要 旨

無線 LAN における
セキュアローミングプロトコルの提案

岡 田　勇

近年，無線 LAN(Local Area Network) は企業や空港，一般家庭で急速に普及しつつある．しかし，無線 LAN は無線通信を行うために，盗聴や成りすましといった行為が容易にできてしまうことからセキュリティ対策が課題とされていた．その中で無線 LAN のセキュリティ規格として IEEE802.11i が標準化された．IEEE802.11i は，ユーザを認証するために多くのコストが必要である．そのために，中小企業や一般家庭といった小規模な環境では IEEE802.11i を使った無線 LAN を構築できない．

本研究では，低コストで安全な無線 LAN 構築を可能とする，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，セキュアローミングプロトコルを提案する．この中で，新たなローミング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．そして，提案プロトコルが，低コストで安全な無線 LAN を実現できることを示す．

キーワード　認証，無線 LAN，IEEE802.11i，ローミング，SAS-2

Abstract

A Secure Roaming Protocol for Wireless LAN

OKADA, Isamu

In these years, wireless LAN is spread rapidly to the company, the airport and the home. Wireless LAN is easy of bugging and spoofing. IEEE802.11i was standardized as a security standard for wireless LAN. IEEE802.11i needs many costs for the certification of the user. The small scale environment such as small-to-medium-sized enterprises and home cannot build the wireless LAN of IEEE802.11i.

In this paper, I propose a roaming protocol for secure wireless LAN at low costs, using one-time password authentication protocol SAS-2(Simple And Secure Password Authentication Protocol, Ver.2). In the wireless LAN, the improvement protocol which roaming safely is needed . Finally, the proposed protocol realized low cost and secure wireless LAN.

key words Authentication, One-time password, SAS-2, Wireless LAN, Roaming