

Web アプリケーションによるパスワード運用管理システムの提案

1130343 新貝 達朗 【 清水研究室 】

1 はじめに

インターネットの普及に伴い、EC サイトやソーシャルネットワークサービスなど様々なサービスが提供されている。年々、Web サービスの利用人口は増加している。Web サービスを利用するためには、認証情報を登録しアカウントを作成する必要がある。多くの Web サービスはユーザの認証にパスワードを用いているのが現状である。そのため、複数の Web サービスを利用するユーザは、それぞれのサービスごとに複数のパスワードを安全に管理する必要がある [2]。

そこで、安全なパスワード管理を実現するために、パスワード運用管理システムが提案されている。多くのパスワード運用管理システムでは、OS の異なる端末ごとにアプリケーションを提供している。そのため、アプリケーションが提供されていない端末からは利用することが出来ない。しかし、ユーザが利用する端末は多種多様であるため、すべての端末で安全にパスワードを運用管理できる方法が必要である。

本研究では、端末の OS に依存しない安全なシステムを考察し、安全なパスワード運用管理システムの提案とシステムの実装する。

2 研究内容

本研究では、端末の OS に依存しない安全なパスワード運用管理システムとして、Web アプリケーションによるパスワード運用管理システムを提案する。

2.1 実装にあたって

本システムを実装にあたって、JavaScript を用いて端末側の操作画面の開発を行う。JavaScript は、Web ブラウザ上で実行可能であるため OS に依存しづらく、また、Web ブラウザは多くの端末で利用できる。そのため、JavaScript による実装で、パスワード情報を安全に管理することが出来る。

2.2 提案システム

提案するシステムのユーザとサーバ間の処理の手順を図 1 に示し、説明する。

1. クライアントがメールアドレスとマスターパスワードを入力し、メールアドレスをサーバへ送信する。
2. サーバは認証データを生成するためのソルトをクライアントへ返す。
3. クライアントはソルトとマスターパスワードを用いて生成した認証データとメールアドレスをサーバへ送信する。
4. サーバは暗号化されたパスワードのデータをクライアントへ返す。

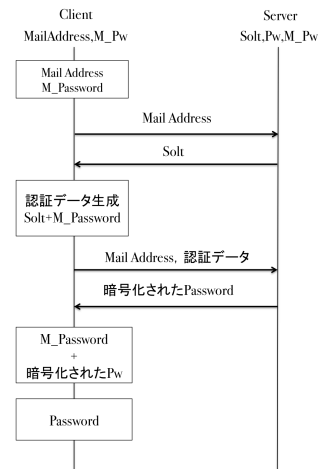


図 1 提案システム

5. マスターパスワードを用いて暗号化されたデータを復号し、パスワードの一覧を表示する。

2.3 実験方法

提案システムを PC、スマートフォン、フューチャーフォンなどの端末で実際に利用し、それぞれの端末からシステムが利用できる事を確認する。

3 評価

提案システムをそれぞれの端末から問題なく利用することができ、安全にパスワードが管理されることを確認した。しかし、保存するパスワードが増加した場合、暗号化と復号の処理に遅延が見られた。

4 おわりに

本稿では、多くの端末上で利用できるパスワード運用管理システムの提案について述べた。しかし、本システムはデータベースの情報を盗聴された場合、パスワード特定をされる可能性がある。更なる安全性をはかるためにデータベースに保存する情報を検討する必要がある。

参考文献

- [1] 平野 亮, 森井 昌克, “パスワード運用管理に関する考察および提案とその開発,” 2011.
- [2] 総務省, “パスワードの検討と管理,” <http://www.soumu.go.jp/>.
- [3] トレンドマイクロ社, “Web サイトのパスワード利用実態調査,” <http://jp.trendmicro.com/>.