新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進

平成 29 年度サイバーセキュリティ政策会議　報告書

サイバーセキュリティ政策会議

はじめに

近年めざましい発展を遂げている情報通信ネットワーク、とりわけインターネットは、私たちの生活の利便性を向上させるにとどまらず、社会・経済活動の根幹を支える重大なシステムとして機能するに至っている。その一方で、サイバー犯罪・サイバー攻撃の多発、インターネット上の違法・有害情報の氾濫、コンピュータ・ウィルスの蔓延が社会問題となるとともに、サイバー空間の脅威に対する国民の不安感も急速に高まっており、効果的な対策を官民が連携して検討・実施する必要性が高まっている。

平成 13 年度には、官民連携したサイバー犯罪捜査及び被害防止対策によりサイバー空間の安全安心を確保することを目的に、サイバー空間の脅威への対処に関する産業界等と警察との連携の在り方について有識者等による検討を行うため、生活安全局長主催の私的懇談会である総合セキュリティ対策会議が設置された。「サイバーセキュリティ政策会議」は、サイバーセキュリティに関するより幅広いテーマを取り扱うため、平成 29 年度に、長官官房サイバーセキュリティ・情報化審議官の私的懇談会として、これを改組したものである。前身となる総合セキュリティ対策会議においては、サイバーセキュリティに関する有識者にとどまらず、電気通信事業、コンテンツ事業等の各種事業に関する知見を有する方々、さらに、法曹界、教育界、防犯団体の方々という広い分野の有識者により、幅広い意見交換が活発に行われてきた。こうした意見交換の結果は、平成 13 年度以降、毎年度、様々な内容の報告書として取りまとめられている。そして、その報告書の内容を踏まえ、これまでの間、様々な施策が取りまとめられ、実施されてきた。例えば、平成 18 年６月のインターネット・ホットラインセンターの運営開始、平成 20 年５月のファイル共有ソフトを悪用した著作権侵害対策協議会の発足、平成 21 年６月の児童ポルノ流通防止協議会の発足、平成 24 年の不正アクセス禁止法の改正、平成 26 年の一般財団法人日本サイバー犯罪対策センターの創設、平成 29 年の青少年ネット利用環境整備協議会の設立等の取組が挙げられる。

平成 29 年度のサイバーセキュリティ政策会議は、「新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進」をテーマに選定し、官民双方が抱える課題、官民が連携した対策の今後の方向性について検討を行った。

各委員には、それぞれが属する企業・組織における知見を背景としつつも、中立的な立場で、関係者が講じるべき具体的な取組等について議論を行っていただいた。本報告書は、これらの議論の結果を取りまとめたものであり、今後のサイバーセキュリティの向上及び安全安心なインターネット社会の発展の一助となれば幸いである。

平成 30 年５月

サイバーセキュリティ政策会議委員長

これまでの総合セキュリティ対策会議の議題

平成 13 年度	情報セキュリティ対策における連携の推進
平成 14 年度	情報セキュリティに関する脅威の実態把握・分析
平成 15 年度	官民における情報セキュリティ関連情報の共有の在り方
平成 16 年度	インターネットの一般利用者の保護及び知的財産権侵害に関する官民の連携の在り方
平成 17 年度	インターネット上の違法・有害情報への対応における官民の連携の在り方
平成 18 年度	インターネット・ホットラインセンターの運営の在り方及びインターネットカフェ等における匿名性その他の問題と対策
平成 19 年度	Winny 等ファイル共有ソフトを用いた著作権侵害とその対応策
平成 20 年度	インターネット上での児童ポルノの流通に関する問題とその対策
平成 21 年度	インターネット・オークションにおける盗品の流通防止対策
平成 22 年度	安全・安心で責任あるサイバー市民社会の実現に向けた対策
平成 23 年度	サイバー犯罪捜査における事後追跡可能性の確保
平成 24 年度	・官民が連携した違法・有害情報対策の更なる推進 ・サイバー犯罪捜査の課題と対策
平成 25 年度	サイバー空間の脅威に対処するための産学官連携の在り方 ～日本版 NCFTA の創設に向けて～
平成 26 年度	官民連携を通じたサイバー犯罪に対処するための人材育成
平成 27 年度	サイバー犯罪捜査及び被害防止対策における官民連携の更なる推進
平成 28 年度	コミュニティサイトに起因する児童被害防止のための官民連携の在り方

本　　編

目　　次

新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進について

ブロックチェーンやIoT等、近年サイバー空間に相次いで登場している新たな技術・サービスは、社会システムを大きく変容させ、市民生活や経済活動に大きな利益をもたらす可能性を持っている。例えば、レンタルサーバ、VPS（仮想専用サーバ）、クラウド等（以下「レンタルサーバ等」という。）を利用して手軽にウェブサイトを作成するなど、サイバー空間における新たな技術・サービスの中には、既に日常生活の一部となっているものもあり、今後もサイバー空間と現実空間の一体化が進展していくと予想される。サイバーセキュリティを確保するための方策が、そうしたサイバー空間におけるイノベーションの芽を摘むことになってはならない。

一方で、例えばレンタルサーバ等は、近年多発しているインターネットバンキングに係る不正送金事犯において、踏み台サーバとして不正アクセスに利用されるなど、新たな技術・サービスを犯罪インフラとして悪用したサイバー犯罪・サイバー攻撃の発生は我が国においても後を絶たない。

とりわけ、サイバー空間における最大の犯罪インフラとなっているボットネットについては、平成28年10月、IoT機器を標的とする不正プログラム「Mirai」に感染したボットネットによる大規模なDDoS攻撃により、アメリカの主要メディア等のウェブサイトが利用できなくなる被害が発生するなど、新たな技術・サービスの登場に伴って一層の多様化、多角化が懸念される。

更に、昨年５月には、約150か国の政府機関、病院、銀行等のコンピュータがランサムウェア「WannaCry」に感染し、一部の国では、個人の財産のみならず、生命、身体にも影響が及ぶ事態となるなど、サイバー空間の脅威は、世界的規模で深刻化していると言わざるを得ない。

東京オリンピック・パラリンピック競技大会の開催を２年後に控え、今後、世界の注目が我が国に向けられることが予想される中、こうしたサイバー空間の脅威に対して有効な策を講じていくことは、我が国にとって喫緊の課題であり、警察において部門の垣根を越えて検討を推進していくことはもとより、関係省庁と緊密に連携し、現実空間における脅威への対処を前提として構築されてきた現行の制度の在り方について、見直しの必要性を含めた議論が早急に進められるべきである。

加えて、自らが提供する技術・サービスがサイバー空間において不正に利用されている事業者は、その防止を図る社会的責任と、どのような被害防止策をとっているかについての説明責任を負っていると言える。そうした技術

・サービスを日常的に利用し、結果としてサイバー空間の脅威の一端を担うこととなっている一般利用者に対して、どのように注意喚起、広報啓発を行っていくべきかについても含め、官民がより一層連携を推進し、それぞれに負うべき責任が適切に果たされる仕組みを検討、構築していく必要がある。

そこで、平成 29 年度サイバーセキュリティ政策会議では、「新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進」をテーマとして議論を行った。本報告書は、新たな傾向のサイバー犯罪等に係る官民双方の現状と課題を整理し、今後の方向性について、本会議における議論の結果を取りまとめたものである。

第１章　レンタルサーバ等を利用した犯罪の現状と対策

１．現状

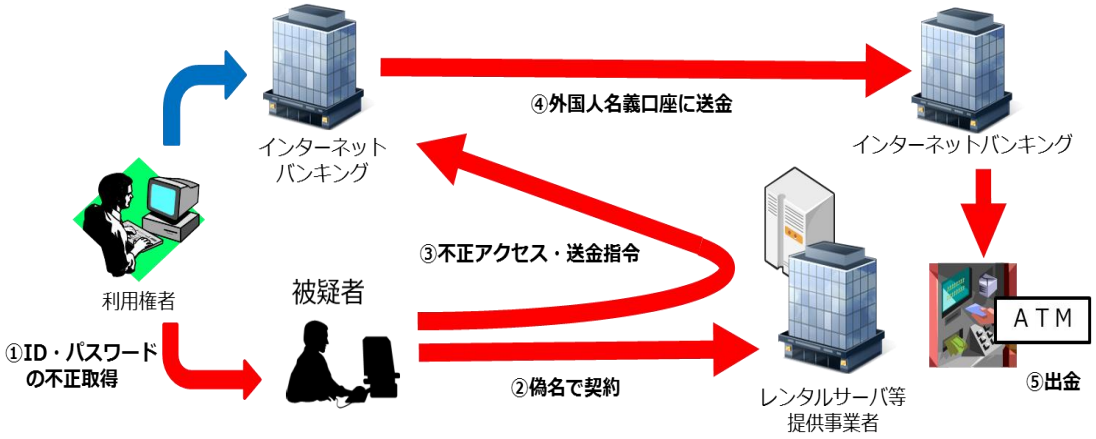
(1)　レンタルサーバ等を利用した犯罪の発生状況

インターネットが市民生活や経済活動に不可欠な社会基盤として定着する中、個人や企業が安価かつ容易にウェブサイトの作成等を行うことができるレンタルサーバ等の利用者が急速に増加している。他方で、インターネット上で簡単に利用契約ができる利便性と、契約に当たっての本人確認が十分でないことに起因する匿名性は、犯罪者にとっても利用価値が高く、レンタルサーバ等が様々なサイバー犯罪・サイバー攻撃に悪用されている状況がある。

平成 28 年頃には、インターネットバンキング利用者の ID・パスワードを不正に取得した被疑者が、虚偽の氏名、住所、電話番号等（以下「偽名等」という。）を用いて契約したレンタルサーバ等を踏み台として、インターネットバンキングに不正アクセスし、不正送金を行う事犯が多発した。同年１月から３月までの間に発生したインターネットバンキングに係る不正送金事犯のうち、不正アクセス元が判明した 747 件についてその IP アドレスを分析したところ、約 47%に当たる 348 件がレンタルサーバ等提供事業者のものであった。警察にとっては、不正アクセス元が偽名等により契約されたレンタルサーバ等であることにより、捜査における事後追跡可能性が低下するという問題が生じている。

また、偽名等により多数のレンタルサーバ等の利用契約をした者が、当該サーバの利用に係る ID・パスワードをインターネット上で大量に販売している状況が見られる。こうして作り出された正規の利用者が明らかでない大量のレンタルサーバ等は、不正に入手したクレジットカード情報等を保管するデータベースサーバとされているほか、標的型メールを送信するメールサーバ、不正プログラムを仕込んだ偽サイト作成用サーバ、不正プログラムに感染したコンピュータに対して攻撃者の指令を送信する C&C サーバ等として、サイバー攻撃に利用されていることが確認されている。

図１　レンタルサーバ等を踏み台としたインターネットバンキングに係る不正送金事犯の手口



(2)　レンタルサーバ等提供事業者による対策

レンタルサーバ等提供事業者の中には、不正利用を未然に防止するため、本人確認の強化に取り組んでいるところもある。例えば、さくらインターネット株式会社では、契約時に登録された電話番号の有効性を確認するため SMS 認証等を実施しているほか、登録された住所の有効性を必要に応じて確認する取組も行っている。GMO インターネット株式会社においても、同様に電話番号の有効性を確認する取組を行っている。ただし、現時点では、いずれもサービスの態様に応じた一部のサービスへの導入に止まっている。

また、各事業者によって対応の詳細は異なるが、不正利用に係る通報窓口を設置して、一般の利用者からの相談、一般社団法人 JPCERT コーディネーションセンター等のセキュリティインシデントに対応する機関からの情報提供、警察からの捜査関係事項照会（以下「照会」という。）等に応じているほか、約款で不正利用を禁止し、提供するサービスに係るシステムの運用・保守を行う中で不正利用が確認されれば、利用契約の解除等を行う場合もある。

警察では、レンタルサーバ等が不正に利用されていることを把握した場合、レンタルサーバ等提供事業者に対して契約解除等を要請しており、事業者がそれに応じた事例がある。例えば、平成 28 年６月、大阪府警察において、インターネットバンキングに係る不正送金事犯に利用された VPS に係る捜査を行い、当該サーバの契約に使われたクレジットカード情報が、同一の事業者における 25 名義 404 件の契約にも使われていることを割り出し、25 名義のいずれについても実在が確認できず、かつ、404 件のうちの一部が不正アクセス元サーバとして利用されていたことを理由として、同事業者に対して契約解除等を要請し、同事業者により全ての契約が解除された。

２．課題

レンタルサーバ等は、インターネット上で安価かつ容易に利用できることを特長とするサービスであることなどから、安全性より利便性が重視され、レンタルサーバ等提供事業者において不正利用対策を疎かにする事例が散見される。一部の先進的な事業者においては、不正利用対策の必要性が理解され、自主的な取組が進められつつあるが、契約時の本人確認について見ても、その実施方法について法的規制がなく各事業者の判断に委ねられていることもあり、運転免許証等の公的証明書の提示を求めていないなど、既に十分な本人確認がなされているとは言い難い。また、レンタルサーバ等は、最近 10 年余りの間に急速に普及してきた新しいサービスであることなどから、各事業者によって不正利用対策への取組状況が大きく異なっており、業界全体としてどのように対策を推進していくかが課題である。

また、レンタルサーバ等提供事業者が提供する多種多様なサービスのうち、特に VPS 等の利用者に広範なサーバ管理権を付与するサービスの場合、通信の秘密との関係から、事業者がサーバの利用状況を詳細に確認することは難しい。したがって、約款において不正利用を禁止していても、大量通信を発生させているなど外形的に明らかな異常を除けば、事業者が不正利用の事実を把握できず、契約解除等につなげることができない場合が多いと考えられる。とりわけ、利用者がサービスの対価を正規に支払っている場合には、事業者において不正利用の事実が見過ごされるおそれが高いことから、レンタルサーバ等提供事業者が不正利用の事実を的確に把握するための方策について、技術面・制度面の両方から検討が進められる必要がある。

３．今後の方向性

(1)　レンタルサーバ等提供事業者における本人確認の強化

これまでに発生しているレンタルサーバ等を利用した犯罪の多くは、レンタルサーバ等提供事業者において利用者の本人確認を強化し、悪意を持つ者による利用契約を排除することで、未然に防止できると考えられる。レンタルサーバ等提供事業者は、現在行っている本人確認の取組の実効性を検証するとともに、他の業界において実施されている本人確認方法を参考に、更なる措置の導入を検討していくべきである。その際、他人・架空名義のクレジットカード情報が使われたり、同一のクレジットカード情報により多数の契約が行われたりといったことを防ぐため、クレジットカード会社との連携を図っていくことが望ましい。

(2)　不正利用対策推進のための連携体制の確立

自らが提供するレンタルサーバ等が犯罪に利用されているレンタルサーバ等提供事業者は、その防止を図る社会的責任を果たすべきである。

不正利用対策の実施が各事業者に委ねられ、事業者間の連携も十分とは言えない現状に鑑みれば、まずは、先進的に不正利用対策に取り組んでいるレンタルサーバ等提供事業者が中心となり、対策が十分に行われていない事業者を含めた情報共有の場を設けるなどして、不正利用対策に係る意識の醸成、取組の推進を図るための体制を確立する必要がある。具体的には、不正利用を未然に防止するための本人確認の強化方策はもとより、ブラックリスト等の活用、脆弱性のあるソフトウェアへの対応等、不正利用を把握するために効果があると認められる方策を講じるためのノウハウ、成功事例について、事業者間で積極的に共有を進めていくとともに、事業者における不正利用対策に係る情報を発信し、利用者に対する注意喚起、広報啓発も行っていくべきである。

警察としても、レンタルサーバ等提供事業者との連携を進め、今後も変遷していくことが予想されるレンタルサーバ等を利用した犯罪の手口等について情報提供するとともに、特に犯罪利用が見られる事業者に対して、どのような対策を行っているかについて説明を求めたり、不正利用を認識した場合の警察への通報を求めたりすることを通じて、事業者の不正利用防止に向けた取組の強化を促していくべきである。また、不正利用に対応する事業者の業務負担を軽減するため、捜査関係事項照会書の郵送により紙ベースで行われている警察からの照会について、電子メールの活用を含めたオンライン化に向けて、引き続き検討を進めていくことも必要である。更には、総務省、経済産業省等の関係省庁とも連携し、事業者が行うべき対策について助言を行うなどして、レンタルサーバ等提供事業者における本人確認等の未然防止対策、契約解除等の事後対策の両方を促進し、レンタルサーバ等が犯罪者にとって利用しにくいサービスになるよう、継続的に働き掛けていくことが望ましい。

第２章　ボットネットの現状と対策

１．現状

(1)　海外におけるボットネットのテイクダウン作戦

不正プログラムに感染したコンピュータ（以下「感染端末」という。）と多数の感染端末に指令を送信する C&C サーバから成るボットネットは、インターネットバンキングに係る不正送金、DDoS 攻撃、情報窃取及びスパムメールの送信等、世界的規模で様々なサイバー犯罪・サイバー攻撃に利用され、サイバー空間における最大の犯罪インフラとなっている。

ボットネットに対しては、平成 22 年頃から、アメリカの FBI 及びマイクロソフトコーポレーションが主導し、国際的なテイクダウン作戦が実施されてきた。ボットネットのテイクダウン作戦は、一般的に、C&C サーバの解析や C&C サーバと感染端末間の通信状況の把握等によるシステム及びネットワークの全容解明を核として、C&C サーバを利用して犯罪を行う被疑者の検挙、感染端末の利用者への注意喚起等による被害の拡大防止の３つから構成されており、C&C サーバと多数の感染端末との間の通信状況を把握し、また、感染端末が C&C サーバからの指令を受け取らないようにするため、作戦の一環として、感染端末等から C&C サーバへの通信を安全が確保された代替サーバに合法的に向けさせる（以下「シンクホール」という。）手法が採られている。

例えば、平成 26 年５月に実施された、インターネットバンキングに係る不正送金事犯に使用される「Game Over Zeus」という不正プログラムに感染した端末から成るボットネットのテイクダウン作戦においては、FBI が、詐欺の差止等を求める民事訴訟を提起し、C&C サーバに割り当てられたドメインを管理するレジストリに対する連邦裁判所の命令を得て、当該ドメインを FBI が管理する代替サーバに割り当てさせることにより、「Game Over Zeus」の感染端末が C&C サーバに自動的に指令を取りに行く通信の状況を把握するとともに、当該感染端末の IP アドレスを収集した。また、マイクロソフトコーポレーションが、同社製の Windows を搭載した感染端末に係る商標権侵害の差止を求める民事訴訟を提起し、同様にレジストリに対する連邦裁判所の命令を得て、シンクホールを行った例も見られる。

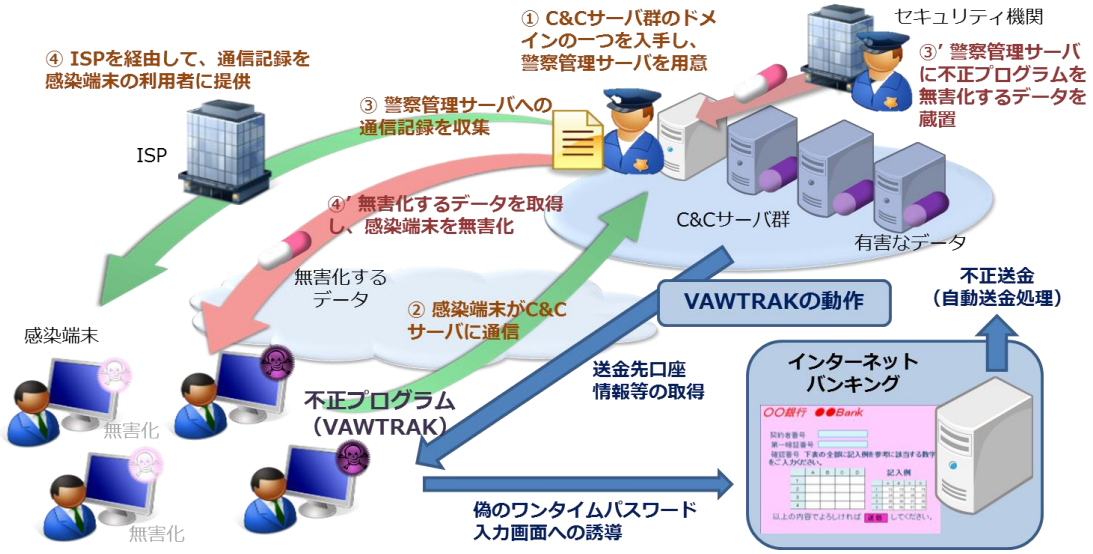
最近では、平成 28 年 11 月、ドイツ警察を中心に、オペレーション・アバランチという大規模なテイクダウン作戦が実施された。同作戦の実施に当たってもシンクホールが行われており、警察庁では、シンクホールによって収集された感染端末の IP アドレスのうち我が国に関係するものの提供を受け、インターネット接続サービスを提供する電気通信事業者（ISP）に提供して、感染端末の利用者に対する注意喚起を行ってもらった。また、ドイツ警察等が押収したサーバに蔵置されていたインターネットバンキング利用者の ID・パスワード、クレジットカード情報等

のうち、我が国に関係する約 27 万件の提供を受け、金融機関、クレジットカード会社等に提供し、不正利用防止のための対策を講じてもらった。

(2)　我が国における取組

平成 27 年４月、警視庁は、インターネットバンキングに係る不正送金事犯に使用される「VAWTRAK」という不正プログラムの感染端末に係る通信状況を把握することにより、国内約４万 4,000 台、国外約３万 8,000 台の感染端末情報を収集した。具体的な手法は、感染端末の解析により判明した、C&C サーバに割り当てられていたドメインの１つが失効していたため、警視庁で当該ドメインを取得し、自ら設置したサーバに割り当てることにより、感染端末から当該サーバへの通信状況を観測したというものである。また、感染端末が C&C サーバに定期的に指令を取りに行く通信を行うことを逆手に取り、警視庁では、この指令に係るデータに代わって、白紙のデータをサーバに蔵置し、感染端末中の不正プログラムを無害化した。

図２　警視庁が実施した「VAWTRAK」の感染端末対策



２．課題

ボットネットをテイクダウンするためには、C&C サーバの解析や C&C サーバと感染端末間の通信状況の把握等によるシステム及びネットワークの全容解明が欠かせない。C&C サーバが国内にある場合は、我が国警察の捜査権が当該サーバに及ぶことから、刑事訴訟法（昭和 23 年法律第 131 号）に基づく差押えの手続により、裁判所の令状を得て、当該サーバを押収して解析を行うことが可能である。また、C&C サーバと感染端末との間の通信状況については、シンクホールによらずとも、同法に基づく検証の手続により、当該サーバの管理者に裁判所の令状を提示した上で観測することがで

きるのではないかと考えられる。加えて、レンタルサーバ等提供事業者が当該サーバの管理権を持っている場合等には、こうした刑事手続を行わなくとも、警察による捜査に対して、サーバ管理者の任意の協力が得られることも想定される。しかしながら、それぞれの手続について、許容される措置の範囲やボットネットのテイクダウンのために得られる効果が十分に整理されているとは言えない。

一方、C&C サーバが海外にある場合は、当該サーバに対して我が国の刑事手続を適用できないことから、我が国の警察は、当該サーバの所在国に対して捜査共助を要請することが原則となるであろうが、我が国で登録された JP ドメインが当該サーバに割り当てられている場合には、当該サーバと感染端末間の通信状況を把握するため、JP ドメインを管理するレジストリである株式会社日本レジストリサービス（JPRS）による対応を求め、シンクホールを行うことが考えられる。これまでのところ、JP ドメインがボットネットの C&C サーバに使用される例があまり見られないことから、JPRS に措置を求める必要が生じていないが、諸外国でドメインの不正利用防止対策が講じられるにつれ、また、東京オリンピック・パラリンピック競技大会の開催に向けて世界の注目が我が国に集まるにつれ、犯罪者が JP ドメインの使用を企むことも想定される中、我が国においてシンクホールを実施する根拠が明らかになっていないことが課題である。

なお、「VAWTRAK」の感染端末対策において警視庁が用いた手法は、既に失効していたドメインを取得することができたものであり、常に利用可能な手法というわけではないと思われる。

３．今後の方向性

(1)　シンクホールの実施に向けた検討の推進

サイバー空間における最大の犯罪インフラとなっているボットネットに対して、我が国の警察として、より主体的、積極的に策を講じていくためには、ボットネットをテイクダウンするための我が国における手法を確立していく必要がある。特にシンクホールは、C&C サーバと多数の感染端末との間の通信状況を把握し、ボットネットの全容解明を行うために必要不可欠な手法であると言え、警察庁と総務省、法務省等の関係省庁及び日本レジストリサービス等の関係事業者との連携を進め、我が国における実施が可能となるよう制度の検討を推進していくべきである。

この点、アメリカでは、FBI 又はマイクロソフトコーポレーションを一方当事者とする民事手続として、ドイツでは、詳細は明らかになっていないが刑事手続の一環としてシンクホールを行ったようであり、我が国でシンクホールを行う手続を検討するに当たってもそれらの手続が参考になるが、それらの国と我が国では法体系が異なることから、それらの手続を直ちに我が国に導入することができるわけではない。

また、平成 28 年 10 月には、IoT 機器を標的とする不正プログラム

「Mirai」に感染したボットネットによる大規模な DDoS 攻撃が発生したが、多種多様な IoT 機器を感染端末とするボットネットに対しては、専ら Windows を搭載したパソコンを感染端末とするボットネットを構築した身元不明の相手方に対してマイクロソフトコーポレーションが商標権侵害の差止めを請求したように、１つの民間企業に対応を委ねることは難しいと思われる。

そこで、我が国の警察が主導してシンクホールを行うことを可能にするためには、JP ドメインを管理する JPRS に対して、誰が何を根拠にどのような措置を求め得るのかについて整理する必要があり、検証等の刑事手続又は JPRS を相手方とする民事手続によることの可能性、JPRS の任意の協力によることの妥当性等について、現行制度の見直しの必要性を含めて幅広く議論を行い、我が国の法体系に則った手続を新たに確立していかなければならない。

(2) ボットネット対策のための官民連携の推進

ボットネットの全容を解明しテイクダウンするための手法は、シンクホールに限られるものではなく、C&C サーバが国内にある場合における当該サーバの差押え、当該サーバと感染端末との間の通信状況の検証といった刑事手続により、どこまでの措置を行うことができ、どういった効果が得られるか、また、当該サーバの管理者の任意の協力により同様の措置を行うことができるかについても、サーバの管理権の侵害や犯罪行為の黙認等の問題にも留意しつつ、関係省庁及び関係事業者の協力を得て、併せて整理していく必要がある。

その際、シンクホールを含め、通信当事者のいずれの同意も得ることなく行う手法は、通信の秘密の侵害等に当たるおそれがあるほか、正当な通信の遮断等にもつながるおそれがあることから、特に JPRS やサーバ管理者等に任意の協力を求める場合には、これらの点にも十分に留意しなければならない。

また、ボットネットによる被害拡大防止の観点から ISP が主体的に行い得る手法として、例えば、ISP が感染端末を検知した場合に、当該端末のインターネット接続を遮断することで感染拡大を防止する Walled Garden と呼ばれるものが考えられる。この点、どのような場合に通信の遮断が許容されるかについては、「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」において一定の整理がなされていることに加え、総務省において開催している「円滑なインターネット利用環境の確保に関する検討会」において継続して検討されているところであり、警察庁としても、ボットネットのテイクダウンに資する措置が可能となるよう、総務省における取組を注視していくことが望ましい。

ボットネット対策に携わる者は、ボットネットを利用する犯罪者の検

挙を目指すべき警察だけではなく、総務省を始めとする関係省庁、レジストリ、サーバ管理者、ISP 等の関係事業者、更には感染端末の利用者に至るまで極めて多岐にわたり、かつ、世界的規模で犯罪インフラのネットワークが構成されることから、国際的な連携が不可欠である。ボットネットをテイクダウンするためには、それぞれの関係者が果たす役割、責任を明らかにしていくとともに、強制的な感染除去（Remote Disinfection）等の更なる手法を行う可能性を含め、様々な対策を検討していくことが重要である。

おわりに

本会議では、レンタルサーバ等を利用した犯罪対策及びボットネット対策のほか、仮想通貨を利用した犯罪対策についても議論を行ったが、本会議の最中である本年１月、我が国の大手の仮想通貨交換業者が管理するサーバから、時価約 580 億円相当に上る仮想通貨が不正に送信されたと見られる事案が発生し、社会に大きな衝撃を与えたところ、当該事案についてまさに警察が捜査中であり未だ詳細が明らかになっていない現時点で、課題を整理し今後の方向性を取りまとめるのは困難と判断した。

サイバー空間をめぐる情勢の変化はめまぐるしく、新たな技術・サービスが次々に登場するとともに、サイバー犯罪・サイバー攻撃の傾向も次々に変遷している。警察としては、こうした情勢の変化に柔軟かつ迅速に対応していくとともに、サイバー空間において暗躍する犯罪者を検挙すべく、現行の制度や捜査手法について、関係省庁とも連携して不断に見直しを検討していく必要がある。加えて、新たな傾向のサイバー犯罪等に的確に対処していくためには、犯罪に利用されている技術・サービスを提供する民間事業者による取組が不可欠である。サイバー空間の脅威に対峙し、我が国のサイバーセキュリティを確保していくため、官民双方の多岐にわたる関係者が、それぞれ主体的に対策を強化していくとともに、より一層連携を推進していくことが求められている。

平成29年度サイバーセキュリティ政策会議委員名簿

前田　雅英 （委員長）	日本大学大学院　法務研究科　教授
岩井　博樹	デロイト トーマツ リスクサービス（株）　シニアマネジャー
岩下　直行	京都大学公共政策大学院　教授
片山　建	日本マイクロソフト（株）　政策渉外・法務本部 サイバーセキュリティ政策担当部長
桑子　博行	違法情報等対応連絡会　主査
小山　覚	ＮＴＴコミュニケーションズ（株）　情報セキュリティ部　部長
坂　明	（一財）日本サイバー犯罪対策センター　理事
寺田　真敏	（株）日立製作所　Hitachi Incident Response Team チーフコーディネーションデザイナ　チーフテクノロジデザイナ
中野目　善則	中央大学　法学部　教授
西本　逸郎	（株）ラック　代表取締役社長
則房　雅也	日本電気（株）　サイバーセキュリティ戦略本部　主席技術主幹
藤川　春久	セコムトラストシステムズ（株）　取締役　常務執行役員
藤原　靜雄	中央大学大学院　法務研究科　教授
別所　直哉	ヤフー（株）　シニアアドバイザー
星　周一郎	首都大学東京　法学部　教授
水越　一郎	（一社）ＪＰＣＥＲＴコーディネーションセンター　理事
谷島　隆彦	（一社）ＩＣＴ－ＩＳＡＣ　事務局長
山下　眞一郎	富士通（株）　サイバーセキュリティ事業戦略本部 ＧＭＳＳ開発統括部　サービスデリバリ部　部長

計　１８人（敬称略・５０音順）

【オブザーバー】内閣官房（ＮＩＳＣ）、金融庁、総務省、法務省、経済産業省

平成 29 年度サイバーセキュリティ政策会議の開催状況

第１回会議　　平成 29 年 10 月 27 日(金)

第２回会議　　平成 29 年 12 月 22 日(金)

第３回会議　　平成 30 年２月 20 日(火)

第４回会議　　平成 30 年３月 15 日(木)