【学生】
情報システムの利用に関わる対策ガイドライン

制　定　日：平成 19 年 4 月 1 日
最終修正日：平成 21 年 11 月 12 日

目　次

1. 目的

この対策ガイドラインは、学校法人愛知大学（以下、「大学」という）の情報セキュリティポリシーに基づくとともに、大学の情報資産が、改竄や破壊から保護され、定められた方法で常に利用でき、情報のセキュリティを確保した状態で、情報の利用が行われることで、大学運営の安定、継続、繁栄に寄与することを目的とする。

2. 基本的な考え方

情報のセキュリティを確保した状態で、大学の情報を利用するため、別途定める「情報セキュリティ対策基準」に則った、適用すべき情報システムの利用のための対策ガイドラインを策定する。

3. 定義

別途定める「情報セキュリティ対策基準」の定義に準ずる。

4. 情報システムの利用に関わる対策ガイドライン

(1) 対策ガイドライン

ア. 情報システムのコンピュータウイルス対策

コンピュータウィルスが情報システムで取り扱う情報の完全性を損なうことを防止するため、コンピュータウィルスに感染することを予防しなければならない。また、感染時の被害を最小化するための対応を実施しなければならない。

①. 悪意のあるソフトウェア（コンピュータウィルス、トロイの木馬等）対策

不正ソフトウェアから保護するため、学生は次のような点に注意することが望ましい。

A) 出所がはっきりしていない、又は許可されていない出所の電子媒体上のファイル、もしくは信頼できないネットワーク上から得られたファイルは、ウイルスやトロイの木馬が含まれていないかどうか使用前にチェックする。

B) 電子メールの添付ファイル及びダウンロードファイルは、不正ソフトウェアでないかどうか使用前にチェックする。

C) 不正アクセスの痕跡（見知らぬファイルの存在）や、コンピュータウィルス、機器の障害などを発見した場合は、速やかに情報メディアセンターに報告する。

イ. 電子メールの利用

電子メールを利用して情報のやり取りを行う場合、以下のような点に注意することが望ましい。

①. 電子メールのセキュリティ

電子メールによってもたらされる恐れのあるセキュリティ上のリスクを軽減するために、次のような点に注意すること。

A) 送信前に宛先メールアドレスを確認する。

B) 電子メールにファイルを添付して送付する場合は、情報の重要度に応じて、ファイルの暗号化もしくは開封パスワードの設定を行う。

C) 他人の信用を傷つけるおそれのある行為、中傷的な電子メールの送信、いやがらせのための使用、認可されていない物品の購入を行わない。

ウ. ホームページなどによる情報発信

ホームページやブログ、BBS、チャット等を用いて情報の発信を行う場合、発信する情報に責任を持ち、次のような行為を行ってはならない。

A) 著作権や著作者人格権、特許権、肖像権、プライバシーの侵害
B) 公序良俗違反
C) 誹謗、中傷

エ. 私有するコンピュータ機器及び可搬媒体等の利用

情報の利用権限の無い者による大学システムの利用、ネットワーク上の不正アクセス、さらにウィルスによる被害を防止するため、私有するコンピュータ機器及び可搬媒体等を利用する場合、学生は次のような対策を実施しなければならない。

①. 私有するコンピュータ等の利用

A) 私有するコンピュータ等を学内ネットワークに接続する場合は、「ホスト接続登録申請書」を情報メディアセンターに提出し、接続許可を得る。
B) セキュリティ・パッチを適用し、当該コンピュータのオペレーティングシステムを最新の状態に保つ。
C) 当該コンピュータにウィルス対策ソフトをインストールし、ウィルス定義ファイルを最新の状態に保つ。
D) 機器の盗難、置き引きに注意し、席や車内に放置しない。

②. 私有する可搬媒体の利用

A) 学内にコンピュータウィルスを持ち込まないよう、可搬媒体を利用するコンピュータにウィルス対策ソフトをインストールし、可搬媒体のコンピュータウィルスの感染を防止しなければならない。

オ. 無許可ソフトウェアのインストール禁止

不正なソフトウェアの利用、コンピュータの誤作動を防止するため、私有するソフトウェアを学内のコンピュータで利用ならびにインストールしてはならない。

カ. 営利行為

大学のドメインを用いた営利行為を行ってはならない。

キ. P2P ファイル交換ソフトウェアの利用

ファイル交換ソフト(以下「P2P ソフト」という。)を利用することで、パソコン内にウィルスが侵入することがあり、それにより PC 内に保存されている重要なデータがネットワーク上に流出する危険がある。また、P2P ソフトによる大量かつ連続したデータ通信は、学内ネットワークを圧迫し、他の利用者の通信阻害にもつながる可能性があるため、次の点に注意することが望ましい。

・ウィルス対策ソフトを PC にインストールし、さらにソフトの更新を行い、常に最新の状態にす

る。

・Microsoft Update 等を定期的に実施し、OS 等を最新の状態に保つようにする。

・P2P ソフトを利用する場合は、個人情報や重要なデータを、コンピュータで扱わない。

・他人の知的財産を無許可で扱うことや、他人の PC に侵入することは法律で禁止されている。著作権法や不正アクセス禁止法等の法令を遵守し、違法な利用はしない。