# 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・物理的対応

技術的・物理的対応は、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・物理的対応」としてチェックポイントを設定した。

技術的・物理的対応は、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。以下に掲げる取り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。

# 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

- 情報資産の作成者、入手先が明確になっているか。
- 情報資産の管理部署・管理責任者は明確になっているか。
- 情報資産の保存場所･保存形態が明確になっているか。
- 情報資産の主な利用目的が記載されているか。
- 情報資産の公開対象が明確になっているか。

### (2)情報資産の重要度

- 情報資産の内容について組織的な重み付けがなされているか。
- 情報資産の重要度の指標について適切な基準が設定されているか。

### (3) 情報資産の管理・運用

- 情報資産の種類に応じて、物理的、電磁的アクセス権の設定がなされているか。
- 適切な時期に情報資産の棚卸しが行われており、変更の履歴が保存されているか。
- 情報資産の重要度に合わせて作成、保管、修正、廃棄、公開の手順が定められているか。

### (4) リスク分析・対応

- 情報資産のリスク評価基準が明確になっているか。
- リスク別にどのような対策をとるべきかの指針が整理されているか。

## 2．組織的対応

### (1)意思決定

- 経営責任の一部として、情報セキュリティの最高責任者を決めているか。
- 情報セキュリティに関して専門に検討する組織が設定されているか。
- 組織単位で情報セキュリティの責任者を決定しているか。

### (2)運用体制

- 組織単位で情報セキュリティに取り組む体制(企画、実行、評価・改善)が確保できているか。
- 情報セキュリティに関する学内外の障害・事故状況を的確に把握し、改善につなげているか。
- ソフトウェアのライセンス管理体制が確立されており、知的財産権を侵害していないか。

### (3)監査体制

- 意思決定の機能(報告・連絡・相談)が正常に働いているかを点検する仕組みがあるか。
- 意思決定内容が適切になされているか、学内外の専門家による評価の仕組みがあるか。
- 組織単位での情報セキュリティの実施状況を点検・評価し、改善する体制が確保できているか。
- 点検・評価は、実績データに基づき継続的に実施され、その結果がフィードバックされ改善に活かされているか。

### (4)情報セキュリティポリシー

- 情報セキュリティポリシーが策定できているか。
- 情報セキュリティポリシーには、「目的」、「基本方針」、「適用者」、「利用者の義務・責任」を定めているか。
- 情報セキュリティポリシーが公開され、学内関係者に周知徹底されているか。

### (5)情報セキュリティポリシーの対策基準

- 組織的セキュリティ、人的セキュリティ、技術的セキュリティ、物理的セキュリティについての遵守事項、PDCAサイクルを意識した運用が明確化されているか。
- 対策基準が公開され、学内関係者に周知徹底されているか。

学外関係者としての関連業者等に業務や情報システムの運用管理を委託する際、情報セキュリティポリシーに基づいた適切な契約がなされているか。

### (6)情報セキュリティポリシーの実施手順

- 対策基準で定められた内容が、各構成員の行動指針としてガイドライン化されているか。
- 組織単位で実施手順を点検・評価し、改善する仕組みができているか。
- 危機管理のための実施マニュアルを作成しているか。

## ３．人的対応

### (1)構成員の把握

- 大学の情報資産に接する教員、職員、学生、関連業者等、構成員の範囲を明確にしているか。

### (2)職務責任

- 構成員に対して、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いるか。

### (3)機密保持

- 構成員である間および構成員でなくなった後の機密保持の取り扱いを適切に定めているか。

### (4)情報の利用

- 各構成員が利用できる情報の所在と利用できる対象者が明確になっているか。
- 身分変更があった場合のアクセス権の設定・制限・緩和・削除が適切に行われているか。

### (5)罰則規定

- 構成員が情報セキュリティポリシーに違反した場合の罰則が規定されているか。

### (6)情報資産の引継ぎ

- 人事異動、休職、退職等に対応した情報資産の引継ぎが適切(明文化、報告等)になされているか。

### (7)情報セキュリティ教育

- 情報セキュリティポリシーに従った教育がすべての構成員（学長などの役職者を含む）に適切に実施されているか。
- 情報セキュリティ教育は定期的に実施され、参加を促す工夫がなされているか。
- 過去の事故事例を共有し、情報セキュリティ教育などに活用しているか

### (8)事故対応と報告義務

- 事故の連絡体制、事故処理の責任体制が確立されているか。
- 重大な事故が発生した場合、警察や報道関係への対応体制及びマニュアルが整備されているか。
- 事故対応に対するトレーニングを定期的に実施しているか。
- 情報資産の管理者及び利用者が情報セキュリティに関する問題点を発見した場合、疑わしい状況を察知した場合の緊急連絡先が周知されているか。

## ４．技術的・物理的対応

### (1)ファイアウォール

- ファイアウォールを導入し、ポリシーに基づきログ管理やパケットの状況を定期的に点検しているか。

### (2)不正侵入検知・防御システム

- 検知対象の情報を日々更新し、ログの保存・解析を行っているか。

### (3)学内LAN

- 組織が管理するネットワークを把握し、トラフィック監視を行っているか。
- 業務・研究・教育など用途ごとにネットワークを分離しているか。
- セキュリティ対策のなされていない無線LANのアクセスポイントはないか。
- ユーザ認証なしでだれでも利用できる情報コンセント等はないか。
- ルータやスイッチなどのアクセスコントロールや時刻同期を行っているか。

### (4)サーバ

- OSやサーバのソフトウェアは信頼できるバージョンを使用し、必要に応じてアップデートを行っているか。
- サーバの稼動状況や利用者ごとのアクセス状況を把握し、正確な時刻設定のもと、ログの保存と解析を行っているか。
- 不要なサービスやポート、アカウント等が稼動していないか。
- 定期的な監査を行い、セキュリティの基準を満たしていないサーバがないかチェックしているか。
- セキュリティホールとなるようなソフトウェアへの対策を行っているか。
- 障害発生時の復旧に備えて、バックアップをとっているか。
- 施錠された安全な場所に設置し、入退室者の記録をとっているか。
- 廃棄する際に、情報資産が流出しないよう、手順や履歴の管理を行っているか。
- パスワードを定期的に変更し、容易に推測できないものとなっているか。
- 不正侵入対策として、学外から管理者権限でサーバにログインできないようになっているか。
- Webサーバ上のコンテンツに対するアクセス権などを適切に設定しているか。
- Webアプリケーションに対する脆弱性対策(XSS,SQLインジェクション等)を行っているか。
- 重要な情報を取り扱う場合は暗号化を行っているか。
- 公開している情報が本当に正しいものなのか定期的にチェックしているか。

| |
|---|
| ・ 迷惑メール対策（ウィルス対策、spam対策、オープンリレー対策等）をしているか。 |
| ・ ネームサーバのデータベースが適切に管理されているか。 |
| ・ ファイルサーバへのアクセス権を適切に設定しているか。 |
| (5)クライアント |
| ・ 悪意のあるソフトウェア対策を行っているか。 |
| ・ OSやソフトウェアは信頼できるバージョンを使用し、必要に応じてアップデートを行っているか。 |
| ・ 不要なサービスやポート、アカウント等が稼動していないか。 |
| ・ 正確な時刻設定のもと、利用者のログの保存と解析を行っているか。 |
| ・ 障害発生時の復旧に備えて、バックアップをとっているか。 |
| ・ 部外者が容易に立ち入らないような監視体制と盗難防止策を講じているか。 |
| ・ 廃棄する際に、情報資産が流出しないよう、手順や履歴の管理を行っているか。 |
| (6)情報媒体の管理 |
| ・ 情報媒体(USBメモリやハードディスクドライブ、ノートパソコン等)の持ち出しや持ち込みについて基準を設けているか。 |
| ・ 情報媒体はパスワード設定や暗号化等の紛失・盗難対策を講じているか。 |
| (7)　情報施設・設備の管理 |
| ・ 地震や火災等、施設に対する安全管理対策はできているか。 |
| ・ 電源や空調の安定運用、盗難防止等、設備や機器等に対する安全対策はできているか。 |

※ ログについては法(プロバイダ責任制限法)の定めるところにより保存する。