平成 28 年３月 11 日

# 平成２７年度総合セキュリティ対策会議（第４回）
# 発言要旨

## １．開会

## ２．平成 27 年度総合セキュリティ対策会議報告書(案)「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

【事務局から、平成 27 年度総合セキュリティ対策会議報告書（案）「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」について説明】

## ３．質疑応答

○（片山委員）　報告書について、とてもよくまとまっており、論点等も整理されていると思いますので、異論はございません。参考までですが、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について、先ほど事務局から御説明もありましたが、法制度がテクノロジーの進歩に追いついていないという点はまさしくそのとおりだと思います。米国の下院司法委員会で２月２５日、情報の越境移転及び法執行機関からのリクエストに関してマイクロソフトから証言をさせていただく機会がございました。米国においては３０年前の法律の枠組みに基づいて物事が動いているところもあり、先日 Facebook 関係者がブラジルで拘束されたという話がありましたが、これが、法律が技術の進歩に追いついていない事例として紹介されました。また、ＭＬＡＴ（刑事共助条約）も、時代に追いついていないことやグローバルで情報が動いている世界になっている中で、どういう法の枠組みの中でとらえていくべきかということが、この総合セキュリティ対策会議の開催中にアメリカの委員会において発言されたのはよいタイミングであったと思います

○（前田委員長）　調査研究を不断に行っていくことに異論ないと思いますので、警察庁が主体的に取り組んでいただきたいと思います。研究結果を差

しさわりのない範囲で発信していただけると、より効果が意味を持つと思います。

○（林委員）　前回、星委員の御発表に感銘を受けたので、今後も引き続き検討いただきたいと思います。ただ、メディアの受け取り方は少し気になっています。今回の報告書の目玉がどのようにとらえられるかということと、打ち出す側としては、どう打ち出すのが一番いいのかということが、少し気になりました。

○（若江委員）　他のメディアがどう受け取るかは分かりませんが、私は星委員の報告を聞き、特に後段の部分は問題提起する価値が大きいと思っています。法制度がテクノロジーに追いついていないとか、社会の意識が追いついていないというのを日々の取材で感じていますので、それをどうすべきか社会に提起する必要があるという意味で、取材したいと思いました。

○（前田委員長）　広報の方針について等、可能な範囲でお考えがあれば事務局から御説明ください。

○（事務局）　未定ですが、今日の議論を踏まえて最終的な調整をした上で、日程としては、４月初旬の国家公安委員会に報告した上で公表するという形になると想定しております。

○（前田委員長）　どの部分を強調してということは特になく、淡々とやるということですね。

○（事務局）　今回は特定の論点というよりは、全般的に今の捜査と被害防止対策をめぐる状況を整理したところ、全体的に説明することになると思います。

○（中野目委員）　報告書案は問題点が指摘されていて、論点を広く知らせるという意味でも、非常に有用であると思います。ただ、プロアクティブという言葉についてですが、横文字で表現されていて、一般の国民の方に読んでいただくことを考えると、日本語の表現を加えたほうがいいと思います。「積極的な」というと、意味が伝わりにくいということもあるように思いますので、「予防的な」とか、「先手を打った」といった言葉が考えられると思います。可能であれば、日本語で意味を補充したほうがよいと思います。

○（前田委員長）　読んでいただいて御理解をいただくことは何より大事

なことだと思います。我々専門家としては例えばプロアクティブという言葉も意味は理解できますが主に誰に理解してもらうかということを考えれば、分かりやすさは重要だと思います。可能な限り分かりやすい文言に修文させていただきたいと思います。それでは、この報告書案に関しては、今までいただいた御意見を踏まえて修文を検討します。ただ、その修文に関しては私にお任せいただくという許可をいただいた上で、報告書案は御承認いただけたということでよろしいでしょうか。（委員から異議なしとの発言あり）それでは、短い期間で、十分な情報提供ができたか不安になるところもありますが、２７年度の総合セキュリティ対策会議の報告書案について御賛同いただけたということで決定したいと思います。残された時間で、各委員から展望的な御意見をいただければありがたいと思っております。

**４．各委員挨拶**

○（片山委員）　　２点に絞ってお話いたします。法律が技術の進歩に追いついていないという観点から言えば、今回、ボットネットのテイクダウンの取組を話させていただきましたけれど、状況は、刻一刻と変わっていきます。技術が進歩し続けている中で、そういった技術が予想されていなかった時代の法律が使われていることについては、今後の展望として議論が続くものと思います。

○（桑子委員）　　インターネットの世界は、ものすごく格差のある世界と承知しております。例えばプロバイダ、事業者の立場も規模によってかなり大きな開きがあるという状況ですし、利用者、ユーザーもまさに同様の状況にあると思っております。今回、報告書をとりまとめたわけですが、この内容は、あくまでもきっかけであると思っております。今後、理解度に非常に大きな差のある事業者、利用者、国民にどうやって理解いただくか、周知するかが一番重要かと思っております。この報告書を理解いただいて、結果として日本の全体のセキュリティレベルがアップすることにつながればよいと考えています。

○（小屋委員）　　３点申し上げたいと思います。１つは、代金の決済方法が多様化し、例えば銀行やクレジットカード会社が相当の金額をコントロール

していると思いますが、今後はそうしたことができにくくなってくると思います。すると、セキュリティベンダーや他の組織はなかなか情報がとれなくなるようなことが予想されます。ですので、警察が捜査で得た情報というのは、非常に有効な対策の基になると思いますので、是非今後一層の情報交換をセキュリティベンダーとしてお願いしたいと思います。また、ＩｏＴ機器が今もう相当汚染させられて、有害なパケットが入っているという現状から見ると、サイバー空間は公衆空間だという認識を持って臨まないと、健全な空間を作ることはできないと思います。インターネット上で悪いパケットを出し続ける者にデメリットがないと、結局ベンダーとか機器ベンダーが頑張っていいものを出しても、それに価値を認めないから買わないということになりますので、こういうことも警察の皆さん以外でも広く議論していくべきであると思っています。最後は、セキュリティに関する人材の育成に関してで、警察において是非たくさん人材を育てていただいて、民間と交流ができると情報の共有もスムーズにいくと思います

○（坂委員）　総合セキュリティ対策会議に参加させていただき、多くの有益なお話を伺えたことを大変ありがたく思っております。報告書についても、日本の現状を踏まえて、様々な官民の協力を具体的に前進させる施策が盛り込まれており、私もありがたく思っているところです。日本は、対応の一元化という観点では、米国等のように多くの機関に捜査権があるという状況とは異なって、警察庁と都道府県警察が一体となってサイバー犯罪に立ち向かうことができる体制があると思います。また、情報共有にしても、このような状況を踏まえて非常によい体制にあると思います。さらに、ＪＣ３フォーラムにおいても、情報の収集・分析、そしてそれを具体的な検挙や対策に活用するインテリジェンスの重要性というお話がございました。今回の議論の中で出た様々な方策、あるいは検討を踏まえ、今後、分析や情報を活用するという意味でのインテリジェンスといった部分も前進し、またその成果が多くの方々と共有されてサイバー犯罪への対応が進むことを期待しております。ＪＣ３もいささかでもお役に立てれば幸いと思っております。

○（佐々木委員）　今回の報告書は、良い方向にまとまりつつあると思っております。一方では御存じのとおりサイバー攻撃はますます厳しく悪質にな

っているわけです。恐らくＡＩ機能付きの悪質性の高いものも近い将来出てくるだろうと思います。そういった観点も考慮しつつ対策を考えていく必要があるわけですから、研究と現場とがいろいろな形で協力していくことが必要であると思います。守る側もセキュリティインテリジェンスと、アーティフィシャルインテリジェンスを組み合わせてやっていくことや、そういったことが恐らく必要になるだろうと思います。さらに、MARC GOODMAN の「FUTURE CRIMES」という本には、単にコンピューターだけではなく、あるいはＩｏＴだけではなく、ロボットか、３Ｄプリンタ、遺伝子工学的なものを媒介にして攻撃するだろうということが書いてあるわけです。そういった時代が、いつか来るだろうということを踏まえて、今からいろいろ考えていく必要があると思います

○（佐藤委員）　今回はいろいろな視点を御示唆いただく機会に参加させていただき、大変に勉強になりました。また、我々の通信事業者の現状を皆様に御理解いただく発表の場をいただくとともに報告書においては、ＩＳＰの考えを十分に汲み取った内容を記述いただき、大変ありがとうございます。今後について考えると、変化に柔軟に対応していくということが、我々の事業者にとって一番重要なことでございまして、その観点では、委員の方々からお聞きできた様々な専門的見地の御見解は、とても参考になるものでございました。今まさに我々ＩＳＰが直面している課題に対して、今回勉強させていただいた内容を参考に、より的確に対応をしていける力を少しずつ養いながら進めていきたいと考えており、今後も警察を始めとする本会議に参加されている方々とより深く連携をしていくべきであると思います。引き続き御指導、御鞭撻をいただきながら、少しでもより良い環境作りをできるように貢献してまいりたいと思います。

○（中野目委員）　この報告書では率直に様々な問題点が指摘されており、いろいろな方々にどう対処していくべきかを考えていただく際の大きな参考になると思います。報告書の中でも触れられておりますが、警察庁がサイバー犯罪の領域でハブの役割を果たすような機関となる必要が高まっていると思います。そういう意味では、この報告書に書かれている方向性がより強まっていくことに、私自身は賛成です。いろんな機関、例えば INTERPOL にして

も、解析のツールを提供するなど、少しずつ変化を見せてきているわけであります。そういう、客観的な状況の変化にあわせて、効果的に対処することができるようなやり方を考えていく必要があるだろうということであります。また、サイバー犯罪というのは、これは国境がないものです。従来の犯罪ですと、ボーダーコントロールということで対処できたところが大きいわけですけれども、サイバー犯罪となるとボーダーがない。しかも、捜査協力が期待できないところから攻撃が仕掛けられてくるという状況にあるわけです。それに対処するために、プロアクティブに対処するために、一体どこまで、どういう方法でやればよいかということを、今後考えていく必要があると思います。

○（西本委員）　セキュリティ対策というと、管理責任を明確にするという部分のアプローチが非常にポイントになるわけです。それは当然として、捕まえる、悪いほうを囲い込む、追い込んでいく方策が非常に重要になるかと思います。そのためには、捜査情報の開示・共有というのは非常に重要なポイントですが、逆に企業の被害情報の共有も非常に重要になると思います。まず１点は、公表される企業の経営層に理解していただくようなアプローチ。もう１点､セキュリティ企業等の守秘義務と公益性との関係を今後何かしらガイドしてもらえると良いと思います。

○（則房委員）　報告書を通して、サイバー犯罪は絶対許さないんだということを日本の人に訴えることは、非常に重要だと思います。その一方で、絶対に犯罪者を検挙できない場合が残ってしまうわけで、それは海外からの組織的なサイバー犯罪だと思いますが、そういうものに対して、どう取り組んでいくのかといった方向性を研究、検討して示してもらえると、被害に遭いそうな重要な企業としては安心感が出てくると思います。

○（林委員）　セキュリティの次を考える上では、キーワードはやはりインテリジェンスではないかと思っております。インテリジェンスといえば、やはり最大の実施者は国で、このあたりをどう考えるかということは、真剣に議論を始めなければいけないのではないかと思っております。１つの例として、シンポジウムでイギリスの Imperial College の情報処理の先生が来られて、プレゼンテーションがありましたが､イギリスのシギント機関でありますＧＣＨ

Ｑのロゴが、16 枚写したパワーポイントの資料の中に３カ所も出てくるわけです。大学が十何校程指定されまして、そこでセキュリティ人材を育成しているわけですが、それにＧＣＨＱが協力しているという図表がありました。イギリスなりの事情として、スノーデン事件以後、アメリカもイギリスもシギント機関は相当社会的非難を浴びており、オープンにする傾向があるようで、対外的に言っていいところは表に出していこうということを強く感じます。現にセキュリティの対策を打っている民間企業その他の官庁で役立っていることもまた事実だと思います。特に２０２０年のオリンピックに向けて考えるときに、この問題は時間の制約の中で考えるべきであるという気がしております。

○（藤川委員）　自社では９７年から情報セキュリティとデータセンターを担当しております。情報セキュリティに関しては、検討すべき対象範囲が非常に広がってきております。特に制御系システムやネットワークに接続される機器のセキュリティ対策も重要となっております。私どもの会社は、大規模なネットワーク網に接続する機器を守るという観点ではＩｏＴも視野にいれたセキュリティ対策が求められております。また、先日はフィンテックの最新動向について説明を受けたのですが、インターネットバンキングで不正送金が大きな問題となる中、新たなサービスが犯罪の温床になる可能性もあると感じています。こうした背景から今回の報告書にもあるように、早期に警察行政の効率化、電子化に必要なシステムインフラの整備を進めて、ネットワーク犯罪の捜査対象となる大量の電子データの解析もできるよう進める必要性を感じます。最終的にはサイバー犯罪においても犯人逮捕に繋げなければ犯罪意識を持たない犯罪者がさらに増加するのではないかと危惧しています。この会議を通じて、また、ＪＣ３にも参加させていただいて、これまでの受身のセキュリティからポジティブのサイバーセキュリティに携われることを願っております。

○（吉川代理（別所委員））　今年度の総合セキュリティ対策会議においては、照会業務、それから差押えに関して、実情・実務がどうなっているのかということを御紹介させていただきました。報告書においても、その状況を記載していただき、私どもがいくつか提起させていただいた課題についても、報告書に記載していただいたことに関して感謝申し上げたいと思っております。

報告書の中では、中長期の課題、短期で進めるべき課題とそれぞれ書き分けられていると受け止めましたけれども、短期のところについては、私どももできる限り御協力して進めてまいりたいと思いますし、中長期的な課題については、今後も整合的、継続的な議論がなされることを望んでおります。

○（星委員）　プロアクティブについてですが、ある時期から好んで使っているところがあります。理由としましては、刑事法の世界では、これまでの歴史的な文脈もあって、未然防止とか予防とかという言葉を使うことを良しとしなかった経緯があったためです。そこで、他に適切な言葉がないかと探しているときに見つけたのがプロアクティブだったもので、それ以来使っているということです。もちろん、バランスをいかにとっていくのかということが非常に難しくなっていくと思います。ただ、それがあるからと言って、躊躇していられない状況になってきているということだろうと思います。積極的に論点、議論を整理して、どこまでできるのかということを明確にした上で、ルールとして示した上で対応していくことが必要であると改めて考えさせていただいたところです。

○（宮下委員）　報告書については、大変よくまとまっていて、これ以上申し上げることはありません。関連して２点ほど申し上げるとすれば、１点目としては、今後の方向性で出されているものは、いずれも継続を前提とした施策だと思います。これを継続していただくことが非常に重要であると思っておりまして、国できちんと検討してもらいたいと思っています。第２点は、今回のテーマが官民連携を更に推進することでありますが、官民連携というその前提としての国民あるいは被害者の意識をどう考えればいいのだろうということがあると思います。例えば、金融機関が攻撃を受けていて、その金融機関も都市銀行が順繰りに攻撃を受ける。その後は地方銀行、信用金庫というように順繰りに攻撃を受けている。その攻撃を受けることについて、最初は誰も免疫がないので、思うように犯罪者から被害を受けてしまうということについて、全く連帯して犯罪を抑止するというベクトルがかかっていないと考えさせられることがあります。それはよく考えてみると、本当に無抵抗のままやられるというのが最初の状況なものですから、例えばスペインのピサロがわずかな軍隊を率いてインカ帝国を滅ぼしてしまったり、そういう

非常に少数なものが国全体を支配してしまうという事態になっているのではないかと思います。そういう状況を許すぐらい、サイバーをめぐる環境は脆弱になっているということを改めて感じた次第です。一体、それを変えるためにどうすべきかということについては、官民連携はやはり、いかにその脆弱であり、犯罪を防止することにどれだけ不向きな状態にあるのかということを、いろいろな場所でいろいろな例えを使って、いろいろな方法で周知させていくことが必要になるのではないかと思います。そうしない限り、新たなパターンが出ると、それで一通り被害に遭うことを永久に続けることになってしまうのではないかという印象を強く持ちました。

○（山下委員）　日頃、サイバーのスレットインテリジェンス（脅威情報）の分析、収集関係を行っておりますが、是非、捜査で得られた情報の利活用を推進していただきたいと思っております。

○（若江委員）　今回はいろいろ勉強させていただき、ありがとうございました。官民連携や捜査における隘路といった問題について整理したことは、とても意義のあることだと思いました。技術も犯罪形態もどんどん変化していくので、今回だけに終わらず、不断に続けていかなければいけない見直しであると思います。是非、来年度以降も取組をされると良いと思いました。整理する問題の中には、犯罪の未然防止のための措置など、もしかすると社会には過剰反応とか、ちょっと踏み込みすぎではないかという意見もあるかもしれませんが、今どういう状況になっていて、何ができていないのかということを、社会に広く情報を開示していけば、議論が喚起され、理解が深まるのではないかと思います。社会に現状を知られていない部分は多く、例えば、今回の会議の中で一番驚いたのは、捜査関係事項照会の件数の多さでしたが、一般の社会の人も、ほとんど知らないのではないかと思います。ですから、不断に情報を開示して国民の理解を求めていくことも必要であると思います。

○（前田委員長）　それぞれ重要な御指摘をいただきありがとうございます。１つの方向性としてはプロアクティブな措置のようなものに対する刑事法の専門家の感覚については、やはり変わろうとしていると思います。それは、インテリジェンスも同様です。インテリジェンスの問題とプロアクティブな

措置は表裏一体だと思います。それを国民が受け入れる前提としては、守秘義務、また、それ以上に重要なのは国民の信頼だと思います。その信頼をどう醸成するかについては、国や文化によって違うと思います。日本においてどういう制度が最も国民の信頼が得られるかということで他の国と比較しながら是非警察でも考えていただきたいと思います。それにつながる話として、各国の制度を調べて、フィードバックしていただけるとありがたいと思います。最後に、この会議をこれまで続けてきたことの最大の成果は、官民連携が実のある形でできてきているというところだと思います。一歩一歩具体的な問題で報告書を書き議論をして、信頼を積み上げていくということが大切であると思います。その意味で官民連携は間違いなく前に進んできたと思います。ここでできている人間の信頼関係が、ある意味で官民連携の核であると感じております。

## ５．生活安全局長挨拶

平成２７年度総合セキュリティ対策会議として、４回にわたって御議論を賜りました。各界で御活躍されている委員の皆様に御出席を賜りまして、本当にありがとうございます。お忙しい中お時間をいただきましたこと、心から感謝を申し上げたいと思います。今回は、サイバー犯罪捜査及び被害防止対策における官民連携というテーマで検討をお願いした訳でありますが、庁内でテーマを決めるときに、私は、「被害防止対策」を「犯罪捜査」と車の両輪として表題に出すべきであると主張いたしました。最終的な提言はどうなるのか、何か実現可能な提言がなされるのだろうかという議論もありました。実際に、今回いろいろ議論していただいたテーマは非常に大きく、直ちに予算措置や制度改正等の形で対策を提示できるものもあるかもしれませんが、ほとんどのものはそうはならないのだろうと思います。ただ、内部で検討したときには、仮に具体的な施策に結びつかなくても、問題をきちんと提起したということ、委員の皆様のような各界で専門的知識をお持ちの方々に議論をしていただいて問題を提起したということ自体が、非常に大きな価値があることになるということで、このテーマを最終的に取り上げることとしました。そういう意味では、対外的に広報するときに、プロアクティブな措置の

部分について大きなテーマを提起していくということに力を入れたブリーフィングをすべきであると思います。また、犯罪捜査を通じて得た情報を、どういう形で有効に使っていくかということは１つ大きなテーマですし、犯罪捜査上、秘密の扱いをすることは重要ですが、公益目的で被害防止に非常に役立つものがあります。さらに、プロアクティブな措置については慎重な検討が必要ですが、例えば、攻めの被害防止ととらえればよいと思います。最後になりますが官民連携は、組織と組織の信頼関係以前の問題として、個人と個人の信頼関係が前提になっております。こういう関係がないと官民連携は進まないと思います。そういう意味で、今後とも是非様々な場面で御協力を賜れればありがたいと考えております。

## ６．　閉会