５－４　情報セキュリティの危機管理能力のセミナー

＜事業計画＞

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支援するため、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」を実施する。２４年度では、特にサイバー攻撃に対する防御体制・システムの課題の洗い出しを行い、知識・技能を身につける。また、災害対策として電源確保、大学全ての情報資産の保護及び利用などの問題について、大学間での連携、クラウドコンピューティングの活用も含め検討する。

＜事業の実施状況＞

事業の実施は、「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、情報セキュリティの危機管理能力のセミナーとして「大学情報セキュリティ研究講習会」を開催した。以下に委員会及び講習会の活動状況を報告する。

情報セキュリティ研究講習会運営委員会

平成２４年６月１５日に９名が出席して１回委員会を開催し、以下の通り準備して講習会を開催した。

（１）開催計画の策定

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開催することにした。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、新しいセキュリティの課題、組織体制について理解を深めることを目指すとともに、標的型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通じた技術力の習得と情報セキュリティ事故発生時の対応策を中心に情報セキュリティの基礎知識の習得、サイバー攻撃の動向・手法等を踏まえ、関係部門との連携や危機管理体制に関するマネジメントの考察を行う場を形成するとして、以下の通り開催要項を策定した。

平成２４年度情報セキュリティの危機管理能力のセミナー
大学情報セキュリティ講習会開催要項

１．開催日程：平成２４年８月２３日(木)
２．会　　場：獨協大学（埼玉県草加市）
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

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、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大学情報セキュリティ研究講習会を開催する。

５．講習会の進め方

近年、スイッチ一つで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ており、その脅威は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。本講習会ではこのような脅威への対策を踏まえた情報セキュリティの

探究を中心に二つのコースを設ける。一つは「情報セキュリティ対策技術部門コース」として、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う。二つは「情報セキュリティマネジメントコース」として、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研究討議する。

6．講習内容

（1）全体会

昨今、政府機関や企業を対象にしたサイバー攻撃が相次いでおり、情報の盗み出し、システム破壊等の被害が発生している。大学情報システムについても攻撃対象となったり、攻撃の拠点として悪用される危険性が現実のものとなりつつある。そこで、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について理解し、新しいセキュリティの課題に対応する知識・理解を深める。また、新しいサイバー攻撃に対する組織体制についても企業の事例から理解を深める。

① サイバー攻撃の分析と防止策
大森雅司　氏（独立行政法人情報処理推進機構技術本部ｾｷｭﾘﾃｨｾﾝﾀｰ研究員）

② サイバー攻撃の脅威と攻撃パターン
高倉弘喜　氏（名古屋大学情報基盤センター教授）

③ サイバー攻撃に対応する組織体制
寺田真敏 氏 （株式会社日立製作所 Hitachi Incident Response Team）

（2）受講コース

＜情報セキュリティ対策技術部門コース＞

本コースでは、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う。具体的には、持続的標的型攻撃に利用される要素技術について学び、その防御対策の演習を大学のネットワークシステムのモデルにおいて行う。

【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、セキュリティ対策に携わっている、または予定されている教職員。

【プログラム内容】

1．持続的標的型攻撃の要素技術と防御方法

持続的標的型攻撃の要素技術をデモや演習によって学び、同時に持続的標的型攻撃による情報流出を防止するための方策を検討する。

① 遠隔操作ツールの紹介と対策実習
② 事例研究「DDoS加害攻撃発生時のインシデントレスポンス」
③ 「出口」対策を重視した大学ネットワーク改善

【到達目標】

攻撃の要素技術と防御方法を技術的な側面から理解できるようになる。

＜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理解し、対策を考える。また、情報セキュリティ事故（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する。

【受講対象者】

サイバー攻撃(標的型攻撃等)の動向や大学等の教育機関における情報セキュリティイ

ンシデントに関心のある教職員。教育機関における危機管理体制の構築・運用に関心のある教職員。

【プログラム内容】

1．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講習を行い、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身に付ける。

2．講義「東海大学における危機管理の事例」

安達精一郎氏（東海大学法人本部総務部総務課課長補佐）

情報セキュリティ事故(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。このような事態にどのような体制で臨むべきか、東海大学における危機管理の事例を取り上げて紹介する。

3．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。ここでは、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について、当時の状況及び対応を紹介する。

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、各自の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・情報セキュリティ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う。

【到達目標】

1．サイバー攻撃や情報セキュリティインシデントの動向を認識する。
2．情報セキュリティに関する基礎知識を身に付ける。
3．インシデント発生時に備えた危機管理に関する体制作りが検討できる。

（2）開催結果

平成２４年８月２３日に５６大学から７３名が参加した。

① 不特定多数のサイバー攻撃の事例から感染ルートとして、以下のようなケースを確認し、サイバー攻撃の「複雑・緻密・巧妙さ」を気づかせることができた。

＊ 政府機関などになりすました電子メールからの感染
＊ ＵＳＢメモリからの感染
＊ フリーソフトからの感染
＊ 郵便物・宅配や配布されたメディアからの感染
＊ Ｗｅｂサイト閲覧からの感染

② 特定の組織や個人を標的とする攻撃は、以下のように複雑な仕組みで行われるため、従来の検知ソフトでは発見できず、完全に阻止することが難しいことが確認できた。

＊ 攻撃対象の周辺にウイルスを感染させ、関係者の情報を集め、その情報を利用したなりすましや偽装メールなどを通じて端末に侵入する。
＊ 必要に応じて周囲の端末にも感染を拡大させ、ネットワーク・サーバ情報、ＩＤ、パスワードなどを入手し、外部との通信・制御等の設定を変更させてしまう。
＊ 侵入端末を踏み台に目的の情報にアクセスして、情報の窃取や改ざんを行い、その際、痕跡となるログ情報などを消去する。

③ 世界中で新種のウイルスが開発されており、従来の検知ソフトでは検知できないことから、侵入されることを前提に情報の入口より出口管理が重要であることが理解された。

④　参加者からは、実際に攻撃された大学の事例を通じて、脅威を実感した、危機感を持った等の意見が多く、研究室などを中心とした情報資産管理の重要性と取り組みの必要性を多くの参加者が持ち帰ることができた。この問題は、大学のみならず日本の資産が外部に窃取されるという経済面、安全保障にも関る重大な問題をはらんでいることから、政府及び企業・大学関係で情報を共有し、対策に取り組んでいくことが喫緊の課題であることが受け止められた。

⑤　事前に実施した加盟大学・短期大学の「情報セキュリティの自己点検」回答結果からセキュリティ対策への取り組みの傾向を分析し、「リスク分析」、「事故対応に対するトレーニング」など対応が遅れている項目が確認された。回答結果の詳細は、巻末のⅢ．事業報告の附属明細書【２－１７】を参照されたい。

なお、開催結果の詳細は、巻末のⅢ．事業報告の附属明細書【２－１６】を参照されたい。