特集

情報セキュリティ

高等教育機関に対するサイバー攻撃の動向と情報セキュリティ対策の考え方

一般社団法人JPCERT
コーディネーションセンター　洞田　慎一

1．はじめに

報道や各大学からのプレスリリース等によれば、大学など国内の高等教育機関は、巧妙な手口を用いた高度化したサイバー攻撃に晒されており、様々なサイバー攻撃が確認されています。大学教職員をターゲットとしていると推測される文面による高度な標的型攻撃メールが、2016年以来毎年確認されており[1][2][3]、2015年には、高度サイバー攻撃による被害も富山大学で報告[4]されています。サイバー攻撃に使用されたマルウエア (コンピュータウィルスや、攻撃ツールなど攻撃者が使うソフトウエアの総称) がケースごとに異なっていることから、様々な攻撃者が大学教職員を対象として攻撃活動を展開しているものと考えられます。また、これらの事例では、攻撃を受けたことを組織が気が付くことができましたが、見過ごされている攻撃や被害の可能性も否定できません。

また、高等教育機関に対するサイバー攻撃は、標的型攻撃メールによる高度サイバー攻撃だけではありません。メールやクラウドなどのサービスの利用者アカウントを詐取するフィッシングメールや、サーバやシステムに対する不正アクセスなどもあります。例えば、2017年には不正アクセスによる情報漏えいが大阪大学において、報告[5]されました。これらの事例から、高等教育機関は、もはやサイバー攻撃とは無縁ではないと言えます。すなわち、すべての高等教育機関が、既に攻撃の只中にあり、被害規模の大小や被害内容の差異はあるにせよ、高度なサイバー攻撃に巻き込まれる可能性があるとの認識をもって、情報セキュリティ対策に臨むことが求められているのです。本稿では、大学で確認され公表されているサイバー攻撃事例をもとに、高等教育機関のどのような弱点が狙われてきたのかを解説し、それをもとに、どのような対策を施していくべきかを解説します。

2．高等教育機関にて確認された高度サイバー攻撃

標的型攻撃や高度サイバー攻撃について見聞きはしていても、「大学や、大学の関係者が狙われることはないだろう」、「機微な研究内容ではないし、特別に価値がある情報が学内に保存されているとも思えない」等と考えて、サイバー攻撃を対岸の火事として思ってはいないでしょうか。しかし、前述した事例を見れば、サイバー攻撃と無関係と言い切れる高等教育機関はないと考えられます。

サイバー攻撃に使われるメッセージは、狙われた組織で日常的にやり取りされる業務メールのように見えます。したがって、受信者がよほど注意をしない限り、メールに添付された添付ファイルを開封したり、メールに記載されたリンク先にアクセスしたりしてしまいます。2016年以来毎年確認されている学研究費助成事業に関する標的型攻撃メールを大学関係者でない人が受け取ったとしても、表題や本文から誤送信かスパムと判断して読み捨てるであろうことに思いを致せば、それらが教職員など高等教育機関の関係者を標的として送付されていることは明らかであり、高度サイバー攻撃で「大学や、大学の関係者が狙われることはないだろう」と考えることは間違いだと分かる

と言えます。毎年のように標的型攻撃メールが確認されていますので、高等教育機関の方が他の企業や組織よりもサイバー攻撃を受けるリスクが高まっていると危機感を強めて、実態の点検と対策を急ぐことが望まれます。

教職員ばかりではなく、サポート・スタッフや学生もサイバー攻撃に狙われています。例えば、富山大学水素同位体科学研究センターで発生した高度サイバー攻撃[4][6]では、標的型攻撃メールが教員と非常勤職員に届き、メールに添付されたファイルを開封した非常勤職員のPCがマルウエアに感染しています。多忙な教員に代わって、メールやスケジュール管理などの日常の事務業務を担当する秘書的な立場の職員などもメールを確認する必要がありましょう。富山大学での事例がそうした状況であったか否かは定かでありませんが、こうした方々は、受信メールに嫌疑を向け難い立場にあり、標的型攻撃メールを開封しがちです。報道によれば、届いた標的型攻撃メールは、教員と学会で出会った学生を名乗り、研究内容に関する質問をしたいとの内容であったと報じられています。富山大学のWebに公表された情報[6]に引用されているメール本文は、日本語として使いまわしや、単語の表記が不自然な点がいくつか認められるものの、まったく意味をなさない文章ではありません。2016年以来継続的に確認されている科学研究費助成事業に関する情報を記載した標的型攻撃メールは文章も自然で、実在する人物の氏名が記載されていた[3]ものもありました。以前は、文章に不自然さがないかどうかで、標的型攻撃メールか否かを見分ける方法も有効[7]でしたが、昨今では、流暢で自然な文章の標的型攻撃メールも増えています。不審なメールを開かないよう利用者に注意するだけでなく、利用者が気づかずに標的型攻撃メールに添付されたファイルを開いたり、リンク先をクリックしたりする可能性を前提とした対策の必要があると言えます。特に、学会活動や研究活動に関する連絡を装ったものであれば、教職員だけでなく学生や研究員らが標的型攻撃メールに触れ、罠にはまる可能性も否定できません。そうしたところから被害が発生することも想定しておく必要があります。

富山大学に対する攻撃で用いられたマルウエアは、感染したPCからの不審な通信先アドレスから、Asruex[8]であったと考えられています。このマルウエアに感染したPCは、攻撃者が遠隔操作できるようになります。このマルウエアは、VirusTotalなどのマルウエア分析データベースに、それぞれ異なる通信先をもつ複数の検体が登録されています。攻撃者は、攻撃先ごとにカスタイマイズして検知を逃れようとしていたと考えられます。また、複数の検体が登録されていることは、富山大学以外の組織にも、マルウエアが添付された標的型攻撃メールが届いていた可能性を示唆しています。いずれにせよ、このようなカスタマイズが施されたマルウエアは、ファイアウォールなどに組み込まれたシグネチャーによる検知をすり抜けることがあります。実際に、富山大学の事例では、外部の組織から照会を受けて初めて攻撃を受けていたことに気が付きました。高度サイバー攻撃では、攻撃を受けている組織がそれに気が付かず、外部からの通報で調査に着手して攻撃を見つけるケースが珍しくありません。

富山大学の事例では、感染したPCに保存されていたほとんどの情報が遠隔操作により持ちだされ、その中には研究に関する情報や個人情報が含まれていた可能性があると考えられています。この攻撃の狙いが何であったのかは分かりませんが、攻撃者が、最先端技術や安全保障などにかかわる機密情報だけを狙っていると即断すべきではありません。高度サイバー攻撃に関する様々なレポートでも、様々な狙いをもつ攻撃者の存在が報告されています。高等教育機関を狙う攻撃者は、教育機関や教職員が持つ情報を窃取しようとしているのかもしれませんし、他の攻撃を仕掛けるための踏み台となるシステムや利用者アカウントを探しているのかもしれません。あるいは、学外の委員会活動などを通じて教職員が得た機微な情報や豊富な人脈、指導している留学生の情報等を狙っている可能性も考えられます。このように見れば、高等教育機関を狙う攻撃者の皮算用の一端を推察できるかと思います。

情報セキュリティ対策の第一歩は、守るべき情報資産の特定であり、そのためにも、まずは学内にどんな利用者が在席して、どんな情報を扱っているのか、教育機関としてどんな情報資産を保持しているのかを知ることが重要です。サイバー攻撃から守るべき情報資産は、教職員が用いるPCに保存されている情報だけではありません。高等教育委機関でも、ここ10年あまりで業務の電算化が進み、受講届けの受付や発注管理などがオンライン化され、図書の検索・貸出予約、eラーニング等の学内の様々なサービスをPCやスマートフォンなどを介して利用できるようになりました。電算化された業務やサービス提供に伴って、オンライン上に存在している情報資産が大量に蓄積されていると考えられます。一台のPC感染をきっかけとして、これら学内に保存される様々な情報資産全体に、攻撃者もアクセスできる可能性が生まれます。

大学全体の情報資産のうち、何を攻撃者が狙っ

ているのかが分からないことを考えると、マルウエアへの感染や攻撃者の侵入に気が付きにくい高度サイバー攻撃は、感染したPCだけの問題ではなく、大学全体に影響範囲を拡げて対応することが求められます。

3．ID、パスワードの窃取や、それを悪用したサイバー攻撃

高等教育機関では、統合的な認証システムを導入し、様々なオンライン・サービスのログインIDとパスワードを一元的に管理し、シングルサインオンによるサービス連携を実現しているケースも珍しいことではないでしょう。学内のシステムにとどまらず、学外のサービスも利用できるようにしているケースも考えられます。

このように統合化された認証システムで管理されたアカウント情報は、奪取すれば様々な情報システムや情報サービスを利用できるようになるので、攻撃者にとって価値ある戦利品と言えます。その視点で、いくつかの大学の情報系センターから発表される注意喚起を改めて見直してみると、教職員や学生のID、パスワードを狙ったフィッシングメールに関連したものが驚くほど多くの大学で散見されます（図１）。Webサイトに掲載された注意喚起からうかがい知れるケースは、この種の事案の氷山の一角にすぎないと考えられます。また、高等教育機関だけでなく、様々な機関やサービスの利用アカウント情報を広く収集しようとした攻撃の一端である可能性も否定できません。

オンライン・バンキングやWeb、メールシステムなどのIDとパスワードを詐取するフィッシング攻撃は目新しくはありません。しかしながら、慣れっこになって問題の程度を軽く評価しているということはないでしょうか。フィッシング攻撃が発端となり、深刻なインシデントに拡大する可能性も否定できません。実際、関西学院大学[9]などで、フィッシングメールを発端とするインシデントが報告されています。

教職員や学生が、学外のオンラインサービスを利用するシーンや、他大学のサービスを利用しているシーン、あるいは、学外から接続できるサーバや、NASなどのストレージを研究室で運用するシーンは、高等教育機関においてさほど珍しいことではないと思われます。仮に、学外のサービスにおけるフィッシング攻撃などでIDやパスワードが窃取されるなど、攻撃者が何らかの方法で、ログインIDやパスワードを入手できた場合、そのリストを用いて不正アクセスを試みる可能性も考えられます。一つのアカウント情報が窃取されたことに端を発して深刻なインシデントに拡大したケースの一つが大阪大学[5]の事例です。次いで、管理者 IDや、他の利用者のIDも窃取され、グルーウエアから学内外の個人情報が持ちだされたとされています。

IDやパスワードが悪用された場合の影響の範囲を考えると、仮に、利用者が、ID、パスワードを誤って入力してしまった場合の対応は、当該の利用者のIDやパスワードをリセットすることのみで対応を終えてもよいのでしょうか。その対応が誤っているわけではありませんが、窃取されたIDやパスワードから、様々なサービスや情報に触れることができる、ということを認識して対応を進め

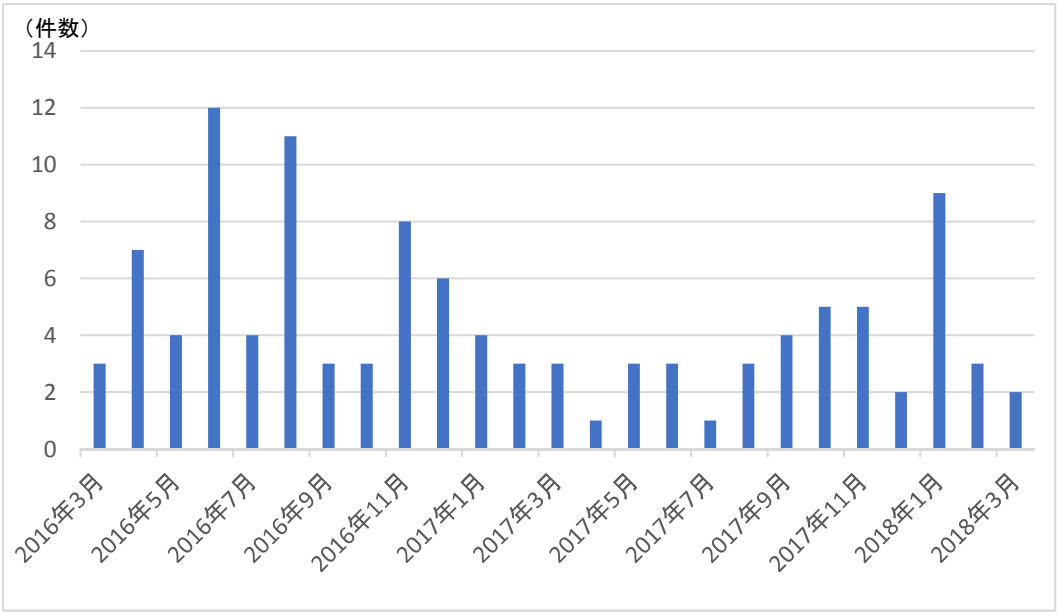


図１　インターネットにて確認できる各大学における注意喚起の発行数（2016年１月～2018年２月）

ることが望まれます。学内の他のシステムに不正アクセスが見られないかを確認することや、利用者には、学外で利用しているサービスにも不正なアクセスがなかったかなどの確認が必要です。パスワードの使いまわしを避けるように求める利用者への注意喚起とともに、アクセス元や日時などの履歴を利用者が確認できるような処理の工夫も重要です。

４．高等教育機関における情報セキュリティ対策の考え方

規模や細部の特徴は様々ですが、大局的に見れば高等教育機関の情報システムは、基本的に類似したサービス・メニューをもち、類似したコンポーネントやツールを使ってシステムを構築し運用していると考えられます。このことは、攻撃者の視点に立つと、高等教育機関向けに特化してカスタマイズした攻撃ツールを用意し、それを使って多数の高等教育機関に攻撃を仕掛けることができることを意味しています。

一方で、一般の企業や官公庁とは情報システムへの要件が大きく異なっていますので、高等教育機関における情報セキュリティに対する対策には、一般の企業などとは異なった視点が求められています。高等教育機関における情報セキュリティ対策について次のポイントを指摘し、それぞれについて掘り下げておきたいと思います。

（1）インシデント対応体制の整備
（2）情報セキュリティポリシーの策定とセキュリティ・ガバナンス
（3）教育訓練の重要性
（4）他の高等教育機関との情報共有

（1）インシデント対応体制の整備

先に説明したように、昨今のサイバー攻撃は高度化し巧妙化しており、どの高等教育機関でも、いつインシデントが発生してもおかしくない状況です。すなわち、突然にインシデントに見舞われ、対応を迫られる事態が差し迫っていることを意味します。そうした事態に備え、各機関にとって、インシデントに対応する体制を整備することが緊急の課題です。

インシデントへの対応体制において、技術的な核となるものが CSIRT (Computer Security Incident Response Team) です。組織内CSIRTは、組織内で発生するインシデント対応の要として活動するチームです。CSIRTは、情報システムの運用を担当しているチームと連携して活動する必要がありますが、運用担当チームとは独立した権限と要員を付与しておく必要があります。さもないと、インシデントが発生した時に様々な業務が集中して混乱に陥ってしまうからです。

インシデントが発生した際には、全体像をすみやかに把握し、脅威に晒されている情報システムやネットワーク、情報資産などへの被害の拡大を抑止し、影響範囲を極小化するとともに、迅速な復旧を行う等、様々な対処を限られた時間の中で進める必要があり、そのための司令塔として、CSIRTが機能しなければなりません。例えば、「３．ID、パスワードの窃取や、それを悪用したサイバー攻撃」で紹介したような、窃取されたIDやパスワードが学内の様々なシステムで悪用されたインシデントが起きたと想像してみてください。様々なシステムの担当者らが集まって情報を整理し、それぞれが行うべき対応を協議する必要があります。インシデント発生時の初動対応の例として、「２．高等教育機関にて確認された高度サイバー攻撃」で紹介した事案における実例が資料[10]にありますので参考にしてください。

組織内 CSIRTを構築する際に手引きとなる資料として、JPCERT/CCではCSIRTマテリアル[11]を公開しています。資料では、構想、構築、運用と三つのフェーズに分けて、それぞれの段階について検討に必要なポイントや、構築プロセス、インシデントハンドリングに向けたマニュアルを示しています。これからCSIRTを設置しようという方々にとって参考になるはずです。

とはいえ、そもそもスタッフが少なく、CSIRT業務を担える人が限られていたり、知見が十分でなかったりで、悩んでいる組織も少なくないと推測されます。しかし、専任者でCSIRTを組織する必要はありません。CSIRTにとって、組織という箱ではなく、必要な機能を備え、いざという時に既存の組織と整合性を保ちつつ実効性のある行動をとれるかどうかという中身が重要です。特に、システムがそれぞれの部局で管理されている場合などは、複数の部門から兼務者を集めた混成編成のCSIRTの方が効果的な場合もあります。

また、インシデント対応に必要な技術をもつ人材がいない等の理由でCSIRTの整備を断念していないでしょうか。情報セキュリティに対する専門知識や技術的な知見は必ずしも組織内から調達する必要はありません。セキュリティベンダにアウトソースするなど外部の協力を仰ぐことも可能です。あるいは、必要に応じてJPCERT/CCのような専門機関などから技術的な助言や情報の提供を受けることもできます。むしろ、自らの技術を過信して無用な深みにはまったり、見落としから独り善がりのリスク判定をし被害を小さく見積もってしま

ったりするよりも、外部の力を利用したほうが方向性を見失うことなく適切に問題解決できるとも言えます。フォレンジックやログ分析など専門的な作業は、外部の専門家に依頼する組織の方が多いと言えましょう。

しかし、組織内の人にしかできない役割があることにも注意してください。組織全体を見渡して統括し、適切な部門に協力を求め、あるいは指示を出し、組織の価値観に基づいて判断を下す等の役割です。CSIRTを構築するにあたって、どんな役割や人材が必要とされるかについては、日本シーサート協議会から公開されているCSIRT 人材の定義と確保[12]なども参考になります。

CSIRTのメンバーが決まったら、インシデント発生時に彼らが的確に行動できるよう、緊急時の行動計画を立案し、事前に訓練しておくことが重要です（図２）。大規模な被害を伴うインシデント対応において、意思決定のための会議に時間を取られて対応に手間取ることは、すべての組織にありがちな問題です。対応に手間取ることにより被害や影響が拡大していくこともしばしばです。その原因は、インシデントが発生してから対応を検討する「泥縄」にあります。当然、不測のインシデントであれば、ある程度は意思決定に時間がかかるのも仕方がありませんが、基本的なインシデント対応手順だけでも事前に計画し、関係者の理解を求めておくことはできるはずです。

インシデント対応手順の計画も、あまり構えて考える必要性はありません。学内を見渡せば、すでにできていること、染みついているルールがあるはずです。例えば、火災や災害など物理的なインシデントについて、取り決めや事前の準備ができているのではないでしょうか。そうした危機管理計画に情報セキュリティインシデントが発生した場合の対処の考え方を書き加えることが出発点です。インシデント発生時に、誰がどのような責任や権限をもって指揮を担うべきかをはっきりさせておくべきです。

インシデントへの対応手順を検討する際の一つのヒントは、インシデント対応におけるゴールから、逆のパスをたどって必要な「アクション」と意思判断の「ルート」を整理してみることです（次ページ図３）。例えば、学外へのインシデント報告をゴールとした場合、どのような情報がいつまでに必要となるか、誰がどのようにしてその情報を集めるのか、そのために必要なリソースや権限は何か等を検討する必要があることが明らかになるはずです。最終的なゴールを定めずに作った対応フローは、いざと言う時に、必要な手順が欠落していたなどの不具合を含んでいて役に立たないことになりがちです。

インシデント対応計画を立案したら、検討した「アクション」や「ルート」が思い通りに機能するかどうかを、事前の演習などにより確認するなどして、不具合が見つかればそれを適切にフィードバックして、対応体制やルールを見直します。

（2）情報セキュリティポリシーの策定とセキュリティ・ガバナンス

教育機関によっては、情報システムを部局ごとに管理していたり、事務関連のシステムと教育研究関連のシステムの管理が別々に分かれていたり

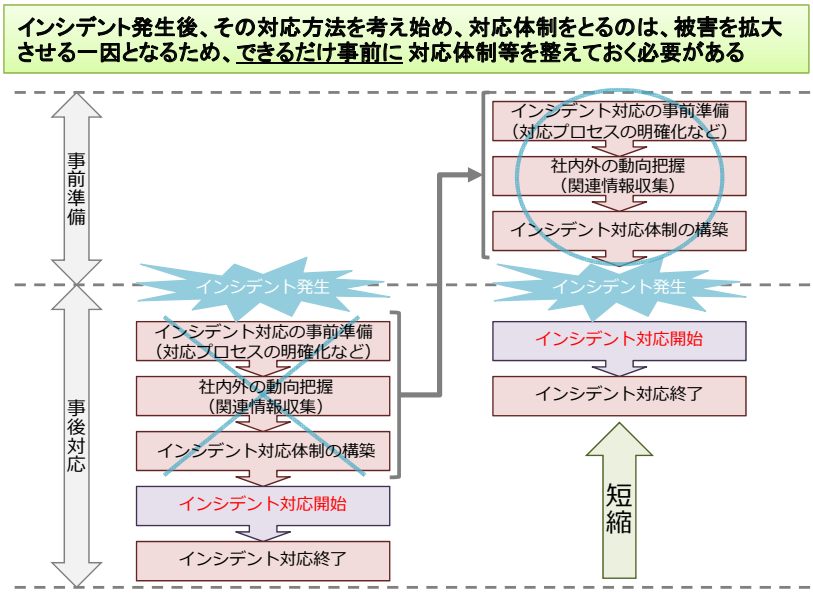


図２　インシデント対応体制等の事前準備の重要性

することでしょう。そうした場合、中核となるCSIRTを整備しても、学内関係部門の協力が得られなければ、インシデント対応を行うことができません。

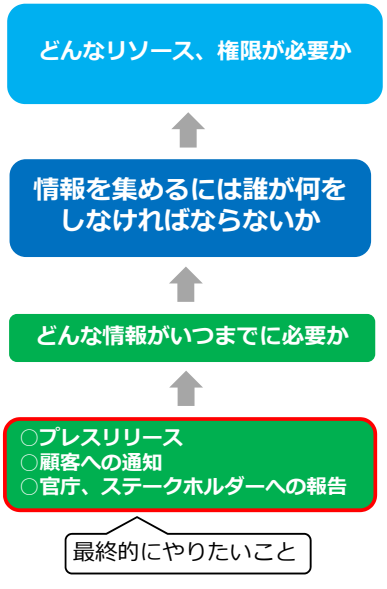
こうした問題を避けるためには、あらかじめ、情報セキュリティに対する基本的な考え方や権限などを含めた、情報セキュリティポリシーを策定して、学内規定の一部として位置づけておく必要があります。高等教育機関用の情報セキュリティポリシーのサンプル[13]が提供されていますので、これを参考に原案を起草してみてはいかがでしょうか。多くの私立大学で、情報セキュリティポリシーの策定がまだなされていないと聞きますが、そうした状況は、インシデント発生時の効果的な対処を妨げ、被害や混乱を拡大させることにつながります。

情報セキュリティポリシーを策定したら、次には、それが絵に描いた餅にならないよう、学内に浸透させるためのガバナンスの仕組みを樹立することが重要です。ネットワークに対する多様なニーズをもつ研究者から学生や研究生に到る様々な利用者を擁する応答教育機関は、一般にガバナンスを効かせにくい組織とされています。しかし、サイバー攻撃による被害を考えれば全学的な課題として、情報セキュリティポリシーに基づいた手順によって、守るべき情報資産を明らかにし、それをサイバー攻撃から守るためのガバナンスを浸透させなければなりません。守るべきは、組織がもつ情報資産全体であり、決して部局や管理主体の問題ではないはずです。

情報セキュリティポリシーの策定が進まない理由として、学内の情報システムにおける情報資産の洗い出しや、情報管理の実態調査の難しさをあげる声も聞きます。重要なことは、調査の網羅性ではなく、サイバー攻撃を受けた際にも、可能な限りの研究教育活動を継続するために守るべき主要な情報資産をまずは明らかにすることです。スモールスタートで、その後に必要に応じて拡充するアプローチを心掛けてください。細部にこだわって「木を見て森を見ず」という状況を避けて、大局観を見失わないことが肝要です。

（3）教育訓練の重要性

「人は城、人は石垣、人は堀」と言う信玄の名言にもあるように、サイバー攻撃に対する対策や対処においても、的確に行動することができる人が最後の防衛線です。そのような人づくりも重要な情報セキュリティ対策の一つです。筆者は、2017年８月に開催された私立大学情報教育協会セキュリティ研究講習会「総合演習」にオブザーバーとして参加をしました。そこでは、複数の大学から集まったセキュリティ担当者がグループを作って、シナリオに基づい提示されるインシデントの状況推移に対してとるべき対処行動を、初動体制から報告まで一連の過程について、他の参加者とのディスカッションを通じて考察されていました。各グループでは、自分自身の状況や工夫している点を共有しあい、与えられる課題状況を様々な角度から検討や議論されていました。この演習は、CSIRTメンバーを主な対象に、インシデント対応における諸課題への気づきを促すことを目的としたものでしたが、セキュリティ対策のためには



【アクションの整理】

事故対応時の情報発信に必要な情報を集めるためのアクションを整理する

（例）漏えい情報数の推定に必要なこと

・侵害を受けたサーバに格納されていた情報の最大数の把握
・攻撃者が持ち出そうとしたデータの確認
・攻撃者の行動をログ分析から確認

【ルートの整理】

アクションを行うために必要なリソース、連絡ルート、決裁ルートを整理する

（例）最短時間で初動対応に取り掛かるために必要なこと

・誰の判断でシステム／サービスを止めることができるか
・どの役員、部門が対応を指揮するのか

図３　「アクション」と「ルート」の交通整理

他にも実施を検討すべき様々な教育訓練があります。

セキュリティ対策のためには、CSIRTメンバー以外のセキュリティ担当者や一般利用者を対象にした教育訓練も、それぞれに応じた内容と形式により実施する必要があります。一般利用者向けの教育訓練では、セキュリティに関する基礎知識と組織が定めているセキュリティポリシーの概要に加えて、情報システムの利用に際して注意すべき事項や異常に気付いた時に報告連絡体制のような実務知識を教えておくことが望ましいと考えられます。CSIRTメンバー以外の各部局などに所属しているセキュリティ担当者向けには、それぞれに期待されている平常時およびインシデント発生時の役割を理解しておいてもらう必要があります。

こうした教育訓練は、入学や着任時における実施に加えて、基本事項等に関しては年に1回などの頻度で実施される定期研修や、情報セキュリティ月間などのタイミングを利用したキャンペーンを組み合わせて計画されることをお勧めします。既に実施しているが、参加者が少ない、効果的にできているか疑問が残るなどの声も聞きます。参加により、得られる情報を工夫したり、普段から情報提供の方法を工夫するなどして、教育訓練をおしきせるせるのではなく、受講者のモチベーションの向上を図る工夫も重要でしょう。

教育訓練の方法については、高等教育機関の皆様に向けて門外漢が言わずもがなの感もありますが、集合教育やｅラーニング、パンフレットや小冊子、電子メールやポータル画面上のバナーなどの電子メッセージなどを、それぞれの特性やコストを勘案して適切なものを選んでいただければと思います。

（4）他の高等教育機関との情報共有

情報セキュリティ強化対策として、CSIRTの設立と情報セキュリティポリシーの策定、教育訓練計画について述べましたが、いずれにしても何もない状態から立案することは手に負えないような難題に見えることでしょう。その困難を乗り越えるために頼りになるのが他の機関における先行事例からの学びです。高等教育機関の情報システムが似通っていますので、情報セキュリティポリシーや教育訓練用のコンテンツは流用できる部分も少なくないはずです。さらに、晒されている脅威についても他の教育機関と似たものがあると推測されますので、サイバー攻撃の情報や分析結果、対策を共有することが非常に効果的であると言えます。

高等教育機関が集まって、各組織の情報セキュリティ対策や攻撃の事例を他の組織に紹介、共有するための複数の機会や枠組みがあります。具体例をあげれば、協議会や学会、システムベンダーのユーザ会などです。そうした機会を活用して、是非とも情報セキュリティ対策のための知見を得ていただきたいと考えます。

他の業界では、サイバー攻撃に対して、自組織のみの対策だけでは防ぐことが難しいなどの理由から、業界内でインシデントに関する情報や、分析情報、対策に関する情報などを共有しあって、対策に結び付ける動きがあります。米国では、このような業界別の仕組みを、情報共有組織(ISAC; Information Sharing and Analysys Center) とか情報共有分析機関 (ISAO; Information Sharing and Analys Organization) 等と呼び、既に複数の業界で組織されています[14]。国内では、通信事業者や放送事業者、システムベンダなどによるICT-ISACや、銀行などの金融機関による金融ISAC、電気事業者による電力ISAC、などがあります。このように、多くの組織で、自組織の情報セキュリティ対策に、他組織との情報共有の場を活用しようとしています。また、日本シーサート協議会のように、業界を超えたCSIRT間での情報共有の機会も存在します。

高等教育機関では、このような組織だった情報セキュリティに対する共有の枠組みはまだないようですが、国立大学間では情報系センター協議会や、情報処理センター等担当者技術研究会などの枠組みがあります。私立情報教育協会も、セミナーや講習会を通じて、担当者間のネットワークを拡げる場を担っていくことを期待しています。インシデント対応体制や情報セキュリティポリシーなど、学内の情報セキュリティ体制を考える上でも、担当者間のコミュニケーションから、ヒントを得られるはずです。CSIRTを運用やインシデント対応を効果的に進める上でも、他の組織の方法論や、対策をぜひ参考にしてみてください。

一方で、担当者が組織の外に出ていくことは用務などの問題で難しい場合もあるでしょう。これもまた高等教育機関に限られた問題でもありません。他のCSIRTが、外部の組織との交流をどのように進めているか、どのような工夫をしているかなど、JPCERT/CCが、日本シーサート協議会と協力して行ったCSIRTの実態調査のアンケート調査[15]で行った、それぞれの組織へのヒアリング結果も参考になると思います。

5．まとめ

高等教育機関に対するサイバー攻撃は、毎年のよう、巧妙化、高度化したインシデントが確認されており、複数の大学からインシデントの報告が

なされています。「２．高等教育機関にて確認された高度サイバー攻撃」や「３．ID、パスワードの窃取や、それを悪用したサイバー攻撃」で、いくつかの大学で報告されたインシデントを取り上げました。攻撃者が、どのような情報を盗み出そうとしているかは想像がつきませんし、安易に「大学には重要な情報はないから、狙われないだろう」と考えてしまうことは危険です。学内における情報資産を認識し、適切な対応を進めることが望まれます。また、学内の複数のサービスがオンライン化されていることを考えると、一台の感染PCや、一つのログインID・パスワードの窃取を発端として、複数の情報システムへの不正アクセスも考慮に入れなければならない状況にあります。

このような状況を考えると、「４．高等教育機関における情報セキュリティ対策の考え方」で説明したように、高等教育機関では、インシデントが発生している、あるいはインシデントが発生しうる段階にあることを認識して、インシデント対応体制を整備していくことが必要なのではないかと考えられます。一方で、CSIRTを設けている大学はまだ十分ではないと考えられます。特に情報セキュリティポリシーが未策定である私立大学では顕著ではないでしょうか。このことは、サイバー攻撃に対し、まだ大学の対応体制が十分に整っていない可能性があることを意味しています。

情報セキュリティポリシーやインシデント対応体制を複雑に考えすぎず、一組織で悩むことなく、他の組織の取り組みなどを参考にして、できる範囲からスタートしてみてください。私立大学情報教育協会での取り組みや演習、その他のセミナーなどに積極的に参加していただき、大学担当者間での意見交換を積極的に行い、それぞれの大学に足りないポイント、実施できるポイントを一つでも増やしていきながら、ぜひ、各大学で効果的な対応体制を構築していただきたいと思います。

参考文献

[1] 慶応義塾大学 湘南藤沢 ITC, “標的型攻撃メールに関する注意喚起”, http://www.sfc.itc.keio.ac.jp/ja/news_targeted_mail_20160524.html, 2016.

[2] 明治大学 情報基盤本部, “日本学術振興会を騙った標的型攻撃メールに関する注意喚起”, http://www.meiji.ac.jp/isc/information/2016/6t5h7p00000mjbbr.html, 2017.

[3] piyolog, “2018年１月の文科省なりすましメールについてまとめてみた”, http://d.hatena.ne.jp/Kango/20180119/1516391079, 2018.

[4] 富山大学, “富山大学水素同位体科学研究センターに対する 標的型サイバー攻撃について（概要）”, https://www.u-toyama.ac.jp/news/2016/doc/1011.pdf, 2016.

[5] 大阪大学, “不正アクセスによる個人情報漏えいについて”, http://www.osaka-u.ac.jp/ja/news/topics/2017/12/13_01, 2017.

[6] piyplog, “富山大学 水素同位体科学研究センターへの不正アクセスについてまとめてみた”, http://d.hatena.ne.jp/Kango/20161010/1476110179, 2016.

[7] IPA,”標的型攻撃メールの見分け方”, https://www.ipa.go.jp/files/000043331.pdf, 2015.

[8] JPCERT/CC, “ショートカットファイルから感染するマルウエアAsruex(2016-06-23)”, , https://www.jpcert.or.jp/magazine/acreport-asruex.html, 2016.

[9] 関西学院大学, “フィッシングサイトへのアクセスによる個人情報漏えいについて”, https://www.kwansei.ac.jp/notice/2016/notice_20161007_013525.html, 2016.

[10] JPCERT/CC, "高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて", https://www.jpcert.or.jp/research/apt-guide.html, 2016.

[11] JPCERT/CC, “CSIRTマテリアル”, https://www.jpcert.or.jp/csirt_material/.

[12] 日本シーサート協議会, “CSIRT 人材の定義と確保 Ver.1.5”, http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf, 2017.

[13] 国立情報学研究所, “高等教育機関における情報セキュリティポリシー策定について”, http://www.nii.ac.jp/service/sp/.

[14] IPA, "米国ISAO関連文書の翻訳", https://www.ipa.go.jp/security/publications/isao/index.html.

[15] JPCERT/CC, “2015年度 CSIRT構築および運用における実態調査", https://www.jpcert.or.jp/research/2015_CSIRT-survey.html.