○宮崎大学情報セキュリティ基本規程

平成19年12月20日
制　　定

改正　平成22年９月22日　平成23年３月29日
平成26年２月27日　平成28年３月25日
平成30年３月22日　令和元年12月26日
令和２年３月13日　令和２年３月26日
令和３年３月25日

（趣旨）

第１条　この規程は、宮崎大学（以下「本学」という。）の情報資産に関するセキュリティ対策に必要な措置についての基本事項を定めるものとする。

（適用範囲）

第２条　この規程は、本学の情報資産を運用、管理、利用する全ての者に適用する。

（定義）

第３条　この規程において、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)　情報ネットワーク　本学により、所有又は管理されている全ての情報ネットワーク、本学との契約又は他の協定に従って提供される全ての情報ネットワークをいう。

(2)　情報システム　情報処理及び情報ネットワークに係わる全てのシステムをいう。

(3)　情報　情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報、情報システムに関係がある書面に記載された情報をいう。

(4)　情報資産　本学が所有又は管理する情報システム及び情報をいう。

(5)　教職員等　本学に勤務する常勤又は非常勤の役員・教職員（派遣職員を含む。）及び雇用契約の有無にかかわらず本学が受け入れを許可した者をいう。

(6)　学生等　学部学生、大学院生、研究生、科目等履修生、特別聴講学生、特別研究学生、外国人留学生及び別科生をいう。

(7)　管理者　情報システム及び機器等、並びに情報を運用・管理する者をいう。

(8)　利用者　教職員等及び学生等で、本学の情報資産、情報ネットワーク又は情報システムを利用する者をいう。

(9)　情報セキュリティ　情報資産の機密性、完全性及び可用性を維持することをいう。

(10)　電磁的記録　電子的方式、磁気的方式などで作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

(11)　情報セキュリティインシデント　情報セキュリティに関し、意図的又は偶発的に生じる、学内規則等又は法律に反する事故・事件をいう。

(12)　明示等　情報を取り扱う全ての者が当該情報の格付けについて共通の認識となるように措置することをいう。

（最高情報セキュリティ責任者）

第４条　本学における情報セキュリティ対策の最高責任者として、最高情報セキュリティ責任者（Chief Information Security Officer；CISO、以下「CISO」という。）を置く。

２　CISOは、本学における情報セキュリティ対策に関する事項を統括するとともに、本学における情報セキュリティ対策の推進体制が十分機能するように管理する。

３　CISOは、本学の教職員等の中から、学長が任命する。

４　CISOに事故があるときは、CISOがあらかじめ指名する者が、その職務を代行する。

（情報セキュリティアドバイザー）

第５条　CISOに情報セキュリティに関する専門的な助言を行う者として、情報セキュリティアドバイザーを置く。
２　情報セキュリティアドバイザーは、CISOが任命する。

（情報セキュリティ委員会）
第６条　情報資産の円滑で適正な運用を実現するための方針及び情報セキュリティに関する事項を審議するため、宮崎大学情報セキュリティ委員会（以下「情報セキュリティ委員会」という。）を置く。
２　情報セキュリティ委員会の組織及び運営に関し必要な事項は、別に定める。

（部局）
第７条　情報セキュリティ対策の運用に係る管理を行う単位として次のとおり部局を定める。
(1)　教育学部（附属学校を含む。）
(2)　工学教育研究部・工学部（フロンティア科学総合研究センター実験支援部門ＲＩ分野ＲＩ木花分室を含む。）
(3)　医学部（医学部附属病院、安全衛生保健センター分室、フロンティア科学総合研究センターのうち清武キャンパスに所在する部門、分野及び分室を含む。）
(4)　農学部（農学部附属施設、産業動物防疫リサーチセンター、フロンティア科学総合研究センター実験支援部門遺伝資源分野を含む。）
(5)　地域資源創成学部
(6)　センター（産学・地域連携センター、教育・学生支援センター、国際連携センター、多言語多文化教育研究センター、ＩＲ推進センター、安全衛生保健センター（分室を除く。）、情報基盤センター、附属図書館、テニュアトラック推進室）
(7)　事務局（監査室、企画総務部、財務部、施設環境部、学生支援部、研究国際部、清花アテナ男女共同参画推進室）

（部局情報セキュリティ責任者）
第８条　部局における情報セキュリティ対策の責任者として部局情報セキュリティ責任者を置く。
２　部局情報セキュリティ責任者は、当該部局における情報セキュリティ対策に関する事項を統括する。
３　部局情報セキュリティ責任者は、部局の長をもって充てる。ただし、前条第６号に定めるセンターについては、情報基盤センター長を部局情報セキュリティ責任者に充てるものとする。

（部局情報技術責任者）
第９条　部局情報セキュリティ責任者は、当該部局に部局情報技術責任者を置く。
２　部局情報技術責任者は、当該部局の情報セキュリティ対策の実施を担当する。
３　部局情報セキュリティ責任者は、当該部局の専任の教職員の中から部局情報技術責任者を任命する。ただし、第７条第６号に定めるセンターについては、情報基盤センター専任教員の中から任命する。

（部局情報技術責任補助者）
第１０条　部局情報セキュリティ責任者は、当該部局の情報セキュリティ管理業務において必要な単位ごとに、部局情報技術責任補助者を置く。
２　部局情報技術責任補助者は、部局情報技術責任者の任務を補助する。
３　部局情報セキュリティ責任者は、当該部局の教職員の中から部局情報技術責任補助者を指名する。

（部局の情報セキュリティに係わる委員会）

第１１条　部局情報セキュリティ責任者は、当該部局に情報セキュリティ対策を推進するための委員会を置く。
２　委員会の組織及び運営に関し必要な事項は、各部局が別に定める。

（情報セキュリティインシデント対応チーム）
第１２条　本学において発生した情報セキュリティインシデントへの速やかな対応のために、宮崎大学情報セキュリティインシデント対応チーム（Computer Security Incident Response Team；CSIRT、以下「CSIRT」という。）を置く。
２　CSIRTの組織及び運営に関して必要な事項は、別に定める。

（情報セキュリティ対策基本計画の策定及び見直し）
第１３条　CISOは、情報セキュリティ委員会における審議を経て、情報セキュリティ対策を総合的に推進するための情報セキュリティ対策基本計画を定める。
２　CISOは、情報セキュリティ対策の実施、監査及び点検結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、情報セキュリティ対策基本計画について定期的な見直しを行う。

（情報セキュリティ対策の推進）
第１４条　情報基盤センターは、情報セキュリティ対策の具体的遂行や遂行の統括等を行う。
２　情報基盤センターは、本学における情報セキュリティ対策に関する実施手順を整備する。
３　情報基盤センターは、情報セキュリティ基本計画に基づき、実施計画を策定し、情報セキュリティ教育を実施する。
４　情報基盤センターに情報セキュリティ対策の推進と実施を行う責任者として、情報セキュリティ対策実施責任者を置き、情報基盤センター長をもって充てる。
５　情報セキュリティ対策実施責任者は、部局情報セキュリティ責任者が実施する対策事項を統括するとともに、宮崎大学情報セキュリティ基本方針及び関連規程（以下「情報セキュリティ関連規程」という。）中の対策項目の遵守を推進する。
６　情報基盤センターは、情報セキュリティ対策に係る各部局間の情報共有及び連絡・調整を行う。

（情報の格付け）
第１５条　教職員等は、業務で取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、また、書面については機密性の観点から、当該情報の格付け及び取扱制限の指定等を行わなければならない。
２　教職員等は、利用する情報に指定等された情報の格付け及び取扱制限に従い、当該情報を適切に取り扱い、自らが担当している教育、研究及び事務の遂行以外の目的で、利用してはならない。
３　情報の格付け及び取扱いに関して必要な事項は、別に定める。

（情報セキュリティの維持）
第１６条　管理者及び利用者は、情報セキュリティ関連規程を遵守し、情報セキュリティを維持しなければならない。
２　管理者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行う。
３　利用者は、本学及び本学以外の情報セキュリティ水準の低下を招く行為を行ってはならない。
４　情報システムを管理するにあたって遵守しなければならない事項は、別に定める。
５　情報システムを利用するにあたって遵守しなければならない事項は、別に定める。

（情報セキュリティの監査）
第１７条　情報セキュリティにおける調査及び情報セキュリティの監査（以下「監査」という。）

等に関する事項を実施する責任者として、情報セキュリティ監査責任者を置き、監査室長をもって充てる。
2　情報セキュリティ監査責任者は、部局情報セキュリティ責任者が所管する組織における監査の実施を統括する。
3　情報セキュリティ監査責任者は、情報システムのセキュリティ対策が情報セキュリティ関連規程に基づく手順等に従って実施されていることを監査する。
4　部局情報セキュリティ責任者及びその他の関係者は、情報セキュリティ監査責任者の行う監査の適正かつ円滑な実施に協力する。
5　監査に関し必要な事項は、別に定める。

（違反及び例外措置）
第１８条　利用者は、情報セキュリティ関連規程への重大な違反（当該違反により本学の業務に重大な支障を来すもの又はその可能性のあるものを含む。）を知った場合には、情報セキュリティ関連規程の実施に責任を持つ部局情報セキュリティ責任者にその旨を報告しなければならない。
2　部局情報セキュリティ責任者は、前項の報告を受けた場合及び自らが重大な違反を知った場合には、速やかに調査を行い、事実を確認し、違反者及び必要な者に対し情報セキュリティの維持に必要な措置を講じるとともに、CISOにその旨を報告しなければならない。
3　情報セキュリティ関連規程の適用が職務の適正な遂行を著しく妨げる等の理由により、情報セキュリティ関連規程の規定とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合については、CISOへ申請し、情報基盤センターの審査を経てCISOの承認により例外措置を行うことができる。

（外部委託管理）
第１９条　本学の情報又は情報システムの運用業務の全て又はその一部を第三者に委託する場合には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じなければならない。
2　外部委託及び約款による外部サービスの利用に関する事項は、別に定める。

（サイバー攻撃への対応）
第２０条　CISOは、被害を受けたサイバー攻撃に係る情報について、可能な限り速やかに文部科学省に連絡する。

（情報セキュリティ関連規程の見直し）
第２１条　CISOは、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、情報セキュリティ関連規程について必要な見直しを行う。
2　情報基盤センターは、情報セキュリティ関連規程の見直しに応じて、情報セキュリティ対策に関する実施手順の見直し、又は整備した者に対して情報セキュリティ関連規程の見直しの指示を行う。

（雑則）
第２２条　この規程に定めるもののほか、情報セキュリティ対策に必要な事項は、別に定める。
2　本学が保有する個人情報のセキュリティについては、国立大学法人宮崎大学個人情報保護ポリシー、国立大学法人宮崎大学個人情報保護規則、宮崎大学保有個人情報管理規程及び情報セキュリティ関連規程に基づき対応する。
3　本学が保有する文書のセキュリティについては、国立大学法人宮崎大学法人文書管理規則及び情報セキュリティ関連規程に基づき対応する。

附　則
この規程は、平成19年12月20日から施行する。

附　則

この規程は、平成 22 年 10 月１日から施行する。

附　則

この規程は、平成 23 年３月 29 日から施行する。

附　則

この規程は、平成 26 年２月 27 日から施行する。

附　則

この規程は、平成 28 年４月１日から施行する。

附　則

１　この規程は、平成 30 年４月１日から施行する。
２　宮崎大学情報セキュリティ実施要項（平成 19 年２月 20 日制定）は、廃止する。

附　則

この規程は、令和２年１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。

附　則

１　この規程は、令和２年４月１日から施行する。
２　宮崎大学情報セキュリティ担当者連絡会細則（平成 26 年３月７日制定）は、廃止する。

附　則

１　この規程は、令和３年４月１日から施行する。
２　宮崎大学情報セキュリティ監査規程（平成 30 年３月 22 日制定）は、廃止する。