Internet Week 2017

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～

本プログラムの焦点 ～IoTの全容に迫る～

2017.11.29

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

[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]

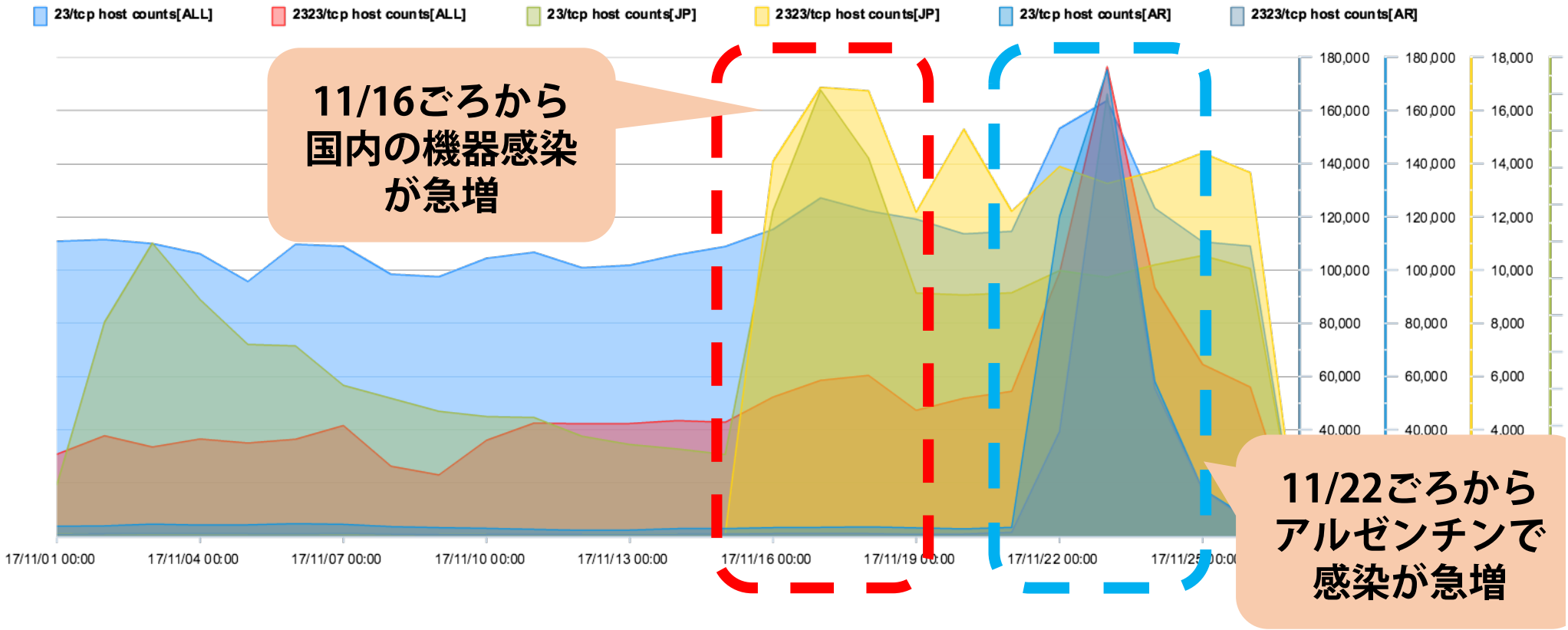
- Both C2s have been sink-holed now by security community.
- admin/CentryL1nk is a typo for admin/CenturyL1nk.

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**.

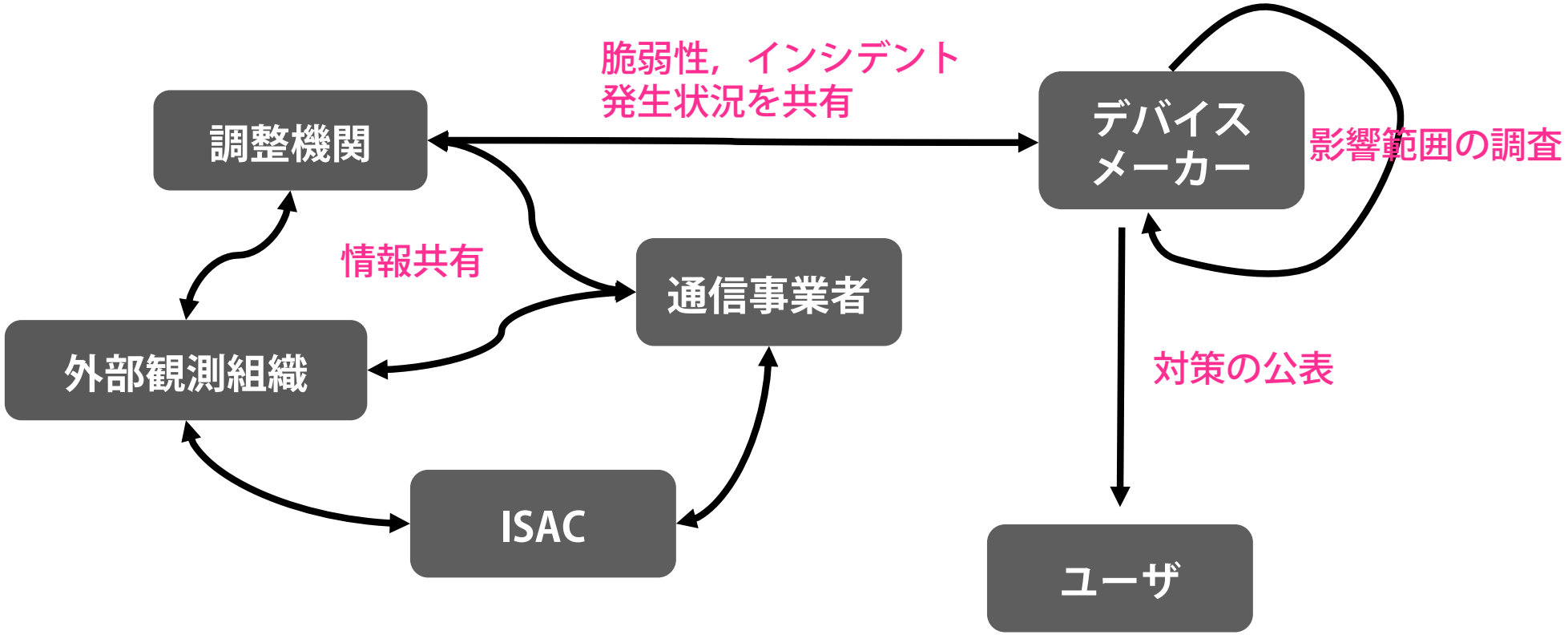
360 NetLab による分析レポート

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**



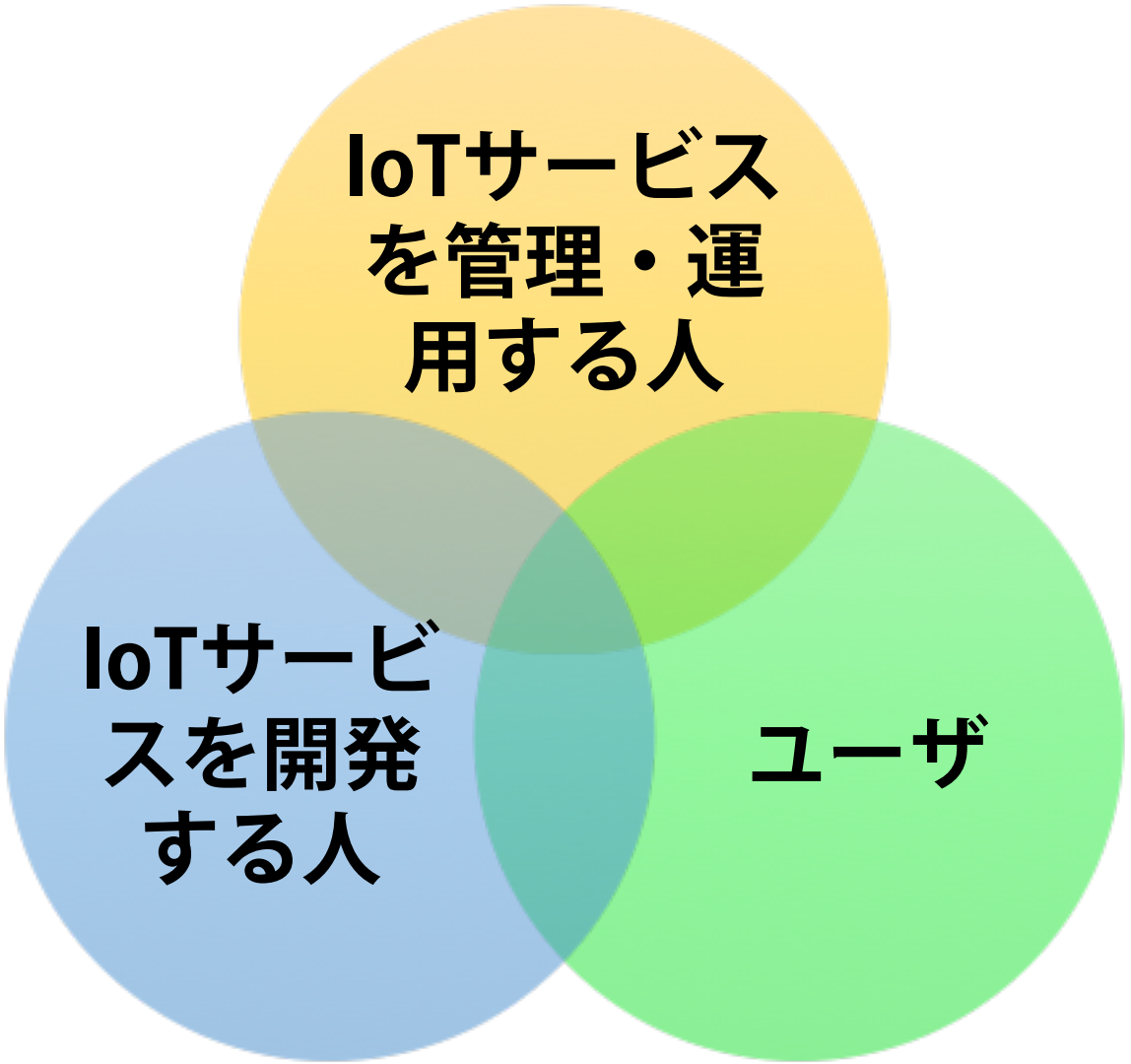
事後対応の限界



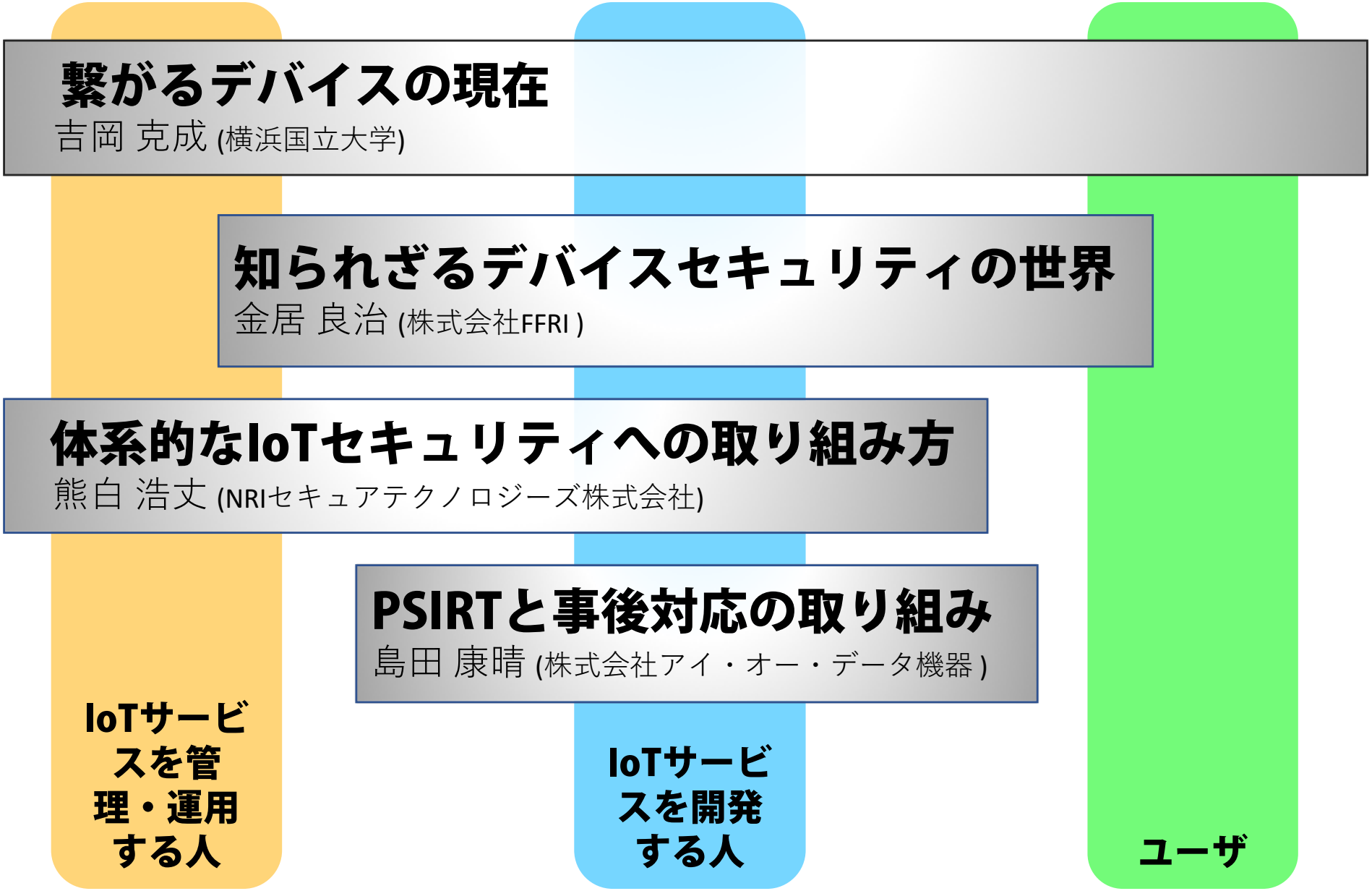
- 👉 数への対応： IoT 機器の市場台数の増加，多様化に追いつかない
- 👉 End of Life / End of Support
- 👉 機器へのパッチ適用

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



本セッションの講演


繋がるデバイスの現在
吉岡 克成 (横浜国立大学)
知られざるデバイスセキュリティの世界
金居 良治 (株式会社FFRI)
体系的なIoTセキュリティへの取り組み方
熊白 浩丈 (NRIセキュアテクノロジーズ株式会社)
PSIRTと事後対応の取り組み
島田 康晴 (株式会社アイ・オー・データ機器)
IoTサービスを管理・運用する人
IoTサービスを開発する人
ユーザ