

## ○学校法人関西大学情報システム利用規程

平成28年3月17日

制定

### (目的)

第1条 本規程は、学校法人関西大学及び法人が設置する学校（以下「本学」という。）における情報システムの利用に関する事項を定め、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する。

### (定義)

第2条 本規程において、次の各号に掲げる用語の意義は、当該各号の定めるところによる。

- (1) アカウント 主体認証を行う必要があると認めた情報システムにおいて、主体に付与された正当な権限をいう。また、狭義には、利用者等に付与されたユーザID（識別コード）とパスワード（主体認証情報）の組み合わせ、又はそれらのいずれかをいう。
- (2) 全学アカウント 本学の全学統一認証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をいう。また、本学が契約し外部委託したシステム及びサービス利用のためのアカウントも含むものとする。

### (適用範囲)

第3条 本規程は、本学構成員及び許可を受けて本学情報システムを利用する者に適用する。

- 2 本学情報システムとは、本学が設置若しくは契約により使用若しくは提供を受けているネットワーク、情報機器及び情報サービスのことである。また、これらに接続した状態の機器も対象とする。
- 3 本学情報システムには、学校法人関西大学文書取扱規程により格付けされた情報を格納する機器を含める。

### (遵守事項)

第4条 本学情報システムの利用者は、本規程及び本学情報システムの利用に関する手順等を遵守しなければならない。

### (IDとパスワード)

第5条 利用者は、アカウント管理に際して次の各号を遵守しなければならない。

- (1) 利用者は、自己のアカウントを他の者に使用させ、又は他の者に開示してはならない。
- (2) 利用者は、他者のアカウントを聞き出し、又は使用してはならない。
- (3) 利用者は、アカウントを利用して、学外から本学情報システムにアクセスする場合

には、定められた手順に従ってアクセスしなければならない。また、アカウントの漏えいが発生しないよう管理しなければならない。

- (4) 利用者は、アカウントを他者に使用された、又はその危険が発生した場合には、直ちにITセンターにその旨を報告しなければならない。
- (5) 利用者は、システムを利用する必要が無くなった場合は、遅滞なくITセンターに届け出なければならない。ただし、個別の届出が必要ない旨をITセンターが定めている場合は、この限りでない。
- (6) 利用者は、ITセンターが別途定めるガイドラインに従ってアカウントを適切に管理しなければならない。

(教職員証及び学生証 (ICカード) )

第6条 利用者は、ICカードの管理を以下のように徹底しなければならない。

- (1) ICカードを本人が意図せずに使われることの無いように安全措置を講じて管理しなければならない。
- (2) ICカードを他者に譲渡又は貸与しないこと。
- (3) ICカードを紛失しないように管理しなければならない。紛失した場合には、直ちにITセンターにその旨を報告しなければならない。
- (4) ICカードを利用する必要がなくなった場合には、遅滞無く、これを本学に返還しなければならない。

(情報機器の利用)

第7条 利用者は、様々な情報の作成、利用、保存等のための情報機器の利用にあたっては以下の各号に従わなければならない。

- (1) 利用者は、本学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、学校法人関西大学情報システム運用基本規程で定める最高情報セキュリティ責任者〔Chief Information Security Officer〕(以下「CISO」という。)に接続の許可を得なければならない。ただし、情報コンセントや本学が提供する無線LANからの本学情報システムへの一時的な接続、又はITセンターが指定した接続方法を利用する場合は、この限りではない。
- (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、ITセンターに届け出なければならない。
- (3) 情報機器は、認証システム及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らない。不正ソフトウェア対策機能が提供されている機器

にあつては、その機能が最新の状態でシステムを保護できるものでなければならない。

- (4) 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でなければならない。
- (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なければならない。
- (6) 利用者は、情報機器の紛失及び盗難を発生させないように注意しなければならない。
- (7) 情報機器の紛失及び盗難が発生した場合は、速やかに担当部署に届け出なければならない。
- (8) ITセンターが別途定めるガイドラインに従い、これらの情報機器の適切な保護に注意しなければならない。

(利用者による情報セキュリティ対策教育の受講義務)

第8条 利用者は、毎年度1回は、年度講習計画に従って、本学情報システムの利用に関する教育を受講することが望まれる。

(情報の取扱い)

第9条 利用者は、格付けされた情報について、学校法人関西大学文書取扱規程に従い、文書に明示された方法に従って取り扱わなければならない。

(禁止事項)

第10条 利用者は、本学情報システムについて、次の各号に定める行為を行ってはならない。

- (1) 当該情報システム及び情報について定められた目的以外の利用
- (2) 指定以外の方法による学外からの全学アカウントを用いた本学情報システムへのアクセス
- (3) あらかじめ指定されたシステム以外の本学情報システムを本学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当たる行為
- (6) 個人情報又はプライバシーを侵害する行為
- (7) 不正ソフトウェアの作成、所持及び配布行為
- (8) 著作権等の財産権を侵害する行為
- (9) 通信の秘密を侵害する行為
- (10) 営業ないし商業を目的とした本学情報システムの利用
- (11) 過度な負荷等により本学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

(13) その他法令に基づく処罰の対象となる行為

(14) 前各号の行為を助長する行為

(違反行為への対処)

第11条 利用者の行為が前条に掲げる事項に違反すると被疑される行為と認められたときは、責任者（所属長）は、CISOと協力して速やかに調査を行い、事実を確認するものとする。事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取しなければならない。

2 責任者は、上記の措置を講じたときは、遅滞なくCISOにその旨を報告しなければならない。

3 調査によって違反行為が判明したときは、責任者はCISOを通じて次の各号に掲げる措置を講ずることを依頼することができる。

(1) 当該行為者に対する当該行為の中止命令

(2) 部署に対する当該行為に係る情報発信の遮断命令

(3) 部署に対する当該行為者のアカウント停止、又は削除命令

(電子メールの利用)

第12条 利用者は、電子メールの利用にあたっては、ITセンターが別途定める利用ガイドラインに従い、規則の遵守のみならずマナーにも配慮しなければならない。

(ソーシャル・ネットワーキング・サービスを含めたウェブの利用及び公開)

第13条 利用者は、ウェブの利用及びウェブによる情報公開に際し、以下の各号に従わなければならない。

(1) 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、ファイルのダウンロード等を行う際には、ITセンターが別途定める利用ガイドラインに従わなければならない。

(2) 利用者は、ウェブページを作成し公開する場合は、本学の社会的信用を失わせることのないように配慮しなければならない。

(3) ウェブページやウェブサーバ運用に関して、規程やガイドラインに違反する行為が認められた場合には、CISOは、公開の許可の取り消しやウェブコンテンツの削除を行うことができる。

(学外からの本学情報システムの利用)

第14条 利用者は、学外からの本学情報システムへのアクセスにおいて、以下の各号に従

わなければならない。

(1) 利用者は、学外からアカウントを使って本学情報システムへアクセスするには指定された方法で利用しなければならない。

(2) 利用者は、アクセスに用いる情報システムを許可された者以外に利用させてはならない。

(安全管理義務)

第15条 利用者は、自己の管理する情報機器について、本学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次的な担当者となることに留意し、次の各号に従って利用しなければならない。

(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こと。

(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こと。

(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なければならない。

(4) 不正ソフトウェア対策機能により定期的に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確認すること。

(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すること。

(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ること。

(インシデント対応)

第16条 利用者は、本学情報システムの利用に際して、インシデントを発見したときは、ITセンターが別途定める「情報セキュリティインシデント対応手順」に従って行動しなければならない。

(事務)

第17条 この規程の事務は、情報推進グループが行う。

附 則

この規程は、平成28年4月1日から施行する。

附 則

この規程(改正)は、2018年4月1日から施行する。