

ミニ特集 情報セキュリティポリシーに寄せて

情報処理センター長 長嶋 豊

近年の情報通信技術の著しい進展は、世界中の大量の情報に手軽にアクセスでき、またこれまでなかった新たなビジネスチャンスを生み出す等、人々の生活や社会経済活動に大きなメリットをもたらしている。本校でも「e-Japan」政策の一環として、昨年、学内ネットワークはギガビットLANへと更新され、教育・研究等に一層活用されている。しかし、このようなネットワーク社会の利便性を今後も享受していくためには、その安全を守る組織・体制、仕組みを充実させ、安心してインターネット等を活用できる環境を構築することが重要である。ネットワークに参加する全ての組織や人々は、それぞれに応じた「情報セキュリティ」対策に取り組むことが、強く求められている。

コンピュータウイルス、ホームページ改ざん、他人のIDやパスワードを用いた不正アクセスなど情報セキュリティに関連する記事やニュースが連日マスコミをにぎわしている。史上最強のウイルスとまでいわれた、今夏の「MSブラスト」は大学・高専間へも感染が拡大し、大きな社会問題となった。情報ネットワークは電気、ガス、水道と同じような社会基盤であるが、極めて重大な情報リスクが隣り合わせであることは意外と認識されていない。

特に、教育・研究機関として考えられる情報リスクには、

- (1)表沙汰になりやすい脅威で、かつ、イメージ低下に陥るものとして、
ホームページ改竄、踏み台、電子メールの不正中継等がある。
- (2)表沙汰にならない脅威で、教育や研究業務継続上のリスクが大きいものとして、
研究情報の流出、個人情報の流出等がある。
- (3)独立法人化後は、経営情報の流出、ネットワーク経由サービスの品質低下等がある。

本号では、佐世保高専での「情報セキュリティポリシー」の策定と運用を機に、ミニ特集として取り上げた。

そもそも情報セキュリティという言葉の意味は、『企業・学校などの組織における情報資産全般の「機密性」、「完全性」、「可用性」を確保する』という意味で使われている。

- ・機密性：アクセス権を持つ者だけが、情報にアクセスできることを確実にすること。
- ・完全性：情報及び処理方法が正確であることと完全であることを保護すること。
- ・可用性：認可された利用者が、必要なときに、情報および関連する資産にアクセスできることを確実にすること。

文部科学省管轄機関では、未だに25%程度しか情報セキュリティポリシーの策定がなされていないのが現実であるが、本校では、ポリシーはもちろん「利用者用」及び「情報処理センターシステム管理者用」実施手順書を策定し、運用に入った。しかし、情報セキュリティを維持するためには、Plan - Do - Check - Action (PDCAと略す)が必要であり、今後、技術、法律、制度、あるいはコンピュータ上のリスクに応じて、常に評価、改善作業を行わなければならない。

最後に、本校情報セキュリティポリシーの策定に取り組んでくださった「情報処理センター運営委員会」及び「情報セキュリティ委員会」の各位、さらに、本号に寄稿して下さった方々に深く感謝いたします。