公立大学法人福岡女子大学情報セキュリティ対策規程

法人規程第８０号
令和４年１月１日制定

（目的）

第１条　本規程は、公立大学法人福岡女子大学（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の実施に当たり必要な事項を定め、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。

（方針）

第２条　前条の目的を達するため、本学は本規程及びその他の規程等の定めるところにより、以下の対策を行う。

(1)　情報セキュリティ対策の実施体制の整備
(2)　情報及び情報システムの保護
(3)　情報システムや情報サービスの管理・運用
(4)　インシデントへの対処
(5)　利用者への啓発・教育
(6)　(1)～(5)を含む情報セキュリティマネジメントの実施

（定義）

第３条　本規程において、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)　情報システム

情報処理及び情報ネットワークに係るシステムで、次のものをいい、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等に従って提供されるもの

(2)　情報

次のものを含めて情報という。

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がある書面に記載された情報

(3)　情報資産

情報システム及び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がある書面に記載された情報をいう。

(4)　情報セキュリティ

全ての情報資産に対して、重要度に応じた機密性を確保しつつ、完全性及び可用性を維持すること、又はその維持された状態をいう。

(5) 実施規定

本規程に基づいて策定される規程、規則等をいう。

(6) 手順

実施規定に基づいて策定される具体的な手順や要領、マニュアル、ガイドライン等を指す。

(7) 教職員

本学に勤務する役員、職員（非常勤職員等を含む。） をいう。

(8) 学生

本学学則及び大学院学則に定める学生、研究生、科目等履修生、特別聴講学生、外国人留学生をいう。

(9) 利用者

教職員、学生、学術研究員、客員研究員で、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。

(10) 臨時利用者

教職員及び学生以外の者で、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) 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。

(12) 情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(13) 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、本学に設置された体制をいう。Computer Security Incident Response Team の略。

(14) 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する措置をいう。

(15) 部局

学部、研究科、各センター、図書館をいう。

（適用範囲）

第４条　本規程において適用対象とする者は、本学情報システムを管理・運用するすべての者、並びに利用者及び臨時利用者とする。

（義務）

第５条　本学の情報及び本学で扱う情報システムを利用する者、管理・運用の業務に携わる者は、本

規程及びその他の規程等を遵守しなければならない。

（最高情報セキュリティ責任者）

第６条　情報システムの運用に責任を持つ者として、本学に最高情報セキュリティ責任者を置き、学長が指名する副学長をもって充てる。

２　最高情報セキュリティ責任者は、本規程の決定や情報システム上での各種問題を総括するほか、情報セキュリティの確保に必要な事項を総括する。

３　最高情報セキュリティ責任者は、情報セキュリティに関する専門的な知識及び経験を有した者を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。

（全学情報セキュリティ実施責任者）

第７条　本学に全学情報セキュリティ実施責任者を置き、IR・情報化推進センター長をもって充てる。

２　全学情報セキュリティ実施責任者は、最高情報セキュリティ責任者を補佐するとともに、情報セキュリティ対策の周知徹底を図るため、部局情報セキュリティ総括責任者に対し情報セキュリティ対策に係る指示及び指導を行う。

３　全学情報セキュリティ実施責任者は、最高情報セキュリティ責任者の下で、本学情報システムの整備と運用に関し、本規程及びそれに基づく実施規定並びに手順等の制定及び改廃、実施を行う。

４　全学情報セキュリティ実施責任者は、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並びに利用及び情報システムのセキュリティに関する教育を企画及び実施し、本規程及びそれに基づく実施規定並びに手順等の遵守を確実にするための措置を講じる。

５　全学情報セキュリティ実施責任者は、セキュリティに関する学内外との連絡調整、周知徹底を行う。

６　全学情報セキュリティ実施責任者は、その実務を管理運営部局に委任することができる。

７　最高情報セキュリティ責任者に事故があるときは、その職務を代行する。

（情報セキュリティ委員会）

第８条　本学における情報セキュリティに関し必要な事項を審議するため、情報セキュリティ委員会を置き、IR・情報化推進センター委員会をもって充てる。

（管理運営部局）

第９条　情報システムの管理運営部局を置き、IR・情報化推進センターをもって充てる。

２　管理運営部局は、最高情報セキュリティ責任者の指示により、次に掲げる事務を行う。

(1)　情報システムの運用及び利用における規程等の総合調整

(2)　情報セキュリティインシデントの再発防止策の総合調整

(3)　講習計画、リスク管理及び非常時行動計画等の実施

(4)　情報システムのセキュリティに関する連絡及び通報

(5)　前各号に掲げるもののほか、情報セキュリティに関し、最高情報セキュリティ責任者が必要と認める事務

（部局情報セキュリティ総括責任者）

第１０条　各部局に部局情報セキュリティ総括責任者を置き、各部局の長をもって充てる。

２　部局情報セキュリティ総括責任者は、部局情報セキュリティ運用責任者及び情報セキュリティ担当者を総括し、これらの者に対し情報セキュリティに関する事項に関して指示及び指導を行う。

（部局情報セキュリティ運用責任者）

第１１条　部局情報セキュリティ総括責任者は、部局の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情報セキュリティ運用責任者を置き、各部局情報セキュリティ総括責任者が任命した者を充てる。

２　部局情報セキュリティ運用責任者は、部局情報セキュリティ総括責任者を補佐するとともに、当該部局の職員への情報セキュリティ対策実施の徹底を図るため、情報セキュリティ担当者に対し情報セキュリティ対策に係る指示及び指導を行う。

（情報セキュリティ担当者）

第１２条　部局情報セキュリティ運用責任者は、必要に応じて情報セキュリティ担当者を置く。

２　情報セキュリティ担当者は、当該所属内の情報セキュリティ対策を実施するため、所属内の情報資産及び情報システムの利用者及び臨時利用者に対して指導及び監督を行う。

（情報セキュリティアドバイザーの設置）

第１３条　最高情報セキュリティ責任者は、情報セキュリティアドバイザーを設置する場合に業務内容を以下のとおり定める。

(1)　本学全体の情報セキュリティ対策の推進に係る最高情報セキュリティ責任者への助言

(2)　情報セキュリティ関係規程の整備に係る助言

(3)　個別のセキュリティ対策推進計画の策定に係る助言

(4)　セキュリティ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)　情報セキュリティ事故への対処の支援

(8)　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

（情報セキュリティ監査責任者）

第１４条　本学情報システムのセキュリティを監視するため、情報セキュリティ監査責任者を置き、経営管理センター長をもって充てる。

２　情報セキュリティ監査責任者は、最高情報セキュリティ責任者の指示に基づき監査に関する事

務を総括する。

（役割の分離）

第１５条　情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないものとする。

(1)　承認又は許可事案の申請者とその承認又は許可を行う者

(2)　監査を受ける者とその監査を実施する者

（CSIRT）

第１６条　インシデントの発生が予見される場合及び発生時に迅速かつ円滑な対応を図り、その拡大及び再発を防止するためにCSIRTを設置する。

２　CSIRTは次に掲げる者をもって組織する。

(1)　管理運営部局

(2)　インシデント発生源の部局情報セキュリティ総括責任者

(3)　その他事案により管理運営部局の長が必要と認めた者

３　CSIRTはインシデント対応に係る次に掲げる業務を行う。

(1)　インシデントの通報、対応及び報告

(2)　インシデントの学内連絡調整

(3)　部局等に対する被害の拡大防止を図るための応急措置の指示又は勧告

(4)　インシデントの発生原因の調査及び再発防止策の立案

（情報の格付け）

第１７条　最高情報セキュリティ責任者は、情報システムで取り扱う情報について、機密性、完全性及び可用性の観点から、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定を整備する。

（本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１８条　全学情報セキュリティ実施責任者は、本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規定を整備する。

２　本学情報システムを管理・運用する者、並びに利用者及び臨時利用者は、本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。

（情報システム運用の外部委託管理）

第１９条　最高情報セキュリティ責任者は、本学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るものとする。

（情報セキュリティの確認及び検査）

第２０条　情報セキュリティ担当者は、情報セキュリティ対策の実施状況を必要に応じ確認及び検査し、問題がある場合には、速やかに是正しなければならない。

２　全学情報セキュリティ実施責任者は、必要に応じ部局の情報セキュリティ対策の実施状況について確認及び検査を行い、問題がある場合には、是正を命じることができる。
３　情報セキュリティ対策の実施状況に係る前２項の確認及び検査は、客観性を確保するために、外部の専門的知識・見識を有する者の協力を得て実施することができる。

（監査）
第２１条　情報セキュリティ監査責任者は、情報セキュリティ対策が、本規程に基づく手順に従って実施されていることを、定期に、又は随時に監査し、その結果を最高情報セキュリティ責任者に報告する。

（見直し）
第２２条　全学情報セキュリティ実施責任者は、本規程、及び本規程に基づく実施規定及び手順について、課題及び問題点が認められる場合には、その見直しを行う。
２　本学情報システムを管理・運用する者、及び利用者は、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。

（罰則）
第２３条　本規程に基づき定められる規程等に違反した場合の利用の制限および罰則は、福岡女子大学学則及び本学が定める就業規則に則って行うほか、それぞれの規程に定めるところによる。

附　則
この規程は、令和４年１月１日から施行する。