

神戸女学院大学情報セキュリティポリシー（抜粋）

2009年1月19日

部長会制定

第1章 総論

（目的）

第1条 本ポリシーは、神戸女学院大学（以下「本学」という。）が教育機関として情報基盤を整備し、情報資産のセキュリティを確保することを目的として、本学が取り扱う情報セキュリティの方法等について定めるものとする。

（基本理念）

第2条 本学の構成員は、本学が所有する全ての情報資産について、以下の各号に定める適切なセキュリティを保障する義務を負う。また、学生についても KC-NET 利用上のマナーを遵守し、接触する情報資産のセキュリティ確保ができる教育を実施する。

- (1) 大学の情報資産に対する侵害の阻止
- (2) 学内外の情報セキュリティを損ねる加害行為を抑止
- (3) 情報資産の重要度に見合った管理
- (4) 情報セキュリティに関する情報取得の支援と啓発

（用語の定義）

第3条 本ポリシーで使用する用語の定義は、次のとおりである。

- (1) 情報セキュリティ…情報資産の機密性、完全性及び可用性を維持すること
- (2) 情報資産…情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称
- (3) 情報システム…同一組織内において、ハードウェア、ソフトウェア、ネットワーク、記憶媒体で構成されるものであって、これら全体で業務処理を行うもの
- (4) 情報セキュリティポリシー（以下「ポリシー」という。）…本学が所有する情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的にとりまとめたもの。どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定

（適用範囲）

第4条 本ポリシーが適用される範囲は次のとおりとする。

- (1) 本学の全ての情報資産
- (2) KC-NET に接続された情報機器
- (3) このポリシーに抵触する行為がなされた情報機器
- (4) 本学の運営に資する全ての関係者（外部委託業者等の本学以外の組織や人員を含む）と本学の学生

(5) 退任、退職、卒業又は契約の解消後に、本ポリシーに抵触する行為があった者
(組織・体制)

第 5 条 情報セキュリティの最高責任者は学長とする。本ポリシー遵守の推進及び改定については情報処理センター運営委員会が所管する。また、本ポリシーへの抵触があった場合の対処については、その案件の所管部署が対応する。

略

第 4 章 人的セキュリティ

略

(免責)

第 16 条 本学の教職員及び学生は、本ポリシー並びに「神戸女学院大学 KC-NET 利用に関する遵守事項 (エチケット)」を遵守しなければならない。ただし、情報セキュリティ障害について自らの行為が原因となった者や管理責任のある者の処分について、その者が障害発生時あるいは判明時に迅速かつ積極的に申告し解決に尽力した場合は、処分を決定する時点で情状を酌量し、免責される場合がある。

略

(教育・研修)

第 18 条 情報処理センターディレクターと大学事務長は、本ポリシーに関する大学教職員向けの研修会を実施しなければならない。また、本学の教職員及び学生は、研修会や説明会又は講義等を通じ、本ポリシーを理解し情報セキュリティ上の問題が発生しないように努めなければならない。

(事故障害の監視協力)

第 19 条 本学の教職員は、情報を扱う者の不審な行動、情報セキュリティに関する事故、情報システムの不審な動作、情報の改ざん、システム上の障害及び欠陥や誤動作を発見した場合には、所属長又は上位の管理者に直ちに報告しなければならない。また、学生が発見した場合は、教職員に直ちに報告しなければならない。

(アクセスのための認証情報等の管理)

第 20 条 本学の教職員及び学生は、パスワードの管理については以下の事項を遵守しなければならない。

- (1) 自己のパスワードは秘密としなければならない。また、セキュリティ保持の為、定期的に変更しなければならない
- (2) 自己のアカウントを他者に使用させてはならない
- (3) 他者のアカウントを使用してはならない
- (4) 他者のパスワードを使用してはならない
- (5) 所属長や情報処理センターあるいは授業科目担当者が、不適切なパスワードの変更を求めた場合、その指示に従わなければならない

略

第5章 技術的セキュリティ

略

(アクセス制御)

第24条 …略… 利用者は、アクセス権のない情報や情報システムにアクセスしてはならない。

(コンピュータウィルス、スパイウェア対策)

第25条 情報機器の管理者及び使用者は、不正アクセス、コンピュータウィルスやスパイウェア等情報システムの運用を妨害し、情報を漏洩しようとする攻撃行為から情報資産を守るために必要な対策を講じなければならない。

2 ファイル交換（共有）ソフトは極力使用してはならない。情報資産を扱うパソコンやサーバがつながった情報機器ではファイル交換（共有）ソフトを使用してはならない。また、情報資産を扱うパソコンでファイル交換（共有）ソフトを使用して作成したファイルを利用する場合はそのデータの検疫を事前に完全に行った後でなければ利用してはならない。

3 ネットワーク上の情報を盗聴するような監視ソフト、ネットワークの状態を探索するセキュリティ関連ソフト及びハッキングソフトは使用してはならない。ただし、…略…。

第6章 運用

略

(運用管理における留意点)

第27条 基本的に本ポリシーを運用するためにプライバシーに対する侵害があってはならない。セキュリティ保持のためにやむを得ず侵害が発生する場合には、慎重に対処すること。

略

(不正使用)

第29条 …略…

2 本学の教職員又は学生が不正使用を行ったときは、就業規則、学則、その他の諸規程に従って処分を受けることがある。

略

附 則

本ポリシーは、2009年1月19日から施行する。