サーバと端末間に安全な通信路を必要としない多端末認証可能なパスワード管理システムの提案

1180344　高橋 錬　【 セキュリティシステム研究室 】

1　はじめに

利用するサービスの ID とパスワード (PW) を一元管理するシステムとして PW 管理システムがある．利用者は必要な ID と PW を 1 組だけ覚えておくだけで良い．しかし，利用する PW は通信路上で固定のまま流れるため，盗聴された場合になりすまされる可能性がある．故にシステム利用には安全な通信路を確保する必要があり，手間とコストが生じる．

また，スマートフォンなどの普及により一人当たりの所有する端末数は増加傾向にある．そのため利用者が異なる端末からでもサービスを利用できる必要がある．

2　ワンタイムパスワード認証方式

ワンタイムパスワード認証方式とは通信路を流れる認証情報が毎回変化する認証方式である．本稿で利用する SAS は排他的論理和と一方向性関数を用いたものであり導入コストが低く処理が高速である．

3　既存方式

既存方式では SAS-X を改良して認証時に安全な通信路を必要とせず，多端末認証に対応したパスワード管理システムが提案されている [1][2]．しかし，多端末化する際に共有する情報は安全な通信路を必要とするため，認証時に安全な通信路が必要であることと同じである．

4　提案方式

端末とサーバ間で安全な通信路を必要としない多端末認証を可能とする方式を提案する．本方式は新規ユーザ登録フェーズ，認証フェーズ，サービス情報登録フェーズ，新規端末登録フェーズから構成される．新規ユーザ登録フェーズではユーザが認証に必要なデータを登録する．端末間のデータのやり取りは Bluetooth4.1 などを用いて安全な通信路上で行う．認証フェーズでは SAS-X を用いて認証を行う．サービス情報登録フェーズではユーザは端末間で共有する秘密鍵を生成し，サービス情報を暗号化して登録する．利用する際には復号する．新規端末登録フェーズのシーケンス図 1 を以下に示す．

- K , L_i , N_i , N_{i+1} , V : 乱数 , PW : パスワード
- $X()$, $H()$: 一方向性関数
- 端末 A の認証に必要な情報 : $A_i = X(P \oplus N_i)$, $F_i = X(A_i)$, $A_{i+1} = X(P \oplus N_{i+1})$, $F_{i+1} = X(A_{i+1})$, $\alpha_A = F_{i+1} \oplus F_i$, $\beta_A = F_{i+1} \oplus A_i$
- 端末 B の認証に必要な情報 : $B_i = B$ の認証情報, $D_i = X(B_i)$, $B_{i+1} = X(P \oplus L_i)$, $D_{i+1} = X(B_{i+1})$, $\alpha_B = D_{i+1} \oplus D_i$, $\beta_B = D_{i+1} \oplus B_i$

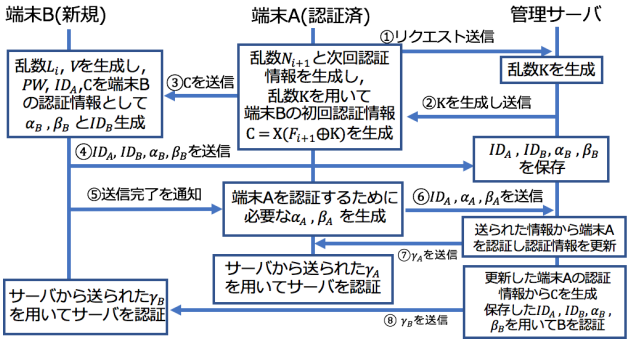

図 1　シーケンス図

5　評価

固定 PW を利用するシステムと既存方式，提案方式を比較した結果を表 1 に示す．評価項目として 1. サーバと端末間に安全な通信路が必要か，2. 通信路を流れる PW が安全か，3. 導入コスト，4. 鍵管理コストについて評価する．

表 1　評価結果

方式	1. 安全な通信路	2.PW の安全性	3. 導入コスト	4. 鍵管理コスト
固定 PW	必要	危険	高	低
既存方式	必要	安全	高	高
提案方式	不要	安全	低	高

6　まとめ

本研究では既存方式の問題点を指摘し，サーバと端末間に安全な通路を必要としない方式を提案した．また，固定 PW を利用するシステムと既存方式，提案方式を評価することで提案方式の優位性を示すことができた．

今後の課題として，実装を行い処理負荷などの検証を行う必要がある．

参考文献

[1] 辻 貴介，中原 知也，“ワンタイムパスワード認証方式の検討，” 電子情報通信学会信学技報 105(529)”，January, 2006.

[2] 渡邊 真悟，“SAS-X を用いた複数端末認証可能なパスワード管理システムの提案”，高知工科大学修士学位論文，March，2017.