2020に向けISPが果たすべき役割り
～未来に向けて「通信の秘密」との関わり方～

NTTコミュニケーションズ株式会社 経営企画部
セキュリティ・エバンジェリスト　小山　覚
2014年11月21日

SEAMLESS CLOUD
FOR THE WORLD

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

自己紹介

小 山　覚 （こやま さとる）

昭和40年生まれ、三重県出身

1988年　日本電信電話株式会社に入社、大阪府や兵庫県で電柱やケーブルの工事・保守業務を経験

1997年　OCNの立ち上げに参加しセキュリティサービス開発に従事

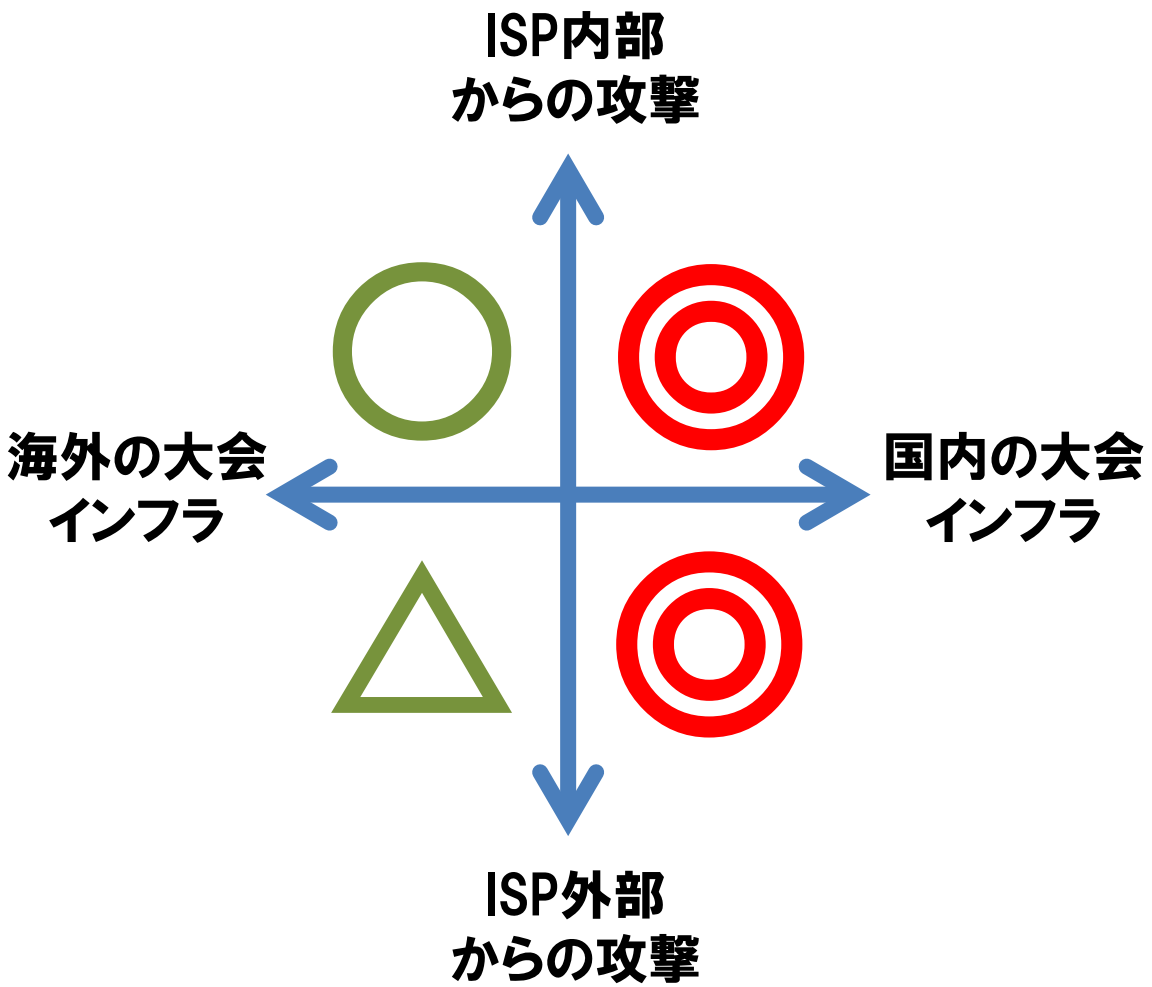
2001年　CodeRedワームの脅威に直面しマルウェア対策を決意

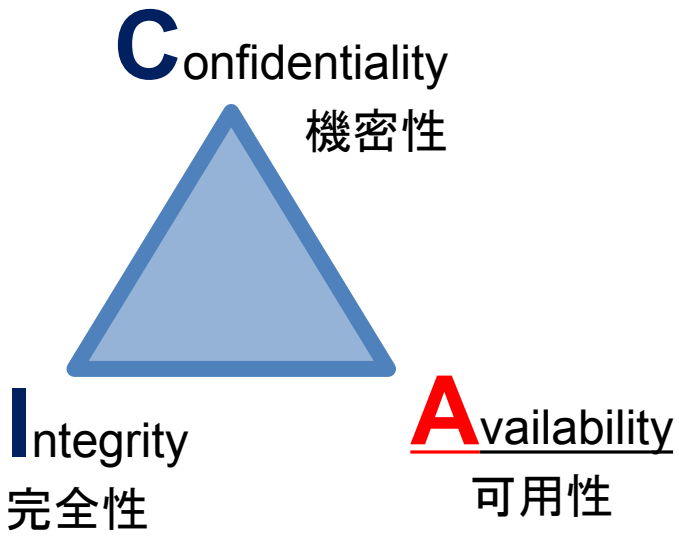
2002年　本来業務の傍らTelecom-ISAC Japanなど、各団体の活動に参加

2006年　セキュリティ対策の国家プロジェクト「サイバークリーンセンタ」の運営委員を5年間務める。

2013年　7月から現職、総務省研究会の構成員として、サイバー攻撃対策と「通信の秘密の侵害」との関係整理に取り組む。

東京オリンピック・パラリンピックで何を守るのか？





NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

東京オリンピック・パラリンピックで何を守るのか？

サービスプロバイダは、自分を守ることを真剣に考えるべき

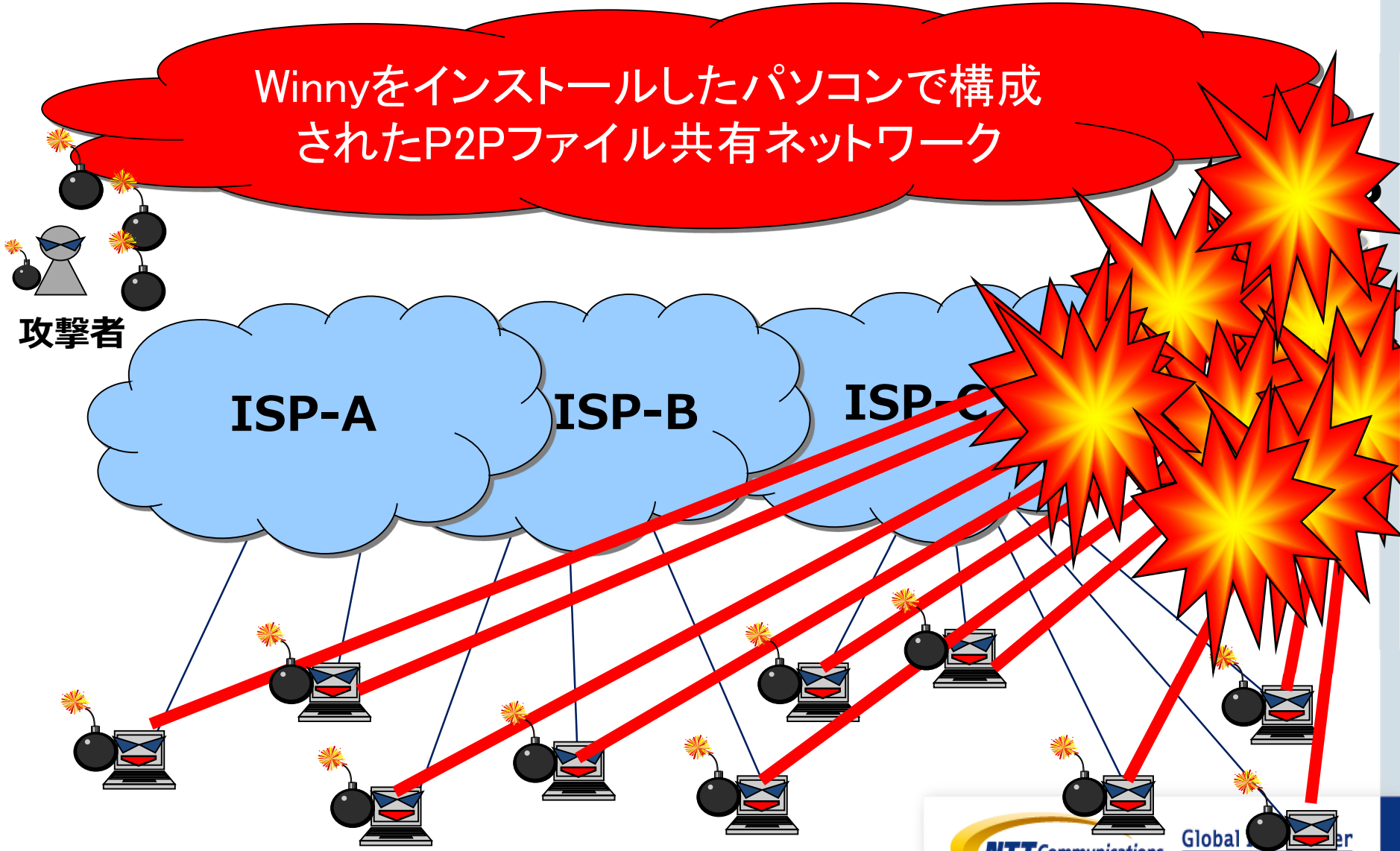
2013年：300Gbpsが史上最大規模

2014年：日本のあるISPで100Gbps超

2020年：想像もつかない、桁違いのトラヒックの暴力と戦いたくない！

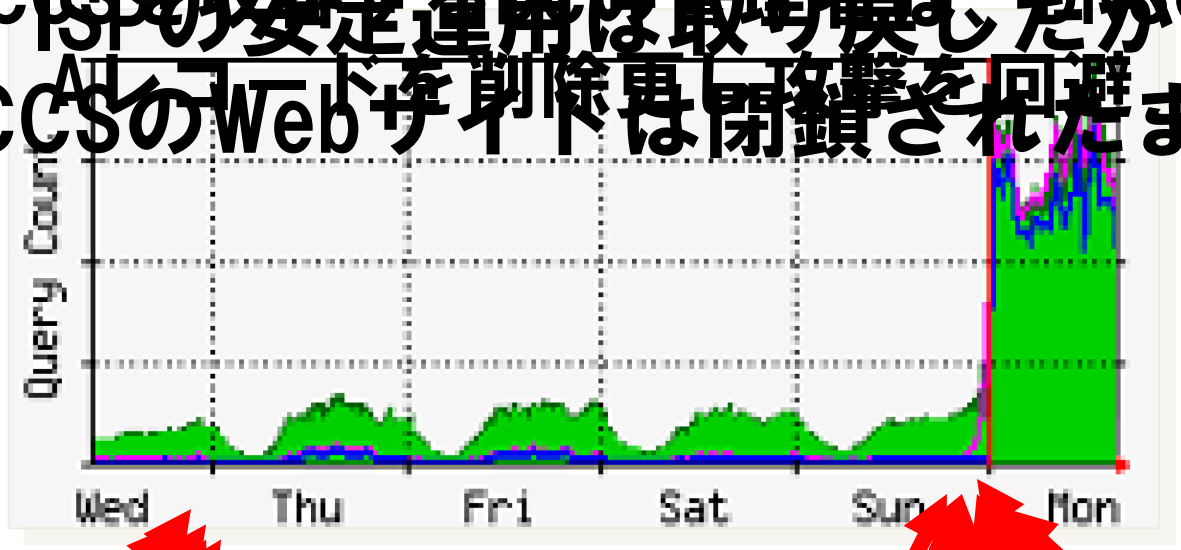
NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

2004年Winnyが媒介したAntinnyのDDoS攻撃



攻撃回避の行動がISPに悪影響

ACCSを収容する多数のPCの管理者は、DNSの
ISPの安定運用は取り戻したが
ACCSのWebサイトは閉鎖されたまま



攻撃者

ACCS

Antinny DDoS攻撃事案の教訓

管理者不在状態の
ネットワークやシステムの恐怖

→はたしてP2Pファイル共有
ネットワークだけか？

現在も2004年比較で5％の
端末が攻撃を継続している

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

通信の秘密侵害罪

（秘密の保護）

第4条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

２　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

第179条　電気通信事業者の取扱中に係る通信の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。

２　電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。

大量通信への対処と通信の秘密ガイドライン

サイバー攻撃や迷惑メールの大量送信などに対しインターネットサービスを提供する電気通信事業者が行なう対応が、主に電気通信事業法4条で定められた通信の秘密の保護について違法性がないかどうかを判断する参考とするため、本ガイドラインを制定

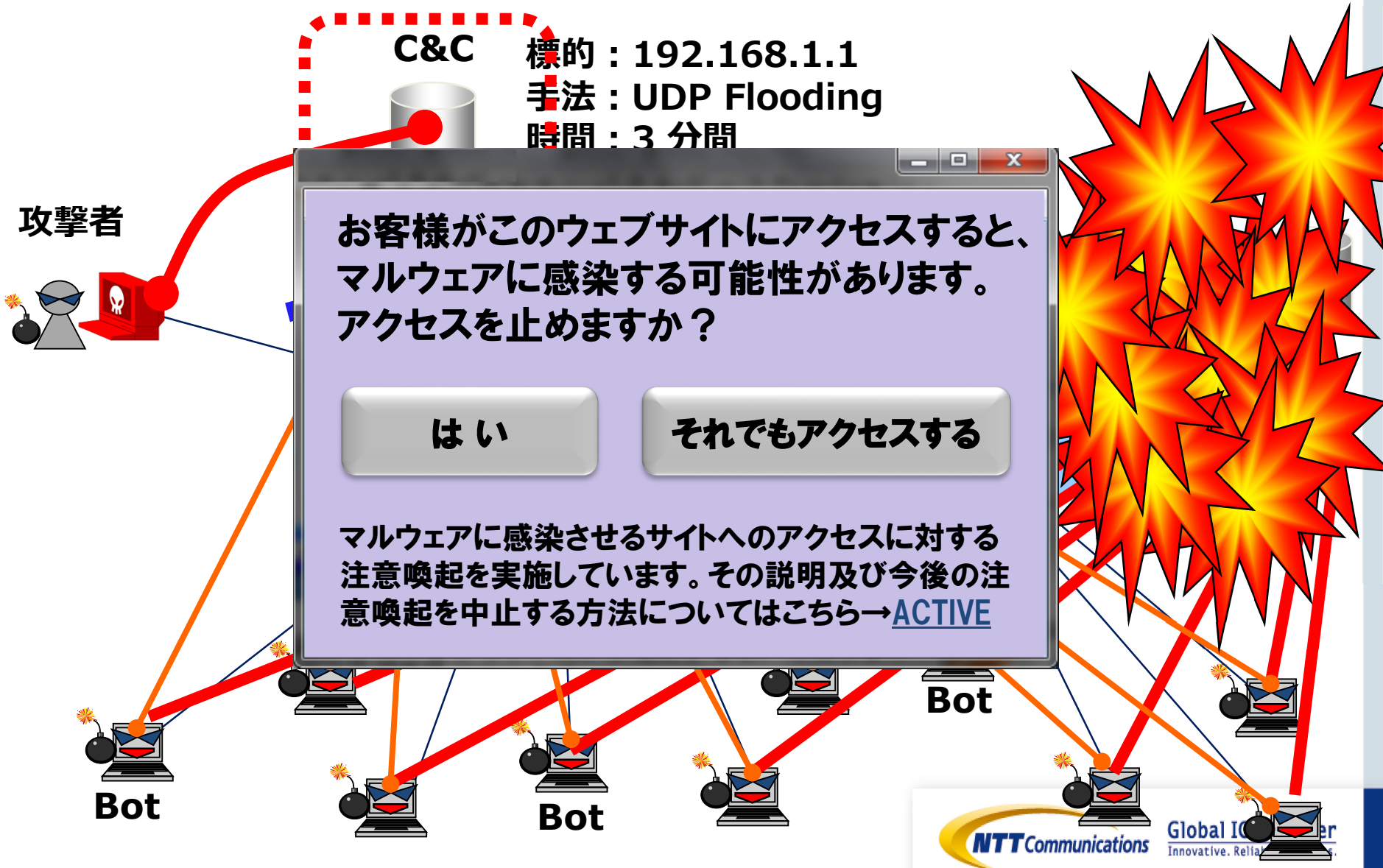
第 1 版 2007 年（H19） 5 月 新規作成（非公開）

第 2 版 2011 年（H23） 3 月 章、条番号の付加、3,4 条追加、2 章内容見直し等

第 3 版 2014 年（H26） 7 月 総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ結果」等を反映

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

ボットネットを利用したDDoS攻撃の例

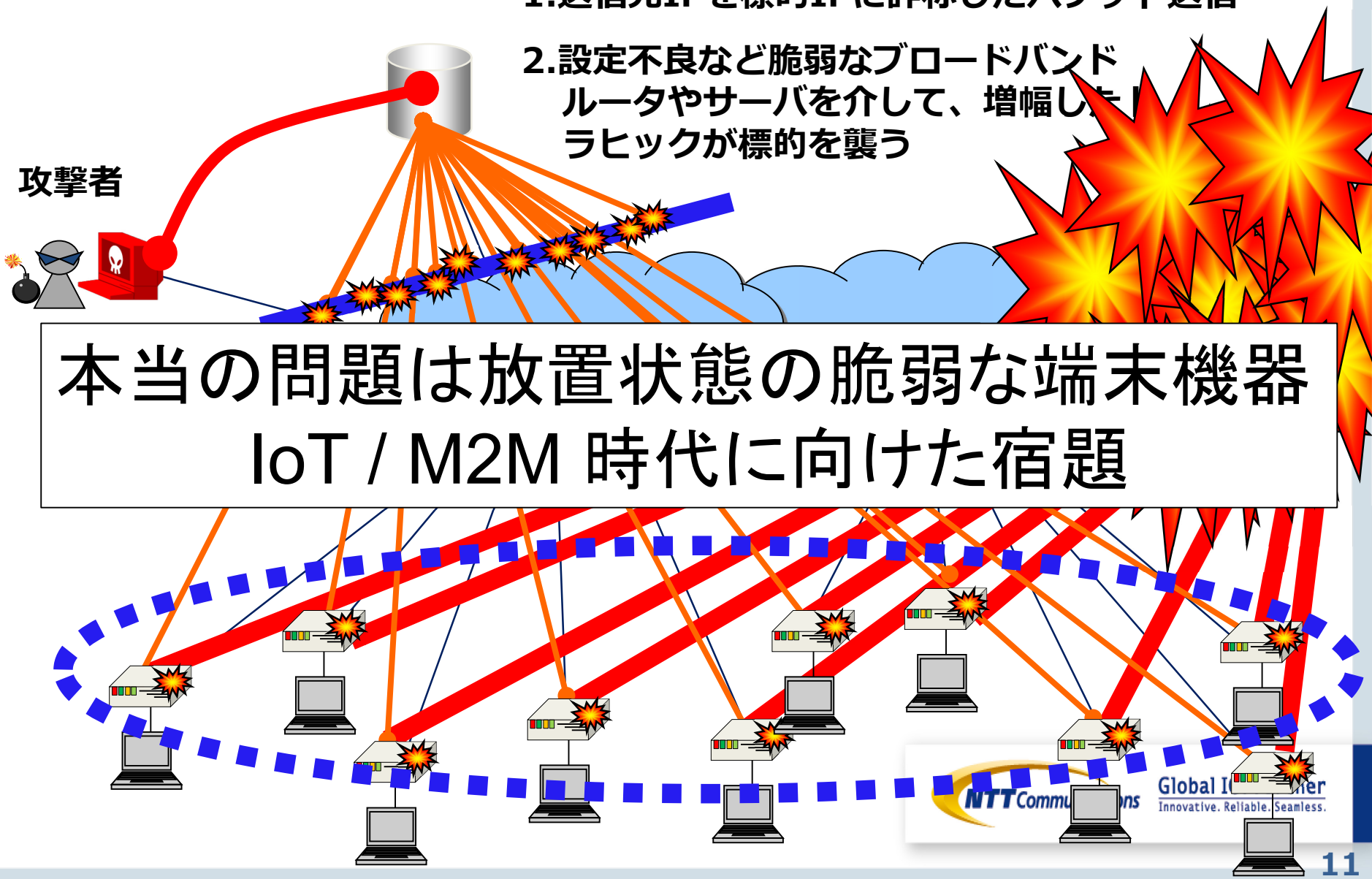


リフレクション型のDDoS攻撃の例

1.送信元IPを標的IPに詐称したパケット送信

2.設定不良など脆弱なブロードバンド
ルータやサーバを介して、増幅したトラヒックが標的を襲う

攻撃者



本当の問題は放置状態の脆弱な端末機器
IoT / M2M 時代に向けた宿題

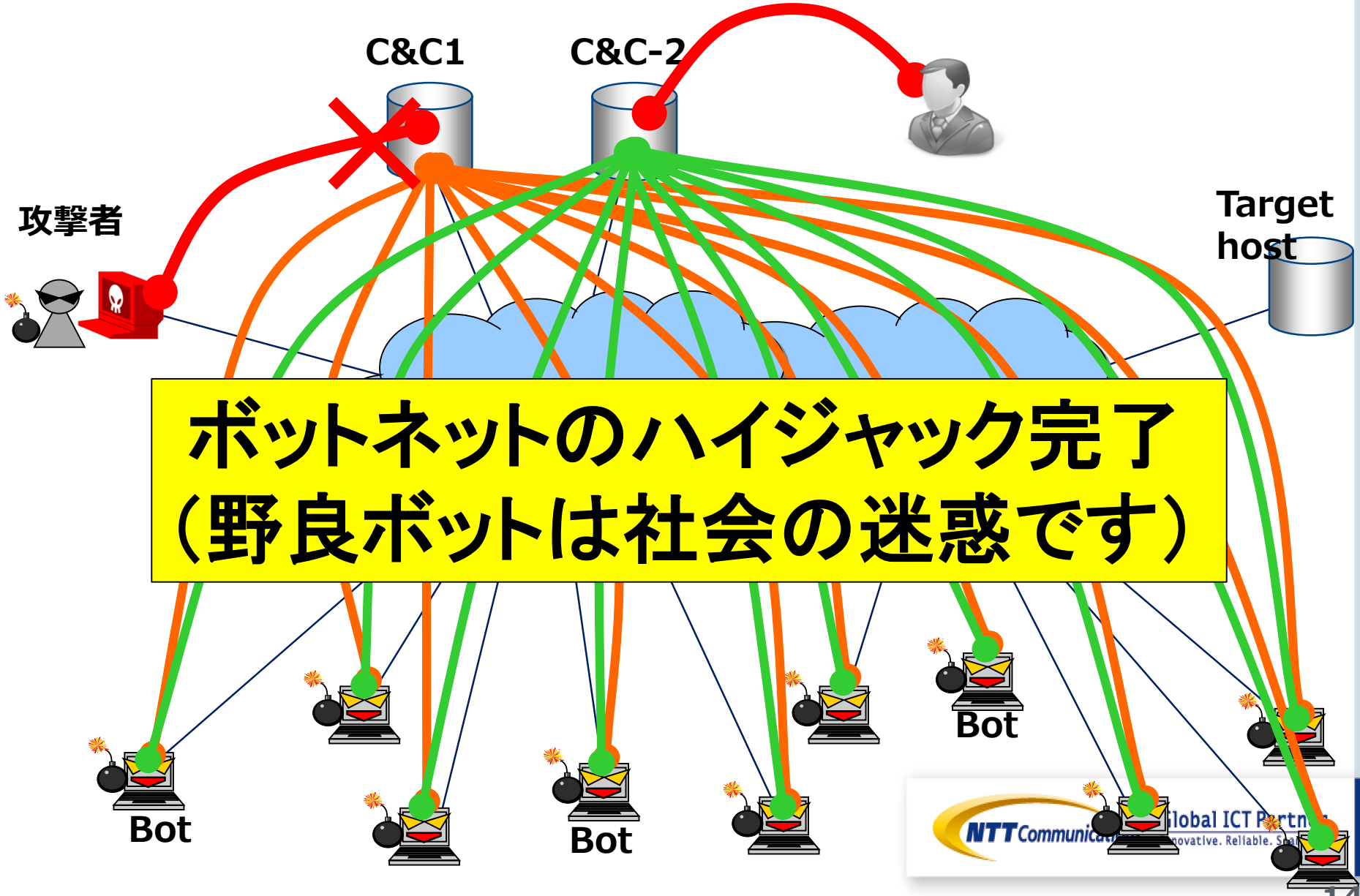
通信の秘密と上手に付き合いつつ、2020に向け安定的なサービス提供を実現していくために

IoT / M2M

との付き合い方が大事ですね

参考資料

管理者不在のネットワークの恐怖



14

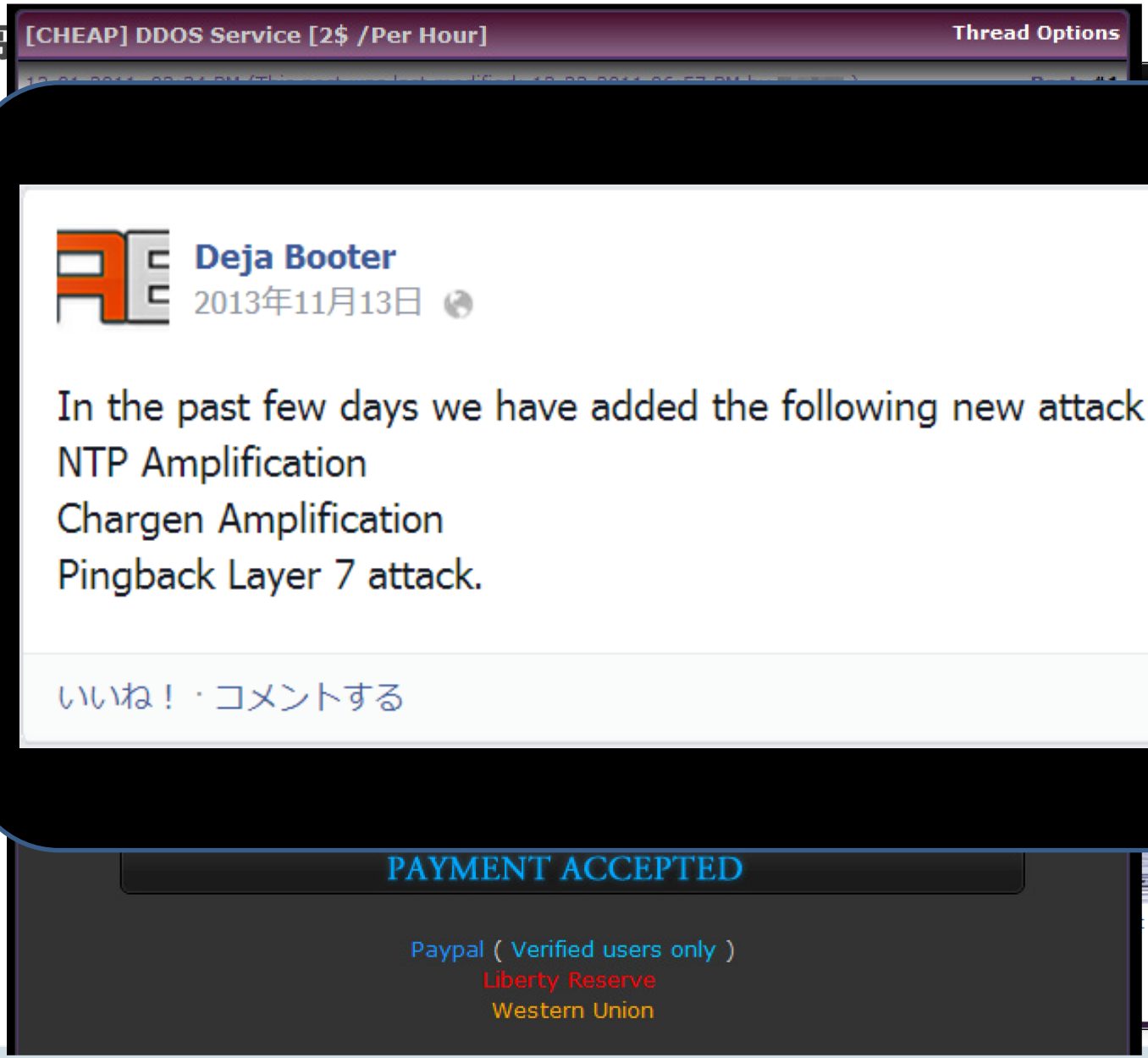
重要ポイント

管理者不在のIoTやM2Mネットワークを作らないこと

管理者不在のIoTやM2Mは、
野良ボット以上に厄介な存在かもしれません

攻撃代行？業者の存在

高



Deja Booter
2013年11月13日

In the past few days we have added the following new attack methods:
NTP Amplification
Chargen Amplification
Pingback Layer 7 attack.

いいね！ · コメントする

総務省研究会　一次取りまとめ結果のダイジェスト

http://www.soumu.go.jp/main_content/000283608.pdf

検討課題	通信の秘密との関係等の考え方
マルウェア配布サイトへのアクセスに対する注意喚起	利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる（**オプトアウトできる**）こと等を条件に、契約約款に基づく**事前の包括同意であっても有効な同意と整理**
マルウェア感染駆除の拡大	C&Cサーバに蓄積されている、同サーバとマルウェアに感染したPC等の端末に係る通信履歴からマルウェアの感染者を特定し、注意喚起を実施することは、**当該端末が正常かつ安全に機能することに対する現在の危難を避けるための緊急避難として許容**される。
新たなDDoS攻撃であるDNSAmp攻撃の防止	利用者が設置しているブロードバンドルータ等のゲートウェイに対するインターネット側からの名前解決要求に係る通信を遮断することは、**電気通信役務の安定的提供を図るための正当業務行為として許容**される。
SMTP認証の情報（ID及びパスワード）を悪用したスパムメールへの対処	他人のID・パスワードを悪用して送信されるスパムメールへの対処として、 当該IDの一時停止や、正規の利用者への注意喚起等を実施することは、**電気通信役務の安定的提供を図るための正当業務行為として許容**される。