

# 要 旨

## 携帯電話端末を用いた FeliCa 統合認証システム

土居 絵美

FeliCa は「かざす」だけでサービスが利用できるという利便性から様々なサービスに用いられている。近年では、携帯電話端末に FeliCa チップが搭載されたことにより、ユーザは 1 台の携帯電話端末で多種多様なサービスを利用することが可能となった。FeliCa を用いて、ユーザの個人情報や金銭情報を扱うサービスでは、第三者による盗聴やなりすましの危険性を回避する必要がある。この危険性に対して現在、認証および暗号化機能を保持した専用のリーダ/ライタが利用されている。しかしながら、専用のリーダ/ライタはリード/ライト機能のみを保持したリーダ/ライタと比べ高価なものとなっており、インフラ整備に掛かるコストが高くなるという問題が挙げられる。

本論文では、非接触 IC チップ FeliCa を搭載した携帯電話端末にワンタイムパスワード認証方式 SAS-2 を適用した FeliCa 統合認証システムを提案し、有用性を示すために評価実験を行う。

キーワード 認証，ワンタイムパスワード，FeliCa，SAS-2

# Abstract

## Authentication Systems using FeliCa on Cellular Phone

Emi DOI

FeliCa is often used in various services because of convenience of usage. In recent years, FeliCa is also equipped on a cellular phone, and the user can use for various services with the one device. The threats which third persons impersonate registered users in FeliCa services with the user's personal information and the digital money must be dealt with appropriately. Nowadays, for tackling of the threats, an exclusive use R/W (reader and writer) which has authentication and encryption functions is most presently available. However, the exclusive use R/W is more expensive than the simple R/W which doesn't have authentication and encryption functions, and it is difficult to build a service infrastructure.

In this paper, authentication systems using FeliCa on a cellular phone is proposed. The systems counter the threat by applying one-time password authentication protocol SAS-2 (Simple And Secure password authentication protocol, Ver.2). Finally, I have shown that the result of the evaluation experiments for showing the expediency of the systems.

***key words*** authentication, one-time password, FeliCa, SAS-2