公立大学法人福知山公立大学情報セキュリティポリシー

1. 基本方針

1.1 情報セキュリティの基本方針

公立大学法人福知山公立大学（以下「法人」という。）が保有・管理するすべての情報資産は、法人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、法人における教育活動・学術研究の停滞、およ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、法人の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。法人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、法人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。

1.2 定義

本ポリシーでの用語の定義については、内閣官房情報セキュリティ対策推進室がとりまとめた「情報セキュリティポリシーに関するガイドライン」に定める定義と同様とする。

1.3 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。

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

1.4 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端末機器および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）およ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。

1.5　具体化

本ポリシーに基づき、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。

1.6　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度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。

2.　対策基準

2.1　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最高情報セキュリティ責任者を置く。また、最高情報セキュリティ責任者を補佐し、各所属における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。

最高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理事兼事務局長をもって充てる。

情報セキュリティにかかる会議の開催にあたっては、最高情報セキュリティ責任者はその他必要とする者の出席を求めることができるものとする。

また、情報基盤ネットワークシステムに支障を及ぼすおそれのあるあらゆる情報セキュリティインシデントに迅速に対処するため、福知山公立大学メディアセンター長の元に情報セキュリティ専門委員会を置く。

2.2　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。

2.3　情報セキュリティ侵害・加害行為の防止

法人は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。

本ポリシーの対象となる者は、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法人が定める規程等を遵守しなければならない。

2.4　違反行為への対応

ポリシー等に違反した教職員が故意または重大な過失により法人に損害を与えた場合においては、公立大学法人福知山公立大学職員就業規則等により処分を行う場合がある。

ポリシー等に違反した学生に対しては、学則等により処分を行う場合がある。

2.5　事故等への対応

情報セキュリティにかかる重大な事故等に対しては、最高情報セキュリティ責任者及び情報セキュリティ管理者及び福知山公立大学危機管理・人権・倫理委員長により、迅速な対策の実施及び再発防止のための対策を講じなければならない。

2.6　情報セキュリティインシデントへの対応

情報セキュリティインシデントに対しては、情報セキュリティ専門委員会が中心となり各部局の協力のもと迅速に対応するものとする。

2.7　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マルウェア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。

情報の改ざんおよ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およ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、マルウェアを検出した場合には適切な処置をしなければならない。

2.8　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

（施行期日）

本ポリシーは、2017 年 4 月 1 日から施行する。

資料：　用語の説明

（内閣官房情報セキュリティ対策推進室：「情報セキュリティポリシーに関するガイドライン」等による。）

・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。

・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。

・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。 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。

・情報セキュリティポリシー：当該法人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。情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。

・情報セキュリティ実施手順等：ポリシーには含まれないものの、対策基準に定められた内容を具体的な情報システム又は業務において、どのような手順に従って実行していくのかを示すもの。

・インシデント：インシデントとは、英語で「出来事」「事変」などを意味する語である。特に情報セキュリティの分野では、コンピュータやネットワークのセキュリティを脅かす事象の意味で用いられる。情報セキュリティでは、主に、情報セキュリティが脅かされ重大事故につながるおそれがあった事例をインシデントと呼ぶ。重大事故に至った場合を含むこともある。発生要因が偶発的であったか仕組まれた意図的なものかは問われない。「セキュリティインシデント」や「コンピュータセキュリティインシデント」などとも呼ばれるが、単に「インシデント」と呼ばれることも多い。情報セキュリティ上のインシデントの例として、不正アクセス、不正中継、システムへの侵入、データの改ざん、サービス妨害行為（DoS）などを挙げている。

・マルウェア：マルウェアとは、コンピューターウイルスに代表される、悪意をもったソフトウェアの総称。malware は malicious software（悪意的なソフトウェア）が複合・省略された造語で、ネットワークやコンピューターに何らかの被害をもたらすように設計されたソフトウェアを指す。例えばネットワークを通じてコンピューターに侵入し、データ

破壊や他のコンピューターへの感染、情報の外部への流出などを行うような、害悪をもたらすソフトウェアがマルウェアと呼ばれる。ウイルス、ワーム、スパイウェア、あるいは一部のアドウェアなどがマルウェアに該当する。