公益社団法人 私立大学情報教育協会

平成３０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/sec2018/

日程：平成３０年８月２３日(木)・２４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、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リストを用いた自己点検・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

１日目は、大学における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セキュリティ対応状況、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を共有する「全体会」を通じて、情報セキュリティリスクの確認を行います。また、情報セキュリティインシデントの事例を踏まえて予防と対応手順について研修・啓発の仕組み及び訓練計画を考えます。

２日目は、最初２つのコースに分かれます。一つは、サイバー攻撃の基本的知識や対策につい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、情報セキュリティの整備計画及び CISO の設置に向けた対策を考える「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。その上で、最後の全体演習では、コースをまとめてセキュリティ課題の解決に向けた計画・提言を行います

３．研究講習会の内容

（１）全体会１「サイバー攻撃の最新動向と対策」

サイバー攻撃の最新動向、大学情報セキュリティベンチマークリスト結果を踏まえた課題、実際に体験したインシデントとその後の対応事例を踏まえて、情報セキュリティリスクの実感を共有します。

１．「サイバー攻撃の最新動向から見る大学の新たなリスク」
　　洞田 慎一 氏（JPCERT ｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ早期警戒グループマネージャー）
２．「ベンチマークリスト結果に見る私立大学のセキュリティ課題」
　　宮川 裕之 氏（青山学院大学社会情報学部教授）
３．「大阪大学において発生した不正アクセス事案について」
　　尾上 孝雄 氏（大阪大学最高情報セキュリティ責任者、副学長）
４．情報セキュリティリスクの確認

（２）全体会２「情報セキュリティインシデント事例から研修・啓発の仕組みを考える」

実際に経験した大学の事例をもとに、情報セキュリティインシデント対応の事前予防や事後対応に必要な手順を理解し、大学構成員全員を対象とした研修・啓発の視点について検討します。

- 情報セキュリティインシデント事例を踏まえた事前予防と事後対応手順の紹介
- グループワーク：大学構成員全員を対象とした予防と対応手順を研修・啓発する仕組み
- 標的型攻撃メール対策の訓練事例を紹介　高橋智広氏（早稲田大学情報企画課長）
- グループワーク：大学構成員全員を対象とした標的型攻撃ﾒｰﾙに対する研修・訓練計画の作成

（３）セキュリティインシデント分析コース

標的型攻撃メールを用いたサイバー攻撃の実態や仕組みを確認し、その具体的な手口や影響範囲について演習を通じて体感します。また、痕跡調査を行うための事前準備や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。さらに重要な情報資産の保護に向けた技術的な対策を紹介します。

【プログラム内容】

１．サイバー攻撃の基本的知識と最新動向の理解
- 標的型攻撃メールによるサイバー攻撃の手口と仕組み
- 痕跡調査を行うための事前の備え

２．サイバー攻撃によるインシデントへの対応演習と対策
- 痕跡調査とインシデント対応演習
- 情報保護のための技術的な対策

【到達目標】

１．サイバー攻撃を受けた場合の対処方法・手順を体得できます。
２．サイバー攻撃への事前の備えや情報保護について理解できるようになります。

（４）セキュリティ政策・運営コース

情報セキュリティは、一部の担当組織だけでは対応できるものではなく、経営執行部による組織的な対応と構成員一人ひとりによる注意と行動が必要です。それには、情報セキュリティポリシーに基づいた実効性のあるセキュリティ対策基準や対策手順を作成し、自己点検・評価・改善を習慣化していくことが重要になります。

本セッションは、自己点検・評価・改善に先進的に取り組んでいるベンチマークを参考に自大学の整備計画を振り返ります。また、組織的に迅速な対応ができるように CISO（最高情報セキュリティ責任者）の設置と強化対策を考察し、情報管理者として理解しておくべき法的知識とその対応について理解を深めます。

【プログラム内容】

１．ベンチマークリストで先進的取組みをしている大学を参考に整備計画を考える
① 情報セキュリティポリシーと対策基準の策定
② 情報セキュリティルールの周知徹底
③ 情報資産の把握とリスク対策
など

２．CISO の設置と強化対策
・CISO の役割と権限の紹介
・グループワーク：CISO の重要性を確認し、設置に向けた対策を考える

３．情報管理者に求められる法的知識とその対応
改正個人情報保護法、不正アクセス禁止法、著作権保護法、GDPR（EU 一般データ保護規則）など
市川 昌 氏（江戸川大学名誉教授）

【到達目標】

１．情報セキュリティ整備計画を立案できるようになります。
２．情報セキュリティの研修計画を提案できるようになります。
３．組織的に迅速な対応を行う CISO の設置について重要性を説明できるようになります。

（５）全体演習「セキュリティ課題の解決に向けた計画・提言」

経営陣に理解と行動を促す一つの手段として、情報セキュリティに関する研修・啓発の必要性と実施計画の提案、自大学の課題解決に向けた情報セキュリティの整備計画を考察します。

【プログラム内容】
- 経営陣に向けた提言（研修・啓発の必要性、整備計画）
- 自大学のセキュリティ課題の解決計画を作成

【到達目標】
- 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 18 日(土)

参加費の支払い：参加費は、8 月 20 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「sec30」の記号を追記願います。
＊ キャンセルの場合は、8 月 20 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23日(木)

全 体 会 1 ［南3－301教室］

10:30

「サイバー攻撃の最新動向と対策」

1.「サイバー攻撃の最新動向から見る大学の新たなリスク」
　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)
2.「ベンチマークリスト結果に見る私立大学のセキュリティ課題」
　宮川 裕之 氏(青山学院大学社会情報学部教授)
3.「大阪大学において発生した不正アクセス事案について」
　尾上 孝雄 氏(大阪大学最高情報セキュリティ責任者、副学長)
4. 情報セキュリティのリスクの確認

12:15　昼食

全 体 会 2 ［南3－401教室］

13:15

研究講習会の進め方

「情報セキュリティインシデント事例から研修・啓発の仕組みを考える」

・ 情報セキュリティインシデント事例を踏まえた事前予防と事後対応手順の紹介
・ グループワーク：大学構成員全員を対象とした予防と対応手順を研修・啓発する仕組み
・ 標的型攻撃メール対策の訓練事例を紹介　高橋智広氏(早稲田大学情報企画課)
・ グループワーク：大学構成員全員を対象とした標的型攻撃メールに対する研修・訓練計画の作成

16:30

8月24日(金)

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］	
9:30	**サイバー攻撃の基本的知識と最新動向の理解** ・ 標的型攻撃メールによるサイバー攻撃の手口と仕組み ・ 痕跡調査を行うための事前の備え	9:30	**ベンチマークリストで先進的取組みをしている大学を参考に整備計画を考える** ① 情報セキュリティポリシーと対策基準の策定 ② 情報セキュリティルールの周知徹底 ③ 情報資産の把握とリスク対策 など
11:30	昼食		
12:30	**サイバー攻撃によるインシデントへの対応演習と対策** ・ 痕跡調査とインシデント対応演習 ・ 情報保護のための技術的な対策	12:30	**CISO(最高情報セキュリティ責任者)の設置と強化対策** ・ CISOの役割と権限の紹介 ・ グループワーク：CISOの重要性を確認し、設置に向けた対策を考える **情報管理者に求められる法的知識とその対応** 改正個人情報保護法、不正アクセス禁止法、著作権保護法、GDPR(EU一般データ保護規則)など 市川 昌 氏(江戸川大学名誉教授)
14:00	休憩		

全体演習 ［南3－401教室］

14:30

「セキュリティ課題の解決に向けた計画・提言」

・ 経営陣に向けた提言(研修・啓発の必要性、整備計画)

・ 自大学のセキュリティ課題の解決計画を作成

16:30

平成30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