平成25年度総合セキュリティ対策会議（第３回）

発言要旨

平成25年９月６日

１．開会

２．トレーニングの提供の在り方について

【委員から、トレーニングの提供の在り方について発表】

【事務局から、ＮＣＦＴＡにおけるトレーニングの提供に関する論点の整理について説明】

○　ＮＣＦＴＡにおけるトレーニングの提供という新しい構想を考えているわけですけれども、民間企業への派遣等のトレーニング等の各都道府県警察における現状を把握していれば教えていただきたいと思います。

○事務局：　１つは、捜査員を民間企業に一定期間派遣して、経験を積むことによって技術を学ぶという方法があり、警視庁の例では、１年近くの期間企業に受け入れていただき、派遣が終了した者をサイバー犯罪捜査部門の中核に配置するなどして、派遣で得た知識、経験及び人脈を活用しております。この方法は、警察と企業の双方で高い評価を受けているものですが、小規模な県警察では、なかなか実施が難しいという面もございます。

　また、それぞれの都道府県警察においては、警察学校等でサイバーに関する専門的な教養を行っています。この教養では、学校の教官による教養以外に関係事業者の協力を得て、例えば民間の方を講師として招へいしたり、あるいは、事業者のところにお伺いしてお話を聞かせていただくなどの方法も取り入れております。

　警察における捜査員に対するトレーニングの在り方としては、部門を超えて全ての捜査員がサイバー犯罪捜査に係る一定程度の知識と技術を身につけるとともに、サイバー犯罪捜査部門やサイバー攻撃対策部門等に属する捜査員については、サイバー犯罪捜査に関する極めて高度な知識と技術を持つ人間をいわばサイバー・エリートとして育成するという二層構造が必要だと思っております。前者の一般的な底上げについては、基本的には各都道府県警察の責任において行い、国、つまり警察庁においては各都道府県警察のサイバー犯罪捜査のトップエリートを引き抜いて国の責任、警察庁の責任において育成していくという二層構造での人材育成に現在取り組んでいるところであります。

○　日本版ＮＣＦＴＡで求められるのは、やはり実践的なスキルといったところが重要だと思います。そういった意味では、トレーニングの果たすべき役割というよりは、日本版ＮＣＦＴＡに対してどういう機能を持たせるかという点に議論が集約するのではないのかなと思います。したがって、捜査員がどういう知識を持って、日本版ＮＣＦＴＡの中でどういう役割を持たせるべきなのかという議論があって、それを実施するためのスキルをどうキープするのかという議論になると思います。その上で、誰をトレーニングするのかという議論になり、その結論というのは官の方々に限るのかあるいは民も含めた相互トレーニングなのかによっても変わってくると考えています。

○事務局：　日本版ＮＣＦＴＡがサイバー犯罪対策の観点でどういう機能を果たすべきかを議論し、その後、警察の業務との関係で、どういう位置を占めるべきかという枠組みについての議論を行い、その上で日本版ＮＣＦＴＡが人材育成においてどのような役割を付加的に果たしていくべきかという議論をすべきだということは御指摘のとおりだと思います。

○　トレーニングについて、一般的には技術内容といった部分を意識しがちですが、日本版ＮＣＦＴＡでは、まず、取り扱う対象範囲を明確にして、プロセス、要望、報告の内容等の標準の部分を整理する必要があると思います。

　また、特定の分野には特定の技術の習得が必須であるというような審査を行うことも必要で、ＩＤＦ等、その辺りを整備されていれるＮＰＯ団体等とうまく連携すればいいと思います。

○　教育対象者をどのように考えるかという問題があって、一般職員と専門家の両方を対象範囲に含めるという議論もあるかと思いますが、日本版ＮＣＦＴＡにおいては、専門家、それもトップクラスの専門家を育成するような仕組みをつくることが必要だと思います。

　そのためには、１度仕組みをつくって終わりということではなく、産官学が協力しながら世界のトップ、あるいは攻撃側に負けないような形で技術を向上することが可能な仕組みを検討するのが一番重要だと考えています。その派生として一般職員向けの教育という議論もあり得るのですが、これはやり方次第で今までの延長でも可能ではないかと考えています。

３．海外の関係機関等との連携の在り方について

【委員から、海外の関係機関等との連携の在り方について発表】

【事務局から、ＮＣＦＴＡにおける海外の関係機関等との連携に関する論点の整理について説明】

○　例えばＤｏＳ攻撃の話でいうと、攻撃を受けているときに、それをいかに緩和するか、いかに企業のビジネスに影響を与えないように対処するかということは考えて実行していますが、なぜ攻撃されているかという根本のところは正直何の手も打てない状態で、そういう意味では、日本の企業等が攻撃を受けないための予防情報のような民間企業では持ち得ない情報は、警察組織が海外の組織と連携する中で多くの情報を得ているのではないかと思います。だとすれば、それをどのようにシェアして国益という観点からいかに利用していくかという観点でＮＣＦＴＡが機能してくれると非常に役に立つのではないかと思います。

○　連携の在り方については、キャッチアップの段階と定常状態になった段階を分けて考えていく必要があるかと思います。日本版ＮＣＦＴＡが世界の先端の国の同じような仕組みにキャッチアップする段階では、やはり海外、特にアメリカの動きやカリキュラムみたいなものを勉強させてもらわなければならないと思います。そうやって、日本版ＮＣＦＴＡと海外の機関が相互に力をつけて、日本国内でも最高水準で循環するような段階に至ったときに、さらにいろいろな形で情報提供していくということが出てくるのかと思っています。

○　情報交換ということを考えた場合、単に情報をもらうだけではだめで、どういう情報を出せるのかという部分が非常に重要だと思います。日本にとって、国外で行われた自国に対する犯罪についての情報は非常に価値があり、これは外国にしても同様です。実は、日本で行われているけれども日本を対象としていない事象であれば誰も調べようとしません。例えば、日本のコンピュータにおいて、内部のデータが改ざんされたり、何らかのデータの蔵置場所にされたり、情報交換の場にされたりする事象が発生したとしても、ただの不正侵入事案としてクリーニングして処理を完了しています。現在、ＪＰＣＥＲＴ等は、海外ベンダー、海外のＣＥＲＴから連絡を受けて、コーディネーションしてテイクダウン等の活動をされていると思います。しかし、そこからもう一歩踏み込んで調査をするため、強制的にというのは難しいと思いますが、協力を要請するとかそのあたりを日本版ＮＣＦＴＡの中の情報発信、海外との情報交換、連携という面で捉えてもいいのではないか思います。

○　海外の機関と既に連携されているとのことですが、連携をより強固にさせていくには一体どういうものが課題であるのか、例えば、こんな情報発信をしたから信頼度が上がったなどの成功事例を教えていただければと思います。

○　ＣＥＲＴ／ＣＣについては個人のつながりのほうが強いのが実態で、そのつながりを個人単位からチーム単位へ育てる必要があります。

インシデントに関してはＪＰＣＥＲＴ経由なので、脆弱性対策に限られているが実態です。今後は、インシデントが起きたときにも組織として対応する必要があり、その点、日本版ＮＣＦＴＡが信頼度の高い枠組みとして機能すれば信頼度も高く、対策を講じやすいと思います。

○　インシデント対応の体制をキープするのは非常に難しいです。また、人材について言えば、集めるのも難しいですが、育てるのはさらに難しいです。例えば、世界レベルのハッカーを集めるためには、育成するだけでは無理で、どちらかと言えば、素養のある人間を連れてきて磨いていくことが必要だと思います。

インシデントは攻撃側とのイタチごっこで、海外から攻撃をしてきたＩＰアドレスは判明しても、その先には手が出せません。

ですから、日本版ＮＣＦＴＡには攻撃している者を潰していただくことを期待しております。潰すための一つの枠組みとしてここが育っていってくれれば、非常にインシデント対応が楽になると思っています。

○　海外機関との連携ということで、今後の議論になるとは思いますが、「連携」とは具体的に何を指すのかというのは明確にする必要があると思います。

○　国としては既にもう海外関係機関と十分連携をされていると思いますが、日本版ＮＣＦＴＡにおける連携になるとどのように増幅、進化、あるいは発展するのかお聞かせいただければと思います。

○事務局：　これまでは事件が起きた後の事後的、また個別的な対応の中で国際連携を図ってきました。しかし、日本版ＮＣＦＴＡの創設は、先制的あるいは包括的な対応をとるということが目的の一つです。そのために、海外の関係団体であるアメリカのＮＣＦＴＡ、カナダのＮＣＦＴＡ、ユーロポールの下におかれているＥＣ３、あるいはインターポールの下で立ち上がる予定のＩＧＣＩ、こういったところと日本版ＮＣＦＴＡは連携します。つまり、産学官が従来個別に行っていた連携の枠から一歩踏み出し、また別な次元で日本版ＮＣＦＴＡとしての国際連携が必要であるというのが事務局としての考えであります。

○　海外連携に関しては、挑戦的・実験的な要素を入れてみてもいいのではないかなと感じました。

民間のセキュリティ専門家は、被害が起きる前、例えば、不正プログラムの開発が始ま

った段階から情報を集めているわけです。開発された不正プログラムはアンダーグラウンドで売買されたりするわけですけれども、そういった情報をＮＣＦＴＡの中でシェアして被害が出る前の段階から、海外関係機関と連携しつつ、この開発者のプロファイリングをすることができれば、その後、不正プログラムが実際にサイバー犯罪に使われたとき、開発者は誰に売ったのかというところまで追跡できるのではないか、そうすることで、対処についても、かなり効果的にできるのではないか。それぐらいの実験的要素を持たせてみても面白いのではないかなと思いました。

○　日本版ＮＣＦＴＡにおいて技術的な制約と相手方の法律的な制度による制約を乗り越えるための両方の調整が必要になってくるのではないかと思っています。

○　経済産業省が運用している情報セキュリティ早期警戒パートナーシップでは、報告された脆弱性情報を公開しなければいけないときには、法律関係の方たちに日本の法制度を踏まえた検討を行っていただいていますので、日本版ＮＣＦＴＡという形で考えたとき、技術の側面と、動かすときの法制度的な検討は必要になると思います。脆弱性対応とインシデント対応というのは両方を常にやらなければいけないので、２つをうまくつなげていただきたいと思います。

○　具体的なところがまだ見えないなというふうに考えています。日本版ＮＣＦＴＡについて、実際に始めるとなると、現実問題としてできることに絞らざるを得ないと考えています。アメリカのＮＣＦＴＡの取組を踏まえた上で日本では何が一番必要なのか、プライオリティーの観点からの整理、議論が欠かせないと考えています。

それから、例えばＴｅｌｅｃｏｍ－ＩＳＡＣ、ＪＰＣＥＲＴ、ＩＰＡ等、既存の組織があるわけで、これらの組織とのすみ分けについては、しっかりと議論する必要があると思っておりますし、これらの組織との連携も非常に重要だと思っています。

○　日本版ＮＣＦＴＡが立ち上がったときに、一体何ができるようになるのか、何ができていれば目標を達成したことになるのか、この点において産官学が同じ目標を持つところがスタートラインだと思います。その目標が明確に定まったところで、機能、組織、持ち寄るものあるいはコスト等の議論に入っていけるのだと思います。

○事務局：　警察庁では、これまでも、事案が発生した際に、その事件捜査あるいは対処の中で産業界や学術機関に協力を仰ぎ、また、連携して対処してきました。

しかし、サイバー犯罪の１つの特徴として、その脅威が短時間で広範囲に広がり、事件が発生した後の個別の対応では後手に回ってしまいます。したがって、事件が起きる前の

段階で関係者が集まり、間もなく遭遇するであろう脅威に対してどのように対応するか、お互いの知見を結集して防御や対処をするような枠組みをつくりたいというのが、日本版ＮＣＦＴＡの創設を考えた原点です。

また、既存の組織との関係は、非常に大事なテーマだと思っています。日本版ＮＣＦＴＡは、現に機能しているそれぞれの団体の意義を減らすものではないと考えております。むしろ相互に連携して、それぞれの持っている意義を果たしてこそ、日本版ＮＣＦＴＡもさらにその機能を強化できると思っていますし、どのような連携ができるかということについては、この会議での議論をさらに深めていただききたいと思っています。

○　米国におけるＩＳＡＣ等の組織は、ある程度大人数でシェアできるような情報レベルを、ＮＣＦＴＡあるいはＦＢＩに近い組織になってくるとかなり秘匿性の高い情報を扱っているので、項目だけ見ると重なっているように見えますが、中身を見ると複数のグループなり組織があって、それが補完関係になるのが実態のようです。

つまり、米国では、対策が脅威の進化とともに弱体化していけば、さらにその上により強力なものを講じる多層構造になっているようです。同様に考えれば、今回の日本版のＮＣＦＴＡの創設は非常に意義があると思っています。

○　Ｃ＆Ｃのサーバが見つかった場合を例にとると、ある団体からすれば早くテイクダウンしたいところですが、そのＣ＆Ｃを監視すれば本体にたどり着く可能性もあるという考え方もあります。結局、そのＣ＆Ｃはテイクダウンした方がいいのか、生かしたほうがいいのか、そういう議論をするところは現時点ではあまりないと思いますが、日本版ＮＣＦＴＡがそのような議論をする場となって、既存の組織とも一緒に、捜査あるいは犯罪というものを背景とした新たな１つの集まりとして機能できるというふうに期待しております。

○　日本のセキュリティの全体を見渡したときに、人材と情報の両方をレベルの高いところに持っていかないと、国際連携という点で壁に当たりそうな気がします。日本版ＮＣＦＴＡが、日本のセキュリティ人材のトップを抱えている、セキュリティをやっている人たちが自分のキャリアパスを考えたときに、最後の仕事をする場所の選択肢の１つとして選べるような位置づけになることを期待しています。また、海外で新しい情報を集めようとしたときに、人材の交流が最初にあると、相手からの情報や信頼感を得られると思います。つまり、優秀な分析官が日本の外にいるのであれば、そういう人たちも日本版ＮＣＦＴＡで仕事ができて、その人たちの国際チャネルを使っていろいろな情報が入ってくるとか、そういう人たちを見ながら日本のセキュリティの技術者がそういうところで仕事をしたい

と思えるように考えられるとか、そういった感じの位置づけみたいなところがＮＣＦＴＡの中で議論されると、目標観であったり、実際に国際連携であったり、その情報を交換する仕組みがうまく回りそうな感じがします。

○　日本版ＮＣＦＴＡという言葉は、何か具体的な日本語にすればＪＰＣＥＲＴ、Ｔｅｌｅｃｏｍ－ＩＳＡＣとの差別化ができる可能性があります。

例えば、ボットネットテイクダウンを専属とした組織をつくるというのも具体化、到達点となると思います。

○　組織が重複するということ自体は悪いことではない印象があります。しかし、数の点から言うと、技術者の数や対応する人の数は圧倒的に不足していると私は思います。また、ユーザー側から見て、どの組織で対応してもらうべきかということがわからない、あるいは、対応してもらったが期待していたものと違ったということが起こってしまうかもしれないという懸念はあります。

したがって、この辺は調整が必要になるだろうと思っていて、特にＪＰＣＥＲＴあるいはＦＩＲＳＴ系、警察系、どこに相談したらいいのかという点は常にユーザー側から見ると心配事にもなっているので、検討が必要なところだと思います。

組織の話でもう１点、デジタル・フォレンジック研究会という組織がありまして、ここには企業とか研究者も参加し、いわゆる情報の共有がかなり進んでいます。

こういった組織が日本版ＮＣＦＴＡとどのように関連するのかという議論もあり、具体的活動にどう関連するのかはわかりませんが、情報交換について、こういうところとの交換も念頭において検討をしていただければと思います。

６．閉会