明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IoT時代を支えるサイバーセキュリティ人材育成

学校法人 岩崎学園　情報セキュリティ大学院大学
内閣府 SIP プログラムディレクタ(PD)
後藤 厚宏

情報セキュリティ大学院大学

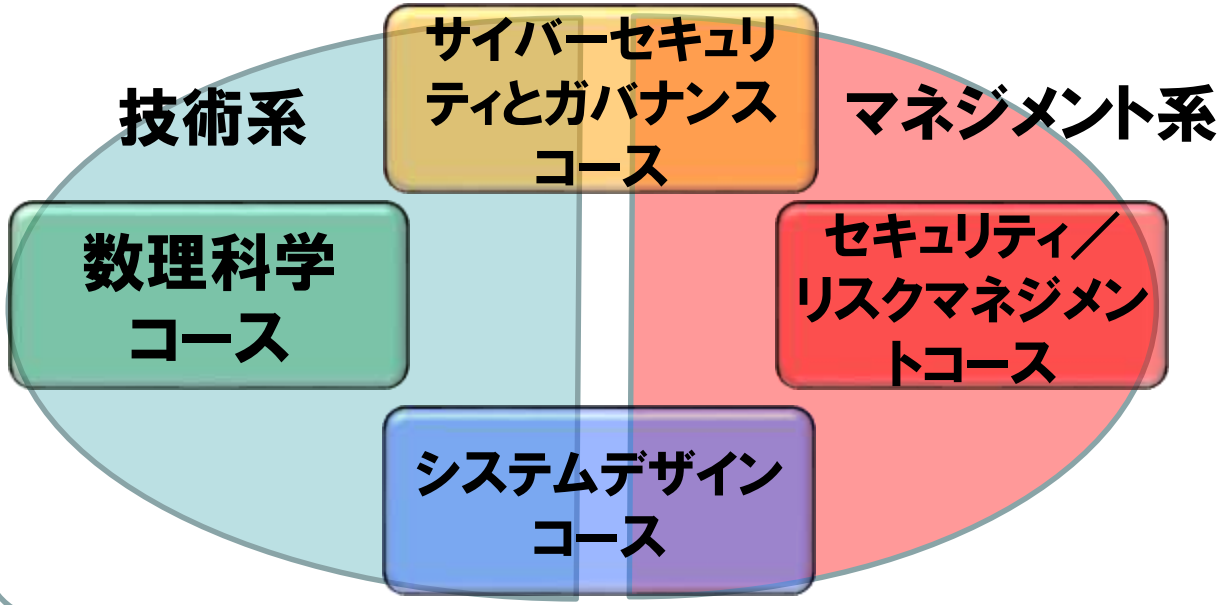
http://www.iisec.ac.jp/

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

学長
後藤厚宏

- 情報セキュリティ専門の独立大学院として2004年開学
- 2017年3月までに、修士339名、博士30名の修了生日本の中核的業務を担う。

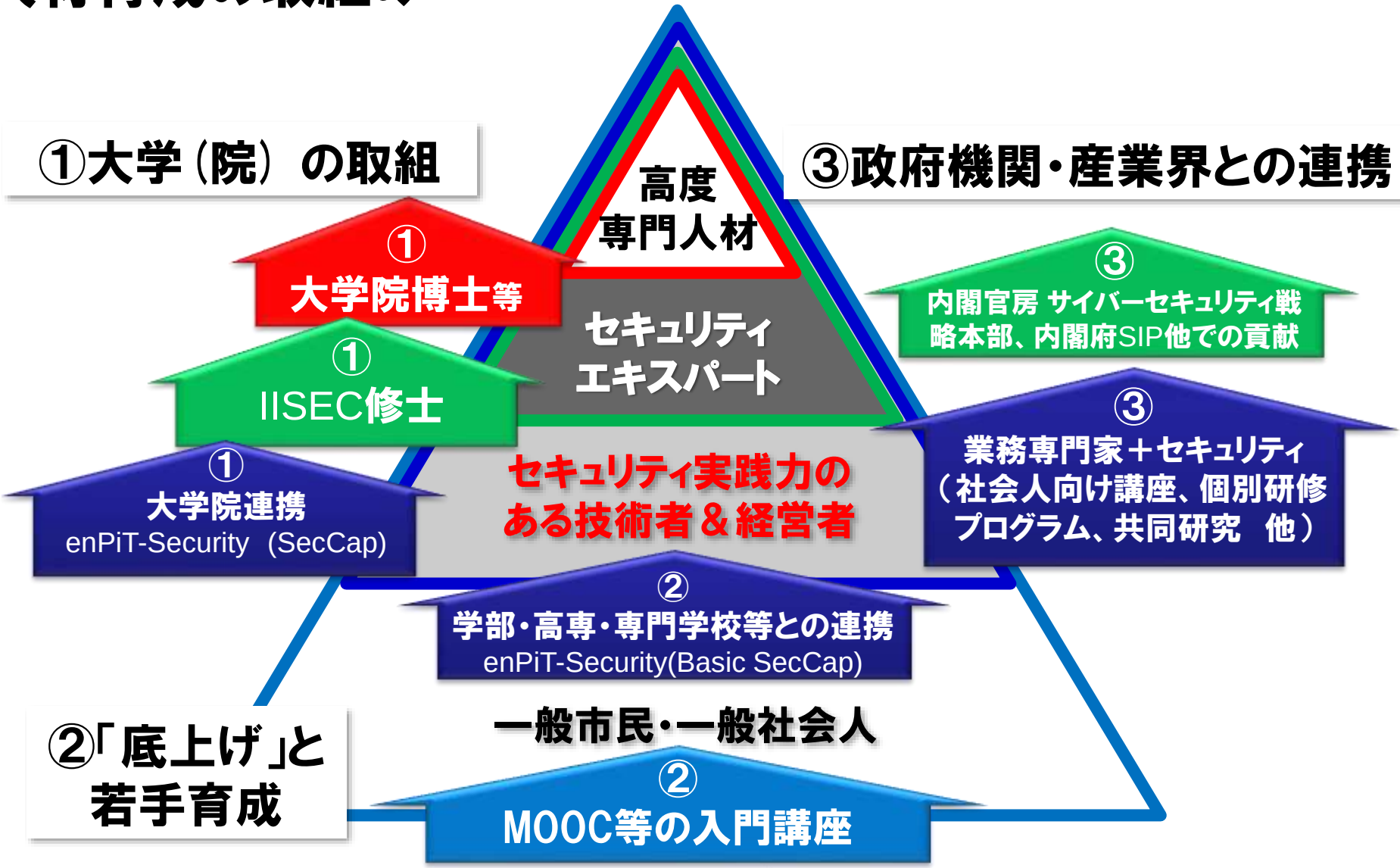
総合科学：情報セキュリティカリキュラム



倫理観を持って、現実の課題解決を担う高度な専門技術者・実務家、及び、将来方向をリードする創造性豊かな研究者を育成

情報セキュリティ大学院大学
人材育成の取組み

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



ATMセキュリティ事案より

一般社団法人

重要生活機器連携セキュリティ協議会(CCDS)

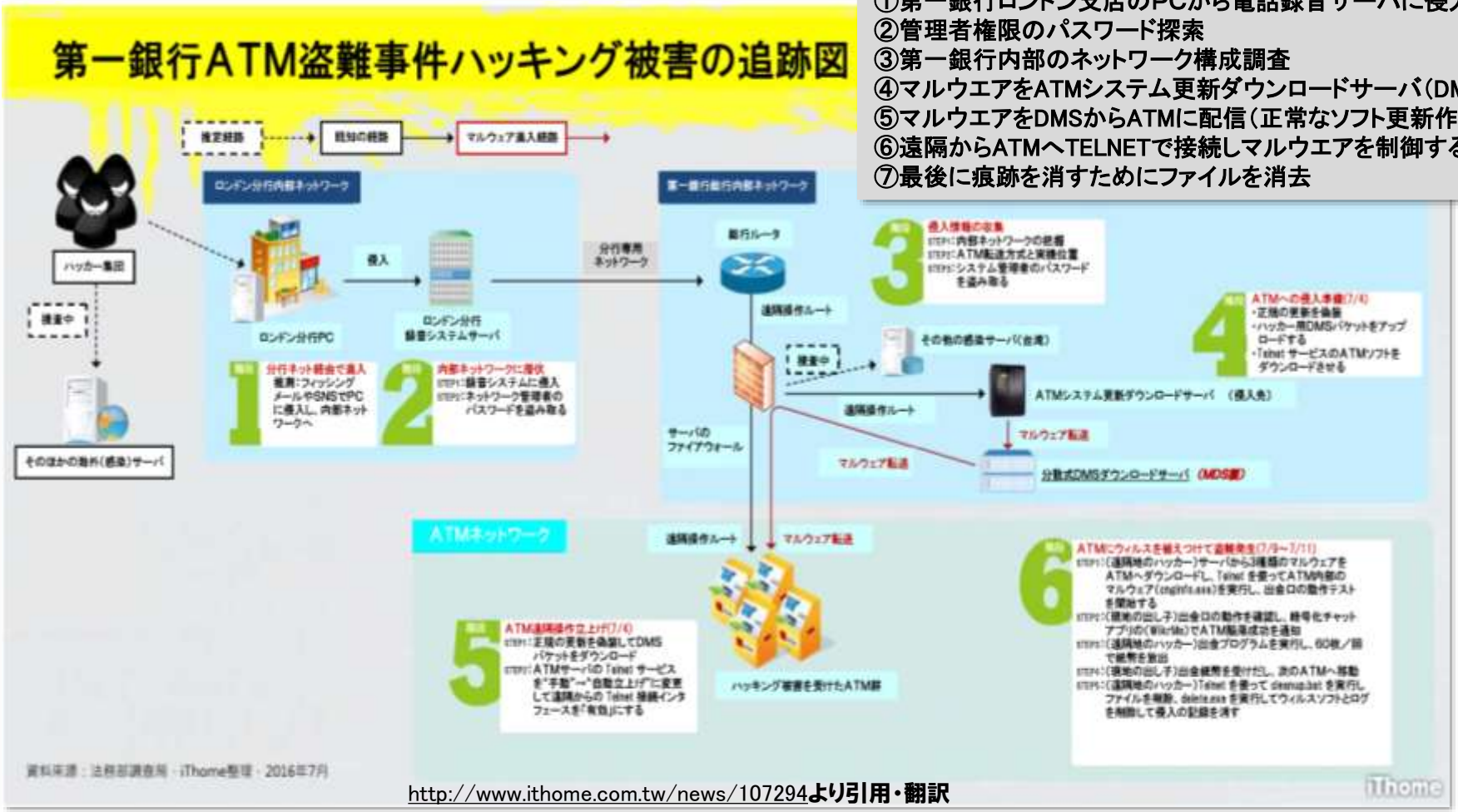
金融端末SWGの分析資料より

ATMマルウェア攻撃事例

–海外支店等がネットワーク侵入の切り口となった事例–

■**最初は管理の手薄な海外支店システムに侵入し、その後、銀行ネットワークの中枢部を探索。ATMシステム更新ダウンロードサーバ経由でATMにマルウェアをダウンロードさせる攻撃。これにより、ATMから不正出金の被害発生（第一銀行、台湾）。**

①第一銀行ロンドン支店のPCから電話録音サーバに侵入
②管理者権限のパスワード探索
③第一銀行内部のネットワーク構成調査
④マルウエアをATMシステム更新ダウンロードサーバ（DMS）に登録
⑤マルウエアをDMSからATMに配信（正常なソフト更新作業に相乗り）
⑥遠隔からATMへTELNETで接続しマルウエアを制御する
⑦最後に痕跡を消すためにファイルを消去



http://www.ithome.com.tw/news/107294より引用・翻訳

弱点を探索して攻撃するパターン

■攻撃者である犯罪者集団は、世界規模でATMマルウェア未対策国を順番に攻撃。
■これはマルウエアが順次高度になっているのではなく、同じものがセキュリティ対策の遅れている国に横展開されているということ。攻撃者の行動パターン（攻撃ツールのブラックマーケット）は、経済原理に基づく側面があることを認識しておく必要がある。

Ploutusマルウェアの世界的展開

Mexico：https://www.symantec.com/connect/blogs/backdoorploutus-reloaded-ploutus-leaves-mexico
Ukraine：https://www.atmmarketplace.com/news/ukraine-hit-by-cyberattack-using-newest-atm-trojan/
Malaysia：https://www.scmagazine.com/backdoorploutus-or-backdoorpadpin-may-be-behind-atm-attacks-in-malaysia/article/539959/

クレジットカードの分野での事例

- 欧州でのICカード普及に伴い、磁気カード利用を続ける米国に不正利用被害がシフトしていることが、統計面で見て取れる。
- 国内でもPOS端末を狙っていた攻撃者がみられていたが、POS端末でのICカード取引の普及が進めば、**未対策のATMに攻撃がシフト**してくる可能性が考えられる。

イギリス発行カードの海外での不正利用の推移（2005-2008）

出典：”クレジットカード取引におけるセキュリティ対策の強化に向けて”,経済産業省／日本クレジット協会,平成28年4月
原出典：APACS Fraud The Facts 2009（2016年2月日本クレジットカード協会IC化に関する調査結果）

攻撃パターンの特徴と対策の考え方

① 攻撃者は、国レベルで、あるいは、システムレベルで、それぞれ弱いところを狙ってくる。

② 攻撃者は、政府機関や軍事機関を標的にするほど高度な攻撃技術を保有している場合もあり。こうした攻撃者を上回る技術力で防御策を導入することは、民間レベルでは技術面でも費用面でも大きな困難が伴う。

攻撃者の標的にされないように一定の水準を保ったセキュリティ対策（攻撃にはコストがかかり、割に合わないと思わせる対策）が現実的か

MiraiとDT事案

IoT機器が重要インフラへサイバー攻撃

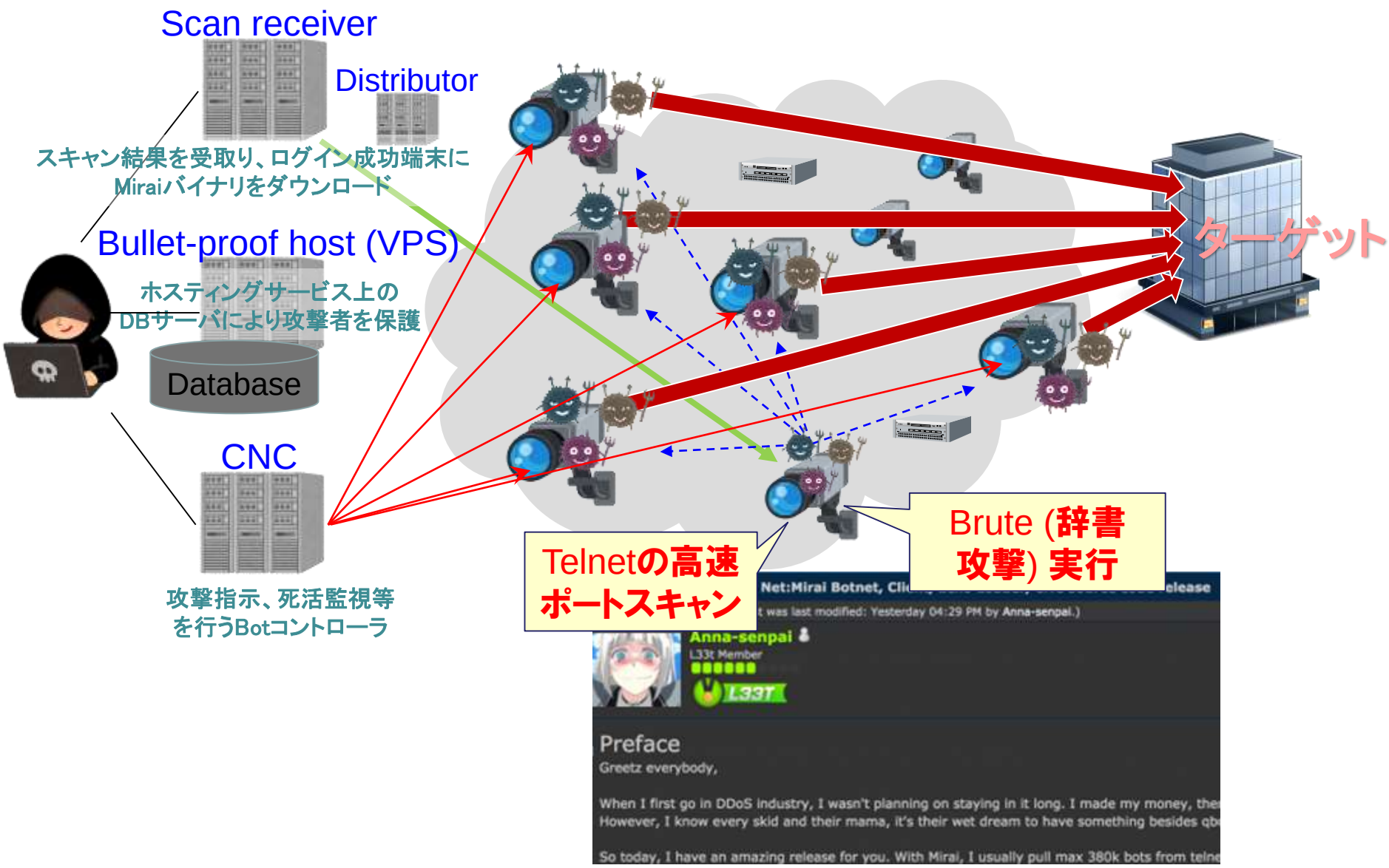
● 脆弱性のあるIoT機器が大規模DDoS攻撃の踏み台

【事例1】 サイバー攻撃によるDNS停止（2016年10月）

- 約6時間にわたりサービスが不安定に
- PayPal, Twitter, Amazon, Netflixなども影響を受けた

【事例2】 DTのSpeedportルータをマルウェア感染させる攻撃
攻撃は失敗したが90万人が影響を受ける（2016年11月）

Miraiの攻撃メカニズム ～NTT研究所による解析～



https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

Mirai関連／出来事タイムライン

日時	出来事
2016/9/20	セキュリティblog「KrebsOnSecurity」への攻撃 (DDoS攻撃の規模は当時最大級の620Gbps)
2016/9/21	仏・ホスティング事業者「OVH」への攻撃 (15万台の監視カメラから、約1Tbpsの攻撃を受ける)
2016/9/30	Miraiソースコード公開 by Anna-senpai (結果、Mirai亜種が作られることになる)
2016/10/21	マネージドDNSサービスを展開する「Dyn」への攻撃 (Twitter等の有名サービスへのアクセスに影響あり)
2016/11/27	Mirai亜種による世界規模の感染活動発生 (Deutsche Telekomの顧客90万人に影響発生)

顧客ルータへの感染活動に伴う通信障害（DT事案）

■ 発生日時

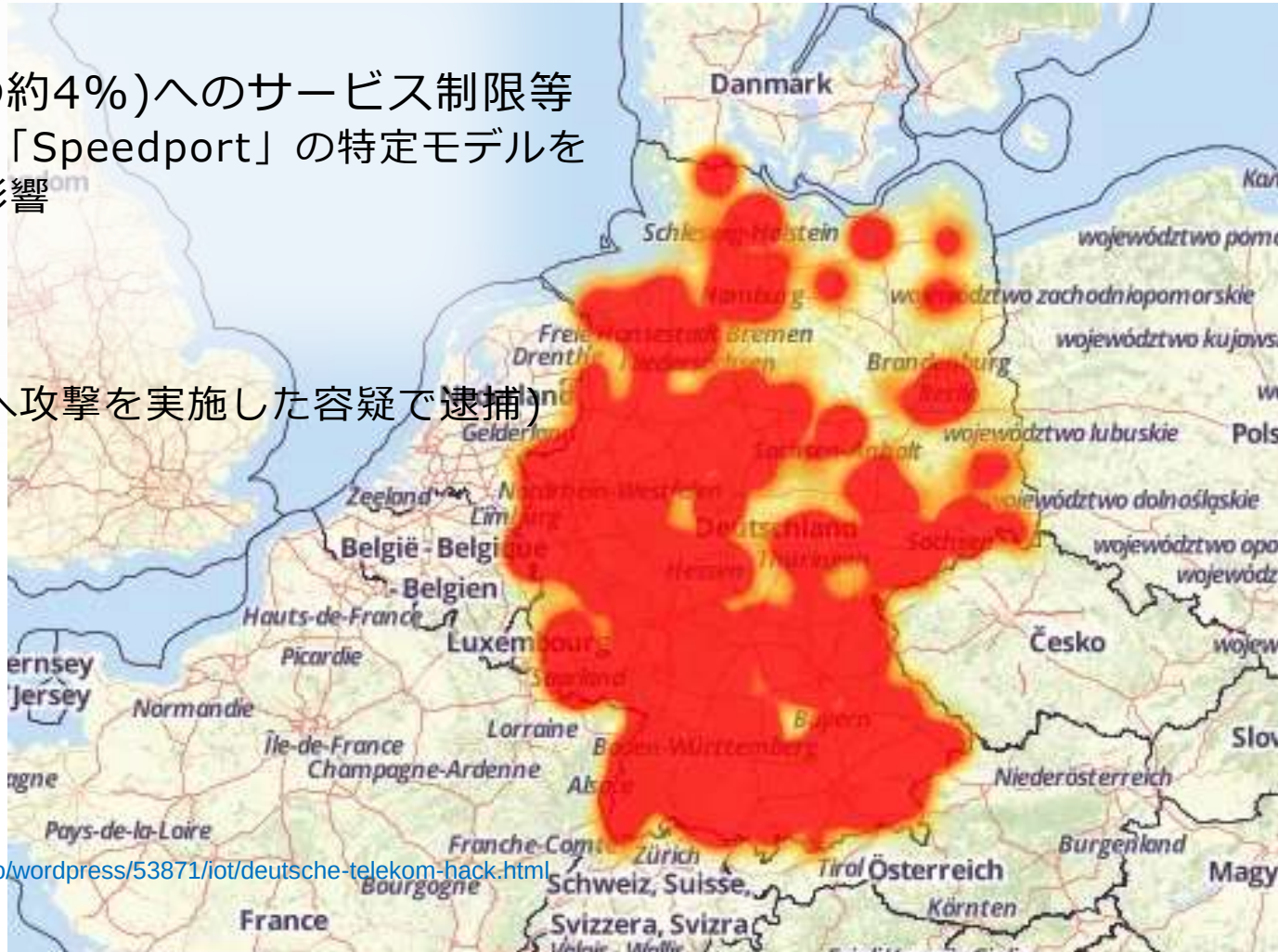
2016年11月27日 17時頃から最低2日間

■ 影響

90万顧客(全顧客の約4%)へのサービス制限等
⇒DTの顧客用ルータ「Speedport」の特定モデルを使っている顧客に影響

■ 攻撃者

29歳の英国在住者
(2017年2月に、DTへ攻撃を実施した容疑で逮捕)

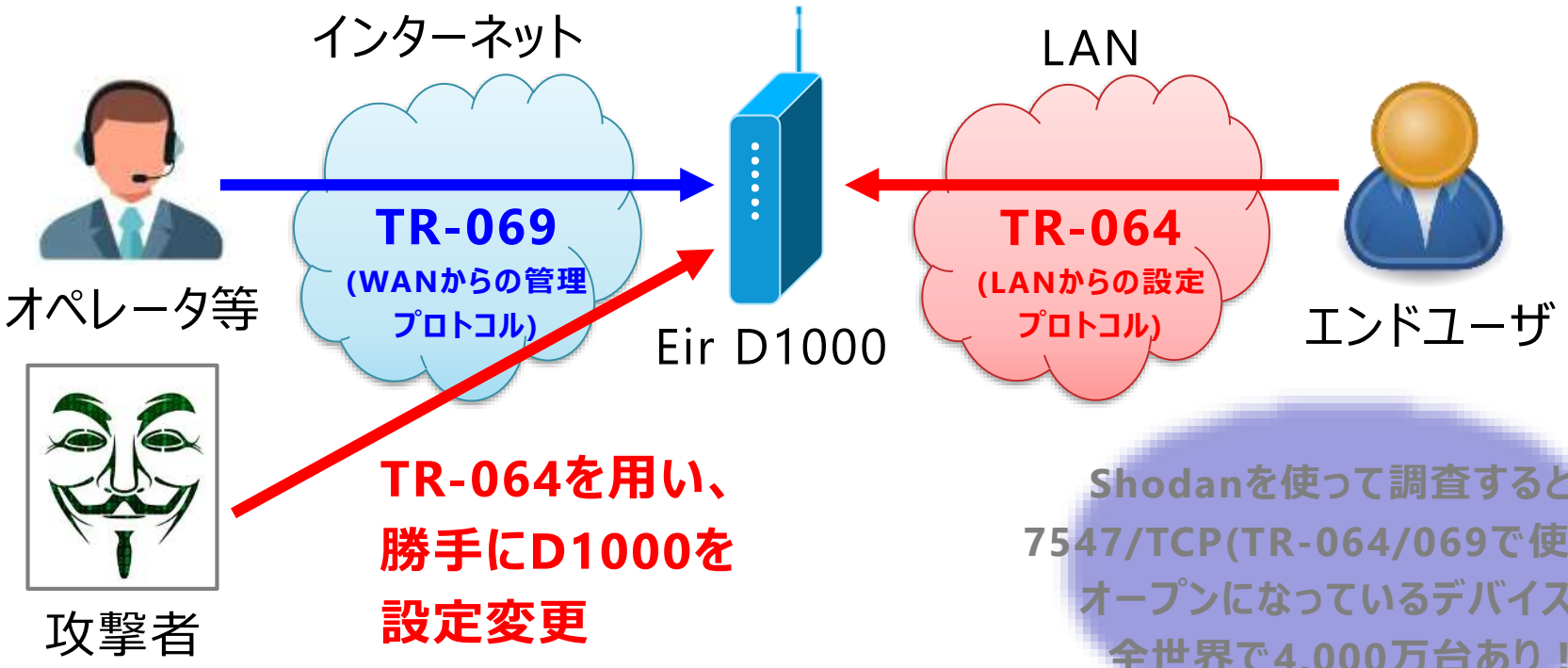


http://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html

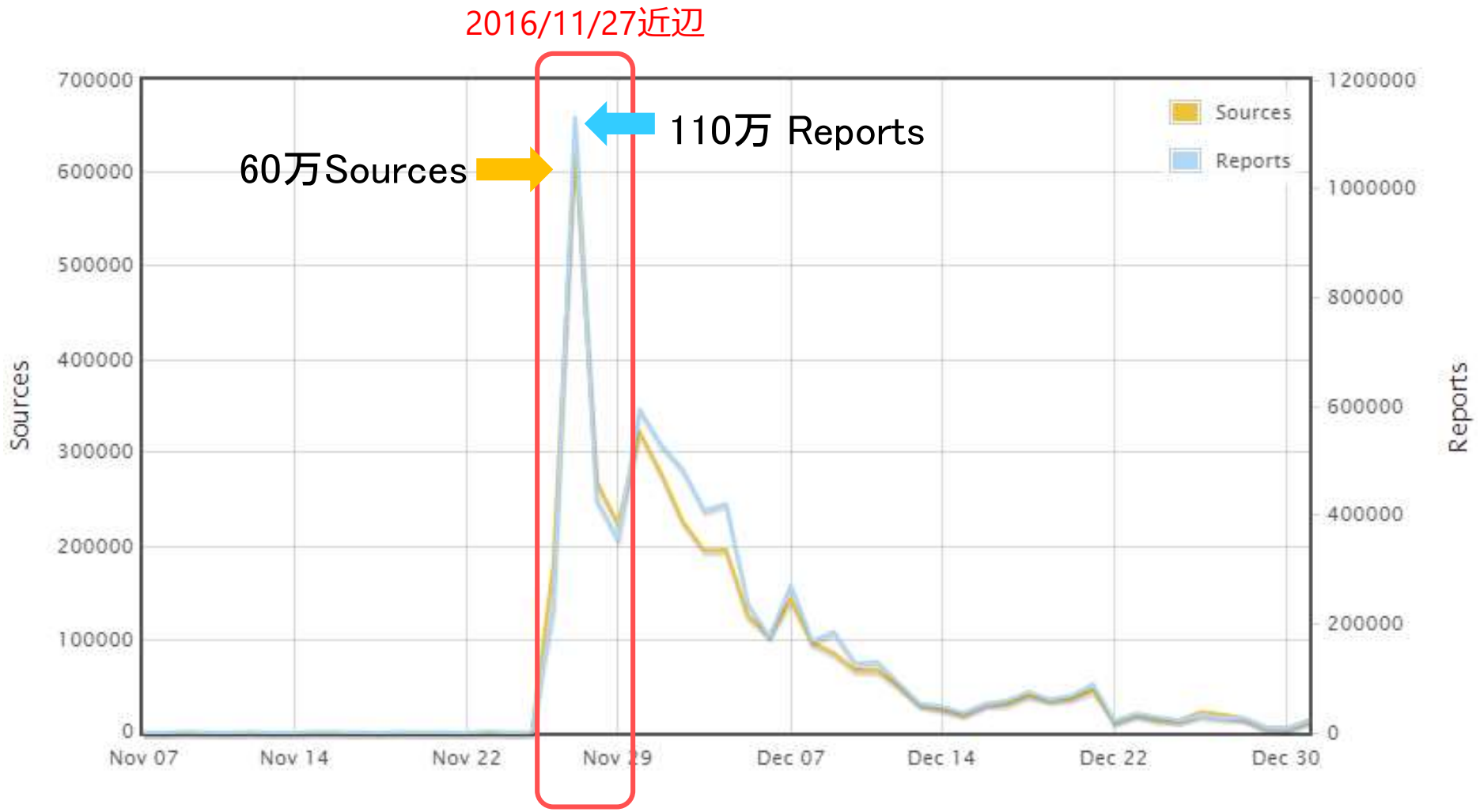
DT事案：背景となった脆弱性

■ アイルランドのキャリアEir製品の脆弱性が公開 (2016/11/07)

- TR-064がインターネット側から実行できてしまう
- DTの顧客ルータは当該脆弱性を持っていなかったが・・・



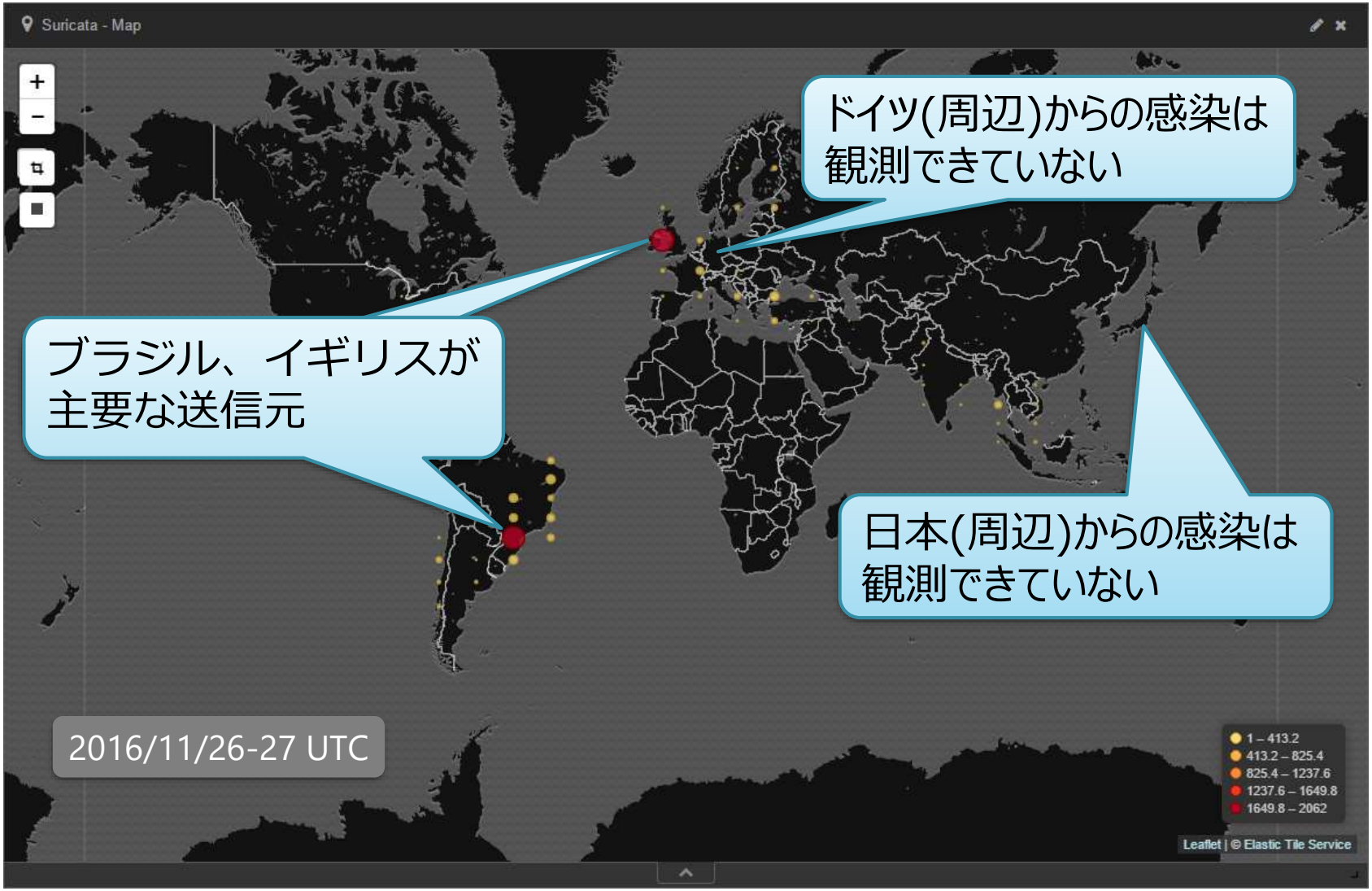
DT事案：米SANS InstituteのPort Activity モニターから



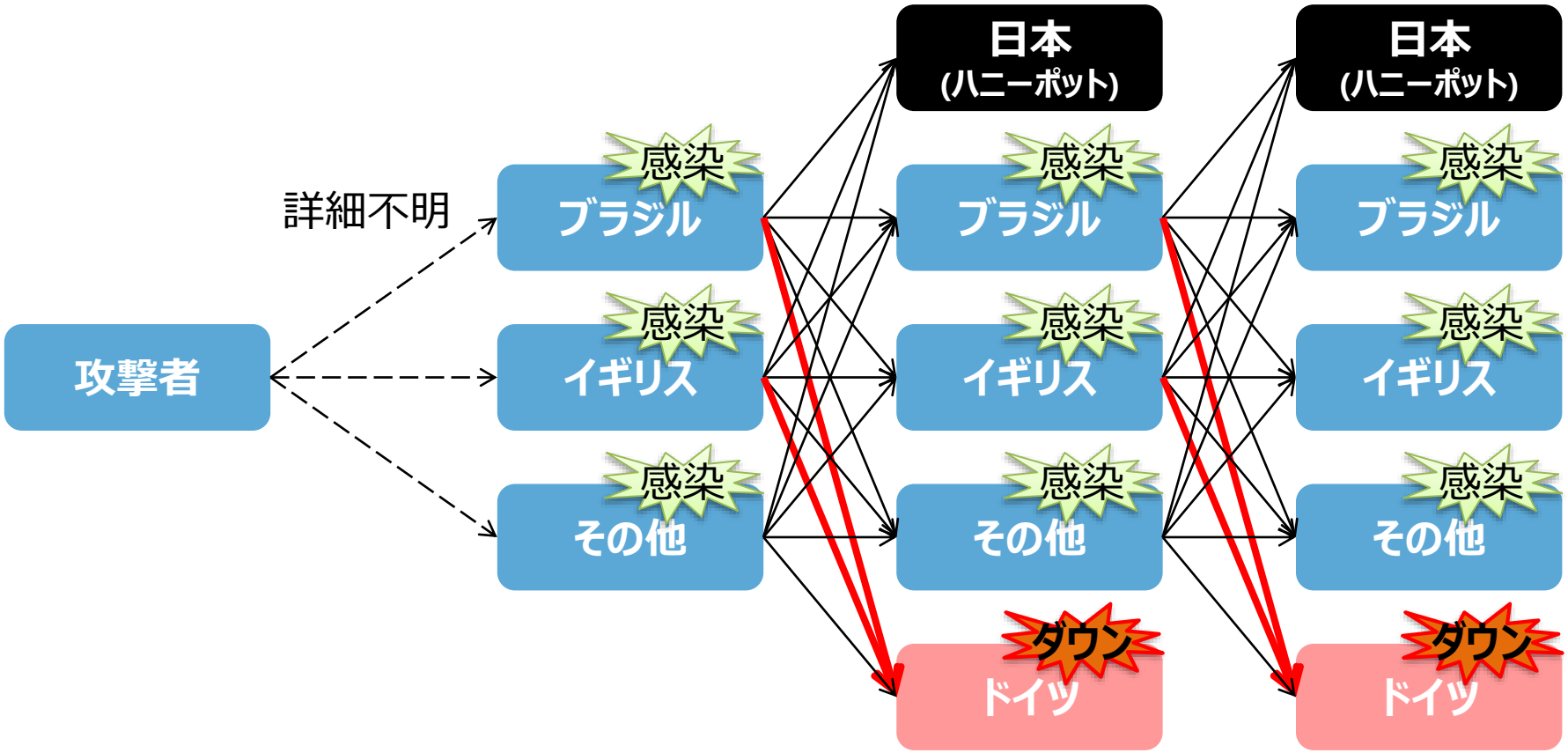
https://isc.sans.edu/port.html?port=7547

DT事案：7547/TCPの送信元
～NTT-CERTによる観測結果～

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



DT事案：影響を与えた経路？
～NTT-CERTによる推測～



DT事案：Deutsche Telekomの対応

- 新たな被害を防ぐために**ネットワークにフィルタを設定**
  - 攻撃者が遠隔保守インタフェースにアクセスすることを防ぐ

ネットワークはしっかりマネージドできていた！

- これと並行して、ルータ製造企業に**修正ファームウェア作成を依頼**
  - 発生からほぼ一日で影響を受けた端末に対して配布開始

機器ベンダとNW事業者の密な連携ができていた！

- 影響の有無に関わらずSpeedportルータの全モデルをチェックし、適切な**ファームウェアをリリース**
  - 以下のモデルが最も早くリリース
    - ✓ Speedport W924V (fiberモデル含む)
    - ✓ Speedport W723V Type B

大量のNW端末の遠隔更新機能が具備できていた！

DT事案から学べること

IoTにもSOCサービス（セキュリティ監視）サービスが必要

サプライチェーン（機器ベンダ）の対応力が重要

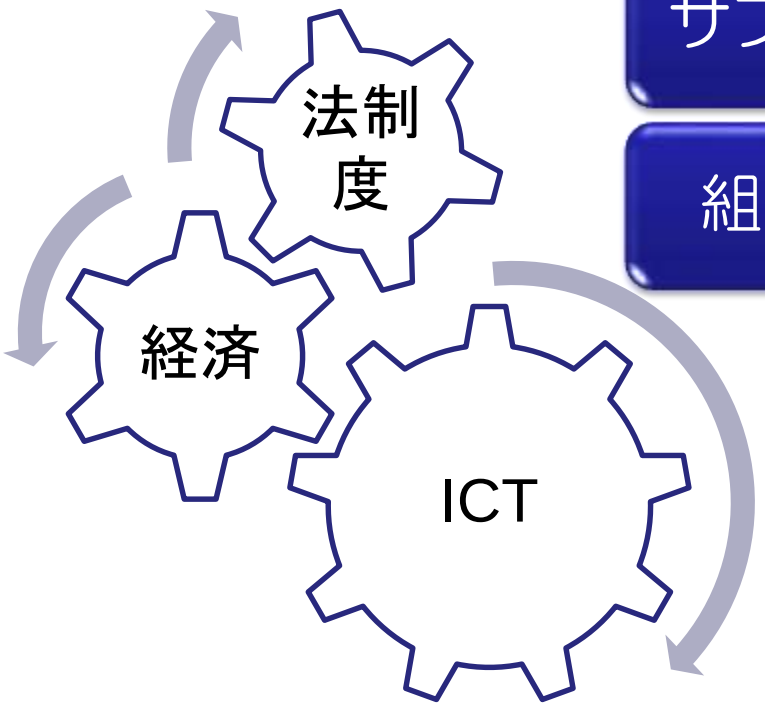
遠隔アップデート機能が必須

サイバーセキュリティ人材育成

サイバーセキュリティ人材育成

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- グローバルな状況判断
- システム全体の監視
- サプライチェーン・ベンダリレーション
- 組織マネジメント・設備マネジメント



サイバーセキュリティ人材は
創造力 creativityが勝負！

ご清聴ありがとうございました。

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY