公益社団法人私立大学情報教育協会
平成 28 年度第 2 回情報セキュリティ研究講習会運営委員会議事記録

Ⅰ．日　時：平成 28 年 5 月 19 日(木)　15：00 から 17：00
Ⅱ．場　所：私立大学情報教育協会 事務局会議室
Ⅲ．参加者：浜委員長、入澤委員、根本委員、服部委員、西松委員、柴田委員、市川ｱﾄﾞﾊﾞｲｻﾞ
（Skype）佐久間委員、岡部委員
（事務局）井端事務局長、野本（記）

Ⅳ．検討事項
８月の大学情報セキュリティ研究講習会について、開催要項策定に向けて基本方針の確認及び全体会、各コース、総合演習などについて以下のような意見交換が行われた。

（１）開催場所
・　８月２３日、２４日の２日間で学習院大学を会場に開催することにした。

（２）研究講習会の目的
・　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働きかけるため、ベンチマークによる情報セキュリティについて課題の洗い出しを行い、自己点検・評価を習慣化する中で段階的なセキュリティ対策・体制や課題を探求するとこが確認された。

（３）全体会について
・　全体会の目標として、「防御意識の徹底などの点検項目についてベンチマークを用いて振り返る重要性の認識を共有する。」、「振り返るための評価指標をどのように決定するのか、松竹梅のモデルレベルを提示し、理解の共有を図る。」ことが確認された。
・　プログラム構成として、①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、②ベンチマークの紹介と評価方法、③評価結果と関連情報を含めた対応策モデルが検討された。
・　経営執行部に求められるガイドラインの表現は厳しいと思われ、中身がわか形での提示が良いのではないか。例えば、サイバーセキュリティ経営ガイドライン（経済産業省、ＩＰＡ）の経営者が認識する必要がある「３原則」など参考にしてはどうか、経営やトップといった言葉が入った方が分かりやすいのではないか。
・　ベンチマークについては、「大学セキュリティ運用ベンチマークテスト」の昨年設定した名称を使用する。ベンチマークは理事長学長等会議でも紹介することを検討する。
・　評価分析はカテゴリに分けるなどできないだろうか。対応策モデルとして提示ができないか。例えば、昨今課題になっている不正通信関連への対応を過去の資料を集約してレベル分けなどして提示ができないか。

（４）総合演習について
・　不正通信（C&C サーバからの通信）が外部から指摘があったことへの対応をシミュレート、ディスカッション含めて経営、管理、技術者の立場での演習を考えている。初動対応を今ま

で研修してきたが、事後対応までを対応することを考えたい。体制の優劣２校で Skype での対処デモンストレーションからベンチマークに準拠した体制の必要性を理解させてはどうか。シミュレーション形式での演習を考えることにした。

- 初動対応は基本の形にして、その後の対応部分を深めることを考えてはどうか。
- 担当者任せて収束させるケースもあり、その体制についての指摘をする必要があるのではないか。
- 情報共有の対応は、委員の中で試行して結果を紹介することを考えている。
- インシデントに対する罰則など規程に見直しなどの範囲も考えるべきではないか。法的な問題などマネジメントコースでの紹介も考えてはどうか。

（５）マネジメントコースについて

- インシデントの対応について対処の全体像（一連の流れ）を理解させ、具体的なケースを掘り下げて対処についてディスカッションさせてはどうか。対応のソリューションも紹介してはどうか。
- １日目として知識を身に付ける、共有の時間としてはどうか。
- マネジメントの名称は、講習内容と参加者の認識に乖離があるよう、大学経営に受け取られるなど感じたことから、コース名は「セキュリティ政策・運営コース」とすることにした。
- 前半で知識の共有を図り（40 分程度）、後半で 2 件程度のディスカッションの進行を考えている。参加者が自分たちの問題として考える場として設定すべきではないか。
- 経営層がしなければならない対応の理解を図る、防御を含めた経営層への投げかける戦略を情報交換してはどうか。
- 防御意識を周知徹底するためのディスカッションが必要ではないか。（２コースそれぞれで含める必要があるか）インシデントが起きる前の対応についても考える必要があるのではないか。予防、ガバナンス対応、インシデント対応の順番で構成してはどうか。
- インシデントはどこにでも起こりうる問題である、情報関係者だけの問題ではないことが訴求出来ればよいのではないか。大学構成員の意識をどのようにリスクを認識してもらうのか、教員個人は大学のリスクとしては認識していない現状があるのではないか。

（６）テクニカルコースについて

- コース名は「セキュリティインシデント分析コース」とすることにした。
- 総合演習のためのどのようなテクニックが必要なのか知識を身に付けさせる。
- マルウェアの動作及び感染するとどのようになるのか理解を共有する。
- 不審な通信をどのように見ていくのか理解を図る。
- 総合演習へのつなぎとなる演習を考えたい。

Ｖ．次回のスケジュール

- 次回の委員会は、５月３０日に開催し、開催要項を検討することにしている。