公立大学法人京都市立芸術大学情報セキュリティポリシー

Ⅰ　基本方針

1　情報セキュリティの基本方針

公立大学法人京都市立芸術大学（以下「法人」という。）が保有及び管理するすべての情報資産は，大学運営においては非常に重要であり，必要不可欠な資産である。

しかしながら，これらの情報資産が外部に漏えいするなどした場合，大学における教育活動・学術研究の停滞，及び社会的信頼失墜などといった極めて重大な事態と被害を招くことになる。

このような事態を未然に防ぐため，教職員，学生，委託業者等すべての関係者が不断の努力をもって，情報資産を保全しなければならない。大学の情報資産を利用する者は，この情報セキュリティポリシー（以下「本ポリシー」という。）を遵守する責任があり，意図の有無を問わず，法人内外の情報資産に対する権限のないアクセスや複写，また，改ざん，破壊，遺漏等をしてはならない。

本ポリシーは，大学の情報資産を利用する教職員，学生，委託業者等すべての関係者が遵守しなければならない最低限の事項をまとめたものである。

2　定義

本ポリシーの用語定義については，以下のとおりとする。

⑴　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をいう。機密性とは，情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。完全性とは，情報及び処理方法の正確さ及び完全である状態を安全防護すること。可用性とは，許可された利用者が，必要なときに情報にアクセスできることを確実にすること。

⑵　情報

法人の教育・研究・管理運営に関わる者が作成し，又は取得した内容が記録された電磁的媒体，紙媒体及びそれに準ずる媒体をいう。

⑶　情報システム

コンピュータ，ネットワーク及び記録媒体で構成され，情報処理を行う仕組みをいう。

⑷　ネットワーク

コンピュータ等を相互に接続するための通信網，その構成機器（ハードウェア及びソフトウェア）をいう。

⑸　情報資産

法人にとって価値を有する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）をいう。

3　目標

本ポリシーは，法人における情報セキュリティの方針を示すものであり，本ポリシーによって目指すものは次のとおりである。

⑴　法人の情報セキュリティに対する侵害を阻止
⑵　法人内外の情報セキュリティを損ねる加害行為を抑止
⑶　情報資産に関して，重要度による分類とそれに見合った管理
⑷　情報セキュリティに関する情報の取得を支援

4　対象とする範囲

本ポリシーの対象設備は，法人が管理するすべての情報システム及びネットワークとこれらの設備に継続的または一時的に接続されるすべての情報システムとする。

本ポリシーの対象情報は，法人が保有する情報資産のうち，情報システム及びネットワーク上で扱われるすべての電磁情報（電子的方式，磁気的方式，その他，人の知覚によっては認識することができない方式で作られる情報）及びそれらを印刷したものとする。

本ポリシーの対象者は，教職員，学生，委託業者，来訪者など対象設備のすべての利用者とする。

5　具体化

本ポリシーを具体的に実施するための基準として「情報セキュリティガイドライン（以下「ガイドライン」という)」を別に定める。

本ポリシー及びガイドラインに基づき，必要な組織編成を行うとともに規程や具体的な実施手順などを必要に応じて定めるものとする。

6　更新

本ポリシーは，情報技術の発展ならびに策定したポリシーの遵守状況などを考慮して定期的に見直し，必要に応じて改定を行うものとする。

Ⅱ　対策基準

1　組織・体制

法人における情報セキュリティに関しての管理体制を整備するため，情報セキュリティに関する権限と責任を有する情報セキュリティ責任者を置く。また，情報セキュリティ責任者を補佐し，情報管理の実施及び緊急時の対応等にあたるため，情報セキュリティ管理者を置く。

情報セキュリティ責任者には理事長を，情報セキュリティ管理者には情報管理主事をもって充てる。

２　守られるべき財産と権利

情報ネットワークや情報システムなどの資源は適正な利用によって保護されなければならない。

情報ネットワークや情報システムのデータを保護するため，情報セキュリティの保護，適切な情報セキュリティ機構の導入，迅速な回復機構の導入，システムの監視など適切な対策を行わなければならない。

ただし，私的利用によって生じたいかなる損失や障害についての責任は負わない。

３　情報セキュリティ侵害・加害行為の防止

不正アクセスを高い確率で常時感知できる監視システムを構築するとともに，外部または内部からの不正アクセスを検出した場合には速やかに対応し，適切な対策を施さなければならない。

法人内外を問わず，あらゆる研究・教育機関，企業，組織団体，個人等の情報資産を侵害してはならない。また，本ポリシーの他，情報セキュリティに関連する法令，知的財産権に関連する法令，個人情報の保護に関連する法令及び大学が定める規程等を遵守しなければならない。

４　情報の分類に応じた管理

すべての情報について，公開・非公開・発信・受信などの分類をするとともに分類に応じて定められた情報漏えいを促すソフトウェアやウィルス等に対する情報セキュリティ対策を講じなければならない。

情報の改ざん及び偽情報流布の防止のため原本性の保障や維持に努めなければならない。

情報の漏洩を防止するため情報機器及び記録媒体を持ち込み・持ち出し・交換・破棄する場合には適切な処置をしなければならない。また，情報漏えいを促すソフトやウィルス等を検出した場合には適切な処置をしなければならない。

５　情報セキュリティ対策の実施

上述の対策基準を満たすため，本ポリシー及びガイドラインに基づき，物理的，人的，技術的な情報セキュリティ対策の実施手順を定めて運用するものとする。

附　則

本ポリシーは，平成２９年４月１日から施行する。