L-025

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
Research and development of Secure Platform (2) Access control policy composition and distribution to server consolidated environment

森田 陽一郎† 中江 政行† 小川 隆一†
Yoichiro MORITA Masayuki NAKAE Ryuichi OGAWA

1. はじめに

企業における組織ルール遵守の徹底のためには，IT システムに対しても一貫したルールの適用が必要となる．そのため，IT システム，特に近年急速に普及が進んでいる仮想化機構を用いて統合されたサーバシステムについて，サーバシステム内に存在する多様なアクセス制御実施機能に対する一元的な管理機能の重要性が増している．そこで，セキュア・プラットフォーム[1]の研究開発では，仮想化機構を用いて統合されたサーバシステムにおける各レイヤ (VM，OS，ミドルウェア，アプリケーション) のアクセス制御実施機能に対して，一元的にアクセス制御ポリシーを管理する，統合アクセス制御情報管理を開発した． 統合アクセス制御情報管理は，アクセス制御ポリシー生成，アクセス制御ポリシー配付，リソース構成情報管理[2]の 3 つの機能で構成される． 本論文では，このうち，所属部門や職務などの組織内での役割 (ロール) に基づくアクセス制御ポリシー (RBAC[3]ポリシー) を生成するアクセス制御ポリシー生成と，RBAC ポリシーに基づいて各サーバや各レイヤのアクセス制御実施機能に適用するアクセス制御設定情報を導出して配付するアクセス制御ポリシー配付について述べる．

2. 統合アクセス制御情報管理の要件

企業全体で守るべきルールを組織の隅々まで徹底するため，仮想化機構を含めたサーバシステム全体にアクセス制御ポリシーを徹底する必要がある．

しかし，企業のサーバシステムには，Windows サーバや Linux サーバなど多様なサーバが複数存在する． また，ミドルウェアやアプリケーションといったレイヤ毎にも，多様なソフトウェアを利用している． そのため，各サーバや各レイヤは，固有のアクセス制御実施機能を持ち，入力するアクセス制御設定情報の書式や，アクセス制御対象のサブジェクト，リソース，アクションに違いがある． 例えば，同じファイルをリソースとするアクセス制御でも，Windows と Linux などサーバの種類が異なると書式に違いがある． OS と仮想化機構などレイヤが異なればリソースの種類 (ファイルとゲスト VM など) が異なり，リソースの違いに伴ってアクション (ファイルの Read や Write，ゲスト VM の start や shutdown など) も異なる． また，様々な認証機構 (/etc/passwd や LDAP サーバなど) を利用しており，同一の人物や組織からのアクセスを制御する場合であっても，サブジェクトの種類 (OS のアカウントと LDAP の特定の属性など) が異なる．

したがって，サーバシステム全体に対してアクセス制御ポリシーを徹底する統合アクセス制御情報管理を実現するためには，次の要件を満たす必要がある．

† 日本電気株式会社 共通基盤ソフトウェア研究所
Common Platform Software Res. Labs., NEC Corporation

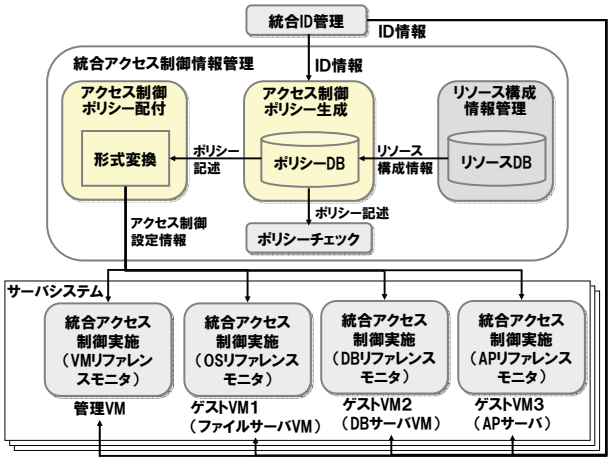

図 1: 統合アクセス制御情報管理の構成

① 多様なサーバ（ゲスト VM）への対応
各サーバの同じレイヤのアクセス制御実施機能に対して，サーバの種類に依存しない共通形式のアクセス制御ポリシーを生成・配付する．

② 多様なレイヤへの対応
各レイヤ (VM，OS，ミドルウェア，アプリケーション) のアクセス制御実施機能に対して，リソースやアクションの種類に依存しない共通形式のアクセス制御ポリシーを生成・配付する．

③ 多様なサブジェクトへの対応
各サーバや各レイヤのアクセス制御実施機能に対して，それらが利用する認証機構やサブジェクトの種類に依存しない共通形式のアクセス制御ポリシーを生成・配付する． 特に，組織ルールで扱われる部門や職務などのロールを単位とした共通形式のアクセス制御ポリシーを生成・配付することが求められる．

3. アクセス制御ポリシー生成・配付の機能

3.1. システム構成

統合アクセス制御情報管理 (図 1) は，アクセス制御ポリシー生成・配付に関し，2章の要件を実現するため，以下の 2 つの機能と，2 つの連携インタフェースを持つ．

- アクセス制御ポリシー生成
  各サーバや各レイヤのリソースを，種類毎に抽象化・グループ化し，リソースグループを生成する． その上で，ロール毎にリソースグループとアクションの組を複数列挙した RBAC ポリシーを，アクセス制御実施機能に依存しない共通形式で生成する．
- アクセス制御ポリシー配付
  アクセス制御ポリシーの配付先となるアクセス制御実施機能を特定し，共通形式のアクセス制御ポリシーを，

配付先のアクセス制御実施機能に固有のアクセス制御設定情報に形式変換して配付する．

- **統合 ID 管理との連携インタフェース**
  統合 ID 管理と連携し，ロールのリスト，ロールと個々の認証機構の扱うサブジェクトとの対応関係などの，ID 情報を取得する．
- **リソース構成情報管理との連携インタフェース**
  リソース構成情報管理と連携し，サーバシステム内の，アクセス制御対象のリソース (ゲスト VM，ファイル，DB テーブル，Web アプリケーション機能など)，リソースに対応するアクション，アクセス制御実施機能などの，リソース構成情報を取得する． アクセス制御実施機能については，名称，利用する認証機構，対象とするサブジェクトやリソースの種類などの情報を取得する．

3.2.アクセス制御ポリシー生成

アクセス制御ポリシー生成では，以下の機能によって，要件を満たしたアクセス制御ポリシーの生成を実現する．

① **リソースの抽象化とグループ化**
各サーバのリソースを抽象化し，同種のリソース，例えばファイルのリソースであれば，Windows のファイルであっても，Linux のファイルであっても同じものとして扱える． また，同種のリソースの中で任意にグループ化を行い，異なるサーバに跨ったリソースグループを生成できる． このリソースグループを用いて，サーバの種類に依存しないアクセス制御ポリシーの生成を実現する．

② **リソースグループによるアクションの抽象化**
ある 1 つのリソースグループは抽象化された同種のリソースで構成されるため，リソースに対応するアクションもリソースグループ毎に 1 種類に抽象化できる．これを利用して，異なるレイヤのリソースグループとアクションの組を 1 つのアクセス制御ポリシーの中で共通の方法で扱える． これにより，各レイヤのリソースやアクションの種類に依存しないアクセス制御ポリシーの生成を実現する．

③ **ロールによるサブジェクトの抽象化**
RBAC ポリシーに対応し，ロールをアクセス制御の単位とするため，ロールを持つ個々の人物が誰か，それらの人物が各サーバにどのようなアカウントを持つかなどを意識することなく，組織ルールで扱われる部門や職務などを，そのままアクセス制御ポリシーのサブジェクトとして扱える． これにより，個々のアクセス制御実施機能の対象とするサブジェクトの種類に依存しないアクセス制御ポリシーの生成を実現する．

3.3.アクセス制御ポリシー配付

アクセス制御ポリシー配付では，以下の機能によって，要件を満たしたアクセス制御ポリシーの配付を実現する．

① **アクセス制御設定情報の書式への変換**
アクセス制御ポリシーから，個々のアクセス制御実施機能に配付するアクセス制御設定情報への形式変換を行う際，アクセス制御ポリシーは，アクセス制御実施機能の種類に依存しない共通形式で記述されているが，アクセス制御設定情報は，同じレイヤのリソース (例えばファイル) を扱うアクセス制御実施機能であっても，その種類によって書式が異なる． この差異を吸収するため，個々のアクセス制御実施機能に対応するプラグインの形で，書式変換手順を追加する機能を持つ． 各プラグインをアクセス制御実施機能の名称と対応付けることで，配付先のアクセス制御実施機能毎に適切な手順を選択する． これにより，サーバの種類に依存しないアクセス制御ポリシーの配付を実現する．

② **リソースグループからリソースへの展開**
異なるレイヤのアクセス制御実施機能には，異なる種類のリソースやアクションについて記述したアクセス制御設定情報を配付するが，アクセス制御設定情報の元となるアクセス制御ポリシーは，リソースグループを用いてリソースやアクションの種類に依存しない共通形式で記述されている． そこで，形式変換を行う際に，アクセス制御実施機能の対象とするリソースの種類に合わせて，リソースグループから個々のリソースへの展開処理を切り替える． これにより，リソースやアクションの種類に依存しないアクセス制御ポリシーの配付を実現する．

③ **ロールからサブジェクトへの展開**
アクセス制御実施機能が利用する認証機構やサブジェクトの種類が異なる場合，配付するアクセス制御設定情報に記述されるサブジェクトの種類が異なるが，アクセス制御設定情報の元となるアクセス制御ポリシーは，ロールを用いてサブジェクトの種類に依存しない共通形式のポリシーで記載されている． そこで，形式変換を行う際に，アクセス制御実施機能の対象とするサブジェクトの種類に合わせて，ロールから個々のサブジェクトへの展開処理を切り替える． これにより，サブジェクトの種類に依存しないアクセス制御ポリシーの配付を実現する．

4. おわりに

統合アクセス制御情報管理について，多様なサーバ・レイヤ・サブジェクトへの対応が要件であることを述べ，リソースグループ・形式変換などを特徴とするアクセス制御ポリシー生成・配付の機能が，これらの要件を満たすことを示した．

謝辞

本研究は，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) へ委託されている「平成 19 年度セキュア・プラットフォームプロジェクト」の成果である．

参考文献

[1]徳谷崇，畠山高久，相澤泰介，栗田享佳，五十嵐功，小川隆一，小谷野修, "セキュア・プラットフォームの研究開発（１） アーキテクチャ", FIT2009, Sep 2009.

[2]但野紅美子, 町田文雄, 川戸正裕, 前野義晴, "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", FIT2009, Sep 2009.

[3]Ravi Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, "Role-Based Access Control Models," IEEE Computer, v. 29, n. 2, pp. 38-47, Feb 1996.