

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

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

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なう対応が、主に電気通信事業法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」を開催し検討した。その結果を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」として制定し、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、当ガイドラインを検証するべく、上記4団体はメンバー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、検討をおこなった結果、本ガイドラインを修正したものを第2版として制定した。

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」が公表されたことから、今般それを踏まえた追加修正を行い第3版とした。

目次

第1章 総則	1
第1条 目的.....	5
第2条 総論.....	5
1 通信の秘密.....	5
2 留意事項.....	6
第3条 定義.....	6
1 大量通信等.....	6
2 攻撃通信.....	7
3 通信.....	7
第4条 見直し.....	9
第2章 各論	10
第5条 大量通信等について.....	10

改版履歴

版数 作成年月

第1版 2007年(平成19年)5月

第2版 2011年(平成23年)3月

第3版 2014年(平成26年)7月

改版理由

新規作成

章、条番号の付加、3,4条追加、2章内容見直し等

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「大量通信等」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。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、このような大量通信等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、大量通信等に係る通信を識別し、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大量通信等への対処が、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大量通信等への対処の参考に資するものである。なお、当然のことながら大量通信等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らない。実際の対処において本ガイドラインに書かれていないものについての対処を否定するものではない。その場合の判断は個別に行な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が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）

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 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、その刑を減輕し、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。

⁴ 帯域制御のほか、OP25B,IP25B も同様

- (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」に分けて基本的な考え方を記述している。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について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。
- (2)各論は、大量通信等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、近年社会問題化している有害情報・フィッシングから利用者を保護する対応等と通信の秘密については別途検討が必要である。
- ただし、以下で述べる各論の整理は、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、大量通信等への対応を実践に移すに当たっては、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。
- 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」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、大量通信等への対応に必要な範囲にとどめるべきこと等に留意する必要がある。
- なお、以下で述べる各論の整理は、通信の秘密の侵害に当たるか否かに関するものであり、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。
- (3)大量通信となる基準はそれを受け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。

第3条 定義

1 大量通信等

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(第1条)⁵

2 攻撃通信

大量通信等のうち受信した設備に異常を来たず通信(第6条)

3 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

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フィックの圧迫、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

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、大量通信等の状況を踏まえて、適宜見直される。

第2章 各論

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

ア 被害者から申告があった場合

(ア) 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フィ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 別へのトラフィ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フィック及びその通信種別情報」は、個別の通信についてその発信者が自社契約者か否か判別した上で作成された情報であり、通信の秘密に当たる。したがって、これらの情報を攻撃通信への対応のために利用することは、通信当事者の意思に反して行われる場合には通信の秘密の侵害(窃用)に当たりうる(ただし、当該情報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加入者から、「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。

【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することは通信の秘密の侵害(知得)に当たりうる。

しかしながら、遮断だけでは侵害の防止に十分ではない場合、攻撃通信を行っている契約者を特定した上、これを止めるよう連絡をすることなどによって、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。

イ 事業者設備に支障が生じる場合

(エ) 特定の受信者宛の大量通信等やマルウェア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フィック等のデータと、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】

- ・ 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) 大量通信等が、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、発生した大量通信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、当該大量通信等の発生を防止してよいか。

【考え方】

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ことは、通信の秘密の侵害に当たりうる。

しかしながら、大量通信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かったようにした。

(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、大量通信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。

【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、大量通信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)

【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。

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

(キ) 大量通信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、当該大量通信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、大量通信等を送信している契約者を特定した上要請を行うため、これらを解析することは、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、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)に当たりうる。

しかしながら、大量通信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、大量通信等が発生し、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、当該遮断をすることも、正当防衛又は緊急避難として違法性が阻却されると解されること、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、大量通信等を送信し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

(ク) 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ふ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

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。

【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 の他の契約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契約者の元へは返信パケットが数多く送信され、当該契約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

(ケ) 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

(コ) 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

(サ) 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】

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することは通信の秘密の侵害(知得)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うことは、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

(シ) 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フィ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、通信の秘密の侵害に当たる。

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、県間トラフィ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。

(ス) 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)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。

(セ) 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) 大量通信等への共同対処

- (イ) 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行なうことは設備等への影響を防止するために必要な範囲で相当な方法により行なわれる場合には、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。

- (ク) 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、「大量通信等により、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行な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なわれる場合には、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

(イ) 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とならない。

受信者又は受信回線の加入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、全加入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、利用者の選択により、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

(ウ) 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。

(テ) 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加入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、利用者の選択により、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

(ト) 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。(なおウイ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(又は加入者)毎に設定されているが、これを多数の利用者(又は加入者)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受信者又は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とならない。

ウイルス対策等については、通常、利用者又は加入者の端末に対する不当な侵害を防止する、又は、事業者の設備等に対する不当な侵害を防止するために行われる正当防衛又は緊急避難として、ウイルスが添付された通信を検知して除去することの違法性が阻却される。

(4) SMTP 認証の情報を悪用した迷惑メールへの対処

- (ナ) 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、又は当該 ID の正規の利用者に連絡を取り、パスワードの変更等を依頼してよいか。
- (ニ) 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。⁶

【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、大量通信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 の正規の利用者に連絡を取り、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大量通信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

⁶ 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 認証に係る通信を利用することは、通信の秘密の侵害には当たらない。

(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。
- ・ 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。

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大量通信等の弊害を防止し、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利用者に対し、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

- (ア) 攻撃の受信者からの申告に基づき、加入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、当該加入者に対し警告することができるか。
- (イ) また、当該加入者に対して何度警告しても改善されない場合には「要注意加入者」として当該加入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大量通信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加入者を特定し、当該加入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、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、当該加入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る、一概に判断することは困難である。

【事例】

- ・ ある ISP では、ある利用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、当該利用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、当該利用者に注意喚起を行ったが、利用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利用者による通信を停止した。

- (イ) 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者を特定した上で、当該加入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 が契約者の接続ログを解析して感染端末の加入者を特定し、当該加入者に対して注意喚起を行うことは、通信の秘密の侵害(知得及び窃用)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険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、大量通信等の「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。

(2) レピュテーションDBの活用

(ハ) 「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、通信遮断や利用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、受信者又は受信回線の加入者(以下、「受信者等」という。)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えることができ、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、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

【①の事例】

ある ISP の接続サービスでは、利用者の選択により、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】

ACTIVE⁷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。

⁷ 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