SDNによる仮想デバイスを用いた セキュアなホームネットワークの検討

塚崎 拓真[1]　滕 睿[2]　佐藤 健哉[1]

A Study of SDN-based Security Platform for Home Networks

TAKUMA TSUKASAKI[1]　RUI TENG[2]　KENYA SATO[1]

1. 概要

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．

しかし，IoT の発展により利便性が高まる一方で，これまでネットワークに接続されていなかった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．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．また，現在のスマートホームデバイスは，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．デバイス間で直接通信を行う場合，各デバイスにおいてどのデバイスと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の制限によって実現できるアクセス制御に制限がある場合や，デバイスのソフトウェア自体の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，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．

そこで本研究では，SDN(Software Defined Networks) の代表的プロトコルである OpenFlow 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した．OpenFlow 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不正な通信の検知を実現する．仮想デバイスというセキュリティ対策を適用可能なデバイスを，ゲートウェイ上に仮想的に作成する．ここに IoT デバイスがリソースの都合上適用できないセキュリティ対策をオフロードし，この仮想デバイスが IoT デバイスの通信を中継し，仮想デバイス間通信も可能にすることで，本来 IoT デバイスに適用したいセキュリティ対策を実現する．セキュリティ対策として，ホームネットワーク内の通信のトラフィック情報は既知であることを考慮し，フローの検証を OpenFlow コントローラで行う．

ルーター内に仮想デバイスとして OpenFlow スイッチを設置し，IoT デバイス間で通信を行うシミュレーションを実装し，ホームネットワークにおいてセキュリティ要件を保つことを示した．

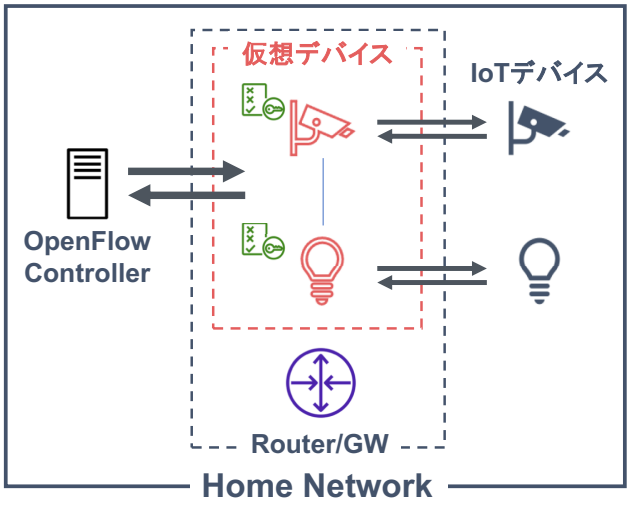

図 1　提案手法の構成

[1] 同志社大学大学院 理工学研究科
Graduate School of Science and Engineering, Doshisha University
[2] 同志社大学モビリティ研究センター
Mobility Reserch Center, Doshisha University