L-024

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

Research and development of Secure Platform (1) Architecture Overview

徳谷 崇†, 畠山 高久†, 相澤 泰介†, 栗田享佳†, 五十嵐 功†,
Takashi Tokutani, Takahisa Hatakeyama, Taisuke Aizawa, Takayoshi Kurita, Isao Igarashi,
小川 隆一‡, 小谷野 修＊
Ryuichi Ogawa, Osamu Koyano

1. まえがき

セキュア・プラットフォーム[1]は，異種混合サーバを仮想化し統合した環境におけるシステム全体の信頼性，性能及びセキュリティを強化する基盤技術である．

本論文では，サーバ仮想化・統合により集約された環境において，仮想化サーバを跨いで統合的にアクセス制御を実現するセキュア・プラットフォームのアーキテクチャを紹介する．

2．背景

J-SOX 法対応で，企業の内部統制監査報告が始まった．

内部統制に必要な IT ガバナンスを強化するためには，機密情報保護などの統制ルール（組織ルール）を企業システム全体で遵守徹底することが不可欠である．しかし，実際に統制ルールを遵守する仕組みを取り入れ，継続して遵守徹底するには，人件費を主とする膨大なコストがかかる．

このため，統制ルール遵守の見える化と，徹底の人手を主とする仕組みを，IT 化し運用コストを削減する技術が求められている．

3. アーキテクチャ研究開発の範囲とねらい

3.1 研究開発の範囲

本研究では，統制ルール遵守の見える化と徹底を実現する統合アクセス制御のアーキテクチャを研究・開発した．

3.2 統制ルール遵守徹底の課題

企業の IT システム全体で守るべき統制ルールをシステムの隅々まで徹底するには，企業内に存在する VM（仮想マシン）層・OS 層・ミドルウェア層・アプリケーション層の全てのソフトウェアが，統制ルール（すなわち統制ルールに従ったアクセス制御の設定）を遵守しなければならない．現状これらのソフトウェアに統制ルールを従わせるには，夫々のソフトウェアに対応する管理機能を用いて部門毎にアクセス権を管理しなければならない．このため，企業システム全体の統制ルールの遵守を見える化し徹底するためには，システム部門毎に人手によりアクセス権の設定，チェック，修正を行い，その結果を統制部門に報告する膨大なコストが必要になる．

3.3 研究のねらい

本研究のねらいは，統制ルールと部門毎に管理されていたアクセス制御を統合管理することで，統制ルールに従い，システム全体のアクセス制御ポリシーを徹底する「統合アクセス制御」の仕組みを実現することである．

4. アーキテクチャ

アクセス制御を統合管理し，同時にポリシーの効率的な運用管理を実現するために，本研究では次のようなアーキテクチャを研究開発した．

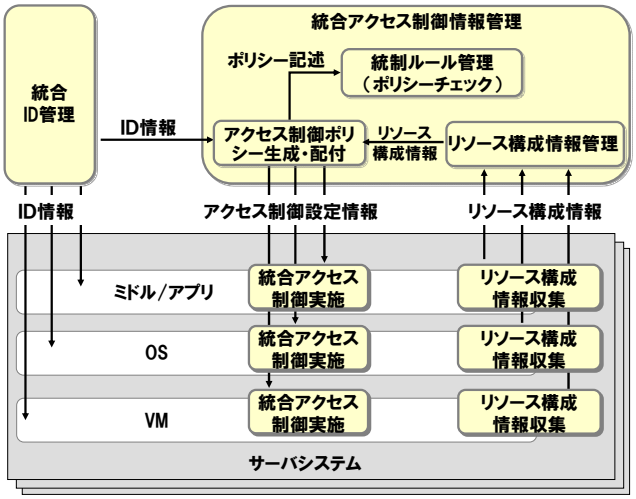

図 1 アーキテクチャ概要

一般のアクセス制御では，「アクセス主体（ユーザ ID やロールなどの ID 情報）」が，「アクセス対象（情報やサービスなどのシステム上のリソース）」に対して，「アクセス（read, write など）」するアクセス制御情報で制御しており，従来個々のソフトウェア自身が管理し保持している．本アーキテクチャでは，これら 3 つの情報各々を，次のコンポーネントを利用して統合管理し，システムを跨いだ統合的なアクセス制御を実現する．

- 統合 ID 管理
  組織変更や人事異動，退職などの機会に必要となる ID 情報の変更を，システム全体に漏れなく対応するために，各ソフトウェアで管理している ID 情報を，システム全体で矛盾なく利用者を特定できる ID（グローバル ID）と結びつけて管理し，変更時にその情報を各ソフトウェアに一括配付し，システム全体の ID 情報を同期する．

† 富士通株式会社 FUJITSU LIMITED
‡ 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 Corp.
＊ 技術研究組合 超先端電子技術開発機構 ASET

- 統合アクセス制御情報管理
  個々のソフトウェアが管理しているアクセス権設定情報を統合管理するために，ID 情報を「統合 ID 管理」から，またアクセス対象であるリソースの構成情報を「リソース構成情報管理」から取得し，アクセス制御ポリシーを「アクセス権ポリシー生成・配付」機能により生成し，各ソフトウェアが解釈可能なアクセス制御設定情報に変換した上で「統合アクセス制御実施」へ配付する[3].

- リソース構成情報管理
  アクセス対象であるリソースについての構成情報を統合管理するために，リソース構成情報管理は，「リソース構成情報収集」から，各ソフトウェアが管理するリソースの構成情報を収集する．ただし各ソフトウェアのアクセス制御機能は，制御可能な対象やアクセスの種類が異なるため，統合管理するには，各アクセス制御機能の仕様に関する情報を収集する必要がある．このため，「リソース構成情報収集」が，アクセス主体やアクセス制御対象などの情報を取得し，リソース構成情報管理へ送付し管理する[4].

- 統合アクセス制御実施
  統合アクセス制御実施は，各ソフトウェアレイヤに配置され，「統合アクセス制御情報管理」から，アクセス制御設定情報を受け取り，ポリシーの内容に従いアクセス要求の可否を制御し，結果をログ出力する[5].

- 統制ルール管理
  IT システムが統制ルールに従って安全に運用されているかを確認するために，統合アクセス制御実施に配付されるポリシーが，統制ルールに違反していないかなどのチェックを行う[6].

5. 効率的な遵守徹底と見える化の実現

5.1 遵守の徹底と見える化の実現

上記アーキテクチャの実装により，VM，OS，ミドルウェア，アプリケーション等のサーバを構成するソフトウェアレイヤのアクセス制御ポリシーを，垂直統合管理することが可能となり，統制ルールとそれに従うアクセス制御ポリシーを遵守徹底，見える化することが実現される．

5.2 効率的なポリシーの管理

上記アーキテクチャのアクセス権ポリシー生成・配付により，アクセス権の効率的管理を実現した．本研究では RBAC (Role Based Access Control) [2]モデルによるアクセス権管理を実現している．

RBAC とは，ユーザ単位でリソースに対して，アクセス権を付与するアクセス制御リスト（ACL）による管理方式とは異なり，ユーザに割り当てられたロール(Role)単位で，アクセス権管理を行なうため，ユーザ単位のアクセス権管理に比べ，ポリシー生成・更新・削除等の管理負荷を大きく削減できる．

さらに，本研究では，複数のアクセス制御対象リソースをひとつにまとめたリソースグループの概念を導入し，リソースグループ単位のポリシーモデル（図２参照）をベースとした記述により，ポリシー生成・更新の簡易化を実現した．

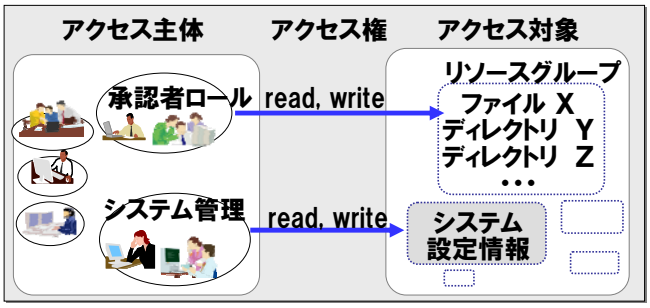

図 2 統合アクセス制御のポリシーモデル

6. おわりに

本稿では，統制ルール遵守の見える化と徹底を IT 化し運用コストを削減するための統合アクセス制御アーキテクチャを紹介した．現在，本アーキテクチャの実装，およびその評価として実証実験を計画している．

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] セキュア・プラットフォーム推進コンソーシアム
http://spf.jeita.or.jp/index.html

[2] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R. and Chandramouli, R. : Proposed NIST standard for role-based access control, ACM Transactions on Information and System Security, Vol.4, No.3, pp.224-274 (Aug. 2001)

[3] 森田 陽一郎，中江 政行，小川 隆一，"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", FIT2009, Sep 2009.

[4] 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.

[5] 林 俊介，恩塚 新治，"セキュア・プラットフォームの研究開発 (4) 仮想システムにおけるアクセス制御機能", FIT2009, Sep 2009.

[6] 寺田 剛陽，長谷部 高行，畠山 卓久，徳谷 崇，"セキュア・プラットフォームの研究開発 (5) システム運用ポリシー遵守チェック", FIT2009, Sep 2009.