資料３－２

IoT / 非 PC 環境における脅威の事例

2016年1月21日

JPCERTコーディネーションセンター

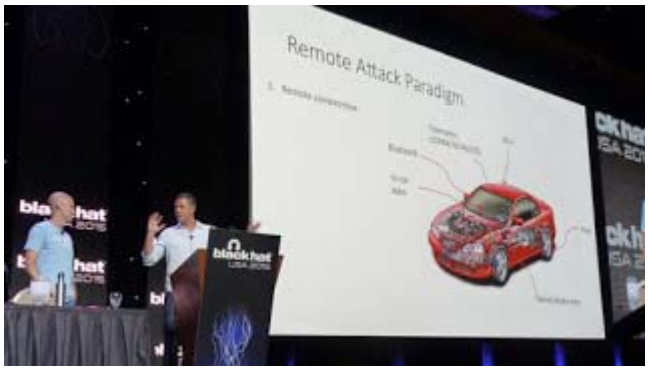
2015年：非 PC 領域へのセキュリティへの関心

- **BlackHat / DEF CON / USENIX 等におけるセキュリティ研究者の熱い視線**
  - —Internet of Things (IoT) 、制御システムに関する話題
  - —スマートフォン (Android, iOS) に関する話題

- **セキュリティ対策の進んだ PC 領域に対して、開発と対策が同時並行している非 PC 領域**
  - —対象として取り掛かりやすい
  - —対象機器の影響から社会的な注目度も集めやすい

事例①　自動車リモート操作

- **FCA Jeep Cherokee / Uconnect を経由したリモート操作**



C. Miler, C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle”, BlackHat.

リモートからの自動車の操作

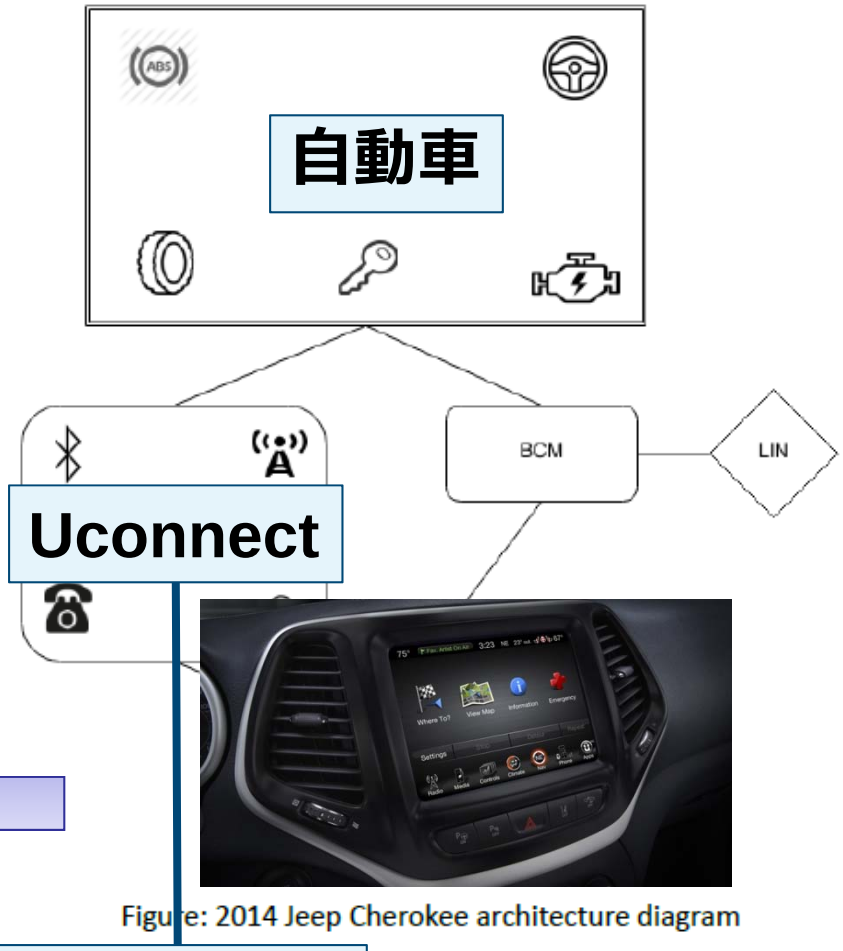
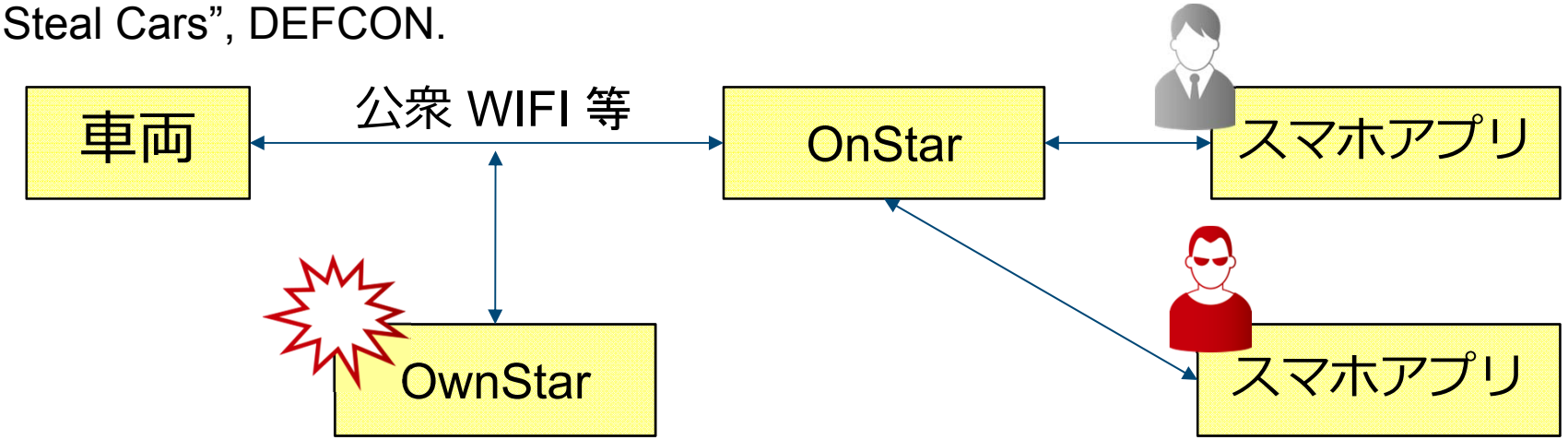


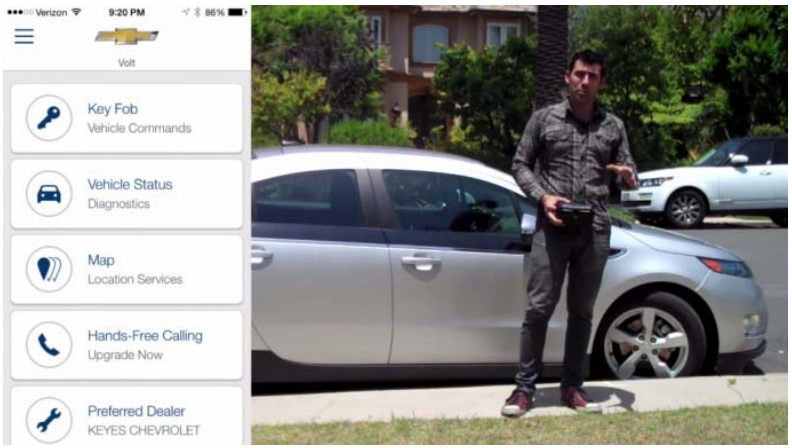
Figure: 2014 Jeep Cherokee architecture diagram

事例②　クラウドサービスへのMITM

GM 社 OnStar クラウドサービスのMITM

S. Kamkar, “Drive It Like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars”, DEFCON.





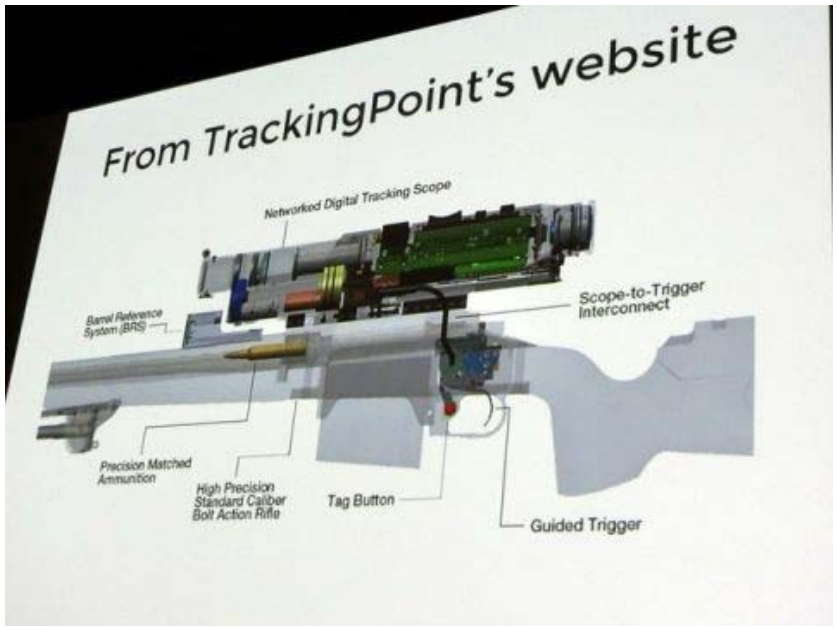
GM 社 OnStarの悪用

インターネットを経由して、ドアロック、エンジンスタート、ライト制御が遠隔から可能

事例③　システム解析と悪用

- **Tracking Point 社製 TP750 ライフルの解析**

  R. Sandvik, M. Auger, “When IoT Attacks: Hacking A Linux-Powered Rifle”, BlackHat USA 2015.

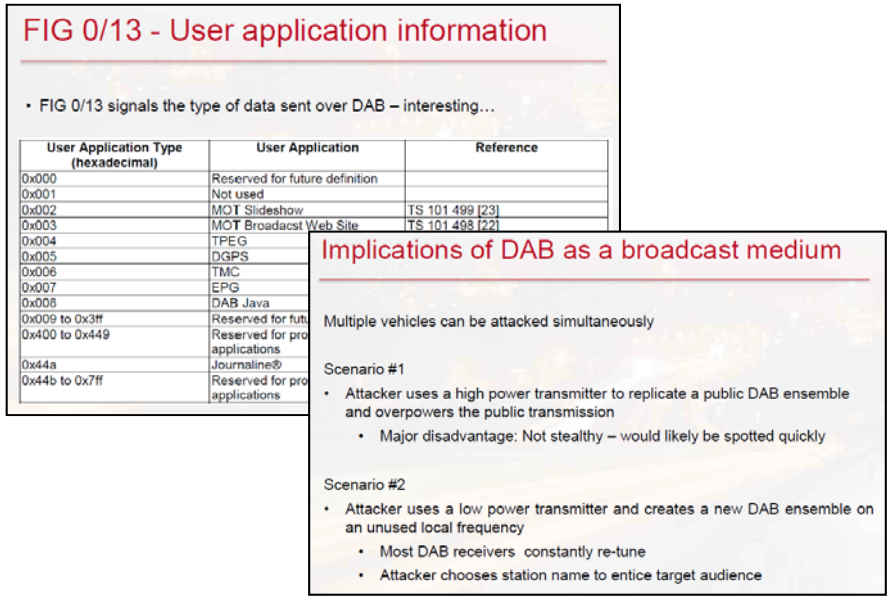


インテリジェントスコープの Wifi 通信を解析し、
API を活用してシステムを改変

事例④　様々な脆弱性の発見

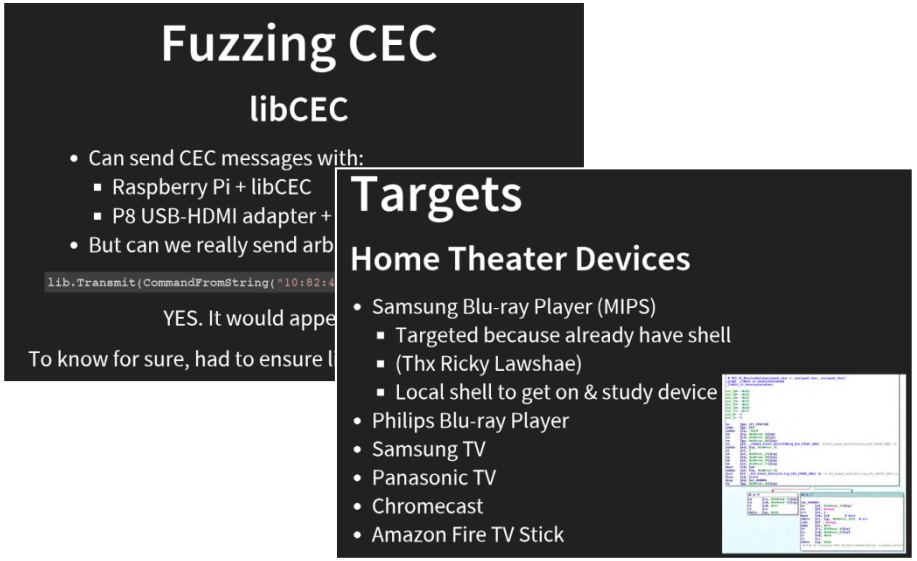
■ ファジングにより様々な脆弱性が浮き彫りにされる

Broadcasting Your Attack: Security Testing DAB Radio in Cars
A. Davis (ncc group)



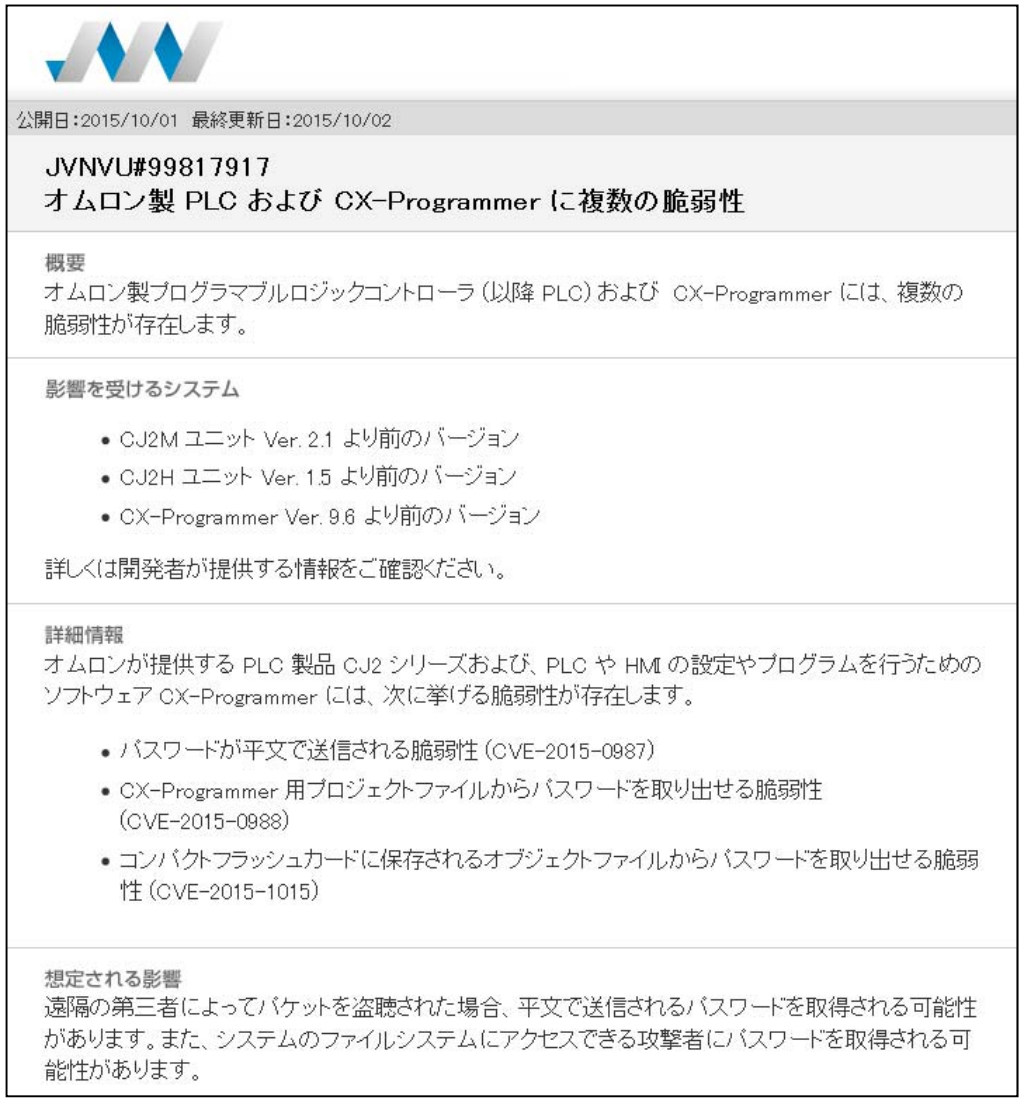
DAB (デジタルラジオ放送) のデータ領域に攻撃コードが挿入できる可能性を示唆

High-Def Fuzzing: Exploring Vulnerabilities in HDMI-CEC
J. Smith (HP ZDI)



HDMI CEC (リンク機能) に対するファジングにより、TV などの脆弱性を示唆

事例⑤　様々な脆弱性の発見 (産業制御装置 / PLC)



公開日:2015/10/01　最終更新日:2015/10/02

JVNVU#99817917
オムロン製 PLC および CX-Programmer に複数の脆弱性

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 には、複数の脆弱性が存在します。

影響を受けるシステム

- CJ2M ユニット Ver. 2.1 より前のバージョン
- CJ2H ユニット Ver. 1.5 より前のバージョン
- CX-Programmer Ver. 9.6 より前のバージョン

詳しくは開発者が提供する情報をご確認ください。

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します。

- パスワードが平文で送信される脆弱性 (CVE-2015-0987)
- 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 (CVE-2015-0988)
- 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 (CVE-2015-1015)

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ります。また、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可能性があります。

- SHODAN などでの検索対象となる可能性
  - 実証コードが公開されている場合もある
  - JPCERT/CC でもパケットや SHODAN での登録を確認
- 2015年で脆弱性が指摘された主な機器
  - MELSEC FX3G Series PLCs (三菱電機製品)
  - CENTUM 他 (YOKOGAWA 製品)
  - CJ2M/2H 他 (オムロン製品)

事例⑥　IoT の先にある物理的な問題

■ IoT 機器の先にある物理的な資産

— スマート家電、ホームセキュリティなど、サイバーからの問題が物理的な実被害を与えかねない

公開日:2015/07/27 最終更新日:2015/07/27

JVNVU#92850780
Honeywell Tuxedo Touch Controller に複数の脆弱性

概要
Honeywell が提供する Tuxedo Touch Controller ソフトウェアには、認証回避およびクロスサイトリクエストフォージェリの脆弱性が存在します。

影響を受けるシステム

- Tuxedo Touch Controller ソフトウェア TUXW_V5.2.19.0_VA より前のバージョン

詳細情報
クライアントサイドの認証の使用 (CWE-603) - CVE-2015-2847
Tuxedo Touch Controller のウェブインターフェースは、Javascript を使ってクライアント側で認証を行っており、認証されていないユーザのアクセスはログインページにリダイレクトされます。攻撃者は、USERACCT=USERNAME:_ や PASSWORD:_ といった文字列を含むリクエストを落とすことで、認証を回避し、制限されたページにアクセスすることが可能です。

クロスサイトリクエストフォージェリ (CWE-352) - CVE-2015-2848
Tuxedo Touch Controller にはクロスサイトリクエストフォージェリの脆弱性が存在します。当該製品にログインしているユーザに細工されたリクエストをアクセスさせることで、遠隔の第三者によって当該製品を操作される可能性があります。これらの操作には、玄関の施錠など Tuxedo Touch Controller で操作できるホームオートメーション用デバイスに対するコマンドの実行が含まれる可能性があります。

想定される影響
遠隔の第三者によって認証を回避され、制限されたページを閲覧されたり、ユーザの意図しない操作をさせられたりする可能性があります。その結果、玄関の施錠操作など、ホームオートメーション用デバイスを操作される可能性があります。

CVE-2015-2848
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
Base Score: 7.5

被害者が罠サイトを被害者に踏ませることで、鍵の解除を含む任意の操作 が可能

事例⑦　常時接続する IoT 機器とマルウエア

- 「IoT 機器を標的とした攻撃の観測について」

@police

平成 27 年 12 月 15 日

Topic

IoT 機器を標的とした攻撃の観測について

インターネットに接続されたデジタルビデオレコーダ等の Linux が組み込まれた IoT 機器を標的とした攻撃を観測しています。この攻撃を受けた機器が、攻撃者の命令に基づいて動作する「ボット」になる事例を確認しています。現在利用している機器について、最新のセキュリティ情報を確認することを推奨いたします。

1　宛先ポート 23/TCP に対するアクセス

23/TCP はネットワークに接続された機器を遠隔で操作する Telnet で利用されていますが、このポートに対するアクセスは、平成 26 年以降、高い水準で推移しています。

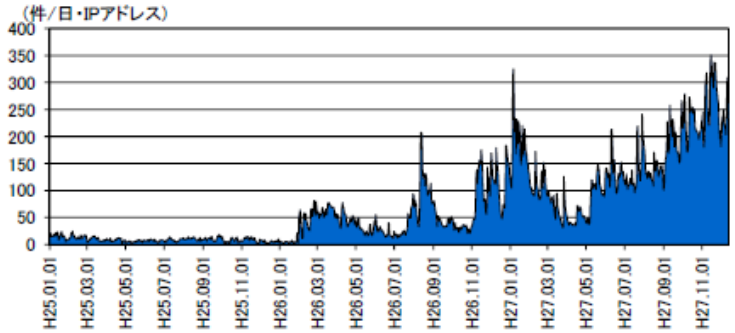


図1　宛先ポート 23/TCP に対するアクセス件数の推移

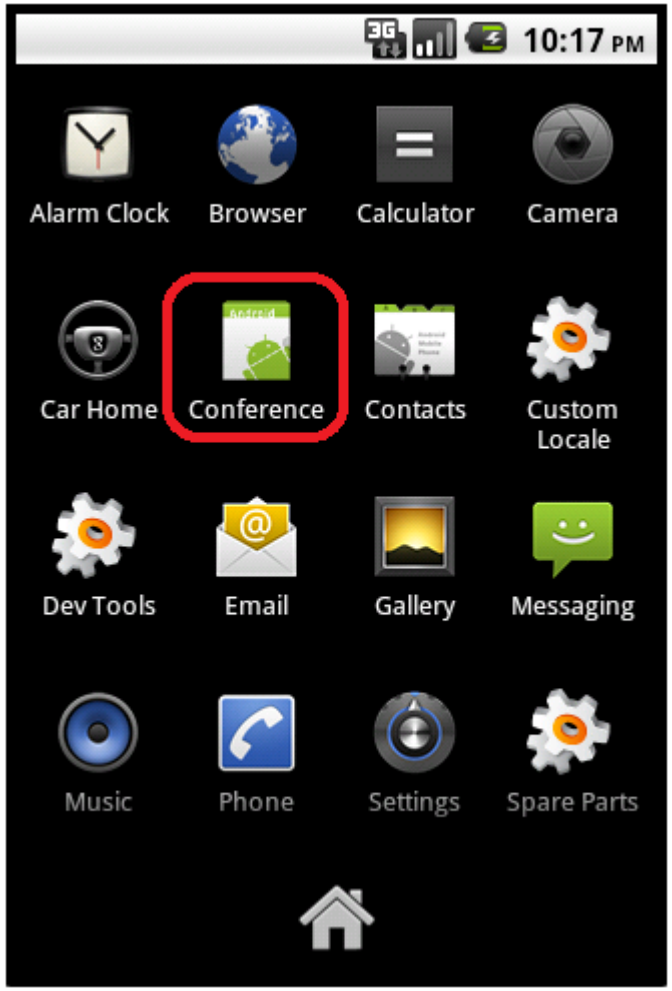
これらのアクセスについては、過去にも注意喚起を実施してきたように、多くはインターネットに接続されたルータ、ウェブカメラ、ネットワークストレージ、デジタルビデオレコーダ等の Linux が組み込まれた IoT 機器（以下「組み込み機器」という。）が発信元であることを確認しています[1]。これらの機器は、何らかの手法により、攻撃者に乗っ取られ、攻撃の踏み台として悪用されていると考えられます。

警察庁 (平成27年12月15日)
https://www.npa.go.jp/cyberpolice/topics/?seq=17323

- 同様の傾向は、JPCERT/CC でも観測
  - マルウエアに感染した非 PC からの攻撃活動の観測
  - VoIP アダプタ、IPTV 、Web カメラ等の IoT 機器
  - Port23/TCP のパケットを送信

事例⑧　Android 端末を使った高度サイバー攻撃

- **チベット、ウイグルの活動家に対する攻撃 (2013年3月)**
  - —標的型メールにより感染
  - —情報を窃取
    - Contacts (SIMと電話両方)
    - Call logs
    - SMS messages
    - Geo-location
    - Phone data (phone number, OS version, phone model, SDK version)



K. Baumgartner, C. Raiu, D. Maslennikov (Kaspersky), Android Trojan Found in Targeted Attack
https://securelist.com/blog/incidents/35552/android-trojan-found-in-targeted-attack-58/

- **高度サイバー攻撃は、既に非 PC 領域に進出**

まとめ

- **IoT 機器は、攻撃のターゲットとなりやすい？**
  - —デフォルトパスワード
  - —脆弱な Web 管理インターフェース
  - —安易な Telnet コンソール解放

- **性能・機能の向上**
  - —“スマート“機器に対する脅威は、PC とほぼ変わらない
  - —手軽な“常時”接続環境

- **アップデート・ライフサイクルの問題**
  - —設置後、放置されやすい