# 京都大学全学情報システム利用規則

〔平成22年　1月12日情報担当理事裁定〕

（目的）

第1条　本規則は、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）第2条第5号に基づき、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4条により指定された全学情報システムの利用に関する事項を定め、京都大学（以下「本学」という。）における情報セキュリティの確保と情報システムの円滑な利用に資することを目的とする。

2　全学情報システムの利用目的は以下とする。

(1) 本学の教育・研究活動のほか国立大学法人法（平成15年法律第112号）に基づき本学が行う業務

(2) その他情報環境機構長が特に認めたもの

（定義）

第2条　本規則において、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) 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。

(2) 情報セキュリティポリシー　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）及び前号の規程をいう。

(3) 実施規程　情報セキュリティポリシーに基づき情報担当の理事が定める京都大学情報セキュリティ対策基準（以下「対策基準」という。）その他の規程、基準及び計画をいう。

(4) 機構利用規程　本学が定める「京都大学情報環境機構教育用コンピュータシステム及び学術情報ネットワークシステム利用規程」（平成24年4月27日情報環境機構長裁定）をいう。

(5) 全学情報システム　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として、対策基準第4条に基づき最高情報セキュリティ責任者が指定した、統合認証システム（第23号に定めるもの）及び学術情報ネットワークシステム（第15号に定めるもの）をいう（平成21年6月9日全学情報セキュリティ委員会了承）。

(6) 特定部局情報システム　部局情報システム（対策基準第2条第8号に定めるものをいう）のうち、第18条第1項に基づき KUINS に接続されたもの又は第19条第1項により統合認証システムに接続されたものをいう。

(7) 利用者端末　学内・学外に関らず利用者等が全学情報システム及び特定部局情報システムを特定利用（第40号に定めるもの）するために用いる情報機器（全学情報システム又は特定部局情報システムを除く）をいう。

(8) 管理運営組織　対策基準第4条第2項に定める情報環境機構をいう。

(9) 教職員等　役員及び本学が定める就業規則に基づき雇用されている教職員をいう。

(10) 学生等　学部学生及び大学院学生、外国学生、委託生、科目等履修生、聴講生、特別聴講学生、特別研究学生、特別交流学生等(京都大学通則（昭和28年達示第3号)第5章に定めるもの)、研究生、研修員等（京都大学研修規程（昭和24年達示第3号）に定めるもの）その他本学規程に基づき受け入れる研究者等をいう。

(11) 利用者　教職員等及び学生等で、全学情報システム又は特定部局情報システムを利用する者をいう。

(12) 全学情報システム臨時利用者　教職員等及び学生等以外の者で、情報環境機構長の許可を受けて、全学情報システムを利用（運用・管理等の業務において取り扱うことを含む。以下同じ）する者をいう。

(13) 特定部局情報システム臨時利用者　教職員等及び学生等以外の者で、特定部局情報システムについて、当該部局の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の許可を受けて利用する者をいう。

(14) 利用者等　利用者及び全学情報システム臨時利用者並びに特定部局情報システム臨時利用者をいう。

(15) KUINS　機構利用規程にいう学術情報ネットワークシステムをいい、グローバル IP アドレスの KUINS（KUINS-II）及びプライベート IP アドレスの KUINS（KUINS-III）からなる。

(16) KUINS 機器管理責任者　機構利用規程第8条第2項に定める「KUINS 接続者」のうち、同規程第10条第1号に定める「グローバル IP アドレスの KUINS」に接続する者をいう。

(17) KUINS 情報コンセント管理担当者　機構利用規程第8条第2項に定める「KUINS 接続者」のうち、同規程第10条第2号に定める「プライベート IP アドレスの KUINS」に接続する者をいう。

(18) サブネット連絡担当者　機構利用規程第11条第1号に定める「サブネット連絡担当者」をいう。

(19) VLAN 管理責任者　機構利用規程第11条第2号に定める「VLAN 管理責任者」をいう。

(20) KUINS 支払責任者　機構利用規程第15条に定める「KUINS 接続者又はこれに代わる者」をいう。

(21) 共通コード体系アカウント　利用者等が、全学情報システム又は特定部局情報システムを利用する際、主体認証（第35号に定めるもの）を行うために用いる教職員アカウント（以下「SPS-ID」という。）及び学生アカウント（以下「ECS-ID」という。）（以下あわせて「全学アカウント」という。）をいう。

(22) 臨時アカウント　全学情報システム臨時利用者に対して発行された全学アカウントをいう。

(23) 統合認証システム　認証システム（第24号に定めるもの）、統合 LDAP サーバ（第25号に定めるもの）、京都大学認証局及び IC カード（第28号に定めるもの）からなる情報基盤をいう。

(24) 認証システム　全学生認証ポータルシステム、教職員グループウェアの認証システム、教育研究コミュニティ認証連携システムをいう。

(25) 統合 LDAP サーバ　全学アカウント、パスワード及び一部の属性を収容しているディレクトリデータベースをいう。

(26) 京都大学認証局　京都大学電子認証局ポリシー及び運用規則（平成21年2月2日情報担当理事裁定）1．3に定める認証局をいう。

(27) 電子証明書　京都大学認証局から発行された証明書でログイン時の主体認証等に利用するため証明書をいう。

(28) IC カード　IC 職員証（第29号に定めるもの）、認証 IC カード（第30号に定めるもの）、IC 学生証（第31号に定めるもの）並びに施設利用証をいう。

(29) IC職員証　「京都大学職員証取扱要項（昭和60年2月23日総長裁定）」に基づき常勤の教職員等に着任時に交付される職員証であって、主体認証情報（第37号に定めるもの）をICに格納するものをいう。

(30) 認証ICカード　「京都大学認証ICカード取扱要項（平成21年11月10日情報環境機構長裁定）」に基づき非常勤の教職員等に着任時に交付されるICカードであって、主体認証情報をICに格納するものをいう。

(31) IC学生証　学部学生及び大学院学生に対して所属部局が交付する学生証であって、主体認証情報をICに格納するものをいう。

(32) 施設利用証　IC職員証、認証ICカード、IC学生証のいずれも交付を受けていない利用者等に対して、「京都大学施設利用証取扱要項（平成21年11月10日情報環境機構長裁定）」に基づき、情報環境機構長が発行する利用証であって、主体認証情報をICに格納するものをいう。

(33) 発行責任組織　IC 職員証においては総務部、IC 学生証においては当該学生の所属する部局、認証 IC カード及び施設利用証においては情報環境機構をいう。

(34) PIN　(Personal Identification Number)　電子証明書を格納した IC カードを使った主体認証時に使われる主体認証情報をいう。

(35) 主体認証　次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。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際には、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。識別コードと共に正しい方法で主体認証情報が提示された際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。

(36) 識別コード　主体認証を行うために、主体が提示する情報のうち、情報システムが主体を正当な権限を有するものとして認識する情報をいう。代表的な識別コードとして、ID等がある。

(37) 主体認証情報　主体認証を行うために、主体が提示する情報のうち、情報システムが主体を正当な権限を有するものとして認識する情報をいう。代表的な主体認証情報として、パスワード及び主体認証情報格納装置等がある。

(38) 不正アクセス対応連絡要領　「コンピュータ不正アクセス対応連絡要領」(平成25年2月5日 全学情報セキュリティ委員会決定)をいう。

(39) 不正アクセス　不正アクセス対応連絡要領 第1に定める、京都大学の情報セキュリティ対策基準に基づき、本学情報システムへの不正侵入(データ破壊、ホームページ改ざん、メール不正中継(迷惑メール)等)やコンピュータウィルス、その他により、被害が発生した場合をいう。

(40) 特定利用　KUINS 接続者又は第18条第7項により許可を受けた利用者等による KUINS の利用(運用・管理等の業務において取り扱うことを含む。以下同じ)、並びに利用者等による全学アカウント、ICカード又は電子証明書による主体認証を伴っての全学情報システム又は特定部局情報システムの利用をいう。

(41) その他の用語の定義は、規程並びに対策基準の定めるところによる。

(適用範囲)

第3条　本規則は教職員等のほか、すべての利用者等に適用する。

2　本規則は、以下の情報システムを対象とする。

(1) 全学情報システム

(2) 特定部局情報システム

(3) 利用者端末(特定利用に用いられているときに限る)

(全学アカウントの申請と交付)

第4条　全学情報システム又は特定部局情報システムを、全学アカウントによる主体認証を伴って利用する利用者等は、情報環境機構長が別途定める手続きにより、申請を行い情報環境機構から全学アカウントを取得しなければならない。

(IC カードと電子証明書の取得)

第5条　全学情報システム又は特定部局情報システムを、IC カードによる主体認証を伴って利用する利用者等は、必要な IC カードを当該の発行責任組織から取得しなければならない。

2　全学情報システム又は特定部局情報システムを、電子証明書による主体認証を伴って利用する教職員等は、情報環境機構から電子証明書を取得しなければならない。

(全学情報システム臨時利用者及び特定部局情報システム臨時利用者への許可)

第6条　情報環境機構長は、教職員等及び学生等以外の者について、次の各号のいずれかに該当し必要があると認めるときは、全学情報システム臨時利用者として、全学情報システムの利用の許可を与えるものとする。

(1) 部局情報セキュリティ責任者より臨時利用の目的・範囲・期間等を明示して申請があったとき

(2) その他情報環境機構長が特に必要があると認めたとき

2　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、教職員等及び学生等以外の者について、必要があると認めるときは、部局の定める手続きに従って、特定部局情報システムの利用の許可を与えるものとする。

3　部局情報セキュリティ責任者は、第1項第1号に基づき情報環境機構長に全学情報システム臨時利用者の利用を申請し許可された際、許可された全学情報システム臨時利用者に対して本規則を遵守させるよう必要な措置を講じなければならない。また、許可された全学情報システム臨時利用者に対して、必要と認めた場合、情報セキュリティポリシー及び実施規程並びに全学情報システムの利用に関する講習を受講させなければならない。

4　情報環境機構長は、第1項第2号に基づき全学情報システムの利用を許可した際、許可した全学情報システム臨時利用者に対して本規則を遵守させるよう必要な措置を講じなければならない。また、許可した全学情報システム臨時利用者に対して、必要と認めた場合、情報セキュリティポリシー及び実施規程並びに全学情報システムの利用に関する講習を受講させなければならない。

5　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、第2項に基づき、特定部局情報システムの利用を許可した際、許可した特定部局情報システム臨時利用者に対して本規則を遵守させるよう必要な措置を講じなければならない。また、許可した特定部局情報システム臨時利用者に対して、必要と認めた場合、情報セキュリティポリシー及び実施規程並びに全学情報システムの利用に関する講習を受講させなければならない。

（本規則で引用する遵守すべき規程等）

第7条　利用者等は、第3条第2項に定める情報システムを利用するにあたって、法令並びに本学の情報セキュリティポリシー、実施規程、本規則に基づく定め、利用に関する手順並びに「京都大学における個人情報の保護に関する規程（平成17年達示第1号）」及び「京都大学における個人番号及び特定個人情報の保護に関する規程（平成27年達示第49号）」を遵守しなければならない。

2　利用者等は、特定部局情報システムを利用するにあたって、本規則に定めるほか、当該部局が別途定める利用に関する規程及び手順等がある場合にはそれを遵守しなければならない。

3　利用者等は、第3条第2項に定める情報システムを利用して、学内・学外に関わらず情報システムを利用する際、法令を遵守するとともに、当該情報システムの利用に関して当該利用者等と当該情報システムの提供者又は管理者との間で契約に基づく定めのある場合にはそれを遵守しなければならない。

4　IC カードを利用する教職員等は、電子証明書の利用については、本規則に定めるほか、別途定める「京都大学電子認証局ポリシー及び運用規則(平成21年2月2日情報担当理事裁定)」を遵守しなければならない。

5　IC 職員証の交付を受けた教職員等は、IC 職員証の利用については、本規則に定めるほか、「京都大学職員証取扱要項（昭和60年2月23日総長裁定）」を遵守しなければならない。

6　認証 IC カードの交付を受けた教職員等は、認証 IC カードの利用については、本規則に定めるほか、「京都大学認証 IC カード取扱要項（平成21年11月10日情報環境機構長裁定）」を遵守しなければならない。

7　IC 学生証の交付を受けた学生等は、IC 学生証の利用については、本規則に定めるほか、発行責任組織が別途定める取扱要項を遵守しなければならない。

8　施設利用証の交付を受けた利用者等は、施設利用証の利用については、本規則に定めるほか、「京都大学施設利用証取扱要項（平成21年11月10日情報環境機構長裁定）」を遵守しなければならない。

（全学アカウント利用の遵守すべき事項）

第8条　利用者等は、全学アカウントの利用に際して次の各号を遵守しなければならない。

（1）　自分の全学アカウントを他の者に使用させたり、他の者の全学アカウントを使用したりしてはならない。

（2） 他の者の主体認証情報(パスワード)を聞き出したり使用したりしてはならない。

（3） 主体認証情報（パスワード）は、情報環境機構長が別途定める利用者パスワードガイドラインに従って適切に管理しなければならない。

(4) 利用者等は、主体認証を伴って全学情報システム又は特定部局情報システムへアクセス中の利用者端末において、他の者が無断で画面を閲覧・操作することができないように配慮しなければならない。

（5） 学外の不特定多数の人が操作（利用）可能な端末を用いて全学情報システム並びに特定部局情報システムへの全学アカウントによる主体認証を伴ってのアクセスを行ってはならない。

（6） 全学アカウントを他の者に使用され又はその危険が発生した際には、直ちに情報環境機構長にその旨を報告しなければならない。

（7） 姓名の変更等全学アカウントの変更が必要になった際は、遅滞なく情報環境機構に届け出なければならない。

（8） 全学情報システムの利用資格を喪失した際又は利用する必要がなくなった際は、遅滞なく情報環境機構に届け出なければならない。ただし、個別の届出が必要ないと、あらかじめ情報環境機構が定めている場合は、この限りでない。

（IC カード及び電子証明書利用の遵守すべき事項）

第９条　IC カードの交付を受けた利用者等は、IC カードの管理について次の各号を遵守しなければならない。

(1) IC カードを本人が意図せずに使われることのないように安全措置を講じて管理しなければならない。

(2) IC カードを他の者に付与又は貸与したり、他の者の IC カードを使用したりしてはならない。

(3) IC カードを紛失しないように管理しなければならない。紛失した際には、直ちに IC カードを発行責任組織にその旨を報告しなければならない。

(4) IC カードを利用する必要がなくなった際、又は利用資格がなくなった際には、遅滞なくこれを発行責任組織に返還しなければならない。ただし、IC 学生証については発行責任組織が別途定める。

(5) IC カードに記載された券面及び格納された電子証明書の内容が変更される場合には、遅滞なく発行責任組織にその旨を報告しなければならない。

(6) 情報環境機構がICカードに格納した電子証明書を、情報環境機構長の許可なく削除してはならない。

(7) IC カード使用時に利用する PIN は、情報環境機構長が別途定める利用者パスワードガイドラインに準じて適切に管理しなければならない。

２ IC 職員証及び認証 IC カードについて、前項第3号の報告を受けた発行責任組織の長は、直ちに情報環境機構長に報告しなければならない。 また、IC 学生証及び施設利用証について、前項第3号の報告を受けた発行責任組織の長は、情報環境機構長が別に定める手順により、情報環境機構長に報告しなければならない。

（全学情報システム利用の遵守すべき事項）

第１０条　利用者等は、第3条第2項で定める情報システムについて、第１条第2項で定める目的以外に利用してはならない。特定部局情報システム及びそれにネットワーク接続される利用者端末については、当該部局情報システムの利用目的について特別の定めのある場合はそれを遵守しなければならない。

２ 利用者等は、第3条第2項で定める情報システムを用いる際は、「京都大学情報資産利用のためのルール（平成１９年９月４日　部局長会議了承）」第４及び第5に定める事項を遵守しなければならない。

（P2P ソフトウェアの利用制限）

第１１条　利用者等は、第3条第2項で定める情報システムにおいて、ファイルの自動公衆送信機能を持った P2P ソフ

トウェア（以下「P2P ソフトウェア」という。）を利用する際は、次の各号を遵守しなければならない。

(1) 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。なお、P2P ソフトウェアを教育・研究目的に利用する際は所属する部局の部局情報セキュリティ責任者（全学情報システム臨時利用者においては情報環境機構長、特定部局情報システム臨時利用者においては許可した部局の部局情報セキュリティ責任者）の許可を得なければならない。

(2) KUINS-IIIにおいて P2P ソフトウェアを利用してはならない。

2 部局情報セキュリティ責任者は、第１項第１号の許可を与えるにあたって、当該 P2P ソフトウェアが KUINS-IIを利用する際には、情報環境機構長に遅滞なく届け出なければならない。

（不正プログラム対策に関する遵守すべき事項）

第１２条 特定部局情報システムを所管する部局情報システム技術担当者は、当該特定部局情報システムに対して、情報環境機構長が別に定める不正プログラム対策ガイドラインに準じた対策を実施しなければならない。

2 本学の情報システムを利用者端末として、利用者等が全学情報システム並びに特定部局情報システムを利用する際、当該利用者端末を所管する部局情報システム技術担当者は、当該利用者端末に対して、情報環境機構長が別に定める不正プログラム対策ガイドラインに準じた対策を実施しなければならない。

（全学アカウントの一時停止と復帰）

第１３条 情報環境機構長は、第7条及び第8条第１号、第2号、第3号に定める遵守事項に違反した全学アカウントの利用を発見したとき、又は主体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、全学アカウントにより主体認証を行っている全学情報システム並びに第１９条第１項に基づき統合認証システムと接続されている部局情報システムの全部又は一部へのアクセス制限を行い、その旨を該当する全学アカウントを利用している利用者等の所属する部局情報セキュリティ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、前項の措置の報告を受けたときには、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 全学アカウントの一時停止あるいはアクセス制限を受けた利用者等が、全学アカウントの復帰を希望するときは、その旨を情報環境機構長に申し出るものとする。

4 情報環境機構長は、前項の申し出を受けたときは、当該の全学アカウントの確認を行った後、速やかに全学アカウントの復帰を行うものとする。

（IC カード及び電子証明書の失効と再発行）

第１４条 情報環境機構長は、第7条及び第９条第2号、第7号に定める遵守事項に違反した IC カード及び電子証明書の利用を発見したとき、又は主体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、当該の IC カードの発行責任組織に通知するとともに、電子証明書を失効し、その旨を該当する IC カード及び電子証明書を利用している利用者等の所属する部局情報セキュリティ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、前項の措置の報告を受けたときには、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 IC カードの失効を受けた利用者等が、IC カード及び電子証明書の再発行を希望するときは、その旨を当該の発行責任組織に申し出るものとする。

4 電子証明書の失効を受けた利用者等が、IC カード及び電子証明書の再発行を希望するときは、その旨を情報環境機構に申し出るものとする。

5　発行責任組織あるいは情報環境機構は、前項の申し出を受けたときは、IC カードあるいは電子証明書を利用する上での安全性の確認を行った後、速やかに IC カードあるいは電子証明書の再発行を行うものとする。

（全学情報システム利用の違反行為への対処）

第15条　情報環境機構長は、第10条に定める遵守事項に違反すると被疑される行為を認めたとき、又は通報を受けたときは、「京都大学情報資産利用のためのルール（平成19年9月4日　部局長会議了承）」第8に基づき、情報ネットワーク倫理委員会に通知するものとする。

（インシデントへの緊急対処）

第16条　情報環境機構長は、全学情報システムにおける不正アクセス（不正アクセスか否か判断できない場合を含む、以下同じ）と被疑される状況その他全学情報システムに関する重大なセキュリティ侵害を認めたとき、直ちに最高情報セキュリティ責任者に通知しなければならない。

2　最高情報セキュリティ責任者は、直ちに情報ネットワーク危機管理委員会へ通知するものとする。また状況に応じて、情報環境機構長へ当該の全学情報システムと当該の特定部局情報システムあるいは利用者端末とのネットワーク接続を一時的に遮断する等被害の拡大防止の指示ができるものとする。

3　情報環境機構長は、対策基準第98条第1項に基づき、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情報ネットワーク危機管理委員会へ報告するものとする。

4　第1項への関与が認められた場合又は疑われた場合、当該部局（本学情報システムでない利用者端末については当該利用者の所属部局）の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の指示の下で情報環境機構長が行うインシデントの原因調査に協力しなければならない。

5　情報ネットワーク危機管理委員会は、情報環境機構長からインシデントについての報告を受けた場合には、対策基準第98条第2項に基づき、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。

（利用者端末のインシデントへの対応）

第16条の2　情報環境機構長は、利用者端末に対する不正アクセス（不正アクセスか否か判断できない場合を含む、以下同じ）と被疑される状況その他セキュリティ侵害を認めたときは、直ちに情報ネットワーク危機管理委員会に通知しなければならない。

2　情報ネットワーク危機管理委員会は、前項による情報環境機構長からの通知を受けた際には、当該利用者端末を利用している利用者の所属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。また状況に応じて、情報環境機構長へ被害の拡大防止の指示ができるものとする。

3　部局情報セキュリティ責任者は、前項による通知を受けた場合には、直ちに当該利用者及び当該利用者端末を特定し、対策基準第98条第1項に基づき、インシデントの原因を調査して再発防止策を策定し、その結果を報告書として情報ネットワーク危機管理委員会へ報告するものとする。

4　情報ネットワーク危機管理委員会は、前項の報告を受けた場合には、対策基準第98条第2項に基づき、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。

（違反行為への対処）

第17条　情報環境機構長は、第7条及び第11条に定める遵守事項に違反すると被疑される行為を認めたとき、又は通報を受けたときは、速やかに調査を行い、事実を確認するものとする。なお、事実の確認にあたっては、可能な限り当該行為を行った者の意見を聴取しなければならない。

2 第1項への関与が認められた場合又は疑われた場合、当該部局（本学情報システムでない利用者端末については当該利用者の所属部局）の部局情報セキュリティ責任者は、情報環境機構長が行う当該行為若しくは特定部局情報システム及び利用者端末についての事実の確認及び調査に協力しなければならない。

3 情報環境機構長は、第1項の措置を講じたときは、遅滞なく最高情報セキュリティ責任者にその旨を報告しなければならない。

4 調査によって違反行為が判明したときは、最高情報セキュリティ責任者は全学情報セキュリティ実施責任者を通じて次の各号に掲げる措置を講ずることができる。

(1) 当該行為者が所属する部局情報セキュリティ責任者に対する当該行為の中止勧告

(2) 部局情報セキュリティ責任者に対する当該行為に係る情報発信の遮断勧告

(3) 部局情報セキュリティ責任者に対する当該行為者の全学アカウントの停止又は削除の通知

(4) 当該行為者の所属部局及び総長への報告

(5) その他法令に基づく措置

（KUINS への機器接続及び利用の許可と停止）

第18条 機構利用規程第8条第1項に基づき KUINS に機器の接続を申請しようとする教職員等は、あらかじめ、KUINS 支払責任者として指定しようとする者の同意を得た上で、所属部局の部局情報セキュリティ技術責任者に届け出なければならない。

2 機構利用規程第8条第1項に基づき KUINS-IIに機器を接続しようとする者は、あらかじめ接続しようとするサブネットのサブネット連絡担当者の同意を得なければならない。また利用申請時に、接続する機器及びその構成に関する情報を届け出なければならない。KUINS 機器管理責任者は、接続する機器又は構成を変更する際は速やかに変更の届け出をしなければならない。

3 部局情報セキュリティ技術責任者は、当該部局において KUINS-III 情報コンセントの設置を希望する際には、当該情報コンセントの KUINS 情報コンセント管理担当者となる者を指定して、情報環境機構長に申請しなければならない。

4 機構利用規程第8条に基づき KUINS-IIIに機器を接続しようとする者は、あらかじめ当該情報コンセントを所属させようとする VLAN の VLAN 管理責任者の同意を得なければならない。

5 KUINS 接続者が、KUINS に機器を接続する必要がなくなったとき又は利用資格がなくなったときは、遅滞なく情報環境機構長並びに所属する部局の部局情報セキュリティ技術責任者にその旨を届け出なければならない。

6 KUINS 機器管理責任者、KUINS 情報コンセント管理担当者、サブネット連絡担当者並びに VLAN 管理責任者は、情報環境機構長が行う第13条第1項又は第2項の事実の確認及び調査に協力しなければならない。

7 部局情報セキュリティ技術責任者の許可を受けて他の利用者等に KUINS を利用させる（他の利用者等に特定部局情報システムを利用させ、又は他の利用者等の利用者端末を特定部局情報システムに接続して、利用のための通信がKUINS を通過することをいう）際には、KUINS 機器管理責任者又は KUINS 情報コンセント管理担当者は、本規則に定める遵守事項が守られるよう、監督しなければならない。

（統合認証システムへの特定部局情報システム接続及び利用の許可と停止）

第19条 部局情報セキュリティ技術責任者は、統合認証システムに対して、特定部局情報システムを接続する（主体認証を目的として IC カードを利用することを含む、以下同じ）際、利用目的及び接続において提供される情報の利用範囲を明示した上で、情報環境機構長に申請し許可を得なければならない。なお、情報環境機構長があらかじめ指定する範囲においてはこの限りでない。

2　部局情報セキュリティ技術責任者は、前項の接続を行った際には、部局情報セキュリティ責任者に報告しなければならない。

3　情報環境機構長は、前項の申請で許可した接続又はあらかじめ指定する範囲の接続において、個人情報（規程第2条第7号に定めるものをいう）が提供される場合には、当該特定部局情報システムと個人情報の利用目的について、対象となる利用者等に通知又は公表しなければならない。

4　部局情報セキュリティ技術責任者は、統合認証システムの接続について、その必要がなくなった際、遅滞なく情報環境機構長にその旨を届けなければならない。

5　部局情報セキュリティ技術責任者は、統合認証システムの接続によって特定部局情報システムに提供された情報の利用の範囲が、接続の申請時に示した利用目的及び情報の利用範囲を逸脱しないよう必要な措置を講じなければならない。

（情報セキュリティ対策教育の受講）

第20条　利用者は、対策基準第104条第3項に基づき最高情報セキュリティ責任者が定める年度講習計画に従って、情報セキュリティポリシー及び実施規程並びに全学情報システムの利用に関する講習を受講しなければならない。

2　教職員等は、京都大学へ着任時に、前項に定める講習の受講方法について、所属部局の部局情報セキュリティ責任者に確認しなければならない。

3　教職員等は、本人の責めに帰すべきではないと判断される事由により、第1項に定める講習を受講できない場合は、その事由について、部局情報セキュリティ責任者を通じて、速やか全学情報セキュリティ実施責任者に報告しなければならない。

4　全学情報システム臨時利用者又は特定部局情報システム臨時利用者は、情報環境機構長又は利用を許可した部局の部局情報セキュリティ責任者が必要と認めた場合、情報セキュリティポリシー及び実施規程並びに全学情報システムの利用に関する講習を受講しなければならない。

5　最高情報セキュリティ責任者は、対策基準第104条第6項に基づき、第1項及び第4項の講習の受講状況を当該利用者の所属する部局の部局情報セキュリティ責任者へ定期的に報告しなければならない。

6　部局情報セキュリティ責任者は、全学情報セキュリティ委員会が指定する利用者等への講習について、当該利用者等に関する受講の実態を把握するとともに、必要に応じて利用者等へ講習を受けることを指示しなければならない。

（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義務）

第21条　全学情報システムを利用する部局の部局情報セキュリティ技術責任者並びに特定部局情報システムを所管する部局情報システム技術担当者は、部局情報セキュリティ責任者の指示の下、次の各号に掲げる事項を実施しなければならない。

(1)　対策基準第88条第1項に基づいて行う通信の監視

(2)　対策基準第89条第1項に基づく利用記録の採取

(3)　接続した特定部局情報システムが全学情報システムのハードウェア及びソフトウェア等に障害や過度な負荷等を与えないための必要な措置

(4)　情報環境機構長が行う第16条第3項及び第17条第1項の事実の確認及び調査への協力

(5)　全学情報システムの障害及びセキュリティインシデントに対するサービス中断等への協力

（利用者等の責務）

第22条　利用者等は、本学支給以外の情報システムを利用者端末として、全学情報システム並びに特定部局情報システムを利用する際、当該利用者端末に対して、情報環境機構長が別に定める不正プログラム対策ガイドラインに準じた不正プログラム対策を実施するよう努めなければならない。

2　利用者等は、情報環境機構長が行う第16条第3項及び第17条第1項の事実の確認及び調査に協力するよう努めなければならない。

3　利用者等は、第7条から第11条に定める遵守事項に違反すると疑われる行為を発見した場合、並びに、全学情報システム又は特定部局情報システムにおける不正アクセスと被疑される状況その他全学情報システムに関する重大なセキュリティ侵害を認めたときは、速やかに情報環境機構長にその旨を通報するよう努めなければならない。

（雑則）

第23条　本規則に定めるもののほか、全学情報システムの利用に関し必要な事項は情報環境機構長が定める。

附　則

本規則は、平成22年1月12日から施行する。

附　則

本規則は、平成25年2月5日から施行する。

附　則

本規則は、平成27年4月1日から施行する。

附　則

本規則は、平成28年4月1日から施行する。

附　則

本規則は、平成29年4月1日から施行する。