ISS-A-051

# DNS に着目した IoT デバイスの不正通信防止手法

佐々木　雄也† 　榎本　智洋† 　二神　友香† 　藤野　貴之†
†近畿大学工学部電子情報工学科

## 1. はじめに

近年，多くの IoT デバイスはセキュリティ的に脆弱であることが指摘されている．全ての IoT デバイスを管理することは困難であるため，IoT ネットワークを監視し，不正な動作を行う IoT デバイスを早期に検知する仕組みが求められている．

## 2. 先行研究

Sperling らは，安価な Raspberry Pi を監視ノードとしてネットワーク上を流れる全ての IP パケットを取得して解析する手法を提案している[1]が，パケットのキャプチャは CPU を始めとするリソースへの負担が大きいという問題がある．

## 3. 提案手法

あらゆる通信は DNS を起点とすることから，監視ノード上で DNS 問い合わせのパケットだけを監視する手法を提案する．具体的に，udp/53 のパケットだけを透過的に DNS proxy に転送するようにする．DNS proxy では，問い合わされた名前を検査し，登録されたホワイトリストにマッチしていれば，名前解決をしてクライアントに返すようにする．マッチしない場合や，使用キャッシュサーバが正当なものでない場合，NXDomain 応答を返すようにする．このようにすることで，正当な DNS キャッシュサーバを指定した正当なホストへの通信だけが行われ，それ以外の通信を全て防止することが可能となる．

## 4. 提案システムの実装

### 4.1 監視ノードの構成

DNS 問い合わせを受信し中継する DNS Proxy を Java で実装した．監視ノードである Raspberry Pi 上で DNS Proxy を稼働させ，iptables の設定により透過的に udp/53 のパケットを DNS Proxy に配送させるようにした．

### 4.2 監視ロジックの実装

ホワイトリストを用意し，問い合わせの QNAME がホワイトリストにマッチする場合は通常どおり中継を行う．マッチしない場合には NXDomain 応答を生成して返すようにする．

### 4.3 NXDomain 応答の生成

例えば、www.example.jp A が問い合わされ，QNAME=www.example.jp はホワイトリストにマッチしなかったとする．その場合，DNS Proxy は QTYPE を A から SOA に変更して問い合わせを中継する．応答を受信すると，応答のヘッダ情報を修正し，ResponseCode を NO_ERROR から NAME_ERROR に，付加情報部の個数を 1 から 0 にする．最後に QTYPE をオリジナルの A に戻して付加情報部を削除する．以上の手順により，任意の問い合わせ名・問い合わせタイプに対して NXDomain 応答が生成できるようになる．

## 5. 動作検証と考察

### 5.1 不正ホストへのアクセス防止

ホワイトリストに無い www.google.com．にアクセスした結果を図に示す．名前解決ができないため通信不能になっていることがわかる．

```
curl www.google.com
curl: (6) Could not resolve host: www.google.com
```

図 1. 不正ホストへのアクセス防御例

### 5.2 負荷の比較

systat を使用して Thales らの手法と提案手法の CPU 使用率を比較した．Thales らの手法は 3.11 で，提案手法は 0.77 であった．我々の提案手法は 1/4 の計算負荷で Sperling らと同等以上の IoT ネットワーク監視を実現できた．

## 6. おわりに

先行研究よりも CPU の負担を軽減し，不正な DNS キャッシュサーバの指定を検知，許可されないドメイン名・ホスト名の名前解決を検知することができた．今後の課題として，DNS 問い合わせに DNS over Https が使用された場合への対策を考える必要がある．

## 参考文献

[1] T.L.von Sperling, F.L.de Caldas Filho, R.T.de Sousa, L.M.C. e Martins and R.L. Rocha, "Tracking intruders in IoT networks by means of DNS traffic analysis," 2017 Workshop on Communication Networks and Power Systems (WCNPS), pp.1-4(Nov.2017).