京都大学情報セキュリティ対策基準

〔平成21年3月2日情報担当理事裁定〕

第1章　総則

（目的）

第1条　この基準は、情報セキュリティポリシーに基づき、京都大学（以下「本学」という。）における情報システムの情報セキュリティ維持及び向上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、並びに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　この基準において、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) 基本方針　本学が定める「京都大学における情報セキュリティの基本方針」（平成27年3月25日役員会決定）をいう。

(2) 規程　本学が定める「京都大学の情報セキュリティ対策に関する規程」（平成15年達示第43号）をいう。

(3) 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、サーバ装置及び端末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、情報コンセント又は無線ネットワークアクセスポイントを含む。）をいう。

(4) 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。

(5) 端末　情報システムの構成要素である機器のうち、利用者等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、本学が調達又は開発するもの及び学内通信回線に接続する本学支給以外のものをいう。端末には、モバイル端末も含まれる。

(6) 本学情報システム　規程第3条第1項第1号及び第3号の情報システムをいう。

(7) 全学情報システム　本学情報システムのうち、第4条第1項に定めるものをいう。

(8) 部局情報システム　本学情報システムのうち、全学情報システム以外のものをいう。

(9) 安全区域　サーバ装置及び端末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（学外のサーバルーム及びデータセンターを含む）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。

(10) 利用者　教職員等及び学生等で、許可を受けて本学情報システムを利用する者をいう。

(11) 臨時利用者　教職員等及び学生等以外の者で、許可を受けて本学情報システムを利用する者をいう。

(12) 利用者等　利用者及び臨時利用者のほか、本学情報システムを取り扱う者をいう。

(13) 主体　情報システムにアクセスする者又は他の情報システムにアクセスするサーバ装置、端末等をいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。

(14) 主体認証　第16号に定める識別コードを提示した主体が、その識別コードを付与された主体、すなわち正当な主体であるか否かを検証することをいう。識別コード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主体を正当な主体として認識する。なお、本基準における「主体認証」については、本学の統合認証システムによる認証のほか、部局情報システムによる認証も含む。

(15) 識別　情報システムにアクセスする主体を、当該情報システムにおいて特定することをいう。

(16) 識別コード　主体を識別するために、情報システムが認識するコード（符号）をいう。代表的な識別コードとして、ユーザ ID が挙げられる。

(17) 主体認証情報　主体認証を行うために、主体が情報システムに提示する情報をいう。代表的な主体認証情報として、パスワードがある。

（18）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。
（19）CSIRT　規程第7条第1項の規定に基づいて置く京都大学情報セキュリティインシデント対応チームをいう。
（20）その他の用語の定義は、別表に定めるほか、規程の定めるところによる。

（適用範囲）
第3条　この基準は、本学における情報資産を運用・管理する教職員等及び利用者等に適用する。
2　法律及びこれに基づく命令の規定により、情報資産の運用・管理に関する事項について特別の定めが設けられている場合にあっては、当該事項については、当該法律及びこれに基づく命令の定めるところによる。

（管理運営組織）
第4条　最高情報セキュリティ責任者は、全学の情報基盤として供される本学情報システムのうち、情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システム（以下「全学情報システム」という。）を指定する。
2　全学情報システムの運用・管理を行う組織（以下「管理運営組織」という。）を置き、情報環境機構をもって充てる。
3　管理運営組織は、前項に定めるほか、情報セキュリティ実施責任者の指示により、以下の各号に定める事務を行う。
（1）全学情報セキュリティ委員会の運営に関する事務
（2）本学情報システムの運用と利用における情報セキュリティポリシーの実施状況の取りまとめ
（3）講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
（4）本学の情報システムの情報セキュリティに関する連絡と通報
（5）全学情報システムと部局情報システムとの接続等の調整及び対外接続に関する取りまとめ
（6）この基準で定める事項の遵守に資する文書等の整備
（組織体制）
第5条　情報セキュリティ実施責任者は、全学情報システムの情報セキュリティに関する連絡と通報において全学情報システムを代表する。
2　全学情報システムの情報セキュリティ対策は、基本方針及び規程に従い、情報セキュリティ実施責任者の下、管理運営組織の部局情報セキュリティ委員会が執り行うものとする。
3　部局情報システムの情報セキュリティ対策は、基本方針並びに規程及び部局の運用方針に従い、当該情報システムを管理する部局の部局情報セキュリティ責任者の下、部局情報セキュリティ委員会が執り行うものとする。
4　情報セキュリティに関する全学及び部局間の技術的な連絡調整は、全学情報セキュリティ技術連絡会が執り行うものとする。
5　情報セキュリティインシデントに関する全学及び部局間の連絡調整及び被害拡大防止を図るための応急措置の指示又は勧告は、企画・情報部情報基盤課セキュリティ対策掛が執り行うものとする。
6　情報ネットワークに関わる危機管理に関する事項は、情報ネットワーク危機管理委員会が執り行うものとする。
7　情報ネットワークにおける人権侵害、著作権侵害等に該当し、又は該当するおそれのある情報の発信防止等に関する事項は、情報ネットワーク倫理委員会が執り行うものとする。

（連絡体制）
第6条　情報セキュリティ実施責任者は、情報セキュリティに関して、以下の各号に定める連絡体制を整備する。
（1）全部局の部局情報セキュリティ責任者に対する連絡網
（2）全部局の部局情報セキュリティ技術責任者に対する連絡網
（3）その他全学の情報セキュリティ対策実施に必要な連絡網
2　部局情報セキュリティ技術責任者は、当該部局の情報システム技術担当者に対する連絡網を整備する。

（禁止事項）
第7条　部局情報セキュリティ技術責任者及び部局情報システム技術担当者は、次に掲げる事項を行ってはならない。また、他の者に行わせてはならない。

（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）部局情報セキュリティ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、サーバ装置及び端末の利用記録を採取する行為
（4）部局情報セキュリティ責任者の指示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）法令又は本学規程に違反する情報の発信
（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

（学外通信回線との接続）
第８条　情報セキュリティ実施責任者は、最高情報セキュリティ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する。また、利用者等による学内通信回線と学外通信回線との接続を禁止するものとする。
２　情報セキュリティ実施責任者は、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。
３　情報セキュリティ実施責任者は、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。
４　情報セキュリティ実施責任者は、定期的に、及び通信回線の変更に際しアクセス制御の設定の見直しを行うものとする。
５　情報セキュリティ実施責任者は、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。
６　最高情報セキュリティ責任者は、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内容を監視するものとする。

（上流ネットワークとの関係）
第９条　情報セキュリティ実施責任者は、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章　情報システムのライフサイクル
第１節　ライフサイクルの概要

（情報システムの計画・設計）
第１０条　部局情報セキュリティ技術責任者は、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、部局情報セキュリティ責任者に求めるものとする。
２　部局情報セキュリティ技術責任者は、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　部局情報セキュリティ技術責任者は、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について定めるものとする。
４　部局情報セキュリティ技術責任者は、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１１条　部局情報セキュリティ技術責任者は、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き定めた情報セキュリティ対策を行うものとする。

（情報システムの見直し）
第１２条　部局情報セキュリティ技術責任者は、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。

（情報システムの移行・廃棄）
第１３条　部局情報セキュリティ技術責任者は、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。

（情報システムの運用継続計画）

第14条　部局情報セキュリティ責任者は、部局において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討するものとする。

2　部局情報セキュリティ責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際に、非常時における情報セキュリティ対策が運用可能であるかを確認するものとする。

第2節　構築時

（調達及び構築）

第15条　部局情報セキュリティ技術責任者は、機器等の選定時において、以下の各号に留意ものとする。

(1) 開発工程において信頼できる品質保証体制が確立されていること。
(2) 設置時や保守時のサポート体制が確立されていること。
(3) 利用マニュアル・ガイダンスが適切に整備されていること。
(4) 脆弱性診断等のテストの実施が確認できること。
(5) ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること。
(6) 当該機器等に求められるセキュリティ要件を満足するセキュリティ機能をもつこと。
(7) 情報セキュリティ維持のためセキュリティ修正を適用する必要がある機器等の場合には、以下の条件を満たすこと。
　（ア）納品時に必要なセキュリティ修正が適用されていること。
　（イ）納品後に必要なセキュリティ修正が継続的に提供され、適用できること。
(8) 以下の保守・点検等のうち、部局情報セキュリティ技術責任者が情報セキュリティの確保に必要と認めるものが適用可能であること。
　（ア）ハードウェアの保守・点検等
　（イ）ソフトウェア及びファームウェアの修正及び更新の提供
　（ウ）部局情報セキュリティ技術責任者が必要と認めた機器等の脆弱性診断その他の保守・点検等

第16条　部局情報セキュリティ技術責任者は、機器等の納入時又は情報システムの受入れ時の確認及び検査において、仕様書等に定められた検査手続きに従い、情報セキュリティ対策に係る要件が満たされていることを確認するものとする。

（セキュリティホール対策）

第17条　部局情報セキュリティ技術責任者は、管理するサーバ装置、端末及び情報ネットワーク機器について、セキュリティホール対策に必要となる機器情報を収集し、書面として整備するものとする。

2　部局情報セキュリティ技術責任者は、管理するサーバ装置、端末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の対策を実施するものとする。

（不正プログラム対策）

第18条　部局情報セキュリティ責任者は、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　部局情報セキュリティ技術責任者は、不正プログラムからサーバ装置及び端末（当該サーバ装置及び端末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。以下同じ。）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実施するものとする。

3　部局情報セキュリティ技術責任者は、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実施するものとする。

（サービス不能攻撃対策）

第19条　部局情報セキュリティ技術責任者は、要安定情報を取り扱う情報システムについては、サービス提供に必要なサーバ装置、端末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。

（標的型攻撃対策）

第20条　部局情報セキュリティ技術責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずるものとする。
2　部局情報セキュリティ技術責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずるものとする。

（安全区域）
第21条　部局情報セキュリティ技術責任者は、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、学内に設置する安全区域については、施設及び環境面から以下の各号の対策を実施するものとする。
(1)　立ち入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、区域外と明確に区分すること。ただし、窓口のある教室、研究室、事務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は教職員等が窓口を常に目視できるような措置を講ずること。
(2)　立入りを許可されていない者が容易に立ち入らないように、教職員等が全員不在時には施錠すること。
2　部局情報セキュリティ技術責任者は、情報システムによるリスクを検討し、学外のサーバルーム及びデータセンターを安全区域として利用する場合は、前項の各号の対策を実施するよう確認するものとする。

（規定及び文書の整備）
第22条　部局情報セキュリティ技術責任者は、サーバ装置及び端末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　部局情報セキュリティ技術責任者は、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　部局情報セキュリティ技術責任者は、すべてのサーバ装置及び端末に対して、サーバ装置及び端末を管理する利用者等を特定するための文書を整備するものとする。
4　部局情報セキュリティ技術責任者は、サーバ装置及び端末関連文書を整備するものとする。
5　部局情報セキュリティ技術責任者は、通信回線及び情報ネットワーク機器関連文書を整備するものとする。

（主体認証と権限管理）
第23条　部局情報セキュリティ技術責任者は、利用者等がサーバ装置及び端末にログインする場合には主体認証を行うようにサーバ装置及び端末を構成するものとする。
2　部局情報セキュリティ技術責任者は、ログオンした利用者等の識別コードに対して、権限管理を行うものとする。

（端末の対策）
第24条　部局情報セキュリティ技術責任者は、端末で利用を禁止するソフトウェアを定めるものとする。
2　部局情報セキュリティ技術責任者は、要保護情報を取り扱うモバイル端末については、学外で使われる際にも、学内で利用される場合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25条　部局情報セキュリティ技術責任者は、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、送受信される情報を暗号化するものとする。
2　部局情報セキュリティ技術責任者は、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　部局情報セキュリティ技術責任者は、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場合には、当該サーバアプリケーションを停止するものとする。また、利用が定められたソフトウェアに該当するサーバアプリケーションであっても、利用しない機能を無効化して稼動するものとする。

（複合機の対策）
第26条　部局情報セキュリティ技術責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付け及び取扱制限に応じ、適切なセキュリティ要件を策定するものとする。

2 部局情報セキュリティ技術責任者は、複合機が備える機能について適切な設定等を行うことにより、運用中の複合機に対する情報セキュリティインシデントへの対策を講ずるものとする。

（特定用途機器）

第27条 部局情報セキュリティ技術責任者は、特定用途機器について、取り扱う情報、利用方法及び通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずるものとする。

（接続の管理）

第28条 部局情報セキュリティ責任者は、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。

（通信回線の対策）

第29条 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、通信回線に接続されるサーバ装置及び端末をセキュリティレベル、管理部署等によりグループ化し、それぞれ論理的又は物理的な通信回線上で分離するものとする。

4 部局情報セキュリティ技術責任者は、グループ化されたサーバ装置及び端末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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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30条 部局情報セキュリティ技術責任者は、情報コンセントを設置する場合には、以下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) 通信を行うサーバ装置及び端末の識別又は利用者等の主体認証
(2) 主体認証記録の取得及び管理
(3) 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
(4) 情報コンセント接続中に他の通信回線との接続の禁止
(5) 情報コンセント接続方法の機密性の確保
(6) 情報コンセントに接続するサーバ装置及び端末の管理

（VPN、無線 LAN、リモートアクセス）

第31条 部局情報セキュリティ技術責任者は、VPN 環境を構築する場合には、以下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) 通信を行うサーバ装置及び端末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 を利用するサーバ装置及び端末の管理

2 部局情報セキュリティ技術責任者は、無線 LAN 環境を構築する場合には、以下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) 通信を行うサーバ装置及び端末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 に接続するサーバ装置及び端末の管理
3 部局情報セキュリティ技術責任者は、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、以下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

（電子メールサーバの対策）
第32条 部局情報セキュリティ技術責任者は、電子メールサーバが電子メールの不正な中継を行わないよう、対策を講ずるものとする。
2 部局情報セキュリティ技術責任者は、利用者等が電子メールを送受信する場合には主体認証を行うように電子メールサーバを構築するものとする。
3 部局情報セキュリティ技術責任者は、電子メールのなりすましの防止策を講ずるものとする。

（ウェブサーバの対策）
第33条 部局情報セキュリティ技術責任者は、ウェブサーバの管理や設定において、以下に掲げる事項を含む措置の必要性の有無を検討し、必要と認めた時は措置を講ずるものとする。
(1) ウェブサーバが備える機能のうち、不要な機能の停止又は制限
(2) ウェブコンテンツの編集作業を担当する主体の限定
(3) 公開してはならない又は無意味なウェブコンテンツが公開されないような管理
(4) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報の適切な管理
(5) サービスを利用する者の個人に関する情報を通信する等、通信時の盗聴等による情報の漏えいを防止する必要がある場合、暗号化の機能及び電子証明書による認証の機能の設定
(6) ウェブサーバに保存する情報の特定及びサービスの提供に必要のない情報がウェブサーバに保存されないことの確認

第3節 運用時

第1款 部局情報セキュリティ技術責任者の役割

（セキュリティホール対策）
第34条 部局情報セキュリティ技術責任者は、情報環境機構等から入手したセキュリティホールに関連する情報を元に、自部局内のサーバ装置、端末及び情報ネットワーク機器に対し、必要に応じて、速やかにその対策を実施するものとする。
2 前項に関し、部局情報セキュリティ技術責任者は、必要に応じて他の部局情報セキュリティ技術責任者と情報を共有するものとする。

（不正プログラム対策）
第35条 部局情報セキュリティ技術責任者は、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36条　部局情報セキュリティ技術責任者は、部局情報セキュリティ責任者の指示に基づき、情報システムに関する脆弱性の診断を年1回以上実施し、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37条　部局情報セキュリティ技術責任者は、適宜、サーバ装置及び端末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　部局情報セキュリティ技術責任者は、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　部局情報セキュリティ技術責任者は、サーバ装置及び端末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、サーバ装置及び端末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。

（資源の管理）
第38条　部局情報セキュリティ技術責任者は、サーバ装置、端末及び情報ネットワーク機器の 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39条　部局情報セキュリティ技術責任者は、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、情報環境機構から割当てを受け、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40条　部局情報セキュリティ技術責任者は、定期的にサーバ装置の構成の変更やソフトウェアの状態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　部局情報セキュリティ技術責任者は、サーバ装置上で証跡管理を行う必要性を検討し、必要と認めた場合には実施するものとする。

（端末の対策）
第41条　部局情報セキュリティ技術責任者は、部局内の端末で利用されているソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図るものとする。

（通信回線の対策）
第42条　部局情報セキュリティ技術責任者は、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コード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。
2　部局情報セキュリティ技術責任者は、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。

第2款　部局情報システム技術担当者の役割

（セキュリティホール対策）
第43条　部局情報システム技術担当者は、サーバ装置、端末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、第17条第1項に基づき整備した書面を更新するものとする。
2　部局情報システム技術担当者は、管理対象となるサーバ装置、端末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　部局情報システム技術担当者は、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。
4　部局情報システム技術担当者は、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。
5 部局情報システム技術担当者は、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。
6 部局情報システム技術担当者は、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サーバ装置、端末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。

（不正プログラム対策）
第44条 部局情報システム技術担当者は、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。

（規定及び文書の見直し、変更）
第45条 部局情報システム技術担当者は、サーバ装置、端末の構成を変更した場合には、当該変更の内容をサーバ装置、端末及び端末関連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。
2 部局情報システム技術担当者は、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コード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。

（運用管理）
第46条 部局情報システム技術担当者は、サーバ装置、端末のセキュリティ維持に関する規定に基づいて、サーバ装置、端末の運用管理を行うものとする。
2 部局情報システム技術担当者は、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。

（サーバ装置の対策）
第47条 部局情報システム技術担当者は、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。
2 部局情報システム技術担当者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録するものとする。
3 部局情報システム技術担当者は、情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期するものとする。

（通信回線の対策）
第48条 部局情報システム技術担当者は、通信回線を利用するサーバ装置及び端末の識別コード、サーバ装置及び端末の利用者等と当該利用者等の識別コード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 部局情報システム技術担当者は、部局情報セキュリティ技術責任者の許可を受けていないサーバ装置、端末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。
3 部局情報システム技術担当者は、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。
4 部局情報システム技術担当者は、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。

第4節 運用終了時

（機器等の対策）
第49条 部局情報セキュリティ技術責任者は、機器等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。

第5節 情報システムの利用

（基本的対策）
第50条　利用者等は、本学の教育、研究その他の業務以外の目的で情報システムを利用しないものとする。
2　利用者等は、部局情報セキュリティ技術責任者が接続許可を与えた通信回線以外に学内の情報システムを接続しないものとする。
3　利用者等は、学内通信回線に、部局情報セキュリティ技術責任者の接続許可を受けていない情報システムを接続しないものとする。
4　利用者等は、情報システムで利用を禁止するソフトウェアを利用しないものとする。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、部局情報セキュリティ技術責任者の承認を得るものとする。
5　利用者等は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずるものとする。
6　利用者等は、要保護情報を取り扱う端末にて情報処理を行う場合は、当該情報の取扱制限に従い適切な措置を講ずるものとする。
7　利用者等は、安全区域に設置された要保護情報を取り扱う情報システムを、安全区域外に持ち出す場合には、当該情報の取扱制限に従い適切な措置を講ずるものとする。
8　利用者等は、端末の運用を終了する場合には、端末に保存されているすべての要保護情報を、第49条に準じて、復元が困難な状態にするものとする。

（不正プログラム対策）
第51条　利用者等は、不正プログラム感染防止に関する措置に努めるものとする。
2　利用者等は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずるものとする。

（電子メール・ウェブの利用時の対策）
第52条　利用者等は、要機密情報を含む電子メールを送受信する場合には、本学が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用するものとする。
2　利用者等は、学外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に本学ドメイン名を使用するものとする。ただし、学外の者にとって、当該利用者等が既知の者である場合は除く。
3　利用者等は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処するものとする。
4　利用者等は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないものとする。
5　利用者等は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名等により当該ソフトウェアの配布元の正当性を確認するものとする。
6　利用者等は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認するものとする。
(1) 送信内容が暗号化されること。
(2) 当該ウェブサイトが送信先として想定している組織のものであること。

（外部電磁的記録媒体）
第53条　利用者等は、外部電磁的記録媒体を用いた情報の取扱に関する以下の事項を遵守するものとする。
(1) 情報の格付け及び取扱制限で指定されている場合、本学支給の外部電磁的記録媒体を使用すること。
(2) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用すること。
(3) 要機密情報は保存される必要がなくなった時点で速やかに削除すること。
(4) 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫及び駆除を行うこと。

（識別コード及び主体認証情報の取扱い）
第54条　利用者等は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報シ

ステムを利用しないものとする。
2 利用者等は、自己に付与された識別コードを適切に管理するものとする。
3 利用者等は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用するものとする。
4 利用者等は、自己の主体認証情報の管理を徹底するものとする。

第3章 外部委託

（外部委託の範囲）
第55条 部局情報セキュリティ技術責任者は、取り扱う情報の格付け及び取扱制限で許可されている場合、以下の各号の業務において、外部委託を実施することができるものとする。
(1) 情報システムの構築及び開発
(2) 情報システムの運用、保守及び点検
(3) 情報の加工及び処理
(4) 情報の保存及び運搬

（外部委託に係る契約）
第56条 部局情報セキュリティ技術責任者は、外部委託を実施する際には、以下の基準に従って委託先を選定するものとする。
(1) 本対策基準の各項目を遵守し得る者であること。
(2) 本対策基準と同等の情報セキュリティ管理体制を整備していること。
(3) 本対策基準と同等の情報セキュリティ対策の教育を委託先の事業従事者に対して実施していること。
2 部局情報セキュリティ技術責任者は、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めるものとする。
(1) 委託先に提供する情報の委託先における目的外利用の禁止
(2) 委託先における情報セキュリティ対策の実施内容及び管理体制の整備
(3) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制の整備
(4) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供
(5) 情報セキュリティインシデントへの対処対応
(6) 情報セキュリティ対策その他の契約の履行状況の確認方法
(7) 情報セキュリティ対策の履行が不十分な場合の対処方法
3 部局情報セキュリティ技術責任者は、委託する業務において取り扱う情報の格付け等を勘案し、必要に応じて以下の内容を仕様に含めること。
(1) 情報セキュリティ監査の受入れ
(2) サービスレベルの保証
(3) 要保護情報を取り扱う場合は、情報システムを設置する区域が、第21条第1項各号の対策と同等以上の対策を実施。
4 部局情報セキュリティ技術責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、前2項の措置の実施を委託先に担保させるものとする。

（外部委託における対策の実施）
第57条 部局情報セキュリティ技術責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認するものとする。
2 部局情報セキュリティ技術責任者は、委託した業務において情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を教職員等から受けた場合は、当該サービスの利用を中止するなど、必要な措置を講じ、委託先に契約に基づく必要な措置を講じさせるものとする。
3 部局情報セキュリティ技術責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却又は抹消されたことを確認するものとする。

（外部委託における情報の取扱い）

第５８条　教職員等は、委託先への情報の提供等において、以下の事項を遵守するものとする。
(1) 委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、第６８条に準じた安全な受渡し方法により提供すること。
(2) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は消去させること。
(3) 委託事業において、情報セキュリティインシデントの発生又は情報の目的外利用を認知した場合は、速やかに部局情報セキュリティ技術責任者に報告すること。

（約款による外部サービスの利用）
第５９条　教職員等は、取り扱う情報の格付け及び取扱制限で許可されている場合、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認し、適切な措置を講じた上で、約款による外部サービスを利用できるものとする。ただし、要保護情報を取り扱う場合は、あらかじめ部局情報セキュリティ責任者に届け出るものとする。
２　教職員等は、約款による外部サービスを利用する場合は、サービスの利用ごとに責任者を定めるものとする。ただし、要保護情報を取り扱う場合は、部局情報セキュリティ責任者が責任者を定めるものとする。
３　前項の責任者は、以下の各号に注意して運用するものとする。
(1) サービス機能の設定に関する定期的な確認
(2) 情報の滅失、破壊等に備えたバックアップの取得
(3) 利用者への注意喚起

（ソーシャルメディアサービスによる情報発信時の対策）
第６０条　部局情報セキュリティ責任者は、部局からの公式な情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービス毎に責任者を定めるものとする。
２　前項の責任者は、利用するアカウントによる情報発信が実際の本学のものであると認識できるようにするためのなりすまし対策として、以下の各号の対策を行うものとする。
(1) 本学からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、本学が運用していることを明示すること。
(2) 本学からの情報発信であることを明らかにするために、本学が本学ドメイン名を用いて管理しているウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。
(3) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている本学ウェブサイト上のページの URL を記載すること。
(4) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。
(5) URL 短縮サービスは、利用するソーシャルメディアが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、使用しないこと。
３　第１項の責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下の各号の対策を行うものとする。
(1) パスワードを適切に管理すること。具体的には、ログインパスワードは十分な長さと複雑さを持たせ、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。
(2) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。
(3) ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭ったりした場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行うこと。
(4) ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。
４　第１項の責任者は、アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、第９７条第３項の規定に基づき整備された対応手順により、適切な対処を行うものとする。
５　部局情報セキュリティ責任者は、なりすましを確認した場合の対処として、本学ウェブサイトに、なりすま

しアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うものとする。
6 教職員等は、要安定情報の提供にソーシャルメディアサービスを用いる場合は、本学が管理するウェブサイトにおいても当該情報をあわせて提供するものとする。

（クラウドサービス利用における対策）
第60条の2 部局情報セキュリティ技術責任者は、クラウドサービスを利用するに当たり、以下の各号の対策を行うものとする。
(1) 取り扱う情報の格付及び取扱制限を踏まえ、情報の取扱いをゆだねることの可否を判断すること。
(2) クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定するものとする。
(3) クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、委託先を選定する際の要件とするものとする。
(4) クラウドサービスの特性を考慮した上で、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定めるものとする。
(5) クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

第4章 情報の格付けと取扱い

（情報の作成又は入手）
第61条 教職員等は、情報システムに係る情報を作成し、又は入手する場合は、本学の教育、研究その他の業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けの決定と取扱制限の検討）
第62条 教職員等は、情報の作成時に、「京都大学情報格付け基準」（以下「格付け基準」という。）に従い当該情報の機密性、完全性及び可用性に応じて格付けを行い、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、格付け基準に従い当該情報の機密性、完全性及び可用性に応じて格付けを行い、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。

（格付けと取扱制限の明示）
第63条 教職員等は、情報の格付け及び取扱制限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。

（格付けと取扱制限の継承）
第64条 教職員等は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承するものとする。

（格付けと取扱制限の変更）
第65条 教職員等は、情報の格付け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、格付け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けを行うものとする。
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。

（格付けに応じた情報の利用）
第66条 教職員等は、情報に明示等された格付け及び取扱制限に従い、情報を適切に取り扱うものとする。
2 教職員等は、外部電磁的記録媒体を用いて情報を取り扱う際、第53条の規定に従い情報を適切に

管理するものとする。

（格付けに応じた情報の保存）
第67条　部局情報セキュリティ技術責任者は、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　部局情報セキュリティ技術責任者は、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ときは、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。
3　部局情報セキュリティ技術責任者は、要保護情報を取り扱う情報システムについては、サーバ装置を安全区域に設置するものとする。

（情報の運搬及び送信）
第68条　教職員等は、要保護情報を安全区域外に持ち出し他の場所に運搬する場合又は学外通信回線を使用して送信する場合には、安全確保に留意して運搬方法又は送信方法を決定し、情報の格付け及び取扱制限に応じて、安全確保のための適切な措置を講ずるものとする。
2　教職員等は、要保護情報が記録又は記載された記録媒体を安全区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付け及び取扱制限に応じて、安全確保のための適切な措置を講ずるものとする。
3　教職員等は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付け及び取扱制限に応じて、安全確保のための適切な措置を講ずるものとする。

（情報の消去）
第69条　教職員等は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去するものとする。
2　教職員等は、電磁的記録媒体を破棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消するものとする。
3　教職員等は、要機密情報である書面を廃棄する場合には、復元が困難な状態にするものとする。

（情報のバックアップ）
第70条　教職員等は、情報の格付けに応じて、適切な方法で情報のバックアップを実施するものとする。
2　教職員等は、取得した情報のバックアップについて、格付け及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理するものとする。
3　教職員等は、保存期間を過ぎた情報のバックアップについては、適切な方法で消去、抹消又は廃棄するものとする。

第5章　主体認証

（主体認証機能の導入）
第71条　部局情報セキュリティ技術責任者は、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。この場合、要保護情報を取り扱う情報システムについては、主体認証を行うものとする。
2　部局情報セキュリティ技術責任者は、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　部局情報システム技術担当者は、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、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。
4　部局情報セキュリティ技術責任者は、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、以下の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　部局情報セキュリティ技術責任者は、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、直ちに当該主体認証情報若

しくは主体認証情報による主体認証を停止する機能を設けるものとする。
6 部局情報セキュリティ技術責任者は、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、以下の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
(3) 主体認証情報を設定する時は、セキュリティ上の強度が指定以上となるように要求する機能
7 部局情報セキュリティ技術責任者は、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、生体情報以外の主体認証方式を用いる場合には、以下の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こと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、以下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) 部局情報システム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こと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 部局情報セキュリティ責任者は、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所有による主体認証を行うための主体認証情報格納装置を発行する場合、発行及び返還についての手続を定めるものとする。
9 部局情報セキュリティ技術責任者は、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。
10 部局情報セキュリティ責任者は、セキュリティ侵害又はその可能性が認められる場合、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6章 アクセス制御

(アクセス制御機能の導入)
第72条 部局情報セキュリティ技術責任者は、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。この場合、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ものとする。
2 部局情報セキュリティ技術責任者は、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。

(適正なアクセス制御)
第73条 部局情報セキュリティ技術責任者は、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じるよう、利用者等に指示するものとする。
2 教職員等は、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けと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74条 部局情報セキュリティ技術責任者及び部局情報システム技術担当者は、無権限のアクセス行為を発見した場合は、速やかに部局情報セキュリティ責任者及び情報ネットワーク危機管理委員会に報告するものとする。部局情報セキュリティ責任者は、上記の報告を受けたときは、遅滞なく最高情報セキュリティ責任者にその旨を報告するものとする。
2 最高情報セキュリティ責任者及び部局情報セキュリティ責任者は、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じるものとする。

第7章 アカウント管理

（アカウント管理機能の導入）
第75条　部局情報セキュリティ技術責任者は、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。この場合、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ものとする。
2　部局情報セキュリティ技術責任者は、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76条　部局情報セキュリティ技術責任者は、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、以下の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　部局情報セキュリティ技術責任者は、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77条　部局情報セキュリティ技術責任者は、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、部局情報セキュリティ技術責任者が、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78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95条第3項第3号によるアカウント停止命令又は削除命令期間中である場合を除き、遅滞な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、期限付きの仮パスワードを発行する等の措置を講じることが望ましい。
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79条　アカウント管理を行う者は、アカウントを発行したときは、速やかにその旨を部局情報セキュリティ技術責任者に報告するものとする。
2　部局情報セキュリティ責任者は、必要に応じて部局情報セキュリティ技術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80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、次の各号に掲げる項目を定期的に確認するものとする。
(1) 利用資格を失ったもの
(2) 部局情報セキュリティ技術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) 一定期間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８１条　アカウント管理を行う者は、前条第１項第１号及び第２号に該当するアカウントを発見したとき又は第９５条第３項第３号によ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、その旨を部局情報セキュリティ技術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し、その旨を部局情報セキュリティ技術責任者に報告するものとする。
３　部局情報セキュリティ技術責任者は、前２項の報告を受けたときは、速やかに、当該報告に係るアカウント削除の対象となった利用者等に、アカウントを削除したことについて通知するものとする。ただし、電子メール、電話及び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。
４　部局情報セキュリティ責任者は、必要に応じて部局情報セキュリティ技術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８２条　アカウント管理を行う者は、第８０条第１項第３号及び第４号に該当するアカウントを発見したとき、第９５条第３項第３号よ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、速やかに当該アカウントを停止し、その旨を部局情報セキュリティ技術責任者に報告するものとする。
２　部局情報セキュリティ技術責任者は、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、電子メール、電話及び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　部局情報セキュリティ責任者は、必要に応じて部局情報セキュリティ技術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８３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、その旨を部局情報セキュリティ技術責任者に申し出るものとする。
２　部局情報セキュリティ技術責任者は、前項の申出を受けたときは、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復帰の可否の検討を指示するものとする。
３　アカウント管理を行う者は、前項の指示に従って当該アカウントの安全性の確認及びアカウント復帰の可否の検討を行い、復帰させる場合は速やかに行うものとする。

（管理者権限を持つアカウントの利用）
第８４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８章　証跡管理

（証跡管理機能の導入）
第８５条　部局情報セキュリティ技術責任者は、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　部局情報セキュリティ技術責任者は、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　部局情報セキュリティ技術責任者は、証跡を取得する必要があると認めた情報システムにあっては、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　部局情報セキュリティ技術責任者は、証跡を取得する必要があると認めた情報システムにあっては、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　部局情報セキュリティ技術責任者は、証跡を取得する必要があると認めた情報システムにあっては、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、電磁的記録媒体等その他の装置・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。

（部局情報システム技術担当者による証跡の取得と保存）
第８６条　部局情報システム技術担当者は、証跡を取得する必要があると認めた情報システムにあっては、

部局情報セキュリティ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 部局情報システム技術担当者は、証跡を取得する必要があると認めた情報システムにあっては、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 部局情報システム技術担当者は、証跡を取得する必要があると認めた情報システムにあっては、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は、前条第4項で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87条 部局情報セキュリティ責任者又は部局情報セキュリティ技術責任者は、証跡を取得する必要があると認めた情報システムにあっては、部局情報システム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88条 規程第13条第1項に規定する範囲は、セキュリティ確保のために必要であり、かつ、通信の内容を不必要に含まないものとして、監視を行わせる最高情報セキュリティ責任者又は部局情報セキュリティ責任者が、具体的に指示した範囲とする。ただし、インシデントに対処するために特に必要と認められる場合、最高情報セキュリティ責任者又は部局情報セキュリティ責任者は、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。
2 前項本文に規定する範囲の監視に係る規程第13条第1項に規定する手続は、当該監視を行わせる者が最高情報セキュリティ責任者の場合には、あらかじめ全学情報セキュリティ委員会の議を経ることを、部局情報セキュリティ責任者の場合には、あらかじめ部局情報セキュリティ委員会の議を経ることをいい、前項ただし書の場合については、当該監視を行わせる者が、規程第13条第1項により指名された者の意見を聴いたうえで、監視又は調査を命じ、報告を受けることをいう。
3 規程第13条第2項に規定する内容は、個人の特定に結びつく情報で、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とし、同項に規定する手続は、監視を行わせる者が重大なセキュリティ侵害としてあらかじめ指示した基準に従い、伝達を行うことをいう。
4 規程第13条第2項に規定する特に定める者は、情報ネットワーク危機管理委員会並びに情報ネットワーク倫理委員会とする。
5 監視によって採取された記録（以下「監視記録」という。）は要保護情報とし、監視を行わせる者を情報の作成者とする。
6 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。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。
7 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、これを閲覧し、かつ、保存することができる。監視記録を不必要に閲覧してはならない。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89条 複数の者が利用する情報機器を管理する部局情報システム技術担当者（以下「情報機器の管理者」という。）は、当該情報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。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る。個人情報の取得を目的とすることはできない。ただし、当該情報機器を管理する部局情報セキュリティ責任者が教育上特に必要と認めた場合は、この限りでない。
3 利用記録は要機密情報、要保全情報とし、当該情報機器の管理者を情報の作成者とする。ただし、部局情報セキュリティ責任者が特に指定した利用記録は、この限りでない。
4 当該情報機器の管理者は、第1項に規定する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。
5 当該情報機器の管理者は、第1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。

6 第1項の規定により情報機器の利用記録を採取しようとする者は、第1項に規定する目的、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、あらかじめ部局情報セキュリティ責任者に申告し、かつ、当該機器の利用者等に開示しなければならない。部局情報セキュリティ責任者は、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。
7 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項に規定する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。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

（個人情報の取得と管理）
第90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、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。
3 部局情報セキュリティ技術責任者は、情報システムで取り扱う個人情報の内容に応じて、当該個人情報の不正な持ち出しが発見できるよう必要な措置を講ずるものとする。
4 部局情報セキュリティ技術責任者は、情報システムで取り扱う個人情報の内容に応じて、その処理を行う端末を限定するために必要な措置を講ずるものとする。

（利用者等が保有する情報の保護）
第91条 利用者等が保有する情報は、情報システム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9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92条 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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93条 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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 部局情報セキュリティ技術責任者は、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安全な方法で提供するものとする。
4 部局情報セキュリティ技術責任者は、暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化に関する情報を定期的に入手し、必要に応じて、利用者等と共有を図るものとする。

（暗号・電子署名の利用時の教職員等の対策）
第94条　教職員等は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うものとする。
2　教職員等は、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、定められた鍵の管理手順等に従い、これを適切に管理するものとする。
3　教職員等は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うものとする。

第10章　違反と例外措置

（違反への対応）
第95条　利用者等は、情報セキュリティ関係規程への重大な違反を知った場合は、部局情報セキュリティ責任者にその旨を報告するものとする。
2　部局情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合又は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。
3　部局情報セキュリティ責任者は、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)　部局情報セキュリティ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)　部局情報セキュリティ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)　その他法令に基づく措置
4　部局情報セキュリティ責任者は、前項第2号及び第3号については、他部局の部局情報セキュリティ責任者を通じて同等の措置を依頼することができる。
5　部局情報セキュリティ責任者は、情報セキュリティ関係規程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又は第3項の措置を講じた場合は、遅滞なく当該行為者の所属部局及び最高情報セキュリティ責任者にその旨を報告するものとする。

（例外措置）
第96条　全学情報セキュリティ委員会は、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、情報セキュリティ実施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、連絡先）
(2)　申請内容
・申請者の情報（氏名、所属、連絡先）
・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等）
・例外措置の適用を申請する期間
・例外措置の適用を申請する措置内容（講ずる代替手段等）
・例外措置の適用を終了した旨の報告方法
・例外措置の適用を申請する理由
(3)　審査結果の内容
・許可又は不許可の別
・許可又は不許可の理由
・例外措置の適用を許可した情報セキュリティ関係規程の適用箇所（規程名と条項等）
・例外措置の適用を許可した期間
・許可した措置内容（講ずるべき代替手段等）
・例外措置を終了した際の報告方法
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11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９７条　最高情報セキュリティ責任者は、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　情報セキュリティ実施責任者は、インシデントについて利用者等から部局情報セキュリティ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　情報セキュリティ実施責任者は、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　情報セキュリティ実施責任者は、インシデントに備え、本学の教育、研究その他の業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、その部局情報セキュリティ技術責任者及び部局情報システム技術担当者の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備するものとする。
５　情報セキュリティ実施責任者は、インシデントへの対処の訓練の必要性を検討し、本学の教育、研究その他の業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、その訓練の内容及び体制を整備するものとする。
６　情報セキュリティ実施責任者は、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。
７　部局情報セキュリティ責任者は、インシデントが発生した場合の連絡及び報告、インシデントの原因の調査、再発防止策の策定等の対応を速やかに行うため、部局内の体制を整備するものとする。

（インシデントの原因調査、再発防止策及び報告）
第９８条　部局情報セキュリティ責任者は、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たうえで再発防止策を策定し、その結果を報告書として CSIRT 責任者に報告するものとする。
２　CSIRT は、インシデントを認知した場合には、前条第３項により情報セキュリティ実施責任者が定める対応手順に従い、直ちに必要な措置を講ずる。
３　情報ネットワーク危機管理委員会及び情報ネットワーク倫理委員会は、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等必要な措置を講ずる。
４　最高情報セキュリティ責任者は、本学情報システムに係るインシデントが発生した場合、当該インシデントに係る情報について、文部科学省に可能な限り速やかに連絡するものとする。また、規程第３条第１項に規定する情報資産のうち、本学情報システムを除くものに係るインシデントが発生した場合、当該インシデントに係る情報について、必要に応じて文部科学省に可能な限り速やかに連絡するものとする。
５　部局情報セキュリティ連絡責任者は、CSIRT 及び当該部局の間の連絡並びに当該部局内の部局情報セキュリティ責任者、部局情報セキュリティ技術責任者、部局情報システム技術担当者及び部局情報セキュリティ委員会の間の連絡を総括する。

第１２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かかる安全管理措置の整備）
第９９条　情報セキュリティ実施責任者は、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。

（本学支給以外の端末の利用許可及び届出の取得及び管理）
第１００条　教職員等は、要保護情報（機密性２情報を除く。）について本学支給以外の端末により情報処理を行う必要がある場合には、部局情報セキュリティ技術責任者の許可を得るものとする。
２　教職員等は、機密性２情報について本学支給以外の端末により情報処理を行う必要がある場合には、部局情報セキュリティ技術責任者に届け出るものとする。ただし、部局情報セキュリティ技術責任者が届出を要しないとした場合は、この限りでない。
３　部局情報セキュリティ技術責任者は、本学支給以外の端末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。
４　部局情報セキュリティ技術責任者は、要保護情報（機密性２情報を除く。）について本学支給以外の端末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、部局情報セキュリティ技術責任者が報告を要しないとした場合は、この限りでない。
５　部局情報セキュリティ技術責任者は、機密性２情報について本学支給以外の端末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１３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101条　本学情報システムを運用・管理する者は、必要に応じて、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して、以下の措置を講ずるものとする。

(1) 提供するアプリケーション・コンテンツについて不正プログラム対策を行うこと。

(2) 提供するアプリケーションについて脆弱性対策を行うこと。

(3) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

(4) 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

(5) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等を利用する者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

(6) サービス利用に当たって必須ではない、サービスを利用する者及びその他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

2 教職員等は、アプリケーション・コンテンツの開発及び作成を外部委託する場合において、前項の各号に掲げる内容を調達仕様に含めること。

（本学ドメインの使用）

第102条　部局情報セキュリティ技術責任者は、学外向けに提供するウェブサイト等が実際の本学のものであることをウェブサイト等を利用する者が確認できるように、.kyoto-u.ac.jp で終わるドメイン名（以下「本学ドメイン名」という。）を情報システムにおいて使用するよう仕様に含めるものとする。ただし、第 59条及び第60条に掲げる場合を除く。

2 教職員等は、学外向けに提供するウェブサイト等の作成を外部委託する場合においては、前項と同様、本学ドメイン名を使用するよう調達仕様に含めるものとする。

（不正なウェブサイトへの誘導防止）

第103条　部局情報セキュリティ技術責任者は、利用する者が検索サイト等を経由して本学のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講じるものとする。

第14章　教育・研修

（情報セキュリティ対策の教育）

第104条　最高情報セキュリティ責任者は、情報セキュリティポリシー及び実施規程について、部局情報セキュリティ責任者、部局情報セキュリティ技術責任者、部局情報システム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、その啓発を行うものとする。

2 最高情報セキュリティ責任者は、情報セキュリティポリシー及び実施規程について、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 最高情報セキュリティ責任者は、教育啓発対象者が毎年度最低一回、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 最高情報セキュリティ責任者は、教育啓発対象者の入学時、着任時、異動時に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 最高情報セキュリティ責任者は、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 最高情報セキュリティ責任者は、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情報セキュリティ責任者に通知するものとする。

7 部局情報セキュリティ責任者は、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、最高情報セキュリティ責任者にその旨を報告するものとする。

8 最高情報セキュリティ責任者は、毎年度、全学情報セキュリティ委員会に対して、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 最高情報セキュリティ責任者は、情報セキュリティポリシー及び実施規程について、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。

（教育の主体と客体）
第105条　情報セキュリティ実施責任者は、本学情報システムの運用に携わる者及び利用者等に対して、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、情報セキュリティポリシー及び実施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ものとする。
2　部局情報セキュリティ技術責任者及び部局情報システム技術担当者は、利用者等に対して、講習計画において定める講習を実施するものとする。

第15章　評価等

（自己点検に関する年度計画の策定）
第106条　最高情報セキュリティ責任者は、情報セキュリティに関する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107条　部局情報セキュリティ責任者は、教職員等の役割ごとの情報セキュリティに関する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108条　部局情報セキュリティ責任者は、最高情報セキュリティ責任者が定める情報セキュリティに関する年度自己点検計画に基づき、教職員等に対して、自己点検の実施を指示するものとする。
2　教職員等は、部局情報セキュリティ責任者から指示された情報セキュリティに関する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109条　部局情報セキュリティ責任者は、教職員等による情報セキュリティに関す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　最高情報セキュリティ責任者は、部局情報セキュリティ責任者による情報セキュリティに関す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110条　教職員等は、自らが実施した情報セキュリティに関する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、部局情報セキュリティ責任者にその旨を報告するものとする。
2　最高情報セキュリティ責任者は、情報セキュリティに関する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情報セキュリティ責任者に改善を指示するものとする。

（監査）
第111条　部局情報セキュリティ責任者その他の関係者は、最高情報セキュリティ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。

（リスク管理の実施）
第112条　最高情報セキュリティ責任者は、情報資産の価値と脅威、脆弱性を評価するための情報システム運用リスク評価手順を定める。
2　最高情報セキュリティ責任者は、情報セキュリティ実施責任者を含む各情報資産の管理者に対して、少なくとも年に一回、リスク管理を次の各号に従って実施し、その結果を報告するよう指示する。
(1)　当該管理者は、自らが扱う情報資産について情報システム運用リスク評価手順に基づきリスク評価を行う。
(2)　当該管理者は、評価結果に従い、リスクに対する事前の対策を必要とするものについてその具体策を定め、あるいはトラブルが発生した場合の具体的な対応について当該情報資産についてのインシデント対応手順を定める。対策を施さないと判断したものについても報告する。

3　最高情報セキュリティ責任者は、前項に基づく管理者からの報告に基づいて、情報セキュリティポリシー及び実施規程等の見直しを行う。
（見直し）
第113条　情報セキュリティポリシー及び実施規程並びにそれに基づく手順等を整備した者は、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。

附　則

この対策基準は、平成21年4月1日から実施する。

附　則

この対策基準は、平成27年4月1日から実施する。ただし、第52条第1項の規定は、平成28年4月1日から実施する。

附　則

この対策基準は、平成29年4月1日から実施する。

附　則

この対策基準は、平成31年4月1日から実施する。

附　則

この対策基準は、令和2年4月1日から実施する。

（別表）

用語集

【あ】

「アクセス制御」とは、情報へのアクセスを許可する者を制限することをいう。

「アプリケーション」とは、OS 上で動作し、サービスの提供、文書作成又は電子メールの送受信等の特定の目的のために動作するソフトウェアをいう。

「アルゴリズム」とは、ある特定の目的を達成するための演算手順をいう。

「暗号化」とは、第三者に容易に解読されないよう、定められた演算を施しデータを変換することをいう。

「委託先」とは、外部委託により本学の情報システムに関する計画、構築及び運用等の情報処理業務の一部又は全部を実施する者をいう。

「受渡業者」とは、安全区域内で職務に従事する教職員等との物品の受渡しを目的とした者のことで、安全区域へ立ち入る必要のない者をいう。物品の受渡しとしては、宅配便の集配、事務用品の納入等が考えられる。

【か】

「外部委託」とは、本学の情報処理業務の一部又は全部について、契約をもって学外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、全てを含むものとする。

「記録媒体」とは、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、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。

「学外」とは、本学が管理する組織又は施設の外をいう。

「学外通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び本学管理又は他組織管理）及び通信回線装置を問わず、本学が管理していないサーバ装置及び端末が接続され、当該サーバ装置及び端末間の通信に利用する論理的な通信回線をいう。

「学外での情報処理」とは、本学外で職務の遂行のための情報処理を行うことをいう。なお、オンラインで学外から本学の情報システムに接続して、情報処理を行う場合だけではなく、オフラインで行う場合も含むものとする。

「学内」とは、本学が管理する組織又は施設の内をいう。

「学内通信回線」とは、物理的な通信回線を構成する回線（有線又は無線、現実又は仮想及び本学管理又は他組織管理）及び通信回線装置を問わず、本学が管理するサーバ装置及び端末を相互に接続し、当該サーバ装置及び端末間の通信に利用する論理的な通信回線をいう。

「可用性」とは、情報へのアクセスを認可された者が、必要時に中断することなく、当該情報及び関連情報

資産にアクセスできる状態を確保することをいう。

「可用性1情報」とは、可用性2情報以外の情報（書面を除く。）をいう。

「可用性2情報」とは、職務で取り扱う情報（書面を除く。）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、本学の教育、研究その他の業務に支障を及ぼす又は職務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

「完全性」とは、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。

「完全性1情報」とは、完全性2情報以外の情報（書面を除く。）をいう。

「完全性2情報」とは、職務で取り扱う情報（書面を除く。）のうち、その改ざん、誤びゅう又は破損により、大学の運営に支障を及ぼす又は職務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報をいう。

「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

「機密性」とは、情報に関して、アクセスを認可さ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。

「機密性1情報」とは、機密性2情報又は機密性3情報以外の情報をいう。

「機密性2情報」とは、職務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、直ちに一般に公表することを前提としていない情報をいう。

「機密性3情報」とは、職務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報をいう。

「共用識別コード」とは、複数の主体が共用するために付与された識別コードをいう。原則として、1つの識別コードは1つの主体のみに対して付与されるものであるが、情報システム上の制約や、利用状況などに応じて、1つの識別コードを複数の主体で共用する場合もある。このように共用される識別コードを共用識別コードという。

「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

「クラウドサービス事業者」とは、クラウドサービスを提供する事業者又はクラウド サービスを用いて情報システムを開発・運用する事業者をいう。

「権限管理」とは、主体認証に係る情報（識別コード及び主体認証情報を含む。）及びアクセス制御における許可情報を管理することをいう。

「公開されたセキュリティホール」とは、誰もが知り得る状態に置かれているセキュリティホールのことであり、ソフトウェアやハードウェアの製造・提供元等から公表されたセキュリティホール、セキュリティ関連機関から公表されたセキュリティホール等が該当する。

【さ】

「サービス」とは、サーバ装置上で動作しているアプリケーションにより、接続してきたサーバ装置及び端末に対して提供される単独又は複数の機能で構成される機能群をいう。

「サービス不能攻撃」とは、悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置又は通信回

線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い通常のサービス利用を妨害する攻撃をいう。

「主体認証情報格納装置」とは、主体認証情報を格納した装置であり、正当な主体に所有又は保持させる装置をいう。所有による主体認証では、これを所有していることで、情報システムはその主体を正当な主体として認識する。
代表的な主体認証情報格納装置として、磁気テープカードやICカード等がある。

「情報機器等管理者」とは、規程第５条の3に定められた部局情報システム技術担当者をいう。

「情報管理者」とは、情報を作成又は入手した教職員（第６１条）であり、格付けの決定と取扱制限の検討（第６２条）及び格付けと取扱制限の明示（第６３条）、格付けと取扱制限の変更（第６５条）などの管理を行なわねばならない。

「情報セキュリティ関係規程」とは、本基準及び本基準に定められた対策内容を具体的な情報システムや業務においてどのような手順に従って実行していくかについて定めた実施手順をいう。

「情報の移送」とは、当該情報に責任を持つ者の管理権限が及ばない情報システム又は組織に対し、電磁的に記録された情報を送信すること並びに情報を記録した電磁的記録媒体、PC 及び書面を運搬することをいう。

「ソーシャルメディアサービス」とは、インターネット上の Web サービスの一種で、サービス利用者間で双方向のコミュニケーションを可能とするものをいう。

「ソフトウェア」とは、サーバ装置及び端末を動作させる手順及び命令をサーバ装置及び端末が理解できる形式で記述したものをいう。オペレーティングシステム、オペレーティングシステム上で動作するアプリケーションを含む広義の意味である。

【た】
「対策用ファイル」とは、パッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイルをいう。

「通信回線」とは、これを利用して複数のサーバ装置及び端末を接続し、所定の通信様式に従って情報を送受信するための仕組みをいう。回線及び通信回線装置の接続により構成された通信回線のことを物理的な通信回線といい、物理的な通信回線上に構成され、サーバ装置及び端末間で所定の通信様式に従って情報を送受信可能な通信回線のことを論理的な通信回線という。

「通信回線装置」とは、通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御を行うための装置をいう。いわゆるハブ、スイッチ及びルータ等のほか、ファイアウォール等pも該当する。

「データセンター」とは、インターネット用のサーバやデータ通信などの装置を設置・運用することに特化した建物の総称をいう。

「特定用途機器」とは、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。

「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。例えば、www.kyoto-u.ac.jp というウェブサイトの場合は、kyoto-u.ac.jp の部分がこれに該当する。

「取扱制限」とは、情報の取扱いに関する制限であって、複製禁止、持出禁止、再配付禁止、暗号化必

須、読後廃棄等をいう。

【は】

「複数要素(複合)主体認証(multiple factors Authentication / composite Authentication)方式」とは、複数の主体認証情報の組合せにより主体認証を行う方法である。例えばICカードに加えてパスワードで主体認証を行う場合などが該当する。

「不正アクセス」とは、サーバ装置及び端末の利用を許可された者が当該サーバ装置及び端末を許可された方法以外で作動させること又は操作すること及びサーバ装置及び端末の利用を許可されていない者がサーバ装置及び端末を操作又は利用することをいう。

「不正プログラム」とは、コンピュータウイルス、ワーム(他のプログラムに寄生せず単体で自己増殖するプログラム)、スパイウェア(プログラムの使用者の意図に反して様々な情報を収集するプログラム)等の情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称をいう。

「不正プログラム定義ファイル」とは、アンチウイルスソフトウェア等が不正プログラムを判別するために利用するデータをいう。

「付与」(主体認証に係る情報、アクセス制御における許可情報等に関して)とは、発行、更新及び変更することをいう。

「本学支給以外の情報システム」とは、本学が支給する情報システム以外の情報システムをいう。いわゆる私物のPCやモバイル端末のほか、本学への出向者に対して出向元組織が提供する情報システムも含むものとする。

「本学支給以外の情報システムによる情報処理」とは、本学支給以外の情報システムを用いて職務の遂行のための情報処理を行うことをいう。なお、直接装置等を用いる場合だけではなく、それら装置等によって提供されているサービスを利用する場合も含むものとする。ここでいうサービスとは、個人が契約している電子メールサービス等のことであり、例えば、本学の業務に要する電子メールを、個人で契約している電子メールサービスに転送して業務を行ったり、個人のメールから業務のメールを発信したりすることである。

【ま】

「明示」とは、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。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなども明示に含むものとする。

「モバイル端末」とは、端末の形態に関係なく、業務で利用する目的により必要に応じて移動するノート型PC、スマートフォン及びタブレット等の端末をいう。特定の設置場所だけで利用するノート型PCは、モバイル端末に含まれない。

【や】

「約款による外部サービス」とは、民間事業者等の学外の組織が定めた規約等の約款に基づきインターネット上で提供する情報処理サービスであって、有料、無料に関わらず、約款への同意及び簡易なアカウントの登録等により、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。電子メール、ファイルストレージ、グループウェア等のサービスが代表的である。ただ

し、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

「要安定情報」とは、可用性2情報をいう。

「要機密情報」とは、機密性2情報及び機密性3情報をいう。

「要保護情報」とは、要機密情報、要保全情報及び要安定情報をいう。

「要保全情報」とは、完全性2情報をいう。

【ら】

「例外措置」とは、教職員等がその実施に責任を持つ情報セキュリティ関係規程を遵守することが困難な状況で、職務の適正な遂行を継続するため、遵守事項とは異なる代替の方法を採用し、又は遵守事項を実施しないことについて合理的理由がある場合に、そのことについて申請し許可を得た上で適用する行為をいう。

「ログイン」とは、何らかの主体が主体認証を要求する行為をいう。ログインの後に主体認証が行われるため、ログインの段階ではその主体が正当であるとは限らない。

「ログオン」とは、ログインの結果により、主体認証を要求した主体が正当であることが情報システムに確認された状態をいう。