要 旨

ワンタイムパスワード認証方式の
高速化に関する検討

藤本 卓

情報通信分野の発展，携帯電話の急速な普及に伴い，携帯電話を使用してのインターネット利用人口が増加している．現在様々なサービスが存在し，それらサービスにおいて資格認証が必要不可欠となっている．その認証技術のひとつである，ワンタイムパスワード認証方式は，ネットワーク上における盗聴や，盗難，紛失時のなりすましを防ぐ．その中でもSAS-2 (Simple And Secure password authentication protocol, ver.2) は，認証時の負荷，通信コストも少なく，モバイル端末には最適な認証方式である．SAS-2 ではハッシュ処理を用いているが，処理能力の低い端末においては，処理負荷の大きいハッシュ関数の適用回数はできるだけ少ないほうがよい．

本研究では，モバイル端末上での認証に視野を絞り，SAS-2 をベースに，ユーザ認証時の負荷を減少，高速化を行う新方式を提案する．そして，従来の SAS-2 の処理時間，CPU 負荷との比較, 評価を行った．

キーワード　ワンタイムパスワード，SAS-2，ハッシュ関数

Abstract

An examination of high-speed password authentication method

Suguru Fujimoto

People using portable phones and the Internet are increasing, because information communication's and portable phone's technologies advance. Then various services using such mobile phones are necessary to authenticate the user. One-time password authentication methods protect against tapping, steal, and impersonation in the Internet. SAS-2 (Simple And Secure password authentication protocol, ver.2) is most simple and secure one-time password authentication method, and the method is useful on mobile communications. However, SAS-2 use hash functions, which have calculation costs.

In this thesis, I propose a new method, which is SAS-2 based and removes the hash overhead. Therefore, this method is high speed. Moreover, I compare and evaluate that new method and SAS-2 about processing speed and calculation load.

key words one-time password, SAS-2, hash function