○東京電機大学情報システム利用者パスワードガイドライン

（平成 30 年 7 月 27 日）
情報統括責任者
情報セキュリティ最高責任者
総合メディアセンター

1. 本ガイドラインの目的

本ガイドラインは、学校法人東京電機大学情報戦略ポリシーに基づき、本学の情報システム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。

パスワードは他人に知られると利用者本人の個人情報が漏洩するだけでなく、漏洩したパスワードを使って本学の情報システムを不正に利用されたり、犯罪などに悪用されたりする危険性がある。

本学の情報システムを利用する者は、パスワードの重要性を十分に理解し、他人から推測されにくく解析されにくい安全性の高いパスワードを設定すること、学外サービスとの間でパスワードの使い回しをしないこと、他人の目に触れないようにパスワードを管理することなど、責任を持って自己のパスワードの適切な管理と利用を行わなければならない。

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直ち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。なお、初期パスワードは発行後一定期間が経過すると利用できなくなるので、その前に変更すること。

2.2. 安全性の高いパスワードの設定

安全性の高いパスワードは、他人から推測されにくく、ツール等によるデータ解析で割り出しにくいものである。攻撃者がパスワードを解析する方法には、インターネット上で流失したパスワードを試す「リスト型攻撃」、文字の組み合わせを全て試す「総当り攻撃」、パスワードによく使われる文字列を試す「辞書攻撃」などがあり、これらからパスワードを守るにはデータ解析に時間がかかり、パスワードを探し当てることが事実上不可能にする必要がある。そのためにはパスワードには様々な文字種を利用し、パスワードの文字列の長さを長くすることが重要である。

利用者は、上記のような安全性の高いパスワードを設定するために、以下の条件を全て満足するように自己のパスワードの文字列を設定する必要がある。

(1) パスワードの文字列の長さを、10 文字以上 20 文字以下で設定する。

(2) パスワードの文字列には、以下の各文字種から各 1 文字以上を含むこと。

・ 英大文字（A～Z）

・ 英小文字（a～z）

・ 数字（0～9）

・ 記号のうち、情報システムで使用可能なもの

(3) 以下の文字列は他人が容易に推測もしくは解析により特定可能であるため、パスワードとして設定してはならない。

・ 利用者個人が保有する情報から容易に推測できる文字列(名前，ユーザ ID，メールアドレス，生年月日，電話番号等)

・ 辞書の見出し語，著名な人名，地名，商標等の固有名詞

・ 上記を複数結合したもの

・ 上記に数字や記号を追加したもの

・ 同じ文字や文字パターンの繰り返し

・ キーボードの文字配置等，容易に推測できる並びの文字列

2.3. 学外サービスで学内パスワードの使い回しをしない

本学の情報システムで使用しているパスワードを学外サービス（学外の Web サイトで提供されるサービス等）で使い回した場合、複雑なパスワードを使っていても 1 箇所でもパスワードが漏れてしまえば、同じパスワードを使っていた学内外の全てのサービスが不正に利用されてしまう。

そのため、利用者は、以下のとおり本学の情報システムで使用しているパスワードを学外サービスで使い回してはならない。学外サービス毎に全く関係のない複雑なパスワードを設定すること。ただし、本学の情報システムとして認証連携している学外サービスについてはこの限りでない。

(1) 学外サービスでは、本学で使用するパスワードを使い回してはならない

(2) 学外サービスでは、本学で使用するパスワードと類似したパスワードは推測されやすいため、使用してはならない

例：パスワードの何文字かだけを変更し、数字や規則性のある文字を付けて設定するなど。

(3) 学外サービスでは、本学で使用するパスワードと法則性があるパスワードは推測されやすいため、使用してはならない

例：複雑なパスワードを部分的に分けて順番を変えて設定するなど。

2.4. パスワードの変更

これまでは世間一般においてパスワードの定期的な変更が推奨とされてきたが、昨今では、むしろ定期的な変更を行うことでパスワードがパターン化し簡単なものになることが問題とされている。そのため、利用者は、短期間にパスワードの定期的な変更を行う必要はない。ただし、パスワードが漏洩した場合、またはその危険が発生した場合は、直ちに東京電機大学シーサート（TDU-CSIRT）にその旨を報告すると共に、パスワードを変更すること。

利用者は、パスワードの変更を以下のとおり実施すること。

(1) 利用者は必要に応じてパスワードを変更すること

(2) 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) 利用者はパスワードを短期間で変更することは不要である

(4) パスワード漏洩による学内システムの不正利用の恐れがある場合や総合メディアセンターからパスワード変更の指示を受けた場合には速やかにパスワードを変更しなければならない

2.5. パスワードの管理

利用者は、自己のパスワードを他人に知られたり自分でも忘れたりすることがないよう、以下のとおりパスワードを厳重に管理しなければならない。

(1) パスワードが記載されたものを他人の目に触れる場所に置いてはならない。特に付箋等でパスワードのメモを端末に貼り付けてはならない。

(2) ブラウザ等にはパスワードを保存しない。ブラウザ等にパスワードを保存すると、席を離れた時に勝手に利用されたり、不正アクセスを受けた際にブラウザ等から多数のシステムを利用されたりする恐れがある。

(3) 不注意でパスワードが他人に知られたり入力中に盗み見られたりすることがないよう最大限の注意を払わなければならない。

(4) 自己のユーザ ID やパスワードを他の者に使用させたり、開示したりしてはならない。

(5) 他の利用者のユーザ ID やパスワードを使用してはならない。

(6) 離席時のログオフ、スクリーンのパスワードロック、電源オフ等を行うことで、他人が画面を盗み見たり、操作されたりすることを適切に防止しなくてはならない。

(7) ノート等にパスワードのメモを作成した場合、メモを他人に盗み見られることやメモの紛失、盗難がないように厳重に管理すること。

(8) パスワード管理に携帯端末のアプリ等を利用する場合、クラウドサービスとの連携機能は使用せず、スタンドアロン状態での利用を優先すること。クラウドサービスにパスワードの情報を置くことにより、情報の保管箇所が多くなり、その分だけ漏洩する可能性が高くなる。

(9) パスワードを管理している携帯端末が紛失や盗難にあった場合、遠隔操作により当該携帯端末のロックやワイプ（データ消去）を行う等、情報流出の回避に最大限努めること。

2.6. パスワード詐取の可能性のある場所での利用の禁止と注意

公共利用の端末やホテル・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)可能な端末で、本学の情報システムへのアクセスのための認証を行ってはならない。端末に残った情報からパスワードが搾取され不正アクセスや情報漏洩に繋がる恐れがある。

また、学外の端末やネットワークから本学の情報システムに認証してアクセスする場合、VPN 接続を行うなど、安全な暗号化通信が行われていることを確認しなければならない。

3. パスワードに関する各種手続き

3.1. パスワードを失念した場合

利用者がパスワードを失念した場合には、総合メディアセンターに対して所定の様式でパスワードの再発行を申請しなければならない。

パスワードの再発行を受けた場合には、速やかに新しいパスワードに変更すること。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。なお、再発行されたパスワードは、再発行してから一定期間経過すると利用できなくなるので、その前に変更すること。

3.2. パスワードに関するインシデント（事故）が発生した場合

利用者は、パスワードが漏洩し、アカウントを他人に使用された場合、またはその危険が発生した場合は、直ちに東京電機大学シーサート（TDU-CSIRT）にその旨を報告すると共に、パスワードを変更すること。

以　上