要 旨

スキミングに耐性を持つ
携帯電話 FeliCa 統合認証プロトコルの提案

坂本　隼人

近年，FeliCa チップが搭載された携帯電話の普及に伴い，FeliCa サービスを利用するユーザが急速に増加している．ユーザの個人情報や金銭情報を扱う FeliCa サービスの場合，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，認証及び暗号化機能を有した専用リーダ/ライタと FeliCa チップの共通領域が利用されている．しかし，専用のリーダ/ライタは非常に高額で，インフラ整備に掛かるコストが FeliCa サービスを提供する企業にとって大きな負担となる．先行研究により，安価な簡易 R/W を用いてユーザ認証およびデータの暗号化を行える FeliCa 統合認証システムが提案されているが，この方式では第三者からのスキミングによるなりすましの危険性があるため，安全な FeliCa サービスを提供できない．

本稿では，スキミングに耐性を持った新たな携帯電話 FeliCa 統合認証プロトコルを提案し，その安全性を評価する．

キーワード　FeliCa，認証，スキミング，なりすまし

Abstract

A Proposal of FeliCa on Cellular Phone Authentication Protocol that avoids Skimming

Hayato SAKAMOTO

In recent years, cellular phone equipped with FeliCa is widely used, and the user using FeliCa services are increasing. In the case of FeliCa services using user's personal data or digital money, it is necessary to evade wire tapping and impersonation attack by third parties. Nowadays, for tackling of the threats, an exclusive R/W (reader and writer) and FeliCa chip common area which has authentication and encryption functions is most presently available. However, exclusive R/W is very expensive. Therefore, a large sum of initial investment is necessary to provide FeliCa services. As an earlier study, the authentication system to be able to encrypt data and authenticate user by using inexpensive multipurpose R/W is proposed. However, this system cannot provide safe FeliCa service because it cannot evade impersonation attack by skimming by third parties.

In this paper, we proposed FeliCa on cellular phone authentication protocol that avoids skimming. Finally, we evaluate the safety of the proposed protocol.

key words FeliCa, authentication, skimming, impersonation