要 旨

Broadband Web サービスに適した認証方式

永井 慎太郎

ブロードバンドの急速な発展に伴い 1 対多，多対多の通信形態を利用したアプリケーションやサービスが普及し始めている中で，一度に多数の Web 情報を参照するブラウジング手法がある．Web ページには認証を必要とするページが多数あるために，一度に参照できるブラウジング手法を使うと，複数のページを同時に認証する必要性がある．認証においては，公開鍵暗号と，共通鍵暗号を応用した方式がある．公開鍵認証においては認証時における負荷が大きいが，それに対して共通鍵の応用である SAS-2 認証では負荷は小さくてすむ．また，認証を一元化できるものとして「シングルサインオン」がある．しかし，認証は一元化できても，公開鍵暗号の応用による認証方式であるため，認証時の処理負荷が大きくなる．また，処理負荷が大きくなることにより，非常に高価なものになってしまうため，学校や個人などでは導入することが困難である．SAS-2 認証を用いた場合の 1 対多，多対多の通信形態では，認証情報を多数保持し処理を行わなければならない．そこで本研究では，認証負荷の小さい SAS-2 認証方式を用いて，通信形態が 1 対多や多対多においてユーザが認証を行うための処理量を軽減し，各ユーザが保持すべき認証情報を減らす方式の提案を行う．この提案方式により，既存技術であるシングルサインオンソフトに比べて認証処理が軽減され，低コストで導入することができるようになる．

キーワード　ブロードバンド，ブラウジング，ワンタイムパスワード認証方式，公開鍵暗号，共通鍵暗号，シングルサインオン

Abstract

The Authentication System for Broadband Web Services

Shintarou Nagai

A multi-view browsing technique is required because broadband services and multipart communication systems are increasing. If a user uses such technique, he has to be authenticated by plural web sites. An authentication procedure is applied by a public-key cryptography or a secret-key cryptography. Public-key authorization systems have costs, and the SAS-2 (Simple And Secure password authentication protocol, Ver.2) authentication method applied a secret-key cryptosystem which has little costs. " Single Sign On " can unify some authentications. However, that system has two problems: expensive and high-load, because such system is applied a public-key cryptosystem. In this thesis, I propose a new method using the SAS-2 and eliminate the problems that trouble to the existing studies.

key words Broadband, Browsing, one time authentication method, public-key cryptography, secret-key cryptography, Single Sign On