公益社団法人私立大学情報教育協会
平成 27 年度第 1 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 6 月 25 日(木)　17：00 から 19：00
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、松坂アドバイザ、
　　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．本小委員会で検討すべき内容について
　情報資産や金融資産に対するサイバー攻撃の脅威を周知し、防御意識に基づく行動が組織的に展開されるよう働きかけの戦略を研究・協議する。具体的には、サイバー攻撃の被害を受けた大学の対応事例のデータ化、大学執行部の関与の在り方、情報資産や金融資産に対する防御の自己点検・評価の仕組み、本協会による外部診断の必要性・可能性について研究することにしており、以下の項目が提示された。
（1）サイバー攻撃の脅威について法人・大学としての受け止め方を整理し、関心を喚起する。
（2）サイバー攻撃の被害を受けた事例及び対応をデータ化し、最新情報を共有できるようにする。
（3）大学執行部として関与すべき範囲と権限を整理し、モデルを提示・改善を呼びかける。
（4）情報資産や金融資産に対する防御の自己点検・評価の仕組み。
（5）本協会による外部診断の必要性・可能性。
・　テクニカル面ではなくガバナンス中心の取組みや情報などを大学に届けることを目指す。例えば、メールの添付ファイルの開封抑止の徹底など。

２．委員の意見
・　情報を流しても現場で上手に運用されない可能性がある。制度や仕組みを優先した方が良いのではないか。
・　理事長学長等会議などガバナンスに対する訴求により関心を高めるため、ガバナンスに提示する素材が必要ではないか。
・　大学として知っておくべきレベルのとりまとめ、大学の特長を考慮した攻撃への注意など、インシデント発生時には、コスト、被害、執行部の対処など課題になり、対策予算が見込めるのか、被害後の時間経過で風化してしまわないか問題点が考えられる。
・　意識を高めるため、踏み台になっている可能性など総点検する必要があるのではないか。
・　メールの問題では、現実的には学生から来るメールなど、添付を開封しなくてはならないことがある。また、一企業では半年で 100 件以上の感染する疑いのあるものがあり、その後の初動が重要になっている。
・　ネットワークや機器で対策する方法も考えられるが、プロキシチェックでログを持たせるのもディスク容量のコストがかかる、自治体では外向けと内向けでネットワークを分けている、大学でも VLAN でネットワークを分けて感染してもセグメントを分離する行動がとれる

が、いずれも費用が大きいことが想定される。

- 標的型攻撃をイメージして、対策予算の例を松竹梅で３つ程度、対処する機器・運用面とコストのバランスで提示できないか。文科省から助成金があれば予算化しやすいと思われる。
- リスクマネジメントの重要性を執行部で共有するためのガイドラインをどのような範囲、役割、責任、権限などを含めて執行部の取組みについて作成してはどうか。
- 現状は被害にあっていないのか本当に大丈夫なのか、確認するための自己点検ツールと発見された時の対応マニュアルが必要ではないか。
- セキュリティ対策とサーバー攻撃対策について、本来どのようにあるべきかなのかチェックリストを作成してはどうか、３０分程度で自己点検の調査ができ、点数化されるもの。どのようなリスクが考えられるのか、点数化で大学による相対的な比較が可能になるのではないか。講習会では５分程度で評価できる自己点検のチェックリストを利用してはどうか。

Ⅴ．次回のスケジュール

- 次回の小委員会では、７月１３日の１８時から開催し、「経営執行部の情報セキュリティに対する取組み」、「情報セキュリティの自己点検リスト」について、研究講習会で討議資料として利用するための検討をすることにしております。