５－４ 情報セキュリティの危機管理能力のセミナー

本研究講習会は、日常化している迷惑メール、情報漏洩事故、ネットでの誹謗・中傷、情報機器盗難など、大学の教育研究を脅かす事態が拡大してきており、情報セキュリティに対して学生、教職員、ステークホルダーに不安が拡大してきていることに鑑み、大学の情報セキュリティを担当する部門として、関係者が備えておくべき危機管理対策の知識と技術について、講習・討議を通じて確認・体系化し、実習により具体的な可能性と限界について検証することを目的としている。研究講習会の企画・運営・実施は、情報セキュリティ研究講習会運営委員会（委員長：宮川裕之、青山学院大学）を継続設置して対応した。以下に活動を報告する。

（１）開催要項の決定と準備

情報セキュリティ対策の要点及び自己点検の重要性と自大学の状況把握を体験することを目指した「情報セキュリティマネージメントコース」と、具体的な情報インシデント事例を想定したサーバやPC、ネットワーク機器の技術対策と人的対応の習得を目指した「情報セキュリティインシデントコース」を設定した。

マネージメントコースでは、本協会が作成した情報セキュリティ対策の点検リストを用いて、解決に向けた組織的な取り組みを模索することにした。

インシデントコースでは、システム管理者としてとるべき初期対応、学内外への通知、システムの改善技術の一部習得をめざすことにして、以下の通り開催要項を決定した。なお、両コースに共通なセキュリティ対策の点検・評価法、最新の情報セキュリティの脅威事例については全体会にて対応することにした。

平成 21年度大学情報セキュリティ研究講習会開催要項

１．開催趣旨

私立大学、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、情報の管理並びに運用対策の専門知識及び情報の管理技術の普及を目標に、本研究講習会を開催する。

２．日程：平成21年8月4日(火)，5日(水)

３．会場：工学院大学　新宿キャンパス（東京都新宿区）

４．講習の進め方：

情報管理のセキュリティ対策をテーマに、二つのコースを設ける。具体的な事案に対する技術対策を習得することを目標に、サーバや PC、ネットワーク機器の操作実習を行うコースと、情報セキュリティのガバナンス機能を高めるための情報セキュリティ対策チェックリストを活用した知識の習得、演習を行うコースを実施する。また、いずれのコース参加者にも求められる情報セキュリティ対策の要点や自己点検・評価法については、セミナー形式の全体会を実施する。

５．講習内容

全体会

1日目(10:30～12:00)：

政府の「第2次情報セキュリティ基本計画」では、「事故前提社会」の到来に向けて対応力強化が求められている。大学においては、多くの業務が情報機器やネットワークにより支えられており、ひとたび情報セキュリティに対する事故が生じると、大学の運営そのものに支障が生じることとなり、教育・研究活動に大きな影響を及ぼす。

そこで、大学として、ITを安心して教育・研究に利用するためには、どのようなセキュリティ対策を施していくべきかについて、当協会で作成した「情報セキュリティ対策チェックリスト」を活用しながら参加者間の共通理解を得ることとするとともに、情報処理推進機構より重大な事故に至る事例を紹介いただき、参加者間で意見交換を行いながら情報セキュリティ対策における組織的な取り組みについて解決策を模索し

ていく。
1)本研究講習会の趣旨説明・情報セキュリティ対策チェックリストの活用
宮川　裕之運営委員長（青山学院大学社会情報学部教授）
2)大学における最新の情報セキュリティ脅威事例
小林 偉昭氏（独立行政法人情報処理推進機構情報セキュリティ技術ラボラトリー長）

2日目(15:20～16:00)：
それぞれのコースで議論、検討、学習した内容について、相互に情報交換を行う。情報セキュリティ対策チェックリストに対して、結論の出た対応策について披瀝し合い、大学に戻ってからのセキュリティガバナンス向上に向けた材料とすることを目的とする。

コース別研究講習

A.情報セキュリティインシデント対応コース
(1日目：13:00～17:00, 2日目 10:00～15:00)

大学においても、フィッシング、spam、コンピュータウィルスやワーム、データの盗聴や改竄、掲示板での誹謗など様々な脅威に晒されており、技術者として被害を発見するスキルと加害者の発生を防ぐシステム運用の必要性が高くなってきている。
本コースでは、大学で起きた実際のインシデント事例を基に、システム管理者として調査や復旧は如何にして行うのか、対応できる範囲はどこまでなのか、学校法人や関係部署への提言は如何にすべきか等をテーマに、実習および演習を行う。

【受講対象者】
情報基盤整備やネットワーク、サーバの運用管理(DNS、電子メール、Web など)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]インシデント調査と初期対応
[2]インシデントの把握と学内・学外への告知
[3]インシデント対応事例の実際
[4]システム改善（例： DNSキャッシュポイズニング等への対策）

B.情報セキュリティマネジメントコース(1日目：13:00～17:00, 2日目10:00～15:00)
各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では、不安感を持ち対応に苦慮しているケースが過去の情報セキュリティインシデントから浮かび上がっている。本コースでは、情報セキュリティの概要を理解し、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」(http://www.juce.jp/sec2009/list.html) を題材に、グループディスカッションを通して大学における情報セキュリティ課題を鮮明にし、対応策を探究することとする。

【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]情報セキュリティの概要
[2]情報セキュリティ対策の自己点検・評価について
[3]情報セキュリティ対策チェックリストのチェック作業とディスカッション
① 情報の資産管理
② 組織的対応
③ 人的対応
④ 技術的・物理的対応
※各自で情報セキュリティ対策チェックリストによるチェック作業を行い、その結果を基に受講者間のディスカッションを通して、情報セキュリティ対策についての必要性、効果的な手法、対策の効果等について検討する。
[4]情報セキュリティ対策の方向性について検討とまとめ
※各グループのディスカッションの内容を発表し、情報共有することで、大学に求められている情報セキュリティ対策の方向性を検討するとともに、本講習会の

まとめを行う。
6．参加対象者
加盟大学・短期大学、非加盟私立大学・短期大学の教職員

（2）開催結果

① 情報セキュリティ対策の要点や自己点検の重要性と自大学の状況把握

事前に情報セキュリティ対策チェックリストによる自己点検や課題の発見を課した。参加者の大学での対策状況について組織的な対応がどの程度のレベルで行われているか、方針やルールがどの程度定まっているかについて調査させたことにより、大学での情報セキュリティ対応状況を把握することができた。

発表では「これまで曖昧であった情報の取り扱いについて、最低限満たしておくべき基準を設けるなど、明文化することが重要である」、「情報セキュリティ対策の年次目標を明確にし、段階的に対応していくことが求められる」、「情報セキュリティ対策は大学の信頼性を証明する指標の一つとなっており、同時に将来の社会人である学生に対するセキュリティ教育でもあり社会的責任を負っていることを自覚するべきである」などの意見が見られ、参加者の意識の高まりが確認された。

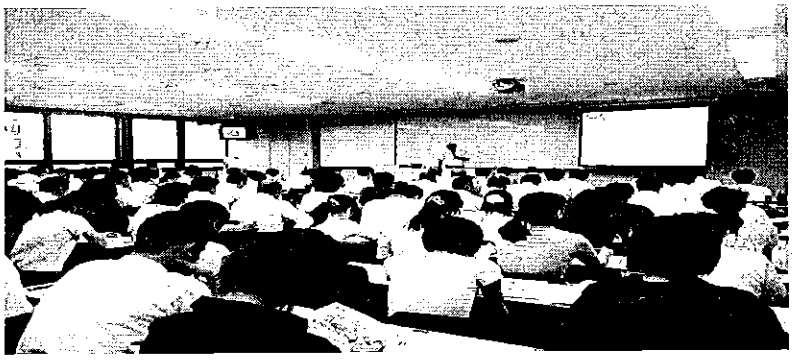
② 具体的な情報インシデント事例を想定した、サーバやPC、ネットワーク機器の技術対策や人的対応の習得

インシデントが発生した際の初期対応として窓口対応、緊急対応や組織体制のあり方、被害状況調査の技術的なアプローチ、更には外部調査機関や警察への捜査依頼の際の留意点等、人的な対応について講義を中心に確認した。技術実習では、フィッシング詐欺への対策として、DNSサーバに対する脅威であるクロスサイトスクリプティング脆弱性の悪用とDNSキャッシュ汚染について、講義とデモで理解を深めたが、DNSSEC実習では、難易度は高くスキルを十分に獲得したとは言えない状況であった。しかし、その重要性は理解されており、大学に戻ってからの対応が期待される。

（3）今後の課題

チェックリストの活用について、参加者レベルでは理解が進んだものの、大学のガバナンスのもとで活用するには、大学の情報管理の責任者が曖昧であるという状況が障害となっている。

技術実習について、DNSの対策は安定して教育環境を運営していくには必須である。本講習では、実践的な対策手法を提供したが、それが大学の情報セキュリティレベル向上に貢献したかどうかは、今後の大学サイトの改善状況を運営委員会として把握する必要がある。



平成21年度 大学情報セキュリティ研究講習会