○国立大学法人山梨大学情報システム運用基本規程

制定　平成２９年３月２７日

（目的）

第１条　この規程は、国立大学法人山梨大学（以下「本学」という。）における情報システムの運用及び管理について必要な事項を定め、もって本学の保有する情報の保護と活用並びに適切な情報セキュリティ対策を図ることを目的とする。

（定義）

第２条　この規程における用語の定義は、次の各号に掲げるとおりとする。

(1) 情報システム

情報処理及び情報ネットワークに係わるシステムで、次のものをいい、本学情報ネットワークに接続する機器を含む。

ア　本学により所有又は管理されているもの

イ　本学との契約又は他の協定によって提供されるもの

(2) 情報

情報には次のものを含む。

ア　情報システム内部に記録された情報

イ　情報システム外部の電磁的記録媒体に記録された情報

ウ　情報システムに関係する書面に記載された情報

(3) 情報資産

情報システム並びに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及び情報システムに関係する書面に記載された情報をいう。

(4) ポリシー

国立大学法人山梨大学情報システム運用基本方針及びこの規程をいう。

(5) 実施規程

ポリシーに基づいて策定される内規、基準及び計画をいう。

(6) 手順

実施規程に基づいて策定される具体的な手順、マニュアル及びガイドラインをいう。

(7) 利用者

本学の教職員等及び学生等で、本学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。

(8) 教職員等

本学の役員、本学に勤務する常勤及び非常勤の教職員（派遣職員を含む）並びにその他部局等の情報システム管理責任者が認めた者をいう。

(9) 学生等

山梨大学学則及び山梨大学大学院学則に規定する学部学生、大学院学生、研究生、科目等履修生、特別研究学生、特別聴講学生及び外国人留学生並びにその他部局等の情報

システム管理責任者が認めた者をいう。

(10)臨時利用者

教職員等及び学生等以外の者で、本学情報システムを臨時に利用する許可を受けて利用する者をいう。

(11)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。

(12)電磁的記録

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、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。

(13)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、意図的または偶発的に生じる、本学の規則又は法律に反する事故若しくは事件をいう。

(14)CSIRT（シーサート）

本学において発生した情報セキュリティインシデントに対処するため、本学に設置される体制をいう。Computer Security Incident Response Team の略。

(15)部局等

山梨大学基本規則に規定する教育研究組織及び山梨大学大学院総合研究部細則に規定する各学域並びに国立大学法人山梨大学事務組織細則に規定する各部（部を置かない部署にあっては課・室等）をいう。

（適用範囲）

第３条　この規程は、本学情報システムを運用・管理するすべての者並びに利用者及び臨時利用者に適用する。

（最高情報セキュリティ責任者）

第４条　本学に最高情報セキュリティ責任者（以下「CISO」という。）を置き、理事（情報担当）をもって充てる。

２　CISO は､本学情報システムの運用において､情報セキュリティに関する業務を統括する。

３　CISO は、全学の情報基盤として供される本学情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

４　CISO は、全学向け教育及び全学情報システムを担当する部局運用担当者向け教育を統括する。

（最高情報セキュリティ責任者補佐）

第５条　本学に、CISO の業務を補佐するため最高情報セキュリティ責任者補佐（以下「CISO 補佐」という。）を置き、CISO がこれを任命する。

２　CISO 補佐は、CISO を補佐し、情報セキュリティに係る技術的支援を行う。

（全学情報システム管理責任者）

第６条　本学に、全学情報システム管理責任者を置き、総合情報戦略部長をもって充てる。

２　全学情報システム管理責任者は、CISO の指示に基づき、本学情報システムの整備と運用に関し、ポリシー及びそれに基づく内規並びに手順等を実施する。

３　全学情報システム管理責任者は、情報システムの運用に携わる者及び利用者に対して、情報システムの運用及び利用並びに情報システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく内規並びに手順等の遵守を確実にするための教育を実施する。

４　全学情報システム管理責任者は、本学の情報システムのセキュリティに関する連絡と通報に係る事項を総括する。

（情報セキュリティ監査責任者）

第７条　本学に、情報セキュリティ監査責任者を置き、監査課長をもって充てる。

２　情報セキュリティ監査責任者は、学長の指示に基づき、情報セキュリティ監査に係る事務を統括する。

（管理運営部局）

第８条　本学情報システムの管理運営部局は、総合情報戦略機構とする。

２　管理運営部局は、全学情報システム管理責任者の指示により、次の各号に掲げる事務を行う。

(1) 本学情報システムの運用と利用におけるポリシーの実施状況取りまとめ

(2) 教育・訓練計画、リスク管理及び非常時行動計画等の実施状況取りまとめ

(3) 情報システムに係る部局情報システム管理責任者等への助言及び支援

(4) 本学情報システムのセキュリティに関する連絡と通報

（情報セキュリティインシデントに備えた体制の整備）

第９条　CISO は、本学における情報セキュリティ対策の実施及びインシデントに対処するための組織として、国立大学法人山梨大学情報セキュリティインシデント対応チーム（以下「山梨大学 CSIRT」）を置く。

２　山梨大学 CSIRT に関し必要な事項は、別に定める。

（部局情報システム管理責任者）

第１０条　部局等に、部局情報システム管理責任者を置き、当該部局等の長をもって充てる。

２　部局情報システム管理責任者は、当該部局等における情報システムの運用方針の決定や各種問題に対する処置を担当する。

（部局情報システム運用責任者）

第１１条　部局等に、部局情報システム運用責任者を置き、部局情報システム管理責任者が任命する。なお、部局情報システム管理責任者と兼務することができる。

２　部局情報システム運用責任者は、部局情報システム管理責任者の指示に基づき、当該部

局等における情報システムの構成の決定や運用上の問題に対する処置を担当する。
3　部局情報システム運用責任者の任命に関し必要な事項は、別に定める。

（部局情報システム運用担当者）
第１２条　部局情報システム運用責任者は、当該部局等の情報システムの管理業務において必要な単位ごとに、部局情報システム運用担当者を置く。部局情報システム運用担当者は、部局情報システム運用責任者が推挙し、部局情報システム管理責任者が任命する。
2　部局情報システム運用担当者は、部局情報システム運用責任者の指示により、当該部局等の情報システムの運用の実務を担当し、部局情報システム運用責任者を補佐する。
3　部局情報システム運用担当者の任命に関し必要な事項は、別に定める。

（全学情報セキュリティアドバイザーの設置）
第１３条　CISO は、情報セキュリティについて専門的な知識及び経験を有する者を全学情報セキュリティアドバイザーとして置くことができる。
2　CISO は、次の各号に倣い、全学情報セキュリティアドバイザーの業務内容を定める。
(1) 本学全体の情報セキュリティ対策の推進に係る CISO への助言
(2) 情報セキュリティ関係規則の整備に関する助言
(3) 対策推進計画の策定に関する助言
(4) 教育実施計画の立案に関する助言並びに教材開発及び教育実施の支援
(5) 情報システムに係る技術的事項に関する助言
(6) 情報システムの設計・開発を外部委託により行う場合に、調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に関する助言
(7) 利用者に対する日常的な相談対応
(8) 情報セキュリティインシデントへの対処の支援
(9) 前各号に掲げるもののほか、情報セキュリティ対策への助言及び支援

（役割の分離）
第１４条　情報セキュリティ対策の運用において、次の役割を同一人が兼務してはならない。
(1) 承認又は許可事案の申請者とその承認又は許可（以下「承認等」という。）を行う者（以下この条において「承認権限者等」という。）
(2) 監査を受ける者とその監査を実施する者
2　前項の規定にかかわらず、教職員等は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認等の可否の判断を行うことが不適切と認められる場合には、当該承認権限者等の上司に承認等の申請をする。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。
3　教職員等は、前項の場合において承認等を得たときは、承認権限者等に係る遵守事項に準じて、措置を講ずるものとする。

（情報の格付け）

第１５条　CISO は、情報システム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、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の規則を整備する。
２　情報の格付け及び取扱制限に関し必要な事項は、別に定める。

（学外の情報セキュリティ水準の低下を招く行為の防止）
第１６条　CISO は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規則を整備する。
２　本学情報システムを運用・管理する者並びに利用者及び臨時利用者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずるものとする。

（情報システム運用の外部委託管理）
第１７条　CISO は、本学情報システムの運用業務のすべて又はその一部を本学以外の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るものとする。
２　外部委託の管理に関し必要な事項は、別に定める。

（情報セキュリティ監査）
第１８条　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、ポリシーに基づく手順に従って実施されていることを監査する。
２　情報セキュリティ監査に関し必要な事項は、別に定める。

（見直し）
第１９条　本ポリシー、実施規程及び手順を整備した者は、各規則の見直しを行う必要性の有無を適時検討し、必要があると認める場合には、その見直しを行うものとする。
２　本学情報システムを運用・管理する者並びに利用者及び臨時利用者は、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ものとする。

（雑則）
第２０条　この規程に定めるもののほか、情報システムの運用及び管理並びに情報セキュリティに関し必要な事項は、別に定める。

附　則
この規程は、平成２９年４月１日から施行する。