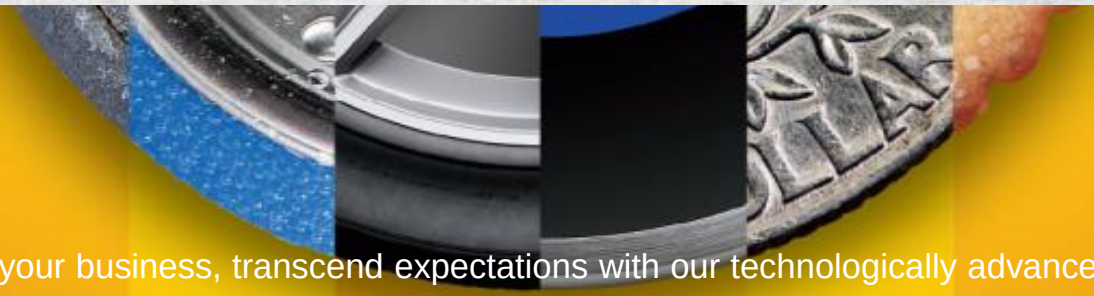
NTT Communications
Transform. Transcend.

サイバー攻撃対策としての IoTセキュリティについて

資料2－3

2017年3月8日

NTTコミュニケーションズ株式会社
小山 覚

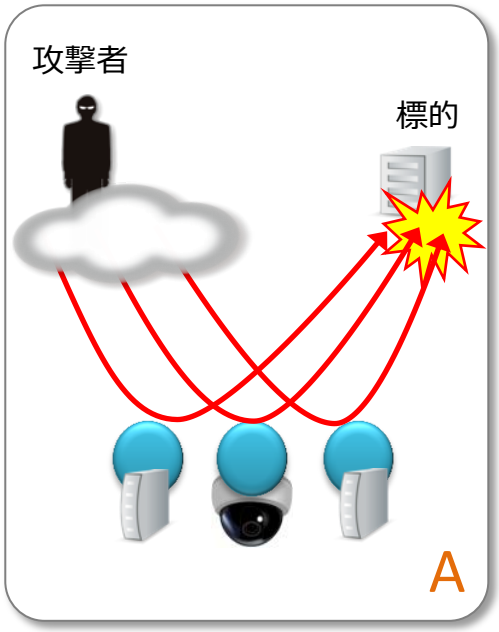


Transform your business, transcend expectations with our technologically advanced solutions.

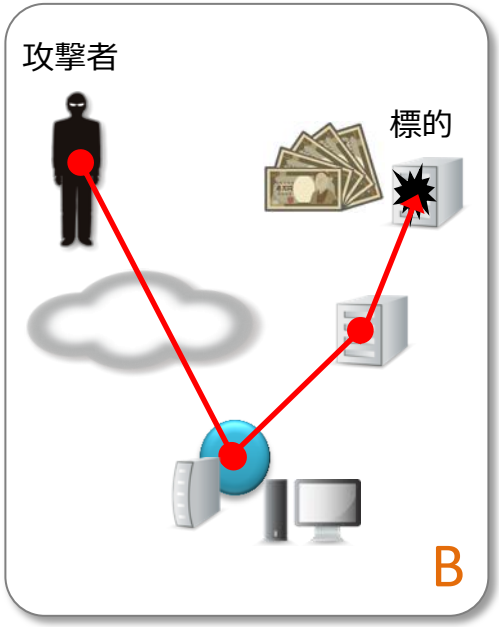
IoTが関係するサイバー攻撃の4パターンと打ち手

●IoTの普及に伴い「愉快犯やイタズラ」でも、社会・生活が混乱する事態を想定すべき

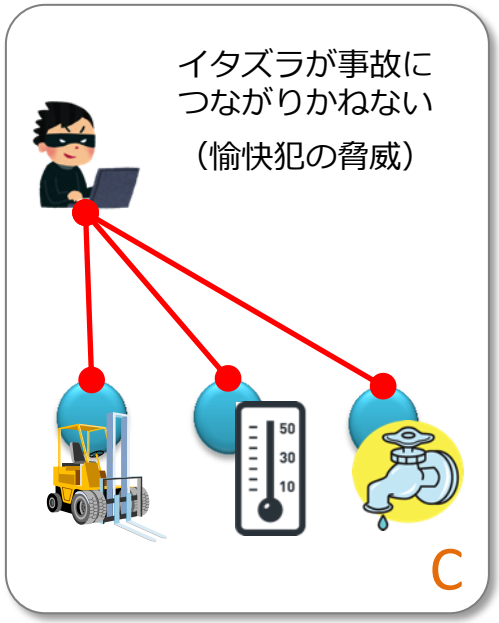
リフレクション攻撃



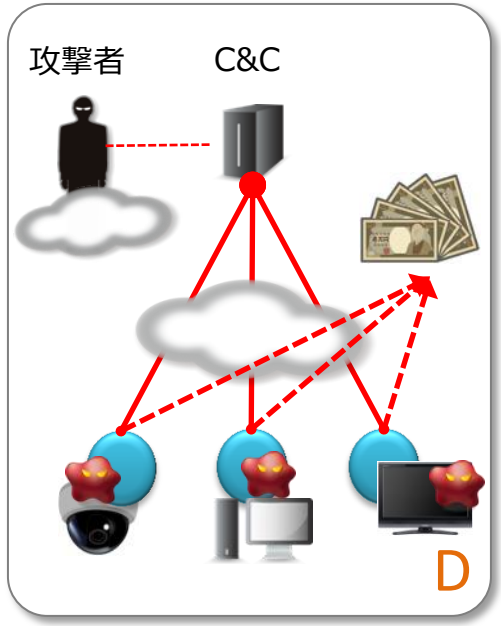
サイバー犯罪の踏み台



社会・生活のリスク



ボットネットの基盤

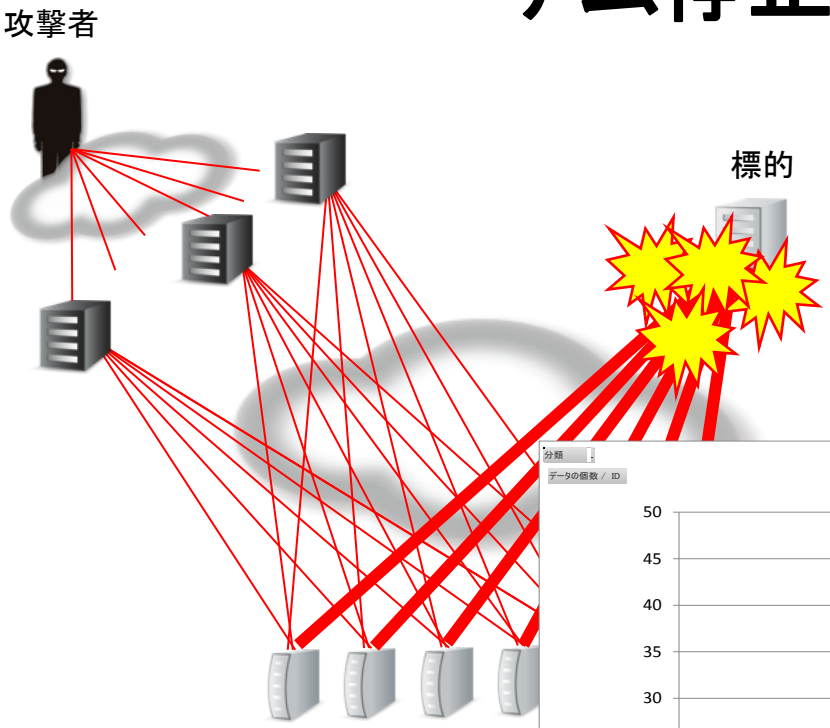


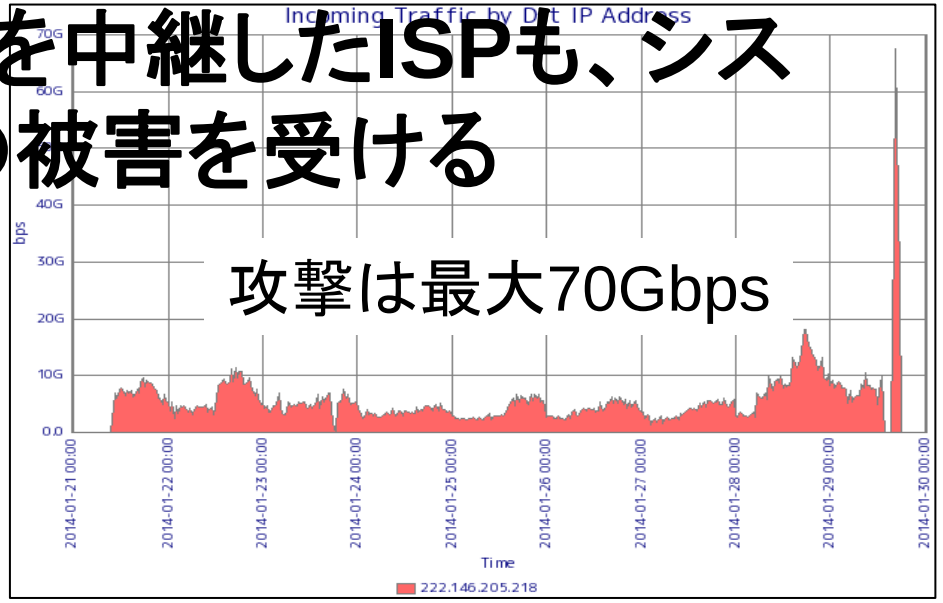
●IoTのセキュリティ対策を「PC・スマホ」並みに高める枠組みが必要

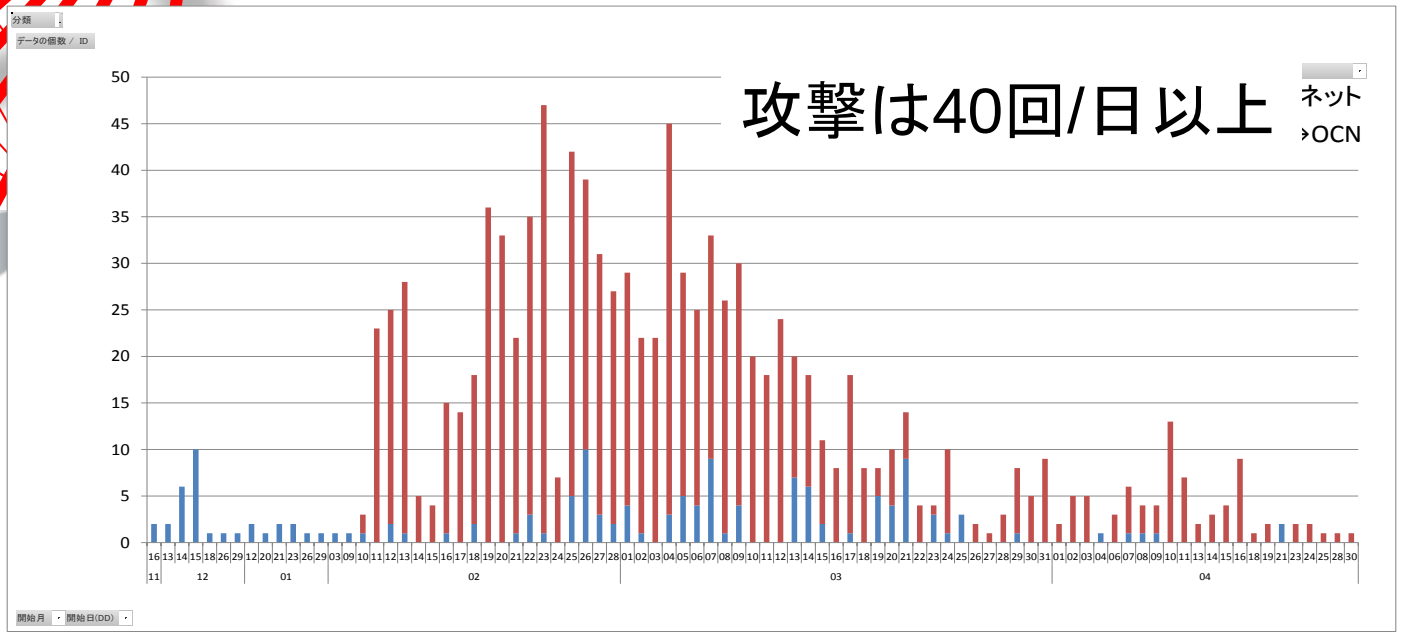
	出荷時の製品 セキュリティ	OS・ファームウェア 更新の容易性	マルウェア対策	セキュリティ研究
PC・スマホ	○	○	○	○
ルータ等NW機器	△	△	×	△
家電・IoT	×	×	×	×

A.リフレクション攻撃事例（2014年1月）

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







B.サイバー犯罪の踏み台（2012年～）

- 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。

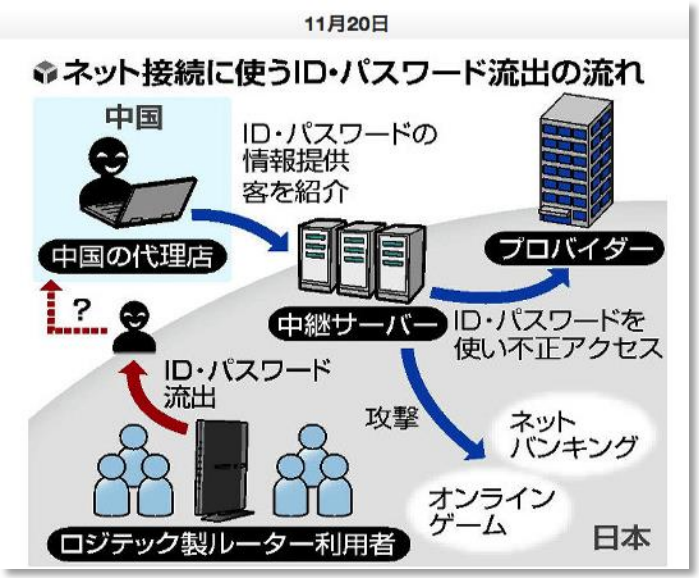
警視庁は19日、サーバー運営会社「大光」（東京・台東）の社長で中国籍の張徳育容疑者（30）＝東京都北区、「SUNテクノ」（東京・豊島）の元役員で中国籍の高志中容疑者（32）＝豊島区＝ら6人を不正アクセス禁止法違反容疑で逮捕した。同庁によると、6人はいずれも「分かりません」などと容疑を否認している。

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

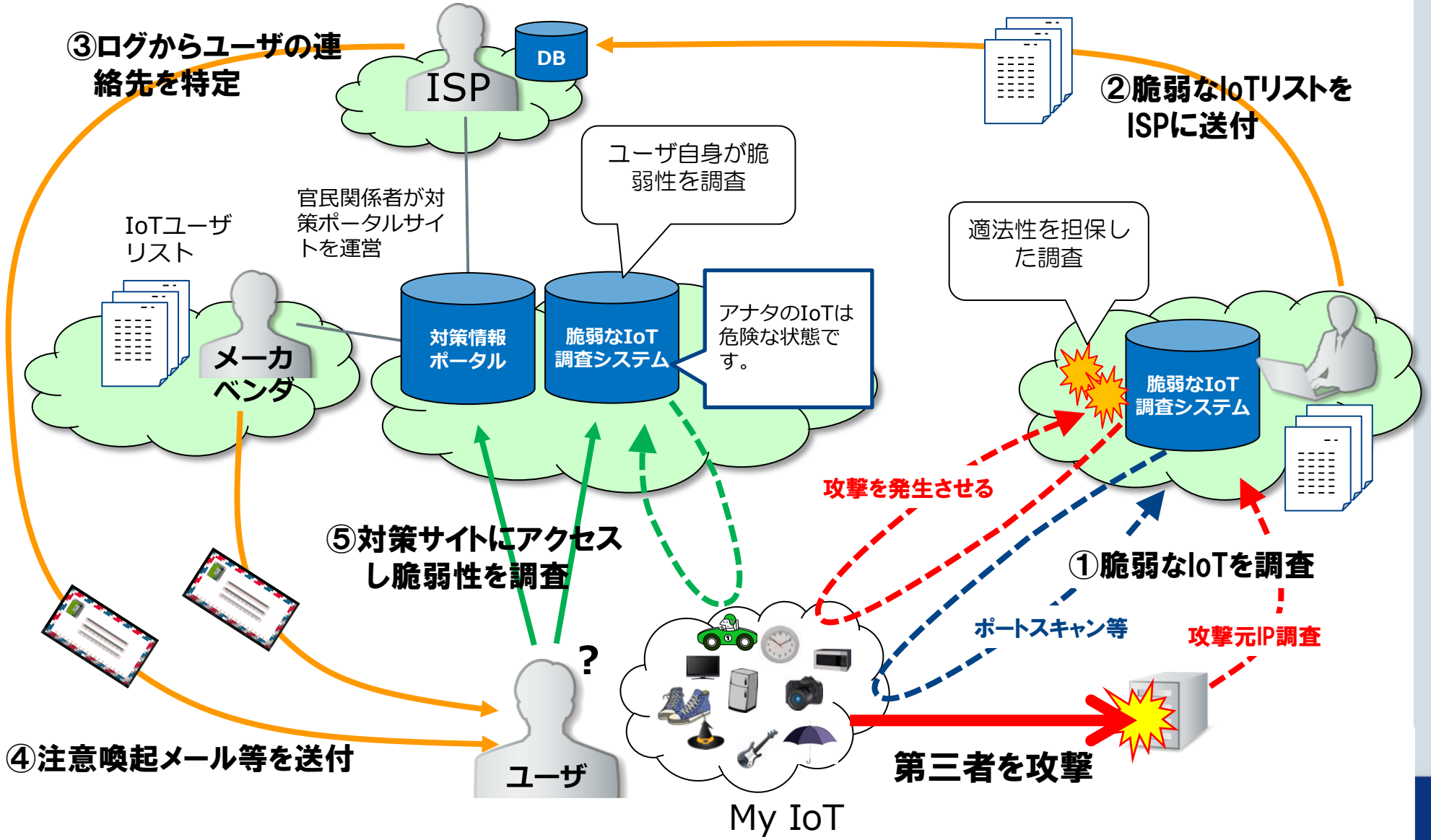
C.モノがネットにつながるリスクを再認識

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

Secure IoT Farmworkの運営イメージ



2015年2月25日　総務省情報セキュリティアドバイザリーボード 戦略ワーキンググループ 資料から抜粋

まとめ

- 放置されたIoT（野良IoT）を極力作らない仕組みづくりが重要
- 野良IoTの管理者を見つけて、対策を促す注意喚起と、適切な対策情報の提供が必要
- 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、安全対策の検討を行うべき
- 通信の秘密や不正アクセス禁止法など、適法性の担保が重要課題
- 日本の成功事例を国際展開する取組みとしたい

2015年2月25日　総務省情報セキュリティアドバイザリーボード 戦略ワーキンググループ 資料から抜粋

対策の結果、無防備なWebカメラ（Insecam）は1年間で1/4に減少

2016年1月21日

1 ... | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | **36** | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | ... 1154

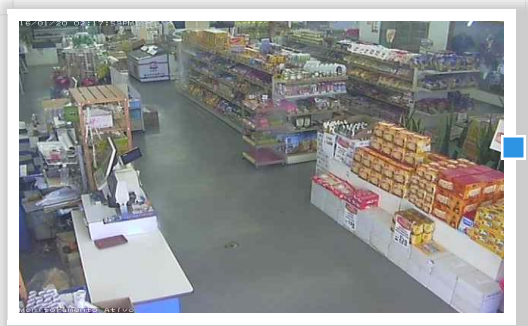
300ページ

（2017年3月5日）

Watch Panasonic camera in
Japan
Shibuya-Ku

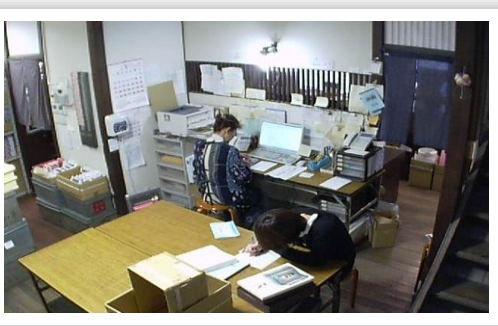
Watch Panasonic camera in
Japan
Inazawa

Watch Panasonic camera in
Japan
Osaka



Watch Panasonic camera in
Japan
Numazu

Watch Panasonic camera in
Japan
Obu

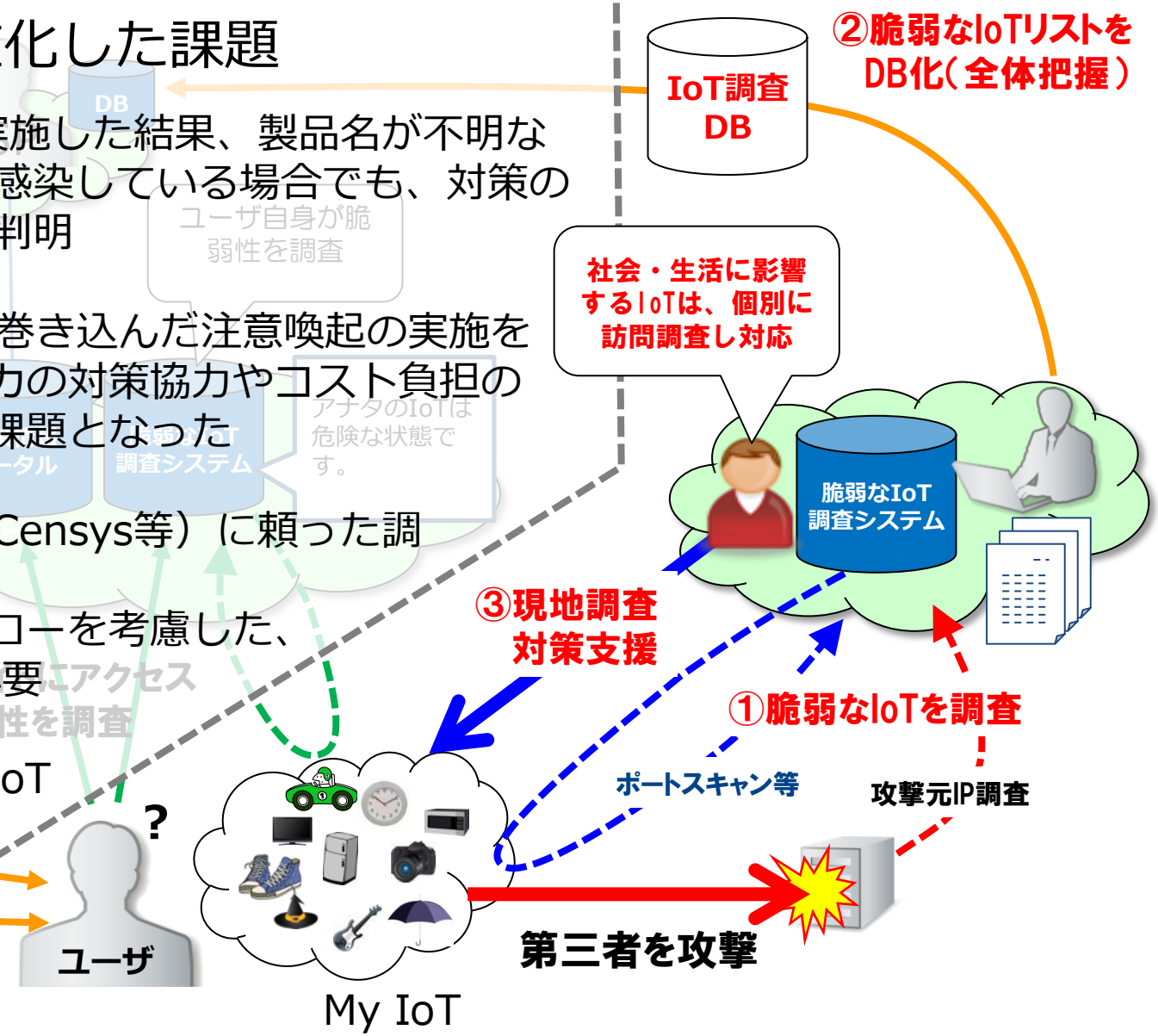


Watch Panasonic camera in
Japan
Takamatsu

IoTセキュリティ対策の現状と課題・今後の打ち手

2015年2月以降に顕在化した課題

- リモートからIoTの調査を実施した結果、製品名が不明な機器が多く、マルウェアに感染している場合でも、対策のアドバイスが難しいことが判明
- 脆弱なIoTに対して、ISPを巻き込んだ注意喚起の実施を目指していたが、製品メーカの対策協力やコスト負担の整理などが実現に向けての課題となった
- 海外の調査DB（SHODAN/Censys等）に頼った調査や対策は限界がある。
  調査から対策までの作業フローを考慮した、
  独自の調査ツールとDBが必要
- 社会や生活に影響がある、IoTについては、現地の設置環境や施工面の状況調査と、対策の支援が必要



P6で示した仮説を検証し、重点3項目を抽出

ご清聴ありがとうございました