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＞

構成員全員がサイバー攻撃の脅威を再確認し、各自の防御行動、組織的な防御対策が進展するよう、大学での対策事例、ベンチマークリストを用いた自己点検・評価・改善、DXに向けたセキュリティの考え方などを通じて、大学の対応力に沿った情報セキュリティ対策の考察力・実践力の獲得を目指す。なお､情報セキュリティ対策問題研究小委員会では、政府や関連機関と連携して情報セキュリティの関連情報を整理し、大学が抱える問題に活用できるよう、プラットフォームを構築して情報発信を行う。

＜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、情報セキュリティ対策問題研究小委員会

2022年(令和4年)10月4日の情報セキュリティ研究講習会運営委員会に8名が出席し、開催要項の策定、実施準備を行った。また、2023年(令和5年)3月1日の合同会議に10名が出席し、研究講習会の振り返りと次年度講習会開催の方向性を検討した。

（１）開催要項の策定

構成員全員がサイバー攻撃の脅威を再確認し、各自の防御行動、組織的な対策が進展するよう、大学で有効と思われる対策事例、ベンチマークリストの結果、サイバー攻撃実情の調査結果などを踏まえて意見交換を行い、大学の対応力に沿った情報セキュリティ対策の考察を目指して、以下のように開催要項を策定した。

2022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：令和4年11月24日(木)
２．会　　場：Zoom会議室
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
　情報セキュリティの不備を狙う攻撃が日常化し、攻撃の手口が巧妙になっており、外部機関からの指摘を通じて被害を受けたことに気づくことが多くなっています。
　そこで本協会では、構成員全員がサイバー攻撃の脅威を再確認し、各自の防御行動、組織的な対策が進展するよう、大学で有効と思われる対策事例、ベンチマークリストの結果、サイバー攻撃実情の調査結果などを踏まえて意見交換を行い、大学の対応力に沿った情報セキュリティ対策の考察を目指します。
５．研究講習会のプログラム
（1）開会挨拶
　　中嶋 卓雄 氏（東海大学学長補佐、情報セキュリティ研究講習会担当理事）
（2）情報セキュリティ関連の最新動向
　　岩本 真人 氏（トレンドマイクロ(株)プロジェクト推進本部）
（3）変化する修学環境とセキュリティ及びベンチマーク結果報告
　　中嶋 卓雄 氏（東海大学学長補佐、情報セキュリティ研究講習会担当理事）
（4）加盟校へのサイバー攻撃実情アンケート結果と考察
　　浜 正樹 氏（文京学院大学情報教育研究センター長、情報セキュリティ研究講習会運営委員）
（5）グループ意見交換１
　※　事前課題のケーススタディに基づいてセキュリティインシデントへの対応

(関連部門への連絡を含む)を整理し、自大学のセキュリティ体制・対策を振り返り、課題を共有します。
(6) 追手門学院 CSIRT の設置と取組み
安井 智美 氏（追手門学院大学図書・情報メディア部情報メディア課長）
(7) ランサムウェア感染当時の実際と、Emotet などの対応
村山 宏幸 氏（神奈川大学情報システム推進部長）
(8) グループ意見交換２
※ ランサムウェアによる病院の被害事例から、今後の自大学での対応を整理し、相互に意見交換を行い、情報セキュリティ対策の改善策をグループで検討します。

（２）実施結果

36 大学から 48 名の参加があった。以下に、実施結果を報告する。

１．情報提供

(1) 情報セキュリティ関連の最新動向

トレンドマイクロ社の「2022 年上半期サイバーセキュリティレポート」という公開資料を基に、最新の情報セキュリティの脆弱性、それを狙った脅威、事故事例などについての解説があった。

初めに、組織への攻撃手法において、これまでのメール開封やリンクのクリックなどの内部者の操作を必要としない直接侵入の手口が増加しているとの指摘があり、続いて、近年、産業界において大きな課題となっているサプライチェーン攻撃について、その類型の解説と、実際に起きた典型的な事故事例の紹介があった。

次に、別のユーザアンケート調査の結果を基に、ランサムウェア攻撃に合った場合の身代金支払いの有無や、データの復号(暗号化されたデータを平文に戻す)の可否及びその復号手段等の実態と、日本と海外の傾向の違いが報告された。

さらに、2021 年から 2022 年における Emotet の活動推移の報告と、ベンダーやユーザ対策に対抗するために、攻撃者が常に攻撃手法を変化させているという実態の紹介があった。また、個人利用者を狙った様々なフィッシング攻撃で使われた、PC やスマートフォンの実際の画面例を基に、これらのネット詐欺攻撃が常態化し、手口は多様化しているとの指摘があった。

最後にまとめとして、IT 技術や業務プロセス、内外の環境などが変化することでそこに新たな脆弱性が生まれ、それを悪用する攻撃手法も進化しているので、常にそれらの最新の情報を入手・共有し、対応を続ける必要性が示唆された。

(2) 変化する修学環境とセキュリティ及びベンチマーク結果報告

「大学情報セキュリティベンチマークリストの結果報告」として、以下の特徴が得られた。①情報セキュリティに対する取組みは、執行部や情報システム部門で進んでいる。②アクセス制御を伴う情報資産管理は進んでない。③外部委託に対する契約内容の厳密化は進んでいる。④今後の UTM(Unified Threat Management：総合脅威管理)など、統合したセキュリティ技術の強化が好まれる傾向にある。詳細は、巻末の 2022 年度事業報告書の附属明細書【2－8】を参照されたい。

「変化する修学環境とセキュリティ」として、次のような東海大学の試みが紹介された。①オフィスをフリースペース空間とすることで文書の電子化を実現し、セキュリティ管理が容易になった。②電話網をクラウド化することにより、FAX の廃止や柔軟な電話コミュニケーションを実現した。③情報資産の格付は、法律、制度などの外部・自組織のルールに沿って情報の機密性について分類し、可用性の観点からアクセス権限の付与を検討している。

(3) 加盟校へのサイバー攻撃実情アンケート結果と考察

加盟校に 10 月末締切で実施したサイバー攻撃実情アンケートの結果(回答率 55%)報告を行った。①2021 年 4 月～2022 年 8 月にサイバー攻撃を受けた大学は、約 80%で、30%の大学で情報漏洩や業務停止などの被害を受けており、大規模大学の方がその傾向が強いことが分かった。②70%以上で無差別不審メールを受信しており、更に 50%以上の大学で特定の教員などへの不審メールを受信している。③25%の大学でランサムウェア以外のマルウェアに感染し、約 8%の大学でランサムウェアに感染した。

④Web 関係では、30%以上の大学で Web サイトへの不正アクセス、25%の大学で DDoS 攻撃(過剰なアクセスやデータを送付するサイバー攻撃)を受けている。どちらも大規模大学の被害が目立つ。これらの結果に関連して Emotet とランサムウェアについて最近の報道事例について触れ、注意喚起及び基本的対策の概説を行った。

(4) 追手門学院 CSIRT の設置と取組み

追手門大学が行うサイバーセキュリティ対策として、その中核を担う CSIRT*の設置とその取組みの紹介が行われた。＊(Computer Security Incident Response Team)

高度化しているサイバー攻撃や不正アクセス等に対する脅威が高まる中で、情報セキュリティインシデントへ迅速に対応することを教育機関の使命としていることと、CSIRT のメンバーとなる職員の部署異動が定期的に行われるため、インシデントが発生しても対応レベルのクオリティを下げないことを課題としていた。

CSIRT 設立の主な目的は、①インシデント対応、②インシデント予防のための教育訓練実施組織の明確化、③インシデントに関する情報収集の 3 点としており、インシデント発生時には CISO(Chief Information Security Officer)の責任下で対応することが細則で定められており、より迅速な対応体制を整備した。

具体的な取組みとしては、情報収集、教育・啓蒙活動、対応マニュアルの作成等、多岐に亘るが、その中で 2022 年度の主な取組みとしては、①事務職員向け標的型攻撃メール訓練、②全教員向け情報セキュリティ研修の実施、③情報セキュリティに関する相談窓口の設置を行った。また、日本シーサート協議会へ加盟しており、情報収集、人材育成等の観点からメリットを感じている。

(5) ランサムウェア感染当時の実際と Emotet などの対応

1 台のサーバがランサムウェアに感染し、機能停止した。当該サーバは Microsoft365 に ID 連携をするための中間サーバで、停止をしても利用上の被害は軽微であるため、システムを切り離した上で、関係各所への連絡と復旧作業を行った。このサーバは、ID・氏名・初期パスワードの情報を保持していたため、ID 生成後に初期パスワードから変更のない ID のパスワードを初期化した。その後にサーバは凍結状態とし、代替システムを別途構築した。感染経路については構築・保守をしていた業者の PC が乗っ取られたことが発端であり、業者選定と指示徹底が重要であることが浮き彫りにされた。別件で、学内の複数名が Emotet に感染する被害があった。啓発活動だけで感染を止めることは限界があるため、一次被害の発生を前提として取組むこととなった。二次被害拡大の防止策を検討した結果、ファイアウォールに C&C サーバとの通信を遮断する機能を実装することで、感染後の情報漏洩を防ぐ対策をとることができた。

(6) グループ意見交換 1 と 2

事前課題のケーススタディに基づき、セキュリティインシデントへの対応を整理し、自大学のセキュリティ体制・対策を振り返り、課題を共有するため、1 グループ 4 名(一部 5 名)でグループとしての検討を行った。その上で、各自が自組織で具体的に実行できるプランを立案するグループディスカッションを 1 時間弱で 2 回実施した。

1 回目は、Emotet に教員が感染した場合をケーススタディとして、自大学のセキュリティ対策・対応力及び改善点について、「緊急」、「重要」、「今後の課題」として優先順位付けを行った。

2 回目は、ランサムウェア被害を受けた徳島の 2 つの病院の事例を参考に、自組織でランサムウェア被害が夏季休暇、年度末の時期に発生したことを想定し、あらかじめ決めておかなければならないこと、およびそれを学内で実現するための障壁とその回避方法を検討した。

2 回に亘る事前課題のケーススタディを通じて、実践的な検討が活発に展開された。セキュリティ関連規程の策定・改定、体制整備などの新たな対策について多岐に亘り他大学との情報を共有し、今後の指針を各自が獲得できたと推測される。

(7) 参加者からのアンケート結果について

参加者 48 名の内、15 名のアンケートを紹介する。①13 名が「他大学との情報・意見交換、ケーススタディからの学びがあった」と評価している。②その上で「大学の事例紹介が参考になった/増やして欲しい」6 件、「他大学との意見交換・議論の時間がもっと欲しかった」4 件あった。これらのことから、大学からの情報提供、グループ意見交換による他大学の状況を学べることは私情協で実施する講習会ならではの特徴であり、受講者から評価されていた。さらに加えて、受講者自身が研修成果について明確に明文化できている、又は具体的なアクションプランが述べられている記述が 11 名あった。短い時間ではあったが受講者にとって有意義な講習会であったことが窺える。

（8）グループ討議での意見の一部を紹介

＊　ランサムウェア被害への備えには、被害時期により業務継続に向けた復旧作業の優先順位が異なるため、あらかじめ順位を決めておく必要がある。
＊　セキュリティインシデントが起こった時に行う行動指針を全教職員に周知させ、定期的な情報教育を行う。
＊　身に覚えのないメール受け取った際の相談窓口を決め、学生・教職員へ周知する。
＊　適切なバックアップ方法の検討と実施が必要。
＊　脆弱性の注意喚起のみに留まっているが、実際の事例共有等を通じて危機意識を高める。
＊　対応できる人材がいないと、有事の際に動けないのでどのように改善するか考える必要がある。
＊　CSIRT の設立に向けた働きかけを行う。

（３）来年度に希望するテーマについて

委員から以下のような意見があり、次年度に研究講習会の企画で検討することにした。

①　技術的な知識の修得に向けて、現場での構築システムなど紹介してはどうか。
②　BCP(事業継続計画)、可用性の確保について、時期的な対応を含む課題の抽出や優先順位付けを行ってはどうか。
③　サイバーセキュリティ監査の実施など、文部科学省のサイバーセキュリティ対策にかかる実施すべき事項の項目に対応してはどうか。
④　経営層にセキュリティの認識を向上させる対策が提示できないか。
⑤　大学関連で年間 30 件以上の情報セキュリティ事故があり、事例として紹介できないか。
⑥　ベンチマークリストは、意思決定現場での有効性から見直しを検討してはどうか。