福井県立大学 情報セキュリティポリシー

2008/4/1

１．情報セキュリティポリシーの策定

コンピュータネットワークを利用した教育・研究環境が、本学に導入されて久しい。現在では、本学のほとんどの情報が、コンピュータネットワーク上で扱われていると言っても過言でない状況であり、教育・研究支援、大学運営のためのインフラとしても重要なものとなっている。このため、「コンピュータ、ネットワークおよびこれらが処理する情報」（以下「情報資産」という。）に関する障害が発生した場合の損失は甚だしいものとなり、「情報セキュリティの確保」は重要命題である。

本学は、情報資産の「機密性」、「完全性」、「可用性」の維持および、情報セキュリティに対する「侵害行為の阻止・抑止」、「情報セキュリティ対策と手順の評価改善」を目的として、情報セキュリティポリシーを策定する。

２．定義

用語の定義は，情報セキュリティ対策推進会議が定めた「情報セキュリティポリシーに関するガイドライン」(http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html)に準ずる。

３．対象範囲ならびに対象者

情報セキュリティポリシーの対象範囲は，本学の管理する機器，ネットワーク，一時的にネットワークに接続された機器、情報システム、情報システム・コンピュータネットワーク上を流通する情報である。

情報セキュリティポリシーの対象者は本学の情報資産を利用する職員、学生等の大学構成員、および本学情報システムに関係する委託業者、外来者等とする。

４．セキュリティ対策の実施

情報セキュリティポリシーの遵守事項、対策、規則等の運用および改善について以下の観点にもとづき策定する。なお、具体的な事項は「情報セキュリティ管理要領」に定める。

⑴組織・体制
- ・情報セキュリティの確保を推進する情報セキュリティ責任者の設置
- ・情報セキュリティに関する調整・検討を行う組織の設置
- ・教育・啓発活動を行う組織の設置

⑵物理的セキュリティ
- ・不正な立入り、損傷および妨害から保護するための設備の設置
- ・出入管理およびパソコン盗難対策等の物理的な対策
- ・モバイル機器を利用した情報漏洩の防止

⑶人的セキュリティ
- ・利用者向けの情報システム利用時の遵守事項
- ・機器操作、パスワード管理等のセキュリティ遵守義務
- ・情報セキュリティに対する研修、説明会の実施および啓発活動の実施
- ・情報セキュリティに関する事故・欠陥発見時の連絡方法・体制
- ・管理者側の安全管理、守秘義務、外部委託等に関する管理

⑷技術的セキュリティ
- ・安全管理のためのユーザに対する利用制限、アクセス制限、禁止事項
- ・情報システムの運用管理手順やデータ交換、ネットワーク管理、記録媒体の保護
- ・ネットワーク各種サービスの運用管理方法、侵害に対する監視・防御等
- ・システム開発、導入、保守等の確実性管理
- ・コンピュータウイルス感染防止対策、感染時の対処
- ・セキュリティ情報の収集体制、分析手順、周知方法

⑸セキュリティ対策の運用
- ・情報システムの監視およびセキュリティ遵守状況の調査・点検
- ・情報セキュリティ侵害時の対応策および防止策
- ・情報セキュリティに関する違反に対する処置
- ・関連する法令への遵守等
- ・実態に即した「情報セキュリティ管理要領」の改善