

【学生】

学外における情報システムの利用ならびにアクセス に関する対策ガイドライン

制 定 日：平成 18 年 4 月 20 日

最終修正日：平成 21 年 11 月 12 日

目 次

1. 目的	1
2. 基本的な考え方	1
3. 定義	1
4. 学外における情報システムの利用ならびにアクセスに関わる対策ガイドライン	1
(1) 対策ガイドライン	
ア. 学外からのアクセス.....	1
①. モバイルコンピューティング	1
②. 自宅からのアクセス	1
③. 公共施設やネットカフェからのアクセス	1

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、学生が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、適用すべき学外における情報システムの利用ならびにアクセス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. 学外における情報システムの利用ならびにアクセスに関わる対策ガイドライン

(1) 対策ガイドライン

ア. 学外からのアクセス

情報の利用権限の無い者への情報の開示、情報の利用権限の無い者による情報の変更、窃盗を防止するため、モバイルコンピューティング又は自宅等から大学のシステムへアクセスする場合、学生は以下のような対策を講じることが望ましい。

①. モバイルコンピューティング

モバイルコンピューティングに利用する装置(例えば、ノート型コンピュータ、パームトップ型コンピュータ、及び携帯電話など)を用いる時、盗難や盗み見、盗み聞きなどによってセキュリティが脅かされることが絶対にならないように、特別な注意を払うことが望ましい。さらに、電車、車などへの置き忘れや置き引きにも注意する。これらは、学外に限らず、学内においても同様の点に注意を払う。

②. 自宅からのアクセス

自宅から大学のシステム(電子メール、UNIVERSALPASSPORT など)を利用する場合や、SSL-VPN システムにより大学のシステム、ファイルにアクセスする場合、学生は次のような点に注意することが望ましい。

- a) コンピュータウイルスによる情報の流出を防止するため、ウイルス対策ソフトを導入し、定義ファイルを常に最新の状態にする。
- b) セキュリティ・パッチを適用し、オペレーティングシステムを最新の状態に保つ。

③. 公共施設やネットカフェからのアクセス

公共施設やネットカフェから大学のシステム(電子メール、UNIVERSALPASSPORT など)を利用する場合、大学の内部システムへの認可されていない遠隔アクセスなどを防止するため、次のような点に注意することが望ましい。

- a) 情報の流出を防止するため、キーロガーなどの悪意のあるプログラムに注意する。
- b) Web サービス利用時にユーザ ID 及びパスワードを入力する場合は、Web ブラウザ

にそれらの情報を保存しない。保存した場合は、履歴を削除する。