要 旨

SAS-2 による VPN を用いた
セキュアな公衆無線 LAN サービスの提案

遠藤　竣

近年，通信キャリアを中心として，駅，空港，街中などあらゆる場所で公衆無線 LAN サービスが提供されている．また，訪日外国人観光客増加への政策として，観光地での無線基地局設置が進められ，年々アクセスポイントが増加している．

しかし，これらの観光客向け公衆無線 LAN サービスは，データの暗号化がされていないものや，共通のパスワードを使用しているものが殆どである．観光地の様な不特定多数が利用する環境下では，第三者による盗聴や改竄等の中間者攻撃の危険性がある．この課題に対応する既存サービス方式として，みあこネットが存在する．既存サービスでは，ファイアウォール制限による設置者の負担や，VPN 利用者限定のサービスであることから，汎用性が低くなる．

本論では，ワンタイムパスワード認証方式 SAS-2 による VPN を用いたセキュアな公衆無線 LAN サービスを提案，構築し，評価した．提案サービスでは，SAS-2 を用いてクライアントと VPN サーバの相互認証を行い，その認証情報を用いて通信データの暗号化を行う．SAS-2 を用いることで暗号化鍵情報を通信路に流すこと無く更新できることや，鍵更新をセッション毎に行う為，公衆無線 LAN 環境においてセキュアな通信を実現する．また，証明書が必要無いこと，ソフトウェアでの実装することにより低コストでの提供が可能である．提案サービスを実際に構築し，安全性，汎用性，コストの 3 項目から評価し，有用性を示す．

キーワード　公衆無線 LAN サービス，VPN，ワンタイムパスワード，SAS-2

Abstract

Proposal of Secure Public Wireless LAN Service using VPN by SAS-2

ENDO, Shun

In recent years, communication carriers provides public wireless LAN services in train stations, airports, the city. The wireless LAN base station install in sightseeing spot is promoted by The Japanese government policy to increase of foreign tourists.

However, these public wireless LAN services for tourists are offered by a non-password or a shared password, and data are not encrypted. In the environment that many people use this service, it have a risks. For example, the eavesdropping, the manipulation and man-in-the-middle attack. The existing service avoiding such risks is The MIAKO Net. This service has the limit of the firewall, and member-limited service. Thus, versatility lowers.

In this paper, I propsaled a secure public wireless LAN service using VPN by SAS-2. Suggestion service using SAS-2, and perform cross-certification. And the encrypted data is generated by certification information that change every time. Encryption key information do not exchange in the Internet and encryption key exchange is every session, because using SAS-2. From the above, This service is able to secure communications in public wireless LAN service that does not safety. Also, it can hold down a price low because it do not use certificates and it is made by Software. I implement this service and evaluate it from three items of safety, versatility, the cost and show usefulnes.

key words Public Wireless LAN Service, VPN, One-time password , SAS-2