学校法人関西外国語大学　情報セキュリティ基本方針

〔 2021 年 6 月 26 日 制定 〕

１．目的

本基本方針は、学校法人関西外国語大学（以下、「本学」）が保有する情報資産の機密性、完全性及び可用性を維持するため、本学が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２．用語の定義

（1）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。

（2）情報システム

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

（3）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。

（4）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（6）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（7）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（8）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（9）通信経路の分割

本学内接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

３．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施す

る。

（1）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

４．適用範囲

（1）対象者の範囲

本基本方針の対象者は、本学情報システムを運用・管理するすべての者、並びに本学情報システムの利用者とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③教職員が作成した大学業務に関連する紙媒体（手書きの資料、メモ等を含む。）

④情報システムの仕様書及びネットワーク図等のシステム関連文書

５．情報セキュリティ対策基準と情報セキュリティ実施手順の策定

下記6，8 及び 9 に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準と、その情報セキュリティ対策基準に基づいた、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。

なお、情報セキュリティ対策基準と情報セキュリティ実施手順は、公にすることにより本学の運営に重大な支障を及ぼすおそれがあることから非公開とする。

６．情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（1）組織体制の構築

本学の情報セキュリティ対策の推進及び管理、並びに情報資産の有効活用及びセキュリティの確保を実現するための組織・体制を整備する。

（2）情報資産の分類と管理

本学で取り扱う情報について、情報の重要度の観点から格付けをすることとし、その重要度に応じた情報の分類とその取扱制限の指定並びに明示等の規定を整備する。

（3）物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び利用者等のパソコン等の管理について、物理的な対策を講じる。

（4）人的セキュリティ

情報セキュリティに関し、利用者等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（5）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（6）運用

情報システムの監視や情報セキュリティポリシーの遵守状況の確認等、情報セキュリティポリシーの運用面の対策を講じる。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を整備する。

（7）外部委託

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

（8）クラウドサービス等の利用

約款によるクラウドサービスを利用する場合には、利用にかかる規定を整備し対策を講じる。ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

7．利用者等の遵守義務

教職員、学生及び本学の情報システムを利用する者（以下「利用者等」という。）は、情報セキュリティの重要性について共通の認識を持ち、情報資産の利用に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

8．情報セキュリティ自己点検及び監査の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ自己点検及び監査を実施する。

9．情報セキュリティポリシーの見直し

情報セキュリティ自己点検及び監査の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が

必要になった場合には、情報セキュリティポリシーを見直す。

附　則

この基本方針は、2021年6月26日から施行する。　(2021年6月26日制定)