4H-6

マルチテナントアプリケーションにおける テナント間の権限委譲方式に関する研究

○小川康志† 入不二 経勝† 小杉 優† 山足 光義†

三菱電機株式会社 情報技術総合研究所†

Abstract

クラウド環境のサービスにおいては、単一のアプリケーションを複数のユーザ企業が共用する「マルチテナント」型のサービス形態が増えつつある。このようなサービスは、同一のソフトウェア・ハードウェアリソースを共有可能となるため、サービス提供コストを低減できるメリットがある。

マルチテナント型サービスは、テナント間でデータアクセスが完全に分離されるため、データエントリなどの業務代行や保守サービスを実現するには、本来のテナントユーザの他に別途ユーザ ID を発行して貸与するなどが必要となり、ユーザ管理コストやセキュリティ上で問題がある。ここでは、仮 ID の発行や他テナントに対して不必要な情報公開を行うことなくテナント間の代行や保守サービスを容易に実現する「テナント間の権限委譲の方式」について報告する。

1. 背景

近年の情報システムにおいては、自社内で管理している設備機器を利用して運用する形態の「オンプレミス」から、自社で設備を所有することなくデータセンターに構築された IT インフラをインターネットを介して利用する「クラウド」への移行が進みつつある。

クラウド型サービスの普及に伴い、単一のアプリケーションを利用して複数のテナントに対してサービスを提供可能とする図 1のような「マルチテナント型」のアプリケーションが注目されている[1]。マルチテナント型のアプリケーションの導入により、複数のテナントがソフトウェア・ハードウェアリソースを共有することが可能となるため、低価格でサービス提供を行うことができる。

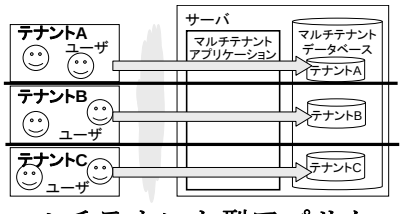

図 1：マルチテナント型アプリケーション

Tenant Authority Delegation Method for Multi-tenancy Application

† Yasushi Ogawa, Nobukatsu Irifuji, Yu Kosugi, Mitsuyoshi Yamatari,
Information Technology R&D Center, Mitsubishi Electric Corporation

2. 課題

通常、マルチテナント型のアプリケーションは、図 2に示すようにテナント内のデータは他のテナントには公開せず、テナントごとにデータアクセスが分離される。

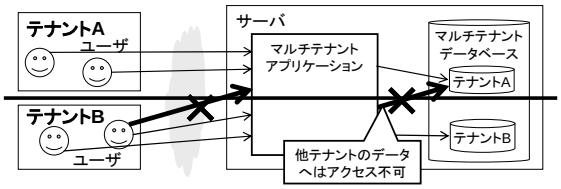

図 2：テナント間のデータアクセス分離

データエントリなどの業務代行や保守を行う場合、対象のテナント上に仮のユーザ ID を発行し、代行業者に仮 ID を貸与することで、テナント内のデータアクセスを許可する方法がとられることもある。しかしながら、この方法では代行用のユーザを管理するコストが必要となる点やユーザ ID を他テナントに貸与することによるセキュリティの点で課題がある。そこで、マルチテナントアプリケーションにおいて、新たにユーザを作成することなく、また、ユーザ ID や組織情報などを不用意に公開することなく、他テナントに対して権限を委譲する方式が求められる。

3. ロールベースのテナント間権限委譲方式

上記課題を解決するため、ロールベースのテナント間権限委譲方式（以下、権限委譲方式と記す）を提案する。ロールを用いてテナント間の権限委譲関係を管理することで、仮 ID の発行や不用意にユーザ ID を公開することなく、テナント間のデータアクセスを柔軟に管理することが可能となる。

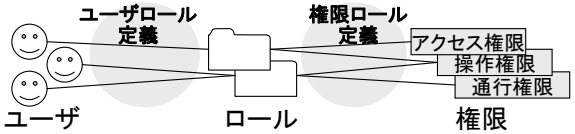

図 3:ロールベースアクセス制御方式

テナント間の権限委譲方式を説明する前に、

一般に広く利用されているユーザ権限の管理方式ロールベースアクセス制御方式について説明する。この方式のイメージを図 3に示す。これは、ユーザに対してロールと呼ばれる”ユーザが果たす役割にあたる概念”を割り当て、そのロールに対して権限を割り当てることで、ユーザと権限の対応関係を柔軟に管理することができる方式である。マルチテナントアプリケーションにこれを適用し、テナント内のユーザのアクセス制御を行う方式も提案されている[2]。しかしながら、これらは他テナントのユーザに対して権限を委譲することはできない。そこで、ロールの作成方式に着目し、テナント間の委譲方式を提案する。

まず、例として２つのテナント（テナント A、テナント B）において、テナント A からテナント B に対して、業務代行を委託するため権限の委譲を行うケースを想定する(図 4)。本方式ではテナント A からテナント B に権限を委譲したとき、権限の委譲元となるテナントＡに「委譲元ロール」を作成し、また、委譲先のテナントＢに「委譲先ロール」を作成する。さらに、これらテナントをまたがる二つのロールを関係付ける「テナント委譲関係定義」を作成し、テナントをまたがる委譲関係を定義する。

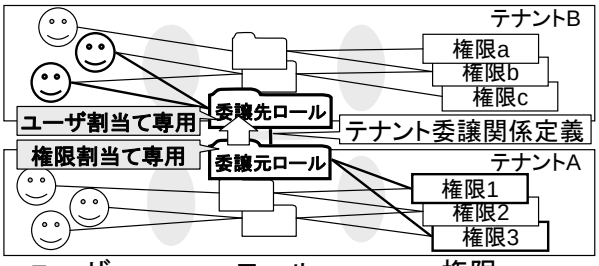

図 4:テナント間の委譲ロール作成イメージ

・**委譲元ロール**：委譲元のテナント上に作成されるロールであり、委譲元テナント内の権限のみを割り当てることができるロール。
・**委譲先ロール**：委譲先のテナント上に作成されるロールであり、委譲先テナント内のユーザのみを割り当てることができる。
・**テナント委譲関係定義**：複数のテナント間をまたがった「委譲元ロール」と「委譲先ロール」の関係を定義したもの。

以上の定義情報を用いることで、複数のテナントをまたがったユーザと権限間の関係管理を可能とする。図 5にテナント間の権限委譲の流れを示す。

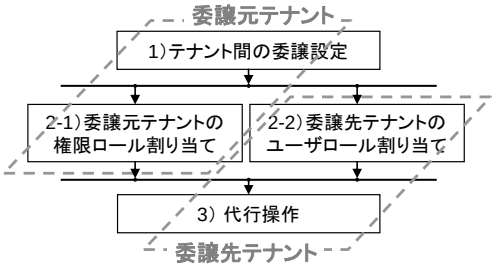

図 5：権限委譲の流れ

1) 権限の委譲はテナント単位で行い、委譲元テナントが委譲先テナントに対して権限の委譲指定を行う。このとき、テナント A・B の「委譲元ロール」・「委譲先ロール」と「テナント委譲関係定義」をセットで作成する。
2-1) 委譲元テナントにおいて、1) で作成された「委譲元ロール」に権限を割り当てる。
2-2) 委譲先テナントにおいて、1) で作成された「委譲先ロール」にユーザを割り当てる。
3) 委譲先テナントにおいて、ロールに割り当てられたユーザでログインすることで、委譲元ロールに割り当てられた権限を利用し、代行操作が可能となる。

この方式は、委譲元テナントの権限そのものを公開しない点、また、委譲先テナントのユーザ情報を委譲元テナントに公開することなくテナント間で権限委譲が行える点にメリットがある。つまり、本方式により、ユーザや権限の管理を自身のテナント内で閉じて管理することが可能となり、不用意な情報公開を行わずにテナント間の権限委譲が実現できる。

4. まとめ

本稿では、マルチテナントアプリケーションにおいて、ユーザや権限などを直接公開することなく、テナント間で、権限の委譲を可能とするテナント間権限委譲方式を示した。

今後は、本方式を実際のマルチテナントアプリケーションへ適用する際のロール構築方式の最適化や評価を行っていく必要がある。

参考文献

[1] Salesforce.com 著, 「Force.com のマルチテナント型アーキテクチャ - セールスフォース・ドットコムのインターネットアプリケーション開発プラットフォーム」, 2009, http://www.developerforce.com/media/ForcedotcomBookLibrary/Force.com_Multitenancy_WP_101508_JP.pdf
[2]キヤノンＩＴソリューションズ株式会社, 「情報処理装置、情報処理方法、及びコンピュータプログラム」, 特開 2011-128994, 2011.6.30