要 旨

非接触式 IC カードを搭載した携帯電話への認証システムの実装

神山　真一

近年，無線通信を利用してデータの送受信を行うことのできる非接触式 IC カードが，電子マネー，乗車券などのサービスに利用されている．また，非接触式 IC カードが，携帯電話にも搭載されたことにより，携帯電話が電子マネーやクレジットカードなどの機能を持つようになってきた．これらのサービスを安全に提供するには，サービス権限のないユーザが不正にサービスを受けることを防止するために認証を行う必要がある．しかし，現状の非接触式 IC カードを利用したサービスの認証は，カードの製造番号やカード内に保存されたパスワードが利用されている．これらの方式では，認証時に送信する認証情報が一定のため，悪意のある第三者が正規の利用者になりすますことが可能になる．

本論文では，非接触式 IC カードを搭載した携帯電話に認証情報を毎回変化させるワンタイムパスワード認証方式 SAS-2(Simple And Secure password authentication protocol ver.2) を適用した認証システムの提案を行い，非接触式 IC カードを搭載した携帯電話に実装して速度評価を行う．

キーワード　　認証，ワンタイムパスワード，非接触式 IC カード，SAS-2

Abstract

An Implementation of authentication system using a cellular phone with a Non-Contact type IC Card

KOUYAMA, Shinichi

In recent years, Non-Contact type IC Card which is sending and receiving of data by using wireless communication is used for service such as electronic money and tickets, etc. Also a cellular phone came to have functions such as electronic money or a credit card because Non-Contact type IC Card was put on a cellular phone. To offer these service safely, it is necessary to perform the certification , which prevent a user who does not have authority that receive the service receive the service at illegality. However, the authentication of the service that used a Non-Contact type IC Card almost used methods of a production number or password which is saved into Non-Contact type IC Card. It is possible for illegal user to pretend regular user because these methods does not change authentication information sending at authentication.

In this paper, I have proposed an authentication system that use a cellular phone which has a Non-Contact type IC Card which applied an one-time password atuhentication methods SAS-2 which changes a certification information every time. I make an proposal of authentication system on cellular phone with Non-Contact type IC Card and evaluate transaction speed.

key words anthentication, one-time password, SAS-2, Non-Contact type IC Card