SAS-2 を用いた複数端末認証可能なセキュア公衆無線 LAN 通信の研究

1205088　横山 拓磨　【 セキュリティシステム研究室 】

Research on Secure Public Wireless LAN Communication with Multiple devices Authentication Using SAS-2

1205088　YOKOYAMA, Takuma　【 Security Systems Lab. 】

1　はじめに

近年，政府による ICT 関係重点政策の一つとして公衆無線 LAN サービス環境 (以下，Wi-Fi サービス) の整備が推進され，多くの場所で Wi-Fi サービスが提供されている．しかし，これらの Wi-Fi サービスには，利用者の利便性から通信の暗号化が行われないものや，共通のパスワードを使用し接続するものがほとんどである．不特定多数が利用するため，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．また，悪意のある第三者が通信の盗聴目的で，正規の Wi-Fi サービスと同一の SSID、暗号化キーを用いた偽装アクセスポイントの危険性も存在する．

この課題に既存研究として，SAS-2(Simple And Secure password authen-tication protocol, ver.2) を用いて VPN(Virtual Private Net-work) を構築する SAS-VPN がある [1]．しかし，認証情報を生成するための乱数がユーザの端末内にあり，他の端末で認証情報の生成することができず，認証を行うことができない．そのため，乱数をサーバに保存し，認証要求時に乱数をサーバが送信し，認証情報を生成する方式を用いることで複数端末での認証が可能となる [2]．しかし，パスワードリスト攻撃などで ID, パスワードが漏洩していた場合，第三者が不正に接続を行うことが可能となる．また，SAS-VPN では，他の安全に通信を行う方式である HTTPS(Hypertext Transfer Protocol Secure) 通信や，L2TP/IPSec や OpenVPN 等の VPN 方式との比較が不十分である

本研究では，複数端末認証可能な SAS-2 を用いた VPN 方式を提案し，HTTPS 通信，VPN 方式との比較評価を行う．

2　既存方式

図 1 は SAS-VPN の概要である．図 2 は SAS-2 の生成情報である．以下で SAS-VPN の問題点と複数認証可能にした SAS-2 方式の問題点を示す．

2.1　SAS-VPN

SAS-VPN では，SAS-2 を用いて相互認証を行い，認証情報を元に VPN で使用される共通鍵の生成を行う．SAS-VPN では，他の VPN システムや HTTPS 通信との比較評価を行っていない．

2.2　複数端末認証

複数端末認証を可能にした SAS-2 認証方式では，ID とパスワード，乱数を用いて初期認証情報を生成し，サーバへ認証情報と共に乱数を保存する．認証が行われた際には，次回認証ように生成された乱数を送信し，認証情報と共に更新を行う．接続端末の追加等で，他の端末から認証が必要になった場合，サーバから乱数を取得し，同じ ID, パスワードを用いて認証情報を生成する．しかし，パスワードリスト攻撃などで ID, パスワードが漏洩していた場合，第三者が認証可能である．

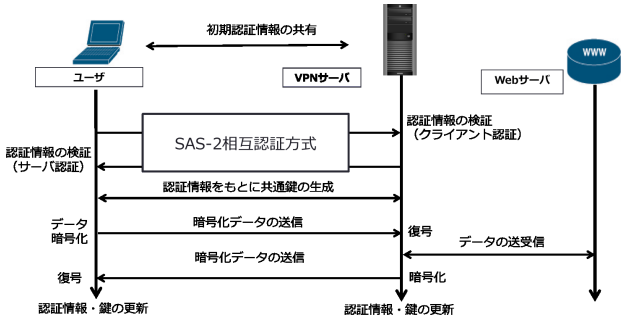

図 1　SAS-VPN 概要

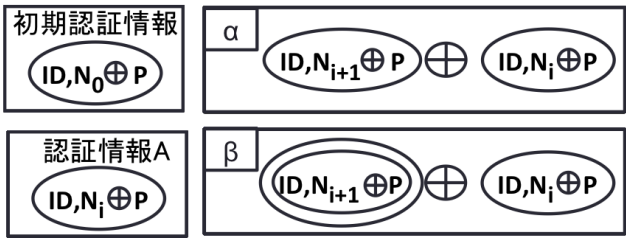

図 2　SAS-2 生成情報

3　提案方式

本研究では，ID，パスワードの漏洩に対応した，複数端末認証を可能とした SAS-2 を用いた VPN 通信の提案を行う．提案方式では，認証に必要となる情報をサーバへ登録する初期登録フェーズ，認証を行う認証フェーズ，端末の登録を行う端末登録フェーズの 3 つの

フェーズがある．表 1 はユーザとサーバで保持する情報である．

表 1　保持情報

ユーザのみ	サーバのみ	共通
パスワード P	乱数情報 N_i 認証情報 A	ユーザ識別子 ID 端末識別子 TID 共有情報 SI

3.1　初期登録フェーズ

ユーザは認証情報を生成するため ID と P を入力する．次に TID と SI,N_0 を生成し，ID と P，N_0 を用いて初期認証情報を生成する．その後，安全な経路を用いて，ID，TID, SI, N_0，初期認証情報を共有し，サーバへ保存する．

3.2　認証フェーズ

ユーザはサーバに対し，ID と TID を送信する．受信したサーバは N_i と SI を排他的論理和し，Nex_i を生成し，ユーザへ送信する．ユーザは受信した Nex_i と SI を排他的論理和し，N_i を取り出し，認証情報 A を生成する．また，新たに乱数 N_{i+1} を生成し，次回認証情報 C の生成を行う．次に認証情報 A,C から認証に必要な α と β の生成と N_{i+1} と SI を排他的論理和を掛け Nex_{i+1} を生成し，α，β，Nex_{i+1} をサーバへ送信する．受信したサーバは，α，β と保持している認証情報を用いて正当性の検証を行う．正当なユーザと判断した場合，サーバは Nex_{i+1} と SI を排他的論理和を掛け，N_{i+1} を取り出し，N_i を SI とし更新し，認証情報の更新と乱数の更新を行う．そして，認証情報を元に返信情報 γ を生成し，ユーザへ送信する．ユーザは，γ の正当の検証を行い，正規のサーバからの返信であると判断した場合，N_i を SI とし更新する．

3.3　端末登録フェーズ

認証を行っている端末からサーバへ端末登録要求を行う．ユーザは他端末用 SI を生成し，認証済みの端末の SI と他端末用 SI を排他的論理和し，サーバへ送信する．受信した端末は認証済みの端末用の SI と受信情報を排他的論理和し，他端末用 SI を取得する．次に他端末用 TID を生成し，ユーザへ返信する．新しく登録する端末から認証を行う際に，ID と P，他端末用の SI,TID を入力し認証を行う．

4　評価

HTTP 通信と HTTPS 通信と提案方式のリクエスト・レスポンスの処理時間の検証，L2TP/IPSec と Open-VPN と提案方式における安全性と共通鍵の共有が行われるまでの通信回数，鍵共有手法の評価を行う．表**??**は，1MB，5MB，10MB のデータを HTTP 通信，HTTPS 通信，提案方式を用いて 1000 回取得した平均時間である．通信時間が提案方式と HTTP 通信では，通信速度が約 32%低下した．また HTTPS 通信と提案方式と比べ，通信速度が約 16%低下した．原因として VPN サーバ間での通信経路の増加がある． HTTPS 通信では，

表 2　各データサイズにおけるリクエスト・レスポンス処理時間 [s]

	1MB	5MB	10MB
HTTP 通信	0.5110	2.5611	5.1294
HTTPS 通信	0.6344	3.2110	6.3953
提案方式	0.7522	3.7889	7.5977

表 3　HTTPS 通信と提案方式の暗号化範囲

	暗号化範囲	適応範囲
HTTPS 通信	HTTP データ	対応ページのみ
提案方式	送信情報全て	全てのページ

HTTP データのみ暗号化され，IP ヘッダは暗号化されない．そのため，通信先のサーバを特定することが可能であり，利用者が利用しているサービスを特定することが可能である． L2TP/IPsec と Open-VPN, 提案方式

表 4　VPN 方式の比較

	安全性	通信回数	共通鍵交換方式
L2TP/IPsec	○	8 回	IKE
Open-VPN	○	6 回	SSL/TLS
提案方式	○	4 回	SAS-2

では，AES 等の安全な共通鍵を用いて VPN を構築するため安全性は高い．共通鍵の生成までに L2TP/IPSec では 8 回，Open-VPN では 6 回，提案方式では 4 回であった．また，L2TP/IPsec，Open-VPN では公開鍵を用いて鍵に用いる共有情報を送信する．提案方式では，SAS-2 の認証情報を用いて共通鍵の生成を行うため，暗号化等の処理が不要である．

5　まとめ

本研究では ID，パスワードの漏洩に対応した，複数端末認証を可能とした SAS-2 を用いた VPN 通信の提案と HTTPS 通信，他の VPN 通信との比較評価を行った．今後の展望として，認証情報の乱数を SI を用いて，排他的論理和を用いて通信を行っているが，安全に共有できる乱数と SI のデータサイズを検証する必要が有る．

参考文献

[1] 遠藤 俊，“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”，高知工科大学 情報学群，2016.

[2] 古田 千春，“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”，高知工科大学大学院 工学研究科 基盤工学専攻 情報システム工学コース，2015.