国立大学法人北海道大学情報セキュリティポリシー

平成１７年１２月１４日
国立大学法人北海道大学

Ⅰ　基本方針

１．情報セキュリティの基本方針

国立大学法人北海道大学（以下「本学」という。）では，教育研究活動を推進するため情報基盤を整備し，情報の創出，収集，共有，伝達，発信などに活用している。このような情報基盤の健全な運用及び発展を図るためには，情報セキュリティの考え方を正しく認識し，情報資産を保全することが不可欠である。一方，情報資産を保護しなければ，本学の教育研究及び大学運営にとって大きな支障を来すばかりでなく，本学への信頼の喪失といった事態に至る可能性もある。

したがって，本学が有するすべての情報資産をあらゆる脅威から守るため，不正アクセス行為の禁止等に関する法律，独立行政法人等の保有する個人情報の保護に関する法律（以下「個人情報保護法」という。），著作権法など関連する法令及び規則を踏まえた本学の情報セキュリティ対策の包括的な指針として，国立大学法人北海道大学情報セキュリティポリシー（以下「本ポリシー」という。）をここに定める。

本学の役員，職員，大学院学生，学部学生，研究生，聴講生など（以下「構成員」という。）及び本学が提供するサービスを利用するすべての関係者は，本ポリシーを理解し，遵守するとともに，本学における教育研究及び大学運営において情報資産の活用と保全に努めなければならない。

２．趣旨及び位置付け

本ポリシーは，次に掲げる目的のために，本学の管理するコンピュータ，ネットワーク等を利用して情報を取り扱う場合に遵守しなければならない基本的な事項をまとめたものである。

（１）本学の情報セキュリティに対するすべての侵害からの防御
（２）学内外の情報セキュリティを損ねる加害行為の阻止
（３）本学の情報資産に関する重要度に応じた管理の徹底
（４）本学内における情報セキュリティ侵害等の早期検出と迅速な対応の実現

３．定義

（１）情報資産

電磁的に記録された情報及びその作成，利用，管理等のための仕組み（ハードウェア及びソフトウェアからなる情報機器並びに有線又は無線のネットワークをいう。）の総称

（２）情報セキュリティ

情報資産の機密性（許可された者だけが情報にアクセスできることをいう。），完

全性（情報及び処理方法が正確かつ完全であることをいう。）及び可用性（許可された者が必要なときに情報にアクセスできることをいう。）を維持すること。

４．対象範囲及び対象者

（１）対象範囲

本学の保有するすべての情報資産及び本学のネットワークに一時的に接続される情報機器

（２）対象者

構成員並びに本学の情報資産を利用する委託業者及び来訪者など

５．ポリシーの改訂及び実施手順の作成

本ポリシーの改訂は，国立大学法人北海道大学情報セキュリティ委員会（以下「委員会」という。）の議を経て総長が行うものとする。

本ポリシーの実施手順については，委員会が別に定める。

II　対策基準

１．組織

情報セキュリティに関する組織として国立大学法人北海道大学情報セキュリティ委員会規程で規定する委員会の他，次の組織を置く。

1.1 最高情報セキュリティ責任者

・本学に最高情報セキュリティ責任者（以下「最高責任者」という。）を置き，総長が指名する理事をもって充てる。

1.2 情報セキュリティ統括管理者

・本学に情報セキュリティ統括管理者（以下「統括管理者」という。）を置き，最高責任者が指名する者をもって充てる。

1.3 部局情報セキュリティ責任者

・各部局等ごとに部局情報セキュリティ責任者（以下「部局責任者」という。）を置き，部局等の長（事務局にあっては事務局長）をもって充てる。

1.4 情報セキュリティ担当者

・構成員のうち，情報機器のアクセス権限，ネットワーク接続等に関する諸設定等情報資産のセキュリティ上の管理に携わる職員を情報セキュリティ担当者とする。

２．人的セキュリティ

2.1 最高情報セキュリティ責任者の責務

・最高責任者は，本ポリシーに基づき，本学のすべての情報セキュリティに関する総

括的な権限と責任を有する。
・部局責任者を通じて，学内の全部局等に本ポリシーを遵守させる。
・情報セキュリティに関する学外との対応のうち，対外的に見て最高責任者としての対処が必要と判断されるものについて，実際に対処する。

2.2 情報セキュリティ統括管理者の責務

・統括管理者は，最高責任者を補佐し，最高責任者に対し全学の情報セキュリティ管理及び監査に関し，必要となる技術的措置がとられるよう意見を具申するとともに，情報セキュリティの保持のため必要と判断した場合は，必要な措置を講じなければならない。
・統括管理者は，インシデントが発生した場合には，次の方法により統括的な窓口として事態に対処しなければならない。
①学内外からの不正アクセス又はこれに類する情報システムの異常事態を発見した場合若しくは通報を受けた場合は，実施手順に従って，関連する通信の遮断又は関連する情報機器の切り離し，電源切断など，技術的に必要な措置を講ずる。ただし，緊急事態への対応に関する実施手順により難い場合は，統括管理者の判断により必要な措置を講ずる。
②統括管理者は，発生した事態についての概要をまとめ，最高責任者及び関連する部局責任者に報告するとともに，再発防止のため必要な措置を講ずる。

2.3 部局情報セキュリティ責任者の責務

・部局責任者は，本ポリシーに基づき，部局内の情報セキュリティに関する総括的な権限と管理責任を有する。
・部局の全構成員に本ポリシーを周知させ，その遵守を徹底させる。
・部局等の規模に応じて，部局情報セキュリティ責任者の実務を補佐する者を置くことが出来る。
・部局内の情報セキュリティに関する委員会等を独自に組織することを妨げない。

2.4 情報セキュリティ担当者の責務

・情報セキュリティ担当者は，次の責務を有する。
①個々の情報機器を維持管理し，運用に即した設定やセキュリティ維持の責任を負うこと。
②不正アクセスを発見した場合，実施手順に従い適切な措置を直ちに講じること。
③職員の監督下において大学院学生等にセキュリティ上の管理業務を補助させる場合は，当該補助業務の範囲を明確に定め，これを厳守させること。
④利用が認められた者以外の者に情報機器の利用を許可してはならないこと。
⑤保守管理業務等のため学外者に本学の情報機器を利用させる場合は，本ポリシーのうち遵守対象となる部分を示し，これを遵守させるとともに，アクセス違反，情報の漏えい，改ざん等の防止を図るために必要な措置を講じなければならないこと。

⑥来訪者等の構成員以外の者に本学の情報機器を一時的に利用させる場合は，本ポリシーのうち遵守対象となる部分を示し，その内容を理解させるよう努めなければならないこと。
⑦セキュリティ情報に注意を払い，最新の安全状況を維持するように努めなければならないこと。

2.5 構成員の責務

・構成員は本ポリシーを理解し，これを遵守しなければならない。また，情報セキュリティに関する問題を起こさぬよう，自己啓発に努めなければならない。
・教育研究上の観点から，本ポリシーと情報資産の利用内容に不整合を生じる場合，最高責任者に対し，本ポリシーの改善を求めることができる。
・すべての構成員は，自己のパスワードを秘密にしなければならない。また，自己のパスワード管理に責任を持たなければならない。他の利用者のアカウントを用いてはならない。

３．情報の管理

3.1 基本事項

・本学で扱われる電磁的に記録されたすべての情報に関し，その重要度に応じて，管理方法及び責任の所在を明確にしておかなければならない。
・本ポリシーのほか，行政機関の保有する情報の公開に関する法律や個人情報保護法に基づいた情報の取り扱いに留意しなければならない。

3.2 情報作成者の原則

・情報を電磁的にアクセス可能な状態におく者（以下「情報作成者」という。）は，原則として自ら作成した情報については管理責任を負うとともに，情報の内容や重要度に応じたアクセス権の設定，バックアップの作成，改ざん防止等の必要な措置を講じなければならない。
・情報作成者は，アクセス権を設定する場合には，個人情報の有無，著作権に係る問題の有無など，情報の内容を十分踏まえなければならない。

3.3 情報利用者の原則

・情報機器を利用する者（以下「利用者」という。）は，情報を入手又は利用する際には，アクセス権のない情報に対して不当にアクセスを試みたり，改変する権限のない情報を改変したりしてはならない。また，アクセス権を不正な手段で入手してはならない。
・利用者は，アクセス権が不適切に設定されていることを発見した場合は，情報作成者又は当該情報セキュリティ担当者に対してその旨を通報しなければならない。
・利用者は，インシデントと思われる事態を発見した場合には，実施手順に従って，情報セキュリティ担当者に遅滞なくその旨を通報しなければならない。

4. 物理的セキュリティ

4.1 基本事項

・情報機器に関わる物理的セキュリティについては，原則として当該情報機器の定常的な利用者が一次的な責任を有する。
・情報機器を設置しようとする者（以下「設置者」という。）は，その設置場所及び設置方法について，情報機器の破壊，盗難及び紛失を防止するために必要な措置を講じなければならない。
・設置者は，使用者を特定できない情報機器の利用を防止するよう努めなければならない。
・設置者は，情報機器を廃棄する場合は，情報の漏えいを防止するために必要な措置を講じなければならない。

4.2 情報基盤機器

本学における情報基盤の維持に寄与するものとして委員会が指定した情報機器（以下「情報基盤機器」という。）の管理については，4.1 に示す基本事項に加え，以下の項目を遵守しなければならない。

・情報基盤機器は，あらかじめ定められた管理区域に置くこと。
・管理区域に出入りできる者は，管理上必要最低限の者とすること。
・管理区域については，入退室履歴を記録すること。
・重要なデータの記憶媒体は，管理区域に保管すること。

5．技術的セキュリティ

5.1 基本事項

・技術的セキュリティの基本単位は個々の情報機器とする。
・情報機器を本学のネットワークに接続する場合は，与えられた条件等に基づき，適切な設定を施さなければならない。
・個々の情報機器へのアクセス制限及びサービスの選択並びに基本ソフトウェア等が有するセキュリティの脆弱性への対処は，当該情報機器を維持管理する情報セキュリティ担当者が行わなければならない。
・利用者は，ウイルス，ワーム等に感染している情報機器及びセキュリティの重大な欠陥が周知となっている情報機器を本学のネットワークに接続してはならない。

5.2 本学のネットワークの包括的制限

・最高責任者は，統括管理者からの申出に基づき，本学のネットワークの利用を全学的見地から包括的に制限することができる。
・最高責任者は，利用に関する制限の内容について周知を図るものとする。
・利用者は，利用に関する制限について異議があるときは，最高責任者に対して，理由を付した文書により異議を申し立てることができる。

5.3 履歴の取り扱い

・情報セキュリティ担当者は，自ら管理する情報機器におけるアクセスログ等の履歴を採取し，不正アクセスの監視に努めなければならない。また，採取した履歴は，情報機器の利用状況に応じて，一定期間以上保存するよう努めなければならない。
・情報セキュリティ担当者は，委員会からの申出があった場合は，保存しているアクセスログ等の履歴を提出しなければならない。
・委員会は，情報セキュリティの維持及び強化のために必要と認めた場合は，本学のネットワークにおける通信履歴を採取することができる。ただし，通信内容の採取は行ってはならない。
・利用者は，通信履歴の採取について異議があるときは，最高責任者に対して理由を付した文書をもって異議を申し立てることができる。

5.4 技術情報の啓発

・委員会は，情報機器の適切な管理に関し，構成員に対する意識の啓発その他の必要な施策を講ずるものとする。

６．評価等

6.1 評価・見直し

・総長は，本ポリシーの評価を少なくとも２年に１回以上実施するものとし，当該評価の結果に基づき必要に応じて本ポリシーの見直しを行うとともに構成員に対して周知するものとする。

6.2 監査

・最高責任者は，本ポリシーに定める各項目に関する監査を定期的に実施し，その結果を総長に報告するものとする。
・監査の公正性及び中立性を確保するため，外部の監査組織の利用を妨げない。