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３回）

平成25年１月31日

発言要旨

１．開会

２．インターネットを利用した犯行予告・ウイルス供用事件に係る誤認逮捕事案の検証結果等について

【事務局から、インターネットを利用した犯行予告・ウイルス供用事件に係る誤認逮捕事案の検証結果等について説明】

３．警察と民間事業者等におけるウイルスに係る情報の共有について

【事務局から、警察と民間事業者等におけるウイルスに係る情報の共有について説明】

４.匿名化システム、不正アプリ等への対抗について

【委員から、匿名化システム、不正アプリ等への対抗について発表】

○発表者１：「匿名化システム及び不正アプリ等への対抗」について、あくまで個人的な意見として、発表させていただきます。

まず、Ｔｏｒ等の匿名化システムについては、インターネットの安易で過度な監視や検閲にかかわる拒否の観点と、インターネットにおける、匿名化システムを乱用した犯罪の温床化への対抗という相対する命題にどう応えるのかという点が課題であろうと思います。そのためには、完全に守られた安心なサイバー空間の実現は不可能であることを認識し、事故を前提にした上での対応力強化を考えることが肝要だと考えています。一方、今回の遠隔操作ウイルスの事件の見方として、警察そのものが狙われたという非常に特殊な例であるというものもあり、過度な対応をすると逆効果にもなる可能性があります。

そこで、以上のような観点から、匿名化システムに対する対抗策を関係者ごとに３つに分類して検討しました。

１つ目は、匿名化システムが犯罪等に悪用されないよう、利用者に対して、適切な利用方法に関する広報啓発を推進することです。

２つ目は、企業や官庁等に対して、匿名化システムの利用に関するポリシーの制定を要請し、その着実な実施を依頼することです。

そして最後に、例えばコマースサイト、インターネット掲示板運営者、ＩＳＰ等のサービス提供者に対して、匿名化システム利用に関するポリシーの制定を要請し、その着実な実施を依頼することが挙げられます。これは例えば、あるコマースサイトや自治体の掲示板において､匿名化システムを用いた書き込みにどう対応すべきかなどについて、事前に決めておくことということです。また、一連のインターネットを利用した犯行予告・ウイルス供用事件では、ＣＳＲＦ(Cross Site Request Forgeries)が用いられている事案もありますが、匿名化システムだけではなくこういった悪用可能な技術についてもポリシーを制定しておくことが考えられます。

このポリシーには、次の３つのパターンが考えられます。

１つ目は、匿名化システムを利用した場合の書き込み等を制限するパターンです。この場合、その方策や通知方法についての検討が必要になります。

２つ目は、利用者に関する詳細な記録を取得した上で匿名化システムの利用を許可するパターンです。このパターンは犯罪の抑制にもつながると思います。手法としては、ホームページにスクリプト等を埋め込み、匿名化システムでは隠すことのできない情報を取得するようにしておくことが考えられます。

３つ目は、匿名化システムを利用しようが利用しまいが、全く考慮しないというパターンです。ただ、そういうポリシーを制定したサイトに対しても、ログの保存を要請するということは必要だろうと思います。利用者が匿名化システムを利用しているかどうかを見極める方法については、具体例を提示できると良いと考えます。Ｔｏｒを例に挙げれば、例えばそのノードリストをデータベース化して、ＤＮＳ等のクエリ等の応用でＴｏｒのノードなのか否かを判別できる仕組みを作ってもよいかなと思います。そういった、関係者への働き掛けと同時に、匿名化システムが悪用された場合に備えをしておく必要もあると思います。現実性があるかどうかは別として、ＩＳＰに対して、匿名化システムを利用するアクセスのログの保存要請をしてみることも考えられると思います。契約者と接続ＩＰアドレスと時刻があれば､かなり動きが把握できると考えられますし、国家的に重大な事件の場合は､適切な手順に従って開示を受けることが可能となります。

最後に、匿名化システムについては解析及び研究も重要だと考えます。具体的には、匿名化システムの脆弱性や動作の研究。また、Ｔｏｒに関して言えば、日本では難しいとも考えますが、Ｔｏｒノードを多数立ち上げて研究することも考えられます。

次に不正アプリ等への対抗策について発表させていただきます。不正アプリとは、いわゆる不正プログラムやウイルスのことです。

まず、最近の傾向として、ウイルスの変化というものがあります。従来は、海外のプロが作成したいかにも「ウイルス」なプログラムが脆弱性を突いてデータを窃取するものが主流でした。最近は、国内の普通のプログラマーが作成した一見普通のプログラムが、人間そのものを騙して感染させ、遠隔操作を行うものが増えてきています。判別も非常に難しく、流通範囲も特定場所に限られます。

また、ウイルス供用罪もしくは作成罪の適用を回避する動きも出てきています。利用約款等でプログラムの説明を偽る、又は利用者が騙されることを見越して個人情報の取得を宣言したままプログラムを配布するケースです。個人情報は拡散すれば取り返しのつかない事態になりますので、この種の犯罪を抑止する、又は犯罪者を確実に検挙するという対策以外に、情報の拡散を防止する対策も必要だと考えています。

さらに、ウイルスに感染した場合等に対する万一への備えについては、ウイルス対策ソフトでは防げないような事案も発生している中で、無実を証明できるよう自分のパソコンの動作を記録しておくボイスレコーダーのような機能をウイルス対策ソフトに組み込むことが考えられると思います。その「ボイスレコーダー」を解析すれば、捜査の効率も上がるでしょうし、また、誤認逮捕の防止にも役立つ。そのために、警察や中立な団体等が、その記録のフォーマット等を示すことも考えられると思います。

不正アプリ等への対抗策としては、解析能力も重要です。解析能力は、私は警察では、もうかなり進んできていると思っているのですが、その規模が不足しているのではないかと思います。今後、３つの能力に関する規模が求められると考えています。

１つ目は、フォレンジックに関する能力です。一般的な犯罪についても、サイバー空間上を捜査しなければならないことが増加してくるはずですので、この状況に対する用意が必要ではないかということです。

２つ目は、不正プログラムの解析に関する能力です。警察が、民間企業では利益にならないため解析を行わない部分についてどうやって規模を維持して解析していくかということです。

３つ目は、暗号やパスワードの解読に関する能力です。暗号やパスワードが強固になればなるほど捜査に対して障壁が出ます。

最後に、「官民連携の模索」として２点、述べさせていただきます。

１つ目として、フォレンジック等について。民間の受け皿がうまく機能するとよいのですが、これはじっくり進める必要があると思います。

２つ目として、情報連携について。インターネットの匿名掲示板やワークショップにおける人的交流で、情報連携を密にしていければと考えています。

５．ウイルス感染による匿名Ｐ２Ｐへの情報漏えいの顛末

【委員より、ウイルス感染による匿名Ｐ２Ｐへの情報漏えいの顛末について発表】

○発表者２：この事件は、業務委託先の社員の業務用パソコンが情報を勝手に開示してしまう暴露型ウイルスに感染して業務データが流出してしまい、そういったデータを意図的に収集する犯人にそのデータが渡ってしまったことでした。犯人は、匿名掲示板やファイル共有ソフト「Share」上にそのデータを流出させ、大騒ぎになりました。そこで、犯人の特定の調査を始めたところ、ファイル共有ソフト上でＩＰアドレスの特定に成功するとともに、匿名掲示板等への犯人の書き込みのＩＰアドレスも特定しました。両者は見事に一致し、こういった事実を積み重ねていきました。

一方、犯人の他に、数百人の野次馬的な存在がデータの拡散に関係していたので、プロバイダを通じて警告書を送付しました。匿名性が突破されたのではないかと野次馬に気付かせるわけです。この警告書の送付を継続することによって、１年後には拡散者はゼロになりました。犯人は、そういった対応が気に入らないようで、更にデータを流出させる報復攻撃に出てきました。そこで、我々はプロバイダに対して、犯人の発信者情報の開示請求をしましたが、本人の同意が必要で、また、民間同士ではなかなか手続を進めるのが難しく開示はされませんでした。よって、犯人の流出させるデータをファイル共有ソフト上でダウンロードしにくくする技術も開発して、導入するなどの対応もしました。

最終的には、裁判所で開示請求の仮処分をとって犯人の氏名、住所等を特定し、また、アップロード禁止の仮処分もとりましたが、犯人によるデータの流出が止まらなかったことから、データを保護するために告訴を行い、犯人は逮捕・起訴され、刑も確定したというのが結末です。

この事例を踏まえての「課題と提言」を５点述べさせていただきます。

１つ目として、発信者情報開示等の仕組みの整備。民間企業同士では、相手が悪質な場合であっても発信者開示情報等は難しいという感触です。

２つ目として、警察の対応の改善。この事例では、警察に何度も足を運んで相談をしましたが、なかなか理解してもらうことが難しかったです。

３つ目として、匿名性の突破の重要性。御紹介したとおり、匿名性を一部でも突破すると事態が好転します。

４つ目として、ＩＰアドレスについて。ＩＰアドレスは論理的なものなので、常にそのＩＰアドレスを使っている人が同じだとは限らないということです。

最後に、サイバー犯罪を未然に防ぐ法律の整備。この事例に対応した当時、法整備は十分ではなかったと感じています。最近で言えばウイルス作成罪の創設や、不正アクセス禁止法の改正というのは、効果が非常に高いと思っております。

６.「サイバー犯罪捜査の課題と対策」の報告書骨子案について

【事務局より、「サイバー犯罪捜査の課題と対策」の報告書骨子案について説明】

- 高度匿名化技術の悪用への対策について
- コンピュータ・ウイルス対策について
- その他サイバー犯罪対処能力の向上方策について

７．自由討議

○　本部会の報告書において、「コンピュータ・ウイルス対策」を大きく扱う必要があるのでしょうか。特に、広報啓発が対策として挙げられていますが、今までも色々な形で報告されているわけですので。また、「コンピュータ・ウイルス対策」と「その他サイバー犯罪対処能力の向上方策」については、順序を逆にしてもよいのではないでしょうか。これは質問ですが、報告書が想定するサイバー犯罪や攻撃のレベルはどれぐらいのものか教えていただければ。

○事務局：１点目については、被害の拡大を防ぐという観点から、広報啓発も対策の１つとして挙げさせていただければと考えています。

○委員長：サイバー犯罪捜査という言葉の中には、犯罪をいかに予防するかということも視野に入れることも多く、また、国民にとってどういう報告書の内容が一番メリットが

あるかという観点もあると思います。

○事務局：御質問については、本部会は、サイバー空間において起こり得るいろいろな事態を想定して警察を含めた社会全体の対処能力を高める必要があるという問題意識から出発しています。よって、報告書の射程は限りがないともいえますが、報告書をまとめていく中で、対象とする範囲についても委員の方々の御意見をいただければと思っております。

○事務局：補足して。「広報啓発」という対策については、遠隔操作の事件の反省教訓事項である「遠隔操作等の可能性に対する認識不足」を踏まえれば、犯罪が発生してから対処したのでは遅いということも教訓であると思います。よって、広報啓発として、起こり得る攻撃というものは認識して準備をすることが、コンピュータ・ウイルス対策において重要だと認識しています。

御質問については、状況から予想し得る様々なレベルの攻撃や犯罪への対応というものを、やはりその都度、状況に応じていろいろ勉強して、準備するという趣旨になると思います。

○　報告書に予防も含むということだと、タイトルは原案の捜査に予防も加えて、「サイバー犯罪の予防及び捜査の課題と対策」のようなものが適切ではないでしょうか。

逆に、現在の報告書のタイトルからすれば「その他サイバー犯罪対処能力の向上方策」がメインになると思います。その内容としては、事務局から発表のあった、一連のインターネットを利用した犯行予告・ウイルス供用事件の検証結果を受けての再発防止策が適当だと思っています。

内容の意見としては、捜査のところで改善しなければいけないことは、捜査部門と情報通信部門の間のコミュニケーションだと思います。遠隔操作が発生すると通常の図式が逆転し、犯人を特定しなければ犯罪現場も特定できません。よって、情報通信部門が「犯罪現場」という言葉を慎重に扱い、遠隔操作などの可能性が少しでもあれば、従来の「犯罪現場」と誤解されないような言葉で捜査部門に伝えるということが重要だと思います。

報告書の範囲のことに戻りますと、報告書のタイトルは部会のタイトルに合わせるために、報告書の内容は捜査に限るものということになってしまうでしょうか。

○委員長：御指摘はそのとおりだと思いますが、総合セキュリティ会議は官民が連携して何ができるかという観点から開催されているものであるので、警察による再発防止策だ

けではなく、もう少し幅広に提言できればと考えています。

例えばＴｏｒについていえば、「捜査」そのものから離れて、Ｔｏｒからのアクセスを制限するというようなことを提言して、国民のコンセンサスを得て、政策として展開していく。本部会では、このような観点から議論していきたいと思っています。

○生活安全局長：部会のタイトルと報告書のタイトルというものについては、必ずしも一致しなければいけないということはなく、議論の中身からタイトルを考えていくべきだと考えていますので、事務局としては柔軟に考えさせていただきたいと考えております。

○　総合セキュリティ対策会議は官民連携に関する意見交換の場であるという観点からは、「新たなサイバー犯罪に対する課題と今後の対策」のようなものが、今回の報告書のタイトルとしては適切だという感じがしています。

また、「その他サイバー犯罪対処能力の向上方策」については、私も、警察による再発防止策をベースに、骨子案として発表のあった内容を追加するという形でまとめることが適当だと思っています。

○　「高度匿名化技術の悪用への対策」の１つとして挙げられている「Ｔｏｒからのアクセスを制限することについて」については、民間でできることの１つとして、実現の可能性を探っていきたいと思っています。

Ｔｏｒはそもそも表現の自由等の保護のために開発されたものだと思いますが、我が国において、Ｔｏｒを積極的に認めなければならない環境にはないのではないかと思っています。悪用のリスクがあるのであれば、サイバー空間の安全を保つためにこの対策が可能であるならやりたいと個人的には思っていますし、報告書に記載できるのであれば、ぜひ記載していただきたいと思っています。

○　「その他サイバー犯罪対処能力の向上方策」として、「国際連携」が挙げられていますが、これは大変重要だと思います。

Ｔｏｒについても、主要な各国の捜査機関がどのような対策をしているのかを確認して、他国と足並みを揃えた方がよいと思います。

○　Ｔｏｒの禁止については拙速にやるべきではないと思いますが、サイト管理者の判断においてＴｏｒを禁止することについては、ぜひ記載していただいた方がよいと思っております。

また、「コンピュータ・ウイルス対策」についてですが、ウイルスによる犯罪の報道がなされた場合、アンチウイルスベンダーには不安感から多数の問い合わせがあります。

そこで、対策の一つとして挙げられている「警察とアンチウイルスベンダーとの連携による被害拡大防止方策」については、連携をどんどん進め、ウイルスによる犯罪が発生した際もアンチウイルスベンダーでは対応済みであるという状況を作り出せれば、国民の安心感は増えていくと思います。今後もより一層の協力をしていきたいと思っています。

最後に、対策としては挙げられていませんが、サイバー犯罪にかかわる捜査員、あるいは支援する情報通信部門の増強等リソースについて記載する予定があるのか教えていただければ。

○事務局：サイバー犯罪対処に当たる警察側のリソースについては、当然、対処能力を高める一番大きな方法です。もし御賛同いただけるのであれば、報告書に記載させていただきたいと考えています。

○　個人的にはサイバー犯罪捜査はこれからもますます増加するというのは明白なので、リソースの増強について記載すれば、読む側は安心できると思います。

○委員長：「Ｔｏｒの禁止は拙速にやるべきではない」という御意見について、国でＴｏｒを禁止することを報告書に記載することはあり得ません。対策として挙げられているのは、サイト管理者の判断で制限をするということの働き掛けです。

○　３点意見があります。まず、国際連携に関しては各国の法執行機関との国際連携以外に、グローバルな官民連携という観点もあると思います。

２つ目は、「コンピュータ・ウイルス対策」と「その他サイバー犯罪対処能力の向上方策」を入れ替えるという意見に私も賛成です。

最後に、「コンピュータ・ウイルス対策」に挙げられている「警察とアンチウイルスベンダーとの連携による被害拡大防止方策」について、官民連携ということであれば、アンチウイルスベンダーに限らず、広く民間事業者等との連携を検討してもよいのではないかと思いますが、どうでしょうか。

○事務局：最後の点は、今御指摘のあったとおりに記載したいと思います。Ｔｏｒについて、諸外国の動向等も踏まえつつ、整合性をとったほうがいいのではないかという御指摘がございました。Ｔｏｒについて諸外国で共通しているのは、Ｔｏｒが悪用された場合には通信履歴の追跡によって犯人を特定することは困難だということです。他方で、それに対する取組は各国ばらばらです。サイバー犯罪が国境を越えて行われることを考えれば、理想的には、世界中の関係国で同じ認識で対応していくことが望ましいのです

が、各国との協調を待っていたのでは、現実にＴｏｒが犯罪に悪用されている状況に対して効果的な手が打てないのではないかというのが出発点です。

そこで、事業者側の自主的な取組ということで、日本国内の事情に照らしてＴｏｒを使う必然性や必要性があまりないという前提に立てるのであれば、日本国内においてはＴｏｒからのアクセスを制限するという手法が犯罪の抑止という観点から有効ではないか、という形の提言には意味があると事務局としては考えております。

○　追跡可能性が確保できないということになると、捜査は不可能です。「Ｔｏｒからのアクセスの制限」という対策は、事後追跡の障害となっているツールへの対策という点で、捜査の課題に応えるものであると思います。また、治安、安全を確保する必要がある一方、Ｔｏｒを使わなければならない必要がどの程度あるのかということとのバランスを考えると、Ｔｏｒを使わなくてもネットはアクセスできますので、民間で一定の制限を加えるということは当然検討されてもいいのではないかと思います。

○委員長：本日の部会では、骨子案の順序や予防の観点をどれだけ取り入れるかという点について御指摘がありましたが、御指摘を踏まえつつ、次回は報告書草案について議論したいと思っています。