コンピュータセキュリティ　1－2
（1998．5．29）

セキュアWWWアクセス制御システム

小林 信博†、藤井 誠司†、田中 学‡

†三菱電機株式会社 情報総合研究所
‡三菱電機株式会社 情報システム製作所

あらまし　今日、インターネットのみならず、イントラネット，エクストラネットにおいても、標準的なプロトコルとしての地位を確立している HTTP 上に、公開鍵暗号をベースとしたディジタル認証書によるユーザ認証、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WWWサーバに対して高い安全性を提供するセキュアWWWアクセス制御システムが可能となった。

Security enhancement and access control for WWW system

Nobuhiro Kobayashi†, Seiji Fujii†, Manabu Tanaka‡

†Information Technology R&D Center, Mitsubishi Electric Corporation

‡Information Systems Engineering Center, Mitsubishi Electric Corporation

Abstract　HTTP has been in use by the World Wide Web since 1990 and its use has increased steadily over the years, mainly because it has proven useful as a generic middleware protocol. Then, we developed secure WWW access control system at the HTTP layer. This system has these features: user authentication by the digital certificate, data encryption of WWW pages and access control to WWW pages. As a result, it provides high safety to an existing WWW system.

1. はじめに

近年、電子化された情報の共有化を低コスト，短期間で実現するために、インターネット／イントラネット／エクストラネットシステムを導入する企業，ユーザの数が大幅に増加している。インターネットの代名詞と言われるWWWシステムも、その利便性から様々なサービスやシステムのベースとして利用されている。しかし、インターネットはオープンな環境，技術であるが故に、「盗聴」「他者へのなりすまし」「改ざん」「否認」等の問題がある。そこで今回、我々はこのような問題を解決するものとして、「セキュア WWW アクセス制御システム」を開発した。本システムの目的は、以下にあげた三点である。

① インターネット／イントラネット／エクストラネット上で、安全な情報通信システムを構築する。
② イントラネットからエクストラネットへと移行する場合に、既に稼動中の WWW システムに与える影響を留めた上で、セキュリティの強化を実現する。
③ WWW システム上のデータを特定の利用者に対してのみ配信する為に、アクセスコントロール機能を付加する。

なお、これらは暗号技術とディジタル認証書技術

を使用して実現する。ディジタル認証書は、PKI(Public Key Infrastructure)であるCA(Certification Authority)により提供される。このCAとしては、当社製 MistyGuard<CERTMANAGER>やJapanNet 等を利用可能とし、他の PKI 利用システムとの連携も強める。

2. 従来の問題点

従来は、WWW システムのセキュリティを確保する為に、SSL (HTTPS) や S-HTTP 等のプロトコルを使用した製品を利用する場合が多かった。しかし、ここには以下の様な問題がある。

① 現在稼働中のシステムへの影響

既にセキュリティ戦略を立て、実際に運用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、セキュリティ戦略の見直しが要求されるために難しい場合が存在する。また、SSL 及び S-HTTP を導入する際の一番の問題は、膨大な数にのぼる既存コンテンツの変更が、非常に煩雑な作業となることである。更に、WWW サーバやプロキシ、ファイアウォール等の既存ネットワーク機器の入替えや変更は、サービス停止や設定不備によるセキュリティホールを招く危険性がある。

② 対象となるプラットフォームの限定

既に各組織及び企業内では、UNIX、Windows 95/NT、Macintoshなどの各プラットフォーム上で、WWWサーバが情報システムとして稼働中である。従って、OSやWWWサーバまでも含めると、多種多様なバージョンの組み合わせへと対応しなければならない。今日の主流であるオープンなシステムにおいては、インターオペラビリティが重視される事もあり、既存環境へのアドオンまたは一部追加、設定変更により実現することが望ましい。

③ 暗号強度の制限

外国製品を日本国内で使用する場合、暗号技術に関する輸出規制の関係で、製品の安全性が低い。例えば、Netscape社製のブラウザに実装されているSSLは、米国の輸出制限により内部で暗号に使用する鍵サイズが40bitに固定されている。しかし、既に40bit程度の鍵サイズでは暗号が解読可能であるとの発表が多数なされており、暗号学的には安全でないとの認識が一般化している。

3. セキュアWWWアクセス制御システム

前章であげた問題点を解決する為に、今回はWWWページのアクセスプロトコルであるHTTP上に、X.509に準拠した認証書によるユーザ認証、暗号アルゴリズムMISTY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機能を持つセキュアWWWアクセス制御システムを開発した。これを図1に示す。

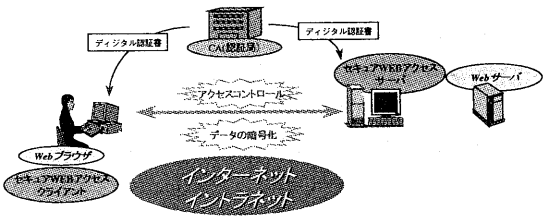

図1 セキュアWWWアクセス制御システム

本システムは、セキュアWEBアクセスクライアントとセキュアWEBアクセスサーバから構成される。クライアントPC上のWebブラウザは、同じくクライアントPC上で動作するセキュアWEBアクセス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アクセス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アクセスサーバは、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。データの暗号化/復号、ユーザ認証、アクセス制御は、セキュアWEBアクセスクライアントとセキュアWEBアクセスサーバ間で行われる。

なお、この他にX.509に準拠した認証書を発行する認証書発行局や社内ネットワークなどのサイトを保護するファイアウォールなども利用できる。

4. 機能・特徴

4.1. 既存システムとの親和性

既存システムを考慮し、WWW サーバへのアクセス制御、並びにインターネット上の WWW コンテンツの暗号化は、セキュア WWW アクセス制御システムが行う。これにより、 WWW サーバに依存することなく、また WWW サーバ上のコンテンツを変更

することなく、セキュリティを向上することが可能となっている。また、CGI 等を使った動的なコンテンツ情報を利用するシステムにも適用可能である。SSL の場合にはファイアウォールへ新たなポート番号の設定が必要となるが、セキュア WWW アクセス制御システムではその必要も無く、既存システムとの親和性が高い。

4.2. データの暗号化

インターネット上のコンテンツの暗号化は、当社の開発した共通鍵暗号アルゴリズム MISTY により実現される。これは、米国商用暗号 DES を超える暗号強度をもち、更に高速な暗号処理が実行可能なアルゴリズムである。また、暗号に用いる鍵長には 128bit を使用しており、米国政府による暗号輸出規制を受けた 40bit のシステムよりも、インターネット上の盗聴を防止できる。従って、安全性とスピードが要求される用途にも安心して使用可能である。

4.3. アクセス制御

WWW サーバへのアクセス制御は、ディジタル認証書を利用して行う。これは従来のユーザ ID とパスワードによる制御と異なり、秘密情報がインターネット上を流れない為、セキュリティが向上する。また、ディジタル認証書は、第三者機関である CA により身元が確認されたうえで発行される為、信頼性の高いアクセス制御が実現できる。

更に、個人単位及びグループ単位でのアクセス制御が可能である。アクセス制御の対象には、コンテンツ（ページ）及びディレクトリ単位で指定可能となっている。従って、イントラネットでの役職に応じたアクセス制御や、会員制情報システム等の構築にも対応できる。なお、ここでは公開鍵暗号アルゴリズムである RSA(鍵長 1024bit)とハッシュアルゴリズムである SHA-1 によるディジタル署名を使用する。

4.4. 集中的サーバ管理

セキュア WEB アクセスサーバは、複数の WWW サーバに対して暗号化およびアクセス制御機能を提供する。従って、複数サーバの設定を一箇所で行うことが可能であり、セキュリティ情報の一元管理が実現できる。また、アクセス制御情報やユーザ情報なども、管理ツールを利用して簡単に設定することが可能であり、実運用時における管理者の負荷を低減している。

5. 実現方式

5.1. ローカルプロキシ

セキュア WEB アクセスクライアントは、ローカルプロキシにより実現される。他の実現方式としては、ブラウザ自体に機能を追加するプラグインやヘルパーアプリケーション、通信プロトコルスタックの置き換えやパケットレベルでの通信データフックなどが考えられるが、この方式のメリットとしては、以下の 4 点が挙げられる。

① 既存のブラウザが利用可能であること
② ブラウザの将来的なバージョンアップに対応可能であること
③ ブラウザの種類に依存しないこと
④ 他のアプリケーションに影響がないこと

一般的なプロキシは、イントラネットとインターネットの接続ポイントに設置される。これは、イントラネット内部に存在するクライアントを、外部の攻撃から保護する目的で利用される。クライアント上のブラウザから送信されたリクエストは、一旦プロキシに送られた後で、本来の送り先である WWW サーバへと転送されている。このように、プロキシは HTTP プロトコルの中継を行うので、リクエストおよびレスポンスの書き換えを行うことが可能である。そこで、このプロキシをクライアントローカルに置くことで、通信データの暗号化・復号、並びにユーザのディジタル署名検証処理を行うこととする。処理手順を以下に示す。

1. ブラウザから送られたリクエストは、ローカルプロキシであるセキュア WEB アクセスクライアントへと送られる。
2. セキュア WEB アクセスクライアントは、受け取ったリクエストにユーザのディジタル署名を付加した後、送信先となるセキュア WEB アクセスサーバ向けの親展（暗号化）を行う。
3. 更に、このディジタル署名と暗号化のついた新しいリクエストを、既に設置されているプロ

キシへと送る。

4. プロキシからセキュア WEB アクセスサーバに転送されたリクエストは、セキュア WEB アクセスサーバにて復号され、ディジタル署名の検証ならびにリクエスト先のアクセス制御を受ける。
5. アクセスが許可されている場合は、本来の送り先である WWW サーバへリクエストを送信する。
6. WWW サーバから送り返されたレスポンスは、セキュア WEB アクセスサーバで暗号化され、再びプロキシを経由してセキュア WEB アクセスクライアントへと送り返される。
7. セキュア WEB アクセスクライアントは、暗号化されていたレスポンスを復号し、最終的なデータをブラウザへと届ける。

なお、セキュア WEB アクセスサーバにて本来の WWW サーバを特定する為の URL は、セキュア WEB アクセスクライアントが作成する新しい HTTP データの中に記述する。

5.2. ユーザ認証・サーバ認証

セキュア WWW アクセス制御システムにおける認証は、ユーザ認証とサーバ認証の２つがある。ユーザ認証は、リクエストを送信してきたセキュア WEB アクセスクライアントのデータに付加されているディジタル署名を利用して行われる。また、サーバ認証は、クライアントから送られてくる暗号化済データを利用して行われる。

図２に本システムの認証のフローを示す。

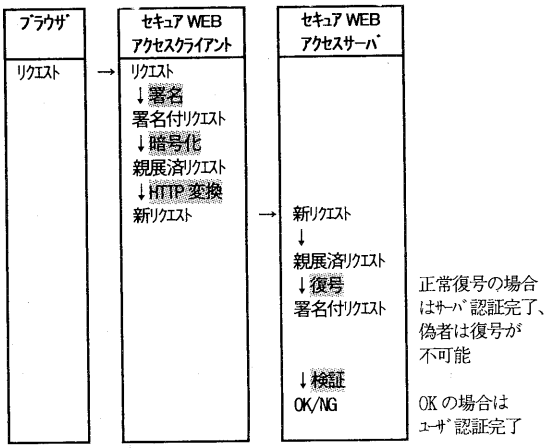

図 2 ユーザ認証・サーバ認証フロー

認証手順について説明すると、

1. セキュア WEB アクセスクライアントが、ブラウザから送られたリクエストに対して、ユーザのプライベートキーを利用して公開鍵暗号方式によるディジタル署名を付加する。
2. このディジタル署名付リクエストに対して、セキュア WEB アクセスサーバ宛の親展（暗号化）を、サーバ認証書中の鍵を用いて施す。
3. 署名＋暗号化された親展済リクエストから新しい HTTP リクエストを作成し、送信する。
4. セキュア WEB アクセスサーバは、まず受け取った HTTP リクエストを復号する。ここでは、クライアントにより親展（暗号化）に用いられた認証書に対応するプライベートキーを使用しなければならない。すなわち、この HTTP リクエストが正常に復号できるということは、プライベートキーを知っている正当なサーバであると確認できる。これにより、サーバ認証が実現されている。
5. 更に、復号された署名付リクエストを、クライアントの認証書により検証することで、正当なユーザであることが検証される。これがユーザ認証である。

5.3. アクセスコントロール

セキュア WWW アクセス制御システムにおけるアクセスコントロール（以後 AC）は、WWW サーバ上のファイルおよびディレクトリ単位で行われる。また、ユーザを複数含むグループを設定可能であり、アクセスコントロールリスト（以後 ACL）設定時の利便性が向上されている。

セキュア WEB アクセスサーバには、ユーザの認証書に含まれる issuer、serial no. とユーザ ID を予め登録しておく。ファイルおよびディレクトリに対する AC は、このユーザ ID をキーにして行う。実際の処理としては、まずセキュア WEB アクセスサーバで、クライアントから送られてきたディジタル署名付リクエストの検証を行う。この結果が正常な場合には、ディジタル署名に含まれる認証書の issuer、serial no. を取り出し、AC のキーとなるユーザ ID を検索する。そして、リク

エストの対象であるファイルまたはディレクトリの ACL を参照することによって、内容を見る権利があるかどうかの判別を行う。なお、ACL の設定ならびにユーザ管理は専用の設定ツールを利用することで、管理負荷を軽減することができる。

5.4. 複数認証書対応

セキュア WWW アクセス制御システムでは、ユーザが複数の認証書を持つことに対応している。従って、異なる認証書系列に属するセキュア WWW アクセス制御システムを、並行して利用することが可能である。これを実現する為に、セキュア WEB アクセスクライアントでは、アクセス情報リスト（以後 AIL）を利用する。AIL には、セキュア WEB アクセスサーバとその管理下におかれる WWW サーバのドメイン名、更にセキュア WEB アクセスサーバへ登録したユーザの認証書情報（issuer、serial no.）が記述されている。セキュア WEB アクセスクライアントが、ブラウザから受け取ったリクエストに署名する際には、この AIL を参照し、リクエスト先の WWW サーバに応じた認証書を選択する。

例えば社内情報にアクセスする場合には、企業から発行された認証書によるアクセスコントロールサービスを利用し、関係会社の取引価格情報にアクセスする場合には、その関係会社から発行された別の認証書によるアクセスコントロールを受けることが可能である。認証書は自動的に選択される為、ユーザが意識する必要はない。

5.5. 通信プロトコル

本システムにおける通信プロトコルは、大きく２つに分けられる。一つは、セッション開始時に行われる「初期ネゴシエーション・フェーズ」であり、もう一つはその後にデータの交換を行う「暗号化通信・フェーズ」である。

5.5.1. 初期ネゴシエーション・フェーズ

図３に示した初期ネゴシエーション・フェーズにおける目的は、クライアント・サーバ間の認証と、暗号化通信・フェーズで利用するセッション鍵の交換である。サーバによるクライントの認証は、認証書を用いたディジタル署名によって行う。クライアントから送るリクエストには、クライアントの署名を付加し、その署名付きデータを受け取ったサーバは署名の検証を行う。また、サーバの認証は、クライアントからサーバ向けの親展（暗号化）を行うことによって実現する。クライアントが送付するデータにサーバ宛の親展を施すことにより、指定したサーバのみが親展を解除可能である。すなわち、認証書に対応したプライベートキーを保持する正当なサーバだけが、その内容を解読可能ということになる。

また、「暗号化通信・フェーズ」にて利用するセッション鍵は、クライアントにて生成され、リクエストと共にサーバへと送付される。サーバは、親展解除，署名検証を行った上でクライアントから指定されたセッション鍵を保存し、後の暗号化通信時に利用する。

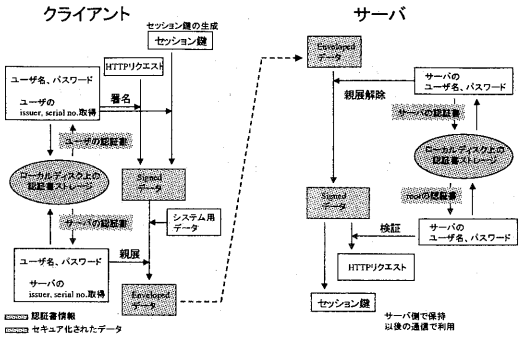

図 3　初期ネゴシエーション・フェーズ

5.5.2. 暗号化通信・フェーズ

初期ネゴシエーション・フェーズ完了後に行われる暗号化通信フェーズを、図 4に示す。

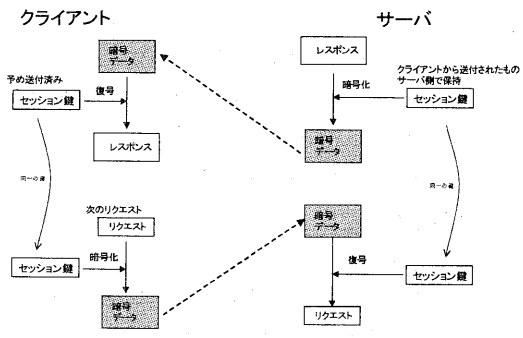

図 4　暗号化通信・フェーズ

ここでは、初期ネゴシエーション・フェーズにて

共有されたセッション鍵を用いることで、クライアント～サーバ間で交換されるリクエストおよびレスポンスの暗号化を行う。これにより、通信データの保護がなされている。

なお、暗号化・復号のアルゴリズムとしては、当社の開発したMISTYを採用しており、秘密鍵暗号方式のメリットである高速な暗号処理が可能であるとともに、高い安全性が保証されている。

6. 考察

暗号通信処理がWWWシステムへ及ぼす影響について、表1の環境で測定を実施した。

表1 性能測定環境

セキュアWEB アクセスサーバ	Mitsubishi FT2200 CPU:Pentium 200MHz OS:Windows NT4.0
セキュアWEB アクセスクライアント	DEC HiNote Ultra II CPU:Pentium 133MHz OS:Windows95

ファイルサイズ60,592[BYTE]の暗号通信処理を行った場合、42.454[SEC]の時間を要した。その際、セキュアWEBアクセスサーバにおいて実行された暗号通信処理の処理時間のうち分けを図4に示す。

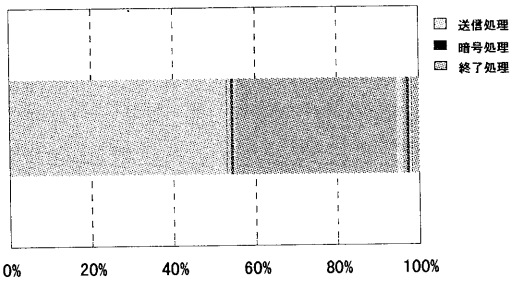

図5 暗号通信処理のうち分け

このうち、暗号処理の消費した処理時間0.360[SEC]である。これは、全体の処理時間のわずか0．8％にしか過ぎず、ほとんど無視できる範囲であった。

7. まとめ

本稿では、セキュアWWWアクセス制御システムの実現方法について述べた。まず、セキュアWEBアクセスクライアントをローカルプロキシとして実現することで、既存システムとの親和性を確保した。また、セキュアWEBアクセスクライアントおよびセキュアWEBアクセスサーバにより、HTTP上でX.509に準拠した認証書によるユーザ認証、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。更に、個人単位およびグループ単位でのユーザ管理、コンテンツおよびディレクトリ単位でのアクセス対象管理を実現し、柔軟なアクセス制御機能を提供している。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することが可能となっている。暗号通信処理における暗号処理時間に関しても、全体の処理時間の中で、ほとんど影響の無いことが分かった。

今後は、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。

参考文献

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

② Alan O. Freier, Philip Karlton, Paul C. Kocher, "The SSL Protocol Version 3.0", http://home.netscape.com/eng/ssl3/ssl-toc.html, Netscape Communications,Apr.1996

③ 集中特集「最新の暗号技術によるセキュリティの実現」, OPENDESIGN 1996年6月号, CQ出版社

④ Simson Garfinkel, Gene Spafford, 安藤進 訳「WEBセキュリティ＆コマース」, オライリー・ジャパン,1998.1.29（初版第1刷）

⑤ 斎藤 誠、「SSL及びSHTTPの仕様と実装」、http://WWW.jnetcom.jeida.or.jp/ec/papers/1-05/index.htm、（株）日立製作所、1997