ISS-A-009

ネットワーク起動型 IoT デバイスの研究

荒木　大和†　　寺澤　卓也†
† 東京工科大学メディア学部メディア学科

1. はじめに

近年、急速に普及してきたものに IoT がある。カメラや炊飯器など身近なものがインターネットに繋がる現代となった。この普及に伴い、IoT のセキュリティーが問題視されるようになった。IoT デバイスを購入した利用者が適切なセキュリティー設定を行わないまま運用してしまうことや、脆弱性が見つかったバージョンのソフトウェアをアップデートせず利用し続けてしまうことで悪意をもった者に不正に利用されるといった事例が多い。

そこで、本研究では利用者が自主的に IoT デバイスの保守を行うのではなく利用者によらず自動で保守が行われる仕組みを本学の卒業生である藤島氏の研究[1][2]を元に考察し、実装する。

2. 近年の IoT デバイス

IoT とは広い概念であるが、この研究では主に家庭内の WiFi ルーターやネットワーク家電を対象とし、IoT デバイスと呼ぶ。IoT デバイスは直接外部との通信を行うことが可能であり、ある程度の計算能力が備わっている。また、汎用的な OS を搭載していることが多く、小型のコンピュータそのものである。さらに、最近の IoT デバイスは組み込み機器のようにハードウェアとソフトウェアがメーカー独自のものであり、ある限られた機能のみを持たせたものとは違い、Raspberry Pi などの汎用化された小型コンピュータと Linux などの汎用 OS を用いることが増えている。そのため、IoT デバイスのソフトウェアは一般的な OS 上で動作するものとなりそれに伴い、不正アクセスなどによる様々なリスクは高まっている。

この問題に対処するためにはメーカーがソフトウェアをアップデートするか、ユーザーがセキュリティーを高める必要がある。メーカーがアップデートをリリースしてもユーザーがアップデートを適用するかはユーザー次第であり、その結果、適切なセキュリティー対策が施されることはほとんどない。

3. ソフトウェアが確実に保守される仕組

適切なセキュリティー対策が施されるには、ユーザー側が意識せずにソフトウェアの保守が行われることが必要である。

これを解決するために、本研究ではソフトウェア部分をハードウェアに書き込むのではなく、クラウド上に保管し起動時にネットワークブートを行うようにして起動することを提案する。これにより、自動で保守が行われるだけでなく異なるイメージを使用してブートすることで IoT デバイスの機能を切り替えることが出来るようになるという利点もある。

一般的なネットワークブートはローカル環境でのみの運用を前提とし設計されている。今回の研究では異なるネットワークからブートする必要があるため、図 1 のように、2 段階のブートという方法でブートを実装した。

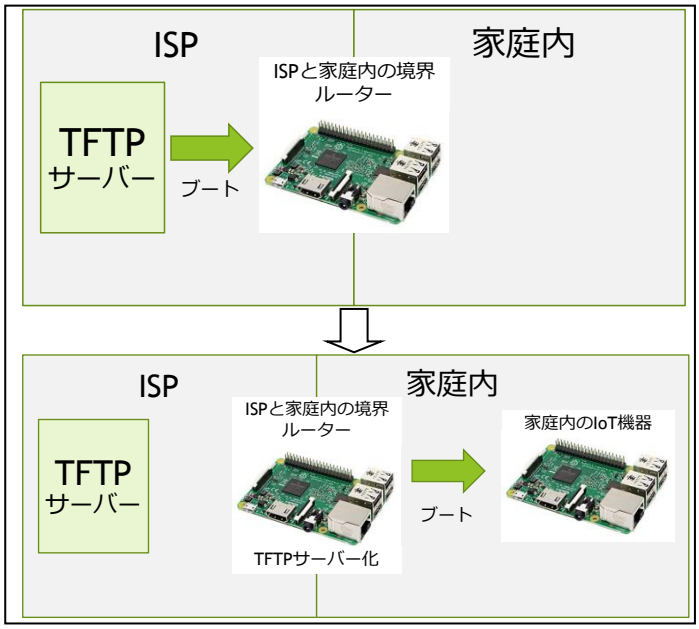

図1. 2 段階のブート

4. 評価

異なるネットワークから問題なくブートするか、自動で保守が行われるか、IoT デバイスの機能を切り替えることが出来るかで評価を行った。結果として上記の 3 点については概ね実装することが出来た。

5. 問題点と課題

今のままではブート元のサーバーを各 ISP ごとに設置する必要があるが、現実的ではない。理想は、ルーティング可能なプロトコルでブートすることである。これを今後の課題とする。

参考文献

[1] 藤島 久麿、 IoT に関するセキュリティーの研究、2017 年度東京工科大学メディア学部卒業論文、2018.

[2] 藤島 久麿、寺澤 卓也、家庭向けネットワーク機器のホワイトボックス化の提案、情報処理学会 第 80 回全国大会講演論文集、2018