情報セキュリティの危機管理能力のセミナー
「平成２８年度大学情報セキュリティ研究講習会」開催結果の概要

１．開催日時：平成２８年８月２３日、２４日
２．開催場所：学習院大学
３．参加者　：７５名（５７大学、１賛助会員）前年度７８名（６０大学、１賛助会員）

４．研究講習会の目標

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ことを目指した。

５．研究講習会の進め方

① 全体会：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
② コース：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・運営コースにて個別課題を演習
③ 総合演習：二つのコースが協働して、インシデント対応を想定した模擬演習

６．研究講習会の成果

（１）「全体会」では、以下の点が確認された。

① サイバー攻撃手法の一例として金銭を要求する攻撃、重要情報搾取の標的型攻撃、愉快犯によるWeb改ざん、不正送金などの報告があり、攻撃の脅威が拡大している。現時点では完全な予防策がないこともあり、被害の発生に即応できるような組織体制の必要性が確認された。
② 大学・法人の全構成員が意識を共有できるように、経営執行部のリーダーシップが不可欠であり、マネジメントを遂行するための役割、責任の範囲、内容に関して理解の共有を図った。
③ 「大学情報セキュリティベンチマークリスト」による点検・評価の仕組みと加盟大学の評価結果を踏まえて、今後重視しなければならない対策や大学の対応力に応じた改善行動について共通理解を図った。

（２）それぞれの「コース」では、以下の演習を通じて手順や方法の習得や組織体制の在り方・課題などの理解を共有した。

① 「セキュリティインシデント分析コース」では、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安全確認、痕跡調査の手順や方法について演習した。
② 「セキュリティ政策・運営コース」では、サイバー攻撃の脅威を理解し、「予防」、「対処」、「報告・公表」に応じた対応内容の確認と、組織体制の在り方や課題について理解を共有した。

（３）「総合演習」では、以下の模擬演習を通じて技術部門と管理部門の協働内容が確認された。

サイバー攻撃を受けていると外部から連絡が入ったこと想定して、連絡内容の信憑性確認、被害状況の調査手順、ネットワーク機器遮断の判断手順、迅速な報告を行うための内部手順、復旧に向けての手順、改善計画に向けての検討手順などについて、技術部門と管理部門における役割や対応の相互理解を深めるとともに、経営執行部の役割の重要性を認識した。