国立情報学研究所ニュース　ISSN 1883-1966（Print）　ISSN 1884-0817（Online）

NII Today

National Institute of Informatics News

75
Mar. 2017

NII Interview

求む、サイバーセキュリティ人材

［内閣官房 NISC 副センター長に聞く］
セキュリティで「学問の自由」を守れ

実践型プログラムでめざすもの

［北海道大学 情報基盤センター］
今、大学に求められる
情報セキュリティ対策とは

Feature

サイバーセキュリティ人材を育てる

脅威から学術ネットワークを守るために

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

求む、サイバーセキュリティ人材

監視と人材育成の両輪で学術機関を守る

喜連川 優［国立情報学研究所 所長］
聞き手：**若江 雅子氏**［読売新聞社 編集委員］

標的型攻撃で情報を盗まれたり、サイトを改ざんされたり――。大学などの研究機関は日々、サイバー攻撃の脅威にさらされている。こうした中、NII が今夏、スタートさせるのが学術情報ネットワーク「SINET5」にきたサイバー攻撃を検知し、その情報を大学などに提供する体制だ。緊急時には対応もサポートし、やり取りの中で大学のセキュリティ人材育成も狙うという一石二鳥の作戦である。喜連川優所長にその狙いを聞いた。

喜連川 優
KITSUREGAWA Masaru

若江　大学のセキュリティ、甘いですねえ。最近も深刻な事故が次々と起きています。

喜連川　悩ましいのは、大学では自由に研究できる風土が重視され、企業のような厳格な情報管理がなじみにくいことです。さまざまな国の研究者を受け入れたり、各自が持ち込んださまざまなコンピュータを大学のネットワークにつないだりする必要もあります。一方で、研究データなど重要な知的財産を保有しており、セキュリティの確保も急務になっています。

若江　大学の中にセキュリティを担う人材が育っていないとの指摘もあります。

喜連川　大学で「IT」というと、かつてはスーパーコンピュータがその象徴でしたが、時代とともに計算サービスよりネットワーク接続サービスの重要性が増し、それに従ってセキュリティの必要性も高まってきました。ところが、そうした需要の変化に組織が十分対応できず、多くの組織ではコンピュータやネットワークの運用担当者が専門外のセキュリティも担う、という状態が生じています。人材育成は急務ですが、国内に1000 を数える研究機関がある中で、それぞれの組織がセキュリティのスペシャリストを準備するのは難しい状況です。

若江　そこで考えたのが今回の取り組みですね。

喜連川　大学や研究機関をつなぐ SINET5 上に、サイバー攻撃を検知するシステムを整備して NII が 24 時間 365 日通信を観測し、攻撃情報や疑わしい通信先などの情報、分析結果などを各組織に伝えます。各組織で対応が難しいケースには緊急度に応じて NII がサポートもします。

若江　つまり、NII に SOC（セキュリティ・オペレーション・センター）を設けて監視サービスを提供するということですね。政府機関の通信はすでに内閣サイバーセキュリティセンター（NISC）が監視していますし、独立行政法人には情報処理推進機構（IPA）が監視サービスを提供することになりましたが、大学にもいよいよ同様のサービスがスタートするのですね。

喜連川　日本でも一部の業界で始まっているセキュリティ情報の共有組織 ISAC（Information Sharing and Analysis Center）の大学版をイメージしています。攻撃者は同じ時期に同じような業界を狙う傾向にあるので、一つの大学で攻撃が発覚した時には、実は他の大学も狙われている可能性があります。でも、被害情報はなかなかオープンになりにくいものです。今後は、NII がマルウェア（悪意のあるプログラム）や疑わしい通信などを検知したら該当の組織に通知した上で、被害組織名を伏せた状態で、防御に有益な情報を他の組織と共有したいと思っています。

若江　被害組織を匿名化すれば情報は流通しやすくなりますね。他の大学も、マルウェアがどんな挙動をするのか、通信先はどこか、といった情報が分かれば対策を取りやすくなります。

喜連川　今回のもう一つの狙いは、各組織のセキュリティ担当者のスキルアップです。まず解析システムの使い方の講習を受けてもらい、その後は日々、NII から観測データや分析結果の提供を受けたり、問題が発生すれば対処のサポートを受けたりしながら、OJT（オン・ザ・ジョブ・トレーニング）方式で実力をつけてもらうのです。大学の教員や学生を客員研究員やインターンとして受け入れ、トレーニングを実施することも検討しています。

若江　監視サービスの対象は？

喜連川　国立大学と大学共同利用機関法人が対象です。SINET5 に加入している国立大学は 86、大学共同利用機関は 16 で計 102 機関あり、現在、その 8 割程度が手を挙げています。

若江　SINET5 には公立大や私立大、高専など計 844 組織が加入していますが、1 割しか参加できないんですね。

喜連川　今回の事業は国立大学法人の運営費交付金でまかなわれるため、私大や高専などは対象外です。それに予算的にも現状が精一杯。今年度の予算は 7.8 億円で、検知のための機材すらまだ当初予定の 3 分の 1 しか買えていません。

若江　え？ SOC ルームの賃料も機材も人件費も入れて、たったそれだけですか？

喜連川　お金がない分、知恵を絞って頑張りますよ。

若江　ところで、今回の監視では膨大な攻撃データも入手できますね。

喜連川　それも今回の目玉。監視で得られたデータは、被害者を特定できないよう加工した上で、学術機関の研究者に無償提供します。しかも観測から 1 週間以内に出すつもりです。今も研究者コミュニティでマルウェアを提供しあう枠組みはありますが、早くても 1 年はかかっています。1 日に数万という新しいマルウェアが作り出される時代、1 年もたてば攻撃パターンは大きく変わってしまいます。セキュリティはスピードが命。その意味で、今回のデータ提供の意義は大きいでしょう。

若江　IoT 機器への攻撃研究にも役立ちそうですね。

喜連川　例えば、SINET5 と商用ネットワークの接点に特定のスキャンを検知するプログラムを組み込めば、IoT 機器への攻撃者の狙いも見えてくるかもしれません。今はデータが研究の成否を左右する時代です。大量でフレッシュなデータの提供により、日本のセキュリティ研究に貢献したいと思っています。

（写真＝佐藤祐介）

インタビュアーからのひとこと

数年前、大学のセキュリティを考える勉強会に顔を出したことがある。参加者の多くは、それぞれの大学でシステムやネットワーク運用を担いつつ、セキュリティも「ついでに」と任された教職員。なのに、専門的な教育を受ける機会もなければ予算もない。しかも大学の自由な雰囲気の中で厳格な情報管理は嫌われて……。サイバー攻撃が増えるなか、どの担当者も焦っていた。

そんな悩みを見聞きしていただけに、今回の取り組みには期待している。何より、各大学で孤軍奮闘してきた担当者たちにスキルアップや情報共有の道を開く意味は大きい。残念なのは対象が国立大などに限定されること。私大や高専にも拡大できないのだろうか。

観測データの研究活用にも期待している。日本のセキュリティを考える時、攻撃データが圧倒的に不足していることはよく指摘されることである。例えば、海外では当然のように構築されているマルウェアのデータベースさえ不十分で、研究者らは海外から高額なデータを買っている。今回の試みが、日本のいろいろな「タブー」を見直すきっかけになるといいのだけれど。

若江 雅子 WAKAE Masako

1988 年青山学院大学卒業、読売新聞社入社。社会部を経て 2014 年から編集委員。

セキュリティで「学問の自由」を守れ

相次ぐ攻撃踏まえ、検討の加速を

三角育生氏

［内閣官房 内閣サイバーセキュリティセンター（NISC） 副センター長 内閣審議官／
国立情報学研究所 客員教授（2017年4月から）］

「サイバーセキュリティの確保はそれ自体が目的ではなく、学術研究、ひいては学問の自由を守るための手段である」。内閣官房内閣サイバーセキュリティセンター（NISC）で副センター長を務める三角育生内閣審議官は、学術機関にとってのセキュリティの意義をこのように語る。学術機関は守るべきものを明確にした上で、必要な資金や人材などのリソースをそれに投入するべきであると提言する。

研究データをサイバー攻撃から守る

――近年、日本年金機構などの公共機関が、相次ぐサイバー攻撃を受けているため、政府はセキュリティ対策に多くの予算を付けるようになりました。

三角　サイバーセキュリティへの意識が高まることは望ましいのですが、セキュリティ対策自体が目的化し、本来守るべきものは何か、の議論がおろそかになっていないかと懸念しています。目的と手段を混同してはいけません。例えば大学や研究機関にとって、学術研究の目的は、世界に先駆けて研究成果を挙げることでしょう。それを世の中の役に立てることができれば、とても素晴らしいことです。

研究成果に関するデータは、特に自然科学系の場合、大半がコンピュータ上にあります。そのデータがサイバー攻撃で盗まれたり、改ざんされたりすると、研究が止まってしまいます。いつ研究の成果を発表するのかといった研究者の研究の自由を含め、研究を守り、学問の自由を守るための「手段」としてサイバーセキュリティの確保が重要なのです。

研究成果は個々の研究者の努力の賜物ですが、その研究環境の多くは国民の税金で支えられています。共同研究であれば、契約上発生するデータを守る義務があります。研究者一人一人が、サイバーセキュリティの確保に対する意識を高める必要があります。

――セキュリティの向上や人材育成に向けた、内閣サイバーセキュリティセンターの役割を教えて下さい。

三角　私が副センター長を務める内閣サイバーセキュリティセンターは、その英語名を「National center of Incident readiness and Strategy for Cybersecurity（NISC）」といいます。この英語名の通り、サイバー攻撃などのセキュリティインシデントに備えて、各省庁のネットワークの監視・監査、サイバーセキュリティ戦略の企画立案を担っています。行政官等の公務員と民間出身者の混成部隊で、当初は70～80人ほどだったのが、ここ2年で大幅に増員し、平成28（2016）年度中に180人規模になる見込みです。

各省庁でセキュリティを担う人材の育成にも力を入れています。各省庁には平成28年4月から審議官クラスのセキュリティ担当を置き、夏には人材確保・育成の計画をつくってもらいました。この計画をもとに職員への教育や訓練を実施し、セキュリティへの知見を高めます。

NISCは、平成27（2015）年、厚生労働省のネットワークを経由した外部への不審な通信を検知し、厚労省に対応を促しました。これが日本年金機構への標的型攻撃の発見につながりました。この事案を受け、サイバーセキュリティ基本法が改正され、NISCの監査・監視の対象が、中央省庁から独立行政法人、一部特殊法人などに広がりました。

――一連のサイバー攻撃事案を受けて、セキュリティの必要性への理解は進んだ一方、具体的な対策には、そのコストをどう捻出するかという問題が立ちはだかっています。

三角　公共機関にせよ民間企業にせよ、サイバーセキュリティはコストではなく、目的を達成するための投資と捉えるべきです。

例えば米国の産業界は、経済発展という目的のためにセキュリティをどう使うか、という問題意識を持っていると承知しています。実は米国では、景気が悪いと企業のIT投資が増えます。これは、米企業はITを、新たな事業を生み出すビジネスイノベーションの道具であり、利益を生み出す投資とみているからだろうと考えます。セキュリティへの出費も、製品やサービスへの信頼を生み、利益に貢献する点で、投資と捉えることができる。一方、日本企業の多くは、ITを主として業務の自動化などによるコスト削減の手段として見ている印象があります。

ITと経営の「橋渡し」をする人材を育てる

三角　なぜ、米国はITをビジネスイノベーションに結びつけられるのか。理由の一つに、企業の幹部候補生の多くが、大学院でMBA（経営学修士）とITのダブルメジャーを取得している点が考えられます。ITと経営の橋渡しをする人材をシステマティックに育成する仕組みがあるのです。このため、サイバーセキュリティについても経営層に適切な助言ができます。

日本では、このような橋渡し人材が不

足しています。ビジネス戦略を立案し、その基礎としてサイバーセキュリティを位置付けるようなものを経営層に進言できる人材を育てる必要があります。

――日本でもセキュリティ人材の不足が叫ばれていますが、エンジニアの話に偏っている印象がありますね。

三角　私が考えるセキュリティ人材は3種類あります。ITを管理する現場のエンジニア、セキュリティへの投資を決める経営層、そして現場のITと経営層とをつなぐ橋渡し人材です。

このうち現場のエンジニアのスキルを高める施策の一つとして、3年で更新となる国家資格「情報処理安全確保支援士」が平成28年10月に新設されました。かつての情報セキュリティスペシャリスト試験の後継となるものです。また、経営層向けには、セキュリティへの意識改革を促す目的で、経済産業省が「サイバーセキュリティ経営ガイドライン」の改訂版を同年12月に公開しました。

その一方、経営層とエンジニアなどの実務者をつなぐ橋渡し人材は、育成が難しく、慢性的に不足しています。米国のように、経営とITに詳しい人材をシステマティックに育てる仕組みもありません。企業や組織の中で橋渡し人材をどう育てていくか、今後の課題になりそうです。

――セキュリティ人材の育成において、NIIや学術情報ネットワーク「SINET」にはどのような役割を期待していますか。

三角　SINETは、学術研究のツールであるとともに、それ自体が高速通信の研究対象でもあります。研究者にとっての使い勝手の良さを維持しつつ、高速通信という先端研究を守るための取り組みが必要になります。

特に、SINETを運営するNIIが果たす役割には期待しています。SINETは常にリアルなデータが流れるため、大学のネットワーク管理者などに向けた実践的なサイバーセキュリティの研修に使えそうです。

学術界は具体的な検討の加速を

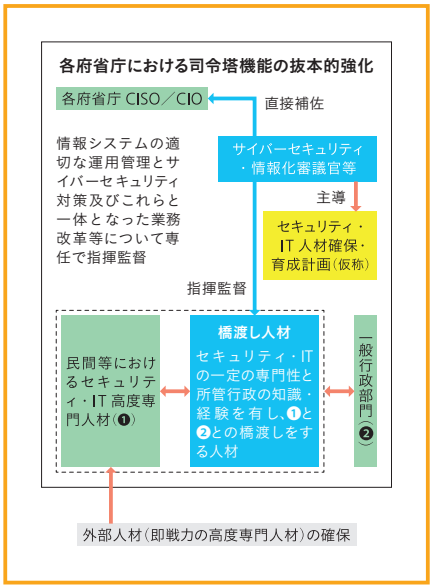
三角　残念ながら平成28年後半に、富山大学など学術機関を対象にしたセキュリティインシデントが相次ぎました[1]。

学術研究をサイバー攻撃の脅威から守るため、人材、資金などのリソースをどこにどれだけ投入するか。どのようにセキュリティ人材を育成するか。まずは学術界で、自主的な検討を加速させることを期待します。

例えば施設面では、東京と大阪にあるSINETとインターネットとの接続点については、重点的に監視する必要があるでしょう。

人材面では、セキュリティの専門家だけでなく、ネットワークの専門家、法律の専門家、それら専門家をチームとして束ねて方針を決める人など、さまざまなスキルを持つ人が求められます。セキュリティに精通した「トップガン」が一人いればセキュリティを保てるわけではありません。こうした具体的な検討を進めていくことが必要になります。

（取材・文＝浅川直輝　写真＝池田亜希子）



図｜政府機関におけるセキュリティ・IT人材の育成

注

［1］富山大学では、水素同位体科学研究センターのPCが標的型攻撃でウイルスに感染し、研究関連ファイルが流出した。防衛医科大学は、大学内のPCがSINET経由で不正アクセスを受けたと報じられた。

三角育生
MISUMI Ikuo

東京大学大学院にて博士（工学）号取得。（独）情報処理推進機構セキュリティセンター長、経済産業省 商務情報政策局 情報セキュリティ政策室長、同省 貿易経済協力局 貿易管理部安全保障貿易審査課長、内閣官房 内閣サイバーセキュリティセンター内閣参事官を経て平成28年6月より現職。

実践型プログラムでめざすもの

NIIのサイバーセキュリティ人材育成プログラムとは

高倉弘喜

［国立情報学研究所 アーキテクチャ科学研究系教授／サイバーセキュリティ研究開発センター長／
総合研究大学院大学 複合科学研究科 教授］

NIIが平成29（2017）年7月から本格的にスタートさせる「サイバーセキュリティ人材育成プログラム」は、一般的な人材育成プログラムとは趣きが異なる。カリキュラムのようなものはなく、座学形式で人材育成を行うものでもない。各大学のネットワーク管理者などが、NIIとの協力体制を取りながら、実際のデータや業務などを通じて、サイバーセキュリティ対策に関するスキルを蓄積し、そうした経験を持つ人材を、全国の国立大学に配備していくというものだ。その目的と概要について、サイバーセキュリティ研究開発センター長の高倉弘喜教授に聞いた。

総合的に判断・実行できる人材を

サイバーセキュリティ人材育成プログラムの端緒は、平成27（2015）年6月に日本年金機構で発生した、マルウェア感染による情報漏洩事件にまで遡る。当時、NIIでは、SINETにおいて、さらなるセキュリティ強化に向けた議論を開始していた時期であり、このタイミングで起こった日本年金機構の情報漏洩は、大学関係者にとって大きな関心事となった。

事件を受けて、文科省は、各国立大学にマルウェア感染がないかを確認するために協力を要請。その結果、複数の国立大学で、同様のマルウェアに感染していた疑いが浮上した。

だが、ここで最も大きな問題だったのは、感染そのものではない。感染が疑われた大学に共通していたのは、それを大学の経営側に報告していなかった点だった。

NII サイバーセキュリティ研究開発センター長の高倉教授は、「どんな大学でも、月に数件はマルウェアに感染しています。でも、駆除できたのは最初に感染したマルウェアだけ、そのマルウェアが後から持ち込んだマルウェアは駆除されていないことが多い。それを完全に駆除できたと判断して、報告をあげなかった例が相次いでいました。深刻な事態に至ってから、慌てて報告していたのです」と指摘する。

ネットワーク管理者やシステム管理者のサイバーセキュリティに対する基本認識に問題があったと言わざるを得ない。

もう一つ、現場における問題は、大学の経営層に対して、マルウェア感染や情報漏洩の危険性について、適切に報告できるスキルを持つ管理者が少ない点であった。

「現場のエンジニアは、マルウェアや攻撃そのものの特徴に関心を寄せてしまう。それが新種のマルウェアともなればなおさらです。ですが、大学の経営層が知りたいのは、現在の状況が大学の経営や運営に、どの程度の影響を及ぼすかという点。そこを的確に報告できる管理者が求められているのです」

学生のデバイスがマルウェアに感染しただけなのか、それとも重要情報を取り扱うサーバーが攻撃を受けたのかによっても、対策の優先度や重要度は異なってくる。何を優先し、どのような対策を施すべきなのか、大学経営への影響はどの程度あるのかを明確に判断し、報告できる体制づくりが、すべての大学に求められているのだ。そうしたことから、サイバーセキュリティ人材育成プログラムは、サイバーセキュリティを理解し、適切に行動できる人材を大学に配備することを目的としている。

「必要なのは、現場で交通整理ができる人。ネットワーク技術、セキュリティ技術の知識と実務経験を持ち、断片的な情報からでも総合的に判断し、状況の変

高倉弘喜
TAKAKURA Hiroki

化に応じた的確な措置を実行できるとともに、法的な知識にも通じ、経営層との意思疎通ができるような“橋渡し人材”を育てたい。各大学で最低２人は育ってほしいですね」と、高倉教授は語る。

NIIは何を提供するのか

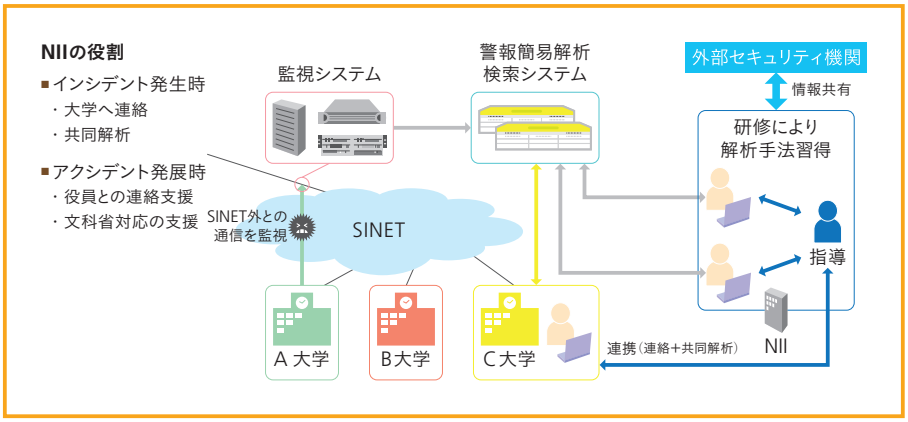
NIIが構築・運用する学術研究ネットワーク「SINET」は、現在、新たなセキュリティ対策強化に取り組んでいるところだ。サイバーセキュリティ人材育成プログラムは、その一環として推進される。

現在、取り組んでいるのは、「NII-SOC（セキュリティオペレーションセンター）」（仮称）の開設であり、この動きが本格化したのも、日本年金機構の情報漏洩事件がきっかけだった。

日本年金機構の例では、NIIにも情報漏洩の発端となったマルウェアが約半年間も潜伏していた疑いがあるとして、NIIのアクセス履歴を半年前まで遡って確認することにした。だが、マルウェアに指令を出していたサーバーのIPアドレスが転々としていることや、有名サイトへのアクセスログが含まれることなどから、膨大な情報を解析する必要に迫られ、NIIのシステム環境では、データを抽出するだけで約１週間もかかっていた。もはや、一つの機関ですらすべてのアクセス情報を対象に解析するには限界ともいえる状況にあった。

一方、サイバーセキュリティ基本法の制定により、中央省庁に加えて、独立行政法人や特殊法人などが、内閣サイバーセキュリティセンター（NISC）の制度に基づく監視・監査対象に追加された。国立大学法人等はその対象から外れたが、独自の対策強化が法律で求められることになった。

これらの状況を踏まえて、NIIでは、平成27年からSINETを俯瞰する新たなサイバーセキュリティ対策の構想に着手した。平成28（2016）年４月にSINET5の運用開始に合わせて、サイバーセキュリティ研究開発センターを発足。同センターを中心に、構想の実現に向けてNII-SOCの構築を開始した。



図｜サイバーセキュリティ人材育成におけるNIIの役割

ただし予算が限られていることから、取り組みには限界があった。そこで、NII-SOCでは、約90の国立大学機関に限定した運用としたほか、まずは平日運用や時間枠を設定した形での運用から始めること、また国立大学には新たなセキュリティ人材の雇用を求めず、各大学の協力を得ながら、サイバーセキュリティ人材を育成することも盛り込んだ。

NII-SOCでは、大学のファイアウォールの外での通信を監視対象にし、それに対応した検知パターンを設定。監視によって不審な通信を検知すると、該当IPアドレスに加え、関連した疑わしい通信情報をまとめて解析し、解析結果を大学側に通知することになる。大学側では、これをもとに対策を検討、判断し、各種対策を実行する。このときに、現場での判断と対策を実行するのが、サイバーセキュリティ人材育成プログラムによって育成された人材ということになる。

サイバーセキュリティ人材育成プログラムの正式なスタートは、平成29年7月の予定だが、同３月から、大規模校から小規模校までさまざまな15大学が参加して、試行を開始している。ここでは、NII-SOCで開発したツールの使い勝手や最適化に向けたチューニング作業なども実施し、人材育成プログラムがスムーズに実行できるかどうか、約３週間に渡って検証する。また、４月からは、対象となる国立大学を約60校にまで拡大し、正式スタートに向けた準備を一気に進める。

サイバーセキュリティ全体の底上げも

サイバーセキュリティ人材育成プログラムに関連して、高倉教授は、NII-SOCを通じて、いくつかの新たな取り組みを開始しようとしている。一つは、マルウェアそのものの検体を大学側に提供する試みだ。

これまで、日本の大学機関が最新の検体を国内で入手することは困難だった。そのため、海外のセキュリティ関連機関およびセキュリティベンダーが早い段階に検体を入手して研究、開発をしてきたのに比べて、日本の大学での研究活動は大幅に制約されていた。「NII-SOCでも配布先に制限はあるが、研究者がフレッシュかつリアルなデータを入手する仕組みをつくることで、いま起きている事象を研究対象にできます。これにより、日本におけるサイバーセキュリティ研究を加速したい」とする。

もう一つは、大学生や大学院生へのインターンシップだ。各種情報を提供することで、将来のサイバーセキュリティ人材の育成に向けた後方支援を、各大学に対して行う考えだ。

実践型ともいえるサイバーセキュリティ人材育成プログラムが、人材育成だけでなく、日本のサイバーセキュリティの底上げを実現できるかどうかも注目される。（取材・文＝大河原克行　写真＝佐藤祐介）

今、大学に求められる情報セキュリティ対策とは

実践的データを用いたプログラムで、人材の底上げを図る

南 弘征

［北海道大学 情報基盤センター 教授／サイバーセキュリティ研究部門 サイバーセキュリティセンター長／
情報環境推進本部 CIO補佐役／情報セキュリティ対策室長／国立情報学研究所 客員教授］

SINETを活用したNIIの「サイバーセキュリティ人材育成プログラム」は、平成29（2017）年3月から試行運用が始まり、試行運用時には国立大学法人86校のうち60校余の参加が予定されている。参加する国立大学を代表し、北海道大学の南弘征教授に、大学の情報セキュリティの現状と課題、それらを踏まえた人材育成プログラムへの期待を聞いた。

大学が直面する課題

近年、大学などの研究機関は常にサイバー攻撃の脅威にさらされ、情報漏洩の疑いなどのインシデント報告も増えている。北海道大学もその例に漏れず、平成27（2015）年12月末には不正アクセスと個人情報の漏洩の疑いが生じている。その後、第三者委員会の調査の結果、情報漏洩は確認されなかったと結論づけられたが、セキュリティに対応する部署がありながら、なぜそのようなことが起こるのかという声も数多く上がったという。

北大でサイバーセキュリティセンター長を務める南弘征教授は、これには一般企業とは異なる大学特有の事情も関係していると話す。

「企業には情報関連の専門部署があり、トップダウンでコンプライアンス・ポリシーを徹底することが可能です。しかし研究者が多い大学では、各人の自主性をある程度重んじる必要もあり、画一的な運用が難しいのです」

その北大も、先の事件以降はトップダウンで厳しい制限をかけたため、不正アクセスや攻撃数は減ったという。しかし、一方で攻撃はますます高度化し、防衛側とのいたちごっこが続いている。これはどこの大学や研究所も同様に抱えている問題である。

大学ならではの課題はほかにもある。

「まず、国内外を問わず、ビジターが多いこと。研究などで数週間以上滞在する海外の研究者に対しては、インターネット環境も提供する必要がありますが、持ち込まれたデバイスがウイルス感染している可能性はゼロではありません」

また、情報セキュリティやコンプライアンスに対する意識レベルが、個々の構成員によってまちまちである点も課題の一つだ。実際に起きた情報漏洩事件をみても、「個人情報をUSBメモリに保存して持ち出して落とした」、「不審なメールの添付ファイルを不用意に開いた」など、不注意が原因のケースは少なくない。

現在、北大では情報リテラシーを高めるために、教職員に対してe-learningによる情報セキュリティの研修を行っている。受講率は毎年度ほぼ100％を達成しているが、それでもインシデントは起こるという。

南 弘征
MINAMI Hiroyuki

北海道大学文学部卒、北海道大学大学院工学研究科情報工学専攻博士後期課程修了（博士（工学））。小樽商科大学商学部社会情報学科、北海道大学情報メディア教育研究総合センターを経て、平成27年10月より現職。

ネットワーク全体を俯瞰し事例を共有する

最近はマルウェアのように、内部から情報を送り出す方式のウイルスも増えているため、攻撃に対する防御に加え、外部に送信されるデータも監視しなくてはならない。また、不正アクセスは外部からの指摘で発見されることが多いが、現在は自主的に対策をとり、いかに異常を早く見つけて他機関に迷惑をかけないようにするかが求められているという。

「セキュリティ人材が不足する中、大学内部のセキュリティ人材の底上げを行うことは急務になっています」

情報セキュリティを担う国立大学法人の技術職員を対象としたNIIのサイバーセキュリティ人材育成プログラムは、まさにそのような状況を踏まえて提供されるものだ。このプログラムでは、NIIが開発したツールを通じて、SINETのネットワーク上で実際に起きた攻撃事例など、生きたデータを用いながら、サイバーセキュリティ技術や、アクシデントやインシデントへの対応、経営層への説明など、実情に即したスキルを身につけることを目指す。

「大学職員は通常、自組織のサイトしか見ることがありませんが、ここではネットワーク全体のデータを活用するなど、他大学で実際に起きた情報漏洩などの事例も共有できます。現場の職員は切迫感をもってスキルアップに臨めるはずです」と南教授は語る。

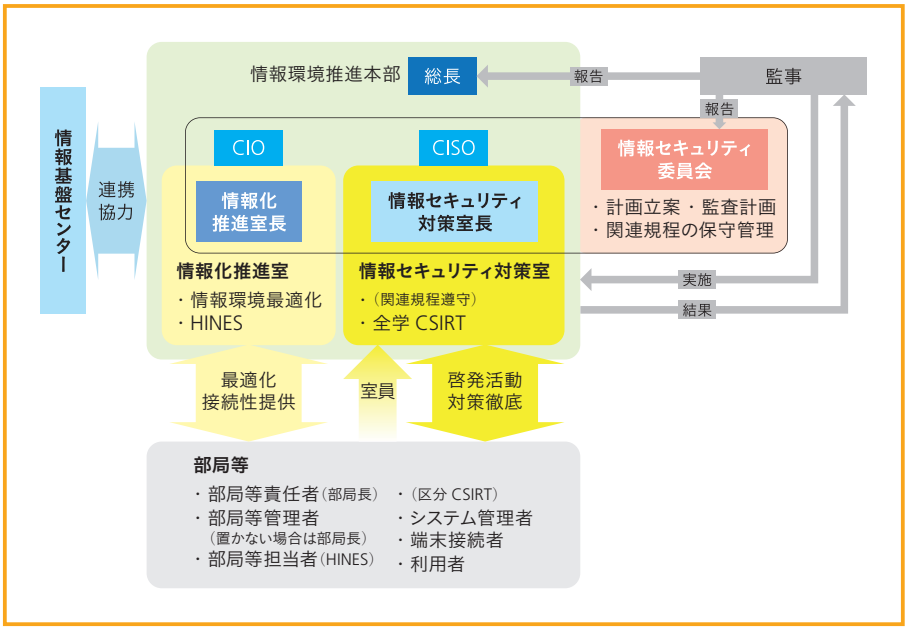
大学の事情に詳しい内部人材の底上げが重要

情報セキュリティ対策としては、民間の教育プログラムの活用やセキュリティベンダーへの外注という方法も考えられる。NIIの人材育成プログラムを用いて、大学内部の人材を育成することには、どのようなメリットがあるのだろうか。

「民間のプログラムは主に企業向けで、大学ならではの事情が考慮されていないことが問題です」と、南教授は言う。「もちろんそれでも一通りの知識は得られますが、大学の実情に即しているとは限らないのです」

例えば、北大の場合は地理的に離れたところにキャンパスが点在しているうえ、水産学部の練習船とのネットワークを有するなど、特殊な事情もある。海外の専門機関から送られてくる暗号化されていないデータなど、企業では受け入れられないようなデータを扱うこともある。研究機関ならではの秘匿性が高いデータも流れているし、近年は画像や動画データも増えている。つまり、大学の場合、一般企業とは明らかにデータの質や量が異なるのだ。

「民間の専門家が派遣で来ても、そういった特殊事情を把握できたころには企業に戻ってしまいます。また、大学では日常のオペレーションとセキュリティが一体化していることが多く、セキュリティ面では有意義でも、日常のオペレーションと齟齬（そご）が生じる方法論は適用できません。だからこそ、事情を理解している内部の人材に、大学の情報セキュリティに特化したプログラムで技術を磨いてもらうことが重要ですし、その方が結果的にはコスト面でのメリットもあると考えます」



図｜北海道大学のセキュリティ体制（関係部分抜粋）

トータルな知識・技術をもつ“橋渡し人材”の育成を

セキュリティの最後の砦は、ネットワークの末端に連なる個々のサイトである。そのサイトを運営し、守っている現場の担当者たちが、実際のネットワーク上の情報を用いて学ぶことにより、ネットワーク全体を俯瞰する意識が生まれてくる。同規模の大学の通信状況も把握できるし、現場の職員同士の横のつながりが生まれ、情報交換もできるようになる。ここから新しい地域コミュニティが生まれてくる可能性さえある。これらはセキュリティを強固にするうえで、非常に役立つことだ。

「情報セキュリティ人材全体の底上げをするべきこの時期に、NIIが先導してスキルアップの機会をつくっていただけるのはとてもありがたいことです。しかも、現在求められているのは、専門分野しか知らない人材ではなく、現場と内部の幹部や外部関係者との橋渡しもできるような、セキュリティ全般を扱える人材です。この実践的なプログラムにより、そのような人材が育つことを大いに期待しています」

（取材・文＝桜井裕子　写真＝佐藤祐介）

News 1 大学院生らが研究成果を発表

国立情報学研究所は、1月4日、総合研究大学院大学と連携大学院に所属する学生や特別共同利用研究員による研究発表会を開催しました。発表会では、1人あたり5分という限られた時間の中、25名の学生から日頃の研究成果についてさまざまな発表があり、参加した学生や教職員が熱心に聞き入っていました。

発表の終了後、国立情報学研究所の教員8名による審査の結果、以下の2件がベストプレゼンテーション賞に選ばれました。

- **関弥史紀さん**

「Discrete curve fitting in the presence of noise」

- **Ning Zhengさん**

「Numerical Solution of Nonnegative Constrained Least Squares Problem and Its Applications」

受賞者には、1月13日に行われた喜連川所長の年頭挨拶の後の表彰式で、所長から記念の楯と表彰状が手渡されました。

News 2 「クラウド利活用セミナー」を開催

大学・研究機関に所属する教員や研究者が、研究教育活動においてどのようにクラウドを活用できるかを体験することを目的とした「クラウド利活用セミナー」の第7回（平成28年12月21日（水））、第8回（平成29年1月17日（火））を開催しました。

第7回は、「クラウドの導入・利用に伴う法的課題と対応策 ～クラウドの導入・利用についてのリーガルリスク低減の観点から」と題して、渥美坂井法律事務所よりクラウドの利用におけるソフトウェアライセンス、個人情報保護法、営業秘密、知的財産権、データセンターが国外にある場合などの法的留意点について講演をしていただきました。また、クラウド利用に際しての契約締結やデータの取り扱い、クラウドサービスの変更・終了、セキュリティインシデント発生時などそれぞれにおける法的課題と対応策、クラウド導入・利用を推進するためのリーガルリスクの低減の方策についてお話いただきました。盛りだくさんの内容で、大学・研究機関から多くの参加申し込みがあり、たいへん好評でした。

第8回は、「SINETクラウド接続サービスを利用したAmazon Web Services（AWS）の活用方法」と題して、NIIの学術基盤課からは、「SINETクラウド接続サービスについて」の説明、アマゾン ウェブ サービス ジャパン株式会社からは、「AWSの概要」と「SINETクラウド接続サービス経由でAWSを利用する具体的な方法について」の講演をいただきました。SINET5の高速・安全なネットワークにクラウドを直結して利用するためのノウハウを習得できるセミナーでした。

クラウド利活用セミナーは平成29年度も継続して開催する予定です。

News 3 CiNii Booksに新機能

CiNii Booksは、日本国内の大学図書館などが所蔵する学術資料（図書や雑誌など）の情報検索サービスです。NIIが全国の大学図書館や研究機関などの参加・協力を得ながら運用しているNACSIS-CAT（総合目録データベース）に蓄積された1千万冊以上（のべ1億冊以上）の情報を収録しており、学術資料の書誌情報（書名、著者名、出版事項、目次、内容紹介等）に加えて、その資料がどこの図書館にあるかという所蔵情報も検索することができます。

NACSIS-CATでは、紙媒体の資料に関しては全国の大学図書館の蔵書をほぼ網羅していますが、一方では、電子資料や各種デジタルアーカイブ（図書館などの資料をデジタル化し、ネットワークを通じて公開する仕組み）についても、CiNii Books上で検索・閲覧できる機能への要望が寄せられていました。

そこで、「CiNii Books」の機能強化として、平成28年3月に全国遺跡報告総覧、同年11月に米国HathiTrust Digital Libraryおよび国立国会図書館デジタルコレクションとの連携機能をそれぞれ追加しました。これらの新機能により、CiNii Booksに情報が収録されている図書・雑誌のうち、それぞれのデジタルアーカイブで電子化された資料群、例えば埋蔵文化財の発掘調査報告書（全国遺跡報告総覧）、Google Booksプロジェクトなどで電子化された米国の大学図書館の蔵書（HathiTrust）、国立国会図書館で収集・保存している古典籍資料や戦前戦後期の図書・雑誌などのさまざまなデジタル資料（国立国会図書館デジタルコレクション）へのリンクが検索結果画面に表示され、クリック一つで本文へアクセスできるようになりました。

平成23年11月にCiNii Booksのサービスを開始して5年、その間、検索項目の追加、APIの提供、ユーザインタフェースのリニューアル、モバイル対応等の改修を実施してきました。学術資料の検索・入手の利便性を一層向上し信頼できる情報検索サービスとしてCiNii Booksを引き続きご利用いただけるよう、このような機能強化やデータ連携を今後も継続・発展させていきます。

――“事務のお仕事”って何をするのでしょうか？（池澤）

酒井　「普通、研究所の事務というと研究者のサポートをしますが、NII には大学共同利用機関として事業を推進する役割があり、ネットワークやクラウド、セキュリティのほか、CiNii（NII 論文情報ナビゲータ）や KAKEN（科学研究費補助金データベース）など各種学術コンテンツサービスを全国の大学などに向けて提供しています。こうしたサービスを推進しているのが、私たち学術基盤推進部です。部は業務内容で学術基盤課と学術コンテンツ課の二つに分かれていますが、どちらもサービスを提供するためのハード・ソフトの整備や、運用予算の獲得を行っています。幅広い業務を、27 人の常勤とほぼ同数のサポートスタッフで分担しており、私は事務方のトップとして業務全体が滞りなく進んでいるかを見ています」

――大学時代、論文検索に CiNii を使っていました！

亀井　「そうですか。NII が行っているサービスに関わる機械のメンテナンスや更新も、私たちがやっています。昨年の熊本地震では、国道にかかる橋が崩落し熊本ー大分間の通信ケーブルが切れてしまいましたが、迂回経路を自動的に確保して通信の切断はありませんでした」

酒井　「最近は、ネットワークに対するサイバー攻撃が激しくなっており、それにどう対応していくかが NII 全体の大きな課題です。セキュリティに関する実際の業務は専門部署がやりますので、そのサポートをします」

NII の人々 Vol.4

研究者とともにサービスを運用 NII の事務のミッションとは

左から、亀井さん、池澤さん、酒井さん。NIIのサービスを支える事務のみなさんの仕事場に、お邪魔しました。

酒井清彦

［学術基盤推進部　次長］

大学では歴史を学ぶ。卒業後、図書館勤務。NIIの前身の学術情報センターで業務に従事する機会があり、それをきっかけにNIIに。その後、管理職として埼玉大学、東京大学、山口大学、名古屋大学で図書館勤務を経験。大学図書館の事情に詳しい。平成27（2015）年より現職。

亀井耕治

［学術基盤推進部　学術基盤課長］

大学では社会科学を学ぶ。千葉大学に採用後、文部科学省に転任。同省関連機関等での勤務経験を経て、平成28（2016）年より現職。山口大学では、酒井次長との勤務経験もある。

――お仕事の魅力は何でしょうか？

酒井　「実は、NII の事務には生え抜きのスタッフはごくわずかです。私も以前は図書館に勤めていましたし、他の多くの職員が大学の図書館や情報センターとの人事交流で NII に勤務しています。いろいろな職場を経験して、NII の仕事には研究者と協力しながら“新しいことをやるワクワク感”があると感じます」

亀井　「研究者がやりたいと思うことを、実現するようにサポートするのが、私たち事務のミッションだと思います。また NII には、大学共同利用機関として『全国の大学の教育環境の充実と向上を支援する』という大きなミッションがあり、自分としてもやりがいを感じています」

――お忙しいと思いますが、何か息抜きをしていますか？

酒井　「何かあった場合には、すぐに連絡が取れるようにしていますが、休日は趣味でドラムをたたいています。ボケ防止にと始めたのですが、いずれ仲間とセッションをやりたいですね」

亀井　「普段は仕事で忙しくしていますが、古いものを集めるのが好きで、休日には NII に近い神保町の古本屋街をのぞくこともあります。とは言え、これまで地方勤務で長年自宅を空けていて、今回の異動で東京勤務となったので、できるだけ家族のために時間を遣うよう心がけています」

（構成＝池田亜希子　写真＝佐藤祐介）

「NII の人々」に会って

NII の事務の方にインタビュー！？　いったい何をしている人たちなの？ と思っていましたが、NII の提供するサービスを強力に支えている方たちでした。お二人とも地方経験が豊富なことに驚きましたが、そこで NII のサービスに求められる広い知識と感覚を身につけてこられたようでした。

池澤あやか

タレント／エンジニア。「Rubyの女神」と呼ばれ、特にIT分野で活躍。著書に『アイディアを実現させる最高のツール　プログラミングをはじめよう』（大和書房）。第６回「東宝シンデレラ」審査員特別賞。

Essay

データの利活用と流通の間

森亮二 MORI Ryoji
［弁護士
国立情報学研究所 客員教授］

これまで、データ、特にパーソナルデータの利活用と流通は、表裏のものとして語られてきました。例えば、政府のIT戦略を示した閣議決定「世界最先端IT国家創造宣言」は、「データ流通の円滑化と利活用の促進」をテーマの一つに掲げています。

しかしながら、パーソナルデータのマネタイズは、これまで「流通」によって実現していたわけではありません。「GAFA」と総称されるグローバル・プラットフォーマーのうち、GoogleとFacebookの収益の中核は広告であり、これは彼らが収集したパーソナルデータを、外には出さず、自分自身で利活用した成果です。日本からもGAFAを追撃するような事業者が出現する「第4次産業革命」を目指すのであれば、データの囲い込みを悪いことと決めつけるべきではないでしょう。加えて、パーソナルデータの「流通」は、プライバシーの脅威であることも忘れてはなりません。また、流通させるとなるとセキュリティのコストもかかります。「流通」「オープン」ばかり強調することは、それらの点からも妥当ではないのです。医療や金融といった社会的な課題が明らかなものを選んでオープンにし、それ以外は、本人や一次取得事業者がしっかり守る「オープン＆クローズド」の制度設計がいいのではないでしょうか。

実は、別の分野でこのような発想をしているものがあります。著作権法改正の方向性を示すものとして文化審議会が先日公表した「新たな時代のニーズに的確に対応した権利制限規定の在り方等に関する報告書（案）」です。長年の懸案であった米国型の一般的フェアユース規定の採否の議論に対する答えを示すもので、「第4次産業革命」の成否を占ううえでも大きな意味を持っています。

報告書は、米国型の一般的なフェアユース規定を採用するのではなく、著作権者の不利益がないかまたは少ないと評価できる類型については、広い権利制限を設ける一方で、それ以外の部分については、公共目的での利用の必要が高い分野について範囲を絞った権利制限を置くべきであるとしています。これは、利用の必要性を確認したうえで、その部分のみオープンにする「オープン＆クローズド」のアプローチです。

しかしながら、これはこれで違和感が残ります。あえて悪く言えば、パーソナルデータはどんどん流通・利用させ、著作物は権利者の不利益をしっかり考えて慎重に流通・利用させるという組み合わせになっていないでしょうか。

第4次産業革命が痛みを伴うものであったとしても、個人の人権に踏み込んでいいものではないでしょう。革命の代償は、旧来のビジネスモデルを変革できない事業者によって支払われるべきものです。

受賞

▶山岸順一准教授（コンテンツ科学研究系）が第13回（平成28年度）日本学術振興会賞を受賞

▶北村大地さん（総研大情報学専攻、小野研究室）が第7回（平成28年度）日本学術振興会 育志賞を受賞

▶高木信二特任助教（コンテンツ科学研究系、山岸研究室）が、一般社団法人情報処理学会 平成28年度山下記念研究賞を受賞

今後の予定

6月7日～9日｜国立情報学研究所学術情報基盤オープンフォーラム2017

6月9日～10日｜国立情報学研究所オープンハウス2017（研究成果発表・一般公開）＝一橋講堂ほか。詳細や事前登録が必要なイベントへの参加申込みは、以下のNIIウェブサイトにて。
http://www.nii.ac.jp/openhouse/

表紙の言葉 サイバーセキュリティを、城砦に入ろうとする侵入者とそれをさえぎる門番の風景になぞらえて描きました。ロボットが演じる道化師風の怪しい侵入者や門番を描くことで、抽象的なサイバー空間に具体的なイメージを与えました。

情報から知を紡ぎだす。
NII
国立情報学研究所ニュース［NII Today］第75号 平成29年3月
発行｜大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
〒101-8430 東京都千代田区一ツ橋2丁目1番2号 学術総合センター
発行人｜喜連川 優　監修｜佐藤一郎
表紙画｜城谷俊也　編集｜田井中麻都佳
制作｜株式会社マツダオフィス／サイテック・コミュニケーションズ
本誌についてのお問い合わせ｜総務部企画課 広報チーム
TEL｜03-4212-2028　FAX｜03-4212-2150　e-mail｜kouhou@nii.ac.jp

http://www.nii.ac.jp/about/publication/today/