2018年11月3日（土）
JSSM 第31回学術講演会

IoTに関するセキュリティ・マネジメント

パナソニック株式会社　製品セキュリティセンター
製品セキュリティグローバル戦略室
中野　学

Panasonic PSIRT

講演者自己紹介

●中野　学（なかの　まなぶ）

●所属：製品セキュリティセンター　　製品セキュリティグローバル戦略室

●略歴：

- 2006年　横浜国立大学 博士課程 修了（情報学博士）

- 2006年～2016年：
  （独）情報処理推進機構においてセキュリティ調査・普及啓発活動に従事
- 担当は家電・自動車・医療機器等の組込みデバイス、インフラ・工場等の制御システム等

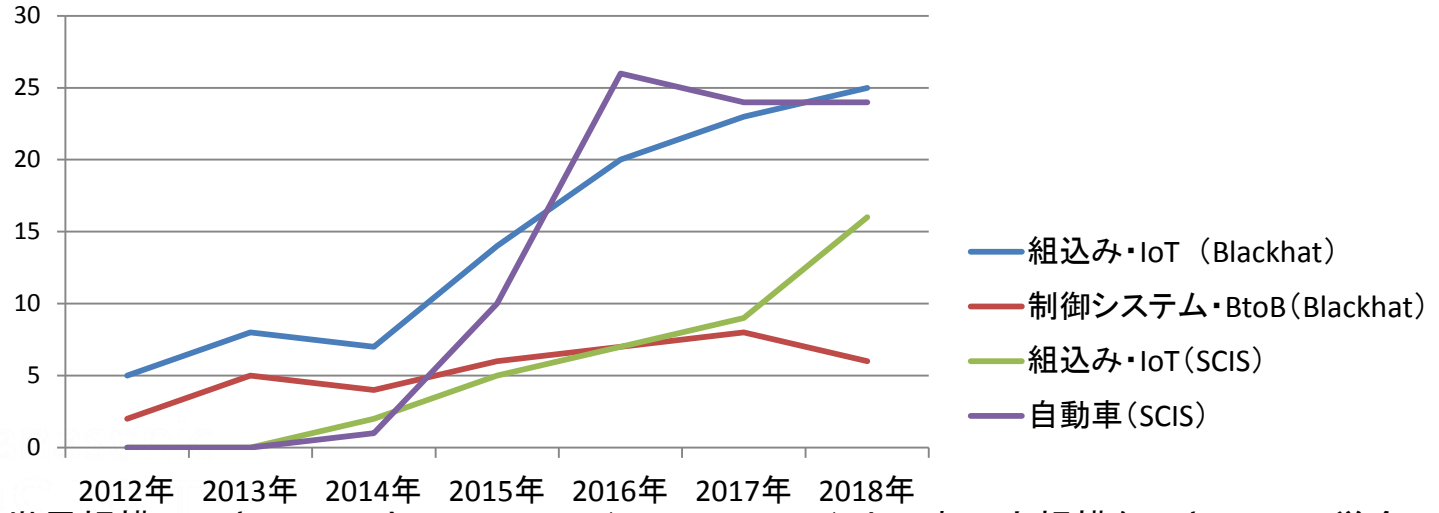
- 2016年4月から現職
- 担当は国内外の製品セキュリティ強化に向けた課題解決、方針策定等
- Panasonic-PSIRTメンバ

目次

- セキュリティが必要とされる背景について
- IoTへのアタック事例
- パナソニックの取組み
- PSIRTの活動
- まとめ

セキュリティが必要とされる背景について

はじめに・・・　IoTセキュリティの変化



- グラフは世界規模のセキュリティカンファレンス（Blackhat USA）や日本の大規模なセキュリティ学会での過去5年の発表件数の推移。
- IoTを含む組込みセキュリティ、工場やBtoBを含む大規模サービスセキュリティへの攻撃者・研究者の興味が高まっている。
  - 自動車のセキュリティ研究・発表は、プレイヤーが定まった感があり、発表件数や注目は高いながら、落ち着いてきた傾向に。
  - IoTは研究対象が組込みソフトから、ハードやセンサーまで裾野が広がる。

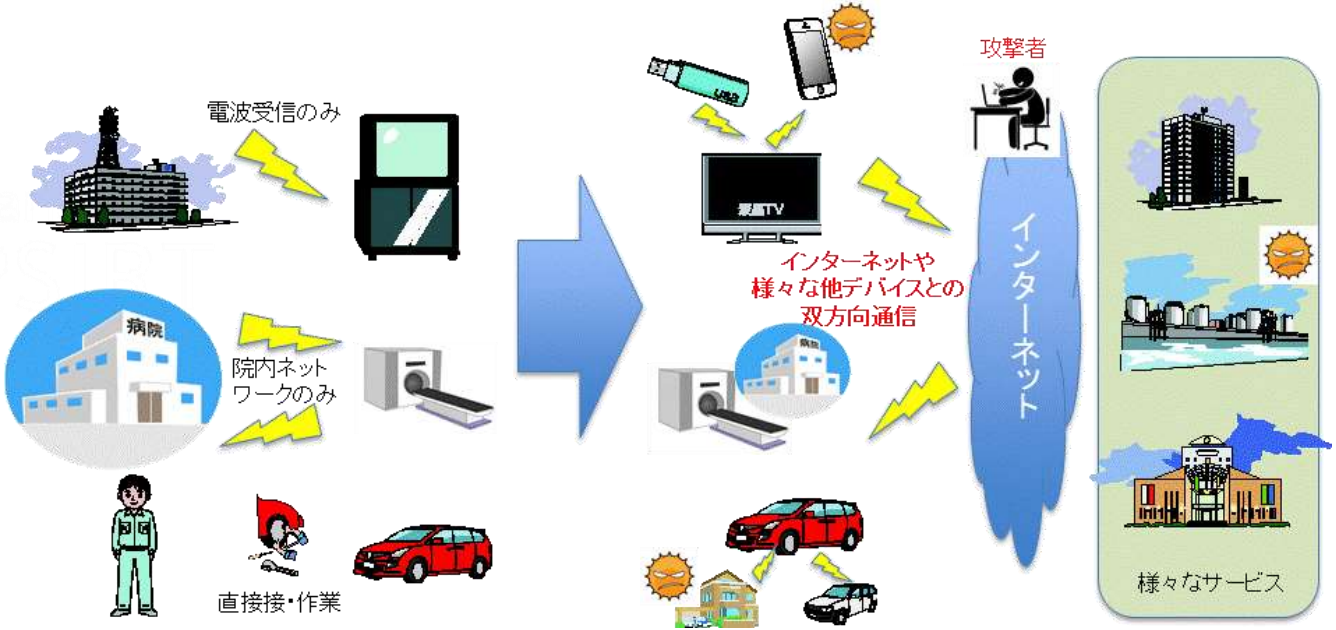
IoTの進化とそれに伴うセキュリティの必要性向上

- 「攻撃者」の視点から見たIoTの進化に伴う狙い所
  - 外部への接続機能
  - 新しいサービスの発達
  - 共通仕様の利用

IoTの進化とそれに伴うセキュリティの必要性向上

●外部への接続機能

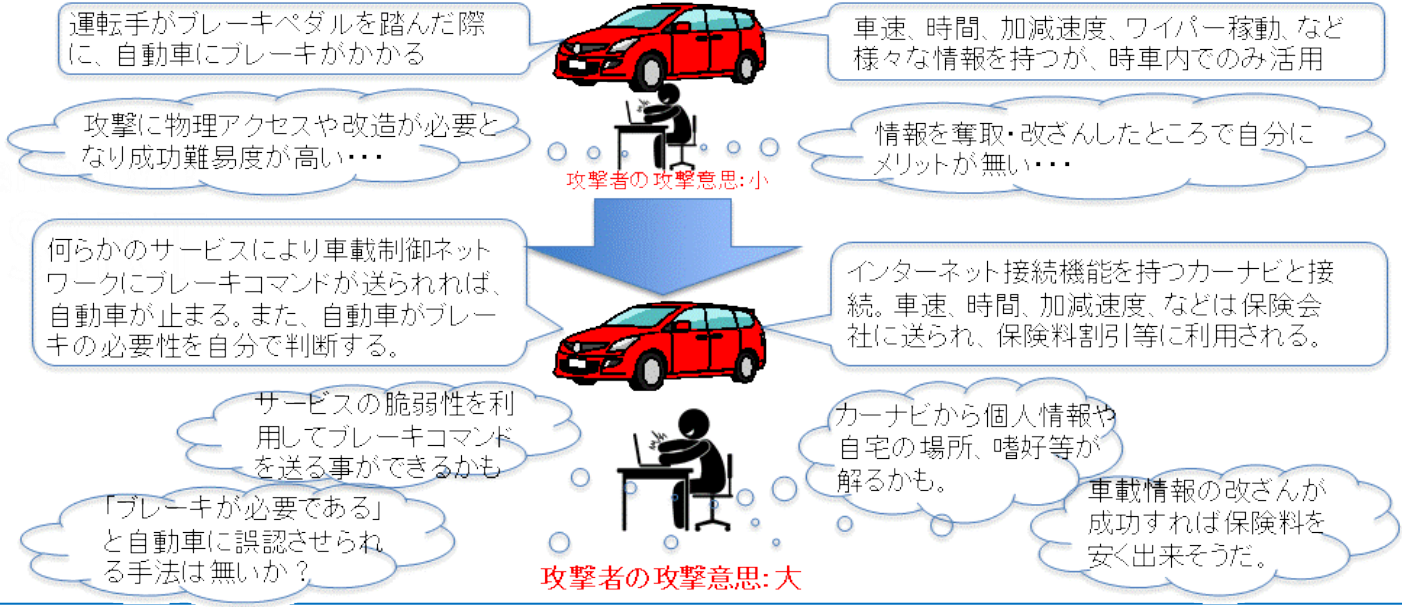
従前の仕様では、外部からの攻撃が考慮されていなかった製品が、今後は攻撃対象となる可能性がある。機器へのアクセスポイントが増えるほど、可能となる攻撃の種類も増加する。



IoTの進化とそれに伴うセキュリティの必要性向上

●新しいサービスの発達

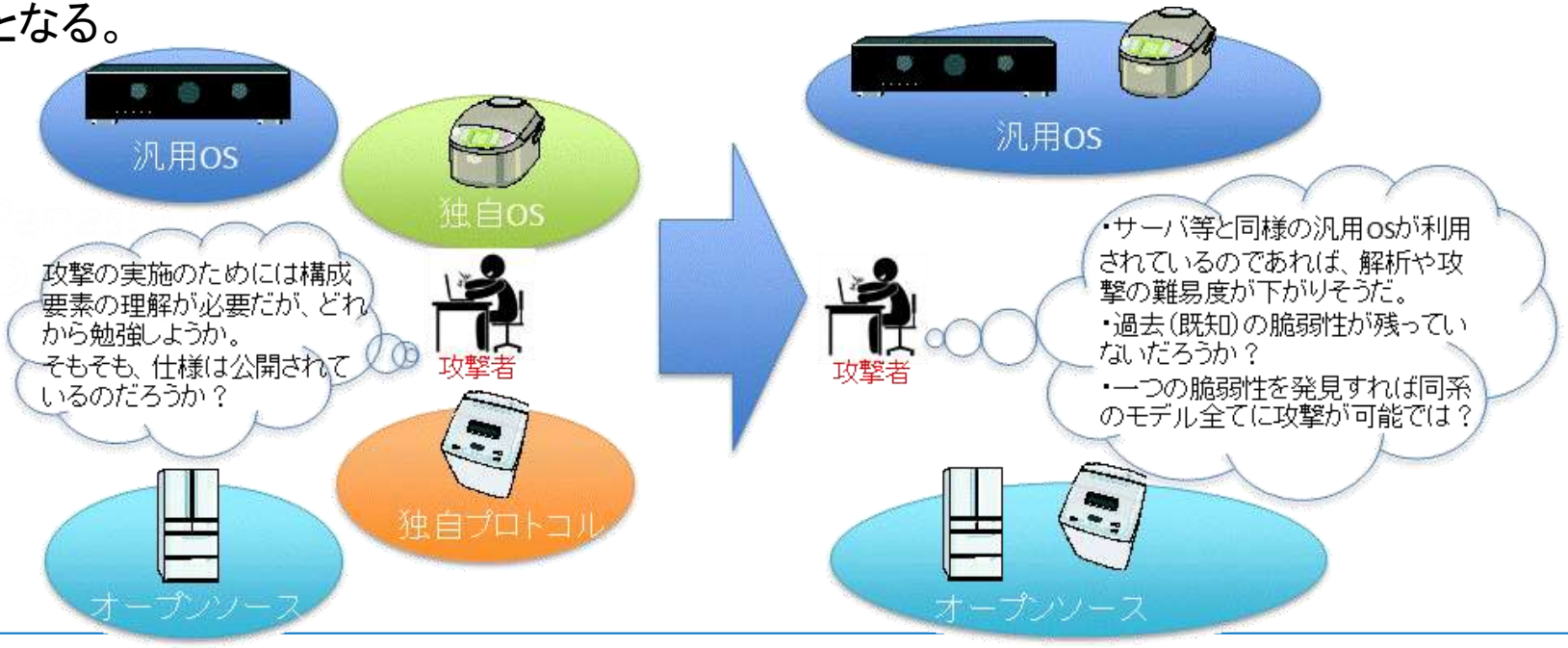
情報の価値の変化に応じて、流行となる攻撃対象や手法が変化することが考えられるため、最新情報を追い続けなければならない。また、サービスの充実等によって情報の価値が上昇すると、攻撃者のモチベーションも向上する。



IoTの進化とそれに伴うセキュリティの必要性向上

●共通仕様の利用

プロトコルや仕様における脆弱性が発見された場合、影響が広範囲となる可能性がある。また、破壊を伴う解析によって得られた情報によって、他の機器を攻撃するといった事も可能となる。

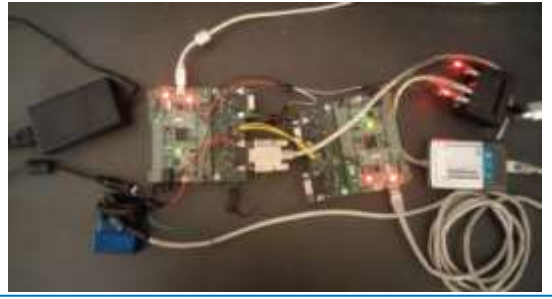


攻撃者のバックグラウンドとモチベーション(1/3)

- バックグラウンド
  - IoTハッキングを目的としたコミュニティの醸成
    - IoT・自動車等を専門とした ハッキングセミナーの公開
    - 大規模カンファレンスで 専門ルームを設置

2017年度
Blackhat/DEFCONの様子

  - 様々な解析ツール、解析ソフトが流通
    - 従来PCのソフトウェアに利用されていたものをIoT向けにカスタマイズ
    - 安価(20＄～30＄)又はフリーの商用・自作ツールも多数存在



2016年・2017年に紹介された自動車のハッキングツール・ソフト

攻撃者のバックグラウンドとモチベーション(2/3)

- バックグラウンド
  - 高機能なIoT製品が安価に複数種類入手可能に
    - 物理的な解析が可能
      →基盤へ直接タッピング等、攻撃の幅が広がる。
      故障・破壊しても次がある。
    - 多数の類似する機器でチャレンジ可能
      →特定の機器を攻撃したいのでは無く、自らの攻撃手法の実用性を証明したい

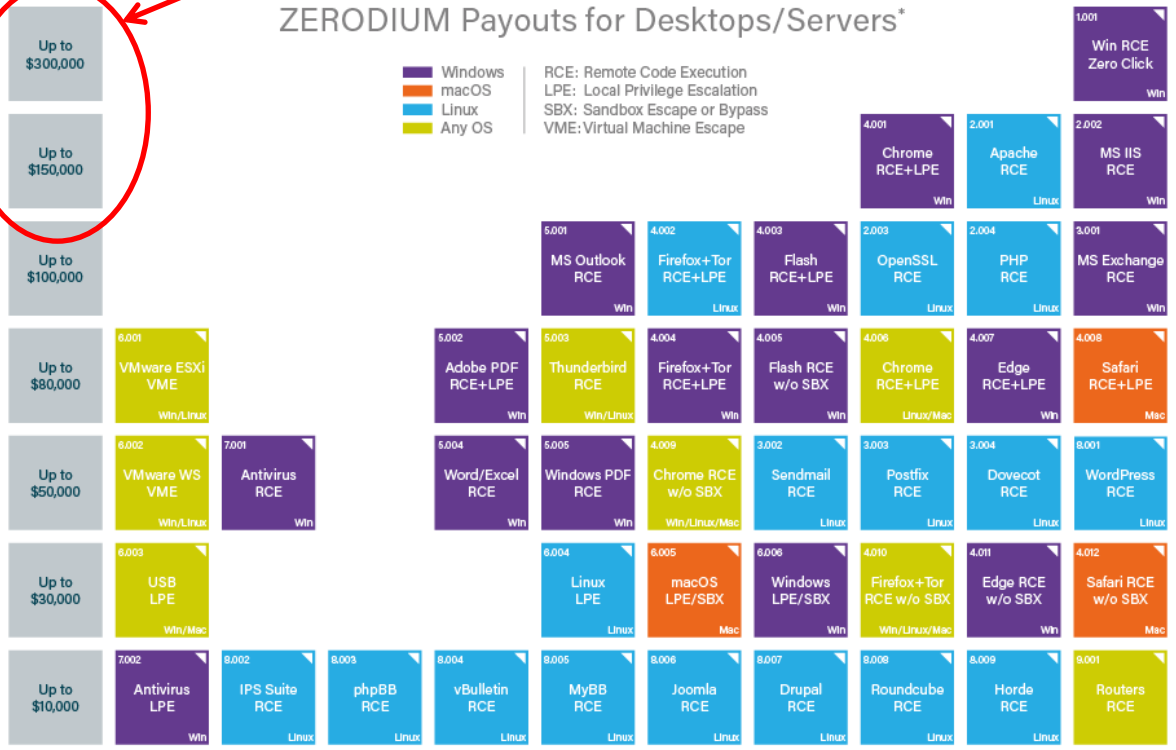
2016年・2017年Blackhat/DEFCONのスライドより

2016年・2017年に紹介された自動車のハッキングツール・ソフト

攻撃者のバックグラウンドとモチベーション(3/3)

- モチベーション
  - 「お金」:実益としてのIoTハッキング
    - ハッキングコンテストや
      バグバウンティなど、
      脆弱性の発見が賞金に。
    - DarkWebのような
      ブラックマーケットでも
      脆弱性関連情報が売買。
      →脆弱性もその影響度や
      深刻度によって市場原理が
      働き、価値が変動する。
    - 脆弱性発見・報告の
      懸賞金によって生計を立てる
      通称「バグハンター」も

ゼロデイ(未発見)の脆弱性報告で
日本円にして1600万円～3200万円以上



IoTへのアタック事例

IoTセキュリティの現状

- 【Picking Bluetooth Low Energy Locks from a Quater Mile Away】
- Bluetoothを使用して動作するスマートロックの解除に挑戦
  - 16種類のスマートロック製品を調査
    →12種類の製品のハッキング成功
- 攻撃成功したものはセキュリティ対策が稚拙
  - パスワードを平文テキストで通信
  - 開錠データを傍受・再送する事でも開錠
  - 特定のデータを受信すると開錠（デフォルト）状態に移行
- ハッキングできなかった錠の特徴
  - パスワードの長文化（16-20文字）及び安全な管理
  - 適切なAES暗号化
  - 多要素認証の選択

講演スライドより
（出展：https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Rose-Ramsey-Picking-Bluetooth-Low-Energy-Locks-UPDATED.pdf ）

物理セキュリティデバイスのソフト面で未熟な部分が存在

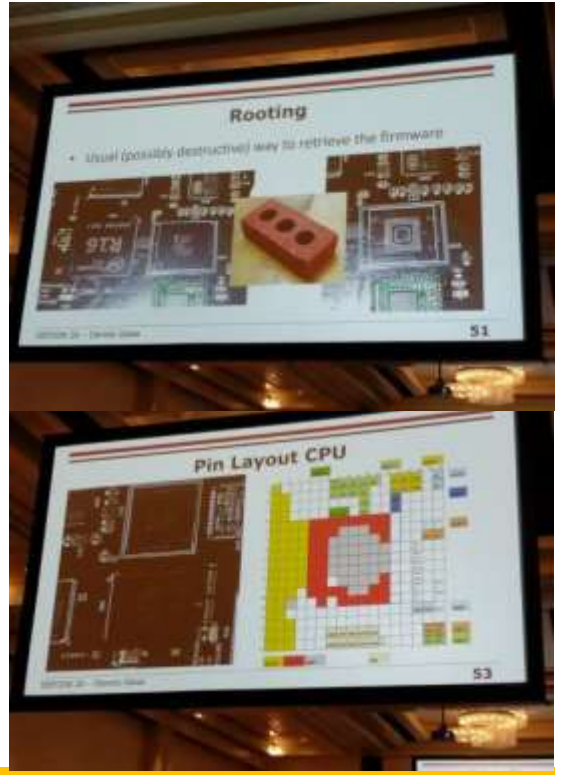
「モノ」を手に入れやすいからこその攻撃

- 【All Your Things Are Belong To Us】
- 22種類のデバイスに対するハッキング成功事例
  - スマートテレビやWebカメラ、ストレージ、WiFi AP等
  - 発表者はexploitee.rsメンバ（ロシアのハッカー集団）
  - 3年前にも大量のデバイスに対するハッキング報告
- 脆弱性の半分（11機種）はハードウェアハッキング
  - 物理接続を利用したRoot権限の取得やメモリ書き換え可能等
  - その他の脆弱性は、不要なポート（特にTelnet）からの不正ログインやアプリの脆弱性等

不要なポートの停止、物理接続への耐性確保が必要
攻撃口を推測する事を困難にする手立ても有効

ロボット掃除機のハッキング

- Xiaomiのロボット掃除機を分解して
  ハードウェアやファームウェアを解析
  - 他の製品のソフトウェアが再利用されており、解析が容易
  - 物理的なテストポートが残存しており、攻撃者にも利用可能
  - メモリ等に空き領域があるため、悪意ある攻撃者が
    マルウェアを埋め込んで転売する事で、第三者の生活を
    盗み見る事の危険性も指摘
  - Xiaomaiセキュリティチームには報告済みで、
    本脆弱性は修正済み



**脆弱性を含んだIoTデバイスが、ソフトウェア的に改造され、
中古市場に流れることも大きな脅威に**

複数の脆弱性の組み合わせによる攻撃事例

●ビジネス用複合機（HP-Officejet Pro）に対するハッキング

- Web上に公開されている古いファームウェアを入手・解析
- 既に公開されていた脆弱性を解析の足がかりに利用
- 内部構造を調べた上で以下の二点を確認
  - FAXの規格「T.30」が受診データを無害化せず、そのまま保存する仕様に
  - HP社の独自ソフトウェアに脆弱性があり、最終的にリモートコードの実行が可能
- 結果としてFAXを送るだけで複合機にコマンドを送る事が可能となり、乗っ取った複合機経由で社内PC等へのマルウェア感染も可能

<u>複数の脆弱性が組み合わさる事で、被害に繋がる事も</u>

IoTを狙ったマルウェア(1/2)

- 2016年10月にIoT機器に感染するマルウェア「Mirai」が登場
  - ネットワークカメラ等、脆弱なIoT機器が15万台感染。感染した機器が攻撃者となる。
  - 感染した機器が一斉にTwitter、Amazon等のWebサイトを攻撃(DDoS攻撃)し、一部のサービスがダウン。攻撃トラフィックは700Gbpsにも。
  - マルウェア「Mirai」は開発者の手によってソースコードが公開されており、誰でもが亜種を作れる状態に。

- 感染が広まった原因は？
  - Telnetポートがオープン
  - ID/Passwordのハードコード
    - 「Mirai」に感染したとされる中国の電子機器メーカーは防犯カメラやIPカメラのリコールを表明。ID/Passwordのハードコードにより、回収以外に修正方法が存在せず。

出展：https://cybersecurity-index.com/2016/10/29/mirai-iot-botnet-software/

IoTを狙ったマルウェア(2/2)

- マルウェア「Mirai」はパナソニック製品も標的としていた。

```
123     // Set up passwords
124     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
125     add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root     vizxv
126     add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
```

中略

```
176     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16", 1);                      // admin    1234
177     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16\x17", 1);                  // admin    12345
178     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x17\x16\x11\x10\x13", 1);                  // admin    54321
```

IP Cameras Default Passwords Directory

Author: Ethan Ace, Published on May 28, 2016

Finding an IP camera's default password can be tedious or aggravating. And keeping up with changes in newer firmwares can be difficult, especially for occasional users.

With that in mind, we have gathered this list of IP camera manufacturers and thei usernames and passwords to help users get started more quickly. After the list changes by manufacturers as well as password security issues.

[Don't miss downloading our free IP video surveillance book.]

- Mobotix: admin/meinsm
- Northern: Previously admin/12345, but firmware 5.3.0 and up requires unique password creation
- Panasonic: Previously admin/12345, but firmware 2.40 requires username/password creation
- Pelco Sarix: admin/admin
- Pixord: admin/admin

マルウェアで社会にインパクトを与えられる事が実証された為、今後のIoTマルウェアの流行にも注意が必要

・・・そして規制へ

- 2018年総務省が通信機器の「技術基準適合認定（Tマーク）」にセキュリティ要件を入れる方針決定。
  - 方針については7/30でパブリックコメントが締め切られコメントの反映の後、規制改定へ
  - Tマークを取得する製品は以下のセキュリティ要件を満たす必要がある
    - アクセス制御機能の導入
    - アクセス制御にID/パスワードを利用する際は、初期値から変更する仕組み等
    - ファームウェア更新機能

今後もインパクトを与えたセキュリティインシデントを受けて対策となる規制が提案・議論、決定される可能性も

社会インフラに影響を及ぼしかねない脅威に対して有用な一方で、
今後も多様な製品・サービスが創出されるIoT業界において、規制で縛ることが、どこまで効果的に稼動するだろうか？

ランサムウェア（1/2）

- 2016年末から2017年にかけてランサムウェアが流行
  - Windowsの既知（修正済み）の脆弱性を狙う「Wannacry」
  - 国内外の工場が停止した事例も
    - ホンダ狭山工場、日産サンダーランド自動車工場、ルノー子会社
    - 日立グループは社全体に影響
    - 欧州の石油化学工場では、Wifi機能を持つコーヒーメーカの設定ミスで本来クローズドなネットワークに感染した事例も（2017年8月）

サンフランシスコの地下鉄
（2016年11月）

アメリカのスマートTV
（2016年12月）

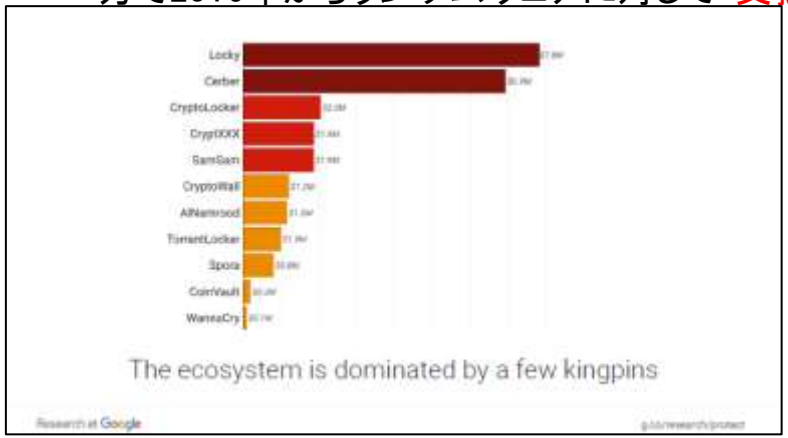
オーストリアのホテル
（2017年1月）

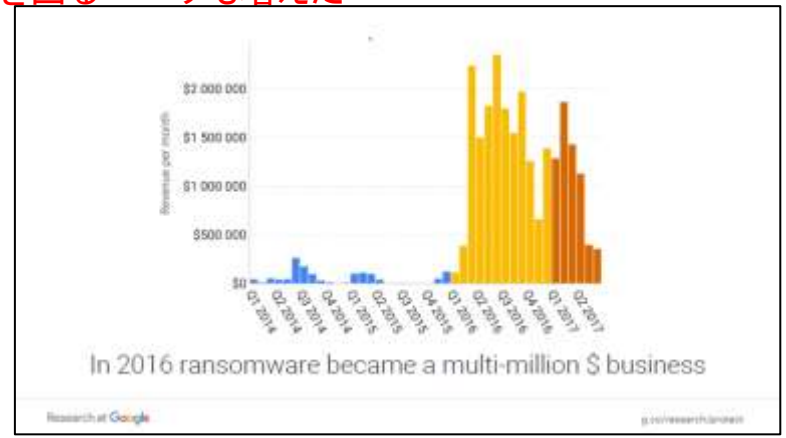
タイのサイネージ
（2017年1月）

2016年末からランサムウェアは様々な機器を対象に猛威を振るう

ランサムウェア(2/2)

- ランサムウェア作成者のモチベーション
  - 3年半34種類約15万件のランサムウェアによる資金の流れが公表(Blackhat USA 2017)
    - 大きく稼いだLocky(8.7億円)、Cerber(7.7億円)は共にメールやWeb経由
    - WannaCryは約1千万円と、他に比べて小額
    - 一方で2016年からランサムウェアに対して「支払って解決」を図るユーザも増えた





ランサムウェアの作成・配布が稼ぎとなる事が明らかに
次はどのような対象を、どうやって狙うかが焦点

脅威が実害となるのはいつ？（1/2）

2015年には自動車を遠隔操作可能な攻撃手法が報告され話題に

クライスラー社のCherokeeに搭載されている車載機Uconnectに脆弱性があり、また、UconnectにはIPアドレスが割り振られていた為、遠隔地からの攻撃が可能となった。

オンラインアップデートが出来なかったため、影響ある140万台に対してリコールが発生。リコール費用だけではなく、メーカの株価にも影響が出た。

（引用：2015年 Blackhat DEFCON講演資料より）

自動運転への機運が高まる中、ハッキングで遠隔操作可能な事例が現れたことは自動車ハッキングの機運を上げる結果に

脅威はいきなり顕在化するのか？

元を探れば2010年頃から脈々と研究されてきた集大成

2010年の段階でワシントン大学のKohno氏によって、ハッキングにより自動車の遠隔操作となる論文が発表される。ただし、当時は攻撃に使う機器が市販製品では機能不足で開発を要するなど、攻撃の敷居が高かった。

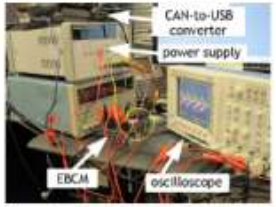


Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (EBCM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.

Figure 7. Road testing on a closed course (a de-commissioned airport runway). The experimented-on car, with our driver wearing a helmet, is in the background; the chase car is in the foreground. Photo courtesy of Mike Haslip.

（引用：http://www.autosec.org/pubs/cars-oakland2010.pdfより）

自動運転への機運が高まる中、ハッキングで遠隔操作可能な事例が現れたことは自動車ハッキングの機運を上げる結果に

過去の事例に学ぶ事は重要

脅威が実害となるのはいつ？(2/2)

- 2010年：Stuxnet：スタンドアロンな産業用制御システムへのワーム感染
  - →2017年：攻撃口や手法、目的について整理がされ始める
  - →20XX年：よりクリティカルな攻撃が実現し、業界がホットになる。

どこかで
見たような？

自動車に
機器を取り付けて
攻撃など
ナンセンス

自動車に通信
機能は搭載さ
れない

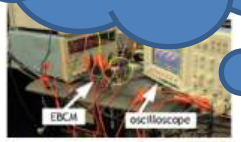


Figure 1. Example bench setup within our lab. The Electronic Brake Control Module (ECBM) is hooked up to a power supply, a CAN-to-USB converter, and an oscilloscope.

Figure 7. Testing on a closed course (a de-commissioned airport runway). The experimented-on car, with our driver wearing a helmet, is in the background; the chase car is in the foreground. Photo courtesy of Mike Hastip.

2010年：米国の研究者によって、自動車ハッキングの可能性が示される

2014年：
攻撃の情報が
整理される

自動車の
高機能化

2015年：リモートアタックが成功
リコール発生

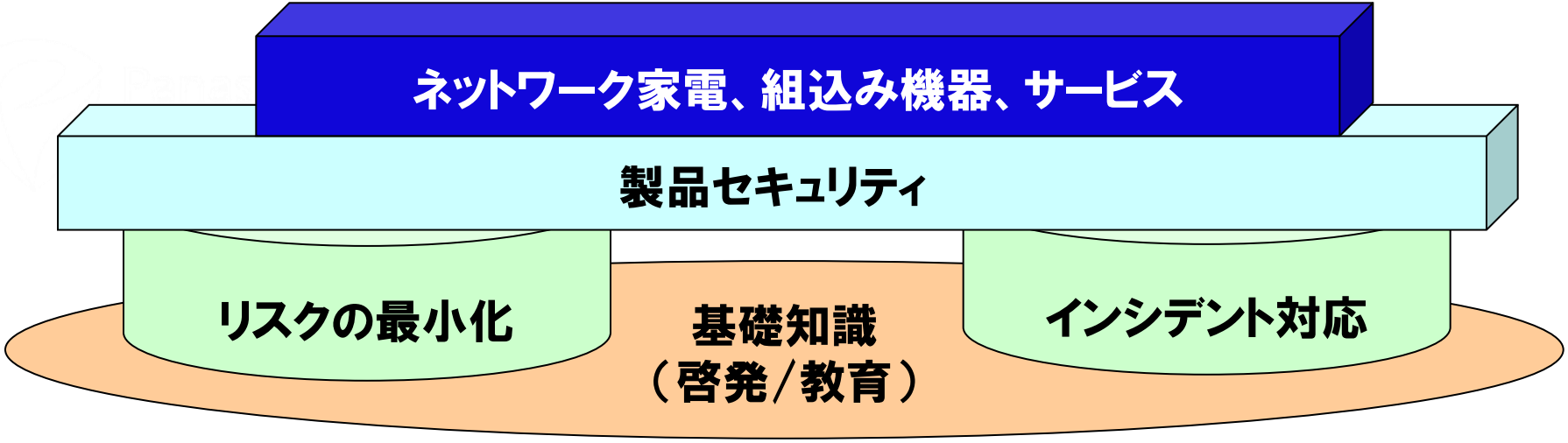
攻撃や対策技術がホットになる「流れ」がある？

パナソニックの取組み

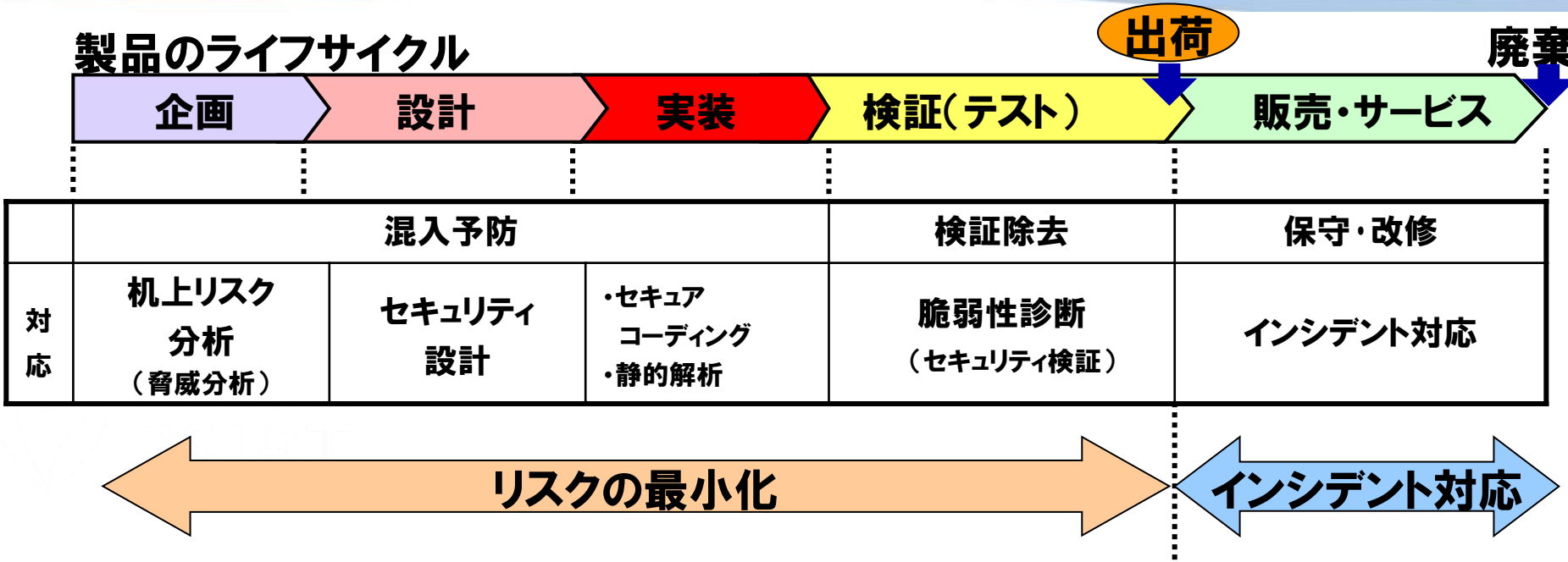
Panasonicにおける脆弱性撲滅に向けた取組み

家電を含む製品のセキュリティ向上はPanasonicを支える重要な要件の一つ

- 製品セキュリティに関する基礎知識という土台
- 二本の柱で製品セキュリティを支える
  - リスクの最小化
  - インシデント対応



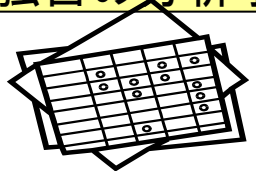
製品ライフサイクルに沿った対応



製品のライフサイクル全般において対応が必要

机上リスク分析（脅威分析）

製品企画および設計の初期段階において
- 想定される脅威への対策を検討
- 検討した対策をセキュリティ要件として設計に入力
- ISMSをベースに独自の分析手法を開発、運用



リスク分析ワークシート

製品の機能を列挙

企画書
仕様書
設計書
・・・

機能が扱う資産を特定

資産に対する脅威を検索

脅威DB

資産と脅威からリスクを定量化

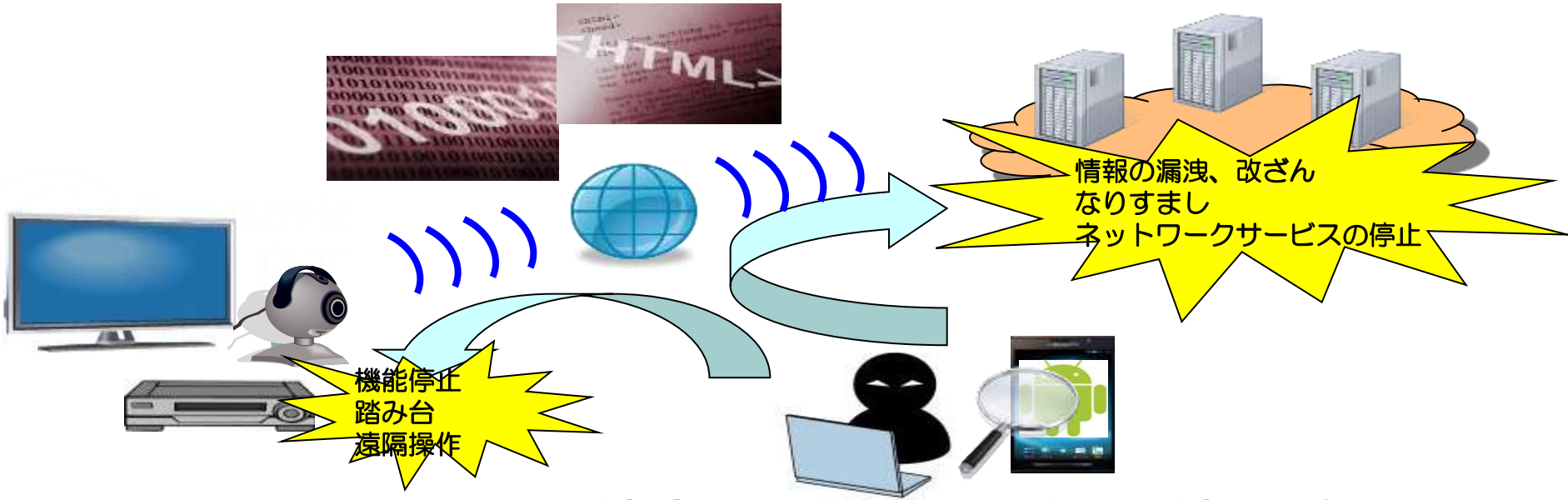
評価基準

脅威への対策を検討

対策例

脆弱性診断（セキュリティ検証）

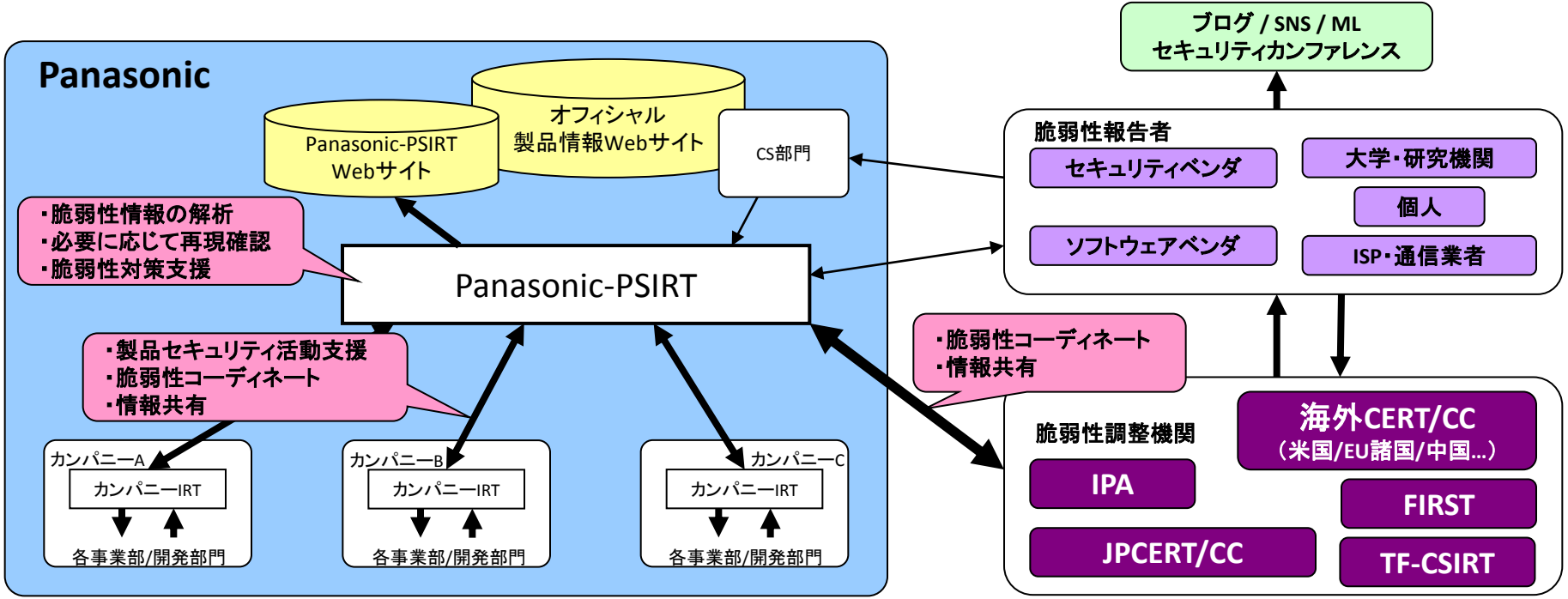
実装および検証（テスト）段階において
- 脅威分析・セキュリティ設計段階で設計された仕組みの確認
- 実装段階で混入する脆弱性を抽出・改修



攻撃者と同じ手法・ツールで製品を攻撃して診断

インシデント対応

インシデントに関する迅速な対応を実現するため
- 社内外との連携・調整の窓口「Panasonic-PSIRT」に一本化
- グループ内分社(カンパニー:複数の事業部の集まり)毎にカンパニーIRTを設置



Panasonic PSIRTの取組み

PSIRTの業務一例

届出・相談対応

脆弱性の
対応方針の策定

開発現場との
調整

PSIRTメンバー例

情報収集

関係者との
良好な
関係構築

通常業務

PSIRTとして必要な心がけ(1/2)

- PSIRTとして一番重要なのは「確実な情報」
  - 風評やメディア、有識者のコメント等に惑わされず確固たるエビデンスを基に判断を下す必要がある
  - 常日頃から手広い情報収集を
    - 必要となる知識は「セキュリティ」だけとは限らない
    - 多様な「専門家」との繋がりは重要
  - 結論・判断根拠は簡潔に。
    - 「上手く伝える」スキルは必要
    - それを支える情報は前広に。

PSIRTとして必要な心がけ(2/2)

- 組織としてのPSIRT
  - 「脆弱性がある、直せ」というだけなら、PSIRTにセキュリティ専門家は必要ない。
  - 脆弱性の質や、商品・サービス内容、開発現場の状況を踏まえた上で、修正に向けた最適解を求め続ける事が必要。
  - 何より怖いのは、「パニック」や「焦り」。冷静に収束に向けた行動を実行に移していくことが大事。
  - 原因の追究以上に、「再発させない」仕組み作りを。

まとめ

まとめ

- 攻撃は、日々行われている
  - 顕在化した攻撃が全てでは無く、脆弱性の発見・対策実施は水面下で常にある
  - 攻撃の「仕込み」は既に行われている可能性も
- 攻撃の手口は、日々進歩・多様化・巧妙化している
  - 技術の高度化により、将来は想定し得ない攻撃が存在する可能性も
  - だからこそ今から、脅威の芽をなるべく摘み取っておく必要がある。
- 攻撃の動機や対象も変化してきている
  - カメラ等のセンサー情報や、モノの動きに関わる脆弱性を狙うのが今の流行
  - ランサムウェアのように「システムを止められる攻撃」はお金に繋がりやすい

IoTデバイスやシステムは、必ず「攻撃される」という意識を持って、設計・開発・施工・運用を行う
また、有事の際の対応体制も整備する

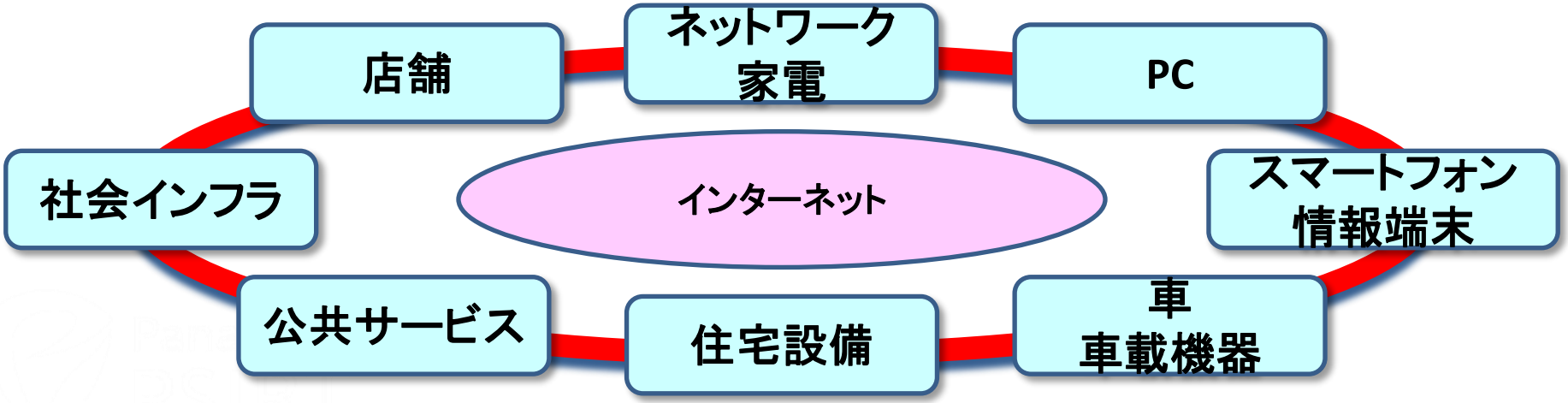
AIと製品セキュリティ

- 2016年 米国でCyber Grand Challenge（CGC）開催
  - 米国DARPAが主催でこの年に初めて実施。
  - 3年の準備期間、予算5500万ドルを投入。
  - 自動化されたプログラム同士で、脆弱性の発見、攻撃及びその対策を競い合う競技。
  - 予選を勝ち抜いた104チームの内7チームが、準備金75万ドルを基にシステムを開発。
  - 優勝チームはカーネギーメロン大学のForAllSecureチームのシステム「Mayhem」、優勝賞金200万ドル。

製品セキュリティの確保には、様々な観点から分析・診断が必要となり、既に膨大な工数が求められている。
セキュリティにAIを利活用していくことは、セキュリティ対策を実施する現場としても、コスト削減や、より「人がやるべき事」への集中に繋がる。

さいごに

- 数十億といわれるIoT(Internet of Things)がつながる時代



- セキュリティ専門家だけの取組み・視点ではセキュリティ確保は困難
- テクニカルな課題だけでなく、ソーシャルな課題も
- 業界/業種/立場を超えた取組みが必要

みなさんの英知を結集してIoTのセキュリティを考えましょう！

御清聴、ありがとうございました。

パナソニック株式会社
製品セキュリティセンター
製品セキュリティグローバル戦略室
中野　学
Email : nakano.manabu@jp.panasonic.com