3－8 大学情報セキュリティ研究講習会

本研究講習会は、日常化している迷惑メール、情報漏えい事故、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：奥山　徹、朝日大学）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

コース設計を検討するにあたり、現場で喫緊の課題となっているインシデント事例を素材に講習を行うことを重視して、サーバ・ネットワーク等へのインシデント対応(Aコース)と、利用者が直面するトラブルへの対応（Bコース）の二つのコースを設定することとした。

Aコースでは、迷惑メール対策、Webアプリケーションの脆弱性対策、Web掲示板への不適切な書き込みへの対応などを実施し、必要に応じてロールプレイを取り入れることとした。Bコースでは、ＰＣの起動不良、ネットワークへの接続、データの復旧等、よくある基本的な事例をもとに講習を行うこととした。また、いずれのコースの参加者にも必須の知識として、不正アクセス事件への対応、情報流出事故の対応手順や著作物の利用範囲等に関して座学による講義を行うこととし、以下の開催計画を決定した。

平成２０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

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、情報機器の盗難など、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、ステークホルダーが抱く不安は日に日に増している。そのような中で、大学の情報セキュリティを担当する部門として備えておくべき危機管理対策の技術について実習や講義を通じて習得するとともに、セキュリティ対策に必要な政策的な問題や法律を踏まえた対応策について講習等を通じて理解することを目標に本研究講習会を開催する。

２．日　程：　平成20年8月5日(火)，6日(水)
３．会　場：　文京学院大学 本郷キャンパス(東京都文京区)
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、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。実習は、その目的や対象により二つのコースを設定している。また、いずれのコース参加者にも求められる法律やセキュリティ政策上の問題についてセミナー形式の全体会を実施する。

５．講習内容
全　体　会

（前編）1日目(10:30～12:00) ： 情報運用管理の安全性を脅かす事例の紹介
情報セキュリティに対する脅威の具体例を示し、スタッフとして求められる対応について共通理解をもつこととする。
事例１： 不正アクセス事件への対応 ・・・・・ 立命館大学
事例２： spam対策の導入と現状の報告 ・・・・ 中部大学
事例３： spam対策・・・・・白梅学園大学

（後編） 2日目(13:00～15:15) ：
1. 情報流出事故への対策と手順
情報の流出や盗難に対して技術面や制度面から防止対策を行っても、100% 安全ということはあり得ない。事故が起こった後のことを想定し、被害が拡大しないよう、また、被害を回復できるよう具体的な対応と手順について学ぶ。
2. 知っておきたい著作権法・個人情報保護法の知識
個人情報保護や違法コピー問題など、情報の適切な利用について理解を深めるため、関連法規の基本的な知識を学ぶ。特に、大学という教育現場、情報ネットワークという環境に固有の問題について取り上げる。
3．質疑応答

コース別研究講習
A.情報システム管理者コース(1日目：13:00～17:00, 2日目10:00～12:00)
Webサイトに対する攻撃やspamメール等、情報の漏洩やシステムの停止に繋がるインシデントが日々起きている。これらのインシデントは重大事故に繋がる恐れがあり、管理者として、未然に防ぐための防御対策や事故発生時の復旧策について技術を身に付ける必要がある。そこで、本コースでは、ネット上に存在する脅威について、特にサーバや外部ネットワークへの出入り口部分での対応が可能なものについて、具体的事案をもとに技術習得を目指した実習を行う。また、インシデント発生時の学内外との連携に必要な、情報収集や調査等についても取り上げる。
【対象】
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。
【実習内容】
大学内のネットワークで複数のセキュリティインシデントが発生したという状況を想定して実習を行う。それぞれのインシデントについて技術的な解説を行った後、ログの解析やサーバの設定変更、機能の追加などによる改善策を実習する。
[1] 迷惑メール対策
迷惑メール対策として送信ドメイン認証(SPF)やグレイリスティング方式等について学ぶ。一方で迷惑メール対策を施したことにより、届くはずのメールが届かないというケースが増えてきていることから、メールログやヘッダの解析等により原因の特定と対策を立てる。また、学内から迷惑メールが発信されるケースについても対応策を学ぶ。
[2] Webアプリケーションの脆弱性対策
サーバ上にある個人情報が漏洩したり、サイトが改ざんされてフィッシングに利用されるケースがある。 SQLインジェクションやクロスサイトスクリプティングといったWebを攻撃する手法や実際の挙動を理解し、対策方法について学ぶ。
[3] 不適切な掲示板投稿への対応
学内利用者が学外のWeb掲示板等に対して不適切な内容の書き込みをしたと想定して対応実習を行う。利用者の特定や操作履歴の確認、クレームへの対応等を行う。

B.情報システム運用支援者コース　（1日目：13:00～17:00，2日目10:00～12:00）

大学の教育・研究および管理業務において、情報システムは今や不可欠なものとなっており、常時安定稼動し、情報の流出等の脅威なく安心して利用できることが求められる。そのためには、さまざまな技術対策が求められるが、ネットワークやサーバによる一元的な管理だけでは足りず、PC教室等の個々のPCに対する設定やソフトウェアの更新等、クライアント側の対策を施すことも求められる。

そこで、本コースでは、具体的なトラブルや事例を題材に、主にクライアント側に絞って、安定運用に必要な基本設定の確認、ログ解析、各種フィルタの設定、暗号化の方法等を実習により学ぶこととする。

【対象】

PC教室等の管理を担当している方。利用者の環境整備を行っている方。

【実習内容】

具体的なトラブルや事例について解説を行いつつ、一人一台のコンピュータを用いトラブル解決やセキュリティ対策の技術実習を行う。

[1] 情報システムの初期トラブルシューティング

サーバやルータあるいはクライアントの基本設定の確認から始まり、DNS、PROXYの設定の確認、電源投入時や再起動時のトラブル、ネットワークの過負荷やコンピュータの接続不良などのトラブル対策について実習する。

[2]クライアント-サーバサービスにおけるクライアントの設定

クライアント側でのパーソナルファイアウォールの設定やSPAM対策、ウイルス対策など、クライアント単独やサーバとの連携によるセキュリティ対策について実習する。

[3]コンピュータ上の情報漏えい対策

スパイウェア対策やフィッシング対策など情報漏えい対策、ノートPCやUSBメモリを安全に持ち歩くための対策、安全な通信路確保など、自分のコンピュータ内の情報をどのように守るかについて実習する。

4．参加申込参加対象者：

加盟大学・短期大学、非加盟私立大学・短期大学の教職員および賛助会員

※賛助会員はオブザーバとして参加が可能です。大学の情報管理の実情を理解していただくとともに、必要に応じて情報提供いただくことを期待しております。また、個別の実習環境はありません。

（２）開催結果と次年度の計画

参加者は９９大学、４短期大学の１０５名であった。開催結果の詳細は、資料編【資料１７】を参照されたい。

いずれのコースも参加者の満足度は高かったが、時間配分や難易度の設定などに今後の検討を要する。Ａコースでは、インシデント発生から原因の調査、その後の対応策という流れを意識した講習手順と受講者自ら考える時間を設けたことは、一定の評価が得られたと考えている。Ｂコースでは、情報センター部門職員などからやや易しいという意見があったものの、情報センター管理者以外の部門で支援に当たっている職員（例えば学部事務室、図書館等）など、対象を広げた今回の講習趣旨からは成功であったと言える。

次年度は、情報セキュリティ対策に大学のガバナンスが求められていることから、大学として情報セキュリティ対策の自己点検・自己評価のためのチェックリストを提示し、各項目の解決策について提示・実習を行う講習会を検討している。