# IoT システムの脆弱性分析に基づく アスペクト指向アーキテクチャの設計

2014SE085 佐野達也

指導教員：張漢明

## 1 はじめに

IoT の普及が進み, 様々な機器がインターネットに接続されるようになった. その結果, 既存の機器に見られなかった脆弱性の顕在化や機器のライフサイクルの長期化による初期の設計では考慮されていなかった欠陥の顕在化 [1] が問題視されるようになった. 今後 IoT を安全に使用していくにはセキュリティ機能を状況に応じて容易に変更できるアーキテクチャの設計が必要不可欠である.

本研究の目的は脆弱性分析に基づいて、既存の IoT システムのための共通アーキテクチャをセキュリティを考慮した IoT アーキテクチャに拡張することである.

目的へのアプローチとして、IoT システムの各コンポーネントの脆弱性とその対策を分析し, それを基にセキュリティアスペクトを定義し江坂らが提案した IoT システムのためのアスペクト指向アーキテクチャ [2] を拡張する. また 3 章ではセキュリティアスペクトを付与するアスペクト間記述を考察することで状況に応じて適切なセキュリティ機能を付与するためのシステムごとの条件をパターンとして示した. 農業システムを取り上げ、提案手法の有効性と妥当性を検証する.

## 2 背景技術

### 2.1 IoT(Internet of Things)

IoT とは様々なモノが通信機能を持ちインターネットに接続して動作することで情報をリアルタイムで通信し相互に制御する仕組み [1] のことである. 自動車などのライフサイクルの長い機器は使用期間内に新たな脆弱性が発見されるなど初期のセキュリティ対策が不十分になる可能性 [1] が考えられる.

### 2.2 アスペクト指向

アスペクト指向とは複数のクラスにまたがってしまい分離できない関心事をアスペクトと見なしアスペクト記述を用いて一つのモジュールとして分離する技術のことである. 本研究ではセキュリティ機能を IoT システムの横断的関心事としてアスペクト指向に基づいてモジュール化することにより, セキュリティ機能の実装・変更を容易化する.

### 2.3 セキュリティ技術

本研究で用いるセキュリティ技術は第 3 章で述べる各コンポーネントの脆弱性分析の結果より多くの IoT システムの脆弱性の対策となる暗号化とファイヤーウォールの 2 種類である. 暗号化とは暗号鍵を用いてデータを暗号化するセキュリティ技術であり、データの解読を困難にするのでデータの盗聴・改ざんに対して効果を発揮する. ファイヤーウォールは送信元と送信先の IP アドレス, ポート番号を確認することでデータの通行の可否を判断することができるセキュリティ技術であり悪質なデータを受け取ることや秘密にしたいデータを外部に漏洩することを防ぐことができる.

## 3 脅威分析に基づいたセキュアな IoT アーキテクチャの設計

### 3.1 各コンポーネントの脅威分析

本節では IPA の ”IoT 開発におけるセキュリティ設計の手引き”[3] を参考に

- デバイス
- ゲートウェイ
- クラウド

各コンポーネントの脆弱性とその対策について分析した. 表 1 に各コンポーネントで共通する脆弱性とそれらの対抗策となるセキュリティ機能を示す.

表 1 各コンポーネントの脅威対策表

| 脅威名 | 対策名 |
|---|---|
| データの改ざん | 通信経路暗号化 |
| データの盗聴 | 通信経路暗号化 |
| 情報漏洩 | データ暗号化 |
| 不正アクセス | FW 機能, ユーザー認証 |

分析の結果、本研究で実装するべきセキュリティ機能は 3 つのコンポーネントに共通して効果を発揮すると予想される暗号化とファイヤーウォールの 2 つであると考えた.

### 3.2 アーキテクチャの設計

セキュリティ機能をアスペクト指向に基づいてモジュール化することによりセキュリティ機能の記述を減らすことで、より容易にセキュリティ機能を付与できる. そこで前節で選択したセキュリティ機能をセキュリティアスペクトとして設計する. 暗号化とファイヤーウォールの 2 つのセキュリティ機能を Security Features としてまとめることでアスペクト間記述に付与しやすくした.

また, セキュリティアスペクトをアーキテクチャに付加するにあたって、IoT システムのために作られておりアスペクト拡張がスムーズに行えるという理由から江坂らが提案 [2] している IoT のためのアスペクト指向アーキテク

チャにセキュリティアスペクトを組み込むことでセキュリティ機能向上を目指した. 図 1 に本研究で設計したアーキテクチャを示す.

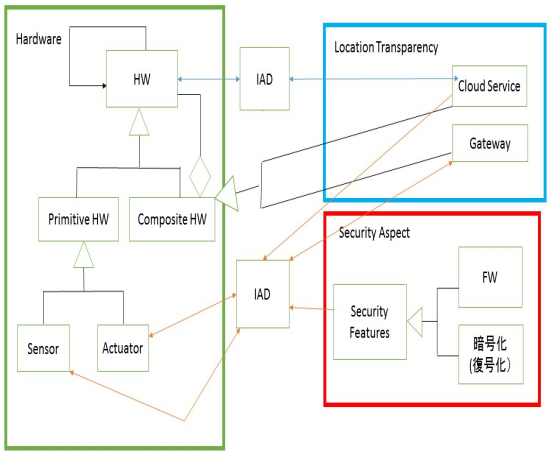


図 1　アーキテクチャ

### 3.3　アスペクト間記述の考察

セキュリティ機能を付与するためには各通信間のアスペクト間記述について考察し、付与するためのパターンを明確化する必要がある. 本研究では以下の条件での付与パターンについて考察した.

- デバイスの設置位置
- デバイスの種類
- ゲートウェイの種類
- クラウドサービスの種類

デバイスの設置位置はデバイスの設置位置に応じてデバイスとゲートウェイ間にセキュリティ機能を付与する.

デバイスの種類はセンサー, アクチュエータ等デバイスの種類に応じてデバイスゲートウェイ間にセキュリティ機能を付与する.

ゲートウェイの種類はゲートウェイの種類に応じて各ゲートウェイと通信している全てのデバイスにセキュリティ機能を付与する.

クラウドサービスの種類はシステムのサービスごとにゲートウェイとクラウド間にセキュリティ機能を付与する.

## 4　事例検証

事例検証の題材としてルートレック・ネットワークス社が開発したゼロアグリ [4] を参考にした農業システムを選択した. 農業システムは 2 つの畑で育てている 4 種類の作物付近に設置してある各温度センサが温度を取得し、システムに送ることで、温度グラフの作成とシャワー制御装置への水放出命令を送るシステムである. アスペクト間記述として以下の 4 パターンについて検証する.

- 作物の種類
- デバイスの種類
- ゲートウェイの種類
- 農業サービスの種類

各パターンにアスペクト間記述の考察を当てはめて検証することで本研究の妥当性を示す. 表 2 に検証結果の一部を示す.

表 2　作物ごとのセキュリティ付与パターン

| | 暗号化 | ファイヤーウォール |
|---|---|---|
| じゃがいも | × | × |
| 秘密のじゃがいも | ○ | × |
| トマト | × | ○ |
| 秘密のトマト | ○ | ○ |

## 5　考察

セキュリティ機能をアスペクトとして分離することで、オブジェクト指向のシステムと比べセキュリティ機能変更の際に最小限のコード変更でセキュリティ機能を付与できるので、迅速なセキュリティ機能の変更が可能になる. またアスペクト間記述の考察によりセキュリティ機能の付与をパターン化することで、システム作成者がセキュリティ機能の選択を考察する時間を短縮することが可能になる. また異種ソフトウェア基盤への対応として各 OS ごとにそれに適したセキュリティ機能を用意する必要がある.

## 6　おわりに

本研究ではデバイス, ゲートウェイ, クラウドの 3 つに対してアスペクト間記述を考察したが IoT システムにはフォグサービスを使ったものも存在するため、そちらの考察も必要である.

## 参考文献

[1] IoT 推進コンソーシアム，総務省，経済産業省: ”IoT セキュリティガイドライン ver1.0”, http://www.soumu.go.jp/main_content/000428393.pdf, 2016.

[2] 江坂篤侍，野呂昌満，沢田篤史: ”コンテキストウェアネスを考慮した組込みシステムのためのアスペクト指向アーキテクチャの設計”. ソフトウェア工学の基礎 XXIV, 2017.

[3] IPA 独立行政法人情報処理推進機構 技術本部 セキュリティセンター: ”IoT 開発におけるセキュリティ設計の手引き”, https://www.ipa.go.jp/files/000052459.pdf, 2016.

[4] 株式会社ルートレック・ネットワークス: ”ZeRo.agri”, https:/www.zero-agri.jp/