仮想サーバ統合環境の権限管理基盤

小川 隆一・前野 義晴・中江 政行

要　旨

仮想サーバ統合環境においては、異なる組織のユーザが、さまざまなソフトウェアを介してリソースを正しく共有し、不正アクセスや情報漏洩を未然に防ぐ必要があります。しかし、リソースの動的配置やサービスの生滅が頻繁に生じるクラウド環境では、アクセス権管理・設定を正しく行うことは大きな運用負担となります。この課題を解決するため、弊社はマルチレイヤ・マルチベンダソフトウェアに対応する統合アクセス権管理技術を開発しました。

本稿では、開発した技術の概要、及びその国際標準化提案について紹介します。

キーワード

●仮想サーバ ●ロールベースアクセス制御 ●権限管理 ●リソースモデル
●自動設定 ●DMTF標準化

1. まえがき

近年、仮想化技術を用いて、異なる組織に属する複数のサーバを一つのサーバに集約する仮想サーバ統合環境が普及しています。この環境においては、異なる組織のユーザが、さまざまなソフトウェアを介してリソースを正しく共有し、不正アクセスや情報漏洩を未然に防ぐ必要があります。しかし、リソースの動的配置やサービスの生滅が頻繁に生じるクラウド環境では、アクセス権管理・設定を正しく行うことが大きな運用負担となります。

この課題を解決するための基盤技術として、弊社は統合アクセス権管理技術を開発しています。その技術的な特長は以下の通りです。

(1) 権限管理で広く用いられるロールベースアクセス制御（RBAC:Role-Based Access Control）方式を拡張し、仮想マシン（VM）層からアプリケーション（AP）層までのアクセス権を統合的に管理

(2) ID管理・リソース管理と連携したアクセス権設定の自動化により、組織・リソース構成・サービスなどの変更に正しく対応

(3) アクセス権管理方式の標準化をDMTF（Distributed Management Task Force）に提案、国際標準として普及推進

本稿では、開発した技術の概要とその国際標準化提案について紹介します。

2. 統合アクセス権管理方式

2.1 統合アクセス権管理の必要性

仮想化によるサーバ統合環境は、リソース集約によるコスト削減の点で重要なクラウドインフラ基盤となります。そこではさまざまな利用者がリソースを安全に共有するため、不正アクセス・情報漏洩が起こらないようアクセス権管理を行うことが求められます。

従来のアクセス権管理では、業務アプリケーションの権限設定自動化、特定OSでのファイル共有など、ソフトウェア個別の対策を実現していますが、クラウドにおいては、マルチレイヤ・マルチベンダソフトウェアに対する統合的な権限管理を行う必要があります。その要件として、

・ VM、OSなどのソフトウェアレイヤごとの多様なアクセス対象（リソース）を統合した権限管理であること（マルチレイヤ対応）

・ 各レイヤにおいて、異なるソフトウェアへの権限設定が容易であること（マルチベンダ対応）

の2つが重要です。以下では、これらの課題を解決する統合アクセス権管理基盤について、詳しく紹介します。

2.2 統合アクセス権管理基盤（IAM）

IAM（Integrated Access control Manager）は、仮想サーバ上

のさまざまなソフトウェアのアクセス権を統合管理する基盤ソフトウェアです。

図1 に、その概要を示します。IAMは管理サーバに置かれ、統合ID管理機能と連携します。制御対象の仮想サーバにはエージェントが置かれ、IAMと通信します。IAMは次の3つの要素で構成されます。

(1) ポリシー生成

統合ID管理サーバから取得したロール（所属部署・職位などのユーザ属性）に対応するRBACアクセス権記述（RBACポリシー）を生成します。RBACポリシーは、ロール・リソース・リソース操作権の3つの要素で構成されており、国際標準XACML（eXtensible Access Control MarkupLanguage）形式でDBに格納されます。

(2) リソース管理

ポリシー生成に必要なリソース情報を管理します。制御対象サーバ上のエージェントから、ゲストVM・ファイル・テーブルなどのリソース情報を収集し、国際標準の管理モデルCIM（Common Information Model）に基づいた構造でDBに格納します[1)、2)]。更に、後述するリソースグループを管理するために、階層型リソース管理モデルを採用しています。

(3) ポリシー配付

RBACポリシーを、指定された仮想サーバ上のアクセス制御ソフトウェアに配付します。XACML形式のRBACポリシーは、配付前に各ソフトウェアの設定ファイル形式に自動変換され、エージェントを介して自動設定されます[3)]。

共通なRBACポリシーを、マルチレイヤ・マルチベンダのソフトウェア群に対して自動設定する技術は、弊社が世界で初めて開発しました。第3節、第4節では、その基盤となる技術を紹介します。

2.3 リソースグループによるRBACポリシーの簡易記述

従来のRBACポリシーでは、アクセス対象をファイルなどの細かい粒度で指定するため、サーバ統合環境では記述が大変煩雑になります。IAMでは、リソースグループを用いて複数のリソースに対するアクセス権を一括指定できるよう、RBACポリシーを拡張しています[2)、3)]。

また、アクセス対象リソースは、ゲストVM・ファイル・DBテーブルなど多様であり、しかも可能な操作が異なります。リソース管理では、さまざまな操作権限を共通な形式で表現できるようにCIMモデルを拡張し、これに基づきリソースと操作権限との関係を管理します。これにより、マルチレイヤ・マルチベンダソフトウェアに対応するポリシー記述が非常に簡易になります。

図2 にその例を示します。リソースグループと操作権限の形式の共通化により、例えば「経理課のメンバーだけ経理課文書を編集できる」「経理課管理者だけ経理課サーバを管理できる」といった抽象度の高いRBACポリシーを、設定対象のソフトウェアレイヤや種別を意識せずに作成できます。

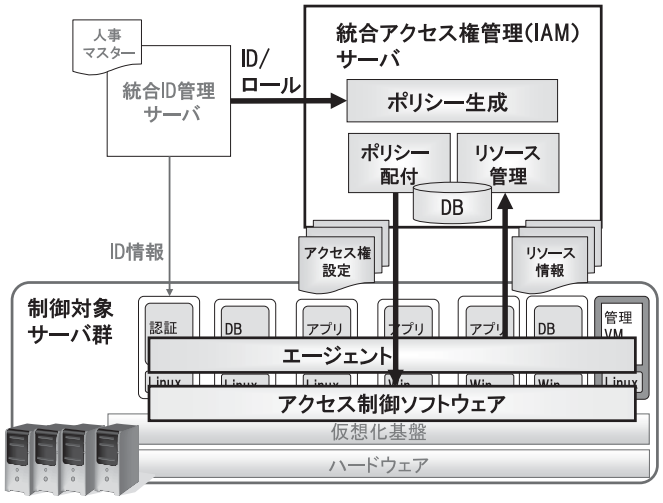

図1　統合アクセス権管理基盤

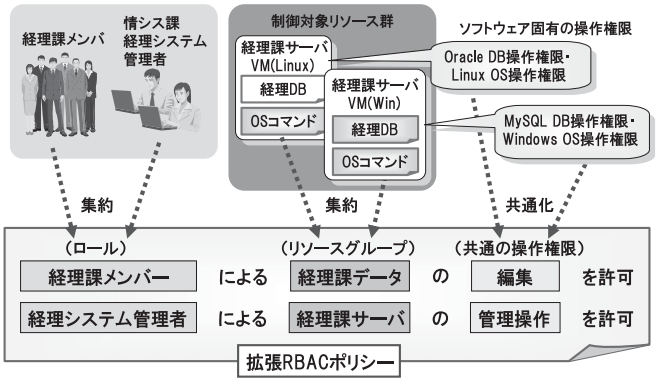

図2　リソースグループを用いたRBACポリシーの簡易記述

2.4 最新のID・リソース情報を反映するRBACポリシー自動設定

ポリシー生成で作成したRBACポリシーは、配付先の仮想サーバと配付スケジュールをGUIであらかじめ指定することで、配付・設定を自動的に行うことができます。このときの処理フローを **図3** に示します。

1) リソース管理機能からリソース情報を取得して、リソースグループに含まれる配付先仮想サーバを特定します。例えばポリシー生成後に仮想サーバがマイグレーションで移動したとしても、リソース管理DBが更新されることにより、正しい配付先が確定します。

2) RBACポリシーに記述されたロールを配付先仮想サーバのID/ロールに変換するために、統合ID管理機能に問い合わせてID/ロール情報を取得します。

3) 取得したID/ロール情報及びリソース情報を用いて、RBACポリシーを、配付先仮想サーバ上のソフトウェアに合わせた設定ファイル形式に変換します。 **図4** は、共通なRBACポリシーが配付先の設定ファイル形式に変換される様子のプレビュー画面です。このように、共通のRBACポリシーをもとに、最新情報に基づく設定ファイルが自動生成でき、更新不徹底や誤入力による不備が解消されます。

4) 変換されたファイルを、配付先仮想サーバ上のエージェントに配付し、個々のアクセス制御ソフトウェアに設定し

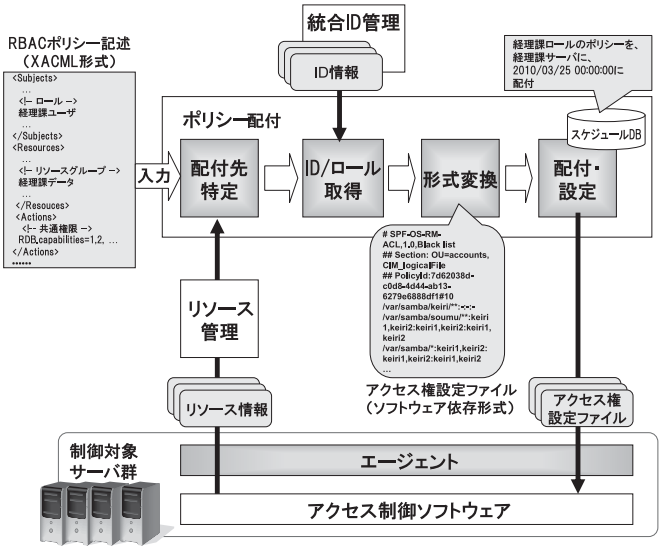

図3　ポリシー配付・設定の処理フロー

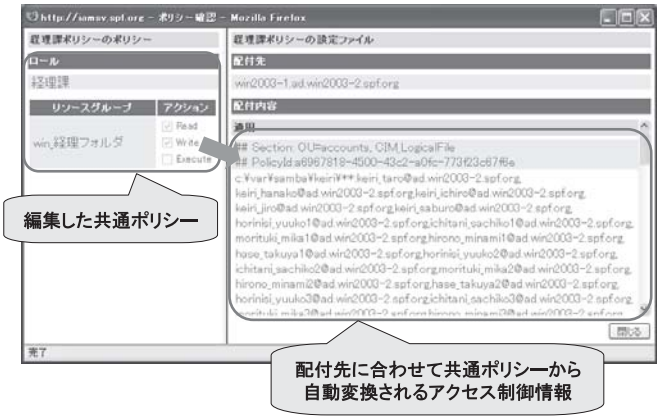

図4　設定ファイル形式変換のプレビュー画面

ます。このとき、定期保守などに合わせて配付スケジュールを指定することができます。

3. 統合アクセス権管理方式の実装と性能実証

IAMサーバはJava言語で実装しており、RedHat Enterprise Linux 5上での動作を確認しています。仮想化基盤ソフトウェアには、ゲストVM管理機能との連携が容易なXenを採用しています。エージェントとの通信には、運用管理プロトコルの国際標準であるWS-Managementを採用し、以下のソフトウェアに対するアダプタを開発することで、権限設定を自動化しています。

VM層：XenのゲストVM管理ソフト（libvirt）
OS層： Linux、Windows
DB層： MySQL、Oracle
AP層： ユーザAP向けアダプタ開発SDKを提供

開発したIAMサーバの有効性を検証するため、2009年11月から3カ月間実証実験を行いました。実験では、3,000人規模の企業において、人事・経理系業務システムを統合するケースを想定して、企業が実際に利用する業務サーバを仮想化した環境を構築し、模擬運用による管理コスト評価、及びスケーラビリティ性能評価を行いました。 **図5** に実証実験システムの概要を示します。本環境の規模は、以下のとおりです。

・ 物理サーバ数：6
（1Gbイーサネットで接続）

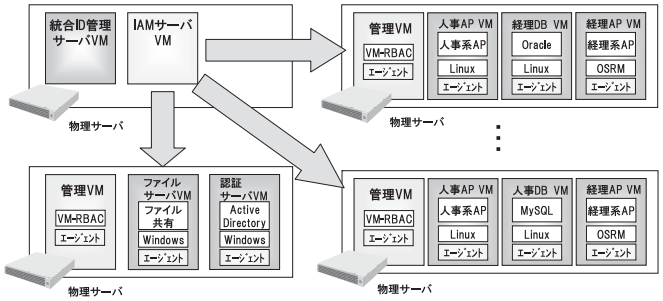

図5　実証実験システムの概要

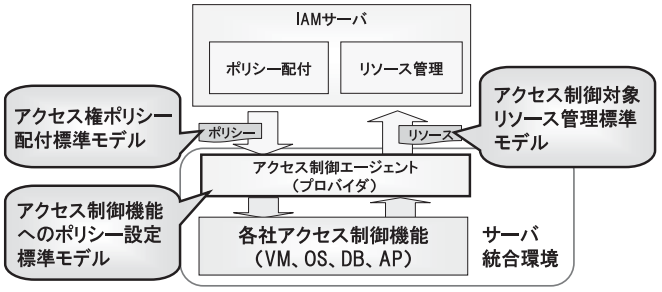

図6　DMTF標準化提案（IAMプロファイル）の概要

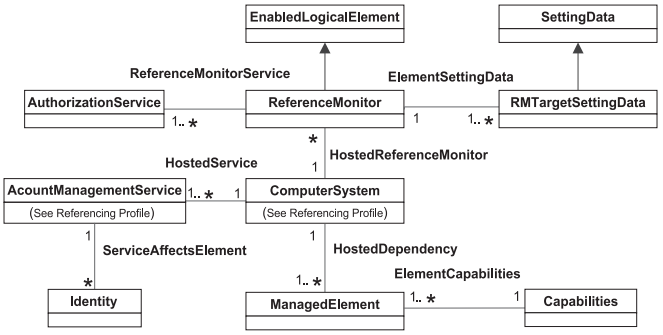

図7　IAMプロファイルで規定したクラス図（部分）

・ ゲストVM数：15
（業務AP・DBサーバ12、ファイルサーバ2、認証サーバ1）
・ 業務アプリケーション数：3
（人事系2、経理系1）

実証実験により、以下の結果が得られました。

(1) 権限管理コストが最大80%削減

仮想サーバ環境のシステム管理者変更に伴うID/アクセス権限の設定に要する作業時間を測定した結果、人手による従来方式と比べて最大80%削減できることを確認しました。削減率は、ゲストVM数が増加すれば更に高くなります。

(2) 10,000人規模の企業の業務システム権限管理に十分なスケーラビリティを確保

10,000ユーザ・200VM規模の業務サーバ統合環境において、ID/アクセス権の一括設定を定期保守時間内（～5時間）で実施できる性能であることを確認しました。

一方で、以下のような課題があることも確認しました。

・ 既存システム移行時の統合ノウハウが不十分
・ ロール設計・ポリシー設計が難しい

これらの課題に対しては、アダプタ開発SDKの強化、簡易な設計手法の確立、システム固有の権限管理との連携方式強化などを検討していきます。

4. 統合アクセス権管理方式の国際標準化

リソース管理方式において、マルチレイヤのアクセス権設定にかかわるソフトウェアの属性を新たに規定し、既存のCIMモデルを拡張することが不可欠となりました。

クラウドなどの大規模な仮想サーバ統合環境では、アクセス権の集中管理・一括設定にかかわるマルチベンダ製品の相互運用性が効率的運用に必須であると考えられます。そこで弊社は、IAMで採用したリソース管理方式・ポリシー配付方式を国際標準として普及させるため、マルチベンダシステム運用の標準化団体DMTFに提案を行いました。提案（IAMプロファイル）の概要を**図6**に示します。

図7に、IAMプロファイルにおいて拡張されたCIMモデルを表すクラス図を示します。図は、実装非依存のシステムモデル言語（UML）で表現されています。IAMプロファイルの中核をなすのが以下の2つの規定です。

・ アクセス権を設定したいソフトウェアのアクセス制御機能の定義（図7のReferenceMonitorクラス）
・ アクセス制御機能の対象リソースとそのリソース操作権限の定義（図7のRMTargetSettingDataクラス）

本提案はDMTFの承認を得て、2010年2月にWork in Progress（標準化予定版）として公開されました[4]。2010年中の標準化完了を目指して活動を継続していきます。DMTF標準化により、マルチベンダ環境でのアクセス権の集中管理・設定を容易に実現できます。

5. まとめ：クラウドサービス適用への課題

IAMにより、仮想サーバ統合環境での権限を統合的に管理し不正アクセスや情報漏洩を防ぐことができます。一方、IAMをクラウドサービスに適用するには課題もあります。

まず、VM層やAP層のソフトウェアだけでなく、ネットワーク層の管理が重要になります。物理・仮想ネットワークの管理操作にかかわるRBACポリシーに対応する必要があります。また、マルチテナントに対応した権限管理、不正アクセスや情報漏洩が起こった場合の責任の所在を明らかにする技術的な仕組みが重要になります。

今後は、このような課題を解決する統合アクセス権管理方式を開発し、特定の企業内で利用するプライベートクラウドだけでなく、不特定多数の企業が利用するパブリッククラウドにも適用可能とする予定です。

なお本研究の一部は、経済産業省から技術研究組合 超先端電子技術開発機構（ASET）へ委託された「平成19年度セキュア・プラットフォームプロジェクト」の成果です。

参考文献

1) K. Tadano, “Automatic Cache Update Control for Scalable Re - source Information Service with WS-Management”, DMTF SVM'09.
2) 但野, 「セキュア・プラットフォームの研究開発(3)リソース構成情報管理」, 情報科学技術フォーラム, 2009.
3) 森田, 「セキュア・プラットフォームの研究開発(2)アクセス制御ポリシー生成・配付」, 情報科学技術フォーラム, 2009.
4) DMTF DSP1106, “Integrated Access Control Policy Management”

執筆者プロフィール

小川 隆一
サービスプラットフォーム研究所
主幹研究員

前野 義晴
サービスプラットフォーム研究所
主任研究員

中江 政行
サービスプラットフォーム研究所
主任研究員