CORBA Security Service と Web 連携の実装

6S－04

清水　麻由子*　　鍛　忠司**　　近藤　勝彦**　　赤尾杉　隆*
(株)日立製作所　*ソフトウェア事業部 **システム開発研究所

1. はじめに

OMG(Object Management Group)の提唱するCORBA(Common Object Request Broker Architecture)[1]などの分散オブジェクト技術によるサーバークライアント型のシステム構築の実用化が進むのと並行して、インタネット、エクストラネットにおいてはWWW(World Wide Web)によるシステムが大きなウェイトを占めている。

WWWシステムにおけるセキュリティはWWWサーバによるWeb認証、SSL(Secure Socket Layer)通信などの技術が事実上の標準として利用され、またCORBA技術においては共通サービスとしてSecurity Serviceが規定され、利用可能となっている。

図1のように、企業・組織の情報システムと外部のネットワーク接続にWWW技術を使用し、企業・組織内のシステムを分散オブジェクト技術で構築していた場合には、それぞれのセキュリティ保持、ユーザ管理を一本化して使用できることが望ましい。このようなシステム運用のために、

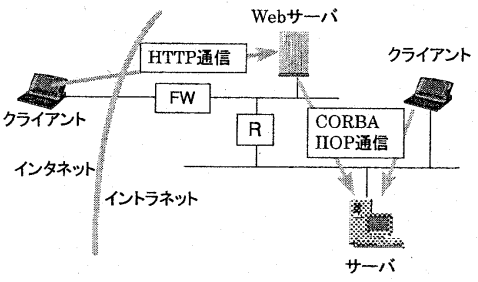

図1. WWWとCORBAを接続したシステム構築例

WWWサーバとCORBA Security Serviceのそれぞれのユーザ認証を、ユーザから一つのセキュリティシステムとして見える方式について述べる。

2. 現状のセキュリティ方式

2.1 WWWシステムのセキュリティ

現在使われているWWWサーバにおいては、アクセスするクライアントを認証する方法として、ユーザIDとパスワードを入力させる方法や、SSLを用いて電子証明書を使用させるものが多く利用されている。SSLを用いるとクライアント認証とサーバ認証が相互に行える他、通信データの暗号化も可能である。

またWWWサーバでは、一度認証したクライアントからの2度目以降のアクセスでは認証を省略するために、CGIプログラム等を利用しクライアントに対してCookieを発行して、2度目以降のアクセスではこのCookieを送付されればアクセスを認める方式を取っている。

2.2 CORBA Security Service のセキュリティ

CORBAのセキュリティ規格であるSecurity Serviceでは、ユーザ認証・識別、アクセス制御、暗号化、監査ログ等のセキュリティ機能を規定している。これらの機能はCORBAの提供するIIOP(Internet Inter-ORB Protocol)[2]通信の中で行われ、アプリケーションプログラムでは意識せずに使用可能であることが求められる。認証の方法は実装に依存するとされているが、本実装で使用

An Integration of CORBA Security Service and Web System
Mayuko SHIMIZU*, Tadashi KAJI**, Katsuhiko KONDO**, Takashi AKAOSUGI*
Hitachi, Ltd. *Software Division, **System Development Laboratory

[1] CORBAは，Object Management Groupが提唱する分散処理環境アーキテクチャの名称です。
[2] IIOPは，OMG仕様によるORB(Object Request Broker)間通信のネットワークプロトコルの名称です。

する Security Service では、クライアントユーザは CORBA 環境へのログインを１度だけ行うことで、CORBA 環境内のすべてのサーバマシンにログインできるようなユーザ認証方式を採用し、認証にはユーザ名とパスワードを用いたものとした。

3. WWW-CORBA 接続のユーザ認証

クライアントユーザがインタネットから WWW サーバを経由してイントラネット内のサーバアプリケーションにアクセスする際に、WWW サーバのクライアント認証のための操作と、サーバアプリケーションのクライアント認証のための操作と、認証のための操作を２度行わなくて済むことがユーザにとっては望ましい。そのため、WWW サーバで認証したユーザはサーバアプリケーションでも自動的に認証する方式を検討し、それを実現した。

システム構成として、クライアント、WWW サーバ、WWW サーバが起動する CGI プログラム、及び CGI プログラムが起動する CORBA で開発したサーバアプリケーションを想定する。

ユーザ認証の統合化方式を図 2 に示す。WWW サーバはクライアントからアクセスがあると、クライアントを認証した際のユーザ ID または SSL 証明書の情報を保存しておく。CGI プログラムは Cookie にクライアント情報を保存しておく。

また WWW サーバ上では、あらかじめ WWW サーバでの認証のためのクライアント情報と、CORBA 認証のためのユーザ情報の対応表を作成しておく。

WWW サーバから起動された CGI プログラムは WWW サーバが保存しておいたクライアントの情報を読み出し、それを元に対応表から CORBA 認証のためのユーザ ID とパスワードを求め、CORBA 環境（CORBA Security Service）へのログインを行う。CORBA 環境で認証されると、サーバアプリケーションへアクセスする。

サーバアプリケーションでは、セション認証で作成されたセキュリティコンテキストにより、クライアントを識別し、アクセスを許可するかを判定する。

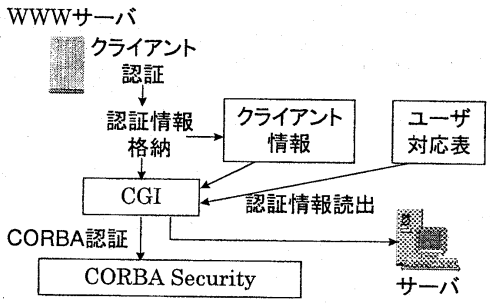

図 2. 認証の統合化方式

4. おわりに

本実装のような異種システム接続におけるセキュリティ構築では、ログイン操作を一本化することでセキュリティ低下をまねかないかという懸念もあり、これはシステム個別のセキュリティ強度の要請と、ユーザの利便性を考慮して検討する必要がある問題である。セキュリティ強度については、暗号やファイアウォールなどのセキュリティ技術の強度も考慮に入れなければならない。またパスワードなどのユーザ情報の管理にも、データの暗号化するなどの注意を払わなければならない。

WWW システムと CORBA システムの接続は、今回の例以外にもクライアントで WWW の HTTP と CORBA の IIOP 通信を併用するなども含めて、今後も多く利用されると思われ、その際のユーザ認証の方式にも、WWW 上、CORBA 上とも種々のものが考えられる。またセキュリティ管理の面では証明書発行・保持の一括管理や、ユーザ情報管理の統合化など運用課題は多いが、多くのタイプのアプリケーションが存在する環境で CORBA および CORBA Security Service による接続は柔軟性が高く、今後も異種システム接続時の応用方法を検討していく。