平成２５年度総合セキュリティ対策会議（第２回）

平成 25 年８月６日

発言要旨

１．開会

２．ＮＣＦＴＡの創設により期待される効果について

【委員２名から、ＮＣＦＴＡ創設により期待される効果について発表】

３．産学官の保有する情報の集約・分析の在り方について

【事務局から、ＮＣＦＴＡにおける情報集約分析に関して整理した論点について説明】

○　先日、米国ＮＣＦＴＡのＣＥＯから直接お話を聞く機会がありましたので、概要を御説明いたします。

米国ＮＣＦＴＡは、いわゆるＮＰＯで、設立されたのは 2002 年ですが、最初からうまくいったわけではなく、うまく回り始めるまでに５年ぐらいかかったようです。当時の問題点というのは幾つかありまして、まず、信頼関係をどうやってつくるのかという問題です。

企業からすると、自分のところの情報を出しても得はないから情報を出さない。それから、技術者が作業するわけですが、時間と労力をかけても、結局、ビジネスにはならず、企業からすれば何の役に立つのかという話になります。さらに、これは大きな要因ですが、法執行機関や警察に情報を出しても企業側は全くフィードバックが得られないという問題があったようです。

それらを解決するため、米国ＮＣＦＴＡでは、集まった情報をあくまでＮＣＦＴＡの管理とし、警察等の政府機関の管理ではなくしました。また、企業は、それぞれ自社のデータを持ち込んで、ＮＣＦＴＡにあるデータベースと連携して自分のセキュリティのために活用することができます。持ち込んだ情報はサニタイズ、いわゆる匿名化をしてデータベース化し、常駐しているＦＢＩ捜査員も情報提供者の合意がなければ、普段は匿名化されたデータベースしか見られないとのことで、この仕組みを５年かけてつくり上げたということです。この仕組みによって被害に遭っている企業にとってはデメリットよりもメリットのほうが大きくなったので、ＮＣＦＴＡに積極的に関与するようになってきたとのこと

です。

○　捜査上、サイバー犯罪に対してくさびを打っていくことが一義的に大きな目的であるとすると、どういう情報をまずは共有化すべきか検討する必要があると思います。

恐らく相手側は組織化されていますから、一企業では対応し切れないというのは自明の理です。となると、具体的にどういう機能でディフェンスをし、やられた場合にはどういう証拠をうまく捕捉し、その後同じような犯罪が出ないようにしていくのかという議論がまずあったほうが、本来の日本版ＮＣＦＴＡの機能、姿の話になるのではないかなと個人的には思います。

○　モチベーションを持ったエンドユーザーがいないと、枠組みをつくっても間違いなく回らないし、細かいところが決められないと思います。また、目的がはっきりしていないと、協力に一歩踏み出せないということがあります。できれば、早いうちに、小さくてもいいから始めたいというのが個人的な意見です。

○　日本版ＮＣＦＴＡの活動に参加すると人材育成できるとか、社内では得られない情報が入手できるということであれば、企業が日本版ＮＣＦＴＡに参加する魅力を感じる気がします。日本の企業の場合、サイバー攻撃をされたときに、対応できる人は非常に限られています。そのハンディキャップを日本版ＮＣＦＴＡの活動の中で補えれば、サイバー攻撃、サイバー犯罪が起こったときに対応できるようになると思います。

○　何らかの形で日本版ＮＣＦＴＡの設置に向けた動きを進めていくことが重要かなと思っていまして、概念整理は非常に重要で、進めていくべきだと思いますが、それを待っていられない部分もあるので、関心事項を少しずつ吸い上げて、進めていくというのはよいと思います。

同時に、日本の場合には、企業に対して、こういうことをやっていかないと非常に危ないぞというところを広めていかないと、小さく始めたものが小さいままで終わってしまう可能性もあると思っていますので、そういう機能を持たせつつ始めていくことも必要だと思います。

○　サイバーセキュリティは、フィジカルと同じように、被害に遭わないようにみずからを守るためには各企業が自助努力しなければいけないと思います。

ただ、自分たちを守ろうとしたときに情報が非常に少ないというのも事実でして、日本版ＮＣＦＴＡに官と民と学が一緒になって情報を集めて、万が一のときに一般企業が問い合わせをしたら、何かの回答が得られるような、一歩前に進めるようなことができるので

あれば、そういう形から始めてもいいのではないかと思います。

○　企業側にとって、情報を提供するだけで何らフィードバックがなければ、前向きになりづらいということを踏まえて、具体的な枠組みの検討を行う必要があると思います。

○　情報セキュリティインシデント対応の現場から見ますと、とにかく人手不足で技術の情報もないので、日本版ＮＣＦＴＡのようなものができれば私個人は非常に有益だと思っています。

　ただ、企業の上層部に対して、これをやってどうなるという説明がつかないので、その点をどう埋めるのかが一番の課題かと思っています。

○　日本では、各県警からの問い合わせが非常に多いので、フォレンジックの情報、つまり、各社の製品の技術情報を日本版ＮＣＦＴＡで集約するような機能も考えられると思います。

○　現在、テレコムＩＳＡＣ、それから、ＪＰＣＥＲＴという組織があって、これまでいろいろな動きをされてきたわけですので、それらとの整理ということも今後の検討における重要なポイントというふうに考えております。

○　どちらかというとセキュリティの場合は専門家の集まりになりがちで、企業のトップから見ると何をやっているかよくわからないというのが正直なところです。ＮＣＦＴＡみたいな組織も大事ですが、それとは別にもう少し上のレイヤーでトップの意識を高めるような枠組みを並行してつくれないものかというのがまず１点です。

　もう１点は、新しい組織をつくることはいいと思うのですが、似たことをやっている組織は既にあり、人材が分散して、結集できないような感じがするわけです。

日本のリソースを集められるような仕組みづくり、すなわち、既存の組織や団体とも連携がとれるような枠組みをつくることが必要ではないかと思います。

○　日本版ＮＣＦＴＡと既存の組織との違いは、業界を横断していかなければいけないということと、海外捜査機関等との連携を進めることにあるのではないかと思います。

　あと、スポンサーシップは非常に重要な点で、被害が増えている業界に働きかけると理解を得られるのではないかと思います。

４．産学官連携した研究開発の在り方について

【委員から産学官連携した研究開発の在り方について発表】

【事務局から、ＮＣＦＴＡにおける研究開発に関して整理した論点について説明】

○　捜査をやっている方の事象を分析する力というのは我々よりも上ではないかと思うことがあります。そういう意味でいきますと、警察の情報がすごく比較優位を持っていることは強調してもいいのではないか思っています。警察情報というのは緻密であったり、根拠に基づいていたりするというのを洗い出してみると比較優位が明確になるのではないかという感じがいたします。

○　警察は、目的が犯罪捜査であることから、その過程で得た情報を民間にフィードバックするという観点がなく、民間からすれば情報を提供するだけで終わってしまう例が多かったと思います。

ですから、研究開発や技術開発などの活動においては、警察が得た情報を民間にもちゃんとフィードバックできるようなパートナーシップみたいなものをつくらないと、民間企業は乗ってこないのではないかと思います。

○　中央大学や情報処理学会の方でマルウェア対策人材育成ワークショップというのを2008年から始めているのですが、データがないと研究できないということで研究者同士が同じデータを持ってお互いに相談ができるといいだろうというのがもともとの始まりでした。その中で、常に同じような形のデータを入手して傾向分析等を継続するのが難しいという現状があります。

また、研究用のデータセットという点では、各企業、研究畑の人に御協力いただいてハニーポットを設置し、そのデータをいただいているのですけれども、結局、ハニーポットということで、ある程度は分かるのですが、それだけでは分からない領域もあります。つまり、実際の事例で分析すべきデータというのがあると考えています。

さらに、それとは別の点について言えば、学会的な活動をしているときの発表において、本来共有すべき情報も、個別組織等が分からないようある程度マスクして発表せざるを得ないこととなっていますので、どうやって成果を共有するのかというのは課題です。この点は日本版ＮＣＦＴＡの枠組みでカバーされるといいのではないかと思います。

○　例えば研究開発というテーマで挙がっていますけれども、捜査のためのマルウェアを含めた捜査ツールの作成であるとか、捜査のために未公開の脆弱性を利用するとか、そういう一歩踏み出すところを目指していくのか、そうではなくもう少し大人しいところで研究していくのかいろいろあると思います。その辺を具体的に示した上で、研究開発というキーワードを１つの核にして情報提供を求めると、実用的な情報が集まるのではないかなと感じました。そういう話が出ると、民から情報が出て、具体的な研究開発のテーマが官

側から出て、学がどういうふうに絡んでくるのかも見えてくると思います。

○　守るべきものというのが法益によって違うのではないかなと思います。

ただ、法益を守るという意味では共通しているのだと思うので、ワーキンググループとか小分科会みたいなものから始めるというのは非常にいい発想なのではないと思います。

○　これまでも、既存の組織や各企業等が、サイバー空間の脅威に対していろいろな対策を講じてきたところですが、それは経済問題と治安問題とが切り離せる、あるいは経済問題のほうがややウエートが多いときの議論だと思います。最近は、非常にグローバルな展開の中で、警察が国際的な規模で出ていかなければならないような脅威が目立ってきており、従来の脅威とは変わってきています。

その結果、既存のものをどう整理するかはともかく、ニーズが新たに出てきているということは事実だと思うのです。リソースの点で、官だけでも民だけでもどうも足りないぞということですね。そこで、じゃあ、どうすればいいかというと、要するに民の側としてはビジネスジャッジメントをして、そのビジネスジャッジメントが会社法的に言えば株主の納得、説明のつくものでないと、要するに当該企業にとってメリットのあるものでないと出ていかない。

これまでは、一方的に協力関係であったり、あるいは一方的に助けてくださいという関係であったのが、実質的に双方向にならなければならないというところで、そのためにはどんなルールが必要かということで、確かにブラックボックスに投げれば不安だというのもそのとおりですし、完全に合意のもとでなければ何も使えないか、じゃあ、その合意の取り方はどうするかという議論も出てくるでしょう。具体的に小さなフォーラムをつくるとの御意見もあり、そういった場で具体的に議論をしたらどうかなと思いますけれども、いずれにせよ、双方向、どちらにもメリットがないと、こういうものは進みませんので、そのためのルールづくりを設定する実験的な場を設けることには、私も賛成です。

○　日本版ＮＣＦＴＡの特徴で海外の関係機関との連携というお話がありますけれども、最終的に海外の関係機関と情報共有・交換をするには信頼関係、それから特色を持ったデータ内容が重要だと思います。つまり、日本版ＮＣＦＴＡでしか持っていないデータがあれば、相手も踏み込んで情報を出してくるという可能性はあると思いますので、何かしら特色を持ったデータ内容の蓄積を考えるべきだと思います。

４．閉会