群馬大学情報セキュリティ対策基本規則

令和 8. 4. 22　制定

（目的）

第１条　本規則は、群馬大学（以下「本学」という。）における情報及び情報システムの情報セキュリティ対策について基本的な事項を定め、もって本学の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

（適用範囲）

第２条　本規則において適用対象とする者は、全ての教職員及び本学の情報システムの利用者並びに臨時利用者とする。

２　本規則において適用対象とする情報は、以下の情報とする。

（１）教職員等が職務上使用することを目的として本学が調達し、又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）

（２）その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報

（３）第一号及び第二号のほか、本学が調達し、又は開発した情報システムの設計又は運用管理に関する情報

３　本規則において適用対象とする情報システムは、本規則の適用対象となる情報を取り扱う全ての情報システムとする。

（用語定義）

第３条　本規則において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（１）運用規程　対策基準に定められた対策内容を個別の情報システムや業務において運用するため、あらかじめ定める必要のある具体的な規程や基準をいう。

（２）学生等　学部学生、大学院学生、研究生、研究員、研修員並びに研究者等、その他、部局情報統括責任者が認めた者をいう。

（３）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、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

（４）教職員等　本学を設置する法人の役員及び、本学に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他、部局情報統括責任者が認めた者をいう。教職員等には、個々の勤務条件にもよるが、例えば、派遣労働者、一時的に受け入れる研修生等も含まれている。

（５）外部委託　本学の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委任」「準委任」「請負」といった契約形態を問わず、全て含むものとする。ただし、当該業務において本学の情報を取り扱わせる場合に限る。

（６）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。

（７）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。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。

（８）CSIRT（シーサート）　情報ネットワーク・コンピュータシステムに関連する危機事象へ対応するため、全学の危機管理室に設置された国立大学法人群馬大学情報セキュリティインシデント対応チームをいう。

（９）実施手順　対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。

(10) 情報　本規則第２条第２項に定めるものをいう。

(11) 情報システム　ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）をいう。

(12) 情報セキュリティインシデント　JIS Q 27000:2019における情報セキュリティインシデントをいう。

(13) 情報セキュリティ関連規程　対策基準及び実施手順を総称したものをいう。

(14) 情報セキュリティ対策推進体制　本学の情報セキュリティ対策の推進に係る事務を遂行するため、学内に設置された体制をいう。

(15) 対策基準　本学における情報及び情報システムの情報セキュリティを確保するための対策の基準として定める「D2101 情報セキュリティ対策基準」をいう。

(16) 情報セキュリティ対策基本計画（以下「基本計画」という。）　情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画をいう。

(17) 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。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。端末には、モバイル端末も含まれる。特に断りを入れた例としては、本学が調達又は開発するもの以外を指す「本学支給以外の端末」がある。また、本学が調達又は開発した端末と本学支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。

(18) 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。通信回線には、本学が直接管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

(19) 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、ルータ等のほか、ファイアウォール等も含まれる。

(20) ポリシー　本学が定める「D1000 情報セキュリティ対策基本方針」及び本規則をいう。

(21) モバイル端末　端末のうち、必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。
(22) 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ものをいう。
(23) 利用者等　利用者及び臨時利用者のほか、本学情報システムを取り扱う者をいう。
(24) 臨時利用者　教職員等及び学生等以外の者で、本学の情報システムを臨時に利用する許可を受けて利用するものをいう。
(25) 部局等　別表に定める情報セキュリティ対策の運用に関わる学部等の組織のまとまり

（最高情報セキュリティ責任者の設置）
第４条　本学における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者（以下「Chief Information Security Officer 。以下「CISO)」という。）を置き、学長が指名する理事をもって充てる。
２　CISOは、次に掲げる事務を統括する。
（１）情報セキュリティ対策推進のための組織・体制の整備
（２）情報セキュリティ対策基準の決定、見直し
（３）対策推進計画の決定、見直し
（４）情報セキュリティインシデントに対処するために必要な指示その他の措置
（５）情報セキュリティ監査の結果を踏まえた改善計画の策定等の必要な措置の指示
（６）前各号に掲げるもののほか、情報セキュリティに関する重要事項

（副CISOの設置）
第５条　CISOを補佐し、CISOに事故あるときはその職務を代行する副CISOを置き、情報化統括責任者補佐（以下「CIO補佐」という。）から選任する。

（全学情報セキュリティ会議）
第６条　本学情報セキュリティの円滑な運用のための審議は、情報化推進室全学情報セキュリティ会議（以下「情報セキュリティ会議」という。）において行う。
２　情報セキュリティ会議に関し必要な事項は、別に定める。

（情報セキュリティ監査責任者の設置）
第７条　CISOは、その指示に基づき実施する監査に関する事務を統括する者として、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、次の事務を統括する。
（１）監査実施計画の策定
（２）監査実施体制の整備
（３）監査の実施指示及び監査結果のCISOへの報告
（４）前各号に掲げるもののほか、情報セキュリティの監査に関する事項

（全学実施責任者・部局情報統括責任者の設置）
第８条　本学に全学実施責任者を置き、総合情報メディアセンター長をもって充てる。

2　全学実施責任者は、次の事務を統括する。
（1）情報セキュリティ対策に関する運用規程・実施手順の整備及び見直し並びに運用規程・実施手順に関する事務の取りまとめ
（2）情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備
（3）例外措置の適用審査記録の台帳整備等
（4）情報セキュリティインシデントに対処するための緊急連絡窓口の整備等
（5）前各号に掲げるもののほか、情報セキュリティ対策に係る事務
3　本学に、別表に定める情報セキュリティ対策の運用に関わる学部等の組織のまとまりである部局等ごとに、部局情報統括責任者を置く
4　前項に定める部局情報統括責任者は、別表に定める部局等の長をもって充てる。
5　部局情報統括責任者は、部局等の情報セキュリティに対して責任を負い、次の事務を統括する。
（1）部局の職場情報セキュリティ責任者の設置
（2）情報システムごとの部局情報責任者、責任者補佐の設置
（3）情報セキュリティインシデントの原因調査、再発防止策等の実施
（4）情報セキュリティに係る自己点検計画の策定及び実施手順の整備
（5）前各号に掲げるもののほか、情報セキュリティ対策に係る事務

（職場情報セキュリティ責任者の設置）
第9条　部局情報統括責任者は、教室、研究室、事務室等の管理組織単位ごとに情報セキュリティ対策に関する事務を統括する職場情報セキュリティ責任者1人を置く。
2　職場情報セキュリティ責任者は、命を受け、教室、研究室、事務室等の管理組織単位における情報の取扱いその他の情報セキュリティ対策に関する事務を統括する。

（情報システム運用委員会）
第10条　情報セキュリティに関する事項の実施は、情報化推進室情報システム運用委員会（以下「情報システム運用委員会」という）において行う。
2　情報システム運用委員会に関し必要な事項は、別に定める。

（部局情報責任者）
第11条　部局情報総括責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、部局情報責任者を置く。
2　前項の規定により設置する部局情報責任者は部局の情報化推進室員とする。
3　前項に該当する者がいない場合は、部局情報責任者は部局の各地区システム運用委員会委員とする。
4　2項及び3項に該当する者がいない場合は、部局情報責任者は全学実施責任者が代行するものとする。
5　部局情報責任者は、部局における運用方針の決定や情報システム上での各種問題に対する処置に関して部局情報統括責任者を補佐する。

（部局情報責任者補佐）

第12条　部局情報総括責任者は、部局で必要な管理単位毎に、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、部局情報責任者補佐を置くことができる。
２　前項の規定により設置する部局情報責任者補佐は、原則として各情報システム運用委員会委員とする。
３　部局情報責任者補佐は、部局における運用方針の決定や情報システム上での各種問題に対する処置に関して部局情報統括責任者及び部局情報責任者を補佐する。

（部局技術担当者・部局技術担当者補佐）
第13条　部局情報責任者は、所管する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技術担当者を置く。
２　部局技術担当者は、所管する情報システムの構成の決定や技術的問題に対する処置を担当する。
３　部局技術担当者は、所管する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技術担当者補佐を置く。
４　部局技術担当者補佐は、所管する情報システムの構成の決定や技術的問題に対する処置に対して部局技術担当者を補佐する。
５　部局情報責任者は、部局等の研究室や部署等のグループを単位とし、必要に応じてサブネットを割り当てる。部局技術担当者はグループ主管理者、部局技術担当者補佐はグループ副管理者とする。

（全学情報セキュリティアドバイザーの設置）
第14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き、以下を例とする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ことができる。
（１）全学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程の整備に係る助言
（３）対策推進計画の策定に係る助言
（４）教育実施計画の立案に係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係る助言
（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係る助言
（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）情報システムの分類に応じた情報セキュリティ対策に係る助言
（10）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又は支援

（情報セキュリティ対策推進体制の整備）
第15条　CISOは、本学の情報セキュリティ対策推進体制を整備し、その役割を規定する。
２　CISOは、以下を含む情報セキュリティ対策推進体制の役割を規定する。
（１）情報セキュリティ関係規程及び対策推進計画の策定に係る事務
（２）情報セキュリティ関係規程の運用に係る事務

（３）例外措置に係る事務
（４）情報セキュリティ対策の教育の実施に係る事務
（５）情報セキュリティ対策の自己点検に係る事務
（６）情報セキュリティ関係規程及び対策推進計画の見直しに係る事務
３　CISOは、情報セキュリティ対策推進体制の責任者を定める。

（情報セキュリティインシデントに備えた体制の整備）
第16条　CISOは、本学における情報セキュリティインシデントに対応する組織としてCSIRTを整備し、その役割を明確化する。
２　CISOは、以下を全て含むCSIRTの役割を規定する。
（１）　本学に関わる情報セキュリティインシデント発生時の対処の一元管理
（２）　情報セキュリティインシデントへの迅速かつ的確な対処
３　CSIRTに必要なその他の事項は、別に定める。

（全学BCPとの整合）
第17条　全学実施責任者は、情報セキュリティ関連規程の整備又は見直しを指示するに際し、当該規程が満たすべき要件として国立大学法人群馬大学危機管理規則及び国立大学法人群馬大学危機管理対応指針（全学BCP）との整合性の確保を含める。

（兼務を禁止する役割）
第18条　教職員等は、情報セキュリティ対策の運用において、以下の役割を兼務しない。
（１）承認又は許可（以下本条において「承認等」という。）の申請者と当該承認を行う許可権限者
（２）監査を受ける者とその監査を実施する者
２　教職員等は、承認等を申請する場合において、自らが許可権限者等であるときその他許可権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該許可権限者等の上司又は適切な者に承認等を申請し、承認等を得る。

（対策基準の策定）
第19条　CISOは、情報化推進室における審議を経て、サイバーセキュリティ戦略本部決定「政府機関等のサイバーセキュリティ対策のための統一基準群」に準拠し、これに相当する情報セキュリティ対策が可能となるように対策基準を定める。また、対策基準は、本学の業務、取り扱う情報、保有する情報システムに関するリスク評価の結果及び対策基準や計画の見直し結果を踏まえた上で定める。

（事務）
第20条　情報及び情報システムの情報セキュリティ対策に関する事務は、研究推進部総合情報メディアセンター課において処理する。

（規則の改廃）
第21条　この規則の改廃は、役員会の議を経て学長が行う。

附　則

この規則は、令和８年４月22日から施行し、令和８年４月１日から適用する。

別表

部局等	部局情報統括責任者	部局等に含まれる学部等の組織
事務局	事務局長	監査室、事務部を含む
共同教育学部	学部長	教育学研究科、共同教育学部附属学校部、特別支援教育特別専攻科を含む
情報学研究科	研究科長	情報学部を含む
医学系研究科	研究科長	医学部を含む。ただし、医学部保健学科、附属病院は除く。
医学部附属病院	病院長	
保健学研究科	研究科長	医学部保健学科を含む
理工学府	学府長	理工学部を含む
食健康科学研究科	研究科長	
パブリックヘルス学環	学環長	
医理工レギュラトリーサイエンス学環	学環長	
生体調節研究所	所長	
総合情報メディアセンター	センター長	
大学教育・学生支援機構	機構長	
研究・産学連携支援機構	機構長	
重粒子線医学推進機構	機構長	
未来先端研究機構	機構長	
食健康科学教育研究センター	センター長	
数理データ科学教育研究センター	センター長	
ダイバーシティ推進センター	センター長	
多職種連携教育研究研修センター	センター長	
多職種人材育成のための医療安全教育センター	センター長	
コアファシリティ総合センター	センター長	