新たなサイバー犯罪に関する課題と今後の対策について

平成 24 年度総合セキュリティ対策会議　報告書

総合セキュリティ対策会議

はじめに

近年めざましい発展を遂げている情報通信ネットワーク、とりわけインターネットは、私たちの生活の利便性を向上させるにとどまらず、社会・経済活動の根幹を支える重大なシステムとして機能するに至っている。その一方で、サイバー犯罪の増加、インターネット上の違法・有害情報の氾濫、コンピュータ・ウィルスの蔓延が社会問題となるとともに、サイバー空間に対する国民の不安感も急速に高まっており、今、正に官民が連携してより効果的な情報セキュリティ対策を検討・実施するべき時期を迎えている。

「総合セキュリティ対策会議」は、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について意見交換を行うことを目的として、平成 13 年度以降開催されているものである。当会議においては、情報セキュリティに関する有識者にとどまらず、電気通信事業、コンテンツ事業、コンピュータ製造・販売業、ソフトウェア産業等の各種事業に関する知見を有する方々、さらに、法曹界、教育界、防犯団体の方々という広い分野の有識者により、幅広い意見交換が活発に行われており、平成 13 年度以降、毎年度、様々な内容の報告書を取りまとめてきた。そして、こうした意見交換の結果は、例えば、平成 18 年６月のインターネット・ホットラインセンターの運営開始、平成 20 年５月のファイル共有ソフトを悪用した著作権侵害対策協議会の発足、平成 21 年６月の児童ポルノ流通防止協議会の発足、平成 24 年の不正アクセス禁止法の改正等の取組に結び付いている。

本年度は、遠隔操作ウイルス等による犯行予告事件を受けて「サイバー犯罪捜査の課題と対策」をテーマに選定し、高度匿名化技術の悪用への対策、コンピュータ・ウイルス対策、警察のサイバー犯罪対処能力の向上方策について議論を行った。各委員には、それぞれが属する企業・組織における知見を背景としつつも、中立的な立場で、各テーマに関して関係者が講じるべき具体的な取組等について議論を行っていただいた。本報告書は、これらの議論の結果を取りまとめたものであり、今後の情報セキュリティの向上及び安全・安心なインターネット社会の発展の一助となれば幸いである。

平成 25 年３月

総合セキュリティ対策会議委員長

前田雅英

総合セキュリティ対策会議の目的

昨今の官民を挙げた取組により、情報技術の急速な進展や高度情報通信ネットワーク社会が実現されつつあり、市民生活や社会・経済活動のあらゆる分野において、情報技術及び情報通信ネットワークが活用されるようになっている。

特に、インターネット等の活用により生活の利便性が向上するなど、高度情報通信ネットワーク社会の光の部分が拡大する一方、サイバー犯罪が年々増加するなど、その陰の部分とも言うべき、情報セキュリティに対する脅威も増大しつつある。情報通信ネットワークの安全性及び信頼性を確保し、国民がこれを安心して利用することができるようにすることは、高度情報通信ネットワーク社会の形成にとって不可欠な条件であり、情報セキュリティの確保は喫緊の課題となっている。

情報セキュリティについては、①情報セキュリティに対する脅威の舞台であるインターネット等の情報通信ネットワークが社会・経済活動の根幹を担う存在であり、産業界等が発展させてきたものであること、②情報セキュリティに対する脅威に的確に対処するためには、急速に発展している高度な技術の活用が必要であること等から、情報通信ネットワークに関わる広範な層の協力によってこそ確保されるものであると言える。

それゆえ、情報セキュリティに関する警察の活動も、産業界を始めとする多くの関係者・関係機関との連携が不可欠である。情報セキュリティに関する産業界等と警察との連携については、都道府県レベルでは「プロバイダ連絡協議会」等を通じた各種の取組がなされていたものの、国レベルではかかる広範な官民連携の場が設けられていなかったところ、平成 13 年５月に東京で開催されたＧ８ハイテク犯罪対策・官民合同ハイレベル会合（東京会合）においては、産業界等と法執行機関との連携を各国内でも議論することの重要性が改めて確認された。

総合セキュリティ対策会議は、こうした状況を受けて、情報セキュリティに知見を有する各界の有識者による意見交換の場として開催に至ったものであり、当会議における議論が産業界等と警察による情報セキュリティ対策の参考となることを期待するものである。

【これまでの議題】

平成 13 年度	情報セキュリティ対策における連携の推進
平成 14 年度	情報セキュリティに関する脅威の実態把握・分析
平成 15 年度	官民における情報セキュリティ関連情報の共有の在り方
平成 16 年度	インターネットの一般利用者の保護及び知的財産権侵害に関する官民の連携の在り方
平成 17 年度	インターネット上の違法・有害情報への対応における官民の連携の在り方
平成 18 年度	インターネット・ホットラインセンターの運営の在り方及び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
平成 19 年度	Winny 等ファイル共有ソフトを用いた著作権侵害とその対応策
平成 20 年度	インターネット上での児童ポルノの流通に関する問題とその対策
平成 21 年度	インターネット・オークションにおける盗品の流通防止対策
平成 22 年度	安全・安心で責任あるサイバー市民社会を実現に向けた対策
平成 23 年度	サイバー犯罪捜査における事後追跡可能性の確保

目　　次

～本編～

～資料編～

発表資料

本　　編

新たなサイバー犯罪に関する課題と今後の対策について

昨年発生した、いわゆる遠隔操作ウイルス等による犯行予告事件(以下「本事件」という。)においては、犯行に踏み台として使用されたコンピュータから、第三者による遠隔操作を可能とするコンピュータ・ウイルスが発見されるなどしたことから、警察が犯人でない方々を誤って逮捕していたことが判明した。本事件においては、新種のコンピュータ・ウイルスによりパソコンが遠隔操作されていたため当時のウイルス対策ソフトでは当該コンピュータ・ウイルスの検知がなされず、また、犯行には Tor という高度匿名化技術が悪用されており、平成 23 年度の本会議の報告書でも指摘していた懸念が現実のものとなった。

本事件により、警察のサイバー犯罪[1]捜査に対する国民の信頼は大きく揺らぐとともに、サイバー犯罪を敢行するに際して高度な匿名化技術が重大・深刻な犯罪に容易に悪用可能となっていることやコンピュータ・ウイルスによる被害が甚大であることが改めて示された。

他方、本事件においては、犯行に用いられた新種のコンピュータ・ウイルスが警察からアンチウイルスベンダー等に提供され、アンチウイルスベンダー等においてパターンファイルが作成されるなどして、ウイルス対策ソフトによる当該コンピュータ・ウイルスの検出が可能となり被害の拡大防止が迅速に図られた。このことは、改めてサイバー犯罪対策における警察と民間事業者との連携の重要性を示すものであった。

インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着している中、情報通信技術を悪用した犯罪やコンピュータ・ウイルスによる犯罪を抑止・検挙し、インターネットの安全性及び信頼性を確保する警察の責務はますます重いものになっている。情報通信技術の急速な進展を踏まえると、警察がこの責務を十分に果たしていくためには、サイバー犯罪への対処能力を不断に向上させていく必要があるところ、そのためには警察自身の努力はもとより、民間事業者の知見の活用、民間事業者との連携を図っていくことが重要である。

そこで、情報セキュリティに知見を有する各界の有識者による意見交換の場である本会議において、本事件を踏まえ、急遽、高度匿名化技術の悪用の現状やコンピュータ・ウイルスの現状、これらに対する対策の在り方、警察のサイバー犯罪対処能力の向上方策について議論を重ね、これらに対する対策及び警察のサイバー犯罪対処能力の向上方策について取りまとめた。

[1] ：高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪

第１章　高度匿名化技術の悪用への対策について

1　高度匿名化技術の概要

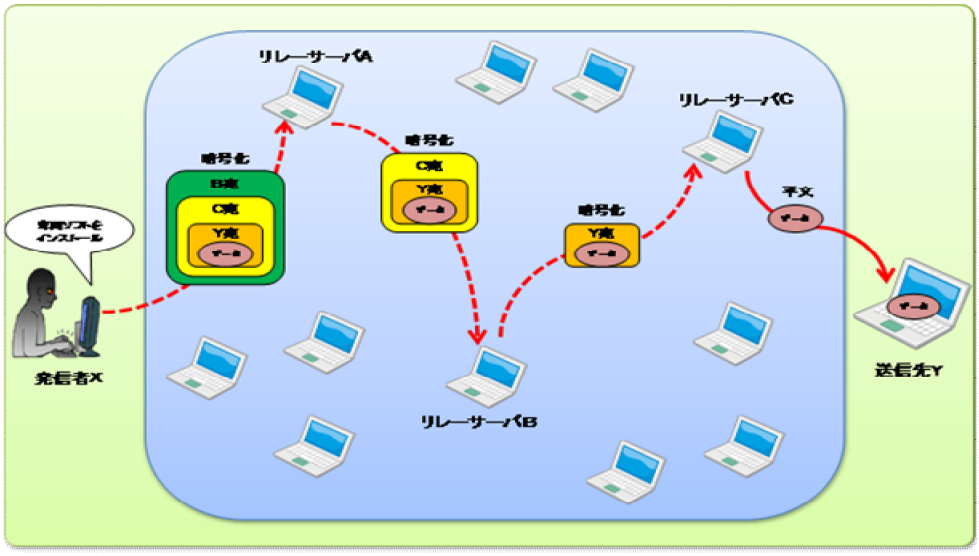
インターネットはその特性として一定の匿名性を有しているところ、種々の観点からより匿名性を高めるための技術が開発されており、本事件のように犯罪への悪用という問題も生じている。

(1) Tor について

インターネット上の高度匿名化技術の一つとして、本事件で使用された Tor(The　Onion Router)がある。Tor はもともと米海軍調査研究所において開発された技術と言われており、今日では、情報統制が行われている海外の国々において国民の表現の自由やジャーナリストのレポートの保護等、インターネット上での自由な活動と当該活動におけるプライバシーの保護等の目的で利用されている。Tor は、インターネット上でフリーソフトウェアとして公開されており誰でもダウンロードが可能である。

Tor は使用者のコンピュータ、これにインストールする専用ソフトウェア及びインターネット網に存在するリレーサーバから構成されている。リレーサーバはＰ２Ｐ技術を応用して発信元のコンピュータから送信先のコンピュータまでの通信を中継するネットワークを構成している。一般的な通信の場合には、発信元のコンピュータと送信先のコンピュータとの間で直接通信が行われるのに対し、Tor を利用した通信の場合は、発信元コンピュータから世界中のインターネット上にあるリレーサーバのうち任意の３台を経由して、送信先のコンピュータと通信が行われる（図１）。このとき、送信先のコンピュータには最後に経由したリレーサーバと通信が行われたという記録は残るものの、経由した各リレーサーバは当該通信に係る記録を残さないように設計されており、また、通信経路のうち最後に経由したリレーサーバと送信先のコンピュータを除いて、発信元コンピュータとリレーサーバ間及び経由したリレーサーバ間の通信は全て暗号化される。これらの仕組みにより Tor は送信先側のコンピュータに残る通信に係る記録から直接経路をたどって発信元を特定することを困難にしている。

図１　Tor の動作概要



(2) その他の高度匿名化技術の概要

Tor 以外にも、インターネット上で匿名性を確保しつつ通信を行うための技術として、例えば Freenet、Invisible Internet Project（I2P）、Java Anon Proxy（JAP）と呼ばれるものが存在している。また、サブリミナルチャネルと呼ばれる通信の存在自体を隠蔽する技術もある。これは、例えば一定の規則性の下、画像の一部に第三者には気付かれない程度の微細な変化を加えたり、通常のパケット通信について、時間当たり通信量をコントロールしたりすることにより、当該規則性を知る者に対してのみ通信の存在及び内容を伝えるものである。

2 高度匿名化技術である Tor の悪用事例

高度匿名化技術のうち、本事件で用いられた Tor は、通信履歴をそもそも残さない設定とされていること等から事後的な追跡は困難である。また、インターネット上において無償で公開されているソフトウェアをインストールするだけで利用が可能となるため、犯罪に容易に悪用され得る状態になっている。国内においては本事件のほか少なくとも次のような悪用事例が認められる上、諸外国においても Tor が犯罪に悪用される事案は多数発生している状況である。

事例１　インターネット掲示板を利用した脅迫事案

Tor を悪用してインターネット掲示板に殺害予告等の書き込みを多数行ったもの。各種捜査の結果、書き込まれていた者とトラブルになっていた被疑者が浮上し、検挙に至ったもの。

事例２　インターネットバンキングに対する不正アクセス等事案

Tor を悪用してインターネットバンキングに不正アクセスし、他人の口座から不正送金を行って、多額の現金を引き出したもの。

事例３　出会い系サイトの掲示板を利用した児童に対する禁止誘因行為事案

Tor を悪用して出会い系サイトの掲示板に、児童を異性交際の相手方となるように誘引する書き込みを行ったもの。

3 高度匿名化技術への対策

(1) 高度匿名化技術に関する調査・研究の推進

サイバー犯罪捜査においては、被害に係るコンピュータ端末等から得られる通信に係る記録を基に発信先を事後的に追跡することとなるが、高度匿名化技術はこの事後追跡を困難にするという点において極めて大きな障害となっている。Tor については、既に我が国においても犯罪に悪用されており悪用への対策の必要性が認められるものの、Tor はあくまでも匿名化技術の一例であり、他にも多く匿名化技術の研究がなされ、また、ツール化されてきている。

今後も、情報通信技術の発達に伴い、様々な高度匿名化技術が研究・開発され、ツール化されることが予想されることから、警察において、海外も含めて高度匿名化技術がサイバー犯罪に用いられた事例やそれへの対応策について情報収集に努めるとともに、最新の高度匿名化技術に係る研究、開発、実用化等の動向について調査・研究を推進していくことが求められる。

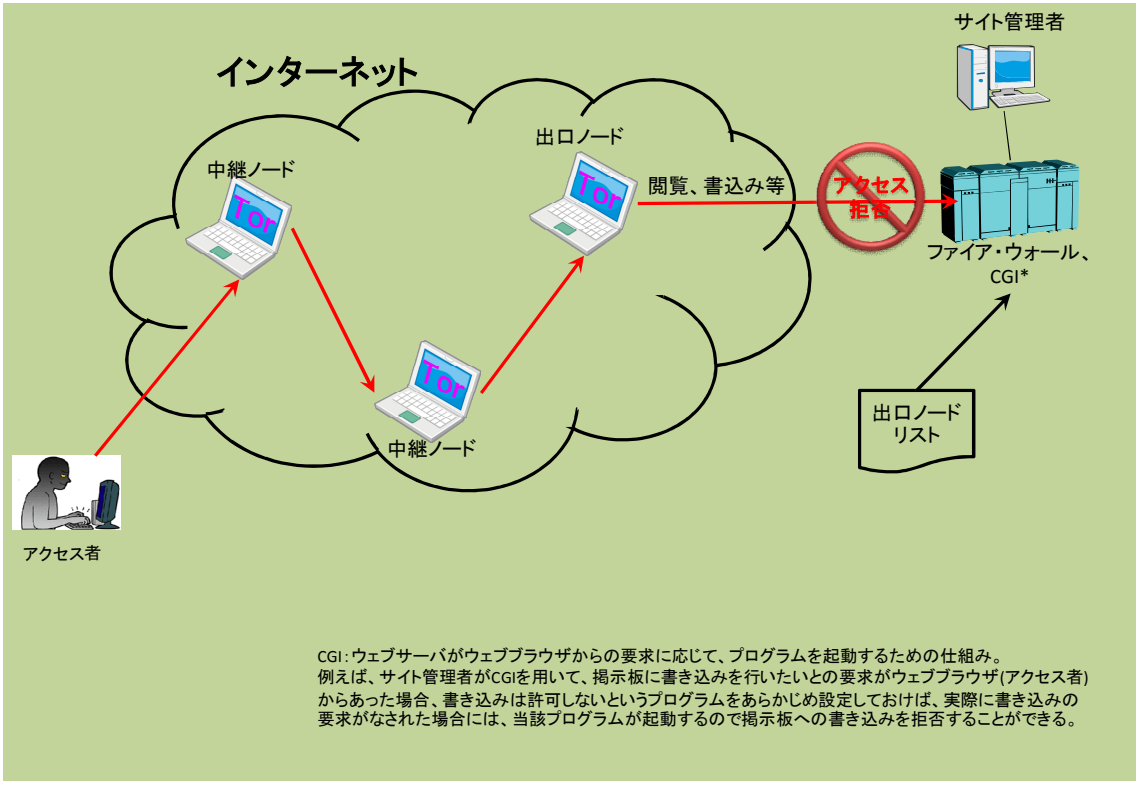
(2) Tor からのアクセスを制限することについて

Tor が本事件を始め、国内外において犯罪に悪用されている状況に鑑みると、Tor の犯罪への悪用を防ぐという観点からの対策が求められる。

Tor を用いて行われる通信を、例えば、下記の手法により技術的に制限することが可能であることから、Tor による通信により被害を受けるおそれのあるサイト等当該サイトの特性に応じ、サイト管理者等の判断により Tor を用いた通信を遮断することとすれば、犯罪抑止の観点から一定の効果があると考えられる。

【例】公表されている Tor の出口ノードリストを活用して、ファイア・ウォールによりサイトの閲覧を制限したり、CGI により掲示板への書き込みを制限したりする。

図２：Tor からのアクセスの制限



第２章　コンピュータ・ウイルス対策について

1　コンピュータ・ウイルスをめぐる情勢

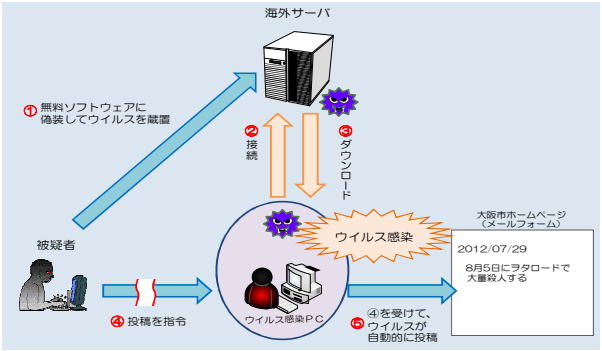
コンピュータ・ウイルスは、コンピュータの使用者の意図とは無関係な動作をさせて使用者の不安を煽るだけでなく、個人情報をインターネット上に流出させたり、コンピュータのデータを損壊させたりするなどコンピュータの安全な使用を害している。また、コンピュータ・ウイルスの作成・使用目的もかつての愉快犯的なものから、金銭詐取や政府・企業の活動を妨害等するための目的へと変化しているほか、その挙動も感染したことに気付かれないよう密かに動作するようになってきている。最近ではコンピュータ・ウイルスを用いてインターネットバンキング口座の ID・パスワードを窃取し、それを用いて他人のインターネットバンキング口座に入り込んで、自らが管理する他人名義の口座に送金するという事案が発生するなどしている。コンピュータ・ウイルスについては、平成 23 年６月の刑法改正により不正指令電磁的記録に関する罪、いわゆるコンピュータ・ウイルスに関する罪が新設されたことで（同年７月 14 日施行）、コンピュータ・ウイルスの作成等といった実質的な被害の発生の前段階における検挙等の対策が可能となっている。しかしながら、世界中で日々多くの新種のコンピュータ・ウイルスが作成されており、本事件（図３）においても、最新のパターンファイルを適用したウイルス対策ソフトを用いても検知することができない新種のコンピュータ・ウイルスが使用されていたことが警察の捜査の過程で明らかとなっておりコンピュータ・ウイルスをめぐる状況は極めて厳しいものとなっている。

事例１　被疑者（無職・男性・38 歳）は、感染するとコンピュータが使用できなくなるコンピュータ・ウイルスを、ファイル共有ソフトの利用者に感染させることを目的として、自宅パソコンに保管したもの。

事例２　平成 24 年 10 月には、利用者が、金融機関等の正規のホームページからログインをすると不正な入力画面が表示され、パスワード等の入力を求められる新たな手口が発生した。

事例３　被疑者（無職・男性・45 歳）ら６人は、インターネット上にスマートフォン専用のアダルト動画サイトを構築し、動画再生専用アプリに偽装したコンピュータ・ウイルスをダウンロードさせることにより、サイトの閲覧料金を支払う義務が生じる旨をスマートフォンの画面に表示させ、アダルト動画サイトの利用料金名目で現金を詐取したもの。

図３　遠隔操作可能なウイルスの動作（概略）



2　コンピュータ・ウイルス対策の課題

本事件において犯行に利用された新種のコンピュータ・ウイルスについては、警察からアンチウイルスベンダーに対して提供がなされ、これを受けたアンチウイルスベンダーにおいて当該コンピュータ・ウイルスに対するパターンファイルが作成されるなどして、被害の拡大防止が図られた。今後も次々と新たなものが出現することが予想されるコンピュータ・ウイルスに対処するためには、こうした警察と民間事業者等との緊密な連携がなされることや警察によるウイルス罪に対する適切な取締りがなされる必要がある。また、本事件においては無料ソフトをダウンロードしたことにより、コンピュータ・ウイルスに感染している例があることから、一般のユーザのコンピュータ・リテラシーの向上方策も検討する必要がある。

3　コンピュータ・ウイルスへの対策

(1)　警察とアンチウイルスベンダー等との連携による被害拡大防止方策（図４）

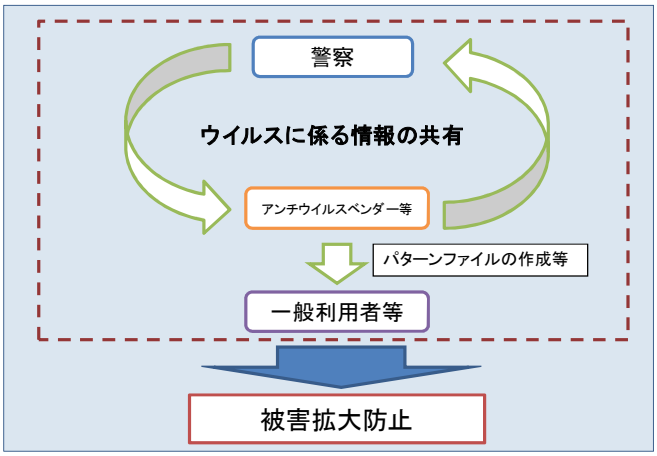
ア　警察からアンチウイルスベンダー等への情報提供枠組みの構築

本事件や平成 24 年秋に発生した１記載の事例２の事案において、被害拡大の防止のため警察は入手したコンピュータ・ウイルスについて、アンチウイルスベンダー等に対する情報提供を行った。これにより当該コンピュータ・ウイルスに係るパターンファイルが作成されるなどして、相当の被害発生防止がされたものと考えられる。このように、警察において新種のコンピュータ・ウイルスが発見された場合、コンピュータ・ウイルスに係る情報が警察からアンチウイルスベンダー等に提供され、ウイルス対策ソフトのパターンファイルの更新等所要の対策がとられることにより大きな被害拡大防止効果が期待されることから、継続的にこうした取組がなされるよう情報提供枠組みの構築が求められる。

イ　アンチウイルスベンダー等から警察への情報提供枠組みの構築

コンピュータ・ウイルスに係る事案が発生した場合には、警察は捜査の過程でコンピュータ・ウイルスの解析を行うこととなるが、警察における効果的な捜査・解析の実施のためには、警察がコンピュータ・ウイルスに係る情報を幅広く収集することが効果的である。加えて、コンピュータ・ウイルスの中には海外で流行した後、日本に持ち込まれ被害を発生させるものも散見されるところ、日本においてコンピュータ・ウイルスに係る被害が発生する前に警察においてコンピュータ・ウイルスに係る情報を収集していれば、効果的な捜査・解析を実施することが可能である上、一般利用者に対して効果的な注意喚起等を実施することが可能となる。アンチウイルスベンダーは世界的規模でコンピュータ・ウイルスに係る情報を収集するなど、様々な種類のコンピュータ・ウイルスに係る情報を大量に保持している。これを可能な範囲で警察に対して当該情報を提供することができれば、警察による犯罪捜査、抑止活動等が一層効果的になるものと考えられる。そこで、アンチウイルスベンダー等から警察に対する情報提供の枠組みの構築が求められる。

図４　ウイルスに係る情報の共有スキーム



(2)　警察におけるコンピュータ・ウイルスに係る情報の蓄積及び分析

コンピュータ・ウイルスについては、そのプログラムの作成者による特徴があることやインターネット上に掲載されているプログラム技術に係るウェブサイト等からプログラムの「パーツ」を集めてコンピュータ・ウイルスを作成するケースがあることが指摘されている。警察の捜査の過程で把握されたコンピュータ・ウイルスに係る情報や先述の枠組みによりアンチウイルスベンダー等から提供されたものも含め、コンピュータ・ウイルスに係る情報等が警察において蓄積され、データベース化されれば、新たな事案において発見されたコンピュータ・ウイルスと当該データベースとの照合が可能となり、コンピュータ・ウイルスの特徴等から、作成者等の特定や絞り込みにつながることが考えられる。そこで、警察において今後、こうした機能を有するデータベースの構築を含め、コンピュータ・ウイルスに係る情報の蓄積及び分析が行われることが求められる。

(3)　広報啓発活動の推進

コンピュータ・ウイルスによる被害を防止するためには、アンチウイルスベンダーの提供する最新のウイルス対策ソフトを使用することが効果的であるが、ウイルス対策ソフトが有する機能は、ユーザが負担できる費用の程度に応じて様々であり、かつ、本事件によっても明らかなとおり、それのみではコンピュータ・ウイルスによる被害の防止は困難である。加えて、コンピュータ・ウイルスによる被害の未然防止のための唯一絶対的な対策を提示することは困難であり、被害の未然防止・拡大防止のためにはインターネット利用者のコンピュータ・リテラシーを高めていく必要がある。そのためには、警察を始め各主体において継続的に次のような広報啓発を推進していくことが求められる。

ア　自己防衛手法の紹介

コンピュータ・ウイルスによる被害を未然に防止するためには、最新のパターンファイルが適用されているなどの最新の機能を有するウイルス対策ソフトを用いるほか、ウイルス対策ソフトにより警告が発せられるなどしているウェブサイトを閲覧しないこと、標的型メールによるコンピュータ・ウイルスの感染を防止するため、発信者の不明な電子メールを開かないこと、無料ソフトウェアを不用意にダウンロードしないこと等が必要とな

る。インターネット利用者に対して継続的にこうした基本行動に係る情報を提供していく必要がある。

イ　新たな手口の紹介

世界中で日々多くの新種のコンピュータ・ウイルスが作成されており、海外で流行したコンピュータ・ウイルスが後に我が国においても用いられるケースも散見される。我が国においても今後流行が予想されるコンピュータ・ウイルスを用いた新たな犯行手口に係る情報提供を行い、利用者の注意喚起を図っていくことも必要である。

ウ　コンピュータ・ウイルスに感染した場合の対処方法の紹介

コンピュータ・ウイルスに感染したことが判明した場合は、自らが使用しているウイルス対策ソフトが最新の機能を有するものか確認するとともに、直ちにインターネット等のネットワークから当該端末を切り離すなどの被害の拡大防止のための措置を実施することが必要であり、こうした情報についても継続的に提供していく必要がある。

第３章　警察のサイバー犯罪対処能力の向上方策について

平成 25 年１月 16 日、本事件を受け、警察庁はサイバー空間において今後起こり得る様々な事態にも対処できるよう、サイバー犯罪対処能力の強化等に向けて「サイバー犯罪対処能力の強化等に向けた緊急プログラム」を策定している。警察において、本プログラムが着実に実行されることが望まれるが、本会議としては、警察のサイバー犯罪対処能力向上のため、外部の幅広い知見、相談を含む情報等を一層積極的に収集し警察組織の中で有効に活用する必要があると考えられることから、次の６点をサイバー犯罪対処能力の向上方策として取りまとめた。

１　民間事業者等の知見の活用

民間事業者等の中には、グローバルに事業展開を行い世界規模でのサイバー犯罪等に関する情報を有しているものや最先端の情報セキュリティに関する知見を有しているものが存在する。海外においてはこうした民間事業者と法執行機関が情報交換等を行う例もあり、我が国においてもこうした情報交換が積極的に行われることが期待される。また、民間事業者等の知見を活用するという観点からは、情報通信技術の発達のスピードは速く、こうした知識・技能を警察部内のみにおいて習得させることには自ずと限界があることを踏まえると、民間事業者等の実施する研修等に捜査員を参加させることや民間事業者等に捜査員への講義委託を行うことも積極的に行われることが求められる。また、より直接的な知見を得る方策として警察と民間事業者等との間での人事交流についても検討がなされることが期待される。

２　諸外国の捜査機関等との連携

サイバー空間はその特性として地理的・時間的制約を受けることが少なく、サイバー犯罪は容易に国境を越えて敢行されることから、外国捜査機関と連携した捜査が積極的になされることが重要である。加えて、犯行手口についても海外で流行した手口が一定の期間をおいて我が国において敢行される傾向にあることから、諸外国の捜査機関等からの情報収集を行い、我が国において今後、敢行されることが予想される犯行形態に対する捜査手法・予防策等事前の備えが行われることが求められる。

３　最新の情報通信技術に係る調査研究

情報通信技術の発達に伴いサイバー犯罪の手口も高度化・複雑化している。高度匿名化技術の一つである Tor についても、今や最新の技術ではなく、新たな匿名化技術の研究が日々行われていることから、これらの新たな技術が犯罪に悪用される前から広く調査・研究を行い、必要な対策が講じられていることが望ましい。また、Tor に対抗する研究も多数行われているところ、Tor の匿名性を減殺あるいは無力化する観点からもこれらの研究動向等に常に留意しておく必要がある。いずれにしても、最新の研究状況等について知見を有していないということは大きな支障を及ぼすことが懸念される。犯罪発生の後、事後的に調査研究するのではなく、必要な体制を構築して恒常的に最新の技術の開発状況等について調査研究していくことが警察に求められている。

4　相談窓口の充実

サイバー犯罪に関する相談の中には、不正アクセス事犯やウイルス事犯のような専門的な知識が必要であり、相談内容を踏まえた適切な対応が求められるものも多い。また、次々に新たな事象が生じるため、事案によっては警察のいずれの部門が対処すべきか予見できない場合等においても、相談者の事情に配意した適切な対応が求められる。警察におけるサイバー犯罪に関する相談を受け付ける体制を整備・充実し、相談者が利用しやすいものとしていくことが求められる。

5　部門間の連携

警察に対して国民が求めるものとしてはサイバー犯罪が発生した際に迅速かつ適切な捜査がなされること、同様の犯罪の発生が防止されること、サイバー犯罪の発生状況や危険性が的確に情報提供なされることが挙げられる。本事件に関し、４都府県警察において実施された検証から得られた主な反省教訓事項の一つとして、各捜査部門、情報通信部門との間で、正確かつ十分な情報共有がなされなかったなど、部門間の連携不足が、誤認逮捕という不適切な結果につながったとされているところである。警察がサイバー犯罪に適切に対処していくためには部門間の実質的な連携の強化が求められる。

6　サイバー犯罪情勢に応じた捜査の推進

本事件では、新種のコンピュータ・ウイルスを用いて無関係の第三者を犯人に仕立て上げるなど、これまでにない方法でコンピュータ・ウイルスが悪用された。サイバー犯罪の手口は今後ますます複雑化・高度化していくことが予想されることから、警察においては、犯罪者の志向の変化を含むこのような情勢の推移に応じた適切な捜査がなされるよう努力を続けるべきである。

おわりに

これまで、本事件で用いられた高度匿名化技術や新種のコンピュータ・ウイルスの新たな悪用方法等に関する現状や課題、その対策並びに警察のサイバー犯罪対処能力の向上方策について述べてきた。それぞれの対策が着実に実施されることで、警察の、また、社会全体としての未然防止も含めたサイバー犯罪への対処能力は向上していくものと考えられるが、今後とも、インターネット空間の自由と開放性を背景に、様々な技術を悪用した形でのサイバー犯罪が行われることが予想される。

社会・経済活動の根幹を支える重要なインフラであるインターネットの安全・安心を確保するためには、インターネット空間においても、犯罪を犯した者は処罰されるということが担保される必要があり、捜査機関たる警察の果たす役割は大きい。

本報告書を踏まえ、警察において適切な対応が図られインターネット空間の安全・安心が確保されることを希望する。なお、こうした対策を警察において主体的に講じていくためには人員、資機材及び予算を含めた警察のリソースの充実が不可欠であることを最後に付言する。

平成２４年度総合セキュリティ対策会議委員名簿
「サイバー犯罪捜査の課題と対策」部会

前田　雅英	首都大学東京 法科大学院教授（委員長）
片山　　建	日本マイクロソフト（株）法務・政策企画統括本部 政策企画本部　次長
桑子　博行	（一社）テレコムサービス協会　サービス倫理委員会　委員長
小屋　晋吾	トレンドマイクロ（株）　執行役員　統合政策担当部長
佐々木良一	東京電機大学　未来科学部教授
佐藤　慶浩	日本ヒューレット・パッカード（株）個人情報保護対策室室長
関口　和一	日本経済新聞社　論説委員兼編集委員
徳田　敏文	（株）シンプレクス・コンサルティング 情報セキュリティ最高責任者
中野目善則	中央大学　法科大学院教授
西本　逸郎	（株）ラック専務理事　セキュリティ事業本部 セキュリティ技術統括
則房　雅也	日本電気（株） ナショナルセキュリティ・ソリューション事業部主席技術主幹
藤原　靜雄	中央大学　法科大学院教授
別所　直哉	ヤフー（株）執行役員 CCO 兼政策企画本部長
松浦　幹太	東京大学生産技術研究所　准教授
宮下　正彦	弁護士
村上　　智	（株）シマンテック　執行役員 セールス　エンジニアリング担当
本橋　裕次	マカフィー（株）　サイバー戦略室長
安冨　　潔	慶應義塾大学大学院　法務研究科教授
矢橋　康雄	（一社）電気通信事業者協会　業務部長

計１９名（敬称略・５０音順）

（オブザーバ）

内閣官房

総務省

外務省

法務省

経済産業省

消費者庁

事務局：警察庁生活安全局情報技術犯罪対策課

「サイバー犯罪捜査の課題と対策」部会の開催状況

第１回会議　　平成 24 年 11 月 12 日(月)

第２回会議　　平成 24 年 12 月４日(火)

第３回会議　　平成 25 年１月 31 日(木)

第４回会議　　平成 25 年３月 13 日(水)