公立大学法人神戸市外国語大学　情報セキュリティポリシー

2008 年 11 月 10 日

規程第 14 号

第１章　情報セキュリティ基本方針

１　目的

公立大学法人神戸市外国語大学（以下「本学」という。）の情報システムが取り扱う情報には，学部生，大学院生，科目等履修生，研究生および教職員の個人情報や運営上重要な情報が多数含まれており，情報資産を人的脅威や災害，事故等様々な脅威から防御することは，プライバシー保護や，質の高い教育研究活動及び適切な大学運営を確保するためにも必要不可欠である。

このため，本学が保有する情報資産の機密性，完全性及び可用性を維持することを目的として公立大学法人神戸市外国語大学情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）を定める。

２　定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム

コンピュータ及びネットワークで構成され，情報処理を行う仕組みをいう。

（３）データ

電子計算機処理に係る入出力帳票，磁気テープ，磁気ディスク，パンチカードその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

（４）情報セキュリティ

情報資産の機密性，完全性及び可用性を維持することをいう。

（５）機密性

情報にアクセスすることを認められた者だけが，情報にアクセスできる状態を確保することをいう。

（６）完全性

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。

（７）可用性

情報にアクセスすることを認められた者が，必要なときに中断されることなく，情報にアクセスできる状態を確保することをいう。

（８）本学構成員

学部生，大学院生，科目等履修生，研究生及び教職員など本学において情報資産

を取り扱うすべての者をいう（以下「本学構成員」という。）。

３　情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは，本学が保有する情報資産に関する情報セキュリティ対策について総合的かつ体系的にまとめられた情報セキュリティ対策の基本となるものであり，情報セキュリティ基本方針及び情報セキュリティ対策基準により構成される。

４　情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は，本学における情報資産及び情報資産に接するすべての本学構成員とする。

また，情報資産の範囲は次のとおりとする。

（１）物理資産

コンピュータ・ネットワーク・記録媒体等物理的な形状を有する資産でありかつ，情報を利用するのに必要な資産

（２）データ資産

データ及び情報システムの設計等に関する情報

（３）ソフトウェア資産

コンピュータ等の情報機器において稼動するプログラム

（４）サービス資産

電源，メールサービス等契約により提供される情報システムに関連する業務

５　本学構成員の義務

本学構成員は，情報セキュリティの重要性について共通の認識を持つとともに，情報資産の利用にあたっては情報セキュリティポリシーを遵守するものとする。

６　情報セキュリティ管理体制

本学の情報資産について，適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

そのために次に掲げるものを置く。

（１）情報セキュリティ最高責任者

理事長の指名する理事を情報セキュリティ最高責任者とする。

（２）部門情報統括責任者

経営企画室長及び専任教員を部門情報統括責任者とする。

（３）情報基盤管理者

経営企画グループ長を情報基盤管理者とする。

（4）情報責任者

総務担当理事，学生担当理事，教務担当理事，学術担当理事を所管する部門の情報責任者とする。

（5）情報管理者

情報資産を取り扱うグループの長を，所管するグループの情報管理者とする。

（6）業務システム責任者

各業務システムを所管する部門の長を，当該業務システムに関する業務システム責任者とする。

（7）業務システム管理者

各業務システムを所管するグループの長を，当該業務システムに関する業務システム管理者とする。

（8）情報監査統括責任者

経営企画室長を情報監査統括責任者とする。

（9）情報管理委員会

情報セキュリティ最高責任者，部門情報統括責任者(専任教員を除く)，情報責任者及び情報最高責任者の指名する教員により構成され，情報セキュリティ対策に関する調整等を行うものとする。

7　情報資産への脅威

情報セキュリティ対策を講じるうえでは，情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に次の脅威については，十分な措置を講じるものとする。

（1）部外者による不正アクセス又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去，機器及び媒体の盗難等

（2）本学構成員等及び部外委託者による意図しない操作，不正アクセス又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去，機器及び媒体の盗難，規定外の端末接続によるデータ漏えい等

（3）地震，落雷，火災等の災害，事故，故障等によるサービス及び業務の停止

8　情報セキュリティ対策

情報資産に対する脅威から情報資産を保護するため，以下の情報セキュリティ対策を講ずるものとする。

（1）情報資産の分類と管理

本学の保有する情報資産を機密性，完全性及び可用性に応じて分類し，当該分類に基づき情報セキュリティ対策を実施することとする。

（2）物理的セキュリティ

コンピュータの設置場所への入退室，サーバ等の管理，通信回線及び端末等への物理的な対策を講じる。

（3）人的セキュリティ

情報セキュリティに関し，すべての本学構成員が遵守すべき事項を定めるとともに，十分な研修・訓練及び啓発を実施するなど人的な対策を講じる。

（4）技術的セキュリティ

コンピュータ等の管理，アクセス制御，コンピュータウィルス等不正アクセス対策等の技術的対策を講じる。

（5）運用面のセキュリティ

情報システムに関し，情報セキュリティポリシーの遵守状況の確認等，情報セキュリティポリシーの運用面の対策を講じる。また，情報資産への侵害が発生した場合等に，迅速かつ適切に対応するため，緊急時対応計画を策定する。

９　情報セキュリティ個別基準の策定

情報セキュリティポリシーを補完するために必要な内容に関して，具体的な内容を定める情報セキュリティ個別基準を策定するものとする。

１０　情報セキュリティ実施手順の策定

情報セキュリティポリシー及び情報セキュリティ個別基準に基づき，情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

１１　情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況を評価するため，定期的及び必要に応じて情報セキュリティ監査及び自己点検を実施する。

１２　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果，情報セキュリティに関する状況の変化等を踏まえ，必要に応じ適宜情報セキュリティポリシーの見直しを行う。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは，情報セキュリティ基本方針に基づき情報セキュリティ対策等を実施するために共通の基準として具体的な遵守事項及び判断基準を定めたものである。

1　権限と責任

情報セキュリティ基本方針で定めた情報セキュリティ管理体制における権限と責任については次のとおりとする。

（1）情報セキュリティ最高責任者

ア　情報セキュリティ最高責任者は，本学における全てのネットワーク，情報システム，データ等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

イ　情報セキュリティ最高責任者は，必要に応じ，情報セキュリティに関する専門的な知識及び経験を有する専門家をアドバイザーとして置くことができる。

（2）部門情報統括責任者

ア　部門情報統括責任者は情報セキュリティ最高責任者を補佐しなければならない。

イ　部門情報統括責任者は，管轄する部門全てのネットワーク，情報システム，データ等の情報資産における開発，設定の変更，運用，見直し等を行う統括的な権限及び責任を有する。

ウ　部門情報統括責任者は，管轄する部門全ての情報資産における情報セキュリティ対策に関する統括的な権限及び責任を有する。

エ　部門情報統括責任者（専任教員は除く。）は，所管する部門情報基盤管理者，情報責任者，情報管理者，業務システム責任者，業務システム管理者に対して，情報セキュリティに関する指導及び助言を行う権限を有する。

オ　部門情報統括責任者は，所管する部門の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に，情報セキュリティ最高責任者の指示に従い，情報セキュリティ最高責任者が不在の場合には自らの判断に基づき，必要かつ十分な措置を行う権限及び責任を有する。

カ　部門情報統括責任者（専任教員は除く。）は，緊急時等の円滑な情報提供を図るため，情報セキュリティ最高責任者，部門情報統括責任者，情報基盤管理者，情報責任者，情報管理者，業務システム責任者，業務システム管理者を網羅する連絡体制を整備しなければならない。

（3）情報基盤管理者

ア 情報基盤管理者は部門情報統括責任者（専任教員は除く。）を補佐し，その実務を担当する。

イ 情報基盤管理者は，本学の共通的なネットワーク，情報システム，データ等の情報資産における開発，設定の変更，運用，見直し等を行う権限及び責任を有する。

ウ 情報基盤管理者は，本学の共通的なネットワーク，情報システム，データ等の情報資産における情報セキュリティ対策に関する権限及び責任を有する。

エ 情報基盤管理者は，本学の共通的なネットワーク，情報システム，データ等の情報

資産に関する情報セキュリティ実施手順を策定し，その維持・管理を行う。

オ 情報基盤管理者は，本学の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合に，情報基盤責任者，部門情報統括責任者（専任教員は除く。），情報セキュリティ最高責任者へ速やかに報告を行い，指示を仰がなければならない。

カ 情報基盤管理者は，本学の共通的なネットワーク，情報システム，データ等の情報資産のうちパーソナルコンピュータ等についての物理的セキュリティに関する管理を情報管理者に行わせることができる。

（4）情報責任者

ア 情報責任者は，所管する部門における情報セキュリティ対策に関する統括的な権限及び責任を有する。

イ 情報責任者は，情報管理者を監督し，所管する部門における緊急時等の連絡体制の整備並びに本学構成員である情報取扱者に対する助言及び指示を行う。

（5）情報管理者

ア 情報管理者は，所管グループ内におけるデータ等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

イ 情報管理者は，情報基盤管理者の指示に従い本学の共通的なネットワーク，情報システム，データ等の情報資産のうち所管組織内のパーソナルコンピュータ等についての物理的セキュリティに関する管理を行う。

ウ 情報管理者は，所管グループ内におけるデータ等の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には，情報基盤管理者，業務システム管理者，情報責任者へ速やかに報告を行い，指示を仰がねばならない。

（6）業務システム責任者

ア 業務システム責任者は，当該業務システムにおける開発，設定の変更，運用，見直し等を行う統括的な権限及び責任を有する。

イ 業務システム責任者は，当該業務システムの情報セキュリティ対策に関する統括的な権限及び責任を有する。

ウ 業務システム責任者は，当該業務システムに関する情報セキュリティ実施手順の維持・管理を行う統括的な権限及び責任を有する。

エ 業務システム責任者は，当該業務システムについて，緊急時等の連絡体制の整備，情報セキュリティポリシーの遵守に関する意見の集約及び本学構成員である情報取扱者に対する助言及び指示を行う。

（7）業務システム管理者

ア 業務システム管理者は，当該業務システムにおける開発，設定の変更，運用，見直し等を行う権限及び責任を有する。

イ 業務システム管理者は，当該業務システムの情報セキュリティ対策に関する権限及

び責任を有する。

ウ 業務システム管理者は，当該業務システムに係る情報セキュリティ実施手順を策定し，その維持・管理を行う。

エ 業務システム管理者は，当該業務システムにおいて情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には，情報基盤管理者，業務システム責任者へ速やかに報告を行い，指示を仰がねばならない。

オ 業務システム管理者は，当該業務システムにおける開発，設定の変更，運用等についての作業を業務システム管理者が指名する者に行わせることができる。

（８）情報監査統括責任者

情報監査統括責任者は，情報セキュリティ監査の計画，実施，報告等を行う権限及び責任を有する。

（９）情報管理委員会

情報管理委員会において，情報セキュリティポリシー等，情報セキュリティに関する重要な事項を審議する。

（１０）兼務の禁止

ア 情報セキュリティ対策の実施において，やむを得ない場合を除き，承認又は許可の申請を行う者とその承認者又は許可者は，同じ者が兼務してはならない。

イ 監査を受ける者とその監査を実施する者は，同じ者が兼務してはならない。

２　情報資産の分類と管理

（１）情報資産の管理責任

ア 管理責任

情報資産は，情報基盤管理者，業務システム管理者及び情報管理者等権限のある者（以下「情報資産管理責任者」という）がそれぞれ所管する情報資産についての管理責任を有する。また，情報資産管理責任者は，当該情報資産の利用範囲を定めなければならない。

イ 本学構成員である情報取扱者の責任

本学構成員である情報取扱者は，情報資産の作成・入手・利用に際しては，十分にその責任を自覚したうえで行わなければならない。

ウ 複製等の管理

データが複製又は送信された場合には，当該複製等も原本と同様に管理しなければならない。

（２）情報資産の分類と管理方法

ア 情報資産の分類

（ア）対象となる情報資産は，各々の情報資産の機密性，完全性及び可用性を踏まえ，次の重要性分類に従って分類する。

機密性

3	本学で取り扱う情報資産のうち，特に機密性を要するもの （次のデータだけではなくそれらが含まれる記録媒体，パーソナルコンピュータ，システム等も同様） ・個人情報に関するデータ ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に本学の信頼を著しく害するおそれのあるデータ ・公開することでセキュリティ侵害が生じるおそれがあるデータ
2	直ちに一般に公表することを前提としていないもの （機密性３には当てはまらないが，広報などは行っていないデータ及びそれらが含まれる記録媒体，パーソナルコンピュータ，システム等）
1	機密性２又は機密性３の情報資産以外のもの

完全性

3	本学で取り扱う情報資産のうち，特に完全性を要するもの （改ざんあるいは誤りがあると学生等の権利が侵害される，又は本学の法人運営の適確な遂行に支障を及ぼす可能性がある） （次のデータだけではなくそれらが含まれる記録媒体，パーソナルコンピュータ，システム等も同様） ・個人情報に関するデータ ・法令の規定により秘密を守る義務を課されているデータ ・部外に知られることが適当でない法人その他団体に関するデータ ・部外に漏れた場合に本学の信頼を著しく害するおそれのあるデータ
2	改ざんあるいは誤りがあると組織に軽微な影響が発生する可能性がある
1	完全性２又は完全性３の情報資産以外のもの

可用性

3	本学で取り扱う情報資産のうち，特に可用性を要するもの （利用できないと学生等の権利が侵害される，又は行政事務の安定的な遂行に支障を及ぼす可能性がある） （次のデータだけではなくそれらが含まれる記録媒体，パーソナルコンピュータ，システム等も同様） ・滅失し又は損傷した場合その復元が著しく困難であるため本学の円滑な運営が妨げられるおそれのあるデータ

2	利用できないことが一定時間以上継続すると学生等の権利が侵害される，又は本学の事務の安定的な遂行に支障を及ぼす可能性がある
1	可用性２又は可用性３の情報資産以外のもの

（イ） 情報資産の機密性，完全性，可用性のいずれかの重要性分類２以上に分類される情報資産は，この対策基準の対象とする。

また，重要性分類１の情報資産も，必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

イ 情報資産に対するリスク分析の実施

（ア） 本学が保有する情報資産に対して，あらかじめ定められた方法に従い，リスク分析を行わなければならない。

（イ） 情報セキュリティ最高責任者は，リスクを受容するための基準を作成し，受容可能なリスクの水準を定めなければならない。

（ウ） リスク分析の結果，リスクの大きさが受容可能なリスクの水準を上回る場合，リスク対応計画書を作成し，情報セキュリティ最高責任者の承認を得たうえで，適切なリスク管理を行わなければならない。リスク対応計画書には，リスク対応を施すための活動内容，資源，責任体制及び優先順位等を記載すること。

（エ） リスク分析及び受容可能なリスクの水準等は，情報セキュリティに関する状況の変化等を踏まえ，定期的に見直しを行うものとする。

ウ 情報資産の管理方法

（ア）情報資産の管理

①情報資産について，第三者が重要性の識別を容易に認識できないよう適切な管理を行わなければならない。

②すべての情報資産を明確に識別し，重要な情報資産に対しては必要に応じて目録を作成して管理しなければならない。

（イ）データの作成

①業務上必要のないデータを作成してはならない。

②データの作成時に重要性分類に基づき，当該データの分類を定めなければならない。

③作成途上のデータについても，紛失や流出等を防止しなければならない。また，データの作成途上で不要になった場合は，当該データを消去しなければならない。

（ウ）情報資産の入手

①本学内の者が作成した情報資産を入手した者は，入手元の情報資産の分類に基づいた取扱いをしなければならない。

②本学外の者が作成した情報資産を入手した者は，重要性分類に基づき，当該情報

の分類を定めなければならない。

③情報資産を入手した者は，入手した情報資産の分類が不明な場合，情報資産管理責任者に判断を仰がなければならない。

（エ）情報資産の利用

①情報資産を利用する者は，情報資産を業務上の目的以外に利用してはならない。

②情報資産の利用においては，情報資産の分類に応じ，利用者並びにアクセス権限を定めなければならない。

③機密性３のデータは，情報資産管理責任者の許可を得た場合，複写，複製，送付，送信を行うことができる。ただし，パスワード等による情報漏えい対策を施さなければならない。

④電子メールにより機密性２のデータを送信する者は，必要に応じパスワード等による情報漏えい対策を施さなければならない。

⑤情報資産を利用する者は，記録媒体に情報資産の分類が異なるデータが複数記録されている場合，最高度の分類に従って，当該記録媒体を取り扱わなければならない。

（オ）情報資産の保管

①情報資産管理責任者は，情報資産の重要性分類に従って，情報資産の保管を適切に行わなければならない。

②最終的に確定したデータを記録した記録媒体は，書込禁止措置を行ったうえで保管しなければならない。

③情報資産管理責任者は，持ち運び可能な記録媒体を，耐火，耐熱，耐水及び耐湿対策を講じたうえ施錠可能な場所への保管等適切な管理を行わなければならない。

④情報資産管理責任者は，情報システムのバックアップで取得したデータを記録する記録媒体を長期保管する場合は，自然災害を被る可能性が低い地域への保管を考慮しなければならない。

⑤機密性２以上の情報資産が保管された記録媒体の搬送にあたっては，必要に応じ鍵付きのケース等に格納し，暗号化又はパスワードの設定を行う等，情報資産の不正利用を防止するための措置を施さなければならない。

⑥機密性２以上の情報資産が保管された記録媒体を運搬する者は，情報資産管理責任者に許可を得なければならない。

（カ）情報資産の提供・公表

①機密性３の情報資産を外部に提供する者は，必要に応じ暗号化又はパスワードの設定を行わなければならない。

②機密性３の情報資産を外部に提供する者は，情報基盤管理者に事前に許可を得たうえで，日時・担当者及び提供概要を記録しなければならない。

③情報資産管理責任者は，公開する情報資産について，完全性を確保しなければならない。

（キ）情報資産の廃棄

①記録媒体が不要となった場合は，当該媒体に含まれるデータの消去を行ったうえで焼却，裁断又は溶解等により復元不可能な状態にして廃棄しなければならない。

②情報資産の廃棄を行う者は，行った処理について，日時，担当者及び処理内容を記録しなければならない。

③情報資産の廃棄を行う者は，情報資産管理責任者の許可を得なければならない。

エ 文書の管理

（ア）情報セキュリティ対策基準を実施していくうえで必要とされる文書は，公立大学法人神戸市外国語大学文書管理規程等の定めに従い管理しなければならない。

（イ）情報セキュリティに係る文書（以下「文書」という）を作成又は更新する場合は，あらかじめ定められた者による承認を受けなければならない。

（ウ）文書は，定期的に見直しを行い，必要に応じて更新しなければならない。

（エ）文書を廃棄する場合は，廃棄文書が誤って使用されないようにしなければならない。ただし，廃棄文書を保持する必要がある場合には，廃棄文書と分かるように適切な識別を施さなければならない。

オ 文書の管理

情報セキュリティ対策基準の効果的運用の証拠を示すために，記録を作成し，適切な管理をしなければならない。

３　物理的セキュリティ

（１）サーバ等の管理

ア 入退室の管理

情報資産管理責任者は，重要性分類３のデータが記録されている記憶媒体の保管場所及びそれを取扱うコンピュータ設置場所の入退室について，適正な管理を行わなければならない。

なかでも，ネットワークの基幹機器及び重要な情報システムを設置し，当該機器の管理及び運用を行う部屋（以下「管理区域」という）については，次の事項に従い厳重な管理を行わなければならない。

（ア）外部からの侵入が容易にできないようにしなければならない。

（イ）施設管理部門と連携して，管理区域から外部に通ずるドアは必要最小限とし，鍵，監視機能，警報装置等によって許可されていない立入りを防止しなければならない。

（ウ）管理区域への入退室は，許可された者のみに制限し，ＩＤカード等による認証及び入退室管理簿の記載による入退室管理を行わなければならない。

（エ）本学構成員である情報取扱者は，管理区域に入室する場合，身分証明書等を携帯し，求めにより提示しなければならない。

（オ）外部からの訪問者が管理区域に入室する場合には，必要に応じて立ち入り区域を制限したうえで，管理区域への入退室を許可された職員が付き添うものとし，外見上職員と区別できる措置を施さなければならない。

（カ）管理区域については，当該システムに関連しないコンピュータ，通信回線装置，記録媒体等を持ち込ませないようにしなければならない。

イ 装置の取付け等

（ア）情報基盤管理者及び業務システム管理者は，ネットワーク機器及び情報システム機器の取付けを行う場合，火災，水害，埃，振動，温度，湿度等の影響を可能な限り排除した場所に設置し，容易に取り外せないよう適切な固定を行う等必要な措置を施さなければならない。

（イ）情報基盤管理者及び業務システム管理者は，システムの停止により，大学事務の執行等に重大な影響を及ぼすおそれがあるものについて二重化等を行い，同一データを保持し，システムの運用が停止しないように努めなければならない。

（ウ）権限のある者以外の者が容易に操作できないように，情報基盤管理者及び業務システム管理者は，利用者のＩＤ，パスワードの設定等の措置を施さなければならない。

ウ 電源

（ア）情報基盤管理者及び業務システム管理者は，サーバ等の機器の電源については，当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

（イ）情報基盤管理者及び業務システム管理者は，落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

エ 配線

（ア）配線の変更，追加については，情報基盤管理者及び業務システム管理者等限られた者の権限とする。

（イ）情報基盤管理者及び業務システム管理者は，施設管理部門と連携し，通信ケーブル及び電源ケーブルの損傷等を防止するために，配線収納管を使用する等必要な措置を施さなければならない。

（ウ）情報基盤管理者及び業務システム管理者は，主要な箇所の通信ケーブル及び電源ケーブルについて，施設管理部門から損傷等の報告があった場合，連携して対応しなければならない。

（エ）情報基盤管理者及び業務システム管理者は，ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

オ 機器等の定期保守及び修理

（ア）情報基盤管理者及び業務システム管理者は，可用性３のサーバ等の機器は，定期保守を実施しなければならない。

（イ）情報基盤管理者，業務システム管理者及び情報管理者は，記憶装置を内蔵する機器を外部の業者に修理させる場合，内容を消去した状態で行わせなければならない。内容を消去できない場合，外部の業者に故障を修理させるにあたり，修理を委託する事業者との間で，守秘義務契約を締結する他，秘密保持体制の確認などを行わなければならない。

カ 消火薬剤及び消防用設備

消火薬剤及び消防用設備等は，機器及び記録媒体に影響を与えるものであってはならない。

キ 敷地外への機器の設置

情報基盤管理者及び業務システム管理者は，大学の敷地外にサーバ等の機器を設置する場合，部門情報統括責任者の許可を得なければならない。また，定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

ク 機器の廃棄等

情報基盤管理者，業務システム管理者及び情報管理者は，機器を廃棄，リース返却等をする場合，機器内部の記憶装置から，すべてのデータを消去の上，復元不可能な状態にする措置を施さなければならない。

ケ 機器等の搬出入

（ア）情報基盤管理者及び業務システム管理者は，機器等を搬入する場合，あらかじめ当該機器等の既存情報システムに与える影響について，職員に確認を行わせなければならない。

（イ）機器等の搬入出には職員が同行する等の必要な措置を施さなければならない。

（２）ネットワークの管理

ア 情報基盤管理者及び業務システム管理者は，学内の通信回線及び通信回線装置を，施設管理部門と連携し，適切に管理しなければならない。また，通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

イ 情報基盤管理者及び業務システム管理者は，通信回線による外部へのネットワーク接続は必要最低限のものに限定し，できる限り接続ポイントを減らさなければならない。

ウ 部門情報統括責任者及び業務システム責任者は，所管する情報システムにおいて機密性３の情報資産を取り扱う情報システムに通信回線を接続する場合，必要なセキュリティ水準を検討の上，適切な回線を選択しなければならない。また，必要に応じ，送受信される情報の暗号化を行わなければならない。

エ ネットワークに使用する回線は送信途上においてデータの破壊，盗聴，改ざん，消

去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。

（３）端末等の管理

ア 情報基盤管理者，業務システム管理者及び情報管理者は，執務室の端末等について，盗難防止のため，ワイヤーによる固定等の物理的措置を講じなければならない。

イ 情報基盤管理者及び業務システム管理者は，情報システムへのログインパスワードの入力を必要とするように設定しなければならない。また，必要に応じてＢＩＯＳパスワード，ハードディスクパスワード等を併用しなければならない。

ウ 情報基盤管理者及び業務システム管理者は，パスワード以外にＩＤカード等による認証を併用しなければならない。

エ 情報基盤管理者及び業務システム管理者は，端末のディスクデータの暗号化等の機能を有効にしなければならない。

４　人的セキュリティ

（１）本学構成員の責務

ア 情報セキュリティポリシー等の遵守義務

本学構成員は，情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守しなければならない。また，情報セキュリティ対策について不明な点，遵守することが困難な点がある場合には，情報管理者等権限のある者に相談し，指示を仰がなければならない。

イ 法令等の遵守義務

本学構成員は，職務の遂行において使用する情報資産を保護するために，法令等を遵守しこれに従わなければならない。

・不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
・著作権法（昭和 45 年法律第 48 号）
・個人情報の保護に関する法律（平成 15 年法律第 57 号）
・神戸市個人情報保護条例（平成９年 10 月条例第 40 号）
・職員就業規則（平成 19 年４月規程第９号）
・文書管理規程（平成 19 年４月規程第 96 号）

ウ 指示に基づいた情報資産の利用等

職員等情報取扱者は，情報管理者等権限のある者の指示等に従い，情報資産を利用するとともに，開発，設定の変更，運用，更新等の作業を行う。

エ 個人所有の情報資産の持ち込み禁止

職員等情報取扱者は，個人の所有するパーソナルコンピュータ及び記録媒体等の持ち込みをしてはならない。ただし，情報セキュリティ最高責任者の許可を得た場合はこの限りではない。

オ 情報資産の持ち出し及びＷｅｂサイト等による送信禁止

職員は情報資産を取り扱う場合，次の行為を行ってはならない。

①学外への持ち出し

ただし，合理的理由のある場合，情報管理者等管理権限のある者の許可を得た場合に限り，記録を作成したうえで学外への持ち出しができるものとする。教員については，別途定める手順に従うものとする。

②所属外への持ち出し

ただし，情報資産のバックアップ等，合理的理由のある場合，かつ情報管理者等管理権限のある者の許可を得た場合に限り，記録を作成したうえで所属外への持ち出しができるものとする。

③Ｗｅｂサイト等を利用した外部への送信

ただし，公開しているデータ及び情報管理者等管理権限のある者の許可を得た国・県・市への報告等は除くものとする。

カ 業務目的外の利用禁止

職員等情報取扱者は，業務目的以外でのパーソナルコンピュータ等の利用，情報システムへのアクセス，電子メールの利用及びインターネットへのアクセス等を行ってはならない。

キ 端末等の利用

（ア）職員等情報取扱者は，端末のソフトウェアに関するセキュリティ機能の設定を情報基盤管理者又は業務システム管理者の許可なく変更してはならない。

（イ）職員等情報取扱者は，端末や記録媒体，データが印刷された文書等について，第三者に使用されること，又は情報管理者等管理権限のある者の許可なく情報を閲覧されることがないように，離席時の端末のロックや記録媒体，文書等の容易に閲覧されない場所への保管等，適切な措置を講じなければならない。

ク 執務室外における情報処理作業の制限

（ア）部門情報統括責任者は，機密性２以上，可用性３，完全性３の情報資産を執務室外で処理する場合における安全管理措置を定めなければならない。

（イ）職員等情報取扱者は，執務室外で情報処理作業を行う場合には，情報管理者等管理権限のある者の許可を得なければならない。

（ウ）職員等情報取扱者は，執務室外で情報処理作業を行う際，個人の所有するパーソナルコンピュータによる情報処理を行ってはならない。

ケ 異動，退職時等の遵守義務

職員等情報取扱者は，異動，退職等により業務を離れる場合には，利用していた情報資産を，返却しなければならない。また，その後も業務上知り得た情報を漏らしてはならない。

コ 人材派遣職員等

人材派遣職員および非常勤嘱託職員が情報資産を取り扱う必要が生じた場合は，情報管理者等管理権限のある者は従事させる事務の範囲を指定する。また，人材派遣職員および非常勤嘱託職員は「４．人的セキュリティ（１）職員等の責務」のア～ケに定める事項を守らなければならない。

（２）研修・訓練

ア 本学構成員に対する研修・訓練の実施

情報セキュリティ最高責任者は，定期的に本学構成員に対する情報セキュリティに関する研修・訓練を実施させなければならない。

イ 研修計画の策定及び実施

（ア）部門情報統括責任者は，本学構成員に対する情報セキュリティに関する研修計画を定期的に策定し，情報管理委員会に報告しなければならない。

（イ）本学構成員を対象とする情報セキュリティに関する研修を毎年度最低１回実施しなければならない。

（ウ）新規採用の職員を対象とする情報セキュリティに関する研修を実施しなければならない。

（エ）研修は，部門情報統括責任者，情報基盤管理者，情報責任者，情報管理者，業務システム責任者，業務システム管理者及びその他の本学構成員に対して，それぞれの役割，情報セキュリティに関する理解度等に応じたものにしなければならない。

（オ）部門情報統括責任者は，毎年度１回，情報管理委員会に対して，情報セキュリティに関する研修の実施状況について報告しなければならない。

（３）事故等の報告・分析等

ア 事故等の報告

（ア）本学構成員は，情報セキュリティに関する事件・事故，システム上の欠陥及び誤動作を発見した場合，若しくは外部から報告を受けた場合，速やかに情報管理者又は業務システム管理者等権限のある者に報告しなければならない。

（イ）報告を受けた情報管理者又は業務システム管理者等権限のある者は，速やかに情報基盤管理者に報告しなければならない。

（ウ）情報管理者は，報告のあった事故等について，必要に応じて情報責任者に報告しなければならない。

（エ）業務システム管理者は，報告のあった事故等について，必要に応じて情報システム責任者に報告しなければならない。

（オ）情報基盤管理者は，報告のあった事故等について，必要に応じて部門情報統括責任者及び情報セキュリティ最高責任者に報告しなければならない。

イ 事故等の分析・記録等

事故等を引き起こした部門の情報管理者又は業務システム責任者は，情報基盤管理者と連携し，これらの事故等を分析し，記録を保存しなければならない。

（４）アクセスのための認証情報及びパスワードの管理

ア ＩＤ等の管理

（ア）情報基盤管理者及び業務システム管理者等権限のある者はＩＤ等の適正な管理を行わなければならない。

（イ）本学構成員は，次の事項を遵守しなければならない。

①ＩＤ等は，本学構成員間で共有しない。ただし，所属等ごとに配布されたＩＤ等については除く。

②ＩＤ等を紛失した場合には，速やかに情報基盤管理者及び業務システム管理者等権限のある者に通報し，指示を仰ぐ。

③情報基盤管理者及び業務システム管理者等権限のある者は，通報があり次第速やかに当該ＩＤ等を使用したアクセス等を停止する。

イ ＩＤの管理

①本学構成員は，他人に自己が利用しているＩＤを利用させてはならない。

②共用ＩＤを利用する場合は，共用ＩＤの利用者以外に利用させてはならない。

ウ パスワードの管理

（ア）職員等情報取扱者は，自己のパスワードに関し，次の事項を遵守しなければならない。

①パスワードは秘密にし，パスワードの照会等には一切応じない。

②情報システム又はパスワードに対する危険のおそれがある場合には，情報基盤管理者及び業務システム管理者等権限のある者に速やかに報告し，パスワードを速やかに変更する。

③原則として，パスワードを記載したメモを作成しない。やむを得ず作成する場合は，他人に分からない場所に保管する。

④パスワードは十分な長さとし，文字列は想像しにくいものとする。

⑤パスワードは定期的又はアクセス回数に基づいて変更し，古いパスワードを再利用しない。

⑥複数の情報システムを扱う場合は，同一のパスワードを複数のシステムで用いない。

⑦暫定パスワードは，最初のログイン時に変更する。

⑧パーソナルコンピュータ等のパスワードの記憶機能を利用しない。

⑨職員等情報取扱者の間でパスワードを共有しない。

（イ）情報基盤管理者及び業務システム管理者は，パスワードの照会等には一切応じてはならない。

（５）外部委託に関する管理

ア 契約書の記載事項

（ア）ネットワーク及び情報システムの開発・保守並びにデータ処理その他情報処理に係る業務を外部委託する場合は，当該委託先事業者との間で，下記事項を明記した契約を締結しなければならない。

①データその他業務上知り得た情報（以下「データ等」という）の秘密の保持に関する事項

②第三者への委託の禁止又は制限に関する事項

③データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項

④データ等の複写及び複製の禁止に関する事項

⑤データ等の取扱いに関する事故の発生時における報告義務に関する事項

⑥データ等の取扱いに関する検査の実施に関する事項

⑦契約に違反した場合における契約の解除及び損害賠償に関する事項

⑧委託業務終了時の資産の返還，廃棄に関する事項

⑨情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項

⑩事故時等の公表に関する事項

⑪委託先の責任者，委託内容，作業者，作業場所の特定に関する事項

（イ）前項に加えて，次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。

①提供されるサービスレベルの保証に関する事項

②従業員に対する研修の実施に関する事項

③委託業務の定期報告及び緊急時報告義務に関する事項

④外部施設等への搬送時における盗聴，不正コピー等の防止に関する事項

イ セキュリティ確保への取組み状況等の調査

情報基盤管理者及び業務システム管理者は，当該委託先事業者のセキュリティ確保への取組み状況，情報セキュリティマネジメントシステムに係る認証取得の状況，個人情報保護に関する取組み状況の調査を行うとともに，契約締結後においても，定期的若しくは随時，調査を行い，安全の確保に努めなければならない。情報基盤責任者から内容の報告を求められた場合には，報告を行わなければならない。

ウ 再委託

再委託を受ける事業者がある場合，「４．人的セキュリティ（５）外部委託に関する管理」のア，イに定める事項は再委託を受ける事業者にも適用する。

５　技術的セキュリティ

（１）コンピュータ及びネットワークの管理

ア データの保存

データの保存については，情報基盤管理者等管理権限のある者の定める方法により保存を行わなければならない。

イ ファイルサーバの設定等

情報基盤管理者がデータを共有するためのファイルサーバを設置する場合には，次の事項を守らなければならない。なお，教育研究用のファイルサーバについては，別途定める。

（ア）職員，人材派遣職員及び非常勤嘱託職員が使用できるファイルサーバの容量を設定し，職員，人材派遣職員及び非常勤嘱託職員に周知しなければならない。

（イ）ファイルサーバを所属等の単位で構成し，職員，人材派遣職員及び非常勤嘱託職員が他所属等のフォルダ及びファイルを閲覧及び使用できないように，設定しなければならない。

（ウ）特定の職員，特定の人材派遣職員及び特定の非常勤嘱託職員のみが取扱う権限を持つデータについては，同一所属であっても，権限のない者が閲覧及び使用できないよう設定しなければならない。

ウ アクセス記録の取得等

（ア）情報基盤管理者及び業務システム管理者は，アクセス記録及び情報セキュリティの確保に必要な記録を取得し，窃取，改ざん，誤消去等を防止する措置を施したうえで一定期間保存する。また，不正アクセスの兆候を発見するために定期的にそれらを分析することとする。

（イ）情報基盤管理者及び業務システム管理者は，システムから自動出力したアクセス記録等について，必要に応じ，外部記録媒体にバックアップしなければならない。

エ 仕様書の保管

情報基盤管理者及び業務システム管理者は，ネットワーク構成図，情報システム仕様書等に関し，記録媒体の形態に関わらず，業務上必要とするもの以外の者が閲覧したり，紛失したりすることがないよう，適切な保管をしなければならない。

オ 情報資産のバックアップ

情報基盤管理者及び業務システム管理者は，必要なものはサーバの二重化対策実施の有無に関わらず，定期的に情報資産のバックアップのための対応を行うものとする。

カ 他団体との情報システムに関する情報等の交換

情報基盤管理者及び業務システム管理者は，他の団体と情報システムに関する情報及びソフトウェアを交換する場合，その取扱いに関する事項をあらかじめ定め，部門情報統括責任者(教員は除く。)及び業務システム責任者の許可を得なければならない。

キ 通信回線によるデータの送信

情報基盤管理者及び業務システム管理者は，通信回線によりデータを送信する場合，専用通信回線を使用する，送信するデータを必要最小限にする等データの保護のために適切な措置を講じなければならない。

ク 外部の者が利用するシステム

情報基盤管理者及び業務システム管理者は，インターネット等により外部の者が利用できるシステムにおいては，必要に応じ他のネットワーク及び情報システムと物理的もしくは論理的に分ける等，情報セキュリティ対策について特に強固に対策をとらなければならない。

ケ Ｗｅｂサイトでの情報公開時の注意事項

情報基盤管理者及び業務システム管理者は，Ｗｅｂサイトにより情報を公開・提供する場合に，当該サイトに係るシステムにおいて情報の漏えい・改ざん・消去，踏み台，ＤｏＳ攻撃等を防止しなければならない。また，メールシステムを含め各業務システムにおいても，他のシステムに対する攻撃の踏み台とならないようにコンピュータウイルス対策など適切な管理をしなければならない。

コ 無線ＬＡＮの制限的利用

職員等情報取扱者は，本学の管理するネットワーク（以下「内部ネットワーク」という）において，原則として，無線ＬＡＮを利用した接続又は端末等の無線機能を利用した端末間通信を行ってはならない。ただし，利用にあたってセキュリティ確保のための必要な対策を講じ，所定の手続きにより情報基盤管理者の許可を得た場合には，この限りでない。

サ 無許可ソフトウェアの導入等の禁止

（ア）職員等情報取扱者は，各自に供与された端末に対して，情報基盤管理者が定めるもの以外のソフトウェアの導入を行ってはならない。ただし，業務を円滑に遂行するために必要なソフトウェアについては，情報基盤管理者の許可を得た場合に限り，利用することができる。

（イ）職員等情報取扱者は，不正にコピーしたソフトウェアを導入又は使用してはならない。

シ 機器構成の変更の禁止

職員等情報取扱者は，ネットワーク及び各自に供与された端末等に対して，端末及びその他機器の増設又は改造を行ってはならない。合理的な理由があり，業務を円滑に遂行するためにモデム，ルータ等の機器を増設して他の環境（インターネット等）へのネットワーク接続を行うことや，学外からのアクセスを可能とする仕組みを構築しなければならない場合は，部門情報統括責任者の許可を必要とする。軽微な機器の増設の場合は，情報基盤管理者等権限のある者の許可を必要とする。

ス 電子メール

（ア）電子メールの利用を希望する事務職員は，各グループ係長が利用者を特定し，各グループ長を経由してメールアドレスの取得を申請するものとする。

（イ）電子メールの利用を希望する教員その他事務職員以外の本学構成員は，経営企画グループ情報メディア班を経由してメールアドレスの取得を申請するものとす

る。

（ウ）部門情報統括責任者は，電子メールの送受信容量の上限を設定し，上限を超える電子メールの送受信を不可能にしなければならない。

（エ）部門情報統括責任者は，電子メールに添付されるファイルについて，セキュリティ上問題があると思われるファイルについては，送受信を制限できるようにしなければならない。

（エ）メールアドレス保有者は，業務上必要のない送信先に電子メールを送信してはならない。

（オ）メールアドレス保有者は，複数のあて先に電子メールを送信する場合，必要がある場合を除き他の送信先の電子メールアドレスがわからないようにしなければならない。

（カ）メールアドレス保有者は，重要な電子メールを誤送信した場合，情報管理者及び情報基盤管理者に報告しなければならない。

セ 電子署名・暗号化

（ア）職員等情報取扱者は，情報資産の分類により定めた取扱制限に従い，外部に送るデータの機密性又は完全性を確保することが必要な場合には，部門情報統括責任者が定める電子署名，暗号化又はパスワード設定等の方法を用いて，送信しなければならない。

（イ）職員等情報取扱者は，暗号化を行う場合に部門情報統括責任者が定める以外の方法を用いてはならない。また，部門情報統括責任者が定める方法で暗号のための鍵を管理しなければならない。

ソ 無許可端末の接続禁止

職員等情報取扱者は，情報基盤管理者等権限のある者の許可なく端末等をネットワークに接続してはならない。

タ 利用可能なネットワークプロトコル

職員等情報取扱者が利用できるネットワークプロトコルは，業務上必要最低限のものとする。

チ 障害記録

情報基盤管理者及び業務システム管理者は，職員等情報取扱者からのシステム障害の報告，システム障害に対する処理結果又は問題等を障害記録として体系的に記録し，適切に保存しなければならない。

（２）アクセス制御

ア 利用者の識別及び認証

情報基盤管理者及び業務システム管理者は，所管するネットワーク又は情報システムに権限がない職員等情報取扱者がアクセスすることが不可能となるように，利用者の識別及び認証等適切な対応を行わなければならない。

イ 利用者登録

（ア）情報基盤管理者及び業務システム管理者は，利用者の登録，変更，抹消，登録した情報資産の管理，異動，出向及び退職時における利用者ＩＤの取扱い等については，定められた方法に従って行わなければならない。

必要な利用者登録・変更・抹消は，情報基盤管理者及び業務システム管理者に対する申請により行う。ただし，所属等ごとに配布されたＩＤ等については除く。

（イ）情報基盤管理者及び業務システム管理者は，利用されていないＩＤが放置されないよう，点検しなければならない。

（ウ）情報基盤管理者及び業務システム管理者は，ＩＤに割り当てているアクセス権の正当性を確保するために，定められた方法に従って点検しなければならない。

ウ 特権管理等

（ア）情報基盤管理者及び業務システム管理者は，管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし，当該ＩＤのパスワードの漏えい等が発生しないよう，当該ＩＤ及びパスワードを厳重に管理しなければならない。

（イ）情報基盤管理者及び業務システム管理者の特権を代行する者は，当該管理者が指名し，部門情報統括責任者が認めた者でなければならない。

（ウ）情報基盤管理者及び業務システム管理者は，特権を付与されたＩＤ及びパスワードの変更について，原則として外部委託事業者に行わせてはならない。

（エ）情報基盤管理者及び業務システム管理者は，特権を付与されたＩＤ及びパスワードについて，職員等情報取扱者の端末等のパスワードと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。

（オ）情報基盤管理者及び業務システム管理者は，特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

エ ネットワークにおけるアクセス制御

情報基盤管理者及び業務システム管理者は，アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また，ネットワークサービスを利用する権限を有しない職員等情報取扱者が当該サービスを利用できるようにしてはならない。

オ 強制的な接続制御，経路制御

（ア）情報基盤管理者及び業務システム管理者は，不正アクセスを防止するため，適切なネットワーク経路制御を施さなければならない。

（イ）情報基盤管理者及び業務システム管理者は，フィルタリング及びルーティングについて，設定の不整合が発生しないように，ファイアウォール，ルータ等に搭載されている通信ソフトウェア等を設定しなければならない。

カ 無人状態にある装置の管理

情報基盤管理者及び業務システム管理者は，サーバ又は端末等の装置が無人の状態

になる場合，適切なセキュリティ対策を施さなければならない。

キ 外部からのアクセス

（ア）外部からのアクセスの許可は，合理的理由を有する必要最低限のものに限定しなければならない。

（イ）内部のネットワーク及び情報システムへのアクセス方法及び使用方法等は，通信途上の機密性及び利用者の真正性が確保できるものでなければならない。

（ウ）職員等情報取扱者は，外部から持ち帰ったパーソナルコンピュータ等の端末を内部ネットワークに接続する前に，コンピュータウィルスに感染していないこと等を確認しなければならない。

ク 内部ネットワーク間の接続

情報基盤管理者及び業務システム管理者は，他の内部ネットワークとの接続については，情報資産に影響が生じないことを確認し，それぞれの情報システムの責任範囲を明確にしたうえで，接続しなければならない。

なお，接続しようとするときは，あらかじめ部門情報統括責任者に協議しなければならない。

ケ 外部ネットワークとの接続

（ア）情報基盤管理者及び業務システム管理者は，外部ネットワークとの接続にあたり，当該外部ネットワークのネットワーク構成，機器構成，セキュリティ技術等を詳細に調査し，本学の情報資産に影響が生じないことを確認したうえで，部門情報統括責任者の許可に基づき接続しなければならない。

（イ）情報基盤管理者及び業務システム管理者は，接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。情報基盤管理者及び業務システム管理者は，当該外部ネットワークの瑕疵により本学のデータの漏えい，破壊，改ざん又はシステムダウン等による業務への影響が生じた場合に対応するため，必要に応じて当該外部ネットワークの管理責任者による損害賠償責任を契約上担保するよう努めなければならない。

（ウ）接続した外部ネットワークのセキュリティに問題が認められ，本学の情報資産に脅威が生じるおそれがある場合には，情報基盤管理者及び業務システム管理者は当該外部ネットワークとの接続を物理的に遮断することができるものとする。

コ ネットワーク機器の自動識別

情報基盤管理者及び業務システム管理者は，本学で使用されるネットワーク機器について，機器固有情報等によって端末とネットワークとのアクセスの可否が自動的に識別されるように必要に応じてシステムを設定しなければならない。

サ ログイン試行回数の制限等

情報基盤管理者及び業務システム管理者は，ログイン試行回数の制限及びアクセスタイムアウトの設定等により，正当なアクセス権を持たない大学構成員が利用できな

いようにシステムを設定するよう考慮しなければならない。

シ パスワードに関する情報の管理

（ア）情報基盤管理者及び業務システム管理者は，大学構成員のパスワードに関する情報を厳重に管理しなければならない。また，大学構成員のパスワードを発行する場合において，暫定パスワードを発行する場合，ログイン後直ちに暫定パスワードを変更させなければならない。

（イ）情報基盤管理者及び業務システム管理者は，パスワードファイルを不正利用から保護するため，オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は，これを活用しなければならない。

（ウ）情報基盤管理者及び業務システム管理者は，暫定パスワードも含めパスワードを発行する場合，パスワードの長さは十分な長さとし，文字列は他者が想像しにくいものとする。

（エ）情報基盤管理者及び業務システム管理者は，パスワードは定期的又は一定のアクセス回数経過後に変更しなければならない。その場合には古いパスワードの再利用は行わないようにしなければならない。

（３）システム開発，導入，保守等

ア 情報システムの調達

（ア）情報基盤管理者及び業務システム管理者は，情報システムの調達にあたっては，一般に公開する調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

（イ）情報基盤管理者及び業務システム管理者は，機器及びソフトウェアの調達にあたっては，当該製品のセキュリティ機能を調査し，情報セキュリティ上問題のないことを確認しなければならない。

イ 情報システムの開発等

（ア）情報基盤管理者及び業務システム管理者は，ネットワーク及び情報システムの開発，導入，更新及び運用保守にあたっては，次の事項を定める。

①責任者及び監督者

②作業者及び作業範囲

③開発するシステムと運用中のシステムとの分離

④開発・保守に関する設計仕様などの成果物の提出

⑤セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止

⑥アクセス制限

⑦機器の搬入出の際の許可及び確認

⑧記録の提出義務

⑨仕様書・マニュアル等の定められた場所への保管

⑩情報システムに係るソースコードの適切な方法での保管

⑪開発・保守を行った者の利用者ＩＤ，パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消

ウ 情報システムの移行

（ア）情報基盤管理者及び業務システム管理者は，システム開発・保守計画の策定時に情報システムの移行手順を明確にしなければならない。また，移行の際，情報システムに記録されているデータの保存を確実に行い，移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（イ）情報基盤管理者及び業務システム管理者は，新たに情報システムを導入する際には，既に稼働している情報システムに接続する前に，十分な試験を行わなければならない。また，既存のシステムを更新する際には，既に稼働している情報システムとの連携において，十分な試験を行わなければならない。

（ウ）情報基盤管理者及び業務システム管理者は，擬似環境による動作確認後に情報システムの移行を行わなければならない。また，作業については，作業経過を確認しながら実施するとともに，作業内容を記録しなければならない。

（エ）情報基盤管理者及び業務システム管理者は，原則として個人情報及び機密性の高い生データを，試験データに使用してはならない。ただし，合理的な理由がある場合で，部門情報統括責任者が許可した場合は，この限りではない。

（オ）情報基盤管理者及び業務システム管理者は，試験に使用したデータ及びその結果を一定期間厳重に管理しなければならない。

エ 情報システムの入出力データ

（ア）情報基盤管理者及び業務システム管理者は，情報システムに入力されるデータについて，範囲，妥当性のチェック機能及び不正な文字列等の入力を除去する機能を必要に応じて組み込むように情報システムを設計しなければならない。

（イ）情報基盤管理者及び業務システム管理者は，内部処理において誤ったデータに書き換えられる等の可能性がある場合に，書き換え等を検出するチェック機能を組み込むように情報システムを設計しなければならない。

（ウ）情報基盤管理者及び業務システム管理者は，情報システムから出力されるデータは，保存された情報の処理が正しく反映され，出力されるように情報システムを設計しなければならない。

オ ソフトウェアの保守及び更新

情報基盤管理者及び業務システム管理者は，ソフトウェア等を更新，又は修正プログラムを導入する場合，不具合及び他のシステムとの相性の確認を行い，計画的に更新し又は導入しなければならない。

また，情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては，情報基盤管理者及び業務システム管理者は，速やかに対応を行わなければな

らない。

カ 委託業務従事者の身分確認

情報基盤管理者及び業務システム管理者は，作業前に委託業務従事者に対して身分証明書の提示を求め，契約で定められた資格を有するものが作業に従事しているか確認をすることができるようにしておかなければならない。

キ 作業の確認

契約により操作を認められた委託業務従事者が重要なシステム変更等の作業を行う場合は，２名以上で作業し，互いにその作業を確認しなければならない。

ク 作業管理記録

情報基盤管理者及び業務システム管理者は，担当するシステムにおいて行ったシステム変更等の作業については，作業記録を作成しなければならない。作成した作業記録は，窃取，改ざん等をされないように適切に管理を行わなければならない

（４）コンピュータウイルス等不正プログラム対策

ア 情報基盤管理者の実施事項

情報基盤管理者は，次の事項を実施しなければならない。

（ア）コンピュータウイルス等の情報について本学構成員に対する注意喚起を行う。

（イ）常時コンピュータウイルス等に関する情報収集に努める。

（ウ）コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たせるよう指導等を行う。

イ 情報基盤管理者等の実施事項

情報基盤管理者，業務システム管理者及び情報管理者は，次の事項を実施しなければならない。

（ア）所管するサーバ及び端末に，コンピュータウイルス等対策ソフトウェアを常駐させる。

（イ）情報システムにおいてフロッピィディスク等の記録媒体を使用する場合，本学が管理しているものを本学構成員に使用させるとともに，当該媒体の使用にあたり，ウイルスチェックを行わせる。

（ウ）コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保つ。

ウ 職員等情報取扱者の遵守事項

職員等情報取扱者は，次の事項を遵守しなければならない。

（ア）端末において，コンピュータウイルス等対策ソフトウェアが導入されている場合は，当該ソフトウェアの設定を変更しない。

（イ）外部ネットワーク及びフロッピィディスク等の記録媒体からデータ又はソフトウェアを取り入れる際には，必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

（ウ）外部ネットワーク及びフロッピィディスク等への記録媒体へデータ又はソフトウェアを送信・書き込みする際には，必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

（エ）差出人が不明な電子メール又は不自然なファイルが添付された電子メールを受信した場合は速やかに削除する。

（オ）端末に対して，コンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い，スキャンの実行を途中で止めない。

（カ）情報セキュリティ管理者が提供するコンピュータウイルス等の情報を常に確認する。

（キ）添付ファイルのあるメールを送受信する場合は，コンピュータウイルス等対策ソフトウェアでチェックを行う。

（ク）コンピュータウイルス等に感染した場合は，ＬＡＮケーブルの即時取り外し又は機器の電源遮断を行う。

エ 専門家の支援体制

部門情報統括責任者は，実施しているコンピュータウイルス等対策では不十分な事態が発生した場合に備え，外部の専門家の支援を受けられるようにしておかなければならない。

（５）不正アクセス対策

ア 使用されていないポートの閉鎖等

情報基盤管理者及び業務システム管理者は，不正なアクセスによる影響を防止するための必要な措置を講じなければならない。

（ア）使用されていないポートを閉鎖する。

（イ）不正アクセスによるデータの書換えを検出し，Ｗｅｂサイトの改ざんを防止する。

（ウ）ソフトウェアにセキュリティホールが発見された場合は，速やかに修正プログラムを適用する。

イ 攻撃の予告

情報基盤管理者及び業務システム管理者は，攻撃の予告等サーバ等に不正アクセスを受けることが明白な場合には，システムの停止，他のネットワークとの切断などの必要な措置を講じなければならない。

また，各関係機関との連絡を密にして情報の収集に努めなければならない。

ウ 記録の保存

情報セキュリティ最高責任者及び部門情報統括責任者は，不正アクセス行為の禁止等に関する法律違反等犯罪の可能性がある不正アクセスを受けた場合，不正アクセスの記録の保存に努めるとともに，警察・関係機関との緊密な連携に努めなければならない。

エ 内部からの攻撃

情報基盤管理者及び業務システム管理者は，職員等情報取扱者が使用している端末からの学内のサーバ等に対する不正アクセスや外部のサイトに対する不正アクセスを監視しなければならない。

オ 職員等による不正アクセス時の措置

職員等情報取扱者による不正アクセスがあった場合，情報基盤管理者及び業務システム管理者は，当該職員等情報取扱者が所属するグループの情報管理者に通知し，適切な措置を求めなければならない。

（6）セキュリティ情報の収集

情報基盤管理者は，セキュリティホール等のセキュリティに関する情報を収集し，必要に応じ関係者間で情報を共有しなければならない。

6　運用面のセキュリティ

（1）情報システムの監視

ア 事象の検知

情報基盤管理者及び業務システム管理者は，セキュリティに関する事象を検知するため，情報システムの監視を行わなければならない。

イ 時刻同期

情報基盤管理者及び業務システム管理者は，重要なアクセスログ等を取得するサーバの正確な時刻設定又はサーバ間の時刻同期ができる措置を施さなければならない。

ウ 常時監視

情報基盤管理者及び業務システム管理者は，外部と接続するシステムを稼働中，常時監視しなければならない。

（2）情報セキュリティポリシー等の遵守状況の確認及び対処

情報基盤管理者，業務システム管理者及び情報管理者は，所管の範囲において情報セキュリティポリシー及びこれに基づく文書の遵守状況について常に確認を行い，問題を認めた場合には速やかに情報基盤管理者に報告しなければならない。情報基盤管理者は，発生した問題について，適切かつ速やかに対処しなければならない。

（3）運用管理における留意点

ア 調査権限のある職員の指名

部門情報統括責任者は，情報漏えい，不正アクセス，コンピュータウイルス等の調査のために，パーソナルコンピュータ，記録媒体，アクセス記録及びメール等の情報を調査する権限を有する職員を指名する。

イ セキュリティポリシー等の閲覧

情報基盤管理者，業務システム管理者及び情報管理者は，職員，人材派遣職員及び非常勤嘱託職員が常に情報セキュリティポリシー及びこれに基づく文書を参照できる

よう配慮しなければならない。

ウ 管理者権限

情報基盤管理者，業務システム管理者及び情報管理者の権限を代行する者は，それぞれが指名する。

エ 職員等の報告義務

（ア）職員等情報取扱者は，情報セキュリティポリシーに対する違反行為を発見した場合，直ちに情報基盤管理者及び情報管理者に報告を行わなければならない。

（イ）違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると部門情報統括責任者が判断した場合は，緊急時対応計画に従って適切に対処しなければならない。

（４）緊急時の対応

ア 緊急時対応計画の策定

部門情報統括責任者及び業務システム責任者は，情報資産への重大な侵害が発生した場合又は発生するおそれがある場合において，連絡，証拠保全，被害拡大の防止，復旧，再発防止等の措置を迅速かつ適切に実施するために，緊急時対応計画を策定しなければならない。

イ 緊急時対応計画に盛り込むべき内容

緊急時対応計画には，次の内容を定めなければならない。

（ア）関係者の連絡先

（イ）意思決定の所在

（ウ）発生した事象に係る報告すべき事項

（エ）発生した事象への対応措置

（オ）再発防止措置の策定

ウ 緊急時対応計画の見直し

部門情報統括責任者及び業務システム責任者は，情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ，必要に応じて緊急時対応計画を見直さなければならない。

（５）例外措置

ア 例外措置の許可

情報基盤管理者，業務システム管理者及び情報管理者は，情報セキュリティポリシーを遵守することが困難な状況で，大学事務の適正な遂行を継続するため，遵守事項とは異なる方法を採用し，又は遵守事項を実施しないことについて合理的な理由がある場合には，情報セキュリティ最高責任者の許可を得て，例外措置を取ることができる。

イ 緊急時の例外措置

情報基盤管理者，業務システム管理者及び情報管理者は，前項に該当する場合であ

って，大学事務の遂行に緊急を要し，情報セキュリティ最高責任者の許可を得る時間的な猶予のないときは，例外措置を実施し，実施後速やかに情報最高責任者及び部門情報統括責任者に報告しなければならない。

ウ 例外措置の申請書等の管理

情報セキュリティ最高責任者は，例外措置の申請書，報告書及び審査結果を適切に保管しなければならない。

７　情報セキュリティ個別基準の策定

部門情報統括責任者は，情報セキュリティポリシーを補完するために必要な全学共通の事項に関して，具体的な内容を定めた情報セキュリティ個別基準を策定する。

８　情報セキュリティ実施手順の策定

部門情報統括責任者及び業務システム責任者は，情報セキュリティポリシーに基づき，所管するシステム等に対する情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。

９　情報セキュリティに関する違反に対する対応

（１）懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した職員及びその監督責任者は，その重大性，発生した事象の状況等に応じて，就業規則等による懲戒処分の対象となる。

（２）再発防止の指導等

職員等情報取扱者に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には，情報基盤管理者，業務システム管理者及び情報管理者は，速やかに次の措置を講じなければならない。

ア 当該職員等情報取扱者に対して違反する行為の事実を通知し，再発防止の指導その他適切な措置を行う。

イ 指導等によっても改善されない場合，当該職員等情報取扱者の情報資産の使用権を停止あるいは剥奪する。

ウ 違反する行為が生じた場合，違反する行為の内容，指導内容その他措置の状況について情報セキュリティ最高責任者に報告する。

１０　評価・改善・見直し

（１）監査

ア 実施方法

情報セキュリティ最高責任者は，情報監査統括責任者に命じ，情報セキュリティ対

策状況について，定期的及び必要に応じて監査を行わせなければならない。

イ 監査を行う者の要件

（ア）情報監査統括責任者は，監査を実施する場合には，被監査部門から独立した者に対して，監査の実施を依頼しなければならない。

（イ）監査を行う者は，監査及び情報セキュリティに関する専門知識を有するものでなければならない。

ウ 監査実施計画の策定及び実施への協力

（ア）情報監査統括責任者は，監査を行うに当たって，監査実施計画を策定し，情報管理委員会に報告しなければならない。

（イ）被監査部門は，監査の実施に協力しなければならない。

エ 委託先事業者に対する監査

情報監査統括責任者は，委託先事業者に対して，委託先事業者からの再委託の事業者も含めて，情報セキュリティポリシーの遵守について監査を定期的及び必要に応じて行わなければならない。

オ 監査結果の報告

情報監査統括責任者は，監査結果を取りまとめ，情報管理委員会に報告する。

カ 監査調書等の保管

情報監査統括責任者は，監査の実施を通して収集した監査証拠，監査報告書の作成のための監査調書を，紛失等が発生しないように適切に保管しなければならない。

キ 指摘事項への対処

部門情報統括責任者は，監査結果を踏まえ，指摘事項に関係する情報管理者等に対し，当該事項への対処を指示しなければならない。また，指摘事項に関係しない情報管理者等に対しても，同種の課題及び問題点がある可能性が高い場合には，当該課題及び問題点の有無を確認させなければならない。

ク 監査結果の活用

情報セキュリティ最高責任者は，情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

（2）自己点検

ア 実施方法

（ア）情報基盤管理者及び業務システム管理者は，所管するネットワーク及び情報システムの情報セキュリティ対策状況について，定期的及び必要に応じて自己点検を実施しなければならない。

（イ）情報管理者は，所管する所属の情報セキュリティ対策状況について，定期的及び必要に応じて自己点検を行なわなければならない。

イ 自己点検結果等の報告

（ア）情報基盤管理者，業務システム管理者及び情報管理者は，自己点検結果と自己

点検結果に基づく改善策を取りまとめ，部門情報統括責任者に報告しなければならない。

（イ）部門情報統括責任者は，報告を受けた点検結果及び改善策を，情報管理委員会に報告しなければならない。

ウ 自己点検結果の活用

（ア）職員等情報取扱者は，自己点検の結果に基づき，自己の権限の範囲内で改善を図らなければならない。

（イ）情報セキュリティ最高責任者は，情報セキュリティポリシー等情報セキュリティ対策の見直し時に点検結果を活用しなければならない。

（３）改善

ア 是正措置

情報基盤管理者，業務システム管理者及び情報管理者は，業務上発見された問題，外部からの指摘による問題，監査及び自己点検において指摘された問題等に対する再発防止のため，その原因を除去するための措置を施さなければならない。

イ 予防措置

情報基盤管理者，業務システム管理者及び情報管理者は，業務上予見される問題，他の組織で発生したものと同種の情報セキュリティ事件・事故，監査及び自己点検において指摘されうる問題等の発生を未然に防止するため，その原因を除去するための措置を施さなければならない。

（４）情報セキュリティポリシーの見直し

情報セキュリティ最高責任者は，監査及び自己点検の結果，改善の状況，残留リスク，情報セキュリティに関する状況の変化等を踏まえ，情報セキュリティポリシーに対して必要があると認めた場合その見直しを行う。

附　則

この規程は，2014 年４月１日から施行する。

附　則

この規程は，2019 年４月１日から施行する。