要 旨

SAS-X による VPN を用いたセキュアな Wi-Fi サービスの提案

合田 亮登

近年，ICT 技術の発達により，空港や駅に加えて，商業施設や観光施設等のあらゆる場所で公共無線 LAN(Local Area Network) サービスが提供されている．ICT サービス・インフラの高度化・利用促進政策の一つとして，Wi-Fi 等による ICT 基盤の整備が推進されているおり，年々アクセスポイントが増加している．しかし，これらの公共無線 LAN サービスの多くはデータの暗号化のなされていなものや，共通のパスワードを用いているものが殆どである．無線 LAN には，第三者による盗聴や改ざんによる中間者攻撃の危険性がある．この課題に対応する既存の方式として，遠藤による SAS-VPN がある．既存方式では，物理媒体を用いて対面で受け渡しするために利便性悪い利用者は SAS-VPN 利用者登録窓口に直接出向く必要があり，SAS-VPN 方式におけるサービスを直ぐに受けることはできない．

本稿では，ワンタイムパスワード認証方式 SAS-X(1) 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，通信の遅延や第三者からの攻撃などの理由によりによって通信に障害が発生することで，サーバとクライアントの認証情報が異なり，その後の認証を行うことができないという同期問題を修正した SAS-X(1) 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-X(1) 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，利便性を評価し，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-X

Goda Ryoto

In recent years, public wireless LAN services are provided at all places such as commercial facilities and tourist facilities in addition to airports and stations. The wireless LAN base station install in sightseeing spot is promoted by the Japanese government policy to improve ICT services and infrastructure. However, these public wireless LAN services 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 sniffing, the wiretapping, and man-in-the-middle attack. As a method to deal with this problem, there is SAS-VPN by Endo.

In the existing method, since it is handed over to the facing side using the physical medium, it is necessary for the user who is not convenient to visit the SAS-VPN user registration window directly and can not immediately receive the service in the SAS-VPN method.

In the proposed service, SAS-X (1) which corrected the synchronization problem, , Mutual authentication between the client and the VPN server is performed, and the communication data is encrypted using the authentication information.

By using SAS-X (1) which fixes the synchronization problem, it is possible to update encrypted key information without flowing the encrypted key information to the communication path, and since the key update is performed for each session, secure

communication is realized in the public wireless LAN environment In addition, it is possible to provide at low cost by not implementing the certificate by implementing it with software, actually constructing the proposed service, evaluating the convenience, and demonstrating its usefulness.

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