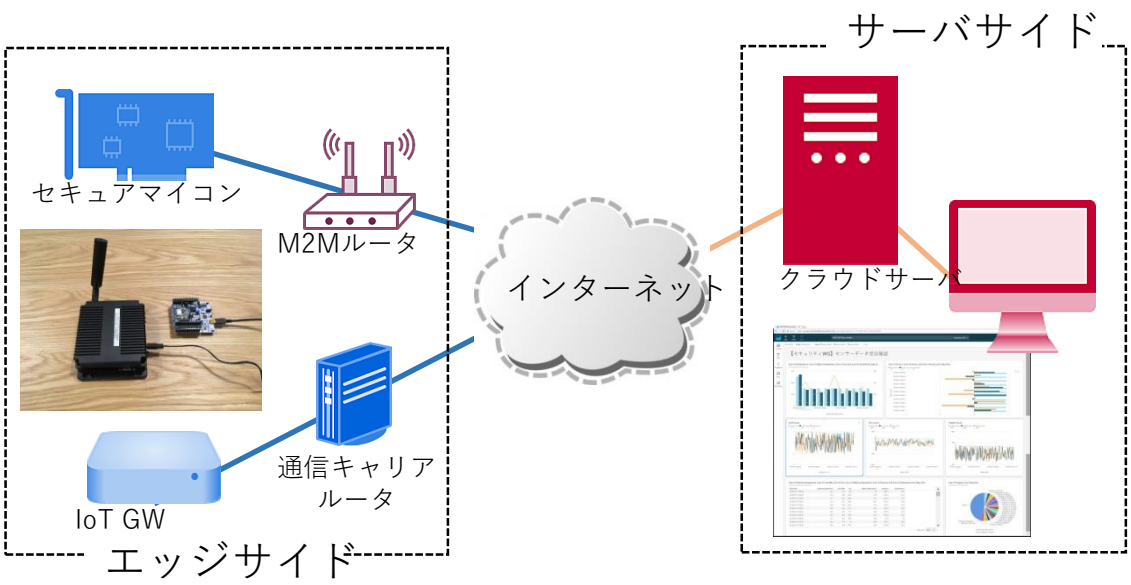
クラウド導入やインターネット通信のセキュリティ対策でお困りの方へ

「IoTセキュリティテストベッド」の構築

株式会社ウフル



IoTセキュリティテストベッドのシステム構成

図はエンジサイド・インターネットから疑似攻撃を仕掛け安全性を検証する環境を示しています。

アピールポイント

個々のIoTセキュリティ対策ソリューションを組み合わせて活用

IoTセキュリティ対策ソリューション共同体を結成！

↓

各社のソリューションを補完する機能を組み込み

セキュリティ検証で安全なIoT機器を流通

セキュリティテストベッドで想定ユースケースを検証！

↓

セキュリティ検証を実施した上で市場に出す

対策後の効果を知見として広め、セキュリティの必要性を啓発

クラウド、エッジ双方の設計者が脅威を視覚共有！

↓

ネットワーク越しの脅威を未然に捉えることができる

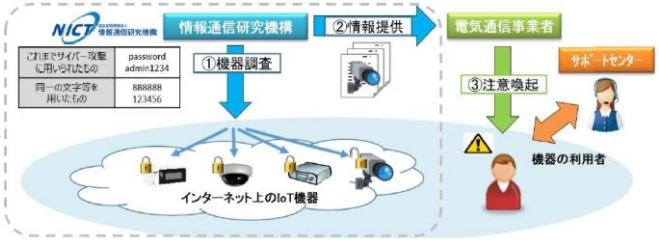
システム概要と開発経緯

多数の機器が相互に接続されるIoTでは、セキュリティリスクが日々増大しています。近年のIoTシステムに対する攻撃は高度化・複雑化しており、単一のソリューションで防ぎきることは難しく、多層防衛の考え方を導入することが重要です。
また、システムの組み合わせによって顕在化するリスクもあります。そこで、システムを組み合わせて脅威分析ができるテスト基盤としてテストベッドを構築することでセキュリティリスクに対する課題を解決！
機器の遠隔保守や環境インフラなどの屋外ネットワークを利用するIoTシステムのサービス提供者・利用者を応援します。

IoT機器のセキュリティ対策の高まりに関する情報（情報提供：総務省）

■2019年2月から脆弱なIoT機器のセキュリティ対策を促す「NOTICE」を開始

■2020年4月からIoT関連のサイバーセキュリティが法令で強化されます。
電気通信事業法に基づく端末機器の技術基準を定める省令を改正（セキュリティ対策　遮断制御機能　初期設定の変更　ソフトウェア更新機能）
販売事業者にこれを課し、基準を満たす認定機器がけが販売できるようになります。



NICTによる「NOTICE」の実施イメージ　出典：ZDNet

成果、効果検証

目指した機能・性能目標	対策の効果(サマリ)
1.　改ざんされたファームウェアを検知し実行を許可しない	■デジタル署名技術を用い、正規のファームウェアかどうかを判定 ■不正な（改ざんされた可能性のある）ファームウェアを検知し実行を許可しない
2.　脅威に対して検知、ブロックできる	■HULFT IoTを用いて、オープンなインターネット回線上のデータを適切に暗号化 ■不正なアクセスを検知してブロックする
3.　不正なアクセスや攻撃を迅速に検知し、アクセスをブロックする	■パブリッククラウド上で稼働しているWebアプリケーションにFirewallを適用 不正なアクセスを検知して、アクセスをブロックする
4.　脆弱性に対するネットワーク経由での攻撃を検知・ブロックできる	■IoTゲートウェイ上で動作するリスク検知機能（TMIS）を導入 IoTゲートウェイに対するリモートからの不正侵入（疑似ウィルスの侵入）を検知し、ブロックする
5.　IoT機器との連携においてシステムに影響なくセキュリティを確保	■クラウド向けサーバセキュリティ製品（Deep Security）であるWebアプリケーションをサーバ上に導入 サーバに対する不正（疑似ウィルス）侵入を検知してブロックする
6.　セキュリティソフトウェアを入れたことによる著しいパフォーマンス低下がない	■複数導入したセキュリティソフトウェアによるゲートウェイの著しい性能低下がない
7.　IoTセンサーへ侵入されない	■IoTセンサ（デバイス）をルーター配下に設置 デバイスに対して、リモートからのアクセスを遮断する