つながる世界の情報セキュリティと人材育成を考える

情報セキュリティ大学院大学
情報セキュリティ研究科　研究科長・教授
後藤　厚宏

×

SEC所長
松本　隆明

IoT時代を迎え、様々なモノがネットワークを介してつながり連携することで、私たちの社会生活はより高度にかつ便利になっていくと期待される。一方で、今まで想定されなかったモノがつながることにより、情報セキュリティのリスクの増大は避けられない。人材育成を中心に情報セキュリティに関して多方面で活躍されている情報セキュリティ大学院大学教授で情報セキュリティ研究科長を務められている後藤先生に、新たな時代を迎えた今後の情報セキュリティ対策のあり方や求められる人材像についてお話を伺った。

情報セキュリティ大学院大学の取り組み

松本　IPAでは、様々なモノがネットワークを介してつながるIoTの時代に、セーフティやセキュリティに関して開発・運用時に、どういうことに気を付けなければいけないかを17の指針としてまとめた「つながる世界の開発指針」を策定しました。後藤先生にはその検討の中心メンバーとしてご活躍いただきましたが、今後ますます重要になる情報セキュリティ対策のあり方や人材育成などについてお話を伺いたいと思っています。最初に、情報セキュリティ大学院大学の概要を教えていただけますか。

後藤　厚宏（ごとう　あつひろ）

1984年東京大学大学院 情報工学 博士課程修了（工博）。同年よりNTTにて情報技術に関する研究開発に従事。情報流通プラットフォーム研究所長、サイバースペース研究所長を歴任。2011年に情報セキュリティ大学院大学教授に転身し、2014年より研究科長。enPiTセキュリティ分野代表として、情報セキュリティ人材育成にも尽力。IEEE Computer Society理事。情報処理学会フェロー。現在、内閣府 SIP プログラムディレクター（重要インフラ等におけるサイバーセキュリティの確保）。

後藤　本学は2004年に設立されました。きっかけは2001年の米国における9.11事件です。9.11以降、広い意味でセキュリティに関する見直しが必要だということから、岩崎学園の岩崎理事長が、情報セキュリティについての高等教育を専門とする教育機関の設立構想を描きました。準備期間を経て2004年に開学、現在12年を経過したところです。

修士課程と博士課程からなる大学院のみというユニークな構成ですが、役割は日本における情報セキュリティのリーダーを育てることです。また、社会人に広く門戸を開放し、学びやすい環境を用意することに努めてきました。例えば平日の夕方や土曜日にも授業を設け、働きながら学べる機会を作っています。それが特徴の一つです。

もう一つの特徴は、セキュリティは決して技術だけの話でも、また、法律だけの話でもありません。組織のマネジメントも含め、すべてを融合したものであると考えています。そこで当初から、社会科学系の講義と技術系の講義の両方を用意しています。単一専攻なので、すべての学生が両方の授業を受けることになります。ただし、講義の選択に迷う学生が出てくるかもしれませんので、目指す方向に分けてモデルカリキュラムのセットを用意しました。最も技術系寄りなのが［数理科学コース］で、暗号のアルゴリズムとかビッグデータのような統計のアナリシスの考え方を中心に学びます。社会科学的なものでは［セキュリティ/リスクマネジメントコース］、それから技術と社会科学の両方を必要とする［サイバーセキュリティとガバナンスコース］と［システムデザインコース］があります。

［システムデザイン］と［サイバーセキュリティとガバナンス］は、それぞれ物を作る段階と運用する段階でのセキュリティを扱います。しばしば「システムデザインは技術だけの話ではないのか」と言われるのですが、それは違います。システムを設計する段階から、システムがどう使われ、どういう法律や制度に合わなければいけないのかということが分かっていなければ安全なシステムの設計はできません。一方、運用時にサイバーセキュリティ上の事故が起こったときには、対策を考え「犯人」を探すわけですが、そのときにも、どういう法律がかかわるのか、という知識が必要です。例えばマルウェアかどうかの分析をするときには、著作権法がかかわってきます。

松本　マルウェアでも著作権を気にするのですか？

後藤　そうなんです。マルウェアと確定するまでは、そのソフトウェアに著作権があるということを意識しないといけません。もちろんマルウェアの管理がまずいと自分がまき散らしてしまいますから、それも警戒しながら、法律を知った上で扱い、分析をしなければいけないわけです。

松本　情報セキュリティ大学院大学における教育の狙いはトップレベルの人材育成というところにあるのでしょうか。

後藤　修士課程を卒業したからといって直ちにトップレベルだ

とは言えないかもしれませんが、それを目指す人、あるいは次の世代を教育できる人を育てることを考えています。

松本　企業で言えばキャリアパスのようなことを意識しながらカリキュラムの選択ができるところは大きな魅力ですね。

後藤　例えば20代で来ている方は技術を磨くという志向が強く、30代以上でとくにIT企業から来ている方は、既に技術レベルは高く一定の自信もある、それを活用する組織構造や法律などを学びたい、という方が多いです。

松本　大学のカリキュラムというと、画一的にコースが決められていて、それに従ってやっていくのが一般的だと思います。キャリアパスを意識しながら、その人なりにキャリアが積めるという点はユニークですね。

後藤　設立当初から産業界の方に意見をいただく“応援団”のような組織を持っていたので、いろいろなリクワイヤメントを出していただきながら作ってきました。その成果だと思います。

セキュアシステム研究所では産学共同研究を進める

松本　後藤先生は情報セキュリティ研究科長を務められると同時に、大学内に設置されているセキュアシステム研究所の所長もされています。この研究所はどういう役割を持っているのですか？

後藤　社会や産業界と共同プロジェクトができる場所として位置付けています。客員研究員として日本や世界のトップレベルの人も招きながら、いろいろなプロジェクトを進めていて、例えばセキュア法制を考えたり、マルウェアの分析を進めたりしています。また、法律関係ではシンクタンク的な役割を持たせています。セキュリティに関する法制度をどう作っていけば良いのか、何をカバーしていかなくてはならないのかといったことを各方面の専門の方が真剣に議論する場所にして、年に１回レポートにまとめて提言しています。

松本　実際に社会に対して提言をしていく機関でもあるわけですね。

後藤　そうです。同時に技術面であればマルウェアの現物を持っている人に入ってもらって共同研究もしています。

松本　解析ツールの制作もするわけですか。

後藤　ツール制作というより、こういうアイデアで取り組んではどうか、という研究や提案ですね。

松本　セキュリティは産業界と連携して対策を進めないと現場で実際に起きていることへの対応が難しい。そういう意味で研究所の存在は大きいですね。

後藤　セキュリティの分野はまだ研究の仕方も対策も確立していない“なまもの”の状態ですから、現場の人と研究者が共同で作業していかなければなりません。

松本　確かに、ある物理法則に従って研究だけを進めていけば良いという世界ではないですからね。人の問題やガバナンスの問題など、幅広い分野から考えていかなければなりませんね。

国が進めるサイバーセキュリティへの取り組み

松本　先生は国の取り組みについても重責を果たされています。とくに文科省の「enPiT-Security」（エンピットセキュリティ）では代表として活動されていますが、どんなことをされているのですか？

後藤　エンピット自体は文科省の事業で、４分野にまたがるものです。一つがセキュリティ、それからクラウド、組込みシステム、ビジネスアプリケーションです。それらについて日本のそうそうたる教育機関が分担して活動しています。セキュリティ分野では本学の他、東北大学、慶應義塾大学、奈良先端科学技術大学院大学、北陸先端科学技術大学院大学の５大学が協力して取り組んでいます。特徴は５大学が共同でセキュリティに関する大学院のコースを作っているところですね。

　このコースは、今回のエンピットの狙いでもありますが「実践力を育成する」ということを考えており、座学を少なめにして多彩な演習――セキュリティの世界では「ハンズオン」という言い方をしますが――を実施し、セキュリティの実践的な様々な技術を、学生が体験を通して学ぶことに力を入れています。また、実践力を高める一環として、産業界の方から直接話を聞くことができる機会を数多く設けています。１年を通して所定の単位を取得すると修了の証であるサーティフィケイトがもらえます。ゆくゆくはこのサーティフィケイトを持っている学生が産業界で引っ張りだこになる、という状況を期待しています。

松本　大学にはそれぞれ校風のようなものがあると思いますが、５大学で共通のコースを作るということに難しさはありませんか？

後藤　確かに大変です。校風だけではなく、成績の点数の付け方も違いますし、細かいことを言えば、修了判定のためのデータの締め切り日も違います。とにかく最初は徹底した打ち合わせを重ねました。更に今は毎月５大学の先生が集まって運営について議論しています。

松本　なるほど、なかなか大変ですね。しかし、大学が連携して一つのコースを設けることには意味がありますね。

後藤　大学ごとに得意不得意があるんです。例えばある大学は暗号に強い、またある大学はネットワークに強いといった具合です。その強みを束ねてひとつのコースにしているところは学生にとって大きな意味があると思います。

松本　先生は内閣府の「SIP（重要インフラ等におけるサイバーセキュリティの確保）」という取り組みでプログラムディレクターをされていますが、こちらはどのような内容ですか？

後藤　SIPというのはCross-ministerial Strategic Innovation Promotion

松本　隆明（まつもと　たかあき）

1978年東京工業大学大学院修士課程修了。同年日本電信電話公社（現NTT）に入社、オペレーティング・システムの研究開発、大規模公共システムへの導入SE、キャリア共通調達仕様の開発・標準化、情報セキュリティ技術の研究開発に従事。2002年に株式会社NTTデータに移り、2003年より技術開発本部本部長。2007年NTTデータ先端技術株式会社常務取締役。2012年７月より独立行政法人情報処理推進機構（IPA）技術本部ソフトウェア・エンジニアリング・センター（SEC）所長。博士（工学）。

Program、つまり戦略的イノベーション創造プログラムと呼ばれるもので、社会イノベーションを起こすテクノロジーの開発を目指しています。２年半ほど前に10テーマでスタートしました。航空機材料やパワーエレクトロニクス、その他のデバイスなどの基礎研究を産学で立ち上げようというのが中心です。その後、2020年オリンピック・パラリンピック東京大会に向けて、セキュリティが大事だ、とくに重要インフラのセキュリティが弱いのではないかということから、昨年の夏にサイバーセキュリティの確保が11番目のテーマとして設定されました。プログラムディレクターが公募されましたので、本学は社会のためのサイバーセキュリティ技術の教育研究を担っていますから、取り組みは当然と考えて立候補し、選任されたという経緯です。

ビルトインとボルトオン ―セキュリティの２つの技術

松本　重要インフラのセキュリティ確保について、具体的にはどういう取り組みを進めるのですか。

後藤　日本政府では重要インフラとして13分野を定義していますが、その中からオリンピックに直結しそうなものにフォーカスし、その産業自体のセキュリティの体力を強める土台作りをしようと考えています。とくにエネルギー分野の電力、それから交通、通信が基本です。セキュリティの強化は２つの観点から考えています。１つ目はインフラシステムを作り上げるときに最初から仕込んでおかなければいけないものです。セキュリティ・バイ・デザインと呼ばれるものですね。いわばセキュリティ機能を“ビルトイン”しておくということです。インフラの場合、設備の更改は何十年単位で行われますから、大変時間がかかります。計画的にしっかり作り上げていくことが必要です。２つ目は、すぐ今日、明日のためにセキュリティを強化しなければならない設備への対策です。つまり、今ある設備を横から動作状況を監視したり、不具合を見つけ出す技術です。こちらは“ボルトオン”と呼んでいます。

松本　なるほど、最初の構築時に使う技術と運用時に使う技術ということですね。

後藤　その二つが基本です。更に言えば、これからのIoT時代に向けて、長く使える要素技術やセキュリティ技術を社会実装するための技術も必要になります。現場に入れ込むということです。単に技術として入れ込むだけではなくて、入れ込むことを助ける仕組み、例えば、適合性の評価や認証制度、人材育成、組織が情報共有する仕組みなども考えられます。コア技術を導入することを助ける仕組みについても研究目標に入れています。

まず現場で気づくことが重要

松本　情報共有の仕組みとして、IPAではサイバー情報共有イニシアティブ（J-CSIP〔ジェイシップ〕）の運用を始めていますが、そういう仕組みを更に活用していくということですか？

後藤　そうですね。情報共有については、例えば現場のオペレーション担当者が「サイバー攻撃かもしれない」と気づいたときに、どういうふうに組織の中に伝えれば良いか、現場の人にとって分かりやすいツールは何かを研究し、重要インフラの現場をJ-CSIPやJPCERT/CCなどとつなげられる仕組みを開発しています。いわば現場の人向けの情報共有システムですね。

松本　現場力を高めていくということですね。

後藤　重要インフラのセキュリティを考えたときに、どこが準備不足かというと、それは現場のオペレーションのところであり、そのための人材育成が必要だと思っています。大学院の学生だけではなくて、現場のエンジニアの人がセキュリティを学ぶための教材や演習コースが必要なんです。システムの不具合があったときに、これは故障ではなくてサイバーアタックかもしれないと判断できないとまずい。それができるようになるための教材が必要です。

松本　おっしゃる通りですね。セーフティという観点からですが、我々も重要インフラの障害の情報共有をきちんとやっていきましょうという取り組みをしています。そして、実際の障害をみんなで分析して何が課題であったかを議論して教訓の形にまとめています。その中にも、最初の気づきが周りの人にうまく伝わっていないために、障害が大きくなってしまったという教訓があります。現場の運用者は何かおかしいと感じていたのですが、そのままにしていた。マニュアルにも気づきを報告しろとは書いていない。その結果大障害につながってしまったという事例があります。現場をどう育てていくかというのはとても大きな課題ですね。

後藤　重要インフラの安定運用は現場の人の力で支えられています。これからはサイバー攻撃への対処も担っていただく必要があります。

松本　2020年オリンピック・パラリンピック東京大会は、セキュリティ上非常に大きなイベントになる可能性があり、とくに重要インフラは狙われるでしょうね。ロンドンオリンピックのときも相当な攻撃があったと聞いています。

後藤　あの頃から重要インフラが狙われ始めているんです。警戒を強めるべきだと思いますね。

専門化、分業化するサイバー攻撃

松本　情報セキュリティを取り巻く環境は大きく変化しているのではないかと思います。つながる世界の出現ということもありますが、それ以上に昨今は対策の範囲がどんどん広がっているような気がします。従来はITのWeb系の攻撃対策をどうするかという範囲だったと思いますが、最近は組込みの世界、航空機や自動車のセキュリティをどうしていくかということなど、範囲が広がる一方です。こうした最近の変化をどうご覧になっていますか？

後藤　おっしゃる通り、広がりは実感しますね。端的に言えば、大学に問い合わせをされる方の業界が変わりました。従来はセキュリティのベンダー側、つまりIT技術でいえば開発側の方が多かったのですが、今はユーザ側の方が増えています。とくに、自動車、家電、金融関係などですね。

松本　そもそも攻撃する側も、従来は有名になりたいといった愉快犯的な傾向が強かったけれども、最近は金銭目的とか、経済的に損失を与えるとか、あるいは国家に対する攻撃であるとか、質が変わってきていると思います。

後藤　言葉は悪いですが「裏社会」ができてしまっている感じがします。サイバー攻撃を使ってビジネスをしている人、あるいはそれを産業にしている国もある。市場が生まれ、サイバー攻撃をする人、それにお金を出す人、サイバー攻撃を成就することによって利益を得る人、この分業ができているんです。よ

く「何のために攻撃するんだろう？」という人がいますが、株価も原油価格も穀物相場も、サイバー攻撃によって大きく変動します。それによって儲ける人がいる。有名企業のWebサイトへの攻撃も、株の売買で利益を出すことにつながります。株価が下がればM&Aも有利に進められますね。大きなお金が裏の市場で動いてしまっているのです。そういう意味ではサイバーセキュリティは、技術だけではなくて国際的な取り組みが必要ということになります。

松本　攻撃も組織的なものになってきたということですね。

後藤　専門化、分業化しています。

松本　守る方も組織的に取り組まなければ、個別の対応では守れないですね。

後藤　おっしゃる通りだと思います。

松本　ところで、IoT時代になり膨大なモノがネットワークにつながってくると、データの拡散の問題も出てきますね。あらゆるところでデータが流通する。データを流通させ、共有することで社会をより便利にしていこうということだと思いますが、逆にリスクも高まるわけですね。データがいろいろなところにばらまかれ、それによって個人データの流出や企業情報の流出が起こる。

後藤　社会的にも産業上も、もはやデータの流通をストップすることはできません。データをうまく活用しないとビジネスが成り立たなくなっています。ITはまずオフィスを変えました。更に業務を変え、産業全体を変えた。データの活用で生産性は桁違いに上がっているわけです。もう後戻りはできません。そこは当然のことだと思って、情報流通の世界をいかに守っていくか、守るのは当然だという意識で動かなければいけない。今まで交通や物流の安全を守ってきたように、情報の流通を守るのは当然だという認識に立たなければいけないと思います。

松本　「データは社会的に重要な価値を持つものだ」と考えていかなければならないでしょうね。

求められる セキュリティ・バイ・デザインの取り組み

松本　セキュリティを取り巻く環境がどんどん変わってきたという意味では、これまでのセキュリティ対策は運用型であった。つまり攻撃されたときにどう守るかという対策が中心だったと思いますが、先ほどの後藤先生のお話にもあったように、これからはそもそも攻撃を受けにくくする、設計時にきちんとセキュリティを考慮してものを作っていくというセキュリティ・バイ・デザインの考え方が重要になりますね。

後藤　その通りだと思います。セキュリティを最初から仕込んでおくということですね。しかも、一つひとつのソフトウェア、ハードモジュールを作っている人のセキュリティ・バイ・デザインがあり、社会的なシステムとして、例えばオリンピックの会場を作るときにどうするかという段階のセキュリティ・バイ・デザインもある。何段階もあると思います。いろいろなレベルのセキュリティ・バイ・デザインが必要です。

松本　適切な例かどうか分かりませんが、例えば住宅や建築のバリアフリーを考えるときに、ここに階段があるからどうしようかという対策と併せて、そもそも最初に全体を設計するときに、バリアフリー化が可能となるように設計しておくということが必要ですよね。そういうふうにセキュリティの分野もなっていくべきなのでしょう。IPAでもセキュリティ・バイ・デザインに関する検討チームを立ち上げ、当面は組込み系を中心に議論を進めていこうと思っているのですが、実際のセキュリティ・バイ・デザインへの取り組みを、どうご覧になっていますか。

後藤　ひと言で言えば、まだまだだと思います。必要だという議論は出ていますが、実際の取り組みとしてはほとんど進んでいない。現場の開発部門の方も、言葉としては知っているけれども具体策としては持っていないという現状ではないでしょうか。先行例も乏しいので、早急に強化しなければいけないと思います。

松本　そうですね。実際に産業界の方とお話しすると「確かにセキュリティ・バイ・デザインの取り組みは重要だよね」という合意はできますが、「でもそれはセキュアコーディングのことじゃないの？」というふうに捉える人が多い。もっと全体的に見ていくことが必要ですよね。やはりまだ実例が見えないのだと思いますね。

後藤　実際にどうするかとなったときに、お手本がないんですね。そこは時間をかけても成功例を示していくしかないのかなと思っています。

松本　情報セキュリティ大学院大学では、そういう観点からの取り組みを進めていらっしゃるんですか？

後藤　まだ計画段階ですが、システムの設計時に脅威分析をどう組み込んだら良いかを学べる場を考えています。これまでは修士論文や博士論文でのチャレンジだったのですが、実際の講義に組み込み、更に演習に取り入れる予定です。今までもWebアプリケーションのシステムの脆弱性を見つけ出す演習を実施してきたのですが、では作るときに何をすべきだったのか、設計段階ではこうやるべきだった、動き出したらこういう観点からチェックすべきだと、両面から取り組むような講座を考えています。

松本　まず設計時にセキュリティ上で守らなければいけないのはこれだよね、というところからスタートしていくわけですね。

後藤　そうですね。このシステムはどう使われるのだろう、そのときに何を考えなければいけないんだろうというところからセキュリティ対策を考え、それが実際にできているのかをチェックするということですね。

松本　実際、何かシステムを想定して演習されるのですか？

後藤　脆弱性が多く残っているWebアプリケーションシステムを例として用意しているので、それを分析しながら、脆弱性が残らないようにするにはどうすれば良いかということを検討していく演習にするつもりです。しかしいずれにしても例題が少ないので増やしていかなければならないですね。組込みソフトがどうなっているか、重要インフラを支える大規模な制御システムがどうなっているか、それを順次検討の俎上に乗せていく必要があると思っています。

松本　脆弱性が多い設計と少ない設計が対比できると良いですね。どういうところに考え漏れがあったからこうなってしまったのかが分かるというように。

後藤　確かにそうですね。

プラスセキュリティという発想が必要

松本　セキュリティ・バイ・デザインの考え方を普及させていくためには、何がキーになるのでしょうか。設計の方法論のようなものを確立していくということでしょうか。

後藤　今物づくりをやっている会社は、会社ごとにルールや手

順があり、技術者はそれを身に付けて設計していると思います。その現場に馴染むものであることが必要です。すぐにはできないので少しずつ進めるしかないと思います。

松本　開発環境のようなものを整備していくことも必要なのでしょうか。セキュア開発環境みたいなものがあれば良いのかもしれません。

後藤　そうですね。それぞれの開発現場で新しい開発環境を実際に使えるようにすることが大事なのだと思います。とにかく実際にやってみて、こうやったらうまくいった、じゃあ真似してみようというような。狭い意味でのツール、手順書に始まって、人材の手当て、その育成まで含めてということになるでしょう。当然、設計のコストや期間という問題が出てきます。その点では産業に対するインセンティブも必要ですね。セキュリティ・バイ・デザインをしている製品は価値が高く、価格面でも高く売れるという市場があるべきだと思います。セミナー会場で言葉として「質の悪いものを出してしまって後々対策で苦労するより、最初からきちんとセキュリティをデザインしておけば、コスト面でもメリットがある」とは言えるのです。しかし、実際の現場の人の共感を得るのはなかなか難しい面があります。

松本　いったんセキュリティが破られたときの影響の大きさを自覚する必要があるかもしれませんね。しかも、バグがあるといったレベルの品質の話とセキュリティ上の品質管理の話では、大きな違いがあります。セキュリティでは外からのアタックに対してどうするかということが出てくる。普通の品質管理ならバグをいかに減らしていくか、ということになり、比較的閉じた世界の話で済みます。しかし、セキュリティの場合は外からの攻撃パターンとか、そういうことまで考慮していかなければいけない。

後藤　そうですね。想定と違うものが来たら、今までバグではなかったものがバグになるわけです。実は今、サイバーアタックの規模が非常に大きくなり複雑になっていて、運用段階では扱いきれません。解決できなくなっています。その複雑さを避ける意味でも、設計段階で頑張っていただくことが重要で、仮に運用段階で問題があったとしても、設計がしっかりしていれば対象がぐんと絞れるので、大きな意味があります。セキュリティアナリストが対応できる範囲に絞っていただければ対応が可能になるんです。

松本　セキュリティのスキルのある設計者を育てていくことが重要になるということですが、そのときに、セキュリティが分かっている人が開発に入っていくのが良いのか、開発がある程度できる設計者がセキュリティの勉強を積んだ方が良いのか、どちらが良いとお考えですか？

後藤　私は後者だと思っています。「プラスセキュリティ」と言っているのですが、それぞれの専門の方がセキュリティも習得する、これしかないのではないかと。物づくりの世界は非常に幅が広いわけです。物づくり以外でも社会システム的なものまで含めれば、例えば金融システムも含まれますから非常に広い。そこにセキュリティだけに特化した専門家を送り込むのは無理がある。であれば、自動車のエンジンを作っている人に少し時間をもらってセキュリティを勉強してもらう。金融のATMを作っている人に、セキュリティを勉強をしてもらう。そういうふうにしていかないとカバーしきれないのではないかと思います。セキュリティの専門家が、物づくりができるかと言えばそうは言えないですからね。それぞれの分野ドメインの人に「プラスセキュリティ」という取り組みをしてもらうのが現実的だと思います。実際、本学に入ってくる方の所属も、以前はICTベンダーの方が中心だったけれども、現在は金融であり鉄道であり、警察であったりしています。「プラスセキュリティ」の中で、今まで機械は作ってきたけれどもセキュリティは知らなかったという人に学んでいただいている。これは大事だと思います。そういう人のために、今後は大学院としての取り組みだけではなく、週単位の短期講座のような機会も作っていきたいと思っています。

松本　確かに「プラスセキュリティ」の考え方が基本なのかもしれないですね。実際の開発現場では、開発プロセスは既に厳密に決められているわけです。その中にどうやってセキュリティの考え方を入れていくべきか、と考えるべきですね。プラスするという発想ですよね。

後藤　開発現場に外部からこうしなさいと言っても絶対に変わってもらえないですね。今のプロセスを理解し分かっている人に、「あ、セキュリティが大事なんだな、じゃあどうすれば良いかな」と自ら気づいていただくことが一番重要なことだし、価値があることだと思います。

セキュリティ・ガバナンスの重要性

松本　もう一つ重要なテーマとして、セキュリティ・ガバナンスということがあると思います。そもそもセキュリティは技術だけでは守れない。ソーシャル・エンジニアリングなど人の要素も含めて考えていかなければいけない。法律面のこともあると思います。そのあたりはどうお考えですか？

後藤　ソーシャル・エンジニアリングについて言えば、ようやくいろいろな人が気づき出したなと感じます。本学でも社会科学と技術の両方が学べるようにしているわけですが、ただ単に学べるだけではなくて、お互いにぶつけ合ってみることに意味があると思います。私自身は技術系の人間ですが、実は法律の先生と一緒に一つの授業を担当しています。私が講義するときは、その先生が学生と一緒に聴いています。そして法律の観点から質問などもされる。逆に法律の先生が講義をするときは私が聴いています。そして学生と一緒に議論を深めていきます。両面あるんだ、ということがその場で理解できるので、非常におもしろいと思います。学生にも好評です。

松本　それはおもしろそうですね。

後藤　例えば認証とかITマネジメントの話を私がするのですが、それを個人のプライバシーとか法制度の観点からどうか。その場合、日本と欧米では違うとか、だから同じ技術ではだめだということが講義の場で分かってくる。技術の使い方の違いや普及度の違い、といったことについてディスカッションしながら考えていくといったことを進めています。技術だけでなくマネジメントやガバナンスが大事だよねということを講義の中で実際に理解するということに意味があると思います。

松本　セキュリティにとっては、法律と並んで、人間的な要素というか、心理学や社会行動学的な要素も重要ですね。

後藤　その通りです。２つあると思いますが、一つは大きな事件は内部犯行だったりしますね。するとそこには働いている人の満足度ということがかかわってきます。もう一つは「割れ窓理論」などと呼ばれていますが、ニューヨークのスラム街や地下鉄で、割れた窓や落書きなどを放置すると、ますます治安が悪化していくけれども、それを直すようにしたら犯罪が減った

といったことが言われています。同じように、ちょっとした社内ルール違反、ポリシー違反を認めていると、最終的に大きな情報漏洩に結び付くといった研究もしています。また、サイバーセキュリティではCSIRT（シーサート：Computer Security Incident Response Team）がオペレーション上非常に大事だと言われていますが、あれは組織経営学としてどう取り組むべきなのか、トリアージみたいな、何を緊急に選ぶべきかという判断であったり、どういう対策をとっていくか。最後は広報活動まで関係してきます。そういうことまで含めて、経営学や社会行動学の先生に来ていただいて講義を受けています。

松本　セキュリティをそこまで総合的に扱っている大学はほとんどないでしょうね。

後藤　そういう意味では貴重な学びの場所になっていると思っていますし、ニーズも高まっていると思います。

松本　セキュリティは経営上の課題として考えるべきだと思います。ただ、そういう意味ではセキュリティは負の側面が強くて、経営者はどこまで費用をかけるかという“コスト”の意識に陥りがちです。しかし、セキュリティを扱うことはプラスの要因なんだ、“投資”なんだという意識に変わっていかなくてはいけないと思いますね。

後藤　それは大事な点ですね。例えば有価証券報告書のようなところでもセキュリティ対策をどうしているかを情報開示して、きちんとしている会社は評価する、投資しやすくするという仕組みも必要なのではないかと思います。保険的な考え方というんでしょうか、自動車では安全運転を続けていれば保険料が安くなるということがありますね。企業活動においても、セキュリティ対策をきちんとしている企業は評価され、投資家が積極的に投資するという文化があるべきだと思います。

松本　運転免許証でも無事故無違反であればゴールド免許になり保険料が安くなるように、企業も長期間セキュリティ事故を起こしていなければ税金が安くなるとか、そういう施策があっても良いですね。セキュリティのプラス面が語られるような取り組みも必要だという気がします。

求められるのはクリエイティビティ

松本　最後に現在はセキュリティ人材が13万人も不足しており、2020年には19万人にも達すると言われています。早急な人材育成が必要だと思いますが、どういうスキルが求められるとお考えですか？

後藤　エンジニアに絞った言い方になりますが、必要なのは、創造性、クリエイティビティだと思います。物を作るときはすべてそうだと思いますが、バラバラにあるものを形のある物にしていく力です。問題解決のスタイルもそうですね。ある事象が起きているときに何が起こっているのかについて仮説を立てる。仮説をクリエイトして、検証して、間違っていたら修正し、情報を収集しながら目的の物を作り上げていく。自分のプラン、戦略に基づいて、それを解決していく。そのようなクリエイティビティが必要なのです。営業の人がマーケットを分析して物を売るときも同じです。ですからセキュリティの教育も総合教育なのだと思います。教科書にはない世界なんです。「OSの勉強をしました、ランゲージの勉強をしました、データベースの勉強をしました」でも、セキュリティの問題は全体に絡んできてしまう。物を作るときも、インシデントに対応するときも、何がいけないんだ、何が起きているんだ、ということを様々な知識を組み合わせ、様々な仮説をクリエイトしていく、その意味でのクリエイティビティが非常に重要なのだと思います。

松本　ある意味ではシステム思考ですね。個別の要素で考えるのではなくてシステム全体で俯瞰してみて開発設計していかなければいけない。IPAでもシステムズエンジニアリングをスタートさせてその重要性を考えてきていますが、まさにセキュリティの世界がそうなのですね。

後藤　大事なのは、上から俯瞰する全体的な視点と個別のしっかりした知識です。そこを目指さなければいけません。

松本　高度ですね。確かにソフトウェアだけ分かっていてもだめで、ハードウェアやネットワークなどの知識がないと全体のセキュリティ設計はできない。そう考えると人材育成はますます難しいという印象ですが、産学が連携した育成の取り組みを更に強化していく必要があるのでしょうね。

　グローバルに活躍できる人材の育成という点ではいかがですか？　企業もグローバル展開していますし、海外も含めてセキュリティが分かる人材というのはどうやって育成していったら良いのでしょうか。

後藤　大事なポイントですが、なおいっそう難しいテーマですね。簡単にはいかない。米国、英国、イスラエルなどはサイバーセキュリティへの取り組みが盛んです。交流しましょうということで海外の大学と国際交流協定（MOU）を結んで情報交換をしています。具体的には、例えばイギリスのロイヤルハロウェイに若手教員が１年間勉強に行ったりしています。イスラエルのベングリオン大学とも情報交換をして、カリキュラムや教え方などについて、お互いに見えるようにしようと話しています。また今後はASEANに交流を広げていくつもりです。留学生の派遣の後押しのような形でASEANにおけるセキュリティ人材の育成に貢献しよう、と考えているところです。

松本　セキュリティは一国だけの問題にはとどまらない。世界的にも連携して取り組んでいかなければいけない課題ですから、そういう意味でも日本はもっと世界に貢献したいですね。大変よく分かりました。本日は貴重なお話をありがとうございました。