ISSUES 2

IoT時代を支えるサイバーセキュリティ
「人」と「技術」の両面で進む慶應義塾大学と日立の共同研究

慶應義塾大学大学院
メディアデザイン研究科 教授
砂原 秀樹

×

日立製作所 サービス＆プラットフォームビジネスユニット
セキュリティ事業統括本部長
斎藤 浩

デジタライゼーションの進展に伴い，サイバーセキュリティの重要性がますます高まっている。そうした状況の中，慶應義塾大学と日立は多種多様なシステムがつながる超スマート社会の実現に向けて，サイバーセキュリティ分野の共同研究を開始し，人財育成や情報共有基盤の技術開発を行っている。
この共同研究を主導する慶應義塾大学の砂原秀樹教授と日立のセキュリティ事業を統括する斎藤浩が，IoT時代に求められるサイバーセキュリティの課題や産学連携による取り組みなどについて語り合う。

サイバー空間の広がりと脅威の多様化

斎藤　IoT（Internet of Things）時代になってオープンとコネクトのトレンドが浸透する一方，サイバーセキュリティの重要性が増してきています。砂原先生は，JUNET（Japan University Network）やWIDE（Widely Integrated & Distributed Environment）プロジェクトを通じ，黎明期から日本におけるインターネットの構築とその研究に携わってこられましたが，サイバーセキュリティの歩みをどのように捉えられていますか。

砂原　日本のインターネットの歴史がスタートして今年（2018年）で30年と言われます。1988年7月，東京大学と慶應義塾大学，東京工業大学の3つの大学が，いわゆる今のインターネットの形でつながったのです。そして米国とつながった1989年1月の直前，「モリスワーム」というコンピュータウイルスが猛威を振るいました。幸い

日本には被害が及ばなかったものの，セキュリティの担保という課題と真剣に向き合うきっかけになりました。当時は，ディスクローズする範囲と価値，さらにそれによって引き起こされる社会的な影響を含めて検討する必要性などを議論していたことを覚えています。

斎藤　今やインターネットは社会基盤になったと言えますが，悪意を持つ人間がいるという前提は初期の段階からあったのでしょうか。

砂原　最初はそういう前提はありませんでした。しかし，いたずらからスタートして，それがエスカレートするケースが多々あります。最近大きく報じられた仮想通貨「NEM」の流出もそうですが，価値とつながるところには悪意は潜入する。ですから，セキュリティインシデントの対応にあたるJPCERT/CC（Japan Computer Emergency Response Team Coordination Center）のような組織を設ける必要があるだろうと初期の頃から仲間と話していましたね。

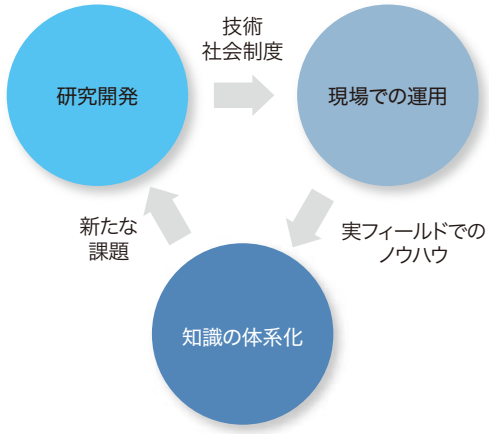
斎藤　日立も，もともと性善説で考えていました。外部からの攻撃には15年ほど前から対処するようになりましたが，そのときのコンセプトは，外からの侵入をきちんと防げば，内部は自由にしていても大丈夫というもので，それ以降も内部はなるべく自由にして情報の伝達を早くするというのを続けていたわけです。

ところが，2017年に世界中に被害をもたらしたランサムウェア（身代金要求型ウイルス）によるサイバー攻撃では，そこを突かれました。感染源は海外のグループ会社の機器で，昔のワームであれば伝達速度が遅く，発覚してからでも対策を取れたのですが，今回はあっという間にワームが世界中のネットワークを駆け抜けました。外部の脅威への対策はもちろん，内部の対策の重要性を改めて痛感しました。システムの脆弱性に加えて，企業の内部に存在し得る悪意にも本気で取り組まなければならない時代になりましたね。

図1｜慶應義塾大学と日立の共同研究のフレームワーク

高度化・大規模化するサイバー攻撃に対するセキュリティ運用管理や，個人情報の安全性に関する技術の開発などに共同で取り組んでいる。

日立製作所	品質，技術力，実フィールドでの経験
慶應義塾大学	インターネット研究を先導，IoTを含む研究開発，技術のみならず社会制度を含む研究実績



産学官連携がセキュリティ人財育成のカギ

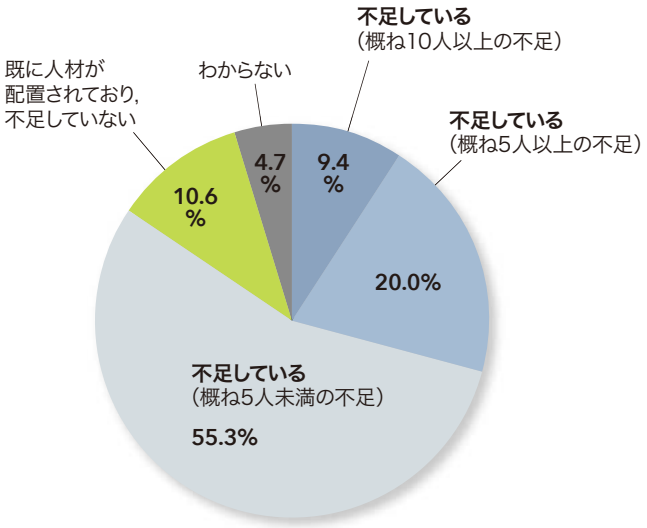
砂原　私は常々，最大の脆弱性は「人」だと強調しています。本人の年齢とは関係なく，大学にはきちんとした大人もいれば，考え方が未熟な者もいます。教育を受けているからといって安心はできず，例えば著作物の違法アップロードに対する意識が薄い学生がいるのも事実です。そういうときには，その行為の違法性をきちんと認識させるなどのケアをしています。

また，技術の観点でいえば，20年ほど前からファイアウォールなどの対策を講じる文化が育ちました。当大学の場合，ファイアウォールが世の中一般とほぼ変わらない部分から，少しフォーマライズされている部分，完全にフォーマライズさ

砂原 秀樹
1988年慶應義塾大学理工学部博士課程修了。電気通信大学情報工学科助手，1994年奈良先端科学技術大学院大学情報科学センター助教授を経て，2001年から教授。2005年情報科学研究科教授。2008年4月より現職。村井純氏（慶應義塾大学環境情報学部教授）らとともに，1984年からJUNET，1988年からWIDEプロジェクトを通じて，日本におけるインターネットの構築とその研究に従事。2005年より東京大学江崎浩教授と共にインターネットを通じて環境情報を共有するLive E!Projectを開始。
現在は，パーソナル情報を安心・安全に利活用するためのフレームワーク「情報銀行」プロジェクトを推進中。

図2｜情報システム部門における サイバーセキュリティ人財の不足

情報システム部門では，調査対象企業の約85%においてサイバーセキュリティ人財が不足している。



出典：内閣サイバーセキュリティセンター
「平成28年度企業のサイバーセキュリティ対策に関する調査（概要）」

れている部分まで分けてあって，かなり大学も変わってきたと言えますね。

斎藤　2016年から慶應義塾大学と日立がセキュリティ分野の共同研究を行うようになって，大学と企業は違う点も少なくないと感じました（図1参照）。一つは，大学は大学内にある脅威（マルウェアなど）が大学外に影響を出さない（加害者にならない）ことに力を入れている。

一方，企業は外の脅威が中に入らない（被害者にならない）ことに力を入れている。そして，企業の人財は大学の学生に比べて同じ組織に長期間とどまる一方，大学は学生さんを含めてどんどん人財が一新していくということです。現在，日立のセキュリティ関連部門は，若い人財を今後どう育てていくのかという悩みを抱えています。大学のセキュリティ教育は，どのような状況なのでしょうか。

砂原　セキュリティ人財の育成は，確かに喫緊の課題ですね（図2参照）。ここ10年ほど情報セキュリティ教育に携わってきましたが，そこで学んだ

斎藤 浩
1985年日立製作所入社，公共システムの構築に長らく従事。2013年日立中国情報統括および北京日立北工大信息系統有限公司董事長，2015年公共システム事業部副事業部長を経て2016年より現職。
現在，サービスプラットフォーム事業本部セキュリティ事業統括本部の統括本部長として日立のセキュリティ戦略を統括。

学生が企業で活躍しているだけでなく，ランクアップするために大学に戻ってスキルを身につけていくというサイクルが回り始めているところです。例えば，JPCERT/CCなどの組織で活躍をしている人財も出てきています。

こうした育成プロセスでは，人財を生み出して終わりではなく，ある種の品質保証が必要です。ブランディングと呼んでいますが，われわれが学生をセキュリティ人財と認めたことを一つのブランドとして，その人がレベルアップしていく様子を外に見せるとともに，連携している企業の中でも見えるようにすることも大切だと考えています。

斎藤　日本では，いったん企業に入ると大学で勉強し直すことは少ないですが，米国では大学と民間，さらに官庁も含めて人財の交流が盛んですね。人財の絶対数の違いもありますが，おっしゃるようなサイクルを回していくことが非常に大事だと思います。

砂原　ええ，人財は数より質が重要です。最終的にCIO（Chief Information Officer：最高情報責任者）やCISO（Chief Information Security Officer：最高情報セキュリティ責任者）になるかはともかく，そういうプロセスを踏む人財を育成するためには大学や企業だけではできないので，官も含めてうまく連携させていきたいですね。

斎藤　こういったサイクルを回すためには，やはり企業の側でキャリアアップの仕組みを整備していくことが必要ですね。

砂原　そのあたりも日立との共同研究の中で考えていきたいと思っています。大学が質を担保しながらセキュリティ人財を育て，企業がそうした人財を採用するようになれば，学生の意欲も向上するでしょう。大学で学んだことが企業に評価されるわけですから。

斎藤　共同研究のねらいの一つは，そこにあります。一般的な採用プロセスで行う数回の面談では，セキュリティ人財のような高度に専門的な職種に適する学生を見いだすことは困難です。しかし，今回のプログラムのように学生の人柄やスキルなどを見ながら指導教員の「お墨付き」も判断材料

にできるのは，実にありがたいですね。

実践的スキルを養う きめ細かな演習

斎藤　慶應義塾大学では，情報セキュリティ教育に力を入れているとお聞きしています。大学入試にはセキュリティの科目がありませんが，学部生のセキュリティ知識を修士課程レベルまで引き上げるためにどのような工夫をされていますか。

砂原　SFC（湘南藤沢キャンパス）の総合政策学部・環境情報学部では，選択科目ですが「情報」の試験があります。ほかの私立大学でも「情報」が入学試験の科目となっているところがあり，ある程度の知識を備えて入学する学生が出始めています。

また，当大学の例でいえば，理工学部とSFCの学部3年生に基礎的なセキュリティ知識を学ぶコースを設けていて，演習の授業もしています。学内でペネトレーションテスト（侵入テスト）やウイルス分析をしたり，セキュリティソフトウェアメーカーのカードゲームを体験させたりすることなどの演習を通じて実践的な技術を身につけさせています。提携企業の現場で行う際は，模擬的な秘密保持契約を締結させて，倫理教育の一環にするといった仕掛けも盛り込んでいます。日立との共同研究では，企業で何が必要でどうステップアップしていくかなど，私もいろいろと教えられ，企業に求められる学生を育てるための多くのヒントを得ることができました。

斎藤　大学で初めて情報セキュリティを勉強するというより，高校ぐらいから情報処理の基礎を固める形であれば大学での飛躍が一層期待できるのではないでしょうか。その点で文部科学省の施策をどのように見ておられますか。

砂原　文部科学省は情報セキュリティ教育の重要性をよく理解していて，さまざまな施策を推進しています。例えば，現在私も関わっているSecCapというプログラムのほか，社会人向けの情報セキュリティ教育もサポートしています。SecCapの大学連合は，セキュリティチームの数が20以上に達しており，最終的には40大学ほどになる予定です。年間100人程度の人財育成がすでに4年続いているので，400～500人が世に出ていることになります。今後，修了認定された学生が教える側に回れば，一層うまくサイクルが回るはずです。

斎藤　われわれ企業は，2020年に向けて重要インフラを守るため，経済産業省とともにサイバーセキュリティの強化に取り組んでいるのですが，そこは文部科学省から経済産業省へとうまくバトンタッチされているわけですね。

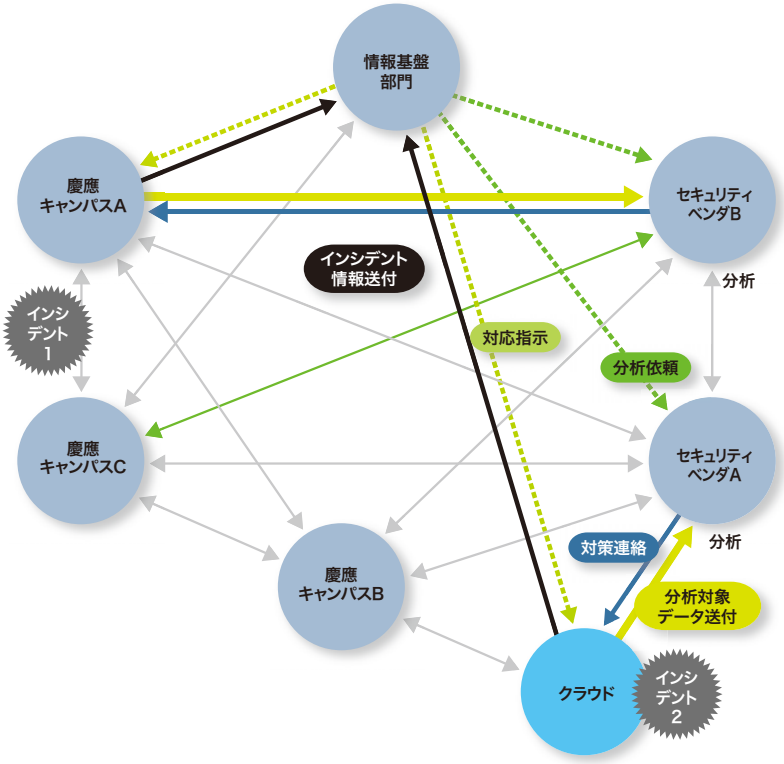
情報共有と国際連携を軸に セキュリティ体制の確立を加速

斎藤　ところで，サプライチェーンや取引先のことを考えると，サイバーセキュリティにおいては他の組織との連携やグローバルな視点も欠かせません。セキュリティ情報のインテリジェンスを含め，常にグローバルな情報を広くつないでいく必要がありますが，企業が前面に出ると営利目的だと見られがちで，ネットワークづくりでは学術的な立場からのアプローチに期待しています。こうした点に関してはどういった活動をされているのでしょうか。

砂原　一つは，情報共有の取り組みです。サイバー空間はボーダレスですから，防御する側も組織の垣根を越えて連携する必要があります。しかし，情報漏えいなどの危険もあるため，セキュリティの情報共有は難しい。そこで，当大学と日立で分散型セキュリティオペレーションと呼んでいる，セキュリティインシデントの情報を共有する基盤技術の開発に取り組んでいます（図3参照）。インシデント対応を自動化し，分析を依頼する処理を1秒以内で完了するという実証結果を得るな

図3｜分散型セキュリティオペレーション構想

各組織で自律分散的にインシデントに対処し，必要に応じて連携する。



ど，共同研究の成果が現れ始めているところです。

斎藤　日立を攻撃したランサムウェアも，事前にその動きを知ることができていたかもしれませんね。

砂原　予兆は見えたはずです。日立と慶應義塾大学の共同研究は，もっと大きな枠組みにしたいと考えており，2017年から中部電力株式会社に加わってもらいました。今後，IDS（Intrusion Detection System：侵入検知システム）やITも活用しながら，重要インフラなどをサイバー攻撃から守るセキュリティオペレーションの実現をめざしていきます。

そしてもう一つは国際連携です。2016年，当大学の呼びかけで米国，英国，日本の大学との間で「InterNational Cyber Security Center of Excellence（INCS-CoE）」を設立しました。国際シンポジウムを開催するなど，情報や成果を共有する場として機能しています。さらに，中国・韓国・日本という枠組みでもアカデミズムの中でサイバーセキュリティの議論が進んでいて，こうした大学間，あるいは企業間も含めて，結節点となるのが大学の役割だと考えています。

斎藤　共同研究によって，日立もできることや視野が広がってきました。冒頭の話に戻ると，世の中がつながりオープンになっていく時代は，防御側の情報ももっとつながっていく必要がありますね。そういう意味からも，「人」と「技術」に限らずこの産学連携を一層深めていきたいですね。

砂原　私も，共同研究が期待できる成果を生み，かつ社会を動かす原動力になればと思っています。

斎藤　これからもよろしくお願いいたします。本日は貴重なお話をしていただき，ありがとうございました。