

IoT機器のクラッキング(ハッキング)の手口と対策 - ホワイトハッカーのぼやき

2018年5月19日(土) 11:00-11:45

オープンソースカンファレンス 2018 名古屋

南山大学国際教養学部

特定非営利活動法人 東海インターネット協議会

後藤 邦夫

goto@nanzan-u.ac.jp

<https://goto920.github.io/TIC/IoTSecurity-OSS-Nagoya.pdf>



目次

1. はじめに
 2. 丸見え監視カメラは減ったか？
 3. ルータの自動設定機能に注意
 4. 自宅(自社)LAN内でポートスキャン
 5. 自動車の話題も少し
 6. おわりに
- 参考文献

1. はじめに

- 自己紹介
 - ネットワークエミュレーション、ネットワーク・セキュリティ
 - 自称ミュージシャン(ボーカル、ドラム、ギターなど)
 - <https://goto920.github.io/>
- 今日のネタは1年前の実験結果(自宅にある機器)
- 基本的な注意
 - 初期パスワードは変更しましたか?
 - ルータの設定を確認しましたか?

2. 丸見えカメラは減ったか？

- Insecam[1] (cityでnagoya)
<https://www.insecam.org/en/bycity/Nagoya/>
 - 2017年5月(86件)、2018年4月(91件)
-



店内のリアルタイム動画
店はこの状態を知らない？
依頼した業者さんがだめ？

2. (続き) 丸見えの原因と対策

- 2つの条件を両方満たすとき
 - IoT機器のパスワードがマニュアル記載の初期値
 - IoT機器がルータを自動設定した結果、外から見える
- 対策
 - パスワード(可能ならユーザ名も)を変更
 - 外から見る設定にしたいなら、パスワード変更だけでOK
 - 外から見る必要がないなら、ルータの設定を変更

3. ルータの自動設定機能に注意

- Universal Plug and Play (UPnP)が曲者[2]
 - LAN側から認証なしでルータの設定変更が可能
 - WAN側からUPnPが使える欠陥ルータもあった
 - ルータの初期設定でonになっていることが多そう
- ルータ設定画面例(某社のHome GW、次ページ)
 - 詳細設定 > 高度な設定 > UPnP設定
 - defaultで使用する(on)になっていた
- PCで見える機器はUPnP対応
 - Windowsのファイルブラウザ、ネットワークで表示される
 - gupnp-toolsのgupnp-universal-cp コマンド
- WAN側の確認はShieldsUp[3] (<https://www.grc.com/x/ne.dll?bh0bkyd2>)

高度な設定

⚠️ ご注意ください

設定変更は即時に有効となります。[設定]ボタンをクリックしたあと、本商品にアクセスできなくなる場合がありますので、その場合は、Webブラウザを-Webブラウザを開きなおしてください。

《高度な設定》画面の[WAN→LAN中継設定]と《静的IPマスカレード設定》画面の内容が競合した場合は、《高度な設定》画面の[WAN→LAN中継設定]を変更を行うと、通話・通信が切断されることがあります。

高度な設定

LANポート通信設定	自動設定	(LAN1)
	自動設定	(LAN2)
	自動設定	(LAN3)
	自動設定	(LAN4)
LAN側MDI/MDI-Xモード	MDI-X固定	
セキュリティ保護機能	<input checked="" type="checkbox"/> 使用する	

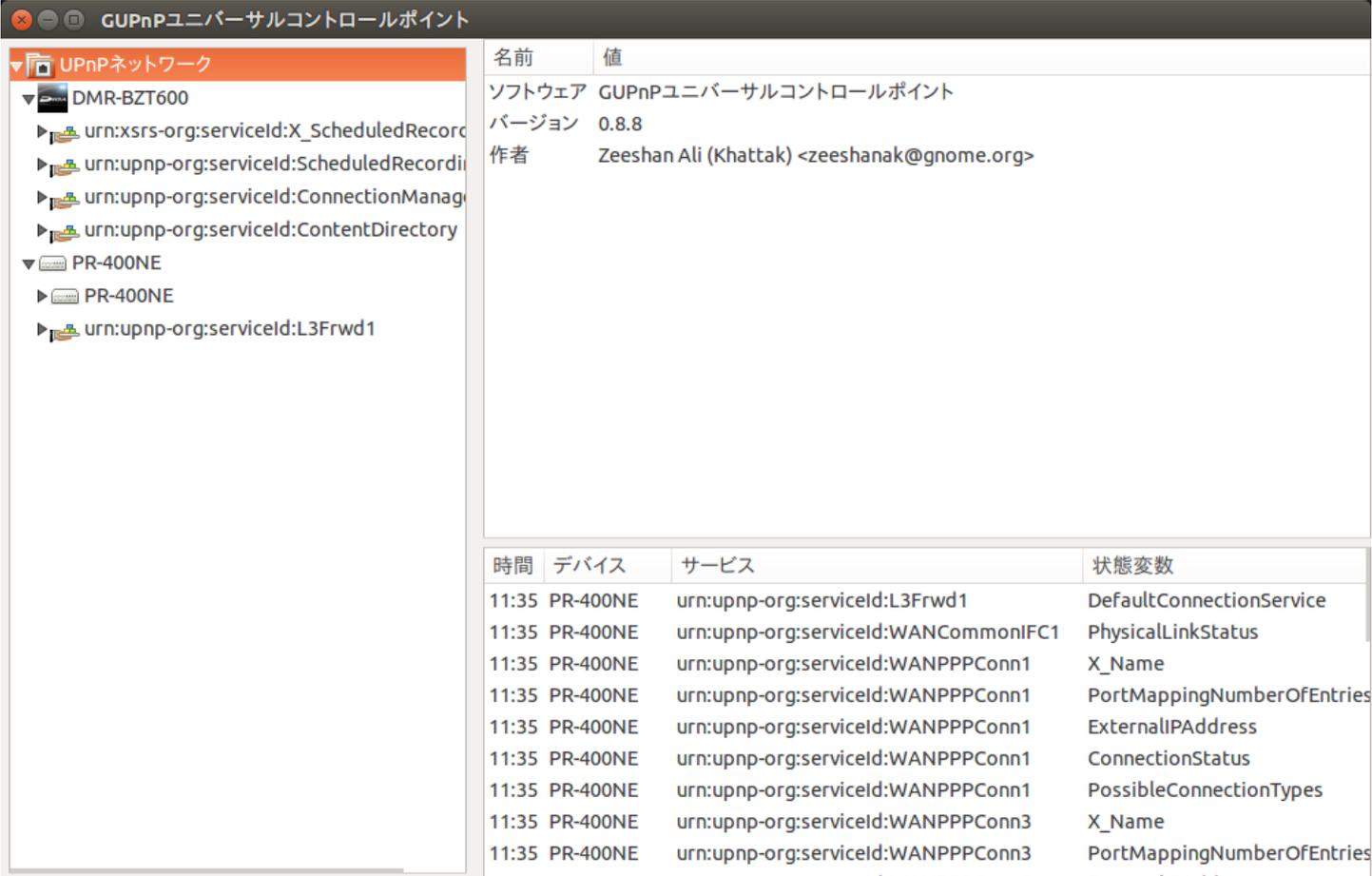
ブリッジ設定

PPPoEブリッジ	<input checked="" type="checkbox"/> 使用する
PPPoEブリッジ自動切断	<input type="checkbox"/> 使用する
PPPoEブリッジ自動切断するまでの時間(秒)	1800

UPnP設定

UPnP設定	<input type="checkbox"/> 使用する
--------	-------------------------------

3(続き) gupnp-univarsal-cpの表示例



The screenshot displays the GUPnP Universal Control Point interface. The left pane shows a tree view of UPnP networks, with 'UPnPネットワーク' expanded to show several devices and services. The right pane shows the details for the selected device, including its name, version, and author. Below this, a table lists the state variables for various services.

名前	値
ソフトウェア	GUPnPユニバーサルコントロールポイント
バージョン	0.8.8
作者	Zeeshan Ali (Khattak) <zeeshanak@gnome.org>

時間	デバイス	サービス	状態変数
11:35	PR-400NE	urn:upnp-org:serviceId:L3Frwd1	DefaultConnectionService
11:35	PR-400NE	urn:upnp-org:serviceId:WANCommonIFC1	PhysicalLinkStatus
11:35	PR-400NE	urn:upnp-org:serviceId:WANPPPConn1	X_Name
11:35	PR-400NE	urn:upnp-org:serviceId:WANPPPConn1	PortMappingNumberOfEntries
11:35	PR-400NE	urn:upnp-org:serviceId:WANPPPConn1	ExternalIPAddress
11:35	PR-400NE	urn:upnp-org:serviceId:WANPPPConn1	ConnectionStatus
11:35	PR-400NE	urn:upnp-org:serviceId:WANPPPConn1	PossibleConnectionTypes
11:35	PR-400NE	urn:upnp-org:serviceId:WANPPPConn3	X_Name
11:35	PR-400NE	urn:upnp-org:serviceId:WANPPPConn3	PortMappingNumberOfEntries

4. 自宅(自社)LAN内でポートスキャン

- 会社の場合は許可が必要(定番nmap[4]使用)

製品	MAC	OS	応答TCPポート	IPv6対応
Pana TV	Matsushita	Linux 2.6.32-3.2	なし	あり
備考: アナログチューナー付きの年式、ファームウェア自動更新				
Pana Video	Panasonic AVC	Linux 2.6.12- 14	多数	なし
備考: 著作権保護コピー回数制限前の年式、ファームウェア自動更新				
PR-400NE	NEC ...	検出出来ず	多数	あり
備考: NTTレンタルホームゲートウェイ、ファームウェア自動更新 アプリケーション応答からNetBSD/1.6.1				
HS2CRC2	Maspro Denkoh	Linux 2.6.15-24	3つ	なし
マsproカメラ、ファームウェア手動更新				
WFS-SR01	I-0 Data...	Linux2.6.13-32	多数	あり
ポケドラ、ファームウェア手動更新				

4. (続き) 気になった点

- Panasonic Video (DMR-BZT600)
 - 1900/udp open|filtered upnp (録画予約等)
- PR-400NE (LAN側)
 - 23/tcp open telnet Pocket CMD telnetd 認証
通過後、すぐ切れるので実害なし
 - 139/tcp open netbios-ssn?, 445/tcp open
netbios-ssn?, メモリカードを差せば使えるファイル共有
機能
 - Workgroup: WORKGROUP

4. WFS-SR01(ポケドラ)

• 対策前[5]

ポート	説明

Wifi(AP) -- 本体裏にSSID、パスワードのシール有り(製品毎に異なる)	
23/tcp telnet Busybox telnetd	☆対策前
80,81/tcp	ユーザ・インタフェース(Webサーバ)
139,445/tcp	ファイル共有 (Samba)
5880/tcp open tcpwrapped	調査中

有線側(100BASE-TX)	
23/tcp open telnet	☆対策前
NASLite-SMB/Sveasoft Alchemy firmware telnetd	
139,445, 5880/tcp	Wifiと同様

問題点:

有線側から23/tcpのtelnetdでloginできてコマンド操作できること。

ルータ機能はおまけ程度、直接インターネット接続の利用は想定外。
ホテルのLAN等や会社のLAN等で他の客からloginされ、マルウェアを仕込まれる危険がある。

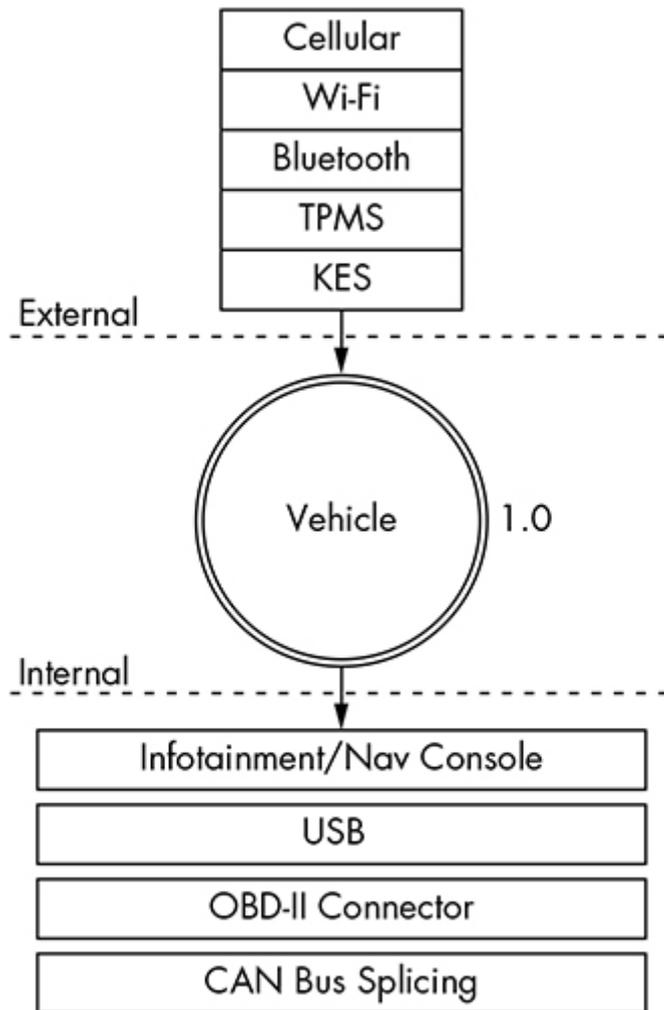
4. (続き) 対策後

- telnetは使えなくなった
 - コマンドを実行される危険はない
 - (ssh loginできると嬉しいのだが)
- WiFi側からしかWeb GUIが使えなくなった
- (改善なし) rootアカウントとパスワードでWeb画面にlogin可
 - パスワードはファームウェアの中のLinux用パスワードハッシュからJohn the ripperで数日(総当りでしょう)
 - 結果はyyyymmddらしき8桁の数字
 - WiFi認証キーは本体ウラ面にあるので、それを読まれたら不正利用される危険は残る

5. 自動車の話題を少し

- <http://opengarages.org/handbook/> [6]
 - 素人にわかりやすい本、ただしITの知識は必要
 - オンライン版は無料、日本語訳の本は3,500円
 - 日本語の概要
<https://gigazine.net/news/20180210-car-haker-handbook/>
- 車にはCAN(Controller Area Network) Busがある
 - 物理的接続 (診断用ポート)
 - Busにつながっている機器に欠陥があれば、侵入口に
 - Bluetooth付きの機器からBusにアクセスできると危険

5. (続き) 説明図[6]



Cellular: 携帯電話システム
TPMS: タイヤ空気圧管理システム
KES: リモコンキー
OBD-II: コネクタ規格名
CAN Bus Splicing: CAN Bus接続

Figure 1-1: Level 0 inputs

5. (続き)

- CAN Bus を使う市販機器[7]
 - USBアダプタ
 - 後付リモコン
 - 後付車速でドアロック
 -
 -
 -
 -

車速ドアロックシステム 車両の走

車両 OBD II コネクターにカプラーオンで簡単取り付け

OBD II
簡単取付

- OBD II コネクター付ハーネス採用で、見た目すっきりな取付けが可能。足元で邪魔になることもありません。
- 消費電流をおさえた省エネ設計。
- エンジンスターター装着車にも取り付け可能。

3年保証

SDL-CT01

JANコード
4950094061332

SDL-CT02

JANコード
4950094061349

¥ 13,500 (税別)

取付・取扱説明書

コネクター形状の確認



- CAN BusにPCを繋げばある程度操作可能

5. (続き2)

- 報告された危険
 - ほとんどは実験用回路か自分の車での実験結果
- ドアを開けられたら、診断用ポートで操作可能
 - プリウスの窃盗手口はこれかも
- ドアを開けずにクラック
 - Bluetooth機器、カーナビゲーション等の欠陥
 - 車の床等やエンジンルームで接続?
 - プロ用大出力機器でCAN Busに接続?

6. おわりに

1. まずパスワード変更、外から見える可能性を意識
2. ルータでuPnPを無効
 1. WAN側で有効な機器は欠陥品
 2. default無効で出荷してほしい
 3. ポート転送設定は手動がお薦め(やや難)
3. ポートスキャンでネットワークサービスをチェック
4. ファームウェア更新できなくなった機器は捨てる

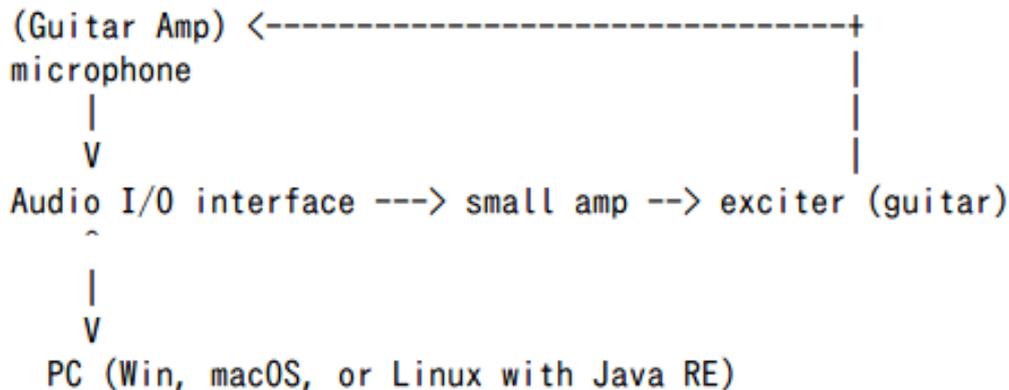
おまけ(自作プログラム紹介)

- <https://goto920.github.io/>
- 新作はJavaScript (Node.js, React)
 - PC、スマートフォン兼用
 - Web Audio API (waaclockモジュール)で正確な時間管理
 - iOS対応に3点注意(キャッシュ、オーディオ、カーソル)
 - 作品1: メトロノーム (自分用、プログラミング練習)
 - ドラマー向け高機能
 - 実ドラム音源で本一冊分のビートパターン収録
 - オフライン利用可能
 - 作品2: 発表用タイマ(自分の授業用)
 - 予鈴、本鈴、セッション終了(色々な音が出せる)

おまけ (続き) Java旧作

- Win10, macOSでも結構使えると思うが、Java REインストール作業のハードルが高い？

1. [ConvertToWave16App.jar](#) Extract wav audio file from various video format file
 2. [TimePitchPlayerApp.jar](#) Time Pitch variable audio player (wav)
 3. [FilteredPlayerApp.jar](#) Making karaoke, drum sound suppressed audio track (wav) using percussive/harm
 4. [FeedbackBoosterApp2.jar](#) Feedback booster for electric guitar (work in progress). Equipments
-



Note: You may omit guitar amp and microphone if effector aux output is fed into Audio I/O interface.

参考文献

- [1] Insecam, "Network live IP video cameras directory," <https://www.insecam.org/> (accessed Apr. 2018).
- [2] Sonet, "ネット機器(IoT機器)が危ない -- 家庭で必須のセキュリティ対策," https://www.so-net.ne.jp/security/news/newsttopics_201611.html (Nov. 2016).
- [3] Gibson Research, "Welcome to ShiledsUp, " <https://www.grc.com/x/ne.dll?bh0bkyd2> (accessed Apr. 2018).
- [4] Nmap.org, "Nmap Security Scanner," <https://nmap.org/> (accessed Apr. 2018).
- [5] I-O Data, "Wi-Fiストレージ「WFS-SR01」セキュリティの脆弱性につきまして," <http://www.iodata.jp/support/information/2016/wfs-sr01/> (Nov. 22, 2016).
- [6] OpenGarages, "Car Hacker's Handbook," <http://opengarages.org/handbook/> (accessed Apr. 2018).
- [7] フジ電気工業(株), "車速ドアロックシステム," <http://www.fuji-denki.co.jp/sdlct/sdlct.htm> (accessed Apr. 2018).
- [8] Goto, K., "KG's App Demos," <https://goto920.github.io/>.