Orchestrating a brighter world

NEC

資料37－5

総務省 情報通信審議会 情報通信技術分科会
IPネットワーク設備委員会（第37回） プレゼン資料

弊社IoT製品・ユースケースご紹介、及びそのインターネット接続形態とセキュリティ対策の整理

2018年 3月 30日

日本電気株式会社　IoT基盤開発本部
ソフトウェアアドバンストテクノロジスト
(サイバーセキュリテイ)
桑田 雅彦

Orchestrating a brighter world

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

目次

- NECグループのIoT製品の例
- IoT製品のユースケースの例
- IoT製品のインターネット接続形態
- セキュリティ対策の必要なIoT機器
  （公衆電気通信サービス保護の観点から）
- IoT機器にかかわるセキュリティ対策の整理
  （同上）

NECグループのIoT製品の例

NECグループのIoT製品の例

Wi-Fi ホームルータ
“Aterm” シリーズ

デジタルサイネージ
”PanelDirector”

POS端末
“TWINPOS” シリーズ

IoTデータ収集基盤
“エッジゲートウェイ”

耐環境・極省電力センサデバイス
“難設置IoTアクセス端末”

IoTデータ収集基盤 “エッジゲートウェイ”

ネットワークに繋げられなかった機器や各種センサのデータを収集、クラウド連携で現場の機器の稼働状況見える化など新たなサービスを創出

導入によるメリット

- **今までネットワークに接続できなかった現場の機器や各種センサからデータを収集し、クラウド連携が可能**
- **エッジソフトウェアにより、現場の安全なIoT化を支援・効率化**

商品情報

小型
A5サイズ

●環境に応じた運用形態
・オンプレミス／クラウド連携などの運用に柔軟に対応
・上位接続支援ソフト(CONNEXIVE IoT Connectivity Engine)に対応

●アプリケーション実装環境
・SDKによるアプリケーション開発支援環境を提供
・サーバやクラウドを介さない処理を実装可能

●セキュリティ(Device Security機能)
・ホワイトリスト方式による通信・デバイスの管理

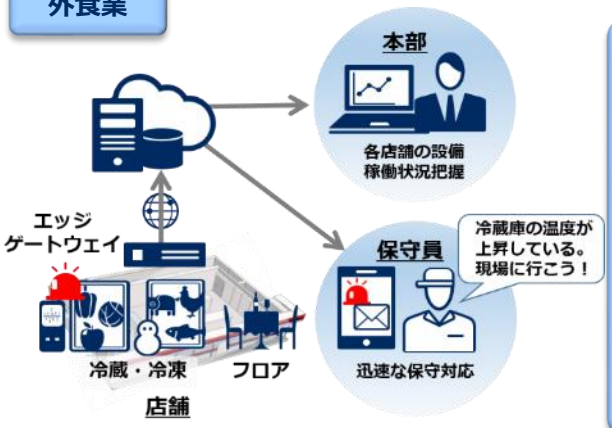
●耐環境性
・動作環境温度（-5～55℃）/湿度（10～90%)に対応
・ファンレス筐体／コネクタ耐サージ性強化により幅広い設備・センサに適用可能

●長期供給・保守対応
・出荷開始後3年間供給（2020年8月末まで供給予定）
・5年間の長期保守（最大2025年8月末まで保守可能）

●無線対応(オプション)
・既存環境に影響を与えず通信可能(3G/LTE/無線LAN/920MHz)

活用イメージ

外食業



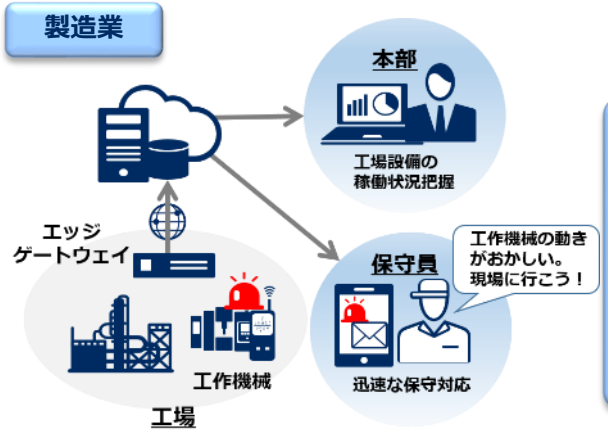
現場設備（冷蔵庫、空調、倉庫）の状況を見える化

温湿度の記録作業を自動化することで、測定漏れや手間（人件費）の削減、HACCP対応を簡略化

遠隔から設備の稼働状況把握や閾値設定

冷蔵庫故障や閉め忘れによる食材廃棄リスクを軽減

製造業



工作機械や業務用機器の設備や振動センサ等のデータ収集、見える化

無線接続（3G/LTE/無線LAN/920MHz）により既存設備に影響なくアドオン可能

メンテナンスを迅速に指示、故障の検知

耐環境・極省電力センサデバイス“難設置IoTアクセス端末”

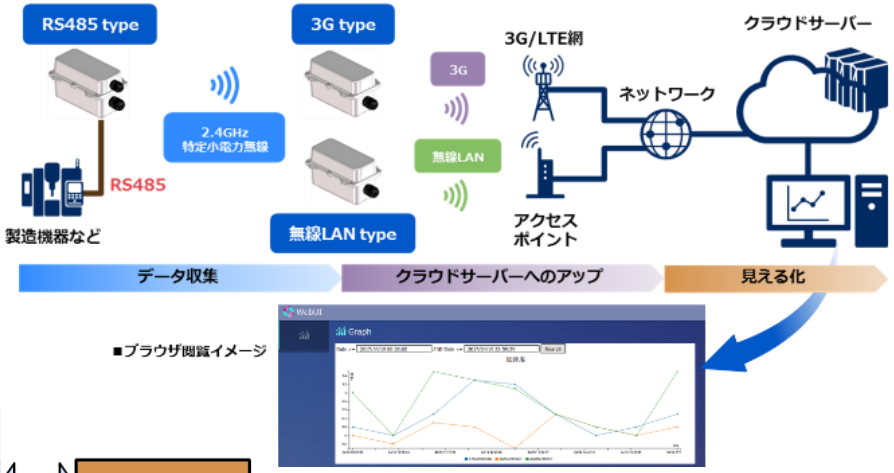
**屋外や電源の無い場所など設置環境を選ばずに、
遠隔モニタリングを実現する、通信機能付きセンサデバイス端末**

導入によるメリット

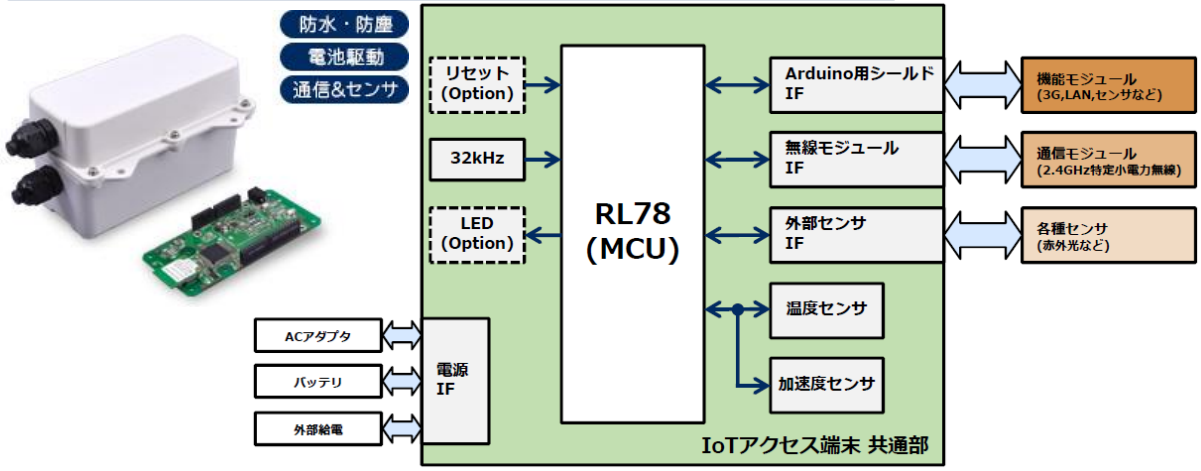
- 各種モジュール・センサを選択、組み合わせることで、システム要件、環境条件にあった機能を実現
- グローバルスタンダードであるArduino用シールドを搭載でき、検証・開発期間を短縮
- 防水・防塵、電池駆動に対応することで、屋外、水周り、電源のない場所などの設備でもネットワーク接続が可能

活用イメージ（スタートセット）

IoTアクセス端末にRS485、3G、無線LANの機能を搭載し、組み合わせて
クラウド・サーバへのデータ送信をOne Stopで実現します。



商品情報



IoT製品のユースケースの例

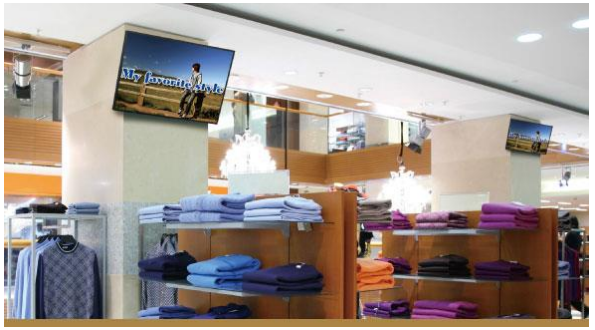
デジタルサイネージのユースケース

交通機関(空港、駅、バス停、港)
- 発着や乗り継ぎ案内の
  リアルタイム表示
- 施設案内や観光案内の表示

自治体・教育機関
- 施設利用者への情報通知
- 防災情報や観光情報の表示

医療機関
- 診察や会計時の番号表示
- 診察時間のご案内や
  医療情報のお知らせ

商業施設
- 館内利用案内で
  エンターティメントを空間演出
- 催事のご案内を発信し集客



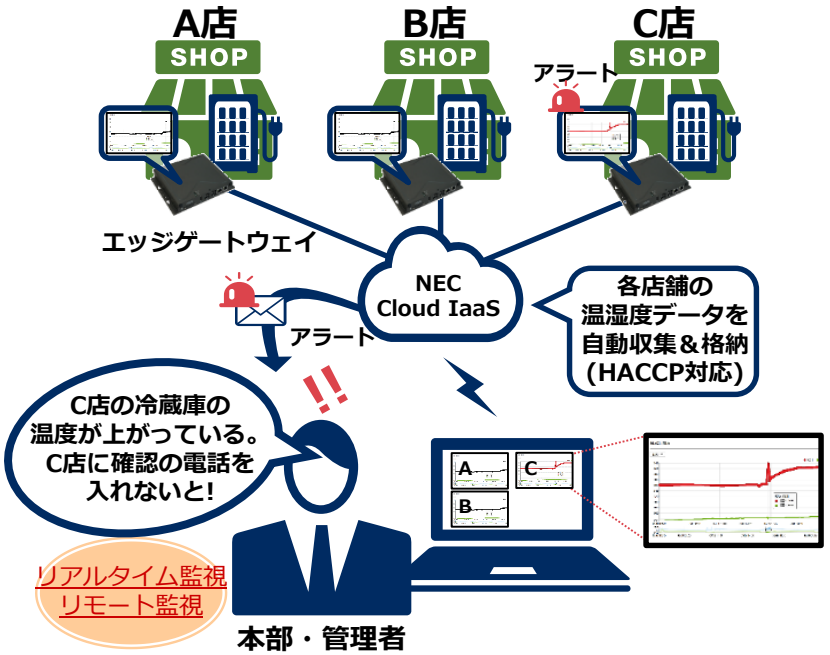
店舗
- 季節ごとの商品プロモーションや
  催事のご案内
- タイムセールなどの
  スポット情報発信

ホテル
- お客様が求める情報を表示し、
  利用者様の満足度を向上
- レストラン情報やイベントの告知

エッジゲートウェイのユースケース

店舗や工場などの設備稼働/環境管理

活用イメージ



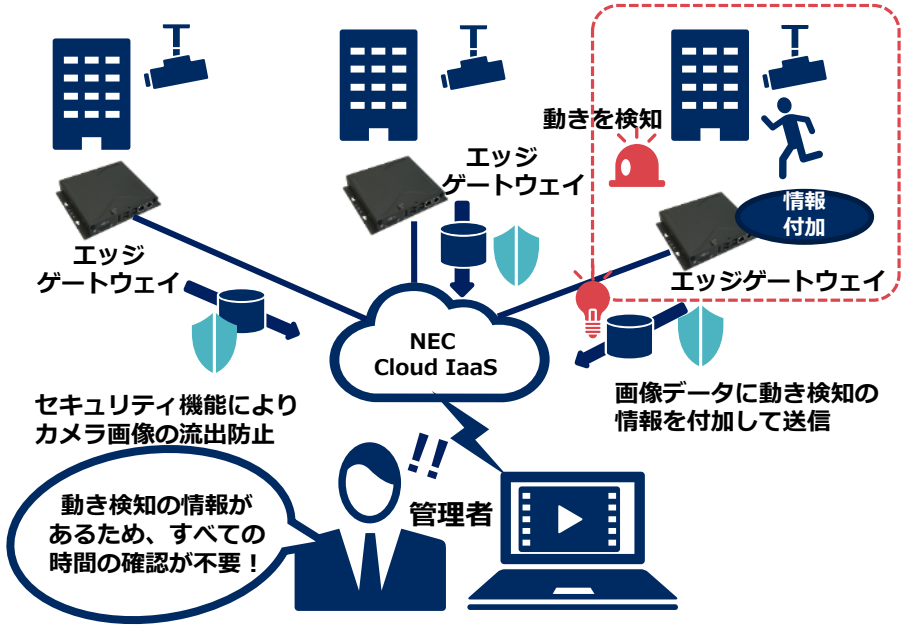
導入によるメリット

- 冷蔵庫、冷凍庫の閉め忘れ等による、食材廃棄や食中毒のリスクを軽減
- 温湿度の記録作業を自動化することで、測定漏れや手間(人件費)を削減し、HACCP※対応を簡略化

※HACCPとは、安全で衛生的な食品を製造するための管理規定の一つ。継続的な監視・記録として温度・時間管理が必要。

カメラ映像監視業務の効率化

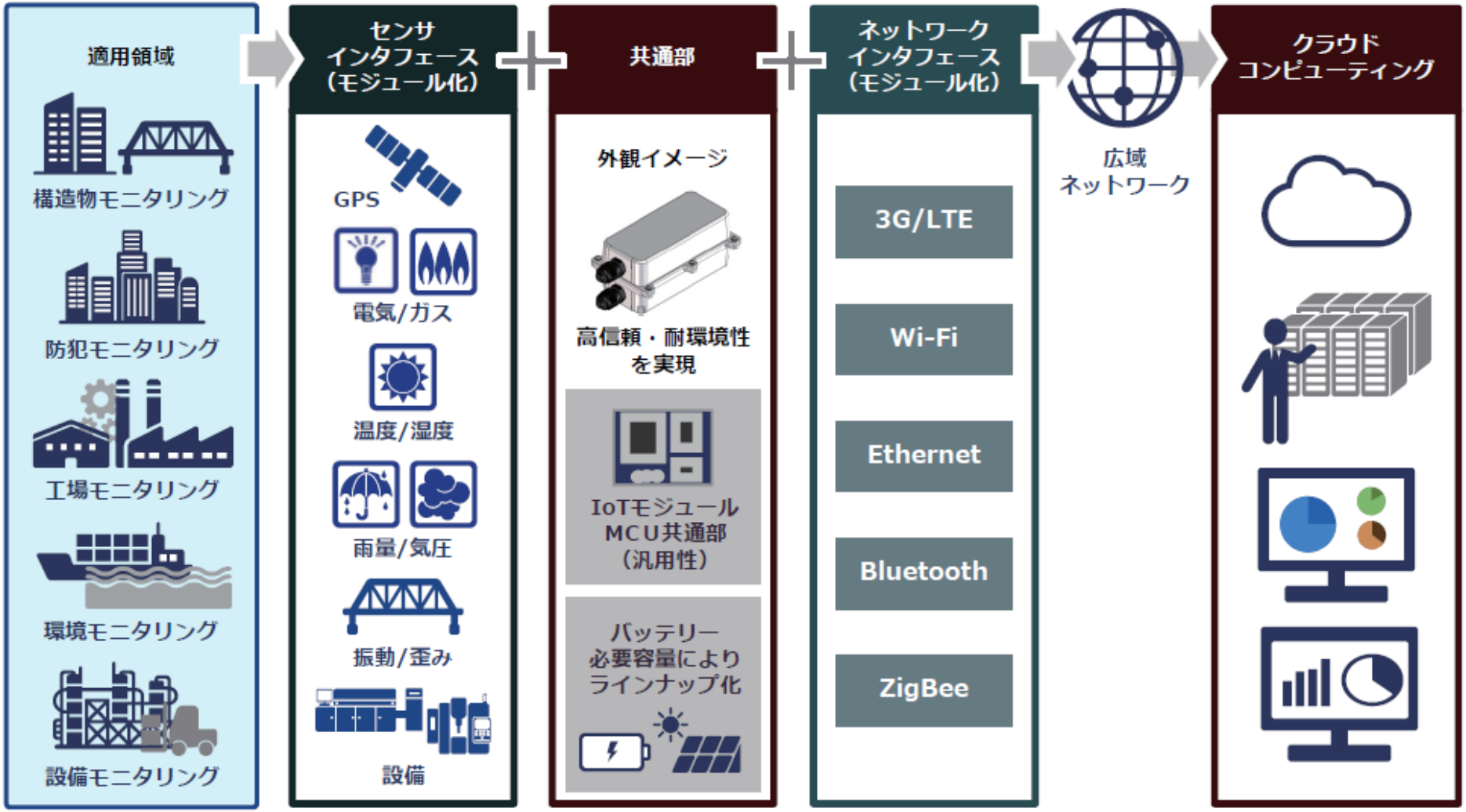
活用イメージ



導入メリット

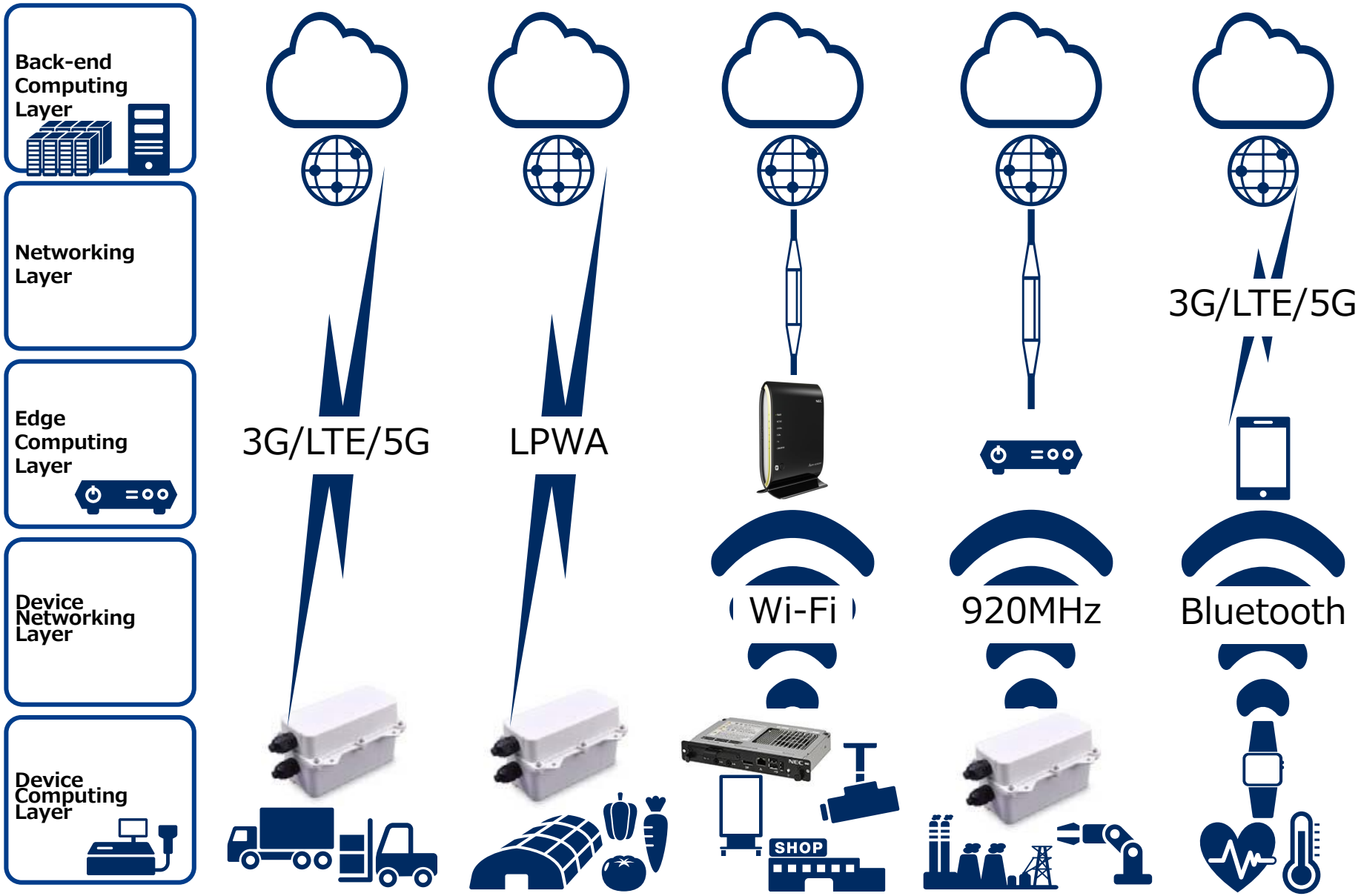
- 遠隔から各ビル・マンションのリアルタイムな監視が可能。既存建物にも導入可能
- 映像用レコーダが不要なため、設置場所の確保や定期メンテナンスも無し
- 映像の時間特定ができるので、確認が効率的
- 設置から運用までトータルコスト削減（エッジ活用による回線負荷軽減）

難設置IoTアクセス端末のユースケース



IoT製品のインターネット接続形態

IoT製品の代表的なインターネット接続形態



セキュリティ対策の必要なIoT機器
（公衆電気通信サービス保護の観点から）

セキュリティ対策の必要なIoT機器

公衆電気通信サービス保護の観点から、
少なくとも以下の条件に当てはまるIoT機器はセキュリティ対策が必要

- 何らかの経路でインターネットに接続され、
  （＝有線/無線を問わず、間接的、非定常的に接続されるものを含む）
  マイコンなどのCPUを搭載しデータ通信処理が実行可能なIoT機器

- 公衆無線通信サービスに影響を及ぼしうる、
  無線通信機能/インタフェースをもつIoT機器

IoT機器にかかわるセキュリティ対策の整理
（公衆電気通信サービス保護の観点から）

IoTにかかわる最近の主なセキュリティ問題

IoTシステムならではの脆弱性を突き、マルウェアを感染させ、
機器の不正制御や、**乗っ取った機器を踏み台にした大規模DDoS※攻撃**を実行
社会的に影響度の大きい被害が発生

※DDoS：サービス妨害

マルウェア Mirai

ルータやWebカメラ等、
エッジ/デバイス機器の管理者用の
初期設定ID/パスワードを不正利用、
機器を乗っ取り、
大規模DDoS攻撃の踏み台に

マルウェア BASHLITE

Webカメラやビデオレコーダ等、
エッジ/デバイス機器の
OSコマンドの脆弱性を突き、
機器を乗っ取り、
大規模DDoS攻撃の踏み台に

マルウェア Stuxnet

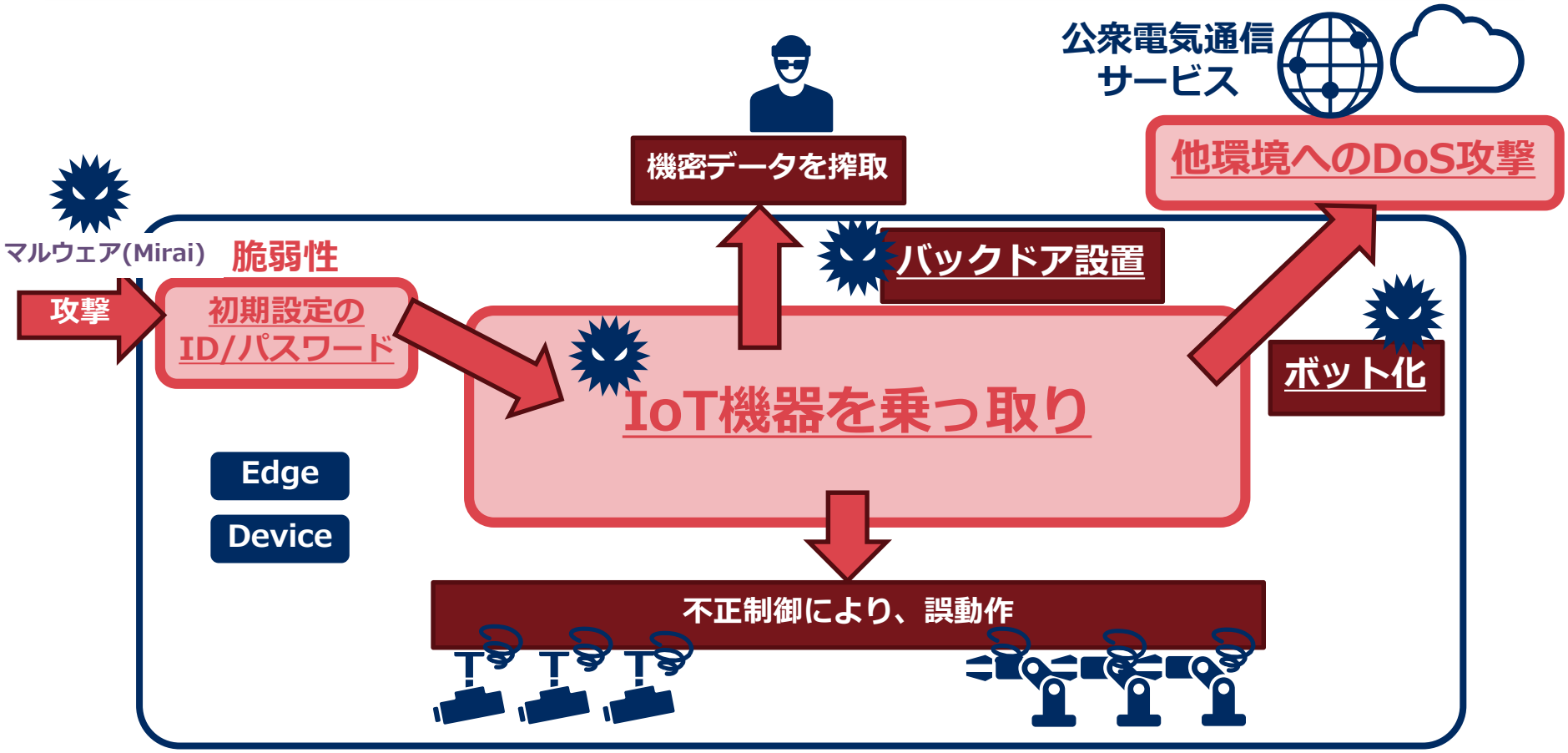
イランの原子力発電所(ウラン濃縮施設)の制御システムの端末に
USBメモリ等の接続を介して感染、
遠心分離機を不正に制御、
異常状態を引き起こし**機器を破壊**

マルウェア BlackEnergy

電力制御システムの端末に
標的型攻撃メールを介して感染、
電力制御のための通信を切断、
大規模停電が発生

IoT機器の主なセキュリティ問題による影響拡大の段階的過程

IoT機器の脆弱性を突かれ、
たとえば初期設定ID/パスワードを不正利用された問題から端を発し、
IoT機器を乗っ取られることで、IoT機器自体の被害に留まらず、
実社会の基盤をなす他の環境へ広範かつ多大な影響を及ぼす事態に

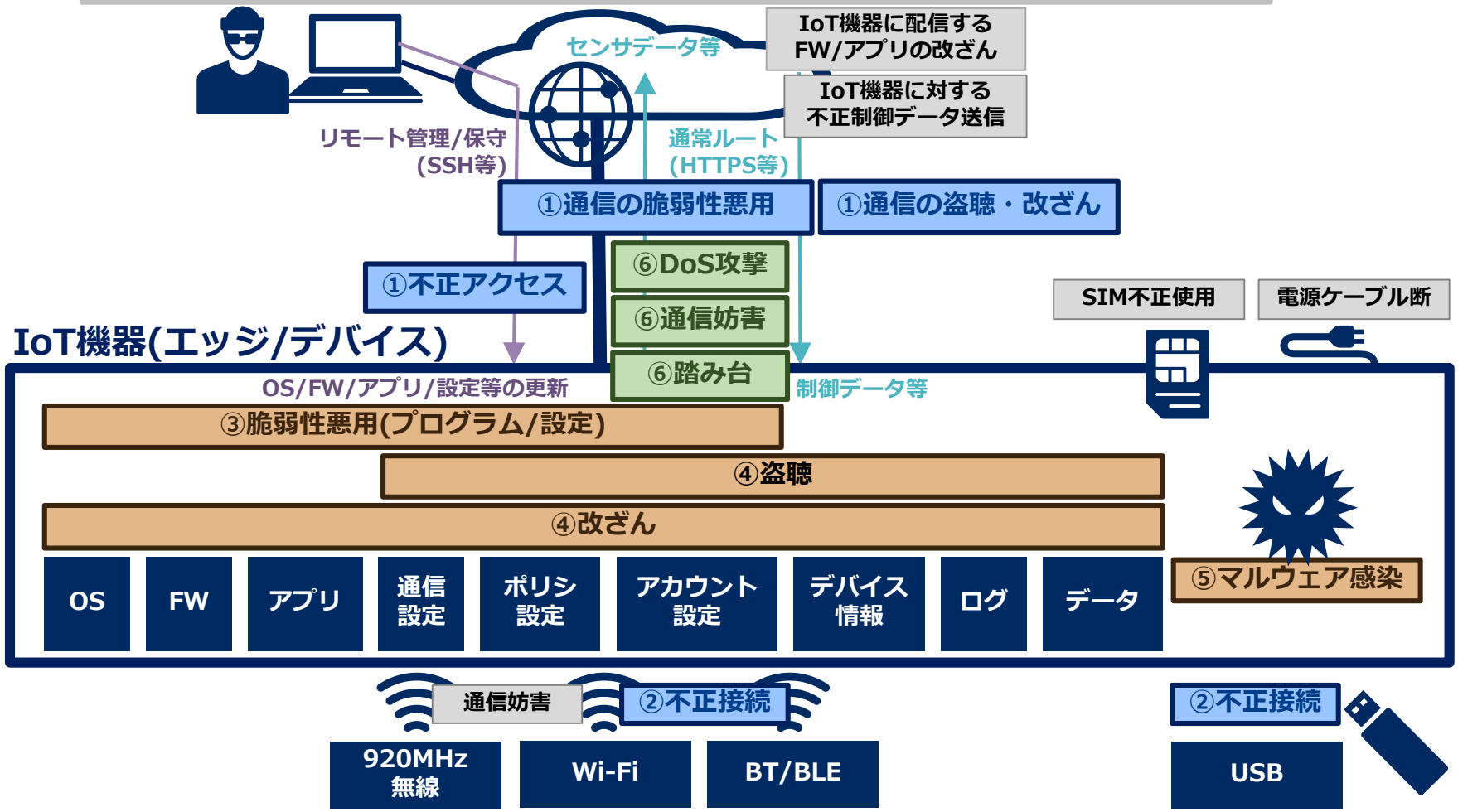


IoT機器が想定すべきセキュリティ脅威の整理

脅威整理のポイント

[入口] ①通信経路(データ送受信用、リモート管理/保守用)を介した
不正アクセス(そのための**脆弱性悪用、盗聴・改ざん**)、
②**不正デバイス接続**(同上)
[内部] ③**脆弱性悪用(プログラム/設定)**、④**盗聴・改ざん**、⑤**マルウェア感染**
[出口] ⑥**踏み台・通信/サービス妨害**(公衆電気通信/クラウドサービスへのDoS攻撃等)

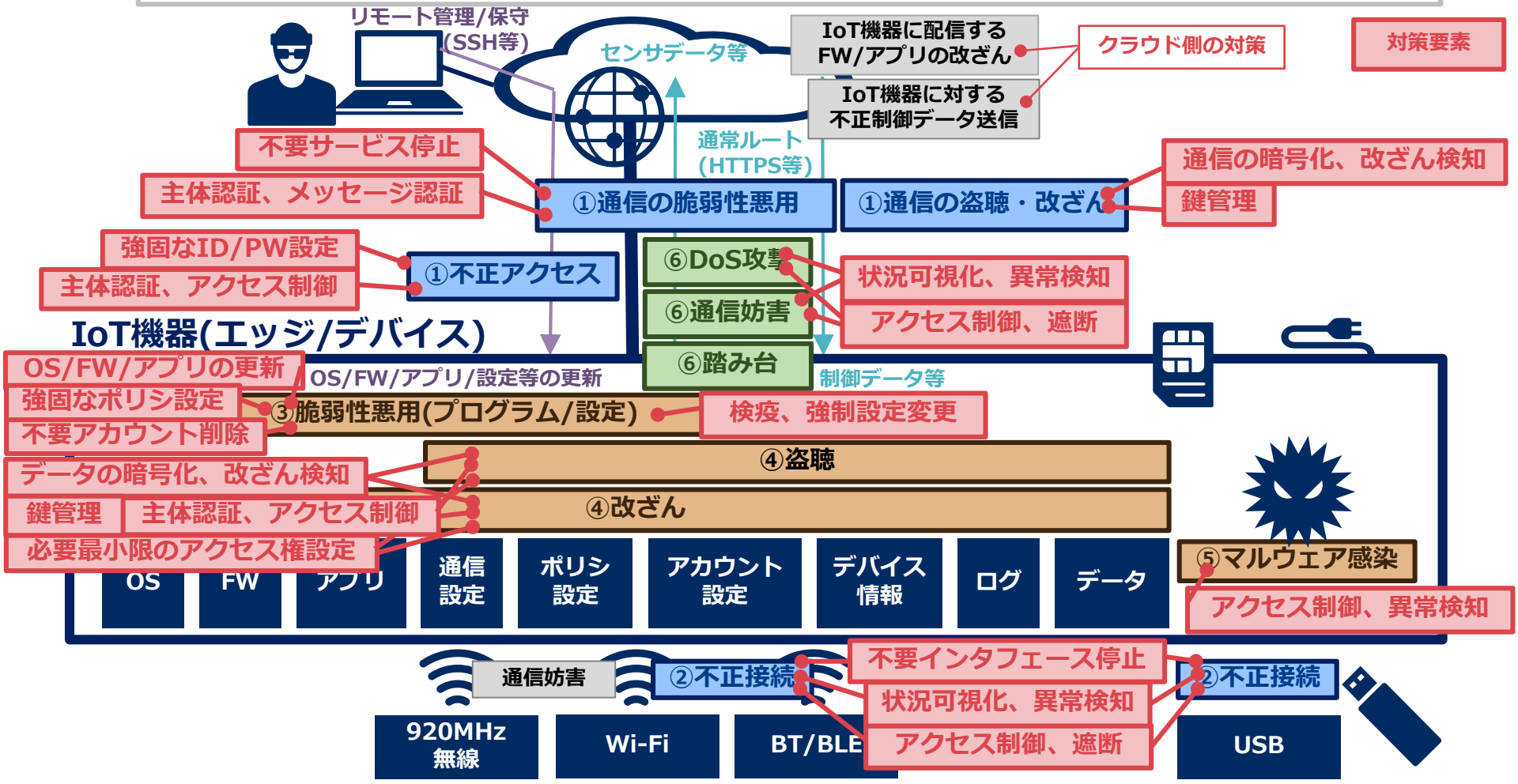
入口脅威(高優先)
出口脅威(高優先)
内部脅威(高優先)



IoT機器に必要な基本的セキュリティ対策の整理

対策整理のポイント

- 保護/管理の基本(1)：**脆弱性を塞ぐ(それを維持する)**ことが最も肝要
  （不要⇒停止/削除、強固な設定、必要最小限の設定、プログラム更新、検疫、強制設定）
- 保護/管理の基本(2)：**暗号化、鍵管理、主体認証、メッセージ認証、改ざん検知**
- 保護/管理の基本(3)：**アクセス制御、必要最小限のアクセス権設定**
- 運用の基本：**状況可視化、迅速な異常検知・対処(遮断、影響の極小化)**



IoT機器に必要な基本的セキュリティ対策（一覧）

1. 強固な管理用ID/パスワード設定
2. 不要なアカウントの停止/削除
3. 不要なインタフェース/サービスの停止
4. 強固なセキュリティポリシ設定
5. OS/ファームウェア/アプリ等ソフトウェアの脆弱性対策(更新)
6. リモートからのOS/ファームウェア/アプリ/設定等更新の保護
7. OS/ファームウェア/アプリ等ソフトウェア改ざん検知/防止
8. 通信/格納データの暗号化
9. 鍵管理
10. 主体認証、メッセージ認証、データ改ざん検知/防止
11. IoT機器の特定、認証
12. ホワイトリスト型アクセス制御、必要最小限のアクセス権設定
13. 状況可視化、異常検知
14. 隔離・遮断
15. 検疫、強制設定変更

IoT機器セキュリティ対策の役割分担、及び実施フェーズ(案)

- エンドユーザに対策を期待するのは実効的に難しく、IoT機器、IoTシステム/サービス、及び公衆電気通信サービスの提供者が役割分担して対策を実施するのが現実解
- Security by Design は重要だが、既に利用されている未対策のIoT機器が今後も長期的に継続利用されるため、利用開始後の対策整備・適用も重要

ライフサイクルフェーズ / アクタ	製品/システム/サービスの設計・開発時	利用/運用開始時	利用/運用中
IoT機器提供者	対策1-15	対策5,6	対策5,6
IoTシステム提供者	対策1-15	–	–
IoTサービス提供者	対策1-15	対策1-5,9,12	対策13-15
公衆電気通信サービス提供者	対策13-15	–	対策13-15
エンドユーザ	–	対策1,5	対策5


Orchestrating a brighter world
NEC