1－2 情報環境に関する研究

教育研究活動の基盤となる情報の管理政策、運用対策、管理技術の点検・評価の判断指標をポートフォリオとして構築し、対応が不十分な場合の行動指針を紹介するセキュリティ支援システムを研究するため、情報セキュリティ研究講習会運営委員会（奥山徹委員長、朝日大学）にて対応することになった。同運営委員会は本来の活動である研究講習会の運営と併せて活動したため、研究事業への対応は１０月からとなった。以下に研究活動を報告する。

（1）セキュリティ支援システム作成の経緯

本協会では、教育の情報化の進展に伴い、大学に修学指導、経営戦略、自己点検・評価、教育研究資料等に関する貴重な情報資産が蓄積され、その有効活用が大学の教育・研究活動、経営活動の成否に大きく影響することに鑑み、大学資産としての情報管理の問題が大きな課題となっていくと判断し、情報の管理・運用政策及び管理・運用体制、管理・運用技術について理解を呼び掛けるため、数年前より「大学情報セキュリティ研究講習会」を設置して、研究討議を続けてきた。多くの大学は、ウイルス対策、ファイヤーウオール対策、迷惑メール対策、利用者認証など、技術的なセキュリティを中心に整備してきたが、情報資産の重み付け、リスク対策を踏まえた情報の重要性に応じた情報資産のセキュリティ対策が進んでいない。また、セキュリティの基本方針・対策・実施に亘るセキュリティポリシーの策定についても、未整備な大学が７割近くあることが判明した。そのような中でセキュリティ対策が進んでいると大学と不十分な大学の格差が開いている状況が見受けられることから、大学の対応能力に応じたセキュリティ対策が進展するよう、自己点検、自己評価のチェックリストを作成し、ポートフォリオ化して、取組むべき行動計画の在り方、対応内容をWebサイトで支援できるようにシステムを構築することにした。

（2）セキュリティ対策チェックリストの作成

チェックリスト作成の目的は、上記の経緯から大学が情報セキュリティに対してガバナンス機能を発揮し、組織的に対策を講じることの重要性を理解し、情報セキュリティ対策の弱点を検証し、改善に結びつけられるように支援するための手段であることを確認した。そのため、点検項目は、必要最小限とし、大学関係者に「気付きを与える」ような内容で以下の通りチェックリストの項目を構成した。

チェックリストの枠組みについては、「情報資産の把握」、「組織的対応」、「人的対応」、「技術的対応」の４つの視点から、以下のような方針で項目を整理した。なお、施設設備の障害など物理的セキュリティの対応については、点検の取組みが他の枠組みと連携することから枠組みとしないで、技術的対応の項目として含めることにした。

① 情報資産の把握では、大学が保有する紙媒体を含む全ての情報を対象とし、情報の管理者、作成者、保存場所・方法、公開対象、重要度等を点検し、情報の資産目録（台帳）の整備を確認する。その上で、情報資産に対する脅威を分析し、セキュリティでの対応策を選択できるように点検項目を設定した。

② 組織的対応では、大学ガバナンスとしての取組みとして、セキュリティの問題を意思決定、企画・実行・評価・改善の面から組織的な対応が構築できるよう、体制、規程の取組みを中心に点検項目を設定した。

③ 人的対応では、専任教職員、非常勤教員、臨時職員、学生、関連業者を対象とする構成員の自覚を促すことを基本とし、その上で構成員として対処すべき機密保持、情報資産の利用及び引き継ぎ、事故対応などの行動指針、セキュリティ教育への参加促進を中心に点検項目を設定した。

④ 技術的対応では、上記での対応ができない部分を技術的に補完する取組み全てを取り上げることにしたが、コンピュータ、ネットワークを使用した電子情報の範囲とし、ファイヤーウオール、不正侵入検知等のシステム、学内ＬＡＮ、サーバー・クライアント、情報媒体の管理として点検項目を設定した。

（３）セキュリティ対策のチェックリストの確定

運営委員会では、点検項目の作成の原案を以下の通り２１年３月下旬にとりまとめた上で、４月上旬に「セキュリティ対策の自己点検・評価チェックリスト案」として、加盟校に対して意見を伺い、その結果を踏まえて最終的にチェックリスト項目を確定することにした。

情報セキュリティ対策の自己点検・評価について

１．情報セキュリティ対策チェックリスト作成の趣旨

私立大学情報教育協会では、セキュリティポリシーの必要性を啓発し、その作成手順を「提言　私立大学向けネットワークセキュリティポリシー」として公表するほか、情報の適正管理を図るために取り組むべき情報の運用管理政策、情報管理の点検・評価、ネットワークのセキュリティ技術について、政策、技術両面から知識・技能の啓発・開発を行ってきた。ところで、平成20年度私立大学情報環境基本調査(中間集計結果)によれば、「セキュリティポリシーを作成し、対策を実施している」大学は26%に留まっており、一日も早い改善が期待されている。一方、大学の多くの業務が情報機器やネットワークにより支えられるようになってきており、ひとたび情報セキュリティに対する事故が生じると、大学の運営そのものに支障が生じることとなり、教育・研究活動に大きな影響を及ぼす。そこで、本協会では、各大学が情報セキュリティに対してガバナンス機能を発揮し、組織的に対策を講じることが喫緊の課題と判断し、大学が常に自己点検・自己評価を通じて、改善を図ることができるようにするため、この度、情報セキュリティ対策のチェックリストを作成し、支援することとした。
このリストは、それぞれの大学における情報セキュリティ対策の弱点を検証し、改善に結びつけることはもちろんのこと、情報セキュリティガバナンスへの注意喚起として用いられることを期待している。

２．情報セキュリティ対策チェックリストの視点

チェックリストは、情報資産の把握、組織的対応、人的対応及び技術的対応の面から、以下のように整理した。

（１）情報資産の把握

情報セキュリティ対策では、その対象となる情報資産について把握することが重要である。大学が保有する情報資産の明確化と、その重要度が正しく認識されていることが必要である。情報資産が正しく把握できていないと、実際の情報セキュリティ対策を検討していく上で、リスク分析の対象範囲を絞り込むことができず、適切な対策が取れなくなることから、情報資産の把握について「目録作成」、「重要度」、「管理・運用」、「リスク分析・対応」をチェックポイントとして設定した。

情報資産とは、組織が保有するすべての情報(形態を問わず、紙媒体も含めたすべての情報)を対象とする。

情報資産の把握は、大学内の文書や書類を整理・分類し、情報の管理者、作成者、保存方法、情報の公開対象、重要度等を洗い出し、情報資産目録として整理する。その次の段階として、情報資産に対する脅威（リスク）を想定し、評価するリスク分析が必要である。この結果から、どのようなセキュリティ対策をとる必要があるかを選択することになる。なお、それらを保存・蓄積するためのハードウェアや処理のためのソフトウェアも情報資産として把握する必要がある。

（2）組織的対応

インシデントが発生しないと真剣に取り組まないのが通例である。しかし、障害が発生した時には被害の大小を問わず大学としての責任体制が大きく問われることになる。大学の財産は教育・研究であり、それらは情報として格納されている。大学は常に障害時に備えて、大学の対応力に応じた組織的な取り組みを構築しなければならない。そのようなことから、大学ガバナンスとしての取り組みとして教職員、学生の視点から「組織的な対応」をチェックポイントとして設定した。点検は、「体制」と「規程」を中心に考えた。

組織としての対応、個人としての対応があるが、これを実効あるものにするためには、セキュリティの問題を意思決定をはじめ、企画・実行・評価(監査)・改善の組織的な仕組みを構築しておくことが望まれる。その上で、大学構成員一人ひとりが問題意識を持って取り扱うことができるよう、共通理解を形成できるように申し合わせおよび規程などの整備、周知徹底などが必要である。

（3）人的対応

組織を動かすのは人である。人に対する情報セキュリティの点検は不可欠である。教員、職員、学生、その他の構成員へのセキュリティ教育、機密保持義務、情報の取り扱い、ネットワークの利用、情報機器の管理についての対応と責任について明らかにし、実現ができるようにすることが重要である。そのようなことから、規程の裏づけとして、個人の行動面での取り組みを「人的対応」としてチェックポイントを設定した。

「人的」の範囲は、教職員、学生のほかに、請負業者及び非常勤、臨時職員を含む構成員とする。個人の行動取り組み以前の問題として、セキュリティに対する問題意識を職務責任の中で明確にしておくことが基本である。その上で、セキュリティ教育、誓約書の提出、契約書の締結、法令・規程の遵守、機密保持の徹底、情報資産の管理、事故対応・報告義務等の点検が整備されていることが望まれる。

（4）技術的対応

技術的対応は、紙媒体から電子情報まで全ての情報資産を対象とするべきである

が、ここでは、コンピュータ・ネットワークを使用した電子情報の範囲に限定する。情報資産の入れ物としてのコンピュータや伝送路としてのネットワーク、情報資産の表現形式や処理の形態を決定するものとしてのソフトウェア、そして、一番重要な要素としてのデータ、これらすべての安全性を検証するため、「技術的対応」としてチェックポイントを設定した。

技術的対応は、組織・体制、規程、構成員の意識等で対応できない部分を技術的に補完するための取り組み全てを取り上げることにした。以下に掲げる取組みを網羅的に対応するには大学の対応能力によって異なる。したがって、各大学は守るべき情報資産の重要度に即して、最小限守るべき情報資産から技術的な取り組みを考えることが適切と思われる。技術的な取り組みの主な例を取り上げると、目的別には、ウィルス対策、ユーザ認証、バックアップ、サーバ・ネットワークの安全運用、不正侵入防止対策、暗号化・シンクライアント化、情報資産の入手・廃棄履歴の管理等が挙げられる。これらの目的を達成するためには、LAN、サーバ等の要素に基づいて点検することが効率的である。本協会では、点検項目の具体的な設定に当たってIPA(情報処理推進機構)等のガイドラインを参考とした。（詳細項目は資料編【資料７】を参照。）

３．チェックリストの項目

１．情報資産の把握
- （１）情報資産の目録作成
- （２）情報資産の重要度
- （３）情報資産の管理・運用
- （４）リスク分析・対応

２．組織的対応
- （１）意思決定
- （２）運用体制
- （３）監査体制
- （４）情報セキュリティポリシー
- （５）情報セキュリティポリシーの対策基準
- （６）情報セキュリティポリシーの実施手順

３．人的対応
- （１）職務責任
- （２）機密保持
- （３）情報の利用
- （４）罰則規定
- （５）情報資産の引継ぎ
- （６）情報セキュリティ教育
- （７）事故対応と報告義務

４．技術的対応
- （１）ファイアウォール
- （２）不正侵入検知・防御システム
- （３）学内ＬＡＮ
- （４）サーバ
- （５）クライアント
- （６）情報媒体の管理