4E-2

IDマッピング情報の登録方式に関する一考察

牧　和宏　　鷲尾　元太郎
三菱電機（株）情報技術総合研究所

1. はじめに

現在，ユーザの情報サービス利用の増大に伴い，一度の認証で複数のサービスを利用可能とするシングルサインオン（SSO）が活用されている[1]．SSO 環境において，サービス毎に異なる ID を維持したまま、ユーザが全てのサービスを共通の ID で利用可能とする為の技術として，ID マッピングがある[2]．

本論文では，ID マッピングを実現する為の ID マッピング情報を登録する作業において，登録者の管理負荷を軽減するとともに，管理者やユーザによるサービスの不正利用を防止する登録方式を提案する．

2. ID マッピングを用いた SSO

IDマッピングを用いたSSOの概念図を図 1に示す．図 1において，WebサービスAはWebサービスA用のログインID管理テーブルを保持する．同様に，WebサービスBはWebサービスB 用のログインID管理テーブルを保持する．認証基盤はSSOに利用する共通ID管理テーブルと，共通IDと各サービスのログインIDとを対応付けるマッピング情報を管理するIDマッピングテーブル（図 2参照）を保持する．共通ID管理テーブル及び各ログインID管理テーブルには，IDとパスワード，その他必要な属性が格納されている．

2.1 SSO の実施手順

SSO の実施手順を以下に示す．ここで，各サービスはポータルからアクセス可能とする．ポータルは認証基盤上に存在し，共通 ID でログインする．

① Web サービス A を利用するユーザが，ポータルに共通 ID でアクセス
② ユーザが共通 ID で認証を行っていない場合，認証基盤がユーザに認証を要求し，共通 ID で認証を実施
③ 認証に成功すると，認証基盤は ID マッピングテーブルを用いて，ユーザの Web サービス A でのログイン ID を特定
④ 特定した ID で Web サービス A にアクセス

A Study of ID-Mapping Registration Mechanism
Kazuhiro MAKI, Gentaro WASHIO
Information Technology R&D Center, Mitsubishi Electric Corporation

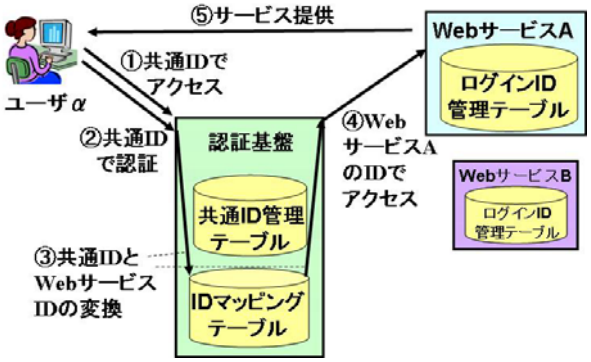

図 1　ID マッピングを用いた SSO の概念図

共通ID	Webサービス	Webサービスのログイン ID
000001	WebサービスA	A999999
000001	WebサービスB	B77B
000002	WebサービスA	A233333

図 2　ID マッピングテーブルの例

⑤ Web サービス A は，ログイン ID とクレデンシャルから，ユーザに対してサービスを提供

一度共通 ID での認証が完了していれば，サービス B にアクセスする際に，認証基盤での認証処理（手順②）は省略される．

2.2 ID マッピング情報の登録における課題

ID マッピングを用いた SSO では，事前に ID のマッピング情報を登録する必要があり，通常は管理者が実施する．しかし，利用対象のサービスやユーザの増加に伴い，管理負荷が増加するとともに管理者が ID マッピング情報を使って不正にサービスを利用するという課題がある．

一方，ユーザ自身が登録を行う場合，他人の ID を不正入手すれば，ユーザ自身の ID と他人の ID とのマッピング情報を登録することが出来る為，他人へのなりすましが可能となる．

そこで，本論文では，上記の課題を解決するセキュア ID マッピング登録方式を提案する．

3. セキュア ID マッピング登録方式

本方式では，管理者ではなくユーザが登録作

業を実施する為，Web サービスの初回利用時に ID マッピング情報の登録処理を自動で起動する．また，ユーザが Web サービス ID を自由に登録できないように、認証基盤と登録したい Web サービスの 2 箇所で認証を実施することとし，両者で認証が成功した場合のみ，ID マッピング情報を登録する．これを実現する為，Web サービス側に ID マッピング指示機能，認証基盤側にセキュア ID マッピング登録機能が必要となる．

3.1 ID マッピング指示機能

本機能は，Web サービスに認証されたユーザの Web サービス初回利用時，または ID マッピング情報登録要求を受付けた時に，認証基盤側に ID マッピング情報の登録を要求する．この時，認証基盤側には認証されたユーザの Web サービスのログイン ID と Web サービスでのクレデンシャルを送付する．また，ID マッピング情報の重複登録を防ぐ為， 要求された Web サービスのログイン ID を含んだマッピング情報が既に登録されているか確認を実施する．

3.2 セキュア ID マッピング登録機能

本機能は，ID マッピング指示機能からの登録要求を受付け，Web サービスのログイン ID と共通 ID のマッピング情報を登録する．Web サービスのログイン ID は ID マッピング指示機能から取得し，共通 ID はユーザに共通 ID での認証を要求し，その結果から取得する．この時，共通 ID での認証に失敗した場合は，マッピング情報の登録は実施せず，その旨を ID マッピング指示機能へ送付する．

3.3 ID マッピング情報の登録手順

本方式の概念図を図 3に示す．本方式では，以下の手順で，IDマッピング情報を登録する．

① ユーザが Web サービス A のログイン ID で Web サービス A にアクセス・認証を実施
② 認証に成功したユーザが Web サービス A を初めて利用する場合，Web サービス A は認証基盤に対して，ユーザの Web サービス A のログイン ID を含んだマッピング情報が存在するか確認
③ ID マッピング情報が存在しない場合，Web サービス A は認証基盤に対して，ID マッピング情報の登録要求を送信
④ 認証基盤はユーザに対して，共通 ID での認証を要求
⑤ ユーザが共通 ID で認証を実施
⑥ 共通 ID で認証が成功すると，ID マッピングテーブルに，共通 ID と Web サービスのログイン ID のマッピング情報を登録

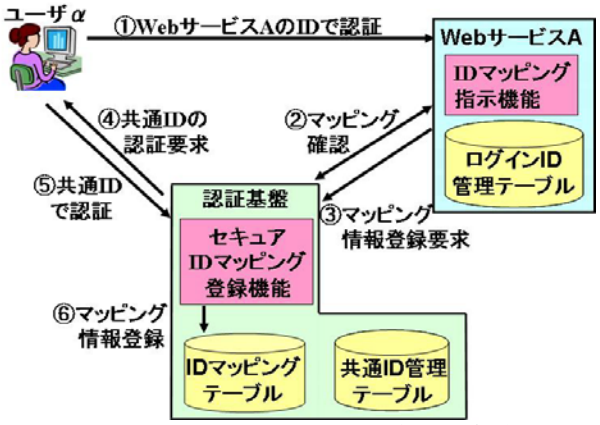

図 3　セキュア ID マッピング登録方式

4. 効果

Web サービス数 M，ユーザ数 N の場合，従来では，管理者が M×N 個の ID マッピング情報を作成・登録する必要があったが，本方式では，各ユーザが M 個の ID マッピング情報を登録するだけでよく，登録者の管理負荷を軽減できる．

また，本方式では，管理者が ID マッピング情報の登録を実施しない為，管理者の ID マッピングを使った不正なサービス利用を防止することが出来る．

さらに，本方式では，Web サービスと認証基盤の 2 つの認証結果を受けて ID マッピング情報の登録を行っている為，他人の ID を不正入手したユーザが他人の ID とのマッピング情報を登録することが出来ず，他人へのなりすましを防止することが出来る．

5. まとめ

本論文では，登録者の管理負荷を軽減するとともに ID マッピング情報をセキュアに登録することが出来る，今後は，提案手法の実装・評価を実施していく．

参考文献

[1]飯田勝吉ほか：”キャンパス共通認証認可システムの構築と運用”，電子情報通信学会論文誌，Vol. J92-B. No. 10. pp. 1554--1565, Oct. 2009

[2]Liberty Identity Web Services Framework (ID-WSF) 2.0, http://projectliberty.org/liberty/resource_center/specifications/?f=liberty/resource_center/specifications