資料１－３－８

# 円滑なインターネット利用環境の確保に関する検討会（第１回）
## ＜木村オブザーバー　提出資料＞

○　協議会では、民間の自主的な指針として「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」を定めている。

- ガイドラインについては、参考資料のとおり

○　新しい攻撃の発生等に対する指針を示すため、総務省における研究会の取り纏め結果なども参照しながら改訂してきた。

○　IoT 機器を踏み台にした攻撃が増加していることなどもあり、今後も継続的な改訂が必要であると認識。

- 既存の方法では対応困難な攻撃等への対策の追加
- 他の事業者等と連携した効率的な対策の推進　　など

○　今回の検討会で議論される課題なども踏まえながら、改訂を進めていきたい。

木村オブザーバー
参考資料

# 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインの概要

2017年 10 月 26 日

インターネットの安定的な運用に関する協議会　主査
日本インターネットプロバイダー協会　会長補佐　木村　孝

## 本ガイドラインについて

- 下記５団体が構成する「インターネットの安定的な運用に関する協議会」において作成 【https://www.jaipa.or.jp/other/intuse/】

一般社団法人日本インターネットプロバイダー協会（JAIPA）
一般社団法人電気通信事業者協会（TCA）
一般社団法人テレコムサービス協会
一般社団法人日本ケーブルテレビ連盟
一般社団法人ICT-ISAC（旧：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）

- 事例毎にQ&A形式で対策と法的考え方を整理したもの
  2005年に大規模なDoS攻撃が発生した際に、ISPが施した対策と法的整理を明文化して今後に備えるため作成
- ガイドラインを踏まえて新たに開始されたサービスもいくつか存在
- ガイドラインを10年運用してきたが、これに基づく対応に関して法的争いが生じた事案は聞いていない

# ガイドライン策定の動機

- 法律解釈についての指針が存在しておらず、対処の実施が運用担当者のリスクとなっている
  - ✓ 最終的な法的判断は裁判所が示すものだが、対処のために判断を待つ時間はない
- 運用担当者においては、通信の秘密の保護に抵触するおそれがある場合に積極的な対応を取り難いというジレンマがある
- 各ISPにより考え方が異なり、対応がバラバラである

通信の秘密の侵害にあたるかどうかについては個別の検討が必要だが、法律の解釈について一定の指針を示すことは可能
ある程度類型化できるものについては指針を設け、できる限り分かりやすい形でISP業界で共有していくために策定



# ガイドラインの位置付け

- 業界の自主基準としての位置づけ
  - 法令上の位置づけがあるガイドラインではなく民間における法令の解釈指針
  - 事業者に対処を強制したり、活動を規制するものではない
  - 総務省はオブザーバとして協議会に参加
- 同様な事例が生じた際に、ISPがその都度解釈に関して総務省に問合せる手間を省略するためのもの
  - ガイドラインに沿って対応すれば免責されるなどの効果はないが、裁判所が法的判断の参考として参照することを期待
- インターネット上で新たに発生する問題に対応するため、定期的な見直しを実施

# ガイドラインの変遷

- ２００７　初版
  「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 」として作成。関係者限りで限定公開
- ２０１１　第２版
  一般にも公開
- ２０１４　第３版
  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の第一次とりまとめ（2014年4月4日）を受けて改正
- ２０１５　第４版
  同研究会の第二次とりまとめ（2015年9月9日公表）を受けて改正

第4版において、ガイドラインの名称が「大量通信等への対処」から「サイバー攻撃等への対処」に変更。



# ガイドラインの構成

第1章　総則
　第1条　目的
　第2条　総論
　　1. 通信の秘密
　　2. 留意事項
　第3条 定義
　　1. サイバー攻撃等
　　2. 電気通信役務の不正享受
　　3. 攻撃通信
　　4. 通信
　第4条　見直し

第2章　各論
　第5条　サイバー攻撃等について
　　1. 攻撃通信への対処
　　2. 迷惑メール等
　　3. その他の情報共有・情報把握について
　第6条　電気通信役務の不正享受について

①攻撃や障害が発生している際の対処法
②攻撃や障害を予防する為の措置
③必要な情報の共有

**等につき、具体的な事例とともに指針となる考え方を整理**

# ガイドラインの構成（第5条の詳細）

第5条　サイバー攻撃等について
- (1)　サイバー攻撃等に係る通信の遮断
  - ア　被害者から申告があった場合
  - イ　事業者設備に支障が生じる場合
  - ウ　**送信元設備の所有者の意思と関係なく送信される大量通信等の場合**
- (2)　**送信元詐称通信の遮断**
- (3)　壊れたパケット等の破棄
- (4)　マルウェア等トラヒックの増大の原因となる通信の遮断
- (5)　受信側の設備等に意図しない影響を及ぼす通信等への対処
- (6)　**網内トラヒックの現状把握**
- (7)　サイバー攻撃等への共同対処

2　迷惑メール等
- (1)　送信元詐称メールの受信拒否
- (2)　**Black Listとの突合に基づくユーザへの注意喚起**
- (3)　**迷惑メールフィルタリングサービスにおけるフィルタ定義の共有**
- (4)　SMTP認証の情報を悪用した迷惑メールへの対処

3　その他の情報共有・情報把握について
- (1)　踏み台端末や攻撃中継機器への対処
- (2)　**レピュテーションDBの活用**

事例①
【事業者設備等へのサイバー攻撃に対する実施可能な措置】

事例②
【マルウェア感染端末とC&Cサーバとの通信の遮断】

事例③
【サイバー攻撃に対する事業者間の情報共有】

次頁以降で代表的な事例を説明

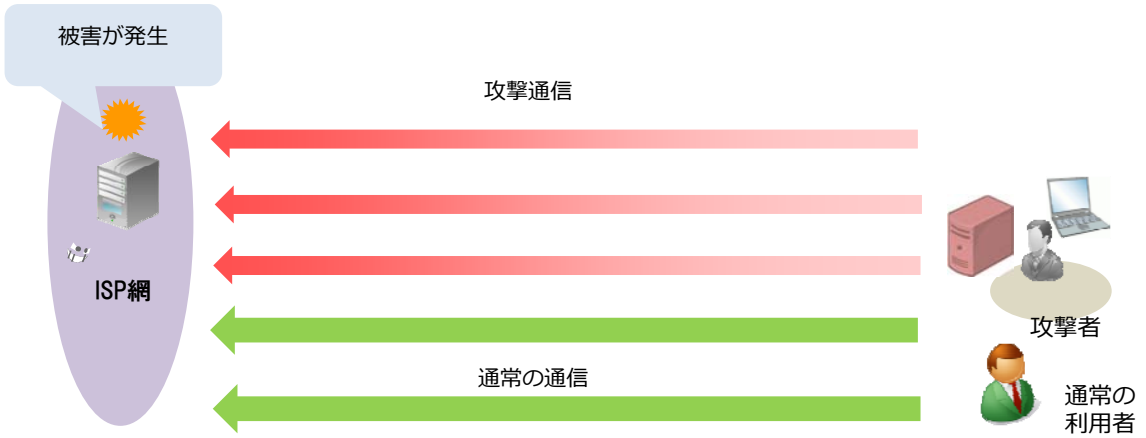


# 事例①　事業者設備等へのサイバー攻撃に対する実施可能な措置

## 送信元設備の所有者の意思と関係なく送信される大量通信等の場合

現行ガイドラインにおける整理

■サイバー攻撃等を行っている契約者を特定した上、これを止めるよう連絡をすることなどによって、事業者設備又は受信者設備等に生じる侵害を防止するため、必要かつ相当な範囲で契約者の接続ログの解析を行い、当該契約者に要請を行うことは、通常は、正当防衛又は緊急避難として違法性が阻却される（P14（ク））

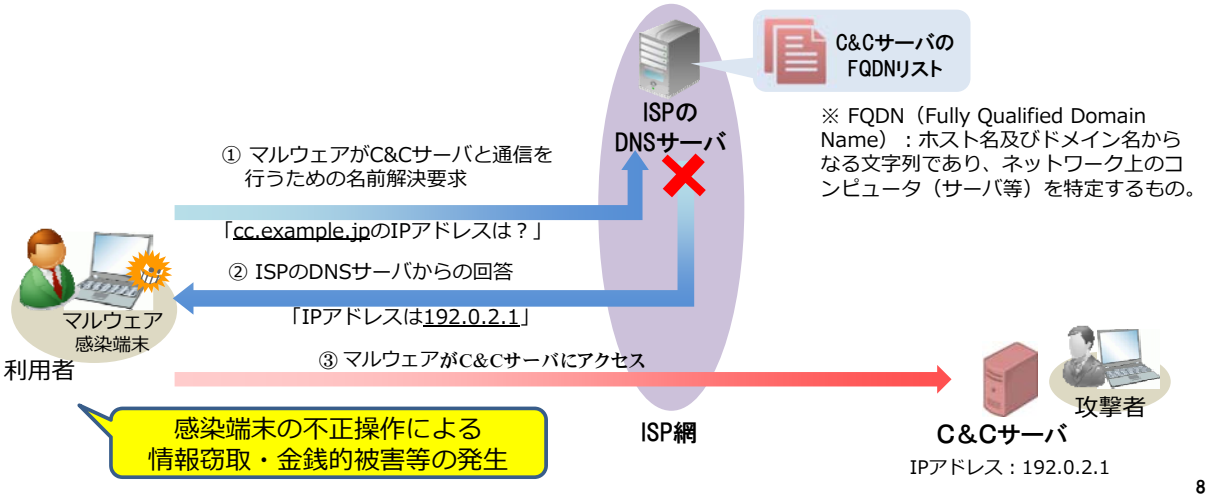


# 事例②　マルウェア感染端末とC&Cサーバの通信の遮断

## レピュテーションDBの活用

### 現行ガイドラインにおける整理

■　マルウェア感染者が情報窃取や金銭的被害等の深刻な被害を受けることを防ぐとともに、感染端末を踏み台にした新たな攻撃の発生を防ぐため、C&Cサーバ（Command and Controlサーバ）のFQDN（サブドメイン＋ドメイン）※が判明している場合において、ISPが自社DNSサーバを通過する利用者のFQDNを検知し、C&CサーバのFQDNの名前解決要求を遮断することについて、通信の秘密に属する情報（アクセス先のFQDN）の利用についての有効な同意として包括同意でも可能。（P26（フ））






# 事例③　サイバー攻撃に対する事業者間の情報共有

**送信元詐称通信の遮断**

**網内トラヒックの現状把握**

**Black Listとの突合に基づくユーザへの注意喚起**

**迷惑メールフィルタリングサービスにおけるフィルタ定義の共有**

### 現行ガイドラインにおける整理

■　攻撃を受けたISPにおいては、攻撃パケットについての情報を発信元ISPと共有（P15　ク）できる。また、ISP間において、正当に統計処理されたログ情報（P18　ソ）、通信の秘密を含まないブラックリスト（P20　ト）、迷惑メールのフィルタ定義（P21　ナ）の共有が可能とされている。