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＞

学校法人及び大学の教育研究資産、金融資産、マイナンバー等の情報資産へのサイバー攻撃を防御するため、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。

防御意識に基づく行動が組織的に展開されるよう執行部による推進計画の提案作り、ベンチマークの結果を踏まえた改善計画の策定、IoT 機器(ルータ、コピー機、プリンタ、カメラなど)に不正アクセスを防ぐ機能を設ける義務化対策、重要情報資産の暗号化対策、AI によるサイバー攻撃防御の可能性と課題、サイバー攻撃被害を想定した検知･調査･分析・事後対応などの演習を行う。なお、情報セキュリティ対策問題研究小委員会では、情報セキュリティの関連情報を体系化し、プラットフォームに格納するため、プラットフォームの構成と管理運営についてとりまとめ、可能な範囲で公開する。

＜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

２０１９年(令和元年)6月２８日、２０２０年(令和２年)3月９日（情報セキュリティ対策問題小員会との合同会議）に平均１１名が出席して２回開催し、開催要項の策定、実施準備、開催結果の振り返りを 実施した。

（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必要なことから、防御行動が組織的に進展するように、CISO（最高情報セキュリティ責任者）を含む経営執行部による対応、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リストを用いた自己点検・評価・改善を通じて、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」とコース別の「研究講習」の２部で構成した。

① 全体会では、大学におけるサイバー攻撃の最新動向、情報セキュリティインシデントと対応事例、ベンチマークによる大学の対応、セキュリティポリシーなど、学内ルールの周知徹底、構成員一人ひとりの防御行動の促進を共有し、対策を考察した。

② インシデント分析コースでは、サイバー攻撃の手法・検知・痕跡調査、ログ解析とインシデント報告書の作成、技術的対策の立案、疑似侵入テストによるシステム脆弱性の点検と対策など技術的な対策を取り扱うことにした。

③ 政策・運営コースでは、構成員一人ひとりの防御行動を促進する対応策、守るべき情報資産の把握とセキュリティ対策、防御対策の注意喚起などグループ討議を通じて理解を深めることにした。

２０１９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：令和元年８月２９日(木)・３０日(金)
２．会　　場：立正大学品川キャンパス（東京都品川区）
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、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。文部科学省においても「大学等におけるサイバーセキュリティ対策等の強化について（通知）」が行われ、一歩踏み込んだ対策としてサイバーセキュリティ対策など組織・体制の整備、情報セキュリティポリシー及び実施手順書の策定が求められています。

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必要なことから、防御行動が組織的に進展するように、CISO（最高情報セキュリティ責任者）を含む経営執行部による対応、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リストを用いた自己点検・評価・改善を通じて、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

１日目の「全体会」では、大学におけるサイバー攻撃の最新動向、大学における情報セキュリティインシデントとその対応事例、ベンチマークリストにもとづく大学の対応、セキュリティポリシーなど学内ルールの周知徹底、構成員一人ひとりの防御行動の促進を共有し、対策を考察します。

２日目は、２つのコースに分かれます。一つは、セキュリティ関係の知識・技能の獲得を目指して演習を交えながら習得する「セキュリティインシデント分析コース」、二つは、リスクに応じた最適な情報セキュリティ対策と構成員全員及び情報センター等部門で注意喚起を呼びかける防御対策について認識を共有し、大学の実状に対応策を考察する「セキュリティ政策・運営コース」で、参加者の希望に応じた研究講習を行います。

6．研究講習の内容

（1）全体会

① 情報セキュリティ１０大脅威 2019
　渡邉 祥樹 氏（独立行政法人情報処理推進機構セキュリティセンター）

② 大学等におけるサイバーセキュリティ対策について
　下地 邦寿 氏（文部科学省大臣官房政策課サイバーセキュリティ・情報化推進室サイバーセキュリティ係長）

③ サイバー攻撃によるリスクと大学等で発生したインシデントの振り返り」
　洞田 慎一 氏（JPCERT コーディネーションセンター早期警戒グループマネージャー）

④ ベンチマークリスト結果に見るセキュリティ課題
　宮川 裕之 氏（青山学院大学社会情報学部長、情報セキュリティ研究講習会委員長）

⑤ 学内ルールの周知徹底の取組み対策
　武藏 泰雄 氏（熊本大学総合情報統括センター情報セキュリティ室長、教授）

⑥ 構成員一人ひとりの防御行動を促進する対応策
　※ セキュリティポリシー及び情報関連規程を整備しても、構成員一人ひとりが自分の問題として捉え・防御行動に結び付けることが難しいことから、システム化することで意識付けを促進する全学的な取組みを考察

（2）セキュリティインシデント分析コース

情報センター等部門の技術者が習得しておくべきセキュリティ関係の知識・技能として、サイバー攻撃の実態や仕組みを、サイバーレンジ（サイバー攻撃および防御の訓練を行うための仮想的な環境）での演習を通じて体感します。さらに攻撃予兆および痕跡の解析等、インシデント発生時の対応方法について演習を行います。

【プログラム内容】

① サイバー攻撃および防御についての基本的知識と演習
　※ サイバー攻撃の手法
　※ サイバー攻撃の検知
　※ 痕跡調査

② インシデント対応演習
　※ ログ解析とインシデント報告書の作成
　※ 技術的対策の立案

③ サイバー攻撃への対策
　※ 疑似侵入テストによるシステム脆弱性の点検と対策

【到達目標】

① サイバー攻撃で用いられる手法や防御の体験を通して、対処方法を身に付けることができます。
② サイバー攻撃への事前の備えができるようになります。
③ 自組織のシステム的脆弱性の発見方法を提案できるようになります。

（3）セキュリティ政策・運営コース

情報セキュリティシステムの防御を効果的に進める方法として、情報の重要度に応じた階層的な対応をすることが必要です。そのために、教職員・学生・関係企業などに危機管理意識を醸成して自律的な防御行動の実質化を図るために、学内の関連規程や対応体制の整備及び教育・訓練や点検・監査の実施、情報関連システムを活用した対策について、具体的な企画・立案の演習をとおして理解を深めます。

【プログラム内容】

① 構成員一人ひとりの防御行動を促進する対応策
※ アイディアを精査して、グループ内で絞り込み、具体的に実施するための企画
② 守るべき情報資産の把握及びそれに基づいたバランスのとれたセキュリティ対策
※ 重要な情報資産の把握を実施している事例を参考に、法人として情報リスクの分析・評価について現状を検証して、その課題を挙げ、それに基づいて情報資産の重要度に応じた組織としての最大の効果を得られるバランスのとれた情報セキュリティ対策を立案
③ セキュリティ対策としての攻撃に対する防御対策の注意喚起
※ 攻撃に対する防御対策の注意喚起を実施している事例を参考に、具体的な注意喚起の方法とその効果についての提案

【到達目標】

① 構成員一人ひとりの防護行動を促す対応策について提案できるようになります。
② リスク分析と情報資産台帳の必要性について説明できるようになり、守るべき情報資産に対するセキュリティ対策の重要性・優先順位を提案できるようになります。
③ 攻撃に対する防御対策の注意喚起の方策と効果について提案できるようになります。

（2）実施結果

３５大学から４２名の参加があった。以下に、実施結果の概要を報告する。

① １日目は、サイバー攻撃の最新動向や事例、文科省の方針・対応、ベンチマークリストにもとづく大学の対応、情報セキュリティ教育・学内ルール周知徹底の取組みを確認し、構成員一人ひとりの防御行動をシステム(画面での注意喚起)で促進させる対策を参加者全員で考察した。ベンチマークリスト評価結果の詳細は、巻末の２０１９年度事業報告の附属明細書【２－１２】を参照されたい。

② ２日目は、「セキュリティインシデント分析コース」と「セキュリティ政策・運営コース」に分かれて、仮想空間でサイバー攻撃の仕組みを体験し、攻撃予兆、痕跡解析、脆弱性点検などの演習、重要な情報資産の把握、情報リスクの分析・評価について考察し、防御対策の注意喚起を含めた情報セキュリティ対策の演習を行い、その上で、参加者全員が学内での提言に向けたアクションプランを整理した。

③ 参加者のアクションプランでは、次のような多くの行動計画が立案された。
・「文科省セキュリティ強化対策の現状把握・行動計画作成」
・「情報資産の洗い出しを計画」 ・「脆弱性診断の起案・実施」 ・「多要素認証の検証」
・「インシデント対応組織の構築を経営層に提案」
・「セキュリティ監査体制の計画や外部監査の実施」
・「情報セキュリティポリシー・規程の見直しや策定」
・「セキュリティ啓発コンテンツ作成により教職員・学生へ意識の浸透を図る」
・「セキュリティ講習会・訓練・e-Learning の見直しや実施、委託・構築費の予算化」
・「執行部の意識向上に他大学を視察」など

④　参加者からのアンケート結果では、セキュリティインシデント分析コースの理解度は「理解できた 3 割、概ね理解できた 7 割」、セキュリティ政策・運営コースは「理解できた 6 割、概ね理解できた 4 割」となっていた。

また、参加者からの感想として、「大学はセキュリティへの対応ができていなことを改めて認識した」、「私立大学が置かれた状況、リスク、国の政策、他大学での具体的な方策等、非常に勉強になった」、「攻撃側の手法を体験したことでセキュリティの脆弱性を減らす設計・運用の理解が深まった」、「実施できていない内部監査、情報資産の洗い出し、文科省通達の対応など参考になった」、「しっかりとした年間計画があれば上層部にも理解を得られるかもしれないと感じた」などが寄せられた。なお、開催結果の詳細は、巻末の 2019 年度事業報告の附属明細書【２－１１】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

２０２０年(令和２年)３月９日に情報セキュリティ研究講習会運営委員会との合同会議に４名が出席し、情報セキュリティの関連情報を体系化し、プラットフォームに格納するため、プラットフォームの構成についてとりまとめ、本協会 Web に掲載した。

＜プラットフォーム構築の検討＞

情報セキュリティ関連情報のプラットフォームについて、以下のような方針を確認し、構築した。

①　プラットフォームの構成は、過去の講習会資料を中心に掲載し、セキュリティ関係の関係機関や賛助会員主催の研修情報を整理・体系化する。

②　過去の講習会資料については、各コースの実施内容から項目立てを行い、階層型のページ構成で整理・掲載することにした。

③　セキュリティ関係の関係機関については、インシデントの届出先情報を中心に掲載することにしたが、相談できる窓口や Q&A などの情報があれば掲載することにした。

④　また、資料の掲載順は、予防・初動・届出など対応の手順別に分けて整理を検討しどうかとの意見もあり、今後の整備課題とした。

情報セキュリティ関連情報のプラットフォーム（http://www.juce.jp/secslide/）

１．大学情報セキュリティ研究講習会資料
１－１　サイバー攻撃の動向と対策事例
（１）サイバー攻撃の動向
（２）サイバー攻撃への対策事例
（３）自己点検評価、ベンチマークリスト結果
１－２　技術関連資料
（１）攻撃手法の理解
（２）痕跡調査・解析、インシデント対応関連
（３）情報セキュリティ対策
１－３　政策立案・運営関連資料
（１）危機管理の共有
（２）セキュリティポリシー、情報資産管理
（３）組織の構築、組織的な取組み
（４）関連法令
（５）災害を想定した対策
（６）演習、ワークシート
２．情報セキュリティ関連情報のリンク
２－１　情報セキュリティ関連情報（届出先、注意喚起など）
２－２　情報セキュリティ関連研修情報