関西国際大学 情報セキュリティポリシー

（2015 年 10 月 1 日制定）

１　情報セキュリティに係わる適用範囲と対象

本情報セキュリティポリシーの適用範囲は、本学が有する教育・研究及び学校運営に係わる情報資産（ハードウェア・ソフトウェア・データ・情報及びこれらに関連する施設設備・ドキュメント・保存媒体等）であり、適用対象者（以下「利用者」という。）は、これらの情報資産を取り扱う次のものすべてとする。

（１）理事
（２）職員(教育職員および事務職員)
（３）学部生、大学院生、研究生、科目等履修生、聴講生
（４）職員と共同して教育研究を行う者
（５）非常勤職員
（６）（１）～（５）の他、派遣社員、委託先業務従事者など、雇用形態、職位、勤務場所を問わず、本学の情報システムを使用する者

２　情報セキュリティに係わる管理体制

本対応マニュアルは、情報セキュリティ責任者（以下「CISO : Chief Information Security Officer」という。）のもとで策定し運用するものとする。

CISO は、当分の間、メディアサポート部門を所掌する副学長とする。

また,「情報セキュリティに対する侵害」「個人情報・保護情報の漏洩」「試験等の成績管理に関する事故」などの不測の事故や障害が発生した場合、必要に応じて CISO を長とする情報セキュリティ対策チームを編成する。

なお、情報セキュリティ対策チームが編成された場合の構成員は次のとおりとする。

（１）CISO
（２）メディアサポート部門を担当する部長および課長
（３）不測の事故や障害が発生した部局や学部の長
（４）その他 CISO が必要と認めた者

３　情報セキュリティの管理責任

（１）情報資産管理者の責務

各部局ならびに各学部が保有する情報資産の管理を行うため、各部局ならびに各学部に情報資産管理者を置く。当分の間、情報資産管理者は、部局長ならびに学部長が兼ねるものとする。情報資産管理者は、その管理対象となる情報資産の保護に関し、本対応マニュアルに則って管理がなされているかを継続的に監視し、違反行為を発見したときは、改善を施すと共に CISO に報告する義務と責任を負う。

（２）利用者の責務

利用者は、所属する部局ならびに学部に係る情報資産の利用権限に応じて、本情報セキュリティポリシーを遵守する義務と責任を負う。

４　利用者の遵守事項

本学の情報システムの利用者に対して、当該情報システムへのアクセスを保証し安定した運用を行うために、利用者が遵守すべき行動の基準（規範）を次のように定める。

（１）他人の利用者 ID を不正に申請したり、他人の利用者 ID を不正に使用したりしてはならない。

（２）自分の利用者 ID を他人に使用させてはならない。

（３）システム資源を大量に消費することにより、他の利用者の正常な使用を妨害したり、コンピュータシステムの正常な運用を妨げたりしてはならない。

（４）営利、非営利を問わず、商用を目的とした利用をしてはならない。

（５）他人のプライバシーを侵害したり、他人を誹謗中傷したりしてはならない。

（６）嫌がらせ、脅迫的行為、公序良俗に反する行為等をしてはならない。

（７）著作権等の財産権を侵害する行為を行ってはならない。

また、利用者は、当該情報システムを使用する際の自らのすべての行為に対して責任を負うとともに、国内の情報セキュリティ関連法規や本学が定める規則を遵守しなければならない。

５　安全性を確保するための遵守事項

本学の情報システムの安全性を確保するために、次の遵守事項を定める。

（１）本学の情報システムを、教育・研究及び設置する学校の運営業務以外の目的に使用してはならない。

（２）本学の情報システムに、コンピュータやネットワーク機器を接続しようとする者は、必要なネットワーク接続手続きを行わなければならない。

（３）本学の情報システムに、コンピュータを接続しようとする者は、該当するコンピュータにウィルスの感染を防止する対策を講じなければならない。

（４）利用者の管理するコンピュータがウィルスに感染した場合又は感染の疑いがある場合は、直ちにネットワークから切り離し、感染の拡大を防止しなければならない。あわせて、直ちに感染を除去する処理を行わなくてはならない。

（５）本学の情報システム管理者は、学内全体のウィルス感染情報を把握した上で、学内の情報システムの運用に影響することが予想される場合は、直ちに当該ウィルスに関する情報を利用者に公開し注意を促さなければならない。

６　安全性を確保するための措置

本学の情報システムの安全性を確保するため、次の措置を講じるものとする。

（１）悪意ある者からの学内ネットワークに対する攻撃やウィルスの侵入を防御するため、ネットワークの出入り口で、FireWall によるパケットフィルタリングや、メールシステムによるウィルス検知を行う。

（２）個人情報などの重要な情報へのアクセスにあたっては、情報の登録時や参照時の認証及びアクセス制御ならびに暗号化等の対策を施し、安全性と信頼性を確立するものとする。

7　情報資産を保護するための遵守事項

本学の情報資産を保護するために、本学の情報システムの利用者は次の各号を遵守しなければならない。

（1）情報の学外への持ち出し

本学の教育・研究及び管理運営業務の遂行以外の目的で、情報資産を学外に持ち出さないこと。当該業務の遂行のために、もし持ち出した場合は、持ち出し先においても学内と同様に情報を扱うこと。

（2）情報資産の複製の制限

本学の情報システム部門が管理する情報資産が収納されたサーバーシステムから目的外に情報を複製してはならない。

（3）守秘義務

公共の利益を優先する必要があると判断される場合、及び業務遂行上必要と認められる場合を除き、業務遂行に際して知り得た情報及び技術を使用し、またこれらを第三者に開示、提供又は漏洩してはならない。また、個人のプライバシーに関する情報を取り扱う場合は、その保護に留意するとともに、事故が発生しないように対策を講じなければならない。

（4）外部委託時のセキュリティ管理

情報資産に関わる業務を本学の外部に委託する場合は、外部委託業者と交わす契約書に、問題が発生した場合に責任の所在が明確になる項目や、本学の情報セキュリティポリシーが遵守されなかった場合の対応に係わる項目等を明記し、情報資産の外部への漏洩を防止するための措置を講じなければならない。

（5）国内の情報セキュリティ関連法規や本法人が定める規則の遵守義務

個人情報の保護に関する法律を始め、不正アクセス行為の禁止等に関する法律、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（通称プロバイダ責任法)、電子署名認証法、電子帳簿保存法、著作権法及び刑法ならびに今後制定される情報セキュリティ関連法規、本学が定める情報セキュリティ関連の規則等を遵守しなければならない。

8　情報セキュリティに係わる禁止事項

利用者は、次に掲げる情報セキュリティを脅かす行為は、いかなる場合も行ってはならない。

本学の情報システムの利用者は、悪意を持って情報セキュリティの行為を行う者が存在することを認識し、被害に遭わないように各々が予防措置を講ずる等、十分な注意を払わなければならない。

（1）不正アクセス

他人の利用者 ID とパスワードを用いて、正当な所有者の許可なくネットワークや情報システムに不正にアクセスし、情報の盗聴、窃盗、漏洩、改ざん、破壊、消失等を行う。

（2）不正侵入

セキュリティ・ホール（システムの欠陥）やサーバーシステムの不適切な設定をついて、管理者権限を奪い情報システムに不正にアクセスし、情報資産の書き換え、情報の漏洩、改ざん、破壊等を行う。

（3）不正攻撃

ポート攻撃などにより、ネットワークや情報システムへの運用妨害を行い、異常停止

に至らしめる。

（4）スパム・メールの送信

受信を希望していない者に不要なメールを大量に送りつけ、混乱を引き起こす。

（5）メール爆弾の送信

大量のメールや大容量の添付ファイルを一度に特定のメールシステムや個人に対して送信し、混乱を引き起こしたり、運用妨害を行ったりする。

（6）なりすまし

他人の利用者 ID とパスワードを用いて、正当な所有者に成り代わってネットワークや情報システムからのサービスを受けたり、情報の窃盗、漏洩、改ざんを行ったりする。

（7）盗聴

ネットワーク上を流れるパスワード情報やメールの内容などを盗聴し、情報の窃盗、漏洩を行う。

（8）窃盗

他人の所有するコンピュータや記録媒体から、情報の窃盗・漏洩を行う。

（9）DoS（Denial of Service：サービス不能）攻撃

意図的に大量のパケットを送り付けて、特定のサービスやコンピュータ及びネットワークを一時的又は継続的に使用不能にする。

（１０）マルウェアの配信

コンピュータウィルス、ワーム、スパイウェア等の不正かつ有害な動作を行うプログラムを広く配信することにより、データの破壊、消失やコンピュータを機能不全に陥れる行為で、拡散により多くのコンピュータに被害を及ぼす。

（１１）フィッシング

本学若しくは他組織の偽の情報システムを用意し電子メールで誘導することによって、利用者 ID やパスワード等の個人情報を不正に獲得する。

（１２）その他

人の心の隙をつくソーシャルエンジニアリング、倫理観又は道徳観の欠如による機密情報の漏洩や窃盗、迷惑メールの発信や掲示板へのいたずら書き、著作権違反や肖像権の侵害、人権侵害やプライバシー侵害等の行為を行う。

９　遵守義務と罰則

本情報セキュリティポリシーは、情報資産利用者であるすべての者にその遵守を義務づける。また、本情報セキュリティポリシーの違反者には罰則を科すことがある。

さらに、情報資産利用者が、本学の情報セキュリティシステムに重大な影響を与える行為、個人のプライバシー侵害に該当する行為、資産損失を招くような悪質な行為等を行ったと認められる場合には、就業規則や学則等に則った処分を科すことがある。

また、不測事態の発生により社会的信用の失墜が避けられない場合は、CISO の判断により、その改善措置がとられるまでの間、本学の情報システムの使用に制限を課すことができる。

以　上