3J-07

IoTにおけるエッジ側アクセス規制のセキュリティ検証

矢島　大嗣†　　岸　知二‡

早稲田大学　創造理工学研究科　経営システム工学専攻

1. 研究の背景と目的

IoT(Internet of Things)システムは家電から自動車、医療・ヘルスケアなど多くの事業に活用されている。同時に不正アクセスやウイルスなどに対するセキュリティ対策が重要な課題となっている。従来クラウド側に対するセキュリティ対策は行われていたが、近年ではセキュリティ対策が相対的に遅れていたエッジ側に対するセキュリティ対策の議論も活発化し始めている。

IoT システムではデバイスに対して多くのアクセスが行われるためアクセス規制の検証を行うことは重要である。アクセス規制とはソフトウェア側が接触可能な相手を識別し、それによってネットワーク内での行動を許可したり拒絶したりすることを指す。本研究ではモデル検査手法を用いてエッジ側のアクセス規制の検証を行う手法を提案する。具体的には IoT デバイスに関するセキュリティガイドライン[1]に記載されている内容からアクセス規制に関わる要求を抽出し，その記述からシステムへの制約を導出し時相論理式に変換して、モデル検査を行うことで検証する。

2. 背景知識

2.1. IoT

IoT は「有線および無線ネットワークを介してリンクされた組み込みセンサを使用して、デバイス同士が互いにデータ通信する機能」である[2]。

2.2. IoT セキュリティガイドライン

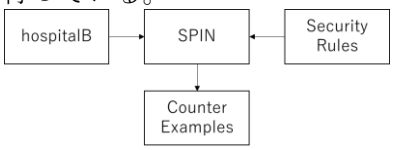
IoT セキュリティガイドラインは、「IoT 機器やシステム、サービスの供給者及び利用者を対象」に「IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめたもの」である[1]。具体的には方針、分析、設計、構築・接続、運用・保守の 5 項目について記述されており、各項目には要点、解説、具体的な対策例が記述されている。

2.3. モデル検査

モデル検査は形式手法の１つである。有限個の状態を持つモデルが満たすべき性質を時相論理で記述し、この性質が成立するかを網羅的に検査する技術である。モデルが性質を満たす場合は真を示し、満たさない場合は偽とその反例を示す。

3. 先行研究

アクセス規制をモデル検査で検証する研究として Maarabani らの研究がある[3], [4]。これらではアクセス規制に関するセキュリティポリシー中に記述されている組織間のセキュリティルールを時相論理式(LTL 式)に変換し、モデル検査器を用いてセキュリティの検証を行う手法を提案している。セキュリティポリシーとは企業や組織において実施する情報セキュリティ対策の方針や行動指針のことを指し、その具体的なルールがセキュリティルールである。図１はモデル化された病院 B に対して正しいかを検証するプロセス図である。入力を病院 B のモデル、セキュリティルールによって変換された LTL 式とし、それらをもとにモデル検査器 SPIN によって検証を行っている。



出典:[3]

図１. 検証プロセス図

4. 提案手法

4.1. 目的

先行研究は組織間でのセキュリティルールを扱ったが、本研究では IoT のデバイスに対するアクセス規制を対象にモデル検査で検証を行う手法を提案する。

4.2. 提案手法の概要

提案手法は以下の手順に沿って進める。本提案手法では主に設計者を対象としたアプローチを提案する。

Security verification of edge side access restriction for IoT device

†1 Department of Industrial and Management Systems Engineering CSE Graduate School, Waseda University

Step1. IoT セキュリティガイドラインより作業者への要求を抽出する。
Step2. 得られた作業者への要求から一般的なシステムへの制約を導出する。
Step3. 一般的なシステムへの制約と対象とするシステム仕様とから，対象とするシステムへの制約を導出する。
Step4. Step3 にて導出した制約を時相論理式で表現する。
Step5. 時相論理式とシステムモデルよりモデル検査を行う。反例が出た場合はモデルを修正し、新たなシステムモデルとして再度モデル検査を行う。

提案手法の全体像は図 2 の通りである。

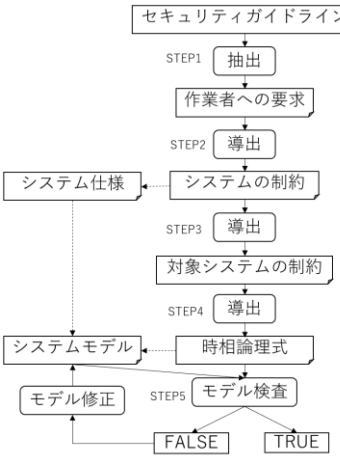


図 2. 提案手法の全体像

4.3 制約の抽出

IoT セキュリティガイドラインはセキュリティ対策の分野を特定しない一般的なものであり、作業者に対するガイドであるため設計者はここから作業者への要求に関する内容を抽出する。次に、作業者への要求からシステムを設計するために必要な一般的なシステムへの制約を導出する。その後、対象とするシステムに合うような制約にするために、対象システムの仕様に照らし合わせて具体的な制約を導出する。この制約を時相論理で記述する。

表 1 は IoT セキュリティガイドラインの要点の一部を示す。

表 1. IoT セキュリティガイドライン要点(一部)

要点9	IoT機器・システムの異常を検知できる設計を検討する
	異常を検知した時の適切な振る舞いを検討する
要点10	安全安心を実現するための設計を見える化する
	安全安心を実現するための設計の相互の影響を確認する
要点11	IoT機器・システムがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する

5. 例題

以下、具体例で説明する。

Step1 にて IoT セキュリティガイドラインの要点 9「つながる相手に迷惑をかけない設計をする」の解説や対策例の中に示されている要求を抽出する。

Step2 では迷惑をかけないための対策例として IoT 機器・システム自身、あるいはそれぞれの監視サーバが状態異常を検知した場合、IoT 機器・システム自身の機能を停止させるかネットワークから切り離すことでこの異常を検知し波及防止することが挙げられている。これより「IoT 機器・システム自身が異常を検知した場合、機能を常に停止した状態にする」という一般的なシステムへの制約を導出する。

Step3 では例えば対象システムが電子ロックであった場合，Step2 で導出した制約から「未登録のデバイスから開錠指示が来た場合，キーをロックして停止する」といった制約を導出する。

Step4 では導出した対象システムの制約から時相論理式に変換する。ここで P:未登録のデバイス、R:キーをロックして停止するだとすると，導出される時相論理式は

$$[](P->[]R)$$

となる。

Step5 では導出した時相論理式にと対象となるシステム仕様をモデル化したものを入力としてモデル検査を行い、アクセス規制に関しての制約が守れていなければモデルや仕様を見直す。

6. おわりに

本稿では IoT におけるエッジ側アクセス規制のセキュリティ検証を提案した。今後実例に適応しながら本手法を洗練したい。

参考文献

[1] 総務省. IoT セキュリティガイドラインライン ver 1.0. 2016.
[2] Createspace Independent Pub, “BIG DATA : SEIZING OPPORTUNITIES, PRESERVING VALUES”, WHITE HOUSE, 2014.
[3] El Maarabani M.; Cavalli, A.; Iksoon Hwang; Zaidi, F.; Verification of Interoperability Security Policies by Model Checking. High-Assurance Systems Engineering (HASE). 2011, pp.376-381.
[4] El Maarabani M.: Andrés Cé.: Ana Rosa Cavalli.: Testing interoperability security policies. In SEKE’12 : The 24th International Conference on Software Engineering and Knowledge Engineering. 2012, pp.464 -469.
[5] 入月 康晴, 大原 衛, 坂巻 佳壽美. セキュアな組込みシステムの構築法. 東京都立産業技術研究センター. 2008, pp.14-17.