# 北海道情報大学情報機器取扱ガイドライン

１．利用者向け利用手順

１．１　利用者は、北海道情報大学（以下「本学」）のネットワーク機器や端末等の設備を損傷する可能性のある行為及び電源等の本学資源の無断使用をしてはならない。

１．２　利用者は、他の利用者の利用を妨げる次の行為をしてはならない。

１）　プリンタ等の共用の設備を長時間にわたり占有する行為

２）　教育研究上必然性のないストリーミングサービス等の利用によりネットワーク帯域を占有する行為

３）　大きなデータのやり取り

４）　高い頻度で問い合わせパケット等を送出するアプリケーションの使用

５）　共用サーバでのファイル等の資源を占有する行為

１．３　利用者は、北海道情報大学情報セキュリティ対策基準において規定されている要保護情報や、その他重要なデータの取り扱いに関して、次に掲げる事項を遵守しなければならない。

１）　要保護情報を情報機器内部あるいは外部記憶メディアに保管する場合は、暗号化するものとし、その暗号化鍵を適切に管理すること。ただし、暗号化以外に十分な保護対策が取られていると管理者が認める場合は、この限りでない。

２）　要保護情報を電子メール等で送信する場合は、暗号化するものとし、その暗号化鍵は、別途安全な手段を用いて送信すること。

３）　教職員は、在宅勤務のために備品となる情報機器あるいは要保護情報を保管した情報機器を持ち出す必要がある場合には、事前に情報セキュリティ総括責任者に届け出なければならない。また、持ち出し利用にあたっては要保護情報が流出しないように細心の注意をはらうものとする。

１．４　利用者は、ＵＳＢメモリ、各種メモリカード等の外部記憶メディアを利用する場合には、次に掲げる事項を遵守しなければならない。

１）　業務利用する外部記憶メディアは、目を離して放置しないこと。

２）　放置してある、又は出所が定かではない外部記憶メディアを端末に挿入しないこと。

３）　使用済みの外部記憶メディアを譲渡又は廃棄する場合には、記録されていたデータが復元されることのないように、専用ツールを用いて消去する、メディアを物理的に破壊する､若しくはボリューム(外部記憶メディアにおけるデータの格納場所)を暗号化し、暗号化キーを破棄すること。

１．５　利用者は、共用の端末を利用する場合は、設置者の指示に従って利用すること。

１．６　利用者は、次に掲げる事項を発見したときは、速やかに情報センター事務室に連絡をするとともに、「インシデント対応手順」に従って行動すること。

１）　共用の端末のＯＳやアプリケーション又は共用サーバやネットワーク機器等について、セキュリティ上の脆弱性など不具合を見つけた場合

２）　学内の情報機器上で、著作権を侵害しているおそれのあるコンテンツ、機密情又は個人情報等にアクセス可能となっていることを発見した場合

３）　学外のサービス上で､本学の機密情報や､構成員の個人情報等が公開されている､又は本学が権利を有するコンテンツが無断で使用されていることを発見した場合

４）　要保護情報の流出を発見した場合

１．７　利用者は、学外のネットワークから学内の情報システム（不特定多数に公開されているもの（Ｗｅｂサービスなど）を除く。）にアクセスする場合は、次に掲げる事項を遵守しなければならない。

１）　アクセスの際に必要となる認証情報（パスワードや秘密鍵）が漏洩しないように細心の注意を払い、万一、認証情報が漏洩した場合又はその可能性がある場合は、迅速に管理者に報告し、その指示を仰ぐこと。

２）　信頼性が保障できない端末（ネットカフェの端末等）からの、本学のサービスのうち認証を要求するものへのアクセスは行わないこと。

２．特権利用者向け利用手順

２．１　特権利用者は、自らが管理する端末が、ウイルス、ワーム等に感染しないように、次に掲げる事項を遵守しなければならない。

１）　利用しているＯＳやアプリケーションの脆弱性情報をはじめとする情報に留意し、ソフトウェアの不具合を迅速に修正すること。

２）　ウイルス対策ソフトウェアをインストールするとともに、ウイルス情報データベースを常に最新に保っておくこと。

２．２　特権利用者は、自らが管理する端末に、アプリケーションをインストールし、利用する際には、次に掲げるものを遵守しなければならない。ただし、教育・研究目的及びそれらを支援する目的であって、対象となるネットワークの管理者が許可する場合には、この限りでない。

１）　ネットワーク帯域を極度に圧迫するアプリケーションをインストール及び利用してはならない。

２）　自端末宛以外のパケットを傍受するアプリケーション（パケットスニファ）をインストール及び利用してはならない。

３）　不正アクセスを目的としたソフトウェアや不正アクセスを助長するおそれのあるソフトウェアをインストール及び利用してはならない。

４）　北海道情報大学情報サービス利用規程、その他の本学ネットワークの利用に係る規程等に反するアプリケーションをインストール及び利用してはならない。

２．３　特権利用者は、自らが管理する端末に関して、次に掲げる事項を遵守すること。

１）　利用者が当該端末を認証なしで利用できるようにしてはならない。ただし、端末が認証機能を有さない場合には、あらかじめ許可された者のみが利用できるように別途手段を講じること。なお、アカウントの発行状況や利用状況（利用者識別の設定できないシステムにあっては、利用状況が把握できるもの）について問題が発生した場合には、報告可能なように記録を確認できること。

２）　不特定多数の第三者が端末にアクセスできないようにすること。

３）　当該端末にアカウントを有さない者に端末を使用させないこと。ただし、教育・研究上必要な場合を除く。

４）　サーバの管理端末においては、アカウントを有さない者が端末に物理的にアクセスできないように設置場所に施錠等の措置をとること。なお、共用端末にあっては、必要に応じて、端末機器にワイヤーロック等の盗難防止措置をとること。

５）　移動可能な端末においては、短時間であっても端末を放置しないこと。なお、保管時は、盗難防止対策をすること。

６）　共用端末等が管理権限をもたない者によって、DVD、USB メモリ又はネットワーク等を用いて起動されないように設定すること。

７）　端末を廃棄又は譲渡する場合は、内部のディスクや不揮発性メモリに、要保護情報やその他重要な情報が残留することのないように、専用ツールを用いて完全に消去するか物理的に破壊すること。

２．４　特権利用者は、自らが管理する情報機器に関して、利用者が学外のネットワークから当該端末にアクセスできるようにする場合は、次に掲げる事項を遵守すること。

１）　北海道情報大学情報サービス利用規程で許可された方法でアクセスすること。

２）　パスワードのみ（ワンタイムパスワードを除く）による認証方式は、原則として避けること。

３）　特権アカウント（root など）によるリモートアクセスは、原則として行えないように設定すること。

２．５　特権利用者は、自らが管理する情報機器を対象として実施される情報セキュリティ監査に対して、必要な協力を行うこと。