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
第四次とりまとめ

令和３年 11 月

目次

（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

○　C&C サーバ検知のためのフロー情報分析

序章

情報通信技術の発展に伴い、複雑化・巧妙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、2013 年（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、2014 年（平成 26 年）４月には「第一次とりまとめ」、2015 年（平成 27 年）９月には「第二次とりまとめ」、2018 年（平成 30 年）９月には「第三次とりまとめ」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、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、例えば、行政機関等の調達先、委託先の脆弱性を突いたマルウェア感染の事例や大手通信事業者を標的とした DDoS 攻撃の事例、大企業を対象とした標的型ランサムウェアによる攻撃などの事例が多発するなど、サイバー攻撃はグローバルなトレンドとして巧妙化・悪質化が進んでいる。また、IoT 機器の普及・利用の急速な拡大や５Ｇサービスの開始など、新たな技術やビジネスが進展するのに併せて、IoT 機器を悪用したサイバー攻撃のリスクもますます高まっており、電気通信事業者が提供するインターネット接続サービスが国民生活や社会経済活動の基盤としてさらに重要な役割を担うようになる中で、サイバー攻撃による被害を防止し、その円滑な利用を確保することは、これまで以上に重要な課題になっている。

本研究会では、第三次とりまとめの公表後のこう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において技術的・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。

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。

---

[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。

第１章　最近のサイバー攻撃に係る課題と対策例

（１）　最近のサイバー攻撃に係る課題

近年、多数の IoT 端末（監視カメラ等）をマルウェア感染[2]させ、C&C サーバ[3]からの指令によりこれらの IoT 端末を踏み台にして特定のサーバ等に大規模な DDoS 攻撃を仕掛ける事例など、インターネット・サービス・プロバイダ（ISP）の提供する電気通信ネットワークに対するサイバー攻撃が複雑化・巧妙化している。

これに対して、これまでは端末機器側（ユーザ側）での対策を中心として措置を講じることを可能とするために本研究会において必要な法的な整理を行ってきたところである。具体的には、第三次とりまとめにおいて、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注意喚起を行うことについて整理した。同整理を踏まえ、2019 年（平成 31 年）２月以降、国立研究開発法人情報通信研究機構（NICT）が、パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのある IoT 機器を調査し、調査結果を ISP に通知し、ISP においてこれら IoT 機器の保有者を特定した上で、同保有者に注意喚起を行う取組（「NOTICE」）を進めている。

こうした取組は一定の成果は挙げているものの、脆弱性を有する IoT 機器の数は減っていないのが現状であり、第三次とりまとめの公表後においても、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、例えば、NICT が保有しているサイバー攻撃の大規模観測・分析システムである「NICTER」によれば、2020 年（令和２年）におけるサイバー攻撃関連の通信数は、2017 年（平成 29 年）の 3.3 倍に増加しており、2020 年（令和２年）の観測の内訳としては IoT 機器を狙った攻撃が最も多くなっている[4]。

---

[2] かつて大規模な通信障害を引き起こした‘Mirai’のソースコードが公開されており、多くの亜種のマルウェアが生み出され、IoT 機器などに感染する事例が多い。

[3] 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、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと（第一次とりまとめ脚注 12 参照）。

[4] このほか、NICT が注意喚起対象として ISP に通知した IoT 機器の件数は、2020 年（令和２年）12 月度分で 2002 件。（同年６月度分で 293 件。）

図1　NICTER で1年間に観測されたサイバー攻撃関連の通信数

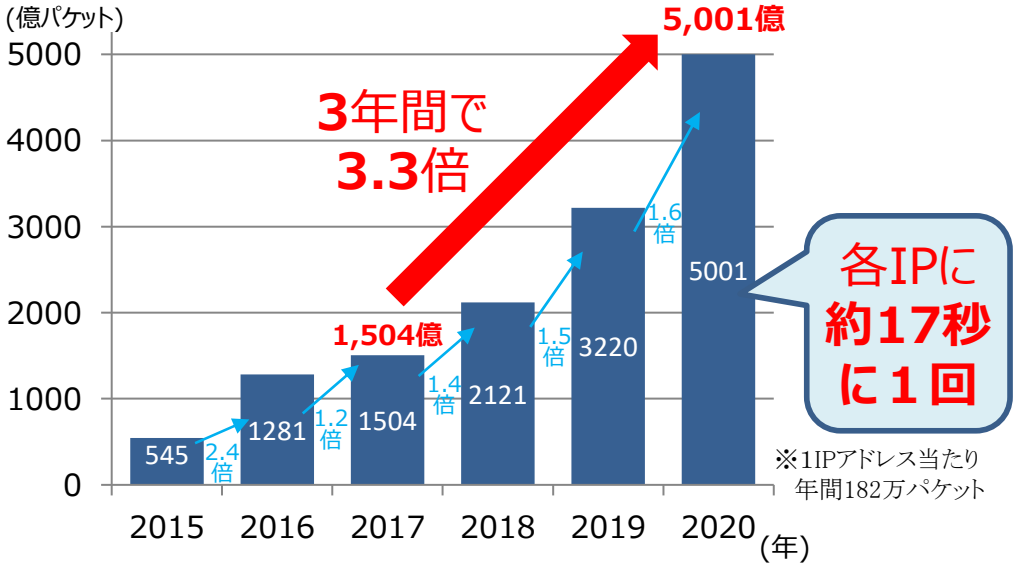
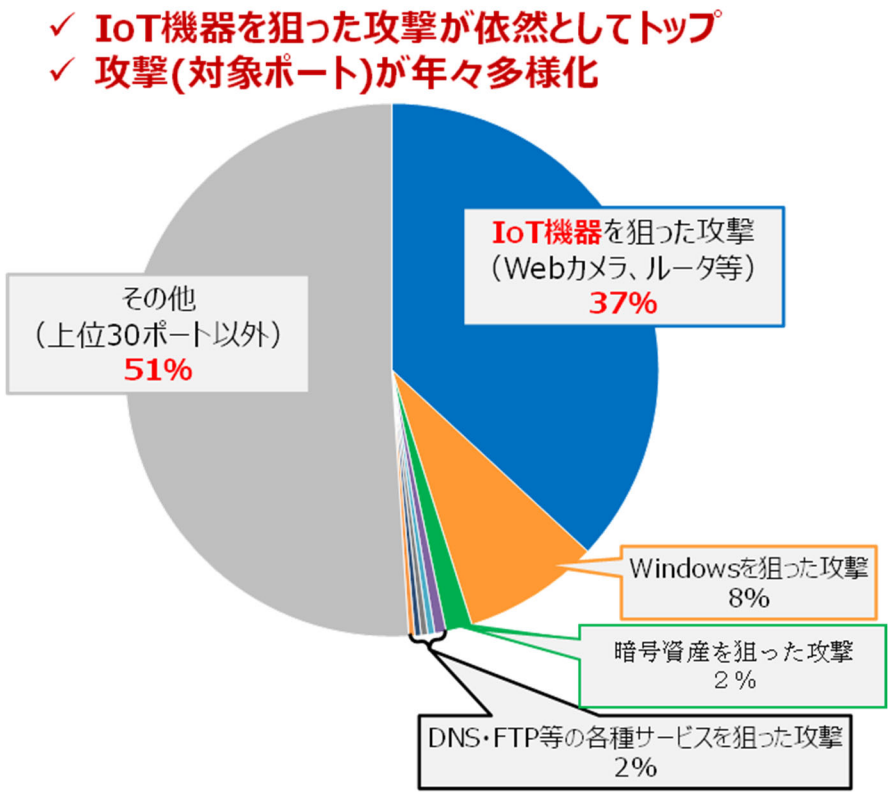


図2　IoT 機器を狙った攻撃の割合



※　NICTERで2020年（令和2年）に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位30ポートを分析したもの。なお、IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

また、今後５Ｇの進展により IoT 機器の利用が増加するに伴って、脆弱性を有する IoT 機器の数も増加していくことが予想され、調査対象となる IoT 機器の IP アドレスが膨大になり、現状のように IoT 機器を検索して注意喚起を行うという端末機器側での対応は難しくなっていくことが予想される。

こうした複雑化・巧妙化したサイバー攻撃が ISP の提供する電気通信ネットワークに対していつ行われてもおかしくない状態であるが、一度攻撃が行われた場合には、ISP による電気通信役務の提供に重篤な支障が生じるおそれがある。

（２） 平時におけるフロー情報の収集・蓄積・分析による C&C サーバである可能性が高い機器の検知

このようなサイバー攻撃に予防的に対処するため、平時から、ISP が、自らのネットワーク内の通信トラフィックに係るデータを収集・蓄積・分析し、C&C サーバである可能性が高い機器の検知等を行うことが電気通信役務の安定的な提供のために必要不可欠であると考えられる。

具体的には、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、IP アドレス及びポート番号等[5]のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（以下「フロー情報」という。）について現状多くの ISP において通信の傾向把握のために収集・活用しているところであるが、これを分析して未知の C&C サーバの検知を行うことが考えられる。C&C サーバ検知のためのフロー情報分析の手法としては、収集・蓄積したフロー情報等から検知した感染端末を起点に未知の C&C サーバを検知する手法、既知の C&C サーバを教師データとして機械学習を行う手法等がある。

このような ISP 規模でのフロー情報の分析による C&C サーバの特定は、未知の C&C サーバをより網羅的に検知可能とする点で、他の手法と比較しても優れたものである[6]。

一方、フロー情報は通信の構成要素であり、ISP において、これらの情報を収集・蓄積し、分析する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

[5] ヘッダの中の IP ヘッダの IP アドレス、TCP/UDP ヘッダの送信元/宛先ポート番号のほか、TCP フラグ情報（相手方との通信を確立するための TCP パケットの制御情報のうち、当該パケットの種類を示す情報）、ToS(Type of Service：パケットの転送の優先順位を示す情報)など、一部の附随的なヘッダ情報も収集・蓄積する。

[6] C&C サーバの検知の手法としては、他に、マルウェア検体の分析やハニーポットによる手法等も存在するが、これらは実際の感染をもとに C&C サーバを特定するため精度は高いものの、最新の検体を網羅的に入手することが困難であるという問題がある。

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。

（３）　フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報についての共有

各ISPがサイバー攻撃に対処し、利用者に対する電気通信役務の安定的かつ円滑な提供を確保する観点から、（２）の取組を実施することで得たC&Cサーバに関する情報をISP間で共有することは有用であると考えられる。このため、フロー情報を収集・蓄積・分析して検知したC&Cサーバに関する情報の共有について、通信の秘密に係る法的整理を行う必要がある。

なお、ISPの提供する電気通信ネットワークへのサイバー攻撃がますます複雑化・巧妙化する中、ユーザが安心して電気通信サービスを利用できるよう、ISPが協力・共同しつつサイバー攻撃に円滑・迅速に対処することにより、電気通信ネットワークの安全と信頼性を確保することの必要性が高まっている。こうした観点から、2018年（平成30年）５月の改正電気通信事業法においては、サイバー攻撃の送信元情報の共有やC&Cサーバの調査研究等の業務を行う第三者機関（認定送信型対電気通信設備サイバー攻撃対処協会。以下「認定協会」という。）を総務大臣が認定する制度を設けたところである[7]。本件対策についても、ISPが協力・共同してサイバー攻撃に対処することの必要性が高まっているとの認識の下、それを実現するための環境の整備を図る観点から検討を行うことが重要である。

[7] 認定送信型対電気通信設備サイバー攻撃対処協会として、2019年（令和元年）1月に一般社団法人ICT-ISACが認定されている。

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[8]。

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、これまでのとりまとめにおいて検討された、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）　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。

（２）　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。

[8] 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。

第２節　平時におけるフロー情報の収集・蓄積・分析による C&C サーバである可能性が高い機器の検知

（１）　対策の概要及び問題の所在

ISP が、自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち、フロー情報を収集・蓄積し、そのフロー情報を分析して、未知の C&C サーバの検知を行うことが考えられる。

フロー情報は、ISP のネットワークの通過パケットのヘッダ情報（IP アドレス、ポート番号等）やタイムスタンプ等の通信の構成要素として通信の秘密の保護の対象となるものであるから、ISP において、フロー情報を収集・蓄積し、それを分析して未知の C&C サーバを検知することは、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「知得」又は「窃用」行為に該当し、通信の秘密の侵害となる。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許容されるものであるかを検討する必要がある[9]。

（２）　違法性阻却事由について

本件対策は、サイバー攻撃が発生していない平時の段階で行われるものであるから、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[10]。

①　目的の正当性

目的の正当性は、その対策が、電気通信事業法が目的としている電気通信役務の円滑な提供を確保するためのものである場合に認められる。

本件対策は、ISP が、電気通信役務の提供に当たって、自らのネットワーク内のルータ等の電気通信設備等を通過する通信トラフィックに係るデータのうち、フロー情報を収集・蓄積・分析して、C&C サーバで

---

[9] 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は正当業務行為として整理されている（本とりまとめ８頁参照）。本件対策は C&C サーバ検知のためにフロー情報を収集・蓄積するものであり、目的が異なることから、改めて検討する必要がある。

[10] なお、「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」（第三次とりまとめ 18 頁以下参照）において、マルウェアに感染している可能性が高い端末等の通信履歴を用いた C&C サーバに係る検知について検討され、当該対策は、「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」と整理された。一方、脚注 11 にもあるように、第三次とりまとめ以降のサイバー攻撃をめぐる状況の変化に伴い、予防的対応の必要性が高まっていることも踏まえ、今般新たにフロー情報の収集・蓄積・分析による C&C サーバに係る検知について整理を検討するものである。

ある可能性が高い機器の検知を行うものである。これは、DDoS 攻撃等の C&C サーバを起点とするサイバー攻撃が発生する前から未知の C&C サーバ等を検知し、その検知した情報をもとに、各 ISP において適切な対処ができるようにすることにより、自己の電気通信役務の提供への重篤な支障の発生を未然に防止し、または、その被害の拡大を最小限に抑え、電気通信役務の円滑な提供を確保するための措置である。

具体的には、各 ISP における対処としては、①利用者の有効な同意を取得した上で、高セキュリティなサービス提供の一環として、検知された C&C サーバとの通信遮断を行うこと、②現に C&C サーバを起点とするサイバー攻撃等により、事業者設備に支障が生じるなど電気通信役務の円滑な提供への支障が発生している場合に、必要最小限の範囲で通信を遮断すること等が考えられる。したがって、本件対策の目的は、当該 ISP における電気通信役務の安定的かつ円滑な提供の確保にあるといえる。

なお、本件対策は、各 ISP がいつサイバー攻撃の標的となってもおかしくない現状の下において、自らが攻撃の標的となる場合や大量の攻撃通信が自らのネットワークに大きな影響を与える場合に備えて行われるものであり、あくまで、自己の電気通信役務の提供における支障の発生を未然に防止することが目的であると考えられる[11]。

以上より、本件対策の目的は、電気通信役務の安定的かつ円滑な提供の確保にあるから、目的の正当性が認められる。

② 行為の必要性

上記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、C&C サーバを起点としたサイバー攻撃が発生していない段階であっても、同攻撃の発生により電気通信役務の安定的かつ円滑な提供に支障が生じる危険の蓋然性がある場合において、他の方法によっては十分に有効な効果が得られないときであると解される。

この点、2018 年（平成 30 年）９月の第三次とりまとめ以降、２年以上が経過しているが、サイバー攻撃の複雑化・巧妙化が進んで攻撃の頻度は高まり、ISP の提供する電気通信ネットワークに対する C&C サーバを起点としたサイバー攻撃がいつ行われてもおかしくない状態にさらされており、役務提供に支障が生じるおそれは以前に比べてより差し迫ったものとなっている。

また、一度電気通信ネットワークに対する C&C サーバを起点としたサ

[11] 本年の事例としては、５月に欧州において政府が出資する大手 ISP が大規模な DDoS 攻撃の標的となり、政府機関や国会、研究機関等のウェブサイトがダウンした事案や、７月に国内でも広く使用されている米国の CDN サービス事業者（コンテンツデリバリーネットワーク：画像や動画等のウェブ上のコンテンツの安定的な配信を実現するために構成されたネットワークを提供する事業者）が通信事業者を含む自身の利用者への大規模な DDoS 攻撃を検知し対処した事案等、ISP をはじめとする電気通信事業者を標的とするサイバー攻撃が発生している。

イバー攻撃が行われた場合には、ISP による電気通信役務の提供に重篤な支障が生じ、当該電気通信役務の利用者に多大な損害と影響を引き起こすおそれがあり、これを防止することが必要不可欠となっている。

今後こうしたサイバー攻撃が大規模に発生した場合には電気通信役務の安定的かつ円滑な提供に甚大な影響がもたらされるリスクがあるところ、当該リスクを低減して電気通信役務の安定的かつ円滑な提供を確保するためには、平時から、ISP が、自らのネットワーク内のフロー情報を収集・蓄積・分析し、C&C サーバである可能性が高い機器の検知を行うことが必要不可欠であり、かつ、極めて有効である[12]。

今後５Ｇの進展により IoT 機器の利用が増加するに伴って、脆弱性を有する IoT 機器の数も増加し、調査対象となる IoT 機器の IP アドレスが膨大になることが予想される中で、これまでの脆弱性を有する IoT 機器に対する注意喚起をはじめとした主として端末機器側の対応により講じられてきた対策のみでは十分に有効な効果が期待できなくなることが懸念されることから、ISP によるフロー情報の収集・蓄積・分析による C&C サーバの検知以外の方法では、技術的・現実的に、有効な対策を講じることが困難になると予想される。

以上の事情に鑑みると、現在の電気通信ネットワークを取り巻く状況においては、C&C サーバを起点としたサイバー攻撃の発生により電気通信役務の安定的かつ円滑な提供に支障が生じる危険の蓋然性があり、他の方法によっては十分に有効な効果が得られないものと認められる。

したがって、このような行為を行う必要性が認められると考えられる。

③　手段の相当性

本件対策は、平時におけるフロー情報の収集・蓄積・分析であり、通信の秘密の侵害の程度は客観的にみて小さいとはいえないため、手段の相当性が認められるのは、C&C サーバの検知のために利用するデータが上記①の目的の達成のために必要最小限である場合に限られると解される。

この点、本件対策において、ISP によって収集・蓄積・分析されるフロー情報は、現状多くの ISP において通信の傾向把握のために既に収集・活用されているものであり[13]、IP アドレス、タイムスタンプ、ポート番

---

12 2018 年度（平成 30 年度）に、総務省の請負事業として、海外ネットワークのフロー情報分析による C&C サーバの検知に係る実証を行った。当該実証において、収集・蓄積したフロー情報等から検知した感染端末を起点に未知の C&C サーバを検知する手法では、検知した C&C サーバの IP アドレスと VirusTotal（ファイルやウェブサイトのマルウェア検査を行うウェブサイト）に登録されていた IP アドレスがすべて一致する（検知した C&C サーバのうち約 20%は VirusTotal による登録よりも早く検知）など、一定の高い精度の結果が示されている。

13 大手 ISP 等においては、平時から、ルータを通過するユーザの通信トラフィックに係るデータを、例えば一万分の一程度のレートで無作為にサンプリングし、ヘッダ情報を自動的に抽出して収集している。

号等のメタデータに留まっており、ペイロード（通信の内容）そのものは取得されない。その限りで実施されるものであれば、C&C サーバ検知のために収集・蓄積・分析するフロー情報は、ISP において、自己のネットワーク内のルータ等を通過するデータから一部をサンプリングし、サンプリングされたデータの中からヘッダ情報のみを自動的に抽出し、ヘッダ情報に機械的に付与されるタイムスタンプ等の情報を加えたものであり、C&C サーバ検知のために必要最小限の範囲のデータのみを用いるものであるといえる。

そして、本件対策は、このようなフロー情報について、収集・蓄積したフロー情報等から検知した感染端末を起点に未知の C&C サーバを検知する手法、既知の C&C サーバを教師データとして機械学習を行う手法等により、C&C サーバ検知のためのみに必要最小限の利用を行うものである。

また、前述の第三次とりまとめにおける検討課題は「通信遮断を目的とする」ものであった一方、ここでは、通信遮断を直接の目的とはせず、その前の段階にすぎない C&C サーバの検知のみを目的とするものであるところ、通信遮断を行う場合には別途利用者の同意が必要とすることで、利用者に対する通信の秘密の侵害が不必要に生じることがないようにすることが可能である。

以上により、必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報を C&C サーバ検知以外の用途で利用しない場合には、上記①の目的に照らして、手段の相当性も認められると考えられる。

④　まとめ

以上のとおり、サイバー攻撃の複雑化・巧妙化が進んで C&C サーバを起点としたサイバー攻撃が頻発し、これまでの方法では十分に有効な効果が得られていない現状においては、本件対策は、必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報を C&C サーバ検知以外の用途で利用しない場合に限り、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平時におけるフロー情報の収集・蓄積・分析を実施する場合であっても、利用者に対し、サイバーセキュリティ対策に活用する目的で必要最小限の範囲で行っていることについて、わかりやすく周知しておくことが適当であると考えられる。

第３節　フロー情報を収集・蓄積・分析して検知した C&C サーバに関する情報についての共有

（１）　対策の概要及び問題の所在

サイバー攻撃の複雑化・巧妙化が進んで攻撃の頻度が高まる中、各 ISP は、DDoS 攻撃などの C&C サーバを起点とする大規模なサイバー攻撃のターゲットにいつなってもおかしくない状況である。一方、各 ISP が当該攻撃を事前に十分な時間的余裕をもって予期し、これに対する防御措置を講じることは困難である。

このため、各 ISP がこうしたサイバー攻撃に対処し、ユーザに対して電気通信役務の安定的かつ円滑な提供を確保できるようにする観点からは、一の ISP が自らの電気通信ネットワーク内のフロー情報の収集・蓄積・分析によって検知した C&C サーバに関する情報（IP アドレス、ポート番号）を、適切な事業者団体[14]等に提供することが有用であると考えられる。

もっとも、フロー情報そのものは通信の構成要素であり通信の秘密として保護されるものであるところ、どのような場合であれば、通信の秘密を侵害することなく提供することが許されるのかについて整理する必要がある。

（２） 検討

上記のとおり、電気通信設備を通過するフロー情報そのもの（C&C サーバである可能性が高い機器が発信元や受信先になっている通信を含む。）は個々の通信の構成要素であることから当該 ISP の取扱中に係る通信に該当し、通信の秘密として保護されるため、フロー情報そのものの情報共有は通信の秘密の侵害に該当し得る[15]。

一方、本件において対象とされる C&C サーバに関する情報は、必要最小限のフロー情報について、C&C サーバを検知する目的のみのために集合的に分析した結果として得られた C&C サーバに関する IP アドレス及びポート番号を取りまとめてリスト化したものである。すなわち、個別の通信と切り離され、個々の通信がいつ誰に対して行われたかといった個々の通信の構成要素を明らかにすることにつながらないものである。

したがって、このように、C&C サーバに関する IP アドレス及びポート番号のリストの情報のみを、サイバーセキュリティ対策を行うために必要最小限の情報として、適切な事業者団体等に提供することは、通信の秘密の

[14] 例えば、一般社団法人 ICT-ISAC が想定される。同法人は、電気通信事業法に基づく「認定送信型対電気通信設備サイバー攻撃対処協会」の認定を受けている（認定協会業務として、サイバー攻撃に対処する電気通信事業者の支援業務を行っている。電気通信事業法第 116 条の２第２項第３号参照。）ほか、サイバーセキュリティに関する情報収集やセキュリティ啓発などに取り組んでおり、C&C サーバに関する情報を同法人に提供することは、これらの活動に資するものと考えられる。

[15] 電気通信事業法第 116 条の２第２項第２号ロにおいて、認定協会に通信履歴の電磁的記録を提供する会員は、当該提供を行う旨を電気通信役務の提供条件に定めていることが必要とされている。これは、当該提供は通信の秘密の侵害に該当するから、違法性阻却事由に該当しない限り、当該提供について利用者の同意を取得することが必要となるためである。（「電気通信事業法逐条解説（改訂版）」499 頁参照。）

保護規定に直ちに抵触するとまではいえないと考えられる[16]。

これを適切な事業者団体等へ提供することは、同団体が最新のサイバー攻撃の傾向の周知やその防御方策の普及啓発等を行うために資するものと考えられる。

なお、当該 C&C サーバに関する情報を、適切な事業者団体等を通じて他の ISP に提供する際には、提供先の ISP においてサイバーセキュリティ対策に活用する目的に限定して用いること、不当にサイバー攻撃者側に漏えいすることのないよう十分な信頼・協力関係が構築されている ISP に提供先が限定されるようにすること、当該情報提供についてその目的や提供範囲について利用者にわかりやすく周知することなどを確保することが適当と考えられる。

[16] 第２節にあるように、必要最小限の範囲でフロー情報を収集・蓄積し、そのフロー情報を C&C サーバ検知以外の用途で利用しない場合に限り正当業務行為として許容されるものと解されており、利用者に対してもサイバーセキュリティ対策に活用する旨をわかりやすく周知しておくことが適当であるとされている。このようなフロー情報の分析の結果として得られた C&C サーバに関する情報をリスト化したものは、サイバーセキュリティ対策に用いられることが想定されているものであって、そのために必要最小限の情報を適切な事業者団体等に提供することは許容されるものと考えられる。

第３章　おわりに

研究会では、サイバー攻撃の複雑化・巧妙化が進み、ISP のネットワークがいつ大規模なサイバー攻撃の標的になってもおかしくない現状の下で、ISP において自らが攻撃の標的となる場合や大量の攻撃通信が自らのネットワークに大きな影響を与える場合に備えて対策をとることが、これまで以上に重要な課題になっていることを踏まえ、フローー情報分析による C&C サーバの検知とその情報共有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、これらの取組により、平時の C&C サーバの検知及びサイバー攻撃発生時の迅速な対処が実現されるとともに、適切な事業者団体等を通じた情報の共有や研究機関等との連携が促進されることで我が国のサイバーセキュリティ対策が向上していくことを期待する。

さらに、サイバー攻撃の複雑化・巧妙化が進む中で、電気通信事業者が単独で自らのネットワークを守ることはますます困難になりつつあることから、今後、総務省においては、サイバー攻撃への適切な対処のための電気通信事業者間の連携・協力を促進するべく、必要な制度的検討を進めることが適当であると考えられる。

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

○　開催経緯

○　C&C サーバ検知のためのフロー情報分析

○　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）	鎮目（しずめ）　征樹（もとき）	学習院大学法学部　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 事務局長
	木村（きむら）　たま代（たまよ）	主婦連合会　事務局長
	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 運営委員長
	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　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ネクサス　ネクサス長
	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 事務局長
	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 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
	鎮目（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）	明治大学法学部　教授
	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在り方に関する研究会＞

- 第７回（令和３年 10 月１日）
  - ー　開催要綱（案）について
  - ー　「第四次とりまとめ（案）」について

＜ワーキンググループ＞

- 第 10 回（令和３年６月 29 日）
  - ー　開催要綱（案）について
  - ー　「サイバー攻撃に関する最近の動向」について
  - ー　「第四次とりまとめ（案）」について

- 第 11 回（令和３年８月 31 日）
  - ー　前回 WG における意見を踏まえた追加説明及び第四次とりまとめ（案）について

＜第四次とりまとめ（案）に対する意見募集の実施＞

（令和３年 10 月６日～11 月４日）

C&Cサーバ検知のためのフロー情報分析

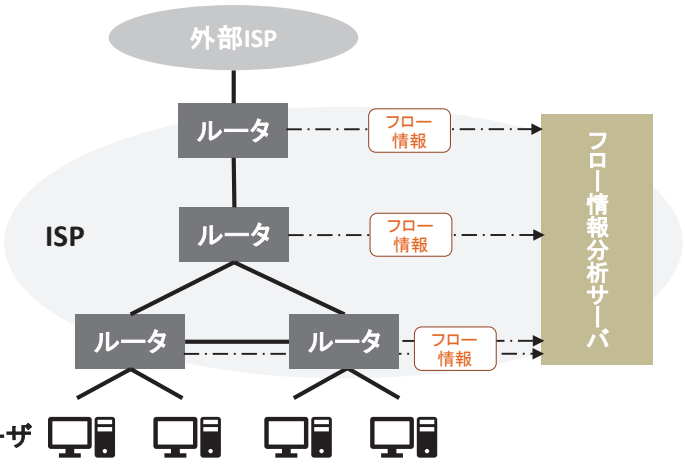
- フロー情報は、大手ISP等において、通信の傾向を把握するために平時から収集されているものであり、IoT機器等の端末を踏み台として悪用するサイバー攻撃が発生する蓋然性の高まりを踏まえ、これをC&Cサーバ※（以下C2サーバ）の検知にも活用するもの。
- C2サーバ検知のためのフロー情報分析は、１）フロー情報の収集・蓄積、２）フロー情報の分析・C2サーバの検知というプロセスで構成される。

※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、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと。

１）フロー情報の収集・蓄積

- ISPのネットワーク内の各所に設置されているルータから、当該ルータを通過するユーザの通信トラフィックに係るデータの一部（IPアドレス、ポート番号等）を収集・蓄積する。
  →詳細は次ページ参照

※大手ISP等においては、通信の傾向を把握し、ネットワークの設計や輻輳対策、DDoS攻撃対策等に活用するべく、平時からフロー情報の収集を行っており、これをC2サーバ検知に活用する。



２）フロー情報の分析・C2サーバの検知

- 踏み台となる感染端末を用いたサイバー攻撃においては、複数の感染端末が共通の相手方（＝標的、C2サーバ等）と通信を行ったり、共通のふるまい（例えば、同種・同サイズのパケットを同時期に大量送信する等）をすることから、フロー情報の中からこうした通信の特徴を抽出し、C2サーバの検知を行う。
  →詳細は3～4ページ参照

１）フロー情報の収集・蓄積

- 大手ISP等においては、平時から、ルータを通過するユーザの通信トラフィックに係るデータをサンプリングするとともに、ヘッダ情報の一部（IPアドレス、ポート番号等）を抽出し、ルータでヘッダ情報を抽出する際に付与される情報（タイムスタンプ等）と併せて収集しており、これをC2サーバの検知にも活用する。

①　サンプリング

- ルータを通過するユーザの通信トラフィックに係るデータを、1/10000程度のレートでサンプリングする。

※大手ISPからのヒアリングに基づき記載しているが、ISPの規模等により必要なレートは変動しうる。

②　ヘッダ情報のみの自動的な抽出

- サンプリングされたデータは、ヘッダ情報のみが自動的に抽出される。（ペイロード（通信の中身）は収集・蓄積の対象外）

※下図のとおり、ヘッダ情報とペイロードの情報量（バイト数）の割合はおおよそ1:30～1:20のため、（1/10000程度のレートでサンプリングした場合、）最終的にフロー情報分析の対象となるのは通信全体の情報量（バイト数）の1/300000～1/200000程度になる。

※平時から収集されている情報を活用するため、C2サーバ検知のための大手ISP等における技術的なハードルは高くない。

③　フロー情報の収集・蓄積

①②を経て、フロー情報分析のために必要な情報として、以下を収集・蓄積。

（１）ヘッダ情報

- 送信元/宛先のIPアドレス
- 送信元/宛先のポート番号　等

→通信の送受信先把握

（２）ルータでヘッダ情報を抽出する際に付与される情報

- タイムスタンプ　等

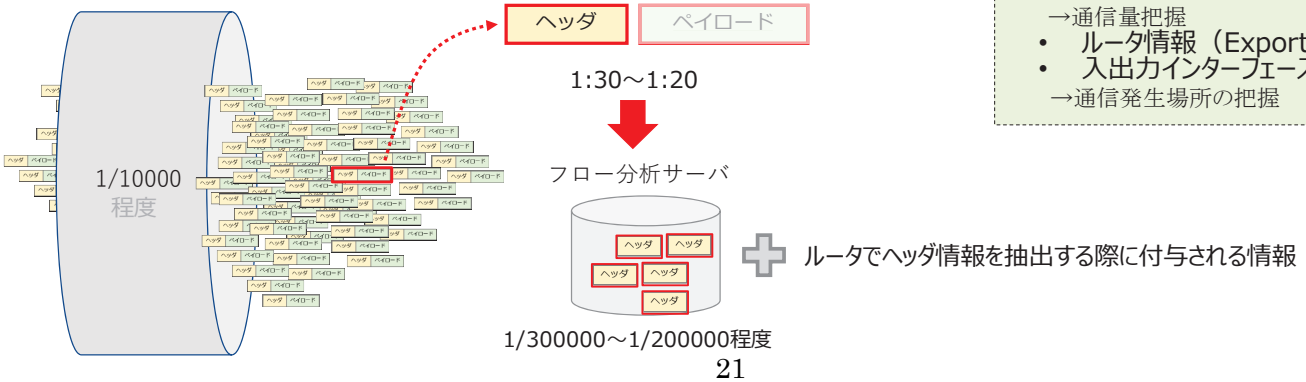
→通信発生タイミング把握

- バイト数　等

→通信量把握

- ルータ情報（ExporterIP）
- 入出力インターフェース　等

→通信発生場所の把握



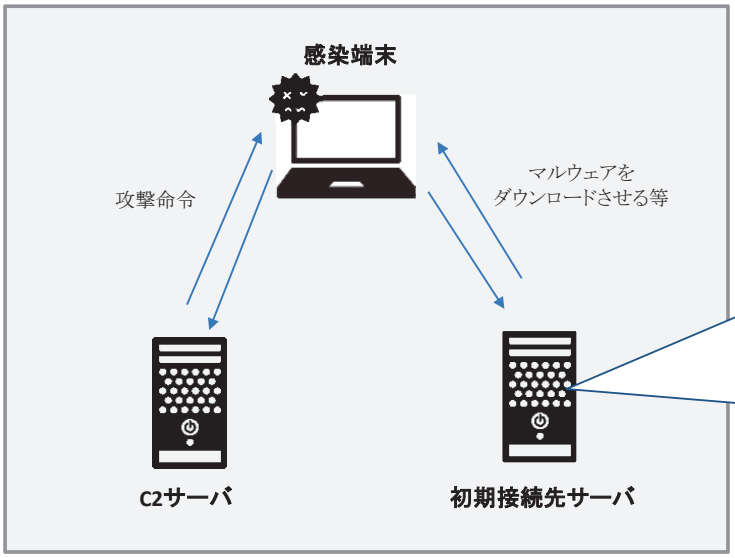
2）フロー情報の分析・C2サーバの検知 ①

3

➢ フロー情報の分析・C2サーバの検知に当たっては、①収集・蓄積したフロー情報等から検知した感染端末を起点に未知のC2サーバを検知する手法と、②既知のC2サーバを教師データとして機械学習を用い未知のC2サーバを検知する手法 の大きく２つがある。

① 収集・蓄積したフロー情報等から検知した感染端末を起点に未知のC2サーバを検知する手法

収集・蓄積したフロー情報等をもとに、既知の初期接続先サーバ（下図を参照）に着目するなどして、トラフィックの特徴から感染端末を検知した上で、当該感染端末の通信の相手方をC2サーバと推定するプロセスを通じて、未知のC2サーバを検知する。



端末に最初にアクセスさせて、マルウェアをダウンロード（感染）させるサイトのサーバ。左図のように、実際に攻撃命令を出すC2サーバとは別のサーバが用いられることが多い。

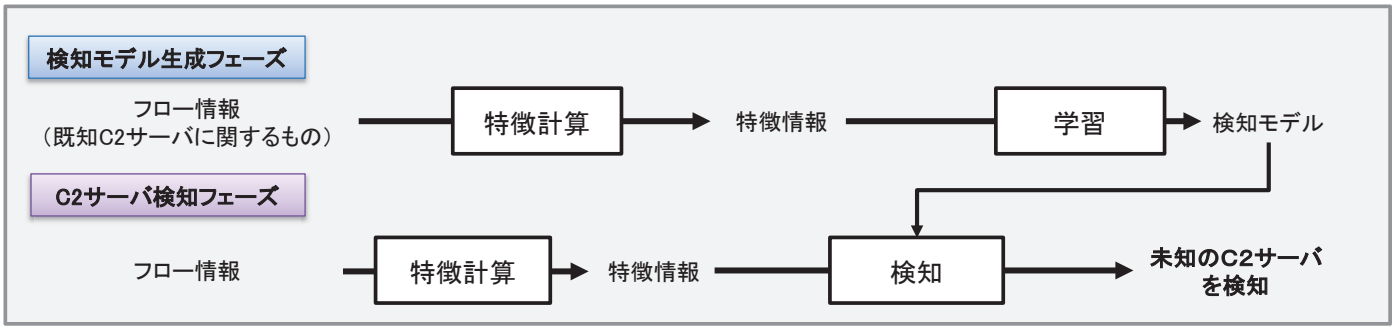
端末側の感染対策を目的とする市販のセキュリティ対策ソフト等のレピュテーションリストにはこの初期接続先サーバが登録されており、C2サーバが網羅されているとはいえないため、フロー情報分析からC2サーバを検知する必要がある。

2）フロー情報の分析・C2サーバの検知 ②

4

② 既知のC2サーバを教師データとして機械学習を用い未知のC2サーバを検知する手法

既知C2サーバのフロー情報から得られる特徴情報（通信時間・通信時刻・パケット流量・通信頻度・通信先等）を、教師データとして機械に学習させ、検知モデルを生成し、これをもとに、未知のC2サーバを検知する。



<フロー情報分析によるC2サーバ検知の精度について>

総務省の請負事業として平成30年度に実施した、海外ネットワークのフロー情報分析によるC2サーバの検知に係る実証においては、一定の高い精度の結果が示されている。

具体的には、

- マルウェア「trickbot」について、「①収集・蓄積したフロー情報等から検知した感染端末を起点に未知のC2サーバを検知する手法」を用いて、１か月半の間に検知した183のC2サーバは、すべてVirusTotal（ファイルやウェブサイトのマルウェア検査を行うウェブサイト）に登録されていたIPと一致。（なお、検知したC2サーバのうち約20%はVirusTotalよりも早く検知したものであったほか、感染ボット23,500以上を検知。さらに、ボットマスター（C2サーバを管理し、命令するボットネットの中心的なサーバ）についても８IPを検知。）
- 一般的なマルウェアについて、「②既知のC2サーバを教師データとして機械学習を用い未知のC2サーバを検知する手法」を用いて、約１ヶ月の間に検知した1075のC2サーバのうち、約87%がVirusTotalに登録されていたIPと一致。（なお、検知したC2サーバのうち約８%はVirusTotalよりも早く検知したものであった。）