○国立大学法人筑波技術大学情報システム運用・管理規程

（平成 21 年 3 月 18 日
規　程　第　6　号）

国立大学法人筑波技術大学情報システム運用・管理規程

第１章　総則

（目的）

第１条　この規程は、国立大学法人筑波技術大学（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関する事項を定めることにより、本学の有する情報資産を適正に保護、活用し、情報システムの信頼性、安全性及び効率性の向上に資することを目的とする。

（定義）

第２条　この規程において、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)　運用基本方針　本学が定める「国立大学法人筑波技術大学情報システム運用基本方針（平成 20 年２月 29 日制定）」をいう。

(２)　運用基本規程　本学が定める「国立大学法人筑波技術大学情報システム運用基本規程（平成 20 年規程第２号）」をいう。

(３)　情報資産　情報処理及び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情報をいう。ただし、別に定める場合を除き、情報は電磁的記録（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た記録をいう。）に限るものとする。

(４)　情報ネットワーク機器　ファイアウォール、ルータ、ハブ、情報コンセント又は無線ネットワークアクセスポイント等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をいう。

(５)　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。

(６)　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、教室又はサーバ室等の内部であって、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。

(７)　利用者等　国立大学法人筑波技術大学情報システム利用規程において定める利用者のほか、本学情報資産及び情報システムを取り扱う者をいう。

(８)　主体認証　識別符号を提示した利用者等又は電子計算機が、情報システムにアクセスする正当な権限を有するか否かを検証することをいう。識別符号とともに正しい方法で主体認証情報が提示された場合に主体認証ができたものとして、情報システムはそれらを提示した利用者等又は電子計算機等を正当な権限を有するものとして認識する。

(９)　識別符号　主体認証を行うために、利用者等又は電子計算機が提示する符号のうち、情報システムが利用者等又は電子計算機を特定して認識する符号をいう。

(10)　主体認証情報　主体認証を行うために、利用者等又は電子計算機が提示する

情報のうち、情報システムが利用者等又は電子計算機を正当な権限を有するものとして認識する情報をいう。

(11) 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、利用者等又は電子計算機に付与された正当な権限をいう。また、狭義には、利用者等又は電子計算機に付与された識別符号及び主体認証情報の組み合わせ、又はそれらのいずれかを指して「アカウント」という。

(12) その他の用語の定義は、運用基本方針及び運用基本規程の定めるところによる。

（適用範囲）

第３条　この規程は、情報資産及び情報システムを運用・管理する者に適用する。

（組織体制）

第４条　全学情報システムの運用・管理は、運用基本方針及び運用基本規程に従い、全学総括責任者の下、全学実施責任者、部局総括責任者及び部局技術担当者等からなる全学情報システム運用委員会が行うものとする。

２　部局情報システムの運用・管理は、運用基本方針及び運用基本規程並びに部局の運用方針に従い、部局総括責任者の下、部局技術責任者、部局技術担当者等からなる部局情報システム運用委員会が行うものとする。

３　全学情報ネットワークと部局情報ネットワークとの調整及び対外接続に関する事項は、管理運営部局が執り行うものとする。

（禁止事項）

第５条　部局技術責任者及び部局技術担当者は、次に掲げる事項を行ってはならない。

(１)　情報資産の目的外利用

(２)　守秘義務に違反する情報の開示

(３)　部局総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

(４)　部局総括責任者の要請に基づかずにセキュリティ上の脆弱性を検知する行為

(５)　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

(６)　管理者権限を濫用する行為

(７)　上記の行為を助長する行為

第２章　情報システムのライフサイクル

第１節　設置時

（セキュリティホール対策）

第６条　部局技術担当者は、電子計算機及び情報ネットワーク機器（公開されたセキュリティホールの情報がない電子計算機及び情報ネットワーク機器を除く。以下この条において同じ。）について、セキュリティホール対策に必要となる機器情報を収集するものとする。

２　部局技術担当者は、電子計算機及び情報ネットワーク機器の構築又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開されたセキュリティホール対策の実施を当該機器の管理者に確認するものとする。

（不正プログラム対策）

第７条　部局総括責任者は、不正プログラム感染の回避を目的とした利用者等に対する留意事項を含む日常的実施事項を定めるものとする。

２　部局技術責任者は、不正プログラムから電子計算機（当該電子計算機で動作可能なアンチウイルスソフトウェア等が存在しない場合を除く。）を保護するため、ア

ンチウイルスソフトウェアを導入する等の対策を講ずるものとする。
3　部局技術責任者は、想定される不正プログラムの感染経路のすべてにおいてアンチウイルスソフトウェア等により不正プログラム対策を講ずるものとする。
（サービス不能攻撃対策）
第８条　要安定情報を取り扱う情報システムについては、サービス提供に必要な電子計算機及び情報ネットワーク機器が装備している機能をサービス不能攻撃対策に活用するものとする。
（安全区域）
第９条　部局技術責任者は、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講ずるものとする。
2　部局技術責任者は、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　部局技術責任者は、要保護情報を取り扱う情報システムについては、電子計算機を安全区域に設置するものとする。ただし、モバイル PC について部局総括責任者の承認を得た場合は、この限りでない。
4　部局技術責任者は、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。
（規定及び文書の整備））
第１０条　部局技術責任者は、電子計算機のセキュリティ維持に関する規定を整備するものとする。
2　部局技術責任者は、通信回線を介して提供するサービスのセキュリティ維持に関する規定を整備するものとする。
3　部局技術責任者は、すべての電子計算機の管理者等を特定するための文書を整備するものとする。
（主体認証と権限管理）
第１１条　利用者等が電子計算機にログインする場合には、主体認証を行うように電子計算機を構成するものとする。
2　ログオンした利用者等の識別符号に対して、権限管理を行うものとする。
（電子計算機の対策）
第１２条　部局技術責任者は、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し、または両者を併用することができる。
2　部局技術責任者は、要安定情報を取り扱う電子計算機については、当該電子計算機に求められるシステム性能を発揮できる能力を、将来の見通しを含め検討し、確保するものとする。
3　部局技術責任者は、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に構成するものとする。
（サーバ装置の対策）
第１３条　部局技術責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときは、送受信される情報の暗号化を定めるものとする。
2　部局技術責任者は、サービスの提供及びサーバ装置の運用管理に利用するソフトウェアを定めるものとする。
3　部局技術責任者は、利用が定められたソフトウェアに該当しないサーバアプリケーションが稼動していることを発見した場合はその管理者に通告し，適切な処置を

求めるものとする。

（通信回線の対策）

第１４条　部局技術責任者は、通信回線構築によるリスク（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、通信回線を構築するものとする。

２　部局技術責任者は、要安定情報を取り扱う情報システムについては、通信回線及び情報ネットワーク機器に求められる通信性能を発揮できる能力を、将来の見通しを含め検討し、確保するものとする。

３　部局技術責任者は、通信回線に接続される電子計算機をグループ化し、それぞれ通信回線上で分離するものとする。

４　部局技術責任者は、グループ化された電子計算機間での通信要件を検討し、当該通信要件に従って情報ネットワーク機器を利用しアクセス制御及び経路制御を行うものとする。

５　部局技術責任者は、要機密情報を取り扱う情報システムについては、通信回線を用いて送受信される要機密情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化するものとする。

６　部局技術責任者は、要保護情報を取り扱う情報システムについては、通信回線に利用する物理的な回線のセキュリティを検討し、選択するものとする。

７　部局技術責任者は、遠隔地から情報ネットワーク機器に対して、保守又は診断のために利用するサービスによる接続についてセキュリティを確保するものとする。

８　部局技術責任者は、電気通信事業者の専用線サービスを利用する場合には、セキュリティレベル及びサービスレベルを含む事項に関して契約時に取り決めておくものとする。

９　部局技術責任者は、情報ネットワーク機器上で証跡管理を行う必要性の有無を検討し、必要と認めた場合には実施するものとする。

（情報コンセント）

第１５条　部局技術責任者は、情報コンセントを設置する場合には、次に掲げる事項を含む措置の必要性の有無を検討し、必要と認めた場合には措置を講ずるものとする。

(１)　利用開始及び利用停止時の申請手続の整備
(２)　通信を行う電子計算機の識別又は利用者等の主体認証
(３)　主体認証記録の取得及び管理
(４)　情報コンセント経由でアクセスすることが可能な通信回線の範囲の制限
(５)　情報コンセント接続中に他の通信回線との接続の禁止
(６)　情報コンセント接続方法の機密性の確保
(７)　情報コンセントに接続する電子計算機の管理

（VPN、無線 LAN 及びリモートアクセス）

第１６条　部局技術責任者は、VPN 環境を構築する場合には、次に掲げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずるものとする。

(１)　利用開始及び利用停止時の申請手続の整備
(２)　通信内容の暗号化
(３)　通信を行う電子計算機の識別又は利用者等の主体認証
(４)　主体認証記録の取得及び管理
(５)　VPN 経由でアクセスすることが可能な通信回線の範囲の制限
(６)　VPN 接続方法の機密性の確保
(７)　VPN を利用する電子計算機の管理

２　部局技術責任者は、無線 LAN 環境を構築する場合には、次に掲げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずるものとする。
(１)　利用開始及び利用停止時の申請手続の整備
(２)　通信内容の暗号化
(３)　通信を行う電子計算機の識別又は利用者等の主体認証
(４)　主体認証記録の取得及び管理
(５)　無線 LAN 経由でアクセスすることが可能な通信回線の範囲の制限
(６)　無線 LAN に接続中に他の通信回線との接続の禁止
(７)　無線 LAN 接続方法の機密性の確保
(８)　無線 LAN に接続する電子計算機の管理
３　部局技術責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、次に掲げる事項を含む措置の必要性の有無を検討し、必要と認めたときは措置を講ずるものとする。
(１)　利用開始及び利用停止時の申請手続の整備
(２)　通信を行う者又は発信者番号による識別及び主体認証
(３)　主体認証記録の取得及び管理
(４)　リモートアクセス経由でアクセスすることが可能な通信回線の範囲の制限
(５)　リモートアクセス中に他の通信回線との接続の禁止
(６)　リモートアクセス方法の機密性の確保
(７)　リモートアクセスする電子計算機の管理

（学外通信回線との接続）

第１７条　全学実施責任者は、全学総括責任者の承認を得た上で、学内通信回線を学外通信回線と接続するものとし、利用者等による、学内通信回線と学外通信回線との接続は禁止するものとする。

２　全学実施責任者は、学内通信回線を学外通信回線と接続することにより情報システムのセキュリティが確保できないと判断した場合には、他の情報システムと共有している学内通信回線又は学外通信回線から独立した通信回線として学内通信回線を構築するものとする。

（上流ネットワークとの関係）

第１８条　全学実施責任者は、本学情報ネットワークを構築し運用するに当たっては、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対策）

第１９条　部局技術担当者は、電子計算機及び情報ネットワーク機器の構成に変更があった場合には、セキュリティホール対策に必要となる機器情報を更新するものとする。

２　部局技術担当者は、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連する公開されたセキュリティホールに関連する情報を適宜入手するものとする。

３　部局技術責任者は、入手したセキュリティホールが情報システムにもたらすリスクを分析し、必要と認めたときは，次に掲げる事項について、セキュリティホール対策計画を作成するものとする。
(１)　対策の必要性
(２)　対策方法
(３)　対策方法が存在しない場合の一時的な回避方法

(４)　対策方法又は回避方法が情報システムに与える影響
(５)　対策の実施予定
(６)　対策テストの必要性
(７)　対策テストの方法
(８)　対策テストの実施予定
４　部局技術担当者は、セキュリティホール対策計画に基づきセキュリティホール対策を講ずるものとする。
５　部局技術担当者は、セキュリティホール対策の実施について、実施日、実施内容及び実施者を含む事項を記録するものとする。
６　部局技術担当者は、信頼できる方法で対策用ファイルを入手するものとする。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うものとする。
７　部局技術担当者は、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には、対処を行うものとする。
８　部局技術責任者は、入手したセキュリティホールに関連する情報及び対策方法に関して、必要に応じ、他の部局技術責任者と共有するものとする。

（不正プログラム対策）

第２０条　部局技術担当者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、利用者等にその対処の実施に関する指示を行うものとする。
２　部局総括責任者は、不正プログラム対策の状況を適宜把握し、その見直しを行うものとする。

（脆弱性診断）

第２１条　部局技術責任者及び部局技術担当者は、情報システムに関する脆弱性の診断を定期的に実施し、セキュリティの維持に努めるものとする。

（規定及び文書の見直し、変更）

第２２条　部局技術責任者は、適宜、電子計算機のセキュリティ維持に関する規定の見直しを行うものとする。また、当該規定を変更した場合には、当該変更の記録を保存するものとする。
２　部局技術責任者は、適宜、通信回線を介して提供するサービスのセキュリティ維持に関する規定の見直しを行うものとする。また、当該規定を変更した場合には、当該変更の記録を保存するものとする。
３　部局技術責任者は、電子計算機を管理する利用者等を変更した場合には、当該変更の内容を、電子計算機を管理する利用者等を特定するための文書へ反映するものとする。また、当該変更の記録を保存するものとする。
４　部局技術担当者は、電子計算機の構成を変更した場合には、当該変更の内容を電子計算機関連文書へ反映させるとともに、当該変更の記録を保存するものとする。
５　部局技術担当者は、通信回線の構成、情報ネットワーク機器の設定、アクセス制御の設定又は識別符号を含む事項を変更した場合には、当該変更の内容を通信回線及び情報ネットワーク機器関連文書へ反映させるとともに、当該変更の記録を保存するものとする。

（運用管理）

第２３条　部局技術担当者は、電子計算機のセキュリティ維持に関する規定に基づいて、電子計算機の運用管理を行うものとする。
２　部局技術担当者は、通信回線を介して提供するサービスのセキュリティ維持に関

する規定に基づいて、日常的及び定期的に運用管理を実施するものとする。

（接続の管理）

第２４条　部局総括責任者は、情報ネットワークに関する接続の申請を受けた場合は、別途定める情報ネットワーク接続手順に従い、申請者に対して接続の諾否を通知し必要な指示を行うものとする。

（資源の管理）

第２５条　部局技術責任者は、電子計算機の CPU 資源、ディスク資源及び情報ネットワーク帯域資源等の利用を総合的かつ計画的に推進するため、これらの資源を利用者等の利用形態に応じて適切に分配し管理するものとする。

（ネットワーク情報の管理）

第２６条　部局技術責任者は、部局情報ネットワークで使用するドメイン名や IP アドレス等のネットワーク情報について、全学情報システム運用委員会から割り当てを受け、利用者等からの利用形態に応じて適切に分配し管理するものとする。

（サーバ装置の対策）

第２７条　部局技術責任者は、定期的にサーバ装置の構成の変更を確認するものとする。また、当該変更によって生ずるサーバ装置のセキュリティへの影響を特定し、対応するものとする。

２　部局技術担当者は、要安定情報を取り扱うサーバ装置に保存されている情報について、定期的にバックアップを取得するものとする。また、取得した情報を記録した媒体は、安全に管理するものとする。

３　部局技術担当者は、管理するサーバ装置の運用管理について、作業日、作業内容及び作業者を含む事項を記録するものとする。

４　部局技術責任者は、サーバ装置上で証跡管理を行う必要性の有無を検討し、必要と認めた場合には実施させるものとする。

５　部局技術担当者は、情報システムにおいて基準となる時刻に、管理するサーバ装置の時刻を同期するものとする。

６　全てのサーバ装置管理者は、前各項に準じた管理運用を行うものとする。

（通信回線の対策）

第２８条　部局技術担当者は、通信回線を利用する電子計算機の識別符号（ホスト ID）、電子計算機の利用者等と当該利用者等の識別符号の対応及び通信回線の利用部局を含む事項の管理を行うものとする。

２　部局技術責任者は、定期的に通信回線の構成、情報ネットワーク機器の設定、アクセス制御の設定又は識別符号を含む事項の変更を確認するものとする。また、当該変更によって生ずる通信回線のセキュリティへの影響を特定し、対応するものとする。

３　部局技術責任者は、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。

４　部局技術担当者は、部局技術責任者の許可を受けていない電子計算機及び情報ネットワーク機器を通信回線に接続させないものとする。

５　部局技術担当者は、要安定情報を取り扱う情報システムについては、日常的に、通信回線の利用状況及び状態を確認、分析し、通信回線の性能低下及び異常を推測又は検知するものとする。

６　部局技術担当者は、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。

（学外通信回線との接続）
第２９条　全学実施責任者は、学内通信回線と学外通信回線の接続において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学内通信回線又は学外通信回線から独立した通信回線に構成を変更するものとする。
２　全学実施責任者は、通信回線の変更に際し及び定期的に、アクセス制御の設定の見直し行うものとする。
３　全学実施責任者は、定期的に、学外通信回線から通信することが可能な学内通信回線及び情報ネットワーク機器のセキュリティホールを検査するものとする。
４　全学実施責任者は、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状況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３０条　電子計算機の運用を終了する場合には、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３１条　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３２条　部局技術責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、情報システムを統括する責任者に求めるものとする。
２　部局技術責任者は、情報システムのセキュリティ要件を決定するものとする。
３　部局技術責任者は、情報システムのセキュリティ要件を満たすために機器等の購入（購入に準ずるリースを含む。）及びソフトウェア開発において必要な対策、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策を定めるものとする。
４　部局技術責任者は、構築した情報システムを運用段階へ導入するに当たって、情報セキュリティの観点から実施する導入のための手順及び環境を定めるものとする。
（情報システムの構築・運用・監視）
第３３条　部局技術責任者は、情報システムの構築、運用及び監視に際しては、セキュリティ要件に基づく情報セキュリティ対策を行うものとする。
（情報システムの移行・廃棄）
第３４条　部局技術責任者は、情報システムの移行及び廃棄を行う場合は、情報の消去及び保存並びに情報システムの廃棄及び再利用について必要性を検討し、それぞれについて適切な措置を採るものとする。
（情報システムの見直し）
第３５条　部局技術責任者は、情報システムの情報セキュリティ対策について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い、必要な措置を講ずるものとする。

第３章　情報の格付と取扱い

（情報の作成又は入手）
第３６条　教職員等は、情報システムに係る情報を作成し又は入手する場合には、本

学の研究教育事務の遂行の目的に十分留意するものとする。

（情報の作成又は入手時における格付の決定と取扱制限の検討）

第３７条　教職員等は、情報の作成時に当該情報の機密性、完全性又は可用性に応じて格付を行い、あわせて取扱制限の必要性の有無を検討するものとする。

２　教職員等は、学外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性又は可用性に応じて格付を行い、あわせて取扱制限の必要性の有無を検討するものとする。

（格付と取扱制限の明示）

第３８条　教職員等は、情報の格付を、当該情報の参照が許されている者が認識できる方法を用いて明示し、必要に応じて取扱制限についても明示するものとする。

（格付と取扱制限の継承）

第３９条　教職員等は、情報を作成する際に、既に格付された情報を引用する場合には、当該情報の格付及び取扱制限を継承するものとする。

（格付と取扱制限の変更）

第４０条　教職員等は、情報の格付を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談するものとする。相談された者は、格付の見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付を行うものとする。

２　教職員等は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談するものとする。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定するものとする。

（格付に応じた情報の保存）

第４１条　部局技術責任者は、電子計算機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講ずるものとする。

２　部局技術責任者は、要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書の複写の保管について、災害等への対策の必要性を検討し、必要があると認めた場合には、同時被災等しないための適切な措置を講ずるものとする。

第４章　主体認証

（主体認証機能の導入）

第４２条　部局技術責任者は、すべての情報システムについて、主体認証を行う必要性の有無を検討するものとする。ただし、要保護情報を取り扱う情報システムについては、主体認証を行う必要性があると判断するものとする。

２　部局技術責任者は、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、識別及び主体認証を行う機能を設けるものとする。

３　部局技術担当者は、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、主体認証情報を秘密にする必要がある場合には、次の各号により、当該主体認証情報が明らかにならないように管理するものとする。

(１)　主体認証情報を保存する場合には、その内容の暗号化を行うものとする。

(２)　主体認証情報を通信する場合には、その内容の暗号化を行うものとする。

(３)　保存又は通信を行う際に暗号化を行うことができない場合には、利用者等に自らの主体認証情報を設定、変更又は提供（入力）させる際に、暗号化が行われない旨を通知するものとする。

４　部局技術責任者は、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、利用者等に主体認証情報の定期的な変更を求める場合には、利用者等に対して定期

的な変更を促す機能のほか、次に掲げるいずれかの機能を設けるものとする。
(１)　利用者等が定期的に変更しているか否かを確認する機能
(２)　利用者等が定期的に変更しなければ、情報システムの利用を継続させない機能
５　部局技術責任者は、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、主体認証情報又は主体認証情報格納装置（IC カード）を他者に使用され又は使用される危険性を認識した場合には、直ちに当該主体認証情報若しくは主体認証情報格納装置（IC カード）による主体認証を停止する機能又はこれに対応する識別符号による情報システムの利用を停止する機能を設けるものとする。
６　部局技術責任者は、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、知識による主体認証方式を用いる場合には、次に掲げる機能を設けるものとする。
(１)　利用者等が、自らの主体認証情報を設定する機能
(２)　利用者等が設定した主体認証情報を他者が容易に知ることができないように保持する機能
７　部局技術責任者は、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、知識、所有又は生体情報以外の主体認証方式を用いる場合には、次に掲げる要件について検証した上で、当該主体認証方式に適用するものとするが可能な要件をすべて満たすものとする。また、用いる方式に応じて、次に掲げるものを含む要件を定めるものとする。
(１)　正当な主体以外の主体を誤って主体認証しないものとする。（誤認の防止）
(２)　正当な主体が本人の責任ではない理由で主体認証できなくならないものとする。（誤否の防止）
(３)　正当な主体が容易に他者に主体認証情報を付与及び貸与ができないものとする。（代理の防止）
(４)　主体認証情報が容易に複製できないものとする。（複製の防止）
(５)　部局技術担当者の判断により、ログオンを個々に無効化できる手段があるものとする。（無効化の確保）
(６)　主体認証について業務遂行に十分な可用性があるものとする。（可用性の確保）
(７)　新たな主体を追加するために、外部からの情報や装置の供給を必要とする場合には、それらの供給が情報システムの耐用期間の間、十分受けられるものとする。（継続性の確保）
(８)　主体に付与した主体認証情報を使用するものとするが不可能になった際に、正当な主体に対して主体認証情報を安全に再発行できるものとする。（再発行の確保）
８　部局技術責任者は、生体情報による主体認証方式を用いる場合には、当該生体情報を本人から事前に同意を得た目的以外の目的で使用しないものとする。また、当該生体情報について、本人のプライバシーを侵害しないように留意するものとする。
９　部局総括責任者は、セキュリティ侵害又はその可能性が認められる場合には、主体認証情報の変更を求め又はアカウントを失効させることができる。

第５章　アクセス制御

（アクセス制御機能の導入）
第４３条　部局技術責任者は、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。ただし、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判断するものとする。

２　部局技術責任者は、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るものとする。

（利用者等による適正なアクセス制御）

第４４条　部局技術責任者は、それぞれの情報システムに応じたアクセス制御の措置を講ずるよう、利用者等に指示するものとする。

２　利用者等は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付及び取扱制限の指示内容に従って、必要なアクセス制御の設定をするものとする。

（無権限のアクセス対策）

第４５条　部局技術責任者及び部局技術担当者は、無権限のアクセス行為を発見した場合には、速やかに部局総括責任者に報告するものとする。部局総括責任者は、上記の報告を受けたときは、遅滞なく全学総括責任者にその旨を報告するものとする。

２　全学総括責任者及び部局総括責任者は、前項の報告を受けた場合は、新たな防止対策等必要な措置を講ずるものとする。

第６章　アカウント管理

（アカウント管理機能の導入）

第４６条　部局技術責任者は、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。ただし、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判断するものとする。

２　部局技術責任者は、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、アカウント管理を行う機能を設けるものとする。

（アカウント管理手続の整備）

第４７条　部局技術責任者は、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、アカウント管理について、次に掲げる事項を含む手続を明確にするものとする。

(１)　主体からの申請に基づいてアカウント管理を行う場合には、その申請者が正当な主体であることを確認するための手続

(２)　主体認証情報の初期配布方法及び変更管理手続

(３)　アクセス制御情報の設定方法及び変更管理手続

２　部局技術責任者は、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、アカウント管理を行う者を定めるものとする。

（共用アカウント）

第４８条　部局技術責任者は、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、共用アカウントの利用許可については、情報システムごとにその必要性を判断するものとする。

２　アカウント管理を行う者は、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、アカウントを発行する際に、それが共用アカウントか、共用ではないアカウントかの区別を利用者等に通知するものとする。ただし、共用アカウントは、部局技術責任者が、その利用を認めた情報システムでのみ付与することができる。

（アカウントの発行）

第４９条　アカウント管理を行う者は、利用者等からのアカウント発行申請を受理したときは、申請者が第６５条第２項第３号に規定する措置期間中である場合を除き、遅滞無くアカウントを発行するものとする。

２　アカウント管理を行う者は、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、情報システムを利用する許可を得た主体に対してのみ、アカウントを発行するものとする。
3　アカウント管理を行う者は、アカウントを発行するに当たっては、期限付の仮パスワードを発行する等の措置を講ずることが望ましい。
4　アカウント管理を行う者は、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、管理者権限を持つアカウントを、業務又は業務上の責務に即した場合に限定して付与するものとする。
5　アカウント管理を行う者は、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、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス制御に係る設定をするものとする。

（アカウント発行の報告）

第５０条　部局総括責任者は、アカウント管理を行う者に、アカウント発行の報告を求めることができる。
2　全学総括責任者は、必要により部局総括責任者にアカウント発行の報告を求めることができる。

（アカウントの有効性検証）

第５１条　アカウント管理を行う者は、発行済のアカウントについて、次に掲げる事項を一か月毎に確認するものとする。
(1)　利用資格を失ったもの
(2)　部局総括責任者が指定する削除保留期限を過ぎたもの
(3)　パスワード手順に違反したパスワードが設定されているもの
(4)　六か月以上使用されていないもの
2　アカウント管理を行う者は、人事異動等、アカウントを追加又は削除する時に、不適切なアクセス制御設定の有無を点検するものとする。

（アカウントの削除）

第５２条　アカウント管理を行う者は、第５１条第１項第１号及び第２号に規定するアカウントを発見したとき又は第６５条第２項第３号に規定する削除命令を受けたときは、速やかにそのアカウントを削除し、その旨を部局総括責任者に報告するものとする。
2　アカウント管理を行う者は、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、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等のアカウントを削除するものとする。
3　アカウント管理を行う者は、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、利用者等が情報システムを利用する必要がなくなった場合には、当該利用者等に交付した主体認証情報格納装置(IC カード)を返還させるものとする。
4　部局総括責任者は、第１項の報告を受けたときは、速やかにその旨を利用者等に通知するものとする。ただし、電話、郵便等の伝達手段によっても通知ができない場合には、この限りでない。
5　全学総括責任者は、必要により部局総括責任者にアカウント削除の報告を求めることができる。

（アカウントの停止）

第５３条　アカウント管理を行う者は、第５１条第１項第３号及び第４号に規定するアカウントを発見したとき、第６５条第２項第３号に規定する停止命令を受けたとき又は主体認証情報が他者に使用され若しくはその危険が発生したことの報告を受けたときは、速やかにそのアカウントを停止し、その旨を部局総括責任者に報告するものとする。

２　部局総括責任者は、前項の措置の報告を受けたときは、速やかにその旨を利用者等に通知するものとする。ただし、電話、郵便等の伝達手段によっても通知ができない場合はこの限りでない。
３　全学総括責任者は、必要により部局総括責任者にアカウント停止の報告を求めることができる。
（アカウントの復帰）
第５４条　アカウントの停止を受けた利用者等がアカウント停止からの復帰を希望するときは、その旨を部局総括責任者に申し出させるものとする。
２　部局総括責任者は、前項の申し出を受けたときは、アカウント管理を行う者に当該アカウントの安全性の確認及びアカウントの復帰を指示するものとする。
３　アカウント管理を行う者は、前項の指示に従い当該アカウントの安全性を確認した後、速やかにアカウントを復帰させるものとする。
（管理者権限を持つアカウントの利用）
第５５条　管理者権限を持つアカウントを付与された者は、管理者としての業務遂行時に限定して、当該アカウントを利用するものとする。

第７章　証跡管理

（証跡管理機能の導入）
第５６条　部局技術責任者は、すべての情報システムについて、証跡管理を行う必要性の有無を検討するものとする。
２　部局技術責任者は、証跡を取得する必要があると認めた情報システムには、証跡管理のために証跡を取得する機能を設けるものとする。
３　部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、事象を証跡として記録するに当たり、事象ごとに必要な情報項目を記録するように情報システムの設定をするものとする。
４　部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できなくなった場合及び取得できなくなるおそれがある場合の対処方針を整備し、必要に応じ、これらの場合に対応するための機能を情報システムに設けるものとする。
５　部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡に対して不当な消去、改ざん及びアクセスがなされないように、取得した証跡についてアクセス制御を行い、外部記録媒体その他の装置・媒体に記録した証跡についてはこれを適正に管理するものとする。
（部局技術担当者による証跡の取得と保存）
第５７条　部局技術担当者は、証跡を取得する必要があると認めた情報システムにおいては、部局技術責任者が情報システムに設けた機能を利用して、証跡を記録するものとする。
２　部局技術担当者は、証跡を取得する必要があると認めた情報システムにおいては、取得した証跡の保存期間を定め、当該保存期間が満了する日まで証跡を保存し、保存期間を延長する必要性がない場合は、速やかにこれを消去するものとする。
３　部局技術担当者は、証跡を取得する必要があると認めた情報システムにおいては、証跡が取得できない場合又は取得できなくなるおそれがある場合には、定められた対処を行うものとする。
（証跡管理に関する利用者等への周知）
第５８条　部局総括責任者又は部局技術責任者は、証跡を取得する必要があると認めた情報システムにおいては、部局技術担当者及び利用者等に対して、証跡の取得、保存、点検及び分析を行う可能性があることをあらかじめ説明するものとする。

（通信の監視）

第５９条　利用者等によるネットワークを通じて行われる通信の傍受を禁止するものとする。ただし、全学総括責任者又は当該ネットワークを管理する部局総括責任者は、セキュリティ確保のため、あらかじめ指定した者に、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　全学総括責任者又は部局総括責任者は、監視の範囲をあらかじめ具体的に定めておかなければならない。ただし、不正アクセス行為又はこれに類する重大なセキュリティ侵害に対処するために特に必要と認められる場合には、全学総括責任者又は部局総括責任者は、セキュリティ侵害の緊急性、内容及び程度に応じて、対処のために不可欠と認められる情報について、監視を行うよう命ずることができる。

３　監視を行う者は、監視によって知った通信の内容又は個人情報を、他の者に伝達してはならない。ただし、前項ただし書きに定める情報については、全学総括責任者及び部局総括責任者並びに全学情報システム運用委員会及び部局情報システム運用委員会に伝達することができる。

４　監視を行わせる者は、監視を行う者に対して、監視記録を保存する期間をあらかじめ指示するものとする。監視を行う者は、指示された期間を経過した監視記録を直ちに破棄しなければならない。ただし、監視記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。

５　監視を行う者及び監視記録の伝達を受けた者は、監視記録を不必要に閲覧してはならない。ただし、ネットワーク運用・管理のために必要な限りで、これを閲覧し、かつ、保存することができる。不必要となった監視記録は、直ちに破棄しなければならない。監視記録の内容を、法令に基づく場合等を除き、他の者に伝達してはならない。

（利用記録）

第６０条　複数の者が利用する情報機器の管理者は、当該機器に係る利用記録（以下「利用記録」という。）をあらかじめ定めた目的の範囲でのみ採取することができる。ただし、当該目的との関連で必要性の認められない利用記録を採取することはできない。

２　前項に規定する目的は、法令の遵守、情報セキュリティの確保、課金その他当該情報機器の利用に必要なものに限られ、個人情報の取得を目的とすることはできない。

３　当該情報機器の管理者は、第１項の目的のために必要な限りで、利用記録を閲覧することができる。ただし、他人の個人情報及び通信内容を不必要に閲覧してはならない。

４　当該情報機器の管理者は、第２項に規定する目的のために必要な限りで、利用記録を他の者に伝達することができる。

５　第１項の規定により情報機器の利用を記録しようとする者は、第２項の目的、これによって採取しようとする利用記録の範囲及び前項により利用記録を伝達する者を、あらかじめ部局総括責任者に申告し、かつ、当該機器の利用者等に開示しなければならない。部局総括責任者は、申告の内容を不適切と認めるときは、これを修正させるものとする。

６　当該情報機器の管理者又は利用記録の伝達を受けた者は、第１項の目的のために必要な限りで、これを保有することができる。不要となった利用記録は、直ちに破棄しなければならない。ただし、当該情報機器の管理者は、利用記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。

（個人情報の取得と管理）
第６１条　電子的に個人情報の提供を求める場合は、提供を求める情報の範囲、利用の目的及びその情報が伝達される範囲を、あらかじめ相手方に示さなければならない。
２　前項の個人情報は、当人の請求により開示、訂正又は削除をしなければならない。また、そのための手続を示さなければならない。
（利用者等が保有する情報の保護）
第６２条　利用者等が保有する情報は、ネットワーク運用に不可欠な範囲又はインシデント対応に不可欠な範囲において、閲覧、複製又は提供することができる。

第８章　暗号と電子署名

（暗号化機能及び電子署名の付与機能の導入）
第６３条　部局技術責任者は、要機密情報（書面を除く。）を取り扱う情報システムについて、暗号化を行う機能を付加する必要性の有無を検討するものとする。
２　部局技術責任者は、暗号化を行う必要があると認めた情報システムには、暗号化を行う機能を設けるものとする。
３　部局技術責任者は、要保全情報を取り扱う情報システムについて、電子署名の付与を行う機能を付加する必要性の有無を検討するものとする。
４　部局技術責任者は、電子署名の付与を行う必要があると認めた情報システムには、電子署名の付与を行う機能を設けるものとする。
５　部局技術責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択するものとする。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リスト又は、本学における検証済み暗号リストがあればその中から選択するものとする。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つをそれらのリストの中から選択するものとする。
（暗号化及び電子署名の付与に係る管理）
第６４条　部局技術責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対応手順等を定めるものとする。
２　部局技術責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の保存媒体及び保存場所を定めるものとする。
３　部局技術責任者は、電子署名の付与を行う必要があると認めた情報システムにおいて、電子署名の正当性を検証するための情報又は手段を署名検証者へ提供するものとする。

第９章　違反と例外措置

（違反への対応）
第６５条　部局総括責任者は、情報セキュリティ関係規定への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、速やかに調査を行い、事実を確認するものとする。事実の確認に当たっては、可能な限り当該行為を行った者の意見を聴取するものとする。
２　部局総括責任者は、調査によって違反行為が判明したときには、次に掲げる措置を講ずることができる。

(１)　当該行為者に対する当該行為の中止命令
(２)　部局技術責任者に対する当該行為に係る情報発信の遮断命令
(３)　部局技術責任者に対する当該行為者のアカウント停止命令又は削除命令
(４)　本学の懲罰委員会等への報告
(５)　その他法令に基づく措置

３　部局総括責任者は、前項第２号及び第３号については、他部局の部局総括責任者を通じて同等の措置を依頼することができる。

４　部局総括責任者は、情報セキュリティ関係規定への重大な違反の報告を受けた場合、自らが重大な違反を知った場合及び上記の措置を講じた場合には、遅滞無く全学総括責任者にその旨を報告するものとする。

（例外措置）

第６６条　全学情報システム運用委員会は、例外措置の適用の申請を審査する者（以下「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、定められた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、以下の項目を含む例外措置の適用審査記録を整備し、全学総括責任者に報告するものとする。

(１)　決定を審査した者の情報（氏名、役割名、所属及び連絡先）
(２)　申請内容
　ア　申請者の情報（氏名、所属及び連絡先）
　イ　例外措置の適用を申請する情報セキュリティ関係規定の該当箇所(規定名と条項等)
　ウ　例外措置の適用を申請する期間
　エ　例外措置の適用を申請する措置内容（講ずる代替手段等）
　オ　例外措置の適用を終了した旨の報告方法
　カ　例外措置の適用を申請する理由
(３)　審査結果の内容
　ア　許可又は不許可の別
　イ　許可又は不許可の理由
　ウ　例外措置の適用を許可した情報セキュリティ関係規定の適用箇所(規定名と条項等)
　エ　例外措置の適用を許可した期間
　オ　許可した措置内容（講ずるべき代替手段等）
　カ　例外措置を終了した旨の報告方法

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、必要な対応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、この限りでない。

第１０章　インシデント対応

（インシデントの発生に備えた事前準備）

第６７条　全学総括責任者は、情報セキュリティに関するインシデント（故障を含む。）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　全学実施責任者は、インシデントについて利用者等から部局総括責任者への報告手順を整備し、当該報告手段をすべての利用者等に周知するものとする。

３　全学実施責任者は、インシデントが発生した際の対応手順を整備するものとする。

４　全学実施責任者は、インシデントに備え、本学の研究教育事務の遂行のため特に重要と認めた情報システムについて、その部局技術責任者及び部局技術担当者の緊急連絡先、連絡手段及び連絡内容を含む緊急連絡網を整備するものとする。
５　全学実施責任者は、インシデントについて学外から報告を受けるための窓口を設置し、その窓口への連絡手段を学外に公表するものとする。
（インシデントの原因調査と再発防止策）
第６８条　部局総括責任者は、インシデントが発生した場合には、インシデントの原因を調査し再発防止策を策定し、その結果を報告書として全学総括責任者に報告するものとする。
２　全学総括責任者は、部局総括責任者からインシデントについての報告を受けた場合には、その内容を検討し、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１１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６９条　全学実施責任者は、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。
（本学支給以外の情報システムの利用許可及び届出の取得及び管理）
第７０条　部局技術責任者及び部局技術担当者は、本学支給以外の情報システムによる要保護情報の情報処理に係る記録を取得するものとする。
２　部局技術責任者及び部局技術担当者は、要保護情報（本学情報システムで取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報を除く。）について本学支給以外の情報システムによる情報処理を行うことを許可した期間が終了した時に、許可を受けた者から終了した旨の報告がない場合には、その状況を確認し、対応を講ずるものとする。ただし、許可を与えた者が報告を要しないとした場合は、この限りでない。
３　部局技術責任者及び部局技術担当者は、本学情報システムで取り扱う情報のうち、秘密文書に相当する機密性は要しないが、その漏えいにより利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報について本学支給以外の情報システムによる情報処理を行うことを届け出た期間が終了した時に、必要に応じて、その状況を確認し、対応を講ずるものとする。

第１２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

（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７１条　全学実施責任者は、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についての規定を整備するものとする。

第１３章　教育・研修

（情報セキュリティ対策の教育）
第７２条　全学実施責任者は、情報セキュリティ関係規定について、部局総括責任者、部局技術責任者、部局技術担当者及び利用者等（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　全学実施責任者は、情報セキュリティ関係規程について、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　全学実施責任者は、教育啓発対象者が毎年度最低１回、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　全学実施責任者は、教育啓発対象者の入学、着任又は異動後三か月以内に受講できるように、情報セキュリティ対策の教育を企画、立案し、その体制を整備するものとする。
５　全学実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況を管理できる仕組みを整備するものとする。
６　全学実施責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講状況について、当該教育啓発対象者の所属する部局の部局総括責任者に通知するものとする。
７　部局総括責任者は、教育啓発対象者の情報セキュリティ対策の教育の受講が達成されていない場合には、未受講の者に対して、その受講を勧告するものとする。教育啓発対象者が当該勧告に従わない場合には、全学実施責任者にその旨を報告するものとする。
８　全学実施責任者は、毎年度１回、全学総括責任者及び全学情報システム運用委員会に対して、教育啓発対象者の情報セキュリティ対策の教育の受講状況について報告するものとする。
９　全学実施責任者は、情報セキュリティ関係規程について、教育啓発対象者に対する情報セキュリティ対策の訓練の内容及び体制を整備するものとする。
１０　全学情報システム運用委員会及び部局情報システム運用委員会は、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。
１１　その他、教育・研修に関する事項については、講習計画に定めるものとする。

（教育の主体と客体）

第７３条　部局情報システム運用委員会は、部局総括責任者、部局技術責任者及び部局技術担当者に対して、情報セキュリティ対策の教育を実施するものとする。
２　部局技術責任者及び部局技術担当者は、利用者等に対して、講習計画の定める講習を実施するものとする。

第１４章　評価

（自己点検に関する年度計画の策定）

第７４条　全学総括責任者は、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７５条　部局総括責任者は、職務従事者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７６条　部局総括責任者は、全学総括責任者が定める年度自己点検計画に基づき、職務従事者に対して、自己点検の実施を指示するものとする。
２　職務従事者は、部局総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７７条　部局総括責任者は、職務従事者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　全学総括責任者は、部局総括責任者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。

（自己点検に基づく改善）

第７８条　職務従事者は、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、部局総括責任者にその旨を報告するものとする。
２　全学総括責任者は、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、部局総括責任者に改善を指示するものとする。

（監査）

第７９条　部局総括責任者その他の関係者は、全学総括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。

附　則

この規程は、平成２１年４月１日から施行する。