

○宮崎大学情報システム利用者規程

〔平成 30 年 3 月 22 日〕
制 定
改 正 令和 2 年 3 月 31 日

(目的)

第 1 条 この規程は、宮崎大学情報セキュリティ基本規程第 16 条第 5 項の規定に基づき、宮崎大学（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 この規程において使用する用語は、宮崎大学情報セキュリティ基本規程及び宮崎大学情報システム管理者規程において使用する用語の例によるほか、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) 利用者 教職員等及び学生等で、本学の情報システムを利用する許可を受けて利用する者をいう。
- (2) 利用者等 利用者及び本学の情報システムを臨時に許可を受けて利用する者をいう。
- (3) 宮崎大学統一認証アカウント 宮崎大学全学認証基盤で主体認証を行う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。宮崎大学統一認証アカウントの付与は、識別コードと主体認証情報の配布、主体認証情報格納装置の交付、アクセス制御における許可、又はそれらの組み合わせ等によって行う。

(適用範囲)

第 3 条 この規程は、本学の情報システムの利用者等に適用する。

(遵守事項)

第 4 条 利用者等は、この規程及び本学の情報システムの利用に関する手順並びに本学の個人情報保護規則等を遵守しなければならない。

(アカウントの交付)

第 5 条 宮崎大学統一認証アカウント（以下「MID」という。）で認証される情報システムを利用する者は、MID の交付を受けなければならない。

- 2 MID 以外のアカウントで認証される情報システムの利用を希望する者は、当該情報システムの管理者から当該情報システムで利用するアカウントの交付を受けなければならない。
- 3 来訪者に本学の情報システムを臨時的に利用させることを目的としてアカウントの交付を受ける場合、申請者は来訪者にこの規程を遵守させなければならない。同目的によるアカウントの利用が不要になった場合、申請者は速やかに当該情報システムの管理者に届け出なければならない。

(認証)

第 6 条 利用者等は、アカウントの利用に際して次の各号に掲げる事項を遵守しなければならない。

- (1) アカウントを利用して、学外から本学の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。
- (2) アカウントを他者に使用させ、又は主体認証情報を他者に開示してはならない。
- (3) 他者の主体認証情報を聞き出し、又は使用してはならない。
- (4) 主体認証情報は、適切に管理しなければならない。
- (5) アカウントによる認証接続中の利用者端末において、他者が無断で画面を閲覧・操作することができないように配慮しなければならない。
- (6) 不特定多数の人が操作（利用）可能な学外の端末を用いてアカウントによる認証接続を行ってはならない。
- (7) アカウントを他者に使用され、又はその危険が発生した際には、直ちに本学の情報システムの管理者に届け出なければならない。
- (8) 姓名の変更等識別コードの変更が必要になった際は、遅滞なく本学の情報システムの管理者に届け出なければならない。
- (9) 本学の情報システムの利用者の資格を喪失した際又は利用する必要がなくなった際は、当該情報システムの管理者にアカウント廃止を届け出なければならない。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、この限りでない。

- (10) 識別コード又は主体認証情報を失念した場合は、当該情報システムの管理者に識別コード再交付の申請を行わなければならない。

(機器等の利用)

第7条 利用者等は、様々な情報の作成、利用、保存等のため機器等の利用に際して次の各号に従わなければならない。

- (1) 本学の情報ネットワークに新規かつ固定的に機器等を接続しようとする場合は、事前に情報基盤センターの許可を得なければならない。ただし、情報コンセントや無線 LAN からあらかじめ指定された方法により本学の情報ネットワークに接続する場合はこの限りでない。
- (2) 前号により許可を受けた機器等の利用を取りやめる場合には情報基盤センターに届け出なければならない。
- (3) 機器等において、認証システム及びログ機能を動作させることが定められている場合には、それらの機能を設定し、動作させなければならない。不正ソフトウェア対策機能が導入されている機器等にあつては、その機能が最新の状態でシステムを保護するように努めなければならない。
- (4) 機器等は既知の脆弱性の影響を被ることのないよう可能な限り最新の状態を保たなければならない。
- (5) 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) 機器等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) 機器等の紛失及び盗難が発生した場合は、速やかに CSIRT に届け出なければならない。
- (8) 別に定めるガイドライン等に従い、これらの機器等の適切な保護に注意しなければならない。

(情報セキュリティ対策教育の受講義務)

第8条 利用者は、本学が実施する情報セキュリティに関する教育を受講しなければならない。

- 2 利用者は、情報セキュリティ対策の教育を受講できず、その理由が本人の責任ではないと思われる場合には、その理由について、部局情報セキュリティ責任者を通じて、CISO に報告しなければならない。
- 3 利用者は、本学が実施する情報セキュリティ対策の訓練に参加しなければならない。

(情報の取扱い)

第9条 利用者等は、格付けされた情報について、指定された取扱方法に従って取り扱わなければならない。

(制限事項)

第10条 利用者等が本学の情報システムについて次の各号に定める行為を行おうとする場合には CISO の許可を受けなければならない。

- (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
- (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、使用及び配布する行為
- (3) ネットワーク上の通信を監視する行為
- (4) 本学の機器等の利用情報を取得する行為及び本学の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) 本学の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)

第11条 利用者等は、本学の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) 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本学の情報システムへのアクセス
- (3) あらかじめ指定された情報システム以外の本学の情報システムを利用者等以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、ハラスメントにあたる行為
- (6) 個人情報又はプライバシーを侵害する行為
- (7) 前条に該当しない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の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) 上記の行為を助長する行為

(電子メールの利用)

第12条 利用者等は、電子メールの利用にあたっては、別に定めるガイドライン等に従い、宮崎大学情報セキュリティ基本方針及び関連規程の遵守のみならずマナーにも配慮しなければならない。

(ウェブの利用及び公開)

第13条 利用者等は、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、ファイルのダウンロード等を行う際には、別に定めるガイドライン等に従わなければならない。

(学外からの本学の情報システムの利用)

第14条 利用者等は、学外からの本学の情報システムへのアクセスにおいて、次の各号に従わなければならない。

- (1) 利用者等は、学外からアカウントを使って本学の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) 利用者等は、主体認証なく学外からアクセスできる本学の情報システムに要保護情報を保持してはならない。

(安全管理義務)

第15条 利用者等は、自己の管理する機器等について、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。
- (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。
- (3) 不正ソフトウェア対策機能の自動検査機能を有効にする。
- (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。
- (5) 外部からデータやソフトウェアを機器等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。
- (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。

(インシデント対応)

第16条 利用者等は、本学の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、速やかにCSIRTに通報しなければならない。

附 則

この規程は、平成30年4月1日から施行する。

附 則

この規程は、令和2年4月1日から施行する。