平成２５年度総合セキュリティ対策会議（第４回）

「サイバー空間の脅威に対処するための産学官連携の在り方」

～日本版ＮＣＦＴＡの創設に向けて～

平成 25 年９月 27 日

発言要旨

１．開会

２．生活安全局長挨拶

３．米国ＮＣＦＴＡ最高責任者による講演

【米国ＮＣＦＴＡ最高責任者による挨拶及び講演】

４．質疑応答

○　協力の枠組みをつくり上げていく上で情報をシェアすることが非常に大切であるということはよくわかります。また、その前提として信頼関係が不可欠だと思います。この点に関して､アナリスト等に関しては､クリアランス等いろいろな方法があるのでしょうが、パートナーの企業等に関してはどうやって情報を共有して大丈夫であることを判断するのでしょうか。どのようにしてどういう関係を築いて情報を共有しているのかを御教示いただけますでしょうか。

○　まず、小さく始めるということが言えるのではないでしょうか。小さくというのは、企業からの情報の共有を、これであれば出してもいいと企業側に納得していただける範囲に最初はとどめておくということです。企業側にとって、情報共有が被害の抑止につながることが分かれば、彼らはより積極的に脅威情報を共有するようになるでしょう。私たちが行ったように、最初、ＮＣＦＴＡは、情報共有を始めるため、より多くの情報を提供することとなりますが、産業界にとって価値のある情報を共有すれば、産業界はもっと相互の情報共有を活発化させたいと考えるでしょう。ですから、初めは、産業界から提供を受ける情報よりも、ＮＣＦＴＡから提供する情報の方が多いと思います。加えて、産業界が必要とする情報を見つけ出し、情報を共有したいという意思、意欲を持つ企業とモデルケースをつくるというのも重要ではないでしょうか。

つまり、最初はＮＣＦＴＡのアナリストがたくさん調査を行って、どんどん情報を提供

していく。そうすることで、産業界も徐々に納得して、あるいは安心感を得て、情報を共有するようになるということです。

我々も新たなイニシアチブを立ち上げる際、その直後は常に痛みを伴います。なかなか情報が集まらず、ＮＣＦＴＡのアナリストが取りまとめたものを出していくほうが多い状態になるのですけれども、時間のかかるこのような過程を経て、産業界に徐々に納得していただく、あるいは納得して意欲的に情報を出していただく状況に変化するのを待つことになると思います。産業界が必要とする情報を提供することにより、彼らの信頼を得ることが、新たな枠組みの成功につながるに違いありません。仮にいずれかの組織が信頼を裏切るようなことがあれば、情報共有の枠組みから脱退させ、機密保持を厳密に行っていることを知らしめる必要があります。

あと、パートナーについては、共有する情報を開示したり売買したりすることを禁止し、企業を守るために内部で利用することしか認めないというＮＤＡを必ず交わしております。そして、ＮＣＦＴＡのアナリストに関しましては、採用前にバックグラウンドチェックを行うことは前提なのですけれども、実はこの情報セキュリティ関係のコミュニティというものは、皆非常に近しく、善い人、悪い人というものがメンバー同士でわかっております。本当に使命を持ってセキュリティ対策に取り組みたいということを強く心に持っている人は誰かということが仲間の中からおのずとわかってくるのです。

○　インテリジェンスにかかわる活動をＮＣＦＴＡが行っていく過程で、その調査活動、あるいは調査権限を支えている法律はあるのでしょうか。

○　アメリカにもいろいろな法律等がありますが、我々は一般的な法律にのっとった形で活動をします。また、共有されている情報についても、個人を特定するような情報は扱いません。パートナーさんとも共有しません。いろいろな法律等が誤解釈されないよう、それらをきちっと理解した上で活動ができるように規制当局やパートナーとなる産業界の方々から法律の解釈について説明していただく機会なども設けております。

○　２つ質問をさせてください。まず、運営の予算については、恐らく参加企業が資金を負担しているかと思うのですが、それは全ての会社が同じ金額なのか、例えばサイバークライムの多い金融とそうでない製造業とで同じ負担金額で参加しているのか、そうでないのか。あるいは参加企業以外からの、例えば国とか、そういったところからの予算が出ているのか、これが１つ目の質問です。

２つ目はアナリストがＮＣＦＴＡにはいらっしゃると思うのですが、これは企業からの出向者なのか、専任で雇っているのか、そこを教えていただければと思います。

○　アナリストの方々は我々の社員、職員です。今現在、ＮＣＦＴＡの職員の職員に加えて、産業界、各企業のほうから出向している方々がおります。

資金については、メンバーシップフィーでまかなわれているのですけれども、業界によっての差はありません。メンバーシップフィーは３段階に分かれています。まず１つ目が、みずからの企業の社員をＮＣＦＴＡに派遣するというものです。２つ目といたしましては、ＮＣＦＴＡのアナリストがある企業の担当となるというものです。３つ目は、リモートパートナーと呼んでおり、職員をＮＣＦＴＡに常駐させているわけではないものの、必要な時に、ＮＣＦＴＡの施設に来訪する又はＮＣＦＴＡのアナリストに依頼することによって、ＮＣＦＴＡが行ったリサーチですとか、あるいは重要な情報にアクセスできるというものです。

なお、どのパートナーに対しても双方向のコミュニケーションをお願いしております。つまり、ＮＣＦＴＡや他のパートナーが提供する情報にアクセスができますから、利用するパートナーにも我々に情報提供をお願いするのです。

もし情報が一方通行になっているパートナーの存在に気づいた場合、そのパートナーに連絡して、もしかしたら情報を伝達する担当者をもっとサイバー犯罪の分野に関心のある人に変えた方がいいかもしれませんというようなアドバイスをしております。

○　パートナーとして参画する企業にレベルがあるとおっしゃったのですけれども、そのレベルに応じてセキュリティクリアランスも異なるのではないかと思うのですが、そのあたりを少し詳しく教えていただけますか。

○　必ず個人レベルでセキュリティチェックを行いますけれども、このセキュリティ業界というのは、善良な人がとても多いです。また、参画される前に他のパートナーから、時には複数名の推薦が必要になることもあります。ただ、お互い個人レベルで強くつながっておりまして、誰が善良な人なのかということは、おおむね把握しているような状態です。さらに、そもそも私たちの活動や集める情報は全て公開情報であり、機密扱いにはなっていないので、ＮＣＦＴＡの施設に入る誰に対しても機密情報を扱うためのクリアランスを求めてはいません。

５．閉会