利用者認証で用いるパスワード管理ガイドライン

（目的）

第１条　このガイドライン（以下「本ガイドライン」という。）は、公立大学法人横浜市立大学情報セキュリティ基本規程（制定　平成 30 年 4 月 1 日規程第 32 号）第 7 条第 2 項の規定に基づき、公立大学法人横浜市立大学の各情報システム（クラウドサービスで利用するものを含む。以下「システム」という。）の認証において用いる際のパスワードについて、利用者、またシステムの管理者（基幹ネットワークシステムにおいては企画総務部ＩＣＴ推進課、その他の個別のシステムについては各所管システム管理者。以下「管理者」という。）が意識し管理すべき事項について定める。

（基本理念）

第２条　不正アクセスやデータの盗難、消去・改ざん等の事故を未然に防止するには、システムの利用にあたって利用者の認証が確実に行われ、適正な権限が付与された者のみが利用できる環境を保証しなければならない。利用者本人（以下「本人」という。）を認証する手段は様々な方法があるが、パスワードなどの知識・文字列情報、ＩＣカードなどの所持・貸与物品、顔や指紋・静脈などの生体情報という三要素のうち、本来は二要素以上の組み合わせにより認証することが望ましい中で、本ガイドラインでは、本人しか知りえないパスワードを用いる認証の本人を識別、また証明するものとしての実効性を担保し、様々な事故を防止するため、利用者及び管理者がその管理において指針となる基準を示すものである。

（定義）

第３条　本ガイドラインで使用する用語は、それぞれ当該各号に定めるところによる。

（１）システム
　　情報処理を行うためのネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成された仕組みをいう。

（２）利用者ＩＤ
　　認証時に用いられる本人識別符号をいう。

（３）パスワード
　　認証を得るために必要な文字及び数字、記号等から構成される文字列をいう。

（４）パスワードクラッキング
　　データ解析や類推により他人のパスワードを不正に探り当てることをいう。

（パスワードの意味）

第４条　本人しか知りえないパスワードを設定する意味は、適正な権限を有しない第三者によるなりすましに起因したシステムへの不正アクセスの防止とあわせて、システムの操作を行った個人を特定できるようにし、もって不正利用を抑止するためにある。そのため、不正アクセスや不正利用により、本人のみならず法人全体、さらには他機関にも影響が生じるような情報漏洩、改ざん等の事故を生じさせないよう、利用者が設定するパスワード文字列について第５条の条件を満たし、またその管理において第６条の運用が徹底されるよう、管理者は必要な措置を講じなければならない。

（推奨すべき文字列設定）

第５条　本人しか知りえないという要件を満たすため、利用者は、パスワードに用いる文字列として以下を遵守すべきであり、また、管理者はその推奨、周知に努めなければならない。
　ただし、生体認証など別の要素による認証手段を併用している場合は、この限りでない。

（１）　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、原則として半角 10 文字以上を推奨とし、可能な限り長くすること。また、パスワードクラッキングを困難にするため、システムが許容する

範囲内で、以下ア～エのうち3種類の文字集合から最低各1文字以上を含み、かつ、同一文字は3文字以上連続させないようにすること。

ア　英大文字（A～Z）
イ　英小文字（a～z）
ウ　数字（0 ～ 9）
エ　記号（@、ドット、ハイフン、アンダースコア等）

（２）　パスワードに設定すべきでない文字列

以下アからオの文字列は、容易に推察可能であるため、利用者はパスワードとして設定すべきではなく、また管理者もその利用を推奨してはならない。

ア　利用者情報から容易に推測できる文字列（利用者ＩＤ、姓・名など）
イ　前項アを並べ替えたもの、又は前項アに数字や記号を安易に追加したもの
ウ　辞書に載っているような一般的な英単語や見出し語
エ　同じ文字の繰り返しや、キーボード上でわかりやすい配列（Q,W,E,R など）を多用する文字列
オ　著名な人物・所在地、又はそれらに数字や記号を安易に追加したもの
カ　別のシステムで使用しているパスワードと同一のもの

（利用者の自己管理）

第６条　利用者は、パスワードとして設定した文字列について、次に掲げる内容を遵守し、みだりに第三者が知ることのないよう十分留意しなければならない。

（１）利用者は、自己の責任においてパスワードを厳重に管理しなければならない。
（２）利用者は、パスワードをメモしたまま放置したり、端末にそのメモを貼り付けたりしてはならない。なお、やむを得ずメモを残す場合は、施錠できる机や金庫に保管するなど、安全な対策を講じなければならない。
（３）利用者は、他の者にパスワードを教えたり、不注意でパスワードが他の者に知られたりしてしまうことがないよう最大限の注意を払わなければならない。

また逆に、正当な理由がある場合を除き他の者のパスワードを探る又は調べるような行為を絶対に行ってはならない。

（４）利用者は、パスワードを電子メールなど形で残る手段で安易にやり取りしてはならない。

（パスワードを変更すべき時）

第７条　本人しか知りえない文字列を設定することを前提として、利用者がパスワードを定期的に変更することは不要とするが、以下に掲げる場合、利用者、また管理者はその例外として、第８条以降に掲げるとおりパスワード変更に対応しなければならない。

（１）初期（仮）パスワードが設定された場合
（２）管理者の指示があった場合
（３）同一の利用者ＩＤを複数の利用者で共有している場合で、かつそのうちの一人でも異動等が生じた場合
（４）パスワードクラッキング等の事故が生じた場合

（初期パスワードの変更）

第８条　利用者は、利用者ＩＤとともに発行された初期（仮）パスワードを速やかに別のものに変更することとし、初期（仮）パスワードのまま、システムの利用を継続してはならない。

（類似パスワードの使用禁止）

第９条　利用者は、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が、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。

（同一の利用者ＩＤを複数の利用者で共有している場合の変更）

第10条　利用者ＩＤに対してパスワードを設定する目的は、第４条に掲げるとおりシステムの操作を行った個人を特定できるようにすることも含まれることから、本来、一つの利用者ＩＤを複数の利用者で共有すべきではない。ただし様々な事情により、これを容認すべき場合もあることから、人事異動等によりその共有した複数の利用者のうち一人でも変更となる以下のような場合については、遅滞なくパスワードを変更することとし、かつ、前条のとおり、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。

（１）複数の利用者で同一の利用者ＩＤを共有している場合（組織の代表メールアドレスの利用者等）で、その利用者の構成が変更になった場合（同一システムに対して複数の利用者が一つのＩＤを共通利用していて、その利用者の中の一人でも人事異動や退職等で利用権限を失効した場合）。

（２）システムの管理権限をもつ複数の利用者で、同一の管理者用ＩＤ（root、Administrator等）を共有している場合に、その管理者の構成が変更になった場合（同一システムに対してシステムの管理権限を持つ担当者が複数存在していて、その中の一人でも変更になった場合）。

（不正アクセスを受けた場合の変更）

第11条　管理者は、パスワードクラッキングなど当該システムの安定運用が脅かされる不正アクセスが生じた場合、又はその疑いが極めて高い事態となった場合には、利用者に事前かつ特段の通達なく、強制的かつ一斉に、全ての利用者のパスワードを臨時的に変更する措置を講じることができる。

２　ただし、前項の措置を講じる場合には、影響が当該システムの利用者全体に及ぶことから、管理者は、利用者の混乱を最小限に抑えるため、不正アクセス等の事実の確認、影響の判断、代替運用や再発防止に関する迅速かつ確実な連絡・周知、相談窓口の確保など、善後策をすみやかに実施するよう努めなければならない。

（失念した場合の手続き）

第12条　利用者は、自分のパスワードを失念してしまった場合、管理者に対し、原則として身分証（学生証又は職員証）を提示するなど、管理者が本人確認を確実に実施できるようにした上で、パスワードのリセット（初期化）を申請しなければならない。

２　前項においてパスワードのリセットを受けた場合、利用者は、第８条の規定により遅滞なくその初期（仮）パスワードを変更しなければならない。

（不正使用が疑われる場合の報告）

第13条　利用者は、利用者ＩＤを不正に他者に使用される事態、又はその疑いが極めて高い事態が生じた場合には、パスワードが外部に流出している可能性があるという認識に立ち、直ちに管理者に対し、その旨を報告しなければならない。

（事務局）

第14条　本ガイドラインの運用にあたっての事務は企画総務部ＩＣＴ推進課が所管する。また、個別の各システムの管理者への周知、指示等については、公立大学法人横浜市立大学情報セキュリティ基本規程に基づき、部局情報セキュリティ運用責任者（ＩＣＴ推進課長）が行う。

（改定）

第15条　本ガイドラインにおいて見直すべき内容等が生じた場合の改定の取扱いについては、セキュリティに関する内容の審議・承認等を行う、ＩＣＴ推進委員会又は情報セキュリティ・情報基盤整備部会などの議論を経て決定するものとする。

附則

（施行期日）

１　このガイドラインは、平成３０年１０月１日から施行する。