セキュリティを考慮したIoTアプリケーションに関する研究

M2017SE007 水田大貴
指導教員：野呂昌満

1　はじめに

Internet of Things(以下，IoT と呼ぶ) は，生活の基盤となっており，個人情報を取り扱うことからセキュリティを確保することは重要である [4]．IoT デバイスはメモリや CPU などの制約が存在するので，ミドルウェア [3] やゲートウェイなどの特定のコンポーネントを用いてセキュリティを強化する手法が取られている．IoT デバイスは移動体なことが多く，セキュリティ要求は変化する．それを考慮して，Yuhong らは，セキュリティを考慮して動的にネットワークの構成を変更可能なアーキテクチャを提案している [5]．

Yuhong らは最適なネットワークの構成のための指針としてユーザ要件，デバイスの種類，ネットワーク環境に応じた再構成条件をセキュリティポリシーとして定義している．一方，セキュリティレベルについて言及されておらず，セキュリティ要求に応じたネットワークの最適構成が不明である．本研究で定義する最適構成とは，非機能要求を満たす中でセキュリティの充足度が一番高いものを指す．

本研究の目的は，セキュリティ要求に応じてネットワークを動的に再構成する IoT アプリケーションの開発支援を行なうことである．セキュリティ要求と最適な構成パターンの関係を明らかにするセキュリティポリシーを定義して，そのポリシーに基づく動的再構成可能なコンテキスト指向アーキテクチャを設計する．

一般的なセキュリティ要求を定義するために SLA(Service Level Agreement)[2] を用いる．特定の要求に応じた構成を抽象化してネットワークの構成パターンを定義する．要求に応じて考えられる構成パターンから最適な構成を選択するセキュリティポリシーを定義する．

アーキテクチャ設計は Yuhong らが提案しているアーキテクチャを参考にし，江坂らの提案した IoT システムのためのアーキテクチャ[1] を拡張して設計する．江坂らはこれまでに動的再構成のためのパターンとして PBR パターン (Policy-Based Reconfiguration) を定義した．Yuhong らのアーキテクチャの提案する動的再構成に関する記述を PBR パターンを用いて，ネットワークの最適構成のためのセキュリティポリシーに基づく動的再構成のための構造を定義する．これにより，単純な構造から動的再構成を実現してセキュリティーポリシーに関する記述を容易にすることが可能になる．

2　関連研究

本研究と関係のある研究について述べる．

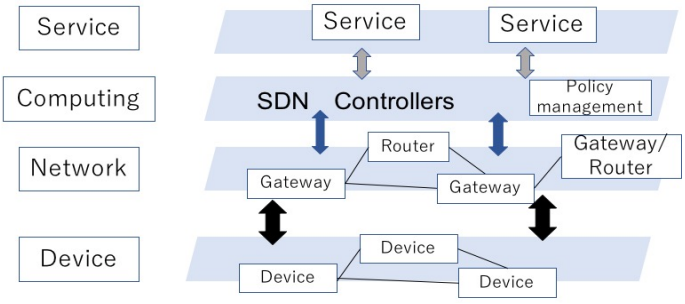

図 1　Yuhong らが提案するアーキテクチャ

2.1　Yuhong らの研究

Yuhong らはセキュリティを考慮して動的にサービスの構成を変更可能な階層アーキテクチャを提案している．Yuhong らのアーキテクチャは次の 4 層からなる（図 1）．

- Device Layer
  大量のデータを収集するセンサーやサービスやアプリケーションからの命令を実行するアクチュエータなど様々なデバイス．
- Network Layer
  SDN Controller の制御下で稼働しているゲートウェイやルータ．
- Computing Layer
  アプリケーションの要求や特定のセキュリティポリシーに従ってデータを転送する SDN Controller．
- Service Layer
  データストアやクラウドを用いたアプリケーションやサービス．

Yuhong らのアーキテクチャではセキュリティポリシーを参考にして，動的にセキュリティ要求を満たすように Network 層と Device 層の要素の構成を変更している．

2.2　PBR パターン

江坂らが提案している PBR パターンを示す．PBR パターンとは自己適用ソフトウェアの設計支援のためのアーキテクチャパターンである．PBR パターンを用いることでコンテキストとアスペクトを共通の構造として扱うことができる．以下に PBR パターンの静的構造（図 2），動的振舞い（図 3）を示す．

- Policy：Component 間のメッセージを横取りして再構成の指針を決定
- Configuration Builder：Policy の指針に従って再構成を実行
- Abstract Configuration：システムの構成を抽象化したもの

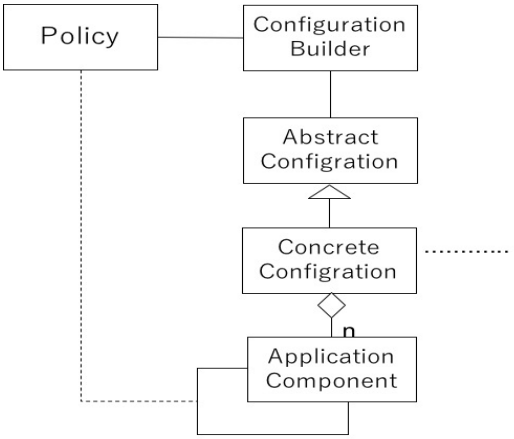

図 2 PBR パターンの静的構造

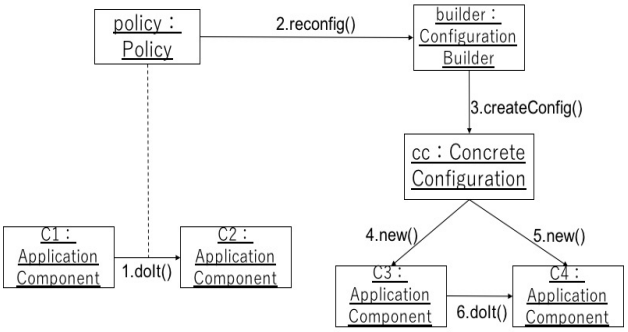

図 3 PBR パターンの動的振舞い

- Concrete Configuration：具体的なシステムの構成
- Application Component：アプリケーションのコンポーネント

PBR パターンは Policy が Application Component 間（C1 と C2）のメッセージを横取りする．Policy はそのメッセージに従って Configuration Builder を起動する．Configuration Builder は Policy の指針をもとに Concrete Configuration を生成する．Concrete Configuration は構成するさいに足りない Component である Application Component（C3 と C4）を生成する．

3 配置パターンを考慮した動的再構成

セキュリティポリシーを定義するために一般的なセキュリティ要求と構成パターンを定義した．以下，それぞれについて説明する．

3.1 セキュリティ要求

この節では，一般的なセキュリティ要求を定義する．一般的に，システムを運用するさいにはセキュリティを確保するための仕組みとして ISMS や ITSMS に沿って運用している．ISMS や ITSMS を運用するための手法として SLA が用いられている．SLA とはサービス提供者と利用者側で結ばれたサービス水準に関する共通の指標である．本研究では，一般的な IoT システムを運用していくために IoT のセキュリティ要求を定義するので SLA を用いる．SLA の項目の要求を満たすことができればシステムのセキュリティが向上できると考え，項目を満たす数を要求されるセキュリティ強度として定義する．以下，SLA のセキュリティに関連する項目を説明する．

- 公的認証取得の要件
- アプリケーションに関する第三者評価
- 情報取扱者の制限
- 通信の暗号化レベル

公的認証取得の要件は JIPDEC や JQA 等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）が取得されていることを指している．アプリケーションに関する第三者の評価は悪意のあるユーザからの不正行為に対する対策について，第三者の客観的なセキュリティチェックが行われていることを指している．情報取扱者の制限はユーザのデータにアクセスできる利用者の限定されていることを指している．暗号化レベルとは，通信の暗号化レベルとは暗号化するさいの鍵の長さのことでレベルが基準を満たしているかどうかを判定する．この 4 つの項目は満たされている場合は単位は有，満たされていない場合は無とする．

3.2 セキュリティポリシー

IoT アプリケーションのセキュリティ要求を SLA を参照して整理する．セキュリティポリシーではアプリケーションの要求されるセキュリティ強度とネットワークの構成要素のセキュリティ強度に応じて考えられるネットワークの構成パターンから最適な構成パターンを選択する．現在抽象化した最適な構成パターンとして，再構成ありパターンと再構成なしパターンに分類できると考えた．次に 2 パターンを例を用いて説明する．

再構成ありパターンの例を挙げる．セキュリティ要求として全ての項目がありの場合として説明する．図 4 のような場合を考えるとネットワークの構成要素（フォグとデバイス 2 つ）に要求を満たしていない要素がある．この場合，満たしていない要素があるのでセキュリティポリシー内で再構成ありパターンを判定する．満たしていない要素を要求を満たしている要素と組み合わせて一つの構成要素として再構成する．これにより，ネットワークの構成要素全てが満たすようになり，ネットワーク全体のセキュリティ強度が向上した．

再構成なしパターンの例を挙げる．セキュリティ要件の公的認証取得と暗号化アルゴリズムの項目が有の場合の説明をする．図 5 のような場合を考えると全ての要素が要求されるセキュリティ強度を満たしている．この場合，セキュリティポリシー内で再構成なしパターンと判定する．これにより，再構成を行なわないのでネットワークの構成は変更されない．

4 アーキテクチャ設計

3.2 節で述べたセキュリティポリシーを基づき，セキュリティ要求を満たすネットワーク構成に動的に再構成可能なアーキテクチャを設計する．図 1 に示した Yuhong らのアーキテクチャのうち再構成に関する層を明らかにす

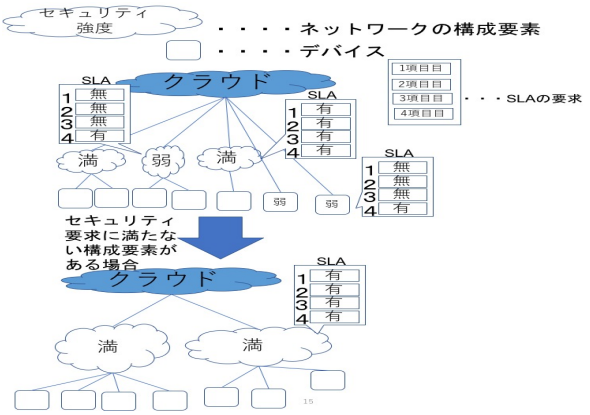

図 4 再構成ありパターン

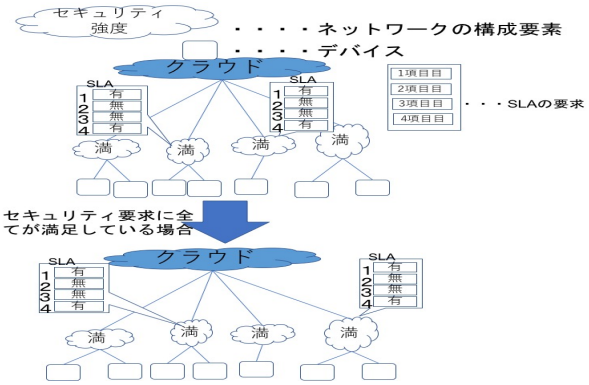

図 5 再構成なしパターン

る． Yuhong らのアーキテクチャを参考にして，ネットワーク構成のセキュリティレベルから状況に応じて動的に再構成を行うので，コンテキスト指向アーキテクチャとして PBR パターンを用いて定義する．PBR パターンを適用することで単純な構造から動的再構成を実現し、セキュリティポリシーに関する記述を容易にする．

Yuhong らは，Computing Layer，Network Layer，Device Layer において，セキュリティポリシーに基づく再構成の仕組みを提案している．ある要求に対して，それぞれの層で再構成が行われることから，我々はこの 3 層にセキュリティコンサーンが横断していると考えた．

ネットワークの構成要素のセキュリティ強度によってネットワークの構成要素が変更されることからネットワークの構成要素のセキュリティ強度をコンテキストとする．構成要素のセキュリティ強度に応じて，最適な構成パターンを選択し，適用して動的にネットワークを再構成する．Computing Layer，Network Layer，Device Layer に横断するセキュリティコンサーンの構造を PBR パターンを用いて定義する．これにより，セキュリティポリシーと動的再構成に関する記述を分離した構造を定義できた．IoT のセキュリティ要求や配置パターンに関して独立して変更できるように設計される．

提案したアーキテクチャを図 6 に静的構造，図 7 に動的振舞いを示す．以下にコンポーネントの説明を行う．

- Context：ネットワークの構成要素のセキュリティレベルの達成状況
- Security Level：ネットワークの構成要素のセキュリティレベル
- Security Policy：IoT アプリケーションの要求されるセキュリティ強度と構成要素のセキュリティ強度から最適な構成パターンを選択
- Network Factory：Security Policy をもとに必最適なネットワークの構成パターンを実装
- Network Element：ネットワークの構成要素（ゲートウェイ，デバイス，ルータ）
- SDN Controller：SDN コントローラ

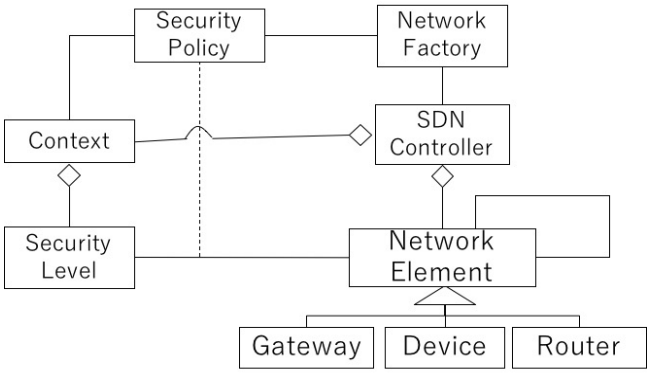

図 6 静的構造

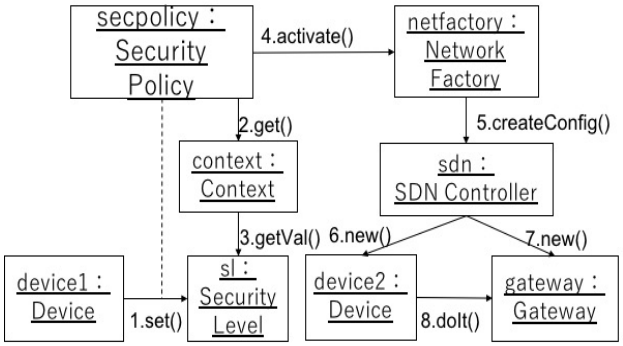

図 7 動的振舞い

ネットワークの構成要素（Network Element）は自分自身のセキュリティ強度を Security Level に送る．Security Policy はそのメッセージを横取りする．Context は Security Level からネットワークの構成要素のセキュリティ強度を取得する．Security Policy は Context からネットワークの構成要素のセキュリティ強度を取得して，IoT アプリケーションの要求されるセキュリティ強度と構成要素のセキュリティ強度からセキュリティポリシー内で最適な構成パターンを決定する．再構成ありパターンの場合には，Network Factory に再構成のメッセージを送る．Network Factory は最適な構成パターンの SDN Controller を生成する．その SDN Controller は起動していないコンポーネント（Gateway）がある場合，起動して通信を行なう．再構成なしパターンの場合は再構成を行わない．

5　考察

考察として，本研究で提案したアーキテクチャの有用性と本研究で提案したセキュリティの強化方法と特定のコンポーネントを用いたセキュリティ強化手法との比較を行なう．

5.1　アーキテクチャの有用性の確認

本研究で提案したアーキテクチャの有用性を考察する．Yuhong らのアーキテクチャでもセキュリティポリシーに応じてネットワークの構成を変更している．Yuhong らのアーキテクチャを用いて，本研究で提案したセキュリティポリシーを実装するとした場合，Policy Management にセキュリティポリシーと動的再構成に関する記述が混在するので複雑化していて，保守性が低下していると考えられる．本研究で提案したアーキテクチャではセキュリティポリシーを管理するコンポーネントと動的再構成に関するコンポーネントを分離して記述しているのでセキュリティポリシー変更の柔軟性を確保している．

5.2　特定のコンポーネントを用いたセキュリティ強化手法との比較

本研究では，IoT アプリケーションのセキュリティの強化の手法として，動的にネットワーク構成を変更して，セキュリティを強化している．Wisasam らはミドルウェアを導入してセキュリティを強化する IoT アプリケーションのアーキテクチャを提案している．この手法では，ミドルウェアにセキュリティ機能を持たせることで，IoT デバイスの制約などによる問題を解決している．要求されるセキュリティレベルが変更される場合には，導入されるミドルウェア全てのセキュリティレベルをあげるように変更しなければならないので，容易ではない．本研究で扱っている手法の場合は，セキュリティレベルを変更するさいには，セキュリティポリシーを変更する．これにより，ネットワークの構成要素全てが要求されるセキュリティレベルを満たすような構成になる．このことから，セキュリティレベルの変更が容易に行えると考察できる．

他方で，Wissam らの手法は，デバイスとフォグの間にミドルウェアを配置することで，セキュリティ機能だけでなく，データ処理機能やデータの種類による転送先の変更などが柔軟に行えるのでネットワーク効率を向上させることができる．本研究では，現状構成を変更するさいにセキュリティポリシーをもとに構成を決定しているので，実行効率や耐故障性について考慮されていない．

6　おわりに

IoT ではセキュリティが重要視されていて，ゲートウェイやミドルウェアでセキュリティを強化する手法が取られている．Yuhong らはセキュリティを考慮して動的にサービスの構成を変更するアーキテクチャを提案しているが，セキュリティレベルについては言及されておらず，セキュリティ要求に応じたネットワークの最適構成が不明である．本研究では，セキュリティの要求に応じて動的にネットワークを最適な構成に変更するためのアーキテクチャを提案した．これにより，ネットワークの構成要素のセキュリティ強度をもとに最適なネットワークの構成を選択できるようになった．

今後の課題として，以下の 3 点が考えられる．

- 配置パターンの洗練
- 他の非機能特性との関係の整理
- 実現可能性の考察

ネットワークの構成に関する研究を調査して，構成パターンを洗練する必要がある．3.2 節において，配置パターンとして，セキュリティ要求を満たさない場合に再構成を行なうパターンと，要求を満たす場合に再構成を行わないパターンを定義した．再構成を行なうパターンは，要求を満たす構成要素を探し，入れ替えを行なう．その他にも，異なる構成要素を中継するように再構成すること等が考えられる．またネットワーク構成の選択肢の特定方法について言及できていない．例えば，それぞれの構成要素は特定の通信プロトコルを前提としていることから，メッセージ通信が可能なものを選択肢として特定する必要がある．

ネットワークの再構成を行なうことで，他の非機能特性に影響を与えることが考えられることから，この関係を整理する必要がある．セキュリティ要求を満たすために再構成をした結果，実行効率や耐故障性に関する要求を満たすことができなくなることが考える．セキュリティと他の非機能特性との関係を明らかにし，総合的に評価して再構成する方法を定義する必要がある．

本研究で提案するアーキテクチャをもとに IoT アプリケーションの設計・実装を行ない，実現可能性とアーキテクチャの有用性を考察する．

参考文献

[1] 江坂篤侍, 野呂昌満, 沢田篤史：インタラクティブシステムのための共通アーキテクチャの設計, コンピュータソフトウェア, Vol. 35, No.4 (2018), pp.78-90.

[2] JEISTA：民間向けＩＴシステムのＳＬＡガイドライン_ 追補版 SaaS 対応編の公表について，https://home.jeita.or.jp/is/committee/solution/guideline/080131/index.html，2008.

[3] Wissam, R., Daniele, S., and Kouichi, S.：A New Security Middleware Architecture Based on Fog Computing and Cloud To Support IoT Constrained Devices, Proceedings of the 1st International Conference on Internet of Things and Machine Learning, No. 35 (2017).

[4] Yuchen, Y., Longfei, W., Guisheng, Y., and Hongbin, Zhao.：A Survey on Security and Privacy Issues in Internet-of-Things, IEEE Internet of Things Journal, vol. 4, No. 5 (2017), pp.1250-1258.

[5] Yuhong, L., Fredrik, B., and Haoyue, X.：IoT Architecture Enabling Dynamic Security Policies, Proceedings of the 4th International Conference on Information and Network Security, ACM, 2016, pp. 50-54.