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、情報担当部門の管理責任者、関係教職員を対象に「大学情報セキュリティ研究講習会」を継続実施し、サイバー攻撃に対するアクセス防御技術の演習及びインシデント情報共有の仕組み作りについて情報処理推進機構の協力を得て研究するとともに、災害時の業務継続性を確保する対策としてガバナンス関係者への働きかけなどのガイドラインを研究討議する。

＜事業の実施結果＞

「情報セキュリティ研究講習会運営委員会」を継続設置し、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２６年４月２４日、５月２２日、６月５日、７月２４日、平成２７年１月２３日に５回開催し、開催計画の策定、実施準備を行った。

（１）開催計画の策定

サイバー攻撃全般への対策と災害を想定した大学間連携による業務継続の可能性について情報を共有し、組織全体として取組むべきセキュリティの方向性を確認することを目指した。 プログラムは、全体会、コース別の研究講習、コース合同による総合演習とした。

全体会では、最新のサイバー攻撃パターン、攻撃への教育訓練事例、組織間における情報共有の重要性について紹介し、課題の確認や対処方法などを考察することにした。

テクニカルコースでは、マルウエア感染の体験を通じて感染の痕跡調査や内部拡散防止に必要なネットワーク設計演習により技術的な理解の促進を目指すことにした。

マネジメントコースでは、災害時の業務復旧・継続のための大学間・地域での連携の在り方、情報資産に限らず金融資産までも攻撃対象とされるインターネット・バンキングのインシデントを含む情報共有の活用方法と連携体制の仕組みについて、方向性を検討することにした。

以上のコース別演習・知識理解に加えて、新たに２コース合同による総合演習を行うことにした。技術面の担当者とマネジメント担当者がチームを編成してサイバー攻撃に遭遇した想定の模擬演習を行い、相互理解による連携体制の構築や課題に対処・改善できる考察力の獲得を目指して、以下のように開催計画を策定した。

大学情報セキュリティ研究講習会開催要項

１．開催日程：平成２６年８月１９日(火)・２０日(水)
２．会　　場：東海大学高輪キャンパス（東京都港区高輪）
３．対 象 者：大学・短期大学の教職員、賛助会員企業の社員でセキュリティに関係又は関心のある責任者及び担当者
４．開催趣旨
　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、教育・研究活動の情報資産の保護、信頼性の高いインフラの提供、安全性・継続性の

ある運用体制の持続可能化を図ることが喫緊の課題となっています。とりわけ、組織へのサイバー攻撃はますます巧妙化し、情報資産の流出や盗用、不正アクセスが常態化され大きな損失をもたらしています。また、情報資産以外の面でインターネット・バンキングにおける不正送金が社会問題となり、今後は大学法人部門もその大きなリスクに晒される可能性もあります。他方、近い将来想定される大規模災害に向けた情報基盤運用の業務継続性への対応について準備が進んでいないのが実情です。

そこで、サイバー攻撃全般への対策と災害を想定した大学間連携による業務継続の可能性について情報を共有し、組織全体として取り組むべき情報セキュリティの方向性を確認するための研究講習会にしています。

5．研究講習の進め方

本研究講習会では、セキュリティ専門家を交えた問題意識の共有化を全体会で行い、技術実習やディスカッションを行う2つのコース、「テクニカルコース」、「マネジメントコース」を設けていますので、下記により受講ください。

「テクニカルコース」では、情報システム部門の技術者を主な対象にしています。攻撃側の技術的な最新傾向を理解した上で、攻撃パターンの調査分析を実習してネットワークでの対処方法を技術的に理解します。

「マネジメントコース」では、教員・センター管理責任者の方を主な対象にしています。サイバー攻撃の最新傾向を大学間で共有するためのルールや仕組みと大学の情報基盤運用の業務継続を目的とした連携について、グループ討議により検討します。

その上で最終セッションでは、テクニカルコースとマネジメントコース双方の受講者が協同した実践的な「総合演習」により、サイバー攻撃全般への対処法を明確化し、情報流出を防ぐためのシステム・ネットワークの改善策について考察します。

6．研究講習の内容

（1）全体会「サイバー攻撃の最新傾向とその対策」

サイバー攻撃の脅威と最新の攻撃パターンを理解し、攻撃への教育訓練を実践している事例を踏まえてその効果と課題を確認し、最新のサイバー攻撃への対処方法として組織間における情報共有の重要性とその活用を考察します。

① サイバー攻撃の脅威と最新攻撃パターン
　高倉 弘喜氏（名古屋大学情報基盤センター教授）
　（情報セキュリティや次世代ネットワークの実践的研究に従事し、内閣官房情報ｾｷｭﾘﾃｨｾﾝﾀ、総務省、経済産業省など情報セキュリティ関連の委員を歴任）

② メールの添付ファイルによる攻撃の防御訓練を実践している広島県庁の事例
　～県庁内における標的型攻撃メールによる感染とその後のセキュリティ向上への取組みについて～
　西田 寛史氏（広島県庁総務局業務プロセス改革課情報基盤グループ主査）

③ 標的型攻撃への具体的な対処法を考察するための組織連携による情報共有」
　松坂　志氏（情報処理推進機構技術本部セキュリティセンター主幹）

（2）テクニカルコース

最初に標的型サイバー攻撃の手法とマルウェア感染の痕跡調査を実習し、その後で最新のネットワーク機器によるマルウェアの監視方法とマルウェアの諜報活動防御に向けたネットワーク設計の考え方を習得します。

【プログラムの内容】

1．典型的な標的型攻撃手法の紹介と実習
　標的型攻撃の要素技術である遠隔操作ツールの機能を紹介し、実習を通じてそのリスクを理解します。

2．標的型攻撃の最新傾向と痕跡調査
　パソコン端末上でのマルウェア感染の痕跡調査を実習し、諜報活動パターンを詳しく理解します。

3．標的型攻撃に強いネットワークの設計

諜報活動を防ぐためのネットワーク設計の様々なアプローチ方法を理解します。

4．最新ソリューションによるマルウェア検知

最新のネットワーク機器導入によるマルウェアの対策を体験します。

【到達目標】

1．標的型攻撃などのサイバー攻撃に用いられる要素技術を理解できる。

2．サイバー攻撃の防御方法、対処方法を技術的な側面から理解できる。

（3）マネジメントコース

災害時における大学の情報紛失及び情報断絶のリスクを想定し、業務の復旧及び継続を実現するための対策について大学間や地域での連携の在り方を探求します。また、サイバー攻撃だけでなく、インターネット・バンキング攻撃のインシデントを含む情報共有の活用方法と連携体制の仕組みについて方向性を検討します。

【プログラムの内容】

1．災害など非常時における情報基盤運用の業務継続性に関する検討

① 情報提供：「大学における情報紛失及び情報断絶のリスク分析と業務継続のための条件」

② 情報提供：「大学間連携による情報基盤ＢＣＰの実現」

③ グループ討議：「非常時を想定した業務復旧・継続に向けた全学的な検討組織と制度設計・リスク対策」

2．サイバー攻撃を含むインシデント情報の紹介及び情報共有の活用と連携体制の検討

① 情報提供：「インターネット・バンキングへの攻撃手口と考えられる対応策」
大坂　元一氏（一般社団法人全国銀行協会企画部次長）

② 情報提供：「インシデント情報共有の仕組みづくりの提案」

③ グループ討議：「インシデント情報共有のためのルール」

【到達目標】

1．非常時における大学情報システムの業務復旧・継続に向けた大学・地域連携の在り方が理解できる。

2．サイバー攻撃を含むインシデント情報の共有と連携体制の必要性と仕組みについて理解できる。

（4）総合演習

テクニカルコースとマネジメントコース双方の受講者が協同して、標的型攻撃を含むサイバー攻撃全般を想定したインシデントへの対応演習を行います。その上で、情報流出を防ぐためのシステム・ネットワークの見直しと改善の方向性を考察します。

【プログラムの内容】

1．インシデントレスポンス概要

標的型攻撃を含むサイバー攻撃全般を想定したインシデント発生時の対応について、センター管理責任者、技術者の立場から対応基準を確認します。

2．「検知」「初期対応」の演習

インシデント発覚後の初動対応についてそれぞれの役割を確認する中で、模擬的に対応を展開し、事後対応の適切性を振り返ります。

3．対応内容の検証

上記の演習を通じて情報資産の流出や盗用、不正アクセスを防止するシステム・ネットワークについて改善の方向性を考察します。

【到達目標】

1．インシデントレスポンスの際に必要な教員・センター管理責任者・技術者の連携体制を構築できる。

2．サイバー攻撃全般から情報を守るためのシステム・ネットワークの見直しと改善の方向性が理解できる。

（２）開催結果

平成２６年８月１９日から２０日の２日に亘り開催し、４３大学から５６名が参加した。

① 「全体会」では、サイバー攻撃の最新傾向とその対策について、攻撃の対象・手法・手順、防御のための模擬訓練、情報共有の重要性について理解の共有を図った。

＊ 標的型攻撃の脅威としてマルウェアの組織拡散による情報漏洩とデータ破壊が説明され、複合機やビル設備制御システムなどからの情報漏洩にも注意喚起が行われた。

＊ 標的型攻撃メールへの防御対策の実例として、フリーメールアドレスからの発信、深夜などの時間帯による発信が多いことから、メールの開封を誘いこむような仕掛けに添付ファイルの開封に一人ひとりが注意することが徹底された。訓練を始めたころは開封してしまう件数が多かったが、訓練を継続している現時点では開封が全くなくなってはいないが、無造作に開封することがなくなるなど訓練の有効性が紹介された。

＊ 最新の攻撃の特徴として、本人に成りすますかのように対話をするイメージで攻撃を仕掛けてくることから、これまでの防御方法に限界がでてきているため、常に最新の攻撃情報を共有する仕組みが必要なことが改めて確認された。

② サイバー攻撃への防御を技術面から探求する「テクニカルコース」では、メールやＵＳＢを媒体としたマルウェア感染を体験するなど実習を通じて技術的に内部拡散防止に必要な知識理解の促進を図った。

＊ 攻撃内容を特定するために感染した端末の痕跡について、実行しているファイルの特定、メモリ上での動作状態の把握などにより調査方法を確認した。

＊ 出口対策や内部拡散防止対策の一手段として、仮想ネットワーク（VLAN）の設計演習を行うとともに、感染状況の様子を可視化し時間経過の中で検出するソフトの紹介を通じて理解の促進を図った。

＊ 参加者からの反応として、「普段体験できない攻撃環境、本物のウィルスによる感染がイメージできた」、「講習内容を自大学に適応したい」などの意見があった。

③ 災害時の業務継続への対応とインシデント情報共有の仕組みを探求する「マネジメントコース」では、業務継続のための大学間連携の在り方、サイバー攻撃情報共有の課題などグループ討議を通じて大学として取り組むべき姿勢について理解を共有した。

＊ 災害時の情報紛失や情報断絶のリスク分析と業務継続に必要な条件や対策について、地域社会と大学などとの連携、大学間による業務継続性の連携を進めることの重要性を共有した。

＊ サイバー攻撃の問題は、情報資産に危害を加えるだけでなく、金融資産までも攻撃されていることから、インターネット・バンキングへの攻撃手口について全国銀行協会からの情報提供をもとに大学としての備えを法人部門などにも拡大し、危機意識の醸成に努めることが確認された。

＊ 参加者からの反応として、「学内での情報共有から始めたい」、「地域での連携からスタートしたい」、「銀行協会の取り組みから情報共有の必要性が理解できた」、「情報基盤共有の共通環境ができることが望まれる」、「一つの大学で共有の仕組みづくりは難しいため第三者機関の主導を望む」などの意見があった。

④ 総合演習では、「テクニカルコース」と「マネジメントコース」合同でサイバー攻撃に遭遇したことを想定した模擬演習を技術担当者と管理担当者の連携による対応策を考察した。演習では、「検知・初期対応」、「想定被害のリストアップ」、「初期対応の準備と内容」についてグループ討議し、それぞれの立場での役割や対応について相互理解を深めた。

開催結果の詳細は、事業報告の附属明細書【２－12】を参照されたい。