平成 28 年 1 月 27 日

平成２７年度総合セキュリティ対策会議（第２回）
発言要旨

１．開会

２．ＮＣＦＴＡ・ＪＣ３型官民連携の状況について

【委員から、ＮＣＦＴＡ・ＪＣ３型官民連携の状況について発表】

３．質疑応答

○（佐々木委員）　ＪＣ３の取組については、非常に楽しみにしております。今後、早い段階でサクセスストーリーができると民間や、技術畑からの参加が進むと思いますが、どの程度成果が出た段階で打ち出していくのかについてお聞かせ願えればと思います。

○（坂委員）　ＪＣ３内ではかなり具体的な事例についての情報共有を行ったり、あるいは新たなオペレーションの可否等、様々な検討を行っております。ある意味ではトライアル・アンド・エラーではありますが、こうした取組の中で成果を出していければ良いと思っております。また、ＪＣ３ならではの情報、あるいは情報共有ということについては、様々な犯行に対して、先制的に対応していくことができればと思います。脅威、攻撃者の組織の像を捉える、あるいは彼らの行動パターンを把握することによって、予測しながら対応していくことができれば大変良い思っております。

○（前田委員長）　昨年１１月、アダルト広告宣伝サイトの一斉取締りにＪＣ３が貢献したことが各社において報道されたとのことですが、大々的に扱われたという意識がありませんでした。佐々木委員がおっしゃったように、ＪＣ３が活躍しているということを積極的に広報していくという意思は本件についてはあまりなかったのでしょうか。

○（坂委員）　本件は警察庁で広報した事案なので詳細は承知しておりませんが、資料のとおり報道はされております。これが難しいところで、ＮＣＦＴＡも非常に大きな事案について関与して実績を上げているのですが、実は

ＮＣＦＴＡが関与したという報道は、ほとんどありません。大体、ＦＢＩが実施したという報道ですが、告訴された場所等からＮＣＦＴＡが関与しているのではないかということは推察できます。内部では情報共有されているのですが、いかに外部に打ち出していくかということが難しいところでございます。この点、いろいろとお知恵をいただきながら今後もやっていきたいと思っております。

○（種谷局長）　本事件については茨城県警が中心となって取締りを行ったのですが、検挙後の会見で、ＪＣ３との連携については示しました。内容は、非常に悪質なアダルト広告の摘発でしたが、マスコミにＪＣ３との連携による初の取締りであるということの意義を上手く伝えられなかったところはあったのかも知れません。

○（佐藤委員）　ＪＣ３で、サイバー空間の脅威への対処経験を集約・分析した情報の具体例やイメージをお教えいただけますでしょうか。

○（坂委員）　例えば様々な攻撃元のＩＰアドレス等は共有されています。一方、攻撃者像の把握については、横串を刺してどういった手法で攻撃してきているのか、あるいはマルウェアを作成する人から出し子、送金者までいるわけですが、このそれぞれのフェーズで横串を刺して、特徴別に分析をして個別の活動を推察するとか、攻撃者をいかに把握して、そこに迫るかということに向けた情報共有や分析を行っております。

○（佐藤委員）　会員の中でそのような情報を、閉じた形で共有をされているということでしょうか。

○（坂委員）　会員の中といいますか、正にＮＣＦＴＡもそうなのですが、Face to Face で、当該テーマについて知見を持っていて、ともに分析できる方々の中で共有していく形で取組を進めております。

○（佐藤委員）　Telecom-ISAC Japan では、手法についてはある程度はわかるのですが、手口についてはなかなか集約できていないので、一般に公開されている情報等があれば是非参考にしたいと思った次第です。

○（坂委員）　情報発信をしていきたいと思うところで、委員の皆様にも対外的な情報発信をしっかりとするべきと御指摘をいただいており、現時点で具体的な情報を発信できる段階にはなっておりませんが、検討を進めていき

たいと考えております。

４．捜査関係事項照会等へのヤフー株式会社の対応について

【委員から、捜査関係事項照会等へのヤフー株式会社の対応について発表】

５．質疑応答

○（若江委員）　電子化というのは具体的にどのようなものをイメージしているのかもう少し詳しく教えていただきたいと思います。また、捜査関係事項照会で対応するものと令状が必要なもので分けるというのは、御社ではどのように分けているのかということと、ヤフー社のどのレベルで判断されているのかという点について教えてください。

○（別所委員）　後段の御質問については、私どもは電気通信事業をやっておりますので、電気通信事業法が定めている通信の秘密を守る義務があります。通信の秘密に該当するものについて言うと、捜査関係事項照会書ではなくて、違法性阻却事由が必要となり、裁判所からの令状をお示しいただいて開示しているということです。線引きが難しい場合は、法務部門で的確に判断をして回答させていただいております。ごく例外的に捜査関係事項照会書や令状では回答できないけれども、メールの中身が必要になるケースというのがあって、それは緊急避難に該当する特殊な例です。緊急避難についても違法性阻却事由を満たしているかどうかを法務部門として判断した上で対応しているというのが現状になります。前半の御質問で、どのようなシステムを念頭に置いているかという点については、私どものイメージどおりに構築していただくというよりも、双方ですり合わせをしていく必要があると思います。捜査関係機関の方々がどういうフォーマット、あるいはどういう画面であれば入力しやすいのか、あるいは連絡を受けたこちらとしてどういうものであれば、結果を送信しやすいのかという観点があると思っております。インターフェースをどう設計するかは、一方的に決められるものではないので、実務に照らして適切なものにしていっていただきたいと思います。

○（林委員）　通信の秘密に関連して伺いたいのですが、照会件数の多さに驚いたと同時に、通信傍受法等の令状発付件数は国会報告と公表がなされて

いますので、それとの対比でも余りにも差があるので驚きました。その上で御質問したいのですが、照会件数のうち、通信の秘密に関連することは多いと思うのですが、差押え対象となったものは、それほど多くない。今まで通信の秘密の解釈を教わってきた者からすると、通信の秘密には、狭義の「通信の秘密」と「他人の秘密」という概念と法律には両方あるのですけれども、「他人の秘密」の範囲を非常に狭くとって、ほとんど「通信の秘密」に入るのだという解釈をしてきたはずなので、ここのギャップに私は驚いたわけです。通信が存在したかどうかも含めて通信の秘密とされているのですが、ヤフー社の運用解釈では、その解釈を少し緩やかにされているのでしょうか。

○(別所委員)　御回答するには典型例をお話しするのがいいと思いますが、オークション等､照会で回答しているものはヤフーＩＤを付していますので、そのＩＤの保有者は誰かという照会になります。

○（林委員）　加入者情報ということですね。

○（別所委員）　そうです。

○（桑子委員）　照会件数、差押え件数とも非常に多いと感じたところでして、通信業界として考えたときには、ヤフー社を除くと大手数社ぐらいがこうした話についていけるレベルなのかなと考えております｡照会件数１万８，０００、差押え３００という年間件数に対して、実際に警察からの照会に対する回答に要する時間は平均的にどれくらいかかるのでしょうか。また、１００％回答できることはないと思いますが、実際にどのぐらい回答できているのか教えてください。また、電子化のメリットとして都道府県警察が相互に捜査状況を把握することが容易になるとありましたが、通信の秘密に関する案件まで相互にというのは実際のところはあり得ない話かなと思っていますが、具体的にはどのようなものを相互に把握できるものとしてイメージをされているのか教えてください。

○（別所委員）　照会に要する時間については手元にデータがないので正確にお答えすることはできません。数年前に直接見ていたときですと、１週間程度の時間はかかっていました。物によって非常にデータの量が多いと、そのコンピュータから出力される時間が１日や２日かかるケースもありますので、対応人数を調整しても、やはり数日かかっております。物理的に人を増

やせば、もう少し早くなるかもしれませんが、こうした業務で扱う情報は秘密に属するものなので、限定した人員でセキュリティを高めた部屋の中で対応しています。どのぐらい回答できないかについても手元に資料がないのですが、回答できていないものはほとんどないと思います。ただ、一部データがないものもございます。２番目の質問の捜査の相互連携について想定していますのは、捜査関係事項照会で来ているものなので、令状ということは特に想定して申し上げていないのですけれども、いろいろなところでいろいろな事件が起きて、同じ犯人の被害者が全国にばらばらに所在しているので、各都道府県警察が別々に動いた結果、照会内容が重なっていることがあります。そういうものがもう少し早くわかるといいのではないかということです。

○（片山委員）　弊社の場合を御紹介させていただくことも御参考であると思いますが、我々も基本的に別所委員のプレゼンとほとんど同じ実態です。まず、我々の場合は全世界で大体年間７万件の照会がございます。Ｗｅｂサイトに公表していますが、半年ずつで公開しており、ここ数年、大体半年で３万５，０００件とか３万件ぐらいなので、単純計算で７万件でございます。日本だけですと約１，０００件でございます。今回、私の本社の同僚に聞いたところ、郵便で照会していることについて、そもそも郵便で照会しているという質問があまりわかってもらえなかったことからも、メールで照会するのが普通なのだろうと実感いたしました。また、先ほど別所委員がおっしゃっていたように、照会の対象となるのはあくまでも登録者情報でございまして、我々の場合はアウトルックドットコムとかホットメールドットコムというメールアドレスがあり、名前と登録した国、ＩＰアドレス等が登録されております。そのアドレスで有料のサービスに加入している場合もありますので、クレジットカード情報を登録していることもございます。なお、グローバルでいろいろ見ると、もともとアドレスというのは、英語となります。日本の警察からの照会文書には、片仮名もつけられており、振り仮名が振ってありますが、基本的には片仮名の情報は必要ございません。別所委員のおっしゃっていたデジタル化とグローバル化の動きは全世界で止まらないと思います。デジタルが基本ということで考えたとき、捜査関係事項照会書で回答できるのは、登録者情報であって、令状が必要となるコンテンツ云々というのは別

の話です。昨年１月７日にフランスの記者が殺されたテロ事件がありましたが、テロリストが弊社のアカウントを使っていたようで、フランスの当局からアメリカの当局にしかるべき手続で情報開示の要請があり該当する情報を数時間以内に返しました。基本的に別所委員のおっしゃっていたことは、ＷｉｎＷｉｎというか、皆さんが助かると思います。現在、郵便で実際送っていただいて、簡易書留で返しておりますが、大体１通当たり５００円、これは警察で御負担されており､弊社の場合で言えば１，０００件なので５０万円の費用がかけられていることになります。繰り返しですが、デジタル化、グローバル化の時代は止まることはありませんので、別所委員の考えには賛成でございます。

○（事務局）　　我々の考えを少し御説明したいと思います。まず、別所委員もおっしゃったようにサイバー犯罪の中で、この手の照会は欠かせないもので、今後も増えることはあっても減ることはないと考えます。それらに効率的に対処していくことは捜査機関にとって負担を軽減するという意味もありますし、当然、警察から照会を受ける事業者の負担軽減ということにもなるだろうと思っておりますので、是非積極的に考えていきたいと思っております。ただし、当然、令状に基づく差押えは捜査関係事項照会と別に考えなければならず、法制的な手当て等が必要なのかどうか、慎重に検討する必要があると思います。また、別所委員が強調されたデータの活用・分析の話についても、やはり慎重に検討する必要があると思っております。捜査関係事項照会について紙でのやりとりをデータ化するということ自体はあまり法制的な問題はないと思いますが、それを蓄積して別途活用するということについては慎重な検討が必要だと思っております。また、実際、捜査の必要性ということから言っても、仮に蓄積したものが手元にあったとしても、やはり当該事件について改めて照会するということが必要になると思っております。

○（種谷局長）　　大変なお仕事をしていただいていることに対して心から感謝を申し上げたいと思います。サイバー犯罪だけではなく、強行犯の捜査でも照会を抜きにして捜査はできません。そういう意味では、サイバー犯罪だけではなく捜査第一課も捜査第二課もいろいろな形で照会をしております。別所委員のお話について、総論としては大賛成だと思いますが、具体的なシ

ステムの構築についてという各論になると、実は乗り越えなければならない問題が多々あると思います。もちろん法律的な問題もありますが、フォーマットを作って単に打ち込む形で果たしていいのだろうかという問題もあります。捜査関係事項照会も刑事訴訟法に基づいた権限でありまして、個々の捜査員が自分の判断のみでできるものではなくて、部内決裁を経る必要があります。決裁権者等は、組織として定められており、原則として所属長の決裁をとらなければなりません。こういったことについて、後で検証ができるようにしなければいけないという問題もありますし、また、いかなる事業者、ＩＳＰ等と専用回線を使ってやりとりするのか、また、インターネットをそのまま使うとすれば、それは非常に安全性に問題があるのでＶＰＮを構築するのかとかといったことを考えると、予算が必要となり厳しい財政状況の中でその予算をどう確保するかという問題もございます。このように、乗り越えなければならない問題は多々あるのだろうと思います。

別所委員から中長期的な検討というお話がありましたように、必要性は非常に感じておりますので、実現に向けて、数年かけて検討を重ねていくべき事業であると考えております。

○（別所委員）　難易度が高いものだというのはよくわかっておりますので、中長期的にフレームワークをつくっていただき、前向きに進めていただければと思っております。現在の捜査関係事項照会は、動的ではなくて静的なデータですけれども、今後は動的なデータも捜査に必要になってくるのではないかと思っております。そうしたものを捜査に活用する時代が早晩来ると思っていますので、電子化も是非実現していただければありがたいと考えております。

○（前田委員長）　電子化に関して中野目委員、星委員、一言あればお願いいたします。

○（中野目委員）　電子化に関しては、裁判所が発付した令状であるということが正確に確認できるようなシステムであればよいと思います。

○（前田委員長）　令状を要しないような照会であれば、その照会したものを蓄積して、それを分析するというようなことに関してはいかがですか。

○（中野目委員）　それはヤフー社で行われるのか、それとも警察で行われ

るという意味のどちらでしょうか。

○（前田委員長）　システムを警察が組むかヤフー社が組むかで違ってくるということでしょうか。

○（中野目委員）　はい。

○（星委員）　蓄積したデータの活用ということは全体像を見えやすくしますので、ＪＣ３の活動も正にそういう形でやっているのだと思います。他方、個別の事件について令状が出て、その個別の事件に使うためにデータを得るということが基本形になっている中で、事件の枠を超えてどこまで使っていけるのかということについての検討は、今後必要になってくると思います。

○（前田委員長）　ヤフー社からの提案は非常に重要で、局長がおっしゃったとおりあまり急ぎ過ぎず、ただ前向きに受けとめていただいて、議論を深めていくということにはなろうかと思います。今後ともぜひよろしくお願いしたいと思います。

６．警察機関との協調による Telecom-ISAC Japan の活動について

【委員から、警察機関との協調による Telecom-ISAC Japan の活動について発表】

７．質疑応答

○（種谷局長）　今回の総合セキュリティ対策会議の目玉であります犯罪捜査と被害防止対策の官民連携ということで、捜査と被害防止対策を車の両輪とし、捜査の過程で得た情報を活用して、官民協力によって被害の防止を図るということを重視していくべきだと考えております。警視庁においても、被害拡大防止に際して警視庁のビラも一緒に配って、警視庁にも問合せが来るように措置するなどいろいろ取り組みましたが、基本的に大変手間のかかる御協力をいただいたことに感謝しております。今後も被害拡大防止に力点を置いていきたいと思っております。中継サーバの事件も３回にわたって取締りを行い被疑者を検挙することができました。正に犯罪捜査と同時に被害防止対策もできたということで成果が上がったものでありました。警察としては民間の方々の御協力を得ながら、被疑者が検挙できなくても、様々な被

害防止対策を行っていることについて国民の皆様にもよく理解をしていただくためにＰＲをしていくべきであると強く感じております。その際に、効果分析が必要であり、例えばネットバンキングの不正送金の被害防止について試算できないかなど検討しております。アバウトな数字になるとは思いますが、世間や協力いただいたＩＳＰの皆様に御提示できるようになれば、協力していただいたことによる社会貢献の大きさを御認識いただけると思います。

○（事務局）　警察機関との連携に関する御要望に関する部分について幾つかコメントさせていただければと思います。まず、１つ目ですが、事前協議は、これはもちろん事案ごとの事情はありますが、可能な範囲で今後も時間的に十分余裕を持って御相談させていただきたいと思っております。役割分担についても、事前の相談の中でやっていきたいと思っております。結局、ウイルスに感染している端末の利用者の連絡先を特定して直接働きかけることは、ＩＳＰ事業者にしかできない部分でありますので、是非引き続き御協力をお願いいたします。その中で問い合わせの窓口や、広報の方法等、警察としても工夫をして、あるいは御相談しながら進めていきたいと思っております。以前の被害拡大防止措置の際は総務省にもお願いして、総務省のホームページに警察との連携を掲載していただいております。今後も警察と連名の資料を作成することや、あるいは警察の広報資料を一緒に入れるといった様々な工夫をしていきたいと思っております。また、問題の原因をつくった事業者への対応についてはケース・バイ・ケースであると考えております。インターネットバンキングについていえば、例えばGame Over Zeusは、不正プログラムの機能から考えて必ずしも金融機関だけが受益者とは言えないと思っております。警察としては、もちろん金融機関に対して直接、あるいはＪＣ３等の場を通じてセキュリティ対策についての要望等を行っており、引き続き働き掛けを行っていきたいと思っております。さらに、ＩＳＰ事業者へのお願いとしまして、インターネット接続サービスは今や社会のインフラとなったサービスを提供している事業者として、一定の社会的責任はあると思っておりますので、是非引き続き連携させていただければありがたいと思っております。最後に情報共有については、フォローが必ずしも十分できず、我々としても反省をしているところであります。今後は是非フィードバック

等をできるように考えていきたいと思っております。また、手口等の情報については捜査情報に直結する場合もあって、なかなか難しいこともあるとは思いますが、逆にこういう情報があれば、こういう自主的な対応が可能であるということを、御相談させていただければ、何らか提供できるものもあると考えております。これまで取り組んでいただいたことも、今後同じようなオペレーションをどう行っていけばいいか、あるいはフィードバックをどう行うか、どういう効果が出たかといったところも、この総合セキュリティ対策会議とは別の実務的な場を設けて御相談させていただければと思っております。

○（小屋委員）　Telecom-ISAC として御発表いただき、課題等を挙げていただいていると思うのですが、ＩＳＰという立場でいろいろな捜査協力をされるにあたって課題等があればお聞かせ願います。

○（佐藤委員）　別所委員からもあったとおり、捜査協力については煩雑で負担になっているという話は聞きます。特に携帯電話事業者は固定系に比べて、件数が多く、また、実はＩＳＰもＭＶＮＯのサービスを提供しており、対応件数は増えている現状であると思います。ヤフー社の御提案のようにデータを活用する仕組みにしないとサイクルが回らない現実が起きると危惧している話は聞きます。

○（小屋委員）　もう一点、意見として例えばヤフー社であれば、６人の工数を割いて､人件費だけで４，０００万以上の金額を拠出して捜査協力されていると思いますが、これからＩｏＴ社会になって小さな企業が多くの情報を持つようになって、それらの企業に照会をかけられると、人件費をあまりかけられず、結果としては捜査が進みにくくなってしまうと思います。この観点からも別所委員、佐藤委員がおっしゃっていた共有の仕組みについては、早急に整備していく必要があると思います。

○（則房委員）　小屋委員の御指摘は､僕も同じような印象を持っています。ＩＳＰは基本的に自分の事業のために設備に投資をしてきたという経緯もあって、情報を保管するためのシステムを追加しないといけなくなってきたときに、動きにくい部分がある気がします。大規模なＩＳＰさえそうではないかなと思うので、うまく動くように全体的な費用面、人材の点で検討すべき

ことがあるのではないかという気がします。

○（前田委員長）　今日の話の中でＪＣ３の具体的な成果について、難しい問題がありつつも、もっと宣伝していくべきであるということがはっきり出てきました。また、Telecom-ISAC 等の協力によって検挙につながったということは非常に重要だと思います。サイバーの問題は、攻撃から防ぐことしかできない、捕まえることができないだろうという何となくの意見があるのですが、そんなことはないと思います。ただ、そのためには官民連携が非常に重要であって御指摘のように、コストをＩＳＰに過大にかけていくということは問題だと思います。コストを軽くするために電子化することも大事である一方、どう合理的に分担していくかを考える必要もあると思います。

コストのかからないものとして、依頼後のフォローはやはり大切だと思います。他方、官民で信頼感が高まってはいますが、結果について対外的に出すべきではない情報を提供すれば、そこからまた情報が流出する可能性があることもまた事実だと思いますので、慎重に行う必要はあると思います。官民連携について、いろいろな考えがあると思いますが、協力することのメリットを考えて前向きなベクトルを意識していただくことは重要だと感じております。

○（種谷局長）　佐藤委員に質問ですが、警察に協力することについて経営層の理解を得ることの難しさについて言及がありましたが、確かにその点、難しい面があると思います。担当者は協力することの重要性を理解していても、経営層の方が、警察への協力の理由について、ＩＳＰの社会的責務というだけの説明をされてもなかなか御納得いただけないところもあると思います。そこで、感謝の気持ちをどう形にしたら最も経営層の方が理解いただけるかについて、予算的な制約はございますので、成果等の情報の形で謝意を表明することも一案としてあると思います。その点、具体的に何かアイディアがあれば教えていただきたいと思います。

○（佐藤委員）　ＩＳＰとしての社会的責任は当然痛感しております。ただ、現実として、ＩＳＰの契約者一人当たり収入はごく少額であるという状況があります。それに対し、注意喚起に多額のコストがかかっております。このような状況下で、警察からの依頼が次から次へと来てしまうと経営層からす

れば、警察はそういう経営環境を理解しているのかという考えには当然なるのが現実だと思います。社会的意義を加味してもなお、商売にならないことにコストを負担するという現実をどう切り崩していくのかが重要だと思います。ＩＳＰは、Telecom-ISAC に参画する一方で完全にビジネス競合しています。情報共有する内容は、正にその会社の競争力の源泉になっています。しかし、それらの情報を集約して対応していくために人対人で対応して理解しあっているのが現実です。経営層に同じ考えを持ってもらえるような環境ができれば、一番いいと思いますが、現実はそうはなっておりません。やはり社会的使命を経営層に理解してもらう取組があればよいのと、警察も感謝しているということを理解してもらう武器をいただければありがたいと思います。

○（前田委員長）　まだまだ御議論いただきたい面があるのですが、次回もこの延長として、具体的な核の部分は同じことについて、海外の連携の話などを御紹介いただくということを伺っていますので、今日のところはこのくらいにしたいと思います。

○（片山委員）　最後に、もう一度クラリファイさせていただきたいのですが、令状を必要とするのはＩＰアドレスをいつ使ったなどの履歴で、その点は全世界共通だと思います。今回はあくまでも登録者情報が必要になったときの手続です。今後、グローバルの事例を含めいろいろお話しすることもできますので、引き続き御協力させていただければと思っております。

８．　閉会