要 旨

セキュアな無線通信システムの構築

岡 村　大

近年，無線通信を用いてネットワークに接続する無線 LAN が普及している．LAN ケーブルが必要ないため，移動が容易，導入や運用コストが安いなどのメリットがある．無線 LAN は電波を扱う性質上，盗聴や成り済ましの危険性があるため，認証や暗号などのセキュリティ対策が必要である．しかし，多くの企業ではコストの問題により，脆弱性のある無線 LAN 機器を使用しており，非常に危険な状態である．本論では，古い無線 LAN 機器を用いたセキュアな無線通信システムを提案，構築し，評価する．提案システムでは，ワンタイムパスワード認証方式 SAS-2 を用いて，通信経路上のデータを暗号化する．SAS-2 を用いることで，古い無線 LAN 環境であってもセキュアな通信を実現する．また，暗号化をソフトウェア処理のみで実現することで，物理コストを大幅に削減する．提案システムを実際に構築し，セキュリティ，コスト，速度の 3 項目から評価し，有効性を示す．

キーワード　無線 LAN, ネットワーク, ワンタイムパスワード, SAS-2，サプリカント

Abstract

A secure wireless communication system

Okamura, Dai

In recent years, the wireless LAN connected to a network using wireless communications has spread. The movement is easy and the cost is cheap, because LAN cable is unnecessary. The wireless LAN treats the electric wave. There is danger of tapping and the disguise. Security countermeasures such as authentication and a code are required. However, there is no money in many companies. Therefore, vulnerable wireless LAN equipment is used. A secure communication system is built using old wireless LAN equipment. It encodes data by using one-time password authentic method SAS-2. A secure communication system is realized in an old wireless LAN environment using SAS-2. Cost is reduced by enciphering by software. A proposal system is actually built. Security, cost, and speed are evaluated.

key words Wireless LAN, Network, One Time Password , SAS-2, Supplicant