事業活動報告 NO. 2

平成26年度 大学情報セキュリティ研究講習会 開催報告

1. 概要

大学、短期大学には、「教育」、「研究」、「組織運営」という三つの柱があり、それぞれにおいてIT環境の情報セキュリティという観点では、「信頼性の高いインフラの提供」、「情報資産の保護」、「安全性・継続性のある運用体制の醸成」が重要である。

その一方で、大学の教育・研究現場でも不正アクセス事件や情報流出事件が繰り返し発生しているという現状である。さらには、今年度はオンラインバンクにおける不正送金問題が社会問題となり、今後は大学の法人部門もその大きなリスクに晒されていくことになる。また、特に大学では近い将来想定される大規模災害などのリスクへの対応が難しく進んでいない点も看過できない。

上記の現状を受け、本協会では、情報セキュリティの危機管理能力の強化を目指して、標的型攻撃などのサイバー攻撃全般への対策と、情報資産の保全及び業務継続に向けたガバナンス強化の指針を提示する講習会を8月19（火）～8月20日（水）に東海大学高輪キャンパスで開催した。本協会の加盟・非加盟の大学・短期大学から参加を募集し、58名(43大学）の参加があった。

本講習会では、全体会としてセキュリティ専門家による講演会、および演習としてディスカッションや技術実習を行うコースを設けた。

さらに、最終セッションでは、新たに、全受講者が共同でインシデント対応を行う演習を設置して、大学としての総合的な対応方法について理解を深めた。

2. 全体会

全体会は、「サイバー攻撃の最新傾向とその対策」を主眼に据えた構成とした。そのアプローチとしては、標的型攻撃を中心とした最新のサイバー攻撃パターンの理解、サイバー攻撃防御のための組織内啓蒙活動の実務的側面、さらに、標的型攻撃の事例収集から判明した攻撃側の戦術を示すことにした。

まず、第一の最新のサイバー攻撃の類型の理解については、**高倉弘喜氏（名古屋大学教授）**より**「サイバー攻撃の脅威と最新攻撃パターン」**と題して講演いただいた。

この講演では、サイバー攻撃として標的型攻撃に注目し、その脅威がマルウェアの組織内拡散による情報漏洩および情報データ破壊にあることが説明された。続いて、その防御対策としては、海外でも「インシデント分析」のみならず「インシデントの封じ込め」が重要視される方向性であることが報告された。封じ込めの実現には、攻撃を受けにくいネットワークの構築を目的に、細かいVLANの設定と監視が必須であり、将来的にはネットワークの自動設計へと進むべき指針が示された。

また、昨今、私立大学でも活用の広がっているクラウドに対しては、監視ポイントを一つに絞ることができるネットワークの設計が留意点になることが示された。その上で、仮想環境でファイル・ディレクトリの世代別保存を行うスナップショット機能を有効活用して、迅速な復旧や 侵入者ツールのrootkitなどの監視・影響排除につなげることが防御対策の要になることを主張された。

さらに、最新の危機として、様々な機器がネットワークに接続されていることに注意喚起がなされた。具体的には、インターネットに接続された複合機を経由した機密情報データの漏洩や大学を含むビル設備制御システムの脆弱性情報がインターネット公開されている問題について紹介された。

最後に、これらの脅威に効果的な対応をするためには、新たな大学間連携の枠組みとして、SINETを活用した監視体制の設置、および大学CSIRT（インシデント調査対応組織）や運用委託企業との連携が必要であろうとの展望を述べて講演は終了した。

次に、**「メールの添付ファイルによる攻撃の防御訓練を実践している広島県庁の事例」**と題して、サイバー攻撃防御のための組織内啓蒙活動の実務的側面について、**広島県庁総務局**の**西田寛史氏**から事例を紹介いただいた。広島県庁では４月に標的型攻撃を受けたが、幸い重大事には至らなかった。しかし、

これを重く見た広島県庁総務局では情報システム全体のセキュリティ改善のみならず、人的セキュリティ向上のための対策に乗り出した。具体的には、標的型攻撃メールを模した訓練メール配信の実施である。この取り組みみの優れた点は、運用SEやサポートダイヤルの契約の範囲内で独自に訓練メール送信やその開封者調査・分析を行っている点である。

講演では、実際の訓練メールの形式や開封率、および訓練継続による効果について具体的に提示され、受講者にも大変好評であった。また、各種研修での啓発内容についても開示され、メールの題名、発信者、アドレス、発信時間といった標的型攻撃メールを見分ける基本的な着眼点とその対処方法について共有されていることが発表された。

セキュリティ対策として、セキュリティポリシー（基本方針）の策定やセキュリティプロシージャ（手順）の配布はある程度徹底されているが、今回の講演内容のような訓練の実施は、全国的に見ても珍しいと思われる。私立大学でのセキュリティ向上のための手法として大変参考になる講演であった。

最後に、**「標的型攻撃への具体的な対処法を考察するための組織連携による情報共有」**と題して、標的型攻撃の事例収集から判明した攻撃側の戦術について、**独立行政法人情報処理推進機構**（以下、**IPA**）の**松坂志氏**から講演いただいた。松坂氏は、官民連携によるサーバー攻撃に関する情報共有の取り組み「Initiative for Cyber Security Information sharing Partnership of Japan」（以下、J-CSIPと表記）を推進している。

今回は、J-CSIPの参加企業の標的型攻撃メール情報を全て時系列に並べ、その状態遷移を俯瞰して検証することにより浮かび上がってきた攻撃者の実態について説明された。関連資料は、下記のURLに掲載されている。

・サイバー情報共有イニシアティブ（J-CSIP）
　2013年度 活動レポート
　～「やり取り型」攻撃に関する分析情報の共有事例～
　http://www.ipa.go.jp/files/000039231.pdf
・「やり取り型」攻撃に関する分析図
　http://www.ipa.go.jp/files/000039233.pdf

今回の講演では、攻撃者は初め偵察用のメールを送信してきており、その偽装内容が徐々に真に迫っていくとともに、返信を行うとその返信内容に即した対応、すなわち「やりとり型」の攻撃を行ってくる様が生々しく報告された。また、一度でも標的型攻撃メールに返信する会社があった場合、その後暫くしてその会社の属している業界全体にも同様の攻撃がなされることも判明した。

つまり、現段階では、攻撃者側も単なる自動的なメール送信だけではなく、返信メールに対応する人的資源まで配置しており、ターゲットにしている業界内に取りこぼしのないよう広範に継続的な攻撃を仕掛けてきていることが判明したのである。

本講演により、大学でも標的型攻撃メールを含めサイバー攻撃情報の共有体制の確立が必要となることが示唆された。

3．テクニカルコース

本コースでは、標的型攻撃等発生時のインシデント対応について、組織として対応するための技術と管理の体制において、技術担当者には、関係する技術および最新の動向等を講義および実習を交えて行い、管理責任者に状況等を的確に報告できるよう素養を習得することを目的とした。

はじめに標的型攻撃の手法、マルウェア感染の痕跡調査の解説および実習を行い、その後最新の技術によるマルウェアの監視、マルウェア諜報活動による内部拡散防御に向けたネットワーク設計について習得する。そして、総合演習では、マネージメントコースの管理責任者とともにインシデント発生時の対応を机上で模擬した。

さらに、本コース２日間の概要について、標的型攻撃の現状とその確認を含め大学としての脅威、事故発生時に「被害を最小限に抑える」ための体制の必要性等の意識付けを行った。

（１）典型的な標的型攻撃手法の紹介と実習

標的型攻撃の流れ（７段階）のうち、
　３段階目：初期潜入、
　４段階目：侵入後の基盤整備、
　５段階目：内部侵入調査
に焦点を絞って演習を行った。

具体的には、
・初期潜入におけるマルウェア感染のメカニズムの解説と実際のマルウェアを用いた感染体験
・侵入後の基盤整備で使用される遠隔操作ツール（RAT）を仮想環境上の攻撃端末と感染端末間に構築し、操作する実習
・内部侵入調査で頻繁に悪用される、パスワード認証を迂回するハッキングテクニック「Pass the

Hash攻撃」の解説と実習
を行った。

また、通常ネットワークに接続されていない端末等環境へのマルウェア感染の手法としてUSBデバイスでのショートカットを悪用した手口の実習も行われ、攻撃の容易さと脅威を実感することができた。

（2）標的型攻撃の最新傾向と痕跡調査

セキュリティ調査会社の専門家に、標的型攻撃の最新傾向と実際に感染した端末での痕跡調査方法の解説いただき、実習も担当いただいた。

標的型攻撃は、攻撃対象・目的が明確になっている。この攻撃のために作成されるマルウェア、および隠蔽処理が行われるため、ウイルス対策ソフトでの検知が難しい。

最初のメールにマルウェアを添付するものではなく、繰り返しの送受信メールから標的ユーザへの安心感や先入観を巧妙に利用する。また、攻撃から情報搾取の目的達成まで長い時間をかける。このため同一業者単位等でのインシデント詳細情報の共有体制が必要であることも理解された。

実際の痕跡調査の実習としては、感染端末のハードディスクイメージの取得、アクセスインデックスのPFファイルによる実行ファイルの特定、感染端末のメモリ上プロセスのチェックなどを行った。

（3）標的型攻撃に強いネットワークの設計

入口対策も重要であるが、これをすり抜け内部端末に侵入するマルウェアがあることを前提とした出口対策および内部拡散防止対策が必要である。

ここでは、IPAが提供している「標的型メール攻撃対策に向けたシステム設計ガイド」に基づき、内部ネットワークの監視強化と防衛遮断策の解説を行い、さらにその知識を応用して、攻撃別の具体的対策をまとめたマトリックスシートを作成することで、標的型攻撃に強いネットワークの設計を行った。

（4）標的型攻撃に強いネットワークソリューション

マルウェアの感染経路、感染後の調査、復旧、対策のための証跡機能を持ったソリューションについて、賛助会員の企業より紹介いただいた。

ウイルス対策ソフトは、既知ウイルスに対し感染を防御することができるが、脆弱性を修復することはできない。

感染した端末のフォレンジック（証拠保全）は、専門家の高い技術が必要とされる。しかし、本ソリューションは、各種ファイルを改変確認技術であるハッシュ値の計算を行って記録し、マルウェアの感染・活動について時間を遡って検出した上で、感染原因の情報を可視化、さらには感染方法を特定して再感染を防止する。また、通信記録をもとに拡散状況を可視化し、内部拡散の防止対策に活用できる機能等が実習を交え、紹介された。

4．マネージメントコース

本コースでは、大学の教育・研究・経営に関する情報資産を守り、大学の事業を継続していくために情報セキュリティをマネジメントという観点から捉え、災害時における大学の業務の復旧及び継続を実現するための大学間や地域での連携の在り方と、大学におけるインシデント情報共有の活用方法と連携体制の仕組みづくりをテーマに取り上げた。

講習では、災害時等を想定した大学の情報基盤運用の業務復旧・継続を実現するための対策・体制、私立大学間における情報セキュリティに関するインシデント情報共有の仕組みづくりについて講演、情報提供及びグループ討議を通して検討し、大学間での連携、情報共有の必要性・有効性を確認し、それらの体制構築への取り組みが重要となっていることを共有した。また、講演では、インターネット・バンキング攻撃を取り上げ、急速に被害が拡大しており、もはや大学の法人部門も大きな脅威に晒されつつあることを確認した。

講習を通して、情報セキュリティの対応・対策において、今後、大学間でさまざまな分野での連携・協力体制の構築がより一層求められることを共有する講習となった。

コースには23名が参加し、所属は約８割が情報システム部門であり、他には教務部門、法人部門、教員等であった。役職は、管理職もしくは教員が約７割以上を占めた。

（1）災害など非常時における情報基盤運用の業務継続性に関する検討

情報セキュリティ対応の基本として、情報漏洩事故対応や個人情報保護法の知識などを交えて情報紛失及び情報断絶のリスク分析と大学の業務継続の条件や対策について情報提供した。また、大学間連携による情報基盤BCPの実現として、情報システム基盤運用における大学間連携の事例から大学間での相互協力の条件などについて情報提供を行った。

グループ討議では、各大学における情報管理の体制がどうなっているのかを意見交換し、短期間で大学の事業復旧・継続を実現するための体制や対策について、検討を行った。グループ討議の成果は模造紙にまとめ、掲示し、グループ間の共通点や相違点などを確認し、共有した。

（2）サイバー攻撃を含むインシデント情報の紹介及び情報共有の活用と連携体制の検討

一般社団法人全国銀行協会からインターネット・バンキングへの攻撃手口と考えられる対応策、全国銀行協会でのインシデント情報の共有に関する取り組みについて講演をいただき、教育・研究部門のみならず、財務部門等の法人部門においても身近なところで情報セキュリティに関する攻撃の危機に晒されていることを認識するとともに、インシデント情報の共有に向けた取り組みの必要性を共有した。

また、情報セキュリティ研究講習会運営委員会での大学インシデントを共有する取り組みの中間報告として、私立大学を中心に大学で起きたインシデント情報を共有し、対策の参考及びガバナンスへの危機意識醸成の素材することを目的とする仕組みづくりの提案に向けた情報提供を行った。

これらの講演及び情報提供を受けて、大学間でインシデント情報を共有するために求められる条件、仕組み及び体制について、ワールド・カフェ手法によるグループ討議で「どうしたらできるか」を検討した。大学間でのインシデント情報共有体制の必要性・有効性を共有するとともに、そのためには先ず学内での情報共有から実現していくことが重要であるとの意見が多くうかがえた。

（3）まとめ

今回の研究講習会では、講習日程が２日間となり、マネジメントコースでは情報セキュリティに関して「業務継続への連携対応」と「インシデント情報共有」という二つのテーマを取り上げることができた。このテーマは共に情報セキュリティ研究講習会運営委員会で今年度から調査・取りまとめの取り組みを行っており、中間報告ではあるが、その成果を反映させることができた。

グループ討議では、時間が短いとの意見もあったが、ワールド･カフェ方式を取り入れるなどで、より多くの受講者と討論し、情報を共有できる機会を提供することができた。今回、大学間での連携・情報共有の実現に向けて、先ず各大学内での連携・情報共有に早急に取り組む必要があることを共有できたことは今後に向けての成果と考える。

また、大学における情報セキュリティに関しては、従来、教育・研究分野に視点が向く傾向にあったが、インターネット・バンキングへの攻撃を取り上げることで法人部門においても大きな脅威になっていることの啓蒙にもつなげることができた。しかしながら、法人部門からの受講者数を増やすことにはつながらず、今後、研究講習会の周知や開催時期などを含めて検討していく必要がある。

5．総合演習

２日間の講習の仕上げとして、テクニカルとマネジメントの受講者と合同でインシデントの机上模擬対応演習を行った。総合研修は、両コースの枠を越えた今年度の新たな取り組みであった。

具体的には、技術担当者と管理責任者に役割を分け、例題標的型攻撃のストーリを題材に「検知・初期対応」フェーズで行う「想定被害のリストアップ」、「初期対応の準備と対応」、さらに対応内容の検証をグループディスカッション形式で実施した。目標としては、グループ別の情報セキュリティ事故最終報告書の作成とした。

これにより、情報セキュリティに関わる技術担当者、管理責任者それぞれ双方の役割や動きを共有することができ、万一に備えた卓上演習という新たな取り組みとして成果があった。

また、グループワークによって、両コースの受講者間で交流が図れたことも成果として挙げられる。

一方、想定の一つではあったが、ディスカッション時間の短さを指摘する内容が多く、時間配分などの課題もみえ、改善していく余地を残した。

今後も、テクニカルとマネジメントの両コースで情報セキュリティに関する対応を一丸となって進めていくことは、実際に行われる対応環境に即しており、研究講習会の効果をより高めることにつながると考える。

最後に、ここ数年講習会参加者の減少が続いており、講義中心ではなく、実習・体験を中心とした内容、およびその内容をわかりやく表現した案内等を今後の課題としたい。

文責：情報セキュリティ研究講習会運営委員会