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。以下「規程」という。）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。以下「対策基準」という。）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) 削除

(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）及び規程をいう。

(3) 実施規程　対策基準その他情報セキュリティポリシーに基づき情報基盤担当理事が定める規程、基準及び計画をいう。

(4) 削除

(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号に定めるものをいう。）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。）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、情報環境機構長の承認を得て全学情報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42号に定めるものをいう。）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章に定めるものをいう。)、研究生、研修員等（京都大学研修規程（昭和24年達示第3号）に定めるものをいう。）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　情報環境機構が管理及び運用する全学の情報基盤に基づく学術情報ネットワークシステムをいい、グローバル IP アドレスで運用するネットワーク及びプライベート IP アドレスで運用するネットワークからなるものをいう。

(16) KUINS 機器管理責任者　情報環境機構長が、グローバルIPアドレスで運用するネットワークに機器を接続することを承認した者をいう。

(17) 削除

(18) サブネット連絡担当者　情報環境機構が部局に割り当てたグローバル IP アドレスのサブネットについて、当該部局及び情報環境機構との間の連絡を担当するために、当該部局の部局情報セキュリティ技術責任者が選出する者をいう。

(19) VLAN 管理責任者　情報環境機構長が、プライベート IP アドレスで運用するネットワークに VLAN を割り当てることを承認した者をいう。

(20) 削除

(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号に定めるものをいう。）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。）（以下これらを「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（次号に定めるものをいう。）、統合 LDAP サーバ（第25号に定めるものをいう。）及び IC カード（第28号に定めるものをいう。）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及び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) 削除

(27) 削除

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

(29) 削除

(30) 認証ICカード　京都大学認証ICカード取扱要項（平成22年2月3日情報環境機構長裁定）に基づき常勤・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（第37号に定めるものをいう。）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　認証ICカード又は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22年2月3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 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) 削除

(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) インシデント対応連絡要領　情報セキュリティインシデント対応連絡要領(平成25年2月5日情報セキュリティ実施責任者裁定)をいう。

(39) インシデント　インシデント対応連絡要領第1に定める、規程第3条第1項に定める情報資産に係るインシデント(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、コンピュータウイルス等による被害、情報機器の紛失・盗難等)をいう。

(40) CSIRT　規程第7条第1項に基づき、最高情報セキュリティ責任者の下に設置された情報セキュリティインシデント対応チームをいう。

(41) CSIRT 責任者　京都大学情報セキュリティインシデント対応チーム(CSIRT)要項(平成29年7月6日情報担当理事裁定)第5第1項に基づき置かれたCSIRT責任者をいう。

(42) 特定利用　KUINS への接続が承認された者による KUINS の利用又は全学アカウント若しくはICカードによる主体認証を伴っての全学情報システム若しくは特定部局情報システムの利用をいう。

(43) 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。)

(全学アカウントの発行)

第4条　情報環境機構長は、部局の長の申請に基づき全学アカウントを発行する。

2　全学アカウントの発行及びその利用に関する責任は、当該アカウントの発行を申請した部局の長が負うものとする。

3　全学アカウントの発行対象、有効期限その他の取扱いの方法については、全学アカウント取扱要項(令和5年3月29日情報環境機構長裁定)に従う。

(IC カードの取得)

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。

(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の利用を申請し全学情報システムの利用の許可をされた際、当該許可を受け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。この場合において、許可された全学情報システム臨時利用者に対して、必要と認めたときは、情報セキュリティポリシー及び実施規程の理解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。この場合において、許可した全学情報システム臨時利用者に対して、必要と認めたときは、情報セキュリティポリシー及び実施規程の理解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。この場合において、許可した特定部局情報システム臨時利用者に対して、必要と認めたときは、情報セキュリティポリシー及び実施規程の理解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及び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、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、学内又は学外にかか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 削除

5 削除

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22年2月3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22年2月3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において遵守すべき事項）

第8条　全学アカウントを発行された者は、全学アカウントの利用に際して、全学アカウント利用規約（令和5年3月29日情報環境機構長裁定）を遵守しなければならない。

（IC カード利用において遵守すべき事項）

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すること。

(2) IC カードを他の者に付与又は貸与したり、他の者の IC カードを使用しないこと。

(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すること。

(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すること。ただし、IC 学生証の返還については、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すること。

2　IC学生証について、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。

（全学情報システム等の利用において遵守すべき事項）

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。）を利用してはならない。

2　前項の規定にかかわらず、教育・研究を目的とする場合は、第3条第2項に定める情報システムにおいて、P2P ソフトウェアを利用することができる。ただし、次の各号に掲げる事項を遵守しなければならない。

(1) 情報環境機構が提供するグローバル IP アドレスで運用するネットワークで利用すること。

(2) 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）の許可を得ること。

(3) 部局情報セキュリティ責任者は、前号の許可を与えるにあたっては、情報環境機構長に事前に届け出ること。

（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又は全学情報システム若しくは特定部局情報システムを利用するために本学が支給した利用者端末に対して、当該特定部局情報システム又は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、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　本学が支給したものではない利用者端末を利用する利用者等が所属する部局の部局情報セキュリティ技術責任者は、当該利用者等に対して、京都大学全学情報システム不正プログラム対策ガイドラインに準じた対策を実施す

るよう求めなければならない。

第13条　削除

（IC カードの失効と再発行）

第14条　情報環境機構長は、第7条並びに第9条第1項第2号及び第7号に定める遵守事項に違反した IC カード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し、その旨を該当する IC カード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　削除

5　発行責任組織又は情報環境機構は、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行為若しくは違反すると被疑される行為を認め、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。

（全学情報システムにおけ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インシデントと被疑される状況を認めたとき、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　前項の通知を受けた、最高情報セキュリティ責任者は、直ちに CSIRT 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全学情報システム及び当該特定部局情報システム又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、全学情報システムにおける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 CSIRT へ報告するものとする。

4　第1項のインシデントと被疑される状況への部局構成員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　CSIRT 責任者は、情報環境機構長から全学情報システムにおける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インシデントその他セキュリティ侵害と被疑される状況を認めたときは、直ちに CSIRT に通知しなければならない。

2　CSIRT 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。情報環境機構長は、CSIRT より被害の拡大防止の指示を受けた際は、直ちに被害の拡大防止策を実施するものとする。

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 CSIRT 責任者へ報告するものとする。

4　CSIRT 責任者は、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　前項の遵守事項に違反すると被疑される行為への部局構成員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 機器管理責任者等の義務）

第18条　KUINS 機器管理責任者、サブネット連絡担当者、VLAN 管理責任者及び全学アカウントを用いて全学情報システムに接続する利用者等は、情報環境機構長が行う第16条第3項及び前条第1項の調査及び事実の確認に協力しなければならない。

2　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 VLAN 管理責任者は、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、本学へ着任時に、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及び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、ソフトウェア等に障害、過度な負荷等を与えないために必要な措置

(4)　情報環境機構長が行う第16条第3項及び第17条第1項の調査及び事実の確認への協力

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

2　利用者端末の利用者等が所属する部局の部局情報セキュリティ技術責任者及び利用者端末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、当該利用者端末に関して、次の各号に掲げる事項を実施しなければならない。ただし、利用者端末が本学が支給したものでない場合には、当該利用者端末の利用者等が所属する部局情報セキュリティ技術責任者は、当該利用者等に対して、当該利用者端末に関して次の各号に掲げる事項を実施するように求めなければならない。

⑴ 対策基準第89条第1項に基づく利用記録の採取

⑵ 接続した利用者端末が全学情報システムのハードウェア、ソフトウェア等に障害、過度な負荷等を与えないために必要な措置

⑶ 情報環境機構長が行う第16条第3項及び第17条第1項の調査及び事実の確認への協力

⑷ 接続した全学情報システム又は特定部局情報システムの障害及び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、全学情報システム及び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項の調査及び事実の確認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条までに定める利用者等の遵守事項に違反する行為又は違反すると疑われる行為を発見した場合及び全学情報システム又は特定部局情報システムにおけるインシデントと被疑される状況を認めた場合には、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。

附　則

本規則は、令和2年4月1日から施行する。

附　則

本規則は、令和3年4月1日から施行する。

附　則

本規則は、令和4年10月21日から施行し、令和4年10月1日から適用する。

附　則

本規則は、令和5年4月1日から施行する。