（別紙１）

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
第三次とりまとめ

平成30年9月

目次

序章 2
第１章　最近のサイバー攻撃に係る課題と対策例 4
第２章　具体的検討 10
第１節　通信の秘密の利用等に関する違法性阻却事由等について 10
第２節　マルウェアに感染している可能性が高い端末の利用者に対する注意喚起について 12
第３節　注意喚起を目的とする、マルウェアに感染している可能性が高い端末の検知について 16
第４節　有効な同意に基づく通信遮断を目的とする、C&C サーバである可能性が高い機器の検知について 18
第５節　マルウェアに感染し得る脆弱性を有する端末の利用者に対する注意喚起について 21
第３章　おわりに 26

（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

○　開催経緯

序章

情報通信技術の発展に伴い、巧妙化、複雑化するサイバー攻撃に対して、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、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、研究会において、優先的に対応すべき課題とそれぞれの課題の解決の方向性について、平成 26 年４月には「第一次とりまとめ」を、平成 27 年９月には「第二次とりまとめ」をそれぞれ公表してきた。インターネット・サービス・プロバイダ（ISP）等の電気通信事業者においても、上記各とりまとめを踏まえて「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」（以下「サイバー攻撃ガイドライン」という。）[1]を改定する等、サイバー攻撃の脅威に対して官民が協働して対処に当たってきた。

上記各とりまとめの公表後においても、インターネット上で人的介在なしに相互に情報交換し、自動的に制御を行うような IoT 機器の利用が爆発的に拡大するなど、サイバーセキュリティを取り巻く環境は変化を続けており、IoT 機器を悪用したサイバー攻撃が広がってきている。具体的には、平成 28 年９月には、マルウェア「Mirai」に感染した約 14 万台以上の IoT 機器から 1.5Tbps の規模の DDoS 攻撃が行われ、南欧諸国から攻撃先の ISP のサーバを利用するサービスへのアクセスがしにくくなり、同年 10 月には、「Mirai」に感染した約 10 万台の IoT 機器から 1.2Tbps の規模の DDoS 攻撃が米国 Dyn 社の DNS サーバに対して行われ、同社から DNS サービスの提供を受けていた世界各国のサービスへのアクセスがしにくくなるという通信障害が発生した。さらに、同年 11 月には、Mirai 亜種のマルウェア「Satori」が登場し、１週間で世界で 26 万台が感染し、日本でも最大 2.4 万の感染ホストが確認された。このようなサイバーセキュリティを取り巻く環境の変化により、国民生活にこれまで以上に大きな影響を与えるおそれが生じている。

そのような中で、研究会では、第二次とりまとめの公表後に発生したサイバー攻撃の動向と環境の変化を踏まえ、引き続き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、ワーキンググループを設けて技術的・制度的な観点から議論を行った上で、電気通信事業者がより能動的にサイバー攻撃に対処できるような取組の実施に向けて条件や留意点等を整理した。

---

[1] 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、一般社団法人 ICT-ISAC が構成する「インターネットの安定的な運用に関する協議会」において策定及び改定。なお、総務省は同協議会にオブザーバーとして参加している。

本とりまとめは、このような議論や検討に基づき、それぞれの課題の解決の方向性について取りまとめたものである。今後、本とりまとめを参照し、電気通信事業者において、引き続き自主的に適正なサイバー攻撃への対処が行われることが期待されるものである。

第１章　最近のサイバー攻撃に係る課題と対策例

（１）　マルウェアに感染している可能性が高い端末の利用者に対する注意喚起

第一次とりまとめにおいて、攻撃者が用意したC&Cサーバ[2]に記録されたマルウェア感染端末のIPアドレスとタイムスタンプの情報等に基づいて、マルウェア感染端末の利用者に注意喚起を行うことについて整理した。本整理を踏まえ、平成26年７月以降、ISPからインターネットバンキングに係るマルウェア感染端末の利用者に対して注意喚起が行われているところである。

この取組を通じてマルウェア感染端末からマルウェアを駆除する試みは一定の成果を上げているが、本取組はあくまでもC&Cサーバに記録された通信履歴等に基づいた注意喚起であるため、C&Cサーバとの間でマルウェアに係る通信を行っていたことが当該C&Cサーバのテイクダウン[3]後の調査によって判明するなど、具体的な根拠に基づいてマルウェア感染端末であるとの確証が得られた後に初めて注意喚起が行われるにとどまっており、その範囲は限定的である。他方、C&Cサーバとの通信については、通信が行われているという事実やその内容について利用者が認知できないままバックグラウンドで実行され、利用者に重大な被害をもたらすとともに、通信ネットワークにも大きな被害をもたらす場合がある。とりわけ、IoT機器は人的管理が難しいものが多いことから、そのような機器の利用者は通信が行われているという事実やその内容についての認知が尚更困難となり、また、IoT機器は演算処理能力が低く、セキュリティソフトを導入できないものが多いことから、利用者側での対処がより困難となってきている。そこで、C&Cサーバ等との通信によって生じる利用者の被害を未然に防止するとともに、ISPの電気通信役務の提供に支障が生じる場合に当該支障を未然に防止するために、マルウェアに感染している可能性が高い端末が把握できた時点における対策の実施について検討する必要がある。

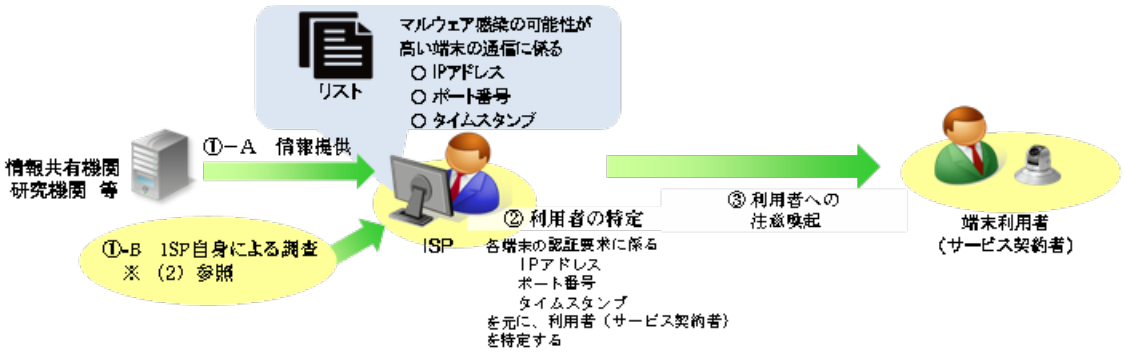
具体的には、信頼できる第三者からの情報提供を受けること、自ら調査を行うこと等により、ISPがマルウェアに感染している可能性が高い端末を認識した場合において、当該端末による通信の送信元IPアドレス、ポート番号及びタイムスタンプと当該IPアドレス及びポート番号の割当て状況を確認して当該端末の利用者を割り出し、電子メールの送付等の方法で個別に注意喚起を行う方法が考えられる。

---

[2] 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。

[3] 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。

一方、通信の送信元 IP アドレス、ポート番号及びタイムスタンプは通信の構成要素であり、ISP において、これらと IP アドレス及びポート番号の割当状況を確認して通信当事者を把握し、注意喚起を行う行為は通信の秘密の侵害に該当し得る。そのため、当該取組の実施に当たっては、どのような場合であれば、通信の秘密に属する事項の利用として許容されるものであるかを検討する必要がある。



【図１　マルウェアに感染している可能性の高い端末の利用者に対する注意喚起】

（２）　マルウェアに感染している可能性が高い端末の検知

（１）のような取組の実効性を向上させるためには、マルウェアに感染している可能性が高い端末を的確に把握した上で、注意喚起を実施する必要がある。

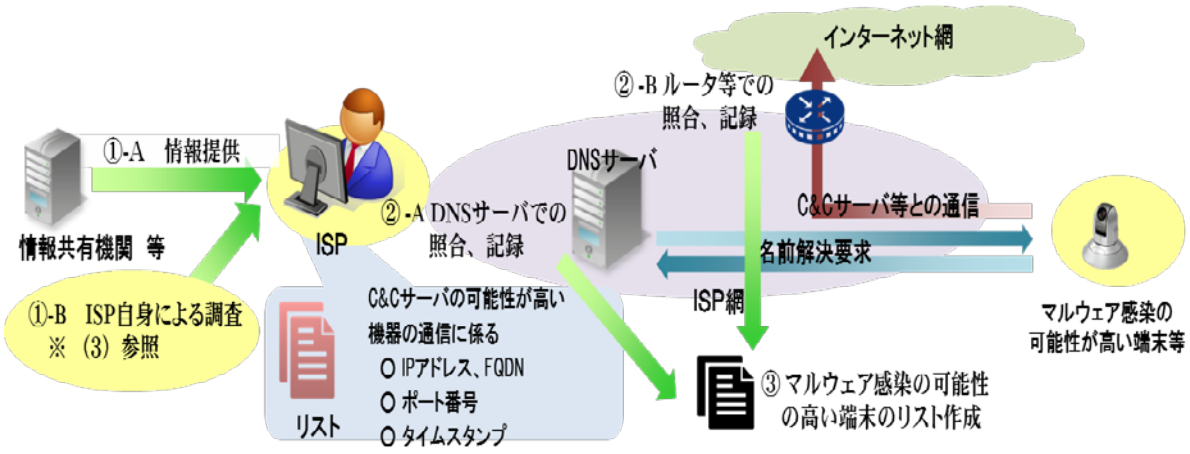
このような端末を把握するための手法としては、ハニーポットを利用して攻撃通信を把握する等の手法が既に実施されているが、これによって把握できるのは、マルウェア感染端末のごく一部に過ぎない。他方、C&C サーバである可能性が高い機器と通信している端末は、マルウェア感染端末と断定はできないものの、マルウェアに感染している可能性は相当程度高いといえ、それら全てを対象として注意喚起を行うことで、結果としてより多くのマルウェア感染端末を対象とした注意喚起を行うことができると考えられる。そのため、電気通信事業者において、利用者の通信を識別して C&C サーバである可能性が高い機器と通信している端末を把握し、当該端末を注意喚起の対象とすることが考えられる。

具体的には、ISP が、C&C サーバに関する情報[4]等に基づいて C&C サーバである可能性が高い機器を把握した上で、DNS サーバ又はルータ等（以下「DNS サーバ等」という。）において、C&C サーバである可能性が高い機器の FQDN 又は IP アドレス、ポート番号及びタイムスタンプと、DNS サー

4 例えば、信頼性の高い C&C サーバに関するレピュテーションデータベースに含まれる情報のうち、C&C サーバであることの確度が高い機器に関する情報等が想定される。

バ等において把握される通信の FQDN 又は IP アドレス、ポート番号及びタイムスタンプとを照合することで、C&C サーバである可能性が高い機器と通信している端末を割り出し、当該端末に係る IP アドレス、ポート番号及びタイムスタンプを記録した上で、IP アドレス及びポート番号の割当状況を確認して当該端末の利用者を割り出し、電子メール等の方法で個別に注意喚起を行う方法が考えられる。

一方、通信に係る FQDN、送信元又は宛先 IP アドレス、ポート番号及びタイムスタンプは通信の構成要素であるから、ISP において、これらの情報を用いて C&C サーバの可能性が高い機器と通信している端末を識別する行為及び C&C サーバの可能性が高い機器との通信履歴を保存する行為は、いずれも通信の秘密の侵害に該当し得る。そのため、当該取組の実施に当たっては、どのような場合であれば、通信の秘密に属する事項の利用として許容されるものであるかを検討する必要がある。



【図２　マルウェアに感染している可能性が高い端末の検知】

（３）　C&C サーバである可能性が高い機器の検知

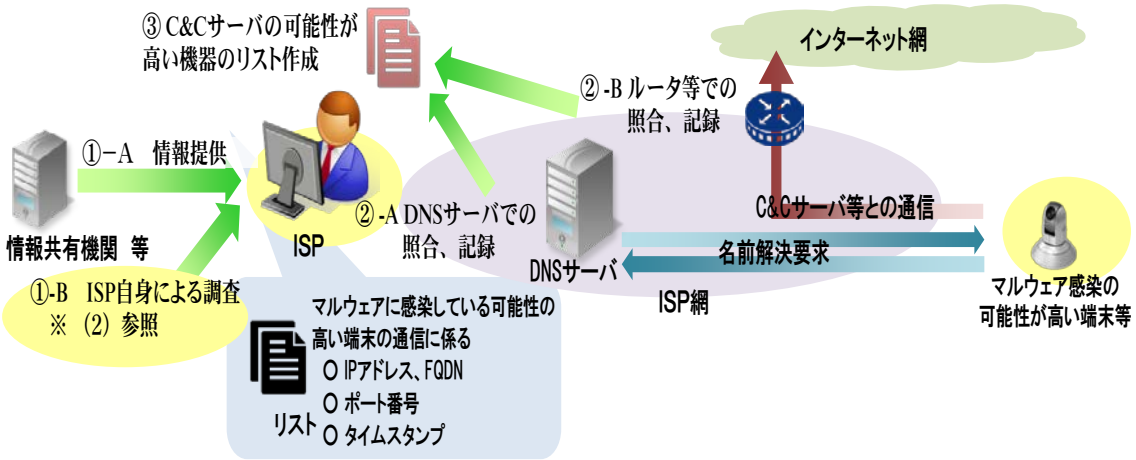
第二次とりまとめにおいて、利用者の有効な同意に基づき、通信の宛先情報を機械的・自動的に検知し、C&C サーバ宛ての通信であるか否かを検知した上で、該当する通信を遮断することについて整理した。本整理を踏まえ、ISP において、利用者の有効な同意に基づいた C&C サーバとの通信の遮断が行われているところである。

この取組を通じて被害を防止する試みは一定の成果を上げているが、現在においては C&C サーバが頻繁にその所在を変更する例が確認されている上に、マルウェアを用いて第三者の管理している機器を C&C サーバとして利用する事案も出てきていることから、C&C サーバを適時捕捉することが困難となってきており、誤遮断のリスクも高まりつつある。誤遮断

を回避しつつ、十分な実効性を上げるためには、C&C サーバに関する情報[5]を随時更新し、その識別精度を上げることが求められていることから、C&C サーバ等との通信によって生じる利用者の被害を未然に防止するために、マルウェアに感染している可能性が高い端末の通信の宛先を分析し、C&C サーバである可能性が高い機器を検知し、その情報を用いて上記のような通信遮断を行うという対策の実施について検討する必要がある。

具体的には、ISP が、マルウェアに感染している可能性が高い端末を把握した上で、DNS サーバ等において、マルウェアに感染している可能性が高い端末の IP アドレス、ポート番号及びタイムスタンプと、DNS サーバ等において把握される通信の IP アドレス、ポート番号及びタイムスタンプとを照合することで、マルウェアに感染している可能性が高い端末の通信を割り出し、当該通信の相手方の FQDN 又は IP アドレス、ポート番号及びタイムスタンプを記録した上で、このような記録を対象として、マルウェアに感染している可能性が高い端末が集中的にアクセスしているかといった相関関係の分析等を行うことで、C&C サーバの可能性が高い機器を割り出し、当該機器宛ての通信を遮断する方法が考えられる。

一方、通信に係る FQDN、送信元又は宛先 IP アドレス、ポート番号及びタイムスタンプは通信の構成要素であるから、ISP において、これらの情報を用いてマルウェアに感染している可能性が高い端末を識別する行為及び当該端末の通信の相手方との通信履歴を保存し、又は分析する行為は、いずれも通信の秘密の侵害に該当し得る。そのため、当該取組の実施に当たっては、どのような場合であれば、通信の秘密に属する事項の利用として許容されるものであるかを検討する必要がある。



【図３　C&C サーバである可能性が高い機器の検知】

[5] C&C サーバに関する情報の内容については、注４に記載したところと同様である。

（４）　マルウェアに感染し得る脆弱性を有する端末の利用者に対する注意喚起

第二次とりまとめにおいて、インターネット側からの名前解決要求等に応答し、DNSAmp 攻撃等のリフレクション攻撃に悪用されるおそれのあるブロードバンドルータの利用者に注意喚起を行うことについて整理した。本整理を踏まえ、ISP において、そのようなブロードバンドルータの利用者に対して、電子メール等による注意喚起を行っているところである。

この取組を通じて、リフレクション攻撃に悪用されるおそれのあるブロードバンドルータの設定の修正が行われることとなったが、本取組はあくまでもインターネット側からの名前解決要求等に応答し、攻撃に悪用され得る状態となっている端末を対象とするものである。他方、近年、IP アドレスを広範にスキャンしてパスワード設定の不備等の脆弱性[6]を有する端末を即座に感染させるマルウェアも出てきており、インターネットに接続されるカメラやセンサーなどの機器が爆発的に増加する中で、これらの IoT 機器には、脆弱性を有し、直ちにマルウェアに感染する危険性が高い状態になっているものがある。そして、それらの機器がマルウェアに感染することにより利用者に重大な被害をもたらすとともに、感染した IoT 機器が DDoS 攻撃等の通信を発することにより、大規模なサイバー攻撃が発生し、通信ネットワークにも大きな被害をもたらす場合がある。そこで、このような IoT 機器のマルウェアへの感染による利用者の重大な被害を防止するとともに、感染した IoT 機器を悪用した DDoS 攻撃等により ISP の電気通信役務の提供に支障が生じる場合に当該支障を防止するために、ISP において、脆弱性を有する端末の利用者を特定し、当該利用者に対して注意喚起を行い、パスワードの設定変更等による予防措置を促すことについて検討する必要がある。

具体的には、信頼できる第三者からの情報提供を受けること[7]により、ISP が脆弱性を有する端末を認識した場合において、当該端末の IP アドレス及びタイムスタンプと当該 IP アドレスの割当て状況を確認して当該

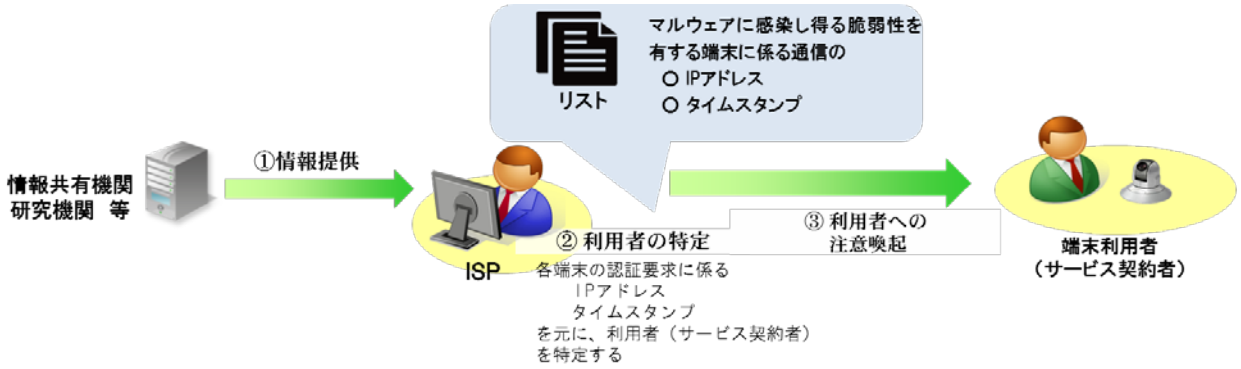
---

6 パスワードが設定されていない、容易に推測されるものであるなどのパスワード設定の問題や不正なコマンドが入力可能であるなどのソフトウェアの脆弱性等を指す。例えば、「Mirai」は、「root/1234」といった簡単な ID・パスワードが設定された IoT 機器に感染するものであり、また、「Satori」は、コマンドインジェクションの脆弱性を悪用して IoT 機器に感染するものである。

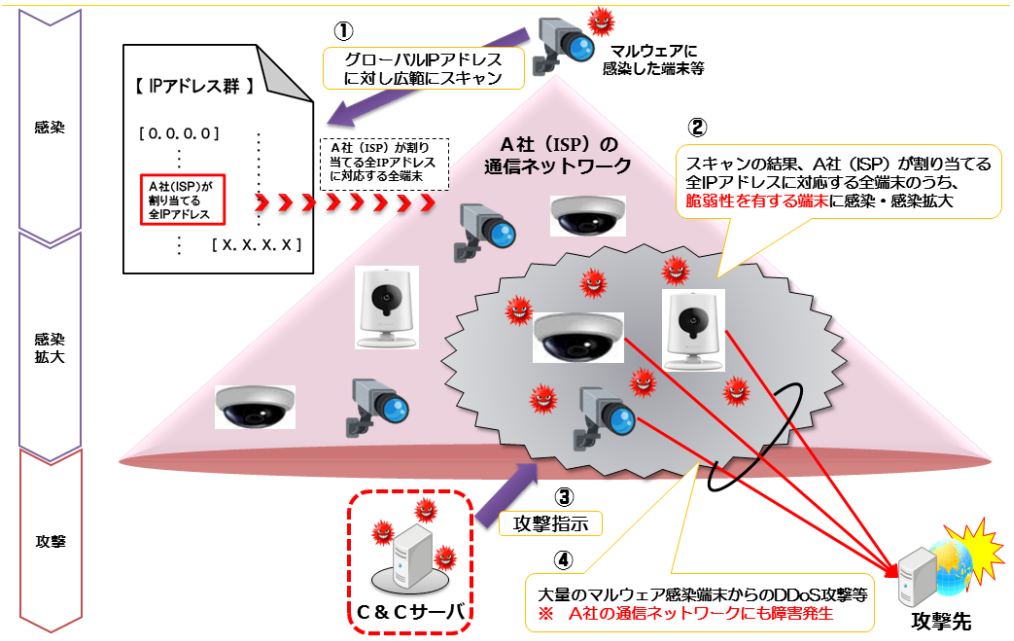
7 平成 30 年に改正された国立研究開発法人情報通信研究機構法（平成 11 年法律第 162 号）において、NICT は、サイバー攻撃の送信元となりうる端末設備等について ISP へ対処を求める通知を行うこととされている。

端末の利用者を割り出し、電子メールの送付等の方法で個別に注意喚起を図ることが考えられる[8]。

一方、IP アドレス及びタイムスタンプは通信の構成要素であり、ISP において、これらと IP アドレスの割当状況を確認して通信当事者を把握し、注意喚起を行う行為は通信の秘密の侵害に該当し得る。そのため、当該取組の実施に当たっては、どのような場合であれば、通信の秘密に属する事項の利用として許容されるものであるかを検討する必要がある。



【図４　マルウェアに感染し得る脆弱性を有する端末の利用者に対する注意喚起】



【図５　マルウェアに感染した端末による DDoS 攻撃等のイメージ】

[8] 利用者に対して注意喚起を行うに当たっては、ポート番号等も必要となる場合がある。

第２章　具体的検討

第１章に記載した最近のサイバー攻撃に係る課題と対策例に基づき、当該対策例と通信の秘密等との関係について以下のとおり検討を行った。

第１節　通信の秘密の利用等に関する違法性阻却事由等について

通信の秘密を侵す行為は、通信当事者の有効な同意に基づく場合又は違法性阻却事由がある場合に限り、通信の秘密の侵害に該当しない[9]。

具体的な考え方は、過去のとりまとめにおいて示してきたところであるが、特に本とりまとめにおいて検討された、通信当事者の有効な同意に関する考え方及び違法性阻却事由のうち正当業務行為、正当防衛及び緊急避難に関する考え方について以下整理する。

（１）　通信当事者の有効な同意

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ことから、通信の秘密を侵す行為であっても通信の秘密の侵害には該当しない。この点に関して、有効な同意があるとは、原則として、通信の秘密を侵すことに対する認識、認容がある場合をいい[10]、通常は契約約款等に基づいた事前の包括同意のみしかない場合を含まない。この理由は、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、通常その性質になじまないこと、事前の包括同意は将来の事実に対する予測に基づいて行われることからその対象、範囲が不明確となることにある。

逆に、①利用者が、ISP において通信の秘密を侵すことについて通常承諾すると想定し得るため、契約約款等による同意になじまないとはいえない場合であって、②利用者に将来不測の不利益が生じるおそれがない場合には、例外的に、契約約款等による事前の包括同意のみしかない場合であっても有効な同意があるといい得る場合がある。ここで、②の将来不測の不利益が生じるおそれがないといえるか否かを判断するに当たっては、

- 侵される通信の秘密の対象・範囲が明確であるか

---

9 通信の秘密についての基本的な考え方は、第１節に記載するほか、第一次とりまとめ 15 頁以下参照。

10 同意の有効性に疑義を招かないためには、外形的にみても明確な同意を得ることが要求されることから、「個別具体的かつ明確な同意」が必要とされている。具体的には、通信の秘密の取扱いについての同意であることを本人が認識した上で行う「個別」の同意であり、かつ、画面上での操作や文書による同意など外部的に同意の事実が「明確」な同意を意味している。

・　利用者が、一旦契約約款等に基づいて同意した後も、随時、容易に同意内容を変更（設定変更）できるか[11]
・　当該契約約款等の内容及び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か[12]
・　契約約款等に基づく措置の内容、同意内容の変更の方法等について、利用者に相応の周知が図られているか[13]

といった点を考慮する必要がある。

（２）　正当業務行為

国民全体が利用する通信サービスの社会インフラとしての特質を踏まえ、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を果たすという見地からみて、①目的の正当性、②行為の必要性、③手段の相当性が認められる行為については、正当業務行為としてその違法性が阻却される。

正当業務行為として整理されている例としては、課金、料金請求のために必要最小限度で通信履歴を確認する行為、通信のヘッダ情報を用いて経路制御を行う等の通信事業を維持、継続する上で必要な行為、大量通信に対する帯域制御等のネットワークの安定的運用に必要な措置等がある。

（３）　正当防衛、緊急避難

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、②自己又は他人の権利を侵害するために、③やむを得ずした行為である必要がある。また、正当防衛においては、行為の相手方は急迫不正の侵害を行っている者でなければならない。

他方、緊急避難として違法性が阻却されるためには、①現在の危難を避けるため、②法益の権衡が図られる限りにおいて、③他に採るべき方策なしに（補充性）行った行為である必要がある。

急迫不正の侵害又は現在の危難の有無にかかわらず行われる対策については、正当防衛又は緊急避難には該当しない。

---

11 利用者に将来不測の不利益が生じるおそれがないようにするためには、利用者が通信の秘密の侵害を許容しなくなった場合には撤回できる状況にあることが求められる。

12 同意しないことによって不利益を受ける場合には、当該不利益を避けるためにやむを得ず同意することがあり得ることから、必ずしも真意に基づく同意があるとはいえない。

13 同意を撤回する方法が用意されていても、実質的に行使できない場合には意味がないことから、十分な周知が求められる。

第２節　マルウェアに感染している可能性が高い端末の利用者に対する注意喚起について

（１）　対策の概要及び問題の所在

ISP が、信頼できる第三者からの情報提供や事業者自身による個別の検知等により、マルウェアに感染している可能性が高い端末が行った通信に関する当該端末の IP アドレス、ポート番号及びタイムスタンプを情報として得た場合において、ISP の保有する契約者情報、通信履歴等と上記 IP アドレス、ポート番号及びタイムスタンプを照合し、当該端末に係る通信回線の契約者及び連絡先を特定した上で、当該契約者に対して電子メールの送付等の方法により注意喚起を行うことが考えられる。

この場合、それらの端末に係る通信の IP アドレス、ポート番号及びタイムスタンプと、ISP が管理している通信履歴等との照合を実施する場合、ISP として取得、管理している通信履歴等を用いて当該事業者の取扱中に係る通信の通信当事者を識別することとなることから、利用者の有効な同意又は違法性阻却事由がない限り、通信の秘密の窃用等に該当し、通信の秘密の侵害となる。

（２）　通信当事者の有効な同意について

通信の秘密を侵害することなく本件対策を実施するためには、原則として個別具体的かつ明確な同意を取得することが必要となるところ、一定の場合には電気通信役務提供契約の締結時又は契約条件の変更時に、契約約款等に基づく包括的な同意を取得することで足りると解する余地はないか検討する。

①　契約約款等による同意になじむか

マルウェアに感染している可能性が高い端末については、第三者から不正な操作を受ける、端末から情報が漏洩するといった被害を受けることが想定されることから、マルウェアに感染している可能性が高い端末の利用者に対する注意喚起を ISP が行うことは、一般的、類型的に見て、利用者における安全なインターネット利用環境の確保に向けられた行為といえる。また、このような注意喚起を行うために、通信の秘密に当たる情報のうち当該端末が行った通信に係る送信元 IP アドレス、ポート番号及びタイムスタンプを元に、タイムスタンプに示された時刻において当該 IP アドレス及びポート番号の割当てを受けていた利用者の具体的な氏名及び連絡先を確認し、当該端末の利用者を特定する行為も、一般的・類型的に見て、利用者における安全なインターネット利用環境の確保に向けられた行為である。したがって、通常の利用者であれば、自らが利用している端末についてマルウェアに感染している可能性が高い場合には、注意喚起に必要最小限の範囲において上記のような形で

ISP が通信の秘密を利用することを承諾することが想定し得ることから、契約約款等に定めを置くことがその性質になじまないとはいえない。

② 利用者において将来生じる不測の不利益が回避し得るか

注意喚起に関して利用される通信の秘密の対象、範囲は既に述べたとおり明確であり、利用者に不測の不利益が生じる可能性は高くない。そのため、本件対策において、

ａ 注意喚起を希望しない者（オプトアウトした者）の利益が侵害されないような態勢を整える[14]

ｂ 利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更できる（設定変更できる）ようにする

ｃ 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内容とする

ｄ 本件対策の内容とともに、注意喚起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）こと及びその方法につき利用者に相応の周知を図る[15]

といった条件が満たされている場合には、契約約款等による包括同意を行った当時において予測し得なかった事情が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といえることから、将来、利用者が不測の不利益を被る危険を回避できるといえる。

③ まとめ

したがって、本件対策については、上記ａからｄまでに示した各条件を満たす場合には、契約約款等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等について有効な同意があるといえるものと考えられる。

（３） 違法性阻却事由について

本件対策は、マルウェア感染駆除の拡大（第一次とりまとめ８頁以下参照）と類似の取組であるが、マルウェアに感染している可能性が高い者全体を対象としている点で異なるものである。そして、マルウェアに感染して被害が生じていると判断できない者を対象としていることから、現在

14 具体的な対応の例としては、第二次とりまとめ 13 頁に記載されているもののほか、顧客データと顧客端末への IP アドレス等の割当て状況とが紐付いたシステムを構築して、これを用いて、注意喚起を希望しない者については IP アドレス等の照合を行わないようにすること等が挙げられる。

15 利用者に対し、契約締結時に書面等を用いて明確に説明することが考えられる。また、既に契約している者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によってマルウェアに感染している可能性が高い端末の利用者に対して注意喚起をすることを周知するとともに随時同意内容を変更できる（設定変更できる）こと及びその方法を説明すること等が考えられる。

の危難又は急迫不正の侵害が生じているとまではいえず、緊急避難又は正当防衛として許容されるとの整理は困難である。また、ISP において自主的に行われる取組であることから、法令に基づく行為にも該当しない。そこで、正当業務行為として整理される余地はないか検討することとする。

① 目的の正当性

本件対策の目的は、マルウェアに感染している可能性が高い端末の利用者に対する注意喚起を行うことにより、電気通信役務の利用者がマルウェアによる被害を受けることを防止するとともに、マルウェアに感染した端末が DDoS 攻撃等の通信を行うことで当該利用者に対して電気通信役務を提供する ISP の電気通信役務の提供に支障が生じる場合に当該支障を防止することにある。当該 ISP の電気通信役務の提供に生じる支障を防止するという目的は、通常、電気通信役務の円滑な提供という観点からみて正当であると考えられる。

なお、対象となっている端末が感染しているマルウェアの性質、予想される攻撃やそれに対する対処の困難性等からみて、電気通信役務の提供に支障を生じさせる通信をするおそれが低い場合は、専ら利用者の被害を防止する目的で行われることとなるから、目的の正当性が肯定できないと考えられる[16]。

② 行為の必要性

①の目的を達成するという観点からみて行為の必要性があるといえるのは、利用者の意思の如何にかかわらず、利用者に対して注意喚起を行って対処を求めなければ DDoS 攻撃等によって電気通信役務の提供に支障が生じるといえる程度に具体的な危険が予見される場合であると解される。

DDoS 攻撃等を行うマルウェアに感染している蓋然性がある端末が、当該端末に係る利用者に対して電気通信役務を提供する ISP において多数存在する場合には、一般には上記のような具体的な危険が予見されるところ、現在、マルウェアの多くは DDoS 攻撃に係る通信の送信をはじめとする様々な機能を内包している上、マルウェアに感染した後に DDoS 攻撃等に係る機能を追加することも極めて容易となっており、このような現状においては、マルウェアに感染している蓋然性がある端末が多数存在すれば、そのことをもって上記のような具体的な危険が予見されるといえる。

16 電気通信事業者において「電気通信役務の円滑な提供の確保」（電気通信事業法（昭和五十九年法律第八十六号）第一条）という目的の達成に期待されるものでない以上、正当業務行為における目的の正当性には該当しないと考えられる。

このため、マルウェアに感染している蓋然性のある端末[17]の数、マルウェアの性質、予想される攻撃やそれに対する対処の困難性等を考慮し、注意喚起して事前の対処を求めなければ当該端末に係る利用者に対して電気通信役務を提供するISPの電気通信役務の提供に支障を生ずる蓋然性が具体的にあるといえる場合には、原則として行為の必要性が肯定できるものと考えられる。

③　手段の相当性

本件対策においてISPによって確認、利用されるのは、IPアドレス、ポート番号及びタイムスタンプといった通信の秘密のほか、氏名、連絡先等のプライバシーに係る情報である。（２）のとおり、多くの利用者は注意喚起に必要不可欠な限度においてこれらを利用することを許容すると解されるものの、具体的な氏名、連絡先等を含むことからすれば、通信の秘密及びプライバシーの侵害の程度は客観的にみて小さいとはいえない。そのため、自らの権利利益を害されたくないと望む利用者を含めた利用者全体に対して注意喚起を行うことにつき手段の相当性が認められるのは、そのような措置を採ることが電気通信役務の提供のために必要やむを得ない場合に限られるものと解される。

すなわち、既にDDoS攻撃等を行った端末やマルウェアに感染している蓋然性のある端末等の利用者に対して注意喚起を行う場合等には、原則として手段の相当性が肯定できるものと考えられる。

④　まとめ

以上のとおり、マルウェアが高機能化し、マルウェア感染端末によるDDoS攻撃等が頻発している現状においては、本件対策は、過去にDDoS攻撃等を行った端末やマルウェアに感染している蓋然性がある端末が、当該端末に係る利用者に対して電気通信役務を提供するISPにおいて多数存在する場合等、注意喚起して事前の対処を求めなければ、当該ISPの電気通信役務の提供に支障が生ずる蓋然性が具体的にある場合であって、当該支障を防ぐために必要な限度でそれらの端末の利用者に対してのみ注意喚起を行うようなときに限っては、本件対策は、正当業務行為として許容されるものと解される。

なお、利用者に対する適切な情報提供という観点をも踏まえると、正当業務行為として注意喚起を実施する場合であっても、有効な同意を得ていない者に対してもなお注意喚起を実施して事前の対処を求めなければ電気通信役務の提供に支障が生ずるおそれがある場合に限定した上で、注意喚起を行う旨についてあらかじめ契約約款等で明示しておく

[17] 例えば、近い時期にDDoS攻撃等を行い通信ネットワークに支障を生じさせた端末、C&Cサーバであることについて合理的な疑いのない機器と繰り返し通信を行っている端末等が挙げられる。

ことが適当であると考えられる。

第３節　注意喚起を目的とする、マルウェアに感染している可能性が高い端末の検知について

（１）　対策の概要及び問題の所在

ISP が、マルウェアに感染している可能性が高い端末の利用者に対する注意喚起を行う目的で、当該 ISP が管理する DNS サーバにおいて C&C サーバである可能性が高い機器の FQDN と名前解決要求の FQDN とを照合し、又は当該 ISP が管理するルータ等において C&C サーバである可能性が高い機器に係る IP アドレス、ポート番号及びタイムスタンプと通信の送信元又は宛先 IP アドレス、ポート番号及びタイムスタンプを照合し、合致した通信についてはマルウェアに感染している可能性が高い端末の通信であるとして、その IP アドレス、ポート番号及びタイムスタンプを記録することが考えられる。

この場合、照合のために FQDN、通信の送信元又は宛先 IP アドレス、ポート番号及びタイムスタンプを利用し、また合致した通信に関してその IP アドレス、ポート番号及びタイムスタンプを保存することとなることから、利用者の有効な同意又は違法性阻却事由がない限り、通信の秘密の窃用等に該当し、通信の秘密の侵害となる。

（２）　通信当事者の有効な同意について

通信の秘密を侵害することなく本件対策を実施するためには、原則として、個別具体的かつ明確な同意を取得することが必要となるところ、一定の場合には電気通信役務提供契約の締結時又は契約条件の変更時に、契約約款等に基づく包括的な同意を取得することで足りると解する余地はないか検討する。

①　契約約款等による同意になじむか

マルウェアに感染している可能性が高い端末については、第三者から不正な操作を受ける、端末から情報が漏洩するといった被害を受けることが想定されることから、ISP が、マルウェアに感染している可能性が高い端末の利用者に対する注意喚起を行うこと及びそのために通信履歴等を利用して通信当事者を識別することは、一般的、類型的に見て、利用者における安全なインターネット利用環境の確保に向けられた行為といえる。また、このような注意喚起を行うために、ISP が管理する機器（DNS サーバ等）において、名前解決要求に係る FQDN や通信に係る送信元 IP アドレス、ポート番号（及びタイムスタンプ）と、C&C サーバである可能性が高い機器の FQDN 等とを照合し、合致した通信について

その C&C サーバである可能性が高い機器と通信している端末を識別した上で、当該端末に係る IP アドレス、ポート番号及びタイムスタンプを記録し、当該端末の利用者に対する注意喚起に用いる行為も、一般的・類型的に見て、利用者における安全なインターネット利用環境の確保に向けられた行為である。そして、照合及び記録のために利用される情報は、IP アドレス、ポート番号及びタイムスタンプに限られており、通信の秘密の中では比較的侵害の程度の小さいものに限定されている。

したがって、通常の利用者であれば、

ａ　自身が利用する端末がマルウェアに感染している可能性が高い場合には注意喚起を受けられるとのサービスが提供されており、これを希望しない者は検知等の対象にもならない

ｂ　記録された情報は他の用途では利用されず、目的達成後速やかに削除される

という前提があれば、C&C サーバである可能性が高い機器と通信している端末に係る IP アドレス、ポート番号及びタイムスタンプを記録するために必要最小限の範囲で、ISP が通信の秘密を利用することについて承諾することが想定し得ることから、契約約款等に定めを置くことがその性質になじまないとはいえない。

② 利用者において将来生じる不測の不利益が回避し得るか

注意喚起に関して利用される通信の秘密の対象、範囲は既に述べたとおり明確であり、上記ｂの条件が遵守される場合には、利用者に不測の不利益が生じる可能性は高くない。そのため、本件対策において、

ｃ　照合及び記録を希望しない者（オプトアウトした者）の利益が侵害されないような態勢を整える[18]

ｄ　利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更できる（設定変更できる）ようにする

ｅ　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内容とする

ｆ　本件対策の内容とともに、照合及び記録を望まない利用者は随時同意内容を変更（設定変更）できること及びその方法につき利用者に相応の周知を図る[19]

といった条件が満たされている場合には、契約約款等による包括同意を

---

18 具体的な対応の例については、第二次とりまとめ 13 頁参照。

19 利用者に対し、契約締結時において書面等により説明することが考えられる。また、既に契約している者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によって、マルウェア感染駆除の注意喚起の目的で照合及び記録をするとともに、随時、同意内容を変更できる（設定変更できる）こと及びその方法について説明をすること等が考えられる。

行った当時において予測し得なかった事情が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といえることから、将来、利用者が不測の不利益を被る危険を回避できるといえる。

③　まとめ

したがって、本件対策については、上記ａからｆまでに示した各条件を満たす場合には、契約約款等に基づく事前の包括同意であっても、注意喚起を行うための照合及び記録に関する通信の秘密に属する事項の利用等について有効な同意があるといえるものと考えられる。

（３）　違法性阻却事由について

本件対策は、ネットワーク内においてマルウェアに感染している可能性が高い端末が存在するか否かを調査するための取組であり、現在の危難又は急迫不正の侵害が認識される前に行われるものであるから、緊急避難又は正当防衛として許容されるとの整理は困難である。また、ISP において自主的に行われる取組であることから、法令に基づく行為には該当しない。そして、本件対策は、役務提供に支障が生じるおそれがあるか否かが不明確な段階で、利用者全体を対象として行う取組であるから、行為の必要性、手段の相当性が肯定し難く、正当業務行為と整理することは困難である。

以上のとおりであるから、本件対策について、現時点において違法性阻却事由があると整理することは困難である。

第４節　有効な同意に基づく通信遮断を目的とする、C&C サーバである可能性が高い機器の検知について

（１）　対策の概要及び問題の所在

ISP が、同意に基づく C&C サーバとの通信の遮断に用いる目的で、当該 ISP が管理する DNS サーバ等において、マルウェアに感染している可能性が高い端末に係る IP アドレス、ポート番号及びタイムスタンプと通信の宛先又は送信元 IP アドレス及びポート番号を照合した上で、合致した通信については送信元 IP アドレス（送信元 IP アドレスとの照合を行った場合は宛先 IP アドレス）、ポート番号及びタイムスタンプを記録し、同様に得られた他の利用者の情報等と併せて相関関係等を分析することで、C&C サーバである可能性が高い機器の FQDN、IP アドレス、ポート番号及びタイムスタンプを検知することが考えられる。

このような場合、通信に係る FQDN、送信元又は宛先 IP アドレス、ポート番号及びタイムスタンプは通信の構成要素であるから、ISP において、

これらの情報を用いてマルウェアに感染している可能性が高い端末の識別を行った上で、当該端末の通信履歴を保存し、分析等に利用することとなることから、利用者の有効な同意又は違法性阻却事由がない限り、通信の秘密の窃用等に該当し、通信の秘密の侵害となる。

（２）　通信当事者の有効な同意について

通信の秘密を侵害することなく本件対策を実施するためには、原則として、個別具体的かつ明確な同意を取得することが必要となるところ、一定の場合には電気通信役務提供契約の締結時又は契約条件の変更時に、契約約款等に基づく包括的な同意を取得することで足りると解する余地はないか検討する。

①　契約約款等による同意になじむか

マルウェアに感染している可能性が高い端末については、第三者から不正な操作を受ける、端末から情報が漏洩するといった被害を受けることが想定されることから、ISP が、マルウェアに感染している可能性が高い端末について C&C サーバとの通信を遮断する行為は、一般的・類型的に見て、利用者における安全なインターネット利用環境の確保に向けられた行為といえる。そして、このような遮断を行うために、ISP が管理するルータ等において、通信の送信元又は宛先 IP アドレス、ポート番号（及びタイムスタンプ）と、マルウェアに感染している可能性が高い端末のそれとを照合し、合致した通信について通信の相手方の IP アドレス、ポート番号及びタイムスタンプを記録した上で分析することにより C&C サーバである可能性が高い機器を検知することもまた、一般的・類型的に見て、利用者における安全なインターネット利用環境の確保に向けられた行為である。もっとも、照合、記録及び分析に利用される情報は、IP アドレス、ポート番号及びタイムスタンプに限られており、通信の秘密の侵害の程度は大きいものではないが、マルウェアに感染している可能性が高い端末の通信については C&C サーバではない機器との通信の履歴も含めて全て保存、分析の対象とされることから、侵害の程度が小さいとまではいえない。

以上の諸点に照らすと、通常の利用者であれば、上記目的のために必要最小限の範囲で、ISP が通信の秘密を利用することについて承諾することが想定し得ることから、契約約款等による定めになじむといい得るのは、

ａ　自身が利用する端末が C&C サーバと通信している場合には当該通信が遮断されるサービスが提供されており、かつこれを希望しない者は検知等の対象にならない

ｂ　保存された情報が他の用途では利用されず、目的達成後速やかに削

除される

という前提がある場合に限られるものと解される。

② 利用者において将来生じる不測の不利益が回避し得るか

注意喚起に関して利用される通信の秘密の対象、範囲は既に述べたとおり明確であり、上記ｂの条件が遵守される場合には、利用者に不測の不利益が生じる可能性は高くない。そのため、本件対策において、

ｃ 照合、記録及び分析を希望しない者（オプトアウトした者）の利益が侵害されないような態勢を整える[20]

ｄ 利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更（設定変更）できるようにする

ｅ 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内容とする

ｆ 本件対策の内容とともに、照合、記録及び分析を望まない利用者は随時同意内容を変更（設定変更）できること及びその方法につき利用者に相応の周知を図る[21]

といった条件が満たされている場合には、契約約款等による包括同意を行った当時において予測し得なかった事情が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といえることから、将来、利用者が不測の不利益を被る危険を回避できるといえる。

③ まとめ

したがって、本件対策については、上記ａからｆまでに示した各条件を満たす場合には、契約約款等に基づく事前の包括同意であっても、有効な同意に基づく通信遮断を行うための照合、記録及び分析に関する通信の秘密に属する事項の利用等について有効な同意があるといえるものと考えられる。

（３） 違法性阻却事由について

本件対策は、C&C サーバ等との通信の遮断（第二次とりまとめ２頁以下参照）と類似の取組であるが、C&C サーバである可能性が高い機器を対象としている点で異なるものである。そして、C&C サーバである可能性が高い機器が存在するか否かを調査するための取組であり、現在の危難又は急迫不正の侵害が認識される前に行われるものであるから、緊急避難又

[20] 具体的な対応の例については、第二次とりまとめ 13 頁参照。

[21] 利用者に対し、契約締結時において書面等により説明することが考えられる。また、既に契約している者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によって、マルウェアに感染している可能性が高い端末については、C&C サーバの検知に用いる目的でその通信の記録及び分析をするとともに、随時、同意内容を変更できる（設定変更できる）こと及びその方法について説明をすること等が考えられる。

は正当防衛として許容されるとの整理は困難である。また、ISP において自主的に行われる取組であることから、法令に基づく行為には該当しない。そして、本件対策は、利用者全体を対象として、役務提供に支障が生じるおそれがあるか否かが不明確な段階で、利用者全体を対象として行う取組であるから、行為の必要性、手段の相当性が肯定し難く、正当業務行為と整理することは困難である。

以上のとおりであるから、本件対策について、現時点において違法性阻却事由があると整理することは困難である。

第５節　マルウェアに感染し得る脆弱性を有する端末の利用者に対する注意喚起について

（１）　対策の概要及び問題の所在

ISP が、信頼できる第三者からの情報提供を受けることにより、脆弱性を有する端末の IP アドレス及びタイムスタンプが明らかとなった場合において、ISP の保有する契約者情報、通信履歴等と上記 IP アドレス及びタイムスタンプを照合し、当該端末に係る通信回線の契約者及び連絡先を特定した上で、当該契約者に対して電子メールの送付等の方法により注意喚起を行うことが考えられる。

この場合、それらの端末に係る通信の IP アドレス及びタイムスタンプと、ISP が管理している通信履歴等との照合を実施する場合、ISP として取得、管理している通信履歴等を用いて当該事業者の取扱中に係る通信の通信当事者を識別することとなることから、利用者の有効な同意又は違法性阻却事由がない限り、通信の秘密の窃用等に該当し、通信の秘密の侵害となる。

（２）　通信当事者の有効な同意について

通信の秘密を侵害することなく本件対策を実施するためには、原則として個別具体的かつ明確な同意を取得することが必要となるところ、一定の場合には電気通信役務提供契約の締結時又は契約条件の変更時に、契約約款等に基づく包括的な同意を取得することで足りると解する余地はないか検討する。

①　契約約款等による同意になじむか

脆弱性を有する端末については、そうでない端末と比較してマルウェアに感染する可能性が高く、その結果として第三者から不正な操作を受ける、端末から情報が漏洩する、DDoS 攻撃等の送信元となるといった被害を受ける可能性も高まると想定されることから、ISP が、脆弱性を有する端末の利用者に対する注意喚起を行うことは、一般的・類型的に見

て、利用者における安全なインターネット利用環境の確保に向けられた行為といえる。また、このような注意喚起を行うために、通信の秘密に当たる情報のうち当該端末が行った通信に係る送信元 IP アドレス及びタイムスタンプを元に、タイムスタンプに示された時刻において当該 IP アドレス等の割当てを受けていた契約者の具体的な氏名及び連絡先を確認し、当該端末の利用者を特定する行為も、一般的・類型的に見て、利用者における安全なインターネット利用環境の確保に向けられた行為である。したがって、通常の利用者であれば、自らが利用している端末について脆弱性が存在する場合には、注意喚起に必要最小限の範囲において上記のような形で ISP が通信の秘密を利用することを承諾することが想定し得ることから、契約約款等に定めを置くことがその性質になじまないとはいえない。

② 利用者において将来生じる不測の不利益が回避し得るか

注意喚起に関して利用される通信の秘密の対象、範囲は既に述べたとおり明確であり、利用者に不測の不利益が生じる可能性は高くない。そのため、本件対策において、

ａ 注意喚起を希望しない者（オプトアウトした者）の利益が侵害されないような態勢を整える[22]

ｂ 利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更できる（設定変更できる）ようにする

ｃ 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内容とする

ｄ 本件対策の内容とともに、注意喚起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）こと及びその方法につき利用者に相応の周知を図る[23]

といった条件が満たされている場合には、契約約款等による包括同意を行った当時において予測し得なかった事情が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といえることから、将来、利用者が不測の不利益を被る危険を回避できるといえる。

③ まとめ

したがって、本件対策については、上記ａからｄまでに示した各条件を満たす場合には、契約約款等に基づく事前の包括同意であっても、当

[22] 具体的な対応の例については、注 12 に記載したところと同様である。

[23] 利用者に対し、契約締結時に書面等を用いて明確に説明することが考えられる。また、既に契約している者に対しては、ウェブサイトへの掲載に加えて、電子メールや郵便等によって脆弱性を有する端末の利用者に対して注意喚起をすることを周知するとともに随時同意内容を変更できる（設定変更できる）こと及びその方法を説明すること等が考えられる。

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等について有効な同意があるといえるものと考えられる。

（３）　違法性阻却事由について

本件対策は、脆弱性を有するブロードバンドルータ利用者への注意喚起（第二次とりまとめ 20 頁以下参照）と類似の取組であるが、マルウェアに感染し得る脆弱性を有するにとどまる段階の端末を対象としている点で異なるものである。そして、被害が生じる前の取組であることから、現在の危難又は急迫不正の侵害が生じているとまではいえず、緊急避難又は正当防衛として許容されるとの整理は困難である。また、ISP において自主的に行われる取組であることから、法令に基づく行為にも該当しない。そこで、正当業務行為として整理される余地はないか検討することとする。

①　目的の正当性

本件対策の目的は、脆弱性を有する端末の利用者に対して注意喚起を行うことにより、脆弱性を有する端末がマルウェアに感染することによって電気通信役務の利用者が被害を受けることを防止するとともに、感染した端末が DDoS 攻撃の送信元となることによって当該利用者に対して電気通信役務を提供する ISP の電気通信役務の提供に支障が生じる場合に当該支障を防止することにある。当該 ISP の電気通信役務の提供に生じる支障を防止するという目的は、電気通信役務の円滑な提供という観点からみて正当であると考えられる。

なお、感染する蓋然性の高いマルウェアの性質、予想される攻撃やそれに対する対処の困難性等からみて、電気通信役務の提供に支障を生じさせる通信をするおそれが低い場合は、専ら利用者の被害を防止する目的で行われることとなるから、目的の正当性が肯定できないと考えられる。

②　行為の必要性

①の目的を達成するという観点からみて行為の必要性があるといえるのは、利用者の意思の如何にかかわらず、利用者に対して注意喚起を行って対処を求めなければ DDoS 攻撃等によって通信ネットワークに支障が生じるといえる程度に具体的な危険が予見される場合であると解される。

マルウェアによっては IP アドレスを広範にスキャンして脆弱性を有する端末を即座に感染させることから、脆弱性を有する端末は、既に DDoS 攻撃等に用いられる状態となっている端末等とほぼ同視し得るものと言える場合もあり、そのようなマルウェアに係る脆弱性を有する端末が、当該端末に係る利用者に対して電気通信役務を提供する ISP にお

いて多数存在すれば、当該端末がマルウェアに感染し、DDoS 攻撃等に用いられたときに、電気通信役務の提供に支障を生じさせる[24]ような DDoS 攻撃等が生じる具体的な危険が予見されることもあるといえる。

なお、脆弱性が明らかとなっている場合においては、端末の製造業者等から一般的な注意喚起が行われることが多いが、IoT 機器については、その利用者は、当該 IoT 機器が脆弱性を有することや、マルウェアに感染した後に DDoS 攻撃等を行っていることも直接認識できることは多くないことから、このような注意喚起によっては、脆弱性の修正を実現することは困難であると考えられ、ネットワーク越しに強制的にアップデートできるような例外的な場合を除き、他の手段によって①の目的を達成できるとは言い難い。

このため、脆弱性を有する端末の数、マルウェアの性質、予想される攻撃やそれに対する対処の困難性等を考慮し、注意喚起して事前の対処を求めなければ、当該端末に係る利用者に電気通信役務を提供する ISP の電気通信役務の提供に支障を生ずる蓋然性が具体的にあるといえる場合には、原則として行為の必要性が肯定できるものと考えられる。

③　手段の相当性

本件対策において ISP によって確認、利用されるのは、IP アドレス、ポート番号及びタイムスタンプといった通信の秘密のほか、具体的な氏名、連絡先等のプライバシーに係る情報であることから、形式的な通信の秘密及びプライバシーの侵害の程度は客観的にみて小さいとはいえない。このため、自らの権利利益を害されたくないと望む利用者を含めた利用者全体に対して注意喚起を行うことにつき手段の相当性が認められるのは、②で述べたように、そのような措置を採ることが電気通信役務の提供のために必要やむを得ない場合に限られるものと解される。

すなわち、②で述べたようなマルウェアに係る脆弱性を有する端末の利用者に対して注意喚起を行う場合等には、原則として手段の相当性が肯定できるものと考えられる。

④　まとめ

以上のとおり、脆弱性を有する端末を容易に感染させ、DDoS 攻撃等の送信元として用いるようなマルウェアが出てきている現状において、その脆弱性が放置されることにより、感染する端末が、当該端末に係る利用者に対して電気通信役務を提供する ISP において多数存在することとなり、当該端末からの DDoS 攻撃等によって当該 ISP の電気通信役務の提供に支障が生じる蓋然性が具体的にある場合であって、当該支障を防

[24] 例えば、ISP における脆弱性を有する端末の数及び想定される攻撃通信の量を勘案し、ISP の電気通信役務に係る通信ネットワークの通常の使用状況及び構造に照らし、当該ネットワークの許容量を超える通信の発生が見込まれる場合などが考えられる。

ぐために必要な限度で脆弱性を有する端末の利用者に対してのみ注意喚起を行うときに限っては、本件対策は、正当業務行為として許容されるものと解される。

なお、利用者に対する適切な情報提供という観点をも踏まえると、正当業務行為として注意喚起を実施する場合であっても、有効な同意を得ていない者に対してもなお注意喚起を実施して事前の対処を求めなければ電気通信役務の提供に支障が生ずるおそれがある場合に限定した上で、注意喚起を行う旨についてあらかじめ契約約款等で明示しておくことが適当であると考えられる。

第３章　おわりに

研究会では、第二次とりまとめ以降に発生した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、過去の各とりまとめと同様に、本とりまとめにおける整理を踏まえたサイバー攻撃ガイドラインの改定、ISP 等の電気通信事業者における対策の実施などの具体的な取組が行われることを期待する。

また、サイバー攻撃についてはその手口や手法が絶えず高度化・巧妙化していることから、情報通信技術等の変化に対応できるよう、今後とも官民の連携と適切な役割分担のもと、必要な検討を進めることで、サイバー攻撃に機動的に対応していくことが重要である。

なお、本とりまとめに記載した事項も含め、研究会における法的整理は社会状況等を踏まえて実施しているものであり、恒久的に妥当する性質のものではない。したがって、利用者の意識の変化などにより包括同意として許容される範囲が変動することや、サイバー攻撃の手法及びその影響の変化などにより正当業務行為として許容される範囲が変動することなどの事態が生じる可能性は否定できず、そのような事態が生じた場合には、その背景となる社会情勢の変化等を踏まえてさらに適切な整理が行われる必要がある。総務省及び各電気通信事業者においても、社会情勢の変化等を注視しながら引き続き適切な対応を行うとともに、必要に応じ、サイバー攻撃ガイドラインの改定などの取組を実施していくことを期待する。

（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 会長補佐　行政法律部会長
	木村（きむら）　たま代（よ）	主婦連合会　消費者相談室長
	小山（こやま）　覚（さとる）	一般社団法人 ICT-ISAC ステアリング・コミッティ 副運営委員長
	鎮目（しずめ）　征樹（もとき）	学習院大学法学部　教授
	中尾（なかお）　康二（こうじ）	国立研究開発法人情報通信研究機構 サイバー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）	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
	吉岡（よしおか）　克成（かつなり）	横浜国立大学大学院環境情報研究院／ 先端科学高等研究院　准教授

・　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
	井上（いのうえ）　大介（だいすけ）	国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所サイバーセキュリティ研究室　室長
	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 会長補佐　行政法律部会長
	小山（こやま）　覚（さとる）	一般社団法人 ICT-ISAC ステアリング・コミッティ 副運営委員長
	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 セキュリティ本部長
	鎭目（しずめ）　征樹（もとき）	学習院大学法学部　教授
	丸橋（まるはし）　透（とおる）	一般社団法人テレコムサービス協会 サービス倫理委員会　委員長
	吉岡（よしおか）　克成（かつなり）	横浜国立大学大学院環境情報研究院／ 先端科学高等研究院　准教授

○　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５回（平成 30 年２月 27 日）

－　開催要綱（案）について

－　「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」について

・　第６回（平成 30 年９月 14 日）

－　第三次とりまとめ（案）について

＜ワーキンググループ＞

・　第６回（平成 30 年３月１日）

－　開催要綱（案）について

－　「電気通信事業におけるサイバー攻撃への適正な対処に関する課題についての検討」について

・　第７回（平成 30 年３月９日）

－　第６回ワーキンググループにおける検討事項の整理状況について

－　電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律案及び法律案に関する課題の検討について

・　第８回（平成 30 年３月 30 日）

－　第三次とりまとめ（案）について

・　第９回（平成 30 年８月 10 日）

－　第三次とりまとめ（案）について

＜第三次とりまとめ（案）に対する意見募集の実施＞

（平成 30 年８月 17 日～８月 30 日）