公立大学法人会津大学情報セキュリティ対策基本規程

（２０２１年４月１日規程第１号）
２０２３年７月１日規程第 11 号

（目的）

第一条　本規程は、公立大学法人会津大学（以下「本法人」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、もって本法人の保有する情報の保護と活用及び本法人情報セキュリティ対策基本方針において目指す情報セキュリティ水準の維持向上を図ることを目的とする。

（適用範囲）

第二条　本規程において適用対象とする者は、本法人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とする。

２　本規程において適用対象とする情報は、以下とする。

一　教職員等が職務上使用することを目的として本法人が調達し、又は開発した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。）

二　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

三　第一号及び第二号のほか、本法人が調達し、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　本規程において適用対象とする情報システムは、本規程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。

４　第１項から第３項の規定にかかわらず、会津大学復興創生支援センター情報セキュリティポリシー（ISMS 等）の適用対象となる情報及び情報システムについては、本規程の対象外とする。

ただし、会津大学復興創生支援センター情報セキュリティポリシー（ISMS 等）の適用対象となる情報及び情報システムのうち、会津大学情報センター（情報処理センター）利用規程に定める University of Aizu Information Network System に接続するものについては、本規程の適用対象とする。

（用語定義）

第三条　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。

一　情報

本規程第二条第２項に定めるものをいう。

二　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、本法人が調達、開発又は利用するもの（管理を外部委託しているシステムを含む。）若しくは本法人の情報ネットワークに接続されるものをいう。

三　重要情報システム

本法人の情報基盤として供される本法人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いう。

四　情報セキュリティポリシー

本法人が定める「公立大学法人会津大学情報セキュリティ対策基本方針」及び本規程をいう。

五　情報セキュリティ関連規程

情報セキュリティポリシーに基づいて策定される規程、基準及び計画を総称したものをいう。

六　対策基準

本法人が定める「公立大学法人会津大学情報セキュリティ対策基準」及び同基準から参照される関連基準をいう。

七　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。

八　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。

九　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。

十　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、本法人が調達又は開発、若しくは利用するもの（管理を外部委託しているシステムを含む。）をいう。

十一　端末

情報システムの構成要素である機器のうち、利用者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、本法人が調達又は開発するもの及び本法人支給以外の端末をいう。端末には、モバイル端末も含まれる。

十二　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。

十三　通信回線

複数の情報システム又は機器等（本法人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、本法人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、本法人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。

十四　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。

十五　情報ネットワーク

本法人の情報システム及び機器等と通信回線で構築されたネットワークをいう。

十六　部局

本法人における部局とは以下の各号に定めるものとする。

一　会津大学（管理部門）

二　会津大学（教育部門）

三　会津大学（研究部門）

四　産学イノベーションセンター（UBIC 部門）

五　復興創生支援センター（LICTiA 部門）

六　会津大学短期大学部（短大部門）

十七　部局総括責任者

部局ごとに情報セキュリティ対策に関する事務を統括する者をいう。

十八　情報セキュリティ対策推進体制

本法人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、法人内に設置された体制をいう。

十九　学生等

本法人の規程等で定める学部学生、大学院学生、科目等履修生、研究生、特別聴講学生及び研修員、その他、部局総括責任者が認めた者をいう。

二十　教職員等

本法人の役員及び、本法人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、部局総括責任者が認めた者をいう。

二十一　利用者

教職員等及び学生等で、本法人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。

二十二　臨時利用者

教職員等及び学生等以外の者で、本法人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。

二十三　外部委託

本法人の情報処理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。

二十四　情報セキュリティインシデント

JIS Q 27000:2014 における情報セキュリティインシデントをいう。

二十五　CSIRT（シーサート）

本法人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、本法人に設置さ

れた体制をいう。Computer Security Incident Response Team の略。

二十六　情報の格付け及び取扱制限

機密性、完全性、可用性について、それぞれ情報の内容に応じ講ずべき情報セキュリティ対策を明確にするための保護レベルを定める基準をいう。

情報の格付け及び取扱制限は、別に定める。

二十七　要管理対策区域

本法人の管理下にある区域（法人外組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域をいう。

（最高情報セキュリティ責任者）

第四条　本法人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を置く。理事長がこれを任命する。

２　最高情報セキュリティ責任者の任期は２年とする。

３　最高情報セキュリティ責任者を助けて本法人における情報セキュリティに関する事務を整理し、最高情報セキュリティ責任者の命を受けて本法人の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副責任者１人を必要に応じて置くことができる。

４　最高情報セキュリティ責任者は、次に掲げる事務を統括する。

一　情報セキュリティ対策推進のための組織・体制の整備

二　情報セキュリティポリシー及び情報セキュリティ関連規程の決定、見直し

三　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

四　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の決定、見直し

５　最高情報セキュリティ責任者は、本法人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ものを重要情報システムに指定することができる。

（公立大学法人会津大学情報セキュリティ委員会の設置）

第五条　最高情報セキュリティ責任者は、情報セキュリティポリシー及び情報セキュリティ関連規程等の審議を行う機能を持つ組織として、情報セキュリティ対策推進体制及びその他業務を実施する部局の代表者等を構成員とする公立大学法人会津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委員長及び委員は、理事長が情報セキュリティ対策推進体制及びその他の業務を実施する部局の代表者等から指名する。

３　情報セキュリティ委員会は、次に掲げる事項を審議する。

一　情報セキュリティポリシー及び関連規程等の制定及び改廃及びその実施に関する事項

二　情報セキュリティに関する啓発、教育及び研修に関する事項

三　情報セキュリティ監査に関する事項

四　情報セキュリティ体制の運用に関する事項

五　情報セキュリティインシデントの再発防止対策に関する事項

六　前各号に掲げるもののほか、情報セキュリティに関し必要な事項

（情報セキュリティ監査責任者）

第六条　最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括す

る者を情報セキュリティ監査責任者に任命する。

（管理運営部局）

第七条　情報セキュリティ委員会は、本法人情報システムの管理運営部局を次のとおり定める。

管理運営部局は主として事務局総務予算課が務める。

（管理運営部局が行う事務）

第八条　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、以下の各号に定める事務を行う。

一　情報セキュリティ委員会の運営に関する事務

二　法人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の取りまとめ

三　講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ

四　本法人の情報システムのセキュリティに関する連絡と通報

（部局総括責任者の設置）

第九条　最高情報セキュリティ責任者は、部局ごとに、情報セキュリティ対策に関する事務を統括する者として、部局総括責任者１人を置く。管理部門の部局総括責任者は、部局総括責任者を統括する。

２　管理部門の部局総括責任者は、最高情報セキュリティ責任者の命を受け、次の事務を統括する。

一　要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定

二　情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務の取りまとめ

三　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

四　例外措置の適用審査記録の台帳整備等

五　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

六　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　部局総括責任者は、最高情報セキュリティ責任者の命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括する。

一　部局の情報セキュリティ責任者の設置

二　情報システムごとの部局技術責任者の設置

三　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

四　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

五　前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務

（情報セキュリティ責任者の設置）

第十条　部局総括責任者は、別に定める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情報セキュリティ責任者１人を置く。

情報セキュリティ責任者は、所属する部局の者とする。

２　情報セキュリティ責任者は、部局総括責任者の命を受け、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。

（部局情報セキュリティ委員会）
第十一条　部局総括責任者は、部局情報セキュリティ委員会を必要に応じて置くことができる。
２　部局情報セキュリティ委員会は以下の各号に掲げる事項を実施する。
一　部局におけるポリシーの遵守状況の調査と周知
二　部局におけるリスク管理及び非常時行動計画の策定及び実施
三　部局における情報セキュリティインシデントの再発防止策の策定及び実施
四　部局における部局技術担当者向け教育の計画と企画及び実施

（部局情報セキュリティ委員会の構成員）
第十二条　部局情報セキュリティ委員会は、委員長及び次の各号に掲げる者を委員として組織する。
一　部局技術責任者
二　部局技術担当者
三　その他部局総括責任者が必要と認める者

（部局情報セキュリティ委員会の委員長）
第十三条　部局情報セキュリティ委員会の委員長は、部局総括責任者をもって充てる。

（部局技術責任者の設置）
第十四条　部局総括責任者は、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、部局技術責任者を、当該情報システムの企画に着手するまでに選任する。
２　部局技術責任者は、部局総括責任者の命を受け、情報システムにおける情報セキュリティ対策に関する事務を担う。
３　部局技術責任者は、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ことができる。

（情報セキュリティアドバイザーの設置）
第十五条　最高情報セキュリティ責任者は、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情報セキュリティアドバイザーに任命する。
２　情報セキュリティアドバイザーの任期は２年とする。
３　情報セキュリティアドバイザーの業務を、以下の各号のとおり定める。
一　本法人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
二　情報セキュリティポリシー及び関係規程の整備に係る助言
三　対策推進計画の策定に係る助言
四　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
五　情報システムに係る技術的事項に係る助言
六　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
七　情報セキュリティインシデントへの対処の支援

八　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）

第十六条　最高情報セキュリティ責任者は、本法人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こと。

２　最高情報セキュリティ責任者は、情報セキュリティ対策推進体制の責任者を定めること。

３　最高情報セキュリティ責任者は、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こと。

一　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

二　情報セキュリティ関係規程の運用に係る事務

三　例外措置に係る事務

四　情報セキュリティ対策の教育及び研修の実施に係る事務

五　情報セキュリティ対策の自己点検に係る事務

六　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

（情報セキュリティインシデントに備えた体制の整備）

第十七条　最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化する。

２　最高情報セキュリティ責任者は、教職員等のうちから CSIRT に属する職員として専門的な知識又は適性を有すると認められる者を選任する。そのうち、本法人における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置く。また、CSIRT 内の業務統括及び外部との連携等を行う教職員等を定める。

３　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。

４　最高情報セキュリティ責任者は、以下を含む CSIRT の役割を規定する。

一　本法人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

・本法人における情報セキュリティインシデント対処の管理

・情報セキュリティインシデントの可能性の報告受付

・本法人における情報セキュリティインシデントに関する情報の集約

・情報セキュリティインシデントの最高情報セキュリティ責任者等への報告

・情報セキュリティインシデントへの対処に関する指示系統の一本化

二　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

・情報セキュリティインシデントであるかの評価

・被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言

・文部科学省及び県への連絡

・外部専門機関等からの情報セキュリティインシデントに係る情報の収集

・他の機関等への情報セキュリティインシデントに係る情報の共有

・情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施

５　最高情報セキュリティ責任者は、実務担当者を含めた実効性のある CSIRT 体制を構築する。

６　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに

得られる体制を構築しておくこと。

７　最高情報セキュリティ責任者は、本法人における情報セキュリティインシデント対処について、CSIRT、情報セキュリティインシデントの当事者部局及びその他関連部局の役割分担を規定すること。

（兼務を禁止する役割）

第十八条　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こと。

一　承認又は許可の申請者と当該承認を行う者

二　監査を受ける者とその監査を実施する者

（対策基準の策定）

第十九条　最高情報セキュリティ責任者は、会津大学情報セキュリティ委員会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「政府機関等の情報セキュリティ対策のための統一基準」に準拠した対策基準を定める。また、対策基準は、本法人の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めるものとする。

（附　則）

この基本規程は、２０２１年４月１日から施行する。

（附　則）

この基本規程は、２０２３年７月１日から施行する。