IoTデバイスの通信セキュリティ向上のための ネットワーク仮想化フレームワークの提案

塚崎 拓真[1]　滕 睿[2]　佐藤 健哉[1]

Proposal of Network Virtualization Framework to Improve Communication Security of IoT Devices

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，IoT デバイスは従来の PC 等の既存機器と比較した場合，CPU 等のリソースを十分に保持していないため，デバイスの計算能力の制限やソフトウェア自体の脆弱性によって，適用できる機能が限られるという問題がある．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．

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内の通信を監視するフレームワークの構築を検討した．提案システムでは，セキュリティ対策を適用可能なデバイスを Proxy と定義し，ルータ上に仮想的に作成する．ここに，IoT デバイスがリソース量の制限により適用できないセキュリティ対策をオフロードし，この Proxy が IoT デバイス間の通信を中継することで，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．

ルータ内にコンテナを配置し，そのコンテナ上に Proxy を作成する．そして，IoT デバイス間で閉じた通信を行うシミュレーションの評価を行い，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．

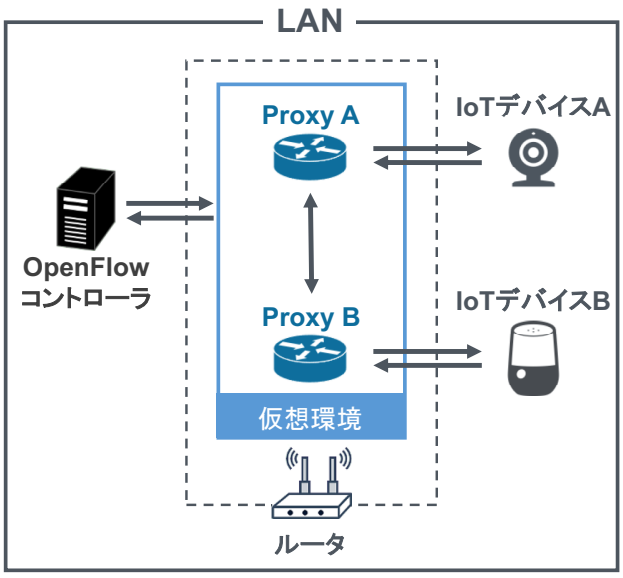

図 1　提案システムの構成

[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