平成２３年度総合セキュリティ対策会議（第５回）

平成２３年１２月２０日

発言要旨

１．開会

２.サイバー空間の脅威に対する警察の取組

【事務局より、資料に基づき説明】

○委員からの発言はなし。

３．情報通信技術の悪用等による違法・有害情報の氾濫に対する警察の取組

（1） 児童ポルノ画像流通・閲覧防止対策

（2） 全国協働捜査方式の実施

（3） 出会い系サイト・コミュニティサイト対策

【事務局より、資料に基づき説明】

○委員：出会い系サイトとコミュニティサイトの定義の違いについてそれぞれ具体例を挙げて教えていただきたい。

○事務局：最近急速に普及しているゲームサイトや、サイト内で共通の自己のプロフィール等を掲載し、仲間を増やしていくようなサイト等をコミュニティサイトと呼んでおります。いずれのサイトについても、現在、児童の被害を防止するための様々な対策がとられているところです。

出会い系サイトについては、検挙件数でみますと、出会い系サイトにおける性的行為等の誘いかけなどの禁止誘引行為の動向等をみましても、かつて最も深刻であった時期よりはかなり改善されております。

ただし、いわゆるレンタル掲示板等を無料で借りて、個人が無届けで出会い系サイトを開設することが可能であり、そういった無届けの出会い系サイトにおいて事件が発生している状況があります。無届けでの出会い系サイト開設は法律違反でありますので、こうしたサイトに対する検挙等に力を入れております。

○委員：最近では出会い系サイトにおいて、様々な詐欺事件が発生しています。出会い系サイトと言ってしまうと、サイトを利用して性的な行為が目的で児童と出会うことが問題であるというイメージを抱かせるのですが、どうも最近ではそれ以外が問題となっているケースが多いという気がします。ならば、新聞やマスコミを活用して広報する際に、コミュニティサイト、出会い系サイトというネーミングでカテゴライズするのではなく、これと異なる名称を用いる、もう少し細かく分類した表現とするなど適切なネーミングをした方が名称現実に起きている犯罪や不正な行為の実態と適合し、効果的なのではないかと考えております。

○事務局：いわゆるメール交換サイトと私どもは呼んでおりますが、出会い系サイトも含めて、メール交換サービスを提供するタイプのサイトにおける詐欺事案等が、相談ベースでも相当増えてきているということについて、認識をしております。そもそも出会い系サイトという言葉を私どもが使うようになったのは、以前は、詐欺事案よりもいわゆるピンクサイトにおける児童の犯罪被害が非常に多かったという現状を踏まえたためです。したがって、法律で、出会い系サイトという男女の交際を目的としたメール交換サイトに限り、そうしたサイトを利用して一定の児童に対して性交等や現金を示すなどして交際の相手方となるように誘うなどの行為を規制することとしたのです。したがって、出会い系サイト規制法の目的は、まさしく児童の被害防止ということです。

　メール交換サイトにおける詐欺については、刑法の詐欺罪の適用が考えられますが、これに関する御指摘については、私ども今後、真摯に受け止め研究していく必要があると思っております。

○委員：出会い系サイトやコミュニティサイトにおける児童の性的被害が随分減っているということを実感しておりますが、一方で、こうしたサイトにおいて金銭被害を伴う事案が大変増えてきております。私どもでは、出会い系サイトをピンク系のものは出会い型、このほかに被害の手口に応じて同情型、利益誘引型等と分類しています。事案のうち増えている手口の一つとして、同情型で有名芸能人のマネージャーや本人を名乗ってメールのやり取りをするためにポイントを買わせるといったものがあります。また、やり取りの際

に、ポイント購入が必要となる都度課金制となっていることや、中には複雑な決済システムとなっていることから、なかなか解決できない場合があります。

もう一つ、被害の大きい手口が利益誘引型です。「悩み事の相談に乗るだけでお金をあげます。」とか、「身寄りのない私の遺産を使ってください。あなたに融資したいです。」というようなメールを送りつけ、さらに「お金を渡したいので会いましょう。会う場所を教えますから、そのためにメールを交換するためのポイントを買ってください。そのために 30 万円をまず入金してください。」などと送るわけです。通常だとこの時点で話がおかしいと思うかもしれませんが、メールの受信者は現金を手にしたいがために、どんどん現金をつぎ込んでしまい、1,000 万円以上の被害に遭ってしまうというようなケースもよくあります。このような場合、消費者は出会い系サイトであることを意識せず利用していることもあります。そういった現状について是非考えていただきたいと思っております。

また、先日全国の弁護士会の方々と一緒に、悪質出会い系サイト 110 番という電話相談を実施しましたので、その分析結果と問題点についても公表していこうと思っているところです。

○委員長：ゲームサイトがかなり普及してきていますが、こうしたサイトにおいても、金銭的な被害が起きているのでしょうか。

○委員：ゲームサイトにおける金銭的な被害も多く発生しております。代表的なものとしましては、ゲームの中では、役に立つ様々なツールやアイテム等をポイントで購入する仕組みとなっていますが、この際、カード決済となっている場合があります。ゲームによっては、そうしたアイテム等を購入することによって、ゲーム内で相手と対戦するときに優位になり、勝つことができるとか、さらに上位のステージで遊ぶことができるといったシステムになっているものがあり、そのために様々なアイテム等をお金で買うのです。親に内緒でアイテム等を買うために、親のカードを勝手に使い、決済してしまい、請求額が 10 万円以上になったといった事例はたくさんあります。

このほかには、ゲームサイトの中で違反行為をしたら強制退会となるといった規約があるようなのですが、本人は何をしたのか分からず自覚がないま

まに一方的に強制退会されてしまい、本人がせっかく購入したアイテム等が全部無駄になってしまったので、これを何とかしてほしいといった相談もあります。あとは、ゲームサイトの中で他人になりすました者に、これまで自分が買い貯めたアイテムを盗まれてしまうといった事例もあるようです。

４．金銭や個人情報の不正な入手等他の犯罪の手段として敢行されるサイバー犯罪の発生に対する警察の取組

(1)　不正アクセス対策

(2)　コンピュータ・ウイルスに関する罪を適用した取締り

【事務局より、資料に基づき説明】

○委員：ウイルス罪に関してですが、今、消費者トラブルの中で多い形態が、ワンクリックサイトと呼ばれるもので、動画ファイルを装ったファイルをクリックさせることにより、あるプログラムをダウンロードし、インストールしてしまうと、これにより代金を支払うまでパソコンのデスクトップに代金請求画面が貼り付いて動かせなくなってしまうという事例があります。これは、代金を払うまでパソコンを自由に操作させないという、半ば恐喝と等しい手口なのではないのかと思いますが、いくら電子消費者契約法上で、契約の無効が主張できるとしても、代金を支払うまでパソコンが使えない状況であると、消費者はやむなく代金を支払ってしまうということになりかねません。契約が有効であったとしても、そのような形で強制的に代金を回収することは自力救済禁止の法理にも反すると思います。これを民事的に解決しようと思っても、支払ってしまった代金を回収するのは困難です。代金を支払わない限りパソコンが使えないということは、現実的に消費者は不利な状況に追い込まれてしまうのです。

　ここで、動画ファイルを装って悪意のあるプログラムを、ダウンロードさせ、実行させてしまうような状況下に置く行為が、今回新設されたコンピュータ・ウイルスの供用罪に該当するのか否かについて検討していただきたいと思っております。もちろんケース・バイ・ケースで、ユーザがファイルを実行することで代金請求画面が表示されることを分かっていながらダウンロードしたのであれば、供用罪は成立しないと思いますが、有料であるという

ことは利用規約の細かいところに書いていても、代金を支払わないと代金請求画面が貼り付くといったことを利用規約に書いているサイトは見たことがないので、そうした点を考慮すると、供用罪は成立するのではないかと思うのです。

もし成立するのであれば、そのような手口で数多くの消費者被害を生んでいる悪質なサイトに対して、警察がコンピュータ・ウイルス供用罪が適用され得る旨を示しつつ、警告なりをしていくことで、かなり犯罪の予防につながるのではないかと思います。また、適用可能なのであれば、是非供用罪で検挙して、大々的に広報していただきたいと思います。

○委員：私どもへの相談の中で特に多いのがアダルトサイト関連で、代金請求画面が貼り付いてしまったというものです。意図してその画面を表示させたというもののみならず、クリックすると全く意図しないのに、アダルトサイトに誘導されてしまい、退会するための処理を行おうとしたところ、代金請求画面が貼り付いてしまうというものもあります。代金請求画面には、例えば、3日以内に払えば6万8,000円だが、これを過ぎると10万円になるなどと書いてあり、これにより金銭的被害が発生しておりますので、確かに御検討いただきたいところです。

○委員長：刑法第168条の2第1項の解釈としても、「その意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令」には十分当たり得ると思うので、今の御指摘の点については、是非検挙に向けて取り組んでいただくべきだと思います。

○委員：ウイルス関連の供用罪についてですが、最近、アプリケーションの操作をするログを取得するアプリケーションや、彼の居場所を把握するようなアプリケーション等が開発され話題となっておりますが、そういったアプリケーションは本当に悪意があって開発されたのか、それとも、そもそも開発者側はそうした行為をやってはいけないかもしれないということを知らなかったのかということについては、どうも後者である気がしています。今後、スマートフォンの普及により、アプリケーションの開発については、非常にビジネスとしてもホットあり、一発当てれば大成功できる可能性がある現状を踏まえますと、こういった行為をやると法律に抵触する可能性があるとい

うような啓発活動が今後重要であると思います。アプリケーション開発をする人については、様々な人に開かれ、参入できるようになっている部分は良いのですが、一方で、開発したアプリケーションを利用して、このような行為を行ったら法律に抵触する可能性があるという部分については、開発者側に対して何らかの情報提供があっても良いのではないかと思います。

○委員：今回、ウイルス作成罪ができたということは非常にすばらしいことだと思っているのですが、実際の検挙が現在までに２件にとどまっているというのは、数として若干少ないという気がしております。この理由に関して、検挙あるいは捜査をするに当たって何か大きな問題等が生じているためということであれば、どういったものがあるのかということを教えていただければと思います。

○事務局：１つには、通常の場合、被害者自身がどこからどうやって感染したのか分からないため、コンピュータ・ウイルスの感染ルートをたどることは非常に難しいということがあります。今回の検挙の事例のように、感染元が他の情報等から大体この辺だろうということが分かったときに、さらに捜査を進めて被疑者を検挙できる場合があるというわけであります。コンピュータ・ウイルスに感染している被害者の方々に関して情報をお持ちの事業者の方々との協力が今後、非常に大切になってくると思っております。

　コンピュータ・ウイルスについては、不正アクセスと同様に、おそらくは一般の利用者も事業者もコンピュータ・ウイルスの被害に遭ったときに警察に相談するという発想にあまりなっておられない場合が多いのではないかと思います。確かに、警察が相談を受理しても、どこでどうやって感染したか分からないものを全て検挙できるわけではありませんが、警察庁では、法施行の前から各都道府県警察本部や各警察署で相談を受理した際に対応ができるようなマニュアルを作成し、配付するなど、相談受理態勢を整えているところであります。また、先生方の御意見等を踏まえつつ、核心に迫ることができる情報を入手するためにどのような努力をすべきか、研究していきたいと思っております。

○委員：先ほどのコンピュータ・ウイルスについてですが、不正に代金を請求する場合にＧＩＦアニメがよく用いられると思うのですが、それは不正指令

電磁的記録の対象に入ってくるのでしょうか。クリックをすると一連の画像が次々に展開して、自動的に代金請求画面が現れるというＧＩＦファイルについては、プログラムとか、コンピュータ・ウイルスとはいえないように思うのですが、いかがでしょうか。

○委員長：コンピュータ・ウイルスの定義は、この刑法第168条の２に規定された文言の解釈ということになります。意図に反する動作をさせるべき不正な指令というのがプログラムでなければならないかどうかということについては、やはり、画像が貼り付いて動かなくなるというＧＩＦファイルを、その意図に反する動作をさせるべき不正な指令を与える電磁的記録とみる解釈は十分可能であると思います。ただ、現場で実際に適用し、検挙できるかどうかについては検討が必要であると思いますが。

　刑法上に規定されたコンピュータ・ウイルスは、一般的にイメージされるコンピュータ・ウイルスとは多少異なると思います。ただ、国民一般が安心してコンピュータを使えるようにするために設けたという立法目的を踏まえると、それが処罰範囲を不当に広げることになるかどうかというバランスを考えることは必要であると思います。もちろんこの場で結論は出せませんが、前向きに検討していただいたくべきだと思います。

○委員：問題が２つありまして、１つは解釈の問題です。どういうものをプログラムというのかということについては少し整理をして、明白にしておくべきかと思います。先ほど、他の委員のお話にあったようなケースでは、そもそもレジストリを書きかえてしまって、何回立ち上げてもＧＩＦファイルが自動的に作動しますので、これはプログラムといって間違いないと思います。もちろん、様々なパターンの仕組みがありますから、全部についてプログラムといえるかどうかは分かりませんが、一般的には、現在問題になっているトラブルになっているようなケースについては、不正指令電磁的記録に該当するのだろうと思っております。

　したがって、そうしたトラブルの原因となっているプログラムが、不正指令電磁的記録に該当する可能性があり、そうしたものの供用等の行為が犯罪になるということが広く認識されるとトラブルの件数はかなり減るのではないかと思います。

先ほどの委員長の御説明を踏まえますと、不正指令電磁的記録というものがかなり広いと感じています。やはり、これは間違いなく犯罪になるという適用範囲を幾つか分かりやすい例を示して、何らかの形で明白な基準を設けるなりする必要があると思います。もちろん、これは最終的には判例が示すこととなりますが、ある程度の具体例や基準が示されないと、かなり後からこれは犯罪であると言われる可能性等が出てくるかと思います。もう少し広く一般の国民が理解できるような形での啓蒙・啓発活動を通じて、情報提供をしていただければと思います。

○委員長：解釈については、やはりグレーな領域は存在しています。また、国民から見て、ここまで処罰するのはおかしいというものを処罰しては、やはりおかしいわけですよね。まず警察が捕まえる前に、マスコミ等の間でこういった問題が起こっているということを議論していくということも大事なことだと思います。

５．国の安全保障に影響を及ぼしかねないサイバー攻撃事案の発生に対する警察の取組

・　サイバーテロ・サイバーインテリジェンス対策

【事務局より、資料に基づき説明】

○委員：特にサイバーテロについては、おそらくなかなか抑止ということは困難であると思うのですが、一方でサイバーインテリジェンスに対する抑止については検討していく必要があると思います。

相手がいわゆる通常の泥棒ではないので、個々の企業が個別にしっかりとした対策を講じていくことはなかなか困難でありますし、さらに、被害が具体的でないだけに、費用対効果の観点から、企業における事業仕分等の対象になりかねないと思います。まずは、被害の実態把握を進めていただき、また抑止を図るための法律についても可能であれば検討してみてもいいかもしれません。民間がどこまでやっていいのか、また、警察と連携すればこういったことができるということを整理し、もう一歩踏み込んだ対策を考えていかないと、今後は対応できないという危機感を持っております。

○委員：標的型攻撃への対策としては、コンピュータ・ウイルスに感染し、実

行されてしまうことを前提に、たとえ実行されてしまったとしても被害が発生しないような環境や情報システム等を構築することが必要であると思います。特に国外からのサイバー攻撃という可能性を考えますと、攻撃そのものを抑止することは非常に困難であると思いますので、攻撃を受けてコンピュータ・ウイルスに感染したとしても、被害が発生しないような、感染に強いシステムを構築するという考え方が非常に重要になってくると考えます。したがって、警察庁の方でも何かしらそういったシステムの構築を企業等に促進させるような対応等をしていただければと考えております。

○委員：一般の方々や企業のセキュリティに対する関心度はまだまだ低いところがあるので、そうした部分をやはり少しずつでも引き上げていく必要があると思います。ウイルス対策ソフトの導入等各種対策を講じたとしても、決して万全ではないという意識を、個々人や個々の企業が持つことが必要だと思っています。これまで、不正アクセス禁止法の改正によるフィッシングの処罰化を強くお願いしてきておりますが、一部にはそこまでしなくてもというような考えをいまだにお持ちの方もいらっしゃるようです。この点につきましては、社会的な問題となっているサイバー空間の脅威に対する認識の違いが原因であると思います。非常に厳しい現状を踏まえていただき、是非様々な取組をしていただければと考えております。

○委員：警察庁はサイバーインテリジェンス情報共有ネットワークを、また、経済産業省はJ-SHIPを構築しているほか、総務省はTelecom-ISAC-JAPAN連携し、また防衛省も役務が伴う事業者に対して３か月以上のログ保存を行うことなどについての指針を出すなど、４省庁で対策をとっているかと思いますが、企業からすると４つの省庁にそれぞれ報告を上げなければならないので、省庁間での情報共有を進め、関係報告要領等について工夫していただければと思います。

　また、日本の多くの企業が海外のクラウドセンターにシステムを置いておりますが、そういった海外での犯罪に関連するデータの転送、移送の取扱いが非常にセンシティブであり、ヨーロッパ、特にドイツではこうしたデータの転送、移送等の取扱いには厳格です。ＩＴ犯罪に関連して申告をするときに、その情報の中に個人情報が含まれていたとしても責任に問われないとい

ったことが米国では検討されているようです。ログ情報の転送する際の個人情報の取扱いについて何かしらの指針等を出していただけると幸いです。

それから、海外ではサイバー演習を防衛部門でやっております。そうした海外機関との間や各省庁間において、ノウハウの共有についても考えていくと良いのではと思います。日本でも、アメリカのサイバーレンジのようなサイバー演習の方法も必要かと思います。

○委員：出会い系サイトについては、実際はそのほとんどがサイト名に出会い系サイトという名称を用いていないと思いますが、出会い系サイトという言葉が文字化されてしまうと子供たちは、私たちが注意しましても「そんなサイトは使ってない。」と言って返すので、私たちが子供たちに対し、気を付けるべきサイトを教示する際に表現する言葉がないのです。こうした点からは、出会い系サイトという名称を少し考えていただきたいと希望しております。

また、児童ポルノについては、子供たちが互いにわいせつなものを写し合って、これをばらまいているといった状況がありますが、このような行為は処罰の範囲ではないのでしょうか。

さらに、無線ＬＡＮについてですが、今、子供たちは昔と違ってあまり外で遊んでおらず、集合住宅周辺に集まって、家庭から漏れた電波を利用して通信ゲーム等で遊んでいるようですが、無線ＬＡＮの使い方を規制していただかないと、子供たちは、そうした無線ＬＡＮの不正利用をし放題という状況になりますので、この点につきまして検討していただきたいと思います。

○事務局：１点目についてですが、出会い系サイトについては、出会い系サイト規制法違反による被害はどれだけかということを必ず報告しなければならず、その際、法律の名称に基づき、出会い系サイトという名称を使って説明しております。近年では、コミュニティサイトにおける問題が大きいので、コミュニティサイトにおける被害がこれだけ広がっているということを強調し広報しております。ですから、御指摘のようなサイトにおける問題については、コミュニティサイトの問題ということで普及啓発を図っていただければと考えております。

また、２点目の児童ポルノについては、子供たちが互いにわいせつなものを写し合っても、結局、そこでできた写真等は児童ポルノであって、例えば

インターネット・ホットラインセンターで取扱う違法情報となり削除要請の対象ということになりますし、少年警察において、補導の対象にもなってくると思います。

さらに３点目の無線ＬＡＮの問題については、まさしく今年度の会議で取り上げているところですが、まだ完全には無線ＬＡＮの問題は消えてなくなっているわけではないと思います。これまで関係の皆様方からお話を伺う中で、昔に比べると問題となるようなアクセスポイントは大分減っているのではないかと感じております。技術的な進歩やそうした技術の普及によって、遠くないうちにかなり改善されるのではないかと思います。一方で、まだセキュリティ設定を適切に実施していない御家庭、企業等がある可能性がありますので、セキュリティ設定の必要性等に係る普及啓発活動は必要であると思っております。

○委員：接続しようとすれば、接続認証画面に切り替わり、パスワードを求められるなど暗号のかかったアクセスポイントがかなり増えております。ただ、暗号のかかっていないアクセスポイントが全くないわけではありませんので、やはりセキュリティ設定等に関する啓蒙活動を推進していく必要があると思っております。

○委員：１点目ですが、最近でも国防関連企業がサイバー攻撃に遭いましたが、これに関する報道を受けて、様々な政府機関から様々なことを聴取され、その対応が非常に大変であったと聞いております。政府内部での情報共有については、難しい部分もあるかとは思いますが、実施していただきたいと思います。

また、２点目ですが、技術開発の部分についても連携が必要であると思います。海外からのサイバー攻撃に対して逆探知するとか、そういうものを、例えば総務省、内閣官房等で研究を進めているかと思いますが、各省庁において開発された技術が、省庁間においてどの程度連携されているのでしょうか。もし、こうした連携が十分進んでいないのであれば、是非進めていただきたいと思います。

○生活安全局長：警察庁としては、サイバー空間の脅威に対して、警察庁や都道府県警察において各部門の枠を超えて連携し、また、政府関係機関におけ

る連携についても進めていき、社会全体の対処能力というものを強化するということが一番の目標であり、通達で指示したところであります。

これから、個々の取組を皆様方に御協力いただきながら進めていかなければならないと考えておりますが、全国警察を挙げて努力していきたいと思っておりますので、よろしくお願いいたします。

本日、出会い系サイトという呼称についての御指摘がありました。出会うことを目的としたサイト内においても詐欺等様々な形態の被害が発生していると思いますが、これらのサイトを全て出会い系サイトと呼ぶことは確かに適切ではないのかもしれません。法律に基づくサイトについて出会い系サイトと呼ぶことは、仕方ないかもしれませんが、事案の内容に応じて呼称を変えるなど対応していくことも必要かと思っておりますので、検討させていただきたいと思います。

警察庁の中でも、サイバー犯罪といっても、児童ポルノ事犯や生活経済事犯等それぞれ担当課が異なりますが、部門間で連携を図らなければ、対策を進めることはできません。また、特に政府機関における連携については、さらに進めていきたいと思っております。

以上