神戸女学院大学情報セキュリティポリシー

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。

第 2 章　　情報の管理と分類

(情報の管理体制)

第 6 条　　各種情報資産は、その管理権限を有する事務組織、個々の教員及び教員組織によって管理される。

(情報の分類)

第 7 条　　情報管理のために、各種情報については文書取扱規程を基本として各管理権限単位において、大きくは「公開情報」「非公開情報」に分ける。非公開情報については「極秘」「機密」「取扱注意」のように分類して取扱方法を区別して管理する。

2　公開情報は、情報の改ざん・偽情報の流布・個人情報の漏洩・著作権等の各種権利の侵害への防止策を講じること。

3　非公開情報は、アクセス権限の設定や複写禁止等の情報の機密性に応じた適切なセキュリティ対策を講じること。

第 3 章　　物理的セキュリティ

(情報管理施設)

第 8 条　　情報資産を保管する場所は施錠、入退室記録、監視カメラ設置等の手段を講じて管理する。

(情報取扱制限)

第 9 条　　情報資産の取扱は以下の方法等から適切な管理方法をもって管理する。

(1)　利用場所の制限
(2)　利用者の制限
(3)　利用者、利用目的等の申請・届出
(4)　謄写・複写・複製の禁止
(5)　アクセスログの管理
(6)　利用端末、利用パソコンの制限
(7)　書き込み・上書き・削除の制限

(ネットワーク設備)

第 10 条　　KC-NET への不正な機器の接続を防止するような方策と、KC-NET 使用の記録をとれる体制を整えなければならない。

2　端末機器とネットワーク設備については、災害、事故及び情報機器の盗難への対策を講じておかなければならない。

(サーバ、パソコン及び情報記録媒体)

第 11 条　　サーバ機器については、保存されたファイルや機能の重要度に応じたセキュリティ管理が施されなければならない。また、特定のサーバの事故により、学内の他機能に重大な影響が予想されるサーバについては、その管理場所・設備についても特段の配慮をしなければならない。

2　パソコン及び情報記録媒体については各管理単位において災害、事故、盗難等の犯罪に対する対策を講じなければならない。

3　サーバ、パソコン及び情報記録媒体等のバックアップについては、その内容の重要度に応じて定期的に行い、文書保存規程を参考として一定期間保管しなければならない。

(廃棄)

第 12 条　　情報資産を廃棄する場合は､その保管状況に応じて､シュッレッダーにかける、物理的に破壊する､廃棄物処理業者に廃棄を依頼し廃棄証明を受け取る等の処理をしなければならない。また、その際には管理責任において上位の管理責任者の立会いのもとに行うことを基本とし､廃棄業者等に業務依頼をする場合においても事前に学内でできる限りのデータ消去作業を施した後に依頼しなければならない。

第 4 章　　人的セキュリティ

(情報セキュリティ最高責任者の責務)

第 13 条　　情報セキュリティの最高責任者は本ポリシーに基づき、本学のすべての情報セキュリティに関する総括的な権限と責任を有し、主として以下の事項を処理する。

(1) 大学組織、主として情報処理センターを通じて、すべての教職員にポリシーの遵守を励行させる

(2) 情報システムの円滑な運用に必要な措置を、それぞれのシステム単位での上位の管理者に要請する

(3) 学院の意思決定機関（理事会、学院常務委員会、部長会）に、情報セキュリティに関する重要事項の報告又は勧告をする

(4) 情報セキュリティに関する学外からの苦情への対応や、学外から受けた被害への対応を指揮する

(情報処理センターディレクター及び大学事務長の責務)

第 14 条　　情報処理センターディレクターは、情報セキュリティの維持と強化のための技術的な調査検討を行う。情報処理センターへは直接、他部署や他教員にはしかるべき組織を通じて適宜勧告や指導を行うことができる。

2　情報処理センターディレクターと大学事務長は、情報セキュリティを守るために緊急避難措置が必要と判断したときは､部署や所属を問わず直接そのシステムや情報資産の管理者に措置を命ずることができる。ただし、措置後速やかに情報セキュリティの最高責任者並びに､該当するシステム及び情報資産管理者の所属長に報告あるいは通知を行わなけれ

ばならない。

(パソコン係)

第 15 条　　パソコンやサーバを使用する事務部署はパソコン係を決めるものとする。パソコン係はその部署内のパソコンやサーバ等情報機器の実務上直接の運用管理者となり本ポリシーを遵守しなければならない。

(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。

(外部委託)

第 17 条　　外部委託業者など本学の構成員でないものに情報システムの開発や運用等の業務を委託する場合は、下請けとして受託する業者を含めて対象範囲に従って本学のポリシーのうち守るべき内容の遵守義務が発生すること、そのための教育を実施すること、遵守されなかった場合の規定（損害賠償等）を明記した契約を行わなければならない。

(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

(プライバシーの保護と例外)

第 21 条　　アカウント、パスワード、ログ及びその他のシステムに関して、プライバシーに関わる情報を業務上必要以上に収集を命じたり、収集をしてはならない。また、業務上知り得たプライバシー情報は、退職後も他者に口外してはならない。ただし、システムを管理する担当者はセキュリティ保持に関わる正当な理由がある場合には、その理由を所属長に申告し、対応を相談した後に情報セキュリティの最高責任者の許可を得て、プライバシー情報を使用してセキュリティ障害回避に使用することができる。なお、障害回避にあたっては、緊急を要するか否かによらず、回避処理遂行者以外に複数の職員の立会いと同意のもとで対応しなければならない。また、緊急の場合の回避処理にあたっては、事後に所属長及び情報セキュリティの最高責任者に直ちに報告しなければならない。

2　いかなる理由があろうとも、正当な手続を経ずしてプライバシーに関わる情報を閲覧あるいは収集したり、その行為を命じてはならない。

第 5 章　　技術的セキュリティ

(コンピュータ及びネットワークの管理)

第 22 条　　情報処理センターは、KC-NET を利用するときに認証によって利用資格が確認されるシステムを構築しなければならない。

(サーバ管理)

第 23 条　　KC-NET に接続されているサーバや、複数の教職員や学生が使用するサーバを管理する者は、アクセス記録を取り、盗難・改ざん・消去等を防止する措置を講じて一定期間保存しなければならない。また、不正使用の疑いがあるときにはその対策に必要なアクセス記録の提出を求められることがあるので、サーバ管理者はこれに迅速に協力しなければならない。

(アクセス制御)

第 24 条　　各情報の管理者は、情報の内容に応じてアクセス可能な利用者を定めアクセス制限を行わなければならない。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、情報処理センターシステム担当者が職務遂行に必要なソフトを使用する場合はこの限りではなく、導入にあたっては情報処理センターディレクターの許可と立会いが必要である。

第 6 章　運用

(情報システムの監視及びポリシーの遵守状況の確認、運用管理)

第 26 条　各情報システムの管理者あるいはパソコン係は、情報システムが安全に稼動していることを監視し、本ポリシーが遵守されるよう担当する情報システムを運用しなければならない。

(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ついては、慎重に対処すること。

(事故時の対応策)

第 28 条　情報資産のそれぞれの管理者は、報告のあった事故等について必要な措置を直ちに講じなければならない。管理者は発生した事故等に関する記録を一定期間保存し、情報処理センター運営委員会に報告するとともに、重大な事故に対しては、迅速な再発防止のための対策を講じなければならない。

(不正使用)

第 29 条　情報システムの管理者は、学内外からの報告や依頼を受けて、情報機器の不正使用の調査を早急に行う。不正使用が確認されたときには、関連する通信の遮断又は該当する情報機器の切り離しを実施する。

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。

3　発生した不正行為の内容と対処については、事故のあった管理部署の所属長が情報セキュリティ最高責任者、大学事務長、情報処理センターディレクター及び情報処理センター課長と相談の上、そのセキュリティを損なわない範囲で公表するかどうかを決定する。

(評価・見直し)

第 30 条　情報処理センター運営委員会は、本ポリシーの点検評価のために以下のような情報を収集して定期的に検討する。

(1) 本学の教職員及び学生からのポリシー遵守についての意見と実施運用上の要望や苦情
(2) 事故、故障、不正行為の事例、対策の成功事例、システム管理担当者からの意見や要望
(3) 本ポリシーの実施状況についての点検・監査結果
(4) 情報システムの機密性、完全性及び可用性並びに犯罪防止の観点からの情報セキュリティ診断結果

情報処理センター運営委員会は、これらの情報を基に、本ポリシーの実効性を評価し、よりセキュリティレベルの高い、かつ、遵守可能なポリシーに更新しなければならない。情報処理センターディレクターは情報セキュリティの最高責任者に点検・評価の結果を報告し、本ポリシーが更新されるごとに本学の教職員及び学生に対してこれを提示して啓発を行う。

(規程の改廃)

第 31 条　　本ポリシーの改廃は、情報処理センター運営委員会の議を経て、部長会が行う。

附　則

本ポリシーは、2009年1月19日から施行する。