HTML5 と公開鍵暗号技術を用いたユーザ認証システム

関　春奈

近年、多くの Web サービスにおいて、ユーザ名とパスワードを使用したパスワード認証という認証方法が使われている。しかし、パスワード認証には、ユーザが複数の異なる Web サービスで同じユーザ名とパスワードの組み合わせを使用しているというパスワードの使い回し問題が存在する。対策として、Web サービスごとに異なるパスワードを使用することが推奨されているものの、「異なるパスワードを設定すると忘れてしまう」などといった理由で、未だ多くのユーザがパスワードの使い回しを行ってしまっているのが現状である。

本研究では、パスワードの使い回し問題を解消する手段として、公開鍵認証に着目した。公開鍵認証には、サーバに不正アクセスが行われたとしてもそこには公開鍵しか預けられていないため、ユーザの秘密鍵は漏えいしないといった利点もあり、より安全性の高い認証になることが期待出来る。現在でも、SSL/TLS 通信の規格オプションや TrustAuth などでの公開鍵認証は可能だが、いずれも広い普及には繋がっていない。そこで本研究では、「公開鍵認証」、「Web 標準に準拠」、「多くの Web サービスで使われるパスワード認証並みの簡単な利用手順」といった 3 つの条件を満たす認証システムを実装し、それを用いた掲示板サイトを試作した。その際、公開鍵認証で使われるユーザの秘密鍵の保存に HTML5 の localStorage を用いて実現した。

実装した公開鍵認証システムは、安全性と利便性の 2 つの観点から比較項目を設け、パスワードの使い回し問題の対策として推奨されているパスワード管理ソフト、既存の公開鍵認証事例である SSL/TLS 通信の規格オプション、TrustAuth と比較を行った。その結果、公開鍵認証を用いているため、パスワード認証よりも安全性が高いのはもちろんのこと、既存の公開鍵認証事例よりも操作の負担が少なく、また、Web 標準に準拠しているため対応するブラウザが多く、利便性も向上していることを示した。

しかしながら、公開鍵認証で使われる鍵ペアに有効期限が設けられていない点や、秘密鍵を保存している localStorage の仕様上、ドメイン名とポート番号が同じ場合に秘密鍵を取り出すことが可能な点などといった課題も残っており、今後解消していかなければならない。また、公開鍵認証の実装に用いた JavaScript の数値型は 64 ビット浮動小数点形式しかなく、これを用いた整数演算による暗号処理を行うため、性能において課題が残る。コンピュータの性能の向上に合わせて、安全性を高めるために鍵ペアのビット数を大きくすると、暗号処理にかかる時間も長くなり、利便性が低下することが考えられる。

（指導教員　阪口哲男）