

要 旨

利用者同士における譲渡プロトコルの提案

中郷 有衣絵

近年の携帯電話の普及率はめざましいものがある．携帯電話におけるインターネットサービスが数多く利用され，その中でも電子マネー等の金額情報を扱うサービスが増加している．そこで，通信路上での盗聴に強く安全な課金方式 SAS-Coin が提案された．しかし，従来の課金方式では利用者同士が金額情報をやり取りが困難である．

本論文では処理負荷が小さく携帯電話に実装でき，利用者同士の金額情報のやり取りが可能な課金方式について提案を行っている．また利用者同士の通信における安全性，携帯電話に実装するに当たっての処理通信コスト，電子マネーの要求条件を満たすかの 3 点について評価を行っている．

キーワード 認証，ワンタイムパスワード，携帯電話，課金

Abstract

Proposal of transfer protocol in user

Yuie Nakagou

The spread of mobile phones is saturation. Many mobile communications are used, and services using electronic money. Then, SAS-Coin was proposed. SAS-Coin has been a safe payment system strong against tapping on the channel. However, as for this payment system, a user and a user cannot exchange money information.

In this paper, a new fee collection system is proposed. Communication can do the fee collection system to propose between users. The evaluation method has been three points of the effectiveness of the safety of the communication of the user and the communication cost.

key words authentication, one-time password, mobile phone, payment