

国立大学法人電気通信大学情報システム運用基本規程

制定 平成22年9月28日規程第89号
最終改正 令和3年9月13日規程第12号

目次

- 第1章 総則（第1条－第3条）
- 第2章 管理・運用（第4条－第21条）
- 第3章 情報システムの利用等（第22条－第26条）
- 第4章 雑則（第27条）
- 附則

第1章 総則

（趣旨）

第1条 国立大学法人電気通信大学（以下「本学」という。）における情報システムの運用については、本基本規程の定めるところによる。

（適用範囲）

第2条 本基本規程は、本学情報システムを運用・管理・利用するすべての者に適用する。

（定義）

第3条 本基本規程において、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

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。）若しくは本学情報ネットワークに接続されるものをいう。

（2）情報ネットワーク

情報ネットワークには次のものを含む。

- ①本学により、所有又は管理されている全ての情報ネットワーク
- ②本学との契約あるいは他の協定に従って提供される全ての情報ネットワーク

（3）情報資産

情報システム、情報ネットワークに接続された情報ネットワーク機器並びに電子計算機、及びそこで取り扱われる電磁的記録をいう。

（4）ポリシー

本学が定める国立大学法人電気通信大学情報セキュリティポリシー及び本基本規程をいう。

（5）手順

ポリシーに基づいて策定される具体的な手順やマニュアル、ガイドラインをいう。

（6）利用者

職員等、学生及び臨時利用者で、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。

(7) 職員等

本学の役員、職員及び非常勤の職員（派遣職員を含む。）をいう。

(8) 学生

本学の学域学生、大学院学生、特別研究学生、研究生、科目等履修生、特別聴講学生、短期海外交流学生、委託生及び外国人留学生をいう。

(9) 臨時利用者

職員等及び学生以外の者で、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。

(10) 機密性

情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保することをいう。

(11) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(12) 可用性

情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連する情報資産にアクセスできる状態を確保することをいう。

(13) 明示等

情報を取り扱うすべ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措置することをいう。明示等には、情報ごとに格付を記載することによる明示のほか、当該情報の格付に係る認識が共通となるその他の措置も含まれる。その他の措置の例としては、特定の情報システムに記録される情報について、その格付を情報システムの規程等に明記するとともに、当該情報システムを利用する全ての者に周知すること等が挙げられる。

(14) 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。

(15) 電磁的記録

電子的方式、磁気的方式その他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。

(16) インシデント

情報セキュリティに関し、意図的又は偶発的に生じる、本学規程又は法律に反する事故又は事件をいう。

(17) CSIRT (Computer Security Incident Response Team)

インシデントに対処するため、設置されたチームをいう。

(18) 部局等

別表に掲げる情報システムの管理単位をいう。

(19) 外部委託

本学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。

(20) 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。

(21) 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。

(22) 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。

(23) 情報セキュリティ関連規程

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。

(24) 対策基準

本学が定める「国立大学法人電気通信大学情報セキュリティ対策基準」をいう。

(25) 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。

第2章 管理・運用

（情報化統括責任者）

第4条 本学に情報化統括責任者（以下「CIO」という。）を置き、本学の理事又は教育研究職員のうちから学長が指名する。

2 CIOは、次の各号に掲げる事項を総括する。

- (1) 本学における情報関連施策の企画、立案及びその実施に関すること。
- (2) ポリシー及びそれに基づく規程の整備及び情報システム上での各種問題に対する処置に関すること。
- (3) 本学情報システムの運用及び利用に関する教育の企画及び実施に関すること。

3 CIOの任期は2年とし、再任を妨げない。ただし、欠員が生じた場合の後任者の任期は、前任者の残任期間とする。

（情報化統括責任者補佐）

第5条 情報システムに関しCIOを補佐するため、本学に情報化統括責任者補佐（以下「CIO補佐」という。）を置き、情報基盤センター長（以下「センター長」という。）をもって

充てる。

- 2 前項の規定にかかわらず、センター長がCIOに指名されたときのCIO補佐は、情報基盤センター副センター長（以下「副センター長」という。）又は情報基盤センター専任の教育研究職員（以下「センター教員」という。）のうちからCIOが指名する。
- 3 CIO補佐の任期は2年とし、再任を妨げない。ただし、欠員が生じた場合の後任者の任期は、前任者の残任期間とする。
- 4 前項の規定にかかわらず、CIO補佐の任期の末日は、CIOの任期の末日以前でなければならない。

（最高情報セキュリティ責任者）

第6条 本学情報システムに係る情報セキュリティに関することを統括的に決定及び実施するため、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、本学の理事又は教育研究職員のうちから学長が指名する。

- 2 CISOの任期は2年とし、再任を妨げない。ただし、欠員が生じた場合の後任者の任期は、前任者の残任期間とする。

（最高情報セキュリティ責任者補佐）

第7条 本学の情報セキュリティの実施に関し、CISO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、センター長をもって充てる。

- 2 前項の規定にかかわらず、センター長がCISOに指名されたときのCISO補佐は、副センター長又はセンター教員のうちからCISOが指名する。
- 3 CISO補佐の任期は2年とし、再任を妨げない。ただし、欠員が生じた場合の後任者の任期は、前任者の残任期間とする。
- 4 前項の規定にかかわらず、CISO補佐の任期の末日は、CISOの任期の末日以前でなければならない。

（情報セキュリティアドバイザー）

第8条 CISO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する職員を情報セキュリティアドバイザーとして置く。

- 2 CISOは、以下を例とする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。

- (1) 全学の情報セキュリティ対策の推進に係るCISO及びCISO補佐への助言
- (2) 情報セキュリティ関係規程の整備に係る助言
- (3) 対策基本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を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

（情報セキュリティ監査責任者）

第9条 本学に情報セキュリティ監査責任者を置き、本学の理事又は職員のうちから学長が指名する。

- 2 情報セキュリティ監査責任者は、情報セキュリティ監査に関する事務を統括する。
- 3 情報セキュリティ監査は、独立性を有する者による実施により、ポリシー及び情報セキ

セキュリティ関連規程が確実に遵守され、問題点が改善されることを目的とする。

- 4 前項のほか、情報セキュリティ監査の実施等に関して必要な事項は、別に定める「国立大学法人電気通信大学情報セキュリティ監査規程」による。

(情報セキュリティ委員会)

第10条 本学の情報システム、ネットワーク及び情報資産における全学的な情報セキュリティ対策を行うため、電気通信大学情報セキュリティ委員会（以下「委員会」という。）を置く。

- 2 委員会に関し必要な事項は、別に定める。

(管理運営部局)

第11条 本学情報システムに関する管理運営部局は情報基盤センター（以下「センター」という。）とする。

(部局総括責任者)

第12条 各部局等に部局総括責任者を置き、部局等の長をもって充てる。

- 2 部局総括責任者は、当該部局等における情報システムの運用方針・管理体制の決定及び情報システム上での各種問題に対する処置を行う。
- 3 部局総括責任者は業務に関して、その権限を部局総括責任者が指名する者又は次条に規定する部局運用責任者に委譲することができるものとする。

(部局運用責任者)

第13条 部局総括責任者は、当該部局等に部局運用責任者を置き、当該部局等の職員のうちから指名する。

- 2 部局運用責任者は、次の各号に掲げる事項を実施する。
 - (1) 部局等の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関すること。
 - (2) 利用者に対する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に関すること。
 - (3) 当該部局等が保有する情報機器と情報資産、割り当てられた情報ネットワーク及びそれらの情報セキュリティの維持に関すること。
 - (4) 前条第2項に規定する事項への協力に関すること。
- 3 部局運用責任者は業務に関して、次条に規定する当該部局等内のいずれかの部局システム管理者を補佐として指名し、権限を委譲することができるものとする。

(部局システム管理者)

第14条 部局運用責任者は、1人又は数人の部局システム管理者を置き、実務を担当させるものとする。部局システム管理者は部局運用責任者が推挙し、部局総括責任者が指名する。

- 2 部局システム管理者は、部局運用責任者の指示により、部局等の情報システムの運用の技術的実務を担当し、利用者への教育を補佐する。

(区域情報セキュリティ責任者)

第15条 部局総括責任者は、CIS0が別に定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者1人又は数人を置くものとする。なお、区域情報セキュリティ責任者は部局運用責任者が兼任してもよいこととする。

(インシデントに備えた体制の整備)

第16条 CIS0は、電気通信大学情報セキュリティインシデント対応チーム（以下「UEC-

CSIRT」 という。) を整備する。

- 2 CISOは、職員等のうちからUEC-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、本学におけるインシデントに対処するための責任者としてUEC-CSIRT責任者を置く。
- 3 CISOは、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。
- 4 CISOは、UEC-CSIRT責任者へ必要な権限を委譲することができるものとする。
- 5 CISOは、UEC-CSIRTの活動が円滑に行えるよう活動環境を整えとともに、必要に応じてUEC-CSIRTの活動内容について助言又は指導を行うものとする。

(UEC-CSIRTの役割)

第17条 UEC-CSIRTの役割は、次の各号のとおりとする。ただし、第3号については、前条第4項に基づき権限の委譲を受け実施する。

- (1) 学内及び学外からのインシデントの報告及び連絡の受付
- (2) インシデント発生時における情報の収集及び分析
- (3) インシデントの発生を未然に防止するための措置及びインシデントの被害の拡大防止を図るための緊急措置(当該情報システムの強制的な遮断・隔離措置を含む。)の実施
- (4) CISOへのインシデントに関する報告及び提言
- (5) インシデントの学外関係機関への報告、連絡及び情報共有
- (6) インシデントの再発防止策の策定
- (7) 職員等のインシデントへの対応能力を向上させるための研修及び訓練等の実施
- (8) 情報セキュリティ対策の自己点検の実施
- (9) その他インシデントに関する事項

(役割の分離)

第18条 情報セキュリティ対策の運用において、次の各号に掲げる役割を同じ者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者又は許可者
- (2) 監査を受ける者とその監査を実施する者

(情報の格付け)

第19条 CIO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定を整備するものとする。

(対策基準の策定)

第20条 CISOは、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ものとする。

- 2 前項の対策基準は、本学の業務、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こと。

(全学BCPとの整合)

第21条 CISO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本学が別に定める事業継続計画(全学BCP)との整合性の確保を含めなければならない。

第3章 情報システムの利用等

(ポリシー及び手順の遵守)

第22条 利用者は、本学情報システムを利用する場合は、ポリシー及び手順を遵守するとともに、情報モラルに反しないよう努めなければならない。

2 利用者は、前項に規定するポリシー及び手順の遵守を誓約した誓約書をCIOに提出するものとする。

(情報システム利用に関する禁止行為)

第23条 利用者は、本学情報システムを利用する場合は、次の各号に定める行為を行ってはならない。

- (1) 当該情報システム及び情報について定められた目的以外の利用
- (2) 差別、名誉毀損、侮辱、ハラスメントにあたる情報の発信
- (3) 個人情報やプライバシーを侵害する情報の発信
- (4) 守秘義務に違反する情報の発信
- (5) 著作権等の財産権を侵害する情報の発信
- (6) 通信の秘密を侵害する行為
- (7) 営業ないし商業を目的とした本学情報システムの利用
- (8) 部局総括責任者の許可（業務上の正当事由）なくネットワーク上の通信を監視し、又は情報機器の利用情報を取得する行為
- (9) 不正アクセス禁止法に定められたアクセス制御を免れる行為、又はこれに類する行為
- (10) 部局総括責任者の要請に基づかずに管理権限のないシステムのセキュリティ上の脆弱性を検知する行為
- (11) 過度な負荷等により本学又は学外の円滑な情報システムの運用を妨げる行為
- (12) その他法令に基づく処罰の対象となり、又は損害賠償等の民事責任を発生させる情報の発信
- (13) 前号の行為を助長する行為
- (14) 本学又は学外の情報システムの円滑な運用を妨げるソフトウェアのインストールやコンピュータの設定の変更を行う行為

2 利用者は、ファイルの自動公衆送信機能を持ったP2Pソフトウェアについては、教育・研究目的以外にこれを利用してはならない。このようなP2Pソフトウェアを教育・研究目的に利用する場合は、CIOの許可を得なければならない。

3 利用者は、ソフトウェアを違法にコピーして利用してはならない。

(大学支給外端末等の学内での使用)

第24条 私物のパソコン又は電磁的記録媒体等その他大学が支給する以外の端末等（以下「支給外端末等」という。）を学内での使用については、次の各号に掲げるとおりとする。

(1) 職員等の場合

職員等が支給外端末等を学内で情報システムに接続して使用することは、原則禁止する。ただし、業務等でやむを得ず学内で情報システムに接続して使用の場合は、部局運用責任者又は部局システム管理者の許可を得なければならない。

(2) 学生の場合

学生が支給外端末等を学内の研究室で使用する場合は、部局システム管理者の許可を得て、部局システム管理者の監督のもと使用しなければならない。

(インシデントが発生した場合の取り扱い)

第25条 インシデントが発生した場合は、次のとおり報告するものとする。

- (1) インシデントを発見した者は、速やかにUEC-CSIRTに報告し、報告を受けたUEC-CSIRTはインシデントが発生した部局等の部局運用責任者に報告するものとする。
 - (2) UEC-CSIRTは、応急の対策を講じたうえでCISOに報告するものとする。
 - (3) CISOは、内容に応じて役員会又は教育研究評議会に報告するものとする。
- 2 インシデントが発生した部局等の部局運用責任者は、UEC-CSIRTと協力して対策を講じるものとする。

(報告)

第26条 CIOは、利用者が次の各号に掲げる行為（以下「禁止行為等」という。）のいずれかを行ったときは、情報ネットワークの利用の制限を科すとともに速やかに学長に報告するものとする。

- (1) 第22条第2項に規定する誓約書の未提出又はポリシー若しくは手順違反行為
 - (2) 第23条に規定する禁止行為
 - (3) 第24条に規定する支給外端末等の学内での使用に関する違反行為
 - (4) インシデントを発生させる行為
 - (5) その他本学又は学外の情報システムの運用を妨げる行為
- 2 前項の規定にかかわらず、CIOが軽微な禁止行為等であると認めたときは、CIOが情報ネットワークの利用に関し制限を科すことができるものとする。

第4章 雑則

(雑則)

第27条 この規程に定めるもののほか、情報システムの運用に関し必要な事項は、別に定める。

附 則

この規程は、平成22年9月28日から施行する。

附 則 (平成24年9月26日規程第111号)

この規程は、平成24年9月26日から施行する。

附 則 (平成27年10月28日規程第14号)

この規程は、平成27年10月28日から施行する。

附 則 (平成28年3月23日規程第60号)

- 1 この規程は、平成28年4月1日から施行する。
- 2 この規程の施行日以降も在学する電気通信学部及び情報理工学部の学生については、なお従前の例による。

附 則 (平成29年1月25日規程第69号)

この規程は、平成29年1月25日から施行する。ただし、改正後の第22条第2項の規

定については、平成29年4月1日から施行する。

附 則 (平成30年3月30日規程第163号)
この規程は、平成30年4月1日から施行する。

- 附 則 (令和2年11月11日規程第26号)
- 1 この規程は、令和2年11月11日から施行する。
 - 2 国立大学法人電気通信大学情報システム運用・管理規程(平成24年9月26日制定)は廃止する。
 - 3 この規程の施行前における情報セキュリティ対策に関する事項については、改正後の第20条第1項の規定に基づく対策基準を定めるまでは、なお従前の例による。

附 則 (令和2年12月22日規程第47号)
この規程は、令和3年1月1日から施行する。

附 則 (令和3年3月31日規程第73号)
この規程は、令和3年4月1日から施行する。

附 則 (令和3年9月13日規程第12号)
この規程は、令和3年9月13日から施行する。

別表(第3条第18号関係)

部 局 等	
情報理工学域	I類(情報系)
	II類(融合系)
	III類(理工系)
	先端工学基礎課程
	共通教育部
大学院情報理工学研究科	情報学専攻
	情報・ネットワーク工学専攻
	機械知能システム学専攻
	基盤理工学専攻
	共同サステイナビリティ研究専攻
	共通教育部
	連携教育部
総合コミュニケーション科学推進機構	
コヒーレント光量子科学研究機構	レーザー新世代研究センター
	量子科学研究センター
先端ワイヤレス・コミュニケーション研究センター	
宇宙・電磁環境研究センター	
脳・医工学研究センター	

i パワードエネルギー・システム研究センター	
人工知能先端研究センター	
ナノトライボロジー研究センター	
燃料電池イノベーション研究センター	
スーパー連携大学院推進室	
グローバル化教育機構	実践的コミュニケーション教育推進室
	I T活用国際ものづくり教育推進室
	国際P B L教育推進室
	グローバル・アライアンス・ラボ推進室
附属図書館	
保健管理センター	
全学教育・学生支援機構	大学教育センター
	学生支援センター
	アドミッションセンター
情報基盤センター	
eラーニングセンター	
実験実習支援センター	
ものづくりセンター	
国際教育センター	
研究設備センター	
産学官連携センター	
U E Cアライアンスセンター	
社会連携センター	
広報センター	
U E C A S E A N教育研究支援センター	
U E C中国教育研究支援センター	
U E Cコミュニケーションミュージアム	
評価室	
内部監査室	
安全・環境保全室	
研究活性化推進室	
研究戦略推進室	
国際戦略推進室	
男女共同参画・ダイバーシティ戦略推進室	
I R室	
教育研究技師部	
事務組織	