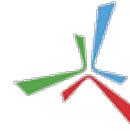




公益財団法人
ひろしま産業振興機構



3つのひかり 未来をつくる
広島市立大学
Hiroshima City University

Smart Factory推進Mgr養成 e-Learningコース

IoTシステムのセキュリティ
～自動車を中心として～

2019/02/28

広島市立大学大学院
情報科学研究科
井上 博之

目次

- IoTシステムの脅威事例
- IoTシステムとしてのコネクティッドカーの情報セキュリティと攻撃事例
- Blackhat USA / DEF CON にみるIoTセキュリティ
- IoTシステムの脅威の現状と開発ガイドライン
- まとめ

IoTシステムの脅威事例

つながるIoT機器のセキュリティモデル

情報セキュリティには、
幅広い知識が必要：

ハードウェア、OS、
通信プロトコル、サーバ、
ソフトウェア、…

Webアクセス
telnet/sshを通じた
不正アクセス

JTAG,UART等の
デバッグポートを
通じた不正アクセス

ファームウェアの入替、
botプログラムの
インストール

IoT機器

ファーム
ウェア

設定

IoT機器

…

OTA
盗聴、
なりすまし

Wi-Fi
3G/LTE

クラウドサービス
クラウドストレージ

不正アクセス、
なりすまし

マルウェアによる工場の生産設備の破壊

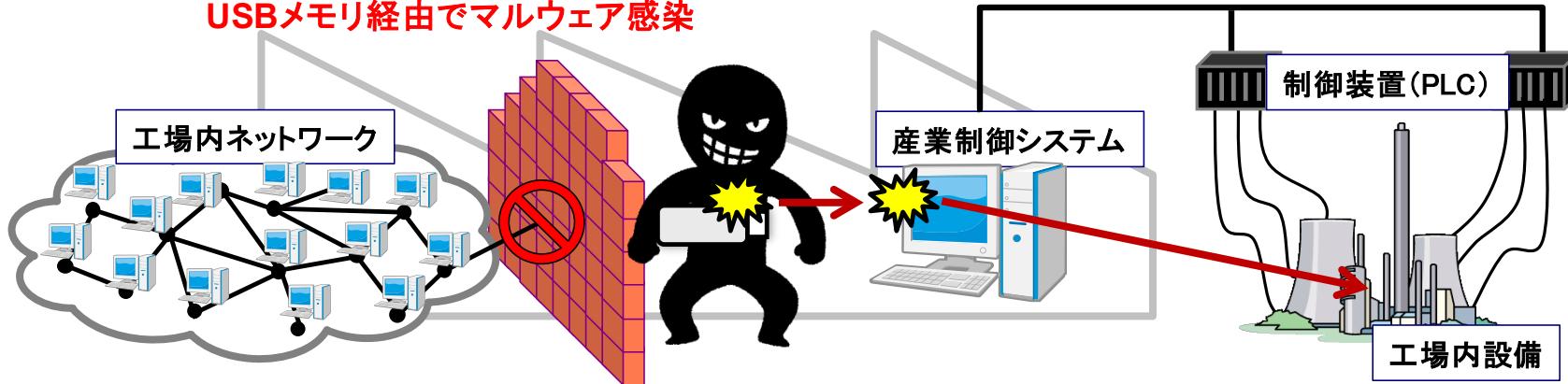
2010年 イランで起こった事件

ターゲット 産業制御システム

概要

- ネットワークから隔離されている産業制御システムにUSBメモリ・持ち込みPCを経由してマルウェアが侵入。不正な命令が実行された結果、工場の設備は大規模に破壊された。
- マルウェアには電動機の回転数制御用インバータの周波数を変更して、回転数を不正に操作する機能が備わっていた。また目立たないよう、他の機能は攻撃しない仕様になっていた。
- マルウェアは未知の複数の脆弱性を突いたものであり、完全な防御は困難であったと指摘されている。

手順1：ネットワークから隔離されたシステムに
USBメモリ経由でマルウェア感染



手順2：不正な命令で特定の設備を破壊

Stuxnet の脅威と今後のサイバー戦の様相(検証論文)

<http://www.bsk-z.or.jp/kenkyucenter/pdf/23kennshouronnbunnijyushousakuhinn.pdf>

ATMのハッキング

2014年 北米で起こった事件

ターゲット ATM

概要

- 14歳の少年2人が、インターネット上で発見したマニュアルを基にATMの管理モードに侵入することに成功。表示画面のメッセージを書き換えた。
- ログイン用のパスワードが初期設定のままだった。
- Symantecは、携帯メールを送信するだけでATMから現金を引き出せるマルウェアが出回っていると警鐘。研究室で実際のATMにPloutusを感染させて、攻撃を再現できたとのこと。

手順1: ATMの外装を外し、内部ユニットにスマホをUSB接続し、ATMにウィルスを感染させる。スマホを繋げたまま外装をもとに戻す。



手順2: 別のスマホで、ATM内に隠されたスマホにSMSを送ると、ウィルスに指示、現金を払い出させる

14歳の少年2人がATMをハッキング(記事)

<http://www.edmontonsun.com/2014/06/09/14-year-olds-hack-bmo-bank-machine-staff-doesnt-believe-them>

スマートフォンでATMをハッキング(記事) <http://www.itmedia.co.jp/enterprise/articles/1403/26/news037.html>

PLC および CX-Programmer に複数の脆弱性

2015年10月 日本で発見された

概要

- オムロン製プログラマブルロジックコントローラ(以降 PLC) および CX-Programmer に複数の脆弱性が発見された

(詳細情報)

- オムロンが提供する PLC 製品 CJ2 シリーズおよび、PLC や HMI の設定やプログラムを行うためのソフトウェア CX-Programmer には、次に挙げる脆弱性が存在する
 - パスワードが平文で送信される脆弱性
 - CX-Programmer 用プロジェクトファイルからパスワードを取り出せる脆弱性
 - コンパクトフラッシュカードに保存されるオブジェクトファイルからパスワードを取り出せる脆弱性

(想定される影響)

- 遠隔の第三者によってパケットを盗聴された場合、平文で送信されるパスワードを取得される可能性がある
- システムのファイルシステムにアクセスできる攻撃者にパスワードを取得される恐れがある

ネットワークビデオレコーダーに複数の脆弱性

2016年1月 韓国で発見された

概要

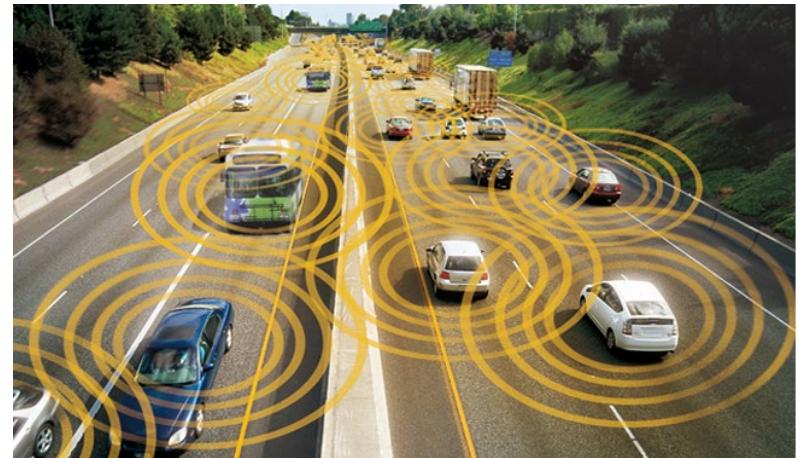
- Samsung が提供するネットワークビデオレコーダー SRN-1670D にて、複数の脆弱性が存在することが確認された

(詳細情報)

- 認可・権限・アクセス制御の問題
 - 説明書に記載されていない URL にアクセスすることで、システム内の任意のファイルを取得することができる
- 情報漏えい
 - エラーメッセージに必要以上の情報が含まれているため、攻撃者はエラーメッセージから有効なユーザ名などを特定することができる
- 不完全またはリスクーなアルゴリズムの使用
 - ファームウェアのファイルシステムは、単純な XOR をもとにした独自の暗号化スキームを使用しており、容易に解読可能

(想定される影響)

- 遠隔の攻撃者によって、機器内の任意のファイルを取得されたり、有効なユーザ名を特定される可能性がある



IoTシステムとしてのコネクティッドカーの 情報セキュリティと攻撃事例

コネクティッドカーの情報セキュリティ

■ 自動車に高機能な機器や多様なサービスが備わる

例: 高機能力ーナビ

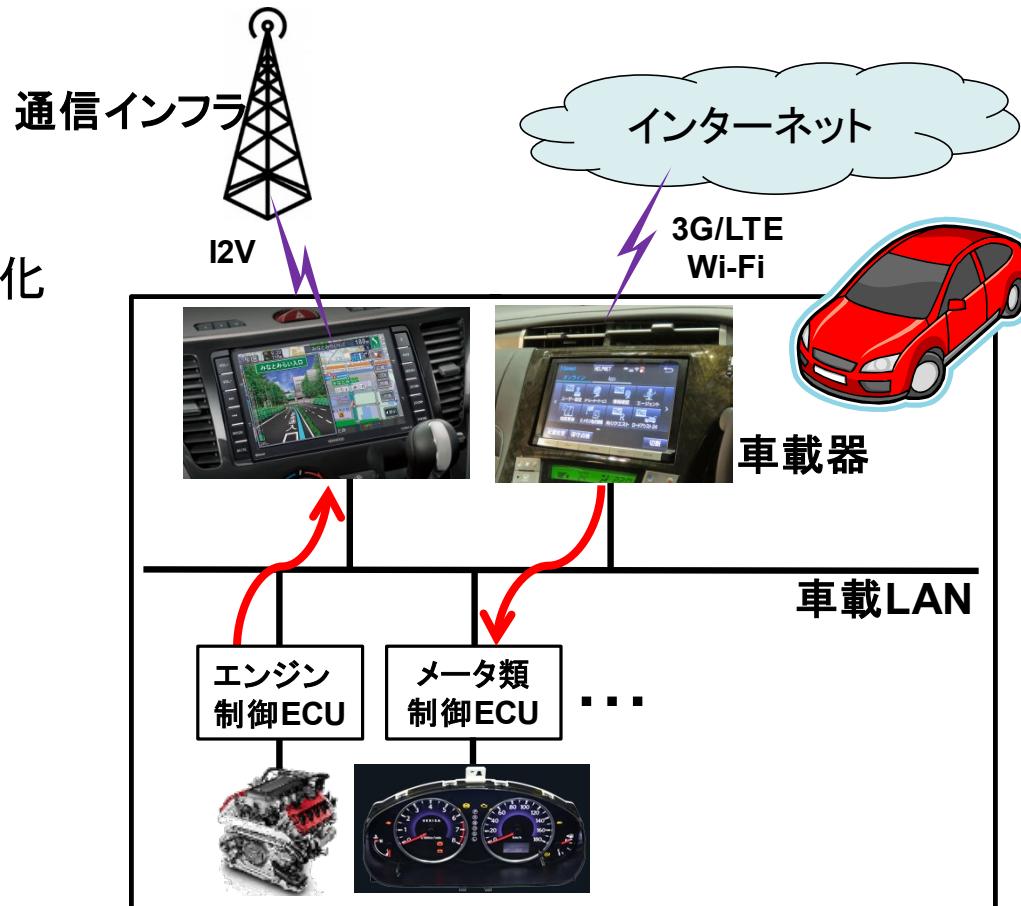
テレマティクス機器など

□ 広域ネットワークと通信

- ◆ データ通信網の高速化、低価格化
- ◆ 路車間、車々間通信
- ◆ クラウドサービスの導入

□ 車載LANに接続

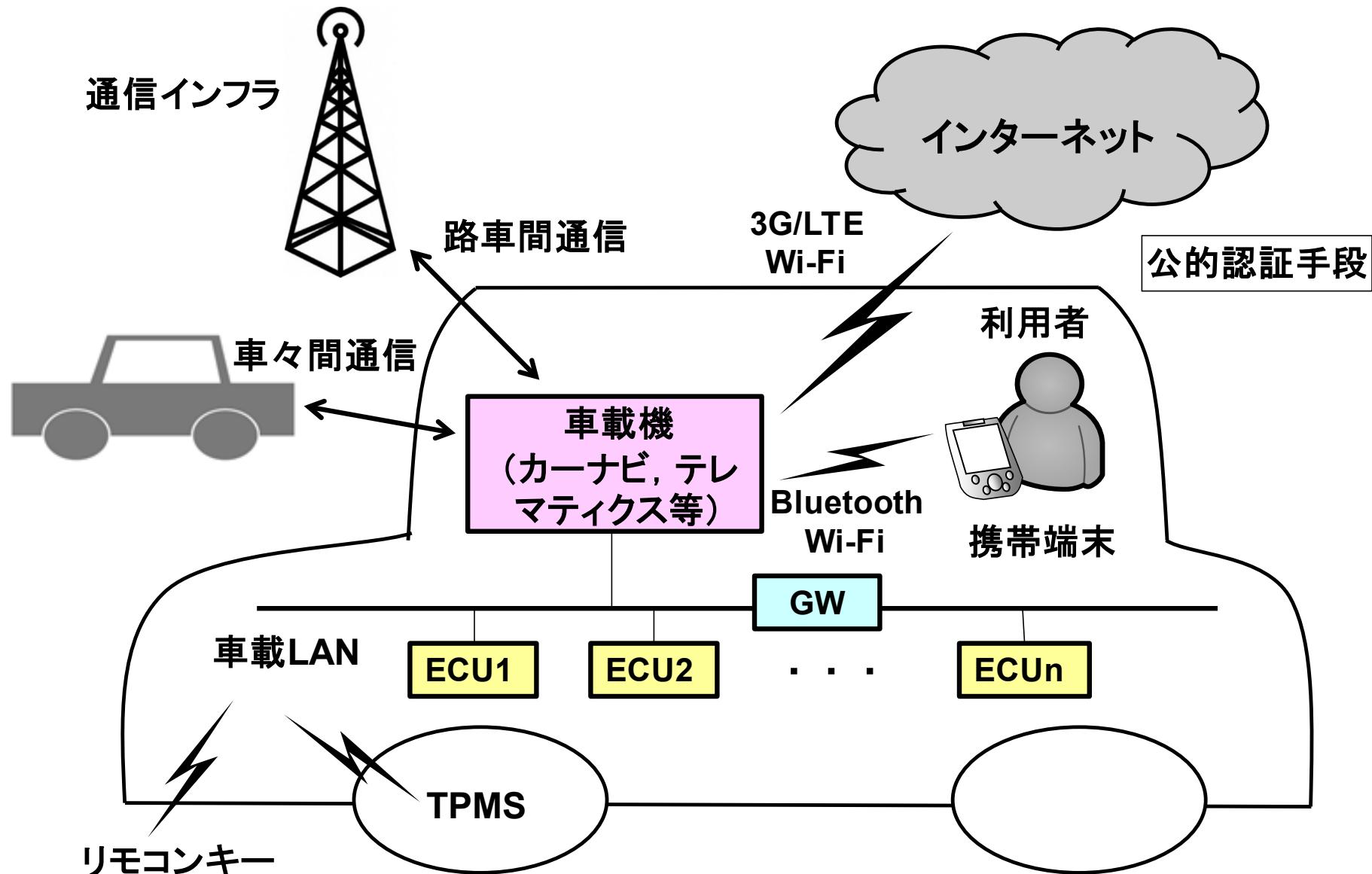
- ◆ ECU(電子制御ユニット)から送信されるメッセージを利用
- ◆ 特定の動作をさせるメッセージをECUに送信



■ 自動運転

□ 大量の車載センサと遠隔からの運転支援により実現

つながるクルマのセキュリティモデル(例)



車載LANの通信プロトコルとCAN

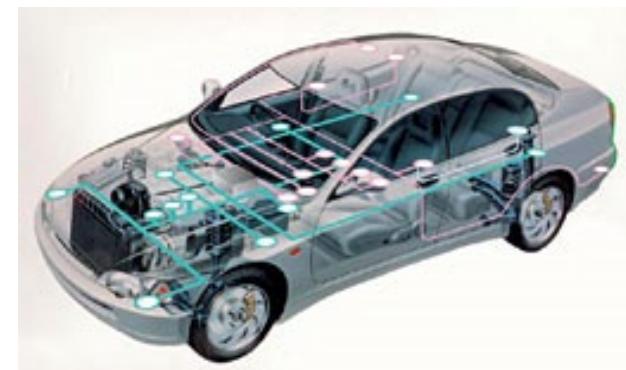
■ 車の中にネットワークとECUの高機能化、複雑化

- 数十～100個以上の**ECU**(電子制御ユニット)
- 燃費対策、アクティブコントロール(ブレーキ、ハンドル)
- 様々なサービスに対応するため(IoT)

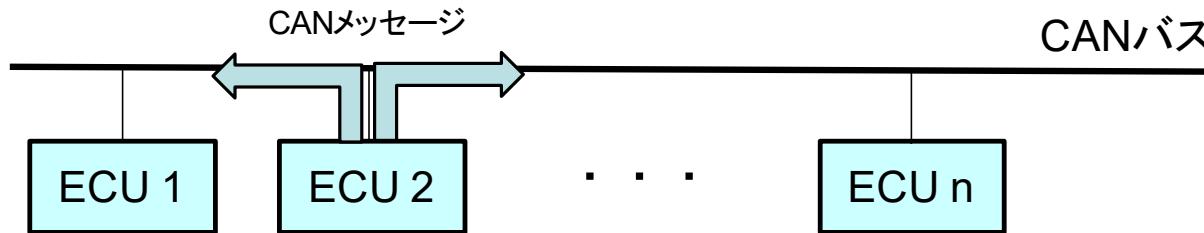
■ ネットワーク(車載LAN)ではCAN, LIN, FlexRay, MOSTなどのプロトコルが使用されている

- CAN, LIN以外は余り使用されていない
- 車載Ethernetも、高級車のインフォテインメント系に搭載されつつある

■ 最も利用されているのは**CAN** (Controller Area Network)



CANプロトコルの特徴と問題点



CANの特徴

- | | |
|--|--------------------|
| <input type="checkbox"/> ペイロードが小さい | 最大8byte |
| <input type="checkbox"/> ソースアドレスがない | 宛先アドレス(CAN ID)しかない |
| <input type="checkbox"/> 共有バスである | 通信が丸見え、他から注入も可能 |
| <input type="checkbox"/> 認証や暗号化の仕組みがない | |
| <input type="checkbox"/> 通信速度が低い | 500kbps(0.5Mbps) |

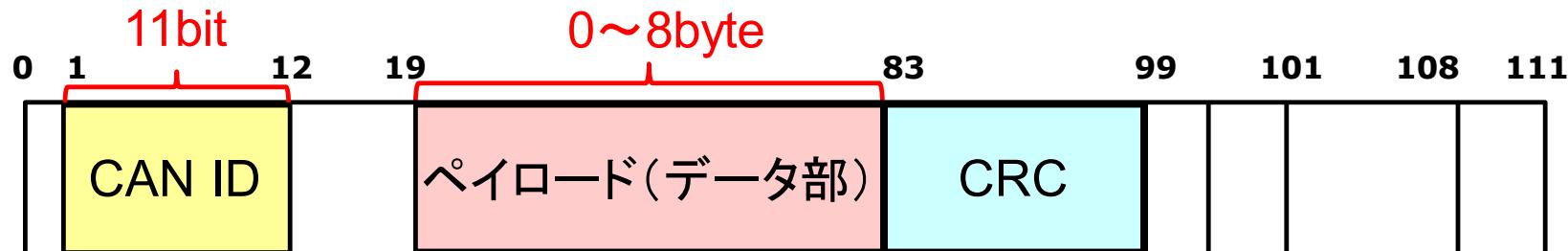


CANはプロトコル上、盗聴、なりすまし、DoS攻撃に本質的に弱い

解析するほうからみると、簡単にわかる(全部見えるし、暗号化もされていない)

CAN ID(送信先アドレス)とペイロード

- CANのメッセージフォーマット(フレームフォーマット)
 - 11ビットのID、8byteのペイロード、その他制御用の数ビット合わせて最大110ビット程度のメッセージ



- IDを使用したメッセージ・アドレッシング
 - 送信元アドレスを持たない
 - ※ 29bit IDのCAN規格もある
 - データの内容に対応する11bitのIDを使用する
 - ノードはIDによって自身が受信すべきかを判別
 - IDにより受信先のECUが決まり、ペイロードの内容と合わせて、その機能が決まる

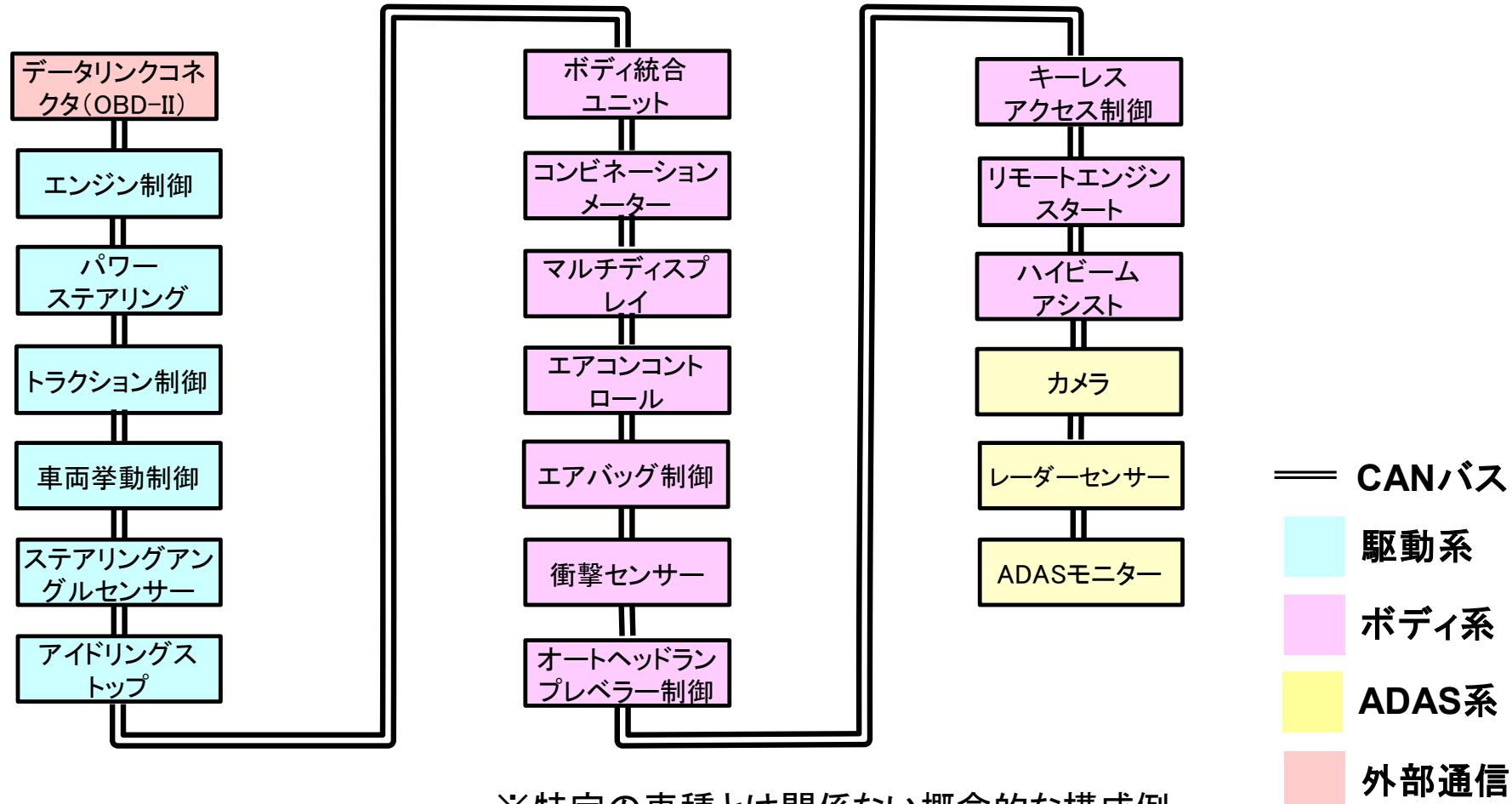
CANとOBD-IIインターフェース

- OBDとは車載コンピュータが行う自己故障診断のこと
 - On-Board Diagnostics
- **OBD-II端子**から、CANバス経由で車内のECUに接続して診断やソフト更新を行うことが可能
 - 車の運転手席の足下周辺にある
 - 車の中にはCANのバスが複数存在することもあり、ゲートウェイを介して接続されている
 - ゲートウェイがない車種は、解析やメッセージ注入が容易
- OBD-II端子を介して、USB接続のCANアダプタ等でCANバスに接続し、**CANメッセージ(パケット)の送受信**を行うことができる



実際の車両のECUの構成例

- 公開情報(ディーラーで販売している車両整備書)の回路図を分析することで、ECUの機能や種類、構成が得られる



※特定の車種とは関係ない概念的な構成例

自動車に対するサイバー攻撃報告の例

Prof. Kohno,
Washington Univ.

車載LANやECU、カーステレオなどに対する
攻撃可能性の論文を
発表

TOYOTA Prius, Jeep Escape
Hacking (DEFCON 2013)

車載ネットワークに直接接続し、
ブレーキなど制御・操作

<https://www.sankei.com/wired/photos/160926/wir1609260002-p1.html>



Tesla Hacking (BlackHat2017)

WiFi経由で侵入し、
遠隔で制御・操作

2016

2017

Jeep Hacking (BlackHat2015)

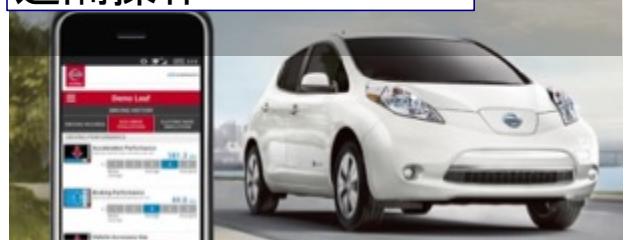
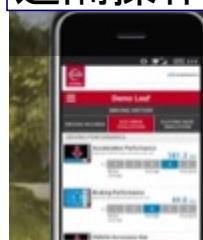
インターネット経由で侵入し、遠隔から制御・操作



<https://www.youtube.com/watch?v=x5ThLMOjoUk>

Nissan LEAF

APIの脆弱性をつき、
遠隔操作



<https://www.troyhunt.com/controlling-vehicle-features-of-nissan/>

ADAS機能を備えた自動車に対する解析の実際

- 自動ブレーキ、全車速追従型オートクルーズ付きの車両
- 2週間程度で解析 & 注入メッセージ作成
 - CANアナライザVspy3を使用
 - CANメッセージ解析
 - ◆ リプレイアタック
 - メッセージ注入によるなりすまし
- 成功した干渉シナリオ
 - 自動ブレーキの強制動作
 - 自動ブレーキの妨害
 - オートクルーズをONにして加速
 - さらに、パーキングブレーキの自動解除
 - 前車追従で停止状態からの発進
- さらに、小型装置へプログラミング
 - ◆ Arduinoベース 約9千円



自動車に対する攻撃事例(初期)

- ワシントン大学 Kohno先生らによる報告(論文)
 - Experimental Security Analysis of a Modern Automobile (2010)
 - Comprehensive Experimental Analyses of Automotive Attack Surfaces (2011)
- 物理インターフェースへのアクセス
 - OBD-II
 - エンターテイメント(ディスク, USB, iPod)
- 近距離無線によるアクセス
 - Bluetooth
 - キーレスエントリ
 - TPMS(タイヤ空気圧モニタリングシステム)
 - RFIDキー(RFIDベースのイモビライザー)
- 長距離無線によるアクセス
 - 携帯電話通信網

DEFCON 21(2013)

- Charlie Miller, Chris Valasekによる
 - Adventures in Automotive Networks and Control Units (2013) …文献1
- OBD-IIポートにCANバスアダプタを接続
 - Ford Escape, Toyota Prius
 - スピードメーター、ブレーキ、アクセル、ハンドルなどの情報のなりすまし
 - 外からのドアロック解除や、ハンドル操作支援機能の乗っ取りなど



※ 文献1より引用

DEFCON23: Remote Exploitation of an Unaltered Passenger Vehicle

21

■ 5つの穴(セキュリティホール)がつながることで大きな脆弱性に

1. 車内無線LANサービスからポートスキャンできる状態だった
そこで、6667/TCPが見えるようになっていた
 2. 6667番ポートにて、コマンド受け付け可能になっており、
パスワードなしで認証できる状態だった
 3. WAN側インターフェース(インターネット側)も同様に6667/TCPが受付可能であった
 4. プロバイダ(Sprint)も6667番ポートをフィルタリングしていなかった(キャリアとしては一般的)
 5. 6667経由で侵入したユニットから、CANバスにつながるV850 CPUのファームウェアを書き換え
可能であった
- そして、Jeepは携帯電話網経由で自由に操作できるようになった
- 公開の少し前に、JeepはECUのファームウェアを
リコールし、ISPIはTCPの6667番をアクセス制限した



■ Jeep問題のまとめ

- 何も機器を追加していない車に対して、遠隔から干渉できた
 - ◆ 機器をつないでの干渉は、2011年や2013年に報告済
– 技術的には、さほど難しくない内容
- 車内のインターネット接続サービスや、車載LAN上のECU、インターネットプロバイダなどに穴(脆弱性)があり、そこを狙われた
 - ◆ 今回の件の公開前に、自動車メーカーとプロバイダは対策済み

そして翌年は(BlackHat2016)

- Advanced CAN Injection Techniques for Vehicle Networks
 - フェイルセーフの基準としているセンサデータをだますことで(該当ECUを保守モードにして機能停止させて)、アクセル、ブレーキ、ハンドルを操作可能に

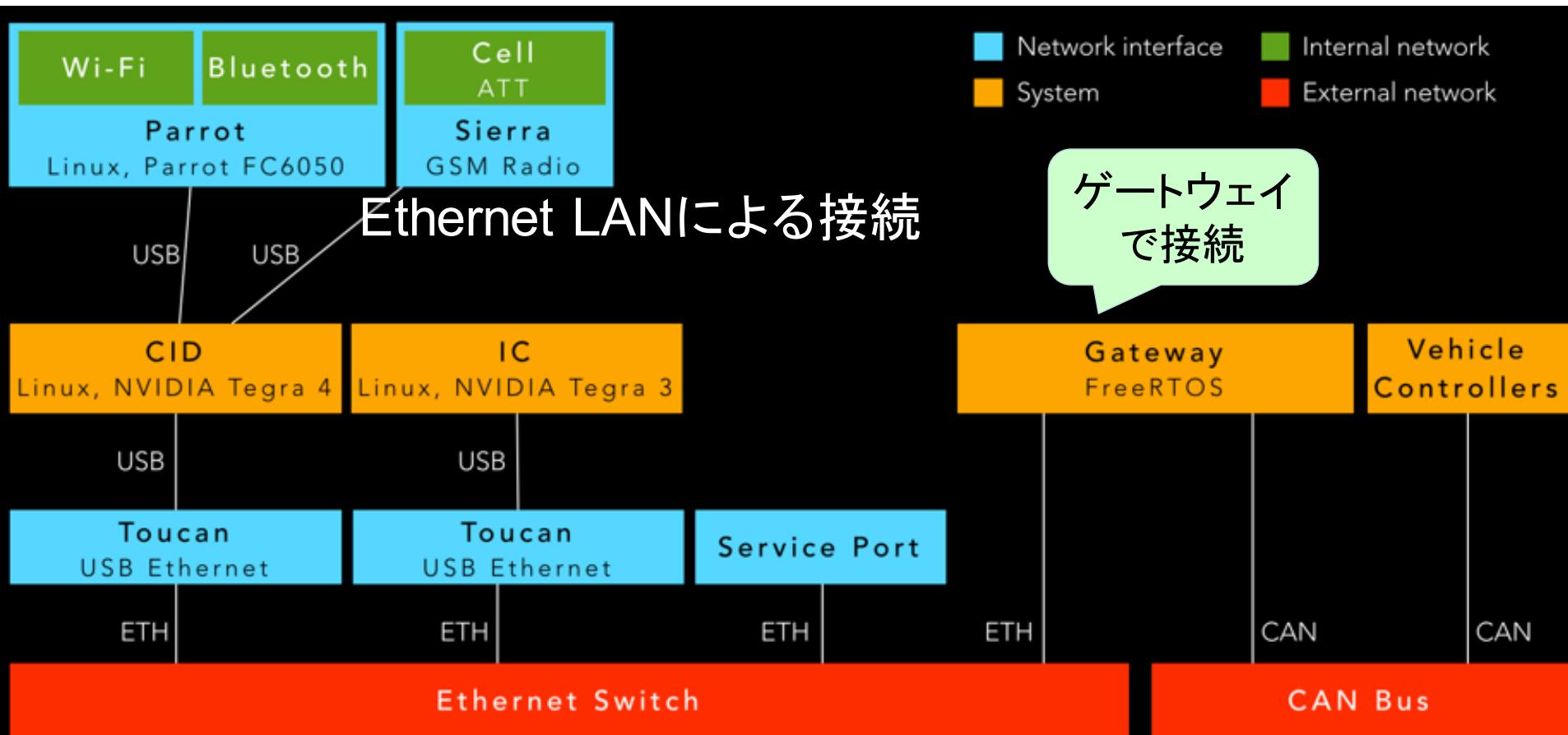
(BlackHat2015) (BlackHat2016)

	2009 Chevy Malibu	2012 Ford Escape	2012 Toyota Prius	2014 Jeep Cherokee (previous)	2014 Jeep Cherokee (now)
Engage brakes	Yes	< 5mph	Yes	< 5mph	Yes
Stop brakes	Yes	< 5mph	No	< 5mph	< 5mph
Steering	No	< 5mph	Partly	< 5mph	Yes
Acceleration	No	No	No	No	Yes

DEFCON23(2015): Hacking the Tesla Model S and the future of automotive security

23

Tesla Model SのInfotainment系の構成



TCP/IPやLinuxを使った部分

→ Linuxサーバへの攻撃手法の多くが適用可能

従来の制御ネットワーク
(CANベース)

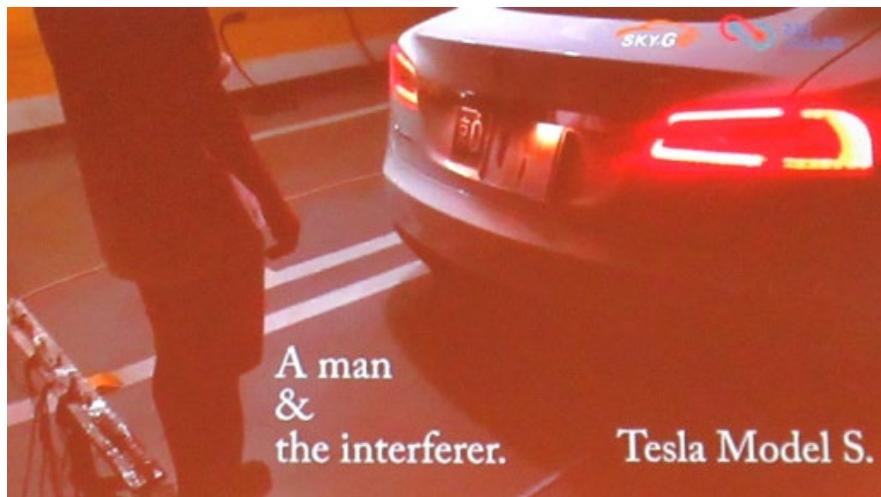
手元のスマートフォンからsshでアクセス



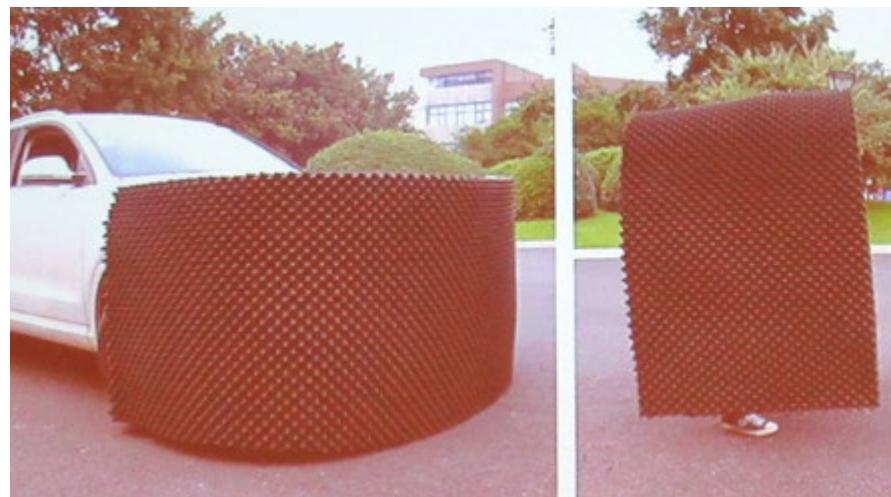
→ トランクドア
(電動)を
遠隔から
開閉

Tesla SのAutopilot / ADAS用センサに対する妨害

1. 超音波センサへのジャミング



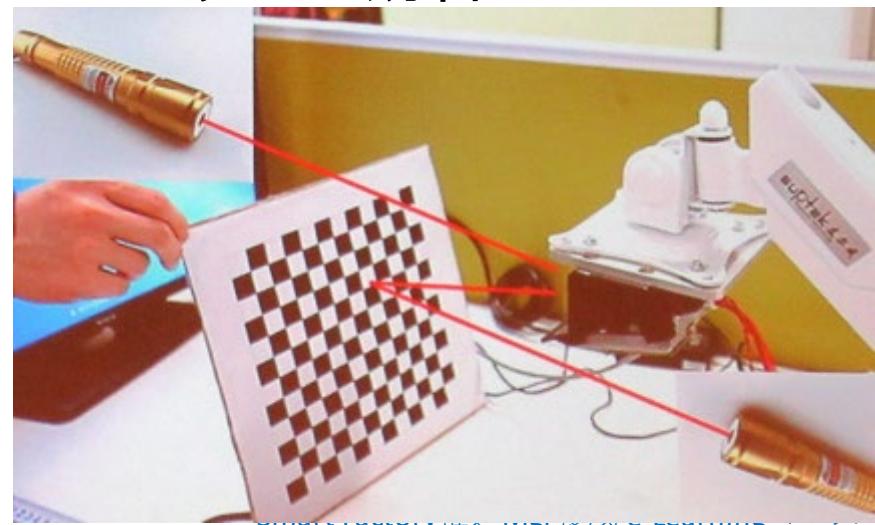
2. 超音波センサへの妨害



3. ミリ波レーダへのジャミング



4. カメラへの妨害



Hacking Tesla from Wireless to CAN Bus

- 中国の研究者からの報告(2016/09の詳細)
- Wi-Fi経由CANバスを経由したなりすまし攻撃
 - メーターパネルへの干渉
 - 電動シートを動かす
 - ワイパー やサンルーフを動かす
 - ブレーキ、ドアロックの操作



現状でのキーレスエントリシステムにおけるRelay Attack

- サイバー攻撃よりも現実的な問題となっており、大きな被害が出ている
→YouTubeで“relay attack car”などで検索すると色々な動画がある
- 鍵からの電波(UHF)と車からの電波(LF)を相互に中継する装置を使う
→単純なアナログ電波のリピータ
 - 家の中にある鍵 ⇄ 駐車場の車
 - ◆ 鍵を持った人が車の前にいると思わせる →解錠
 - ◆ 鍵を持った人が車の中にいると思わせる →エンジンスタート
 - ◆ 逃走し、新しい鍵を作って海外輸出または部品として販売
 - 装置同士は60m以上でも使える
 - ◆ 2cm角のアンテナ。一般的な電波のスキヤナに似ている
 - 保険会社にとって頭の痛い問題に

現実的に盗難被害
が多く出ている方法
まったくサイバ
セキュリティではない

- 対処
 - 物理的な方法
 - ◆ 家の中で、車の鍵を電波シールドされたところに置く
 - アルミパウチされた袋や缶の中でもよい。冷蔵庫や電子レンジには入れない方がよい
 - ◆ 最近の鍵にはOFFスイッチが付いているものもある(電池節約モードなど)
 - ◆ ステアリングロックを併用(実際は、そんな面倒なことはしないと思われる)
 - キーレスエントリシステムの改善
 - ◆ 鍵が自動的にOFFになるようにする(ただし運転中にOFFにならない仕組みが必要)
 - ◆ PINを入れないと有効化されない鍵(passive keyless entryとは呼べなくなるが)
 - ◆ 往復時間を測定してリレーされていることを検出する(光速につき難しい)
 - ◆ UWBを使って、短いパルスで処理する(位置検出を可能にし、リレーされにくくする)
 - ◆ Bluetoothを導入し、ペアリングや暗号化の導入(すると、スマートフォンを鍵にもできる)

■ インフォテインメント系

□ EthernetやLinuxと相性がよい

- ◆ マルチメディア、Wi-Fi/USB/Bluetoothなどの最新のインターフェースや通信プロトコル(TCP/IP, Web, Secure通信)のサポートなどが容易
- ◆ AGL(Automotive Grade Linux)を使ったIVIシステムも発売

■ 脆弱性の報告

□ Linuxを使った統合情報ディスプレイ

- ◆ 特定のボタンの組合わせや長押しなどで、メンテナンスマードに入れる、など
- ◆ Linuxの場合は、rootユーザ(特権ユーザ)になってしまふと、ソフトウェアの入れ替えや、周辺デバイスの任意の操作が可能になつてしまふ

□ Tesla S

- ◆ 走る、曲がる、止まるの部分は従来のCANのネットワーク
- ◆ ナビゲーションを含むインフォテインメントは、Linux+Ethernet

つながる自動車の情報セキュリティ

- ネットにつながる家電や自動車、産業機器にひそむ脆弱性
 - 世界中からのアタックに対する防御策
 - ライフサイクルと、ファームウェア更新の難しさ
- EthernetおよびLinuxベースの増加
 - 従来からのサイバーセキュリティの手法が有効
 - クラウド連携によりサーバ側も対象となる
- 便利なツールや解析ソフトウェアの入手性の向上
 - だれでもリバースエンジニアリングが可能に。よいハッカーと、悪いハッカーの問題
 - 家電製品や自動車のような身近なIoTは対象となりやすい
 - ◆ 利用者への影響も大きく、報道もされやすい

BlackHat USA および DEFCONにみる IoT・自動車セキュリティ

BlackHat USA とは

ビジネス寄り



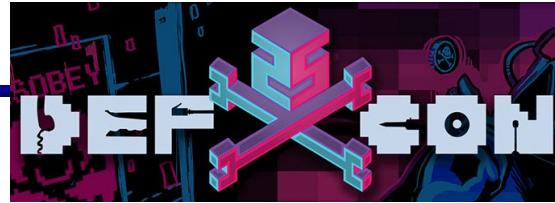
- 会期: 2018年8月8~9日(ブリーフィング)
- 会場: Mandalay Bay Convention Center
- 参加者数: 1.5万人以上、日本から100名以上
 - 主に社会人
- ブリーフィングのカテゴリ
 - カテゴリ: 暗号、HW/組込み、ネットワーク、モバイル、IoT、
生体認証、OS/ホスト、セキュリティ開発ライフサイクル、
防衛策、スマートグリッド/インダストリ、企業、バーチャリゼーション、
探索技術、マルウェア、リバースエンジニアリング、Webアプリ、フォ
レンジックス/インシデントレスポンス、リスクマネージメント/コンプラ
イアンス
- 解析ツール紹介
 - アーセナル
 - ◆ 解析・モニタリングツール(HW、SW様々)の紹介コーナー
 - スポンサーセッション・ワークショップ
 - ◆ セキュリティベンダーのツール紹介や活用ワークショップ

DEF CON とは

かなりカジュアル

■ DEF CON Hacking Conference

- 世界最大のハッキングイベント @ラスベガス
 - ◆ 2018年は8月9～12日 → 2019年は8月8～11日
 - ◆ 2018年が26回目: DEFCON 26
 - ◆ BlackHat USA のイベントに引き続き開催
- 講演、CTF大会、ワークショップ、Village、デモ展示など

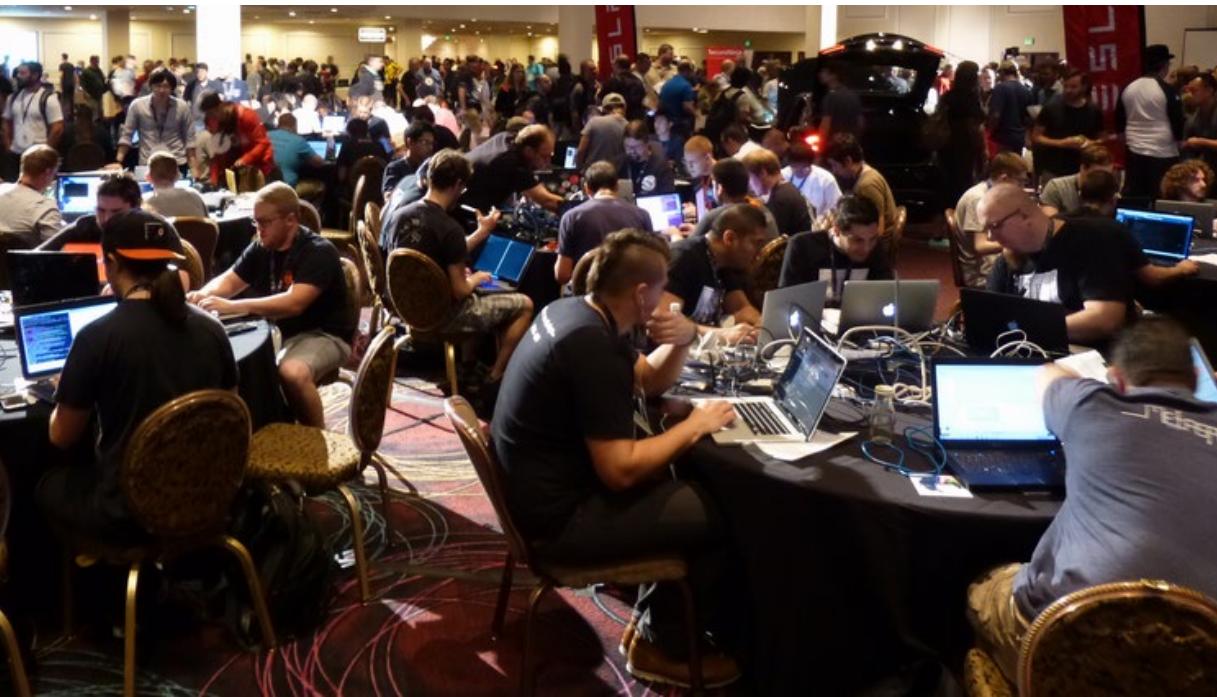


入場者バッジ(2018)



CTF(Capture The Flag; 旗取り大会)

- ファイルやWebサイトに隠されているキーワード(フラグと呼ばれる)を探す
 - 1つ見つけるたびに、そのポイントが加算される
 - 日本でも、SECCON CTFやCTF for Beginners として各地で実施 → <http://2017.seccon.jp/>
 - 世界大会と、その場で開かれるOpenCTFの2つが開催



08-Aug-15 16:42:02 ... SCOREBOARD			
Rank	Team Name	Points	No.
1	0x0f	3410	1
2	neq9	2710	2
3	leldongs	1560	3
4	vulscryptos	1410	4
5	dcua	1160	5
6	knightsec	850	6
7	z3p	850	7
8	rpisec	810	8
9	pr0v3rb3s	710	9
10	badhaxers	650	10
11	shadowcats	610	11
12	team_reddit	560	12
13	atx2000	410	13
14	rubes	310	14
15	tripl3monitors	310	15
16	droidis	260	16
17	NordSlayaz	210	17
18	coshypolitans	210	18
19	ilovedata	160	19
20	SecConFlossy	160	20

即売会

- ハッキングツール、ノベルティ、書籍などをその場で販売



USB接続のWi-Fiアナライザ、SDR解析装置、など
数十ドル程度のツールを販売 →最終日には完売

ワークショップ(講習会)

- ちょっとしたハッキングツールを作ったり、ツールを使って実際にハッキングしたりというワークショップ
- 物理セキュリティ
 - ピッキング
 - シール剥がし(はがした痕が残るテープ)
- ちょっとした電子回路の作成
 - BadUSB
- 車載LANへアクセスして目的のパケットを探す、など



Village (同好の集まり)

- 興味を持った人たちが集まって、ミニ講演会やワークショップや展示などを実施 (BoF→birds of a feather)
- Bio Hacking Village
- **Car Hacking Village**
- Crypto and Privacy Village
- Data Duplication Village
- Hardware Hacking Village
- ICS Village (ICS/SCADA: 産業制御システム)
- Internet of Things (IoT) Village
- Lockpick Village
- Packet Hacking Village
- The Social Engineer Village
- Tamper Evident Village
- Wireless Village (SDR)

2014年から

2015年から



IoT Village

- 2015年に新設
 - ネットワークにつながるコンシューマー製品のセキュリティの向上を目指す
 - ◆ 広い意味でのIoT
 - 前年にICS Villageも新設されており、組込み機器のセキュリティへの関心が大きくなっている

- プрезентーションの例(2016年)
 - Exploiting a Smart Fridge: a Case Study in Kinetic Cyber
 - 冷蔵庫の温度をインターネット経由で変更
 - Picking Bluetooth Low Energy Locks from a Quarter Mile Away
 - Hot Wheels: Hacking Electronic Wheelchairs
 - Live Drone RF Reverse Engineering (WS)
 - 電波とプロトコルを解析し、乗っ取る
 - Thermostat Ransomware (WS)
 - 空調の温度調節機をリプログラミング



IoT Village Hacking Contest

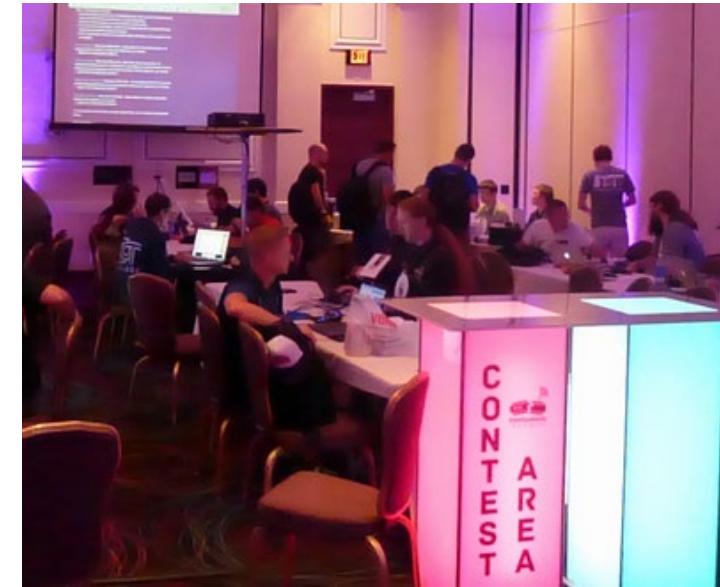
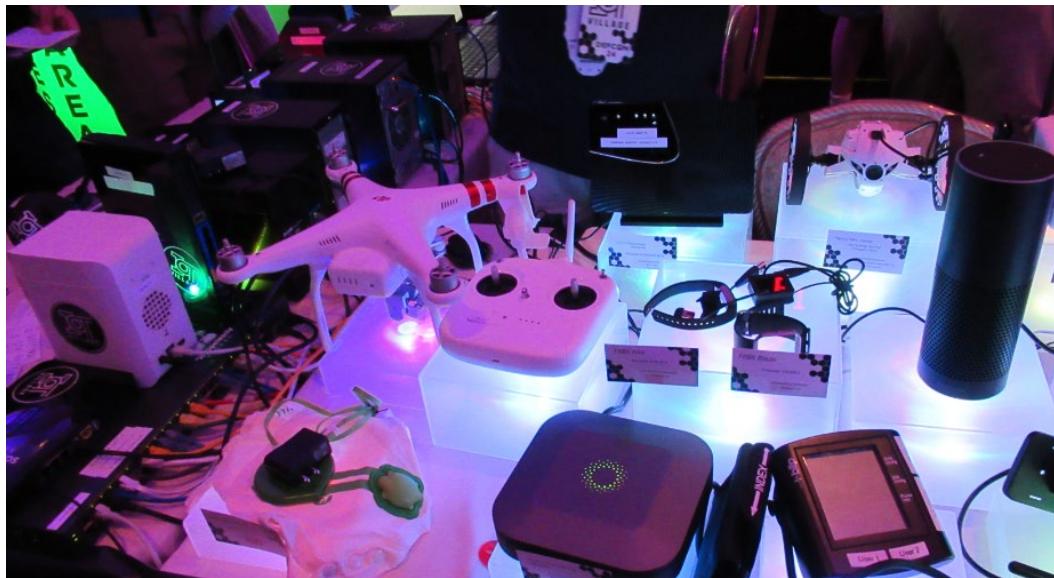
■ ハッキングコンテスト

= ZERO-DAY TRACK =

- ◆ 所有するIoT機器の0-day脆弱性を見つけ
(まだ公知になっていない脆弱性)、それをデモする

= CTF TRACK =

- ◆ 用意された市販の家庭用ルータやIoTデバイスをハックする
- ◆ 内容と数で獲得ポイントが決まる

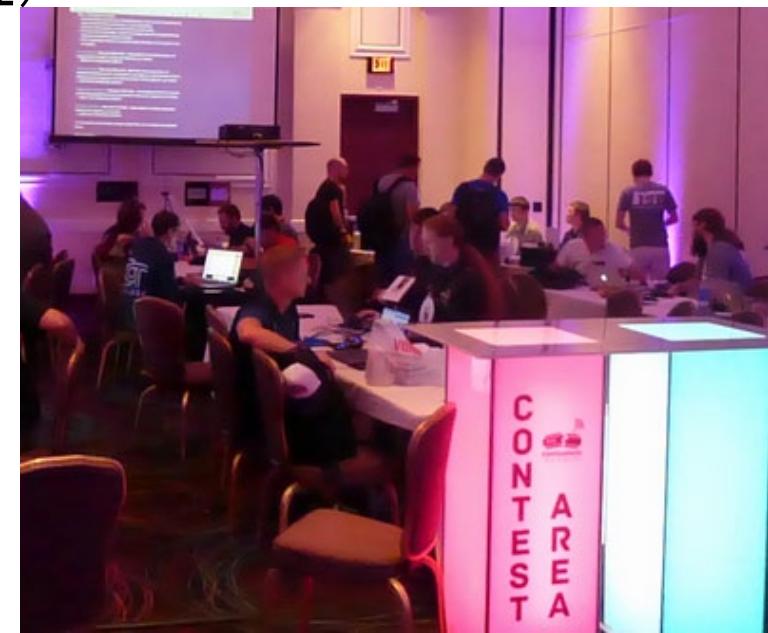


IoT Village: コンテストの例(DEFCON23)

■ ハッキングコンテスト

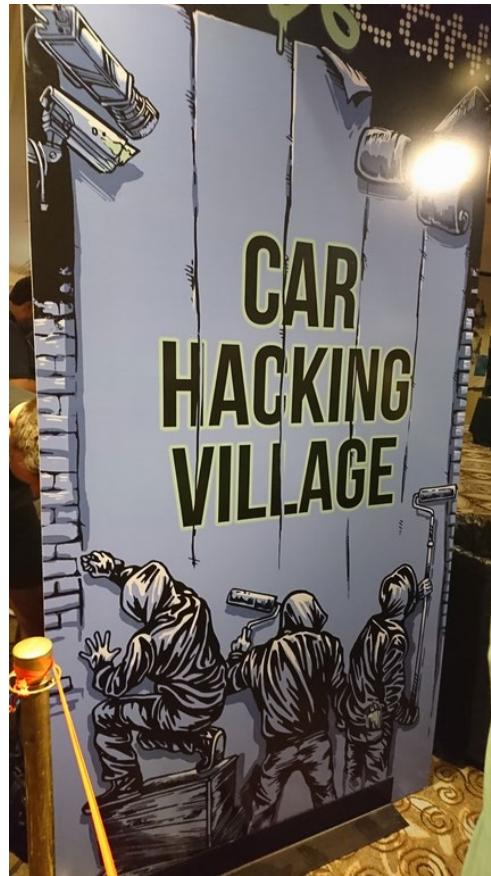
□ コンシューマー製品のハッキング大会(ワークショップ)

- ◆ 家庭用ルータ(ASUS, Zyxel 社)
- ◆ 防犯カメラ(Netgear, Forscam 社)
- ◆ 赤ちゃんモニター(Samsung 社)
- ◆ Wi-Fi対応血圧モニター(Blipcare 社)
- ◆ Wi-Fi対応体重計(Fitbit Araia 社)
- ◆ タイムカード記録装置(ZK Software 社)
- ◆ NAS(Apple社タイムカプセル)
- ◆ ガレージ開閉装置(Chamberlain 社)
- ◆ 電気錠(LockState, Hysoon 社)
- ◆ 冷蔵庫(Samsung 社)
- ◆ おもちゃ(HappyCow社
カメラ付き戦車模型(Wi-Fi接続))
- ◆ 2016年はドローンが追加



DEFCON26: Car Hacking Village

- 自動車セキュリティの関する情報、ツールなど
- 2017年からは CTF大会を開催
 - ECU、ヘッドユニット、車両などを用意
 - 2018年CHV CTFは、1位はNIO、2位はTrillium
 - ◆ コンテストの1つのKaramba Challengeでは日本人が1位であった



Car Hacking Village CTF



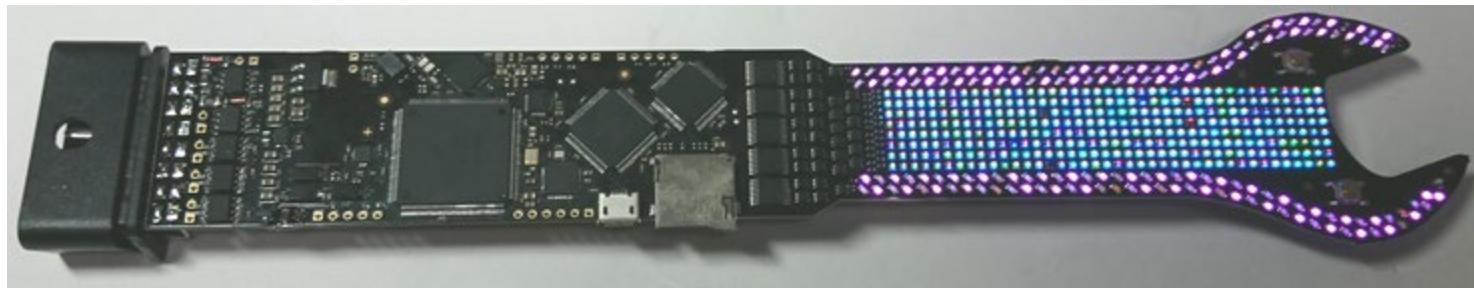
ハックしてみようCTFコンテスト



2017年はマツダ車がCTF対象に →特にハックされず

Badge: Car Hacking Village

- 每年、OBD-II端子につながる電子バッジを販売
 - US\$60~80、初日に行かないと売り切れてしまう
 - SDKを提供、CANバスの解析やメッセージ送信が可能



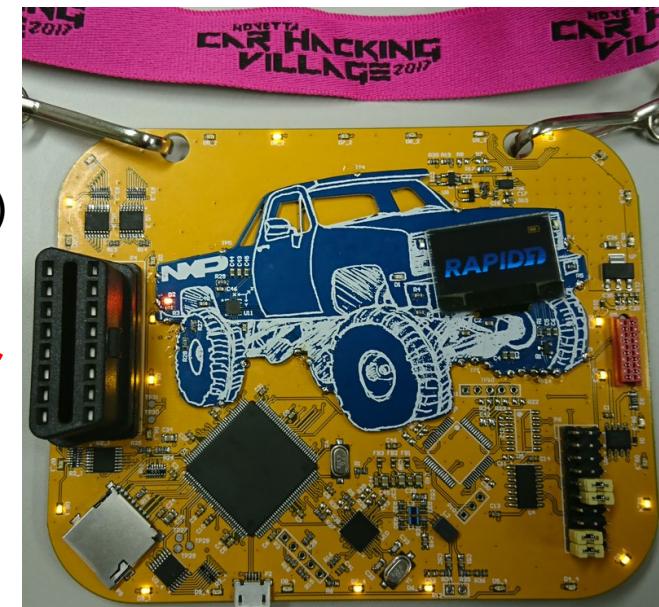
CHVバッジ(2018)

OBD-IIコネクタ
がある！

CHVバッジ(2017)



OBD-IIコネクタ



講演

■ 暗号解析から物理セキュリティ、ハッキングの事例
など色々な発表あり

- 1時間ずつ
- 10:00～19:00
5トラック並列
- 百件以上の発表



2018年の自動車関係の発表

■ BlackHat 2018

- There will be Glitches: Extracting and Analyzing Automotive Firmware Efficiently
 - ◆ フォルトインジェクションのようなハードウェアに対する攻撃を使って、ソフトウェア上の脆弱性がないようなセキュアECUからファームウェアを抜き出す方法を紹介。
- Applied Self-Driving Car Security
 - ◆ Jeepのハッキングで有名になったCharlie MillerとChris Valasekによる講演で、自動運転車をセキュアにする試み、脅威モデル、防御の戦略、また、アタックサーフェースを減らすためにセキュアなコード、セキュアなデバイス、冗長性を無くし、内部接続を無くすことなどの解説。
- Over-the-Air: How we Remotely Compromised the Gateway, BCM, and Autopilot ECUs of Tesla Cars
 - ◆ Tesla Model SおよびXに対して、遠隔からゲートウェイECU、ボディ制御ECU、オートパイロットECUに対して、どのようにして攻撃を実現できたかの説明で、前年のBlack Hat USA 2017で発表したTeslaのハッキングについて、詳しく説明を行ったもの。

(参考) 2017年の自動車関係の発表

■ BlackHat 2017

- Free-Fall: Hacking Tesla from Wireless to CAN Bus

昨年テスラのモデルSに複数のセキュリティ脆弱性が存在することを発表していた中国Tencentの研究者が、攻撃手法の詳細を解説した

- Sonic Gun to Smart Devices: Your Devices Lose Control Under Ultrasound/Sound

加速度計やジャイロスコープに使われるMEMSセンサーに対し、特定の周波数の音響波を外部から照射することで制御を失わせる攻撃手法を紹介。セグウェイやドローンへの攻撃だけでなく、車に対しても攻撃の可能性を示唆している

■ DEF CON 25

- Linux-Stack Based V2X Framework: All You Need to Hack Connected Vehicles

車車間(V2X)通信に使われるWAVE/DSRCプロトコルの解析で脆弱性を明らかにした

- Driving down the rabbit hole

日産リーフで見つけた3つの脆弱性の詳細と、悪用法、影響について解説した

IoTシステムの脅威の現状と開発ガイドライン

IoTデバイスを悪用したサイバー攻撃の現状

横浜国立大学 吉岡准教授の研究発表から以下のことがわかった

- インターネット経由で同大学に攻撃を仕掛けたマルウェア感染の機器・システムは、**約60万台・500種類**以上存在した(2016年1月から6月までの6ヶ月間)
- これはハニーポットによる観測に基づき、IPアドレスによって識別された
- 種類は型番が確認できたもののみであり、全体の3割以下である

2016年から現在に至るまで更に増大しており、
その大量感染の元凶は**Telnet(TCP/23)**である

※総務省研究開発委託「国際連携によるサイバー攻撃の予知技術の研究開発(PRACTICE)」より

IoTデバイスを悪用したサイバー攻撃の現状

- Telnetは多くの機器で動作し、容易にアクセスできる
- しかもTelnetログインID/パスワードは、デフォルトのままか、もしくは弱いパスワードで解析しやすい
- デフォルトパスワードはWebで公開され、簡単に入手可能

```
[SHOGO@WWW9058UP ~]$ TELNET x.x.243.13
TRYING x.x.243.13...
CONNECTED TO x.x.243.13.
ESCAPE CHARACTER IS '^]'.

xxxxxxI.3.0.0m800s
xxxxxxE.LOGIN:ROOT
PASSWORD:12345
```

IoT機器のデフォルトのIDとパスワードの組み合わせは多くないため、辞書型攻撃ですぐに破られる

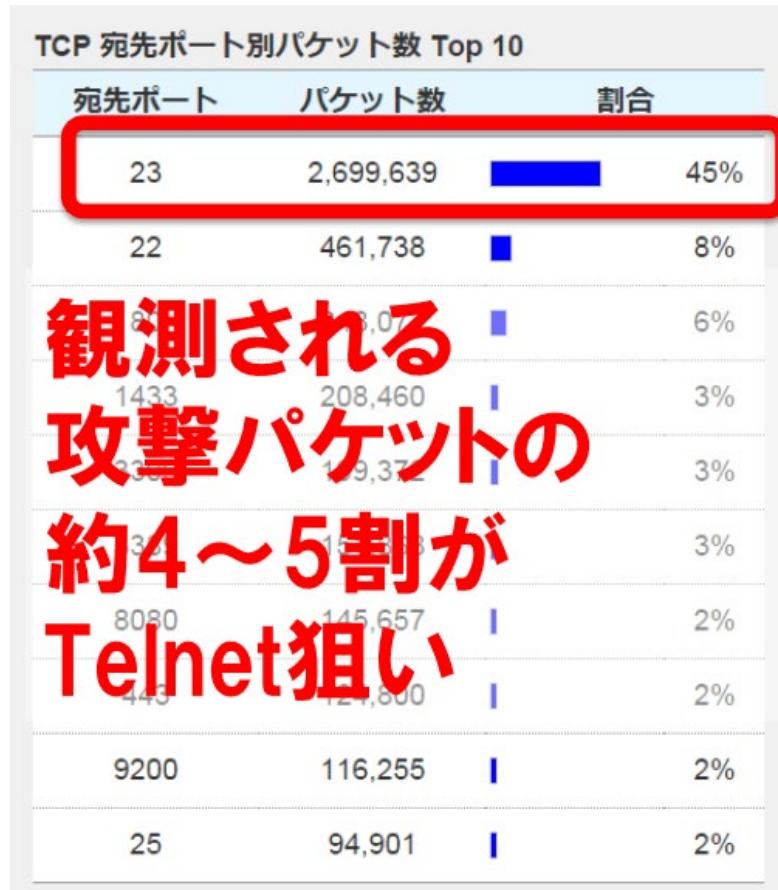
```
BusyBox v1.1.2 (2007.05.09-01:19+0000) BUILT-IN SHELL (ASH)
ENTER 'HELP' FOR A LIST OF BUILT-IN COMMANDS.
```

リモートログイン成功!

引用: <https://tech.nikkeibp.co.jp/it/atclact/active/16/110900124/110900002/>

※総務省研究開発委託「国際連携によるサイバー攻撃の予知技術の研究開発(PRACTICE)」より

IoTデバイスを悪用したサイバー攻撃の現状



- ダークネットへの攻撃
- 2014年からTelnet(TCP/23)への攻撃は急増(9割がLinux系)
- 年間攻撃数
 - 2013年 128.8億
 - 2014年 256.6億
 - 2015年 545.1億
 - 2016年 1,281億

引用: http://www.soumu.go.jp/main_content/000544772.pdf

※総務省研究開発委託「国際連携によるサイバー攻撃の予知技術の研究開発(PRACTICE)」より

IoTポットネット: Mirai

■ 現象

- 2016年10月 米国Dyn社のDNSサーバへの大規模DDoS攻撃(2回)
- Dyn社DNSサービスを使っていた企業(TwitterやNetflix)のサービスにアクセスしにくくなる障害発生

■ 原因

- 「Mirai」というマルウェアによるもの
- Telnetサービスを使い、50万台以上のIoT機器類に感染

■ 特徴

- 23/TCP, 2323/TCPをスキャン
- 辞書攻撃
- スキャン先IPアドレスとTCPシーケンス番号が同じ
- 送信先、windowサイズ、送信ポートはランダム(らしい)

■ 2016年9月にAnna-senpaiと名乗る人物がHackforumsにソースコードを公開

■ 続々と亜種も出現

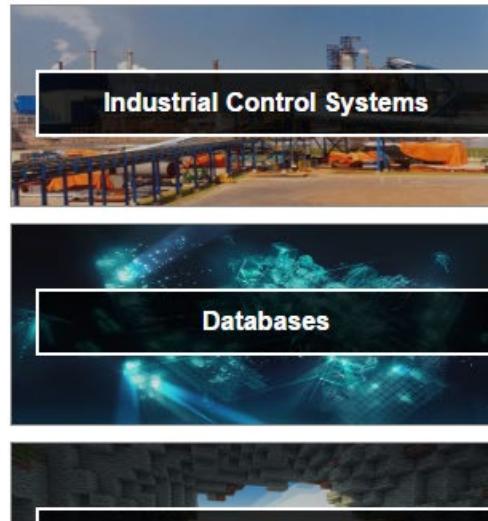
参考：組込み機器検索サイト「SHODAN」

- オフィス機器、家電、信号機、発電所などの産業制御システムやIoT機器を検索できる

<https://www.shodan.io/explore>

The screenshot shows the Shodan Explore interface. At the top, there's a navigation bar with links for 'Shodan', 'Developers', 'Book', and 'View All...'. On the right side of the bar are 'Show API Key', 'My Account', and an 'Upgrade' button. The main header says 'Explore' and has a sub-instruction 'Discover the Internet using search queries shared by other users.' Below the header, there's a search bar containing the IP address '165.242.42.0/24'. The search results are displayed in a grid format. The first result is a card for a 'Webcam' with a red '8,786' badge, labeled 'best ip cam search I have found yet.' It includes tags 'webcam', 'surveillance', and 'cams', and a timestamp '2010-03-15'. The second result is a card for 'Cams' with a red '3,376' badge, labeled 'admin admin'. It includes tags 'cam' and 'webcam', and a timestamp '2012-02-06'. The third result is a card for 'Netcam' with an orange '1,944' badge, labeled 'Netcam'. It includes the tag 'Netcam'. To the left of the search results, there's a sidebar titled 'Featured Categories' with cards for 'Industrial Control Systems' (with an image of industrial pipes) and 'Databases' (with an image of abstract data structures).

Featured Categories



Top Voted

8,786	Webcam	best ip cam search I have found yet.	2010-03-15
3,376	Cams	admin admin	2012-02-06
1,944	Netcam	Netcam	

Recently Shared

2	Samba servers	2017-05-25
1	Jumpline - Samba Servers	2017-05-25
1	SMB Status =Authentication: disabled SMB Status Authentication: disabled ^_^	

セキュリティ開発ガイドラインの例(自動車とIoT関係)

- JASO(日本自動車技術会規格)
 - 自動車 情報セキュリティ分析ガイド TP15002:2015 (2015/03)
- 総務省、経産省、IoT 推進コンソーシアム
 - IoTセキュリティガイドライン ver1.0 (2016/07)
- IPA
 - つながる世界のセーフティ&セキュリティ設計入門 (2015/10)
 - つながる世界の開発指針 (2016/03)
 - IoT開発におけるセキュリティ設計の手引き (2016/05)
 - 自動車の情報セキュリティへの取組みガイド 第2版(2017/03)
- CCDS
 - CCDS製品分野別セキュリティガイドライン (2016/06)
 - ◆ 車載器編、IoT-GW編、金融端末(ATM)編、オープンPOS編

目的

製品分野ごとに対策すべき脅威が異なることから、IPA「つながる世界の開発指針」を参考に、各分野ごとの視点でセキュリティの取組みを整理し、業界にセキュリティ・バイ・デザインの考え方を普及しやすくする。

対象分野

車載器

IoTゲートウェイ

金融端末(ATM)

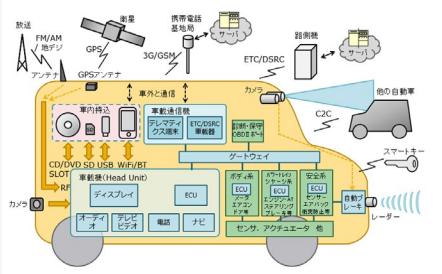
決裁端末(POS)

ガイドラインの主な内容

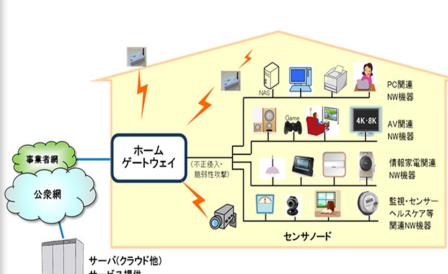
- ・対象とするシステム構成
- ・想定されるセキュリティ上の脅威
- ・製品ライフサイクルの各フェーズにおけるセキュリティの取組み
(IPA「つながる世界の開発指針」との相関)
- ・脅威分析・リスク評価の方法
- ・製品全体およびセキュリティ対策機能の第三者セキュリティ評価



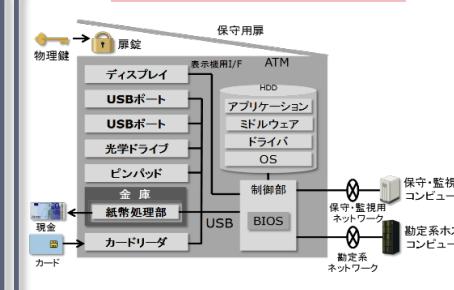
車載器システム構成



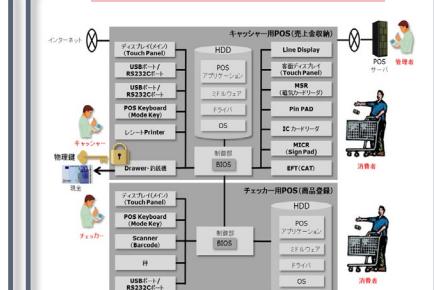
IoT-GW: ホームGWケース



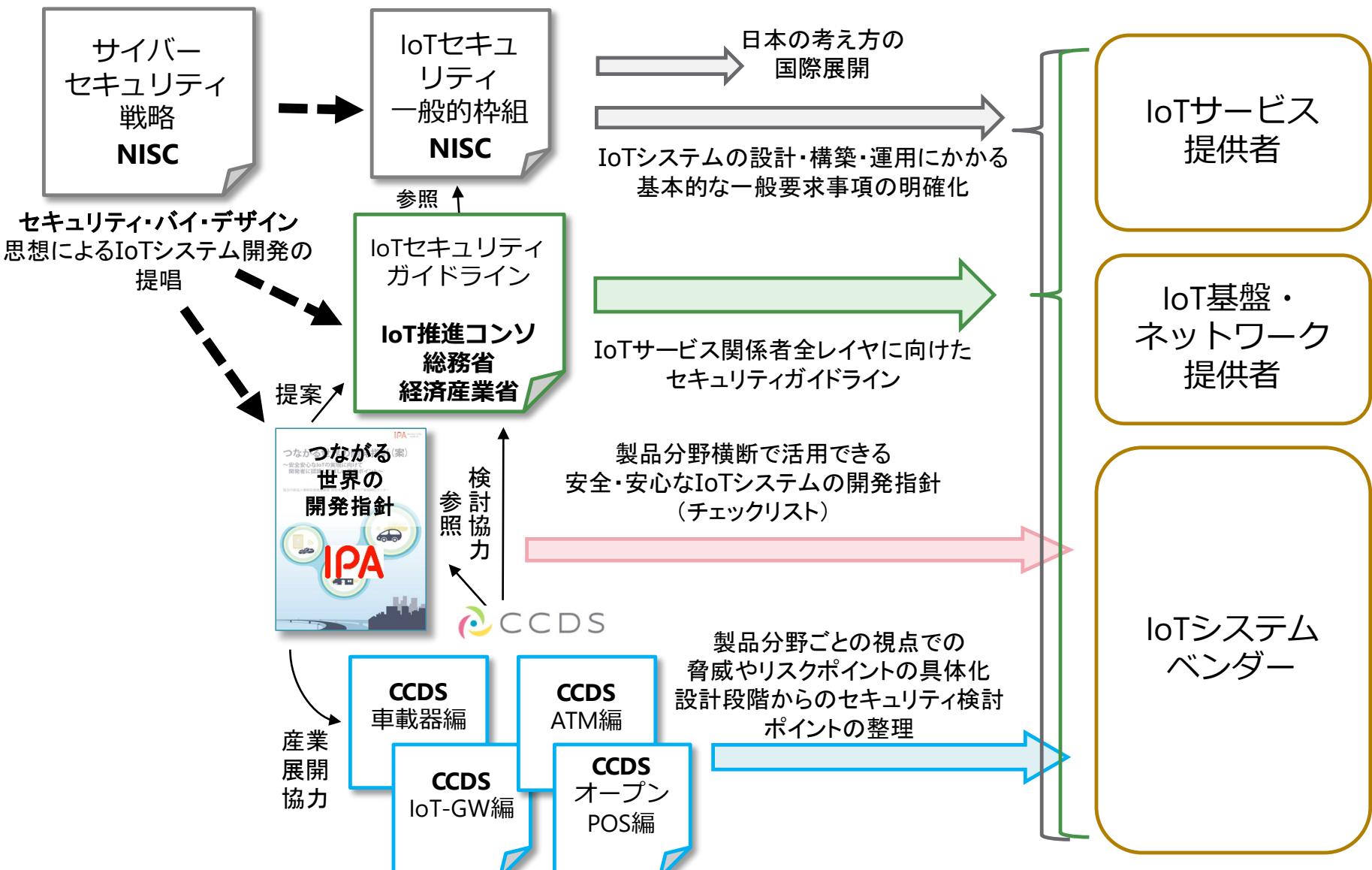
ATMシステム構成



POSシステム構成



CCDS分野別ガイドラインの位置づけ



IoTセキュリティガイドラインの例(海外)

- Dept. of Homeland Security
 - STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)
- oneM2M:
 - Security Solutions v2.4.1 (TTCより日本語版あり)
 - Security v2.0 (TR analysis)
 - End-to-End Security and Group Authentication v2.0
- CSA:
 - Security Guidance for Early Adopters of the Internet of Things (IoT)
 - Identity and Access Management for the Internet of Things – Summary Guidance
 - Security Guidance for Smart Health, for Smart Cities, for Smart Retail
 - Analysis of Hardware Security Options for the IoT
 - Checklist for Secure IoT Device Development
 - Internet of Things (IoT)インシデントの影響評価に関する考察 (CSAジャパンより日本語版あり)
 - Future-proofing the Connected World: 13 steps to Developing Secure IoT Products(同上)
- OWASP
 - IoT Security Guidance (Draft)
 - https://www.owasp.org/index.php/IoT_Security_Guidance
- GSMA:
 - IoT Security Guidelines (Overview, for Service Eco-Systems, for End Point Eco-Systems, and for Network Operators)
 - IoT Security Self-Assessment
- SAE:
 - J3061(Cybersecurity Guidebook for Cyber-Physical Vehicle)
- Continua Health Alliance
 - End-to-End Security for Personal Telehealth

他にもある

自動車セキュリティガイドラインの例(海外)

- SAE International (Society of Automotive Engineers)
 - J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016/01)
 - ISO/SAE 21434: Automotive Security Engineering (2019年末から2020年を予定)
 - UN WP29 (国際連合 自動車基準調和世界フォーラム)
 - WP29 Recommendation (2018年末に最終版予定)
- ※WP29は自工会、ISO/SAE21434は自技会が主体となって提案している
- NHTSA (米国運輸省道路交通安全局)
 - Cybersecurity Best Practices for Modern Vehicles (2016/10)
 - Federal Automated Vehicles Policy (2017/9) 自動運転政策ガイドライン
 - ENISA(欧洲ネットワーク・情報セキュリティ機関)
 - Cyber Security and Resilience of smart cars (2017/01)
 - Security and Resilience of Intelligent Public Transport. Good practices and recommendations (2016/01)

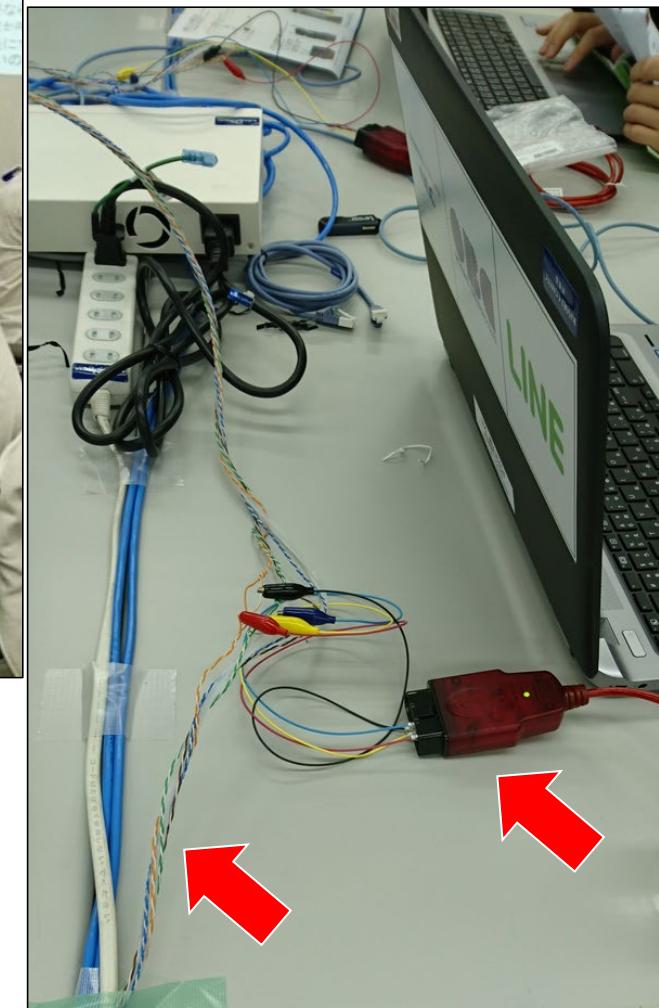
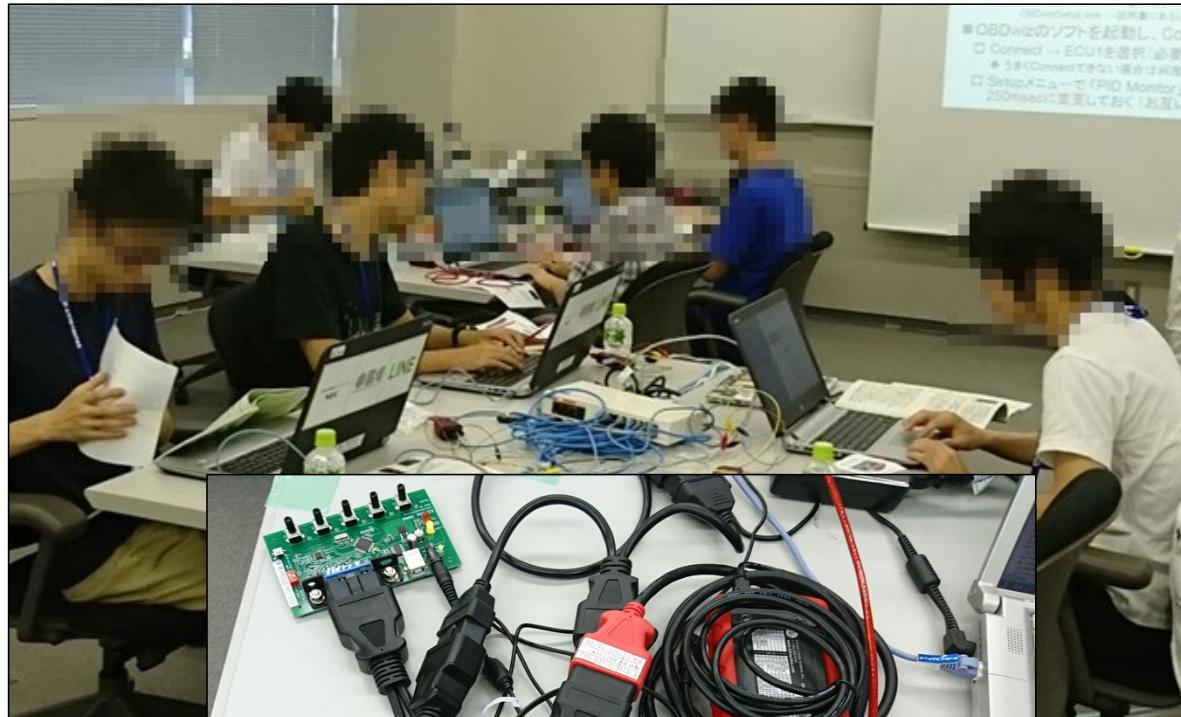
IoT・車載システムの情報セキュリティ教育

- IPA セキュリティ・キャンプ（学生・生徒のみ）
 - 全国大会と地方大会(ミニキャンプ)
- NICT SecHack365(25歳以下、学生は無料)
- SECCON（セキュリティコンテスト）
 - CTF 予選、決勝大会
 - SECCON Beginners、Girls、地方大会
- CTF世界大会 - DEF CONにて
- IPA・経済産業省
 - 産業サイバーセキュリティ人材育成(ICS CoE)
- NICT・総務省
 - ナショナルサイバートレーニングセンターによるCYDER、サイバー・コロッセオ、SecHack365
- escar Asia(10月)
- Code Blue(11月)
 - 2017,2018年には、車載システムの解析コンテスト
- 自動車技術会
 - 自動車サイバーセキュリティ講座、など

情報セキュリティには、幅広い知識が必要：
ハードウェア、OS、通信プロトコル、サーバ、ソフトウェア、…

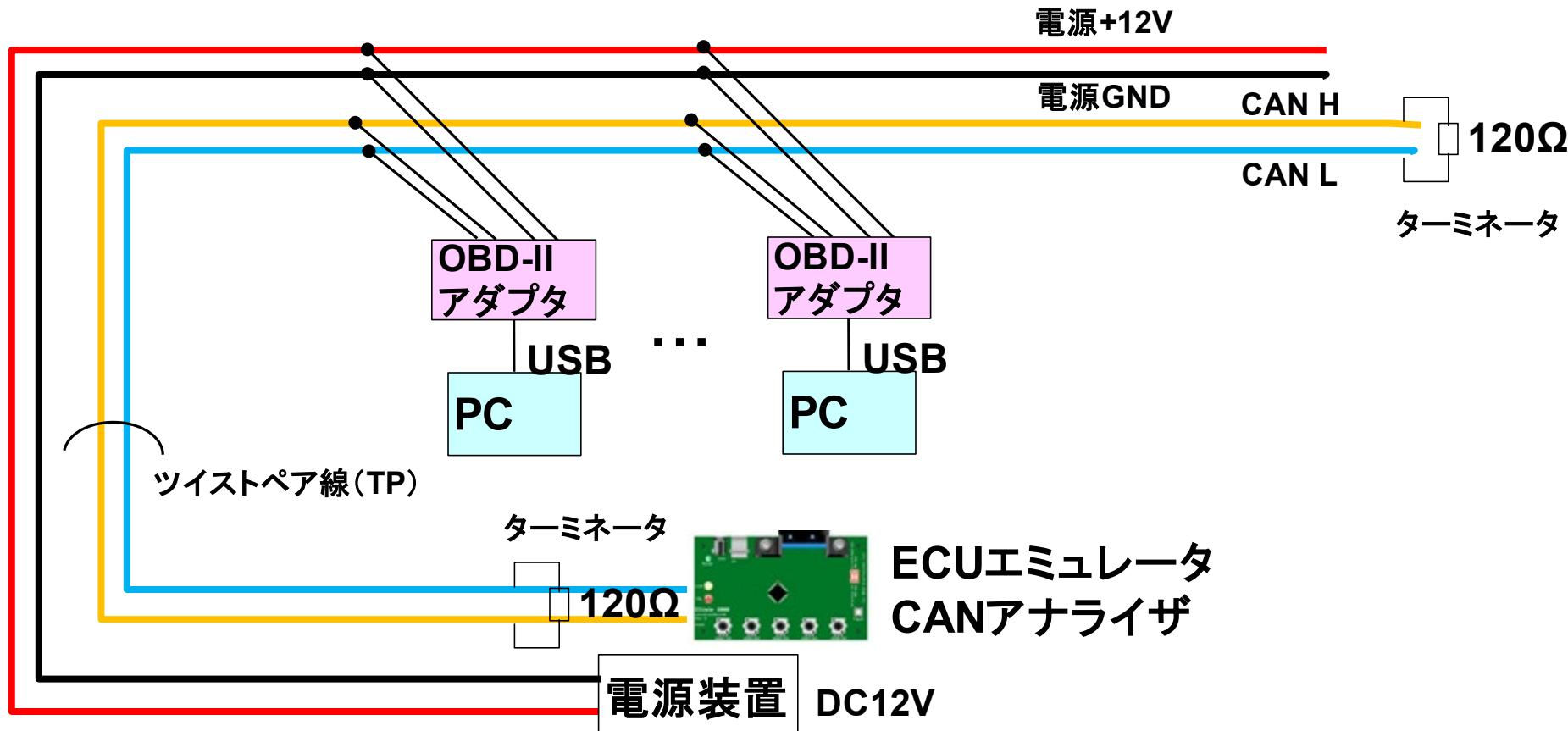
若手への教育： セキュリティ・キャンプ全国大会での様子

- 自動車CANパケット キャプチャ＆解析演習
 - Pythonで解析プログラムを作成する



自動車ネットワークのデータ解析演習の例

- CANはバスなので、複数のノードを並列に接続する
 - ECUエミュレータ、CANアナライザ、データ表示器
 - 解析用PCにつながるOBD-IIアダプタ
- CANの配線はCat6のUTP線を用い、両端にターミネータ抵抗



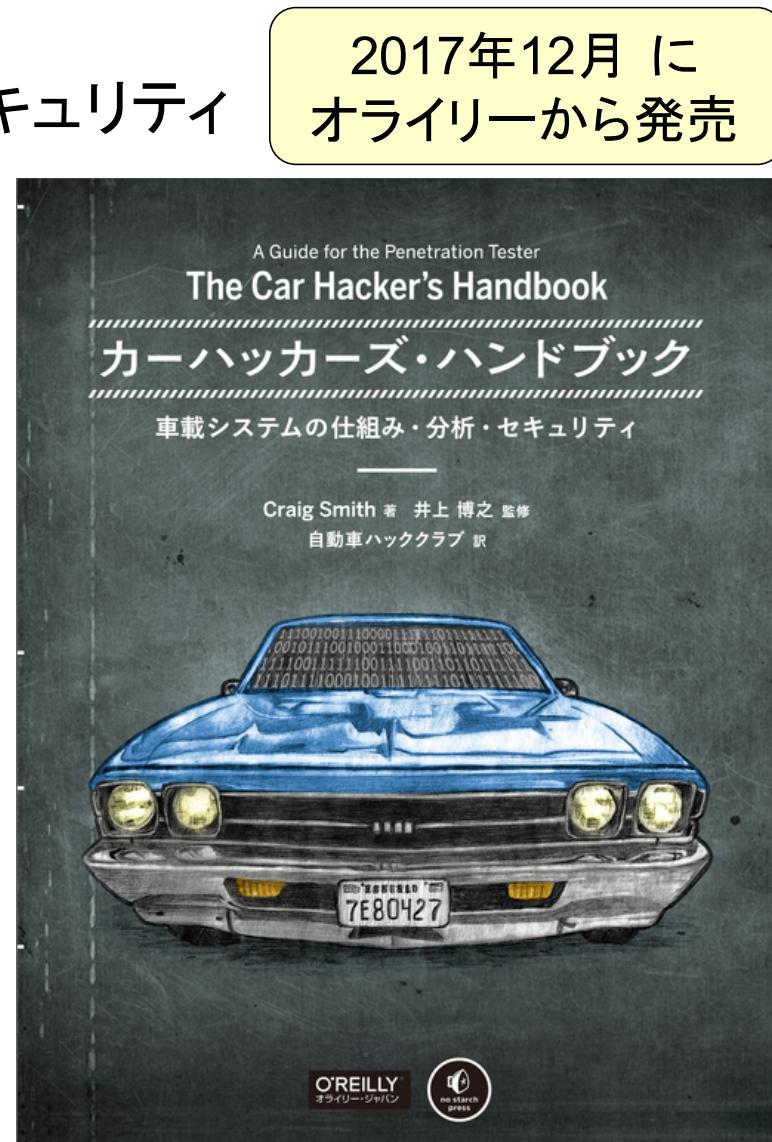
Car Hacker's Handbook を翻訳・監修

■ カーハッカーズ・ハンドブック — 車載システムの仕組み・分析・セキュリティ

■ 目次

- 第1章 隊威モデルの理解
- 第2章 バスプロトコル
- 第3章 SocketCANによる車載通信
- 第4章 診断とロギング
- 第5章 CANバスのリバースエンジニアリング
- 第6章 ECUハッキング
- 第7章 ECUテストベンチの構築と利用
- 第8章 ECUや他の組込みシステムへの攻撃
- 第9章 車載インフォテイメントシステム
- 第10章 車車間通信
- 第11章 攻撃ツールの作成
- 第12章 SDRを用いた無線システムへの攻撃
- 第13章 パフォーマンスチューニング
- 付録A 市販のツール
- 付録B 診断コードのモードとPID
- 付録C 自分たちのOpen Garagesを作ろう

2017年12月に
オライリーから発売



まとめ

IoTシステムにおけるセキュリティ確保

■ サービス指向の考え方

□ 何のためにネットにつなぐのかを考える

1. そもそもインターネット全体につなぐ必要があるのか
 - ◆ 自社のデータセンターだけにつなぐことも検討
2. 製造者やサービス提供者が知りたい情報は何か?
 - ◆ サービス利用状況
 - ◆ 故障診断、機器状態
3. 利用者が使いたいサービスは何か?
 - ◆ Web、メール、SNS ?
 - ◆ トランスペアレントなProxyによる実現はできないか？

■ 情報セキュリティはいたちごっこ

- 穴を全て塞ぐことはできない
- 暗号(方式、現在のレベル)は、いつか破られる
- 家電や自動車の**ライフサイクルは長い**
 - ◆ PCやサーバであれば、OSの更新サイクルに依存
 - ◆ 遠隔でのソフトウェアや暗号キーの更新の仕組み

まとめ

■ IoTシステム、車載システムの情報セキュリティ

□ 最近の脅威事例

- ◆ 組込みLinuxのような**共通プラットフォームの導入による問題**
 - サーバ等のサイバーセキュリティと同一の脆弱性
- ◆ 攻撃の**手口が一般化**(オープンソースで様々なことができる)

□ ネットにつながる家電や自動車、産業機器にひそむ脆弱性

- ◆ 世界レベルからのアタックに対する防御策
- ◆ **ライフサイクル**とファームウェア更新の難しさ

□ DEFCON、BlackHat

- ◆ 解析能力の向上 → 対策能力の向上
- ◆ 便利な**ツールや解析ソフトウェア**の入手性の向上
 - だれでもリバースエンジニアリングが可能に。よいハッカーと、悪いハッカー

■ 設計開発ガイドライン

□ セキュアなシステムの設計 & 開発

□ セキュアなIoT製品・サービスを開発するには、**まず設計段階からセキュアなシステム作りを考える**

- ◆ 考えるポイント・やり方はいろんなところにガイドラインがある

□ すべての脅威はつぶせない。コスト効果高く、安心安全を確保する

□ セキュアな製品になっているかの**セキュリティ検証サービス**