事業活動報告

2022 年度 大学情報セキュリティ研究講習会　開催報告

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て、研究講習会を令和 4 年 11 月 24 日(木) オンラインで開催し、48 名（36 大学）の参加があった。

（1）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）

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、データの復号の可否、及び、その復号手段等について、それらの実態と、日本と海外とでの傾向の違いが報告された。

さらに、2021 年から 2022 年までの Emotet の活動の推移の報告と共に、その間、攻撃者がベンダーやユーザの対策に対抗するために、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、対応を続けることが必要であるとの示唆があった。

（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

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）

「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は進んでいる。②アクセス制御を伴う情報資産管理については進んでない。③外部委託に対する契約内容の厳密化については進んでいる。④今後の UTM（Unified Threat Management）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。

「変化する修学環境とセキュリティ」として、東海大学の試みについて紹介した。①オフィスをフリースペース空間とすることにより、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情報の格付について、機密性の観点から情報資産について、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

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）

10 月末締切で加盟校に協力頂いたサイバー攻撃実情アンケート結果(回答率 55%)の報告を行った。2021 年 4 月～2022 年 8 月でサイバー攻撃を受けた大学は約 80%である。また、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。70%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。また、25%の大学でランサムウェア以外のマルウェア感染被害、約 8%の大学でランサムウェア感染被害があった。Web 関係では、30%以上の大学で Web サイトへの不正アクセス、実に 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、注意喚起およ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

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）

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（Computer Security Incident Response Team）の設置とその取組みについて、紹介された。

昨今、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が、教育機関の使命として挙げられることが背景にある。また、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、いつインシデントが発生したとしても対応レベルのクオリティを下げないことも課題であった。

CSIRT 設立の主な目的としては、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）の責任下で対応にあたれ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、多岐に渡るが、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をしており、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

村山 宏幸 氏（神奈川大学情報システム推進部長）

１台のサーバがランサムウェアに感染し、機能停止を起こした。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が行われた。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する対応をした。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、一次被害は発生する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。

（7）グループ意見交換

4 名(一部 5 名)が 1 グループとなり、所属組織のセキュリティに関する規程や資料などを見直し、グループとしての検討結果に加えて、自組織の課題を明確にすること、ならびに各自が自組織で具体的に実行できる計画を立案できるようになることを目指してグループディスカッションを 1 時間程度で 2 回実施した。

講習会に先立ち、事前課題として Emotet に教員が感染した場合の自組織で起こりそうな不適切な

対応を含むストーリーに基づいて、情報セキュリティインシデント発生時の文科省報告様式に記載し、自組織で不足していること、およびストーリーの対応で改善すべきことをメモとして各自がまとめ、講習会に参加した。

1回目は、事前課題の内容をグループ内で共有し、改善点について、「緊急」、「重要」、「今後の課題」の視点で優先順位付けをし、加えて自組織で準備・整備しなければならないことと、その実現のための方策を検討した。各グループからは、情報セキュリティインシデントに備えるために、教育、報告、対応の視点から以下のようなことが挙げられた。

- インシデントの種類や情報資産の重要度に基づいたインシデント発生時の対応手順を明文化しておく
- 学生・教職員に対して、感染時の対処法や不審メールの見分け方などのセキュリティに対する啓発をする
- 情報セキュリティインシデント対応組織を整備し、セキュリティに関するスペシャリストの育成や外部協力も検討する

2回目は、ランサムウェア Lockbit2.0 によりデータが暗号化され復旧まで2カ月を要した徳島県の病院と3日で診療再開した同県の病院の2つの事例を参考に、自組織でランサムウェア被害が夏季休暇や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。各グループからは、繁忙期と閑散期では、復旧までの優先順位などの対応が異なることが確認され、万一の情報セキュリティインシデントに備えて、以下のようなことが挙げられた。

- 復旧対応の計画と代替手段を準備しておく
- バックアップはシステムの重要性や影響範囲に応じて適切に設定する
- 復旧対応は、優先順位・最終決定者などのルールや手順書の整備、関係各所との連携を明確にしておく

最後に総括として、高倉弘喜氏(国立情報学研究所)から、情報セキュリティインシデントへの対応は、大規模自然災害対応にシフトして、フォレンジックスや証拠保全の優先度を下げることも今後検討しなければならない。何か正解か、わからない状況になっている、との解説が加えられた。

本研修会では、具体的な事例に則って実践的な検討が活発に行われていた。そして、これらの活動をとおして、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わたり他大学との情報を共有した。今後の指針を各自が獲得できていたと推測される。

（8）参加者からのアンケート結果について

オンライン開催であったため、講習会終了後に自由記述にて、研修内容、ならびに研修成果・アクションプラン、および今後の要望についての2つの設問でアンケートをオンラインで実施した。2つの設問の回答が明確に分かれていなかったので、15名から収集したすべての記述を一つにまとめて、SCAT手法で集計した。その結果を表1に示す。

表1 アンケート結果

分類項目	件数
他大学との情報・意見交換/他大学の事例からの学び	13
大学の事例紹介が参考になった/増やして欲しい	6
他大学との意見交換・議論の時間がもっと欲しかった	4
今年度の研修実施方法への肯定的評価	4
今後の講習会への題材・開催方法への希望/研修設計への要望	18
受講者自身の明確な学びの成果/研修成果を実務に活かしたい/学内共有したい	11
構成員に自分事として捉えて貰う/セキュリティ教育・学内研修の実施	4
その他	2

講習内容(情報提供とグループ意見交換)からの学びがあったと13名が評価している。さらに、「大学の事例紹介が参考になった/増やして欲しい」が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」が4件あった。これらのことから、大学についての情報提供、および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る。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/具体的なアクションプランが述べられている記述が 11 名からあった。よって、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うかがえる。