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

2023年(令和5年)10月6日の情報セキュリティ研究講習会運営委員会に11名が出席し、開催要項の策定、実施準備を行った。

（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、攻撃被害時の対応、大学事業継続の強化に向けた対応などの事例研究・意見交換を通じて、各大学の状況にあわせたサイバーセキュリティ対策の向上計画の立案を目指して、以下のように開催要項を策定した。

2023年(令和5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5年12月5日(火)13時～17時
２．会　　場：オンラインによるテレビ会議室（Zoom使用）
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、ランサムウェアなどにより大学の学事が滞る可能性も高くなっています。
　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、攻撃被害時の対応、大学事業継続の強化に向けた対応などの事例研究・意見交換を通じて、各大学の状況にあわせたサイバーセキュリティ対策の向上計画の立案を目指します。
５．研究講習会のプログラム
（1）開会挨拶
　井口 信和 氏（近畿大学総合情報基盤センター長、情報セキュリティ研究講習会担当理事）
（2）最新のサイバーセキュリティ動向とインシデントレスポンス
　西城 泰裕 氏（情報処理推進機構セキュリティセンター情報分析官）
（3）ランサムウェア感染時のBCP
　酒井 正幸 氏（日本ネットワークセキュリティ協会中小企業支援施策WGサブリーダー、IT&キャリアコンパス代表）
（4）グループ意見交換１
　※　事前課題である文部科学省へのインシデント報告をグループで共有確認・考察し、自大学のセキュリティ体制・対策を振り返り、課題を整理します。
（5）グループ意見交換２
　※　ランサムウェア感染を想定したインシデントレスポンスとBCP対策について、つるぎ町立半田病院インシデント報告書を事例とし、対応と再発防止策について対策・課題をグループで整理します。

（6）インシデントレスポンス時のセキュリティベンダー活用と課題
　　石山 隆弘 氏（明治大学情報メディア部生田メディア支援事務室）
（7）グループ意見交換 3・4
　※　グループ討議の内容を再確認し、事業継続の強化に向けた対策・計画をグループで整理します。
（8）個人ワーク
　※　自大学におけるアクションプランの作成

（2）実施結果

17 大学から 21 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）最新のサイバーセキュリティ動向とインシデントレスポンス

最新のサーバーセキュリティ動向では、ネットワーク貫通型の攻撃が急増しており、脆弱性を悪用されると二要素認証もバイパスされる恐れがあることが説明された。本来はセキュリティを高めるために用いられる VPN などの脆弱性を突いてネットワークに侵入し、攻撃が展開される。その際、悪用された脆弱性リスト、アプローチ方法、今後悪用されそうな脆弱性なども紹介された。

インシデントレスポンスでは、サイバーレスキュー隊（J-CRAT：Cyber Resucue and Advice Team against targeted attack of Japan）の概要と目的が提示され、組織の活動イメージおよび平時、事案未確認段階、事案対処時などあらゆる場面を想定したレスキュー対応と支援が紹介された。また、インシデント発生原因の特定、検知の方法、適切な調査と判断が、標的型サイバー攻撃に対して非常に重要であることが強調された。インシデント対応時のポイントとして、「自組織で行うこと」、「専門機関に任せること」、「どの専門機関に任せるのか」など、確認事項を平時に予め決めておくことが示唆された。

（2）ランサムウェア感染時の BCP

警察の資料を基にランサムウェア被害の状況が報告された。最近のランサムウェアの手口は、復旧を引き換えに金銭を要求するだけでなく、情報を窃取して多重脅迫を行うように変わってきている。VPN から侵入されるケースが多く、脆弱性パッチの未適用や初期パスワードを変えていないといった運用上の問題が原因として挙げられた。復旧にかかる費用は、100 万円以上が 7 割強を占めており、企業の社会的信頼を損ねた結果、操業停止に発展するケースもあると報告された。

感染時の事業継続計画は、インシデント発生確率の低減とインシデント発生時のダメージを少なくして事業復旧を行うためのサイバーセキュリティフレームワークの解説があった。インシデント発生直後は、情報共有の手段がとても重要となり、事前のマニュアル等整備と、対応の記録も重要である。CSIRT の設置組織も増えており、統括を自組織で行う必要はあるが、必要に応じて外注も考慮すべきとしている。また、自前システムは復旧に時間がかかるため、クラウドの利用も推奨された。

（3）インシデントレスポンス時のセキュリティベンダー活用と課題

インシデント対応時に準備しておくべきことやフォレンジック調査で配慮すべき点など、IT ベンダーの対応で実務に基づく知見の共有がされた。

インシデント発生時には、OS とネットワークのログが重要であり、その管理をするベンダーの関与が大きくなる。仕様や契約でのベンダーに、どこまで運用支援を依頼するのか、管理が重要である。フォレンジック調査の実施判断は、調査結果に期待できること、期待できないことを理解し、目的を定める必要がある。

また、フォレンジック調査の発注は、レポートの内容や、調査メンバーの指定等に十分配慮しなくてはならない。発注後も調査に必要なヒアリング等の発生を見据えて準備を進めておく必要がある。調査が終わり、インシデント対応の終息となった際にも、業務委託仕様や契約内容を見直すことが推奨される。平時からベンダーとの積極的な関わりで、より良いサービス提供につなげていくことが望ましい。

2．グループ意見交換

インシデント発生時には、文科省へ報告しなければならないなど、インシデント対応の手順が近年変わってきており、情報セキュリティ確保の視点も、機密性から可用性に移行してきている。このような背景から、シナリオと各種システム保守内容の場

合分けを参考にインシデント対応のために備えておくべき事柄について検討した。
学習目標は、①インシデント発生時の速やかな対応準備として、あらかじめ決定しておかなければならないことなど、自組織で今後改善しなければならない事項を説明できる。②BCP 対策として、災害が発生した際の自大学のシステム運用を維持するための計画に加えて、情報セキュリティインシデントに対する対応を立案するために必要な事項を説明できるとして、3・4 名が 1 グループとなり、グループディスカッション 1 時間程度を 2 回実施した。また、具体的な事例として、徳島県つるぎ町立半田病院コンピュータウイルス感染事案有識者会議調査報告書を活用した。
講習会に先立ち、事前課題として、つるぎ町立半田病院の報告書に基づいて、セキュリティインシデント発生時の文科省報告書を作成し、参加者は講習会に参加した。
1 回目は、事前課題を共有した後、インシデント発生に備えて、日常からベンダー管理において実施しておくべきこと、フォレンジック調査が発生することも見据えた視点を盛り込み整理した。
2 回目は、明治大学の情報提供を受けて、フォレンジックを実施する場合のシナリオに沿って、ベンダーに何を期待し、どう活用していくのか、障害となる箇所はどこにあるかを整理した。

3．グループ討議での意見の一部を紹介
＊　避難訓練のようなインシデント発生を想定した訓練の実施が必要となる。
＊　専門業者へコンサル的な依頼・検証を行う必要がある。
＊　BCP 対策について、検討する体制、必要なシステムベンダ、対策範囲、重要性順位を明確にしたシステム対応が必要となる。
＊　どのシステムで何を保全するか重みづけ、システム代替案、危機管理体制、BCP 設置予算の確保などが必要となる。
＊　バックアップ・データ復旧設備の拡充、BCP 予算の策定、学内保有データの洗い出し、情報システム部門での対応可能範囲、学内関係部署での対応作業範囲などを検討しておく必要がある。
＊　バックアップ取得とリストアの確認、緊急時連絡手段・順番、ネットワークに頼らないものや別回線の準備、どこまで授業を止めることができるのか、各部署と共有するなどの課題がある。

4．参加者アンケートの一部を紹介
＊　重大インシデント発生時の対応方法などは実際に起きなければ実践する機会がないので、今回の事前課題もよい経験となった。
＊　実際に起きたインシデントの報告書を読むことで、何を準備しておくべきかを自分事として理解できたこと、一人では考え付かなかったこともグループで意見交換することにより新たな気付きがあった。
＊　インシデント発生時は初動対応が重要であり、関連部署との連携・マニュアル整備の連携を再確認する機会となった。
＊　ランサムウェア対策を考える上で、直接的な被害だけでなく、社会的責任等における間接的な被害に関しても想定した上で，本学の BCP 策定に寄与したい。
＊　異なる機関との交流機会が少ないため、今回のように意見を出し合いながら所属の話を聞けるスタイルが大変勉強になった。

なお、開催結果の詳細は、巻末の 2023 年度事業報告書の附属明細書【2－8】を参照されたい。