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 27 年度総合セキュリティ対策会議　報告書

総合セキュリティ対策会議

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、サイバー犯罪の増加、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。

「総合セキュリティ対策会議」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、平成 13 年度に設置された生活安全局長主催の私的懇談会である。当会議においては、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、コンピュータ製造・販売業、ソフトウェア産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おり、平成 13 年度以降、毎年度、様々な内容の報告書を取りまとめてきた。そして、こうした意見交換の結果は、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等の取組に結び付いている。

平成 27 年度は、「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」をテーマに選定し、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について、官民双方におけるサイバー犯罪捜査及び被害防止対策をめぐる現状と課題を改めて整理・共有すること及び海外におけるサイバー犯罪捜査及び被害防止対策の手法を検証することにより、一層効果的・効率的な方策を検討した。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 28 年４月

総合セキュリティ対策会議委員長

前田雅英

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等

本　　編

目　　次

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について

インターネットが市民生活や社会経済活動に不可欠な社会基盤として定着し、サイバー空間が日常生活の一部となっている。こうした中、平成27年中のサイバー犯罪の検挙件数は8,096件であり、高水準で推移しているほか、警察に対するサイバー犯罪等に関する相談件数は128,097件であり、前年と比べ9,997件増加するなど、サイバー空間における脅威は深刻なものとなっている。

特に、高度な情報技術を用いたサイバー犯罪であるインターネットバンキングに係る不正送金事犯（以下「不正送金事犯」という。）については、平成27年中の発生件数が1,495件に減少したものの、被害額が30億円を超えて、過去最悪の被害額になった。

こうした現下の厳しいサイバー犯罪情勢に対処するため、警察においては、民間事業者等と連携し、徹底した捜査を推進するとともに、積極的な被害防止対策（被害の拡大を防止する対策を含む。以下同じ。）を講じているところである。

特に、官民の連携については、平成25年度総合セキュリティ対策会議における議論の結果等を受けて設立された一般財団法人日本サイバー犯罪対策センター（以下「JC3」という。）が、平成26年11月、業務を開始している。JC3の目的は、産学官それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、脅威を特定、軽減及び無効化するための活動に貢献することであり、平成27年11月には、JC3の協力を得て、18都道府県警察が海外サーバ利用の違法アダルトアフィリエイトサイト一斉集中取締りを実施するなど、成果がみられ始めている。

しかしながら、サイバー犯罪が増加・複雑化する中、様々な隘路が警察の捜査を困難なものとしている。また、警察の捜査が様々な課題に直面する中、民間事業者における捜査への協力に要する人員・コストも増大しているのが実情である。さらに、犯人の追跡とともに、捜査と並ぶ対策の両輪として、被害防止対策がより重要なものとなっている。

日進月歩で進化する高度なサイバー犯罪が次々と発生する中、サイバー犯罪捜査及び被害防止対策について、官民双方の現状と課題を改めて整理・共有し、また、海外における手法を検証することにより、一層効果的・効率的な方策を検討することは、現在だけでなく将来にわたって効果的な諸対策を講じていく上で、必要不可欠であるといえる。

そこで、平成27年度総合セキュリティ対策会議では、「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」をテーマとして選定して、議論を行った。本報告書は、サイバー犯罪対策におけ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、議論の結果を取りまとめたものである。

第１章　サイバー犯罪対策における警察側の現状と課題

１．現状

(1)　捜査の現状

ア　地理的無制限性に関する現状

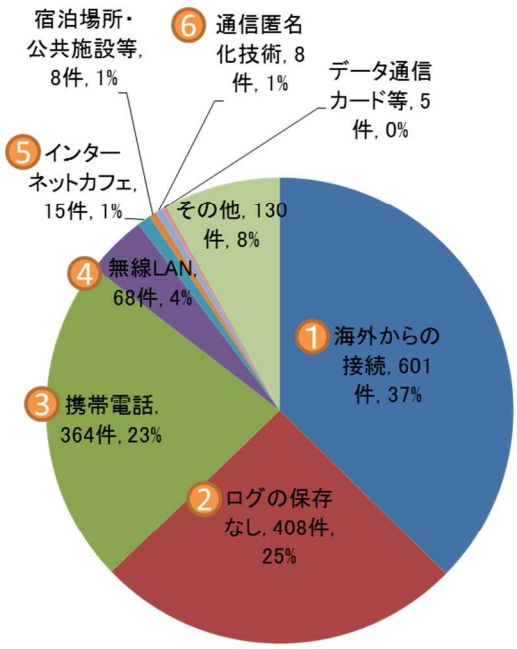
サイバー犯罪捜査においては、地理的無制限性というインターネットの特性上、発信地等が直ちに特定できない上、発信地の特定等に必要な情報を保有するプロバイダ等が東京都内に集中していることから、各道府県警察が頻繁に東京都内に出張してプロバイダ等に対する差押えを行う必要があるなど、捜査活動の負担が大きなものとなっている。

例えば、不正送金事犯の捜査においては、①金融機関からの被害申告を受理する都道府県警察（多くは警視庁）、②不正送金元口座名義人の居住地を管轄する都道府県警察、③不正送金先口座名義人の居住地を管轄する都道府県警察、及び④現金引出場所を管轄する都道府県警察というように、４以上の都道府県警察が捜査に関係することが多いため、関係都道府県警察間における連携がなければ、事案の全容解明は不可能となっている。

また、そもそも指令サーバが海外に所在しているなど、容易に国境を越えるサイバー犯罪の捜査においては、外国捜査機関の協力が不可欠であることも多い。

なお、サイバー犯罪捜査における事後追跡上の障害について、平成26 年 10 月、警察庁により実態調査が実施されている。これは、平成25 年中に認知したサイバー犯罪（刑法犯及び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）違反に限る。）のうち、インターネット上における事後追跡に係る障害により未検挙であると判明した 1,607 件について、その障害の内容を調査したものであり、このうち、海外からの接続が障害となったものは 601 件（37%）であり、最多であった。

図１　サイバー犯罪捜査における事後追跡上の障害に関する実態調査の結果
（平成 26 年 10 月、警察庁）



1 海外からの接続
- 被疑者が被害者に攻撃を行う過程で、海外からのインターネット接続が行われていた場合、海外に所在するヒト・モノに対し直接的に捜査権を行使できず、国際捜査共助を要請する必要がある。

2 通信履歴等(ログ)の保存なし
- サイバー空間における通信の痕跡であるログが被害サーバ、プロバイダ、中継サーバ等において保存されていないことにより、被疑者の事後追跡が困難となる。

3 携帯電話
- 不正に入手等された携帯電話がツールとして悪用されることにより、被疑者の事後追跡が困難となる。

4 無線ＬＡＮ
- 悪意ある者が、セキュリティ設定が簡易で無防備なアクセスポイントに不正に接続して犯行を行うと、当該アクセスポイントの利用者が複数存在することとなり、被疑者の特定が困難となる。

5 インターネットカフェ
- 利用者の本人確認が実施されていない、又は入退店時刻やコンピュータの使用状況が記録されていないことにより、当該利用者の特定が困難となる。

6 通信匿名化技術
- Torを始めとする高度匿名化技術が悪用されることにより、発信元コンピュータの特定が困難となる。

イ　匿名性等に関する現状

前述の実態調査の結果においても示されているとおり、サイバー犯罪捜査には、地理的無制限性のほかにも多くの隘路が存在している。例えば、不正アクセスに使用された IP アドレスが割り当てられた契約者の情報に関してプロバイダへの捜査関係事項照会（以下「照会」という。）・差押えを実施した後、この情報を基にして回線設置場所や契約者の情報に関する回線提供事業者への照会・差押えを実施するなど、サイバー犯罪捜査においては多段階の照会・差押えを要するが、この過程で、ログの保存期間が超過する場合がみられる。

また、悪質な中継サーバの利用、不正な入手等による携帯電話の悪用、無線 LAN のただ乗り、Tor 等の高度匿名化技術の悪用等により、犯罪が匿名化されていることも、追跡が行き詰まる要因となる場合がみられる。

(2) 被害防止対策の現状

警察においては、被疑者を検挙した場合においても、また、前述のとおりの捜査の隘路により被疑者の特定が困難である場合においても、不正プログラムに感染していることが把握された国内の端末の利用者（以下「感染端末利用者」という。）に対して、民間事業者等を通じて、不正プログラムの駆除を促すなどの被害防止対策を講じている。

こうした対策は、①感染端末利用者が対策を講じることにより、被害が未然に防止されたり被害の拡大が防止されたりする意義があるだけでなく、②被疑者に対して、仮に同人の検挙に至らない場合であっても、警察等が対策を講じていると認識させる意義、及び③セキュリティの重要性に加え、検挙に至らない事案であっても警察等が適切な対策を講じていることについて、広く一般に理解を得る意義を有するものであり、サイバー犯罪の増加・複雑化に伴い、その必要性が増大している。

２．課題

(1) 体制整備による効率的・効果的な捜査の推進

サイバー犯罪の地理的無制限性に関し、警察においては、平成 23 年から順次、警視庁に各道府県警察から捜査員を派遣する全国協働捜査方式等を採用している。当該捜査員は、各道府県警察からの捜査共助の依頼を受け、東京都の区域内に所在するプロバイダ等に対する差押え・検証等に従事しており、これにより捜査を一定程度効率的に行うことが可能となっている。

しかしながら、不正送金事犯の発生状況・捜査状況に関する多くの情報が、全国の都道府県警察から警察庁に報告されているにもかかわらず、これらの情報が十分な体制の下で一元的に分析され、捜査や被害防止対策に効果的に活用されてきたとは言いがたい。

また、警視庁の全国協働捜査方式等において、捜査員は、捜査の過程の一部に携わっているにすぎず、基本的には各道府県警察の捜査員が大部分の捜査を行っているため、効率化には限界がある。

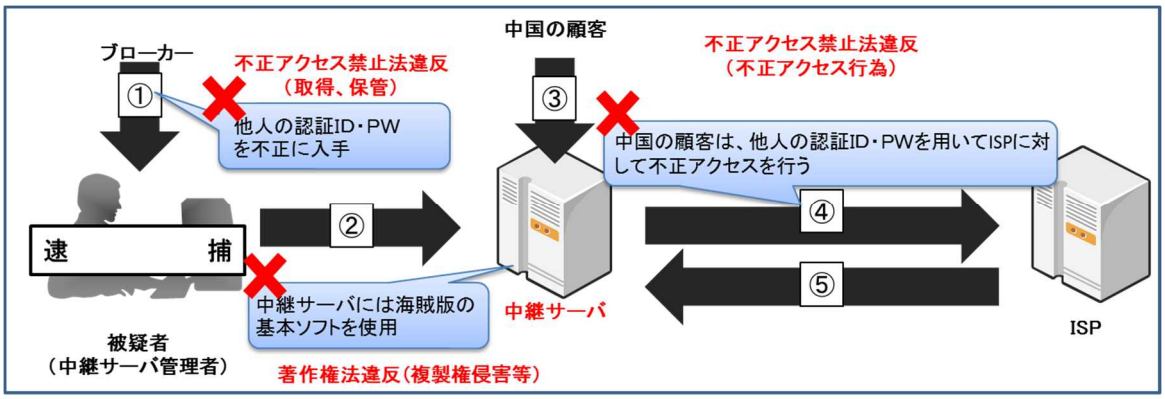
この点、欧米各国においては、我が国とはそもそも捜査体制が異なっており、国の警察機関が直接的にサイバー犯罪捜査、特に国境を越える犯罪の捜査や国際共同捜査への参画を担うことが多い。例えば EUROPOL においては、共同捜査本部を設置して国際共同捜査を行う際、EU 加盟国以外の国とも必要に応じて捜査情報・証拠の共有に関する申合せを締結することができ、その対象は原則として国の警察機関とされている。

国の警察機関である警察庁が直接的には捜査権限を有しない我が国において、効率的・効果的にサイバー犯罪捜査を推進するため、いかに体制を整備していくべきかが課題である。

(2)　捜査の隘路の打破

サイバー犯罪捜査には匿名性等に伴う様々な隘路が存在するものの、警察では、捜査に工夫を凝らし、例えば、悪質な中継サーバ事業者等の一斉取締り、無線 LAN のただ乗り行為を利用したインターネットバンキング不正送金事犯に係る電波法違反及び電子計算機使用詐欺等事件の検挙のように、積極的な事件検挙を行っている。

図２　悪質な中継サーバ事業者等の一斉取締り



また、ログの保存については、平成 27 年６月、総務省により、「電気通信事業における個人情報保護に関するガイドライン」の解説が改正され、接続認証ログの保存が許容される期間が具体的に例示されたことを踏まえ、警察庁では、同省と連携し、関係事業者における適切な取組がなされるよう必要な対応を行っている。

しかしながら、諸外国においては、我が国とは異なり、プロバイダ等に対するオンラインによる照会・差押えが可能となっている国があり、捜査が効率的に推進されているとともに、サイバー犯罪捜査において、通信傍受や仮装身分捜査を始めとする多様な手法が活用されている。加えて、大量のデータが国境を越えて保存されている中、捜査における迅速なデータ取得のための枠組みについて検討がなされる必要があると考えられる。

こうした状況を踏まえれば、我が国において、捜査の隘路を打破する制度が必ずしも十分に整っているとはいえないため、捜査手法等の深化が課題である。

(3)　戦略的・継続的な被害防止対策の推進

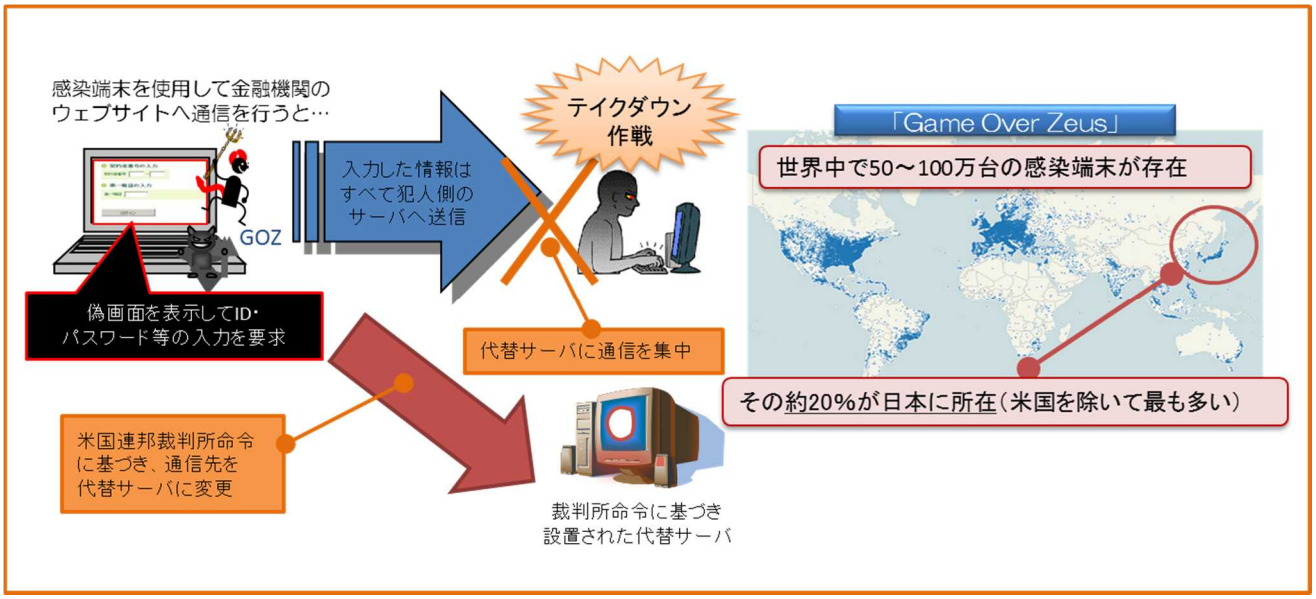
次に掲げる措置のほか、警視庁が海外の法執行機関に対して協力を要請した結果、不正送金事犯に係る不正プログラムの通信先の C&C サーバ（不正プログラムに感染したコンピュータに指令を送り、制御の中心となるサーバ）が停止された事案等、警察では、様々な被害防止対策を講じている。

①　国際的なボットネットのテイクダウン作戦（平成 26 年５月）

不正送金事犯に使用されているとみられる不正プログラム「Game Over Zeus」が世界的にまん延したことから、FBI 及び EUROPOL を中心に、我が国を含む協力国の法執行機関が連携して同プログラムに感染した端末の情報を収集し、当該端末を特定した上で、プロバイダ等を通じて当該端末の利用者に対して不正プログラムの駆除を促し、ネットワークを崩壊させる「国際的なボットネットのテイクダウン作戦」を決行した。

我が国においては、確認された約 15 万 5,000 件の感染端末の利用者に注意喚起を実施した。

図３　国際的なボットネットのテイクダウン作戦



②　悪質な中継サーバの利用による不正アクセス事案等の未然防止対策等（平成 27 年４月及び 12 月）

警視庁は、悪質な中継サーバ事業者の一斉取締りの結果、中継サーバに蔵置されたインターネットサイトの ID・パスワード等を把握したことから、当該サイトの運営会社へ ID・パスワード等、約 315 万件を提供し、不正アクセス事案等の未然防止を要請した。

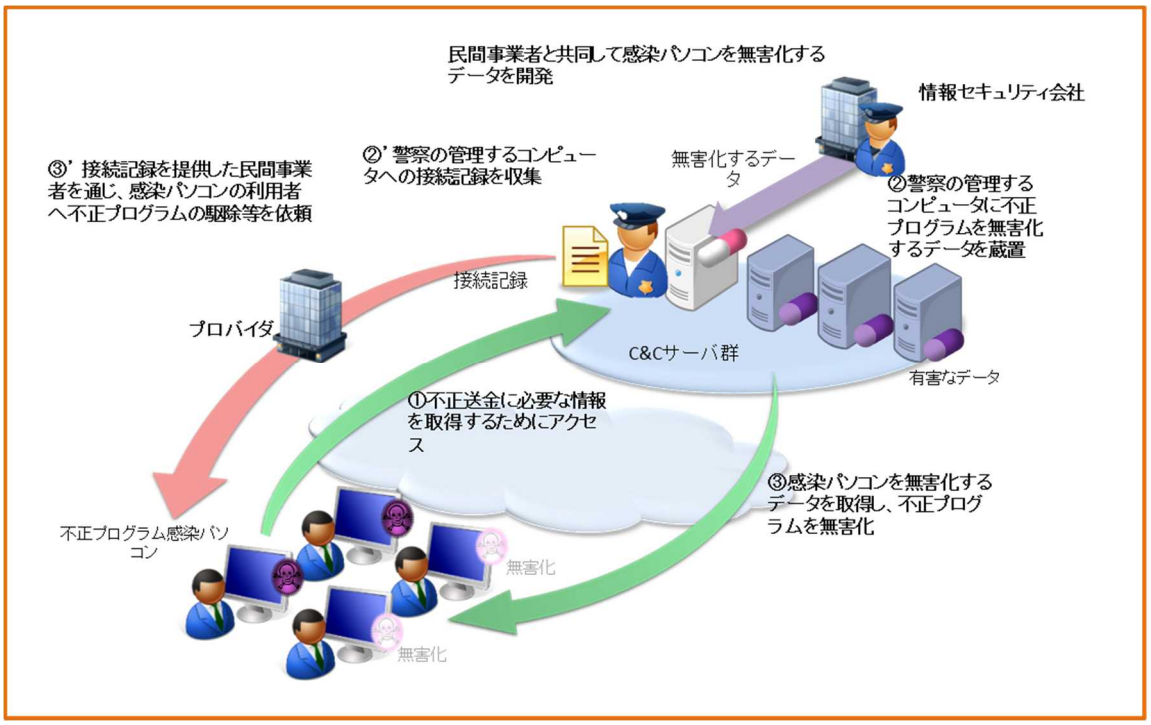
また、被害拡大防止の観点から、中継サーバ事業者に回線を提供する電気通信事業者に対し、契約の強制解約を要請した結果、当該電気通信事業者が契約約款を改正し、契約解除に応じることとなった。

③　不正送金事犯に係る不正プログラムによる被害の拡大防止措置（平成 27 年４月）

警視庁は、不正送金事犯に利用される C&C サーバの動作を観測することにより、国内外の約８万 2,000 台の端末が不正プログラムに感染していることを把握し、被害の拡大防止措置を実施した。

具体的には、プロバイダを通じた国内の感染端末利用者に対する注意喚起及び警察庁を通じた外国捜査機関に対する情報提供を実施するとともに、C&C サーバと定期的に通信を行うことで不正送金に必要な情報を入手するというこの不正プログラムの性質を逆手に取り、その代わりに無害なデータを取得させることにより、この不正プログラムを無害化した。

図４　不正送金事犯に係る不正プログラムによる被害の拡大防止措置



しかしながら、こうした被害防止対策には高度な技術的知見や一定の人員を要すること等から、従来は、主に警視庁によりアドホックに実施されている状況であるといえる。

この点、例えば、上記①の国際的なボットネットのテイクダウン作戦に関し、米国においては、連邦裁判所の命令に基づき、感染端末が自動的に犯人側コンピュータに指示を求める通信を行う際、その通信先を当該命令に基づいて設置された代替サーバに変更し、当該代替サーバに通信を行う感染端末の IP アドレスを FBI が収集するという手法が用いられている。また、同国においては、顧客のセキュリティを確保することを目的として、

マイクロソフトコーポレーションが民事的な手続を用いて積極的にテイクダウンを実施しているとともに、こうした取組に各国の法執行機関も参加している。

したがって、国際的にみれば、我が国において必ずしも戦略的・継続的に被害防止対策が実施されているとはいえない状況であるため、今後、どのように推進していくかが課題である。

第２章　サイバー犯罪対策における民間事業者側の現状と課題

１．現状

(1)　サイバーセキュリティに対する意識に関する現状

民間事業者においては、近年のサイバー空間における脅威の深刻化に伴い、サイバーセキュリティに対する意識が高まっている。このため、シーサート（CSIRT: Computer Security Incident Response Team）活動を例にとると、平成19年に設立された日本コンピュータセキュリティインシデント対応チーム協議会において、各組織のシーサート間の連携が図られているところ、平成24年以前に同協議会に加盟したシーサートは比較的活動経験のあるものであったが、その後に加盟しているシーサートは設立されたばかりのものであり、連携に工夫が必要な状況となっている。

すなわち、各組織に所属する情報技術に関して高度な知見を有する者が、平素からの人間関係を基礎として、暗黙のうちに緊密に連携してインシデントに対応していた従来の状況が変化し、必ずしもインシデント対応の経験が豊富ではない者が各組織のサイバーセキュリティ担当者となる例がみられており、民間事業者間における連携のため、ある程度、連絡窓口のリスト化や対応手順のマニュアル化が必要となっている。

(2)　警察からの捜査関係事項照会・差押えへの対応の現状

警察からの照会・差押えへの対応について、民間事業者の負担は大きなものとなっている。負担の大きさや内容については、民間事業者の事業規模により異なると考えられるが、事業規模が大きく対応件数の多い民間事業者の中には、照会への回答の効率化を図ることや、個人情報を警察へ提供した事実を記録・管理することを目的として、警察からの照会への対応に自社のシステムを活用している事業者がある。

しかしながら、現行の警察からの照会が、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ため、こうした民間事業者においては、捜査関係事項照会書に記載されたメールアドレス等を自社のシステムに逐一手入力して検索することにより、該当の有無が確認された後、回答内容が紙ベースの回答書に出力され、郵送により警察への回答がなされている。

例えば、インターネット・オークションやメール等のサービスを提供しているヤフー株式会社においては、毎月1,000件から1,500件（平成27年中の合計は18,103件）、警察からの照会を受けているが、これに６名で対応している。また、同社においては、毎月20件から40件、警察からの差押えへの対応を行っているため、平均するとほぼ毎日、全国の都道府県警察の捜査員が、東京都に所在する同社の本社を訪れている状況である。

(3) 被害防止対策の現状

被害防止対策について、警察から感染端末に関する大量の情報の提供を受けた民間事業者側の負担は、非常に大きなものとなっているのが実情である。

例えば、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（以下「テレコム・アイザック」という。）は、総務省と複数の民間事業者が連携して国民のマルウェア感染防止と駆除の取組を行うACTIVE（Advanced Cyber Threats response InitiatiVE）という官民連携プロジェクトを統括・推進しており、第１章２．(3)③に記載した被害の拡大防止措置の際、このテレコム・アイザックを始めとする民間事業者側が行った具体的な作業内容は、次のとおりであった。

① 警視庁から43,565件の感染端末リストの提供を受けたテレコム・アイザックがプロバイダ単位でリストを仕分け、協力を得られる16のプロバイダに係るもの（33,196件）のみを抽出し、これらのプロバイダに渡す。
② 次に、各プロバイダにおいて、リスト中のIPアドレスと時刻により、認証サーバのログを検索し、そのときに通信を行っていたユーザーID等を抽出する。そして、このユーザーID等により顧客データベースを検索し、該当する感染端末利用者を特定した上で、重複を省くため名寄せし、注意喚起の対象者を確定する。
③ 各プロバイダにおいて、Webサイトへの掲載、手紙の作成及びメールの送信により、注意喚起を実施する。
④ その後、各プロバイダにおいて、注意喚起を受けた感染端末利用者からの問合せに対応する。

こうした注意喚起の作業については、一般的には、事業規模の大きなプロバイダであれば、その分利用者が多く、感染端末利用者も多くなるため、作業量が多くなり、重い負担となっていると考えられる。他方、中小規模のプロバイダであれば、その分利用者は少なく、感染端末利用者・作業量ともに少なくなっているとみられるものの、そもそも対応に当たることのできる人員が限られているため、やはり一定程度重い負担になっていると考えられる。

２．課題

(1) 警察からの捜査関係事項照会への対応の効率化

警察からの照会への対応に自社のシステムを活用している民間事業者に関しては、照会が郵送で行われていることによる問題点として、①照会内容を自社のシステムに手入力する作業が生じており、業務負担となっていること、②郵送作業や膨大な手入力作業により一定の処理日数を

要する分、結果として警察の捜査が遅延すること、③あくまでも手入力の作業である以上、ヒューマンエラーが生じる可能性があること、④紙媒体での情報管理には、紛失のリスクや情報にアクセスした者の把握の困難さが伴うこと等が挙げられる。

また、前述のとおり、諸外国においては、オンラインによる照会が可能となっている国がある点にも留意する必要がある。

したがって、郵送による照会の見直しにより、民間事業者の対応を効率化させることが課題である。

(2) 継続的・効果的な被害防止対策の推進

被害防止対策を講じるに当たり、民間事業者においては多くの人員・コストを要することから、被害防止対策を継続的・効果的に推進するため、引き続き、十分な時間的余裕を持って、警察から民間事業者に対する事前協議が行われることが望ましい。

また、第１章２．(3)③に記載した被害の拡大防止措置の際には、一部のプロバイダが感染端末利用者に送付する封筒に、警視庁サイバー犯罪対策課の名前を記載するとともに、同庁作成に係るチラシを同封した結果、感染端末利用者からの問合せが警視庁にもなされてプロバイダに集中しなかった。こうした取組により、プロバイダの負担が軽減されただけでなく、警察も共に取り組んでいることの周知にもつながったと考えられるため、今後も継続されることが望ましい。

さらに、従来は、被害防止対策の実施後、警察と民間事業者側との間において、対策の結果に関する情報が共有されていなかったため、民間事業者側にとっては、対策の費用対効果が判然としなかった。すなわちインターネット接続サービスを提供している主体として、インターネット利用者の安全安心を確保する一定の社会的責務があるということは、民間事業者側において一定程度理解が得られているものの、被害防止対策の具体的な効果が分からない以上、こうした社会的責務を果たすという意義の大きさを測りかねる状況であった。

したがって、民間事業者側においては、今後も同種の取組に継続的に対応するべきであるという判断を下すことが困難な一面があったところ、こうした事情を踏まえた取組としていくことが課題である。

第３章　今後の方向性

１．効率的・効果的な捜査に向けた体制の在り方の検討

我が国においては、都道府県警察が全面的に警察の事務を遂行し、一定限度で国（警察庁）が関与することにより、国と地方の権限の競合が生じず、都道府県警察間の競合については、警察庁が関与することにより解決できるようになっている。

したがって、今後、国の警察機関がサイバー犯罪捜査を直接的に行うFBIのような制度を採用するのではなく、あくまでも現行制度の基本的な枠組みの長所を生かしつつ、サイバー犯罪捜査を効率的・効果的に行うための体制の在り方を検討することが望ましい。

まずは、喫緊の課題である不正送金事犯について、JC3を始めとする民間事業者等と連携しながら、警察庁において一元的に情報を分析し、捜査や被害防止対策に効果的に活用することが可能となるよう、体制を強化することが考えられる。

また、将来的には、サイバー犯罪捜査の地理的無制限性を踏まえた上で、より効率的・効果的に捜査を推進するため、警察庁がどのように関与するべきかを検討することも考えられる。

このように、捜査が効率的に推進される体制を整備することは、民間事業者にとっても、警察との効率的・効果的な連携に資するものであり、望ましいものであると考えられる。

２．捜査関係事項照会業務の効率化の検討

(1)　捜査関係事項照会業務のオンライン化の検討

照会業務について、オンライン化を含めた効率化方策を検討することが望ましい。例えば、各都道府県警察の捜査関係事項照会書に関するデータについて、警察庁において一括してプロバイダ等に送信し、プロバイダ等からの回答もデータで受信することにより、警察にとっては、回答を受領するまでの期間が短縮され、より迅速に捜査を進めることが可能となるとともに、郵送に要していた費用が不要になり、コストの削減も可能となる。

また、プロバイダ等にとっても、照会内容を自社システムに手入力する作業が不要となり、業務負担が軽減される上、ヒューマンエラーの可能性を限りなく減少させられる。

さらに、官民双方にとって、オンラインシステムのセキュリティ確保という新たな課題は生じるものの、紙媒体での情報管理に伴う問題が解消される。

こうしたオンラインシステムの構築には、予算措置が必要となるため、実現に向けた具体的なスケジュールを立てることは容易ではないと思われるが、まずは、警察庁とプロバイダ等の間において、いかなる方策が官民双方にとって適当であるかについて、検討を開始することが望まし

い。

その際、プロバイダ等の事業規模により、警察からの照会への対応に伴う負担が異なるという民間事業者側の事情を踏まえることが重要であるため、警察庁と各プロバイダ等の間において、基本的には個別に検討が進められることが望ましい。

(2) 捜査関係事項照会に係る情報の蓄積・活用に伴う問題点の整理

当会議においては、過去に照会された情報を警察が蓄積できるようなシステムを構築することが提案され、①これにより、重複した照会が不要となるのではないかという意見、②蓄積された情報の分析・活用が新たな捜査手法の導入を可能とするのではないかという意見、③サイバー空間において圧倒的なデータ量が取り扱われている中、警察における取扱いも自動化しなければ、警察内部の業務のみならず、部外との連携にも支障を来すのではないかという意見、④今後、IoT（Internet of Things）化が進むと、小規模な民間事業者であっても多くの情報を持ち、警察から多くの照会を受けるものの、それほど人件費をかけられないという事態に陥ると考えられるため、情報を活用する仕組みを早急に整備する必要があるという意見、⑤効率化そのものは望ましいが、警察活動を電子化することにより、アナログで実施する活動とは異なる問題が生じ得るため、透明性の確保と結果の検証が必要であるという意見等が出された。

このうち、重複した照会の回避という点について、警察実務としては、以前に照会した後に登録者情報等が変更されている可能性がある以上、捜査中の個別の事件に関する照会をその都度実施し、当該捜査の対象時期における情報を収集する必要性があると考えられる。

また、照会に係る情報を蓄積し、これを分析・活用することについては、法的な整理を含めた慎重な検討が求められるため、中長期的な課題であるといえる。

３．継続的・効果的な被害防止対策の在り方の検討

(1) 効果的な被害防止対策に資する情報提供の推進

被害防止対策を継続的・効果的な取組とするためには、官民双方にとって持続可能であり、かつ意義のあるものとする必要があると考えられる。そのためには、既に行われている取組、すなわち時間的な余裕を持った警察からの事前協議や官民で共同した注意喚起は、今後も確実になされることが適当である。

また、後述の５．にも関連するが、警察が保有している被害防止対策の手法等に関する情報の中には、民間事業者側の自主的な対応につながる可能性のあるものが含まれていることが考えられる。

したがって、捜査情報の取扱いに留意しつつ、どのような情報が民間

事業者側にとって有益であり、警察から提供可能であるかなどについて、テレコム・アイザックや各プロバイダとの間において、平素から実務レベルで意見交換する場が設けられることが望ましい。

なお、前述したように、日本コンピュータセキュリティインシデント対応チーム協議会において連絡窓口のリスト化や対応手順のマニュアル化が必要となっている民間事業者側の現状を踏まえても、今後、被害防止対策を継続的なものとするために平素から官民連携の場を設け、官民双方の役割について認識を共有しておくことは、重要であると考えられる。

(2) 被害防止対策の効果の測定・分析及び情報発信の推進

警察は、民間事業者等の知見を活用しながら、被害防止対策により、どの程度犯罪が減少したかなどの効果を測定・分析することを試みる必要がある。

また、こうした分析結果については、前述した実務レベルの意見交換の場等を通じて、確実に関係事業者にフィードバックされる必要がある。

さらに、分析結果や官民連携の成果については、可能な範囲で効果的に広報され、国民や、今後、協力が依頼される可能性のある他の民間事業者に対しても情報発信されることが望ましい。情報発信は、対策が社会的な意義を有することを民間事業者が再認識する意味においても、また、対策に関する国民の理解を深める意味においても、重要である。

この点、一般的に、起訴された事件の捜査に関しては、検挙時の広報や公判において、その活動の成果が一定程度明らかになるのに対し、検挙に至らない事案に関する被害防止対策や平素の官民での情報共有に関しては、積極的な情報発信が行われない限り、その成果は警察等、一部の関係者の間でしか共有されない。

当会議において、JC3 の活動の成果に関する広報が課題であるという議論がなされたとおり、こうした被害防止対策の効果等について情報発信する際には、タイミングや内容を工夫することが求められると考えられる。

(3) 被害防止対策を講じるべき主体の検討

当会議においては、被害防止対策を講じる主体についても、様々な意見が出された。まず、①不正送金事犯に係る不正プログラムによる被害の拡大防止措置に関して、金融機関やインターネットの利用者は受益者であるといえるので、これらの主体に対して自主的な対策を講じるよう、警察から働き掛けてほしいという意見や、②脆弱性を有する無線 LAN ルータを製造し、当該脆弱性を突いたサイバー攻撃の原因を生み出したといえる民間事業者に対しても自主的な対策を講じるよう、警察から働き掛けてほしいという意見が、プロバイダからの要望として出された。

このほか、③そもそもプロバイダは、インターネットの利用者の安全安心を確保するため、インターネット接続サービスを提供している主体として、どの程度の責務を果たす必要があるのかが問題となるという意見、④プロバイダが果たすべき責務について、事業規模を考慮する必要があるという意見、⑤逆に、中小規模のプロバイダであっても、一定の責務はあるのではないかという意見も出された。

いずれの主体に自主的な対策を求めることが適当かについては、事案次第であると考えられるため、今後も、事案の内容に応じた取組がなされることが望ましい。なお、不正送金事犯に関し、警察は金融機関に対して、直接又は JC3 の場を通じて、自主的な対策を講じるよう働き掛けており、こうした取組は引き続き積極的に推進されることが望ましい。

４．諸外国のサイバー犯罪対策の手法等に関する調査研究の実施

「世界一安全な日本」創造戦略（平成 25 年 12 月 10 日閣議決定）において、「サイバー犯罪捜査においては、事後的な犯人の追跡に困難を伴うケースが多々あることから…新たな捜査手法について検討する」とされているとおり、サイバー犯罪対策の新たな手法等については、不断の検討が求められる。

しかしながら、前述した欧米各国のサイバー犯罪対策の手法等については、従来、警察庁において、その制度の詳細に関して、必ずしも体系的な調査と評価がなされてきたとはいえない。

当会議においても、欧米各国のサイバー犯罪対策に係る手法等が紹介され、①法制度がテクノロジーに追いついていないと考えられ、見直しが必要ではないかという意見、②国により法制度が異なるものの、国民を犯罪から守るという観点から必要となる対策の手法等については共通する考え方もあると思われ、国境を容易に越えるサイバー犯罪に対する諸外国の取組には、我が国の参考となる点も多いのではないかという意見、③なぜ、そのような手法等が必要であるのかという観点や、どのような条件であれば実施が可能となるのかという観点が重要であるという意見、及び④具体的な成果、問題が生じたケース等、諸外国における運用実態を把握する必要があるという意見が出された。

したがって、今後、我が国のサイバー犯罪対策において有効であると考えられる手法等の導入可能性を検討する際の参考とするため、まずは警察庁において、こうした手法等に関する制度の詳細、根拠法令、普及状況、有効性等について調査研究を進める必要がある。

５．戦略的な被害防止対策に向けた法的整理の検討

被害防止対策については、その重要性が高まっている中、アドホックな形ではなく戦略的に講じられる必要があると考えられる。そして、戦略的な対策として、いかなる方策が適切であるかについて、その前提となる法

的な観点から論点の整理が進められることが望ましい。

(1) 捜査で得られた情報の利用に関する法的整理

第一の法的な観点として、サイバー犯罪捜査の過程で得られた情報の被害防止対策目的での利用に関する論点が挙げられる。すなわち、捜査の過程で得られた情報は、被害防止対策に有用なものが多いため、こうした情報を公表することや、民間事業者と共有することが法的に許容される場合があるのではないかという論点である。

この点、刑事訴訟法（昭和 23 年法律第 131 号）第 47 条においては、「訴訟に関する書類は、公判の開廷前には、これを公にしてはならない。但し、公益上の必要その他の事由があつて、相当と認められる場合は、この限りでない。」と規定されており、これは、刑事訴訟に関する記録が公判開廷前に公開されることによって、訴訟関係人の名誉を毀損し、公序良俗を害し、又は裁判に対する不当な影響を引き起こすことを防止するための規定であると理解されている。

そこで、同規定の趣旨を踏まえ、サイバー犯罪の被害防止の観点から、公益上必要かつ相当と認められる範囲内であることを前提としつつ、積極的な情報の利用を推進する必要がある。

(2) 積極的な措置に関する法的根拠の付与の検討

第二の法的な観点として、サイバー空間における安全安心の確保に向けた積極的な措置に関する論点が挙げられる。すなわち、従来のような受動的な防御にとどまらず、いかなる根拠に基づき、いかなる措置を言わばプロアクティブに（先制的に）講じることができるのか、当該措置を講じるためには新たに法的根拠を付与する必要があるのかという論点である。

この点、現実空間においては、交通一斉検問や警察官職務執行法（昭和 23 年法律第 136 号）第５条（犯罪の予防及び制止）及び第６条（立入）に基づく警察官による行政処分が行われているほか、被害者保護等の気運の高まりに伴い、配偶者からの暴力の防止及び被害者の保護等に関する法律（平成 13 年法律第 31 号）、ストーカー行為等の規制等に関する法律（平成 12 年法律第 81 号）、児童虐待の防止等に関する法律（平成 12 年法律第 82 号）等が制定され、これらに基づき、警察等の公的機関により被害防止に資する措置が講じられている。

しかしながら、サイバー空間における安全安心の確保については、今や現実空間における個人の保護と並ぶ大きな課題となっているにもかかわらず、積極的な措置に関する議論が進められておらず、対策が後手に回っていると言わざるを得ない。前述のとおり、現に米国のテイクダウンにおいては、連邦裁判所の命令に基づき、FBI により通信先を代替サーバに変更する措置や、マイクロソフトコーポレーションにより民事的な

手続による措置が執られていることを踏まえれば、我が国においても、更なる措置を執る余地があるように考えられる。

今後、積極的な措置に関して整理されるべき法的論点としては、その措置により利益侵害が具体的にどう生じるのかという論点、サイバー空間におけるプライバシーの侵害とは何かという論点、通信の秘密との関係をどう考えるのかという論点、前述した現実空間における措置のうち、いずれの措置と同程度の利益侵害が生じることとなるのか、又は、現実空間における措置と比較することは困難であり別に整理することが適当であるのかという論点等があると考えられる。

そして、官民連携は、積極的な措置においても不可欠であり、いかに連携して措置を講じるべきかという論点も検討が必要である。インターネットの利用者の日常的な安全は、そのサービスを提供している民間事業者により支えられている部分が大きいため、積極的な措置においては、民間事業者が果たす役割が大きいという点を考慮する必要がある。また、民間事業者にとっては、犯罪の危険が迫っている時点で、警察から情報提供を受けて連携することにメリットがある点も重要である。さらに、執るべき措置の内容についても、公的機関の対処能力を踏まえることはもちろんのこと、民間事業者側の要望も踏まえて検討されることが望ましい。

以上のとおり、積極的な措置に関する法的根拠の付与については、多岐にわたる論点の整理が必要であり、中長期的な課題となるが、刑事法・行政法の垣根を越えた検討が開始されることが望ましい。

平成 27 年度総合セキュリティ対策会議委員名簿

前田　雅英	日本大学大学院　法務研究科　教授
（委員長）	
片山　　建	日本マイクロソフト(株)　法務・政策企画統括本部
	政策企画本部　次長
桑子　博行	違法情報等対応連絡会　主査
小屋　晋吾	トレンドマイクロ(株)　執行役員　統合政策担当部長
坂　　明	(一財)日本サイバー犯罪対策センター　理事
佐々木　良一	東京電機大学　未来科学部　教授
佐藤　晴樹	(一財)日本データ通信協会テレコム・アイザック推進会議
	企画調整部長
寺田　真敏	(株)日立製作所　ＨＩＲＴ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　取締役　最高技術責任者
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
林　　紘一郎	情報セキュリティ大学院大学　教授
藤川　春久	セコムトラストシステムズ(株)　情報セキュリティサービス本部
	常務取締役本部長
藤原　靜雄	中央大学　法科大学院　教授
別所　直哉	ヤフー(株)　執行役員　社長室長
星　　周一郎	首都大学東京　都市教養学部法学系　教授
宮下　正彦	弁護士
山下　眞一郎	富士通(株)　セキュリティマネジメントサービス事業本部
	サイバーディフェンスセンター　シニアマネージャー
若江　雅子	(株)読売新聞東京本社　編集委員

計　１９人（敬称略・５０音順）

【オブザーバー】内閣官房、総務省、法務省、経済産業省

平成 27 年度総合セキュリティ対策会議の開催状況

第１回会議　　平成 27 年 12 月 22 日(火)

第２回会議　　平成 28 年１月 27 日(水)

第３回会議　　平成 28 年２月 22 日(月)

第４回会議　　平成 28 年３月 11 日(金)