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、情報担当部門の管理責任者、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。教育・研究活動情報及び教職員のマイナンバー情報を含む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て防御行動が組織的に展開されるよう、全学的な取り組みについてベンチマークによる課題の洗い出しと対応策を参加大学間で研究・協議する。なお、「情報セキュリティ対策問題研究小委員会」では、大学執行部として関与すべき範囲と権限のモデル、ベンチマークによる点検・評価方法、外部診断の可能性について研究する。

＜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

４月２１日、５月１９日、６月３０日、７月２８日、11月２８日、平成２９年１月２０日に平均８名が出席して６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理解の普及を徹底するため、情報セキュリティ対策をベンチマーク化し、課題の洗い出しを行い、自己点検・評価を習慣化する中で構成員一人ひとりがサイバー攻撃の脅威を認識し、大学として段階的にセキュリティ対策や体制を整備できるように課題の共有を目指した。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、サイバー攻撃に対する防御意識を徹底できるようにするため、情報セキュリティに最小限必要な対策・対応をベンチマークにより振り返ることの重要性及び課題を共有することにした。

セキュリティインシデント分析コースでは、インシデント対応に関する知識の習得及び実習を行うことで技術的な理解の促進を目指すことにした。

セキュリティ政策・運営コースでは、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探求することにした。

上記の２コース合同による総合演習では、防御意識に基づき行動ができるようにインシデント対応を想定した模擬演習を行い、セキュリティ向上のための組織対応の在り方及び取り組み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２８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２８年８月２３日(火)・２４日(水)
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、非常に巧妙になっており、官公庁、企業、学校でも情報資産の窃取・漏洩などが頻発化してきており、大きな社会問題となっています。とりわけ、学校現場では成績情報・個人情報がネットワーク経由で窃取されるなど情報セキュリティ管理の甘さが問題視されています。このような問題は、以前から種々指摘されその対策について学校としての対応が求められてきていますが、組織的にサイバー攻撃の脅威を周知し、防御行動が展開されるよう構成員全員による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理解の普及を徹底するため、情報セキュリティの対策をベンチマークし、課題の洗い出しを行い、自己点検・評価を習慣化する中で構成員一人ひとりがサイバー攻撃の脅威を認識し、大学として段階的にセキュリティ対策や体制を整備できるように課題を共有するための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防御意識を徹底できるようにするため、情報セキュリティに最小限必要な対策・対応をベンチマークにより振り返ることの重要性及び課題を共有する場として「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「セキュリティインシデント分析コース」と、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「セキュリティ政策・運営コース」を設けています。その上で、二つのコース双方の受講者が協働して、防御意識に基づき行動ができるようにインシデント対応を想定した「総合演習」を設けています。

6．研究講習の内容

（1） 全体会「サイバー攻撃の動向と防御行動の点検・評価」

サイバー攻撃の最新動向を理解した上で、「大学情報セキュリティベンチマークリスト」による点検・評価の仕組みや、今後改善に向けて取組むべき対策・対応を紹介し、経営執行部の情報セキュリティに対する取組み、情報資産の把握と管理対策、組織的・人的な対応、技術的・物理的対策の課題を共有化します。

① サイバー攻撃の最新動向について
　満永　拓邦　氏（東京大学情報学環特任准教授）

② 経営執行部の情報セキュリティに対する取組みについて
　宮川　裕之　氏（青山学院大学情報メディアセンター所長）

③ 大学情報セキュリティベンチマークリストの紹介と評価方法
　井端　正臣　氏（公益社団法人私立大学情報教育協会事務局長）

④ ベンチマークリストの評価結果と改善に向けて取組むべき対策・対応
　満永　拓邦　氏（東京大学情報学環特任准教授）

（2） セキュリティインシデント分析コース

標的型サイバー攻撃のマルウェアによる情報窃取の実態などを確認し、不正通信を検知した時の調査・対応方法について演習で学びます。

【プログラム内容】

① 標的型サイバー攻撃による情報窃取
　情報窃取・情報流出のリスクと手口、インシデントレスポンスの基本的な流れについて確認します。

② 標的型サイバー攻撃のインシデントレスポンス演習
　不正通信の痕跡調査、情報流出の拡大を防ぐための緊急対応手段について技術的な理解の促進を図ります。

【到達目標】

① 標的型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 標的型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） セキュリティ政策・運営コース

役員・教職員・学生一人ひとりがサイバー攻撃の脅威を理解し、防御の手立てを

浸透させるための組織的な仕組みづくり及びインシデント発生時・事後の具体的な対応策を考察します。

【プログラム内容】

① 情報セキュリティ対策のための組織的施策

全体会の「ベンチマークリストの評価結果と改善に向けて取組むべき対策・対応」をもとに参加大学の現状を踏まえ、情報セキュリティ対策で何をなすべきか具体的な施策を探求します。 また、サイバー攻撃の脅威に対する組織的な仕組みとして、被害に遭わないための手立て「予防」、インシデント発生時には被害を最小限にする「対処」、事後の対応「報告・公表」を適切に遂行するために必要な組織体制について考察します。

② 情報セキュリティを学内に周知徹底するための対策

情報セキュリティ対策の実施においては、情報や情報システムの取り扱いに関する法律として、例えばサイバー犯罪を取り締まるための法律、プライバシー・個人情報を扱う事業者規制のための法律などがあります。組織的対応として、関連法令を遵守するための規程・ガイドラインの見直し及びその効果的な周知方法について考察します。

【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及び方法を提供できるようになります。

（4） 総合演習

２つのコース受講者が協働して実践的な演習ストーリーによるインシデントレスポンスと事後対策・対応の模擬演習を行うとともに、大学におけるセキュリティ向上のための組織対応の在り方及び取組みについて考察します。

【プログラム内容】

① 個人情報流出インシデント対応演習

外部機関から不正通信の通知を受けた例題をベースに手順を遂行(体験)します。なお、関係者への連絡・報告、社会への公表、規程の見直し、防止策（現状対応環境の確認と問題点）など対応の可否や優先順位について整理します。

② サイバー攻撃防御の組織化に向けた戦略の考察

経営執行部を中心として防御意識を高め持続するための体制・取組み課題、セキュリティ対策システム・規程等の見直し、セキュリティ対策予算の計上、構成員全員に向けた防御対策の取組みを具体的な問題を挙げながら考察します。

【到達目標】

① サイバー攻撃に対する大学部門間での協働体制を理解できます。

② 全学で情報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・取組みの方向性を理解できます。

（２）実施結果

８月２３日、２４日の２日に亘り開催し、５７大学１賛助会員から７５名の参加があった。

① 全体会の成果として、一つは、完全な予防策がない中では、被害の発生に即応できる組織体制の必要性が確認された。二つは、大学・法人、全構成員が脅威の認識を共有できるよう経営執行部のリーダーシップが不可欠で、経営執行部の役割、責任の範囲、内容に関して理解の共有を図った。三つは、情報セキュリティの状況を把握するために本協会で作成した「大学情報ベンチマークリスト」で点検・評価を行い、その結果を踏まえて、今後重視すべき対策、大学の対応力に応じた改善行動について理解

を共有した。

② コースの研究講習及び総合演習の成果として、「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」に別れ、手順や方法の習得、組織体制の在り方・課題などの理解を共有した。その上で、サイバー攻撃を受けていると外部機関から連絡が入ったことを想定して、総合演習で技術部門と管理部門において協働すべき内容が何であるかを確認した。なお、開催結果の詳細は、巻末の平成２８年度事業報告の附属明細書【２－１２】を参照されたい。

（３）大学情報セキュリティベンチマークリストの自己点検・評価の実施

７月に加盟校２１９校を対象に　ベンチマークリストの自己点検・評価を実施した結果、１２５校から回答があり、回答率は５７％であった。大学規模・種別の評価結果は、大規模大学で６３点、中規模大学５５点、中小規模大学５０点、単科大学及び短期大学４７点であり、平均は５２点であった。なお、ベンチマークリストの自己点検・評価結果の詳細は、巻末の平成２８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２２日、７月１１日に平均６名が出席して２回開催し、「大学情報セキュリティベンチマークリスト」、「ベンチマークリストの評価配点表と情報セキュリティベンチマーク評価のガイドライン」について、具体的かつ詳細な検討を行い、その結果を「情報セキュリティ研究講習会」及び「教育改革FD/ICT理事長・学長等会議」に提案した。

（１）研究内容の概要

① 大学情報セキュリティベンチマークリストの見直し

平成２７年度に作成した大学情報セキュリティベンチマークリストについて、経営執行部の関与に関する取組みに重点を置くとともに、大学組織としての対応状況を簡潔に点検・評価できるよう、ベンチマークリスト全般を見直し、「第１部：経営執行部の情報セキュリティに対する取組み」、「第２部：重要な情報資産の把握と管理対策について」、「第３部：組織的・人的な対応について」、「第４部：技術的・物理的対策について」として再構築した。「大学情報セキュリティベンチマークリスト」の詳細は、巻末の平成２８年事業報告の附属明細書【２－１３】を参照されたい。

② ベンチマークリストの評価配点表と情報セキュリティベンチマーク評価のガイドラインの作成

「ベンチマーク評価の視点」としては、アウトカム評価に不可欠な要素を設定し、大学執行部として情報セキュリティに関与することを重視し、その上で情報資産の把握、組織的な対応、技術・物理的対応との関係性をマッチングすることにした。

「ベンチマークによる対応状況の確認」は、経営執行部の取組み状況をもとに、一貫した情報セキュリティ対策の展開状況を振り返ることにより、不足している取組みについて改善に向けて組織的に計画・行動できるようにした。

「情報セキュリティの改善に向けた対策」としては、ベンチマークリストのガイドラインの４つの視点に沿って、特に重視すべき項目として「危機意識の共有化対策」、「構成員に学内ルールの周知徹底と遵守の対策」、「情報セキュリティに関する意思決定や脅威となる事象に対応する組織」、「重要な情報資産の把握対策」、「教職員への危機意識の対策」、「不用意な情報漏えい対策」の改善行動に向けた取組みを例示した。

「自己点検・評価結果を受けた段階的な改善行動」としては、大学の対応力に応じ

た「ベンチマーク評価の中で検討中または対応していない場合」、「経営執行部が関与していないが情報センター等部門で対応している場合」、「経営執行部が関与している場合」の例示を取りまとめた。

以下に、「ベンチマークリストの評価配点表」と「情報セキュリティベンチマーク評価のガイドライン」を掲載する。

ベンチマークリストの評価配点表

第１部	経営執行部の情報セキュリティに対する取組み		３０点
	問１ 危機意識の共有化	１０	
	問２ 学内ルールの徹底	8	
	問３ 防御体制の構築	7	
	問４ 予算	5	
	問５ 予算の内容 （配点なし）		
第２部	重要な情報資産の把握と管理対策について		２０点
	問１ 目録作成	１０	
	問２ アクセス権とリスク評価	5	
	問３ 個人データ管理	5	
第３部	組織的・人的な対応について		２０点
	問１ 意思決定組織	5	
	問２ 罰則規定	1	
	問３ 責任体制	1	
	問４ 外部契約	2	
	問５ 実施内容		
	（１） 危機意識の共有化	3	
	（２） ルールの徹底	3	
	（３） 防御対策	5	
第４部	技術的・物理的対策について		３０点
	問１ ログ管理	3	
	問２ 侵入検知の導入	5	
	問３ 持ち出し制限	3	
	問４ ＩＤ管理と認証	3	
	問５ アクセス制限	4	
	問６ ネットワーク分離	6	
	問７ ぜい弱性対策	3	
	問８ バックアップ	3	

情報セキュリティベンチマーク評価のガイドライン

１．ベンチマーク評価の視点

ベンチマーク評価は、昨年度作成した「大学セキュリティ運用ベンチマークテスト」の点検項目について評価の重み付けをする観点から大学として情報セキュリティ対策を振り返る上で基本となる４つの視点で再構成しました。内容としては、アウトカム評価に不可欠な要素を設定し、点検項目及び対策内容について見直しを行い、昨年度の５１項目から２３項目に選別して情報セキュリティの対応状況を一覧できるようにしました。とりわけ、大学執行部として情報セキュリティに関与することを重要視し、その上で情報資産の把握、組織的な対応、技術・物理的対応との関係性をマッチングすることにしました。

２．ベンチマークによる対応状況の確認

情報セキュリティに関する対応状況を確認するため、別紙の「ベンチマークリストの評価配点表」にもとづき、「経営執行部の情報セキュリティに対する取組み」に３０点、「重要な情報資産の把握と管理対策」に２０点、「組織的・人的な対応」に２０点、「技術的・物理的対策」に３０点を配点し、４つの視点に重み付けを行いました。特に、「経営執行部の取組み」に３０点の重み付けを行うことで、大学が組織をあげて対応することの重要性を強調しました。

以上の視点によるベンチマークは、経営執行部の取組み状況をもとに、一貫した情報セキュリティ対策が展開されているか否かを振り返ることにより、情報資産の把握と組織や技術的な対応の関係性について自己点検・評価し、不足している取組みについて改善に向け組織的に計画・行動できるようにしました。

３．情報セキュリティの改善に向けた対策

ベンチマークリストによる評価結果にもとづき、各大学が今後改善に向けて取組むべき対応及び個別の対策について、どのように改善行動を進めていくべきか、参考となる取組みについていくつかのパターンを例示的に掲げます。

（１）４つの視点で重視すべき改善対策

① 「危機意識の共有化対策」としては、情報セキュリティの脅威となる事象がもたらす被害の重大性について全学的に理解を普及し、大学構成員一人ひとりが危機回避のために気づきができるよう周知徹底を図る意思決定を行う必要があります。具体的な対策としては、脅威となる事象の被害事例を説明し、自大学で起きた場合のリスクを想定して大学構成員一人ひとりが心得るべき気づきを促します。

※ 学内外の情報セキュリティ研修会参加の義務化（例えば2年に1回）
※ FD・SD、教授会、職員会議などでの定期的な情報提供
※ Webサイトや学内文書による定期的な情報提供
※ 学生に対する注意喚起（学部・学科の履修説明会など）

② 「構成員に学内ルールの周知徹底と遵守の対策」としては、ＩＰＡ（情報処理推進機構）の情報セキュリティに関する脅威や対策などの映像コンテンツを学内LANで強制的に視聴させるなどのほか、心掛けが必要な最小限度の学内ルールの遵守状況についてアンケートで確認する必要があります。

③ 「情報セキュリティに関する意思決定や脅威となる事象に対応する組織」としては、統括責任者の役割と権限を明確にした上で、専門の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規定化します。その上で、インシデントに緊急対応する権限や防御の仕方及び外部機関や業者と情報の交換・共有をする組織を設置する必要があります。

④ 「重要な情報資産の把握対策」としては、職員は、組織的に重要な情報資産に対するアクセス制御及びリスク評価を義務付ける必要があります。教員は、情報資産を研究室単位で管理するために、情報資産の一元管理、アクセス制御、ネットワーク制御の実施を行うか、あるいは学内クラウドのように全学一元管理システムの利用などが必要となります。

⑤ 「教職員への危機意識の対策」としては、パソコン画面に「メール開封時の注意喚起」を掲示し、注意履行の確認を行わせる仕組みを設ける必要があります。また、「不審メール見極めの対策」としては、ウイルス拡散、機密情報の外部漏えい、システム破壊など被害の重大性について認識できるよう、学科単位、部署単位の関係代表者を対象にワークショップなどの見極め対策を行う必要があります。

⑥ 「不用意な情報漏えい対策」としては、大学構成員が USBなどで重要な情報資産の持ち出しをできないように規定し、システム上で禁止する対策を講じておく必要があります。

（２）自己点検・評価結果を受けた段階的な改善行動

①　「ベンチマーク評価の中で検討中または対応していない場合」については、危機意識が不足していると思われますことから、情報セキュリティの脅威について関心が高まることを優先し、情報センター等部門または委員会などで私情協や報道関係の資料を学内に発信する取組みを早急に始めることが必要です。なお、「情報セキュリティポリシーなど学内ルールを策定していない場合」については、私情協のWebサイトに掲載されている他大学の規定を参考にセンター等部門または委員会組織で早急に策定する必要があります。

②　「経営執行部が関与していないが情報センター等部門で対応している場合」については、まず執行部に対して、脅威となる事象による被害の想定や情報セキュリティに関する映像コンテンツを用いて、大学として対応すべき対策の重要性について説明します。その上で、大学として取組んでいる状況のベンチマーク評価結果を踏まえて問題点を抽出し不足している対策について認識を共有します。

③　「経営執行部が関与している場合」については、ベンチマーク評価結果にもとづき、不足している対策について他大学及び他機関での対応状況を踏まえて、改善計画を提案し、予算化を含めて実現に向けた行動の準備をする必要があります。

なお、最適な改善計画を整備するために、他大学及び他機関との情報共有の仕組みを構築する必要があります。