C3255 利用者パスワードガイドライン

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2007年2月15日  A3205 | 新規作成 | 国立大学法人等における情報セキュリティポリシー策定作業部会 |
| 2015年10月9日  C3255 | パスワードの最短文字数を修正（6文字→8文字） | 高等教育機関における情報セキュリティポリシー推進部会事務局 |
| 2017年10月17日  C3255 | パスワードの安全性に関する最近の考え方を反映 | 高等教育機関における情報セキュリティポリシー推進部会事務局 |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

**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を利用する際のパスワードに関し、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。

解説：パスワードの望ましい管理方法として、かつては「定期的な変更」や「記号を含む多様な文字列の利用」が推奨されていたが、現在は総当たり攻撃への対策の観点から、それらの方策よりもむしろ長い（少なくとも9文字以上）文字列（パスワードでなく、パスフレーズと呼ばれることもある）を設定することが推奨される傾向にある。ただし、パスワードとして長い文字列の設定や識別が不可能な情報システムやサービスも存在し、こうした情報システムやサービスでは多様な文字列の利用が引き続き有用である。  
パスワードの管理を含めた最適な情報セキュリティ対策は情報システムの仕様や脅威の動向などとともに変化することから、本ガイドラインの規定内容については、定期的に見直しを行うことが望ましい。

**2. パスワードに係る全般的な注意事項**

2.1 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情報システムの利用を継続してはならない。

2.2 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、以下の条件を全て満足するものでなければならない。

・最低限8文字以上の長さを持つ。

・以下ア～ウの文字集合から各最低１文字以上を含み、エを加えても良い。

ア）英大文字（A～Z）

イ）英小文字（a～z）

ウ）数字（0～9）

エ）システムで使用可能な記号（@!#$%&=-+\*/.,:;[]|）

また、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。

・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）

・上記を並べ替えたもの、上記に数字や記号を追加したもの

・辞書の見出し語

・著名人の名前等固有名詞

解説：パスワードとして設定可能な文字列の長さや使用可能な記号の種類は情報システムによって異なるので、ガイドライン策定に先立ち当該情報システムやサービスの仕様を確認する必要がある。

2.3 パスワードの変更

　利用者は、アカウント発行者（全学アカウントに関しては情報メディアセンター、個別システムについてはシステム管理者）からパスワードの変更の指示を受けた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。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。

解説：パスワード漏えいによる不正利用やパスワード破りによるリスクを減らす手段として、パスワードの定期的な変更には一定の効果があるという考えもある。パスワードの有効期間やパスワード文字列構成検査および世代管理が可能なシステムでは、パスワードポリシーを強制することも可能である。一方で、強固なパスワードを設定し、変更しない方がよいという考え方もある。ここでは、後者の考えを基本に、パスワード漏えいによる不正利用の可能性をシステム管理者が検知したり、一般的なパスワード検査ツールで容易に解読されるようなパスワードの利用者を発見したりした場合に、システム管理者がパスワードの変更を要求するというモデルを想定している。

2.4 パスワードの管理

　利用者は、自己のパスワードについて、以下の管理を徹底しなければならない。

・自己のパスワードを他者に知られないように最大限の注意を払うこと。

・自己のパスワードを他者に教えないこと。

・パスワードを忘却しないように努めること。

・他の情報システムやサービス等で用いているパスワードと同じものを用いない（シングルサインオンの場合を除く）。

解説：他の情報システムやサービス等で用いているパスワードと同じパスワードを用いることは、それらのシステムでパスワードの漏えい事故が発生した場合の影響が懸念されることから避けるべきである。この結果、利用者が管理すべきパスワードが増えることになるため、失念を避ける観点からパスワードをメモすることを禁止する必要はないが、パスワードをメモする場合は他者への漏えいを防止するために以下のいずれかの方法を用いることが望ましい。  
・パスワードを構成する文字列の一部を伏せる。  
・鍵などの物理的手段で保護可能な場所に保存する。  
・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。

**3. パスワードに関する各種手続き**

解説：本項で扱う事項は実施手順等で別途定めておくべき内容であるが、利用者の便宜を図るためにガイドラインにおいて手続きを説明している。

3.1 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、発行部局に対して、所定の様式で、身分証（学生証もしくは職員証等）を持参し、パスワードのリセットを申請しなければならない。パスワードの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。

3.2 パスワードの事故の報告

　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、直ちに全学実施責任者にその旨を報告しなければならない。

**4. パスワード取扱に関する注意**

解説：本項で扱う事項は利用者向けのガイドラインに記述してもよい。A大学では利用者向けガイドラインに相当する文書が学内機器の利用を対象とするもののみであるため、学生等の私物機器での励行を対象に含める意図により、本ガイドラインに含めている。

4.1 パスワードの詐取の可能性のある場所での利用の禁止

　パスワードやアカウントを詐取される可能性があるので、学外のインターネットカフェなどに設置されているような不特定多数の人が操作（利用）可能な端末を用いての学内情報システムへのアクセスを行ってはならない。

4.2 画面ロックの励行

　利用者は、使用中のコンピュータにログインしたまま離席する場合は、他者が画面を閲覧したり操作したりすることができないよう、画面のロック操作を行わなければならない。

解説：画面ロックの方法としては、パスワードのほか、ジェスチャーや顔認証などがある。パスワードを用いる場合、短い数字（４桁以内）や他者から容易に推測されるような文字列を設定するべきではない。