【パネリスト発表①】「サイバー空間の脅威に対する情報共有組織の意義」

首都大学東京都市教養学部法学系教授　　星　周一郎

はじめに

私からは「サイバー空間の脅威に対する情報共有組織の意義」ということで、今までの基調講演と重なる話もあろうかと思いますが、若干お話をさせていただきます。

1．サイバー空間の位置づけ【図１】

まずはそもそも論になってしまいますが、―10年ぐらい前の話ですが―サイバー空間は、従来、インターネット・サービス・プロバイダ（ISP）の提供する空間であり、ISP事業者は当然のことながら民間企業ですから、そうすると、「ネット空間の中での通信は、どちらかといえば私的な領域における事象である。」という位置付けがなされてきたところがありました。

また、電気通信事業法上の通信の秘密が一つ重要なものとしてありますし、青少年インターネット環境整備法においては、業者の自主的な取組をまず行っていただいて、それを国が尊重するといった規定もあったところから、事業者等の民間の自主規制に委ねられるという面が大きく、それ自体は現在でも重要なファクターであることは間違いないと思われます。

ただ、皆様方も御承知のとおり、サイバー空間は、「民間事業者の提供するサービス空間だから私的な空間である」ということでは片付けられない、重要なインフラになってきています。また、ここ数年、SNS等のコミュニケーション・ツールが急速に発達し、むしろ、サイバー空間での情報のやり取りが現実社会にフィードバックされてくるといったような形での影響力の拡大が見られるようにもなってきています。

2．サイバー空間における安全の意義～「場」としての対策の必要性～【図２】

次に、サイバー空間における安全の意義について見ますと、これも当初は、サイバー空間において行われる不正行為・脅威は、従来型の犯罪―例えば業務妨害罪、詐欺罪、名誉毀損罪、わいせつ物陳列罪といった犯罪など―との関連において、偶然ネットを利用したものに過ぎないという位置付けがなされてきました。逆に言えば、そうしたものの予備罪や準備罪といった性質を帯びるに止まっていたと言えるのではないかと思います。予備罪・準備罪については、日本の刑法は謙抑的であり、したがって、そこに対して刑事法が入っていくのは慎重であるべきだという議論が大きかったように思います。

ところが、先ほども述べたようにサイバー空間がインフラになってきた状況を前提にすると、旧来型の個別の財産犯といった個人法益や風俗犯といった社会法益の侵害には還元できないような、社会生活の基盤を侵害するという、パブリック・インタレストに直接関係してくる公的な保護法益が認められるようになり、それを侵害するのがサイバー空間における脅威・違法行為という扱いになってきているのではないかと思われます。

そこで、サイバー空間については、旧来の個別の犯罪や保護法益に基づいた縦割りのものとして考えていくのではなく、サイバー空間を一つの「場」として捉え、その「場」の安全について、横断的に対策を考えていくことが必要であり、かつ、有効でもあるということになってくると思います。

それに加え、これはサイバーのみに限られる話ではありませんが、そもそも現在の警察活動・刑事法に対する期待が、従来のように犯罪が起こってから事後的に対応することでは足りない、事前に抑えてほしいという

方向に完全にかじを切っています。これを踏まえてサイバー空間における脅威の性質と被害の拡大を考えると、サイバー空間における安全の意義は、ますます重要になってきていると言えます。

３．サイバー空間の安全と官民連携の現状【図３】

以上のように考えますと、社会インフラとしての色彩を強めているサイバー空間の安全対策について、もちろんこれまでも手をこまねいてきたわけではないのは皆様方におかれては釈迦に説法でしょう。時間の関係もありますので、数を絞ってお話しします。

⑴　NISCにおける取組について

一つは平成17年に発足したNISCです。これは、官民をあげた統一的・横断的な情報セキュリティ対策における中核的な機関として、現在でも重要な機能を果たしていることは間違いなく、ここでの取組が非常に大きな成果を上げていることは、改めて申し上げるまでもないかと思います。

ただ一方で、サイバー空間における脅威への対処が―言葉は多少きついかもしれませんが―従来はいわば「守り」としての、受け身としてのセキュリティが中心であり、サイバー空間における安全を脅かす行為に対する積極的な対応には必ずしも力点が置かれてこなかったところがあったのではないかと思われます。

それは、サイバー空間が私的な空間であり、刑事法はなるべく関与すべきではないという、従来あった議論を若干引きずっていたところもあったのかもしれません。しかし、少なくともネットの安全あるいはサイバー空間の安全の確保は、防御のみでは後手の対応にならざるを得ません。もっとプロアクティブに、「誰がやっているのか」という、端的に言えば犯人検挙も考えていかざるを得なくなり、それがますます重要になってきている。そうしないと、根本的な安全確保にはつながらないのではないかと思います。

⑵　インターネット・ホットラインセンターにおける取組について

そういった観点で見ると、インターネット・ホットラインセンター（IHC）はかなり定着した取組となっていて、実績も上げています。

ただ、ホットラインセンターで扱う違法・有害情報は、情報自体が違法であるとか、犯罪が行われている疑いがあるとか、公共秩序の維持の観点から問題のある情報を対象にしています。その意味では、プロアクティブな対応に資するものというところもあるのかもしれませんが、これは発足の経緯等に引きずられている面―すなわち、警察によるサイバーパトロールだけでは十分対応しきれない現状に対し、それを補うかたちでIHCがスタートしたということ―とも無関係ではないように思われます。

そうすると、サイバー空間における脅威に対する先手を打つ対応という観点から見た場合には、やはり、必ずしも制度的に十分な対応がなされていなかったという点は、否定できないようにも思われます。

４．サイバーセキュリティの意識の「転換」【図４】

さらに、セキュリティ対策からプロアクティブな対応への意識の転換、その必要性が強調されるようになってきたのは、これも皆様方には釈迦に説法かとは思いますが、この2～3年ぐらいで幾つかの重大事象が出てきております。

細かく挙げればきりがありませんが、一つは2年前の8月に発生した三菱重工に対するサイバー攻撃です。防衛産業という国にとって重要な意味を持っている企業が、あっさり攻撃されてしまったわけです。そして、同じ年に衆・参両議院に標的型メール攻撃がありました。少なくとも衆議院に関しては全議員のIDとパスワードが流出するという、国の統治機構に関わる、国家の存立に関わる問題が発生しています。

また、これらと若干文脈は違いますが、いわゆる遠隔操作ウイルスの問題もありました。iesys.exeを使い、遠隔操作による業務妨害行為の書き込みがなされたことについて、残念ながら捜査機関の第一線まで十分な情報共有ができていなかったがために、冤罪事件を引き起こしてしまいました。

さらに、日本からすればまだ他人事のようにも見えますが、海を隔てた反対側の韓国において、銀行のATMが使えなくなる、放送がうまくできなくなるといったサイバーテロがありました。これは決して他人事ではなく、我が国でいつ起こってもおかしくない状況になってきています。

このように、サイバーセキュリティが従来の犯罪の延長では済まされない脅威になってきているということが、刑事法は謙抑的であるべきだという立場からも、「もう少し積極的な関与が必要だ。」という方向に動いてきた大きなきっかけではないかと思っています。

5．「日本版NCFTA」に求められるもの【図５】

(1)　捜査活動をより重視した情報共有体制の構築

そういった文脈の中で、今回、日本版NCFTAという議論が出てきているのではないかと、私は考えています。

ここには、先ほど申し上げたとおり、サイバーセキュリティの意識の転換があると思います。問題が起こった、それに対するウイルス対策や新たなセキュリティ体制の構築といった受け身の対応では十分ではなく、誰がどういう手段を使ってどういうルートで行っているのかを積極的に捜査・調査をしていく。端的に言ってしまえば「犯人検挙」というかたちに持っていかないと、なかなか安全が十分に確保できない。そのための捜査の重要性が高まってきているのではないかと思います。

こうしたことに対し、法律においてもまだまだ不十分な点があろうかと思いますが、不正アクセス禁止法も改正され、法定刑の引き上げ、対象行為の拡大もありました。

また、刑法改正により、大きな懸案であったウイルス罪も成立しました。そこでは、ウイルスに感染したコンピュータが業務妨害をされたといった捉え方ではなく、文書偽造罪の後に規定され、正に社会法益に対する罪として位置づけられるものになっています。これは刑事実体法の側面での対応と言えるかと思います。もちろん、それと同時に刑事訴訟法の改正があったことは、ここで申し上げるまでもないことかと思います。

以上を前提にしますと、今後、より重要視されるべきなのは、サイバー犯罪の捜査活動を従来以上に重視した情報共有体制を構築していくことではないかということです。

もちろん、サイバー空間における脅威への対応を捜査機関だけで行うことができるのかということになってくると、これだけ偏在的な存在であるサイバーに対して、一つの機関だけでは対応しきれないことは誰も異論のないところであります。正に、産学官の協力が必要になってくるのではないかと思います。

(2)　捜査情報の適正管理

ア　捜査で得られた情報の蓄積と活用の在り方について

他方、セキュリティ情報に関する情報の共有ということではなく、捜査に関わる情報の共有ということになってくると、これはサイバーに限られたことではありませんが、捜査情報はセンシティブ情報の一つの典型ですから、こういったものが適正に管理できるのかが極めて重要なファクターに、すなわち、情報共有組織体制を作る上で考えなければならない要素になってくるかと思います。

捜査の結果得られた情報のデータベース化は、これまで必ずしも十分に考えられてこなかったところだと言えます。刑事訴訟法の枠組みそのものがそうであり、強制捜査において捜索・差押えをするという場面が典型ですが、どういう場合に強制力を使って情報を取ることができるか。情報を取るという側面に関して、刑事訴

訟法は強い関心を持っております。そして、これまでの捜査実務もそこを中心に適正な捜査をやってきているわけですが、その裏側として取った情報をどう扱うのかは、あまり考えられていないわけです。

刑事訴訟法においては、特に強制捜査の場合には被疑事実が特定されているので、令状によって得られた情報はその事件だけに用いるというのが、無意識的に前提にされてきたかと思います。もちろん、その考え方も大事ではありますが、サイバー犯罪は展開が非常に早く、専門性が高い犯罪です。インシデントが起こる度に一から捜査を開始しているようでは間に合わないという現実がある中で、取った情報をデータベース化し、他の事件にも使えるといった枠組みも、今後考えていかざるを得ないのではないでしょうか。

実は、こうした枠組みについては、刑事訴訟法において、明文規定はないものの、禁止もされていないと私自身は考えています。色々な体制作りの中で、こうしたことも考えていかざるを得ないと思っています。

イ　ログの保存について

もう一つ捜査情報に関して申し上げれば、「iesys.exeというウイルスが出回っている。だから気を付けよう。」では、やはり不十分です。そうではなくて、誰が作ったのか、どこからどういう形で配布されたのか、誰が使ったのかというところまで押さえないと、犯人の検挙につながっていきません。

ただ、そうなると、どうしてもログの保存という問題が出てきます。ログの保存に関しては、インターネット・サービス・プロバイダは民間企業ですが、広い意味でのCSR[1]といった中でサービスを提供する裏側として、ログについても一定程度の保存をお考えいただければと思っています。もちろん、できないことを強制するわけにはいかないので、相応のインセンティブは考えていかざるを得ないとは思いますが、そうしたものを含めた情報共有体制について、考えていく必要があろうかと思います。

---

[1] Corporate Social Responsibility の略。企業の社会的責任のこと。

【発表資料】

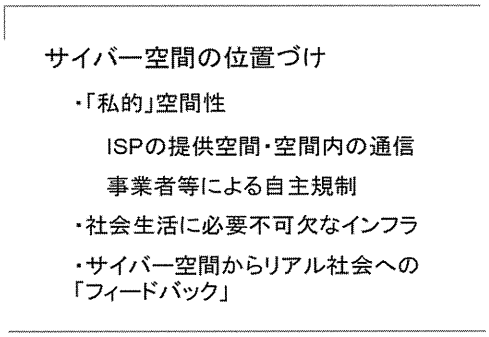

図１

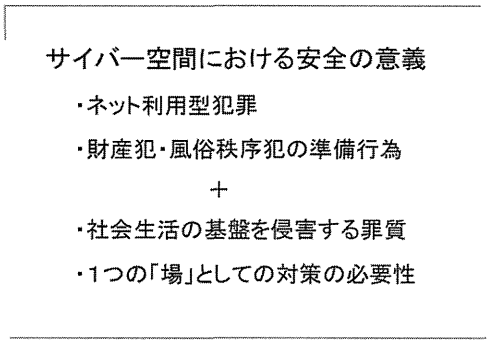
サイバー空間における安全の意義
・ネット利用型犯罪
・財産犯・風俗秩序犯の準備行為
＋
・社会生活の基盤を侵害する罪質
・1つの「場」としての対策の必要性

図2

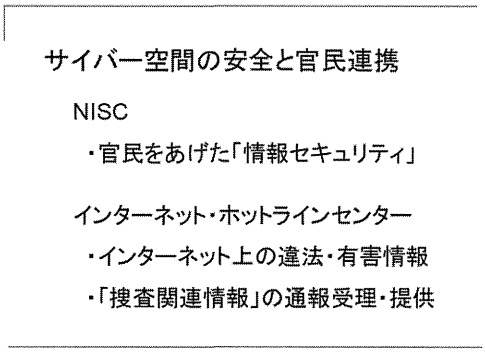
サイバー空間の安全と官民連携
NISC
・官民をあげた「情報セキュリティ」
インターネット・ホットラインセンター
・インターネット上の違法・有害情報
・「捜査関連情報」の通報受理・提供

図3

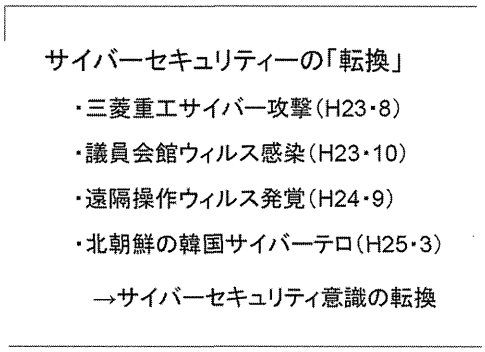
サイバーセキュリティーの「転換」
・三菱重工サイバー攻撃（H23・8）
・議員会館ウィルス感染（H23・10）
・遠隔操作ウィルス発覚（H24・9）
・北朝鮮の韓国サイバーテロ（H25・3）
→サイバーセキュリティ意識の転換

図4

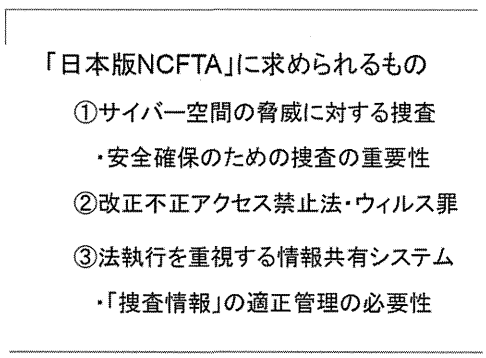
「日本版NCFTA」に求められるもの
①サイバー空間の脅威に対する捜査
・安全確保のための捜査の重要性
②改正不正アクセス禁止法・ウィルス罪
③法執行を重視する情報共有システム
・「捜査情報」の適正管理の必要性

図5

【パネリスト発表②】「警察におけるサイバー犯罪対策」

警察庁生活安全局情報技術犯罪対策課長　緒方　禎己

はじめに【図１、２】

まず、本日、基調講演をいただいたアメリカ NCFTA の CEO 兼理事長のマリア・ヴェロ氏、田中学長、近藤様の御三方に対し、大変示唆に富む貴重なお話を伺わせていただいたことに深く感謝を申し上げます。

今日のフォーラムでは、私は産学官連携における「官」を代表する立場と心得ています。そこで、しばらくお時間を頂戴し、始めにサイバー犯罪の現状について簡単に御説明し、次に、現在行われている官民の連携について御紹介をし、最後に今後の産学官連携強化の取組への警察の期待を申し述べたいと思います。

１．サイバー犯罪の現状【図３、４】

まず、サイバー犯罪の現状ですが、サイバー犯罪の検挙件数は、昨年、過去最高を記録しました。量・質の両面で、サイバー空間の脅威は増大・深刻化しています。

近年のサイバー犯罪の特徴的な傾向や手口について、四点ほど簡単に御説明します。

まず、遠隔操作です。

昨年発生した遠隔操作ウイルスを用いた犯行予告事案は、まだ皆さんの記憶に新しいところかと思います。インターネットを使っているだけで本人の知らないうちに犯罪に荷担させられてしまう恐怖、これは今や誰にとっても身近で現実のものになっています。

次に、スマホアプリによる情報流出です。

スマホの急速な普及に併せて様々なアプリが出現する中で、個人情報を盗み取る目的の不正なアプリが急増しています。昨年６月には、電話帳等に登録されている個人情報を勝手に収集し、これを部外に送信するアプリを動画再生アプリと偽ってネット上に公開していた被疑者を、警視庁がウイルス供与罪等で検挙しました。

そして、DDoS 攻撃です。

DDoS 攻撃は、ウェブサイトの閲覧ができなくなる事態を引き起こすほか、攻撃に用いられるボットネットは攻撃主による遠隔操作が可能です。一度の命令で膨大な数のコンピュータを同時に動かすという特徴を持つことから、迷惑メールの大量送信等、様々な違法行為に悪用されます。

最後に、インターネットバンキングに係る不正送金事案です。

これはインターネットバンキング利用者の端末をコンピュータウイルスに感染させ、ID、パスワード等を盗み取り、それを基に不正アクセスをし、不正送金を行うものです。

この種の事案の被害は、平成 23 年に顕在化しました。この年は年間で３億円を超える被害をもたらし、金融機関に打撃を与えましたが、その後、金融機関の側の対策も奏功し、昨年は被害額を 5,000 万円弱にまで抑え込むことができました。ところが、今年に入って被害が急増し、８月末現在で被害額は４億 7,500 万、直近の９月 20 日現在の数字では、５億 5,000 万にまで被害が拡大し、これまで過去最悪であった平成 23 年中の被害額を既に大幅に上回る危機的な事態に至っています。

被害の発生は全国に及んでいるほか、個々の事案を見ても、被害口座の名義人の居住地と現金引き出し場所が大きく離れているなど、時間的・場所的制約を受けないサイバー空間の特性を最大限に悪用した、組織的背景を有する者らによる犯行であり、現在、全国警察を挙げて捜査を進めております。

２．警察と民間事業者等との連携【図５～８】

次に、現在行われている警察と民間事業者等との連携について、四点御説明します。

⑴　コンピュータウイルスに係る情報の共有について

まず、コンピュータウイルスに係る情報の共有についてです。

昨年の遠隔操作ウイルス事案では、犯行に使用された新種の不正プログラムを警察からアンチウイルスベンダーに提供し、アンチウイルスベンダーにおいてパターンファイルを作成し、不正プログラムを駆除するためのソフトを速やかに利用者に配布するなどして、被害の拡大防止を図りました。

実は警察の伝統的な考え方からすると、捜査の過程で警察が把握したこの種の情報は、正に犯罪の証拠であるとともに、被疑者しか知らない秘密の暴露に属するものであり、特に捜査の初期段階において、警察以外に提供することはもってのほかということになります。しかし、この種のサイバー犯罪においては、捜査の都合から来るそうした要請よりも、更なる被害拡大をいちはやく防止することの方が優先されるべき、との判断によるものであります。

今年の４月には、警察とアンチウイルスベンダー等との間でこの種の情報提供に関して必要なルールを盛り込んだ協定を締結し、現在、インターネットバンキングに係る不正送金事案においてもこの協定に基づく情報共有を進めています。

⑵　ボットネット対策について

次に、ボットネット対策について、成功事例を交えてお話しします。

この事例は、インターネットバンキングに係る不正送金事案に関し、国内の情報セキュリティ会社から警察庁に対してコンピュータウイルスの指令サーバに関する情報が寄せられ、それを基に当該サーバの管理者から警察においてアクセスログ等を入手し、これを分析することによって、この指令サーバと通信を行っている、コンピュータウイルスに感染している可能性が高い国内約１万6,000の端末を割り出し、関係するプロバイダを通じて当該端末の利用者に対して注意喚起を行った、というものです。

こうした指令サーバが実際に特定され、その通信状況が具体的に把握されることは、極めて稀です。民間事業者の持つ高い知見と技術に警察の捜査権限が結びつくことで、迅速な事態の解明が可能となった好事例と考えています。

⑶　共同対処協定の締結について

次に、共同対処についてです。

サイバー犯罪は、警察への通報が行われにくく、その結果、被害が潜在化しやすいことが特徴の一つとしてあります。しかし、これを放置しておくと、警察がサイバー犯罪の実態を掴めぬまま、言い換えれば、犯罪者が捜査の対象とされず野放しとなり、サイバー空間の脅威が増大していくおそれがあります。

そこで、昨年６月以降、各都道府県警察と民間事業者との間で共同対処協定を締結し、事業者がサイバー犯罪を認知した際の迅速な警察への通報や警察による積極的な事件化等を確認しました。今年上半期までに、オンラインゲーム企業、金融機関等170を超える団体との間でこの協定を締結しています。

⑷　違法・有害情報対策について

最後に、違法・有害情報対策についてです。

インターネット上には、流通する膨大な量の情報に紛れて、児童ポルノの画像や覚せい剤の密売等に関する違法情報、さらには爆発物の製造方法や集団自殺の呼びかけ等の有害情報が氾濫しています。警察では、一般のイ

ンターネット利用者からの通報を受理し、その中から予め定められた基準に従って違法情報・有害情報を選別し、警察への通報やサイト管理者等への削除依頼を行うインターネット・ホットライン業務を平成 18 年から民間に委託して行っています。

昨年のインターネット・ホットラインセンターの通報受理件数、違法・有害情報該当件数は、いずれも過去最多を記録しています。このうち、警察による対応が必要な情報については、警視庁に置かれた情報追跡班において当該情報の発信元に関する捜査を一元的に行い、その結果に基づいて関係道府県警察が事件捜査に着手するという、全国協働捜査方式が既に定着し、相当の実績を収めているところです。

３．警察としての産学官連携への期待【図９～11】

⑴　新たな枠組みとしての産学官連携

以上申し述べたとおり、警察ではサイバー犯罪捜査の分野において、これまでも民間との連携について様々な取組を推進し、一定の成果を収めてきました。

他方、昨年の遠隔操作ウイルスを用いた犯行予告事案、そして、被害が急速に拡大しているインターネットバンキングに係る不正送金事案等に象徴されるサイバー空間の脅威の飛躍的な高まりを背景に、警察として民間企業や学術団体との間で、従来とは次元の異なるレベルで、共にサイバー空間の脅威と戦うパートナーとして、新たな連携の枠組みを構築する必要性を感じています。

⑵　経験を通じて警察が学んだこと

一連の経験を通じて我々警察が学んだことの一つは、警察は、サイバー空間で起きていること、また近い将来起き得ることを、必ずしも十分に把握しているわけではないということです。

確かに警察は犯罪捜査等の警察活動を通じて、その限りで切り取ったサイバー空間の特定の脅威については、誰よりも詳細にこれを知り得る立場にあります。しかし、サイバー空間全体を隅々まで把握しているわけではありません。

この点、サイバー空間の脅威に日々その身を晒している民間企業は、サイバー空間で起きていること――この中にはサイバー犯罪の新たな手口あるいはサイバー犯罪に悪用可能な技術の動向を含みますが――についての生の情報を持ち、また、近い将来起き得ることについてもいち早く認識しています。

我々が学んだことのもう一つは、サイバー犯罪捜査の中には、警察の力だけで全容解明を目指すことが効率的ではないものがあるということです。この点、情報セキュリティ関連企業やアンチウイルスベンダー等による捜査への協力の取組は始まっていますが、まだまだ緒に就いたばかりです。これを、より恒常的な協力のための安定した枠組みに発展させる必要があります。

つまり、現状では、官も民もそれぞれにサイバー空間の脅威への対処の経験を有しているものの、それを全体で蓄積・共有する仕組みがないということです。警察、民間企業、学術団体のそれぞれが持つ経験と知見を、その場限り、当事者限りのものとせずに、これを蓄積・共有することで、全体としてサイバー空間の脅威への対処の精度と練度を向上させることが必要だと考えています。

⑶　サイバー空間全体を俯瞰した上で脅威の根本を断つ対処　～先制的・包括的対応～

以上の現状を言い換えれば、サイバー空間全体を俯瞰した上で、しかも脅威の根本を断つという対処が不足しているということです。

例えば、フィッシングサイトが立ち上がったことを認知し、これをテイク・ダウンすることは、民間企業でも可能であり、現に行っていただいております。しかし、それだけでは、こちらをつぶしてもまた別なところで立

ち上がるという、いたちごっこが続くだけというのも事実です。

コンピュータウイルスに感染した端末に指令を出すC&Cサーバを見つけ出すことは、民間でも可能であり、むしろ民間の方がより優れています。しかし、そのサーバのアクセス記録等を速やかに入手することは、民間では困難です。ここに、産業界の持つ情報と学術団体の持つ知恵と、「官」、すなわち警察の持つ権限を結合した、新たな枠組みが必要な所以があります。

こうした問題意識を踏まえ、警察として新たな産学官連携の取組に期待することを一言で申し上げれば、産学官がそれぞれ持つ知見と技術を持ち寄ることでサイバー空間の脅威を的確に把握し、脅威の内容や程度等に応じて速やかにこれを軽減あるいは無効化することです。従来の事後的・個別的な対応を超え、先制的・包括的な対応が可能になるものと期待しています。

⑷　警察が産学官連携に参画する意義

法執行機関である我々警察が参画することの意義ですが、一つは、単なる情報共有や注意喚起にとどまらず、対処の手段として捜査権限の行使に基づく事態の解明が可能となり、迅速な事態の収拾が担保されるということです。

被害の拡大・継続を阻止することにとどまらず、犯罪の実行者や動機等を解明することで脅威の根本を断つことが可能になり、脅威への対処の幅が大きく広がるものと認識しています。

もう一つは、海外の法執行機関とのネットワークを活用することで、サイバー空間をグローバルに俯瞰することが可能になるということです。

ただ、こうした機能を果たすためには、産学官が保有する情報を共有し分析する仕組みが不可欠です。多種多様な分野、業界を幅広くカバーすることに加え、共有された情報について産学官による重層的な分析が行われ、その分析結果もまた共有され、検証されることが大事であろうかと思います。産業界、学術団体には、それぞれの知見と経験に基づく分析があります。我々警察には捜査機関としての独自の分析がある。それらが有機的に結合することで、複眼的な分析が可能となり、脅威の真相、実態により近づくことができると思っています。

⑸　産学官連携における留意事項

最後に、産学官連携における留意事項について、三つほどお話しします。

まずは、当然ですが、産学官それぞれにとってメリットがあるということです。この三者のうちのいずれかの一方的な負担と犠牲の上に成り立つような制度では、長続きはしません。情報の流れ一つをとっても、双方向のものであることが大事です。産業界や学術団体から警察に対して情報が流れるのみで、警察から一切情報のフィードバックがないということでは、機能などしないでしょう。

警察としても、個別具体の事件捜査に支障を及ぼさない形での情報の提供は十分に可能であり、また、しなければならないと考えています。いずれにせよ、産学官が対等なパートナーとして参画できる枠組みが必要と考えています。

次に、情報が適切に取り扱われることです。連携の重要な基盤は、情報の集約と分析です。その前提は、信頼できるメンバーのみが情報にアクセスできること、そして保秘等の観点から情報の取扱いが適切なものであること、さらにプライバシー保護等の観点から蓄積される情報の匿名化等について適切な措置が講じられていること、これらが不可欠です。こうしたことが担保されて初めて、産業界も情報を提供することが可能になるものと考えています。

最後に、既存の組織等との間で適切な連携が図られることです。法執行機関である警察が参画する産学官連携の仕組みは、捜査権限の行使に基づく事態の解明、あるいは海外の法執行機関とのネットワークを活用できる等

の点で、既存の情報共有を図る他の組織や枠組みにはない特徴を持つものです。したがって、この新たな取組、新たな枠組みは、既存の他の情報共有の組織、仕組みとも十分に共存し得るものであり、むしろそうした重層的・多層的な仕組みこそが必要だと考えています。

４．最後に

以上、縷々申し上げましたが、警察庁では既にこの新たな産学官連携の在り方について、産業界・学術団体御出身の有識者委員の方々とともに検討に着手しています。本日のこのフォーラムの結果等も踏まえて検討作業を加速させ、本日のフォーラムでも議論になったアメリカのNCFTAを参考にしつつ、我が国の法制度や国情に見合った「日本版NCFTAの創設」に向けて、議論と検討を進めてまいりたいと考えております。

【発表資料】

警察におけるサイバー犯罪対策

警察政策フォーラム
平成２５年９月２６日

警察庁生活安全局
情報技術犯罪対策課

図１

目次

① サイバー犯罪の現状
② 警察と民間事業者等との連携
- ✓ アンチウイルスベンダー等との情報共有
- ✓ ボットネット対策
- ✓ 共同対処
- ✓ インターネット・ホットラインセンター

③ 警察としての産学官連携への期待
- ✓ 現状の課題
- ✓ 産学官連携への期待
- ✓ 留意事項

図２

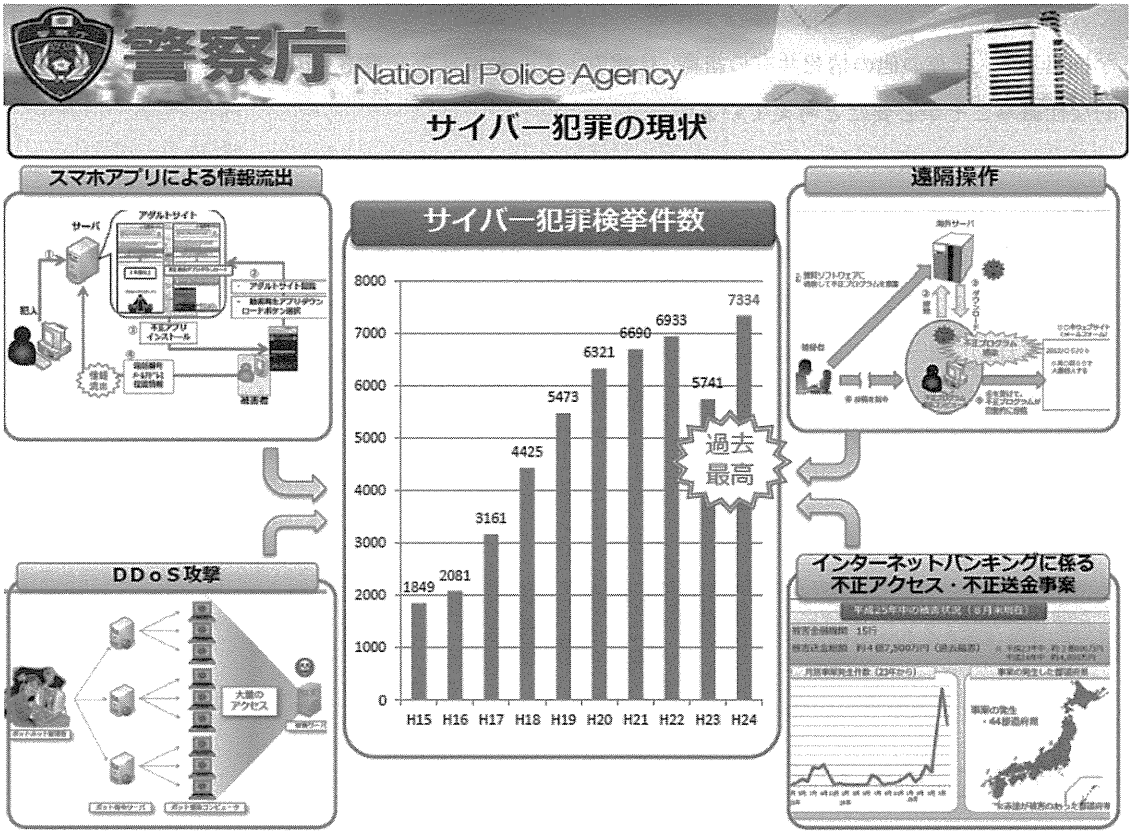
警察庁
National Police Agency
サイバー犯罪の現状
スマホアプリによる情報流出
サーバ
アダルトサイト
犯人
不正アプリインストール
情報流出
被害者
サイバー犯罪検挙件数
8000
7000
6000
5000
4000
3000
2000
1000
0
1849
2081
3161
4425
5473
6321
6690
6933
5741
7334
過去最高
H15 H16 H17 H18 H19 H20 H21 H22 H23 H24
遠隔操作
海外サーバ
ダウンロード
不正プログラム
DDoS攻撃
大量のアクセス
インターネットバンキングに係る不正アクセス・不正送金事案
事案の発生
・44都道府県

図３

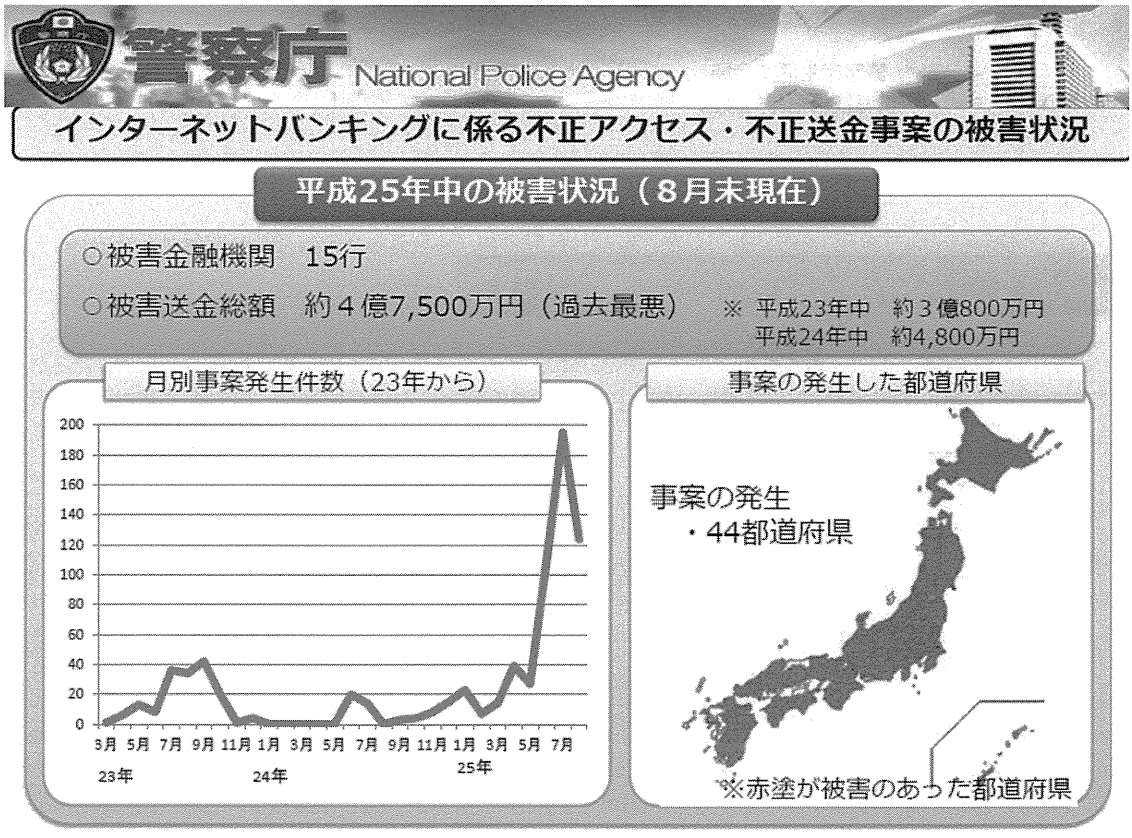
警察庁
National Police Agency
インターネットバンキングに係る不正アクセス・不正送金事案の被害状況
平成25年中の被害状況（８月末現在）
○被害金融機関　15行
○被害送金総額　約４億7,500万円（過去最悪）
※ 平成23年中　約３億800万円
平成24年中　約4,800万円
月別事案発生件数（23年から）
200
180
160
140
120
100
80
60
40
20
0
3月 5月 7月 9月 11月 1月 3月 5月 7月 9月 11月 1月 3月 5月 7月
23年
24年
25年
事案の発生した都道府県
事案の発生
・44都道府県
※赤塗が被害のあった都道府県

図４

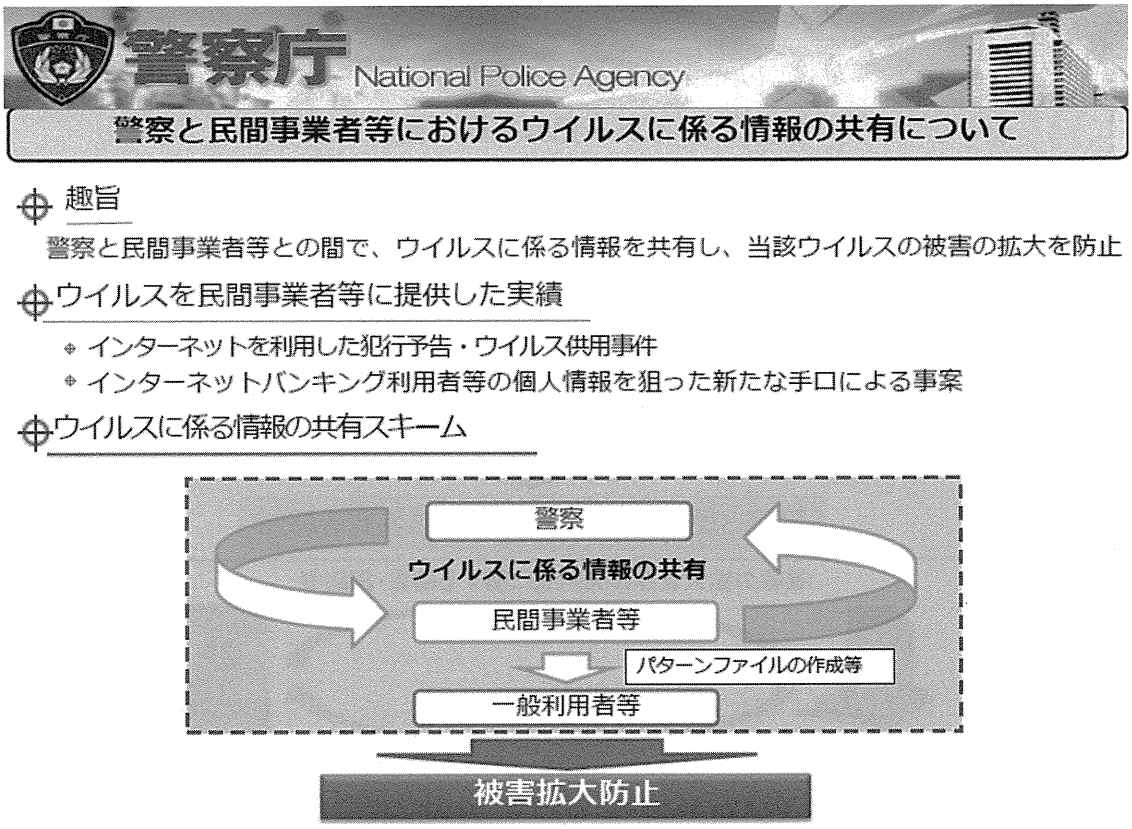
警察庁 National Police Agency
警察と民間事業者等におけるウイルスに係る情報の共有について
趣旨
警察と民間事業者等との間で、ウイルスに係る情報を共有し、当該ウイルスの被害の拡大を防止
ウイルスを民間事業者等に提供した実績
インターネットを利用した犯行予告・ウイルス供用事件
インターネットバンキング利用者等の個人情報を狙った新たな手口による事案
ウイルスに係る情報の共有スキーム
警察
ウイルスに係る情報の共有
民間事業者等
パターンファイルの作成等
一般利用者等
被害拡大防止

図５

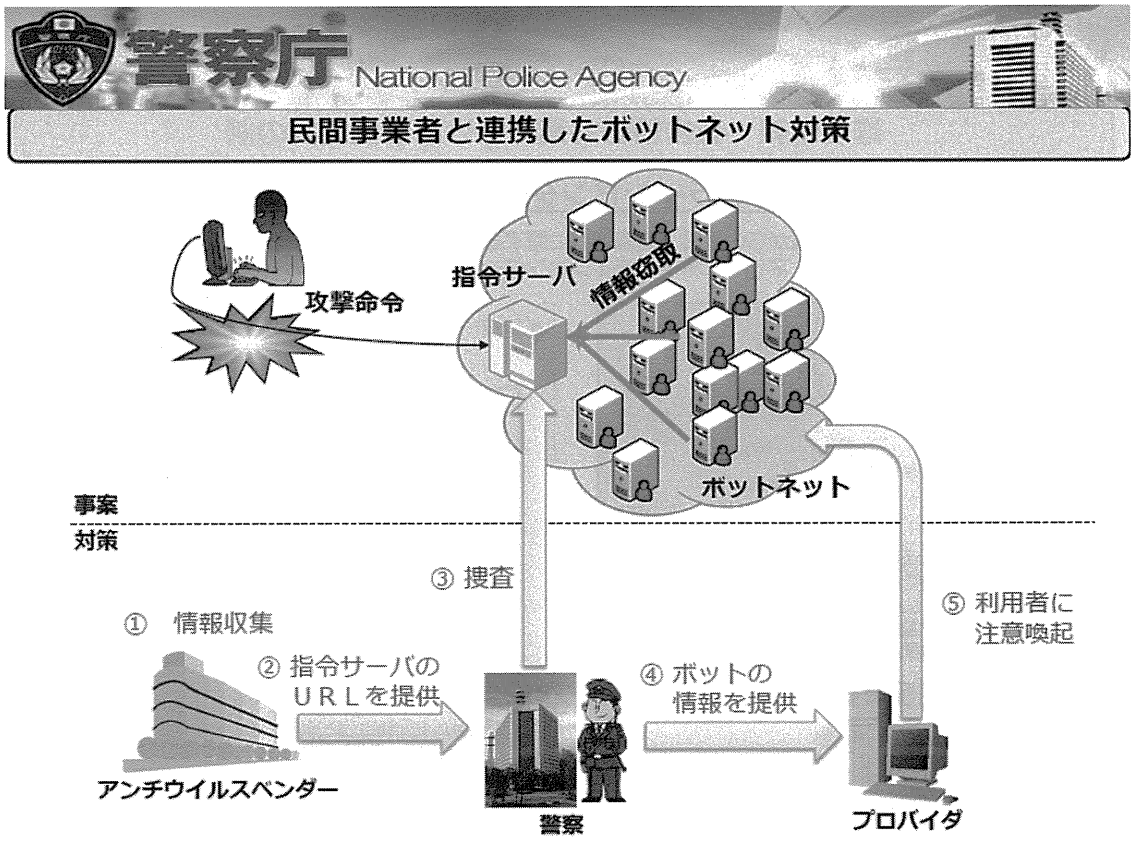
警察庁 National Police Agency
民間事業者と連携したボットネット対策
攻撃命令
指令サーバ
情報窃取
ボットネット
事案
対策
③ 捜査
① 情報収集
② 指令サーバのＵＲＬを提供
④ ボットの情報を提供
⑤ 利用者に注意喚起
アンチウイルスベンダー
警察
プロバイダ

図６

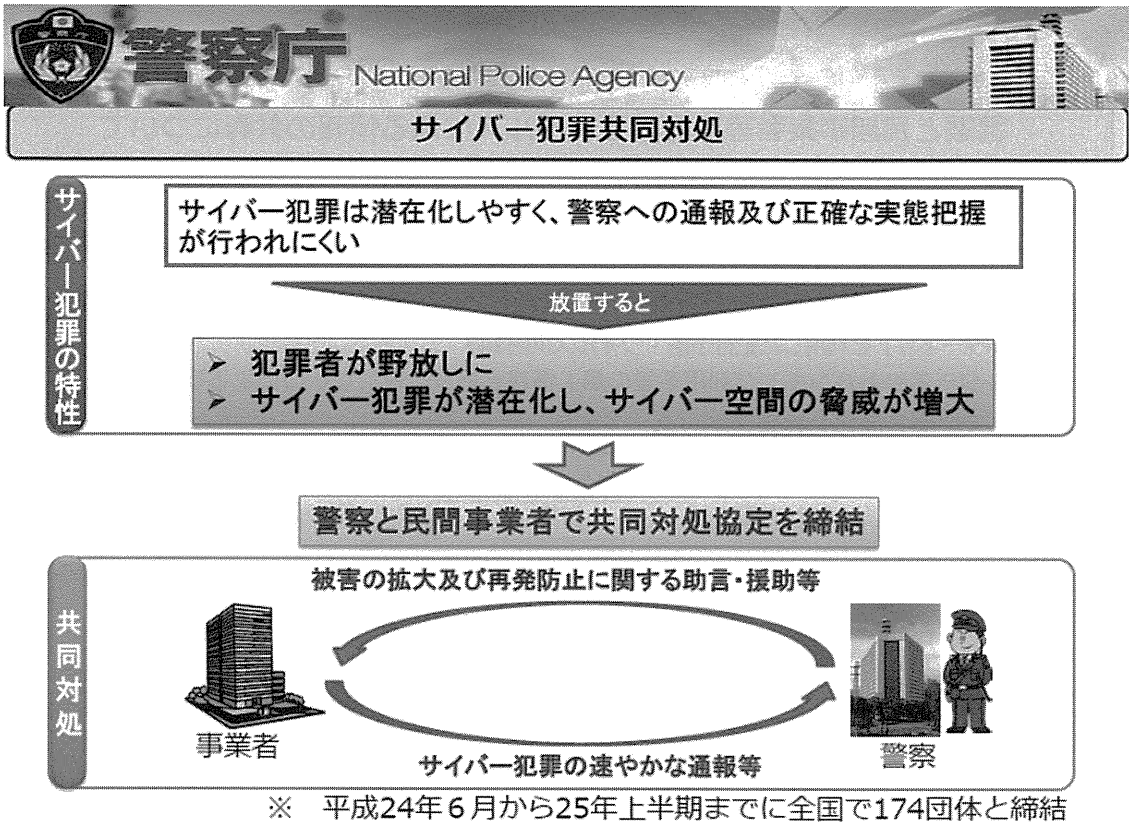
警察庁 National Police Agency
サイバー犯罪共同対処
サイバー犯罪の特性
サイバー犯罪は潜在化しやすく、警察への通報及び正確な実態把握が行われにくい
放置すると
犯罪者が野放しに
サイバー犯罪が潜在化し、サイバー空間の脅威が増大
警察と民間事業者で共同対処協定を締結
共同対処
被害の拡大及び再発防止に関する助言・援助等
事業者
サイバー犯罪の速やかな通報等
警察
※　平成24年６月から25年上半期までに全国で174団体と締結

図７

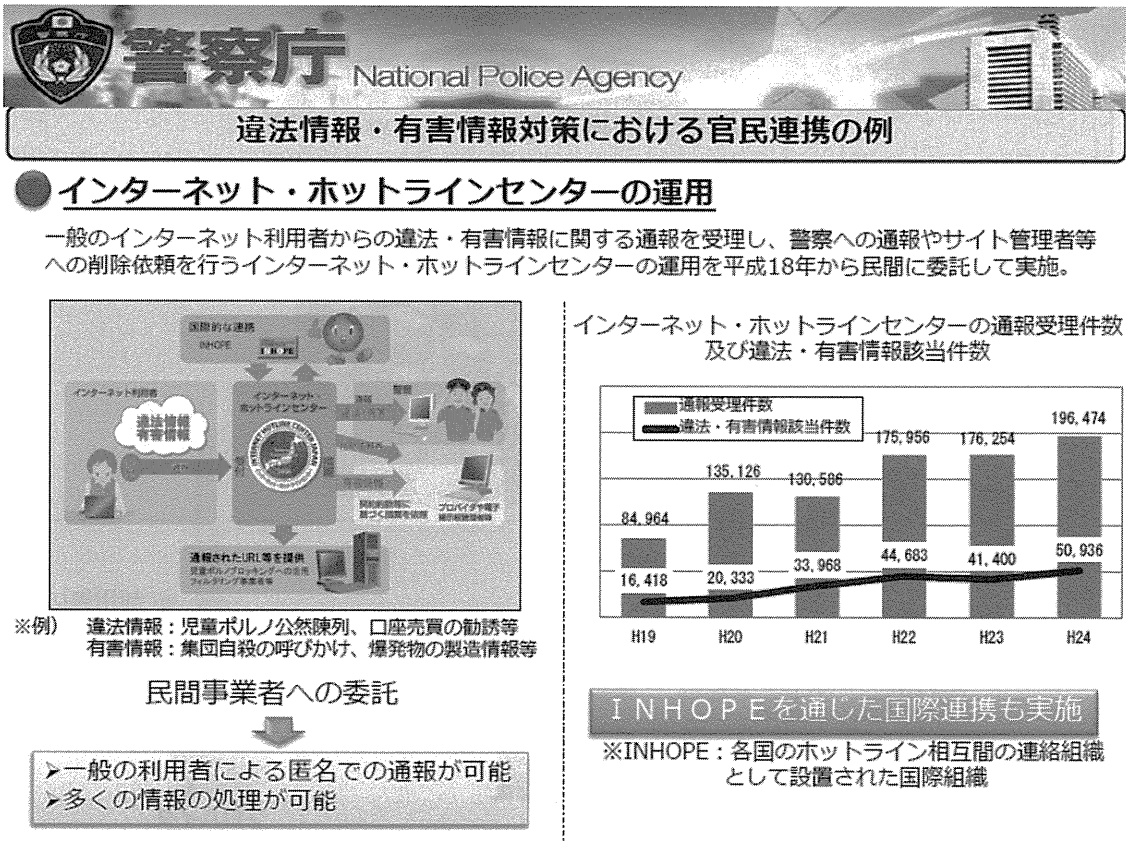
警察庁 National Police Agency
違法情報・有害情報対策における官民連携の例
インターネット・ホットラインセンターの運用
一般のインターネット利用者からの違法・有害情報に関する通報を受理し、警察への通報やサイト管理者等への削除依頼を行うインターネット・ホットラインセンターの運用を平成18年から民間に委託して実施。
※例）　違法情報：児童ポルノ公然陳列、口座売買の勧誘等
有害情報：集団自殺の呼びかけ、爆発物の製造情報等
民間事業者への委託
一般の利用者による匿名での通報が可能
多くの情報の処理が可能
インターネット・ホットラインセンターの通報受理件数及び違法・有害情報該当件数
通報受理件数
違法・有害情報該当件数
84,964
16,418
135,126
20,333
130,586
33,968
175,956
44,683
176,254
41,400
196,474
50,936
H19
H20
H21
H22
H23
H24
ＩＮＨＯＰＥを通じた国際連携も実施
※INHOPE：各国のホットライン相互間の連絡組織として設置された国際組織

図８

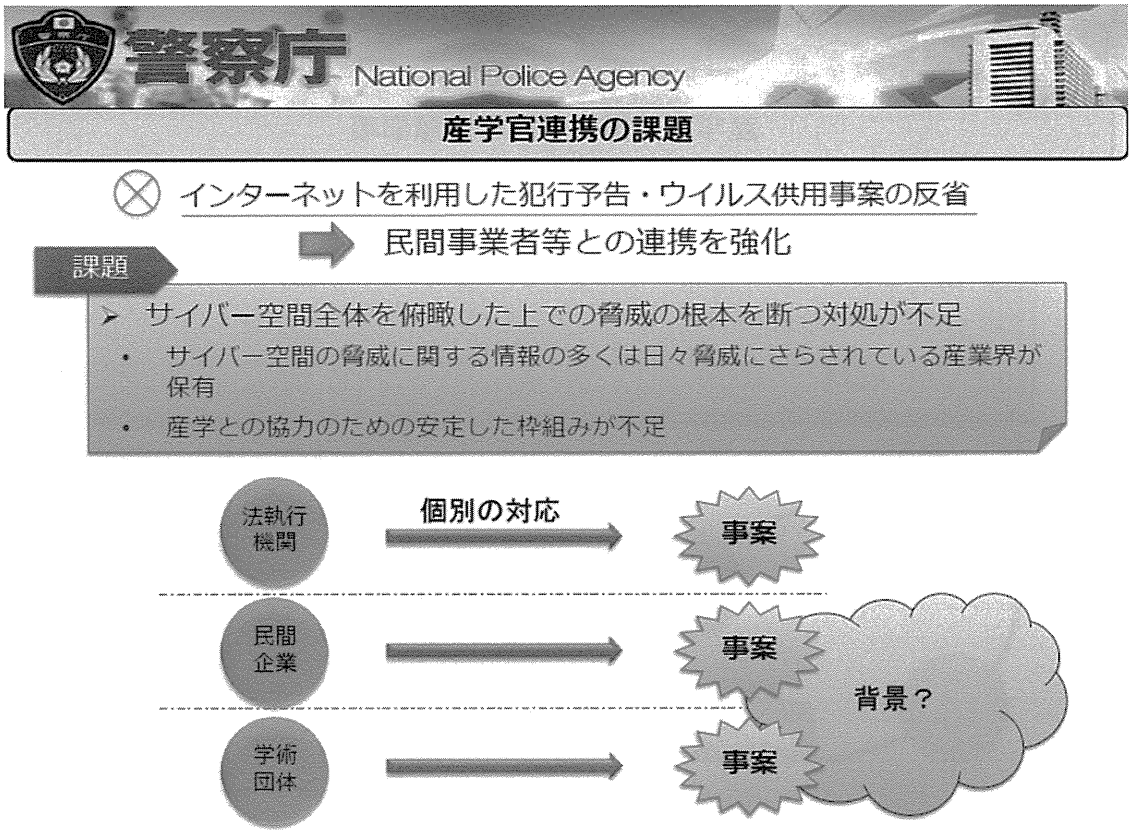
警察庁 National Police Agency
産学官連携の課題
インターネットを利用した犯行予告・ウイルス供用事案の反省
民間事業者等との連携を強化
課題
サイバー空間全体を俯瞰した上での脅威の根本を断つ対処が不足
サイバー空間の脅威に関する情報の多くは日々脅威にさらされている産業界が保有
産学との協力のための安定した枠組みが不足
法執行機関
個別の対応
事案
民間企業
事案
背景？
学術団体
事案

図９

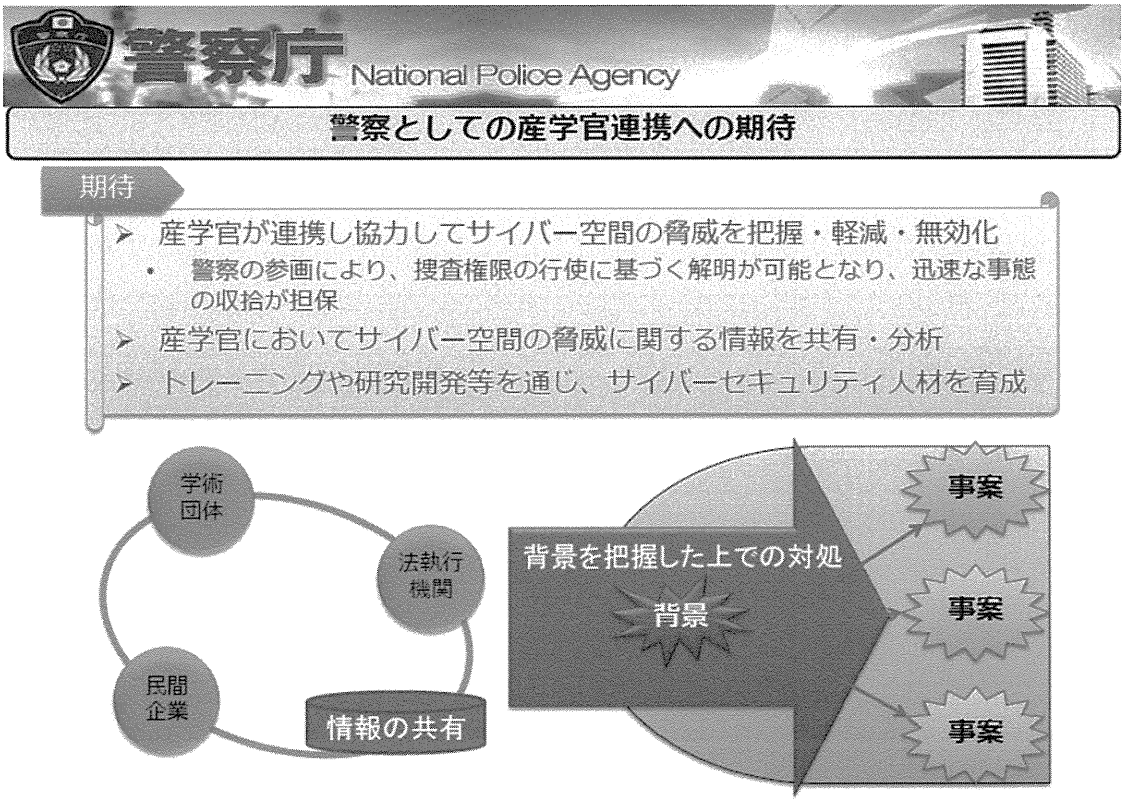
警察庁 National Police Agency
警察としての産学官連携への期待
期待
産学官が連携し協力してサイバー空間の脅威を把握・軽減・無効化
警察の参画により、捜査権限の行使に基づく解明が可能となり、迅速な事態の収拾が担保
産学官においてサイバー空間の脅威に関する情報を共有・分析
トレーニングや研究開発等を通じ、サイバーセキュリティ人材を育成
学術団体
法執行機関
民間企業
情報の共有
背景を把握した上での対処
背景
事案
事案
事案

図10

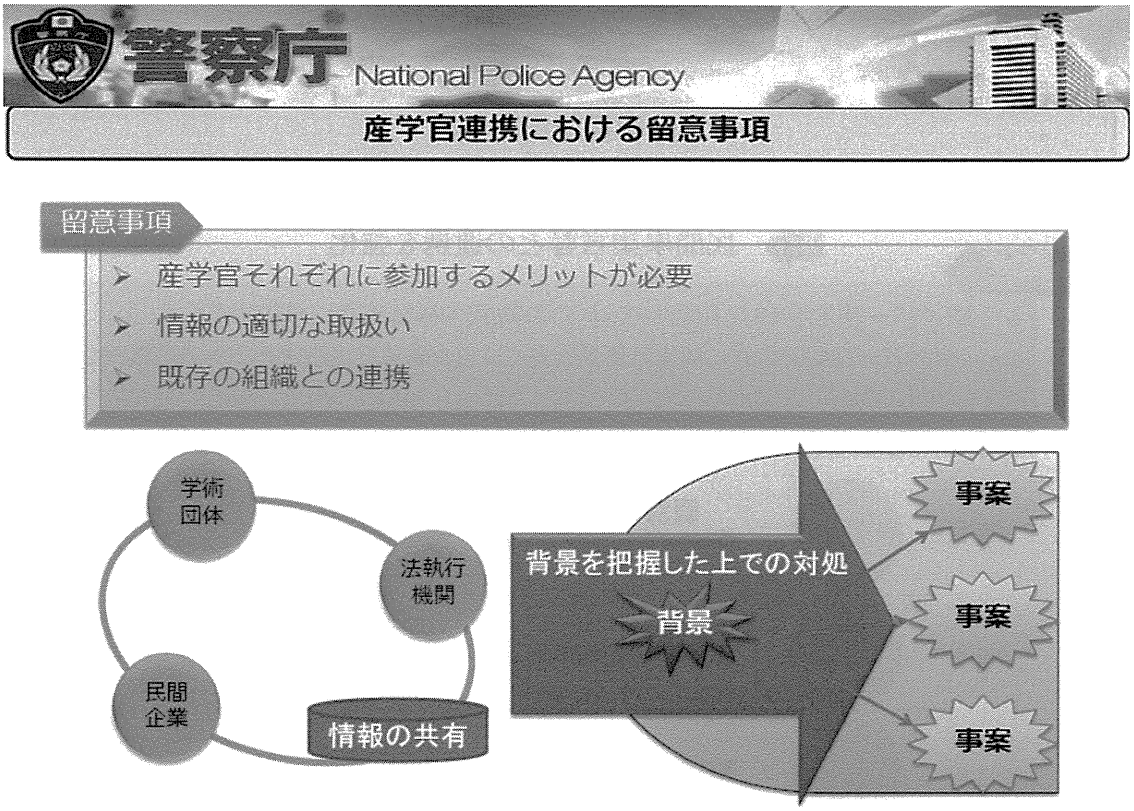
警察庁 National Police Agency
産学官連携における留意事項
留意事項
産学官それぞれに参加するメリットが必要
情報の適切な取扱い
既存の組織との連携
学術団体
法執行機関
民間企業
情報の共有
背景を把握した上での対処
背景
事案
事案
事案

図11

【ディスカッション（討論）】

佐々木　これから、産学官の連携の在り方について議論をしていきたいと思います。

これまで皆様の御講演・御発表、あるいは会場から事前にいただいた期待・要望に関する御意見、本日いただいた御質問なども踏まえ、論点を三つに絞りました。一つ目は情報集約あるいは共有、管理の在り方について。二つ目が人材育成とトレーニング、研究開発について。そして、三つ目が既存の組織との関係についてです。この三つに絞ってまずは議論を進めていきたいと思います。

１．情報集約・共有・管理の在り方

佐々木　まず、情報集約あるいは共有、そして管理の在り方について議論していきます。会場からは、「『日本版 NCFTA』の枠組み自体への期待は非常に大きいものの、企業の側では自らのセキュリティレベルを開示すること等に抵抗感もあるのではないか。」といった御意見、「具体的なインシデント情報は企業の中ではトップシークレットである。」といった御意見もありました。また、サイバー空間は無限定であるので、海外との連携の在り方も課題になるように思われます。

こうした点について、情報共有をためらわせる要因をいかにして打破し、円滑に運用していくか。世界的グローバル企業としてサイバー空間の脅威を最も直接に受ける立場におられる近藤執行役員、この点はいかがでしょうか。

近藤　基調講演の中でもお話しさせていただき、また、マリア・ヴェロ様にも途中でお話を伺ったことですが、一つは、この仕組みが企業にとってプラスになる、インセンティブになるということ、それが非常に重要だと思います。

米国の NCFTA を見ますと、我々メーカーという立場だけではなく、脅威のターゲットになり得る色々な企業体が入っています。そこが「自分たちの情報を開示することで安全な空間を保障できる。」「それによってお客様に対してきちんとしたサービスを提供できる。」と感じることができるよう、まずはフィードバックがきちんとなされることが重要かと思います。

その上で、企業を含めた情報提供者の情報をどう守るかについて、きちんとした枠組みをここで作っておく必要があります。匿名化というのもあるし、米国の場合、例えばトレード・シークレットに関わるデータやフォーミュラがあれば、それは隠すという話もございました。何が企業をためらわせているのかというきちんとした調査をして、それに対してここは保障されるということを、透明性を持って出していくところが非常に重要ではないかと思います。

佐々木　田中教授、追加のコメントがあればお願いします。

田中　情報を収集して共有していくときにためらう、企業にとってみると難しいというのは、最初はそうだと思います。これは、先ほど近藤さんがおっしゃったように少しずつ丁寧な対応を通して進めていく必要があります。

しかし、我々にとってありがたいことに、これには成功例が米国にあります。向かうべきターゲットがはっきりしているのだから、それに向けてともかく進めるということでプッシュするのがよいのではないかと思います。

また、情報収集の際には、「データを渡しておしまい。」ということではなく、そのデータをどう利用するか

というところにつき、誰が利用するかに関して、使い方を決めることによってコントロールできるという気がします。情報そのものを渡すか渡さないか以外に、どう使うかというところでコントロールができると思います。もう少しフレキシブルなインターフェースを作ることができるのではないかという気がしますね。

佐々木　情報の管理について、官側から見ると、特に捜査情報をどのように取り扱うかという問題があり、産業界においても、インシデントに顧客が関係している場合には顧客の秘密を守る義務があるという御意見もありました。なかなか難しいハードルはありそうですが、NCFTA では情報をどのように共有しているのか、そのルールはどうなっているのか、この点についてマリア・ヴェロ最高責任者に伺いたいと思います。

ヴェロ　私どもはパートナーに対して情報共有をお願いするわけですが、共有すべきものを一方的に指定したり、要望したりすることはありません。あくまで納得して共有していただくことを前提としています。

ただ、連携を通じて徐々に信頼は高まっていくので、まずは、何か共有できるもの、しかも、納得して共有できるものを共有していく。そうすると時間が経つにしたがって、より多くの情報を共有してくれるようになります。というのも、その効果を実感するからです。点と点を結んで線にして、誰がスレット・アクター（threat actor）で、犯罪者はどこにいるのかが徐々に分かってくると、情報共有のメリットが実感できると思います。

NCFTA では、メンバー間で NDA（Non-Disclosure Agreement：秘密保持契約）を常に交わしているので、共有した情報をどこかに持ち出して販売するというようなことは決してできません。情報はあくまでもメンバー間で利用されるものであり、犯罪者を特定するためのものとして用いられています。

我々が情報を共有すると、必ず匿名化し、どこに帰属するかが分からないようにしてデータベースに格納します。そして、匿名化した情報にメンバーとなった方々だけがアクセスする権限を持っています。

メンバー間でデータをプッシュする場合も、もちろん安全な方法で暗号化した形で送信しています。セキュリティに対して何も侵害が起きないように担保しているのです。

佐々木　NCFTA においては納得した上での共有、また、NDA を結んだ対応、情報の匿名化、そうしたことがポイントであると理解いたしました。我が国の捜査に関する情報の共有・管理の在り方については、星教授、刑事法的にいかがでしょうか。

星　捜査機関が持っている捜査情報を産学と共有するということについては、例えば鑑定嘱託をする際に必要な情報を提供するというような個別的な対応はあったかと思いますが、それを一般的に共有する仕組みは、これまで必ずしもなかったのではないかと思います。

ただ、全く前例がないわけではありません。私の狭い知見で知り得たものにはなりますが、平成 21 年から 22 年にかけて川崎駅前を対象にして警察庁生活安全企画課で防犯カメラのモデル事業を行ったことがあります。その際に、産の側からある企業が参加されていたのですが、異常行動検知機能が機能するかどうか、正に先ほど田中先生のお話にもありましたが、現場情報を使って実証したいということがありました。実際に、川崎駅前に川崎警察署が設置した防犯カメラ映像をその企業が解析するということが行われました。

その際、ある種の NDA だと思いますが、企業側が生活安全企画課に誓約書を提出するかたちで、「秘密保持」、「目的外使用はしない」、「データを運ぶときにはデータが記録されたディスクは暗号化する」などの取決めをした上で情報共有を行い、無事に済んだという事例があります。このように、捜査情報を共有する仕組みが、今

まで全くなかったわけではありません。

もちろん、防犯カメラ映像の場合は99.9%以上が何ということはないデータなので、サイバー上のインシデント情報とは違うという御意見も中にはあろうかと思います。しかし、この時、その企業が解析対象にした異常行動検知が機能するかどうかという実証実験は、正に犯罪ないしは犯罪につながり得る場面を切り取って行っていたということがあるので、やはり実績が全くないわけではないと言えると思います。

もう一つは、先ほど若干お話ししましたが、捜査情報のデータベース化は、従来の一般的な捜査における情報の扱い方とはだいぶ違う面があるということです。データベース化自体が、産学との共有を除いたとしても、だいぶ異なった使い方になってくるので、詰めていくべき点は多々あろうかと思います。サイバー空間における情報を証拠化することも含め、どの情報をどこまで共有化していくのか、データベース化していくのかに関しては、今後詰めるべき点が多々あろうかと思いますが、是非検討を行って有益な枠組みを作っていただきたいと思います。

２．人材育成とトレーニング、研究開発

佐々木　次に、人材育成とトレーニング、そして研究開発の点に移りたいと思います。人材育成の重要性については、既に田中教授、近藤執行役員の御講演でも触れていただいたところですが、改めて田中教授に「日本版NCFTA」における人材育成や研究開発の在り方について御意見を頂戴したいと思います。

田中　人材が少ないことは前から言われていました。最近の企業活動は情報に依存するところが大きいので情報は非常に大切な資産ですが、それを失ったときの状況認識に基づいてのしっかりした対策を施すまでにはなかなか至っていないし、セキュリティ担当という部門の設置も少ないように思います。現代という時代は、世界と密に繋がっている時代です。情報セキュリティに対する認識を深める必要があるのではないでしょうか。

キャリアパスにしても未だ確立しているとは思えませんが、若いときは専門家として集中して働き、もう少し経つとマネジメントを担当し、更には情報をコントロールするというかたちでの CIO（Chief Information Officer：最高情報責任者）になっていくなど、キャリアパスがうまく形成できると、若い人の目指すターゲットが明らかになりますので、人が集まると思います。

トレーニングに関して申し上げますと、勉強するときに座学に加えて手を動かす実習や現場経験を味わうようなトレーニングをすると、目を開かされる良い契機になります。重要性も分かるし、「なるほど、ここが勘どころか。」ということが分かるのです。そういう意味で、トレーニングする場を是非増やしていただき、利用していただくのが良いと思います。

研究開発については、サイバー犯罪がどう行われるか、どう捜査すれば良いかという、犯罪の観点から見たときの研究は警察の非常に重要な役割です。そういうことは他のところではやっていませんから、この分野における研究開発は必要であり、かつ、とても重要な項目の一つだと思います。

もちろん、それ以外にも、サイバー分野は変化が激しく、新しい技術がどんどん出てきますので、常に新しい検出技術の研究や状況把握と隣り合わせで仕事をしなければいけないわけですから、研究は不可欠な要素だと思います。

佐々木　「日本版 NCFTA」を考える上で、人材育成、研究開発は大変重要なテーマであることを再認識いたしました。

また、トレーニングという意味では、犯罪捜査を行う警察官の育成も重要だと思います。この点は緒方課長、「日本版 NCFTA」の中での警察官のトレーニングの在り方についてコメントをお願いします。

緒方　サイバー犯罪は、生活安全部門のみならず警察のあらゆる部門に広がっており、警察としては、部門を超えて、犯罪捜査に携わる全ての捜査員がサイバー犯罪について一定の知識と技術を身につけることが必須だと思っています。

育成の方向性としては、全体を一定程度底上げした上で、民間企業のトップレベルの技術者と伍し、また、ハッカーとも会話ができ、高度な技術・知見に加えてサイバー犯罪捜査要領にも習熟した特別の捜査員、サイバー犯罪捜査エリートのような者を育成していくという、二つの育て方が警察には求められていると思っています。

前者は、全体の底上げ、全ての捜査員に必要な教養、警察が単独で対応すべき領域の話であろうと思います。

我々としては、できれば後者、正にプロ中のプロを育てることにおいて、産学官連携の枠組みを活用できれば大変にありがたいと考えています。NCFTA という産学官が集う場において、産業界、学術団体が警察に求めるもの、そのニーズを正しく踏まえた上で、産学の関与を得るかたちで、その求めに見合った法執行を行うに足る捜査員を育成することができれば、独りよがりではない人材育成も可能になると思いますし、それがひいては、警察のみならず産業界や学術団体においても通用し得る、本当の意味のサイバーセキュリティに関するプロフェッショナルを育成することができるのではないかと考えています。

また、そもそも NCFTA という組織において、そうしたプロの捜査員、高度な技術を持った民間のエンジニア、体系的な知識を持った学術エリート、こうした人たちが一堂に会して犯罪対策という分野でその知見と技術を披瀝し合って分析等の作業を行うという、この工程自体がそれぞれの能力向上に資するものであり、広く産学官におけるサイバーセキュリティに関する人材の育成にも貢献できるかとも思います。

望むべくは、米国の NCFTA が米国内の法執行機関の職員のみならず全世界の法執行機関の捜査員に対して門戸を開き、法執行機関としての能力向上に大変な尽力をいただいているように、「日本版 NCFTA」が将来アジア地域においてそうした役割を担うことができれば、一つの新しい組織の大きな役割にもなると思っています。

３．既存の組織との関係

佐々木　それでは次に、既存の他組織との関係に移りたいと思います。現在、我が国では、NISC はもとより IPA、テレコム・アイザック等、情報セキュリティ対策に関する官民連携の枠組みが既に様々あります。会場から事前にいただいた御意見の中には、「『日本版 NCFTA』を新たに設立するよりも、既存の機関・協議会などの枠組みをうまく利活用することが重要ではないか。」といった趣旨のものもありました。この点につき御意見を伺いたいと思いますが、まず、近藤執行役員はいかがでしょうか。

近藤　既存の組織に関しては、それぞれ設立した経緯や趣旨があります。各省庁が先頭に立って設立している経緯もあって、業界や業態などが中心となった集合体になっているところもありますよね。もちろん NISC に関しては、そういった意味よりは国全体の戦略を立てていくという位置付けなので、少し違った立場だと思いますが。

ただ、そうした中で、今回の「日本版 NCFTA」を見ていくと、これは法執行機関が背景にいるのが非常に大きな特徴です。それぞれの業界に横串を刺して、全体として色々な情報を共有できる仕組みであって、そこではより深い情報を取り得るものと思います。ここで解析された動向などが既存の各組織で検討され、更にその業界の中での色々なルールや方向性が定められるという意味では、相互補完的にこういうものが働くと思っています。

佐々木　星教授はいかがでしょうか。

星　近藤先生のおっしゃったことと重なりますが、NCFTA と既存の情報共有等のスキームとの最大の違いは、法執行を前面に押し出しているかどうかにあります。

先ほど申し上げたとおり、サイバー空間で脅威が生じた場合に、セキュリティ対策をリアクティブに取ることも大事です。しかし、それだけでは立ち行かなくなっていく中で、誰がどういう形でそれを行ったのかという捜査・検挙、場合によってはプロアクティブな対応も含めた観点をこれまで以上に重視していかなければ、サイバー空間における脅威の除去について十分な対応はできなくなってきていることについて、考えなければならないと思います。

他方、そうしたインシデントがあった場合に、当面の対策としてセキュリティ対策をまず打たなければいけないといった需要がなくなるのかというと、そういうわけでもないとも思います。両者は共に大事なものであり、それぞれがそれぞれの比重を置いた組織が併存あるいは共存していくのは、全く無駄ではなく、サイバーにおける様々な事象・脅威に対する対応の在り方としては、むしろ必要なことなのではないかと思っています。

佐々木　田中教授はいかがでしょうか。

田中　基本的にはお二人と似たような感じになりますが、従来の組織は、それぞれの立場での定点観測やモニターを通して状況を把握することが中心だったと思います。

一方、ここで議論している「日本版 NCFTA」の最終目的は、サイバー犯罪をどうするかが中心になっていると思います。

そのために色々な情報を集めるのは当然あり得ますし、そのために既存の組織から情報をもらうこともちろん必要だと思います。しかし、サイバー犯罪対応は今後強化すべき新しい組織横断的な仕事ですから、そういうことをやるのは新しい組織の責務であり、既存の組織に取り込めるものではないように思います。新しい組織と既存の組織とで協力してやるべき話ではないかと思いますね。

佐々木　皆様の御意見をまとめると、仮に既存の組織と重複したとしても差し支えない、あるいは今回はそもそも違った切り口、いわば法執行の側面であるので、より能動的な対応に応える組織の枠組みを新たに作る必要性があるということになりましょうか。

さて、これまでそれぞれの論点ごとに各パネリストから「日本版 NCFTA の創設」を検討していくに当たっての留意点について御意見を伺いましたが、最後に、これまでのパネルディスカッションを踏まえ、また NCFTA の運営経験を踏まえ、マリア・ヴェロ最高責任者から我々に向けて、どのような点に留意すべきかアドバイスをいただきたいと思います。

ヴェロ　幾つかのことを申し上げたく思います。

まず、先ほど「Industry First（民間を第一に）」という話をしました。

皆様方も産業界の情報を強調なさいました。民間から情報を得ることは必要です。情報を受け取ったら、それについて何かをしなければならない。予防的、積極的でなければなりません。もちろん、積極的に逮捕・検挙を

していきますが、同時に犯罪を防止する、防犯的なことも積極的にやっていきます。

サイバー空間の脅威に関する何かが民間で起きたとき、私の同僚や他の部門に対して何かが起きたことを知らせ、それがどういうふうに起きたかを知らせれば、彼らは防御することができます。民間に耳を傾け、情報を共有していくこと、そして、それを迅速にやることが重要です。

また、もう既に機能している組織があれば、それと相互補完的なことを行っていく、あるいは、既存の組織を強化することを考えていくことにも留意する必要があります。

次に、グローバルなアプローチを取ることが重要です。本日は、皆様と次の点を共有しました。犯罪を防ぐ、あるいは回避するだけではなく、犯罪者を捕まえたいのだということです。

「モグラたたき」のようなことはすべきではありません。よりハイレベルの大物を捕まえることが重要です。それをするためには部門間で共有をする、産学官で共有をすることが重要です。様々なリソースを共有しなければならないし、中でも特に訓練を受けた人的資源が必要です。どうやって分析をするか、オープンソースをどうやって使うかについて訓練するだけでなく、どういう疑問を産業に投げかけるべきか、法執行当局とどうやって相互作用を高めていくかについても考えていかなければなりません。私どもの産業パートナーは私ども法執行者に対し、その犯罪を解決するための正しい情報を得るためにはどういう質問をしたら良いかに関する訓練をしてくれています。皆が協力してお互いに学び合うのです。

協力・連携・共有をし、今あるものは、最大限強化・補完していく。これらは積極的・先行的にやらなければなりません。犯罪を止めなければ、産業は、役に立っていないと見なしてしまいます。例えば、企業秘密などが盗まれてしまったならば、後になってもどうしようもありません。先行的にその対処をしなければならないわけです。犯罪を止めるということだけでなく、その帰属、すなわち誰がやったかを確認するのです。

そして、何よりも、産学官で信頼関係を構築することです。今申し上げた全てのことについて、基盤になるのは信頼関係ですから。

４．他の主体に求めるニーズ・期待

佐々木　全ての前提として信頼構築が大事であるというアドバイスをいただきました。

それでは、各主体の皆さんから、これまでの議論を踏まえて他の主体に求めるニーズ・期待、あるいは、今日の発表について皆さんの講演・発表に関する御感想でも結構ですから、自由に御意見・御感想などをいただきたいと思います。まず、近藤執行役員、いかがでしょうか。

近藤　私どもはこういった形でサイバーとの戦いに参画していますが、人材育成の観点で、どうしても急速に人材を立ち上げることができません。学校・大学に対しては、トレーニング・コースを作っていくことに非常に大きな期待があります。

例えば、大学院大学で２年間やらないと強い人材は育たないのかもしれませんが、まず即戦力として使える人たち、底辺を支える人たちを育てていくようなやり方について、大学ではどのようにお考えか、田中先生に伺いたいのですが。

田中　私は現在、情報セキュリティ大学院大学におります。この大学院は 2004 年に設立されたばかりで、ようやく 10 目年に入ったところですが、設立理由を振り返れば、9.11 で米国に攻撃があったのを見た理事長が、こ

れはいかんということで、情報セキュリティを専門とする大学院を創ったのです。

設立以降、今までずっとやってきたわけですが、専門的な教育をやっているというのが外からはなかなか見えません。また、企業の方とお話をしていると、近藤さんがお話しになったように、非常に短期間で育ててほしいというニーズがあります。大学院であれば本来２年間ですが、そんな長い期間はやっていられないということで、バラエティを設けることにしました。

例えば、非常にシンプルですが、ある科目だけ聴講することを認める。また、2 カ月間で、ある目的に合わせた集中したコースを受講できる仕組みも作りました。「2 カ月」という意味は、クォーター制ということです。大学は普通２学期制ですが、それを更に半分に分けるというものです。そうすると非常に対応が柔軟になります。

もう一つは一年制です。一年制は、1 年間でマスターを取ることができますが、その代わり、毎日来学して集中的に学ぶ必要があります。つまり、一年制の場合は、日中は働きながら大学に通うというわけにはいきません。きっちり１年間来れば、マスターが取れるというものですから。なお、二年制になると、夜３日と土曜日を使うことによって、科目の単位がほぼ取れるので、働きながら学位を取ることができます。２年制は、自ら研究することで成長するというところに大きな利点があります。

また、今年からは、講義だけではなくて実習コースもたくさん設けて活動しています。全部で 10 数コースありまして、フォレンジクス、ネットワークセキュリティ、インフォメーションマネジメント等項目に合わせた実習を設けています。

このように、色々なセットを準備して対応しているところであり、是非使っていただければありがたいと考えております。

佐々木　引き続き田中教授から、他の主体に期待するニーズ、あるいは今日の御発表についての感想等があればお願いしたいと思います。

田中　警察には、情報を共有する上での困難さを解決するために、色々な組織との協定も含めて、法的な整備をしっかりやってほしいと思います。ソフト・ローもこれに含まれます。

また、近藤さんがおっしゃったように、企業間の情報共有が難しいというのはそのとおりだと思います。これは、情報を出すと公的に役立つと思ってはいるものの、企業内の制約から出すのが大変だということですね。ただ、これは、やってみることから新しい状況が生まれるのではないでしょうか。ここまで大丈夫ということの積み重ねと、それによる長期的なメリットの認識が大事でしょう。

近藤さんもマリア・ヴェロさんもおっしゃったように、信頼を作っていく。その過程で、どれだけ出した方が良いのかなどが、はっきりしてくると思います。最初から決め打ちでかかるというのではなく、それこそトライアル・アンド・エラーでやっていくべき話だと考えています。

佐々木　続いて、緒方課長からお願いします。

緒方　産学に対する要望ということでは必ずしもありませんが、私どもは、この「日本版 NCFTA」を創設することの検討を始めた時から、我々警察にとって、産業界・学術団体にとって、この組織のメリットは何かをずっと考えてきました。

警察にとってのメリットははっきりしています。最大のメリットは、捜査機関として、犯罪捜査に産業界・学

術団体の知見と技術を活用することで、合理的あるいは効率的に事案の解明を進められることです。

ただ、それだけでは、特に産業界にとってのメリットにはならないと思っています。

産業界がこの組織に望むことは、誤解をおそれずに言えば、被害を受けてから犯人を捕まえてくれということではなく、被害が起きないようにしてくれということであろうかと思います。そもそも我々警察の警察活動の目的も、事件が起きてから犯人を捕まえることそれ自体が警察活動の目的ではなく、犯罪や事故のない社会を築き上げること、安全・安心な社会を築き上げることが警察の本来の目的です。

我々が創ろうとしている「日本版 NCFTA」も、単なる犯罪捜査のための便利なツールということではなく、サイバー空間における脅威をその兆し、あるいは芽の段階で把握し、それがいかなる脅威に発展するかについて、産学官の英知を結集して分析・評価をし、それに基づいていち早く対処し、被害を未然に防止することを主眼としています。

先ほどマリアさんからも防犯というお話がありました。“Industry First”という理念は正にそこにあるのだろうと思います。そこに重きを置いて初めて、この組織が官のみならず民にとっても本当の意味で有益な仕組みになると思いますし、信頼を得られ、その結果様々な情報が寄せられてくるようになるのだろうと思います。そこを勘違いしないように、原点をしっかりと踏まえて制度設計を進めていかなければならないと思っております。

佐々木　星教授から、今日のこれまでの色々な議論を踏まえ、改めてコメントがあればお願いします。

星　色々なお話を伺っていて、私自身も痛烈に思っているところですが、サイバー空間における脅威は、社会的インフラに対するものということだけではなく、国家の存立をも危うくさせるものと言っても決して冗談ではないような事象になってきています。サイバー空間における脅威が従来とは質的に異なってきていることを踏まえた上で、発想の転換と言いますか、捜査情報の在り方や従来の情報共有システム・組織との連携の在り方などを考えていかなければいけない段階に来ていると、本日の基調講演や先生方のお話を伺って非常に強く思いました。

佐々木　ありがとうございました。

ここで、会場からいくつか質問をいただいたので、その質問に対するお答えをお願いしたいと思います。

まず、マリア・ヴェロさんに対して御質問です。「米国の NCFTA について費用負担も含めた組織の運営方法（意思決定方法などの意味を含めて）どうなっているのか、関係者の協力体制はどうなっているのか。」ということですが、いかがでしょうか。

ヴェロ　NCFTA に資金提供をしているのは会員です。パートナーになるためには会員として会費を払う必要があります。また、寄附も受け取っており、これらを用いて組織の運営を賄っています。

どのように意思決定を行うのかということについてですが、私が最終的な意思決定を行っています。ただ、もちろんそれ以前に、我々のパートナーとして一緒に仕事をしている方々、つまり産業界、民間であり法執行機関であり学術団体である彼らにとって何が重要かについてきちんと聞き、インプットを受け取っています。私が申し上げている“Industry First”というのはそういうことです。その上で、何が新しい脅威なのか、どういった脅威があるのかを踏まえ、どういった取組を今後すべきかを決めていきます。

また、パートナーも NCFTA の一部であり、責任も持っておりますから、もっと上手なやり方がある、もう少しデータベースを強化するやり方があるなどといった、組織をより良くするための施策として彼らの方に良いア

イデアがあるということであれば、彼らに耳を傾けます。もちろん、全てを実行することはできませんが、正しい方向性である―全てのパートナーにとって、組織にとって良い方向性である―ということであれば、助言に耳を傾けて実施していきます。

“Industry First”を実行し、全員にとって正しいと思われることを実施していく、そうした観点からも、NCFTAは非常に積極的に動いているところです。

佐々木　もう１問、やはりマリア・ヴェロさんに対して質問がございます。「各参加主体の情報共有のインセンティブにはどういうものがあるのか。」というものと、「集めた情報をどのような形でフィードバックしているのか。」という御質問ですが、いかがでしょうか。

ヴェロ　インセンティブは、正にパートナーが得る価値です。

情報共有とは、偽造ID、不正口座、模倣品などといったものに関する情報を共有することです。情報を得ることができれば、口座に対してフラグを立てることができ、送金をストップすることができる。悪意のある口座をストップさせることができれば、被害を食い止めることができ、顧客を保護することができます。

はっきり申し上げて、そこに金銭的なインセンティブはありません。彼らが得る価値、つまり被害を防止すること自体がインセンティブになっていると考えています。

攻撃を受ける、例えばDDoSが銀行で発生した際に、正にDDoS攻撃が行われている最中に、その裏でお金の送金が行われていたということであれば、こうした手口を銀行間で情報共有できるようにしたり、「ここを見ろ。」といった情報を提供したりします。我々は何のルールも犯すことなくこうした作業を行っていますし、パートナーも、そういった情報を得て、必要な分野を確認し、被害を防止することができるのです。

また、被害防止に有効なツールを作れば、これも共有します。そうすることによってリソースやコストを節約することができるわけです。

パートナーが得られる価値は既に実証されています。

ある銀行は、１週間に２日間NCFTAに来てくれていました。それがやがて１週間になりました。つまり、銀行員がここで働くようになったわけです。そして、更にその銀行は２人に増やし、今は３人になっています。我々は、パートナーの方々にNCFTAで働いてもらうことに対するお金は払っていません。パートナーは、NCFTAに投資をし、リソースを提供することによって、それに見合った価値を受け取ることができているのです。

彼らは全ての情報を持っているというわけではありませんが、10の異なる組織から10の異なる情報を得ることができれば、非常に有用なものになります。より賢明になり、いかにして自らを防御したら良いかを学ぶことができると思います。

佐々木　「集めた情報をどのような形でフィードバックしているのか。」という点についてはいかがですか。

ヴェロ　ある情報を入手した場合、その情報を匿名化してから情報を取り出すことにしています。マルウェアの研究所があり、業界の情報を基に最新のマルウェアなどの研究もしています。そこで得られたマルウェアの色々な亜種や関係するIPアドレスなどは、全てパートナーにフィードバックしています。

もちろん、IPアドレスは常に変わります。我々は、口座、悪意のあるIPアドレス、詐欺的な行為を行う者の

氏名等に関する情報を毎時間出していますから、もしブラックリストを作るような場合でも、そうしたプロセスはストップさせないよう注意しています。なお、マルウェアに関しては、一晩に一回セキュア・コミュニケーションで情報を出しています。

佐々木　次の質問に移ります。「マリア・ヴェロ氏の話の中でサイバー犯罪の組織化について触れられていたが、組織的なサイバー犯罪に対抗するために、NCFTA はどのように各国へ働きかけをしておられるのか。」「各国が協力した国際的なサイバー犯罪対策機関の設立を望んでいる。」というコメントが付いておりますが、NCFTA として国際的な各国への働きかけについて、いかがでしょうか。

ヴェロ　国際インターンシッププログラムを通じて、各国から法執行当局の方々をお招きして信頼関係を作っています。もちろん、それ以前に既に情報の共有はしていますが、これが各国との関係をよりオープンなものにしています。ベストプラクティスや経験から得られた教訓などに関する情報が各国から求められています。

英国では、今年の３月に CISP センターという、NCFTA に類似するセンターができました。以前、彼らは NCFTA に来ており、我々が得た教訓やベストプラクティスを学び、それを持ち帰って組織を作り上げています。

彼らとは、非常に頻繁に会合を開き、情報共有をしています。どんなマルウェアがあるか、ノウハウがない英国に米国のノウハウをどのようにしたら差し上げることができるか、あるいはその逆についても検討しています。昨日は、私どもが見ていないマルウェアが英国から提供されました。リバースエンジニアリングをしてターゲットも判明したということですが、彼らは、自分たちの情報を全て提供し、そのマルウェアのターゲットについても情報を提供してくれました。その中には、十数の企業が含まれており、我々は、この情報をパートナーに渡すことができました。

これは英国との連携の非常に良い例で、うまくいっていることの証左だと思います。「日本版 NCFTA」ができた暁には、両国の間にある十分な信頼関係を基にして、同じようなことができればと願っています。

他国が接している脅威は、自国のそれとは異なる場合もあります。自国にない脅威が初めて他国で見られたということであれば、我々は、どんなものがこれから来るかを知ることができます。逆に米国で何かが始まって、それが他国に波及する場合もあります。使っている機器によって、特定の脅威が出てくるということもあります。こういうものが他国で起きているということが分かれば、米国の組織では予防的活動を展開して被害を阻止することが可能となります。もちろん、逆もまた然りです。

なお、CISP センターとは、人材交流についても協定を結びました。一緒に作業をして話すことによって信頼が構築されますから、こうした国際連携にはプラス面しかないと思っています。

佐々木　最後に、これは事前に参加者の方から寄せられた質問の中で多かったものですが、「現下のサイバー犯罪に対応するためには、警察の捜査能力の強化も必要である。警察庁として、今後のサイバー対策に向けて組織的改変、あるいは各県警察との連携、海外との連携といった方向性を聞きたい。」という質問です。このコメントは、緒方課長にお願いします。

緒方　御質問は、サイバー犯罪への対処能力の強化の中でも特に組織的な観点からのお尋ねかと思います。

まず、警察庁では、サイバー犯罪については様々な部門にまたがって対応しています。生活安全部門、刑事部門、警備部門、もちろん情報通信部門などがそうですが、これらまたがる部門全体を調整する警察庁としての司

令塔機能を強化する観点から、現在でもサイバーセキュリティ戦略担当審議官が置かれているが、この審議官をサイバーセキュリティに専任化をし、かつ、この審議官の下にサイバー担当の専任の参事官と所要のスタッフを置くという組織改編の作業を進めているところです。もし、予算や組織としての容認が得られれば、来年度からのスタートになります。

また、都道府県警察においても、平成23年度から3年間をかけて地方警察官の増員を行ってきています。国・地方を通じて大変に厳しい財政事情の中ではありましたが、サイバー犯罪捜査、サイバー攻撃対策を含め、3年間で900名を超える警察官の増員を措置していただいたところです。

加えて、サイバー犯罪は時間的・場所的な制約を受けません。瞬時にオールジャパンで起きます。これは現在起きているインターネットバンキングに係る不正送金事案においてもそのとおりなのですが、これに対し、都道府県警察単位の現在の警察制度を維持しつつ、その上で警視庁に情報追跡班を置いたり、サイバー犯罪特別対処班を置いたりするなど、全国警察が連携して対処できるような枠組みを整えています。併せて、共同捜査、合同捜査という、一つの県だけではなく関係する県警が連携を組んで捜査を行うやり方も、他の部門に比べてサイバーは大変に進んでいると思っています。

国際的な連携という意味では、サイバー犯罪は正に容易に国境を越えます。ありとあらゆるものが他国のサーバに立ち上がる状況である。これに対しては、G8コンタクトポイントあるいはICPO等様々なルートを使い、国際捜査共助要請を含めて国際連携を強めているところです。

この観点で付け加えさせていただきますと、基調講演の中で近藤様の御説明の中に、来年シンガポールに立ち上がるICPOのサイバー版の調整機関であるIGCIのお話がありました。IGCIとも是非しっかりと連携し、グローバルな対応を強めていきたいと考えています。ちなみにIGCIの初代総局長には、警察庁からICPOに行っている中谷昇君が就任予定であり、そうした人脈もフルに活用して国際連携を更に強めていきたいと思っているところです。

また、先ほどマリア・ヴェロさんから大変暖かい激励のお言葉がありました。仮に「日本版NCFTA」が創設され、その組織が軌道に乗ることになれば、ぜひ米国のNCFTAと連携を取って、正にグローバルな対応の大きな柱となるように努力をしてまいりたいと考えています。

【総括・閉会】

佐々木　本日はサイバー空間の脅威に対抗するための産学官の連携をテーマに議論を進めてきました。現状の課題を克服するためには、米国のNCFTAを一つのモデルとして、産学官が情報を共有して各主体が一体となって対応するという方向性について、それは検討に値する十分なメリット、有効性を持っているということが明らかになったと思います。

一方で、その実現に向けていくつかの課題もありますが、その課題をどのように克服するかについても皆様から有益な御示唆をいただきました。

「日本版NCFTA」の創設と言っても、米国と日本では事情が違うこともあり、その実現にはまだまだ時間がかかるかもしれませんが、方向性はしっかりと示されたのではないかと思います。本日の議論が今後我が国における産学官の連携の新しい展開の一助となることを願っております。

パネリストの皆様に御礼申し上げ、また、会場の皆様にも、長時間御清聴いただき御礼申し上げます。これをもってパネルディスカッションを終了いたします。

（終了）