# セキュアＷＥＢアクセスシステム

１Ｔ－４

小林 信博、藤井 誠司、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／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、難しい場合が存在する。特に、以下のような問題が指摘されている。

●現在稼働中のシステムへの影響

WWWページの変更が必要

WWWサーバの入替えが必要

ﾌｧｲｱｳｫｰﾙへ新しいﾌﾟﾛﾄｺﾙ用の設定が必要

●対象となるプラットフォームの限定

既にUNIX, Windows 95/NT, Macintoshなどのプラットフォーム上でWWWサーバが稼働中

●暗号強度の制限

輸出規制の関係で製品の暗号部分に対して制限・制約が加わっており安全性が低い

そこで我々は、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、暗号アルゴリズムＭＩＳＴＹ[2]による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。

本稿では、このセキュアＷＥＢアクセスシステムの実現方法について報告する。

## 2. セキュアＷＥＢアクセスシステムの概要

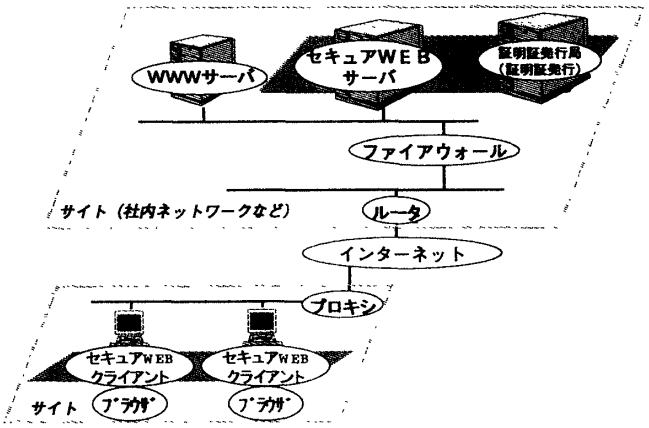


図１：セキュアＷＥＢアクセスシステムの構成

図１に今回開発したセキュア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。ブラウザは、クライアントＰＣ上のセキュアＷＥＢクライアントをプロキシとして指定し、代わりにセキュアＷＥＢクライアントがサイト外アクセスのプロキシを指定する。セキュアＷＥＢサーバは、クライアントからのリクエストをWWWサーバへとリレーし、WWWサーバからのレスポンスをクライアントへとリレーする。このリレーの際にデータの暗号化/復号、ユーザ認証、アクセス制御を行う。なお、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。

---

A Secure Web Access System

Nobuhiro Kobayashi, Seiji Fujii, Yasuhide Kitayama, Masafumi Harada, Manabu Tanaka, Toru Kameta, Mitsubishi Electric Corporation

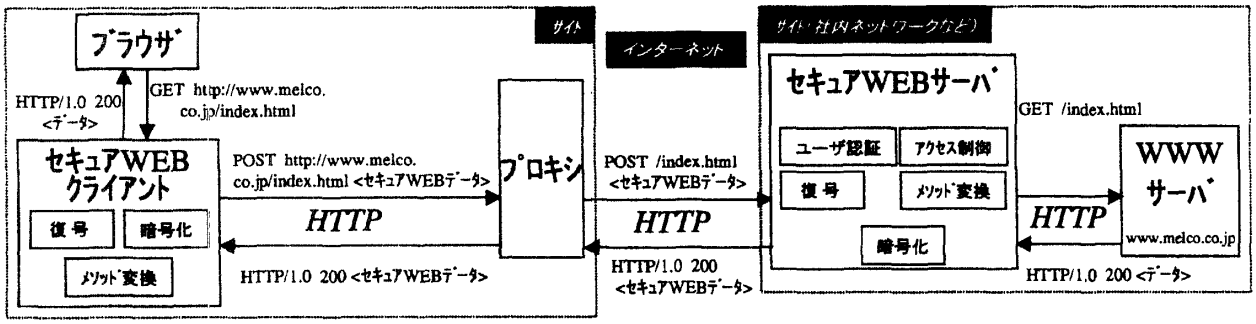


図２：動作メカニズム

## 3. セキュアＷＥＢアクセスシステムの動作

図２にセキュアＷＥＢアクセスシステムの動作メカニズムを示す。セキュアＷＥＢクライアントはブラウザと同一のクライアントＰＣ内にあり、アプリケーションゲートウェイプログラムとして動作する。まず、ブラウザの要求するリクエスト（ex. GETメソッド）が、CERN プロキシプロトコル準拠の形でセキュアＷＥＢクライアントへ送られる。この時URL にはドメイン名が付加されている。セキュアＷＥＢクライアントは、このリクエストにユーザのディジタル署名を付加し、共通鍵暗号方式(ＭＩＳＴＹ)により暗号化する。更に、この共通鍵をセキュアＷＥＢサーバの証明証の公開鍵で暗号化した上で、新たなリクエストを作成する。ただし、このリクエストをそのままプロキシへ送ると、プロキシがＵＲＬからドメイン名を取り除いたリクエストをセキュアＷＥＢサーバへ送る為、セキュアＷＥＢサーバが本来のアクセス先であるWWWサーバのドメイン名を入手できないという問題が発生する。そこで、今回はセキュアＷＥＢクライアントでＧＥＴメソッドをＰＯＳＴメソッドに変換した上で、ＰＯＳＴメソッドのもつデータ部分に元のＵＲＬと、ディジタル署名や暗号化された共通鍵を含む「セキュアＷＥＢデータ」を格納した。セキュアＷＥＢサーバでは、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判断すると、「セキュアＷＥＢデータ」から情報を取り出し、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。その後、ユーザ認証とWWWサーバのページアクセス制御を行った上で、目的とするWWWサーバへアクセス要求を送る。この際には、ＰＯＳＴメソッドをＧＥＴメソッドへ変換し、通常のリクエスト形式に戻す。WWWサーバから提供されたデータは、セキュアＷＥＢサーバにてユーザの証明証の公開鍵で暗号化され、「セキュアＷＥＢデータ」としてセキュアＷＥＢクライアントへと送られる。セキュアＷＥＢクライアントでは、ユーザの秘密鍵にて「セキュアＷＥＢデータ」を復号し、ブラウザへと渡す。以上の手順により、ブラウザはWWWサーバ上のデータを入手することが可能となっている。

## 4. おわりに

本稿では、セキュアＷＥＢアクセスシステムの実現方法について述べた。セキュアＷＥＢクライアントをプロキシとして実現し、更にセキュアＷＥＢクライアントおよびセキュアＷＥＢサーバにメソッドの変換手段を持たせることにより、ＨＴＴＰ上で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した。これにより、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。今後は、セキュアＷＥＢクライアントをユーザに意識させないＷＥＢアクセス方式や、WWWサーバ自体の盗難などに対応した安全な情報公開システム等について、検討を進める予定である。

## 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