C-001

# 組込みシステムへのネットワーク不正アクセスの検出と隔離方法の提案と実現

# Proposition and realization of the detection and isolation method for unauthorized network access of an embedded system.

森内貴洋† 荒木英夫‡
Takahiro Moriuchi Hideo Araki

## 1. はじめに

IoT(Internet of Things)の普及により、スマートフォンやセンサ内蔵機器をインターネットに接続し、サービスを提供する動きが盛んになってきており、家電の分野ではスマート家電等が普及し始めている。また、IoT は昨年政府が掲げた「日本再興戦略 2016」の鍵となる第 4 次産業革命の一部でもあるため、ますます接続機器が増えることが予想される[1]。しかし、これらの機器はインターネットに接続されている為、サイバー攻撃を受ける恐れがある。そのため、IoT 機器を含む組込みシステムのネットワークセキュリティを実現し、安全を確保することは喫緊の課題として大変重要である。このためのアプローチとして暗号化機能をハードウェアで提供し、デバイスに実装したソフトウェアのマルウェアによる改ざんや改造の有無の検知をすることができる TMP(Trusted Platform Module)[2]や、ホスト間連携を可能にするパスワード総当たり攻撃対策手法[3]など不正な攻撃や侵入を阻止することを目的とした研究がおこなわれている。しかし、例えば監視カメラといった無人観測設備やセキュリティメインテナンスの行き届かない僻地などに設置された IoT 機器においては、全ての機器について不正アクセスなどを阻止することは困難であると考える。例えば、ネットワーク上に MAC アドレスや IP アドレスを偽装した不正アクセス用のデバイスと正規のデバイスを交換されることも考えられる。そこで本研究では、MAC アドレスや IP アドレスでは判別不可能な、不正な機器の接続を検出することを試み、不正な機器のネットワークからの隔離を行うシステムの実現を目指す。

## 2. 提案手法と評価システム

本提案手法が対象とする機器は前提として、屋外にある監視カメラなど常時管理することができないシステムあること、複数のデバイスが同一のネットワーク上に存在することである。また、対策として効果が現れるのは、デバイスの差し替えといった攻撃を受けた後であり、最後に IP アドレスを切り替えるということは攻撃者に知られていないとする。

本稿で想定するシステムの構成を図 1 に示す。マイコンに IP アドレスを管理する機能を実装し、監視カメラなどのデバイスと通信を行う。その後、一定期間後などの決められたアルゴリズムに従い、IP アドレス管理マイコンから各デバイスに IP アドレスを変更するように指示を送る。もし、一つのデバイスが差し替えなどの攻撃を受け乗っ取られたとしても、IP アドレスを変更することができないのでネットワーク上から隔離され、通信を行うことができなくなる。また、本システムを利用する利用者のアクセスはすべて IP アドレス管理マイコンを経由するので、不正なデバイスにアクセスすることはない。

次に評価システムと通信手順を図 2 に示す。IP アドレス管理マイコンとデバイスマイコンはソケット通信でやり取りを行う。デバイスのサービスとしてはユーザが入力した 2 つの数字を足し合わせ、その結果を返すというものである。サービスを提供している最中に IP アドレス管理マイコン側から IP アドレスの変更を通知し、デバイス側は IP アドレスを変更する。IP アドレスを変更した後もサービスは提供され続ける。

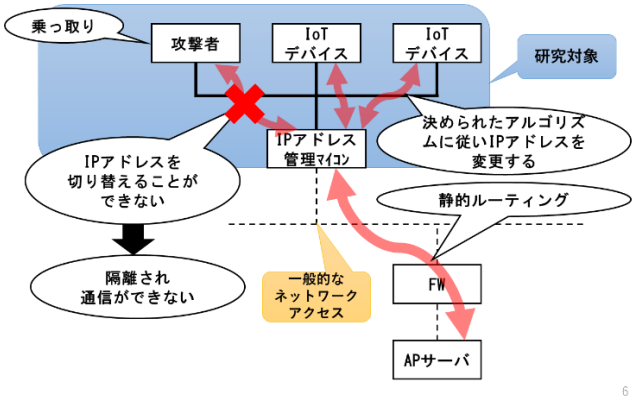


図 1　想定システムの構成図

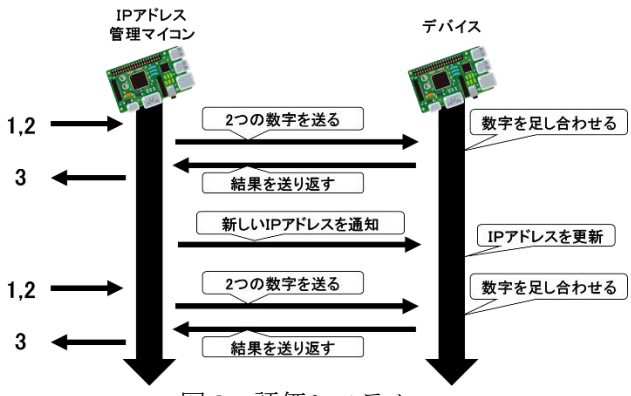


図 2　評価システム

†大阪工業大学　大学院　情報科学研究科 Graduate School of Osaka Institute of Technology
‡大阪工業大学　情報科学部 Osaka Institute of Technology

## 3. 実験環境について

本システムの有効性を検証するために、次のような構成で評価実験システムを構築した。

まず、本システムで使用するマイコンボードは全て Raspberry Pi 2 を使用した。この Raspberry Pi 2 を 3 台用いて、IP アドレス管理側、サービスの提供を行うデバイス側、攻撃者側としてネットワークに接続した。システムの運用状態の想定として、デバイス側で足し算のサービスを提供中に、一台のデバイスが攻撃者によって差し替えられたという設定を行った。また、すべてのマイコンは同一ネットワーク上に配置し、ネットワーク監視機能のあるルータ(Yamaha FWX120)にそれぞれ接続した。今回は、ルータ上の防御機能などは用いていない。さらにパソコンを同一ネットワーク上に接続しパケットキャプチャを行い、通信が正しく行われているかを確認した。実際に評価実験を行っている様子を図 3 に示す。

次に、IP アドレスの管理方法として次の 3 つの方法を IP アドレス管理側システムに実装し評価を行った。

1. 最下位 8 ビットの数字を 1 ずつ変えていく。
2. 1～8 の乱数を用意し、相応するビットの場所を 0 または 1 にし、それをアドレスとする。
3. マイコンの現在時刻を取得し、その時刻を基に計算を行いアドレスに加算する。

今回 IP の変更タイミングは IP アドレス管理マイコンからデバイス側のマイコンに指示を行った。そして、IP が変更され、攻撃側が正常にネットワークから切り離されたことの確認は、攻撃側のプログラムをモニタすることにより行った。

図 3　実験環境の写真

## 4. 実験結果

評価実験では、デバイス側でサービスを提供中に攻撃者から DoS 攻撃のように計算サービスを要求するデータを送り続けた。また、今回は通常のサービス要求として、IP アドレス管理側でも一定間隔でサービス要求を行うプログラムを実行し、通常のサービスが提供され続けていることを確認しながら実験を行った。

そして実験を開始して一定時間経った後に、IP アドレス管理マイコンからデバイス側に対し、IP アドレスの変更要求を送り IP アドレスを切り替えた。この時、切り替える前後のトラフィック量を FWX120 の機能を用いて測定した。

IP アドレスを切り替えた直後の動作として、攻撃側のプログラムはソケット通信にエラーを発生し、サービス要求が行えなくなることを確認した。また、攻撃者がデバイス側にアクセスすることができなくなったため、トラフィック量が下がっていることが確認できた。また、22 分に IP アドレスの変更を行ったが、その際に多くのパケットが送られていることも確認できた。トラフィックの測定結果を表 1 に示す。

表 1　トラフィック量の推移

| 時刻 | 入力(平均) | 入力(最大) |
|---|---|---|
| 14:18:21 | 7 | 90 |
| 14:19:21 | 0 | 0 |
| 14:20:21 | 2 | 90 |
| 14:21:21 | 0 | 0 |
| 14:22:22 | 68 | 1639 |
| 14:23:22 | 0 | 0 |
| 14:24:22 | 1 | 60 |

## 5. まとめと今後の課題

今回の実験では想定通り IP アドレスを切り替えることで、攻撃者のシステムへのアクセスを拒否することが確認できた。そして、実装を行った 3 種類の IP アドレスの管理方法も正常に動作することを確認できた。

今後の課題として、現在の評価システムでは変更する IP アドレスを通信で通知しているが、盗聴されると新しい IP アドレスが攻撃者に知られてしまったり、次の IP アドレスを推測されてしまったりする可能性があるので、暗号化などを併用したシステムの実現が必要である。また、現状、デバイス側の IP アドレスは変更しているが、IP アドレス管理側の IP アドレスは変更していないので、正常に設置されたマイコン全ての IP アドレスを変更する手順に実装を行っている。

そして、IP アドレス管理マイコンにファイアウォールの機能を実装し、デバイスに対するすべての通信を IP アドレス管理マイコン経由で行う予定である。

### 参考文献

[1]首相官邸,「日本再興戦略 2016 –第 4 次産業革命に向けて-」,2016-06-02

[2]畠中伸敏,井上博之,佐藤雅明,伊藤重隆,折原秀博,永井庸次,「IoT 時代のセキュリティと品質」,日科技連,p31-32,2017-04-17

[3]大隅淑弘, 山井成良,「ホスト間連携を可能にするパスワード総当たり攻撃対策手法」, 情報処理学会研究報告インターネットと運用技術（IOT） 2007(93(2007-DSM-047)), 49-54, 2007-09-21