国立国会図書館 調査及び立法考査局

Research and Legislative Reference Bureau
National Diet Library

論題 Title	サイバーセキュリティの確保と通信の秘密の保護―この 20 年の議論と能動的サイバー防御導入等に向けた課題―
他言語論題 Title in other language	Ensuring Cybersecurity and Protecting the Secrecy of Communications: Discussions over the Past 20 Years and Issues towards the Introduction of Active Cyber Defense and Other Measures
著者 / 所属 Author(s)	落合 翔（OCHIAI Syo）/ 国立国会図書館調査及び立法考査局　国土交通課
雑誌名 Journal	レファレンス（The Reference）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
通号 Number	879
刊行日 Issue Date	2024-3-20
ページ Pages	89-115
ISSN	0034-2912
本文の言語 Language	日本語（Japanese）
摘要 Abstract	通信の秘密の保護に関するこれまでの議論を、サイバーセキュリティの確保との関係に焦点を当てて整理する。また、能動的サイバー防御も含めた今後の取組に向けての関連する論点をまとめる。

サイバーセキュリティの確保と通信の秘密の保護
―この 20 年の議論と能動的サイバー防御導入等に向けた課題―

国立国会図書館　調査及び立法考査局
国土交通課　落合　翔

目　　次

キーワード：サイバーセキュリティ、通信の秘密、能動的サイバー防御、電気通信事業法、
国立研究開発法人情報通信研究機構法、インターネットの安定的な運用に関する協議会、
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

要　旨

① 通信の秘密の保護は憲法等に規定されており、サイバー攻撃からの防御のために通信の情報を得ることも、通信の秘密を侵す行為に該当する。通信の秘密に関わる行為で違法性が問われないためには、緊急避難、正当業務行為等の違法性阻却事由の要件を満たす必要がある。

② 2006年から実施された官民連携の取組「サイバークリーンセンター」では、サイバーセキュリティ対策を行うに当たり通信の秘密を侵害することが課題となった。しかし、緊急避難の要件を満たす等の問題のない手法が選択され、マルウェア感染者の特定と注意喚起が行われた。

③ 2006年には民間による「インターネットの安定的な運用に関する協議会」も発足した。同協議会は、サイバーセキュリティ対策等の事業者の行為について電気通信事業法上の通信の秘密の保護規定に係る違法性の有無を検討し、ガイドラインをまとめる活動を行っている。

④ 2013年から実施された官民連携の取組「ACTIVE」は、マルウェア拡散サイトにアクセスしようとする利用者に警告を発するものである。これも通信の秘密の侵害を伴う行為となるが、利用者から個別の同意を取得し、違法性が阻却される条件を整えて実施された。

⑤ 2013年から総務省が開催する「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」では、通信の秘密等に配慮しつつ事業者が新たな対策や取組を講じられるよう議論が行われ、新たなサイバー攻撃対策の事例ごとに違法性阻却事由の解釈がまとめられてきた。そうして整理された法的解釈に基づき、ACTIVEの活動の拡充等が図られてきた。

⑥ 2019年から国立研究開発法人情報通信研究機構や事業者等により実施されている、脆弱なIoT機器を検知し利用者へ注意喚起を行う取組「NOTICE」等については、開始に先立ち電気通信事業法等の法改正も行われ制度整備がなされた上で、違法性阻却事由の解釈が整えられた。

⑦ こうして実施され成果を上げてきた官民連携のサイバーセキュリティ対策だが、違法性阻却事由解釈の積上げというアプローチには限界も指摘される。法的解釈を整え、手法に工夫を凝らしつつ進められてきた日本の取組は、世界的にも独自性があるものとして評価されることもあるが、「能動的サイバー防御」の導入といった今後の対策の強化に向けては、より直接的な立法措置による制度整備の必要性も指摘されている。

はじめに

2022年12月に閣議決定された国家安全保障戦略では、サイバー攻撃（インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為(1)）を未然に排除等するために「能動的サイバー防御」を導入することが掲げられた(2)。その導入に当たっては、これが専守防衛を逸脱するものにならないか等といった多くの論点が存在するが、その中の1つに、この行為と、法律で定められている「通信の秘密」の保護との関係の整理が必要であるということがある。例えば、サイバー攻撃からの防御を目的として、攻撃に用いられている通信の情報を得ようとする場合、通信の秘密を侵すことになる。そのため、そうした情報の取得や共有が法的に問題とならない要件を検討すること等が必要となる(3)。

サイバーセキュリティ(4)に対する脅威は今日において社会的に大きな問題となっているが(5)、サイバーセキュリティ対策と通信の秘密との関係については、政府やインターネット接続サービスを提供するインターネットサービスプロバイダ（Internet Service Provider: ISP）を始めとする事業者(6)等によって約20年前から継続的な検討が行われており、近年には関係する法改正も行われている。能動的サイバー防御の導入に向けた検討は、サイバーセキュリティ対策という観点で従来行われてきた通信の秘密に係る議論も踏まえながら進められるものと思料される。

以上を踏まえ、本稿では通信の秘密の保護に関するこれまでの多様な議論(7)のうち、サイバーセキュリティの確保との関係に焦点を当てて整理し、政府や関係する事業者の取組を見ていく（全体像については本稿末尾の別図も参照）。その上で、能動的サイバー防御も含めた今後の取組に向けて、関連する論点をまとめる。

＊本稿におけるインターネット情報の最終アクセス日は、2024年2月1日である。

(1) 内閣サイバーセキュリティセンター『インターネットの安全・安心ハンドブック　Ver 5.00』2023, p.196. <https://security-portal.nisc.go.jp/guidance/pdf/handbook/handbook-all.pdf>

(2) 「国家安全保障戦略」（令和4年12月16日国家安全保障会議決定・閣議決定）pp.21-22. 内閣官房ウェブサイト <https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf> 国家安全保障戦略は日本の安全保障に関する最上位の政策文書との位置付けで策定され（同, p.4.）、能動的サイバー防御については「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。」（同, p.21.）等と記述している。

(3) 「通信の秘密保護 例外検討」『日本経済新聞』2023.6.30.

(4) サイバーセキュリティとは「情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること」である（サイバーセキュリティ基本法（平成26年法律第104号）第2条）。ただし、「情報セキュリティ」とは異なり、「電磁的方式」で扱われる情報に限られる概念である。本稿では、サイバーセキュリティを確保する活動をまとめて「サイバーセキュリティ対策」と表記する。

(5) サイバー攻撃被害が企業や医療機関、公的機関等で続発していることに警鐘が鳴らされている（総務省『令和5年版　情報通信白書』2023, pp.134-136. <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/pdf/n4a00000.pdf>）。

(6) 本稿における事業者の表記は、国内法制の説明においては法律上の用語（「電気通信事業者」等）に統一する。その他の箇所においては、インターネット接続サービスを提供する事業者は「ISP」、そうした事業者以外も含み得る場合は「ISP等」に統一する。ただし、海外法制の説明箇所や、引用した文章についてはこの限りではない。

(7) サイバーセキュリティ以外の論点としては、児童ポルノブロッキング、海賊版サイトブロッキング、発信者情報の開示等がある。こうした論点を幅広く整理するものとしては以下を参照。神足祐太郎「通信の秘密をめぐる議論の諸相」『レファレンス』834号, 2020.7, pp.43-61. <https://doi.org/10.11501/11516811>

Ⅰ　通信の秘密の概要

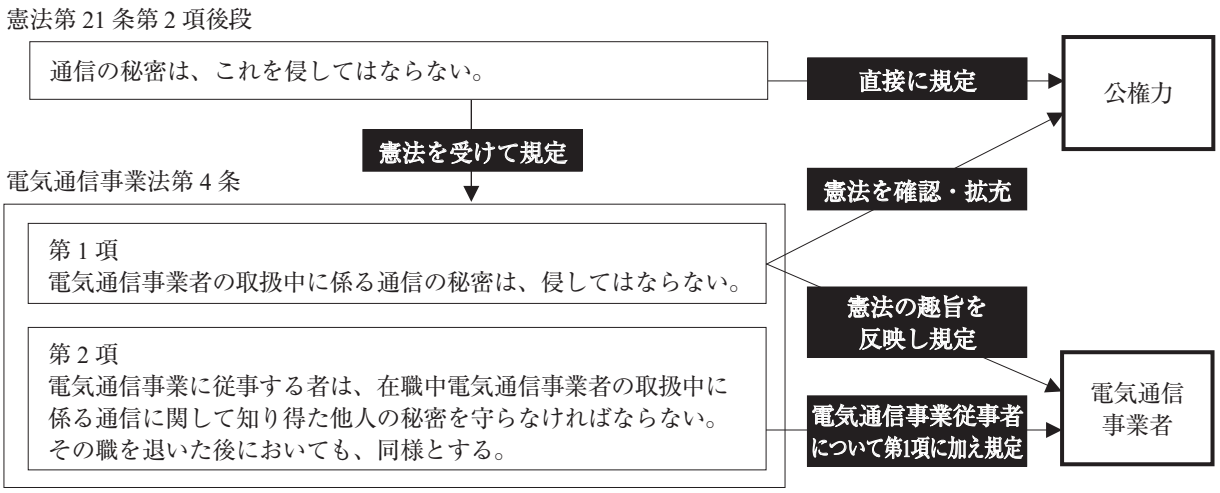
Ⅰでは、日本の通信の秘密に関する法制度を概観する。通信の秘密の解釈についてはいまだ論点が残されているとの指摘もあるが、ここでは通説と考えられる解釈に沿って整理を行う(8)。

1　憲法及び電気通信事業法における規定

憲法第21条第2項後段は「通信の秘密は、これを侵してはならない」と定めており、基本的人権の1つとして通信の秘密を保障している。また、個別の業法である電気通信事業法（昭和59年法律第86号）等(9)にもそれぞれ通信の秘密に関する規定がある。電気通信事業者(10)が主に媒介することとなるインターネット通信における通信の秘密については、直接には同事業者の規制等を行う電気通信事業法上の規定が問題となる(11)。

憲法及び電気通信事業法による規定とその関係は図1のとおりである。憲法における人権の保障は、その人権が国家権力に侵されることがないように定められたものとされ、通信の秘密の保障もこれに当てはまる。他方、電気通信事業法等は国家に限らず効力を持ち得る。よって、

図1　憲法及び電気通信事業法の通信の秘密に関する規定とその関係



（注）図中では略したが電気通信事業法第4条第1項は私人にも適用される。
（出典）小向太郎『情報法入門―デジタル・ネットワークの法律―　第6版』NTT出版, 2022, pp.36-37; 多賀谷一照監修, 電気通信事業法研究会編著『電気通信事業法逐条解説　改訂版』情報通信振興会, 2019, pp.35, 37; 曽我部真裕ほか『情報法概説　第2版』弘文堂, 2019, p.51を基に筆者作成。

---

(8)　例えば「憲法上の通信の秘密については、その内容・趣旨・適用範囲の核心については［多くの識者による見解で］一致が見られるものの、その外延についてはなお解決されるべき論点が残されている。」（［ ］内は筆者補記）といった評価がある（宍戸常寿「通信の秘密について」『企業と法創造』35号, 2013.2, p.18.）。通信の秘密の解釈に関する現在の議論を概観するものとしては、神足　同上, p.48.

(9)　電波法（昭和25年法律第131号）、有線電気通信法（昭和28年法律第96号）等にも通信の保護規定がある。

(10)　電気通信事業を営むことについて総務大臣の登録を受けた又は総務大臣に届出をした事業者をいう。電気通信事業とは、電気通信設備（有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けることを行うための電気的設備）を用いた電気通信役務（他人の通信を媒介し、その他電気通信設備を他人の通信の用に供する役務）を、他人の需要に応ずるために提供する事業のことである（電気通信事業法第2条）。電気通信事業者はISPを包含する（総務省「電気通信事業参入マニュアル　追補版」2005.8.18策定 (2023.1.30改定), p.16. <https://www.soumu.go.jp/main_content/000477428.pdf>）。

(11)　小向太郎『情報法入門―デジタル・ネットワークの法律―　第6版』NTT出版, 2022, pp.36-37.

電気通信事業法の通信の秘密の保護規定は、公権力にとっては憲法を確認し拡充した規定、電気通信事業者にとっては憲法の趣旨が反映された規定という位置付けとなる(12)。電気通信事業法では通信の秘密の侵害に対する罰則も定められており(13)、特に電気通信事業に従事する者には他の者よりも重い罰則が適用される(14)。

2　通信の秘密の範囲と保障内容

憲法及び電気通信事業法等で保護されるものには、電子メールの本文といった通信の内容が当然に含まれる。それに加えて、「通信の外形的事項」（通信の送信者や受信者、通信の個数や通信日時等）についても、それらをもって通信の内容が推知される可能性があるため、通信の秘密の範囲に含まれるというのが一般定な考え方である(15)。

通信の秘密を侵害する行為としては、①知得（通信当事者以外の第三者が積極的意思をもって通信の秘密を知ろうとすること）、②窃用（本人の意思に反して自己又は他人の利益のために用いること）及び③漏えい（他人が知り得る状態にしておくこと）の3つがある。通信の秘密として保障されるのは、こうした行為からの保護であるとされる(16)。

3　通信の秘密侵害の違法性阻却事由

サイバーセキュリティ対策を行うに当たっては、その対策が通信の秘密を侵害するものとして違法性が問われるか否かが問題となる。例えば、電気通信事業者が通信を媒介するために通信の送信先や送信元等を知得等することさえも、形式上は通信の秘密侵害に該当する。この行為については、後述する正当業務行為に該当し違法性が阻却されるという考え方がとられているが、このように、電気通信事業者による通信の秘密に関わる行為の多くは、秘密の侵害があることを前提とした上で、違法性阻却事由が認められる範囲内で実施されている(17)。

違法性阻却事由は、主に刑法（明治40年法律第45号）に定められている。第1に「緊急行為としての正当化事由」として、①正当防衛(18)及び②緊急避難(19)がある。第2に「日常行為としての正当化事由」として、③法令行為(20)及び④正当業務行為(21)がある。さらに第3に「超法規的違法性阻却事由」（刑法上に明文の定めはないものの実質的見地から違法性を阻却する

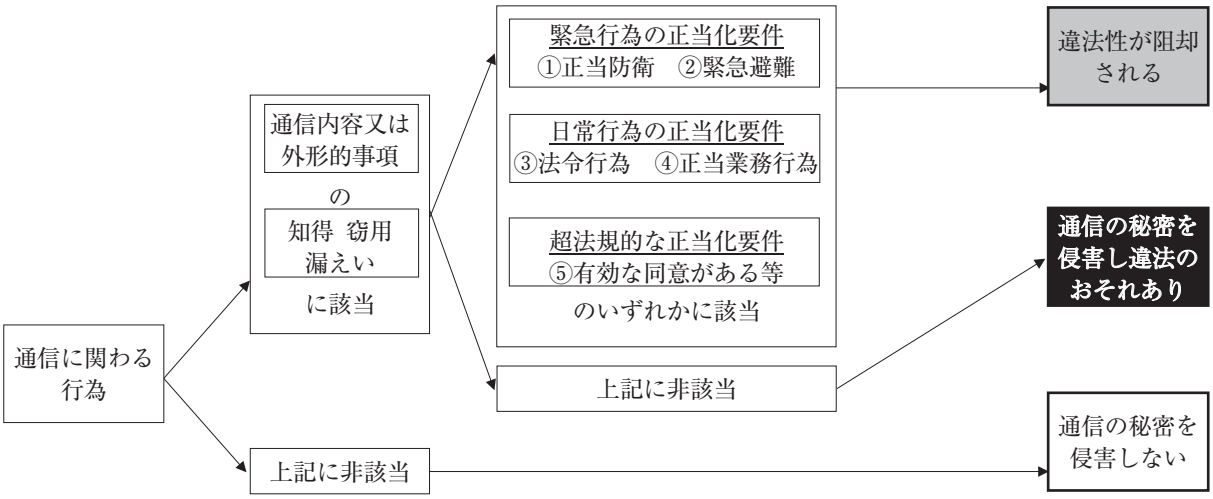
⑿　同上
⒀　2年以下の懲役又は100万円以下の罰金が科せられる（電気通信事業法第179条第1項）。
⒁　3年以下の懲役又は200万円以下の罰金が科せられる（電気通信事業法第179条第2項）。
⒂　曽我部真裕ほか『情報法概説　第2版』弘文堂, 2019, p.53. 電気通信事業法上、通信の外形的事項が通信の秘密の範囲に含まれることについては、例えば以下の判示がある。東京地方裁判所平成14年4月30日判決（平成11年（刑わ）3255号）
⒃　同上, p.54.
⒄　小向　前掲注⑾, pp.38-39.
⒅　正当防衛の要件は、①「急迫不正の侵害」に対する②「自己又は他人の権利を防衛するため」であって、③「やむを得ずにした行為」であることである（刑法第36条第1項）。
⒆　緊急避難の要件は、①「現在の危難」（法益侵害の危険が切迫したこと）を②「避けるため」、③「やむを得ずにした」（補充性（他に方法がないこと）と相当性（条理上肯定し得ること）を満たす）行為であって、④「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」（害の均衡（法益の権衡）の要件を満たす）ことである（刑法第37条）。
⒇　法令行為（刑法第35条）とは、行為が法令により命じられ又は特に許されているものを指す。通信の秘密を侵害する行為とは異なるが、Ⅱ5で後述する「特定アクセス行為」は、本来不正アクセス禁止法に抵触し得る行為について法令行為として認められているものである。
(21)　正当業務行為（刑法第35条）の要件として、多数説は①目的の正当性、②行為の必要性、③手段の相当性を挙げている。

もの）として、⑤法益侵害の被害者による侵害への有効な同意[22]といったものがある[23]。これらを前節の内容も踏まえて整理すると図２のようになる。

なお、⑤有効な同意については、各種のサイバーセキュリティ対策においては、利害関係者が広範囲に及ぶことが多く、問題が生じるたびに個別的な同意を得ることには限界がある。そこで、契約約款等を通じて事前に得られた包括的な同意をもって有効な同意とできないかが問題となり得る[24]。ただし、電気通信事業法上の通信の秘密に関する有効な同意の在り方を整理した2021年の総務省の文書においては、有効な同意とは一般に「個別具体的[25]かつ明確な[26]同意」である必要があって、原則として、包括同意すなわち契約締結時の約款同意や約款変更による同意では要件を満たさないという解釈を示している[27]。

なお、こうした同意の取得については、通信の送り手と受け手の双方から取得することが必要なのか、一方のみからで十分なのかということも問題となる[28]。この点については、通信にサイバー攻撃の意図がある場合においては、同意を取得すべき対象は通信を受ける側のみで足り、送信側の同意は不要であるとの見解が総務省により示されている[29]。

図２　通信の秘密の侵害と違法性



（出典）鎮目征樹ほか編, 荒木泰貴ほか『情報刑法Ⅰ―サイバーセキュリティ関連犯罪―』弘文堂, 2022, pp.65-83; 曽我部真裕ほか『情報法概説　第２版』弘文堂, 2019, pp.53-54 を基に筆者作成。

---

[22] 有効な同意の要件は、①同意能力を備えた法益主体が、②侵害される法益の内容や侵害の程度を認識した上で、③自由な意思に基づいて当該法益の処分に同意したことであるとされる。

[23] 鎮目征樹ほか編, 荒木泰貴ほか『情報刑法Ⅰ―サイバーセキュリティ関連犯罪―』弘文堂, 2022, pp.65-83.

[24] 同上, p.82. 包括同意が有効であるためには、①問題となる法益侵害行為が一般的・類型的に当事者の利益に適うものであり、法益主体の同意を推定し得る点において契約約款による同意になじむ事項であること、②契約時点以降の事情変化により法益主体に不測の不利益が生じるおそれがないこと、が必要になると解されている。

[25] ①「個別」のサービスごとに同意を取得するという意味、②契約約款事項としての包括的な同意（契約締結時の約款同意や約款変更による同意）ではなく通信の秘密に関する特定の事項を本人が「具体的に」認識した上で同意を取得するという意味、の２つを含む。

[26] 画面上でのクリック、チェックボックスへのチェックや文書による同意等、外部的に同意の事実が明らかな場合を意味する。

[27] 総務省「同意取得の在り方に関する参照文書」[2021], pp.11-13. <https://www.soumu.go.jp/main_content/000735985.pdf>

[28] 田川義博「インターネット利用における「通信の秘密」」『情報セキュリティ総合科学』５号, 2013.11, p.20. <https://www.iisec.ac.jp/proc/vol0005/tagawa13.pdf>

[29] 第208回国会衆議院総務委員会議録第16号　令和４年５月10日　p.14.（二宮清治総務省総合通信基盤局長答弁）

Ⅱ　これまでのサイバーセキュリティ対策と通信の秘密

1　サイバークリーンセンター（2006 ～ 2011 年）

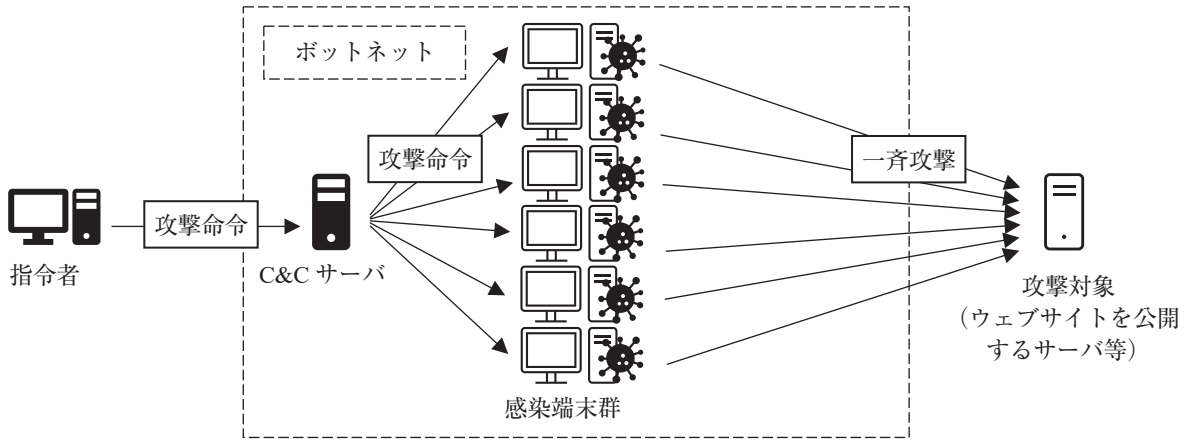
(1) 取組の概要

政府と ISP 等が共同で実施したサイバーセキュリティ対策で、通信の秘密に関する議論が見られたものには、まず 2006 年 12 月から 2011 年 3 月まで実施されていたサイバークリーンセンター（Cyber Clean Center: CCC）の取組がある(30)。

CCC は総務省及び経済産業省が連携して実施した、「ボットから我が国のインターネットを守ること」を目的としたプロジェクトである。2004 年、当時日本であまり知られていなかった「ボットネット」を利用したとみられるサイバー攻撃が国内の ISP に対して行われたことが、官民を挙げてのボット対策プロジェクト誕生の契機となった(31)。

ここでボット（bot）とは、マルウェア（Malware. 悪意のあるソフトウェア）の一種である。ボットに感染したコンピュータ（以下､マルウェアに感染した各種機器をまとめて「感染端末」）は他の機器にも感染を広げ、ボットネットと呼ばれる多数の感染端末から成るネットワークを形成する。ボットネットの指令者は、C&C サーバ（Command and Control Server）と呼ばれるコンピュータを介して感染端末を遠隔操作し、DDoS 攻撃（Distributed Denial of Service Attack. 多数のコンピュータから攻撃対象に一斉に大量の問合せ等を行う攻撃）(32)等の様々な不正行為に利用する（図 3）。多くの場合、ボットはコンピュータ上では目に見える不審な動きは見せないため、感染端末の利用者（以下「感染者」）は自身の機器が感染していることに気付くことが難しい(33)。

図３　ボットネットを用いた DDoS 攻撃のイメージ



（出典）吉川孝志「PC を乗っ取るマルウェアの手口」『日経 network』239 号, 2020.3, pp.64-65 等を基に筆者作成。

---

(30)　「サイバークリーンセンターについて」T-ISAC-J ウェブサイト <https://www.telecom-isac.jp/ccc/>

(31)　有村浩一「ボット対策プロジェクト「サイバークリーンセンター」からみた国内のマルウェア対策」『情報処理』541 号, 2010.3, p.275. <http://id.nii.ac.jp/1001/00069233/> CCC の設立契機となったサイバー攻撃については、ISP へのサイバー攻撃と同時期に始まった一般社団法人コンピュータソフトウェア著作権協会のウェブサイトへの DDoS 攻撃を挙げる文献もある（小山覚・中川文憲「DoS/DDoS 攻撃観察日記（2）―Antinny による ACCS サイトへの DDoS 攻撃―」『情報処理』578 号, 2013.5, p.15. <http://id.nii.ac.jp/1001/00091480/>）。

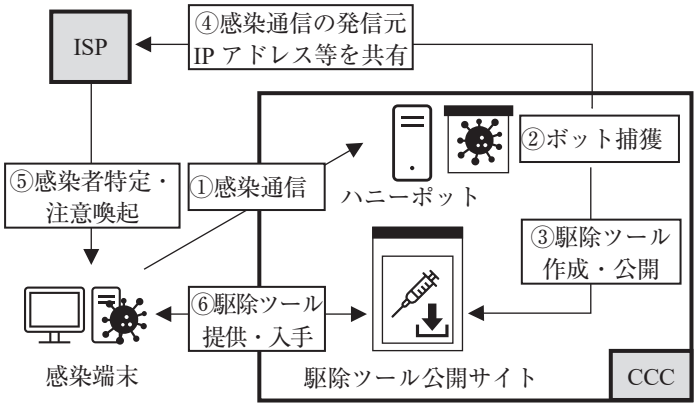
(32)　内閣サイバーセキュリティセンター　前掲注(1), p.190.

(33)　サイバークリーンセンター「ボットの脅威との戦い―サイバークリーンセンター（CCC）活動レポート―」2010.9.13, pp.2-3. T-ISAC-J ウェブサイト <https://www.telecom-isac.jp/ccc/report/h21ccc_report.pdf>

CCC では、まず「ハニーポット」と呼ばれるおとりのコンピュータを用意し、ボットにあえて感染させる。そうして捕獲したボット検体を分析し、駆除ツールを作成してインターネット上に公開する。また、ボットの感染のためになされた通信（以下「感染通信」）の発信元情報等[34]を ISP に送付し、それを基に ISP が感染者を特定する。その上で、感染者に ISP から注意喚起の電子メールを送信し、駆除ツールを入手してボットの駆除等を行うことを促す[35]（図4）。

この CCC の取組には最終的に 76 社の ISP が参画した[36]。約 4 年間にわたる CCC の活動の結果、約 2 万 6 千の検体に対して駆除ツールが作成され、約 11 万人の感染者に注意喚起が行われた[37]。国内のボット感染率は、CCC 開始前の 2005 年に行われた調査では 2 ～ 2.5% であったが、2008 年には 1% まで減少、さらに 2010 年には約 0.6% となった。当時のこの数字は海外と比較しても低く、CCC の活動が少なからず貢献していたと言われる[38]。

図４　サイバークリーンセンター（CCC）の取組



（出典）「サイバークリーンセンターについて」T-ISAC-J ウェブサイト <https://www.telecom-isac.jp/ccc/> 等を基に筆者作成。

(2) 通信の秘密に係る解釈

感染端末の急増によってボットネットの存在が認知された 2004 年はボット対策の黎明期と言われるが、総務省の有識者会議「次世代 IP インフラ研究会」[39]がその翌年にまとめた提言「情

34　具体的には、特定しようとする通信当事者の IP アドレス（いわゆる「インターネット上の住所」）及び通信が発生したタイムスタンプ（時刻情報）が ISP に共有される。IP アドレスは ISP から通信当事者へ都度割り当てられている「動的 IP アドレス」であることが多いため、通信当事者を特定する情報としては IP アドレスだけでは不十分であり、いつ当該 IP アドレスが割り当てられていたのかを示す情報、すなわちタイムスタンプと IP アドレスの組合せを用いて通信当事者を特定することとなる（清水陽平『サイト別ネット中傷・炎上対応マニュアル第 4 版』弘文堂, 2022, pp.83-85.）。次節以降で説明する CCC 以外の各種取組においても、基本的に同様の方法で通信当事者を特定する。

35　則武智「総務省・経済産業省連携プロジェクト「サイバークリーンセンター」の取組み―ボットウイルスの最近の傾向と対策―」『日本データ通信』160 号, 2008.3, pp.10-11.

36　「サイバークリーンセンターについて」前掲注30

37　「サイバークリーンセンター活動実績 2011 年 01 月度の注意喚起活動実績」T-ISAC-J ウェブサイト <https://www.telecom-isac.jp/ccc/report/201101/1101monthly.html> CCC の活動のうち、注意喚起は 2011 年 1 月で終了した。

38　サイバークリーンセンター　前掲注33, p.65; 情報処理推進機構『情報セキュリティ白書　2011―広がるサイバー攻撃の脅威―求められる国際的な対応―』2011, p.85. ボット感染率は、ブロードバンド（高速・大容量のインターネット接続サービス）利用者を対象とした調査による。

39　次世代の IP インフラ整備の在り方について展望するとともに、インフラ整備に対する政策支援の在り方等について検討することを目的に 2004 年 2 月から開催された（「次世代 IP インフラ研究会 開催要綱」（次世代 IP インフラ研究会（第 1 回）資料 1-1）2004.2.3, p.1. 総務省ウェブサイト（国立国会図書館インターネット資料収集

報セキュリティ政策2005」においては、ボット対策のために情報収集をするに当たって、通信の秘密の保護規定等に抵触しないような手法を検討することが早くも課題として認識されている(40)。そして、「情報セキュリティ政策2005」等に基づく取組の1つとして位置付けられたCCC(41)の開始に当たっては、考えられる各種手法について通信の秘密の保護の観点等から検討され、当時において問題ないと考えられた上述の手法が採用された（表1）。なお、CCCの準備段階では法的問題を回避するために電気通信事業法を改正することも検討されていたが(42)、結果として関係する法改正は行われていない。

表1　サイバークリーンセンター（CCC）の手法に係る通信の秘密に関する整理

検討対象としたボット対策手法	通信の秘密との関係	違法性阻却事由の整理
ハニーポットへの感染通信を検知し、通信の発信元IPアドレス等をISPに共有する。ISPは発信元である感染者を特定し、注意喚起の連絡を行う。	通信の発信元IPアドレス等は通信の秘密の保護対象であり、それをISPへ共有する行為や、ISPがIPアドレス等と顧客情報を突合して感染者を特定することは通信の秘密の窃用等に該当する。	感染通信はCCCが通信当事者の一方であるため、IPアドレス等のISPへの共有は通信当事者の同意を得た行為である。また、ISPによる感染者の特定は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違法性が阻却される。
ボットネット指令者の通信を傍受し指令者を特定する。 感染端末からC&Cサーバへの通信を遮断する。	通信の秘密の侵害に該当し、実施不可。（CCCの手法として不採用）	―

（出典）サイバークリーンセンター「ボットの脅威との戦い―サイバークリーンセンター（CCC）活動レポート―」2010.9.13, pp.5-6. T-ISAC-Jウェブサイト <https://www.telecom-isac.jp/ccc/report/h21ccc_report.pdf>;「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」2014.4, p.4. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000283608.pdf> を基に筆者作成。

2　インターネットの安定的な運用に関する協議会（2006年～）

(1) 取組の概要

CCCの取組が始まった同時期、「インターネットの安定的な運用に関する協議会」（以下「協議会」）と呼ばれるISP等による活動も始まった。協議会は2006年6月に社団法人日本インターネットプロバイダー協会（Japan Internet Providers Association: JAIPA）等の電気通信事業関連4団体で設立され(43)、サイバー攻撃等に対するISPの対応について、主に電気通信事業法上の通信の秘密の保護規定に係る違法性の有無を検討し、それをガイドライン（以下「協議会ガイドライン」）にまとめる活動を行っている(44)。

従来、サイバー攻撃等に対してISPが通信の遮断等を行う場合、法律解釈の基準がない中で

保存事業（WARP）により保存されたページ）<https://warp.ndl.go.jp/info:ndljp/pid/283520/www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip/pdf/040203_1_s1.pdf>）。

(40)「次世代IPインフラ研究会第二次報告書―「情報セキュリティ政策2005」の提言―」2005.7.7, pp.21-22, 33. 総務省ウェブサイト（国立国会図書館インターネット資料収集保存事業（WARP）により保存されたページ）<https://warp.ndl.go.jp/info:ndljp/pid/283520/www.soumu.go.jp/s-news/2005/pdf/050707_2_2.pdf>

(41)　総務省『平成19年版　情報通信白書』2007, p.287. <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h19/pdf/j3030000.pdf>

(42)　中道理「国家レベルでボットを締め出す―ついに始まる総務省と経産省の共同プロジェクト―」『日経コミュニケーション』458号, 2006.3.15, pp.86-87.

(43)　日本インターネットプロバイダー協会ほか「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の改定について」2011.3.25. <https://www.jaipa.or.jp/other/2015/12/11325.php> 現在、協議会には設立当初からの4団体に加えてICT-ISAC（Ⅱ5で後述）も参加している。

(44)　日本インターネットプロバイダー協会ほか「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　第2版」2011.3.25, p.2. <https://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf>

対応を行うことがリスクになっていること、通信の秘密の保護規定に抵触するおそれがある場合に後ろ向きの対応となってしまうこと等の課題があった。そこで、それまで総務省に個別相談を行いながら実施してきた対策の情報をガイドラインとして明文化した(45)。なお、協議会においては総務省もオブザーバーとして位置付けられているが(46)、通信の秘密に関する課題は民間事業者だけでは克服できないため、関係機関に行政もオブザーバーとして参加すべきという方針は、前節で述べた「情報セキュリティ政策 2005」でも示されていたものである(47)。

協議会ガイドラインは 2007 年 5 月に第 1 版が策定され、関係者限りで配布された(48)。2011 年 3 月に策定された第 2 版以降は公表され、今日に至るまで改定が続けられ運用されている(49)。

(2) 通信の秘密に係る解釈

協議会ガイドラインの内容のうち、特に 2014 年 7 月に策定された第 3 版以降に追加された項目の運用については、次節以降で整理する取組と密接に関係するため次節で詳述する。本節では 2011 年 3 月に策定された第 2 版までの内容について整理することとする。

協議会ガイドラインの第 1 版は概要を除き非公表であったが、その概要によれば、通信の秘密の範囲、侵害についての違法性阻却事由の整理等が行われていたことが分かる(50)。また、第 2 版で公表された内容では、そうした整理に加え、通信の秘密の侵害とその違法性阻却事由が、ISP による具体的なサイバー攻撃対策の事例に即して整理されている（表 2）。

ガイドラインの効果について述べた 2013 年時点の資料によれば、ISP の自社設備に影響があるようなサイバー攻撃への対応には、ガイドラインを参考にして能動的な対応をとることができるようになったという。一方、インターネットの利用者（以下、単に「利用者」）の端末に影響があるサイバー攻撃に対しては「業界のコンセンサスが得られず、対策の方向性が定まっていない」とされ(51)、そうした課題は後年の取組に引き継がれていくこととなった。

3 ACTIVE（2013 ～ 2018 年）

(1) 取組の概要

官民連携のマルウェア対策の取組として、CCC に続いて実施されたのが ACTIVE（Advanced Cyber Threats response InitiatiVE）である。当時、ボットの主な感染経路が、閲覧によってマルウェアに感染するおそれのあるウェブサイト（以下「マルウェア拡散サイト」）を経由するものに

---

(45) 木村孝「インターネット上の情報セキュリティ関連ガイドラインの紹介等について―「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」を中心に―」（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 1 回）資料 4）2013.11.29, pp.[5]-[7]. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000262679.pdf>

(46) 藤田潔・髙部豊彦監修, 髙嶋幹夫『実務電気通信事業法』NTT 出版, 2015, p.798.

(47) 「次世代 IP インフラ研究会第二次報告書―「情報セキュリティ政策 2005」の提言―」前掲注(40), p.20.

(48) 日本インターネットプロバイダー協会ほか　前掲注(43)

(49) 「インターネットの安定的な運用に関する協議会」JAIPA ウェブサイト <https://www.jaipa.or.jp/other/intuse/> 第 1 版から第 3 版までは「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」という名称で策定された。第 4 版以降は「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」に変更されている。最新版は第 6 版である。

(50) 日本インターネットプロバイダー協会ほか「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の策定について」2007.5.30. <https://www.jaipa.or.jp/info/2007/info_070530.html>

(51) 小山覚「サイバー攻撃対策の取り組みについて―マルウェア対策と通信の秘密―」（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 1 回）資料 3）2013.11.29, p.[10]. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000262678.pdf>

表２　協議会ガイドライン第２版での通信の秘密に関する整理

サイバー攻撃対策(注1)	通信の秘密との関係	違法性阻却事由の整理
協議会ガイドライン　第２版（2011 年３月）		
攻撃通信(注2)の受信者から通信の遮断依頼を受け、依頼者への通信を機械的に遮断する。または、依頼者のみならず一律に遮断する。攻撃通信元(注3)を特定し、通信を止めるよう連絡する等の措置を行う。	攻撃通信の分析、検知や遮断に用いる通信の発信元 IP アドレス等は通信の秘密に当たるため、通信の秘密の窃用等に当たり得る。	本対策について遮断対象者から個別の同意を取得すれば通信の秘密の侵害とならない。一律の遮断や攻撃通信元の特定は、攻撃を受けている受信者の設備等に生じる侵害を防止するための正当防衛又は緊急避難として違法性が阻却される(注4)。
大量通信等(注2)の発生により通信設備に支障が生じた場合に、機械的に通信を遮断する。または、影響範囲を最小限にとどめつつ通信遮断を行う。	大量通信等の分析、検知や遮断に用いる通信の発信元 IP アドレス等は通信の秘密に当たるため、通信の秘密の窃用等に当たり得る。	機械的な遮断は通信設備への侵害を防止するための正当防衛又は緊急避難として違法性が阻却される(注4)。遮断範囲を絞りつつ行う遮断のための名前解決要求の拒否(注5)等は正当業務行為に当たる(注4)。
攻撃の意図がないままマルウェア等に起因する大量通信等(注2)を行っているような通信元を特定し、マルウェア等を駆除するよう連絡等を行う。また、個別に通信を遮断する。	大量通信等の通信元の特定、検知や遮断に用いる通信の発信元 IP アドレス等は通信の秘密に当たるため、通信の秘密の窃用等に当たり得る。	通信設備に生じる侵害を防止するための正当防衛又は緊急避難として違法性が阻却される(注4)。

（注 1）出典資料においては、迷惑メール受信の拒否といった必ずしもサイバー攻撃に関係するとは限らない事例の整理もなされているが、本表ではサイバー攻撃に直接的に関係すると考えられる主な事例に絞って取り上げた。
（注 2）DDoS 攻撃等による通信を「大量通信等」、そのうち受信した設備に異常を来す通信を「攻撃通信」とする。
（注 3）攻撃通信元へ自社がインターネットサービスを提供している場合が想定されている。
（注 4）必要な範囲で相当な方法により行われること等が条件となる。
（注 5）通信の前段で行われる通信先 IP アドレスの問合せ（名前解決要求）で、正規の IP アドレスを応答しないことで通信を遮断する。ある IP アドレス宛の通信を機械的に全て遮断するよりも、遮断範囲を絞り込むことができる。
（出典）インターネットの安定的な運用に関する協議会による文書（日本インターネットプロバイダー協会ほか「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　第２版」2011.3.25, pp.10-13. <https://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf>）を基に筆者作成。

移行してきていたが、そうしたマルウェアには CCC の手法では対応できない。そうした背景を踏まえ、2013 年３月から総務省で開催されていた有識者会議「情報セキュリティ アドバイザリーボード」（以下「アドボード」）(52)は、同年４月にまとめた提言で、CCC に新たな取組を加えたマルウェア対策を実施することを掲げていた(53)。その方針は、情報セキュリティ政策会議(54)が同年６月に策定した「サイバーセキュリティ戦略」に内容を具体化しつつ反映され(55)、

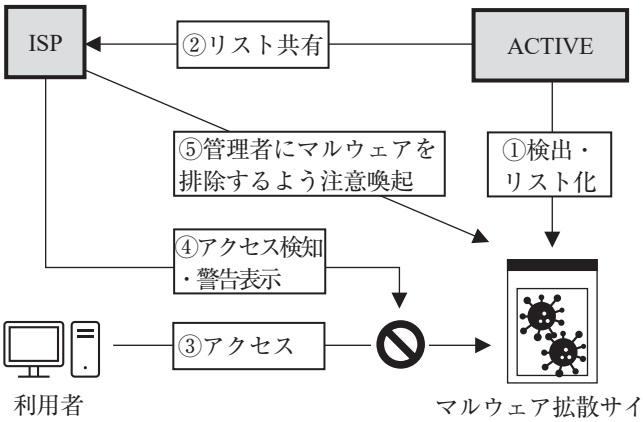
(52)　情報セキュリティ上の課題に対する効果的な対策等について有識者から助言を得ることを目的として開催された（「「情報セキュリティ アドバイザリーボード」開催要綱」（情報セキュリティ アドバイザリーボード（第１回）資料 1-1）2013.3.5. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000211534.pdf>）。
(53)　情報セキュリティ アドバイザリーボード「総務省における情報セキュリティ政策の推進に関する提言」2013.4.5, p.5. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000217000.pdf>
(54)　官民における統一的・横断的な情報セキュリティ対策の推進を図るため、内閣に当時置かれていた高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）に 2005 年に設置された会議（内閣官房情報セキュリティセンター「情報セキュリティ政策会議の設置について」2005.5.30.（国立国会図書館インターネット資料収集保存事業（WARP）により保存されたページ）<https://warp.ndl.go.jp/collections/content/info:ndljp/pid/12213293/www.nisc.go.jp/press/pdf/050530seisaku-press.pdf>）。2015 年に廃止された（「規程の改廃について」p.1. 首相官邸ウェブサイト（国立国会図書館インターネット資料収集保存事業（WARP）により保存されたページ）<https://warp.ndl.go.jp/collections/content/info:ndljp/pid/9450764/www.kantei.go.jp/jp/singi/it2/kettei/pdf/20150630/siryou8.pdf>）。
(55)　情報セキュリティ政策会議「サイバーセキュリティ戦略―世界を率先する強靭で活力あるサイバー空間を目指して―」2013.6.10, p.31. NISC ウェブサイト <https://www.nisc.go.jp/pdf/policy/kihon-s/cyber-security-senryaku-set.pdf>; 情報セキュリティ アドバイザリーボード「政府における情報セキュリティ政策の動きについて」（情報セキュリティ アドバイザリーボード（第３回）資料 3-1）2013.7.5, p.6. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000243681.pdf>

同年 11 月に実際の取組が ACTIVE として開始された(56)。

ACTIVE は総務省が財政支援等を行い、ISP 等が参画する体制で進められた(57)。ACTIVE では、まず「マルウェア駆除」の取組として、CCC と同様にハニーポットを用いたマルウェアの活動の分析や感染者への注意喚起等を行うこととした。加えて実施されたのが、ウェブサイトからの新規感染防止（以下「マルウェア感染防止」）の取組である。「マルウェア感染防止」では、マルウェア拡散サイトに利用者がアクセスした際に、ISP 等が検知し、警告画面を表示して注意喚起する等の働きかけを行った（図 5）。

ACTIVE には 36 社の ISP が参画した(58)。総務省が設定した ACTIVE の実施期間は 2017 年度末までであり(59)、この実施期間を通じ、マルウェア拡散サイトにアクセスしようとした利用者に対して行われた注意喚起は、約 7 万 7 千回に上ったという(60)。

図５　ACTIVE による「マルウェア感染防止」の取組



（出典）湯口高司「ACTIVE（Advanced Cyber Threats response InitiatiVE）プロジェクトの取り組み」（Internet Week 2013 S6（サイバー犯罪の動向と対策、インターネットのセキュリティと通信の秘密）資料）2013.11.28, pp.4-6, 12. JPNIC ウェブサイト <https://www.nic.ad.jp/ja/materials/iw/2013/proceedings/s6/s6-yuguchi.pdf> 等を基に筆者作成。

(2) 通信の秘密に係る解釈

「マルウェア感染防止」の注意喚起を行うためには、利用者がウェブサイトにアクセスする都度、アクセス先の情報とマルウェア拡散サイトのリストとを ISP 等が照合する必要がある。つまり、利用者による通信を常に確認する必要があり、通信の秘密を侵害する。そのため、ACTIVE 開始の時点では注意喚起は個別の同意に基づいて行うものと整理された（表 3）。

---

(56)「「ACTIVE」の実施及び「ACTIVE 推進フォーラム」の開催」2013.10.1. 総務省ウェブサイト <https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000059.html>

(57) 湯口高司「ACTIVE（Advanced Cyber Threats response InitiatiVE）プロジェクトの取り組み」（Internet Week 2013 S6（サイバー犯罪の動向と対策、インターネットのセキュリティと通信の秘密）資料）2013.11.28, p.7. JPNIC ウェブサイト <https://www.nic.ad.jp/ja/materials/iw/2013/proceedings/s6/s6-yuguchi.pdf>

(58)「参加企業・団体」ICT-ISAC ウェブサイト <https://www.ict-isac.jp/active/active/group.html>

(59) 竹内芳明「重要インフラを中心としたサイバーセキュリティ政策」（セミナー「経営戦略としてのサイバーセキュリティ―国民生活の基盤を支える重要インフラへの提言―」資料）2019.5.29, p.33. 日本 HP ウェブサイト <https://jp.ext.hp.com/content/dam/jp-ext-hp-com/jp/ja/ec/business-solution/pdf/190529_security_1_soumu.pdf> 2018 年度以降は、ISP 等が自主的に実施する扱いとなっている。

(60) この数値は ACTIVE におけるマルウェア感染防止活動の実績数が最後に公表された 2018 年 1 月度の活動報告による。「活動実績詳細レポート」（2018 年 1 月度）p.1. ICT-ISAC ウェブサイト <https://www.ict-isac.jp/active/archives/001/201802/1801monthly.pdf>

表３　ACTIVE の手法に係る通信の秘密に関する整理

マルウェア対策手法	通信の秘密との関係	違法性阻却事由の整理
ACTIVE（マルウェア感染防止） マルウェア拡散サイトへのアクセスに対して注意喚起を行う。	注意喚起に利用等されるアクセス先の情報は通信の秘密の保護対象であり、通信の秘密の窃用等に該当する。	利用者の個別の同意に基づいて行うため違法性が阻却される。

（出典）「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」2014.4, p.5. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000283608.pdf> 等を基に筆者作成。

よって、注意喚起を受けるためには、利用者から何らかの形で個別の同意を取得する必要があった(61)。当時、例えば有害なウェブサイトを閲覧不能とするような ISP のサービスにおいて、ACTIVE から提供されたマルウェア拡散サイトのリストが活用されていた例がみられるが(62)、個別の同意はこうしたサービスの申込時等に利用者から取得していたとみられる。

４　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（2013 年～）

(1) 取組の概要

ACTIVE が始まった 2013 年 11 月、もう 1 つの動きとして、総務省における通信の秘密に関する有識者会議の立ち上げがあった。前節で述べた 2013 年の「サイバーセキュリティ戦略」では「情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について検討する」という方針も掲げられていたところ(63)、そうした検討を行う場として「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」（以下「サイバー攻撃対処研究会」）が開催されることとなった(64)。

サイバー攻撃対処研究会は、2014 年から 2021 年にかけて、第一次から第四次までの「とりまとめ」を策定している。そして、これらが策定される都度、その内容を反映し協議会ガイドラインが改定され、ISP 等による実際の運用が行われるというサイクルとなっている(65)。

サイバー攻撃対処研究会による議論のうち、2018 年 9 月に策定された第三次とりまとめ以降のものについては、次節以降で整理する取組と密接に関係するため次節で詳述する。本節では、第二次のとりまとめまでの内容について整理することとする。

(2) 通信の秘密に係る解釈

2014 年 4 月に策定された第一次とりまとめでは、サイバー攻撃に係る複数の新たな対策例を挙げ、それぞれについて通信の秘密との関係が整理された。具体的には、①（個別の同意に

(61)　湯口　前掲注(57), pp.10-11.

(62)　「ネットバリアベーシック（有害サイトブロック）」ぷららウェブサイト（Internet Archive により保存されたページ）<https://web.archive.org/web/20131120130456/http://www.plala.or.jp/option/nbb/>

(63)　情報セキュリティ政策会議　前掲注(55), p.31.

(64)　サイバー攻撃対処研究会の目的は、サイバー攻撃が巧妙化・複雑化する中で、協議会ガイドラインによる対応を行っている電気通信事業者が、通信の秘密等に配慮しつつ、新たな対策や取組を講じられるようにする検討を行うこととされた。総務省総合通信基盤局長及び政策統括官（情報通信担当）の研究会として位置付けられている（「「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」開催要綱（案）」（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 1 回）資料 1）2013.11.29, p.1. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000262668.pdf>）。

(65)　日本インターネットプロバイダー協会ほか「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の改定について」2014.7.22. <https://www.jaipa.or.jp/topics/2014/07/695.php> 等

基づき実施中の）ACTIVE のマルウェア感染防止の取組は、契約約款に基づく事前の包括同意であっても有効である、②テイクダウン（停止措置）がなされた C&C サーバ等に残された通信履歴に基づく感染者の割出しと注意喚起は緊急避難に該当する等の法的整理が示された(66)。

また、2015 年 7 月には「第三者による IP 電話等の不正利用への対策について」という文書が策定され、③ IP 電話(67)の不正利用を検知し電話の休止措置をとること等は正当業務行為に該当するという法的整理が示された上で(68)、総務省による ISP 等への不正利用対策の要請が行われた(69)。さらに、同年 9 月に策定された第二次とりまとめでは、④感染端末から C&C サーバ等への通信の遮断は包括同意であっても有効である等の法的整理が示された(70)。なお、この第二次とりまとめの内容は、同年 5 月のアドボードによる 2 回目の提言で検討が促されていたものである(71)。以上のとりまとめ等の法的整理をまとめると、表 4 のようになる。

これらとりまとめ等の内容を反映し、2014 年 7 月に協議会ガイドラインの第 3 版が、2015 年 11 月に第 4 版が策定され、ISP 等がこれらに基づく対策ができるようになった(72)。例えば、②の法的整理に基づいて感染者であると判明した利用者へ ISP から注意喚起を行い(73)、マルウェアの駆除を促す活動（以下「マルウェア駆除促進」）が、ACTIVE の官民連携の枠組みを利用して 2014 年から 2017 年にかけて 3 回にわたり実施された(74)。これは国内外の警察組織によるボットネットを崩壊させるテイクダウン作戦の成果として得られた情報等を利用したものである(75)。

---

66 「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」2014.4, pp.19-32. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000283608.pdf>

67 インターネットで用いられている通信方式（Internet Protocol: IP）を利用した音声電話サービスのこと。通信方式が同一であるだけなく、実際にインターネット回線を通じて音声を授受するものもある（「インターネット用語 1 分解説「IP 電話とは」」『JPNIC News & Views』vol.85, 2003.6.12. <https://www.nic.ad.jp/ja/mailmagazine/backnumber/2003/vol085.html>）。

68 「第三者による IP 電話等の不正利用への対策について」2015.7.7, pp.4-8. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000367498.pdf>

69 「第三者による IP 電話等の不正利用への対策について（要請）」2015.7.7. 総務省ウェブサイト <https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000096.html> 当時、インターネットと電話機をつなぐ交換機に不正に侵入し、IP 電話を乗っ取るサイバー攻撃が多発していた。攻撃者は乗っ取った IP 電話で国際電話をかけ続け、乗っ取られた側には高額の電話料金が請求されることになる（「IP 電話 乗っ取り多発」『読売新聞』（大阪版）2015.6.12.）。

70 「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 第二次とりまとめ」2015.9, pp.12-24. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000376396.pdf>

71 総務省情報セキュリティ アドバイザリーボード「サイバーセキュリティ政策推進に関する提言」2015.5.22, pp.7-8. <https://www.soumu.go.jp/main_content/000359287.pdf>

72 日本インターネットプロバイダー協会ほか「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　第 3 版」2014.7.22, pp.13, 21-25. <https://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf>; インターネットの安定的運用に関する協議会「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　第 4 版」2015.11.30, pp.12-14, 24-27. JAIPA ウェブサイト <https://www.jaipa.or.jp/other/mtcs/guideline_v4.pdf>

73 「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」2018.9, p.4. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000575399.pdf>

74 「Game Over Zeus」及び「VAWTRAK」と呼ばれるマルウェア並びに「Avalanche」と呼ばれるボットネットを構成するマルウェアが駆除対象となった（「インターネットバンキングに係るマルウェアへの感染者に対する注意喚起の実施」2014.7.18. 総務省ウェブサイト <https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000080.html>;「インターネットバンキングに係るマルウェアへの感染者に対する注意喚起の実施」2015.4.10. 同 <https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000092.html>;「インターネットバンキングに係るマルウェアに感染した端末の利用者に対する注意喚起の実施」2017.3.23. 同 <https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000120.html> 等）。

75 「インターネットバンキングに係る不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について―国際的なボットネットのテイクダウン作戦―」警察庁ウェブサイト（国立国会図書館インターネット資料収集保存事業（WARP）により保存されたページ）<https://warp.ndl.go.jp/info:ndljp/pid/8698606/www.npa.go.jp/cyber/goz/index.html> 総務省としての ACTIVE 実施期間の終了後にも、2019 年 10 月以降に日本国内で感染事例

表４　サイバー攻撃対処研究会第一次・第二次とりまとめ等での通信の秘密に関する整理

検討対象としたサイバー攻撃対策(注1)	通信の秘密との関係	違法性阻却事由の整理
第一次とりまとめ（2014 年 4 月）		
ACTIVE（マルウェア感染防止） マルウェア拡散サイトへのアクセスに対して注意喚起を行う。	注意喚起に利用等されるアクセス先の情報は通信の秘密の保護対象であり、通信の秘密の窃用等に該当する。	本対策のための同意は契約約款になじまないとまでは言えず、契約約款による事前の包括同意であっても有効である(注2)。
ACTIVE 活用の取組（マルウェア駆除促進） テイクダウンがなされた C&C サーバ等に残された通信履歴に基づいて感染者を割り出し、注意喚起の連絡を行う。	利用する履歴（通信の発信元 IP アドレス等）は通信の秘密の保護対象であり、通信の秘密の窃用等に該当する可能性がある。	感染端末が正常かつ安全に機能することについての現在の危難を避けるための緊急避難として違法性が阻却される(注3)。
第三者による IP 電話等の不正利用への対策について（2015 年 7 月）		
ISP 等による実施を総務省が要請 正規の利用者以外の者が利用している蓋然性の高い国際電話について休止措置等を行う。	不正利用の割出し等に用いる発信元電話番号等は通信の秘密の保護対象であり、通信の秘密の窃用等に該当する可能性がある。	電気通信役務の円滑な提供を確保するための正当業務行為として違法性が阻却される(注3)。
第二次とりまとめ（2015 年 9 月）		
ACTIVE（マルウェア被害未然防止） 感染端末から既知の C&C サーバ等への通信を遮断する(注4)。	C&C サーバ宛て通信の検知や遮断に用いる通信の内容は通信の秘密の保護対象であり、通信の秘密の窃用等に該当する。	本対策のための同意は契約約款になじまないとまでは言えず、契約約款による事前の包括同意であっても有効である(注2)。

（注 1）出典資料で整理されている事例のうち、本表では官民連携してのサイバー攻撃対策（下線にて示す。）に直接的に関係すると考えられるものに限って取り上げた。
（注 2）通信の秘密を侵害して得た情報を当該サイバー攻撃対策以外の用途で用いないこと、一旦利用者が約款に同意した後も随時同意内容を変更できること等が条件となる。
（注 3）通信の秘密を侵害して得た情報を当該サイバー攻撃対策以外の用途で用いないこと等が条件となる。
（注 4）厳密には、通信の前段で行われる通信先 IP アドレスの問合せ（名前解決要求）を遮断する。
（出典）「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」2014.4, pp.19-24. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000283608.pdf>;「第三者による IP 電話等の不正利用への対策について」2015.7.7, pp.4-8. 同 <https://www.soumu.go.jp/main_content/000367498.pdf>;「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 第二次とりまとめ」2015.9, pp.12-14. 同 <https://www.soumu.go.jp/main_content/000376396.pdf> を基に筆者作成。

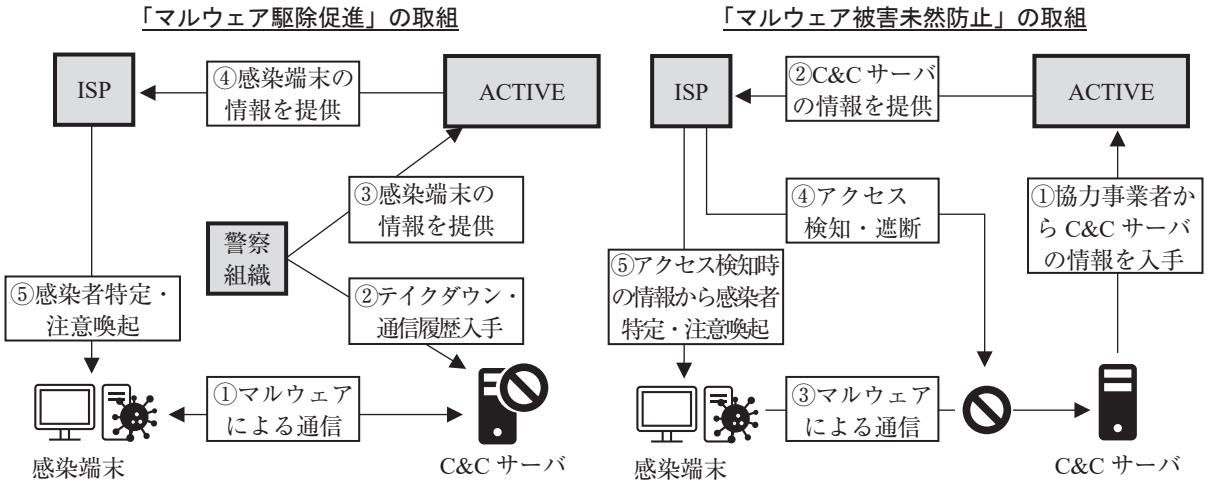
さらに、④の法的整理に基づく ACTIVE による新たな取組「マルウェア被害未然防止」が 2016 年 2 月から実施された。この取組では、ACTIVE が入手した C&C サーバの情報を ISP へ共有し、ISP で利用者との通信を抑止する。また、この通信を行おうとする利用者は感染者である可能性があるため、当該利用者へ注意喚起も行う(76)。この取組により、ACTIVE の実施期間を通じて 5 億回を超える通信遮断が行われている(77)。これらの取組のイメージを図 6 に示す。

が相次いでいるマルウェア「Emotet」の感染者に、国外の警察組織からの情報提供に基づいて注意喚起を行う取組が、ACTIVE 等の一環として 2021 年 2 月から実施されている（サイバーセキュリティ戦略本部「サイバーセキュリティ 2021（2020 年度年次報告・2021 年度年次計画）」2021.9.27, pp.16, 44. NISC ウェブサイト <https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf>）。

(76)「マルウェアに対する被害未然防止の実施」2016.2.26. 総務省ウェブサイト <https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000106.html> ④の法的整理のとおり、こうした通信遮断は、個別の同意を得ずに ISP のサービスの一環として開始されていることが当時の ISP による広報からも確認できる（NTT Communications「国内 ISP として初めて、マルウェアによる情報漏洩から利用者を守る「マルウェア不正通信ブロックサービス」の無料提供を開始―お客さまによるお申し込みも設定も不要、不正通信を判別して自動ブロック―」2016.2.1. <https://www.ntt.com/content/dam/nttcom/mig2/release/monthNEWS/detail/pdf/20160201.pdf> 等）。

(77) この数値は ACTIVE におけるマルウェア被害未然防止活動の実績数が最後に公表された 2018 年 2 月度の活動報告による（「活動実績詳細レポート」（2018 年 2 月度）p.3. ICT-ISAC ウェブサイト <https://www.ict-isac.jp/active/archives/001/201803/1802monthly.pdf>）。

図６　サイバー攻撃対処研究会のとりまとめを踏まえた ACTIVE による追加の取組



（出典）「インターネットバンキングに係るマルウェアへの感染者に対する注意喚起の実施について」2019.4.10. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000352800.pdf>;「マルウェア被害未然防止活動について」ICT-ISAC ウェブサイト <https://www.ict-isac.jp/active/active/damage_prevention.html> 等を基に筆者作成。

５　NOTICE・NICTER 注意喚起（2019 年～）

(1) 取組の概要

2019 年 2 月、総務省及び国立研究開発法人情報通信研究機構（National Institute of Information and Communications Technology: NICT）は、近年 IoT 機器[78]を悪用したサイバー攻撃が増加しているとして、悪用されるおそれのある脆弱（ぜいじゃく）な IoT 機器を調査し、ISP を通じて機器使用者へ注意喚起を行う取組「NOTICE（National Operation Towards IoT Clean Environment）」を開始した。NOTICE では、まず NICT がインターネットを通じてアクセスできる IoT 機器に、容易に推測されるパスワード（「password」「123456」等）を入力する等して、脆弱な機器を特定する。特定結果は ISP に通知され、ISP にて当該機器の使用者の特定を行い、その使用者へパスワードの設定変更を促す等の注意喚起を行う。また、総務省が設置した NOTICE サポートセンターが、当該使用者からの問合せに応じて適切なセキュリティ対策等を案内する[79]。

さらに 2019 年 6 月には、NOTICE に加え、既にマルウェアに感染している IoT 機器を NICT が特定し、NOTICE の枠組みを活用して ISP から機器使用者へ注意喚起を行う取組（以下「NICTER 注意喚起」という。）も開始された。この取組では、NICT が特定した感染端末について、NOTICE の枠組みを活用し ISP から感染者へマルウェアの駆除を促す等の注意喚起を行う。感染端末の特定には、NICT が実施している「NICTER プロジェクト」[80]で得られた、サ

78　IoT（Internet of Things）機器とは、インターネットに接続が可能な機器のことである。センサーやウェブカメラ等の IoT 機器は、機器の性能が限定的、管理が行き届きにくい等、サイバー攻撃に狙われやすい特徴を持つ。

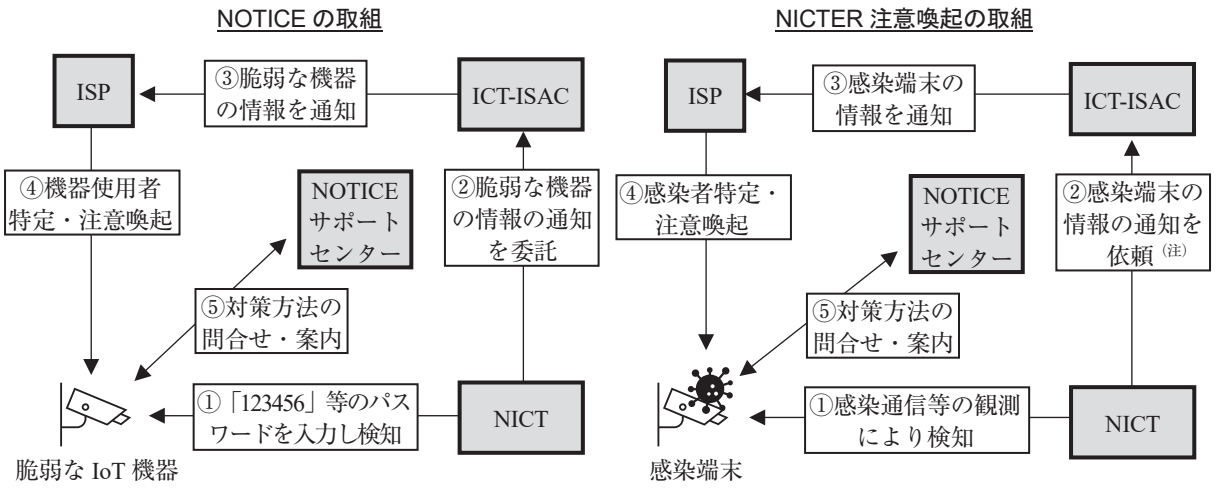
79　総務省・情報通信研究機構「IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施」2019.2.1. <https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00011.html>

80　NICTER（Network Incident analysis Center for Tactical Emergency Response）は無差別型サイバー攻撃の大局的な動向を把握することを目的としたサイバー攻撃観測・分析システムであり、ダークネットと呼ばれる未使用の IP アドレス群を大規模に観測する。本来、未使用の IP アドレスへ通信はなされないはずであるが、感染端末による感染通信等は未使用の IP アドレスにも大量に送られるため、ダークネットで観測された通信の分析によりサイバー攻撃の動向を把握できる（「NICTERWEB」NICTER ウェブサイト <https://www.nicter.jp/>）。

イバー攻撃の観測等に基づく情報を用いる[81]。次項（ⅱ）で後述する認定協会（ICT-ISAC）の位置付けも含め、これら取組のイメージを図7に示す。

2023年12月時点で、これらの取組には82社のISPが参画している。NICTからISPになされた通知数は、開始から同月までにNOTICEが約13万件、NICTER注意喚起が約88万件となっている[82]。

図7　NOTICE・NICTER注意喚起の取組



（注）公表されている資料においてNICTER注意喚起におけるICT-ISACの役割を明示したものは見当たらないものの、NICTER注意喚起にICT-ISACが参画していること、NICTER注意喚起はNOTICEの枠組みを活用しているとされていることから、本図では感染端末の情報の通知に際してICT-ISACが介在するよう表現した。
（出典）「IoT機器のセキュリティ対策に係る取組について」2019.6.16. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000626522.pdf> 等を基に筆者作成。

(2) 取組のための立法措置

NOTICE及びNICTER注意喚起の開始に先立ち、2018年5月にNICTの設立根拠等を定める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。以下「NICT法」）及び電気通信事業法の改正法[83]が成立した。この法改正にはサイバーセキュリティに関する内容が含まれるが、それは2017年10月から総務省で開催された「円滑なインターネット利用環境の確保に関する検討会」（以下「円滑検討会」）[84]を始めとするサイバーセキュリティに関する政府の3つの会議による提言等で、法律上の位置付けも含めて制度整備の検討の必要性が示されていたことを踏まえたものである（表5）[85]。

81　総務省ほか「マルウェアに感染しているIoT機器の利用者に対する注意喚起の実施」2019.6.14. <https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00025.html>
82　「実施状況」NOTICEウェブサイト <https://notice.go.jp/status>
83　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（平成30年法律第24号）
84　2020年に開催予定（当時）の東京オリンピック・パラリンピック競技大会に際して日本に対する大規模なサイバー攻撃の発生が懸念されること等から、電気通信事業においてインターネットの障害を防ぐ適切な対策が講ぜられるための方策について検討することを目的として開催された（「「円滑なインターネット利用環境の確保に関する検討会」開催要綱」（円滑なインターネット利用環境の確保に関する検討会（第1回）資料1-1）2017.10.26. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000517235.pdf>）。
85　影井敬義ほか「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」『情報通信政策研究』2(1), 2018, pp.168-170. <https://doi.org/10.24798/jicp.2.1_167>

表５　2018 年の電気通信事業法及び NICT 法改正に係る提言等

文書策定時期	会議	文書	法改正に係る内容
2017 年 7 月	サイバーセキュリティ戦略本部（内閣）	サイバーセキュリティ戦略中間レビュー	ボット撲滅に向け継続的かつ広範な実態調査ができるよう、必要となる法的整理を行うべきである。
2017 年 10 月	サイバーセキュリティタスクフォース（総務省）	IoT セキュリティ総合対策	IoT 機器等のサイバー攻撃の踏み台となってネットワークに悪影響を及ぼすおそれのある機器について、所要の脆弱性調査と当該調査結果に基づく対策を講じる必要がある。脆弱性調査の効果を高める観点から所要の法制度の整備についても検討する必要がある。
2018 年 2 月	円滑なインターネット利用環境の確保に関する検討会（総務省）	対応の方向性	通信ネットワークを保護する目的で行われる情報共有を促進するため、結節点となる第三者機関を法律上位置付け、通信の秘密を含む情報の収集、分析、共有等の枠組みを明確化する必要がある。

（出典）「2020 年及びその後を見据えたサイバーセキュリティの在り方について―サイバーセキュリティ戦略中間レビュー―」（2017 年 7 月 13 日サイバーセキュリティ戦略本部決定）NISC ウェブサイト <https://www.nisc.go.jp/pdf/policy/kihon-s/csway2017.pdf>; サイバーセキュリティタスクフォース「IoT セキュリティ総合対策」2017.10, p.5. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000510701.pdf>;「円滑なインターネット利用環境の確保に関する検討会　対応の方向性」2018.2, p.12. 同 <https://www.soumu.go.jp/main_content/000534017.pdf> を基に筆者作成。

この 2018 年の法改正では、サイバー攻撃又はそのおそれへの対処に係る 2 つの制度の整備が行われている。以下の（ｉ）及び（ii）では、NOTICE 及び NICTER 注意喚起の開始につながる事項を中心に、これら制度整備の内容をそれぞれ整理する。

（ｉ）NICT 法改正（NICT の業務への IoT 機器調査の追加）

NICT 法の改正では、NICT による新たな業務として、パスワード設定等に不備のある電気通信設備を調査し、電気通信事業者に対して当該設備の使用者への直接の注意喚起を求める通知を行うことが定められた（NICT 法第 14 条第 1 項第 7 号ロ[86]）。電気通信事業者への通知については、認定協会（（ii）で後述）に委託できるとした（同法第 18 条第 6 項第 2 号[87]）[88]。NOTICE はこの制度整備に基づき開始された取組である[89]。

NICT がパスワード設定等の不備を確認するために行う通信は「特定アクセス行為」と定義される。これは不正アクセス禁止法（不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号））で禁じられている不正アクセス行為に該当するおそれがあるため、改正後の NICT 法では、特定アクセス行為に係る不正アクセス行為からの除外措置も定められている（同法第 18 条第 8 項[90]）[91]。

なお、この NICT による業務は、2018 年の NICT 法改正では 2024 年 3 月までに限るものと定められた。これは、5 年間実施された CCC が成果を上げたことを踏まえ、同程度の実施期間があれば一定の成果を見込めるためと説明された[92]。その後、2023 年 8 月に、総務省の有

86　2023 年の NICT 法改正の施行（後掲注96）までは第 8 条第 2 項
87　2023 年の NICT 法改正の施行（後掲注96）までは第 8 条第 3 項
88　影井ほか　前掲注85), pp.174-176.
89　総務省・情報通信研究機構　前掲注79)
90　2023 年の NICT 法改正の施行（後掲注96）までは第 8 条第 7 項
91　影井ほか　前掲注85), p.175.
92　第 196 回国会衆議院総務委員会議録第 9 号　平成 30 年 4 月 12 日　p.19.（谷脇康彦総務省政策統括官答弁）

識者会議「サイバーセキュリティタスクフォース」[93]及びその下に開催された「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」[94]が、同年までのNOTICE等による取組を振り返った上で、当初の期限以降も取組の継続が必要である等とする提言をまとめた[95]。これを受ける内容を含んだNICT法の再改正法が同年12月に成立し、期限が撤廃されるとともに、NICTによる調査対象の拡充に向けた制度整備が行われている[96]。

（ⅱ）電気通信事業法改正（認定送信型対電気通信設備サイバー攻撃対処協会に係る制度の創設）

電気通信事業法の改正では、サイバー攻撃[97]への対処に係る電気通信事業者の情報共有の結節点として位置付けられる、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」）に係る制度整備が行われた。認定協会は、電気通信事業者が設立した一般社団法人であって、総務大臣の認定を受けた第三者機関である（電気通信事業法第116条の2第1項）。認定協会は、パスワード設定等に不備がある機器の使用者へ注意喚起を行うよう、当該使用者にインターネット接続サービスを提供している電気通信事業者へ通知を行う業務を、NICTからの委託に基づき実施する。また、ある電気通信事業者からサイバー攻撃の送信元に係る情報の提供を受け、その送信元にインターネット接続サービスを提供している他の電気通信事業者に対処を求める通知を行う、といった役割も担う（NICT法第18条第8項[98]による読替え後の電気通信事業法第106条の2第2項）[99]。

この制度整備を踏まえ、2019年1月にはISP等の事業者団体である一般社団法人ICT-ISAC[100]が認定協会として認定を受けている[101]。NOTICEでは、NICTの調査で特定した情報を基に

---

93 IoT/AI時代を見据えたサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として開催された（「「サイバーセキュリティタスクフォース」開催要綱（案）」（サイバーセキュリティタスクフォース（第1回）資料1-1）2017.1.30. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000463347.pdf>）。

94 NOTICE等の取組を含めた情報通信ネットワークにおけるサイバーセキュリティ対策について検討を行うことを目的として開催された（「「情報通信ネットワークにおけるサイバーセキュリティ対策分科会」開催要綱」（情報通信ネットワークにおけるサイバーセキュリティ対策分科会（第1回）資料1-1）2023.1.18. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000856808.pdf>）。

95 総務省サイバーセキュリティタスクフォース「ICTサイバーセキュリティ総合対策2023」2023.8, pp.12, 52, 68-78. <https://www.soumu.go.jp/main_content/000895981.pdf>

96 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等の法律（令和5年法律第87号）による。施行日は2024年4月1日である。この改正では、NICTによる調査の対象をファームウェア（機器内蔵のソフトウェア）等に脆弱性があるIoT機器や既にマルウェアに感染しているIoT機器にも拡げられるようにするためとして、特定アクセス行為に係るNICTの中長期目標の策定に関する規定（改正法施行後のNICT法第18条第2項から第5項）等が整備された（「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等の法律の概要」総務省ウェブサイト <https://www.soumu.go.jp/main_content/000917691.pdf>）。

97 認定協会に係る制度は「送信型対電気通信設備サイバー攻撃」を対象とする。同攻撃は、送信先の電気通信設備の機能に障害を与える電気通信の送信や、そうした送信を指令する送信による攻撃を指し、DDoS攻撃のほか、ランサムウェア（データを暗号化し、その復元と引換えに金銭を要求するマルウェア）を感染させる通信も含む。

98 2023年のNICT法改正の施行（前掲注96）までは第8条第7項

99 影井ほか　前掲注85, pp.170-176.

100 ISAC（Information Sharing and Analysis Center）はサイバーセキュリティ対策のための連携を行う団体であり、業種別に設置される。日本初のISACとして2002年に発足した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（Telecom-ISAC Japan: T-ISAC-J）は、CCC、協議会、ACTIVE及びサイバー攻撃対処研究会にも参画してきた。T-ISAC-Jを発展的に継承したのが2016年に発足したICT-ISACである（中尾康二「ISACを活用する情報共有について」（サイバーセキュリティタスクフォース（第17回）資料17-4）2019.11.22, p.8. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000661593.pdf> 等）。

101 「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」2019.1.8. 総務省ウェブサイト <https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000057.html>

ISPへ通知を行う業務を、認定協会としてのICT-ISACがNICTから委託されているとみられる(102)。

なお、2021年7月のサイバーセキュリティタスクフォースの提言では、NOTICE等の従来の取組だけでは必ずしも対策が十分でないおそれがあるとして、サイバー攻撃の予兆を捉えて早期に対処するための制度的な観点の検討を行うことが重要等とされた(103)。2018年の法改正で定められていた認定協会による業務は、実際に行われたサイバー攻撃への対応にとどまっていたが、そうした提言もなされる中、2022年6月に電気通信事業法の再改正法が成立し、サイバー攻撃発生の予兆と言える行為への対応も認定協会の業務に含まれることとなった（電気通信事業法第116条の2第1項第1号ロ）(104)。

(3) 通信の秘密に係る新たな法規定・解釈

NOTICEで行われているような、認定協会の業務として定められている電気通信事業者への通知では、サイバー攻撃に係る通信履歴等、通信の秘密に該当する情報を取り扱うこととなる。そうした通信の秘密の適切な取扱いを担保する観点から、2018年の法改正では認定協会の業務について特に守秘義務が規定された（電気通信事業法第116条の4）。さらに、認定協会でそうした業務に従事する者は電気通信事業に従事する者とみなし（同法第164条第4項及び第5項）、通信の秘密を侵した場合の罰則を加重している（同法第179条第2項）(105)。

また、NOTICEやNICTER注意喚起の開始に先立ち、2018年9月にサイバー攻撃対処研究会がこれら取組に関する法的整理等を行った第三次とりまとめを策定している(106)。これは、今後のDDoS攻撃等に対応していくに当たり、改めてサイバー攻撃対処研究会において通信の秘密等に係る整理を行うべきとする円滑検討会の提言(107)を踏まえたものである(108)。

さらに、2021年11月には第四次とりまとめが策定されているが(109)、こちらはサイバー攻撃の予兆を捉える手段として、同年7月のサイバーセキュリティタスクフォースの提言で言及されていた(110)「フロー情報」（ネットワーク内を通過する通信の外形的情報をサンプリングしたもの）(111)の分析に係る内容となっている（表6）。

---

(102) NICTは「パスワード設定等に不備のある機器情報を電気通信事業者へ通知する作業」について、「法令等の規定により契約の相手方が明確に一に特定される」ことを理由に、ICT-ISACと随意契約を結んでいる（例えば2018年度について、「随意契約の公示」2019.5.10, p.[31]. NICTウェブサイト <https://www.nict.go.jp/tender/lde9n2000000b8t9-att/butsuekizuiih30.pdf>）。

(103) サイバーセキュリティタスクフォース「ICTサイバーセキュリティ総合対策2021」2021.7, pp.13-15. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000761893.pdf>

(104) 電気通信事業法の一部を改正する法律（令和4年法律第70号）による。中川将史ほか「電気通信事業法の一部を改正する法律」『情報通信政策研究』6(1), 2022, p.193. <https://doi.org/10.24798/jicp.6.1_181>

(105) 影井ほか　前掲注(85), pp.173-174. 電気通信事業従事者への罰則の加重についてはⅠ1を参照。

(106) 「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」前掲注(73)

(107) 「円滑なインターネット利用環境の確保に関する検討会 対応の方向性」2018.2, pp.6-9. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000534017.pdf>

(108) 林紘一郎・田川義博「サイバー攻撃の被害者である民間企業の対抗手段はどこまで可能か―日米比較を軸に―」『情報セキュリティ総合科学』10号, 2018.11, pp.57-58. <https://www.iisec.ac.jp/proc/vol0010/hayashi-tagawa18.pdf>

(109) 「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」2021.11. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000779208.pdf>

(110) サイバーセキュリティタスクフォース　前掲注(103)

(111) 流れる通信の1万分の1程度を採取し、その送信元・送信先IPアドレス等を機械的に抽出する。収集・蓄積したフロー情報を分析し、複数の感染端末が共通の相手方（サイバー攻撃対象、C&Cサーバ等）と通信するような特徴を見いだすことで、未知のC&Cサーバを検知し得るとされている（「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」前掲注(109), pp.21-22.）。

表６　サイバー攻撃対処研究会第三次・第四次とりまとめでの通信の秘密に関する整理

検討対象としたサイバー攻撃対策(注1)	通信の秘密との関係	違法性阻却事由の整理
第三次とりまとめ（2018 年 9 月）		
NOTICE 信頼できる第三者からの情報提供に基づいて、脆弱性を有する機器の情報が明らかとなった場合に、当該機器の使用者を特定し、注意喚起の連絡を行う。	機器使用者の特定のために利用する ISP の保有する通信履歴等は通信の秘密の保護対象であり、通信の秘密の窃用等に該当する。	本対策のための同意は契約約款になじまないとまでは言えず、契約約款による事前の包括同意であっても有効である(注2)。限定的な条件下(注3)においては、電気通信役務の提供に生じる支障を防止するための正当業務行為としても違法性が阻却される。
NICTER 注意喚起 信頼できる第三者からの情報提供や自らの調査に基づいて感染者の可能性が高い使用者を特定し、注意喚起の連絡を行う。		
第四次とりまとめ（2021 年 11 月）		
フロー情報分析の実証事業 平時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(注4)。	フロー情報は通信の秘密の保護対象であり、通信の秘密の窃用等に該当する。	電気通信役務の安定的かつ円滑な提供の確保のための正当業務行為として違法性が阻却される(注5)。
フロー情報分析の実証事業 フロー情報により検知した C&C サーバに関する情報を、適切な事業者団体（認定協会である ICT-ISAC 等）等に提供する。	C&C サーバに関する情報は個別の通信と切り離されたものであり、通信の保護規定に直ちに抵触するとまでは言えない。	―

（注 1）出典資料で整理されている事例のうち、本表では官民連携してのサイバー攻撃対策（下線にて示す。）に直接的に関係すると考えられるものに限って取り上げた。
（注 2）一旦利用者が約款に同意した後も随時同意内容を変更できること等が条件となる。
（注 3）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り、当該支障を防ぐために必要な限度で機器の使用者に対してのみ注意喚起を行うことが条件となる。
（注 4）複数の感染端末が共通の相手方（サイバー攻撃対象、C&C サーバ等）と通信するような特徴を見いだすことで、未知の C&C サーバを検知し得るとされている。
（注 5）通信の秘密を侵害して得た情報を当該サイバー攻撃対策以外の用途で用いないこと等が条件となる。
（出典）「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」2018.9, pp.12-16, 21-25. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000575399.pdf>;「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」2021.11, pp.9-14. 同 <https://www.soumu.go.jp/main_content/000779208.pdf> を基に筆者作成。

これらとりまとめの内容を反映し、協議会ガイドラインも 2018 年 11 月に第 5 版が、2021 年 12 月に第 6 版が策定されている(112)。これに基づいて NOTICE や NICTER 注意喚起が行われているほか、第四次とりまとめの法的整理に基づく取組として、ICT-ISAC 等によって総務省の実証事業「電気通信事業者におけるフロー情報分析による C&C サーバ検知に関する調査」が、電気通信事業法再改正による認定協会の業務範囲拡大後の 2022 年 9 月から実施され、サイバー攻撃に予防的に対処する手法や有効性が検証されている(113)。NOTICE やこうした調査による情報の収集・蓄積、分析により、ボットネットを観測する官民連携の「統合分析対策センター（仮称）」を立ち上げるという構想もなされている(114)。

(112)　インターネットの安定的運用に関する協議会「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 第 5 版」2018.11.30, pp.25-28, 30-32. JAIPA ウェブサイト <https://www.jaipa.or.jp/other/mtcs/guideline_v5.pdf>; 同「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　第 6 版」2021.12.15, pp.35-37. 同 <https://www.jaipa.or.jp/other/mtcs/guideline_v6.pdf>

(113)　ICT-ISAC「電気通信事業者におけるフロー情報分析による C&C サーバ検知に関する調査について」2022.9.16. <https://www.ict-isac.jp/news/news20220916.html>; 同「電気通信事業者におけるフロー情報分析による C&C サーバ検知に関する調査について（C&C サーバリスト共有トライアルの実施）」2023.8.25. <https://www.ict-isac.jp/news/news20230825.html>

(114)　総務省サイバーセキュリティタスクフォース　前掲注(95), pp.82, 86-87.

なお、サイバー攻撃対処研究会のとりまとめや協議会ガイドラインはISP等の行為について整理したものであるが、他方、NOTICEにおけるNICTの行為について、通信の秘密を侵害しないのか疑問が呈されることがある(115)。これについては、NICTの特定アクセス行為によって収集するのはIoT機器の使用者とNICTとの通信に係る情報であり、当該機器と第三者との間の通信とは関係がなく、通信の秘密の保護対象には当たらないと説明されている(116)。また、NICTER注意喚起におけるNICTの行為も、NICTが感染端末等からの通信を受けて分析するものであるため、同様に第三者との間の通信とは関係がないことが説明されている(117)。

Ⅲ　これまでのサイバーセキュリティ対策の評価と論点

1　違法性阻却事由解釈の積上げの成果と限界

Ⅱで述べてきたように、ISP等によるサイバーセキュリティ対策は、通信の秘密に関する違法性阻却事由についての解釈が積み重ねられた上で、合理的なサイバーセキュリティ対策を可能とする枠組みがとられてきている(118)。このように、日本において通信の秘密の要素と考えられる事項に関する電気通信事業の実務は、一貫して慎重な議論の末に方針が定まる傾向にある。これは、通信の秘密の侵害に関する判断が簡単ではない上に、その判断を誤ると罰則適用の対象になりかねないため、ISP等としては慎重にならざるを得ないことが背景にある(119)。

本来であれば、然るべき立法を行い、法令行為による違法性阻却を活用していくことが積極的に検討されるべきであるが、技術の進展が著しいサイバーセキュリティの領域においては、立法を適切なタイミングで行うことには限界がある。そこで、処罰されない行為の要件の判断については、所管官庁や業界の専門家等によって解釈・運用の指針が積極的に策定されるべきとされる(120)。こうした考え方に沿った、サイバー攻撃対処研究会の検討を受けて協議会がガイドラインを策定するといった取組は、「日々進化するサイバー攻撃への対策にとにかく一歩踏み出すため」の「極めて現実的な判断」に基づくものであったと言われる(121)。

しかし、慎重なアプローチであったとしても、各種取組は一定の評価を得てきた。特に、サイバー攻撃対処研究会による法的整理は「通信の秘密を墨守することに慣れていた通信事業者には、善悪の判断が逆転するほどの大きな変化」であり(122)、罪に問われない範囲や手法が明確になったことで、ISP等はサイバー攻撃対策を安心して実施できるようになったという(123)。

---

(115)　例えば「「通信の秘密に抵触のおそれ」無差別侵入し調査へ」『NHK政治マガジン』2019.1.25. <https://www.nhk.or.jp/politics/articles/statement/13452.html> 当記事では、IoT機器へ侵入し当該機器の通信先が分かってしまった場合に通信の秘密を侵害する、との指摘を取り上げている。

(116)　第212回国会衆議院総務委員会議録第3号　令和5年11月9日　p.6.（山内智生総務省サイバーセキュリティ統括官答弁）

(117)　「マルウェアに感染しているIoT機器の利用者への注意喚起」2019.6.14. NOTICEウェブサイト <https://notice.go.jp/nicter>

(118)　宍戸常寿「円滑なインターネット利用環境の確保に関する検討会（第1回）＜宍戸構成員提出資料＞」（円滑なインターネット利用環境の確保に関する検討会（第1回）資料1-3-3）2017.10.26. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000517241.pdf>

(119)　髙嶋幹夫『教材電気通信事業法』日本データ通信協会, 2021, pp.193-194.

(120)　鎮目ほか編, 荒木ほか　前掲注(23), p.75.

(121)　藤田・高部監修, 高嶋　前掲注(46), pp.793-794.

(122)　小山覚「第304号コラム：サイバー攻撃対策と「通信の秘密」の考え方」2014.3.31. デジタル・フォレンジック研究会ウェブサイト <https://digitalforensic.jp/2014/03/31/column304/>

(123)　小山覚「第326号コラム：サイバー攻撃対策と「通信の秘密」の考え方 その2」2014.9.1. デジタル・フォレンジック研究会ウェブサイト <https://digitalforensic.jp/2014/09/01/column326/>

ただし、法律の最終的な解釈を行うのは総務省ではなく裁判所である。また、協議会ガイドラインもあくまで業界の自主ガイドラインであり、法的な効果はない。訴訟等になった際には、協議会ガイドラインが裁判所の判断の参考とされることが期待されてはいるものの(124)、本来、違法性阻却事由等は個別の事例ごとに判示される性格のものであるとも指摘される(125)。

また、次々と起こる新しい問題に対処するためには、個別の技術的手段を一つ一つ検討していくアプローチには限界がある(126)。サイバー攻撃対処研究会の構成員からも、日々巧妙化し激しさが増すサイバー攻撃に対しては、スピード感の面から課題が多いと述べられている(127)。

２　日本のサイバーセキュリティ対策の独自性

法的解釈を整え、通信の秘密の侵害により違法性が問われないように手法に工夫を凝らしつつ進められてきた日本のサイバーセキュリティ対策は、世界的にも独自性のあるものとして評価されることがある。例えば、CCC のような官民連携のボットネット対策は、CCC 開始当時は世界的にも稀有な取組とされていた(128)。CCC 実施時には、海外で CCC を参考にした組織の発足も検討され、CCC には各国からの問合せが寄せられていた(129)。日本の影響を受け、実際に官民連携のボット対策プロジェクトがドイツで導入されるといった事例もあった(130)。また、CCC に続く ACTIVE も、世界初のタイプの官民連携プロジェクトとされていた(131)。

さらに、NOTICE は海外にも例がない先進的な取組であることが、開始時に総務省からアピールされていた(132)。同様の取組は、2023 年時点でも依然として日本以外では確認されておらず(133)、海外からの関心も高いと言われている(134)。

他方、通信の遮断による DDoS 攻撃の抑止といった、サイバー攻撃等への ISP 等による直接的な対応は、日本に限らず海外でも実施されている(135)。多くの国でも通信の秘密の保護は法律等で規定されているが(136)、サイバー攻撃等への対応もまた法律や規則に基づく行為として行われている（表 7)。法律に基づかず、あくまで違法性阻却事由の検討に基づき対応を進めてきた日本は、この点でも独自性のあるアプローチをとってきたと言える。

---

(124)　木村　前掲注(45), p.16.
(125)　小向　前掲注(11), p.44.
(126)　同上
(127)　小山覚「第 687 号コラム：サイバー攻撃対策と「通信の秘密」の考え方 その 5」2021.10.18. デジタル・フォレンジック研究会ウェブサイト <https://digitalforensic.jp/2021/10/18/column687/>
(128)　サイバークリーンセンター「平成 18 年度　サイバークリーンセンター活動報告」p.27. T-ISAC-J ウェブサイト <https://www.telecom-isac.jp/ccc/report/h18ccc_report.pdf>
(129)　情報処理推進機構　前掲注(38)
(130)　高橋郁夫「インターネット媒介者の役割と「通信の秘密」」『Nextcom』16 号, 2013.Win, p.7. ドイツでは 2010 年 9 月に連邦情報技術安全庁（Bundesamt für Sicherheit in der Informationstechnik: BSI）及びインターネット産業協会（eco）の連携によるボットネット対策プロジェクト「Botfrei」が立ち上がった（pmeyer, “Wir Haben Geburtstag: 10 Jahre Botfrei,” 2020.9.15. Botfrei Website <https://botfrei.de/wir-haben-geburtstag-10-jahre-botfrei/>）。
(131)　湯口　前掲注(57), p.4.
(132)　「NOTICE キックオフイベント開催 総務省―NICT、電気通信事業者が連携強化」『電波タイムズ』（電子版）2019.2.20. <https://www.dempa-times.co.jp/administration/1550625717_78481/>
(133)　第 212 回国会衆議院総務委員会議録第 3 号　前掲注(116), p.8.（鈴木淳司総務大臣答弁）
(134)　「サイバーセキュリティタスクフォース（第 44 回）議事要旨」2023.6.29, p.[4]. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000897119.pdf>
(135)　情報セキュリティ大学院大学「インターネットと通信の秘密」研究会「インターネット時代の「通信の秘密」各国比較」2014.5, p.6. <https://lab.iisec.ac.jp/~hayashi/2014-7-7.pdf>
(136)　ドイツ及び韓国は憲法上に明文の規定がある。また、英国、ドイツ、フランス及び韓国については法律においても定められている。米国には直接的な法律上の規定はないものの、プライバシーの保護の観点等による関連する規定が存在する（同上, p.2.）。

表７　直接的なサイバー攻撃対策を通信事業者が法的根拠に基づき実施している諸外国の例

	サイバー攻撃対策に係る事項(注1)	規定を行う法律等
米国	通信事業者の権利、財産を保護するため、通信事業者による通信の傍受、開示又は利用を認める。そうした目的又はサービスの不正利用等から利用者を保護するための通信履歴の記録を認める。	・合衆国法典第 18 編第 2511 条（18 U.S.C. § 2511）第 2 項第 a 号 (i) 及び第 h 号 (ii) ・合衆国法典第 18 編第 3121 条（18 U.S.C. § 3121）第 b 項
欧州連合（EU）	通信事業者による、ネットワーク、ネットワークを介して提供されるサービス及び利用者の機器のセキュリティ等を確保するための通信制限等を認める(注2)。	EU 規則第 2015/2120 号第 3 条第 3 項第 b 号
英国	（EU 離脱後も EU 規則第 2015/2120 号を国内法化し規律）	―
ドイツ	通信事業者は、攻撃検出システムを含む手段によりサイバー攻撃等に適切に対応すること。また、通信事業者による、通信障害の発生元からの通信の遮断等を認める。	電気通信法（Telekommunikationsgesetz）第 165 条第 1 項から第 7 項及び第 169 条第 6 項及び第 7 項
フランス	通信事業者は、EU 規則第 2015/2120 号に定めるネットワーク中立性を確保すること(注3)。	郵便・電子通信法典（Code des postes et des communications électroniques）L. 第 33-1 条第 I 項第 q 号
韓国	通信事業者は、利用者のシステムでの異常現象がネットワークに深刻な影響を及ぼすおそれがある等の場合、利用約款に基づき、サービスの全部又は一部を中断できる。	情報通信網利用促進及び情報保護等に関する法律（정보통신망 이용촉진 및 정보보호 등에 관한 법률）第 46 条の 2 第 1 項

（注 1）各規定の対象となる主体の定義は各国で異なるが、本表上の表現は「通信事業者」に統一した。
（注 2）EU 加盟国の通信分野の規制当局をメンバーとする EU の専門機関 BEREC（Body of European Regulators for Electronic Communications）が EU 規則第 2015/2120 号第 5 条第 3 項に基づき定めた各国の規制当局向けガイドラインによると、第 3 条第 3 項第 b 号を遂行する手段にはサイバー攻撃の発信元からの通信の遮断等が含まれる。
（注 3）ネットワーク中立性とは、全ての利用者はネットワーク上で平等なアクセスが可能であるべきとする考え方。フランスの通信分野の規制当局である ARCEP（Autorité de Régulation des Communications Électroniques et des Postes）は、EU 規則第 2015/2120 号の制定以前から、ネットワーク中立性確保を目的とした、ネットワークの安全対策のための帯域制御（通信量の制限）を認めている。
（出典）BEREC, “BEREC Guidelines on the Implementation of the Open Internet Regulation,” 2022.6.9, pp.27-28. <https://www.berec.europa.eu/sites/default/files/files/document_register_store/2022/6/BoR_(22)_81_Update_to_the_BEREC_Guidelines_on_the_Implementation_of_the_Open_Internet_Regulation.pdf>; Ofcom, “Net Neutrality Review,” 2023.10.26, pp.7-8. <https://www.ofcom.org.uk/__data/assets/pdf_file/0017/270260/Statement-Net-Neutrality-Review.pdf>; ARCEP, «Neutralité de l’internet et des réseaux: Propositions et recommandations,» 2010.9, pp.24-25. <https://www.arcep.fr/uploads/tx_gspublication/net-neutralite-orientations-sept2010.pdf> 及び各法令を基に筆者作成。

なお、表 7 で示したのはあくまで ISP 等による対策についての法的規定である。日本における能動的サイバー防御で想定されているように、サイバー攻撃に対して政府が先制的な被害防止措置を行う場合には、これらとは別に、政府機関の権限を定める規定、ISP 等への政府機関への協力義務を定める規定等が多くの国で整備されていることに留意が必要である(137)。

３　解釈論から立法論への展開

サイバー攻撃対処研究会開催につながる提言を含む 2013 年の「サイバーセキュリティ戦略」を検討していた情報セキュリティ政策会議の場では、既に「通信の秘密の過剰な保護」をやめるべき、現行法制の問題を解消しサイバー攻撃の予防を目的とした通信の傍受を可能にすべき、との趣旨の発言がなされていた(138)。その後、サイバー攻撃対処研究会等による法的解釈の整理だけでなく、電気通信事業法及び NICT 法の改正を伴う新しいサイバーセキュリティ対策の取組も進められてきたが、このような取組は既存の枠組みにおける「漸進的な改善策、弥縫策」

(137)　米国、英国、ドイツ及びフランスにおけるそうした法的根拠等をまとめているものとして以下を参照。日工組社会安全研究財団「諸外国におけるサイバー事案の捜査手法等に関する調査研究報告書」2023.3. <https://www.syaanken.or.jp/wp-content/uploads/2023/03/cyber202303_01.pdf>
(138)　「高度情報通信ネットワーク社会推進戦略本部 情報セキュリティ政策会議 第 33 回会合 議事要旨」2013.3.26, p.6. NISC ウェブサイト（国立国会図書館インターネット資料収集保存事業（WARP）により保存されたページ）<https://warp.ndl.go.jp/info:ndljp/pid/10955906/www.nisc.go.jp/conference/seisaku/dai33/pdf/33gijiyoushi.pdf>

にすぎず、根本的な解決にはつながらないとの指摘もある(139)。

そうした中で、より直接的な立法措置に向けた議論もなされてきた。特に、通信の秘密との関係が問題となっている各種の措置については、法律上に位置付けるべきとの指摘がみられる(140)。こうした指摘は、例えば、法律の内容や解釈については必ずしも憲法の通信の秘密条項に準じる必要はなく、一定程度柔軟な制度設計が可能である、といった解釈に基づいている(141)。

具体的に提唱されている立法措置としては、例えば、サイバー攻撃の予防を目的として通信を監視することを、立法措置等によって容認する必要があるという指摘がある(142)。さらに、サイバー攻撃対処研究会のとりまとめで法的整理がなされたような通信の秘密を最小限の範囲で検知する行為についても、許容される具体的行為の類型を法律で規定し、許容又は義務化すべきであるとの意見がある(143)。能動的サイバー防御の導入に当たっても、一定の条件下でISP 等から自衛隊等へネットワーク上を流れる通信の外形的情報を常時提供できるよう、電気通信事業法の通信の保護規定に例外を設ける法改正が必要だとする見解がある(144)。

他方、通信の秘密を守り、利用者のプライバシーを守ってきたとするISP 等の立場からは、法改正といった措置によって、通信内容の把握のようなことにまで事業者の役割が拡大されることには懸念が示されており(145)、留意が必要であろう。

おわりに

本稿では、通信の秘密に係る議論を軸として、官民連携で取り組まれてきたサイバーセキュリティ対策を整理した。また、それに係る論点等をまとめた。

なお、本稿で整理したサイバー攻撃対処研究会等の官民連携の取組は、これまで「積極的サイバー防御」という名称の施策の下で取り組まれてきた(146)。この語と能動的サイバー防御との関係性は必ずしも明らかではないが、能動的サイバー防御の導入に当たっては、従来の積極的サイバー防御の取組やその法的解釈を踏まえた議論は避けられないであろう(147)。これらの関係性については、国家安全保障戦略に示された「能動的サイバー防御を含む…（中略）…取

---

(139) 松村昌廣「我が国のサイバーセキュリティ戦略の欠点と展望―「平和国家」体制の桎梏への対応を考える―」『情報通信政策研究』5(2), 2022.3, pp.89-90. <https://doi.org/10.24798/jicp.5.2_73>

(140) 曽我部真裕「通信の秘密の憲法解釈論」『Nextcom』16 号, 2013.Win, p.20; 石井夏生利「国家安全と通信の秘密」『Nextcom』16 号, 2013.Win, p.30 等

(141) 曽我部　同上

(142) 石井　前掲注(140), pp.30-31. この指摘は、サイバー攻撃そのものの排除は緊急避難の要件を満たすものの、特に「現在の危難」の要件を満たすことを事前に把握するためには通信監視が必要であるとの考え方に基づく。

(143) この主張を行う論者は、秘密を侵害する行為の類型を法律上に示すこと等も提案している（海野敦史「サイバーセキュリティ対策と通信の秘密」『総合政策研究』30 号, 2022.3, pp.53-55. <https://chuo-u.repo.nii.ac.jp/records/13946>）。また、異なるアプローチとしては、電気通信役務の提供に係る「利用の公平」を定める電気通信事業法第 6 条に着目した立法論もある。これは、同条が定める電気通信役務に係る公平な取扱いの対象からサイバー攻撃を行う者を除外し、そうした者への通信サービス提供を拒否することを認めることで、電気通信事業者がサイバー攻撃を止められるようにするというものである（林・田川　前掲注(108), pp.65, 75-76.）。

(144) 「サイバー防衛 高いハードル」『読売新聞』2023.3.18.

(145) 小山　前掲注(127)

(146) サイバーセキュリティ戦略本部　前掲注(75), pp.128-130. 積極的サイバー防御とは、サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じることと定義される（同, p.356.）。

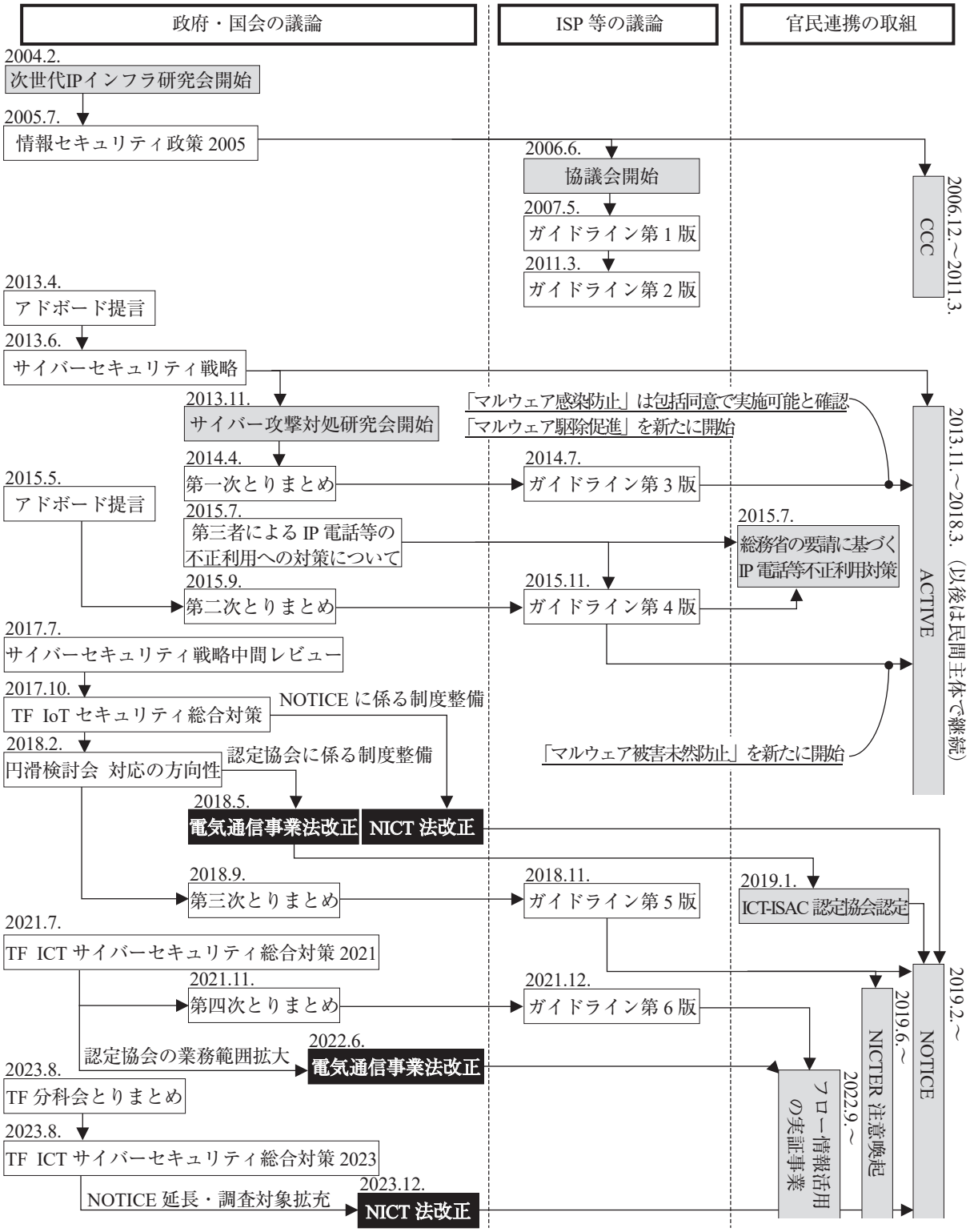
(147) CCC、ACTIVE 等における違法性阻却事由の議論も踏まえつつ、能動的サイバー防御を論じる文献としては以下がある。渥美友里「安全保障の新戦略 能動的サイバー防御」『日経コンピュータ』1104 号, 2023.9.28, p.47.

組」の類型の１つである「国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知する」こと(148)と、サイバー攻撃対処研究会第四次とりまとめで違法性が問われないと整理された事項との類似性等に注目し、能動的サイバー防御の中でもこの部分については容易に導入が進むのではないか、とする指摘もある(149)。サイバーセキュリティ対策やサイバー攻撃への対応を更に強化していくに当たり、長年にわたって積み重ねられてきた通信の秘密に関する議論がどういった方向へ展開していくのか、注目される。

（おちあい　しょう）

(148)「国家安全保障戦略」前掲注(2), pp.21-22.
(149) 郡義弘「「能動的サイバー防御」を考える、この言葉の指すところは何なのか？」2023.2.10. NEC ウェブサイト <https://jpn.nec.com/cybersecurity/blog/230210/>

別図　これまでの通信の秘密に係る議論と官民連携のサイバーセキュリティ対策の系譜



（注）本稿中で関連性を述べた文書、取組及び法改正の間に矢印を示した。図中で略した会議名は以下のとおり。
・協議会：インターネットの安定的な運用に関する協議会
・アドボード：情報セキュリティ アドバイザリーボード
・サイバー攻撃対処研究会：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
・円滑検討会：円滑なインターネット利用環境の確保に関する検討会
・TF：サイバーセキュリティタスクフォース
・分科会：情報通信ネットワークにおけるサイバーセキュリティ対策分科会
（出典）各会議資料等を基に筆者作成。