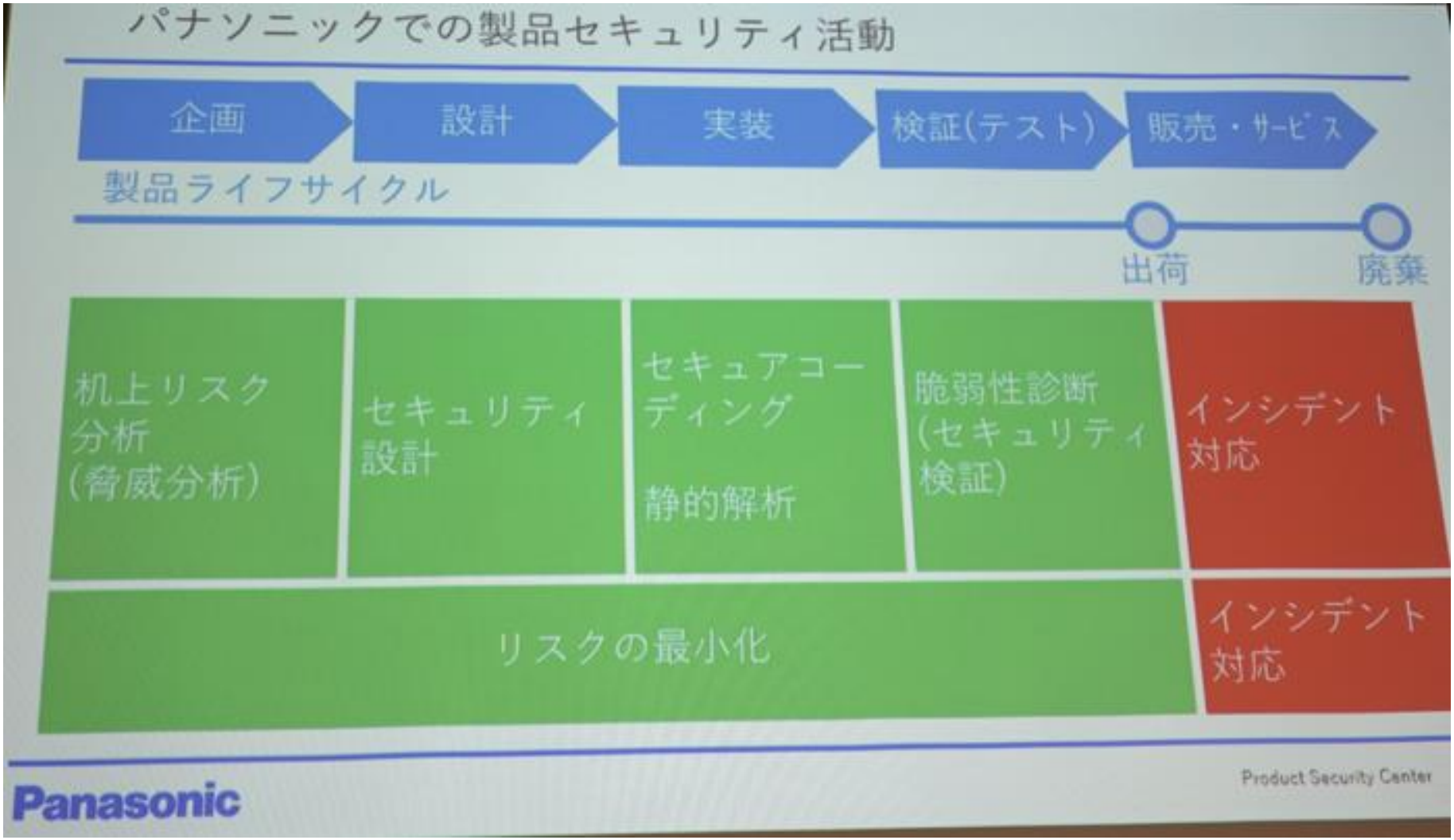
IoTのセキュリティ:
先手のインシデント対応

～ 早期警戒によるアプローチ～

東京大学大学院
情報理工学系研究科
准教授 落合秀也

背景：IoTサービスはインシデント対応と一体化する方向に進んでいる



引用：増加するIoT機器への攻撃 - パナソニックが進めるセキュリティの見える化
https://news.mynavi.jp/article/20191028-915343/

先手のインシデント対応が明暗を分ける

- デバイス自体は侵入等の対策ができていたとしても
  ネットワークを含めて考えたら、まだまだ脆弱：
  - 例1：ECHONETは、簡単に乗っ取られる・・・
  - 例2：LAN内でのDoS攻撃があれば、簡単に止められる
  - 例3：サイドチャネル攻撃により、たとえ、通信を暗号化していたとしてもプライバシーが暴かれる
- LAN内に侵入したマルウェアによりいつでも攻撃されうる
- ベンダーは、IoTデバイスを導入した現場のセキュリティ管理が求められる状況になっている・・・
  - 導入後のインシデント発生 → ベンダーに対応が求められる
- 攻撃の前兆に気付くことが大切
  →「先手の行動に出ること」こそが、インシデント対応となる

先手のインシデント対応: LAWSONの事例

ローソンにサイバー攻撃 - 公式サイトやアプリを一時停止

ローソンは、サイバー攻撃が行われていることを確認したとして、同社サイトやアプリのサービスを一時停止した。

同社によれば、9月24日20時ごろ、公式サイトと公式アプリを管理しているサーバが攻撃を受けていることを確認したもの。同社は攻撃の影響を抑制するため、アクセスを遮断した。

今回の対策の影響により、同月25日17時の時点においてもウェブサイトやアプリを閲覧できない状態となっている。

同社では、攻撃元の調査やセキュリティ対策の実施など対応を進めている。

（Security NEXT - 2019/09/25 ） B! ツイート

引用: http://www.security-next.com/108405

「先手のインシデント対応」のポイント

- ネットワーク上の振る舞いの異常を検知する
- その異常が悪意のあるものであることを判定する
  → 警報の発令

- システム全体を避難モードに移行し、隔離する。
  → 隔離することで、致命的な攻撃から身を守る

- 犯罪者（攻撃の土台となっているコンピュータ）の特定を急ぐ、そして、取り除く。

Smart な「先手のインシデント対応」

サイバー攻撃が発生したときには:

1. 現場のお客さんが気付くよりも先に
2. IoTサービス事業者がその事象に気付き
3. インシデント対応のアクションを取って
4. お客さんに通知する
5. 同時に、原因となっているコンピュータを特定し、
6. それがネットワークから取り除かれたら、
7. 元のサービスを復旧させる

インシデント対応・・・世の中の言葉では

- SOC: Security Operation Center
  - 一次受け インシデント対応組織 (24時間365日稼働)
  - 発生したセキュリティ・インシデント (検知された脅威も含む)に、迅速に技術的に対応する組織
- CSIRT: Computer Security Incident Response Team
  - SOCと連携し、インシデント後の対応（顧客対応等）を行う組織
  - 平時は、脆弱性情報などを常に Watchし、組織内のパッチ適用管理などを行う組織
- PSIRT: Product Security Incident Response Team
  - 脆弱性情報などを常に Watchし、開発チームと連携し、自社製品のパッチ適用管理などを行う組織
  - IoT展開現場でインシデントが起きた際の一次対応組織ではない

    ➔ IoTサービス事業者は どう 一次対応を実現するのか？？

提案事項
PSOC: Product Security Operation Center

- IoTサービス事業者が展開するIoT機器が、現場において、サイバー攻撃の脅威に遭遇したとき、自らの集中管理センター (= PSOC) で、アラートが発生する。

- PSOCがなければ、自社IoT機器の目前まで脅威が迫っていたとしても、IoTサービス事業者は気付くすべ無し

- PSIRT (Product Security Incident Response Team) は「IoT機器のインシデント対応」と読み替えられがちだが、個別の現場対応機能がないことは前述の通り

侵入検知システムによる

先手のインシデント対応

ポイントは早期警戒

（できるだけ早く、身近に現れた潜在的な脅威に気付いて、取り除く）

(一般的な)侵入検知システム Intrusion Detection System (IDS)

- イントラネットやLAN内にマルウェアが侵入し、
  - マルウェアが C&C (Command and Control)サーバ (ブラックリストIPやドメイン名)と通信しようとすると、それを上流のルータ等で検知し、警報を出す。
  - マルウェアが インターネット上のホストを手あたり次第にアクセスしようとすると、それを上流のルータ等で検知し、警報を出す。
- 通常、組織のネットワーク管理者により運用されている。

  → IoTサービス事業者には、この情報は共有されない
- 小規模なネットワークでは、そもそも IDSは運用されていない。

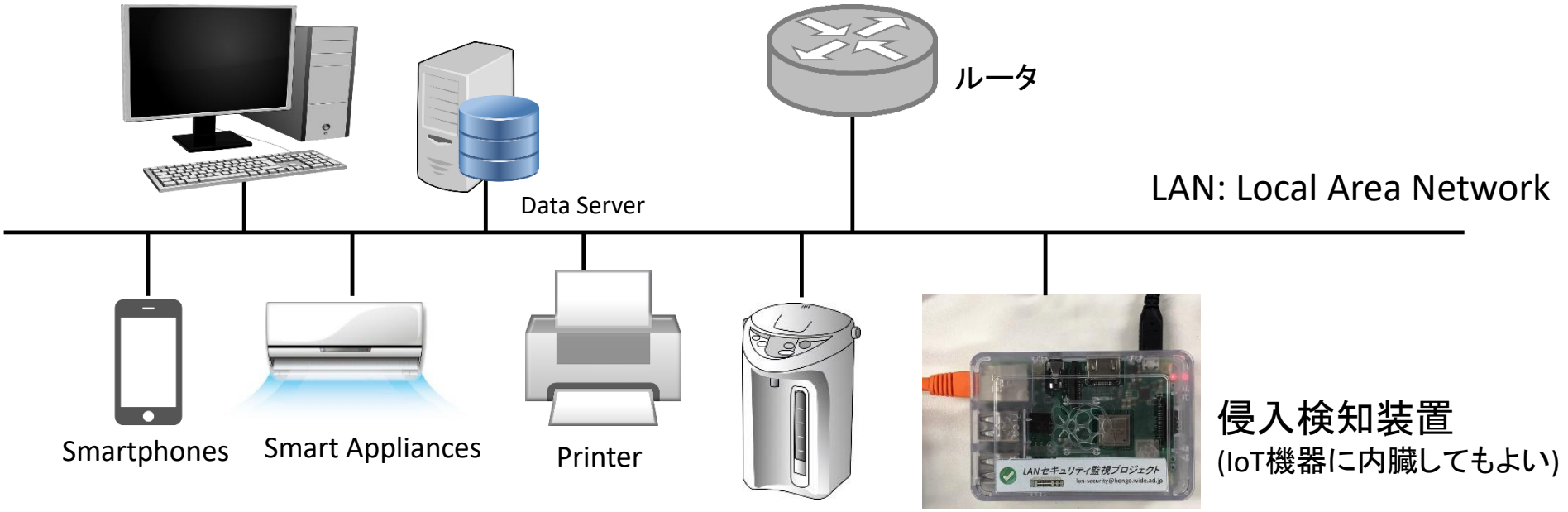
  →侵入したマルウェアは野放し状態になる

IoTサービス事業者(*注)ができる ネットワーク末端での侵入検知

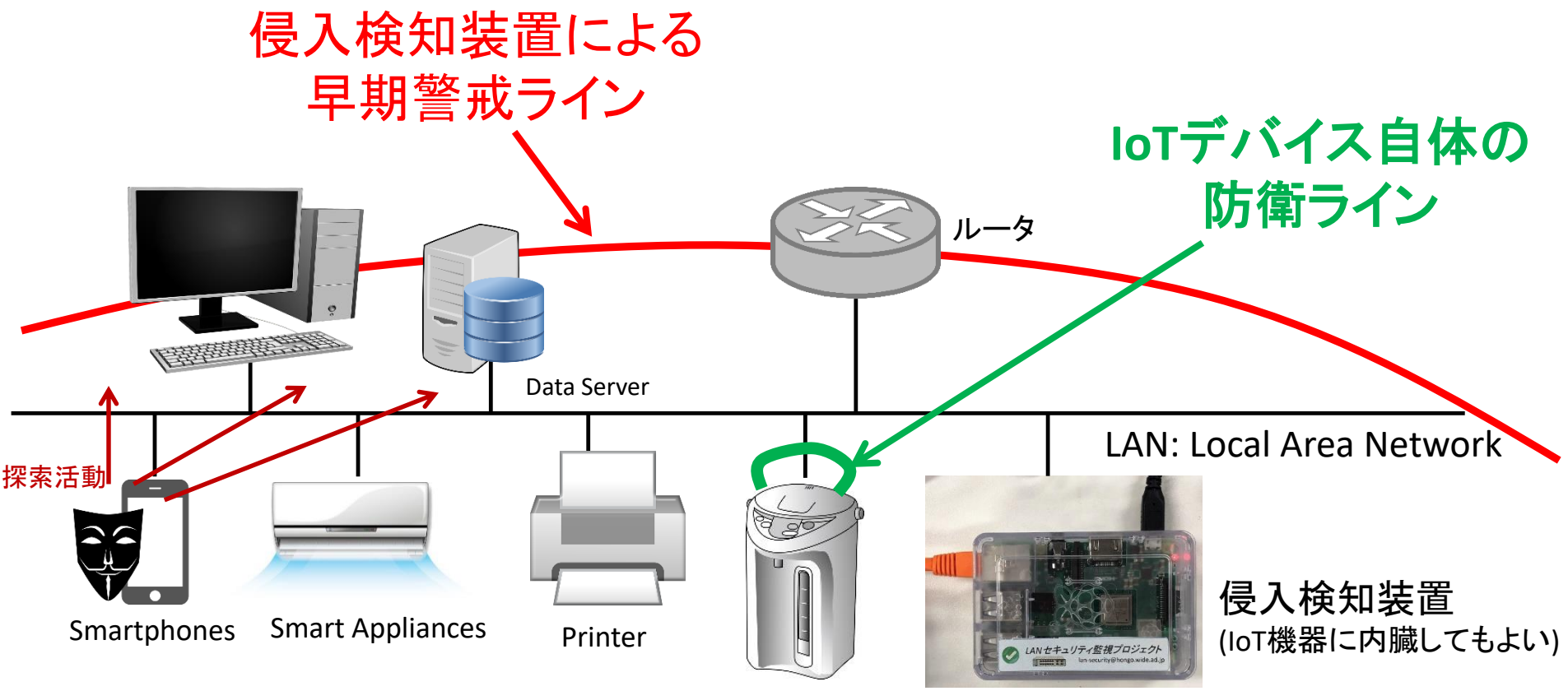
(*注) ここでのIoTサービス事業者とは、遠隔地のLANを利用している事業者のことを指します。

- LAN-Security Monitoring Project 方式で、侵入検知を行うと、LAN内部で発生する前兆に気付くことができる。
- 前兆行動の例： ARP Scan, TCP SYN, Samba Session構築

  ➔「悪意のあるもの」と判定されれば、警報発令



侵入検知装置による早期警戒：LAN内に LAN-Aware Malware が侵入したら警報発令可能



LAN内探索活動 – 怪しさのレベル

Level 3	監視ノードとのTCPセッションの構築およびその上でのアプリケーション・データ交換
Level 2	TCP SYN スキャンの発生
Level 1	ARP スキャンの発生

Attack to TCP554, TCP445, TCP9100, TCP80, TCP515, TCP139

ランサムウェアに見られる特徴

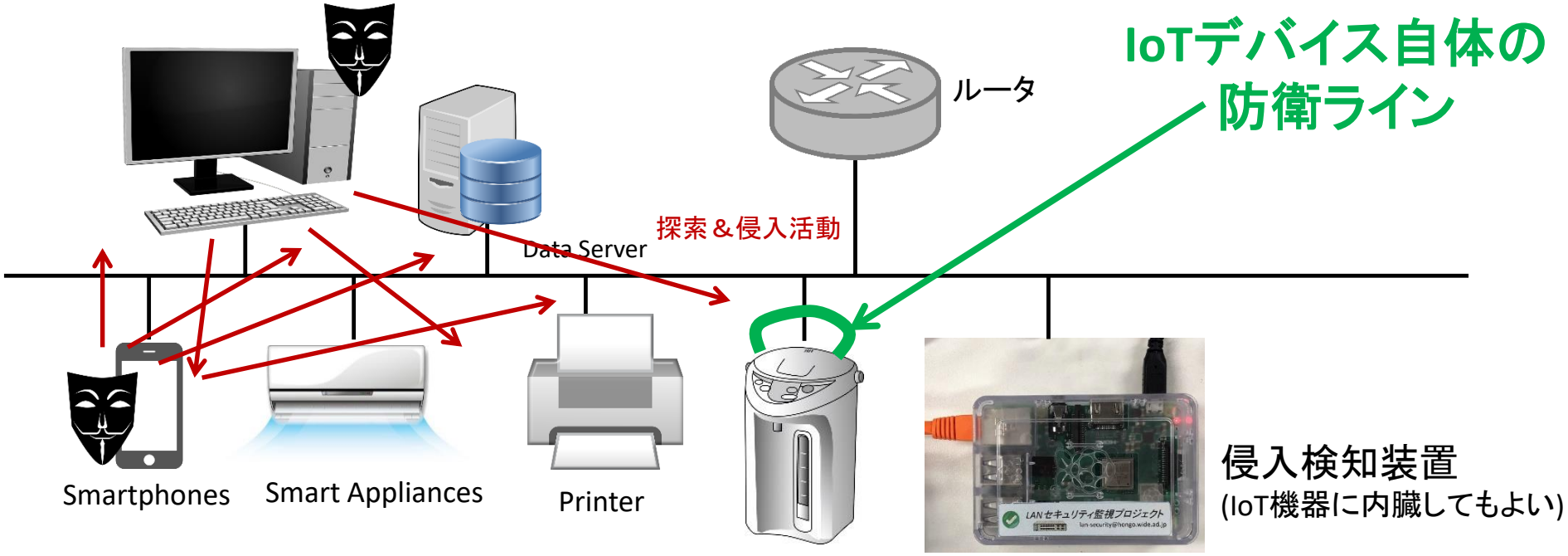
LAN内探索活動 – 怪しさのレベル

(*) LAN Security Monitoring Projectにより作られたモデル

Level 3	監視ノードとのTCPセッションの構築およびその上でのアプリケーション・データ交換	Deep Penetration Testでのみ発生する。通常、このようなテストは、周知＆管理されたうえで実行されるため、マルウェアによる事象との区別は容易。
Level 2	TCP SYN スキャンの発生	比較的簡単に手に入る脆弱性検査ツール（nmap や 簡易セキュリティツール）を実行すると、発生しうる。
Level 1	ARP スキャンの発生	一部のアプリケーション、プログラムが引き起こすことがある。

Level 3 とはどういう状況か？

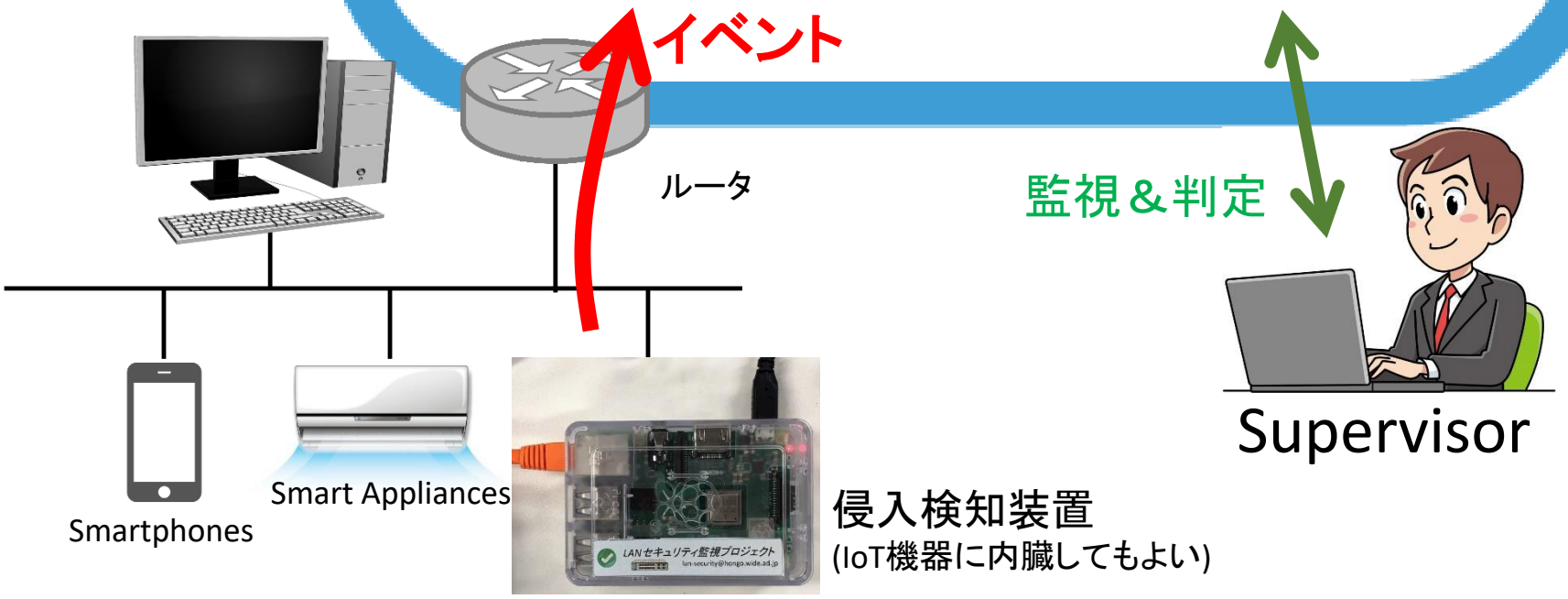
- 常に、LAN内部で、マルウェアがさらに侵入可能なホストを探している状態
- IoTデバイス自体が基本の守りを持っていたとしても、IoTデバイスの目前にまで脅威は迫っている
- 彼らが本気のアクション(プライマリ・アクション)を実施したら、やられてしまう。



LAN Security Monitoring Project方式の侵入検知システムの発展

侵入検知・警報管理システム (機械学習適用)

Event ID	詳細	提案	判定
1	ARP scan	正常	正常
2	ARP scan, TCP SYN …	正常	正常
3	ARP scan, TCP SYN, Samba …	警報	警報
4	ARP scan …	正常	正常
…			



侵入検知・警報管理システムの動作

- Anomaly (通常と違う状況)があれば、イベントとして発報する
- Supervisorが「正常」または「警報」の判定をする。
- この判定をもとに、正常と警報を自動的に分類できるようになる。

- 導入時は、多くのイベントが発報されることが予想されるが、運用を積み重ねるにつれ、判定精度の向上が期待される。

迷惑メールフィルタ判定の学習（メーラーの画面）を
イメージしていただけるとわかりやすいかも。。。。

さらなる発展形

- ネットワーク監視データを Cloud に Exportしない形での運用
  - Edge Computing
  - Federated Learning
- Federated Learning : Google 等により提案

  フェデレーテッドラーニングは、データサンプルを交換することなく、ローカルデータサンプルを保持している複数の分散型エッジデバイスまたはサーバーにわたってアルゴリズムをトレーニングする機械学習技術です。

  (from WikipediaのGoogle自動翻訳)

まとめ

- IoTの展開においては、展開先の現場のネットワークに現れた潜在的な脅威にいち早く気付いて、（顧客より先に）行動を起こすこと、が大事。
- Product Security Incident Response Team (PSIRT)は、一見、IoT機器の「インシデント対応チーム」と読めるが、実際には、製品内に見つかった脆弱性を除去するための組織の在り方を示したもの。
- Product Security Operation Center (PSOC) の概念が必要・・・現場のIoT機器に対する目前の脅威に気付くため
- IoTでは、製品だけ守っても、ネットワーク的に守らなければ、サイバー攻撃から身を守ることは不可能である。
- LAN内の侵入検知システムは、身近に現れた潜在的な脅威に顧客より先に気付くためにも、有用である。