５－４　情報セキュリティの危機管理能力のセミナー

私立の大学、短期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推進するため、情報担当部門の関係教職員を対象に「大学情報セキュリティ研究講習会」を実施している。講習会の企画・運営・実施は、情報セキュリティ研究講習会運営委員会を継続設置して対応している。以下に活動を報告する。

（１）開催要項の決定と準備

① 大学が所有する情報資産の管理並びに運用対策に関する専門知識と情報セキュリティに求められるリスクマネージメント等の管理技術を普及することを目的としている。

② 情報セキュリティ対策チェックリストの結果を把握して、大学としてどのレベルまで対応すべきかを判断できるようにすることの意見があり、チェックリストの結果をもとに情報セキュリティ対策をテーマに、二つのコースを設けた。

③ 具体的なインシデント対応演習とその事後対応に関する課題を探り、その解決策を提言できる能力を身につける「情報セキュリティ技術部門コース」と、受講者間の情報交換やグループディスカッションを通して、情報セキュリティガバナンスのあり方や情報漏えい対策について探求し、セキュリティ対策のアクションプランについて検討する「情報セキュリティマネジメントコース」を設定することにした。

④ 情報セキュリティに対する意識改革の重要性と方策、組織全体のセキュリティマネジメントの中で情報部門の果たす役割は、全体会にて対応することにした。

平成２２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２２年８月２７日(金)～２８日(土)
２．会　　場：学習院大学目白キャンパス（東京都豊島区）
３．対 象 者：加盟大学・短期大学、非加盟私立大学・短期大学の教職員
４．開催趣旨

大学は、情報の創造・発信拠点として、社会的責任を遂行する重要な責務を担っている。しかしながら、個人情報の流出、ＵＳＢメモリの紛失、不正アクセスによる情報の持ち出しなどの事故・事件の発生が後を絶たない。大学は、情報のセキュリティポリシーの策定、不正侵害等の技術的な対応などの対策を進めてきているが、情報を直接扱う構成員一人々に情報の適切な取り扱いを呼びかけていない。

そこで、本研究講習会では、情報管理の重要性と危機意識を周知徹底し、構成員が適切に対応できるようにすることを目指して、情報セキュリティ担当部門として対応すべき取り組みの戦略を模索することにした。

５．講習会の進め方

情報セキュリティ対策をテーマに、二つのコースを設ける。私情協が作成した「情報セキュリティ対策チェックリスト」の結果を基に、インシデント対応演習とその事後対応に関する課題を探り、その解決策を提言できる能力を身につける「情報セキュリティ技術部門コース」と、受講者間の情報交換やグループディスカッションを通して、情報セキュリティガバナンスのあり方や情報漏えい対策について探求し、会員校における情報セキュリティ対策のアクションプランについて検討する「情報セキュリティマネジメントコース」を実施する。

6．講習内容

【全体会】

大学の教育活動、研究活動ならびに管理運営活動等は情報機器やネットワークによる情報システム機能に大きく依拠している。このため、ひとたび情報セキュリティに対する事故が生じると、大学運営そのものに多大な支障が生じることが想定される。

全体会では、構成員一人ひとりの情報セキュリティに対する意識改革の重要性と方策、組織全体のセキュリティマネジメントの中で情報部門の果たす役割について模索していく。

【事例１】情報セキュリティ問題への対応を如何に教職員に徹底するか

講師：濱中　正邦氏（青山学院大学事務局長）

【事例２】コンピュータウイルス感染事故発生時の対応とその後の防止対策等についての事例

講師：矢藤　邦治氏（近畿大学総合情報システム部教育システム課課長代理）

＜情報セキュリティ対策技術部門コース＞

近年、大学で発生した情報セキュリティインシデントでは、情報漏洩、不正アクセス、なりすましなどが大学全体の持続的事業の継続や信頼を脅かす事態を招いていることが多い。これらの脅威を防ぐためには、大学組織内にセキュリティマネジメントのPDCAサイクルを確立させて、セキュリティレベルの維持・向上に努めることが必須である。特に、大学のネットワーク管理やシステム管理に携わる部門から、マネジメント層の方針に基づき事前対策や事後対応に関するルールや体制の案を作成する役割が必要となっている。

本コースでは、私情協が作成した「情報セキュリティ対策チェックリスト」の結果より、インシデント対応演習とその事後対応についてシミュレーションを行って課題を探り、その解決策を提言できる能力を身につける。

【受講対象者】

情報基盤整備やネットワーク、システムの運用管理を担当しており、セキュリティインシデントの対応に携わっている方、または予定されている方。

【プログラム内容】

（１）大学のセキュリティ対策とリスクの把握

情報セキュリティ対策チェックリストの結果をもとに構成された大学のセキュリティモデルについて、「リスクの低減」「リスクの保有」「リスクの回避」「リスクの移転」について状況分析する。

（２）インシデント対応

実際にインシデント対応を演習することで、大学における情報技術部門の果たさなければならない役割をトレーニングする。

（３）技術的な事後対応と改善

技術部門の立場から行う事後対応と再発防止のためのシステム改善を演習する。

（４）体制とルールの見直し

事前対策の反省と事後対応の結果からルールや体制の課題点を検討し、マネジメント部門への事後対策方法の提言を行うためのトレーニングを行う。

【到達目標】

（１）セキュリティ対策の分析を行って、大学におけるリスクについて把握する能力を身につける

（２）大学におけるセキュリティインシデント対応に必要な技術的能力を身につける

（３）大学におけるセキュリティインシデントの事後対応に必要な情報整理・発信能力を身につける

＜B情報セキュリティマネジメントコース＞

大学において必要なセキュリティ対策を行っているものの、組織全体を通してのマネジメントにおいては不安感があり、対応に苦慮している事例が過去の情報セキュリティの事件・事故から浮かびあがっている。

本コースでは、情報セキュリティ部門として取り組むべき課題を整理・確認した上で、対応すべき取り組みの内容・手法及び課題について共通理解を形成する。その上で、大学全体の問題として対応が展開されるよう、情報センター等部門から情報管理の徹底に関する政策や構成員への意識付け、罰則の設定など、種々の提案を大学執行部へ働きかけられるようマネジメント力の強化を目指す。

【受講対象者】

大学の各部門（修学指導、進路・キャリア支援、経営戦略、自己点検・評価、研究支援、情報センター部門、法人部門等）において、情報セキュリティに関わる教職員。

【プログラム内容】

（1）情報セキュリティポリシー策定に伴う留意点の確認

情報セキュリティポリシー作成の意義、規定すべき主な内容、規程を運用する際の留意点、とりわけ構成員一人々が問題意識をもって対応できるようにするための工夫について、大学の事例及び企業の事例を踏まえて実効性の高い規定作りの在り方について考察する。

（2）情報セキュリティ対策の現状把握と課題解決に向けた準備確認

私情協の「情報セキュリティ対策の自己点検・評価チェックリスト」の回答結果を踏まえ、大学の規模・種別による対策状況の傾向を把握し、対応が遅れている主な課題を中心に、取り組みに必要な課題の洗出し・優先度の確認、PDCAサイクルによるセキュリティマネジメントの在り方を受講者間のディスカッションを通じて確認する。

（3）大学全体の問題とするための戦略の考察

情報セキュリティは、大学組織、構成員一人々に切実な問題として受け入れられていない。ひとたび事件・事故が起きると、教育・研究・経営活動、ひいてはステークホルダーなどその影響は図り知れない。しかしながら、大学は実際に事件・事故に遭遇しないと大学全体の問題として対応しないため、同じ過ちは繰り返されることになる。問題意識がない中で如何に情報セキュリティに関する理解を深めることができるのか、「情報漏えい対策の推進」を話題に、情報管理を担当する部門としての「大学執行部への関与の在り方」についてディスカッションを通じて整理し、その結果をアクションプランとして公開する。

【到達目標】

（1）情報セキュリティポリシー策定の効果と限界を理解する。

（2）情報セキュリティ対策の現状と今後取り組むべき対策の方向性を確認する。

（3）情報担当部門の役割として大学ガバナンスへの関与の仕方を理解する。

（2）開催結果と今後の課題

① 参加者は、５２大学、２短期大学、６９名であった。詳細は、資料編【資料１６】を参照されたい。

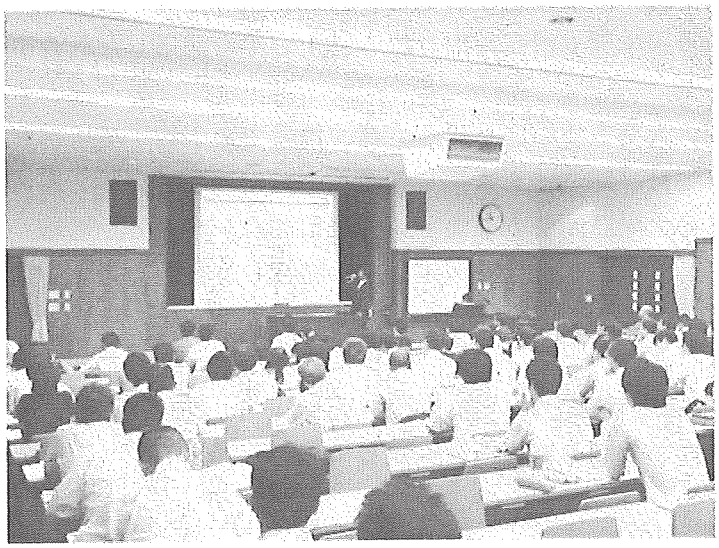
② 情報セキュリティ対策技術部門コースでは、「情報資産の再点検と活用の検討を始める」「自大学の運用の甘さを痛感・見直しをする」「課内でインシデント発生から報告までの対応策を共通認識させる」「報告して緊急性の高いものから対応を検討したい」など到達目標を達成することができた。

クラウドについては、導入自体は早いが、サービス水準合意の凍結が難しいことやシステム管理ツールなど運用面での困難は大きいことが確認された。結果として、クラウドの使用は問題のない範囲に限定したことが確認された。

③　情報セキュリティマネジメントコースでは、情報セキュリティポリシー作成の意義、規定すべき内容、運用の留意点について、大学・企業の事例を紹介した。

その上で「情報セキュリティ対策チェックリスト」の回答結果より、セキュリティ対策への取り組みの傾向分析、対応が遅れている項目の洗い出し、先進的な取り組み事例の紹介を踏まえてグループ討議を通じて取り組みに必要な課題の洗い出し、優先度の確認、PDCAによるセキュリティマネジメントの在り方を確認した。（資料編【資料９】）

さらに「情報漏えい対策の推進」をテーマに大学執行部への関与の在り方について、グループ討議を行い、その結果を「情報セキュリティに対する教職員の意識の向上」「人的対応への取り組みの弱体化が課題」「安易な情報持ち出しへの警鐘」「情報セキュリティポリシーの具体的な行動計画等の策定とPDCAサイクルの実現」「大学執行部との温度差を埋めるための方策」としてアクションプランをとりまとめ、グループごとに得ら　れた知見に関してコース参加者全体での共有が図れた。



平成22年度　大学情報セキュリティ研究講習会