事業活動報告 NO. 5

平成27年度 大学情報セキュリティ研究講習会 開催報告

1. 概要

サイバー攻撃は、非常に巧妙になっており、大学現場でも情報資産の漏洩、不正アクセスが発見されるなど衝撃を与え大きな社会問題となっていること、インターネット・バンキングにおいても法人部門が攻撃されインターネット全体に対するリスクマネジメントの対策強化が求められている。

そこで、本協会ではサイバー攻撃に対する脅威について、法人の役員、学内の執行部、教員、職員、学生など構成員一人ひとりが防御意識に基づき行動できるようセキュリティ対策組織の構築と運用体制、課題を探求することを目指した研究講習会を８月25日（火）～26日（水）に工学院大学で開催した。本協会の加盟・非加盟の大学・短期大学及び賛助会員から参加を募集し、78名（60大学、１賛助会員）の参加があった。

講習会の進め方としては、サイバー攻撃に対する脅威について認識を共有化するため、危機意識徹底の重要性を働きかける場として「全体会」を行った上で、インシデント対応に関する知識の習得及び実習を行う「テクニカルコース」とセキュリティ対策の実施及びセキュリティ意識の醸成を学内に推進・普及していく方策を検討する「マネジメントコース」を設けた。その上で、テクニカルコースとマネジメントコース双方の受講者が協働して、実践的な演習ストーリーによる模擬演習と防御意識に基づき行動ができるよう、「総合演習」を設けてセキュリティ対策組織の在り方及び取り組みについて点検評価の内容を確認した。

2. 全体会

（1）「サイバー攻撃の最新手口と防御対策」

松坂　志 氏（情報処理推進機構ｾｷｭﾘﾃｨｾﾝﾀｰ主幹）

冒頭に情報処理推進機構で作成されたビデオ「あなたの組織が狙われている！標的型攻撃その脅威と対策」を通じて、標的型攻撃のリスクについて基本的な事柄が紹介され、その後、松坂氏から攻撃の手口と防御について説明された。松坂氏は、サイバー情報共有イニシアティブの担当者であり、重工業系を中心とした企業への標的型攻撃メールを収集・分析し情報共有を行っている。その豊富な知見から、ある攻撃者が平成24年から平成27年まで31ヶ月に亘って送信したと推測される112通の標的型攻撃メールを例にあげ、その文面や添付されたマルウェアがどのように微修正を加えられながら、長期に亘って継続して攻撃利用されているか具体的に説明された。

この攻撃者の使ったマルウェアの攻撃手法には、マクロウイルスや実行ファイルの拡張子隠蔽のように既に古典的なものも見られた。しかし、進化の早いICT分野では、かえって古い攻撃手法を知らない場合も増えてきており、意外にも効果的な攻撃になるなど盲点と言える例も紹介された。また、攻撃時期やメール送信時刻の統計からも明らかに日本企業をターゲットと想定しており、注意を怠ると簡単にマルウェア感染の被害に合うことが分かった。

その上で、対策や心構えとして、攻撃者の存在を認知すること、基本的なセキュリティ対策の実施の徹底及び攻撃手法の理解、攻撃情報の共有が重要であることが強調された。

（2）「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」

大坂　元一 氏（全国銀行協会企画部次長）

昨年度の本講習会マネジメントコースに引き続いての講演であった。インターネット・バンキングは、個人・法人ともに普及しつつあるが、不正送金の被害が社会問題化している。特に、平成25・26年度は被害件数が1,000件を超えて被害額も14～16億円に達している。また、被害金融機関の内訳では、地方銀行や信用金庫・信用組合に被害が増えており、もはや個別金融機関での対応は限界が見えていることが示された。これらの事実を踏まえて、犯罪者の主な手口として、フィッシング、マルウェア感染、

スパイウェアによる電子証明書の搾取などがあげられた。

対策としては、利用者側でのセキュリティ対策が必須であり、具体的に銀行の提供するセキュリティ対策を複数組み合せることや犯罪の手口を知っておくことの重要性が言及された。

また、不正送金の被害に遭った場合にも、個人契約は原則として銀行が補償し、法人契約の場合も銀行による補償を検討するという申し合わせであることが強調された。

その他、大学生が深く考えないまま口座の名義貸しを行ってしまい、その口座が不正送金に悪用されたことが分かると、その口座名義がブラックリストに載ってしまい、就職後の給与口座として使えないなどの実害が発生していることも報告され、大学で何らかの指導が必要となろう。

（3）「大学における情報セキュリティ対策の取組と経営執行部の役割」

三浦　文博 氏（愛知大学情報システム課長）

大学におけるセキュリティガバナンスの模範となり得る同大学より、その内容や導入経緯など具体的に紹介された。同大学では、情報セキュリティポリシーと、それに基づく組織整備を実施しており、まず、情報セキュリティポリシーと付随するマニュアル群の体系が紹介された。情報セキュリティポリシーの重要性はもとより、マニュアルも教員・職員・学生向けに分けて整備されている点が特長になっている。実際の運用面では、学生向けの新入生ガイダンスでセキュリティ意識の喚起を行った上で、情報処理推進機構の動画を活用した自習用コンテンツなどを提供していることが言及された。また、教員には、セキュリティ手引きの配布、定期的な情報提供や注意喚起のメール配信などが行われ、事務職員には内部監査や講習会まで実施されていることが紹介された。

次に、情報セキュリティ管理体制が紹介され、危機管理委員会の一部会として感染症対策や防災と並列して情報セキュリティ部会を構成している。情報セキュリティ部会長は、理事（副学長または学部長）であること、また部会委員にも理事（大学評議員）が選出されているなど、大学の方針決定に実効性を持たせる工夫が大きな特長である。

さらに、危機対策管理のためには、非常時の立ち上げに緊急対策本部を設けることと、その対策本部の役割と構成員について言及された。コンパクトながら実効性のあるセキュリティガバナンスの構成が示されたが、課題としては実際の緊急時に体制が機能するのかといった点や、まだまだ教職員・学生へのセキュリティ意識醸成が必要であるとした。

会場からの関心も高く、様々な質問が出たが、本体制を構築するきっかけについて質問があり、当時の情報システム担当課長の具申から発足したという経緯が紹介された。

3．テクニカルコース

本コースでは、「標的型サイバー攻撃の疑いがある場合の調査、対処方法の習得」及び「標的型サイバー攻撃を受けた場合の対処方法・手順の習得」を行い、それぞれのケースにおいてシステム担当者としての適切な行動がとれることを目標とした。

まず、標的型サイバー攻撃の疑いがある場合の診断と初動対応の習得をするために、疑わしいメールの添付ファイルの開封やリンク先への接続を保護領域としてのサンドボックス環境を用いて、安全に確認する方法の講義と実習を行った。さらにマルウェア（遠隔操作ウィルス）へ感染した場合にどのような脅威があるのか、どのようなことが可能となるのか、実際にマルウェアの挙動を実習で確認することにより理解を深めた。

次に標的型サイバー攻撃を受けた場合の対処方法・手順を習得するために、攻撃者の「内部侵入・調査」手法を、具体的な攻撃手法を例にあげて実習を行った。さらに実習で得た知見をもとに、想像上の大学システムを例として、標的型サイバー攻撃を受けた場合の被害を予想した演習を行った。

（1）標的型攻撃などが疑われる場合の診断と初動対応の演習

標的型サイバー攻撃は、業務上重要なメールを装って送られてくる場合が多い。それ故、受信したメールを一読しただけでは、標的型メール攻撃なのか否かを判断するのは非常に難しい。この判断には、不審なメールを見分けるための一般的な知識を習得するばかりでなく、開封した際に観測されるマルウェア特有の不審な振る舞いについても理解する必要がある。本セッションでは学内者より、不審なメールを受け取ったとの相談を情報システム部門が受けた場合を想定し、仮にどうしてもメールの添付ファイルの内容を確認しなければならない場合にどう対応するのかについて

・複数のウィルスチェックで検査する
・外部のウィルスチェックサイトを活用する
・サンドボックス環境で実際に添付ファイルを開き、挙動を確認する

という手法を例にとり、それぞれの有効性とリスクについて実習を通して確認した。

中でも「外部のウィルスチェックサイト」の活用には、機密保持の観点から細心の注意が必要であるとの紹介があった。

さらに、マルウェアに感染したPCを足掛かりとして、攻撃者はどのような操作が可能になるのかを事前に理解することは、防御側が適切な初動対応を取るうえで極めて重要である。そこで、マルウェアに感染させた仮想PCを用意し、感染側PCのリモートコントロールやファイルの送受信、キー入力情報の搾取などが可能なことを、攻撃者の立場で体験し、マルウェアに対する理解を深めた。

（2）インシデント発生時の対応フローチャートに基づく演習

標的型サイバー攻撃を受けていることが明らかになった場合は、事前に定められたインシデント対応フローチャートに基づき、組織的な対応を進めることになる。情報システム部門で最初に検討すべきことは、「被害の調査・範囲の予想」とそれをもとにした関連部門への「報告・連絡」である。本演習は、システム担当者がこれらの対応を迅速にとれる知識を得ることを目標とした。

まず、「被害の調査・範囲の予想」を行うために、攻撃者はPCをマルウェア等に感染させた後、どのような技術を用いて内部システムの調査や侵入行為を行うのかを紹介した。最初の「ネットワークの調査」段階では、代表的なポートスキャンの手法を取り上げた。次に「端末間の侵害拡大」段階ではPass the Hash攻撃、ネットワークモニタリング、オートコンプリート機能で保存したパスワードの盗用など、他端末への代表的な攻撃手法を取り上げるとともに、何故そのような攻撃が可能なのか、OSのどのような機能を悪用しているのかを解説し、例として共有のためのSMBサービスの役割について紹介した。最後に「サーバへの侵入」段階ではPass the Hashの他にPsTools等を用いた方法を紹介した。各段階での攻撃手法については、それぞれ実習にて動作確認を行い、理解を深めることとした。

次に、ここまでで得た知見をベースに「被害の調査・範囲の予想」の演習を行った。演習は、想像上の大学のシステム構成図と設定ポリシーを提示した上で、仮にある１台のPCでマルウェア（遠隔操作ウィルス）が発見された場合、

・どのサーバや端末を調査すべきなのか
・どのような情報が流出した可能性があるのか

を受講者各自で考察する、机上演習の形式で行った。

攻撃者による「内部侵入・調査」に対しては、「ネットワークレベルの対策」、「端末レベルの対策」、「ドメインレベルの対策」等があるが、業務との関係でサービスの制限を行う等の対策は困難な場合が多い。また仮に対策を行ったとしても、内部侵入の拡大を遅らせる効果しか期待できないという意見もある。もはや標的型サイバー攻撃における「入口対策」、「出口対策」には限界があることから、防御側は、侵入されたことにいかに早く気づき、被害を最小限に抑えるか、その対策と準備を行うのが重要と考え、本演習のまとめとした。

４．マネジメントコース

サイバー攻撃は巧妙化し、官公庁・企業・大学等での不正アクセス、情報漏洩が社会問題となっている。本コースは、情報セキュリティをマネジメントするという観点から、大学の役員・教職員一人ひとりが標的型サイバー攻撃への被害を最小限に抑えるための対策意識を持つとともに、大学執行部としての組織的な働きかけの工夫ができるよう講習プログラムを構成した。プログラムの流れとして、サイバー攻撃の脅威について理解を深めた上で、インシデント対応組織の必要性と整備課題を考察し、また、情報セキュリティ対策のPDCAサイクルの活用のため、セキュリティ自己点検基準について講習を実施した。

（1）大学内でのインシデント対応組織の構築・取り組みについて考える

全体会のテーマである「サイバー攻撃の脅威と危機意識の徹底対策」について各大学における問題としてグループ内で意見交換することで、サイバー攻撃の脅威についての課題認識を深めた。

次に、「インシデント対応チーム（CSIRT）の構築と情報共有について」をテーマとした満永拓邦氏（JPCERTコーディネーションセンター）の講演では、「情報セキュリティを取り巻く現状と情報セキュリティ緊急対応体制（CSIRT）」、「CSIRTスタータキ

ットの紹介」、「CSIRT連携と情報共有」について説明され、理解を深めることができた。引き続き「大学内でのインシデント対応組織の構築・取り組みについて」をテーマにグループ討議を行い、大学内インシデント対応組織の必要性、その構築に向けての問題点と課題、対応組織のあり方と組織イメージ、インシデント情報の大学間共有の必要性について理解を深めることができた。

（2）ガバナンスの役割とセキュリティ自己点検基準について考える

現在、本協会で検討を進めている「大学情報セキュリティ運用ベンチマークテスト」について、昨今の情報セキュリティ基盤を揺るがすインシデント発生状況、マイナンバー制度での安全管理措置の義務化、情報セキュリティ対策のPDCAサイクルのCheck（評価）として活用するなど、その必要性及び概要を説明し、参加者によるテストを実施した。

ここでは、ベンチマークテストの必要性を理解し、ベンチマークテストの項目（1）情報セキュリティ対策のガバナンス、（2）情報セキュリティ対策全般、①情報セキュリティに対する組織的な取組状況、②物理的（環境的）セキュリティ上の施策、③情報システム及び通信ネットワークの運用管理、④情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況、⑤情報セキュリティ事故対応状況の内容について理解の共有を図った。

今年度の情報セキュリティ研究講習会運営委員会の課題としては、サイバー攻撃の脅威を周知し、防御意識に基づく行動が組織的に展開されるよう大学及び大学連携による対策の働きかけを研究・協議すること、業務継続性確保の点検があげられている。マネジメントコースにおいて、「大学内でのインシデント対応組織の構築と取り組み」と「セキュリティ自己点検基準」をテーマに取り上げることで、今年度課題にその成果を反映させることができたと考える。

本コースの進め方については、テーマを絞ることで受講者が意見を出しやすく議論を深めるための工夫をした結果、大学内インシデント対応組織の必要性、その構築に向けての問題点と課題について各大学の状況における課題を抽出し、共有することができた。

また、本コースへの部門別参加状況は、情報システム部門：71%、教育・研究部門11%、法人部門：17%となっている。情報セキュリティへの対応課題は、情報システム部門に留まらず、大学全体のリスク管理の課題であることから法人部門を含む多くの部門から参加が求められる。今後、講習会への参加者増に加え、各部門からの参加を促すことができるようテーマ設定、周知方法について検討していく必要がある。

5．総合演習

「総合演習１」では、昨年度より取り入れた演習形態としてテクニカルコースとマネジメントコース双方の受講者が協働し、三つの想定例によるインシデントレスポンスを模擬する演習とした。

演習形態は、インシデントの技術的確認情報をもとに組織としてどのような手順や判断をするのか、インシデントレスポンスワークシートにより対応の進め方を確認できるものとした。

ワークシートは、想定例毎に何をどのように調査するのか、調査結果から管理者が何をどのように判断して次の手順に進むのか、穴埋め回答をする方式で模擬体験できるものとした。

当初は多くの回答をテクニカルとマネジメント双方のグループデスカッションと対応例の提示を含めて進めていく予定としていたが、当日の受講者数と会場構成の関係から、説明をSkypeで一斉に行うことにした。そのため準備した体制や運営では想定したすべての内容を進行させることが困難なことから、内容を大幅に削減して行い、回答の対応例等の資料は後日ホームページよりダウンロードする対応とした。

「総合演習２」では、「大学情報セキュリティ運用ベンチマークテスト」について、前日にマネジメントコースで行った回答の集計結果を報告するとともに、自己診断の一つの指標として活用し、経営執行部に向けたセキュリティ対策状況のまとめとして活用されたいとの説明及び紹介を行い、防御意識を高め、持続させるための体制・取り組みについて理解の共有を図った。

受講者からは時間不足の意見があり、素材の精査や演習方法・時間配分等について、今後の改善課題としたい。

文責：情報セキュリティ研究講習会運営委員会