要 旨

SAS-2 鍵開閉システム

中原 知也

近年， 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で入退室管理のために使われている．セキュリティポリシによる本人確認の重要性が増していくにつれて，このような電子鍵システムは今後あらゆる場面で用いられることが期待されているが，その反面，電子鍵認証方式の応用に関する研究は，これまでほとんどされていない．また従来の電子鍵システムでは，利用者が鍵を複製できずオフィスのような組織単位での利用には不向きである．

本論文では，特にオフィスビル環境において，個々のオフィス管理者による鍵複製を可能とする，ワンタイムパスワード認証方式 SAS-2(Simple And Secure password authentication protocol, Ver.2) を用いたノードキー型鍵開閉システムを提案する．この中で，新たなスペア鍵生成フェーズの必要性について示し，当フェーズの提案と評価を行う．これにより，提案したスペア鍵生成フェーズを含めたワンタイムパスワード認証方式 SAS-2 を適用することで，安全で利便性の高い電子鍵システムが実現できることを示す．

キーワード　認証, ワンタイムパスワード, 電子鍵, オフィスシステム, SAS-2

Abstract

SAS-2 Key-free Application System

Tomoya NAKAHARA

In recent years, electronic key systems with IC (integrated circuit) cards or special-purpose machines are used at office buildings for gate control. From now on, that these electronic key systems come to be used in various scenes will be expected as the importance of the security policy with identification increases. However, the research on application of an electronic key authentication system is not done almost until now. By the conventional system, it is unsuitable for use in an organization unit like office because a user can't duplicate an electronic key in security.

In this paper, I have proposed a node key system applied to a one-time password authentication protocol, SAS-2 (Simple And Secure password authentication protocol and Ver.2), which enables the key duplicate by each office administrators in office building especially. In this system, the improvement protocol which can duplicate a spare key safely is needed. I have proposed this improvement protocol and evaluated the usefulness of this system. Finally, I have shown that the high convenient key-free system for office buildings is realizable by using improvement SAS-2 protocol.

key words authentication, one-time password, electronic key, office system, SAS-2