第22回日本インターネットガバナンス会議

Internet Week 2017
IoTセキュリティセッションの
論点は何だったのか？

2017.11.30

情報通信研究機構 サイバーセキュリティ研究室

上席研究技術員

久保 正樹

国立研究開発法人
情報通信研究機構

自己紹介

- 久保 正樹（くぼ まさき）
- 情報通信研究機構 (NICT) サイバーセキュリティ研究所 サイバーセキュリティ研究室
  - **Darknet & Livenet** 解析チームリーダー

- 他にも
  - **Internet Week 2017** のプログラム委員
  - **JPCERT** コーディネーションセンター専門委員兼共同研究員

今日のお話

- 昨日の Internet Week 2017 のセッション「**S10 転ばぬ先のIoTセキュリティ〜コウカイする前に知るべきこと〜**」の発表を振り返り，IoT セキュリティのキーワードを考えたいと思います．

[今週のニュース] マルウェア感染する IoT 機器の急増

- 国内でマルウェア感染するIoT機器が急増
  - 約1万8000台（NICT 観測）
  - Miraiの新たな亜種の疑い
- 感染機器は？
  - ブロードバンドルータ
  - ネット家電等
- 感染の原因は？
  - **機器の部品に存在する脆弱性**
  - デフォルトパスワード

ＩｏＴ機器を狙うウイルス感染 100倍に急増 先月から

11月26日 16時56分　IT・ネット

さまざまなものをインターネットに接続する「ＩｏＴ」の普及が進む中、日本国内でＩｏＴ機器を狙ったコンピューターウイルスの感染が今月に入って先月の１００倍に急増し、大規模なサイバー攻撃の危険が高まっていることが、大手通信事業者の調査でわかりました。

NHK NEW WEB の報道（2017年11月26）

海外（アルゼンチン）でも同時期に感染が拡大

ISPがユーザに配布した**ルータに脆弱性**
- telnet / デフォルトパスワード
- ハードコードされた su パスワード

↓

2017-10-31
脆弱性のPoC（user/password）が公開

↓

（推測）
Mirai の亜種にPoCが実装される

↓

2017-11-22
当該機器が感染.
感染機器からのスキャンを観測

Early Warning: A New Mirai Variant is Spreading Quickly on Port 23 and 2323

24 NOVEMBER 2017 on IoT Botnet, Mirai, ScanMon, New Threat, Botnet Measurement

[Updates on 2017-11-28]

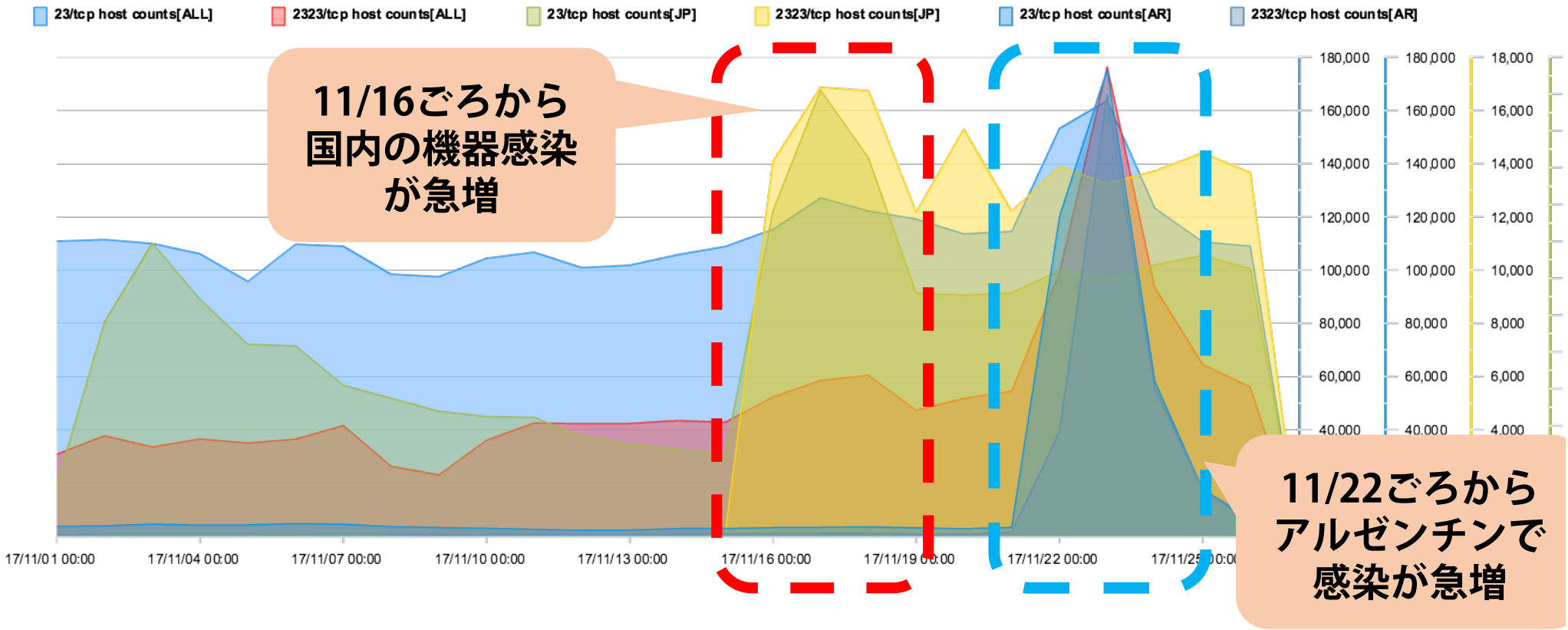
- Both C2s have been sink-holed now by security community.
- admin/CentryL1nk is a typo for admin/CenturyL1nk.

About 60 hours ago, since 2017-11-22 11:00, we noticed big upticks on port 2323 and 23 scan traffic, with almost 100k unique scanner IP came from Argentina. After investigation, we are quite confident to tell this is a **new mirai variant**.

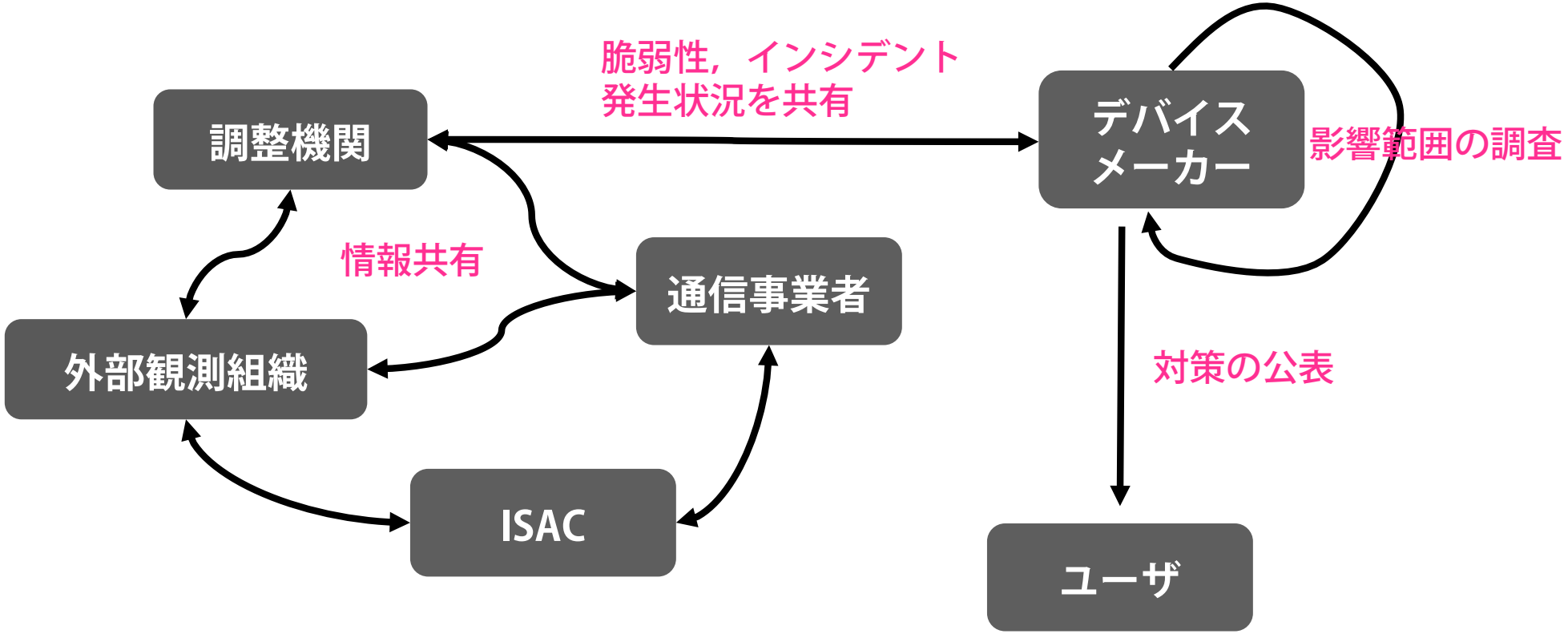
360 NetLab による分析レポート

感染したIoT機器からのスキャン

スキャン元IPアドレス数の増加 ≒ **感染機器の増加**



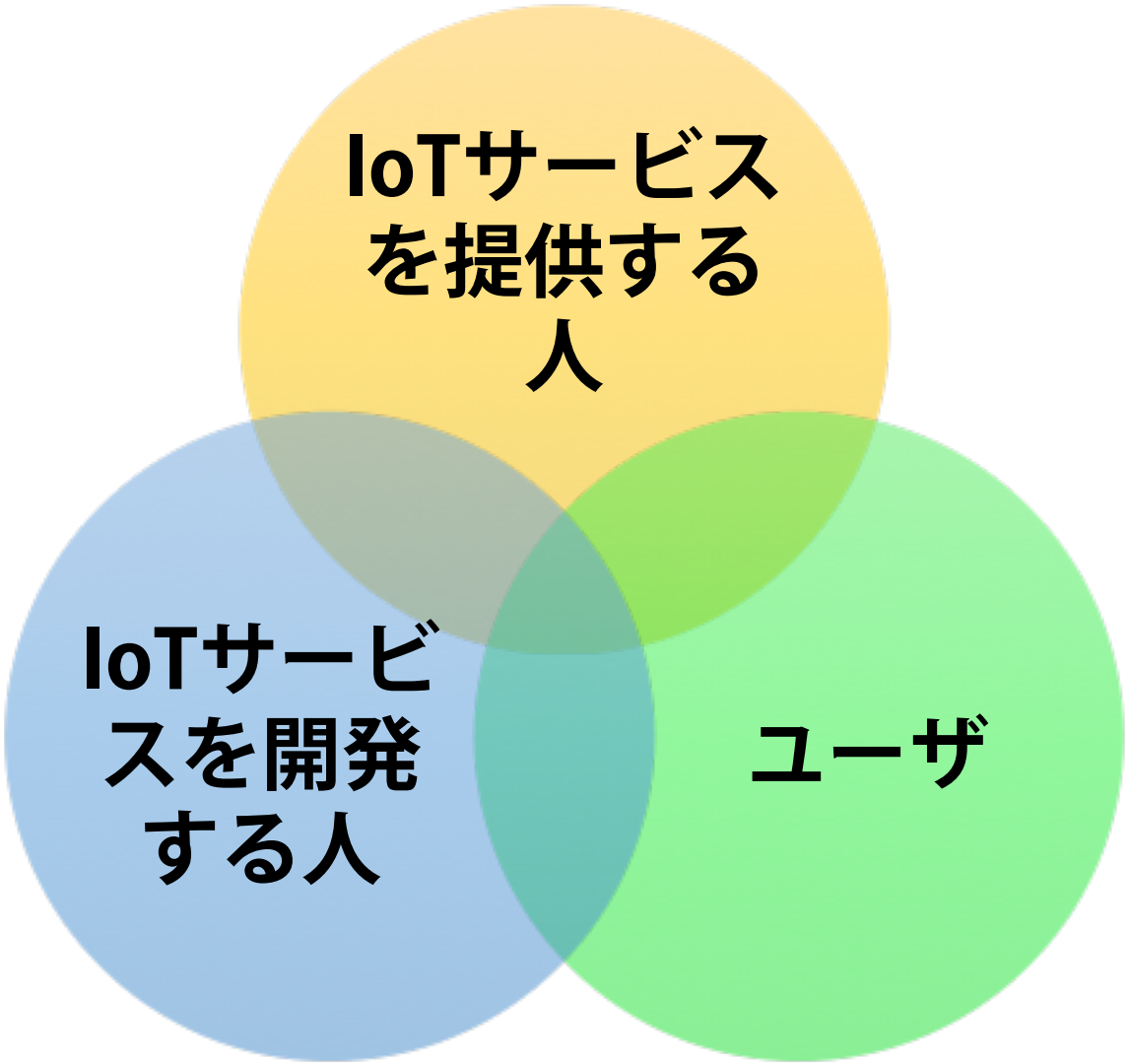
事後対応の限界



- 👉 IoT 機器の増加 / 攻撃の多様化
- 👉 End of Life / End of Support
- 👉 パッチ適用のスケーリング

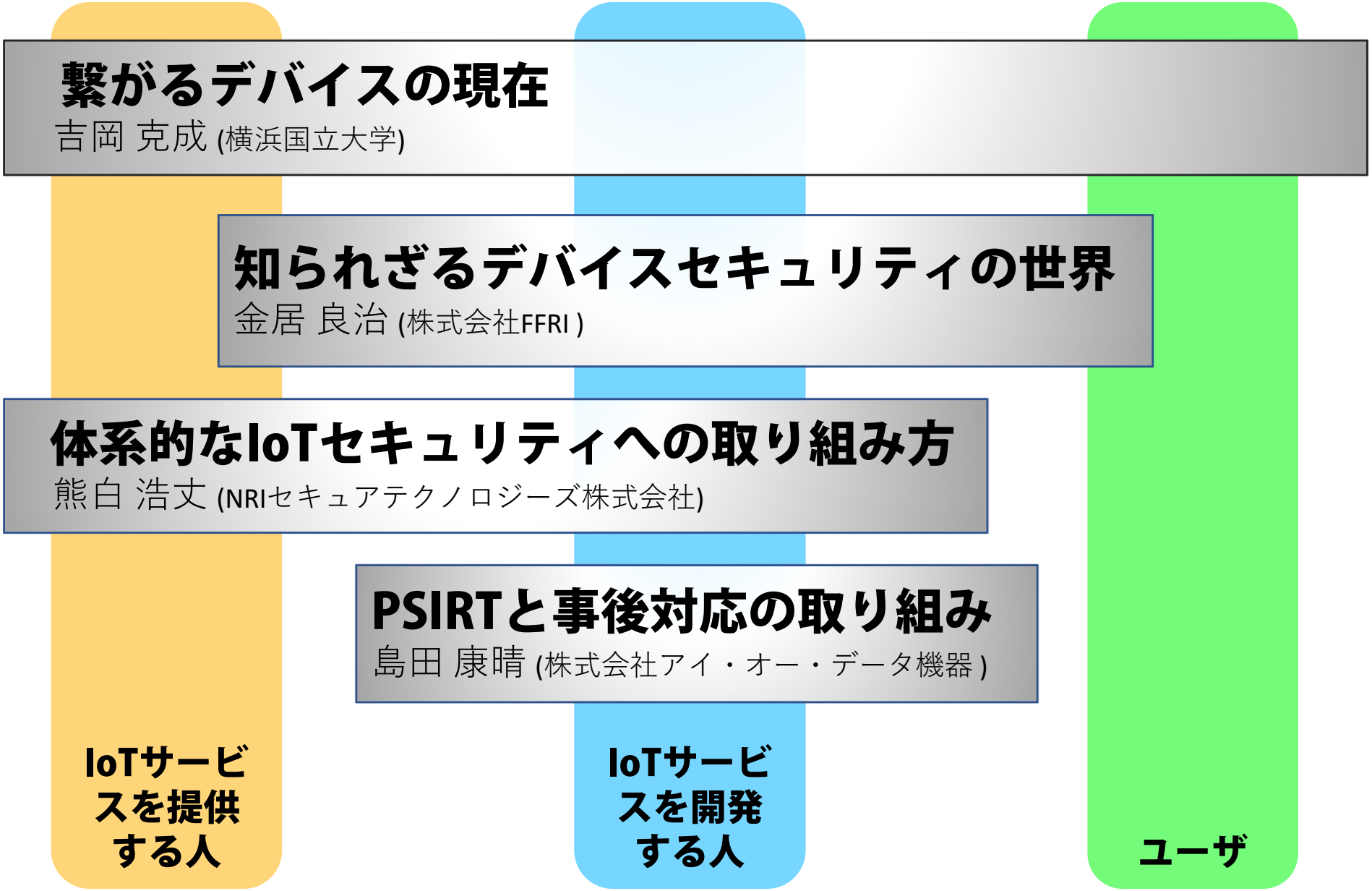
誰が
どうすれば
防げるのか？

IoTセキュリティのプレイヤー



ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA) より

IW IoTセキュリティセッションの講演内容



攻撃の実態・攻撃者像の最新動向

吉岡 克成氏 (横浜国立大学)

攻撃する側

- IoT マルウェアの侵入方法が多様化
  - 感染原因 No.1 は telnet
  - 攻撃カメラの”のぞき見”
- 攻撃規模の拡大
  - 100Gbpsを超えるDDoS攻撃の基盤として感染したIoT機器が悪用される
- 攻撃目的の多様化
  - 広告クリック
  - 有料放送の認証情報の取得
  - 機器の破壊
- 攻撃インフラの堅牢化
  - C2サーバ（インフラとして）もIoT機器
- **攻撃者はこれら全てを把握**

守る側

- **IoTのサービス提供者・開発者は攻撃者の実態を知らない**
- 駆除の方法論の検討，情報共有が必要

吉岡氏の講演スライドより

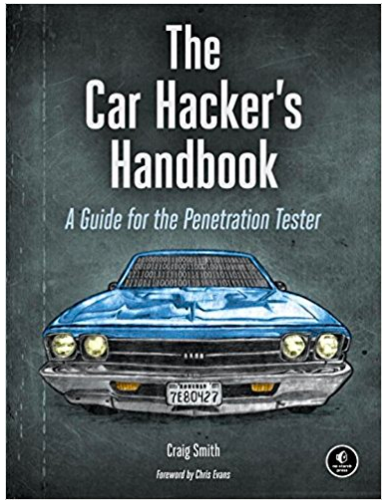
ネットワークカメラ画像無断公開サイト
Insecam（ロシア）

デバイスのセキュリティ

金居 良治氏 (株式会社FFRI)

- **デバイス解析技術が高度化し，機器の脆弱性を見つける土壌が成熟している**
  - ファームウェア解析技術が手軽な「道具」に
  - ハードウェア解析の方法論，ノウハウの成熟

- **対策アプローチの地道な適用以外の道はない**
  - プロセス（SDLC）
  - ファジング
  - テスト
  - 脅威分析
  - アップデート配信の仕組み



金居氏の講演スライドより

FFRI,Inc.

ファームウェア解析に関する問題

- ファームウェア解析を支援するツールが年々、整備されており、難易度は下ってきている

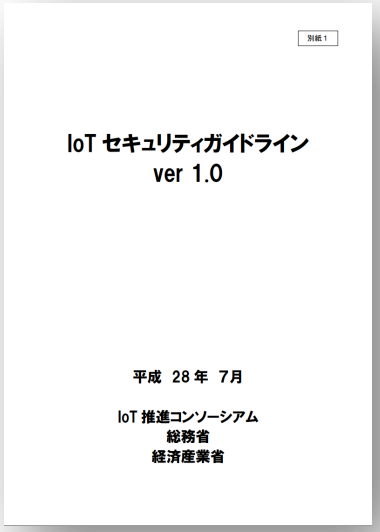
- 解説ページなども存在するため、もはやファームウェア解析は容易である前提での製品開発が必要

IoTセキュリティガイドラインの活用

熊白 浩丈氏 (NRIセキュアテクノロジーズ株式会社)

- **IoT セキュリティガイドラインは策定途上かつ乱立**
  - 各ガイドの詳細度，対象読者（運用・管理者，開発者，ユーザ）が異なる
  - 見極めが必要

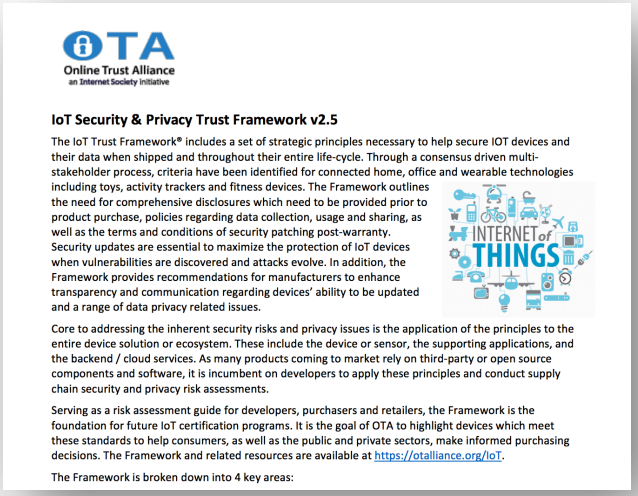
- 製品，事業分野に応じて，**必要なガイドを組合せて使う**「ボトムアップ」的アプローチがおすすめ


別紙１

IoT セキュリティガイドライン
ver 1.0

平成 28 年 7月

IoT 推進コンソーシアム
総務省
経済産業省


OTA
Online Trust Alliance
an Internet Society initiative

IoT Security & Privacy Trust Framework v2.5

The IoT Trust Framework® includes a set of strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices. The Framework outlines the need for comprehensive disclosures which need to be provided prior to product purchase, policies regarding data collection, usage and sharing, as well as the terms and conditions of security patching post-warranty. Security updates are essential to maximize the protection of IoT devices when vulnerabilities are discovered and attacks evolve. In addition, the Framework provides recommendations for manufacturers to enhance transparency and communication regarding devices' ability to be updated and a range of data privacy related issues.

Core to addressing the inherent security risks and privacy issues is the application of the principles to the entire device solution or ecosystem. These include the device or sensor, the supporting applications, and the backend / cloud services. As many products coming to market rely on third-party or open source components and software, it is incumbent on developers to apply these principles and conduct supply chain security and privacy risk assessments.

Serving as a risk assessment guide for developers, purchasers and retailers, the Framework is the foundation for future IoT certification programs. It is the goal of OTA to highlight devices which meet these standards to help consumers, as well as the public and private sectors, make informed purchasing decisions. The Framework and related resources are available at https://otalliance.org/IoT.

The Framework is broken down into 4 key areas:


SEC BOOKS

IPA Better Life with IT

つながる世界の開発指針

～安全安心なIoTの実現に向けて
開発者に認識してほしい重要ポイント～

第2版

独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター

熊白氏の講演スライドより

２．ITとは異なるセキュリティ対策

例：自社製品がIoTデバイスの場合

	米国				欧州	グローバル			国内
	CSA	OTA	FTC	FBI	ENISA	GSAMA	OWASP	IEEE	IoT推進コンソーシアム
①デバイス	○		○	○		○		○	
②NW					○	○	○	○	○
③PF					○	○		○	○
④マネジメント			○			○	○		○

全領域に配慮されたもの＋
詳しいもの・粒度の細かいもの
を組み合わせる。

・5つを全部見るのも大変・・・
上記だと「GSMA＋CSAでまずは見てみる」など
必要最小限の材料でアプローチしてみる。

© Copyright NRI SecureTechnologies, Ltd. All Rights Reserved. Proprietary & Confidential　無断での引用・転載を禁じます。

PSIRT における製品セキュリティの取組み

島田 康晴氏 (株式会社アイ・オー・データ機器)

- **製品を市場に出せば，必ず誰かが脆弱性を見つけ，報告する**

- 外部からの報告に対応できる社内体制（PSIRT）の整備と脆弱性ハンドリングの成熟度の向上
  - ex. 開発部門だけでなく，管理部門，情シス，カスタマーサポートもメンバー

- **脆弱性を積極的に公表する企業文化**

島田氏の講演スライドより

この事例のポイント

- 脆弱性情報が公開されたら、できるだけ速やかに脆弱性の内容を把握して、該当する商品がないかの調査を開始します。
- 調査の段階で該当商品が見つかった場合、速やかに調査中の旨の公開を行うことが望ましいです。
- 市場の脆弱性に対する意識の高まりから、時には顧客などからの問い合わせがすぐに届きます。会社としての対応を明示するためにも情報公開は有効です。
- 該当商品の調査を何処まで遡って調査するかは、商品リストのテンプレート化するなどしてあらかじめ決めておくと、楽になります。

[まとめ] IoTセキュリティのキーワード

- **機器の脆弱性対策がIoTセキュリティ実現の鍵**
  - 脆弱性の悪用が被害の原因になっている

- **PSIRT**（**P**roduct **S**ecurity **I**ncident **R**esponse **T**eam）
  - デバイスセキュリティ
  - ガイドラインの活用
  - 製品インシデント対応
  - 脆弱性情報の公表

- **「対策」をいかに末端の機器にまで届けるか**

- **IoT に対する脅威の観測と分析**