事業活動報告 NO. 5

平成29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、巧妙・大規模になっており、情報資産・金融資産の窃取・漏洩・破壊などが日常化し、大きな社会問題となっています。大学の教育・研究現場でも入試・成績情報、個人情報、その他機密情報がネットワーク経由で窃取されるなどの事例が頻発化してきており、情報セキュリティ管理の甘さが問題視されています。そのためには、構成員全員がサイバー攻撃の脅威を理解し、防御行動を意識して実践するなどのリスクマネジメント対策の強化が求められます。

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にするため、経営執行部による組織的な対応、構成員一人ひとりによる注意と行動、情報担当部門としてのベンチマークによる自己点検・評価・改善の習慣化を通じて、大学の対応力に応じた情報セキュリティ対策の考察を目指して、大学情報セキュリティ研究講習会を平成29年８月24日（木）～25日（金）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者を募集し、60名（51大学）の参加があった。

研究講習会の進め方としては、サイバー攻撃の最新動向、ベンチマークリストにもとづく大学の対応状況、攻撃に緊急対応する専門チームの課題を共有する「全体会」を行った上で、ランサムウェア型攻撃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、情報セキュリティの促進政策と周知徹底する方策を学ぶ「セキュリティ政策・運営コース」を設けた。その上で、技術部門と政策部門の混成チームによる模擬演習と規模別グループによる課題解決演習を行う「総合演習」を実施した。

2. 全体会

「サイバー攻撃の動向と防御行動の点検・評価」

今年度は、サイバー攻撃の最新動向を理解した上で、「大学情報セキュリティベンチマークリスト」によって明らかになったセキュリティ対策・対応の成果を紹介し、経営執行部の情報セキュリティに対する取り組み、情報資産の把握と管理対策、組織的・人的な対応、技術的・物理的対策の問題点を共有化することを目的とし、下記３件の情報提供を行った。

（１）「情報セキュリティ10大脅威」から見るサイバー攻撃の動向
亀山　友彦氏（独立行政法人情報処理推進機構情報セキュリティ技術ラボラトリー）

（２）「ベンチマークリスト評価結果の動向」
情報セキュリティ研究講習会運営委員会

（３）「情報セキュリティ事故に緊急対応するための体制組織化への取り組み」
上原　哲太郎氏（立命館大学情報理工学部教授）

（１）では、独立行政法人情報処理推進機構（以下、IPAと表記）亀山友彦氏がIPA刊行『情報セキュリティ10大脅威2017』（https://www.ipa.go.jp/security/vuln/10threats2017.html）から「標的型攻撃による情報流出」、「ランサムウェアによる被害」、「IoTにおけるセキュリティ脅威の顕在化」について詳しく説明した。本年度の本講習会では、ランサムウェア感染時の対応を具体的なテーマとして扱うため、全大会で理解を深めてから実習に移ることができた。

（２）では、平成28年度・29年度と継続して調査している情報セキュリティベンチマークテストの結果について、満永拓邦氏、松田亘氏、藤本万里子氏（東京大学情報学環）の支援を基に加盟校のセキュリティ対策状況を浜正樹運営委員長が分析・発表した。本協会の加盟校は中・小規模大学（入学定員2,000人未満）が多くを占めるが、今回の調査結果も回答校の約50％が中・小規模大学であった。項目としては、情報セキュリティ脅威に対する危機意識共有やポリシー策定・運用における大学経営層のリーダーシップ、セキュリティ対策予算、情報資産目録の作成、CSIRT設置状況、具体的な対策状況について紹介・講評された。

（３）では、立命館大学の上原哲太郎氏が、「サイバー諜報が当たり前になった世の中で何をどのように守るのか」といった視点で、国立・私立大学や公的機関で発生しているセキュリティインシデント事例をあげながら、組織内での経営層や情報システム担当部門の役割を説明された。特に、最

近注目を浴びているCSIRTについては、火災への対応に譬えて、「緊急時対応の連絡網」という認識でスタートするべきとの主張がなされた。最後に、立命館大学で進行中である「緊急危機対策」（実質的なCSIRT）の設立経緯について紹介された。

3．セキュリティインシデント分析コース

本コースでは、「マルウェア感染被害の状況把握」と「マルウェア感染時の対応手順」をテーマに、マルウェアを用いたサイバー攻撃の実態や仕組みを理解し、サイバー攻撃の疑いがある場合の調査方法およびサイバー攻撃を受けた場合の対処方法・手順を習得することを目標とした。今回は特に、身代金要求型マルウェア（ランサムウェア）感染時の調査・対応方法について演習を行った。

（1）マルウェアの脅威と実例

「マルウェア」とは不正な動作を行う悪意あるソフトウェアの総称として用いられるが、その振る舞いの違いは、感染発覚後の調査活動の内容および範囲に影響する。本セッションではマルウェアに感染した時の影響範囲をいち早く想像できるよう、個々のマルウェアについて自己増殖性の有無や、攻撃者の目的・機能に着目して分類を行った。さらに、過去の感染事例におけるマルウェアの振る舞いを分析することで、マルウェアに対する理解を深めた。

（2）ランサムウェアへの感染と対策

IPA「2017年情報セキュリティ10大脅威」によると、ランサムウェアの脅威は前年度7位から2位へと急激に増している。本セッションではランサムウェアの動きをより詳細に理解するために、実際のランサムウェアによる「感染」、「被害」、「暗号化されたファイルの復元」、「ランサムウェア対策ツールの効果」を仮想環境上のPCを用いて実習と演習を行った。このことを通して、ランサムウェアに感染した場合の被害の範囲を確認するとともに、事前対策、事後対応についての理解を深めた。

（3）標的型サイバー攻撃

ランサムウェアなどマルウェアの感染は、実は大掛かりなサイバー攻撃の序段に過ぎない恐れがある。本セッションは、自組織が標的型サイバー攻撃を受けていると仮定した時の流れ、つまり、初期潜入、内部調査、侵入拡大から情報搾取に至るまでの手法について講習を行った。さらに仮想環境上でPCがマルウェアに感染する様子や、攻撃者からPCのリモートコントロールやファイルの送受信等が可能になることを実習により体験した。そして攻撃者が行う内部調査や侵入手法について確認し、標的型サイバー攻撃の一連の流れと、攻撃を受けた場合の影響範囲についての理解を深めた。

（4）サイバー攻撃に対する調査と対応

本セッションでは、複数のマルウェアを用いた標的型サイバー攻撃を想定し、被害側組織として状況の把握や痕跡調査、一次対応について実習を行った。まず感染したPCにおいてプロセスの実行状況やネットワーク通信を調べ、不審なプロセスが存在しないかどうか、そのプロセスはマルウェアである可能性はないかどうかを確認した。次にログファイルを調査することにより、情報漏えいや内部調査・侵入拡大の痕跡がないかどうか確認を行った。また業者にPCの詳細調査を委託するための準備作業として、PCの証拠保全作業を体験することで、本格的な痕跡調査（フォレンジック）に対する理解を深めた。

セキュリティインシデントへの一次対応は、情報センターのスタッフが行うことが多い。この際、復旧あるいは原因調査のいずれを優先すべきなのか、その方針によって対応内容は異なってくる。特にPCからの情報漏えいの有無などを確認するために、外部の業者に本格的なフォレンジック（記録を収集・分析し、証拠を明らかにする手段や技術）を委託する場合は、電源を入れたまま、ネットワークに接続したままの状態を保ち、なるべく現状のままで調査に着手することが原則である。また、フォレンジックには多大な時間や費用を要する。情報センターのスタッフは、何を優先して一次対応にあたるべきなのかは、マルウェアに感染したPCは誰が使用しているのか、どのような情報が保存されているのか、どのような外部ストレージにアクセスできるのか等、その役割により異なってくるはずである。的確なインシデント対応を行うためには、事前に様々なケースを予想し、対応計画を策定することが大切であるとして、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

経営執行部による組織的な対応、構成員一人ひとりによる注意と行動、情報担当部門としてのベンチマークによる自己点検・評価・改善の習慣化を目指して、被害に遭わないための手立て「予防」、被害を最小限にする「対処」、事後の対応「報告・公表」を適切に遂行するための取り組みについて考察することを目的に個人ワークやグループディスカッションを中心に演習を行った。

テーマとしては、セキュリティ対策の組織対応に関して事前に提示した課題および、個人情報保護法改訂にあたって検討すべき内容をあげた。

（1）情報セキュリティを促進するための政策

最初のセッションでは、事前課題として与えられた下記の３つのテーマから、それぞれの受講者の回答をグループ内で共有した。

① 情報セキュリティインシデント防止対策のための施策
② 情報セキュリティインシデント防止対策を学内周知徹底するための対策
③ インシデント発生時の組織的対応

この内容を基に、ペアワーク等を通して課題の解決策を他大学の受講者からアドバイスしてもらうセッションを持った。その成果をグループ内でまとめ掲示・発表することで全体の課題・解決策の共有を行った。

（2）法改正に伴う情報セキュリティ業務の課題

次に、市川運営委員（江戸川大学名誉教授）より、「業務上知っておきたい個人情報保護法・不正アクセス禁止法の改正のポイント」について解説を行った。この内容を基に、受講者は、「関連法律の改正と業務との関連」をテーマに再度グループワークを行って、法改正に伴う業務の課題をまとめた。

本コースでは、最後に、これまでの議論を経て、受講者自身のアクションプランを作成し、受講後の施策実施のモチベーション向上を狙ってグループ内宣言を行って修了した。

5．総合演習１

総合演習ではこれまでと同様に２コースの参加者（各２名、計４名／グループ）が、ランサムウェア感染のインシデントに対応する模擬の机上演習を行った。

演習ではインシデント発生時に技術担当者と部署責任者が、まずは各自の立場での対応に必要な項目の洗い出しとその方法・内容を二人で検討し、整理する作業を行った。そして、立場を入替え（技術担当者は部署責任者の立場）、各担当者で整理された資料を技術担当者は部署責任者がどのような情報を求めるのか、あるいは部署責任者は技術担当者がどのような指示が必要としているのかなど、違った立場・目線で内容を確認し、情報交換を行いインシデント対応時の必要な項目を整理した。

次に、想定インシデントに対し「SJK大学インシデント対応フロー」による対応演習をグループで行った。この対応フローでは、自大学組織のみの対応には限界（作業時間の確保とインシデント分析結果の信頼性等）があると想定し、専門のセキュリティベンダーを対応プレヤーとして組み入れた。実際の講習では、セキュリティベンダーの顧客対応事例等を含めた相談対応窓口担当者からの解説を行った。

演習の一つの目標として、本インシデントによる個人情報漏えいを想定し、本年５月末に施行となった改正個人情報保護法での委員会への報告義務のための報告書を作成し、CISO役としての本講習会運営委員へ報告するストーリーとした。なお、CISOとの質疑応答も組み入れ、最後に全体に対し各CISOの講評を行った。

総合演習を行ってみて、各大学とも「実際のインシデント対応時に対応フローの手順に沿い進めることができるのか？」といった視点での事前準備ができているかは大変疑問である。実際に、対応フローが作成されている大学も数件見られたが、実際の作成者とは異なって実務担当者からは、その有用性を疑う意見もあった。対応フローを作成することよりも、PDCAによる対応フローの成熟が必要であり、高等教育機関として共通的な対応フローモデルが必要と思われる。

6．総合演習２

最終セッションの総合演習２では、２日間の全講習を振り返って、インシデント対応フローの見直しを行うことを目標とした。

（1）情報提供：「インシデント対応のコスト」

見直しに際しては、大学のセキュリティ対応現場で問題となるコスト面についても検討項目となるため、岡部運営委員（中部大学総合情報センター次長）より「インシデント対応のコスト」の情報提供を行った。ベンダーがセキュリティインシデントに対応する場合の時間的・経済的コストやセキュリティ監視システムの構築費用、また事前アンケートで得た加盟校のセキュリティ対策費用の実際などの概要を述べることにより、現実的な対策状況が共有された。

（2）インシデント対応フローの見直し

次に、グループワークとして、これまでの演習を通して得た知見を基に、事前課題の解決策について改めて検討し、実現性のあるアクションプランのポイントを作成した。その成果については、運営委員が分担して講評した。

7．参加者からのアンケート結果について

インシデント分析コースの理解度は「理解できた５割、概ね理解できた５割」、政策・運営コースは「理解できた３割、概ね理解できた６割、あまり理解できなかった１割」、総合演習は「理解できた１割、概ね理解できた７割、あまり理解できなかった２割」であった。また、参加者からは、感想として、「実施すべき内容が洗い出されて良かった」、「非常時にスムーズな行動の難しさからシミュレーションしておく重要性を感じた」、「報告に必要な情報を整えることが難しく感じた」、「第三者調査を想定した対応や予算化を行いたい」などが寄せられた。

文責：情報セキュリティ研究講習会運営委員会