IoT システムのためのセキュリティ技術導入プロセスに関する研究

2012SE080 鎌田貴斗
指導教員：沢田篤史

1 はじめに

IoT(Internet of Thing) と呼ばれる様々なモノがインターネットに接続される技術が普遍化して繋がるデバイスの対象が増加することにより，サイバー攻撃者が IoT システムの脆弱性を狙った攻撃を行う可能性が考えられる．

本研究の目的は，IoT システムへの円滑なセキュリティコンポーネント導入の支援である．セキュリティコンポーネント導入プロセス, IoT アーキテクチャ構築プロセス, セキュリティコンポーネント開発を，IoT のためのセキュリティ技術導入プロセスとしてまとめる．これにより，IoT システムへの円滑なセキュリティコンポーネントの導入プロセスを確立する．

目的へのアプローチとして，本研究のセキュリティコンポーネントの導入プロセスを提示する．セキュリティコンポーネント導入プロセスは，セキュリティ上の脅威を精査し，除去すべき脅威を決定する．IoT アーキテクチャ構築プロセスは，参照アーキテクチャを決定し，アーキテクチャの構築を行う．セキュリティコンポーネント開発は，除去すべき脅威を考慮したシステム開発を行う．

本研究の考察として，温度収集システムに対するセキュリティ技術導入プロセスの適用により，妥当性を検証した．

2 背景技術

2.1 IoT のセキュリティ上の脅威

IoT のセキュリティ上の脅威は，J.Sathish Kumar ，Dhiren R.Patel の研究 [2] で提示されている．脅威の発生源は，外界と直接データのやり取りを行うフロントエンド，IoT デバイスとサーバをつなぐネットワーク，データの保存や処理を行うバックエンドに分類される．

2.2 Architecture Tradeoff Analysis Method

Architecture Tradeoff Analysis Method (以下 ATAM)[1] は，アーキテクチャの評価手法である．シナリオによってシステムの振る舞いを分析し，リスク並びにトレードオフの特定アーキテクチャの改良が可能になる．

3 IoT のためのセキュリティ技術導入プロセス

3.1 セキュリティコンポーネント導入プロセス

セキュリティコンポーネント導入プロセスは，システムの脅威提示，脅威のリスクアセスメント，脅威への対策提示の順に行う．

システムの脅威提示では，IoT のセキュリティに関する研究事例を背景に脅威を提示する．フロントエンドから発生する脅威，ネットワークから発生する脅威，バックエンドから発生する脅威を研究事例の脅威を参考に考察する．

脅威のリスクアセスメントでは，リスクを数値化することで対策すべき脅威の優先順位を決定する．
リスク値を算出するために主に用いられている計算式 [4] を参考に，本研究のリスク評価値の計算式を以下に示す．

$$\text{リスク評価値} = \text{情報資産価値} \times \text{脅威} \times \text{脆弱性}$$

情報資産価値の基準は，失われたときに被る損害の大きさで数値化する [5].
脅威の基準は，攻撃の発生しやすさで数値化する [5].
脆弱性の基準は，対策状況で数値化する [5].

脅威への対策提示では，表を用いたセキュリティ対策を施す．表 1[3] は，セキュリティ対策，セキュリティ対策の機能と目的，対応する脅威例をまとめたものである．脅威を除去可能であることや，システムに組み込みやすいなどの目的にあったセキュリティ対策を提示する．

表 1 脅威の対策提示一覧 (一部抜粋)

対策名	機能・目的	脅威例
脆弱性対策	脆弱性混入防止	不正アクセス
ファイアウォール	接続先の制限	DoS 攻撃

3.2 アーキテクチャ構築プロセス

アーキテクチャ構築プロセスは，参照アーキテクチャの決定，アーキテクチャの構築の順に行う．参照アーキテクチャの決定基準は，セキュリティコンポーネントを導入する IoT システムと参照するアーキテクチャのシステムが類することが望ましい．

セキュリティコンポーネントを導入する IoT システムのアーキテクチャ構築は，参照するアーキテクチャを模倣することを基本とする．IoT は多種多様のデバイスで動作することを前提としているため，参照アーキテクチャの模倣に加え，ツリー状にしたアーキテクチャも構築する必要がある．

3.3 セキュリティコンポーネント開発

セキュリティコンポーネント開発は，設計と実装の二つに分けられる．一般的な IoT システムの開発と比較して，開発方法や使用言語の規制は無い．

3.4 セキュリティ技術導入プロセスの手順

セキュリティ技術導入プロセスの抽象化を図式化したものが図 1 である．図の四角は，セキュリティ技術導入プロセスをモジュールに要素分割したものを指し示す．図の矢

印は，プロセスの流れを指し示す．図の 2 本の平行線は，データの源泉を指し示す．

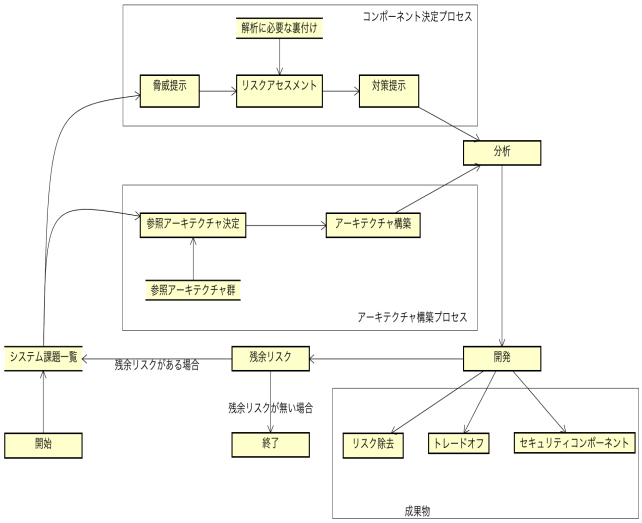

図 1 セキュリティ導入プロセス

4 事例

事例とする IoT システムは，温度収集システムである．温度収集システムは，気温を温度センサが取得し，取得した温度をユーザの端末へ通知させるシステムである．

セキュリティ技術導入プロセスのシステムの脅威提示を元に，温度収集システムの脅威を一部抜粋する．

- 温度センサを始点とする脅威
  - サーバへの過剰な温度情報の送信
- ネットワークを始点とする脅威
  - 温度センサとサーバ間の盗聴と改ざん
- サーバを始点とする脅威
  - サーバへの不正アクセス

セキュリティ技術導入プロセスの脅威のリスクアセスメントを元に，温度収集システムのリスクアセスメントを行う．評価値の高い脅威上位 3 つは以下の通りである．

1. ウィルス感染 (温度センサ)
2. 温度センサとサーバ間の盗聴と改ざん (ネットワーク)
3. 意図しない温度センサへの温度送信 (温度センサ)

セキュリティ技術導入プロセスの脅威への対策提示を参考に，温度収集システムで行うべきセキュリティ対策を決定する．本研究では，ソフトウェアアーキテクチャに組み込むことが可能であることを理由として，本研究で行うセキュリティ対策をデータ暗号化とする．

温度収集システムの参照アーキテクチャは，Microsoft Azure[6] と呼ばれるプラットフォームとする．

参照アーキテクチャを模倣した温度収集システムアーキテクチャとツリー状にしたアーキテクチャを構築する．

温度収集システムのセキュリティコンポーネント開発は，設計として，暗号化モジュールを組み込んだ温度収集システムのクラス図を作成する．実装では，クラス図を元に Python を用いたプログラムを記述を行う．

5 考察

事例として取り上げた温度収集システムを通して，提案したセキュリティ技術導入プロセスの妥当性を考察する．成果を上げられたと言えるプロセスを以下に示す．

- システムの脅威提示
- 脅威のリスクアセスメント
- 脅威への対策提示
- アーキテクチャの構築

ATAM との比較を元に，本研究が提案するセキュリティ技術導入プロセスの有用性は以下の 2 つである．

- 文献や裏付けを利用したプロセスで，より信憑性のある対策を考察することが可能
- 参照となるアーキテクチャの存在による，アーキテクチャの構築にかかる時間，工数の削減

6 おわりに

本研究の成果として，IoT システムへの円滑なセキュリティコンポーネントの導入プロセスを提案した．その結果，IoT システムへの円滑なセキュリティコンポーネント導入の支援を可能とした．

今後の課題として，現実世界の IoT 機器の動作の制御セキュリティを考察する必要がある．

参考文献

[1] Carnegie Mellon University, “Architecture Trade-off Analysis Method”, http://www.sei.cmu.edu/architecture/tools/evaluate/atam.cfm , 2016.

[2] J. Sathish Kumar, Dhiren R. Patel, “A Survey on Internet of Things: Security and Privacy Issues”, International Journal of Computer Applications, vol. 90, no. 11, pp. , 2014.

[3] IPA 独立行政法人情報処理推進機構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] 後藤邦夫, “情報通信セキュリティ 講義資料 第 3 週”, https://www-p.st.nanzan-u.ac.jp/classes/2016/77380/03.html , 2016.

[5] ピーター・イールズ, ピーター・クリップス, 榊原彰, 西原裕善, 吉田幸彦, 五十嵐正裕, 山本久好, 金元隆志, “システムアーキテクチャ構築の実践手法”, 翔泳社, 2010.

[6] Microsoft Azure, “モノのインターネットのセキュリティアーキテクチャ”, https://docs.microsoft.com/ja-jp/azure/iot-hub/iot-hub-security-architecture , 2016.