(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6069580号
(P6069580)
(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月6日(2017.1.6)

(51)Int.Cl.　F I
G06F 9/46 (2006.01)　G06F 9/46 350

請求項の数 19 (全 35 頁)

(21)出願番号	特願2016-507639 (P2016-507639)
(86)(22)出願日	平成26年4月9日 (2014.4.9)
(65)公表番号	特表2016-522919 (P2016-522919A)
(43)公表日	平成28年8月4日 (2016.8.4)
(86)国際出願番号	PCT/US2014/033524
(87)国際公開番号	WO2014/169054
(87)国際公開日	平成26年10月16日 (2014.10.16)
審査請求日	平成27年12月9日 (2015.12.9)
(31)優先権主張番号	61/899,468
(32)優先日	平成25年11月4日 (2013.11.4)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	61/810,480
(32)優先日	平成25年4月10日 (2013.4.10)
(33)優先権主張国	米国 (US)

早期審査対象出願

(73)特許権者　515268467
イルミオ，　インコーポレイテッド
Ｉｌｌｕｍｉｏ，Ｉｎｃ．
アメリカ合衆国，カリフォルニア州　９４０８６，サニーベイル，サン　ガブリエル　ドライブ　１６０
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　ポール　ジェイ．キルナー
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内

最終頁に続く

(54)【発明の名称】論理的多次元ラベルベースのポリシーモデルを使用した分散型ネットワークマネージメント

(57)【特許請求の範囲】
【請求項１】
１つまたは複数のルールのセットを備える管理ドメイン規模のマネージメントポリシーに従って、管理ドメイン内の特定のマネージドサーバに関するマネージメント命令を生成する方法であって、前記管理ドメインは複数のマネージドサーバを含み、前記方法は、
前記ルールのセット内のどのルールが、前記特定のマネージドサーバに関連するのかを判定するステップと、
関連すると判定された前記ルールに基づいて、機能レベルの命令を生成するステップと、
前記特定のマネージドサーバに関連するマネージドサーバのセットを選択するステップであって、前記選択するステップは、前記特定のマネージドサーバに関連する前記ルールにより参照される、エニュメレートされたマネージドサーバを識別するために、前記複数のマネージドサーバの記述の表現を検査することを含むステップと、
前記特定のマネージドサーバに、前記機能レベルの命令と前記選択されたマネージドサーバのセットに関する情報とを送信するステップと
を備え、
前記特定のマネージドサーバは、前記機能レベルの命令と前記選択されたマネージドサーバのセットに関する情報とを用いてマネージメントモジュールを構成し、前記構成されたマネージメントモジュールは前記管理ドメイン規模のマネージメントポリシーを実装することを特徴とする方法。

【請求項２】
前記特定のマネージドサーバは仮想サーバであることを特徴とする請求項１に記載の方法。
【請求項３】
前記管理ドメイン規模のマネージメントポリシーは、マネージドサーバがアクセスすること、もしくはデバイスによりアクセスされることを許可されるかどうか、または、どのように、マネージドサーバがアクセスすること、もしくはデバイスによりアクセスされることを許可されるかを指定することを特徴とする請求項１に記載の方法。
【請求項４】
ルールはマネージドサーバの次元および次元に関する値を指定することによりマネージドサーバを特定し、前記次元は、役割、環境、アプリケーション、業種、およびロケーションを含むグループの１つの要素であることを特徴とする請求項１に記載の方法。
【請求項５】
ルールは、どのマネージドサーバがサービスを提供することを許可されるかを指定し、ルールは、前記特定のマネージドサーバがサービスを提供することを許可されることを指定する場合に、前記ルールは前記特定のマネージドサーバに関連することを特徴とする請求項１に記載の方法。
【請求項６】
ルールは、マネージドサーバがサービスを消費することを許可されるかどうか、または、どのように、マネージドサーバがサービスを消費することを許可されるかを指定し、ルールは、前記特定のマネージドサーバがサービスを消費することを許可されるかどうか、または、どのように、前記特定のマネージドサーバがサービスを消費することを許可されるかを指定する場合に、前記ルールは前記特定のマネージドサーバに関連することを特徴とする請求項１に記載の方法。
【請求項７】
前記マネージドサーバに関する情報は前記マネージドサーバのネットワーク公開情報を含むことを特徴とする請求項１に記載の方法。
【請求項８】
前記マネージメントモジュールは、下位レベルのネットワークエンジン、またはセキュリティエンジンを備えることを特徴とする請求項１に記載の方法。
【請求項９】
前記複数のマネージドサーバのどのマネージドサーバが、前記特定のマネージドサーバに関連するかを判定する前に、前記複数のマネージドサーバの前記マネージドサーバをエニュメレートするステップを、さらに含むことを特徴とする請求項１に記載の方法。
【請求項１０】
１つまたは複数のルールのセットを備える管理ドメイン規模のマネージメントポリシーに従って、管理ドメイン内の特定のマネージドサーバに関するマネージメント命令を生成するコンピュータプログラムモジュールを記憶する、非一時的なコンピュータ可読記憶媒体であって、前記管理ドメインは複数のマネージドサーバを含み、前記コンピュータプログラムモジュールは、
前記ルールのセット内のどのルールが、前記特定のマネージドサーバに関連するのかを判定するステップと、
関連すると判定された前記ルールに基づいて、機能レベルの命令を生成するステップと、
前記特定のマネージドサーバに関連するマネージドサーバのセットを選択するステップであって、前記選択するステップは、前記特定のマネージドサーバに関連する前記ルールにより参照される、エニュメレートされたマネージドサーバを識別するために、前記複数のマネージドサーバの記述の表現を検査することを含むステップと、
前記特定のマネージドサーバに、前記機能レベルの命令と、関連すると判定された前記マネージドサーバに関する情報とを送信するステップと

を実行するために実行可能であり、
前記特定のマネージドサーバは、前記機能レベルの命令と前記マネージドサーバに関する情報とを用いてマネージメントモジュールを構成し、前記構成されたマネージメントモジュールは前記管理ドメイン規模のマネージメントポリシーを実装することを特徴とするコンピュータ可読記憶媒体。
【請求項１１】
前記特定のマネージドサーバは仮想サーバであることを特徴とする請求項１０に記載のコンピュータ可読記憶媒体。
【請求項１２】
前記管理ドメイン規模のマネージメントポリシーは、マネージドサーバがアクセスすること、もしくはデバイスによりアクセスされることを許可されるかどうか、または、どのように、マネージドサーバがアクセスすること、もしくはデバイスによりアクセスされることを許可されるかを指定することを特徴とする請求項１０に記載のコンピュータ可読記憶媒体。
【請求項１３】
ルールはマネージドサーバの次元および次元に関する値を指定することによりマネージドサーバを特定し、前記次元は、役割、環境、アプリケーション、業種、およびロケーションを含むグループの１つの要素であることを特徴とする請求項１０に記載のコンピュータ可読記憶媒体。
【請求項１４】
ルールは、どのマネージドサーバがサービスを提供することを許可されるかを指定し、ルールは、前記特定のマネージドサーバがサービスを提供することを許可されることを指定する場合に、前記ルールは前記特定のマネージドサーバに関連することを特徴とする請求項１０に記載のコンピュータ可読記憶媒体。
【請求項１５】
ルールは、マネージドサーバがサービスを消費することを許可されるかどうか、または、どのように、マネージドサーバがサービスを消費することを許可されるかを指定し、ルールは、前記特定のマネージドサーバがサービスを消費することを許可されるかどうか、または、どのように、前記特定のマネージドサーバがサービスを消費することを許可されるかを指定する場合に、前記ルールは前記特定のマネージドサーバに関連することを特徴とする請求項１０に記載のコンピュータ可読記憶媒体。
【請求項１６】
前記マネージドサーバに関する情報は前記マネージドサーバのネットワーク公開情報を含むことを特徴とする請求項１０に記載のコンピュータ可読記憶媒体。
【請求項１７】
前記マネージメントモジュールは、下位レベルのネットワークエンジン、またはセキュリティエンジンを備えることを特徴とする請求項１０に記載のコンピュータ可読記憶媒体。
【請求項１８】
１つまたは複数のルールのセットを備える管理ドメイン規模のマネージメントポリシーに従って、管理ドメイン内の特定のマネージドサーバに関するマネージメント命令を生成するシステムであって、前記管理ドメインは複数のマネージドサーバを含み、前記システムは、
前記ルールのセット内のどのルールが、前記特定のマネージドサーバに関連するのかを判定するステップと、
関連すると判定された前記ルールに基づいて、機能レベルの命令を生成するステップと、
前記特定のマネージドサーバに関連するマネージドサーバのセットを選択するステップであって、前記選択するステップは、前記特定のマネージドサーバに関連する前記ルールにより参照される、エニュメレートされたマネージドサーバを識別するために、前記複数

のマネージドサーバの記述の表現を検査することを含むステップと、
前記特定のマネージドサーバに、前記機能レベルの命令と、関連すると判定された前記マネージドサーバに関する情報とを送信するステップと
を実行するために実行可能なコンピュータプログラムモジュールを記憶する、非一時的なコンピュータ可読記憶媒体と、
前記コンピュータプログラムモジュールを実行するコンピュータプロセッサと
を備え、
前記特定のマネージドサーバは、前記機能レベルの命令と前記マネージドサーバに関する情報とを用いてマネージメントモジュールを構成し、前記構成されたマネージメントモジュールは前記管理ドメイン規模のマネージメントポリシーを実装することを特徴とするシステム。
【請求項１９】
前記関連するマネージドサーバのセットを選択するステップは、
各々のエニュメレートされたマネージドサーバに関して、前記エニュメレートされたマネージドサーバが前記ルールのいずれかにより参照されるかどうかを判定するために、前記特定のマネージドサーバに関連する前記ルールを分析するステップと、
前記ルールのいずれかにより参照される前記エニュメレートされたマネージドサーバに応答して、前記エニュメレートされたマネージドサーバを、前記関連するマネージドサーバのセットに追加するステップと
をさらに備えることを特徴とする請求項１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書に記載される主題は、概して、管理ドメインのマネージングサーバ（物理的または仮想的）の分野に関し、特に、論理的多次元ラベルベースのポリシーモデルを遵守する、管理ドメイン規模のポリシーに係るマネージングサーバに関する。
【背景技術】
【０００２】
管理ドメインのサーバ（物理的または仮想的）は、ポリシーに従って管理される。例えば、セキュリティポリシーは、アクセス制御および／またはセキュア接続を指定することができ、一方、リソース利用のポリシーは、管理ドメインのコンピューティングリソース（例えば、ディスクおよび／または周辺機器）の利用を指定することができる。従来のポリシーは、物理的デバイスを参照し、インターネットプロトコル（ＩＰ）アドレス、ＩＰアドレスレンジ、サブネットワーク、および、ネットワークインターフェースなどの下位レベルの構成概念の観点で表現される。
【発明の概要】
【発明が解決しようとする課題】
【０００３】
これらの下位レベルの構成概念は、きめの細かいポリシーを、抽象的で自然な方法で書くことを困難にする。
【課題を解決するための手段】
【０００４】
上記および他の問題は、非一時的コンピュータ可読記憶媒体、および、１つまたは複数のルールのセットを備える管理ドメイン規模のマネージメントポリシーに従って、管理ドメイン内の特定のマネージドサーバ用のマネージメント命令を生成するためのシステム、によって対処される。管理ドメインは、複数のマネージドサーバを含む。方法の一実施形態は、ルールのセット内のどのルールが、特定のマネージドサーバに関連するのかを判定するステップを含む。方法は、関連すると判定された命令に基づき、機能レベルの命令を生成するステップをさらに含む。方法は、複数のマネージドサーバ内のどのマネージドサーバが、特定のマネージドサーバに関連するのかを判定するステップをさらに含む。方法

は、特定のマネージドサーバに、機能レベルの命令と関連すると判定されたマネージドサーバに関する情報とを送るステップをさらに含む。特定のマネージドサーバが、機能レベルの命令とマネージドサーバに関する情報とを使用してマネージメントモジュールを構成し、構成されたマネージメントモジュールが管理ドメイン規模のマネージメントポリシーを実装するようにされる。

【０００５】

媒体の一実施形態には、ステップを実行するべく実行可能なコンピュータプログラムモジュールを記憶する。当該ステップには、ルールのセット内のどのルールが、特定のマネージドサーバに関連するのかを判定するステップが含まれる。当該ステップには、関連すると判定された命令に基づき、機能レベルの命令を生成するステップがさらに含まれる。当該ステップには、複数のマネージドサーバ内のどのマネージドサーバが、特定のマネージドサーバに関連するのかを判定するステップがさらに含まれる。当該ステップには、特定のマネージドサーバに、機能レベルの命令と、関連すると判定されたマネージドサーバに関する情報とを送るステップがさらに含まれる。特定のマネージドサーバが、機能レベルの命令とマネージドサーバに関する情報とを使用してマネージメントモジュールを構成し、構成されたマネージメントモジュールが管理ドメイン規模のマネージメントポリシーを実装するようにされる。

【０００６】

システムの一実施形態には、ステップを実行するべく実行可能なコンピュータプログラムモジュールを記憶した非一時的コンピュータ可読記憶媒体が含まれる。当該ステップには、ルールのセット内のどのルールが、特定のマネージドサーバに関連するのかを判定するステップが含まれる。当該ステップには、関連すると判定された命令に基づき、機能レベルの命令を生成するステップがさらに含まれる。当該ステップには、複数のマネージドサーバ内のどのマネージドサーバが、特定のマネージドサーバに関連するのかを判定するステップがさらに含まれる。当該ステップには、特定のマネージドサーバに、機能レベルの命令と、関連すると判定されたマネージドサーバに関する情報とを送るステップがさらに含まれる。特定のマネージドサーバが、機能レベルの命令とマネージドサーバに関する情報とを使用してマネージメントモジュールを構成し、構成されたマネージメントモジュールが管理ドメイン規模のマネージメントポリシーを実装するようにされる。

【図面の簡単な説明】

【０００７】

【図１】一実施形態に係る管理ドメインのマネージングサーバ（物理的または仮想的）のための環境を説明する、上位レベルのブロック図である。

【図２】一実施形態に係る、図１で説明されるエンティティのうちの１つまたは複数として使用するための、コンピュータの一例を説明する上位レベルのブロック図である。

【図３】一実施形態に係るグローバルマネージャの詳細な概念を説明する上位レベルのブロック図である。

【図４】一実施形態に係るマネージドサーバのポリシー実装モジュールの詳細な概念を説明する上位レベルのブロック図である。

【図５】一実施形態に係る特定のマネージドサーバ用のマネージメント命令を生成する方法を説明するフローチャートである。

【図６】一実施形態に係るマネージドサーバのマネージメントモジュールの構成を生成する方法を説明するフローチャートである。

【図７】一実施形態に係るマネージドサーバのローカル状態を監視し、かつ、ローカル状態情報をグローバルマネージャに送る、方法を説明するフローチャートである。

【図８】一実施形態に係る管理ドメインのコンピュータネットワークインフラの状態に対する変更を処理する方法を説明するフローチャートである。

【発明を実施するための形態】

【０００８】

図面および以下の記載では、単なる説明として、特定の実施形態について記載する。当

業者は、本明細書において説明される構造および方法の代替の実施形態が、本明細書に記載される原理から逸脱することなく具現化されてよいことを、以下の記載から容易に認識するであろう。ここで、いくつかの実施形態が参照され、その例が添付の図面において説明される。実用的である限り、同様または同類の参照番号が、図面において使用されてよく、また、類似または同様の機能性を示してよいことに留意されたい。

【０００９】

図１は、一実施形態に係る、管理ドメイン１５０のマネージングサーバ（物理的または仮想的）１３０のための環境１００を説明する、上位レベルのブロック図である。管理ドメイン１５０は、例えば、サービスプロバイダ、法人、大学、または政府系機関などの企業に相当してよい。環境１００は、企業自体により、または、企業がそのサーバ１３０を管理するのを助ける、サードパーティ（例えば、第２の企業）により、維持されてよい。図示のように、環境１００には、ネットワーク１１０、グローバルマネージャ１２０、複数のマネージドサーバ１３０、および、複数のアンマネージドデバイス１４０が含まれる。複数のマネージドサーバ１３０および複数のアンマネージドデバイス１４０は、管理ドメイン１５０に関連付けられる。例えば、これらは、企業、または、企業の代わりにサードパーティ（例えば、公的クラウドサービスプロバイダ）によって操作される。図１に示す実施形態では、明確にするために、１つのグローバルマネージャ１２０、２つのマネージドサーバ１３０、および、２つのアンマネージドデバイス１４０が、図示されるが、他の実施形態では、異なる数のグローバルマネージャ１２０、マネージドサーバ１３０、および／またはアンマネージドデバイス１４０を有することができる。

【００１０】

ネットワーク１１０は、グローバルマネージャ１２０、マネージドサーバ１３０、およびアンマネージドデバイス１４０の間の通信経路を表す。一実施形態において、ネットワーク１１０は、標準の通信技術および／またはプロトコルを使用し、インターネットを含むことができる。別の実施形態において、ネットワーク１１０上のエンティティは、カスタムおよび／または専用のデータ通信技術を使用することができる。

【００１１】

マネージドサーバ１３０は、管理ドメイン規模のマネージメントポリシー３３０（図３に示す）を実装する機械（物理的または仮想的）である。一実施形態において、サーバは、オペレーティングシステムのカーネルが、１つのみのインスタンスの代わりに、複数の分離されたユーザ空間のインスタンスを有効にする、サーバ仮想化方法である、オペレーティングシステムのレベル仮想化に従う、仮想サーバ（コンテナ、仮想化エンジン、仮想プライベートサーバ、またはジェイルとも称されることがある）のユーザ空間のインスタンスである。マネージドサーバ１３０が物理的機械である場合、マネージドサーバ１３０は、コンピュータまたはコンピュータのセットである。マネージドサーバ１３０が仮想機械である場合、マネージドサーバ１３０は、コンピュータまたはコンピュータのセット上で実行される。管理ドメイン規模のマネージメントポリシー３３０は、管理ドメイン１５０に関連付けられるエンティティが、他のエンティティにアクセスすること（もしくは、他のエンティティによってアクセスされること）、または、他の方法でサービスを消費すること（もしくは提供すること）を許可されるかどうか、および／または、管理ドメイン１５０に関連付けられるエンティティが、どのように、他のエンティティにアクセスすること（もしくは、他のエンティティによってアクセスされること）、または、他の方法でサービスを消費すること（もしくは提供すること）を許可されるのかを指定する。例えば、管理ドメイン規模のマネージメントポリシー３３０は、セキュリティまたはリソース利用を指定する。セキュリティポリシーは、アクセス制御、セキュア接続、ディスク暗号化、および／または、実行可能処理の制御を指定することができ、一方、リソース利用のポリシーは、管理ドメインのコンピューティングリソース（例えば、ディスク、周辺機器、および／または、帯域幅）の利用を規定することができる。

【００１２】

マネージドサーバ１３０には、マネージメントモジュール１３２、マネージメントモジ

ュール構成１３４、および、ポリシー実装モジュール１３６が含まれる。マネージメントモジュール１３２は、管理ドメイン規模のマネージメントポリシー３３０を実装する。例えば、セキュリティの場合、マネージメントモジュール１３２は、オペレーティングシステムレベルのファイアウォール、インターネットプロトコルセキュリティ（ＩＰｓｅｃ）エンジン、またはネットワークトラフィックフィルタリングエンジン（例えば、ウィンドウズフィルタリングプラットフォーム（ＷＦＰ）開発プラットフォームに基づく）などの下位レベルのネットワークまたはセキュリティエンジンとすることができる。リソース利用の場合、マネージメントモジュール１３２は、ディスク利用のエンジンまたは周辺機器利用のエンジンとすることができる。

【００１３】

マネージメントモジュール構成１３４は、マネージメントモジュール１３２の動作に影響を与える。例えば、セキュリティの場合、マネージメントモジュール構成１３４は、ファイアウォールによって適用されるアクセス制御ルール、ＩＰｓｅｃエンジンによって適用されるセキュア接続ポリシー（例えば、Ｌｉｎｕｘオペレーティングシステムのｉｐｔａｂｌｅｓエントリーおよびｉｐｓｅｔエントリーとして、具現化される）、または、フィルタリングエンジンによって適用されるフィルタリングルールとすることができる。リソース利用の場合、マネージメントモジュール構成１３４は、ディスク利用のエンジンによって適用されるディスク利用のポリシー、または、周辺機器利用のエンジンによって適用される周辺機器利用のポリシーとすることができる。

【００１４】

ポリシー実装モジュール１３６は、ａ）グローバルマネージャ１２０から受け取るマネージメント命令、および、ｂ）マネージドサーバ１３０の状態に基づき、マネージメントモジュール構成１３４を生成する。マネージメント命令は、管理ドメイン規模のマネージメントポリシー３３０に部分的に基づき生成される。ポリシー実装モジュール１３６によって生成されるマネージメントモジュール構成１３４は、その管理ドメイン規模のマネージメントポリシー３３０を実装する（ポリシーがマネージドサーバ１３０に関与する範囲で）。この２段階のプロセス（マネージメント命令を生成する、および、マネージメントモジュール構成１３４を生成する）は、マネージメントポリシーの「インスタンス化」と称される。ポリシー実装モジュール１３６はまた、マネージドサーバ１３０のローカル状態を監視し、ローカル状態情報をグローバルマネージャ１２０に送る。

【００１５】

一実施形態において、ポリシー実装モジュール１３６は、より大きなプロプライエタリモジュール（図示せず）の一部である。プロプライエタリモジュールは、マネージメントモジュール１３２およびマネージメントモジュール構成１３４を既に持っているデバイスにロードされ、それによって、デバイスを、アンマネージドデバイス１４０からマネージドサーバ１３０に変換する。ポリシー実装モジュール１３６については、図４、６、および７を参照して、以下でさらに説明する。

【００１６】

アンマネージドデバイス１４０は、ポリシー実装モジュール１３６を含まないコンピュータ（またはコンピュータのセット）である。アンマネージドデバイス１４０は、管理ドメイン規模のマネージメントポリシー３３０を実装しない。しかし、マネージドサーバ１３０とアンマネージドデバイス１４０との間の対話処理が、（マネージドサーバ１３０により実装されるような）管理ドメイン規模のマネージメントポリシー３３０に従うようにされてよい。アンマネージドデバイス１４０の一例は、管理ドメイン１５０によって使用されるネットワーク回路である。アンマネージドデバイス１４０の別の例は、管理ドメイン１５０（例えば、ノートブックもしくはデスクトップコンピュータ、タブレットコンピュータ、または携帯電話）に対して自身を認証する人によって使用されるデバイスである。

【００１７】

グローバルマネージャ１２０は、マネージドサーバ１３０用のマネージメント命令を生

成して、生成したマネージメント命令をサーバに送る、コンピュータ（またはコンピュータのセット）である。マネージメント命令は、ａ）管理ドメインのコンピュータネットワークインフラの状態３２０、および、ｂ）管理ドメイン規模のマネージメントポリシー３３０に基づいて生成される。管理ドメインのコンピュータネットワークインフラの状態３２０には、マネージドサーバ１３０の記述と、（選択的に）アンマネージドデバイス１４０の記述とが含まれる。グローバルマネージャ１２０はまた、マネージドサーバ１３０から受け取るローカル状態情報を処理する。

【００１８】

管理ドメイン規模のマネージメントポリシー３３０は、ＩＰアドレス、ＩＰアドレスレンジ、サブネットワーク、およびネットワークインターフェース、などの下位レベルの構成概念を使用してもマネージドサーバ１３０を参照しない、論理的マネージメントモデル基づく。代わりに、論理的マネージメントモデルは、本明細書では「ラベル」と称される、上位レベルの特徴に基づいてマネージドサーバ１３０を参照する。ラベルは、「次元」（上位レベルの特徴）と、「値」（上位レベルの特徴の値）とを含む一対である。この多次元空間内に構築されるマネージメントポリシーは、単一特徴ネットワーク／ＩＰアドレスベースのポリシーモデルに従って構築されるマネージメントポリシーよりも、表現豊かである。特に、より上位レベルの抽象化である「ラベル」を使用してマネージメントポリシーを表現することで、人々が、マネージメントポリシーをより良く理解、可視化、および修正することを可能にする。

【００１９】

論理的マネージメントモデル（例えば、利用可能な次元の数および型と、それらの次元の可能性のある値）は、構成可能である。一実施形態において、論理的マネージメントモデルには、表１に示すように、以下の次元と値とが含まれる。

【００２０】

【表１】

次元	意味（Ｍ）、値（Ｖ）
役割	Ｍ：管理ドメイン内のマネージドサーバの役割 Ｖ：ウェブ、ＡＰＩ、データベース
環境	Ｍ：マネージドサーバのライフサイクル段階 Ｖ：プロダクション、ステージング、開発
アプリケーション	Ｍ：マネージドサーバが属する論理アプリケーション（マネージドサーバの、より上位レベルのグループ分け） Ｖ：取引、人材
業種	Ｍ：マネージドサーバが属する事業単位 Ｖ：マーケティング、エンジニアリング
ロケーション	Ｍ：マネージドサーバのロケーション。物理的（例えば、国もしくは地理的領域）または論理的（例えば、ネットワーク）、とすることができる。物理的な場合は、地理的コンプライアンス要件の表現には特に有用である。 Ｖ：ＵＳまたはＥＵ（物理的）、ｕｓ－西－１またはｕｓ－東－２（論理的）

表１－論理的マネージメントモデルの例

【００２１】

論理的マネージメントモデルは、グループ内のマネージドサーバ１３０の全てを記述する１つまたは複数のラベル（本明細書において、「ラベルセット」と称する）を指定することにより、複数のマネージドサーバ１３０がまとめてグループ化されることを可能にする。ラベルセットは、論理的マネージメントモデルにおいて、１つの次元について、複数のゼロの値または１の値のどちらかを含む。ラベルセットは、論理的マネージメントモデ

ルにおいて、全ての次元についてラベルを含む必要があるわけではない。このように、論理的マネージメントモデルは、管理ドメインのマネージドサーバ１３０の区分および分類と、マネージドサーバ１３０の任意のグループ分けの作成とを可能にする。論理的マネージメントモデルはまた、単一のマネージドサーバ１３０が、複数の重複するセット（すなわち、マネージドサーバの複数の重複するグループ）内に存在できるようにする。論理的マネージメントモデルは、単一のマネージドサーバ１３０を、ネストされたセットの階層内に存在することに限定しない。

【００２２】

例えば、セキュリティの場合、区分は、アクセス制御ポリシーと共に使用されて、特定のポリシーに従うマネージドサーバ１３０のグループを定義することができる。同様に、区分は、セキュア接続ポリシーと共に使用されて、マネージドサーバ１３０のグループと、グループ内通信およびグループ間通信に適用されるポリシーとを定義することができる。従って、第１のグループのマネージドサーバ１３０（第１のラベルセットにより指定される）内での通信は、第１のセキュア接続設定（例えば、要求されないセキュア接続）に制限されてよく、第１のグループのマネージドサーバおよび第２のグループのマネージドサーバ（第２のラベルセットにより指定される）との間の通信は、第２のセキュア接続設定（例えば、ＩＰｓｅｃ暗号ペイロード（Ｅｎｃａｐｓｕｌａｔｉｎｇ Ｓｅｃｕｒｉｔｙ Ｐａｙｌｏａｄ（ＥＳＰ））／認証ヘッダ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｈｅａｄｅｒ（ＡＨ）高度暗号化規格（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＡＥＳ））／セキュアハッシュルゴリズム－２（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ－２（ＳＨＡ－２））））に制限されてよい。

【００２３】

環境１００内の各マネージドサーバ１３０は、管理ドメイン規模のマネージメントポリシー３３０を実装する（ポリシーがマネージドサーバ１３０に関与する範囲で）。その結果、管理ドメイン規模のマネージメントポリシー３３０が、管理ドメイン１５０全体に分散するように適用され、チョークポイントが無い。また、管理ドメイン規模のマネージメントポリシー３３０は、管理ドメインの物理ネットワークトポロジおよびネットワークアドレッシングスキームとは無関係の論理レベルで適用される。

【００２４】

グローバルマネージャ１２０、管理ドメインのコンピュータネットワークインフラの状態３２０、および管理ドメイン規模のマネージメントポリシー３３０について、図３、５、および８を参照して、以下でさらに説明する。

【００２５】

図２は、一実施形態に係る、図１で説明されるエンティティのうちの１つまたは複数として使用するための、コンピュータ２００の一例を説明する上位レベルのブロック図である。チップセット２０４に結合される少なくとも１つのプロセッサ２０２について、説明される。チップセット２０４には、メモリコントローラハブ２２０、および入力／出力（Ｉ／Ｏ）コントローラハブ２２２が含まれる。メモリ２０６およびグラフィックアダプタ２１２が、メモリコントローラハブ２２０に結合され、ディスプレイ装置２１８が、グラフィックアダプタ２１２に結合される。記憶装置２０８、キーボード２１０、ポインティングデバイス２１４、およびネットワークアダプタ２１６が、Ｉ／Ｏコントローラハブ２２２に結合される。コンピュータ２００の他の実施形態は、異なるアーキテクチャを有する。例えば、メモリ２０６は、いくつかの実施形態において、プロセッサ２０２に直接結合される。

【００２６】

記憶装置２０８には、ハードドライブ、ＣＤ－ＲＯＭ（ｃｏｍｐａｃｔ ｄｉｓｋ ｒｅａｄ－ｏｎｌｙ ｍｅｍｏｒｙ）、ＤＶＤ、またはソリッドステートメモリデバイスなどの１つまたは複数の非一時的コンピュータ可読記憶媒体が含まれる。メモリ２０６は、プロセッサ２０２により使用される命令およびデータを保持する。ポインティングデバイス２１４は、キーボード２１０と組み合わせて使用され、データをコンピュータシステム

２００に入力する。グラフィックアダプタ２１２は、画像および他の情報をディスプレイ装置２１８上に表示する。いくつかの実施形態において、ディスプレイ装置２１８には、ユーザの入力および選択を受け取るためのタッチスクリーン機能が含まれる。ネットワークアダプタ２１６は、コンピュータシステム２００をネットワーク１１０に結合する。コンピュータ２００のいくつかの実施形態は、図２に示すものとは異なるおよび／または他の構成要素を有する。例えば、グローバルマネージャ１２０および／またはマネージドサーバ１３０は、複数のブレードサーバで形成されて、ディスプレイ装置、キーボード、および他の構成要素が無くてもよく、一方、アンマネージドデバイス１４０は、ノートブックもしくはデスクトップコンピュータ、タブレットコンピュータ、または携帯電話であってよい。

【００２７】

コンピュータ２００は、本明細書に記載される機能性を提供するためのコンピュータプログラムモジュールを実行するべく適合される。本明細書で使用されるとき、用語「モジュール」は、コンピュータプログラム命令および／または特定の機能性を提供するために使用される他の論理を指す。従って、モジュールは、ハードウェア、ファームウェア、および／またはソフトウェアで実装されてよい。一実施形態において、実行可能コンピュータプログラム命令から形成されるプログラムモジュールは、記憶装置２０８上に記憶され、メモリ２０６にロードされ、プロセッサ２０２によって実行される。

【００２８】

図３は、一実施形態に係る、グローバルマネージャ１２０の詳細な概念を説明する上位レベルのブロック図である。グローバルマネージャ１２０には、リポジトリ３００、およびプロセシングサーバ３１０が含まれる。リポジトリ３００は、管理ドメインのコンピュータネットワークインフラの状態３２０と、管理ドメイン規模のマネージメントポリシー３３０とを記憶するコンピュータ（またはコンピュータのセット）である。一実施形態において、リポジトリ３００には、要求に応じて、プロセシングサーバ３１０に、管理ドメイン状態３２０とマネージメントポリシー３３０とへのアクセスを提供するサーバが含まれる。

【００２９】

管理ドメインのコンピュータネットワークインフラの状態３２０には、マネージドサーバ１３０の記述と、（選択的に）アンマネージドデバイス１４０の記述とが含まれる。マネージドサーバ１３０の記述には、例えば、一意識別子（ＵＩＤ）、オンライン／オフラインインジケータ、１つまたは複数の構成特徴（選択的）、ネットワーク公開情報、サービス情報、およびマネージドサーバ１３０を記述する１つまたは複数のラベル（ラベルセット）が含まれる。

【００３０】

ＵＩＤは、マネージドサーバ１３０を一意的に識別する。オンライン／オフラインインジケータは、マネージドサーバ１３０がオンラインかオフラインかを示す。「構成特徴」は、マネージドサーバ１３０に関連する値を記憶し、任意のタイプの情報（例えば、どのオペレーティングシステムがマネージドサーバ上で実行中であるのかの指標）であってよい。構成特徴は、ルールの条件部分（以下で説明する）と組み合わせて使用される。

【００３１】

ネットワーク公開情報は、マネージドサーバのネットワークインターフェースに関与する。一実施形態において、ネットワーク公開情報には、マネージドサーバのネットワークインターフェースのそれぞれについて、ネットワークインターフェースがアタッチされる「双方向到達可能ネットワーク（ｂｉｄｉｒｅｃｔｉｏｎａｌｌｙ－ｒｅａｃｈａｂｌｅ　ｎｅｔｗｏｒｋ（ＢＲＮ））」の識別子、および、ＢＲＮ内での動作に使用されるゼロ個以上のＩＰアドレス（およびそのサブネット）が含まれる。別の実施形態において、ネットワーク公開情報には、ルーティング情報、および／または、マネージドサーバが、ネットワークアドレス変換器（ＮＡＴ）の後方にあるかどうか（および、ＮＡＴの後方にある場合は、どのタイプのＮＡＴ、すなわち、１：１または１：Ｎ、であるのか）が含まれ

る。ＢＲＮは、組織内の、または組織を超えた、サブネットのセットであり、ＢＲＮ内のいずれのノードも、ＢＲＮ内の任意の他のノードとの通信を確立することができる。例えば、ＢＲＮ内のノードの全てが、一意ＩＰアドレスを有する。換言すると、ＢＲＮは、ＮＡＴを何も含まない。ネットワーク公開情報（例えば、ネットワークインターフェースのＢＲＮ識別子）は、ルールの条件部分と併せて使用されてよい。

【００３２】

サービス情報には、例えば、プロセス情報および／またはパッケージ情報が含まれる。プロセス情報には、例えば、マネージドサーバ１３０が実行中のプロセスの名称、どのネットワークポートおよびネットワークインターフェース上で、それらのプロセスがリスンしているのか、どのユーザがそれらのプロセスを起動したのか、それらのプロセスの構成、および、それらプロセスのコマンドラインｌａｕｎｃｈ引数が含まれる。（それらのプロセスは、マネージドサーバ１３０がサービスを提供すること、または、サービスを利用すること、に相当する。）パッケージ情報には、例えば、どのパッケージ（実行ファイル、ライブラリ、または他の構成要素）がマネージドサーバ１３０にインストールされるのか、それらのパッケージのバージョン、それらのパッケージの構成、および、それらのパッケージのハッシュ値が含まれる。

【００３３】

アンマネージドデバイス１４０の記述には、例えば、ネットワーク公開情報（例えば、アンマネージドデバイスのＩＰアドレス、および、アンマネージドデバイスが接続されるＢＲＮの識別子）が含まれる。アンマネージドデバイス１４０は、「アンマネージドデバイスグループ」（ＵＤＧ）の一部である。ＵＤＧには、１つまたは複数のアンマネージドデバイス１４０が含まれる。例えば、「本部ＵＤＧ」には、管理ドメインの本部によって使用される一次回路およびアックアップ回路が含まれてよく、各回路はＩＰアドレスに関連付けられる。ＵＤＧは、一意識別子（ＵＩＤ）に関連付けられる。ＵＤＧに関する管理ドメイン状態３２０内に記憶される情報には、ＵＤＧのＵＩＤ、およびＵＤＧ内のアンマネージドデバイス１４０に関する情報（例えば、アンマネージドデバイスのネットワーク公開情報）が含まれる。

【００３４】

マネージドサーバ１３０およびアンマネージドデバイス１４０の記述は、種々の方法で、例えば、グラフィカルユーザインターフェース（ＧＵＩ）またはアプリケーションプログラミングインターフェース（ＡＰＩ）を介して、グローバルマネージャ１２０と対話処理することにより、管理ドメイン状態３２０にロードされてよい。マネージドサーバ１３０の記述はまた、マネージドサーバから受け取るローカルステータス情報（以下で説明する）に基づき、管理ドメイン状態３２０にロードされてよい。

【００３５】

特にマネージドサーバのラベル（および、ある場合は、構成特徴）に関して、次元についての値の割り当て（または再割り当て）（または、構成特徴の値の設定）が、さらに多くの方法で実行されてよい。例えば、割り当て／設定は、マネージドサーバ１３０をプロビジョニングニングすることの一部として、展開および構成のツールを使用して実行されてよい。任意のそのようなツールが使用可能であり、既成のサードパーティのツール（例えば、Ｐｕｐｐｅｔ　Ｌａｂｓ社のＰｕｐｐｅｔというソフトウェア、Ｏｐｓｃｏｄｅ社のＣｈｅｆというソフトウェア、または、ＣＦＥｎｇｉｎｅ　ＡＳ社のＣＦＥｎｇｉｎｅというソフトウェア）、および、管理ドメイン１５０が有してよいカスタムツールが含まれる。

【００３６】

別の例として、割り当て／設定は、ラベルおよび／または構成特徴（「ＣＣ」）値を計算する「ラベル／構成特徴エンジン」（図示せず）によって実行されてよい。一実施形態において、ラベル／ＣＣエンジンが、ラベル／ＣＣ割り当てルールに基づき、ラベル／ＣＣ値を計算する。ラベル／ＣＣ割り当てルールは、管理ドメイン状態３２０からのデータにアクセスし、ラベルまたはＣＣ値を割り当てる（または、割り当てを示唆する）、機能

である。ラベル／ＣＣ割り当てルールは、プリセットまたはユーザ構成可能であってよい。例えば、グローバルマネージャ１２０には、あらかじめ定義されたルールのセットが含まれるが、エンドユーザは、それらのルールを修正および／または削除すること、および、ユーザ自身のカスタム要件に基づき、新しいルールを追加することができる。ラベル／ＣＣ割り当てルールは、初期化プロセス中に、マネージドサーバ１３０について評価されてよい。そして、ラベル／ＣＣ値の示唆は、任意の次元／ＣＣについてなされてよく、エンドユーザは、それらの示唆を受け入れても拒否してもよい。例えば、マネージドサーバ１３０が、Ｐｏｓｔｇｒｅｓデータベースまたは ＭｙＳＱＬデータベースを実行中である場合、示唆されたラベルは、＜役割，データベース＞であってよい。マネージドサーバが、Ｌｉｎｕｘオペレーティングシステムを実行中である場合、オペレーティングシステムについて示唆された値ＣＣは、「Ｌｉｎｕｘ」であってよい。

【００３７】

別の実施形態において、ラベル／ＣＣエンジンは、クラスタ分析に基づき、ラベル／ＣＣ値を計算する。例えば、ラベル／ＣＣエンジンは、追加の発見的問題解決法と共に、連結したグラフの、ｍｉｎ－ｃｕｔアルゴリズムおよびＫ－ｍｅａｎｓアルゴリズムの組み合わせを使用して、上位に接続されたマネージドサーバ１３０のクラスタを自動的に識別する。マネージドサーバ１３０のクラスタは、管理ドメイン１５０における「アプリケーション」（表１を参照）に相当し得る。エンドユーザは、アプリケーション次元（または、任意の他の次元）について値を、それらのマネージドサーバ１３０に、一斉に適用することを選択することができる。

【００３８】

管理ドメイン規模のマネージメントポリシー３３０には、１つまたは複数のルールが含まれる。大まかに言うと、「ルール」は、サービスの１つまたは複数のプロバイダと、そのサービスの１つまたは複数の消費者との間のリレーションシップを指定する。

【００３９】

ルール機能－リレーションシップは、ルールの実際の影響である、「ルール機能」に統轄される。例えば、セキュリティの場合、ルール機能は、アクセス制御、セキュア接続、ディスク暗号化、または、実行可能処理の制御であってよい。アクセス制御機能でのルールは、消費者が、プロバイダのサービスを使用できるかどうかを指定する。一実施形態において、アクセス制御機能は、純粋な「ホワイトリスト」モデルを使用し、これは、許容可能なリレーションシップのみが表現され、全ての他のリレーションシップが、デフォルトでブロックされる、ということを意味するセキュア接続機能でのルールは、どのセキュアなチャンネル上（例えば、２地点間データ暗号化を使用する、暗号化されたネットワークセッション）で、消費者がプロバイダのサービスを使用することができるのかを指定する。例えば、セキュア接続機能でのルールは、プロバイダが米国に置かれ、消費者がＥＵに置かれているときは、プロバイダのサービスの利用が暗号化されなければならない、ということを指定することができる。ディスク暗号化機能でのルールは、プロバイダが、そのデータを暗号化ファイルシステム上に記憶しなればならないかどうかを指定する。実行可能処理の制御機能でのルールは、プロバイダが、暗号化ファイルシステム上で実行しなければならないかどうかを指定する。

【００４０】

リソース利用の場合、ルール機能は、ディスク利用または周辺機器利用とすることができる。ディスク利用機能でのルールは、消費者がプロバイダ上に記憶可能なデータの量を指定する。ここで、ルールは、単なるアクセス制御、セキュア接続、ディスク暗号化、実行可能処理の制御、ディスク利用、および周辺機器利用を超えて、他のルール機能を指定することが可能である。例えば、ルール機能は、どの開放型システム間相互接続（ＯＳＩ）モデルの第７層のサービスを、ネットワークトラフィック、セキュリティ分析のための収集すべきメタデータの量、または、完全なネットワークパケットを取得するためのトリガに適用するのかを指定する。マネージメントポリシーモデルは、適用可能な任意の数のルール機能をサポートする。

【００４１】
ルール機能は、ルールの実際の影響に関する詳細を指定する、１つまたは複数の設定（本明細書においては「機能プロファイル」と称する）に関連付けられてよい。例えば、セキュア接続のルール機能に関連する設定は、ネットワークトラフィックの暗号化に使用される暗号アルゴリズムのリストであってよい。一実施形態において、ルール機能は、複数の機能プロファイルに関連付けられ、機能プロファイルには優先度が含まれる。この優先度は、以下で説明するように、機能レベル命令生成モジュール３６０によって使用される。
【００４２】
サービス－ 一般に、「サービス」は、指定のネットワークポート上で、指定のネットワークプロトコルを使用して、実行される任意のプロセスである。マネージメントポリシー３３０内のルールのサービスは、ポート／プロトコルの対と、プロセス情報および／またはパッケージ情報（管理ドメイン状態３２０内のマネージドサーバ１３０の記述について、上記で説明した）などの、（選択的）追加の適正とによって指定される。マネージドサーバ１３０が、複数のネットワークインターフェースを有する場合、サービスを、全てのネットワーク上、または、それらのネットワークのサブセット上のみに、公開させることができる。エンドユーザは、どのネットワーク上に、サービスを公開させるかを指定することができる。
【００４３】
プロバイダ／消費者－サービスの１つまたは複数のプロバイダ、および、サービスの１つまたは複数の消費者（すなわち、ユーザ）は、マネージドサーバ１３０および／またはアンマネージドデバイス１４０である。
【００４４】
一実施形態において、ルールは、ルール機能部分、サービス部分、提供元部分、使用元部分、および選択的ルール条件部分を含む情報のセットを使用して、管理ドメイン規模のマネージメントポリシー３３０内に表される。ルール機能部分は、ルールの実際の影響を記述し、１つまたは複数の設定（機能プロファイル）に関連付けられてよい。サービス部分は、ルールが適用されるサービスを記述する。サービス部分が「Ａｌｌ（全て）」を示す場合、ルールは全てのサービスに適用される。
【００４５】
提供元（ＰＢ）部分は、どのマネージドサーバ１３０および／またはアンマネージドデバイス１４０が、サービスを提供可能であるか（すなわち、誰が「プロバイダ」なのか）を記述する。ＰＢ部分が「Ａｎｙｂｏｄｙ（誰でも）」を示す場合、誰でも（例えば、任意のマネージドサーバ１３０またはアンマネージドデバイス１４０）、サービスを提供することが可能である。ＰＢ部分が「Ａｎｙ ｍａｎａｇｅｄ ｓｅｒｖｅｒ（どのマネージドサーバでも）」を示す場合、どのマネージドサーバ１３０でも、サービスを提供することが可能である。（「Ａｎｙ ｍａｎａｇｅｄ ｓｅｒｖｅｒ」は、ワイルドカードを含むラベルセットを指定することと等価であり、それによって、全てのマネージドサーバ１３０をマッチングする）。使用元（ＵＢ）部分は、どのマネージドサーバ１３０および／またはアンマネージドデバイス１４０が、サービスを使用可能であるか（すなわち、誰が「消費者」であるのか）を記述する。ＰＢ部分と同様に、ＵＢ部分は、「Ａｎｙｂｏｄｙ」または「Ａｎｙ ｍａｎａｇｅｄ ｓｅｒｖｅｒ」を示すこともできる。
【００４６】
ＰＢ部分およびＵＢ部分内には、マネージドサーバ１３０が、ラベルセット（すなわち、マネージドサーバを記述する１つまたは複数のラベル）またはＵＩＤを使用することにより、指定される。ラベルセットを使用してマネージドサーバ１３０を指定する機能は、論理的マネージメントモデルに由来するもので、マネージドサーバを、その次元および値（ラベル）に基づき参照する。アンマネージドデバイス１４０は、アンマネージドデバイスグループ（ＵＤＧ）のＵＩＤを使用することにより指定される。ルールがＵＤＧを指定する場合、ルールには、そのグループ内のアンマネージドデバイス１４０に関する追加情

報（例えば、デバイスのネットワーク公開情報）が含まれる。ルールのＰＢ部分および／またはルールのＵＢ部分には、ラベルセット（マネージドサーバ１３０を指定するための）、マネージドサーバのＵＩＤ、および／またはＵＤＧのＵＩＤを含む複数の項目が含まれてよい。

【００４７】

ルール条件部分は、選択的なものであり、ルールが、特定のマネージドサーバ１３０、および／または、そのマネージドサーバの特定のネットワークインターフェースに適用されるかどうかを指定する。ルール条件部分は、１つまたは複数の構成特徴（「ＣＣ」；管理ドメイン状態３２０内のマネージドサーバの記述の一部である）、および／または、ネットワーク公開情報（例えば、ネットワークインターフェースのＢＲＮ識別子、これも管理ドメイン状態３２０内のマネージドサーバの記述の一部）を含む、ブール式である。式のＣＣ部分は、ルールが、特定のマネージドサーバに適用されるかどうかを指定し、一方、ネットワーク公開情報部分は、ルールが、そのマネージドサーバの特定のネットワークインターフェースに適用されるかどうかを指定する。式が、特定のマネージドサーバの構成特徴について（詳細には、そのマネージドサーバの構成特徴の値について）、および、特定のネットワークインターフェースの情報について、「真」と評価する場合、ルールは、そのマネージドサーバ、および、そのマネージドサーバの関連ネットワークインターフェースに適用される。式が「偽」と評価する場合、ルールは、そのマネージドサーバ、および、そのマネージドサーバの関連ネットワークインターフェースには適用されない。例えば、構成特徴が、どのオペレーティングシステムがマネージドサーバ上で実行中であるかの指標を記憶する場合、その構成特徴を含むルール条件部分は、ルールが特定のマネージドサーバに適用されるかどうかを、そのサーバのオペレーティングシステムに基づき、制御することができる。

【００４８】

管理ドメイン規模のマネージメントポリシー３３０内のルールは、ルールリストとして編成される。詳細には、マネージメントポリシー３３０には、１つまたは複数のルールリストが含まれ、ルールリストには、１つまたは複数のルールと、（選択的に）１つまたは複数のスコープとが含まれる。「スコープ」は、どこに（すなわち、どのマネージドサーバ１３０に）ルールが適用されるのかを制約する。スコープには、ルールリスト内のルールの適用を制限する、提供元（ＰＢ）部分および使用元（ＵＢ）部分が含まれる。スコープのＰＢ部分はルールのＰＢ部分を制限し、スコープのＵＢ部分はルールのＵＢ部分を制限する。スコープのＰＢ部分およびＵＢ部分は、マネージドサーバ１３０のグループを、ラベルセットを使用することにより指定する。ラベルセットが、指定の次元のラベルを含まない場合、結果として得られるマネージドサーバ１３０のグループについて、その次元のスコーピングが無い。ルールリストが、何のスコープも含まない場合、そのルールはグローバルに適用される。

【００４９】

異なるスコープが、単一のルールリストに適用されてよい。例えば、エンドユーザは、どのように、ウェブサービス層が、データベース層からサービスを消費するのか、どのように、ロードバランシング層が、ウェブサービス層からサービスを消費するのか、などを表現するルールのセットを構築することができる。そして、エンドユーザが、このルールリストを自分のプロダクション環境および自分のステージング環境に適用したい場合、エンドユーザは、ルールリストをコピーも複製もする必要が無い。代わりに、エンドユーザは、複数のスコープを単一のルールリストに適用する。スコープの抽象化により、有用性の観点および計算の観点の両方から、ルールリストが拡大／縮小される。

【００５０】

ここで、管理ドメイン規模のマネージメントポリシー３３０が、記述されていることは、いくつかの例に対処することに役立つ。ユーザデバイスがウェブサーバ（第１の層）にアクセスし、ウェブサーバがデータベースサーバ（第２の層）にアクセスする、２層アプリケーションを用いる管理ドメイン１５０について検討する。第１の層において、ユーザ

デバイスは消費者であり、ウェブサーバはプロバイダである。第２の層において、ウェブサーバは消費者であり、データベースサーバはプロバイダである。管理ドメイン１５０には、このアプリケーションの２つのインスタンスが含まれ、１つはプロダクション環境内、１つはステージング環境内にある。

【００５１】

ウェブサーバおよびデータベースサーバは、マネージドサーバ１３０であり、それらの記述（例えば、ラベルセット）は管理ドメイン状態３２０内に存在する。例えば、それらのラベルセットは、

プロダクションにおけるウェブサーバ：＜役割，ウェブ＞および＜環境，プロダクション＞

プロダクションにおけるデータベースサーバ：＜役割，データベース＞および＜環境，プロダクション＞

ステージングにおけるウェブサーバ：＜役割，ウェブ＞および＜環境，ステージング＞

ステージングにおけるデータベースサーバ：＜役割，データベース＞および＜環境，ステージング＞

（アプリケーション次元、業種次元、およびロケーション次元は、この例に関連しないため、それらのラベルは省略する。）

【００５２】

ここで、アクセス制御およびセキュア接続を指定するセキュリティポリシーである、以下の管理ドメイン規模のマネージメントポリシー３３０について検討する。

ルールリスト＃１

・スコープ

○＜環境，プロダクション＞

○＜環境，ステージング＞

・ルール

○＃１

●機能：アクセス制御

●サービス：アパッチ

●ＰＢ：＜役割，ウェブ＞

●ＵＢ：Ａｎｙｂｏｄｙ

○＃２

●機能：アクセス制御

●サービス：ＰｏｓｔｇｒｅＳＱＬ

●ＰＢ：＜役割，データベース＞

●ＵＢ：＜役割，ウェブ＞

ルールリスト＃２

・スコープ：無

・ルール

○＃１

●機能：セキュア接続

●サービス：Ａｌｌ

●ＰＢ：＜役割，データベース＞

●ＵＢ：Ａｎｙ　ｍａｎａｇｅｄ　ｓｅｒｖｅｒ

【００５３】

なお、上記のルールは、明確にするために、単に「アパッチ」および「ＰｏｓｔｇｒｅＳＱＬ」として、サービスを参照する。サービスが、プロセスであり、ポート／プロトコルの対と、プロセス情報および／またはパッケージ情報（管理ドメイン状態３２０内のマネージドサーバ１３０の記述について、上記で説明した）などの、（選択的）追加の適正、によって指定されるということを、思い出されたい。

【００５４】

ルールリスト＃１／ルール＃１では、任意のデバイス（例えば、ユーザデバイス）が、ウェブサーバに接続して、アパッチサービスを使用することが許可される。詳細には、接続の許可が、機能部分の「アクセス制御」によって指定される。「任意のデバイス」が、ＵＢ部分の「Ａｎｙｂｏｄｙ」によって指定される。「ウェブサーバ」が、ＰＢ部分の「＜役割，ウェブ＞」（１つのラベルのみを含むラベルセット）によって指定される。アパッチサービスが、サービス部分の「アパッチ」によって指定される。

【００５５】

ルールリスト＃１／ルール＃２では、ウェブサーバが、データベースサーバ上のＰｏｓｔｇｒｅＳＱＬに接続することが許可される。詳細には、接続の許可が、機能部分の「アクセス制御」によって指定される。「ウェブサーバ」が、ＵＢ部分の「＜役割，ウェブ＞」によって指定される。「ＰｏｓｔｇｒｅＳＱＬ」が、サービス部分の「ＰｏｓｔｇｒｅＳＱＬ」によって指定される。「データベースサーバ」が、ＰＢ部分の「＜役割，データベース＞」（１つのラベルのみを含むラベルセット）によって指定される。

【００５６】

ルールリスト＃１ではまた、環境間の接続を防ぐ。例えば、ウェブサーバとデータベースサーバとの両方が、同じ環境内にある場合（例えば、両方ともプロダクション環境内にある、または、両方ともステージング環境内にある）、ウェブサーバは、データベースサーバ上のＰｏｓｔｇｒｅＳＱＬに接続することが許可される。プロダクション環境内の両サーバは、スコープ部分の＜環境，プロダクション＞」（１つのラベルのみを含むラベルセット）によって指定され、一方、ステージング環境内の両サーバは、スコープ部分の「＜環境，ステージング＞」（１つのラベルのみを含むラベルセット）によって指定される。その結果、サーバが、異なる環境内にある場合（例えば、ウェブサーバがステージング環境内にあり、データベースサーバがプロダクション環境内にある場合）は、ウェブサーバは、データベースサーバ上のＰｏｓｔｇｒｅＳＱＬにアクセスすることが許可されない。

【００５７】

ルールリスト＃２は、任意のマネージドサーバが、データベースサーバに接続するときはいつでも、その接続が暗号化されたチャンネルを介して実行されなければならない、ということを提示する。詳細には、「データベースサーバ」が、ＰＢ部分の」＜役割，データベース＞」によって指定される。「暗号化されたチャンネル」が、機能部分の「セキュア接続」によって指定される。「任意のマネージドサーバ」が、ＵＢ部分の「Ａｎｙ ｍａｎａｇｅｄ ｓｅｒｖｅｒ」によって指定される。「いつでも」が、サービス部分の「Ａｌｌ」によって指定される。

【００５８】

上記の例から離れて、以下の２つのマネージドサーバ１３０について検討する。サーバ１は、プロダクションの一部であり、ａｐｐ１の一部であり、カリフォルニアのエンジニアリングが所有するウェブサーバである。以下のようにラベル付けされる。

＜役割，ウェブ＞
＜環境，プロダクション＞
＜アプリケーション，ａｐｐ１＞
＜業種，エンジニアリング＞
＜ロケーション，ＵＳ＞

サーバ２は、プロダクションの一部であり、ａｐｐ１の一部でもあり、ドイツのエンジニアリングが所有するデータベースサーバである。以下のようにラベル付けされる。

＜役割，データベースサーバ＞
＜環境，プロダクション＞
＜アプリケーション，ａｐｐ１＞
＜業種，エンジニアリング＞
＜ロケーション，ＥＵ＞

【００５９】

アクセス制御ルールが、ａｐｐ１の一部である全てのマネージドサーバ１３０への全てのアクセスを許可すると仮定する。このルールでは、サーバ１とサーバ２とが互いに通信することが許可され、ａｐｐ２の一部であるドイツのマネージドサーバ１３０がサーバ１またはサーバ２と通信することが許可されない。ここで、セキュア接続ルールが、ＥＵとＵＳとの間の全てのネットワークトラフィックは、暗号化されなければならないことを指定すると仮定する。ルール機能は、単独で適用される。換言すると、セキュア接続ルールは、アクセス制御ルールとは無関係に適用される別個のポリシーである。その結果、サーバ１からサーバ２へのネットワークトラフィックが、許可されて（アクセス制御ルールが与えられて）、暗号化される（セキュア接続ルールが与えられる）。

【００６０】

図３に戻って、プロセシングサーバ３１０は、マネージドサーバ１３０用のマネージメント命令を生成して、生成したマネージメント命令をサーバに送る。プロセシングサーバ３１０はまた、マネージドサーバ１３０から受け取るローカル状態情報を処理する。プロセシングサーバ３１０には、ポリシーエンジンモジュール３４０、関連ルールモジュール３５０、機能レベル命令生成モジュール３６０、アクターエニュメレーションモジュール３７０、関連アクターモジュール３８０、および、管理ドメイン状態更新モジュール３８５などの種々のモジュールが含まれる。一実施形態において、プロセシングサーバ３１０には、リポジトリ３００と通信して、データを（例えば、ポリシーエンジンモジュール３４０、関連ルールモジュール３５０、機能レベル命令生成モジュール３６０、アクターエニュメレーションモジュール３７０、関連アクターモジュール３８０、および管理ドメイン状態更新モジュール３８５を実行することにより）処理するコンピュータ（またはコンピュータのセット）が含まれる。

【００６１】

関連ルールモジュール３５０は、管理ドメイン規模のマネージメントポリシー３３０と、特定のマネージドサーバ１３０の指標（例えば、そのサーバのＵＩＤ）とを入力として取り込み、そのサーバに関連するルールのセットを生成し、ルールのセットを出力する。これは、関連ルールモジュール３５０が、マネージメントポリシー３３０を検査して、所与のマネージドサーバ１３０用の関連ルールのみを抽出するために用いる、フィルタリングプロセスである。関連ルールモジュール３５０は、フィルタリングの実行を、マネージメントポリシー３３０内のルールリストの全てを反復すること、各ルールリストのスコープを分析して、スコープがこのマネージドサーバ１３０に適用されるかどうかを判定すること、および（スコープがこのマネージドサーバ１３０に適用される場合）各ルールリストのルールを分析して、それらのルールがこのマネージドサーバ１３０に適用されるかどうかを判定することによって行う。ルールがマネージドサーバ１３０に適用されるのは、ａ）ルールのＰＢ部分および／またはルールのＵＢ部分が、マネージドサーバを指定する場合、および、ｂ）ルールの条件部分（存在する場合）が、そのマネージドサーバについて（詳細には、マネージドサーバの構成特徴の値およびネットワーク公開情報について）、「真」となる場合である。最終結果（本明細書において、マネージメントポリシー観点」と称する）は、２セットのルールのコレクションであり、１つは、このマネージドサーバ１３０がサービスを提供するルール、１つは、このマネージドサーバ１３０がサービスを消費するルールである。

【００６２】

機能レベル命令生成モジュール３６０は、ルールのセット（例えば、関連ルールモジュール３５０により生成されるマネージメントポリシー観点）を入力として取り込み、機能レベルの命令を生成し、その機能レベルの命令を出力する。機能レベルの命令は、後で、マネージメント命令の一部としてマネージドサーバ１３０に送られる。機能レベルの命令は、それぞれが、ルール機能部分、サービス部分、ＰＢ部分、およびＵＢ部分を含むという点で、ルールに類似する。しかし、ルールが、そのＰＢ部分および／またはＵＢ部分内に複数の項目（ラベルセット、マネージドサーバＵＩＤ、および／または、ＵＤＧのＵＩＤを含む）を含むことができる一方、機能レベルの命令は、そのＰＢ部分内に１項目のみ

、およびそのＵＢ部分に１項目のみしか含まない。また、ルールが、そのＰＢ部分および／またはＵＢ部分内に、マネージドサーバ（その複数のネットワークインターフェースを含む）を指定することができる一方、機能レベルの命令は、そのＰＢ部分およびＵＢ部分内に、１つのネットワークインターフェースのみしか含まない。

【００６３】

機能レベル命令生成モジュール３６０は、ルールを分析し、そのルールに基づき１つまたは複数の機能レベルの命令を生成する。ルールのＰＢ部分が、複数の項目を含む場合、ルールのＵＢ部分が、複数の項目を含む場合、または、ルール（ＰＢ部分またはＵＢ部分）により参照されるマネージドサーバが、複数のネットワークインターフェースを有する場合、機能レベル命令生成モジュール３６０は、複数の機能レベルの命令（例えば、ＰＢ項目、ＵＢ項目、および特定のネットワークインターフェースの、可能な組み合わせごとに１つの機能レベルの命令）を生成する。

【００６４】

ＰＢ部分に２つの項目（ＡおよびＢ）、ならびに、ＵＢ部分に２つの項目（ＣおよびＤ）を含むルールについて検討する。機能レベル命令生成モジュール３６０は、以下のＰＢ部分およびＵＢ部分を用いて４つの機能レベルの命令を生成する。１）ＰＢ＝Ａ、ＵＢ＝Ｃ；２）ＰＢ＝Ａ、ＵＢ＝Ｄ；３）ＰＢ＝Ｂ、ＵＢ＝Ｃ；４）ＰＢ＝Ｂ、ＵＢ＝Ｄ。ここで、ＰＢ部分またはＵＢ部分でマネージドサーバをカバーするルール（例えば、ＵＩＤまたはラベルセットを指定することにより）であって、そのマネージドサーバが複数のネットワークインターフェースを有する場合を検討する。機能レベル命令生成モジュール３６０は、複数の機能レベルの命令（例えば、マネージドサーバのネットワークインターフェースごとに１つの機能レベルの命令）を生成する。

【００６５】

機能レベル命令生成モジュール３６０は、ルール、それらのルール内の機能、および、それらのルールにより参照される機能プロファイルを分析する。ルールリストに、複数のスコープが含まれる場合、機能レベル命令生成モジュール３６０は、それらのスコープをルールリストに、複数回繰り返し適用する（それによって、スコープごとに機能レベルの命令の完全なセットを生成する）。ルール機能が、複数の機能プロファイルに関連付けられてよいこと、および、機能プロファイルが優先度を含むことができることを思い出されたい。機能レベル命令生成モジュール３６０は、種々の機能プロファイルの優先度に基づきルールを順序付けて、優先度の最も高い機能プロファイルが使用されるようにする。機能レベル命令生成モジュール３６０は、順序付けされたルールを、マネージドサーバ１３０が実行できるように、機能レベルの命令に変換する。機能レベルの命令は、適切なマネージドサーバ１３０および／またはアンマネージドデバイス１４０（例えば、入力されたルールにおいて参照されたマネージドサーバ１３０および／またはアンマネージドデバイス１４０）を参照し、ルールに関連するサービスのネットワーク公開の詳細を考慮に入れる。

【００６６】

ここで、機能レベル命令生成モジュール３６０は、特定のマネージドサーバ１３０用の機能レベルの命令を生成することができるが、該命令は、そのサーバには無意味なものとなる。例えば、そのマネージドサーバが、ルールの提供元（ＰＢ）部分によりカバーされ、そのため、機能レベル命令生成モジュール３６０が、対応する機能レベルの命令を生成する。しかし、ルールには、マネージドサーバのローカル状態を指定する部分も含まれる（例えば、提供されるサービスを記述するサービス部分）。グローバルマネージャ１２０には、マネージドサーバのローカル状態（例えば、マネージドサーバが実際にそのサービスを提供中であるかどうか）が分からないため、生成された機能レベルの命令がマネージドサーバに送られる。マネージドサーバは、そのローカル状態をチェックし（例えば、そのサービスを提供中であるかどうか）、それに従って、ポリシーコンパイルモジュール４１０を参照して以下で説明するように、機能レベルの命令を処理する。

【００６７】

アクターエニュメレーションモジュール３７０は、マネージドサーバ１３０およびアンマネージドデバイスグループ（ＵＤＧ）の記述（例えば、管理ドメインのコンピュータネットワークインフラの状態３２０）のコレクションを入力として取り込み、サーバおよびＵＤＧのそれらの記述の表現を、エニュメレート（列挙）された形式（「アクターセット」と称する）で生成し、アクターセットを出力する。例えば、アクターエニュメレーションモジュール３７０は、マネージドサーバ１３０およびＵＤＧを、管理ドメイン状態３２０および可能性のあるラベルセット内にエニュメレートし、それぞれに一意識別子（ＵＩＤ）を割り当てる。これらのアクターセットは、次に、ルールおよびスコープの、ＵＢ部分およびＰＢ部分、と併せて使用されてよく、これにより、マネージドサーバのＵＩＤ、ＵＤＧのＵＩＤ、および／または、ラベルセットを使用して、アクターを指定する。

【００６８】

Ｎ個の次元D_i（ｉ＝１，．．．，Ｎ）の集合を含み、各次元D_iが、可能性ある値V_j（ｊ＝１，．．．，Ｍｉ）の集合S_iを含む（ここで、ワイルドカード「＊」は可能性のある値のうちの１つである）、論理的マネージメントモデルについて検討する。一実施形態において、アクターエニュメレーションモジュール３７０は、論理的マネージメントモデルに基づき可能性のある全てのラベルセットをエニュメレートし、これは、$S_1 \times S_2 \times \ldots \times S_N$で得られるデカルト積に等しい。この集合のサイズは$M_1 \times M_2 \times \ldots \times M_N$である。エニュメレーションプロセスでは、マネージドサーバ１３０の多次元ラベル空間を、単純なエニュメレートされた形式に縮約する。

【００６９】

別の実施形態において、アクターエニュメレーションモジュール３７０は、管理ドメイン状態３２０に基づき（例えば、管理ドメイン１５０内のマネージドサーバの記述に基づき）可能性のあるラベルセットだけをエニュメレートする。例えば、２つの次元（ＸおよびＹ）を含み、各次元が３つの可能性のある値（Ａ、Ｂ、および＊）を含む、論理的マネージメントモデルについて検討する。ラベルセット「＜Ｘ＝Ａ＞，＜Ｙ＝Ｂ＞」を持つマネージドサーバは、以下の４つの可能性のあるラベルセットのうちのメンバーであり得る。１）「＜Ｘ＝Ａ＞，＜Ｙ＝Ｂ＞」、２）「＜Ｘ＝Ａ＞，＜Ｙ＝＊＞」、３）「＜Ｘ＝＊＞，＜Ｙ＝Ｂ＞」、および、４）「＜Ｘ＝＊＞，＜Ｙ＝＊＞」。ここで、マネージドサーバのラベルセットは、二次元空間（ＸおよびＹ）に存在し、一方、可能性のあるラベルセット２、３、および４は、マネージドサーバのラベルセットの、サブ次元空間への投影である（ラベルセット２は一次元空間（Ｘ）、ラベルセット３は一次元空間（Ｙ）、ラベルセット４は０次元空間）。それ故、アクターエニュメレーションモジュール３７０は、それら４つの可能性のあるラベルセットをエニュメレートする。ラベルセット「＜Ｘ＝Ａ＞，＜Ｙ＝Ｂ＞」を持つマネージドサーバが、ラベルセット「＜Ｘ＝Ａ＞，＜Ｙ＝Ａ＞」のメンバーであることはなく、そのため、アクターエニュメレーションモジュール３７０は、そのラベルセットをエニュメレートしない。

【００７０】

アクターセットには、ＵＩＤおよび、ゼロ個またはそれ以上のアクターセットレコードが含まれる。アクターセットレコードには、ＵＩＤ（マネージドサーバのＵＩＤまたはＵＤＧのＵＩＤのいずれか）、アクターのオペレーティングシステムの識別子、および、指定のＢＲＮが与えられたアクター（マネージドサーバ１３０またはアンマネージドデバイス１４０）のＩＰアドレスが含まれる。例えば、アクターセットには、＜役割，データベース＞および＜環境，プロダクション＞のラベルセットによりカバーされるマネージドサーバ１３０の全てに対応するＩＰアドレスを持つ、アクターセットレコードが含まれてよい。別の例として、アクターセットには、本部ＵＤＧにおけるアンマネージドデバイス１４０の全てに対応するＩＰアドレスを持つ、アクターセットレコードが含まれてよい。単一のアクター（例えば、マネージドサーバ１３０またはアンマネージドデバイス１４０）が、複数のアクターセット内に見られてよい。

【００７１】

アクターセット計算における別の要因は、複数のネットワークインターフェースを持つ

アクターと、ネットワークアドレス変換器（ＮＡＴ）などのネットワークトポロジを含むことである。従って、＜役割，データベース＞および＜環境，プロダクション＞のラベルセットついて２つのアクターセットがあり得、１つのアクターセットが、それらマネージドサーバ１３０のインターネットに接続するＩＰアドレス（すなわち、第１のＢＲＮに関連する）を持ち、それら同じマネージドサーバ用の異なるアクターセットが、それらマネージドサーバのプライベートネットワークに接続するＩＰアドレス（すなわち、第２のＢＲＮに関連する）を持つ。

【００７２】

一実施形態において、アクターエニュメレーションモジュール３７０は、管理ドメインの状態３２０に対する変更に基づき、アクターセットを更新することもできる。例えば、アクターエニュメレーションモジュール３７０は、アクターセット（以前、アクターエニュメレーションモジュールによって出力された）、および、マネージドサーバの記述（管理ドメイン状態３２０内の）に対する変更を入力として取り込み、更新されたアクターセット（変更されたサーバ記述と一致する）を生成し、更新されたアクターセットを出力する。アクターエニュメレーションモジュール３７０は、マネージドサーバの記述に対する変更のタイプに応じた異なる方法で、更新されたアクターセットを生成する。

【００７３】

オフライン／オンラインの変更－記述変更が、サーバがオンラインからオフラインになったことを示す場合、アクターエニュメレーションモジュール３７０は、サーバのアクターセットレコードを、サーバがメンバーだった全ての入力アクターセットから削除することにより、更新されたアクターセットを生成する。記述変更が、サーバがオフラインからオンラインになったことを示す場合、アクターエニュメレーションモジュール３７０は、サーバのアクターセットレコードを、任意の関連する入力アクターセットに追加することにより、更新されたアクターセットを生成する。（必要に応じて、アクターエニュメレーションモジュール３７０は、新しいアクターセットを作成し、サーバのアクターセットレコードをその新しいアクターセットに追加する。）

【００７４】

ラベルセットの変更－記述変更が、サーバのラベルセットが変更されたことを示す場合、アクターエニュメレーションモジュール３７０は、これを、第１のサーバ（古いラベルセットを持つ）がオフラインになり、第２のサーバ（新しいラベルセットを持つ）がオンラインになる、というように扱う。

【００７５】

ネットワーク公開情報の変更－記述変更が、サーバがネットワークインターフェースを削除したことを示す場合、アクターエニュメレーションモジュール３７０は、サーバのアクターセットレコードを、サーバがメンバーだった全ての入力アクターセット（そのネットワークインターフェースのＢＲＮに関連する）から削除することにより、更新されたアクターセットを生成する。記述変更が、サーバがネットワークインターフェースを追加したことを示す場合、アクターエニュメレーションモジュール３７０は、サーバのアクターセットレコードを、任意の関連する入力アクターセット（そのネットワークインターフェースのＢＲＮに関連する）に追加することにより、更新されたアクターセットを生成する。（必要に応じて、アクターエニュメレーションモジュール３７０は、新しいアクターセット（そのネットワークインターフェースのＢＲＮに関連する）を作成し、サーバのアクターセットレコードをその新しいアクターセットに追加する。）記述変更が、サーバがネットワークインターフェースのＢＲＮを変更したことを示す場合、アクターエニュメレーションモジュール３７０は、これを、第１のネットワークインターフェース（古いＢＲＮを持つ）が削除され、第２のネットワークインターフェース（新しいＢＲＮを持つ）が追加される、というように扱う。記述変更が、サーバがネットワークインターフェースのＩＰアドレス（ＢＲＮではなく）を変更したことを示す場合、アクターエニュメレーションモジュール３７０は、サーバがメンバーだった全ての入力アクターセット（そのネットワークインターフェースのＢＲＮに関連する）内のサーバのアクターセットレコードを修正

することにより、更新されたアクターセットを生成する。
【００７６】
関連アクターモジュール３８０は、１つまたは複数のアクターセット（例えば、管理ドメイン状態３２０内の、エニュメレートされた形式のマネージドサーバ１３０およびＵＤＧ）と、ルールのセット（例えば、マネージメントポリシー観点）と、を入力として取り込み、どのアクターセットが、それらのルールに関連するのかを判定し、それらのアクターセットのみを出力する。これは、関連アクターモジュール３８０が、アクターセットを検査して、所与のルールのセット用の関連アクターセットのみを抽出するために用いる、フィルタリングプロセスである。関連アクターモジュール３８０は、フィルタリングの実行を、入力アクターセットの全てを反復すること、および、入力されたルールのＰＢ部分およびＵＢ部分を分析して、特定のアクターセットが、ルールのＰＢ部分またはＵＢ部分のいずれかによって参照されるかどうかを判定することによって行う。最終結果（本明細書において、「アクター観点」と称する）は、アクターセットのコレクションである。アクター観点は、後で、マネージメント命令の一部としてマネージドサーバ１３０に送られる。
【００７７】
一実施形態において、関連アクターモジュール３８０は、入力されたルールのセットを使用して、「アクターセットフィルタ」を生成する。アクターセットフィルタは、入力アクターセットから、入力されたルールに関連するアクターセットのみを選択する。換言すると、関連アクターモジュール３８０は、アクターセットフィルタを使用して、入力アクターセットをフィルタリングして関連アクターセットにする。
【００７８】
ポリシーエンジンモジュール３４０は、マネージドサーバ１３０用のマネージメント命令を生成して、生成したマネージメント命令をサーバに送る。ポリシーエンジンモジュール３４０は、ａ）管理ドメインのコンピュータネットワークインフラの状態３２０、および、ｂ）管理ドメイン規模のマネージメントポリシー３３０に基づき、（関連ルールモジュール３５０、機能レベル命令成モジュール３６０、アクターエニュメレーションモジュール３７０、および関連アクターモジュール３８０を用いて）マネージメント命令を生成する。
【００７９】
例えば、ポリシーエンジンモジュール３４０は、関連ルールモジュール３５０を実行して、管理ドメイン規模のマネージメントポリシー３３０と、特定のマネージドサーバ１３０のＵＩＤとを入力として提供する。関連ルールモジュール３５０は、そのサーバに関連するルールのセット（「マネージメントポリシー観点」）を出力する。ポリシーエンジンモジュール３４０は、アクターエニュメレーションモジュール３７０を実行して、管理ドメイン状態３２０を入力として提供する。アクターエニュメレーションモジュール３７０は、管理ドメイン状態３２０内のエニュメレートされた形式の、マネージドサーバ１３０およびアンマネージドデバイスグループ（ＵＤＧ）の記述の表現（「アクターセット」）を出力する。ポリシーエンジンモジュール３４０は、機能レベル命令生成モジュール３６０を実行して、マネージメントポリシー観点（関連ルールモジュール３５０によって出力された）を、入力として提供する。機能レベル命令生成モジュール３６０は、機能レベルの命令を出力する。ポリシーエンジンモジュール３４０は、関連アクターモジュール３８０を実行して、アクターセット（エニュメレーションモジュール３７０により出力された）と、マネージメントポリシー観点（関連ルールモジュール３５０により出力された）と、を入力として提供する。関連アクターモジュール３８０は、それらのルールに関連するアクターセット（「関連アクターセット」）のみを出力する。ポリシーエンジンモジュール３４０は、機能レベルの命令（機能レベル命令生成モジュール３６０により出力された）と、関連アクターセット（関連アクターモジュール３８０により出力された）とを、特定のマネージドサーバ１３０に送る。
【００８０】

一実施形態において、ポリシーエンジンモジュール３４０は、上記のプロセスの間に生成された情報をキャッシュする。例えば、ポリシーエンジンモジュール３４０は、特定のマネージドサーバ１３０に関連して、マネージメントポリシー観点、機能レベルの命令、アクターセットフィルタ、および／または関連アクターセットをキャッシュする。別の例として、ポリシーエンジンモジュール３４０は、（特定のマネージドサーバ１３０に特有でない）アクターセットをキャッシュする。

【００８１】

管理ドメインのアクターセットは、管理ドメイン状態３２０に基づくため、管理ドメイン状態３２０に対する変更により、管理ドメインのアクターセットに対する変更を要求することができる。同様に、マネージドサーバのマネージメント命令は、管理ドメイン状態３２０および管理ドメイン規模のマネージメントポリシー３３０に基づくため、管理ドメイン状態３２０に対する変更および／または管理ドメイン規模のマネージメントポリシー３３０に対する変更により、マネージドサーバのマネージメント命令に対する変更を要求することができる。一実施形態において、ポリシーエンジンモジュール３４０は、管理ドメインのアクターセットを更新すること、および／または、マネージドサーバのマネージメント命令を更新することができ、これらの変更を（必要に応じて）マネージドサーバ１３０に配布することができる。上記で言及したキャッシュされた情報は、ポリシーエンジンモジュール３４０が、管理ドメインのアクターセットおよび／またはマネージドサーバのマネージメント命令を、より効率的に更新して、変更を分配することに役立つ。

【００８２】

一実施形態において、ポリシーエンジンモジュール３４０は、以下のように、管理ドメインのアクターセットを更新し（管理ドメイン状態３２０に対する変更に基づき）、変更をマネージドサーバ１３０に分配する。ポリシーエンジンモジュール３４０は、アクターエニュメレーションモジュール３７０を実行して、（以前、アクターエニュメレーションモジュールに出力された）キャッシュされたアクターセットと、管理ドメイン状態３２０の変更された部分（すなわち、変更されたサーバ記述）とを入力として提供する。アクターエニュメレーションモジュール３７０は、更新されたアクターセットを出力する。一実施形態において、ポリシーエンジンモジュール３４０は、次に、更新されたアクターセットの全てを、管理ドメイン１５０内のマネージドサーバ１３０の全てに送る。ただし、その実施形態は効率的ではなく、それは、全てのアクターセットに対する変更によって、全てのマネージドサーバが影響を受けるわけではないからである。

【００８３】

別の実施形態において、選択されたアクターセットのみが、選択されたサーバに送られる。例えば、特定のマネージドサーバには、ａ）以前に、そのサーバに送られたアクターセット、および、ｂ）変更されているアクターセットのみが送られる。キャッシュされた関連アクターセットは、どのアクターセットがそのサーバに以前送られたのかを示す（上記（ａ）を参照のこと）。ポリシーエンジンモジュール３４０は、キャッシュされたアクターセットを、更新されたアクターセットと比較して、どのアクターセットが変更されているかを判定する（上記（ｂ）を参照のこと）。そして、ポリシーエンジンモジュール３４０は、（ａ）と（ｂ）との共通部分を計算する。その共通部分のアクターセットが、特定のマネージドサーバに送られる。一実施形態において、さらに効率を上げるために、アクターセットが「ｄｉｆｆ」形式で送られる。例えば、ｄｉｆｆ形式は、アクターセット識別子、アクター識別子（例えば、マネージドサーバのＵＩＤまたはＵＤＧのＵＩＤ）、および、そのアクターが、追加、削除または修正されるべきかどうかの指標を指定する。

【００８４】

さらに別の実施形態において、２つの表が保持され、効率を向上させるために使用される。第１の表では、マネージドサーバ１３０を、そのマネージドサーバがメンバーであるアクターセットに関連付ける。第２の表では、マネージドサーバ１３０を、そのマネージドサーバに関連するアクターセットに（例えば、関連アクターモジュール３８０により判定されるように）関連付ける。これらの表において、マネージドサーバ１３０は、例えば

、そのマネージドサーバのＵＩＤによって表され、アクターセットは、例えば、そのアクターセットのＵＩＤで表される。ポリシーエンジンモジュール３４０は、管理ドメイン状態３２０の変更された部分（すなわち、変更されたサーバ記述）を使用して、どのマネージドサーバの記述が変更されたのかを判定する。ポリシーエンジンモジュール３４０は、第１の表を使用して、そのマネージドサーバが、どのアクターセットのメンバーだったのかを判定する。それらのアクターセットは、変更されたサーバ記述の結果として、変更されてよい。従って、ポリシーエンジンモジュール３４０は、第２の表を使用して、どのマネージドサーバに、それらのアクターセットが関連するのかを判定する。ポリシーエンジンモジュール３４０は、それらのマネージドサーバのみについて、上記で説明した共通部分の計算を実行する。

【００８５】

一実施形態において、ポリシーエンジンモジュール３４０は、以下のように、マネージドサーバのマネージメント命令を（管理ドメイン状態３２０に対する変更に基づき）更新し、更新されたマネージメント命令をマネージドサーバに送る。ポリシーエンジンモジュール３４０は、関連ルールモジュール３５０を実行して、管理ドメイン規模のマネージメントポリシー３３０と、マネージドサーバ１３０のＵＩＤとを入力として提供する。関連ルールモジュール３５０は、そのサーバに関連するルールのセット（「マネージメントポリシー観点」）を出力する。ポリシーエンジンモジュール３４０は、出力されたばかりのマネージメントポリシー観点を、キャッシュされたマネージメントポリシー観点と比較して、それらが異なるかどうかを判定する。出力されたばかりのマネージメントポリシー観点と、キャッシュされたマネージメントポリシー観点が同一の場合、ポリシーエンジンモジュール３４０は、それ以上何の行動も取らない。この状況において、以前生成されたマネージドサーバのマネージメント命令（詳細には、機能レベルの命令および関連アクターセット）は、管理ドメイン状態３２０に対する変更と一致し、再生成されてマネージドサーバに再送信される必要はない。

【００８６】

出力されたばかりのマネージメントポリシー観点と、キャッシュされたマネージメントポリシー観点が異なる場合、ポリシーエンジンモジュール３４０は、どのルールが、キャッシュされた観点に追加されるべきなのか、どのルールが、キャッシュされた観点から削除されるべきなのかを判定する。ポリシーエンジンモジュール３４０は、機能レベル命令生成モジュール３６０を実行して、追加すべきルールと、削除すべきルールとを入力として提供する。機能レベル命令生成モジュール３６０は、（以前マネージドサーバに送られた、キャッシュされた機能レベルの命令に比較して）追加すべき機能レベルの命令と、削除すべき機能レベルの命令とを出力する。ポリシーエンジンモジュール３４０は、必要に応じて、マネージドサーバに命令して、種々の機能レベルの命令を追加または削除させる。一実施形態において、より効率を上げるために、機能レベルの命令が、「ｄｉｆｆ」形式で送られる。例えば、ｄｉｆｆ形式は、機能レベルの命令識別子、および、機能レベルの命令が、以前送られた機能レベルの命令に対して追加、または、削除されるべきかどうかの指標を指定する。

【００８７】

ポリシーエンジンモジュール３４０は、アクターエニュメレーションモジュール３７０を実行して、キャッシュされたアクターセットと、管理ドメイン状態３２０の変更された部分（すなわち、変更されたサーバ記述）とを入力として提供する。アクターエニュメレーションモジュール３７０は、更新されたアクターセットを出力する。ポリシーエンジンモジュール３４０は、関連アクターモジュール３８０を実行して、更新されたアクターセットと、出力されたばかりのマネージメントポリシー観点とを入力として提供する。関連アクターモジュール３８０は、それらのルール（「更新された関連アクターセット」）に関連する、更新されたアクターセットのみを出力する。

【００８８】

ポリシーエンジンモジュール３４０は、更新された関連アクターセットを、キャッシュ

された関連アクターセットと比較して、それらが異なるかどうかを判定する。更新された関連アクターセットと、キャッシュされた関連アクターセットとが同一の場合、ポリシーエンジンモジュール３４０は、アクターセットをマネージドサーバに送らない。この状況において、以前生成された関連アクターセットは、管理ドメイン状態３２０に対する変更と一致し、マネージドサーバに再送信される必要はない。更新された関連アクターセットと、キャッシュされた関連アクターセットとが異なる場合、ポリシーエンジンモジュール３４０は、どのアクターセットが、キャッシュされた関連アクターセットに比較して、追加、削除、または修正されるべきかを判定する。ポリシーエンジンモジュール３４０は、必要に応じて、マネージドサーバに命令して、種々のアクターセットを追加、削除、または修正させる。一実施形態において、より効率を上げるために、アクターセットが「ｄｉｆｆ」形式で送られる。例えば、ｄｉｆｆ形式は、アクターセット識別子、および、そのアクターセットが、以前送られたアクターセットに比較して、追加、削除または修正されるべきかどうかの指標を指定する。

【００８９】

ポリシーエンジンモジュール３４０が、マネージドサーバのマネージメント命令を（管理ドメイン規模のマネージメントポリシー３３０に対する変更に基づき）更新し、更新されたマネージメント命令を、マネージドサーバに送ることができることを思い出されたい。マネージメントポリシー３３０に対する変更は、例えば、ルールまたはルールのセットの追加、削除、または修正である。一実施形態において、マネージメントポリシー３３０に対する変更が、ＧＵＩまたはＡＰＩを介したグローバルマネージャ１２０との対話処理により生成される。別の実施形態において、マネージメントポリシー３３０に対する変更が、グローバルマネージャ１２０内で、（例えば、グローバルマネージャにより検出されるセキュリティ脅威に応じて）自動化されたプロセスにより生成される。ポリシーエンジンモジュール３４０は、マネージメントポリシー３３０に対する変更または管理ドメイン状態３２０に対する変更があるかどうかにかかわらず、同様の方法で、マネージドサーバのマネージメント命令を更新し、更新されたマネージメント命令を、マネージドサーバに送る。しかし、多少の違いが存在する。

【００９０】

マネージメントポリシー３３０に対する変更の場合、ポリシーエンジンモジュール３４０は、必ずしも全てのマネージドサーバ１３０用のマネージメント命令を更新するわけではない。

【００９１】

代わりに、ポリシーエンジンモジュール３４０は、以前のマネージメントポリシー３３０を、新しいマネージメントポリシー３３０と比較して、どのルールが、以前のマネージメントポリシー３３０に比較して、追加、削除、または修正されるべきかを判定する。ポリシーエンジンモジュール３４０は、どのマネージドサーバ１３０が、変更されたルールにより影響を受けるのか（例えば、どのマネージドサーバが、ａ）ルールおよび／またはスコープの、ＰＢ部分および／またはＵＢ部分、および、ｂ）ルールの条件付きの部分（ある場合）、によりカバーされるのか）を判定する。ポリシーエンジンモジュール３４０は、関連ルールモジュール３５０を実行し、変更されたルール（新しいマネージメントポリシー３３０全体の代わりに）と、マネージドサーバ１３０のＵＩＤ（変更されたルールにより影響を受けるサーバのみについて）とを入力として提供する。

【００９２】

管理ドメイン状態更新（ＡＤＳＵ）モジュール３８５は、管理ドメイン状態３２０に対する変更を受け取り、それらの変更を処理する。管理ドメイン状態３２０に対する変更は、例えば、マネージドサーバ１３０の記述の、追加、削除、もしくは修正（マネージドサーバのラベルセットまたは構成特徴の修正を含む）、または、アンマネージドデバイスもしくはアンマネージドデバイスグループの記述の、追加、削除、もしくは修正である。一実施形態において、管理ドメイン状態３２０に対する変更が、特定のマネージドサーバ１３０から受け取るローカル状態情報に由来する。別の実施形態において、管理ドメイン状

態３２０に対する変更が、ＧＵＩまたはＡＰＩを介したグローバルマネージャ１２０との対話処理により生成される。さらに別の実施形態において、管理ドメイン状態３２０に対する変更が、グローバルマネージャ１２０内で、（例えば、グローバルマネージャにより検出されるセキュリティ脅威に応じて）自動化されたプロセスにより生成される。

【００９３】

例えば、ＡＤＳＵモジュール３８５は、特定のマネージドサーバ１３０に関する変更を受け取る。ＡＤＳＵモジュール３８５は、新しい情報を、特定のマネージドサーバ１３０の記述の一部として、管理ドメイン状態３２０内に記憶する。そして、ＡＤＳＵモジュール３８５は、（選択的に）そのマネージドサーバの記述を分析して、サーバに関する追加情報を判定し、その情報を記述内に記憶する。次に、ＡＤＳＵモジュール３８５は、マネージドサーバの記述に対する変更に基づき、管理ドメインのアクターセットおよび／またはマネージドサーバのマネージメント命令を更新すべきかどうかを判定する。ＡＤＳＵモジュール３８５が、管理ドメインのアクターセットを更新すると判定する場合、ＡＤＳＵモジュール３８５は、ポリシーエンジンモジュール３４０に命令して、管理ドメインのアクターセットを更新させる。一実施形態において、ＡＤＳＵモジュール３８５は、イベントが発生するのを待ってから、ポリシーエンジンモジュール３４０に命令して管理ドメインのアクターセットを更新させる。ＡＤＳＵモジュール３８５が、マネージドサーバのマネージメント命令を更新すると判定する場合、ＡＤＳＵモジュール３８５は、ポリシーエンジンモジュール３４０に命令して、マネージドサーバのマネージメント命令を更新させる。一実施形態において、ＡＤＳＵモジュール３８５は、イベントが発生するのを待ってから、ポリシーエンジンモジュール３４０に命令してマネージドサーバのマネージメント命令を更新させる。上述のイベントとは、例えば、ユーザコマンドの受領、または、特定のメンテナンスウィンドウの発生であってよい。

【００９４】

ＡＤＳＵモジュール３８５が、管理ドメインのアクターセットおよび／またはマネージドサーバのマネージメント命令を更新する、と判定するかしないかは、マネージドサーバの記述に対する変更のタイプに依存する。一実施形態において、ＡＤＳＵモジュール３８５は、この判定を、表２に示すように行う。

【００９５】

【表２】

変更のタイプ	更新するかどうか
オンラインからオフラインへ	管理ドメインのアクターセット：はい マネージドサーバのマネージメント命令：いいえ
オフラインからオンラインへ	管理ドメインのアクターセット：はい マネージドサーバのマネージメント命令：はい
ラベルセット	管理ドメインのアクターセット：はい マネージドサーバのマネージメント命令：はい
構成特徴	管理ドメインのアクターセット：いいえ マネージドサーバのマネージメント命令：はい
ネットワーク公開情報	管理ドメインのアクターセット：はい マネージドサーバのマネージメント命令：はい （ＩＰアドレスが唯一の変更であるのではない場合）
サービス情報	管理ドメインのアクターセット：いいえ マネージドサーバのマネージメント命令：はい （指定の状況においてのみ）

表２－サーバ記述変更のタイプに基づいた、管理ドメインのアクターセットおよび／またはマネージドサーバのマネージメント命令を更新すべきかどうかについて

【００９６】
一実施形態において、ＡＤＳＵモジュール３８５は、ラベル／構成特徴エンジンを実行して、サーバの記述を入力として提供することにより、サーバに関する追加情報を判定する。ラベル／ＣＣエンジンは、サーバの記述と、ラベル／ＣＣ割り当てルールとに基づき、サーバについてラベル／ＣＣ値を計算する。
【００９７】
別の実施形態において、ＡＤＳＵモジュール３８５は、サーバが、ネットワークアドレス変換器（ＮＡＴ）の後方にあるかどうか（および、ＮＡＴの後方にある場合は、どのタイプのＮＡＴ、すなわち、１：１または１：Ｎ、であるのか）、を判定する。例えば、ＡＤＳＵモジュール３８５は、（ａ）グローバルマネージャとサーバとの間のＴＣＰ接続に係る、サーバのＩＰアドレスと、（ｂ）サーバから受け取るローカル状態情報に係る、サーバのＩＰアドレスとを比較することにより、ＮＡＴが、グローバルマネージャ１２０とマネージドサーバ１３０との間に存在するかどうかを判定する。（ａ）と（ｂ）とが異なる場合、ＮＡＴは、グローバルマネージャ１２０とマネージドサーバ１３０との間に存在する。ＮＡＴが存在しない場合、ＡＤＳＵモジュール３８５は、データセンター決定を実行することにより、ＮＡＴのタイプ（１：１または１：Ｎ）を判定する。例えば、ＡＤＳＵモジュール３８５は、サーバのデータセンターを、データセンターのパブリックＩＰアドレスによって、識別する。（あるいは、マネージドサーバが、サーバの外部だが、データセンター内部にある情報を問い合わせることにより、データセンター決定を実行する。そして、サーバが、その情報をグローバルマネージャに、ローカルステータスの一部として送る。）構成情報は、どのタイプのＮＡＴがどのデータセンターによって使用されるのか、を示す。何のＮＡＴ情報も、特定のデータセンターに関連付けされない場合、ＡＤＳＵモジュール３８５は、ＮＡＴのタイプが１：Ｎであると想定する。
【００９８】
図４は、一実施形態に係る、マネージドサーバ１３０のポリシー実装モジュール１３６の詳細な概念を説明する、上位レベルのブロック図である。ポリシー実装モジュール１３６には、ローカル状態リポジトリ４００、ポリシーコンパイルモジュール４１０、および、ローカル状態更新モジュール４２０が含まれる。ローカル状態リポジトリ４００は、マネージドサーバ１３０のローカル状態に関する情報を記憶する。一実施形態において、ローカル状態リポジトリ４００は、マネージドサーバのオペレーティングシステム（ＯＳ）、ネットワーク公開、およびサービスに関する情報を記憶する。ＯＳ情報には、例えば、どのＯＳが実行中であるかの指標が含まれる。ネットワーク公開情報およびサービス情報については、管理ドメイン状態３２０内のマネージドサーバ１３０の記述に関して、上記で説明した。
【００９９】
ポリシーコンパイルモジュール４１０は、マネージメント命令と、マネージドサーバ１３０の状態とを入力として取り込み、マネージメントモジュール構成１３４を生成する。例えば、マネージメント命令は、グローバルマネージャ１２０から受け取られ、（機能レベル命令生成モジュール３６０により生成される）機能レベルの命令と、（関連アクターモジュール３８０により出力される）関連アクターセットとを含む。マネージドサーバ１３０の状態は、ローカル状態リポジトリ４００から回収される。一実施形態において、ポリシーコンパイルモジュール４１０の実行は、ａ）マネージドサーバの電源が入るか、オンラインになる、ｂ）マネージドサーバが機能レベルの命令を受け取る、および／または、ｃ）ローカル状態リポジトリ４００の内容が変更されることによりトリガされる。
【０１００】
ポリシーコンパイルモジュール４１０は、機能レベルの命令および関連アクターセットを、マネージメントモジュール構成１３４にマッピングする。例えば、ポリシーコンパイルモジュール４１０は、アクセス制御機能レベルの命令（ポートおよびアクターセット参照含む）を、Ｌｉｎｕｘオペレーティングシステムのｉｐｔａｂｌｅｓエントリーおよびｉｐｓｅｔエントリー、または、ウィンドウズオペレーティングシステムのウィンドウズ

フィルタリングプラットフォーム（ＷＦＰ）のルールにマッピングする。

【０１０１】

マネージドサーバ１３０におけるマネージメントポリシーの適用は、そのサーバのローカル状態により影響を受け得る。一実施形態において、ポリシーコンパイルモジュール４１０は、受け取った機能レベルの命令に関連する条件を評価し、その評価の結果に基づき、マネージメントモジュール構成１３４を生成する。例えば、ポリシーコンパイルモジュール４１０は、マネージドサーバのピア（すなわち、リレーションシップ内の他方のアクター）のオペレーティングシステムを参照する条件を評価し、その評価の結果に基づき、機能プロファイル属性を選択し、選択した機能プロファイル属性は、マネージメントモジュール構成１３４内に表現される。

【０１０２】

別の例として、マネージドサーバ１３０が、そのサーバには無意味なものとなる機能レベルの命令を受け取り得ることを思い出されたい。例えば、ルールには、マネージドサーバのローカル状態を指定する部分（例えば、提供されるサービスを記述するサービス部分）が含まれる。グローバルマネージャ１２０には、マネージドサーバのローカル状態（例えば、マネージドサーバが実際にそのサービスを提供中であるかどうか）が分からないため、生成された機能レベルの命令がマネージドサーバに送られる。ポリシーコンパイルモジュール４１０は、マネージドサーバのローカル状態をチェックする（例えば、マネージドサーバがそのサービスを提供中であるかどうかを判定する）。この判定は、マネージドサーバのローカル状態を参照する条件を評価することを意味する。ポリシーコンパイルモジュール４１０は、それに従って、機能レベルの命令を処理する。ポリシーコンパイルモジュール４１０が、条件が「真」となる（例えば、マネージドサーバが、そのサービスを提供中である）と判定する場合、ポリシーコンパイルモジュール４１０は、その機能レベルの命令を、マネージメントモジュール構成１３４に組み込む。詳細には、ポリシーコンパイルモジュール４１０が、機能レベルの命令をマネージメントモジュール構成１３４に組み込むのは、（そのサーバのローカル状態に関与する）関連付けられた条件を評価した後だけである。条件の評価が「偽」の場合、ポリシーコンパイルモジュール４１０は、機能レベルの命令をマネージメントモジュール構成１３４内に表現しない。特定の条件（例えば、その種類および特定の値）は、拡張可能である。一実施形態において、条件は、「サービス」の定義に関連し、プロセス情報および／またはパッケージ情報を含む（管理ドメイン状態３２０内のマネージドサーバ１３０の記述に関して、上記で説明した）。

【０１０３】

例えば、ポート８０にインバウンドするアパッチサービスのみへのアクセスを許可する機能レベルの命令について検討する（すなわち、マネージドサーバ１３０が、「プロバイダ」またはエンドポイントである）。マネージドサーバ１３０が、この機能レベルの命令を、マネージメントモジュール構成１３４内に表現して、ポート８０上でのアクセスの許可を、ポート８０上でリスンしている（そのサーバ上で実行中の）アプリケーションが、実際にアパッチであって、何らかの他のアプリケーションではない（不正なもの、その他）かどうか、に関与する関連付けられた条件を評価した後だけに行う。マネージドサーバ１３０は、この機能レベルの命令をマネージメントモジュール構成１３４内に表現するのは、関連付けられた条件が「真」となると判定した後だけである。関連付けられた条件が、「偽」となる場合、マネージドサーバ１３０は、この機能レベルの命令をマネージメントモジュール構成１３４内に表現しない。その結果、ネットワークトラフィックがブロックされる。

【０１０４】

一実施形態において、マネージドサーバ１３０は、そのアウトバウンド接続を監視する。マネージドサーバ１３０は、アウトバウンドネットワークトラフィックを、その内部処理テーブルと比較して、そのテーブル内のどのプロセスが、それらのアウトバウンド接続を確立しているのかを判定する。マネージドサーバ１３０は、（上記で言及した、要件のセットが与えられた）特定の処理のみに、アウトバウンド接続を確立することを許可する

ルールを、履行する。

【０１０５】

一実施形態において（図示せず）、ポリシーコンパイルモジュール４１０が、マネージドサーバ１３０に代えて、グローバルマネージャ１２０に配置される。その実施形態において、グローバルマネージャ１２０は、マネージメント命令をマネージドサーバ１３０に送らない。代わりに、マネージドサーバ１３０は、そのローカル状態をグローバルマネージャ１２０に送る。ポリシーコンパイルモジュール４１０が、マネージメントモジュール構成１３４を（グローバルマネージャ１２０にて）生成した後、マネージメントモジュール構成１３４は、グローバルマネージャ１２０からマネージドサーバ１３０に送られる。

【０１０６】

ローカル状態更新（ＬＳＵ）モジュール４２０は、マネージドサーバ１３０のローカル状態を監視し、ローカル状態情報をグローバルマネージャ１２０に送る。一実施形態において、ＬＳＵモジュール４２０は、マネージドサーバ１３０の初期ローカル状態を判定し、適切なローカル状態情報をローカル状態リポジトリ４００に記憶し、そのローカル状態情報をグローバルマネージャ１２０に送る。ＬＳＵモジュール４２０は、マネージドサーバ１３０のローカル状態を、サーバのオペレーティングシステム（ＯＳ）および／またはファイルシステムの種々の部分を調査することにより判定する。例えば、ＬＳＵモジュール４２０は、サービス情報を、ＯＳのカーネルテーブル（ネットワーキング情報）、ＯＳのシステムテーブル（パッケージ情報）、および、ファイルシステム（ファイルおよびハッシュ値）から取得する。ＬＳＵモジュール４２０は、ネットワーク公開情報を、ＯＳのカーネルおよび／またはＯＳレベルのデータ構造から取得する。

【０１０７】

ＬＳＵモジュール４２０は、初期ローカル状態情報をグローバルマネージャ１２０に送った後、ＬＳＵモジュールは、ローカル状態に対する変化を監視する。ＬＳＵモジュールは、例えば、ポーリングする（例えば、調査を周期的に実行する）こと、またはリスンする（例えば、イベントストリームにサブスクライブする）ことにより変更を監視する。ＬＳＵモジュール４２０は、直近に取得されたローカル状態情報を、ローカル状態リポジトリ４００に記憶済みの情報と比較する。情報が一致する場合、ＬＳＵモジュール４２０は、（ローカル状態情報が再度取得されるまで）それ以上何の行動も取らない。それらが異なる場合、ＬＳＵモジュール４２０は、直近に取得された情報を、ローカル状態リポジトリ４００内に記憶し、ポリシーコンパイルモジュール４１０を実行して、マネージメントモジュール構成１３４を再生成し（および、それに従って、マネージメントモジュール１３２を再構成し）、グローバルマネージャ１２０に変更を通知する。一実施形態において、ＬＳＵモジュール４２０は、ローカル状態情報に対する変更を、グローバルマネージャ１２０に「ｄｉｆｆ」形式で送る。例えば、ｄｉｆｆ形式では、ローカル状態情報のタイプ（例えば、オペレーティングシステム）、および、その情報タイプについての新しい値を指定する。別の実施形態において、ＬＳＵモジュール４２０は、ローカル状態リポジトリ４００の全体の内容を、グローバルマネージャ１２０に送る。

【０１０８】

図５は、一実施形態に係る、特定のマネージドサーバ１３０用のマネージメント命令を生成する方法５００を説明するフローチャートである。他の実施形態が、異なる順番でステップを実行することができ、異なるおよび／または追加のステップを含むことができる。加えて、ステップのうちのいくつかまたは全てが、図１に示されるもの以外のエンティティによって実行されてよい。一実施形態において、方法５００は、複数回実行される（例えば、管理ドメイン１５０内のマネージドサーバ１３０ごとに１回）。

【０１０９】

方法５００が開始されるとき、管理ドメインのコンピュータネットワークインフラの状態３２０と、管理ドメイン規模のマネージメントポリシー３３０とは、グローバルマネージャ１２０のリポジトリ３００内に既に記憶されてある。この時点で、方法５００が開始される。

【０１１０】
ステップ５１０において、管理ドメイン状態３２０と、管理ドメイン規模のマネージメントポリシー３３０が、アクセスされる。例えば、ポリシーエンジンモジュール３４０が、リポジトリ３００に要求を送り、管理ドメイン状態３２０と、管理ドメイン規模のマネージメントポリシー３３０とを応答として受け取る。
【０１１１】
ステップ５２０において、１つまたは複数の関連ルールが判定される。例えば、ポリシーエンジンモジュール３４０は、関連ルールモジュール３５０を実行して、管理ドメイン規模のマネージメントポリシー３３０と、特定のマネージドサーバ１３０のＵＩＤとを入力として提供する。関連ルールモジュール３５０は、そのサーバに関連するルールのセット（マネージメントポリシー観点）を出力する。
【０１１２】
ステップ５３０において、アクターがエニュメレートされる。例えば、ポリシーエンジンモジュール３４０は、アクターエニュメレーションモジュール３７０を実行して、管理ドメイン状態３２０を入力として提供する。アクターエニュメレーションモジュール３７０は、管理ドメイン状態３２０内のエニュメレートされた形式の、マネージドサーバ１３０およびアンマネージドデバイスグループ（ＵＤＧ）の表現（「アクターセット」）を生成する。
【０１１３】
ステップ５４０において、１つまたは複数の機能レベルの命令が生成される。例えば、ポリシーエンジンモジュール３４０は、機能レベル命令生成モジュール３６０を実行して、マネージメントポリシー観点（ステップ５２０にて生成された）を入力として提供する。機能レベル命令生成モジュール３６０が、機能レベルの命令を生成する。
【０１１４】
ステップ５５０にて、１つまたは複数の関連アクターが判定される。例えば、ポリシーエンジンモジュール３４０は、関連アクターモジュール３８０を実行して、（ステップ５３０にて生成された）アクターセットと、（ステップ５２０にて生成された）マネージメントポリシー観点とを入力として提供する。関連アクターモジュール３８０は、それらのルールに関連するアクターセット（関連アクターセット）のみを出力する。
【０１１５】
ステップ５６０にて、マネージメント命令が特定のマネージドサーバ１３０に送られる。例えば、ポリシーエンジンモジュール３４０は、機能レベルの命令（ステップ５４０にて生成された）と、関連アクターセット（ステップ５５０にて生成された）とを特定のマネージドサーバ１３０に送る。
【０１１６】
なお、ステップ５２０および５４０は、特定のマネージドサーバ１３０についてのマネージメントポリシー観点（および、結果として得られる機能レベルの命令）を生成することに関与し、一方、ステップ５３０および５５０は、そのマネージドサーバについてのアクター観点を生成することに関与する。ステップ５２０で、ステップ５５０によって使用されるルールのセットが生成されるため、マネージメントポリシー観点の生成と、アクター観点の生成とは、最小限にお互いに依存する。そうであっても、マネージメントポリシーの計算（すなわち、ステップ５２０および５４０）と、アクターセットの計算（すなわち、ステップ５３０および５５０）とを別々に維持することは、ポリシーエンジンモジュール３４０の拡張性を向上させる。マネージメントポリシーの計算と、アクターセットの計算が、ほとんど別々に維持されるため、それらは、（例えば、同じマネージドサーバ１３０についてであっても）並行して実行されてよい。加えて、異なるマネージドサーバ１３０についての観点の計算も、並行して実行されてよい。また、アクターが変更される場合、アクターセットのみが、再計算されればよい（機能レベルの命令は、再計算される必要が無い）。ルールが変更される場合、機能レベルの命令および関連アクターセットのみが再計算されればよい（アクターは、再エニュメレートされる必要が無い）。

【０１１７】
図６は、一実施形態に係る、マネージドサーバ１３０のマネージメントモジュール１３２の構成１３４を生成する方法６００を説明するフローチャートである。他の実施形態が、異なる順番でステップを実行することができ、異なるおよび／または追加のステップを含むことができる。加えて、ステップのうちのいくつかまたは全てが、図１に示されるもの以外のエンティティによって実行されてよい。
【０１１８】
方法６００が開始されるとき、マネージドサーバ１３０のローカル状態に関する情報が、マネージドサーバ１３０のポリシー実装モジュール１３６のローカル状態リポジトリ４００内に既に記憶されてある。この時点で、方法６００が開始される。
【０１１９】
ステップ６１０にて、マネージメント命令が、グローバルマネージャ１２０から受け取られる。例えば、ポリシーコンパイルモジュール４１０は、機能レベルの命令と、関連アクターセットとをグローバルマネージャ１２０から受け取る。
【０１２０】
ステップ６２０にて、ローカル状態がアクセスされる。例えば、ポリシーコンパイルモジュール４１０は、ローカル状態リポジトリ４００内に記憶される、マネージドサーバ１３０のローカル状態に関する情報にアクセスする。
【０１２１】
ステップ６３０にて、マネージメントモジュール構成１３４が生成される。例えば、ポリシーコンパイルモジュール４１０は、（ステップ６１０にて受け取られた）マネージメント命令と、（ステップ６２０にてアクセスされた）ローカル状態と、を入力として取り込み、マネージメントモジュール構成１３４を生成する。
【０１２２】
ステップ６４０にて、マネージメントモジュール１３２が構成される。例えば、ポリシーコンパイルモジュール４１０は、マネージメントモジュール１３２を、（ステップ６３０にて生成された）マネージメントモジュール構成１３４に従って動作するべく、構成する。
【０１２３】
図７は、一実施形態に係る、マネージドサーバ１３０のローカル状態を監視し、かつ、ローカル状態情報をグローバルマネージャ１２０に送る、方法７００を説明するフローチャートである。他の実施形態が、異なる順番でステップを実行することができ、異なるおよび／または追加のステップを含むことができる。加えて、ステップのうちのいくつかまたは全てが、図１に示されるもの以外のエンティティによって実行されてよい。
【０１２４】
方法７００が開始されるとき、マネージドサーバ１３０のローカル状態に関する情報が、マネージドサーバ１３０のローカル状態リポジトリ４００内に既に記憶されてある。この時点で、方法７００が開始される。
【０１２５】
ステップ７１０にて、マネージドサーバ１３０の現在のローカル状態に関する情報が判定される。例えば、ＬＳＵモジュール４２０は、マネージドサーバ１３０のローカル状態を、サーバのオペレーティングシステム（ＯＳ）および／またはファイルシステムの種々の部分を調査することにより判定する。
【０１２６】
ステップ７２０にて、現在のローカル状態に関する情報が、ローカル状態リポジトリ４００内に記憶された情報と異なるかどうかに関して、判定が行われる。例えば、ＬＳＵモジュール４２０がこの判定を実行する。情報が異ならない場合、方法はステップ７３０に進み、終了する。情報が異なる場合、方法はステップ７４０に進む。
【０１２７】
ステップ７４０にて、異なる情報が、ローカル状態リポジトリ４００内に記憶される。

例えば、ＬＳＵモジュール４２０が、このステップを実行する。
【０１２８】
ステップ７５０にて、マネージメントモジュール構成１３４は、（ローカル状態リポジトリ４００の内容が変更されたため）再生成され、マネージメントモジュール１３２がそれに従って、再構成される。例えば、ＬＳＵモジュール４２０は、ポリシーコンパイルモジュール４１０を実行し、これによりマネージメントモジュール構成１３４が再生成される。
【０１２９】
ステップ７６０にて、異なる情報が、グローバルマネージャ１２０に送られる。例えば、ＬＳＵモジュール４２０が、このステップを実行する。
【０１３０】
図８は、一実施形態に係る、管理ドメインのコンピュータネットワークインフラの状態３２０に対する変化を処理する、方法８００を説明するフローチャートである。他の実施形態が、異なる順番でステップを実行することができ、異なるおよび／または追加のステップを含むことができる。加えて、ステップのうちのいくつかまたは全てが、図１に示されるもの以外のエンティティによって実行されてよい。
【０１３１】
ステップ８１０にて、特定のマネージドサーバ１３０に関する変更が受け取られる。例えば、管理ドメイン状態更新（ＡＤＳＵ）モジュール３８５は、オンライン／オフラインインジケータ、オペレーティングシステムインジケータ、ネットワーク公開情報、および／または、サービス情報を、マネージドサーバ１３０から、ローカル状態情報の一部として受け取る。
【０１３２】
ステップ８２０にて、受け取った情報が記憶される。例えば、ＡＤＳＵモジュール３８５は、受け取ったオンライン／オフラインインジケータ、ネットワーク公開情報、および／または、サービス情報を、管理ドメイン状態３２０内（詳細には、情報が関連するマネージドサーバ１３０の記述内）に記憶する。
【０１３３】
ステップ８３０にて、サーバ記述が分析されて、サーバに関する追加情報を判定する。
【０１３４】
例えば、ＡＤＳＵモジュール３８５は、ラベル／構成特徴エンジンを使用して、サーバについてラベル／ＣＣ値を計算し、および／または、サーバが、ネットワークアドレス変換器（ＮＡＴ）の後方にあるかどうか（および、ＮＡＴの後方にある場合は、どのタイプのＮＡＴ、すなわち、１：１または１：Ｎ、であるのか）を判定し、その情報をサーバ記述内に記憶する。ステップ８３０は選択的なものである。
【０１３５】
ステップ８４０にて、管理ドメインのアクターセットを更新すべきかどうかに関して、判定がなされる。例えば、ＡＤＳＵモジュール３８５はマネージドサーバの記述に対する変更に基づき、管理ドメインのアクターセットを更新すべきかどうかを判定する。管理ドメインのアクターセットを更新するという判定がなされる場合、方法はステップ８５０に進む。管理ドメインのアクターセットを更新しないという判定がなされる場合、方法はステップ８６０に進む。
【０１３６】
ステップ８５０にて、管理ドメインのアクターセットが更新される。例えば、ＡＤＳＵモジュール３８５は、ポリシーエンジンモジュール３４０に命令して管理ドメインのアクターセットを更新させる。一実施形態（図示せず）において、ＡＤＳＵモジュール３８５は、イベントが発生するのを待ってから、ポリシーエンジンモジュール３４０に命令して管理ドメインのアクターセットを更新させる。
【０１３７】
ステップ８６０にて、マネージドサーバのマネージメント命令を更新すべきかどうかに

関して、判定がなされる。例えば、ＡＤＳＵモジュール３８５は、マネージドサーバの記述に対する変更に基づき、マネージドサーバのマネージメント命令を更新すべきかどうかを判定する。マネージドサーバのマネージメント命令を更新するという判定がなされる場合、方法はステップ８７０に進む。管理ドメインのアクターセットを更新しないという判定がなされる場合、方法はステップ８８０に進む。

【０１３８】

ステップ８７０にて、マネージドサーバのマネージメント命令が更新される。例えば、ＡＤＳＵモジュール３８５は、ポリシーエンジンモジュール３４０に命令してマネージドサーバのマネージメント命令を更新させる。一実施形態（図示せず）において、ＡＤＳＵモジュール３８５は、イベントが発生するのを待ってから、ポリシーエンジンモジュール３４０に命令してマネージドサーバのマネージメント命令を更新させる。

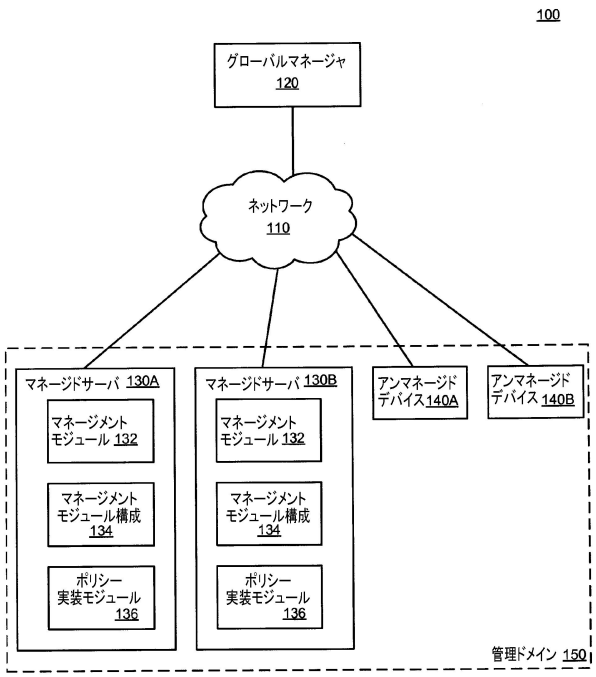
【０１３９】

ステップ８８０にて、方法が終了する。

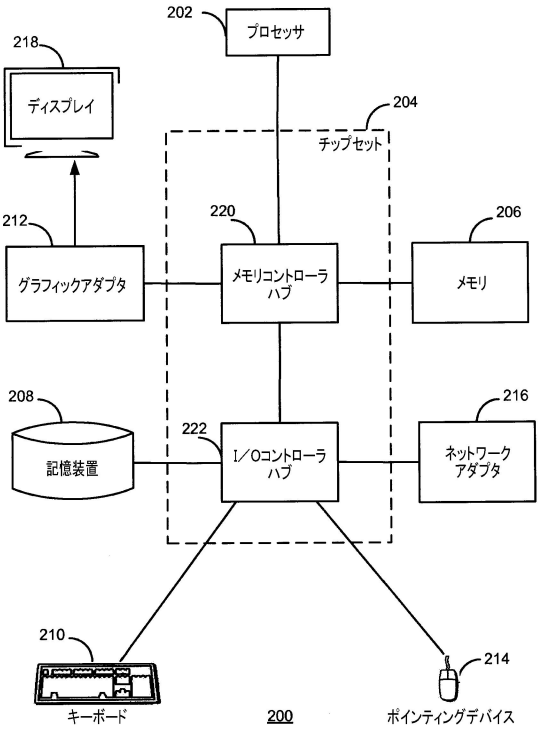
【０１４０】

上記の説明は、特定の実施形態の動作を説明するために含まれ、本発明の範囲を制限することは意図されない。本発明の範囲は、以下の請求項によってのみ、制限されるべきである。上記の検討から、当業者には、本発明の精神および範囲によってさらに網羅されるであろう多くの変形が明らかとなるであろう。

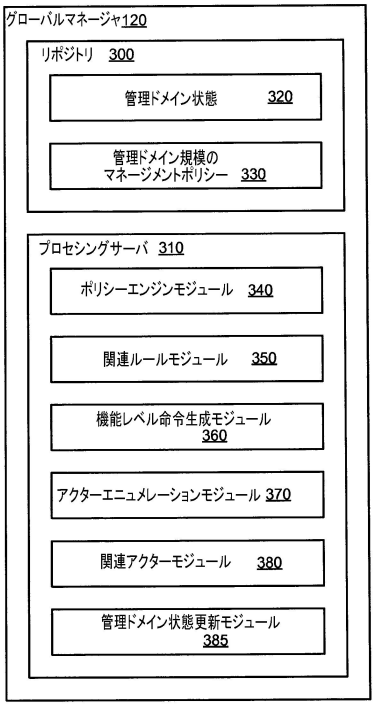
【図１】



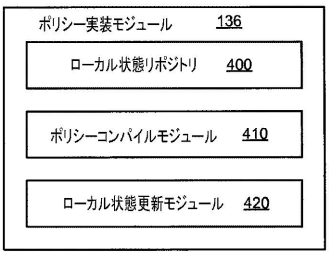
【図２】



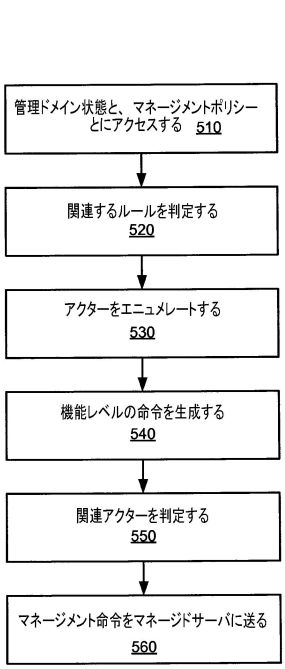
【図３】


グローバルマネージャ120
リポジトリ 300
管理ドメイン状態 320
管理ドメイン規模の
マネージメントポリシー 330
プロセシングサーバ 310
ポリシーエンジンモジュール 340
関連ルールモジュール 350
機能レベル命令生成モジュール
360
アクターエニュメレーションモジュール 370
関連アクターモジュール 380
管理ドメイン状態更新モジュール
385

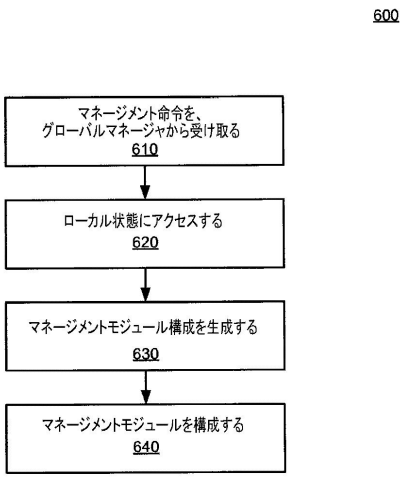
【図４】


ポリシー実装モジュール 136
ローカル状態リポジトリ 400
ポリシーコンパイルモジュール 410
ローカル状態更新モジュール 420

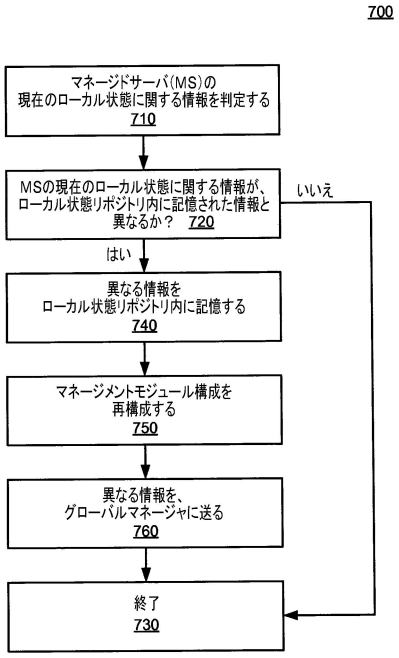
【図５】


500
管理ドメイン状態と、マネージメントポリシー
とにアクセスする 510
関連するルールを判定する
520
アクターをエニュメレートする
530
機能レベルの命令を生成する
540
関連アクターを判定する
550
マネージメント命令をマネージドサーバに送る
560

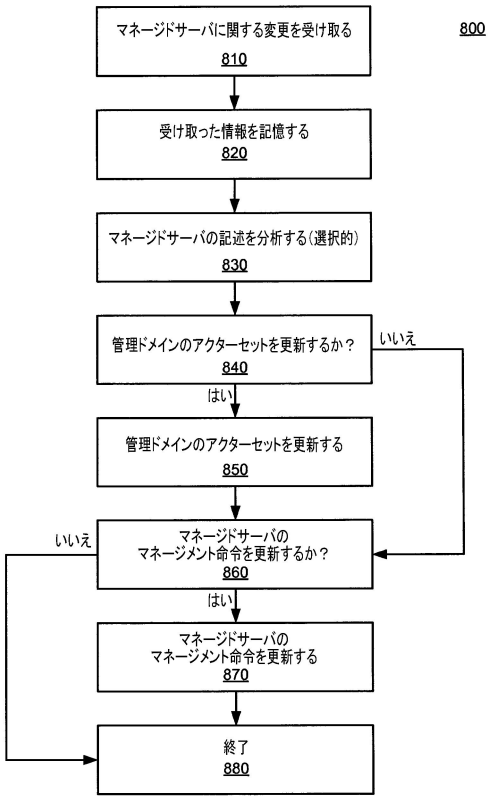
【図６】


600
マネージメント命令を、
グローバルマネージャから受け取る
610
ローカル状態にアクセスする
620
マネージメントモジュール構成を生成する
630
マネージメントモジュールを構成する
640

【図７】


700
マネージドサーバ(MS)の
現在のローカル状態に関する情報を判定する
710
MSの現在のローカル状態に関する情報が、
ローカル状態リポジトリ内に記憶された情報と
異なるか？ 720
いいえ
はい
異なる情報を
ローカル状態リポジトリ内に記憶する
740
マネージメントモジュール構成を
再構成する
750
異なる情報を、
グローバルマネージャに送る
760
終了
730

【図８】


マネージドサーバに関する変更を受け取る
810
800
受け取った情報を記憶する
820
マネージドサーバの記述を分析する(選択的)
830
管理ドメインのアクターセットを更新するか？
840
いいえ
はい
管理ドメインのアクターセットを更新する
850
マネージドサーバの
マネージメント命令を更新するか？
860
いいえ
はい
マネージドサーバの
マネージメント命令を更新する
870
終了
880

フロントページの続き

(72)発明者　ダニエル　アール．クック
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内
(72)発明者　ユライ　ジー．ファンドリ
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内
(72)発明者　マシュー　ケー．グレン
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内
(72)発明者　ムケシュ　グプタ
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内
(72)発明者　アンドリュー　エス．ルビン
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内
(72)発明者　ジェリー　ビー．スコット
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内
(72)発明者　セホ　チャン
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内
(72)発明者　アラン　ビー．ストコル
アメリカ合衆国　９４０８６　カリフォルニア州　サニーベール　サン　ガブリエル　ドライブ　１６０　イルミオ　インコーポレイテッド内

審査官　田中　幸雄

(56)参考文献　特表２００２－５０７２９５（ＪＰ，Ａ）
特開２０１１－２４３１１２（ＪＰ，Ａ）
米国特許出願公開第２０１０／０３３３１６５（ＵＳ，Ａ１）
特開２０１２－４３４４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　９／４６