公立大学法人長野県立大学情報システム運用基本規程

平成 30 年４月１日　規程第 606-2 号
最終改正　令和 6 年 11 月 25 日

（目的）

第１条　本規程は、公立大学法人長野県立大学（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基本事項を定め、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　本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

(1)　情報システム　基幹ネットワークシステム及び個別の学内情報システムを含む、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　本学との契約等に従って提供されるもの

(2)　基幹ネットワークシステム　情報システムのうち、本学情報ネットワークを構成するネットワーク機器及びサーバ類のことをいい、本学情報ネットワークに個別に接続された端末や学内情報システムはこれに含まない。

(3)　学内情報システム　情報システムのうち、教育支援に係わるシステム、事務処理に係わるシステム等個別のシステム並びに各システムを構成するサーバ類及び端末をいう。

(4)　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がある書面に記載された情報

(5)　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がある書面に記載された情報をいう。

(6)　ポリシー　本学が定める公立大学法人長野県立大学情報システム運用基本方針及び本規程をいう。

(7)　実施規程　ポリシーに基づいて策定される規程及び、基準、計画をいう。

(8)　手順　本規程に基づいて策定される具体的な手順やマニュアル、ガイドラインを指す。

(9)　教職員等　本学法人の役員及び勤務する常勤又は非常勤の教職員（客員教員は含まない）及び第４条に定める最高責任者が認めた者をいう。

(10)　学生等　長野県立大学学則及び長野県立大学大学院学則に定める学生及び最高責任者が認めた者をいう。

(11)　利用者　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ものをいう。

(12)　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ものをいう。

(13)　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。
(14)　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。
(15)　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、本学の定める規程または法律に反する事故又は事件をいう。
(16)　CSIRT（シーサート）　本学において発生した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。

（適用範囲）
第３条　本規程は、前条第 1 項第 1 号から第 5 号に定める情報システム及び情報並びに情報資産に係る運用及び管理並びに利用に適用する。
２　前条第 1 項第 9 号から第 12 号及び第 14 条並びに第 17 条に定める者に適用する。

（最高責任者）
第４条　本学における情報システム、情報セキュリティの運用及び管理に関する責任及び権限を有する最高責任者をおき、理事長をもって充てる。
２　理事長は、ポリシー及びそれに基づく規程の決定や情報システム上での各種問題に対する処置を総括する。
３　理事長は、全学向け教育及び本学情報システムを担当する管理運営部局システム担当者向け教育を総括する。
４　理事長に事故があるときは、副理事長がその職務を代行する。

（実施責任者）
第５条　本学における情報システム、情報セキュリティの運用及び管理実務における実施責任者をおき、事務局長をもって充てる。
２　事務局長は、理事長の指示により、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規程並びに手順等の実施により運用管理を行う。
３　事務局長は、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し、ポリシー及びそれに基づく規程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　事務局長は、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を行う。
５　事務局長は、情報セキュリティインシデントの原因調査、再発防止策等を実施する。
６　事務局長は、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を行う。
７　事務局長は、例外措置の適用審査記録の台帳整備等を行う。
８　事務局長は、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を行なう。
９　事務局長は、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おいて本学情報システムを代表する。

（システムの管理者）

第６条　事務局長は、各情報システムにおける管理者（以下、「システム管理者」という。）を置く。

２　事務局長は、システム管理者に、同一の所管課内等における複数のシステムを管理させることができる。

３　システム管理者は、担当する情報システムの構成の決定や技術的問題並びに管理運用課題に対する処置を担当する。

４　各システム管理者は、実施責任者の指示により情報セキュリティインシデント対応を行う。

５　各システム管理者は、第９条に定めるシステム担当者に対して、ポリシー及びそれに基づく規程並びに手順、並びにシステム管理者の所管する規程等の遵守を確実にするための教育を実施する。

（基幹ネットワークシステムの管理者が行う事務）

第７条　基幹ネットワークシステムのシステム管理者は、事務局長の指示により、以下の各号に定める事務を行う。

(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の取りまとめ
(2)　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
(3)　本学情報ネットワークの利用方法の周知
(4)　ポリシー及びそれに係わる各種規程等の見直しとその事務
(5)　その他必要とされる事項

（学内情報システムの管理者が行う事務）

第８条　各学内情報システムのシステム管理者は、事務局長の指示により、以下の各号に定める事務を行う。

(1)　学内情報システムの運用状況の管理監督
(2)　学内情報システムの利用方法の周知
(3)　基幹ネットワークシステムの管理運営部局への連絡と情報共有
(4)　基幹ネットワークシステムの管理運営部局からの指示による事務処理及びその他の処置、対応等
(5)　その他必要とされる事項

（システム担当者）

第９条　第６条第１項に定めるシステム管理者は、個別の教職員等（以下、「システム担当者」という。）を指名して実務を担当させることができる。

２　システム担当者は、システム管理者の指示により、各情報システムの運用の技術的及び管理運用実務を担当し、利用者への教育を補佐する。

（情報システムの運用及び管理に係わる者の禁止事項）

第 10 条　本学の各情報システムに係る運用及び管理に携わる者は、次に掲げる事項を行ってはならない。

(1)　運用及び管理上の理由なく各情報システム上の通信を監視し、または利用内容及び記録を閲覧・採取、または持ち出す行為
(2)　管理、運用を行ううえで得た情報資産の目的外使用及び流出させる行為
(3)　管理者権限を悪用、乱用する行為
(4)　上記の行為を助長する行為

（違反行為への対処、利用停止・制限）
第 11 条　理事長は、利用者及び臨時利用者が基本方針及び本規程並びにその他本学の規程に違反する、または違反する恐れがある行為を行った場合、次に掲げる措置を行うことができる。
(1)　当該行為の中止命令
(2)　当該行為に係る情報発信、通信等の遮断命令
(3)　当該行為者の各情報システムへの接続禁止
(4)　当該行為者のアカウントの停止、削除または取り消し
(5)　その他本学の規程等に基づく措置、または手続の開始
2　理事長は、利用者及び臨時利用者が本学情報システムを利用するにあたり不適格であると認められる場合、各情報システムの利用停止または制限等の措置を講じることができる。

（役割の分離）
第 12 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こととする。
(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（以下、本項において「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　前項の定めに係わらず、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又は許可（以下「承認等」という。）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与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずる。

（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 13 条　本学情報システムを運用・管理する者は、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。
2　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を行ってはならない。

（情報システム運用の外部委託管理）
第 14 条　理事長は、本学情報システムの運用業務のすべてまた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契約書類に明示

する等の必要な措置を講じるものとする。

（情報セキュリティインシデントに備えた体制の整備）
第 15 条　理事長は、CSIRT を整備し、その役割を明確化する。
２　理事長は、教職員等のうちから CSIRT に属する職員として各情報システムのシステム担当者及び専門的な知識又は適性を有すると認められる者を選任し、本学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。
３　理事長は、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。

（点検・見直し）
第 16 条　ポリシー、実施規程及び手順を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。
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。
３　本学情報システムを運用・管理する者は定期および必要に応じて自己点検を実施しなければならない。その結果、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。

（情報セキュリティアドバイザーの設置）
第 17 条　理事長は、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として置くことができる。
２　情報セキュリティアドバイザーの業務は以下のとおりとする。
(1)情報セキュリティ対策の推進に係る理事長への助言
(2)情報セキュリティ関係規程の整備に係る助言
(3)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
(4)情報システムに係る技術的事項に係る助言
(5)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
(6)利用者に対する日常的な相談対応
(7)情報セキュリティインシデントへの対処の支援
(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

（その他）
第 18 条　本規程に定めるもののほか、必要な事項は別に定める。

附　則
この規程は、平成 30 年４月１日から施行する。
附　則
この規程は、令和６年 11 月 25 日から施行する。