平成２４年度総合セキュリティ対策会議

「サイバー犯罪捜査の課題と対策」部会（第１回）

平成 24 年 11 月 12 日

発言要旨

１．開会

２．生活安全局長挨拶

本日は、平成 24 年度総合セキュリティ対策会議「サイバー犯罪捜査の課題と対策」部会の初回の会合でございます。前田委員長を始め委員の皆様方には、大変お忙しい中、御出席を賜りまして誠にありがとうございます。

一連の遠隔操作ウイルスを用いた犯行予告事案につきましては、誤って逮捕した４名の方々に対しまして、関係警察がそれぞれ謝罪をいたしたところであります。現在、捜査の経緯について検証を進めるとともに、真犯人の検挙に向けて百数十名体制の合同捜査本部を警視庁に設置して強力に捜査を進めているところでございます。あわせて、全都道府県警察に対しまして、サイバー犯罪捜査に当たってはウイルスによる遠隔操作等の可能性も念頭に置き、事案に応じた各種捜査を実施すること等当面の留意事項等を指示したところであります。今後更なる徹底を図りまして、同種事案の再発防止に万全を期してまいりたいと考えております。

また、ウイルス感染の拡大防止のため、犯行に利用されたウイルスを対策ソフト事業者の皆様に提供いたしましてパターンファイルを作成していただくとともに、インターネットの利用者に向けて、ウイルス対策ソフトを導入し、最新の状態にすることや、不審なサイトにアクセスしないこと等につき、情報提供と注意喚起を行ったところであります。

今回の一連の事案によりまして、警察のサイバー犯罪捜査に対する信頼が大きく揺らぐとともに、高度な情報通信技術が重大・深刻な犯罪に容易に悪用可能となっていることを改めて認識させられたところであります。今後、インターネット空間の自由と開放性を背景に、匿名化技術を悪用して卑劣な犯行を重ねる者が増大することが危惧され、このような情勢に強い危機感を抱いているところでございます。

警察としましてはこうしたサイバー空間を取り巻く情勢の変化に的確に対応するため、

緊急にサイバー犯罪対処能力の強化を図る必要があると考えております。こうした事情から、今回、急遽検討テーマを追加するとともに、ウイルス等のサイバー犯罪に悪用され得る技術の動向に詳しい有識者の方々にも委員として加わっていただきまして、本部会の開催に至ったところでございます。

インターネットへの依存が飛躍的に高まった現代社会において、サイバー技術の悪用による犯罪被害を防止するという警察の責務はますます重いものになっていると認識をしております。ただ、その警察の責務を果たす上では、特に匿名性という課題を克服することが重要でありますが、それは高い技術を有する民間の方々の御支援と御協力があって初めて可能となるものでございます。

かかる経緯と事情、警察としての強い危機感、これをぜひ御理解賜りまして、今、目の前にある事態のみならず将来起こり得る事態にも対処すべく、それぞれの分野の御経験、御見識を踏まえて闊達な御議論を賜りますようお願い申し上げまして、私の挨拶とさせていただきます。

３．委員紹介

【委員長挨拶】

この部会は一連のインターネット掲示板等への犯行予告等の事案を受けまして、「サイバー犯罪捜査の課題と対策」というテーマで急遽開催するものでございます。

今、局長から強い危機感が表明されましたけれども、私も昨今のサイバー犯罪の情勢には懸念を強く抱いており、まさに同じ思いでいたわけです。

実は昨年のこの総合セキュリティ対策会議におきまして、個別の名称こそ用いなかったわけですけれども、いわゆるＴｏｒ等の高度匿名化技術について検討してまいりました。その検討結果を取りまとめ、「サイバー犯罪捜査における事後追跡可能性の確保に向けた対策について」という報告書を出し、そこで問題点を指摘させていただいていたわけですけれども、今回、高度匿名化技術が使われた可能性が高いということで、これは非常に問題であり、これが顕在化しつつあるということについて更に検討しなければいけない。昨年度の会議において、ある意味でその問題を予測して検討していたということで、まさにささやかながら自負するところもないわけではないですが、改めて謙虚に新たな問題としてきちっと取り組んでいく必要があると思います。

今回はアンチウイルスベンダーそれから学識経験者の方に更に加わっていただきまし

て、「サイバー犯罪捜査の課題と対策」というテーマにつきまして、ぜひ活発な御議論をいただきたいと思います。我が国の生活の基盤、産業の基盤でもあるインターネットを安心・安全で使えるようなものにしていくということは非常に重要な課題だと思いますので、何とぞよろしく御協力いただきたいと思います。

【事務局による新たに就任した委員の紹介】

４．平成 24 年度総合セキュリティ対策会議「サイバー犯罪捜査の課題と対策」部会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「サイバー犯罪捜査の課題と対策」部会の開催趣旨について説明】

○事務局：本部会は今回の一連の遠隔操作ウイルス事案を受けて新たに検討テーマを追加し、緊急に開催させていただいたものであります。本部会のテーマであります「サイバー犯罪捜査の課題と対策」、これは一連の事案を契機として警察のサイバー犯罪捜査の在り方が厳しく問われている折、高度な情報通信技術が容易に犯罪に悪用されている情勢を前にして、官と民が連携してこうした事態にいかに効果的に対処していけるか、未然防止も含めたサイバー犯罪への対処能力の強化を図る必要があるとの趣旨で設定をしたものです。

本テーマについて議論を進めていく際の検討項目として、事務局としては３つの点を考えております。

情報通信技術の発達に伴いまして、サイバー犯罪の手口はますます巧妙化、悪質化しており、コンピュータ・ウイルスの他にも高度匿名化技術が犯罪に悪用される事態に至っていることから、今後のサイバー犯罪捜査における重大な隘路として、まずは「高度匿名化技術の悪用への対策」及び「コンピュータ・ウイルス対策」の２つに焦点を当てることとし、またこれらに加えて未然防止も含めて幅広い観点から御議論をいただくという趣旨で、「その他サイバー犯罪対処能力の向上方策」という検討項目を提示しました。

検討の視点としては３つの点を考えております。

まず、「民間事業者との連携」との視点を挙げております。例えば警察は今回の遠隔操作ウイルス事案において、その感染拡大防止のため、犯行に利用されたコンピュータ・ウイルスをいち早くウイルス対策ソフト事業者に提供し、パターンファイルを作成していただきました。こうした関係をいかにして更に発展させ、かつ双方向のものにしてい

けるかという視点があると思います。

次に、サイバー犯罪の特性の一つである「地理的制約を受けない」ということにより、捜査に当たっては海外捜査機関との連携が不可欠です。また、「高度匿名化技術の悪用への対策」につきましても一国のみでは意味がなく、同じ問題に直面している諸外国との間で認識を共有していく必要があります。その意味で、「国際連携の推進」という視点も重要なものであると考えています。

３つ目に、「広報啓発」という視点を掲げています。一連の遠隔操作ウイルス事案においては、警察はインターネットの利用者に向けて、ウイルス対策ソフトの導入や不審なサイトにアクセスしないこと等について情報提供と注意喚起を行いました。被害の未然防止に加えて、関連情報の収集という観点からも、今後、いかにして広報啓発の実効性を上げていくかということは重要な論点であろうと考えています。

サイバー犯罪への対処については警察と民間がそれぞれの立場の違いを認識しつつも、社会・経済活動を支える根幹をなす情報通信システムの安心と安全を守るという一点において手を携え、有機的に連携することが極めて重要だと考えております。

５．遠隔操作ウイルス事案の概要について

【事務局から、遠隔操作ウイルス事案の概要について説明】

６．Ｔｏｒ（Ｔｈｅ　ｏｎｉｏｎ　ｒｏｕｔｅｒ）の秘匿技術について

【事務局より、Ｔｏｒ（Ｔｈｅ　ｏｎｉｏｎ　ｒｏｕｔｅｒ）の秘匿技術について説明】

○事務局：Ｐ２Ｐ技術を応用したＴｏｒネットワークがインターネット上に展開されております。Ｔｏｒ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。Ｔｏｒ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係る情報は消去されます。

このような特徴から、Ｔｏｒ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。

７．質疑応答

○　今回の捜査の過程で、高度匿名化技術があることを想定した捜査が行われたのでしょうか。昨年度の本会議では議論はしていたけれども、捜査を担当する警察ではそこまでの認識がなかったのか、お聞きしたいと思います。

○事務局：現在、検証中でありますので、最終の結論はその検証結果を待たざるを得ないところです。警察庁が関係都府県警察から聴取している限りでは、第三者による遠隔操作ウイルスが技術的に可能だということは専門の捜査員は承知していたようですが、今回の事案を直接担当した警察署の刑事課員は、そこまでの認識はなかったようです。

○委員長：昨年度の本会議で、Ｔｏｒを取り上げ、報告書で取りまとめて危険性についての共通認識はしましたが、Ｔｏｒについてはプラス面が全くないわけではないなど色々な御意見もありました。

　昨年度の報告書では、Ｔｏｒが事後追跡可能性を困難にするということを指摘しましたが、それほど悪用されている実績は出ていないことから、今後検討しなければいけないと取りまとめたところです。昨年度報告書の本会議としての発信の仕方にも責任があるのではないでしょうか。

○生活安全局長：いずれにしても検証中ということになりますが、捜査員一人一人にまできっちりと伝わっていたかというと、ばらつきがあったというのが実情ではないかなと思います。

　したがって、警察庁としてはこれから均一化していく必要があるということです。

○　２点お伺いしたいと思います。掲示板等への悪質な書き込みというのは非常に多発しているとも聞いていますが、その一件一件で捜査をあまり丁寧にやると、結局本物を逃すこともあるのではないか、という点についてどう考えているのでしょうか。

　２点目は、ウイルスをインストールした、不正なプログラムをインストールしたというのは、何らかの自己責任があるかと思うのですが、警察としては啓発についてどう考えているのでしょうか。

○事務局：まず、最初の捜査の関係については、ＩＰアドレスしか被疑者を特定する証拠がないものについては、慎重を期すべきである一方、ＩＰアドレス以外の周辺捜査等で立証できるものについては、第三者によるなりすましという可能性を相当程度排除できますので、実際にはそれぞれの捜査上、濃淡はあります。

ただ、今回のような誤って無関係の人を逮捕するということが二度と起きないように、捜査に慎重を期すという精神は全ての事案において共通しているということです。

２つ目の啓発の関係については、危険なサイトに近寄らない、あるいは危険なサイトから不用意に不正なプログラムをダウンロードをしないということについては、これまで以上に広報啓発をする必要があり、その責務を警察としても担っていると認識をしているところです。

○　今回の事件はいずれも威力業務妨害罪の通常逮捕ですが、刑事部だけが担当されたのでしょうか。サイバー犯罪を担当する捜査員とどのように情報を共有して捜査を進められたのかということをお答えいただけたらと思います。

また、これは意見ですが、今後起こり得る様々な事象は、刑事、生安等多方面にわたる犯罪事象ではないかなと。だとすると、情報を共有して捜査を適切に進められるような工夫・運用も考えていかなければならないのではないでしょうか。

○事務局：お尋ねの点については、現在、４都府県警察で行われている検証の１つの大きなポイントのところです。したがって、最終的な回答は検証を待たざるを得ません。

ただ、この種のサイバー犯罪捜査につきましては、ＩＰアドレスから発信元の契約者を特定する作業等で、通常はサイバー犯罪捜査部門が一定の関与をします。その後は、ケースごとに様々です。今回の事件での教訓は、各捜査部門、サイバー犯罪捜査部門、情報技術解析部門の３つが実質的な連携を図っていくことが必要だということです。今回の事件で、サイバー犯罪捜査については、一般の事件に比してこの３つの部門の連携が重要だということの認識を新たにしました。

○　Ｔｏｒ等の技術は、情報を盗みたい、自分の技術を試したいという人たちが本当に使うのでしょうか。サイバー攻撃は相手の手口が分からないので、攻撃された側がどうやっていいのか分からないというところで悩んでいるのだと思いますが、相手の手口をもう少し解析していくような活動や情報交換があると良いと思います。

また、追跡に関して、攻撃経路のＩＳＰのルータにある程度のログを残しておくと、実証実験の結果では、10 分程度のログでどのあたりから攻撃が来たのかなどが判明する

とされています。実は、サイバー攻撃は単純な手法を複雑に組み合わせているだけではないかと思っていまして、多分何回も何回も攻撃を繰り返してくるのでしょうから、そういう単純な手口に対して可能なことを適用していき、その内に徐々に近くまでたどり着いていくという手法が現実的な話になるのではないかと思います。

○委員長：Ｔｏｒは普通のパソコンユーザーであれば簡単に使えるものになっています。そうすると、非常に利便性のあるツールであって警察に絶対捕まらないというような使い方がされ出してしまうと、放置できないのではないかという感じはします。

○　それはそのとおりだと思います。ただ、もっと単純な技術の組み合わせで行える犯罪が、例えば７割、８割あったときに、どこに焦点を置いて議論しましょうかという話だとも思います。先ほどの追跡に関する話ですが、技術的にある程度可能であれば、法的な問題等技術ではないところの話を取り扱わないと、最終的に犯罪者の近くまで追跡できないのではないでしょうか。

○　今後の捜査上の留意事項について、ＩＰアドレスに過度に依拠するのではなくて、遠隔操作等の可能性も念頭に置くとの話がありました。今回の件はもうこれに尽きるもので、初のケースとしては不可避だったと思います。

　従来であれば、犯罪に使われた物の特定をして、それからその場所の特定をして、時刻の特定をして、そこに誰かがいればその人が被疑者という順序が、遠隔操作で、事実上物が特定の根拠に使えなくなったとの割り切りをする時代になったのかなと思います。今回の件があって、遠隔操作ということによって物の特定というのが事実上意味をなさないとなると、場所と時間の特定も事実上吹き飛ぶわけですから、そうすると残ったもので捜査をするという可能性が出てきたのだというふうな捉え方で。

　全く同じケースでの遠隔操作がされれば特定することはできるかもしれないですが、また次の手法が出たらこれは追っかけられないというリスクが存在する、という形での取り組みも併せてやっていく必要があるのかなと思います。被疑者の特定に関して、原点に返る必要が出てきたのだと考えるのが良いのではないかと思います。

○　先ほど部門間の連携ということで各捜査部門、サイバー犯罪捜査部門、それから情報技術解析部門の連携が重要であるという御指摘がありましたが、これをアドホックに事件が起きたときにその事件ごとにということで考えるのか、それともデジタル証拠自体が物的な証拠を上回るほどの量と重要性を帯びてきているということに鑑みると、アドホックというよりは常設的に連携をするという体制を今後考えていったほうが良いので

はないか、という、いずれかの選択があると思いますが、いずれの方向でお考えでしょうか。

また、Ｔｏｒについては、必要性や利便性が指摘されていますが、我が国の場合にこういうものを使わなければいけないというほどの必要性があるのかどうか、疑問に思う面が多々あります。弊害が今回の事件のように相当大きなものが出てきてしまったということになると、利便性、必要性と、他面で弊害とを比較考量した上でどうすべきかという結論を引き出していかなければならないと思います。

さらに、外国の捜査機関に対する積極的な捜査共助の要請について、海外のＩＴに関してかなり先端的な技術を持っているという捜査機関と早期に技術的な情報の交換を行い、また、法的な枠組みとしてどういう共助をすることができるのかを検討することも必要であると思います。国によってＴｏｒを使う必要があるということを強く意識している国と、そんなものはなくても良いという国と色々あると思います。その温度差の調整・分析等も含めて、あまり遅くない時期にすり合わせ、あるいは情報の交換等を進めていくことが必要なのではないかと思います。

○事務局：連携を実効的にするために、常設的な組織という考えもあるという御指摘でしたが、今後、体制の問題や組織の在りよう等に関し、検討していきたいと考えています。

そのほかの御指摘の点については、まさにそのとおりでありまして、そういう観点からもこの会議でも御議論をいただきたいと思っていますし、また、何らかの方向性をいただければ大変ありがたいと考えています。