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、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、記録媒体に加え、クラウドサービス（SaaS・PaaS・IaaS）、アイデンティティ基盤（IdP／SSO）、及びこれらに付随する認証・認可・ログ管理機能を含む仕組みをいう。

(2)　利用者 ID　認証時に用いられる本人に一意に割り当てられた識別子をいう。やむを得ない場合を除き共有を認めない。

(3)　パスワード　認証を得るために必要な本人が記憶する秘密の文字列をいい、パスフレーズを含む概念とする。

(4)　パスフレーズ　12 文字以上（推奨 16 文字以上）の意味のある語句の連結等により構成される長い秘密の文字列をいう。従来の複雑性（大小英字・数字・記号の組合せ）よりも長さと推測耐性を重視する。

(5)　パスワードレス(パスキー等)　公開鍵暗号にもとづく秘密鍵を用いた認証(例: FIDO2／パスキー）で、パスワードを用いずに本人確認を行う方式をいう。対象サービスでは本ガイドラインの文字列品質要件は適用除外とする。

(6)　多要素認証（MFA）　知識（例：パスワード）／所持（例：認証器）／生体の二要素以上を組み合わせる認証をいう。学外からの接続や重要度の高い操作に対して必須とする。

(7)　パスワードクラッキング　総当たり（ブルートフォース）、辞書攻撃、規則ベー

ス攻撃等により他人のパスワードを不正に推測・解読する行為をいう。

(8)　パスワードスプレー　多数のアカウントに対し、よくあるパスワードを低頻度で試行して認証突破を試みる攻撃をいう。

(9)　推奨パスワードマネージャー　組織が承認し、MFA を必須とする資格情報保管ツールをいう。

(10) ブラウザ内蔵パスワードマネージャー　Web ブラウザ（Edge／Chrome 等）の内蔵保存機能をいう。マルウェア感染時に同権限で復号・持ち出されるリスクがあるため､本ガイドラインにおける｢推奨パスワードマネージャー｣には含めない。

(11) 類似パスワード　編集距離が小さい、または部分一致等により、過去に使用したパスワードの軽微な変更に該当するものをいう。

(12) 身元属性情報　氏名、利用者 ID、学籍・職員番号、所属、著名な人名・地名等の本人や広く知られた属性をいう。

(13) アイデンティティプロバイダー（IdP）　利用者ＩＤの管理・認証・シングルサインオン（SSO）を提供する基盤をいう。

（パスワードの意味）

第４条　パスワードを設定する意味は、当該各号に定めるところによる。

(1)　パスワード（パスフレーズを含む）は、知識要素として本人しか知りえない秘密を用いることにより､適正な権限を有しない第三者によるなりすましを防止し、併せて操作主体を個人に紐づけて特定可能（アカウンタビリティの確保）とするために用いる。これにより不正利用の抑止を図る。

(2)　クラウドサービスの利用が一般化した現在においては、パスワード単独での保護は十分でないため、多要素認証（MFA）やパスワードレス（FIDO2／パスキー等）と組み合わせることを原則とする。

(3)　パスワードの漏えいは被害を急速に拡大させることから、利用者は第５条第１号を満たす強固なパスフレーズを設定し、第６条第１号に定める適切な管理を徹底する。

(4)　利用者および管理者は、パスワードの不適切な取扱いや不正アクセスにより、本人のみならず法人全体、さらには他機関に影響が及ぶ事故（情報漏えい・改ざん等）を招かないよう、発見時の速やかな変更・失効、トークンの失効、再認証の強制等、関連規程に基づく是正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確実に満たすため、利用者は、パスワード（パスフレーズを含む）の品質基準を次のとおり遵守し、管理者はその推奨・周知に加え、IDP 基盤等による技術的強制を講じなければならない。

(1)　パスフレーズの品質基準

ア　長さは最小１２文字、推奨１６文字以上とし、可能な限り長い文字列を用いること。

イ　文字種は大文字・小文字・数字・記号の組合せを必須とはしない。ただし、本項第２号及び第３号に定める禁止・拒否要件を重視すること。

(2)　パスワードに設定してはならない文字列（使用禁止）

ア　身元属性情報から容易に推測できる文字列（利用者 ID、氏名、学籍・職員番号、所属等）

イ　アに掲げるものの並べ替え、または数字・記号の安易な付加によるもの

ウ　一般的な辞書語や見出し語の単独使用

エ　同一文字の反復、連番、またはキーボード配列等の規則的パターン（例：QWER、1234）

オ　著名な人物・所在地、またはそれらに数字・記号を安易に付加したもの

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（使い回し）

キ　既知漏えいパスワードおよびその軽微変形（例：末尾に１～２文字を付した程度

(3)　再利用・類似の禁止

ア　同一システム内の再利用を禁止する。

イ　過去のパスワードと編集距離が小さい等の軽微変更による類似パスワードは禁止する。

ウ　異なるサービス間でのパスワード再利用（使い回し）を禁止する。

（利用者の自己管理）

第６条　利用者は、パスワード（パスフレーズを含む）について、次の各号を遵守し、みだりに第三者が知ることのないよう厳格に管理しなければならない。

(1)　厳格な自己管理

ア　パスワードは本人のみが知る秘密として管理し、他者との共有を一切行ってはならない。使い回しの禁止、推測容易な設定の禁止等、第５条の品質基準を遵守する。

イ　不審なサインイン通知、フィッシング入力、端末のマルウェア感染の疑い等が生じたときは、直ちに当該パスワードを変更し、ICT 推進課に報告する。

(2)　保管と記録の取扱い

ア　Web ブラウザに内蔵されたパスワードマネージャー（ Edge、Chrome 等）を利用したパスワードの保管は非推奨とする。これらのパスワード保存機能を利用する場合は、マルウェア感染時に保存された認証情報が第三者に取得される可能性があることを理解したうえで、保存対象を厳選する。

イ　パスワード（パスフレーズを含む）の保管・共有が必要な場合は、推奨パスワードマネージャーを用いる。

ウ　平文での記録（テキスト、スクリーンショット、チャット貼付、付箋等）を禁止する。やむを得ず一時的に記録する場合は、暗号化（例：Word／Excel のファイル暗号化）を施したうえで保管する。

(3)　第三者への開示・授受の禁止

ア　パスワードを求める要求（メール、チャット、電話、チケット等）に応じてはならない。正当な理由がある場合を除き、第三者への通知・授受を禁止する。

イ　業務連絡においても、パスワードを電子メール等の形で残る手段で安易にやり取りしてはならない。

(4)　入力・利用時の注意

ア　ログイン時は接続先の正当性（URL／ドメイン）を確認し、フィッシングサイトでパスワードを入力してはならない。判断に迷う場合は生成 AI を含む複数の情報源を用いて確認し、その結果を踏まえて正当性を判断する。

イ　共用端末からのログインは避ける。やむを得ず共用端末からログインした場合は、必ずブラウザのセッション情報等を削除する。

(5)　システムアカウントの取扱い（特権・管理用途）

ア　システムアカウントや特権アカウントのパスワードは、管理専用端末（PAW）でのみ取り扱うことを推奨する。やむを得ず管理専用端末以外からログインした場合は、必ずブラウザのセッション情報等を削除する。

イ　当該パスワードは、推奨パスワードマネージャーで厳重に保管する。

(6)　禁止行為

ア　他者のパスワードを探る、取得を試みる、または不正に利用する行為を一切行ってはならない。正当な理由がある場合を除き、監視・覗き見・解析を目的とした行為を禁止する。

（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（パスフレーズを含む）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。ただし、次の各号のいずれかに該当する場合は例外として、利用者および管理者は速やかにパスワード変更（ローテーション）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、速やかに変更する。仮パスワードのまま、システムの利用を継続することは禁止する。

(2)　管理者から指示があった場合

(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、パスワードスプレー等の事故が生じた場合

(5)　フィッシングサイト等でパスワードを入力したおそれがあるとき、または利用端末のマルウェア感染が疑われるとき

(6)　クラウドのアイデンティティ基盤（IdP／SSO）または利用中 SaaS から、当該資格情報に関する高リスクの通知（既知漏えいパスワード照合での一致、異常サインインの検知等）があったとき

(7)　人事異動、権限変更（特権付与・剥奪を含む）、組織改編、委託先変更等により、アクセス権限の見直しが必要となったとき

(8)　他のサービスにおけるインシデント等により、同一または類似のパスワードの使用が判明したとき（使い回しの判明を含む）

（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８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、様々な事情によってこれを容認すべき場合もあることから、次の各号にお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)　組織の代表メールアドレスの利用等、複数の利用者で同一の利用者 ID を共有している場合で、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９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 10 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 11 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、直ちに直属の管理者および ICT 推進課に対し、その旨を報告しなければならない。

（事務局）

第 12 条　本ガイドラインの運用にあたっての事務は 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、情報セキュリティ運用責任者（ICT 推進課長）が行う。

（改定）

第 13 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

このガイドラインは、平成 30 年 10 月 1 日から施行する。

附　則

このガイドラインは、令和８年４月１日から施行する。