パスワード管理システムの処理負荷軽減に関する研究

1250379　安江　匠馬　【 セキュリティシステム研究室 】

1　はじめに

昨今では，IoT 化の進行に伴い，Web サービスは増加，ユーザ個人が管理する必要がある ID とパスワードの組も増加している．ユーザが記憶する形で組を保管する方法には記憶できる限度があるうえ，ユーザが ID とパスワードの組を忘れてしまう事による情報の損失リスクも高い．

このようなリスクを軽減するために，現代ではパスワード管理システムが提案されている．パスワード管理システムもまた悪用されないために他 Web サービスと同様な認証を要求しているが，このサービスは一般的なサービスとは異なり高頻度の利用が想定されるため，情報処理コストがもたらす遅延がユーザに与える影響は大きい．

本研究では既存方法にて認証時に要求される情報処理コストを削減した手法を SAS-L で実現し，比較の元情報処理コストの面から当該認証方法を採用する有用性について実証する．

2　実装方式

2.1　DH(Diffie-Hellman) 法

DH(Diffie-Hellman) 法は事前に秘密鍵を共有する必要が無い，公開鍵暗号方式の暗号プロトコルである [1]．通信を行いたい 2 者がそれぞれ秘密鍵と公開鍵を用意し，相手には公開鍵のみを送信する．計算の元，受信した公開鍵と保持している秘密鍵から共有鍵を生成し，これが相手側で生成されたものと一致していれば，それを共有鍵として扱う．

2.2　SAS-L

SAS-L は多数のクライアントが接続されるサーバにおいて，大幅に処理負荷を削減することができるワンタイムパスワード認証方式である [2]．同時に鍵配送を行う事が可能であり，人相側での疑似乱数関数，一方向性変換関数の適用回数は双方 0 回，被認証側での疑似乱数関数の適用回数は 1 回，一方向性変換関数の適用回数は 2 回となる．

3　実験方法

プログラムはクライアント側，システム稼働用サーバ，パスワード保管用サーバに分けられ，全て開発言語には Python を用いる．また，すべてのプログラムは同一の PC で実行される．

DH 法と SAS-L それぞれで，クライアント側とサーバ側双方で処理完了にかかる時間を 10 回計測し，処理に要した時間の平均を 1 回ごとの利用にかかる時間として扱う．

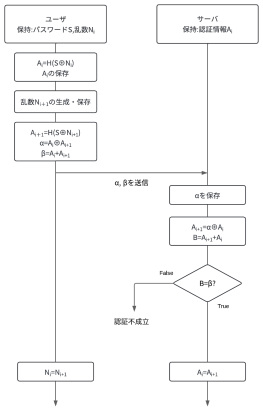

図 1　SAS-L の認証手順

4　評価

DH 法と SAS-L による処理時間の平均値を下表に示す．SAS-L での実装は DH 法での実装と比べ処理速度が速く，ユーザごとの平均処理時間が短い事が分かる．

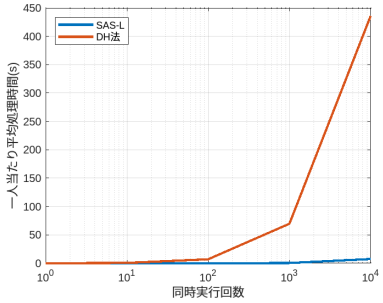

図 2　SAS-L と DH 法における一人当たり処理時間の比較

5　まとめ・考察

本研究では，DH 法と SAS-L を用いてパスワード管理システムを開発し，その結果の比較から SAS-L を用いたシステムの有用性を示した．より正確な評価を行うためには，認証情報の暗号化手法の検証や実際に多人数が利用する前提でのシステム設計が必要となり，それらが今後の課題となる．

参考文献

[1] E. Rescorla. “RFC2631: Diffie-Hellman Key Agreement Method”. In: *RTFM Inc.* (June 1999).

[2] 溝口 洸熙，清水 明宏. “IoT 環境に適したワンタイムパスワード認証方式”. In: *ISEC2024-79* vol.124.ISEC-255, pp.112-117 (2024/11/15).