特集　情報セキュリテイ

私立大学における
情報セキュリティ対策強化のための取り組み手順

情報セキュリティ対策強化取り組み手順検討の必要性

平成28年12月26日付けの「私立大学等を設置する学校法人等における情報セキュリティ対策の強化について（通知）」が、私学部長から発出されました。

それによりますと、「個人情報を含む多くの情報に、万が一情報セキュリティインシデントが発生した場合、私立大学の学校法人の信用失墜を招くだけでなく、多くの関係者に多大な影響を及ぼすことになります。公共性の高い学校法人において、情報セキュリティ対策は社会的に求められるものであり、経営上の重要課題となっています。ついては、セキュリティポリシーの策定やその運用状況の確認など、情報システムからの漏えい等を防止するための対策に漏れがないかの点検を改めて実施するとともに、情報セキュリティに関する体制や規定の整備等、情報セキュリティの対策強化に努めていただくよう改めてお願いします。」として、「セキュリティポリシーを未策定の法人は、早急に策定を行うこと。また、セキュリティポリシーを策定済みの法人においても最新のセキュリティ脅威や脆弱性、環境の変化等を意識して、必要に応じて改訂を行うことが望まれること。各法人において取り扱う情報に応じて適切な情報セキュリティ対策を実施すること。」が法人に要請されました。

そこで、情報システム上のセキュリティ対策の問題点を点検し、改善に向けた取り組みの強化が大学法人全体に要請されていることに鑑み、本協会では、平成29年７月に「情報セキュリティ対策問題研究小委員会」において、早急に対応していくための手順について検討し、以下の通り、対応手順の要素を例示することにしました。

手順１．情報セキュリティの自己点検・評価

本協会が作成した「情報セキュリティベンチマークリスト」で課題の洗い出しを行い、情報セキュリティのリスクを評価する。

手順２．情報セキュリティリスクに基づく改善計画の策定

以下に例示する情報セキュリティ対策を計画的に進めるため、各大学で優先順位に沿って予算措置を行い、組織体制、責任範囲の明確化、権限の設定などの見直しを踏まえて、改善計画を策定する必要がある。

＜情報セキュリティ施策の例＞

- 経営執行部による危機意識の共有
- 情報セキュリティポリシーや情報セキュリティ管理に関する規程(実施規程、実施手順)などの策定・充実と周知徹底(教育・訓練を含む)
- 重要な情報資産の把握とリスク回避のための対策
- サイバー攻撃に対する防御対策(組織的・人的対策、技術的・物理的対策)
- セキュリティ事件・事故に緊急対応する組織体制と対応手順
- 情報セキュリティ被害情報の文部科学省への業務連絡及び内閣府外局の個人情報保護委員会への報告体制

手順３．改善計画の遂行と実施状況の確認

改善計画を策定しても計画倒れになることが予想されることから、計画が確実に進むことを確認する仕組みを設ける必要がある。

その際、組織レベルによる実施状況の確認としては、例えば、事務部門であれば情報センター等部門が中心となって情報セキュリティに関する対策活動の進捗状況を聞き出す場を年に数回設けるなどの方法が考えられる。教員組織であれば学部の教授会または全学教授会で対策活動の進捗状況を報告する機会を年に数回設けることが考えられる。

構成員レベルであれば、対策状況の確認を学内ポータル画面で強制的に数ヶ月に１回程度の割合で確認を行い、注意喚起を定着させるなどの工夫が考えられる。