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

初版　2007 年 5 月 30 日

第 2 版　2011 年 3 月 25 日

第 3 版　2014 年 7 月 22 日

第 4 版　2015 年 11 月 30 日

インターネットの安定的運用に関する協議会

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

はじめに

DoS 攻撃等のサイバー攻撃や迷惑メールの大量送信などに対してインターネットサービスを提供する電気通信事業者が行う対応が、主に電気通信事業法第4条で定められた通信の秘密の保護について違法性がないかどうかを判断する参考とするため、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の 4 団体(以下、電気通信関連 4 団体)は、「インターネットの安定的運用に関する協議会」を開催し、これらの点について検討を行った。その結果を取りまとめたものが本ガイドラインであり、2007年 5 月に第 1 版を制定し、関係者限りで配布した。

その後、インターネットを巡る環境変化などを踏まえ、本ガイドラインを検証するべく、上記 4 団体に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を加え、「インターネットの安定的運用に関する協議会(第 2 期)」を開催し、その検討結果を取りまとめたものを第 2 版として制定・公表した。

2013 年 11 月から、総務省において「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」が開催され、2014 年 4 月に研究会の「第一次とりまとめ」、2015 年 8 月に「第二次とりまとめ」が公表されたことから、これを踏まえた追加修正を行い、それぞれ第 3 版、第 4 版とした。第 4 版に改版するに当たって、題名を「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」から「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」に変更した。

目次

改版履歴

版数　作成年月	改版理由
第1版 2007 年(平成 19 年) 5 月	新規作成
第 2 版 2011 年(平成 23 年) 3 月	章、条番号の付加、3,4 条追加、2 章内容見直し等
第 3 版 2014 年(平成 26 年) 7 月	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 第一次とりまとめ結果等を反映
第 4 版 2015 年(平成 27 年)11 月	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 第二次とりまとめ結果等を反映

第1章　総則

第 1 条　目的

DoS 攻撃、DDoS 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及び壊れたパケット等（以下「サイバー攻撃等」という。）は、その対象となる利用者の設備に支障を与えるのみならず、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も影響を与えかねない事態をしばしば引き起こす。また、第三者が他人の認証情報等を悪用し、不正にインターネットや IP 電話を利用する行為（以下「電気通信役務の不正享受」という。）は、正規の利用者に金銭的被害等をもたらすだけでなく、電気通信事業者による契約に基づく適正な課金・料金請求を阻害し、通信事業の維持・継続に支障をきたすおそれがある。電気通信事業者としては、円滑な電気通信役務の提供を確保するためには、このようなサイバー攻撃等や電気通信役務の不正享受に係る通信を遮断する等の対応が必要となる。

しかしながら、このような通信を識別し、それに対応するにあたっては、通信の秘密（電気通信事業法（昭和 59 年法律第 86 号。以下「事業法」という。）第 4 条）との抵触が避けられない場合も考えられるため、関係法令に留意し、適法に実施することが必要である。

本ガイドラインでは、遮断等を始めとするサイバー攻撃等や電気通信役務の不正享受への対処が、通信の秘密の侵害に該当しうるのか否か、また、通信の秘密の侵害に該当したとしても、違法性が阻却されうるのか否かについて、基本的な考え方を整理すると共に、該当する事例を挙げることにより、電気通信事業者におけるサイバー攻撃等や電気通信役務の不正享受への対処の参考に資するものである。なお、当然のことながらサイバー攻撃等や電気通信役務の不正享受のパターンやそれらに対する対処方法は当ガイドラインにあるものだけにとどまるものではなく、実際の対処において本ガイドラインに書かれていない手段を用いることを否定するものではない。その場合の判断は個別に行われるべきであるが、迷う場合には監督官庁である総務省に照会することが好ましい。また、本ガイドラインに記述されているものであっても、個々の判断は実際の状況に応じて個別になされるべきものである。

第 2 条　総論

1　通信の秘密

第1節　通信の秘密の保護に関する規定

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）とともに、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であることから、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。これを受けて、電気通信事業法において、罰則をもって、「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。」ものとして、通信の秘密を保護する規定が定められており（電気通信事業法第4条第1項、同第 179 条）、電気通信事業法上も、通信の秘密は厳格に保護されている。

第2節 「通信の秘密」の意義

「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。

第3節 「侵す」の意義

（1） 侵害の3類型

一般に、通信の秘密を侵害する行為は、通信当事者以外の第三者による行為を念頭に、以下の3類型に大別されている。

① 知得：積極的に通信の秘密を知ろうとする意思のもとで知得しようとする行為

② 窃用：発信者又は受信者の意思に反して利用すること

③ 漏えい：他人が知り得る状態に置くこと

ここにいう、知得や窃用には、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。

（2） 通信当事者の同意

なお、通信当事者の有効な同意がある場合には、通信当事者の意思に反しない利用であるため、通信の秘密の侵害に当たらない。もっとも、次の理由から、原則として契約約款等に基づく事前の包括同意のみでは、一般的に有効な同意と解されていない 。

① 約款は当事者の同意が推定可能な事項を定める性質であり、通信の秘密の利益を放棄させる内容はその性質になじまない。

② 事前の包括同意は将来の事実に対する予測に基づくため対象・範囲が不明確となる。

ただし、以下の第 2 章第 5 条3（2）②及び③にあるように、マルウェアの感染防止に有効な手段であるマルウェア配布サイトへのアクセスに対する注意喚起における IP アドレス又は URL の利用、マルウェア感染による被害の防止に有効な手段であるマルウェア感染端末と C&C サーバ等へのアクセスの遮断における FQDN の利用等の場合に関しては、個別の同意がある場合のほか、契約約款に基づく事前の包括同意であっても、一定の条件の下においては、有効な同意と考えられる。

（3） 違法性阻却事由

通信当事者の同意を得ることなく通信の秘密を侵した場合であっても、正当防衛（刑法第 36 条）、緊急避難（刑法第 37 条）に当たる場合や、正当行為（刑法第 35 条）に当たる場合等違法性阻却事由がある場合には、例外的に通信の秘密を侵すことが許容されることになる。

いずれか一つの違法性阻却事由があれば、通信の秘密の侵害が許容されることとなるが、緊急時に行われる対策については、一般的に、正当防衛、緊急避難の要件を満たす場合には通信の秘密の侵害について違法性が阻却される。

「正当防衛」として違法性が阻却されるためには、①急迫不正の侵害に対して、②自己又は他人の権利を防衛するために、③やむを得ずした行為であることであることが必要となる[1]。また、「緊急避難」として違法性が阻却されるためには、①現在の危難の存在、②法益の権衡、③補充性の全ての要件を満たすことが必要となる[2]。

常時行われる対策については、一般的には、急迫性、現在の危難といった要件を必ずしも満たさないため、正当防衛、緊急避難には該当しないが、正当行為の一類型である正当業務行為に当たる場合には違法性が阻却される[3]。

ところで、電気通信事業者による通信の秘密の侵害行為について違法性阻却事由があると考えられる場合については、実務上の運用事例を通じて一定の考え方が整理されてきている。

これまで緊急避難が認められると整理された事例としては、

ア. 人命保護の観点から緊急に対応する必要のある電子掲示板等での自殺予告事案について、ISP が警察機関に発信者情報を開示する場合、

イ. ウェブ上において流通し得る状態に置かれた段階で児童の権利等に重大かつ深刻な法益侵害の蓋然性があるといえる児童ポルノに対するブロッキングを行う場合

といったものが挙げられる。

また、正当行為については、法令に基づく行為及び正当業務行為があるが、これまでに正当業務行為が認められると整理された事例としては、

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）

---

[1] 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。

[2] 刑法
（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、その刑を減軽し、又は免除することができる。

[3] 刑法
（正当行為）
第 35 条 法令又は正当な業務による行為は、罰しない。

等が挙げられる。[4]

こうした事例の根底にある基本的な考え方は、国民全体が共有する社会インフラとしての通信サービスの特質を踏まえ、利用者である国民全体にとっての電気通信役務の円滑な提供という見地から正当・必要と考えられる措置を正当業務行為として認めるものである。

2 留意事項

（1）各論の検討においては、概括的に、「攻撃通信への対応」、「迷惑メールへの対応」、「その他の情報共有・情報把握」、「電気通信役務の不正享受」に分けて基本的な考え方を記述している。

各論は、サイバー攻撃等や電気通信役務の不正享受が発生した場合に想定される対処策の例を挙げ、それらの行為について通信の秘密の侵害に当たるか否かを整理したものである。したがって、電気通信事業法第6条に定める「利用の公平」や、個人情報の保護、契約解除の可否、財産権の侵害など、その他の法的問題については、別途検討が必要な場合があることに留意する必要がある。

（2） 各論の整理は、抽象化された事案をもとに検討したものであるため、実際に、サイバー攻撃等や電気通信役務の不正享受への対応を行うに当たっては、具体的な事実関係を踏まえた上で更に検討を行うことが必要な場合があることに留意する必要がある。サイバー攻撃等や電気通信役務の不正享受への対応の方法は、関係する事業者の回線の規模や状況、攻撃の手法などにより異なることから定量的基準を設けることは適当でないと考えられ、それぞれがこのガイドラインの適用事例となるかどうかはそれらを考慮し、個別に判断されるべきものである。また、正当業務行為等の違法性阻却事由の判断における、「手段の相当性」等の判断においては、通信の秘密の検知・確認を可能な限り機械によって行うべきこと、サイバー攻撃等や電気通信役務の不正享受への対応に必要な範囲内にとどめなければならないこと等に留意する必要がある。

なお、各事案に関する個別具体的な検討については、技術等詳細な事実関係が必要であること、攻撃等の変化に応じて対処策も日々変化することなどから、事例集等の形で随時整理することが適当であるため、本ガイドラインにおいては記述しない。

第3条　定義

1 サイバー攻撃等

DoS 攻撃、DDoS 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及び壊れたパケット等[5]

[4] 帯域制御のほか、OP25B,IP25B も同様

[5] インターネットの特定ユーザや特定アプリケーションによるトラヒックの圧迫、占有については、電気通信関連 4 団体連名による「帯域制御の運用基準に関するガイドライン」（2008 年 5 月策定、2010 年 6 月改定）を参照されたい

２ 電気通信役務の不正享受

第三者が他人の認証情報等を悪用し、インターネット接続や IP 電話等の電気通信役務を不正に利用する行為

３ 攻撃通信

サイバー攻撃等によって引き起こされた大量通信のうち受信した設備に異常を来たす通信

４ 通信

電気通信事業法第 2 条 1 号でいう電気通信を意味し、有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けることをいう。「送り」「伝え」「受ける」の各行為は、それぞれ単独でも「電気通信」となるものであるが、各行為はそれぞれ関連性を有すると解釈される。（平成 20 年版電気通信事業法逐条解説より）

第4条　　見直し

本ガイドラインは、インターネットの安定的運用に関する協議会により、インターネットの利用環境や技術の進展、サイバー攻撃等や電気通信役務の不正享受の状況を踏まえて、適宜見直される。

第 2 章　各論

第 5 条　サイバー攻撃等について

1　攻撃通信への対応

(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

（ア）攻撃通信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。

【考え方】

「自社契約者から特定の ISP 別へのトラヒック及びその通信種別情報」及び「特定の ISP 別から自社契約者へのトラヒック及びその通信種別情報」等を取得して作成した統計処理したデータに基づき、攻撃通信を分析し、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を遮断することは、通信の秘密の侵害（窃用等）に当たりうる（なお、統計処理したデータの取得自体については(6)を参照）。

この点、受信者又は受信回線の契約者から、「特定の受信回線宛の通信について、その内容等を分析し、一定の攻撃特性を有する通信のみを遮断する（通信の秘密を侵害する）」ことについて個別の同意を取得すれば、通信の秘密の侵害とならない。

【事例】

・ 利用者から Web サーバに対する攻撃が発生したとの申告があり、利用者の依頼に基づき、ISP において事業の設備増強見積もり等のために常時取得している統計データをもとに、通信総量、方向、パケットサイズの分布、プロトコル分布、通信の送信元の分布について調査を行った。その結果、特定地域(特定IPアドレス空間)から利用者の Web サーバのIPアドレスのポート 80 番に対し、TCP の接続開始を示す Syn パケットが大量に送出されていることが判明した。

（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】

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契約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。

【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。

（ウ） 送信側ISPにおいて、受信者から提供された受信ログ等の被害を示す情報と、送信者の接続ログを突合し、当該受信者宛に攻撃通信を行っている契約者を特定した上で、契約者に対し攻撃通信を止めるよう連絡をするなど何らかの措置を採ってよいか。

【考え方】

通信履歴（ログ）は通信の秘密として保護されるものであり、攻撃通信を行っている契約者を特定するため、自社の契約者の接続ログを解析し、当該契約者に連絡をすることは通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、侵害の防止に他に有効な手段がない場合、攻撃を受けている受信者の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、攻撃通信を行っている契約者を特定した上、これを止めるよう当該契約者に連絡をすることは、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と考えられる。

イ 事業者設備に支障が生じる場合

（エ） 特定の受信者宛のサイバー攻撃等やマルウェアなどに起因するサイバー攻撃等の発生によって、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、当該サイバー攻撃等の特性（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】

発生しているサイバー攻撃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、その特性を把握し、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（窃用等）に当たりうる。

しかしながら、サイバー攻撃等が発生し、これにより事業者設備に生じる侵害を防止するために、原因となっているサイバー攻撃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。

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サイバー攻撃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】

- ブロードバンド利用者の構築した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とブロードバンドアクセス回線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。
- 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。

（オ）サイバー攻撃等が、マルウェアや攻撃ツールにより攻撃先のIPアドレスをDNSサーバで検索・取得した上で行われていることが判明した場合、当該IPアドレス宛通信のうち、別のドメイン名宛の通信まで遮断してしまうことを防ぐため、発生したサイバー攻撃等そのものを遮断するのではなく、その前段で行われるDNSサーバへの検索において、本来のIPアドレスではなく、通信破棄用のIPアドレスを返答することで、当該サイバー攻撃等の発生を防止してよいか。

【考え方】

サイバー攻撃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ことは、通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、サイバー攻撃等により事業者設備に生じる侵害を防止するために行われる行為として、当該特性を有する通信を遮断するのではなく、DNSサーバへの検索において一時的に通信破棄用のIPアドレスを返答することも、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、このような対応も、事業者の設備等に生じる支障のおそれを防止するとともに、別のドメイン名宛の通信まで遮断してしまうことを防ぐために行われる場合には、その目的は正当であるといえ、必要かつ相当な方法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】

- あるWebサイト宛の大量の通信により通信設備の運営に支障をきたす状況が発生した。当該攻撃対象Webサイトを収納するサーバには、他のサービスも共存していたため、当該サーバに割り当てられたIPアドレス宛の通信全体を遮断対象とした場合、他のサービスへの通信も遮断される可能性があったため、DNSの設定変更により当該Webサイトのドメイン名の検索に対しては、通信破棄専用のIPアドレスを返答するようにすることで、当該Webサイト宛の通信のみが行われないようにした。

（カ）想定されていない外部からの問い合わせを受ける設定となっているルータ等（オープンリゾルバ等）を利用して、DNSやNTP等の通常のインターネットの機能を悪用し、サイバー

攻撃等を発生させる攻撃（DNSAmp 攻撃や NTPAmp攻撃等）がある。これらの攻撃は、ISP の電気通信役務の安定的提供に影響を及ぼすことから、当該攻撃を未然に防止するため、ISP のネットワーク網の入口又は出口において、そこを通過する全ての通信の宛先 IP アドレス及びポート番号を常時確認し、当該 ISP の管理下の動的 IP アドレス宛てであって、当該問い合わせに係る特定のポートに対して送信された通信を割り出し、これを遮断してよいか。

（キ） 特に、オープンリゾルバとなっているルータ等を踏み台にし、DNS の機能を悪用することでサイバー攻撃等を発生させる DNSAmp 攻撃やランダムサブドメイン攻撃[6]に関して、ISP において、攻撃に悪用されている名前解決要求の FQDN[7]を収集したリストを活用し、自社 DNS サーバを通過する通信を検知した上で、名前解決要求に係る FQDN とリストにある 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してよいか。

【考え方】

通常想定されていないネットワーク外部からの問い合わせを受ける設定となっているブロードバンドルータ等を利用して、DNS 等の通常のインターネットの機能を悪用し、サイバー攻撃等を発生させる攻撃（DNSAmp 攻撃等。以下「Amp 攻撃等」と呼ぶ。）に対して、全ての通信の宛先 IP アドレス及びポート番号を常時確認し、動的 IP アドレス宛てであって、特定のポート番号に対して送信された通信のみを機械的に遮断することは通信の秘密の窃用等に当たりうる。

しかしながら、当該行為は、Amp 攻撃等により ISP の通信設備が過負荷状態になることによるインターネットアクセスやメールの遅延等の発生を防止し、もって、インターネット接続役務等の電気通信役務の安定的提供を図るためのものであり、通常の通信環境下において、ブロックの対象となる、動的 IP アドレス宛てであって、特定のポート番号に対して送信されるネットワーク外部からの通信は想定されず、侵害される通信の秘密も宛先 IP アドレス及びポート番号のみと相当な限度で行われることから、正当業務行為として違法性が阻却されると考えられる※。

※詳細な検討は「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」（以下「第一次とりまとめ」という。） P24 参照
（http://www.soumu.go.jp/main_content/000283608.pdf）

また、DNSAmp 攻撃やランダムサブドメイン攻撃によるサイバー攻撃等から事業者設備に生じる侵害を防止するために、自社 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、攻撃に係る名前解決要求の FQDN のリストに基づいて、名前解決要求に係る FQDN とリストにある 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することは通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、当該行為は攻撃により ISP の通信設備が過負荷状態になることによるインタ

---

[6] 特定のドメインを攻撃対象とし、当該ドメインのサブドメイン部分をランダムにした文字列に関する名前解決要求を行い、権威 DNS サーバ及び ISP の DNS サーバに大量の名前解決要求の処理を発生させることで、権威 DNS サーバ及び ISP の DNS サーバを応答不能にする攻撃。

[7] Fully Qualified Domain Name の略。サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ（サーバ等）を特定するもの。

ーネットアクセスやメールの遅延等の発生を防止し、もって、インターネット接続役務等の電気通信役務の安定的提供を図るためのものであり、また、侵害される通信の秘密も名前解決要求に係る FQDN のみと相当な限度で行われることに加え、その手法についても攻撃に係る通信のみを遮断するものであるから、正当業務行為として違法性が阻却されると考えられる※。

※詳細な検討は「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」（以下「第二次とりまとめ」という。） P22 参照
（http://www.soumu.go.jp/main_content/000376396.pdf）

【事例】

- DNS 及び NTP の仕組みを悪用した Amp 攻撃が急増している状況を踏まえ、ある ISP において、当該攻撃によるインターネットアクセスやメールの遅延等の発生を未然に防止するため、自社のネットワーク網の入口又は出口を通過する全ての通信の宛先 IP アドレス及びポート番号を常時確認し、自社の管理下の動的 IP アドレス宛てであって、UDP53 番ポート又は UDP123 番ポートに対して送信された通信を割り出し、これを遮断した。
- DNS の仕組みを悪用した DNSAmp 攻撃やランダムサブドメイン攻撃の状況を確認するため、ある ISP において、あえてオープンリゾルバの脆弱性を残した DNS サーバ（DNS ハニーポット）を用意（ISP が利用者に提供するキャッシュ DNS サーバとは別に用意し、通常、利用者は当該ハニーポットには接続しない）し、当該ハニーポットに対して行われた名前解決要求の情報を分析することで、攻撃に係る名前解決要求の FQDN を収集してこれをリスト化した。このリストを活用し、自社の DNS サーバを通過する全ての名前解決要求を常時確認して、名前解決要求に係る FQDN とリストにある FQDN とが一致した場合に、当該名前解決要求は攻撃に係る通信であると判断し、これを遮断した。

ウ 送信元設備の所有者の意思と関係なく送信されるサイバー攻撃等の場合

（ク） サイバー攻撃等がマルウェアなどに起因したものであり、不特定多数の送信元から送信され続けている状況下において、①通信パケット及び接続ログから送信元の契約者を特定し、当該契約者に対しマルウェアなどを駆除するよう要請することを通じ、当該サイバー攻撃等の漸減を図ってよいか。また、②当該契約者からの送信に限り遮断の対象となるよう事業者設備を設定することで、通信遮断を行ってよいか。

【考え方】

個々の通信パケットの内容及び接続ログは、いずれも通信の秘密として保護されるものであり、サイバー攻撃等を送信している契約者を特定するため、これらを解析し、当該契約者に要請を行うことは、通信の秘密の侵害（窃用等）に当たりうる。また、把握した特性に基づき、特定の契約者からの送信に限って通信を遮断することは通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、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と考えられる。

また、サイバー攻撃等が発生し、これにより事業者設備への侵害又は受信者設備等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は、一時的に当該通信を遮断することも、正当防衛又は緊急避難として違法性が阻却されうると解されるところ、事業者設備の設定により、遮断による影響が及ぶ対象者を、サイバー攻撃等を行っている契約者に限定することは、そのための手段として相当と考えられる。

【事例】

・ 特定サイトがマルウェアによるDoS攻撃の対象となっていた。ISP は、攻撃の脅威から ISP の電気通信設備を守るため、攻撃通信そのものを減少させる必要があった。ISP は、攻撃パケットのヘッダ情報（発信元情報等）を分析し、その情報を攻撃パケットの発信元のISPと共有することにより攻撃パケットの送信者を特定し、メールにより注意喚起を行った。

(2) 送信元詐称通信の遮断

（ケ） 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に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の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、別途通信の秘密の侵害（窃用等）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と下位レベルの設備等が侵害されるような場合には、通常、当該通信を一時的に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。

【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。

・ ある ISP において、当該 ISP が契約者に割り当てたIPアドレスを送信元アドレスとするパケットが、他の ISP や当該 ISP の他の利用者との接続点など本来ありえない経路で流入している事象が確認され、網内に送信元詐称パケットが流入していることが判明した。詐称されたIPアドレスを使用している善意の利用者の元へは返信パケットが数多く送信され、当該利用者を収容する通信設備に通信が集中して機器が過負荷となり、サービス提供に支障をきたすおそれ

があった。このISPでは、サービス提供への影響を防止するため、契約者を収容する通信設備において契約者に割り当てたIPアドレスを送信元とする通信のみを許可しそれ以外を破棄する設定を行った。同時に、当該 ISP が契約者に割り当てたIPアドレスを送信元とする通信が、他のISPとの相互接続点から流入するのを遮断する設定を行った。

(3) 壊れたパケット等の破棄

(コ) 明らかにIPパケットの規格を逸脱したり、通常発出してはならない通信方式など、中継する事業者設備に異常をきたす通信がなされた場合、そのような通信であるかを機械的に判断し、自動破棄してよいか。

【考え方】

① 壊れたパケット等の送信により、事業者の設備等に支障を生じるなど業務の適正な遂行に支障が生じるおそれがある場合において、これらのパケットを自動破棄することは、正当業務行為により違法性が阻却される。

② また、壊れたパケット等を破棄せずそのまま送信することによりエンドユーザを含む下位レベルの設備が侵害されるおそれがある場合には、当該パケットを一時的に自動破棄することは、通常、正当防衛又は緊急避難として違法性が阻却されると解される。

【①の事例】

・ IPヘッダのみのIPパケット、実際のパケット長と length field の値が異なるパケット、送信元IPアドレス=送信先IPアドレスのパケットなどの流入が観測され、ルータに負荷を与えサービス提供に支障をきたすおそれがあったため、これらのパケットを破棄する設定を行った。

(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

(サ) ソフトウェアの脆弱性などを悪用することで人による操作を経ることなくコンピュータに感染するマルウェア等、当該通信を媒介することで、近日中にトラヒックの莫大な増加が発生する蓋然性が極めて高い通信について、通信設備への影響を予防する観点から、遮断してよいか。

【考え方】

マルウェア等の通信を遮断する場合、当該通信がマルウェア等の通信であるかを把握した上、これに合致する通信を遮断することになると考えられるが、個別の通信についてその特性等を把握することは、通信の秘密の侵害(知得)に当たりうる。また、把握した特性等に基づき、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、当該通信を媒介することにより、トラヒックの莫大な増加により事業者設備への支障又は受信者設備等への侵害であっても事業者設備への支障が生じる蓋然性が高い場合は、それを防止する必要性があると考えられ、マルウェア等トラヒック増加の原因となるような通信のみを遮断するなど、必要な範囲で相当な方法により行われる対応については、正当業務行為に当たると解される。

(5) 受信側の設備等に意図しない影響を及ぼす通信等

(シ) マルウェアなど、受信者の設備等に意図しない影響を及ぼすデータを送付する通信の受信者や、ポートスキャンなど、攻撃の準備行為と考えられる通信の受信者から、電気通信事業者に対して当該通信を行う者に警告を発するよう要請があった場合、受信者から提供された受信ログと、契約者の接続ログを突合し、当該通信を行っている契約者を特定した上で、当該通信を止めるよう連絡をするなど何らかの措置を採ってよいか。

【考え方】

受信側の設備等に意図しない影響等を及ぼす特定の通信を行った契約者を特定するため、自社の契約者の接続ログを解析し、当該通信を行った契約者に連絡をすることは通信の秘密の侵害(窃用等)に当たりうる。

これについて、受信者の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、当該通信を行っている契約者に連絡を取ることは、通常、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。

(6) 網内トラヒックの現状把握

(ス) 現在、電話網におけるネットワークオペレーションセンターによる流量把握をIP網でも実施している。電話網であれば、(通信内容を含まない)共通信号線内の信号から、流量や流束の方向が把握可能であるが、IP通信の場合、パケットヘッダ部の統計データを取得する以外に手段がない。設備増強の必要性の判断や通信設備の障害発生時に障害の原因究明の円滑化などを目的として、網内トラヒックの現状把握をすべく統計データを取得してよいか。

【考え方】

「自社契約者から特定の ISP 別へのトラヒック及びその通信種別情報」及び「特定の ISP 別から自社契約者へのトラヒック及びその通信種別情報」を収集することは、個別の通信に係る送信元及び送信先IPアドレスを検知して利用しているため、通信の秘密の侵害(窃用等)に当たりうる。

ただし、設備増強の必要性の判断その他の自社業務を適正に遂行する等の業務目的のために、必要な範囲でそれらの情報を収集することは、正当業務行為として違法性が阻却される。

【事例】

・ ある ISP では、網の設備増強等の見積りのために、ルータにおいて、流入インタフェース、通信総量、パケット総量、パケットサイズ、TCP および UDP のポートの分布、IPオプションの有無などの通信に係る情報を取得し、統計処理したデータを利用している。また、網の構成や、回線容量の計画のために、送信元送信先IPアドレスの分布、通信の方向、県間トラヒックに関する情報を取得し、統計処理したデータを利用している。

（セ） 通信設備の中には、DNSサーバのように、負荷が急速に高まった際に、当該負荷の発生原因を把握するためには、どのドメイン名に関する又はどのIPアドレスからの検索が多いのかまでを含めた履歴データを平時より取得し、現時点での傾向と照らし合わせなければならないものも存在する。このような設備について、過負荷により通信の媒介に影響が及んだ際の復旧を可能とすることを目的として、平時より履歴データを取得してよいか。

【考え方】

DNSサーバの検索履歴データは、個別の通信についてその宛先や送信元等に関する情報を取得して作成されるものであるところ、これらを取得することは、通信の秘密の侵害（知得等）に当たりうる。

もっとも、DNSサーバの過負荷により通信の媒介に影響が及んだ際の復旧を可能とすることを目的として、これに必要最小限の範囲内のデータを取得しておくことは、正当業務行為として違法性が阻却されると解される。

（ソ） 電気通信事業者が設備増強等の判断のために取得している通信ログデータの分析を容易化するため、これら通信ログデータを統計処理したものについて、平時より事業者間でリアルタイムに共有してよいか。

【考え方】

設備増強の必要性等の判断その他の自社業務を適正に遂行する等の目的のために取得した通信ログデータを、他の目的に利用することは、通信の秘密の侵害（窃用）に当たりうる。

もっとも、個別の通信との関連性がないなど、通信の秘密の保護が及ばない形にデータが統計処理されている場合には、これを事業者間で共有しても問題はない。

(7) サイバー攻撃等への共同対処

（タ） 多数の攻撃者による一斉攻撃については受信者と直接契約している電気通信事業者による対応のみでは遮断が困難と推測されるが、①当該通信の経路を運用する電気通信事業者に対し当該攻撃通信の特性にかかる情報を提供し、②情報提供を受けた電気通信事業者において当該特性に合致する通信を遮断してよいか。

【考え方】

特定の発信者（発信端末のIPアドレス）発の特定のデータ列も通信の秘密に当たる。この点、

受信側 ISP 等において、受信者から提供された情報、受信者の同意を得て収集した情報等をもとに、「当該発信者（IPアドレス）から攻撃通信が発信されている」と判断した情報を、発信側 ISP 等に提供することは、受信者の同意に基づく行為として通信の秘密の侵害とはならない。そして、受信側 ISP 等の判断を受け取った送信側 ISP 等において、「当該発信者（IPアドレス）から攻撃通信が発信されている」と判断して、当該発信者への対応（警告、利用停止等）を行うことは、不正な攻撃通信による受信者の端末等の設備に対す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。

また、当該通信に係る ISP 等の設備等に影響が生じ、通信業務の遂行に支障が生じるおそれが認められる状況であれば、当該通信への遮断などを一時的に行うことは設備等への影響を防止するに必要な範囲で相当な方法により行われる場合には、正当防衛又は緊急避難として違法性が阻却される。

なお、インターネットにおいては通常複数の事業者が介在するので、ここでいう受信側 ISP 等、発信側 ISP 等とは当該大量通信に係る事業者すべてを意味する。

（チ） 電気通信事業者が設備増強等の判断のために業務上正当に取得している通信ログデータを検証している際に「外形上明らかに異常な通信」の存在に気付いた場合、当該異常通信の原因分析（①自社設備の問題（設定誤りなど）、②新たな通信利用形態の出現、③攻撃によるもの等が考えられる）のため、受信者からの被害申告がない状況であっても、当該通信の経路となっている電気通信事業者間で通信ログデータの分析結果を交換することは可能か。また、当該分析結果により、当該通信が攻撃によるものと判明した場合に当該通信の遮断をしてよいか。

【考え方】

外形上明らかに異常な通信を認知した場合に、当該通信によるサービス提供への影響を考慮するための原因分析に必要な範囲で、相当な方法により通信ログデータを分析すること（利用すること）は正当業務行為に当たると考えられる。この点、個別の事業者における分析結果だけでは「外形上明らかに異常な通信」の原因が判明せず、「サイバー攻撃等により、自社設備等に支障が生じるなどして、自社業務の遂行に支障が生じるおそれ」が認められる状況であれば、原因の特定に必要な範囲で、当該通信の経路となっている電気通信事業者間で通信ログデータの分析結果を交換することも正当業務行為として認められると考える。ただし、交換する通信ログデータの分析結果については、できる限り個別の通信が特定できない形で交換されることが望ましい。また、当該通信に係る事業者の設備等に影響が生じ、通信業務の遂行に支障が生じるおそれが認められる状況であれば、自社設備等もしくは分析結果を交換した事業者の設備等において当該通信への遮断などを一時的に行うことは設備等への影響を防止するに必要な範囲で相当な方法により行われる場合には、正当防衛又は緊急避難として違法性が阻却される。

【事例】

あるISPにおいて、網内の複数のルータのCPU利用率が異常に高くなる現象が観測された。この異常の原因究明のため、ISP において事業の設備増強見積もり等のために常時取得している統計データから、通信総量、方向、パケットサイズの分布、プロトコル分布、通信の送信元の分布について調査を行った。この結果、当該ルータに非常に小さなIPパケットが大量に流入しており、その転送処理のために過負荷となったことが判明した。このIPパケットは、インターネット相互接続点を通じて接続しているとなりのISPから流入していたため、そのISPに対して通信の概要情報を開示し、原因究明の補助を依頼した。

2 迷惑メール等

(1) 送信元詐称メールの受信拒否

(ツ) ヘッダ情報の矛盾などに基づき、当該メールの受信をメールサーバにて拒否してよいか

【考え方】

受信側 ISP が、ヘッダ情報の矛盾などに基づき、当該メールの受信をメールサーバにて拒否することは、受信回線の契約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とならない。

受信回線の契約者からの個別の同意がない場合でも、送信元詐称メールが大量送信されており、電子メール送受信上の支障が生じるおそれがある場合には、その業務の支障のおそれを防止するために必要な範囲で、全契約者を対象に恒常的な対策を行うことも正当業務行為に当たると解される。

ただし、ここでいう「送信元詐称メールが大量送信されており、電子メール送受信上の支障が生じるおそれがある場合」の判断については、恣意的なものとならないよう留意しなければならない。

【事例】

・ あるISPの迷惑メールフィルタリングサービスでは、契約者の選択により、メールサーバのヘッダ情報に不整合のあるメールは受信拒否の設定を行うことができる。

(2) Black Listとの突合に基づくユーザへの注意喚起

(テ) メールアドレスやドメイン名、発出元メールサーバのIPアドレスなどが、Black List と合致したメールについて、メールサーバからユーザへの自動配信の留保や、ヘッダに注意喚起情報を付加してよいか。

(ト) また、Black Listについて、電気通信事業者間で共有してよいか。

【考え方】

Black List に記載されたメールアドレス等との突合の結果、迷惑メールに該当すると判断された電子メールについて、メールサーバから受信回線の契約者への自動配信の留保をしたり、ヘッダに注意喚起情報を付加したりすることは、受信回線の契約者から個別の同意を取得して行う場合には通信の秘密との関係では問題ない。

また、個別のメール送信に係らないBlack Listの情報は、通信の秘密に属する情報ではなく、本ガイドラインの検討範囲ではないが、プライバシー保護等別の観点から慎重な検討が求め

られることに留意する必要がある。

【事例】

・ ある ISP の迷惑メールフィルタリングサービスでは、契約者の選択により、外部の Black List を参照し、Black List に掲載されているIPアドレスからのメールを受信拒否する設定と、Black List に掲載されていたことを示す拡張ヘッダを当該メールのヘッダに付与する設定の、二つを選択することができる。

(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

（ナ） 現状提供されている迷惑メールフィルタリングサービスにおいては、利用者毎にフィルタ定義を別途用意しているが、これを多数の利用者で共有化し、検索を一括実施してよいか。（なおウィルス対策サービスなどでは、フィルタは全利用者共通であることが多い。）

【考え方】

迷惑メールフィルタの定義については、受信側 ISP において利用者毎に設定されているが、これを多数の利用者で共有化し一括検索できるようにすることは、当該フィルタを設定している契約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とならない。

（4） SMTP 認証の情報を悪用した迷惑メールへの対処

（ニ） SMTP 認証の ID・パスワードが不正に利用され、大量の迷惑メールが送付されている場合に、メールサーバに滞留したメールに係る SMTP 認証のログ（発信元 IP アドレス、タイムスタンプ、メールアドレス）を解析し、不正利用の蓋然性が高い ID からの SMTP 認証を一時停止し、当該 ID の正規の契約者に連絡を取り、パスワードの変更等を依頼してよいか。

（ヌ） 大量の SMTP 認証の失敗の発生は、SMTP 認証の ID・パスワードの不正取得が行われている蓋然性が高いことから、このような場合に、SMTP 認証に係るログ（発信元 IP アドレス、タイムスタンプ、認証回数、認証間隔）を解析し、特定の IP アドレスから SMTP 認証の失敗が短期間に大量に発生している等アカウントハッキングの蓋然性が高いものについては、当該攻撃期間中、当該 IPアドレスからの SMTP 認証を一時停止してよいか。[8]

[8] なお、インターネット接続や、メール送信等の利用者間の通信を媒介するサービスとは異なり、会員向け情報提供サイト等、ISP自身が通信の一方当事者となる場合、ISPが該当利用者からのID認証に係る通信を必要かつ相当な範囲で利用することは、通信の秘密との関係では問題ない。一方、ISP において、インターネット接続に係る利用者からの認証に係る通信を利用することについては、第6条1（1）（ヘ）を参照されたい。

（例）

・ ISP の会員向け情報提供サイト等のアカウント情報を取得するために、ブルートフォースやリスト型攻撃で、認証サーバに対し、正規の利用者以外と思われる者から大量のアクセスがある場合、認証に関するログを分析することにより、認証 ID・パスワードの不正利用の蓋然性が高いものについて、当該 ID からの認証を一時停止する。

【考え方】

攻撃者がSMTP認証のID・パスワードを不正に利用して迷惑メールを送付し、サイバー攻撃等が発生している場合において、当該ISPが、メールサーバに滞留したメールに係るSMTP認証の発信元IPアドレス、タイムスタンプ及びメールアドレスを分析し、SMTP認証のID・パスワードの不正利用の蓋然性が高いIDからのSMTP認証を一時停止する又は当該IDの正規の契約者に連絡を取り、パスワードの変更等を依頼することは、通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、これらの行為は、正規の利用者以外の者が不正に電気通信役務を享受することを防止するとともに、SMTP認証のIDを不正に利用した迷惑メールの大量送信によって、SMTPサーバの負荷が急増することにより生じるメールの遅延等を防止し、もって、電気通信役務の安定的運用を図るために行うものであり、侵害される通信の秘密もSMTP認証の発信元IPアドレス、タイムスタンプ、メールアドレス及びSMTP認証のIDのみと相当な限度で行われることから、正当業務行為に当たり違法性が阻却されると考えられる。

また、SMTP認証のID・パスワードの不正取得から生じ得るサイバー攻撃等の発生を防ぐために、大量のSMTP認証の失敗が発生した場合において、SMTP認証に係るログから、発信元IPアドレス、タイムスタンプ、認証回数、認証間隔を解析し、特定のIPアドレスからSMTP認証の失敗が短期間に大量に発生している等、アカウントの不正取得を試みている蓋然性が高いIPアドレスからのSMTP認証を遮断又は制限することは、通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、当該行為は、正規の利用者以外の者が不正に電気通信役務を享受することを防止するとともに、SMTP認証のID・パスワードの不正取得から生じ得るサイバー攻撃等の被害を防止し、もって正規の契約者に対する安定的な電気通信役務の提供を確保するために行うものであり、侵害される通信の秘密も、認証の発信元IPアドレス、タイムスタンプ、認証回数、認証間隔のみと相当な限度で行われることから、正当業務行為に当たり違法性が阻却されると考えられる※。

※詳細な検討は「第一次とりまとめ」 P28 参照

【事例】

・ SMTP認証に必要なID・パスワードをあらかじめ窃取した攻撃者が、当該ID・パスワードを悪用して大量の迷惑メールの送信を行ったため、当該認証に係るSMTPサーバを保有するISPにおいて送信メールが滞留し、電子メールの遅配が発生した。そのため当該ISPにおいて、メールサーバに滞留したメールに係る、SMTP認証の発信元IPアドレス、タイムスタンプ、メールアドレス及びSMTP認証のIDを分析し、一のSMTP認証のIDを用いて送信されているにもかかわらず当該認証の発信元IPアドレスが瞬時に別の国や地域に移動している等SMTP認証

・ ISPの会員向け情報提供サイト等のアカウント認証に関わるログを分析し、特定のIPアドレスから認証の失敗が短期間に大量に発生している等アカウントハッキングの蓋然性が高いものについて、当該攻撃期間中、当該IPアドレスからの認証を一時的に停止する。

のID・パスワードの不正利用の蓋然性が高いものが確認できたため、当該IDからのSMTP認証を一時停止するとともに、そのID・パスワードの正規の契約者に対し、個別に連絡を取り、パスワードの変更を依頼した。

・ ISPにおいて大量のSMTP認証の失敗が発生し、SMTP認証のID・パスワードの不正取得の可能性が考えられたため、SMTP 認証に係るログから、認証の発信元 IP アドレス、タイムスタンプ、認証回数、認証間隔を分析した。その結果、特定のIPアドレスからSMTP認証の失敗が短期間に大量に発生している等アカウントの不正取得である蓋然性が高いことが確認できたため、当該IPアドレスからのSMTP認証を一時停止した。

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

（ネ） 攻撃の受信者からの申告に基づき契約者の保有する端末が「踏み台」として悪用されていることが判明した場合、当該契約者に対し警告することができるか。

（ノ） また、当該契約者に対して何度警告しても改善されない場合には「要注意契約者」として当該契約者に関する情報を電気通信事業者間で共有してよいか。

【考え方】

攻撃者が第三者の端末を介してサイバー攻撃等を行っていることを、第三者が加入しているISPが認識した場合において、当該ISPが、通信ログを確認して踏み台端末の契約者を特定し、当該契約者に対して警告を発すること、及び必要な範囲で利用停止することは、通常、正当防衛又は緊急避難に当たり違法性が阻却される。その際、緊急に利用停止を行う必要性が認められる場合には、利用停止を行った後に通知を行うことも可能である。（約款に規定している場合はもちろん、規定していない場合でも問題はないと考える。）

ただし、当該契約者に関する情報を電気通信事業者間で情報共有することについては、交換の目的、必要性、交換する情報の範囲、交換した情報の利用方法等を踏まえて、通信の秘密の保護との関係を整理する必要があり、一概に判断することは困難である。

【事例】

・ あるISPでは、ある契約者が大量の通信を第三者に対して発生させているという申告を受けた。このISPでは、事業の設備増強見積もり等のために常時取得している統計データから、当該契約者の通信状況を調査し、他の利用者の通信を侵害するほどの大量の通信が発生していることを確認した。このため、当該契約者に注意喚起を行ったが、契約者による改善が望めなかったため、当座の措置として当該契約者による通信を停止した。

（ハ） 第三者から提供されたマルウェア感染端末情報（IP アドレス及びタイムスタンプ）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を特定した上で、当該契約者に対して注意喚起を行うことができるか。

【考え方】

マルウェアに感染し、「踏み台」として悪用される又は情報が漏えいする等の危険がある端末に

関する情報（IP アドレス及びタイムスタンプ）を第三者から ISP に提供された場合において、当該 ISP が当該情報に係る接続ログを解析して感染端末の契約者を特定し、当該契約者に対して注意喚起を行うことは、通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、当該行為については、マルウェアの感染による当該端末が正常かつ安全に機能することに対する現在の危難を避けるための緊急避難として、違法性が阻却される※。

※詳細な検討は「第一次とりまとめ」 P22 参照

【事例】

- 第三者において、テイクダウンされた C&C サーバに蓄積されている通信履歴の情報が分析された結果、ある端末が当該 C&C サーバと通信を行い、サイバー攻撃等の「踏み台」となっているほか、当該端末に保存されている情報の漏えい等の危険があることが確認できた。このため第三者は当該 C&C サーバとの通信を行っている端末の IP アドレス及びタイムスタンプについて ISP に情報提供を行い、当該 ISP において、提供のあった IP アドレス及びタイムスタンプの情報を基に、タイムスタンプにおいて示された時刻において当該 IP アドレスをどの利用者に割り当てたか確認して、該当利用者を割り出し、メール等によって個別に注意喚起を行った。
- マルウェアの感染行動を検知するハニーポットを保有しており、当該ハニーポットにおいて検知した情報からマルウェアに感染している端末が見つかったとして、当該ハニーポットの保有者から ISP に対して、当該端末の IP アドレス及びタイムスタンプの提供があった。このため、当該 ISP において、提供のあった IP アドレス及びタイムスタンプの情報を基に、タイムスタンプにおいて示された時刻において当該 IP アドレスをどの契約者に割り当てたか確認して、該当契約者を割り出し、メール等によって個別に注意喚起を行った。

（ヒ） 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に関して、ネットワーク上に存在するこれらの脆弱性を有する機器を調査し、調査により判明した機器の情報（IP アドレス及びタイムスタンプ）と契約者の接続ログを突合し、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た上で、当該契約者に対して注意喚起を行うことができるか。

【考え方】

リフレクション攻撃やインターネットの不正利用等の危険があるブロードバンドルータに関する情報（IP アドレス及びタイムスタンプ）を調査し、ISP において契約者の接続ログを解析して感染端末の契約者を特定し、当該契約者に対して注意喚起を行うことは、通信の秘密の侵害（窃用等）に当たりうる。しかしながら、当該行為は、リフレクション攻撃によるインターネットアクセスやメール送信の遅延等発生を防止すること、又は、正規の利用者以外の者が正規の利用者になりすまし、不正に電気通信役務を享受することを防止することで、電気通信役務の安定的提供等を図るために行われるものであり、通信の秘密の侵害の程度についても IP アドレス及びタイムスタンプに限られること、また、当該 IP アドレス及びタイムスタンプの情報も、契約者に注意喚起を行う限りにおいて利用されるものであるから、正当業務行為として違法性が阻却される。

なお、第三者（事業者団体等）において脆弱性のあるブロードバンドルータを調査し、その調査

結果を ISP に提供する行為については、調査を行った者は調査に係る通信を送受信した一方当事者であるから、これらを他の ISP に提供することは、通信の秘密の侵害にあたらないと考えられる※。

※調査自体に関する不正アクセス禁止法との関係の整理及び通信の秘密に関する詳細な検討は「第二次とりまとめ」 P16 参照

【事例】

・ 事業者において、リフレクション攻撃に悪用されうる脆弱性や 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について調査を行い、当該ブロードバンドルータに関する情報（IP アドレス及びタイムスタンプ）を、当該 IP アドレスを管理している ISP に提供した。各 ISP において、提供のあった IP アドレス及びタイムスタンプの情報を基に、タイムスタンプにおいて示された時刻において当該 IP アドレスをどの契約者に割り当てたか確認して、該当契約者を割り出し、メール等によって個別に注意喚起を行い、ファームウェアの更新等を依頼した。

(2) レピュテーションDBの活用

(ｱ) 「レピュテーションDB（利用者等の申告に基づき、悪意の行為を行うドメインやIPアドレスの「悪評」を蓄積するデータベース。これにより、当該ドメインやIPアドレスの「悪さ度合い」を定量的に評価可能とする。）」を活用し、通信遮断や契約者への注意喚起を行ってよいか。

【考え方】

① いわゆるレピュテーションDB（利用者等の申告に基づき、悪意の行為を行うドメインやIPアドレスの「悪評」を蓄積するデータベース）をもって、ドメインやIPアドレスの「悪さ度合い」を定量的に評価可能とし、その評価に基づいて通信の遮断や利用者への注意喚起を行うことは、受信回線の契約者の個別の同意を取得して行う場合には通信の秘密の侵害とならない。

② また、個別の同意を取得していなくても、レピュテーションDBに基づいてマルウェア配布サイトへのアクセスに対する注意喚起を行う場合であって、その際、通信の秘密に当たる情報のうち必要最小限度の事項（アクセス先 IP アドレス又は URL）のみを機械的・自動的に検知した上で該当するアクセスに対して注意喚起画面等を表示させ、当該データベースが一定の正当性（目的の正当性、正確性、客観性等）を有するものである場合には、契約約款に基づく事前の包括同意でも、次の条件の下においては、当該注意喚起を行うための通信の秘密に属する事項の利用についての有効な同意ということができ、通信の秘密の侵害とならないと解される※。

・契約者が、契約約款に同意した後も、随時、同意内容を変更できる契約内容であって、マルウェア配布サイトへのアクセスに対する注意喚起における同意内容の変更の有無にかかわらず、その他の提供条件が同一である。

・契約約款の内容や随時同意内容を変更できることについて相応の周知が図られている。
・注意喚起画面に、注意喚起の説明に加え、随時同意内容を変更できること等の説明がされている。

※詳細な検討は「第一次とりまとめ」 P19 参照

③　同様に、個別の同意を取得していない場合として、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 に基づいて遮断する行為について、通信の秘密に当たる情報のうち必要最小限度の事項（名前解決要求に係る FQDN）のみを自社 DNS サーバにおいて機械的・自動的に検知した上で、データベースにある FQDN と合致する名前解決要求を遮断する行為は、当該データベースが一定の正当性（目的の正当性、正確性、客観性等）を有するものである場合には、契約約款に基づく事前の包括同意であっても、次の条件の下においては、当該遮断を行うための通信の秘密に属する事項の利用についての有効な同意ということができ、通信の秘密の侵害とならないと解される※。

・利用者が、契約約款に同意した後も、随時、同意内容を変更できる契約内容であって、C&C サーバ等との通信の遮断における同意内容の変更の有無にかかわらず、その他の提供条件が同一である。
・契約約款の内容や随時同意内容を変更できることについて相応の周知が図られている。

なお、本対策について、マルウェア感染端末と C&C サーバ等との通信については、ブラウザ経由の注意喚起画面を表示することができないまま、利用者の望まない通信が自動的に行われるものであることに着目して遮断という手法をとるものであり、違法・有害なコンテンツ等へのアクセスに対する遮断一般を認めるものではないことに留意する必要がある。

※詳細な検討は「第二次とりまとめ」P12 参照

【①事例】

ある ISP の接続サービスでは、契約者の選択により、迷惑メールの Black List に掲載されているIPアドレスからの通信を遮断することができる。

【②の事例】

ACTIVE[9]におけるマルウェア感染防止の取り組みとして、ある ISP においては、契約約款に基づく事前の包括同意に基づき、マルウェア配布サイトへのアクセスに対して注意喚起を行っている。

【③の事例】

ある ISP において、マルウェア感染による利用者への被害を防止するため、契約約款に基づく事前の包括同意に基づき、C&C サーバ等へのアクセスの遮断を行うとともに、遮断を行った契約者に対して、メールにより C&C サーバ等との通信の遮断を行ったことや端末のマルウェア駆除が必要であること、遮断を望まない場合は変更が可能であること等を周知した。

[9] 平成 25 年 11 月から総務省と ISP 等が連携して実施している、マルウェア感染防止・駆除プロジェクト

第 6 条　電気通信役務の不正享受について

1　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

（ヘ）　PPPoE 認証の ID・パスワードが悪用され、第三者にインターネットが不正に利用されているおそれがある場合に、認証サーバにおける PPPoE 認証に係るログ（PPPoE 認証の ID、当該 ID に対して割り当てた IP アドレス、タイムスタンプ）を解析し、不正利用の蓋然性の高い ID に係るインターネット接続を切断、当該 ID からの認証を一時停止するとともに、当該 ID の正規の契約者に連絡を取り、パスワードの変更等を依頼して良いか。

【考え方】

第三者が他人の PPPoE 認証の ID・パスワードを悪用してインターネットを不正に利用しているおそれがある場合において、当該 ISP が、認証サーバにおける PPPoE 認証の ID、当該 ID に対して割り当てた IP アドレス、タイムスタンプを分析し、PPPoE 認証の ID の不正利用の蓋然性の高い ID に係るインターネット接続を切断し、当該 ID からの認証を一時停止するとともに、当該 ID の正規の契約者に連絡を取り、パスワードの変更等を依頼することは、通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、これらの行為は、正規の利用者に対して電気通信役務を円滑に提供するとともに、通信事業を維持・継続するため、正規の利用者以外の者が正規の利用者になりすまし、不正に電気通信役務を享受することを防止することにより、電気通信役務の円滑な提供を確保するために行うものであり、侵害される通信の秘密も PPPoE 認証の ID、当該 ID に割り当てた IP アドレス、タイムスタンプのみと相当な限度で行われることから、正当業務行為に当たり違法性が阻却されると考えられる※。

※詳細な検討は「第二次とりまとめ」P14 参照

【事例】

・　PPPoE 認証に必要な ID・パスワードをあらかじめ窃取した第三者が、当該 ID・パスワードを悪用して不正にインターネットを利用し、サイバー攻撃を行った際、当該認証行為が幾度となく行われたため、ISP の認証サーバにおいて異常が検出された。そのため、当該 ISP において、認証サーバに記録された PPPoE 認証の ID、当該 ID に対して割り当てた IP アドレス、タイムスタンプを分析し、同一の ID に対して通常の利用では想定されないような短時間で大量の認証要求が行われている、又は当該認証に対して割り当てている IP アドレスが瞬時に別の地域に移動している等、PPPoE 認証の ID の不正利用の蓋然性が高いものが確認できたため、当該 ID に係るインターネット接続を切断し、当該 ID からの認証を一時停止するとともに、その ID の正規の契約者に対し、個別に連絡を取り、パスワードの変更を依頼した。

(2) IP 電話等の電話サービスの不正利用への対処

（ホ） 第三者により IP 電話等の電話サービスが不正に利用され、国際電話料金等が平時と比較して急増した場合に、国際電話サービス提供事業者において、通信先の相手国（国番号）、発信元電話番号や発信元 IP アドレス（IP 電話の場合に限る。以下同じ。）を分析し、正規の利用者以外の者が利用していた蓋然性が高い場合に、その利用に係る回線からの国際電話の利用を休止して良いか。

【考え方】

IP 電話等の電話サービスが第三者に不正に利用され、契約者に多額の国際電話料金の請求が行われることを防ぐために、国際電話サービス提供事業者において国際電話料金等を一定の頻度で検知した上で、平時と比較して急増する等不正利用が疑われる場合において、通信先の相手国（国番号）、発信元電話番号や発信元 IP アドレスを分析し、正規の利用者以外の者が利用していた蓋然性が高い場合に、当該通信に係る回線の契約者を割り出して連絡を取ること、また緊急性が高いと認められる場合に当該回線に係る国際発信を休止すること等は、通信の秘密の侵害（窃用等）に当たりうる。

しかしながら、当該行為は、契約に基づく適正な課金・料金請求を行うことにより正規の利用者に対して電気通信役務を提供するとともに、通信事業を維持・継続するため、正規の利用者以外の者が正規の利用者になりすまして不正に電気通信役務を享受することを防止することにより、電気通信役務の円滑な提供を確保するために行うものであり、侵害される通信の秘密も通信先の相手国（国番号）、発信元電話番号や発信元IPアドレス等上記事項のみであって、また、契約者の同意を得ずに不正利用に係る契約者回線からの国際電話の利用を休止する措置についても、同意の取得を原則とし、契約者と連絡が取れない等緊急性が高いと認められる場合にのみ行う限りにおいては、正当業務行為に当たり違法性が阻却されると考えられる※。

※詳細な検討は「第三者による IP 電話等の不正利用への対策について」P4参照
http://www.soumu.go.jp/main_content/000367498.pdf

【事例】

・ IP 電話等の電話サービスが第三者に不正に利用され、契約者に多額の国際電話料金の請求が行われる事態が頻発していることを踏まえ、ある国際電話サービス提供事業者において、契約者の国際電話料金等を一定の頻度で検知した上で、平時と比較して急増した際に、通信先の相手国（国番号）、発信元電話番号や発信元 IP アドレスを分析した結果、正規の利用者以外の者が利用していた蓋然性が高いことが判明した。これを踏まえ、事業者において当該通信に係る回線の契約者に国際電話の利用休止を促すべく、料金高騰の旨を周知しようとしたところ、当該契約者と連絡がつかなかったため、事業者の判断により、当該契約者に係る国際電話の利用休止を行うとともに、当該契約者に対しては連絡がつき次第、利用休止を行ったことについて周知を行った。

（マ） 第三者により IP 電話等の電話サービスが不正に利用され、国際電話料金等が平時と比較して急増した場合に、国際電話サービス提供事業者において、通信先の相手国（国番号）、当該発信に係る SIP 認証の ID 及び認証の要求元 IP アドレスを分析し、正規の利用者以外の者が利用していた蓋然性が高い場合に、当該 IP アドレスからの SIP 認証を一時停止して良いか。

【考え方】

IP 電話等の電話サービスが第三者に不正に利用され、契約者に多額の国際電話料金の請求が行われることを防ぐために、国際電話サービス提供事業者において、国際電話料金等を一定の頻度で検知した上で、平時と比較して急増する等不正利用が疑われる場合において、通信先の相手国（国番号）、当該発信に係る SIP 認証の ID 及び認証の要求元 IP アドレスを分析し、SIP 認証の ID の不正利用の蓋然性が高い場合に、当該 IP アドレスからの SIP 認証を一時停止することは、通信の秘密の侵害（窃用等）に該当する可能性がある。

しかしながら、当該行為は、契約に基づく適正な課金・料金請求を行うことにより正規の利用者に対して電気通信役務を提供するとともに、通信事業を維持・継続するため、正規の利用者以外の者が正規の利用者になりすまして不正に電気通信役務を享受することを防止することにより、電気通信役務の円滑な提供を確保するために行うものであり、侵害される通信の秘密も通信先の相手国（国番号）、当該発信に係る SIP 認証の ID 及び認証の要求元 IP アドレス等上記事項のみであるから、分析の結果を本件対策以外の用途で利用しない場合においては、正当業務行為として違法性が阻却されると考えられる※。

※詳細な検討は「第三者による IP 電話等の不正利用への対策について」P5参照

【事例】

・ IP 電話の利用に必要な SIP 認証に係る SIP サーバを保有する国際電話サービス提供事業者において、契約者の国際電話料金等を一定の頻度で検知していたところ、当該 SIP 認証に係る契約者の国際電話料金等が急増した。そのため当該事業者において当該発信に係る通信先の相手国（国番号）、SIP 認証の ID 及び認証の要求元 IP アドレスを分析したところ、一の SIP 認証の ID を用いて発信されているにも関わらず、当該認証の要求元 IP アドレスが平時の利用とは異なるものである等、SIP 認証の ID の不正利用の蓋然性が高いものが確認できたため、当該 IP アドレスからの SIP 認証を一時停止した。

（ミ） 第三者により IP 電話等の電話サービスが不正に利用され、国際電話料金等が平時と比較して急増した場合であって、その他の不正利用対策では対応が困難な場合に、国際電話サービス提供事業者において、専ら不正利用に用いられていると認められる特定国宛ての発信一般を、不正利用がなされている期間中に限り、一時的に規制して良いか。

【考え方】

IP 電話等の電話サービスが第三者に不正に利用され、契約者に多額の国際電話料金の請求が行われることを防ぐために、国際電話サービス提供事業者において、国際電話料金等を一定の頻度で検知した上で、平時と比較して急増する等不正利用が疑われる場合であって、

その他の不正利用対策では対応困難な場合に、通信先の相手国（国番号）、発信元電話番号や発信元 IP アドレスを分析し、専ら不正利用に用いられていると認められる特定国を把握した上で、当該特定国宛ての通信を確認し、一時的に規制することは、通信の秘密の侵害（窃用等）に該当する可能性がある。

しかしながら、当該行為は、契約に基づく適正な課金・料金請求を行うことにより正規の利用者に対して電気通信役務を提供するとともに、通信事業を維持・継続するため、正規の利用者以外の者が正規の利用者になりすまして不正に電気通信役務を享受することを防止することにより、電気通信役務の円滑な提供を確保するために行うものであり、侵害される通信の秘密も通信先の相手国（国番号）、発信元電話番号や発信元IPアドレス等上記事項のみであって、その実施についても、当該特定国宛ての通常の通信量、当該特定国と我が国の交易関係、当該時点において緊急の通信が行われる可能性等を勘案し、専ら不正利用に用いられていると認められる場合に限られ、不正な電気通信役務の享受を防止する他の有効な手段が認められないときには、当該特定国宛ての発信一般を一時的に規制することも正当業務行為として違法性が阻却されると考えられる※。

※詳細な検討は「第三者による IP 電話等の不正利用への対策について」P7参照

【事例】

・ IP 電話等の電話サービスが第三者に不正に利用され、相当多数の国際通話が同時多発的に発信されている状況にあり、個別の発信規制等その他の対策では不正利用による被害の抑止に十分な効果が得られない場合において、国際電話サービス提供事業者において、通信の相手国（国番号）、発信元電話番号や発信元 IP アドレスを分析し、当該特定国宛ての通信について、当該特定国宛ての通常の通信量、当該特定国と我が国の交易関係、当該時点において緊急の通信が行われる可能性等を勘案し、専ら不正利用に用いられていることが認められたため、不正利用が認められている期間中に限り、当該特定国宛ての通信を一時的に規制した。