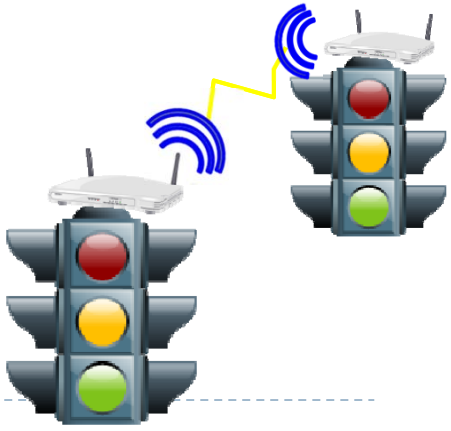
機器のネットワーク化によって深刻化するサイバー攻撃

高倉弘喜
名古屋大学

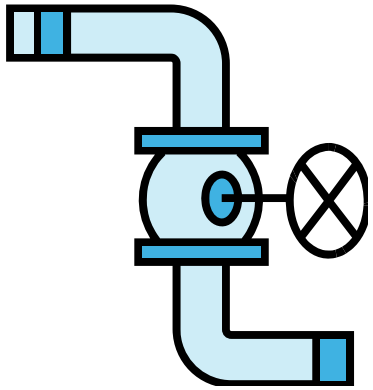
インターネット技術が社会インフラへ

- 単なる情報伝達手段から様々な生活の場に
  - 電子メールやWeb
    - 情報の交換や流通
    - 商業活動
      - ✓ B2B、C2C、B2B2C…
    - 金融取引
      - ✓ オンラインバンキング、オンライントレード…
- インターネット技術の活用分野拡大
  - 公共インフラ制御：ガス、上下水道、電力…
  - 道路：電光掲示板、信号機
  - 建物設備
  - 家電も黒モノから白モノへ



社会インフラを支えるソフトウェア

- あらゆるディバイスをソフトウェアで制御
  - Windows, MacOS, FreeBSD, Linux, Symbian…
  - Java, Flash…
- パソコン
  - 周辺機器：無線LAN基地局、プリンタなど
- 携帯電話
- 家電
  - テレビ、電子レンジ、冷蔵庫…
- 自動車もコンピュータ制御へ
  - ナビ＋各種センサ＝エンジン＆ステアリング制御
  - 油圧制御から電子制御へ
    - Steer-by-Wire、ブレーキ制御
- 航空機は常時ネット接続の時代



飛行機のコンピュータ化

ラムエア　タービン(B757)

どちらもBoeing737の操縦席

Internet of Thing (IoT, モノのインターネット)

- 単に「インターネットを使う」という意味ではない
  - インターネット技術をフルに活用
    - 規格の共通化
      - ✓ 配線の特性、端子の割り当て
      - ✓ 電気信号
      - ✓ 符号化(電圧・周波数変化⇔0/1のデジタル情報)
      - ✓ 通信プロトコル(IP, TCP, UDP…)
    - 共通規格上でのアプリケーション開発
      - ✓ 高い相互接続性の維持
      - ✓ 開発コスト削減と開発時間の短縮

- OS、ミドルウェアまでが共通規格に…
  - Linuxベースの家電
  - Webサーバ(apache)やDBサーバ(MySQL)搭載の家電

ありとあらゆるものでOSの汎用化

- 組込みシステム
  - 専用のファームウェア、OS、アプリ
  - 組込みにカスタマイズされたPC OS、アプリ
    - Windows Embedded Automotive

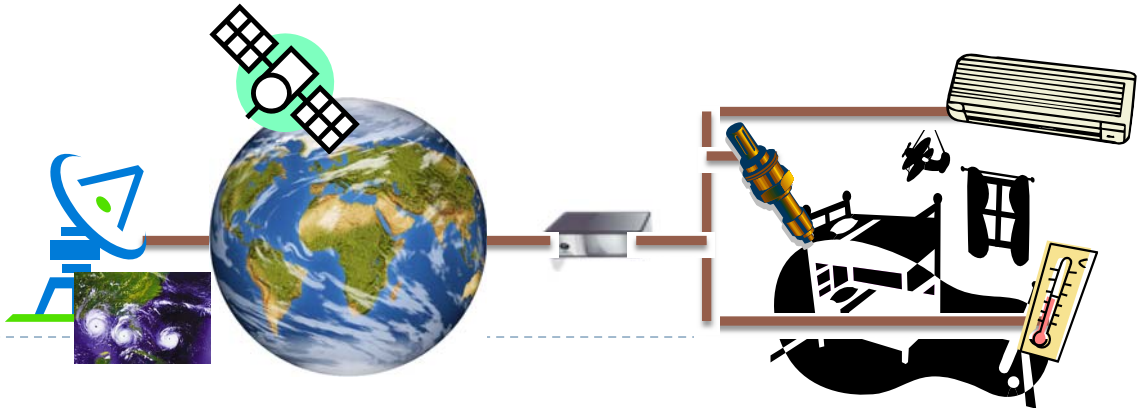
http://www.microsoft.com/windowsembedded/ja-jp/evaluate/windows-embedded-automotive-7.aspx

- 接続機器の汎用性維持
  - iPhoneが繋げるカーナビ、オーディオアンプ
  - PDAによる整備
  - PowerPoint、Word、PDFファイルが編集可能なプリンタ
- 石油掘削プラントでも汎用OS化&ネット化が進む
  - 産油量、精製量を全て本社で管理
  - 原油価格の変動にリアルタイムに対応

ネットは皆さんのすぐそばに…
お部屋の中までも…

- 地球に優しいエネルギー消費
  - 急速冷暖房を避ける
    - 極論を言えば、こまめにon/offしない方がエコ
    - とは言っても、実践し難い…考えるのメンドクサイ
  - インターネット技術を駆使した電力消費管理
    - 気象情報
      - ✓ 今日の気温・湿度変化予想&過去の履歴
    - センサー情報
      - ✓ 外気温、二酸化炭素濃度、在室者の人数
    - 利用履歴
      - ✓ 曜日・時間帯毎

→エアコンを自動制御



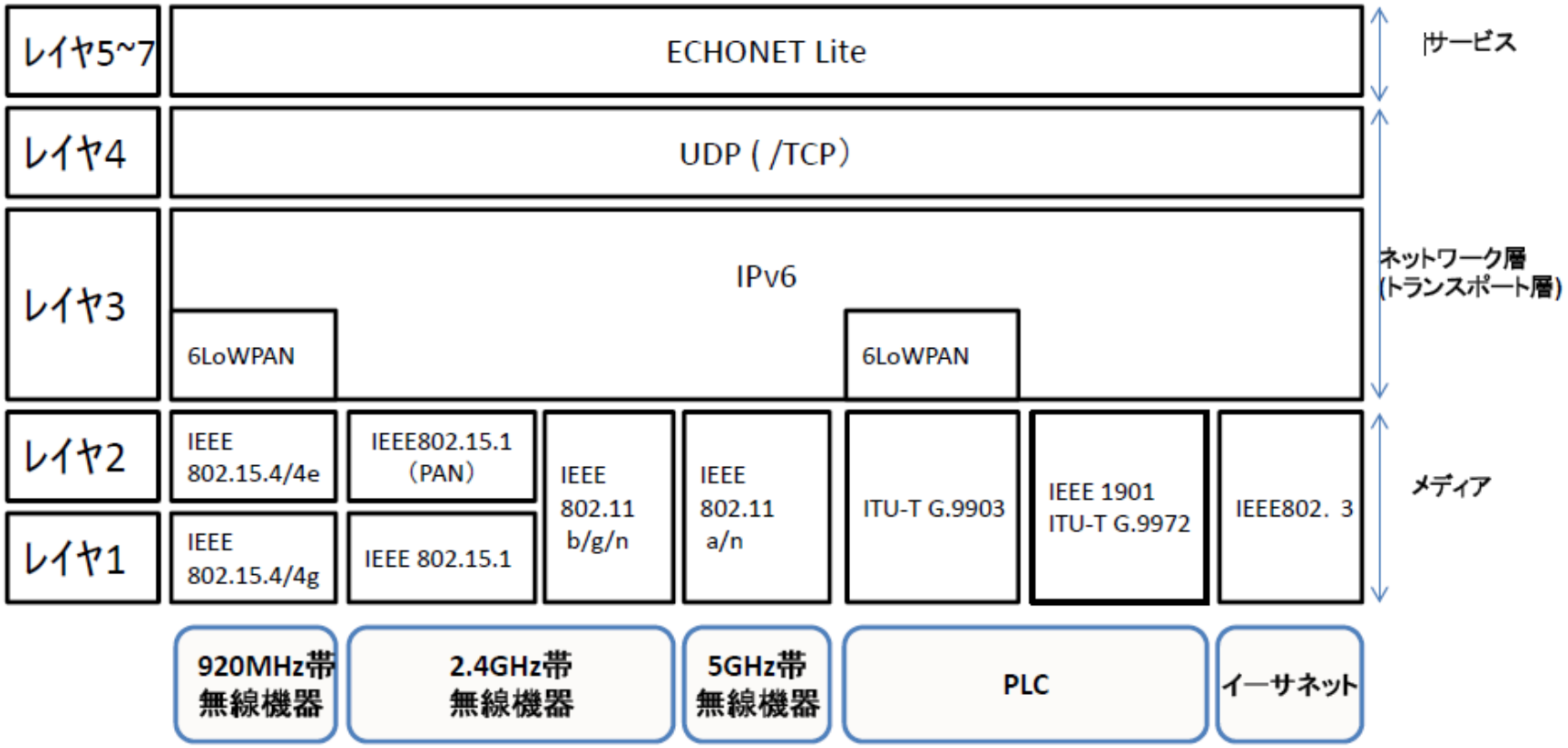
HEMS(Home Energy Management System)

- センサー＋IT技術の活用
  - ネットワーク接続型家電の増大
- 効率的な住宅のエネルギー管理
  - 使用状況把握
  - 家電機器の一括制御
  - エネルギー使用量の最適化
- 物理層
  - PLC、Ethernet、無線(2.4GHz, 5GHz, 920MHz)
  - 家電種別毎、サービス毎に異なる物理層は非現実的
  - 同一物理層の相乗りとなる可能性大

→用途の異なるトラフィック混在

HEMSとIPv6

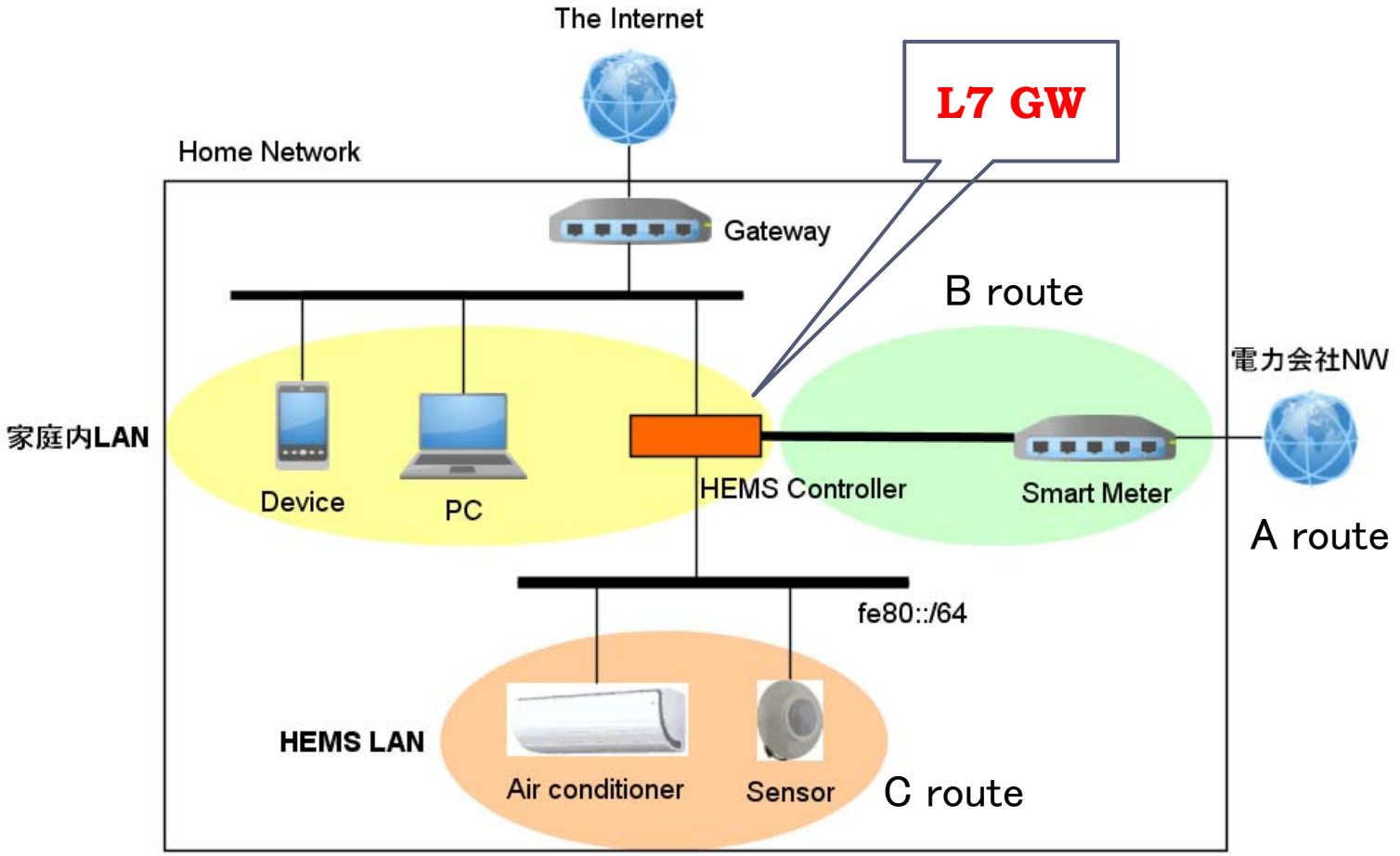
- HEMSにおける標準メディアプロトコル・スタック
  - レイヤ3(ネットワーク層)はIPv6が基本
  - 通常はUDP…相互認証の機構は？



出典：HEMSスマートメーター（Bルート）運用ガイドライン［第1.0版］

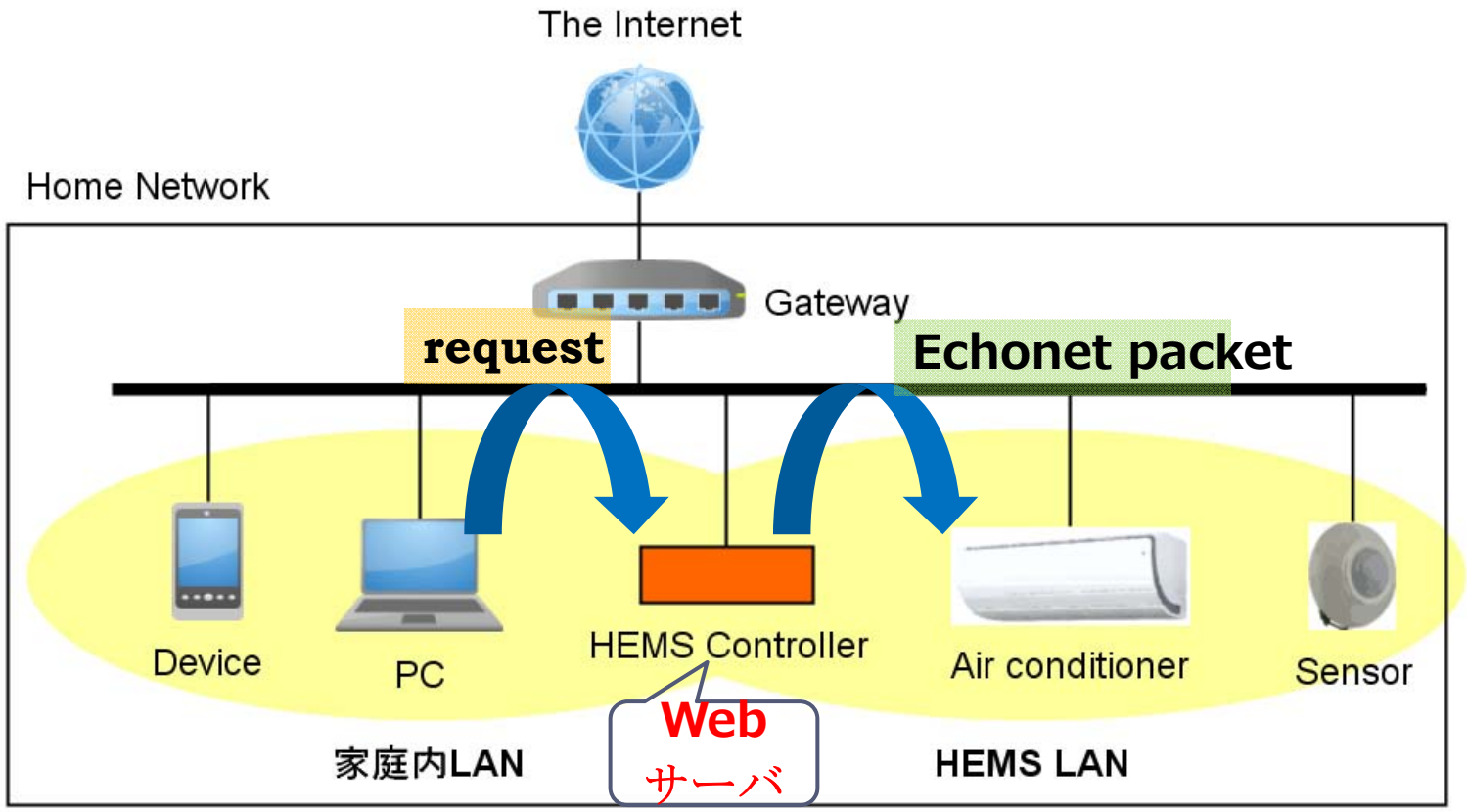
家庭内NW論理構成

- ガイドライン：各ドメインは分離(L3的に)すべき



HEMS穂来の動作

- 家電の操作、情報の取得の仕組み(LAN内から)
  - HEMSコントローラーはproxyとして動作



HEMSコントローラの役割

- 家庭内LANとHEMS LANの分離

  HEMS-スマートメーター(Bルート)運用ガイドライン [第1.0版](案) p.17より…

  - http://www.meti.go.jp/press/2013/05/20130515004/20130515004-5.pdf

  ◆ Aルート、Bルート、Cルート、一般LAN

  - L3的には分離すべき…

  →ネットワーク屋的には別物理(L2)回線

  - 家庭に4系統の物理線？

  ◆ 一体型機器を想定

  - ブロードバンドルータ(Gateway) + HEMSコントローラ

  →用途の異なるトラフィック混在の可能性

  Cルートと一般LAN混在な実装の出現

汎用化が進んだ結果...
意外なものにまで発生する脆弱性

JVNDB-2009-004384 - JVN iPedia - 脆弱性対策情報データベース

jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-004384.html

最終更新日:2012/09/25

JVN iPedia 脆弱性対策情報データベース

JVNDB-2009-004384

Jura Internet Connection Kit におけるサービス運用妨害 (DoS) の脆弱性

概要

Jura Impressa F90 コーヒーメーカー用の Jura Internet Connection Kit は、特権関数へのアクセスを適切に制限しないため、サービス運用妨害 (物理的損害) 状態となる、コーヒーの設定を変更される、およびコードを実行される脆弱性が存在します。

CVSS による深刻度 (CVSS とは?)

基本値: 10.0 (危険) [NVD値]

- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 低

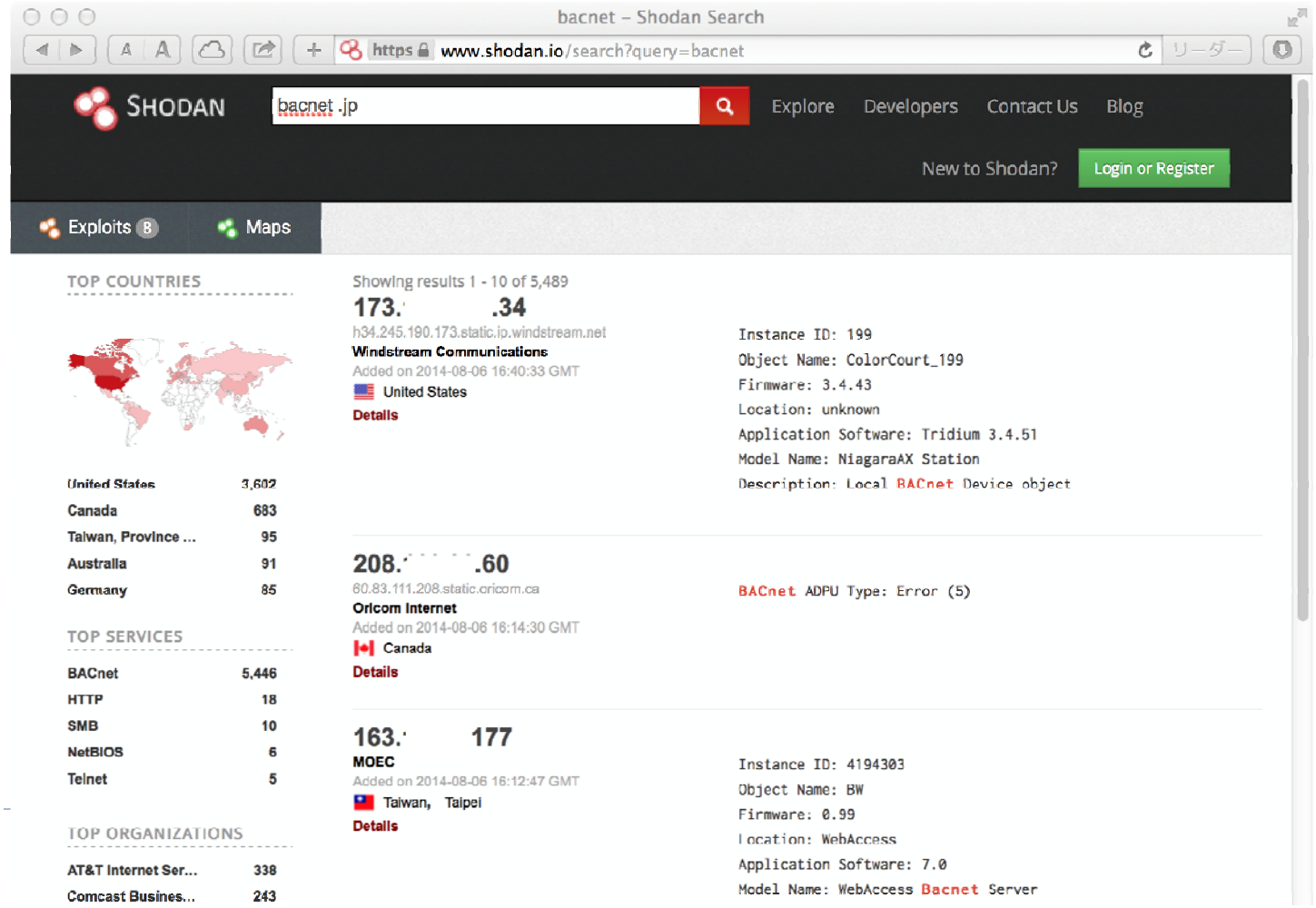
ハッカーも皆さんのすぐそばに…
お部屋の中までも…

- 電化製品の制御
  - 対象製品や制御項目の増加
  - 製品(メーカ)ごとに異なるアクセス元

  →アクセス元を制限したセキュリティ確保し難い…
  いやできない
- 電化製品の中身
  - パソコンとほぼ同じソフトウェアで構成
  - パソコンに生じる不具合も

一般公開される調査情報

- 脆弱な機器の情報も検索可能(Shodan Search)
  - 様々な目的で利用されている



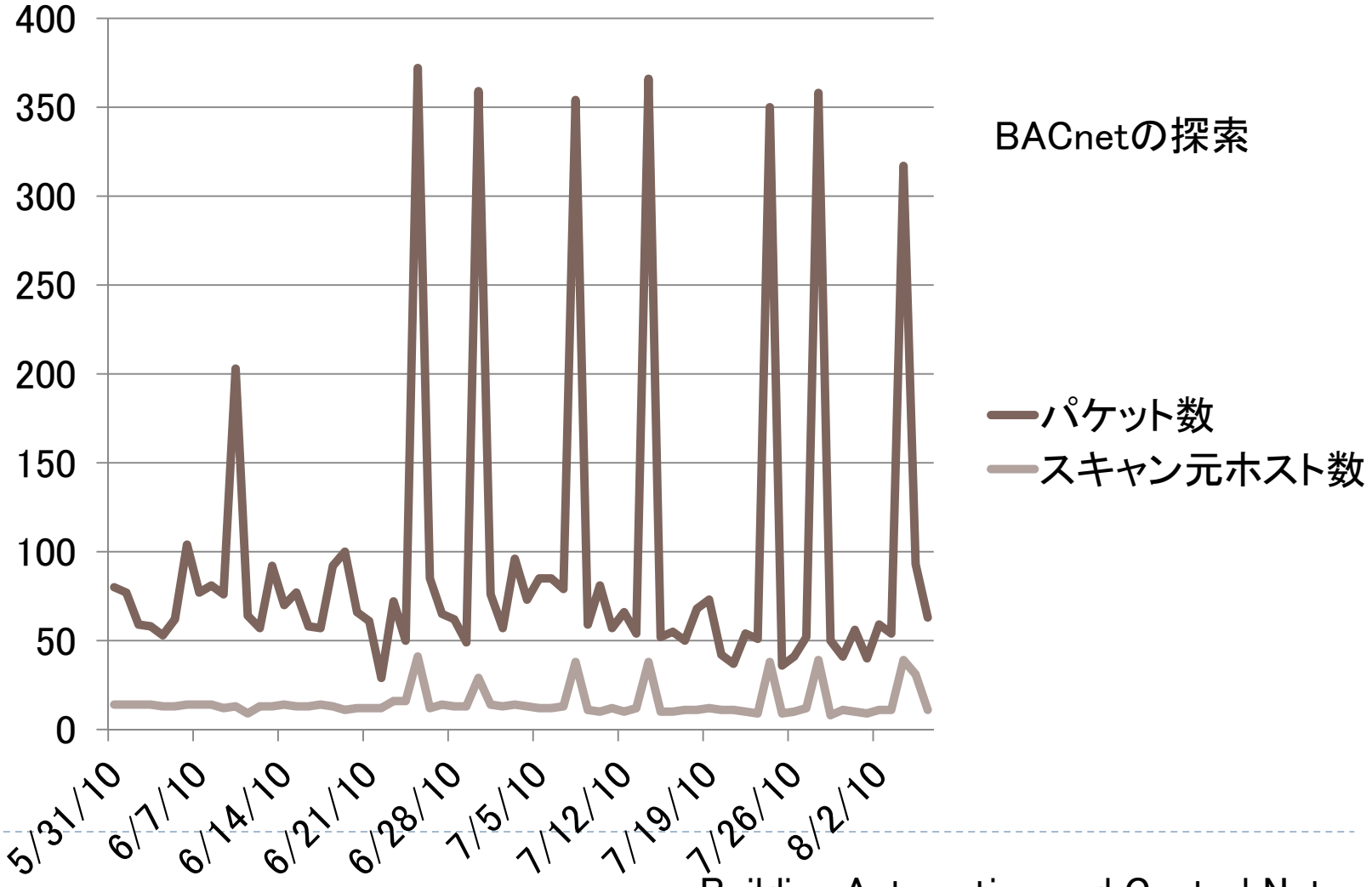
執拗なIoT機器探索

- BACnet (Building Automation and Control Network)

Receive Time	Type	Source	Source Country	Destination	From Port	To Port	IP Protocol	Application
08/07 15:09:07	end	82. 5.7	IS	133.6. 140	40000	47808	udp	bacnet
08/07 15:08:34	start	82. 5.7	IS	133.6. 140	40000	47808	udp	bacnet
08/07 15:06:29	end	82. 5.6	IS	133.6. 38	40000	47808	udp	bacnet
08/07 15:06:19	end	93. .62	RO	133.6. 211	40000	47808	udp	bacnet
08/07 15:06:06	end	82. 5.6	IS	133.6. 225	40000	47808	udp	bacnet
08/07 15:05:56	start	82. 5.6	IS	133.6. 38	40000	47808	udp	bacnet
08/07 15:05:53	end	82. 5.7	IS	133.6. 9	40000	47808	udp	bacnet
08/07 15:05:46	start	93. .62	RO	133.6. 211	40000	47808	udp	bacnet
08/07 15:05:33	start	82. 5.6	IS	133.6. 225	40000	47808	udp	bacnet
08/07 15:05:20	start	82. 5.7	IS	133.6. 9	40000	47808	udp	bacnet
08/07 15:03:26	end	82. 5.6	IS	133.6. 30	40000	47808	udp	bacnet
08/07 15:02:53	start	82. 5.6	IS	133.6. 30	40000	47808	udp	bacnet
08/07 15:02:19	end	82. 5.7	IS	133.6. 26	40000	47808	udp	bacnet
08/07 15:01:47	start	82. 5.7	IS	133.6. 26	40000	47808	udp	bacnet
08/07 15:00:06	end	93. .62	RO	133.6.	40000	47808	udp	bacnet
08/07 14:59:33	start	93. .62	RO	133.6.	40000	47808	udp	bacnet
08/07 14:59:28	end	82. 5.7	IS	133.6. 25	40000	47808	udp	bacnet
08/07 14:58:55	start	82. 5.7	IS	133.6. 25	40000	47808	udp	bacnet
08/07 14:58:40	end	93. .62	RO	133.6. 211	40000	47808	udp	bacnet
08/07 14:58:08	start	93. .62	RO	133.6. 211	40000	47808	udp	bacnet

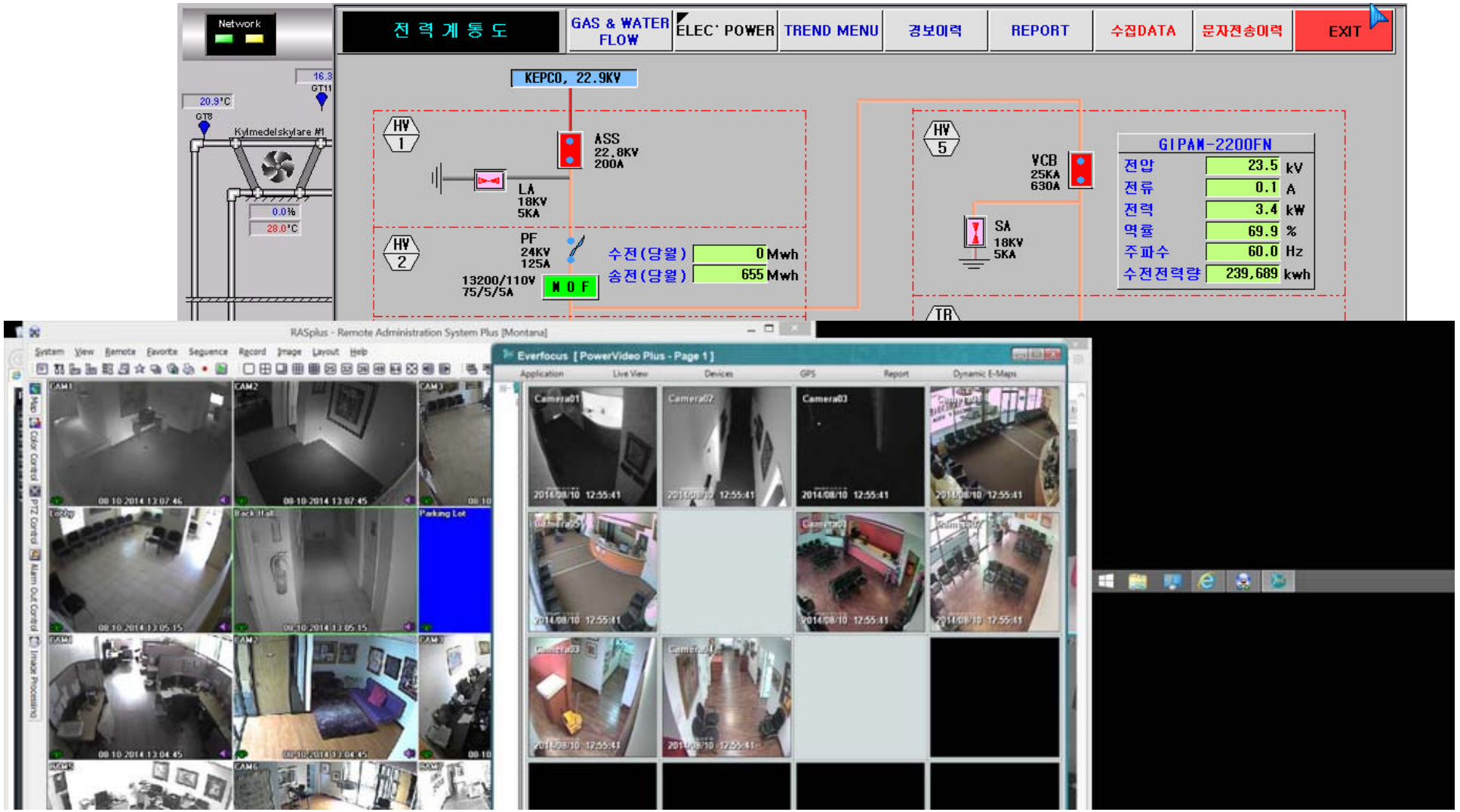
増加傾向にあるIoT探索

- 基本的に、何かが見つかりそうになると活発化



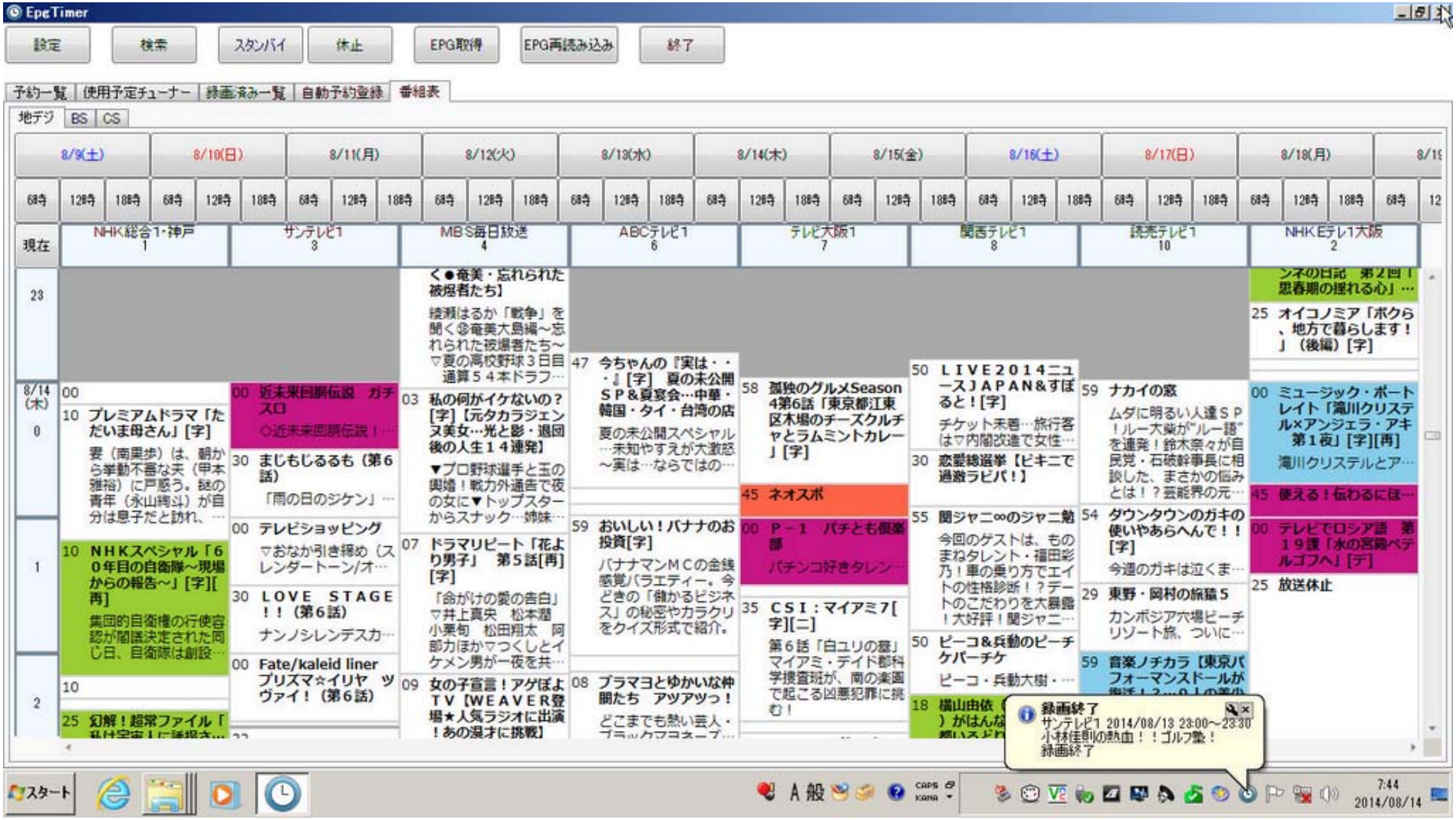
知らないうちに全世界に公開

- 海外だととんでもないものまでアクセス可能



利用者に気付かれる事なく情報流出

- 我が国での実例は少ない＆軽微だが…IoT導入の遅れ？



IoTは攻撃の敷居も下げる

- WiFiを使った信号システム
  - 緊急車両用の信号制御
- 実証実験での攻撃

  →直ぐに出て来る攻撃ツール

  後手に回る対策

  インフラ化後の改修コスト問題

Use Traffic Light Hacker to trigger a preemptive sensor on a traffic light that causes it to change from red to green.

Sometimes called a MIRT, these devices are usually given to individuals who operate emergency and police vehicles.

Now YOU can have TOTAL CONTROL of your intersections. Just point and click!

You will have to maintain a clear line of sight between your phone and the traffic light for the application to work properly, it takes about 10 seconds on usual.

This application is meant for entertainment purposes only.

Tags: traffic light hack, hack traffic light, how to hack traffic li
smart phones, how to hack traffic lights from, software for ha

スクリーンショット **Traffic Light Hacker**

http://www.telegraph.co.uk/news/newstopics/howaboutthat/4918092/Zombies-ahead-warns-electronic-road-sign.html

米国のIoT事情…公共インフラの脆弱性問題

- 3,000社以上の電力事業会社
  - 一定時間間隔での最安値競争
  - 競争激化による維持管理コスト大幅削減
    - 相互接続のための汎用性を重視
      - ✓ 汎用システム＝PC OS + PCアプリ
      - ✓ 汎用回線＝インターネット
    - 高い可用性を重視
      - ✓ 多くの接続先→認証なし/簡易な認証でのインターネット直結

- インターネット上のサイバー攻撃の影響
  - 他所へのサイバー攻撃が自分にも支障

- 第5の戦場発言
  - 戦場を作ったのは誰？

IoT製品の抱える課題

- 情報機器とは異なる製品寿命
  - パソコンやスマホ
    - 3年～5年
    - 買い替えも容易
      - ✓ データ移行ツールの普及、古いデータは廃棄？
  - IoT機器
    - 10年以上も珍しくない
    - 難しい買い替え
      - ✓ 同等機種の存在が想定できない
      - ✓ データ移行が困難
      - ✓ そもそも簡単に交換できる設置状態なのか？
        - 2000年問題再び
- IoT機器にS◯nyタイマー義務化？





一番の問題は…

- サポート体制の違い
  - 情報機器
    - (常時)オンラインな状態を想定した設計
    - ユーザが自発的にOS/firmware差分更新
    - 自動更新機能
      - ✓ 失敗時は自己責任で
    - 多いとは言ってもメーカで追跡・管理可能な規模
      - ✓ 更新後の継続利用性を重視
  - IoT機器
    - オンラインを想定できない設計
    - 保守員によるOS/firmware全更新
      - ✓ 失敗時の影響大のため
    - 自動更新は…TV系のみ？
    - インフラ化すると普及台数が半端ではない
      - ✓ IoTではセンサー一つ一つにOS搭載
      - ✓ 更新後の完全互換を保証し難い

IoTにも及ぶ脆弱性問題

- Heartbleed問題
  - OpenSSLの実装にバグ
    - 秘密情報ダダ漏れに
- 多くのIoT機器に影響

News Feed Item

Lantronix(R) Products Not Affected by Heartbleed Bug

Lantronix Products Do Not Incorporate Versions of OpenSSL Technology Vulnerable to

BY MARKETWIRED .

APRIL 10, 2014 07:29 PM EDT

ARTICLE RATING: ☆☆☆☆☆

READS: 964

RELATED | PRINT | EMAIL | FEEDBACK | ADD THIS | BLOG THIS

Why Lantronix Is Not Affected

Standard Lantronix products and firmware do not use v1.0.1 or v1.0.2 of OpenSSL, the versions that have been identified as vulnerable. Many of the company's standard products use a proprietary version of SSL that is not based on the vulnerable versions of Open SSL, while other products use other versions of OpenSSL, while still others do not incorporate SSL at all.

About Heartbleed

The Heartbleed bug is a serious vulnerability in the security software used by millions of Web sites. According to www.openSSL.org, the affected versions are 1.0.1 and 1.0.2-beta of OpenSSL, a technology that is used by many Internet services to keep user data secure.

Why Lantronix Is Not Affected

Standard Lantronix products and firmware do not use v1.0.1 or v1.0.2 of OpenSSL, the versions that have been identified as vulnerable. Many of the company's standard products use a proprietary version of SSL that is not based

- 弊社製品は大丈夫…
  - と書いていたが
  - アナウンスがない場合？

http://iot.sys-con.com/node/3053839

次々と明らかになる新たな脆弱性

- ShellShock
  - Linux由来のbash(bourne-again shell)
    - 多くのプログラムが内部で利用
  - Webアクセスするだけでプログラムを起動可能に
    - malwareのインストール、bot化、データ破壊…
- IoT機器の多くがLinuxベース
  - bashは必須機能…しかし搭載の有無の確認不可能
    - NAS(Network Attached Storage)
    - ネットワーク装置
    - テレビ会議システム
    - …未検証機多数
  - OSに比べ、組み込み系で数日の対応遅れ
    →多くの被害発生

http://www.st.ryukoku.ac.jp/~kjm/security/memo/2014/10.html#20141003_Bash

求められる対策

- 製品寿命を想定したシステム設計
  - 10年は使えるだけのハードウェアスペック

    …そりゃそうだが…非現実的
  - IoT技術(セキュリティ)は3年程度で大きく変わることを想定
    - ネットワーク接続なし or 直結なしでも動作するモードを実装
      - ✓ 遠隔設定できる機能が望ましいが、セキュリティ的に大丈夫か？
- 機器異常を想定したシステム設計
  - 本来想定すべきはずなのだが…
  - 故障機器からの異常データの扱い
    - 「機器乗っ取り＝機器故障」として扱う
    - 仕様には従っているが、異常な値(嘘つき)を検出/排除する手法
      - ✓ 多数決？

設置環境に応じた機構

- さまざまなIoT機器が同一ネットワークに相乗りする環境
  - WiFi、PLC…
- 他のIoT機器との干渉を想定した設計
  - 機器故障(乗っ取り)
    - 破損(攻撃)データの大量送信(DoS攻撃)
    - 影響を受けない or 受け難いシステム
- 相互接続の可能性
  - 想定外の値を出す機器の存在
    - これも異常機器と判断
    - ただし、使えるデータについての取扱は？
- 理想は出荷後も仕様変更できる柔軟性
  - firmware更新できるだけでもリスク軽減
    - 最悪機能停止のためのfirmware公開

安全性を考慮したIoTシステム

- 今後、組込みシステムが主流に
  - PCよりも圧倒的に長い製品寿命
    - 自動車、飛行機、家電、プラント…
  - 一旦取り付けると不具合発生時に簡単には外せない
    - 人工衛星、海底地震計、ペースメーカー
- バグを潜在させないシステム開発
  - 想定外の入力を想定する？
- 経年劣化に対応するシステム開発
  - 10年後のアップデートにも対応？
- ネットワーク接続を想定したシステム設計
  - (10年前) テレビがネットにつながるとは…