L-027

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

Research and development of Secure Platform (4) Access control function for virtual system

林 俊介† 恩塚 新治†
Syunsuke Hayashi Shinji Onzuka

1. はじめに

複数のサーバを１台のサーバ上の仮想マシン（VM）に統合する仮想化技術の普及に伴い，オープンソースコミュニティでもXen[1]などの仮想化ソフトが開発されている．しかし，これらの仮想化ソフトによるサーバ統合環境では，VMやOSのリソースに対するアクセス制御に課題があった．

まず，これらの仮想化ソフトでは，絶対権限(root)を持ったユーザでしか VM を操作することができず，管理者が異なるサーバを VM に統合した場合，VM 毎に操作者を分けるということができない．

また，ポリシーに基づく VM や OS のリソースアクセス制御機構がないため，多数のサーバを統合する場合，VM や OS リソースのアクセス制御の設定負担が大きい．

これらの課題を解決するため，我々は，Xenをベースとしたサーバ統合環境において，統合アクセス制御情報管理[2]により一元化されたポリシーに基づいてVMとOSリソースのアクセス制御する機能を開発した．本機能は，RBAC(Role Based Access Control)[3]の機構を取り入れたVMアクセス制御機能(VM-RBAC)と，VM上のOSで動作するアクセス制御機能(OS-RM)で構成されている．

2. VM-RBAC の機能および実装

2.1 VM-RBACの機能

VM-RBAC は，VM 操作コマンドのアクセス制御機能とリソースの量的制限機能から成る．

VM操作コマンドのアクセス制御機能は，VMを操作する管理者の役割を幾つかに細分化し，各々の役割(ロール)に対して必要最低限の権限だけを与えるものである．本機能を利用すれば，特定のVMを操作する権限をロールに記述でき，ロールを割り当てられたユーザは，そのVMを操作可能な管理者となる．例えば，VMの登録・解除権限の持ったロール，VMの起動・停止権限を持ったロールを作成し，それぞれを管理者に割り当てることで図 1で示すような管理体系を実現できる．

VM 操作コマンドのアクセス制御可否は，ロール名と VM 名，VM 操作コマンドの組み合わせから成る RBAC ポリシーにより定義される．VM-RBAC が備えるポリシー編集ユーザインタフェースを利用することで，容易にポリシーを確認・編集できるようにしている．また，ポリシーの編集ユーザインタフェースに対してもアクセス制御機能が実装されており，特定の管理者からしか編集できないような制限をかけることが可能である．

リソースの量的制限機能は，あるリソースグループ(グループで利用できるリソース量を定義するもの)に属している複数の VM の資源量の総和が，そのリソースグループに割り当てられたリソース量を超えないようにする．本機能を利用すれば，ある VM がリソースを不正もしくは独占利用するといった状況を防止できる．リソースの量的制限機能に関する設定は，リソースグループで利用できるリソース量を定義するマスタファイルとリソースグループに属している VM 名を定義するリソース配分ファイルで定義される．VM-RBAC が備えるポリシー編集ユーザインタフェースを利用することで，容易に両ファイルを確認・編集できる．

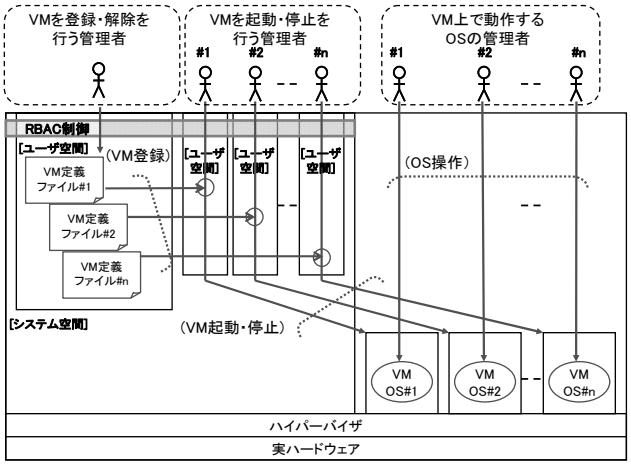

図 1 VM-RBAC を適用した場合の管理体系例

2.2 VM-RBACの実装

前項の機能を実現するため，我々は，VM操作コマンドの入力段階で実行制御を行うアーキテクチャを採用し，VM操作コマンドのアクセス制御部とVM資源の量的制限部をVMの共通APIであるlibvirt[4]に実装した．図 2は，VM-RBACの処理の流れを示したものである．VMの操作コマンド単位でアクセス判定を行う部分をアクセス判定モジュール，VMが利用するリソース量を判定する部分を量的判定モジュールとすることで，ポリシー編集ユーザインタフェースのコマンドに対してもアクセス制御可能とした．

アクセス判定モジュールは，VM 操作コマンドを入力時に，ユーザ定義ファイルおよびポリシー設定ファイルを読む．コマンドを実行したユーザ名，VM 名，VM 操作コマンドおよびポリシー設定ファイルの内容を比較することにより，ユーザが VM に対して操作可能かどうか判定する．量的制限判定モジュールは，VM 起動時にリソースマスタファイルおよびリソース配分ファイルを読む．そして，操作時に要求されたリソース量と設定ファイルの内容を比較することにより，リソースを利用可能かどうか判定する．

† 富士通株式会社, FUJITSU LIMITED

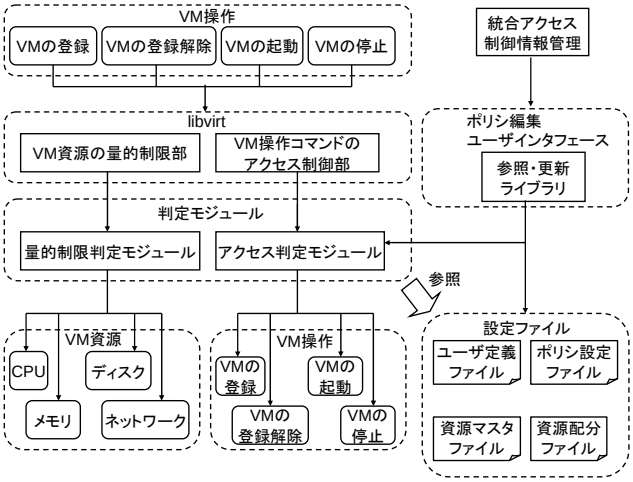

図 2 VM-RBAC の処理の流れ

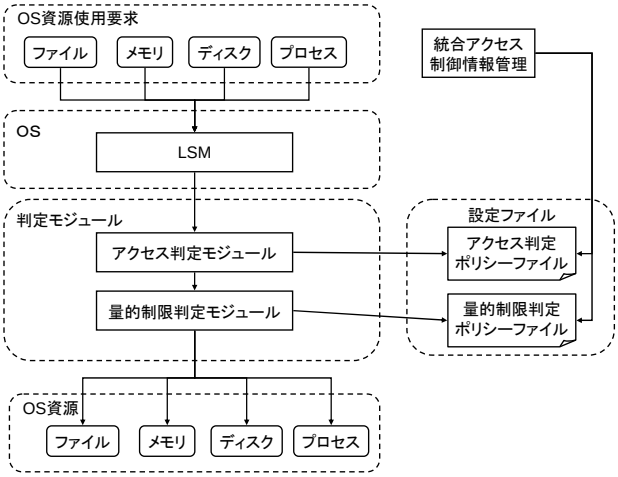

図 3 OS-RM の処理の流れ

3. OS-RM の機能および実装

3.1 OS-RMの機能

OS で動作する OS-RM は，ファイルのアクセス制御機能と，メモリ，ディスク，プロセスの量的制限機能から成る．OS-RM は，これらのリソースを操作する利用者および管理者，プログラムの役割を細分化し，各々の役割に対して必要最低限の権限だけを与えるものである．本機能を使用すれば，利用者毎のアクセス権限の付与，絶対権限（root/Administrator）の抑止が可能となり，ファイルの漏洩，改ざん，不正利用の脅威を最小限にすることができる．

アクセス制御可否は，アカウントとリソース，リソースに対するアクション(読書き，実行など）の組み合わせから成るポリシーにより定義される．統合アクセス制御情報管理が備えるポリシー編集ユーザインタフェースを利用することで，容易にポリシーを確認・編集できるようにしている．また，ポリシーの編集ユーザインタフェースに対してアクセス制御機能が実装されており，特定の管理者からしか編集できないような制限をかけることが可能である．

量的制限機能は，リソースグループに属している複数のメモリ，ディスク，プロセスが予め許可されたリソース量を超えないようにリソース量を制限するものである．この機能を使えば，メモリ，ディスクの不正・独占利用するといった状況を防止できる．

3.2 OS-RMの実装

前項の機能を実現するため，我々は，Linuxに対してのOSリソースのアクセス制御機能，量的制限機能の実装を行った．図 3は，アクセス制御機能，量的制限機能の処理の流れを示したものである．LSM(Linux Security Module)[5]のアーキテクチャを採用して実装している．アクセス判定モジュールおよび量的判定モジュールをLSMのプラグインモジュールとして開発することでアクセス制御機能を実現した．

4. おわりに

本論文では，Xen をベースとしたサーバ統合環境の VM と OS リソースのアクセス制御機能である VM-RBAC および OS-RM を提案した．我々は評価実験において，VM-RBAC と OS-RM は，統合アクセス制御情報管理から配布されるポリシーに従ってアクセス制御が行われていることを確認した．VM-RBAC のリソースの量的制限機能に関しては，今後，統合アクセス情報管理と連携させ評価する予定である．

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]Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, Andrew Warfield, “Xen and the Art of Virtualization”, In Proc. SOSP 2003. Bolton Landing, New York.U.S.A, Oct 19-22 2003.

[2]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.

[3]David F. Ferraiolo and D. Richard Kuhn, “Role-Based Access Controls”. 15th National Computer Security Conference, Baltimore MD pp. 554 – 563, 1992.

[4]The virtualization API, http://libvirt.org/

[5]Chris Wright ,Crispin Cowan, James Morris, Stephen Smalley, Greg Kroah-Hartman “Linux Security Modules: General Security Support for the Linux Kernel”,USENIX, 2002.