○宮崎大学情報システム管理者規程

（平成 30 年３月 22 日
制　　定）
改　正　令和２年３月 31 日

目次

第１章　総則

（趣旨）
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４項に基づき、宮崎大学（以下「本学」という。）における情報システムを運用・管理するにあたり必要な事項を定めるものとする。

（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、当該各号に定めるところによる。
(1)　利用者等　利用者及び本学の情報を臨時に許可を受けて利用する者をいう。
(2)　機器等　情報システムの構成要素（サーバ装置、端末、通信回線装置、特定用途機器、ソフトウェア）、外部電磁的記録媒体等の総称をいう。
(3)　サーバ装置　情報システムの構成要素である機器のうち、通信回線等を経由して接続してきた端末等に対して、自らが保持しているサービスを提供するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいう。
(4)　端末　情報システムの構成要素である機器のうち、利用者等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいう。端末には、モバイル端末も含まれる。
(5)　通信回線　複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りのない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。
(6)　通信回線装置　通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチルータ、無線 LAN アクセスポイント等のほか、ファイアウォール等も含まれる。
(7)　特定用途機器　プリンタ、スキャナ、NAS、複合機、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。
(8)　記録媒体　情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内

蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R 等の外部電磁的記録媒体がある。
(9) 機密性　情報に関して、アクセスを認められた者だけがこれにアクセスできる特性をいう。
(10) 完全性　情報が破壊、改ざん又は消去されていない特性をいう。
(11) 可用性　情報へのアクセスを認められた者が、必要時に中断することなく、情報にアクセスできる特性をいう。
(12) 要機密情報　機密性２情報及び機密性３情報をいう。
(13) 取扱制限　情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必須、読後廃棄その他情報の適正な取扱いを確実にするための手段をいう。
(14) 主体　情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。
(15) 識別　情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。
(16) 識別コード　主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。
(17) 主体認証　識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コードとともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した主体を正当な主体として認識する。なお、「認証」という用語は、公的又は第三者が証明するという意味を持つが、この規程における「主体認証」については、公的又は第三者による証明に限るものではない。
(18) 主体認証情報　主体認証をするために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワード等がある。
(19) アクセス制御　情報へのアクセス可能な者を制限することをいう。
(20) 権限管理　主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。
(21) 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。
(22) 暗号化　第三者に容易に解読されないよう、定められた演算を施しデータを変換することをいう。
(23) 電子署名　情報の正当性を保証するための電子的な署名情報をいう。

（適用範囲）
第３条　この規程は、本学の情報システムを運用・管理する者に適用する。

第２章　情報システムのライフサイクルにおける対策

（実施体制の確保）
第４条　情報システムの管理者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制を確保する。

（情報システムのセキュリティ要件の策定）
第５条　情報システムの管理者は、機器等を調達する場合には、情報システムが提供するサービス及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に策定し、仕様書等に明記する。

（情報システムの運用・保守を外部委託する場合の対策）
第６条　情報システムの管理者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために必要な要件を仕様書等に記載し、適切に実施させる。

（情報システムの構築時の対策）
第７条　情報システムの管理者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずる。
２　情報システムの管理者は、構築した情報システムを運用保守段階へ移行するに当たり、

移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずる。

（納品検査時の対策）

第８条　情報システムの管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等に定められた情報セキュリティ対策に係る要件が満たされていることを確認する。

（情報システムの運用・保守時の対策事項）

第９条　情報システムの管理者は、情報システムのセキュリティ監視を行う場合は、監視手順を定め、適切に監視運用する。

２　情報システムの管理者は、情報システムに実装されたセキュリティ機能を適切に運用する。

３　情報システムの管理者は、情報システムの管理情報について、当該情報の格付け及び取扱制限が適切に守られていることを確認する。

４　情報システムの管理者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずる。

（情報システムの更改・廃棄時の対策）

第１０条　情報システムの管理者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付け及び取扱制限を考慮した上で、適切な措置を講ずる。

（情報システムについての対策の見直し）

第１１条　情報システムの管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずる。

第３章　情報システムのセキュリティ機能

（主体認証機能の導入）

第１２条　情報システムの管理者は、情報システムや情報へのアクセスを管理するため、主体を特定し、それが正当な主体であることを検証する必要がある場合、識別及び主体認証を行う機能を設ける。

２　情報システムの管理者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずる。

（アクセス制御機能の導入）

第１３条　情報システムの管理者は、情報システムが取り扱う情報へのアクセスを、主体によって制御する必要がある場合、当該情報システムにアクセス制御を行う機能を設ける。

（権限管理機能の導入）

第１４条　情報システムの管理者は、情報システムを利用する主体に対して、主体認証を行う必要がある場合、情報システムの管理を実現するための権限に係る管理の機能を設ける。

（ログの取得・管理）

第１５条　情報システムの管理者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行う必要がある場合、ログを取得する。

２　情報システムの管理者は、情報システムにおいて、ログとして取得する情報項目、ログの保存期間、要機密情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理する。

３　情報システムの管理者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施する。

（通信の監視）

第１６条　情報システムの管理者は、ネットワークを通じて行われる通信を傍受してはならない。ただし、CISO 又は当該ネットワークの管理者は、セキュリティ確保のため、あらか

じめ指定した者に、ネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

（個人情報の取得と管理）
第１７条　電子的に個人情報の提供を求めようとする者は、提供を求める情報の範囲、利用の目的、その情報が伝達される範囲を、あらかじめ相手方に示さなければならない。
２　前項の個人情報は、当人の請求により開示、訂正又は削除をしなければならない。また、そのための手続を示さなければならない。

（利用者等が保有する情報の保護）
第１８条　情報システムの管理者は、利用者等が保有する情報を情報システムの運用に不可欠な範囲又は情報セキュリティインシデントへの対処に不可欠な範囲において、閲覧、複製又は提供することができる。

（暗号化機能・電子署名機能の導入）
第１９条　情報システムの管理者は、情報システムで取り扱う要機密情報の漏えいや改ざん等を防ぐため、暗号化や電子署名等の措置を講じ得る場合は、当該措置を実施する。

第４章　情報システムの脅威への対策

（ソフトウェアに関する脆弱性対策の実施）
第２０条　情報システムの管理者は、機器等の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施する。
２　情報システムの管理者は、公開された脆弱性の情報がない段階において、機器等で採り得る対策がある場合は、当該対策を実施する。
３　情報システムの管理者は、機器等で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずる。
４　情報システムの管理者は、機器等で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処する。
５　情報システムの管理者は、機器等で利用するソフトウェアの脆弱性対策が講じられていない状態の機器を学内通信回線に接続しない。

（不正プログラム対策の実施）
第２１条　情報システムの管理者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入する。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。
２　情報システムの管理者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずる。
３　情報システムの管理者は、不正プログラム対策の状況を適宜把握し、必要な対処を行う。

（不正プログラム対策ソフトウェア等に係る対策）
第２２条　情報システムの管理者は、不正プログラム対策ソフトウェア等及びその定義ファイルを常に最新のものが利用可能となるよう構成する。
２　情報システムの管理者は、不正プログラム対策ソフトウェア等により定期的に全てのファイルを対象としたスキャンを実施する。

（物理的な脅威から保護するための対策）
第２３条　情報システムの管理者は、機器等の盗難及び不正な持ち出しを防止するために、対策を講ずる。
２　情報システムの管理者は、第三者による不正操作を防止するために、対策を講ずる。
３　情報システムの管理者は、要機密情報を取り扱う情報システムについては、学内に設置する。ただし、学内への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにする。

（第三者により情報窃取されることを防止するための対策）
第２４条　情報システムの管理者は、第三者により情報窃取されることを防止するために、対策を講ずる。

（標的型攻撃対策の実施）
第２５条　情報システムの管理者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策を講ずる。
２　情報システムの管理者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策を講ずる。

第５章　端末・サーバ装置等

（端末の導入時の対策）
第２６条　端末の管理者は、要機密情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作等の物理的な脅威から保護するための対策を講ずる。
２　端末の管理者は、要機密情報を取り扱う端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずる。
３　端末の管理者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める。

（端末の運用時の対策）
第２７条　端末の管理者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行う。
２　端末の管理者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図る。

（端末の運用終了時の対策）
第２８条　端末の管理者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消する。

（サーバ装置の導入時の対策）
第２９条　サーバ装置の管理者は、要機密情報を取り扱うサーバ装置については、学内に設置する。ただし、学内への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにする。
２　サーバ装置の管理者は、要機密情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずる。
３　サーバ装置の管理者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定める。
４　サーバ装置の管理者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずる。

（サーバ装置の運用時の対策）
第３０条　サーバ装置の管理者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行う。
２　サーバ装置の管理者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図る。
３　サーバ装置の管理者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を監視する措置を講ずる。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

（サーバ装置の運用管理作業の記録に係る対策）

第３１条　サーバ装置の管理者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録する。

（サーバ装置の運用終了時の対策）
第３２条　サーバ装置の管理者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消する。

（特定用途機器の導入時の対策）
第３３条　特定用途機器の管理者は、特定用途機器が備える機能、設置環境及び取り扱う情報の格付け及び取扱制限に応じ、当該特定用途機器に対して想定される脅威へ対抗するためのセキュリティ要件を策定し、仕様書等に明記する。

（特定用途機器の運用時の対策）
第３４条　特定用途機器の管理者は、特定用途機器が備える機能について適切な設定等を行うことにより運用中の特定用途機器に対する、情報セキュリティインシデントへの対策を講ずる。

（特定用途機器の運用終了時の対策）
第３５条　特定用途機器の管理者は、特定用途機器の運用を終了する際に、特定用途機器の電磁的記録媒体の全ての情報を抹消する。

第６章　通信回線

（通信回線の導入時の対策）
第３６条　通信回線の管理者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付け及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずる。
２　通信回線の管理者は、通信回線装置を学内に設置すること。ただし、学内への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにする。
３　通信回線の管理者は、学内通信回線にインターネット回線、公衆通信回線等の学外通信回線を接続する場合には、学内通信回線及び当該学内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずる。
４　通信回線の管理者は、学内通信回線と学外通信回線との間で送受信される通信内容を監視するための措置を講ずる。
５　通信回線の管理者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決める。

（通信経路の分離に係る対策）
第３７条　通信回線の管理者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付け及び取扱制限に応じて、通信経路の分離を行う。

（通信回線の秘匿性確保に係る対策）
第３８条　通信回線の管理者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設ける。

（通信回線への情報システムの接続に係る対策）
第３９条　通信回線の管理者は、学内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能を設ける。

（通信回線及び通信回線装置の保護に係る対策）
第４０条　通信回線の管理者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策を講ずる。

（遠隔地から通信回線装置に対して行われるリモートアクセスに係る対策）
第４１条　通信回線の管理者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、対策を講ずる。

（通信回線の運用時の対策）
第４２条　通信回線の管理者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずる。
２　通信回線の管理者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行う。

（作業記録・設定情報等の取得と保管）
第４３条　通信回線の管理者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管する。

（通信回線の運用終了時の対策）
第４４条　通信回線の管理者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずる。

（リモートアクセス環境導入時の対策）
第４５条　通信回線の管理者は、リモートアクセス環境を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずる。

（無線 LAN 環境導入時の対策）
第４６条　通信回線の管理者は、無線 LAN 技術を利用して学内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化等のその他の情報セキュリティ確保のために必要な措置を講ずる。

（情報コンセント設置時の対策）
第４７条　通信回線の管理者は、情報コンセントを設置する場合は、情報セキュリティ確保のために必要な対策を講ずる。

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。