

情報セキュリティ基本方針

2002年10月11日 理事会 決定

1. 前文

学校法人関西学院（以下「本学院」という。）は、本学院が所有し管理する情報システム・関連設備、プログラム及びデータ等、すべての情報資産について、適切なセキュリティを保障する義務と責任を有する。また、本学院の全構成員とシステム・ネットワークの利用を許可された者も同様に、情報資産の使用権限に応じてセキュリティ管理の義務と責任を負うものとする。

2. 定義と役割

1) 情報セキュリティの定義

情報セキュリティとは「情報の機密性・完全性・可用性を実現するために情報資産を維持・管理すること」と定義され、以下に掲げる情報資産の損失や漏えいなどを招く潜在的原因からそれらを保護することである。

保護されるべき情報資産

情報資産とは、本学院が組織として管理すべき情報及びそれを管理する仕組みの総称(クラウドサービス含む)

- ・ コンピュータ及び情報通信施設・設備
- ・ コンピュータの周辺機器
- ・ 関連物品、及びデータ記憶メディア
- ・ システムプログラム及び関連文書
- ・ アプリケーションプログラム及び関連文書
- ・ データ
- ・ 本学院が調達、又は開発した情報システムの設計や運用管理に関する情報
- ・ 電磁的記録媒体に記録した情報並びにこれらを印刷した文書

これらの損失や漏えいなどを招く潜在的原因を「脅威」とする。これらの脅威には人為的もしくは自然発生的、偶発的、故意によるものが含まれる。

2) 情報セキュリティポリシーの役割

情報セキュリティポリシーは、本学院における情報セキュリティの方針を示すものである。これは、本学院の全構成員とシステム・ネットワークの利用を許可された者が遵守すべきものであり、本学院の情報資産の保護を目的としている。したがって、本学院のすべての構成員とシステム・ネットワークの利用を許可された者は、情報資産の使用権限に応じてセキュリティ管理についての義務と責任を負わなければならない。

3. 適用範囲

情報セキュリティポリシーは、本学院が所有するすべての情報資産を対象とし、本学院の情報システムを利用するすべての構成員及びシステム・ネットワークの利用を許可された者に適用される。

4. 構成

本学院の情報セキュリティポリシーは、「情報セキュリティ基本方針(本文書)」(以下「基本方針」という。)と複数の「基準とガイドライン」から構成される。

1) 関西学院情報セキュリティポリシー

「基本方針」と各「基準とガイドライン」を総称して「関西学院情報セキュリティポリシー」とする。

2) 基準とガイドライン

一般ユーザ及びシステム管理者が情報セキュリティへの責任を果たすための情報セキュリティ基本方針の附則であり、情報セキュリティ基本方針を詳細に定義しているものである。

5. 管理体制

1) 情報セキュリティ管理体制

本学院の情報セキュリティ対策を推進するために情報セキュリティ管理統括責任者（以下「統括責任者」という。）及び情報セキュリティ管理総括責任者（以下「管理総括責任者」という。）を置く。

統括責任者は情報担当理事とし、管理総括責任者は情報化推進機構長とする。

情報セキュリティ総括部署（以下「セキュリティ総括部署」という。）は情報化推進機構とする。

統括責任者は、教育、研究、事務、図書、ネットワークなどの主要システムについて、それぞれ情報セキュリティ管理者（以下「セキュリティ管理者」という。）を置く。また必要に応じて部局毎にセキュリティ管理者を置くことができる。

統括責任者は、情報セキュリティ監査責任者を置く。

管理総括責任者は、情報セキュリティインシデント対応体制を整備し、対策・対応を行う。

各セキュリティ管理者は、必要に応じて、情報セキュリティ担当者（以下「セキュリティ担当者」という。）を置くことができる。

2) 関西学院情報セキュリティポリシーの管理

関西学院情報セキュリティポリシーの作成、管理・運用は、情報化推進機構長が責任をもって行う。

関西学院情報セキュリティポリシーは、法的・社会的要求、予想される危険など、必要に応じて変更する。

「基本方針」の制定及び変更については、情報化推進機構長室会で協議の上、理事長及び学長の承認を得る。

「基準とガイドライン」の策定及び変更については、情報化推進機構長室会で協議の上、情報化推進機構長の承認を得る。

6. 遵守義務と責任及び罰則

1) 遵守義務と責任

・ユーザ

すべてのユーザは、関西学院情報セキュリティポリシーの関連項目に精通し、情報資産の利用にあたって、これを遵守しなければならない。また、関連する法令・学院諸規程を遵守し、これに従わなければならない。

すべてのユーザは、情報セキュリティに関する問題が発生した場合には、速やかにセキュリティ担当者もしくは、セキュリティ管理者に報告しなければならない。

個人研究室、共同研究室等で教職員ユーザ自らが直接管理する情報資産については、各自がそのセキュリティに関する責任を負わなければならない。

・情報セキュリティ統括責任者

全学院の見地から、本学院の情報セキュリティの維持・向上に努め、セキュリティ対策を立案・推進する。

・情報セキュリティ管理総括責任者

セキュリティ統括責任者を補佐し、本学院の情報セキュリティの実際的な維持と、具体的なセキュリティ対策を立案・推進する。またセキュリティインシデント対応体制を整備し、対策・対応を行う。

・情報セキュリティ総括部署

関西学院情報セキュリティポリシーの維持及びセキュリティ対策を企画、推進する。また、情報セキュリティ教育の推進及び啓発を行う。

・情報セキュリティ管理者

情報セキュリティ総括部署と協力し、セキュリティ確保のための技術導入、セキュリティ対策の立案・推進、管理規程の策定等を行い、情報セキュリティの維持・向上を行う。

- ・情報セキュリティ担当者

セキュリティ管理者と協力し、セキュリティ対策の推進と関西学院情報セキュリティポリシーの徹底と普及をはかり、情報セキュリティの維持・向上を行う。

2) 違反者に対する措置

関西学院情報セキュリティポリシーの違反者に対しては、ネットワーク利用倫理規程に基づき、相当の措置をとることができるものとする。

7. 例外措置

情報セキュリティが脅威に晒された場合には、そのセキュリティリスク及び損失等を最小化するためにセキュリティ管理者が行った行為について、その遵守義務を免除することがある。

また、関西学院情報セキュリティポリシーの遵守によって、その損失等が避けられない場合については、セキュリティ統括責任者の許可の下に、その改善措置がとられるまでの時限的例外措置を設定することができる。

これらの場合には、情報化推進機構長室会に顛末が報告されなければならない。

【用語の定義】

- ・情報の機密性 (confidentiality)

第三者に情報が漏れないようにすること。

情報へ権限のない者のアクセスを許さず、情報が正規の方法で承認を受けた者にのみ開示されること。

- ・情報の完全性 (integrity)

情報が正確かつ完全に維持されること。

情報及び情報システムやプログラム等が規程に基づき承認を受けた方法でのみ変更されること。

- ・情報の可用性 (availability)

許可された利用者が、必要な時に情報にアクセスできる状態を確保すること。

障害の発生等で情報及び情報システムが利用できないような状態に置かないこと。

- ・ユーザ

本学院の情報資産を利用するすべての者。

附 則

1 この基本ポリシーは 2020 年（令和 2 年） 4 月 1 日から改正施行する

2 この基本ポリシーは基本方針と名称を変更し、2021 年（令和 3 年）4 月 1 日から改正施行する。

以 上