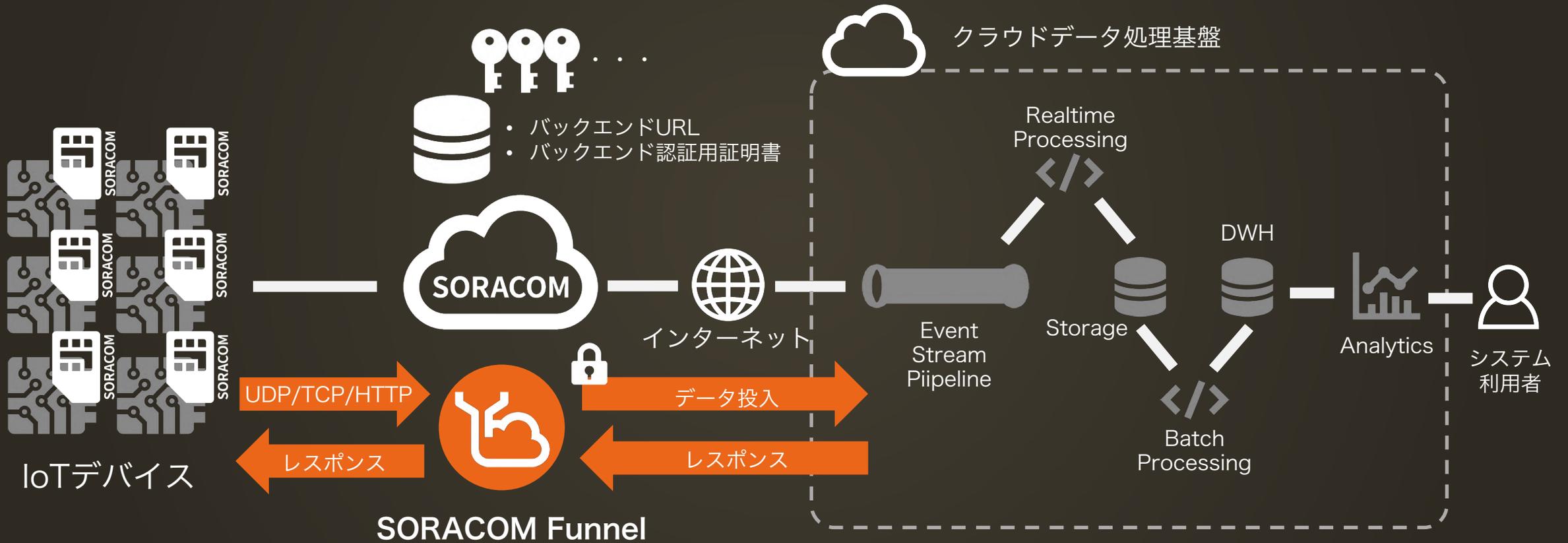
1. IoTデバイスを既存のWebシステムと連携する
2. クラウドベースのサーバレスシステムと連携する
3. 現場からの大量データを収集する
4. デバイスとバックエンドを閉域網で接続する
5. 現場のデバイスにセキュアリモートアクセスする

3. 現場からの大量データを収集する



大量のデータアップロードに対応できるか？
データ処理基盤と連携できるか？
セキュリティは？

3. 現場からの大量データを収集する



SORACOM Funnelとは？

デバイスからのデータを特定のクラウドサービスに直接転送
クラウドリソースアダプター



SORACOM Funnel 対応アダプタ



※ 2019年7月現在



AWS IoT Core



Amazon Kinesis
Data Streams



Amazon Kinesis
Data Firehose



Amazon Kinesis
Video Streams



Azure
Event Hubs



Google
Cloud Pub/Sub

Partner Hosted Adaptor

— SORACOMのパートナーによって提供される SORACOM Funnel アダプタ

《Acroquest Technology》

Torrentio

ストリームデータ処理エンジン

《Saison Information Systems》

DataSpider

ノンプログラミングデータ連携

《ウイングアーク1st》

MotionBoard Cloud

データ可視化BIツール

《YE DIGITAL》

MMCloud

デバイス&データ
ライフサイクルマネジメント

《ブレインズテクノロジー》

Impulse

リアルタイム大規模
データ分析基盤

《アステリア》

Platio

モバイルアプリ開発

《Kii》

Kii

IoTアプリケーション
バックエンドサービス

《日本テラデータ》

IntelliCloud

データ分析プラットフォーム



《ESRIジャパン》

ArcGIS

位置情報可視化
プラットフォーム

《ランドログ》

LANDLOG

建設生産プロセス向け
IoTプラットフォーム



《OPTiM》

OPTiM Cloud IoT OS

AI・IoT活用統合
プラットフォーム

《Fusic》

mockmock

IoTシステム開発向け
疑似データ生成サービス

お客様事例: ダイドードリンク様



毎日、明日が楽しみになる。未来型自販機！



スマイルスタント
Smile STAND

SORACOM Funnelを
活用し安全かつ容易に
データを送信

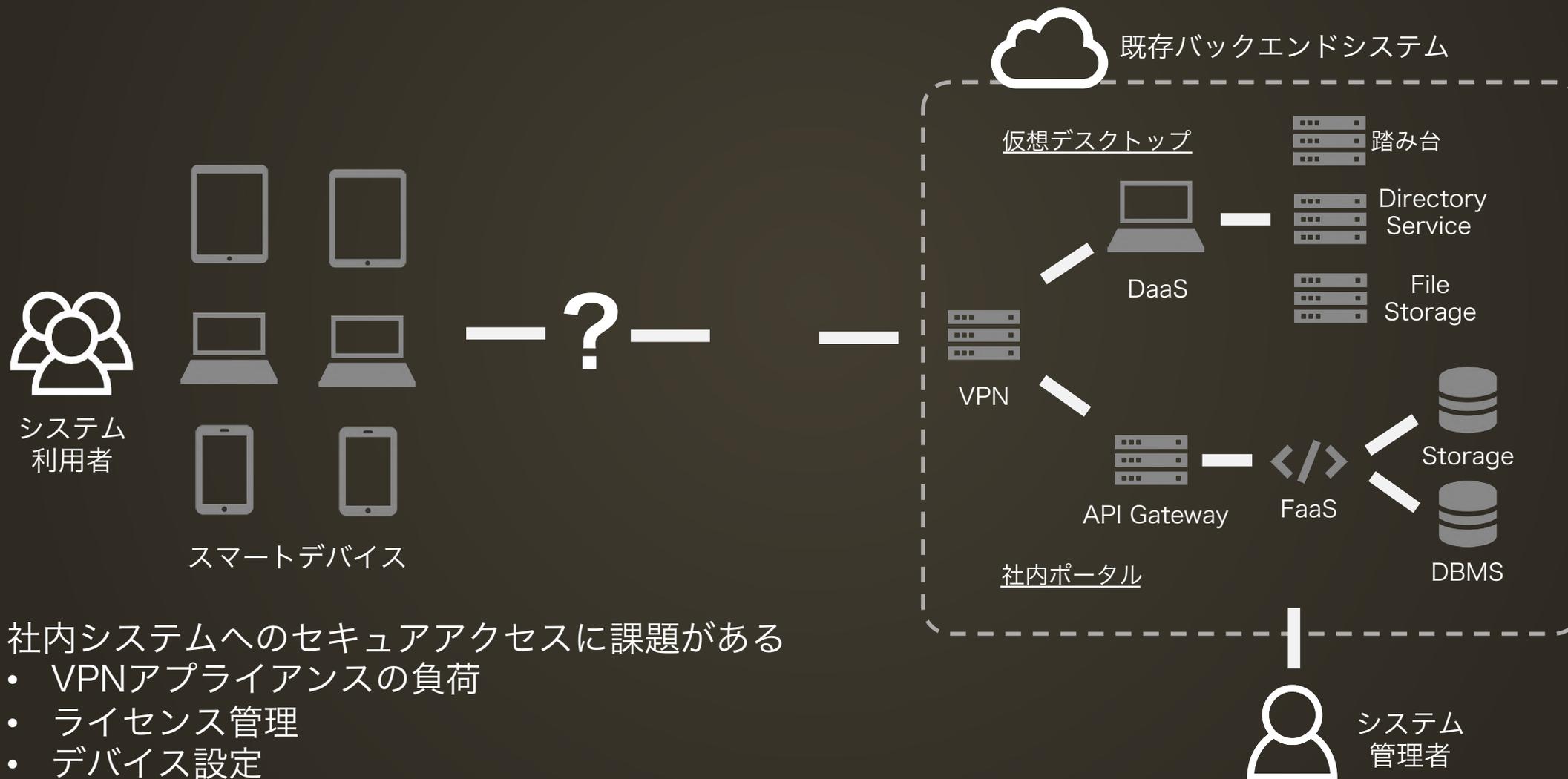
SORACOM Funnelの特徴

- 高頻度データ送信に最適
 - バッファリングによってスケーラビリティを提供
 - 複数のイベントを配列に格納してバックエンドに転送
 - 非同期連携
- バックエンドへの転送にリトライ処理を提供
 - Funnelからバックエンド転送エラーはSORACOMでリトライ
 - デバイスはFunnelまでのリトライ処理が責務
- IoTでのイベント処理をシンプル化
 - デバイス認証、固有情報をペイロードに追加

IoTのデザインパターン

1. IoTデバイスを既存のWebシステムと連携する
2. クラウドベースのサーバレスシステムと連携する
3. 現場からの大量データを収集する
4. デバイスとバックエンドを閉域網で接続する
5. 現場のデバイスにセキュアリモートアクセスする

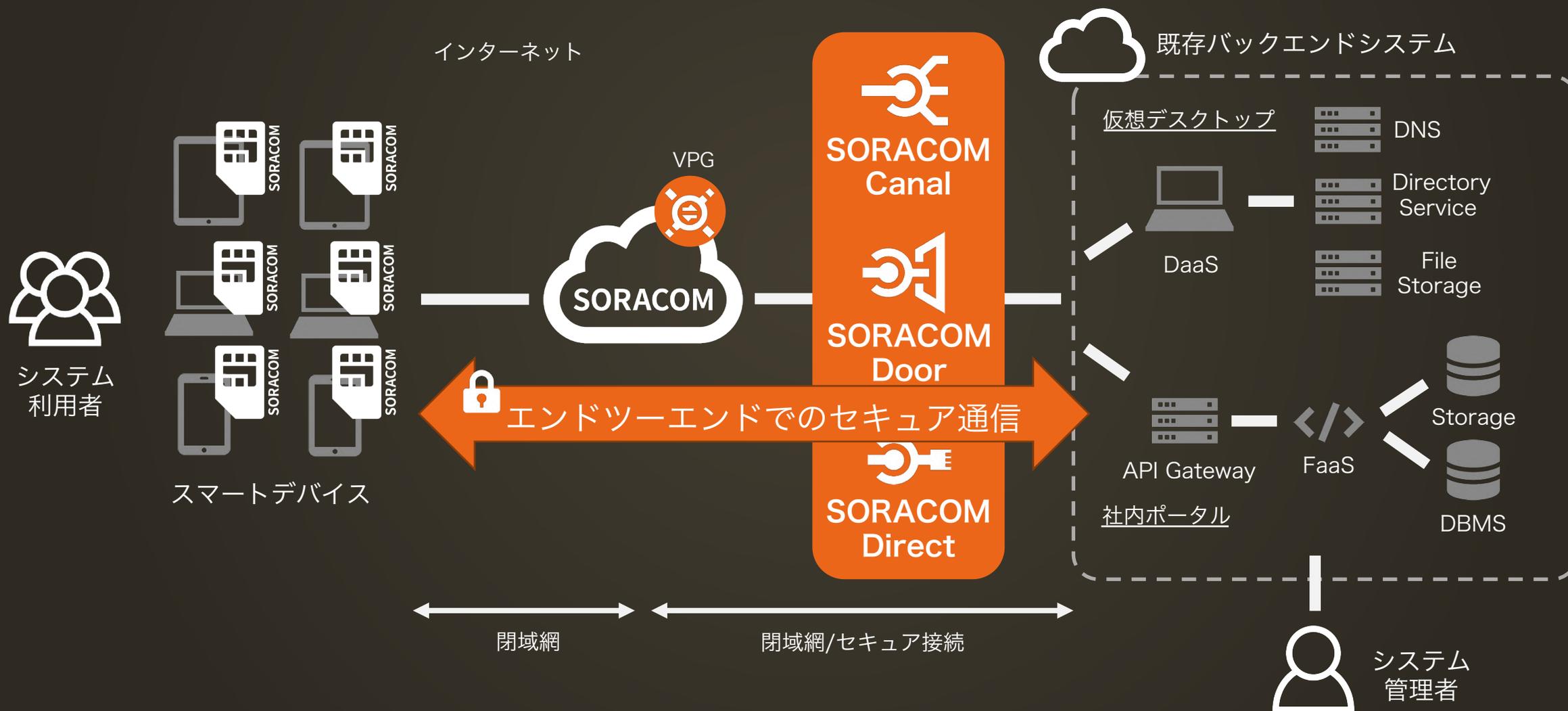
4. デバイスとバックエンドを 閉域網で接続する



社内システムへのセキュアアクセスに課題がある

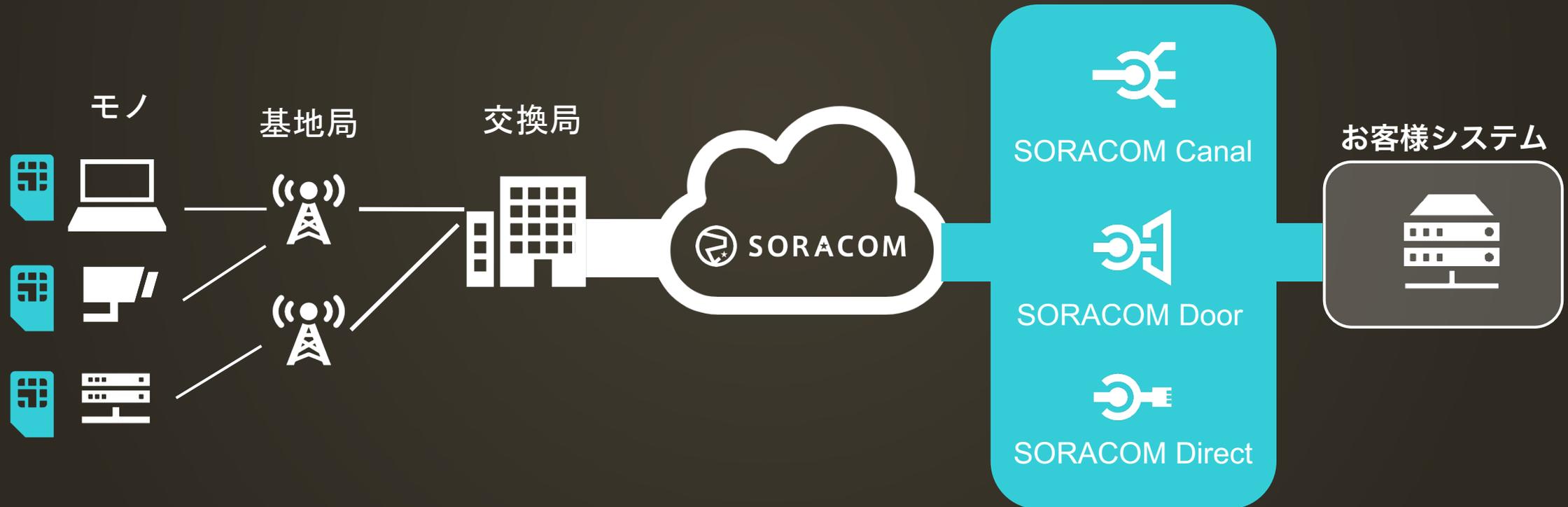
- VPNアプライアンスの負荷
- ライセンス管理
- デバイス設定

4. デバイスとバックエンドを 閉域網で接続する



SORACOM Canal/Door/Direct とは？

お客様ネットワークとセキュア接続
機密性の高いデータの取り扱いをサポート



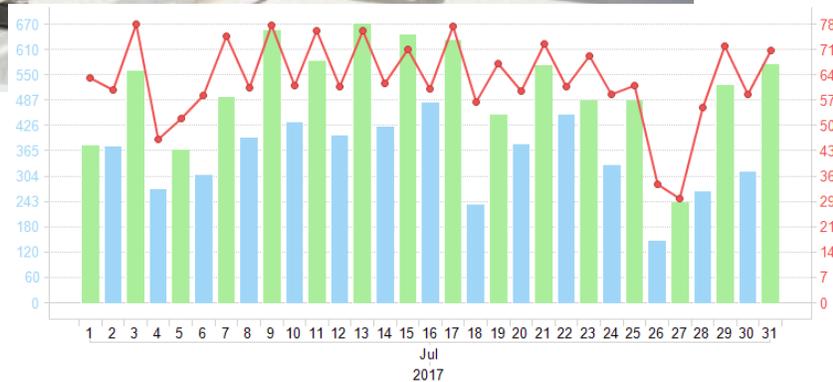
お客様事例：まちづくり松山様

店舗用端末とサーバとのセキュアな通信にSORACOM

SORACOM AirとCanalを利用し、商店街にポイント、電子マネー、お買物券決済システムを導入



お客様事例：協和エクシオ様



室温をクラウドで分析、
空調制御型省エネサー
ビスを顧客に提供

Air SIMで施工コストを
3割減、SORACOM
Canalでセキュアに接続

SORACOM Canal/Door/Directの特徴

- デバイスに閉域接続を組み込み
 - 電源オンからいきなり閉域網に接続できる
- 好きな通信プロトコルを利用できる
 - 例1：バーチャルデスクトップに閉域網内でRDP接続
 - 例2：クラウド上の社内システムに閉域アクセス
- 既存の閉域網にSORACOMを追加可能
 - 100.64.0.0/10のCIDRを持つ拠点が增えるイメージ
 - デバイスサブネットで指定のCIDRではないので注意
 - VPGでNATされる

ネットワーク構成のイメージ (Canal)



ネットワーク構成のイメージ (Door/Direct)



IoTのデザインパターン

1. IoTデバイスを既存のWebシステムと連携する
2. クラウドベースのサーバレスシステムと連携する
3. 現場からの大量データを収集する
4. デバイスとバックエンドを閉域網で接続する
5. 現場のデバイスにセキュアリモートアクセスする

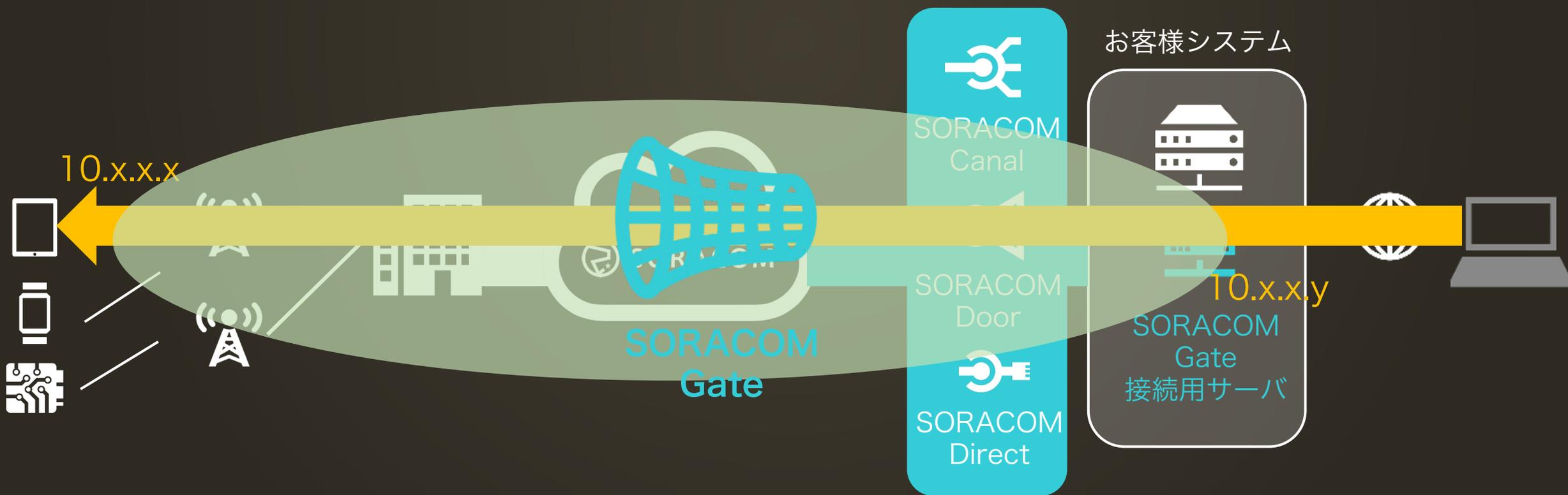
どのリモートアクセス手法を選ぶべきか？



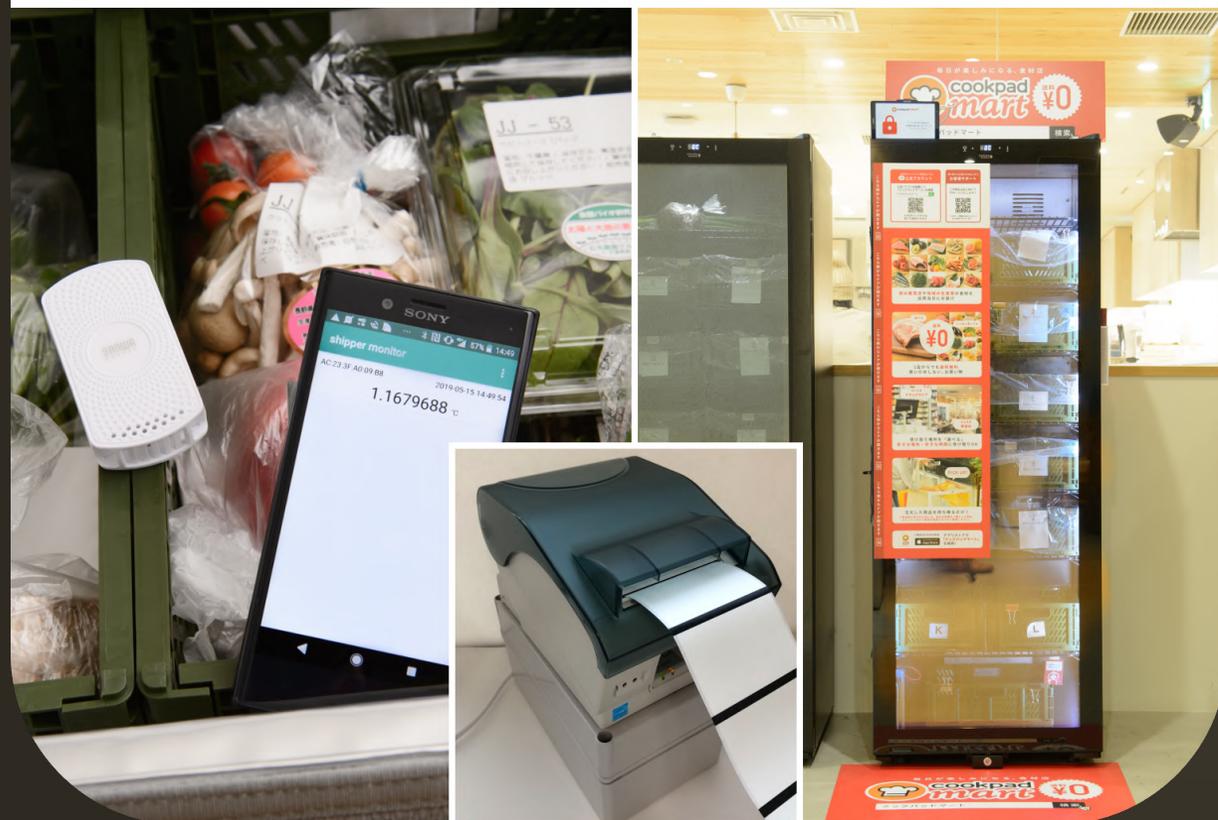
リモートアクセスのアーキテクチャパターンをご紹介します

SORACOM Gate – デバイスLAN接続

デバイスとクラウドを1つの大きなプライベートLANに
クラウドからのリモートアクセスを可能にするサービス



お客様事例：クックパッド



クックパッドマートに SORACOM Air Canal/Gateを利用

閉域網通信でラベルプリンターの安定したリモート印刷とリモートメンテナンスを実現

AMANO



ロボット掃除機RcDCの 遠隔サポートに SORACOM Gate

夜間施錠中のお客様先で稼働するロボット掃除機とセキユアに通信し、運用をサポート

SORACOM Gateの特徴

- SIM間通信が可能
 - 小規模なりモートアクセスであればSIM2枚で実現できる
- アプリケーションがデバイス固有のIPアドレスを識別する場合に最適
 - サーバ => デバイスの通信が可能
 - デバイス => サーバの場合にデバイスごとのIPアドレスを識別できる
 - VPGのNATを超えられる
- ネットワークの複雑さも上がるので用途に合わせて利用する
 - サーバ => デバイスの通信にはVXLANによるオーバーレイネットワークを構築する必要がある
 - お客様環境にGate Peer (VXLANのVTEP) が必要になる (※SIM間通信では不要)
 - 機能と複雑さとのトレードオフ

SORACOM Napter -

オンデマンドリモートアクセス

必要な時に**短時間**だけデバイスへ**リモートアクセス**し
操作・閲覧を可能にするサービス



SORACOM Napterの特徴

- 現場のデバイスにリモートアクセス可能
 - デバイス => サーバは通常のSORACOM Air for Cellularと同一
 - アクセス元IPとアクセス可能な期間を制限可能
- 非セキュアサービスをセキュア化可能
 - 例1：ルータのHTTPの管理画面にリモートからHTTPSでアクセス可能
 - 例2：Webカメラの映像をセキュアに確認できる

SORACOM Gate or Napter?

リモートアクセスのワークロードに応じてアーキテクチャを3パターンに分類

- **1対1接続**

- アクセス元とアクセス先がそれぞれ1つずつのパターン
- もしくはデバイスはたくさんあるけど時折しかアクセスが発生せず、同時に1台ずつアクセスするパターン

- **1対多接続**

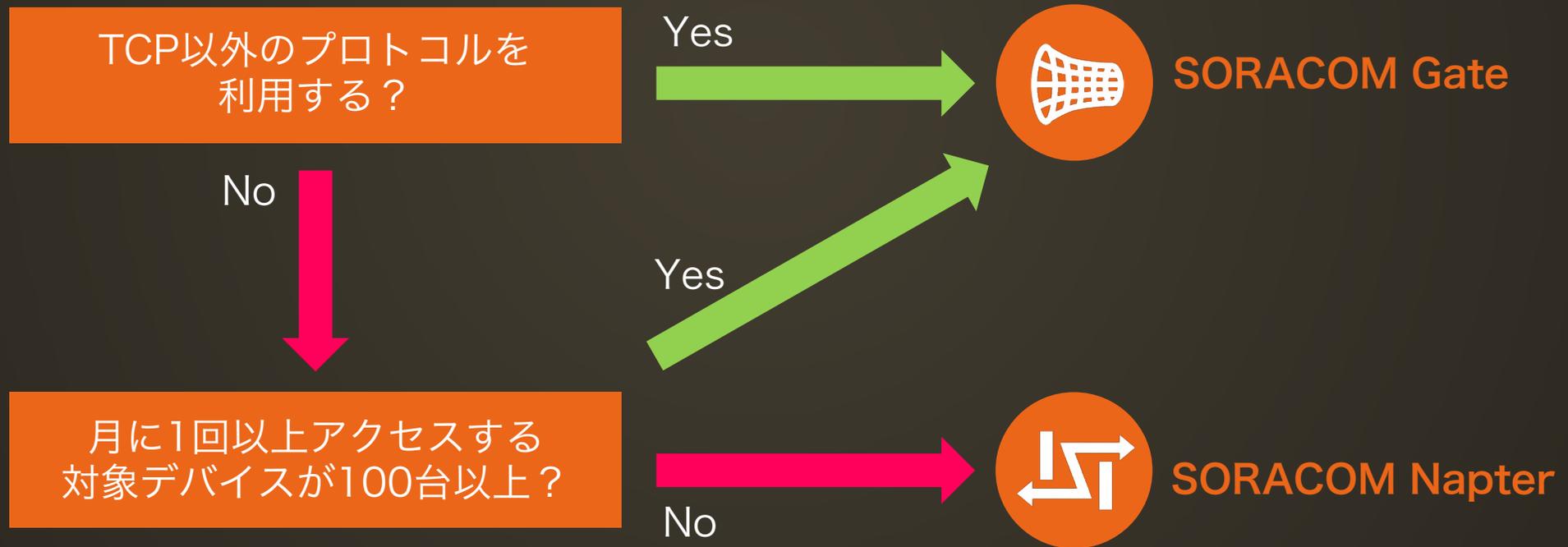
- アクセス元は1つだが同時に複数のデバイスにリモートアクセスしたいパターン

- **多対多接続**

- 複数のアクセス元から複数のデバイスに同時にリモートアクセスするパターン

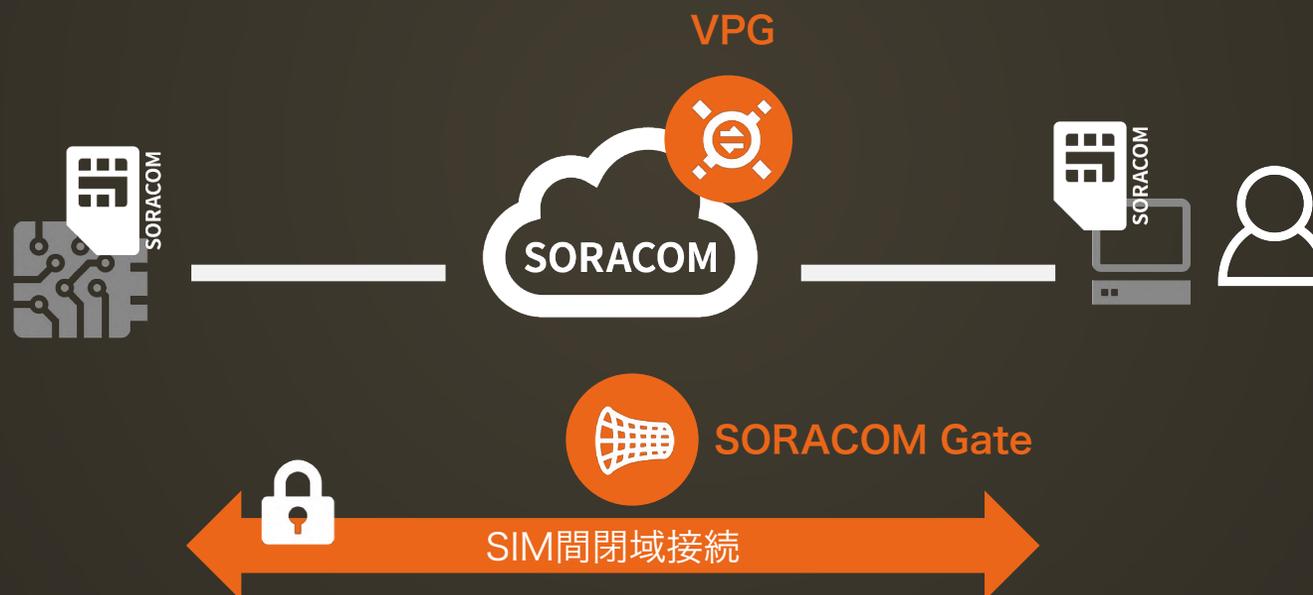
1対1接続

アクセス元とデバイスが1対1になる場合、利用したいプロトコルやアクセス頻度に応じて活用サービスを変えることを推奨



1対1接続

リモートアクセスに用いるプロトコルがTCP以外の場合や、ランダムな複数のTCPポートが必要になる場合は**SORACOM Gate**のSIM間接続の利用を推奨



Public Gateの利用も可能、ただしセキュリティリスクについて正しく理解したうえでの利用を強く推奨

参考URL : https://dev.soracom.io/jp/docs/public_gate/

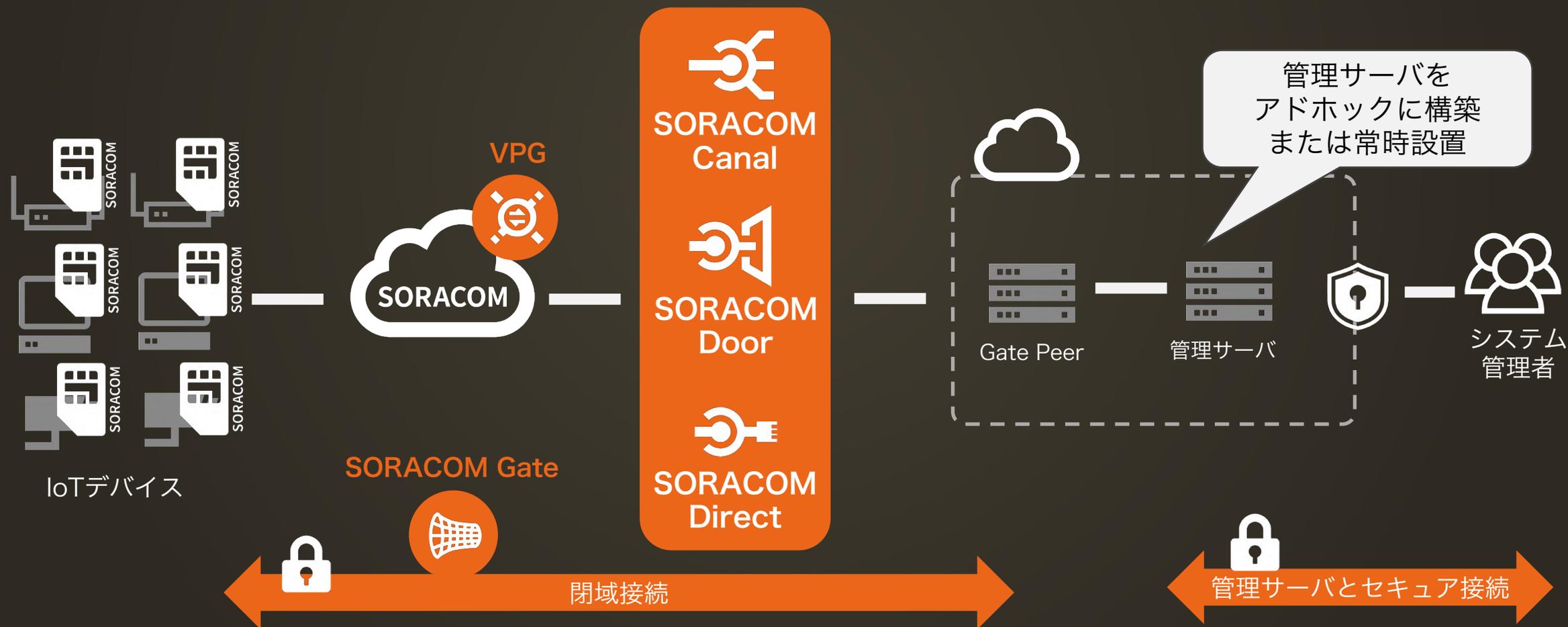
1対1接続

リモートアクセスに用いるプロトコルがTCPの場合やアクセス先デバイスが少ない場合は**SORACOM Napter**の利用を推奨



多対多接続

アクセス元拠点に複数の担当者がいる場合はあらかじめ管理サーバとの接続方法を整理しておくことを推奨



応用編：デザインパターンの組み合わせ

- これまでご紹介したデザインパターンを組み合わせる
 - 例1：SaaSと閉域内の社内システムの両方にアクセス
 - 例2：データ収集しながらリモートアクセス



必要な時に必要なだけ利用する
コストを最適化しセキュリティリスクを低減

まとめ

- SORACOMサービスの背景にはIoTの課題がある
 - 同様にクラウドサービスの背景にもIoTの課題がある
- IoTの課題にはパターンがある
 - 課題を整理し既存のサービスを活用できるか検討する
 - 予め課題解決のデザインパターンを理解しておく
 - デザインパターンを組み合わせて課題解決

SORACOMの願い



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