平成２３年度総合セキュリティ対策会議（第４回）
平成２３年１１月２日

１．開会

２．サイバー犯罪の抑止と事後追跡可能性について

【事務局より、サイバー犯罪の抑止と事後追跡可能性について説明】

○委員：未検挙件数のうち、事後追跡上の障害のうち「ログの保存なし」について、いわゆるＩＳＰの接続ログが保存されなかったケースは多くあるとは思えないので、恐らく掲示板への投稿者のログが保存されていないために、そこからプロバイダを特定できなかったケースが大部分を占めるのではないかと想像しますが、その点については、実際どうなのでしょうか。

また、検挙された事件のうち匿名化手段としてデータ通信カードが使用された件数については、平成 17 年から平成 22 年にかけて、大幅に増えておりますが、この部分に関しては、データ通信カードが匿名化手段として使われたとしても、最終的には検挙に至る件数はそれなりにあるという見方もできます。そうすると、従来の捜査手法により犯人が特定されているのではないかと思われます。それであれば、ログの保存がないことが事後追跡上の障害となり未検挙になっている件数が多いということについては、なぜ、従来の捜査手法で検挙できないのでしょうか。

○事務局：１点目についてですが、ログの保存がないということが障害となって未検挙であったものの内訳つきましては、当方での調査の結果、最も多いのがプロバイダ、次に被害サーバ、次にプロキシサーバ、そしてその他となっています。

また、２点目についてですが、ログの保存につきましては、今般、刑事訴訟法が改正され、事業者に対してログの保存の延長を依頼することが可能となります。私どもとしては、この法律の施行状況を注視しながら、今後の状況を踏まえつつ、検討していきたいと考えております。

○委員：実際に報告書としてまとめる際には、例えば、「正当なインターネット

ユーザー、事業者等に対して支障がないように、十分な配慮が必要だ。」というような断り書きは必要だと思います。特に制度化を目指すものについては、何らかの法的な義務が伴うものであれば、十分な配慮が必要だと思います。

さらに、現在もやっているとは思いますが、民間のセキュリティ専門チームとの連携強化等を含めて対応していくという方向が望ましいのではないかと思います。

○委員：事後追跡が可能にならないと、どうしても犯罪で訴追をする場合に証拠が得られませんので、その点の配慮は是非とも必要だと考えます。また、私も民間との協力体制については、不可欠だと考えております。

３．匿名化手段におけるサイバー犯罪対策等の今後の在り方について

(1) データ通信カード、無線ＬＡＮ

【事務局より、データ通信カード、無線ＬＡＮにおけるサイバー犯罪対策等の今後の在り方について説明】

○委員：事業者といたしましても、データ通信カードが様々な犯罪行為で利用され、事後追跡可能性の障害となっているということに関しまして、特に利用契約時等の本人確認の問題につきましては、今回の会議で御指摘をいただきまして、改めて重要な課題であることを認識いたしました。御指摘に対しましては、現在、事業者で情報を持ち寄り、関係業界からお話を伺いながら、現状を把握しつつ、議論を進めているところです。

○委員：ユーザーの意識を啓発、啓蒙していくといったところも重要だと思います。製品にセキュリティの設定がなされていても、ユーザーが暗号設定を解除してしまうというようなことや自分で覚えやすいように簡単なパスワードに変えてしまうといった行為を防ぐことができませんので、ユーザーにおいてセキュリティに対する意識を高めていただくような方策も必要であると考えております。

○委員：ログの保存がなかったことが事後追跡上の障害となり未検挙となった件数が非常に多いのに対し、一方、データ通信カードについては、本人確認をしていなくても基地局からの位置情報等を頼りに検挙ができるとなると、ログの保存がないということはサイバー犯罪の捜査において、そもそも入口

の部分で完全に可能性が閉ざされているということになるのではないのでしょうか。

例えば、ログの保存がなくても検挙に至ったサイバー犯罪の事案はあるのでしょうか。

仮に刑訴法改正によりログの保全要請で期間が延長されても、ログの保存自体を義務付けるものではないので、そうであればログの保存の義務付けを立法化することがサイバー犯罪の捜査には非常に重要ではないのかと思いますがいかがでしょうか。

○事務局：まず、１点目でログの保存がないと一切検挙ができないのかということにつきましては、捜査実務の観点からは、事案によっては、検挙できる場合もあり、全く絶無ではありません。ただ、警察の立場としては、当然、そのログといったものが基本的に残されることが望ましいということで、通信事業者に対して保存を依頼してきました。

今回の議論のテーマにつきましては､積極的に犯人側が匿名化工作を行い、それを盾にして訴追を逃れながら大量の犯罪を敢行しているという問題についてであり、より重要性緊急性等が高いため、その部分に焦点を絞っております。従いまして、今回の議論ではログの保存の問題については触れないこととしております。

（2）インターネットカフェ

【事務局より、インターネットカフェにおけるサイバー犯罪対策等の今後の在り方について説明】

○委員:正当にインターネットカフェを利用しようとする人が何らかの理由で、たまたま身分証明ができないというケースがあり得るのではないかと思います。最終的な報告書には、そうした者に対する配慮の部分もお願いできればと思います。

○委員長：立法作業においては、例えば、ウイルス作成罪等の規定について「正当な理由がない」場合という縛りをかけているように、いわゆるアンチウイルスソフトを作る会社の場合はどうするのかなど、様々な具体的な検討を行った上で、こういう場合は除くというような議論をして、構成要件等を固め

ていくわけです。インターネットカフェ対策についてもそういう点は十分考慮した上で、慎重に検討していくべきだと思います。

○委員：今、業界団体の加盟率が下がっている理由については、業界団体の会員になり、規約、ガイドライン等を守ることをしなくても、条例で厳しい行為規制がなされているため、加盟して、業界団体に入る意味がないと事業者が考えているからなのでしょうか。

○委員：業界団体への加盟率が減っている要因について説明いたします。

もともと、インターネットカフェは法的には２つの問題に直面しております。１つは、不正アクセス行為等のサイバー犯罪を敢行する際の匿名化の問題です。また、もう１つが、青少年の健全育成という点で、いわゆる風俗営業としての側面からの問題です。協会のガイドラインを作りまして、１つは匿名性という意味におきましては会員制を平成 20 年から義務付けましたが、まずは、これを嫌って脱退したところがかなり多かったわけです。この部分に関しましては、昨年、東京都条例が施行されたことによっても加盟率が上昇しなかったという状況があります。

また、もう一つの風俗営業としての側面から、ガイドラインでは不適切な使用を防ぐため、個室の見通しに関する規定等を設けるなどなかなか厳しい内容となっておりまして、インターネットネットカフェ事業者の中には協会に入ることで相当厳しい規制を受けてしまうということを嫌っているという側面がかなりあるのだろうと思います。従いまして、法制化に当たっては、匿名性にどう対処するかということと、さらにもう一つは風営法の側面を可能であれば取り込んで、健全なインターネットカフェの発展に資するような方向で取りまとめをしていただければと期待しております。

○委員：条例によって規制がなされていない東京以外の大都市に立地されていて、都心と同じような環境にあるインターネットカフェでも協会から脱退する業者が多いという実態があるのでしょうか。

○委員：確かに都市部におきましては、加盟率はかなり低いという実態になっています。

また、一点補足しますと、本人確認の制度化につきましては、システム上、会員制を採るということに繋がりますが、インターネットカフェが会員制を

採ることによって新しいビジネスが生まれる可能性が極めて高いと考えており、業界団体としては、むしろ前向きな姿勢で臨んでおります。

○委員：東京都だけではなくて、各地方でも条例があった方がよいという声はあるのでしょうか。

○委員：東京都条例ができた以上、できれば他の道府県においても同じようなルールが欲しいという声はあります。インターネットカフェ事業者の５割程度はフランチャイズチェーンで展開しておりますので、東京都の店舗だけが規制を受け、例えば神奈川県、埼玉県は規制を受けないということになりますと、不具合が生じてしまいますので、全国で同じルールをという声は大きいです。

（3）インターネット上の高度匿名化技術

【事務局より、インターネット上の高度匿名化技術に対するサイバー犯罪対策等の今後の在り方について説明】

○委員：基本的にここで使われている技術は、決して新しいものではなくて、かなり古い世代の暗号技術です。ですから、暗号の技術者から見ると、技術的に特に何がすばらしいということはありませんが、実際に、様々な民主化の動き等に関わる人々同士の通信によく使われている。

　暗号理論の世界のトップコンファレンスが、毎年アメリカ西海岸で開催されておりますが、この会議に、このインターネット上の高度匿名化技術を構築したリーダーが招かれて講演をしております。すなわち、暗号理論に基礎を置く情報セキュリティ分野では、世界のアカデミックなコミュニティの中でそれだけ高い評価を得ている取組として、非常にポジティブに捉えられている動きが、また確認されたという状況ではないかと思います。

　実際、そのリーダーも、自分たちの技術が利用されるシナリオというものには様々なものがあるということは認識をしておりますが、基本的には良いことに多く利用されているというようなことを強調しておりました。また、この技術に対して意見を持つ様々な人々と対話をする用意はあるということを話していたと記憶しております。もちろん、彼らは対話をするというだけで、その他の何かを保証しているわけではありませんが。

まとめますと、少なくとも現時点で、科学、学術等の観点から、その匿名化技術に携わっている人々の間で、この技術を利用禁止にするような動き、あるいは利用制限するための政策についてどうするかという考え方は基本的には話題に上ってこないということです。その場での質疑応答でも、この技術が悪用されたら大変であるので、それを防ぐためにはどうするのかということについては全く議論にも上らないという状況であったということです。

○委員長：この技術については、現時点で、普通の人でもかなり容易に使いこなせるソフトになっているということですね。

○委員：容易に使いこなすことができるソフトであるということと、この技術そのものとは、実は全く関係がありません。要はそのソフトウェアのインターフェースが使いやすいものであるかどうかというだけの話であります。誰かがインターフェースを使いやすくすれば、当然、使いやすくなる。ですから、もともとのこの匿名化技術、すなわちこの暗号技術自体がインターフェースを使いやすくしても使いにくいような技術であるかというと、それは違います。

さらに、おそらくは、日本人にとっては、使いやすさという点で最も影響する部分は、言語ではないかというのが私の個人的な印象です。日本人の一般ユーザーにとっては英語を自由に操るということは、一部の人を除くとハードルが高いと思います。基本的に、彼らの言語は英語ですので、その部分が少なからず影響しているのかもしれません。

４．サイバー犯罪の事後追跡可能性の保障について

【事務局より、サイバー犯罪の事後追跡可能性の保障について説明】

○委員：新しい穴としてモバイルＷｉ－Ｆｉルーターについては、今後主流になってくるのではないかと思います。そうすると、契約上はモバイルＷｉ－Ｆｉルーターの本人確認ができていても、要するに他人のモバイルＷｉ－Ｆｉルーターをただ乗りして通信を悪用するというケースというのが増えてくるのではないかなと思いますので、そういったところに詳しく言及してもいいのではないかと思います。

また、インターネット上の高度匿名化技術についてですが、現時点では悪

用された事例がないということですが、今後、少し注視していく必要があると感じています。何故かといいますと、利用者がクライアントソフトウェアをインストールしたところで自分がリレーサーバになってしまう点で、いわゆる匿名Ｐ２Ｐと言われるようなものに似た通信のネットワーク網を世界中で作ってしまうということなりかねず、これがずっと安全な状態を保つことができるという点が不明であるからです。

例えば、メッセージのやりとりだけの通信なのか、それとも直接システムにアクセスしてログインするような通信もこの技術を用いてできるのかどうかといった悪用のシナリオのようなものについて、考えられるのかというのを考えてみると、もう少し理解でき、深い議論ができるのではないかと思っています。

○委員長：モバイルＷｉ－Ｆｉルーターについては、ものすごい勢いで普及していきますし、ここ数年でというより、もっと短いタイムスパンで動いていきますので、逆に言うと、それもある程度予測した形での報告書でないと意味がなくなる。また、高度の匿名化技術に関しても、将来の悪用のシナリオ等を含めたシミュレーションを踏まえて提言するというのも、できる範囲でやっていかなければいけないと思います。

○委員：モバイルＷｉ－Ｆｉルーターにつきましては、位置情報のＷｉ－Ｆｉポイントのデータベース、いわゆるプラットフォームは事業者が作っているわけですね。Ｗｉ－Ｆｉのアクセスポイントの住所等が分かるシステムというものは、実はプラットフォーマー側が整備し、情報を持っている可能性があるわけですので、そういったところにも捜査要請をしていく。若しくは、彼らが可能なのであれば、そういったデータベースを我が国において構築してもらう。そうしたことも検討してみてもいいのかもしれません。これは、いわゆるＷｉ－Ｆｉの位置ポイントのデータベースだけではなくて、スマートフォンではもうやっているので、３Ｇ回線についても導入して、犯罪捜査に活用していくという観点もあるのではないでしょうか。

インターネット上の高度匿名化技術については、今、日本でどのくらい使われているかよく分からない状況です。ですから、例えばＷｅｂメール等にこの技術における最終ノードからのアクセスがどの程度あるのか、統計的な

データというのを拾っておいて、今後の犯罪への悪用の予測等について考えてもいいのではないかと思いました。

○委員：将来的に新しい通信手段・環境が出現してくることを想定して、事前に事後追跡可能性について検討することについては良いことであると思いますが、必ずしも新しい通信手段、環境だけが問題ではないと思っております。通信手段自体は従前からあるのだけれども、例えば、プロバイダが新しい顧客を獲得する、あるいは携帯の事業者が、顧客を獲得するために無料でお試し期間を設けて、端末を提供する機会が非常に多いのですが、その無料の利用期間中も事後追跡を可能とするよう本人確認を実施していただくことも必要だと思っています。

○委員：高度匿名化技術については、これは政治的な自由という点から重要な技術であるという御指摘があったわけですが、他方でそれが犯罪使われてしまったらどうするのかという問題があります。特に、昨今、様々な所に標的型という形での攻撃が仕掛けられているというニュースがありますが、そうした犯罪に使用されるという側面に対してどう対処するのかということについて、真剣に考えなければならないだろうと思います。

　リレーサーバの仕組みがあり、一国内だけでは、有効な対処ができないという問題があるので、やはりヨーロッパ、アメリカ、その他の国々とすり合わせをして、こういう技術について、犯罪に使用されないようにするために、どのような対処をすべきか話合いを進めていく。今後の在り方についてはその点を強調したものにすることが必要であると思います。

５．報告

【事務局より、インターネットバンキングに対する不正アクセスやフィッシングの手口等に係る報告】

○委員：仮に不正アクセス禁止法において、フィッシングサイトを開設した時点で何らかの処罰化をする場合に、例えば金融機関とそっくりな偽のサイトを作れば、著作権法違反、業務妨害罪等の他法令違反でおそらく捜査できるのではないか思いますが、その場合の他法令における罰則と、フィッシング自体を処罰化した場合の不正アクセス禁止法における罰則とを比べた場合に

不正アクセス禁止法における罰則の方がもし低いようなことになるのであれば、わざわざ罰則を設ける必要はないのではないかと思います。

　また、最近の新しいフィッシングの中には、乱数表の数字自体を記入させるようなものが出てきたということから鑑みますと、乱数表を使っての本人確認方法は、もはや万全とは言えないと思います。しかしながら、ワンタイムパスワードの場合には、銀行側がいわゆるトークンと呼ばれるパスワード生成器を発行しますので、さすがにパスワードを盗み出すというのは、困難であると思います。今後、この手の新しいフィッシングに強い認証方法として、このパスワード生成器を使ったワンタイムパスワードの導入を推奨していくことは、被害防止に貢献するのではないかと思っております。

○事務局：著作権法についてですが、この種の事案に対してなかなか適用が難しいということがあります。著作権法あるいは不正競争防止法の法律が保護しようとしているのは、どちらかというと事業者の事業上の権利、営業上の権利です。著作権で処罰しなければいけない場合というのは、犯罪者が著作物を勝手に何の了解も取らずに作ったので、本来であれば著作物の著作者に利益が上がっていたはずが、犯罪者が収益を上げてしまったために、その利益が逸失したとき等であり、処罰することによって民事上の権利を保護しようとするものであります。他に商標法及び不正競争防止法の法律についてもすべて営業上の権利を守っている法律です。この今回のようなケースでは、被疑者は、フィッシングサイトを作ることによって識別符号を不正に取得するということなのですが、識別符号は財産性のあるものではありませんし、必ずしもそれによって反射的に本来の著作者が民事上の権利を侵害されるということになりません。したがって、著作権法違反については場合によっては適用できないこともあるということでございます。

○委員：業務妨害の観点からも難しいのでしょうか。

○事務局：業務妨害については、適用の余地がないわけではないのですが、事案によっては、フィッシングサイトを作った行為と業務に支障が出たことの因果関係をどうやって結び付けるかというところを立証することが難しい場合もあるかと思います。

○委員：預貯金の過誤払いについてですが、被害者は誰になるのかということ

が重要です。業務妨害罪の適用については、銀行の業務を妨害されたかというと、適切なＩＤ・パスワードが入力された結果、払戻しをすれば、銀行が免責されるという前提があるため、適用が難しい。このような場合に銀行が免責されるというのは、世界的に見ても日本ぐらいであり、一方、預貯金者が、警察に被害届を出すと、「あなたは被害者ではない。」、「あなたは、通帳や印鑑を盗まれただけです。」とか、「不正なＩＤ・パスワードの入力により、お金を取られたのは銀行なのだから、銀行が被害者です。」ということで刑法が適用される状況でありますが、その辺の発想については何とかならないものなのでしょうか。

○事務局：現行法の使い勝手が非常に悪いということは、私どもも認識しております。フィッシングにより誘引をした段階で処罰が可能なように取締り法規を整備すべきであるというのが昨年度の総合セキュリティ対策会議の御提言の内容ですので、それらを踏まえまして、私どもは現在、法改正に向けて検討を進めているところでございます。

○委員：私は、攻撃者のモチベーションを下げるにはどうしたらいいのかということをよく考えます。まず、攻撃者、犯罪者がフィッシングを、預金された現金を盗むという目的で手段として選ぶという理由は、フィッシングにより入手したＩＤとパスワードを用いて比較的簡単に預金されたお金を盗むことができるからではないかと思っています。フィッシングのメールが送られてきた場合に、これを行っていいかどうかわからないですが、例えば、偽のＩＤとパスワードを大量に攻撃者に送り付けるというような方法は有効かもしれません。結局、そのＩＤとパスワードを使って、その口座にログインしたときにほとんどが失敗することになりますので、ここで犯罪者のモチベーションが下がり、フィッシングという手法を採らなくなるのではないでしょうか。

　また、例えば、特定のＩＰアドレスから不正なアクセスがあれば、銀行側で一時的にシャットダウンするというようなことも考えてもいいのではないかと思います。

　また、私ども不正プログラムを収集するに当たって、わざと脆弱なコンピュータをインターネット上に置いて攻撃させて、不正プログラムを収集する

という範囲ポットという仕組みがありますが、それと同じような考え方で、フィッシングサイト、フィッシングメール不正プログラム等に関する情報を入手した際にダミー口座を用意しておき、ＩＤとパスワード、乱数表を入力させるなどすれば、例えば、ログインがあって、お金の動きがあった際には、詐欺罪の既遂ということで、ここからトラッキングすることができるのではないかと考えました。

○生活安全局長：最近のこのサイバー空間を取り巻く情勢を踏まえまして、警察の取組について、次回、簡単に御説明させていただきたいと思います。例えばサイバー攻撃についての対策は別部門が担当しており、サイバー犯罪についての対策は生活安全局が担当しているといった、担当の切り分けもありますが、どのように多くの被害情報を収集し、それを一般の方にフィードバックしていくのかという観点では、全庁的に全国警察を挙げて体制を構築していくということで、現在取り組んでいるところです。

また、昨年の総合セキュリティ対策会議において御答申いただいたような、例えば制度面、法制面等の問題についても着実に検討を進めるとともに、警察庁内部における体制強化、さらには、様々な民間の方々との連携の強化についても推進していく。このような３つの柱で、サイバー犯罪、サイバー攻撃について組織を挙げて取り組んでいきたいと思っております。「サイバー空間の脅威に対する社会全体の対応能力の強化」が目標であると考えております。

以上