Vol.2017-DPS-170 No.26
Vol.2017-CSEC-76 No.26
2017/3/3

IoT エッジ端末をボットネット化から防ぐ認証プラットフォームの提案

半田 富己男[†1]　矢野 義博[†1]

概要：つながるクルマ(コネクテッドカー)の車載システムに対するハッキング事例が報告され，IoT エッジデバイス間の機器認証の不備を狙ったサイバー攻撃が脅威となっている．コネクテッドカーやスマートハウスの普及が進む中で，IoT 機器を安心・安全に利用するための通信システム基盤が求められている．本稿では，認証サーバとの間でクレデンシャルを用いて認証された IoT エッジデバイス群(認証済み IoT エッジデバイス群)に所属する通信元 IoT 機器が，同一の認証済み IoT エッジデバイス群に所属する通信先 IoT 機器との間で，安全な VPN 通信セッションを開設するプロトコルと，それを実現する認証サーバを提案する．本稿で提案する方式は，IoT エッジデバイスが NAT 配下(NAT Traversal)に存在していても適用可能である．

キーワード：IoT，VPN，機器認証，コネクテッドカー

A proposal of authentication platform that prevents IoT edges from being built into botnet

FUKIO HANDA, CISSP[†1]　YOSHIHIRO YANO[†1]

1. はじめに

つながるクルマ(コネクテッドカー)の車載システムに対するハッキング事例が紹介されている．[1][2]
さらに，ネットワークカメラや家庭用ルータ等のインターネット接続された IoT 機器がマルウェア「Mirai」に感染し，感染した機器によって構築されたボットネットから大規模な DDoS 攻撃が行われるという事案([3][4])が報告されている．(図 1)
このマルウェアは以下の手順で感染を拡大する：

① すでに感染した機器が新たな感染対象を探索する．これはランダムに生成したグローバル IP アドレスの IoT 機器へのログイン試行のため，辞書攻撃を試みる．
② レポートサーバーに探索結果を報告
③ レポートサーバーがダウンローダーに攻撃対象の IoT 機器へのログイン情報を連絡
④ ダウンローダーが感染対象に侵入し，ボットをダウンロードさせる．

こうした事例では，辞書攻撃で比較的容易に破られるユーザ名，パスワードを使っていた IoT 機器が被害に遭っている．この種の攻撃への対策として，ユーザ名とパスワードを類推されにくいものに変更する，信頼できる接続元 IP アドレスに限定する，脆弱性対策が施されたファームウェアにアップデートする等の対策が求められている．[4]

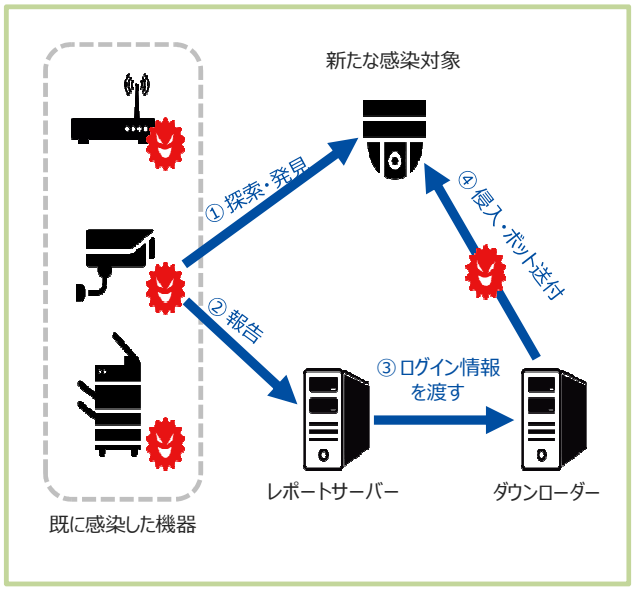

図 1 IoT 機器を狙うボット化マルウェア「Mirai」

本稿では，IoT エッジデバイス群をクレデンシャルを用いて認証して登録し，認証済機器群の間でエンド・ツー・エンドに安全な VPN 通信セッション開設を仲介する認証サーバを提案する．

第 2 章で提案方式を説明し，第 3 章で実装例を述べ，第

†1 大日本印刷(株)
Dai Nippon Printing Co., Ltd.

Vol.2017-DPS-170 No.26
Vol.2017-CSEC-76 No.26
2017/3/3

4 章でまとめと今後の課題を述べる．

2. 提案方式

本章では，提案方式の認証サーバと認証済み IoT エッジデバイス群で構成される認証プラットフォームを説明する．2.1 節で認証サーバの機能を，2.2 節で認証済み IoT エッジデバイス群に所属する IoT 機器間でのエンド・ツー・エンド通信(E2E)機能について述べる．なお，本スキームに参加する IoT 機器には，ユニーク ID が付与されており，エージェント SW を搭載しているものとする．

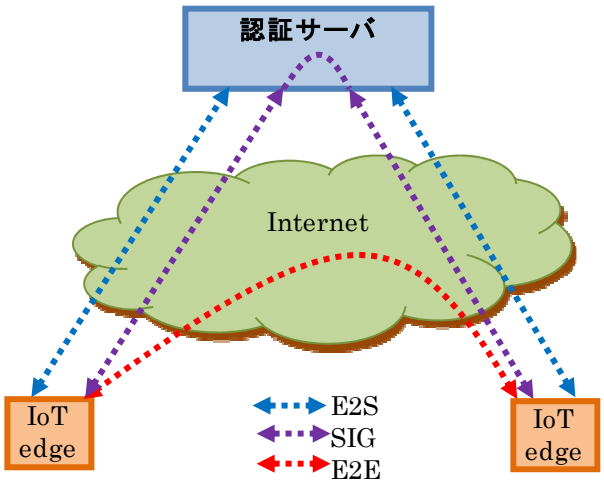

図 2 提案方式の構成

2.1 認証サーバの機能

認証サーバと IoT 機器は，以下の手順で SA (Security Association)を確立した後に，相互に機器認証を行う．

Phase 1:

認証プラットフォームへの登録を希望する IoT 機器は，認証サーバにアクセスし， ID とクレデンシャルを用いて TLS ハンドシェイクシーケンス等により，認証サーバとの間に SA(Security Association)を確立する．図 2 に E2S として示す経路である。

Phase 2:

SA 確立直後，IoT 機器と認証サーバの間で，機器認証と属性情報の交換を行う．ここでは IoT 機器ごとにユニークなユニーク ID を用いて強固な機器認証を行う．

NAT 配下に配置された IoT 機器の場合は，STUN プロトコルを使って認証サーバへの経路上の NAT 種別を調査した結果を属性情報交換メッセージに指定することができる．これによって，IoT 機器と認証サーバの間に，トンネリング転送(図 2 の E2S)およびシグナリング(図 2 の SIG)が可能な状態となる．

Phase 3:

認証済み IoT 機器は，認証サーバとの VPN 接続を維持するため，一定時間パケットが流れない状態が発生したときに，キープアライブ目的で認証済み IoT 機器に対して ECHO メッセージを送信する．このシーケンスで，認証サーバは，認証済み IoT 機器の最新状態を知ることができる．

Phase 4:

VPN トンネルの開放(閉鎖)である．SA の開放を行うとともに，アプリケーションパケットのトンネリングを停止する．
トンネルの開放は，例えば，TLS の ALERT メッセージの送信によって，認証済み IoT 機器，認証サーバのどちらからでも行うことができる．

2.2 認証済み IoT 機器間の VPN 通信

2.1 節の手順で認証サーバに登録された認証済み IoT エッジデバイス群に所属する IoT エッジデバイス同士で Peer to Peer に VPN トンネリング接続(図 2 の E2E)する手順について説明する．

Phase 1: Signaling (図 2 の SIG)

通信元 IoT 機器は，通信先 IoT 機器の端末 ID を指定して，認証サーバに対しピア接続要求メッセージを送信し，通信先 IoT 機器のアドレスを問合せる．

認証サーバは，接続指示メッセージに接続方式情報を設定して通信先 IoT 機器に送信する．

また，認証サーバから接続指示メッセージを受信した通信先 IoT 機器は，認証済み IoT エッジデバイス群に所属する他の IoT 機器から接続要求があったことを認識し，接続指示メッセージに設定された接続方式に応じた処理を行い，認証サーバに対して，ピア接続確認メッセージを送信する．

認証サーバは，ピア接続確認メッセージを受信すると，ピア接続要求メッセージ送信元の通信元 IoT 機器に対し，ピア接続応答メッセージを送信する．
図 2 に SIG として示す経路である．

Phase 2:

通信元 IoT 機器と通信先 IoT 機器は，クレデンシャルを用いて TLS ハンドシェイクシーケンス等により，相互認証を行い，通信元 IoT 機器と通信先 IoT 機器の間に，SA(Security Association)を確立する．図 2 に E2E として示す経路である．

Phase 3:

SA 確立直後，通信元 IoT 機器と通信先 IoT 機器の間で，機器認証を行う．

Vol.2017-DPS-170 No.26
Vol.2017-CSEC-76 No.26
2017/3/3

Phase 4:

通信元 IoT 機器と通信先 IoT 機器は，アプリケーションパケットのトンネリング転送が可能な VPN 接続状態にある．

Phase 5:

VPN トンネルの開放(閉鎖)である．SA の開放を行うとともに，アプリケーションパケットのトンネリングを停止する．

トンネルの開放は，例えば，TLS の ALERT メッセージの送信によって，通信元 IoT 機器，通信先 IoT 機器のどちらからでも行うことができる．

3. 提案方式の実装例

DNP が開発した DNP Multi-Peer VPN では，提案方式の認証サーバ機能を「マネジメントサーバ」として実装している．また，エージェント SW を各種 OS に対応した SDK として提供しているので，車載機器等の IoT 機器に組み込むことができる．(図 3, [5])

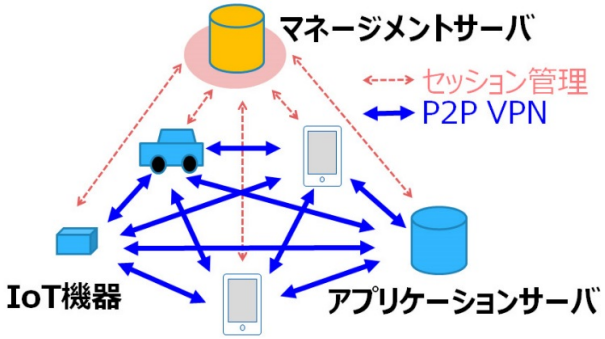

図 3 DNP Multi-Peer VPN の構成

図 4 は，ネットワークカメラに DNP Multi-Peer VPN を組み込んだユースケースである．

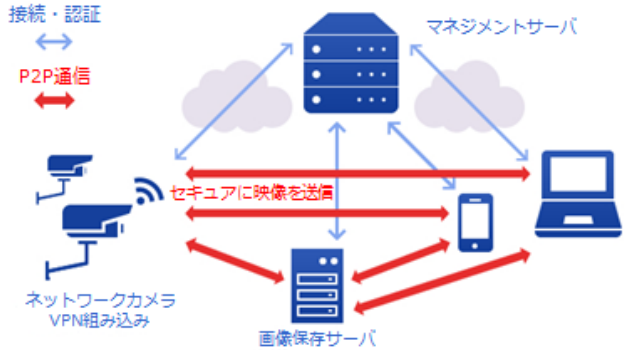

図 4 ネットワークカメラへの VPN 組込み

4. まとめ

認証サーバとの間でクレデンシャルを用いて認証された IoT エッジデバイス群(認証済み IoT エッジデバイス群)に所属する通信元 IoT 機器が，同一の認証済み IoT エッジデバイス群に所属する通信先 IoT 機器との間で, 安全な VPN 通信セッションを開設するプロトコルと，それを実現する認証サーバについて提案した．

本稿で提案した IoT 機器認証プラットフォームは，あらかじめ認証サーバに登録された認証済 IoT エッジデバイス群に属する IoT 機器同士で，エンド・ツー・エンドに安全な VPN 通信セッションを確立する．対象となる IoT エッジデバイスは，NAT 配下に存在して，グローバル IP アドレスを通信相手に知らせなくても，認証サーバの仲介(図 2 の SIG)により，VPN 接続が可能なため，「Mirai」のようなグローバル IP アドレスによるランダム接続を試みるマルウェアの攻撃を受けない．「Mirai」に対する対策として，接続元を信頼できる IP アドレスに限定することも謳われているが，本稿で提案した IoT 機器認証プラットフォームでは，接続元をあらかじめ認証サーバに登録された認証済 IoT エッジデバイス群に IoT 機器だけに限定している．このため，インターネットからの接続元が一定範囲に限定されるコネクテッドカーやスマートハウスで，IoT 機器を安心・安全に利用するための通信システム基盤として有益である．

今後の課題として，IoT 機器台数のスケールに応じたマネジメントサーバの負荷分散の仕組みを検討している．

参考文献

[1] Charlie Miller, Chris Valasek.,“Remote Exploitation of An Unalterd Passenger Vehicle,” black hat USA 2015, https://www.blackhat.com/us-15/briefings.html#remote-exploitation-of-an-unaltered-passenger-vehicle , (参照 2016-12-12)

[2] Charlie Miller, Chris Valasek.,“Advanced CAN Injection Techniques for Vehicle Networks,” black hat USA 2016, https://www.blackhat.com/us-16/briefings.html#advanced-can-injection-techniques-for-vehicle-networks , (参照 2016-12-12).

[3] JVNTA#95530271, “Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威,”, 2016 年 11 月 4 日, http://jvn.jp/ta/JVNTA95530271/ , (参照 2016-12-12).

[4] 警察庁 @police, “インターネット観測結果等(平成 28 年 9 月期),” 2016 年 10 月 20 日, https://www.npa.go.jp/cyberpolice/detect/pdf/20161020.pdf ,(参照 2016-12-12).

[5] DNP Multi-Peer VPN, https://www.dnp.co.jp/vpn/ ,(参照 2016-12-12)