○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

（趣旨）

第１条　この規程は、宮崎大学（以下「本学」という。）の「情報セキュリティ基本方針」に基づき、本学の情報資産、情報ネットワーク及び情報システム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　本規程は、本学における情報資産、情報ネットワーク及び情報システムを運用、管理、利用する全ての者に適用する。

（定義）

第３条　本規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　情報資産　記録の媒体を問わず、本学が所有又は管理する情報全般をいう。

(2)　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。

(3)　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。

(4)　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。

(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。）をいう。

(6)　学生等　学生、研究生、研究員、研修員、研究者をいう。

(7)　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。

(8)　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。

(9)　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。

(10)　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。

(11)　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。

５　CISOは、情報セキュリティに関する専門的な知識等の助言を受けるために情報セキュリティアドバイザーを置く。情報セキュリティアドバイザーには、CIO補佐官をもって充てる。

（情報セキュリティ委員会）

第５条　本学の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決定する機関として、宮崎大学情報セキュリティ委員会を置き、次に掲げる事項を審議する。

(1)　情報化推進会議及び情報基盤センターにおいて企画又は策定される情報セキュリティに関連する各種事案に関する事項

(2)　情報セキュリティ対策活動に係る実施計画及び実施結果に関する事項

(3)　インシデントへの対応及び再発防止対策に関する事項

(4)　情報運用におけるリスク管理に関する事項

(5)　その他情報セキュリティに関する事項

２　情報セキュリティ委員会は、次に掲げる委員をもって組織する。

(1)　CISO

(2)　情報化統括責任者（CIO）
(3)　情報基盤センター長
(4)　副情報基盤センター長
(5)　部局情報セキュリティ責任者
(6)　その他CISOが必要と認める者
3　情報セキュリティ委員会に委員長を置き、委員長は前項第１号の委員をもって充てる。
4　委員長は情報セキュリティ委員会を招集し、その議長となる。

（部局情報セキュリティ責任者）
第６条　CISOは、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の部局を定め、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、部局の長又は部局情報運用を統括する者をもって充てる。
４　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し、部局の情報システムに対する情報セキュリティ対策の実施を委任する。
５　部局情報セキュリティ責任者は、部局情報セキュリティ委員会を設置し、当該部局における情報セキュリティ対策を推進する。

（情報セキュリティ担当者連絡会）
第７条　本学の情報セキュリティ対策、インシデント対応及び再発防止策等の推進並びに各部局間の情報共有及び連絡・調整を行うため、宮崎大学情報セキュリティ担当者連絡会を置く。
２　宮崎大学情報セキュリティ担当者連絡会の組織運営に関し必要な事項は、別に定める。

（情報セキュリティの監査・点検）
第８条　情報基盤センターは、情報セキュリティにおける調査及びセキュリティ監査・点検等に関する事項を実施する。
２　情報基盤センターに情報セキュリティの監査・点検を行う責任者として、情報セキュリティ監査責任者を置き、部局情報セキュリティ責任者が所管する組織における情報セキュリティ監査・点検の実施を統括する。
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本学の情報セキュリティポリシー及び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。

（情報セキュリティ対策の推進）
第９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、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。また、情報セキュリティ対策実施責任者は、情報セキュリティ関連規程中の対策項目の遵守を推進する。

（情報の格付け）
第１０条　情報の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並びに明示等を行わなければならない。

（利用者による情報セキュリティ維持）
第１１条　利用者は、本学の情報セキュリティポリシー及び関連規程を遵守し、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。
２　利用者は、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。

（外部委託管理）
第１２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。

（違反及び例外措置）
第１３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）を知った場合には、当該規程の実施に責任

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、前項に規定する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、違反者及び必要な者に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、情報基盤センターの審査承認によって例外措置を行うことができる。
４　情報基盤センターは、前項に規定する例外措置を承認した場合、CISOにその旨を報告しなければならない。

（サイバー攻撃への対応）
第１４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。

（見直し）
第１５条　情報基盤センターは、情報セキュリティポリシー及び関連規程等について、適時見直しを行う。

（雑則）
第１６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、情報セキュリティに関する実施要項として別に定める。

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。