事業活動報告 NO. 4

平成30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、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にするため、CISO（最高情報セキュリティ責任者）を含む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リストを用いた自己点検・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、研究講習会を平成30年８月23日(木)～24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を募集し、66名（54大学、２賛助会員）の参加があった。

研究講習会の進め方としては、最初に、大学における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、大学における不正アクセス事案とその事後対応事例を共有する「全体会」を通じて、情報セキュリティリスクの確認を行った。次に、全体演習１では、大学における標的型攻撃とその事後対応事例を踏まえて、グループに分かれて研修・啓発の仕組み及び標的型攻撃メール対策訓練計画を検討した。

また、標的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整備計画及びCISOの設置に向けた対策を考える「セキュリティ政策・運営コース」を設けた。その上で、最後の全体演習２では、セキュリティ対策課題の解決に向けた計画・提言を行った。

2. 全体会

「サイバー攻撃の最新動向と対策」

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、さらに大学で起きた大規模インシデントの事後対応事例を詳細に知ることで、情報セキュリティリスクを確認することを目的とし、３件の講演を行った。

（1）「サイバー攻撃の最新動向から見る大学の新たなリスク」

洞田 慎一 氏（JPCERT/CC早期警戒グループマネージャー）

情報セキュリティインシデントについての概要説明と大学で実際に発生した大規模情報セキュリティインシデントの事例紹介があった。特に、標的型攻撃と呼ばれるインシデントが近年大学を対象としていることが強調された。大学における情報セキュリティインシデントに対しては、もはや放置できないため、その脅威やリスクの認識と対策の浸透が重要であることが課題とされた。具体的には、大学内でのマネジメントとして、関係部門と連携したインシデント対応体制の構築と対処能力の向上、情報セキュリティポリシーや情報の取扱規程等の見直し、多様な構成員に対応した教育・訓練や啓発活動の実施、構成員の役割に応じた自己点検や中立性を有する者による監査の実施、また、技術面では、組織内の情報機器の把握と適切なアクセス制御の実施、重要情報を扱う機器へのアクセス等を監視する機能等の実装と組織内で利用しているソフトウェアの適切の更新が大切という結論であった。

（2）「ベンチマークリスト結果に見る私立大学のセキュリティ課題」
宮川 裕之 氏（青山学院大学社会情報学部教授）

私情協の加盟校は、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51％が中小規模大学であった。情報セキュリティの脅威に対する危機意識の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（Computer Security Incident Response Team）設置状況、具体的な対策状況などの項目について紹介・講評された。

（3）「大阪大学での不正アクセス事案とセキュリティ体制の強化」
尾上 孝雄 氏（大阪大学最高情報セキュリティ責任者、副学長）

本インシデントは、平成29年６月に、大阪大学で利用しているグループウェアに不審なログインの形跡が発見されたことがきっかけで被害調査を開始したものであるが、文部科学省への報告は10月、最終的な公表は同年12月であった。この６ヶ月間には、被害状況の調査、組織面・管理面・技術面での課題の洗い出し、さらに再発防止策の実施までが行われており、その多大な労苦について具体的に示された。

本講演によって、大学に大規模な情報セキュリティインシデントが発生した場合に、ガバナンスとしてCISOやCSIRTといった組織が中心となって必要な対応が何かを平時から準備していくべきことが示唆された。

3．全体演習１

本演習では、実際の大学の事例をもとに、情報セキュリティインシデント対応の事前予防や事後対応に必要な手順を理解し、大学構成員全員を対象とした研修・啓発の視点について検討した。

（1）イントロダクション「インシデント対応概論」
本セッションでは、浜運営委員長より、標的型攻撃による情報漏洩を例に、一般的なインシデント対応の流れを概説し、このセッションの方向性について理解を促した。

（2）講演「標的型攻撃メール対策の訓練事例」
早稲田大学情報企画課の高橋智広氏より、学内における標的型攻撃のメール対策の訓練の開始、運営方法、その成果まで詳細に紹介された。

訓練はサイバー攻撃への耐性を高めることを目的とし、「感染予防対応」と「感染拡大防止対応」の２つを目標としている。また受講者へのフィードバックを行っていることも紹介された。

運用面で特徴的な点は、訓練メール受信者にアンケート調査を行い、受信後の行動を把握している点である。

（3）グループワーク「偽装メールの作成」
本セッションでは、冒頭に浜運営委員長より標的型攻撃メールの偽装方法の特徴について情報提供を行い、その後、グループに分かれて、自大学での標的型攻撃メール対策訓練を想定して、偽装メールの作成を行った。

標的型攻撃メール対策訓練には、関心のある受講者が多かったこともあり、大変活発なワークセッションとなった。

（4）標的型攻撃メール対策訓練ソリューション「ITセキュリティ予防接種」解説
JPCERT/CCで2009年度に開発・実験利用した標的型攻撃メール対策訓練ソリューションについて、洞田慎一氏から概要と仕様が示された。pythonが使えるコンピュータと学内のメールシステムがあれば、手軽に訓練メールの送信が可能である。本ソリューションは、既に開発が終了しているが、本講習会受講者が希望すれば無償で提供されることが示された。

（5）教育啓発計画書
全体演習１の総括として、受講者それぞれが自大学で教育啓発計画を経営陣に提案することを想定して、その計画書を各自で作成した。この計画書は、２日目の全体演習２のペアワークで使うことを予告して、初日の全セッションは終了した。

4．セキュリティインシデント分析コース

本コースは「サイバー攻撃の最新動向と対策」と「インシデント対応」をテーマに、標的型攻撃メールを用いたサイバー攻撃の手口と技術的仕組みを理解し、サイバー攻撃に対する事前の備えや攻撃を受けた後の痕跡調査およびインシデント対応手順を習得することを目標とした。さらに最近の情報セキュリティ関連の法整備に対応するために、情報システム部門が考慮すべき対策とシステ

ム設定の演習を行った。

（1）標的型サイバー攻撃

標的型サイバー攻撃とは、ターゲットとなる組織を絞ったメールによる攻撃であり、添付ファイルを開いたり、本文に記載されているリンクから悪意のあるウェブサイトへアクセスしたりすることによって、マルウェアに感染することが多い。本セッションでは、標的型サイバー攻撃の典型的なステップ、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した。さらに仮想環境を用いて、PCがマルウェアに感染する様子や、攻撃者によって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。また、攻撃者が内部調査に用いる手法を確認し、標的型サイバー攻撃を受けた場合の影響範囲について理解を深めた。

（2）痕跡調査のための事前準備

標的型サイバー攻撃を受けた疑いがある場合、個々のPCにてマルウェア感染の事実やアクセスされたファイルなど、様々な不正アクセスの痕跡を調査する必要がある。しかし、有効な痕跡調査を行うためには、PCのデフォルト設定では不十分である。攻撃者の操作内容や実行したツール等の痕跡をイベントログ等から追跡するためには、あらかじめ監査ポリシーを強化しておく必要がある。本セッションでは有効な痕跡調査のための事前準備として、Windows端末の監査ポリシーの強化とsysmonツールの導入作業を実際に行い、イベントログの監視強化とその効果について理解を深めた。

（3）サイバー攻撃の痕跡調査

標的型サイバー攻撃の被害側組織として行うべき一次対応について、実習を行った。まず、感染が疑われるPCの状態を保全するために、フォレンジックツールを用いたメモリやプロセス、ログ等の証拠保全の実習を行った。続いてイベントログより、各種ツールの実行やネットワーク通信の記録を調べ、標的型サイバー攻撃がどの段階まで進んだのか、例えば、内部侵入の拡大まで行われた痕跡があるのかどうかを確認した。最後に、侵入の拡大に用いられる手法としてPass-the-Hash攻撃とPass-the-Ticket攻撃を紹介し、標的型サイバー攻撃を受けたときの影響範囲と事前の対策について理解を深めた。

（4）サイバー攻撃への対策

改正個人情報保護法やGDPR（EU一般データ保護規則）の施行など、様々な法規制が整備される中、我々情報システム担当者もこれらを考慮したシステムレベル、ユーザレベルでの対策が必要となっている。本セッションでは、最新のレギュレーションや動向を紹介し、自大学システム側での対応や改善点を見出すことを目的とした。そして対策技術の一つとして、認証情報の保護とアプリケーションの起動制限を強化したシステム管理専用端末の設定実習を行い、標的型サイバー攻撃への対策と多層防御の考え方に対する理解を深めた。

5．セキュリティ政策・運営コース

本コースでは、情報セキュリティポリシーに基づいた実効性のあるセキュリティ対策基準や対策手順の作成や経営陣を含めた組織的対応のためのヒントとして、次の三つの柱を題材とした。

① 先進的取り組みを行っている大学の事例を参考にして自大学の整備計画を検討
② 組織的に迅速な対応ができるようにCISOの設置と強化対策の考察
③ 情報管理者として理解しておくべき法的知識とその対応についての理解

（1）ビデオ講義「高等教育機関におけるセキュリティポリシーとは」

まず、「高等教育機関におけるセキュリティポリシーとは」と題して、NII（国立情報学研究所）の高倉弘喜氏のビデオ講義を行った。私情協のベンチマーク結果でもセキュリティポリシー策定自体は８割近くが実施しているが、その実効性が求められていることから、改めてセキュリティポリシーの基本的な位置付けを確認した。なお、本ビデオ講義は、私情協のサイトで閲覧可能である。

（2）事例紹介・グループワーク「ベンチマークリストで先進的取組みをしている大学を参考に整備計画を考える」

ベンチマーク結果から、下記の三つのテーマで先進的な取り組みがされている大学の事例を紹介した。

① 情報セキュリティポリシーと対策基準の策定
② 情報セキュリティルールの周知徹底
③ 情報資産の把握とリスク対策

以上の事例を基に、自大学の課題の解決策を受講者同士でアドバイスする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。

（3）講演・グループワーク「CISOの役割と権限の紹介」

洞田氏より、「CISOの役割と権限の紹介」と題して講演が行われた。CIOとCISOの違いから大学におけるCISOの位置付け、およびCSIRTの役割と重要性が説明された。また、企業におけるCISOが果たす役割についても経済産業省・IPA（サイバー経営ガイドライン）からの引用も紹介された。

講演後に、ペアワークとグループワークによる課題と解決案の共有を行った。

（4）情報共有「情報管理者に求められる法的知識とその対応」

市川運営委員（江戸川大学名誉教授）より、「情報管理者に求められる法的知識とその対応」について解説が行われた。

具体的には、改正個人情報保護法、不正アクセス禁止法、著作権保護法、GDPRについて、システム管理やコンテンツ・情報保護の観点で留意すべき点が整理された。

6．全体演習２

２日間の全講習を振り返って、セキュリティ課題の解決に向けた計画・提言を行った。

（1）演習成果の共有

初日の全体演習１の中で行った標的型攻撃メール対策訓練用に作成した偽装メールについて、洞田氏から、「受講者の作成した偽装メールはどれも良くできていたが、最も重要なポイントは、偽装の巧拙が目的ではなく、訓練が目的であることを意識するべき。特に、訓練と演習は異なることを忘れてはならない。訓練のためには、訓練の趣旨の説明、実施告知や添付ファイル開封後の対応手順まで明確にした上での実施が大切である。偽装自体に凝り、受講者を引っ掛けることに方向性が向かうと、無用な混乱を生じ、本来の訓練目的が達成できなくなる恐れがある。」との講評が行われた。

また、受講生同士のペアワークとして、初日の宿題で作成した教育啓発計画書を相互に説明し合い、内容理解を深めた。

（2）セキュリティ課題解決案の策定

セキュリティ課題解決案の策定のために、技術者側と組織管理者側それぞれの視点から、構造化されたクエスチョンシートに受講者自身で回答する形式で、自大学の情報セキュリティ課題と解決案について検討した。

その後、ペアワークとしてそのクエスチョンシートを使いながら、受講者同士でこれまでのコースから得た知識でお互いにアドバイスするセッションを行った。

（3）CISOへの提言・アクションプラン作成

浜運営委員長より、前セッションで使ったクエスチョンシートを今後の大学業務で活かせるように、CISOの立場から業務指示一覧として整理しなおして解説した。最後に、これまでの演習を通して得た知見を基に、受講者自身が実現性のあるアクションプランを作成し、各グループ内において受講者自身がその実行を宣言した。

全体演習の様子

7．参加者からのアンケート結果について

セキュリティインシデント分析コースの理解度は「理解できた４割、概ね理解できた６割」、セキュリティ政策・運営コースは「理解できた３割、概ね理解できた７割」、全体演習は「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」となっていた。また、参加者からの感想として、全体を通じて「学内の人材育成について考える良い機会だった」、「セキュリティ対策はまだまだということに気付いた」。演習を通じて「不正侵入の挙動を確認できたのは大きな経験だった」、「構成員全員に危機意識の共有を図りたい」、「ルール、体制整備など経営層への提案を行いたい」などが寄せられた。