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に執行部への理解促進に向けた行動計画作り、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、情報セキュリティポリシーの要素及び関連規程作成を解説したビデオ・オンデマンド化を完成し、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

平成３０年４月１９日、５月２２日、６月１２日、平成３１年３月１４日に平均８名が出席して４回開催し、開催要項の策定、実施準備、大学情報セキュリティベンチマークリストの自己点検・評価を実施した。

（１）開催要項の策定

サイバー攻撃に対する防御行動が組織的に展開されるようにするため、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組織的な対応、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・改善の習慣化を通じて､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」、コース別の「研究講習」、コース合同による「全体演習」の３部で構成した。

① 全体会では､「サイバー攻撃の最新動向と対策」について理解した上で､「情報セキュリティインシデント事例から研修・啓発の仕組みを考える」ために事前予防や事後対応に必要な手順の理解、大学構成員全員を対象とした標的型攻撃メールに対する研修・啓発の視点をワークショップしながら考察することにした。

② インシデント分析コースでは、標的型攻撃メールによるサイバー攻撃の出口と仕組み、痕跡調査とインシデントの対応、暗号化を含む情報保護のための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、ベンチマークで先進的取組みをしている大学の事例を参考に情報セキュリティポリシーと対策基準の策定とセキュリティルールの周知徹底、重要な情報資産の把握とリスク対策など自大学の整備計画を考案､CISO(最高情報セキュリティ責任者)の設置と強化対策､情報管理者に求められる法的知識の理解を行うことにした。

④ 全体演習では、２コースが合流し、グループにおいてセキュリティ課題の解決に向けた研修・啓発の実施計画案を考察した上で、経営執行部に向けた自大学の整備計画を作成することにした。

平成３０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３０年８月２３日(木)・２４日(金)
２．会　　場：学習院大学（東京都豊島区）
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、情報資産・金融資産の窃取・漏洩・破壊などが日常化し、大きな社会問題となっています。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。そのためには、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求められます。

そこで本協会では、サイバー攻撃に対する防御行動が組織的に展開されるようにするため、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組織的な対応、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・改善の習慣化を通じて、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日目は、大学におけるサイバー攻撃の最新動向、ベンチマークリストにもとづく大学のセキュリティ対応状況、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を共有する「全体会」を通じて、情報セキュリティリスクの確認を行います。また、情報セキュリティインシデントの事例を踏まえて予防と対応手順について研修・啓発の仕組み及び訓練計画を考えます。

２日目は、最初２つのコースに分かれます。一つは、サイバー攻撃の基本的知識や対策につい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、情報セキュリティの整備計画及びCISOの設置に向けた対策を考える「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。その上で、最後の全体演習では、コースをまとめてセキュリティ課題の解決に向けた計画・提言を行います

６．研究講習の内容

（１）全体会１「サイバー攻撃の最新動向と対策」

サイバー攻撃の最新動向、大学情報セキュリティベンチマークリスト結果を踏まえた課題、実際に体験したインシデントとその後の対応事例を踏まえて、情報セキュリティリスクの実感を共有します。

①「サイバー攻撃の最新動向から見る大学の新たなリスク」
　　洞田 慎一 氏（JPCERT ｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ早期警戒グループマネージャー）
②「ベンチマークリスト結果に見る私立大学のセキュリティ課題」
　　宮川 裕之 氏（青山学院大学社会情報学部教授）
③「大阪大学において発生した不正アクセス事案について」
　　尾上 孝雄 氏（大阪大学最高情報セキュリティ責任者、副学長）
④　情報セキュリティリスクの確認

（２）全体会２「情報セキュリティインシデント事例から研修・啓発の仕組みを考える」

実際に経験した大学の事例をもとに、情報セキュリティインシデント対応の事前予防や事後対応に必要な手順を理解し、大学構成員全員を対象とした研修・啓発の視点について検討します。

＊情報セキュリティインシデント事例を踏まえた事前予防と事後対応手順の紹介
＊グループワーク：大学構成員全員を対象とした予防と対応手順を研修・啓発する仕組み
＊標的型攻撃メール対策の訓練事例を紹介：高橋智広氏（早稲田大学情報企画課長）
＊グループワーク：大学構成員全員を対象とした標的型攻撃メールに対する研修・訓練計画の作成

（3）セキュリティインシデント分析コース
　標的型攻撃メールを用いたサイバー攻撃の実態や仕組みを確認し、その具体的な手口や影響範囲について演習を通じて体感します。また、痕跡調査を行うための事前準備や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。さらに重要な情報資産の保護に向けた技術的な対策を紹介します。
【プログラム内容】
① サイバー攻撃の基本的知識と最新動向の理解
　＊標的型攻撃メールによるサイバー攻撃の手口と仕組み
　＊痕跡調査を行うための事前の備え
② サイバー攻撃によるインシデントへの対応演習と対策
　＊痕跡調査とインシデント対応演習
　＊情報保護のための技術的な対策
【到達目標】
① サイバー攻撃を受けた場合の対処方法・手順を体得できます。
② サイバー攻撃への事前の備えや情報保護について理解できるようになります。
（4）セキュリティ政策・運営コース
　情報セキュリティは、一部の担当組織だけでは対応できるものではなく、経営執行部による組織的な対応と構成員一人ひとりによる注意と行動が必要です。それには、情報セキュリティポリシーに基づいた実効性のあるセキュリティ対策基準や対策手順を作成し、自己点検・評価・改善を習慣化していくことが重要になります。
　本セッションは、自己点検・評価・改善に先進的に取り組んでいるベンチマークを参考に自大学の整備計画を振り返ります。また、組織的に迅速な対応ができるように CISO（最高情報セキュリティ責任者）の設置と強化対策を考察し、情報管理者として理解しておくべき法的知識とその対応について理解を深めます。
【プログラム内容】
① ベンチマークリストで先進的取組みをしている大学を参考に整備計画を考える
　＊情報セキュリティポリシーと対策基準の策定
　＊情報セキュリティルールの周知徹底
　＊情報資産の把握とリスク対策など
② CISO の設置と強化対策
　＊CISO の役割と権限の紹介
　＊グループワーク：CISO の重要性を確認し、設置に向けた対策を考える
③ 情報管理者に求められる法的知識とその対応
　改正個人情報保護法、不正アクセス禁止法、著作権保護法、GDPR（EU 一般データ保護規則）など：市川昌氏（江戸川大学名誉教授）
【到達目標】
① 情報セキュリティ整備計画を立案できるようになります。
② 情報セキュリティの研修計画を提案できるようになります。
③ 組織的に迅速な対応を行う CISO の設置について重要性を説明できるようになります。
（5）全体演習「セキュリティ課題の解決に向けた計画・提言」
　経営陣に理解と行動を促す一つの手段として、情報セキュリティに関する研修・啓発の必要性と実施計画の提案、自大学の課題解決に向けた情報セキュリティの整備計画を考察します。
【プログラム内容】
① 経営陣に向けた提言（研修・啓発の必要性、整備計画）
② 自大学のセキュリティ課題の解決計画を作成
【到達目標】
＊大学での情報セキュリティ対策への課題解決策を獲得できます。

（２）実施結果

５４大学、２賛助会員から６６名の参加があった。以下に、実施結果の概要を報告する。

① 初日の全体会では、サイバー攻撃の最新動向と情報セキュリティ対策のベンチマークによる大学の対応状況を把握し、大学で実際に起きた情報セキュリティ事故から予防策の一環として研修・啓発の重要性とその仕組み・訓練計画を参加者全員で考察した。なお、ベンチマークリスト評価結果の詳細は、巻末の平成３０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、サイバー攻撃の基本的知識や対策についての演習、情報セキュリティの整備計画及び CISO の設置に向けた対策の演習を行い、その上で、参加者全員による「全体演習」では、情報セキュリティ課題の解決に向けて今後の計画・提言作成の演習を行った。

③ 技術部門と政策部門が合同して作成した経営陣向けの提言では、「組織の構築（情報セキュリティ担当委員会、CISO、CISRT 設置含む）」、「情報セキュリティポリシーや規程の策定・見直し」、「経営陣へのサイバー攻撃によるリスクの説明」、「サイバー攻撃に対する教育・啓発」、「情報セキュリティ事故対応手順の確立」、「情報資産台帳の作成・整備」などがアクションプランとしてとりまとめられた。

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 4 割、概ね理解できた 6 割」、セキュリティ政策・運営コースは「理解できた 3 割、概ね理解できた 7 割」、全体演習は「理解できた 3 割、概ね理解できた 6 割、あまり理解できなかった 1 割」となっていた。

また、参加者からの感想として、全体を通じて「学内の人材育成について考える良い機会だった」、「セキュリティ対策はまだまだということに気付いた」、演習を通じて「不正侵入の挙動を確認できたのは大きな経験だった」、「構成員全員に危機意識の共有を図りたい」、「ルール、体制整備など経営層への提案を行いたい」などが寄せられた。開催結果の詳細は、巻末の平成３０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

平成３０年５月８日、６月１９日に平均６名が出席して２回開催し、情報セキュリティポリシーの要素及び関連規程作成を解説したビデオを作成し、研究講習会で活用するとともに本協会 Web に掲載した。

（１）研究内容の概要

情報セキュリティポリシーや関連規程作成の必要性と整備について以下のような検討を行った。

① 大学に対するサイバー攻撃は、研究データ、人脈、学生の家庭環境などの情報を窃取する目的もあるが、攻撃拠点として加害者になり得る可能性も考える必要があるので、大学構成員全員が社会的な責任が大きくなっていることを改めて認識し、情報セキュリティに関して一人ひとりの心掛けや周知徹底が必要となる。

② その上で、自ら担当すべき範囲を明確にして対策を決め、活動に移していく必要性について、情報セキュリティポリシーの関連文書に方針や基準を定め、実行できるようにしていくことが確認された。

③ 大学構成員全員が情報セキュリティの関連規程を理解し、一人ひとりが対応できるようにすることが喫緊の課題であるが、なぜ関連規程を遵守しなければいけないかと

いう感覚が構成員一人ひとりに理解されていないことを重視し、標準的な関連規程を作成し参考に供することよりも、基本となる要素を整理して理解の周知徹底を図ることを優先すべきと判断し､情報セキュリティポリシーのビデオを作成することにした。

④　ビデオの作成に当たっては、国立情報学研究所の「高等教育機関の情報セキュリティ対策のためのサンプル規程集」を参考にして、以下の視点で解説することにした。

高等教育機関におけるセキュリティポリシーとは

１．情報セキュリティ対策の必要性
２．セキュリティポリシーの構成
　（１）ポリシー（運用方針、運用基本規程）
　（２）実施規程（組織体制の定義、運用・管理ルール、情報の格付けなど）
　（３）手順・ガイドライン
３．サンプル規程集を利用して作成するポイント

⑤　情報セキュリティポリシーの構成は、大学の情報セキュリティに対する姿勢や考え方を示すものとして、「ポリシー（情報セキュリティ基本方針)」、「実施規程（対策基準)」、「手順・ガイドライン」を標準的に整備する必要がある。

ポリシーと実施規程は「規程」として位置付けられているため１０年程度は変更されないが、手順・ガイドラインは「内規」として位置付け、社会情勢の変化に合わせて更新していく必要がある。

なお、ビデオは「情報セキュリティ関連の動画コンテンツ」として、本協会の Web に掲載しており参考とされたい。（http://www.juce.jp/sec2018/secpol.html）