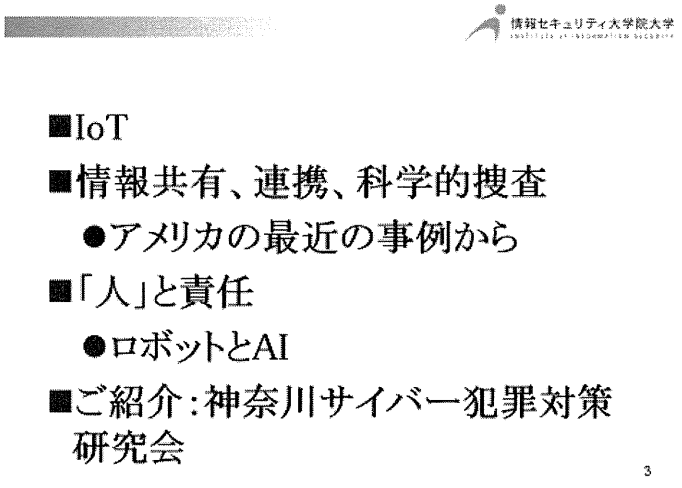
【基調講演③】サイバー空間の脅威に対処するための法制度の在り方

情報セキュリティ大学院大学教授　　湯淺　墾道

1　はじめに

今日は、サイバー空間の安全に向けて、どのような法制度をこれから考えていったら良いかを少しお話しさせていただく。非常に幅広いトピックを含んでおり、その全てを取り上げることは難しいので、まず最近よく聞くようになったIoT（Internet of Things）の問題をどう考えるかということを取り上げる。



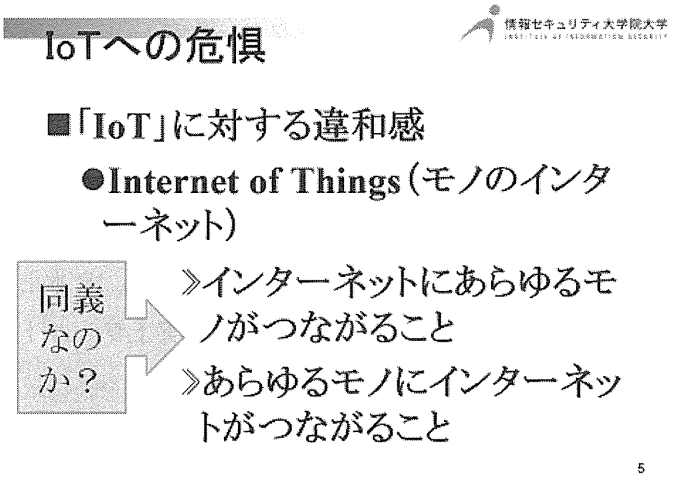
また、今日も既にウルクニエミ氏、ゴダート氏の基調講演の中にもあった情報の共有や連携を具体的に進めていく上で、日本の法律の下ではどういう制約があるかということや、あるいは、フォレンジックを進めていく上でどういう問題があるかということを、先進国の１つであるアメリカで最近裁判になった事例をご紹介しながら考えてみたい。

そして、最近ブームになっていることの１つにロボットの問題がある。日本では最近ドローンについての規制が注目されるようになったばかりであるが、ドローンとラジコンヘリはどこが違うのかと言われると、ドローンは自律をし得るところが１つの大きな違いだと思う。つまり、人間が操作をしない、あるいは人間が介在をしないものがこれからどんどん増えていく。あるいは、最近シンギュラリティという言葉が流行しているが、やがて人工知能が人工知能を作れるようになるかもしれない、そういう時が来るというような説が唱えられており、その際に法律との関係をどう考えていかなければならないかをお話しさせていただく。

2　IoT

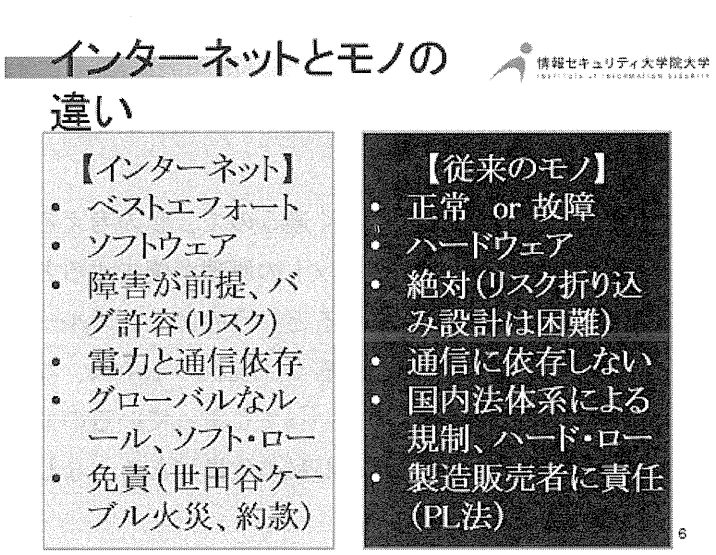
(1) IoTへの危惧

さて、最初にIoTについてお話しさせていただく。私も最近、プライバシーや個人情報の保護の関係で、技術系の学会や技術者の皆様がお集まりになる会合に招かれてお話しさせていただく機会が多々あり、その際よくIoTの問題が取り上げられる。しかし、私自身は正直なところ、IoTという言葉に対しては非常に違和感があるし、危惧を持っている。IoTは「インターネットにあらゆるモノがつながること」あるいは「あらゆるモノにインターネットがつながること」と日本語に訳している場合が多いが、これは本当に同じ意味なのだろうかと思っている。実は違うのではないかというのが私の考えである。



(2) インターネットとモノの違い

インターネットは、今日多くのサイバー犯罪を生んでいるが、それはサイバー犯罪を生む土台があるからである。まず基本的には、通信そのものが絶対的に安定しているものではないということ、常にベストエフォートでしか提供されていないこと、そして、ハードウェアではなくてソフトウェアによって制御されているので、マルウェアその他によって簡単に乗っ取られやすいことである。逆に言えば、ソフトウェア製品というのは、障害があったりバグがあったりすることを前提としており、完成品であることを求められていない。ソフトウェアはパーフェクトに動かなくて良いということになっている。



また、当然であるが、電力と通信がなければインターネットはつながらない。日本では2011年に東日本大震災と呼ばれる非常に大きな災害が起きた。当初は携帯電話・スマートフォン等がつながっていた地域も、次々に基地局の非常用発電機の石油がなくなり、電力供給が止まった途端につながらなくなってしまったのは、既にご案内のとおりである。

法律の面から考えると、実はインターネットは、国家権力を背景とした法律、私どもは

それをハード・ローと呼ぶようになっているが、ハード・ローではなくて、技術標準や様々な国際団体が定めた本来ボランタリーなルールによって統治される領域が非常に増えている。これを私どもは最近ソフト・ローと呼ぶようになってきた。

海外で購入したiPad、iPhoneを日本に持ち込んで、SIMカードをそこに挿して使う場合に、通信することは可能だが、いわゆる技適、日本の技術基準適合証明を取得していないものを日本国内で使うことは、本来は違法なはずである。しかし、事実上それはコントロールできない状態になっている。逆に言えば、日本と海外とで技術認証さえ同じ国際的な技術標準を通っているものであれば、事実上ワールドワイドで使えてしまうという問題がある。

最後に、何か起こったときの責任について、通信事業者にはそれを問わないというのが常識になっている。これはかつて30年以上前に、世田谷で当時の電電公社がケーブル火災を起こして以来の常識になっている。これがインターネットの世界のルールである。

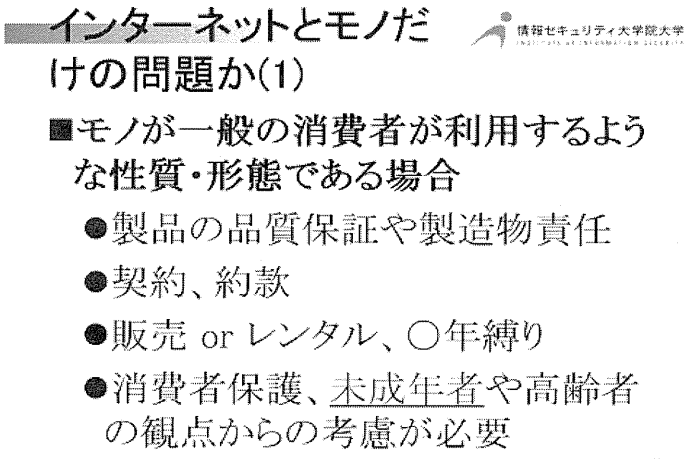
これに対して、モノというのはインターネットと全く違うものであり、正常に動くか故障するかどちらかでしかあり得ない。制御の対象となっているのは基本的にはハードウェアである。特に原子力発電所などのように非常に大きなものについては、故障する可能性があるということは分かっていても、現実に事故を起こすかもしれないという前提で建設することは事実上許されない。

基本的には、今までのモノというのは国内の法律で規制することができた。具体的には、例えば製造物責任法で製造物の欠陥により損害が生じた場合に製造者等に責任を負わせることが可能である。

このように両方の考え方は全く違うので、私の考えるところ、インターネットにモノをつなげるというのはインターネットの原理が優先するということを意味するであろうし、モノがインターネットにつながるというのはモノのルールを守ったままでインターネットにつなげることを意味するであろう。現状のIoTは、なし崩し的にインターネットのルールにどんどんモノを取り込んでいってしまっているのではないか、そうしているのではないかと見えてならないというのが私の危惧である。なし崩し的にモノに関するルールがなくなりつつあるように思う。

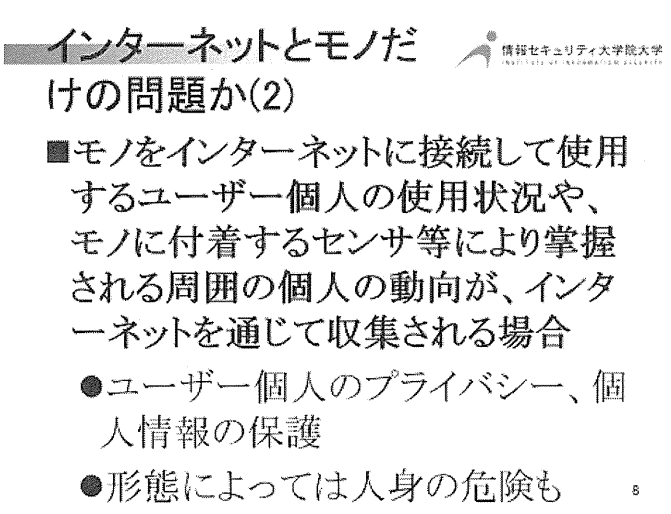
(3) インターネットとモノだけの問題か

その時に幾つか考えなければならない点がある。インターネットにつながるものが一般の消費者が利用するようなものである場合には、さまざまな品質保証や製造物責任、あるいは販売なのかレンタルなのかという



問題も生じると思うが、一番留意すべきなのは未成年者に関する問題である。今日、未成年者がサイバー犯罪の被害者になる場合もあれば、加害者になっている場合も多々見受けられる。正直なところ、子どもに対するサイバー犯罪に関する教育の機会は全く不十分なのが現状である。各都道府県警その他のレベルにおいて、サイバーパトロール又はサイバー出前講座のようなものを学校で行っているが、現実に小学生でも不正アクセス禁止法で禁止されていることを犯し得る時代であり、学校の正規の教育の中にサイバー犯罪に関する内容を入れていかないといけない。この教育に関する問題は、非常に重要であると思われる。

２点目は、あらゆるモノがインターネットにつながってきた時の最も大きな懸念として言われているプライバシーと個人情報保護の問題である。これは別にサイバー犯罪を考える上では大きな問題ではないととらえられるかもしれないが、情報化の進展によって、個人情報やプライバシーの持つ意味が大きく変わってきている。

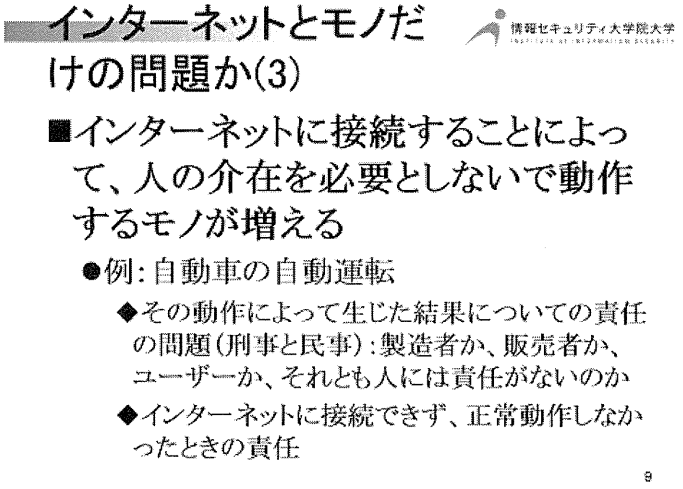


例えば、以前は住所については、こんなに神経質に取り扱う必要はなかったように思う。しかし、今日では、住所さえ分かってしまえばグーグルのストリートビューにそれを入れることによって、家の形あるいは庭の形がどうなっているかということすら検索可能である。将来的にはライブストリートビューのようなものになってきて、今現在家に灯りがついているとか、今は無人に見えるというようなところまで、インターネットで提供される時代になるかもしれない。そうすると、プライバシーや個人情報をどう守るかについての法律の改正・強化が必要になってくるだろう。

要するに、プライバシーや個人情報は、主観的なあるいは精神的な問題ではなくて、現実に人身の危害が生じ得るし、現に危害が生じている問題だということである。したがって、適切な法制度によって、人身を守っていかないといけない。

３番目は非常に大きい問題であるが、インターネットに接続することによって、人の介在を必要としないで動作するモノがどんどん増えていくであろうという問題である。その一例が、最近話題になっている自動車の自動運転の問題である。日本では外国にも負けないように自動運転の開発を進めていくということになっている。既にアメリカなどでは幾つか実証実験的なものが行われているが、事故も起きていることは皆様もご存じかと思う。半分冗談かもしれないが、自動運転の車のドライバーが寝てしまったので自動運転の車がドライバーを置き去りにしてどこかへ行ってしまったとか、そのような事例も報じられて

いる。これは本当に起こり得ることである。

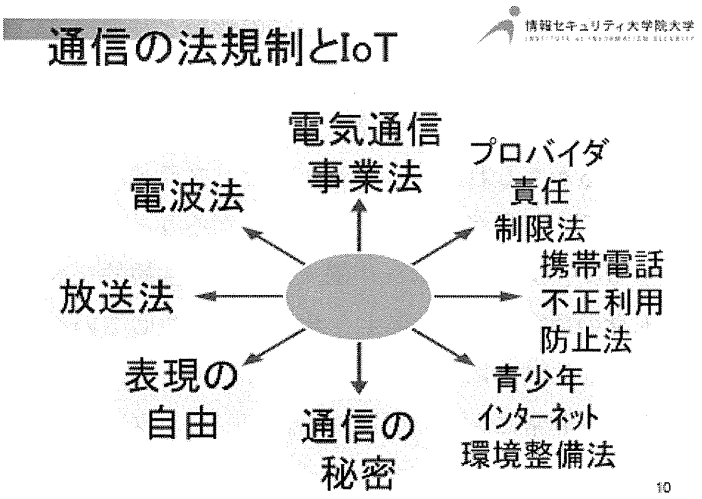


やはり一番の問題は、人間の介在を必要としないで動作した結果、事故が起きた時にその責任は誰が取るのかという問題である。これは刑事と民事の両方の責任が生じ得るが、そういうものを作った製造者なのか、そういうものを販売した販売者なのか、それともユーザーなのか、それとも人間が介在していないのだから人間には責任はないのか、ここが非常に曖昧なまま自動運転をどんどん実用化しようということで進んでいるように見える。

さらに、通信が途絶したらどうなるか。先ほど申し上げたようにインターネットはベストエフォートであるから、切れるということは当然あり得る。通信が切れたために動作しなくなった場合には一体誰が責任を取るのかも考慮しながら、法制度を作っていく必要がある。

(4) 通信の法規制と IoT

最後に、通信の問題である。今日はウルクニエミ氏とゴダート氏のお二方からご講演をいただいたが、日本の法制度の一番大きな特色は、通信の秘密が法律上の権利・義務ではなく、憲法上の規定であるということである。したがって、通信の秘密は常に非常に大きな壁として立ちふさがってきた。最近、サイバー犯罪の捜査のために、通信の秘密の今までの厳格な解釈を少し緩めようという努力が行われているが、依然として非常に大きな問題として立ちふさがっていることは間違いない。



さらに、通信の秘密の問題だけではなく、通信の法規制が非常に様々な法律に分散している。通信事業者を規制する法律、電波を規制する法律、放送に関する法律、インターネ

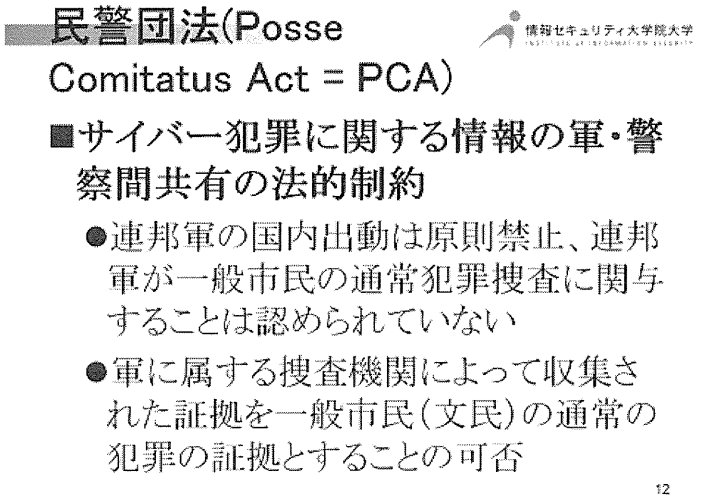
ットサービスプロバイダー（ISP）に関する法律、携帯電話に関する法律、その他非常に大きく散らばっている。これらをもう１回リセットして新しい法律を作り直すことは非常に大変な作業である。かといって、何かサイバー犯罪を防ぐための新しいルールを作ろうと思ったときには、これら全てのルールとバッティングしている箇所を全て調整しなければいけないというのが現状である。果たして通信法制の全体構造はこのままでいいのだろうか、ということが近い将来問題になるのではないか。以上、IoT について最近私が考えていることを申し上げさせていただいた。

３　情報共有、連携、科学的捜査―アメリカの最近の事例から

次に、本日のテーマにもなっている連携を具体的に進める上で、やがて日本でも問題になるかもしれない事例を幾つか取り上げてみたい。

(1) 民警団法（Posse Comitatus Act = PCA）

この後、JC3 の坂理事からお話をいただくように、日本でも最近、情報の共有・連携が始まったばかりである。情報共有や連携の先進国の１つであるアメリカでは、共有の在り方をめぐって早くも幾つかの訴訟が生まれてきている。

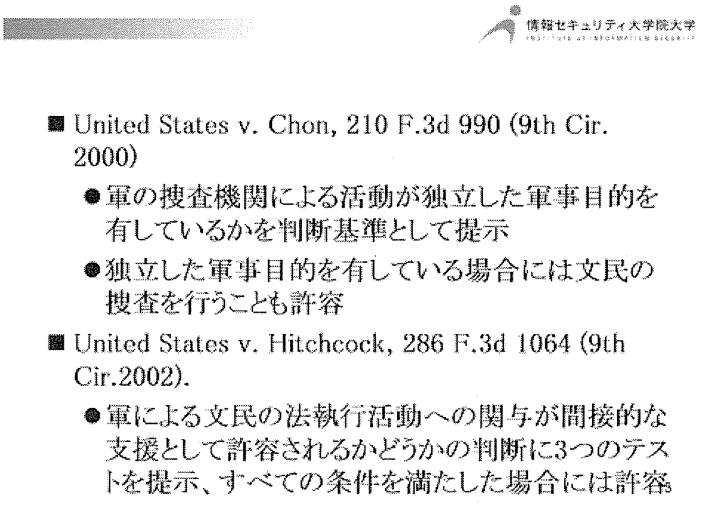


ちなみに、これはアメリカ特有の制約であるが、アメリカでは軍が法執行（law-enforcement）、つまり警察活動に関わることは原則として禁じられている。これは、Posse Comitatus Act（PCA）という連邦法によって禁じられているためである。したがって、軍が収集した証拠を文民の犯罪の証拠にするということは禁じられている。先ほどゴダート氏のお話の最後にインテリジェンスとロー・エンフォースメントの連携の話があったが、アメリカでは基本的にはディフェンスとロー・エンフォースメントの間で連携をすることについて法律上のバリアがある。

さて、この問題に関していくつか裁判例が出ている。今から十数年前に日本でいう高等裁判所に当たるフェデラルサーキットコート(Federal Circuit Court)で、軍の捜査機関による活動が独立した軍事目的を持っているのであれば、軍がその活動においてシビリアンのロー・エンフォースメントと連携して捜査を行っても構わないという判決が出ている。

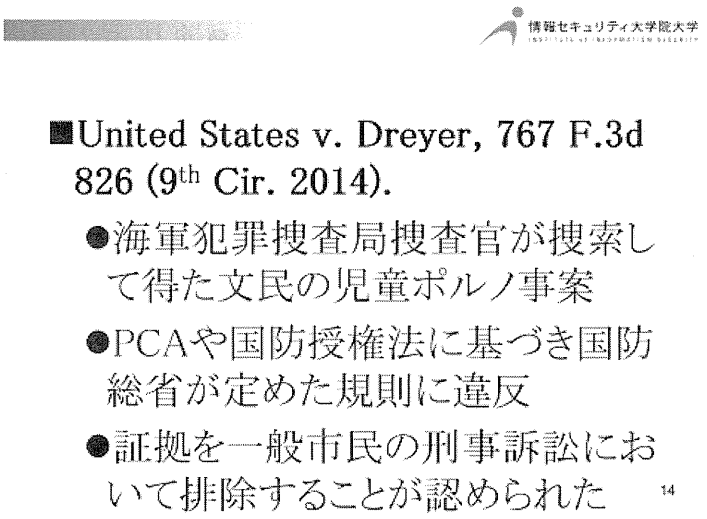
さらにその２年後、United v. Hitchcock という判決で、具体的にそれはどういう場合

であれば許されるのか３つの基準を出して、その３つの基準にすべて合っているのであれば共有して構わないということが述べられている。今日は時間がないので詳細なテストの中身をご紹介しないが、この 10 年ほどは、この流れに沿って、安全保障機関である軍と法執行機関である警察との間である程度の情報共有が進んできたということである。



ところが、昨年、次のような判決が出た。海軍の犯罪捜査局の捜査官が捜索して得た文民の児童ポルノに関する事案であるが、海軍の捜査官がラウンドアップというツールを使ってファイル共有ソフト（P2P）であるグヌーテラによってシェアされている児童ポルノのファイルを検索していたところ、ある IP アドレスのパソコンの中に大量の児童ポルノがあることを突き止めた。

インターネットサービスプロバイダに照会して、この IP アドレスのコンピュータを使っているのは誰かという情報を入手し、それについて調べてみたところ、軍人ではないことが分かった。その時点で軍としては、これ以上の捜査をすることができないので、ここまで調べて得た情報をあとは警察の方で捜査をしてほしいと言って渡した。警察ではその得られた証拠をベースにさらに捜査を行い、被疑者の家に家宅捜索を行い、コンピュータを押収してデジタルフォレンジックを行ったところ、暗号化されていた大量の児童ポルノのファイル類を見つけたので起訴をしたという事例である。



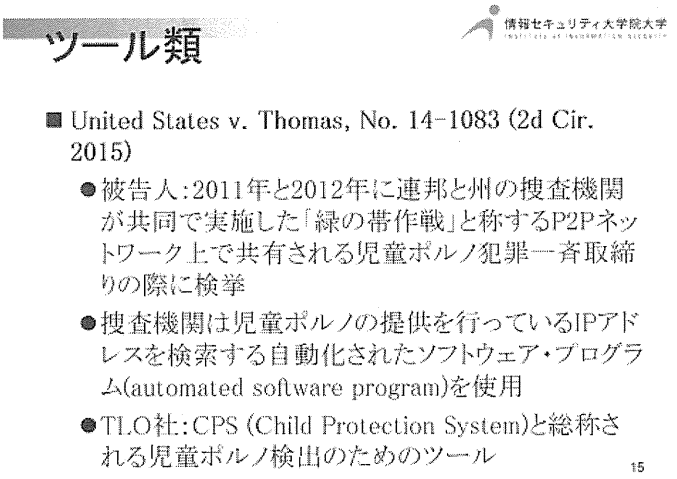
そうしたところ被告人が、これは先ほどもご紹介した Posse Comitatus Act（PCA）に違反していると主張したのである。軍の捜査機関が最初に着手して得た証拠を基に文民を起訴することは違法であると被告人が訴えた。そして、何と驚くべきことに、その訴えは認められてしまった。被告人には第９連邦管轄巡回裁判所において無罪判決が出ている。こ

れまでの 10 年少々、情報に関する連携について、こういう条件の下であれば共有することが許されるとされてきたのがひっくり返ってしまったという事例である。

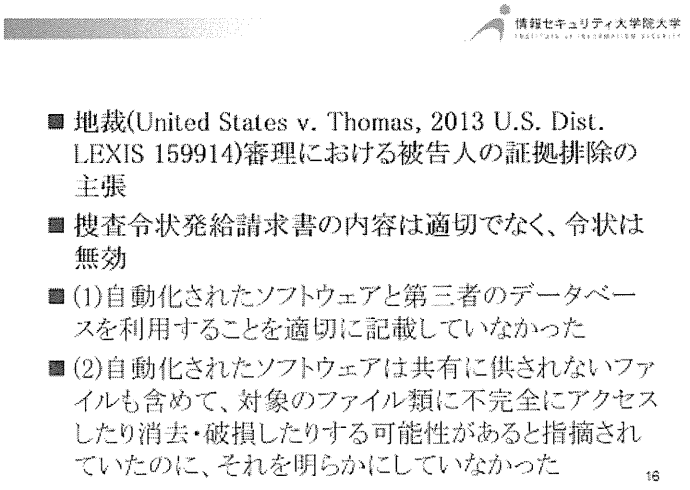
もちろん、日本はアメリカとは全く制度が違っているから直接の参考にはならないかもしれないが、あのアメリカにおいてすら、性質の異なる機関の間での情報の共有には法的な制約がかなり大きいということを示す１つの例である。

(2) ツール類

もう１つはツール類についてである。これは逆に捜査機関が高等裁判所で勝った事例である。この事例では、児童ポルノを提供している IP アドレスを検索するための自動化されたソフトウェアプログラム（automated software program）、具体的には TLO という会社が提供している CPS (Child Protection System) と呼ばれるツールを使って、警察が捜査を行った。高等裁判所では警察側の主張が認められて被告人の訴えは退けられたのだが、地方裁判所において被告人は、ツールの利用に関して次のようなことを訴えている。ツールを使うということを適切に記載しておらず、また、そのツール類によってフォレンジックする際に証拠が壊れる可能性があることを黙っていた。

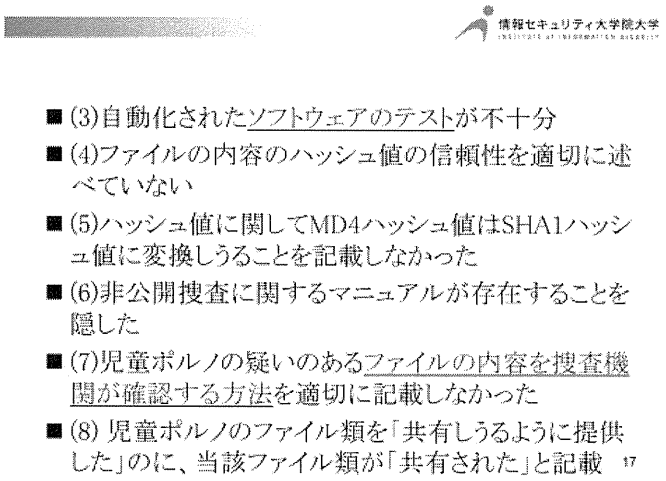


一番の問題は、ツール類が本当に正しく動作をしているかどうか、公的な機関においてテストされていないのではないかという点であり、この点を被告人は主張した。実はここが、日本のデジタルフォレンジックの抱えている問題の１つかもしれない。海外製のツールも含めてさまざまなツールが使われているが、必ずしも公的な機関によってきちんと動作の確認を経ないで使われているツールもあるように聞いており、日本においても問題になる点だと思っている。



もう１つが(7)に記載されている問題である。そのツールは、どういう原理でどうやっ

て証拠を確実に復元しているのかが必ずしもきちんと確認できていないではないか。言葉を換えると、フォレンジックツールがブラックボックスではないかという主張である。

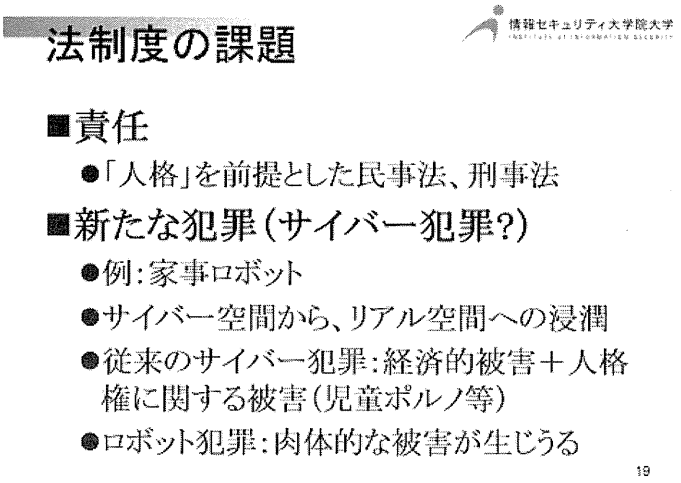


このような主張について、一部それが認められるような事例が出てきている。

このような問題が現実にアメリカでも生じている以上、今後、日本においても同様の問題が生じる可能性がある。

4　「人」と責任（法制度の課題）

最後に、今後の法制度の課題として、日本において最も問題になるであろうことを幾つか申し上げて終わりたいと思う。



基本的に日本の法律は人格をベースにした法体系になっており、これは民事法も刑事法も変わらない。民事においても刑事においても、人格を基に責任が生じ得るということである。したがって、人格がないところには責任は生じないし、自然人でないものには、特に法律で授権されていない限り、そもそも権利能力はないということになっている。

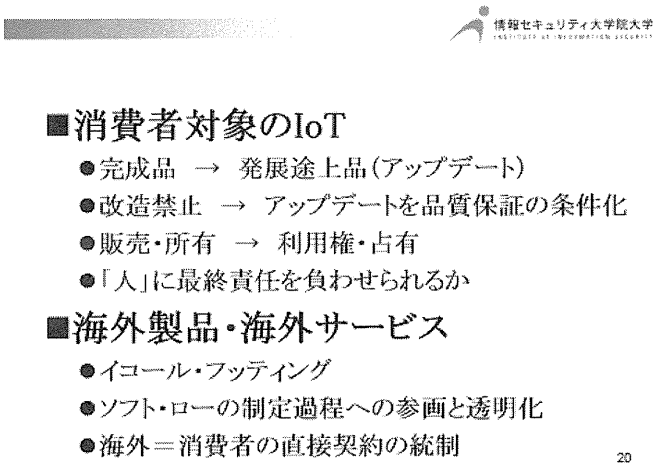
しかしながら、今後生じ得る新たな犯罪の中には、人格がないものによって発生させられるサイバー犯罪がかなり増えてくることが予想される。例えば、今後家事ロボットが家庭にもどんどん普及すると考えられるが、家事ロボットがサイバー攻撃を受けたりして乗っ取られた場合には、家事ロボットが人間を攻撃して人間が怪我をするなど、サイバー犯罪が家庭の中のリアル犯罪の方に入り込んでくる。そうすると、一体これについては誰に責任があるのか。

ロボットには人格がないから、ロボットを罰することはおそらくできない。そのロボットがマルウェアに感染した場合、もちろんマルウェアを作った人間が悪いわけだが、ロボットの脆弱な制御システムを作った人にも責任を負わせることはできるのか。あるいは購

入者、そのロボットを家庭で使った人間に責任があるのか。こういう問題は必ず生じてくると思われる。

つまり、従来のサイバー犯罪の多くは経済的な犯罪であり、また、児童ポルノのように人格に関わるような犯罪が多かった。しかし、ロボットが乗っ取られた場合には、まさに肉体的な被害が生じ得るので、かなり重大な犯罪になってくることが考えられる。そうした場合に、どこに人格があるのか分からないのである。一体その時にはどうやって人に責任を問うことができるかという、非常に難しい課題がある。

そういうことを考えると、今後ますます消費者を対象とした製品がインターネットにつながってくると思うが、今までの考え方を大きく変えないとおそらく対応できないだろう。現在は製品というのは完成品であることが前提になっているが、これからは発展途上品であると考えないといけないのではないか。それから、現在では製品は改造すると保証を受けられなくなるが、今後は逆で、改造しないまま、つまりアップデートをしないまま使っていると保証を受けられないというように変えていかないといけないのではないか。また、所有の在り方も変えないといけない。つまり、販売したものについて購入者に所有権があるままでは、販売者がリモートによりアップデートすることは難しいので、その点を考えていかないといけないだろう。



何よりも、今申し上げたように、人が介在しないのに犯罪が起こり得る、人が介在しないのに現実に被害が起こり得る時に、誰にその責任を負わせることができるかということを考える必要がありそうである。

さらに申し上げると、消費者が海外の製品や海外のサービスを直接利用する場合が今後ますます増えてくるように思う。その際に、日本の国内事業者の間から、国内事業者は日本法において非常に厳しい規制を受けているのに、海外事業者はその規制を受けていない、アンフェアだという主張が既にかなり強く出てきている。これは、最近イコール・フッティングと言うことがあるが、イコール・フッティングを実現しないと、国際的な競争上、日本の事業者の競争力が落ちて負けてしまう。これをどう考えるかという問題もある。

さらに、先ほど申し上げたようなソフト・ローや技術標準の制定に日本としてどのように関わっていき、また、そのガバナンスをどうするかという問題もある。場合によっては、かつてギャンブルサイトを日本国内から利用する人が増えたときに問題になったように、消費者が直接海外サイト・海外サービスを利用することを規制するということも、法的に

は考えざるを得ないかもしれないと私は最近考えている。

５　ご紹介

最後に１つご紹介をさせていただきたい。サイバーセキュリティ、そして安全なサイバー空間を実現するための非常にささやかな試みではあるが、私ども情報セキュリティ大学院大学、NPO 情報セキュリティフォーラム、神奈川県警察が連携をして神奈川サイバー犯罪対策研究会というものを発足させた。３カ月に１回ぐらいの間隔で研究会を開催しているが、これはまさに情報共有をすることが第一の目的で、県警からは最近のサイバー犯罪の傾向あるいはサイバー犯罪の最新動向を提供していただき、私どもはそれに対抗するための技術、あるいは私がホストをするときにはサイバー犯罪に対応する法制度の最新の知見について、研究者や弁護士の先生方においでいただいてお話ししていただくという研究会を行っている。

実は、神奈川県警だけではなくて、時々ゲストメンバーとして埼玉県警、千葉県警など他の警察の方にもご参加いただいている。もしご興味がある方がいらっしゃったらぜひご連絡いただき、ご参加いただきたいと思う。

最後に、まとめとしては、人が介在しない犯罪、人が介在しない様々な被害がますます増えていったときにどのように対応する法律を作るかというのが、今後の私どもの課題と考えている。警察の方々とも連携しながら、この課題について検討していきたい。

【パネリスト発表①】サイバー空間の脅威への対処

警察庁長官官房参事官（サイバーセキュリティ担当）　白井　利明

１　はじめに

私は、警察庁の長官官房でサイバーセキュリティ担当の参事官をしている。私からは、「サイバー空間の脅威への対処」ということで、最近における日本警察の取組を簡単にご説明させていただきたい。

最初に、長官官房参事官というのは聞き慣れないポストだと思われる方もいらっしゃるかと思うので申し上げると、私の上司である長官官房のサイバーセキュリティ担当の審議官と併せて平成 26 年の４月に設置されたポストであり、現在やっと１年半たったところである。

警察のサイバー関係の取組というとサイバー犯罪対策、サイバー攻撃対策ということで、サイバー犯罪対策であれば生活安全部門であるし、サイバー攻撃であれば警備部門である。そういった部門の技術支援をする情報通信部門というものもある。こういった部門でこれまでサイバー犯罪対策、サイバー攻撃対策を講じてきている。

それに加えて、なぜ昨年長官官房に参事官、審議官ができたのかということである。今年の日本年金機構事案も１つのターニングポイントであるかもしれないが、ご案内のとおり、一昔前まではサイバー犯罪対策であれば生活安全部門、サイバー攻撃であれば警備部門がやっておけばいいというようなことが通用する時代であったが、今はそういう時代ではなくなってきている。

加えて、警察はいつも外側のところばかりに気を配っているのだが、ナショナルセキュリティという観点から申し上げれば、警察も非常に重要な情報を持っており、そういった内側の情報セキュリティの部分もきちんとやらなければいけない。

また、先ほど湯淺先生からもお話があったとおり、新しい事案、これまで考えもつかなかったような事案も起きるような世の中になってきている。５年後に 2020 年のオリンピックを控え、やることはいっぱいあるが、警察も部門横断的に組織を挙げてやっていかないといけない時代になり、長官官房という、会社であれば総務部門のところで施策をまとめて進めていく部署が必要になったということで、施策を進めている状況である。

前置きが長くなったが、私が常々室員に言っているのは、「サイバー犯罪やサイバー攻撃に従来から問題意識を持ってやっている人たちは良い。そうではなくて、自分たちは関係ないと思っているような部門の人、県警の人、それから仮に幹部職員の人がいれば、我々の営業対象はそういうところにある。」ということである。ぜひ警察一丸となってサイバー空間の脅威に対抗していきたいと考えている。

２　サイバー空間をめぐる脅威の情勢

それでは、説明に入らせていただく。まず、簡単に情勢をご説明したい。警察にいらっ

しゃる方には改めて申し上げるまでもないが、サイバー犯罪については生活安全部門でやっているものであり、典型的なものとしてはインターネットバンキングに係る不正送金事犯などが最近非常に大きな問題になっている。

サイバーテロ、サイバーインテリジェンス、海外ではサイバーエスピオナージと呼ばれているが、こちらがサイバー攻撃対策であり、警察であれば警備部門で対応している。サイバー犯罪、サイバー攻撃を分類し、簡単に申し上げるとこの３つになる。

26年中のサイバー犯罪は、ネットワーク利用犯罪、不正アクセス禁止法違反、刑法に規定するコンピュータ・電磁的記録対象犯罪等で、年間8,000件ぐらい検挙しているという状況である。

インターネットバンキングに係る不正送金事犯ということでは、平成24年は5,000万円ぐらいしか被害がなかったのが、26年の１年間で約50倍の29億円、27年の上半期では15億円の被害が発生した。以前は都市銀行に対する被害が多かったが、27年上半期の特徴としては、弱いところに攻撃が行っているということで地方の信用金庫等、多くの金融機関に被害が出てきている。

次に、サイバーインテリジェンスとサイバーテロに関する事例である。サイバーインテリジェンスは先ほど申し上げたとおり年金機構事案ということで今さら申し上げるまでもない。サイバーテロに関して、攻撃によりシステムがダウンしてしまった事例として、海外の事例であるが、26年のソニー・ピクチャーズエンタテインメントに対する攻撃、27年に入って、ISILの賛同者と称する者によってフランスのテレビ局のシステムがダウンした事案が起きている。

脅威の情勢について、７月に実施した世論調査であるが、インターネット利用犯罪は増加するかということに関して、国民の肌身の感触として当然増えると90%以上の方が回答している。インターネット利用をしていて非常に不安に感じることとしては、個人情報が取られるのではないかということである。この調査は年金機構事案の直後だったので、このように非常に不安感を持っている。サイバー犯罪等に関する相談件数も１年間に12万件に届くような数で増えている。

以上が情勢である。

３　政府におけるサイバーセキュリティ

そういった情勢を受けて、政府におけるサイバーセキュリティということで、27年に新しくサイバーセキュリティ基本法が施行されたことに伴い、内閣官房にサイバーセキュリティ戦略本部が置かれ、NISCがその事務局として機能する形になっている。

また、27年の９月に政府の戦略が出されている。こちらについては、年金機構事案前に出るという話はあったが、年金機構事案の発生を受けてそれの対処も含めた形で９月に出ている。

政府の戦略の中で、サイバー犯罪対策、サイバー攻撃対策といった警察の伝統的なサイ

バー関係の業務は安全・安心関係、安全保障関係の施策の部分に位置づけられるが、私としては県警の方などに申し上げる際には、経済社会の活力の向上及び持続的発展という部分を見落としてはいけないという話をいつも強調している。例えば、セキュリティマインドを持った企業経営の推進、経営層の意識改革、組織内体制の整備という点について、餅は餅屋に任せておけばいいというような時代ではなくなって、会社全体、組織全体でセキュリティを考えていかなければならない時代になったということを警察部内では強調して申し上げている。

４　警察におけるサイバーセキュリティ

次に、警察におけるサイバーセキュリティである。冒頭申し上げたとおり、審議官、参事官が長官官房におり、警察各局のサイバーセキュリティ全般を担当している。局によってサイバーとの関与に濃淡はあるが、この時代、リアルとネットがこれだけくっついている中で、ネットのことを考えなくていいという局はない。警察業務を実施するに当たってはサイバーのことを必ず考えていただくということで、横串的に見ている状況である。

今年９月に政府戦略と併せてサイバーセキュリティの戦略を出している。対処能力の強化、サイバー空間の脅威の低減、組織基盤の強化という３本柱である。対処能力の強化とサイバー空間の脅威の低減の部分はこれまでサイバー犯罪、サイバー攻撃対策をやってこられた方々にとってみればその延長線だが、この戦略で強調したいのは組織基盤の強化の部分である。部門横断的にサイバーセキュリティのことを考えていかなければならない、外側と内側のこともしっかりと考えなくてはいけないというようなことを特に強調して、県警の方などにもお話しさせていただいている。

５　対処能力の強化

この戦略に基づいて、細かいところは割愛するが色々な取組をやっている。対処能力の強化ということで、これは技術サイドの話であるが、デジタルフォレンジックの関係やサイバーフォースセンターにおける 24 時間体制でのサイバー攻撃に関する予兆把握といったものについての能力強化などを図っている。

通信履歴、ログの保存の関係については、「電気通信事業における個人情報保護に関するガイドライン」の解説が６月に改正されたということで、多少捜査にとって環境が好転する部分かと思っている。

人材育成についても、これまでもやってきているが、サイバー犯罪捜査やその指揮といったことに加えてサイバーセキュリティの運営といったところも、逆に言うと警察の幹部を対象にしてそういった意識を持っていただくような人材育成の取組、研修なども導入してまいりたい。

６　官民連携の推進

続いて、官民連携については、５年後のオリンピック・パラリンピックを見据えて、それぞれ重要インフラ事業者や大会の組織委員会、運営関係者とのネットワークを作っている。ロンドンオリンピックのときにもかなり攻撃があったという話を聞いており、５年後にどういった状況になるか分からないが、対応してまいりたい。

オリンピック以外でも、それぞれ重要インフラ事業者、先端技術を有する事業者等との連携の枠組みも幾つか作って推進しているところである。

これは後ほど坂理事からお話があるところだと思うが、日本サイバー犯罪対策センター（JC3）については26年11月に業務を開始し、１年たったところである。産学官の情報共有の枠組みを国レベルで作っている。

都道府県警察の産学官の連携の枠組みについては、大企業は色々対策を講じる費用もあり、問題意識も高いが、日本の企業は中小企業が殆どであり、ノウハウもなく、対策したくてもお金をかけられないという現状である。そういったところにきめ細かく働き掛けていくことは、日本警察が持っている強みを生かせる部分かと思っている。都道府県警察の方々に先駆的な取組をしていただいている状況である。

７　国際連携の推進

最後に国際連携についてである。今日は INTERPOL Global Complex for Innovation（IGCI）、European Cybercrime Center（EC3）のお二人にもいらしていただき貴重なお話を伺ったが、国際会議への参画、外国捜査機関・国際機関等との共同オペレーションもある。テイクダウンについては先ほどお話もあったが、そういった機関、民間の方々との協力も不可欠である。それから、ネットワークの強化も進めてまいりたい。キャパシティビルディングについても先ほどお話があったが、我が国警察としてもアジア地域を中心にキャパシティビルディングを進めてまいりたいと考えている。

【パネリスト発表②】サイバー犯罪と戦う産学官協働の取組－日本サイバー犯罪対策センターJC3の活動―

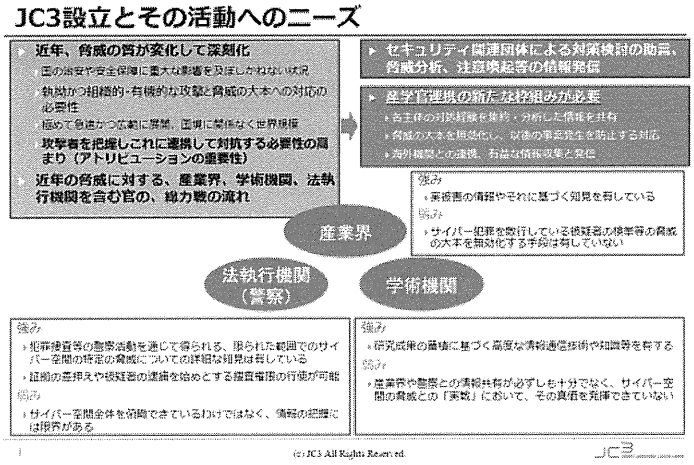
(一財)日本サイバー犯罪対策センター理事　　坂　明

本日は、ご指導をいただいている先生方、あるいは日本サイバー犯罪対策センターのプラットフォームでともに脅威と戦っている同志の皆様がたくさんいらっしゃっており、ともに戦っている皆様の思いを会場の皆様に伝えられるかなと心もとないところはあるが、頑張って色々お話しさせていただければと思う。

１　JC3設立とその活動へのニーズ

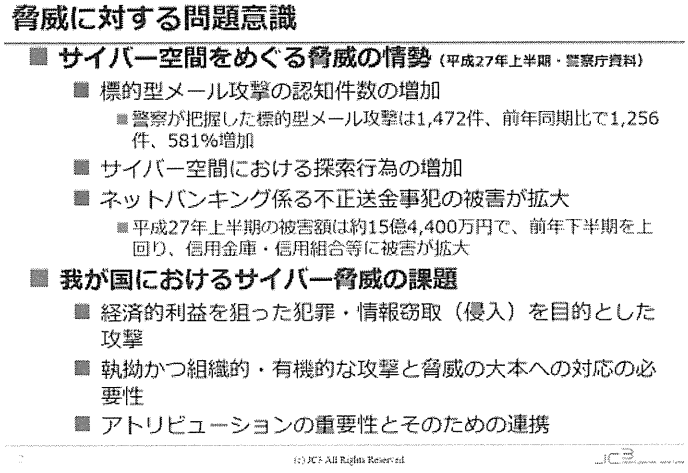
まず、私ども日本サイバー犯罪対策センター（JC3）の設立とその活動へのニーズということでお話しさせていただく。

何でJC3かだが、Japan Cybercrime Control Centerということで、JapanのＪとＣが３つということでJC3という略称にさせていただいている。



JC3設立とその活動へのニーズだが、オレンジのところを見ていただきたい。先ほど来ずっとお話があるとおり、近年、脅威の質が変化して深刻化している。その点について言うと、攻撃者が、経済的な利益、情報の窃取あるいは組織に対する攻撃など明確な目的を持って、執拗に攻撃をしてくる。先ほども弱いところを突くというお話があったが、弱点を突く、そうしたことを組織的にやってきている。そうした意味では攻撃者を把握して、これに連携して対抗する必要性が非常に高まっている。言いかえれば、アトリビューションの重要性が認識されてきているということかと思う。

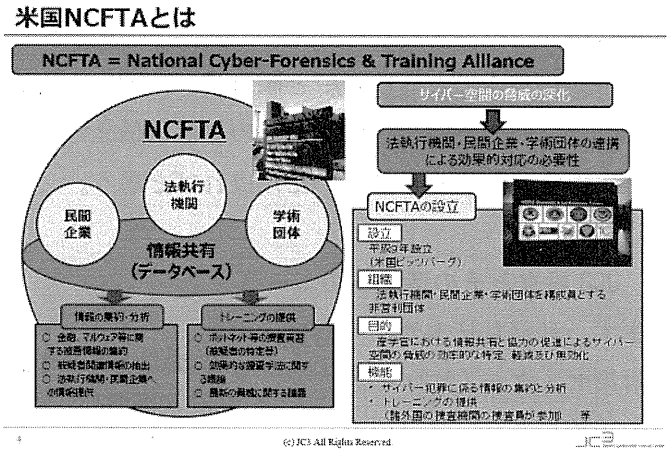
こうした近年の脅威に対して、産業界、学術機関、法執行機関を含む官の総力戦を行っていく必要があるのではないか、という認識が高まった。こうした流れを踏まえて、JC3という、産業界、学術機関、そして法執行機関が協働して立ち向かうための体制が作られた。しかも、そ



れが民主導で作られたというところに大きな意味があると考えている。

２　米国 NCFTA とは

JC3 の設立の経緯だが、実は警察政策研究センターで主催されたフォーラムで２年前に、私どものモデルである米国 NCFTA のプレジデントのマリア・ヴェロさんがお見えになってお話しをされた。その際のセミナーにも参加されている方がいらっしゃるかもしれない。



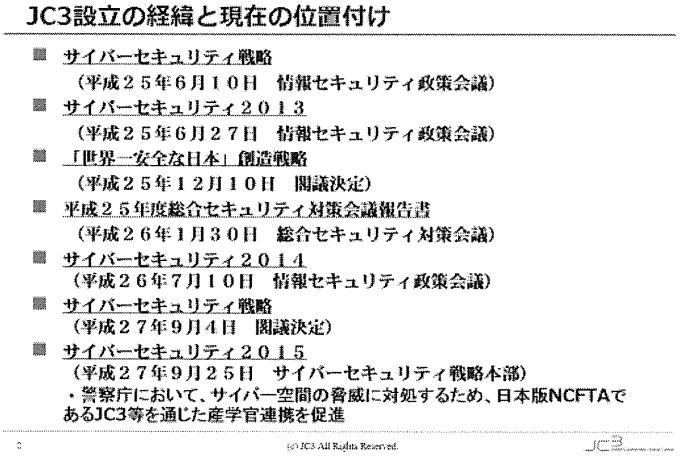
NCFTA は National Cyber-Forensics & Training Alliance の略である。民間企業、法執行機関、学術機関がいわば一体となって情報共有をし、その情報の集約・分析を行い、脅威に立ち向かう。そして、トレーニングを提供するということであるが、これもいわば実践の中で関係者を鍛え上げていくということである。そうしたトレーニングも通じて大きな成果を上げているというところである。

オープンになっている情報でも、平成９年の設立以来、300 以上の事件の検挙に貢献している。NCFTA は、秘密保持契約を、会員の方々あるいは私どもと結んで情報を共有しながら活動を進めており、実態を申し上げられなくて私も歯がゆいところがあるが、公になっている活動以上のすばらしい成果を上げておられる。

NCFTA の特徴は、法執行機関と民間企業、学術機関の方々がいわば席を並べてともに勤務をして信頼関係を構築し、その信頼関係をベースにさまざまな脅威に立ち向かっていく。ここに１つの特徴がある。

３　JC3 設立の経緯と現在の位置付け

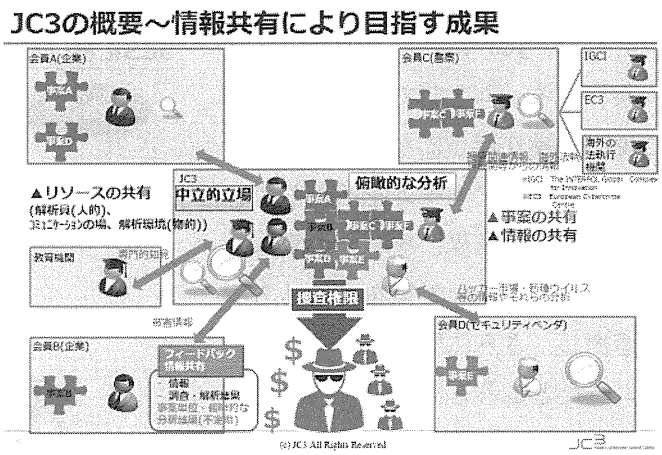
そうした NCFTA の成功例を踏まえ、「JC3 の設立の経緯と現在の位置付け」というスライドにあるように、政府レベルの様々な会議、閣議決定などでその設立について検討すべしという決定をいただいて 26 年から業務を開始した。つい先ごろの



サイバーセキュリティ 2015 の中でも「警察庁において、サイバー空間の脅威に対処するため、日本版 NCFTA である JC3 等を通じた産学官連携を促進」といった形で盛り込まれている。

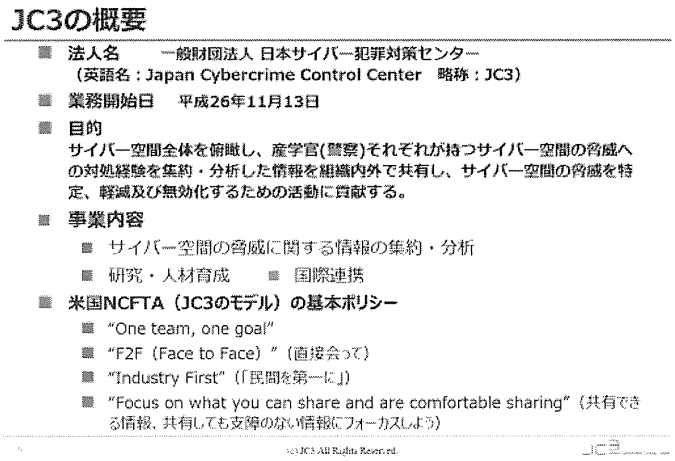
４　JC3 の概要

まず、JC3 の特色としては、産学官いずれからも中立的な立場で１つのプラットフォームを作るというところがある。まさに NCFTA のコンセプトである。



ここで、情報あるいは人的なリソース、コミュニケーションの場、そして解析環境、こういったものを共有する。そして、それぞれの持つパズルのピース（とよく NCFTA のプレジデントのマリア氏もおっしゃるのだが）を組み合わせて、事案あるいは今起こっていることの全体像を把握し、それを活用して俯瞰的な分析をし、警察、法執行機関の持つ捜査権限も活用して脅威の大本に迫っていく。そして、この俯瞰的な分析の結果について会員の方々とも共有し、そのフィードバックをいただく、あるいは提供する。こういった形で活動を進めていく。

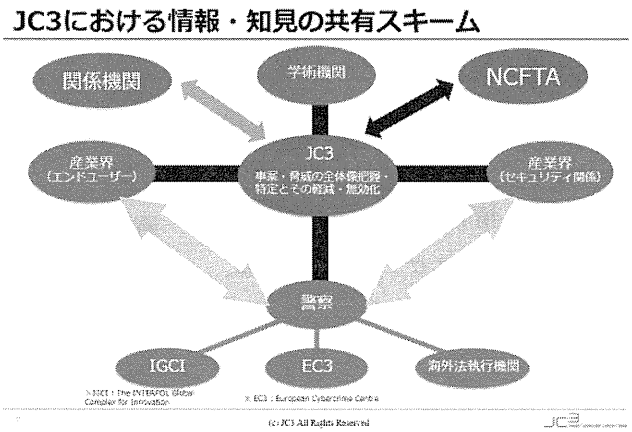
次に、概要だが、目的はサイバー空間の脅威を特定、軽減、無効化するための活動への貢献であり、情報を共有し、ともにこの目的を達成していくという点で、やはり米国の NCFTA にならったものとなっている。事業内容としては、情報の集約・分析、研究・人材育成、国際連携ということで、これも米国の NCFTA にならっている。



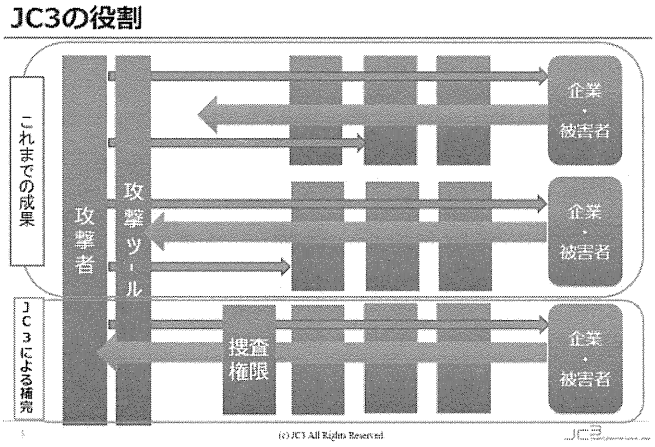
米国 NCFTA においては、基本ポリシーを掲げている。One team, one goal ということで、みんなで力を合わせて脅威の大本に迫るという目的を達成していこう、これがまず１つ。Face to Face、直接会って信頼関係を基にさまざまな活動を展開していこうということ。Industry First、民間主導でできたというところもあるが、民間の立場を第一にということ。これは、いわば被害者の立場に立つということである。私も昨年まで警察にいたので、

警察としては被害者の立場に立つということを非常に大切にしておられるが、そういった言葉で言えるかと思う。Focus on what you can share and are comfortable sharing、共有できる情報、共有しても支障のない情報にフォーカスしようということで情報の共有を大切にしている。その際に、comfortable という印象的な言葉が使われているが気持ちよく情報をシェアして戦っていく。そういったことが基本ポリシーになっている。こういったポリシーを私どもも大切にしていく必要があると思っている。

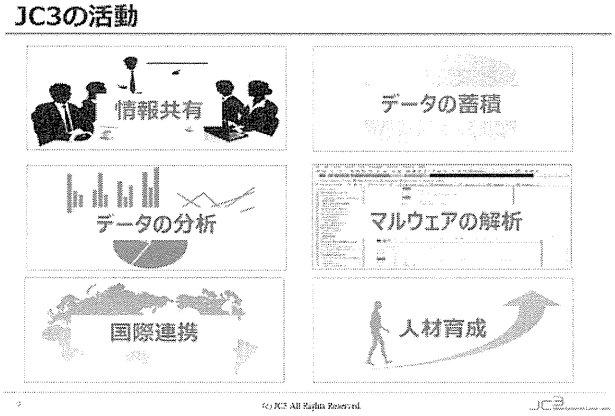
そして、JC3 における情報・知見の共有スキームとしては、今までのご説明の繰り返しになるが、JC3 というプラットフォームを活用して、学術機関、産業界、そして被害を受ける方々、様々な対策を講じる方々と連携し、さらに警察や IGCI、EC3 といったところとも警察を通じて連携をしながら活動を進めていければと思っている。



次に、JC3 の役割をポンチ絵として描いたものだが、サイバー攻撃に対し、国民の生活を支える様々な活動、あるいは企業を経営して様々なお客様のニーズに応えるという活動を継続していくことについてはしっかりと取り組んでおられ、そのための情報共有や様々な取組がこれまでになされてきて大きな成果を上げてこられた。この重要性はこれからも全く減ずることはないわけで、引き続き取り組んでいくことになる。

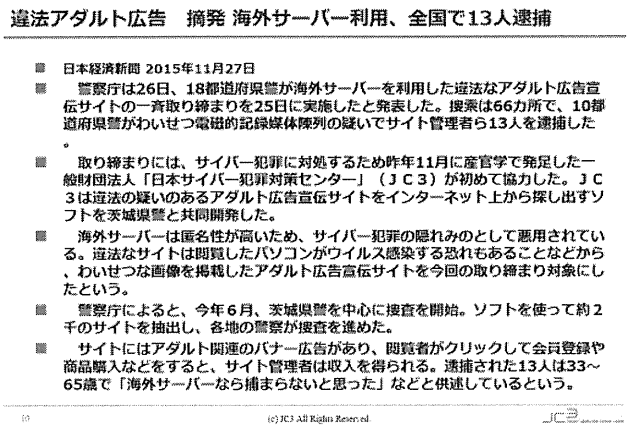


JC3 は、こうした様々なこれまでの取組を補完し、様々な方々とともに警察も入っていただく形で、捜査権限を活用しながら攻撃者の大本に迫っていく。そして、これまでの様々な取組と合わせて社会全体として安全なサイバー空間を作っていく、こうしたところに役割があるかと思っている。



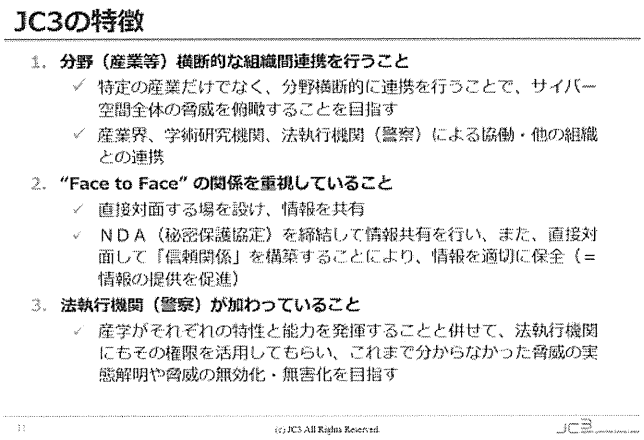
JC3 の具体的な活動としては、これも繰り返しになるかもしれないが、情報の共有、データの蓄積、データの分析、マルウェアの解析、国際連携、人材育成ということで、様々な活動を展開している。データベースを構築し、今も様々な実際の事案のプロセスの分析をし、あるいはマルウェアを解析するための環境を整備し、NCFTA とも関係の強化を図っている。

次は 11 月 27 日の『日経新聞』の記事から引用したものだが、先ほど申し上げたようなマルウェアの解析環境あるいは様々なネットを調査するような環境等を私どもは整備している。そうしたものをご活用いただいて、事件の摘発に警察で結びつけていただいた事案がある。


違法アダルト広告　摘発 海外サーバー利用、全国で13人逮捕

- 日本経済新聞 2015年11月27日
- 警察庁は26日、18都道府県警が海外サーバーを利用した違法なアダルト広告宣伝サイトの一斉取り締まりを25日に実施したと発表した。捜索は66カ所で、10都道府県警がわいせつ電磁的記録媒体陳列の疑いでサイト管理者ら13人を逮捕した。
- 取り締まりには、サイバー犯罪に対処するため昨年11月に産官学で発足した一般財団法人「日本サイバー犯罪対策センター」（ＪＣ３）が初めて協力した。ＪＣ３は違法の疑いのあるアダルト広告宣伝サイトをインターネット上から探し出すソフトを茨城県警と共同開発した。
- 海外サーバーは匿名性が高いため、サイバー犯罪の隠れみのとして悪用されている。違法なサイトは閲覧したパソコンがウイルス感染する恐れもあることなどから、わいせつな画像を掲載したアダルト広告宣伝サイトを今回の取り締まり対象にしたという。
- 警察庁によると、今年６月、茨城県警を中心に捜査を開始。ソフトを使って約２千のサイトを抽出し、各地の警察が捜査を進めた。
- サイトにはアダルト関連のバナー広告があり、閲覧者がクリックして会員登録や商品購入などをすると、サイト管理者は収入を得られる。逮捕された13人は33～65歳で「海外サーバーなら捕まらないと思った」などと供述しているという。

そして、JC3 の特徴についてである。様々な形での分野ごとの情報共有は、それぞれ深い情報共有、実践的な共有ができるが、JC3 の場合はあえて言えば分野横断的な組織間連携が行える。したがって、サイバー空間全体の脅威を俯瞰することを目指していける。そしてまた、組織としても様々な組織が加わっている。


JC3の特徴

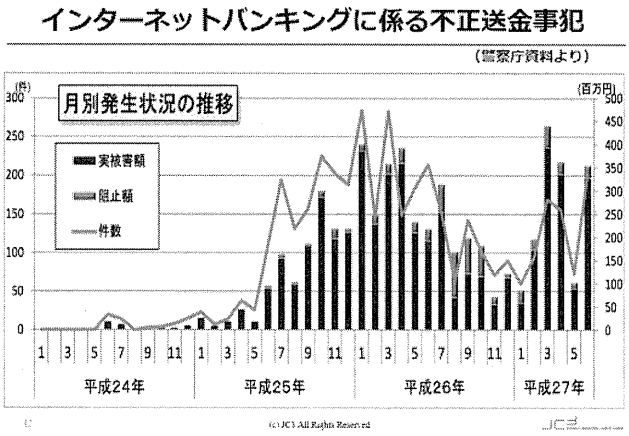
1. 分野（産業等）横断的な組織間連携を行うこと
   - ✓ 特定の産業だけでなく、分野横断的に連携を行うことで、サイバー空間全体の脅威を俯瞰することを目指す
   - ✓ 産業界、学術研究機関、法執行機関（警察）による協働・他の組織との連携
2. “Face to Face” の関係を重視していること
   - ✓ 直接対面する場を設け、情報を共有
   - ✓ ＮＤＡ（秘密保護協定）を締結して情報共有を行い、また、直接対面して「信頼関係」を構築することにより、情報を適切に保全（＝情報の提供を促進）
3. 法執行機関（警察）が加わっていること
   - ✓ 産学がそれぞれの特性と能力を発揮することと併せて、法執行機関にもその権限を活用してもらい、これまで分からなかった脅威の実態解明や脅威の無効化・無害化を目指す

Face to Face の関係を重視しているということだが、私どもは 27 年の 11 月から広い事務所に移り、NCFTA ほどたくさんの皆様が一緒にやれるわけではないが、以前と比べかなり多くの方々と一緒にやれる体制が整った。民間の方々、法執行機関の方々とともに活動を行っており、信頼関係を構築するという観点で、様々に直接対面する場面を設け情報を共有することに取り組んでいる。

また、秘密保護協定（NDA）を締結して情報共有を行い、情報を適切に保全しながら共有できるような体制も構築している。

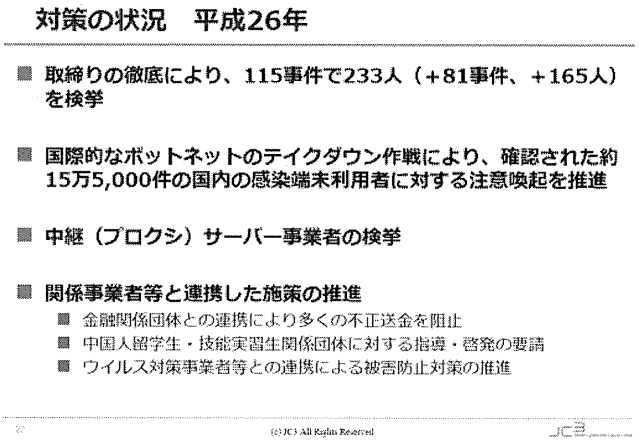
そして、もう一つの特徴として法執行機関が加わっていること。これは先ほど図でお示ししたとおりであり、脅威の大本に迫っていくという目的のために法執行機関の方々にもご活躍いただくことができる。

５　インターネットバンキングに係る不正送金事犯及びその対策

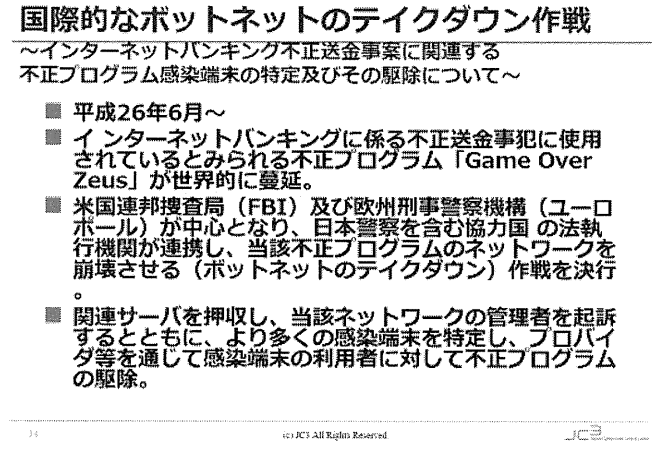


今までのところがJC3の活動のご紹介だが、今後は、私が考えている、あるいは最近の現実を見て思うことを少し申し上げたい。

１つは、先ほど白井参事官から既にご紹介いただいた、インターネットバンキングに係る不正送金事犯の推移である。非常に凹凸があるのがお分かりいただけるかと思う。25年の後半から急激に増加して、26年の前半もその傾向が続き、一方26年の後半に減少を見ているのがこの推移からご理解いただけるかと思う。そして、27年にはまた増加をしている。これがインターネットバンキングに係る不正送金事犯の状況である。



次に、26年に取られた対策だが、警察が取締りの徹底を行ったということがある。見ていただくと、115事件、233人の検挙。事件の方は115事件検挙で前年に比べてプラス81件の増加。人数の方は233人の検挙で前年比165人の増加。劇的な増加である。この検挙の多くは不正送金先口座や出し子、お金の引き出し役の検挙であるが、そうした彼らの足回りを徹底的にたたいたということがある。

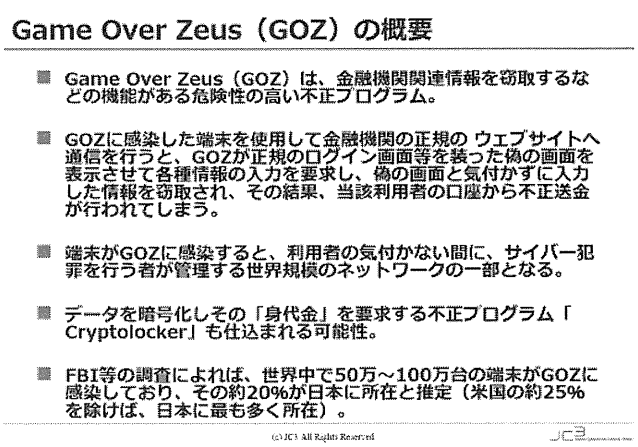


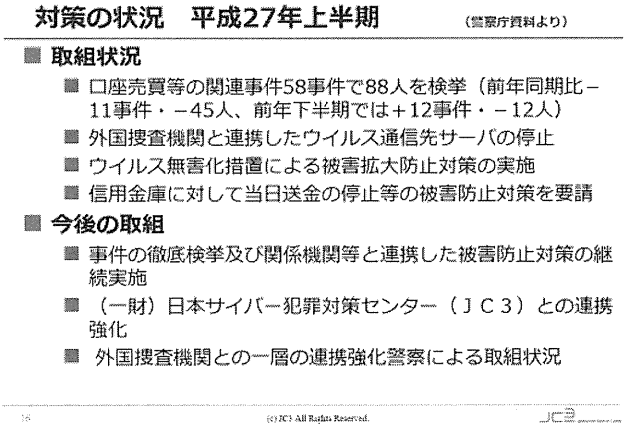
それから、国際的なボットネットのテイクダウンということで、非常に多く使われていたいわゆるZeus系と言われるボットを、ピッツバーグにあるFBIが主導して、EC3のクレジットも出ているが、世界的に展開してこれをたたいた。日本警察もこれに加わって対応したというところがある。

それから、ネットバンキングをやるに当たってID、パスワードの入力が必要であるが、それを盗み出すようなサイトに誘導するフィッシングメールの発出を行ったり、あるいは

不正なサイト自体を立ち上げるようなことをやっているサーバの事業者を、全国一斉で検挙されている。

また、金融機関の皆様が多くの不正送金、例えば個別の送金についてチェックをして止めておられる。それから、不正送金先の口座として中国人の方の口座、あるいは引き出し役としても中国人の方がするようなこともあったので、そういった方に対する指導・啓発の要請を行う。さらに、マルウェアについての情報をいち早くウイルス対策事業者等と連携して防いでいく。このように見ていただくとお分かりになるかと思うが、国際的にも国内的にも多くの方々がまさに官民連携をして、総力を挙げて対策を採った結果がこの 26 年の後半の減少につながっている。



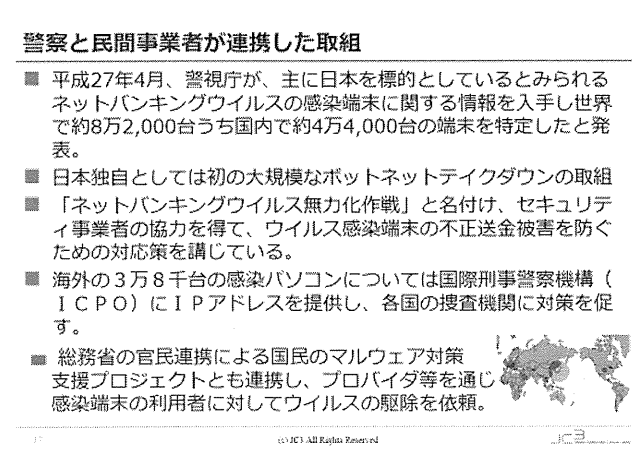


しかしながら、さらに見ていただくと分かるように、攻撃側はこの対策を上回る攻撃をさらに仕掛けて、本年、また被害が出てきている。

当然ながら 27 年の上半期にも様々な取組がなされている。また、今後の取組として、これは警察庁の発表資料からであるが、JC3 との連携等も掲げられている。

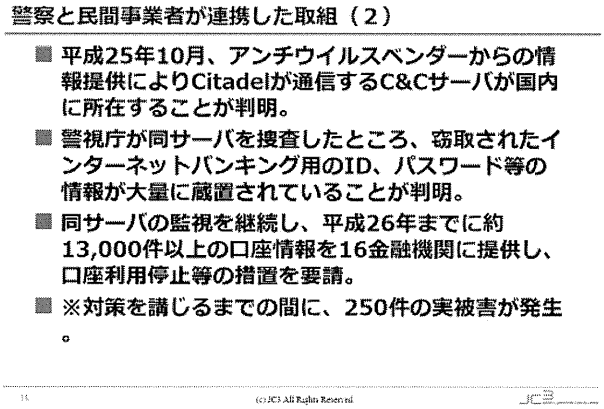
６　警察と民間事業者が連携した取組

ここで１つご紹介したいのは、警察と民間事業者の方の連携した取組として、27 年４月に警視庁が主に日本を標的としているとみられるネットバンキングウイルスの感染端末に関する情報を入手して、世界で約８万 2,000 台、うち国内で約４万 4,000 台の端末を特定したと発表されている。日本独自としては初の大規模なボットネットのテイクダウンの取組である。「ネットバンキングウイルス無力化作戦」と名付け、セキュリティ事業者の協力を得てウイルス感染端末の不正送金被害を防ぐための対応策が講じられている。多くの海外の端末についての情報があった



ので、それについてICPOにお願いをしてIP アドレスを提供して各国の捜査機関に対策を促したということがある。

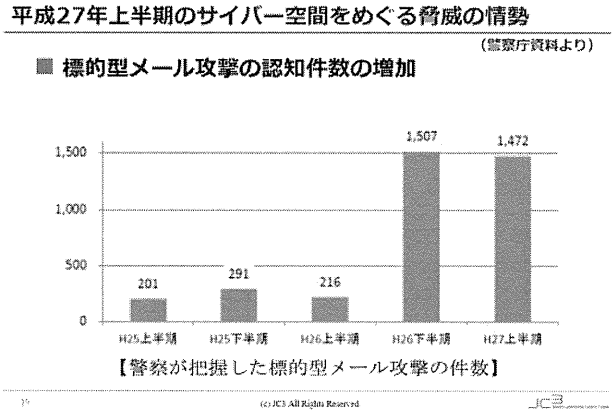
そして、総務省の官民連携プロジェクトACTIVEとも連携をし、プロバイダ等を通じて感染端末の利用者に対してウイルスの駆除を依頼するということで、日本においてもこうした形でさまざまな官民連携が行われ大きな成果を上げている。



こうした形で官民連携は、成果に向けてそれぞれの方が持ち場で力を尽くしていく、こうした取組がされてきている。

7　平成27年上半期のサイバー空間をめぐる脅威の情勢

従来から行われているC&Cサーバ[1]についての情報共有ももちろんある。白井参事官からお話があった標的型メール攻撃であるが、こうした日本の技術情報を狙ってくる、あるいは様々な政府関係機関の情報を狙ってくる攻撃についてはどのような対応をしていくのか。情報を共有してしっかりと防いでいくといったことは当然しっかりとやっていくことになるが、それでは攻撃自体の脅威の大本に迫るにはどうしていったらいいか。



１つ参考になるのは米国の取組かと思う。例えば、皆様方もよくご存じのソニー・ピクチャーズエンタテインメントに対する攻撃については、FBIが北朝鮮からの攻撃であることを発表し、これに基づいて北朝鮮に対して経済制裁を発動した。

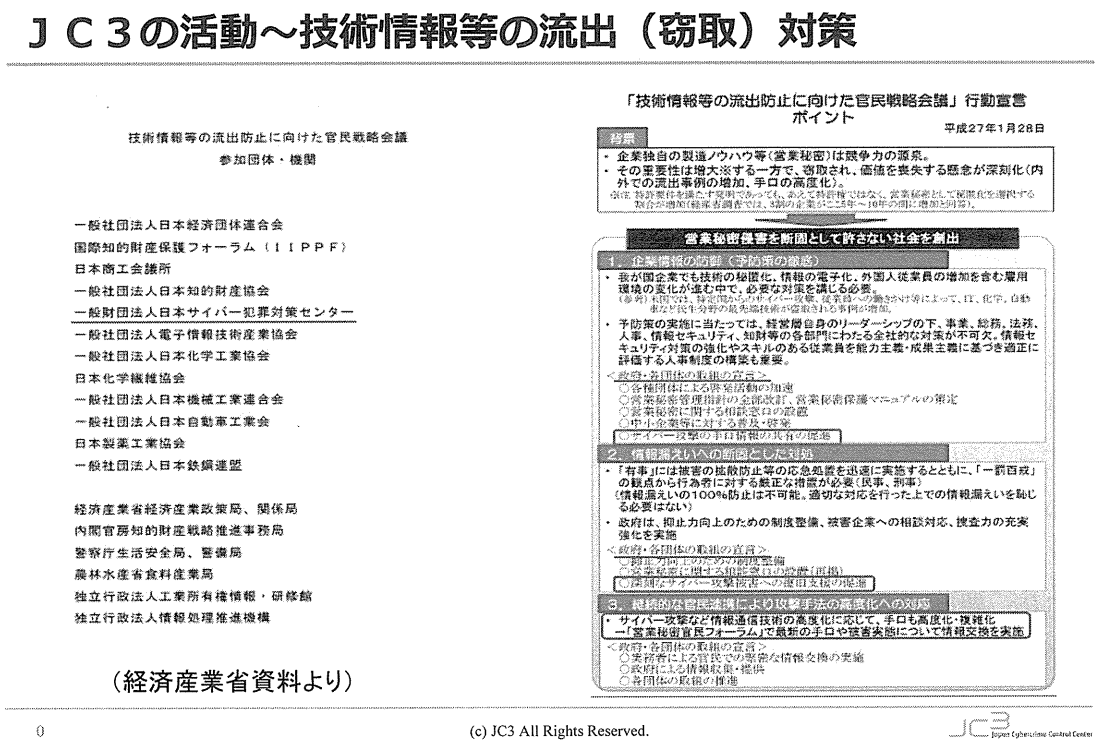
つまり、民間の方々が様々な調査活動、アトリビューションを行い、FBIがそういった方々と協力し、捜査権限も活用して明らかにしていく。それをベースに国として経済制裁にまで持ち込むといったような形の対応をされている。これも大きな意味での総力戦と言えるのではないか。一つ一つのサイバーインシデント、あるいはそれらを全体として見たオペレーションは、これ自体がいわば国と国との戦いとも言えるような状態になってきているのではないかと思う。こうした意味でも官民の連携の重要性は非常に大きいと考える。

---

[1] Command and Control Serverの略。攻撃者の命令に基づいて動作する不正プログラムに感染したコンピュータに指令を送り、制御の中心となるサーバのこと。

８　JC3 の活動～技術情報等の流出（窃取）対策

最後に、私どもも参加させていただいている経済産業省の「技術情報等の流出防止に向けた官民戦略会議」の関係である。こうした取組も含めて様々に展開していくことが重要かと思っている。



【パネルディスカッション】

名和　それでは、残された時間でパネリストの皆様方からお話を伺っていきたいと思う。まず最初に、アトリビューションの問題を取り上げたい。IGCIのウルクニエミ氏からのお話の中でも、IGCIが研究開発に取り組んでいる中で一番最初の課題としてアトリビューションの問題を挙げておられた。また、その重要性については坂理事からもお話があった。

そこで、まずウルクニエミ氏にお伺いしたい。捜査手法にも関する問題であり、話せないこともあるかと思うが、IGCIでのアトリビューションに関する研究の状況について可能な範囲で教えていただきたい。また、ボットネットのテイクダウン作戦にIGCIが関わられたオペレーションのお話もあったが、そこでこのような研究開発が生かされているのかどうかも含めて、お話しいただければと思う。

ウルクニエミ　アトリビューションについては、IGCIにおける研究課題の１つである。現在はダークネットに関して研究中である。ダークネットを加害者が使うことは困難な課題であり、また、今回のパリのテロリストにも見られたように暗号化された通信を行うことはアトリビューションを非常に困難なものとする。

また、クリプトカレンシー（暗号型通貨）の問題もある。主なものとしてはビットコインがあるが、これは、組織犯罪などで使われている。サイバー空間で行われる犯罪であり、背後にどういった人間がいるのかを特定することが非常に重要になっているが、いつビットコインを入手したかやいつアクセスしたかなど金の流れを追うことによって、背後の人間を明らかにすることができる。また、ビットコインについては、比較的背後の人間を特定しやすいが、他のクリプトカレンシー、例えばダークコインについては特定するのが非常に難しい。

このほか、ソーシャルメディアの解析も研究課題の１つである。犯罪者がどのように行動・活動していくのかやどのような時に活動的になるのかなどを分析するが、これはサイバー犯罪だけでなく、組織犯罪やテロリズムにも生かすことができる。また、この分析はインターポールだけでなく世界中の学術機関においても実施している。この分析に関する各国へのツールの提供は行っておらず、コンセプトを提供しているのみである。また、ソーシャルメディアを通じて収集した情報の提供も各国の法執行機関に対して行っている。

また、ボットネットに関してだが、どんなことを申し上げたらよいだろうか。

名和　ボットネットのテイクダウン作戦についてお話しいただいたが、まさに背後にいる攻撃者を特定するという意味でアトリビューションの研究が関係しているのかどうかを伺いたい。

ウルクニエミ　ボットネットのテイクダウン作戦を数多く実施してきたが、背後にいる犯罪者集団を明らかにすることが重要である。オペレーションの中で民間企業と連携して情報、マルウェアを収集し、分析することにより背後にいるのが誰かを明らかにしている。また、ボットネットのテイクダ

ウンを行うことも重要であるが、それ以上にこの背後の人間にターゲットを当てることによってより良い結果をもたらすことにもなる。

名和　アトリビューションの問題に関して湯淺先生にもお伺いしたい。講演の中でプライバシー保護を強化する必要もあるというようなお話があった。そうしたことも踏まえながら、アトリビューション、攻撃者を特定して措置を講ずる上で、法的な課題としてどのようなものがあるか、お考えをお聞かせいただきたい。

湯淺　最初に、私ども法律を研究している人間の一番悪い癖は何でも定義をしたがるということであるが、その意味で言うと、そもそもアトリビューションというのは何を指しているのかが法的にまだ明確でない。様々なアトリビューションの文献を読んでも、これがアトリビューションである、あれがアトリビューションであるというのは少し違うかと思うので、そもそもアトリビューションとは何かということをある程度明確化しないと法的な対応が難しいというのが第１点である。

もう１点が、坂理事からもウルクニエミ氏からも民間企業や民間団体にアトリビューションにかなり貢献をしていただいた事例をご紹介いただいたが、日本法の下で私企業がアトリビューションをすることについて、それは合法であるという明確な裏づけはあるのだろうか。どこまでだったら日本法人である会社はアトリビューションをやってよくて、ここから先は法律に違反してしまう、あるいは民法上の不法行為になる危険性があるというこの線引きがきれいでないと、民間企業がアトリビューションに協力をしたくても協力をしにくいところがあるかと感じている。

まさにご質問いただいたように、アトリビューションは通信の秘密やプライバシー侵害の危険性があることは事実である。もちろん攻撃者を特定しようと思ってアトリビューションするわけだが、特にその過程で全然関係ない第三者のアトリビューションも結果として行ってしまう事例があると思われる。その場合、第三者のプライバシー侵害のおそれはないか。

最後に、背後に国家や国家に支援された団体がいると思われる攻撃のアトリビューションの問題で、これはうっかりやると大変なことになる。背後に国家がいるということがアトリビューションの結果分かった瞬間に、問題が変質してしまう。しかし、国際法上も、国家が背後にいる攻撃のアトリビューションは非常にホットなイシューになっている。これは当然そういう問題も生じ得るということを考えて対応していかないといけないのではないだろうか。

名和　法的にも難しい問題が多々あるようだということがうかがえるところであるが、そうした中で、アトリビューションの重要性について強調しておられた坂理事から、攻撃者を特定して対抗措置を講じることを進める上で今後解決すべき課題としてどのようなものがあるとお考えかをお聞かせいただきたい。

坂　アトリビューションの重要性については先ほど申し上げたとおりである。アトリビューションは攻撃者がいて攻撃対象に攻撃を仕掛けてくるということがあるが、その攻撃自体の経路があるし、調査活動から様々な行為をやってくる。これらを把握していくことはいろんなネット上のアクター

がおり、また、彼らの目的が経済的なもの、あるいは情報でもいいが、要は現実的なものであって、場合によってはそれに対して現実的な手法も組み合わせてくるかもしれない。そういうことを考えると、かなり色々な方々が情報を共有しないといけない。したがって、攻撃者のプロセスを念頭に置きながら、関係する方々がそれぞれ自分の持ち場でしっかりと力を尽くしていかないとこのアトリビューションはできないという意識を持っていただく。これがまず１つ重要かと思う。

それから、湯淺先生から色々課題をいただいたので全部ここで申し上げることはできないが、先ほど合法と非合法がクリアでないと民間の方々に協力いただけないのではないかという話があった。そのあたりは確かにクリアな部分、現行法の中でできるところをやり、またある意味では捜査の一環として、先ほど申し上げたような米国の例においても、一定のところまでは民間の方々がレポートを出し、そこから先はいわば捜査機関と一緒に権限行使をやっているところもあると思う。マイクロソフトも民事上の手続を使いながらやっている。そうした部分はしっかりと連携をして担保しながら進めていくことは重要と思っている。

名和　今後、技術的な側面あるいは法的な側面の両面から研究が進むことが期待される。また、攻撃者を特定するあるいは犯罪者を特定する観点からは、ログの保存がよく問題にされる。これに関連してゴダート氏にお伺いしたい。EU ではログの保存に関して一定の法制度もあると聞いているが、最近のヨーロッパにおけるログの保存に関する実情について、ご存じのところをお教えいただきたい。

ゴダート　EU レベルでは、正しいやり方が何なのかハイレベルな議論をしつつ解決策を探っているような状況である。法執行機関にとってデータを保存することは極めて重要であるが、その中で懸念されるのは、やはりセキュリティとプライバシーの問題である。

EU 各国が従わなければならない指令により、民間企業はログを半年から３年保存しないといけないとされていたが、EU 司法裁判所はその指令を無効であると判決した。実務家としては、捜査のプロセスを遅らせるものであると考えている。

ドイツではログは７日間保存するとされているが、ほかの国ではもっと長く２年くらい保存しなければならないとされているところもある。例えば、児童の性的搾取をめぐる問題では、イギリスに対して 120 の容疑者の情報を提供したところ 110 人を逮捕することができたが、他方で、ドイツにはデータがなかったので、うまくいかなかったというようなこともある。

また、プライバシーと匿名性の間に違いがあるということを知らせることも重要である。プライバシーを守るために暗号化するということはルールとなってきており、その方向に進んでいるが、オンライン上でオフラインの仕事をしなければならない場合、データを保存したり、証拠を収集したりするツールが必要だといった懸念もある。

最後に、個人について、Facebook などで自分の情報を公表している割には、個人情報の保護といったことも主張するので、一貫性がないのが現状である。非常に難しい問題であるが、あらゆる利害関係者の調整を行った上で、最終的には国民が望むような形にしていくのがよいのではないか。

名和　実情も踏まえて法執行機関の立場でこの問題についてお話をいただいた。ここで湯淺先生にもお

伺いしたい。やはりどうしても個人情報保護の問題とも絡んでくるが、ログの保存に関する法制度としてどのようなものが望ましいとお考えかお教えいただきたい。

湯淺　ログの保存は喫緊の課題であることは言うまでもない。先ほど申し上げたIoTによって次々にインターネットにつながるものが増える。また、各種のセンサーデータ等の通信量も莫大に増えていくので、このログをどうするかは喫緊の課題である。

さらに、最近は、サービス事業者に聞くと、サービス間での連携を行うことによってサービス間同士の通信ログが非常に増えているという問題も聞く。そのときに、そのログを全て保存しなければならない、しかも長期間保存しなければならないということになると、大量のログデータが発生する。おそらく最大の問題は、そのログの保存に関する費用を一体誰が負担するのかというコスト負担の問題だと思う。

今ご指摘いただいたが、個人情報保護法の改正によって匿名加工情報という概念が新しくできる。つまり、データから個人を特定できるものを取り除いたデータについては、本人の同意を得なくても目的外利用、第三者提供して良いということになる。ログデータについても、そういう形で匿名化してある程度それを使ったビジネスもできるという経済的なインセンティブと組み合わせないと、ただ単純に事業者の負担でログを保存しなさいとすると、それは全て最終的にはサービスを利用する消費者の負担になって返ってくるので、そこは経済的なインセンティブが必要かと思っている。

最後に、ログを保存するのは結構だが、ログの保存費用が非常に高額だからとそれを海外で保存すると意味がない。国内で保存してもらう必要がある。そうするとますます費用が増えると予想される。国内の法執行機関が容易に捜査できるようにどのようにして国内に置いてもらうかということも、課題かと思っている。

名和　時間も押してきたが、もう１点だけ官民連携に関連して、お話をいただければと思う。官民連携に関して今日、IGCI、EC3、それぞれ非常に進んでいるという印象を持った。今後、日本で官民連携をさらに進めていくためにどういったことを官の側、民の側それぞれが配慮すべきかについて、JC3の坂理事からお話をいただきたい。

坂　情報共有はこれまでも様々な形で取り組まれてきた。１つは目的の認識ということかと思う。つまり、脅威の大本に迫っていく必要性が高まってきているということがあるので、それに向けて情報共有をやっていく必要性があるという認識を、One team, one goalではないがみんなが持つというのは大切かと思う。

もう１つは、それぞれの立場をよく理解するということである。企業にとっては情報関係のインシデントは企業の存亡を左右するものになっているかと思う。そうした意味では、人間にとってみれば生死に関わるような事案だという意識を持って法執行機関の皆様もやっていただいていると思うが、そうした認識をさらに高めていく必要はあるかと思う。

一方、民間の方々にとっても、先ほどのような共通認識に加えて、例えば標的型メールを開いた人を必要以上に責めたりすることがあるが、そうではなくて、非常に巧妙になってきているので、

ある意味ではレジリエンスというか、そういうメールを開いた場合であっても大きな被害を生じさせないためにはどうしたらいいか、あるいは開いたという情報が迅速に上がってくるような体制を作り、それを共有するというような、そうした部内での意識を高めるといったところにもご配慮いただければいいのではないか。

名和　白井参事官にもお伺いしたい。官民連携の重要性は白井参事官も指摘しておられたが、民に望むもの、あるいは官の立場でこういったことを考えていきたいというようなことについて何かあればお話しいただきたい。

白井　民に望むものという、そんなおこがましいことは申し上げられないが、これだけネットが浸透している中で、大企業以外の中小企業が数多くあり、今までのサイバー攻撃や犯罪のパターンを見ていると、ゼロデイ攻撃みたいな形で対策を万全に講じていてもやられるものよりは、基本的な対策をしておけば防げたようなものについてお金がないからできなかったとか、知識のある人がいなかったみたいなところが結構ある。先ほどのインターネットバンキングのように、対策ができていない弱いところにこれから犯罪が増えていく、攻撃が行われていく傾向になっていくだろうと思っている。

そういう意味では、繰り返しになるが都道府県警察単位できめ細やかなアウトリーチを、警察署単位でやっていくような話かもしれないが、そういったことによって中小企業等が持っている情報が窃取されないとか、当然県境・国境がないので知らないうちにサイバー攻撃の踏み台になるといったことも抑止できるかと思っている。ローカルなレベルでの官民連携は、まさに日本が警察としてできる部分かと思っている。こういった部分を都道府県警察の方々の協力も得ながら進めてまいりたい。

名和　まだまだお話を伺いたいところであるが、時間も迫ってきた。本日は、サイバー空間の安全の確保をテーマとして講演及び議論をしていただいた。これらを通して、安全確保のために必須とも言える国際連携あるいは官民連携についてIGCIやEC3あるいはJC3の果たす役割が極めて重要であるということを再認識することができたと思う。

また、各国の法執行機関相互の間や法執行機関、産業界及び学術機関の間でフェース・トゥ・フェースの関係によって築かれる信頼関係を基礎として連携を深めていくことの大切さも学ぶことができたように思う。

さらに、サイバー空間における法制度の在り方をめぐる議論も大変示唆に富むものであったと思う。

そのほか、議論の中では、近年脅威の質が変化し、深刻化している中で、攻撃者を把握し、これに連携して対抗する必要性が高まっているというご指摘もあった。今後、この分野での研究が進展することが望まれる。

サイバー空間の脅威が増している状況の下で、日本では昨年、サイバーセキュリティ基本法が制定され、この法律に基づき今年９月にはサイバーセキュリティ戦略が閣議決定されるなど、対策は

強化されつつある。今後、この戦略を的確に実施し、自由・公正かつ安全なサイバー空間を実現していくことが求められている。その実現のためには、戦略にも述べられているように政府のみならず重要インフラ事業者、企業、個人といったサイバー空間に関係する全てのステークホルダーがそれぞれの役割や責務を果たす必要がある。本日のフォーラムが、参加していただいた皆様がそれぞれの役割や責務を果たすための助けとなるならば、このフォーラム開催の目的を達成したことになるものと考える。

結びに、本日の講演者及びパネリストの皆様に心から御礼を申し上げる。どうぞ皆様からも拍手をお願いしたい。