公立大学法人大分県立看護科学大学情報セキュリティ基本方針に関する規程

平成２４年　５月　１日
規程第　　１０１　号

（目的）第一条 公立大学法人大分県立看護科学大学（以下「本学」）情報セキュリティ基本方針に関する規程（以下「基本方針」という。）は、本学の保有する情報資産に関する機密の保持及び正確さの維持を確保するため、情報資産の取り扱いと情報セキュリティ対策に対する基本的な考え方を定めることにより、情報資産の管理徹底を図り、安全で円滑な業務の遂行と、本学に対する学外の信頼を確保することを目的とする。

（用語の定義）第二条 基本方針において掲げる用語は、以下の各号の定義するところによる。一 情報セキュリティ　情報資産の機密性を保持し、完全性及び正確性を維持するとともに、予め許可された範囲内においては必要とする情報資産の利用を確実に出来る状態を確保することをいう。

二 情報資産　本学が業務において取り扱うすべての情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）をいう。三 情報システム　ハードウェア、ソフトウェア、プログラム、ネットワーク及び記録媒体で構成されるもので、これら全体を用いて教育・研究および事務処理を行うための情報処理の体系をいう。

四 ネットワーク　電子計算機、関連機器等の多目的利用及び各種オンラインシステムのデータ伝送を目的とした構内及び施設間通信網により構築された情報通信基盤をいう。五 アクセス　情報資産に対し、何らかの利用目的を持って接触又は接続することで、大学の業務に関する資料および帳票や簿冊等の記載内容を閲覧・転記するために接すること及び情報システムへネットワークを介したデータ取得のために端末を接続すること等をいう。

（適用範囲）第三条 基本方針の適用範囲は、情報資産に接するすべての教職員（臨時的任用又は非常勤の職にある者を含む。以下「職員等」という。）とする。

（職員等の義務）

第四条 すべての職員等に対して基本方針及び関連法令等の趣旨を理解・認識し、遵守させるため必要な措置を講じる。また、業務委託等により従事する事業者（下請けを行う者を含む。以下「学外業者」という。）に対しても、業務委託等により知り得た情報の守秘義務を認識させるため、契約又は別途取決めを行い、情報セキュリティの確保に必要な措置を講じる。

２ 職員等は、基本方針及び関係法令等の趣旨を尊重し、自らの行動が大学の業務の信用に影響を及ぼすことを強く認識したうえで、本学の情報資産に接するにあたっては最大限の配慮を払う等、本学の情報セキュリティの確保及び維持に対して、自発的で最善の努力をしなければならない。

（情報セキュリティ管理体制）第五条 基本方針に基づく情報セキュリティの確保・維持を担保するため、最高情報統括責任者、情報セキュリティ責任者及び管理者を置く。
２ 最高情報統括責任者、情報セキュリティ責任者及び管理者は、本学の保有する情報資産について、それぞれの所掌に応じて、自ら率先して情報セキュリティ対策を推進・管理するものとし、以下の各号に掲げる者をもって充てる。

一 最高情報統括責任者 理事長二 情報セキュリティ責任者　情報ネットワーク委員会の長三 情報セキュリティ管理者　情報ネットワーク委員のセキュリティ管理担当者３ 情報ネットワーク委員会は、本学の情報資産に関する一元的な情報セキュリティ対策を実施するとともに、本学の情報セキュリティの確保や維持に係る各種施策の評価及び見直し並びに教育・啓発等を行い、必要な施策を理事長に助言するものとする。

（情報資産の分類）第六条 本学の保有する情報資産を調査し、保護すべき資産を特定するとともに、それぞれの重要度に応じて情報セキュリティを確保するため、分類を行う。

（情報資産への脅威）第七条 本学の情報資産を前条の分類に基づき、特に次の各号に掲げる事項を認識のうえ、各々の情報資産に対する様々な脅威の規模及びその発生頻度並びに情報管理の脆弱性を特定するものとする。

一 物理的脅威　地震、落雷、火災等の災害による施設の倒壊や電力供給の停止、情報システムの事故及び故障、悪意を持った部外者の侵入並びにネットワークの回線異常による正常なサービスの停止

二 人的脅威

職員等及び学外業者による誤操作、パスワードの不適正管理、故意の不正アクセス又は不正操作による情報資産の持出・盗聴・不正利用・改ざん・損壊・複製、機器及び記録媒体の盗難及び無許可のアクセスによるデータ漏えい等

三 技術的脅威　部外者による故意の不正アクセス又は不正操作による情報資産の持出・盗聴・不正利用・改ざん・損壊、機器及び記録されたデータの盗難、コンピュータウイルスの侵入、故意の障害発生行為等

（情報セキュリティ対策）第八条 前条により特定された脅威から情報資産を保護するため、次の各号に掲げるセキュリティ対策を講ずるものとする。一 物理的セキュリティ対策　情報システムを設置する場所への不正な立入り、情報資産への損傷・妨害等から保護するため、適切な設備設置、入退室管理及び盗難防止対策等、物理的な対策を講ずる。

二 人的セキュリティ対策　情報セキュリティ管理者を定め、職員等に基本方針及び情報セキュリティに関する法令等の内容を周知し、守秘義務を徹底する等、十分な教育及び啓発を行うため、必要な対策を講ずる。

三 技術的セキュリティ対策　情報資産を外部からの不正なアクセス等から適切に保護するため、ネットワーク管理、情報資産へのアクセス制御、コンピュータウイルス対策等の技術面の対策を講ずる。

四 運用におけるセキュリティ対策　基本方針及び情報セキュリティに関する法令等の遵守状況の確認、情報システムへの接続記録を取得・分析する等、運用面の対策を講ずる。また、緊急事態が発生した場合に迅速な対応を可能とするための危機管理対策を講ずる。

２ 技術面、費用面等の制約から、基本方針等に定められた対策基準の達成が極めて困難な場合には、情報ネットワーク委員会に報告し、承認を得るものとする。

（情報セキュリティ対策ガイドラインの策定）第九条 前条の対策を講ずるに当たって、遵守すべき行為及び判断等の基準を一元的に定めるため、必要となる基本的な要件を明記した「情報セキュリティ対策ガイドライン」（以下「対策ガイドライン」という。）をそれぞれの所掌に応じて策定するものとする。

（情報セキュリティ実施手順の策定）第十条 基本方針及び対策ガイドラインを遵守して情報セキュリティ対策を実施するため、個々の情報システムについて、所管する所属において具体的な実施手順を明記した「情報セキュリティ実施手順」（以下「実施手順」という。）を策定するも

のとする。

（職員の教育）第十一条基本方針及び対策ガイドラインの職員等への浸透と情報セキュリティ意識の向上を図るため、研修、説明会、その他の啓発活動等、情報セキュリティに関する教育内容を策定し、実施するものとする。

（違反への対応）第十二条職員等が基本方針に違反する行為を行ったと認められる場合は、その違反の程度に応じ、公立大学法人大分県立看護科学大学職員就業規則に基づく懲戒処分、訓告又は厳重注意等の人事管理上必要な処分等を講ずるものとする。

（事故発生時の対応）第十三条職員等は、情報システムに事故や欠陥を発見した際には、直ちに情報セキュリティ管理者へ報告し、その指示に従わなければならない。２ 情報セキュリティ管理者は、情報システムの障害を直ちに復旧し、事故等の障害原因を分析するとともに、必要に応じて再発防止策を講じなければならない。

（情報セキュリティ実施状況の検証）第十四条基本方針及び対策ガイドラインが遵守されていることを確認するため、定期的に情報セキュリティ実施状況の検証を行う。

（評価及び見直しの実施）第十五条前条に基づく情報セキュリティ実施状況の検証結果等を踏まえ、本学の情報セキュリティを取り巻く状況の変化に対応するため、基本方針に定める各規定並びに別途定める対策ガイドライン及び実施手順の評価及び見直しを適宜行う。

附 則 （施行期日）１この規程は、平成２４年５月１日から施行する。