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
改正
平成25年 3月22日
平成25年 6月27日
平成26年 2月26日
平成26年12月24日
平成27年 3月27日
平成28年 3月23日
平成28年 6月22日
平成28年12月27日
平成29年 1月26日
平成29年 2月28日
平成30年 3月30日
平成30年10月29日

目次

第１章　総則

（趣旨）

第１条　この規程は、国立大学法人電気通信大学情報システム運用基本規程（以下「運用基本規程」という。）第２８条の規定に基づき、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適切な運用・管理に関し、必要な事項を定めるものとする。

（定義）

第２条　運用基本規程に定めるもののほか、この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 情報ネットワーク機器　情報ネットワークの接続のために設置され、電子計算機により情報ネットワーク上を送受信される情報の制御を行うための装置（ファイアウォール、ルータ、ハブ、情報コンセント及び無線ネットワークアクセスポイントを含む。）をいう。

(2) 電子計算機　コンピュータ全般のことを指し、オペレーティングシステム及び接続される周辺機器を含むサーバ装置及び端末をいう。

(3) 安全区域　電子計算機及び情報ネットワーク機器を設置した事務室、研究室、教室又はサーバルーム等の内部であって、利用者等以外の者の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域をいう。

(4) アカウント　主体認証を行う必要があると認めた情報システムにおいて、主体に付与された正当な権限をいう。

(5) 要機密情報　運用基本規程第３条第１１号に規定する機密性を考慮した取扱いをすべき情報のうち、次に掲げるものをいう。

ア　秘密文書に相当する機密性を要するもの

イ　秘密文書に相当する機密性は要しないが、漏えいにより、利用者等の権利が侵害され、又は本学の業務の遂行に支障を及ぼすおそれのあるもの

(6) 要保全情報　運用基本規程第３条第１２号に規定する完全性を考慮した取扱いをすべき情報のうち、改ざん、誤びゅう又は破損により、利用者等の権利が侵害され、又は本学の業務の的確な遂行に支障（軽微なものを除く。）を及ぼすおそれのあるものをいう。

(7) 要安定情報　運用基本規程第３条第１３号に規定する可用性を考慮した取扱いをすべき情報のうち、その滅失、紛失又は当該情報が利用不可能であることにより、利用者等の権利が侵害され、又は本学の業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれのあるものをいう。

(8) 要保護情報　前３号に掲げる情報をいう。

（適用範囲）

第３条　この規程は、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。

（組織体制）

第４条　全学情報システムの運用・管理体制は、運用基本規程第４条から第２０条までに定めるところによる。

２　運用基本規程第３条第１９号に規定する部局等は、別表のとおりとする。

（禁止事項）

第５条　本学の情報ネットワーク機器と電子計算機、通信回線の運用・管理を行う者は、次に掲げる事項を行ってはならない。

(1) 部局統括責任者の許可なく情報ネットワーク上の通信を監視し、又は情報ネットワーク機器及び電子計算機の利用記録を採取する行為

(2) 管理者権限を濫用する行為

(3) 上記の行為を助長する行為

第２章　情報システムの設置、運用及び運用終了の際の遵守事項

第１節　設置時

（情報ネットワーク機器と電子計算機の保護）

第６条　部局システム管理者は、電子計算機及び情報ネットワーク機器の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する以下の情報セキュリティ対策を実施するものとする。

(1) セキュリティホール対策

(2) 不正プログラム対策のためのアンチウイルスソフトウェア等の導入

(3) サービス不能攻撃対策

(4) 踏み台対策

（安全区域）

第７条　部局システム管理者は、情報システムによるリスク（物理的損壊又は情報の漏えい若しくは改ざん等のリスクを含む。）を検討し、安全区域に施設及び環境面からの対策を実施するものとする。

２　部局運用責任者は、安全区域に不審者を立ち入らせない措置を講ずるものとする。

３　部局運用責任者は、要保護情報を取り扱う情報システムについては、安全区域に設置すべきかを判断し必要に応じ安全区域に設置するものとする。

４　部局運用責任者は、情報ネットワーク機器を安全区域に設置するものとする。

（電子計算機の対策）

第８条　部局システム管理者は、電子計算機で利用可能なソフトウェアを定めるものとする。ただし、利用可能なソフトウェアを列挙することが困難な場合には、利用不可能なソフトウェアを列挙、又は両者を併用することができる。

２　部局システム管理者は、要保護情報を取り扱うモバイルPCについては、学外で使われる際にも学内で利用される電子計算機と同等の保護手段が有効に機能するよう構成するものとする。

（通信回線の対策）

第９条　学内外の通信回線は、情報化統括責任者（以下「CIO」という。）及び情報基盤センターが、通信回線のリスクやセキュリティレベル及びサービスレベルを検討した上で、通信回線と情報ネットワーク機器を確保し、運用するものとする。

２　部局システム管理者は、無線LANを設置する場合は、その必要性を検討するものとする。この場合において無線LAN機器が他の無線LAN機器と干渉しないようにするものとする。

３　部局システム管理者は、学外通信回線を利用する場合は、情報基盤センターに届け出るものとする。この場合において、情報基盤センターは、CIOの承認を得た上で、学外通信回線の利用を許可するものとする。

（上流ネットワークとの関係）

第10条　CIOは、本学情報ネットワークを構築し運用するにあたっては、本学情報ネットワークと接続される上流ネットワークとの整合性に留意するものとする。

第２節　運用時

（セキュリティホール及び攻撃に対する対策）

第11条　部局システム管理者は、管理対象となる電子計算機及び情報ネットワーク機器上で利用しているソフトウェアに関して、公開されたセキュリティホールやソフトウェアに対する各種攻撃に関連する次の各号に掲げる事項を継続的に行うものとする。

(1) セキュリティホール情報及び攻撃に関する情報の入手とそれらのリスクの分析
(2) 対策の必要性の検討
(3) 対策方法又は一時的な回避方法の検討
(4) 対策の実施
(5) 対策試験の必要性の検討と実施
(6) 対策の実施内容の記録
(7) 対策に関する情報の共有

２　部局システム管理者は、定期的にセキュリティホール対策及びソフトウェア構成の状況を確認、分析し、不適切な状態にある電子計算機及び情報ネットワーク機器が確認された場合の対処を行うものとする。

（通信回線の対策）

第12条　部局運用責任者は、情報システムのセキュリティの確保が困難な事由が発生した場合には、他の情報システムと共有している通信回線から独立した閉鎖的な通信回線に構成を変更するものとする。

２　部局システム管理者は、運用基本規程第２３条に従い電子計算機及び情報ネットワーク機器の通信回線への接続を管理するものとする。

３　部局システム管理者は、情報システムにおいて基準となる時刻に、情報ネットワーク機器の時刻を同期するものとする。

４　部局システム管理者は、無線LAN機器及びVPN装置は必ず暗号化を設定するものとする。

５　情報システムセキュリティ責任者（以下「CISO」という。）は、学内通信回線と学外通信回線との間で送受信される通信内容を監視するものとする。

第３節　運用終了時

（電子計算機の対策）

第13条　部局システム管理者は、電子計算機の運用を終了する場合に、データ消去ソフトウェア若しくはデータ消去装置の利用、又は物理的な破壊若しくは磁気的な破壊等の方法を用いて、すべての情報を復元が困難な状態にするものとする。

（情報ネットワーク機器の対策）

第14条　部局システム管理者は、情報ネットワーク機器の利用を終了する場合には、情報ネットワーク機器の内蔵記録媒体のすべての情報を復元が困難な状態にするものとする。

第４節　ＰＤＣＡサイクル

（情報システムの計画・設計）

第15条　部局統括責任者は、部局等内の情報システムセキュリティ要件を決定するものとする。

２　部局運用責任者は、前項の部局等の情報システムセキュリティ要件を満たす情報システムのＰＤＣＡサイクルの手順と対策を定め、それらを実施するものとする。

第３章　情報システムに係る文書及び台帳整備

（情報システムの文書整備）

第16条　部局運用責任者は、所管する情報システムについて以下の事項を記載した文書を整備するものとする。

(1) 情報システム名、管理部署及び管理責任者の氏名・連絡手段

(2) システム構成

(3) 接続する学外通信回線の種別

(4) 取り扱う情報の格付け及び取り扱い制限に関する事項

(5) 当該情報システムの設計・開発、運用、保守に関する事項

２　部局運用責任者は、所管する情報システムについて整備した文書に基づいて、情報システムの運用管理において情報セキュリティ対策を行うものとする。

（情報システムの台帳整備）

第17条　CIOは、各部局等の所管する情報システムについて整備した文書を収集し、台帳として整備するものとする。

２　部局運用責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システムの台帳の記載事項についてCIOに報告するものとする。

第４章　情報の取扱い

（情報の目的外使用の禁止）

第18条　職員等は、業務の目的の範囲で、情報を作成、入手又は利用するものとする。この場合において、当該情報は業務の目的に則して適切に取り扱わなければならない。

（要保護情報の取扱い）

第19条　職員等は、業務の目的以外で要保護情報を学外に持ち出してはならない。

２　要保護情報は、必要以上に複製及び配布してはならない。

（情報の保存）

第20条　職員等は、電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行うものとする。

２　職員等は、情報が保存された電磁的記録媒体を適切に管理するものとする。

（情報の保存期間）

第21条　職員等は、電磁的記録媒体に保存された情報の保存期間が定められている場合には、当該情報の保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去するものとする。

（情報の移送に関する許可）

第22条　職員等は、要保護情報を移送する場合には、部局統括責任者の許可を得るものとする。

（電磁的記録の保護対策）

第23条　職員等は、電磁的記録を移送する場合には、次の対策を検討し、安全な移送方法により実施するものとする。

(1) パスワード又は暗号化による保護

(2) 電子署名の付与

(3) バックアップ

(4) 複数経路での移送

（電磁的記録の消去方法）

第24条　職員等は、電磁的記録媒体を廃棄する場合には、すべての情報を復元が困難な状態にする（以下「抹消する」という。）ものとする。

２　職員等は、電磁的記録媒体を他の者へ提供又は他の目的に利用する場合には、当該電磁的記録媒体に保存された不要な情報を抹消するものとする。

第５章　アクセス制御

（アクセス制御機能の導入）

第25条　部局システム管理者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討するものとする。この場合において、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があるとみなす。

２　部局システム管理者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設け、適切に設定するものとする。

第６章　アカウント管理

（アカウント管理機能の導入）

第26条　部局システム管理者は、すべての情報システムについて、アカウント管理を行う必要性の有無を検討するものとする。この場合において、要保護情報を取り扱う情報システムについては、アカウント管理を行う必要があるとみなす。

２　前項の場合において、アカウントの認証機能は、次の各号を満たすものとする。

(1) 認証情報は暗号化して保存すること。

(2) 盗難及び盗聴の危険がないように保管すること。

(3) 利用者が自らの認証情報を設定・更新・変更する機能を用意すること。

(4) アカウントの認証機能は十分に信頼性のおける方式であること。

(5) セキュリティ侵害が認められるときに部局システム管理者がアカウントの認証を停止させる機能を持つこと。

３　部局システム管理者は、アカウント管理を行う必要があると認めた情報システムにお

いて、アカウントの管理を行う機能を設け、設定するとともにアカウント管理の手続を設け、実施するものとする。

第７章　ログ管理

（ログ管理機能の導入）

第27条　部局システム管理者は、すべての情報システムについて、ログ管理を行う必要性の有無とその保存期間を検討するものとする。

２　部局システム管理者は、ログを取得する必要があると認めた情報システムには、ログ管理のためにログを取得する機能を設けるものとする。この場合において、ログは定められた保存期間中は不当な消去､改ざん及びアクセスがされないようにするものとする。

３　部局システム管理者は、定期的に取得したログを確認し、インシデントがあれば運用基本規程第２４条に従うものとする。

（通信の監視）

第28条　情報システムを運用・管理・利用する者は、ネットワークを通じて行われる通信を傍受してはならない。ただし、CIO又は当該ネットワークを管理する部局統括責任者は、セキュリティ確保又は教育研究目的のため、あらかじめ指定した者に、あらかじめ指定した範囲でネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。

２　監視を行う者及び監視記録の伝達を受けた者は、ネットワーク運用・管理のために必要な限りで、これを取得、閲覧し、かつ、保存することができる。

３　前項の者は、次の各号に掲げる行為を行ってはならない。ただし、教育研究目的で利用及び発表する場合はCIOの監督の下で利用及び発表することができる。

(1) 監視記録を不必要に閲覧すること。

(2) 不必要となった監視記録を保存すること。

(3) 法令に基づく場合等を除き、監視記録の内容を他の者に伝達すること。

第８章　例外措置

（例外措置）

第29条　CIOは、例外措置の適用の申請を審査する者（以下、本条において「許可権限者」という。）を定め、審査手続を整備するものとする。

２　許可権限者は、利用者等による例外措置の適用の申請を、前項の審査手続に従って審査し、許可の可否を決定するものとする。また、決定の際に、例外措置の適用審査記録を作成し、CIOに報告するものとする。

３　許可権限者は、例外措置の適用を許可した期間の終了期日に、許可を受けた者からの報告の有無を確認し、報告がない場合には、許可を受けた者に状況を報告させ、必要な措置を講ずるものとする。ただし、許可権限者が報告を要しないとした場合は、この限りではない。

４　CIOは、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査責任者からの求めに応ずるものとする。

第９章　インシデント対応

（インシデントが発生した場合の体制整備と再発防止）

第30条　CISOは、情報セキュリティに関するインシデントが発生した場合、被害の拡大を防ぐとともに、インシデントから復旧するための体制を整備するものとする。

２　部局運用責任者は、インシデントが発生した場合には、UEC-CSIRTと協力して再発防止策を実施するために必要な措置を講ずるものとする。

第10章　本学支給以外の情報システム

（本学支給以外の情報システムに係る安全管理措置の整備）

第31条　CIOは、要保護情報について本学支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置についての規定を整備するものとする。

第11章　学外の情報セキュリティ水準の低下を招く行為の禁止

（規定の遵守）

第32条　CIOは、利用者等に対して、別に定める学外情報セキュリティ水準低下防止手順に基づいて必要な措置を講ずるよう指示するものとする。

第12章　教育・研修

（情報セキュリティ対策の教育の実施）

第33条　CISOは、情報セキュリティ対策について、部局統括責任者、部局運用責任者、部局システム管理者、利用者等（以下「教育啓発対象者」という。）に対し、その啓発をするものとする。

２　CISOは、情報セキュリティ対策について、教育啓発対象者に教育すべき内容を検討し、教育のための資料を整備するものとする。

３　CISOは、教育啓発対象者が受講できるように、情報セキュリティ対策の教育に係る計画（以下「講習計画」という。）を企画、立案するとともに、その実施体制を整備するものとする。

４　情報基盤センターは、利用者等からの情報セキュリティ対策に関する相談に対応するものとする。

５　情報基盤センターは、部局統括責任者、部局運用責任者及び部局システム管理者に対して情報セキュリティ対策の教育を実施するものとする。

６　部局運用責任者及び部局システム管理者は、利用者等に対して、講習計画に定める講習を実施するものとする。

第13章　評価

（自己点検に関する年度計画の策定）

第34条　CIOは、年度自己点検計画を策定するものとする。

（自己点検の実施に関する準備）

第35条　部局統括責任者は、職員等の役割ごとの自己点検票及び自己点検の実施手順を整備するものとする。

（自己点検の実施）

第36条　部局統括責任者は、CIOが定める年度自己点検計画に基づき、職員等に対して、自己点検の実施を指示するものとする。

２　職員等は、部局統括責任者から指示された自己点検票及び自己点検の実施手順を用いて自己点検を実施するものとする。

（自己点検結果の評価）

第37条　部局統括責任者は、職員等による自己点検が行われていることを確認し、その結果を評価するものとする。

２　部局統括責任者は、自己点検の結果をCIOへ報告するものとする。

（自己点検に基づく改善）

第38条　職員等は、自らが実施した自己点検の結果に基づき、自己の権限の範囲で改善できると判断したことは改善し、部局統括責任者にその旨を報告するものとする。

２　CIOは、自己点検の結果を全体として評価し、必要があると判断した場合には部局統括責任者に改善を指示するものとする。

（監査）

第39条　部局統括責任者その他の関係者は、情報セキュリティ監査責任者の行う監査の適正かつ円滑な実施に協力するものとする。

第14章　雑則

（雑則）

第40条　この規程に定めるもののほか、情報システムの管理・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２４年９月２６日から施行する。

附　則

この規程は、平成２５年４月１日から施行する。

附　則

この規程は、平成２５年６月２７日から施行し、平成２５年４月１日から適用する。

附　則

この規程は、平成２６年２月２６日から施行し、平成２６年２月１日から適用する。

附　則

この規程は、平成２７年１月１日から施行する。

附　則

この規程は、平成２７年４月１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　この規程改正後のネットワーク部局における管理体制が整備されるまでの間、大学院情報理工学研究科及び大学院情報システム学研究科のネットワーク部局はなお従前の例による。

附　則

この規程は、平成２８年７月１日から施行する。

附　則

この規程は、平成２９年１月１日から施行する。

附　則

この規程は、平成２９年２月１日から施行する。

附　則

この規程は、平成２９年３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。

附　則

この規程は、平成３０年１１月１日から施行する。

別表（第４条関係）

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	
脳科学ライフサポート研究センター	
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	
先端領域教育研究センター	
フォトニックイノベーション研究センター	
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
	ＩＴ活用国際ものづくり教育推進室
	国際ＰＢＬ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	
ものつくりセンター	
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	
ＵＥＣアライアンスセンター	
社会連携センター	
広報センター	
ＵＥＣ　ＡＳＥＡＮ教育研究支援センター	
ＵＥＣ中国教育研究支援センター	
ＵＥＣ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	
研究戦略統括室	
国際戦略室	
男女共同参画・ダイバーシティ戦略室	
ＩＲ室	
教育研究技師部	
事務局	