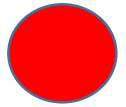
沖縄ICTフォーラム2018in名護

事業法改正とISPの取り組みについて

2018/07/06

株式会社インターネットイニシアティブ(IIJ)
ICT-ISAC Japan (IIJ)
齋藤 衛


は非公開資料

本日のAgenda

- はじめに
- これまでの取り組み
- 現状
- 事業法改正によってできるようになること
- 事業法改正を受けてISPがやらなければならないこと

はじめに
ISPが通信の秘密を侵害しようと考えてしまうとき

- 自らの事業を追行するため
- 自らの事業を保護するため
- 人命保護レベルの重大事に対する社会的要請
- 通信事業者しか知りえない情報があるとき、対応できない事象があるとき

これまでの取り組み
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

- （2005年 通信事業者有志による討ち入り事件）
- 2007年より「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」
  通信関連4団体+1団体による民間自主ガイドライン
  - 正当防衛および緊急避難での整理
- 2013年11月「電気通信事業におけるサイバー攻撃の適正な対処の在り方に関する研究会」
  - 包括同意の有効性
  - 正当業務行為での整理

これまでの取り組み
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(2)

- 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
  - ・ACTIVE 普及啓発(マルウェア配布サイトへのアクセス防止)
  - ・C&Cサーバで入手した情報を元にしたマルウェア感染駆除の拡大
  - ・新たなDDoS攻撃であるDNSAmp攻撃の防止
  - ・SMTP認証の情報を悪用した迷惑メールへの対処
  - ・攻撃の未然の防止と被害拡大の防止

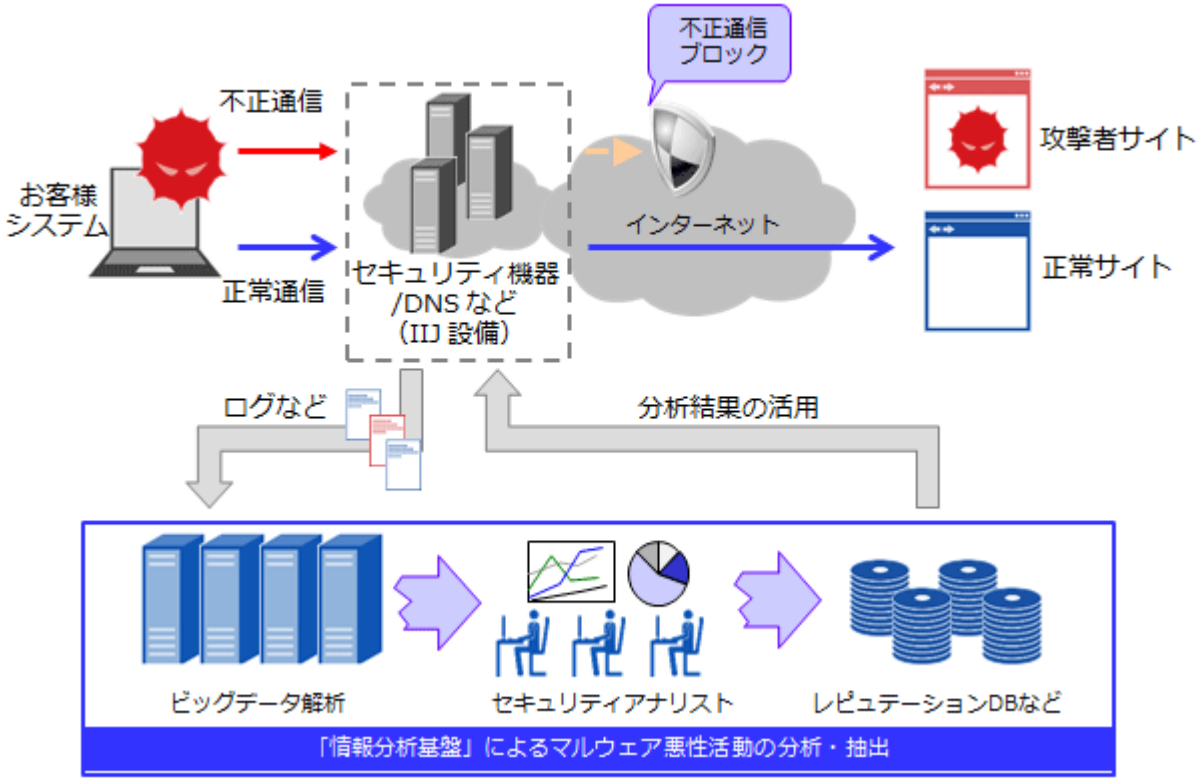
これまでの取り組み
電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会(2)

- 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二次とりまとめ」
  - ・C&Cサーバ等との通信の遮断
  - ・他人のID・パスワードを悪用したインターネットの不正利用への対処
  - ・脆弱性を有するブロードバンドルータの利用者への注意喚起
  - ・DNSの機能を悪用したDDoS攻撃に用いられる名前解決要求に係る通信の遮断

現状
C&Cサーバ等への通信の遮断

- サーバのFQDNの名前解決の阻害
- 大手ISPによる先行事例

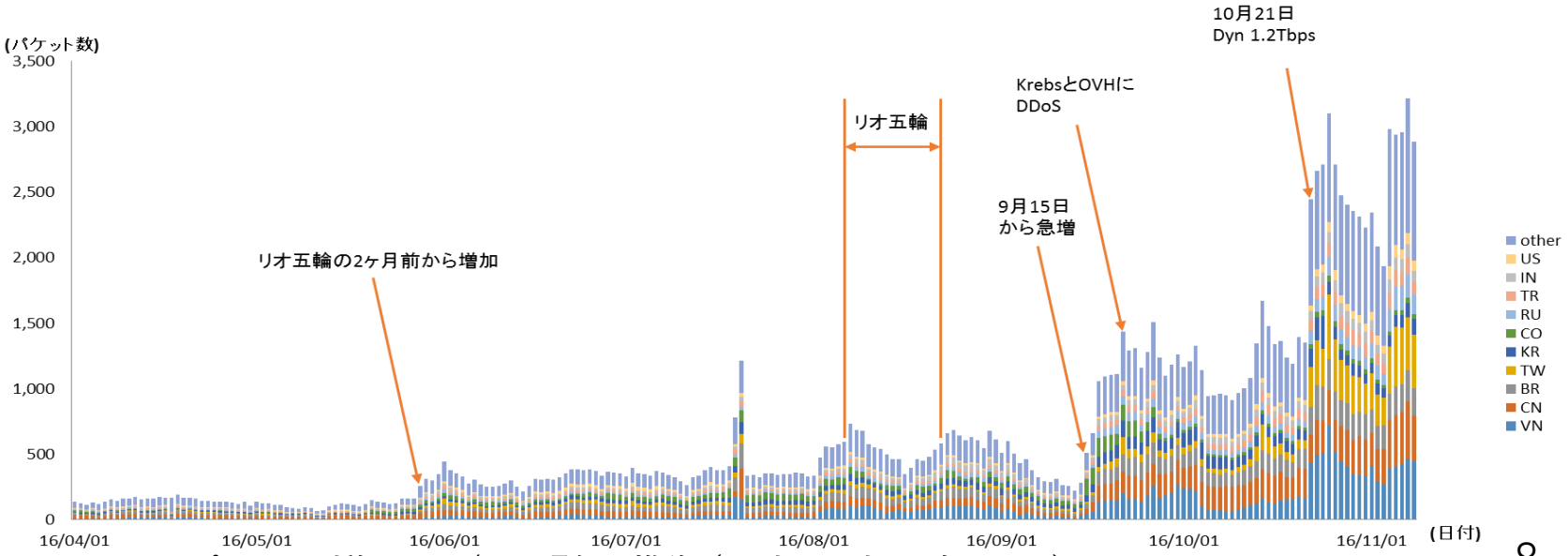
- IIJとしては
  - 2016年12月15日から
  - 分析、遮断について



https://www.iij.ad.jp/sec-statement/

現状
脆弱なIoTデバイスとIoTボット

- ともかく数が多い
- 1Tbps以上のDDoS攻撃を引き起こした
- IoTな場所家庭、移動体、公共の場所
- ウイルス対策が存在しない
- 運用管理されない



ハニーポットに到着した23/TCP通信の推移（日別・国別・一台あたり）

事業法改正によってできるようになること

- 電気通信事業者とサイバー攻撃対策
  - （技術的基準を提出すれば）通信の調査や分析、遮断ができる。
  - サイバー攻撃に関する情報共有（提供、受領）ができるようになる。

- 脆弱なIoT装置の対策
  - NiCTさんから脆弱なIoT端末に関する情報（IPアドレスなど）の提供を受け、利用者に注意喚起できる。
  - IoTのサポート体制ができる。

事業法改正を受けてISPがやらなければならないこと

- 電気通信事業者とサイバー攻撃対策
  - サイバー攻撃対策の同意
  - 認定送信型対電気通信設備サイバー攻撃対処協会に参加とは
  - 特定会員になるには（技術的条件とは）
  - 情報の共有だけをしてどうする
- 脆弱なIoT装置の対策
  - IoTのサポートってどうやる？

事業法改正を受けてISPがやらなければならないこと(2)

- サイバー攻撃対策の同意のありかた
  - 包括同意か個別同意か
  - 同意の得方
  - 同意対象範囲の考え方
  - （攻撃している輩の検出対処）

事業法改正を受けてISPがやらなければならないこと(3)

- 認定送信型対電気通信設備サイバー攻撃対処協会に参加とは
  - ある団体が認定を受けたら
  - 申込書
  - 会費を払う
- 特定会員になるには（技術的条件とは）
  - アクセス制御、認証情報の管理、ファーウェアの管理、記録の管理などに問題のある (IoT)端末は接続してはいけないようなことを明文化すればよいのではないか。
  - 例文の提示、ガイドライン化？
  - 手続きの明確化

事業法改正を受けてISPがやらなければならないこと(4)

- 情報の共有だけをしてどうする
- 現状、DDoS対策、マルウェア対策、IoT機器対策については、事業者間連携はほぼ行われていない.
  - 特定事案に関する協調 (脆弱性を有するホームルータへの対策)
  - マルウェア対策におけるレピュテーションの受け入れ（ISPがレピュテーションを作っているわけではない）
- ICT-ISAC Japan　DoS即応WGの実績
  - 特定事案について観測情報の共有
  - 同時多発的DDoS攻撃の全容の構築
  - 攻撃規模の相場感や攻撃手法、対策手法などの共有
  - リフレクション攻撃やIoTボットの登場に際しては、他のWGや研究機関と協力して調査

事業法改正を受けてISPがやらなければならないこと(5)

- 情報の共有をしてどうする(2)
- DDoS攻撃について
  - 事業法上の通信の秘密に抵触するような内容を共有しないと伝わらないことがある（誰がいつどのような手法でどの程度攻撃された）.
  - 技術的な詳細を共有することで、顧客名そのもの、顧客の利用の仕方、顧客の構成の規模などが推察される可能性がある.
  - また、他社の顧客を保護しようというモチベーションは低い.

  - 一方で、サミット関連サイトや、オリンピック関連サイト、.JPのDNSサーバなど、誰が見ても重要なサイトの保護などでは、協調対処の議論は活発にできている.
    - 重要のサイトの定義があって
    - 管理主体からそれぞれのサイトに対する包括的な対処依頼があって
    - そのサイトに対する通信を分析、判断、遮断することができる
    - 遮断の方法に関する調整は別途必要(対応品質のコミット)

事業法改正を受けてISPがやらなければならないこと(6)

- IoTのサポートってどうやる？
  - 「サポート体制」は認定団体で実現することになる
  - 多数の製品、大量の利用、太陽な利用状況
  - 「製品」なのか「部材」なのか
  - 「とりあえずアンチウイルス」ができない
  - 利用者の認識も改めなければならない

まとめ

- はじめに
- これまでの取り組み
- 現状
- 事業法改正によってできるようになること
- 事業法改正を受けてISPがやらなければならないこと