3E-2

認証連携 ID・アカウントロック方式の提案

石川 祐輔† 白木 宏明† 大松 史生†
三菱電機(株) 情報技術総合研究所†

1. はじめに

近年、グローバル化が進み、海外拠点を複数持つ企業が増加している。また海外拠点では各国毎に業務システムが存在し、セキュリティ確保のため、個人の ID が管理されている[1]。
しかし、従来、海外拠点を持つ企業内の ID 管理は拠点によって ID の採番ロジックやユーザに付与する属性の相違といった異なるポリシーを持つため、各国各拠点で独自に実施されており、連携するためには運用でカバーする必要がある。また、人事情報のメンテナンスは各国各拠点のレベルに依存しており、提供される情報を信頼する前提で連携するしかないのが現状である[2]。

拠点毎に独自に ID が管理されていることから、ID が拠点毎に必要となるだけ生成されるため、ID の多重管理が発生する。人事情報のメンテナンスはどの拠点であっても基本的に手作業で行われるため ID の削除漏れが発生する可能性がある。

本稿では異なるポリシーを持つ拠点における ID 管理システム間で ID 情報を連携するために、「ID 多重管理の防止」と「拠点を跨る異動時の ID 削除漏れ回避」を実現する方式を提案する。

2. 従来方式

2.1. 従来方式の概要

従来の ID 管理方式では、拠点毎にポリシーが違うことから各拠点で ID 管理が個別に構築されており、海外拠点への異動時、該当ユーザの ID は異動先拠点の ID 管理で別に発行されるため、ID の多重管理となる。また、再度採用元拠点に異動となった際、ある海外拠点では申請が紙媒体ベースであることや、人事情報のメンテナンスは基本的に手作業で実施されるといった理由から、異動先で使用していた ID の削除漏れが発生する可能性がある。

図 1 にて従来の ID 管理方式について記載する。
①ユーザ X が A 国用のユーザ ID を使用し、A 国認証サーバにて A 国 ID 管理内のデータと比較し、認証が完了し、A 国の業務システムを利用
②A 国人事担当から B 国人事担当へユーザ X の人事情報を提供
③B 国人事担当は提供された人事情報から手作業でメンテナンスした人事データを B 国 ID 管理にインプット
④ユーザ X が A 国から B 国拠点へ異動する
⑤B 国拠点内で用意された B 国用ユーザ ID にてログイン処理を行い、B 国内の業務を利用

ここで、ユーザ X は A 国が採用元拠点であることから A 国用のユーザ ID は消去されることがない。図 1 で示す通り、ユーザ X に対するユーザ ID は A 国と B 国で 2 つ存在し、それぞれの拠点にて管理されることとなる。つまり、ID の多重管理となっていることがわかる。

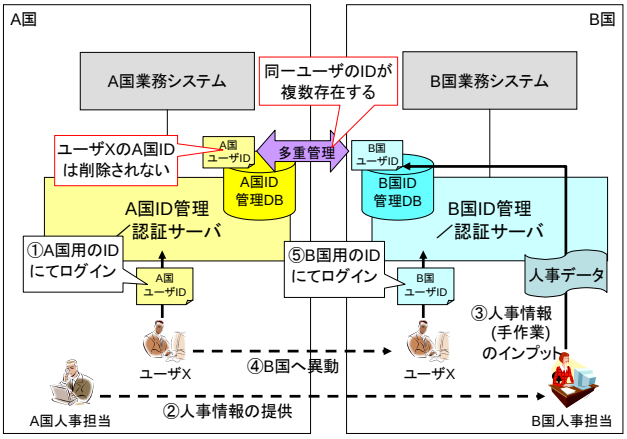

図 1 従来の ID 管理方式

2.2. 従来方式の課題

従来方式では以下のような課題が存在する。
【課題 1】ID 多重管理による ID 削除漏れの発生
【課題 2】ID 削除漏れによる不正アクセスによるデータ改ざんなどのセキュリティリスク発生

3. 課題の解決策

2 章 2 節に挙げた【課題 1】の解決には「ID 多重管理の防止」、【課題 2】の解決には「拠点を跨る異動時の ID 削除漏れ回避」の 2 つの機能を実現する必要がある。
【解決策 1】「ID 多重管理の防止」ではマスタ ID とマスタ ID を基に生成されるサブ ID を階層

Proposal of account locking system to work with federated Identity
†Yusuke Ishikawa, Hiroaki Shiraki, Fumio Ohmatsu
Information Technology R&D Center, Mitsubishi Electric Corporation

構造にて管理することで解決する(図 2 参照)。マスタ ID はサブ ID を管理する ID であり、サブ ID はユーザがシステムにログインするための ID である。

【解決策２】「拠点を跨る異動時の ID 削除漏れ回避」ではある拠点用のサブ ID を使用している場合、その他のサブ ID を全てロックするという手法にて解決する(図 3 参照)。

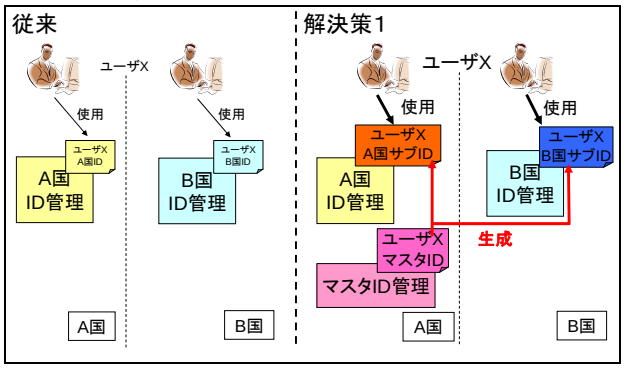

図 2【解決策１】ID 多重管理の防止

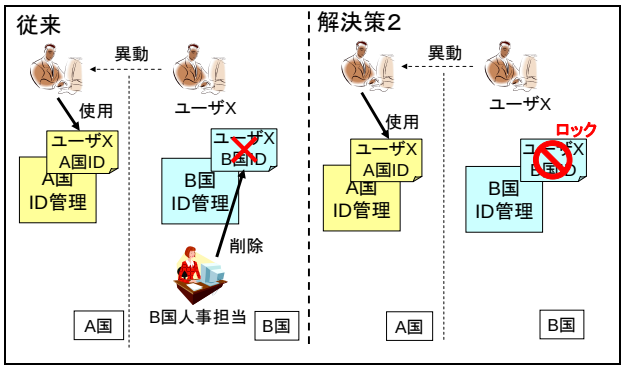

図 3【解決策２】ID 削除漏れの回避

4. 提案方式

解決策１および解決策２を満たす認証連携 ID・アカウントロック方式を提案する。

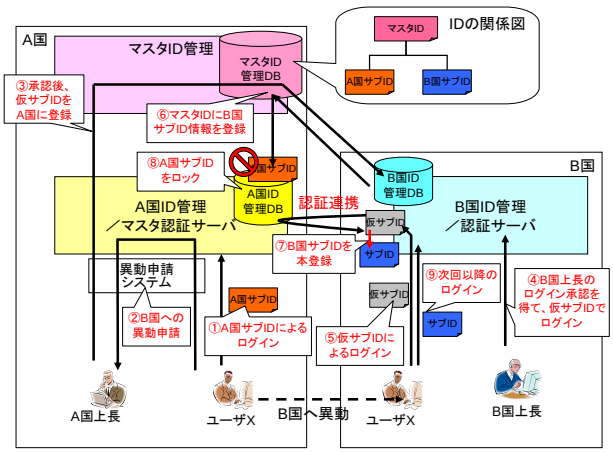

図 4 認証連携 ID・アカウントロック方式

4.1. 提案方式のフロー

図 4 のフローについて説明する。

①ユーザ X は A 国サブ ID にて A 国システムへログインする

②ユーザ X が A 国システムから B 国への異動申請を行う

③A 国での所属上長による承認後、B 国の ID 管理システムに B 国用のポリシーが付加されたユーザ X の仮サブ ID が生成される

④B 国にて初回ログイン時、B 国上長のログイン承認を得て、ユーザ X が仮サブ ID を使用し、B 国の認証サーバへログイン処理を行う。

⑤A 国のマスタ認証サーバは B 国認証サーバからのリクエストを受取り、認証連携する。

⑥ユーザ X のマスタ ID に B 国サブ ID が登録される

⑦B 国の仮サブ ID が本登録(B 国サブ ID)となる

⑧ユーザ X の A 国サブ ID のアカウントをロックし、使用不可とする

⑨次回以降の B 国でのログインは B 国サブ ID を使用し、B 国認証サーバへのリクエストのみ実施

4.2. 提案方式による効果

本提案方式により、全ての課題の解決が可能となり結果、成りすましなどによる不正アクセスおよび不正アクセスによるデータ改ざん等のセキュリティリスクの防止の効果を得る。

5. おわりに

本稿では従来の方式における【課題１】【課題２】を挙げ、これらの解決策としてそれぞれ「【解決策１】ID 多重管理の防止」「【解決策２】拠点を跨る異動時の ID 削除漏れ回避」を提示した。また、上記の解決策を導入した認証連携 ID・アカウントロック方式について提案した。

認証連携 ID・アカウントロック方式ではマスタ ID にてユーザが使用するサブ ID を管理するため、ID 多重管理の防止が可能となり、使用しないサブ ID をロックするという機能により ID の削除漏れを回避することが可能となることを評価した。

今後は実機での検証を行い、本方式の有用性を確立することで、認証および ID 管理技術の発展に尽力する。

［参考文献］

[1] 独立行政法人 情報処理推進機構技術本部 セキュリティセンター, “アイデンティティ管理技術解説” (2010)

[2] 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)