平成２３年度総合セキュリティ対策会議（第１回）
平成 23 年６月 27 日
発言要旨

１．開会

２．生活安全局長挨拶

本日は、平成 23 年度総合セキュリティ対策会議初回の会合でございます。前田委員長を始め、各委員の皆様方には、御多用の中を御出席賜りまして、誠にありがとうございます。

この対策会議は本年度で 11 年目になります。近年の成果について振り返りますと、児童ポルノのブロッキングが、今年４月 21 日からインターネットサービスプロバイダによる自主的な取組としてスタートしておりますが、これは、この対策会議の提言に基づく大きな成果と言えます。昨年度は、不正アクセス対策、違法・有害情報対策及びサイバーボランティア育成について御検討いただき、御提言をいただきました。既に不正アクセス対策につきましては、所要の法改正を視野に入れた官民連携の検討が始まるなど、御提言内容に沿った施策の実現に向けた作業が着々と進められているところでございます。

本年度は、インターネット上の高度匿名化技術、インターネットカフェ、そして無線ＬＡＮ及びデータ通信カードの３つのテーマについて御議論いただきたいと考えております。これら３つのテーマに共通いたしますのは、匿名性の問題でございまして、時宜に適った重要なテーマであろうかと存じます。

サイバー犯罪にありましても、現実世界における犯罪と同様、犯罪を抑止し、被害の発生を未然に防ぐということが一番の上策でございまして、そのためにできる限りの対策を講じなければなりませんが、それでも犯罪が発生してしまった場合には、早期に事件を検挙、解決することにより、安心を回復するとともに、被害の回復に努めなければなりません。そのためには、犯行に利用された端末や経由したサーバの記録等を手掛かりに、ネットワーク上を追跡し、被疑者、行為者を特定しなければなりません。

以上のことから、インターネット上の高度匿名化技術、インターネットカフェ及び無線ＬＡＮとデータ通信カードが犯罪に悪用されないようにするにはどうあるべきか、さらに、犯罪に悪用されてしまった場合におけるトレーサビリティの確保についてはどうあるべきかが、非常に大きな課題となっております。特にインターネットカフェにおける匿名性の問題につきましては、平成 18 年度にも御議論をいただいており、その結果、インターネットカフェを利用した犯罪等を防止するための総合対策が取りまとめられておりますが、本年度は、その後の４年間における諸対策の進捗状況を検証した上で、法的整備の必要性、内容等について御議論をいただければと考えているところでございます。委員の皆様方には、闊達な御意見を賜りますようお願いを申しあげまして、冒頭の挨拶とさせていただきます。

３．委員紹介

【委員長挨拶】

先日、サイバー犯罪に関する条約の締結に向けた法整備として刑法及び刑訴法が改正されましたが、その成立の背景には、インターネットに関連する業界と警察を始めとする官の世界との溝が狭まってきたということがあります。官民の相互理解の上で、ウィルスを作成する罪やログの保存要請等が可能になってきたのだと思います。この会議では、これまで、官民の連携を一番柱として考え、その溝を埋めるためにいろいろな努力をしてきたと考えております。

先ほど局長からお話がありましたように、良い意味の匿名性は残しながらも、どのようにして問題を除いていくか。「事後追跡可能性の確保」は、やはり急務なのだと思います。インターネットカフェについても、この会議で提言し、警視庁を始め、いろいろな取組をしていただいて、それなりの効果はあったと思いますが、なお問題が残されていることが明らかになってきていると思います。

プロバイダやいろいろな関連の方々の御意見を踏まえ、また、インターネットカフェ業界の方々の議論も踏まえた上で、確実に前に進むための議論をしてまいりたいと思います。何とぞ皆様の御協力をお願いしたいと思います。

【事務局による委員紹介の後、新たに就任した委員による自己紹介】

４．平成 23 年度総合セキュリティ対策会議の開催趣旨について

【事務局から、本年度の総合セキュリティ対策会議の開催趣旨について説明】

○事務局：サイバー犯罪の発生の抑止のためには、サイバー犯罪の取締りが十分に行われることが必要ですが、その前提として、事件が発生した後で追跡ができる、すなわち追跡可能性が確保されていることが不可欠です。しかし、現状では、幾つかの環境から事後追跡を困難にする障害が存在している状況にあります。

そこで、本年度の対策会議は「事後追跡可能性の確保」をテーマに、インターネット上の高度匿名化技術、本人確認が行われていないインターネットカフェの問題及び無線ＬＡＮ、データ通信カードの運用等の問題について検討課題とさせていただきました。

事後追跡可能性の問題については、捜査上警察が困るというだけではなく、サイバー空間における表現の自由、あるいはプライバシーの確保、通信の秘密という大切な自由を侵害するような犯罪行為に対して捜査ができないということは、被害者がいつも泣き寝入りをすることになり、一般ユーザーの方々がインターネットを安心して利用できないということになってしまうという点で、避けては通れない課題であると思っておりますので、御審議をお願いいたします。

５．事後追跡可能性の確保に関する課題について

①　インターネット上の高度匿名化技術について

○事務局：インターネット上の高度匿名化技術は、発信者を匿名化することを目的に開発された技術です。この高度匿名化技術が犯罪者に使用された場合、事後追跡による犯罪者の特定が極めて困難となります。

この会議において、インターネット上の高度匿名化技術の危険性について情報共有を行っていただき、技術的、法的な面の双方について、どのような対策が考えられるのか御検討いただきたいと考えております。

②　インターネットカフェについて

○事務局：インターネットカフェについては、平成 18 年度総合セキュリティ対策会議において、インターネットカフェ等における匿名性その他の問題と対策の中で議論され、その中で、事業者の自主的な取組で利用者の本人確認を確実に実施し、その特定に資する情報を一定期間保存する、各利用者の入退

店時刻と利用者が使用したコンピュータに関する情報を一定期間保存するなど、利用者の匿名性を排除するための取組や、このほかネット・オークション詐欺の防止、利用者の識別符号等及びプライバシーの保護、優良店舗の明示等、利用者に対する注意喚起、子どもによる違法・有害情報の閲覧を防止するための取組について提言がなされ、同提言を受けて、平成19年４月に各都道府県警察に対し、インターネットカフェの実態把握とともに、事業者との連携を強化し、サイバー犯罪の防止、少年の健全育成等の観点から総合対策の推進について指示いたしました。

総合対策の推進を指示して今年で約４年が経ち、各事業者等の努力や都道府県警察の指導等もあり、これらの総合対策はある程度は推進されましたが、これまでは行政指導の形で行われ、また、各事業者等の任意の協力で行われたため限界があり、総合対策に基づく各措置は、一定の割合でいまだに実施されていない状況にあります。

この会議においては、これまでの総合対策に基づく各措置の実施状況を踏まえた上で、今後のインターネットカフェ対策について御検討いただきたいと考えております。

③　無線ＬＡＮ、データ通信カードについて

○事務局：無線ＬＡＮについては、家庭、ファーストフード店、家電量販店等において、暗号化せずに広く電波を使わせている状況がありますが、暗号化していないと不特定多数の者がインターネット接続可能となり、また、通信履歴が残らないため、これを悪用する犯罪者が後を絶たないという状況になっております。

データ通信カードについては、他人名義で契約して悪用した事件が目立っており、契約時の本人確認が十分に行われないと、犯人を特定することが困難になってしまいます。

このような状況を踏まえまして、無線ＬＡＮ及びデータ通信カードについて今後の対策の在り方について御検討いただきたいと考えております。

○　企業に対して不正と思われるアクセスをしている送信先について調べてみると、ホテルではないかという事例が結構ありまして、インターネットカフェに限らず、匿名で泊まれるところもあるみたいですので、そうしたホテルでの自由なアクセスについても検討課題に入れてはどうでしょうか。

○事務局：ホテル等につきましては旅館業法というのがございまして、いわゆ

る宿帳に記入するという法律上の枠組みがあります。それをどうやって徹底していくかという課題はあろうかと思いますが。

○　無線ＬＡＮについては、家庭における無線ＬＡＮの設定も問題になってくると思います。いわゆるゲーム機で、認証及び暗号の度合いが低く、ＷＥＰのみでしか通信できないような機器があるために、家庭において、せっかく他の製品が持っている高度な認証をセットできないということについても課題の１つとしてもいいと思います。

○事務局：確かに、ゲーム機や古い形のパソコンでは、初期はＷＥＰしかなく、暗号の強度について設定上個々にできないので、一番低いところにどうしても合わせざるを得ないのですが、今後、どのようにして暗号の高度化を図るかということについて御議論いただきたいと思います。

６．インターネット上の高度匿名化技術解説

○事務局：Ｐ２Ｐ技術を応用した高度匿名化技術がインターネット上に展開されております。当該技術は、世界中で稼働しているノードの中からランダムに選ばれた数台のノードを経由して、目的のホストと通信するものです。当該技術を用いたネットワークにおいては、最終段のノードと目的のホストの間では、平文による通信が行われておりますが、ノード間通信を暗号化しているため、ネットワークをモニターしても、我々はその通信内容を知ることができません。また、通信中でも、データを直接やり取りする隣接ノードの情報しか持たず、その他の区間の情報は、暗号化され見ることができない、認識することができない仕組みになっており、さらに、通信が完了した時点で、ネットワークの中継にかかる情報は消去されます。

　このような特徴から、インターネット上の高度匿名化技術がサイバー犯罪に用いられると、被害ホストから行為者を特定することが困難であり、サイバー犯罪の行為元が隠匿される可能性があると思います。また、設定により特定のノードを出口ノードに集中させることが可能であることから、加担意図のない者が被疑者として常に浮上する可能性も含まれているのではないかと考えるところです。

○　送信先のコンピュータ等にどういった目的で、具体的にはどういった不正なデータを送ることが多いのでしょうか。

○事務局：不正なデータに限らず、何でも送れます。

○　Ｗｉｎｎｙ、Ｓｈａｒｅ等についても、インターネット上でＰ２Ｐの網を形成しており、ノード間で暗号化通信をしていますが、現在では暗号が全部解かれていて、いわゆるクローリングという方法で送信者にたどり着くことができ、ノード間の通信を蓄積して時系列でまとめることによって、ほぼ初発のデータ発信者を特定することが可能なのですが、このような手法を、今回のこの高度匿名化技術に適用することはできないのでしょうか。

○事務局：Ｗｉｎｎｙ、Ｓｈａｒｅ等においては、ファイル情報を広めるところがネットワークの弱点となったのに対し、この高度匿名化技術については、自身がリレーする情報は、そのコンピュータだけに限られており、広くネットワークをモニターしても知ることができないため、直接的な手法の展開が難しいところがあると思います。

○　これが許されるかどうかは分かりませんが、例えば、セッション情報を破棄しないようなプログラムの入っているノードを作ることによって、追跡できる可能性がないかと思ったのですが。

○事務局：そのようなノードが全体のそれなりの割合、九十何％も占めるようであれば可能だと思います。あくまで理論的な話ですが。

○　この高度匿名化技術が使われると追跡が非常に困難である、通信者の特定が困難であると一言で言っても、全く何もない状態から一体誰が、あるいは誰と通信しているのかということを議論するのと、既に候補が絞られていて、この人と通信しているのか、あるいはこの人が通信しているのかをイエス・ノーで検証することとの間には大きな違いがあり、どちらを目指すのかによって、把握すべき技術レベルが全く違ってくることになります。

　この高度匿名化技術は、これに繋がっているノードが一般的な計算機なのか、より大きなパワーを持ったサーバなのか、あるいはより非力なスマートフォンのような新しいタイプのデバイスなのか、いろいろあると思いますが、どれと繋ぐにしても、インターネットとの接点のところではＴＣＰ／ＩＰを使っており、全く新しいインターネットを、匿名通信の目的で作る技術ではありません。この高度匿名化技術を使って通信しているときにでも、それ以外の通信も持っており、どこからどこへデータを送っているという一方向の矢印ばかりでなく、逆向きの矢印もあるということです。

　したがって、観測点が決まっていれば、そこを観測していると、どのくらいの大きさの小包が何個連続して出て行ったのか、その次にどのくらいの大

きさの小包が何個連続して入ってきたのか、その次にどのくらいの大きさの小包が何個連続して出て行ったのかを観測できます。これをトラフィック分析と言いますが、これを用いれば、少なくともこの高度匿名化技術を使っていても一定の情報を取ることができます。研究レベルにおいて、ある設定の下では、この高度匿名化技術に対する一定の対策が可能であることは、少なくとも分かっておりまして、まずは現状として、本当に対策のレベルが成熟しているのかどうかについても考えた上で、その後どうすべきかということを見ていくべきだと思います。そういう意味では、少なくともトラフィック分析の観点は必要になるだろうと思います。

○　我々はよくオープンソースを扱うときには、やはりオープンソースのコミュニティと会話をするわけですが、このコミュニティに対して、例えばこういう犯罪に対しての協力をしてもらえないか、あるいは安全性もあるのでこういう運用方法に変えてみては、というようなアプローチはできないのでしょうか。また、そのコミュニティ、あるいはオルグについては、どのような性格の組織なのでしょうか。

○　この技術を推進しているのは、学術研究の集団です。

○　Ｐ２Ｐの技術は、良い方向に使えば非常に良い技術ですし、そうでないと大変なことになります。インターネット上の高度匿名化技術については、技術開発という観点で考えれば、ある意味で素晴らしいものであると思いますが、問題はその利用法だと思います。

○　アイルランドのホットラインから、少し前にこの高度匿名化技術を使った児童ポルノのホスティングの話がありまして、アイルランドが問題視しているのは、児童ポルノをあるサーバにアップロードする際に、そのホストとなっているサーバがこの高度匿名化技術によって秘匿されているケースであり、ホットラインが、どこのサーバに児童ポルノが蔵置されているのかを追跡しようとしてもできないと聞いています。

　そこで、何らかの形でこの高度匿名化技術を利用しているノードを特定することはできるのでしょうか。特定できるのであれば、そのリストを、例えばブラックリスト化するなどして、サービスプロバイダにおいて、この高度匿名化技術を用いたネットワークを利用する人を排除する方法が取れないのかと思っております。

○事務局：この高度匿名化技術のアプリケーションプログラムから、一覧とし

て表示されるノードのリストは入手することは可能ですが、このリストは、実在するノード全てかというと、必ずしもそうではない場合もあるようです。

○　不法アップロードという件を考えますと、サーバ側の運用者に対して、相手方の情報を公開させないと投稿できないようにするよう指導をすることで、この高度匿名化技術を使用した匿名での投稿をできないようにするといった活動もやってもいいと思いました。

○　この問題に関して、外国で犯罪に利用された場合の対応、それに関する資料について何か把握していますでしょうか。

○事務局：現時点では、外国での対応状況を把握しておりませんが、先生方に御教示いただきまして、それを手掛かりに研究を進めていきたいと思っております。今後、情報収集に努めていきたいと思っているところでございます。

以上