公益社団法人 私立大学情報教育協会

2019 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/sec2019/

日程：令和元年８月２９日(木)・３０日(金)

会場：立正大学品川キャンパス（東京都品川区）

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、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。文部科学省においても「大学等におけるサイバーセキュリティ対策等の強化について（通知)」が行われ、一歩踏み込んだ対策としてサイバーセキュリティ対策など組織・体制の整備、情報セキュリティポリシー及び実施手順書の策定が求められています。

そこで本協会では、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必要なことから、防御行動が組織的に進展するように、CISO（最高情報セキュリティ責任者）を含む経営執行部による対応、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リストを用いた自己点検・評価・改善を通じて、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

１日目の「全体会」では、大学におけるサイバー攻撃の最新動向、大学における情報セキュリティインシデントとその対応事例、ベンチマークリストにもとづく大学の対応、セキュリティポリシーなど学内ルールの周知徹底、構成員一人ひとりの防御行動の促進を共有し、対策を考察します。

２日目は、２つのコースに分かれます。一つは、セキュリティ関係の知識・技能の獲得を目指して演習を交えながら習得する「セキュリティインシデント分析コース」、二つは、リスクに応じた最適な情報セキュリティ対策と構成員全員及び情報センター等部門で注意喚起を呼びかける防御対策について認識を共有し、大学の実状に対応策を考察する「セキュリティ政策・運営コース」で、参加者の希望に応じた研究講習を行います。

３．研究講習会の内容

（１）全体会（１日目 10:30-17:00）

１．「情報セキュリティ１０大脅威 2019」
　　渡邉 祥樹 氏（独立行政法人情報処理推進機構セキュリティセンター）

２．「大学等におけるサイバーセキュリティ対策について」
　　下地 邦寿 氏（文部科学省大臣官房政策課ｻｲﾊﾞｰｾｷｭﾘﾃｨ・情報化推進室ｻｲﾊﾞｰｾｷｭﾘﾃｨ係長）

３．「サイバー攻撃によるリスクと大学等で発生したインシデントの振り返り」
　　洞田 慎一 氏（JPCERT コーディネーションセンター早期警戒グループマネージャー）

４．「ベンチマークリスト結果に見るセキュリティ課題」
　　宮川 裕之 氏（青山学院大学社会情報学部長、情報セキュリティ研究講習会委員長）

５．「学内ルールの周知徹底の取組み対策」
　　武藏 泰雄 氏（熊本大学総合情報統括センター情報セキュリティ室長、教授）

６．構成員一人ひとりの防御行動を促進する対応策
　　※　セキュリティポリシー及び情報関連規程を整備しても、構成員一人ひとりが自分の問題として捉え・防御行動に結び付けることが難しいことから、システム化することで意識付けを促進する全学的な取組みを考察

（２）セキュリティインシデント分析コース（２日目 9:30-16:30）

情報センター等部門の技術者が習得しておくべきセキュリティ関係の知識・技能として、サイバー攻撃の実態や仕組みを、サイバーレンジ（サイバー攻撃および防御の訓練を行うための仮想的な環境）での演習を通じて体感します。さらに攻撃予兆および痕跡の解析等、インシデント発生時の対応方法について演習を行います。

【プログラム内容】

１．サイバー攻撃および防御についての基本的知識と演習

※　サイバー攻撃の手法

※　サイバー攻撃の検知

※　痕跡調査

２．インシデント対応演習

※　ログ解析とインシデント報告書の作成

※　技術的対策の立案

３．サイバー攻撃への対策

※　疑似侵入テストによるシステム脆弱性の点検と対策

【到達目標】

１．サイバー攻撃で用いられる手法や防御の体験を通して、対処方法を身に付けることができます。

２．サイバー攻撃への事前の備えができるようになります。

３．自組織のシステム的脆弱性の発見方法を提案できるようになります。

（３）セキュリティ政策・運営コース（２日目 9:30-16:30）

情報セキュリティシステムの防御を効果的に進める方法として、情報の重要度に応じた階層的な対応をすることが必要です。そのために、教職員・学生・関係企業などに危機管理意識を醸成して自律的な防御行動の実質化を図るために、学内の関連規程や対応体制の整備及び教育・訓練や点検・監査の実施、情報関連システムを活用した対策について、具体的な企画・立案の演習をとおして理解を深めます。

【プログラム内容】

１．構成員一人ひとりの防御行動を促進する対応策

※　アイディアを精査して、グループ内で絞り込み、具体的に実施するための企画

２．守るべき情報資産の把握及びそれに基づいたバランスのとれたセキュリティ対策

※　重要な情報資産の把握を実施している事例を参考に、法人として情報リスクの分析・評価について現状を検証して、その課題を挙げ、それに基づいて情報資産の重要度に応じた組織としての最大の効果を得られるバランスのとれた情報セキュリティ対策を立案

３．セキュリティ対策としての攻撃に対する防御対策の注意喚起

※　攻撃に対する防御対策の注意喚起を実施している事例を参考に、具体的な注意喚起の方法とその効果についての提案

【到達目標】

１．構成員一人ひとりの防護行動を促す対応策について提案できるようになります。

２．リスク分析と情報資産台帳の必要性について説明できるようになり、守るべき情報資産に対するセキュリティ対策の重要性・優先順位を提案できるようになります。

３．攻撃に対する防御対策の注意喚起の方策と効果について提案できるようになります。

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 24 日(土)

参加費の支払い：参加費は、8 月 26 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「sec19」の記号を追記願います。
　＊ キャンセルの場合は、8 月 26 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29日(木)

10:30	1.「情報セキュリティ10大脅威 2019」 渡邉 祥樹 氏(独立行政法人情報処理推進機構セキュリティセンター) 2.「大学等におけるサイバーセキュリティ対策について」 下地 邦寿 氏(文部科学省大臣官房政策課サイバーセキュリティ・情報化推進室サイバーセキュリティ係長)
12:00	昼食
13:00	3.「サイバー攻撃によるリスクと大学等で発生したインシデントの振り返り」 洞田 慎一 氏(JPCERTコーディネーションセンター早期警戒グループマネージャー) 4.「ベンチマークリスト結果に見るセキュリティ課題」 宮川 裕之 氏(青山学院大学社会情報学部長、情報セキュリティ研究講習会委員長) 5.「学内ルールの周知徹底の取組み対策」 武藏 泰雄 氏(熊本大学総合情報統括センター情報セキュリティ室長、教授) 6. 構成員一人ひとりの防御行動を促進する対応策
17:00	

8月30日(金)

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	
9:30	1. サイバー攻撃および防御についての基本的知識と演習 ・サイバー攻撃の手法 ・サイバー攻撃の検知 ・痕跡調査	9:30	1. 構成員一人ひとりの防護行動を促進する対応策 グループワーク: 具体的に実施するための企画 2. 守るべき情報資産の把握及びそれに基づいたバランスのとれたセキュリティ対策(その1) 事例紹介 グループワーク: ・ 情報リスクの分析・評価について現状を検証 ・ 課題分析、課題解決のアイディアと効果の検討 ・ 実施方法の検討 ・ 情報資産の重要度に応じた情報セキュリティ対策を立案
12:15	昼食		
13:15	2. インシデント対応演習 ・ ログ解析とインシデント報告書の作成 ・ 技術的対策の立案 3. サイバー攻撃への対策 ・ 疑似侵入テストによるシステム脆弱性の点検と対策	12:30	2. 守るべき情報資産の把握及びそれに基づいたバランスのとれたセキュリティ対策(その2) グループワーク: ・ 情報資産の重要度に応じた情報セキュリティ対策を立案 3. セキュリティ対策としての攻撃に対する防御対策の注意喚起事例紹介 グループワーク: ・ 現状の課題認識、課題解決のアイディアと効果の検討 ・ 実施方法の検討 ・ 注意喚起の方法とその効果についての提案
15:40	研修の振返り・アクションプランの作成(2コース合同)		
16:30			

2019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