パスワード利用ガイドライン

関西大学 IT センター

1　本ガイドラインの目的

本ガイドラインは、本学情報システムのアカウント利用者がパスワードを適切に管理するために予め理解しておくべき事項を定めることを目的とする。なお、適切なパスワードの設定方法は利用する情報システムの仕様に応じて選定する必要がある。また、最適な情報セキュリティ対策は脅威の動向とともに変化することから、利用者は定期的に情報を入手して対策の見直しを行うことが望ましい。

2　本ガイドラインの対象者

⑴ 対象者

本ガイドラインは、本学情報システムのアカウントを教育や研究目的で利用する本学のすべての構成員（以下利用者と呼ぶ）を対象とする。

3　パスワードの設定・管理

⑴ 初期パスワードの変更

利用者は速やかに初期パスワードを安全なものに変更する。本学情報システムで利用するパスワードは、他の情報サービスで利用中のパスワードや過去に利用したことのあるパスワードと同一にしない。

⑵ 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、以下のア～ウを満たすものとする。

ア　８文字から 16 文字までの長さの文字列である。

イ　２文字以上の英小文字を含む文字列である。

ウ　１文字以上の数字を含む文字列である。

以前に利用したことのあるパスワードや、それらと酷似するパスワードを利用することは著しいセキュリティ低下を招く恐れがあり、推奨されない。

また、以下のア～エに相当する文字列をパスワードとして利用しない。

ア　利用者のアカウントから第三者が推測することが可能な文字列。利用者の氏名やユーザ ID 等がこれに当たる。

イ　上記を並べ替えたものや、上記に数字や記号を追加したもの。

ウ　辞書の見出し語。

エ　著名人の名前等固有名詞。

パスワードに英大文字や特殊記号を含めることにより、セキュリティを高める効果が期待できる。本学の情報システムの利用者パスワードに含めることができる記号は、次の文字列である。

! # $ % & ( ) * + - . ; : < = > ? @ ~ [ ] ^ _ { | } /

⑶ パスワードの変更

情報セキュリティに関するリスクを IT センターが検知した場合、IT センターは利用者にパスワード変更の指示を与えることができる。利用者は、IT センターからパスワードを変更するよう指示を受けた場合に

は、遅滞なくパスワードを変更する。また、利用者自身がパスワード漏えいや不正利用のリスクを感知した場合には、速やかにパスワードを変更することが望ましい。

なお、パスワードの定期的な変更は、情報セキュリティ対策として必須ではない。これまで、パスワードを適切に管理する方法として「定期的な変更」や「記号を含む多様な文字列の利用」が推奨されてきた。しかし、これらの方法は、総当たり攻撃への対策を講じるうえで十分とは言えず、定期的な変更によってパスワードが簡易で推測されやすいものになるリスクもあることから、現在では「定期的な変更」よりも「長い文字列の利用」が推奨される傾向にある。長い文字列とは、少なくとも９文字以上の文字列を指す。意味のある文字列の頭文字を組み合わせるなどの方法で作成されるパスワードは、パスフレーズと呼ばれることもある。「長い文字列」と「記号を含む多様な文字列」の併用によって、より堅固なパスワードを作成することが望ましい。

⑷ パスワードの管理

パスワードを適切に管理するために、以下のア～ウを遵守することが望ましい。

ア　パスワードを他者に教えない。

イ　自己のパスワードを他者に知られないよう最大限の注意を払う。

ウ　パスワードを忘却しないよう努める。

パスワードを紙媒体や電子媒体等に記録して保管する場合は、以下のア～ウのいずれかの方法を用いることが望ましい。

ア　パスワードを構成する文字列の一部を伏せる。

イ　鍵などの物理的手段で保護可能な場所に保存する。

ウ　パスワード管理用アプリケーションを利用し、そのアプリケーションへのアクセスを何らかの方法で保護する。

4　パスワードに関する各種手続き

⑴ パスワード紛失の手続き

利用者がパスワードを紛失あるいは失念した場合は、所定の手続きによりパスワードを再設定することができる。パスワードを再設定するためには、IT センターの窓口、高槻・高槻ミューズキャンパスの各オフィス、堺キャンパスのパソコン教室の窓口で、身分証（学生証もしくは職員証等）を提示し、申請を行う。

⑵ パスワード事故の報告

アカウントの不正利用やパスワード漏えいのリスクを検知した利用者は、直ちに IT センターにその旨を報告する。

5　パスワードの取扱いに係る注意事項

⑴ パスワード詐取の恐れがある場所での利用禁止

学外のインターネットカフェや公共の無線を利用して本学情報システムへのアクセスを行わない。不特定多数が利用する端末や無線サービスを用いて本学情報システムにアクセスする行為は、パスワードやアカウントを詐取されるリスクを伴う。

⑵ 画面ロックの励行

コンピュータにログインしたまま離席する場合は、第三者が画面を閲覧したり端末を操作したりできないよう、画面のロック操作を行う。画面のロック操作にパスワードを用いる場合、他者から推測可能な文字列の利用を避け、長い文字列のパスワードを利用することが望ましい。

附　則

1　このガイドラインは、2019年11月６日から施行する。