要 旨

SAS-2 鍵開閉システムにおける
同期問題の解決

井 上　翔 太

近年，従来の物理的な鍵に変わり，IC カードや専用機器による電子鍵システムがオフィスビルや大学，金融機関や工場などで入退室管理のために使われ始めている．そのような中，ワンタイムパスワード認証方式 SAS-2(Simple And Secure password authentication protocol, Ver.2) を用い，鍵複製機能も搭載したノードキー型鍵開閉システム SAS-2 鍵開閉システムが提案された．しかし，SAS-2 鍵開閉システムには通信障害や，第三者による通信遮断などによって鍵と錠側の値にずれが生じ，その結果として認証が失敗してしまう同期問題が残る．

本論文では SAS-2 鍵開閉システムにおける同期問題を解決する．この中で，SAS-2 鍵開閉システムを構成する 3 つのフェーズについて，同期問題を解決するプロトコルの提案と評価を行う．これにより，提案した SAS-2 鍵開閉システムが実際の使用に耐えうる安全性を持つことを示す．

キーワード　認証，ワンタイムパスワード，電子鍵，同期問題，SAS-2

Abstract

Resolving Asynchronous Problem of SAS-2 Key-free Application System

INOUE, Shota

In recent years, electronic key systems with Smart Cards or special purpose machines are used at office buildings or university buildings for gate control. SAS-2 Key-free Apllication System, which uses a one- time password authentication protocol SAS-2(Simple And Secure password authentication protocol Ver.2) for electronic keys authenticaion is proposed. This system has already demonstrated, but asynchronous problem is not resolved yet.

In this paper, we resolve asynchronous problem of SAS-2 Key-free Application System. We will propose and identificate the protocol that we propose. Finally, we have shown that the high convenient key-free system for gate control is realizable by using SAS-2 Key-free Application System.

key words Authentication, One-time password, Electronic Key, Asynchronous Problem, SAS-2