# 「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（第2版）」について

2011年4月

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

# 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」の場において、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議論しています。
- 2007年5月30日に「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（第1版）」を策定し、その概要について報道発表しました。
- 今般、その改定を行ない、第2版として3月２５日に報道発表しました。
- 第1版は一般には非公開としましたが、今回改定版を作成するにあたっては、この点を見直し一般にも公表することになりました。
- 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

# 通信の秘密の保護

○電気通信事業法（昭和59年法律第86号）
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（略）
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、2年以下の懲役又は100万円以下の罰金に処する。
　　２（略）

**通信の秘密の対象**

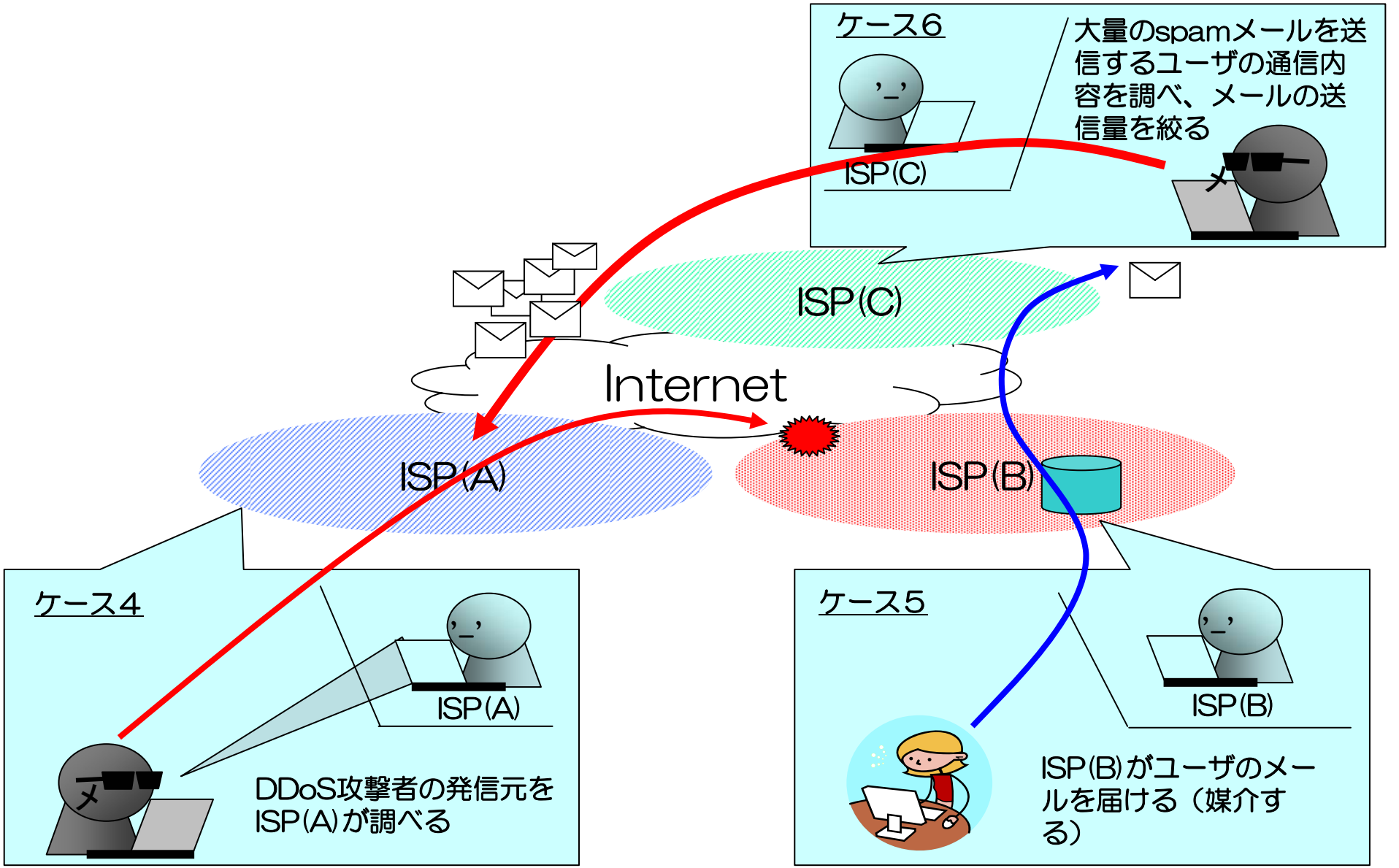
- **通信内容**
  - 通話の内容
  - メールの本文
- **通信当事者の住所、氏名、発信場所等通信の構成要素**
  - 発信者電話番号
  - メールのヘッダ
- **通信回数等通信の存在の事実の有無**
- **その他、これらを推測させるような事項**

# 侵害しても違法とされない場合

## 「違法性阻却事由」という法律用語

- 正当行為
  - 業務上必要な知得
  - 令状による開示，プロバイダ責任制限法4条など
- 正当防衛
  - 自己又は他人への急迫不正の侵害からの防衛
- 緊急避難
  - 自殺予告事案における警察への情報提供，110番の逆探知など

# インターネットにおける「通信の秘密」の侵害のケース



# インターネットにおける「通信の秘密」の侵害のケース

その他にも・・・

- 自ISPの契約者から、「自社のホームページが攻撃を受けているので、攻撃パケットをブロックしてほしい」との依頼があった
- 特定のユーザ宛の大量通信によって、事業者設備に支障が生じている
- ウイルスに起因する大量通信が不特定多数の送信元から送信され続けている
- 送信元詐称パケットが送信されている

・・等

**事業者が対処措置の実施可否を判断しなければならない**

# ガイドライン策定の動機

しかし・・・

- 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

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

# ガイドラインの概要

- サイバー攻撃等への対処と通信の秘密との関係について、Q&A形式で考え方を整理したもの
- テレコム4団体＋T-ISACが作成した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）
- 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必ず免責されるといった効果までは無いが、仮に法的な紛争があった際にはガイドラインに沿った対応を行っていることが考慮されるものと期待される
- 今後も継続的に議論を重ね、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、ガイドラインの更新を実施する予定
- 今回改訂にあたっては業界団体経由、事業者にガイドライン第1版への要望などをヒアリングを実施

# 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

# 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。

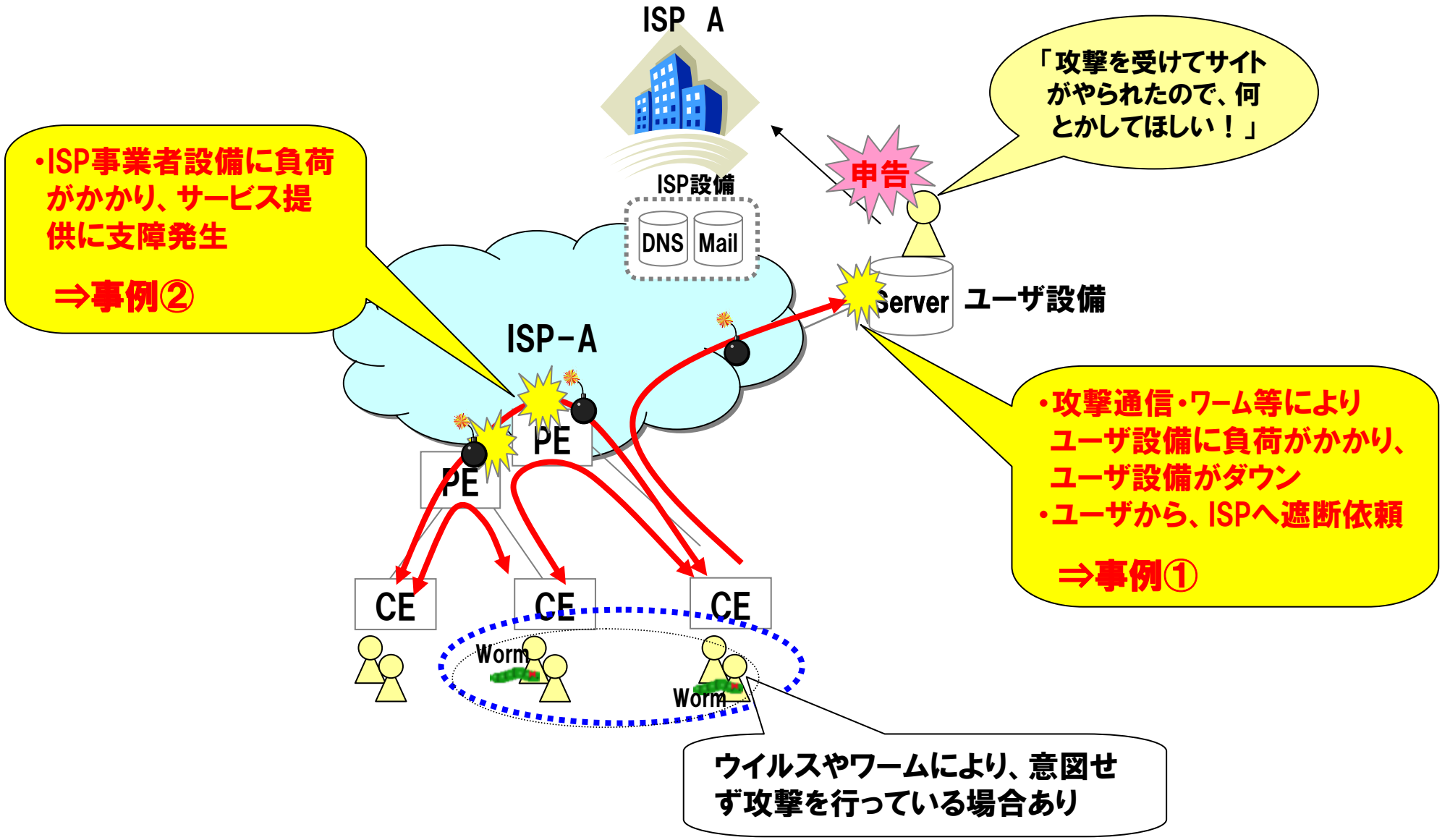
しかしながら、大量通信等が発生し、これにより事業者設備に生じる侵害を防止するために、原因となっている大量通信等の特性を把握した上で、これに合致した通信のみを遮断することは、通常は、正当防衛又は緊急避難として違法性が阻却される。

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


ISP A
ISP設備
DNS
Mail
申告
「攻撃を受けてサイトがやられたので、何とかしてほしい！」
•ISP事業者設備に負荷がかかり、サービス提供に支障発生
⇒事例②
ISP-A
PE
PE
Server
ユーザ設備
•攻撃通信・ワーム等によりユーザ設備に負荷がかかり、ユーザ設備がダウン
•ユーザから、ISPへ遮断依頼
⇒事例①
CE
CE
CE
Worm
Worm
ウイルスやワームにより、意図せず攻撃を行っている場合あり

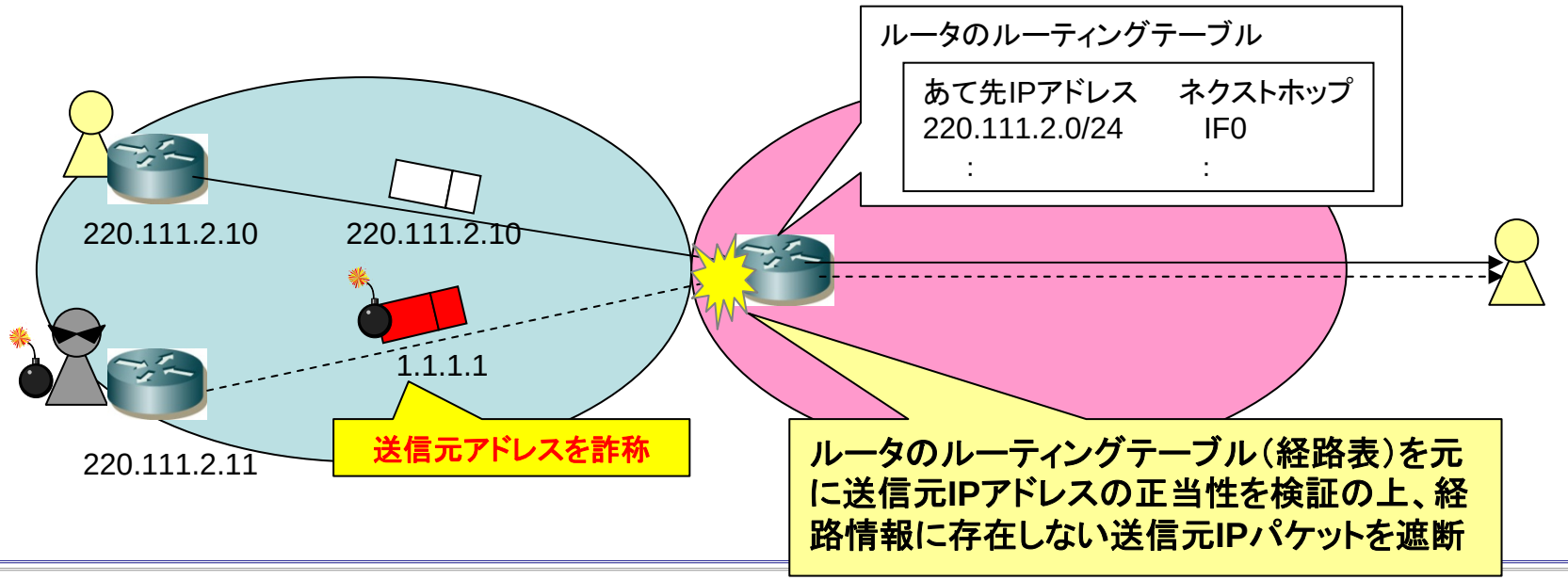
# 事例③：送信元詐称通信への対処

（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。

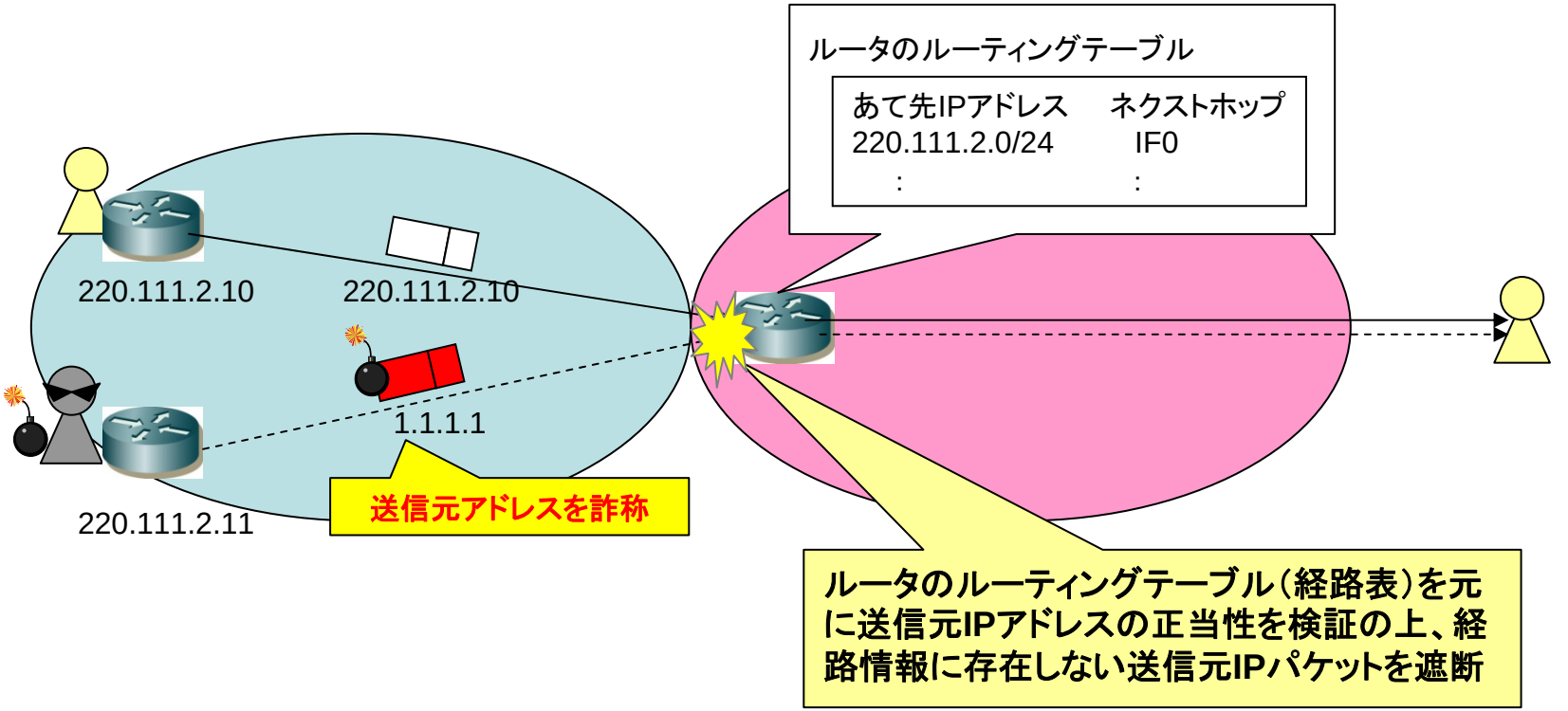
この点、一般的に、送信元詐称通信により事業者の業務遂行に支障が生じるおそれがある場合には正当業務行為として当該通信を遮断することができる。また、当該通信を遮断しない場合には下位レベルの設備等が侵害されるような場合には、通常、当該通信を遮断することは正当防衛又は緊急避難に当たるものと解される。



# 【参考】事例③

【事例】

- あるISPの網内に、インターネット上に経路の存在しないIPアドレス（プライベートIPアドレスや、未割り当てのIPアドレス）を送信元アドレスとした送信元詐称パケットが数多く流入しており、通信機器が過負荷となってサービス提供に支障をきたすおそれがあった。このため、このISPでは他のISPから網内に流入する通信の送信元IPアドレスとインターネット上の経路情報とを突合し、経路情報が存在しない場合には当該パケットを遮断する設定を行った。



# まとめ

- 大量通信等への対処の前提として、運用担当者レベルで法律解釈を知っておくことが重要
  - 通信の秘密は国民（利用者）の重要な権利
  - 通信の秘密侵害の罪は重い（3年以下の懲役又は200万円以下の罰金）
  - 知らないで対処するのは大きなリスク
  - ただし、やってはいけないことをやっているわけではない
  - 運用担当者、会社、業界としてのリスク軽減にもつながる

- 今後必要な業界横断的な対応を容易にする
  - 今回のガイドラインは、業界の共通認識の形成につながるもの
  - 共通の法律解釈をISPが共有することにより、ISPが連携して行わなければならない対処策の実施を法制度面からバックアップする