国立大学法人電気通信大学情報システム運用基本規程

平成22年 9月28日
改正
平成24年 9月26日
平成27年10月28日
平成28年 3月23日
平成29年 1月25日
平成30年 3月30日

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

情報処理及び情報ネットワークに係わるシステムをいう。

(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

情報には次のものを含む。

①情報システム内部に記録された情報

②情報システム外部の電磁的記録媒体に記録された情報

③情報システムに関係がある書面に記載された情報

(4) 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。

(5) 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。

(6) 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。

(7) 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。

(8) 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。

(9) 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。

(10) 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。

(11) 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。

(12) 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。

(13) 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。

(14) 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。

(15) 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。

(16) 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。

(17) 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。

(18) 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。

(19) 部局等

各類・専攻、各センター等情報システムの管理単位をいう。

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。
（情報システム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、本学に情報システム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。
（情報システム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、情報システム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した職員を情報セキュリティアドバイザーとして置く。
（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､本学の職員のうちから CIOが推挙し、学長が指名する。
2　情報セキュリティ監査責任者は、情報セキュリティの監査に関する事務を統括する。
（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。

（部局統括責任者）

第12条　各部局等に部局統括責任者を置き、部局等の長をもって充てる。

２　部局統括責任者は、当該部局運用責任者と協力し、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　部局統括責任者は業務に関して、その権限を部局統括責任者が指名する者、又は、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　部局統括責任者は、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。

３　部局運用責任者は業務に関して、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、部局統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。

（インシデントに備えた体制の整備）

第15条　CISO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るとともに、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16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) その他インシデントに関する事項

（役割の分離）

第17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18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。

（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19条　CIO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の規定を整備するものとする。

２　本学情報システムを運用・管理・利用する者は、原則として、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じるものとする。

（情報システム運用の外部委託管理）

第20条　CIOは、本学情報システムの運用業務のすべ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。

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21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22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) 部局統括責任者の許可（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) 部局統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。

（私物パソコン等の学内での使用）

第23条　私物（大学の所有物以外のものをいう。）のパソコン又は電磁的記録媒体（以下「私物パソコン等」という。）を学内で使用する場合は、次の各号に掲げるとおりとする。

(1) 職員等の場合

職員等が私物パソコン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する場合は、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

学生が私物パソコン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24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25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２１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２２条に規定する禁止行為

(3) 第２３条に規定する私物パソコン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　監査・見直し

（情報セキュリティ監査）

第26条　情報セキュリティ監査責任者は、情報システムのセキュリティ対策がポリシーに基づく手順に従って実施されていることを監査する。

２　情報セキュリティ監査に関する事項は、別に定める。

（見直し）

第27条　CIOは、ポリシー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・利用する者は、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。

（雑則）

第28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

この規程は、平成２４年９月２６日から施行する。

附　則

この規程は、平成２７年１０月２８日から施行する。

附　則

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

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

この規程は、平成３０年４月１日から施行する。