資料１１－２

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

平成26年4月

目次

（参考資料）

序章

インターネットは、今やあらゆる社会経済活動を支える基盤であり、これによる経済成長や国民生活の利便性の向上が期待されている。一方で、このようなインターネット利用の普及に伴って、企業、個人、政府組織を狙ったサイバー攻撃が顕在化するとともに、情報通信技術の発展も相まって、DDoS[1]攻撃やマルウェア[2]の感染活動等、サイバー攻撃の手法そのものも巧妙化、複雑化している状況にある。

従来から、インターネット・サービス・プロバイダー（ISP）等電気通信事業者は、利用者が安心し安定的に利用できるインターネット環境を確保するため、「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（以下「大量通信ガイドライン」という。）」[3]を策定する等、業界連携や官民連携を通して、サイバー攻撃に対処してきた。しかし、技術革新に伴い高度化する新たなサイバー攻撃に有効に対応するためには、これまでの手法に加えて、新たな対策や取組を講じていくことが喫緊の課題となっている。

このため、総務省では、平成 25 年 11 月から「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」（以下「研究会」という。）を開催し、サイバー攻撃が巧妙化、複雑化する中で、電気通信事業者が通信の秘密等に配慮した適切な対応を行うことが可能となるよう、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ついて検討を行った。研究会では、最近のサイバー攻撃の動向を踏まえ、優先的に対応すべき課題とその対策を洗い出し、これらについて集中的に、技術的・制度的な観点から議論を行った。

本報告書は、研究会における議論や検討を踏まえ、それぞれの課題の解決の方向性について、一定のとりまとめを行ったものである。今後、本報告書を参照し、電気通信事業者において、自主的に適正なサイバー攻撃への対処が行われることを期待する。

---

1 分散型サービス妨害（Distributed Denial of Service）のこと。相手のコンピュータやルータ等に不正なデータを送信して使用不能に陥らせたり、トラヒックを増大させて相手のネットワークを麻痺させたりする攻撃を DoS(Denial of Service)攻撃といい、複数のネットワークに分散する大量のコンピュータが一斉に特定のサーバへパケットを送出し、通信路をあふれさせたり、大量の処理を実施させたりすることによって機能を停止させてしまう攻撃を DDoS 攻撃と呼ぶ。

2 malicious software を組み合わせた造語。コンピュータウイルス、ワーム、スパイウェアなどの「悪意のあるソフトウェア」の総称。

3 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から構成される「インターネットの安定的な運用に関する協議会」が策定。総務省はオブザーバーとして参加。

第１章　サイバー攻撃をめぐる環境

第１節　これまでの状況とそれに対する取組

サイバー攻撃は、近年、高度化、複雑化するとともに、愉快犯から経済犯・組織犯的なものに移行しており、インターネットが国民生活や社会経済活動にとって必要不可欠なものとなっている中で、大きな社会的脅威となっている。

最近のマルウェアの傾向としては、メール等による他のコンピュータへの感染拡大や、感染したコンピュータの正常な動作を妨げる「ワーム」に加えて、感染したコンピュータを遠隔操作し、スパムメールの送付や過剰な通信の送付等を行う「ボット[4]」、ウェブサイトを改ざんし、当該ウェブサイトを閲覧した利用者が気付かないうちにマルウェアをダウンロード若しくは実行する「ドライブバイダウンロードによる攻撃[5]」が流行する等、異変が分かり駆除しやすいものに加えて特段の不具合を感じさせず駆除されにくいものが増えており、悪質化している。

また、サイバー攻撃の目的も、攻撃者が自己の知名度を高めたり、技術の高さを他人に誇示したりする等、サイバー攻撃そのものを動機とした好奇心によるものから、現在では、インターネットバンキングの不正送金や知的財産の窃取等を目的とした、計画的な金銭目的のものへと移行している。

このようなサイバー攻撃の多様化・悪質化を背景として、攻撃の対象も、個人・企業から政府機関等に拡大しており、被害も深刻化している。

---

[4] マルウェアの一種であり、感染したコンピュータを攻撃者が用意したネットワーク上のサーバに接続し、攻撃者からの指令通りの処理を感染者のコンピュータ上で実行するプログラム。

[5] ドライブバイダウンロードによる攻撃手法としては、ウェブサイト管理者の端末をマルウェアに感染させることでサイトの管理権限を取得し、サイトを改ざんすることで、サイトを閲覧した利用者の端末をマルウェアに感染させる「ガンブラー」と呼ばれるものが有名である。

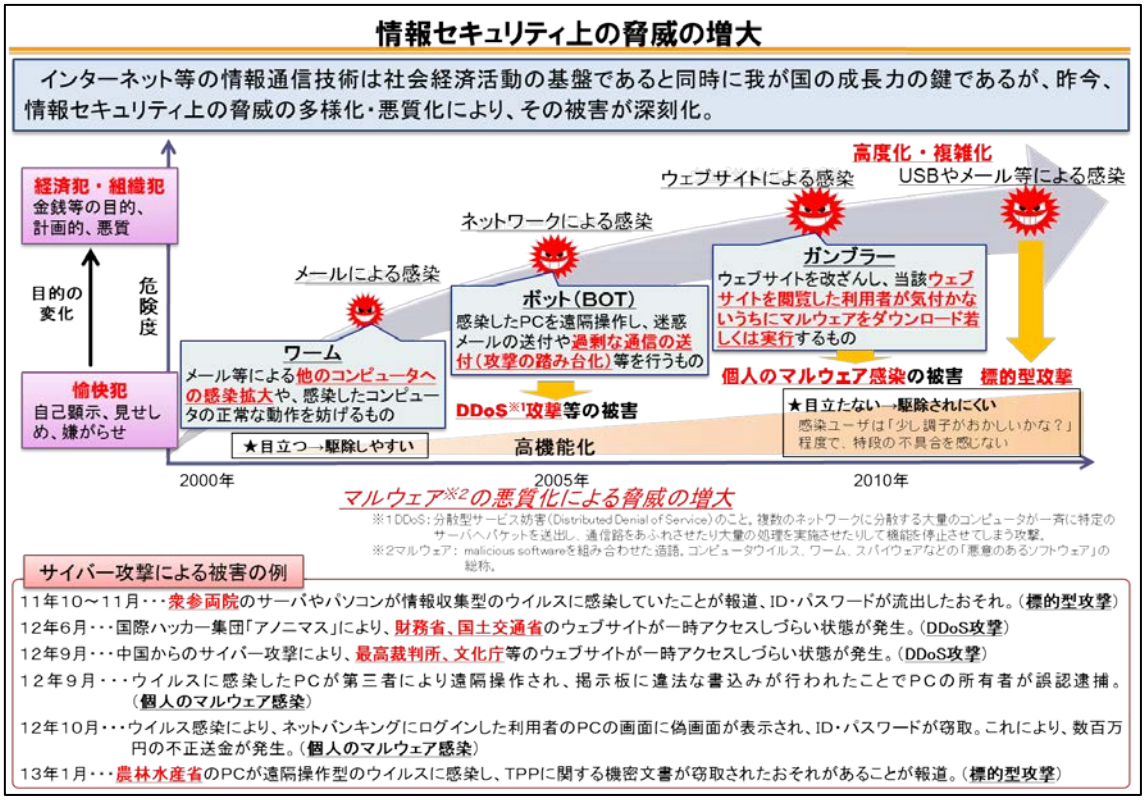

図１　情報セキュリティ上の脅威について

サイバー攻撃の多様化・悪質化に対しては、従来から、ISP 等の電気通信事業者による業界連携、官民連携等の取組を通して、対応されてきたところである。

例えば、平成 17 年の大規模な DoS 攻撃の発生を契機に、業界横断的な取組として、平成 19 年には大量通信ガイドラインが策定された。

これは、DoS 攻撃、DDoS 攻撃等の大量通信の発生やマルウェアの感染拡大は電気通信事業者の設備、ひいては、電気通信役務の提供に影響を与えるところ、円滑な電気通信役務の提供の確保のためには一定の通信の遮断等の措置が必要となるが、通信の遮断等の措置を採るに当たっては、通信の秘密と抵触する場合があるため、業界の自主基準として、法律の解釈について一定の指針を示したものである。通信の秘密の侵害該当性について、ある程度類型化できるものについてガイドラインとしてまとめ、業界でこれを共有することにより、各社によって対応が必ずしも同じではなかったサイバー攻撃に対して、電気通信事業者は、通信の秘密の保護に最大限配慮しながら、業界横断的な協調対処を行うことが可能となった。

また、DoS 攻撃、DDoS 攻撃等の大量通信が頻発しはじめた当初、その主な原因はインターネットに接続しただけで感染してしまう、いわゆるネットワーク感染型マルウェアの「ボット」の感染拡大であったことから、平成 18 年から

平成 22 年まで、総務省・経済産業省と情報セキュリティ関係機関が連携し、ボット対策プロジェクト「サイバークリーンセンター（Cyber Clean Center。以下「CCC」という。）」を実施した。

この取組は、インターネット利用者が「ボット」の感染を容易には認知できないことから、感染行動を検知するハニーポット[6]を設置することにより、ボットに感染しているインターネット利用者を特定し、ISP から当該利用者に対して、注意喚起及びウイルス駆除対策の実施の奨励を行うことで、サイバー攻撃の踏み台等となる「ボット」を撲滅しようとしたものである。

具体的には、①ハニーポットに来た通信の送信元 IP アドレス（動的 IP アドレス）とタイムスタンプに関する情報を、当該 IP アドレスの割当てを実施した ISP に提供し、②当該 ISP が、当該 IP アドレスをどの契約者に割り当てたかについて顧客情報と突合することにより、ボット感染者の割り出しを行い、当該感染者に対して注意喚起を実施した[7]。

本取組には、最終的に 76 もの ISP が参加し、全体で我が国のブロードバンド利用者の 80%以上をカバーしたこともあり、結果的に、世界トップクラスの低ボット感染率を実現[8]することができた。

---

6 攻撃者の侵入手法やマルウェアの振る舞い等を調査・研究するためにインターネット上に設置された、わざと侵入しやすいよう設定されたサーバやネットワーク機器のこと。

7 後述の通信の秘密との関係については、通信の送信元 IP アドレス及びタイムスタンプ（電子データに属性として付与される時刻情報）は、通信の構成要素として通信の秘密の保護の対象であるところ、①の行為については、CCC の事務局は、当該通信を受信する一方当事者であるから、これらを ISP に提供することは、通信の秘密の侵害に当たらないと考えられる（これらは、通信当事者間で共有されている情報であり、その秘密性を当事者間で相手に委ねているため、第三者への関係で、一方当事者の同意により秘密性が解除されるためである（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（平成 22 年５月）（以下「第二次提言」という。）11 頁より））。②の行為については、通信の秘密の窃用に該当するが、マルウェアの感染活動という現在の危難を避けるための緊急避難として、通信の秘密の侵害に係る違法性は阻却されると考えられる。

8 平成 17 年の約２～2.5%から平成 23 年には約 0.6%に低下した。

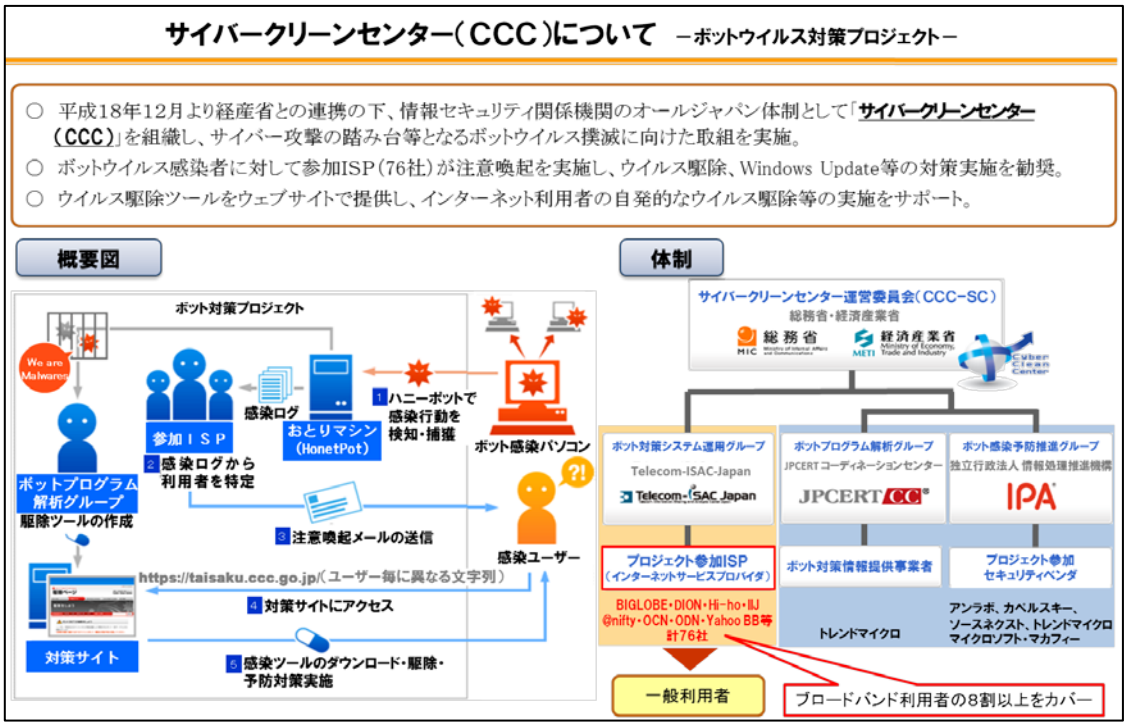

図２　サイバークリーンセンター（CCC）について

さらに、官民連携の取組としては、新たに、平成 25 年から、総務省と ISP 等が連携し、マルウェア感染防止・駆除プロジェクト「アクティブ（Advanced Cyber Threats response InitiatiVE。以下「ACTIVE」という。）」を実施している。

これは、最近では、ウェブサイトにアクセスしただけで感染してしまう、いわゆるウェブ感染型マルウェアが主流となっており、そのようなマルウェアに感染させる可能性の高いウェブサイト（以下「マルウェア配布サイト」という。）であるかどうかは、インターネット利用者にとって認知されにくいことから、CCC のようなマルウェア駆除の取組に加えて、インターネット利用者がマルウェア配布サイトにアクセスしようとする際に、ISP から注意喚起を行うことにより、マルウェア感染を未然に防止しようとする取組である。

具体的には、あらかじめ、マルウェア配布サイトの URL 情報をリストとしてデータベース化し、インターネット利用者がウェブサイトにアクセスする際に、ISP において、当該ウェブサイトと当該データベースを照合し、当該ウェブサイトがマルウェア配布サイトであると判明した場合には、当該利用者にその旨の注意喚起を実施するものである[9]。

[9] 後述の通信の秘密との関係については、注意喚起を行うに当たって利用等されるアクセス先 URL は、通信の構成要素であり、通信の秘密に属する事項であるが、利用者の個別の同意に基づいて行われており、通信の秘密の侵害に当たらないと考えられる。

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であることから、ACTIVE は、マルウェア駆除対策である CCC と比較して、マルウェア感染防止の対策を新たに追加し、これに重点を置いて、進められているところである。

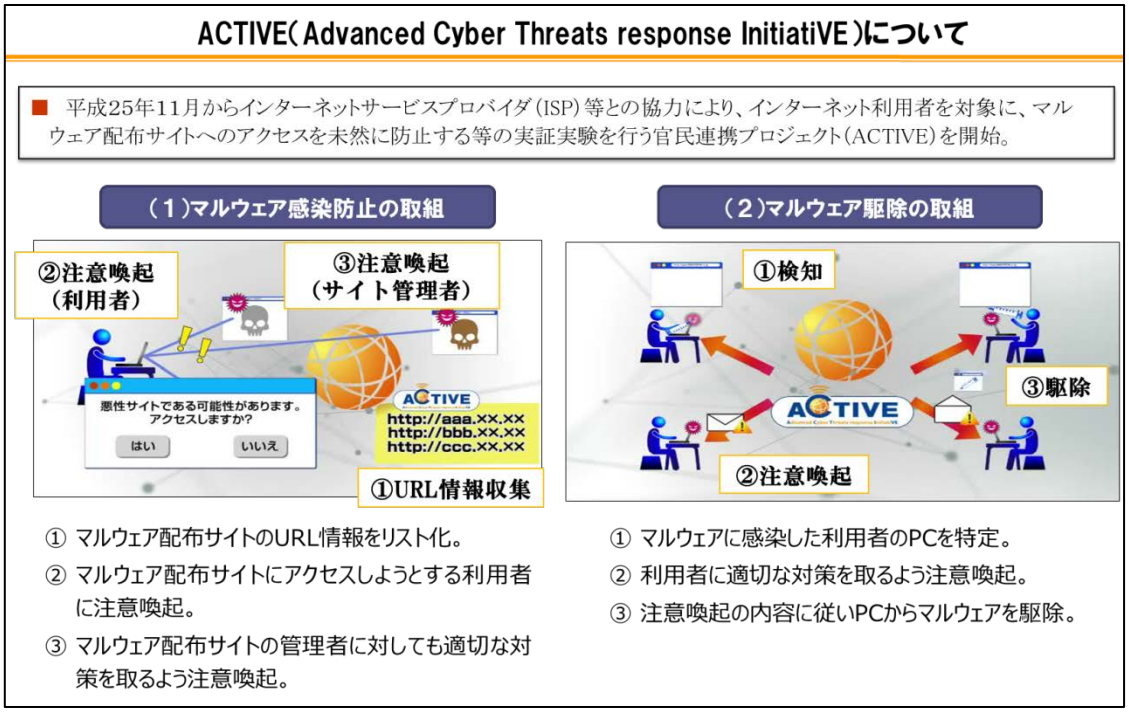

図３　ACTIVE について

第２節　最近のサイバー攻撃に係る課題と対策例

上述のとおり、サイバー攻撃への対策は、その態様の変遷に伴って、これまで、業界あるいは官民が連携して、様々な取組が行われてきたところである。しかし、これらの取組を更に効果的なものとするためには、例えば注意喚起の拡大等、改善すべき課題がある。

また、最近のサイバー攻撃の具体的な事案を見ていくと、必ずしもマルウェア感染によるものではなく、DNS[10]の仕組み等インターネット上想定されている正常な機能を悪用するような新たな攻撃手法も発生しており、従来のマルウェア感染駆除や感染防止の取組がそのまま有効であるとは言いがたい場合も出てきている。

そこで、研究会では、そのような事例を洗い出し、これらに対する対策について検討を行った。まとめると表１及び図４のとおりである。

10 Domain Name System の略で、インターネット上のコンピュータ同士が通信する際に、通信相手を特定するためにドメイン名と IP アドレスを対応づける仕組みのことをいう。

表１　最近のサイバー攻撃に係る課題と対策例

	解決すべき課題	その対策例
（１）	ACTIVE の普及展開	有効な同意の在り方の明確化による ACTIVE の対象者の拡大
（２）	マルウェア感染駆除の拡大	C&C サーバ等に蓄積されている情報に基づく感染者へのマルウェア駆除を促す注意喚起の実施
（３）	新たな DDoS 攻撃である DNSAmp 攻撃の防止	一定の通信（動的 IP アドレス宛てで、UDP53 番ポートを通る通信）の遮断
（４）	SMTP 認証の情報を悪用したスパムメールへの対処	SMTP 認証を不正利用されている利用者に対する注意喚起等
（５）	サイバー攻撃の未然の防止と被害の拡大防止	①サイバー攻撃に係る通信の遮断 ②ISP の業界横断的な連携

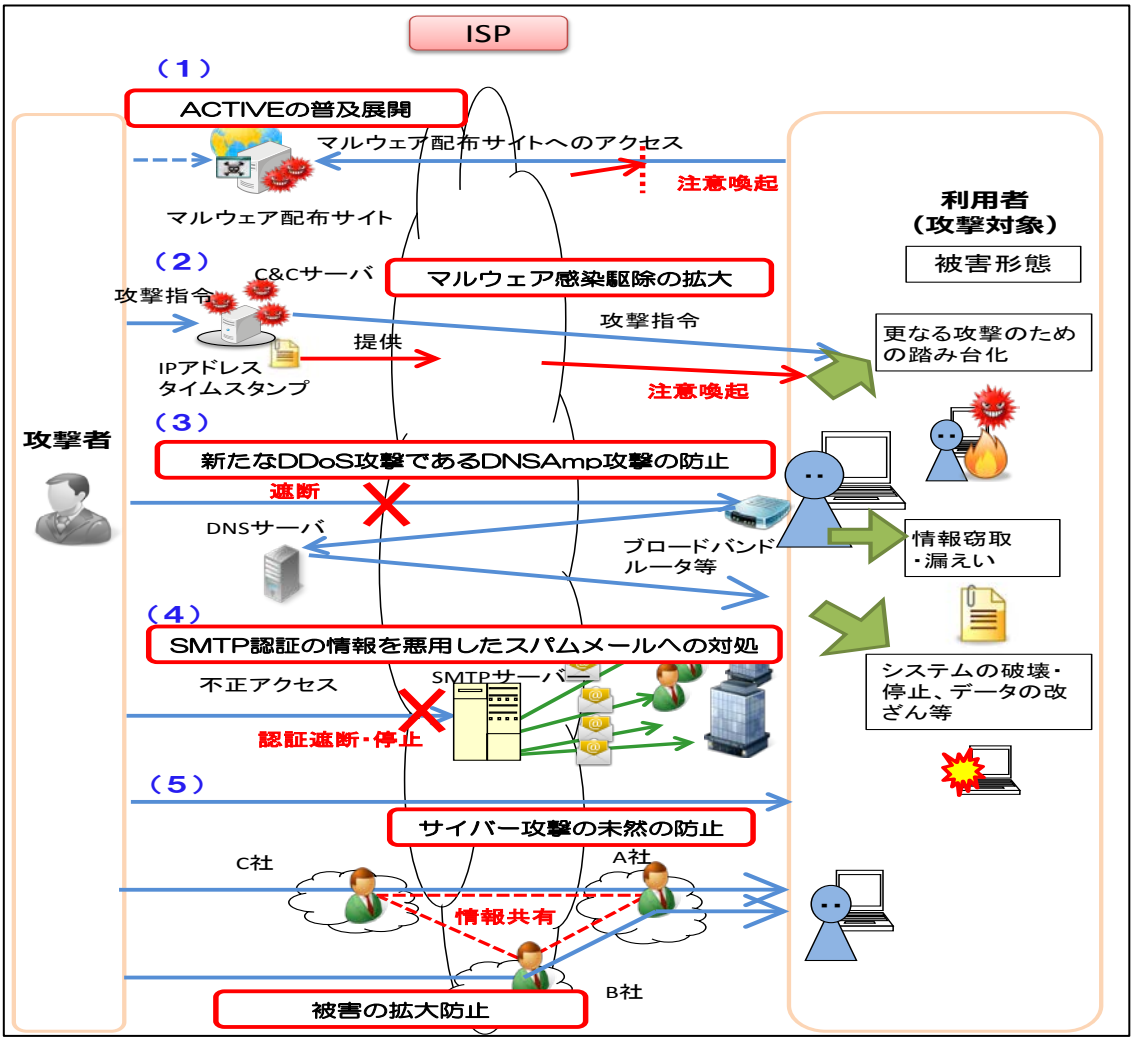

図４　課題と対策例のイメージ

（１）ACTIVE の普及展開

ACTIVE は、最近の主流であるウェブ感染型マルウェアの感染を未然に防止する取組として平成 25 年から官民が連携して進めているところである。

一方、ISP において、利用者の有効な同意を得ずに、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、通信の秘密の侵害に該当することから、ACTIVE の実施にあたっては、あらかじめ、利用者（当該 ISP のインターネット接続サービスの利用者）から個別の同意を得た上で行っているところである。

しかし、運用上、個別の同意について、契約締結時ではなく、既に契約をしている利用者から改めて得ることは困難であり、また、仮に個別の同意について呼びかけをしたとしても、利用者が当該呼びかけに気が付かなければ、個別に同意を得ることは難しく、結果的に、ACTIVE の利用者の拡大につながらず、マルウェア感染の防止が進まないという結果となる。

このため、利用者の個別の同意について、どのような場合であれば「有効な同意」と考えられるのか検討する必要がある。

（２）マルウェア感染駆除の拡大

最近のマルウェアは、インターネット利用者がその感染を認知しにくいものとなっていることから、利用者がそのリスクを認識し、自主的な対応を実施するような仕組みを構築することが重要となる。このような観点から、これまで、CCC や ACTIVE の対策が講じられてきたところであるが、マルウェアの数はこの６年間で約 140 倍に増加しており[11]、従来の活動だけでは、全てのマルウェア感染者に対してリーチすることが、難しい状況となっている。

マルウェア感染の駆除を更に進めるためには、マルウェアに感染していると思われる利用者を、なるべく多く見つけ出すことが重要なファクターとなる。

これまでの CCC や ACTIVE では、マルウェアに感染したコンピュータの挙動に注目して、マルウェアの中には自ら自動的に感染活動を行うものがあることから、このような感染活動を検知するハニーポットを設置し、マルウェア感染者の特定を行っている。他方、最近顕著となっているマルウェアに感染したコンピュータの挙動としては、攻撃者が用意した C&C サーバ[12]等の攻撃に係るサーバ（以下「C&C サーバ等」という。）に自動的に接続されるも

11 トレンドマイクロ株式会社によれば、マルウェアの種類は平成 19 年の約 59 万種から平成 24 年には約 8,300 万種に増加。

12 Command and Control サーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に指令を送って制御するサーバコンピュータのこと。

のもあり、これらは C&C サーバを通じた指令を受けて、スパムメール等の大量送信や DDoS 攻撃等のサイバー攻撃の踏み台となるほか、キーボードの操作履歴や保存された情報の漏えい、データの破壊・改ざん等を行うよう遠隔操作されているものがある[13]。このような通信は、ハニーポットの設置によっては検知することができないが、C&C サーバ等に蓄積されている通信履歴の情報を分析すると、C&C サーバとの通信の相手を特定できる場合もあり、このような特定が可能となれば、なるべく多くのマルウェア感染者に注意喚起を行うことが可能になる。

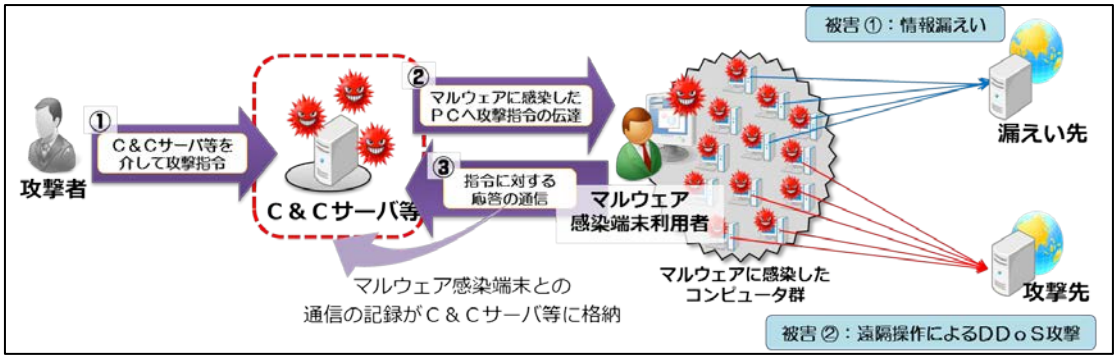

図５　C&C サーバ等を通じた攻撃

昨今では、ISP と連携したセキュリティ事業者や捜査機関等が C&C サーバ等をテイクダウン[14]する事例も出てきている。

一般的に、マルウェアに感染しているコンピュータは、一つの C&C サーバだけから攻撃の指令を受けるわけではなく、複数のものから受けている。このため、一つの C&C サーバをテイクダウンして、その機能を停止させたとしても、別の C&C サーバから攻撃の指令が発せられる可能性があり、マルウェアに感染しているコンピュータは、依然として、情報漏えいやサイバー攻撃の踏み台になる等、不正に操作される危険が続いている状態にある。

C&C サーバ等には、攻撃に係る指令を送る過程で、マルウェアに感染しているコンピュータとの通信の記録（例えば、当該コンピュータの IP アドレスやタイムスタンプ等）が残っている場合があり、テイクダウンされた C&C サーバ等から特に IP アドレス及びタイムスタンプの情報が分かれば、ISP においてタイムスタンプに示された日時分秒において当該 IP アドレスをどの利用者に割り当てたかを確認し、該当利用者を割り出すことで、メール等によって、当該利用者に対して、個別に注意喚起を行うことが可能となる。

---

13 このように、C&C サーバとボットに感染したコンピュータ群から構成される攻撃システムを「ボットネット」という。

14 C&C サーバやボットネットの機能を停止させる行為を指す。

（３）新たなDDoS攻撃であるDNSAmp攻撃の防止

DDoS攻撃は、従来は、「ボット」の感染拡大によるものが多かったが、最近では、必ずしもマルウェア感染によるものではなく、特にDNSの仕組みを悪用したDDoS攻撃（以下「DNSAmp攻撃」という。）等[15]、インターネット上の正常な機能を悪用した攻撃が発生している。平成25年３月には、欧州で、DNSAmp攻撃により特定の機関や企業に対して、300Gbpsを超える最大規模のDDoS攻撃が発生し、欧州地域でインターネットの遅延が起こり、何億人もの利用者に対して影響を与えた[16]。このような攻撃は、マルウェア感染活動に係る通信と異なり、正常な通信と不正な通信の見分けがつきにくいため、従来のマルウェア感染駆除や感染防止の取組では対応ができないという問題がある。

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、攻撃先に増幅されたパケットを何度も送り、大量のトラヒックを発生させる攻撃である。

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[17]の問合わせがあった場合には、増幅された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。）。

ⅱ　その後、攻撃者は、発信元IPアドレスをDNSAmp攻撃の標的（以下「攻撃先」という。）のものに詐称して、一般のインターネット利用者が設置しているブロードバンドルータ等インターネット接続のためのゲートウェイに対して名前解決要求を出し[18]【図６の①部分】

---

15 小さなパケットを送るだけで、その何倍ものサイズにパケットを増幅（amplification）させる性質の攻撃をAmp攻撃と呼び、DNSの仕組みを悪用したものについてはDNSAmp攻撃と呼ばれる。

16 平成25年３月にスパム対策組織のSpamhaus Projectやインターネットセキュリティ会社のCloudflare社に対し、300Gbpsを超える大量のトラヒックを発生させたDDoS攻撃が１週間以上にわたって継続的に発生。攻撃によりインターネット全体が崩壊寸前まで追い込まれた、もしくはある地域のインターネットが長期にわたって継続的にダウンしたといった事実は確認されなかったものの、欧州の複数のインターネットエクスチェンジ（ISP同士のトラヒックを交換する相互接続点）において一時的な遅延や通信障害が発生した。Cloudflare社の調査により、今回の攻撃は要求に対して応答を返すというDNSサーバのリフレクターとしての特性を悪用したもの（DNSAmp攻撃）であり、攻撃においてはその中でもオープンリゾルバ（※）と呼ばれる脆弱性を有したDNSサーバが悪用されたことが判明（Cloudflare社資料より）。

※　オープンリゾルバ：不適切な設定やデフォルト設定の不備などにより本来必要なアクセスコントロールが実施されていないため、インターネット上のどこからの要求であっても応答を返してしまう状態にある脆弱性のこと。

17 ドメイン名からIPアドレスを得る行為のことを指す。

18 ブロードバンドルータ等のゲートウェイへの名前解決要求は、ゲートウェイに接続されているコンピュータ等の端末から行われるのが通常であるが、ゲートウェイの中にはネッ

iii　当該ブロードバンドルータ等のゲートウェイはISPのDNSサーバを経由して当該攻撃用DNSサーバに問合せを行い【図６の②、③部分】

iv　当該攻撃用DNSサーバは当該問合せに対応して、上記ｉの増幅されたパケット（問合せに係る通信量と比較して増幅した応答となっている。）をISPのDNSサーバを経由して送信元として詐称された攻撃先IPアドレスに送信する【図６の④、⑤、⑥部分】。

この一連の攻撃が、複数のゲートウェイに対し、複数回行われることで、攻撃先のシステムに多大な影響が発生する。

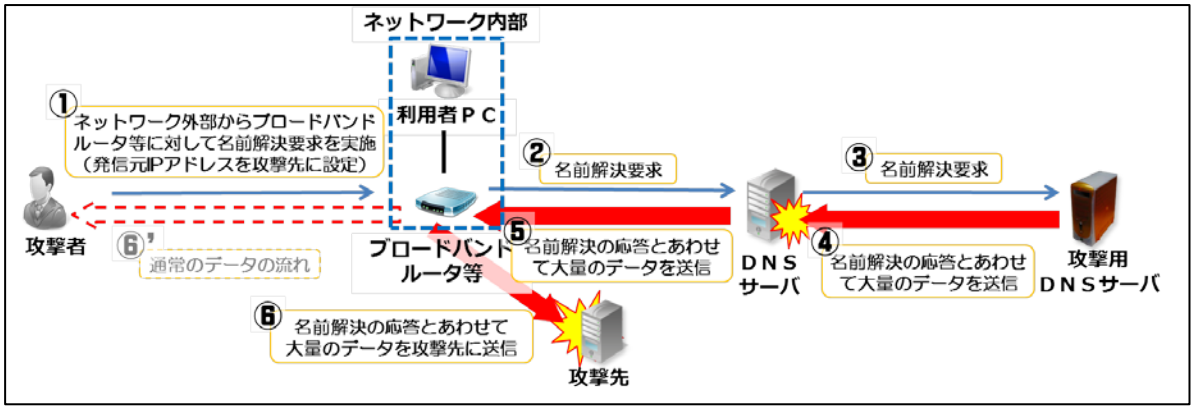

図６　DNSAmp攻撃

日本国内においても、複数のISPがDNSAmp攻撃によるものと見られるDDoS攻撃を受けたという報告があり、ISPによるインターネット接続役務等の電気通信役務を安定的に運用するためには、このような新たな攻撃への対策を検討する必要がある。

DNSAmp攻撃を未然に防止するためには、インターネット利用者が設置しているブロードバンドルータ等のインターネット接続のためのゲートウェイに対して、ネットワークの外側から名前解決要求を行う通信をブロックする手段が考えられる。

一般的に、インターネット利用者にISPから割り振られているIPアドレスは、動的IPアドレス[19]であって、名前解決要求を行う通信は、UDP53番ポート[20]に対して送信される。そこで、ISPのネットワーク網の入口又は出口

トワーク外部からの名前解決要求にも応答するようになっているものがあり、DNSAmp攻撃はこの性質を悪用したものである。

[19] インターネットに接続された機器に一意に割り当てられたIPアドレスについて、接続のたびに異なるIPアドレスが割り当てられるものを「動的IPアドレス」と呼び、常に決まったIPアドレスが割り当てられるものを「固定IPアドレス」と呼ぶ。

[20] UDP（User Datagram Protocol）はトランスポート層における通信プロトコルの１つであり、DNSの名前解決要求に関する通信については、高速に処理を行うために通常UDP

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確認し、動的 IP アドレス宛てであって UDP53 番ポートに対して送信された通信を割り出し、これを遮断する方法が考えられる。

なお、DNSAmp 攻撃における DNS の仕組みと同様に、ネットワークに接続される機器の時計を正しい時刻へ同期するための仕組み（Network Time Protocol）を悪用した攻撃（NTPAmp 攻撃）も直近では発生している。

このようなインターネット上の正常な機能を悪用した攻撃は、今後も発生してくるものと考えられることから、それぞれの攻撃の実態や影響を分析し、考えられる具体的な対策を検討したうえで、その実現のためには通信の秘密の観点からどのような課題があるのか等について、引き続き検討していくことが必要である。

（４）SMTP 認証の情報を悪用したスパムメールへの対処

スパムメールについても、新しい手法が出現している。

一般的に、利用者が電子メールを送信する際は、当該利用者が契約している ISP の SMTP サーバ[21]に対して、正規の利用者であることの認証が行われている。

最近のスパムメールは、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・パスワードを用いて不正に SMTP サーバにアクセスし、正規の利用者になりすまして、大量のスパムメールを送信するという類型のものがある。具体的事例として、なりすましが複数回にわたり行われ、その結果、瞬時に通常の数百倍の通信量が発生し、ISP の SMTP サーバ内で送信メールが滞留したことにより、電子メールの遅配が発生したものがある。

さらに、この現象は、一見すると、ある ISP の SMTP サーバから大量のスパムメールが送信されているように見えるので、海外の Spamhaus 等のスパムメール送信元ブラックリスト作成団体が作成しているスパムメールの発信元リストに当該 ISP の SMTP サーバの IP アドレスが掲載され、当該リストの提供を受けた組織において、当該 ISP からの通常の電子メールの受信が拒否されてしまうという被害も発生している。

このような攻撃は、正規の利用者のインターネット利用を阻害し、ひいては、ISP の電気通信役務の安定的な提供に支障を及ぼすものであるため、対策を講じる必要がある。

が使用される。また、ポート番号は、コンピュータが通信に使用するプログラムを識別するための番号であり、DNS については 53 番ポートが使用されている。

[21] SMTP（Simple Mail Transfer Protocol）サーバはメールを送信するときに接続するサーバである。

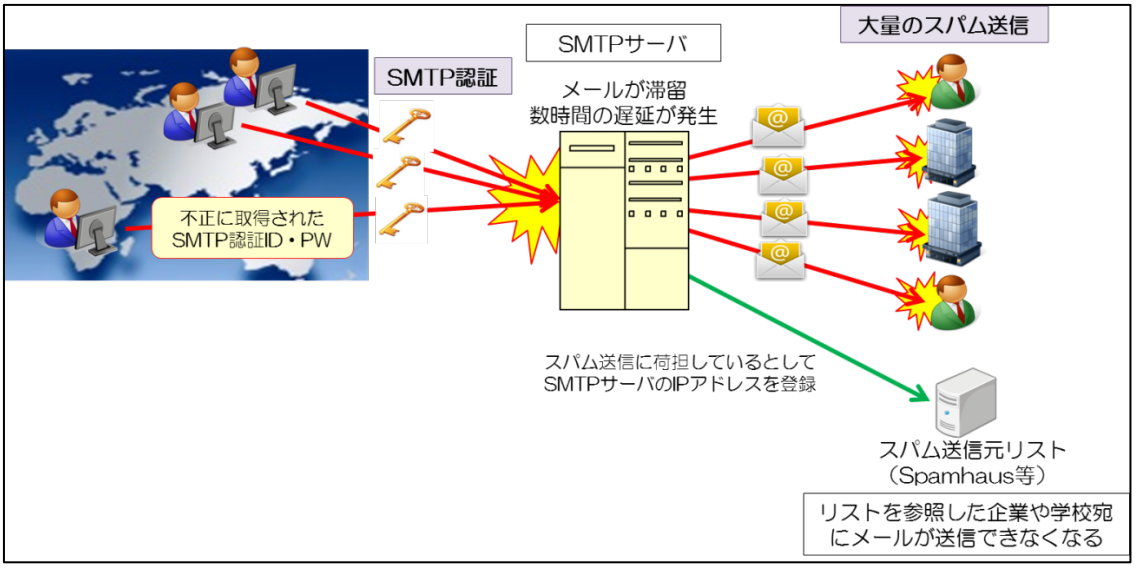

図７　SMTP 認証の情報を悪用したスパムメールの送信

具体的な対策としては、①SMTP 認証の ID・パスワードを不正に利用されていると思われる利用者に対する注意喚起、②大量の SMTP 認証の失敗を発生させている特定の IP アドレスからの SMTP 認証の遮断が考えられる。

①は、ISP において SMTP サーバの負荷が急増した際に、当該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、同一の SMTP 認証において、瞬時に別の国や地域に移動している発信元 IP アドレスがある場合には、当該 SMTP 認証の ID・パスワードは不正に利用されていると考えられることから、当該 ID からの SMTP 認証を一時的に停止するとともに、正規の利用者に対して個別に連絡を取り、パスワードの変更を依頼する方法である。

②については、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（頻度）を分析し、特定の IP アドレスから当該認証の失敗が短期間に大量に発生している場合には、SMTP 認証の ID・パスワードが不正に取得される可能性が高いことから当該 IP アドレスからの SMTP 認証を遮断する方法である。

（５）サイバー攻撃の未然の防止と被害の拡大防止

サイバー攻撃の未然の防止と被害の拡大防止についても検討課題として挙げられた。

①　サイバー攻撃の未然の防止

サイバー攻撃が実際に行われるまでには、例えば、ソフトウェアの脆弱性を突いてマルウェアをダウンロードさせる攻撃の場合は、当該マルウェアのダウンロードに係る通信が発生するため、これらの通信の特徴を捉えて、当該通信を遮断する方法が対策として考えられる。

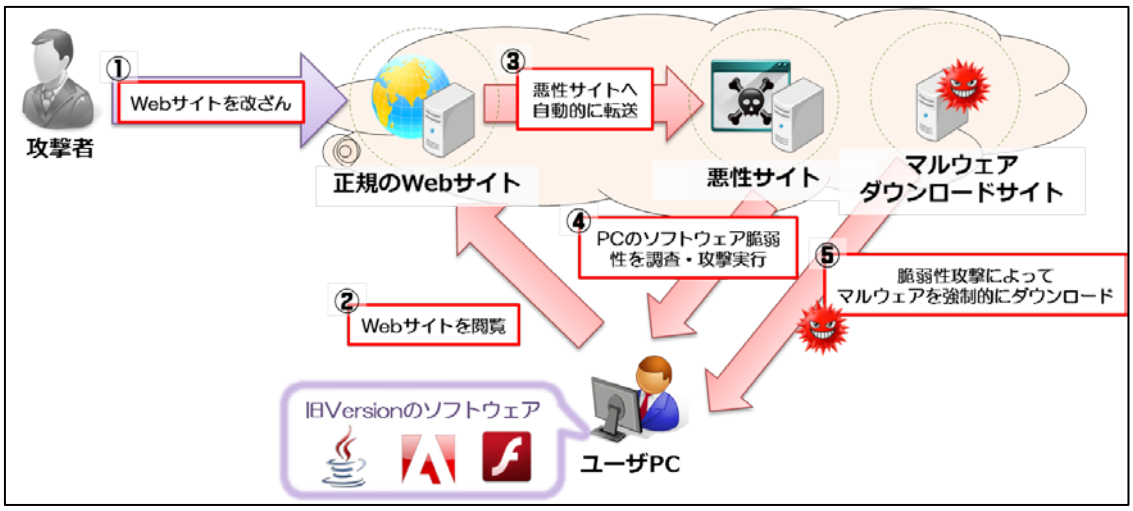

図８　ソフトウェアの脆弱性を突いた攻撃

特に、ソフトウェアに脆弱性があることが判明してから修正プログラムが提供されるまでの前に攻撃が行われた場合（いわゆる「ゼロデイ攻撃」）、コンピュータがマルウェアに感染する可能性は非常に高くなる。このため、マルウェア感染防止の根本的な対策として、サイバー攻撃に係る通信を遮断することが考えられるが、その実現可能性も含め、慎重な検討が必要である。

② サイバー攻撃の被害の拡大防止

一般的に、通信は送信者と受信者の双方が存在することで成立するものであり、DDoS 攻撃等のサイバー攻撃においても送信者（攻撃者）と受信者（攻撃先）が存在し、送信者及び受信者の背後には、それぞれにインターネット接続サービスを提供する複数の ISP が存在している。そこで、インターネットの運用に多大な影響を及ぼすサイバー攻撃に対して、攻撃に関する情報を多く持つ ISP が、業界横断的に情報を共有すること等により、被害拡大の防止が期待できる。

具体的な連携が期待できる場面としては、例えば DDoS 攻撃発生時に、攻撃先側の ISP において攻撃を認識し、攻撃者側の ISP と情報共有を図ることで当該攻撃に対処する場合や、攻撃先側・攻撃者側の二事業者間にとどまらず、多くの事業者間で広く情報を共有することで、攻撃の被害を受けていない ISP においても事前に対策を講じる場合等が考えられる。

このため、サイバー攻撃の被害の拡大防止あるいは未然防止等のため、ISP 間でどのような業界横断的な連携が可能か、検討する必要がある。

第２章　通信の秘密についての基本的な考え方

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[22]。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[23]。

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[24]。

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。

---

22 日本国憲法
第 21 条
２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

23 電気通信事業法
（秘密の保護）
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。
第179条　電気通信事業者の取扱中に係る通信（第164条第２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。

24 東京地裁平成 14 年４月 30 日判決は、「「通信の秘密」には、通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数なども含まれると解する。」と判示している。

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、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[25, 26]。

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。

（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。

---

25 第二次提言 12 頁より。

26 なお、スパムメールのフィルタリング（脚注 49 参照）サービスと通信の秘密の保護の関係の検討においては、原則としてデフォルトオフによる同意取得を条件として提供すべきとしながらも、以下の５要件全てを満たす場合には、例外的に通信当事者から同意が得られたものと同視し得るとして、フィルタリングをデフォルトオンの状態で提供することも可能とされてきた。①利用者が、いったんフィルタリングの提供に同意した後も、随時、任意に同意内容を変更できること、②フィルタリング提供に対する同意の有無にかかわらず、その他提供条件が同一であること、③フィルタリングの内容等が明確に限定されていること、④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、⑤利用者に対して、フィルタリングの内容等につき事前の十分な説明を行うこと。（第二次提言 12 頁より）

「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[27]。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[28]。

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[29]。

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[30]、

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[31]

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[32]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、

---

27 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。

28 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。

29 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。

30 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、一般社団法人日本インターネットプロバイダー協会、一般社団法人日本ケーブルテレビ連盟「インターネット上の自殺予告事案への対応に関するガイドライン」（平成 17 年 10 月）より。

31 「安心ネットづくり促進協議会法的問題検討サブワーキング報告書」（平成 22 年３月）より。

32 例えば、裁判官の発付した令状に従って通信履歴を捜査機関に提供する場合。

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[33]。

[33] 第二次提言より。

第３章　具体的検討

第１章第２節に記載した最近のサイバー攻撃に係る課題の対策例に基づき、前章を踏まえ、当該対策例と通信の秘密との関係について以下のとおり検討を行った。

第１節　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

（１）　問題の所在

ACTIVE におけるマルウェア感染防止の取組の概要は、マルウェア配布サイトの URL 情報をリスト化し、利用者がマルウェア配布サイトにアクセスしようとする場合に、ISP が、リスト化されたマルウェア配布サイトへのアクセスに係る IP アドレス又は URL を検知し、そのアクセスを一時停止した上で、当該サイトへのアクセスを継続するか否か確認する注意喚起画面等を表示するものである。このような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利用等されるアクセス先URL 又は IP アドレスは、通信の構成要素であり、通信の秘密の保護の対象であることから、利用者の有効な同意がない限り、通信の秘密の窃用等に該当し、通信の秘密の侵害となる。

通信の秘密についての同意は、前章第３節（２）で述べたとおり、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らず、個別の同意でなくてはならないと解されている。しかしながら、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 の利用等に当たり、常に個別の同意を必要とすれば、当該取組の普及が滞り、マルウェア感染の防止が進まないといった問題がある。そこで、この場合に関しては、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、有効な同意ということはできないか検討を行う。

（２）　考え方

前述のとおり、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[34]のものであり、通信の秘密の利益を放棄させる

[34] なお、法務省「民法（債権関係）の改正に関する中間試案（平成 25 年２月）」の「第 30 約款」では、「２ 約款の組入要件の内容」として「契約の当事者がその契約に約款を用いることを合意し，かつ，その約款を準備した者（以下「約款使用者」という。）によって，

内容はその性質になじまないこと、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ことが挙げられる[35]。なお、理由②を補足すると、同意の対象・範囲が不明確となることにより、利用者に不測の不利益が生じることに問題意識がある。

これを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考えてみると、理由①との関係では、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。

理由②との関係では、契約約款による包括同意であっても、利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる(設定変更できる)契約内容であって、そのことについて利用者に相応の周知が図られており、注意喚起画面等においても、本件注意喚起対策の説明に加え、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こと及びその方法が説明されている場合には、契約約款による包括同意当時において予測し得なかった事情が将来生じた場合についても、随時、利用者が同意内容を変更することができることから、将来、利用者が不測の不利益を被る危険を回避できる。

したがって、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、

ア. 利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる(設定変更できる)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こと

契約締結時までに，相手方が合理的な行動を取れば約款の内容を知ることができる機会が確保されている場合には，約款は，その契約の内容となるものとする。」と、「3 不意打ち条項」として「約款に含まれている契約条項であって，他の契約条項の内容，約款使用者の説明，相手方の知識及び経験その他の当該契約に関する一切の事情に照らし，相手方が約款に含まれていることを合理的に予測することができないものは，上記2によっては契約の内容とはならないものとする。」と記載されている。

[35] 第二次提言 12 頁より。

イ．　当該契約約款の内容及び事後的に同意内容を変更できる（設定変更できる）ことについて利用者に相応の周知[36]が図られており、

ウ．　注意喚起画面等においても、本件注意喚起対策の説明に加え、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）こと及びその方法が説明されている（これらの説明がなされたウェブサイトへのリンクの掲載等）

場合であれば、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考えられる。

上記の契約約款においては、少なくとも以下のような内容を規定すべきと考えられる。

＜契約約款に記載すべき事項＞

・　検知を行うこと

（例）検知を行う

・　ウェブアクセスに係る通信の検知の目的

（例）利用者がアクセスしようとするウェブサイトが、アクセスするとマルウェアに感染する可能性が高いサイトである場合には、アクセスを一時停止し、注意喚起を行うため

・　検知の時期

（例）利用者がウェブサイトに対するアクセス要求をした際

・　検知の対象となる情報の範囲

（例）利用者のアクセス要求に係るアクセス先 IP アドレス又は URL について

・　事後的に同意内容を変更できる（設定変更できる）こと

（例）当該検知等は、利用者が設定変更を申し出た場合、中止できる

[36] 当該契約約款の内容及び事後的に同意内容を変更できる（設定変更できる）ことについて、ウェブサイトへの掲載を始め利用者にわかりやすい方法により、周知を図ることが推奨される。

また、注意喚起画面の例としては、下図のようなものが考えられる[37]。

注意喚起のイメージ

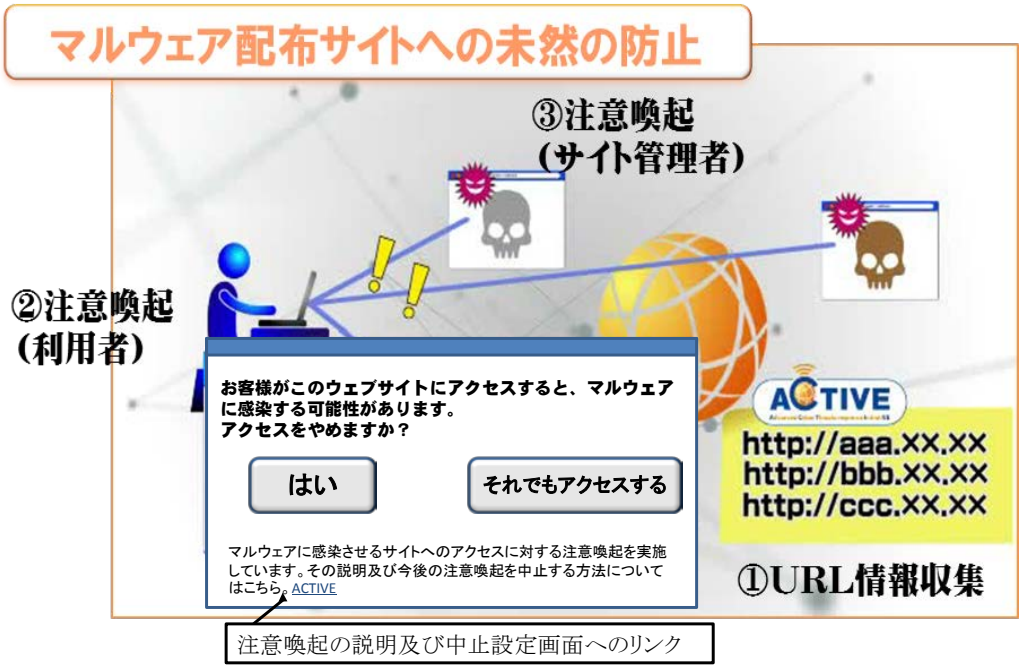

図９　注意喚起のイメージ

なお、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取得した通信の秘密に当たる情報（アクセス先 IP アドレス又は URL）を当該注意喚起以外のために利用することは、同意の範囲を超えることとなるため、通信の秘密の窃用となり、通信の秘密を侵害することとなる。

第２節　マルウェア感染駆除の拡大

（１）　対策の概要及び問題の所在

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（以下「マルウェア感染端末」という。）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

[37] 注意喚起画面については、ISP の名称を入れる等、同画面を見た利用者が注意喚起の主体を了知できるよう配慮することが望まれる。

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が考えられる[38]。

これについて、通信の発信元 IP アドレス及びタイムスタンプは、通信の構成要素として通信の秘密の保護の対象であることから、ISP において、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、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すことは、通信の秘密の窃用等に該当する可能性がある。もっとも、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ところ、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。

（２） 緊急避難該当性

① 現在の危難の存在

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から、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ることができる[39]。

こうした制御がなされることにより、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、深刻な被害につながるものである。

② 法益の権衡

本件対策によって避けようとする害は、上記①のとおり看過し難いものであり、他方、上記対策を講ずるに当たって侵害される通信の秘密は、ISP において、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、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、該当利用者を割り出すという限度であり、そ

---

[38] C&C サーバは、ボットネットに指令を送る制御サーバであり、このような C&C サーバと通信をしていることそれ自体から、C&C サーバと通信を行ったコンピュータ等の端末は、マルウェアに感染している可能性が極めて高い。また、通常、C&C サーバとボットとの通信の暗号化や、C&C サーバへのアクセスの認証制限等、第三者がボットネット等のマルウェアネットワークに侵入することを拒む仕組みが実装されており、特殊な方法を用いなければ、C&C サーバとの通信は困難であることから、マルウェアに感染していないコンピュータ等の端末が C&C サーバと通信を行うことは通常想定できない。

[39] 一般的に検知されているマルウェアにおいては、感染すると DDoS 攻撃等のサイバー攻撃の踏み台となることや、端末機器に保存された情報の漏えいやデータの破壊・改ざん等、深刻な実害を及ぼすような危険な振る舞いをするものが多数を占めている。

の確認結果を感染者への注意喚起以外の用途で利用しない場合には、法益の権衡を認めることができると考えられる。

③　補充性

マルウェア駆除を促すための利用者への他の対応方法としては、インターネットを通じた一般的な注意喚起や、C&C サーバ等に蓄積されていた IP アドレス等の通信の記録を公開して注意を喚起することも考えられるが、インターネット利用者の多くは、自らサイバー攻撃の被害を受けない限り具体的な行動には移りにくいと考えられるため、インターネットを通じた一般的な注意喚起ではマルウェアの駆除という所期の目的を達成することが困難である[40]。

また、C&C サーバ等に蓄積されていた IP アドレス等の通信の記録を公開して注意を喚起する方法についても、通信時に自己が使用した IP アドレスを認識又は記録している利用者はまれであるため、IP アドレスの公開は注意喚起として実効性に欠けるだけでなく、マルウェア感染端末に係る IP アドレスが第三者に明らかにされることにより、それらの端末が更なる攻撃の標的にされるおそれがある。

以上から、本件対策以外には、マルウェアの駆除という所期の目的を達成するための有効な手立ては考え難く、補充性についても認めることができると考えられる。

④　まとめ

以上から、本件対策は、当該 IP アドレスをどの利用者に割り当てたか確認した結果を感染者への注意喚起以外の用途で利用しない場合には、緊急避難として違法性が阻却されると考えられる。

第３節　新たな DDoS 攻撃である DNSAmp 攻撃の防止

（１）　対策の概要及び問題の所在

DNSAmp 攻撃を未然に防止するためには、その引き金となっている、利用者が設置しているブロードバンドルータ等のゲートウェイに対するインターネット側からの名前解決要求に係る通信をブロックする必要があり、このような通信は、一般的には、動的 IP アドレス宛てであって UDP53 番ポート

[40] ある ISP では、平成 17 年に Antinny 対策において、ウェブ媒体や利用者への一斉メールによる一般的な注意喚起を行ったが、これにより対策を行った利用者は８％未満であった。他方、利用者に個別に注意喚起を実施した場合、電話やメール、郵送等、手法により差はあるが、少なくとも 30%以上の利用者が対策を行った。

に対して送信された通信である。そこで、ISPの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て、動的IPアドレス宛てであってUDP53番ポートに対して送信された通信を割り出し、これをブロックすることが考えられる。

通信の宛先IPアドレス及びポート番号は、通信の構成要素として通信の秘密の保護の対象であるから、これらを常時確認し、動的IPアドレス宛てであってUDP53番ポートに対して送信された通信を検知し、ブロックすることは、通信の秘密の窃用等に該当する。もっとも、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ところ、上記対策は、常時行われる対策であり、一般的には、急迫性、現在の危難といった要件を満たさないため、正当防衛又は緊急避難には該当しないが、正当業務行為に当たる場合には違法性が阻却される。そこで、正当業務行為に当たると考えることが可能か否かについて検討する。

（２）　正当業務行為該当性

①　目的の正当性

利用者のブロードバンドルータ等のゲートウェイを悪用したDNSAmp攻撃は、前述のとおり平成25年３月、欧州において、300Gbpsを超える過去最大規模の攻撃が発生し、欧州地域でインターネットの渋滞がみられ、何億人もの人々が影響を受けた[41]ほか、国内においても、あるISPでは平成25年４月から12月までの間、35回もDNSAmp攻撃の被害が発生している。また別のISPにおいても頻繁にこのような攻撃を受けており、平成25年には国内最大規模の攻撃が発生し、あるISPのすべてのDNSサーバがプロセスを停止し、全利用者が約40分間にわたりインターネットが使えない状態に陥った。

DNSAmp攻撃が発生した場合には、攻撃に利用された側のISPだけでなく、攻撃先が属するISPにおいても回線が逼迫して輻輳等の現象が発生し、攻撃先と同一回線に収容されている利用者の電気通信役務利用を妨げることとなる。

このようなDNSAmpによるDDoS攻撃を防止する措置は、ISPにおいて、自社のDNSサーバが過負荷状態となることによる、インターネットアクセスやメール送信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、目的の正当性を認めることができると考えられる。

[41] 脚注16参照。

② 行為の必要性

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、攻撃先に増幅されたパケットを何度も送り、大量のトラヒックを発生させる攻撃である。

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増幅されたパケットを応答するものを用意し

ⅱ その後、送信元 IP アドレスを攻撃先 IP アドレスに詐称させて、一斉に利用者が設置しているブロードバンドルータ等のゲートウェイに対してインターネット側から名前解決要求を出し【図６の①部分】

ⅲ 当該ブロードバンドルータ等のゲートウェイから、ISP の DNS サーバを経由して、当該攻撃用 DNS サーバに問合せをさせ【図６の②、③部分】

ⅳ 当該攻撃用 DNS サーバから、問合せに対応して、上記ｉの増幅されたパケット（問合せに係る通信量と比較して増幅された応答となっている。）を、ISP の DNS サーバを経由して、送信元として詐称された攻撃先 IP アドレスに送信する【図６の④、⑤、⑥部分】。

DNSAmp 攻撃を防止するために、攻撃用 DNS サーバのすべてを発見して対応を講ずることは現実的ではないため、上記ｉの部分での対応は困難である。次に、上記ⅲ及びⅳの部分での対応についても、ISP としては、自社の DNS サーバ上の通信の挙動等を仮にモニタリングしたとしても、DNSAmp 攻撃に係る通信は、外形上は通常の名前解決要求であり、しかも、その発信元についても詐称された者からの通常の通信に見えることから、他の正常な通信と区別することができないため、この部分での対応は困難である。

また、DNSAmp 攻撃は、ISP の DNS サーバに大きな影響を与えることから、一旦攻撃が発生すればただちに大規模な被害に至るほか、利用者のブロードバンドルータ等のゲートウェイには通信ログが残らないのが通常の仕様であること等から、攻撃者の事後追跡も困難である。

他方、上記ⅱの部分においては、利用者のブロードバンドルータ等のゲートウェイは、通常、利用者のコンピュータ等の端末側からの名前解決要求を受け付け、インターネット側にある利用者が所属する ISP の DNS サーバに名前解決要求を行うものであり、インターネット側から名前解決要求を受けることは通常想定されていないため、このような通信のみを検知してブロックすることが可能であり、それによって DNSAmp 攻撃を防止することができる。利用者が設置するブロードバンドルータ等のゲートウェイ

には、通常、動的 IP アドレスが割り当てられており[42]、TCP/IP プロトコル上、名前解決要求に関しては UDP53 番ポートが使用されることから、利用者が設置しているブロードバンドルータ等のゲートウェイに対するインターネット側からの名前解決要求に係る通信は、動的 IP アドレス宛てであって UDP53 番ポートに対して送信された通信であり、このような通信をブロックするためには、ISP の網の入口又は出口において、管理下の動的 IP アドレス向けに入ってくる通信を検知し、UDP53 番ポートに入ってくる通信のみ遮断することとなる。この場合、DNSAmp 攻撃を防止するために、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て、該当する通信をブロックする必要がある。

③　手段の相当性

本件対策を講ずるに当たって侵害される通信の秘密は、宛先 IP アドレス及びポート番号のみであり、これを機械的・自動的に確認して、動的 IP アドレス宛てであって UDP53 番ポートに対して送信された通信を検知しブロックする限度であるから、その確認結果を本件対策以外の用途で利用しない場合であれば、通信の秘密侵害の程度は相対的に低いということができる。しかも、前述のとおり、通常の通信環境下においては、ブロックの対象となる動的 IP アドレスに対するインターネット側からの名前解決要求は想定されないため、このような通信をブロックすることによる通常のインターネット利用への影響は考え難く、以上によれば、手段の相当性についても肯定することができると考えられる。

④　まとめ

以上から、本件対策は、宛先の IP アドレス及びポート番号を確認した結果を DNSAmp 攻撃の防止以外の用途で利用しない場合には、正当業務行為として違法性が阻却されると考えられる。

[42] 通信の宛先のポート番号が UDP53 番ポートであっても宛先の IP アドレスが固定 IP アドレスである通信については、利用者がインターネットアクセスの際に通常利用することとなる ISP 自身の DNS サーバ（同サーバには固定 IP アドレスが割り当てられている。）への名前解決要求や、利用者が設置した固定 IP アドレスを割り当てられた DNS サーバへの名前解決要求等、ブロックすべきではない通信が存在する。

第４節　SMTP 認証の情報を悪用したスパムメールへの対処

（１）　対策の概要及び問題の所在

他人の SMTP 認証の ID・パスワードを悪用したスパムメールの送信を防止するには、SMTP サーバの負荷が急増し警告が出た場合、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 を分析することにより、スパムメールが一の 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[43]について、当該 ID からの SMTP 認証を一時停止するとともに、その ID・パスワードを不正に利用されている利用者に対し、個別に連絡を取り、パスワードの変更を依頼することが考えられる（以下「対策１」という。）。

さらに、SMTP 認証の ID・パスワードの不正取得それ自体を防ぐために、大量の SMTP 認証の失敗が発生し警告が出た場合、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（頻度）を分析し、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のアカウントハッキング[44]である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 SMTP 認証を止めることで、SMTP 認証の ID・パスワードの不正取得を防ぐことが考えられる（以下「対策２」という。）。

対策１については、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 アドレスや、タイムスタンプ、メールアドレス及び SMTP 認証の ID は、通信の構成要素として通信の秘密の保護の対象であるから、これらを分析し、不正利用の蓋然性が高い ID からの SMTP 認証を一時停止等することは、通信の秘密の窃用等に該当する可能性がある。また、対策２についても、SMTP 認証ログ（発信元 IP アドレス、タイムスタンプ、認証回数、認証間隔（頻度））を分析し、アカウントハッキングである蓋然性が高いものについて、当該 IP アドレスからの SMTP 認証を一時停止することは、通信の秘密の窃用等に該当する可能性がある。

43　例えば、①送信元メールアドレスを確認して、同一のメールアドレスから大量のメールが送られていること等を確認し、②当該メールアドレスに係る SMTP 認証のアカウントについて、認証の発信元 IP アドレスを確認し、③その結果、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ことを認知した場合。

44　ID・パスワード等のアカウント認証を破る行為。

しかしながら、いずれにしても、両者の対策については、以下のとおり、少なく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。

（２） 対策１について

① 目的の正当性

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。

このような状況に対処するため、対策１をとる目的は、ISP において、SMTP 認証の ID・パスワードの不正利用を防止することにより、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とともに、SMTP 認証の ID・パスワードを不正に利用したスパム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送信の遅延等を防止し[45]、もって、電気通信役務の安定的運用を図ることにあり、目的の正当性を認めることができると考えられる。

② 行為の必要性

大量のメールが一の SMTP 認証の ID を用いて送信されているにもかかわらず、当該認証に係る発信元 IP アドレスが瞬時に別の地域・国に移動している場合[46]、当該 SMTP 認証の ID・パスワードが不正に利用され、スパムメールの大量送信が行われている蓋然性が高い。

このため、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 を分析することにより、上記の特徴を有する SMTP 認証の ID を特定した上で、当該 ID からの SMTP 認証を一時停止するとともに、その ID・パスワードを不正に利用されている利用者に対し、個別に連絡を取り、パスワードの変更を依頼することは、上記目的との関係で、行為の必要性を肯定できると考えられる。

---

45 平成 25 年 11 月、大手 ISP において、利用者の SMTP 認証の ID・パスワードが不正利用され、当該 ID から、数時間のうちに数十万通～数百万通規模のスパムメールが発信され、その影響によりメールが滞留して送信遅延が発生し、復旧に約 18 時間を要したことがあった。

46 例えば、特定の SMTP 認証の ID に対し、1 日で国をまたがった 1000 以上の IP アドレスから認証が行われ、スパムメールが送信されるような事例が日常的に発生している。

③　手段の相当性

そして、分析する通信の秘密は、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 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であって、当該 ID からの SMTP 認証の一時停止についても、正規利用者がパスワードを変更する等、不正利用の危険が解消されるまでの間に限られる場合には、手段の相当性も認められる。

以上から、対策１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。

（３）　対策２について

①　目的の正当性

対策２の目的は、ISP において、SMTP 認証の ID・パスワードの不正取得を防止することにより、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ことにあり、目的の正当性を認めることができると考えられる[47]。

②　行為の必要性

特定の IP アドレスから短期間に大量の SMTP 認証失敗が発生した場合には、その認証行為は、アカウントハッキングである蓋然性が高く、当該アカウントハッキングの継続を放置すれば、SMTP 認証の ID・パスワードの不正取得が生じ得ることから、それを阻止するために、当該 IP アドレスからの SMTP 認証を阻止することは、上記目的との関係で、行為の必要性を肯定できると考えられる。

---

47 SMTP 認証の ID・パスワードが不正に取得・利用され大量のスパムメールが送られた事案についての ISP の被害状況の例は以下のとおり。

・A 社：毎月平均 50 件の SMTP 認証の ID・パスワードが不正にスパムメール送信に利用されている（平成 24 年 11 月には２日間で 50 件発生）。

・B 社：10 ヶ月間で 49 件の SMTP 認証の ID・パスワードが不正にスパムメール送信に利用されている（平成 25 年 5 月以降増加傾向）。

・C 社：毎週平均一桁の SMTP 認証の ID・パスワードが不正にスパムメール送信に利用されている（平成 24 年 11 月には１日に 60 件弱のアカウントからのスパム送信が確認）。

③　手段の相当性

また、分析する通信の秘密は、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（頻度）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であって、当該 IP アドレスからの SMTP 認証の一時停止についても、当該攻撃期間中に限られる場合には、手段の相当性も認められる。

以上から、対策２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。

第５節　サイバー攻撃の未然の防止と被害の拡大防止

このほか、サイバー攻撃の未然の防止と被害の拡大防止について、①サイバー攻撃に係る通信の遮断及び②サイバー攻撃が発生した場合の ISP 業界横断的な連携の実施については、主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及び一般社団法人日本インターネットプロバイダー協会を中心に検討が進められ、以下のとおり報告があった。

①　サイバー攻撃に係る通信の遮断

対策の対象となる「サイバー攻撃に係る通信」については、通信システムの停止に至らせるような外部からの攻撃、攻撃指令を第三者に伝達する通信、OS 等のソフトウェアのセキュリティホールをつくような外部からの攻撃等、多種多様なものが考えられる。通信を遮断するためには、まず、どのような通信を検知し、どのような場合にその遮断を行うのか、対策の対象を明確化する必要があることから、今後、これらの整理について、ISP において引き続き慎重に検討を進めることが必要である。

さらに、対象を明確化した上で、それぞれについてどのような対策を講ずることが可能かつ有効なのか検討することも必要である。例えば、これまでも、ISP は、OP25B[48]やスパムメール等のフィルタリング[49]等、様々な対策を

---

48 Outbound Port 25 Blocking。ISP の網内の動的 IP アドレスから外部の IP アドレスに対して TCP25 番ポートの通信を行うことを禁止すること。契約者のコンピュータから ISP のメールサーバを経由せずに直接外部に迷惑メールが送信されることを防ぐため、ISP において実施されている。

49 一定の条件に基づいてデータ等を選別・排除する仕組みのこと。ネットワークの境界等に設置されたファイアウォールやルータ等が、内外で送受信されるデータのパケットの中から一定の基準に基づいて不正なものを検知し、破棄する機能を「パケットフィルタリング」、メールソフトやメールサーバ等が、受信したメールの内容や添付ファイル等からスパムメールやウイルスメールと疑わしいメールを選別し、専用のフォルダに集めたり破棄したりする機能を「スパムフィルタリング」、「メールフィルタリング」等という。青少年保護等を目的として、インターネット上にある性的あるいは反社会的な情報を含んだサービスやウェブサイトを一定の基準に基づいて選別し、青少年の利用する携帯電話やウェブブ

講じてきたところであり、これらの他にも、技術革新に伴い、新たな対策の可能性も期待できる。これらの対策は、当然、場合によって有効性は異なる上、特に、ヘッダやパケットの中身等通信の秘密を検知する行為を要する場合もあることから、通信の秘密の侵害可能性にも留意した上で、検討する必要がある。

② サイバー攻撃が発生した場合の ISP 業界横断的な連携の実施

ISP の業界横断的な連携の目的は、サイバー攻撃が発生した場合の被害拡大の防止、あるいは、サイバー攻撃の予兆を捉え、その予防的な措置を行うことであるが、連携が必要となる場面は、問題となっているサイバー攻撃の動向や ISP それぞれの状況によって異なってくると考えられる。このため、今後、具体的なモデルケースについて、ISP において、引き続き整理を行い、検討を進めることが必要である。

さらに、モデルケースをいくつか想定した上では、それぞれの場合に、どのような対策を講じていくことが可能かつ有効なのか、検討することも必要である。例えば、業界横断的な連携が必要となる場面として、DDoS 攻撃が発生している間に、当該攻撃を受けている利用者にインターネットサービスを提供している ISP(A)が攻撃を認識し、ISP(A)が、当該攻撃を行っている者に対してインターネットサービスを提供している ISP(B)に連絡を行い、ISP(A)及び(B)の間で情報共有を図り、当該攻撃に対処することが考えられるが、具体的にどのような情報を共有することが可能で、また、どのような情報が必要なのか、それはいつの時点か等、詳細なシミュレーションが不可欠となる。

ラウザから閲覧できないようにするシステムやサービス（コンテンツフィルタリング、未成年フィルタリング）を指すこともある。

第４章　おわりに

本研究会では、最近のサイバー攻撃の動向を踏まえ、優先的に対応すべき課題とその対策について、主に通信の秘密の観点から検討し、一定の整理を行った。

今後は、ISP など電気通信事業者等において、本報告書における整理を踏まえ、大量通信ガイドラインの改定など具体的な取組が行われることを期待する。

また、技術の進歩や新たな攻撃手法の発生などサイバー攻撃を取り巻く環境は絶えず変化していることから、今回引き続きの検討が必要とされた対策も含めて、時宜に適した対策を講じられるよう、今後とも、官民が連携して必要な検討を進め、機動的に対応していくことが重要である。

（参考資料）

○　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　構成員

・　構成員

（座長）	佐伯（さえき）　仁志（ひとし）	東京大学大学院法学政治学研究科教授
（座長代理）	宍戸（ししど）　常寿（じょうじ）	東京大学大学院法学政治学研究科教授
	木村（きむら）　孝（たかし）	一般社団法人日本インターネットプロバイダー協会
	木村（きむら）　たま代（よ）	主婦連合会
	小山（こやま）　覚（さとる）	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
	中尾（なかお）　康二（こうじ）	独立行政法人情報通信研究機構 ネットワークセキュリティ研究所　主管研究員
	藤本（ふじもと）　正代（まさよ）	富士ゼロックス（株）　パートナー／ 情報セキュリティ大学院大学客員教授
	森（もり）　亮二（りょうじ）	英知法律事務所　弁護士

・　ワーキンググループ構成員

（主査）	宍戸（ししど）　常寿（じょうじ）	東京大学大学院法学政治学研究科教授
（主査代理）	森（もり）　亮二（りょうじ）	英知法律事務所　弁護士
	衛藤（えとう）　将史（まさし）	独立行政法人情報通信研究機構 ネットワークセキュリティ研究所　主任研究員
	木村（きむら）　孝（たかし）	一般社団法人日本インターネットプロバイダー協会
	小山（こやま）　覚（さとる）	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
	齋藤（さいとう）　衛（まもる）	株式会社インターネットイニシアティブ サービスオペレーション本部 セキュリティ情報統括室長
	丸橋（まるはし）　透（とおる）	ニフティ株式会社　法務部長
	村主（むらぬし）　亘（わたる）	ソフトバンクテレコム株式会社　お客様相談室

○　開催経緯

＜電気通信事業におけるサイバー攻撃への適正な対処のあり方に関する研究会＞

・　第１回（平成 25 年 11 月 29 日）

－　本研究会の開催趣旨等

・　第２回（平成 26 年２月 19 日）

－　第一次とりまとめ（案）について

・　第３回（平成 26 年３月 25 日）

－　第一次とりまとめ（案）に対する意見募集の結果について

＜ワーキンググループ＞

・　第１回（平成 25 年 12 月 11 日）

－　検討の方向性について

－　関係者からのヒアリング

株式会社 FFRI

トレンドマイクロ株式会社

日本マイクロソフト株式会社

NTT セキュアプラットフォーム研究所

・　第２回（平成 26 年１月 30 日）

－　検討事項に対する整理状況について

・　第３回（平成 26 年２月 14 日）

－　第一次とりまとめ（案）について

＜第一次とりまとめ（案）に対する意見募集の実施＞

（平成 26 年３月４日～３月 17 日）