要 旨

SAS-2 の同期問題対策時における なりすまし防止に関する研究

藤田　寛泰

近年, インターネット技術やモバイル端末の普及に伴い，多種多様な Web サービスが登場している．オンラインショッピングやインターネットバンキングなどの Web サービスは，ユーザの個人情報を扱うため，認証による不正アクセス対策が必須である．SAS-2 は，ワンタイムパスワード認証方式の一種であり，安全かつ高速な認証が可能である．しかし，このプロトコルは，サーバで次回認証情報が更新された後に障害により処理が中断した際にユーザ-サーバ間で認証情報が不一致となる問題 (同期問題) が生じる．この問題に対して認証情報のバックアップによる同期問題対策方式が提案されたが，その方式はリプレイ攻撃に対して脆弱である．本研究では，同期問題対策方式におけるなりすましの問題をチャレンジ/レスポンスの導入により解決する．

キーワード　認証，ワンタイムパスワード，SAS-2，同期問題，なりすまし，チャレンジ/レスポンス

Abstract

Study on Method to Prevent a Impersonation on an Asynchronous Problem of SAS-2

Hiroyasu Fujita

Development of internet communication and spread of mobile devices allow us to take various Web services. Web services such online shoppings and internet bancking deal user's private information which need to be protected, and authentication is highly required. SAS-2 (Simple And Secure password authentication protocol, ver.2) which is a one-time password authentication method, is able to provide strong authentication. However, an asynchronous problem of authentication information is occured by some troubles after a server stores next authentication information. Although the problem is resolved by backing up authentication information on the server, this solution lead the SAS-2 protocol to be vulnerable against impersonation attacks. In this paper, a method of resolving the impersonation problem is proposed. It has the mechanism of challenge-response authentication.

key words Authentication, One-time password, SAS-2, Asynchronous problem, Impersonation