3F-2

アクセス権限集約型認証連携方式

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、企業およびその傘下グループ企業では業務効率化のため、グループ内にて共有すべき業務システム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、利用者の認証を行っている。さらに、各企業間の業務システムを一度の認証で相互利用する場合、認証情報をキーとして異なる認証システムを連携[1]させることが有効となる。これを認証連携と呼ぶ。

従来の認証連携では、利用者の個人情報は各所属企業内で管理し、通常は同期されることがない。例えば、企業 A が企業 B の業務システムを利用する場合、「企業 A での権限に応じた企業 B の特定 ID に集約する」もしくは、「企業 A の利用者のうち企業 B のシステムを利用する利用者を登録する」の 2 つが挙げられる。

後者は企業 B の利用者 ID に加え、企業 A の利用者 ID の登録もする必要があり、運用負荷の増大やアカウントの消し忘れ等による情報漏洩等の理由から前者の採用が多い。前者の例として、N：1 マッピング利用者特定方式[2]が挙げられる。

本来、企業の利用者個人情報では個人に対し約 100～200 属性、利用者認証情報では約 20～30 属性を管理し、利用していることが多い。

しかし、上記方式ではグループ企業の業務システムへのアクセス可否を制御するアカウント(権限 ID)が単一属性から関連付けられているため、適切なアクセス制御ができない課題がある。

本稿では企業で管理する属性を組合せることで、適切かつ決め細かいアクセス権限を可能とする認証連携方式について提案する。

2. 従来方式

2.1. N：1 マッピング利用者特定方式概要

従来、提案してきた方式として当該方式が存在する。この方式は単一属性を基に権限 ID を生成し、権限 ID にて連携先の認証システムにアクセスするものである。当該方式の認証フローを図 1 に示す。①企業 A の認証システムで利用者の認証後、②権限情報および利用者 ID を基に生成した仮名 ID を認証情報に格納する。③認証情報を企業 B の認証システムへ送付し、④格納されている権限情報に応じた権限 ID に変換して⑤業務システムにアクセスする。

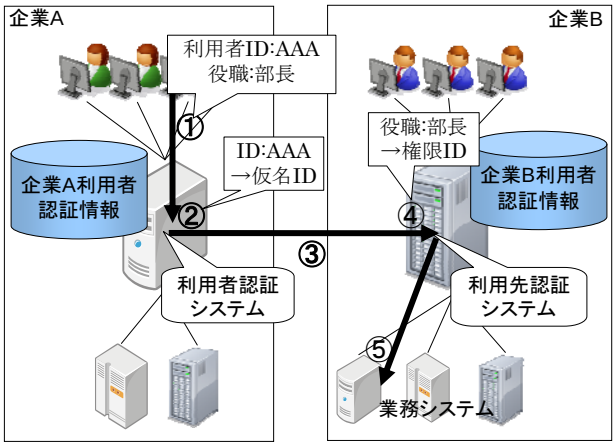

図1 N：1 マッピング認証連携フロー

2.2. 従来方式の課題

前記の方式では、利用できる権限情報が単一の属性であり、単一属性だけでは適切なアクセス制御ができず、認証情報に権限情報を不正に格納することで権限の持たない利用者でも自由にアクセスを許してしまう危険性を孕んでいる。セキュリティ確保のため、きめ細かく適切なアクセス制御を実現する必要がある。

3. 課題の解決策

前記の課題解決策として利用できる属性を増やすことが挙げられる。しかし、単純に認証情報に格納する属性を増やすだけでは認証サーバへの負荷増大による性能劣化等も懸念される。また、現状では利用者認証情報から属性を利用しているが、グローバル化による属性の追加やセキュリティ向上のため、利用者個人情報の属性も利用したいという要件がある。課題解決には以下の 3 点を実施する必要がある。

(解決策1) 利用者認証情報からの属性だけでなく利用者個人情報からの属性も利用する
(解決策2) 利用できる属性を増やす
(解決策3) 性能劣化回避のため、利用する複数属性を集約する

Federated Identity by Using Aggregative Access Privileges
†Yusuke Ishikawa, Hiroaki Shiraki, Fumio Omatsu
Information Technology R&D Center, Mitsubishi Electric Corporation

4. 提案方式

4.1. 追加前提条件

従来方式では利用者認証情報のみであったが、認証システムと直接接続のない利用者個人情報と自企業に 3 つのテーブル、連携先に 1 つのテーブルを新規に追加構築する。

表1　本方式による追加テーブル

自企業	連携先企業
権限 ID テーブル	権限 ID アクセス許可テーブル
URL-ID テーブル	
権限 ID 条件式テーブル	

4.2. アクセス権限を集約した権限IDの生成

アクセス権限を集約し、権限 ID を生成するまでのフローを以下に説明する。

①利用者(ID：A123)が業務システム(https://xxx.yyy.jp)にアクセス後、利用者の行き先URLから権限ID条件式テーブルを検索

表2　権限 ID 条件式テーブル

ok_logon	(“所属=A 部”and“役職=部長”) or”兼務 1=X プロジェクト”	https://xxx.yyy.jp

②権利 ID 条件式テーブルから権限 ID テーブルのベースを作成

表3　権限 ID 条件式テーブル(②処理時)

ok_logon			(“所属=A 部”and“役職=部長”)or”兼務 1=X プロジェクト”

③利用者 ID を権限 ID テーブルに格納

表 4　権限 ID 条件式テーブル(③処理時)

ok_logon	A123		(“所属=A 部”and“役職=部長”)or”兼務 1=X プロジェクト”

④利用者 ID のレコードを利用者認証情報と利用者個人情報から検索**(解決策 1)**

表5　利用者認証情報テーブル

利用者 ID	部	課	役職	…
A123	A 部		部長	…

表6　利用者個人情報テーブル

利用者 ID	氏名	部	兼務情報	…
A123	山田太郎	A 部	X プロジェクト	…

⑤権限 ID 条件式と④で検索したデータを比較

表7　条件式比較

条件式	(“所属=**A 部**”and“役職=**部長**”)or ”兼務 1=**X プロジェクト**”				
利用者認証	A123	**A 部**		**部長**	…
利用者個人	A123	山田太郎	**A 部**	**X プロジェクト**	…

比較により、条件を満たす場合のみ次の処理に移行し、満たさない場合は処理は終了する。

⑥URL-ID テーブルから行き先 URL と対応する URL-ID を権限 ID テーブルに格納**(解決策 2)**

表8　URL-ID テーブル

https://xxx.yyy.jp	kaihatsu

表9　権限 ID テーブル(完成版)

ok_logon	A123	kaihatsu	(“所属=A 部”and“役職=部長”)or”兼務 1=X プロジェクト”

⑦権限 ID テーブルが完成したらテーブルから権限 ID を抽出する「ok_logon」**(解決策 3)**

4.3. 権限IDによる認証連携

4.2 章で生成した権限 ID を利用し、認証連携を行うが、従来のままでは単一属性によるアクセス制御しかできないため、本方式による権限 ID を活用することができない。ここで発生する課題については連携先の企業に権限 ID アクセス許可テーブルを配置することで解決する。

表10　権利 ID アクセス許可テーブル

権利 ID	アクセス許可 URL	許可業務システム名
ok_logon	https://xxx.yyy.jp	開発ポータル

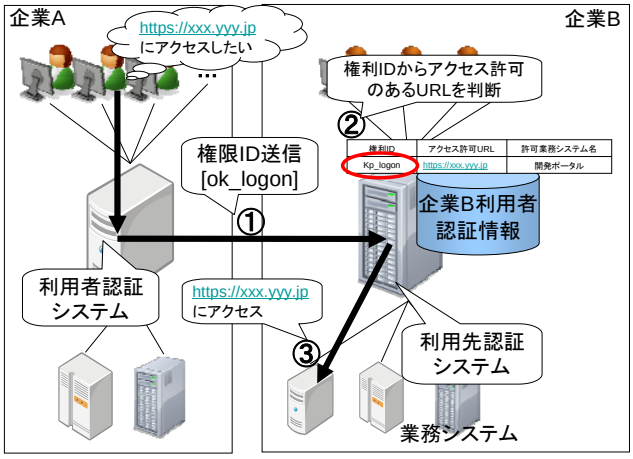

図2　本方式の認証連携フロー

認証連携の流れは図 2 に示す通りである。①認証連携の送信された権利IDから②権利IDアクセス許可テーブルにてアクセス許可URLを検索し、利用者の行き先URLとマッチングする。マッチングが成功した場合、③行き先https://xxx.yyy.jpにアクセスを許可する。

以上より、本方式にて 3 つの解決策全てを満たすことが確認できる。

5. おわりに

本稿では従来の認証連携方式の課題策から 3 点の解決策を挙げ、全てを解決可能とする手法としてアクセス権限集約型認証連携方式の提案を行った。従来の方式に本方式を適用することで従来方式の機能を損なわず、きめ細かい適切なアクセス制御を可能とする。

今後、実機による検証を行い、本方式の有用性を確立し、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] 石川 祐輔, 白木 宏明, 菅野 幹人 “企業間認証連携における利用者特定方式” FIT2011 第 10 回情報科学技術フォーラム (2011)