要 旨

SAS 認証を用いた Web 通信方式

小西 竜也

安全かつ高速な暗号化通信を実現する新しい方式を提案し，従来技術との比較を行う．

Web 上での通信において，保全性と機密性を確保する暗号化ベースのプロトコルとして，現在最も広く普及している技術は SSL(Secure Socket Layer) である．SSL は公開鍵暗号方式を用いての共通鍵共有を行っているため，コンピュータや携帯電話等の各端末にかける処理負荷が大きい事や，また，認証部分についても幾つかの問題点が存在する．

本稿では，既存技術の問題点を解決するための，新しい方式を提案する．提案方式には SAS（Simple and Secure）認証方式を用い，SSL の暗号化通信方式との比較・検証を行う．

キーワード　SSL，公開鍵暗号方式，鍵共有，SAS

Abstract

An Encription Communication Method with SAS

Tatsuya Konishi

I propose a new method that realizes secure and speedy encription communications. Moreover, I compare with a existing method.

The SSL(Secure Socket Layer) is most used in Web communication systems. However, the SSL has costs because the SSL uses a public-key cryptography for a key agreement. Therefore, such technique is useless for many machines: mobile phones and servers which has many user.

In this thesis, I propose a new method which solves such problems. The new method applies SAS(Simple and Secure) password authentication method, In addition I evaluate and compare with SSL that is encipherment communication form.

key words SSL, Public-key cryptography, key agreement, SAS