# 要 旨

## SAS-2 鍵開閉システムの実装

大 岸 弘 和

近年，オフィスビルや大学といった高いセキュリティが必要とされる多くの場所で入退室管理のために，IC カードや専用機器による電子鍵システムが普及してきている．電子鍵システムとは，IC カードや携帯端末等の専用機器を電子鍵として利用した鍵開閉の許可/非許可を電子的に制御するシステムのことである．

現在広く導入されている電子鍵システムは，鍵を開けるために行う電子鍵と認証サーバとの認証に，同じパスワードを繰り返し使用する固定パスワード方式を用いているものが多い．しかし，固定パスワード方式では，電子鍵と認証サーバ間でのパスワードのやりとりを第三者に盗聴されてしまうと，なりすましといった被害を受ける危険性がある．そういったなりすましに対して高い安全性を持つ認証方式に，パスワードが毎回変わるワンタイムパスワード認証方式がある．

本論文では，なりすましに対して高い安全性を持ち，携帯電話のような小型端末でも高速処理が可能なワンタイムパスワード認証方式 SAS-2 (Simple And Secure password authentication protocol, Ver.2) を用いた鍵開閉システムの実装及び評価について示す．

**キーワード**　認証, ワンタイムパスワード, 電子鍵, 電気錠, SAS-2

# Abstract

## Implement Of SAS-2 Key-free Application System

OGISHI, Hirokazu

In recent years, electronic key systems with with IC cards or special purposemachines are widespread at office buildings and university buildings for gate control. eectronic key systems is a system that controls permission/non-permission of the key opening and shutting that uses IC card and special purposemachines as an electronic key in the electron. There are a lot of one of the electronic key system that has been introduced widely at present to use the Reusable Password method used repeating the same Password. but, Reusable Password method has danger of receiving damage of disguising it when password between an electronic key and the authentication server will be being communicated. There is a one time password method of Every time password is changed for the disguise.

In this paper, High safety for the disguise and possible to high-speed process it even with a small terminal like the cellular phone, implement and the evaluation of the electronic key system that uses the one time password method SAS-2(Simple And Secure password authentication protocol, Ver.2)) .

***key words*** authentication, one-time password, electronic key, electronic lock, SAS-2