資料２

北海道公立大学法人札幌医科大学情報セキュリティ対策規程（令和■年■月■日規程第　号）

目次

第１編　総則

第１章　通則

（目的）

第１条　この規程は、情報セキュリティ基本方針（令和■年規程第■号）に基づき、北海道公立大学法人札幌医科大学（以下「本法人」という。）が取り扱う電子情報及びその処理装置等並びにこれらに対する様々な脅威に関して必要な事項を定めることで、本法人における教育研究活動、業務運営その他の活動を推進するための基盤を構築することを目的とする。

（定義）

第２条　この規程において、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)　情報セキュリティ対策　情報資産等の機密性、完全性及び可用性を維持することをいう。
(2)　機密性　情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保することをいう。
(3)　完全性　情報が破壊され、改ざんされ及び消去されていない状態を確保することをいう。
(4)　可用性　情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。
(5)　情報セキュリティ責任者等　情報セキュリティ責任者、情報セキュリティ担当者、情報システム担当者及び補助者をいう。
(6)　教職員等　本法人の教員及び職員（いずれも非常勤その他の任用形態の者を含む。）並びに派遣契約職員をいう。
(7)　学生等　本法人の学部生、専門課程生、大学院生、研究生、聴講生及び科目等履修生並びに実習その他の教育を受ける目的で本法人の情報資産を利用する者をいう。
(8)　訪問者等　共同研究者、研究委託者、訪問研究員、本法人の退職者その他の本法人に所属しない者で、情報資産を利用する権限を付与された者をいう。
(9)　利用者　教職員等、学生等、訪問者等、受託者等及び退職日以降においても情報資産を利用する者をいう。
(10) 派遣契約職員　労働者派遣事業者との契約に基づき本法人の施設内において教育研究その他の業務等を行う者で自己のアカウント等を付与されて本法人の情報資産を利用する者をいう。
(11) 受託者等　本法人の施設内若しくは施設外又はその双方において、契約に基づき本法人の情報資産に関する業務を履行する者をいう。
(12) 所属等　附属総合情報センター長が別に定める所属等をいう。
(13) 業務等　本法人が行う学術研究、教育、医療、社会貢献及び業務運営に関する全ての活動並びに利用者が本法人に関連して行うこれらの活動をいう。ただし、学内データの利用を伴わない専ら個人的な目的による活動を除く。
(14) 情報資産　学内データ及びその記録媒体、電子データを処理し、若しくは伝送するための設備及び機器、プログラムのライセンス及びその権利を証明するための部材並びに電子データを入力するための帳票及び情報システムの仕様書その他の文書で、本法人の所有、占有又は管理に属するものをいう。
(15) 準情報資産　利用者が本法人の情報システムに接続して使用する本法人の所有、占有又は管理に属しない各種の情報処理設備、機器、記録媒体等及びこれらの関連文書をいう（インターネットを経由して本法人の情報システムに接続して使用するものを除く。）。
(16) 情報資産等　情報資産及び準情報資産をいう。
(17) 学内データ　本法人の権利が及ぶ全ての電子データをいう。
(18) 特定機密情報　北海道公立大学法人札幌医科大学電子情報の格付及び取扱制限に関する規程（令和■年規程第■■号）第６条第2項に定める学内データをいう。
(19) 機密性5情報　特に配慮が必要な学内データとして、次の各号に掲げるものをいう。
ア　個人が特定可能な患者に関する学内データ
イ　入学試験の作問、成績、合否決定等に関する学内データ（合格発表、成績の統計的集計値その他の入学試験の秘匿性保持に影響しない学内データを除く。）
ウ　学生の成績、学納金の減免、その他個人情報に該当する学内データ
エ　前３号に相当する機密性を有する、その他の学内データ
(20) 特定個人情報　個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報をいう。

(21) サーバー等　情報システムの構成機器のうち、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周辺機器を含む。）をいう。

(22) パソコン等　ネットワークへの接続の有無にかかわらず、利用者が電子データの処理を行うために直接操作する情報処理機器（搭載されるソフトウェア及び直接接続されて一体として扱われる周辺機器を含む。）をいう。

(23) 外部記録媒体　電子データを記録するための媒体のうち、コンピューターに内蔵された記録媒体を除いたものをいう。

(24) 情報システム　特定の業務遂行等を目的として構築された、コンピューターのハードウェア、ソフトウェア、通信伝送装置、情報保管蓄積装置、記録媒体その他の周辺機器、電子データ、関連文書等により構成される、情報の収集、蓄積、処理、伝達及び利用のための一連の体系をいう（単体のパソコン等を除く。）。

(25) 侵害等　データの漏えい、不正プログラムへの感染、不正アクセス、システムの障害その他次に掲げる例示を含め、情報セキュリティを損ね、又は損ねるおそれのあるあらゆる事象をいう。

ア　不正アクセス、不正プログラムによる攻撃、サービス不能攻撃等のサイバー攻撃、部外者の侵入等又は内部不正による、情報資産の漏えい、破壊、改ざん、消去、情報の窃取等

イ　情報資産の無断持出、不適正ソフトウェアの使用、開発上の不備、プログラムの欠陥、操作上の過誤、設定上の過誤、保守上の不備、監査機能の不備、受託者等に対する管理の不備、システム管理上の不備及び機器の故障等の要因による情報資産の漏洩、破壊及び消去

ウ　暴風雨、地震、落雷、火災、津波等の災害によるサービス、業務等の停止

エ　大規模な又は広範囲にわたる疾病に起因する情報資産の機能不全

オ　通信、電力、水道、公共交通網等のライフラインの途絶等の公共社会資本の障害からの波及

(26) 不適正プログラム　情報資産等において導入及び使用することが危険又は望ましくないプログラムとして、この規程に基づき指定されたものをいう。

(27) 不正プログラム　ウイルス、ワーム、マクロウイルス、トロイの木馬、スクリプトウイルス、スパイウェア等、名称及び挙動の種類を問わず、不正な又は有害な動作を行う意図で作成されたプログラム、コード等を総称していう。

(28) 不正アクセス　正当なアクセス権限を有しない者による不正なコンピューターの利用及びそのような不正利用を試みる行為をいう。

(29) ログ　情報システム又はパソコン等におけるハードウェアの状況、OSの動作状況、サービスの稼働状況、サービスへのアクセス状況、ユーザー認証の状況及びエラー及び警告の発出状況その他のシステムの管理作業等のために必要なデータの記録をいう。

(30) 約款による外部サービス　ネットワークを経由してサービス提供者が管理するサーバーを用いて利用者が情報の作成、保存、送信等を行うサービスで、当該サービスの開始に当たり約款への同意が必要なものをいう。

(31) ソーシャルメディアサービス　ネットワークを通じて情報発信、情報交換、参加者間のコミュニケーションその他の人の結びつきを利用した情報流通等を行う社会的要素を有する情報メディアサービスの総称をいう。

(32) クラウドサービス　サービス提供者がサーバー等に蓄積した情報等を用いて、情報システム、ソフトウェアその他の機能を提供するサービス（国、地方公共団体その他公的団体等が運営するものを含む。）をいう。

(33) インターネット外部サービス　約款による外部サービス、ソーシャルメディアサービス、

クラウドサービス及び第98条第2項の外部サービス（定めのない外部サービス）をいう。
2　この規程において用いられる、患者、電子データ、学内データ、情報その他これらに類する用語は、死者に関するものを含むものとする。

（人的適用範囲）

第３条　この規程は、教職員等に適用する。
2　この規程は､本法人が付与したアカウント等を使用している学生等及び訪問者等に適用する。
3　この規程は、業務の履行中である受託者等に適用する。
4　前３項の規定にかかわらず、第５条第２項第２号及び第26条の規定は、前３項に規定する身分を失った後においても、当該身分を失った者に適用する。

（物的適用範囲）

第４条　この規程は、情報資産等に適用する。

（利用者の一般的義務）

第５条　利用者は、情報資産等の利用に当たっては、関係法令、この規程及びこの規程に基づく関連規程、各種の通知等を遵守しなければならない。
2　利用者は、前項に定めるもののほか、次に掲げる義務を負う。
(1) 情報資産を業務等の遂行等の目的外に利用しないこと。
(2) 情報資産について適正な手続を経た許可を得ることなく外部の者に開示､漏洩しないこと。
(3) 善良なる管理者の注意をもって情報資産を取り扱うこと。
(4) 情報セキュリティ対策に関する情報の収集及び知識の習得に努めること。
(5) その他情報資産に対する情報セキュリティ対策上の危険性の回避に努めること。

（教職員等の一般的義務）

第６条　教職員等は、情報資産等の利用に関し、次に掲げる義務を負う。
(1) 他の教職員等及び学生等に対し、情報資産等の利用及び情報セキュリティ対策上の危険性の回避について、各々の権限に基づき、必要な助言、指導及び指示をすること。
(2) 情報資産等の利用及び情報セキュリティ対策上の危険性の回避に関して不適切と思われる事項を発見し、又は報告を受けた場合は、速やかに附属総合情報センターに報告すること。

（学生等の一般的義務）

第７条　学生等は、情報資産等の利用に関し、次に掲げる義務を負う。
(1) 正確に知りうる範囲において、情報資産等の利用及び情報セキュリティ対策上の危険性の回避について、他の学生等に対し情報の提供に努めること。
(2) 前条第１号に基づく教職員等による指導又は指示に従うこと。
(3) 情報資産等の利用若しくは情報セキュリティ対策上の危険性の回避を妨げ、又は害する他の利用者の行為を発見した場合は、速やかに教職員等に報告すること。

（報告内容の非開示）

第８条　教職員等は、前条第３号の規定による報告を受けたときは、当該報告の報告者、被報告者、内容その他の事項について、本法人が正式に公開の実施及び公開する情報の範囲を決定するまでの間、必要最小限の教職員等を除き当該事項を開示してはならない。

（契約に基づく業務履行等の特則）

第９条　教職員等は、情報資産の使用、保管、処分、開発、保守、修繕等の業務等を受託者等に履行させる場合又は非常勤職員若しくは派遣契約職員を配属する場合は、これらの者にこの規程その他の関連規程等が適用されること及び業務上知り得た情報の守秘義務その他の情報セキュリティに関して守るべき内容を理解させ、受託者等にあっては、契約締結の時、非常勤職員にあっては任命の時、派遣契約職員にあっては、任命に代わる行為の時までに書面による同意を得なければならない。
2　前項の規定にかかわらず、入札により第２条第10号又は第11号の契約を締結する場合は、

当該入札の公告又は通知によりあらかじめ前項の同意を当該契約締結の条件とする旨の告知をしなければならない。

（兼務禁止の原則）

第10条　教職員等は、情報資産等の利用又は情報セキュリティ対策に関する手続において、次に掲げる者を兼務してはならない。

(1) 許可又は承認の申請者並びにその許可権限者及び承認権限者

(2) 監査を受ける者及びその監査を実施する者

2　前項第１号の規定にかかわらず、教職員等は、許可等を申請しようとする場合において、自らが許可等の権限者等である場合は、申請内容が適正か否かについて他の教職員等の確認を受けなければならない。

3　前２項の規定にかかわらず、１名のみをもって構成される所属等である場合、所属等に属しない場合又はその他の代替的措置のないやむを得ない事情により許可若しくは承認の申請者及びその許可権限者若しくは承認権限者を兼ねる必要がある場合は、これらを兼ねることができる。

4　第１項に反しない場合においても、許可等の権限者が当該許可等の可否を決することについて、当該権限者等が属する部局の長が不適切であると認めるときは、当該部局の長又は当該部局の長が指定する者に許可等を申請しなければならない。

（代理使用の禁止）

第11条　利用者は、各種のアカウント、情報システム及びパソコン等の権限その他の属人的事項を本人に代わって使用させてはならない。

2　前項の規定にかからわず、次に掲げる場合は、本人による代理使用者の限定的指名及び承諾の下、同項に定める事項について代理使用させることができる。

(1) 傷病の療養のために休む間、他者が代理使用をする必要があるとき。

(2) 長期間の出張等の間、他者が本人に代わって業務等を処理する必要があるとき。

(3) 自己の特定の業務等を他の教職員等に行わせる場合で、当該教職員に代理使用させる業務遂行上の必要があるとき。

(4) 情報資産等の点検、調整、修理、保守等のため、当該作業を行う者が代理使用をする必要があるとき。

3　利用者は、前項各号により代理使用をさせる場合は、目的の範囲内における必要最小限の事項以外の情報を代理使用者に告知してはならない。

4　利用者は、前2項の規定による代理使用が終了した場合は、パスワード等の認証情報の変更をしなければならない。

5　代理使用者は、本人による承諾の目的の範囲を逸脱した代理使用を行ってはならない。

6　前５項の規定にかかわらず、利用者は、異動、退職その他の理由により情報資産の使用を終える場合は、当該情報資産を引き継ぐ者に対して、その使用に必要な全ての事項を書面により告知しなければならない。

第２章　組織体制

第１節　執行体制

（最高情報セキュリティ責任者）

第12条　情報セキュリティ対策を本法人全体で総合的に実施するため、最高情報セキュリティ責任者を置く。

2　最高情報セキュリティ責任者は、理事長がその職責に任ずる。

3　前項の規定にかかわらず、理事長は、本法人の理事を最高情報セキュリティ責任者に指名することができる。

4　最高情報セキュリティ責任者は、本法人における全ての情報セキュリティ対策に関する最終

的な決定権限を有する。

（情報セキュリティ統括責任者）

第13条　情報セキュリティ対策に関する業務を統括するため、情報セキュリティ統括責任者を置く。

2　情報セキュリティ統括責任者は、理事長が指名する者がその職責に任ずる。

3　情報セキュリティ統括責任者は、次に掲げる権限を有し、かつ、責任を負う。

(1) 本法人における情報セキュリティ対策を実施し統括すること。

(2) 最高情報セキュリティ責任者を補佐すること。

(3) この規程の施行及び運用に必要な方針、細則、ガイドラインその他の規程類を制定すること。

(4) 情報資産の危機管理に関すること。

(5) 利用者に対し情報セキュリティに関する教育等及び訓練等を行うこと。

(6) 利用者に対し、情報セキュリティ対策に関する助言、指導及び指示を行うこと。

(7) この規程の規定に基づき利用者の情報システム又はネットワークを使用する権限を一時停止し又は剥奪すること。

(8) 前号に規定する権限の一時停止又は剥奪に際し聴聞を主宰すること。

(9) この規程の改正の発議に関すること。

(10) その他、この規程の施行及び運用に必要な事務に関すること。

（情報セキュリティ責任者）

第14条　情報セキュリティ対策を適正かつ確実に実施するため、各所属等に情報セキュリティ責任者を置く。

2　情報セキュリティ責任者は、各所属等の長がその職責に任ずる。

3　情報セキュリティ責任者は、次に掲げる権限を有し、かつ、責任を負う。

(1) 最高情報セキュリティ責任者若しくは情報セキュリティ統括責任者の指導及び指示に基づき又は自らの判断により､所管する各所属等における情報セキュリティ対策を実施すること。

(2) 所管する利用者に対して、この規程その他の関連規程等の遵守、その他の情報セキュリティに関する助言、指導及び指示を行うこと。

(3) この規程に基づき自らが所管する利用者の情報システム及びネットワークを使用する権限を一時停止し、又は剥奪すること

(4) 情報セキュリティ担当者及び情報システム担当者を指名し、又は自らこれらを兼務すること。

4　前項第２号の所管する利用者には、当該所属等に在籍し本学から退職した者を含むものとする。

（情報セキュリティ担当者）

第15条　情報セキュリティ対策の具体的措置を実施するため、各所属等に情報セキュリティ担当者を置く。

2　情報セキュリティ担当者は、次に掲げる権限を有し、かつ、責任を負う。

(1) 所管する所属等における情報セキュリティ対策の実務に関すること。

(2) 情報セキュリティ責任者を補佐すること。

(3) 所管する所属等における情報セキュリティ対策について、当該所属等の構成員に対し実務面での助言、指導及び指示をすること。

(4) 情報セキュリティ対策の状況の把握等を行うこと。

(5) 所管する所属等の構成員の情報セキュリティ対策に関する知識及び情報の取得を支援すること。

3　情報セキュリティ担当者は､情報セキュリティ責任者の権限及び義務に属する事項について、

委任を受けて実施することができる。

（情報システム担当者）

第16条　各情報システムにおける情報セキュリティ対策の技術的措置を実施するため、情報システムを所管する所属等に情報システム担当者を置く。

2　情報システム担当者は、情報システムの開発又は運用を担当する教職員のうち、情報セキュリティ責任者が指名する者とする。

3　情報システム担当者は、情報セキュリティ責任者又は情報セキュリティ担当者の助言、指導及び指示に基づき、所管する情報システムにおける情報セキュリティ対策の技術的実務を実施する権限を有し、かつ、責任を負う。

（補助者の設置）

第17条　情報セキュリティ担当者及び情報システム担当者は、その所管する権限及び義務を遂行するため、情報セキュリティ責任者の承認を得て、補助者を指定することができる。

（最高情報セキュリティアドバイザー等）

第18条　最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する本法人内又は本法人外の者を最高情報セキュリティアドバイザーとして指名し、若しくは任命し、又は委託することができる。

2　情報セキュリティ統括責任者は、情報セキュリティ対策及び情報システムの開発、運用、保守その他の情報システム全般について専門的な知識及び経験を有する本法人内又は本法人外の者を情報化推進アドバイザーとして指名し、若しくは任命し、又は委託することができる。

3　最高情報セキュリティアドバイザー及び情報化推進アドバイザーは、最高情報セキュリティ責任者、情報セキュリティ統括責任者及び情報セキュリティ責任者の権限を代理行使することができない。

（情報セキュリティ顧問会議）

第19条　最高情報セキュリティ責任者は、この規程その他の関連規程等、その他の情報セキュリティ対策の審議を行う機能を有する組織として、本法人内又は本法人外の知見を有する複数の者により構成される情報セキュリティ顧問会議を設けることができる。

2　情報セキュリティ顧問会議は、最高情報セキュリティ責任者に直属する常設又は非常設の諮問機関とする。

（学生等に関する実施体制の特例）

第20条　各学部生及び専門課程の学生に対する情報セキュリティ対策に関する助言、指導及び指示については、次の各号に掲げる職につき、当該各号に定める者がその職責に任ずる。

(1) 情報セキュリティ責任者　各学部長が指名する者

(2) 情報セキュリティ担当者　前号の情報セキュリティ責任者が指名する者

2　大学院生、研究生、訪問研究員、その他所属等に属する者に対する情報セキュリティ対策に関する助言、指導及び指示については、当該所属における情報セキュリティ責任者等がその職責に任ずる。

3　前項の規定にかかわらず、所属が決定していない大学院生に対する情報セキュリティ対策に関する助言、指導及び指示については、所属が決定するまでの間は、当該大学院生が在籍する研究科の長の指名する者が、情報セキュリティ責任者の職責に任ずる。

第２節　監査体制

（情報セキュリティ監査責任者）

第21条　情報セキュリティ監査を統括し、適正な情報セキュリティ対策を確保するため、情報セキュリティ監査責任者を置く。

2　情報セキュリティ監査責任者は、理事長が指名する本法人内又は本法人外の者がその職責に任ずる。

3　情報セキュリティ監査責任者は、全ての情報資産等における情報セキュリティ対策に関する事項について監査を行う権限を有する。
4　前項の規定にかかわらず、情報セキュリティ監査責任者は、学生等を直接の対象とした監査を行う権限を有しない。
（情報セキュリティ監査担当者）
第22条　情報セキュリティ監査責任者は、本法人内又は本法人外の相当名の者を情報セキュリティ監査担当者に指名し、又は当該業務を外部に委託して監査を実施させることができる。
2　前項の場合において、学外の者を情報セキュリティ監査担当者に指名するときは、情報セキュリティ監査責任者は、事前に最高情報セキュリティ責任者に協議しなければならない。
3　情報セキュリティ監査担当者は、情報セキュリティ監査責任者の授権の範囲内において監査を実施する権限を有する。
（特定機密情報に関する監査）
第23条　情報セキュリティ監査責任者は、特定機密情報の閲覧又は内容調査にわたる監査を行う権限を有しない。
2　前項の規定にかかわらず、情報セキュリティ監査責任者は、監査の目的を達成するため、特定機密情報の閲覧又は内容調査をすることが必要不可欠であると認められる場合は、あらかじめ当該特定機密情報を特定の上、最高情報セキュリティ責任者に対し書面により協議しなければならない。
3　最高情報セキュリティ責任者は、前項の規定による協議を受理した場合は、監査の目的及び当該監査事項の重要性並びに不可欠性等を総合的に勘案し、当該監査の対象となる範囲を明示した上で、特定機密情報に関する監査を許可することができる。ただし、他の代替的手段により当該監査の目的が相当程度達成できると認められる場合はこの限りでない。

第２編　情報資産

第１章　利用者の義務等

（利用者の管理責任）
第24条　利用者は、情報資産の機密性、完全性、可用性その他の健全性を害するいかなる行為も行ってはならない。
（利益相反行為の禁止）
第25条　利用者は、情報資産等を大学の利益に反して自己の利益を図る行為及び第三者を利する行為に用いてはならない。
（協力義務）
第26条　利用者は、情報セキュリティ責任者等による指導、指示、協力要請等を正当な理由なく拒否してはならない。
（脅威の把握）
第27条　情報セキュリティ責任者等は、情報資産等に対する脅威となり得る事項の把握に努めなければならない。

第２章　情報資産の保護措置

（認証情報等の秘密保持）
第28条　利用者は、情報システムの利用に必要な認証情報、認証媒体その他の認証手段等について、漏えい、紛失又は毀損のないよう努めなければならない。
2　利用者は、自己の認証情報等が漏れ、又は自己のアカウント等に通常と異なる事象を発見した場合は、速やかに当該アカウント等を用いる情報システムを所管する情報セキュリティ責任者等に報告しなければならない。
（不適正プログラムの導入禁止）
第29条　利用者は、情報セキュリティ統括責任者又は情報セキュリティ責任者が不適正プログ

ラムとして指定したプログラムを情報資産等に導入してはならない。

（無許可でのネットワーク接続の禁止）

第30条　利用者は、情報セキュリティ統括責任者又はネットワークを所管する情報セキュリティ責任者の許可を得ることなく、パソコン等その他の機器を情報資産たるネットワークに接続させてはならない。

（情報資産の取扱い）

第31条　本法人が現に所有し、占有し又は管理する電子データのみならず、利用者の意思、記録されている場所又は方法その他の態様にかかわらず、本法人における業務等に関連する全ての電子データは、学内データとみなす。

2　利用者は、業務等上の必要性その他の正当な理由及び権限を有することなく学内データを複製してはならない。

3　前項の規定は、紙媒体の情報を電子データにする場合に準用する。

4　利用者は、情報資産が第三者によって閲覧され若しくは盗難され又は紛失することがないよう、容易に触れることのできない場所への保管その他の適切な取扱いをしなければならない。

（印刷物及び転記物への準用）

第32条　前条の規定は、学内データの印刷物及び転記物に準用する。

（データの暗号化及び匿名化等）

第33条　利用者は、取り扱う学内データの格付、取扱制限その他の性質に応じて、当該学内データに対して暗号化、匿名化等の処理を行わなければならない。

（準情報資産の使用）

第34条　利用者は、情報セキュリティ責任者の許可を得ることなく、準情報資産を本法人の情報システムに接続して使用してはならない。

2　情報セキュリティ責任者は、次の各号のいずれかに該当する準情報資産の本法人の情報システムにおける使用を許可することができる。

(1) 情報セキュリティ統括責任者が別に定める仕様等の要件を満たす準情報資産

(2) 短期間の使用等でかつ相応の情報セキュリティ対策上の措置がなされた準情報資産で、本学の情報セキュリティ対策上の脅威となるおそれが少ないものとして、情報セキュリティ統括責任者が個別案件ごとに事前に承認した準情報資産

(3) その他情報セキュリティ統括責任者が別に定める準情報資産

3　前項の規定にかかわらず、情報セキュリティ責任者は、利用者が前項第１号の仕様等の要件を具備するためのセットアップ作業及びその他の必要な作業を行うために必要がある場合は、当該準情報資産を本法人の情報システムに接続して使用することを許可することができる。

4　前3項の規定にかかわらず、情報セキュリティ統括責任者は、情報資産等に該当しないパソコン等の本法人の情報システムにおける使用について、別に定めることができる。

（学内データの格付等）

第35条　利用者は、北海道公立大学法人札幌医科大学電子情報の格付及び取扱制限に関する規程（平成■■年規程第■■号。）（以下「格付規程」という。）の規定に基づく格付及び取扱制限に従い、学内データを適切に取り扱わなければならない。

（特定機密情報の取扱いの原則）

第36条　利用者は、格付規程による特定機密情報に属する学内データをインターネットに接続したパソコン等に保存してはならない。

2　前項の規定にかかわらず、利用者は、前項のパソコン等で電子メールその他のデータ伝送方法により特定機密情報に属する電子データを受信した場合は、当該特定機密情報を遅滞なく当該パソコン等から退避させなければならない。

3　前２項の規定にかかわらず、利用者は、特定機密情報を当該パソコン等に保存する業務遂行

上の必要性がある場合で、かつ、他の代替手段がないときは、あらかじめ情報セキュリティ責任者の書面による許可を得なければならない。

4　前項の規定は、機密性５情報には適用しない。

（法人外からの特定機密情報の受領）

第37条　利用者は、外部から特定機密情報に相当すると認められる電子データを受領する場合は､原則として当該電子データの提供元における格付及び取扱制限を承継しなければならない。

2　前項の規定にかかわらず、利用者は、次に掲げる場合については、格付規程に基づく格付及び取扱制限により当該電子データを取り扱わなければならない。

(1) 提供元における格付及び取扱制限よりも本法人の格付規程における格付が上位である場合又はより厳格な取扱制限に該当する場合

(2) 提供元において格付及び取扱制限がなされていない場合

（パソコン等の物理的分離）

第38条　恒常的に特定機密情報を取り扱う利用者及びその情報セキュリティ責任者は、インターネットに接続するパソコン等と特定機密情報を取り扱うパソコン等を物理的に分離するよう努めなければならない。

（情報資産の持ち出し禁止）

第39条　利用者は、情報資産を法人外に持ち出してはならない。

2　前項の規定にかかわらず、利用者は、情報資産を法人外に持ち出す業務等上の必要性がある場合は、次条に該当する場合を除き、情報セキュリティ責任者の書面による許可を得なければならない。

3　電子メールによる添付ファイルの送付その他の通信手段による学内データの本法人外への伝送は、情報資産の法人外への持ち出しとみなす。

（許可手続の免除）

第40条　前条第２項の規定にかかわらず、利用者は、次の各号のいずれかに該当する場合は、同項の許可手続を省略することができる。ただし、次条に該当する場合はこの限りでない。

(1) 特定機密情報に該当しない学内データについて前条第３項の伝送を行うとき。

(2) 一定範囲の業務等に関連する特定の情報資産で反復継続して持ち出す必要のあるものについて３月を超えない期間で持ち出しの許可を得た場合で、かつ、持ち出しの都度、持出記録を作成したとき。

(3) 契約の相手方に対して学内データを提供する場合において、該当する情報につき書面による秘密保持の合意がなされているとき。

(4) 外部の者と研究その他の事業等を協働して実施する場合で、当該研究その他の事業等の内容、目的及び契約内容に照らし、あらかじめ提供が予定されている匿名加工情報その他の学内データを当該外部の者に提供するとき。

(5) 単独の利用者の管理下にある複数の電子メールアカウント間で電子メールを転送する場合で、当該電子メールのサービス提供者において、電子メール及び添付ファイルの電子データについて二次利用を行わないことが確認されているとき。

(6) 自己の監督権限に属する学内データであり、当該情報の漏洩、消失その他の事故等が発生した場合においても、本法人及び第三者に不利益が発生しないとき。

(7) 自己を含む複数人の共同の監督権限に属する学内データであり、当該学内データの持ち出しについて、当該共同者及びその承継人全員の同意がある場合で、かつ、当該情報の漏洩、消失その他の事故等が発生した場合においても、本法人及び第三者に不利益が発生しないとき。

(8) その他情報セキュリティ統括責任者が別に定める事案に該当するとき。

（持出条件の加重）

第41条　第39条第２項に基づき情報資産の持ち出しを許可しようとする情報セキュリティ責任者は、当該情報資産が格付規程第７条に規定する機密性５情報に該当する場合は、あらかじめ情報セキュリティ統括責任者を経由して最高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　前２条の規定にかかわらず、情報セキュリティ責任者又は情報資産を事実上管理する教職員等は、重要性又は秘匿性が高いと認める情報資産について、特定の場所からの持ち出しを禁じ、又は第39条第２項若しくは前項の許可に加えて自らによる許可を要する情報資産として指定することができる。

（機密性５情報の伝送禁止）

第42条　第39条第２項及び前条の規定にかかわらず、教職員等は、機密性５情報に該当する学内データについて、電子メールその他の通信手段による伝送をしてはならない。

（持ち出し等の方法）

第43条　第39条第２項及び第41条の規定により学内データを持ち出し又は伝送する利用者は、安全確保に留意して運搬方法等又は伝送方法等を決定し、当該学内データの格付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じなければならない。

２　前項の場合において、特定機密情報に該当する学内データを持ち出し又は伝送する利用者は、あらかじめ第33条の処理がなされていることを確認しなければならない。

（電子メールの転送）

第44条　電子メールを用いて学内データを伝送しようとする利用者は、伝送先において当該電子メールの情報が自動転送等により拡散される危険性を十分に考慮し、伝送対象としている学内データの機密性保持等について、あらかじめ慎重な検討を行わなければならない。

（ネットワークの接続制限）

第45条　利用者は、第36条第３項及び第39条第２項の許可を得て特定機密情報を保存したパソコン等を外部に持ち出した場合は、当該パソコン等を管理者が不適当又は明らかでないネットワークに接続させてはならない。

２　前項の場合において、当該特定機密情報が機密性５情報に該当する場合は、利用者は当該パソコン等を外部のネットワークに接続させてはならない。

（情報の提供及び開示）

第46条　教職員等は、職務上の閲覧権限を有する者以外の者に学内データを提供し、又は開示してはならない。

２　前項の規定にかかわらず、教職員等は、前項の提供又は開示をする業務等遂行上の必要が生じた場合は、情報セキュリティ責任者の許可を得なければならない。

３　前項の場合において、提供又は開示をする学内データが、格付規程第７条に規定する機密性５情報に該当する場合は、情報セキュリティ責任者は、あらかじめ最高情報セキュリティ責任者の許可を得なければならない。

４　前２項の場合において、教職員等は、当該学内データを提供し、又は開示する者において、当該学内データに付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱上の留意事項を確実な方法で伝達しなければならない。

（情報の保全）

第47条　情報システムを所管する情報セキュリティ責任者等は、サーバー等に記録された電子データについて、定期的なバックアップを実施しなければならない。

２　教職員等は、自らが使用するパソコン等及び外部記録媒体に保存された重要な学内データについて、定期的にバックアップを実施しなければならない。

３　教職員等は、前２項のバックアップを行うに当たり、情報の格付及び取扱制限に応じて保存場所、保存方法及び保存期間等を定め、適切に管理しなければならない。

（記録等の管理）

第48条　情報システムを所管する情報セキュリティ責任者は、次に掲げる基準に従い、記録等が業務等上の正当な権限を有する者以外の者に閲覧され、又は利用されることのないよう適切に管理しなければならない。

(1) 情報システムの仕様書、運用記録その他の文書等を整備すること。

(2) 前号に定める文書等を当該情報システムが存続する限り適切に保管すること。

(3) 各種のログその他の情報セキュリティの確保に必要な記録等を取得すること。

(4) 前号の記録等を第93条及び第94条に規定する情報セキュリティ対策実施手順において定めた期間、適切に保管すること。

（情報資産の処分）

第49条　利用者は、情報資産を処分するときは、情報セキュリティ責任者の承認を得なければならない。

2　前項の場合において、記録媒体を含む情報資産を処分するときは、利用者は、電子データの復元が完全に不可能な状態に処置しなければならない。

3　前２項の規定は、リース物件等の返却の場合に準用する。

（特定個人情報に関する情報セキュリティ対策）

第50条　特定個人情報を取り扱う情報システムを所管する情報セキュリティ責任者は、当該情報システムに関する情報セキュリティ対策について、この規程で定める基準のほか、個人情報保護委員会が定める特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）その他のガイドライン等（以下「ガイドライン等」という。）の基準を満たさなければならない。

2　前項の場合において、この規程で定める基準がガイドライン等が定める基準に抵触するときは、ガイドライン等の基準を適用する。

第３章　外部記録媒体の管理

（外部記録媒体の管理責任）

第51条　情報セキュリティ責任者は、外部記録媒体の紛失、盗難及び電子データの漏えいを防止するための必要な措置を講じなければならない。

（外部記録媒体の管理方法）

第52条　利用者は、次に掲げる方法その他の方法により、情報資産たる外部記録媒体を管理しなければならない。

(1) 所管する外部記録媒体の数量、配置箇所、使用者等の使用状況について常に把握すること。

(2) 第33条の遵守を確認すること。

2　前項第１号の規定にかかわらず、利用者は、所管する情報資産たる外部記録媒体のうち、要機密情報が記録された外部記録媒体の数量、配置箇所、使用者、記録内容、記録件数等の使用状況について、管理簿その他の記録が残る方法をもって常に把握しなければならない。

3　前項の場合において、当該特定機密情報が機密性５情報に該当する場合は、利用者は、現に作業を行っている間を除き、当該外部記録媒体を施錠した場所に保管しなければならない。

（情報資産に該当しない外部記録媒体）

第53条　利用者は、情報資産に該当しない外部記録媒体を学内ネットワークに接続した情報資産等たるパソコン等で使用する場合は、前条の規定に準じて当該外部記録媒体を管理しなければならない。

2　前項の規定は、不特定の者の利用に供することを目的として配備された情報資産たるパソコン等で当該外部記録媒体を使用する場合には、適用しない。

（適用除外）

第54条　前２条の規定は、次に掲げる場合においては、適用しない。

(1) 業務等上の目的により教職員等と学生等との間で電子データを授受する場合
(2) 一般に公開が可能な電子データを外部の者に提供する場合
(3) 信頼に足る企業等から販売促進物品等、広報を主たる目的とした電子データの提供を受ける場合
(4) 契約の相手方たる事業者等から契約の目的物を受領する場合で、当該外部記録媒体全体について不正プログラムの検索済みであることが当該事業者によって証明されている場合

2　前項に該当する外部記録媒体を使用する利用者は、当該外部記録媒体を接続するパソコン等に不正プログラム対策ソフトウェアを常駐させた状態を維持しなければならない。

（定期点検）

第55条　情報セキュリティ責任者は、所管する外部記録媒体の管理状況について定期的に点検を行わなければならない。

2　情報セキュリティ責任者は、前項の点検の結果、外部記録媒体の紛失その他の管理簿との不符合が判明した場合は、速やかに情報セキュリティ統括責任者に報告しなければならない。

第３編　情報セキュリティ対策

第１章　管理区域

（一般管理区域）

第56条　情報資産を保管する全ての場所を一般管理区域とする。

2　情報セキュリティ責任者等は、一般管理区域に教職員等がいない時間が生じないよう努めなければならない。

3　教職員等は、一般管理区域に教職員等がいない場合は、当該区域の出入口を施錠しなければならない。

4　情報セキュリティ責任者等は、次に掲げるいずれかの措置を行うことによって前項の施錠に代えることができる。

(1) 教職員等が不在の場合に、教職員等に代わる信頼に足る者を配置すること。
(2) 特定機密情報に該当する情報資産がない一般管理区域又は特定機密情報に該当する情報資産がすべて施錠管理された状態にある一般管理区域において、物理的な方法により情報資産の盗難等に対する防止措置を行うこと。

（部外者への確認）

第57条　教職員等及び前条第４項第１号に規定する者は、一般管理区域内で部外者と思われる者を発見した場合は、身元及び用件等を確認の上、必要に応じ当該者を一般管理区域外へ移動させなければならない。

（特定管理区域）

第58条　サーバー等の重要な機器を設置した場所を特定管理区域とする。

2　特定管理区域を所管する情報セキュリティ責任者は、当該区域が特定管理区域であることを外部の者が判断できる表示を行ってはならない。

3　特定管理区域を所管する情報セキュリティ責任者は、特定管理区域を常時施錠管理しなければならない。

（入退室管理）

第59条　特定管理区域を所管する情報セキュリティ責任者は、特定管理区域への入退室を許可した者のみに制限し、入退室管理簿の記録等による入退室管理を行わなければならない。

2　情報システムを所管する情報セキュリティ責任者は、第三者又は特定管理区域に設置された情報システム等に必要な作業等を行おうとする事業者等が特定管理区域に立ち入る必要がある場合は、必要に応じて立入区域を制限するとともに、身分証明書等の本人確認ができる書証を常時携帯させ、かつ、外見上教職員等と区別できる措置を講じなければならない。

3　第１項の規定により特定管理区域を所管する情報セキュリティ責任者が当該区域への立入を

許可する場合は、情報システムを所管する情報セキュリティ責任者は、前項の第三者又は事業者等に自ら付き添い、又は所管する教職員等を付き添わせなければならない。

（物品の持ち込み）

第60条　情報システムを所管する情報セキュリティ責任者は、前条の規定により立入を許可した者に、電子データの持ち込み又は持ち出しが可能な物品等を持ち込ませてはならない。

2　前項の規定にかかわらず、情報システムを所管する情報セキュリティ責任者は、次に掲げる物品等の持ち込みを許可することができる。

(1) 特定管理区域における情報システム又はその他の機器等の設置、点検、保守、処分等に必要な物品等

(2) 前号に規定する作業を行うに当たり通常必要とされる物品等で、かつ、用途、使用方法、数量等を限定の上、特別に持ち込みを認める物品等

（法人外への機器の設置）

第61条　情報システムを所管する情報セキュリティ責任者は、本法人の施設外にサーバー等の機器を設置しようとする場合は、当該設置場所がこの規程及び関連規程類が特定管理区域に求める要件を満たす等、適切な情報セキュリティ対策が実施されていることを事前に確認しなければならない。

2　前項の規定により、本法人の施設外にサーバー等の機器を設置した情報セキュリティ責任者は、１年を超えない範囲で定期的に当該機器及び設置場所の情報セキュリティ対策の状況について確認しなければならない。

第２章　人的対策

（情報収集）

第62条　情報セキュリティ統括責任者及び情報セキュリティ責任者等は、ソフトウェアの脆弱性に関する情報、不正プログラムに関する情報その他の情報セキュリティに関する情報の収集に努めなければならない。

2　情報セキュリティ統括責任者及び情報セキュリティ責任者等は、情報セキュリティに関する情報が必要な利用者の間で迅速に共有できる体制の整備に努めなければならない。

（新たな脅威への対応）

第63条　情報セキュリティ統括責任者は、情報セキュリティに関する社会環境及び技術環境の変化による情報セキュリティ上の新たな危険性を認知したときは、情報資産に対する侵害等を未然に防止するための対策を講じなければならない。

（ソフトウェアの更新）

第64条　利用者は、自らが使用するソフトウェアを常に最新の状態に保たなければならない。

2　情報セキュリティ統括責任者及び情報セキュリティ責任者等は、ソフトウェアの脆弱性に関する情報を収集したときは、必要に応じ修正プログラム等の適用を所管する利用者に指示する等の適切な措置を講じなければならない。

3　情報セキュリティ担当者及び情報システム担当者は、前項の規定による指示がなされた場合は、所管する利用者が修正プログラム等を確実に適用するよう、必要な助言、指導及び指示をしなければならない。

（更新の延期等）

第65条　前条の規定にかかわらず、ソフトウェアを最新の状態に保つための修正プログラム等の適用により、情報システム又はパソコン等の正常な稼働が維持できなくなるおそれがある場合は、情報セキュリティ統括責任者及び情報セキュリティ責任者等は、当該修正プログラム等の適用の延期又は取りやめを利用者に指導し、又は指示することができる。

2　前項の規定により修正プログラム等の適用の延期又は取りやめを利用者に指導し、又は指示した情報セキュリティ統括責任者又は情報セキュリティ責任者等は、継続的に当該修正プログ

ラム等の情報を収集し、時宜に応じた適切な指導又は指示をしなければならない。

（不正プログラムの情報）

第66条　情報セキュリティ統括責任者及び情報セキュリティ責任者等は、不正プログラムに関する情報を収集したときは、その緊急性、分布状況、不正プログラム対策ソフトウェアの対応状況その他の情報に基づき、必要に応じてその所管する利用者に対して警告を発する等の適切な措置を講じなければならない。

2　前項の規定による警告が発せられた場合は、情報セキュリティ担当者及び情報システム担当者は、所管する利用者に必要な助言、指導又は指示をしなければならない。

第３章　技術的対策

（技術情報の収集）

第67条　情報セキュリティ統括責任者及び情報システムを所管する情報セキュリティ責任者等は、情報システムの安全性及び信頼性を確保するため、常に情報技術に関する情報の収集及び知識の習得並びにその評価に努めなければならない。

（アクセス制御の設定）

第68条　情報システムを所管する情報セキュリティ責任者等は、次に掲げるアクセス制御の設定等を行わなければならない。

(1) 所管する情報システムにおいて取り扱う電子データの性質に応じた利用者認証の仕組みを当該情報システムに装備すること。

(2) 正当な権限を有しない者によるアクセスを防止するためのシステム上の制限を設けること。

(3) 所管する情報システムにおける利用者の登録、変更及び抹消を適切かつ確実に行うこと。

2　前項の情報セキュリティ責任者は、内部の情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の範囲に限定しなければならない。

（他のネットワークとの接続制限等）

第69条　利用者は、次項の許可を得ることなく本法人が管理するネットワークを他のネットワークに接続させてはならない。

2　ネットワークを管理する情報セキュリティ責任者は、所管するネットワークを他のネットワークと接続する場合は、当該ネットワークの構成及びセキュリティの状況を調査し、情報資産に影響が生じないことを確認した上で、情報セキュリティ統括責任者の許可を得なければならない。

（ネットワークの情報窃取防止対策）

第70条　ネットワークを管理する情報セキュリティ責任者は、情報の窃取を防止するための適切な措置を講じなければならない。

（無線LANの使用制限）

第71条　利用者は、情報セキュリティ統括責任者の許可を得ずに無線LAN通信機器を本法人が管理するネットワークに接続させてはならない。ただし、パソコン等に内蔵された無線LAN通信機器及びこれと同等の追加装備用機器はこの限りでない。

（不正プログラムの侵入防止）

第72条　ネットワークを所管する情報セキュリティ責任者は、外部のネットワークを経由して電子データを受信する通信について、当該電子データが内部のネットワークに至る以前に不正プログラムの検査を行う等の方法により、不正プログラムの内部のネットワークへの侵入の防止に努めなければならない。

2　ネットワークを所管する情報セキュリティ責任者は、外部のネットワークを経由して電子データを送信する場合は、当該電子データが外部のネットワークに至る以前に不正プログラムの検査を行う等の方法により、不正プログラムの外部のネットワークへの拡散の防止に努めなけ

ればならない。

（不正プログラム対策ソフトウェア）

第73条　情報セキュリティ責任者は、所管する利用者が使用するパソコン等に不正プログラム対策ソフトウェアを常駐させなければならない。

2　利用者は、情報セキュリティ責任者の許可を得ることなく、前項の規定による常駐を解除してはならない。ただし、システム障害からの復旧作業を行う場合等の必要やむを得ない場合については、この限りでない。

3　前2項及び次条の規定のほか、不正プログラム対策ソフトウェアの運用に関する詳細は、情報セキュリティ統括責任者が別途定めるところによる。

（不正プログラム対策ソフトウェアの更新）

第74条　情報セキュリティ統括責任者及び情報セキュリティ責任者は、利用者が不正プログラム対策ソフトウェアを常に最新の状態に保つことができるよう環境を整備しなければならない。

2　利用者は、不正プログラム対策ソフトウェア及びそのパターンファイル等を常に最新の状態に保たなければならない。

（適用除外）

第75条　前2条の規定は、次の各号のいずれかに掲げる場合で、かつ、安全確保のための代替的な措置が行われる場合については、適用しない。

(1) サーバー等又はパソコン等のソフトウェア環境上、不正プログラム対策ソフトウェアの同時稼働が不可能なとき。

(2) 他の機器を制御するための専用のサーバー等又はパソコン等で、技術的理由によりソフトウェア環境を変更することができないとき。

(3) その他、情報セキュリティ統括責任者が指定する事案に該当するとき。

（データの授受）

第76条　利用者は、外部記録媒体、電子メールの添付ファイル又はネットワーク経由での電子データの伝送等の手段により、外部と電子データを授受する場合には、不正プログラムの検査を行わなければならない。

（攻撃からの防御）

第77条　情報セキュリティ統括責任者及び情報セキュリティ責任者等は、攻撃による被害を最小限にするため、攻撃の種類に応じた適切な対応策を検討し、これを実行しなければならない。

2　最高情報セキュリティ責任者は、前項の対応策の検討に関して、必要に応じて外部の専門家の支援を受けることができる体制の整備に努めなければならない。

（記録の保存）

第78条　情報システムを所管する情報セキュリティ責任者等は、情報システムに攻撃を受けた場合は、第45条第3号の記録その他の必要な記録を相当の期間保存しなければならない。

（利用者による不正アクセス）

第79条　情報セキュリティ統括責任者及び情報セキュリティ責任者等は、利用者の故意又は過失による不正アクセスを覚知した場合は、直ちに当該利用者に対し不正アクセスの停止を指示するとともに、当該利用者を所管する情報セキュリティ責任者に告知し、適切な対処を求めなければならない。

第4編　運用

第1章　運用体制

（運用の一般原則）

第80条　情報セキュリティ責任者は、所管する情報システム及びパソコン等の管理体制の明確化、所管する利用者に対する指導その他の必要な措置を講じ、当該情報システムの円滑かつ効

率的な運用及び管理に努めなければならない。

（権利及び法益の保護）

第81条　利用者は、情報システム及びパソコン等の利用、運用、管理及び処分に当たり、個人情報、著作権その他の権利又は法益の保護に万全を期さなければならない。

2　情報セキュリティ責任者は、所管する利用者が前項の権利又は法益を侵すことのないよう、指導しなければならない。

（適合状況の報告）

第82条　情報セキュリティ責任者等は、所管する情報システム及びパソコン等のこの規程への適合状況に齟齬を覚知した場合は、適切かつ速やかに対処しなければならない。

2　前項の場合において、当該齟齬が本法人全体又は複数の情報システム若しくはパソコン等にわたる場合その他情報セキュリティ責任者が必要と認めるときは、速やかに情報セキュリティ統括責任者に報告しなければならない。

3　前項の規定による報告を受けた情報セキュリティ統括責任者は、当該齟齬に対し適切かつ速やかに対処しなければならない。

（情報セキュリティ対策の状況把握）

第83条　情報システムを所管する情報セキュリティ責任者は、所管する情報システム、パソコン等及びネットワークの情報セキュリティ対策の状況を常に把握しなければならない。

2　情報セキュリティ責任者は、所管する情報システム及びパソコン等のこの規程への適合状況について必要の都度調査を実施しなければならない。

（利用状況の調査）

第84条　情報セキュリティ統括責任者、情報セキュリティ責任者及びこれらの委任を受けた者は、不正アクセス、不正プログラムその他この規程に違反する行為等の調査を目的として、利用者が使用しているパソコン等の利用状況を調査することができる。

2　前項の規定による調査に当たり、情報セキュリティ統括責任者、情報セキュリティ責任者及びこれらの委任を受けた者は、当該パソコン等の現状の変更の禁止、引渡その他の必要な措置を当該利用者に指示することができる。

3　前２項の場合において、当該利用者は、調査及び必要な措置を拒否することができない。

4　情報セキュリティ統括責任者、情報セキュリティ責任者及びこれらの委任を受けた者は、第１項の利用状況の調査において、必要な範囲を超えて個人的事項に属する電子データを閲覧、複製、改変、消去等をすることのないよう配慮しなければならない。

第２章　侵害等発生時の対応

第１節　情報資産への侵害等発生時の対応

（侵害等発生時の対応）

第85条　利用者は、情報システム又はパソコン等の異常を発見した場合は、速やかに情報セキュリティ責任者等にその状況を報告しなければならない。

2　前項の規定による報告を受けたときは、当該情報セキュリティ責任者等は、情報セキュリティ上の懸念がある場合その他必要と認める場合は、当該状況を情報セキュリティ統括責任者に報告しなければならない。

3　情報セキュリティ責任者等は、前２項の状況が情報資産への侵害等と認められるときは、情報セキュリティ統括責任者と協議の上、適切に対処し、対処結果を情報セキュリティ統括責任者に報告しなければならない。

（関係機関との連携）

第86条　情報セキュリティ統括責任者及び情報セキュリティ責任者は、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）その他の法律に違反するおそれがある侵害等が発生した場合は、第48条第３号の記録及び侵害等に関するその他の記録を保全するとともに、

警察及び関係機関と連携し、迅速な対応を行わなければならない。

（不正プログラムへの感染が疑われる場合の対応）

第87条　利用者は、パソコン等への不正プログラムへの感染が疑われる場合は、直ちに当該パソコン等をネットワークから取り外し電源を切断する等の方法により、不正プログラムの拡散防止のための迅速な対応を行わなければならない。

（ネットワークの遮断）

第88条　情報セキュリティ統括責任者、ネットワークを所管する情報セキュリティ責任者及びこれらの委任を受けた者は、情報資産への侵害等その他不適切な状況が発生し、又はそのおそれがある場合において必要と認めるときは、ネットワークの全部又は一部を遮断することができる。

2　情報セキュリティ統括責任者及びネットワークを所管する情報セキュリティ責任者は、前項の規定によりネットワークの遮断の対象となった所属等に対して、情報セキュリティ対策上の必要な措置を命ずることができる。

3　ネットワークを所管する情報セキュリティ責任者は、第１項の規定によりネットワークを遮断したときは、当該遮断の原因となった事項及びその状況、遮断の範囲その他の必要事項を速やかに情報セキュリティ統括責任者に報告しなければならない。

4　前項の規定による報告に当たっては、報告の迅速性を優先することとし、判明している情報の範囲で迅速に第１報を行わなければならない。

5　情報セキュリティ統括責任者は、第１項及び第２項に該当する事態が発生した場合で、当該事態が重大な案件であると認めるときは、速やかに最高情報セキュリティ責任者に報告しなければならない。

（侵害等発生後の取扱い）

第89条　情報セキュリティ統括責任者は、侵害等が発生した場合は、当該侵害等が発生した所属の情報セキュリティ責任者と連携して、当該侵害等の記録を保存し、かつ、原因を究明の上、再発防止策を検討し、最高情報セキュリティ責任者に報告しなければならない。

2　最高情報セキュリティ責任者は、情報セキュリティ統括責任者から前項の規定による報告を受けたときは、その内容を確認し、再発防止策を実施するために必要な指示をしなければならない。

第２節　例外措置

（例外措置の許可）

第90条　情報セキュリティ統括責任者は、この規程を遵守することが困難な状況で、業務等を適正に遂行するため、この規程とは異なる方法を採用し、又はこの規程に規定された事項を実施しないことにつきやむを得ない理由がある場合は、理事長の許可を得て、例外措置を実施することができる。

（緊急時の例外措置）

第91条　情報セキュリティ統括責任者は、理事長の許可を得るいとまがなく、かつ業務等の適正な遂行に緊急を要し例外措置が不可避であると認めるときは、自らの判断により当該例外措置を実施することができる。

2　前項の場合において、情報セキュリティ統括責任者は、事後速やかに理事長に当該例外措置について報告しなければならない。

（例外措置の記録管理）

第92条　情報セキュリティ統括責任者は、例外措置の実施に関する記録を適切に保全しなければならない。

第３章　情報セキュリティ対策実施手順

（情報セキュリティ対策実施手順の策定）

第93条　情報システムを所管する情報セキュリティ責任者は、この規程を遵守し情報セキュリティ対策を円滑に実施するため、所管する情報システムにおける情報セキュリティ対策の具体的な実施事項等を明記した情報セキュリティ対策実施手順を策定しなければならない。

2　情報セキュリティ対策実施手順は、非公開とする。

（情報セキュリティ対策実施手順の必要的記載事項）

第94条　情報システムを所管する情報セキュリティ責任者は、情報セキュリティ対策実施手順において、次に掲げる事項を定めなければならない。

(1) 関係者間の連絡体制に関する事項
(2) 関係者の役割分担に関する事項
(3) 連絡又は報告をすべき内容に関する事項
(4) 証拠の記録及び保管に関する事項（第48条第４号及び第78条の期間を含む。）
(6) 関係機関への報告等に関する事項
(7) 物理的、人的及び技術的情報セキュリティ対策に関する事項
(8) 当該システムにおいて起こりうるリスク及び当該リスクへの対応に関する事項
(9) 緊急時におけるサーバー等の機器のオペレーションマニュアル

2　前項の規定にかかわらず、情報システムを所管する情報セキュリティ責任者は、情報セキュリティ対策実施手順に前項に掲げる事項以外の任意的記載事項を記載することができる。

第４章　外部サービスの利用

第１節　外部委託等

（契約の相手方の選定）

第95条　情報セキュリティ責任者は、契約の受託者等の選定に当たり、業務等の内容に応じた十分な情報セキュリティ対策が確保されることを確認しなければならない。

（選定条件）

第96条　情報セキュリティ責任者は、他の規程に別の定めがある場合を除き、次に掲げる情報セキュリティ対策を行うことを契約の受託者等を選定する条件とし、かつ同内容を契約の仕様に含めなければならない。

(1) 受託者等に提供する情報の当該受託者等による目的外使用の禁止
(2) 受託者等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
(3) 業務の実施に当たり、受託者等、その従業員、再委託等先その他の者による情報資産への意図せざる変更が加えられないための管理体制
(4) 受託者等の資本関係、役員等、契約履行実績、受託業務の実施場所並びに業務従事者の所属、技術的水準、実績及び国籍に関する情報
(5) 情報資産に対する侵害等への受託者等による対処方法
(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

2　情報セキュリティ責任者は、委託する業務において取り扱う学内データの格付等を勘案し、必要に応じて次に掲げる内容を仕様に含めなければならない。

(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　情報セキュリティ責任者は、受託者等が受託業務の一部を再委託する場合は、当該再委託により生じ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項の措置の実施を当該受託者等に担保させるとともに、再委託等先の情報セキュリティ対策の実施状況を確認するために必要な事項について本法人による承認を受けるよう、契約の仕様に含めなければならない。

（受託者等における情報の取扱い）

第97条　情報セキュリティ責任者は、受託者等への学内データの提供等において、次に掲げる事項を　遵守しなければならない。

(1) 提供する学内データを必要最小限とし、あらかじめ定めた安全な受渡方法により提供すること。

(2) 提供し、又は委託業務で使用し、若しくは作成した情報が受託者等において使用済み又は不要になった場合は、これを確実に返却させ、又は抹消させること。

(3) 委託業務の履行に当たり、情報セキュリティインシデント、学内データの目的外使用等、契約の内容又は関係法令若しくはこの規程その他の関連規程等に反する事項を覚知した場合は、直ちに情報セキュリティ責任者に報告させること。

（秘密保持契約）

第98条　情報セキュリティ責任者は、業務等の内容等に応じて必要と認めるときは、委託契約の締結に先立って、秘密保持契約を締結しなければならない。

（確認及び措置等）

第99条　情報セキュリティ責任者は、受託者等が必要な情報セキュリティ対策を確保していることを確認しなければならない。

2　前項の規定による確認の結果、不適当と認める事項がある場合は、情報セキュリティ責任者は、当該受託者等に対し必要な改善を求めなければならない。

3　情報セキュリティ責任者は、前項により求めた改善の履行が困難であると認められるときは、当該受託者等に対して業務の一時中断及び代替措置案の提出を求めることができる。

第２節　インターネット外部サービス

（インターネット外部サービスの利用）

第100条　利用者は、インターネット外部サービスを利用する場合は、他の規程において別の定めがある場合を除き、本条から第106条までの規定に従わなければならない。

（格付による利用制限）

第101条　利用者は、次条第１項の許可を得ることなく学内データをインターネット外部サービスで取り扱い、又は学内データの連絡手段として利用してはならない。

2　前項の規定は、格付規程による機密性１情報には、適用しない。

3　第１項の規定にかかわらず、特定の利用者のみの監督権限に属する情報であり、情報の漏洩、消失その他の事故等が発生した際においても、本法人及び第三者に直接の不利益が発生しない情報については、当該利用者は、情報セキュリティ責任者の許可を得ることなくインターネット外部サービスを用いて当該情報を取り扱うことができる。

（インターネット外部サービスの利用許可）

第102条　情報セキュリティ責任者は、所管する利用者においてインターネット外部サービスを用いて学内データを取り扱う業務等上の必要があると認める場合は、その利用を許可することができる。

2　情報セキュリティ責任者は、この規程において規定されていない外部サービスを利用する必要があると認める場合は、前項の規定に準じて利用を許可することができる。

（外部サービス利用要綱）

第103条　前条の許可を申請する利用者は、あらかじめ次に掲げる事項を定めた外部サービス利用要綱を策定しなければならない。

(1) 当該サービスを利用できる業務等の範囲

(2) 当該サービスで取り扱うことができる情報の範囲

(3) 利用手続及び運用手順

(4) 運用責任者となる利用者の職及び氏名

2　前項の規定にかかわらず、第１項の許可を申請する利用者は、当該規程に前項各号に掲げる

事項以外の事項を記載することができる。

（危険性の評価）

第104条　第102条第１項の許可を申請する利用者は、あらかじめ当該サービスの約款、各種の仕様、提供条件等その他の調査結果等に基づき、次に掲げる事項について検討を行い、危険性に関する評価を行わなければならない。

(1) 取り扱う情報の格付及び取扱制限に照らし、学内データの取扱いを委ねることの適否

(2) 当該サービスの提供事業者による学内データの二次利用の有無

(3) 当該サービスの運用場所、契約又は約款等に定める準拠法及び合意管轄等の適否

(4) 当該サービスの提供が中断し、又は終了した場合において、業務等を円滑に施行するための方法の存否及び当該方法の適否

(5) 当該サービスにおける情報セキュリティ対策の適否

(6) 当該サービス提供事業者に対する外部の者による情報セキュリティ監査の結果、各種の認定及び認証制度等の取得状況その他の情報から判断される当該サービス及び当該サービスの提供者の信頼性の程度

(7) 前6号に定めるもののほか、当該サービスの危険性の評価に必要な事項がある場合は、当該事項の適否

２　前項の調査、検討及び危険性の評価は、書証その他の客観的に確認できる証拠として記録され、及び保存されなければならない。ただし、公知の事実又は他の事実から容易に推定可能な事実については、この限りでない。

（許可の要件）

第105条　情報セキュリティ責任者は、次の各号の全てに該当する場合でなければ、その利用を許可してはならない。

(1) 当該サービスの利用が業務の遂行上必要不可欠であること。

(2) 通常の利用において、情報セキュリティを脅かすおそれがないこと。

(3) 前条第１項の評価がなされており当該評価の証拠が信頼できるものであること。

(4) 学内データの格付及び取扱制限に照らし、前条第１項の評価により想定されるリスクが許容できる範囲内のものであること。

(5) 既存の情報システムの運用に影響を及ぼさないこと。

(6) 当該外部サービスの利用が国公立大学又は医療機関における業務の遂行手段として社会通念上肯定できること。

(7) 格付及び取扱制限に従った学内データの取扱いが確保されること。

(8) 当該サービスの利用を否定すべきその他の事由がないこと。

（特定機密情報の利用許可）

第106条　情報セキュリティ責任者は、インターネット外部サービスを用いた特定機密情報に属する学内データの取扱いを許可してはならない。

２　前項の規定にかかわらず、情報セキュリティ責任者は、次のいずれかに該当する場合は、インターネット外部サービスを用いて特定機密情報を取り扱うことを許可することができる。

(1) 国、地方公共団体、独立行政法人、地方独立行政法人又はその他の個別法により設置が義務付けられた公的団体が提供するサービスの利用

(2) 前号の国又は団体等が民間事業者等に委託して運営するサービスの利用

(3) 第１号の国又は団体等が設置者である法人が提供するサービスの利用

(4) 情報の漏洩、消失その他の事故等が発生した際に本法人が負う損害賠償責任及び関連経費を当該サービス提供事業者が負担すること並びに秘密の保持について明文の合意がなされた日本国内の事業者が提供するサービスの利用

３　前２項の場合において、情報セキュリティ責任者は、格付規程第７条に規定する機密性５情

報のインターネット外部サービスによる処理を許可しようとするときは、あらかじめ情報セキュリティ総括責任者及び最高情報セキュリティ責任者の許可を得なければならない。

（サービス提供拠点等の地理的制約）

第107条　情報セキュリティ責任者は、サービス提供拠点又はサーバーその他の電子データを保存する機器等が日本の国外に設置されているインターネット外部サービスを用いた学内データの取扱いを許可してはならない。

2　前項の規定にかかわらず、情報セキュリティ責任者は、次のいずれかに該当する場合は、当該インターネット外部サービスの利用を許可することができる。

(1) 個人情報に該当しない学内データであり、かつ、サービスの運営事業者から漏洩又は第三者への情報提供等があっても本法人及び関係者に不利益をもたらさない学内データを取り扱う場合

(2) 国内の法人が運営するサービスであり、かつ、日本の国内法を契約の準拠法とする場合（当該サービスの運営等を外国の法人又は個人に委託等により行わせている場合を除く。）

(3) 次のア又はイに掲げる細分のいずれかに該当する場合

ア　個人情報の保護に関する法律（平成15年法律第57号）における、外国にある第三者への個人データの提供に該当しないとき。

イ　当該サービスの運営事業者が個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第３号）で定める要件を満たしている場合で、外国にある第三者への個人データの提供を認める旨の本人の同意があるとき。

（許可関係書面の保存）

第108条　インターネット外部サービスの利用の許可に関する全ての書面は、当該外部サービスの利用を終了した後、５年間保存しなければならない。

第３節　情報発信行為に関する追加規定

（外部サービス利用規程の追加記載事項）

第109条　第103条の規定にかかわらず、ソーシャルメディアサービスの使用等、情報発信を行うことを目的としてインターネット外部サービスの使用の許可を申請しようとする利用者は、同条に定める事項の他、次の各号に掲げる事項を外部サービス利用要綱に追加して規定しなければならない。

(1) 法人名、大学名、学内の所属名又は職名等を表示して運用しているアカウント等（以下「当該アカウント等」という。）からの情報発信が真正なものであることを明らかにするため、大学のウェブサイトに当該情報を掲載して相互に参照可能にし、かつ、当該アカウント等の運用組織を明示する等のなりすまし対策における相互参照先に関する事項

(2) パスワードその他の認証方法及びこれらを記録した媒体等を厳格に管理し、当該アカウント等の乗っ取りに対する対策を行うための管理方法に関する事項

(3) その他当該アカウント等の正常な利用を侵害する行為を防止するために必要な措置に関する事項

（発信する情報の制限等）

第110条　利用者は、情報資産等又はインターネット外部サービスを用いて、次に掲げる情報発信行為をしてはならない。

(1) 公序良俗に反する情報

(2) 真偽のいずれかにかかわらず、特定の個人又は法人の不利益となるおそれのある情報

(3) 他者の権利、法益若しくは名誉を傷つけ、又は静謐な生活を妨げる情報

(4) 特定の企業又は事業者等の便宜又は利益となる情報

(5) 社会通念上大学又は医療機関が発信することがふさわしくない情報

(6) その他大学に対する信頼を損なうおそれがある情報

2　第１項第４号の規定は、本法人における業務等を公表するに当たり当該企業又は事業者等の名称を公表することが必要又は妥当と認められる場合で、かつ、当該公表によって当該企業又は事業者等に発生が推定される便宜又は利益が社会通念上相当な範囲と認められる場合には、適用しない。

3　第103条第１項第４号の運用責任者は、前項に該当する場合を除き、第１項の規定に違反する情報発信を発見した場合は、速やかに当該情報を削除の上、第85条の場合に準じて必要な報告をしなければならない。

第５章　違反及び処分等

（法令遵守）

第111条　関係法令並びに第５条、第８条、第10条、第11条、第24条から第26条まで、第28条から第30条まで、第71条、第73条、第76条、第81条、第84条第３項、第101条、第110条及び第119条の規定に違反した教職員等及び学生等並びにこれらを監督する職責にある者は、違反の程度、被害又は損害の発生状況等に応じ懲戒処分等の対象とする。

2　前項に規定する以外の規定に違反した教職員等及び学生等並びにこれらを監督する職責にある者は、違反の程度、被害又は損害の発生状況、違反状況の解消の有無その他の事情を勘案の上、懲戒処分等の適否を審議する。

（違反発見時の対応）

第112条　情報セキュリティ統括責任者は、自らが利用者によるこの規程その他の関係規程等に違反する行為を覚知した場合は、当該違反者を所管する情報セキュリティ責任者に連絡し、適切な措置を指示しなければならない。

2　情報セキュリティ責任者等は､自らが所管しない利用者による前項の行為を覚知した場合は、速やかに情報セキュリティ統括責任者及び当該違反者を所管する情報セキュリティ責任者に報告し、適切な措置を要請しなければならない。

3　前２項の指示又は要請を受け、又は自らが所管する利用者による第１項の行為を覚知した情報セキュリティ責任者は、当該違反者に対して必要な指導又は指示を行うとともに、情報セキュリティ統括責任者にその状況等を報告しなければならない。

（利用者による通告）

第113条　利用者は、他の利用者によるこの規程その他の関係規程等に違反する行為を覚知した場合は、自己を所管する情報セキュリティ責任者等に報告しなければならない。

（利用権限の停止又は剥奪）

第114条　第112条の場合において、情報セキュリティ統括責任者又は情報セキュリティ責任者の指導又は指示によっても違反が改善されない場合は、情報セキュリティ統括責任者又は情報セキュリティ責任者は、当該違反者の情報システム又はネットワークを利用する権限を一時停止し、又は剥奪することができる。

2　情報セキュリティ責任者は、前項の権限の一時停止又は剥奪を行った場合は、情報セキュリティ統括責任者及び当該違反職員等の所属を所管する情報セキュリティ責任者に対し速やかに当該一時停止又は剥奪について報告しなければならない。

3　情報セキュリティ統括責任者は、前項の規定による報告を受けた場合又は自ら第１項の規定による権限の一時停止又は剥奪を行った場合は、最高情報セキュリティ責任者に対し、速やかに当該一時停止又は剥奪について報告しなければならない。

（聴聞）

第115条　前条の規定により情報システム又はネットワークを使用する権限を一時停止し、又は剥奪しようとする情報セキュリティ統括責任者又は情報セキュリティ責任者は、当該一時停止又は剥奪の決定の前に聴聞を行い、違反者に対して弁明の機会を付与しなければならない。

2　前項の聴聞は、情報セキュリティ統括責任者が主宰する。

3　違反者及び当該違反者を所管する情報セキュリティ責任者は、第１項の聴聞に出席しなければならない。
4　情報セキュリティ統括責任者は、自らの補佐人を聴聞に参加させることができる。
5　第3項の情報セキュリティ責任者は、情報セキュリティ統括責任者の承認を得て、自ら及び違反者の補佐人を聴聞に参加させることができる。
（仮処分）
第116条　前条の規定にかかわらず、情報セキュリティ統括責任者は、違反行為に関連して情報セキュリティ対策上の危険が生じるおそれがあると認めるときは、聴聞の実施前に情報システム又はネットワークの一時利用停止の仮処分を行うことができる。
（即時停止）
第117条　情報セキュリティ統括責任者及び情報システムを所管する情報セキュリティ責任者は、違反行為に関連して情報セキュリティ対策上の危険が生じている場合で、かつ、次に掲げる場合に該当するときは、自らの判断により情報システム又はネットワークを即時停止とすることができる。
(1) 第112条第３項の情報セキュリティ責任者による指導又は指示を待つ暇がないと認められる場合
(2) 違反者が不明又は不在の場合
（準用規定）
第118条　第114条第２項及び第３項の規定は、第116条の仮処分及び前条の即時停止の場合に準用する。
第５編　評価及び改正
第１章　情報セキュリティ監査
（監査の実施）
第119条　情報セキュリティ監査責任者は、所属等における情報セキュリティ対策の実施状況及びこの規程に定める責務等の履行状況について、監査実施計画を策定のうえ情報セキュリティ監査を行うことができる。
2　情報セキュリティ監査責任者は、前項の監査実施計画につき、あらかじめ最高情報セキュリティ責任者の承認を得なければならない。
3　前２項に定めるもののほか、最高情報セキュリティ責任者は、情報セキュリティの状況に応じ、情報セキュリティ監査責任者に対し監査の追加実施を求めることができる。
（受託者等への監査）
第120条　情報セキュリティ監査責任者は、再委託事業者等を含む受託者等に対し、契約書等において合意された範囲において、契約に定める義務の履行状況について監査を行うことができる。
（受監義務）
第121条　監査の対象とされた所属等に属する者は、監査の実施を拒むことができない。
2　前項の所属等に属する者は、監査の実施に協力しなければならない。
（監査の実施及び報告）
第122条　情報セキュリティ監査責任者は、監査の実施後、監査結果を監査報告書として取りまとめの上、最高情報セキュリティ責任者に報告しなければならない。
（監査結果に応じた対処）
第123条　最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘された事項等に対する改善計画の策定等を情報セキュリティ統括責任者及び情報セキュリティ責任者に指示することができる。
2　情報セキュリティ統括責任者及び情報セキュリティ責任者は、前項の規定による指示を受け

た場合は、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告しなければならない。

第２章　見直し及び改正

（教育、訓練及び監査結果等の活用）

第124条　情報セキュリティ統括責任者は、情報セキュリティ対策に関する教育、訓練及び監査等の実施結果並びに情報セキュリティインシデントの発生原因その他の必要な事項を分析し、適時に情報セキュリティ対策上の危険性を評価しなければならない。

（対策等の見直し）

第125条　統括情報セキュリティ責任者は、前条の規定による評価及び情報セキュリティに関する環境等の変化等を踏まえ、時宜に応じた情報セキュリティ対策の見直しを図らなければならない。

２　利用者は、情報セキュリティ対策の見直しをすべき事項を覚知したときは、速やかに情報セキュリティ責任者に報告しなければならない。

３　情報セキュリティ責任者は、前項の場合において必要と認めるときは、情報セキュリティ統括責任者に協議しなければならない。

（規程の改正）

第126条　理事長は、第123条の規定による評価及び前条の規定による見直し並びに情報セキュリティに関する社会環境及び技術環境の変化を踏まえ、適時に、この規程の改正その他の効果的な情報セキュリティ対策を実施するものとする。

附　則（令和■年■月■日規程第■号）

（施行期日）

１　この規程は、平成　年　月　日から施行する。

（規程の廃止）

２　次に掲げる規程は廃止する。

(1) 札幌医科大学情報セキュリティ基本方針（平成24年３月８日附属総合情報センター運営委員会決定）

(2) 札幌医科大学情報セキュリティ対策基準（平成24年３月８日附属総合情報センター運営委員会決定）

（経過措置）

３　本規程の施行の日から1年を経過する日以前に運用を開始した情報システムについては、当該情報システムの次期更新の時まで、第33条は適用しない。

４　第36条第４項の規定は、本規程の施行の日から１年を経過するまでの間は、適用を猶予する。

５　第52条第３項の規定は、本規程の施行の日から６月を経過するまでの間は、適用を猶予する。

６　第26条、第34条、第48条、第49条、第57条、第66条、第76条、第４編第４章第２節及び第３節の規定は、該当する事実があった時又は該当する機器等若しくはサービス等の利用開始の時に遡って適用する。