サイバーセキュリティ 最後の砦

セキュリティ専門家が語るわが国の目指すべき方向性

西尾 素己
デロイト エクスポネンシャル マネジャー
多摩大学ルール形成戦略研究所客員研究員
パシフィック・フォーラム CSIS ヤング・リーダー

中島 明日香
日本電信電話
CTF for GIRLS 発起人

名和 利男
サイバーディフェンス研究所専務理事・
上級分析官

サイバー攻撃を「正しく」怖がる社会をつくる

Society 5.0では、あらゆるモノ・世界がサイバー空間と融合していくことが予想されるため、サイバーセキュリティは最重要課題の一つとなっている。
そこで、サイバーセキュリティの最前線で活躍する3人の専門家に、自身の経験を踏まえて、セキュリティ人材の育成における課題、国民の意識や社会のあり方など目指すべき方向性を議論してもらった。

司会
産業技術本部上席主幹
小川 尚子

「サイバーセキュリティとの出会い」

小川　はじめに、自己紹介を兼ねて、これまでのキャリアパス、現在携わっている業務などをそれぞれお話しいただけますか。

高専を中退して、セキュリティの世界に

西尾　私の場合、人生設計自体が少し変わっているかもしれません。小学生のころから独学でプログラミングを始め、世界中の「ホワイトハット」と情報交換しながら、システムの脆弱性を発見・報告する活動をしていました。2010年ごろ実家の家業が傾いたこともあって、高等専門学校を2年で中退。その後、IT系ベンチャー企業に就職し、プログラマーとして新規事業の立ち上げに携わりました。続いて、国内のセキュリティベンダーに転職しセキュリティ業界へ。そこで攻撃と防御の基礎概念の基礎研究に従事するなど、業務として経験を積むことで、体系的かつ学術的に知識と技術を整理することができたのは大きかったです。

その次に、大手検索エンジン企業に転職し、役員層にセキュリティ技術についてアドバイスをしたり、社内ホワイトハットの育成などをしていました。現在は、コンサルティングファームのほか、日本と米国の2つの安全保障系シンクタンクに身を置き、大企業や政府機関に対して、アドバイザーとしてセキュリティ技術に関する提言を行っています。企業のサイバーセキュリティと、国家の安全保障にかかわるナショナルセキュリティ、双方が絡まる部分が今の仕事ということになるでしょうか。

高校生の時からセキュリティの仕事をやりたかった

中島　私は、高校生の時からセキュリティの仕事に進みたいと思っていました。高校時代は私も独学で、本格的に情報科学やプログラミングの勉強を始めたのは、大学に入って、武田圭史教授に師事してからです。

大学の4年間は、研究室でセキュリティの研究をする傍ら、CTF（Capture The Flag：情報セキュリティ技術の高さを競う競技）などのコンテストに出たり、セキュリティ関係

名和 利男

Toshio Nawa

サイバーディフェンス研究所専務理事・上級分析官

海上自衛隊で護衛艦のCOC（戦闘情報中枢）の業務、航空自衛隊で、信務暗号・通信業務／在日米空軍との連絡調整業務／航空総隊指揮システム等のセキュリティ担当（プログラム幹部）業務等に従事。その後、国内ベンチャー企業のセキュリティ担当兼教育本部マネージャー等を経て、サイバーディフェンス研究所に参加。専門分野であるインシデントハンドリングの経験と実績を活かして、サイバー演習（机上演習、機能演習等）の国内第一人者として、支援サービスを提供。最近は、サイバーインテリジェンスやアクティブディフェンスに関する活動を強化中。

西尾 素己

Motoki Nishio

デロイト エクスポネンシャル マネジャー
多摩大学ルール形成戦略研究所客員研究員
パシフィック・フォーラムCSISヤング・リーダー

幼少期より世界各国の著名ホワイトハットとともに互いに同意のもとサーバー侵入能力を競う「模擬戦」を通じてサイバーセキュリティ技術を独学。IT系ベンチャー企業、国内セキュリティベンダーで幅広い領域への脅威分析と、未知の攻撃手法やそれらに対応する防衛手法等の基礎技術研究に従事。大手検索エンジン企業でサイバー攻撃対策や社内ホワイトハット育成、キャピタルファンドへの技術協力に従事後、2016年11月より現職。2017年にサイバーセキュリティの視点から国際動向を分析する米シンクタンクヤング・リーダーに着任。

中島 明日香

Asuka Nakajima

日本電信電話／CTF for GIRLS 発起人

1990年、大阪府生まれ。2013年慶應義塾大学環境情報学部卒。同年4月、日本電信電話入社、セキュアプラットフォーム研究所配属。入社後はソフトウエアセキュリティ分野のなかでも、特に脆弱性発見・対策技術の研究開発に従事。2014年度より、日本最大のセキュリティコンテスト（ハッキングコンテスト）を運営する「SECCON」の実行委員就任。SECCONの支援のもと、日本初となる女性セキュリティ技術者団体（企画）「CTF for GIRLS」を発起人として設立・運営。2018年には、情報セキュリティ分野における、世界最大級の国際会議Black Hat（Asia）のRegional Review Board（査読委員）に就任。

の企業などでインターンをしたりと、実践で技術を磨きました。NTTセキュアプラットフォーム研究所に就職してからは、ソフトウエアセキュリティ、特に脆弱性発見に関する研究開発をしてきました。現在は、主にIoT（Internet of Things）機器の脆弱性発見・対策をテーマに研究をしています。

同時にセキュリティ人材の育成にも携わっていて、日本最大のセキュリティコンテストを開催する「SECCON」実行委員会の委員として、「CTF for GIRLS」という女性限定のCTFワークショップや大会を運営しています。

30歳で初めてWindows PCに触る

名和　私は、高校卒業後、自衛隊に入隊し、海上自衛隊や航空自衛隊で情報監視、通信業務などに従事してきました。2000年に発生した中央官庁のウェブサイト改ざん事案と、2001年の海南島事案による大規模なサイバー攻撃という2つのサイバーテロに遭遇し、現場で対峙するところから、セキュリティにかかわることになったわけです。

自分から希望してというよりは、適性検査の結果で情報システム（専用技術）関係をやることになり、30歳で初めてWindows PC（汎用技術）に触りました。その当時は、新たなシステムを構築・運用するという段階で、セキュリティ技術は必要であるものの積極的にその分野に進もうと手を挙げる人が少なく、消去法で私が担当になってしまいました。こはセキュリティ分野の「エリート」ではありません。教育を受けるというよりも、自ら学んできたという面が強いです。例えば「与えられた環境のなかで自分に期待されていた実務能力を上げるために、やむを得ず海外のインターネット上のコミュニティーに参加」して、汎用技術分野の開発技術やセキュリティに関する知識を習得していきました。その多くは多国籍のコミュニティーでしたが、一部にロシアのハッカーがリードしていたものがあり、皮肉にもそこでの経験が今の活動に役立っています。彼らとの直接的なやり取りにより、実践的な観点とスキルを体得できたことは、今の活動に役立っています。そうして、ADCS（Air Defense Command System）という航空総隊指揮システムの開発・構築に関与していきました。

その後、民間に移り、JPCERTコーディネーションセンターを経て、サイバーディフェンス研究所に入りました。現在は、PwCサイバーサービスやArbor Networksの顧問、経済産業省の臨時職員、あるいは外国政府のアドバイザーなどを務めています。

小川　お話を伺い、皆さんの多彩な経歴に驚きました。そうした方々が、これまでどのような思いでセキュリティ分野に携わり、どのように技術や知識を身に付けてこられたのか。名和さん、もう少し掘り下げて伺ってもよろしいですか。

組織として「なかったこと」にしたい風潮がある

名和　きっかけは「ほかにやる人がいなかったので消去法でやることになった」というのが正直なところです。当時は、セキュリティはまだキャリアに結び付かない仕事でしたから。教材もロシア語や英語のものしかなく、それで勉強しました。たくさんあるプログラミング言語のマニュアルを読みあさり、そうして得た知識を現場で応用しながら、現在に至っています。

小川　組織のなかにいながらも、ほぼ独学で学ばれたということですね。

名和　そうですね。その背景には組織を運営する側の理解不足があります。サイバーインシデントは、組織内における不正行為と同じように、「なかったことにしたい」もの、「現場の責任」として済ませたいもの、とされてきました。そのため、セキュリティの仕事自体を「認めることが難しい仕事」とみなす状況が長く続いてきたように思います。

小川　その状況は、最近になって変わりつつあるのでしょうか。

名和　残念ながらあまり変わってはいないかもしれません。企業も国も、自分たちの側に責任があるとは考えない傾向は、いまだにあります。ただ、この分野に明るい、優秀な人材も出てきているので、意識の高い組織と、そうでない組織で二極化していると感じています。

小川　なるほど。そのあたりをいかに改善していくかについては、後ほどあらためて伺いたいと思います。

中島さんは、どのようなきっかけでかかわるようになられたのでしょう。

大学で学んだことが仕事に活かされている

中島　高校時代に『Project SEVEN』（七瀬晶著、アルファポリス）という小説を読んだことがきっかけです。女子高生ハッカーがサイバーテロリストから世界を守るという内容で、著者が元プログラマーなので、フィクションとはいえ、かなりリアリティーがある内容でした。私はもともと「ITオンチ」だったのですが、「パソコン1つでこんなことができるのか」と感動して、この道に入りました。

小川　ITオンチだったのですか。

中島　はい。メールとゲームぐらいしかできませんでしたね。もともと文系で、得意科目は英語や国語だったのですが、途中から理系に転向して、大学は慶應義塾大学の環境情報学部という文理融合の学部に進み、そこで情報学を専攻し、プログラミングやコンピューター・アーキテクチャーに関する基礎的な知識と技術を学びました。

小川　西尾さんは、いかがでしょうか。

ネット上のコミュニティーが「学校」だった

西尾　叔父が1980年代からプログラマーをしていて、私が7、8歳ぐらいの時に、パソコンをプレゼントしてくれました。最初は内蔵されていたプログラムで遊んでいたのですが、そのうち新しい機能を自分でつくりたいとプログラミングを始めました。小さいころからプログラマーだった叔父が身近にいたので、ほかの人たちよりもスタートが早かったのだと思います。

ある時、自分で書いたプログラムがエラーで落ち、エラーコードを検索エンジンで調べていくうちに、具体的な内容は理解できなかったものの、ネット上には面白いことをやっている人たちがいることがわかりました。加えて、そこで情報交換されている内容は、どうやらプログラムの作者が意図しない動作をさせるように書き換えられそうだと気づき、早速自分のパソコン内で試してみました。叔

撮影：工藤裕文

父に報告したところ、「それは俺も知らないなあ」と。「バッファオーバーフロー」と呼ばれる、初歩的ですがメモリ破損系の脆弱性を突く基礎となる方法で、偶然にもこれが出会いです。

社会に出たのは２０１３年、16歳の時でした。サイバー攻撃が少しずつ一般にも認知され始めたころで、セキュリティをなりわいにしている人がメディアで取り上げられるようにもなってきていました。従来の「ネットワーク系」あるいは「組み込み系」からセキュリティ系に行く、という人材の流れとは別に、いわゆるセキュリティネイティブな人材を採用し始めたのがこのころです。２０１０年ごろから「セキュリティの波はいずれ大きくなる」という直感のようなものがありました。

小川　１人で勉強をしていくなかで、苦労されたことはありますか。

西尾　独学といっても、ネット上、世界中のホワイトハッカーとのつながりがありました。「ダークウェブ」などの言葉ができる以前からメンバーが自腹で世界中に建てたサーバーで構成される独自サーキット上にコミュニティーがあり、そこでいろいろなことを教わりました。一般の人には「ハッキング」というと悪いイメージがあると思いますが、われわれは美学を持っています。技術的な部分だけでなく、倫理観を含めて、正しく、しかしリアリティーをもってそれらを分かち合えるコミュニティーの存在は大きかったですね。孤独感はありませんでした。

名和　うらやましい。私が入ったコミュニティーでは、倫理観はまったくありませんでした。守るのではなく、攻撃する側のコミュニティーに入ったので。そこの目的は明確で、お金をもうけること。その能力に関しては、すごいものがありました。彼らが私のような新参者を助ける理由は、自分たちの仲間にするためです。いわゆる「ミッション・アシュアランス（任務保証）」、標的に対する攻撃を何としてでも成功させるとするミッションの達成を最優先にして、利用できるものは何でも利用しようとする考え方です。そこにある種の潔さを感じました。

小川　倫理的な部分で悩まれることもあったのですか。

名和　結構ありました。最初は周囲から期待された業務を実現するために、自分自身の実務能力や知識力を向上させるためにやっていたわけですが、「このようなやり方でよいのか」という疑問は常に感じていました。

そして、「これで十分なのか」という大きな懸念も抱いていました。例えば、子どもが歩いていて、その先にある深い穴に落ちるということがわかっていれば、身をていして守るのが親の本能であり責務です。倫理観のない人たちが攻撃してくることはわかっているわけですから、それを防ぐことが自分の仕事なのだと今は考えています。日本の政府機関や大企業がサイバー攻撃に遭って、記者会見で頭を下げる姿を見るたびに、じくじたる思いがあります。

セキュリティ人材育成に向けての課題

小川　Society 50に向けて、サイバーセキュリティ人材を質量ともに充足させることが喫緊の課題であり、経団連では、社会全体でサイバーセキュリティ人材を育成し、循環させていくエコシステムの必要性を提言しています。サイバーセキュリティ人材の育成に関して、名和さんは、日本の現状をどのように見ておられますか。

危機意識は二極化、企業の将来が大きく左右される

名和　人材育成の面のみならず、サイバーセキュリティ全般についていえることですが、日本国内を見ると、いまだに「島国」という意識を持っていることに危機感を覚えています。きつい言い方をすれば、「平和ボケ」している。

企業でも、国内中心にビジネスをしているところは、やはり危機感が薄いといえます。一方、グローバルに展開している企業は、現地の厳しいルールに対応するなど、世界の現実に直面しているので、危機感が強いと感じます。

そういう意味では、今、二極化しているのではないでしょうか。人口減少のもとでグローバル化は避けて通れない、Society 50という超スマート社会が確実に到来する、という状況のなかで、経営層がどれだけ危機感を抱いているか、企業の将来が大きく左右されてしまうと思います。

小川　国内の状況を海外と比較したとき、最もギャップが大きいのは、どのような部分でしょうか。

名和　日本はレガシーによって、結果的にサイバー攻撃の脅威から社会が守られてきたという点でしょうか。電話のメタル回線が典型例ですが、２０２５年にはこの回線がＩＰ網へ移行する予定です。日本が維持してきたメタル回線は、端末同士が直接つながるＰ２Ｐ（ピアツーピア）です。局給電で電力を送ることができ、停電があってもある程度システムが動きます。今後、すべてＩＰ網に切り替わっていくと、電源を失えばシステムは完全に停止してしまいます。

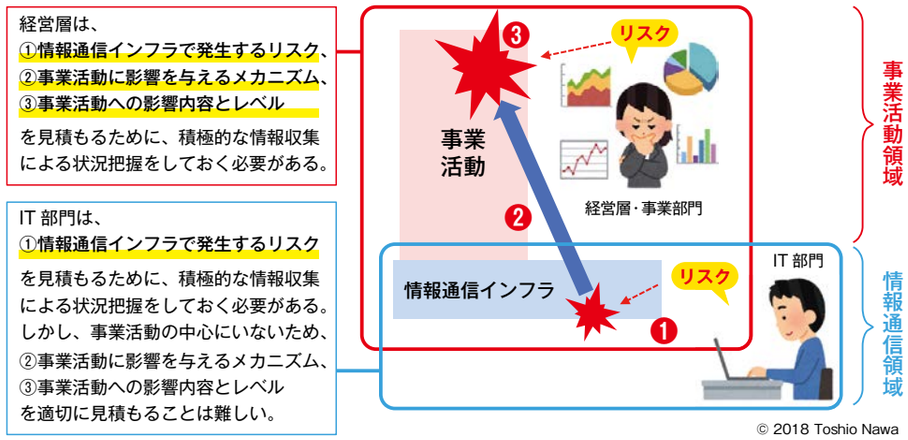
欧米各国はメタル回線からＩＰ網への移行を経験していますが、日本は、レガシーを堅ろうに守っているが故に、見えないファイアーウォールに守られてきたわけです。それが、東京オリンピック・パラリンピック前後、一気にサイバー脅威にさらされることになります。環境が大きく激変し、非常に危険な領域に入っていくことを認識する必要があると思います。

小川　まず経営層の意識を変えることが、重要な課題だということですね。

名和　そうですね。これまで経営層は、サイバーセキュリティのみならずＩＴ関連のことは専門組織に丸投げしていたため、その変化に気づいていないのだと思います。ただ「意識してください」と言っても、あまり効果は期待できません。やはり、自ら経験し、現実をしっかり認識することによって、初めて意識が変わるのではないでしょうか。

小川　経営層を育成することが喫緊の課題です。ただし中長期的に考えると、経営層あるいは事業部門でサイバーセキュリティの素養を持たせるための育成プロセスがほとんどないことが気になっています。ＩＴ部門またはインフラの部分は、攻撃を許せばすべてダメになる、１か０かの世界です。しかし、事業を継続するために、１か０かではなく、何とか０・８で防いでコアの部分は残そう、といった判断は、経営層、事業部門の人材で

図表　経営層が、「積極的な状況認識」をする必要がある



なければできません。

小川　西尾さんは企業のコンサルティングもなさっていますが、企業内におけるＩＴ部門と経営層、事業部門とのギャップについて、どのようにみておられますか。

サイバー攻撃を「正しく」怖がることが必要

西尾　どちらが優れていて、どちらが劣っているというような話ではないのですが、日本企業の経営層は「セキュリティはコストである」という古い考え方を払拭できていないと感じています。ただ、感度の高い経営層の方も増えてきており、セキュリティ対策をしていないと企業の価値そのものが失われることに気づき始めています。

　一般的に、２つのパターンがあるのではないでしょうか。１つは、ＩＴ部門の現場の意識が低いというパターンです。例えば、１人の役員がセキュリティの重要性に気づいて、私たちのようなコンサルティングファームを使おうとしたとき、ＩＴ部門の現場が納得しないというケースがあります。「今まで自分たちは、しっかりやってきたし問題はなかったじゃないか」という声が現場から上がれば、それを無視するのは容易ではありません。経営層は、会社全体でコンセンサスを得なければ、大きな投資はできません。やはり他の役員を巻き込んで、会社全体で経営課題としてとらえることが必要だと思います。

　もう１つは、現場は危機感を持っていて、やる気もあるのだけれど理解されず、経営判断が下りないというパターンです。

小川　何か解決する道はあるでしょうか。

西尾　おこがましいかもしれませんが、私たちのような、サイバー攻撃の危険性を知っていて、攻撃が起きたときにどうなるかも知っている者たちが、矢面に立って大きくルール形成をしていかなければならないと思っています。

　それと同時に、皆さんには、サイバー攻撃を「正しく」怖がっていただかないといけません。どういうことかというと、世の中には「サイバー攻撃が来ますよ。うちの製品を買ってください」という営業をしている会社が多くあります。私の印象では２０１３年以降、急速に増えたように思います。

　その結果、「また製品の売り込みか…」というような風潮が、残念ながら日本にできてしまっている。われわれがお伝えしたいのは、どのような脅威が存在し、どのような対策方法があるのかではなく、セキュリティ対策をしていないことで、グローバルマーケットでいかにその企業が不利になるかということです。いつ来るかわからないようなサイバー攻撃の恐怖を振りかざして仕事を得てきた企業と、明確にわれわれが違う点はここです。サイバー攻撃対策は世界中のさまざまなルールになりつつあります。そしてその多くが２０１８～19年にかけて効力を発揮し、さまざまな経済原理とひも付けた国家戦略として世界中に展開されるでしょう。そのような状況下でマーケットシェアが急落するという「正しい恐怖感」を形成していかなくてはいけません。啓蒙活動を含めて、産学官民がしっかり連携して、日本社会全体でサイバーセキュリティというものをとらえ直していく必要があると考えています。

小川　なるほど。「正しく怖がる」というのは、とてもわかりやすく、大事な言葉ですね。

　中島さんは、先ほど「CTF for GIRLS」を主催されているというお話もありましたが、やはり女性にとってサイバーセキュリティはハードルが高い、入りにくい世界というところがあるのでしょうか。

なぜ「CTF for GIRLS」を始めたか

中島　大学生のころからいろいろな勉強会に出てきましたが、参加者のうち女性は私１人だけ、という会合も多くありました。周りの女性に聞いても同じような状況で、そうなると目立ってしまい居心地が悪かったり、話に入りづらかったりということがありました。

技術に男女差はない、でも、そうした社会的、心理的なハードルから、サイバーセキュリティコミュニティー業界には女性が少ないという状況が続いているのではないでしょうか。

　そもそも理系に進む女性が少ないことが根本的な原因ですが、それは私が解決できる問題ではないので、まずは目の前のサイバーセキュリティ業界の現状を変えていこうと考えました。その一環として、心理的なハードルを下げるために、女性限定のＣＴＦのワークショップを２０１４年６月から続けています。第１回のワークショップでは募集開始から３日間で80人が集まり、「こんなにたくさんいたのか」と、反響に本当に感動しました。今年が４年目になりますが、これまでワークショップは計９回、女性限定の大会も３回開催していて、延べ６００人近くの人が参加しています。今後の課題は、ロールモデルとなるような人材の輩出です。同時に、女性コミュニティーを、もっともっと大きくしていきたいという目標も持っています。


CTF for GIRLSワークショップの様子

小川　経団連も理系に進む女性を増やそう、という取り組みを進めていますが、キャリアパスを示すことは大切ですよね。サイバーセキュリティ分野でも、ロールモデルとなる人たちが出てくると、目指す人たちが増えるのではないでしょうか。

名和　サイバーディフェンス研究所に８年いて、さまざまな方々をスタッフとして迎えてきました。そのなかで、女性、しかも、帰国子女の人が粘り強く良い仕事を続けています。日本の教育にも問題があるのかもしれませんね。新しくチャレンジする分野は、女性が特に向いているように感じます。

小川　サイバーセキュリティには、どのような人材に適性があるとお考えですか。

名和　この仕事は、絶えず新しい脅威があって、新しい技術、知識を組み合わせていかなくてはいけません。そのため、好奇心やチャレンジ精神が旺盛な人が、この業界で力を発揮しやすいように思います。サラリーマン的な安定を求める人には難しいですね。

　日本の教育や文化にも少なからず問題があると思っています。「出る杭は打たれる」ではなく、能力のある人が、素直にそれを伸ばせるような環境をつくってあげることが必要ではないでしょうか。

小川　西尾さんは、いろいろな職場を経験されて、そうした環境について、どのように感じられましたか。

単純に「人材の質も量も上げる」という考え方ではダメ

西尾　セキュリティ人材を「どう使えばよいかわからない」という企業が多いような気がします。例えば中島さんのように、研究もできて技術も持っている人材が入社してきたときに何をやってもらうか、明確に解を出せる会社が非常に少ない。「自社製品に一日中張り付いて脆弱性特定をしていてください」というわけにはいかないでしょう。意欲も技術もある人材をいざ活用しようにも、見合う仕事がないといった状況。私自身、そうした状況にもまれてきた経験が、今のコンサル業務

ことは不可能です。仮に人材育成が成功したとしても、当人は能力を持て余しますし、中小企業としては過剰投資になってしまいます。

ですから、人材の適正な配置先を明確にしたうえで、必要な適正量を確保するべきだと思います。読者の皆さんが普段されている投資意思決定の流れと何ら変わりはありません。そういった観点から、セキュリティ人材に関して、もう一度しっかりと定量評価をしなくてはいけないと考えています。

小川　そこはやはり国主導でやっていくべきでしょうか。

西尾　そうですね。ただ、業界によって、基礎部分は同じでもディテールを突き詰めると全然違うものになりますので、業界団体主導でオリジナリティーを出していった方がいい。

声の大きい人が「全員この基準でやれ！」というのは簡単ですが、漏れがあるし、過剰な場合もあります。官に求められるのは、最低限の基準、ベースを上手に定めることだと思います。「これだけはやってください。あとは業界主導で」というラインを引くことです。このラインが高すぎるとあつれきを生むし、低すぎるとリスクが高まるので、バランスが非常に重要となります。

小川　中島さんにお伺いしたいのですが、通信業界のなかで、どのような人材が必要、といった議論はされていますか。

もっとグローバルに活躍できる人材を増やすべき

中島　当社では、初級・中級・上級というかたちでセキュリティ人材をランク付けしています。初級は基礎知識を持っている人、中級は例えば情報処理安全確保支援士などの資格を持っている人、上級は世界の第一線で活躍している人、といった感じです。

「質と量」の「量」の部分でいうと、1万人の確保という目標を当初掲げ、NTTグループ内で求められているセキュリティ人材像（①セキュリティマネジメント・コンサル、②セキュリティ運用、③セキュリティ開発）を定義したうえで、育成のための取り組みを行っていました。私は中級人材に相当しますが、勤務している研究所では、やはり新しいセキュリティ技術を創出するような上級の人材が求められています。

少し話がずれるかもしれませんが、個人的には、もっとグローバルに活躍できる人材を増やすべきだと思っています。私自身、帰国子女で英語が苦手ではないことから、海外で開催される学会などに行くことが多く、最近では米国のカーネギーメロン大学と共同研究をしていて、世界の第一線の研究者と議論できる機会もあります。

「ブラックハット」という情報セキュリティの国際会議で論文の査読委員をしていると、日本人の投稿者があまりにも少ないと感じます。いくつかの国際会議では、「君が日本人初の発表者だ」と言われました。アカデミックな世界では、海外の状況を把握していないと取り残されてしまいます。査読委員には実は大きなメリットがあって、発表される半年～1年前に内容を知ることができるので、その情報を使って自分の研究をさらに進められます。しかし日本人の研究者でそうした委員をやっている人は少ないと思います。

インターネットで情報収集すればよいと考えられがちですが、やはり人と相対してのつながりは非常に大切です。新しい情報、新しいチャンスが得られます。トップレベルを目指すセキュリティ人材には、もっと国際会議や海外の技術者が集まる場に出ていってほしいと思っています。

小川　この分野に限らず、日本人が苦手な部分かもしれませんね。そこが、先ほど名和さんがおっしゃっていた海外と日本のギャップを生んでいるとも考えられます。

名和　西尾さんのお話で、米国が2000年代のサイバーセキュリティ人材に関し判断を下したというのは、非常に示唆的です。日本でも、2006年からJPCERTコーディネーションセンターでサイバーセキュリティ人材育成の議論を始めていて、今年で12年目になりますが、その進展があまりに遅いと感じています。

やはり、日本のビジネスマンには「日本の産業は製造業で成り立っていて、ITはあくまで利用するものだ」という感覚の人が多いと思います。こうしたマインド、世界観は負のレガシーであり、これからそれを変えていく必要があります。

Society 5.0、未来社会に向けて

小川　今後ますますサイバー空間への依存が高まるなか、その安全性を確保しながら明るい未来を築いていくために、社会のあり方や国民の意識はどうあるべきか、皆さんにお伺いしたいと思います。西尾さんから、お願いします。

サイバー攻撃は「天災」ではなく「人災」

西尾　米国のNIST（National Institute of Standards and Technology：アメリカ国立標準技術研究所）が作成したサイバーセキュリティのフレームワークでは、セキュリティ対策を①特定、②防御、③検知、④対応、⑤復旧、の機能別に分類しています。まず、①攻撃された／されそうな端末などをいかに特定するか。②実際に攻撃が来たら、いかに防御して、入られないようにするか。③入られたら、それをいかに検知するか。④検知したら、いかに内部感染拡大に対応するか。⑤それでも被害を受けた場合、いかに復旧するか。米国ではこの5段階で考えられています。

日本企業、とりわけ経団連の会員企業では、ISMS（Information Security Management System：情報セキュリティマネジメントシステム）の取得率が非常に高いだろうとみています。ISMSのベースはISO27000シリーズですが、先ほどの5段階でいうと、特定、防御までが集中的に語られており、それ以降は内容としては非常に薄いのです。いかに入られないかにフォーカスしたフレームだということです。この背景には、ISO27000シリーズが策定されたころのサイバー攻撃は、きちんと守りを固めれば攻撃を止められたということがあります。しかし、現在の攻撃、特にここ数年メディアで取り上げられ続けている「標的型攻撃」となると、未知の脆弱性を使う攻撃チームも多く、入られて当たり前の世界となっています。そうなると、検知、対応、復旧という後段の部分を、しっかり意識しなければいけません。今回の経団連の政策提言では、そこを入れていただいている点が非常に良かったと思っています。

われわれも、その啓蒙活動に努めたいと考えています。

超スマート社会が来るということは、これまで「サイバーセキュリティなんて関係ない」と考えていた企業であっても、IoTによってサイバー空間との接点が増えることを意味します。これは、サイバー攻撃という名の「ミサイルの射程圏内に入った」ということです。そういう自覚を持っていただきたいと思います。

私のリサーチでは、最近、空売り専業ファンドが、サイバー攻撃に目をつけ始めていることがわかっています。ハッカーを雇って攻撃を仕掛けるパターンもあるし、実際にサイバーインシデントが起きたという情報を、報道が出る前に入手するというパターンもあります。

また、世界中の船舶の運行を管理しているシステムは、ある国の大学生がつくったソフトを使用していて、現在も彼がメンテナンスしているのですが、そこが攻撃されるという可能性もあるわけです。例えば、タンカーが一隻到着しなかったとき、企業どころか、小さい国であれば、それだけでGDPが大きく下がってしまうこともあり得ます。

つまるところ、企業の経営層には、サイバー攻撃とは経済的観点で見た際には敵対的買収と同様のリスクだととらえていただく必要があります。間違っても「災害」だと考えてはいけません。確実に誰かが意図的にやっていることなのです。止められなければ、それは事故ではなく防衛失敗である。そういう意識を持っていただきたいと思います。

「サイバー演習」で経験を通して学んでほしい

小川　天災ではなく人災だということですね。名和さん、いかがでしょうか。

名和　自衛隊時代にも「最後の砦だ」と言われていました。サイバーセキュリティに関しても、常にその思いで対峙しています。ただ、やはり限界は感じていただきたい。

最近、仮想通貨取引所がハッキングされ、大きなニュースになりました。これは一般の企業でも十分に起こり得ることです。そこにある脅威を、わからないからと見ないのでは困ります。自分が認識しようとさえすれば、わかるはずです。今は人間がサイバー攻撃を行っているので、人間の行動・思考パターンとして理解できないことはありません。それについて専門家やエンジニアと議論してみることで、ある程度の見通しはついてくると思います。

あえて挑発的な表現をすると、小学生が教室で「先生、何をしたらよいですか」と言っているようなレベルでは、「あなたの会社は危ない」ということです。先生＝専門家に丸投げするという姿勢ではなく、自らが現実を知り、理解する努力をしていただきたいと思います。

小川　何か秘策はありますか。

名和　ひと言でいえば「経験」です。私たちは「サイバー演習」を行っていて、参加者がプレーヤーとしての意識を感じられるようなシナリオを経験してもらっています。現場に近いかたちのシミュレーションを2時間やるだけで、数カ月間勉強するのと同じくらいの効果があります。

米国のFEMA(Federal Emergency Management Agency：アメリカ合衆国連邦緊急事態管理庁)や欧州のENISA(European Network and Information Security Agency：欧州ネットワーク・情報セキュリティ機関)も、こうしたシミュレーションを作成して、民間に提供しており、先進国では日本だけがやっていないという状況に、危機感を覚えています。

小川　今後に期待したいと思います。中島さん、お願いします。

生産性やイノベーションとセキュリティの両立を

中島　やはりSociety 5.0、超スマート社会は確実に到来します。ただ、その柱として「生産性」と「セキュリティ」が挙げられていますが、両者は、現実社会では相反する場合もあります。つまり、「セキュリティを厳しくしすぎると生産性が下がる」ということは、現実としてよくあることです。

当社でも、パソコン内のファイルを全部暗号化するとか、外部のウェブサイトにつなぐときは定期的に認証しなければならないとか、セキュリティのルールがあり、この運用で生産性が下がってしまっている面があります。生産性とリスク、経営者の考えと現場の状況を天秤にかけて、うまい具合にセキュリティレベルを設定することが、今後の課題だと思います。

また、セキュリティを厳しくしすぎることによって、イノベーションが妨げられるという側面もあると思います。そうした意味でも、Society 5.0の実現には、生産性やイノベーションなど、他の要素を妨げないセキュリティレベルを考えていくことが重要になってくるのではないでしょうか。

小川　企業としてしっかり取り組んでいくべき課題です。経団連としても、呼びかけていきたいと思います。

では、最後に、西尾さん、いかがでしょうか。

ものづくりの精神を活かして

西尾　サイバーセキュリティも、サイバー犯罪も、カウンターカルチャーという立ち位置が重要です。最近は、学術的な姿勢でとらえる方もいますが、私は、根っこはカウンターカルチャー、権威的なものに対して挑戦してやろうという文化だと考えています。守る側にもそういった、権威の裏をかいてやろうという精神がないと、絶対に見つけられない脆弱性というものがあるのです。例えば、学術的なアプローチでは、プログラムを解析して間違っているところを探す、といったやり方をいかに効率的にできるかという見方をするわけですが、そういう部分ではなく、高レイヤーと低レイヤーが複雑に入り混じる中間領域や、人間へのソーシャルエンジニアリング等こそ重大インシデントのトリガーとなっているのです。

守る人材を育てるにあたっても、カウンターカルチャー的な精神をベースにしておく必要があります。どんな銃を使って、どんな弾を撃ってくるかわかっていても、自分が銃の撃ち方を知らない状態では対抗できません。

入門として基礎的な知識をカリキュラム化したり競技化したりするのは、業界人口の増加という観点では非常に良いことだと思います。一方で、本当に中核として防御プランを立てるような人材には、ぜひカウンターカルチャーをベースとしたハッキングの美しさの定義まで、しっかり理解してほしいと思っています。

もう1つ、全体として「日本は遅れている」という話が多かったわけですが、日本の良いところは、ものづくりの国、技術の国だということです。私の実家は金属加工が生業ですが、ものをつくるときの丁寧さというのは、諸外国よりも非常に優れています。こうした風土や伝統は、当然、セキュア設計思想や、プログラムやシステムを構築する際のきめ細かさなどに影響してくると思います。

そうしたベースがあるわけですから、米国に倣うだけではなく、日本のものづくり文化をてこに、こちらから発信していく攻めのルール形成もできるはずです。職人の息子としては、そんなことを考えています。

小川　最後に明るいお話を聞くことができました。皆さん、本日は貴重なご意見をありがとうございました。

（2018年2月5日　経団連会館にて）