【2026 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。

関西学院 情報セキュリティポリシー

学校法人関西学院は、構成員が安心・安全にICT環境を利用できるよう、情報セキュリティに関する基本方針（情報セキュリティ基本方針）と対策基準（情報セキュリティ対策基準）からなる「情報セキュリティポリシー」を整備する。

目次

【情報セキュリティ基本方針】 3
第1章 総則 3
第2章 義務・罰則 3
第3章 例外措置 4
第4章 組織・体制 4
【情報セキュリティ対策基準】 6
第1章 総則 6
第2章 運用 6
第1節 情報セキュリティ関係規程の運用 6
第2節 違反への対処 6
第3節 例外措置 7
第4節 教育 7
第5節 情報セキュリティインシデントへの対処 7
第3章 点検・見直し 9
第1節 情報セキュリティ対策の自己点検 9
第2節 情報セキュリティ監査 9
第3節 情報セキュリティ対策の見直し 10
第4章 情報の取扱い 10
第1節 情報の取扱い 10
第2節 情報を取り扱う区域の管理 13
第5章 外部委託 14
第1節 外部委託 14
第2節 約款による外部サービスの利用 15
第3節 ソーシャルメディアサービスによる情報発信 15
第4節 クラウドサービスの利用 16
第6章 情報システムのライフサイクルの各段階における対策 16
第1節 情報システムに係る文書等の整備 16
第2節 情報システムの企画・要件定義 16
第3節 情報システムの調達・構築 17
第4節 情報システムの運用・保守 17
第5節 情報システムの更改・廃棄 18

第6節 情報システムについての対策の見直し 18
第7章 情報システムの運用継続計画 18
第1節 情報システムの運用継続計画の整合的運用の確保 18
第8章 情報システムのセキュリティ機能 18
第1節 主体認証機能 18
第2節 アクセス制御機能 19
第3節 権限の管理 19
第4節 ログの取得・管理 19
第5節 通信の監視・利用記録 20
第6節 暗号・電子署名 21
第9章 情報システムの脅威への対策 21
第1節 ソフトウェアに関する脆弱性対策 21
第2節 不正プログラム対策 21
第3節 サービス不能攻撃対策 22
第4節 標的型攻撃対策 22
第10章 アプリケーション・コンテンツの作成・提供 22
第1節 アプリケーション・コンテンツ作成時の対策 22
第2節 アプリケーション・コンテンツ提供時の対策 23
第11章 端末・サーバ装置等 23
第1節 端末 23
第2節 サーバ装置 24
第3節 複合機・特定用途機器 25
第12章 電子メール・ウェブ等 25
第1節 電子メール 25
第2節 ウェブ 25
第3節 ドメインネームシステム（DNS） 26
第4節 データベース 26
第13章 通信回線 27
第1節 通信回線 27
第14章 情報システムの利用 29
【本ポリシーの改廃】 31
附 則 31

【情報セキュリティ基本方針】

第1章 総則

（目的及び方針）

第1条 学校法人関西学院（以下「本学院」という。）の教育、研究、その他の活動を行うにあたっては、情報システムの活用にあわせて、情報資産を損失や漏えいなどのセキュリティの脅威から保全することが必要不可欠である。そのため、本学院の全ての構成員及び関係者は、情報資産の価値と保全の重要性を認識し、本学院の保有する情報の機密性、完全性及び可用性の維持に努めなければならない。情報セキュリティ水準の適切な維持のため、本学院は「情報セキュリティ基本方針」（以下「本基本方針」という。）及び「情報セキュリティ対策基準」からなる「関西学院情報セキュリティポリシー」（以下「本ポリシー」という。）を定め、以下の対策を行う。

1 情報セキュリティ対策の実施体制の整備
2 情報及び情報システムの保護
3 情報システムのセキュリティの維持
4 情報セキュリティインシデントへの対処
5 利用者への啓発・教育
6 前各号に掲げるものを含む情報セキュリティマネジメントの実施

（適用範囲）

第2条 本ポリシーにおいて適用対象とする者は、本学院の情報システムを運用・管理する全ての者、並びに利用者及び臨時利用者とする。

2 本ポリシーにおいて適用対象とする情報は、次に掲げる情報とする。

1 本学院が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報を含む。）
2 その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報を含む。）であって、教職員等が職務上取り扱う情報
3 前各号に掲げるもののほか、本学院が調達し、又は開発した情報システムの設計又は運用管理に関する情報

3 本ポリシーにおいて適用対象とする情報システムは、本基本方針の適用対象となる情報を取り扱う全ての情報システム及び学内通信回線に接続する全ての情報システムとする。

（用語定義）

第3条 本基本方針における用語の定義は、別に定める。

第2章 義務・罰則

（義務）

第4条 本学院の情報及び本学院で扱う情報システムを利用する者、並びに管理・運用の業務に携わる者は、本ポリシー及びその他の規程等を遵守しなければならない。

（罰則）

第5条 本ポリシーに基づき定められる規程等に違反した場合の利用の制限および罰則は、本学院が定める就業規則及びネットワーク利用倫理規程に則って行うほか、それぞれの規程に定めるところによる。

第3章 例外措置

（例外措置）

第6条 本ポリシーを遵守することが困難な状況で、本学院の業務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、別に定める手続きに従い例外措置をとることができるものとする。

第4章 組織・体制

（最高情報セキュリティ責任者（CISO））

第7条 本学院における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者（以下「CISO」という。）を置く。情報担当理事をもってこれに充てる。

2 CISOは、次に掲げる事務を統括する。

1 情報セキュリティ対策推進のための組織・体制の整備
2 情報セキュリティインシデントに対処するために必要な指示その他の措置
3 前各号に掲げるもののほか、情報セキュリティに関する重要事項

（情報セキュリティ監査責任者）

第8条 CISOは、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者を置くものとする。

（統括情報セキュリティ責任者の設置）

第9条 CISOを補佐する者として、統括情報セキュリティ責任者を置く。情報化推進機構長をもってこれに充てる。

2 統括情報セキュリティ責任者は、次の事務を統括する。

1 情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務
2 情報セキュリティ対策に係る教育の推進及び当該実施体制の整備
3 情報セキュリティインシデントに対処するための緊急連絡窓口等の整備
4 情報セキュリティインシデントに係る理事会への報告
5 前各号に掲げるもののほか、情報セキュリティ対策に係る事務

（情報セキュリティ統括部署）

第10条 情報化推進機構を情報セキュリティ統括部署とする。

2 情報セキュリティ統括部署は、統括情報セキュリティ責任者の指示により、統括情報セキュリティ責任者の管轄する事務の実務を担当する。

（部局情報セキュリティ責任者の設置）

第11条 部局の情報セキュリティ対策に関する事務を統括する部局情報セキュリティ責任者を置く。当該部局の長をもってこれに充てる。

2 部局情報セキュリティ責任者は、所管する部局における情報セキュリティ対策を推進するため、次の事務を統括する。

1 部局の職場情報セキュリティ責任者の設置

2 情報システムごとの個別情報システム責任者の設置

3 情報セキュリティインシデントの原因調査、再発防止策等の実施

4 前各号に掲げるもののほか、部局の情報セキュリティ対策に関する事務

（職場情報セキュリティ責任者の設置）

第12条 部局情報セキュリティ責任者は、教室、研究室、事務室等の管理組織単位ごとに情報セキュリティ対策に関する事務を統括する職場情報セキュリティ責任者を置くものとする。

2 職場情報セキュリティ責任者は、部局情報セキュリティ責任者の下で、教室、研究室、事務室等の管理組織単位における情報の取扱いその他の情報セキュリティ対策に関する事務を統括する。

（個別情報システム責任者の設置）

第13条 部局情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、個別情報システム責任者を、当該情報システムの企画に着手するまでに選任しなければならない。

2 個別情報システム責任者は、情報システムにおける情報セキュリティ対策に関する事務を担う。

3 個別情報システム責任者は、所管する情報システムの管理業務において必要な単位ごとに個別情報システム担当者を置くものとする。

（情報セキュリティアドバイザーの設置）

第14条 CISOは、情報セキュリティについて専門的な知識及び経験を有する者を情報セキュリティアドバイザーとして置くことができる。

（情報セキュリティインシデントに備えた体制の整備）

第15条 CISOは、CSIRTを整備し、円滑に活動が行えるよう環境を整備しなければならない。

2 CISOは、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備するものとする。

3 CISOは、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築するものとする。

4 部局情報セキュリティ責任者は、本学CSIRTと連携して、情報セキュリティインシデントの発生に備えた連絡、報告、情報集約及び被害拡大防止のための緊急対応に必要な体制を整備しなければならない。

（兼務を禁止する役割）

第16条 教職員等は、情報セキュリティ対策の運用において、以下の役割を兼務してはならない。

1 承認又は許可の申請者と当該承認を行う者（CISOと統括情報セキュリティ責任者はその限りでない）

2 監査を受ける者とその監査を実施する者

【情報セキュリティ対策基準】

第1章 総則

2101-1（趣旨）

第1条 この基準は、「情報セキュリティ基本方針」に基づき、学校法人関西学院（以下「本学院」という。）における適切な情報セキュリティ対策に関する基準について必要な事項を定める。

2101-2（適用範囲）

第2条 本基準において適用対象とする者は、本学院の情報システムを運用・管理する全ての者、並びに利用者及び臨時利用者とする。

2101-3（定義）

第3条 この基準における用語の意義は、別に定める。

第2章 運用

第1節 情報セキュリティ関係規程の運用

2101-4（情報セキュリティ対策に関する実施手順の整備・運用）

第4条 統括情報セキュリティ責任者は、本学院における情報セキュリティ対策に関する実施手順を整備し（本基準で整備すべきものを別に定める場合を除く。）、実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者（以下「CISO」という。）に報告しなければならない。

2 部局情報セキュリティ責任者又は職場情報セキュリティ責任者は、利用者等より情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告しなければならない。

3 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じてCISOにその内容を報告しなければならない。

第2節 違反への対処

2101-5（違反への対処）

第5条 利用者等は、情報セキュリティ関係規程への重大な違反を知った場合は、部局情報セキュリティ責任者又は職場情報セキュリティ責任者にその旨を報告しなければならない。

2 部局情報セキュリティ責任者及び職場情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、統括情報セキュリティ責任者に報告しなければならない。

2101-6（違反に対する措置）

第6条 統括情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合には、「関西学院ネットワーク利用倫理規程」に基づき取り扱うものとする。

2 統括情報セキュリティ責任者及び部局情報セキュリティ責任者は、緊急の必要があると認める場合には、前項による措置が決定するまでの間、必要最小限の範囲で以下の措置を講ずることができる。
1 当該行為者に対する当該行為の中止命令
2 個別情報システム責任者に対する当該行為に係る情報発信の遮断命令
3 個別情報システム責任者に対する当該行為者のアカウント停止・削除命令、データやログの保全命令

3 部局情報セキュリティ責任者は、前項第2号及び第3号については、他部局の部局情報セキュリティ責任者を通じて同等の措置を依頼することができる。

4 部局情報セキュリティ責任者は、第2項の措置を講じた場合には、統括情報セキュリティ責任者にその旨を報告しなければならない。

第3節 例外措置

2101-7（例外措置手続の整備）

第7条 統括情報セキュリティ責任者は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び審査手続を定めるものとする。

2101-8（例外措置の運用）

第8条 利用者等は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請しなければならない。ただし、教育・研究・事務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出なければならない。

2 許可権限者は、利用者等による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定しなければならない。

第4節 教育

2101-9（教育体制等の整備）

第9条 統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、定期的に実施するための計画を策定し、その実施体制を整備しなければならない。

2101-10（教育の実施）

第10条 職場情報セキュリティ責任者は、利用者等に対して、情報セキュリティに係る教育を適切に受講させなければならない。

2 利用者等は、指示に従って、適切な時期に教育を受講しなければならない。

第5節 情報セキュリティインシデントへの対処

2101-11（本学院CSIRTの役割）

第11条 CSIRTは、次に掲げる業務を行うものとする。
1 本学院における情報セキュリティインシデントの報告窓口として、学内外からの情報セキュリティイン

シデントの可能性のある事象に関する情報を受け付けるとともに、本学院情報ネットワークの監視に関する情報も活用することにより、情報セキュリティインシデントに関する事象の正確な把握に努める。

2 情報セキュリティインシデントに関する外部機関との連絡窓口機能を、広報等の関係部局と連携して提供する。

3 情報セキュリティインシデントの発生時に、必要に応じて被害の拡大防止、復旧及び再発の防止にかかる技術的支援や助言を行う。

2101-12（情報セキュリティインシデントに備えた事前準備）

第12条 統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性を認知した際の報告窓口を含む本学院関係者への報告手順を整備し、利用者等に周知しなければならない。

2 統括情報セキュリティ責任者は、情報セキュリティインシデントを認知した際の学院外との情報共有を含む対処手順を整備しなければならない。

3 統括情報セキュリティ責任者は、情報セキュリティインシデントの可能性に備え、教育・研究・事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段を含む緊急連絡網を整備しなければならない。

4 統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、教育・研究・事務の遂行のため特に重要と認めた情報システムについては、訓練を実施しなければならない。

5 統括情報セキュリティ責任者は、情報セキュリティインシデントについて学外の者から報告を受けるための窓口（CSIRT）を整備し、その窓口への連絡手段を学外の者に明示しなければならない。

2101-13（情報セキュリティインシデントへの対処）

第13条 利用者等は、情報セキュリティインシデントの可能性を認知した場合には、本学院の報告窓口に報告し、指示に従わなければならない。

2 CSIRTは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行うものとする。

3 CSIRT責任者は、情報セキュリティインシデントであると評価した場合、CISOに速やかに報告しなければならない。

4 CSIRTは、情報セキュリティインシデントに関係する部局情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示又は勧告を行うものとする。

5 個別情報システム責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、本学院で定められた対処手順又はCSIRTの指示若しくは勧告に従って、適切に対処しなければならない。

6 CSIRTは、本学院の情報システムについて、情報セキュリティインシデントを認知した場合において、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うものとする。

7 CSIRTは、情報セキュリティインシデントに関する対処状況を把握し、必要に応じて対処全般に関する指示、勧告又は助言を行うものとする。

8 CSIRTは、情報セキュリティインシデントに関する対処の内容を記録しなければならない。

9 CSIRTは、情報セキュリティインシデントに関して、本学院を含む関係機関と情報共有を行うものとする。

2101-14（情報セキュリティインシデントの再発防止・教訓の共有）

第14条 部局情報セキュリティ責任者は、CSIRTから応急措置の実施及び復旧に係る指示又は勧告を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、統括情報セキュリティ責任者に報告しなければならない。

2 統括情報セキュリティ責任者は、部局情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示するものとする。

3 CSIRT責任者は、情報セキュリティインシデント対処の結果から得られた教訓を、統括情報セキュリティ責任者、関係する部局情報セキュリティ責任者等に共有するものとする。

第3章 点検・見直し

第1節 情報セキュリティ対策の自己点検

2101-15（自己点検の実施）

第15条 利用者等は、各々が責を負う情報セキュリティ対策について、定期的に自己点検を実施するものとする。

2101-16（自己点検結果の評価・改善）

第16条 利用者等は、自己点検において問題を認めた場合には、改善又は例外措置の申請を行わなければならない。

第2節 情報セキュリティ監査

2101-17（監査計画の策定）

第17条 情報セキュリティ監査責任者は、情報セキュリティ監査計画を策定し、CISOの承認を得るものとする。

2101-18（情報セキュリティ監査の実施に関する指示）

第18条 CISOは、情報セキュリティ監査計画に従って、情報セキュリティ監査責任者に対して、監査の実施を指示するものとする。

2 CISOは、情報セキュリティの状況の変化に応じて必要と判断した場合、情報セキュリティ監査責任者に対して、情報セキュリティ監査計画で計画された事案以外の監査の実施を指示するものとする。

2101-19（情報セキュリティ監査の実施）

第19条 情報セキュリティ監査を実施する者は、情報セキュリティ監査責任者の指示に基づき、監査実施手順に従って監査を実施するものとする。

2 情報セキュリティ監査を実施する者は、必要に応じて、情報システムへのアクセス権限を付与され、監査調書を作成し、あらかじめ定められた期間保存するものとする。

3 情報セキュリティ監査責任者は、監査調書に基づき監査報告書を作成し、CISOへ提出するものとする。

2101-20（情報セキュリティ監査結果に対する対応）

第20条 CISOは、監査報告書の内容を踏まえ、被監査部局の部局情報セキュリティ責任者に対して、指摘事案に対する対応の実施を指示するものとする。

2 CISOは、監査報告書の内容を踏まえ、監査を受けた部局以外の部局においても同種の課題及び問題点がある可能性が高く、かつ緊急に同種の課題及び問題点があることを確認する必要があると判断した場合には、他の部局の部局情報セキュリティ責任者に対しても、同種の課題及び問題点の有無を確認するように指示するものとする。

3 部局情報セキュリティ責任者は、監査報告書に基づいてCISOから改善を指示された事案について、対応計画を作成し、報告するものとする。

4 CISOは、監査の結果を踏まえ、本ポリシー及び関連規程に基づく既存の手順の妥当性を評価し、必要に応じてその見直しを指示するものとする。

第3節 情報セキュリティ対策の見直し

2101-21（情報セキュリティ関係規程の見直し）

第21条 統括情報セキュリティ責任者は、情報セキュリティに係る重大な変化等を踏まえ、本ポリシー及びそれに基づく規程等について必要な見直しを行わなければならない。

第4章 情報の取扱い

第1節 情報の取扱い

2101-22（情報の格付け）

第22条　教職員等が取り扱う情報の格付けの区分及び分類の基準は、機密性、完全性、可用性について、それぞれ次の各号のとおりとする。

1 機密性についての格付けの区分及び分類の基準

格付けの区分	分類の基準
機密性3情報	本学院で取り扱う情報のうち、秘密保全の必要が高く、その漏えいが本学院の利益に甚大な損害を与えるおそれのある情報又は本学院の信頼を大きく失墜させるおそれのある情報を含む情報
機密性2情報	本学院で取り扱う情報のうち、その漏えいにより関係者の権利が侵害される又は本学院の活動の遂行に支障を及ぼすおそれがある情報であって、「機密性3情報」以外の情報
機密性1情報	機密性3情報又は機密性2情報以外の情報

2 完全性についての格付けの区分及び分類の基準

格付けの区分	分類の基準
完全性2情報	本学院で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、関係者の権利が侵害され又は本学院活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性1情報	完全性2情報以外の情報（書面を除く。）

3 可用性についての格付けの区分及び分類の基準

格付けの区分	分類の基準
可用性2情報	本学院で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、関係者の権利が侵害され又は本学院活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。
可用性1情報	可用性2情報以外の情報（書面を除く。）

2 前項第1号に規定する格付けの区分のうち、機密性2情報及び機密性3情報を「要機密情報」という。

3 第1項第2号に規定する格付けの区分のうち、完全性2情報を「要保全情報」という。

4 第1項第3号に規定する格付けの区分のうち、可用性2情報を「要安定情報」という。

5 第2項、第3項及び第4項に規定する要機密情報、要保全情報及び要安定情報を「要保護情報」という。

2101-23（取扱制限の種類）

第23条 情報の取扱制限の種類及び指定方法は、機密性、完全性、可用性について、それぞれ次の各号のとおりとする。

1 機密性についての取扱制限の種類及び指定方法

取扱制限の種類	指定方法
複製について	複製禁止、複製要許可
配付について	配付禁止、配付要許可
暗号化について	暗号化必須、保存時暗号化必須、通信時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り
期限について	○月○日まで○○禁止

2 完全性についての取扱制限の種類及び指定方法

取扱制限の種類	指定方法
保存期間について	○○まで保存
保存場所について	○○において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

3 可用性についての取扱制限の種類及び指定方法

取扱制限の種類	指定方法
復旧までに許容できる時間について	○○以内復旧
保存場所について	○○において保存

2101-24（情報の目的外での利用等の制限）

第24条 教職員等は、自らが担当している教育・研究・事務の遂行以外の目的で、情報を利用等してはならない。

2101-25（格付け及び取扱制限の決定）

第25条　教職員等は、情報の作成時又は情報を入手しその管理を開始する時に、当該情報について、電磁的記録については機密性、完全性、可用性の観点から、書面については機密性の観点から、格付け及び取扱制限の定義に基づき、その決定を行うものとする。

2101-26（格付け及び取扱制限の指定）

第26条 教職員等は、前条の規定により決定した格付け及び取扱制限に基づき、その指定を行うものとする。

2101-27（格付け及び取扱制限の明示等）

第27条 教職員等は、情報の格付け及び取扱制限を指定した場合には、必要に応じて、それを認識できる方法を用いて明示等するものとする。

2101-28（格付け及び取扱制限の継承）

第28条 教職員等は、情報を作成する際に、参照した情報又は入手した情報が既に本学院内において格付け又は取扱制限の指定がなされている場合には、元となる情報の機密性に係る格付け及び取扱制限を継承又は参酌しなければならない。

2101-29（格付け及び取扱制限の見直し）

第29条 教職員等は、指定した情報の格付け及び取扱制限を見直す必要があると認めた場合には、第25条及び第26条の規定に準じて処理するものとする。

2 教職員等は、情報の格付け及び取扱制限を変更した場合には、その以前に当該情報を参照した者に対して、その旨を可能な限り周知し、同一の情報が異なる格付け及び取扱制限とならないように努めるものとする。

2101-30（情報の利用・保存）

第30条 教職員等は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱わなければならない。

2 教職員等は、機密性3情報について要管理対策区域外で情報処理を行う場合は、個別情報システム責任者及び職場情報セキュリティ責任者の許可を得なければならない。

3 教職員等は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講じなければならない。

4 教職員等は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理しなければならない。

5 教職員等は、USBメモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、必要な安全措置を講じ

なければならない。

2101-31（情報の提供・公表）

第31条 教職員等は、情報を公表する場合には、当該情報が機密性1情報に格付されるものであることを確認しなければならない。

2 教職員等は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従わなければならない。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講じなければならない。

3 教職員等は、機密性3情報を閲覧制限の範囲外の者に提供する場合には、部局情報セキュリティ責任者又は職場情報セキュリティ責任者の許可を得なければならない。

4 教職員等は、電磁的記録を提供又は公表する場合には、当該電磁的記録等からの不用意な情報漏えいを防止するための措置を講じなければならない。

2101-32（情報の運搬・送信）

第32条 教職員等は、要保護情報が記録又は記載された記録媒体を要管理対策区域外に持ち出す場合には、安全確保のための適切な措置を講じなければならない。

2 教職員等は、要保護情報である電磁的記録を電子メール等、ネットワークを経由して送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講じなければならない。

2101-33（情報の消去）

第33条 教職員等は、端末や電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去しなければならない。

2 教職員等は、端末や電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消しなければならない。

3 教職員等は、要機密情報である書面を廃棄する場合には、復元できない状態にしなければならない。

2101-34（情報のバックアップ）

第34条 教職員等は、情報の格付に応じて、適切な方法で情報のバックアップを実施しなければならない。

2 教職員等は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理しなければならない。

3 教職員等は、保存期間を過ぎた情報のバックアップについては、前条の規定に従い、適切な方法で消去、抹消又は廃棄しなければならない。

第2節 情報を取り扱う区域の管理

2101-35（要管理対策区域における対策の決定）

第35条 部局情報セキュリティ責任者は、要管理対策区域の範囲を定めるものとする。

2 部局情報セキュリティ責任者は、施設及び環境に係る対策を行う単位ごとの区域を定めるものとする。

3 部局情報セキュリティ責任者は、各区域について、周辺環境や当該区域で行う教育・研究・事務の内容、

取り扱う情報等を勘案し、以下の観点を含めて当該区域において実施する対策を決定しなければならない。

1 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。

2 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。

2101-36（要管理対策区域における対策の実施）

第36条 利用者等は、利用する区域について部局情報セキュリティ責任者が定めた対策に従って利用しなければならない。また、利用者等が学外の者を立ち入らせる際には、当該学外の者にも当該区域で定められた対策に従って利用させなければならない。

第5章 外部委託

第1節 外部委託

2101-37（外部委託に係る契約内容の精査）

第37条 個別情報システム責任者又は職場情報セキュリティ責任者は、本基準及び関連規程の要件を満たしていることを委託先の選定条件とし、以下の内容を契約原案の策定時に確認し又は仕様内容に含めなければならない。

1 委託先に提供する情報の委託先における目的外利用の禁止

2 委託先における情報セキュリティ対策の実施内容及び管理体制

3 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制

4 委託事業の実施場所、情報システムの設置場所に関する情報提供（個人情報を取り扱う場合は国内法令が適用されること）

5 情報セキュリティインシデントへの対処方法

2 個別情報システム責任者又は職場情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めなければならない。

1 情報セキュリティ監査の受入れ

2 サービスレベルの保証

3 個別情報システム責任者又は職場情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、第1項及び前項の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本学院に提供し、本学院の承認を受けるよう、仕様内容に含めなければならない。

2101-38（外部委託における対策の実施）

第38条 個別情報システム責任者又は職場情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認しなければならない。

2 個別情報システム責任者又は職場情報セキュリティ責任者は、委託した業務において、情報セキュリテ

ィインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を利用者等より受けた場合は、委託事業を一時中断するなどの必要な措置を講じた上で、契約に基づく必要な措置を講じさせなければならない。

3 個別情報システム責任者又は職場情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認しなければならない。

2101-39（外部委託における情報の取扱い）

第39条 利用者等は、委託先への情報の提供等において、以下の事項を遵守しなければならない。

1 委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。

2 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。

3 委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに個別情報システム責任者又は職場情報セキュリティ責任者に報告すること。

第2節 約款による外部サービスの利用

2101-40（約款による外部サービスの利用における対策の実施）

第40条 利用者等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認し、適切な措置を講じた上で約款による外部サービスを利用できるものとする。ただし、要保護情報を取り扱う場合は、部局情報セキュリティ責任者又は職場情報セキュリティ責任者の許可を得なければならない。

2 部局情報セキュリティ責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定めなければならない。

3 利用者等は、約款による外部サービスの利用において要機密情報を取り扱ってはならない。

第3節 ソーシャルメディアサービスによる情報発信

2101-41（ソーシャルメディアサービスによる情報発信時の対策）

第41条 部局情報セキュリティ責任者は、本学院が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めなければならない。

1 本学院のアカウントによる情報発信が実際の本学院のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。

2 パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。

2 部局情報セキュリティ責任者は、本学院において情報発信のためにソーシャルメディアサービスを利用する場合は、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なければならない。

3 利用者等は、ソーシャルメディアサービスにおいて要機密情報を公表してはならない。

4 利用者等は、要安定情報の一般利用者への提供にソーシャルメディアサービスを用いる場合は、必要に応じて本学院の自己管理ウェブサイトに当該情報を掲載して参照可能としなければならない。

第4節 クラウドサービスの利用

2101-42（クラウドサービスの利用における対策）

第42条 個別情報システム責任者は、クラウドサービス（民間事業者が提供するものに限らず、政府等が提供するものを含む。以下同じ。）を利用するに当たり、取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。

2 個別情報システム責任者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。

3 個別情報システム責任者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件としなければならない。

4 個別情報システム責任者は、クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めなければならない。

5 個別情報システム責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

第6章 情報システムのライフサイクルの各段階における対策

第1節 情報システムに係る文書等の整備

2101-43（情報システム関連文書の整備）

第43条 個別情報システム責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる情報システム関連文書を整備しなければならない。

第2節 情報システムの企画・要件定義

2101-44（実施体制の確保）

第44条 導入時に個別情報システム責任者を定めたうえで、個別情報システム責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制が確保されていることを確認した上で、情報システムを導入しなければならない。

2101-45（情報システムのセキュリティ要件の策定）

第45条 個別情報システム責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、構築する情報システムをインターネットや、インターネットに接点を有する情報システム（クラウドサービスを含む。）から分離することの要否を判断した上で、以下の事項を含む情報システムのセキュリティ要件を策定しなければならない。

1 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件

2 情報システム運用時の監視等の運用管理機能要件（監視するデータが暗号化されている場合は、必要に応じて復号すること）

3 情報システムに関連する脆弱性についての対策要件

2 個別情報システム責任者は、インターネット回線と接続する情報システムを構築する場合は、標的型攻撃を始めとするインターネットからの様々なサイバー攻撃による情報の漏えい、改ざん等のリスクを低減するための多重防御のためのセキュリティ要件を策定しなければならない。

3 個別情報システム責任者は、機器等を調達する場合には、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定しなければならない。

2101-46（情報システムの構築を外部委託する場合の対策）

第46条 個別情報システム責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させなければならない。

1 情報システムのセキュリティ要件の適切な実装

2 情報セキュリティの観点に基づく試験の実施

3 情報システムの開発環境及び開発工程における情報セキュリティ対策

2101-47（情報システムの運用・保守を外部委託する場合の対策）

第47条 個別情報システム責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させなければならない。

2 個別情報システム責任者は、情報システムの運用・保守を外部委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、速やかに報告させなければならない。

第3節 情報システムの調達・構築

2101-48（情報システムの構築時の対策）

第48条 個別情報システム責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講じなければならない。

2 個別情報システム責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講じなければならない。

2101-49（納品検査時の対策）

第49条 個別情報システム責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

2 個別情報システム責任者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

第4節 情報システムの運用・保守

2101-50（情報システムの運用・保守時の対策）

第50条 個別情報システム責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用しなければならない。

2 個別情報システム責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理しなければならない。

第5節 情報システムの更改・廃棄

2101-51（情報システムの更改・廃棄時の対策）

第51条 個別情報システム責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講じなければならない。

1 情報システム更改時の情報の移行作業における情報セキュリティ対策

2 情報システム廃棄時の不要な情報の抹消

第6節 情報システムについての対策の見直し

2101-52（情報システムについての対策の見直し）

第52条 個別情報システム責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

第7章 情報システムの運用継続計画

第1節 情報システムの運用継続計画の整合的運用の確保

2101-53（情報システムの運用継続計画の整合的運用の確保）

第53条 部局情報セキュリティ責任者は、本学院において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討しなければならない。

2 部局情報セキュリティ責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認しなければならない。

第8章 情報システムのセキュリティ機能

第1節 主体認証機能

2101-54（主体認証機能の導入）

第54条 個別情報システム責任者は、情報システムや情報へのアクセスを管理するため、主体を特定し、それが正当な主体であることを検証する必要がある場合、主体の識別及び主体認証を行う機能を設けなければならない。

2 個別情報システム責任者は、学内及び外部機関との間の申請、届出等のオンライン手続を提供する情報システムを構築する場合は、オンライン手続におけるリスクを評価した上で、主体認証に係る要件を策定しなければならない。

3 個別情報システム責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講じなければならない。

2101-55（識別コード及び主体認証情報の管理）

第55条 個別情報システム責任者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与し、管理するための措置を講じなければならない。

2 個別情報システム責任者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するための措置を速やかに講じなければならない。

第2節 アクセス制御機能

2101-56（アクセス制御機能の導入）

第56条 個別情報システム責任者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けなければならない。

2 個別情報システム責任者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用しなければならない。

第3節 権限の管理

2101-57（権限の管理）

第57条 個別情報システム責任者は、主体から対象に対するアクセスの権限を適切に設定するよう、措置を講じなければならない。

2 個別情報システム責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。

第4節 ログの取得・管理

2101-58（ログの取得・管理）

第58条 個別情報システム責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得しなければならない。

2 個別情報システム責任者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理しなければならない。

3 個別情報システム責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

第5節 通信の監視・利用記録

2101-59（通信の監視）

第59条 情報システムを運用・管理する者及び利用者等は、ネットワークを通じて行われる通信を傍受してはならない。ただし、統括情報セキュリティ責任者又は当該ネットワークを管理する部局情報セキュリティ責任者は、セキュリティ確保のため、あらかじめ指定した者に、ネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

2 統括情報セキュリティ責任者又は部局情報セキュリティ責任者は、監視の範囲をあらかじめ具体的に定めておかなければならない。ただし、不正アクセス行為又はこれに類する重大なセキュリティ侵害に対処するために特に必要と認められる場合、統括情報セキュリティ責任者又は部局情報セキュリティ責任者は、セキュリティ侵害の緊急性、内容及び程度に応じて、対処のために不可欠と認められる情報について、監視を行うよう命ずることができる。

3 監視を行う者は、監視によって知った通信の内容又は個人情報を、他の者に伝達してはならない。ただし、前項ただし書きに定める情報については、CISO、統括情報セキュリティ責任者及び部局情報セキュリティ責任者に伝達することができる。

4 監視によって採取された記録（以下「監視記録」という。）は要機密情報、要保全情報、要安定情報とし、監視を行わせる者を情報の作成者とする。

5 監視を行わせる者は、監視を行う者に対して、監視記録を保存する期間をあらかじめ指示するものとする。監視を行う者は、指示された期間を経過した監視記録を直ちに破棄しなければならない。ただし、監視記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

6 監視を行う者及び監視記録の伝達を受けた者は、ネットワーク運用・管理のために必要な限りで、これを閲覧し、かつ、保存することができる。監視記録を不必要に閲覧してはならない。不必要となった監視記録は、直ちに破棄しなければならない。監視記録の内容を、法令に基づく場合等を除き、他の者に伝達してはならない。

2101-60（利用記録）

第60条 複数の者が利用する情報機器を管理する個別情報システム担当者（以下「当該情報機器の管理者」という。）は、当該機器に係る利用記録（以下「利用記録」という。）をあらかじめ定めた目的の範囲でのみ取得することができる。当該目的との関連で必要性の認められない利用記録を取得することはできない。

2 前項に規定する目的は、法令の遵守、情報セキュリティの確保、課金その他当該情報機器の利用やその改善に必要なものに限られる。個人情報の取得を目的とすることはできない。

3 利用記録は要機密情報、要保全情報とし、当該情報機器の管理者を情報の作成者とする。

4 当該情報機器の管理者は、第1項の目的のために必要な限りで、利用記録を閲覧することができる。他人の個人情報及び通信内容を不必要に閲覧してはならない。

5 当該情報機器の管理者は、第2項に規定する目的のために必要な限りで、利用記録を他の者に伝達することができる。

6 当該情報機器の管理者又は利用記録の伝達を受けた者は、第1項の目的のために必要な限りで、これを保有することができる。不要となった利用記録は、直ちに破棄しなければならない。ただし、当該情報

機器の管理者は、利用記録から個人情報を削除して、ネットワーク運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

2101-61（利用者等が保有する情報）

第61条 情報セキュリティ統括部署及び複数の者が利用する情報機器を管理する個別情報システム担当者は、利用者等が保有する情報をネットワーク運用に不可欠な範囲又は情報セキュリティインシデントへの対処に不可欠な範囲において、復元、閲覧、複製又は提供することができる。

第6節 暗号・電子署名

2101-62（暗号化機能・電子署名機能の導入）

第62条 個別情報システム責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講じなければならない。

1 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けなければならない。

2 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けなければならない。

2 個別情報システム責任者は、暗号化された情報の復号又は電子署名の付与に用いる鍵を適切に管理しなければならない。

第9章 情報システムの脅威への対策

第1節 ソフトウェアに関する脆弱性対策

2101-63（ソフトウェアに関する脆弱性対策の実施）

第63条 個別情報システム責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施しなければならない。

2 個別情報システム責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上でとり得る対策がある場合は、当該対策を実施しなければならない。

3 個別情報システム責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認しなければならない。

4 個別情報システム責任者は、脆弱性対策の状況の定期的な確認により、脆弱性対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策の計画を策定し、措置を講じなければならない。

第2節 不正プログラム対策

2101-64（不正プログラム対策の実施）

第64条 個別情報システム責任者は、必要に応じて、サーバ装置及び端末に不正プログラム対策ソフトウ

ェア等を導入しなければならない。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合はこの限りではない。

2 個別情報システム責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行わなければならない。

第3節 サービス不能攻撃対策

2101-65 (サービス不能攻撃対策の実施)

第65条 個別情報システム責任者は、要安定情報を取り扱う情報システム(インターネットからアクセスを受ける情報システムに限る。以下この条において同じ。)については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行わなければならない。

2 個別情報システム責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築しなければならない。

3 個別情報システム責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視しなければならない。

第4節 標的型攻撃対策

2101-66 (標的型攻撃対策の実施)

第66条 個別情報システム責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策(入口対策)を講じなければならない。

2 個別情報システム責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する対策、侵入範囲の拡大の困難度を上げる対策、及び外部との不正通信を検知して対処する対策(内部対策)を講じなければならない。

第10章 アプリケーション・コンテンツの作成・提供

第1節 アプリケーション・コンテンツ作成時の対策

2101-67 (アプリケーション・コンテンツのセキュリティ要件の策定)

第67条 個別情報システム責任者は、アプリケーション・コンテンツの提供時に学外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の対策を講じること。

1 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。

2 提供するアプリケーションが脆弱性を含まないこと。

3 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

4 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

5 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのOSやソフトウェア等

の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

6 サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

2 教職員等は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前項に掲げる内容を調達仕様に含めなければならない。

第2節 アプリケーション・コンテンツ提供時の対策

2101-68（関西学院ドメイン名の使用）

第68条 個別情報システム責任者は、学外向けに提供するウェブサイト等が実際の本学院提供のものであることを利用者が確認できるように、kwansei.ac.jpで終わるドメイン名（以下「関西学院大学ドメイン名」という。）を情報システムにおいて使用するよう仕様に含めることが望ましい。ただし、ソーシャルメディアサービスによる情報発信の場合はこの限りではない。

2 教職員等は、学外向けに提供するウェブサイト等の作成を外部委託する場合においては、前項と同様、関西学院大学ドメイン名を使用するよう調達仕様に含めることを推奨する。

2101-69（不正なウェブサイトへの誘導防止）

第69条 個別情報システム責任者は、利用者が検索サイト等を経由して本学院のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講じなければならない。

2101-70（学外のアプリケーション・コンテンツの告知）

第70条 アプリケーション・コンテンツを告知する場合は、告知する対象となるアプリケーション・コンテンツに利用者が確実に誘導されるよう、必要な措置を講じなければならない。

2 利用者等は、学外の者が提供するアプリケーション・コンテンツを告知する場合は、告知するURL等の有効性を保たなければならない

第11章 端末・サーバ装置等

第1節 端末

2101-71（端末管理責任者）

第71条 部局情報セキュリティ責任者は、学内通信回線に接続する端末及び本学院の業務に係る情報処理を行う端末の安全管理措置を管理する責任者（以下「端末管理責任者」という。）を定めなければならない。ただし、本学院支給以外の端末の端末管理責任者はその所有者もしくは使用者とする。

2101-72（端末の導入時の対策）

第72条 端末管理責任者は、端末に第63条及び第64条の措置を講じなければならない。ただし、支給外端末はその限りではない。

2 端末管理責任者は、要保護情報を取り扱う端末（支給外端末を含む）について、端末の盗難、不正な持ち出し、第三者による不正操作等の物理的な脅威から保護するための対策を必要に応じて講じなけ

ればならない。

3 個別情報システム責任者及び端末管理責任者は、要機密情報を取り扱う本学院が支給する端末（要管理対策区域外で使用する場合に限る）及び本学院支給以外の端末について、盗難、紛失、不正プログラムの感染等により情報窃取されることを防止するための技術的な措置を必要に応じて、講じなければならない。

4 個別情報システム責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末（支給外端末を除く）で利用を認めるソフトウェア又は利用を禁止するソフトウェアを定めるものとする。

2101-73（端末の運用時の対策）

第73条 個別情報システム責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行わなければならない。

2 端末管理責任者は、所管する範囲の端末（支給外端末を含む）で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図らなければならない。

2101-74（端末の運用終了時の対策）

第74条 端末管理責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消しなければならない。ただし、支給外端末はその限りではない。

第2節 サーバ装置

2101-75（サーバ装置の導入時の対策）

第75条 個別情報システム責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、不正な操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講じなければならない。

2 個別情報システム責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保しなければならない。

3 個別情報システム責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェアを定めなければならない。

4 個別情報システム責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講じなければならない。

2101-76（サーバ装置の運用時の対策）

第76条 個別情報システム責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図らなければならない。

2 個別情報システム責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講じなければならない。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

3 個別情報システム責任者は、要安定情報を取り扱うサーバ装置について、サーバ装置が運用できなく

なった場合に正常な運用状態に復元することが可能になるよう、必要な措置を講じなければならない。

2101-77（サーバ装置の運用終了時の対策）

第77条 個別情報システム責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消しなければならない。

第3節 複合機・特定用途機器

2101-78（複合機）

第78条 個別情報システム責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定しなければならない。

2 個別情報システム責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

3 個別情報システム責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消しなければならない。

2101-79（IoT機器を含む特定用途機器）

第79条 個別情報システム責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講じなければならない。

第12章 電子メール・ウェブ等

第1節 電子メール

2101-80（電子メールの導入時の対策）

第80条 個別情報システム責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定しなければならない。

2 個別情報システム責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えなければならない。

3 個別情報システム責任者は、電子メールのなりすましの防止策を講じなければならない。

4 個別情報システム責任者は、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、電子メールのサーバ間通信の暗号化の対策を講じなければならない。

第2節 ウェブ

2101-81（ウェブサーバの導入・運用時の対策）

第81条 個別情報システム責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講じなければならない。

1 ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

2 ウェブコンテンツの編集作業を担当する主体を限定すること。

3 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。

4 ウェブコンテンツの編集作業に用いる識別コード及び主体認証情報を適切に管理すること。

5 インターネットを介して転送される情報の盗聴及び改ざんの防止のため、必要に応じて、全ての情報に対する暗号化及び電子証明書による認証の対策を講ずること。

2 個別情報システム責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認しなければならない。

2101-82（ウェブアプリケーションの開発時・運用時の対策）

第82条 個別情報システム責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行わなければならない。

第3節 ドメインネームシステム（DNS）

2101-83（DNSの導入時の対策）

第83条 個別情報システム責任者は、要安定情報を取り扱う情報システムの名前解決を提供するコンテンツサーバにおいて、名前解決を停止させないための措置を講じなければならない。

2 個別情報システム責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講じなければならない。

3 個別情報システム責任者は、コンテンツサーバにおいて、本学院のみで使用する名前の解決を提供する場合、当該コンテンツサーバで管理する情報が外部に漏えいしないための措置を講じなければならない。

2101-84（DNSの運用時の対策）

第84条 個別情報システム責任者は、コンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持しなければならない。

2 個別情報システム責任者は、コンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認しなければならない。

3 個別情報システム責任者は、キャッシュサーバにおいて、名前解決の要求への適切な応答を維持するための措置を講じなければならない。

第4節 データベース

2101-85（データベースの導入・運用時の対策）

第85条 個別情報システム責任者は、データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行わなければならない。

2 個別情報システム責任者は、取り扱う情報の機密性要求、完全性要求により必要と認める場合には、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずるものとする。

3 個別情報システム責任者は、取り扱う情報の機密性要求、完全性要求により必要と認める場合には、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずるものとする。

4 個別情報システム責任者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用し

た、データの不正な操作を防止するための対策を講じなければならない。

第13章 通信回線

第1節 通信回線

2101-86（通信回線の導入時の対策）

第86条 個別情報システム責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講じなければならない。

2 個別情報システム責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けなければならない。

3 個別情報システム責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講じなければならない。

4 個別情報システム責任者は、利用者等が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講じなければならない。

5 個別情報システム責任者は、通信回線装置を要管理対策区域に設置しなければならない。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにしなければならない。

6 個別情報システム責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講じなければならない。

7 個別情報システム責任者は、学内通信回線にインターネット回線、公衆通信回線等の学外通信回線を接続する場合には、統括情報セキュリティ責任者の許可を得なければならない。

8 個別情報システム責任者は、学内通信回線及び当該学内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講じなければならない。

9 個別情報システム責任者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視するための措置を講じなければならない。

10 個別情報システム責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保しなければならない。

11 個別情報システム責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておかなければならない。

2101-87（通信回線の運用時の対策）

第87条 個別情報システム責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講じなければならない。

2 個別情報システム責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行わなければならない。

3 個別情報システム責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、不適切な状態にある通信回線装置を認識した場合には、改善を図らなければならない。

4 個別情報システム責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更しなければならない。

2101-88（通信回線の運用終了時の対策）

第88条 個別情報システム責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講じなければならない。

2101-89（リモートアクセス環境導入時の対策）

第89条 個別情報システム責任者は、VPN回線を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

2 個別情報システム責任者は、利用者等の業務遂行を目的としたリモートアクセス環境を、学外通信回線を経由して本学院の情報システムへリモートアクセスする形態により構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

2101-90（無線LAN環境導入時の対策）

第90条 個別情報システム責任者は、無線LAN技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講じなければならない。

2101-91（情報コンセント設置時の対策）

第91条 個別情報システム責任者は、情報コンセントを設置する場合は、以下の対策を講じなければならない。

1 利用者の認証又は利用責任者の指定
2 主体認証ログの取得及び管理
3 情報コンセント経由でアクセス可能な情報システムの明確化
4 情報コンセント接続中の他の通信回線との接続禁止
5 情報コンセント接続方法の機密性の確保

2101-92（端末の学内通信回線への接続の管理）

第92条 部局情報セキュリティ責任者は、端末（支給外端末を含む）の学内通信回線への接続の申請を受けた場合は、別途定める接続手順に従い、申請者に対して接続の諾否を通知し必要な指示を行わなければならない。

2101-93（上流ネットワークとの関係）

第93条 統括情報セキュリティ責任者は、学内通信回線を構築し運用するにあたっては、学内通信回線の上流ネットワークとなる学外通信回線との整合性に留意しなければならない。

第14章 情報システムの利用

2101-94（情報システム利用者の規定の遵守を支援するための対策）

第94条 個別情報システム責任者は、利用者等による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築するものとする。

2101-95（情報システムの利用時の基本的対策）

第95条 利用者等は、本学院の教育・学習・研究・事務の遂行以外の目的で情報システムを利用してはならない。

2 利用者等は、管理者権限を持つ識別コードを付与された場合には、管理者権限を濫用する行為を行ってはならない。

3 利用者等は、接続を許可された通信回線以外に本学院の情報システムを接続してはならない。

4 利用者等は、学内通信回線に、接続許可を受けていない情報システム及び通信回線装置を接続してはならない。

5 利用者等は、学内通信回線に接続している端末等（支給外端末を含む）を、統括情報セキュリティ責任者の許可なくインターネット回線や公衆通信回線等の学外通信回線へ同時に接続してはならない。

6 利用者等は、以下のソフトウェアが動作する端末（支給外端末を含む）を学内通信回線に接続してはならない。

1 ネットワークモニタリングツール

2 ファイルの自動公衆送信機能を持ったファイル交換ソフトウェア

7 利用者等は、情報システムで利用を禁止するソフトウェアを利用してはならない。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを教育・研究・事務上の必要により利用する場合は、個別情報システム責任者の承認を得なければならない。

8 利用者等は、接続が許可されていない機器等を情報システムに接続してはならない。

9 利用者等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講じなければならない。

10 利用者等は、端末（支給外端末を含む）を学内通信回線に接続する場合は、当該端末から学内通信回線を経由して情報システムが不正プログラムに感染することのないよう、必要な安全管理措置を講じなければならない。

11 利用者等は、私用の外部電磁的記録媒体を本学院の業務に使用してはならない。

12 利用者等は、自組織以外の組織から受け取った外部電磁的記録媒体は、自組織と当該組織との間で情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこれに情報を書き出す場合の安全確保のために必要な措置を講じなければならない。

13 利用者等は、要保護情報が記録されたUSBメモリ等の外部電磁的記録媒体を本学院外に持ち出す場合には、部局情報セキュリティ責任者又は職場情報セキュリティ責任者の許可を得なければならない。

2101-96（要保護情報を取り扱う本学院が支給する端末（要管理対策区域外で使用する場合に限る）及び本学院支給以外の端末の導入及び利用時の対策）

第96条 職員等は、本学院支給以外の端末を用いて要保護情報を取り扱う場合には、職場情報セキュリ

ティ責任者の許可を得なければならない。

2 職場情報セキュリティ責任者は、本学院支給以外の端末の利用について、取り扱うことになる情報の格付及び取扱制限、当該端末の管理は本学院ではなくその所有者が行うこと等を踏まえて本学院支給以外の端末の利用の可否を判断しなければならない。

3 利用者等は、本学院が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱う場合は、部局情報セキュリティ責任者又は職場情報セキュリティ責任者の許可を得なければならない。

4 部局情報セキュリティ責任者及び職場情報セキュリティ責任者は、利用者等が本学院が支給する端末（要管理対策区域外で使用する場合に限る）を用いて要保護情報を取り扱うことについて、これらの端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえて可否を判断しなければならない。

5 利用者等は、本学院が支給する端末（要管理対策区域外で使用する場合に限る）及び本学院支給以外の端末に要機密情報を保存してはならない。ただし、以下の場合には、自動的に暗号化される機能が有効な電磁的記録媒体への保存に限り、これを妨げない。

1 作業上、やむを得ず一時的に保存しなければならない場合

2 端末を支給されていない場合（ただし、職員等を除く。）

6 利用者等は、情報処理の目的を完了した場合は、本学院の業務に係る情報を本学院支給以外の端末から消去しなければならない。

2101-97（電子メール・ウェブの利用時の対策）

第97条 利用者等は、要機密情報を含む電子メールを送受信する場合には、本学院が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用しなければならない。

2 利用者等は、不審な電子メールを受信した場合には、不用意に開いてはならない。

3 利用者等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行ってはならない。

4 利用者等は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認しなければならない。

1 送信内容が暗号化されること

2 当該ウェブサイトが送信先として想定している組織のものであること

2101-98（識別コード・主体認証情報の取扱い）

第98条 利用者等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用してはならない。

2 利用者等は、自己に付与された識別コード及び自己の主体認証情報を適切に管理しなければならない。

3 利用者等は、自己に付与された識別コードを他者が主体認証に用いるために付与及び貸与してはならない。

4 利用者等は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用しなければならない。

5 利用者等は、自己の主体認証情報を他者に教えてはならない。

6 利用者等は、主体認証情報格納装置を他者に付与及び貸与してはならない。

2101-99（暗号・電子署名の利用時の対策）

第99条 利用者等は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、適切に保存、管理しなければならない。

2101-100（不正プログラム感染防止）

第100条 利用者等は、不正プログラム感染防止に関する措置に努めなければならない。

2 利用者等は、情報システム（支給外端末を含む）が不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講じなければならない。

2101-101（利用制限等）

第101条 統括情報セキュリティ責任者及び部局情報セキュリティ責任者は、情報セキュリティインシデントへの対処に不可欠な範囲において、以下の措置を講ずることができる。

1 情報システムの停止又は利用の制限
2 アカウントの停止
3 利用者等が保有する情報の変更又は削除
4 その他情報システムの保護のために必要な措置

【本ポリシーの改廃】

（本ポリシーの改廃）

このポリシーの改廃は、情報化推進機構長室会の議を経て、学部長会、各学校および園の意向を徴したうえ、理事会で決定する。

附 則

1 このポリシーは2023年（令和5年）6月1日から施行する。

経過措置：「情報の格付け」については、各現場での現状の把握と整理が必要となることから、1年間の経過措置を適用する。