事業活動報告 NO.3

平成24年度 大学情報セキュリティ研究講習会 開催報告

本講習会は、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、サイバー攻撃に対する脅威の認識、攻撃パターンの理解、想定される対策について理解を深めることを目的として、課題の洗い出しを行い、情報セキュリティとしての全体の姿を整理し、不測の事態を想定した対応策の探究を行うセミナーとして８月23日に獨協大学（埼玉県草加市）で開催された。本協会の加盟・非加盟の大学・短期大学から参加を募集し、73名（56大学）の参加があった。

今年度は、社会の機能を停止させるようなサイバー攻撃が政府や企業を脅かし、その驚異が高度な研究の情報資産を有している大学にとっても重要な課題となりつつある現状を踏まえ、最近のサイバー攻撃の動向と具体的な対策に向けた防御システムや、新しいサイバー攻撃に対処するための組織体制などをテーマとした「全体会の講演」および、二つの専門コースを設定した。

専門コースのうち「情報セキュリティ対策技術部門コース」では、サイバー攻撃に対する要素技術の理解と防御対策の演習を中心に行った。「情報セキュリティマネジメントコース」では、サイバー攻撃のパターンを理解し、攻撃を受けた場合に必要な危機管理チームなどの組織化と関係部門との連携体制や、大学全体の教育・研究・経営に関する情報資産のセキュリティマネジメントについてグループワークなどで討議した。

全体会

全体会では新しいタイプのサイバー攻撃の仕組みや、脅威ならびに技術面・組織面における対応策等に関して以下の三つの講演を行った。

「サイバー攻撃の分析と防止策」
講師：大森　雅司氏
（独立行政法人 情報処理推進機構：IPA）

昨年８月にIPA技術本部セキュリティセンターからリリースされた「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」が紹介され、APT攻撃のような新しいタイプのサイバー攻撃の概要や分析ならびに対策法などについて講演が行われた。（詳細は25年発行のNo.4に掲載予定です）

「サイバー攻撃の脅威と攻撃パターン」
講師：高倉　弘喜氏（名古屋大学教授）

標的型サイバー攻撃の脅威や攻撃パターンについて詳細な説明がなされた後、防御側がすべき具体的かつ現実的な対応策について講演が行われた(詳細は25年発行のNo.4に掲載予定です)

「サイバー攻撃に対応する組織体制」
講師：寺田　真敏氏（株式会社日立製作所）

情報セキュリティ事故（インシデント）に対する組織的対応の事例として、日立製作所におけるインシデントレスポンスチームの活動が紹介され、サイバー攻撃に対処するための人材育成と組織体制構築の実践事例について講演が行われた。

情報セキュリティ対策技術部門コース

今年度は、最近日本でも被害例が確認された持続的標的型攻撃を題材に、大学として考えておくべき防御の仮想演習を行った。参加対象は、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、セキュリティ対策に携わっている、または予定されている教職員である。

具体的には、下記の三つのセッションに分けて演習と事例研究を行った。

１．持続的標的型攻撃に利用される要素技術の理解
（遠隔操作ツール（RAT）の紹介と対策実習）

持続的標的型攻撃に利用される要素技術の核となるRATについて、実際にインストール・操作することで、その脅威を具体的に理解した。また、RATとの攻撃者の間のHTTP偽装通信のパケットキャプチャーやログ解析を通して、その対策の技術的な難しさを理解した。

２．持続的標的型攻撃と共通攻撃動作を含むDDoSインシデントへの対応事例研究（事例研究「DDoS加害攻撃発生時のインシデントレスポンス」）

複合型DDoS攻撃には、持続的標的型攻撃と共通の攻撃動作要素が含まれ、未然に防ぐことが難しい。今回のセッションでは、実際に発生した大学からのDDoS加害攻撃事例について、そのインシデントレスポンス記録を検証した。インシデント発生現場では、セオリー通りのアプローチをとることが難しく、様々なノイズ情報の中から真のインシデント要因を把握するまでの困難さについて経験値として共有を図った。

３．持続的標的型攻撃を想定した大学ネットワークの「出口」対策（「出口」対策を重視した大学ネットワーク改善）

大学で、情報窃取を目的に持続的標的型攻撃を受ける可能性を想定し、典型的な大学ネットワーク構成図を用いて、IPAが提唱する「出口」対策の解説および実装のシミュレーションを行った。

情報セキュリティマネジメントコース

本コースでは、情報セキュリティの基礎を確認した上で、新しいセキュリティ脅威としてのサイバー攻撃について具体的事例を基に理解し、自校での危機管理体制の現状と課題を共有することで情報セキュリティ対策について考察した。また、インシデントが発生した場合に必要な関係部門との連携や、危機管理体制の構築を通じて、大学の教育・研究・経営に関する情報資産を守るためのセキュリティマネジメントについて研究討議した。

コース参加者の所属は約６割が情報部門と多いものの、教務部門、研究部門、事務部門（総務・施設部門）からの参加があった。役職では、管理職もしくは教員の方が約半数を占めた。また、昨年に引き続き、所属名から情報管理・危機管理等が主な職務と思われる参加者があり、これらの分野において大学が組織的に取り組むための体制整備が行われつつあることをうかがわせた。

１．2012年度「情報セキュリティ対策の自己点検・評価」結果について

今年度で３年目となる本協会による「大学の情報セキュリティ対策の自己点検・評価」について、結果および３年間の比較について解説した。特に、情報資産の重要度、リスク・分析対応、監査体制の整備など、各大学で取り組みが遅れている現状を報告した。

２．情報セキュリティの概要

大学における情報資産を守るために必要な情報セキュリティの考え方について、情報資産の定義、リスクの考え方、取り得る対策などに関する基本的な知識をワークシートによる実習を交えて講習した。

３．大学におけるサイバー攻撃の事例紹介

（１）危機管理における組織的対応の事例紹介

インシデントが発生した場合、大学として組織横断的に対応が求められる。このような事態への対応体制に関して、安達精一郎氏（東海大学法人本部総務部総務課）から、東海大学における危機管理の事例を基に講演が行われた。

（２）大学に対するサイバー攻撃関連の事例紹介

大学がサイバー攻撃に巻き込まれる事例は、規模の大小によらず現実に発生している。身近に迫った問題として、実際に被害・影響を受けた大学の事例（東海大学、立命館アジア太平洋大学）について、当時の状況および対応を紹介した。

４．大学における危機管理体制に関するグループディスカッション

各セッションの内容を踏まえて、大学における危機管理体制の現状をもとに、サイバー攻撃・インシデントの発生時に備えた関係部門との連携・意思決定等、危機管理体制作りに必要なマネージメントについてグループディスカッションを行った。

インシデント事例としては、１）標的型攻撃のメールの添付ファイルを開いたため、ウィルス感染の恐れのあるケース、２）大学公式サイトが何者かに書き換えられたことが判明したケース、３）学科のネットワーク機器に対するDDoS攻撃が発生したケースを取り上げた。

各グループでは、各インシデントについて議論し、検討結果を発表することで、大学における危機管理体制のあり方について理解を深めることができた。

文責：情報セキュリティ研究講習会運営委員会