スマートホームにおける SDN を用いたセキュリティプラットフォームの検討

A Study of SDN-based Security Platform for Smart Home

塚﨑 拓真 / Takuma Tsukasaki

1　はじめに

近年，IoT(Internet of Things) が注目を集めるようになり，今後あらゆるモノがネットワークに接続され，利用されることが予想される．それに伴い，ネットワーク内には様々な端末や機器 (まとめて，デバイス) が混在することになり，ホームネットワークの形態は多様化していくと考えられる．

しかし，IoT の発展で利便性が高まる一方で，これまでのネットワークに接続されていないモノが接続されることにより，セキュリティ上のリスクも高まっている [1]．IoT デバイスは十分なセキュリティを考慮せずに開発されたものが多いため，悪意のある攻撃者によるサイバー攻撃の標的になりやすい．セキュリティ上の脅威が各種デバイスに顕在した場合，個別に対処するとコストや時間がかかってしまうため，脅威に対し一括に対処する必要がある．しかし，ホームネットワーク内には異なる規格のハードウェアや様々なアプリケーションが混在しているため，それら全てに対応したシステムの構築や更新を続けるのは困難である．そのため，ホームネットワーク内で通信するのであれば，どのデバイスも必ず利用するネットワークを利用したシステムを構築することが望ましい．本研究では，SDN を用いて，ホームネットワークに適した形での不正な通信の検知を検討する．

2　関連研究

2.1　OpenFlow を用いた不正アクセス防御

村上らは，OpenFlow を用いてホームネットワーク内に，動的な認証システムを構築し，不正アクセスによる被害を軽減する手法を提案した [2]．認証時に頻繁に利用される情報を用いることで，ネットワークに接続する端末を制限すると共に，万が一認証が突破された場合でも不正アクセスが検出できるシステムを構築した．しかし，一度攻撃者に認証を突破された場合，不正アクセスの検出までに時間を要すると考えられ，ホームネットワーク内に不正アクセスが拡大してしまう問題点がある．現在の IoT デバイスは，クラウド上のシステムと連携することで，デバイス間の連携を可能にしているが，今後はホームネットワーク内で閉じたデバイス間の通信によって連携を行う形になることが想定される [3]．デバイス間で直接通信を行う場合，各デバイスでどのデバイスの通信を受け入れるかアクセス制御を行う必要がある．しかし，全てのデバイスがアクセス制御に対応しているとは限らず，デバイスの計算能力や脆弱性によってアクセス制御が機能しない場合が考えられる．そのため、同じホームネットワークに他の多くのデバイスが何の制限もなく接続されているという事実を利用して，個人情報の漏洩やサービスの操作など，悪意のある活動が行われる可能性がある [4].

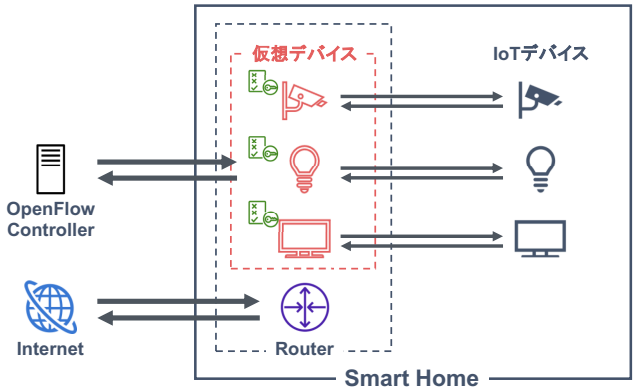

図 1: 提案システムの構成

2.2　論理デバイスを用いた IoT プラットフォーム

今野らは、セキュリティ対策を施し仮想的に作成した論理デバイスを利用し、実際の IoT デバイスの通信を中継することで、セキュアな通信環境を提供するプラットフォームを提案した。これにより、IoT デバイスのリソース量に依存しないセキュリティ対策の実現が可能となる。しかし、事前にて提供していたセキュリティ対策では想定していなかったインシデント等が発生した際に、追加のセキュリティ対策を提供することとなり、早急な処理を施すことができない問題点がある。

3　提案システム

前述の問題点を受けて，不正アクセス拡大を防ぐことを考慮し，ホームネットワーク内においての検知も必要である．提案システムでは，SDN の代表的なプロトコルである OpenFlow [6] を利用することで，既存 IoT デバイスや異なる規格などに対応でき，ホームネットワークに適した形で

表 1: IPA による IoT 高信頼化要件の定義

IoT 高信頼化要件	
開始	[要件 1] 導入時や利用開始時に安全安心が確認できる
予防	[要件 2] 稼働中の異常発生を未然に防止できる
検知	[要件 3] 稼働中の異常発生を早期に検知できる
回復	[要件 4] 異常が発生しても稼働の維持や早期の復旧ができる
終了	[要件 5] 利用の終了やシステム・サービス終了後も安心安全が確保できる

不正な通信の検知を実現する．また，動的に接続を管理することで，不正通信による被害を軽減する．

3.1 想定環境

ホームネットワークにおける閉じたデバイス間の通信，ルーター・デバイス間の通信を想定する．また，デバイス数は一般的に利用されているルーターの推奨接続台数である 10~15 台を想定する．

3.2 構成

OpenFlow を用いて，トラフィック監視を行うことで，ホームネットワーク内で行われる通信を制限する．本提案手法の構成を図 1 に示す．既存 IoT デバイスに OpenFlow スイッチ (OFS) の機能を導入することは困難であると考え，OpenFlow スイッチの機能を持った仮想デバイスを既存 IoT デバイスの前に配置する．通信が行われる際に，仮想デバイスを通して，OpenFlow コントローラ (OFC) に接続し，トラフィック情報から通信の許可を判断する．

3.3 動作手順

本提案手法の動作手順を以下に述べる．

1. 仮想デバイス (OFS) と OFC は互いに，Echo Request/Reply メッセージを定期的に送信
2. 接続要求デバイスは仮想デバイス (OFS) に通信
3. 仮想デバイス (OFS) は OFC に対して，Packet In メッセージを送信
4. OFC はトラフィック情報を調査
5. OFC は仮想デバイス (OFS) に対して，許可/不許可メッセージとして，Flow Mod メッセージを送信
6. OFC は仮想デバイス (OFS) に対して，Packet Out メッセージを送信

4 評価

4.1 評価項目

本研究では，実用性と信頼性を評価する．実用性では，システムの負荷がネットワークに与える影響を測定したいため，遅延を評価する．信頼性では，IoT デバイスを用いたシステムの安心安全を確保するための機能として，表 1 のように，IPA により IoT 高信頼化要件・機能要件が定義されている．本研究では，システムの稼働中の局面である予防，検知，回復の 3 つにおける高信頼化要件に対し，提案システムの有効性について考察する．

4.2 評価シナリオ

評価シナリオとしては，IoT デバイスが 1 対 1，1 対 N($2 \leqq N \leqq 14$) で通信を行っている状況を想定し，各状況において評価を行う．

5 まとめ・今後の課題

本稿では，ホームネットワークの形態の多様化からセキュリティ上の課題として，近年，増加傾向が見られる不正アクセスに着目した．また，今後のスマートホームデバイスは，ホームネットワーク内で閉じたデバイス間の通信によって連携を行う形になることが想定される．そこで本研究ではその対策として，OpenFlow を用いてホームネットワーク内で動的なトラフィック監視を行い，デバイス間通信における不正アクセスによる被害を軽減する手法を提案した．本提案手法では，デバイスの前に OpenFlow スイッチの機能を持った仮想デバイスを配置し，トラフィック情報を OpenFlow コントローラで管理することで，不正アクセスを防ぐ．

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 ver 1.0", 2016.

[2] 村上萌, 中村嘉隆, 高橋修, "OpenFlow を用いたホームネットワークへの接続端末制御による不正アクセス防御手法の提案", 研究報告コンピュータセキュリティ (CSEC), Vol.2016-CSEC-72, No.29, pp.1-6, 2016.

[3] C. Vallati et al., "Mobile-Edge Computing Come Home Connecting things in future smart homes using LTE device-to-device communications", IEEE Consumer Electronics Magazine, Vol.5, No.4, pp.77-83, 2016.

[4] M. Serror et al., "Towards In-Network Security for Smart Homes", Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018), No.18, pp.1-8, 2018.

[5] IPA 技術本部 ソフトウェア高信頼化センター (SEC), "「つながる世界の開発指針」の実践に向けた手引き", 2017

[6] Nick McKeown et al., "OpenFlow: enabling innovation in campus networks," SIGCOMM Computer Communication Review, Vol.38, pp. 69 - 74, 2008.