情報セキュリティ実施手順

平成３０年　４月　１日　制定
（最終改正：平成３１年３月６日）

はじめに

この「手順」は、札幌市立大学情報セキュリティポリシー（以下「ポリシー」という。）及び情報セキュリティポリシー対策基準（以下「対策基準」という。）に基づいて、教職員等が情報セキュリティ対策を行うための、具体的な手順を定めたものである。

１　情報資産の管理

本学が保有する情報資産については、対策基準２(1)によって定められた分類により重要度を分類し、適正に管理を行うこと。

(1)　情報資産の管理方法

①　機密性４情報（秘情報）

職務上必要な限定された関係者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必ず実施するとともに、必要な対策を取ること。

【実施事項】

・個人フォルダや、ネットワークから切り離されたパソコンに保存する。共有フォルダに保存する場合には、職務上必要な者のみにアクセス権限を設定する。
・情報資産管理簿（対策基準 別紙１）に登録し、組織責任者の確認を得る。
・ファイル自身に適切なパスワードを設定するか、ファイルを暗号化する。
・その存在の有無についても、職務上必要な最低限の者以外に漏れないよう、厳格に扱う。

②　機密性３情報（関係者外秘情報）

関係者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必要に応じて実施するとともに、必要な対策を取ること。

【実施事項】

・個人フォルダや、ネットワークから切り離されたパソコンに保存する。共有フォルダに保存する場合には、関係者のみにアクセス権限を設定する。
・ファイル自身に適切なパスワードを設定するか、ファイルを暗号化する。

③　機密性２情報（学外秘情報）

学内者のみにアクセスを制限し、それ以外の者にアクセスさせないために、以下のことを必要に応じて実施するとともに、必要な対策を取ること。

【実施事項】

・共有フォルダに保存する場合には、関係者のみにアクセス権限を設定する。
・ファイル自身に適切なパスワードを設定するか、ファイルを暗号化する。

④　機密性１情報（公開情報等）

公開情報は不特定の者がアクセス可能であるため、情報の改ざんや偽情報の流布の防止策のために、以下の例を参考に必要な対策を取ること。

【対策例】

・公開情報の修正等の作業は限られた者のみが行えるようにパスワード等を設定する。

(2)　情報資産の複製、持ち出し及びメール送信

情報資産を複製、持ち出し及びメール送信する場合も、情報資産の分類に応じて、以下のことを必ず実施するとともに、必要な対策を取ること。

①　機密性４情報（秘情報）

【実施事項】

・学内の安全性のある場所に保管し、原則として、保管場所からの複製、持ち出し及びメール送信はしない。
・やむを得ず保管場所以外に複製、持ち出し及びメール送信する場合は、情報資産管理簿（対策基準 別紙１）に記録し、当該情報を所管する組織責任者の承認を事前に得るとともに、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・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（対策基準 別紙２）に記録するとともに、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・情報資産の持ち出し時には、肌身離さず所持し、盗難、紛失等に十分注意する。
・複製、持ち出し及びメール送信した情報資産は、不要になり次第速やかに削除し、情報の漏えいを防ぐ。

②　機密性３情報（関係者外秘情報）

【実施事項】

・学内の安全性のある場所に保管し、原則として、保管場所からの複製及び持ち出しはしない。
・やむを得ず保管場所以外に複製及び持ち出す場合は、当該情報を所管する組織責任者の承認を事前に得るとともに、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・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し、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。
・情報資産の持ち出し時には、必ず目の届く場所にデータを置き、盗難、紛失等に十分注意する。

③　機密性２情報（学外秘情報）

【実施事項】

・学内の安全性のある場所に保管し、原則として、保管場所からの複製及び持ち出しはしない。

・保管場所以外に複製及び持ち出す場合は、記録媒体のアクセスを制限するための適切なパスワードの設定や、データ自体を暗号化するなどの措置を行う。

・情報資産の持ち出し時には、必ず目の届く場所にデータを置き、盗難、紛失等に十分注意する。

④　機密性１情報（公開情報等）

【実施事項】

・情報資産の持ち出し時には、目の届く場所にデータを置き、盗難、置き忘れ等に十分注意する。

(3)　機密性４情報、機密性３情報及び機密性２情報の開示について

原則として、機密性４情報、機密性３情報及び機密性２情報は、開示してはならない。

ただし、やむを得ず一部又は全部を第三者に開示する場合は、札幌市個人情報保護条例に基づき以下のことを必ず実施するとともに、必要な対策を取ること。

【実施事項】

・開示の要求を受けた情報資産を管理している部局は、開示要求の理由が適正か判断し、当該情報を開示して問題ないか十分に協議する。

・個人情報の漏えい、プライバシーや著作権の侵害に十分注意し、場合によっては、開示する情報の抽出や統計処理による秘匿措置などを行う。

・開示する場合は、開示を要求した第三者以外に開示されないように、開示を要求した第三者に対して指導、監督する。

(4)　情報処理機器の廃棄について

情報処理機器の廃棄をする際には、情報資産の分類に関係なく、データの消去等を確実に行い、情報の漏えい防止策のために、以下の例を参考に必要な対策を取ること。

【対策例】

・データの消去には、破砕処理や、磁気によるデータの消去、データ消去ソフトウェアを用いた消去等を行い、データの復元ができないようにする。

・情報機器の記憶媒体を保守契約により交換する場合又はリース機器の撤去を行う場合は、撤去後の記憶媒体の処理法についても保守業者に確認を取り、データ消去を確実にする。

・データの消去を外部に委託する際には、データ消去証明書等の提出を義務付ける。

２　セキュリティの確保

利用者及び部局は、本学が保有する情報資産を守るため、当該情報資産を管理している組織責任者の指示の下、対策基準３によって定められたセキュリティ対策を実施する。

(1)　物理的セキュリティ

①　情報システムのセキュリティ対策

パソコン等の情報システムについては、以下の例を参考に必要な対策を取ること。

【パソコン、サーバ類の対策例】

・機器に適切なパスワードを設定し、不要なアクセスを防ぐ。

・パソコンを離れる際には、ロック画面（スクリーンセーバー）にするなど、他人にパソコンを閲覧されないようにする。

【外部記憶装置の対策例（USB メモリ、外付けハードディスクなど)】

・外部記憶装置は、セキュリティ機能付きのものを使用する。

・私物の外部記憶装置を本学のパソコンに接続しない。

・大学で購入した外部記憶装置は、原則として大学管理外のパソコン等へは接続しない。やむを得ず一時的に接続しなければならない場合は、必ずウイルスチェック等を行う。

②　入室の制限

サーバ室のように重要な情報機器が設置してある部屋の管理については、以下の例を参考に必要な対策を取ること。

【対策例】

・施錠管理し不正な入室を防ぐ。

・特に重要な部屋については電子錠により施錠管理し、入退室の自動記録を行う。

・入室できる者を制限する。また、入室を予定していない者が入室を行う際には、入室権限を持つ者が同行する又は部屋の管理者に事前に許可を得る。

・入退室記録の管理や防犯カメラを設置し、不正な入室が行われないようにする。

③　盗難の防止

情報システム及び情報資産（以下「情報資産等」という。）の盗難を防ぐため、以下の例を参考に必要な対策を取ること。

【対策例】

・パソコンやプリンタなど、持ち運びのできる物は盗難防止のため、セキュリティワイヤー等で固定のうえ施錠する。

・情報資産を管理するキャビネット等は、施錠管理を行う。

④　災害対策

サーバ機器のような重要な情報処理機器のシステム停止を可能な限り防ぐために、以下

の例を参考に必要な対策を取ること。

【対策例】

・情報処理機器の備え付けにあたっては、耐震対策を充分に考慮する。

・災害により情報システムが停止しないように、構築時に冗長化を行う。

・災害等によりデータが消失することがないように、サーバ機器は定期的にバックアップを取る。

・停電等による不測のシステム停止によりハードウェア障害が起きないように、無停電電源装置等を用いて、電源断時に自動で終了処理を行う。

⑤　ネットワークへの不正接続対策

ネットワークの接続口が不特定の者によって接続されないよう、以下を参考に必要な対策を取ること。

【対策例】

・有線 LAN を使用する場合は、悪意又は過失によるケーブルの切断を防ぐ対策を行う。

・使用していない接続口は、市販の LAN ポート用のセキュリティ製品等を使用して、不正な接続を防止する。

(2)　人的セキュリティ

①　情報資産の管理

部局は、組織責任者の指示の下、情報資産の重要度を適切に分類し、以下の例を参考に情報資産の管理を行うこと。

【対策例】

・情報資産の重要度を適切に設定する。（不要に重要度を高くすると、利便性が著しく低下し、業務や研究等に支障が出ることも考えられるため、重要度の分類は適切に行う必要がある。）

・機密性４情報及び機密性３情報の権限範囲が適切であるか定期的に確認する。

・情報資産台帳等を作成し、守るべき情報資産を整理する。

②　情報セキュリティポリシーの徹底

利用者は、情報セキュリティポリシー（以下「ポリシー」という。）を遵守しなければならない。

【遵守事項】

・部局において、定期的にポリシーが遵守されているか確認する。

・情報セキュリティに関する研修に参加する。

・総務課情報担当から通知されるセキュリティ情報を確認し、セキュリティ対策を実施する。

③　パスワードの設定

利用者等は、パスワードの設定を行う際には、以下の例を参考にパスワードを設定すること。

【パスワードを設定する基準例】

・推測しにくいパスワードを設定する。
・8 文字以上のパスワードにする。
・英字・数字・記号を組み合わせる。

【パスワードを保護するための対策例】

・初期に設定されているパスワードは使用せず、必ず変更する。
・パスワードをメモしたものを人目の付くところに置かない。
・パスワードを他人に教えない。
・複数のシステム（メールアカウントや SNS のアカウントなど）に同じパスワードを設定しない。

④　電子メールのセキュリティ対策

電子メールの利用の際には、以下の例を参考に必要な対策を取ること。

【コンピュータウイルス・不正アクセス対策例】

・電子メール内に記載されている URL は、不用意にリンク先にアクセスすると、ウイルス感染、フィッシング詐欺等の危険があることから、URL に間違いがないか、信頼のおける URL であるかなど、十分に注意する。
・添付ファイルがある場合、コンピュータウイルス感染しているファイルの可能性があるため、不用意に開封しない。開封する場合は、ウイルスチェックを行ってから開封する。
・電子メールの送信者のアドレスが正しいことを確認する。（メールアドレスを企業等のメールアドレスに類似させて、偽装する場合などが考えられるため。）
・身に覚えのない送信主からのメール、明らかに不自然な内容のメール等は不用意に応答せず、必要に応じて総務課情報担当に相談する。

【誤送信による情報漏えい対策例】

・送り先のメールアドレス入力の際には、予測変換を利用すると間違える場合があるので注意する。
・添付ファイルを送信するときには、添付ファイルにパスワードを設定する。

⑤　プリンタ印刷のセキュリティ対策

プリンタ印刷の際には、情報の漏えいを防ぐために、以下の例を参考に必要な対策を取ること。

【対策例】

・印刷した情報資産の取り忘れ、取り間違いに注意する。

(3) 技術的セキュリティ

① 情報システムのセキュリティ対策

パソコン等の情報システムについては、以下の例を参考に必要な対策を取ること。

【パソコン、サーバ類の対策例】

・本学で包括契約しているウイルス対策ソフト又は同等レベルのソフトをインストールし、リアルタイム検索を有効化すること。また、定期的（最低でも月に 1 回）にウイルス感染チェックを行うこと。

・OS 又はインストールされているソフトウェア等で、セキュリティの脆弱性が発覚した場合には、速やかにセキュリティアップデートを行う。

・不正なアクセスや攻撃を防ぐために、不要な常駐プログラム等を停止する。

・アカウントの管理者は、アカウントの整理を定期的に実施し、不要なアカウントは削除する。

【ネットワーク接続機器の対策例（プリンタ、スキャナ、プロジェクタなど)】

・機器の利用は IP アドレス等で、利用可能な範囲を制限する。

・管理用途で遠隔から機器にアクセスする際は、IP アドレス制限やパスワード等でアクセスを制限し、不特定多数のアクセスを禁止する。

・不正なアクセスを防ぐため、不要なサービスは停止する。

【ネットワーク接続型の記憶装置の対策例（NAS、ストレージなど)】

・パスワード等の設定を行い、アクセスできる者を制限する。

・IP アドレスでの利用制限の設定を行い、不要なアクセスを防ぐ。

【通信制御装置の対策例（無線 LAN のアクセスポイント、ルーターなど)】

・登録された MAC アドレスやサブネット、IP アドレス以外から接続できないように設定する。

・無線 LAN のアクセスポイントは WPA2 方式又はそれと同等以上のセキュリティ強度の方式で暗号化通信ができるように設定する。

・SNMP の設定をする場合は、IP アドレスによる接続制限やコミュニティ名を標準設定から変更するなど、不特定多数の読み書きができないようにする。

② ネットワークへの不正接続対策

ネットワークの接続口が不特定の者によって接続されないよう、以下を参考に必要な対策を取ること。

【対策例】

・不特定多数が出入りする部屋では、ケーブルを接続するだけで学内ネットワーク及びインターネットが利用できるようになる DHCP サーバの設置は行わない。

・ルータモードを持つ機器を学内ネットワークに設置する場合は、必ず総務課情報担当に相談する。

3　禁止事項

本学の情報資産等を利用するにあたり、以下の行為はしてはならない。

(1)　法令に違反する行為

・閲覧権限及び利用権限のない情報資産等へ不正にアクセスする。

・情報資産等を破壊及び改ざんする。

・コンピュータウイルスを配布する。

・他人の写真や音声を当人に無断でホームページ等に公開する。

・他人の作成した文書、写真等を無断でホームページ等に公開する。

・有償ソフトウェアを無断でコピーして使用する。

・ファイル共有ソフト（Winny など）を用いて、著作権のあるソフトウェア、音楽ファイル、動画ファイル等を入手したり、入手した情報を公開して提供したりする。

・その他、法令に違反するとみなされる行為。

(2)　公序良俗に反する行為

・他人になりすまして、ネットワーク上で発言する。

・事実と異なる情報を意図的に流す。

・猥褻とみなされる文章や画像をホームページ等で公開する。

・人権、性別、思想信条などに基づく差別的な文章等をホームページ等で公開する。

・メーリングリスト等に他人を無断で登録する。

・他人のファイル等を当人に無断で参照する。

・その他、公序良俗に違反するとみなされる行為。

(3)　本学の運営・教育・研究目的等に反する行為

・学内ネットワークを商業目的等の運営・教育・研究目的以外に用いる。

・運営・教育・研究目的でないソフトウェアをダウンロードして利用する。

・ネットワークを意図的に混雑させる。

・組織責任者や総務課情報担当の指示に従わない。

・データ量の多いファイル等をメールで大量に送る。

・アカウントの貸し借りを行う。

・その他、本学の運営・教育・研究目的等に反するとみなされる行為。

4　インシデントに対する対応と報告

インシデントが発生した場合には、その被害を最小限に抑えるため、以下のとおり対応しなければならない。

(1) 重要度の区分

インシデントが発生した場合には、その事象から、以下のように重要度を区分する。

区　分	事　象
重要度高	・本学の信用や利益を大きく損なうもの。 ・本学全体の業務・運営に支障があるもの。 ・違反行為の内容が法律等に違反するもの。 ・事象が重大で解決に時間を要するもの。 ・その他、重要度が高いと認められるもの。
重要度低	・本学の信用や利益を損なう可能性がないもの。 ・本学の業務・運営に支障が少ないもの。 ・事象が軽微ですぐに対応が可能なもの。

(2) インシデントに対する対応

① 利用者等は、インシデントを発見した場合には、速やかに当該事象が発生している部局の組織責任者に連絡をしなければならない。また総務課情報担当にも同様に連絡をすること。

② 当該事象が発生している部局の組織責任者は、インシデントが発生した場合には、速やかに事実関係の確認、問題の解決に努めるとともに、再発防止策の検討及び実施をしなければならない。

③ 当該事象が発生している部局の組織責任者は、発生したインシデントの重要度に関わらず、情報セキュリティ責任者にインシデントの内容や対応状況、再発防止策等について報告しなければならない。

この場合、情報セキュリティ責任者は当該事象の重要度（４(1)）について判断する。

(3) 「重要度高」と判断されたインシデントへの対応

① 報告

ア 当該事象が発生した部局の組織責任者は、「インシデント報告書」を作成し、総務課情報担当へ提出するとともに、情報セキュリティ責任者に報告しなければならない。

イ 情報セキュリティ責任者は、組織責任者からインシデントの報告を受けた後、情報セキュリティ総括責任者へ報告しなければならない。

ウ 情報セキュリティ責任者は、組織責任者からインシデントの報告を受けた後、総務委員会を開催し、報告を行わなければならない。

② 調査等

ア 総務委員会は、インシデントが発生した部局に対して、ポリシーの遵守等に問題がなかったか調査を行う。

イ　情報セキュリティ責任者は、総務委員会の調査結果に基づき、以下の対応を行う。

・原因が、当該事象が発生した部局にある場合

当該組織責任者に対して、ポリシーの遵守を徹底させる。

・原因が、対策基準及び手順の不備にある場合

情報セキュリティ総括責任者に対して、対策基準及び手順の見直しを進言する。

５　見直し

情報セキュリティ総括責任者は、対策基準及び手順に課題及び問題点が認められる場合又は情報セキュリティ責任者からポリシーの見直しの進言があった場合は、見直しを行うものとする。

様式

インシデント報告書

平成　　年　　月　　日

報告者所属・氏名	
組織責任者所属・氏名	

インシデントの概要

発生日：　　年　　月　　日
事象の概要：
被害の概要：
原因：
応急措置：

対処

技術的対処：
事務的対処：

再発防止策

技術的対応：
意識向上等その他の対応