クラウドにおける統合権限管理アーキテクチャ

小川 隆一　　中江 政行　　山形 昌也

日本電気株式会社 サービスプラットフォーム研究所
211-8666　神奈川県川崎市中原区下沼部 1753
r-ogawa@jp.nec.com, m-nakae@bp.jp.nec.com, yamagata@da.jp.nec.com

あらまし 筆者らは，仮想サーバ上のマルチベンダーソフトウェアに対する統合アクセス権管理方式の開発，標準化を推進している．本方式をIaaS型クラウド環境に適用する場合，管理者権限(ロール)の統合，仮想サーバ・仮想ネットワークのモデル統合，クラウド運用標準化方式との整合，などの拡張が必要になる．本稿では，現行のクラウド運用におけるセキュリティ要件，ロール・リソース統合管理について，関連標準化団体の検討状況を述べる．またその結果をもとに，課題を整理し，クラウド環境における統合アクセス権管理方式のあるべき姿を検討する．

Integrated Authorization Management Architecture for Cloud Environment

Ryuichi OGAWA　　Masayuki NAKAE　　Masaya YAMAGATA

Service Platforms Research Laboratories, NEC Corporation
1753 Shimonumabe, Nakahara-ku, Kawasaki 211-8666, JAPAN
r-ogawa@jp.nec.com, m-nakae@bp.jp.nec.com, yamagata@da.jp.nec.com

Abstract The authors have been engaged in the development of integrated authorization management method for virtual servers and its standardization. In order to apply the method to cloud management, model integration for virtual server and virtual network resources, role integration among organizations, and adoption of cloud related standards would be major technical challenges. In this paper, based on our experience of development and standardization, we specify these technical challenges and discuss desirable architecture of authorization management for cloud environment.

1　はじめに

筆者らは，マルチベンダ仮想サーバ環境における統合アクセス制御方式IAM（Integrated Access Control）の研究開発、および、システム相互運用に関する標準化団体DMTF[1]における同方式の標準化を推進している[1][2][3].

IAM は，当初単一企業の仮想サーバシステムの権限管理方式として開発されたが，複数組織が混在するデータセンター/IaaS 型クラウドへの適用を考える場合，ネットワークに対応していないことが課題である．クラウド環境では，テナントごとの隔離性を高めるため，サーバ・ネットワークの仮想化は必然であり，それらの統合アク

[1] Distributed Management Task Force

セス制御は，安全性の担保・運用コスト削減のために必須である．

しかし，この統合は難度が高い．アクセス権管理でいえば，主体（ID）の統合は比較的容易だが，客体（アクセス対象リソース）の統合が容易でない．例えば，サーバ仮想化とネットワーク仮想化は独立に開発され，リソースモデルも個々に最適化されてきた．また，サーバに比べネットワークの構成自由度が高く，ネットワークの抽象化モデルはデファクトといえるものがない．クラウドの普及により，関連標準化団体がようやくモデル統合の検討に着手した段階である．

本稿では，IAM のクラウド適用を事例として，クラウドにおける統合アクセス権管理方式のあるべき姿を検討する．2 章では，IAM の概要と拡張課題について述べる．3 章では，現在議論されているクラウドセキュリティ要件を概観し，統制ルール（アクセスポリシー）実施に関連するクラウド標準化の状況を述べる．最後に 4 章で，これらをふまえた統合権限管理方式のアーキテクチャについて検討する．

2　IAMの概要と拡張

2.1　IAMの概要

IAM は，RBAC（Role Based Access Control）ポリシー[4]の一元管理とその形式自動変換・自動配付により，組織の仮想サーバ群のアクセス権設定を一括して行う方式である．**図1**に動作概要を示す．

図でリソース管理部は，エージェントを介して設定対象資源の属性データ収集・管理を行う．ポリシー管理部は，RBAC 形式のポリシーを制御対象資源のフォーマットに変換して配付する．

IAM では，複数リソースを集約する「リソースグループ」とその「抽象操作」を記述できるようにした拡張 RBAC ポリシー[1]を用いる．これにより，例えば「人事データを編集する」という高い抽象度でアクセス権を記述できる．ポリシー管理部では，「人事データ」は「人事テーブル名」，「編集」は「update, insert, 」といった個々の操作名に置換した ACL を生成し，エージェント経由で設定対象ソフトウェアに配付する．

エージェントは，対象ソフトウェアごとに固有のアダプタを必要とする．多様なソフトウェアへの設定を容易にするため，筆者らはポリシー配付およびアダプタの仕様を，国際標準の情報管理モデルCIM[2][5]で規定し，DMTFに提案を行っている．提案は 2011 年末に標準として認定される予定である．

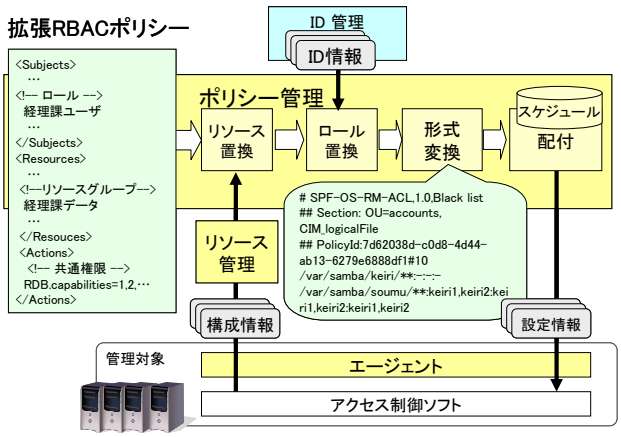

図1　IAM の動作

2.2　リソースモデルの制約

前節のとおり，IAM では拡張 RBAC ポリシー配付時に

1）ロール⇒ID

2）リソースグループ名⇒個別リソース名

3）抽象操作名⇒個別操作名

の名前解決処理を行う．1）の処理は，ID 管理機能との連携により実現する．

一方2）3）の処理のため，リソース管理部では CIM 準拠のスキーマで情報を管理している．しかし，現在の CIM は計算機のモデル化を指向しており，ネットワークについて十分対応していない．例えば VLAN 等の仮想ネットワークや，ルータ等の中継ノードのモデル化は未対応である．

[2] Common Information Model

3　クラウドセキュリティと標準化

3.1　クラウドセキュリティ要件

本節ではまず，IAM のアクセス権配付機能が，クラウドセキュリティ要件の中にどう位置づけられるかを確認する．クラウドに対するセキュリティの要件は様々な団体で検討が進み，ガイドラインが公開されている．主なものを**表1**に示す．

表1　クラウドセキュリティガイドライン

団体	仕様	内容	ステータス
NIST	Guidelines on Cloud Security and Privacy in Public Cloud Computing	パブリッククラウド向けのクラウドセキュリティガイドライン規定（主要9トピック）	ドラフト公開
CSA	Security Guidance For Critical Areas of Focus in Cloud Computing	クラウドセキュリティ・コンプライアンスの主要13トピック（ドメイン）に関するガイダンス	Ver.2.1リリース Ver.3.策定中
CSA	Cloud Control Matrix	セキュリティ・リスク分析・コンプライアンスを統合したクラウド統制フレームワーク（ISO 27001/27002等の既存標準とマップ）	Ver.1.1 リリース
OASIS	Identity in the Cloud Use Cases	クラウドID管理のユースケース規定	Ver.1.0 策定中

例えばCSA[3]は，セキュリティ要件を統制・運用，の 2 カテゴリで大別し，整理する．統制は，クラウド環境での利用者ガバナンスを維持するため，運用と同様に重視される．運用は通常のセキュリティ施策（ID管理，隔離，監視，データ管理等）だが，クラウドらしく仮想化対策が特記される．

最も網羅的な仕様は CSA の Cloud Control Matrix（CCM）[6] だが，項目数が膨大（約 100 項目）であり，かなりの管理者負担が懸念される．このためクラウドプラットフォームの支援が必須となるが，IAM を適用すれば，アクセス権に関する統制ルールを拡張 RBAC ポリシーで共通化し，アクセス権設定を自動化することで，統制・運用コスト削減に貢献できる．

次節では，現行クラウドにおいて共有な RBAC ポリシーの徹底がどの程度可能か，プラットフォーム側の対応を見ていく．

[3] Cloud Security Alliance

3.2　クラウド特権管理におけるロール

統制主体（ID/ロール）の統合についてみてみると，ID 統合は SAML 等の連携機構で実現されている．しかし，ロールの統合は課題がある．

ロール統合（ありるいはクラウド間共通化）は，特権管理で重要である．クラウド間で相互運用可能な特権ロールを定義できれば，クラウド A の業務をクラウド B でも実施する場合，A，B ともに共通なロールで統制ができる．しかし，ロール定義は一般に，業務依存・組織依存の面が強く，共通語彙策定に非常な手間がかかると予想される．

これを推進する団体は現時点で見当たらない．例えば**表1**の OASIS は，クラウドにおける ID 管理ユースケースを策定している[7]が，ID 統合の例のみがまとめられている．

3.3　リソースモデルの統合

統制対象（リソース）の統合については，クラウド標準化団体の動向をもとに説明する．

3.3.1　クラウド標準化活動の俯瞰

図2に関連標準化団体（IT系，NW系，De jure 系に分類）の活動の相関を示す．このうち，リソース管理に最も関係するのがIT系のDMTF（システム運用管理），OGF/OCCI[4]（オープンクラウドAPI策定），SNIA[5]（ストレージ管理）である．

DMTFは，仮想マシンイメージの共通フォーマットOVF[6][8]をいち早くクラウド標準として提案，ISOに認定された．さらに，インターオペラブルなクラウド管理APIを策定中で，関連する情報モデル・プロトコルをOCCI，SNIAが実装する，という役割分担が合意されている．

[4] Open Grid Forum/Open Cloud Computing Interface
[5] Storage Networking Industry Association
[6] Open Virtualization Format

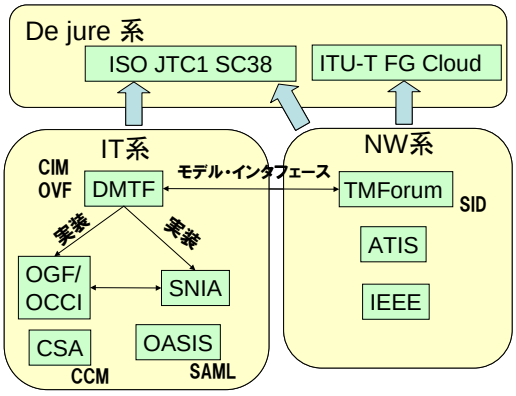

図2 クラウド関連標準化活動の相関

NW系では，TMForum[7]がキャリアクラウドサービス構築・運用の標準化を推進しており，独自の情報モデルSID[8][9]を策定している．またDMTFとリエゾンし，SIDとCIMの整合を試みている(後述)．

この他，セキュリティガイドライン策定で CSA がリエゾンし，各団体の提案整理，de jure 化を ISO，ITU-T が担う構図となっている．

3.3.2 DMTFのクラウド管理API

DMTFは 2010 年より，クラウド管理API策定の活動を開始した[10][11]．このインタフェースは，クラウドプロバイダ・デベロッパー・クラウドユーザ間のインターオペラブルなリソース操作を規定するもので，セキュリティ視点からみると，クラウドユーザ・プロバイダ間の (1)ID情報/鍵情報 [9]，(2)ポリシー，(3)ログ・監査情報 の交換がなされる予定である．

DMTF では，CIM に準拠した基盤(例えば CIM プロトコルを備えた Windows，Linux)上のクラウドオーケストレーションソフトウェアが，上記 API を持つ，というアーキテキクチャを想定している(**図3**参照)．

しかし，下位プロトコルまで CIM 準拠で実装，というのは強い制約である．筆者らは，下位プロトコルが必ずしも CIM 準拠でない，例えばOSS系クラウドをたばねた管理ポータルとしても，上記 API は活用されると考えている．

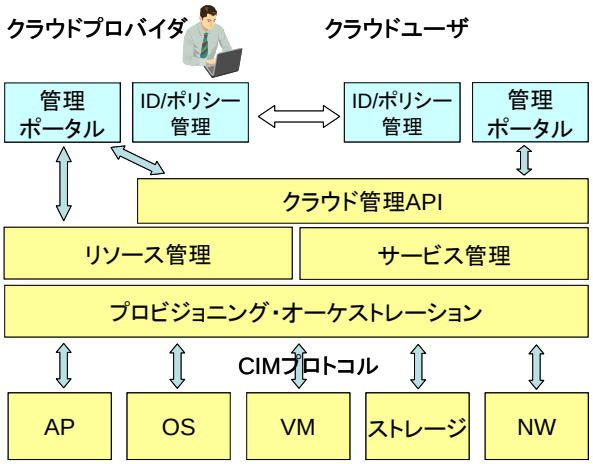

図3 クラウド管理 API の適用イメージ

3.3.3 クラウド管理モデル

DMTF Cloud Management WG では，クラウド管理 API の基盤となるクラウド管理モデル策定を進めている．

1) 管理ユースケース

ユースケースとして，クラウドサービスライフサイクル管理で必須となる最小ケース(契約，ディプロイ，運用，資源解放など)が選定された．筆者らはセキュリティプロビジョニングをケースに含めるよう提案したが，ケース最小化のため，第一版では見送られた．

2) クラウド管理モデル

ユースケースに基づき，管理対象リソースのモデル化を行っている．**図4**にE-R図による暫定仕様を示す．図には、仮想マシン(VM)・仮想ストレージ・仮想ネットワークの各クラス，SLAのためのログクラス・計測クラスが含まれるが、DMTFがVM管理標準(VMAN[10])[12]を先に策定した経緯から，VMを主体とするモデル化となっている．

このためネットワークについては，VM とネットワークの接続ノード(仮想スイッチ)をまず規定し、ネットワーク自体の記述は拡張の余地を残している．最近、新しい通信制御方式

[7] TeleManagement Forum
[8] Shared Information and Data model
[9] ID 連携は別途既存方式を利用する．
[10] Virtualization Management

OpenFlow[13][14]が DMTF に提案されたが，こうした仮想ネットワークモデルの自由度を考慮する必要がある．

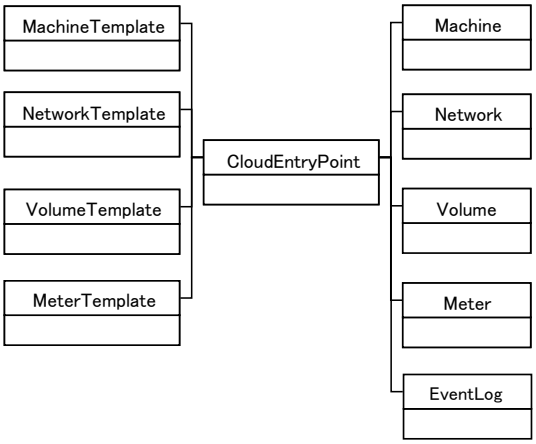

図4　クラウド管理モデル（暫定版，部分）

3）今後の見通し

クラウド管理 API は，デファクトのクラウド API に比べ，インターオペラブルな操作のためのモデル（CIM）を必要とする．しかし，モデルの正確さを追求すると API の理解が困難になる，との懸念から，2011 年 8 月時点で CIM 準拠性の議論が決着していない．Cloud Management WG では，クラウド管理モデル第一版を至急確定させる予定である．

3.3.4　TMForumの情報モデル

TMForum はキャリアを中心とする業界団体で，キャリアクラウドサービス構築の標準化を推進している．サービス指向が強く，ビジネスプロセス・アプリケーションフレームワーク，その基盤となる情報モデル SID の標準化を行っている．

SID はサービス指向を反映して，市場・顧客・サービスからリソースにいたる幅広いエンティティを階層的にモデル化している（**図5**参照）．リソースについては，CIM のような詳細なモデルはなく，記述粒度は大きい．

DMTF と TMForum は同じゴールを目指す分野（モデル，操作インタフェース，構成管理 DB，計測等）で連携の検討を開始している．CIM と SID の整合は重要課題であるが，モデルのセマンティクス・記述力のギャップが大きいため，まずユースケース・語彙の共有から検討を開始している．

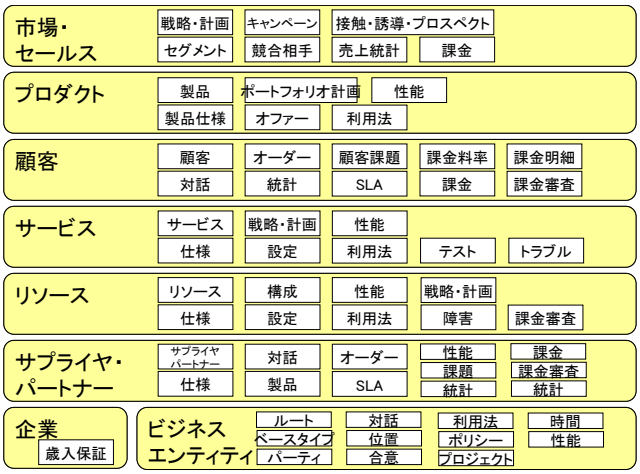

図5　SID の記述階層

4　統合権限管理アーキテクチャ

図3のクラウド管理アーキテクチャに，IAM を適用した統合権限管理アーキテクチャの概念を**図6**に示す．IAM は ID 管理と並んでオーケストレーションソフトウェアの外にあり，クラウド管理 API 経由でアクセス権情報が自動設定される．これとは別に，クラウドのリソース管理部と IAM のインタフェースが規定される．

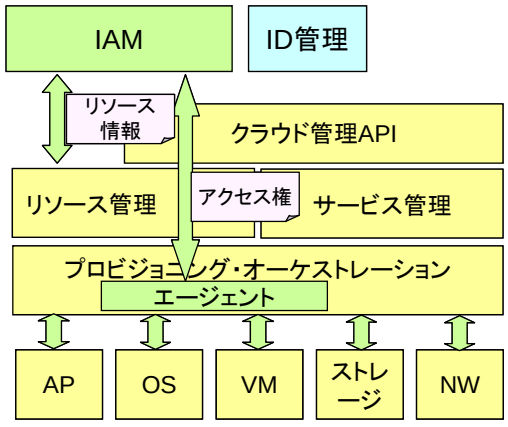

図6　IAM による統合アクセス権管理

しかし，3章の議論から，クラウド間のロール統合，仮想マシン・仮想ネットワークのモデル統合がともに容易でないことがわかった．上記ア

ーキテクチャの実現には，モデル拡張に加え，プラットフォームの柔軟な対応が必要である．

現在筆者らは IAM のクラウド適用について，以下のようなアプローチを検討中である．

1）ロール統合では，SID/CIM のモデル階層に準拠した管理範囲をロールとすることで，クラウド間の特権ロールの共通化を図る．

2）仮想ネットワークモデルの自由度が大きいため，「仮想ネットワーク」というリソースグループ定義に柔軟性を持たせる．例えば，サーバ・端末などのエンドノードの情報を必須要素とし，中継ノードの構成をオプションとすることで，中継ノード情報が不要な OpenFlow，必要な VLAN などのレガシーネットワークに対応する．

これは，RBAC ポリシー・CIM 準拠という基盤は変えず，管理ロールとリソースモデルとのバインド，リソースグループ記述の柔軟化でモデル統合の困難をカバーするアプローチと言える．

5　おわりに

本稿では，仮想サーバ統合環境における統合アクセス権管理方式（IAM）のクラウド適用について議論した．ロール統合・リソースモデル統合の課題について，クラウド標準化団体の検討状況を吟味し，RBAC ポリシー実施・CIM 準拠を基盤とする統合アクセス権管理アーキテクチャの参照モデルを策定した．また，モデル統合の困難をプラットフォームの柔軟化で補うアプローチを検討した．

これに基づき筆者らは，IAM によるネットワークアクセス制御の試験実装を行っている．結果については別途報告したい．

参考文献

[1] 小川隆一,中江政行，前野義晴，森田陽一郎，町田文雄，但野紅美子，“仮想サーバ統合環境におけるアクセスポリシー管理方式,” 電子情報通信学会技術研究報告 110(114), pp. 93-100, 2010.

[2] F. Machida, K, Tadano et al., “CIM-based Resource Information Management for Integrated Access Control Manager,” in Proceedings of DMTF SVM08, October 2008.

[3] DMTF DSP1106, “Integrated Access Control Policy Management Profile 1.0.0,” February 2010.

[4] R. S. Sandhu et al., “Role-based access control models,” Computer, vol. 29, no. 2, pp. 38-47, 1996.

[5] Common Information Model (CIM) Standards, http://www.dmtf.org/standards/cim/

[6] Cloud Control Matrix (CCM), https://cloudsecurityalliance.org/research/projects/cloud-controls-matrix-ccm/

[7] OASIS Identity in the Cloud TC, http://www.oasis-open.org/committees/id-cloud/

[8] DMTF DSP0243, “Open Virtualization Format Specification 1.1.0,” January 2010.

[9] Information Framework (SID), http://www.tmforum.org/BestPracticesStandards/InformationFramework/1684/Home.html

[10] DMTF DSP-IS0102, “Architecture for Managing Clouds 1.0.0,” June 2010.

[11] DMTF DSP-IS0103, “Use Cases and Interactions for Managing Clouds 1.0.0,” June 2010.

[12] DMTF DSP2013, “CIM System Virtualization Model White Paper,” November 2007.

[13] 西原基夫，岩田淳，矢野由紀子，“OpenFlow 技術の概要,” 情報処理 51(8), pp. 1023-1029, 2010.

[14] N. McKeown et al., “OpenFlow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, 38(2), pp. 69-74, April 2008.