5G－3

SAS暗号通信方式を利用したHTTPベースの安全、簡便な認証方式 *1

真島 大介*2　羽田 知良*3　田鍋 潤一郎*4　清水 明宏*5
NTTアドバンステクノロジ㈱*6　高知工科大学*7

1 はじめに

インターネット上の各種認証方式には、ネットワーク上のデータが暗号化されない、サーバ上のデータが暗号化されない、クライアント側に認証に必要な情報を記憶しておく必要がある等の問題がある。我々は、SAS（Simple And Secure）暗号通信方式をHTTPプロトコルに実装することにより、このような課題を解決した。

2 SAS暗号通信方式

SAS 暗号通信方式（http://www.ntt-at.co.jp/product/sas/sas_index.html）は、次回認証情報予告型のワンタイムパスワード方式であり、次の特長をもつ。

① 入力されたパスワードから毎回異なった認証情報を生成して安全に認証可能

② 次回の認証情報を予告することによって、極めて少ない計算量で認証を実現可能

（補足）SAS 方式を適用した「携帯端末用軽量認証システム」は、NetWorld+Interop 2001 Best of Show Award プロダクトアワード部門 ネットワーク・セキュリティ製品の部でグランプリを受賞した。

3 既存の認証方式の課題

我々は、TAO（通信・放送機構）から受託した研究開発「学校インターネットI」の一環として、小中学校へのインターネット導入に取り組んでいる。学校のように、複数の生徒や教師が1台のPCを共有するような環境では、簡便に各自のセキュリティを確保する必要があるが、既存の技術には次のような問題がある。

① ワンタイムパスワード：カードを用いて毎回パスワードを生成し、さらにそのパスワードをシステムに入力しなければならず、費用面、操作面から問題がある。

② SSL（Secure Sockets Layer）：学校環境にPKI（Public Key Infrastructure、公開鍵暗号基盤）を導入する必要があり、費用面の問題がある。

③ Basic認証、Digest認証：Basic認証ではネットワーク上のデータが暗号化されない。この問題に対処したDigest認証でもサーバにパスワードは平文のまま保存されるため、サーバアタックに弱い。

4 考案した方式

我々は、HTTPの通信環境にHTTPベースのSASProxyおよび認証サーバを挿入し、そこにSASの技術を適用することにより、簡便、安全かつ低コストな認証方式を考案した（図1）。

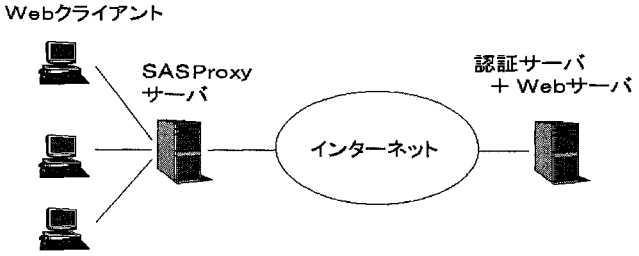

図1 考案した方式

*1 HTTP based secure and simple certification method using SAS

*2 Daisuke Mashima　*3 Tomoyoshi Hada　*4 Junichiro Tanabe　*5 Akihiro Shimizu
*6 NTT Advanced Technology Corporation　*7 Kochi University of Technology

5 処理方式

考案した方式の暗号の処理手順は次の通りである(図2)。

① Web クライアント(ブラウザ)からのリクエストを SASProxy サーバが受け取る。

② SASProxy サーバは認証サーバと HTTP を用いた通信を行い、ユーザの認証回数、セッション ID などの取得、および、それらの情報とユーザのパスワードなどを用いて暗号化鍵の計算を行う。

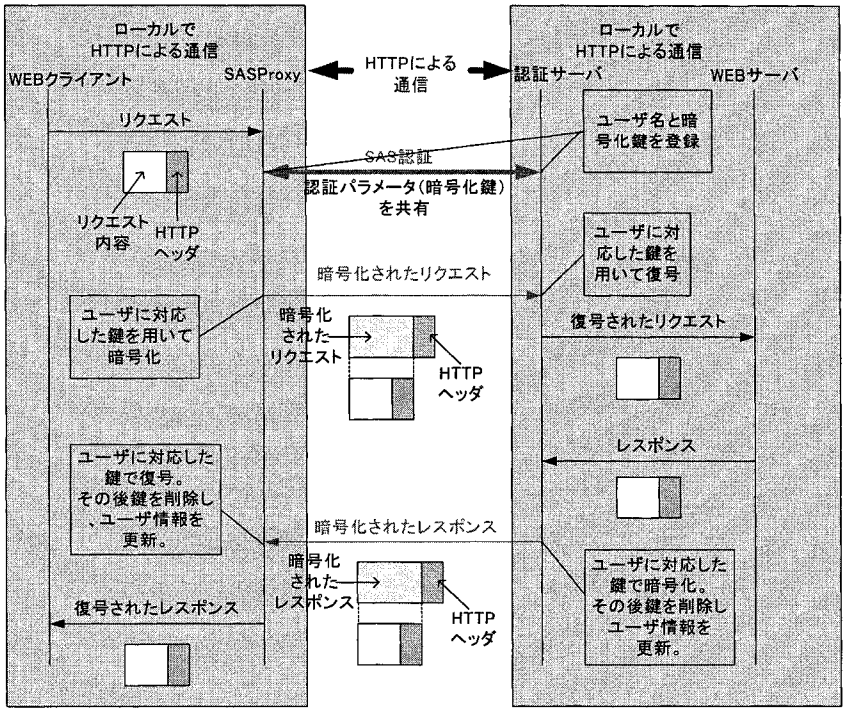

図2 暗号処理方式

③ SASProxy サーバは②で計算した暗号化鍵を用いて Web クライアントから受け取ったリクエストを暗号化し、認証サーバに送信する。

④ 認証サーバは登録されているユーザ情報から復号のための鍵を計算し、受信したリクエストデータを復号する。ここで同時に正しく復号できたかどうかの検証を行う。パスワードが不正である場合は正しく復号できないため、この時点でエラー(認証失敗)となる。

⑤ 正常にリクエストデータを復号できた場合、認証サーバは復号したリクエストデータに基づいて処理を行い、その結果を復号の際に用いた鍵で暗号化して、レスポンスとして SASProxy サーバに送信する。

⑥ SASProxy サーバは、受け取ったレスポンスデータを②で計算した鍵を用いて復号する。この際、レスポンスデータが正しく復号されたかどうかの検証を行う。正しく復号されなかった場合は、ネットワーク上でデータの改ざんが行われた可能性が考えられるため、処理をやり直す。

⑦ 正常にレスポンスデータを復号できた場合、SASProxy サーバは、復号されたレスポンスデータを Web クライアントに対して送信する。

⑧ SASProxy サーバ、認証サーバとも、処理終了時には、鍵およびユーザ情報を削除する。

6 おわりに

現在、今回実現したシステムを性能評価中であるが、非常に短い時間で処理できることが確認できている。今回考案した方式は、管理(入力)すべきパスワードが 1 個(回)であるため、小中学校ならば、フロッピーディスクに保存して各自に持たせることで、非常に安価にシステムを実現できる。さらに、パスワードをキーボードから入力する必要もなくなるというメリットもある。今後は、実際に学校の環境に適用して、機能および性能の評価を行う予定である。