平成 27 年 4 月 1 日
ネットワーク管理責任者

下関短期大学　情報セキュリティポリシー

＜基本方針＞

1. 基本方針

下関短期大学（以下「本学」という。）が教育活動および学術研究を円滑に行い、広く社会に貢献するためには、情報基盤の整備に加え、情報セキュリティを保護することが不可欠である。このため、本学においては、情報セキュリティに対する侵害を阻止し、学内外の情報資産を損なう加害行為を防ぎ、社会的信頼を確保するための包括的なポリシーとして、この情報セキュリティポリシー（以下「ポリシー」という。）を策定する。

2. 対象範囲

ポリシーの対象範囲は、本学で使用するハードウェア、ソフトウェア、ネットワーク、記録媒体等の情報システム等、情報システムに記録される情報、および一時的に接続されたコンピュータとする。ポリシーの対象者は、すべての学生・教員・職員・委託業者および来学者とする。

3. ネットワーク管理責任者

ネットワーク管理責任者は、個々の情報システムを維持、管理する者で、セキュリティを維持するための責任を持つ。

4. 対象者の義務

すべての対象者は、ポリシーの実施に責任を負うとともに、ポリシーを遵守しなければならない。さらに、ネットワーク管理責任者からセキュリティの維持管理のために協力を依頼された場合には従わなければならない。

＜対策基準＞

1. 内部利用（学内にあるコンピュータやネットワーク、システムの利用に関して）

(ア) コンピュータやネットワーク、メールの利用のために必要なＩＤはネットワーク管理責任者が付与する。

(イ) ＩＤとパスワードは本人のみが利用できる。そのため、他の利用者ＩＤを用いたり、他人に自分のＩＤを貸与したりしてはならない。

(ウ) 他人にわかりやすいパスワードは避けなければならない。

(エ) コンピュータやネットワークを教育研究、事務作業以外に使ってはならない。

(オ) 席を離れるときは他人に勝手にコンピュータを利用されないようにしなければならない。

(カ) 休退学、休退職、人事異動の際は、すみやかにネットワーク管理責任者に報告しなければならない。ネットワーク管理責任者は、この報告を受けた後、すみやかに設定変更等の対応をしなければならない。

2. インターネット利用（電子メール、Ｗｅｂの閲覧、ダウンロード等に関して）

(ア) 第三者の人権やプライバシーを尊重するとともに、知的所有権に配慮しなければならない。

(イ) マルチ商法、ネットワーク詐欺などの悪徳商法や詐欺事案に荷担してはならない。

(ウ) 不適切なサイトや信頼できないサイトにサクセスしてはならない。

3. ウイルス対策

(ア) 万一のウイルス被害に備えるために、データのバックアップを行わなければならない。

(イ) ウイルスに感染しないよう、ワクチンソフトを搭載、稼働していなければならない。

(ウ) ウイルス発見時・感染時にはネットワーク管理責任者に報告しなければならない。

(エ) ウイルスを作成したり、配布したりしてはならない。

4. 外部公開（Ｗｅｂ公開、掲示板への書き込み等に関して）

(ア) 公序良俗に反する情報を発信してはならない。

(イ) 第三者の人権やプライバシーを尊重するとともに知的所有権に配慮しなければならない。

5. 人的セキュリティ

(ア) 業務上、知りえた情報を業務以外で使用してはならない。

(イ) 法令違反行為または法令違反のおそれのある行為をしてはならない。

(ウ) 個人、法人への誹謗・中傷をしてはならない。

(エ) 個人、法人に不利益をもたらす行為をしてはならない。

(オ) 個人、法人の著作権の侵害をしてはならない。

(カ) その他、ネットワーク管理責任者が不適当と判断した行為をしてはならない。

6. 物理的セキュリティ

(ア) コンピュータや記録媒体等を破棄する場合は、データが流出しないよう、その処分方法に注意しなければならない。

(イ) コンピュータや記録媒体等を盗難されないよう、設置場所、保管方法に注意しなければならない。

(ウ) コンピュータや記録媒体等が破損しないよう取扱いに注意しなければならない。