事業活動報告 NO. 3

2023年度 大学情報セキュリティ研究講習会 開催報告

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て、研究講習会を令和５年12月５日（火）オンラインで開催し、21名（17大学）の参加があった。

（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

情報処理推進機構セキュリティセンター 情報分析官

西城　泰裕　氏

最新のサーバーセキュリティ動向では、直近の動向としてネットワーク貫通型と呼ばれるAPT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り、警戒が必要なことが説明された。本来はセキュリティを高めるために用いられているVPNやFortiOSの脆弱性をついてネットワークに侵入され、攻撃が展開される。講演では悪用された脆弱性のリストやアプローチ方法、また、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の原因の特定や検知の方法、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」などを確認しておくなど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

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

酒井　正幸　氏

はじめに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。ランサムウェアは身代金要求型不正プログラムであるが、最近の手口としては、単に復旧を引き換えに金銭を要求するだけではなく、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といった解説があった。VPN装置から侵入されるケースが多く、装置のパッチ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ている。復旧にかかる費用についても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。

感染時における事業継続計画として、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では情報共有の手段がとても重要となり、そのためにマニュアル等の整備を事前に行い、どのような対応をとったかの記録も重要であると説明された。インシデント発生時にスムーズに対応するためCSIRTを設置している組織も増えており、全体の統括は自組織で行う必要があるが、その他の対応としては必要に応じて外注することも考慮すべきとしている。また、自前でシステムを構築していると復旧に時間がかかるため、できるだけクラウドを利用することも推奨された。

（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

明治大学情報メディア部生田メディア支援事務室

石山　隆弘　氏

インシデント対応時のITベンダーとの関係について、準備しておくべきことや、とりわけフォレンジック調査をする際に配慮すべき点について、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、ここを管理するベンダーの関与が大きくなる。仕様や契約を通して、これらのベンダーにどこまで運用支援を依頼するのか管理することが重要である。フォレンジック調査の実施判断をする際には、調査結果に期待できることとできないことを理解した上で、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の際には、レポートに含める内容や、調査メンバーの指定等に十分配慮しなくてはならない。なお、発注後も調査に必要なヒアリング等が発生するため、それらを見据えて準備を進めておく必要がある。無事に調査が終わりインシデント対応の終息となったところで、業務委託仕様や契約内容を見直すことが推奨される。平時からベンダーに積極的に関わり、よりよりサービス提供につなげていくことが望ましい。

（4）グループ意見交換

近年、インシデント発生時に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いる。また、情報セキュリティ確保のための視点は、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、シナリオと各種のシステムの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に速やかに対応できるための準備として、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、（2）BCP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名あるいは４名が１グループとなり、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。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、事前課題について共有した後、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について、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回目のグループ意見交換のための情報提供として、明治大学の石山氏からフォレンジックベンダー全般に関する所感、発注後のフェーズで起きがちな事例などの紹介があった。これを受けて、２回目は、フォレンジックを実施することとなった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。

（5）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、12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
研修成果が明文化されている 具体的なアクションプラン	11
今年度の研修内容への肯定的評価	10
今後の講習会への題材・開催方法への希望	5
グループワークの設問が多かった	3
グループワークの模範解答を示して欲しい	3
次回も参加したい	3
他大学のと情報・意見交換 他大学の事例からの学び	3
研修設計への要望	3
日程・時間・開催方法への肯定的評価	3
講習会運営への要望	2

４名の方が、サイバー攻撃によるリスクを事業継続計画（BCP）の策定に含める必要性、および今後のアクションプランとして述べられていた。短い時間で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。