［講演会抄録］

2010年度連続研究講座：
グローバル化時代のリスクを考える
第3回「サイバー犯罪の現状とグローバル化」

2010年7月8日

四方　光（警察庁生活安全局情報技術犯罪対策課長）

●サイバー犯罪の仕事に就くまで

警視庁刑事部捜査第1課管理課というのがあります。警視庁の捜査1課というのは殺人だとか強盗だとかを担当する課なのですけれども、管理課というのはいわゆる特捜本部のプロジェクトリーダーをやる仕事であります。1年間だけ、警視になりたてのころの1年間だけ管理課をやらせていただきました。

当時、たとえば殺人事件が起こりますと、この管理課では、その事件の担当者を決め、担当以外の人も必ず最初みんなで集まるようになります。事件発生の直後というのが一番大切だからです。東京では、週に1回か2週に1回ぐらいは殺人事件が起こったりします。ですので、昼夜問わず、そのぐらいの頻度で必ずどこかの現場へ、いわゆる「赤灯」、つまり私服パトに乗って、現場に急行します。

そのほかいろいろな仕事をやらせていただいたのですけれど。この2月まで、ちょうどこの大学のある神奈川県の刑事部長というのをやらせていただきました。またこれもたった11か月ぐらいで短かったのですけれども。神奈川県というのは実はいわゆる大府県ですね。人口でいくと大阪を抜いて全国第2番の大県大きな県なのです。犯罪率といいまして、人口を分母にして犯罪の発生件数を分子にした犯罪率でいくと、こういう大都市を抱えている県の中では、かなり犯罪が少ないほ

うなのです。そういう意味で非常にいいところですね。

それでも、それでもやはりいろいろな事件があります。特にやはり皆さん方、せっかくの機会ですから、防犯指導ではございませんけれど注意していただきたいのは、性犯罪です。そんなに頻繁に起こっているわけではありませんけれども、少ないわけでは決してない。よく、「日本は安全だから、夜、女性が１人で歩いても大丈夫」と言われていますけれど、そんなに大丈夫ではありません。ですので、性犯罪について三点お話ししておきます。

一つは、性犯罪というのは自宅・アパート、あるいはその周辺で一番起こるということです。ご自宅のあるところの最寄り駅の駅前に性犯罪者というのは大体うろうろしているのです。そして、可愛い女性がいないかなと見ているのです。で、「あ、この子、この人いいな」というときに、後ろを実際つけていくのです。だから、夜道で後ろをだれかつけてくるなと思ったら、気を付けなければいけないというのはそのとおりです。ずっとつけてくるやつがいたら、ちょっとまた駅に戻るとかしてもらったほうがいいですね。

実際の犯行現場というのは駅からご自宅の間だということがわりとあります。ですから、皆さん方としては、駅に着いたから、ちょっとほっとしたりするところだと思うのですけれども、そこが実は危ないというのがあります。

それから、発生現場で一番多いのは、この女性のご自宅そのものなのだということです。一人暮らしの場合は特にそうです。手口も幾つもあるのですけれども、一つはやはり、例えばマンションだとかアパートの1階2階ではなくて、3階、4階、5階、6階ぐらいだったらそんなの侵入なんざしてこないだろうと思いきや、まさしくクモ男のようにして、屋上から降りてきたり、一生懸命登ったりするのですよ。執念を持ってね。性犯罪者というのはね。ですので、やはりよく言われ

ていますけれども、夏、窓を開けて寝ない。結構大事かもしれませんね。

それからさっき言いましたずっとつけてくるタイプのやつね。これがずっとつけていって、最後皆さん方がおうちの中に入るときに、一緒に入って、入り込んでしまう。要するに鍵を開けたところで一緒にがーっと入ってしまって、部屋の中でというのも実はあったりします。

いずれにしても、頻度としてはそんなに全体からすると大きいわけではないかもしれませんけれども、わりと発生をしております。もし、最悪のケース、実際に被害に遭われた場合でも、警察は特別の支援体制を取っております。最初に駆けつけるのはひょっとしたら交番のお巡りさんだったり、パトカーの警察官だったりするかもしれませんけれども、必ず性犯罪の場合は女性警察官が担当をやります。いろいろ思い出したくないことも必ず女性警察官が担当するようになっていますし、それからこれは県庁とも協力して、特別な相談所も作っているのです。犯罪被害者相談センターというのが横浜のほうにあります。これも女性の臨床心理士などがおりまして、きっちりご相談に乗るということになっております。

性犯罪者というのは、必ず１人だけ狙うという話ではないのです。定期的に必ず何人もの女性を狙っていきますものですから、最悪の場合には大変ですけれども、ぜひ警察へ申告していただきたい。

●警察組織のしくみ

まず警察の組織について申し上げます。まず警視庁と警察庁の違い、検察庁とかいう機関もありますが、それをご説明します。

警察庁というのは国の機関で霞が関にあります。警視庁というのは実は東京都警察のことなのです。歴史的な経緯から、日本の近代警察はいわゆる明治維新の後できたのですけれども、最初に警察ができた

のが警視庁だったので、その立派な名前をちょっとなくして東京都警察というのは忍びないなというので、そのまま警視庁といって呼んでいるのです。

検察庁というのは、警察とはまた違っていわゆる法律家、法曹三者の中の、裁判官・弁護士と、もう一つある検察官がいるところです。警察が事件をやった結果を検察庁に送りまして、そこで公判請求と言いまして、犯罪者を起訴し裁判にかけます。それを遂行するのが検察庁です。

日本の警察の本体といいますか、実際に日常的な活動をしているのは、実は都道府県警察です。神奈川でしたら神奈川県警察が実際の仕事をします。交番のお巡りさんも神奈川県警察の職員ですし、それから警察本部、横浜のほうにある警察本部も、実際の事件、性犯罪でも殺人事件でも、捜査をするのは、この県警察です。

そのなかで、私がいる生活安全部門というのは、皆さん方に比較的身近な犯罪を担当します。私が今やっているのはサイバー犯罪という分野のほか、少年非行、DV、ストーカーの問題、それからいわゆる防犯指導の仕事、そんなことをやっているのが生活安全です。

殺人だとか強盗、放火をやっているのが刑事部です。暴力団対策も刑事部でやっています。

交通部は、いわゆる交通安全の関係ですね。駐車違反でありますとか、交通事故の対策。

警備部といいますのは、今年11月にあるAPECのように大きな催しがあったりしたときに、世界のVIPが悪者に襲われないようにいろいろ警備をするというような仕事をやっております。

現在の私の担当はいわゆるネット犯罪の担当です。

●インターネットの世界

インターネットはグローバルにつながっています。ネットであれば外国のサイトもすぐ見られます。外国の法制はどうなっているんだろうなとかいうときに、やはりアメリカだとかイギリスだとか、例えばFBIなりアメリカの司法省のサイトを引いたり、それからイギリスだと内務省とか、そういうところのホームページを見ると、外国の法令がわかります。

先進国ではこのインターネットの普及率が、もう70％を超えて、80％に届こうとしています。

それから、皆さんがよく使っているネット上のサービスがあります。実はホストコンピュータは海外というのは結構多いのです。話題になっていますツイッターだとか、あと2ちゃんねる、ああいうのも実際のデータが保存されているのはアメリカです。実は日本でよく利用していて皆さん見ていても、その間、実はアメリカと瞬時に通信を行き来させてやっているのです。

結構重要なこのサービスの会社が、そのデータの蔵置場所をアメリカだとか、今後は多分中国なども増えていくのではないかと思いますけれども、日本の総務省のほうはちょっとあせっておりまして、国内にそういうコンテンツサーバーを置いてもらいたいというので、コンピュータ特区でも作ろうかと検討しています。そういうデータコンピュータを置くのに適した場所で、いろいろな優遇措置を取るような場所を作ろうかという検討もしているところです。

いろいろな意味でのグローバル化が起こっているところです。

我々の生活は、すごくネットに依存しています。コンピュータだけではなくて携帯電話もそうです。インターネットの利用者は現在、大体9,400万人と言われています。人口が1億2,000万ぐらいの中で、ネット利用者が9,400万人です。

ネットでの買い物も多くなってきました。商売でこのネットを使うようになりますと、犯罪者にとっても犯罪のやりがいのある場所が増えてくることになります。

昔ですと、コンピュータを使うなどというのは、相当そういうのが好きな人だけというイメージがあったのですけれども、今はそんなことは当然ありません。皆さん方の世代のことを、私ぐらいの大人世代は、「デジタル・ネイティブ」と呼んでいます。私たちの世代よりも、パソコンの使い方というのをいっぱい知っています。

そういうふうになっていくと、この本当に10年、20年、まあ20年前ぐらいのインターネットが使われ出したころは、使う人も、悪いことをする人も、両方とも専門家でした。そのころ、ハッカーなどは、基本的には、そんなに悪いやつではないのだけれどもちょっと技術があるので盗み見をちょっとしたいと思っているだけの人だという議論があったのですけれども、現在のコンピュータ犯罪は、大半がお金目当てです。皆さん方がネットでいろいろ取り引きをする、その隙を狙って金もうけをしようというふうに狙っているやつらがやるのが、現在のコンピュータ犯罪、サイバー犯罪だと思っていただきたいと思います。

●サイバー犯罪の定義と現況

サイバー犯罪というのはべつに法律上の定義ではないものですから、三つぐらいの定義を私どもは持っています。

一つは「不正アクセス禁止法違反」。これは、他人のIDパスワードを勝手に使ってしまう。それからセキュリティホールといって、コンピュータの穴みたいなところを突いて他人のコンピュータを使ってしまうというタイプのものです。

第二の定義はつぎのようなものです。刑法典の中に、コンピュータ

を使った詐欺とか、コンピュータの記録を勝手に改ざんするとか、そういうようなものがいくつか犯罪として定められていますので、それに違反したものというカテゴリーがあります。

第三の定義はつぎのようなものです。出会い系サイトで18歳未満の子たちに誘いをかけたり、児童ポルノを売ったり買ったりする人たちがいます。買うほうは今のところ犯罪ではないのですけれど、売るほうは犯罪になっております。

これらを「インターネット、ネットワーク利用犯罪」と言っております。件数は右肩上がりのグラフになります。

昨年のトータルではサイバー犯罪が6,690件ということですが、実は刑法犯全体の中では、まだまだたいした数ではありません。刑法犯全体では、今13万件とか14万ぐらいです。大半は自転車泥棒とか、万引きとか、軽微な犯罪が大半ではあるのですけれど。6,000件か7,000件の間というのはトータルとしてはまだたいしたことはないのですけれども、これからどんどん増えていく可能性のある犯罪です。

先ほど説明した三つのカテゴリー、具体的にはどんなものがあるかをグラフにしてあります。

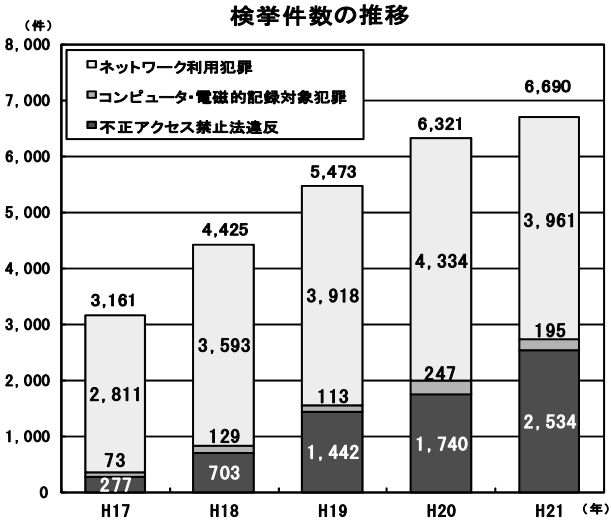

図1　国民生活を脅かすサイバー犯罪の現状

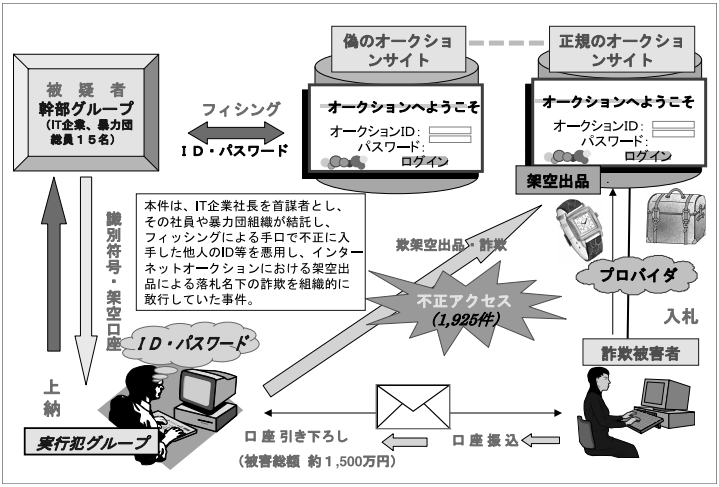

図2　フィッシング利用組織的・広域的な不正アクセス・詐欺事件

下のほうのネットワーク利用犯罪の詐欺。多いのは、ネットオークションでの詐欺です。架空出品をするわけです。ネットオークションだと写真だけで現物がなくても一応出品した顔ができますので、写真だけ張り付けてお金を振り込んでもらったにもかかわらず、品物を送らないという古典的な犯罪です。これが結構多いです。

それから児童買春だとか児童ポルノ等々です。わいせつ系というのもわりと多い犯罪です。

これはフィッシングという、詐欺とその前段の、詐欺をするための不正アクセス禁止法違反の事例です。

フィッシングというのは、正規のオークションサイトのふりをして、偽物を出させるような仕掛けを作るわけです。そこでIDパスワードを打ち込んでしまうことによって、そのオークションサイトの取り引きの他人の権限を使えるようにするわけです。そのフィッシングの仕組みを作っておいて、IDとパスワードを相当、たとえば2,000ぐらいの他人のIDとパスワードを盗んで、それを基に本当のオークションサイトで、写真だけ張り付けて架空出品して、被害者のお金を払い込んでとってしまいます。

払い込みの口座も大概他人の口座を用意します。暴力団は、大体他人の口座、他人の携帯電話を持っています。しかも、そういうのを売買する闇サイトが結構あるのです。そんなところで入手した口座に振り込ませて、取ったお金をまた上納、暴力団の幹部のところの手元に行くというような仕組みがあったわけです。

●ファイル共有ソフトによる犯罪

ファイル共有ソフト、ウィニーとかシェアとか使っておられる方もおられるかもしれませんけれど、その中で第3のファイル共有ソフトと言われているパーフェクトダークというのがあります。これは発信者

が、比較的わかりにくくなっていて、ウィニーとかシェアは「最近は捕まるぞ」というので、パーフェクトダークの使用が広がっています。

ファイル共有ソフトについて、一応念のため言いますと、映画だとか音楽だとか、マンガの場合だとか、それこそ児童ポルノの場合もあるのですけれども、この画像を分散させて、みんなで共有しようという仕組みです。発信者のほうは著作権法違反とかで犯罪者になりますので、我々一生懸命見つけて捕まえておりまして、結構ひょっとしたら身近な犯罪になってしまっています。皆さんに喜んでもらえると思ってやっている人もいるのかもしれませんけれども、完全に犯罪ですので、ずっとやり続けると、そのうち捕まったりいたします。

パーフェクトダークを使って捕まった人は、「パーフェクトダークだったら捕まらないと思った」と言います。う捜査手法は申し上げられませんけれど、我々もいろいろ工夫をいたしまして、確かに見つけにくい犯人の見つけにくい犯罪でも捕まえるように努力しているところです。

ちなみに、ウィニー、シェア、パーフェクトダークみたいなファイル共有ソフトがはやっているのは実は日本だけだというのです。外国にも合法的なファイル共有ソフトというのはあるのですが、こういう著作権法違反のためにすごくはやっているというのは、実は日本だけだとかいう話で、ちょっとショックなのですが、こういう犯罪も最近ではあるということです。

●サイバー犯罪を追跡する仕組み

インターネット上にいろいろそういう犯罪があるものですから、インターネットホットラインセンターという、皆さん方がもし、「あ、これちょっと犯罪じゃないか」と思ったときに、受け付けてくれる場所があります。「インターネットホットラインセンター」「インターネット

協会」で検索していただきますと出ますので、もしお気付きのときは通報してください。

そこで違法、有害、通報を受けたものが実際に犯罪だったというタイプのものも、年々増えておりまして、昨年、3万3、4千件近くあったという状況です。

インターネットホットラインセンターの仕組みをご説明します。一般のユーザーの方が、例えば児童ポルノもそうですし、あと銃器・薬物の 売買サイトなどをたまたま見つけたときに、基本的にはメールで受け付けをするようになっています。ホットラインセンターのホームページを開いていただいて、ちょうどその通報用のフォームがありますので、そこに書き込んでいただいて通報を受けるのです。

そこから違法なものにつきましては、私ども警察のほうに通報いただいて、捜査を始めます。即違法ではないものも若干ありますので、そういうものにつきましてはサイト管理者かプロバイダーに、「削除してください」という要請をします。外国のサーバーにある場合には、外国と日本とでいろいろ法律が違います。児童ポルノはほぼ世界中で違法な情報になっていますけれども、大人を対象にしたわいせつ文書は国によって犯罪になっていないときもあります。このINHOPEといいまして、「国が違っても児童ポルノを見つけたらお互いに通報し合いましょう」という仕組みがありまして、そこに通報して削除してもらうというようなことをしています。

それから、フィルタリング会社に通報して、フィルタリングのときにそういうのが見られないようにしてもらうというような活動をしているのが、インターネットホットラインセンターということであります。

●闇サイト

いわゆる闇サイトというのがいろいろあります。たとえば各種「公」の証明書を手配しますというサイトもあります。犯罪者にとっては身分証関係だとか、他人名義の銀行口座、他人名義の携帯電話など非常にほしいのですね。今の法律では、「公」の証明書を偽造したら犯罪ですけれども、自分の口座、自分の携帯電話も他人に売ったら犯罪になります。自分が使うという振りをして作っておいて他人に売ると、犯罪になっているのですけれども。非常にお金に困って、背に腹は代えられないというので売ったりする人がいたりするのです。それを生業にするような人もいたりします。

銀行とか携帯電話会社も、そんな人を見つける努力をしているのですけれども、完全には根絶ができておりませんで、「他人の口座ありますよ」「他人の携帯電話売りますよ」というサイトも結構あります。

それから「自殺手伝います」とかですね「一緒に犯罪やらないか」とか、その手のサイトがやはりあります。

少し前に話題になりましたのは、埼京線だったですかね「この電車のこの時間、可愛い女の子が多いから、みんなで痴漢しようぜ」とかですね、そんなとんでもない奴も一時期出たりいたしました。

そんなのがサイバー犯罪の現在での主たる例ということであります。

●サイバー犯罪の特徴

サイバー犯罪の特徴をあげてみましょう。

まずは匿名性。みんなサイバー犯罪の犯罪者は、匿名性が高いからバレないと思ってやっている人が多いのですけれども、捜査し始めるとちゃんとわかるのが通常であります。ただ、ぱっと見では確かにわからないですし、警察でも少し手間がかかるのは確かなのです。リアルの世界での犯罪よりも、少しやはり手間がかかったりします。そう

いう意味で、少なくとも、皆さん方の間で、相手と通信しているときの相手方がいい人なのか悪い人なのか、名乗っている名前が本物なのかどうかとかいうのはわからないですよね。そういう匿名性があります。

それから直接悪いことをする人たちだけではなくて、そういう場を提供しているサイトだとか掲示板にも、いいところ、悪いところ、の区別が実はあり、苦情の申し立てを受け付けないサイトがわりとあります。苦情申し立ての窓口がちゃんと書いてあるかどうかは法律上の義務にはなっていないのです。努力義務ぐらいですので、それが書いてないところもわりとありますね。

そうすると、例えばその掲示板などで言い合いになって名誉棄損みたいなことが起こると、とんでもないひどいことが書いてあるので消してほしいと思っても、全然消さないわけです。だれにも言えない。そのサイト管理者の連絡先を何も書いていないので、何も言えないというようなことがあったりします。

これは法務省のいわゆる人権擁護局だとか、相談に、あるいは弁護士さんとかに相談すれば対処する方法はないことはないのですけれども、簡単に対処が必ずできるようには必ずしもなっていないというような問題があるのです。

それから瞬時性、大量性です。ネットでは、瞬時に大量の悪さができるということです。いわゆる自殺ほう助サイトとか、そういうものでよく問題になるのは、今のこの刑事法の体系というのは、具体の犯罪、実際に「この人を殺すぞ」とか、実際に「ここの家の何を盗むぞ」とか、かなり具体性が出てこないと、共犯や、教唆犯として捕まえることができないようになっています。したがって、例えば「悪さの仕方を教えます」「自殺のやり方教えます」「犯罪のやり方教えます」とか、そんなサイトがあったときに、今の日本のこの刑法の体系では、基本

的には処罰ができないようになっているのです。

普通の犯罪ではないですけれど、有名なのはアルカイダが全国のイスラム教徒、世界中のイスラム教徒に向けてテロ、「こうこうこうやってやれ」というアルカイダ系のサイトというのが何千とあります。もちろん見つかったらそのプロバイダー等には削除要請などを、それぞれの国がしていくのだろうと思いますけれども、イタチごっこです。

日本の場合は「犯罪のやり方教えます」というだけでは犯罪にならないものですから、削除要請ぐらいはしますけれども検挙することはできないです。現実の世界で、昔、学生運動が華やかだったときに、爆弾の作り方を書いた本が出版されて問題になったことがあるのですけれども、当時、そんなものが流通するのは仲間内だけでした。現在のネットの場合はだれでも見られるものですから、それこそ、とっくの昔に忘れられていた「爆発物の作り方」なんかも結構載っているのです。

その影響度は口コミなら範囲が狭いわけですけれども、ネットではだれでも見られるというところがやはりすごく大変なわけであります。

●サイトを用いた金儲け

犯罪者にとっては非常に楽をしてもうける場所がいっぱいあるのが、このサイバー犯罪の特徴です。これが我々にとっても非常に大きな脅威の一つになっているのですが、ボットネットというのがあります。

これは何かと言いますと、このボットネットを立ち上げようとしている人が、不正アクセス等でいくつかの中心的なサーバーに侵入し、それを通じて今度はウイルスを作るのです。ウイルスを作って、感染させるのです。感染すると、ある日、このボットネット管理者が「よし、ここの企業を攻撃しよう」と決めると、このボット指令サーバーのほうにそういう指令を送り、すでに侵入することができるようにし

てあるサーバーに指令を出し、感染した個人や中小の事業者のパソコンに今度は指令を送って、ターゲットになったコンピュータに一斉に大量の文書を送りつける。そういう指令を流したりするわけです。ボットネットを使ったDoS攻撃のことをDDoS攻撃といいます。

ちょっと前のことですが、韓国とかアメリカで実際に政府機関のコンピュータが実際にやられました。

どういうやつがやっているのかまだよくわからないところがあります。一つはまさしく犯罪組織の人間。日本人がやっているのかどうかもわからないですけれどね。外国で捕まった例ぐらいしか私も知らないのです。それから、組織犯罪の人間が企業恐喝に使ったというのがあります。要は、「おまえの会社のコンピュータ、DDoS攻撃かけるぞ。かけられたくなかったら金よこせ」と言ってです。その捕まった例は金を取りにきたところで捕まったという、そんな、例があるわけですけれど、そういうふうに組織犯罪者が使うものもある。

防衛関係の専門家によると、これはいわゆるサイバー攻撃の最大の手段になると言うわけです。例えばある国が、これから隣国を攻めていこうというときに、先にこのボットネットによるDDoS攻撃で政府機関だとか、あるいは主要なインフラ、電気・ガス・鉄道だとか空港会社、そういうところのコンピュータをダウンさせて社会全体が動けなくなったところで実際攻めていこうというふうにするのではないかと、防衛の関係の専門家の方々は言ったりします。

そういう意味で、その専門家によると、いわゆる陸、海、空、宇宙の次の第5の戦場がこのインターネットであるとか言う人がいたりするわけです。

●サイバー犯罪のグローバル化

そこでサイバー犯罪に見る犯罪のグローバル化について考えてみま

しょう。これもちょっと想像すればすぐわかることですが、世界中どこからでも違法情報を発信することは可能です。

それからさっき見ましたように、日本語のサイトですけれども実はコンテンツは外国にあるということがあります。先ほど言いましたように、まっとうな活動をしているところでも、外国にコンテンツがあったりします。日本人が管理しているものでも外国から、あるいは、外国で何か犯罪がされた。例えば、管理している外国のコンピュータに、同じその国の外国人の人が不正アクセスをしたり何か悪さしたりしたとしても、日本の警察は、現行の法制では何もできないです。

それから、悪い人が日本の警察の追っ手をまくために、コンテンツを外国のコンピュータに置くケースがあります。外国でも違法な情報なんかをやっていると、削除したり、捜査したりすることはあるのですけれども、日本語サイトだと、外国の捜査機関にとってはやはりよくわからないということがあるものですから、なかなか捜査できないということで、わざわざ外国にコンテンツを置くということがあります。いますべての犯罪が全体的にグローバル化していると言われているのですけれども、このサイバー犯罪というのは、その典型的な一つです。

ちょっと前に起こった事案をひとつお話致します。犯罪と一応言えるのかなとは思うのですが。冬季オリンピックの後に、たしかキム・ヨナ選手の悪口が2ちゃんねるにちょっと出たということで、それを発端に韓国からすさまじいDDoS攻撃が行われたのです。ところが、この2ちゃんねるのサーバーはアメリカにあるのです。アメリカで一生懸命対応されたみたいですけれども、要するに韓国からアメリカですから、日本ははっきり言って犯罪の場所という点では関係ないわけです。実際に2ちゃんねるが見られなくなって日本のユーザーは困るわけですけれども、日本の捜査権限の外というようなことがあるわけです。

●サイバー犯罪のグローバル化とプロキシサーバー

プロキシサーバーという言葉もご存じかもしれませんけれども、要は中継サーバーというような意味です。「他人を装うためにその中継を受け付けますよ」という悪いプロキシサーバーというのも世界中にあります。要は、どこのだれかわからないように中継してあげますというものです。このプロキシサーバーが世界中にあります。あと自分たちで立てるというタイプ。

オンラインゲームで一生懸命やったら相手が何か非常に強くなっていくのです。一生懸命やっていると、強いアイテム、ゲーム上の武器がもらえるわけです。その武器が実は売買ができるようになっているのです。ゲーム上の武器が売買できるようになっていまして、その武器の売買市場があるのです。そこで、ゲーム上の武器を盗むために中国の犯罪グループが中国人の留学生に頼んでプロキシサーバーを国内に立ててもらう。なぜこういうことをするかというと、ゲーム会社は、中国人の犯罪グループがゲームの武器をよく盗むというのを知っているものですから、中国からの直接接続ができないようにしているのです。たとえば、日本国内でのオンラインゲームは、中国から直接だと接続できないようになっているのですけれども、国内にプロキシサーバーを立てて、それで不正アクセスをして、ゲーム上の武器を盗り、それを売買するというような犯罪があるのです。たかだかゲームのアイテムならいいではないかという話もないではないのですけれども、やっている人にとってはかなりショックなようです。すごくがんばって作るアイテムが盗られるというのは、被害者にとってはかなりショックだということのようです。

●海外サーバーの問題

それから、これもやはりさっき言いました海外サーバー蔵置の問題

です。海外サーバーの場合はもちろん当該外国で作られた外人の所持のものもあるのですけれど、日本人が、追っ手を逃れるために外国に蔵置するとかいうのもあります。

このように、ネットの世界は本当に国境がないのです。ネットには国境がないのですけれども、政府の機関とか法律の世界には、もう厳然として国境があります。警察機関ももちろん違いますし、それから刑法自体が違ったりすることがあります。やはり国境の壁というのは大きいと言われます。

それから通信の秘密の壁というのも、我々は非常に感じることがあります。もちろん通信の中身ですね。メールをやり取りしているメールの文言自体は当然守られるべきで、私ども捜査機関だって令状がなかったら見てはいけないのです。現在の電気通信事業法に「通信の秘密を守ろう」と書いてあります。あて先、送り先も通信の秘密なのだという解釈になっておりまして、そのため、捜査上難しいことがいろいろ起こるのです。

憲法にも通信の秘密を侵してはならないと書いてありますが、これはちょっと説が分かれていまして、あて先情報も憲法上の通信の秘密だという人もいれば、いや、それはちょっと違うんじゃないのという説と両方あります。少なくとも電気通信事業法という法律の上での通信の秘密は、あて先情報も含まれますので、令状を取らぬ限り、我々でもすぐにはわからないという壁があります。

そのため、皆さん方が、いわゆる民事訴訟とかで相手方を知りたいというときに、それがハードルになるということがあるわけです。

あと、ログの保存がなければ話にならないというのは、これは外国でもよく問題になるのですけれど、ログの保存問題と言いましてですね。今、大手のプロバイダーとかだったら３か月ぐらいは大体ログを保存していきます。ログというのは通信記録ですね。通信の中身は消え

ていますけれど、どことどこの間で通信が行われたというあて先は残してくれています。それがあると、犯罪者にたどり着くのです。

犯罪捜査の観点から言うと、3か月が短すぎるのです。日本の場合は本当に精密手法と言われていまして、皆さん方が思うよりも、いっぱい、いっぱい証拠を集めないと犯人の逮捕というのは実はできないようになっています。その証拠を集めるのに2、3か月ぐらいすぐたってしまうものですから、犯人の手前まで行ったときにもうログが消えているということが残念ながらあるということがあります。

●捜査機関の国際協力とサーバー犯罪

これは、フランスのリヨンというところに国際刑事警察機構、ICPOとかインターポールとか言いますが、国境の壁を一応ちょっとは超えようという仕組みなのです。ただし、これも、いろいろ問題点なり限界もあったりするのです。

ルパンⅢ世というアニメで銭形警部というのが出てきますね。「ICPOの銭形だ」と言って出てきますけれども、世界中にああいう銭形警部みたいな人って何人ぐらいいると思いますか、想像してみてください。千人ぐらいいるかな、数十人ぐらいかな。実は0なのです。いないのです。ICPOの職員はいるのですけれどね。各国の警察から出向してICPOの職員はそれなりにいるのですけれども、国を超えて捜査権を持っている警察官というのはいないのです。そういう意味で銭形警部みたいな人はいない。

このことには説明が必要かと思います。捜査権というのは国家主権の最たるものなのです。ですので、この日本でも、被疑者が外国に逃げた、ここにいるのがわかっているとしても、我々警察官が自分たちで行って手錠かけて連れてくることはできないのです。そういうときはそこの国の警察に頼んで捕まえてもらうというような手続きになっ

ていますが、その手続きがすごく大変なのです。

犯人を捕まえるだけではなくて、いろいろな情報交換も含めて、外国の捜査機関と連携をする仕組みは三つあるのです。

一つはICPOルートと言いまして、今紹介した国際刑事警察機構を通じた連携の仕組みです。これは警察機関同士で直にやり取りができます。ところが基本的には情報交換だけでして、例えば犯罪の証拠を取ってきてもらいたい、あるいは犯人逮捕してもらいたいというのは、このICPOルートではできないのです。情報交換だけです。さっきのログの問題とか、そういうのでできることはあるのですけれども、ログの問題でも、令状執行してやってくださいとかいうのはこちらではできません。

それから2番目。それでは本当に犯人逮捕したり、捜索、外国で捜索したりするときにどうしたらいいかというと、外交ルートというのがあります。都道府県警察から警察庁、警察庁国家公安委員会のほうへ行って、それから外務省にお願いして、外務省がそこの相手国の大使館、あるいは日本国内にある大使館に言って、それで相手国の外務省に言って、それから外国の外務省から外国の捜査機関に言って、それでやっていくというので、これは数か月大体かかるのです。さっきログの保存最大で3か月とか言っている話ではもう全然間に合わないのです。だけど本当の、本格的な捜査をしようと思ったら、実はこれをやらなければいけない。

もうちょっとマシにしようではないかというので、条約でバイの相手国と直にやる条約でもうちょっと楽にしましょうやというのをやるのが、第三の中央当局ルートと言いまして、検察庁系だったら法務大臣、警察系だったら国家公安委員会、警察庁のほうですけれども、そこから相手国の警察機関なり、法務省などに頼んでやる方法があります。令状の関係、強制捜査を伴う場合でも、この場合だったら使える

ようになっています。ただ、これは個別の条約がいります。日本はたしか、アメリカと韓国と中国ですね、3か国だったと記憶していますが、直接のやり取りができるようになっていますが、そのほかの国とはそういうような仕組みがない。

この仕組みがあっても、そんなにすぐではない。直接ですから、そこそこの連携はできますけれども、わりと暇がかかったりするということであります。

●サイバー犯罪のグローバル化と、今後の展望

インターネットの世界というのはこの世の中でも最も成長の速い分野です。いろいろなインフラ、私たちが活用できるいろいろな空間、新しい空間、いろいろなツールもどんどんと出ていくわけですけれども、残念ながら、法律、ある意味では法文化と言うのですかね、すごく変わりにくいのです。それから捜査権というのは国家主権の最たるものでありますので、お互いにそうそう勝手にできないというようなことがあります。

それから、これは、法律を改正したりはしておりますけれども、学界の中には、「法律などというのは普遍的・恒久的なものであるから、社会情勢などによって変えるなんてとんでもない」とかいう学説もないことはない。特に刑事法の世界ではそういう考え方が強いのです。そういう中でどうやったらいいのかということを、私どもは日々悩みながらやっております。

サイバー犯罪が発生しやすい内的な要因といたしましては、ツールを本人は単に技術者魂だと言って、本人自身が犯罪するわけではないけれども、犯罪に使えるようなツールを開発するのがいいことだと思っている人たちが若干いまして、そんな人たちが犯罪ツールを開発したりするということをあげることができます。

それから、そういう犯罪ツールを取り引きする場所がある。それから、楽をしてもうけたい犯罪者というのが、そういうノウハウを継承していく。私はこの2月に、今のポストに就いたばかりでこの世界では浅いほうなのですけれども、当初、このサイバー犯罪とかハイテク犯罪というのはすごく技術のある人たちがやっていると思っていたのです。実際は違っていまして、そういう人たちもいるのですけれども、そうではなく、昔から不良やってたような人たちが、「蛇の道は蛇」というようにノウハウを伝達するのだということがわかりました。こういう世界では、フィッシングから詐欺を働くようなグループ、元々大してハイテクではない人たちがやれるということがあったりします。

そうは言っても、私たちも指をくわえて見ているわけにはいかないものですから、サイバー犯罪の新しい手口に追いつくために、いろいろな努力を今しているわけです。

一つは新しい技術の開発です。警察庁には、情報通信局という技術者集団もあります。その中に情報技術解析課という、私は除法技術犯罪対策課ですけれども、そのちょうどパートナーみたいな技術的課があり、いろいろ研究をするわけです。サイバー犯罪の技術的な面での研究をします。さっきのファイル共有ソフトを捜査して検挙するという話をしましたけれども、新しいタイプのサイバー犯罪、高度な技術が使われているときにはどんなふうになっているのかというのを技術開発し解明する組織があるということがあります。

それから警察の捜査力を上げていくということも大事な分野であります。サイバー犯罪の担当者というのは、日本の警察の中ではまだまだ少ないほうなのです。日本で警察官が25万人ぐらいるのに対して、まだまだ極めて少ないです。人員の増強が必要です。

それから、本当の専門の担当者でなくても、ちょっと何か犯罪があったらすぐパソコンが出てくるし、携帯電話が出てくるわけですから、

一般の警察官でも、そこそこの知識が必要です。それを教えたりするという仕事も実は重要な仕事になっております。

それから、リアルの世界を念頭に置いた現在の法律の体系がうまく適合していないところがあります。これは警察が法律案を作って国会にお願いすることのできる分野もあれば、ほかの役所でないと権限がないところもありますが、この新しい法律で対応するということも必要になってまいります。

それからその次、国際的な連携をもっと緊密にやらなければいけないなということも大変大きな課題であります。

国際社会の中でもこのサイバー犯罪条約というのがあります。欧州評議会の条約なのですけれども、主要国も一応参加しております。日本は、一応参加することになっているのですけれども、条約ができたからといってすぐ国内で適用できるわけではないものですから、国内法の整備というのが実はできていなくて、ずっと宙ぶらりんになっております。

このサイバー犯罪条約に対応の中身をすこしお話します。例えば、ウイルスだとかマルウェア。これは現在では、作ったり配ったりしても基本的には犯罪にならないのです。このサイバー犯罪条約ではそれを犯罪にしなさいと書いてありまして、そのために国内法、日本の刑法を改正する法律案というのがずっと何年か宙ぶらりんでまだ通っていないという状況にあるわけです。

このいろいろな社会情勢に対応して法律を変えるという立法政策を考える仕組みと理論が本当は必要ではないかということで、私の経歴にもありますように、警察の役人をしながら、一定の研究をしておりました。それは、実際現実に適用する法律を作っていくためには、法律を設計する上で、現実がどうなっていて、それにどうやって適合させるかという発想が必要なのだと思います。しかし、法律学そのもの

はそんな仕組みになっていません。そこで法政策学というような発想もいるのではないかなということを申し上げて、今回の講演の締めくくりにしたいと思っております。

最後あまり時間がございませんが、質問をお受けしたいと思います。いずれにいたしましてもご清聴どうもありがとうございました。