WWWと分散オブジェクトを組合わせたシステムにおけるユーザ認証モデル

5G－10

林　重年　小瀧　伯泰　内田　稔
（株）日立製作所 ソフトウェア開発本部

1．はじめに

Web ブラウザの統一された操作性で業務システムを構築したいニーズが高まっている。一方，クライアントサーバシステムの基盤として分散オブジェクト技術 CORBA が注目されており、業務システムの拡張性やアプリケーション開発効率の向上が期待されている。

報告者らは、この WWW と分散オブジェクトを組合わせて業務システムを構築する場合において、シングルサインオンを実現するためのユーザ認証モデルについて検討を行った。シングルサインオンにより、1回のユーザ認証で複数の業務システムを利用できるようになる。本稿では、日立ディレクトリサーバ(LDAP)を使ったユーザ管理とユーザ認証及び認証済みユーザの管理方式の枠組みについて報告する。また、本報告のユーザ認証モデルは、WWW と分散オブジェクトという技術を利用して，効率よくシステムを構築することを目的とした，実行環境及び開発環境である Framework - Web for Enterprise で提供予定であり、分散オブジェクト基盤として TPBroker を使用している。

2．WWW-分散オブジェクト基盤の業務システム

WWW と分散オブジェクトを組合わせた業務システムは、図1のようになる。WWW ブラウザからの入力情報を取得し、サーバでの実行結果から動的にページを生成する CGI プログラムと、CGI プログラムからのリクエストを処理する業務プログラムからなる。業務プログラムは分散オブジェクト環境のアプリケーションオブジェクトであり、基本的に各業務でユーザ認証を必要とする。

WWW-分散オブジェクト基盤を使った業務システムで、シングルサインオンを実現する上で考慮すべき点についてまとめると、(1)WWW 環境の通信プロトコル HTTP（Hypertext Transfer Protocol）は接続状態を管理しないので、認証されたクライアントからの一連のリクエストを、サーバ側の各業務オブジェクトを跨って一つのセッションとして処理する必要がある。ここで、あるリクエストが同じクライアントからの要求かどうかの認識は、ユニークな識別子を Cookie で引き継ぐことで可能である。(2)拡張性が高く、負荷分散が容易な分散オブジェクト基盤の上に業務を実現することから、システム変更に対してユーザ認証機能が影響を受けないといった独立性が必要である。

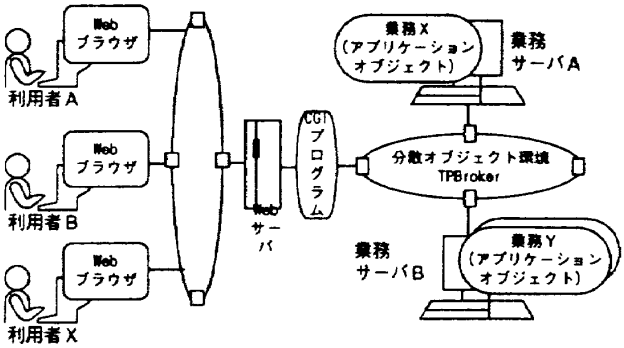

図1．WWWと分散オブジェクトを使った業務

3．システム構成と機能

ユーザ認証モデルのシステム構成を図2に示す。ここでは、ユーザ ID(UID)とパスワード(PWD)による認証方式について述べているが、IC カード方式でも枠組みは同様である。またセッションの識別子をセッション ID(SID)と呼び、CGI プログラムが付与と Cookie への設定を行う。以下にユーザ認証機能の概要を述べる。

① ユーザ認証オブジェクト

指定されたユーザ ID とパスワードをディレクトリサーバ（LDAP）で認証する。認証したユーザ ID は、

A Study of Authentication Model for an Enterprise System based on WWW-Distributed Objects.
Shigetoshi HAYASHI, Michiyasu ODAKI, Minoru UCHIDA
HITACHI Ltd.

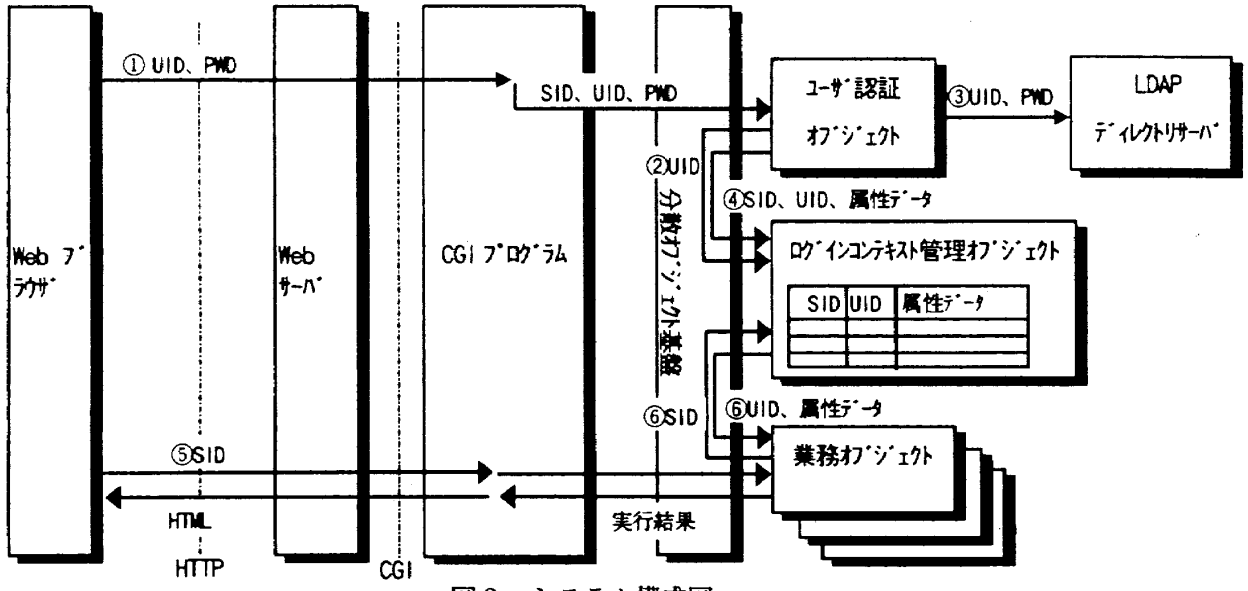

図２．システム構成図

セッション ID とともにログインコンテキスト管理オブジェクトに登録する。

②ディレクトリサーバ

ユーザ ID やパスワード等のユーザ情報の管理と認証を行う。

③ ログインコンテキスト管理オブジェクト

認証済みのセッションのユーザ情報（UID、属性データ）を管理し、セッションが認証済みであるかを判定する。

4．実行手順

図２のシステム構成でのユーザ認証の実行手順を述べる。

（1）ログイン処理

① ブラウザで入力したユーザ ID とパスワードは、Web サーバに送信され CGI プログラムに渡る。CGI プログラムは、セッション ID が渡ってこなければ生成し、ユーザ認証オブジェクトのログインメソッドを呼出す。

② ユーザ認証オブジェクトは、UID を引数にしてログインコンテキスト管理オブジェクトの二重ログインチェックメソッドを呼出す。ログイン済みの場合、ログアウトを要求するページをブラウザに返す。

③ ログイン済みでない場合、ユーザ認証オブジェクトは、ディレクトリサーバでユーザ認証を行う。

④ セッションを認証済み状態にするために、SID、UID 及び属性データをログインコンテキスト管理オブジェクトに登録する。

（2）業務呼出し処理

⑤ CGI プログラムは、ブラウザから渡ってくる SID を使って他の引数とともに、業務オブジェクトのメソッドを呼出す。

⑥ 業務オブジェクトは、SID を使ってログインコンテキスト管理オブジェクトでセッションが認証済みか確認する。認証済みで無い場合、ログインを要求するページをブラウザに返す。認証済みの場合、UID と属性データを必要に応じて取得する。

5．評価

ユーザ認証機能を業務から切り離し、認証済みのセッションをユーザ情報とともに管理しておくことで、業務オブジェクトは必要に応じてセッションの認証状態を問い合わせることができる。これによりシングルサインオンを実現でき、業務オブジェクトの追加・変更にも対応しやすい枠組みと言える。

6．おわりに

本報告では、WWW-分散オブジェクト基盤を使った業務システムでのユーザ認証モデルの枠組みの検討結果について報告した。今後の課題としては、SSL V3 による認証との連携について検証していく予定である。