2E-03

IoT-GW向けホワイトリストの機械学習期間における暫定的なホワイトリストの提供手法の提案

野村公輝 † 永渕幸雄 † 谷川真樹 †
日本電信電話株式会社 NTT セキュアプラットフォーム研究所 ‡

1 はじめに

IoT 機器はパソコンと比較してリソースが少ないため，セキュリティ対策ソフトウェアの導入が困難な場合がある．そのため，IoT 機器のセキュリティ対策として，IoT 機器が接続する IoT ゲートウェイ（以降，IoT-GW）でホワイトリストによるアクセス制御が利用される．

ホワイトリストによるアクセス制御は，許可する通信以外をアクセス不可にする制御方法である．IoT 機器に関するホワイトリストの作成方法として機械学習が有効である [1]．しかし，機械学習でホワイトリストを作成する場合は，数日程度の期間を要する場合がある．このホワイトリスト作成期間中に IoT 機器が危険なサイトへ通信すると，マルウェアに感染する可能性がある．そこで，本稿ではホワイトリスト作成期間中に暫定的なホワイトリストを提供する方法を提案する．

2 IoT-GW におけるアクセス制御

本稿では，IoT 機器のセキュリティ対策として，IoT-GW に適用するホワイトリストによるアクセス制御を提案する．

IoT-GW に適用するホワイトリストによるアクセス制御を実現する際の全体構成を図 1 に提示する．

図 1 の各要素を下記に記載する．

IoT-GW

- IoT-GW 配下の IoT 機器がインターネットに通信する際に経由する．
- IoT-GW 配下の IoT 機器情報（機種，台数）を定期的に収集する．
- IoT-GW 配下の IoT 機器ごとに許可される通信内容（ホワイトリスト情報）を指定したホワイトリストを機械学習により定期的に作成し，適用する．

IoT 機器

- IoT-GW を経由してインターネットに通信する．
- IoT-GW に適用されたホワイトリストで許可された通信のみインターネットに通信することが可能である．

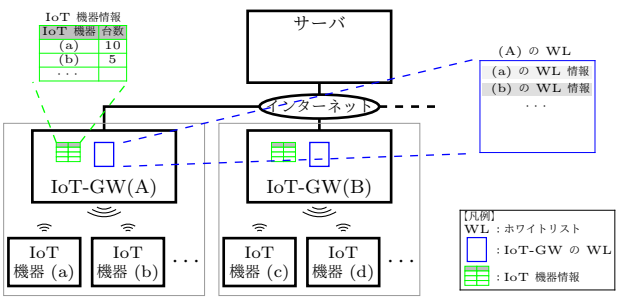

図 1 全体構成

サーバ

- IoT-GW にてホワイトリストを機械学習により作成する処理の実施が（IoT-GW の）性能面で厳しい場合，処理を分担あるいは代替で実施する．

3 提案手法

暫定的なホワイトリストを作成し，IoT-GW に提供する手法を図 2 を利用して説明する．

1. IoT-GW に適用されている既存のホワイトリスト，IoT-GW 配下の IoT 機器情報を IoT-GW から収集する．
2. 収集したホワイトリストには各 IoT 機器のホワイトリスト情報が記載されている．収集した全てのホワイトリストについて，サーバが所有する IoT 機器情報と照合し，条件 (*) を満たす IoT 機器のホワイトリスト情報のみ抜粋する．（図 2 の例では，IoT 機器が 20 台以上であることを条件としている．）
   2 つ以上の既存のホワイトリストに同一 IoT 機器のホワイトリスト情報が存在し，その内容に差分がある場合は，網羅的に抜粋する．
3. 抜粋したホワイトリスト情報から構成される暫定的なホワイトリストを作成する．
4. 暫定的なホワイトリストを IoT-GW に提供する．
5. 既存の IoT 機器には既存のホワイトリストを，新規の IoT 機器には既存のホワイトリストと暫定的なホワイトリストの両者を結合したホワイトリストを適用する．
6. 上記 1.~5. を定期的（1 日 1 回など）に繰り返し実施する．

(*) 具体的な条件は，利用場面ごとで適宜決定する．例として，IoT 機器の台数や存在拠点数などに基づいて決定する．

暫定的なホワイトリストを提供することにより，自 IoT-GW 配下にない機種の IoT 機器のうち，他 IoT-GW 配下にある機種の IoT 機器については，暫定的なホワイトリストに基づき，自 IoT-GW から危険なサイトへ通信することを防止することができる．（図 2 の例では下記の通りとなる．）

- IoT-GW(A) では新規機器として IoT 機器 (a)(b)(y) 以外に，IoT 機器 (c) も接続することが可能になる．
- IoT-GW(B) では新規機器として IoT 機器 (a)(c)(x) 以外に，IoT 機器 (b) も接続することが可能になる．

A proposal of a method for providing provisional whitelist during machine learning period of whitelist for IoT-GW
† Kouki Nomura, Yukio Nagafuchi, Masaki Tanikawa
‡ NTT Secure Platform Laboratories NTT Corporation

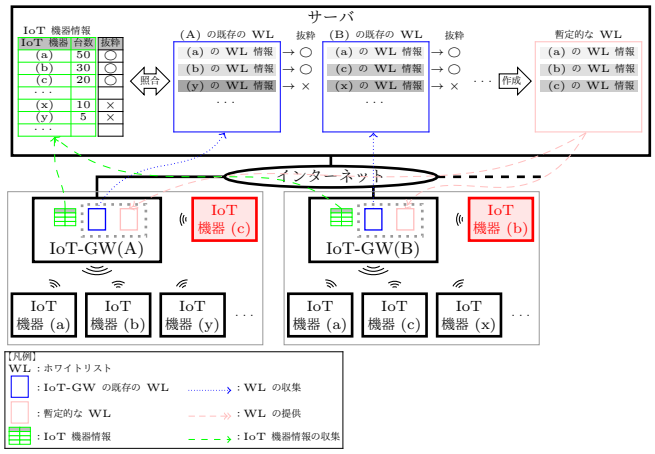

図 2 提案手法

4 数値例

3 章で提案した手法を適用した数値例を確認する．

IoT-GW，IoT 機器についての仮定，IoT 機器のホワイトリスト情報の抜粋条件，確認内容を下記に記載する．

仮定

- IoT-GW の全台数は 2000 台とする．
- IoT 機器の全機種数は 20000 種類とする．
- 1 台の IoT-GW 配下にある IoT 機器の台数は 10 台とする．
  このとき，各機種とその台数（の組合せ）は一様乱数で仮定する．

抜粋条件

- 全ての IoT-GW から収集した IoT 機器情報を基に，ホワイトリスト情報を抜粋する条件として IoT 機器が一定台数以上存在することとする．

確認内容

- 抜粋条件である IoT 機器の台数を 1 台以上，2 台以上，⋯ と変化させていき，各条件ごとにホワイトリスト情報を抜粋できる IoT 機器の機種数を確認する．

上記の確認内容の結果を下記に記載する．

結果

- 抜粋条件の台数とホワイトリスト情報を抜粋できる IoT 機器の機種数の関係を図 3 に提示する．

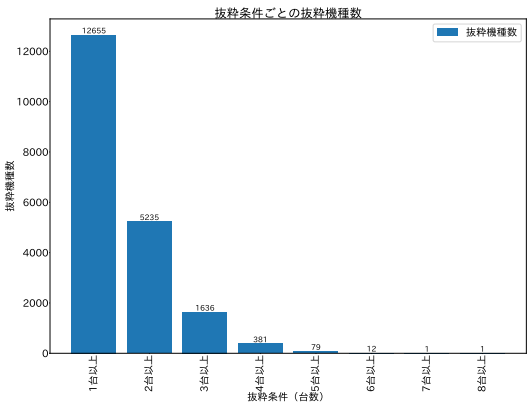

図 3 抜粋条件の台数とホワイトリスト情報を抜粋できる IoT 機器の機種数の関係

抜粋条件である IoT 機器の台数の増加に伴い，ホワイトリスト情報を抜粋できる IoT 機器の機種数は反比例のグラフのような形で減少した．

- 複数の IoT-GW からホワイトリストを収集することで，抜粋条件である IoT 機器の台数が 2 台以上であっても，大量の IoT 機器のホワイトリスト情報を抜粋することが可能である．
- 抜粋条件である IoT 機器の台数が少ないほどホワイトリスト情報を抜粋できる IoT 機器の機種数は多い．しかし，暫定的なホワイトリストの容量や，台数の少ない IoT 機器のホワイトリスト情報が不正な内容である可能性を考慮したい場合は，抜粋条件である IoT 機器の台数を多くすることでホワイトリスト情報を抜粋できる IoT 機器を厳選することになる．
- 利用場面に応じて，最適な抜粋条件の台数を選定することが望ましいと考えられる．

5 おわりに

本稿では，ホワイトリスト作成期間に IoT 機器が危険なサイトへ通信することを防止するため，暫定的なホワイトリストを提供するための方法を提案し，数値例で確認した．

本稿の提案方法の成果と課題例を下記に記載する．

成果

- 本稿の提案方法は，IoT-GW の既存のホワイトリストにホワイトリスト情報が記載されている IoT 機器に対して有効である．
- 本稿の数値例のように IoT 機器の機種と台数にバラつきがある場合，ホワイトリスト情報の抜粋条件を IoT 機器の台数とすることで，暫定的なホワイトリストの容量を少なくしつつ，台数が多い IoT 機器を新規機器として接続することが可能になる．

課題

- IoT-GW の台数が多いほど，収集できる IoT 機器のホワイトリスト情報は多くなるが、偽のホワイトリスト情報が混在する可能性も大きくなる．
- 本稿では，IoT 機器の各機種とその台数（の組合せ）を一様乱数で仮定したが，現実には一様ではなく機種により台数に偏りがあると考えられる．機種による台数の偏りを考慮した上で数値例を確認し，提案手法の効果を確認する必要がある．

参考文献

[1] 山井美和：Internet Infrastructure Review （IIR） Vol.28, Internet Initiative Japan, pp.18～20（2015）.