札幌市立大学情報セキュリティポリシー対策基準

改正　令和８年　４月１日

１　組織・体制

本学の情報セキュリティ対策に係る役割、権限及び責任を次のとおり定める。

（１）情報セキュリティ総括責任者

情報セキュリティ総括責任者を置き、理事長がその任にあたる。情報セキュリティ総括責任者は、本学の情報セキュリティに関するすべての責任及び最終決定権限を有し、情報セキュリティに関する事項を総括し、必要な指示・指導を行う。

（２）情報基盤センター

本学の情報セキュリティに関する事項は、情報基盤センターが所管するものとする。情報基盤センターの組織及び運営に関しては、公立大学法人札幌市立大学情報基盤センター規則（令和２年規則第５号）に定めるとおりとする。

（３）情報セキュリティ責任者

情報セキュリティ責任者を置き、情報基盤センター長をもって充てる。情報セキュリティ責任者は、情報基盤センターでの審議・決定、情報セキュリティ総括責任者の指示等に基づき、学内において情報セキュリティ対策に係る指示・指導を行う責任と権限を有する。

（４）組織責任者

部局長（事務局長を除く）及び共同研究等の事業におけるプロジェクトの長並びに事務局における課長は、組織責任者として、各組織内でのポリシーの遵守に関し責任と権限を有する。

（５）情報資産管理担当者

情報資産を作成又は入手した教職員等（派遣職員、委託業者、学外の共同研究者、共同研究機関を含む）は、情報資産管理担当者として、当該情報資産をポリシーに基づき適正に管理する。

（６）CSIRT（Computer Security Incident Response Team）

情報セキュリティに関するインシデントに初期対応する CSIRT Level1（以下、CSIRT-1）を置き、情報基盤センター長、総務課情報担当者、保守担当常駐 SE により構成する。CSIRT-1 はインシデントの重要度を判定し、重要度が高いと判断した場合には、CSIRT Level2（以下、CSIRT-2）を招集し、学内外の対応を行う。CSIRT-2 は、CSIRT-1 の構成員に、理事長、事務局長、事務局次長、広報室長を加えるものとする。また、必要に応じて担当者を加えて構成する。

２　情報資産の分類と管理

（１）情報資産の分類及び取扱方法の設定等

ア　情報資産管理担当者は、作成又は入手した情報資産について機密性の観点から、別表１

の基準により分類を行い、分類された区分に基づいて情報資産を適正に取り扱う。なお、別表１の基準適用開始以前に作成又は入手した情報資産についても同様の取扱いとすることが望ましい。

イ　情報資産管理担当者は、上記アの実施に当たっては、必要に応じて組織責任者の判断を仰ぐものとする。

ウ　情報資産作成の元となる情報が、すでに別表１の基準に基づき分類及び取扱方法について設定されている場合には、元となる情報資産の分類及び取扱方法を継承するものとする。

エ　利用者は設定された分類及び取扱方法にしたがって情報資産を取り扱わなければならない。

（２）情報資産管理簿の作成等

ア　情報資産管理担当者は、別表１に基づき「機密性４」に分類した情報資産については、情報資産管理簿（別紙１）に登録し、組織責任者に確認を得るものとする。

イ　情報資産管理担当者及び利用者は、情報資産管理簿に登録した情報資産について、複製、学外への持ち出し、メール送信、消去または利用者範囲の変更を行うときは、情報資産管理簿に記録し、組織責任者の許可・確認を得るものとする。

３　情報セキュリティ対策

情報セキュリティ責任者は、物理的・人的・技術的セキュリティの全ての観点から、適切な情報セキュリティ対策を講じなければならない。また、本基準のすべての対象者に、それぞれに応じた教育、研修、啓発等を定期的に行い、情報セキュリティの重要性を理解させなければならない。

（１）物理的セキュリティ

ア　パソコン端末機器

全構成員は、自らが管理するパソコン端末機器について、無断で使用されることがないように、認証等の必要な措置（パスワードの設定）をとらなければならない。また、パソコン端末機器には、災害、事故及び盗難等を防止するための対策を講じなければならない。

イ　サーバ機器

情報セキュリティ責任者は、サーバ機器をその重要度に応じたセキュリティ対策が施された管理場所に設置し、管理場所には許可を得ていない者の入室を禁じなければならない。

サーバ機器を管理する者は、サーバ機器に対して、原則として認証を行わなければならない。また、サーバ機器に記録されるデータについて、その重要度に応じて定期的にバックアップを行わなければならない。

サーバ機器を管理する者は、サーバ機器やデータをバックアップした記録媒体について、災害、事故及び盗難等を防止するための対策を講じなければならない。

ウ　ネットワーク機器

情報セキュリティ責任者は、ネットワーク機器について、許可を得ていない者が容易に使用することができないよう、必要な措置をとらなければならない。また、災害、事故及

び盗難等を防止するための対策を講じなければならない。

エ　無線ＬＡＮ

許可を得ていない者は、本学の無線ＬＡＮを用いた通信を行ってはならない。無線ＬＡＮを使用する者は、暗号化をせずに通信を行ってはならない。ただし、フリーWiFi を除く。

オ　防犯設備

情報セキュリティ責任者は、サーバ機器及びネットワーク機器の管理場所について、その重要度に応じ、鍵管理、入退室管理等必要な対策を取らなければならない。

（２）人的セキュリティ

全構成員は、ポリシーに定めた事項を的確に実行し、情報セキュリティを適正に維持するよう努めなければならない。

情報セキュリティ責任者は、全構成員が実施すべき事項を周知徹底するなど、ポリシーを遵守する対策を講じなければならない。

ア　パスワード管理

全構成員は、自己のパスワードを他人に知られないように適切に管理しなければならない。また、十分な情報セキュリティを維持できるよう、自己のパスワードを設定しなければならない。

イ　利用範囲

全構成員は、あらかじめ許可された目的以外のために情報機器やネットワーク機器を利用してはならない。また、アクセスが許可されていない情報資産にアクセスしてはならない。なお、意図せずアクセスした場合は、速やかに退出しなければならない。

ウ　システム管理

情報セキュリティ責任者は、利用資格を有する者のみに情報機器のアカウントを発行し、利用資格を失った者のアカウントについては、速やかに除去しなければならない。また、構成員のアカウント情報を第三者に漏えいしてはならない。

なお、情報セキュリティ責任者は、学外者について、本学の業務、研究、教育等に必要と認めた場合に限り、アカウントを発行することができる。

情報セキュリティ責任者は、業務上必要な場合に、ログ情報および通信内容の閲覧・解析を行うことができる。また、全構成員に対し、必要なアクセス記録等の提出を求めることができる。この場合には、構成員のプライバシーに十分配慮しなければならない。

エ　情報機器の管理者の選任

情報機器を情報ネットワークに接続するときは、その管理者を定め、情報セキュリティ責任者から承認を得なければならない。

オ　外部委託

情報資産（機密性１情報を除く）を取り扱う業務を発注する場合は、契約書等にポリシーの遵守を明記しなければならない。

（３）技術的セキュリティ

情報セキュリティ責任者は、情報機器を不正なアクセス等から保護するため、情報機器へのアクセス制御等、情報セキュリティ管理についての対策を講じなければならない。

ア　コンピュータウイルス、スパイウェア対策

情報セキュリティ責任者は、不正アクセス、コンピュータウイルスやスパイウェア等、情報システムの運用を妨害しようとする攻撃行為を防ぐために、必要な対策を講じなければならない。

全構成員は、本学の情報ネットワークに接続する機器には、ウイルス対策ソフトウェアの導入等の対策を講じなければならない。

イ　情報システムの導入、保守等

情報セキュリティ責任者は、情報システムの導入、更新及び日常の運用保守にあたって、セキュリティホールの有無の確認、システムの修正プログラム（パッチ）の定期的な適用等、適切な情報セキュリティ対策を施さなければならない。

また、重要な情報機器については、故障や停電などの事故の際、迅速に復旧できる体制を整えておかなければならない。

情報システムの導入・更新及び日常の運用保守を事業者に発注する場合は、契約書面にポリシーの遵守を明記しなければならない。

4　運用

（1）情報セキュリティ上の脅威への対応

CSIRT-1 は、外部または内部からの不正アクセス等、情報セキュリティ上の脅威が検出された場合、関連する通信の遮断、該当する情報機器の切り離し及び停止等必要な措置をとることができる。全構成員は、情報セキュリティ上の脅威を発見した場合、直ちに CSIRT-1 に申告しなければならない。

（2）違反者への対応

情報セキュリティ責任者は、ポリシーに違反した者に対しては、本学の構成員であるなしに関わらず、本学の情報資産の利用制限を行うことができる。

また、重大な違反をした者で本学の構成員である者に対しては、関係規定に基づき処分を行うことがある。

5　点検・評価・見直し

（1）情報セキュリティの自己点検・評価と見直し

情報セキュリティ責任者は、適切な物理的・人的・技術的セキュリティ対策が実施されているか、定期的に点検、評価及び見直しを実施しなければならない。改善が必要と認められた場合は、速やかに必要な措置をとらなければならない。

（2）情報セキュリティの監査

情報セキュリティ対策の有効性および適切性を確認するため、定期的に外部の第三者機関による監査を受けなければならない。監査内容は、情報セキュリティ対策の実施状況、各種

規程類や関連法令等への遵守状況などとする。監査により指摘事項が発見された場合、情報セキュリティ責任者は速やかに改善計画を策定し、必要な是正措置をとらなければならない。監査結果および改善状況は、次回監査時における確認対象とし、継続的改善を図るものとする。

（3）ポリシーの評価と更新

情報セキュリティの評価等を行う場合は、ポリシーの実効性の観点から検討を加え、改善が必要と認められた場合には、実効性の高いポリシーに更新しなければならない。

別表１　情報資産の分類及び取扱方法

（１）情報資産の分類

区分	機密性4情報 （秘情報）	機密性3情報 （関係者外秘情報）	機密性2情報 （学外秘情報）	機密性1情報 （公開情報等）
分類の基準	本学の情報資産のうち、秘密文書に相当する機密性を有し、その漏えい等により本学の信用及び個人の名誉を著しく毀損し、本学及び個人に対し損失を与えるおそれがある情報	本学の情報資産のうち、秘密文書に相当する機密性は有しないが、その漏えい等により本学及び共同研究者の権利が侵害され又は本学の活動の遂行に支障を及ぼすおそれがある情報	本学の情報資産のうち、秘密文書に相当する機密性は有しないが、その漏えい等により本学の活動の遂行に支障を及ぼすおそれがある情報	機密性４情報、機密性３情報又は機密性２情報以外の情報
分類例	入試関連情報 学生情報 学生成績関連情報 入学料・授業料等減免関連情報 職員等人事関連情報 学内ネットワーク関連情報 情報セキュリティ監査関連情報	共同研究者関連情報 卒論・修論等研究論文関連情報 学会等発表前研究論文関連情報 学会誌掲載審査研究論文関連情報 講義試験関連情報 学内各種委員会関連情報 教授会関連情報 部局内会議関連情報 図書館貸出等利用者関連情報 外部委託関連情報 学内情報システム関連情報	人事異動関係情報 研究費申請等事務関連情報 学内・部局内連絡関連情報 勉強会・研修会・研究会・講義等関連情報 図書館等入館者関連情報 研究業績関連情報	大学案内 HP 掲載関係情報 大学広報誌 本学年報 受験案内 学会等発表済研究論文関連情報
取扱者	限定された関係者限り	関係者限り	教職員等限り	全て公開

※　情報資産管理担当者は、「分類の基準」に従って、作成・入手した情報資産を分類し、必要に応じて組織責任者の判断を仰ぐものとする。（必ずしも分類例の通りではない）

（２）取扱方法

区分	取扱方法
機密性４情報（秘情報）	・情報資産管理担当者が情報資産管理簿（別紙１）に記録して管理 ・暗号化（パスワード保護）必須 ・データの複製、学外への持出し、関係者以外への配布、メール送信、使用済データの再利用は原則禁止 ※教育・研究活動等のため、一時的に情報資産を持ち出す場合や業務受託者等に必要最小限の情報提供を行う場合は、所管の組織責任者（部局長、共同研究等の事業における PJ の長、事務局課長等）の許可を事前に得ることで可とする（情報資産管理簿への組織責任者からの確認印が必要） ※学生成績関連情報については、科目責任者を「組織責任者」とし、情報資産取扱届（別紙２）により科目責任者が管理を行う。
機密性３情報（関係者外秘情報）	・データの複製は原則禁止とするが、必要最小限のバックアップの作成・保存は可。 ・学外への持出し、関係者以外への配布、使用済データの再利用は原則要許可。 ・携帯端末や外部記憶媒体により一時的に学外へ情報資産を持ち出す場合は、パスワード保護のうえ、学内でバックアップを取り、持ち出した情報資産を明らかにすること。 ※許可は組織責任者からメール等で事前に得ること。 ※講義試験関連情報については、科目責任者を「組織責任者」とする。
機密性２情報（学外秘情報）	・学外者への配布は原則要許可 ・携帯端末や外部記憶媒体により一時的に学外へ情報資産を持ち出す場合は、パスワード保護のうえ、学内でバックアップを取り、持ち出した情報資産を明らかにすること。 ※許可は組織責任者からメール等で事前に得ること。

※　上記の取扱方法によることができない場合は、各組織において実施手順を策定し、組織責任者及び情報セキュリティ責任者の許可を得ること

別紙1　情報資産管理簿

◎情報資産（機密性4）登録

No.	作成（入手）日	名称（ファイル名等）	情報内容	保管場所		利用者範囲制限	管理担当者	※1　確認者 （組織責任者）	※2　確認印 （又は確認日）
									印

◎取扱記録（複製、持出、メール、消去、保管場所及び利用者範囲の変更に係る記録）

取扱	日付	取扱の目的		保管場所 （複製の保管場所又は保管場所の変更の際に記入）	複製媒体 あるいは 持出媒体 （持出する場合に記入）	持出先 （持出する場合に記入）	メール送信先 （送信する場合に記入）	利用者範囲制限 （利用者の制限範囲を変更する場合に記入）	管理担当者又は利用者（変更、複製、持出、メール送信を行う者）	※1　許可・確認者 （組織責任者）	※2　確認印 （又は確認日）	複製・持出した情報資産の消去日時	消去確認者 （組織責任者）	※2　確認印 （又は確認日）
											印			印
											印			印
											印			印
											印			印
											印			印
											印			印
											印			印
											印			印
											印			印

※1　許可・確認者：事務局が管理する情報資産については所管課の課長、その他の情報資産についてはその属性・内容から判断される組織責任者

※2　許可・確認印による事務処理が難しい場合、メール等による許可・確認をもって代えることができる。その場合、許可・確認を受けた日付を記載する

別紙２

情 報 資 産 取 扱 届

科目名＿＿＿＿＿＿＿＿＿＿＿＿

科目責任者＿＿＿＿＿＿＿＿＿＿＿＿

日付	名称（ファイル名等）	相手先	受け渡し方法	持出しの有無