資料３－３

IoT時代のサイバー攻撃対策の課題

平成28年1月21日

一般財団法人　日本データ通信協会
テレコム・アイザック推進会議
小山　覚

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

モノがネットにつながるリスクとは

交通標識が「ゴジラ襲来」と警告、米国でハッキング被害

[ボストン　6日　ロイター] - 米政府は5日、サンフランシスコなどで電子交通標識がハッキングされ、交通情報が不正に変更されたことを受け、電子標識を運営する企業などにセキュリティー強化に向けた防止策を講じるよう勧告した。2014年 06月 9日 14:38 JST

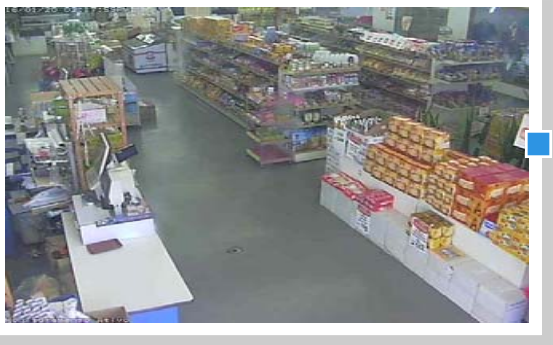
http://jp.reuters.com/article/oddlyEnoughNews/idJPKBN0EK0A020140609

無防備なWebカメラの監視画像を見せるInsecam

Watch Panasonic camera in
Japan
Shibuya-Ku

Watch Panasonic camera in
Japan
Inazawa

Watch Panasonic camera in
Japan
Osaka



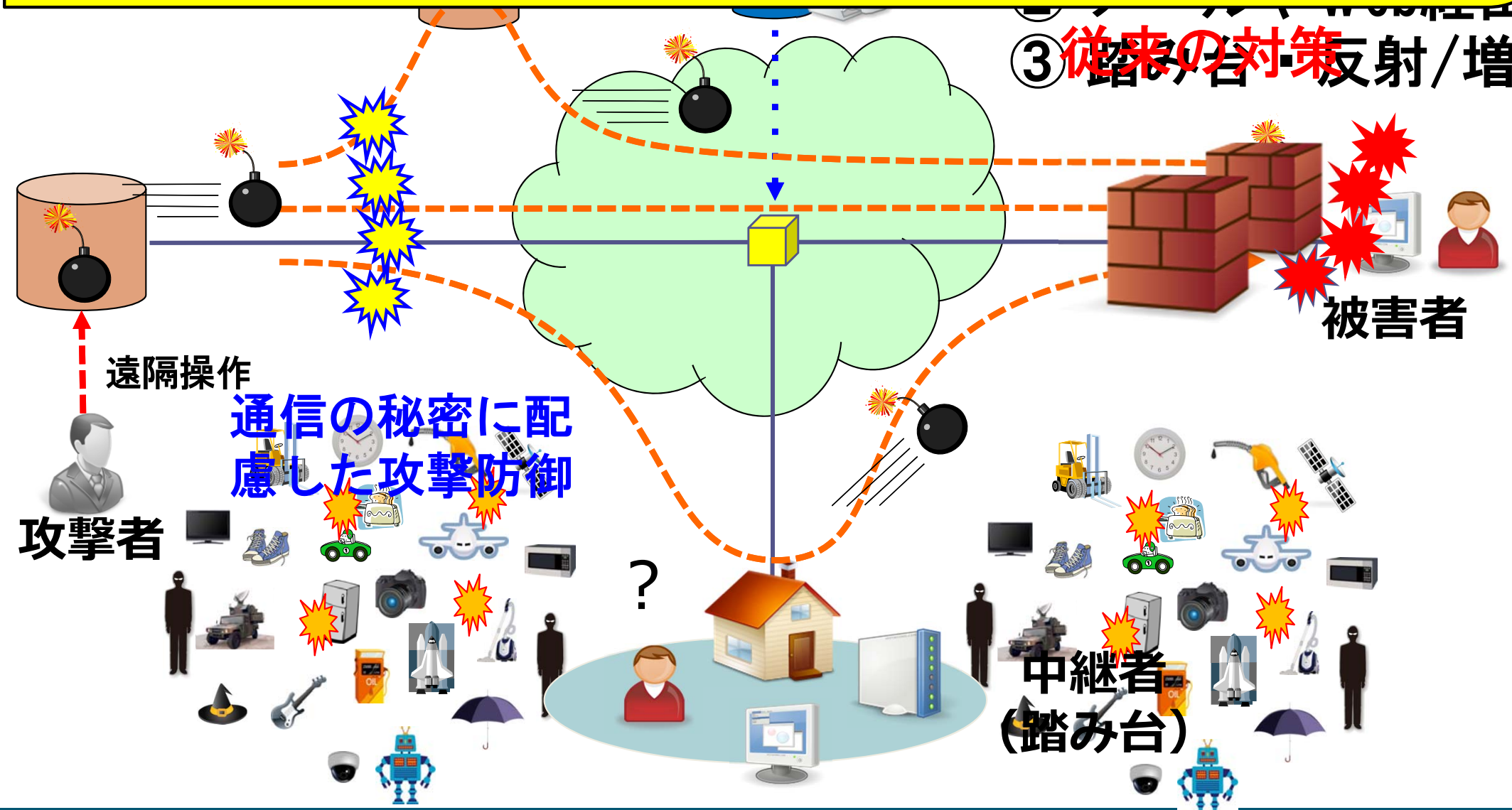
Watch Panasonic camera in
Japan
Numazu

Watch Panasonic camera in
Japan
Obu

Watch Panasonic camera in
Japan
Takamatsu

サイバー攻撃対策と通信事業者の現在の役割

脆弱な機器を踏み台にした攻撃対策が課題

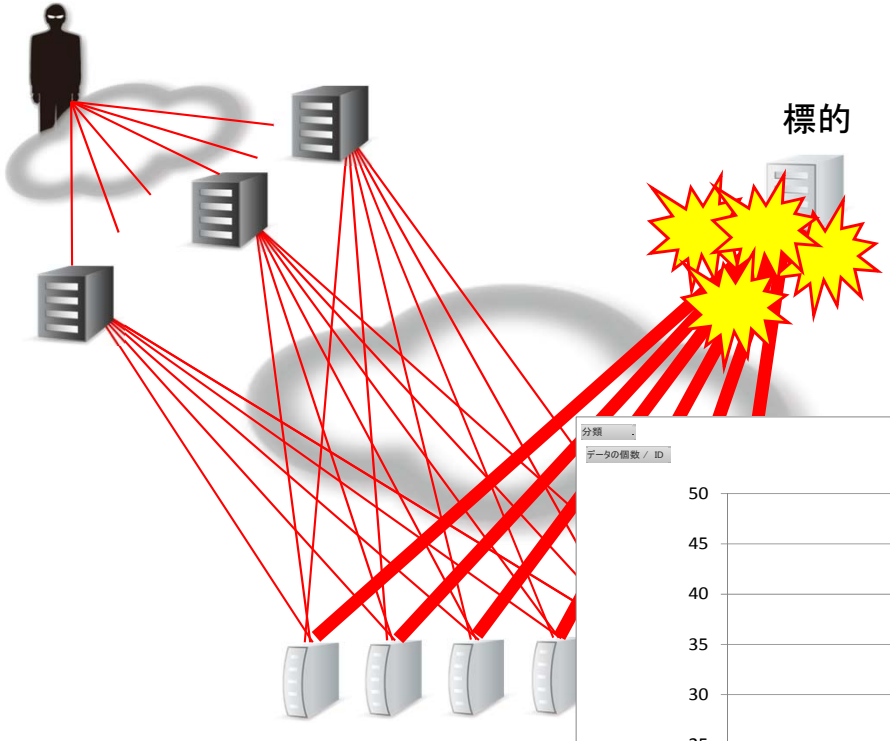


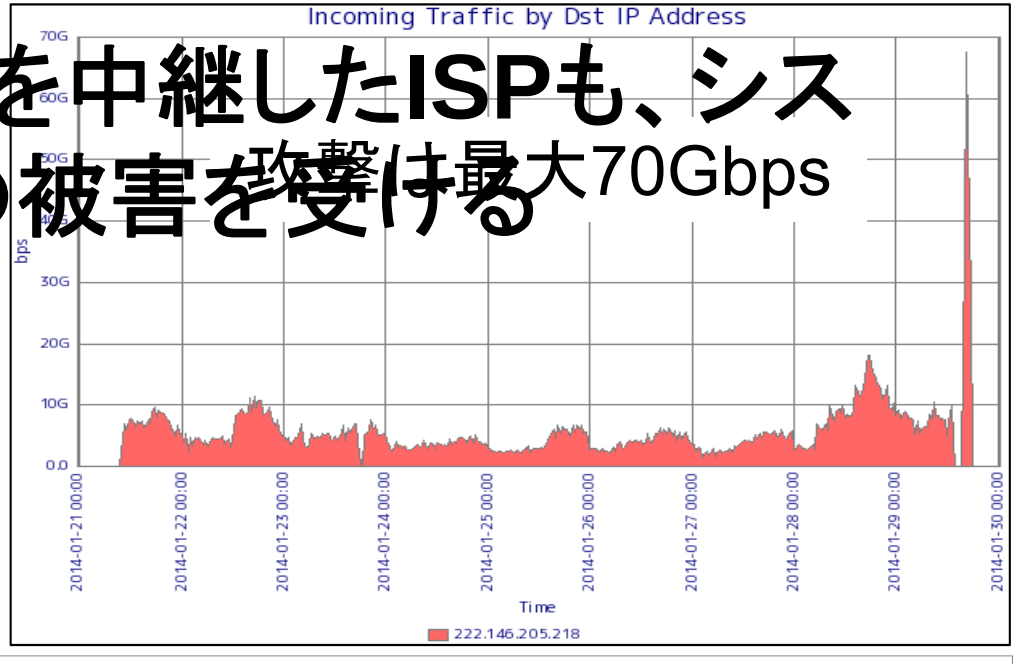
反射・増幅(リフレクション)攻撃事例

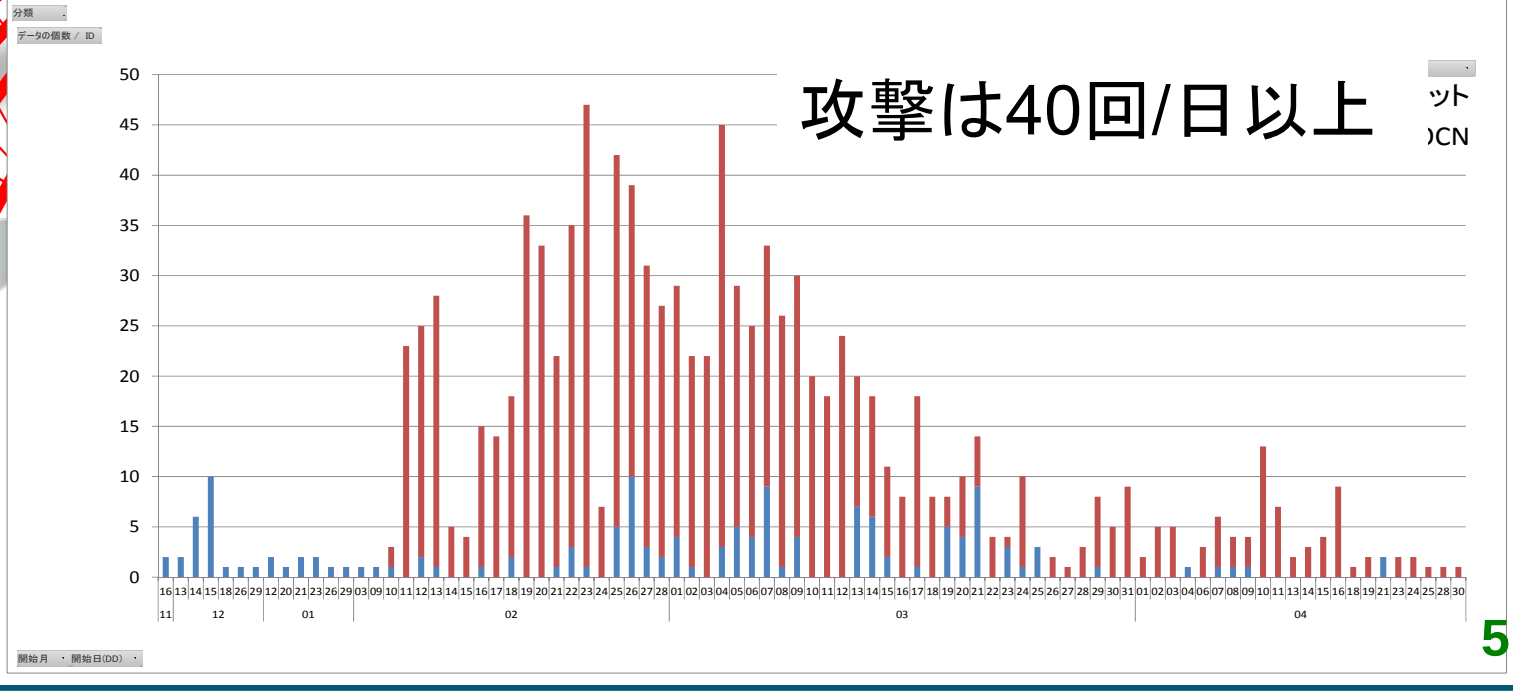
Telecom SAC Japan

標的だけでなく、攻撃を中継したISPも、システム停止等の被害を受ける

攻撃者







DD4BC攻撃の事例

■2015年7月13日21時47分の朝日新聞より抜粋
セブン銀など2社にサイバー攻撃　サービスに一時支障

大量のデータを送りつけてサーバーの機能を止める「DDoS（ディードス）」と呼ばれるサイバー攻撃をセブン銀行など2社が受け、ネット上のサービスに支障が出ていたことが分かった。相談を受けた警視庁によると、セブン銀には、攻撃を止める条件として仮想通貨ビットコインでの支払い要求もあったという。

攻撃があったのはセブン銀と、金融サービスを展開するGMOクリックホールディングスの子会社、FXプライムbyGMO。

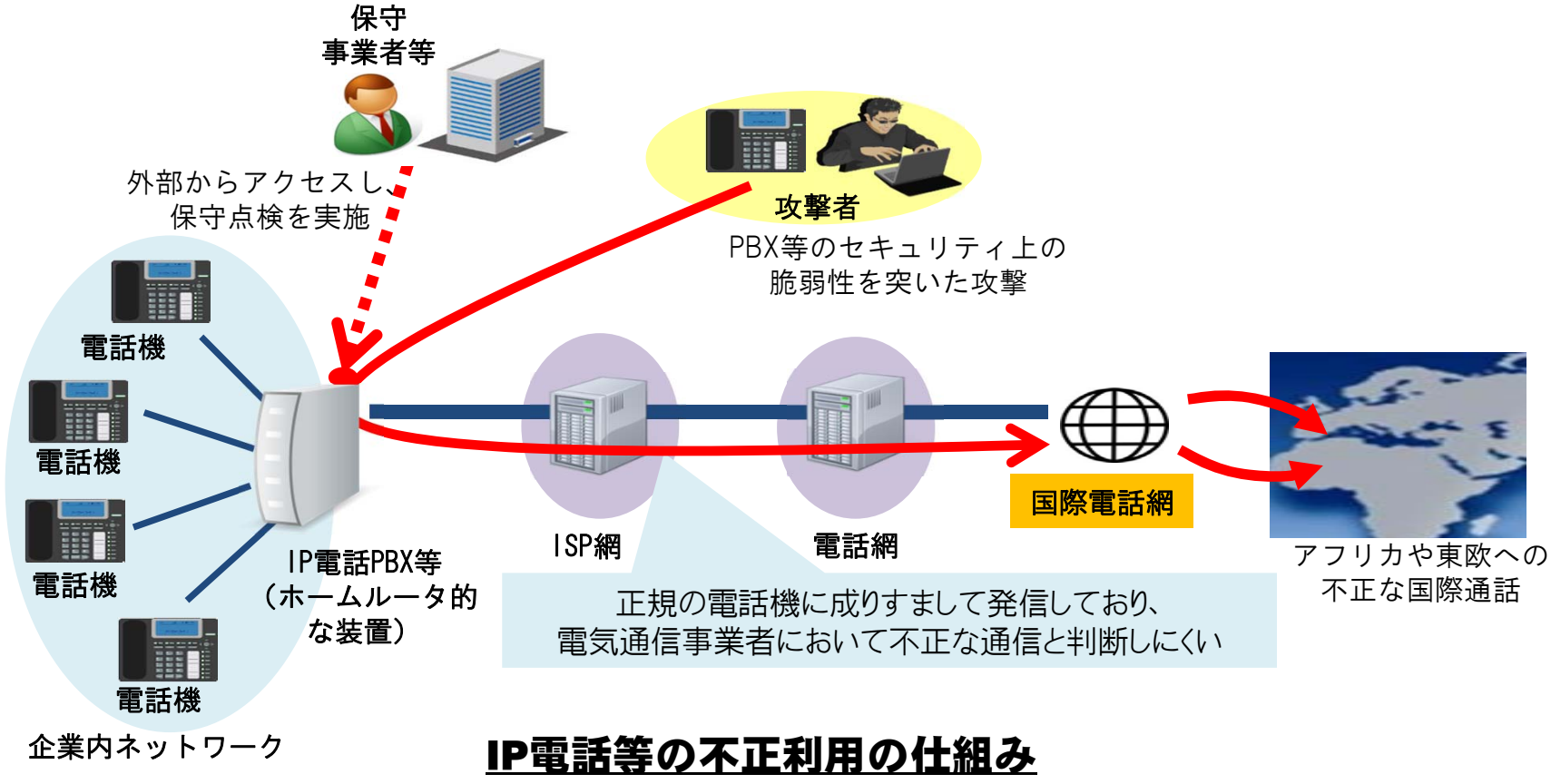
両社の発表によると、セブン銀では6月25日午前の2時間近く、パソコンやスマートフォンから残高照会や振り込みができるサービスの取引画面につながりにくくなった。GMO子会社では5月22日の正午前後の1時間余り、外貨取引のサイトに利用者がアクセスできなくなった。攻撃に伴う個人情報の流出やデータ破損などは両社とも「ない」としている。

警視庁はセブン銀から通信記録の提出を受けるなどして捜査を進める方針。

第三者によるIP電話等の不正利用

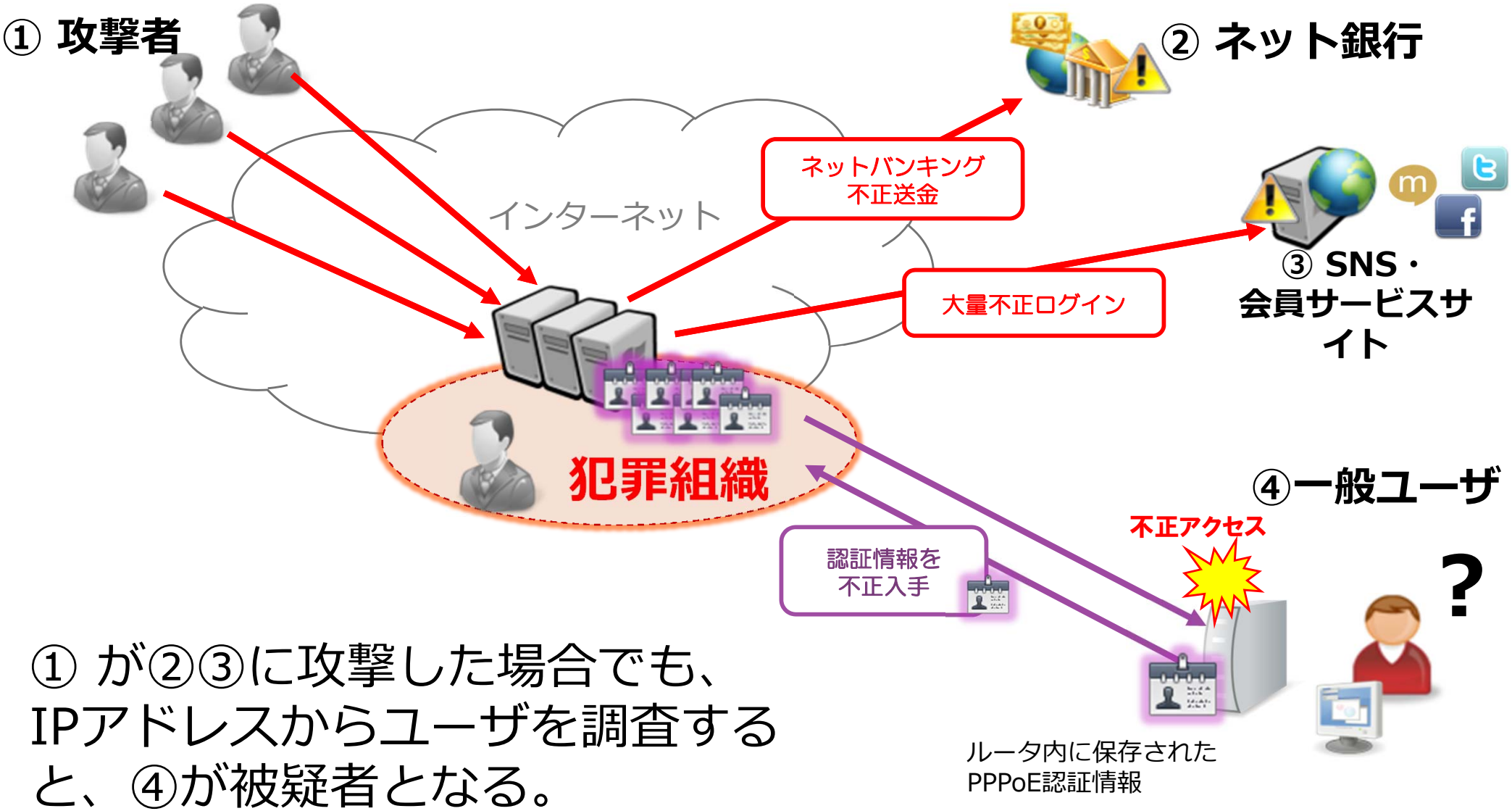
○平成22年頃から多くのIP電話事業者等で発生　→　**平成27年7月7日総務省から対処要請発出**

○**個人事業主などの中小企業等が利用しているPBX**（内線電話を実現するための交換装置）のうち、**保守等のため外部からのアクセスが可能な装置がセキュリティの脆弱性をつかれる**サイバー攻撃を受け、**PBXが海外に電話をつなぎっぱなし**となるといった事象。



IP電話等の不正利用の仕組み

ホームルータが犯罪の温床（踏み台）



① が②③に攻撃した場合でも、IPアドレスからユーザを調査すると、④が被疑者となる。

[2014年11月]　警察によるプロキシ業者の一斉摘発

- 2014年2月に引き続き、11月20日、サーバー運営会社「大光」「SUNテクノ」に所属する中国人国籍の容疑者６人を逮捕。上記2社は約1500人分の認証情報を不正に取得
- 警察の調べでは両者のプロキシサーバを通じて、約4.5億円のネットバンキング不正送金が行われていた(2014年1～6月)ほか、企業の顧客情報(10万件)流出事件でも使用されていた

IDなど1500人分取得、摘発のサーバー2社　中国人に売る

2014/11/20 0:47

小 中 大　保存　印刷　リプリント　▼共有

インターネット接続を中継する「プロキシサーバー」の運営会社による不正アクセス事件で、警視庁が摘発した2社が、計約1500人分のIDやパスワードを不正に取得し、中国人の顧客に売っていたことが19日、同庁の調べで分かった。同庁はこれらのIDなどがインターネットバンキングの不正送金などに使われたとみている。

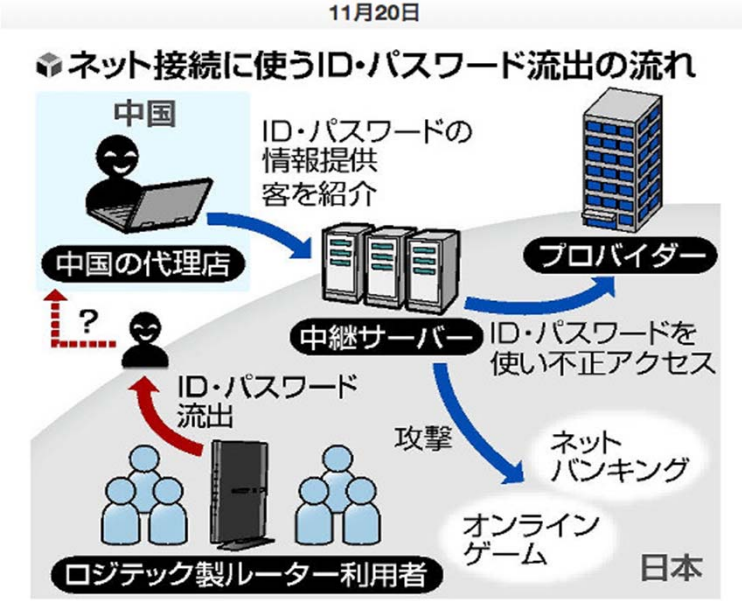
警視庁は19日、サーバー運営会社「大光」（東京・台東）の社長で中国籍の張徳育容疑者（30）＝東京都北区、「SUNテクノ」（東京・豊島）の元役員で中国籍の高志中容疑者（32）＝豊島区＝ら6人を不正アクセス禁止法違反容疑で逮捕した。同庁によると、6人はいずれも「分かりません」などと容疑を否認している。

警視庁によると、両社はIDなどをブローカーから不正に取得し、中国の代理店を通じて中国人顧客に1件あたり1700～5千円程度で販売していた。大光は少なくとも計8千万円、SUNテクノは計4600万円を得ていたという。

顧客は両社のプロキシサーバーを通じ、不正取得したIDやパスワードで日本の接続業者にアクセスしていた。

警視庁は今年1～6月に300件超、4億5千万円のインターネットバンキングの不正送金が両社のサーバーを通じて行われたとみている。携帯電話レンタル会社の顧客情報約10万件が流出した事件でも、大光のサーバー経由でシステムが攻撃されていたという。

(出典) 日本経済新聞(11月20日)



(出典) KandaNewsNetwork

脆弱なホームルータ対策は時間とお金がかかる

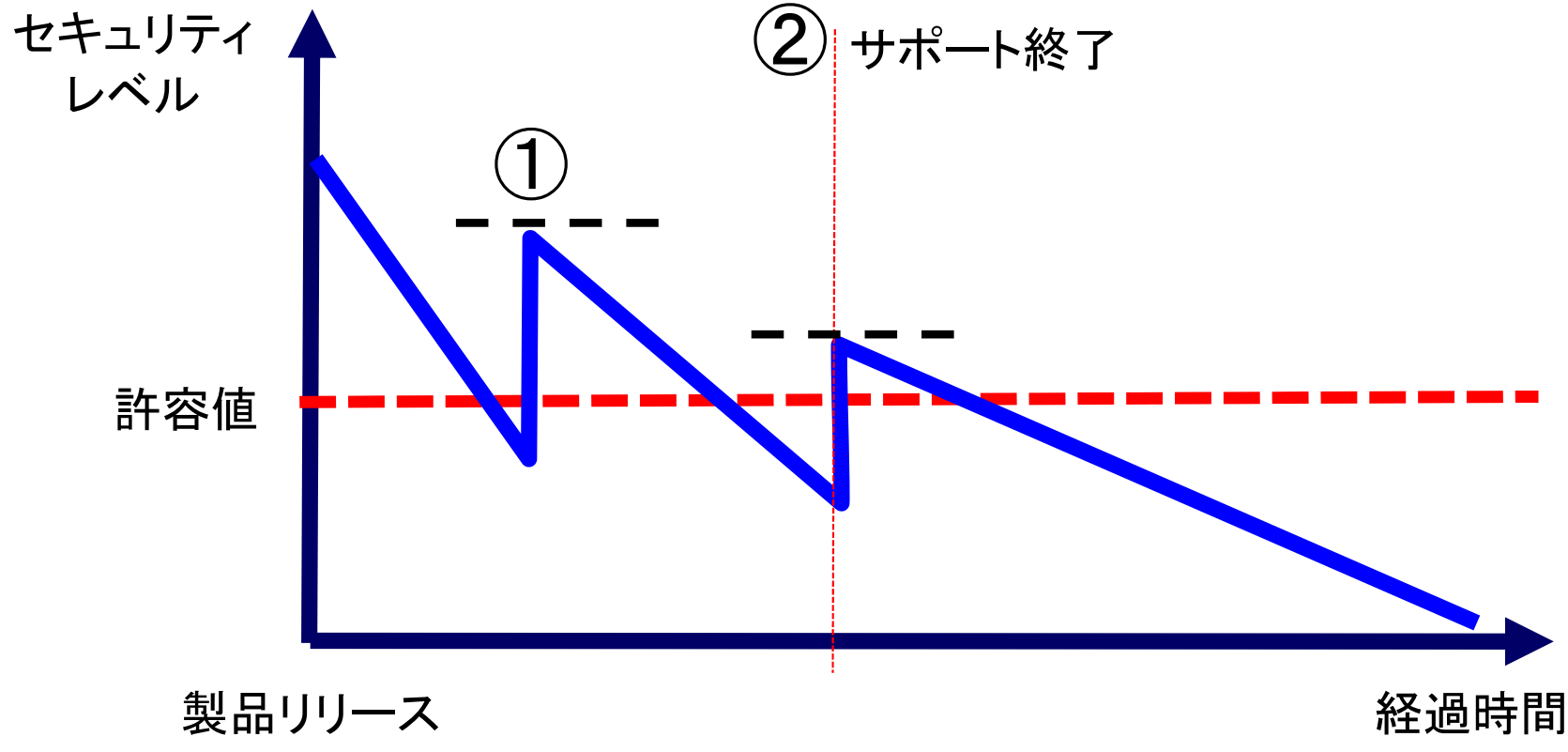
- ソフトウェアアップデートする利用者は1%未満
  →利用者への注意喚起のみでは効果が無い
  強制的なアップデートが必要？

- ユーザサポートコストは１万円／件以上
  →1台数千円の機器に対するサポートコストをトータルで最小化する検討と実装が急務

- 本事例では、
  - 問題の沈静化まで３年
  - 数億円の費用

- 再発を防止する社会システムは誰が検討するのか？

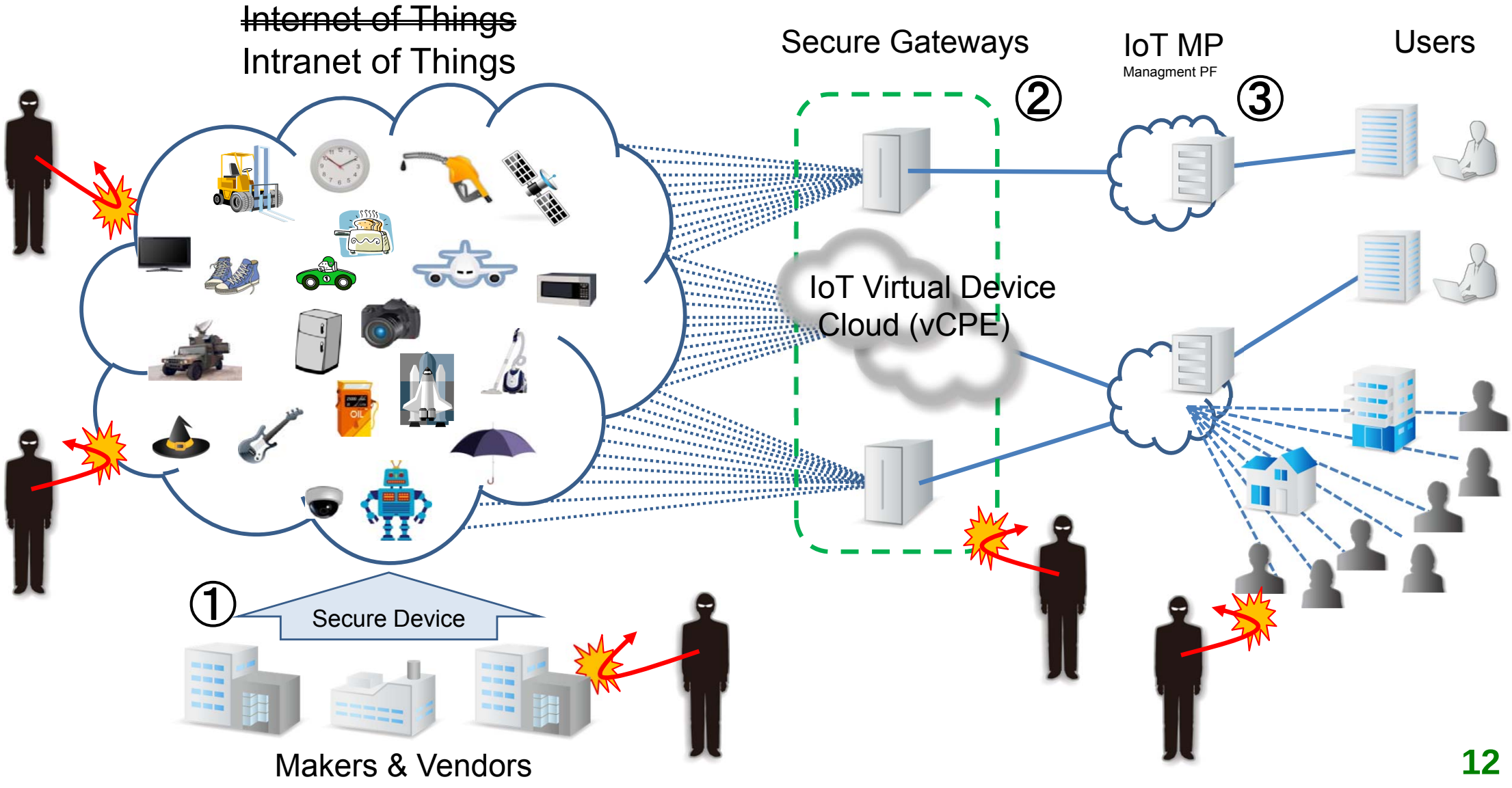
機器の売り切りからサービス提供的なビジネスへ



能動的にファームウェアを更新する利用者が極めて少い前提で、セキュアIoTフレームワークの構築が急務

Secure IoT Framework 1/3

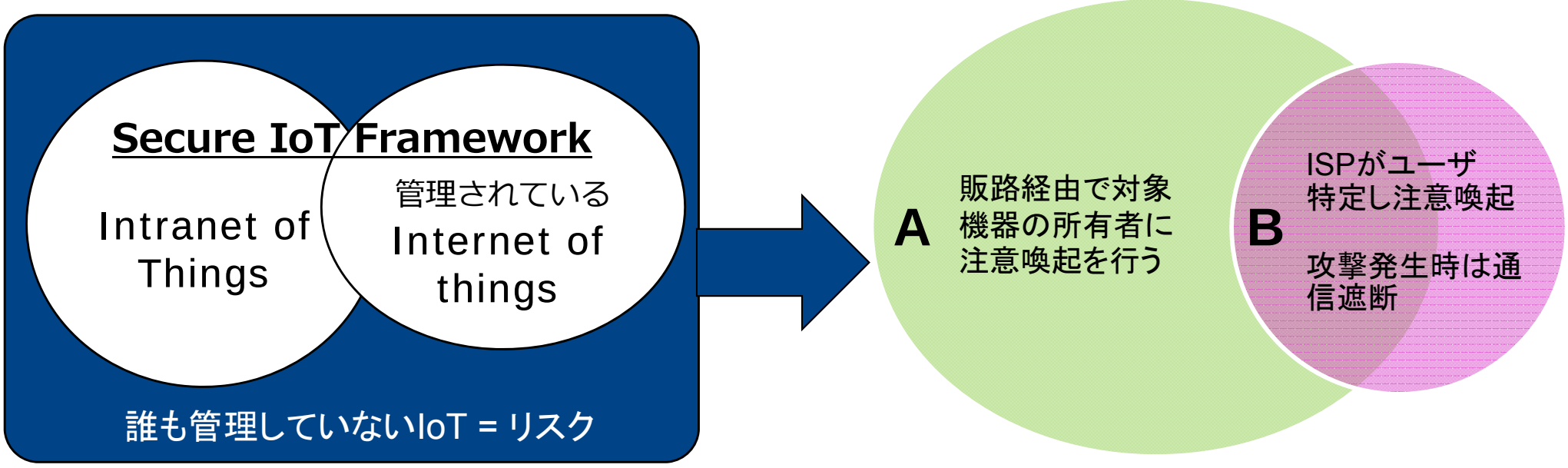
- 10年後も有効に機能する「Secure IoT Framework」をICT関係者で検討
- 各関係業界のガイドラインを作成していきたい。



Secure IoT Framework 2/3

- 脆弱なIoT対策コストのミニマム化を最初から考えておきたい

IoTデバイス250～500億

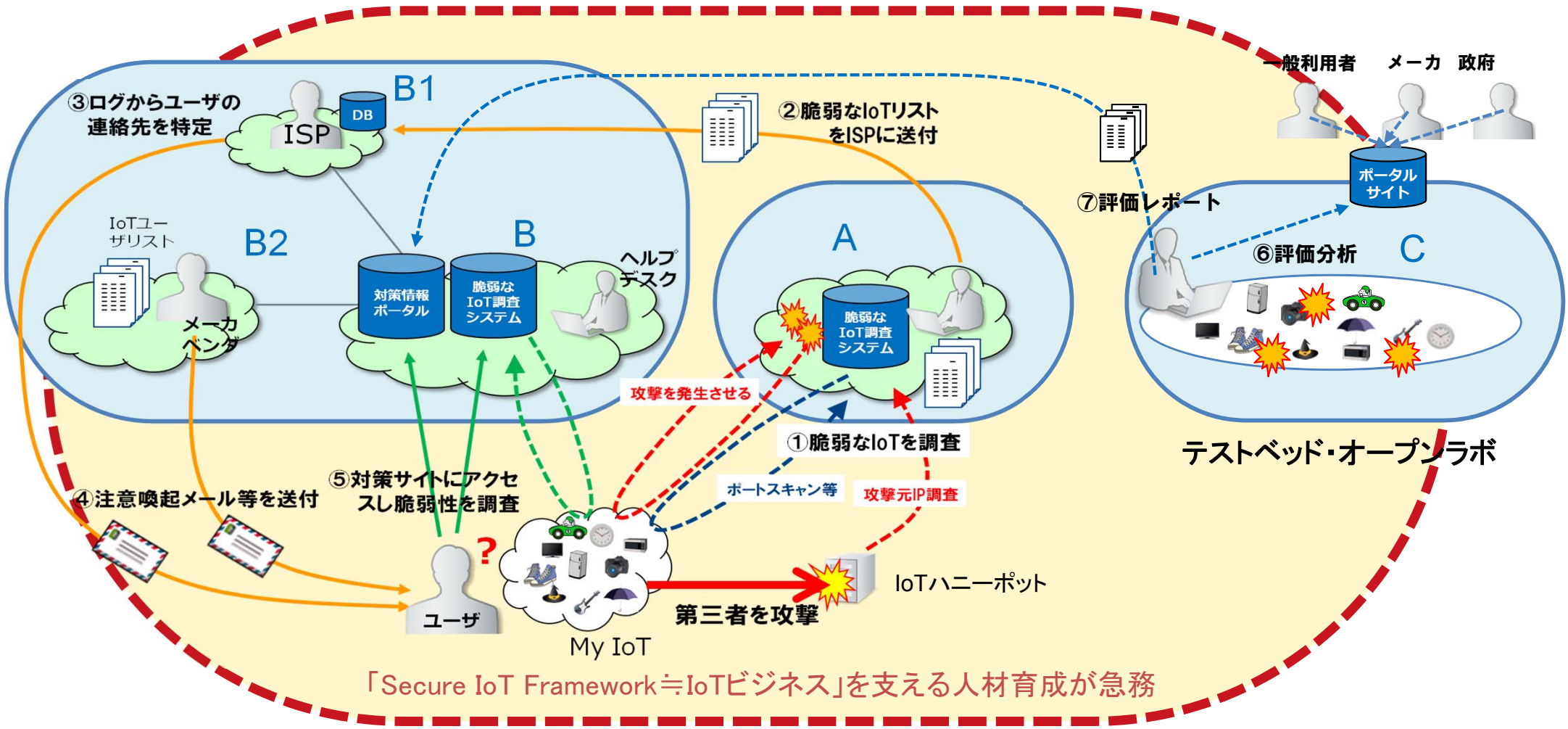


安心・安全なIoTの普及は
ビジネスとして民間が解決する課題

危険な野良IoT対策は、
官民が連携して取り組むべき課題

A：IT機器業界と流通・小売り業界の協力が必要
B：通信の秘密との関係整理が必要

Secure IoT Framework 3/3



2020に向けて関係者間の情報共有と実践的演習の必要性

A：脆弱IoTの調査＆DB化
攻撃の踏み台となるデバイスを調査しDB化

B：注意喚起スキーム
脆弱なIoTデバイスの利用者に注意喚起を行う。

C：テストベット＆オープンラボ
IoTデバイスの脆弱性を調査し製品やサービスの品質の向上の提言。
新技術やサービス開発などベンチャー育成の場（競争力向上）

まとめ

●放置IoTを極力作らない仕組みづくりが重要（ガイドライン）
→Intranet of Things（安くて便利なIoTサービス）
→ファームの自動アップデートなど、長期安心デバイス

●脆弱IoTのDB化と、管理者への注意喚起、対策情報の提供
→官民連携した取り組み（費用「ミニマム化」の枠組み）
適法性に配慮した脆弱IoT調査の検討

●テストベット＋オープンラボ（競争力強化）
→新規ビジネス加速化・ベンチャー創出

●止むを得ない場合は、IoTをネットワークから切り離すなど、緊急避難策の検討（国としての安全弁）

●実践的な演習・訓練の充実化（演習の広さと深さ）

●日本の成功事例を国際展開する取組みとしたい

ご清聴ありがとうございました