日立システムズとともに産学連携の
セキュリティ人財育成の
取り組みを続ける

布広永示
インタビュー

工学博士
東京情報大学 学長
学校法人 東京農業大学 理事

取材・文・撮影＝吉澤亨史
編集＝斉藤健一

写真提供：東京情報大学

この春、東京情報大学の学長に就任した布広永示氏は、17 年間の日立製作所勤務を経て、大学の教員へと転身。以来、日立システムズとの産学連携を 11 年にわたって継続しており、多くのセキュリティ人財を輩出している。IT や IoT のセキュリティ知識を備えた人財は、デジタル化が進むあらゆる業界で高い能力を発揮すると考えられる。今回は、布広氏に産学連携や人財育成、今後の取り組みなどについてお話を伺った。

11 年間にわたって
日立システムズとの連携で人財を輩出

吉澤（以下 Y）：まず、経歴についてお願いします。

布広（以下 N）：大学で博士課程を経て、1985 年に日立製作所に入社しました。以降、2002 年 3 月までの 17 年間、一貫してスーパーコンピューター関連の開発に携わってきました。そして、2002 年 4 月に東京情報大学に移り、主に言語処理や、人工知能を取り入れた学習支援システムの研究に取り組んできました。東京情報大学は、学校法人 東京農業大学が 1988 年に設立した大学です。2002 年当時は助教授でしたが、2007 年に教授となり、以降は情報サービスセンター長、大学院総合情報学研究科委員長、先端データ科学研究センター長、副学長などを経て、2023 年 5 月から東京情報大学の第 7 代目となる学長、また学校法人 東京農業大学の理事に就任しました。

Y アカデミアでのキャリアは一環して東京情報大学なのですね。

N 日立製作所勤務時代の縁から、2011 年に日立情報システムズ（現日立システムズ）と産学連携の話が持ち上がりました。企業が持っているノウハウを大学教育に活かし、そして学修した卒業生を企業へと送り出す取り組みです。

Y その産学連携がサイバーセキュリティに関わるきっかけになったのでしょうか。

N 2011 年当時、わが国のセキュリティ人財不足がさまざまなところで指摘されており、内閣府が人財育成強化のために産学連携を推進していました。当時、防衛関連企業へのサイバー攻撃が発覚し、大々的に報じられたり、2020 年の東京オリンピック誘致を目指している時期でもあったりしたことから、サイバーセキュリティが社会全体の課題になっていました。

Y 2011 年が政府のサイバーセキュリティに対する取り組みの転換点だと言うセキュリティ業界関係者は多いですね。

N サイバー攻撃に対する技術的な対策の不足だけでなく、サイバー攻撃を受けた後に何をすれば良いのかを適切に判断できる情報セキュリティ人財の不足も明らかになりました。一方で、大学におけるセキュリティ教育はセキュリティ技術の理論が中心で、セキュリティ技術者に必要な実践的な教育内容が不足していたのです。これでは産学連携の目的である、企業に必要な人財を即戦力として送り出すことが難しくなってしまいます。そこで、持ち上がったのが、日立システムズとの産学連携の話です。2013 年に東京情報大学で第 1 回目のサイバーセキュリティ人財育成のための授業が開始されました。今年で 11 年目となります。

Y 11 年も継続されているのは素晴らしいです。

N サイバーセキュリティの人財育成には、セキュリティ技術の理論だけでなく、実際に企業の現場で起きている問題を活用した実践的な技術を学ぶ必要があります。そこで日立システムズと連携し、講師の派遣、研究課題の提示、研究のサポート、研究成果の実証、そして、セキュリティ関係の評価基準などをしていただいています。東京情報大学からは、設備が整っていることから教育環境の提供や活用の機会を設けているほか、研究活動の推進、そして質の高い人財を送り出すことに努めています。これらの活動で使う教材は日立システムズと共同で開発していて、研究成果も共有しています。

セキュリティ人財育成における 3 つの課題

Y 現在の日本のサイバーセキュリティ人財の状況と課題について教えてください。

N IPA（独立行政法人 情報処理推進機構）から「情報セキュリティ白書 2023」が公開されています。それによると日本における 2022 年のサイバーセキュリティ関連従事者は約 38.8 万人と推定されるが、まだ 5.6 万人不足しているとあります。

Y 常に不足している状況が続いていますね。

N 増えてはいるのですけどね。サイバーセキュリティ人財育成の課題については、大きく 3 つあると考えています。1 点目は、サイバーセキュリティの技術者に求められる知識が広範囲になっていることです。IoT はあらゆる業界で採用されていますし、DX の推進によってデジタル化が進み、多くの企業がテック企業へと変わっています。それらの技術をすべて習得しながらサイバーセキュリティを実施していくことは非常に困難だと思います。2 点目は、セキュリティ技術者の評価が十分ではないということです。企業はセキュリティ技術者の重要性を強く認識しているのですが、ビジネスとして考えたときに、収益面での存在感や価値観に対して、経営層がもっと真剣にセキュリティに取り組むべきだと思います。特に、サイバーセキュリティの運用への対価が少ない印象があります。

布広永示（ぬのひろ・えいじ）
1985 年日本大学大学院生産工学研究科博士後期課程単位取得満期退学（数理工学専攻）。株式会社日立製作所勤務。1987 年工学博士（日本大学）。2002 年東京情報大学助教授。2007 年同大学教授。2023 年同大学学長、および学校法人 東京農業大学理事に就任。

Y 確かに、経営から見るとセキュリティは利益を生み出しませんから、コストとして捉えられ、重視されないことも多いと聞きます。

N 3 点目は、セキュリティエンジニアの仕事に対して学生が明確な目標を持ちにくいという点にあります。学生に聞くと、情報分野では成果を競うことがよくあります。例えば、コンピューターであれば、性能や操作性をいかに上げていくかという競争があるわけです。その効果は実際に目に見えますし、体感もできます。また、運用面におい

てもいかに業務効率を上げるかという競争があります。しかし、サイバーセキュリティはそういう感覚を持つことが難しいのです。

Y そうした日本のサイバーセキュリティ人財の課題に対して、東京情報大学では特にインシデント対応ができる人財にフォーカスしています。取り組んでいること、工夫していることはありますか。

N 日立システムズとの連携が始まった 2011 年当時は、セキュリティはネットワーク分野の一部でした。そのため、学生がセキュリティ人財に興味を持ってもらうところから始める必要がありました。そこで、サイバーセキュリティ人財育成の認知度向上のために 3 つのポイントを挙げて啓発活動を行いました。まず「動機付け」です。サイバーセキュリティ人財の不足が深刻化している状況であるため、キャリアパスが充実しており、就職しやすいこと。次に「充実感」。セキュリティ人財は国家的に推進されている事業であるため、やりがいがあること。そして「学習意欲」。サイバーセキュリティ技術を習得することで、幅広い情報技術に関する知識が身につくことです。

Y 講座には、具体的にどのような内容が盛り込まれているのでしょうか。

N データ解析、AI、システム開発などが挙げられます。こうした内容をサイバーセキュリティの人財育成の枠組みの中で学習することで、達成感が得られるようになりますし、就職にも役立ちます。これを 2013 年から続けていることで、学生が興味を持って講座に参加してくれるようになったと思っています。また、単位認定講座として「IT システムセキュリティ・インシデントレスポンス概論」を設けました。CSIRT の役割とセキュリティインシデント発生時の対応フローおよび事前準備、デジタルフォレンジックの基礎とマルウェア解析入門で構成されています。

産学連携を最大限に活かした単位認定講座

Y 講座は日立システムズの現役セキュリティエンジニアが講義を担当しているのですよね。

N はい。実際に日立システムズで調査対応を行ったインシデント事例や、日々収集しているサイバーセキュリティの新たな情報を反映し、毎年ブラッシュアップしているので、学生にとっては新鮮な内容だと思います。受講した学生の反応も良く、「実際に挙動を見ながら解析を行うことができた」などの声があります。現役のセキュリティエンジニアによる講義は、学生によい緊張感をもたらしてくれます。さまざまな講師と触れ、セキュリティは需要があるし、関心が高いということを肌で感じてくれたと思います。また、単に単位認定講座を立ち上げるだけでなく、「インシデントレスポンス概論」といった公開セミナーも開催しました。こうした取り組みには、地域の方々をはじめ、防衛関係者や法執行機関の方々にも参加していただきました。

Y 学生に対して何かフォローしていることなどありますか。

N 講義を受けて身についた能力、成果を実感してもらうために、「MWS Cup」に参加させています。MWS Cup は CSS（情報処理学会主催のコンピュータ・セキュリティ・シンポジウム）内の企画として開催されるセキュリティコンテストで、日立システムズと東京大学や明治大学、静岡大学などの学生連合などが参加しており、優勝すると SECCON（日本ネットワークセキュリティ協会内の有志によるセキュリティコンテスト）への出場権が得られます。2014 年と 2015 年は東京情報大学の学生がメンバーとして加わったチームが優勝し SECCON に出場しています。

Y 実績も残されているわけですね。これまで輩出

した人数はどのくらいですか？

N PC の台数や環境の問題で、講座は 40 名に抑えています。開始した当時は 350 名を目標にしていましたが、それからの 11 年で約 400 名が単位認定を受けています。当初の目標は達成しましたが、さらに継続していきたいと考えています。

Y 最近、高度セキュリティ教育を受けた人財がサイバー攻撃をして逮捕された事件が注目されましたが、セキュリティ教育は技術と共にリテラシーやモラルも併せて高めていく必要があると考えます。東京情報大学ではリテラシーやモラルについて、どのような方針を持たれていますか。

N 東京情報大学では、情報モラルに関する講習を学部に関係なく全学を対象に実施しています。学生はみな学内ネットワークを使うわけですから、正しい使い方を学ばなくてはなりません。この講習を受けてレポートを提出しないと、学内ネットワークのアカウントが発行されません。これまでに数人、アカウントが停止されています。単位認定講座においては、講義の最初に合意書を熟読させて署名をしてもらいます。講義で扱うセキュリティ関係の情報や習得する技術は、実際に使ってしまうと社会に大きな影響を及ぼす危険性が高いためです。合意書には、技術を悪用した場合に受ける法的措置についても明記されています。

これからのセキュリティ人財に必要になるものを見極めていく

Y 2023年4月、東京情報大学は総合情報学部を「情報システム学系」「データサイエンス学系」「情報メディア学系」の 3 学系 9 研究室の新体制としました。これを含めて、今後の展望について教えてください。

N 情報システム学系はゲーム・IoT 研究室、AI・システムデザイン研究室、ネットワーク・セキュリティ研究室の 3 つ、データサイエンス学系は心理学研究室、データサイエンス基盤研究室、生命・環境科学研究室の 3 つ、情報メディア学系は経営情報研究室、メディアデザイン研究室、メディア文化研究室の 3 つとなります。ただ、セキュリティを実践的に学ぶ上で、どのような科目が必要になるのかは、柔軟に対応していくつもりです。また、学ぶべき技術をセットにして計画的に学生の理解を促すようにしています。今後は、こうしたセットを達成目標に応じてグルーピングしていくことも重要だと考えています。

Y 具体的にはどのようなイメージでしょうか。

N サイバーセキュリティの人財育成に必要な教育内容を広範囲に考えて、フォレンジックの講座に横断的な技術教育の要素を加え、知っておくべき関連技術を拡大するということです。例えば、ディープラーニングでは、セキュリティの挙動、兆候などを評価するために、AI を活用する研究が増えています。また、情報システムのセキュリティ対応においても、ソフトウェアやネットワークの構成や DX 化などについて理解しておく必要があります。そうした関連技術の知識をセットにしてサイバーセキュリティの教育プログラムを考えていくことが必要だと思います。

Y より実践的なカリキュラムになりそうです。その反面、基準がないので難しいとも言えますね。

N はい。産学連携の中で企業側から「こういう技術レベルのエンジニアが必要なので、こういう内容の教育をしてほしい」などの提案していただきながら教育内容や達成度の検討を進めていくことが良いと考えます。

Y サイバーセキュリティ人財の育成や確保に苦労している組織に対して、どのように取り組めばいいのか、アドバイスをお願いします。

N 最近では、リスキリングやリカレント教育に大学を活用するケースが増えている印象があります。最近の例でいえば、日立システムズの関連企業に就職した東京情報大の卒業生が企業人のまま本学の博士課程に在籍しています。こうした形でセキュリティ人財を育成する方法もあると思います。業務に支障がない範囲でエンジニアが博士の学位を取得するといったことも良いことだと考えます。

Y セキュリティ人財をどんどん輩出されることを期待しています、今回はありがとうございました。