21世紀政策研究所新書―38

シンポジウム

サイバー攻撃の実態と防衛

The 21st Century Public Policy Institute

第101回シンポジウム（2013年4月11日開催）

ごあいさつ

21世紀政策研究所では、わが国経済社会が直面するさまざまな課題を取り上げ、内外の学者や有識者、実務家の方々にご参加いただき、積極的に研究・提言活動を行っています。本日のテーマ「サイバー攻撃の実態と防衛」は、今日皆様のご関心の非常に高い課題だと思います。

インターネットがグローバルな社会インフラとして定着するにつれ、私たちの経済活動や生活は非常に便利になりましたが、一方でサイバーセキュリティの問題が深刻化しています。これまで政府機関や特定の産業・個人に対して行われてきたサ

イバー攻撃は、いまや一般の企業や個人も巻き込んで大きな社会的問題を生じています。

そこで当研究所では、昨年7月に土屋大洋 慶應義塾大学大学院 政策・メディア研究科教授に研究主幹をお願いして研究会を立ち上げ、私たちがサイバー空間においてどのようなリスクに見舞われていて、どのような対応をしたらよいのか、検討してきました。ワシントンやロンドンにも出張していただき、専門家と精力的に議論しました。

本日は内閣官房情報セキュリティセンターの占部副センター長から「新たな情報セキュリティ戦略の方向性」と題して政府の対応をお話しいただいた後、土屋先生から当研究会の研究成果をご報告いただき、その後パネルディスカッションで「サイバーセキュリティ――政府と企業が取り組むべき課題」について議論していただくことにしています。

本日のシンポジウムが皆様にとりまして有意義なものになることを祈念して、私からのごあいさつとさせていただきます。

二〇一三年四月十一日

21世紀政策研究所所長　森田富治郎

基調講演

新たな情報セキュリティ戦略の方向性

内閣官房情報セキュリティセンター副センター長
内閣審議官
占部浩一郎

すべてが繋がる時代

本日は「新たな情報セキュリティ戦略の方向性」というタイトルで、前半はいま、どういうことが起こっているかということに触れ、後半はいま、われわれがつくっている戦略の話をしたいと考えています。

いま、どのようなことが世の中で起こっているかというと、歴史的には、非常に大きなパラダイムが変わったことが挙げられます。それは、パソコンの歴史を考えればよくわかります。

最初に私が家でパソコンを買った90年代に入る前後は、インターネットの世界はなく、単にワープロの代わり、一太郎が使えればよいという感じでした。パソコンはウィンドウズ95が出た１９９５年に爆発的に広がり、当時はパソコンの中にモデムが実装されて、なんとなくインターネットに繋がることができました。家に帰ってパソコンにスイッチを入れて、メールを取りに行くなど本当に必要なときだけ、

占部審議官

ダイヤルアップでインターネットに繋ぎ、電話線を通してジジジ……と拾っていた時代です。

２０００年になってウィンドウズＸＰなど、ネットに繋がる基本的な機能が極めて高いレベルで実装され、非常に使いやすい環境が整ってきました。当時、ＩＴ戦略本部で「月３０００円で使う」という、その当時としては無体な計画を打ち出しましたが、いまでは十分実現されています。まさにブロードバンドが広がったということです。

ネットに繋がらない時代から、電源を入れ、電話をかけたら繋がった時代。２０００年にな

ってからは、電源を入れた瞬間にもうネットに繋がっている時代。そして２０１０年というとスマートフォンなど電源が切れない時代になった。要するに何千万台のデバイスが、常にネットワーク上に繋がっている時代。これがいま、われわれが過ごしている時代です。

そして、ここまで言った話は全部、基本的に人間がインターネットを使う時代ですが、今度はそうではなくて、機械と機械が会話する時代、人間の意識しないところで、既にすべてのものがネットワークに繋がっているというのが次の時代になります。もう始まりつつありますが、そういうフェーズに入ってきたのです。

サイバー空間を取り巻くリスクが深刻に

そうすると何が起こるかというと、資料１に「甚大化するリスク」「拡散するリスク」「グローバルリスク」と書きましたが、リスクが極めて深刻化することにな

資料１　サイバー空間を取り巻くリスクの深刻化例

●：国内外で実際起こったもの。　○：可能性が指摘されているもの。

甚大化するリスク

●標的型攻撃により、国家機密、企業機密の窃取が発生。数年前からの窃取も発見。

●海外にて、クローズな制御系システムがウイルス感染。核関連施設が稼働不能化

●海外にて、元契約社員により、制御系システムが不正操作され、川に汚水が流入

○ITS やスマートグリッドへの攻撃による交通混乱やブラックアウトの恐れが指摘

拡散するリスク

●常時、電源 ON・ネット接続で携帯されるスマートフォンから情報流出が多発

●コンビニにおける防犯カメラが踏み台となり、DDoS 攻撃が実施される

○ネット接続の家電や自動車から生活情報や位置情報が流出する恐れが指摘される

○オフィスにおけるコピー機等の複合機が情報窃取の起点となる恐れが指摘される

グローバルリスク

●海外にて、外国政府の関与が疑われる政府機関等に対する DDoS 攻撃が発生

●海外にて、企業秘密の窃取等を狙った外国軍隊の関与が疑われる攻撃が発生

●国内の個人 PC 等が踏み台となり、指令サーバーとして外国に DDoS 攻撃が実施される

○武力攻撃の一環としてのサイバー攻撃が国内を起点に外国へ行われる恐れが指摘される

（出所）内閣官房情報セキュリティセンター

ります。

まず、標的型攻撃（資料1の左欄の一番目）ですが、これについては、後ほどお話しします。

同左欄の一番下に書いてありますように、ＩＴＳ（高度道路交通システム）やスマートグリッドの問題もあります。ＩＴＳは、自動車が自動で運転してくれますし、スマートグリッドでは、電力が適切な配分をされて、極めて効率的な電源ネットワークができます。ただそこに「誰も電気を使っていないので、いま電力の発電量は少なくてよい」という偽の情報が入った途端にブラックアウト（停電）してしまいます。また、ＩＴＳが攻撃されて信号機が変な制御をされたらぶつかります。車と車が会話をしだすと、たとえば「この道は空いているよ」とか「どんどんスピードを出せるよ」という嘘の情報を出されると、ゴツンとぶつかる。そういう極めて甚大な事態が起こる可能性があると考えています。

その上に書いた、「海外にて、元契約社員により、制御系システムが不正操作され、川に汚水が流入」というのは実際に起きた例です。

中央の欄の「拡散するリスク」というのは、皆がスマホを使っている状況があり、いろいろなところに、危険な因子が転がっているということです。

その2番目に「コンビニの監視カメラ」を挙げています。パソコンと同じような機能はスマホだけでなく、監視カメラや、情報家電も持っています。普通のテレビでもネットに繋げることができるのです。そのためのソフトは専門のものではなく、リナックスをチャチャッと直して、基本的なコンポーネントとして使っています。そうすると、その部分は完全にパソコンであり、かつ無防備な状態で置いてあるのです。コンビニの監視カメラもそうで、そこを踏み台としてよそを攻撃するということが実際に起こっています。

4番目に、「オフィスにおけるコピー機等の複合機が情報窃取の起点となる」と

書きましたが、これも非常に考えられる例で、複合機というのはすごい機能を持っています。昔のコピーは、スキャンしたものをそのまま機械的に吐き出していたのです。しかしいまは、全部サーバーに溜め込んで、貴重な情報に「極秘」という判子を押して、複合機に送りつけて、それをプリントアウトしています。サーバーになっていますから、そこのデータベースの中に情報が残って、情報窃取が起きる可能性があります。サーバーは、ネットでローカルな保守がなされることもありますし、保守員が来てそこの中を見ることもあります。もちろん非常に高いセキュリティレベルを取った製品はありますし、ＩＳＯの認証を取った機械もあって、すべてそういうところまで対策してあればよいですが、実際には情報窃取が複合機で起こり得るということを非常に強く認識しておかなければなりません。

右欄の「グローバルリスク」というのは、そのようなことが国内だけで完結しない時代だということです。いろいろなところに外から攻撃できるし、われわれも逆

に外に対して攻撃できるわけです。技術自体によい、悪いがあるわけではありません。包丁は料理に使えるし、犯罪にも使えるのと同じことです。メンテナンスはしなくてはいけないし、個々の端末を一個一個制御するわけではないのだから、システム管理者にとって遠隔操作するのは当然のことです。その意味でソフト自体に悪意があるわけではなくて、結局使い方なのです。

本当に大きい近代的なビルになると、エアコンも、エレベータも、すべてのものがコンピュータで制御されます。そういうところを仮に乗っ取られると、何が起こるかはわかりません。ではエレベータの保守員を必ずこのビルに何人も常駐させるかというと、そうはしません。結局そこはリモートで見て、誰かが閉じ込められたらすぐに助けに行くようにする。リモートで外から見られるようにしないと、いい機能にはならないわけです。だから利便性をどんどん追求して、かつ実空間とサイバー空間がくっついてしまっています。それは非常によいことです。ただそれに伴

って、いろいろな問題が発生しているのがいまの状況であるという認識を持っているわけです。

標的型メールによる攻撃

最近よくあるサイバー攻撃のテクニックは、標的型メールを送りつけるパターンです。標的型メールとは、ある種の人に狙いを澄まして不審メールを送りつけ、それを開かせてウイルス感染させるということです。

「不審メール」と言いましたが、実はほぼ真正なメールが送りつけられる例があります。どこをどう見てもおかしくありません。非常に高度化してきています。おそらく、メールは何人にもディストリビュート（配信）されているので、どこかの人に狙いをつけて、その人が送った本物のメールを拾っていると思います。それに細工をして、添付ファイルを付けて開かせるようにしてあります。だからよく気を付

けていないとわかりません。

普通に添付ファイルをくっつけて不審メールを送ると、アンチウイルスソフトがチェックして弾く可能性があります。おそらく攻撃者はありとあらゆるソフトウエアを買ってきて、不審メールに引っかからないかどうか自分でウイルスチェックをしてみて、これだったらどのソフトにも引っかからないと思って送りつけています。それでもまだ、引っかかる可能性があります。

最近よくあるパターンは、圧縮をかけてZIPファイルにして、それを付けて送ってきます。そうすると暗号化されるので、実はウイルススキャンが効かないのです。ZIPファイルは基本的にそのままスルーで来ます。

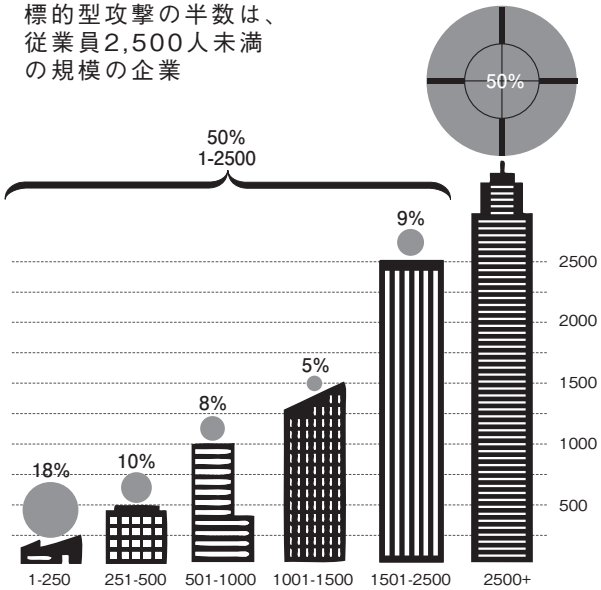
でもおかしいところが1カ所あります。「安全のためパスワードをかけてあります。パスワードは何番です」と、そのZIPファイルが付いたメールの中にパスワードも入っています。これは、よくよく考えるとおかしいわけです。電話でパスワ

ードを教えるとか、最低限、違うメールで「先ほど送ったメールのパスワードはこうですよ」と伝えれば少しはいいのですが、一緒にパスワードを書いてくるなんて、それは絶対におかしい。もしそのようなメールを送られたら直ちに削除してください。

こういうことを、本当に職員一人ひとりのレベルに徹底していかないとだめです。われわれも政府職員に対し、昨年度、十数万人に向けてそういう不審メールを送って訓練しました。開けてはいけないと命ずるのではなくて、つい開けてしまうことを気付かせるとともに、もし開けてしまったときに、ＬＡＮケーブルを抜くとか、そういう非常時のオペレーションがちゃんとできるかという意味で訓練しています。そういう末端の対策は必要です。

標的型メールなどが送られてくる対象は、「大企業だけだから大丈夫だ」というのは嘘です。資料２にある通り、実際に送られてきたのは２５００人未満の企業が

資料2 Attacks By Size Of Targeted Organization



（出所）INTERNET SECURITY THREAT REPORT：2011 Trend Volume 17
（2012 年 4 月、Symantec 社）

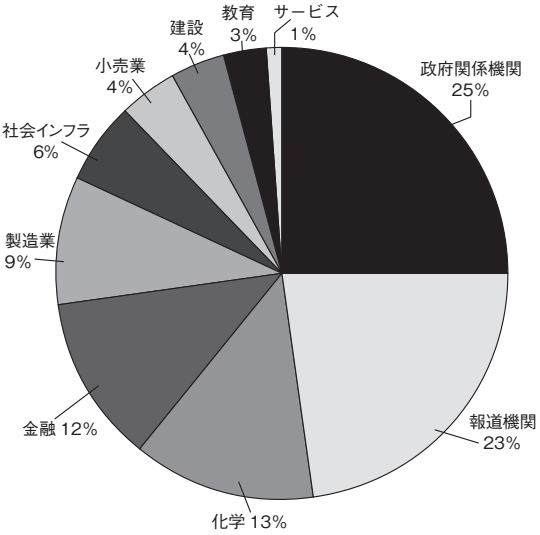
半数を占め、中小・中堅企業が相当程度ターゲットになっています。

送られる対象としては政府や報道機関がトップで、ここを直接やっつけようという意図があります（資料3参照）。もう1点は、報道機関や政府機関から来たものは比較的信じやすいものですから、それを使えば次の攻撃をするときに非常にやりやすいということです。政府機関、自治体など公的機関は全部、そういうことで攻撃ターゲットになっているのが現状です。

最近、こういうサイバー攻撃を受けたことがあるか調べましたら、２００７年は「経験がありません」というのが91％で、２０１１年には45％でした。「あります」は２００７年が５％で、２０１１年が33％です。「標的型攻撃が増えたのだな」というのが素直な解釈です。

しかし、より本質的な解釈は、45％が「ない」と言っているのが非常に怪しいということです。要は「ない」ということを証明するのは大変難しく、きっと気が付

資料３ 標的型メール攻撃のターゲットとなった組織の業務別割合



（出所）「2012 年上半期 Tokyo SOC 情報分析レポート」
（IBM、東京 SOC 調べ　2012 年 1月～6月）

いていない人が多いのです。

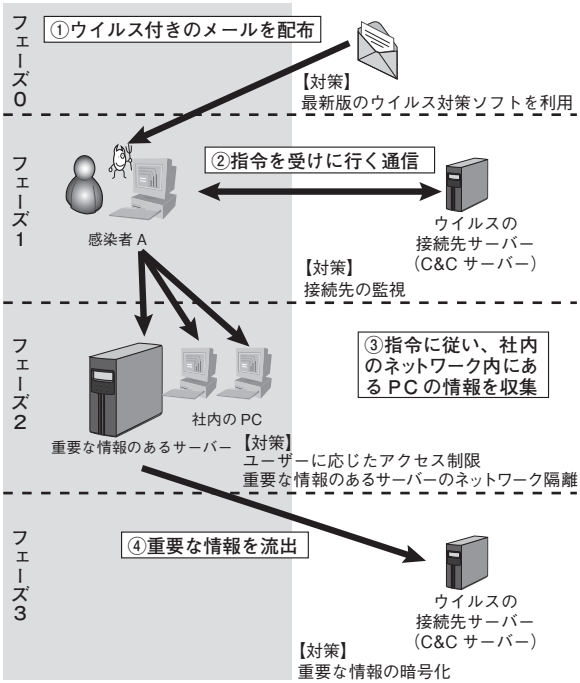
中国のサイバー攻撃のレポートをつくった米国のセキュリティ会社マンディアントの新しいレポートを見ても、自ら気が付くというのは非常に少ないパーセンテージです。では「その侵入された状態がどれだけ続いていたか」と調べると、先ほどのマンディアントのレポートだと最新の数字は8カ月くらいです。また、その前年のレポートを見ると2年、ひどいものは5年くらい気が付かなかったものがあります。だから認識をすることは非常に大事で、わからないと対策の打ちようもないのです。わからない間は、ずっと全部のぞき見をされていた可能性があります。自分の会社が一生懸命つくってきたものが、既に全部見られていた可能性があるということです。

1通のウイルスメールで1台のパソコンを乗っ取っただけで、なぜ重要な情報が抜き取られるのかという疑問があります。実は何回もやり取りがあり、システムが

脆弱であるとわかると取られてしまいます。たとえば資料4（24ページ）で、フェーズ1は普通の従業員の端末がウイルスに感染して、まずこれが乗っ取られる。しかし最後にどうやって会社の秘密情報の端末までたどりついたのか――実はちゃんとシステムをつくっていないためです。一般の従業員である感染者Aが、自分の端末から会社の機微な秘密情報や人事情報などにアクセスできるというのがそもそも問題なのです。普通はパスワードや管理の権限を設定しています。

でもそこにいろいろな間違いをしでかしているので、たった1台の端末がやられただけで、パスワードから何から全部持っていかれる可能性があります。細かいことは説明しませんが、いろいろな段階で各種の対策をしなければいけないのです。単にウイルスソフトだけではだめで、外への出口のモニターもするとか、システムをちゃんと領域ごとに隔離するとか、本当に大事なものは金庫に入れるとか、暗号をかけてしまっておくとか、リスクに応じて考えてやらないと、全部抜かれてしま

資料４ ウイルス付きのメールで重要な情報を抜き取る



（出所）内閣官房情報セキュリティセンター

います。

敵はとにかく一番弱いところを狙ってきます。システムをしっかりとつくっても、従業員のところに穴があれば、そこから侵入をかけることがあります。逆に人間のほうが強くて、機械のほうが弱いケースもあります。一番弱くて、かつ一番強いのが人間で、その中間におそらく機械があるということかもしれません。

普通の社内や取引先間でやり取りをするメールは、気を付けて開けたり開けなかったりというコントロールをします。ところが最近よくあるのが、たとえばお客様のクレームを受けるところ、役所でいうと、ご意見受付番みたいな窓口へのメールです。「どこそこの誰です。今度このレポートを書きました。読んでほしいのですが、送っていいですか」。そんなことを言いながら、やり取りを何回かして「ではここに送らせてもらいます」と言って送ってきて、開けるとドンというのがあります。絶対に開けざるを得ないところを狙ってくるのです。

それから、一つの企業は一生懸命守っていても、たとえば団体として工業会があって、その工業会が非常に弱かったりすると、工業会のサーバーをのぞき見されていれば、工業会の名前を使って「明日の会議の資料を送ります」、これを開けてしまうということがあります。いろいろな企業や団体が繋がっているので、その弱いところからプチッとやられるのです。親会社はしっかりしているけれども、買収した子会社や協力会社に弱さがあることもあります。職員はよいけれども、たとえば派遣で来た方から出てしまうなど、いろいろなことがあるのです。

新たな情報セキュリティ戦略の策定

いまのようなあぶなっかしい話を、ではどうしようかということで、われわれはいま、対策を考えています。本日お話しになる土屋先生、野原先生はそれぞれ、情報セキュリティ政策会議という実際の政策をつくる会議のメンバーであって、実は

われわれは事務局です。そこで議論していることを紹介させていただきます。

新たな情報セキュリティ戦略については、何回か議論してきて、最終的にはおそらく２０１３年５月半ばくらいに最終公表しようと作業中です（２０１３年５月21日に最終案を公表、６月10日に「サイバーセキュリティ戦略」を決定した）。

資料５（28ページ）にありますように、新たな情報セキュリティ戦略では、最初に「環境の変化」を挙げています。先ほど言ったようにサイバー空間と実空間が一体化してきて、それに伴ってリスクが非常に深刻化していきます。しかしながら、これからの経済発展・成長を考えたときには、ＩＣＴがないとまったくやっていけません。ですので、強靭であって活力がある空間をつくるということで、サイバーセキュリティ立国に取り組んでいきたいということを基本的な方針にしています。

その中で大事なのは、情報がきちんと自由に流通できること、インターネットの開放性等を確保するということです。その開放性は、脆弱なネットワーク空間では

資料５　新たな情報セキュリティ戦略の方向性（概要）

環境の変化

サイバー空間と実空間の融合・一体化 ［普及・高度化・更なる進展、グローバルな拡大・浸透］ ▶ サイバー空間を取り巻くリスクの深刻化 ［甚大化、拡散、グローバル・ボーダレス］

基本的な方針

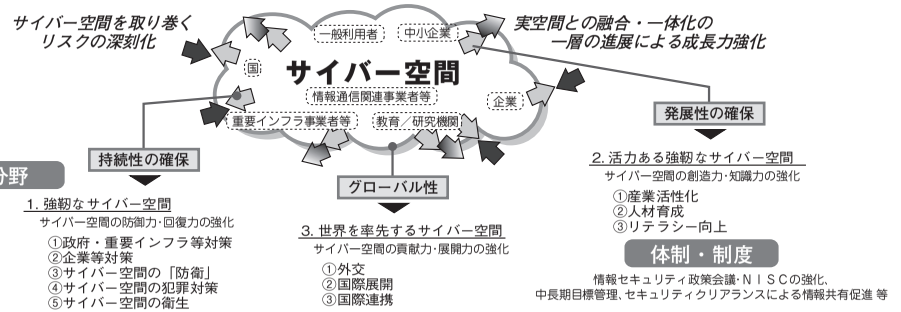
国家の安全保障及び経済発展、国民の安全・安心を確保するため、世界を率先する強靭で活力あるサイバー空間を実現　「サイバーセキュリティ立国」

① 情報の自由な流通の確保　② リスクの深刻化への新たな対応
③ リスクベースによる対応　④ 社会的責務を踏まえた行動と共助

各主体の役割の明確化

国による積極的／先導的な役割	重要インフラ事業者等による安定的な役割	企業や教育・研究機関による協調的な役割	一般利用者や中小企業による自律的な役割	情報通信関連事業者等による自浄的／自立的な役割

取組分野



（出所）内閣官房情報セキュリティセンター

実現できません。自由な流通を保証するためにリスクの深刻化に対応した強靭なものをつくらなければいけないのです。

基本的な方針には、「リスクベース」ということも挙げています。さっき「本当に大事なものは金庫に入れてしまっておく」と言いましたが、全部繋がっている世界では「全部を守ろう」というのは無理なので、リスクの具体的可能性に応じた対応強化をしなければなりません。

それから「社会的責務を踏まえた行動と共助」ということも書きました。要は1人でできることではありません。いままでは個々の人が、それなりに対策をしていれば「まあいいか」ということになりましたが、全部繋がっているので、そういうことではできないのです。サイバー空間の「空間」ということに着目して、われわれがコンセプトとして今度出そうと思っている中に、「公衆衛生」という概念があります。

インフルエンザがはやったときに何をするかというと、当然マスクをして手洗い・うがいをしてくださいということになります。他方、薬をつくる人がしっかりとつくってくれなければいけません。それから保健所があって、「いまインフルエンザがピークを迎えているので注意してください」と、きちんと皆に言わなければいけません。そういういろいろなことをやって、いろいろな役割を担っている人がしっかりとセキュリティに取り組むという共助の世界をつくっていかなければいけないということです。

その中で「取組分野」についても書きました。強靭なサイバー空間をつくろう。活力ある、いろいろな新しい先端的な技術も含まれるものをつくろう。それからグローバルに展開していこうということを、全体としてやっていく戦略を立てているところです。

いまは非常に便利な時代になりました。それに伴ってリスクが発生します。１０

0%リスクがなくなることは絶対にありません。絶えずそのリスクが隣にあることを考えながら、生活していかなければなりません。だからといって怖がる必要はまったくない。体力のない人がインフルエンザにかかると死んでしまうかもしれませんが、きちんと日ごろ体力をつけておけば、少々リスクがあっても大丈夫です。

最近、サイバー空間では、「防御」という言葉よりも、「レジリエンス」という言葉が使われます。しなやかで強靭、回復力があるという意味です。要するに何かダメージを受けても、それほどダメージが効かないのです。今後はしょっちゅう変わるものに、いかに動的にダイナミックに対策を変えていくかということが必要なので、やはり皆で取り組んでいくことが必要だと考えています。

報告

サイバー攻撃の実態と防衛

21世紀政策研究所研究主幹／
慶應義塾大学大学院政策・メディア研究科教授　土屋　大洋

土屋研究主幹

多種多様なサイバー攻撃

先月、韓国でサイバー攻撃が大きく話題になりました。たくさんの取材が私のところにも、後でお話しいただく伊東さんのところにも来まして、一体これはどうなっているのだと聞かれました。「おそらく北朝鮮だろう」ということを、テレビや新聞、ラジオで申しあげてきたところです。

でも、別の可能性もあるのではないかということも指摘されてきました。２００９年７月にも韓国では大きな攻撃がありました。あるいは２０１１年にも大きな攻撃があったわけです。

そのときに、「おそらく北朝鮮だ」と言われながら、なかなか韓国政府は確定情報を出しませんでした。ところが昨日、今回の攻撃については「北朝鮮の犯行だ」と、韓国政府がわざわざ記者会見で言ったわけです。「北朝鮮軍の偵察総局による犯行だと判断している」と言いました。これは私にとってはそれなりの驚きで、よくそこまで言い切ったと思いました。別の報道によりますと、昨年6月以降、北朝鮮から1590回の接続があったことも出ています。

サイバー攻撃というのは、悪いハッカーがコチョコチョとパソコンをいじるとできると思いがちですが、そんなことはなくて、非常に手の込んだ作戦をしないと大掛かりなものはできません。1590回もアクセスがあったら、今回の攻撃もわかりそうなものですが、他のたくさんの接続にまぎれてきていることがありますから、なかなかわかりにくかったのかもしれません。今後この分析はもっと進むかもしれませんが、こういったことがこれからも、いろいろな国で起きてくる可能性は

否定できないと思います。

サイバー攻撃にはどんなものがあるのかといえば、多種多様です。90年代からはホームページを書き換えるとか、あるいは愉快犯的にサーバーの中に入っていって何かしら情報を取ってくるということが行われてきましたが、それとは違う次元の攻撃が近年は始まってきています。

その一つが2007年に行われた、エストニアに対するDDoS攻撃というものです。DDoSというのは、簡単に言いますと、皆さんのご自宅の玄関の前に何百人、何千人もの人がいきなり集まってきて、一斉に呼び鈴をピンポンピンポンと押しまくるというものになります。そうすると中にいる人は対応できなくなって機能を停止せざるを得なくなる。皆さんの会社のウェブサーバーや何らかの金融取引をやっているサーバー、メールサーバー、そういったものが狙われてしまう。その結果、一時的に業務を停止せざるを得ない状況に追い込まれるというものです。

エストニアの場合は、きっかけはこのブロンズ像（資料６）でした。もともとエストニアの首都であるタリンの中心部の広場に置かれていました。ブロンズ像の下にはソ連時代の兵士の遺体が眠っていたと言われています。しかしエストニアの人たちから見るとロシアは目障りなわけです。自分たちの首都の真ん中からこういったものは取り除きたいということで、ちょっと離れた郊外にある戦没者記念墓地に移したいと言いました。そうしたところ、それがロシアのニュースで取り上げられ、一斉にロシアからと思われる攻撃がエストニアで始まったわけです。

エストニアは、われわれが考える以上に進んだ情報社会です。街中を歩いている人たちはほとんど現金を持ち歩いていません。日本でいうスイカみたいなものを使ってあらゆるところで電子決済をやっていますが、それがまったく機能しなくなりました。こういったＤＤｏＳ攻撃は、その後も次々と行われるようになっていきます。

資料６　エストニアのブロンズ像

（注）2011年11月撮影

その一例が、われわれが東日本大震災で苦しんでいるときに行われました。２０１１年3月11日の20日後、政府の皆さんにいくつかの電子メールが届きました。「昨日の放射線レベルについて」というタイトルが付いていたそうです。当然われわれは、福島第一原発の問題について気にかけていたところですから、開いてしまいます。その中にカスタマイズされたウイルスが仕込まれていたと言われています。先ほど占部審議官がおっしゃいましたが、どう見ても騙されるという仕込みをしたウイルスが送られてきます。それも、ウイルス対策ソフトウエアで引っかからないことをあらかじめ確かめた上で送ってくるのです。

実際に私のところに送られてきたものをご紹介します（資料7）。「どこかの室長さんとの意見交換についてまとめたものを転送する」というふりをしています。ところが差出人は、ヤフーの無料アドレスを使っています。一番下に見える添付ファイルが、先ほどおっしゃっていたように、ＺＩＰファイルになっています。私は差

資料7 偽メールの例


差出人: [redacted]@yahoo.co.jp
件名: Fw: [redacted]室長との意見交換会
日時: 2013年1月24日 12:28:40 JST
宛先: [redacted]
返信先: [redacted]@yahoo.co.jp

各位

お疲れ様です。
[redacted]室長との意見交換会（closed）に関する資料をお送りいたします。

****
[redacted]
内閣官房 [redacted]
〒107-0052
東京都港区 [redacted]
Tel : 03-[redacted]
Fax : 03-[redacted]
E-mail : [redacted]@cas.go.jp
****

出人を存じ上げませんので、おかしいなと。そもそも本文がなくて、転送で来ているのもおかしいです。ということで、これはその筋のものだと思って、室長さんに電話をしたところ、「すみません、いっぱい送っちゃっているみたいです」とのことでした。実際にこういうことが起きています。

この中身、当然ファイルは開きませんでしたが、しばらく経ってからウイルス対策ソフトで調べて

みると「トロイの木馬」が入っていることを検知できました。送られてきた当日は、検知できなかったのですが、しばらくすると検知できるようになっています。最初の段階ですり抜けてしまうと、乗っ取られてしまう。

イランのナタンズにある核施設がサイバー攻撃の対象になったのは、非常に有名な事例です。この施設の遠心分離機に対し、スタックスネット攻撃が行われました。誰がやったのか最初はわからなかったわけですが、後の報道でイスラエルとアメリカが共同作戦としてやった、つまりイランの核開発を遅らせるために行ったものだろうと言われています。アメリカ政府は公式には認めていませんが、この記事を書いたニューヨーク・タイムズの記者は、アメリカ政府の複数のルートから情報提供を受けたと言っています。

その後イランは、急速にサイバー攻撃の能力を高めていくことになります。今度はイランがやったと言われているのが、サウジアラビアの石油会社アラムコに対す

るサイバー攻撃です。ある日アラムコのコンピュータが起動しなくなりました。これは、先月行われた韓国に対する攻撃と似ているところがあるのではないかと、私は思っています。

まったくの推測ですが、イランと北朝鮮は核、ミサイル、その他で協力関係を深めていますので、何らかの示唆があったと考えてもおかしくはない。手法としてはそんなに新しいものではなくて、ウイルスに感染させてパソコンを起動させなくするということですから、それほど難しいこともありません。しかしこれも韓国の例と同じく、たぶん長い時間をかけて準備を行った結果行われた攻撃と考えたほうがよいと思います。

アメリカのコカ・コーラ社も、サイバー攻撃を受けたのではないかと言われています。コカ・コーラ側は一切公表していないようですが、さまざまな報道でわかってきています。

コカ・コーラは中国市場を目当てに中国のフイユアンというジュース会社を買収しようとしました。ところが買収を計画していることを発表した途端に、サイバー攻撃が始まったと言われています。どうやら副社長が先ほどの標的型のメールで引っかかったようです。交渉の中身がばれていたようで、コカ・コーラは買収に失敗し、中国系のファンドがこの会社を買うことになりました。ですから皆さんの会社の中でもそういうことが行われていたら、事業に直結するような被害があり得ると思います。

中国のサイバー攻撃とアメリカの対応

これも先ほど占部審議官からお話がありましたが、マンディアントという会社が2月に報告書を発表しました。それによれば、中国・上海のあるビルの中で人民解放軍がサイバー攻撃を行っていたのではないかと言われています。

名指しをされたのが、上海にあるビルです。そのビルが本当にサイバー攻撃目的で使われたのかどうかは、報告書を読んでも確たる証拠はなくて、推測の域を出ないところがあります。しかしニューヨーク・タイムズがこの報告書について報道したため、アメリカでは大騒ぎになっていきます。

伊東さんは、第一報を聞いたときに「何かおかしいと思った」と言っていました。

それはなぜかというと、「プロジェクト２０４９研究所」というアメリカのシンクタンクの報告書が既にあったからです。２０１１年に出たものですが、伊東さんは「この報告書の中に書いてあることだよ。マンディアントの報告書の中身は」とおっしゃいました。なるほどそうかもしれないと思って、私も読んでみたところ、やはり書いてあるのです。

先ほどのビルの中に「６１３９８部隊というものが入っていた」とマンディアン

トの報告書は言っていますが、その６１３９８部隊の名前自体も、プロジェクト２０４９研究所の報告書に出ています。そうすると、これは何なのでしょう。マンディアントの報告書は、アメリカ側の中国に対する一つの警告として取り上げられた、あるいはうまくショーアップされたと考えたほうがよいのではないかと思います。

ではなぜアメリカは、これだけ怒っているのかということになります。オバマ政権は４年ごとに防衛計画を見直す中で、２０１０年に出された「ＱＤＲ（４年毎の国防計画見直し）」において、「サイバースペースは独立した作戦空間だ」ということを言い出しています。

陸・海・空がいままでの作戦空間だったわけです。ところがこのころからアメリカ政府は、宇宙というのが第４、サイバースペースが第５の作戦空間だと、さまざまな報告書の中で言い始めています。これは、サイバー空間を通じた戦争が起きる

かもしれないということを想定し始めたのです。実際にサイバー軍というものも、アメリカ軍の中につくられました。

三つ星の将軍だったキース・アレクサンダーという人が、このサイバー軍のコマンダーになるときに星をもう一つもらって、四つ星の最高位の将軍に昇格しました。その上でこの問題に取り組めと言われたわけです。アメリカの決意は、徐々にステップアップして公表されてきています。

２０１２年10月、当時のパネッタ国防長官は業界団体の席でスピーチを行いました。その中で彼は「サイバー・パールハーバー」という言葉を使いました。彼はそれまでも何度かこの言葉を使っていますが、かなり強い調子で、「特に人命の損失、あるいは物理的な被害に繋がるサイバー攻撃がこれから起こるかもしれない」と警告を出しました。その席で彼は30億ドル、1ドル90円で換算しますと２７００億円くらいのお金を、国防総省だけで使うという声明を出しています。

オバマ大統領はこの話を受けて、今年2月の一般教書演説でサイバーセキュリティを取り上げました。「われわれはこの問題をもう見過ごすことはできない」と言ったわけです。

その演説の中で大統領はさらに、「私はこの一般教書演説に来る前に大統領令にサインをしてきた」と言ったのです。それが「重要インフラのサイバーセキュリティ改善のための大統領令」というものです。

大統領令というのは、法律の一段下の法的効力を持った命令です。なぜこれが出てきたのかというと、アメリカ議会がサイバーセキュリティに対応する法律をつくれないからです。私が数えてみたところ、前回の会期中、2年間に76本くらいの法案、決議案が出てきているのですが、ほとんど成立していません。予算に関連するものだけが成立していて、サイバーセキュリティを一歩進めるような強い法案はほとんど成立しませんでした。大統領はそれにいら立ちを隠せず、この大統領令をあ

えて出してきたのです。「1年以内に議会は法案を通しなさい」と強い口調で言っています。

それに対応するわけではないのですが、3月になって「H.R.933」という法案が作定されました。この法案は、ほとんどは政府関連機関の予算を承認するものでしかないのですが、その中の「SEC.516」が非常に注目を浴びています。

この中でアメリカの商務省、司法省、宇宙を担当しているＮＡＳＡ（航空宇宙局）、科学技術政策を担当しているＮＳＡ（国家安全保障局）が、「中国製の情報技術システムを購入する際にはＦＢＩ（連邦捜査局）の検査を受けてからにしろ」と言ったわけです。これは非常に問題のあるものだろうと思います。いろいろな情報機器の中に中国製品が入っていますから、本当に達成できるのかということが議論になっています。そういう面で、これは経済戦争にも繋がりかねない措置と言えると思います。

イギリスの対応

われわれの調査チームは、イギリスにも行ってまいりました。イギリスはキャメロン首相が、サイバーセキュリティでは非常に強いリーダーシップを取っています。キャメロン政権は何度かサイバーセキュリティに関する報告書を出していますが、最新のものは2011年に出た「サイバーセキュリティ戦略」というものです。「デジタル世界の中でイギリスを守り、その能力を高めていく」ということを言っています。

キャメロン首相は、サイバー攻撃というのは「ティア1の攻撃」「ティア1の脅威」だと言っています。「ティア」というのは層とか列ということです。いくつか脅威の序列があるとして、その一番上にある脅威の一つとしてサイバー攻撃があるのだということを、強い調子で言っています。確か6億5000万ポンド（約1000億円）くらいの予算をつぎ込んで内閣府主導でこの対応を取っていくと言って

いました。日本ともぜひ協力したいと、常々イギリスは言っています。

日本の対応について

日本政府においては「情報セキュリティ政策会議」が２００５年につくられて、戦略を積み重ねてきました。先ほど占部審議官からお話があったように、２０１０年につくられた「国民を守る情報セキュリティ戦略」が今年期限切れになりますので、新しい戦略をつくっているところです。ここは大きくフェーズが変わってきていると思うのです。

先ほど占部審議官はいろいろな論点を紹介してくださいましたが、私は、第一に自衛隊の問題をどうするかを考えなくてはいけないと思います。自衛隊とは、そもそも国民を守るために存在しているはずです。ところが、このサイバー空間の中で自衛隊は何ができるかということは、いまだにはっきりと決められていません。は

っきりしていることは、自衛隊と防衛省のシステムを守ることです。しかし国民のネットワークをどこまで守れるのか、何ができるのかということは、これから論じなければいけないポイントだと思います。

第二に、通信の秘密が日本の法制の中では過剰に保護されていると私は思っています。もちろん通信の秘密を守ることはとても重要な人権の一つだと思います。しかしこの問題を過剰に守りすぎているがゆえに、われわれは危険な通信を止めることもできない。不正な通信を止めることもできない。そういうリスクを冒しているのではないかと思います。

三つ目が情報共有です。政府と民間との情報共有も難しくなっていますし、日本政府と諸外国との情報共有も難しくなっている側面があります。たとえばいま、機密保全法が安倍政権によって提起され、たくさんの方々が反対の声を上げています。しかし私は賛成しています。というのは、秘密を守れない国に情報共有はでき

ないからです。

皆さん、ペラペラと秘密をしゃべる人と情報を共有できるでしょうか。日本政府はそのように世界中から見られています。日本には秘密法制がないではないか。日本の公務員は秘密をきちんと守ってくれるのか。尖閣のビデオ、あの始末はなんだと言われているわけです。もちろん政府が過剰に秘密を守ることは危険です。それを監視する国会がしっかりすべきだと思います。国会の中にそれを監視する委員会をつくった上で機密保全法制を進め、サイバーセキュリティを進めていく。こういったことも必要ではないかと思っています。そういった方向で次のサイバーセキュリティ戦略が進めばよいと考えます。

サイバーセキュリティ10箇条

皆さんのお手元に報告書の暫定版をお配りしています。その冒頭に「企業ダメー

ジ最悪のシナリオ」というものを書きました。あくまでシナリオであって、空想上のものでしかありません。しかしそんなにひどい空想話ではないと思っています。

皆さんの会社のシステムが攻撃されることによって、皆さんの会社の業績に直結するような被害が起きる可能性があります。皆さんが積み重ねてきた企業秘密あるいは知的財産が、そこから奪われていくことになります。先ほどコカ・コーラの例でご紹介したように、交渉事がうまくいかなくなることも大いにあり得る話だと思います。それが皆さんの会社だけで留まらずに、産業全体に波及していく可能性も否定できません。

たとえば業界の中のA社がやられたときに、そのやり口をうまくまねて、B社、C社、その他の企業に芋づる式に攻撃が行われることは、いろいろなところで起きています。それを止めるためには当然、皆さんが最初に攻撃されたときに対応していただくことが必要になってきます。それがうまくいかなかった場合には、社会機

能の喪失、国全体に大きな被害が及ぶ可能性があります。そのリスクを皆さんの対応が担っていることを、皆さんと共有できればと思い、このシンポジウムを開きました。

情報の共有というのは、実はとても難しいと思います。たとえば皆さんの株価に直結する可能性があります。「うちの会社が攻撃を受けました。情報を失った可能性があります」。これを記者会見でしゃべることは非常に厳しい。ですが、何も記者会見でしゃべる必要はないわけです。

情報を業界の団体の中で共有していく、あるいは政府と共有していく。それによって業界の中の他の会社に波及することを止められるかもしれないのです。情報を共有することは、世間一般に知らせることでは必ずしもありません。そして情報を共有するだけではだめで、それを行動にどうやって繋げていくかです。

今日は残念ながらＪＰＣＥＲＴコーディネーションセンター専務理事の早貸（はやかし）淳子

さんはご都合で参加できませんでした。ですが、われわれの研究会の中では非常に大きな貢献をしてくださいました。ＪＰＣＥＲＴというのは、そのように皆さんが対応に困っていらっしゃるときに、何らかの助けをしてくださる非営利団体です。たとえば伊東さんの㈱ラックのような会社に「助けてください」と電話をかけることもあり得ますし、あるいはＪＰＣＥＲＴのようなところに対応をお願いすることもあると思います。

また、われわれはこの研究会の一つの目標として、あるいは政府も戦略に挙げている目標としては、情報セキュリティ産業をもっと強くしていきたい、もっと大きくしていきたいと思っています。そういう面で皆さんのご理解をいただき、情報共有を進めていっていただきたいと思います。

最後に今日私たちが提案したいのは、資料８のサイバーセキュリティ10箇条で、特に企業経営をされている皆さん方にお願いしたいと思います。サイバー攻撃はも

資料8 企業経営者のための サイバーセキュリティ10箇条

1. 狙われないようにする。
2. 専門家の話を聞く。
3. 過去の経験は役に立たない。
4. 情報セキュリティ投資は必要不可欠なコストである。
5. 守れない規則を強要するな。
6. 記録を取る。
7. 内部犯行の可能性を忘れない。
8. 事実関係を承知してから判断をする。
9. 対策の優先順位付けをする。
10. 情報を共有する。

う避けることができません。やられることを前提に、何か対応を取っていかなくてはいけないと思います。特にこの7番にあるように、内部の方々が対応を手伝うという犯行が行われた場合には、ほぼ間違いなくやられると考えたほうがよいと思います。ですから、そうなることを前提にしたセキュリティ対策を取っていかなくてはいけないのではないでしょうか。

これからパネルディスカッションの中でこれについても、あるいはその他の論点についても、深めていければと思っています。

パネルディスカッション

サイバーセキュリティ
――政府と企業が取り組むべき課題

【パネリスト】
内閣官房情報セキュリティセンター副センター長・内閣審議官　占部浩一郎
㈱イプシ・マーケティング研究所社長　野原佐和子
㈱ラック理事・サイバーセキュリティ研究所長　伊東　寛
慶應義塾大学総合政策学部准教授　加茂　具樹

【モデレータ】
世界平和研究所主任研究員　大澤　淳

大澤委員

大澤　本日モデレータを務めさせていただきます、公益財団法人世界平和研究所の大澤と申します。先ほど占部副センター長、土屋先生からご紹介がありました標的型攻撃が、最初に当研究所の研究員にまいりましたのが、当研究所の副会長から新年に届いたメールでした。「今年は年賀状をエクセルでつくってみた。開いてみてほしい」とあったのですが、全員、その91歳の副会長がコンピュータを使わないことがわかっていましたので、標的型攻撃だと気付いて対処ができました。その話が２００８年のことですから、かなり前から標的型攻撃がなされて

いたわけですが、社会での認知は２０１１年に新聞報道があってからということになります。

パネルディスカッションでは最初に㈱ラック理事でサイバーセキュリティ研究所長の伊東さんから、セキュリティ事業者からの視点ということでサイバー攻撃の現状についてお話しいただきます。

２番目に、慶應義塾大学の総合政策学部の准教授で、中国政治がご専門の加茂さんから、中国の政策も含めてお話しいただきます。特に中国で、実際に何が起きているのかということを伺います。

二つの事例の後、占部副センター長にコメントをいただき、最後に㈱イプシ・マーケティング研究所の野原佐和子さんから、企業経営者や利用者の視点ということで問題提起をしていただいて、ディスカッションを進めたいと思います。

伊東委員

日本を取り巻くサイバー攻撃の現状

伊東　私はラックという会社で、研究所の所長をしております。ラックはサイバーセキュリティ上の防御をアウトソーシングする会社です。宝石店を外部のガードマンが守るように、私たちは企業のシステムを外から守ることをしています。したがって、たくさんの攻撃の事例について承知する立場にあります。そういう具体的事例をここで申しあげて個別の話をすると非常にわかりやすいのですが、守秘義務があるので、それは禁じられています。そういうわけで、今日私がお話しすることにあまり具体性が

ないのではないかという点については、ご寛恕願いたいと思います。

併せてラックという会社に来る前、私は自衛隊に27年間勤務しました。その3分の1くらいは情報関係をやっていたため、そういう観点から物事を見る癖がついています。今日はサイバーセキュリティ会社社員と自衛隊出身者という観点を合わせて、報告をさせていただきたいと思います。

最初に、日本を取り巻いているサイバー攻撃の現状についてお話ししたいと思います。

日本を取り巻く大きな攻撃事件と言いますと、２０１１年９月に、大手防衛産業のサーバーにサイバースパイが侵入したという報道がありました。この方たちが特段に油断をしていたということではありません。実はたくさんの攻撃が日本に対してなされています。はっきり言って、こういう事件は氷山の一角です。

なぜこうなってしまうかというのを先に言えば、結局人間的な問題なのです。攻

撃をされていること自体、まずわかっていない企業がたくさんあります。

次に、それはわかっても担当者の方がそのことを上司に報告しないケースが、ないとは言えません。それを正直に言うと「お前がボヤボヤしているからだめになった」と怒られるかもしれません。だから、黙って自分で処置してしまう。この誘惑はとても大きいので、よくわかります。私自身が、実はそういう目にあったことがあるのです。

それは、私自身ラックというセキュリティの会社の研究所長でいながら、私のパソコンに怪しげなファイル等が入っていたのを自分で発見した時のことです。いろいろと深いところを見ていたらマルウェアが入っていたのです。幸い、これらはウィンドウズ用のウイルスであり、私はマックユーザーだったのでこれらのウイルスが発症することはありませんでした。ともかくマルウェアが私のパソコンの中に入っていたのですから、正直言って迷いました。自分のスキルをもってすれば、この

マルウェアを消してしまい、なかったことにできるわけです。だけどそれはだめなのです。やはりしかるべき報告をしました。そして、予期した通り、思い切り皆にばかにされたあげく、1時間の事情聴取を受けまして、本当に参ったなと思いました。でも正しいことをしたと考えて自分を慰めています。

次に会社の担当者が正直に上に報告したとしましょう。この時上の人が事の重大さがわからない場合があります。「どうだったのか」「こうなったのですが、私が処置しましたのでご安心を」「よかったね、ありがとう」。これではこの事例が何の警告にもならず終わってしまいます。

一番ありそうなのは、さっき土屋先生もおっしゃっていましたが、偉い方がそれを聞いて、事の重大性が真にわかった場合です。公表すれば会社の信用が下がり、株価が下がります。「大変なことだ。これは絶対に言ってはいかんぞ」というわけです。

このようなわけで、企業がサイバー攻撃を受け、情報が漏れたとしても、なかなか新聞の一面で大きく報道されることがありません。しかし実際は、皆さんが思う以上にたくさんの攻撃がなされています。

さて、もう一つ有名な事件といえば、２０１２年８月に起きた遠隔操作ウイルス事件です。私は、これもなかなか21世紀的でこれからのインターネットの不安全性に対する象徴的な事件だと思っています。

この事件のウイルスですが、私たちの研究所でも入手して中を見ました。担当した研究員に、このウイルスの特性を一言で言えといったら、彼はこう言いました。「つくりが雑です」。これは何を意味するのでしょうか。

昔はハッカーとかスーパーハッカーという人たちが、自分のスキルを自慢するためにウイルスをつくっていました。だからある種の美学があったのです。ソフトウエアをつくるプログラムに美しさがあったり、揃え方に癖があったり。その点、遠

隔操作ウイルス事件の場合は、動けばよいというソフトウエアでした。

これは逆に言うと怖いことです。いまは一般の人でもちょっとその気になって勉強すると、インターネット上に悪いことをするための知識がいっぱいあり、この犯人はそれを利用できたということになるのです。

というわけで、最初の私の話をまとめますと、報道の陰にはもっともっとたくさんのサイバー攻撃・サイバー事件があるということです。サイバー攻撃の被害にあうのは他人事ではなく、また、皆さんも加害者になる可能性があるし、これからお話しするもっと大きな危険も存在します。

懸念されるもっと大きな危険

伊東　最近韓国でサイバー攻撃事件が大騒ぎになったのを見て、皆さんもびっくりしたと思います。それでは日本はこういうことはないのかというと、そうではあり

ません。実は皆さんもその気になって新聞をよく読んでいると、某銀行のシステムダウンとか、大手交通機関のシステムエラーとか、新幹線が麻痺したとか、飛行場トラブルなどが出ているのです。ただそれが大騒ぎになっていないから皆さんの関心を引いていないだけで、実はたくさんの原因不明のシステム事故が起こっています。

さて、昔ソビエト連邦が元気いっぱいだった時代に、私は自衛官だったわけですが、その当時定期的にソビエトの爆撃機が日本に向けて飛んできていました。これは「東京急行」と呼ばれていました。ソビエトの飛行機が飛んでくると、航空自衛隊のレーダーがそれをつかまえてレーダーで照射します。彼らはその電波を受信して、そのレーダーの電波の特性を記録していたのです。これは、もし日本とソビエトが戦争になったときに、日本のレーダーに電波的な目つぶしをかけるために必要な技術情報だったのです。これを定期的に丹念に取っていれば、日本側がレーダー

を新しい機械に替えたときも、新しい情報として手に入ります。

ではソビエト軍というのは、そういう人の秘密を盗む悪い人たちなのでしょうか。そうではないのです。普通、軍隊というのは、平時には戦争に備えて相手の弱点を調べます。実は私自身が陸上自衛隊の陸幕調査部にいたときにやっていた仕事の一部は、そういうことでした。

ここで私が言いたいのは、こういうことです。いま、たくさんの得体の知れないシステム事故が報道されている――それはすべて人間系の故障、ハードの故障として片付けられていますが、本当に全部がそうなのでしょうか。もしかすると故障に見せかけられているかもしれないけれども、「サイバー上の東京急行」が混じっているのではないでしょうか。これは、私がいま持っている危惧です。証明することはできないのですが、あってもおかしくありません。

そうだとするといま、日常的に日本にサイバー攻撃が行われています。そして、

以前のように目に見えるものが減っています。昔はいたずらだったので、すぐにわかりました。いまは犯罪者の金銭目的、あるいは、もしかすると外国が日本の弱点を調べているような情報収集活動です。企業の技術を盗むことが多発している一方で、国の弱点や、電力システムや交通システム、通信システムなど社会のインフラの弱点を探るための攻撃が行われているのではないかというのが私の懸念です。

サイバー攻撃の具体的事例

伊東　具体的事例について簡単にご説明します。そもそもサイバー攻撃について、普通皆さんが思っているのは、「情報を取ること」そして「業務を妨害すること」の二つです。そしてもう一つ、私が付け加えたいのが、もしかすると将来の攻撃を考えた準備活動としてのサイバー攻撃です。これは先ほどご説明した「サイバー上の東京急行」です。

その他に自己主張である「アノニマス型」のサイバー攻撃もあります。それからテロ。そして将来は本当にもしかするとサイバー攻撃は、戦争そのものになるかもしれません。

さて、犯罪についても、以前よりも大変なことがたくさん起こっています。昔、ID・パスワードを盗むのはキーボードの動きを監視していてこっそりそれを記録するなど単純な手口だったのですが、いまは、悪いアイデアが数限りなくあります。たとえばインターネットバンキングで振り込むときに、ある特別なマルウェアに感染していると、ほとんどの手続きは全部うまくいくのですが、最後の「OK」を押した瞬間に送金する先の口座が犯人の口座に書き換えられたりします。そういうものがバーッと撒かれると、攻撃者にはお金がたくさん入るわけです。その他にも株価操作とか、いろいろなものが考えられています。悪人の金儲けのアイデアには限りがないわけです。

現在、私が一番危ないと思っているのが標的型攻撃です。標的型攻撃につきましては土屋先生からご説明がありましたのでここでは省略します。

あと皆さんに関心を持っていただきたいのは、産業用制御システムの安全性に対する攻撃です。このようなシステムの特徴は、動けばもうそれ以上触らないほうがよいということです。古い、たとえばＰＣ98でシステムを組んだ後で完全にバグが取れて稼働していれば、そこにパッチを当てるなどというのはとんでもない話です。かえってバグが入るかもしれません。だからそのままでやっている。しかもクローズしているので、アンチウイルスソフトを入れたいという予算要求をかけたとしてもなかなか認められません。当たり前ですね。繋がっていないから安全だと思っているわけです。

ところがそういうものが往々にして外のインターネットに繋がっているという結果が出ています。これは案外、偉い人が知らないことなのです。

私がもしある工場のシステムの管理者だとします。システムに何か万が一起こったとしても、夜中の3時に電話がかかってきてタクシーを飛ばして工場に行ってシステムを見るのは、やはりしんどいです。できればそのシステムをインターネットで繋いでおいて、自分の家からリモートで中を見られるようにすると、情報が早くわかるし、対策もすぐ打てます。そう思い、クローズしているはずのシステムを勝手にインターネットと繋いでおこうという誘惑にかられるのは当然のことです。そういうことをもしかすると本当にしている人がいるかもしれません。

しかし、そういう方がいると、もう問題です。外と繋がっていないはずだからアンチウイルスソフトも入っていないし、OSのバージョンは古いままで脆弱性だらけ。でも外から叩くと見えてしまうのです。実際に2007年の経済産業省の調査では36・8%が外部ネットワークに接続しています（資料9参照）。この危険性については経産省が対策を打ち始めています。

資料９ 産業用制御システムの安全性

- 2009年の経済産業省調査によれば
  - 国内にある234のシステム（サンプル）のうち
  - 36.8％は外部ネットワークに接続
  - そのうちの約55％はリモートメンテナンス用
  - 約43％はインターネットで繋がっていた
  - 設備で使われているOSの88.9％がWindows
    （おそらく古いバージョン）

それにもかかわらず、その危険性は
あまり認識されていない。

また、物流関係にもリスクがあります。いまアメリカですごく問題になっているのがシスコシステムズのルーター（コンピュータ・ネットワークの制御装置）の偽造品です。私も見ましたが、どっちが本物でどっちが偽物だかさっぱりわかりません。このような巧妙な偽物が出ていて、単純に品質の悪い安物というだけであればメーカーが大迷惑をするだけで終わるかもしれないのですが、実はこういうものに意図的に悪いものを入れているという噂が出ています。この危険性はサプライチェーンリスクと呼ばれています。

ありがちな五つの罠

伊東　サイバー攻撃の中には、たぶん日本の弱点を調べるような国家的なレベルの攻撃が行われている。攻撃され、守っているのは企業の皆さんなのです。これはアンバランスだと思います。やはり国が何かしっかりとした対策を取らねばなりません。

　このようなたくさんの攻撃がある中で、土屋先生がおっしゃったように「私は関係ない」というのはあり得ません。本当のターゲットを狙うために、その踏み台として、一歩手前として脇の甘い偉い人を狙ったりすることもあり得るからです。皆さん個人や組織が狙われている可能性があると思います。

　最後に教訓事項として、ありがちな五つの罠を挙げたいと思います。

　一つ目は「システムの構築」についてです。一般的には動くことが優先され、使い勝手が良いことがその次、セキュリティにはお金や時間が回らないことが多い。

二つ目は「システムの運用」についてです。外部システムと繋がっていないと思われているものでも、案外繋がっていることがあります。そして繋がっていないと思われるために、アンチウイルスソフトを入れていないとか、しかるべき対策が取られていないことが散見されます。

三つ目は「システムの更新」。一度安定して動いてしまうと、更新するのにすごく勇気がいります。お金と手間暇がかかるからです。数年前の話ですが、まだウィンドウズ98を使っているところがありました。ウィンドウズ98には脆弱性がいっぱいあることがわかっていますので、これは由々しき大問題です。

四つ目が「規則」。守れないような規則は、絵に描いた餅。陰で楽をしようとするのが人間です。

最後に「システム事故の発生時」です。さっき言った人間的な理由から報告が上がらない場合があります。上げても上司がその重要性を理解できない場合がありま

すし、理解できても隠そうとする上級役員もいる。そうした上級役員がいてはいけないから、土屋先生がさっきおっしゃった勇気を持って情報共有する仕組みが必要だと、私も考えています。結局、最大の弱点は人間だということです。

終わりにサイバー攻撃に関する現状は、攻撃者や犯罪者が優位であって、今後、より有効な防御技術・対策が必要だと考えています。

大澤　伊東さんの報告の最初にあった、サイバーのインシデントを発見した場合の隠蔽。それをどうわれわれは情報共有していくのかというのは一つの論点です。後ほどディスカッションしていきたいと思います。

それから二つ目、サイバー攻撃の可能性もあるシステム事故が最近増えてきている点です。私もそうですし、安全保障を専門にしておりますと、実はこの3～4年、国と国の対立という安全保障環境の悪化が、こういったサイバー攻撃に結びつく事例がいくつか散見されております。われわれの報告書の中にも、サウジアラビ

アのサウジアラムコの事例とコカ・コーラの事例があります。前者のサウジアラムコの事例は、西側とイランの対立という安全保障上の背景から出てきたものです。後者のほうは純粋に企業に対する情報の窃取を狙った攻撃です。

そういった企業に対する攻撃としては、今年1月30日、ニューヨーク・タイムズが自社のネットワークが中国から攻撃を受けていたと発表しました。アメリカでは中国が悪いのではないかという論調が非常に多く、日本でも中国からではないかという報道が見られます。しかし逆に中国自身は、われわれは非常に被害を受けている、他国から攻撃されていると主張しております。その辺の中国国内の事情について、次に加茂さんからお話をいただければと思います。

サイバー攻撃「中国犯人説」だけでいいのか

加茂　私は国際関係や安全保障の専門ではなく政治学が専門です。

国際社会の中において中国がサイバー攻撃をしているという、中国犯人説がたくさんあります。私自身はこの分野についてはそれほど詳しくはないけれども、確かにそういう部分もあるとは思っていました。ただ一方で、主語を全部「中国」とするところに、少し違和感を抱いています。一体、中国の中でどんなことが起きているのかを少し勉強してみたい。その観点からこのプロジェクトに貢献することができるのではないかと考えて活動してきました。

土屋先生のご報告の中でも出てきましたが、2月18日のニューヨーク・タイムズの中でマンディアント社の報告を引用して、「中国がこのビルから攻撃をしている」という記事がありました。私は台湾で今学期だけ授業をしているのですが、実は台湾も中国から非常に多くの攻撃を受けているということを、国家安全局の局長が台湾の立法会で報告をして、台湾メディアの中でも非常に多く報道されていました。台湾と中国は事実上、戦争状態にあるわけだから、当然そういう攻撃があっ

加茂委員

て、それについて台湾企業あるいは台湾、中華民国が非常に対応に迫られているのだと感じました。

では、こういう報道などに中国がどういう反応したのかは、多くの媒体で確認できます。中国の外交部（外務省）や国防部（国防省）のスポークスマンは、「サイバー攻撃というのはグローバルな問題であって、相互の信頼と相互の尊重の基礎の上に建設的に解決しなければいけないのだ」「これに関する根拠のない無責任な批判は問題の解決にはならない」と言った上で、「中国はサイバー攻撃の攻撃者ではなく被

害者なのだ」という主張を繰り返すわけです。

攻撃者なのか被害者なのか、そのどちらが真実なのかはわからないにしても、その被害者とはどういうことなのだろうかというのを探ってみようというわけです。

ネット空間における実名制徹底を求める中国の動き

加茂　２０１２年12月28日に、中国の国会に相当する全国人民代表大会でインターネット情報の保護強化に関する決定がなされました。なぜこのタイミングなのか、どうしてこれを決定しなければいけないのでしょうか。

これに関する日本の報道、世界の報道は一点に集約されています。この決定の第６項に「ネット環境を提供する業者は利用者のＩＤをきちんと確認しなければいけない」ということを盛り込んでいます。この観点から「中国は言論の自由がない」、つまり言論を統制するためにこの法律をつくったのだと捉えています。

資料10 中国の実名制に関する法制定の取り組み

- 2002年11月15日：「インターネットサービスを提供する空間における管理条例」
- 2004年12月28日：「高等教育機関のキャンパスネットワークの管理の強化に関する意見」（国家教育部）
- 2010年9月1日：工業情報化部の通達にもとづき、携帯電話の購入に際しての実名制を実施。
- 2011年12月：北京、上海、天津、広州、深圳の5都市において微博（マイクロ・ウェブ）を利用する際に実名制を導入。
- 2012年12月28日：全国人民代表大会常務委員会、「インターネット情報の保護強化に関する決定」を採択。

確かにいま、中国がネット空間において体制を批判する言論が起き、またネットを介してデモ活動が組織されて、それが体制にとって非常に脅威になってきています。それに対して国家安全の部門がしきりに強いコントロールをしているという文脈の中で、この法律をわれわれ外国人は理解するわけです。

しかし、本当にそれだけなのかと考えて、もう少し歴史をさかのぼって考えてみます。資料10は中国の実名制という問題に関しての法律の制定の取り組みです。私は昔、中国に留学して携帯電話を買ったときに全然ＩＤのチェックがなかったので、自由な

んだな、この辺は結構いい加減だなと思った覚えがあります。それがほぼ10年前から少しずつ条例をつくったり、意見を出したり、通達を出して携帯電話の購入に対して実名制を実施する動きが出ています。２０１１年12月には一部の都市において、中国のツイッターに相当する微博（ウェイボー）を利用する際に実名制を導入して、この辺から中国の言論統制が強化されているという話が流布されるようになります。

一面はそうなのでしょうけれども、もうちょっと考えてみる必要性があります。ここから先は政治学の発想になります。中国を含めてあらゆる非民主主義国家、それは当然、北朝鮮も含めますが、その９割以上に議会があります。独裁国家、非民主国家において、政党を組織していて議会があって、なぜそんなコストのかかる面倒くさいものをつくるのかというのが、政治学の分野においては非常に大きなイシューになります。

非民主国家がなぜ、なかなか壊れないのか――壊れない理由は、実は支配者は議会を使って社会の諸問題を集約している。社会にどんな問題が起きて、どんな疑問、不満があるのかというのを、こういう議会を通じて吸収している。だから独裁者、非民主主義国家の支配者は、体制の安定あるいは社会の変化に柔軟に適応できるのだという理解がなされています。

その観点から、私は中国の議会がどんなことを話しているのか、どんな問題を支配者・共産党は把握しているのかというところに注目して、調べてみました。今回はサイバーセキュリティの観点からこういった議会の中でどんなことが議論されているのかを、ここ1年詳細に観察してきました。

そこから明らかになったことは、非常にたくさんの情報セキュリティ、サイバー空間の安全の問題に関する意見や議論が議案として出ていることです。つまりこの議案の目標は、要するに共産党にこれをしっかりと考えてくださいという提案なわ

けです。そうすると、なぜこんな問題が出てくるのか、誰が出すのかというところが重要になってきます。

この議案を「出す人たち」というのは、中国国内における電気通信業界のトップや、民営企業の社長など、中国における経済活動の中で利益を得て、繁栄を享受している人たちです。彼らが議員になり、たくさん議案を出している。それが、年々増えてきています。その中で彼らが出す一つの重要な提案とは、「実名制をもっと徹底しなければならない」ということになるわけです。

経済活動をするのになぜ実名制が必要なのかと考えて、彼らの発言、メディアに出てくるものや、彼らが出す提案をつぶさに読んでいくと、一点に集約されます。経済活動の中で利益を享受する意味において、ネット空間の安全が保てないと自分が経済活動をできない。なおかつ外国の企業は、ネット空間の安全が保たれなければ中国に入ってこない。つまり中国の市場の環境が悪化する、あるいは荒れている

中に外国の企業が入ってくるわけがないではないか。だから情報に関する安定性を維持するために情報セキュリティ、つまり実名制が必要だというわけです。

中国のネット空間は非常に荒れた環境

加茂　ではどんな問題が起きているのでしょうか。中国でも当然、アマゾンのようなネットビジネスが非常に盛んであって、ネットを通じて物を買うということがはやっています。「インターネット情報の保護強化に関する決定」ができる1年前、その業界の中の有名どころのほとんどすべてに近いところで情報のデータが盗まれ、銀行のアカウントからパスワードから抜かれて、非常に大きな問題になってきたことが報道されています。このことは中国の百度（バイドゥ）、日本でいうとグーグルに相当するものがあるのですが、そこに非常につぶさに書いてあって、なるほどと思いました。こういうネット環境が不安定な中で、中国自身が問題にさらさ

れています。

もちろん中国自身は、中国が攻撃者だということを、公式の中では批判しますが、「適切な情報を収集する活動を行っているけれども、それがアタックだと認知されるかもしれない」という文脈での発言はあります。

一方で、「同時に中国は被害者だ」というのは、まさにその被害を指します。中国の体制のウェブサイトが容易に書き換えられるとか、いろいろな報道があります。つまり中国は非民主主義国家であるがゆえに、体制をひっくり返したい、民主化したいという勢力との間の対立もあるし、またビジネスをする中で相手の企業から情報を盗みたいという欲求にかられて、こういう情報セキュリティの問題が発生してくると思われます。われわれ外国人が「中国けしからん」「攻撃者だ」という文脈で中国を見るだけでは、もう一つの重要な視点を見落としてしまっているのではないかと感じるのです。

中国の議会の中でこういう議案が出てくるのは、本当に深刻な問題を議案として出すわけですので、やはり中国のネット空間は誰が誰を攻撃しているのか、誰が誰による被害者なのかは抜きにしても、われわれが理解する以上に非常に厳しい荒れた環境であることを示唆しているのではないかと思います。

中国に進出する、あるいはビジネスをするということにおいては、あの地のネット空間に非常に注意して接触しなければいけない。中国がどこそこを攻撃するという発想よりも、中国のネット空間が極めて難しい問題を抱えていることを常に理解しておかなければいけないと感じました。

大澤　中国は実名制を導入したということで、あれだけ監視社会ですので、インターネットも全部監視されているのかと思ったら、実はそうでもなさそうだなというところもあります。中国の情報ネットワーク自体もかなりセキュリティ上の問題を抱えているということです。おそらく中国以外の国が抱えている問題と同じような

問題を抱えているのだろう、そういうところに話し合いの土壌が将来的にはあるという感じがします。

経済学的、社会科学的なアプローチが不可欠

大澤　お二人のお話を伺ったところで、占部審議官から中国の情報の問題、それから情報共有の問題等をコメントをいただければと思います。

占部　いろいろとお話を伺って、非常に難しい問題だなと再認識しました。先ほどグローバルな話は飛ばし気味に説明しましたが、国際的な連携はいろいろなところでなされています。一番大きいものでいうと、サイバー空間に関する国際会議みたいなものがここ2年間くらい開催されていて、第1回目が一昨年、ロンドンでした。去年の11月にハンガリーでありました。今年は10月にソウルでそういう会議があります。

一方、国連でどのような取り扱いをするのかという議論があります。でもなかなか決着がつきません。大きく言うと、欧米グループと、中国やロシアという二つのグループがあって、前者はインターネットの開放性や相互運用性、つまり情報の自由な流通が大事だという意見です。後者はきちんとネットにも主権を及ぼした上で、その中を国がしっかりと管理するという意見です。

それとは別に、ブダペスト条約（サイバー犯罪条約）というものがあって、「サイバー犯罪があったらきちんと取り締まり、協力しましょう」というものです。日本はやっと昨年、批准して発効しましたが、中国などは入っていないことが問題になっています。

日本は、昨年政策会議で決めた言葉で言うと、「過度な規制を行わなくて自由な流通を確保するようなサイバー空間が大事」だと考えています。インターネットは先ほどお話ししたように発達してきたのですが、いま、それをきちんと使いこなす

のがものすごく大事です。したがって情報がしっかりと自由に流れる空間をつくらなければならない。自由に流すといっても、ポロポロと穴が開いていてこぼれ落ちるのでは困るので、それは強靭なものでなければなりません。だから自由なものを守るために当然リスクに対応したものをやっていかなければいけないということで構築しているわけです。

最初にも言いましたが、いろいろなところで意見の違いがあります。たとえば会社の中では「こういうものを守るのにお金をかけるのか」「いや、そんなものにはお金はかけられない」。人材を雇うにしたって「そんなセキュリティ人材を雇っているよりは、きちんと物をつくる人を雇ったほうがよほどいいじゃないか。工場に投資しろ」。そんなふうに諸々のところですべてが対立します。絶えず「何とかvs何とか」ということを考えなければいけないのです。

われわれは、その「何とかvs何とか」というのを、同じ目的地に向くような、対

立概念ではないところで片付けられないかということを絶えず考えています。たとえばあちらこちらでサーバーをつくるのではなく、1個つくって穴をふさいだほうがよほど安全ではないか。おそらくもう少し知恵を出せば、もう一段上のセキュリティが考えられるのではないか。この辺をしっかりと考えていくのです。

その中で大きな要素が、これまでわれわれは情報セキュリティと言いながらも、システムに着目しすぎて、技術の問題だとあまりにも思いすぎたのではないかと考えています。さっきの標的型攻撃など、まさに真理を突いているようなものです。そういう意味で、もっと経済学的、社会科学的なアプローチをしていかないと、解決できないのではないでしょうか。

一体どれだけのリスクがあって、どれだけのことをやれば、どう合理的に防げるかとか、これを防ぐためのモチベーションをどう持たせなければいけないかとか、そういう全体のことを考えなければいけません。それを各社皆でやる中で考えるに

は、まさに経営判断を伴ったような判断をしていかないといけません。

もちろん、国だってそうです。実は各省にもCISO（最高情報セキュリティ責任者）を置いていて、だいたい官房長などがなっています。ではその人が本当に、このシステム、情報セキュリティ、これはどうなんだと言ってわかるかというと、わからないのです。それが変わることはあるのかもしれないけれども、それを変えるには非常に時間もかかります。

だったらわれわれから言うと、そういうトップに近い人にわかってほしいのは、「システムの守り方はお任せください」、でも、「どれを守るか」「何が一番大切か」――これはあなたがきちんと判断してください。「これは何があっても守りきれ」「最後はしょうがない」「これはまあ、いい。俺が謝っておくから」。そのくらいのメリハリをつけてやっていかないとだめではないかと考えています。だからといって、いい加減でいいと言っているわけではありません。

そういう社会学的、経済学的、ステレオタイプに言うと文科系的発想をしっかりと持ってやらないと、おそらく技術屋さんだって参ってしまうだろうし、実はうまくいかないと考えています。そういう意味で、価値観なり何なり、投資であるかコストであるかでなく、投資であり、かつコストであり、会社の成長の源泉であると言ってやっていければと考えています。

希望的にいつも申しあげているのは、日本は物づくりで生きてきて、自動車だって何だって日本の製品は安いし安全だし、これさえ買っておけば安心していられる。日本に来て商売をすると、非常にきれいな空間があって、自由な情報の流通もあって安心してできる。そういう「Made in Japan」と並ぶ、「Secured by Japan」のような、日本品質のセキュリティをしっかりとつくっていく。それが結局、サイバーセキュリティ立国になると思うのです。そのようなアプローチをして日本が今後成長していく絵を描けたらと考えているところです。

大澤　ありがとうございます。サイバーセキュリティ立国の肝を発表前にお伺いして、得した気分になっております。

セキュリティ対策のバランスを図る

大澤　今日、会場には会社の経営に実際にかかわっておられる方や、総務や情報システムの方が来られていますので、野原さんから、企業経営者の立場で若干お話をいただきたいと思います。

野原　私は情報セキュリティ政策会議に２００５年からメンバーとして入っていますが、決してサイバーセキュリティの専門家というわけではなくて、日ごろはシンクタンクとしてインターネットビジネスやＩＴビジネスに関する調査や事業戦略コンサルを行う立場です。サイバーセキュリティをテーマとして調査をすることはありますが、決してそれが私の専門というわけではありません。専門ではない者が政

策会議に入っていることの意味を出したいと思いながら政策会議に入っています。今回、21世紀政策研究所での研究会でも、皆さんからいろいろな情報をいただいて勉強するとともに、バランサーの役目を果たせればと思ってやってきました。

というのも、サイバーセキュリティは特にそうだと思うのですが、専門の方々が集まってラウンドテーブルを囲んでどうしたらよいかという議論が始まると、どんどんセキュリティを高めることのほうに議論が行ってしまいます。ふと考えると、なぜそんなことまでやらなければいけないのだろうとか、あるいは先ほどからバランスの話が出ていますが、コスト的に全然成り立たない話であったり、できそうにもない人材を要求するような話であったり、あるいは利便性や自由が失われるような意見がどんどん出てきて、それを否定できなくなっていくという部分があります。

今日、皆さんからいただいた話はすべて真実だと思いますし、重要な論点だと思

野原委員

うのですが、サイバーセキュリティ対策に対して重要なことはもう一つ、それだけに集中してフォーカスして考えてしまうよりも、いろいろな情報を自由にやり取りするとか、利便性だとか、生産性のことだとか、あるいはコストのことだとか、日ごろから実現しなければいけないこととのバランスがすごく重要だということを、忘れてはいけないと思っています。

ゼロデイ攻撃と具体的対応策

野原　まず今日のディスカッション・ポイントとして、来ていただいている方々に議論を投げ

かけられたらと思っている点が4点あります。それをお話しする前提には、他の皆さんもさんざんおっしゃっているサイバーセキュリティ事象の深刻化・甚大化があるわけですが、一番重要なのは、私は資料11（96ページ）の上の枠の4番目に書いてある変化だと思っています。

ざっくりと言えば、これまではゼロデイ攻撃というのは主にアメリカで起こることが多くて、日本はアメリカでなされる対策や体制をフォローしていけば、それで十分間に合ったというところがあったと思うのです。それだけインターネットはアメリカ中心で形成されてきましたし、政治的にもアメリカは大きな役割を担っていますから、狙われることが多かったのに対し、日本がメインになって狙われることは多くはなかったと思います。

でも最近の政治的な日中関係、北朝鮮との関係もありますし、いろいろなセキュリティ攻撃の質の変化も相まって、結果的に日本が直接ゼロデイ攻撃を受けること

資料 11　4つのディスカッション・ポイント

□サイバー・セキュリティ事象の深刻化・甚大化

- ➢標的型メール攻撃
- ➢スタックスネット等、制御システムを攻撃
- ➢通常兵器と組み合わせたサイバー攻撃
- ➢ゼロデイ攻撃は米国で。対策は米国をフォロー⇒日本がゼロデイ攻撃を受ける

■“リスクベース” でのセキュリティ対策で、生産性・利便性とのバランスを
■攻撃を受けたとき、速やかにインシデント情報を共有するルール・体制・気運・常識を構築
■セキュリティ人材の育成・採用・キャリアパス形成
■セキュリティ関連産業創出の迅速化策

が結構あるという話になってきました。そこが一番大きな違いで、これまでのセキュリティ戦略や計画とフェーズを変えなければいけない――次元が変わったと皆さんは言われているのですが、その一番の肝はそこなのではないかと私は思っています。

ゼロデイ攻撃というのは、今までどこにもやられていなかった攻撃をハッカーが仕掛けてくることなので、今までの事例を基に何らかの対策を打つことが、できないということです。そのような状況に、これからは日本の企業各社が本格的に立ち向かわなければいけ

なくなっていることが重要な論点だと思います。

資料11の下の枠に挙げている四つは、わりと具体的な話です。まず第1に〝リスクベース〟でのセキュリティ対策で、生産性・利便性とのバランスを取らなくてはいけません。これは冒頭で申しあげたバランスが重要ということに直結します。

たとえばビジネス環境全体に、リスクベースではなくて一律の高いセキュリティ対策が施されることは多いと思うのです。なんだかんだと言って、セキュリティは低いより高いほうがよいのではないか、社員の方々のPC環境を一律バーッと一緒にしてしまえということについついなりがちで、なかなか適材適所なセキュリティ対策を打つことは難しいのではないかと思います。でも実際には部署ごとだとか、事業所ごととか、業務の内容ごと、あるいはその立場によってリスクは違うわけで、それをリスクベースにどうやって実現していくのかということを、考えないといけないようになってきていると思います。

ところが、実際にはシステム全体を一気にデザインして更改することはほとんどないわけで、部分的な更改のたびにちょっとずつ、その都度セキュリティ対策をそこへ織り込んでいかなければいけないわけで、必ずしも毎回正しく判断するのは容易なことではないと思います。

あるシステムを更改する際に、ベンダーの方がA案とB案があって、「A案がいいですよ」と提案されてきます。どうしてかというと、「そのほうが、セキュリティが高いですから」と言うと、「そうか」と皆さん思うわけです。本当はその一言のために、どれくらいのセキュリティが確保されていて、その引き換えに、逆に利便性が損なわれることは本当にどれくらいあるのか、コスト的にはどう違うのか、生産性に対してはどういう変化が起きるのか、そこだけのセキュリティを高めることが全体の系の中でどういう意味があるのかといったことを常にチェックしながら、その一言を解釈していかなければいけない。そういう意味で、非常に難しい

ことではあるのですが、常にリスクベースでのセキュリティ対策をいろいろな項目とのバランスを取って実現していくことが重要だと思います。それをどうしていったらよいのか考えたいというのが1点目です。

2点目は、攻撃を受けたとき、速やかにインシデント情報を共有するルール、体制、気運、常識をつくっていかなければいけません。今回、研究会でつくった報告書の冒頭の最悪のシナリオを読まれると、たぶんここにおられる経営層の皆さんはドキッとするのではないかと思います。どんなに一生懸命いろいろな環境を整えていても、サイバー攻撃を受けて被害にあうことがあり得ます。もしそういうことになった場合に、本当に適切に速やかに公表すべきところへ、共有すべきところへインシデント情報を共有できるのかということが重要な課題だと思います。

そのときになって考えるというのはなかなか難しい話で、日ごろからそれをどうするのかをルール化する、そうしたときにどうするか体制を考えるとともに、隠さ

ないできちんと必要な情報を必要な範囲内で共有することを業界の中での常識にしていくことが重要なのではないかと思います。

その意味で、今回の報告書はぜひいろいろな業界の方々に読んでいただきたいと思います。それを基に、関係する業界の方々で、お酒でも飲みながら、食事をしながら、お茶を飲みながら、あるいはミーティングの中ででも、話をしていただければ何か始まるのかなという気がします。また、単なる気運だけではなく、もっときちんと体制をつくることもやっていかなければいけないと思います。

そして3点目は、セキュリティ人材の育成、採用、キャリアパスの形成が非常に遅れていて、これをなんとかしなくてはいけないということです。これはあまりにも大きな話ですし、皆さん、問題の所在はわかっていらっしゃると思うのです。一点だけ例で挙げたいと思います。

実は大学でも、セキュリティの専門人材が足りないと言われていて、いくつかの

大学の中では少しずつそういうものが充実されようとしています。一方で企業でも現場にはセキュリティ専門人材が足りないという認識があって、必要であれば何年かに一度か、あるいは毎年、規模によると思うのですが、「人材を採ろう」という気持ちもあったりします。ところが新卒を採用するときの動きになると、そこが断絶されてしまうことが多いのです。

大手企業の人事部門の中で、「今年は何百人採る」という話があったときに、その中にセキュリティ人材確保のプランがある会社がどれだけあるのでしょうか。ほとんどないのが実態

だと伺っています。なので、大学側がセキュリティ人材を育成してきていても、それがいろいろな業界のセキュリティ部門にうまく繋がっていないという状況があります。卒業する学部生や院生のところに、一般企業のセキュリティ人材を欲しがっている人が行けていない――そういう採用ルートについても、まだまだ充実させていく必要があります。当然、採用した後のキャリアパスの形成も重要ですし、同じ企業でずっと専門でやるとは限りませんので、その中で人材が流動的に動きながら、でもキャリアアップしていける仕組みもつくっていく必要があると思います。

最後はセキュリティ関連の産業創出を迅速に進めるにはどうしたらよいのかという話です。これは非常に難しい話だと思うのですが、実は今回の報告書の中にも一つ例が出ています。

アメリカの場合には、国がファンドをつくってセキュリティ関連のベンチャーに計画的に投資しています。それは5社であったり、10社であったり、20社であった

りという数なのですが、国が投資をするとその10倍の出資が民間から集まるという関係があるので、国が目利きをして、いくつかの企業に投資をすることで産業創出を加速することができているという例が出ています。

この話をすると、日本では「だけど、そんな官製ファンドがうまくいったためしがないじゃないか」という話もあったりして、そのまま直輸入はできないと思います。でも少なくとも米国ではそのような工夫をしてセキュリティ産業の創出を早めようという動きが既にあるわけで、では日本らしくやるにはどうしたらよいのか、日本もそれに代わる方法を考えていくことが産業界としても重要なのではないかと思います。

大澤　野原さん、問題提起ありがとうございます。セキュリティリスクをどうリスクとして捉えるか。それから情報共有の仕組みをどうしていったらよいのか。セキ

ュリティ人材の育成を会社内でどのように考えたらよいのか。それから国としてセキュリティ関連企業の創出をどうやって考えるのか。というところで、一番下のほうから論点を議論していきたいと思います。

占部審議官に、セキュリティ関連産業の創出という点では、国の政策としてはどういうことをお考えなのか、お話をいただければと思います。

セキュリティ産業の創出

占部　公式答弁をすると、「研究開発プログラムをつくっています」とか、そういう答えになるのですが、さっき野原さんがおっしゃった官製ファンドについて、実は私自身の経験の中でも官製ファンドに色濃くかかわっていたことがあります。国が10を出したら民間が１００を出してくると考えたときに、なぜうまくいっているのかを考えてみると、きっと国がほしい技術がまず先にあって、たぶんそれを実装

してくれる会社を見つけてきて、そこに国が10を出して民間が90か１００を出しているのではないかと思います。

そういう意味では、国自身、特に防衛省や警察もあるかもしれませんが、実はわれわれがほしいものがあって、それを実装してくれるところを何社かファンディングするということをやっていかなければいけないのかなとは考えています。ただその一方で、さんざん「随意契約はいけない」とか、「競争入札にしろ」とか、「ＷＴＯがどうしたこうした」とか、手足をがんじがらめに縛られていて、このくびきをどう解くかと悩んでいます。これは非常に正直なところで、政府の公式見解とは言えません。

でも、セキュリティはそれなりに求められているのですから、まさにデマンドを、「こういうものがあったらいいよね」と出してファンディングするのは、茫漠たる投資よりは可能性が高い。もうちょっとスペシフィックに技術を捉えて、ぜひ

「日本の若人諸君、これをつくってくれ」ということを、本当はすべきではないかと考えています。

大澤　ありがとうございます。アメリカの情報セキュリティ産業の育成を調べましたときに、政府、たとえば軍の情報関係の人間が、ちょうど伊東さんのように、政府を出られて産業を立ち上げられたりしている例が結構見受けられるのです。そういった点では、人材育成の話と産業育成の話はかなり密接に関わる話なのかなと考えております。

後ろから2番目の人材育成のほうに移ります。伊東さんのところではセキュリティを担う人材を長年育成されてきていると思うのですが、何かコツはあるのでしょうか。ハッカー選手権とかでハッカーを雇ってくれば企業防衛ができるのではないかといった報道や雑誌の記事も見るのですが、その辺はどのように考えたらよいの

でしょうか。

セキュリティを担う人材育成

伊東　人材育成は本当にいま、大変な問題です。これだけ問題が起こっているのに、それを解決するためのマンパワーが足りないのです。いまご質問にあった当社の人材育成は、ご参考になるかどうか、お話ししてみようと思います。

　創業者の理念がありまして、基本的に中途採用はしないことになっています。新卒で高専とか大学でコンピュータを専攻した人を採って、ゼロから育てていき、徒弟制の中で人物を評価していって、最後に選ばれた人たちがセキュリティの実際の担当者、オペレーターになる仕組みになっています。正直に言うと、最近、大手企業がたくさん参入してこられ、うちの会社でせっかく育てた人材を引き抜こうとするのが若干目に余るのですが、そういうやり方もあります。

ついでに、人材育成について世界がどうしているかという話が面白いと思うので、お話しします。三つくらいあって、北朝鮮方式、アメリカ方式、中国方式と私は呼んでいます。

北朝鮮方式というのは、あの国はコンピュータがあまりない国なのですが、特待生制度があって、小学校で成績がよい子は中学校で特待生、中学校で成績がよい子は高校で特待生というふうに、国として将来のＩＴ技術者を育てるための制度ができています。その奨学金で上がってきて、大学まで行くと、聞いた話では親御さんの生活の面倒まで国がお金を出してくれます。

これで何が起こるかというと、「私が勉強してここまで来られたのは将軍様のおかげです」という、揺るぎない忠誠心を持つ子が育ち、さらにお父さんとお母さんは、体のいい人質に取られているわけです。こうして裏切らないＩＴ技術者を計画的に育てて、これが北朝鮮のサイバー部隊の要員になるのではないかと言われてい

ます。

アメリカ方式というのは、アメリカでは昔、ハッカーを雇えばいいじゃないかという話がありました。どうやってハッカーを雇うか。FBIとその他の政府機関が一緒になって、全米ハッカー一斉検挙をやったのです。一流は無理だけれども、一流半から二流のハッカーをごっそり捕まえました。そしてアメリカには司法取引制度がありますから、「ブタ箱か犬か」選べと言ったら、皆「犬」になります。それで連邦政府はハッカーを大量に雇用したそうです。

その顛末ですが、3年前に私が飛行機に乗っていたときに読んだ記事に、この作戦をやった指揮官の手記が載っていて、こう書いてありました。「あれは失敗だった。どいつもこいつも皆、政府を裏切っていた」。当たり前だと思いませんか、ハッカーで、もともと犯罪者なのですから。そういう人たちを捕まえて、いくらやれと言われても、結局裏切るわけです。

アメリカはそれで反省して、青田刈り作戦に変えました。これは、日本ももしかするとできるかもしれないと思います。サイバーに関する競技会、ＣＴＦというものをたくさん、高校生レベルでやるのです。それを人事担当者が見ていて、光る子がいたら肩を叩いて「君はなかなかよい子だね」「連邦政府の奨学金をあげるので、大学へ行ってもっとコンピュータの勉強をしないか」と。

これで、４年間、その子に管理官が付くのです。４年間ちゃんと人柄も見ていて、４年後に卒業するときにこの若者に見込みがあるなら、連邦政府のＮＳＡとかＦＢＩに採用されることになると聞いています。これがアメリカ方式、青田刈りです。

最後は中国方式です。中国では人民解放軍がかなり早い時期にサイバー戦部隊をつくったのですが、これがあまりうまくいきませんでした。なぜかというと、いわゆる富裕層のパソコンを最初から使える子は人民解放軍へは来ないのです。来るの

は農村部の貧乏な子弟が来るわけです。それで人民解放軍がサイバー戦士にしようと思ってコンピュータをがっちり教えるわけですが、もうおわかりですね。そういう子たちはすぐに人民解放軍を辞めて給料がよい民間企業に行ってしまうのです。

そこで人民解放軍はどう変えたかというと、以前からある民兵制度を活用して、サイバー民兵ということを、いまやっています。IT企業や大学の電子系の者を丸ごと、民兵という準軍事組織に組み込んでしまうのです。要するに社長さんが大隊長で、部長さんが中隊長で。

インターネットで探してみると、みんな戦闘服を着て、「サイバー民兵の結束式」という写真が出たりしています。

このようにして、IT企業を丸ごと軍の下部組織として組み込むことによって、レベルを下げないサイバー戦部隊を持つということを中国はやっています。

最後に人材育成を私はどう考えるかというと、よい子を採ってきて、大事に育

て、そして逃がさない。これが大事だと思っています。

大澤　実体験に基づいて、非常に説得力のあるお話をいただきました。

最後に中国のところですが、加茂先生にお伺いします。コカ・コーラの事例だと、中国は企業と政府、情報機関と軍とかが一体となって情報を取りに来ているような感じもするのですが、中国の仕組みの中で人的なネットワークとか、そういうものは企業等とか、企業と政府とか、繋がりがかなりあると考えたほうがよいのでしょうか。

加茂　それはもちろん、会社によって随分と違うと思います。よく言われているのは、90年代あたりから中国で成長している企業は、もともと党や国家の幹部がリタイヤして、あるいは途中退職して、民間に下りていっているという点です。その人は民間企業の立場なのだけれども、国家や党に人脈があるので、そういう人たちとうまくコネクションをして、お金を借りやすいとか、資源がどこにあるかとか、あ

るいはどのタイミングでどう株を売ったらよいかというのを知っていて、あるいは自分の親類に株を売却したり、そういう形でビジネスとしてやってきています。ですので、おそらく企業がどういうバックグラウンド、どういう人的ネットワークを持っているのかというのは、どういう人たちが董事長（取締役会議長）や会長であるのかを観察することによって、非常に容易に観察できるだろうと思います。

大澤　ありがとうございます。日本はずっと規制改革の中で、たとえば金融庁と銀行のように、民間と政府が人的にあまりコネクションを持ってはいけないということが続いてきました。先ほど野原さんがご指摘になった情報共有の仕組みについても、政府と企業がちょっと離れすぎたのではないかということです。もう少し近付いて、たとえば中国のようにコネクションを深める。経済的な利益が懐に入るのはまずいですが、外国からのサイバー攻撃に備えるとか、そういう点では少し情報共

有のあり方や、政府と民間企業の情報ネットワークのあり方は考える必要があるかと思います。

その一つが、冒頭の報告で土屋先生からお話があったＪＰＣＥＲＴで、皆さんの企業のセキュリティのインシデント情報を企業の名前を出さずに集めているという話です。われわれはヒアリングで聞いていますので、そういったところも使っていただければよいのではないかと思います。

占部審議官、情報共有の仕組みというのは、何か政府で考えられていることはあるのでしょうか。

政府が進める情報共有の仕組み

占部　情報共有は、おそらくこの1年間くらいでずいぶん進んでいます。実はもっと前に戻ると、政府の中でも全然情報共有がされていませんでした。やはり「政府

の中では情報共有しなくてはいけない」と、いまは政府、特に霞が関は、A省に攻撃があったら直ちにB省、C省、D省と、ほとんどすぐに対策が取れるメカニズムをつくってあります。

重要インフラ事業者関係では、われわれ政府を媒介にする場合もありますし、いまは業界の中、それから業界を超えて情報共有をしたりしています。たとえばウイルスがあったら、それを解析するとかの情報も入ってきています。ウェブサイトがどういうレスポンスをしているか観測をして、シェアするというメカニズムを、重要インフラのほうでつくってきているということです。

その次のレイヤーは、先ほど三菱重工のサイバースパイ侵入の話が出ていましたが、ああいう中で議論して、「では官民も含めて」ということでいくつかのスキームができています。経産省などを中心としてやっているのはIPA（情報処理推進機構）など、よりクローズドなネットワークをつくって進める情報共有がありま

す。他方、警察はもうちょっと広い、何千社かが入ったようなネットワークがあって情報共有をしているということです。

絶えず悩ましいのは、シェアする相手を広げれば広げるほど、実はそれはほぼ公知の情報になってしまうのです。要するに攻撃者も見られる情報になってしまうということです。だから、どこかで割り切って、「これは攻撃者が見てもよい」というくらいの割り切りをして、落とし込んでいかなくてはいけないと思っています。先ほどの経産省ではＮＤＡ（秘密保持契約）を結んで絶対に秘密というふうにやっている、そういうものもあります。

おそらくこう説明すると、政府はやたらと情報共有の仕組みをいくつもつくって、各省がバラバラなどと思われるかもしれませんが、実はそうではなくて、本質的に相当ガチッとしたネットワークをつくるのと、相当ルーズな形で情報共有をするという分け方の問題です。あとは情報共有なんかしなくて、ウイルスみたいなも

のだったら、セキュリティベンダーとかウイルス対策ベンダーに全部検体を渡してしまって、放っておいても全部対策をしてもらう。これも一つの手なので、見えるところ、見えないところ、結構いろいろなところの手当てをしているのですが、なかなか言える話、言えない話があるというのが、正直なところです。

大澤　ありがとうございます。政府の情報共有、もう少し距離を近付けていただいてもいいかなと思います。

セキュリティコストをどう考えるか

大澤　資料11（96ページ）の一番上の問題に戻りたいと思います。サイバーセキュリティの話を企業の経営リスクとしてどのように考えるかというところで、これはおそらく野原さんから解答をいただきたいと思います。

ちょっと古いデータですが、アメリカの企業が平均でどれくらいセキュリティ投

資をしているのかという、ガートナーという情報セキュリティ情報会社の２０１０年のデータがあります。アメリカの企業は総売上高（収入）の３・６％、事業費の４・６％をＩＴの投資に使っているのです。従業員のパソコンやサーバーも含めてです。このうちの約５～７％をセキュリティに投資をしています。もう３～４年前のデータですので、いまはもうちょっと数値が上がっているかもしれませんが、１兆円の売上高の企業であれば、18億～25億円くらい情報セキュリティに特化して投資をしている、ということになります。

企業のリスクとして考えたときに、情報セキュリティの投資というのは、損害保険のようなものなのかなと思います。当然そのセキュリティが破られて情報が流出したときに企業が被る損害を担保することになりますので、実際にお金がかかりますし、効果が目に見えないというところもある。そういった観点からすると、このリスクとはどのように考えて経営の中に取り込んだらよいのでしょうか。その辺を

野原さんから。次いで伊東さんから、企業として、経営資源をどれくらいリスク管理に割り振るべきなのかの指標をお聞かせください。

野原　私からは、そんなに解はないのです。保険として考える部分と、実際にきちんと環境を整えて手を打つ部分と、それから人的な体制によって緩やかにやる部分など、いくつか項目を分けられると思うので、それを分けて。必ずしもそれがコストとピタッと直結はしないと思うので、「何%をかければそれでよい」ということではないと思います。そういうことを総合すると、やはりもう少し丁寧な分析をする必要があって、この研究会の次でもいいですし、国の調査でもいいのですが、本当にどのような枠組みで、どれくらい実際にかけられているのかという現状把握をすることと、今後に向けてどんな指標を持って見ていけばよいかを整理していく必要があると思います。

伊東　私はセキュリティ企業におりますので、正直に言うと、皆さんが青天井でお

金を出してくれるとすごくうれしいのですが、そういうことは期待されていないと思います。そこで企業における防護のヒントをまとめてみました。

当たり前ですが、安全はタダではないわけです。一番弱いところがやられるというのも皆さんおわかりだと思います。それでまず最初に強調したいことは、いくらハッカーだ、ウイルスだといっても、正面玄関から入られたら何もならない。IDとパスワードの管理に今非常に目が行っていない気がしています。

さて、ご質問についてですが、いくらコストをかけても絶対の安心はありません。また、かけたコストに対応して得られる安心の度合いを測る指標もありません。その中でどうすればよいのかというと、私の個人的な見解ですが、少なくとも同業他社よりはしっかりとやっておくことです。なぜ「少なくとも同業他社」という言い方をするか、おわかりでしょうか。最近のサイバー攻撃には、先ほど申しあげた国家のものもあるのですが、犯罪者がお金目当てで攻撃するものがたくさんあ

ります。この場合では犯罪者もある意味のコスト管理があるわけで、むやみに攻撃してくるわけではなくて、ある程度目星を付けてからやります。

たとえば現実の世界での泥棒が宝石店を襲おうとチームをつくって実行するときに、いきなり目の前の宝石店に泥棒に行くわけではありません。何軒か宝石店があって、どこを攻撃するかと考える。片方はこうこうと電気がついて、ガードマンが24時間見ているところ。もう片方は夜になったら電気を消してシャッターを閉めて帰ってしまうところ。当然、帰ってしまうほうに泥棒に行くわけです。たぶんいまのサイバー犯罪の攻撃者も似たような心理があって、攻撃する前にある程度調査をします。それから実際の犯罪に及びますので、同業他社と比べて明らかにその対策が少し上であれば、そこは避ける可能性が高い、つまり若干の予防になるというわけです。

ただ蛇足ですが、あまりそこで社長が気張って「では業界随一」などと言ってパ

ーッと金をかけると、今度は別の人たちを招き寄せることになるので、それはあまり宣伝しないほうがいいと思います。つまり腕自慢のハッカーが狙ってきます。うちの会社も実はあまり言わないのですが、結構攻撃されていて、一番汗をかいているのは自社を守る部門だったりします。

大澤　ありがとうございます。最後にパネリストの皆さんから一言ずつまとめのコメントをいただければと思います。

中国のサイバーセキュリティは日本とは別次元

加茂　中国のサイバーセキュリティの問題を考えるときに、おそらく先ほど大澤さんがおっしゃっていた企業と政府との距離感を考えると、中国の場合はもう企業も政府もいわゆる運命共同体になっています。つまり体制を維持することによって企

業が安全に発展するわけです。そういう問題を考えると、中国におけるサイバーセキュリティの問題というのは日本で行われている問題とはまた別次元の問題だという印象を持っています。

国としてしっかりとした法律制度をつくるべき時期

伊東　いまのこの、インターネットを使っている社会はどういう社会でしょうか。私の感覚では、自動車が発明された直後の世界です。自動車が発明されて、貴族とかお金持ちが乗り回しているのですが、道路交通法もなく、車検制度もありません。もちろん交通警察官もいません。皆、好き勝手やっているわけです。だからこの状態を早く是正しなければいけません。要するに技術の進歩に、法律も制度も追いついていないということです。まずそれを追いつかせなければいけません。

具体的にどうするかということの一つは、さっき土屋先生がおっしゃったと思い

ます。インターネットは自由な世界だと私も思っていましたが、犯罪者とかインターネットを悪用する人の活動が目に余ります。やはり国としてしっかりとした法律制度をつくるということです。併せて、元自衛官なので言いますが、日本のシステムインフラに対する防護もまったくできていないと私は思っています。これも皆さんが心を合わせて訴えて、国を動かしていかなければいけないと思っています。危機感を持って行動しましょう。

一人ひとりができるだけ自分で考えて判断する体制

野原　今回の研究会の中でワシントンに土屋先生と一緒に行って、いろいろな方とディスカッションをする機会がありました。その中で先ほども発言したようなことを感じ、気付きました。やはりアメリカのほうが危険にずっとさらされているので、考えていることが先に行っているということを強く感じました。戻って見てみ

ると、日本のいろいろな、ＮＩＳＣ（内閣官房情報セキュリティセンター）でやっている仕組みとかも、アメリカのことを勉強して、この体制をつくっていたんだとか、カテゴライズもそうやっていたんだとか、いろいろと気付くこともあって、それはそれで有効性もあるし、納得できたのです。

でもこれからのフェーズになっていくときに最も気を付けなければいけないことは、ルール化したり、たとえばチェックリスト化とかガイドライン化して、トップダウンで「これをやれ」と言ってみんなにやらせるやり方では、だめになってきている。フェーズが変わったというのはそこだと思っています。

もちろん最低限のウイルス対策とか、そういうことはやらないといけないのだけれども、そういうことをギリギリと攻めていっても、その先には次に行ける解はないのです。それがどうしてないかというと、個々のアクションを丁寧に指示すればするほど、一人ひとりは何も考えなくなっていくわけです。そのチェックリストを

チェックすればいいというふうになっていく。個々の人が柔軟に考えて判断する機能をどんどん失わせていくということだと思うのです。そうすると、それは想定外のゼロデイアタックにすごく弱い組織になっていくということなのだと思うのです。

なので、これからのフェーズが変わった、ゼロデイアタックにも耐え得るような日本の経済環境とか社会にというときには、ただルールに則って動くのではなくて、一人ひとりがきちんと自分で考えて判断するというステップを間に入れ込んでいくという姿勢がすごく大事なのではないかと思います。それが実はアメリカに行って一番強く感じたことです。議論の中で、たとえばいろいろなことを効率化して「ここの1カ所に集めればいい」みたいな話をつい言ってしまうと、「そうするとそこだけ狙えばよくなるのだ」みたいな話があったり。非常に柔軟に現実的に一個一個を考えているということを強く感じました。

ぜひ現場の人たちも、一人ひとりができるだけ自分で考えて判断するという形をつくれるように気を付けて、体制をつくっていただければと思います。

経営層にしっかりとしたセキュリティ意識を持っていただきたい

占部　せっかくこの経団連の場所で議論させていただいているので、やはり経営層の方にしっかりとした意識を持ってほしいというのが、私からの唯一のお願いです。

われわれは、サイバー空間を公衆衛生にたとえてやっていますが、結局個々人それぞれの取り組みと、それを守るような取り組み、それから会社としての取り組みが必要だと思います。会社でいうと、なぜ会社は職員に対して健康診断をするのかというのを突き詰めていけば、最後は自社の健保組合の財務みたいなところまでたどりつく――実は外部経済になっているところをどんどん内製化して、そのコスト

を弾くと、意外とセキュリティは真面目にやっておかないとだめだということになると思います。人の迷惑というところを全部外に散らしてしまっているのです。

だから経済を内部で捉えていると、非常にセキュリティ自体の重要性がわかってくると思っています。先ほど「ちょっと技術から離れて」と申しあげたのはそういうことだったのですが、ここの場に来られた方にそういう意味でしっかりと捉えていただいて、対策をしていただきたいのです。もちろんわれわれも一生懸命やっていきますが、やはり最後は各主体がどう動くかということなので、しっかりと取り組んでいただければと考えているところです。

大澤　ありがとうございました。水と安全はタダだと言われてきたわが国ですが、情報の世界もやはりリスクがありコストがかかるということをしっかりと認識して、官と民ができるだけ距離を近付けてやっていくことが必要ではないかと思います。

野原 佐和子（のはら・さわこ）

㈱イプシ・マーケティング研究所代表取締役社長／ IT 戦略本部情報セキュリティ政策会議有識者構成員
1958年 三重県生まれ。1980年 名古屋大学理学部卒業、三菱油化（現三菱化学）に入社。その後、お茶の水女子大学大学院修士課程、生活科学研究所、1995 年に情報通信総合研究所（NTT グループのシンクタンク）EC ビジネス開発室長を経て、2000 年 IT ビジネスに関する調査およびコンサルテーションを行う㈱イプシ・マーケティング研究所を設立、代表取締役社長に就任（現職）。この間、日本電気取締役（2006 ～ 2012 年）、慶應義塾大学大学院政策・メディア研究科特任教授（2009 年～）、損害保険ジャパン監査役（2012 年～）を歴任。また、「IT 戦略本部」有識者本部員、IT 戦略本部「情報セキュリティ政策会議」、経済産業省「産業構造審議会総会」「産業構造審議会情報経済分科会」、総務省「電気通信事業競争評価アドバイザリーボード」、公正取引委員会「独占禁止懇話会」、文化庁「文化審議会著作権分科会」をはじめ、政府・各府省庁の審議会・委員会委員を多数歴任。

伊東　寛（いとう・ひろし）

㈱ラック理事・サイバーセキュリティ研究所長
1980年 慶應義塾大学大学院（修士課程）修了、陸上自衛隊入隊。以後、技術、調査、システム関係部隊の指揮官および幕僚等を歴任。1987年慶應義塾大学工学博士。2007年 退官、シマンテック総合研究所入社、2010年㈱ラック入社。

加茂　具樹（かも・ともき）

慶應義塾大学総合政策学部准教授
1972年 横浜市生まれ。慶應義塾大学総合政策学部卒業、同大学院政策・メディア研究科博士課程修了。博士（政策・メディア）。専門は現代中国政治論、比較政治論。香港日本国総領事館専門調査員、慶應義塾大学法学部准教授を経て、2008年より現職。カリフォルニア大学バークレー校現代中国研究センター訪問研究員、國立政治大学（台湾）国際事務学院客員准教授も歴任。

報告者等略歴紹介（敬称略、2013 年 4 月 11 日現在）

占部　浩一郎（うらべ・こういちろう）

内閣官房情報セキュリティセンター副センター長／内閣審議官
1982年 通商産業省（大臣官房情報管理課）入省、2004年 内閣官房 IT 担当室参事官、2007年 独立行政法人情報処理推進機構理事、2010年 経済産業省経済産業政策局調査統計部長、2011年より現職。

土屋　大洋（つちや・もとひろ）

21世紀政策研究所研究主幹／慶應義塾大学大学院政策・メディア研究科教授／ IT 戦略本部情報セキュリティ政策会議有識者構成員
1970年生まれ。慶應義塾大学法学部卒業後、1999年同大学大学院政策・メディア研究科後期博士課程修了。博士（政策・メディア）。国際大学グローバル・コミュニケーション・センター（GLOCOM）主任研究員などを経て、2011年より慶應義塾大学大学院政策・メディア研究科教授兼同大学グローバルセキュリティ研究所副所長。専門は国際関係論、情報社会論、公共政策論。

大澤　淳（おおさわ・じゅん）

世界平和研究所主任研究員
1971年生まれ。1994年 慶應義塾大学法学部卒、1996年 同大学院修士課程修了。1995年より世界平和研究所研究員。2003年 明治学院大学国際学部講師、2004年 外務省国際情報局専門分析員、2004～2006年 外務省国際情報統括官組織専門分析員、2007～2009年 外務省総合外交政策局外交政策調査員を併任の後、2009年より現職。現在、海上自衛隊幹部学校講師、政策研究大学院大学（GRIPS）客員研究員を併任。専門は国際政治学（安全保障、外交戦略）。

第101回 シンポジウム

サイバー攻撃の実態と防衛

2013年7月25日発行

編集　21世紀政策研究所

〒100-0004　東京都千代田区大手町1-3-2
経団連会館19階

TEL　03-6741-0901
FAX　03-6741-0902

ホームページ　http://www.21ppi.org

21世紀政策研究所新書一覧（※は刊行予定）

01 農業ビッグバンの実現―真の食料安全保障の確立を目指して（2009年5月25日）
02 地球温暖化政策の新局面―ポスト京都議定書の行方（2009年11月25日）
03 国際金融危機後の中国経済―2010年のマクロ経済政策を巡って（2009年12月14日）
04 これからの働き方や雇用を考える（2010年2月9日）
05 わが国企業を巡る国際租税制度の現状と今後（2010年2月10日）
06 地域主権時代の自治体財務のあり方―公的セクターの資金生産性の向上（2010年3月2日）
07 税・財政の抜本的改革に向けて（2010年7月9日）
08 日本の経済産業成長を実現するIT利活用向上のあり方（2010年11月10日）
09 気候変動国際交渉と25％削減の影響（2010年11月17日）
10 新しい雇用社会のビジョンを描く―競争力と安定：企業と働く人の共生を目指して（2010年12月10日）
11 中国経済の成長持続性―いつ頃まで、どの程度の成長が可能か？（2010年12月17日）
12 国際租税制度の世界的動向と日本企業を取り巻く諸課題（2011年1月17日）
13 戸別所得補償制度―農業強化と貿易自由化の「両立」を目指して（2011年2月3日）
14 新しい社会保障の理念―社会保障制度の抜本改革に向けて（2011年2月14日）
15 会社法改正への提言―ドイツ実地調査を踏まえて（2011年2月21日）

16 アジア債券市場整備と域内金融協力（２０１１年３月３日）
17 地域主権時代の地方議会のあり方（２０１１年５月16日）
18 いま、何を議論すべきなのか？～エネルギー政策と温暖化政策の再検討～（２０１１年７月８日）
19 自治体の経営の自立と「地域金融主義」の確立に向けて（２０１１年７月27日）
20 税制抜本改革と地方税・財政のあり方―グローバル化と両立する地方分権をいかにして進めるか（２０１１年10月６日）
21 変貌を遂げる中国の経済構造―日本企業に求められる対中戦略のあり方（２０１１年12月９日）
22 政権交代時代の政治とリーダーシップ（２０１１年12月14日）
23 会社法制のあり方―米・仏の実地調査を踏まえて（２０１２年２月７日）
24 社会保障の新たな制度設計に向けて（２０１２年２月23日）
25 企業の成長と外部連携―中堅企業から見た生きた事例（２０１２年２月29日）
26 日本の通商戦略のあり方を考える―ＴＰＰを推進力として（２０１２年３月21日開催）
27 日本の農業再生のグランドデザイン―ＴＰＰへの参加と農業改革（２０１２年４月10日開催）
28 グローバルＪＡＰＡＮ―２０５０年 シミュレーションと総合戦略―（２０１２年７月４日開催）
※29 中国の政治経済体制の現在―「中国モデル」はあるか―（２０１２年12月21日開催）

30 持続可能な医療・介護システムの再構築（２０１３年２月４日開催）
31 国際租税をめぐる世界的動向―ＯＥＣＤ、ＢＩＡＣの取り組み―（２０１３年２月７日開催）
32 格差問題を超えて―格差感・教育・生活保護を考える―（２０１３年２月14日開催）
33 グローバル化を踏まえた我が国競争法の課題（２０１３年２月21日開催）
34 日本経済の成長に向けて―ＴＰＰへの参加と構造改革―（２０１３年３月１日開催）
35 金融と世界経済―リーマンショック、ソブリンリスクを踏まえて―（２０１３年３月７日開催）
36 新政権のエネルギー・温暖化政策に期待する（２０１３年３月13日開催）
37 日本政治における民主主義とリーダーシップのあり方（２０１３年３月21日開催）
38 サイバー攻撃の実態と防衛（２０１３年４月11日開催）

21世紀政策研究所新書は、21世紀政策研究所のホームページ（http://www.21ppi.org/pocket/index.html）でご覧いただけます。


21世紀政策研究所