公衆無線 LAN を安全に利用するための VPN 方式

1240340　田之上陽向　【 セキュリティシステム研究室 】

1　はじめに

近年，様々な場所で公衆無線 LAN サービスが提供されている．便利である反面，セキュリティ上の様々な問題が指摘されており，VPN により安全な通信路を確保する手段が有効である．本論文では．SAS-L2(Simple And Secure password authentication protocol, Light-processing version type-2) ワンタイムパスワード認証方式 [1] を適用した SAS-VPN を提案する．

2　公衆無線 LAN への脅威と既存対策方式

公衆無線 LAN は利便性が高いが，通信内容や個人情報の漏洩の危険性が存在する．この対策として VPN が有効である．

株式会社トリニティーセキュリティーシステムズが考案した IPN(Identified Private Network) は，SAS-2 ワンタイムパスワード認証方式を適用し，情報送信単位毎に鍵を更新して通信を暗号化する方式である．

IPN を実装した無線 LAN は、パケット毎 (レイヤ 3) に SAS-2 による鍵更新を行うハードウェアソリューションである [2]．その後，ソフトウェアでの開発も試みられたが，専用ハードウェアを用いないため処理速度が低下し，セッション毎 (レイヤ 5) に鍵更新を行う方式に変更され、安全性の検討が必要となった．

3　提案方式

当研究室で新たに考案した，SAS-L2 ワンタイムパスワード認証方式を鍵更新に用いることで，ソフトウェア実装においても，実用的な処理速度を確保し，同時に安全性を確保できる新しい VPN 方式である SAS-VPN を提案する．

3.1　SAS-L2 ワンタイムパスワード認証方式

SAS-L2 は，従来最高速であったワンタイムパスワード認証方式 SAS-2 に比較してさらに高速で，特に，被認証側において処理負荷の大きい一方向性変換の適用を必要としない，すなわち，処理負荷がほぼゼロに近い方式である．

3.2　SAS-VPN

SAS-VPN は，VPN クライアントがパケットを送信する度に，SAS-L2 により鍵更新を行い，データの暗号化には AES-128-GCM を採用することで通信の秘匿を実現する．SAS-VPN の概要を図 1 に示す．

4　評価

SAS-2 および SAS-L2 認証方式による鍵更新を，送信パケット毎に適用して暗号通信を行う VPN 2 方式と，VPN を用いない方式の合わせて 3 つの通信環境について速度評価を行った．結果を図 2 に示す．

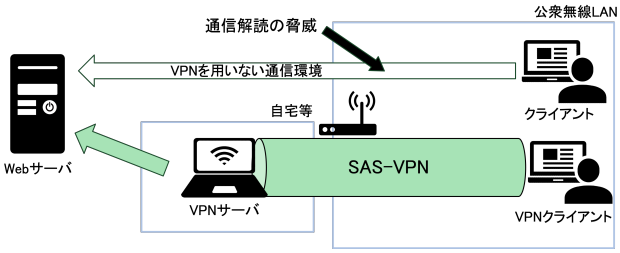

図 1　SAS-VPN 通信の概要

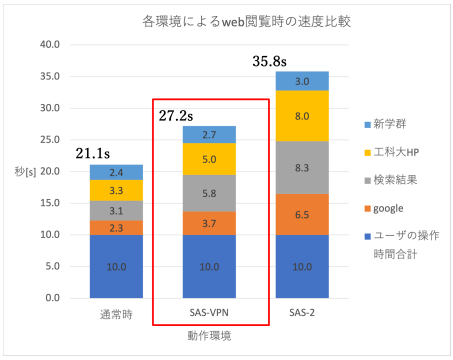

図 2　各通信環境による Web サイト閲覧時の速度比較

SAS-L2 を用いる提案方式では，SAS-2 を用いた場合に比較して，約 24 %の処理時間削減を実現した．また，鍵更新の実回数は約 4.4 パケット毎に 1 回であったため，既存方式よりもセキュリティの向上を実現できた．

5　むすび

本論文では，送信パケット毎に異なる鍵で暗号通信を行う SAS-VPN を提案した．SAS-VPN は，SAS-2 を用いた従来方式に比較して，約 24 %の処理時間削減を実現した．

今回は，開発プログラム言語として Python を利用して機能確認を行ったが，実用化に向け，C 言語等で実装を行うことでより高速化を図る必要がある．

参考文献

[1] 清水 明宏，“認証システム、認証装置、認証方法、およびプログラム，”特許 7119071 号，August.2022.

[2] ITmedia，“IPN によるウルトラセキュリティ～無線 LAN におけるセキュリティの不安を完全に解決，”https://atmarkit.itmedia.co.jp/ad/tss/ipn0609/ipn.html，October.2006.