

札幌医科大学情報セキュリティ対策基準

第1章 総則 (趣旨)

第1 この基準は、札幌医科大学（以下「本学」という。）情報セキュリティ基本方針第6に基づき、本学の情報セキュリティ対策に関し必要な事項を定めるものである。

第2章 組織及び体制 (情報セキュリティ統括者及び情報セキュリティ副統括者)

第2 情報セキュリティ対策を適正かつ確実に行うため本学に情報セキュリティ統括者及び情報セキュリティ副統括者を置く。

- 2 情報セキュリティ統括者は学長とし、情報セキュリティ副統括者は附属情報センター所長とする。
- 3 情報セキュリティ統括者は、評議会及び運営委員会の議を経てセキュリティ対策の重要事項の決定に当たる。
- 4 情報セキュリティ副統括者は、情報セキュリティ統括者を補佐するとともに、この基準に定める事務を処理する。

(情報セキュリティ管理者)

第3 情報セキュリティ対策を各所属において適正かつ確実に実施するために、情報セキュリティ管理者を置く。

- 2 情報セキュリティ管理者は、各所属における所属長とし、所管する所属において次の業務を行う。
 - (1) 情報セキュリティ対策の実施及び状況の把握
 - (2) 教職員等に対する情報セキュリティ対策に関する啓発及び研修の実施
 - (3) 情報セキュリティ対策に関する事故等の報告
 - (4) 緊急時における情報セキュリティ副統括者への報告
 - (5) 第1号から前号までに掲げるもののほか、情報セキュリティ統括者が定めた事項の実施に必要な事項
- 3 情報セキュリティ管理者は、前項に定める業務の全部又は一部をあらかじめ指定した教職員等に補助させることができる。

(情報システム管理者)

第4 各情報システムにおける情報セキュリティ対策を適正かつ確実に実施するため、情報システム管理者を置く。

- 2 情報システム管理者は、情報システムの開発又は運用を所管する者であって、所管する情報資産に関して次の業務を行う。
 - (1) 管理する情報システムについての情報セキュリティ対策実施手順の策定
 - (2) 情報セキュリティ対策の実施と状況の把握
 - (3) 情報セキュリティ対策実施手順の改定
 - (4) 障害発生時の情報セキュリティ副統括者への連絡
 - (5) 情報システムの開発又は運用を担当する教職員等の情報セキュリティ対策に関する知識習得の支援
- 3 情報システム管理者は前項に定める業務及び所管する情報資産に関する業務の全部又は一部をあらかじめ指定した教職員等に補助させることができる。

(教職員等)

第5 教職員等は、この基準に定められている事項を遵守し、情報セキュリティの侵害等の問題発生を未然に防止するように努めるとともに、当該問題を発見した場合は速やかに、情報セキュリティ管理者に報告するなど適切な措置を執らなければならない。

(外部委託)

第6 情報システムの開発及び運用管理を事業者へ委託しようとする情報システム管理者は、この基準の遵守義務や知り得た情報の守秘義務を認識させるとともに、この基準が遵守されなかった場合の損害賠償等の規定を契約書等に明記すること。

第3章 情報資産の管理

(情報資産の管理責任)

第7 情報システム管理者は、所管する情報資産についての管理責任を有する。

- 2 情報システム管理者は、所管する情報資産に関して次の業務を行う。

- (1) 情報の利用目的とアクセス権限の設定
- (2) 情報資産に対する脅威となり得る事項の把握と情報セキュリティ対策の実施
- (3) 第1号から前号までを実施するために必要な事項

(情報の利用目的とアクセス権限の設定)

第8 情報システム管理者は、管理する情報の利用目的を明らかにするとともに、情報の利用者に対して、その利用目的に沿ったアクセス権限を設定しなければならない。

(情報資産に対する脅威の把握と情報セキュリティ対策の実施)

第9 情報システム管理者は、次に掲げる事項その他の管理する情報資産に対する脅威となり得る事項を明らかにするとともに、その発生度合や発生した場合の影響等から特に脅威となり得る事項については重点的な対策を講ずるものとする。

- (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及びプログラムの持出し、盗聴、改ざん、消去、機器及び媒体の盗難、障害発生行為によるサービスの停止等
- (2) 教職員等及び受託事業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出し、盗聴、改ざん、消去、機器及び媒体の盗難並びに規定外の端末接続によるデータ漏えい等
- (3) 地震、落雷、火災等の災害及び事故、故障等によるサービスの停止

2 情報システム管理者は、適切な情報セキュリティ対策を講ずることが困難な状況が生じた場合には、その状況について情報セキュリティ副統括者へ報告しなければならない。

(情報資産の管理方法)

第10 情報システム管理者は、取り外し可能な記録媒体で情報を保管する場合、次の措置を施さなければならない。

- (1) 最終的に確定した情報を記録した媒体は、書込み及び消去の禁止の措置を行った上で保管すること。
- (2) 情報を記録した媒体は、施錠管理すること。
- (3) 情報を記録した媒体を外部業者に貸与する場合に複製の禁止や媒体管理に関するルールを定めること。
- (4) 情報を記録した媒体が不要になった場合に、情報の復元が不可能な消去方法や記録媒体を粉砕する等の方法を施して、情報を完全に再利用不可能な状態とした後破棄すること。

2 情報システム管理者は、管理する情報をネットワーク又は記録媒体により他の情報システムに提供する場合は、その取扱いに関し必要な事項をあらかじめ提供を受ける情報システム管理者に連絡するものとする。

3 前号の規定による提供を受けた情報システム管理者は、その取扱いに関し必要な事項に留意し、適切に管理しなければならない。

第4章 物理的セキュリティ対策

(重要な情報処理機器の取付け)

第11 情報システム管理者は、ネットワークを構成する機器の取付けに当たっては、火災、水害、埃、温度、湿度等の影響を可能な限り排除した場所に設置しなければならない。

(管理区域)

第12 情報システム管理者は、学内の基幹システムのサーバ等、重要な情報処理機器については、設置場所を常時施錠し、また、当該設置場所に入室できる者については、事前に承認を与えるなどして、入退室管理を行わなければならない。なお、他のサブシステムにおいては、情報システム管理者の責任において、所管する情報処理機器をセキュリティ上適正に管理しなければならない。

(執務室等の施錠管理)

第13 情報セキュリティ管理者は、執務室等に教職員等がいない場合は、執務室等の出入口を施錠するなどしてパソコン等の盗難防止に努めなければならない。

第5章 人的セキュリティ対策

(教育)

第14 情報セキュリティ統括者は、教職員等に対し、研修の実施等の情報セキュリティ対策に関する啓発を行うよう努めなければならない。

2 情報セキュリティ管理者、情報システム管理者及び教職員等は、指定された研修に参加し、情報セキュリティ対策に関する知識の習得及び関連規程等の理解をしなければならない。

(情報システムの利用)

第15 教職員等は、学習、教育、研究、業務目的（以下「業務等」という。）以外に情報システムを利

用してはならない。

- 2 教職員等は、情報システム利用のために発行された認証情報及びカード等の認証媒体については、情報システム管理者が定める実施手順を遵守し、漏えい及び紛失のないよう留意しなければならない。また、認証情報については、安易に判明するようなものは使用せず、定期的に変更するようにしなければならない。
- 3 教職員等は、情報システムの利用に際し、当該情報システムへのログイン時間が必要最小限になるように留意するとともに、離席時には、原則としてログアウトしなければならない。

(パソコン等の管理)

- 第16 教職員等は、ネットワークに接続されている各情報システム管理者及び各情報セキュリティ管理者が管理するパソコン等を執務室等外に持ち出してはならない。業務等の都合によりやむを得ず持ち出す場合には、理由及びパソコン等の管理番号を当該管理者に申告し、承認を得なければならない。
- 2 教職員等は、情報システム管理者の承認を得ないでパソコン等をネットワークに接続してはならない。
- 3 教職員等は、情報システム管理者が許可した以外のアプリケーションソフト等を情報システム管理者が管理するパソコン等にインストールしてはならない。業務等上必要な場合は、理由及びインストールするアプリケーションソフトの名称を当該パソコン等を管理する情報システム管理者に申告し、許可を得なければならない。
- 4 教職員等は、情報システム管理者が管理するパソコンに対し、改造、機器の増設・交換、ネットワークとの切り離し、接続等を行ってはならない。業務等上必要な場合は、理由及び変更の内容を当該パソコン等を管理する情報システム管理者に申告し、許可を得なければならない。

第6章 技術的セキュリティ

(技術の活用)

- 第17 情報システム管理者は、情報システムのより高度な安全性及び信頼性を確保するため、常に最新の情報技術に関する知識を獲得し、その評価に努めなければならない。

(情報システムの開発・運用)

- 第18 情報システム管理者は、情報システムを調達しようとする際、当該情報システムで必要となるセキュリティ要件を調達仕様書に記述しなければならない。
- 2 情報システム管理者は、ハードウェア及びソフトウェアを導入する際、当該製品が情報セキュリティの確保の上で問題のないことを確認しなければならない。
- 3 情報システム管理者は、設計、製造、テスト及び導入後の運用の各段階において、情報セキュリティ機能の品質を適切に管理しなければならない。
- 4 情報システム管理者は、情報システムが安定的に稼働することができるよう、適切な保守作業を実施しなければならない。また、保守作業等により情報システムを停止する場合には、教職員等に周知しなければならない。
- 5 情報システム管理者は、記録媒体が含まれる機器の修理を外部の事業者へ委託する場合には、記録された情報を完全に消去した上で修理を依頼することとする。この対応が困難な場合には、委託契約書上に情報の守秘に関する条項を明記する等の情報について適切な取扱いを求めなければならない。
- 6 情報システム管理者は、記録媒体が含まれる機器の廃棄を外部の事業者へ委託する場合には、記録された内容を完全に消去し、又は復元不可能な状態にして行わなければならない。

(情報システムのアクセス制御)

- 第19 情報システム管理者は、所管する情報システムに対し、当該情報システム及びその扱う情報の重要度に応じた、適切な利用者認証の仕組みを組み込まなければならない。
- 2 各情報システム管理者は、当該情報システムの実施手順に従って、利用者の登録、変更及び抹消を行わなければならない。

(ネットワークのアクセス制御)

- 第20 ネットワークを管理する情報システム管理者は、不正アクセスを防止するため、適切な経路制御を施さなければならない。
- 2 ネットワークを管理する情報システム管理者は、管理するネットワークを外部のネットワークと接続する場合には、当該外部ネットワークの構成及びセキュリティレベルを詳細に検討しなければならない。
- 3 ネットワークを管理する情報システム管理者は、接続されている外部ネットワークの情報セキュリティ対策に問題が認められ、本学の情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークを物理的に切り離さなければならない。
- 4 ネットワークを管理する情報システム管理者は、管理するネットワークをインターネットに接続す

る場合、管理するネットワーク内からのインターネット利用に対し、必要があれば、適切なフィルタリング処理を行う等、業務等の利用目的以外の使用を制限するとともに不正な使用が発見された場合には、適切な措置を施さなければならない。

- 5 情報システム管理者は、教職員等によるネットワーク外部からのアクセスについては、それぞれの情報システムの特性に応じ、適切な対策を講じなければならない。
- 6 情報システム管理者は、不正アクセス等を防止するため定期的に認証情報調査を実施し、該当者に対し、適切な処置を講じなければならない。
- 7 ネットワークを管理する情報システム管理者は、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）に違反する行為が行われたおそれがある場合には、当該不正アクセス等の記録の保存に努めるとともに、警察及び関係機関との密接な連携の下、迅速な対応に努めなければならない。

（コンピュータウィルス対策）

- 第21 情報セキュリティ統括者は、常にコンピュータウィルス（以下「ウィルス」という。）に関する最新の情報の収集に努めるとともに、必要に応じて教職員等へ情報提供を行わなければならない。
- 2 情報セキュリティ統括者は、ウィルス感染時等の対応マニュアルを教職員等に周知徹底させるとともに、ウィルスの発生状況を常に把握していなければならない。
 - 3 情報セキュリティ統括者は、ウィルス発見時には教職員等に適切な指示を与えなければならない。また、必要に応じて外部組織へも連絡を行わなければならない。
 - 4 情報システム管理者は、その管理するすべてのパソコンにウィルス対策ソフトを導入しなければならない。また、サーバについても必要に応じて同様の措置を講じなければならない。
 - 5 情報システム管理者は、その管理するサーバ及びパソコン上に導入したウィルス対策ソフト用のパターンファイルが常に最新の状態となるよう維持しなければならない。
 - 6 教職員等は、光ディスク、磁気ディスク、電子メールの添付ファイル及びネットワーク経由でのファイルのダウンロード等の手段により、外部との間でデータを授受する場合には、必ずウィルスチェックを行わなければならない。
 - 7 教職員等は、ウィルスを発見した場合は、速やかに情報システム管理者へ連絡し、適切な指示を受けなければならない。

（記録の取得と管理）

- 第22 情報システム管理者は、情報システムを用いた業務等が定められた手順等に基づき処理されたことを確認するため、システムへのアクセス記録、システム変更等の記録、障害記録、その他情報セキュリティの確保に必要な記録を取得しなければならない。
- 2 情報システム管理者は、前項の記録が窃取され、改ざんされ、又は消去されないよう必要な措置を講じなければならない。

第7章 運用

（情報セキュリティ実施手順の策定）

- 第23 情報システム管理者は、この基準を遵守して情報セキュリティ対策を実施するため、管理する情報システムのそれぞれについての情報セキュリティ対策の具体的な手順を明記した情報セキュリティ実施手順（以下「実施手順」という。）を策定しなければならない。

（情報セキュリティ実施手順の策定にかかる指導及び助言）

- 第24 情報セキュリティ統括者は、情報システム管理者の実実施手順の策定に当たり、適切な指導及び助言を行うことができる。

（障害時の対応）

- 第25 教職員等は、情報セキュリティ対策に関する事故、不正アクセス及び操作不適により生じたシステム上の欠陥及び誤作動（以下「事故等」という。）を発見した場合には、速やかにその旨を情報セキュリティ管理者に報告し、情報セキュリティ管理者の指示に従い、必要な措置を講じなければならない。
- 2 情報セキュリティ管理者は、前項の事故等への対応策について情報システム管理者に協議するとともに、教職員等又は関係する者に必要な措置を講ずるよう指示しなければならない。また、速やかに事故の発生及び対応状況について、情報セキュリティ副統括者に報告しなければならない。
 - 3 情報システム管理者は、情報資産への侵害が明確になった場合における連絡、情報システムの保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講ずるために、次の項目からなる障害時対応手順を策定しなければならない。
 - （1）障害時の連絡体制及び責任者
 - （2）障害内容の調査方法
 - （3）証拠の記録及び保管

- (4) 障害への対処方法
- (5) 再発防止の措置
- (6) 関係機関への報告
- (7) 第1号から前号までに掲げるもののほか、障害時対応として必要な事項

4 情報システム管理者は、環境の変化や情報セキュリティ技術の変化に応じて、適宜障害時の対応手順の見直しを行わなければならない。また、必要に応じて障害時対応の訓練計画を策定し、実施しなければならない。

(法令遵守)

第26 教職員等にあつては、情報資産を使用する業務等の遂行に当たっては、地方公務員法（昭和25年法律第261号）、著作権法（昭和45年法律第48号）、不正アクセス行為の禁止等に関する法律、北海道個人情報保護条例（平成6年3月31日条例第2号）、北海道文書管理規程（平成10年3月31日訓令7号）、北海道電子情報管理要綱（平成15年9月29日法文第798号）、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成14年法律第137条）等の関係する法令等を遵守しなければならない。

2 教職員等は、本学のネットワークの利用については、各情報システム管理者が定める実施手順を、公式ホームページの管理・運営については、「札幌医科大学公式ホームページの管理及び運営方針」、「ホームページによる情報公開に関するガイドライン」、「ホームページ作成・改訂のための技術マニュアルーガイドライン」及び「札幌医科大学公式ホームページプライバシーポリシー」を遵守しなければならない。

(本基準の公開)

第27 この基準は、情報セキュリティ対策を効果的に実施するため、原則として非公開とする。

(監査等)

第28 各情報システムにおける情報セキュリティ対策の実施状況及びセキュリティポリシーが遵守されているかどうかについて、監査等により定期的に検証されなければならない。

(点検)

第29 情報システム管理者は、管理する情報システムの情報セキュリティについて、定期的に点検を行わなければならない。

(評価及び見直し)

第30 情報セキュリティ統括者は、新たな情報セキュリティ対策の実施が必要な場合、又は情報セキュリティ実施状況の監査及び点検により問題点が発見された場合には、この基準等の実効性を評価し、当該部分の改定を行わなければならない。

附 則

この基準は、平成24年4月1日から施行する。