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。標的型サイバー攻撃から大学の情報資産を守るための国、大学間等との連携の在り方、教職員による危機管理意識の醸成、管理体制及び監視技術、攻撃の可視化等の防御対策について、事例を踏まえて研究講習を実施する。以上の他に、災害時に向けての大学間による情報資産の預かりの可能性、大学全体の情報セキュリティ対策の自己点検・評価の課題と具体的な取り組み等について理解を深める。

＜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２５年６月１４日に１回委員会を開催し、９名が出席して、以下の通り準備して講習会を開催した。

（１）開催要項の策定

サイバー攻撃は日を増して激化してきており、サイバー戦争とも言われる状況の中、政府機関及び企業の重要な情報が窃取・流出する事態が頻発していることから、大学としても組織で「情報資産を守る」という視点から、サイバー攻撃への対策と情報資産の保全及び災害を想定した業務継続に向けた対応について、情報セキュリティ対策の現状及び問題点について意識合わせするとともに今後のセキュリティ対策の仕組み及びガバナンス強化を目指すことにした。

そこで、サイバー攻撃に対する問題の重要性の理解を図るとともに、攻撃と対処についての情報の共有化や大学間・政府関連機関との連携の仕組み及び災害対策として遠隔地の大学と情報資産の相互補完及び業務継続性について、事例を踏まえて可能性を模索することにした。また、サイバー攻撃に対する防御対策の演習を通じた技術力の習得、攻撃パターンを想定した教員・職員・学生による組織的な防御体制、大学間及び社会の関係機関との連携体制の仕組み、情報資産のセキュリティマネジメント、災害時のリスクマネジメントの考察を行う場を形成することにして、以下のとおり開催要項を策定した。

平成２５年度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２５年８月２７日(火)
２．会　　場：学習院大学（東京都豊島区目白）
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、大学が組織として「情報資産を守る」という視点から、サイバー攻撃への対策と情報資産の保全及び災害を想定した業務継続に向けた対応について、情報セキュリティ対策の現状及び問題点について意識合わせするとともに今後のセキュリティ対策の仕組み及びガバナンス強化を目指します。

5．講習会の進め方

サイバー攻撃は日を増して激化してきており、サイバー戦争とも言われる状況の中、政府機関及び企業の重要な情報が窃取・流出する事態が頻発しています。大学においても昨年国立大学の５大学で論文・研究報告・教職員のメールアドレスなどがハッカー集団に窃取されその情報が公開されました。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全体会および二つのコースを設けます。

第一のコースは「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防御対策の演習や業務継続性を確保するための技術面での条件整理などを行います。

第二のコースは「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から攻撃を想定した教員・職員・学生による一体的な防御体制などの組織化と大学間及び社会の関係機関との連携体制の仕組み、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、災害時のリスクマネジメントについて研究討議します。

6．講習内容

（1）全体会１「サイバー攻撃への対策」

「大学力が日本の競争力の源であり、成長戦略の柱」とされている中で、大学が知を集積して創造する教育・研究活動の情報資産管理が大きな課題となってきます。昨今、政府機関、企業、大学を対象にしたサイバー攻撃が相次いでおり、情報の窃取・流出が常態化してきています。問題は攻撃の手口が複雑でステルス化しているため窃取されている実感がないことと、大学の情報資産管理が組織的に対応されておらず、現場任せとなっております。そこで、サイバー攻撃に対する問題の重要性を理解いただき、その上で攻撃情報及び対処方法など関連情報の共有化を図るために大学間連携と政府関連機関との連携の仕組みについて可能性を模索します。

① 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）

② サイバー攻撃対策の情報共有組織「J-CSIP」の取り組み
　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任）

（2）全体会２「災害時を想定した対策」

大規模な震災が予測されており、いつ震災が起きても不思議ではない状態にあります。大学の社会的責任を果たすためには、教育・研究活動の成果としての情報資産及び災害時での情報通信体制の確保が喫緊の課題とされていますが、大学に危機意識が薄く十分な災害対策が進んでいないのが現状です。そこで、遠隔地の大学との情報資産の相互補完及び業務継続性の可能性について、大学間による補完の範囲や方式及び条件合わせなど先進的に進められている実践例を伺い、大学間での連携協定に至るプロセスを踏まえて配慮すべき点を明確にします。

＊ 大学間業務継続連携事業によるIT-BCP基幹システム
　永井 明 氏（宇都宮大学学長補佐・総合メディア基盤センター長）

（3）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、一つは標的型サイバー攻撃の攻撃手法や攻撃を受けた場合の対処方法を演習などによって理解を深め、情報流出の出口対策としてのシステム管理技術とネットワーク技術の必要性と課題を整理します。二つは災害対策の一環として平常時から大学情報システムの業務継続性を確保するため、事前準備及び復旧対策のシミュレーションや訓練の在り方について理解を深めることを目指します。

【受講対象者】

情報セキュリティを担当する現場責任者、情報基盤整備やネットワークなどの運用管理の担当者などとします。

【プログラム内容】

① 標的型サイバー攻撃の攻撃手法と防御方法

攻撃を受けた場合にどのような対応をとるべきか選択肢を設けて判断させ、その判断基準を自ら振り返ることができるように模擬体験の演習を行います。その上で情報の流出を防止するための防御方法について階層的なネットワークの構築も含め

た方策を検討します。
② 大学情報システムの事業継続性の確保
大学情報システムの事業継続計画を立案する上で、情報システムの緊急復旧計画及び代替運用計画を業務分析ワークシートに基づいてシミュレーションすることで、例えば、ＤＮＳの設定変更やドメイン管理事業者の確認など大学が最小限行うべき項目を検討します。

【到達目標】
① 攻撃の要素技術と防御方法、対処方法を技術的な側面から理解できるようになる。
② 大学情報システムの事業継続計画のポイントを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、大学の教育・研究・経営に関する情報資産を守るため情報セキュリティマネジメントの観点から、喫緊の課題であるサイバー攻撃の対策、災害を想定した対策をテーマに取り上げ、攻撃や災害により脅威やリスクの重要性を確認するとともに学内教職員による協力体制の構築と大学間及び外部組織との連携による情報資産保護の仕組みについて協議し、情報セキュリティに対する大学組織としての対応を目指します。

【受講対象者】
情報セキュリティを管轄するガバナンス責任者(センター部門長など)及び情報セキュリティを担当する現場責任者などとします。

【プログラム内容】
① 情報セキュリティ対策の自己点検・評価の結果分析と活用
情報セキュリティ対策への経営執行部による関与が極めて低く、大半は情報部門の責任者と現場担当者が中心となっています。そのために情報資産の保護を中心とした対策への取り組みは極めて低く、危機管理に対する意識が十分でない。そこで本協会が作成した「情報セキュリティ対策の自己点検・評価リスト」を用いて各大学にセキュリティに対する危機意識を振り返りさせるとともに、サイバー攻撃対策・災害対策に情報セキュリティが基盤的に必要であることの関連付けを行います。
② サイバー攻撃への危機意識の共有と連携体制の検討
サイバー攻撃は、もはや日常的に行われており、大学等の教育機関も標的型サイバー攻撃の対象となることは免れない。また、標的型攻撃の被害を受けるだけでなく、標的型サイバー攻撃に組織の名称等を利用されるなど、知らずの内に攻撃に関わってしまう事例も起こっています。そこで、実際に発生したサイバー攻撃の事例を紹介し、インシデント発生後の対応や事後の予防策、学内で教職員が一体となって情報資産を守るための協力体制や大学間による情報共有の仕組み等について検討します。
③ 災害を想定した情報セキュリティ対策の検討
本協会の２３年度調査によれば、災害に対する安全管理への対応は６割が未実施となっており、災害対策が進んでいない状況にあります。これらの問題解決には、日常から危機管理体制に向けたシミュレーションや訓練が必要であるが、ガバナンスによる組織的な対応が十分でないことから、教職員が一体として動ける体制が構築されていない。ここでは、震災発生からこれまでの対応について被災した大学の災害対策の現状報告を踏まえて、遠隔地域の大学間連携による業務継続性の確保、重要情報資産の二重化対策などの可能性について検討します。その際、大学間での協定による連携の可能性についても検討します。

【到達目標】
① サイバー攻撃の手法や情報セキュリティインシデントの動向を認識し、対策を検討できる。
② 災害に関して情報システムが備えておくべき対策について検討できる

（２）開催結果

平成２５年８月２７日(火)に開催し、５８大学から教職員７４名の参加があった。

① サイバー攻撃情報及び対処方法の情報共有の仕組みについて、大学として今後考えていくべき重要な課題であることが理解された。

＊ サイバー攻撃は被害発生の半年前から内部に侵入している場合が多く、その攻撃全ての把握には１年程度の時間が必要になるなど、攻撃のステルス化が確認された。また、個人持ち込み機器を経由した意図しない攻撃が新たな脅威として確認された。

＊ 攻撃への「出口」対策等の見直しとしてVLANによるアクセス制御など攻略し難いネットワークへの移行やサーバ・クライアントの仮想化促進の必要性が確認された。

＊ 情報処理推進機構（IPA)によるサイバー攻撃に関する情報共有の取組みは、類似する攻撃の早期発見による被害の回避に有用であることが確認された。

＊ 架空の標的型攻撃シナリオによりサイバー攻撃を体験し、攻撃を受けた場合の初動対応や痕跡調査について演習で対処方法の理解を深めた。

＊ 講習後のアンケート結果からは、「情報担当者への啓蒙を進めたい」、「職員の意識を変えていきたい」、「学内のネットワーク利用者講習会に内容を盛り込みたい」、「情報共有の有効性を再認識した」など大学全体の問題として、「情報資産を守る」組織的な取組みの必要性を参加者が持ち帰ることができた。

② 災害時を想定した情報資産の相互補完及び業務継続性の可能性について、実際の導入事例から今後の取組みとしての課題ととなることを理解した。また、大学組織として今後求められる対応を見据えた検討が行われた。

＊ 大学ガバナンスが主導する大学間業務継続の連携事例から、２大学の仮想化基盤の共有や職員交流と相互の運用提携の取組みなど利用環境を含めた総合的な業務連携の計画が紹介され、大学全体で災害への危機対策に取組むことの必要性を確認した。

＊ 情報資産の保護など組織的な取組みについてグループ討議することで、大学間での連携の可能性や更なる改善・継続的な取組みの必要性が確認された。

＊ 大学間での情報共有や情報の相互補完については必要性は理解されたが、実現に向けては運用の仕組みなど継続的な検討が必要とされることが確認された。

開催結果の詳細は、巻末の事業報告の付属明細書【２－１２】を参照されたい。