三菱セキュアWebアクセス MistyGuard<TRUSTWEB>

2F－8　原田雅史、北山泰英、藤井誠司、小林信博、田中学、亀多徹
三菱電機株式会社

1. はじめに

近年、インターネット/イントラネットをはじめとする情報通信ネットワーク上で、Web サーバを利用した情報共有・発信システムが急速に普及しつつある。特に、イントラネットでの利用の広がりに伴い、Web システムのセキュリティ確保が重要な課題となってきている。本稿では、三菱セキュア Web アクセス MistyGuard<TRUSTWEB>(以下“TRUSTWEB”という)による、セキュアな Web システムを構築する上での課題の解決方法及び TRUSTWEB の実際のシステム適応事例について報告する。

2. TRUSTWEB の概要

セキュアな Web システムを構築する際には、次の課題がある。

・盗聴やなりすまし、データ改竄に対する防御
・コンテンツに対する柔軟なアクセス制御
・既存システムとの親和性の確保

図1に TRUSTWEB の構成を示す。本システムは、

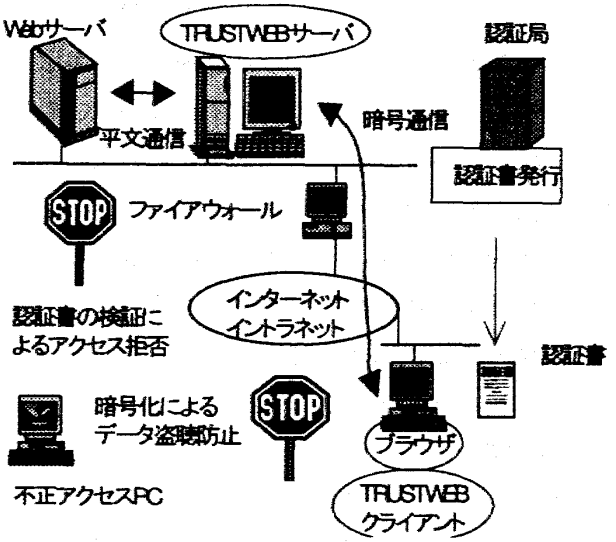

図1．TRUSTWEB の構成

TRUSTWEB サーバと TRUSTWEB クライアントから構成される。その他に認証書を発行する認証局やサイト内の資源を保護するファイアウォールが必要である。ブラウザと Web サーバ間を流れるデータは、弊社の共通鍵暗号アルゴリズム“MISTY”[2]により暗号化される。“MISTY”は、業界標準の“DES”と比較して暗号強度が強いことが証明されており、通信経路での盗聴に対して高い秘匿性を実現している。

本システムでは、ユーザ認証に ITU-T X.509 規格に準拠した電子認証書を用いる。電子認証書は、企業内の認証局や第三者認証機関で発行されたものが使用可能である。電子認証書は従来のユーザ名とパスワードの組合せによる単純な認証方法に比べ、なりすましが極めて困難であり、確実かつ安全にユーザ認証を行うことができる。

Web サーバ上のコンテンツのアクセス制御は、アクセス制御リストと呼ばれるツリー構造のデータベースを TRUSTWEB サーバ上で管理することで、ファイル又はディレクトリ単位で個人又はグループに対して設定できる。更に、GUI ベースの設定ツールを用意して管理者の操作手順の簡略化を図っている。

TRUSTWEB では、通信時のプロトコル処理をすべて HTTP[1]で実現している。このため SSL のように新たな設定をファイアウォールやルータに対して行う必要がない。

ブラウザから出された Web サーバへのリクエストはローカルプロキシとして設定された TRUSTWEB クライアントを経由して TRUSTWEB サーバへ送られる。TRUSTWEB サーバは受信したリクエストを解析して、該当する Web サーバへリクエストを転送するかどうかの判定を行う。更に、暗号通信、ユーザ認証及びコンテンツのアクセス制御は TRUSTWEB サーバと TRUSTWEB クライアント間で隠蔽されており、他のア

Mitsubishi Secure Web Access MistyGuard<TRUSTWEB>
Masafumi Harada, Yasuhide Kitayama, Seiji Fujii, Nobuhiro Kobayashi, Manabu Tanaka, Toru Kameta
Mitsubishi Electric Corporation

プリケーション(ブラウザや Web サーバ)から独立している。従って、既存システムに対して高い親和性を確保している。

Web サーバからのレスポンスは、TRUSTWEB サーバで暗号化され TRUSTWEB クライアントへ送られる。TRUSTWEB クライアントでは、レスポンスを復号してブラウザへ転送する。

TRUSTWEB は表１に示すような環境で動作する。

表１．TRUSTWEB の動作環境

サーバ	OS	Windows NT Server
	その他	Microsoft Proxy Server
クライアント	OS	Windows NT Windows 95
	ブラウザ	Internet Explorer Netscape Navigator

3. TRUSTWEB の適用事例

現在、弊社にて TRUSTWEB を用いてシステム提案、システム構築を行っている主な事例を紹介する。

3.1 エクストラネットシステム

既に、Web をベースとしたイントラネットシステムを構築している場合も含め、社内に TRUSTWEB サーバを設置し、クライアント PC に TRUSTWEB クライアントをインストールする。その結果、その PC を用いて社外（出張先や家庭）から社内のイントラネットシステムにセキュアなアクセスが可能になる。

更に、このような TRUSTWEB システムを関連会社間に展開することでセキュアなエクストラネットシステムを構築でき、関連会社間の業務に適応できる。

3.2 営業支援システム

管理会社に Web サーバと TRUSTWEB サーバを設置し、販売会社の PC に TRUSTWEB クライアントをインストールする。管理会社は、販売会社に対して次のような情報を提供する。

① 製品情報
② 製品の仕切り価格
③ 製品のサポート情報

①は、すべての販売会社に提供するが、②及び③は、販売会社の種類や販売会社との契約内容によって提供内容が異なる。

“MISTY” による暗号化通信、認証書を用いた強力なユーザ認証とコンテンツのアクセス制御を行うことで、第三者はもちろんのこと、販売会社間においても情報の秘匿性を保証する。

3.3 電子コミュニティシステム

地域の住民に対して新しいコミュニケーション手段や行政サービスを提供するシステムである。電子メール、電子掲示板、インターネット放送局といった新しいコミュニケーション手段を提供することで地域の活性化を図ると共に、住民票、印鑑証明、戸籍抄本の発行といった行政サービス（ワンストップサービス）をコミュニケーションセンターや家庭のパソコンから利用可能にする。

認証書と秘密鍵を格納した IC カードを住民に配布する。利用者は、IC カードをパソコンに挿入して、上記サービスを受ける。コミュニケーションセンターには、Web サーバと TRUSTWEB サーバを設置する。家庭又はコミュニケーションセンターのパソコンには、TRUSTWEB クライアントをインストールする。個人のプライバシーに関する情報は、TRUSTWEB によって確実なユーザ認証とデータの秘匿性を保証する。

4. おわりに

三菱セキュア Web アクセス MistyGuard<TRUSTWEB>について、その概要と適用事例について述べた。最近急増しているインターネット上での個人情報の漏洩事件や Web サーバのデータ改竄事件が示すようにネットワーク上でのセキュリティの確保は、益々重要度を増してきている。本システムは、これらの問題を解決するための適応性の高い製品である。今後は、管理者の負担をより軽減する諸機能の実装、利用者の利便性を高める IC カードへの対応などと共に弊社の他の関連製品との連携を深め、製品の適用範囲を拡大していく予定である。

5. 参考文献

[1]Berners-Lee,T.,Fielding,R.,and H.Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0.", RFC1945 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”、SCSI96-10A, Jan. 1996