大学のサイバーセキュリティの現状

グローバルなネットワーク社会の加速は、時間・距離といった物理的制約の壁を越えて世界中のあらゆる人々とのコミュニケーションや情報共有を可能にし、膨大なデータ管理の利便性という面においても私たちに多くの恩恵をもたらした。その一方で、大学等の教育・研究機関は、日常的に世界からのサイバー攻撃の脅威に晒されており、昨今はウイルス感染やデータ改ざん、情報漏洩等のサイバーインシデントが増加するなど、世界中の人々が容易にネットワークにアクセスできる社会環境であるが故に発生する課題に直面している。わが国では、サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、2015年1月にサイバーセキュリティ基本法が施行され、官民が連携して情報資産を守るための対応を進めてきた。

CONTENTS

Cyber Secur

企業組織では、情報関連を管理する専門部署によって組織的な情報セキュリティについて一定のガバナンスを効かせることが可能であるものの、大学等の教育・研究機関は、研究を目的として国内外を問わず、多方面からのアクセスが多い特殊性や研究者の自主性を尊重する風潮もあり、組織にとって統一的な情報セキュリティマネジメントが難しい一面をもつのではないだろうか。年々高度化する情報通信機器へのサイバー攻撃に対して、大学は保有する情報資産を守るためにどのような情報管理や体制整備を行っていかなければならないのか。本特集では、大学における組織体制を紹介するとともに、教育啓発を通じたサイバーセキュリティ人材育成の取り組み等を共有し、社会的責務を担う大学のサイバーセキュリティの現状と対応を社会に示す機会としたい。

高等教育機関のサイバー攻撃耐性の向上
―大学間連携に基づく情報セキュリティ体制の基盤構築―

高倉 弘喜
国立情報学研究所教授・
ストラテジックサイバーレジリエンス
研究開発センター長

はじめに

従来の生活環境であるフィジカル空間とインターネットなどに代表されるサイバー空間の融合が進みつつある現在、従来フィジカル空間で起きていた諸問題がサイバー空間でも生じるようになってきた。例えば、サイバー攻撃は単なる技術力を誇示する愉快犯的なものから攻撃で利益を得ようとする犯罪ビジネスへ移行している。ビジネス化すれば新たな攻撃手法への投資が活発になるのは当然で、今や数年前の対策手法では太刀打ちできないほど巧妙になっている。

例えば、インターネットに直結された情報機器に攻撃が着弾しても何事も起こらないのに、着弾情報の転送先である後方機器の脆弱性を突いて被害を生じさせる攻撃も登場している。多くの組織では後方機器は外部への接続はできるが外部からは接続できないので、電子メールを除けばサイバー攻撃が及ばないのがこれまでの常識であった。

また、通信盗聴やデータ改ざんの対策として一般的となった暗号通信やファイル暗号化により、かえってセキュリティ監視が困難になった。[表1]は本稿で取り上げるNII-Security Operation Collaboration Services(NII-SOCS)で分析したある1日のアプリケーションの比率を示している。この内、web-browsingのような平文通信でも通信中で交換されるデータ本体(ファイル)は暗号化されている場合も珍しくない。明らかに平文通信かつ通信中のデータ本体も暗号化されていないものはdnsだけである。また、incomplete、unknown-tcpやunknown-udpも大部分はアプリケーションの識別ができなかった暗号通信である。日によって多少の差はあるが、NII-SOCSが観測している通信の80~90%は何らかの暗号を使用している。さらに木を隠すには森の中と言われる通り、サイバー攻

撃で使用される通信も一般的な暗号方式を採用している。

このような環境の変化により、大学とインターネットの接続点を監視するだけでは、被害を生じた後方機器から外部への通信を検知したとしても、その原因となった攻撃を特定するのは難しくなった。新たな対策の導入とそれを使いこなす高度な人材の確保が喫緊の課題ではあるが、そのような人材が居なければ有効な対策を導入できないし、そのような対策がなければ人材は育たない〝鶏と卵〟の状態に陥っている大学は多い。

アプリケーション	比率	通信路の暗号化
incomplete	39.46%	不明
ssl	18.41%	有り
unknown-tcp	8.56%	不明
quic	6.48%	有り
non-syn-tcp	5.03%	不明
insufficient-data	4.93%	不明
dns	3.89%	無し
google-base	3.79%	有り
web-browsing	2.84%	無し (*)
icloud-base	1.08%	有り
outlook-web-online	0.84%	有り
unknown-udp	0.75%	不明
apple-maps	0.62%	有り
ocsp	0.58%	有り
sharepoint-online	0.56%	有り
twitter-base	0.51%	有り
ms-update	0.44%	有り

(*) コンテンツが暗号化されている場合もある

[表 1]アプリケーションの種別例

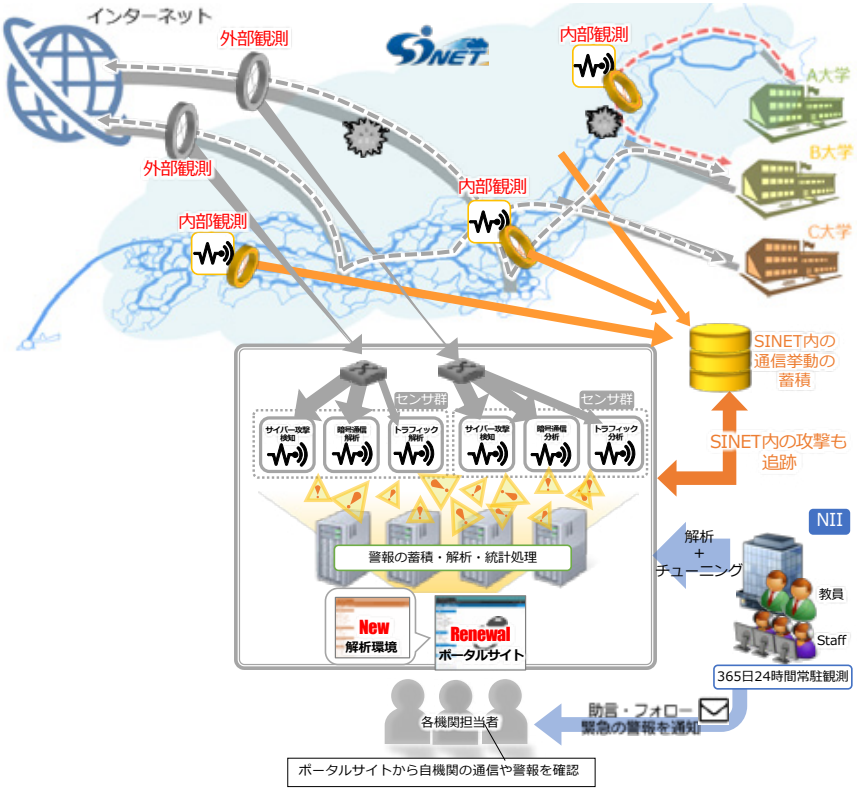
1 NII-SOCSの発足

本問題の解決策の一つとして、国立情報学研究所(NII)では2015年度の概算要求を経て、2016年度より国立大学法人等に対する「大学間連携に基づく情報セキュリティ体制の基盤構築(NII-SOCS)」事業を開始した。2022年4月の時点で約100の国立大学法人等が本事業に参加している。

[図1]にNII-SOCSの観測体制の概要を示す。過度の観測を回避するため、および、観測システムのコスト増を抑えるため、平常時は外部観測センサー群で警報や通信の発生傾向の把握だけに留めている。外部観測で不審な通信を察知すると、当該通信との関連性が推測されるSINET内の通信を内部観測センサー群で精査する多段構成を採用している。これにより被害を受けた機器がSINETに接続された他学を攻撃するか否かの状況も把握できる。

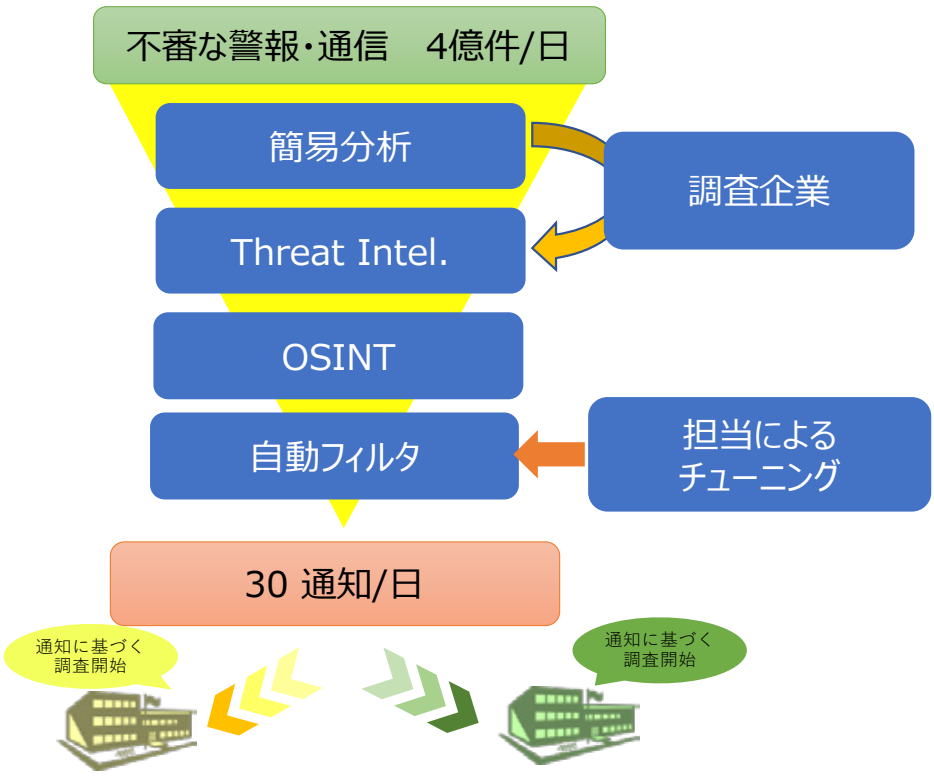
なお、NII-SOCSの大原則として、NII-SOCSの担当は大学の許可なく通信の内容を目視確認することはできない。平文通信の場合、各センサー群は検知の根拠となった部分のみを警報に付随した情報として記録する

が、この情報はポータルサイトに保存される際に暗号化されており、大学の許可なしには復号できない仕組みを導入している。一方、観測対象の大部分を占める暗号通信は内容を保存することはない。いずれにせよ、NII-SOCSの正式運用後、大学の許可を得て平文通信を復号・目視確認したことはない。



［図 1］NII-SOCS の観測体制

通信の内容を見ることなくサイバー攻撃の存在を察知するため、NII-SOCSでは警報や通信の挙動分析で不審な通信を炙り出す手法を導入している［図 2］。



［図 2］分析の流れ

(1) 簡易分析

簡易分析では、警報や通信の発生パターンの変異、前述したunknownとなる通信の急増などの変化点分析や機械学習、各連携先から提供される情報、NII-SOCS担当者が調査研究で得た情報による分析で警戒すべき警報・通信を絞り込む。ここで使用する分析技術はNIIストラテジックサイバーレジリエンス研究開発センターの研究成果を適用することで実現している。

(2) 脅威インテリジェンス(Threat Intelligence)との照合

脅威インテリジェンスとの照合では、NII-SOCSが契約している複数のインテリジェンスを検索し、攻撃グループの特定、その攻撃が始まった時期、狙っている情報の推定などによりリスクの度合いを求め、さらなる絞り込みを行う。

(3) Open Sourceインテリジェンス(OSINT)との照合

OSINTとの照合では、脅威インテリジェンスとの差分を把握している。OSINTでは把握しにくい国家関与が疑われる活動や水面化で進行する活動などを洗い出す。つまりOSINTが存在しない高度かつ最新の攻撃を炙り出す。

(4) 自動フィルタ

最後に、各大学への過剰通知とならないよう、NII-SOCS担当の知見に基づくフィルタリングを経て該当する大学へ通知している。なお、簡易分析の際にさらなる調査が必要な場合は、専門の調査企業に攻撃者の背景や意図、攻撃対象の推定、攻撃者グループで交換される情報の調査を委託している。以上の分析により、1日平均4億件の不審な警報や通信を30件程度に絞り込み、NII-SOCSの参加機関に通知している。

さらに、NII-SOCSは、大学が提出する調査報告から機関名などを特定する情報を削除し、さまざまな分析情報を付加して参加機関に提供する情報共有分析センター(ISAC)の役割も担っている。

2 NII-SOCSを通じた人材育成

NII-SOCSの目的は前述の観測体制の整備に留まらない。この体制を通じて、高度なサイバーセキュリティ技術と組織運営能力を兼ね備えた人材を育成すること、サイバーセキュリティ研究の促進に寄与することも目的である。

人材育成の観点からは、サイバーセキュリティの最前線で戦っている担当者のキャリアパスとして、将来も技術職を続

ける者と管理職に進む者に分かれると想定した育成プログラムを提供している。

技術職に進む場合、常に最新技術を習得し続ける必要がある。サイバー攻撃手法の巧妙化に追従して対策技術は日々進歩しており、AIなどによる自動分析や自動防御といった新たな手法が開発されている。近い将来、NII-SOCSにおける分析作業や大学での初動対応の大部分は自動化されるとすれば、サイバーセキュリティ担当者の仕事は自動技術を活用しつつ安全なサイバー空間を維持することに移行すると考えられる。そこで、NII-SOCSの機能をそのような次世代技術と見立て、実際の攻撃通知によるOJT環境を提供している。

一方、管理職については、最新技術の概要を理解すると同時に組織運営の知識も兼ね備えた人材が必要となる。このためNII-SOCSでは、サイバーセキュリティ管理能力の向上を目的とし、実際に国内外で発生したサイバー攻撃の実例を元にシナリオ化した机上演習も提供している。本演習では以下のような課題を繰り返しかつ矢継ぎ早に提示する。

- 攻撃は自組織で解決できるか？それとも専門組織の応援を必要とするか？
- 被害発生箇所の特定はできるか？被害規模は把握できるか？
- 被害は大学運営の他の部分に拡大するか？
- 被害拡大防止のため情報システムを停止すべきか？
- 運用継続と判断する場合、被害緩和のためのダメージコントロールはできるのか？
- 情報システム停止やダメージコンロールに伴い、デグレーションする大学の機能はあるか？
- 右記判断の根拠となった報告に誤報や虚偽が見つかった場合の作戦変更はあるのか？

また研究支援として、最近のデータ改ざんなどの増加を受けて、必須となりつつある研究公正のため研究証跡を記録した研究データの提供を始めている。実用的なサイバーセキュリティ研究のためには、現実かつ最新のサイバー攻撃データを扱わざるを得ない。一方、本当のサイバー攻撃により得られたデータである場合、オリジナルデータの公開を行うことは難しい。この相反する条件を満たす研究データ管理の整備が急務となっている。

そこでNII-SOCSでは、実際の最新サイバー攻撃

情報として、マルウェアデータと匿名化・統計化されたトラフィックデータの2種類の研究データをNII-SOCS参加機関の研究者に提供している。マルウェアデータについてはファイル本体だけでなく、取得日時とハッシュ値などの情報を研究証跡として保存し、必要があれば提示できるようになっている。一方、トラフィックデータについては、通信の秘密の保護の観点からオリジナルデータを匿名化・統計化処理後に破棄している。このため厳密な証跡とはならないが、処理に使用したプログラムと処理パラメータ、NII-SOCSのセンサー群が発した警報などを研究証跡として保存している。

3 大学に期待すること

暗号通信の比率増大、新たなネットワーク構成技術の登場、新型コロナ禍を契機とする新たな生活様式の普及、フィジカル空間とサイバー空間のさらなる融合などにより、NII-SOCSで行える攻撃察知はいずれ限界を迎えると想定している。

このため、各大学は自組織にサイバーセキュリティ技術と大学運営能力を兼ね備えた人材の育成を努力してもらいたい。大学によって組織文化が少しずつ異なることを鑑みると、運営能力を習得するには自組織での育成が必須となる。また、そのような人材を育てるために、キャンパスLANの更新の際には次世代を見越した安全かつ高機能なネットワークを構築していただきたい。

先行者であるが故の脆弱性への対応

土屋 大洋
学校法人慶應義塾常任理事

慶應義塾大学は、1990年に開設した湘南藤沢キャンパス(SFC)においていち早く、今まで一部の研究者のみが利用していたインターネットを全学生・教職員向けに導入した。特別教室に高性能のワークステーションが並ぶとともに、ラップトップパソコンも割安で入手できるよう手配された。学生一人一人に電子メールアカウントを付与するという、今では当たり前になった取り組みも先駆的に行った。ほどなく、全学部・研究科、全キャンパスにそうしたインターネット環境は波及した。

今では情報コンセントにつなぐ有線ケーブルではなく、無線LANがどこでも使えるようになり、共用のパソコン教室を徐々に廃止し、自分の端末を持ち込むよう学生に促している。

1 無数に開く脆弱性の窓

大学が用意・管理する端末だけではなく、多種多様な端末が接続されるようになり、それぞれの端末のセキュリティレベルが異なれば、キャンパスや大学全体のセキュリティも、より脆弱になる。また、インターネット導入が早かったために、SFCや、理工学部のある矢上キャンパスなどでは、個人や研究室で立ち上げたサーバーがたくさんあり、事務部門でも独自システムが立ち上げられ、適切なメンテナンスがされないまま放置されているものもあった。

そうしたセキュリティ対策が不十分なコンピュータは外部から狙われやすい。大学にはサイバーセキュリティ上、脆弱な窓が無数に開いていると言って良い。

そのため、2020年11月に、慶應義塾情報セキュリティインシデント対応チーム(CSIRT)を立ち上げた。そのミッションは、慶應義塾において発生した、あるいは発生し得る情報セキュリティインシデント(意図的あるいは偶発的に生じる、義塾規定あるいは法律に反する情報セキュリ

ティ上の事故あるいは事件）に主導的に対応し、影響を最小限に抑制し、情報資産の安全を確保することである。

ＣＳＩＲＴは、学内の他部門から独立し、最高情報責任者（情報基盤担当常任理事）から、インシデント調査に関する一定の権限を委譲されている。また、慶應義塾の情報基盤の運用部門であり、セキュリティオペレーションセンター（ＳＯＣ）の役割を担う情報技術センター（ＩＴＣ）と密接に協力をしながらも、中立公平な立場でインシデント対応を行っている。つまり、ＣＳＩＲＴそのものは少人数で運用されており、インシデントが起きた場合に実働部隊として対応するのはＩＴＣという組織構成になっている。その分、ＣＳＩＲＴはインシデントの予防措置や、ネットワークやシステムにおける不審な動きの発見に注力するとともに、外部組織との連携を行っている。

2 ウェイクアップコールとなる事案

２０２０年９月、まもなく入れ替えを予定していたシステムから個人情報が漏洩するという深刻な事案が判明した。

最高情報責任者である情報基盤担当常任理事と関係学部長、および関係教員がすぐにオンライン会議を開き、対応策を練った。新学期の開始が迫っており、残された時間は少なかった。ＩＴＣが、後にＣＳＩＲＴを構成するメンバーを中心に被害状況を確認し、取り得る選択肢を示した。学部の了解を得て、被害を受けたシステムをネットワークから外した。もっと早く古いシステムを置き換えておけば良かったと後悔せざるを得なかった。

この事案は、重要なウェイクアップコールとなった。その後、慶應義塾全体でどのようなシステムがどこで使われているのか、徹底的に洗い出す作業が行われた。セキュリティと利便性は時にトレードオフになる。セキュリティのための監視を強めれば、自由な情報活動はやりにくくなる。しかし、大学には高いセキュリティが要求される個人情報や研究資産が大量にある。もはや、利便性一辺倒ではいられない。

無数のシステムが乱立する中ではＣＳＩＲＴがその能力を発揮し、セキュリティを維持することは難しい。システムと業務を整理するデジタル・トランスフォーメーション（ＤＸ）とセキュリティ対応を連動させながら進めていかなくてはならない。

組織としてのサイバーセキュリティ教育

岡村 耕二
九州大学サイバーセキュリティセンター長

はじめに

九州大学では、2014年12月にサイバーセキュリティセンターが設置された。基幹教育から専門教育にわたって国際標準となるようなサイバーセキュリティ教育プログラムに基づいた教育に重点を置きつつ、未知の脅威を即時的に発見し対応できる次世代的なセキュリティ技術やサイバー空間を絶対的に頑健にする先進的基盤研究、ならびに国内外との組織と連携し法制度や社会現象に関するサイバー空間そのものの研究を持続的に行うことを目的としている。本稿では、サイバーセキュリティセンターが責任を持つ基幹教育におけるサイバーセキュリティ教育について紹介する。なお、基幹教育とは、学びの〈基〉となり〈幹〉となる「ものの見方・考え方・学び方」を培う本学学部1年生向けの独自のシステムである。

1 カリキュラム構成

現在、サイバーセキュリティセンターが責任を持つ基幹教育の講義は、全学1年生必修のサイバーセキュリティ基礎論と、総合科目でフロンティア科目に指定されている、サイバーセキュリティ演習と企業から見たサイバーセキュリティである。総合科目とは、教員の申請によって認められたものが開講できる選択科目であり、教員によってある程度自由な企画が可能であるという性格を持つ。多種多様なものがあり、基幹教育でありながら、講義によっては2年生以上の学生の受講も多い。そして、学生が自分の意思で自由に選択して履修できるオープン科目と、学部から必修科目として指定されているフロンティア科目に分かれている。そのため、サイバーセキュリティ演習と企業から見たサイバーセキュリティは選択科目でありながら毎年受講生が多い。

2 サイバーセキュリティ基礎論

サイバーセキュリティ基礎論は、近年、サイバーセキュリティに関する正しい知識や基礎的な技術情報を持つことが、よりよい教育を受けたり、研究を行ったりする上でとても重要になり、また、将来、IT社会を生き抜くために必要になってきたことが背景になっている。また、サイバー空間には、パソコンをインターネットに接続しオンラインで使用している時だけではなく、インターネットに接続されていないパソコンやUSBなどの周辺機器をオフラインで扱っている時も含めている。そのため、サイバーセキュリティの教育は、技術的なことはもちろん、法律、倫理に関する正しい知識と理解が常に求められており、文系、理系を問わず、すべての専門分野において共通的に必要なものとなっている。さらに、我が国のサイバーセキュリティ基本法でも、大学は学生にサイバーセキュリティに関する教育を十分行うことが定められている状況で、サイバーセキュリティ基礎論は2014年度から総合科目で、2017年度からは全学必修科目として開講している。現在のサイバーセキュリティ基礎論は、春学期の8週で、(1)サイバーセキュリティの概要や最近起きた事件の解説、(2)(3)身近なパソコンやスマートフォンといったICT機器のパスワード管理、データ管理、無線利用の安全な設定と使用について、(4)研究・情報倫理、(5)暗号技術、(6)サイバーセキュリティに関する様々な法律、(7)著作権、(8)サイバーセキュリティと社会について学ぶ。評価は各講義の最後に毎回小テストを行い、総合的に行っている。

(1)サイバーセキュリティの概要や最近起きた事件の解説では、サイバーセキュリティ脅威のトレンドを客観的に取り上げるため、IPA(独立行政法人 情報処理推進機構)が提供している情報セキュリティ10大脅威をテキストとして用いている。(2)(3)身近なパソコンやスマートフォンといったICT機器のパスワード管理は、新入生がパソコンやスマートフォンを使用する上で事故を防止するための内容になる。どちらかといえばリテラシー教育に近い内容だが、基幹教育がちょうどよい機会なので是非取り上げてほしいという大学からの要望もあり取り上げられている。(4)研究・情報倫理も同様に、今後実験や研究を学生が行う上で、知らないで研究不正などを行うことを防止するためのもので、これも大学からの要望である。内容は研究倫理が主で、教員、大学院生が定期的に受講する一般財団法人公正研究推進協会が作成した教材に基づいた内容である。(5)暗号技術では、情報セキュリティを

構成する3大要素や、各暗号方式の解説を行っている。(6)ではサイバーセキュリティに関連する法律を取り上げている。(7)著作権では、文化庁が提供している著作権を理解するための教材を用いている。(8)サイバーセキュリティと社会については、SNSなどを取り上げて、実社会でのサイバー空間の匿名性や、また、本人が匿名と思っていても技術的には本人を特定できるケースがあることなどを解説している。

サイバーセキュリティ基礎論は、約2700名の学生を15クラスに分けて実施。サイバーセキュリティセンターが準備した教材を用いて、サイバーセキュリティセンター、情報基盤研究開発センター、大学院システム情報科学研究院の教員によって担当されている。2020年度、2021年度は新型コロナウイルス感染拡大を防止するために、基幹教育のほとんどの授業がオンラインで開講され、サイバーセキュリティ基礎論もオンラインで開講した。オンライン2年目の2021年度は教員がオンライン授業の実施に慣れてきたため、サイバーセキュリティ基礎論については同一時間に複数の教員が同じ内容を座学で教えていることを利用して、複数のクラスをまとめて授業することで教員の負担を下げることができた。しかし、対面型の講義が重要視されてきた2022年度からは再び対面に戻した。対面授業時の感染拡大防止策の一つとして、一教室あたりの学生数の上限が従来の7~8割に設定されたため、コロナ前は15クラスであったのが、23クラスに増えて開講をしている。

講義の評価は困難であるが、最近、大学院でデータ駆動型関連のデータセキュリティを担当した際に、「一部は学部1年生の時に受講したサイバーセキュリティ基礎論で習った内容なので復習になる」と話したところ、本学から大学院に進んだ学生は飲み込みがよかったように感じられた。

3 企業から見たサイバーセキュリティ

総合科目・フロンティア科目の一つである、企業から見たサイバーセキュリティは2016年度から開講している。Yahoo! JAPANの社員が講師となり、近年発生している社会を脅かすサイバーセキュリティの事件や事故の背景で起きていることをわかりやすい言葉で解説する。前期・後期それぞれ夏学期、冬学期に開講しているこの授業は、サイバーセキュリティ基礎論を春学期に受講した上で、そのアドバンスト版的な位置づけになる。講義では、今の世の中でトレンドを形成している分野(決済系サービスや、個人情報保護等)を中心にその

分野とセキュリティがどのように関わり、お客様に安心・安全なサービスを提供しているかについて、企業の現場の事例を元にリアリティのある話題を提供している。この講義は学生に人気があり毎学期厳しい抽選が行われている。しかし、感染拡大防止のためのオンライン開講の際、すべての履修希望を受け入れたところ、1000名近い学生がオンラインで受講していた。

4 サイバーセキュリティ演習

もう一つの総合科目・フロンティア科目の講義は、サイバーセキュリティ演習である。サイバーセキュリティ演習は、専攻教育の3~4年向けに演習を行いながら開発が行われた、文部科学省の事業(2016-2020年度)であるenPiT2(成長分野を支える情報技術人材の育成拠点の形成)の演習を基にしている。最近は、IPAが提供している脆弱性体験学習ツール AppGoatを教材として用いている。演習では、まず、Webアプリケーション・サーバの脆弱性について知識を持った学生が誤って事故を発生させることを予防するため、enPiT2で別途作成した、情報倫理教育を徹底的に行っている。enPiT2で作成した教材の内容には、サイバーセキュリティ基礎論で習った内容も含まれているが、復習としてちょうどよい内容になっている。実際の演習は2日間の集中講義で、この情報倫理教育の後に開講されるため、AppGoatのすべての内容を扱うことはできないため、典型的なWebアプリケーション・サーバの脆弱性についてハンズオン形式で演習を行っている。内容は、クロスサイトスクリプティング、ディレクトリトラバーサル、セッションのハイジャック、SQLインジェクションと典型的なものを扱っている。感染拡大防止のためのオンライン授業が主流だった時期はこの演習もオンラインで実施した。対面では20名くらいを上限にして開講していたが、オンラインでは100名以上を受け付けて演習を行った。2022年度からは、対面型の演習に戻す。なお、演習は理系・文系問わず履修を希望するすべての学部1年生が取り組めるような内容にしている。

このように九州大学サイバーセキュリティセンターでは全学1年生に入学してすぐの春学期にサイバーセキュリティの基礎となるものや、夏学期以降にIT企業によるより進んだサイバーセキュリティに関する講義、さらに、学部1年生向けのサイバーセキュリティのハンズオン形式の演習を提供し、本学のサイバーセキュリティ教育を行っている。

大学における情報セキュリティ対策とKINDAI-CSIRTの体制及び活動について

池田 勝
学校法人近畿大学
経営戦略本部デジタル戦略室長

1 KINDAI-CSIRTの設立

学校法人近畿大学では、2013年以降「情報セキュリティポリシー」、「情報システム運用基本規程」などの情報関連規程及び情報システムガイドラインの制定を行ってきた。しかし、2015年に国内で多発した個人情報漏洩事件は他人事でなく、サイバー攻撃は高度化・巧妙化し、情報セキュリティインシ

年度	インシデント件数	内容
2015 年度	4	・学内プリンタ管理画面への外部からアクセス可能な状態　1 件 ・サーバー配下に新規ディレクトリと不正な HTML ファイルを置かれる　1 件 ・ランサムウェア感染　2 件
2016 年度	12	・メールアカウント乗っ取り及び SPAM メール送信　2 件 ・ランサムウェア感染(全データ暗号化)　1 件 ・不審なメール　5 件　・ウイルス検知　1 件 ・学内サーバの授業ページ改ざん　1 件　・マルウェア感染　1 件 ・不正な書き込み　1 件
2017 年度	8	・ID/PW 窃取の可能性のあるアプリの存在　1 件 ・バックドア検知　1 件　・ランサムウェア感染疑い　1 件 ・Web サーバからの個人情報漏洩　1 件　・ランサムウェア感染　1 件 ・Web サイト改ざん　1 件　・フィッシングメールへの ID/PW 入力　1 件 ・PCのウイルス感染　1 件
2018 年度	3	・メールアカウント乗っ取りの可能性　1 件 ・遠隔操作被害　1 件　・フィッシング SMS　1 件
2019 年度	2	・メールアカウント乗っ取りの可能性　1 件　・DDoS 攻撃　1 件
2020 年度	1	・マルウェア感染　1 件
2021 年度	10	・フィッシング SMS による Apple ID/PW 窃取の疑い　1 件 ・学内の別プリンタからの個人情報アウトプット発覚　1 件 ・メール誤送信　5 件　・メールアドレス /PW 漏洩の疑い　1 件 ・Web ページ改ざん及びフィッシングサイト遷移　1 件　・DDoS 攻撃　1 件
合計	40	

[図 1]年度別インシデント発生件数と内容(疑い含む)

デントが経営に与える影響も増大している。このことを背景に、情報セキュリティインシデントを早期に発見・解決するとともに、事前対策、事後対応を行うことを目的として、2016年10月、本法人の教育・研究・事務及び医療に係る情報システムを統括する総合情報システム委員会のもとに、「情報セキュリティインシデント対応チーム」（以下「KINDAI-CSIRT」という）を設立した。チーム長には総合情報システム委員会の委員長（当時）が就任し、メンバーには本法人のICT運用担当部門である総合情報システム部の職員を配置した。主にこのチームが、大学の各キャンパス及び附属学校等のインシデントを全て受け付けて対応する組織として稼働することとなった。また、併せて日本シーサート協議会にも2017年1月に加盟した。

2 KINDAI-CSIRTの初期の活動

KINDAI-CSIRTは、チーム長（兼任）1名を含む5名でスタートし、［図1］に示すように、本法人内の全ての情報セキュリティインシデントについて対応を行ってきた。また、インシデントを防ぐための事前対策として、理工学部情報学科（現：情報学部情報学科）教員の協力のもと、教職員向け情報セキュリティ研修やサイバー攻撃メール対応訓練を定期的に実施してきた。さらに、Webサイトなどの脆弱性診断も、情報セキュリティ専門会社に委託して計画的に行ってきた。

しかしながら、西日本各地に点在する6つのキャンパスや多数の附属学校等を有する本法人の情報セキュリティ対策をわずか5名のスタッフで対応するには限界があり、本法人内の各拠点に情報セキュリティ対策を担うスタッフを置く必要性が生じてきた。

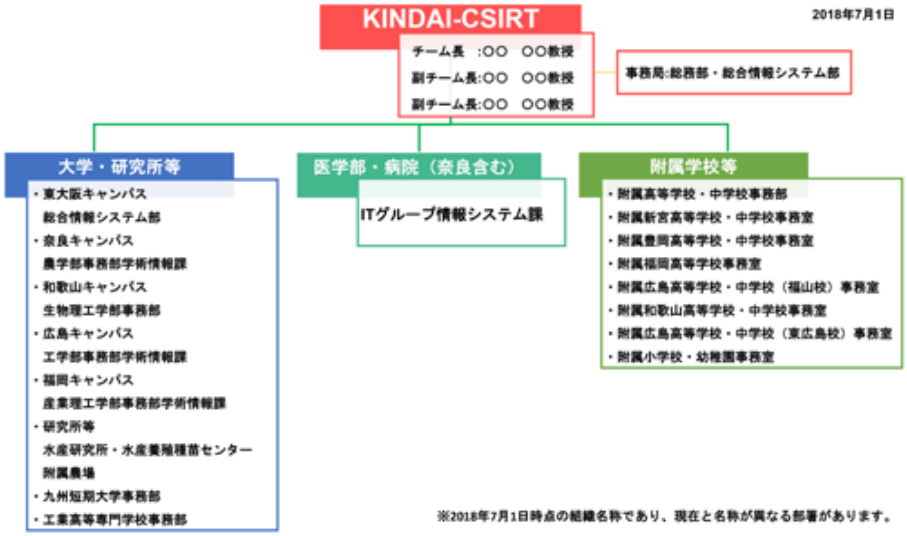
3 KINDAI-CSIRTの体制強化

法人内の情報セキュリティインシデントについて組織的に対応するため、2018年度第1回総合情報システム委員会において「情報セキュリティインシデント対応チーム（KINDAI-CSIRT）運営規程」が承認され、同年7月に施行された。同規程の内容は、要約すると次の2点である。

①各キャンパス・附属学校等において、情報セキュリティ

インシデントが発生した際に対応窓口となる「情報セキュリティ担当者」の設置

②KINDAI-CSIRTチーム長を補佐する副チーム長の2名以上の設置（内1名は医学部・病院の情報システム委員会から推薦を受けて任命）



[図 2]近畿大学情報セキュリティインシデント対応チーム構成

これにより、各キャンパス・附属学校等での情報セキュリティインシデント発生時の対応について、KINDAI-CSIRTを中心とした組織づくりができた[図2]。併せて、情報セキュリティ担当者向けの研修を毎年実施することで、担当者の意識高揚を図っている。

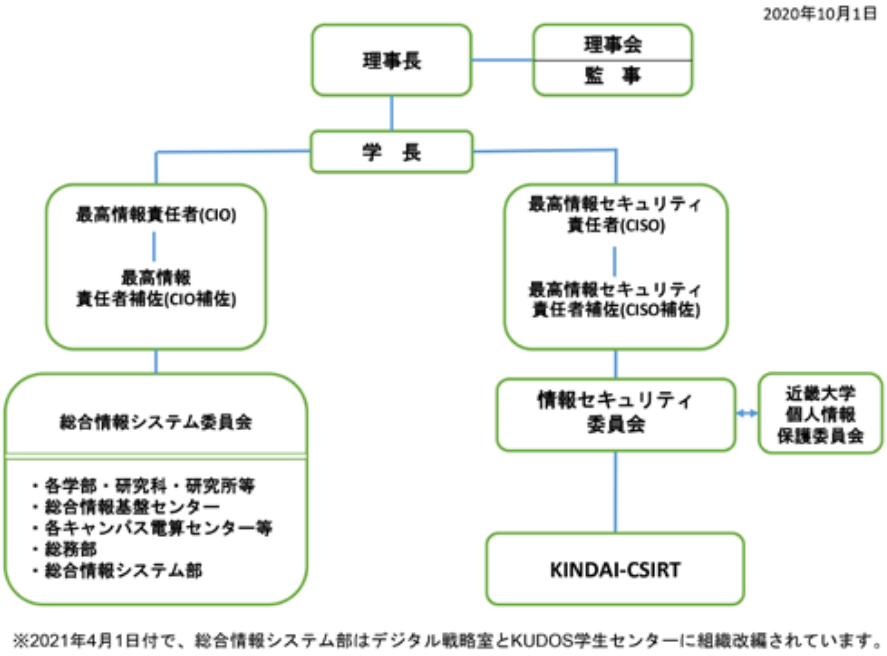
4 最高情報セキュリティ責任者（CISO）の設置

2019年5月24日付で、文部科学省から「大学等におけるサイバーセキュリティ対策等の強化について」の通知があり、本法人においても、さらなるサイバーセキュリティ対策に向けての体制づくりが必要との認識が強くなった。そのため、総合情報システム委員会の承認を受けて文部科学省通知に沿った体制づくりの検討を行い、他大学や民間企業も参考にしながら組織づくりを行った。

2020年10月には、文部科学省通知に基づいて情報セキュリティ体制を一新[図3]。総合情報システム委員会から独立して、情報セキュリティ委員会が新たに設置され、最高情報セキュリティ責任者（CISO）及びCISO補佐が任命された。この組織変更に伴い、KINDAI-CSIRT

は情報セキュリティ委員会の下に置かれることとなり、CISOの指揮の下、法人内の情報セキュリティ体制が強化された。

また、2021年4月には、KINDAI-CSIRTの中心的な所管部署である総合情報システム部が、経営戦略本部デジタル戦略室と大学運営本部KUDOS学生センターに組織改編された。両所管ともKINDAI-CSIRTの構成員であるが、情報セキュリティインシデント対応等の専門的な業務は、経営戦略本部デジタル戦略室の職員が担うこととなった。



[図 3]情報システムおよび情報セキュリティに関する新体制

5　KINDAI-CSIRTによるインシデント対応及び対策

KINDAI-CSIRTは、前述のように取り巻く環境の変化に順応しながら、現在はチーム長と3名の副チーム長に、各拠点2名ずつの情報セキュリティ担当者を加えた、総勢50名ほどの体制となっている。

本法人内における2015年度からの情報セキュリティインシデント報告は総数40件[図1]であるが、とりわけ2021年度は東京2020オリンピックの開催国としてサイバー攻撃を受けやすい状況にあり、本法人でもWebサイトの改ざんやDDoS攻撃など様々なインシデントが発生した。また、こうした外部からの攻撃だけでなく、個人情報漏洩の可能性のあるメール誤送信という事案も発

生した。内容によっては、文部科学省への報告を行ったうえで本法人公式Webサイトにおいて謝罪・報告を行った。

いずれもKINDAI-CSIRTによって迅速に対応することができ、重大なインシデントに至ることはなかったが、臨時の情報セキュリティ担当者ミーティングを開催して注意喚起をするとともに、メール誤送信防止ソフトの導入や、該当所管に対する全員参加の情報セキュリティ研修の実施といった改善対策を行った。

こうした特別な対応はKINDAI-CSIRTの活動のほんの一部であり、主な活動としては日頃からすべきことを継続して行うことが重要であると考えている。継続的な対策として行っているのは、以下の3点である。

①教職員向け情報セキュリティ研修
②サイバー攻撃メール訓練
③Webサイト等の脆弱性診断

①の情報セキュリティ研修は、2015年度から東大阪キャンパスの教職員を対象として開始したものである。当初は同じ内容で複数回開催し、最後にWebで確認テストを行って受講確認とした。2019年度からは、東大阪キャンパスで実施した研修を録画し、後日、本法人全体に公開することで、対象を本法人内の全教職員とした。2020年度からは、新型コロナウイルス感染症拡大防止のため、事前に収録した研修動画をYouTubeで配信している。受講履歴は、最後に行う確認テストの受験状況で判断している。（2015年度・2016年度は満点を取るまで繰り返しテストを受験させていたが、現在は、テスト結果から理解度が低い分野を分析し、翌年度の研修内容に反映している。）

②のサイバー攻撃メール訓練は、2015年度から東大阪キャンパスの教職員を対象に実施し、2019年度からは本法人内の全教職員を対象として年2回行っている。対象者のうち1000名程度をランダムに抽出して訓練メールを配信、2021年度からは対象人数を2000名に拡大して実施している。当初はトラップファイルを仕込んだ訓練メールを自前で作成していたが、2021年度2回目の訓練からは情報セキュリティ専門会社に委託することとした。これにより、最新の情勢に基づく形で訓練することができており、分析結果も提出されるので対策に活用している。

訓練を開始した当初は、「悪戯なメールを送付して業務に混乱をきたすとはけしからん」といった意見もあっ

た。しかし、報道等で情報セキュリティインシデントが世間を騒がせ、KINDAI-CSIRTの活動によってインシデント対策の重要性が認知されたことによって、徐々にこの訓練の意義が認識されてきたと感じている。とはいえ、訓練を行うと、トラップファイルを開いてしまった者から情報セキュリティ担当者へ報告がされないケースが未だにあることも確認している。KINDAI-CSIRTとしては、インシデント発生時の速やかな情報連携を重要視しており、報告漏れは大きな問題だと捉えている。今後も継続して訓練を行うことに加え、新たな対策を検討する必要もあるだろう。

③の脆弱性診断は、本法人が管理するWebサイトのコンテンツ管理画面等を対象として、年に1回、情報セキュリティ専門会社に委託して実施しているものである。2014年度末から2015年夏頃にかけて、Webサイトの改ざん及びネットワーク共有ドライブやネットワークプリンタからの情報漏洩が数件発生したことを受けて実施するようになった。診断結果を受けて、誤って学外からアクセス可能な状態にあるものを非公開にするなどの直接的な対処にとどまらず、修正すべき点として指摘のあった内容を取りまとめて「公開Webサイト運営における遵守事項」として本法人内に周知するなど、インシデント発生前に先手を打つ活動にもつなげている。

6 KINDAI-CSIRTの今後の活動

2021年度開催の情報セキュリティ委員会において、2018年から導入した2段階認証（本法人の多くのサービスで利用しているシングルサインオンに実装）の必須化が可決され、段階的に実現している。また、USBメモリ等の可搬型記憶メディアの原則使用禁止も決定しており、今後その対応を行っていく予定である。

情報セキュリティインシデントはいつでも発生する可能性があり、内容によっては重大な機密情報や個人情報の漏洩を引き起こして、関係者や大学に重大な損害を与えることになる。そのため、KINDAI-CSIRTでは、常に本法人内のインシデントに対して警戒を行っており、万が一、発生してしまった場合にもスムーズな情報連携を可能にする体制づくりや、教職員への継続的な啓発活動が必要であると強く認識している。

変化する修学環境とセキュリティ

中嶋 卓雄
東海大学学長補佐（情報統括担当）

1 カレッジ構想とオフィス構想の実現

東海大学では建学80周年にあたる2022年4月に「日本まるごと学び改革実行プロジェクト」と題した全学的な改組改編を実施し、キャンパス構成を見直して全国5キャンパス8校舎に整備したほか、新学部の設置や学科を再編し23学部62学科・専攻体制とした。従来のキャンパス単位から、複数の学部を統合して〝カレッジ〟という概念を入れ、湘南キャンパスで5カレッジ、全国で10カレッジとして構成し、事務組織も教員組織の構造的な変革に合わせ、カレッジオフィスとして大幅に構成を変え再出発した。

今回の改組のように教員・職員組織の異動が今後も活発化することも踏まえて、人の属性に紐づくアクセス権限の設定について、勤怠系のシステムとの連動についても議論を始めている。また、異動の活性化を想定して、湘南キャンパスのPBXによる内線網をWi-Fi網＋IP網によってクラウド化し、公衆網とも相互接続させることにより、リモートワークでの内線網の活用も始めている。またIVR（Interactive Voice Response）を一部で導入し、録音や自動応答により問い合わせに対応している。クラウド化により電話による場所に縛られることがなくなったため、より柔軟な業務形態が実現できたが、新しいセキュリティ体制と、その強化が必要になっている。

2 サイバー空間での多様な教育環境とセキュリティ

コロナ禍によって大学における教育手段も大きく変化し、教育環境として補助教材を充実させた。本学は、近畿大学、帝京大学と「私立総合3大学アライアンス」を2021年4月16日に締結した。このアライアンスは、志を共有する私立総合3大学が、コロナ後とその先の次代を見据え、より高い次元の教育・研究成果を社会へ還元していくこと

を目指している。このアライアンスの具体的な実現として、2021年から「NHKライブラリー」の111番組の共同利用を実現し、2022年度においては201本の番組を提供している。毎月の利用は実現時点から月3千人程度となっており学生への補助教材として充分に利用されている。ユーザ認証に学術認証フェデレーションを利用して学内の認証サーバとの連携により容易に全学の学生に利用環境が提供できている。一方で、図書館の利用が大きく制限されることになったため、図書コンテンツを電子図書に移行してきた。電子ブックは丸善、紀伊國屋が提供している合計15440タイトルを導入し、教科書および参考書として活用している。認証は複数用意し、学内認証だけではなくベンダーの認証系でも利用できる。学生への電子データの利用拡大と同時にセキュリティ面での教育は必須となっている。SNSへの投稿などの社会的ルール、著作権の遵守など、情報倫理などに対する教育が必要である。今後も学生向けのセミナーなどを企画する予定である。

コロナ禍により教育手段・手法も遠隔講義に大きく移行した。これは本学のように全国的にキャンパスを展開する大学にとって、最大である湘南キャンパスの人的リソースが全学に提供できるため、開講科目の増加などの多様性が増えることになった。遠隔講義に利用したシステムはクラウドに移行し、OpenLMSおよび動画も自由に配置できるMicrosoft365について、科目に沿ってシステムを選択して利用してきた。動画や動的なノートの整理・管理など幅広く利用が可能であった。クラウド化と認証を学内の認証系を利用することにより、学生にとって多様な講義が提供できている。

一方、入学予定者および卒業生向けのシステム整備を進めてきており、学内の認証系に追加するなど、一部のコンテンツについては、それぞれ個人向けのサービスを提供している。また、卒業生向けに証明書のコンビニ発行を実現するなど、徐々に遠隔サービスの向上を実現している。セキュリティ的な視点からは、個人情報の収集と、その情報に対するアクセス権限の設定については、厳密に議論しながら進めているが、〝可用性〟との関係から、業務改善も伴った作業となっている。

教育環境・コンテンツについてはクラウド化に移行したため、クラウド上でのアクセス制限に関係するセキュリティ対策が必要となっている。

3 情報の質によるセキュリティの強化

事務・業務系のデータについては、学内のFirewallの下、情報へのアクセス権を制限したストレージで運用している。しかし、業務の電子化に伴いそのボリュームの増加スピードは早く、今後はBoxなどのクラウドストレージの導入を検討している。クラウドストレージの利点として、①容量設定が無制限、②スマホを含めた多様な端末からのアクセス、③多様なグループによる情報アクセス権限の設定、④セキュリティ監査に必要なログや履歴管理等が可能であることが挙げられる。特に多要素認証や、データアクセス管理において柔軟なセキュリティ機能が強化されているなどの理由から、導入に向けて活動している。ストレージ環境が充実することにより、事務・業務系の端末もVirtual Desktopなどへの移行が容易になる。コロナ禍においてすでにRemote Desktopなどは導入済みであるが、アクセス権限の多様さとリモート業務の容易さによりクラウドストレージの導入が有効である。

一方、学生・保護者からの問い合わせ、学内での問い合わせなど、情報がデジタル化するに従って、HPや学内のコミュニティサイトへ公開される情報の系統的な配置、管理が必要になってきている。従来、業務上の理由により、業務組織構造に準じて情報・ファイルが配置されていたが、公開のレベル、問い合わせのカテゴリーレベルも考慮して情報の階層的な配置が必要となってきている。本学でも学生・保護者からの問い合わせにチャットボットなどの利用を検討しているが、問い合わせの回答に早くリーチするために、問い合わせの分類から、逆にファイルの配置や共有化などが必要だと考えており、抜本的な情報配置について検討している。

大学で扱う情報には学生の個人情報や、研究活動によって得られた機密性が高い情報が多く存在する。このような情報は、政府が定めた情報セキュリティ対策基準（ガイドライン）に準じて、組織での対策を決定する必要があると考えている。情報の質の定義において、従来の「取扱注意」ではなく、セキュリティの3要素（機密性、完全性、可用性）のそれぞれに対して、どのような「格付け」を実施するのかについて、議論が必要である。情報の格付け区分に対して情報の取扱制限を設定し、情報のライフサイクルの各段階において特性に応じた対策が必要になる。情報の格付けは、セキュリティの3要素ごとに異なった意味を持っており、その本来の意味を理解した上で、学内の重要な情報資産につい

て、それぞれ3要素に対する格付けをする方向で議論を始めている。また、取扱制限について、例えば、機密性の場合、単なる「注意」ではなく、コピー、配布、印刷、転送、再利用などの個別の行為に対して「禁止」である旨の制限を定義し、情報資産ごとに設定する方向で議論している。

4 組織としての持続的なセキュリティ強化

組織としてのセキュリティ強化に関して、運用・管理に関係した組織と、主にエンドユーザを対象として情報システムの利用者に分け、それぞれ規定の定義と実体化に向けて検討を続けている。運用・管理体制としては、情報資産として登録している管理部署のセキュリティ責任者が、情報セキュリティ対策の手順を決定し、委員会組織の中で合意をとりながら実施する予定である。また、新年度になった段階で前年度の情報セキュリティインシデントの発生状況とその対応方法について、自己点検をし、その年度の方向性を決定していく予定である。

具体的なサイバー攻撃に対応する組織として、ネットワークやサーバなどの監視体制の強化が必要である。トラフィックの日常的な収集や自動的に検知し隔離するシステムの導入など一部で実施してきた。これらの対応は、タイムリーに実施する必要があり、もし攻撃を発見した場合には、すぐに運用管理者において情報を共有するとともに、対策を実施する必要がある。エンドユーザに対しては、セキュリティ教育が必要であり、FD、SDによるセキュリティの必要性を訴えている。また、端末やUSBの持ち出しの禁止や、移動における注意点、さらには業務用に利用するPCに対するアプリのインストールの制限など、具体的な対策としてセキュリティに対する認識を強めてもらっている。特に、一般ユーザへ広まりやすいEmotetなどの攻撃に対しては、その対策も含めて迅速な対応が必要である。

おわりに

学内におけるセキュリティ管理体制の充実とその質的向上は重要な問題であることは認識されているが、まだ十分とは言えない。また、関連組織との十分な情報交換や、PDCAの確立など、今後も議論が必要である。一方で、セキュリティの強化により費用的な問題も発生するので、その重要性を正確に評価しながら対策の強化を推進していきたい。

シーサートの設立とセキュリティ強化
―東京電機大学における取り組み事例―

高橋 陽子
東京電機大学総合メディアセンター事務部長
TDU-CSIRT CSIRT長

はじめに

東京電機大学は1907年に東京・神田に創立された「電機学校」を前身とし、創立以来受け継がれる建学の精神「実学尊重」、教育・研究理念「技術は人なり」のもと、時代の変化に柔軟に適応しながら、技術を通して社会の未来に貢献できる人材を育成している。大学と大学のブランド価値を守るために必要なセキュリティインシデント対応および発生の予防を行う組織として、本学では2016年に東京電機大学シーサート［TDU-CSIRT（CSIRTはComputer Security Incident Response Teamの略）］を設立した。

本稿では、本学におけるシーサートの設立から、これまでに実施したセキュリティ強化の取り組み、情報セキュリティに対する大学関係者（学生・教職員）の意識向上に向けた啓発活動などについての事例を紹介する。

1 TDU-CSIRT設立の経緯・背景

本学では、2016年度より社会人向けに履修証明プログラム「国際化サイバーセキュリティ学特別コース（CySec）」を開講。セキュリティ分野で本学が注目される中、学内のセキュリティ強化は本学の「顔」の一つであるとして、理事長・学長・情報統括責任者（CIO）の主導によりシーサート立ち上げのプロジェクトを推進した。

シーサート設置にあたり、最初の目標として、シーサート間の連携を目的とする日本シーサート協議会（正式名称：日本コンピュータセキュリティインシデント対応チーム協議会）への大学組織としての初の加盟を目指して急ピッチで作業を進めた。専門のワーキンググループにおいて、

シーサートに関する体制や関連規程、インシデント対応フロー等の整備を進め、2016年6月に情報セキュリティ最高責任者（CISO）およびTDU-CSIRTを設置、同時並行で進めていた日本シーサート協議会への加盟（大学組織として第一号）も実現した。

2 TDU-CSIRTの概要

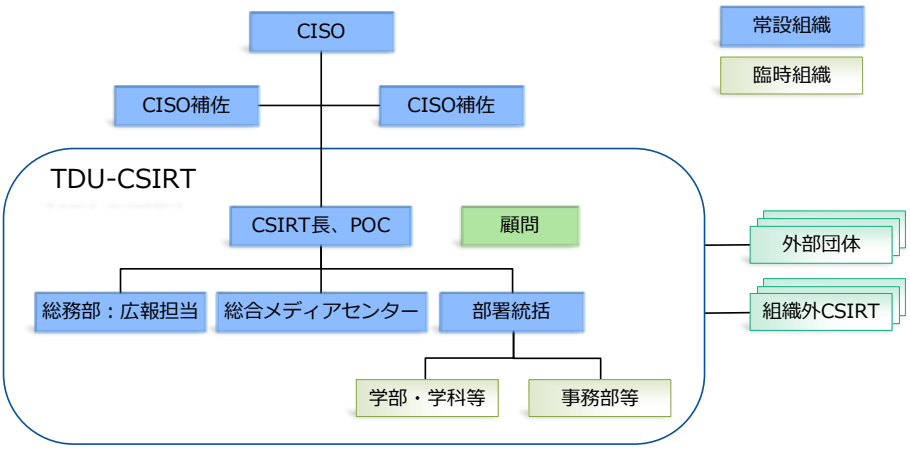
シーサートは大学内のインシデントの「消防団」として機能し、信頼できる対応・対策窓口を提供する。

インシデントは必ず起きるものという前提のもと、インシデントを「起こさない対策」から「起きたときの対策」に移行する。それとともに、インシデントによる被害の拡大防止と迅速な復旧を図ること、日常の訓練を行い、学内のセキュリティに関する意識向上を図ること等もシーサートの重要な役割である。

体制としては、情報基盤（インフラ）を担当する総合メディアセンターが中心となり、［図1］に示す体制とした。

TDU-CSIRTはCISOの直属組織として、専任職員は置かずに部署を超えた兼任組織として構成している。

インシデント対応や各種セキュリティ対策の実施等は総合メディアセンターが担当、マスコミ対応や文部科学省への報告等は総務部が担当する。また、CSIRT長はCISOやCISO補佐と連携しながら対応にあたり、CISOは必要に応じて理事長・学長へ報告を行うこととしている。



CISO　：Chief Information Security Officer
POC　：Point Of Contact

［図 1］体制図

3 TDU-CSIRT設立後に実施したこと

TDU-CSIRTの設立後、まずは学生・教職員等にCISOとTDU-CSIRTを知ってもらう必要があった。メール等で周知するだけでは不十分であると考え、本学では初の試みとなる「標的型メール攻撃の訓練」を併せて実施することとした。

この訓練は全教職員（非常勤教員を除く）を対象に疑似攻撃メールを送信し、メールの添付ファイルの開封やメール本文に記載したURLへのアクセス状況を集計した。結果としては担当業者が実施している訓練の開封率の平均値である約20%に比べて比較的良好な開封率（約15%）であった。その後、標的型メール攻撃の訓練は、2018年度までの3年間継続して実施し、開封率は約3%にまで低減し、着実に訓練の成果が出ていることを確認した。

あわせて、TDU-CSIRTのWebサイトを立ち上げ、情報を発信する環境を整えた。注意喚起からセキュリティの啓発的な内容の提供等、シーサートではさまざまな情報発信が必要となる。TDU-CSIRTのWebサイトは学外からも閲覧可能なページと学内者のみがアクセスできるページの2部構成とし、学内者のページでは学内向けのインシデントや注意喚起情報を掲載している。

それとともに学内者のページでは、セキュリティの啓発的な内容をブログで分かりやすく説明するようにした。このようなブログ記事等のWebサイトの情報更新は多くのマンパワーが必要であるが、注意喚起情報等をWebサイトで広く周知するため、普段から多くの人に見てもらえるようなコンテンツ作り等、魅力あるWebサイトを提供することが今後の課題である。

4 セキュリティ対策の全面刷新

TDU-CSIRT設置前はインシデントを検知するための機器がなく、インシデントの検知や調査が非常に困難で、外部指摘により発覚することが多かった。このような状況に強い危機感を持ち、2017年度にセキュリティ対策の全面刷新を行った。

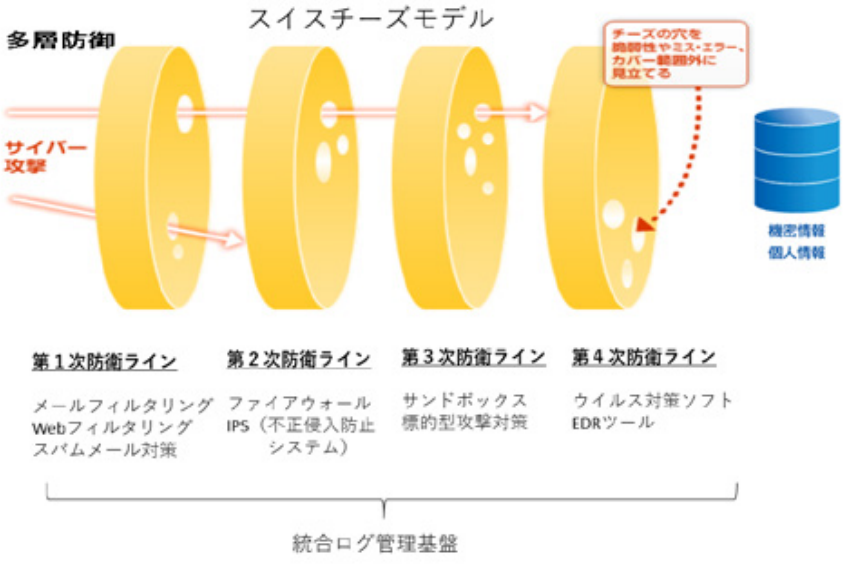
導入検討段階では、大学ネットワークの出入口で全て

の通信を監視し、インシデントを検知するための「ネットワークセンサ（サンドボックス）」、インシデント対応のためのツールである「EDR（Endpoint Detection and Response）」、多くのインシデントの発生源となる「メール対策」の3つを中心として複数ベンダの製品を実際に本学のネットワーク内に設置して検証した。

それとともにTDU-CSIRT顧問の佐々木良一教授のセキュリティ研究と連携し、標的型攻撃に対してコストとリスクを考慮したセキュリティ対策の最適解を導き出した※1。その結果、メールフィルタ等の入口対策で全ては防げないが、初期段階で攻撃メールを防ぐことは攻撃者の侵入を防ぐ効果が大きいこと、侵入後の内部対策・出口対策は必須であることを確認し、［図2］のとおり入口から出口までの対策をバランスよく配置した「多層防御のセキュリティ対策」を構築した※2。人間の病気に例えると、入口対策が予防医学、内部・出口対策が臨床医学に相当し、どちらも重要かつ不可欠である。

それに加えて、大学の情報システムに脆弱性が認められたため、新たに認証用のクラウドサービスを導入し、ポータルサイト等で2段階認証を必須とした※3。

セキュリティ対策の全面刷新により、本学では9割以上のインシデントの早期発見・対処が可能となり、外部指摘による発覚がほとんどなくなった。



［図 2］多層防御のセキュリティ対策

5 インシデント対応の流れ

TDU-CSIRTのインシデント対応の流れは大まかに次のようになる。

1 セキュリティ機器のアラートでインシデントを検知
2 アラートのIPアドレス等の情報により端末の設置場所、管理者を特定
3 管理者にインシデントについて説明と協力依頼
4 隔離処理および一次対応
5 詳細調査
6 対処および復旧、再発防止策の検討

本学ではセキュリティ機器のアラートを起点にインシデント対応を行うケースが多い。隔離処理（ネットワーク遮断）については、セキュリティ機器とファイアウォール等を連動させ、自動で行っている大学もあるが、過検知の恐れもあり、本学では自動での強制隔離は今のところ実施していない。研究室等の管理者（教員等）に十分な説明を行った後に隔離処理を行うことにしている。その後、管理者がICTに詳しい場合には調査を依頼し、それが難しい場合にはTDU-CSIRTが直接調査を行う。

6 外部シーサート関連組織との連携

巧妙かつ複雑化するサイバー攻撃に迅速に対応するためにはシーサート単独では困難な状況であり、同じような状況や課題を持つシーサート同士による情報共有が大変重要である。TDU-CSIRTは連携組織として、「日本シーサート協議会」と「学術系CSIRT情報交流会」に加盟している。

「日本シーサート協議会」は業界を問わずに400を超える企業・団体等のシーサートが加盟し、多くの専門的なワーキンググループでさまざまな活動が行われている。TDU-CSIRTは、その活動実績が認められ、2018年に日本シーサート協議会より表彰を受けた［図3］。

「学術系CSIRT情報交流会」は千葉大学が中心となり、約40の大学や研究機関等の学術機関のシーサートや情報セキュリティ部門が活発に情報共有を行っており、いち早く大学等に特化したセキュリティ情報を得ることができる。交流会は現時点で10回実施され、第5回交流

会は本学を会場とした。

[図 3]日本シーサート協議会からの表彰

おわりに

TDU-CSIRTについて設立の経緯からこれまでに実施したセキュリティ対策についての事例を紹介したが、シーサートはただ設置すればよいということではなく、それを契機として必要な対策を繰り返し行っていくことが重要である。シーサート関連機関等から得られた情報からいち早く対策を立て、インシデントを未然に防ぐこと、発生したインシデントを分析し、自組織に不足する対策を導き出して再発防止を行うこと等、シーサートの地道な活動が大学と大学のブランド価値を守っていくことに繋がっていく。

本学のシーサートはまだ発展途上ではあるが、今後もセキュリティ向上への活動を着実に進めていくとともに、本学の取り組みの事例が他大学のセキュリティ向上の一助となればと願っている。

※1 情報処理学会論文誌 Vol.59 No.3 1082-1094(Mar. 2018)
「イベントツリーとディフェンスツリーを併用した標的型攻撃に対するリスク分析手法の提案と適用」

※2 FireEye（現 Trellix）導入事例
https://www.fireeye.jp/company/customers/tokyo-denki-university-customer-story.html

※3 Swivel Cloud 導入事例
https://www.securitystrings.com/download/sw_pdf/CS_TDU_191023.pdf