事業活動報告 NO. 2

平成28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、官公庁、企業、学校でも情報資産の窃取・漏洩などが頻発化し、大きな社会問題となっている。とりわけ、学校現場では成績情報・個人情報がネットワーク経由で窃取されるなど情報セキュリティ管理の甘さが以前から種々指摘され、その対策について学校としての対応が求められてきている。具体的には、組織的にサイバー攻撃の脅威を周知し、防御行動が展開されるよう構成員全員によるリスクマネジメント対策の強化が求められているといえる。

そこで、本協会では、サイバー攻撃に対する防御行動が組織的に展開されるよう理解の普及を徹底するため、情報セキュリティの対策をベンチマークし、課題の洗い出しを行い、自己点検・評価を習慣化する中で構成員一人ひとりがサイバー攻撃の脅威を認識し、大学として段階的にセキュリティ対策や体制を整備できるように課題を共有することを目的に、研究講習会を平成28年８月23日（火）～８月24日（水）に学習院大学で開催した。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、75名（56大学、１短期大学、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防御意識を徹底できるようにするため、情報セキュリティに最小限必要な対策・対応をベンチマークにより振り返ることの重要性及び課題を共有する場として「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「セキュリティインシデント分析コース」と、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「セキュリティ政策・運営コース」を設けた。その上で、２つのコースの受講者が協働して、防御意識に基づき行動ができるようにインシデント対応を想定した「総合演習」を設けて大学現場において必要な対応全体の俯瞰およびそれぞれの参加者大学における課題を議論した。

2. 全体会

（1）「サイバー攻撃の最新動向について」

満永　拓邦氏（東京大学情報学環特任准教授）

最初に、満永氏は、サイバー攻撃の実行者を「愉快犯／ハクティビスト」、「金銭目的の攻撃者」、「標的型攻撃の実行者」の３つのクラスに分類し、それぞれ目的のみならず技術力にも差異があることを説明された。それぞれのクラスの攻撃者が起こした事例も紹介したうえで、ここ数年は最も高い技術力を有している標的型攻撃の実行者が起こすインシデントが増加していることに警告を鳴らしていた。攻撃対象は、政府系組織、重要インフラ事業者、研究機関、機密情報を保有する組織が多く、米国のセキュリティ企業の試算では、これまで数百テラバイトの情報が窃取されているとのことである。実際のところ、侵入の発見は殆どが外部からの通知であり、平均侵入期間が365日という極めて防御が難しい状態であることが示された。また、侵入による経済的被害も大きいこと、つまり情報セキュリティ対策は経営問題の１つであることを主張された。満永氏は、これらの状況を踏まえ、被害が発生した場合に備えた事前準備が重要であると結論された。

（2）「経営執行部（役員）の情報セキュリティに対する取り組みについて」

宮川　裕之氏（青山学院大学情報メディアセンター所長）

私情協情報セキュリティ対策問題研究小委員会で検討した標題の内容について宮川担当理事より

説明した。

大学の経営執行部が取り組むべき４つの柱として、サイバー攻撃による情報資産・金融資産の脅威やインシデントに対する危機意識の共有、情報セキュリティに関する学内ルールの構築と周知徹底、情報セキュリティ委員会や情報センター部門による防御体制の構築と点検評価の徹底、教職員に対する教育や模擬訓練の実施とその徹底をあげた。

（3）「大学情報セキュリティベンチマークリストの紹介と評価方法」

井端　正臣氏（公益社団法人私立大学情報教育協会事務局長）

昨年度公開した大学情報セキュリティベンチマークリストを、より大学現場に必要な観点に絞り込み、重み付き評価が可能な配点を設定した。更に、ベンチマーク評価結果に従って、どのようなセキュリティ対策を実施するかモデルを提示した。このセッションでは、その概要について解説した。

（4）「ベンチマークリストの評価結果と改善に向けて取り組むべき対応」

満永　拓邦氏（東京大学情報学環特任准教授）

本講習会に先立ち、加盟校に依頼したベンチマークリストの集計結果を用いて、満永氏が解説を行った。各設問に対しは、改善に最低限必要な対応状況を提示した点が明確な指針を与えていた。また、具体例として、セキュリティ対策にかける予算の割合や対策費費用の項目なども目安を得ることが出来た点は、受講者にとって今後の実務に活かせるであろう。

3．セキュリティインシデント分析コース

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と対処方法の習得」と「標的型サイバー攻撃を受けていることが明らかな場合の調査・対処方法の習得」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調査と対処方法」を習得するために、メールの信憑性を判断する手法並びに標的型サイバー攻撃の典型的な手法について講義と実習を行った。

次に、「標的型サイバー攻撃を受けた場合の対処方法」を習得するために、攻撃の痕跡調査と一時対応についてネットワークレベルでは何が行えるのか、そして、攻撃を受けたPCでは何が行えるのか、それぞれ講義と実習を行った。

（1）標的型サイバー攻撃の疑いがある場合の調査と対処方法の演習

標的型サイバー攻撃は、メールを利用して初期潜入を行うケースが多い。その一方で、自組織が標的型サイバー攻撃を受けている可能性を指摘する外部からの通報もメールによる場合が多い。そこで受信したメールの信憑性を確認するために、最低限どのような点に着目し判断をすればよいのかを、メールの本文やヘッダー情報、添付ファイル等から確認する方法を紹介した。

次にサイバー攻撃の有無を確認する際の前提知識として、初期潜入に成功した攻撃者がどのようなステップを経て内部侵入を進めていくのかを講習した。さらにインターネット等から切り離された閉鎖的なネットワーク環境において、PCが実際にマルウェアに感染する様子や、感染後にはリモートコントロールや画面のモニタリング、ファイルの送受信が攻撃者から可能になることを実習により体験した。そして攻撃者はどのような手法を用いて内部調査や侵入を進めていくのかを、コマンドを実行しながら確認し、標的型サイバー攻撃の一連の流れに対する理解を深めた。

（2）標的型サイバー攻撃の痕跡調査と一時対応の演習

標的型サイバー攻撃を検知することは一般的に非常に困難であるが、組織内にあるネットワーク機器のログを丹念に調べることにより、攻撃の有無を確認できる可能性がある。ここではマルウェアに感染したPCと攻撃者が用意したサーバ（C&Cサーバ）との間で行われる不審な通信の痕跡を、ファイアウォールや侵入検出装置（IDS）あるいはProxyサーバのログ等から探し出す手法について紹介し、PC上に構築した仮想ルータを用いて実習を行った。さらに感染側PCの痕跡調査の手法として、イベントログや実行履歴、レジストリエントリ等から、攻撃者が内部調査や感染拡大の際によく用いるコマンドの実行痕跡を確認する手法についても実習を行った。

なお、ファイアウォールにおける痕跡調査の結果、感染PCとC&Cサーバとの通信が現在も継続している場合は、一時的な対応として、通信を強制的に遮断する措置が考えられる。遮断方法には感染PC側で対応する方法と、ファイアウォールで行う方法があるが、今回はファイアウォールを用いて通信の遮断をする実習を行った。

ネットワークレベルでの痕跡調査は有効な手法ではあるが、通信ログが大量に生成されてしまうことや、攻撃者がC&Cサーバとの通信を暗号化することによってIDSによる検知が困難になる等の問題がある。さらにファイアウォールでの通信遮断は、具体的にどのコンピュータやサービスを対象とするのか、情報漏えいのリスクと事業継続の重要性とのバランスの面で、大学毎に事情が異なる。このことについては平常時から方針を検討することにより、インシデント発生時の対応が迅速になることを指摘した。

感染PCの痕跡調査についても、外部に漏えいしたファイルの特定など本格的な調査は、専門機関によるフォレンジックが必要になってくる。そこでこのことを見据えた調査、例えばPCの電源は切らずにLANケーブルのみを抜線するなど、後のフォレンジック作業への影響が少ない対応が必要であることを指摘した。

実際にインシデントが発生した場合、技術担当者は本コースで扱ったような初動対応に加え、再発防止策の検討も必要になる。再発防止のための技術的な改善案として、マルウェアにPCが感染した後、攻撃者による内部侵入や調査を「防ぐ」あるいは「遅らせる」そして「すみやかに検知する」仕組みを導入することがあげられる。最後にこれらを実現するための手法をいくつか紹介し、本コースのまとめとした。

4．セキュリティ政策・運営コース

サイバー攻撃の脅威に対し大学の役員・教職員一人ひとりがそ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、参加大学の状況を共有することでその被害と対策の現状理解を深めた上で、インシデント対応組織の必要性と整備課題を考察した。また、情報や情報セキュリティ関連法令の遵守のための施策について、講演と質疑応答を行った。

（1）各大学のセキュリティ状況の共有と課題化

「各大学のセキュリティ状況の共有と課題化」をテーマとし、グループディスカッションを行った。ディスカッションのポイントは①自大学のセキュリティ対策への現状②セキュリティ対策の進むべき方向性と課題とし、全体会の講演内容、特に、「経営執行部の情報セキュリティに対する取り組について」、「ベンチマークテストの評価結果と改善に向けての取り組むべき対策・対応」を踏まえて行った。議論の中、サイバー攻撃の脅威が各大学で認識される一方、そのための施策の具体化が各大学とも困難である、等の意見が出されていた。また、私情協が進めているベンチマークテストは、今後各大学で進める情報セキュリティ対策の指標となり得るとの認識を持つことができた。

（2）情報や情報セキュリティ関連法令の遵守のための施策を考察

知っておきたい情報漏えい関連の法律と、最近の個人情報保護法と不正アクセス禁止法の改正状況について、当講習会委員であり江戸川大学名誉教授市川昌氏より講演し、次のセッションである「情報セキュリティ対策のための組織的施策」に繋げた。

（3）情報セキュリティ対策のための組織的施策

はじめに、サイバー攻撃の脅威に対応するため、経営執行部、システム部門、利用部門の役割とインシデント発生に対する「予防」、「対処」、「報告、公表」を行うための組織としてのCSIRT（Computer Security Incident Response Team、シーサート）について説明を行った。その上で、グループディスカッションを行い、その中で①サイバー攻撃の脅威に対する組織体制はどのようなものか、②組織整備ための課題は何か、についてこれまでの講演内容、各大学の状況を踏まえた議論を行うことができた。最後に、各グループより考察内容の発表を行いまとめとした。

本コース全体を通じて情報セキュリティ対策の認識を深めること、組織的施策としての体制整備のあり方について考察することができた。次年度向けては、経営執行部での取り組むべき課題とその方策、CSIRTなどの組織体制整備での課題と解決策の考察ができるよう更なる内容の充実を図る必要がある。

5．総合演習

総合演習の形態は、「セキュリティインシデント分析コース」と「セキュリティ政策・運営コース」の受講者が協働し、インシデント対応を模擬する机上演習とし、３年目となった。

これまでの演習形態の反省を生かし、各コース１名ずつの２名を１組として前半のインシデント対応演習を行い、後半では、３組を１班としたグループ討議も行うものとした。

また、「情報セキュリティ事故最終報告書」（サンプル）の記載を目標とし、インシデント対応フェーズを検知、調査および対応、回復・復旧、事後対応の４つのフェーズに分け、各対応フェーズごとに時間配分し演習を進めた。

各対応フェーズにおいては、各コースでの習得事項を踏まえた質問に対し、誰が穴埋め回答するかの役割分担を明示し、以後どのように協議するかの方向を示すものとした。穴埋め回答例は、フェーズ毎に示した。一連のインシデント対応に必要と思われる各種資料（「インシデント対応の机上模擬演習ワークシート」を含む12種）を準備した。

これまでの演習では、一連のインシデント対応手順の終結に至ることができなかったが、今回は内容の優劣は別として目標到達が時間内に完遂でき、総合演習の一つの成果と言えよう。最後にその結果を３つのグループに発表いただき、総括のまとめを行い終了した。

インシデント対応（総合演習）の体制は、SOC（Security Operation Center）、CSIRT（Computer Security Incident Response Team）の２つの役割が必要とされる。情報処理部門はSOCを主業務とし、CSIRTの調整役が行うのが現状である。CSIRTの組織体制は重要なものであるが、情報インシデントの教育・啓蒙活動により小さなインシデントの初期情報の収集（問い合わせ、相談）窓口の設置、運用などの小さな活動からのCSIRT導入も一策である。

文責：情報セキュリティ研究講習会運営委員会