情報システム利用ガイドライン

（目的）

1　このガイドラインは、学校法人近畿大学（以下「本学園」という。）における情報システムの利用において、学校法人近畿大学情報システム利用規程の運用に関する具体的指針を定め、情報セキュリティの確保と円滑な情報システムの利用に資することを目的とします。

（定義）

2　このガイドラインにおいて、次の各号に掲げる用語は、それぞれ当該各号の定めるところによります。

（１）運用基本方針
本学園が定める「学校法人近畿大学情報セキュリティポリシー」を指します。

（２）運用基本規程
本学園が定める「学校法人近畿大学情報システム運用基本規程」を指します。

（３）全学アカウント
本学園が運用する認証システムに対応した情報システムの利用に当たって用いるアカウント及び本学園が契約又は外部委託したシステム又はサービスのためのアカウントを指します。

（４）その他の用語の定義は、運用基本方針、運用基本規程又は学校法人近畿大学情報システム管理・運用規程で定めるところによります。

（ガイドラインの適用範囲）

3　このガイドラインは、本学園構成員及び許可を受けて情報システムを利用する者に適用します。

（１）構成員は、次のとおりです。

①　教職員：本学園専任教職員、非常勤講師、客員教員、嘱託職員、契約職員、定時職員、派遣職員などです。

②　学生等：学部学生、大学院生、留学生、研究員、大学院研修生、科目等履修生、聴講生、公開講座の受講生に加え、生徒、児童を含みます。

（２）このガイドラインにおける情報システムは、格付けされた本学園の情報を格納する機器であれば、本学園のネットワークに接続されていないものであっても含みます。

（利用目的）

4　情報システムの利用は、原則として、教育、研究及び医療を目的とするものに限ります。ただし、本学園の管理・運営及び学生・教職員の福利厚生に資するための利用は認めます。

（遵守事項）

5　情報システムの利用者は、このガイドラインに従って情報システムの利用に関する手順・諸規程を遵守するとともに、本学園の規定する個人情報保護に関する諸規程を遵守してください。

（利用上の遵守事項）

6　情報システムの利用者は、次の事項を遵守してください。

（１）セキュリティについて

①　データ・個人情報・パスワード・機密データを保護してください。
②　コンピュータのファイルセキュリティ機能を最大限に利用してください。
③　セキュリティ強度の高いパスワードを設定してください。

（２）機密性について

① 他の利用者のプライバシーを尊重してください。
② 許可なく他の利用者の所有するファイル等をコピー、修正してはいけません。
③ みだりに大学の所有するファイル等をコピー、修正してはいけません。
④ 他の利用者の権利を尊重してください。
⑤ 著作権や商標権など法的保護を尊重してください。
⑥ 電子メール・ネットニュース・www などの意図された使用法を尊重してください。

（アカウント）

7 情報システムの利用者は、アカウント（ID 及びパスワード）の管理に際して、次の点を遵守してください。

（１）アカウントとパスワードの管理と利用

利用者は、本学園が提供するシステムやサービスを利用するために付与されたアカウント・パスワードを適切に管理して、利用してください。

（２）貸与・譲渡の禁止

利用者は、他の者のアカウントを使用してはいけません。

（３）ロック又はログアウト

利用者は、使用中のコンピュータをロック又はログアウト（ログオフ）せずに、長時間自らの席を離れてはいけません。

（４）アカウント流出時の対応

利用者は、アカウントを他者に使用され、又はそのおそれがある場合には、すみやかに総合情報システム部教育システム課（KUDOS）にその旨を報告してください。

（５）パスワードの変更

パスワードは定期的に変更してください。

（６）設定パスワードの制限

以下の３つの条件を満たすパスワードにしてください。

① パスワードの長さは、８文字～１６文字とします。
② 使用できる文字は、半角英字数字（A～Z，a～z，0～9）とします。
③ 「自身のユーザ ID」や「password」など推測されやすい文字列を含めないようにしてください。

（７）アカウント漏えい時の対応

万が一、他人に知られた可能性がある場合は、すみやかにパスワードを変更してください。

（８）利用終了時

利用者は、システムを利用する必要がなくなった場合は、遅滞なく当該情報システムの管理者に届け出てください。ただし、個別の届出が必要ないと、あらかじめ定めている場合は、この限りではありません。

（９）パスワードの管理方法

パスワードは記憶するようにしてください。漏えい防止の観点から、書き留めないようにしてください。

（情報機器の利用）

8 利用者は、様々な情報の作成、利用、保存のために情報機器を利用する際には、次の事項を遵守してください。

（１）利用者は、本学園の情報ネットワークに新規に情報機器を接続しようとする場合は、事前に接続を行おうとする部局の責任者に接続の許可を得てください。ただし、情報コンセント等からの情報システムへの一時的な接続についてはこの限りではありません。

（２）利用者は、許可を受けた情報機器の利用を取りやめる場合には、部局の責任者に届け出るようにしてください。

（３）情報機器が認証システムおよびログ機能を備えている場合には、それらの機能が設定され動作していなければなりません。不正ソフトウェア対策機能が提供されている機器については、その機能が最新の状態でシステムを保護できるようにしてください。

（４）情報機器は脆弱性を持たないようにし、可能な限り最新の状態を保つようにしてください。

（５）利用者は、情報漏えいを発生させないように対策し、情報漏えいの防止に努めてください。

（６）利用者は、情報機器の紛失又は盗難を発生させないように注意してください。

（７）情報機器の紛失又は盗難が発生した場合は、すみやかに総合情報システム部教育システム課（KUDOS）に届け出てください。

（８）別途定める情報機器取扱ガイドライン等に従い、これらの情報機器の適切な保護に注意してください。

（制限事項）

９　利用者は、情報システムについて次の行為をしてはいけません。

（１）ファイルの自動公衆送信機能を持ったP2Pソフトウェアを教育・研究目的で利用する行為

ファイル共有ソフトとは、インターネット上で不特定多数のユーザとファイルのやりとりをするためのソフトウェアで、WinnyやShareなどがあります。ファイル共有ソフトを介して、音楽、映像、ゲームソフトなどの著作物が無断でやりとりされており、大きな問題となっています。

ファイル共有ソフトには、P2P（Peer to Peer）と呼ばれる技術が使われており、一般のWebサイトのような「クライアント・サーバ・モデル」とは異なります。

（２）教育・研究目的で不正ソフトウェア類似のコードやセキュリティホール実証コードを作成、所持、使用又は配布する行為

（３）ネットワーク上の通信を監視する行為

（４）本学園の情報機器に関する利用情報を取得する行為及び情報システムのセキュリティ上の脆弱性を検知する行為

（５）情報システムの機能を著しく変える可能性のあるシステムの変更

（禁止事項）

１０　利用者は、情報システムについて、次の行為をしてはいけません。

（１）当該システム又は情報について定められた目的以外の利用、及び本学園の教育研究目的に

反する利用

（２）指定以外の方法での本学園外からの全学アカウントを用いてのアクセス

（３）あらかじめ指定されたシステム以外のシステムを本学園外の者に利用させる行為

（４）守秘義務に違反する行為

（５）差別、名誉毀損、侮辱又はハラスメントにあたる行為
近畿大学人権宣言、近畿大学人権教育基本方針、学校法人近畿大学倫理憲章、学校法人近畿大学職員倫理規程及び法人倫理推進のためのガイドライン、近畿大学学園ハラスメント防止のためのガイドラインに抵触する行為
なお、ハラスメントとは、サイバー・ハラスメントをはじめ、近畿大学学園ハラスメント防止のためのガイドラインにおいて定義されているすべてのハラスメントを含みます。

（６）個人情報やプライバシーを侵害する行為
利用者は、本学園の個人情報保護基本規程及び特定個人情報等取扱規程に定義されている個人情報や機微（センシティブ）情報をパソコンで取り扱う場合は、これらの情報が不用意に流出しないように注意してください。

（７）前条の許可を得ずに行う不正ソフトウェアの作成、所持又は配布及び有害なコンピュータプログラム等を送信、掲載又は書き込む行為

（８）知的財産権を侵害する行為
知的財産権は、次のとおりです。
・産業財産権
　特許権、実用新案権、意匠権、商標権
・その他
　著作権、回路配置利用権、育成者権、営業秘密（ノウハウ等）

（９）通信の秘密を侵害する行為

（１０）営業又は商業を目的とした利用
他の利用者又は第三者に対し無断で広告、宣伝、勧誘等の電子メールを送信する行為

（１１）過度な負荷等により本学園の円滑な情報システムの運用を妨げる行為

（１２）不正アクセス禁止法に反する行為又はこれに類する行為
不正アクセス禁止法では、不正アクセス行為及び不正アクセスを助長する行為を禁止しています。不正アクセスを助長する行為とは、例えば、A さんに無断で A さんの ID・パスワードを第三者に提供する行為（口頭伝達、電子掲示板に掲示、販売等）を指します。

（１３）その他法令に基づく処罰の対象となる行為
公職選挙法で認められていないネットでの選挙運動、わいせつ等不適切な内容の画像、文書等を掲載する行為など

（１４）上記の行為を助長する行為

（１５）計算機資源を不当に占有又は浪費する行為

（１６）公序良俗に違反する行為
わいせつ等不適切な内容の画像、文書等を送信する行為。

（違反行為への対処）

１１　利用者の行為が前条に掲げる事項に違反すると認められたときは､学則又は就業規則に基づき、利用停止を含め、処分を受けます。なお、利用者の不適切な使用によって生じた重大な損害について、本学は当該利用者に対して賠償を求めることができます。

（電子メール）

１２　電子メールの利用については、別途定める「電子メール利用手引き」に従って、適切に利用してください。

（ウェブの利用）

１３　利用者は、ウェブブラウザを利用したウェブサイトの閲覧、情報の送信及びファイルのダウンロード等を行う際には、不正プログラムの感染、情報の漏えい及び誤った相手への情報の送信等の脅威に注意するだけでなく、コミュニケーションサイトへの不適切な書き込みにより、本学園の社会的信用を失わせることのないように注意してください。

（セキュリティ対策）

１４　OS やアプリケーションは常にアップデートし、最新の状態にしてください。セキュリティ修正パッチやサービスパックを適宜適用してください。

（学外からの情報システムの利用）

１５　利用者は、学外からの情報システムのアクセスにおいて、次の事項に従ってください。

（１）利用者は、学外から全学アカウントを使って情報システムを利用することが認められたシステム以外は、学外から利用することができません。

（２）利用者は、学外から全学アカウントを使って情報システムを利用する際においても、これを他者に利用させてはいけません。

（安全管理義務）

１６　利用者は、自己の管理する情報機器について、本学園の情報ネットワークとの接続状況に関わらず、安全性を維持する一時的な担当者となることに留意して、次の事項に従って利用しなければなりません。

（１）ソフトウェアの状態及び不正ソフトウェア対策機能を最新に保つようにしてください。
（２）不正ソフトウェア対策機能により不正プログラムとして検知されるファイル等を開かないようにしてください。
（３）不正ソフトウェア対策機能の自動検査機能を有効にしてください。
（４）不正ソフトウェア対策機能によりすべての電子ファイルに対して、不正プログラムが存在しないことを定期的に確認してください。
（５）外部からデータやソフトウェアを情報機器に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正ソフトウェアが存在しないことを確認してください。
（６）常に最新のセキュリティ情報に注意し、不正ソフトウェア感染の予防に努めてください。

（インシデント対応）

１７　利用者は、情報システムの利用に際して、インシデント（中断・阻害、損失、緊急事態、危機に、なり得るまたはそれらを引き起こし得る状況）を発見したときは、別途定めるインシデント対応手順等に従って行動してください。

（在籍期間終了時）

１８　本学園に在籍しなくなった場合は（卒業・退職等)、自己のデータが通知なく本学園の情報システムから削除されるので注意してください。

（クラウドの利用について）

１９　昨今、クラウドサービスの発展にともない、インターネットを経由してソフトウェア等のサービスを容易に利用できるようになりました。利用者は、本学園のシステムであるかに関わらず、クラウドサービスを利用するにあたり、安全性を確保するために、次の事項に留意してください。

（１）　ID とパスワードが漏えいすると第三者でもサービスが利用できます。アカウントの管理には細心の注意を払ってください。

（２）　保存したデータがどの範囲まで公開されているのか、利用の前にプライバシー設定を確認してください。

（３）　サービスの障害によりデータが消失し、復旧できなくなる恐れがあります。定期的なバックアップをおすすめします。

（４）　サービスを利用する前に、利用規程の内容をよく読み、セキュリティ対策や保証の範囲を確認してください。

平成２８年６月２０日　総合情報システム委員会