北海道情報大学情報セキュリティ対策基本規程

（目　的）

第１条　この規程は、北海道情報大学（以下「本学」という。）における情報セキュリティ対策について基本的な事項を定め、もって本学が保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図ることを目的とする。

（用語の定義）

第２条　この規程における用語の定義は、次の各号に定めるところによる。

（１）　情報

- 教職員等が職務上使用することを目的として本学が調達又は開発した情報処理若しくは通信の用に供するシステム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）
- その他の情報システム又は外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）であって、教職員等が職務上取り扱う情報
- 同号に掲げるものの他、本学が調達又は開発した情報システムの設計又は運用管理に関する情報

（２）　情報システム

ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいい、特に断りのない限り、本学が調達又は開発するもの（管理を外部委託しているシステムを含む。）若しくは本学の情報ネットワークに接続されるものをいう。

（３）　学生等

学校法人電子開発学園北海道情報大学学則（以下「学則」という。）第３条に定める学部・学科及び課程に在籍する者、及び学則第３条の２に定める大学院に在籍する者、並びに学則第８章に定める聴講生、科目等履修生、特別科目等履修生、委託生及び研究生として学長に許可された者、その他、情報センター長が認めた者をいう。

（４）　教職員等

学校法人電子開発学園就業規則第２条に定める教職員の他、非常勤教職員（派遣職員を含む）その他、情報センター長が認めた者をいう。教職員等には、勤務条件により、一時的に受け入れる者を含むものとする。

（５）　利用者

学生等及び教職員等で、本学の情報システムを利用する許可を受けて利用する者をいう。

（６）　臨時利用者

学生等及び教職員等以外の者で、本学の情報システムを臨時に利用する許可を受けて利用する者をいう。

（７）　外部委託

本学の情報処理業務の一部又は全部について、契約をもって外部の者に実施させることをいい、「委任」「準委任」「請負」の契約形態を問わないものとする。

（８）　機器等

情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

（９）　記録媒体

情報が記録され、又は記載される有体物をいう。記録媒体には、文字、図形等人の知覚によって認識することができる情報が記載された紙その他の有体物（以下「書面」という。）と、電子的方式、磁気的方式その他人の知覚によっては認識することができない

方式で作られる記録であって、情報システムによる情報処理の用に供されるもの（以下「電磁的記録」という。）に係る記録媒体（以下「電磁的記録媒体」という。）がある。
また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ等の外部電磁的記録媒体がある。

（１０）　サーバ装置

情報システムの構成要素である機器のうち、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キーボードやマウス等の周辺機器（以下「周辺機器」という。）を含む。）をいい、特に断りがない限り、本学が調達又は開発するものをいう。

（１１）　端末

情報システムの構成要素である機器のうち、利用者が情報処理を行うために直接操作するもの（周辺機器を含む。）をいう。特に断りがない限り、本学が調達又は開発するものをいい、モバイル端末も含まれる。本学が調達又は開発するもの以外は、「本学支給以外の端末」といい、端末及び本学支給以外の端末の双方を合わせて「端末（支給外端末を含む）」という。

（１２）　モバイル端末

端末のうち、必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

（１３）　通信回線

複数の情報システム又は機器等（本学が調達等を行うもの以外のものを含む。）の間で所定の方式に従って情報を送受信するための仕組みをいい、特に断りがない限り、本学の情報システムにおいて利用される通信回線を総称したものをいう。通信回線には、本学が管理していないものも含まれ、その種類（有線又は無線、物理回線又は仮想回線等）は問わない。

（１４）　通信回線装置

通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置をいう。通信回線装置には、いわゆるハブやスイッチ、ルータ等のほか、ファイアウォール等も含まれる。

（１５）　ポリシー

本学が定める「情報セキュリティ対策基本方針」及びこの規程をいう。

（１６）　情報セキュリティ関連規程

ポリシーに基づいて策定される規程、基準及び計画を総称したものをいう。

（１７）　対策基準

本学が定める「情報セキュリティ対策基準」及び同基準から参照される関連基準をいう。

（１８）　実施手順

対策基準に定められた対策内容を個別の情報システムや業務において実施するため、あらかじめ定める必要のある具体的な手順をいう。

（１９）　情報セキュリティインシデント

JIS Q 27000:2014 における情報セキュリティインシデントをいう。

（２０）　ＣＳＩＲＴ（Computer Security Incident Response Team／シーサート）

本学において発生した情報セキュリティインシデントに対処するため、本学に設置された体制をいう。

（２１）　情報セキュリティ対策推進体制

本学の情報セキュリティ対策の推進に係る事務を遂行するため、学内に設置された体制をいう。

（２２）　要管理対策区域

本学の管理下にある区域（学外組織から借用している施設等における区域を含む。）であって、取り扱う情報を保護するために、施設及び執務環境に係る対策が必要な区域を

いう。

（適用対象者）

第３条　この規程において適用対象とする者は､本学情報システムを運用･管理するすべての者、並びに利用者及び臨時利用者とする。

２　この規程において適用対象とする情報は、前条第１項第１号に定めるものをいう。

３　この規程において適用対象とする情報システムは、前条第１項第２号に定めるものをいう。

（総括責任者）

第４条　本学における情報セキュリティに関する事務を統括する総括責任者を置き、事務局長をもって充てる。

２　総括責任者は、次に掲げる事務を統括する。

（１）　情報セキュリティ対策推進のための組織・体制の整備

（２）　情報セキュリティ対策基準の決定、見直し

（３）　対策推進計画の決定、見直し

（４）　情報セキュリティインシデントに対処するために必要な指示その他の措置

（５）　前各号に掲げるもののほか、情報セキュリティに関する重要事項

３　総括責任者は、情報基盤として供される本学情報システムのうち、情報セキュリティが侵害された場合に特に影響が大きいと想定される情報システムを指定することができる。この指定された情報システムを「全学情報システム」という。

（組　織）

第５条　総括責任者は、対策基準等の審議を行う組織として、情報セキュリティ対策推進体制及び情報センター長、総務課長、情報システム管理室長を構成員とする情報セキュリティ委員会を置く。

２　情報セキュリティ委員会は、次に掲げる事項を審議する。

（１）　情報セキュリティ対策基準

（２）　対策推進計画

（３）　前各号に掲げるもののほか、情報セキュリティに関し必要な事項

（情報セキュリティアドバイザー）

第６条　総括責任者は、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者を情報セキュリティアドバイザーとして置くことができる。

２　総括責任者は、次の各号に定める情報セキュリティアドバイザーの業務内容を定めるものとする。

（１）　情報セキュリティ対策の推進に係る総括責任者への助言

（２）　情報セキュリティ関係規程の整備に係る助言

（３）　対策推進計画の策定に係る助言

（４）　教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援

（５）　情報システムに係る技術的事項に係る助言

（６）　情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言

（７）　利用者に対する日常的な相談対応

（８）　情報セキュリティインシデントへの対処の支援

（９）　前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援

（対策推進体制）

第７条　総括責任者は、本学の情報セキュリティ対策推進体制を整備し、その役割を定めるものとする。

２　総括責任者は、情報セキュリティ対策推進体制の責任者を定めるものとする。

３　総括責任者は､次の各号に定める情報セキュリティ対策推進体制の役割を定めるものとする。
（１）　情報セキュリティ関係規程及び対策推進計画の策定に係る事務
（２）　情報セキュリティ関係規程の運用に係る事務
（３）　例外措置に係る事務
（４）　情報セキュリティ対策の教育の実施に係る事務
（５）　情報セキュリティ対策の自己点検に係る事務
（６）　情報セキュリティ関係規程及び対策推進計画の見直しに係る事務

（ＣＳＩＲＴ）
第８条　総括責任者は、ＣＳＩＲＴを整備し、その役割を定めるものとする。
２　総括責任者は、教職員等のうちからＣＳＩＲＴに属する職員として専門的な知識又は適性を有すると認められる者を選任することができる。そのうち、本学における情報セキュリティインシデントに対処するための責任者としてＣＳＩＲＴ責任者を置くことができる。また、ＣＳＩＲＴの業務統括及び外部との連携等を行う教職員等を定めることができる。
３　総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備するものとする。
４　総括責任者は、次の各号に定めるＣＳＩＲＴの役割を規定するものとする。
（１）　本学に関わる情報セキュリティインシデント発生時の対処の一元管理
・情報セキュリティインシデントの可能性の報告受付
・本学における情報セキュリティインシデントに関する情報の集約
・情報セキュリティインシデントの総括責任者等への報告
・情報セキュリティインシデントへの対処に関する指示系統の一本化
（２）　情報セキュリティインシデントへの迅速かつ的確な対処
・情報セキュリティインシデントであるかの評価
・被害の拡大防止を図るための応急措置の指示又は勧告を含む情報セキュリティインシデントへの対処全般に関する指示、勧告又は助言
・文部科学省への連絡
・外部専門機関等からの情報セキュリティインシデントに係る情報の収集
・他の機関等への情報セキュリティインシデントに係る情報の共有
・情報セキュリティインシデントへの対処に係る専門的知見の提供、対処作業の実施
５　総括責任者は、実務担当者を含めた実効性のあるＣＳＩＲＴの体制を構築するものとする。
６　総括責任者は、情報セキュリティインシデントが発生した際に、情報セキュリティインシデント対処に関する知見を有する外部の専門家等による必要な支援を速やかに得られる体制を構築するものとする。
７　総括責任者は、本学における情報セキュリティインシデント対処について、ＣＳＩＲＴ、情報セキュリティインシデントの当事者部局及びその他関連部局の役割分担を規定するものとする。

（対策基準）
第９条　総括責任者は、情報セキュリティ委員会における審議を経て、サイバーセキュリティ戦略本部決定「政府機関等の情報セキュリティ対策のための統一基準」に準拠した対策基準を定めるものとする。また、対策基準は、本学の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた上で定めるものとする。

（管理運営部局）
第１０条　本学情報システムの管理運営部局を情報センターに置く。

（情報センター長の事務）
第１１条　情報センター長は、命を受け、次の事務を統括する。
（１）　要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定

（２）　情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務の取りまとめ
（３）　情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備
（４）　例外措置の適用審査記録の台帳整備等
（５）　情報セキュリティインシデントに対処するための緊急連絡窓口の整備等
（６）　前各号に掲げるもののほか、情報セキュリティ対策に係る事務

（情報システム管理室の事務）
第１２条　情報システム管理室は、情報センター長の指示により、次の各号に定める事務を行う。
（１）　情報セキュリティ委員会の運営に関する事務
（２）　本学情報システムの運用と利用におけるポリシーの実施状況の取りまとめ
（３）　講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ
（４）　本学の情報システムのセキュリティに関する連絡と通報
（５）　総括責任者の支援

（教職員等の役割）
第１３条　教職員等は、情報セキュリティ対策の運用において、次の各号に定める役割を兼務することができないものとする。
（１）　承認又は許可（以下本条において「承認等」という。）の申請者と当該承認等を行う者
（２）　監査を受ける者とその監査を実施する者

（改　廃）
第１４条　この規程の改廃は、情報セキュリティ委員会の議を経て、学長が行う。

附　則
１　この規程は、令和４年６月６日から施行する。
２　北海道情報大学情報セキュリティポリシー（平成２１年９月１日制定）は、廃止する。

附　則
この規程は、令和７年４月１日から施行する。