平成 27 年 12 月 22 日

平成２７年度総合セキュリティ対策会議（第１回）
発言要旨

１． 開会

２． 生活安全局長挨拶

警察庁生活安全局長の種谷でございます。本日は前田委員長をはじめ、委員の皆様方には、年末の大変お忙しい時期にお集まりいただきまして、誠にありがとうございます。また、日頃から警察行政に多大な御理解と御協力を賜りまして、この場をお借りいたしまして御礼を申し上げたいと思います。

総合セキュリティ対策会議は、本年で１５年目になります。これまでいただいた御提言は多くございますが、例えば平成１８年に運用が開始されたインターネット・ホットラインセンターや、昨年、業務が開始されました日本版ＮＣＦＴＡであるＪＣ３といった具体的な施策に結実をしてきているところでございます。そういう意味で、私たちにとっては大変ありがたい会議ということでございます。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の更なる推進」という題目で御議論をいただきたいと考えているところでございます。警察では、現下の大変厳しいサイバー犯罪情勢に対処するために捜査を推進してきているところでありますが、捜査だけではなく、被害防止対策、被害拡大防止対策をもう一つの車の両輪として重視してきているところでございます。

御承知のように、Game Over Zeus の国際的なボットネットのテイクダウンへの参加、Ｃ＆Ｃサーバの無害化、さらに３回にわたって中継サーバを摘発し、その中継サーバの中に入っていた他人のＩＤ、パスワード等につきまして民間事業者を通じて注意喚起をさせていただくなど、被害拡大防止についても注視をしてきているところでございます。ただ、こういった中でいろいろな捜査上の隘路、また被害拡大防止上の隘路にもぶつかってきているところでございます。もちろん匿名性の隘路、国境の隘路もありますが、やはり技術的な隘路や、法律的な隘路といった問題が多数あるわけであります。こ

れらの問題には警察のみで対処するわけにはいかないと考えているところでありまして、官民連携、民間の方々のお知恵を拝借して、その隘路に何とか対応していかなければならないと考えているところであります。

そういう意味合いにおきまして、今回は捜査を進めていく上、さらに被害拡大防止を図っていくために対処していかなければならない、様々な課題、隘路を共有化しまして、それに対してどう対処していけるのかという点について御議論をしていただきたいと考えているところでございます。委員の皆様におかれては、それぞれの分野での御経験ですとか、御見識を踏まえ、是非闊達な御意見を賜ればと考えておりますので、どうぞよろしくお願いします。

３．　委員長挨拶

４．　総合セキュリティ対策会議の提言を受けて実施された主な施策及び平成 27 年度総合セキュリティ対策会議のテーマについて

【事務局から、総合セキュリティ対策会議の提言を受けて実施された主な施策及び平成 27 年度総合セキュリティ対策会議のテーマについて説明】

５．　警察におけるサイバー犯罪捜査及び被害防止対策について

【事務局から、警察におけるサイバー犯罪捜査及び被害防止対策について説明】

６．　警視庁におけるサイバー犯罪対策について

【警視庁から、警視庁におけるサイバー犯罪対策について発表】

７．　国内におけるシーサート活動について

【委員から、国内におけるシーサート活動について発表】

８．　質疑応答

○（津幡代理（西本委員））　警視庁の発表の中にサイバー犯罪を行う組織の

イメージがありましたが、非常にアクターが多く、これはすごいなと思ったのですけれども、普通、犯罪というのは仲間が多ければ多いほどばれやすいというか、裏切りやすいという印象があります。たくさんアクターを増やすことは犯罪者側にとって逆効果ではないかなと思いますが、アクターが増えることによって警察としてより困っている点、また、通常の犯罪とサイバー犯罪で異なる点があれば教えていただきたいと思います。

○（警視庁）　サイバー犯罪者同士はお互いをネット上のハンドルネームでしか知らず、人数が増えることによるリスクはあると思いますが、お互い一部しか知らないので逆に安心しているということもあるのではないかと思います。ただ、悪い者同士が騙し合うという例もありまして、お互いある程度は信用しているが、ある程度は警戒しているというところだと思います。

○（津幡代理（西本委員））　逆に言うと、１人捕まえても芋づる式にはなかなか検挙できないという実態があるわけですね。

○（警視庁）　全くそのとおりだと思います。

○（中野目委員）　事務局の説明で、ウイルスを無害化するデータを置くという説明がございましたが、これは相手のパソコンに存在している不正なアクセスをするためのプログラムを無害化するべく、相手が目的とするデータをダウンロードしたときに、相手のコンピュータに一定の操作を加えるということを意味するのでしょうか。

○（事務局）　ウイルスが設定情報を取りに定期的に通信する特徴を逆手に取り、白紙の情報をウイルスに与えることで無害化を行うということです。

○（種谷局長）　捜査の細かい情報なので、もちろんお話しできないことがたくさんありますが、実際に相手のサーバに入りこんでプログラムを書きかえるという手法ではありません。こうした法的な隘路の問題をくぐり抜けて、現行の法制下でできる限界事例であると思います。

○（前田委員長）　関連していろいろな問題、隘路の問題でやはり法的な制限を動かさなければいけないところまで来ていれば動かすのでしょうし、また議論を進めてまいりたいと思います。

○（小屋委員）　２点教えていただければと思います。１点目は不正送金事犯の件ですが、昨年は非常に阻止額が増えて送金のディレイとか、海外口座

の送金をしないなど、銀行側の対策が功を奏していたと思いますが、今年については結構、阻止額が減ってきてしまっている。この点、手口の変更があるのでしょうか。

○（事務局）　いろいろな要素があると思いますが、昨年後半に阻止額が増えたのは地方銀行に当日送金の停止措置という対策をとっていただいて、これが非常に有効であったためだと思います。今年に入って被害が、信用金庫にシフトしてしまい、信用金庫がそういう対策を必ずしもとっていなかったことから、結果として阻止率が下がってしまったという状況でございます。

○（小屋委員）　もう１点、逆にサイバーの事案に対する海外からの日本への照会について傾向等があれば教えていただけますか。

○（事務局）　正式に受けた照会件数は、実はそれ程多くはありません。その数だけを見て、日本発のものが増えているとか、減っているということは必ずしも読み取れないと思います。実態のごく一部しか、海外からの照会はされていないと思います。

○（片山委員）　これまで検挙してきた案件で、被害を受けた側の特徴があれば教えてください。以前、ドイツの警察の方とお話しさせていただいたとき、出し子や運び屋は意外とインターネットの知識が低かったり、インターネットのユーザー側の知識が比較的低かったり、ウイルス対策ソフトを入れていない場合が多かったりすると聞いたのですが、被害を受けた側の特徴というのは何かあるのでしょうか。

○（警視庁）　不正送金に関して言えば、被害者のパソコンにはアンチウイルスソフトは入っている場合が多いです。特にコンピュータリテラシーが低いということはないと思います。他方、その他の犯罪に関しては、例えばウイルスを提供している人や欲する人がいるわけで、ちょっとした好奇心でコンピュータウイルスを集めてみたかったとか、提供する人とコンタクトをとってやってしまった、そういうことは言えると思います。

○（山下委員）　最近、緊急インシデントで出動しますとお客様が実際に、ＡＰＴ攻撃を受けていらっしゃいます。Ｃ＆Ｃサーバは海外も一部残っておりますけれども、最終的な奪取データをアップするサーバに関しては、最近は国内が大変多いと感じております。このあたりはどうお感じでしょうか。

○（警視庁）　国内、国外にかかわらずそのような被害にあったサーバがかなりあるというのは承知しております。そのサーバを調べても、所有者には悪意がない場合がほとんどでありますが、不正なツールが仕込まれており、ログが取られない設定にされており、調べようもないということが多いです。

そういう意味では、セキュリティが弱いために知らないうちに犯罪の手を貸してしまう危険性があることについても啓発活動は必要であると感じております。

○（藤川委員）　２０２０年のオリンピックに向けて、ＩｏＴという背景もありますが、制御系システムに対する不正アクセスや知的財産の情報漏洩に関する事件が具体的に発生しているかどうか教えてください。

○（事務局）　最近の例として、日本の漫画が発売前に海外のサイトに翻訳された上で掲載されていた事案があり、著作権法違反で検挙したという事例はございます。

○（藤川委員）　ある日本の企業が研究開発して製品化しようとしていた製品が、それよりも早く海外の企業から出されたという新聞記事を拝見したのですが、そういった事案は国内で認識されているのでしょうか。

○（事務局）　直ちにはわかりかねます。

○（佐藤委員）　不正送金の口座名義は中国人が過半数を占めるというようなお話がございますが、中国人以外ではどういった方々が口座名義人になっているのか、また、その辺りの手法や、事例があれば、是非お教えいただきたいと思います。

○（事務局）　一時送金先の口座の名義人を国籍別で見たデータによると、今年の上半期は中国人が一番多く５４．５％。次いで多いのは日本人で約３２％ということです。

また、不正送金後にどうやって現金化しているかということについては、６割方は出し子が現金で出金するというもので、その他は数は減ってまいります。資金移動業者を介して国外送金するとか、さまざま、はっきり判明しないというものもございますけれども、数は圧倒的に出し子による現金出金が一番多いです。

○（前田委員長）　先ほどの局長の話にもありましたけれども、犯罪捜査だ

けではなくて被害防止についても、シーサートの活動につながり、官民連携や、ある種、官官連携というような問題にもつながり、非常に大事なポイントだと思います。

○（則房委員）　　２０２０年までに全ての企業でシーサートを持ったほうがよいという話はありますが、個々の企業でシーサートを持っても、その実力はあまり出ず、やはり攻撃を受けたらやられるだけという話にもなります。非常にレベルの高い中核のようなシーサートが、他の企業のシーサートを取りまとめたり、リアルタイムでの情報交換を行なったりという、対応プロセスが必要なのではないかという話になるのですが、こうしたシーサート間連携など有効に機能させる方策について日本シーサート協議会でどのような見解を持たれているのでしょうか。

○（寺田委員）　　シーサート協議会としては、国内各所にシーサートが３，０００チームできたときを想定し、連携できる運営体制の整備を進めています。分野を全般的にカバーしていくこと、基礎体力をサポートしていくことが役割であると考えています。このシーサートの運営体制基盤の上に、分野毎の分析センター、例えばテレコム・アイザックや金融アイザックといった組織が階層化されることで、多角的に良い協力関係ができるのではないかと考えています。中核的な役割に関しては分野毎の分析センターやＪＣ３もありますので、これらの組織に取りまとめていただきつつ、シーサートの運営体制基盤として機能するよう各シーサートの基礎体力を上げるところに力を入れていこうと考えています。

○（則房委員）　　２０２０年までに対策が間に合うように、どこか中核として頑張ってくれるところが出て手を挙げてくれるとよいという話もあったりしますので、この点はディスカッションのポイントであると思います。

○（桑子委員）　　本日のお話を伺っていましてインターネットバンキングの不正送金事犯は、実態として起きている問題の被害防止対策という観点で非常に重要であると思います。そういった観点からすると、本来、今年度のメンバーの中に銀行業界の方も参加すべきではないかなと感じた次第です。銀行業界がしっかり対応することがまずは一般の国民にとっても効果が大きいと感じております。

○（前田委員長）　　今回はサイバー犯罪捜査一般を念頭に置きつつ、犯罪捜査だけでなく、予防やオリンピック対応で、広めに官民連携という話になると、官同士のつながりも見えてくると思います。銀行業界は入れない方向で出発していますが、今の御発言は、重要な御指摘と踏まえて進めていきたいと思います。

○（事務局）　　御指摘はごもっともなところだと思うのですけれども、前田先生からもお話がありましたように、インターネットバンキングに係る不正送金事犯というのは、一番わかりやすいサイバー犯罪の例ということで御説明させていただいております。インターネットバンキングの関係は、警察としても金融機関と直接、対策についてお願いをしたり、あるいはＪＣ３の場でいろいろな情報共有をして対策を検討しております。総合セキュリティ対策会議ではインターネットバンキングの不正送金事犯に固有の問題ということではなく、もう少し広い観点から御検討いただきたいということでございます。

○（前田委員長）　　今日は、警察庁、警視庁、民間からはシーサートということで、まず、現状の認識を共有していただくということで御発表いただき、かなり熱心な御質問を出していただきました。こういう方向で次回以降も、ＪＣ３、テレコム・アイザック等に御発表いただく場面もございますので、それらを踏まえて議論を深めてまいりたいと思います。

９．閉会