資料６－２

産官+国際連携による
セキュア IoT フレームワーク構築について
～東京2020に向けた取組み～

NTTコミュニケーションズ株式会社
小山　覚
2015年4月6日

Copyright © NTT Communications Corporation. All rights reserved.

顕在化しているIoTのリスク（ブロードバンドルータ）

●脆弱なブロードバンドルータが踏み台となり様々な攻撃が発生している

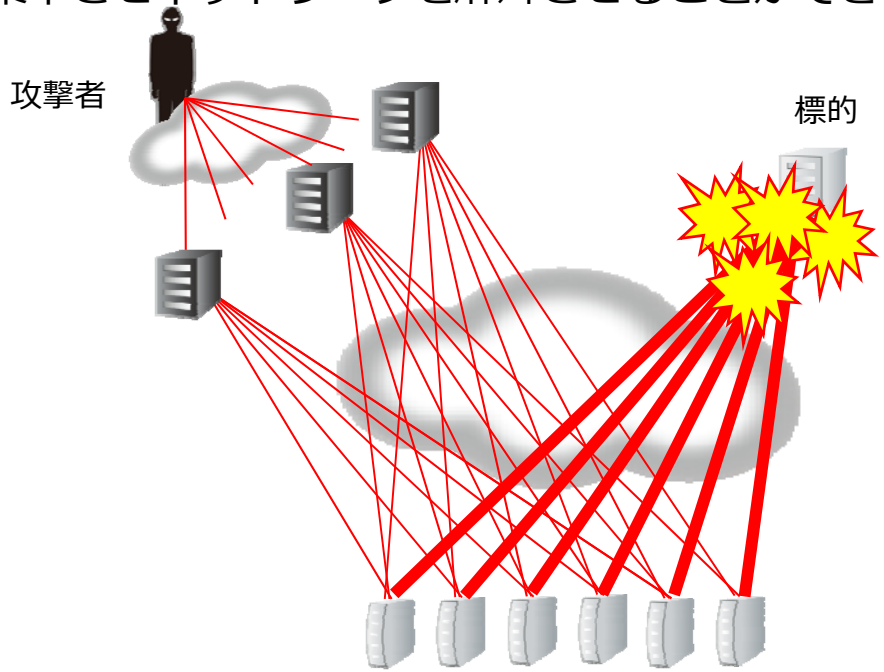
手口	悪用例	被害例	
機器の脆弱性を外部から悪用し、第三者に攻撃を行う	DNSAmpやNTPAmpなどのリフレクション攻撃	標的だけでなく、攻撃を中継したISPも、システム停止等の被害を受ける	①
機器の脆弱性や容易なパスワードから侵入し、攻撃や犯罪に利用する	機器を不正に操作し、攻撃の踏み台として悪用する	犯罪行為の隠れ蓑として悪用される被害を受ける	②
	ISP接続情報が抜かれ、別の機器から、第三者に成りすまして悪事を働く	ネットバンキング不正送金等の犯罪の温床となる不正プロキシに利用 SPAM送信、IP電話不正課金などの被害も受ける	③

Copyright © NTT Communications Corporation. All right reserved.

①リフレクション攻撃の事例（NTPAmp攻撃の一例）

- NTP(Network Time Protocol)は、パソコンの時刻を自動で補正する等の目的で、NTPサーバに問合せを行う際に用いられる。

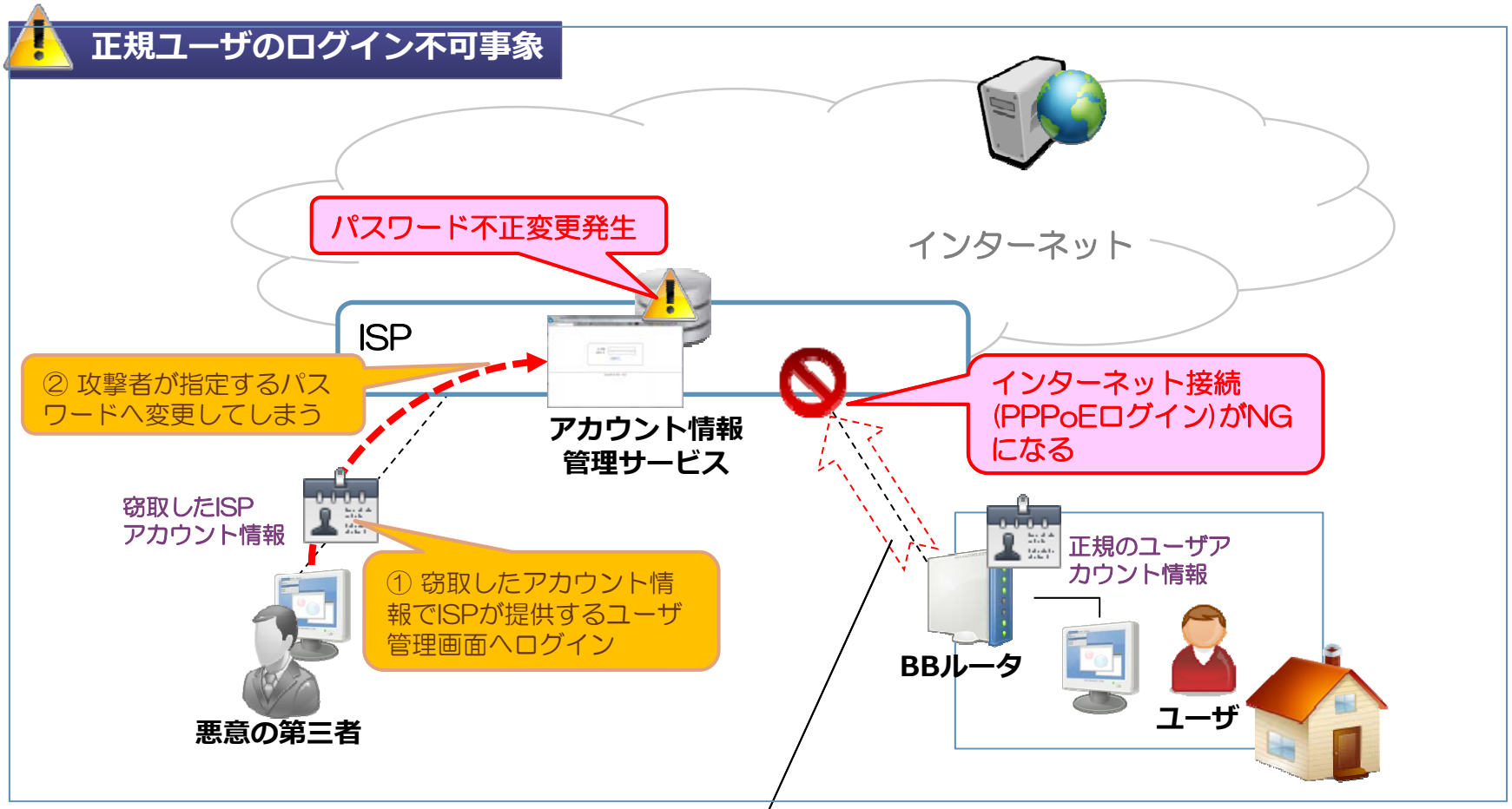
  ※ある問合せの回答先IPアドレスを他人のIPアドレスに書き換えることで、大量の通信を集中させネットワークを麻痺させることができる。



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

Copyright © NTT Communications Corporation. All right reserved.

②機器を不正に操作し攻撃の踏み台として悪用する

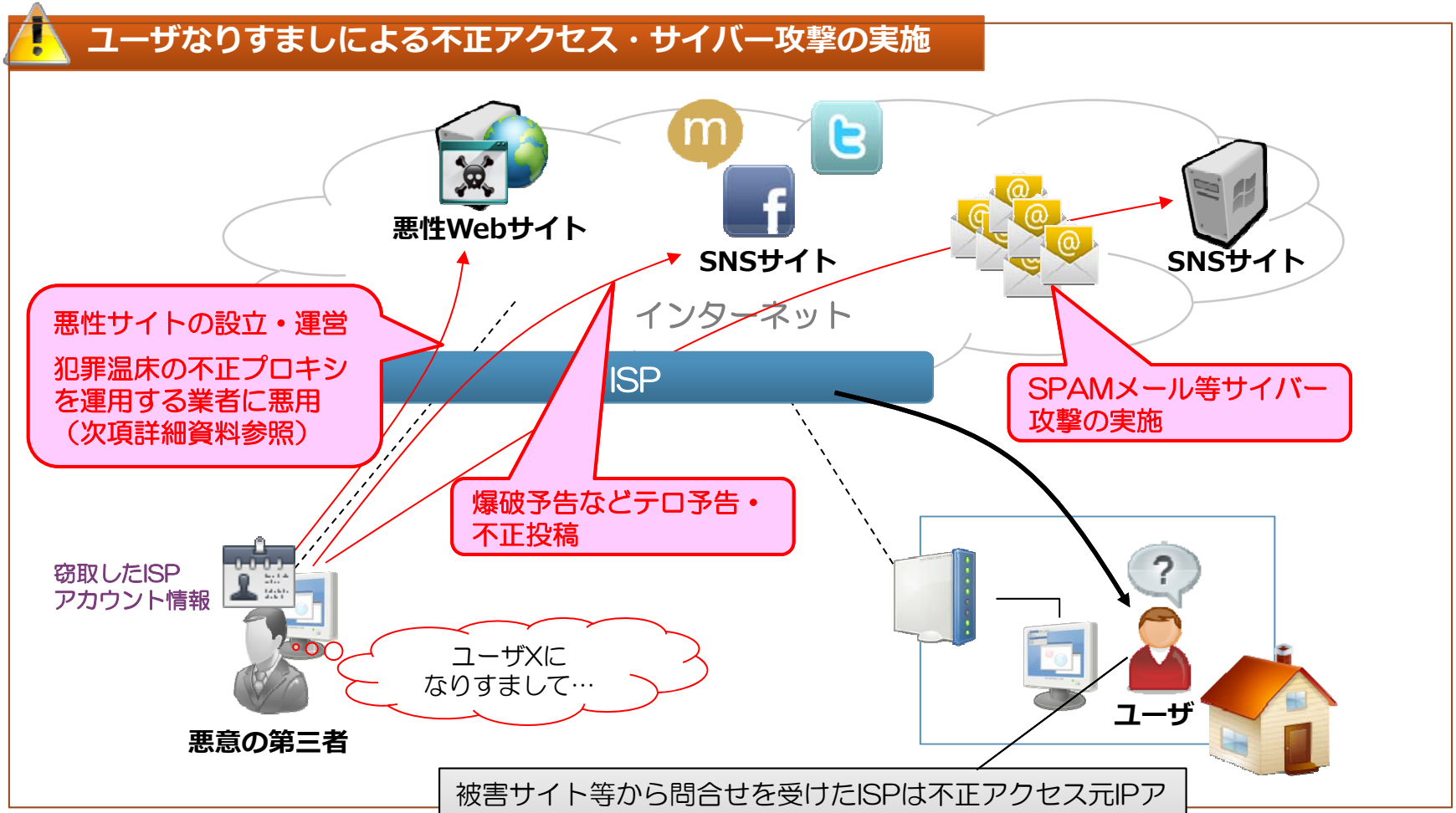


意図せずネット接続がNGとなり、ユーザはISPへ問合せを行う。
※ただし、既に確立済みPPPoEセッションが不正変更後もそのまま残っているケースもあり、不正変更に気づかないユーザも多い。

ユーザ問合せによって、アカウント不正窃取事象が発覚した。

Copyright©2004-2015 Telecom-ISAC Japan. All Rights Reserved.

③成りすましによる犯罪等の不正行為の温床



Copyright©2004-2015 Telecom-ISAC Japan. All Rights Reserved.

IoT時代のリスク対策

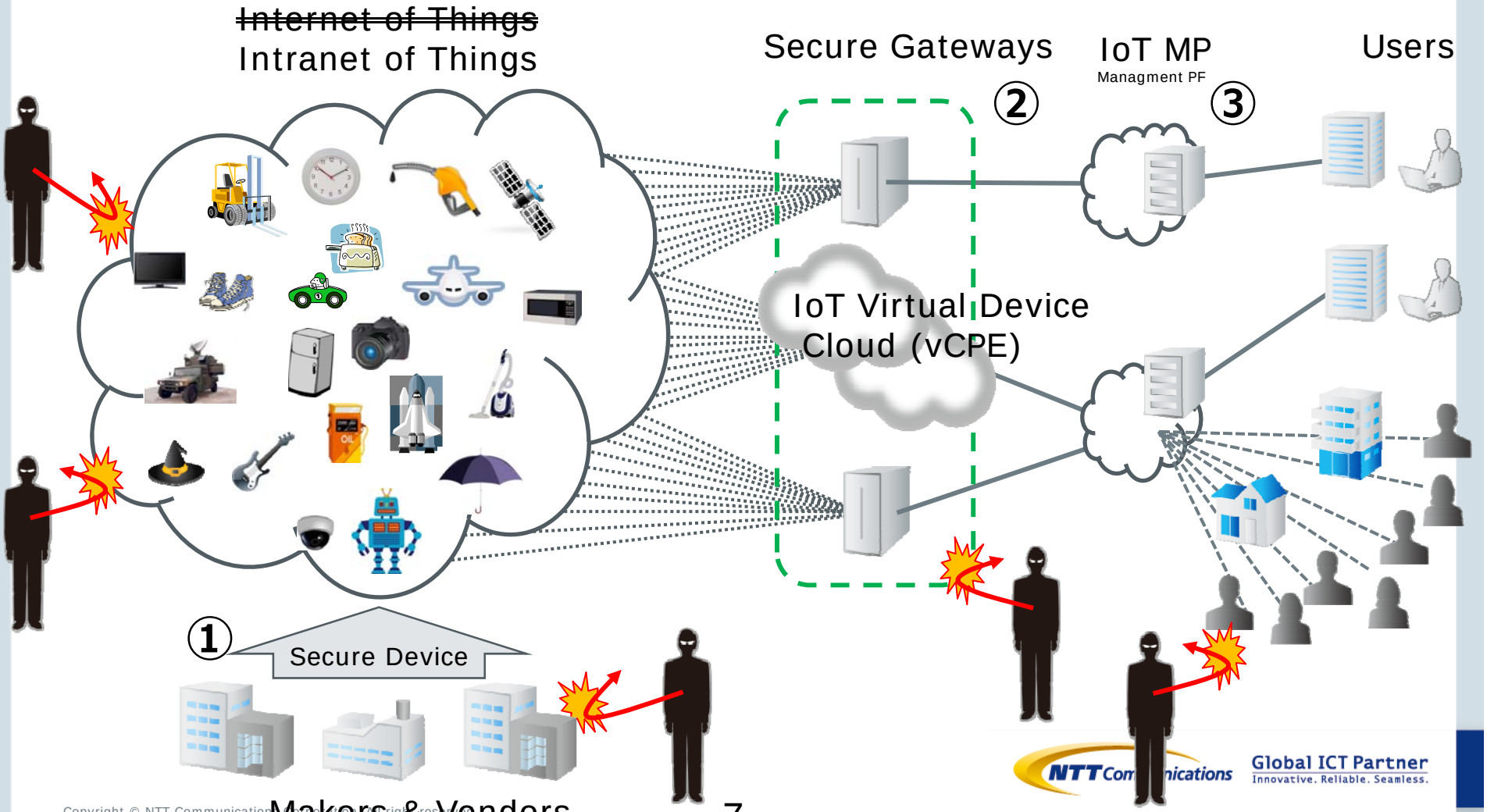
- IoTのセキュリティ対策は、ネットワークに接続された管理者不在の「モノ」との戦いになるかもしれない
  - ・所有者への注意喚起と脆弱性対策
  - ・NWからの切り離しによる安全確保
- 新しい「モノ」が限りなくネットに接続され、中には10年以上使い続けられる「モノ」も大量に発生すると想定
  - ・セキュリティ バイ デザイン
- 人が常時操作している「パソコン・スマホ」でも、攻撃の踏み台になるため、人の関与が少ない「モノ」は更に注意が必要
  - ・現在でも、ブロードバンドルータなど、人が常時操作しない「モノ」が攻撃の踏み台になると対策が困難
- 2020年には250億の「モノ」が繋がる。世界中で最もセキュアで利便性の高いIoT社会の実現に向け取組んではどうか？

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

Copyright © NTT Communications Corporation. All right reserved.

Secure IoT Framework 1/2

- 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。

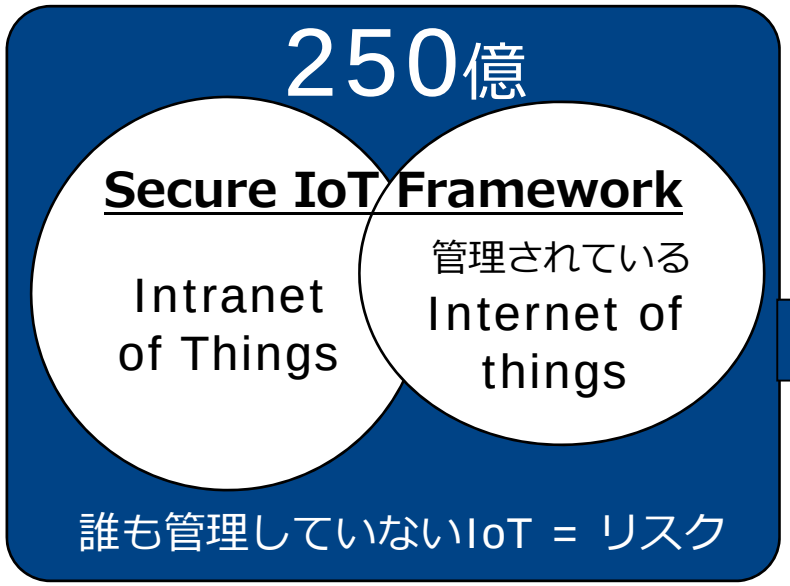


Copyright © NTT Communications Corporation All rights reserved.

Secure IoT Framework 2/2

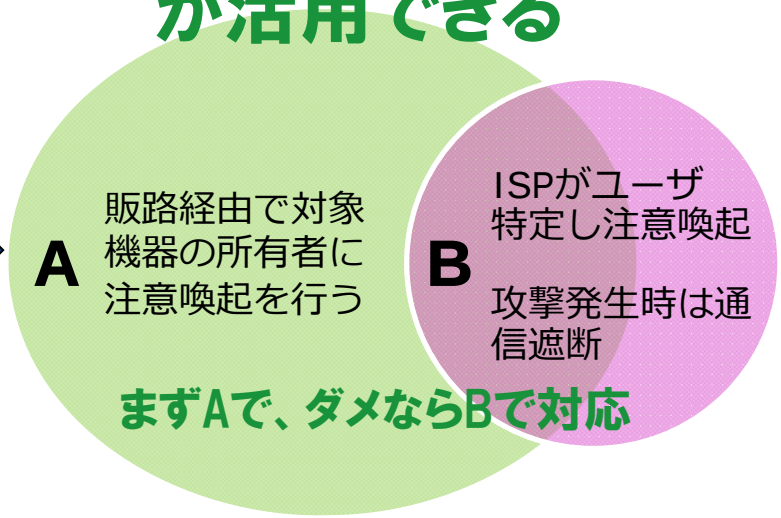
●脆弱な「モノ」の持ち主を探して対策を呼びかけるコストを全体的にどう下げるかを、最初から考えておきたい

全てのIoTデバイス



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

CCCやACTIVEのノウハウが活用できる



悪用されるIoTの対策は、
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

Copyright © NTT Communications Corporation. All right reserved.

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→民間ビジネス（安くて便利なIoTサービス）
- 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
  →官民連携した取り組み（費用負担の枠組み）
- 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
  →国としての安全弁の考え方
- 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

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

Copyright © NTT Communications Corporation. All right reserved.

ご清聴ありがとうございました

Copyright © NTT Communications Corporation. All right reserved.

10