

公益社団法人 私立大学情報教育協会

平成28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/sec2016/>

日程：平成28年8月23日(火)・24日(水)

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、非常に巧妙になっており、官公庁、企業、学校でも情報資産の窃取・漏洩などが頻発化してきており、大きな社会問題となっています。とりわけ、学校現場では成績情報・個人情報ネットワーク経由で窃取されるなど情報セキュリティ管理の甘さが問題視されています。このような問題は、以前から種々指摘されその対策について学校としての対応が求められてきていますが、組織的にサイバー攻撃の脅威を周知し、防御行動が展開されるよう構成員全員による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理解の普及を徹底するため、情報セキュリティの対策をベンチマークし、課題の洗い出しを行い、自己点検・評価を習慣化する中で構成員一人ひとりがサイバー攻撃の脅威を認識し、大学として段階的にセキュリティ対策や体制を整備できるように課題を共有するための研究講習会としています。

2. 研究講習会の進め方

サイバー攻撃に対する防御意識を徹底できるようにするため、情報セキュリティに最小限必要な対策・対応をベンチマークにより振り返ることの重要性及び課題を共有する場として「全体会」を行った上で、インシデント対応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、セキュリティ意識の醸成を学内に推進・普及していく方策を検討する「セキュリティ政策・運営コース」を設けています。その上で、二つのコース双方の受講者が協働して、防御意識に基づき行動ができるようにインシデント対応を想定した「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防御行動の点検・評価」

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」による点検・評価の仕組みや、今後改善に向けて取り組むべき対策・対応を紹介し、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・物理的対策の課題を共有化します。

「サイバー攻撃の最新動向について」

満永 拓邦 氏（東京大学情報学環特任准教授）

「経営執行部の情報セキュリティに対する取り組みについて」

宮川 裕之 氏（青山学院大学情報メディアセンター所長）

「大学情報セキュリティベンチマークリストの紹介と評価方法」

井端 正臣 氏（公益社団法人私立大学情報教育協会事務局長）

「ベンチマークリストの評価結果と改善に向けて取り組むべき対策・対応」

満永 拓邦 氏（東京大学情報学環特任准教授）

(2) セキュリティインシデント分析コース

標的型サイバー攻撃のマルウェアによる情報窃取の実態などを確認し、不正通信を検知した時の調査・対応方法について演習で学びます。

【プログラム内容】

1. 標的型サイバー攻撃による情報窃取

情報窃取・情報流出のリスクと手口、インシデントレスポンスの基本的な流れについて確認します。

2. 標的型サイバー攻撃のインシデントレスポンス演習

不正通信の痕跡調査、情報流出の拡大を防ぐための緊急対応手段について技術的な理解の促進を図ります。

【到達目標】

1. 標的型サイバー攻撃の疑いがある場合の調査・対処方法を習得します。
2. 標的型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

役員・教職員・学生一人ひとりがサイバー攻撃の脅威を理解し、防御の手立てを浸透させるための組織的な仕組みづくり及びインシデント発生時・事後の具体的な対応策を考察します。

【プログラム内容】

1. 情報セキュリティ対策のための組織的施策

全体会の「ベンチマークリストの評価結果と改善に向けて取り組むべき対策・対応」をもとに参加大学の現状を踏まえ、情報セキュリティ対策で何をなすべきか具体的な施策を探求します。

また、サイバー攻撃の脅威に対する組織的な仕組みとして、被害に遭わないための手立て「予防」、インシデント発生時には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に必要な組織体制について考察します。

2. 情報セキュリティを学内に周知徹底するための対策

情報セキュリティ対策の実施においては、情報や情報システムの取り扱いに関する法律として、例えば、サイバー犯罪を取り締まるための法律、プライバシー・個人情報を扱う事業者規制のための法律などがあります。組織的対応として、関連法令を遵守するための規程・ガイドラインの見直し及びその効果的な周知方法について考察します。

【到達目標】

1. 学内でのインシデント対応組織の構築・取り組みについて理解できるようになります。
2. セキュリティ対策を学内へ周知徹底するために必要な視点及び方法を提供できるようになります。

(4) 総合演習

2つのコース受講者が協働して実践的な演習ストーリーによるインシデントレスポンスと事後対策・対応の模擬演習を行うとともに、大学におけるセキュリティ向上のための組織対応の在り方及び取り組みについて考察します。

【プログラム内容】

1. 個人情報流出インシデント対応演習

外部機関から不正通信の通知を受けた例題をベースに手順を遂行(体験)します。なお、関係者への連絡・報告、社会への公表、規程の見直し、防止策(現状対応環境の確認と問題点)など対応の可否や優先順位について整理します。

2. サイバー攻撃防御の組織化に向けた戦略の考察

経営執行部を中心として防御意識を高め持続するための体制・取り組み課題、セキュリティ対策システム・規程等の見直し、セキュリティ対策予算の計上、構成員全員に向けた防御対策の取り組みを具体的な問題を挙げながら考察します。

【到達目標】

1. サイバー攻撃に対する大学部門間での協働体制を理解できます。
2. 全学で情報セキュリティ対策意識を醸成し、社会的責任を果すための体制・取り組みの方向性を理解できます。

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(金)

参加費の支払い：参加費は、8月19日(金)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「sec28」の記号を追記願います。
- * キャンセルの場合は、8月19日(金)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、ご確認くださいませよう願います。
 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23日(火)

全体会 [南3-301教室]			
10:30	開会挨拶 宮川 裕之 氏(青山学院大学情報メディアセンター所長) 「サイバー攻撃の最新動向について」 満永 拓邦 氏(東京大学情報学環特任准教授) 「経営執行部(役員)の情報セキュリティに対する取組みについて」 宮川 裕之 氏(青山学院大学情報メディアセンター所長) 「大学情報セキュリティベンチマークリストの紹介と評価方法」 井端 正臣 氏(公益社団法人私立大学情報教育協会事務局長) 「ベンチマークリストの評価結果と改善に向けて取組むべき対応」 満永 拓邦 氏(東京大学情報学環特任准教授)		
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	標的型サイバー攻撃による情報窃取 標的型サイバー攻撃のインシデントレスポンス演習	13:00	情報セキュリティ対策のための組織的施策 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24日(水)

総合演習 [南3-401教室]	
9:30	個人情報流出インシデント対応演習 ①
12:00 昼食	
13:00	個人情報流出インシデント対応演習 ② サイバー攻撃防御の組織化に向けた戦略の考察
16:30	

平成28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

