要 旨

モバイルコンテンツ課金プロトコル

大石 恭裕

本研究室では，コンテンツ流通支援方式の研究を行っている．近年，i-mode に代表される携帯電話でのコンテンツ流通が注目を浴びており，課金システムの開発が急務となっている．コンテンツを円滑に流通させるために，課金システムは重要であり，その中核として認証方式が位置付けられる．

本検討の目的は，本研究室で提案している SAS(Simple And Secure) と呼ぶワンタイムパスワード認証プロトコル，SAS をベースとした小額課金システムである SAS コインを，モバイルコミュニケーション，特に携帯電話等の処理能力の低い端末へ適用する際の最適な実装方式を確立することである．

本検討では，SAS に対する問題点を指摘し，それらを解決する SAS-K を提案し，評価を行った．さらに，SAS-K を用いた小額課金システムである SAS コインのプロトコルについて考察した．実装フィールドとして，ユーザ，コンテンツプロバイダ，課金センタの三者から構成される小額課金システムのプラットフォームを作成し，その環境において SAS-K および SAS コインの実装を行った．

提案方式 SAS-K を利用することにより，モバイル環境を含むあらゆる環境において，極めて安全な認証を行うことを可能とした．

キーワード　ワンタイムパスワード，パスワード認証方式，SAS，盗聴，なりすまし

Abstract

Billing Protocols in Mobile Communication Environments

Yasuhiro OISHI

We are studying on contents communications systems. Contents communication using "browser phones", particularly i-mode, have been getting popular. Billing systems are located as many functions in contents communications systems.

The research is aiming to install security functions, which are a one-time password authentication protocol, called SAS, and billing system, called SAS-Coin, to mobile communication environments with lower processing abilities.

First, SAS-K, a new type of one-time password authentication method, is proposed to cope with some attacks on SAS. Next, the SAS-Coin is studied, which is a simple billing method applying SAS-K. The SAS-K and SAS-Coin protocols are installed on a platform which has three players, Customer, Vendor, and Broker.

SAS-K, and an SAS-K based billing method, SAS-Coin have brought secure functions to mobile communications environments.

key words one-time password, password authentication, SAS, wiretapping, inpersonation