L-031

企業間認証連携における利用者特定方式
Digital identity aggregation with the traceability of the original account for the federated identities across multiple enterprises

石川 祐輔† 白木 宏明† 菅野 幹人†
Yusuke Ishikawa Hiroaki Shiraki Mikihito Kanno

1. はじめに

企業グループ内では、業務効率化のために各グループ企業の業務システム（専用ポータル等）を相互利用している。各企業では業務システム利用時の本人特定のために認証システムが導入され、業務システムを利用するためには各認証システムで利用者の認証が必要になる。各グループ企業で業務システムを一度の認証で利用するためには異なる認証システム間の連携[1]が有効である。これを企業間認証連携と呼ぶ。企業間認証連携を実現するためには業務システムを持つ利用先企業に利用者のアカウント(ID／パスワード等)を登録する方式があるが、利用者の個人情報が秘匿できず利用先企業はアカウントの管理義務を負うというデメリットが生じる。業務システムの利用者に対し、属性に応じた権限(利用者アカウント内の役職、所属情報等)による制限を設ける必要があり内部統制のため、監査を行い利用者特定ができる仕組みも備える必要がある。規模として利用者数 1000 人～30 万人を対象とする。上記の要件を満たすためには以下の三点の課題を解決しなければならない。

(1) 利用者情報の秘匿
(2) 利用者の権限に応じたアクセス制御
(3) 監査時の利用者特定

本稿は、企業間認証連携において上記三点の課題全てを解決するための方式について記述する。

2. 既存方式の概要

本章では既存方式とその課題について記述する。認証連携の既存方式では、アカウントとアカウントを対応付けるマッピングという技術を利用する。

2.1 1：1 マッピング方式

既存の企業間認証連携のモデルとして、利用先に利用者のアカウントを直接登録する 1：1 マッピング方式がある。図 1に 1：1 マッピング方式を示す。

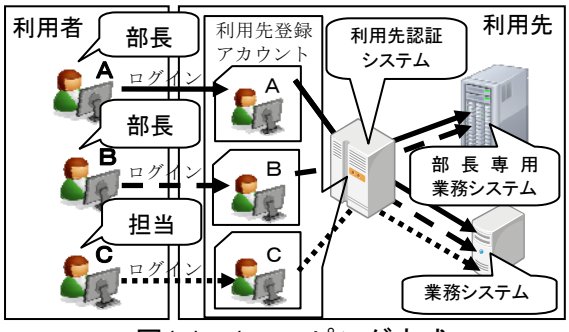

図1 1：1 マッピング方式

前記の 1：1 マッピング方式では、利用者本人のアカウントを利用先に登録するため、適切なアクセス制御と監査時の利用者特定を可能とする。

2.2 N：1 マッピング方式

既存の企業間認証連携のモデルとして、属性に応じた権限のアカウントに集約する N：1 マッピング方式について記述する。図 2に N：1 マッピング方式を示す。

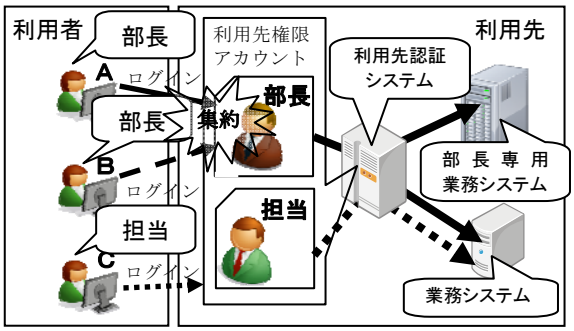

図2 N：1 マッピング方式

上記の N：1 マッピング方式ではログインした利用者のアカウントを利用者の属性に応じた権限(図 2では部長と担当)によって集約し、利用先に登録されている権限アカウントによるアクセス権限を付与している。そのため、利用者情報の秘匿が可能であり、適切なアクセス制御を可能とする。

2.3 既存方式と課題の比較

既存方式である 1：1 マッピング方式と N：1 マッピング方式と1章で明記した課題との比較を表 1に示す。

表1 既存方式と課題の比較

課題	1：1マッピング	N：1マッピング
(1) 利用者情報の秘匿	× 利用者本人のアカウントを利用先に登録	○ 属性に応じた権限アカウントに集約
(2) 利用者の権限に応じたアクセス制御	○ 利用者本人アカウントの権限に応じてアクセス制御が可能	○ 属性に応じた権限によるアクセス制御が可能
(3) 監査時の利用者特定	○ 利用者本人アカウントから利用者の特定が可能	× アカウント集約により利用者特定が不可能

表 1から既存方式では、1章で明記した課題を全て解決することができない。1：1 マッピング方式では、利用者本人のアカウントを直接利用先に登録するため、利用者情報の秘匿ができず、異動によるシステム利用者の変更等で削除

† 三菱電機 情報技術総合研究所 情報システム構築技術部
Information System Integration Technology Dept., Information Technology R&D Center, Mitsubishi Electric Corporation

忘れが発生し、不正アクセスの危険性がある。また、利用先では自他両企業のアカウントを登録、管理、同期等、運用負荷の増大が発生する。N：1 マッピング方式では、利用者のアカウントを属性に応じた権限アカウントに集約されるため、同権限を持つ利用者がアクセスした場合、利用者の特定が不可能である。

3. 本方式の概要

本章では、1章にて明記した三点の課題を全て解決する方式について記述する。課題(1)の解決には、アカウントを集約することが必要となるため、N：1 マッピング方式を採用し、課題(3)の解決のため、ログを利用した利用者特定機能を導入する。本方式での認証プロトコルは、SAML[1] を使用する。

3.1 N：1 マッピング利用者特定方式

利用者側の認証システムでは利用者のログイン後、アカウントから仮名 ID を生成する。次に、仮名 ID と権限情報（役職等）を利用先の認証システムに送信する。利用先の認証システムでは、権限情報から権限 ID を生成し、権限 ID による認証を行う。双方の認証システムが導入されているサーバでログを記録し、ログを突合せることで利用者の特定を可能とする方式である。図 3に本方式のフローを示す。

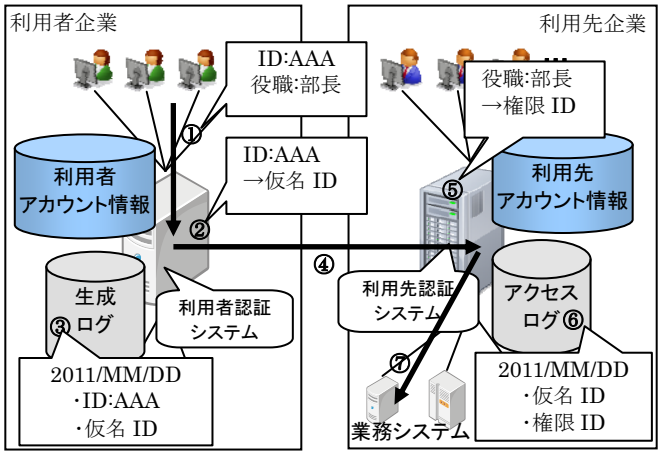

図3 利用者特定方式認証フロー

① 利用者が ID／パスワードを入力しログイン
② 認証後、入力された利用者の ID から仮名 ID を生成
③ 利用者 ID と仮名 ID を生成ログとして利用者側の認証システムに記録
④ 認証情報を発行し、権限情報と仮名 ID を利用先に送信 **【課題(1)利用者情報の秘匿】**
⑤ 権限情報を権限 ID に集約し、認証 **【課題(2)利用者の権限に応じたアクセス制御】**
⑥ 仮名 ID と権限 ID をアクセスログとして利用先に記録
⑦ 業務システムへアクセス

前記のように利用者側のサーバには、生成ログとして利用者の ID と仮名 ID が記録されており、利用先のサーバには、アクセスログとして仮名 ID と権限 ID が記録されている。相互のサーバにログを記録し、監査時にはログ情報の問い合わせにより、利用者を特定することが可能である。利用者特定のフローを図 4に示す。

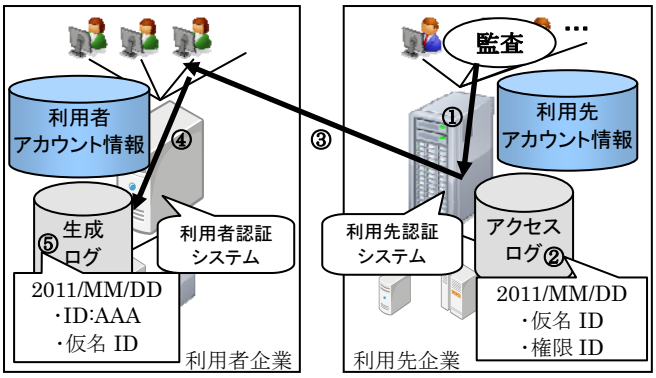

図4 利用者特定フロー

① 監査時、利用先サーバのアクセスログを調査
② アクセス時間と仮名 ID の特定
③ 利用者側にログデータを問い合わせ
④ 利用者側で問い合わせの仮名 ID を生成ログで検索
⑤ 利用者を特定 **【課題(3)監査時の利用者特定】**

上記のように、利用者特定方式を用いることで三点全ての課題を解決することができる。

3.2 仮名 ID 生成モジュール

本方式では、図 3の②で利用者の ID から仮名 ID の生成を行うが、既存製品ではこの機能がないため、仮名 ID 生成モジュールを新規開発した。仮名 ID は、利用先で複号されてしまえば利用者の ID が露呈してしまうため、秘匿性が失われることになる。このため、仮名 ID は不可逆であることが条件となる。本方式における仮名 ID 生成モジュールはアカウントから利用者の ID を取得し、ハッシュ関数からハッシュ値に変換した値を仮名 ID とし、生成ログに記録する機能を持つ仕組みとなっている。

4. おわりに

本稿では、企業間認証連携における利用者特定方式において、既存方式の課題を挙げ、仮名 ID の生成、権限 ID でのアカウント集約、双方ログの突合せによる利用者特定の三機能により課題解決する方式について記述した。関連研究では属性加工を施し、属性での制御を行うもの[2]も存在するが本方式のような技術は他に見受けることがない。本方式については、実際に既存製品にて環境を構築し、プラグインとして仮名 ID 生成モジュールの開発を行い、実証検証にてプログラム試験、ソフトウェア試験、非機能要求による評価を行った。結果、1章にて明記した全ての課題をクリアしていることを確認した。

今後、今回実現した方式を認証連携基盤技術として活用し、企業における認証技術、企業間における認証連携技術の発展に尽力する。

参考文献

[1]伊藤 宏樹, “クラウドにおけるアイデンティティ管理の課題” 情報処理 2010 年 12 月号 (2010)
[2]阿部 英司, 伊藤 栄典, 笠原 義晃, “認証フェデレーションにおける IdP の属性制御” 電子情報通信学会 2010 年総合大会講演論文集(2010)

SAML[1]：Security Assertion Markup Language の略。標準化団体 OASIS によって策定された、ID やパスワードなどの認証情報を安全に交換するための XML 仕様。