千葉県立保健医療大学情報セキュリティ運用規程

第１章　総論

１．趣旨

千葉県立保健医療大学（以下「本学」という。）が保有する情報資産は、学生等の個人情報や教育・学術研究に係る情報など外部に漏えい等した場合に重大な結果を招く情報が含まれており、本学が社会的信頼の下、教育や研究、社会活動、大学運営を安全・円滑に行うためには、その安全性を確保することは必要不可欠である。

県では、情報セキュリティ基本方針、情報セキュリティ対策基準から構成される情報セキュリティポリシー（以下「ポリシー」という。）を定め、情報セキュリティの確保に努めているところだが、大学は他の行政事務とは異なり、教職員だけではなく学生においても守るべき情報資産に触れる機会がある等の特徴を有する。

そこで、本学においては、学生及び教職員とも情報資産の価値を認識し、それぞれの立場で注意深く取り扱うことができるよう、千葉県立保健医療大学情報システム委員会規程第１０条第１項の規定に基づき、ポリシーと整合性があり、大学として必要な情報セキュリティ対策の基本的事項を取りまとめた「千葉県立保健医療大学情報セキュリティ運用規程（以下「運用規程」という。）」を策定する。

なお、運用規程の目指すところは次のとおりである。

①　本学の情報セキュリティに対する侵害を阻止すること
②　学内外の情報セキュリティを損ねる加害行為を抑止すること
③　情報システムで取り扱う電磁的記録情報に関して、重要度に見合った管理を行うこと
④　情報セキュリティに関する情報の取得を支援すること

２．用語の定義

（１）運用規程で使用する用語の意義は、以下のとおりとする。

ア．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、その構成機器（ハードウェア及びソフトウェア）のことであり、本学の教育研究系、事務系、図書館系、インターネット系の各ネットワークをいう。

イ．情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

ウ．情報セキュリティ

情報の機密性、完全性、可用性を維持することをいう。

①　機密性　情報にアクセスすることが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。

② 完全性　情報が破壊、改ざん、又は消去されていない状態を維持することをいう。

③ 可用性　情報にアクセスすることが認められた者が、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いう。

エ．情報セキュリティ対策

情報セキュリティを確保するための対策のことであり、意図の有無を問わず不正なアクセス（攻撃）による改ざん、破壊、漏えい等から情報資産を防御するための対策等をいう。

オ．情報セキュリティインシデント

不正アクセス、情報漏えい、データの改ざん、ウイルス感染等により情報セキュリティに脅威が発生している又は発生する恐れがある事象をいう。

カ．リスク分析

情報セキュリティを侵害された場合（想定を含む）の影響評価

キ．所属

健康科学部各学科・専攻及び事務局

ク．教職員

本学に勤務する教員及び職員をいう。非常勤職員及び臨時職員を含む。

ケ．学生

本学に在籍する学生、聴講生及び科目等履修生をいう。

（２）この他、運用規程において使用する用語の意義は、文部科学省が決定した「教育情報セキュリティポリシーに関するガイドライン」（以下「文科省ガイドライン」という。）で使用する用語の例による。

３．対象範囲

（１）情報資産の適用範囲

運用規程が対象とする情報資産は次のとおりとする。

ア．本学のコンピュータ（本学が教職員に配付したコンピュータ及び外部資金で調達したコンピュータを含む。）、ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ．本学のコンピュータ、ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ．本学の情報システムの仕様書及びネットワーク構成図等のシステム関連文書

エ．本学以外のコンピュータで本学のネットワークに一時的に接続されるコンピュータ及びそれらが扱う情報（クラウドコンピューティング等により学外のネットワーク及びシステム上で取り扱う情報資産を含む。）

（２）適用対象者

本学の学生、教職員、本学で研究活動を行う研究員、本学の委託業者及び来学者等の

本学の情報資産を利用するすべての者（以下「学生・教職員等」という。）とする。

4．情報資産を取り扱う者の責務

大学は、情報の公開性と利便性を確保するために安全な情報システムを整備するとともに、情報セキュリティの重要性を学生・教職員等に周知徹底しなければならない。また、本学からの不正な情報提供や不正アクセスをなくし、学外に対しても本学の情報システムの信頼性を高めていくこととする。

学生・教職員等は、運用規程等の遵守を徹底するとともに、本学が保有する情報資産の価値を認識し、自身の情報を守るだけでなく、他者の情報資産も侵してはならないものとして行動しなければならない。

5．組織体制

本学が保有する情報資産について、情報セキュリティ対策の推進及び管理のための組織体制を確立するものとする。

6．情報資産の分類・管理

本学が保有する情報資産については、その内容に応じて分類し、その重要度に応じた情報セキュリティ対策を講じなければならない。

7．情報資産の脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（1）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去・詐取、内部不正等

（2）情報資産の無断持ち出し、ソフトウェア等の使用における規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい、破壊、消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

8．情報セキュリティ対策

前記7で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じるものとする。

（1）物理的セキュリティ

情報機器や情報保管施設等の機密性や安全性を維持するために、入室管理等の必要な物理的対策を講じて情報資産を保全する。

（2）人的セキュリティ

情報セキュリティの役割を定め、学生・教職員等に運用規程の内容を理解させ遵守することを周知徹底させるとともに、セキュリティ教育や啓蒙を行う等の必要な対策を講じる。

（3）技術的セキュリティ

情報資産に対する不正侵入や不正利用等から適切に保護するために、情報資産へのアクセス制限や認証等の必要な対策を講じる。

（4）運用

運用規程の遵守状況や実効性を確認するための必要な措置を講じるとともに、情報セキュリティインシデント発生時の対応策を定める。

9．評価・見直し

運用規程及び情報セキュリティ対策の実施状況を定期的に検証・評価するとともに、情報セキュリティに関する情報収集等を行うことにより、情報セキュリティの脆弱性が発見された場合は、新たな脅威等への対策を講じるほか、必要に応じて運用規程等の見直しを行う。

10. 個人情報の保護

学生・教職員等は個人情報の保護に関する関係法令及び個人情報の取扱に関する各種ガイドライン等を遵守しなければならない。また、業務上の権限を有しないものは、許可なく個人情報を閲覧してはならない。

第２章　情報セキュリティ運用規程

１．組織体制・役割

本学における情報セキュリティ対策の推進・管理のための組織体制・役割は次のとおりとする。

（1）最高情報セキュリティ責任者

① 本学に最高情報セキュリティ責任者（以下「最高責任者」という。）を置き、学長をもって充てる。なお、最高責任者は、県の対策基準に規定された所属情報セキュリティ責任者にあたり、その役割を担う。

② 最高責任者は、本学の情報セキュリティに関する総括的な権限及び責任を有する。

（2）情報セキュリティ実施責任者

① 本学に情報セキュリティ実施責任者（以下「実施責任者」という。）を置き、副学長をもって充てる。

② 実施責任者は、最高責任者を補佐するとともに、本学の情報セキュリティ対策の実施に関する権限及び責任を有する。
③ 実施責任者は、情報セキュリティ対策の実施に当たって、各所属の情報セキュリティ管理者と連絡調整を行うが、具体的な対策については、情報システム管理者に職務を代行させることができる。
④ 実施責任者は、情報セキュリティの侵害が発生又は発生が予想される場合には、緊急避難措置を実施することができる。緊急避難措置を実施した場合には、速やかに関連する責任者及び管理者への報告を行う。
⑤ 実施責任者は、最高情報セキュリティ責任者が不在の場合等、その役割を代行することができる。

（3）情報システム管理者

① 実施責任者の下に情報システム管理者を置き、最高責任者が指名する。
② 情報システム管理者は、実施責任者を補佐するとともに、重要事項を除き情報セキュリティ対策実施に係る事務を総括管理する。
③ 情報システム管理者は、情報セキュリティ対策の実施に当たって、実施責任者と情報ネットワーク支援管理者と連絡調整を行い、情報セキュリティ管理者又は情報資産管理者に対して対策の指示徹底を行う。
④ 情報システム管理者は、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、実施責任者の指示に従い、又は実施責任者が不在の場合は自らの判断に基づき、必要かつ十分な措置を実施する責任を有する。
⑤ 情報システムに関する一般的な情報セキュリティの啓発及び教育について、学生及び教職員に対する幅広い初心者教育を行う。

（4）情報ネットワーク支援管理者

① 情報システム管理者の下に、情報ネットワーク支援管理者を置き、最高責任者が指名する。
② 情報ネットワーク支援管理者は、本学の情報資産の管理及び情報セキュリティ対策に関する統一的な窓口の役割を担うとともに、学生・教職員等から相談・報告を受けた場合は、その状況を確認し必要な措置を実施する。
③ 情報ネットワーク支援管理者は、緊急時の対応を含め情報セキュリティ対策の実施に当たって、各所属の情報セキュリティ管理者又は情報資産管理者を支援する。
④ 情報ネットワーク支援管理者は、必要に応じて情報資産及び情報セキュリティ対策に係る運用の脆弱性について調査検討等を行い、課題、問題点及び運用状況等を把握するとともに、実施責任者、情報システム管理者にその内容を報告しなければならない。
⑤ 情報ネットワーク支援管理者は、実施責任者、情報システム管理者等関係者と連携・

協議し、情報システムの開発、設定の変更、運用、更新等の作業を行う。

（５）情報セキュリティ管理者

① 各所属に情報セキュリティ管理者を置き、学科・専攻の長又は事務局長をもってこれに充てる。

② 情報セキュリティ管理者は、各所属で取り扱う情報資産の情報セキュリティに関する権限と責任を有する。

③ 情報セキュリティ管理者は、情報セキュリティ対策の実施に当たっては、実施責任者、情報システム管理者又は情報ネットワーク支援管理者と連絡調整を行い、当該所属の教職員又は情報資産管理者に対して対策の指示徹底を行う。

④ 情報セキュリティ管理者は、情報セキュリティの侵害が発生又は発生が予想される場合には、情報システム管理者又は情報ネットワーク支援管理者へ速やかに報告を行い、指示を仰がなければならない。

⑤ 情報セキュリティ管理者は、各所属での情報セキュリティ対策の実施状況について、教職員へのアンケート等で定期的に確認を行い、その結果を情報システム委員会に報告しなければならない。

（６）情報資産管理者

① 各所属は必要に応じて情報資産管理者を置くことができ、各所属の教職員の中から情報セキュリティ管理者が指名する。

② 情報資産管理者は、所属が所管する情報資産等を管理・監督し、情報セキュリティを維持するための責任を負う。また、管理業務の実施の際には、情報セキュリティ対策及び運用の脆弱性についての調査検討を行い、結果を情報ネットワーク支援管理者に報告する。

③ 情報資産管理者は、情報セキュリティを適切に維持し運用するための実施手順（マニュアル）等を運用規程に則して整備し、当該システムを利用する者への普及教育を行う。

④ 情報資産管理者は、所管する情報資産に対する情報セキュリティの侵害が発生又は発生が予想される場合は、情報セキュリティ管理者及び情報システム管理者と協議し、必要な措置を実施できる。

２．情報資産の分類・管理

（１）情報資産の分類・管理

運用規程の適用範囲における情報資産は、機密性、完全性及び可用性により、下表のとおり分類し、当該分類に応じた管理を行うものとする。なお重要性分類別の情報の標準例は別表による。

重要性分類	機密性	完全性	可用性	定義
Ⅰ	3	2	2	秘密文書に相当する機密性を要し、その漏えい等により個人等の権利が侵害される、又は本学の事務・事業の適格な遂行に支障を及ぼすおそれがある情報
Ⅱ	2	2	2	秘密文書に相当する機密性は要しないが、直ちに一般公表することを前提としていない情報資産であり、その漏えい等により個人等の権利が侵害される、又は本学の事務・事業の適格な遂行に支障を及ぼすおそれがある情報
Ⅲ	1	1	1	公開している情報、又は内外を問わず不特定多数の者に開示できる情報

（2）情報資産の管理

ア．重要性Ⅰ情報の管理

① 職務上必要な者のみにアクセスを許可し、それ以外の者にアクセスさせてはならない。

② 情報を学外に持ち出してはならない。

③ 重要性Ⅱ情報の取扱制限に加え、本学のコンピュータ又はネットワークへの接続を登録したコンピュータ以外での作業を禁止する。

④ 情報を保有するサーバ等をインターネットに繋げてはならない。

イ．重要性Ⅱ情報の管理

① 学内、所属内など限定された者のみにアクセスを許可し、それ以外の者にアクセスさせてはならない。

② 原則として情報を学外に持ち出してはならない。やむを得ず持ち出す場合は、以下の持ち出し方法に応じて必要なセキュリティ措置をとったうえで、所属の情報セキュリティ管理者又は情報セキュリティ管理者から業務を委任された者の許可を得なければならない。

・ ネットワークを利用して外部のサーバ等に情報資産を保存する方法
保存するデータは暗号化（ZIP パスワード等）を行う。

・ 電子メールに情報資産を添付し外部に送信する方法
添付するデータは暗号化（ZIP パスワード等）を行う。また、送信時には上長又は所属の管理責任者にメールの同報送信を行う。

・ 外部クラウドサービスに情報資産を保存する方法
保存するデータは暗号化（ZIP パスワード等）を行う。

・　コンピュータや電磁的記録媒体（USB や CD（DVD）等）に情報を保存する方法

この方法は原則禁止とするが、やむを得ない場合は暗号化（ZIP パスワード等）を行う。

・　冊子等紙媒体で情報資産を外部に持ち出す方法

通年にわたり学生及び教職員等が持ち出す場合は、年 1 回の許可申請でも可とする。ただし、年度末や退職時等利用が終了した際には、持ち出した情報資産を回収する。

③　取扱制限

・　必要以上の複製及び配付禁止
・　保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止
・　復元不可能な処理を施しての廃棄
・　信頼のできるネットワーク回線の選択
・　バックアップ、電子的署名付与
・　外部で情報処理を行う際の安全管理措置
・　電磁的記録媒体の施錠可能な場所への保管

ウ．重要性Ⅲ情報の管理

①　保管方法など管理に関する事項を、必要に応じて定めなければならない。

②　不特定の者がアクセス可能な性質を持つものであるため、当該情報資産を管理する者は情報の改ざんや偽情報の流布に対し、必要に応じて防止策を講じなければならない。

エ．情報の部分的公開

重要性Ⅱ以上の情報の一部を不特定の者に開示する場合には、個人情報の漏えい、プライバシーや著作権の侵害に十分注意し、公開できる情報だけを抽出するか、あるいは統計処理などの加工を行わなければならない。

オ．外部委託に伴う情報の持ち出し

外部業務委託等のため、重要性Ⅱ以上の情報を限定された第三者に開示する必要がある場合は、情報セキュリティ要件を明記した契約を結ばなければならない。

カ．情報資産の廃棄等

情報資産の廃棄やリース返却を行う場合は、情報を記録している電磁的記憶媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

3．物理的セキュリティ

（1）サーバ等機器の管理

ア　機器の取付け

情報システム管理者は、サーバ等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する対策を講じた場所に設置し、不正持ち出し、傾倒を防止するため必要な措置を講じなければならない。

イ　サーバの冗長化

情報システム管理者は、停止等した場合に教育研究等の遂行に重大な影響を及ぼすサーバについては冗長化しなければならない。

ウ　機器の電源

情報システム管理者は、施設管理担当者と連携し、サーバ等機器の電源について、停電等による電源供給の停止に備え、必要な措置を講じなければならない。

エ　通信ケーブル等の配線

情報システム管理者は、施設管理担当者と連携し、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、配線収納管を使用する等必要な措置を講じなければならない。

オ　機器の定期保守

情報システム管理者は、サーバ等の機器の定期保守を実施しなければならない。また、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合は内容を消去した状態で行うものとし、それができない場合は守秘義務契約を締結し、秘密保持体制の確認等を行わなければならない。

カ　学外への機器の設置

情報システム管理者は、学外にサーバ等の機器を設置する場合（委託事業者の施設内に機器を設置し、又は委託事業の提供する機器を利用する場合を含む。）は、最高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。

キ　システムの脆弱性

情報資産を取り扱う PC 及びサーバ等のシステムの脆弱性については、速やかに対策を行い、利用期限の切れたシステムは使用しない。

ク　機器の廃棄等

情報システム管理者は、機器の廃棄、リース返却等する場合、機器内部の記録装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（2）情報システム室の管理

ネットワーク及び情報システムの基幹機器等を設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）は常時施錠することとし、入室は、原則として、当該情報システム室を管理する教職員、室内に基幹機器等を設置している情報システム等の担当者など入退室を許可された教職員のみとしなければならない。

また、学外の訪問者が情報システム室に入る場合には、入退室を許可された教職員が付き添うものとし、情報システム室の機器等を搬入出する場合には、職員等を立ち会わせなければならない。

（3）通信回線及び通信回線装置の管理

情報システム管理者は、学内の通信回線及び通信回線装置を適正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正に保管しなければならない。

また、外部のネットワーク接続を必要最小限に限定し、できる限り接続ポイントを減らさなければないない。

（4）コンピュータや電磁的記録媒体等の管理

教職員は、盗難及びデータ漏えい防止のため、執務室等で利用するコンピュータ及び電磁的記録媒体等について、使用時以外は施錠管理を行うなど物理的措置を講じなければならない。

4．人的セキュリティ

（1）学生・教職員等の遵守事項

ア　運用規程等の遵守義務

学生・教職員等は、運用規程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等がある場合は、速やかに情報システム管理者に相談し、指示を仰がなければならない。

イ　教育研究等業務以外の目的での利用の禁止

学生・教職員等は、教育研究等業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

ウ　本学から配付されたコンピュータ等の持ち出し等

学生・教職員等は、原則として本学から配付されたコンピュータ等を学外に持ち出してはならない。学外に持ち出す場合は、情報セキュリティ実施責任者又は情報セキュリティ管理者から業務を委任された者の許可を得なければならない。

また、本学から配付されたものではないコンピュータ等をインターネット系以外の学内ネットワークに原則接続してはならない。接続する場合は、事務局を通して最高責任者の許可を得て学内ネットワークに登録しなければならない。学内ネットワークに接続されたコンピュータにおいては、教育・研究・学習・業務に関連したソフトウェアのみ使用することができる。

エ　コンピュータ等の管理

学生・教職員等は、使用するコンピュータ、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に不正に使用又は閲覧されないように、離籍時のパソコンのロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管など、適正な措置を講じなければならない。

オ　セキュリティ設定変更等の禁止

学生・教職員等は、コンピュータ等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システム管理者の許可なく変更してはならない。

カ　退職時等の遵守事項

教職員は、異動、退職等により教育研究等から離れる場合には、利用していた情報資産を返却しなければならない。また、その後も教育研究等の遂行上に知り得た情報を漏らしてはならない。

ケ クラウドサービス利用時等の遵守事項

学生・教職員等は、クラウドサービスの利用にあたっても運用規程を遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

（2）研修・訓練

情報システム管理者は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（3）ＩＤ・パスワード等の管理

ア　ID の取扱い

学生・教職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

① 自己が利用しているＩＤは、他人に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。

イ　ID パスワードの取扱い

学生・教職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

① パスワードは、他者に知られないように管理しなければならない。

② パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③ 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にしなければならない。

④ パスワードが流出したおそれがある場合には、情報システム管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤ 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑥ 学生・教職員等間でパスワードを共有してはならない（ただし共有ＩＤに対するパスワードは除く）。

（4）非常勤職員等への対応

情報セキュリティ管理者は、学生・教職員等のうち非常勤職員、学生及び来学者に対し、情報資産の利用開始時に、運用規程等のうち守るべき内容を理解させ、遵守させなければ

ならない。

（５）外部委託

最高責任者は、ネットワーク及び情報システムの開発、保守等を外部委託する場合は、ポリシー及び運用規程に基づく外部委託事業者が守るべき内容の遵守及び委託業務上知り得た情報資産に関する守秘義務を契約に明記しなければならない。

５　技術的セキュリティ

（１）外部ネットワークとの接続制限等

外部へのネットワーク接続は、必要最小限に限定するとともに、情報システム管理者は、外部ネットワークとの接続点において、ファイアウォール等の情報セキュリティ機器を導入し、外部からの脅威に対する措置を講じなければならない。

（２）無線ＬＡＮの対策

情報システム管理者は、教育研究等に無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務づけなければならない。また、本学の敷地内に公衆通信回線（フリーWiFi）を設置する場合、教育研究等に利用するネットワークから分離させなければならない。

（３）ネットワーク及び情報システムの管理

ア　ID・パスワード等

本学で使用するシステムは、使用時に認証 ID・パスワード等で本人確認を必要とする。

イ　アクセス記録の取得等

情報システム管理者は、アクセス記録その他情報セキュリティの確保に必要な記録を取得し、一定期間保存するとともに、アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じなければならない。

ウ　ソフトウェアの修正及び更新

ネットワーク及び情報システムのソフトウェアに情報セキュリティに重大な影響を及ぼすセキュリティホールが発見された場合、情報システム管理者は、修正プログラムを速やかに適用しなければならない。

エ　電子メールのセキュリティ管理

情報システム管理者は、電子メールの中継処理その他の不正な電子メールの送受信が行われないよう、電子メールサーバの設定を行わなければならない。

（４）バックアップデータの作成

情報システム管理者は、ネットワーク及び情報システムで取り扱う情報について、故障その他からの復旧用としてバックアップデータを作成し、一定期間保存しなければならない。

（5）アクセス制御等

情報システム管理者及び情報資産管理者は、所管するネットワーク又は情報システムに権限のない学生・教職員等がアクセスできないよう制限しなければならない。

（6）不正プログラム対策

情報システム管理者は、コンピュータウィルス等の不正プログラムから情報資産を守るために必要な対策を講じなければならない。

（7）不正アクセス対策

情報システム管理者は、不正アクセスを防止及び早期検知するため必要な措置を講じなければならない。

（8）セキュリティ情報の収集

情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。

6 運用

（1）情報セキュリティインシデント発生時の対応

ア　学生・教職員等は、情報セキュリティインシデントを認知した場合、情報ネットワーク支援管理者又は情報資産管理者への報告を速やかに行わなければならない。

イ　情報ネットワーク支援管理者又は情報資産管理者は、学生・教職員等から情報セキュリティインシデントの発生について報告を受けた場合、その状況を確認し、速やかに実施責任者及び情報システム管理者へ報告するとともに、必要に応じて外部の関係機関等に連絡しなければならない。

ウ　情報システム管理者は、実施責任者の指示に従い、又は実施責任者が不在の場合は情報システム管理者の判断に基づき、必要かつ十分な措置を実施する。

エ　重大な情報セキュリティインシデントが発生又は発生が予想される場合には、実施責任者は、実施責任者、情報システム管理者及び情報ネットワーク支援管理者からなる会議を開催し、緊急避難措置等の迅速な措置及び再発防止のための対策を講ずることができる。緊急避難措置を実施した場合には、速やかに関連する責任者及び管理者への報告を行う。

オ　本学のネットワーク又は情報システムに支障を及ぼす恐れのある情報セキュリティ

インシデントに迅速に対処するため、必要に応じて情報システム管理者の元に情報セキュリティインシデント対応チーム（Computer Security Incident Response Team：「CSIRT(シーサート)」)を設置することができる。CSIRT の構成員は情報システム管理者が指名する。

カ　実施責任者は、情報セキュリティインシデントの発生によりやむを得ない場合は、ネットワークの切断及びシステム停止等の措置を講じることができる。

キ　情報システム管理者は、情報セキュリティインシデントの内容及び発生原因を分析し、セキュリティ侵害防止の暫定措置を講じた上で、所管するネットワーク及び情報システムを復旧する。

ク　情報システム管理者は、情報資産等に対してのリスク分析を行い、その結果に基づき運用規程に則した情報セキュリティ対策の適応実施及び管理を行わなければならない。

（２）運用規程の遵守状況の確認

ア　情報システム管理者は、情報セキュリティ管理者と連携して、本運用規程の遵守状況の確認を行い、問題を認めた場合には、速やかに実施責任者に報告しなければならない。

イ　実施責任者は、発生した問題について、適正かつ速やかに対処しなければならない。

ウ　情報システム管理者及び情報資産管理者は、ネットワーク及びサーバ等のシステム設計等における運用規程の遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（３）運用規程の具体化

必要に応じて、運用規程を具体的に実施するための実施手順（マニュアル）等の規程を別に定め、一体的に運用するものとする。当該規程の原案又は改正案の作成は、情報システム委員会が行う。

附　則

この規程は、令和７年４月１日から施行する。

附　則

この規程は、令和７年５月１日から施行する。

（別表）重要性分類別の情報標準例（第２章２（１）関係）

重要性分類	定義・標準例
Ⅰ	秘密文書に相当する機密性を要し、その漏えい等により個人等の権利が侵害される、又は本学の事務・事業の適格な遂行に支障を及ぼすおそれがある情報 ①個人情報(注1)のうち、個人識別符号(注2)を含む個人情報、特定個人情報（マ

	イナンバーをその内容に含む個人情報）及びこれに相当する個人を特定する情報（個人の銀行口座、自宅住所等） ②学生・教職員等の要配慮個人情報（注３） ③実施前の各種試験問題作成に関する情報 ④産業競争及び安全保障上の観点から、漏えい等により、政治的、法的な問題を生じるおそれのある未公開の研究情報 ⑤その他、担当者限りに取扱制限をすることが相応しい情報 ⑥上記各項目を扱う情報システムの ID、パスワード、情報セキュリティ関連情報
II	秘密文書に相当する機密性は要しないが、直ちに一般公表することを前提としていない情報資産であり、その漏えい等により個人等の権利が侵害される、又は本学の事務・事業の適格な遂行に支障を及ぼすおそれがある情報 ①個人情報のうち重要性分類Ｉに相当する機密性は要しないがその漏えい等により個人の権利が侵害される情報 ②受験生・学生の成績関連情報 ③入学料・授業料等減免関連情報 ④特許取得の可能性等、権利関係が複雑な研究情報 ⑤未公開の研究情報 ⑥学生・教職員の健康診断 ⑥その他、関係者限りに取扱制限をすることが相応しい情報 ⑦上記各項目を扱う情報システムの ID、パスワード、情報セキュリティ関連情報
III	公開している情報、又は内外を問わず不特定多数の者に開示できる情報。 ①個人情報のうち慣行として公にされ、又は公にすることが予定されている情報 ②ホームページ掲載関連情報 ③広報誌等を通じて積極的に発信する情報 ④その他、公開することが前提となっている情報

（注１）個人情報：以下２つに該当する情報（個人情報保護法２条１項)。

①氏名・生年月日その他の記述等により、特定の個人を識別できる情報

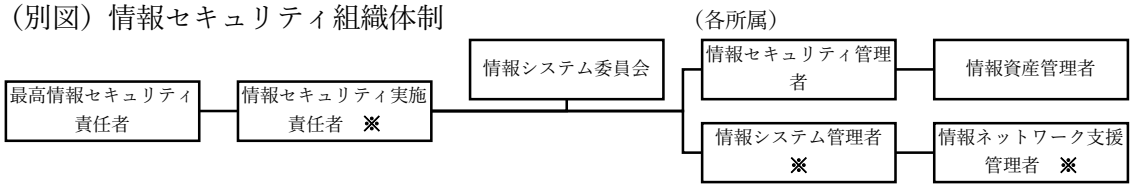
②個人識別符号（注２）が含まれる情報

（注２）個人識別符号： DNA 情報や容貌など身体的特徴を変換した符号、旅券番号、基礎年金番号、免許証番号、住民票コード、個人番号（マイナンバー)、健康保険証の被保険者記号、番号など（同条２項、個人情報保護法施行令１条、個人情報保護法施行規則３条、４条）

（注３）要配慮個人情報：本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により

害を被った事実、身体障害・知的障害・精神障害等があること、健康診断等の結果、保健指導・診療・調剤に関する情報、逮捕・差押えなどの刑事事件に関する手続が行われたこと（犯罪の経歴を除く)、少年の保護事件に関する手続が行われたこと、ゲノム情報（個人情報の保護に関する法律についてのガイドライン（通則編）2-3）

（別図）情報セキュリティ組織体制



※　情報セキュリティインシデント発生時には、※印の情報セキュリティ実施責任者、情報システム管理者及び情報ネットワーク支援管理者が中心となり連携して対応する。