D3255 認証情報管理ガイドライン

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 |
| 2019年12月27日  D3251 | 全面改定 | 長谷川明生（中京大学） |

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。

解説：認証情報として用いられることが多い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. 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、次のように分類される。

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２要素認証がある。２要素認証とは、上記の認証方式のうち２つを組み合わせて認証する方法である。２要素認証の例として、ICカードとPINコード、ICカードとパスワード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、以下の条件を全て満足するものでなければならない。

・パスワードの長さは8文字以上で、なるべく長い文字列とし、英字、数字および記号を含むこと。

・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

・"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

・著名人の名前等、周知の固有名詞

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。

3.3 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、およ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。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。

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、以下の管理を徹底しなければならない。

・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。

・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。

・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。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をよい。

・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（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）。

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。

**4. アカウント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。

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、所定の手続きで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、発行者が要求する場合には、アカウント発行者にその旨を報告しなければならない。

（参考情報）

　パスワードに対する攻撃法として、文字列を総当りする方法（ブルートフォース・アタック）やパスワード・リスト攻撃（漏洩したパスワードやよく使われるパスワードのリストを使う）が知られている。もっとも効率的な方法は、本人から直接聞き出すとか、盗み見るといった攻撃である。

　２要素認証は、IDとパスワードによる方法に比べると安全だが、SMSに２段階認証に使われる認証コード類似の数値を送りつけて、phishingサイトに誘導し、認証情報を詐取しようとする攻撃が観測されている。この場合、正規サイトのパスワードが破られたかどうかはわからないので、冷静に対処することが必要である。