公益社団法人 私立大学情報教育協会

平成２９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/sec2017/

日程：平成２９年８月２４日(木)・２５日(金)
会場：学習院大学（東京都豊島区）
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

サイバー攻撃は、巧妙・大規模になっており、情報資産・金融資産の窃取・漏洩・破壊などが日常化し、大きな社会問題となっています。大学の教育・研究現場でも入試・成績情報、個人情報、その他機密情報がネットワーク経由で窃取されるなどの事例が頻発化してきており、情報セキュリティ管理の甘さが問題視されています。そのためには、構成員全員がサイバー攻撃の脅威を理解し、防御行動を意識して実践するなどのリスクマネジメント対策の強化が求められます。

そこで本協会では、サイバー攻撃に対する防御行動が組織的に展開されるようにするため、経営執行部による組織的な対応、構成員一人ひとりによる注意と行動、情報担当部門としてのベンチマークによる自己点検・評価・改善の習慣化を通じて、大学の対応力に応じた情報セキュリティ対策の考察を目指します。

２．研究講習会の進め方

サイバー攻撃の最新動向、ベンチマークリストにもとづく大学の対応状況、攻撃に緊急対応する専門チームの課題を共有する「全体会」を行った上で、身代金要求型攻撃に関する知識の習得及び実習を行う｢セキュリティインシデント分析コース｣と、情報セキュリティの促進政策と周知徹底する方策を学ぶ｢セキュリティ政策・運営コース｣を設けています。その上で、技術部門と政策部門の混成チームによる模擬演習と規模別グループによる課題解決演習を行う「総合演習」を設けています。

３．研究講習会の内容

（１）全体会「サイバー攻撃の動向とセキュリティ施策の成果」

サイバー攻撃の最新動向を理解した上で、「大学情報セキュリティベンチマークリスト」によって明らかになったセキュリティ対策・対応の成果を紹介し、経営執行部の情報セキュリティに対する取り組み、情報資産の把握と管理対策、組織的・人的な対応、技術的・物理的対策の問題点を共有化します。

「情報セキュリティ 10 大脅威」から見るサイバー攻撃の動向
　　独立行政法人情報処理推進機構
「ベンチマークリスト評価結果の動向」
　　情報セキュリティ研究講習会運営委員会
「情報セキュリティ事故に緊急対応するための体制組織化への取り組み」
　　上原 哲太郎 氏（立命館大学情報理工学部教授）

（２）セキュリティインシデント分析コース

マルウェアを用いたサイバー攻撃の実態や仕組みを確認し、特に身代金要求型攻撃（ランサムウェア）感染時の調査・対応方法について演習で学びます。

【プログラム内容】

１．マルウェア感染被害の状況把握

マルウェアの振る舞いについて理解を深め、さらに感染が発覚した際に行う PC の痕跡調査や他システムへの影響など、被害の状況を把握する手法について確認します。

２．マルウェア感染時の対応手順

被害の状況を調査した結果、不正通信や情報流出の恐れがある場合の緊急対応について確認します。さらに被害拡大を防ぐための事前の取り組みについて、技術的な理解の促進を図ります。

【到達目標】

１．サイバー攻撃の疑いがある場合の調査方法を習得します。
２．サイバー攻撃を受けた場合の対処方法・手順を習得します。

（３）セキュリティ政策・運営コース

経営執行部による組織的な対応、構成員一人ひとりによる注意と行動、情報担当部門としてのベンチマークによる自己点検・評価・改善の習慣化を目指して、被害に遭わないための手立て「予防」、被害を最小限にする「対処」、事後の対応「報告・公表」を適切に遂行するための取り組みについて考察します。

【プログラム内容】

１．情報セキュリティを促進するための政策

「予防」、「対処」、「報告・公表」を組織的に展開する必要性を共有するため、「大学情報セキュリティベンチマークリスト」をもとに参加大学の規模に応じた実態を確認し、それぞれの特徴や課題を整理する中で、情報セキュリティの改善に向けた対策を探求します。

２．情報セキュリティを学内に周知徹底するための対策

大半の大学が Web サイトによる情報セキュリティ対策の周知を行っていることを踏まえ、教職員一人ひとりに情報セキュリティの意識を日常化していく工夫を考える必要がある。そこで、情報セキュリティに関心が向けられるよう、組織として構成員一人ひとりにサイトの活用状況を点検・確認する方法や分かりやすい情報提供の内容、例えば改正個人情報保護法・不正アクセス禁止法・著作権法への適用、偽装メールの注意喚起、被害事例などについて具体的な周知徹底の取り組みを考察します。

【到達目標】

１．規模に応じた情報セキュリティの改善に向けた対策が理解できるようになります。
２．情報セキュリティ対策を周知徹底する視点及び取り組み方法を提供できるようになります。

（４）総合演習

マルウェアを用いたサイバー攻撃を想定した実践的な演習ストーリーにもとづき、被害遭遇時の対処方法及び今後の課題整理を模擬演習により獲得します。その上で、サイバー攻撃全般に対する情報セキュリティ対策の問題点を洗い出し、大学での取り組みを考察します。

【プログラム内容】

１．技術部門と政策部門の混成チームによるサイバー攻撃への対応演習

① 被害遭遇時の対処方法などをワークシートで確認
② 技術的、組織的な課題の整理

２．規模別グループによる情報セキュリティ対策への課題解決演習

① 情報セキュリティ対策の具体的な問題点の洗い出し
② 課題解決策の策定と発表

【到達目標】

１．サイバー攻撃への対処方法を理解できます。
２．大学での情報セキュリティ対策への課題解決策を獲得できます。

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：セキュリティインシデント分析コース 40 名
　　セキュリティ政策・運営コース　　40 名　（申込先着順）
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 19 日(土)

参加費の支払い：参加費は、8 月 21 日(月)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「sec29」の記号を追記願います。
　＊ キャンセルの場合は、8 月 21 日(月)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24日(木)

全 体 会 ［南3-301教室］			
10:30	「情報セキュリティ10大脅威」から見るサイバー攻撃の動向 「ベンチマークリスト評価結果の動向」 「情報セキュリティ事故に緊急対応するための体制組織化への取り組み」		
12:00	昼食		
セキュリティインシデント分析コース［南3-101教室］		**セキュリティ政策・運営コース［南3-401教室］**	
13:00	マルウェア感染被害の状況把握	13:00	情報セキュリティを促進するための政策
	マルウェア感染時の対応手順		情報セキュリティを学内に周知徹底するための対策
16:30		16:30	

8月25日(金)

総合演習 ［南3-401教室］	
9:30	技術部門と政策部門の混成チームによるサイバー攻撃への対応演習 ①
12:00	昼食
13:00	技術部門と政策部門の混成チームによるサイバー攻撃への対応演習 ②
	規模別グループによる情報セキュリティ対策への課題解決演習
16:30	

平成29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)
セキュリティインシデント分析コース　・　セキュリティ政策・運営コース

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)
セキュリティインシデント分析コース　・　セキュリティ政策・運営コース

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)
セキュリティインシデント分析コース　・　セキュリティ政策・運営コース

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)
セキュリティインシデント分析コース　・　セキュリティ政策・運営コース