【2022 年 4 月現在】

関西学院ネットワーク利用倫理規程

（目的）
第１条　この規程は、学校法人関西学院における教育研究及びこれらに関する業務を推進するために、本学院が設置するネットワーク及びネットワークに接続されている機器（以下、総称して「システム」という。）を利用する場合に必要な倫理事項を定めることを目的とする。
（システム管理者）
第２条　利用倫理に関する統括的なシステム管理者は、ネットワーク管理者とし、情報化推進機構長がその任にあたる。
（不正利用）
第３条　次の各号に該当する事項をシステムの不正利用とし、システム利用者は、これらの行為を行ったり、または事態を招いたりしてはならない。
1　本学院のシステムに損害もしくは不利益を与える行為または事態
2　前号の行為を行う旨脅迫する行為または事態
3　公与良俗・建学の精神に反する行為または事態
4　本学院のシステムを利用した営利を目的とする商行為または事態
5　他者に損害もしくは不利益を与える行為または事態
6　他者の人権を侵害する行為または事態
7　法令に違反する行為または事態
8　学内の諸規程・関西学院情報セキュリティポリシーに違反する行為または事態
9　その他、システム管理者が不正利用に相当すると認めた行為または事態
２　前各号に該当する不正利用があり、緊急の措置をとる必要があるとシステム管理者が認めた場合、システム管理者は、関係する機器のネットワークからの切断、行為者のシステム利用停止等の措置をとることができる。
（ネットワーク調査委員会）
第４条　本学院にネットワーク調査委員会（以下「調査委員会」という。）を置く。
２　調査委員会は、前条に規定する不正利用が発生した場合、その状況を調査し、第６条に規定するネットワーク倫理委員会委員長へ報告・提言を行う。
３　前項の調査の結果、不正利用の内容・程度が軽微な場合、情報化推進機構長は、調査委員会からの勧告に基づき、所属長と協議の上、本人への警告、システムの一定期間の利用停止等、行為者に対する措置をとることができる。
第５条　調査委員会は次の委員をもって構成し、情報化推進機構副機構長１名がコンビーナを務める。
1　情報化推進機構副機構長　３名以内
2　学長補佐　１名
3　広報室長
4　調査委員会コンビーナが委嘱した教職員　若干名
２　不正利用の内容により調査委員会が必要と認めた場合は、前項に規定する者のほかに委員を追加することができる。
（ネットワーク倫理委員会）
第６条　本学院にネットワーク倫理委員会（以下「倫理委員会」という。）を置く。
２　倫理委員会は、調査委員会からの報告・提言に基づき、不正利用等システムの利用倫理に関して協議を行う。
３　倫理委員会は、不正利用の軽重によって行為者に対し次の措置を決定することができる。
1　所属長への懲戒の勧告
2　その他相当と認められる処分
第７条　倫理委員会は次の委員をもって構成し、副理事長（学長）がコンビーナを務める。
1　副理事長（学長）
2　情報化推進機構長
3　各学部長、専門職大学院各研究科長及び言語コミュニケーション文化研究科委員長
4　大学図書館長
5　短期大学学長
6　高等部長

7　中学部長
8　初等部校長
9　千里国際中等部・高等部校長
10　大阪インターナショナルスクール校長
11　人事部長
12　情報化推進機構副機構長　３名以内
２　倫理委員会が必要と認めた場合は、前項に規定する者のほかに委員を追加することができる。
（プライバシーの保護）
第８条　調査委員会、倫理委員会の委員及び業務担当者は、プライバシーの保護に努めるとともに、職務上知り得たことを他に漏らしてはならない。
（事務局）
第９条　この規程に関する事務は、情報化推進機構が行う。
（規程の改廃）
第10条　この規程の改廃は、倫理委員会及び情報化推進機構長室会の議を経て常務委員会で決定する。

附　則
1　この規程は1996年（平成8年）12月13日から施行する。
略
12　この規程は、2021年（令和３年）4月1日から改正施行する。

情報セキュリティ基本方針

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

全学院的見地から、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。