WASEDA University

WASEDA NEO Smart SE

スマートエスイー 修了制作

システムモデリング技法を活用したIoTシステムのアーキテクチャ設計（セキュリティ）

所属： 富士ゼロックス　　名前： 青木康祐　　メールアドレス：aoki.kousuke@fujixerox.co.jp

開発における問題点

IoT開発は従来のITソリューション開発と比較してデバイス・ネットワーク・クラウドと異種技術を組み合わせて構築される複雑さがある。

そのため、セキュリティを曖昧にした状態でPoCを実証しても、商品開発・運用フェーズで想定以上のコストが必要となり、ビジネスとして成立しない事態に陥ってしまう。

手法・ツールの適用による解決

本修了制作ではスマートエスイで学んだ複数の手法を取り入れながら、IoTシステム開発（PoC案件）を題材に上流工程におけるセキュリティ設計を実践した。

	内容	適用ツール
機能要件	・事業目標との整合 ・要求抽出 ・要求記述、管理	・GQM+Strategies ・BABOK ・SysML
セキュリティ要件	・セキュリティ方針 ・セキュリティ分析 ・セキュリティ設計	・IoTセキュリティガイドライン

■セキュリティ設計の進め方

総務省・経済産業省が策定した「IoTセキュリティガイドライン」を活用して、図1の4つのステップでセキュリティ設計を実践。

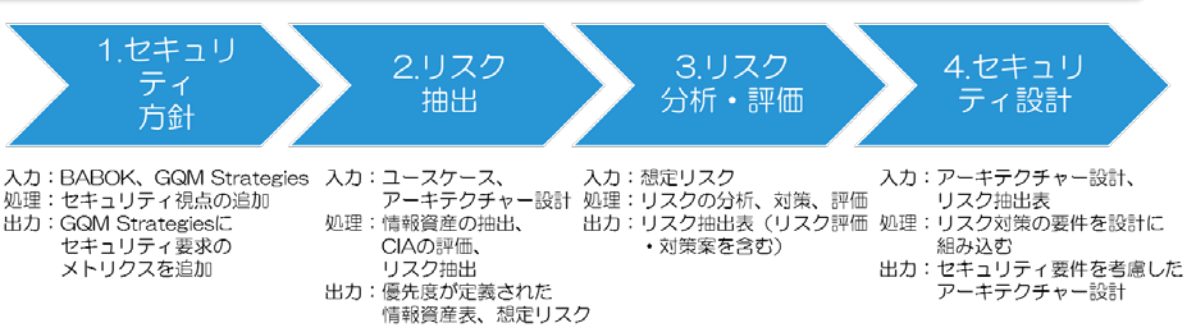

図1.セキュリティ設計の進め方

1. セキュリティ方針

GQM+Strategiesのフレームワークを活用してセキュリティ要件を測定可能な指標項目に定義

2. リスク抽出

守るべき資産を特定するためにユースケースから情報資産を抽出し、1.で定義した要件と情報セキュリティを軸に評価を実施(図2)。

評価が高い情報区分に関しては、ガイドラインの過去事例を参照しながらリスクを抽出。

情報区分	守るべき情報資産	GQM業務と疲労度データ			機密性(C)			完全性(I)			可用性(A)			評価
		なし	小	甚大	なし	小	甚大	なし	小	甚大	なし	小	甚大	
ユーザー情報	ID、パスワード			○			○			○	○			高
生態情報（Rowデータ）	心拍データ（1秒1回） 脳波データ（1秒1回）			○			○			○	○			高
環境情報	気温、湿度、CO2濃度、気圧、騒音		○		○				○			○		小
生態情報（推定データ）	ストレス（心拍） 集中（脳電位）			○			○			○	○			高
デバイス情報（心拍計、脳設計、環境センサー）	機種、シリアル、ID等	○			○			○			○			小
測定アプリ	ゲートウェイアプリ（スマホ）	○				○		○			○			小
設定情報	ゲートウェイアプリの設定情報（スマホ）	○				○		○			○			小

図2.守るべき資産の評価

3. リスク分析・評価

2.で抽出したリスクを分類し（物理接触リスク、内包リスク、外部IFリスク）し、攻撃手法の難易度、ビジネス影響度で評価をし、セキュリティ要件となる対応策を定義。

4. セキュリティ設計

3.で抽出したセキュリティ要件をアーキテクチャ設計へ追加することでセキュリティを視覚的に確認(図3)

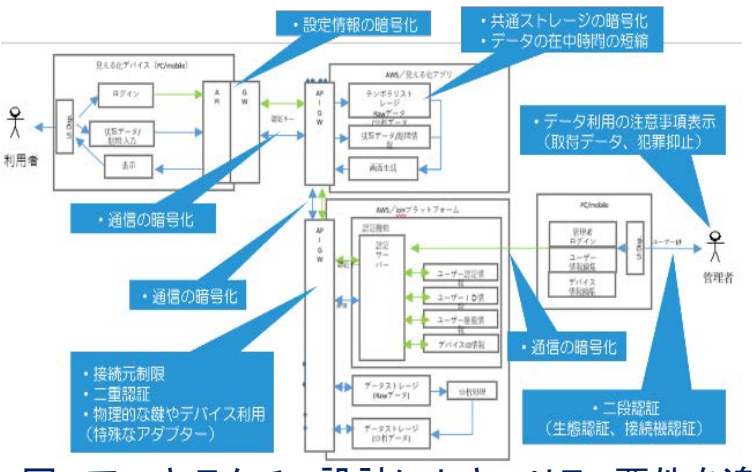

図3.アーキテクチャ設計にセキュリティ要件を追加した図