O-008

シングルサインオン実現方法に関する考察

菊地 克朗†

(株)日立製作所 中央研究所†

1. はじめに

企業情報ポータル(EIP:Enterprise Information Portal)は、企業情報システム(EIS:Enterprise Information System)を統合することにより、利用者のシステム利用効率を改善し、IT システム全体の ROI(Return On Investment)を向上させる。EIP の重要な機能のひとつにシングルサインオン(SSO:Single Sign-On)機能がある。EIP におけるシングルサインオン機能とは、『ユーザがポータルに認証をうける(ログインする)だけで、ポータルに統合されている企業情報システムの機能を利用できるようになる認証方式』である。

一方、多くの EIS は Web アプリケーションとして構築されている。Web アプリーションを実現するための HTTP や HTML は、元々ドキュメントの公開・閲覧システムを目的として開発されたため、アプリケーション基盤としては機能不足と言える。そのためユーザ認証機能やセッション管理機能といったアプリケーションを構築する上での基盤機能は、アプリケーション毎に独自に作りこんでいることが多い。近年、Sun Microsystems 社の提唱する J2EE や Microsoft 社が提供する.Net Framework など Web アプリケーションフレームワークが整備され、ユーザ認証、セッション管理方式はある程度集約されてきているが、一本化されるには至っていない。EIP 構築において SSO を実現するには、既存の様々な Web アプリケーションのユーザ認証機能やセッション管理機能に対応するサインオン方式を検討する必要ある。

2. EIP におけるシステム統合

EIP は IT システムのフロント側の EAI (Enterprise Application Integration)基盤とも言える。ここでフロント EAI とは主にユーザに対するインターフェイス層の統合を意味する。EIP におけるユーザインターフェイス層の統合は表 2-1に示すように大きく 3 つの方法がある。既存 Web アプリケーションの統合を考えた場合、疎結合による統合が費用対効果の点で有効の場合が多いといえる。そこで、本稿では、疎結合での EIP 統合についてシングルサインオン方式の提案を行う。なお、疎結合での SSO において、リンク型とサマリ型は EIS へ要求する URL が異なるだけで、SSO の処理方式については同一である。(相違点は、SSO 先の URL が、リンク方式の場合は主にログイン後のトップページ、サマリ方式の場合はサマリ内の項目に対する詳細情報であるという点である。)本稿は、SSO の処理方式が主題であるので、前者のリンク方式の場合について説明することとする。

Study of Single Sign-On

† Central Research Laboratory, Hitachi Ltd.

表 2-1 統合方式

統合方式	特徴
密結合	・ポータル用のビューを作成し、ポータルの画面内に EIS の画面を統合する。 ・ポータルにアクセスするだけで様々な EIS の必要な情報を取得可能となる。 ・ポータル対応ビューの作成工数が大きい。
疎結合 (リンク型)	・EIS へのリンクをポータル上に表示する。リンククリック時に EIS に SSO を行い、以降 EIS を直接操作する。 ・SSO のみの開発で済むので、短期間で統合を実現できる。 ・情報を確認するには全ての EIS を確認する必要があるので、ユーザの手間があまり減らない場合もある。
疎結合 (サマリ型)	・ポータル上に EIS の新着情報などユーザが必要とする情報を表示する。情報へのリンクをクリックするとリンク型疎結合方式と同様に SSO を行い、以降直接 EIS を操作する。 ・ユーザはポータルにアクセスするだけで必要な情報を確認する事が可能。また、SSO 開発およびサマリ画面のみの作成で済むので、ポータル対応の工数が比較的小さい。

3. シングルサインオン実現方式

シングルサインオンを実現する場合、EIS を改変することにより実現する方式も考えられるが改変にはそれなりのコストが必要となる。そこで、本稿では既存 EIS に手を入れることなくシングルサインオンを実現する方式を提案する。以下、代表的なユーザ認証方式である Basic 認証および Form 認証について SSO 手法を説明する。

3.1 Form 認証

Form 認証でシングルサインオンを実現するためには、基本的には『ポータルサーバが EIS のセッション維持情報を取得し、その情報をブラウザに引渡し、その情報を付加して EIS にアクセスさせる』必要がある。Form認証に対する SSO 方式としてポータル代行ログイン方式および直接ログイン方式を提案する。

(1) ポータル代行ログイン方式

ポータル代行ログイン方式の処理概要を図 3-1に示す。本方式では、『(1)ポータルサーバはブラウザから SSO の要求を受け取り、ブラウザのポータルセッションすなわちログインユーザに対応する EIS の認証情報(主にユーザ ID、パスワード)を SSO テーブルから取得、(2)ポータルサーバが EIS へ代行ログイン、(3) EIS のログイン応答に含

まれるセッション ID を取得、(4)ブラウザに前記ステップで取得したセッション ID を引き継がせると共に EIS に直接アクセスするよう応答を返却』のステップにより SSO を実現する。セッション ID の引継ぎは EIS のセッション維持方法が Cookie を利用している場合には Cookie の domain 指定を利用してポータルサーバと EIS 間で Cookie を共有させることで実現する。また、URL 書き換えの場合は(4)のブラウザから EIS へのアクセス URL 中にセッション ID を埋め込むことにより実現する。

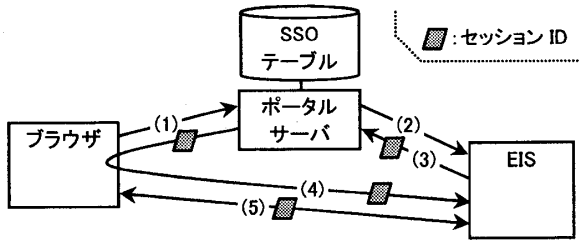

図 3-1 ポータル代行ログイン

(2) 直接ログイン方式

直接ログイン方式の処理概要を図 3-2に示す。直接ログイン方式ではポータルサーバがログイン代行は行わず、ブラウザに対して EIS へのログイン命令を発行して SSO を実現する。具体的には、『(1)ポータルサーバはブラウザから SSO の要求を受け取り、ブラウザのポータルセッションに対応する EIS の認証情報を SSO テーブルから取得、(2)前記ステップで取得した認証情報を HTML Form の hidden フィールドに埋め込み、さらに Form を自動的に EIS にサブミットするようスクリプトを埋め込んだ HTML をブラウザに応答(3)ブラウザはスクリプトに従い EIS に Form をサブミットしてログイン(4)ログイン完了応答』のステップによりSSOを実現する。

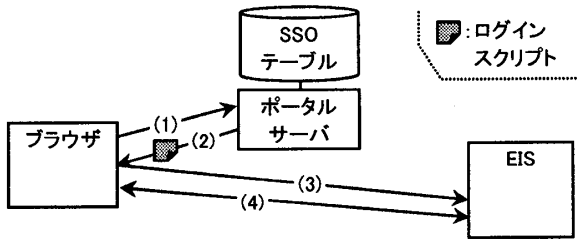

図 3-2 直接ログイン

3.2 Basic 認証

Basic 認証では、全てのリクエストにユーザ ID、パスワードを付加する必要があるが、通常は、ブラウザがユーザからの入力を受け付けてブラウザ内部に保存し、サーバアクセス時に自動的にユーザ ID、パスワードを付加することにより実現されている。また、ブラウザの外部からユーザ ID、パスワードをブラウザに保存させることは基本的に不可能である。従って、Basic 認証の SSO を実現するには、ブラウザから EIS へのリクエストをトラップして、Basic 認証用ヘッダを付加する必要がある。認証情報を付加する位置に応じて表 3-1示す2種類の SSO 方式を提案する。

表 3-1 Basic 認証でのシングルサインオン方式

方式	説明
SSO プロキシ	ブラウザと EIS の間にベーシック認証用ヘッダ情報を付加するプロキシサーバを設置して、SSO を実現。
エージェント	EIS を構成する Web サーバの拡張機能を利用して SSO を実現する。具体的には、ブラウザのリクエストが EIS のプログラムに渡る前に Web サーバ内でリクエストをトラップしてベーシック認証用ヘッダ情報を付加することにより SSO を実現する。

4. 評価

Form 認証の 2 方式に関しては、直接ログイン方式は SSO が容易に実現可能な反面、予めセッション ID を取得するといった前処理が不可能といった点や、ユーザ ID、パスワードなどの情報を HTML に埋め込んでブラウザに応答するためセキュリティレベルが低いといった問題がある。一方、代行ログイン方式は、多少の作り込みが必要ではあるが、ポータルサーバでログインの前処理なども可能で、ほとんどの Web アプリケーションに対応できる柔軟性の高い方式といえる。機密性がそれほど重要ではないシステムへの SSO 適用や SSO 効果の評価といった場合には直接ログイン方式、本格的に SSO を実現する場合には代行ログイン方式を適用するとよい。

一方、Basic 認証の2方式に関しては、SSO プロキシ方式は汎用性が高く、エージェント方式は Web サーバのプラグインとして動作するため必要とする計算機リソース量が小さい。汎用性の高い SSO プロキシで SSO を実現し、SSO プロキシの負荷を軽減するため必要に応じてエージェントモジュールを開発していくと良い。

5. おわりに

企業情報ポータルにおける企業情報システム統合の必須機能の一つであるシングルサインオンを、情報システムに手を加えることなく容易に実現可能とする方式を検討した。シングルサインオンの対象となる Web アプリケーションのユーザ管理方式を調査および分類し、分類したユーザ管理方式にそれぞれ対応し、企業情報システムの改変を必要としないシングルサインオン方式を提案した。これにより、低コストかつ迅速に構築可能なシングルサインオンソリューション実現の見通しを得た。

参考文献

[1] The Internet Engineering Task Force, "Hyper Text Transfer Protocol - HTTP/1.1"
[2] The Internet Engineering Task Force, "HTTP Statement Management Mechanism"
[3] The Internet Engineering Task Force, "HTTP Authentication: Basic and Digest Access Authentication"