2B-7

統合アクセス制御モデルの標準化について

芦野 佑樹† 中江 政行† 小川 隆一†
†日本電気株式会社 サービスプラットフォーム研究所

1. はじめに

筆者らは、複数のマルチレイヤ・マルチベンダのソフトウェアが稼働するサーバ統合環境に対するアクセス制御設定（アクセスポリシー）の統合管理基盤（IAM: Integrated Access Control Manager）を開発している[1]。IAM は、ゲスト VM・ファイル・DB テーブルなどの制御対象リソースの操作権限などが記載されたリソース情報を設定対象サーバから収集し、当該情報に応じて共通形式で書かれたアクセスポリシーを、対象依存のアクセス制御リスト（ACL）に自動変換・配付することで、多様なソフトウェアでアクセス制御を一括して実施できる。

こうした統合アクセス制御方式の実現には、ソフトウェアベンダの対応も不可欠となることから、筆者らは上記リソース情報収集・ACL 配付に関する管理モデル（統合アクセス制御モデル）を、国際標準化団体 DMTF（Distributed Management Task Force）[2]で標準化している。本稿では、提案中の統合アクセス制御モデル[3]とその標準化活動状況について報告する。

2. 統合アクセス制御モデル

2.1 統合アクセス制御とは

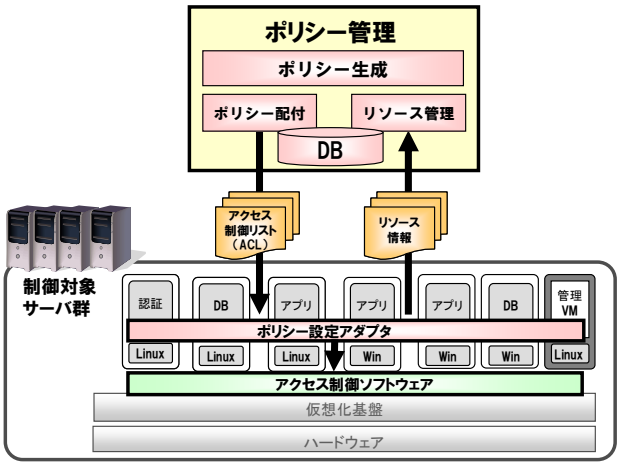

図 1 統合アクセス制御の概要

IAM とは、制御対象サーバ群上に存在するゲスト VM、OS（ファイルシステム）、DB などのソフトウェアに対して統合的にアクセス制御の管理を一括して行うシステムである。IAM では、大きく分けてリソース管理とポリシー配付の二つの機能によって構成されている（図１）。リソース管理機能は、ポリシー設定アダプタによってリソース情報の収集や管理を行う。たとえば、DB ソフトウェアのリソース情報には、DB テーブル名やテーブル操作権（select/update 等）の一覧が含まれる。ポリシー配付機能は、リソース情報を基にアクセスポリシーを制御対象依存の設定情報へ自動変換してポリシー設定アダプタに配付・実施を指示する。

ここでアクセスポリシーは、たとえば「人事データを編集してよい」という抽象度で記述されており、配付時に「人事データ」は人事テーブル名に、「編集」は「update, insert, ...」といった DB 操作権などで表現された ACL に変換され、DB 用ポリシー設定アダプタを介して設定対象 DB ソフトウェアに設定される[1]。

これまでに筆者らは Xen 仮想化ソフトウェアや Windows OS 向けのアダプタを開発ずみであるが、さらに多様なソフトウェアに対応するために、アダプタ仕様を国際標準として公開することが有効であると考えた。そこで、次節に示す統合アクセス制御モデルを設計し、DTMF に標準化提案を行った。

2.2 提案モデル

統合アクセス制御モデルは、リソース管理およびポリシー配付・実施に必要な管理情報をモデル化したものであり、ポリシー設定アダプタのデータ仕様・API 仕様に相当する。以下に、提案モデルを概説する。

(1) リソース管理

ポリシー設定アダプタは、以下のようなリソース情報を提供するものと定義した。

(a) アクセス制御ソフトウェアが扱うアカウントの種類とリソースの種類
(b) アクセス制御ソフトウェアが制御する操作権
(c) 操作対象リソース ID の列挙

図２に OS のファイルアクセス制御に関するモデルを示す。これにより、アクセス主体がユーザ ID であり、アクセス対象がファイルである、

Standardization and Open Source Implementation of Integrated Access Control Policy Management
† Service Platforms Research Labs., NEC Corporation
Yuki Ashino, Masayuki Nakae, Ryuichi Ogawa

というファイルアクセス制御ソフトウェアの属性情報が収集できる。

また、全てのファイル・ディレクトリはファイルオブジェクトとしてモデル化され、これを介してパス名などの属性情報が収集できる。

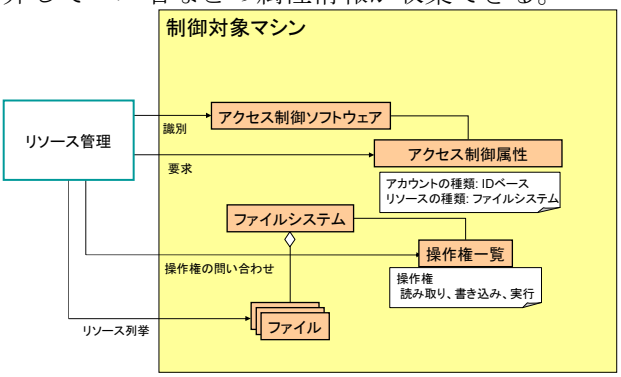

図２　リソース管理モデル

(2)　ポリシー配付と実施

ポリシー設定アダプタには、ACL の配付および実施するために、次にあげるインタフェースを持つと定義した。

(a) ACL の配付先 URL の応答

(b) ACL の格納場所（リポジトリ）に対応するアクセスポリシーグループ（APG）

(c) 配付された ACL の実行受け付け

図３の例において、ポリシー管理は、まず ACL の配付先 URL を制御対象マシンのポリシー転送先情報に問い合わせる。ポリシー管理は、FTP 経由で ACL を送付し、ポリシー適用サービスに ACL の実行要求を行う。送られた ACL は、ポリシー適用サービスによってポリシーオブジェクトとして扱われ、APG に登録される。ポリシー適用サービスは、ポリシー管理の要求に従って、アクセス制御ソフトウェアに対して ACL の実施要求を行い、アクセス制御を実施する。

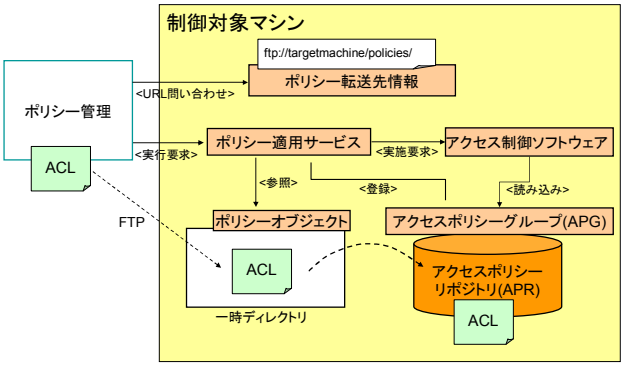

図３　ポリシー配付 CIM モデル

3. 標準化活動

アクセス制御モデルの標準化について、筆者らは DMTF ポリシー作業部会を中心に提案を行っている。これまでに提案文書（IAM プロファイル）の Work in Progress 版[3]が一般に公開され、現在 DMTF メンバによるレビューを経て、モデル改訂をほぼ終えた段階にある。

今後、本モデルが正式採択されるには、改訂版文書の DMTF 承認に加えて、提案者以外の第三者によるモデル実装も求められる。そこで、兼ねてから本提案に関心を示していた韓国 ETRI（Electronics and Telecommunications Research Institute）と連携し、提案モデルの Linux 向け試験実装および IAM 接続実験を実施した。本実験では、筆者らが開発した IAM サーバと、ETRI が開発したポリシー設定アダプタとを、図４に示す構成で接続し、Linux ファイルシステムの ACL（POSIX1.e ACL）が正しく行えることを確認した。

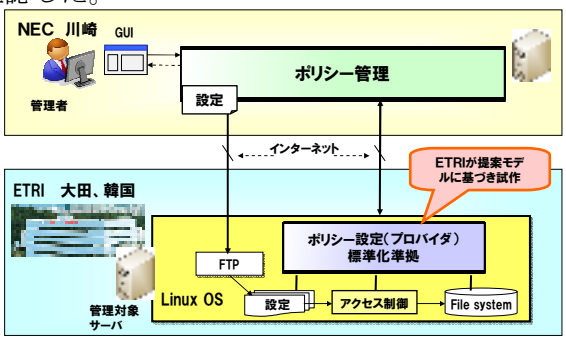

図４　ETRI との実証実験システム構成

4. まとめ

筆者らは、大規模で複雑化するシステムに対して一括してアクセスポリシーを管理する IAM を開発した。さらに、様々なベンダのソフトウェアに対応するためのアダプタ仕様である統合アクセス制御モデルを設計、国際標準化団体 DMTF に提案している。また、ETRI による Linux 向け試験実装を実施し、筆者らが開発した IAM との接続を確認した。この第三者実装により、正式採択に向けた標準化活動の加速が期待できる。

参考文献

[1] 小川 隆一ほか, “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] Distributed Management Task Force, http://www.dmtf.org/

[3] DSP1106, Integrated Access Control Policy Management Profile, 1.0.0.