

## 公益社団法人私立大学情報教育協会

### 平成 27 年度第 2 回情報セキュリティ対策問題研究小委員会議事記録

- I. 日 時：平成 27 年 7 月 13 日(月) 18:00 から 20:00
- II. 場 所：私立大学情報教育協会 事務局会議室
- III. 参加者：浜主査、佐々木委員、高倉アドバイザー、松坂アドバイザー、  
トレンドマイクロ、日本電気  
(事務局) 井端事務局長、野本 (記)

#### IV. 検討事項

##### 1. 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

サイバー攻撃など情報セキュリティの問題は、社会・経済全体に波及する可能性があることから、大学・法人が意識を共有して組織的に取り組む必要がある。そこで、大学法人全体で問題意識の共有化、学内ルールの確立、教職員に対する教育・訓練、運営体制などマネジメントを遂行する役割・責任の範囲・内容に関して経営執行部として役員のリーダーシップが極めて重要となっていることから取り組みについて整理を進めた。

- ・ 緊急時の対策、守るべきものの設定、保護・監視するシステム・委託・費用、組織をつくっておくことなどの意見があった。
- ・ 緊急の暫定措置のイメージは、端末を切断、スイッチ・セグメントの切断など一旦機器の電源を切る判断をし、その後に検討する必要がある。切断することを全学的に周知が求められる。
- ・ パソコンやサーバ以外の機器もネットワークにつながっており、それが正しく保護されているのかを徹底する必要がある。
- ・ セキュリティポリシーや体制が重要で、実際に運用されているか課題ではないか。
- ・ 事故の賠償・損害を想定すると対策コスト比較では優位性が出ない判断も考えられる。
- ・ 危機意識を共有化する必要性を最初にうたえかける必要があるのではないかと。教職員一人ひとりの問題として、例えば就業規則などで定義する必要があるのではないかと。メンバーなどの個人情報や研究資産など攻撃の可能性がある。
- ・ 危機意識を浸透させるためのチェックリストが必要ではないかと。例えば項目として、危機意識を教職員にどのように伝えているか、研修会などを実施しているか、インシデント例を共有しているか、攻撃の備えをしているか、自分のこととして意識しているか、対策費用にどの程度かけられるのかなど考えられないか。

##### 2. 情報セキュリティの自己点検リストについて

情報セキュリティ対策についての自己点検ができるようなベンチマークテストが提示され、講習会での利用を想定して検討された。

- ・ 項目は、ポリシー・規程の整備、対策推進体制、情報資産の棚卸、管理・保管、教育、入室制限、安全設置、不正なアクセス・プログラムへの対策、暗号化などの保護、記録媒体の

取り扱い、利用者識別・認証、アクセス制御、システム障害・停止を想定した対策、事件・事故を想定した備えなどが考えられる。

- 大学の状況把握として、規模、システム依存度、システム停止の影響、漏洩など事故の影響度、事故の有無などが考えられる。
- 実際にベンチマークテストとしての項目にアンケート的な内容も含めて集計できる形で大学での比較も考えられるのではないか。
- セキュリティ対策体制として、チーム作りの基準や参考となるものはあるのか。インシデントの内容や判断においてどのレベルを経営層まで報告するのかなど情報の流れのコントロールなど考慮する必要があるのではないか。

#### V. 次回のスケジュール

- 「経営執行部の情報セキュリティに対する取り組み」「情報セキュリティのベンチマークテスト」について更新内容をメールで確認し、講習会運営委員で検討した上で8月25,26日の講習会で利用することになっている。