北海道情報大学認証情報管理ガイドライン

１．目　的

本ガイドラインは、北海道情報大学（以下「本学」）における情報システム（以下「本学情報システム」）のアカウントを利用する際の認証情報の扱いに関し、利用者が予め理解しておくべき事項を示すことを目的とする。

２．認証の方法について

一般に用いられている認証の方法は、次のように分類する。

（１）　利用者が知っていることを用いた認証
　　（例）ID とパスワード

（２）　利用者が保有しているものを用いた認証
　　（例）IC カード、スマートフォン、ハードウェアセキュリティキー等

（３）　利用者の生体的特徴を用いた認証
　　（例）指紋等

さらに、これらの組み合わせによる認証方法として多要素認証がある。多要素認証とは、前述の認証方法のうち、２つ以上を組み合わせて認証する方法である。多要素認証の例として、IC カードとパスワードやパスワードとスマートフォンを組み合わせて使うといった例があげられる。このうち、ID とパスワードに加えて、SMS で送られてきたコードを入力する方法や、認証用のコードジェネレータが生成したコードを入力するといった方法のことを２段階認証と呼ぶことがある。ID とパスワードのみを用いる方法に対し、２要素認証を用いることで安全度を高めることができるが、完全とはいえない。ID とパスワードによる認証法は、もっとも古くから使われていて広く普及している方法ではあるが、もっとも破られる危険度の高い方式である。

３．パスワードに係る全般的な注意事項

３．１　初期パスワードの変更

利用者は、アカウントが発行されたら速やかに初期パスワードを自己のものに変更すること。初期パスワードのまま本学情報システムの利用を継続してはならない。

３．２　パスワードに使用する文字列

利用者が設定するパスワード文字列は、次の条件を全て満たすものでなければならない。

１）　パスワードの長さは 8 文字以上で、大文字、小文字、数字及び記号を含むこと。7 文字以下の文字列は容易に推察可能であるため、パスワードとして設定してはならない。

２）　利用者のアカウント情報から容易に推測できる文字列（名前、ユーザ ID 等）

３）　１）と２）を並べ替えたもの、１）と２）に数字や記号を追加したもの

４）　″123456″や″abcd″といった単純なもの・辞書の見出し語、それを並べ替えたもの

５）　著名人の名前等、周知の固有名詞

３．３　パスワードの変更

利用者は、アカウント発行者からパスワードの変更指示を受けた場合及びアカウント情報の漏洩が疑われる場合には、遅滞なくパスワードを変更しなければならない。なお、

変更後のパスワードは変更前のパスワードと類似のものであってはならない。

３．４　アカウント情報の管理

利用者は、自己のアカウントについて、次の管理を徹底しなければならない。

１）　自己のアカウントを他者に知られないように最大限の注意を払うこと。

２）　他人にアカウント情報について尋ねられても絶対に教えないこと。

３）　アカウント情報は、必要な場面で思い出せるように管理すること。なお、アカウント情報の管理に専用のアプリケーションを使ってもよい。

４）　他の情報システムやサービス等で用いているアカウント情報と同じものを用いないこと（本学情報システムの仕様で同一のアカウント情報の利用を強制される場合を除く）。

４．アカウントに関する各種手続き

４．１　パスワードを失念した場合

利用者がパスワードを忘れた場合には、発行者に対して、所定の手続きによりパスワードのリセットを申請すること。リセットを受けた場合には、速やかに新しいパスワードに変更すること。

４．２　パスワードの漏洩時の対応

利用者は、アカウントを他者に使用され又はその危険が発生した場合には、直ちにアカウント情報を変更しなければならない。また、発行者が要求した場合には、アカウント発行者にアカウント情報を変更した旨を報告しなければならない。