コンテナ基盤を活用したIoTサービスと eSIMアプレット連携の取り組みについて

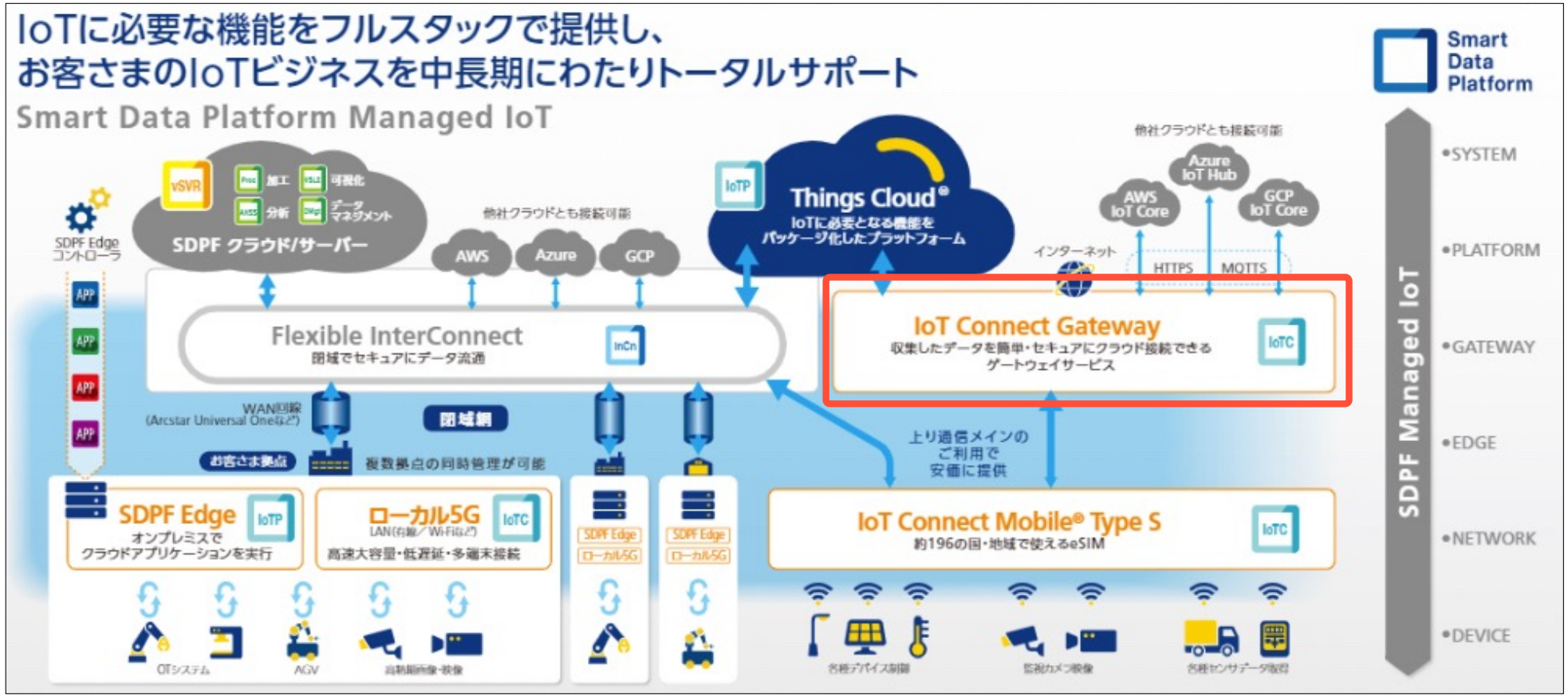
Open Networking Conference Japan
2023/11/10

NTTコミュニケーションズ株式会社
PS本部5G&IoTサービス部
角田佳史
村田一成

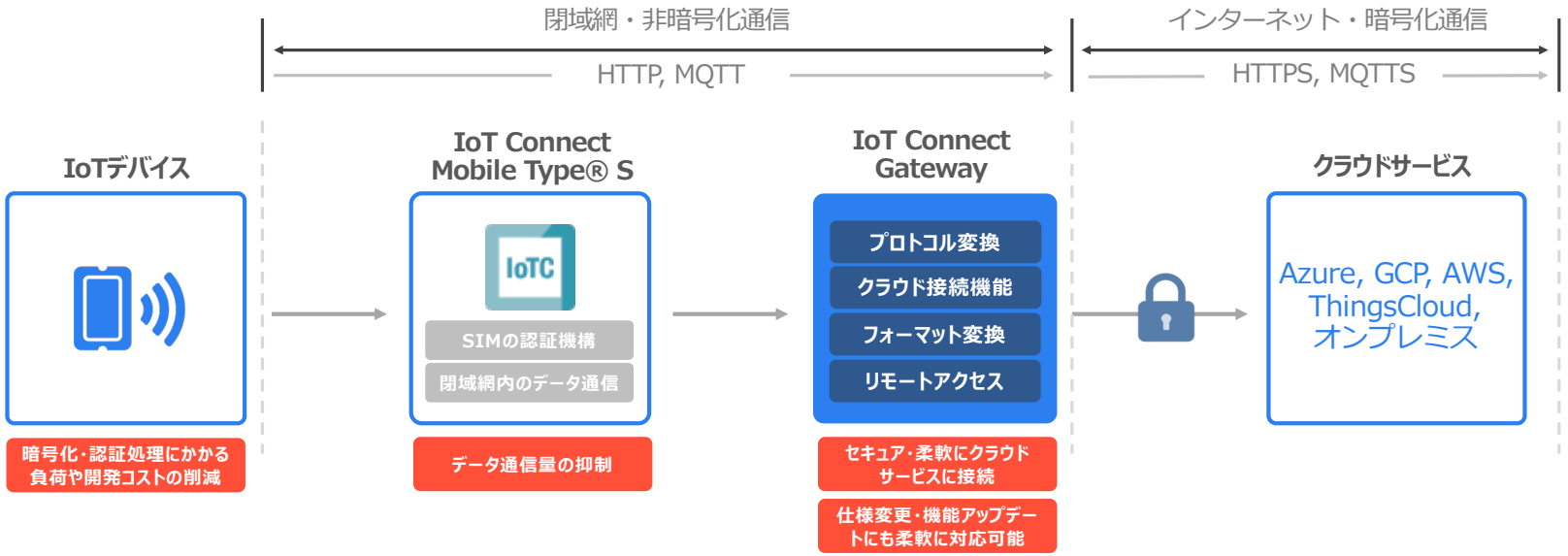
アジェンダ

1. IoT Connect Gateway概要
2. IoT Connect Gatewayリモートアクセス機能
3. IoT Connect GatewayとeSIMアプレット連携
    1. アプレットを使うことによる運用保守時の課題に対するアクション
4. eSIMアプレット概要
5. まとめ

Smart Data Platform Managed IoT



IoT Connect Gateway



クラウドサービス接続

プロトコル変換

IoTデバイスから送られた非暗号化データを、IoT Connect Gatewayサービスにて暗号化

クラウドアダプタ

また、各クラウドサービスへの接続時に必要となる接続情報や鍵交換を代理で実行

コンフィグマネージャー機能

- 各種デバイスのパラメータを元に設定ファイルを生成するコンフィグ生成機能
- デバイスごとに個別の設定ファイルを配信可能なコンフィグ配信機能

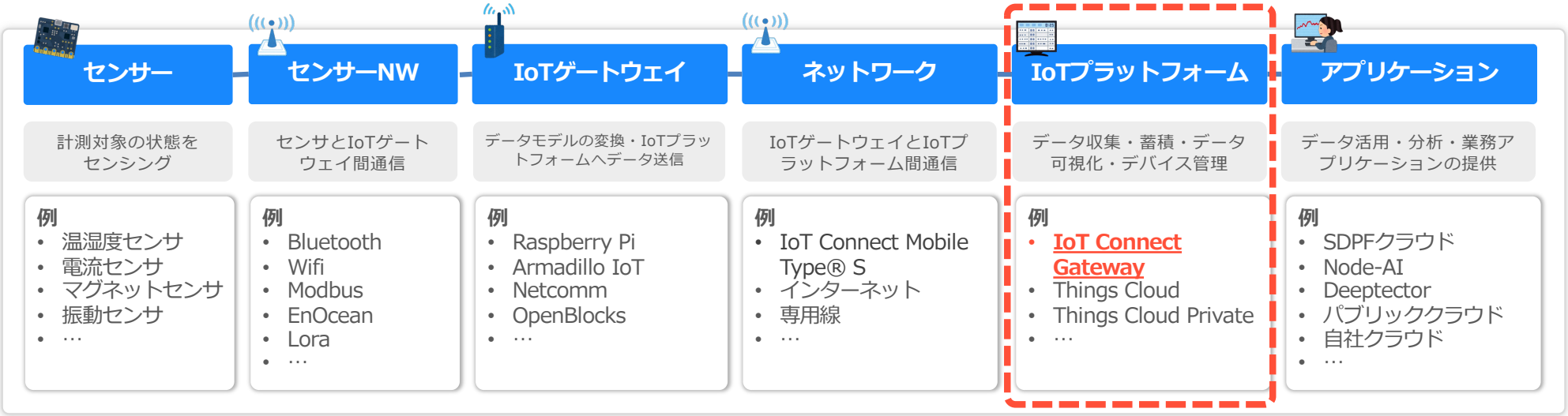
リモートアクセス機能

- 必要なときにのみお客様拠点からIoTデバイスにアクセスを許可する機能を提供
- IoT端末の遠隔保守管理やセキュリティ対策が簡単に

IoTシステム構築時の課題

- 既存システムのIoT化には開発コストやリードタイムが必要
- デバイスからアプリなど広範囲な要素を組み合わせる必要がありハードル高い
- 開発・構築時さながら保守・運用時においてもデバイス更改や障害時対応など考えることは多く
  如何にそれらのリードタイムを抑えられるかが重要

IoTシステムでよく見られる構成



IoTシステム構築時の課題

開発・構築時の課題

- IoTデバイス毎にクラウドサービスに応じた実装や、証明書・鍵情報を配布しなければならない ―― クラウドサービス接続

- デバイスとクラウドサービスのデータ形式が異なるため、個別のカスタマイズが必要になる ―― フォーマット変換機能

- 利用用途によってクラウド環境が異なるため、データを複数回送信する必要がある ―― ミラーリング機能

IoTシステム構築時の課題

保守・運用時の課題

- 各拠点に点在するIoTデバイスの設定変更作業を実施するために多大なコストが必要 —— コンフィグマネージャ機能

- 遠隔地に設置された多数のデバイスの不具合時に迅速に現地確認しにいくことが難しい —— **リモートアクセス機能**

- SIM関連情報や電波強度などの情報を送信したいが、IoTデバイス側に追加開発が必要 —— **eSIMアプレット連携**

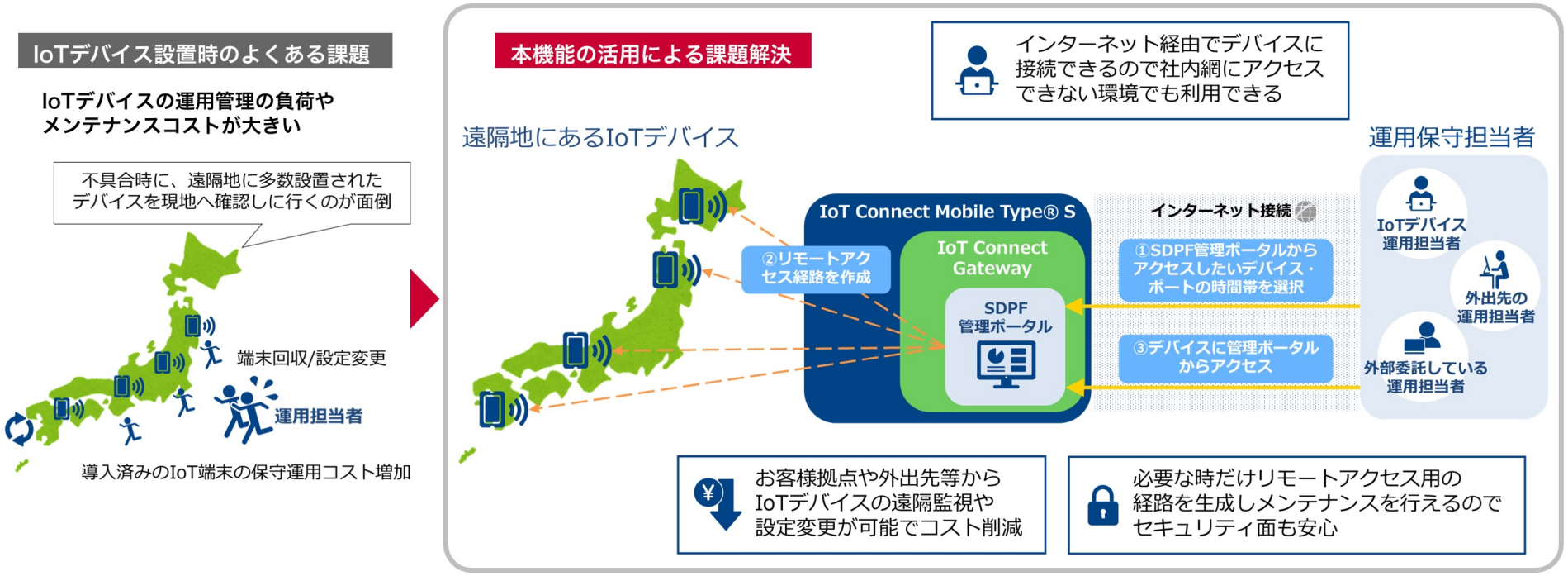
IoT Connect Gatewayサービスメニュー一覧

メニュー	サービスカテゴリ	概要	Input Protocol	Output Protocol	転送先クラウドサービス
クラウドサービス接続	**スタンダード (Pconv)**	IoTデバイスから通信をプロトコル変換を行うための Adaptor	HTTP MQTT	HTTPS MQTTS	任意のHTTP Server 任意のMQTT Server
		IoTデバイスから各種クラウドIoTプラットフォームに プロトコル変換を行い接続するためのCloud Service Adaptor	HTTP MQTT	HTTPS MQTTS	AWS IoT Core Azure IoT Hub NTTCom Things Cloud
	イベント(Event)	IoTデバイスから直接クラウドのイベントHUB系のサービスに 接続する Cloud Adaptor	HTTP	HTTPS	GCP Pub/Sub Azure IoT Hub
	ファンクション (Func)	IoTデバイスからクラウドサービスの Function を 直接実行するためのCloud Adaptor	HTTP	HTTPS	AWS　Lambda GCP Functions Azure Functions
	ストレージ (Storage)	IoTデバイスからクラウドサービスの Storage へ接続する Cloud Adaptor	HTTP	HTTPS	AWS S3 S3互換　Wasabi等

メニュー	機能	提供プロトコル	概要
コンフィグマネージャー	IoTデバイスの設定をICGW基盤から配信、一括変更を実現し、 キッティングコストや設定変更コストを簡略化する機能	HTTP	IoTデバイスが利用する設定ファイルの生成と 遠隔からの更新
リモートアクセス	任意のIoTデバイスに遠隔ログインできる機能をオンデマンドに提供する機能	ポータルから指定の任意の TCPポートに対応	IoTデバイスへのリモートアクセスを提供する
フォーマット変換	IoTデバイス、クラウド側のシステムを変更することなくデバイス、 クラウド間のデータフォーマットの相違を吸収する機能	クラウドアダプタプロトコルに準拠 (スタンダード、イベント、ファンクション)	データ・フォーマットを任意の形式に変換する機能
ミラーリング	IoTデバイスから送信したデータをクラウドアダプタの複数の 送信先にデータを複製して送信する機能	HTTP	IoTデータからのデータを複製し、複数のクラウド アダプタに送信する機能

リモートアクセス機能

- ユーザ拠点や外出先などから遠隔地にあるIoTデバイスにリモートアクセスすることで、現場に行くこと無しにメンテナンス作業が可能に
- IoTデバイスに固定のグローバルIPを割り振ることなく、セキュアにリモートアクセスを実現
  - 送信元IPアドレス制限、接続可能な時間の制限(最大8h)



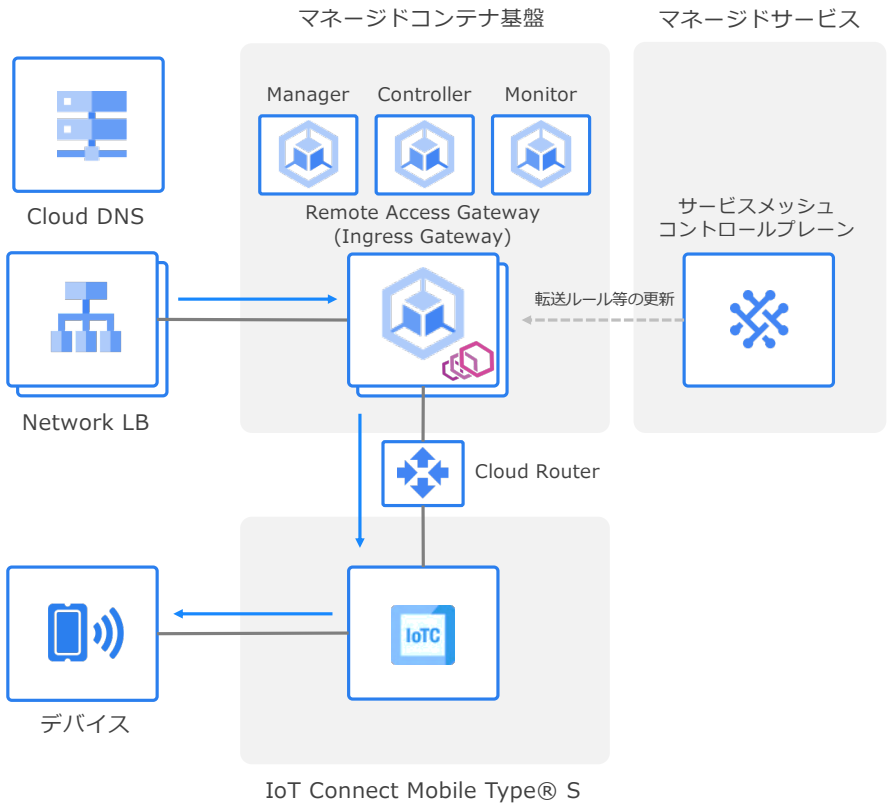
リモートアクセス機能

サービスメッシュの活用

- サービスメッシュとクラウドサービスを連携し、機能要件を満たしたサービスを迅速に開発できる
  - 接続先のポート管理や転送ルールなども KubernetesのAPIとして柔軟に管理できる
- 将来的なユーザのトラヒック需要増に応じて、柔軟にスケールアウト・スケールダウンできる
  - データプレーン自体もコンテナとして動作

Kubernetes Operatorの活用

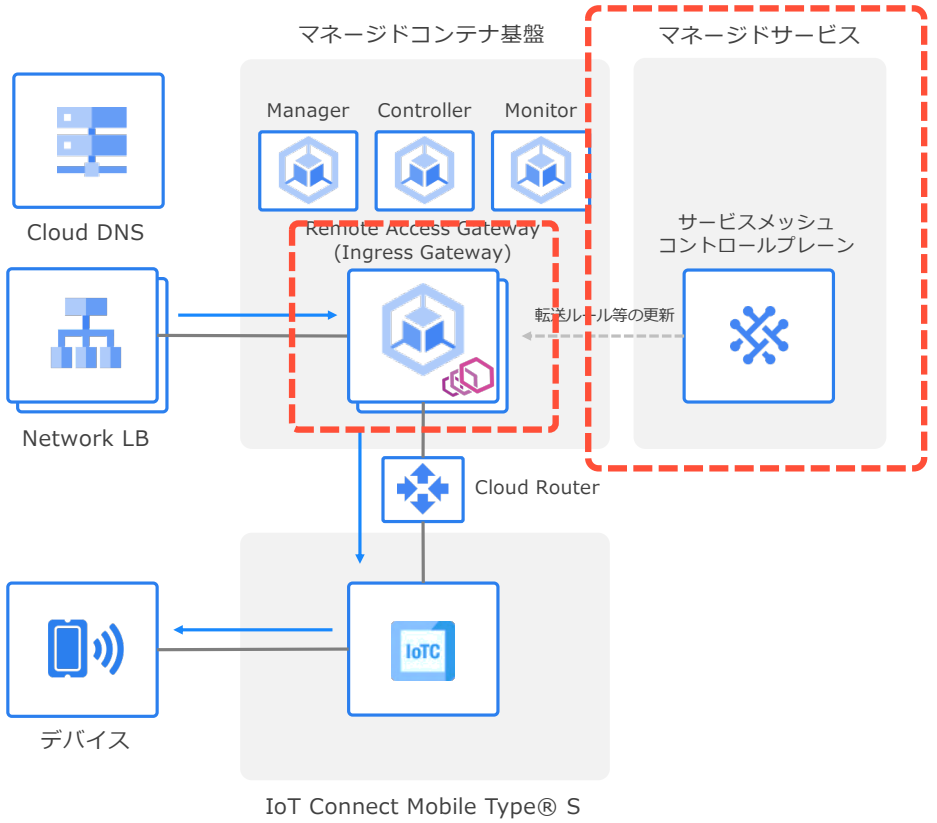
- Kubernetesの機能を活用できるため、スクラッチで機能開発を行うよりも、効率的に開発が可能



リモートアクセス機能

サービスメッシュの活用

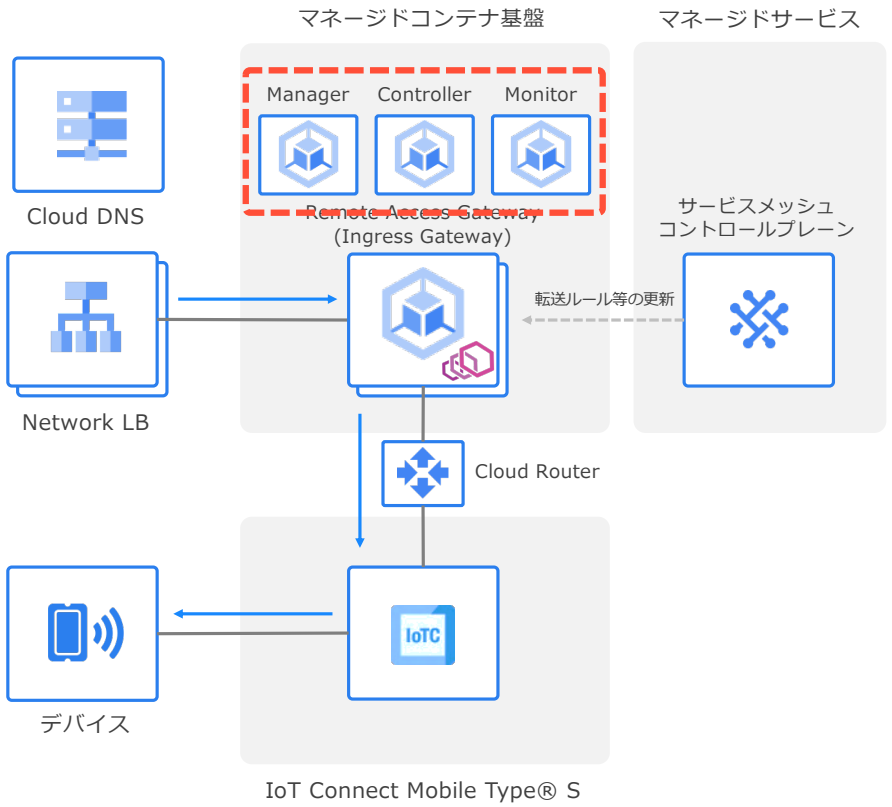
- マネージドコントロールプレーンを使用
  - 定期的なアップグレードなど運用負荷を下げつつ、主要な機能開発にスコープを当てたい
- データプレーンはセルフマネージドを利用
  - マネージドデータプレーンも提供されているが、データプレーンの更新はユーザ通信にダイレクトに影響するためセルフマネージドを使用
    - メンテナンス時間でデータプレーンを更新で対応
- サービスメッシュのデータプレーンはプロキシの機能単体で利用している
  - ポッドへのサイドカープロキシなどは未使用



リモートアクセス機能

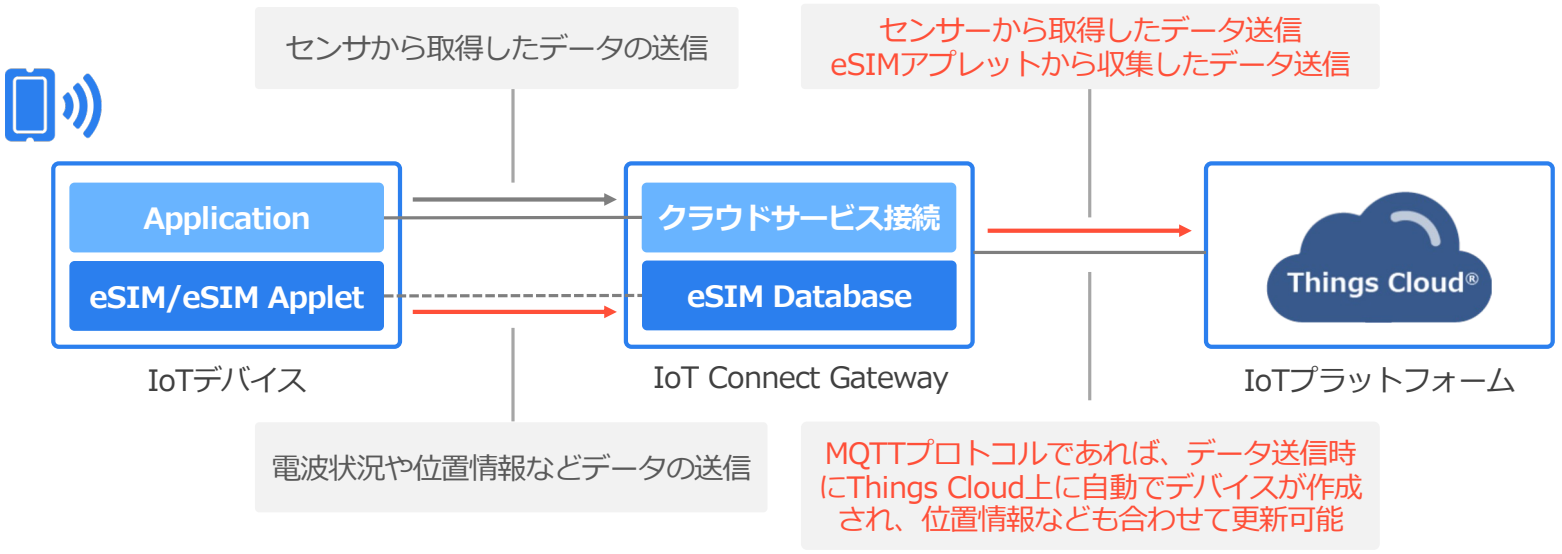
Kubernetes Operatorの活用

- リモートアクセス関連の各種リソースを管理するコントローラを独自に実装
  - 接続先デバイスに関する設定をカスタムリソースを定義し、サービスメッシュの既存リソースと連携
    - Gateway, VirtualService, ServiceEntry..
  - サービスメッシュの活用により、主要な機能であるコントローラや関連機能の開発に注力できる
- デバイスに対する接続性確認のため、定期的にユーザ設定ポートを監視する仕組みを動作
  - Operatorの機能が膨らむのを避けるため、接続性確認のためのコンテナは別で動作
  - 接続性が確認できた場合にのみ、コントローラから動的に払い出されたエンドポイントを通じデバイスへ接続可



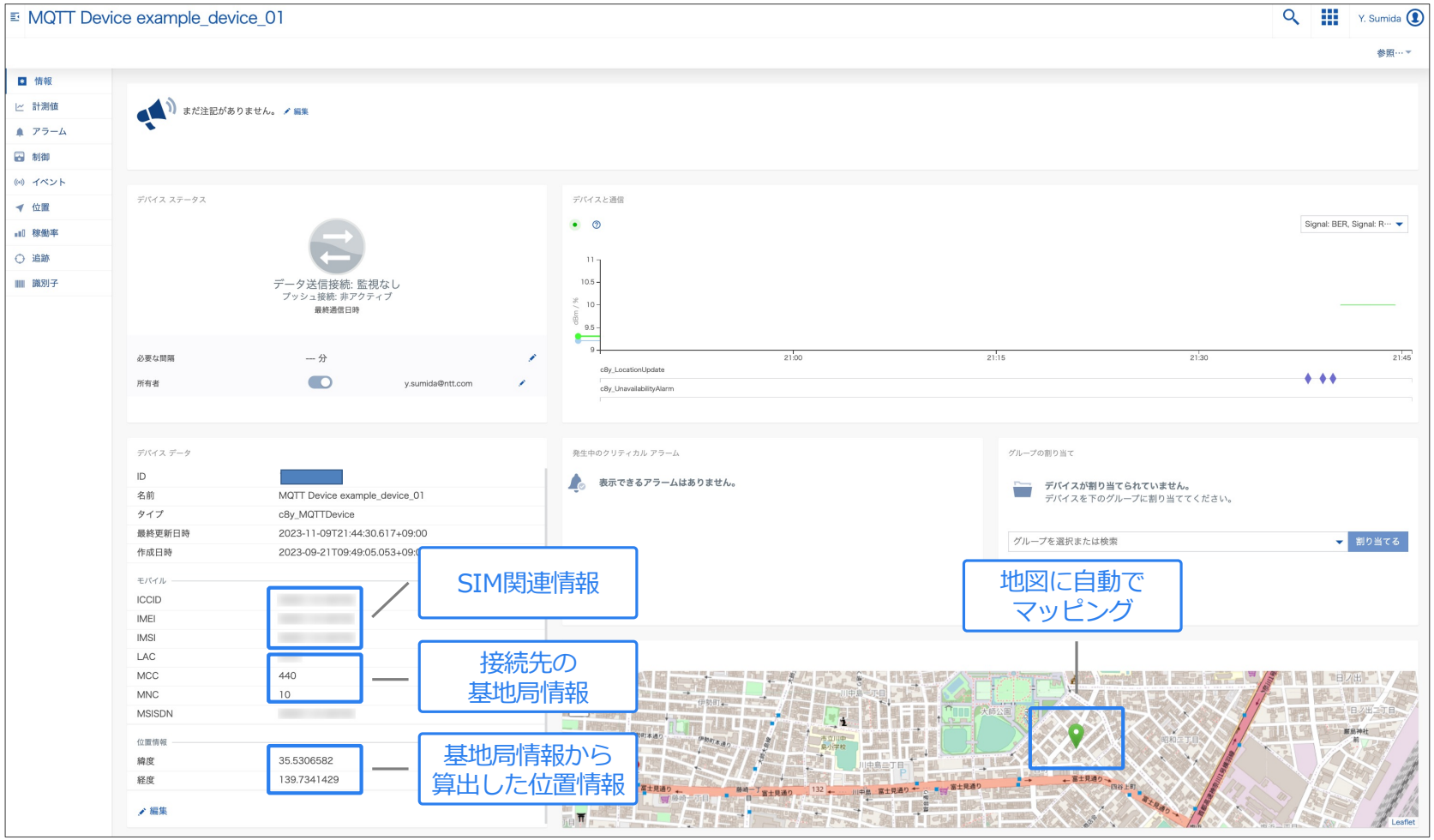
ICGW x eSIMアプレット連携

- eSIMアプレットが有効化されたSIMをデバイスに挿入するだけでデータ連携が可能
  - eSIMアプレットのプログラマブルな特徴を活かし、様々なユースケースに対応可能
  - ICGWとの連携では、位置情報や電波状況など幅広いケースで必要とされるデータ連携を想定
- IoTプラットフォームのデバイス管理の仕組みと簡単に連携できるという点を意識
  - ICGWを介して、eSIMアプレットから収集したデータとIoTプラットフォームを自動連携するなど
  - 現在はIoTプラットフォームの１つであるThings Cloudとの連携を検証



ICGW x eSIMアプレット連携 – IoT Connect Gateway 画面

ICGW x eSIMアプレット連携 – Things Cloud 画面



ここまでのまとめ

IoTシステムの開発や運用をコンパクトに実現するサービス開発

- 開発・運用のリードタイムを抑え、簡単に使い始められるサービス群を提供
  - IoTデバイスの証明書や鍵管理の集中管理やデータ通信量の削減に寄与するクラウドサービス接続機能
  - 遠隔拠点からIoTデバイスに対して簡単にアクセスできるリモートアクセス機能など
- IoT Connect Gatewayとして全体的にマネージドサービスを活用しつつ、
  モダンな技術を取り入れることで将来的なユーザ需要に応じた柔軟なシステム開発
  - サービスメッシュやオペレータなどの技術の取り込みなど

効率的なIoTシステムの開発をサポートするeSIMアプレット連携

- プログラマブルなeSIMアプレットの特徴を活かし、
  IoT Connect GatewayやThings CloudなどのIoTプラットフォームとの連携を推進
  - よりコンパクトに簡単にIoTシステムを導入したいユーザをサポート

eSIMアプレット
開発中の新機能

SIMの特徴を活用し、新たなSIMカードの使い方をご提案します

NTTコミュニケーションズ株式会社
IoTサービス部門　村田 一成

- ICカードとアプレット領域について
- アプレット活用のユースケース
- 活用に向けた開発機能について

詳しい仕様は弊社ナレッジセンターに掲載しております
https://sdpf.ntt.com/services/docs/icms/service-descriptions/applet/applet.html

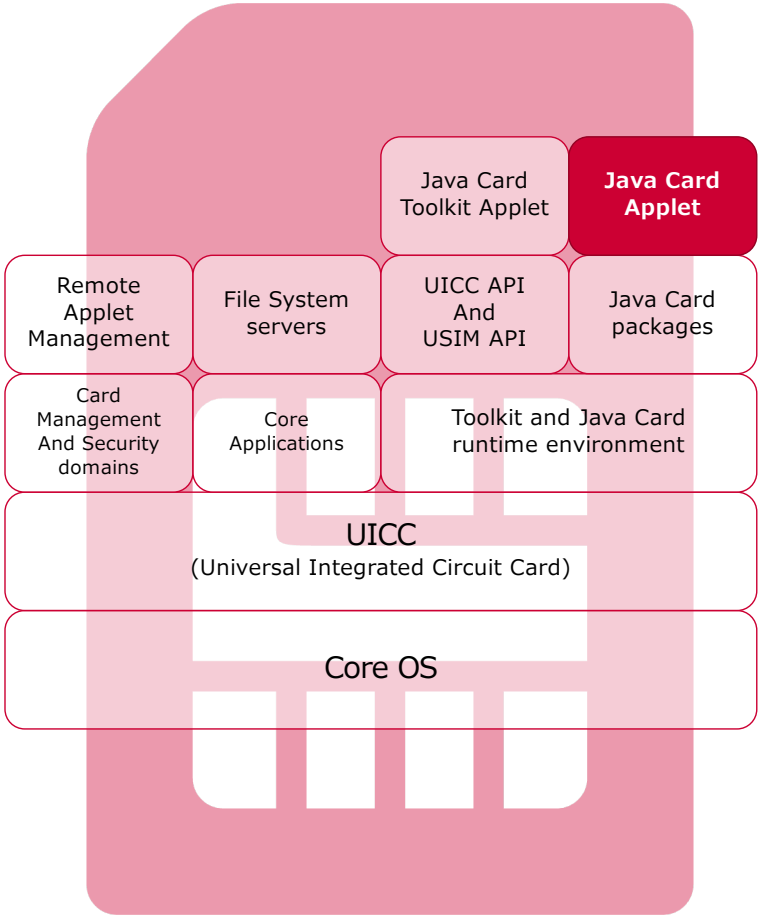
ICカードの特徴

・金融／決済関係
・交通関係
・サービス／流通関係（ポイントカード，メンバカード等）
・企業セキュリティ（身分証明，入退出管理等）
　など幅広く普及している

強固なセキュリティ（耐タンパ性）

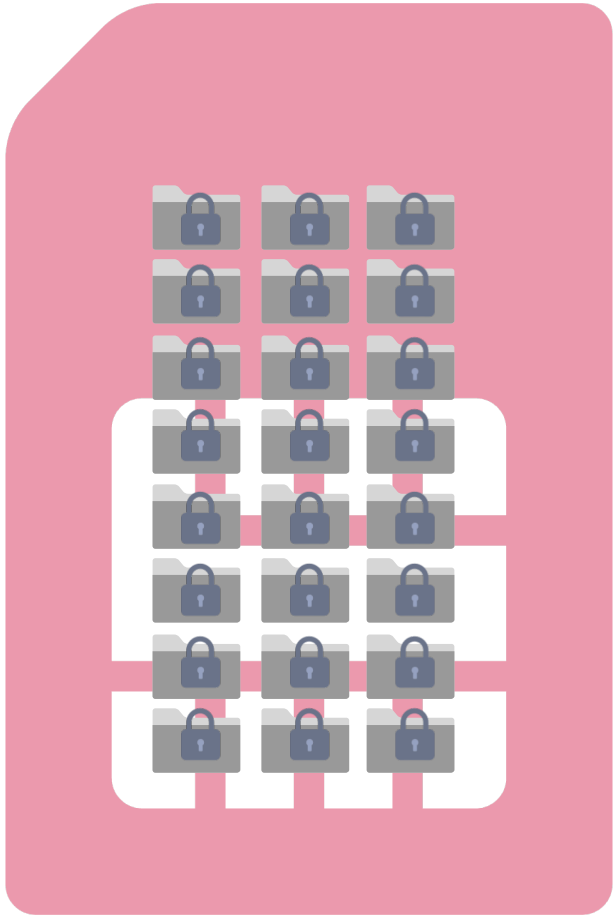
・外部からの不正アクセスや情報の改ざん操作が非常に困難
・物理的に開封した場合は、チップの回路が破壊される構造

アプレット領域



SIMカード内部にはOSが搭載され
Javaアプレットの実行環境が
あらかじめ用意されています

アプレット領域



SIMカード内部にはファイルシステムが存在し、そのアクセスは厳重な鍵で管理されています

また、この鍵は一般的に通信事業者やISP側で管理され、利用者（ユーザーやIoT事業者など）には解放されていない為ファイルシステムへのアクセスは制限されています

ユースケース

運用保守性の向上

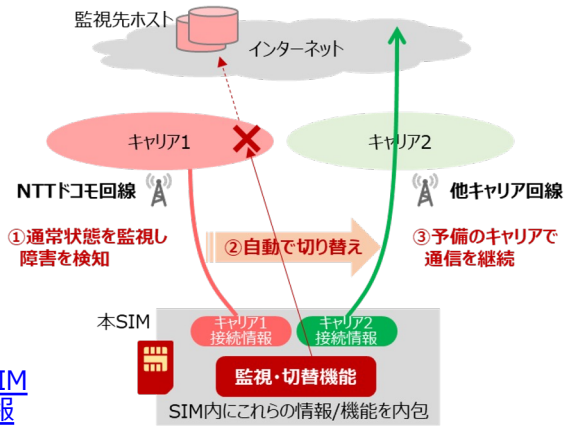
デバイス追加開発なく位置情報や電波強度等の動的情報の抽出

機微情報の安全な取り扱い

決済情報・個人情報をSIM領域に保存・サーバ送受信により更新

高可用性

接続キャリアの切替

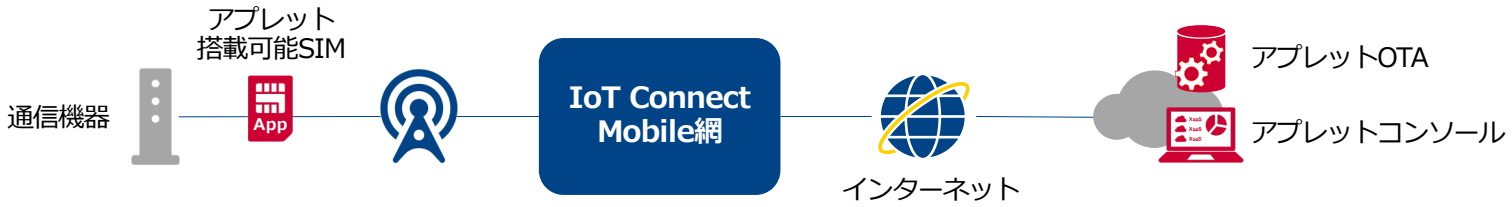


[ニュース 2023年3月28日:日本初 幅広い端末でキャリア冗長を実現できるIoT向けSIMを開発、トライアル提供開始 | ドコモビジネス | NTTコミュニケーションズ 企業情報]

開発中の機能について

IoT Connect Mobile type-S（ICMS）の付加機能として開発を進めています

1．アプレット搭載可能SIM
2．アプレットコンソール機能
3．アプレットOTA機能

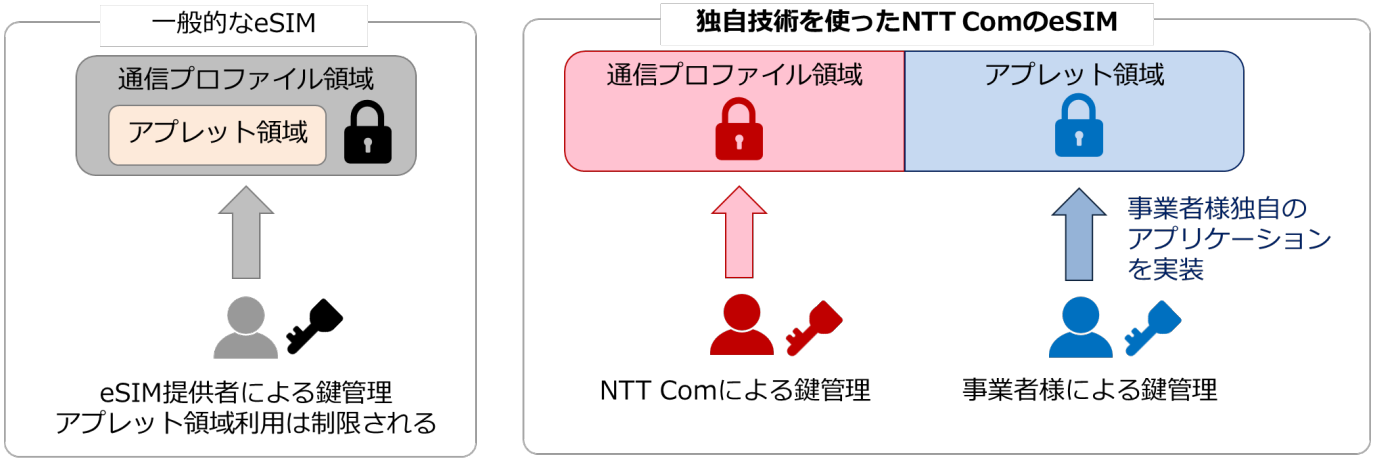


開発中の機能について

１．アプレット搭載可能SIM

弊社独自技術により、通信プロファイル領域とアプレット領域の管理を分離管理する事が可能になりました。
これにより、アプレット領域を事業者様にて管理／活用が可能になります。

アプレット領域の管理方法の違い　特許出願中



アプレット搭載可能SIMはサンプルアプリをインストールした状態でご提供します。
アプレットとして活用できる領域は凡そ３００ＫＢ程度。

開発中の機能について

2．アプレットコンソール

アプレットの管理コンソール機能を提供します。SIMに初期インストール済のサンプルプログラムから送信されるデータを一元的に参照管理可能。またAPIも実装している為、利用したいデータをお客様システムと連携する事も可能です。

SIMsメニューで参照可能でデータの一覧

ICCID	SIMカードの識別子
Status	契約状態
Connection	オンライン or オフライン状態
IMSI	加入者の識別子
MSISDN	電話番号
IMEI	機器の固有識別番号
RSRP	基準信号受信電力(-44 ～ -140)
RSRQ	基準信号受信品質(-3 ～ -19.5)
LAC	携帯電話の基地局の地域コード
Cell ID	基地局の識別子
Modified	作成・変更日時

その他、以下の機能も実装しています。

・ユーザー管理
・テーマ設定
・システムメール設定
・ログ機能
　システム、SIMデータ
・多要素認証設定

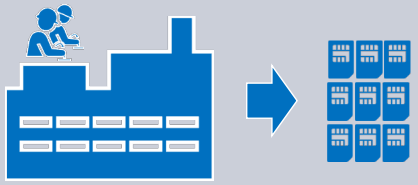
デモンストレーションさせて頂きます

開発中の機能について

3．アプレットOTA機能

SIMへアプレットをインストールする為に生じる煩雑な工程をOTA（Over The Air）で解決します。

①SIMメーカーによる生成

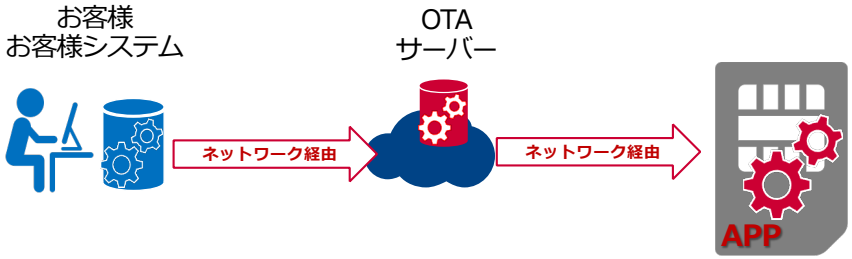


想定される課題
・最低発注ロット　・納期　・コスト

②手作業による生成

想定される課題
・作業稼働量　・品質　・コスト

SIMへのアプリケーションインストールに関わる課題を
安全且つスピーディにOTAで解決します



- ✓ 1枚のSIMから対応可能
- ✓ 数分～数営業日でインストール
- ✓ 低コスト（主に導入後の更新）
- ✓ 特殊なスキルは不要

まとめ と メッセージ

- SIMは耐タンパ性を備えていて安全
- アプレットは自社開発しトライアンドエラー可能
- スモールスタートに対する導入障壁が低い
- APIで自社システムと連携可能
- 導入後の維持管理もOTAにて容易且つ低コストに実現

本機能を使った様々なユースケースやビジネスモデルを
一緒に検討いただける事業者様を探しています

ご興味をお持ちの企業様がおられましたら、
ぜひお声がけいただければと思います。

docomo business

ご清聴ありがとうございました