パスワードデータ移行及び保存方式仕様書

成田市立図書館

趣旨

図書館システムが変更されても、利用者のパスワードがリセットされることなく継続して利用できるようにするため、パスワードの暗号化処理及び保存方式をプログラム言語Pythonのライブラリ Passlibと完全互換とする。また、第7次図書館システムにおいて移行データとして抽出する利用者パスワードデータを移行する。

機能　ハッシュアルゴリズムは、PythonのPasslibのPBKDF2(SHA-256)によるハッシュアルゴリズムを実装する。Passlib完全互換とすることで、外部実装による検証を可能とする。

仕様

1)移行データフォーマット

利用カード番号、$pbkdf2-sha256$<ストレッチング回数>$<ソルト>$<ハッシュ>

2)暗号化処理及び保存方式

暗号化方式	内容
ハッシュアルゴリズム	PBKDF2(SHA256)Passlibと完全互換とする。 参考URL https://passlib.readthedocs.io/en/stable/lib/passlib.hash.pbkdf2_digest.html
保存方式	Modular Crypt Formatと完全互換とする。 参考URL https://passlib.readthedocs.io/en/stable/modular_crypt_format.html パスワードハッシュに識別子を設け、複数のハッシュ化パラメータを混在できる設計とすること 保存方式の形式 $pbkdf2-sha256$<ストレッチング回数>$<ソルト>$<ハッシュ>
ソフト	ユーザ毎にランダムな16byteのデータを生成して、ハッシュと一緒に保存する。
ストレッチング回数	パラメータで変更できるよう設計すること。概ねパスワード検証が10ミリ行以下となるように調整することを想定している。

次の処理が行われたときに暗号化処理(A)と保存処理(B)を行うことを想定している。

新規パスワード発行時	・利用登録されている者に仮パスワードを発行したとき(A、B) なお、当館では利用登録時に全員発行を原則としている。
Myページログイン時	・Webサイト上でMyページにログインするとき(A)
パスワード変更時	・Myページで利用者自身が行ったとき(A、B)
パスワード再発行時(Webから利用者自身による)	・パスワードを忘れたときに、Webサイト上でパスワードのリセットと同時に行ったとき(A、B)
パスワード再発行時(業務端末から)	・パスワードを忘れた旨窓口に申請してきた者にパスワードをリセットし、再度仮パスワードを発行したとき(A、B)

5年後データ移行時には、1)データ移行フォーマットと同様の移行データを抽出すること

提案その他標準化　第7次図書館システムでは、PBKDF2(SHA-256)でパスワードハッシュ化しているが、このデータ移行を行った後、パスワードのシステムを超えた可搬性と、オープンソース等検証可能性により安全性を担保しているパスワードハッシュ化関数を活用する趣旨を踏まえた上で、bcryptやscrypt等への移行により安全性を高める提案及びパッケージ化提案をする場合は、積極的に協力する。