

Internet Week 2015

S9 ISPによる昨今のセキュリティ事案対応と通信の秘密のガイドライン

ガイドライン改定内容について

2015年11月18日

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

通信の秘密のガイドラインとは



- ▶ 正式名称は「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」
- ▶ 電気通信関連の4団体とテレコムアイザックで構成する「インターネットの安定的な運用に関する協議会」（次頁）が作成しています。
- ▶ あくまでも民間の自主基準、法令の解釈指針という性質のガイドラインであって、法令上の位置づけがあるガイドラインではありません。

インターネットの安定的な運用に関する協議会





構成員

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

オブザーバー 総務省

ガイドラインの変遷

- ▶ 2007 初版 非公開
- ▶ 2011 第2版 これ以降、公開
- ▶ 2014 第3版  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」(2014年4月4日公表)
- ▶ 2015 第4版  (予定) 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」(2015年9月9日公表)

ガイドラインの名称を大量通信から、サイバー攻撃に改める予定です。

ガイドライン策定の背景

- ▶ 初版（2007年）非公表 概要のみ公開
- ▶ この前後、botnetやantiminyウイルスによるDDoS攻撃が多発したことが背景。
- ▶ 具体的攻撃手法の事例を記述したため、読み方によっては、ISPが対処できない攻撃方法を考えられることが懸念されたため。
- ▶ ISPなど通信事業者に対しては、4団体会員以外にも提供

初版の概要

- ▶ 通信の秘密の定義
- ▶ 機械的検索と通信の秘密の関係の整理
- ▶ 正当業務行為、違法性阻却事由が成立するための要件を整理

通信の秘密って、よく聞くけど

- ▶ 通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段
- ▶ 通信の秘密は、個人の私生活の自由を保護し、個人生活の安寧を保護する（プライバシー保護）
- ▶ 憲法上の基本的人権の一つとして憲法第21条第2項において保護されている。
- ▶ 電気通信事業者は勿論、一般国民でも通信の秘密を侵すと罰せられることがあります。
(一般人でも、電話の盗聴とかすると罰せられます。)

でも、法律には、これしか書かれていません。



(秘密の保護)

- ▶ 第四条 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。

(罰則)

- ▶ 第一百七十九条 電気通信事業者の取扱中に係る通信（第一百六十四条第二項に規定する通信を含む。）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。
- ▶ 3 前二項の未遂罪は、罰する。

法律の解説本にも詳しくは書かれていません。

- ▶ 電気通信事業者の取扱中に係る通信とは？
- ▶ 通信の秘密とは？
- ▶ 通信の秘密を侵すとは？

- ▶ でも5ページ位の抽象的な記述

- ▶ これでは、、、



そもそも通信の秘密の対象となる通信とは？



- ▶ インターネット接続
- ▶ 電子メール

- ▶ 公開されているホームページへのアクセス（閲覧、書き込み）

- ▶ ECサイトにおけるショッピングサービスは？

- ▶ ホスティングサービスの場合は？

- ▶ SNS内のメッセージは？

秘密を侵すって？

- ▶ プライバシーなど、他人の権利を侵すことはいけないことですよね。
- ▶ でも「『通信の秘密』の範囲には、個別の通信に係る通信内容のほか、個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号等の当事者の識別符号等これらの事項を知られることによって通信の意味内容を推知されるような事項全てが含まれる。」*とか言われて

*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
P15,16 平成26年4月

秘密を侵すって？(続)

- ▶ しかも、「機械的・自動的に特定の条件に合致する通信を検知し、当該通信を通信当事者の意思に反して利用する場合のように機械的・自動的に処理される仕組みであっても該当し得る。」*となると、
- ▶ ISPのやっていることで、通信の秘密の侵害にあたることって沢山ありそうです。

*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
P15,16 平成26年4月

しかも、こういう解説は

- ▶ 総務省の研究会の報告書とか、裁判の判例とか見ないと書かれていません。
- ▶ 普通の人には研究会の報告書とか、裁判の判例とかはまず見ないですね。
- ▶ しかも裁判の判例は、電話、電報を例にした古いものが多いです。平成14年とかはまだ新しいほう。

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

それでガイドラインを作りました。

- ▶ インターネットを運用する人が、実際の対応において通信の秘密の問題との関係でやっていかどうか判断するため。
- ▶ 抽象的な規定のみでは、現場が困るから、具体的事例を出して。
- ▶ まったく同じ事例でなくても、考え方を示すことで応用も効くように。

ガイドラインを作って整理されたこと



- ▶ 侵害しても、違法でなければ良い。
- ▶ これを「違法性阻却事由に該当」と言います。
- ▶ 違法性阻却事由
 - 正当行為
 - 正当業務行為
 - 法令に基づく行為
 - 正当防衛、緊急避難
- ▶ あと、そもそも当事者の同意があれば、秘密でなくなるので、通信の秘密の問題ではなくなります。
 - でも、同意って？ 約款（利用規約のみ）で良いの？

ISPの場合、正当業務行為って？

- ▶ ア. 電気通信事業者が課金・料金請求目的で顧客の通信履歴を利用する行為、
- ▶ イ. ISP がルータで通信のヘッダ情報を用いて経路を制御する行為等の通信事業を維持・継続する上で必要な行為、
- ▶ ウ. ネットワークの安定的運用に必要な措置であって、目的の正当性や行為の必要性、手段の相当性から相当と認められる行為（大量通信に対する帯域制御等）
 - 帯域制御のほか、OP25B,IP25Bも同様

こういうことが、ガイドラインの総論部分に書かれています。

同様に、正当防衛はどういう時？

こちらは、ガイドラインの各論部分に沢山でてきます。

- ▶ 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一時的に遮断することは、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。

(第5条 大量通信等について1 攻撃通信への対応 (1) 大量通信等に係る通信の遮断 イ 事業者設備に支障が生じる場合)

刑法(正当防衛)

第36条 急迫不正の侵害に対して、自己又は他人の権利を防衛するため、やむを得ずにした行為は、罰しない。

(緊急避難)

第37条 自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その程度を超えた行為は、情状により、その刑を減輕し、又は免除することができる。

(難しくいうと)ガイドラインの目的は

- ▶ 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する。
- ▶ 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。

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。

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

大量通信等から変更

NEW

ガイドラインの構成(続)

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

(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

例えば、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って、



- ▶ つまり、マルウェア感染者への対応
- ▶ マルウェア感染者からの通信を遮断したり、通信ログの解析を行って利用者を特定して、マルウェアを削除するよう連絡していいか？

ガイドラインの構成(続々)



第6条 電気通信役務の不正享受

- (1) 他人の認証情報を悪用したインターネットの不正利用への対処
- (2) IP電話等の電話サービスの不正利用への対処

PPPoEアカウントの乗っ取り、IP電話による国際電話不正架電など実際に発生した事案に対応

今回の改正のポイント

DNS の機能を悪用した DDoS 攻撃に用いられている名前解決要求に係る通信の遮断	DNSAmp攻撃やランダムサブドメイン攻撃による攻撃等への対処で、DNSサーバを通過する全ての名前解決要求に係るFQDNを常時確認し、リストに基づいて、FQDNが一致する場合に当該名前解決要求に係る通信を遮断
脆弱性を有するブロードバンドルータ利用者への注意喚起	リフレクション攻撃に悪用され得る脆弱性やPPPoE認証の情報を窃取され得る脆弱性を有するブロードバンドルータを、ネットワーク上で調査し、契約者の接続ログから、当該ブロードバンドルータを保有している契約者を特定し、契約者に対して注意喚起
C&C サーバ等との通信の遮断における有効な同意	個別の同意を取得していない場合であっても、契約約款等に基づく事前の包括同意として、マルウェア感染端末とC&Cサーバ等との通信をレピュテーションDBに基づいて遮断
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	電気通信役務の不正享受への対処(1) 他人の認証情報を悪用したインターネットの不正利用への対処 従来SMTP認証だったものにPPPoE認証も追加
IP電話等の不正利用への対策	IP電話等の電話サービスの不正利用への対処

前回の改正のポイント

大量通信等に係る通信の遮断	従来は全加入者に影響がなくては、遮断できないような記述だったものを、一定の条件を満たせば全加入者に影響がなくても遮断
DNSAmP攻撃等への対応	正当業務行為として違法性が阻却される
マルウェア感染者の通信の遮断	従来、事業者設備への支障が現実には生じている場合しか遮断は認められなかったと読めたものを、事業者設備への侵害の防止、あるいは受信者設備への侵害であっても、事業者設備への侵害となるような場合にも遮断できると明確化
テイクダウンしたC&Cサーバの情報からのマルウェア感染者への注意喚起	第三者から提供されたマルウェア感染端末情報と契約者の接続ログを突合し、当該感染端末を保有している契約者を特定した上で、当該加入者に対して注意喚起
Black Listの活用	従来、Black Listの活用について否定的な表現であったものを削除
レピュテーションDBの活用	ACTIVE!を想定し、一定の正当性を有するデータベースを活用するものについては、契約約款に基づく事前の包括同意が有効な同意で、通信の秘密の侵害とならないとした
SMTP認証の情報を悪用したspamへの対処	不正利用の蓋然性が高いSMTP認証の利用者に連絡を取りパスワードの変更を依頼、あるいはアカウントを一時停止。
マルウェア配布サイトとの通信の警告における有効な同意	個別の同意を取得していない場合であっても、契約約款等に基づく事前の包括同意として、マルウェア感染端末とマルウェア配布サイトとの通信をレピュテーションDBに基づいて注意喚起

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。
- ▶ 今のところ8年近く運用してきて、法的な問題が生じ、争いとなったことはないと思われる。

法的効果におけるガイドラインの位置



憲法

日本国憲法

法律

電気通信事業法

省令

電気通信事業法施行規則など

告示

電気通信事業における個人情報保護
に関するガイドライン

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

ガイドラインの今後



- ▶ 今回の改訂（第4版）は、うまくいけば協議会のホームページで本年11月中に公開される予定です。
- ▶ 新しいサイバー攻撃等の登場や対応手法に応じて事例の修正、追加などが必要
- ▶ 関連するほかの解釈文書などとの統合の必要性があることは感じています。（迷惑メール対策とか）