

## ○京都学園大学情報セキュリティポリシー

## 1. 情報セキュリティの基本方針

高度情報社会において、京都学園大学（以下「本学」という）が学術研究・教育活動を高めようとするためには、情報基盤の整備に加えて、本学の情報資産のセキュリティを確保することが不可欠である。

情報セキュリティの大切さを本学の全構成員に十分意識させ、情報資産を確固として守るため、情報セキュリティポリシー（以下「ポリシー」という）を定めるものである。

## 2. ポリシーの用語の定義

## (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。ただし、特段の定めのない限り、情報資産は情報システムにかかるものに限る。

## (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、記録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) 情報セキュリティ対策基準（以下「対策基準」という。）

情報セキュリティを確保するために遵守すべき行為及び判断等の基準、つまりポリシーを実現するために何をやらなければいけないかを示すもの。

## (5) 実施手順(ガイドライン)

対策基準に定められた内容を、対象者ごとに、どのような手順に従って実行していくのかを示すもの。

## (6) 部局

各学部及び各研究科並びに事務局（各課・事務室等）をいう。

## 3. 対象範囲

ポリシーの対象範囲は、本学の情報資産に加えて、本学のコンピュータで、本学のネットワークに一時的に接続されたコンピュータを含む。

ポリシーの対象者は、教職員、臨時職員、非常勤教職員、契約教職員、委託業者、大学院生、大学生、研究生、科目等履修生、聴講生、委託生、来学者などで、本学の情報システムの利用を認められた者とする。

対象者は、ポリシーの重要性を認識し、遵守しなければならない。

## 4. ポリシー等の公開

ポリシーは、公開する。

対策基準は、情報セキュリティ委員会委員及び情報センター職員に公開する。

実施手順（ガイドライン）は、該当者に公開する。

公開の手順は、情報センターの定めるところによる。

## 5. 組織・体制

## 5.1 管理・運用組織の構成（図 1）

## 5.1.1 最高情報セキュリティ責任者

本学に最高情報セキュリティ責任者を置き、学長をもって充てる。

最高情報セキュリティ責任者は、本学の情報セキュリティに関する総括的な権限及び責任を負う。

## 5.1.2 全学セキュリティ管理責任者

本学に全学セキュリティ管理責任者を置き、情報センター長をもって充てる。

全学セキュリティ管理責任者は、全学の情報システム管理の実施に関し、緊急時の連絡など、総括的な対応に当り、最高情報セキュリティ責任者を補佐する。

### 5.1.3 部局セキュリティ管理責任者

本学に部局セキュリティ管理責任者を置き、次の者をもって充てる。

- (1) 各学部長及び、各研究科長
- (2) 事務局長及び、次長・部長・課長・事務長

部局セキュリティ管理責任者は、当該部局が管理する次の各事項について責任を負う。

- (1) 所管する情報機器の管理。
- (2) 所管する情報資産の公開・非公開。
- (3) 所管する情報の改ざん及び、偽情報流布の防止
- (4) 所管する情報機器及び、記憶媒体の処分
- (5) 所管する利用者のポリシーの運用実態等の把握
- (6) その他、所管する情報に関すること

### 5.1.4 情報セキュリティ委員会

本学に情報セキュリティ委員会を置き、最高情報セキュリティ責任者並びに情報センター運営委員会で構成する。

情報セキュリティ委員会に委員長を置き、最高情報セキュリティ責任者をもって充てる。副委員長は、全学セキュリティ管理責任者とし、委員長が校務その他の事由により職務を遂行することができない場合に、その職務を代行する。

委員長は、委員会を招集し、議長となる。

委員長が必要と認めた場合、部局セキュリティ管理責任者の出席を求め、その意見を聞くことができる。

事務局は、情報センターとし、全学の情報システムのセキュリティ管理を実施するための連絡調整及び支援を行う。

情報セキュリティ委員会は、次の各号の事項について審議する。

- (1) ポリシーの策定及び、改訂
- (2) ポリシーの遵守の励行及び、違反に対する措置
- (3) ポリシーの実施状況にかかる監査
- (4) 対策基準及び、実施基準の策定及び、改訂
- (4) 情報セキュリティに関する学内ルールの制定並びに、啓発及び教育の実施
- (5) 学内の他の意思決定機構との調整。
- (6) 外部との折衝。
- (7) ポリシー運用の監査
- (8) 緊急時の対応
- (9) その他情報セキュリティに関することで重要なこと

## 5.2 不正アクセス等への対応

情報センターは、外部又は内部からの不正アクセスを検出した場合、情報セキュリティ委員会が定めた緊急措置手順に従い、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。ただし、あらかじめ手順に定められていない状況には、最高情報セキュリティ責任者が判断する。

情報セキュリティ委員会は、不正アクセスが継続する場合に、当該情報機器又はそれを接続するネットワークについて、定常的な利用の停止などの抑止措置をとることができる。

## 6. 情報の管理

サーバに保存された情報は、部局セキュリティ管理責任者が管理しなければならないが、個人的に管理されたコンピュータ内の情報に関しては、そのコンピュータの部局セキュリティ管理責任者と利用者が管

理しなければならない。

## 6.1 アクセス制限

情報の内容に応じて、情報にアクセス可能な利用者を定めることができる。

利用者は、アクセス権のない情報システムや情報に入り込もうとしてはならない。意図的でなく入り込んだときは、速やかに出てくるよう周知徹底するべきである。

アクセスの制限方法としては、ID とパスワード、IC カード等による。

## 6.2 情報の分類

### 6.2.1 非公開情報

許可された者以外がコンピュータに非公開情報を保管してはならない。また、一時的であっても、教職員が日常的に使用するコンピュータに非公開情報を不特定の者が可読な状態で複製してはならない。

非公開情報を扱うネットワークは、学術研究・教育用の一般ネットワークと論理的に異なるものとし、暗号化や、盗聴防止策を講じることが望ましい。

一般ネットワークと非公開情報ネットワークの間でアクセスする必要がある場合は、非公開ネットワークからのみアクセス可能としなければならない。さらに、両ネットワークの接続点を必要最小限とすべきで、できれば必要と時のみ通信を可能とすることが望ましい。

物理的な盗難等を防止するため、利用を許可された場所から外部に非公開情報を持ち出してはならない。同様に、盗聴防止のため、インターネット等の公衆回線を介して不特定の者が傍受可能な方式で非公開情報にアクセスすることも原則禁止する。

外注などのため、非公開情報を限定された第三者に開示する必要がある場合は、開示の都度、守秘義務契約を結ばなければならない。

### 6.2.2 公開情報

公開情報は任意の場所からアクセス可能な性質を持つため、情報の改ざんや偽情報の流布に対し、2.3 に掲げる防止策を講じなければならない。

### 6.2.3 発信情報(プッシュ型メール等)

大学側から不特定多数の者に発信する情報は公開情報と同じく 6.3 に掲げる防止策を講じるだけでなく、正規の発信者であることを証明する必要がある。

## 6.3 情報の公開化

非公開情報を公開化する場合には、個人情報の漏洩、プライバシーや著作権の侵害に十分注意し、公開できる情報だけを抽出する、あるいは、統計処理などの加工を行う必要がある。

## 6.4 情報の限定公開

特定の利用者に特定の情報を開示する必要がある場合、情報の登録及び閲覧は、許可された者が許可された操作だけを行えるように、認証及びアクセス制御機能を設けなければならない。さらに、異常な登録や閲覧が行われていないか、定期的に状況を確認しなければならない。

## 6.5 情報改ざん及び偽情報流布の防止

非公開情報及び公開情報の原本は、CD-ROM/CD-R 等の書き換え不能な記憶媒体に保存するなどにより原本性を保証しなければならない。

一方、公開情報は改ざんへの対策を講じなければならないが、常に進化する不正アクセス技術の脅威に対し、改ざんを受けた場合の速やかな回復機構も備えなければならない。さらに、公開情報(Web での掲示情報やメールマガジンによる情報発信を含む)の複製・加筆による偽情報の作成及び流布を防止するため、原本性の維持に努める必要がある。このため電子署名の導入を検討することが望ましい。

## 6.6 情報機器及び記憶媒体の処分

公開・非公開を問わず、情報機器及び記憶媒体を破棄する場合は、その処分方法に注意しなければならない。特に、ハードディスク及びフロッピーディスク等の記憶媒体は、通常の消去操作では管理情報のみが消去されるだけでデータそのものは消去されないため、また、数回の上書き消去では残留磁気情報の読み出しによって、情報を復元できる点に十分配慮しなければならない。

さらに、情報機器の記憶媒体を保守契約により交換する場合、又はレンタル機器の撤去を行う場合は、撤去後の記憶媒体の処理法についても十分配慮しなければならない

## 7. 評価・見直し

### 7.1 ポリシーの運用実態

最高情報セキュリティ責任者は、ポリシーの運用実態等を把握するため、情報セキュリティ委員会及び情報センターに対し、次のような措置を求めなければならない。

#### 7.1.1 ポリシー運用実態等の把握

全学セキュリティ管理責任者は、情報セキュリティ委員会を定期的で開催し、収集した情報を分析・整理し、部局セキュリティ管理責任者を通じて得られた全学におけるポリシーの運用実態に基づいて、定期的及び必要に応じて随時検討し、ポリシーの不完全さを認識しなければならない。

#### 7.1.2 利用者の意見

全学セキュリティ管理責任者は、教職員及び学生からポリシー遵守に関する意見を収集し、情報セキュリティ委員会に報告しなければならない。

#### 7.1.3 情報セキュリティ診断

全学セキュリティ管理責任者は、情報システムの機密性、完全性及び可用性並びに犯罪予防の観点から情報システムに対する情報セキュリティ診断を実施し、その結果を情報セキュリティ委員会に報告し、情報セキュリティ診断として取りまとめなければならない。

なお、診断過程で重大なセキュリティの脆弱性が発見された際は、緊急避難措置をとるとともに、部局セキュリティ管理責任者と情報セキュリティ委員にその事実を速やかに連絡すると共に、最高セキュリティ責任者にも、速やかに報告しなければならない。

#### 7.1.4 情報セキュリティ監査

全学セキュリティ管理責任者は、定期監査及び抜き打ち監査を実施し、各部局が法令並びにポリシー及びこれに関連する規定・基準等を遵守しているか運用実態を把握すべきである。その結果を情報セキュリティ委員会に報告し、情報セキュリティ監査結果としてまとめなければならない。

#### 7.1.5 セキュリティ対策費

情報セキュリティ委員会は、情報セキュリティ対策に要した直接的経費を把握しなければならない。不正アクセス等の検出のために購入した装置（ハードウェア、ソフトウェア、ソフトウェアのバージョンアップを含む）、ウイルス対策ソフトウェア、外注したセキュリティ診断及び監査などに要した費用が含まれる。

情報セキュリティを維持し続けるためには、経費を正しく見積もり、予算措置をとることが不可欠である。予算がないために重大な情報セキュリティの脆弱性を放置することは許されない。

## 7.2 セキュリティレベル向上策

最高情報セキュリティ責任者は、ポリシーに添った対策がどの程度実施されているかを評価するとともに、セキュリティレベルの向上に必要な措置を講じるため、情報セキュリティ委員会を年1回以上招集しなければならない。

### 7.2.1 ポリシーの更新

情報セキュリティ委員会は、7.1の結果に基づき、ポリシーの実効性を少なくとも年1回評価し、必要

な部分を見直して内容の変更及び実施時期の決定を行い、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。

### 7.2.2 情報セキュリティ計画及び予算案の作成

情報セキュリティ委員会は、評価・見直しの結果を踏まえ、次年度の情報セキュリティ計画及び予算案の作成を行わなければならない。

### 7.2.3 報告義務

最高情報セキュリティ責任者は、学内の最高意思決定組織（理事会、評議会、教授会等）に評価・見直しの結果を報告しなければならない。さらに、ポリシーの遵守を啓発するためにも、その要約を利用者に提示しなければならない。

(図 1) 管理・運用組織の構成

