学校法人近畿大学 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･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）情報機器
パソコン、サーバ、タブレット PC、スマートフォン等のコンピュータ本体及びディスプレイ、プリンタ、ネットワーク HDD（NAS）等の周辺機器を指します。

（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方に適用します。

（１）構成員は、次のとおりです。

①　教職員：本学園専任教職員、常勤・非常勤講師、客員教員、嘱託職員、契約職員、定時職員及び派遣職員です。

②　学生等：学部学生、大学院生、通信教育部生、留学生（別科生含）、研究員、大学院研修生、科目等履修生、生徒、児童及び幼児です。

（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やサービスであれば、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、医療及び法人業務（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などを含みます。）を目的とするものに限ります。

（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　個人情報・パスワード・機密データなどは厳重に管理してください。
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。

④ サーバ等を外部に公開する場合、所属の責任者の許可を得たうえで、必要最低限の通信ポートのみ開放してください。通信ポートの開放には総合情報システム部の審査が必要です。

（2）機密性について

① 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。
② みだりに業務で使用するファイル等を公開、私物等の情報機器への保存をしてはいけません。
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 著作権や商標権などによる法的保護を遵守してください。
⑤ 電子メール・ネットニュース・Web・SNS 等の意図された使用法を遵守してください。

（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。また、自身のアカウントを他の者に貸与・譲渡してはいけません。

（3）ロック又はログアウト

利用者は、使用中の情報機器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たり、目の届かないところに放置したりしてはいけません。

（4）アカウント流出、不正利用時の対応

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、速やかに KINDAI-CSIRT（情報セキュリティインシデント対応チーム・総合情報システム部所管）にその旨を報告してください。万が一、他人に知られた可能性がある場合は、速やかにパスワードを変更してください。

・KINDAI-CSIRT Web サイト　https://kudos.kindai.ac.jp/security/kindaicsirt

また、流出や不正利用のおそれがあると判断した場合、当該利用者への事前の通告なく、当該アカウントを停止する場合あります。

（5）設定パスワードの制限

以下の４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文字以上に設定してください。
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 や氏名ローマ字、「12345678」や「password」など、推測されやすい文字列にしないでください。
④ 半角英字数字が混在しているパスワードにしてください。
⑤ パスワードの使い回し（本学園で使用しているパスワードと同一のパスワードを他のサービスで使うこと）は行わないでください。

（6）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、速やかに当該情報システムの管理者に届け出てください。なお、本学教務システムや人事システムに登録されている学生・専任教職員等のユーザ（源泉ユーザ）は卒業・退職・出向等によって本学園に在籍しなくなった時点でアカウントが削除されます。教務システムや人事システムに登録されていないユーザ（非源泉ユーザ）は予めアカウントに有効期限が設定されます。

（7）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。他者に推測されにくく、覚えやすいパスワードの作り方について KUDOS WEB で紹介していますので参考してください。
KUDOS WEB（パスワード管理について） https://kudos.kindai.ac.jp/security/password

（8）２段階認証（多要素認証）
各サービスのアカウントに対し、２段階認証（多要素認証）の設定が可能なものは設定を行ってください。

（情報機器の利用・持ち出し）
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） 本学園の情報ネットワークに私物等の情報機器（大学が所有していない機器）を新規に接続する場合、KUDOS SECURE/KUDOS SECURE X 等の持ち込み機器用ネットワークのみ接続が可能です。私物等の情報機器で、教育・研究、法人業務用のシステム（HUE、Gmail、K-SHARED、Slack 等）を利用することは必要最小限にしてください。

（2）教育・研究用、法人業務用の大学所有の情報機器を本学園の情報ネットワークに新規に接続する場合は、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。

（3）許可を受けた情報機器の利用を取りやめる場合は、所属の責任者に届け出ることが必要になります。

（4）情報機器が認証システム及びログ機能を備えている場合は、それらの機能が動作するよう設定され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、常に最新の状態になるよう設定してください。

（5）情報機器は脆弱性を持たないよう、可能な限り最新の状態にしてください。

（6）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。

（7）情報機器の紛失又は盗難が発生しないよう十分に注意してください。

（8）個人情報や重要な情報、機密情報等の入った情報機器の紛失又は盗難が発生した場合は、速やかに所属の責任者及び総務部総務課に届け出てください。

（9）個人情報や重要な情報、機密情報等の入った情報機器を学外に持ち出す場合、情報の盗難・漏洩等を防止するため、情報機器へのログインパスワードを強固なものにし、ハードディスクやソリッドステートドライブ等の記憶装置に暗号化や盗聴防止策を講じ、かつ盗難防止策を講じてください。また、ログイン時にはパスワードに加え、
指紋認証や顔認証等の生体認証を併用することが望ましいです。

（１０）USB メモリ、SD カード等の可搬型の記憶装置の使用は、ウィルス混入・感染及び紛失のリスクが高いため、個人情報を含む機密性の高いデータの取り扱いを禁止します。情報機器間でのデータのやり取りを行う場合、２段階認証（多要素認証）設定済みアカウントにて、Google ドライブや Slack、学内ポータルシステム等を利用してください。ただし、教育・研究目的かつ限定された範囲での使用はこの限りではありません。

（禁止事項）

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、大きな社会問題となっています。著作権等の侵害は、法的な処罰の対象となります。

（2）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。ただし、教育・研究目的かつ限定された範囲での使用はこの限りではありません。

（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

（6）Tor（トーア）等の接続経路を匿名化するツールを利用する行為

（7）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

（8）指定以外の方法での全学アカウントを用いてのアクセス

（9）本学園のシステムを許可なく本学園外の者に利用させる行為

（１０）守秘義務に違反する行為

（１１）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。

（１２）個人情報やプライバシーを侵害する行為
利用者は、個人情報や機微（センシティブ）情報を情報機器で取り扱う場合は、これらの情報が流出しないようにしてください。また、肖像権など個人のプライバシーを侵害する行為は行わないようにしてください。

（１３）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。ただし、教育・研究目的かつ限定された範囲での使用はこの限りではありません。

（１４）知的財産権を侵害する行為
・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）など

（１５）通信の秘密を侵害する行為

（１６）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

（１７）過度な負荷等により本学園の円滑な情報システムやネットワークの運用を妨げる行為

（１８）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。

（１９）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

（２０）計算機資源やネットワーク帯域を不当に占有又は浪費する行為

（２１）上掲の行為を助長する行為

（違反行為への対処）
１０　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、本学園は当該利用者に対して賠償を求めることができます。

（Web の利用）
１１　利用者は、Web ブラウザを利用した Web 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）
１２　OS やアプリケーションは常にアップデートし、可能な限り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。ウィルス対策ソフトウェアは、その機能やパターンファイルを最新にした上で、システムを保護可能な状態に保ってください。

（学外からの情報システムの利用）
１３　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）
１４　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）
１５　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、危機になり得る又はそれらを引き起こし得る状況）を発見したときは、KINDAI-CSIRT（情報セキュリティインシデント対応チーム・総合情報システム部所管）の Web サイトに記載の手順に沿って、報告してください。
・KINDAI-CSIRT Web サイト　https://kudos.kindai.ac.jp/security/kindaicsirt
また、流出や不正利用のおそれがあると判断した場合、当該利用者への事前の通告なく、当該アカウントを停止する場合あります。

（在籍期間終了時）
１６　卒業・退職・出向等によって本学園に在籍しなくなった場合は、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）
１７　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。項目７を参考に、アカウントを管理してください。
（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　作成
平成３１年２月　１日　改定
近畿大学 総合情報システム委員会