HP IceWall技術レポート:

改定された「電子政府推奨暗号リスト」と HP IceWall SSO 10.0 パスワード暗号化ライブラリのご紹介

1. はじめに

現在のITの世界においては、ある時点で安全とされた暗号アルゴリズムやハッシュ関数（以降、まとめて「暗号」と表記します）がハードウェアの性能やソフトウェア技術の向上により年月を経るにつれて安全でなくなっていく傾向があります。そのためアルゴリズムの改良は常に行われていて、より強度が高く安全に使用できる暗号が続々と作られています。

この状況の中で、2013年3月に「電子政府における調達のために参照すべき暗号のリスト」、略称「電子政府推奨暗号リスト(CRYPTREC暗号リスト)」が10年ぶりに改定されました。改定されたリストではいくつかの暗号が推奨リストから外れ、その代わりに新しいものが追加されています。

このように日々進化している暗号に対応するため、HP IceWall SSO10.0の認証モジュールでは認証データベースに格納するパスワードを暗号化する部分がパスワード暗号化ライブラリと呼ばれる独立した1個の共有ライブラリとなっています。パスワード暗号化ライブラリを入れ替えれば新しい暗号に容易に切り替えることができます。

本レポートでは、「電子政府推奨暗号リスト」の改定内容を簡単に説明すると共に、HP IceWall SSO 10.0のパスワード暗号化ライブラリの機能と、暗号を入れ替えた場合の運用についてご紹介します。

2. 電子政府推奨暗号リスト

「電子政府における調達のために参照すべき暗号のリスト」、略称「電子政府推奨暗号リスト(CRYPTREC暗号リスト)」はCPYPTREC※1により作成されています。従来の改定前のリストと、今回改定されたリストは以下のURLから取得できます。
(改定前) http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_fy2005.pdf
(改定後) http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf

上記の2つのリストを比較しますと、今回の改定のポイントは以下の通りです。

- 運用実績と今後の普及の見込みによる暗号の大幅な整理。
- 現在でも多く使用されていると思われるストリーム暗号RC4、ハッシュ関数SHA-1の「運用監視暗号リスト」入り。

特に大きなポイントは、ハッシュ関数SHA-1が「運用監視暗号リスト」に入ったことです。「運用監視暗号リスト」は「実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術のうち、互換性維持のために継続利用を容認するものの互換性維持以外の目的は推奨しない」と定義づけられています。つまり、新規に使用することは推奨されませんが、現在運用している所では当面継続利用が可能です。しかしながら、継続利用であってもより強度の高いものに移行するのが望ましいのは言うまでもありません。

HP IceWall SSO10.0にとっても従来のシステムで多く使われてきたSHA-1からより強度の高いハッシュ関数への移行は大きなポイントです。次に、HP IceWall SSO10.0のパスワード暗号化ライブラリについて説明します。

※1: 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。http://www.cryptrec.go.jp/index.html

3. HP IceWall SSO 10.0 のパスワード暗号化ライブラリ

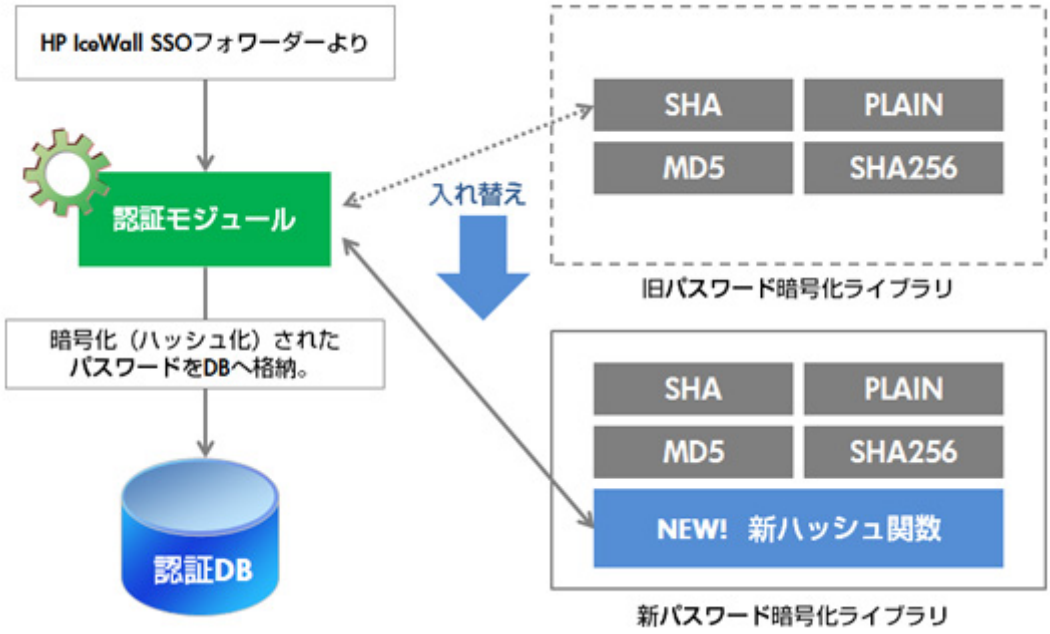
3.1. パスワード暗号化ライブラリとは

HP IceWall SSO10.0のパスワード暗号化ライブラリは、認証に使われるパスワードを認証データベースに保存する際に暗号化して秘匿するための機能を持ったモジュールです。

パスワード暗号化ライブラリはHP IceWall SSO 10.0の認証モジュール本体とは別の共有ライブラリとして提供されています。製品として新しい暗号がサポートされる場合にはパスワード暗号化ライブラリがパッチとしてリリースされ、認証モジュール本体は入れ替えずにパスワード暗号化ライブラリの共有ライブラリだけを入れ替えて使用することができます。別の共有ライブラリに分離されていることで、認証モジュール本体の更新

リリーススケジュールに依存せず、柔軟かつタイムリーに新しい暗号を使用できるようになっています。

また、認証モジュールとパスワード暗号化ライブラリが分離されている仕組みを利用して、ユーザーが独自のパスワード暗号化ライブラリを開発することができ、そのためのインターフェース仕様やサンプルプログラムも公開されています。



パスワード暗号化ライブラリの入れ替えによる新しい暗号の使用

3.2 使用可能なハッシュ関数

HP IceWall SSO 10.0の最新のパスワード暗号化ライブラリで使用可能な暗号（ハッシュ関数）は、以下のとおりです。

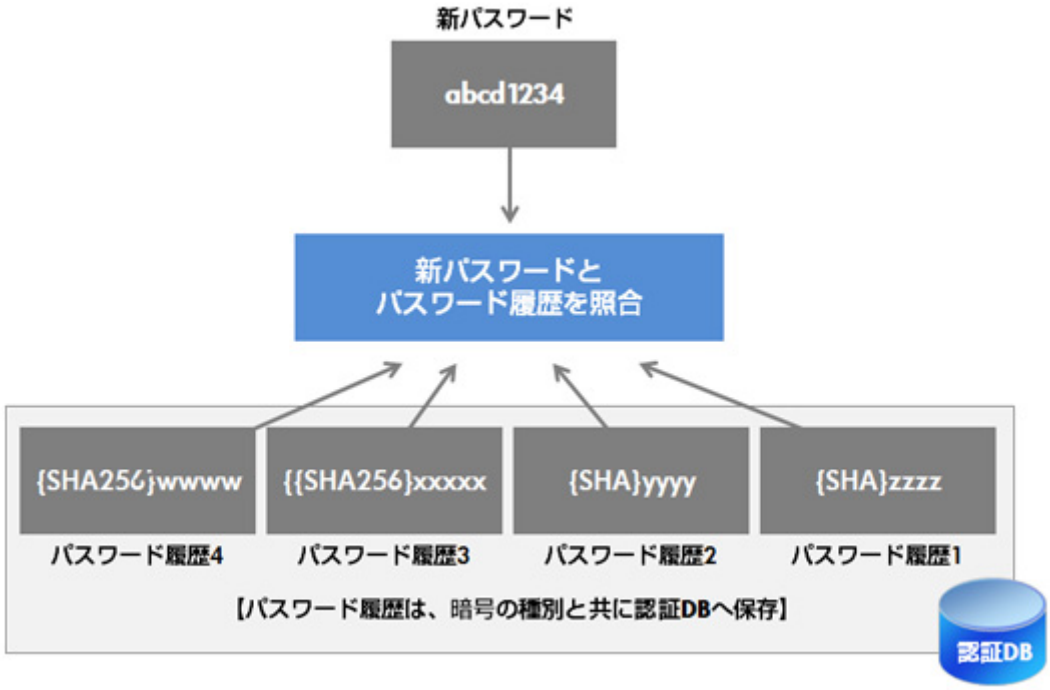
- プレーン（暗号化なし）
- MD5
- SHA（SHA-1）
- SSHA（ソルト付きSHA、Patch Release 1 から使用可能）
- SHA256（SHA-256）

前述の更新された「電子政府推奨暗号リスト」で推奨されているSHA-256も使用可能です。また、SSHA（ソルト付SHA）は、2013年8月30日に公開されたパッチ（Patch Release 1）で新たに取り入れらました。これ以外の暗号についても順次取り入れたモジュールをパッチとしてリリースして行く予定です。

3.3 より強度の高い暗号へのスムーズな移行

システムで使用している現在の暗号が問題ないとしても、将来ITの進歩によって強度不足になり、新しい暗号への移行が必要になる可能性があります。
HP IceWall SSO10.0のパスワード暗号化ライブラリでは、認証モジュールの設定ファイルに2，3行の変更を加えるだけで、容易に別の暗号へ移行できます。暗号を変更した後でユーザーがパスワードを変更した際には、新しい暗号化によるパスワードが認証データベースに保存されます。

暗号を移行した際に問題となるのがパスワードの履歴管理です。パスワードの履歴管理とは「同じパスワードの使用を何世代まで許可しないか」をパスワードのポリシーとして設定し、ユーザーが過去のパスワードを使い回す事を防ぐものです。このためには、今まで設定したパスワードを履歴として必要な世代分を保存しておいて、ユーザーが変更しようとしたパスワードと同じものが履歴の中にあるかどうか照合する必要があります。暗号を変更した前後においては、パスワード履歴に新旧の暗号化されたパスワードが混在している状態になることがあります。
HP IceWall SSO 10.0のパスワード暗号化ライブラリは、そのような状態でもパスワード履歴中のパスワードがどの暗号によって処理されたかを認識して正しく照合を行います。つまり、暗号を変更しても、以前のパスワード履歴を引き継いだ運用をすることができます。



HP IceWall SSO10.0でのパスワード履歴の照合

4. おわりに

HP IceWall SSO10.0のパスワード暗号化ライブラリは、認証モジュール本体とは別の交換可能なコンポーネントとして実装されているため新しい暗号への変更を容易にしています。また過去の異なる暗号のパスワード履歴も正しく扱うことができ、パスワードポリシーを維持した変更を行う事ができます 。

HP IceWall SSO10.0のパスワード暗号化ライブラリは、今後も普及や標準化した新しい強力な暗号を随時導入し、時代に合わせたセキュリティや使い勝手も含めた改善を継続して行います。

2013.8.30　新規掲載

執筆者　日本ヒューレット・パッカード テクノロジーコンサルティング統括本部
セキュリティスペシャリスト CISSP-ISSJP
藤波 勉