５－４　情報セキュリティの危機管理能力のセミナー

＜事業計画＞

サイバー攻撃から教育研究資産、金融資産を防御するために、経営執行担当役員、情報担当部門の責任者、関係教職員を対象に「大学情報セキュリティ研究講習会」を実施する。サイバー攻撃に対する脅威の周知と危機意識を高めるため、ベンチマークテストを踏まえた防御対策の点検と改善策の探求、実践的な情報セキュリティ技術の修得を通じて、参加大学間で研究・討議する。なお、「情報セキュリティ対策問題研究小委員会」では、情報セキュリティ対策に取り組む大学情報のアーカイブ化、関連規程作成のビデオ・オンデマンド化を図る。

＜事業の実施結果＞

「情報セキュリティ研究講習会運営委員会」と「情報セキュリティ対策問題研究小委員会」を継続設置し、情報セキュリティの危機管理能力のセミナーとして「大学情報セキュリティ研究講習会」を実施した。以下に、委員会及び研究講習会の活動を報告する。

情報セキュリティ研究講習会運営委員会

４月２７日、６月５日、７月２４日に平均９名が出席して３回開催し、開催要項の策定、実施準備、大学情報セキュリティベンチマークリストの自己点検・評価を実施した。

（１）開催要項の策定

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すことにした。

プログラムは「全体会」、コース別の「研究講習」、コース合同による「総合演習」の３部で構成した。

① 「全体会」では、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することにした。

② 「セキュリティインシデント分析コース」では、マルウェアを用いたサイバー攻撃の実態や仕組みを確認し、特に身代金要求型攻撃（ランサムウェア）感染時の調査・対応方法について演習することにした。

③ 「セキュリティ政策・運営コース」では、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、予防・対処・報告・公表を適切に遂行するための取り組みを考察することにした。

④ ２コース合同による「総合演習」では、マルウェアを用いたサイバー攻撃を想定した実践的な演習ストーリーにもとづき、被害遭遇時の対処方法及び今後の課題整理を模擬演習により獲得し、情報セキュリティ対策の問題点を洗い出し、大学での取り組みを考察することにした。その上で、以下のように開催要項を策定した。

平成２９年度大学情報セキュリティ研究講習会開催要項

１．開催日程：平成２９年８月２４日(木)・２５日(金)
２．会　　場：学習院大学（東京都豊島区）
３．対 象 者：大学・短期大学の教職員、賛助会員企業の社員でセキュリティに関係・関心のある責任者及び担当者
４．開催趣旨

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ます。

５．研究講習の進め方

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、身代金要求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」を設けています。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」を設けています。

６．研究講習の内容

（１）全体会「サイバー攻撃の動向とセキュリティ施策の成果」

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します。

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（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
　浜 正樹 氏（情報セキュリティ研究講習会運営委員会委員長）
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）

（２）セキュリティインシデント分析コース

マルウェアを用いたサイバー攻撃の実態や仕組みを確認し、特に身代金要求型攻撃（ランサムウェア）感染時の調査・対応方法について演習で学びます。

【プログラム内容】

①　マルウェア感染被害の状況把握
　マルウェアの振る舞いについて理解を深め、さらに感染が発覚した際に行うPCの痕跡調査や他システムへの影響など、被害の状況を把握する手法について確認します。
②　マルウェア感染時の対応手順
　被害の状況を調査した結果、不正通信や情報流出の恐れがある場合の緊急対応について確認します。さらに被害拡大を防ぐための事前の取り組みについて、技術的な理解の促進を図ります。

【到達目標】

① サイバー攻撃の疑いがある場合の調査方法を習得します。
② サイバー攻撃を受けた場合の対処方法・手順を習得します。

（3）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します。

【プログラム内容】

① 情報セキュリティを促進するための政策

「予防」、「対処」、「報告・公表」を組織的に展開する必要性を共有するため、「大学情報セキュリティベンチマークリスト」をもとに参加大学の規模に応じた実態を確認し、それぞれの特徴や課題を整理する中で、情報セキュリティの改善に向けた対策を探求します。

② 情報セキュリティを学内に周知徹底するための対策

大半の大学がWebサイトによる情報セキュリティ対策の周知を行っていることを踏まえ、教職員一人ひとりに情報セキュリティの意識を日常化していく工夫を考える必要がある。そこで、情報セキュリティに関心が向けられるよう、組織として構成員一人ひとりにサイトの活用状況を点検・確認する方法や分かりやすい情報提供の内容、例えば改正個人情報保護法・不正アクセス禁止法・著作権法への適用、偽装メールの注意喚起、被害事例などについて具体的な周知徹底の取り組みを考察します。

【到達目標】

① 規模に応じた情報セキュリティの改善に向けた対策が理解できるようになります。
② 情報セキュリティ対策を周知徹底する視点及び取り組み方法を提供できるようになります。

（4）総合演習

マルウェアを用いたサイバー攻撃を想定した実践的な演習ストーリーにもとづき、被害遭遇時の対処方法及び今後の課題整理を模擬演習により獲得します。その上で、サイバー攻撃全般に対する情報セキュリティ対策の問題点を洗い出し、大学での取り組みを考察します。

【プログラム内容】

① 技術部門と政策部門の混成チームによるサイバー攻撃への対応演習
※ 被害遭遇時の対処方法などをワークシートで確認
※ 技術的、組織的な課題の整理
② 規模別グループによる情報セキュリティ対策への課題解決演習
※ 情報セキュリティ対策の具体的な問題点の洗い出し
※ 課題解決策の策定と発表

【到達目標】

① サイバー攻撃への対処方法を理解できます。
② 大学での情報セキュリティ対策への課題解決策を獲得できます。

（2）実施結果

５１大学から６０名の参加があった。以下に、全体会、コース、総合演習の実施結果の概要を報告する。

① 初日の全体会では、最近のサイバー攻撃の動向、セキュリティポシリー作成と緊急時における対応計画の必要性とネットワークを緊急遮断できる強力な権限をもつ組織の例が報告された。また、加盟校を対象にした情報セキュリティベンチマークの結果

について、今後重視すべき対策や改善に向けた課題について報告が行われた。なお、ベンチマークリストの評価結果の詳細は、巻末の事業報告の附属明細書【２－13】を参照されたい。

② 「セキュリティインシデントコース」では、技術部門のセンター職員を対象に、身代金要求型攻撃の仕組みなどを確認し、感染した時の調査・対応方法の演習を行った。

③ 「セキュリティ政策・運営コース」では、政策部門の職員を対象に、サイバー攻撃の脅威を理解して、予防・対処の仕方、学内外への報告・公表に応じた手順などを確認した上で、グループ討議を通じて対応策の企画案作成を演習した。

④ ２日目の技術部門と政策部門による混成チームの総合演習では、身代金要求型攻撃に感染したという前提でワークシート上の模擬演習を行い、初動対応の仕方、調査の対応の仕方、個人情報保護委員会への報告の仕方など、対応すべき内容をとりまとめ、レビューを経て、経営管理者の視点から洗い出しを行った。

⑤ 以上、研究講習会の成果についてアンケートした結果、技術部門コースでは、「理解できた５割、おむね理解できた５割」。政策・運営部門コースでは、「理解できた３割、おおむね理解できた６割、１割が理解できなかった」。総合演習では、「理解できた１割、おおむね理解できた７割、あまり理解できなかった２割」であった。今後、運営方法について見直すことにしている。

なお、参加者からは、「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が取れないのでシミュレーションしておく重要性を感じた」、「第三者調査を想定した対応や予算化を行いたい」など、研究講習会で得られた成果の感想が寄せられた。開催結果の詳細は、巻末の平成２９年度事業報告の附属明細書【２－12】を参照されたい。

情報セキュリティ対策問題研究小委員会

７月１１日、３月１９日に平均７名が出席して２回開催し、「私立大学における情報セキュリティ対策強化のための取り組み手順」について検討を行い、その結果を「大学情報セキュリティ研究講習会」、「教育改革FD/ICT理事長・学長等会議」、「事務部門管理者会議」に提案・紹介した。

（１）研究内容の概要

平成２８年１２月に文部科学省の私学部長から、「私立大学等を設置する学校法人等における情報セキュリティ対策の強化について(通知)」が発出されたことを受けて、本協会の情報セキュリティ対策問題研究小委員会において、「私立大学における情報セキュリティ対策強化のための取り組み手順」を作成することにした。

内容としては、本協会で実施している情報セキュリティベンチマークリストで課題の洗い出しを行い、各大学の優先順位に沿って、例えば、経営執行部による危機意識の共有化、情報セキュリティポリシーや規程の策定と周知徹底、緊急対応する組織体制と手順など、改善計画の策定を呼びかけている。その上で、改善計画が確実に進められるように、教授会、事務部門で対策活動の進捗状況を報告・聞き出す機会を年単位で設ける。構成員各自には、学内ポータル画面で対策状況の確認を強制的に数カ月の間隔で行う等の提案を行った。

また、情報セキュリティ対策に取り組む大学を支援するため、これまで実施してきた大学情報セキュリティ研究講習会の資料（平成２５年度～２９年度）を本協会Web（http://www.juce.jp/secslide/）に掲載した。なお、規程作成の資料については、平成３０年度

に国立情報学研究所のガイドラインや大学の事例を参考に、情報セキュリティポリシーの要素及び関連規程作成を解説したビデオ・オンデマンド化を完成させ、公開することにしている。以下に、「私立大学における情報セキュリティ対策強化のための取り組み手順」を掲載する。

私立大学における情報セキュリティ対策強化のための取り組み手順

【情報セキュリティ対策強化取り組み手順検討の必要性】

平成２８年１２月２６日付けの「私立大学等を設置する学校法人等における情報セキュリティ対策の強化について（通知）」が、私学部長から発出されたことに基づき、私立大学法人においてもセキュリティポリシーの策定やその運用状況の確認など情報システム上のセキュリティ対策の問題点を点検し、改善に向けた取り組みが大学法人全体に要請されていることに鑑み、本協会としても早急に対応していくための手順をとりまとめることにした。以下に、対応手順の要素を例示する。

１．情報セキュリティの自己点検・評価

本協会が作成した「情報セキュリティベンチマークリスト」で課題の洗い出しを行い、情報セキュリティリスクを評価する。

２．情報セキュリティリスクに基づく改善計画の策定

以下に例示する情報セキュリティ対策を計画的に進めるため、各大学で優先順位に沿って予算措置を行い、組織体制、責任範囲の明確化、権限の設定などの見直しを踏まえて、改善計画を策定する必要がある。

【情報セキュリティ施策の例 】

- 経営執行部による危機意識の共有化
- 情報セキュリティポリシーや情報セキュリティ管理に関する規程（実施規程、実施手順）などの策定・充実と周知徹底（教育・訓練を含む）
- 重要な情報資産の把握とリスク回避のための対策
- サイバー攻撃に対する防御対策（組織的・人的対策、技術的・物理的対策）
- セキュリティ事件・事故に緊急対応する組織体制と対応手順
- 情報セキュリティ被害情報の文部科学省への業務連絡及び内閣府外局の個人情報保護委員会への報告体制

３．改善計画の遂行と実施状況の確認

改善計画を策定しても計画倒れになることが予想されることから、計画が確実に進むことを確認する仕組みを設ける必要がある。

その際、組織レベルによる実施状況の確認としては、例えば、事務部門であれば情報センター等部門が中心となって情報セキュリティに関する対策活動の進捗状況を聞き出す場を年に数回設けるなどの方法が考えられる。教員組織であれば学部の教授会または全学教授会で対策活動の進捗状況を報告する機会を年に数回設けることが考えられる。

構成員レベルであれば、対策状況の確認を学内ポータル画面で強制的に数ヶ月に１回程度の割合で確認を行い、注意喚起を定着させる工夫が考えられる。