公益社団法人 私立大学情報教育協会

平成２６年度 大学情報セキュリティ研究講習会

開 催 要 項

http://www.juce.jp/sec2014/

日程：平成２６年８月１９日(火)・２０日(水)
会場：東海大学高輪キャンパス（東京都港区高輪）
受講対象者：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・関心のある責任者及び担当者

１．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があります。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ことにしています。

２．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。

３．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。

「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ー、総務省、経済産業省などにおいて情報セキュリティ関連の委員を歴任）

「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」
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）

「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任）

（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。

【プログラム内容】

１．遠隔操作ツール（ＲＡＴ）の機能

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．標的型攻撃のインシデント分析

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．ネットワークセキュリティの基本技術と設計

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．標的型攻撃に強いネットワークソリューション

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。

【講師】

- 岩井博樹氏(デロイトトーマツサイバーセキュリティ先端研究所主任研究員、デロイトトーマツリスクサービス株式会社マネジャー)は、被害サーバの解析や攻撃検知におけるプランニングを専門とし、 著書に「標的型攻撃セキュリティガイド」などがあります。本コースでは上記1. 2. の実習を担当する予定です。
- 葛生晋一氏(シスコシステムズ合同会社:私情協賛助会員)は、エンジニアで講師経験も豊富です。本コースでは上記4. の実習を担当する予定です。

【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復旧・継続のための対策」

② 情報提供「情報基盤運用の業務復旧・継続を実現するための大学間連携の在り方」

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 事例紹介「インターネット・バンキングの攻撃手口と考えられる対応策」（一般社団法人全国銀行協会）

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．インシデントレスポンス演習

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．サイバー攻撃に強いシステム・ネットワークの見直し

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。

参　加　申　込

対 象 者：大学・短期大学の教職員、賛助会員企業の社員
募集定員：テクニカルコース 60 名　　マネジメントコース 60 名
参 加 費：加盟校・・・30,500 円、非加盟校・・・61,000 円
申込方法：本開催要項に添付の申込書に記入の上 FAX 願います。
申込締切：8 月 12 日(火)

参加費の支払い：参加費は、**8 月 13 日(水)**までに銀行振込によりお支払いください。
＜振込先＞　りそな銀行 市ヶ谷支店 普通預金口座
口座番号：００５４４０９
名 義 人：**私情協**
シジョウキョウ
＊ お願い：振込手数料は負担願います。また、振込名義に「sec26」の記号を追記願います。
＊ キャンセルの場合は、**8 月 13 日(水)**までにご連絡いただければ、振込手数料を差し引いた参加費を返金します。
それ以降のキャンセルは、資料代等の実費を請求します。

お問い合わせ先：　電話：03-3261-2798 FAX：03-3261-5473
その他：申込に関する情報は Web サイトに随時更新しますので、ご確認くださいますようお願いいたします。また、参加者へのご連絡は電子メールにて行いますので、申込の際にアドレスを必ずご記入くださいますよう、お願い申し上げます。

進　行　予　定

8月19日（火）

全 体 会			
13:00	「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） 「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」 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） 「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任）		
14:50	休憩、移動		
テクニカルコース		**マネジメントコース**	
15:00	・テクニカルコース概要説明 ・遠隔操作ツール（RAT）の機能	15:00	・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 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復旧・継続のための対策」 情報提供「情報基盤運用の業務復旧・継続を実現するための大学間連携の在り方」 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」
16:30	・標的型攻撃のインシデント分析 マルウェア感染痕跡調査 感染経路のパターン解説とその調査方法		
18:00		18:00	

8月20日（水）

テクニカルコース		**マネジメントコース**	
9:00	・本日の進め方 ・ネットワークセキュリティの基本技術と設計 ・標的型攻撃に強いネットワークソリューション	9:00	・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 事例紹介「インターネット・バンキングの攻撃手口と考えられる対応策」（一般社団法人全国銀行協会） 情報提供「インシデント情報共有の仕組みづくりの提案」 グループ討議「インシデント情報共有のためのルール」
12:00	昼食		
総合演習			
13:00	・インシデントレスポンス概要 ・インシデントレスポンス演習 ・サイバー攻撃に強いシステム・ネットワークの見直し		
15:00			

平成２６年度 大学情報セキュリティ研究講習会 参加申込書

※ 必要事項を記入の上、FAX（03-3261-5473）にてお申し込みください。
※ 本紙はコピーしてお使いください。

・ご記入いただいた個人情報は、本研修に関する事務連絡およびその他の研修事業への案内に限定して利用させていただきます。
・データベース管理作業の外部委託の際には目的外の利用や情報の流出がないよう、十分留意いたします。

『事務連絡担当者記入欄』

大学名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

担当者名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

所属・役職：＿＿＿＿＿＿＿＿＿＿＿＿　E-Mail：＿＿＿＿＿＿＿＿＿＿

電話番号：＿＿＿＿＿＿＿＿＿＿＿＿　FAX**番号**：＿＿＿＿＿＿＿＿＿＿

大学所在地：（郵送でご連絡差し上げる場合の連絡先）

（〒　　）

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

種　別：（どちらか一つに○をつけてください）　**加盟校**　・　**非加盟校**

『参加者記入欄』

① **氏　名**：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
E-Mail：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
所属・役職：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
参加コース：（どちらか一つに○をつけてください）
テクニカルコース　・　**マネジメントコース**

② **氏　名**：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
E-Mail：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
所属・役職：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
参加コース：（どちらか一つに○をつけてください）
テクニカルコース　・　**マネジメントコース**

③ **氏　名**：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
E-Mail：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
所属・役職：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
参加コース：（どちらか一つに○をつけてください）
テクニカルコース　・　**マネジメントコース**

④ **氏　名**：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
E-Mail：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
所属・役職：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
参加コース：（どちらか一つに○をつけてください）
テクニカルコース　・　**マネジメントコース**