

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6336041号  
(P6336041)

(45) 発行日 平成30年6月6日(2018.6.6)

(24) 登録日 平成30年5月11日(2018.5.11)

(51) Int.Cl.

F I

G 0 6 F 13/00 (2006.01)

G 0 6 F 13/00 3 5 1 N

請求項の数 15 (全 37 頁)

(21) 出願番号 特願2016-507642 (P2016-507642)  
 (86) (22) 出願日 平成26年4月9日 (2014.4.9)  
 (65) 公表番号 特表2016-521415 (P2016-521415A)  
 (43) 公表日 平成28年7月21日 (2016.7.21)  
 (86) 国際出願番号 PCT/US2014/033540  
 (87) 国際公開番号 W02014/169062  
 (87) 国際公開日 平成26年10月16日 (2014.10.16)  
 審査請求日 平成29年4月10日 (2017.4.10)  
 (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)

(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 94  
 086, サニーベール, 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. カーナー  
 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

早期審査対象出願

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ジメントシステム

(57) 【特許請求の範囲】

【請求項1】

管理ドメイン内で特定の被管理サーバの状態に対する変化を処理するための方法であって、前記管理ドメインは、マネージメントモジュールを構成するためのマネージメント命令を使用する複数の被管理サーバを含み、当該構成されたマネージメントモジュールが1つまたは複数のルールセットを含む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し、前記方法が、

前記1つまたは複数のルールセットを記憶するステップであって、各ルールは、コンピュータネットワークを介して提供されるサービスを特定し、提供元部分は、どの被管理サーバが前記コンピュータネットワークを介して前記サービスを提供するルールによって制御されるかを示し、使用元部分は、どの被管理サーバが前記コンピュータネットワークを介してアクセスされる前記サービスを使用するルールによって制御されるかを示す、ステップと、

前記特定の被管理サーバの第1の記述を修正して、前記特定の被管理サーバの修正された記述を生成し、前記特定の被管理サーバの変更された状態を示すステップと、

前記第1の記述を、前記修正された記述と比較し、それによって、記述変更を特定するステップと、

前記記述変更に基づき、前記特定の被管理サーバに以前送信された現在のマネージメント命令を更新するかどうかを判定するステップと、

前記特定の被管理サーバの現在のマネージメント命令を更新するという判定に応答して

、  
前記修正された記述に基づき、前記ルールセット内のどのルールが前記特定の被管理サーバに適用可能な提供元部分又は前記特定の被管理サーバに適用可能な使用元部分を特定するのかを判定するステップであって、それによって、現在の関連ルールを特定するステップと、

前記第1の記述に基づき以前に判定された、キャッシュされた以前の関連ルールを取得するステップと、

前記現在の関連ルールが、前記特定の被管理サーバのための前記キャッシュされた以前の関連ルールと異なるかどうかを判定するステップと、

前記現在の関連ルールが、前記特定の被管理サーバのための前記キャッシュされた以前の関連ルールと異なるという判定に応答して： 10

前記キャッシュされた以前の関連ルールに応じて追加、除去又は修正されるべきルールを判定するステップと、

当該判定されたルールに基づいて前記キャッシュされた以前の関連ルールを更新するステップと、

前記判定されたルールに基づいて前記特定の被管理サーバによって実行される管理命令を生成するステップと、

前記管理命令及び前記特定の被管理サーバ上での前記管理命令を追加、除去又は修正するための命令を前記特定の被管理サーバに送るステップと、  
を含むことを特徴とする方法。 20

#### 【請求項2】

前記特定の被管理サーバのマネージメント命令を更新するという判定に  
応答して、かつ、前記現在の関連ルールが、前記キャッシュされた以前の関連ルールと異なるという判定に  
応答して、

キャッシュされたアクターセットを更新して、前記特定の被管理サーバの変更された状態を示し、それによって、更新されたアクターセットを特定するステップと、

どの更新されたアクターセットが、前記特定の被管理サーバに関連するのかを判定するステップであって、それによって、現在関連する更新されたアクターセットを特定するステップと、

前記現在関連する更新されたアクターセットが、前記特定の被管理サーバに以前送られたアクターセットと異なるかどうか、を判定するステップと、 30

前記現在関連する更新されたアクターセットが、前記以前送られたアクターセットと異なるという判定に  
応答して：

前記以前送られたアクターセットに応じて追加、除去又は修正されるべき、更新されたアクターセットを判定するステップと、

前記更新されたアクターセット及び前記更新されたアクターセットを追加、除去又は修正するための第2の命令を前記特定の被管理サーバに送るステップと、  
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3】

前記記述変更は、オンライン／オフラインの変更、ラベルセットの変更、構成特徴の変更、またはネットワーク公開情報の変更を含むことを特徴とする請求項1に記載の方法。 40

#### 【請求項4】

前記特定の被管理サーバに以前送られたマネージメント命令を更新するかどうかを判定するステップが、

前記記述変更が、前記特定の被管理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かどうかを判定するステップと、

前記記述変更が、前記特定の被管理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、という判定に  
応答して、前記特定の被管理サーバのマネージメント命令を更新する、と判定するステップと、  
を含むことを特徴とする請求項1に記載の方法。 50

## 【請求項 5】

前記特定の被管理サーバに以前送られたマネージメント命令を更新するかどうかを判定するステップが、

前記記述変更が、ラベルセットの変更または構成特徴の変更を含むかどうかを判定するステップと、

前記記述変更が、ラベルセットの変更または構成特徴の変更を含む、という判定に応答して、前記特定の被管理サーバのマネージメント命令を更新すると判定するステップと、を含むことを特徴とする請求項 1 に記載の方法。

## 【請求項 6】

前記特定の被管理サーバに以前送られたマネージメント命令を更新するかどうかを判定するステップが、

前記記述変更が、ネットワーク公開情報の変更を含むかどうかを判定するステップと、

前記記述変更が、ネットワーク公開情報の変更を含む、という判定に応答して、前記特定の被管理サーバのマネージメント命令を更新すると判定するステップと、を含むことを特徴とする請求項 1 に記載の方法。

## 【請求項 7】

前記第 1 の記述を、前記修正された記述と比較する前に、

前記修正された記述に基づき、前記特定の被管理サーバに関する追加情報を判定するステップと、

前記修正された記述を修正して、前記追加情報を示すステップと、  
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 8】

管理ドメイン内で特定の被管理サーバの状態に対する変化を処理するためのコンピュータプログラムを記憶する、非一時的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、マネージメントモジュールを構成するためのマネージメント命令を使用する複数の被管理サーバを含み、当該構成されたマネージメントモジュールが 1 つまたは複数のルールのセットを含む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し、前記コンピュータプログラムは、

前記 1 つまたは複数のルールのセットを記憶するステップであって、各ルールは、コンピュータネットワークを介して提供されるサービスを特定し、提供元部分は、どの被管理サーバが前記コンピュータネットワークを介して前記サービスを提供するルールによって制御されるかを示し、使用元部分は、どの被管理サーバが前記コンピュータネットワークを介してアクセスされる前記サービスを使用するルールによって制御されるかを示す、  
ステップと、

前記特定の被管理サーバの第 1 の記述を修正して、前記特定の被管理サーバの修正された記述を生成し、前記特定の被管理サーバの変更された状態を示すステップと、

前記第 1 の記述を、前記修正された記述と比較し、それによって、記述変更を特定するステップと、

前記記述変更に基づき、前記特定の被管理サーバに以前送信された現在のマネージメント命令を更新するかどうかを判定するステップと、

前記特定の被管理サーバの現在のマネージメント命令を更新するという判定に応答して、

前記修正された記述に基づき、前記ルールのセット内のどのルールが前記特定の被管理サーバに適用可能な提供元部分又は前記特定の被管理サーバに適用可能な使用元部分を特定するのかを判定するステップであって、それによって、現在の関連ルールを特定する  
ステップと、

前記第 1 の記述に基づき以前に判定された、キャッシュされた以前の関連ルールを取得するステップと、

前記現在の関連ルールが、前記特定の被管理サーバのための前記キャッシュされた以前の関連ルールと異なるかどうかを判定するステップと、

10

20

30

40

50

前記現在の関連ルールが、前記特定の被管理サーバのための前記キャッシュされた以前の関連ルールと異なるという判定に応答して：

前記キャッシュされた以前の関連ルールに応じて追加、除去又は修正されるべきルールを判定するステップと、

当該判定されたルールに基づいて前記キャッシュされた以前の関連ルールを更新するステップと、

前記判定されたルールに基づいて前記特定の被管理サーバによって実行される管理命令を生成するステップと、

前記管理命令及び前記特定の被管理サーバ上での前記管理命令を追加、除去又は修正するための命令を前記特定の被管理サーバに送るステップと、  
をコンピュータプロセッサに実行させることを特徴とする非一時的コンピュータ可読記憶媒体。

10

#### 【請求項 9】

前記コンピュータプログラムは、

前記特定の被管理サーバのマネジメント命令を更新するという判定に  
応答して、かつ、前記現在の関連ルールが、前記キャッシュされた以前の関連ルールと異なるという判定に  
応答して、

キャッシュされたアクターセットを更新して、前記特定の被管理サーバの変更された状態を示し、それによって、更新されたアクターセットを特定するステップと、

どの更新されたアクターセットが、前記特定の被管理サーバに関連するのかを判定する  
ステップであって、それによって、現在関連する更新されたアクターセットを特定する  
ステップと、

20

前記現在関連する更新されたアクターセットが、前記特定の被管理サーバに以前送られたアクターセットと異なるかどうか、を判定するステップと、

前記現在関連する更新されたアクターセットが、前記以前送られたアクターセットと異なるという判定に  
応答して：

前記以前送られたアクターセットに応じて追加、除去又は修正されるべき、更新されたアクターセットを判定するステップと、

前記更新されたアクターセット及び前記更新されたアクターセットを追加、除去又は修正するための第 2 の命令を前記特定の被管理サーバに送るステップと、

30

を前記コンピュータプロセッサにさらに実行させることを特徴とする請求項 8 に記載の非一時的コンピュータ可読記憶媒体。

#### 【請求項 10】

前記記述変更は、オンライン／オフラインの変更、ラベルセットの変更、構成特徴の変更、またはネットワーク公開情報の変更を含むことを特徴とする請求項 8 に記載の非一時的コンピュータ可読記憶媒体。

#### 【請求項 11】

前記特定の被管理サーバに以前送られたマネジメント命令を更新するかどうかを判定するステップが、

前記記述変更が、前記特定の被管理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かどうかを判定するステップと、

40

前記記述変更が、前記特定の被管理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、という判定に  
応答して、前記特定の被管理サーバのマネジメント命令を更新する、と判定するステップと、  
を含むことを特徴とする請求項 8 に記載の非一時的コンピュータ可読記憶媒体。

#### 【請求項 12】

前記特定の被管理サーバに以前送られたマネジメント命令を更新するかどうかを判定するステップが、

前記記述変更が、ラベルセットの変更または構成特徴の変更を含むかどうかを判定するステップと、

50

前記記述変更が、ラベルセットの変更または構成特徴の変更を含む、という判定に  
応答して、前記特定の被管理サーバのマネージメント命令を更新する、と判定する  
ステップと、  
を含むことを特徴とする請求項8に記載の非一時的コンピュータ可読記憶媒体。

【請求項13】

前記特定の被管理サーバに以前送られたマネージメント命令を更新するかどうかを判定  
するステップが、

前記記述変更が、ネットワーク公開情報の変更を含むかどうかを判定するステップと、

前記記述変更が、ネットワーク公開情報の変更を含む、という判定に  
応答して、前記特定の被管理サーバのマネージメント命令を更新すると判定する  
ステップと、  
を含むことを特徴とする請求項8に記載の非一時的コンピュータ可読記憶媒体。

10

【請求項14】

管理ドメイン内で特定の被管理サーバの状態に対する変化を処理するためのシステムで  
あって、前記管理ドメインは、マネージメントモジュールを構成するためのマネー  
ジメント命令を使用する複数の被管理サーバを含み、当該構成されたマネー  
ジメントモジュールが1つまたは複数のルールをセットを含む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し、前記システムが、

コンピュータプログラムを記憶する非一時的コンピュータ可読記憶媒体と、

コンピュータプロセッサと、

を含み、

前記コンピュータプログラムは、前記コンピュータプロセッサに、

前記1つまたは複数のルールを記憶するステップであって、各ルールは、コン  
ピュータネットワークを介して提供されるサービスを特定し、提供元部分は、どの被管理  
サーバが前記コンピュータネットワークを介して前記サービスを提供するルールによっ  
て制御されるかを示し、使用元部分は、どの被管理サーバが前記コンピュータネット  
ワークを介してアクセスされる前記サービスを使用するルールによって制御されるか  
を示す、ステップと、

20

前記特定の被管理サーバの第1の記述を修正して、前記特定の被管理サーバの修正  
された記述を生成し、前記特定の被管理サーバの変更された状態を示すステップと、

前記第1の記述を、前記修正された記述と比較し、それによって、記述変更を特定する  
ステップと、

30

前記記述変更に基づき、前記特定の被管理サーバに以前送信された現在のマネー  
ジメント命令を更新するかどうかを判定するステップと、

前記特定の被管理サーバの現在のマネージメント命令を更新するという判定に  
応答して、

前記修正された記述に基づき、前記ルールのセット内のどのルールが前記特定の被  
管理サーバに適用可能な提供元部分又は前記特定の被管理サーバに適用可能な使用元部分  
を特定するのかを判定するステップであって、それによって、現在の関連ルールを特定する  
ステップと、

前記第1の記述に基づき以前に判定された、キャッシュされた以前の関連ルールを取  
得するステップと、

40

前記現在の関連ルールが、前記特定の被管理サーバのための前記キャッシュされた以  
前の関連ルールと異なるかどうかを判定するステップと、

前記現在の関連ルールが、前記特定の被管理サーバのための前記キャッシュされた以  
前の関連ルールと異なるという判定に  
応答して、

前記キャッシュされた以前の関連ルールに応じて追加、除去又は修正されるべきル  
ールを判定するステップと、

当該判定されたルールに基づいて前記キャッシュされた以前の関連ルールを更新す  
るステップと、

前記判定されたルールに基づいて前記特定の被管理サーバによって実行される管理

50

命令を生成するステップと、

前記管理命令及び前記特定の被管理サーバ上での前記管理命令を追加、除去又は修正するための命令を前記特定の被管理サーバに送るステップと、  
を実行させることを特徴とするシステム。

【請求項15】

前記ルールセット内のどのルールが前記特定の被管理サーバに適用可能な提供元部分又は前記特定の被管理サーバに適用可能な使用元部分を特定するのかを判定するステップと、前記現在の関連ルールが、前記特定の被管理サーバのための前記キャッシュされた以前の関連ルールと異なるかどうかを判定するステップとは、制限されたルールセットを識別して、前記特定の被管理サーバが前記制限されたルールセットを効率的に分散することを可能にすることを特徴とする請求項1に記載の方法。

10

【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忠実に守る、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（Internet Protocol（以下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。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。

20

【発明の概要】

【0003】

上記および他の論点は、管理ドメイン内の特定の被管理サーバの状態に対する変更を処理するための、方法、非一時的コンピュータ可読記憶媒体、およびシステム、によって対処される。管理ドメインが、複数の被管理サーバを含み、被管理サーバは、マネージメント命令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、1つまたは複数のルール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を実装するようにする。方法の一実施形態は、特定の被管理サーバの第1の記述を修正して、特定の被管理サーバの変更された状態を示し、それによって、特定の被管理サーバの第2の記述を指定する、ステップを含む。方法は、未修正の第1の記述を、第2の記述と比較し、それによって、記述変更を指定するステップを、さらに含む。方法は、記述変更に基づき、特定の被管理サーバに以前送られたマネージメント命令を更新すべきかどうかを判定するステップを、さらに含む。方法は、特定の被管理サーバのマネージメント命令を更新するという判定に回答して、第2の記述に基づき、ルールセット内のどのルールが、特定の被管理サーバに現在関連するのかを判定し、それによって、現在の関連ルールを指定する、ステップと、現在の関連ルールが、以前の関連ルールと異なるかどうかを判定するステップであって、以前の関連ルールは、未修正の第1の記述に基づき判定された、ステップと、現在の関連ルールが、以前の関連ルールと同一であるという判定に回答して、それ以上何の行動も取らないステップと、をさらに含む。

30

40

【0004】

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。ステップには、特定の被管理サーバの第1の記述を修正して、特定

50

の被管理サーバの変更された状態を示し、それによって、特定の被管理サーバの第2の記述を指定する、ステップが含まれる。ステップには、未修正の第1の記述を、第2の記述と比較し、それによって、記述変更を指定するステップが、さらに含まれる。ステップには、記述変更に基づき、特定の被管理サーバに以前送られたマネージメント命令を更新すべきかどうかを判定するステップが、さらに含まれる。ステップには、特定の被管理サーバのマネージメント命令を更新するという判定に応答して、第2の記述に基づき、ルールセット内のどのルールが、特定の被管理サーバに現在関連するのかを判定し、それによって、現在の関連ルールを指定する、ステップと、現在の関連ルールが、以前の関連ルールと異なるかどうかを判定するステップであって、以前の関連ルールは、未修正の第1の記述に基づき判定された、ステップと、現在の関連ルールが、以前の関連ルールと同一であるという判定に応答して、それ以上何の行動も取らないステップと、が含まれる。

10

#### 【0005】

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する非一時的コンピュータ可読記憶媒体が含まれる。ステップには、特定の被管理サーバの第1の記述を修正して、特定の被管理サーバの変更された状態を示し、それによって、特定の被管理サーバの第2の記述を指定する、ステップが含まれる。ステップには、未修正の第1の記述を、第2の記述と比較し、それによって、記述変更を指定するステップが、さらに含まれる。ステップには、記述変更に基づき、特定の被管理サーバに以前送られたマネージメント命令を更新すべきかどうかを判定するステップが、さらに含まれる。ステップには、特定の被管理サーバのマネージメント命令を更新するという判定に応答して、第2の記述に基づき、ルールセット内のどのルールが、特定の被管理サーバに現在関連するのかを判定し、それによって、現在の関連ルールを指定する、ステップと、現在の関連ルールが、以前の関連ルールと異なるかどうかを判定するステップであって、以前の関連ルールは、未修正の第1の記述に基づき判定された、ステップと、現在の関連ルールが、以前の関連ルールと同一であるという判定に応答して、それ以上何の行動も取らないステップと、が含まれる。

20

#### 【図面の簡単な説明】

#### 【0006】

【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）のため環境を説明する、上位レベルのブロック図である。

30

【図2】一実施形態に係る、図1で説明される1つまたは複数のエンティティ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、被管理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、特定の被管理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、被管理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。

40

【図7】一実施形態に係る、被管理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】

#### 【0007】

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。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

50

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。実用可能な限り、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、同様または同類の機能性を示してよい、ことに留意されたい。

#### 【0008】

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、企業自身により、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）によって、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、複数の被管理サーバ130、および、複数の非管理デバイス140、が含まれる。複数の被管理サーバ130および複数の非管理デバイス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つの被管理サーバ130、および、2つの非管理デバイス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、被管理サーバ130、および／または非管理デバイス140を、有することができる。

#### 【0009】

ネットワーク110は、グローバルマネージャ120と、被管理サーバ130と、非管理デバイス140と、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。

#### 【0010】

被管理サーバ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の空間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レベルの仮想化に従う、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）のユーザの空間インスタンスである。被管理サーバ130が物理的機械である場合、被管理サーバ130は、コンピュータまたはコンピュータのセットである。被管理サーバ130が仮想機械である場合、被管理サーバ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する。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）を許可されるかどうか、またはサービスを消費する（もしくは提供する）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）に許可されるのか、またはサービスを消費する（もしくは提供する）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、実行可能プロセスの制御、を指定することができる。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。

#### 【0011】

被管理サーバ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

10

20

30

40

50

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（Windows Filtering Platform（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。

#### 【0012】

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エントリおよびipsetエントリとして、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。

#### 【0013】

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) 被管理サーバ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（ポリシーが被管理サーバ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、被管理サーバ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。

#### 【0014】

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をすでに有するデバイス上にロードされ、それによって、デバイスを、非管理デバイス140から被管理サーバ130に変換させる。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。

#### 【0015】

非管理デバイス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。非管理デバイス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、被管理サーバ130と非管理デバイス140との間の相互作用が、（被管理サーバ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に統轄されてよい。非管理デバイス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。非管理デバイス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。

#### 【0016】

グローバルマネージャ120は、被管理サーバ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

10

20

30

40

50

インフラの状態 3 2 0、および、b) 管理ドメイン規模のマネージメントポリシー 3 3 0、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 3 2 0 には、被管理サーバ 1 3 0 の記述と、（選択的に）非管理デバイス 1 4 0 の記述と、が含まれる。グローバルマネージャ 1 2 0 はまた、被管理サーバ 1 3 0 から受け取るローカル状態情報を処理する。

#### 【0 0 1 7】

管理ドメイン規模のマネージメントポリシー 3 3 0 は、I P アドレス、I P 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する被管理サーバ 1 3 0 を参照しない、論理的マネージメントモデルに基づく。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く被管理サーバ 1 3 0 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／I P 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。

#### 【0 0 1 8】

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。

#### 【0 0 1 9】

【表 1】

| 次元       | 意味 (M) 、 値 (V)                                                                                                                                              |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 役割       | M：管理ドメイン内の被管理サーバの役割<br>V：ウェブ、A P I、データベース                                                                                                                   |
| 環境       | M：被管理サーバのライフサイクル段階<br>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：被管理サーバが属する論理アプリケーション（被管理サーバの、より上位レベルのグループ分け）<br>V：取引、人材                                                                                                   |
| 業種       | M：被管理サーバが属する事業単位<br>V：マーケティング、エンジニアリング                                                                                                                      |
| ロケーション   | M：被管理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。<br>V：U S または E U （物理的）、u s - 西 - 1 または u s - 東 - 2 （論理的） |

表 1－論理的マネージメントモデルの例

#### 【0 0 2 0】

論理的マネージメントモデルは、グループ内の被管理サーバ 1 3 0 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、複数の被管理サーバ 1 3 0 がまとめてグループ化されることができるようになる。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 つの次元についてゼロ個の値または 1 個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、管理ドメインの被管理サーバ130の区分および分類と、被管理サーバ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、単一の被管理サーバ130が、複数の重複するセット（すなわち、被管理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、単一の被管理サーバ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。

#### 【0021】

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、特定のポリシーに統轄される被管理サーバ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、被管理サーバ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のグループの被管理サーバ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のグループの被管理サーバおよび第2のグループの被管理サーバ（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））／セキュアハッシュアルゴリズム（Secure Hash Algorithm-2（SHA-2）））に制限されてよい。

#### 【0022】

環境100内の各被管理サーバ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（ポリシーが被管理サーバ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。

#### 【0023】

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。

#### 【0024】

図2は、一実施形態に係る、図1で説明される1つまたは複数のエンティティ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に連結される少なくとも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に連結され、ディスプレイ装置218が、グラフィックアダプタ212に連結される。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に連結される。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に直接連結される。

#### 【0025】

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て、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信するためのタッチスクリーン能力が含まれる。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に連結する。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／または被管理サーバ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、非管理デバイス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。

10

#### 【0026】

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。

#### 【0027】

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、およびプロセッシングサーバ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、プロセッシングサーバ310に、要求に応じて、管理ドメイン状態320とマネジメントポリシー330とへのアクセスを提供するサーバが含まれる。

20

#### 【0028】

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、被管理サーバ130の記述と、（選択的に）非管理デバイス140の記述と、が含まれる。被管理サーバ130の記述には、例えば、一意識別子（`unique identifier`（以下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）、ネットワーク露出情報、サービス情報、および、被管理サーバ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。

30

#### 【0029】

UIDは、被管理サーバ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、被管理サーバ130がオンラインかオフラインか、を示す。「構成特徴」は、被管理サーバ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被管理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、

40

#### 【0030】

ネットワーク露出情報は、被管理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、ネットワーク露出情報には、被管理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`（以下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、ネットワーク露出情報には、ルーティング情報、および／または、被管理サーバが、ネットワークアドレス変換器（`network address trasnlator`（以下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

50

、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。ネットワーク露出情報（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。

#### 【0031】

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、被管理サーバ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ニングしているのか、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、被管理サーバ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）が被管理サーバ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。

#### 【0032】

非管理デバイス140の記述には、例えば、ネットワーク露出情報（例えば、非管理デバイスのIPアドレス、および、非管理デバイスが接続されるBRNの識別子）が含まれる。非管理デバイス140は、「非管理デバイスグループ」（`unmanaged device group`（以下UDG））の一部である。UDGには、1つまたは複数の非管理デバイス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バ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（`unique identifier`（以下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内の非管理デバイス140に関する情報（例えば、非管理デバイスのネットワーク露出情報）、が含まれる。

#### 【0033】

被管理サーバ130および非管理デバイス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（`graphical user interface`（以下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（`application programming interface`（以下API））を介して、グローバルマネージャ120と相互作用することにより、管理ドメイン状態320にロードされてよい。被管理サーバ130の記述はまた、被管理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。

#### 【0034】

特に被管理サーバのラベルに関して（および、ある場合は、構成特徴）、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、被管理サーバ130をプロビジョ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CF Engine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。

#### 【0035】

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／C

10

20

30

40

50

C 値を計算する。ラベル／C C 割り当てルールは、管理ドメイン状態 3 2 0 からのデータにアクセスし、ラベルまたは C C 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／C C 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 1 2 0 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／C C 割り当てルールは、初期化プロセス中に、被管理サーバ 1 3 0 について評価されてよい。そして、ラベル／C C 値の示唆は、任意の次元／C C 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、被管理サーバ 1 3 0 が、P o s t g r e s データベースまたは M y S Q L 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。被管理サーバが、L i n u x 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 C C は、「L i n u x」であってよい。

10

**【0036】**

別の実施形態において、ラベル／C C エンジン、は、クラスタ分析に基づき、ラベル／C C 値を計算する。例えば、ラベル／C C 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、m i n - c u t アルゴリズムおよび K - m e a n s アルゴリズムの組み合わせを使用して、上位に接続された被管理サーバ 1 3 0 のクラスタを自動的に識別する。被管理サーバ 1 3 0 のクラスタは、管理ドメイン 1 5 0 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、アプリケーションの次元（または、任意の他の次元）について値を、それらの被管理サーバ 1 3 0 に、一斉に適用することを選択することができる。

20

**【0037】**

管理ドメイン規模のマネージメントポリシー 3 3 0 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。

**【0038】**

ルール機能ー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、となり得る。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、ということの意味する。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け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。

30

40

**【0039】**

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、であってよい。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、同様に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（O S I）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獲得するためのト

50

リガー、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。

#### 【0040】

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を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。

10

#### 【0041】

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内の被管理サーバ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。被管理サーバ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、露出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、サービスを露出させるかを指定する。

#### 【0042】

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、被管理サーバ130および／または非管理デバイス140である。

20

#### 【0043】

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。

30

#### 【0044】

提供元（provided-by（以下PB））部分は、どの被管理サーバ130および／または非管理デバイス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」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、任意の被管理サーバ130または非管理デバイス140）が、サービスを提供することが可能である。PB部分が「Any managed server（どの被管理サーバでも）」を示す場合、どの被管理サーバ130も、サービスを提供することが可能である。（「Any managed server（どの被管理サーバでも）」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、全ての被管理サーバ130をマッチングする）。使用元（used-by（以下UB））部分は、どの被管理サーバ130および／または非管理デバイス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（どの被管理サーバでも）」を示すこともできる。

40

#### 【0045】

PB部分およびUB部分内には、被管理サーバ130が、ラベルセット（すなわち、被管理サーバを記述する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被管理サーバ130を指定する能力は、論理的マネージメントモデルに由来するもので、被管理サーバを、その次元および値（ラベル）に基づき参照する。非管理デバイス140は、非管理デバイスグループ（UDG）のUIDを使

50

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、そのグループ内の非管理デバイス140に関する追加情報（例えば、デバイスのネットワーク露出情報）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（被管理サーバ130を指定するための）、被管理サーバの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。

#### 【0046】

ルール条件部分は、選択的なものであり、ルールが、特定の被管理サーバ130、および／または、その被管理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内の被管理サーバの記述の一部である）、および／または、ネットワーク露出情報（例えば、ネットワークインターフェースのBR識別子、これも管理ドメイン状態320内の被管理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、特定の被管理サーバに適用されるかどうかを指定し、一方、式のネットワーク露出情報部分は、ルールが、その被管理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、特定の被管理サーバの構成特徴について（詳細には、その被管理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」となる場合、ルールは、その被管理サーバ、および、その被管理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」となるを評価する場合、ルールは、その被管理サーバ、および、その被管理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被管理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、ルールが特定の被管理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。

#### 【0047】

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、どの被管理サーバ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、被管理サーバ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被管理サーバ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。

#### 【0048】

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、ウェブサービスティアが、データベースティア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ティアが、ウェブサービスティア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。

#### 【0049】

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、記述されてあることは、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のティア）にアクセスし、ウェブサーバがデータベースサーバ（第2のティア）にアクセスする、2ティア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のティア

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のティアにおいて、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。

#### 【0050】

ウェブサーバおよびデータベースサーバは、被管理サーバ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＞

10

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。）

#### 【0051】

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。

20

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

30

- #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（どの被管理サーバでも）

40

#### 【0052】

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内の被管理サーバ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。

#### 【0053】

50

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、アプリケーション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。アプリケーションサービスが、サービス部分の「アプリケーション」によって指定される。

#### 【0054】

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。

#### 【0055】

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。

#### 【0056】

ルールリスト#2は、任意の被管理サーバが、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、ということを示す。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。「任意の被管理サーバ」が、UB部分の「Any managed server（どの被管理サーバでも）」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。

#### 【0057】

上記の例から離れて、以下の2つの被管理サーバ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＞

#### 【0058】

アクセス制御ルールが、a p p 1の一部である全ての被管理サーバ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、お互いに通信することが許可され、a p p 2の一部であるドイツの被管理サーバ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）。

#### 【0059】

図3に戻って、プロセッシングサーバ310は、被管理サーバ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。プロセッシングサーバ310はまた、被管理サーバ130から受け取るローカル状態情報を処理する。プロセッシングサーバ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、アクターエニユ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、プロセッシングサーバ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、アクターエニユ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。

#### 【0060】

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、特定の被管理サーバ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、所与の被管理サーバ130用の関連ルールのみを抽出することによる、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、スコープがこの被管理サーバ130に適用されるかどうかを判定すること、および（スコープがこの被管理サーバ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被管理サーバ130に適用されるかどうかを判定すること、によって行う。ルールが被管理サーバ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、被管理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、その被管理サーバについて（詳細には、被管理サーバの構成特徴の値およびネットワーク露出情報について）、「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、この被管理サーバ130がサービスを提供するルール、1つは、この被管理サーバ130がサービスを消費するルール、である。

#### 【0061】

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、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被管理サーバ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、被管理サーバ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

10

20

30

40

50

UB部分内に、被管理サーバ（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。

#### 【0062】

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）により参照される被管理サーバが、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を生成する（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）。

10

#### 【0063】

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ならびに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部分で被管理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、その被管理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を生成する（例えば、被管理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）。

20

#### 【0064】

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、最高優先度の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、被管理サーバ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、適切な被管理サーバ130および／または非管理デバイス140（例えば、入力されたルールにおいて参照された被管理サーバ130および／または非管理デバイス140）を参照し、ルールに関連するサービスのネットワーク露出の詳細を考慮に入れる。

30

#### 【0065】

ここで、機能レベル命令生成モジュール360は、特定の被管理サーバ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、その被管理サーバが、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、被管理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、被管理サーバのローカル状態（例えば、被管理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被管理サーバに送られる。被管理サーバは、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、以下で説明するように、ポリシーコンパイルモジュール410を参照して、機能レベルの命令を処理する。

40

#### 【0066】

アクターエニュメレーションモジュール370は、被管理サーバ130および非管理デバイスグループ（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

50

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のこれらの記述の表現を、エニユメレート(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、アクターエニユメレーションモジュール370は、被管理サーバ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ユメレートし、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、被管理サーバの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。

#### 【0067】

N個の次元 $D_i$  ( $i = 1, \dots, N$ )の集合を含み、各次元 $D_i$ が、可能性ある値 $V_j$  ( $j = 1, \dots, M_i$ )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、アクターエニユ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ユメレートし、これは、 $S_1 \times S_2 \times \dots \times S_N$ で得られるデカルト積に等しい。この集合のサイズは $M_1 \times M_2 \times \dots \times M_N$ である。エニユメレーションプロセスでは、被管理サーバ130の多次元ラベル空間を、単純なエニユメレートされた形式に縮約する。

#### 【0068】

別の実施形態において、アクターエニユ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内の被管理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ユメレートする。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「 $\langle X=A \rangle, \langle Y=B \rangle$ 」を持つ被管理サーバは、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)「 $\langle X=A \rangle \langle Y=B \rangle$ 」、2)「 $\langle X=A \rangle \langle Y=* \rangle$ 」、3)「 $\langle X=* \rangle \langle Y=B \rangle$ 」、および、4)「 $\langle X=* \rangle \langle Y=* \rangle$ 」。ここで、被管理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、被管理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、アクターエニユ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ユメレートする。ラベルセット「 $\langle X=A \rangle, \langle Y=B \rangle$ 」を持つ被管理サーバが、ラベルセット「 $\langle X=A \rangle, \langle Y=A \rangle$ 」のメンバーであることはなく、そのため、アクターエニユメレーションモジュール370は、そのラベルセットをエニユメレートしない。

#### 【0069】

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(被管理サーバの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(被管理サーバ130または非管理デバイス140)のIPアドレス、が含まれる。例えば、アクターセットには、 $\langle$ 役割, データベース $\rangle$ および $\langle$ 環境, プロダクション $\rangle$ のラベルセットによりカバーされる被管理サーバ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における非管理デバイス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、被管理サーバ130または非管理デバイス140)が、複数のアクターセット内に見られてよい。

#### 【0070】

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、 $\langle$ 役割, データベース $\rangle$ および $\langle$ 環境, プロダクション $\rangle$ のラベ

10

20

30

40

50

ルセットについて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、それら被管理サーバ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、それら同じ被管理サーバ用の異なるアクターセットが、それら被管理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。

#### 【0071】

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、被管理サーバの記述（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、被管理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。

10

#### 【0072】

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。）

20

#### 【0073】

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。

#### 【0074】

ネットワーク露出情報の変更－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。

30

40

#### 【0075】

50

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、エニユメレートされた形式の被管理サーバ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被管理サーバ130に送られる。

10

**【0076】**

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。

**【0077】**

ポリシーエンジンモジュール340は、被管理サーバ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320の状態、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、マネージメント命令を生成する（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、アクターエニユ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を使用して）。

20

**【0078】**

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、特定の被管理サーバ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、アクターエニユ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。アクターエニユメレーションモジュール370は、管理ドメイン状態320内のエニユメレートされた形式の、被管理サーバ130および非管理デバイスグループ（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（エニユ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、特定の被管理サーバ130に送る。

30

40

**【0079】**

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、特定の被管理サーバ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

50

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、（特定の被管理サーバ 130 に特有でない）アクターセットをキャッシュする。

#### 【0080】

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 に対する変更が、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、被管理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 に対する変更が、被管理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、被管理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）被管理サーバ 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／または被管理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。

#### 【0081】

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）、変更を被管理サーバ 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  
20  
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（以前、アクターエニメレーションモジュールにより出力された）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 内の被管理サーバ 130 の全てに送る。しかし、その実施形態は不十分であり、それは、全てのアクターセットに対する変更によって、全ての被管理サーバが影響を受けるわけではないからである。

#### 【0082】

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、特定の被管理サーバには、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、特定の被管理サーバに送られる。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、被管理サーバの UID または UDG の UID）、および、その  
40  
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。

#### 【0083】

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、被管理サーバ 130 を、その被管理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、被管理サーバ 130 を、その被管理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、被管理サーバ 130 は、例えば、その被管理サーバの 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、どの被管理サーバの記述が変更された  
50

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、その被管理サーバが、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、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、どの被管理サーバに、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、それらの被管理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。

#### 【0084】

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、被管理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被管理サーバに送る。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、被管理サーバ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、以前生成された被管理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、再生成されて被管理サーバに再送信される必要はない。

#### 【0085】

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到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到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、（以前被管理サーバに送られた、キャッシュされた機能レベルの命令と比較して）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、被管理サーバに命令して、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。

#### 【0086】

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。

#### 【0087】

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、アクターセットを何も被管理サーバに送らない。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、被管理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と比較して、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、被管理サーバに命令して、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と比較して、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。

#### 【0088】

ポリシーエンジンモジュール340が、被管理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、被管理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との相互作用により、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、自動化されたプロセスにより生成される（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）。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、被管理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、被管理サーバに送る。しかし、多少の違いが存在する。

#### 【0089】

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、必ずしも全ての被管理サーバ130用のマネージメント命令を更新するわけではない。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と比較して、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、どの被管理サーバ130が、変更されたルールにより影響を受けるのか（例えば、どの被管理サーバが、a）ルールおよび／またはスコープの、PB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、被管理サーバ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。

#### 【0090】

管理ドメイン状態更新（administrative domain state update（以下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、被管理サーバ130の記述の、追加、削除、もしくは修正（被管理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、非管理デバイスもしくは非管理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、特定の被管理サーバ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との相互作用により、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、自動化されたプロセスにより生成される（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）。

#### 【0091】

例えば、A D S Uモジュール385は、特定の被管理サーバ130に関する変更を受け取る。A D S Uモジュール385は、新しい情報を、特定の被管理サーバ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、A D S Uモジュール385は、（選択的に）被管理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、A D S Uモジュール385は、被管理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／または被管理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。A D S U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、A D S U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、A D S U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。A D S Uモジュール385が、被管理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、A D S U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、被管理サーバのマネージメント命令を更新する。一実施形態において、A D S U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に命令して被管理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。

10

#### 【0092】

A D S Uモジュール385が、管理ドメインのアクターセットおよび／または被管理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、被管理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、A D S Uモジュール385は、この判定を、表2に示すように行う。

20

#### 【0093】

#### 【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<br>被管理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<br>被管理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<br>被管理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<br>被管理サーバのマネージメント命令：はい                            |
| ネットワーク露出情報    | 管理ドメインのアクターセット：はい<br>被管理サーバのマネージメント命令：はい<br>(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<br>被管理サーバのマネージメント命令：はい<br>(指定の状況においてのみ)           |

30

40

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／または被管理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

#### 【0094】

一実施形態において、A D S U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／C Cエンジンは、サーバの記述と、ラベル／C C割り当てルールとに基づき、サーバについてラベル／C C値を計算する。

#### 【0095】

50

別の実施形態において、A D S Uモジュール385は、サーバが、ネットワークアドレス変換器（N A T）の後方にあるかどうか（および、N A Tの後方にある場合は、どのタイプのN A T、すなわち、1：1または1：N、であるのか）、を判定する。例えば、A D S U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T C P接続に係る、サーバのI P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I Pアドレスと、を比較することにより、N A Tが、グローバルマネージャ120と被管理サーバ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、N A Tは、グローバルマネージャ120と被管理サーバ130との間に存在する。N A Tが存在しない場合、A D S U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、N A Tのタイプ（1：1または1：N）を判定する。例えば、A D S U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I Pアドレスによって、識別する。（あるいは、被管理サーバが、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N A T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N A T情報も、特定のデータセンターに関連付けされない場合、A D S Uモジュール385は、N A Tのタイプが1：Nであると想定する。

10

#### 【0096】

図4は、一実施形態に係る、被管理サーバ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、被管理サーバ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、被管理サーバのオペレーティングシステム（O S）、ネットワーク露出、およびサービス、に関する情報を記憶する。O S情報には、例えば、どのO Sが実行中であるかの指標が含まれる。ネットワーク露出情報およびサービス情報は、管理ドメイン状態320内の被管理サーバ130の記述について、上記で説明した。

20

#### 【0097】

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、被管理サーバ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、機能レベルの命令（機能レベル命令生成モジュール360により生成される）と、関連アクターセット（関連アクターモジュール380により出力される）と、を含む。被管理サーバ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）被管理サーバが電源が入るか、オンラインになる、b）被管理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、ことによりトリガーされる。

30

#### 【0098】

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、L i n u xオペレーティングシステムのi p t a b l e sエントリおよびi p s e tエントリ、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（W F P）のルール、にマッピングする。

40

#### 【0099】

被管理サーバ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、被管理サーバのピア（すなわち、リレーションシップ内の他方のアクター）の

50

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。

#### 【0100】

別の例として、被管理サーバ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、被管理サーバのローカル状態を指定する部分が含まれる（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、被管理サーバのローカル状態（例えば、被管理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被管理サーバに送られる。ポリシーコンパイルモジュール410は、被管理サーバのローカル状態をチェックする（例えば、被管理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、被管理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、被管理サーバが、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内の被管理サーバ130の記述について、上記で説明した）。

#### 【0101】

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、被管理サーバ130が、「プロバイダ」またはエンドポイントである）。被管理サーバ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。被管理サーバ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、被管理サーバ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。

#### 【0102】

一実施形態において、被管理サーバ130は、そのアウトバウンド接続を監視する。被管理サーバ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。被管理サーバ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。

#### 【0103】

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、被管理サーバ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被管理サーバ130に送らない。代わりに、被管理サーバ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 から被管理サーバ 130 に送られる。

#### 【0104】

ローカル状態更新 (local state update (以下LSU)) モジュール 420 は、被管理サーバ 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、被管理サーバ 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、被管理サーバ 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 (ネットワークング情報)、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、ネットワーク露出情報を、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。

10

#### 【0105】

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、それ以上何の行動も取らない (ローカル状態情報が再度取得されるまで)。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。

20

30

#### 【0106】

図 5 は、一実施形態に係る、特定の被管理サーバ 130 用のマネ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 内の被管理サーバ 130 ごとに 1 回)。

#### 【0107】

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。

40

#### 【0108】

ステップ 510 にて、管理ドメイン状態 320 と、管理ドメイン規模のマネジメントポリシー 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ジメントポリシー 330 と、を応答として受け取る。

#### 【0109】

ステップ 520 にて、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

50

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、特定の被管理サーバ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。

#### 【0110】

ステップ530にて、アクターがエニューメレートされる。例えば、ポリシーエンジンモジュール340は、アクターエニュー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。アクターエニューメレーションモジュール370は、管理ドメイン状態320内のエニューメレートされた形式の、被管理サーバ130および非管理デバイスグループ（UDG）の表現（「アクターセット」）を生成する。

10

#### 【0111】

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。

#### 【0112】

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、アクターセット（ステップ530にて生成された）と、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）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。

20

#### 【0113】

ステップ560にて、マネージメント命令が特定の被管理サーバ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、を特定の被管理サーバ130に送る。

#### 【0114】

なお、ステップ520および540は、特定の被管理サーバ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、その被管理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pointsの生成とは、最小限でもお互いに依存する。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、並行して実行されてよい（例えば、同じ被管理サーバ130についてであっても）。加えて、異なる被管理サーバ130についての観points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、再エニューメレートされる必要が無い。）

30

40

#### 【0115】

図6は、一実施形態に係る、被管理サーバ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。

#### 【0116】

方法600が開始されるとき、被管理サーバ130のローカル状態に関する情報が、被

50

管理サーバ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。

【0117】

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。

【0118】

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、被管理サーバ130のローカル状態に関する情報にアクセスする。

10

【0119】

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、マネージメント命令（ステップ610にて受け取られた）と、ローカル状態（ステップ620にてアクセスされた）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。

【0120】

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構成134（ステップ630にて生成された）に従って動作するべく、マネージメントモジュール132を構成する。

20

【0121】

図7は、一実施形態に係る、被管理サーバ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。

【0122】

方法700が開始されるとき、被管理サーバ130のローカル状態に関する情報が、被管理サーバ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。

30

【0123】

ステップ710にて、被管理サーバ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、被管理サーバ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。

【0124】

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。情報が異なる場合、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。

40

【0125】

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。

【0126】

ステップ750にて、マネージメントモジュール構成134は、再生成され（ローカル状態リポジトリ400の内容が変更されたため）、マネージメントモジュール132がそれに従って、再生成される。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。

【0127】

50

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。

#### 【0128】

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。

#### 【0129】

ステップ810にて、特定の被管理サーバ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、ネットワーク露出情報、および／または、サービス情報を、被管理サーバ130から、ローカル状態情報の一部として受け取る。

10

#### 【0130】

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、ネットワーク露出情報、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、情報が関連する被管理サーバ130の記述内)に記憶する。

#### 【0131】

20

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。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(optional)なものである。

#### 【0132】

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は被管理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。

30

#### 【0133】

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。たとえば、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。

#### 【0134】

40

ステップ860にて、被管理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、被管理サーバの記述に対する変更に基づき、被管理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。被管理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。被管理サーバのマネージメント命令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。

#### 【0135】

ステップ870にて、被管理サーバのマネージメント命令が更新される。たとえば、ADSUモジュール385は、ポリシーエンジンモジュール340に命令して被管理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

50

ル 3 8 5 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 3 4 0 に命令して被管理サーバのマネージメント命令を更新させる。

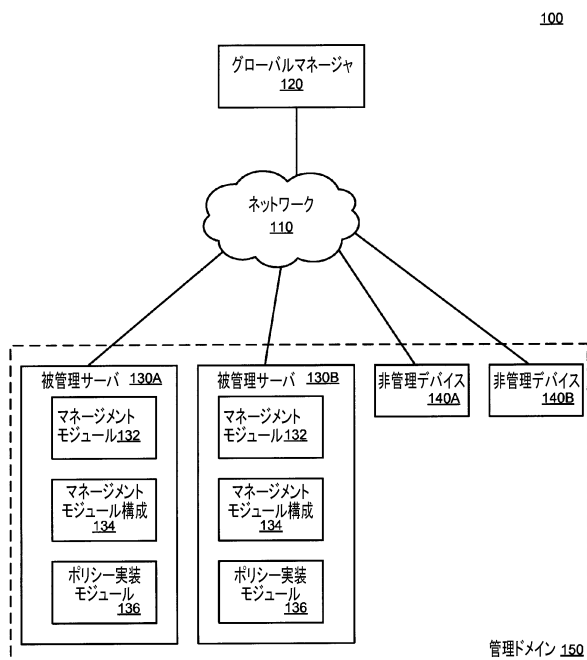
【0136】

ステップ 8 8 0 にて、方法が終了する。

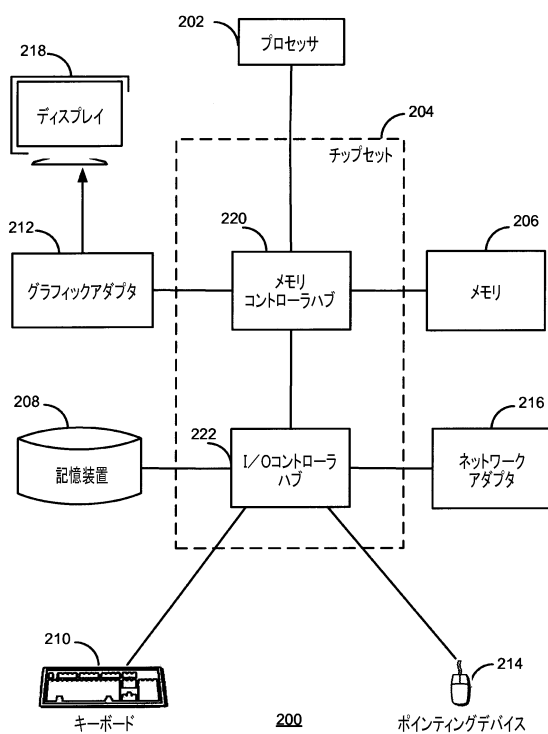
【0137】

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。

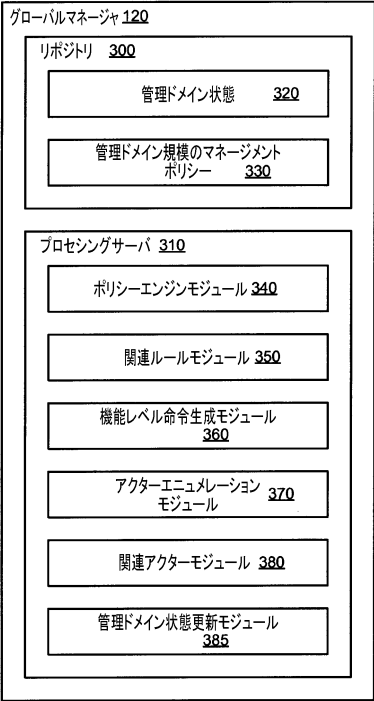
【図 1】



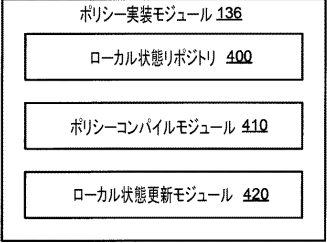
【図 2】



【図 3】

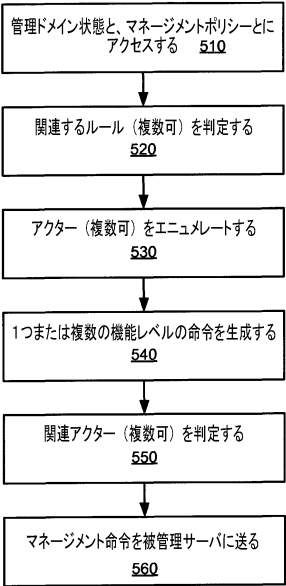


【図 4】



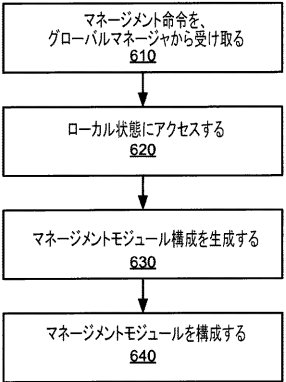
【図 5】

500

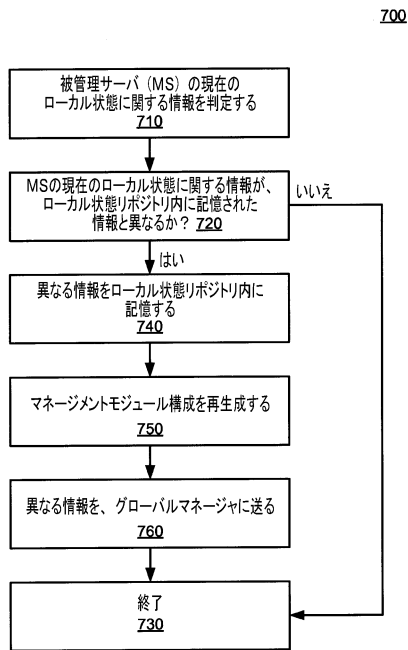


【図 6】

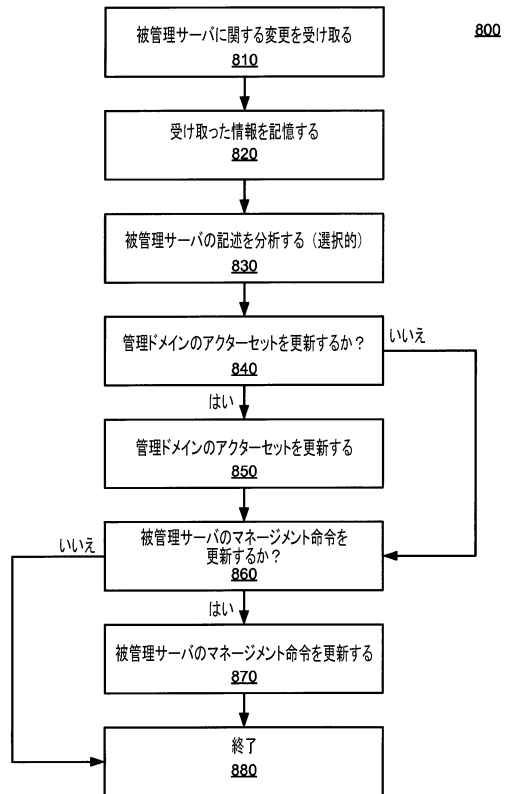
600



【図 7】



【図 8】



## 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 セヒョ 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 北川 純次

- (56)参考文献 国際公開第2006/043322 (WO, A1)  
米国特許出願公開第2012/0023546 (US, A1)  
特開2005-174201 (JP, A)  
岡 英一・他, 分散処理システム運転管理方式の一考察, 電子情報通信学会技術研究報告 Vo  
1. 94 No. 362, 日本, 社団法人電子情報通信学会, 1994年11月24日, 第94巻  
第362号, pp.43~48

- (58)調査した分野(Int.Cl., DB名)  
G06F 13/00  
H04L 12/24