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＞

私立大学における情報セキュリティの危機管理能力の強化を支援するため、私立大学の情報担当部門責任者、関係教職員を対象に「大学情報セキュリティ研究講習会」を継続実施する。大学関係教職員に情報資産や金融資産に対するサイバー攻撃の脅威を周知し、防御意識に基づく行動が組織的に展開されるよう大学及び大学連携による対策の働きかけを研究・協議する。また、災害時での業務継続性の確保を点検するベンチマークリストの作成や大学間による模擬的な訓練のあり方等についても研究する。研究を行う組織として「情報セキュリティ研究講習会運営委員会」の中に専門家による組織として「情報セキュリティ対策問題研究小委員会」を設け対応する。

＜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」を継続設置するとともに、新たに情報セキュリティ対策の研究を行う組織として「情報セキュリティ対策問題研究小委員会」を設置し、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

６月２６日、７月１５日、平成２８年３月１８日に平均８名が出席して３回開催し、開催要項の策定、実施準備を行った。

（１）開催要項の策定

サイバー攻撃に対する脅威について、法人の役員、学内の執行部、教員、職員、学生など構成員一人ひとりが防御意識に基づき行動できるよう、セキュリティ対策組織の構築と運用体制、課題を探求することを目指した。プログラムは、全体会、コース別の研究講習、コース合同による総合演習とした。

全体会では、サイバー攻撃の手口と脅威を紹介し、情報資産及び金融資産までを含めたリスクマネジメントの重要性について認識を共有化することにした。

テクニカルコースでは、サイバー攻撃について第一通報現場での初期対応及びインシデント発覚後の対応を演習することで技術的な理解の促進を目指すことにした。

マネジメントコースでは、役員や教職員一人ひとりがサイバー攻撃への被害を最小限に抑えるための対策意識を持てるように組織的な働きかけの工夫を探求することにした。

２コース合同による総合演習では、実践的な演習ストーリーによる模擬演習を行うとともに、セキュリティ対策組織の在り方及び取り組みを点検評価するベンチマークテストの可能性について認識を深めることにした。その上で、以下のように開催要項を策定した。

平成２７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：平成２７年８月２５日(火)・２６日(水)
２．会　　場：工学院大学（東京都新宿区）
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、非常に巧妙になっており、官公庁のみならず大学現場でも情報資産の漏洩、不正アクセスが発見されるなど衝撃を与え、大きな社会問題となっています。また、インターネット・バンキングにおいても法人部門が攻撃されており、インターネット全体に対するリスクマネジメントの対策強化が求められています。

このような状況は各大学においても想定されることから、大学執行部をはじめ組織的にサイバー攻撃の脅威について認識を深めることが急がれます。

そこで、サイバー攻撃に対する脅威について、法人の役員、学内の執行部、教員、職員、学生など構成員一人ひとりが防御意識に基づき行動できるようセキュリティ対策組織の構築と運用体制、課題を探求する研究講習会としています。

5．研究講習の進め方

サイバー攻撃に対する脅威について認識を共有化するため、危機意識徹底の重要性を働きかける場として「全体会」を行った上で、インシデント対応に関する知識の習得及び実習を行う「テクニカルコース」とセキュリティ対策の実施及びセキュリティ意識の醸成を学内に推進・普及していく方策を検討する「マネジメントコース」を設けています。　その上で、テクニカルコースとマネジメントコース双方の受講者が協働して、実践的な演習ストーリーによる模擬演習と防御意識に基づき行動ができるよう、「総合演習」を設けてセキュリティ対策組織の在り方及び取り組みについて点検評価の内容を考察します。

6．研究講習の内容

（1）全体会「サイバー攻撃の脅威と危機意識の徹底対策」

サイバー攻撃の手口と脅威を紹介し、情報資産及び金融資産までを含めたリスクマネジメントの重要性について認識を共有化します。

① サイバー攻撃の最新手口と防御対策
　松坂　志　氏（情報処理推進機構セキュリティセンター主幹）

② インターネット・バンキングへの攻撃手口と考えられる対応策
　大坂　元一氏（全国銀行協会企画部次長）

③ 大学における情報セキュリティ対策の取り組みと経営執行部の役割
　三浦　文博氏（愛知大学情報システム課長）

（2）テクニカルコース

標的型サイバー攻撃などについて、第一通報現場での初期対応及びインシデント発覚後の対応を演習で学びます。

【プログラム内容】

① 標的型サイバー攻撃などが疑われる場合の診断演習

疑わしい「メールの添付ファイル」の開封や「リンク先」の接続を想定し、サンドボックス技術などを用いて診断して、安全確認する方法を演習します。

② インシデント発生時の対応フローチャートに基づく演習

標的型サイバー攻撃の疑いが強い場合を想定して、インシデント対応フローチャートに基づく緊急遮断の判断、システムのログ解析、被害の全容把握、関係者への報告書作成などを演習します。

【到達目標】

① サイバー攻撃の疑いがある場合の調査・対処方法を習得します。

② サイバー攻撃を受けた場合の対処方法・手順を習得します。

（3）マネジメントコース

学内で役員・教職員一人ひとりが標的型サイバー攻撃への被害を最小限に抑えるための対策意識を持てるよう、大学執行部としての組織的な働きかけの工夫について考察します。

【プログラム内容】

① 大学内でのインシデント対応組織の構築・取り組みについて考える
サイバー攻撃への備えとして、緊急対応組織の必要性と役割・機能について検討します。
※ 情報提供 「インシデント対応チーム(CSIRT)の構築と情報共有について」
（ＪＰＣＥＲＴ コーディネーションセンター）
② ガバナンスの役割とセキュリティ自己点検基準について考える
セキュリティ対策の取組みとして、経営執行部の役割を整理し、その上で学内の各組織で自己点検評価すべき枠組みや対応の在り方について検討します。
【到達目標】
① 学内でのインシデント対応組織の構築・取り組みについて理解できるようになります。
② セキュリティ対策を学内へ周知徹底するために必要な視点を提供できるようになります。
（４）総合演習
「テクニカルコース」と「マネジメントコース」双方の受講者が協働して実践的な演習ストーリーによる模擬演習を行うとともに、セキュリティ対策組織の在り方及び取り組みについて点検評価するため、セキュリティ対策全般に関わるベンチマークリストの可能性を考察します。
【プログラム内容】
① システム管理者側とマネジメント部門双方によるインシデント対応の演習
標的型サイバー攻撃を受けた場合を想定して、緊急措置の範囲、ガバナンス・執行部への通報と全構成員への連絡、社会への説明などについて検討します。
② セキュリティ対策の運営組織、取り組み内容などの点検評価リストの検討
防御意識を高め、持続させるための体制・取り組みについて、自己点検・評価の重要性を理解し、改善に向けた課題の解決を考察します。
【到達目標】
① サイバー攻撃に対し、テクニカル部門とマネジメント部門の協働体制を理解できます。
② 全学でセキュリティ対策意識を醸成し、社会的責任を果すための体制・取り組みへの方向性を持つことができるようになります。

（２）実施結果

８月２５日、２６日の２日に亘り開催し、６０大学１賛助会員から７８名の参加があった。

参加者のアンケートでは、「実際のマルウェアを仮想環境技術で観察し理解が深まった」、「模擬演習や被害時の対応マニュアルの作成を検討したい」、「情報セキュリティ管理体制、緊急対応組織を構築する必要性を感じた」、「上層部への提案につなげたい」などの感想が寄せられ、防御意識の共有化やセキュリティ対策組織の必要性が認識され、セキュリティ対策の強化に向けて推進する姿勢が見られた。

研究講習会で目指した到達目標について、以下のような成果が見られた。

※ 危機意識徹底の重要性を働きかけるための対策として、メールによる不審な添付ファイルやＵＲＬリンクを開かない注意喚起を促すことが理解された。
※ 現場での初期対応及びインシデント発覚後の対応について、対処の方法・手順が確認された。
※ 一人ひとりがサイバー攻撃への対策意識を持てるよう、セキュリティ対策組織の在り方及び取り組みを点検評価する「ベンチマークテスト」の重要性について、理解の

共有化が図れた。
※　緊急対応、経営執行部への通報、社会への説明に臨機に対応できるよう、技術担当者と管理担当者それぞれの立場での役割について相互理解が深められた。

なお、プログラムごとのアンケート内容については、平成２７年度事業報告の附属明細書【２－１３】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

６月２５日、７月１３日に平均６名が出席して２回開催し、「経営執行部（役員）の情報セキュリティに対する取組み」と「大学セキュリティ運用ベンチマークテストのリスト化」について研究を行い、その結果を研究講習会に提案した。

（１）研究内容の概要

①　経営執行部（役員）の情報セキュリティに対する取組み

学内全ての情報資産及び金融資産を攻撃から守るリスクマネジメントの最重要課題として意思決定機関が関与することの重要性を明確化するため、経営執行部が関与すべき情報セキュリティへの取り組みを「１．サイバー攻撃による情報資産・金融資産の脅威やインシデントに対する危機意識の共有化を推進」、「２．学内ルールの構築と周知徹底」、「３．情報セキュリティ委員会、情報センター等部門による防御体制の構築と点検評価の徹底」、「４．教職員に対する教育や模擬訓練の実施とその徹底」の観点から、以下のように整理した。

経営執行部（役員）の情報セキュリティに対する取組みについて

サイバー攻撃などによる情報セキュリティの問題は、一大学の問題に留まることなく社会・経済全体にも波及する可能性があることから、大学・法人の全構成員が意識を共有し、組織的に取組むことができるよう経営執行に携わる役員のリーダーシップが極めて重要となっています。

そこで、情報セキュリティに対する取組みについて、大学法人全体としての問題意識の共有化、学内ルールの確立、教職員に対する教育・訓練、運営体制などのマネジメントを遂行するための役割・責任の範囲・内容に関して経営執行部として以下の視点で振り返る必要があります。

１．サイバー攻撃による情報資産・金融資産の脅威やインシデントに対する危機意識の共有化を推進

※　危機意識の共有化を推進していくには、法人組織（理事会）でサイバー攻撃の防御を全学的な課題として捉え意思決定しておくことが望まれる。

※　全学的に展開していくためには、担当役員もしくはそれに準ずる法人・大学執行部の関係者を配置し、法人及び大学の構成員全員にサイバー攻撃による脅威の認識を徹底する必要がある。

※　脅威を周知徹底していくには、構成員一人ひとりがサイバー攻撃や情報セキュリティの確保に向けて意識の持続化を図るとともに、振り返りをさせる仕組みが必要となる。

※　構成員一人ひとりによる自己点検・評価の結果を踏まえて、全学的な取り組みに

ついて見直し・改善する仕組みが必要となる。

2．学内ルール（情報セキュリティポリシー、情報資産の把握など）の構築と周知徹底

※　法人・大学の危機管理の一部として情報セキュリティポリシーに関する取り扱いの判断基準を構築するとともに、構成員全員にサイバー攻撃から法人・大学の情報資産・金融資産を守るために最小限度の行動基準に関するガイドラインを作成し、理解の徹底を図る必要がある。

※　そのためには、法人・大学の構成員一人ひとりが利用または作成する情報資産の所在を明確にし、被害の重大性を想定して情報資産別に防御の仕方を共有しておく必要がある。また、請負業者についても情報セキュリティに対する問題意識を職務責任として契約などで明確にしておく必要がある。

※　なお、攻撃を受けたときの緊急対応としては、被害の拡大を防ぐために別途ネットワークの切断などの初動対応について予め定めておく必要がある。

3．情報セキュリティ委員会、情報センター等部門による防御体制の構築と点検評価の徹底

※　防御体制の組織としては、担当役員もしくはそれに準ずる法人・大学執行部による統括責任者の配置、防御に関する全学的な取り組み対策のとりまとめや点検・評価のガイドラインなどを検討する情報セキュリティ委員会の設置、防御の実施と点検・評価の徹底を働きかける情報センター等部門の充実が求められる。

※　防御体制を実質的に機能させていくためには、統括責任者の役割と権限を明確にした上で、情報セキュリティ委員会が危機管理マネジメントの内部統制組織として機能できるよう位置づけを確保する。また、委員会の下でガイドラインに沿って構成員一人ひとりに防御行動を働きかけるとともに緊急対応としてのインシデントに対応する情報センター等部門の役割と権限を強化しておく必要がある。

4．教職員に対する教育や模擬訓練の実施とその徹底

※　大学構成員一人ひとりに防御意識を持たせて対応できるようにするには、担当役員もしくはそれに準ずる法人・大学執行部の関係者による全学的な呼びかけによる危機管理研修が不可欠である。

※　研修は、サイバー攻撃の事例を通じて脅威に関する認識を持たせるとともに、脅威に遭遇したときの緊急対応について関連知識の活用を模擬訓練などにより修得させる。

※　その際、最小限度心がけておくべき対応として、不審メール見極めの模擬訓練を体験させることを通じて、ウイルス拡散、機密情報の外部への漏えい、システムの破壊など想定される被害について知識の共有を図るとともに被害を防止する意識の向上を図る。また、被害の拡散を防ぐための対応として速やかに相談・連絡する手順を修得させる。

② 大学セキュリティ運用ベンチマークテストのリスト化

サイバー攻撃に対する技術的・物理的な防御体制、意思決定機関の関わり方や運用体制、セキュリティポリシーの構築と遵守状況などを振り返るためのシートとしてベンチマークリストを「情報セキュリティ政策会議のセキュリティ対策統一基準」などを取捨選択し、「第１部情報セキュリティ対策へのガバナンス」、「第２部情報セキュリティ対策全般」、「第３部大学の規模等」で構成して作成した。なお、ベンチマーク結果の外部診断の可能性については次年度の研究テーマとしている。ベンチマークテストの詳細は、平成２７年度事業報告の附属明細書【２－１３】を参照されたい。