「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（案）に対する意見募集の結果について

別紙２

1　概要

・ これまでの議論の内容をまとめた第一次とりまとめ（案）について、総務省ホームページ及び電子政府の総合窓口を通じ幅広く国民より意見募集を実施。

2　意見募集期間

平成26年3月4日（火）～3月17日（月）

3　意見募集の結果

12者から23件の意見提出

4　意見提出者（計12者）

（1）個人（6者）

（2）民間事業者等（6者）

- アーバーネットワークス株式会社
- 一般社団法人日本士業協会
- 株式会社ケイ・オプティコム
- 株式会社日本レジストリサービス
- ヤフー株式会社　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（案）」に対して提出された御意見
【意見募集期間：平成 26 年3月4日（火）～同3月 17 日（月）】

番号	項目 頁	章	節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
1				とりまとめ（案）全体	ウイルス感染の警告のために通信傍受を例外事項として許可するのは構いませんが、その目的外で違法な通信傍受が行われないように、執行する関係者と全く利害のない、第 3 者の数人の立ち合いとチェックを求めます。執行した後にはその取りまとめとして、具体的にどんなウイルス感染の警告のために、何時何人に対して通知したか通信遮断した場合などは、その実行の時間いつからいつまでや影響の出た人数の詳細等を必ずweb サイトに状況報告するようにして下さい。また、作業の過程で収集した個人情報に関しては、安全な場所に保管し、3か月、半年、1年など、必ず期限を設けてデータを全て廃棄するよう求めます。収集したデータの目的外利用が行われないようにして下さい。収集したデータが外部に漏れたりする事がないよう厳密に取り扱って下さい。漏れた場合や目的外利用に対して罰則を設けて下さい。	本とりまとめにおいて整理されたマルウェア配布サイトへのアクセスに係る注意喚起（ACTIVE）については、利用者の同意に基づき、通信傍受ではなく、利用者の通信について機械的・自動的に検知を行うものです。 なお、ACTIVE の実施状況については、ホームページにおいて公表しております。 （https://www.active.go.jp/） さらに、収集されたデータについては、事業者において適切に管理されるよう、指示しているところです。	個人①

番号	項目 頁	章	節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
2				とりまとめ（案）全体	現状のサイバー攻撃が、国民の多くに不安を与えているということは事実であるし、私もサイバー攻撃に不安を感じる一人だ。ゆえに、サイバー攻撃対策自体はなされるべきであるのだが、私はサイバー攻撃対策を理由に、通信の秘密を侵害する方法をなすべきではないと考える。その理由について、とりまとめ案を読む限りサイバー攻撃という言葉の意味があいまいであり、「サイバー攻撃」を口実としてサイバー攻撃と関係のないサイトをアクセスできなくしたり、通信の秘密を不当に侵害し国民のプライバシー権が侵害される可能性がないともいえず、またサイバー攻撃を理由に通信の秘密の侵害の違法性を阻却することは難しいと考える。とりまとめ案を見る限り、正当防衛・緊急避難・正当行為どの行為においても第三者がするものではなく、被害を受けた本人によりその正当防衛・緊急避難・正当行為を行わなければ違法性の阻却は難しいであろう。サイバー攻撃への対策は必要だが、それを通信の秘密を侵す方法で対策を行うことにより、サイバー攻撃以上に通信の秘密を侵される不安が増大してしまっては本末転倒である。通信の秘密を侵す方法での対策については、慎重に考える必要があろう。	サイバー攻撃対策の実施にあたっては、攻撃に係る通信に関する情報の取得・利用が必要となる場合があり、「通信の秘密」について留意することが必要と認識しております。このため、本とりまとめにおいては、通信の秘密を保護する観点から慎重に検討を行いました。いただいた御意見は今後の検討においても参考にさせていただきたいと思います。	個人②
3				とりまとめ（案）全体	ターゲットとなりうる日本企業のルータ情報等を隠す方法を考えるべき。例えば fw.xxxx.co.jp といった会社のルータと思われる情報。会社案内的な WEB サイトが停止しても業務は直ぐには困らないが、上記アドレスへ DDoS されると直ちに支障が出る。 例えば、中国関連ニュースサイトを閲覧していたら、実はそこは人民解放軍のフロント企業で、アクセスログから日本企業のネットワーク情報を収集しており、有事の際に攻撃するつもりなのかもしれない。	本とりまとめは、電気通信事業におけるサイバー攻撃への対処について検討したものであり、御意見については本研究会の検討対象ではございませんが、いただいた御意見は今後の検討においても参考にさせていただきたいと思います。	一般社団法人日本士業協会

番号	項目 頁	章	節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
4				とりまとめ（案）全体	サイバー攻撃は、世界各国の深刻な脅威問題だと思います。厳正に対処し、何処が原因で何処に問題があったか等究明する事も大変重要です。とにかく、国を守っていく上で大変重要な課題だと思いますので総力をあげて取り組んで欲しいです。	いただいた御意見は、本とりまとめに対する賛同意見として承ります。	個人③
5				とりまとめ（案）全体	○ 本とりまとめ（案）に賛同します。 ○ 本とりまとめ（案）により、電気通信事業者はサイバー攻撃へのより適正な対処と電気通信役務の円滑な提供を両立することができるものと考えます。	いただいた御意見は、本とりまとめに対する賛同意見として承ります。	株式会社ケイ・オプティコム
6				とりまとめ（案）全体	とりまとめ案に記載されているDNS Amp攻撃防止のための対策および通信の秘密との関係を示した本内容はDNS の安定運用につながるため、とても良い内容である。	いただいた御意見は、本とりまとめに対する賛同意見として承ります。	株式会社日本レジストリサービス
7	6	1	1	ウェブ感染型マルウェアの感染者は、ハニーポットの設置等により特定することが困難	埋め込まれがちなJavaScriptのコマンドをGoogle等で検索すると汚染サイトがかなり見つかるものです。それ専用のスパイダー（クローラ）を開発してもよいかもしれません。	御指摘のとおり、ACTIVE においては、マルウェア配布サイトを探すため、クローラを用いております。	一般社団法人日本士業協会
8	8	1	2	（1）ACTIVEの普及展開	ACTIVE について、マルウェア配布サイトが危険なことはいうまでもありませんが、マルウェア配布をしないフィッシングサイトについても、オンラインバンキングの認証情報を窃取しようとするなど、国民生活上の脅威となっております。つきましては、フィッシングサイトへのアクセスについても ACTIVE の対象に含めるべきだと思います。	マルウェアの感染経路はウェブ感染が主流になっている現状を踏まえ、ACTIVE はマルウェア配布サイトを現在の対象としております。いただいた御意見については今後の検討においても参考にさせていただきたいと思います。	企業（匿名）

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
9	8	1	2	（1）ACTIVE の普及展開	「利用者がアクセスするウェブサイトがマルウェア配布サイトであるかどうかを検知する行為」は、ネットワークの安定的運用の観点（P.18）から、利用者から同意を得て行うのみならず、利用者から同意を得ていない場合においても正当業務行為として認められるべきか否かの検討をする必要がある。そのため、同項目の最後に以下を追記すべきである。「あわせて、利用者から「有効な同意」が得られていない場合において、利用者がアクセスするウェブサイトがマルウェア配布サイトであるかどうかを検知する行為が正当業務行為に当たり通信の秘密の侵害に係る違法性は阻却されると考えることが可能か否かについて検討する必要がある。」上記の通り「有効な同意」が得られていない場合における対応についても検討することは、現にそのような実態が存在すること、かつ、利用者の安全な利用及びネットワークの安定的な運用を確保する観点から重要である。この場合の対応につき、検討を排除する場合には、その理由を具体的かつ網羅的に示されたい。	本研究会では、構成員から、優先的に対応すべき課題として、 ACTIVE における利用者同意のあり方が検討課題として挙げられました。利用者同意があれば、そもそも通信の秘密を侵害することにはならず、また、本とりまとめにおいて、契約約款に基づく事前の包括同意であっても、有効な同意といえる場合について整理されたことにより利用者のさらなる拡大が見込まれると考えております。本件注意喚起対策を望まない利用者は、随時、同意内容を変更できる（設定変更できる）ことを要件としており、これによって通信が利用等されることを望まない利用者が不測の不利益を被ることを回避することが可能となっています。マルウェア対策と通信の秘密との関係については、今後も必要に応じて検討を行って参りたいと考えております。	ヤフー株式会社

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
10	10 ～ 12	1	2	(3)新たなDDoS攻撃である DNSAmp 攻撃の防止	一般家庭のブロードバンドルータを使った DNS Amp 攻撃に焦点を当てているが、ホスティング事業者の専用サーバやVPSもオープンリゾルバになっていることがある。それらについてもブロードバンドルータと同様の対策が必要である。増幅率を増やすために攻撃用 DNS サーバは用意すると記載されているが、DNSSEC 署名している権威 DNS サーバを利用することでも攻撃が可能であり事例として追記し、対策についても記載すべきである。「新たな DDoS 攻撃である DNS Amp 攻撃」と記載されているが、DNS Amp 攻撃は特に新しい攻撃手法ではない。	本研究会では、構成員から、 優先的に対応すべき課題として挙げられたものを中心に検討を行ったところです。いただいた御意見については、これに限らず、技術の進歩や新たな対策などサイバー攻撃を取り巻く環境の変化に応じて、引き続き検討させていただきたいと思います。また、DNSSEC 署名している権威 DNS サーバを利用した攻撃については、御指摘を踏まえ、P10 及び P26 の記載を次のように修正します。 <P10> 「DNSAmp 攻撃は、下記ｉの『準備』の下、下記 ii からiv の一連の動作を繰り返し行うことによって、攻撃先に巨大なパケットを送信させる攻撃である。ｉ　攻撃者はあらかじめインターネット上に公開されているDNSサーバに『関して』、あるドメイン名の名前解決 の問合わせがあった場合には、大量のパケットを応答する『ものを用意する』（以下『当該 DNS サーバ』を「攻撃用 DNS サーバ」という。）。」 <P26> 「DNSAmp 攻撃は、前述のとおり、下記ｉの『準備』の下、下記 ii からiv の一連の動作を繰り返し行うことによって、攻撃先に巨大なパケットを送信させる攻撃である。ｉ　攻撃用DNSサーバとして、あらかじめ公開 DNS サーバに対してある名前解決の問合わせがあった場合に大量のパケットを応答する『ものを用意し』」	株式会社日本レジストリサービス

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
11	19～22	3	1	第3章第1節 全体	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有効な同意に関し、マルウェア配布だけでなく、マルウエア配布をしないフィッシングサイトについても対象に含めるべきだと思います。	マルウェアの感染経路はウェブ感染が主流になっている現状を踏まえ、ACTIVE はマルウェア配布サイトを現在の対象としております。いただいた御意見については今後の検討においても参考にさせていただきたいと思います。	企業（匿名）
12	19	3	1	（1）問題の所在	「利用者がアクセスするウェブサイトがマルウェア配布サイトであるかどうかを検知する行為」は、ネットワークの安定的運用の観点（P.18）から、利用者から同意を得て行うのみならず、利用者から同意を得ていない場合においても正当業務行為として認められるべきか否かの検討をする必要がある。そのため、同項目の最後に以下を追記すべきである。「あわせて、利用者から「有効な同意」が得られていない場合も現に多いことから、このような場合においても利用者の安全な利用及びネットワークの安定的な運用を確保するため、利用者がアクセスするウェブサイトがマルウェア配布サイトであるかどうかを検知する行為が正当業務行為に当たり通信の秘密の侵害に係る違法性は阻却されると考えることが可能か否かについて検討を行う。」上記の通り「有効な同意」が得られていない場合における対応についても検討することは、現にそのような実態が存在すること、かつ、利用者の安全な利用及びネットワークの安定的な運用を確保する観点から重要である。この場合の対応につき、検討を排除する場合には、その理由を具体的かつ網羅的に示されたい。	本研究会では、構成員から、優先的に対応すべき課題として、 ACTIVE における利用者同意のあり方が検討課題として挙げられました。利用者同意があれば、そもそも通信の秘密を侵害することにはならず、また、本とりまとめにおいて、契約約款に基づく事前の包括同意であっても、有効な同意といえる場合について整理されたことにより利用者のさらなる拡大が見込まれると考えております。本件注意喚起対策を望まない利用者は、随時、同意内容を変更できる（設定変更できる）ことを要件としており、これによって通信が利用等されることを望まない利用者が不測の不利益を被ることを回避することが可能となっています。マルウェア対策と通信の秘密との関係については、今後も必要に応じて検討を行って参りたいと考えております。	ヤフー株式会社

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
13	20	3	1	(2)考え方「通常の利用者であれば、その限りにおいてこれらの事項が利用されることについて許諾することが想定し得る」	「許諾することが想定し得る」とする根拠を明らかにすべきと考える。p.16、脚注 26 で引用されている通り、「通常の利用者であれば同意することがアンケート結果等により合理的に推定されること」が従来の整理による基準である。しかし、本件文書では「アンケート結果等」に相当する根拠が示されていなく、文書内で齟齬が生じている。利用者の意思を根拠なく推定することを認めた場合、今後、利用者の同意が不確かな情報利用が際限なく広がるおそれが生じる。よって、「許諾することが想定し得る」とする根拠を明らかにすべきと考える。	契約約款等に基づく事前の包括同意のみでは、一般的には有効な同意と解されていないところ、本研究会においては、契約約款に基づく事前の包括同意であっても有効な同意として認められる場合について整理したところです。一般的・類型的に見て、ISP が、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に当たって、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ることについては、安全なインターネットアクセスを確保するためのものであり、インターネットアクセスサービスの通常の利用者であれば、その限りにおいてこれらの事項が利用されることについて許諾することが想定し得ることから、契約約款の性質になじまないとまでは言えないこと等から、一定の条件を満たす場合には、契約約款に基づく事前の包括同意であっても、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ると整理しています。	個人④

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
14	19～22	3	1	(2)考え方	「契約約款等に基づく事前の包括同意のみでは、一般的には有効な同意と解されていない理由としては、①契約約款は当事者の同意が推定可能な事項を定める性質のものであり、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こと」という前提条件に対して、20 頁 6 行目、「理由①との関係では、…(中略)…該当するアクセスに対して、注意喚起画面等を表示させることについては、安全なインターネットアクセスを確保するためのものであり、インターネットアクセスサービスの通常の利用者であれば、その限りにおいてこれらの事項が利用されることについて許諾することが想定し得ることから、契約約款の性質になじまないとまでは言えない。」としている。 これは、前提として、上記①から、「通信の秘密」に関する事項について、当事者の同意が推定可能な事項を定める性質のものである契約約款に基づく事前の包括同意は許されない趣旨(即ち、推定的承諾が得られると思われる事項で構成された契約約款では通信の秘密に関する利益を放棄できない)であると思われる。 にもかかわらず、その結論として「インターネットアクセスサービスの通常の利用者であれば、その限りにおいてこれらの事項が利用されることについて許諾することが想定し得ることから、契約約款の性質になじまないとまでは言えない。」という論旨は、仮に契約約款の性質に合致したとしても、通信の秘密の利益について放棄できる合理的説明にはなっていないと考えられる。 今回の取りまとめ案としては、この①に関して、その理由に対して「変遷」と考えて、新たな指針を設けるか、①の考えはそのままに、合理的な前提条件を設定し、当該前提条件であれば通信の秘密に関する事項について、契約約款等に基づく包括同意が許される旨の理論構成にすべきであると考える(この場合は、このような前提条件を設定するに当たった状況・環境の変化を説明することも必須であると考える)	契約約款は当事者の同意が推定可能な事項を定める性質のものであり、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等の理由から、契約約款等に基づく事前の包括同意のみでは、一般的には有効な同意と解されておりません。 しかしながら、上記の解釈を前提としても、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ついて見れば、一般的・類型的に見て、ISPが、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に当たって、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ることについては、安全なインターネットアクセスを確保するためのものであり、インターネットアクセスサービスの通常の利用者であれば、その限りにおいてこれらの事項が利用されることについて許諾することが想定し得ることから、契約約款の性質になじまないとまでは言えないと考えられるため、本とりまとめにおいては、一定の条件を満たす場合には、契約約款に基づく事前の包括同意であっても、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ると整理しています。	個人⑤

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
15	19～22	3	1	(2)考え方	「利用者がアクセスするウェブサイトがマルウェア配布サイトであるかどうかを検知する行為」は、ネットワークの安定的運用の観点(P.18)から、利用者から同意を得て行うのみならず、利用者から同意を得ていない場合においても正当業務行為として認められるべきか否かの検討をする必要がある。そのため、本項目において、正当業務行為に該当するか否かの検討を、正当業務行為として整理した第 3 節「新たな DDoS 攻撃である DNSAmp 攻撃の防止」及び第 4 節「SMTP 認証の情報を悪用したスパムメールへの対処」と整合的な形で検討し、記載すべきである。 その検討において正当業務行為に当たらないと整理する場合には、第3節及び第4節における整理との差異を、詳細かつ明示的に示されたい。	本研究会では、構成員から、優先的に対応すべき課題として、 ACTIVE における利用者同意のあり方が検討課題として挙げられました。利用者同意があれば、そもそも通信の秘密を侵害することにはならず、また、本とりまとめにおいて、契約約款に基づく事前の包括同意であっても、有効な同意といえる場合について整理されたことにより利用者のさらなる拡大が見込まれると考えております。本件注意喚起対策を望まない利用者は、随時、同意内容を変更できる(設定変更できる)ことを要件としており、これによって通信が利用等されることを望まない利用者が不測の不利益を被ることを回避することが可能となっています。マルウェア対策と通信の秘密との関係については、今後も必要に応じて検討を行って参りたいと考えております。	ヤフー株式会社

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
16	23	3	2	（1） 対策の概要及び問題の所在	23 頁 9 行目、「本件対策は、マルウェアへの感染という緊急時に行われる対策として、少なくとも緊急避難の要件を満たすと考えることはできないか検討する。」とあるが、このようなマルウエアへ感染した場合に個別に注意喚起する行為は、常時通信を監視していないと効果をあげることは難しいと思われる。また、緊急避難は「将来の危難」も含まれるが、「危難が現存するか、間近に押し迫っている場合」※とされており、この場合における「緊急時」の判断が容易ではなく、積極的な対策実施することを躊躇することも考えられる。また実際に通信に多大な影響を与えてる事態となった文字通りの「緊急時」が到来した場合の対策としては遅きに失していると思われる。 従って、このようなマルウエア感染駆除の営みは、緊急性を必要条件としない「正当業務行為」として整理する方向性も検討すべきである。※前田雅英刑法総論講義第 3 版 257 頁「２緊急非難の要件」、「(1)正当防衛のとの違い」より抜粋	本とりまとめにおいては、C&C サーバ等がテイクダウンされた場合において、当該C&C サーバ等に蓄積されている、C&C サーバとマルウェアに感染したコンピュータ等の端末との間の通信の履歴のうち、マルウェア感染端末に係るIP アドレス及びタイムスタンプを基に、ISP において、タイムスタンプに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うことについて、マルウェアへの感染という緊急時に行われる対策であることから緊急避難として整理しています。「現在の危難の存在」については、C&C サーバからの指令に従ってコンピュータ等の端末を制御する機能を有するマルウェアに感染し、C&C サーバと通信をしている端末については、C&C サーバによる制御が実際に行われていることをもって、コンピュータ等の端末が正常かつ安全に機能することについて、法益の侵害が現に存在しており、現在の危難が存在すると考えられます。したがって、マルウェア感染により、当該端末に保存された情報の漏えいやデータの破壊・改ざんのほか、DDoS 攻撃等のサイバー攻撃の踏み台となる等、深刻な被害を受ける前であっても、当該利用者に対して注意喚起を行うことが可能と考えられます。なお、通信の秘密との関係で問題が生じ得る場合であっても、利用者の同意ないし緊急避難等の違法性阻却事由の一つがある場合には、電気通信事業法第４条第１項に違反しないこととなります。本検討項目においては、緊急避難となる場合について整理しております。	個人⑤

番号	項目 頁	章	節	該当部分	提出された御意見	御意見に対する考え方	意見提出者
17	24～27	3	3	第3章第3節全体	○ 第3章第3節「新たなDDoS攻撃であるDNSAmp攻撃の防止」では、DNSAmp 攻撃のみに着目して具体的検討がなされておりますが、DNS 以外の通信プロトコル（NTP、SNMP等）を活用してDNSAmp攻撃とほぼ同一のしくみで攻撃できることは広く認知されているところです。 ○ そのため、本節においては、活用する通信プロトコルは異なるものの、攻撃のしくみが DNSAmp 攻撃とほぼ同一と見なすことができる攻撃（少なくとも、第1章第2節に記されているNTPAmp攻撃）についても具体的検討の対象に加えるとともに、正当業務行為として違法性が阻却されるか否かを検討・整理いただくことを要望します。 ○ インターネット上の正常な機能を悪用した攻撃は、今後も新たなものが出現すると考えられます。一方、新たな攻撃が確認される都度、通信の秘密との関係を検討していては、それを終えるまでの間、電気通信事業者は新たな攻撃に対して即応できない恐れがあり、場合によっては、電気通信役務の円滑な提供が困難となることが懸念されます。 ○ そのため、既知の攻撃に対する検討にとどまらず、未知の攻撃への対処のあり方についても検討・整理いただくことを要望します。	いただいた御意見については、これに限らず、技術の進歩や新たな対策などサイバー攻撃を取り巻く環境の変化に応じて、引き続き検討させていただきたいと思います。	株式会社ケイ・オプティコム
18	24～25	3	3	（1）対策の概要及び問題の所在	ブロードバンドルータへのフィルタが唯一の対策に読める書き方になっているが BCP38 が根本対応であり、そのことを追記すべきである。	本研究会では、構成員から、 優先的に対応すべき課題として挙げられたものを中心に検討を行ったところです。いただいた御意見については、これに限らず、技術の進歩や新たな対策などサイバー攻撃を取り巻く環境の変化に応じて、引き続き検討させていただきたいと思います。	株式会社日本レジストリサービス

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
19	25	3	3	（2）正当業務行為該当性	17ページにおいて、正当防衛及び緊急避難に関しては、明確な要件設定がなされているのに対し、正当業務行為に関してはその記載がないにもかかわらず、24ページ「第3章具体的検討第3節 新たな DDoS 攻撃である DNSAmp 攻撃の防止」において突如として、①目的の正当性、②行為の必要性、③手段の相当性の観点からの議論を展開しており、唐突感が否めない。総務省として、上記3点を正当業務行為の判断要素として考えている旨を明確にしていただきたい。本分野は技術進展が著しく速く、今回整理された個別対応策はすぐに陳腐化する恐れがある。個別の対策についての整理を待った上で対策をしていては、サイバー攻撃に対して迅速な対応ができない。効果的な対策を行うには、正当業務行為に該当する要件を示した上で、対応が行われる必要があるものと考える。	本とりまとめ P17～P18 において、「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。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。」（平成 22 年 5 月総務省「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」第二次提言より）とされています。	ヤフー株式会社
20	25～27	3	3	（2）正当業務行為該当性	ブロードバンドルータが DNS Amp 攻撃に利用されている状況下で、必要最低限の通信内容を見てフィルタリング制御しており、技術的にも必要最低限な内容になっていると考える。 DNS Amp 攻撃の根本対応である BCP38 と通信の秘密の関係を明確にすべきである。	本研究会では、構成員から、 優先的に対応すべき課題として挙げられたものを中心に検討を行ったところです。いただいた御意見については、これに限らず、技術の進歩や新たな対策などサイバー攻撃を取り巻く環境の変化に応じて、引き続き検討させていただきたいと思います。	株式会社日本レジストリサービス

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
21	29	3	4	（2） 対策1について ① 目的の正当性	29 頁 5 行目に「ある中小 ISP において、SMTP 認証 ID・パスワードを悪用したスパムメールの送信により、メールの滞留が通常の 50 倍以上に急増し、これにより、メールの送信システム自体を再起動する措置を採らざるを得ず、その結果、短時間だがその間利用者からメールの送信が行えない状況となった事例がある。」という記述があるが、殊更「ある中小ISP」の例を列挙することが適当なのか、また「中小 ISP」と記載する必要があるのか疑問がある。更に、同頁 10 行目に「このような状況に対処するため」と記載してあることからも、当該対策については「中小 ISP」をターゲットしているようにも読め、妥当な記述や例示適示とは思えない。 なお、24 頁以下に記載されている「第3節 新たな DDoS 攻撃である DNSAmp 攻撃の防止 （2） 正当業務行為該当性 ① 目的の正当性」において、欧州における大規模な影響事例を提示しており、この点からも上記例示について、適切な表現・引用とは思えない。	中小 ISP におけるスパムメールによる被害事例、欧州における DNSAmp 攻撃による被害事例については、いずれもそれらの攻撃の事例として記載しているものです。	個人⑤

番号	項目			該当部分	提出された御意見	御意見に対する考え方	意見提出者
	頁	章	節				
22	31 ～ 32	3	5	第3章第5節全体	サイバー攻撃の予兆を捉えることは非常に困難であると思います。しかしその一助として世界中のインターネット上のトラフィックを把握することにより、サイバー攻撃の傾向を認識出来ると考えております。弊社ではASERT (Arbor Security Engineering and Research Team)というリサーチチームが全世界のインターネット上のトラフィックを分析しており、その情報をatlas.arbor.net というサイトで公開しております。このサイトでは過去 24 時間のトラフィックの情報をご覧になることが出来、その中に 24 時間以内に全世界で発生したDDoS 攻撃の回数や攻撃トラフィックの規模等が含まれております。またこの情報は ww.digitalattackmap.com というサイトにも反映されております。そこでこのような情報を ASERT のメンバーから総務省様および関係機関様に提供させていただくことにより、皆様のお役に立てるのではないかと考えております。また“通信の秘密”の保護に関する規定があるため、日本からは情報を提供していただくことが難しい状況にございます。もし日本からも情報提供をしていただくことが出来れば、日本国内のトラフィックに関してもより詳細な分析が可能だと考えております。そこについては、どうお考えでしょうか？	いただいた情報については、参考とさせていただきます。また、日本からの情報提供については、現在も、通信の秘密に配慮しながら事業者間で必要な情報共有を行うことを可能としているケースもあり、今後、必要に応じて検討を行って参りたいと考えております。	アーバーネットワークス株式会社