事業活動報告 NO. 3

2019年度 大学情報セキュリティ研究講習会 開催報告

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必要なことから、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、研究講習会を令和元年８月27日（火）～28日（水）に立正大学品川キャンパスにて開催し、大学・短期大学から42名（35大学）の参加があった。

研究講習会は、「全体会」と演習を交えた「セキュリティインシデント分析コース」、「セキュリティ政策・運営コース」で実施した。

全体会

（1）「情報セキュリティ10大脅威 2019」

渡邉 祥樹 氏（独立行政法人情報処理推進機構セキュリティセンター）

独立行政法人情報処理推進機構（IPA）が毎年発行している「情報セキュリティ10大脅威2019」をもとに、組織向け脅威の上位にランクされている「標的型攻撃による被害」、「ビジネスメール詐欺による被害」、「不注意による情報漏えい」の攻撃手口、被害事例、対策について具体的な紹介があった。その中で、特に注意すべき脅威を網羅的に把握し、組織の構成員や役割に応じて、必要な対策を講じていくことの重要性が強調された。

（2）「大学等におけるサイバーセキュリティ対策について」

下地 邦寿 氏（文部科学省大臣官房政策課サイバーセキュリティ・情報化推進室サイバーセキュリティ係長）

令和元年５月に文部科学省より通知された「大学等におけるサイバーセキュリティ対策の強化について（通知）」に関して、その背景とそれを踏まえ大学等で策定する中期的（2019年10月から2022年３月まで）対策の目標及び実施方針（サイバーセキュリティ対策等基本計画）の基本的考え方および対策の方向性が紹介された。大学等のサイバーセキュリティ対策の強化については、平成28年に国立・公立・私立の大学に通知され、約２年半が経過したが、大学等でセキュリティ対策の進展が見られるものの、インシデントが多く発生していることや、大学・研究機関を標的とした先端技術情報等を狙った標的型攻撃事例が発生していること、加えて、2020年オリンピック・パラリンピックに関連した攻撃が今後予想されることから、改めて「サイバーセキュリティ対策等基本計画」を大学等へ示し、インシデント対応体制の整備やセキュリティ教育訓練・啓発活動の実施などセキュリティ対策強化が求められた。

（3）「サイバー攻撃によるリスクと大学等で発生したインシデントの振り返り」

洞田 慎一 氏（JPCERTコーディネーションセンター早期警戒グループマネージャー）

大学で発生する情報セキュリティインシデントとその対応にについて紹介された。大学は、構成員が国際的なつながりを持ち、教育研究等の諸活動を通して多様な情報を組織や個人が保有していることから、個人も標的型攻撃のターゲットとなり、その被害は極めて広範囲に及ぶ可能性がある。

インシデント対応体制の実効性をより高めるためには、攻撃・被害の認知（受け取り窓口）、初動対応（調査する術、意思決定）、原因調査（被害の全容調査に向けた関係者間の認識）、事後対応（効果的な対策を提案する上での事前の認識）の一連の流れの中で、誰が、いつ、どのように対応するのかといったアクションとルートの交通整理を事前に準備しておくことに、経営層の関与は不可欠であることの重要性が強調された。

（4）「ベンチマークリスト結果に見るセキュリティ課題」

宮川 裕之 氏（青山学院大学社会情報学部長、情報セキュリティ研究講習会委員長）

経営執行部による防御態勢への関与は、依然として１割未満であり、情報センター等部門に依存している。重要な情報資産の目録作成は６割が実施していないが、他方アクセス制御は６割が実施しており、重要な情報資産の把握をしない中で行われている。USBメモリやノートPCの持ち出し・持ち込みについて、対策の進展は見られるが、まだ４割が制限を行っていない。特に今後の課題として考えなければならないことは、重要な情報資産の防御を如何に行うか、また、構成員全員への危機意識の徹底を如何に行うかを優先することが課題として指摘された。

（5）「大学構成員全員を対象とした予防と事後対応手順の紹介」

武藏 泰雄 氏（熊本大学総合情報統括センター情報セキュリティ室長、教授）

トップダウンでのセキュリティ対策を実現するために、役割・権限を持った情報セキュリティ担

当責任者が階層的に全学に置かれ、各責任者のもとで教育・啓発活動が実施されている。具体的には、多くの大学と同様にｅラーニング研修を行っている。教材は、業者が作成したｅラーニング教材と自己点検項目、アンケート項目でポータルサイトを全学Moodle学習支援システムと連携させている。未受講の教員は学長にリストを渡して受講を呼びかけ、ログイン時に未受講の旨を連絡している。研修後は、各部局の正答者の分布状況を作成し、正答率の低い学科・部局の理解度を把握して次回の行動計画などに反映させている。

遵守確認方法の取組みとして、外部に監査を依頼し、準拠性、技術面、フォローアップの監査を実施し、報告書を作成した。報告書をもとに、情報資産の棚卸（格付け）を行うようにした。

（6）グループワーク「構成員一人ひとりの防御行動を促進する対応策」

構成員一人ひとりの防御行動を促進する具体的な対応策について、ペアワークでアイディア出しを行い、その成果からグループで具体的な有効案を作成し、２日目のセキュリティ政策・運営コースで継続検討した。

セキュリティインシデント分析コース

サイバー攻撃を受けた場合の対処方法を身に付け、自組織におけるシステムの脆弱性検査などを通じて、事前の備えが行えることを目指した。

（1）サイバー攻撃および防御演習

サイバー攻撃の手法や痕跡の調査を理解するため、産業技術大学院大学で開発されたCyExecを活用し、受講生は仮想環境上で攻撃側、防御側それぞれの立場から操作を行った。最初に攻撃側では、Webサーバから不正に機密情報を搾取する演習を行い、システムの脆弱性やサイバー攻撃の手法について理解を深めた。次に防御側では、Webサーバのログからサイバー攻撃を検知し、さらに攻撃内容を分析、被害を特定するまでの演習を行い、サイバー攻撃の検知や調査手法について理解を深めた。

（2）インシデント対応演習

防御側で明らかになった攻撃の手法、被害の状況をまとめ、インシデント報告書を作成する演習を行った。インシデント報告書はCISOに提出することを想定して、参加者がペアを組み、報告者とCISO役で報告書の内容を吟味し、インシデント報告書としての完成度を高めた。

（3）サイバー攻撃への対策

公開されている脆弱性の情報や検査ツールを活用することで、サイバー攻撃を受ける前に対策を行うことを目指した。最初にシステムの脆弱性につけこんだインシデント事例、脆弱性関連情報の入手方法、検査ツールを紹介した後、無償で利用できる検査ツール「OpenVAS」を用いて演習を行った。次に、明治大学で実施した脆弱性検査を取り上げ、検査にかかる人的な負担や技術的な課題、検査の効果について理解を深めた。

セキュリティ政策・運営コース

情報の重要度に応じた段階的な対応ができるよう、構成員一人ひとりの危機管理意識の醸成、自律的な防御活動に向けた組織的対応策について、①先進的な取組みを行っている大学の事例を参考に、自大学で整備できる方策、実現のための課題、推進体制の整備、②経営層を含めた組織的な体制整備推進の企画と課題を検討した。

（1）グループワーク「構成員一人ひとりの防御行動を促進する対応策」

１日目のグループワークの成果を参考にして、グループ内で企画書をまとめ、グループ間で発表し、例えば「PC起動時に画面への注意喚起」、「不定期テストでフィッシングメールを開封した場合にポップアップ画面で反省を促す」など成果を共有した。

（2）「守るべき情報資産の把握及びそれに基づいたバランスのとれたセキュリティ対策」

最初に情報提供として、守るべき情報資産の把握及びそれに対応した防御対策について、トレンドマイクロ株式会社の岩本真人氏から説明があり、続いて、高橋運営委員（早稲田大学情報企画部事務副部長）から大学での情報資産把握の取組み紹介があった。その上で、情報資産台帳をグループで作成する演習を通じて、現状の課題、社会的・技術的動向、対応策とスケジュールを討議・発表し、共有した。また、文部科学省の対策等基本計画に向けた企画をまとめ成果を共有した。

参加者からのアンケート結果について

① 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３割、概ね理解できた７割」
② セキュリティ政策・運営コースは「理解できた６割、概ね理解できた４割」
③ 参加者からの感想として、「大学はセキュリティへの対応ができていないことを改めて認識した」、「私立大学が置かれた状況、リスク、国の政策、他大学での具体的な方策等、非常に勉強になった」、「攻撃側の手法を体験したことでセキュリティの脆弱性を減らす設計・運用の理解が深まった」、「実施できていない内部監査、情報資産の洗い出し、文部科学省通知の対応など参考になった」、「しっかりとした年間計画があれば上層部にも理解を得られるかもしれないと感じた」などが寄せられた。