資料4

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資料

インターネット上の情報セキュリティ関連ガイドラインの紹介等について

「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」を中心に

2013年11月29日

一般社団法人日本インターネットプロバイダー協会（JAIPA）
行政法律部会　部会長 木村　孝

はじめに

- 電気通信関連の4団体とテレコムアイザックは、「インターネットの安定的な運用に関する協議会」（次頁参照）を構成し、サイバー攻撃等の大量通信等への対処と通信の秘密の関係について民間の自主的ガイドラインを策定しました。
- このガイドラインは「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」（以下、ガイドライン）の名前で、2007年に策定され、2011年に改訂されました。
- 本ガイドラインはJAIPAのホームページから入手することができます。
- http://www.jaipa.or.jp/other/mtcs/info_110325.html

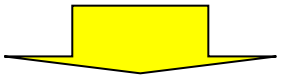
インターネットの安定的な運用に関する協議会

構成員

- 一般社団法人日本インターネットプロバイダー協会
- 一般社団法人電気通信事業者協会
- 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

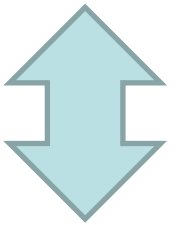
ガイドラインの趣旨

DoS攻撃、DDoS攻撃等のサイバー攻撃、マルウェアの感染拡大、迷惑メールの大量送信および壊れたパケット等（以下、大量通信等）は電気通信事業者の設備に支障を与え、電気通信役務の提供に影響を与える。



円滑な電気通信役務の提供の確保のためには、大量通信等に係る通信の遮断等が必要

通信の識別や遮断は、通信の秘密の侵害に該当するため、法的に考え方の整理が必要とされる。



電気通信事業法
（検閲の禁止）
第3条　電気通信事業者の取扱中に係る通信は、検閲してはならない。
（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。

ガイドラインの目的

- 本ガイドラインは、大量通信等のネットワークに対する攻撃に対して、通信の秘密の保護に最大限配慮しながら電気通信サービスの円滑な提供の確保に資することを目的としています。
- 電気通信事業者が大量通信等を識別しその**通信の遮断などの対処**を実施するにあたって、電気通信事業法等の関係法令に留意し適法に実施するための参考資料として、本ガイドラインを策定しました。

ガイドラインの規定内容

- 「大量通信等によって電気通信事業者の設備に支障が生じる場合」や「送信元を詐称した通信が送信された場合」等の事象に即して、大量通信等への対処を行った場合の通信の秘密の保護との関係について、考え方を示しています。
- 設備基準、管理基準、ポリシー策定ではなく、大量通信等が発生した場合の対応について、事例毎に整理しています。
- 例：

> 大量通信等のうち受信した設備に異常を来たす通信（以下「攻撃通信」という。）の受信者から当該攻撃に係る通信の遮断依頼を受けた場合、①遮断依頼が正当なものか否かの判断をするため、ネットワークの適正運営等のために通常時より取得しているトラヒックの統計データと依頼時点の統計データとを機械的に突合せ「異常な状況」であるか否かを判断するとともに、②異常な状況であった場合、当該攻撃にかかる通信がどのような特性を有するものであるかを分析し、③その分析結果に基づいて攻撃通信の特性に合致する通信のみを遮断してよいか。

ガイドライン策定の動機

- 法律解釈についての基準が存在しておらず、対処の実施が運用担当者のリスクとなっている
- 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後ろ向きな対応しかできな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
- 2005年に大規模なDoS攻撃が発生した際に、ISPが施した対策（総務省に個別相談実施済）を明文化して今後に備える

通信の秘密の侵害にあたるかどうかについては本来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であり、ある程度類型化できるものについては、できる限り分かりやすい形でISP業界で共有していくべき

ガイドラインの概要

- 事例毎にQ&A形式で考え方を整理したもの
- 業界の自主基準としての位置づけ（総務省はオブザーバとして協議会に参加）
- 同様な事例でISPがその都度総務省に解釈について問合せる手間を省く。
- 業界の自主ガイドラインとしての性質上、ガイドラインに沿った対応をすれば免責されるといった効果はない。
- 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、ガイドラインは定期的に見直し。
- 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。

参考

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 機械的検索と通信の秘密
3 大量通信等への対応に関する一般論
4 留意事項
　第3 条 定義
1　大量通信等
２　攻撃通信
３　通信
　第4条　通信の秘密とISPの対処に関する基本的な考え方
1 通信当事者の同意のある場合
2 ISP 自身が通信当事者である場合
3 法令行為、正当業務行為、正当防衛、緊急避難に相当する場合
　第5条　見直し

参考

構成（続）

第6条　大量通信等について
（1） 大量通信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
（6） 網内トラヒックの現状把握
（7） 大量通信等への共同対処
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
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:受信者からの遮断依頼

(イ)　受信者からの遮断依頼に応じて、受信者宛攻撃通信を遮断するために、当該通信の特性(送信元アドレス、受信元アドレス、ポート番号、パケットの送信頻度など)を把握の上、取扱中に係る通信について当該特性に合致するか否かを機械的に突合し、当該特性に合致する通信のみを遮断してよいか。

【考え方】

①　攻撃に係る通信の特性を把握した上、当該特性を有する通信のみを機械的に遮断することは、通信の秘密の侵害に当たりうるが、受信者又は受信回線の加入者から個別の同意を取得して行う場合には通信の秘密の侵害にはならない。

②　他方、受信者又は受信回線の加入者から個別の同意を得ず、全加入者を対象に前記のような遮断を一律に行うことは、不正な攻撃通信により全加入者の端末に生じる侵害を防止するために必要な範囲で相当な方法により行われる場合には、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と考えられる。

【①の事例】

・ 利用者から、Webサーバに対する攻撃通信を発生させている特定のIPアドレス空間から、利用者のWebサーバのIPアドレスに向かった、ポート80番の通信の遮断を依頼された。この依頼を受け、ISPでは網内の装置に当該通信の遮断の設定を行った。

【②の事例】

・ 特定のIPオプションが付与された通信が送信されることによりISPの通信設備に過負荷を与えるおそれがあったため、あるISPでは当該IPオプションが付与されたパケットの遮断を行った。

事例②:事業者設備に支障が生じた場合

（エ） 特定の受信者宛の大量通信等やウイルス・ワームなどに起因する大量通信等の発生によって、ルータやDNSサーバなどの通信設備に支障が生じ、他の通信に影響を及ぼした場合、当該支障を解決するためには、通信の間引き・遮断を行う必要があるが、遮断する通信の範囲を最小限に留める必要がある。そこで、通常時より取得しているトラヒック等のデータと、現時点のデータとを突合した上で、当該大量通信等の特性（送信元アドレス、受信元アドレス、ポート番号、パケットの送信頻度、クエリなど）を把握の上、当該特性に合致する通信のみを遮断してよいか。

【考え方】

発生している大量通信等の特性を把握した上、当該特性を有する通信のみを機械的に遮断する場合、その特性を把握することは、通信の秘密の侵害（知得）に当たりうる。また、把握した特性に基づき、当該特性に合致する通信を遮断することは通信の秘密の侵害（窃用）に当たりうる。

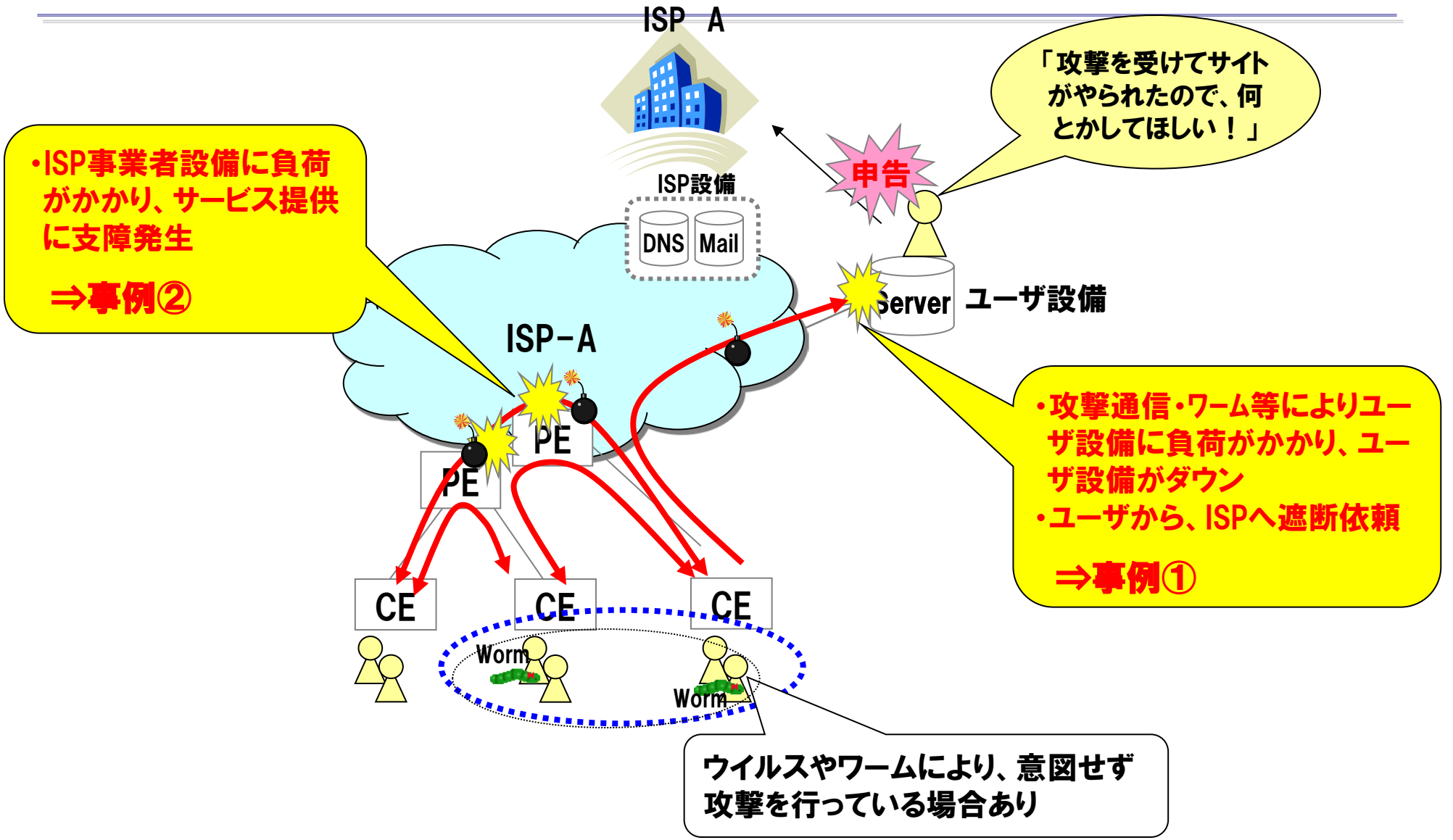
しかしながら、大量通信等が発生し、これにより事業者設備に生じる侵害を防止するために、原因となっている大量通信等の特性を把握した上で、これに合致した通信のみを遮断することは、通常は、正当防衛又は緊急避難として違法性が阻却される。

また、事業者の設備等に支障が生じうるが、これを回避するためには通信の間引き・遮断を行う必要がある場合において、当該支障のおそれを防止するとともに、遮断する通信の範囲を最小限に留めるために行われる大量通信等の特性の把握及びそれに合致した通信の遮断については、そのために相当な限度で行われる場合には、正当業務行為に当たると解される。

【事例】

・ ADSL利用者の構築したWebサーバに対して、インターネットから過度のトラフィック集中が発生し、その利用者を収容しているISPとADSL事業者との相互接続点において、ネットワーク機器が過負荷となり、他の利用者の通信が正常に行えなくなる事態が発生した。このためISPでは、当該利用者に断りをいれる前に、当該利用者の利用するIPアドレスに対する通信を遮断して他の利用者の通信を確保したうえで、当該利用者に状況を連絡した。

【参考】事例①、事例②



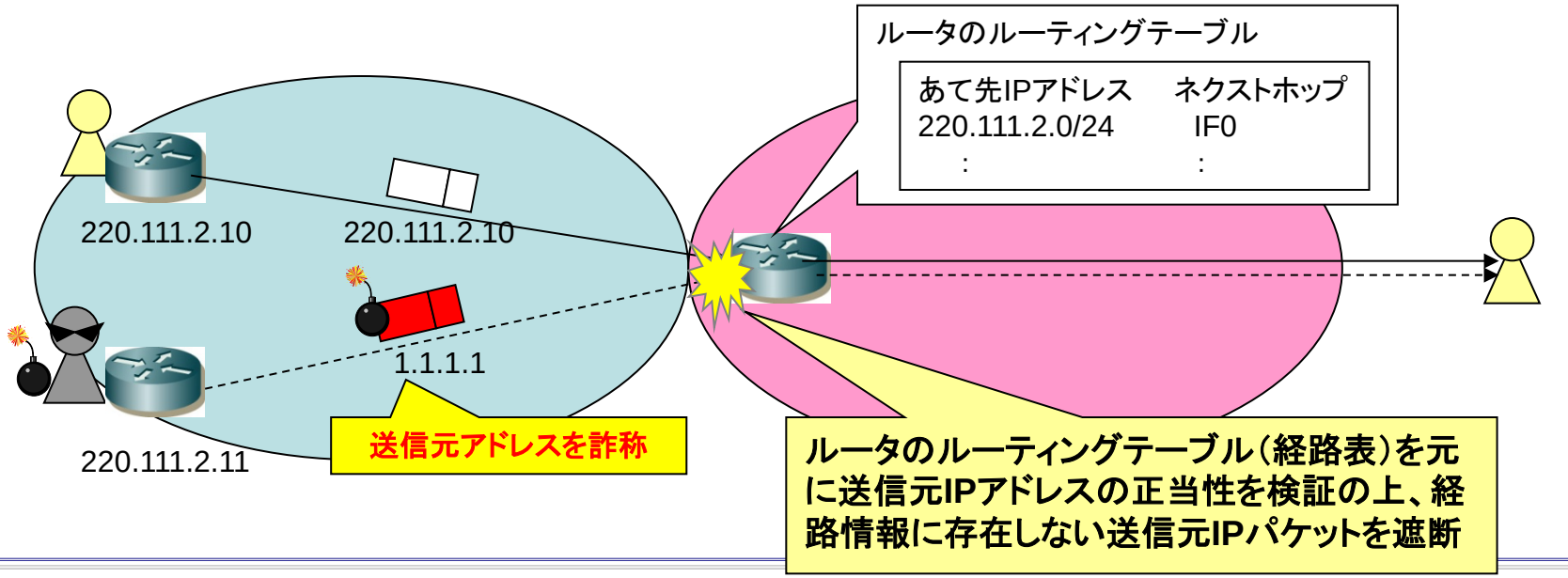
事例③：送信元詐称通信への対処

（キ）　IPによる通信は「送信元IPアドレス」を詐称している場合には成立しないため、送信元IPアドレスが詐称された通信は、攻撃を企図しているか設定の誤りより間違えて送出された通信と判断可能であるが、送信元IPアドレスを詐称した通信について、事業者において当該通信を自動的に遮断してよいか。

【考え方】

送信元IPアドレスを詐称した場合は、攻撃を意図しているか設定の誤りによって間違えたかいずれかと判断できる。事業者は、通信を成立させるという業務行為のために送信元IPアドレスの確認（認証）をしているが、送信元IPアドレスに関する情報を、送信元詐称通信を自動遮断するために利用することは、別途通信の秘密の窃用に当たりうる。

この点、一般的に、送信元詐称通信により事業者の業務遂行に支障が生じるおそれがある場合には正当業務行為として当該通信を遮断することができる。また、当該通信を遮断しない場合には下位レベルの設備等が侵害されるような場合には、通常、当該通信を遮断することは正当防衛又は緊急避難に当たるものと解される。



ガイドライン策定の意義

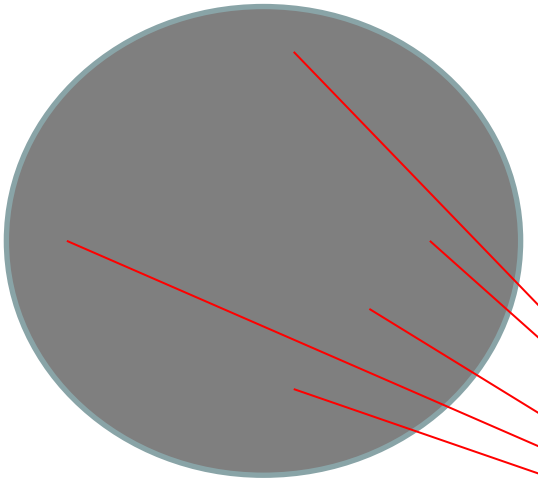
ガイドライン策定により期待されること

- 大量通信等への対処に法律解釈上の根拠を与え、運用担当者のリスクを軽減する
- 攻撃等への適法な対処に該当する具体的事例を記載することにより、円滑なサービス提供の確保する
- 業界内の共通認識を形成することにより、複数ISPの連携による対策が促進される
- 通信の秘密の保護についての正しい知識を、運用担当者レベルで共有することにより、通信の秘密の保護につながる

ガイドラインの効果

- あくまでも業界における解釈に過ぎず、ガイドラインに法的な効果はない。
- 法律の解釈指針は、一義的には行政庁（この場合は総務省）によって示されるが、解釈は最終的には裁判所により決定される。
- しかし、通信の秘密に関わる判例は少なく、判例ができるまでには時間がかかるため、日々刻々と進化するサイバー攻撃への対策の是非について決定されるまで待つことはできない。
- 仮に訴訟等になって、裁判所が判断を行うときでも、法的判断の解釈の参考として、参照されることを期待。

最近のspam攻撃の例
（大手、中小を問わずほとんどのISPで発生）



外国と思われるIPアドレス
（主に東欧、旧ソ連邦あたり）

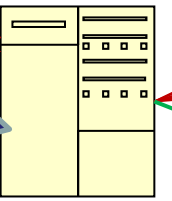
②ISPのユーザーのIDとパスワードを用いて、大量（例：数千）のIPアドレスから、587番（サブミッションポート）を使ってspamメール送信＊
（例：瞬間的に通常の数百倍の量）
（不正アクセスの可能性大）

④海外にあるspam送信元ブラックリストにISPのメールサーバーが掲載される。

SPAMHAUS

Beware of Cheap Imitations
ESTABLISHED spamcop.net 1998

大量のspam送信



③メールが滞留、数時間の遅延が発生

ISPのメールサーバー
（SMTPサーバー）

①日本のISPのユーザーのアカウント情報（IDとパスワード）を何らかの手段で取得したと思われる。

＊587番ポートを使うと、世界中のどこからでもISPのメールサーバーを使ってメール送信ができる。

⑤上記のブラックリストを参照する企業や学校宛にはメールが送信できなくなる。

⑥送信者からクレームを受けて、ブラックリストに解除申請するが、手続きに1週間程度かかる