セキュアＷｅｂアクセスシステムにおけるユーザ認証方式

１Ｔ－１

藤井 誠司、小林 信博、北山 泰英、原田 雅史、田中 学、亀多 徹
三菱電機(株)

1. はじめに

近年、インターネット／イントラネット／エクストラネットをはじめとする情報通信ネットワーク上で、WWWサーバを利用した情報共有システムが普及しつつあり、WWWサーバ上に重要な情報を置いて安全に共有するための仕組みが求められている。現在でも、ＳＳＬを使用したＨＴＴＰＳのようなプロトコルによってブラウザとサーバとの間で、ユーザ認証およびWWWページの暗号化を実現したシステムが多く存在する。しかし、すでにセキュリティ戦略を立て、運用を実施している既存のシステムへ新しいプロトコルを導入することは、セキュリティ戦略を見直すことを要求されるために、導入が難しい場合が存在する。我々は、WWWページのアクセスプロトコルであるＨＴＴＰ[1]上に、X.509 に準拠した証明証によるユーザ認証、WWWページの暗号化およびWWWページのアクセス制御の機能を持つセキュアＷｅｂアクセスシステムを開発した。このシステムでは、既存のサイト上のセキュリティ戦略を変更せず、WWWサーバによる安全性の高い情報共有システムを容易に実現できることを特徴とする。本稿では、このセキュアＷｅｂアクセスシステムにおけるユーザ認証方式の実現方式について報告する。

User Authentication on Secure Web access system
Seiji Fujii, Nobuhiro Kobayashi, Yasuhide Kitayama, Masafumi Harada, Manabu Tanaka, Toru Kameta, Mitsubishi Electric Corporation

2. セキュアＷｅｂアクセスシステムの概要

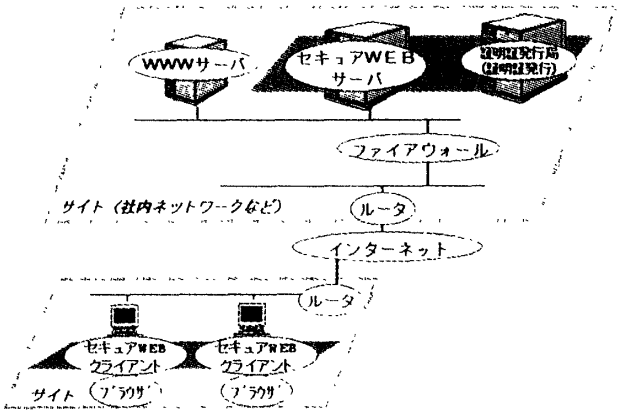

図１：セキュアＷｅｂアクセスシステムの構成

図１に開発中であるセキュアＷｅｂアクセスシステムの構成を示す。本システムは、セキュアＷｅｂクライアントとセキュアＷｅｂサーバから構成される。この他に、X.509 に準拠した証明証を発行する証明証発行局や社内ネットワークなどのサイトの資源を保護するファイアウォールを必要とする。セキュアＷｅｂクライアントはクライアントＰＣ上にインストールされ、ブラウザの通信を横取りして処理を行う。また、セキュアＷｅｂサーバはWWWサーバ側のサイトのファイアウォールとWWWサーバの間に設置する。WWWサーバへアクセスするユーザは、証明証発行局から自分の証明証の発行を受け、その証明証をクライアントＰＣへ登録する。セキュアＷｅｂクライアントは以下の機能を持つ。

- ユーザ認証のためのデジタル署名付きアクセス要求の送信
- デジタル署名付きアクセス要求の共通鍵暗号方式(ＭＩＳＴＹ)による暗号化
- WWWページに添付されたデジタル署名の検証
- WWWページの共通鍵暗号方式（ＭＩＳＴＹ）

による復号

また、セキュアＷｅｂサーバは、以下の機能を持つ。

- ユーザ毎のWWWページのアクセス制御
- WWWページの共通鍵暗号方式(ＭＩＳＴＹ)による暗号化

3. セキュアＷｅｂアクセスシステムのユーザ認証方式

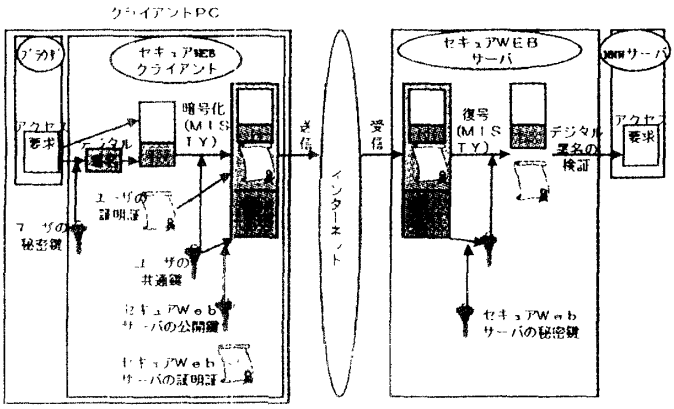

図２：ユーザ認証方式の手順

図２にユーザ認証方式の手順を図示する。セキュアＷｅｂアクセスは、セキュアＷｅｂサーバの証明証とユーザ個人の証明証を保持している。セキュアＷｅｂサーバでユーザ認証を行うために、初めてWWWサーバへアクセスする時に、ユーザのWWWページのアクセス要求とユーザの秘密鍵からデジタル署名を作成する。アクセス要求、そのデジタル署名とユーザの証明証をまとめて、共通鍵暗号方式（ＭＩＳＴＹ）で暗号化する。この暗号化で使用した共通鍵をセキュアＷｅｂサーバの証明証の公開鍵で暗号化する。暗号化されたアクセス要求と暗号化された共通鍵をまとめて新しいコンテントとして、アクセス要求を作成し、セキュアＷｅｂサーバへ送信する。セキュアＷｅｂサーバは受信したアクセス要求がセキュアＷｅｂクライアントからの要求であることをアクセス要求のコンテントタイプから判断する。アクセス要求から暗号化された共通鍵を取り出し、セキュアＷｅｂサーバの公開鍵暗号方式の秘密鍵で復号する。復号された共通鍵で暗号化されたアクセス要求を復号する。復号されたアクセス要求のデジタル署名とユーザの証明証でユーザ認証を行う。正しいユーザであると認証されれば、セキュアＷｅｂサーバのページのアクセス制御とアクセス要求に従って、WWWサーバへアクセス要求を送る。以上のようなユーザ認証方式を実施することにより、セキュリティの高いユーザ認証を既存のサイトに実現することができた。また、以下のような特徴を持つ。

- デジタル署名によるアクセス要求の改ざんの確認
- アクセス要求の暗号化による秘匿通信

4. おわりに

本稿では、セキュアＷｅｂアクセスシステムにおけるユーザ認証方式の実現方式について報告した。ＨＴＴＰ上に、X.509 に準拠した証明証によるユーザ認証、WWWページの暗号化およびWWWページのアクセス制御の機能を実現することによって既存のサイト上で安全性の高い情報共有システムを実現している。課題として、セキュアＷｅｂアクセスクライアントをユーザに意識させないＷｅｂアクセス方式の検討、セキュアＷｅｂアクセスクライアントをインストールしないユーザのＷｅｂページへのアクセス制御方式の検討を進めている。

5. 参考文献

[1]Berners-Lee, T., Fielding, R., and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0.", RFC 1945 MIT/LCS, UC Irvine, May 1996.

[2]太田英憲他,"汎用性を考慮した高速暗号ライブラリの開発と評価",SCIS96-10A,Jan.1996