

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2017-502620

(P2017-502620A)

(43) 公表日 平成29年1月19日(2017.1.19)

(51) Int.Cl. F I テーマコード (参考)
H04L 12/71 (2013.01) H04L 12/71 5K030

審査請求 未請求 予備審査請求 未請求 (全 53 頁)

(21) 出願番号	特願2016-552416 (P2016-552416)	(71) 出願人	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, サニーベイル, サン ガブリエル ドライブ 160
(86) (22) 出願日	平成26年9月8日 (2014.9.8)	(74) 代理人	110001243 特許業務法人 谷・阿部特許事務所
(85) 翻訳文提出日	平成28年7月4日 (2016.7.4)	(72) 発明者	ポール ジェイ. カーナー アメリカ合衆国, カリフォルニア州 94 086, サニーベイル, 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
(86) 国際出願番号	PCT/US2014/054505		
(87) 国際公開番号	W02015/076904		
(87) 国際公開日	平成27年5月28日 (2015.5.28)		
(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	14/474,916		
(32) 優先日	平成26年9月2日 (2014.9.2)		
(33) 優先権主張国	米国 (US)		

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セキュリティ

(57) 【要約】

管理ドメイン内のマネージドサーバ (MS) が隔離される。管理ドメインには、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する複数MSが含まれ、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行するようにされる。隔離されたMSを、他のMSから分離する。MSの記述を変更して、MSが隔離されることを示し、それによって、隔離されたMSの記述を指定する。キャッシュしたアクターセットを更新して、隔離されたMSの変更後状態を示し、それによって、更新されたアクターセットを指定する。更新されたアクターセットのどれが他のMSに関連するのか、に関して判定を行い、それによって、現在関連する更新後アクターセットを指定する。現在関連する更新後アクターセットが、他のMSに以前送ったアクターセットと異なるかどうか、に関して判定を行う。現在関連する更新後アクターセットが、以前送ったアクターセットと同一である、という判定に応じて、それ以上アクションを取らない。

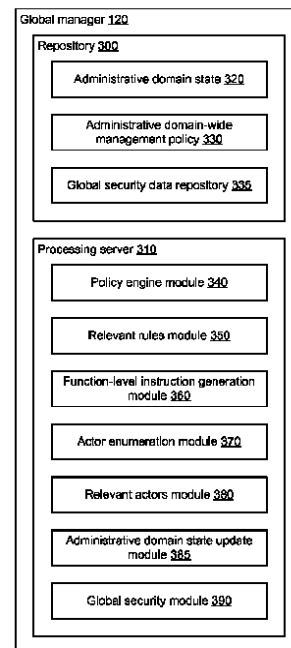


FIG. 3

【特許請求の範囲】**【請求項 1】**

不正プロセスを検出して報告する方法であって、前記方法は、

マネージドサーバ上で実行しているプロセスから、アクションを実行するための要求を受信するステップと、

前記マネージドサーバ内のマネージメントモジュールに従って、前記アクションが不適切であることを判定するステップであって、前記マネージメントモジュールが、グローバルマネージャから受信されたマネージメント命令を使用して、管理ドメイン規模のマネージメントポリシーを実行するように前記マネージドサーバによって構成された、ステップと、

前記不適切なアクションに関する情報、または前記プロセスに関する情報を前記グローバルマネージャに送るステップと

を備えたことを特徴とする方法。

【請求項 2】

前記不適切なアクションに関する情報が、前記不適切なアクションのタイプ、前記不適切なアクションのタイプに基づく前記不適切なアクションの詳細、または前記不適切なアクションがいつ発生したのかを示しているタイムスタンプを含むことを特徴とする請求項 1 に記載の方法。

【請求項 3】

前記プロセスに関する情報が、前記プロセスの名称、前記プロセスがリッスンしているネットワークポート、前記プロセスがリッスンしているネットワークインターフェース、前記プロセスを起動したユーザ、前記プロセスの構成、前記プロセスのコマンドライン `launch` 引数、または前記プロセスの依存関係を含むことを特徴とする請求項 1 に記載の方法。

【請求項 4】

前記プロセスが、ドメイン名システム（DNS）ルックアップを要求したことを判定するステップと、

前記 DNS ルックアップに関する情報を前記グローバルマネージャに送るステップとをさらに備えたことを特徴とする請求項 1 に記載の方法。

【請求項 5】

前記プロセスが、ネットワーク接続を行うことを試みたことを判定するステップと、

前記グローバルマネージャに、前記ネットワーク接続に関する情報を送るステップと

をさらに備えたことを特徴とする請求項 1 に記載の方法。

【請求項 6】

前記グローバルマネージャに送られた情報が、前記グローバルマネージャにより使用され、前記マネージドサーバが隔離されるべきかどうかを判定することを特徴とする請求項 1 に記載の方法。

【請求項 7】

前記アクションが、ネットワーク接続を起動するこ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 8】

前記アクションが、ネットワークポート上でリッスンすること、またはネットワークインターフェース上でリッスンするこ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 9】

前記アクションが、ユーザのコンテキストで実行するこ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 10】

前記アクションが、共有オブジェクトをロードするこ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 11】

管理ドメイン内のマネージドサーバを隔離する方法であって、前記管理ドメインには、構成し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行するように、隔離したマネージドサーバが、複数のマネージドサーバにおける他のマネージドサーバから分離されるように、マネージメント命令を使用して前記マネージメントモジュールを構成する前記複数のマネージドサーバを含み、前記方法は、

前記マネージドサーバの記述を変更して、前記マネージドサーバが隔離されることを示し、それによって、前記隔離したマネージドサーバの記述を指定するステップと、

キャッシュしたアクターセットを更新して、前記隔離したマネージドサーバの変更後状態を示し、それによって、更新したアクターセットを指定するステップと、

更新したアクターセットのどれが他のマネージドサーバに関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定するステップと、

前記現在関連する更新後アクターセットが、前記他のマネージドサーバに以前送っ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後アクターセットが、前記以前送ったアクターセットと同一であるという判定に応じて、それ以上アクションは取らないステップと

を備えたことを特徴とする方法。

【請求項 1 2】

前記隔離したマネージドサーバの第 1 の記述を変更して、前記隔離したマネージドサーバが隔離されることを示すステップが、前記隔離したマネージドサーバの隔離固有に構成した特徴に対して値を設定するステップを含むことを特徴とする請求項 1 1 に記載の方法。

【請求項 1 3】

前記マネージドサーバを隔離することを判定するステップをさらに備えたことを特徴とする請求項 1 1 に記載の方法。

【請求項 1 4】

前記マネージドサーバを隔離することを判定するステップが、ネットワーク攻撃が前記マネージドサーバから生じたことを判定するステップ、または前記マネージドサーバが脆弱性を有することを判定するステップを含むことを特徴とする請求項 1 3 に記載の方法。

【請求項 1 5】

前記現在関連する更新後アクターセットが、前記以前送ったアクターセットとは異なるという判定に応じて、

前記以前送ったアクターセットと比較して、追加、削除または変更されるべき、更新したアクターセットを判定するステップと、

前記更新したアクターセット、および前記更新したアクターセットを追加、削除、または変更するための命令を前記他のマネージドサーバに送るステップと

をさらに備えたことを特徴とする請求項 1 1 に記載の方法。

【請求項 1 6】

前記更新したアクターセット、および前記命令を送るステップは、前記隔離したマネージドサーバから生じたインバウンドのネットワークトラフィックを前記他のマネージドサーバにブロックさせることを特徴とする請求項 1 5 に記載の方法。

【請求項 1 7】

前記キャッシュしたアクターセットを更新するステップの前に、

前記隔離したマネージドサーバの前記記述に基づき、前記隔離したマネージドサーバに関する追加の情報を判定するステップと、

前記隔離したマネージドサーバの前記記述を変更して、前記追加の情報を示すステップと

をさらに備えたことを特徴とする請求項 1 1 に記載の方法。

【請求項 1 8】

前記隔離したマネージドサーバの前記記述に基づき、前記ルールのセット内のルールの

10

20

30

40

50

どれが前記隔離したマネージドサーバに現在関連するのかを判定して、それによって、現在関連するルールを指定するステップと、

前記現在関連するルールが、以前関連したルールと異なるかどうかを判定するステップであって、前記以前関連したルールは、前記マネージドサーバの非変更の記述に基づき判定された、ステップと、

前記現在関連するルールが前記以前関連したルールと同一であるという判定に応じて、それ以上アクションは取らないステップと

をさらに備えたことを特徴とする請求項 11 に記載の方法。

【請求項 19】

前記現在関連するルールが、前記以前関連したルールと異なるという判定に応じて、

前記以前関連したルールと比較して、追加、削除または変更されるべきであるというルールを判定するステップと、

前記判定したルールに基づき、機能レベル命令を生成するステップと、

前記機能レベル命令、および前記機能レベル命令を追加、削除、または変更するための命令を前記隔離したマネージドサーバに送るステップと

をさらに備えたことを特徴とする請求項 18 に記載の方法。

【請求項 20】

前記機能レベル命令、および追加、削除、または変更するための前記命令を送るステップは、アウトバウンドのネットワークトラフィックを前記隔離したマネージドサーバにブロックさせることを特徴とする請求項 19 に記載の方法。

【請求項 21】

前記機能レベル命令、および追加、削除、または変更するための前記命令を送るステップは、管理のインバウンドのネットワークトラフィックのみを前記隔離したマネージドサーバに許可することを特徴とする請求項 19 に記載の方法。

【請求項 22】

更新したアクターセットのどれが前記隔離したマネージドサーバに関連するのかを判定し、それによって、第 2 の現在関連する更新後アクターセットを指定するステップと、

前記第 2 の現在関連する更新後アクターセットが、前記隔離したマネージドサーバに以前送られた第 2 の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、

前記第 2 の現在関連する更新後アクターセットが、前記以前送られた第 2 のアクターセットと同一であるという判定に応じて、それ以上アクションは取らないステップと

をさらに備えたことを特徴とする請求項 11 に記載の方法。

【請求項 23】

管理ドメイン内のアンマネージドデバイスグループの状態に対する変更を処理する方法であって、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構成されたマネージメントモジュールが実行するように、前記管理ドメインは、マネージメント命令を使用して前記マネージメントモジュールを構成する複数のマネージドサーバを含み、前記方法は、

前記アンマネージドデバイスグループの記述を変更して、アンマネージドデバイスを前記アンマネージドデバイスグループに追加するステップと、

キャッシュしたアクターセットを更新して、前記アンマネージドデバイスグループの変更後状態を示し、それによって、更新したアクターセットを指定するステップと、

更新したアクターセットどれがマネージドサーバに関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定するステップと、

前記現在関連する更新後アクターセットが、前記マネージドサーバに以前送っ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後アクターセットが、前記以前送ったアクターセットと同一であるという判定に応じて、それ以上アクションは取らないステップと

を備えたことを特徴とする方法。

【請求項 24】

前記アンマネージドデバイスを前記アンマネージドデバイスグループに追加することを判定するステップをさらに備えたことを特徴とする請求項 2 3 に記載の方法。

【請求項 2 5】

前記アンマネージドデバイスを前記アンマネージドデバイスグループに追加することを判定するステップが、前記アンマネージドデバイスがセキュリティ脅威をもたらすことを判定するステップを含むことを特徴とする請求項 2 3 に記載の方法。

【請求項 2 6】

前記現在関連する更新後アクターセットが、前記以前送ったアクターセットとは異なるという判定に応じて、

前記以前送ったアクターセットと比較して、追加、削除または変更されるべきである、更新したアクターセットを判定するステップと、

前記マネージドサーバに、前記更新したアクターセット、および前記更新したアクターセットを追加、削除、または変更するための命令を送るステップと

をさらに備えたことを特徴とする請求項 2 3 に記載の方法。

【請求項 2 7】

前記更新したアクターセット、および前記命令を送るステップは、前記アンマネージドデバイスから生じたインバウンドのネットワークトラフィックを前記マネージドサーバにブロックさせること、または前記アンマネージドデバイスに向けられたアウトバウンドのネットワークトラフィックを前記マネージドサーバにブロックさせることを特徴とする請求項 2 3 に記載の方法。

【請求項 2 8】

管理ドメイン内のマネージドサーバを隔離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コンピュータ可読記憶媒体であって、

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行するように、隔離したマネージドサーバが、複数のマネージドサーバのうちの他のマネージドサーバから、分離されるように、前記管理ドメインは、マネージメント命令を使用して前記マネージメントモジュールを構成する前記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が、

前記マネージドサーバの記述を変更して、前記マネージドサーバが隔離されることを示し、それによって、前記隔離したマネージドサーバの記述を指定するステップと、

キャッシュしたアクターセットを更新して、前記隔離したマネージドサーバの変更後状態を示し、それによって、更新したアクターセットを指定するステップと、

更新したアクターセットのどれが他のマネージドサーバに関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定するステップと、

前記現在関連する更新後アクターセットが、前記他のマネージドサーバに以前送っ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後アクターセットが、前記以前送ったアクターセットと同一であるという判定に応じて、それ以上アクションは取らないステップと

を含むステップを実行可能であ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。

【請求項 2 9】

管理ドメイン内のマネージドサーバを隔離するシステムであって、前記管理ドメインは、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行するように、隔離したマネージドサーバが、複数のマネージドサーバのうちの他のマネージドサーバから、分離されるように、マネージメント命令を使用して前記マネージメントモジュールを構成する前記複数のマネージドサーバを含み、前記システムは、

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であって、前記コンピュータプログラムモジュールが、

前記マネージドサーバの記述を変更して、前記マネージドサーバが隔離されることを

示し、それによって、前記隔離したマネージドサーバの記述を指定するステップと、

キャッシュしたアクターセットを更新して、前記隔離したマネージドサーバの変更後状態を示し、それによって、更新したアクターセットを指定するステップと、

更新したアクターセットのどれが、他のマネージドサーバに関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定するステップと、

前記現在関連する更新後アクターセットが、前記他のマネージドサーバに以前送っ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後アクターセットが、前記以前送ったアクターセットと同一である、という判定に応じて、それ以上アクションは取らないステップと

を含むステップを実行可能である、非一時的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

を備えたことを特徴とするシステム。

【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、ポリシーに従ってマネージされる。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。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。

【発明の概要】

【0003】

上記および他の論点は、管理ドメイン内のマネージドサーバを隔離するための、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。管理ドメインには、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する複数のマネージドサーバが含まれ、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行するようにされる。隔離したマネージドサーバは、該複数のマネージドサーバの中の他のマネージドサーバから分離される。方法の一実施形態は、マネージドサーバの記述を変更して、マネージドサーバが隔離されることを示し、それによって、隔離したマネージドサーバの記述を指定するステップを含む。方法は、キャッシュしたアクターセットを更新して、隔離したマネージドサーバの変更後状態を示し、それによって、更新されたアクターセットを指定するステップをさらに含む。方法は、更新されたアクターセットのどれが他のマネージドサーバに関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定するステップをさらに含む。方法は、現在関連する更新後アクターセットが、他のマネージドサーバに以前送っ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をさらに含む。方法は、現在関連する更新後アクターセットが、以前送ったアクターセットと同一である、という判定に応じて、それ以上アクションは取らないステップをさらに含む。

【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。上記ステップは、マネージドサーバの記述を変更して、マネージドサーバが隔離されることを示し、それによって、隔離したマネージドサーバの記述を指定

10

20

30

40

50

するステップを含む。上記ステップは、キャッシュしたアクターセットを更新して、隔離したマネージドサーバの変更後状態を示し、それによって、更新されたアクターセットを指定するステップをさらに含む。上記ステップは、更新されたアクターセットのどれが他のマネージドサーバに関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定するステップをさらに含む。上記ステップは、現在関連する更新後アクターセットが、他のマネージドサーバに以前送っ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をさらに含む。上記ステップは、現在関連する更新後アクターセットが、以前送ったアクターセットと同一である、という判定に応じて、それ以上アクションは取らないステップをさらに含む。

【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。上記ステップは、マネージドサーバの記述を変更して、マネージドサーバが隔離されることを示し、それによって、隔離したマネージドサーバの記述を指定するステップを含む。上記ステップは、キャッシュしたアクターセットを更新して、隔離したマネージドサーバの変更後状態を示し、それによって、更新されたアクターセットを指定するステップをさらに含む。上記ステップは、更新されたアクターセットのどれが他のマネージドサーバに関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定するステップをさらに含む。上記ステップは、現在関連する更新後アクターセットが、他のマネージドサーバに以前送っ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をさらに含む。上記ステップは、現在関連する更新後アクターセットが、以前送ったアクターセットと同一である、という判定に応じて、それ以上アクションは取らないステップをさらに含む。

【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行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。

【図9】一実施形態に係る、不正プロセスを検出して報告する方法を説明するフローチャートである。

【図10】一実施形態に係る、管理ドメイン内のマネージドサーバを隔離する方法を説明するフローチャートである。

【図11】一実施形態に係る、管理ドメイン内のアンマネージドデバイスのグループ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（単数または複数）および以下の記載では、単に例として、特定の実施形態について説明する。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

10

20

30

40

50

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をマネージするのを助ける、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。

【0009】

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】

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）を実行する機械（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、実行可能プロセスの制御、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。

【0011】

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、ポリシー実行モジュール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を実行する。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。

【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】

ポリシー実行モジュール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。ポリシー実行モジュール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を実行する（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。ポリシー実行モジュール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。

【0014】

一実施形態において、ポリシー実行モジュール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。ポリシー実行モジュール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】

アンマネージドデバイス140は、ポリシー実行モジュール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を実行しない。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との間の相互作用が、（マネージドサーバ130により実行されるような）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。

【0016】

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

10

20

30

40

50

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。

【0017】

管理ドメイン規模のマネージメントポリシー330は、「ラベル」と称される、上位レベルの特徴に基づくマネージドサーバ130を参照することができる論理的マネージメントモデルに基づく。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、および変更することを可能にする。

【0018】

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。

【0019】

【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

【0020】

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。

【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を実行する（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ス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については、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、ディスプレイデバイス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け取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。

【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行されてよい。一実施形態言において、実行可能なコンピュータプログラム命令で形成されるプログラムモジュールが、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 により実行される。

【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、グローバルセキュリティデータリポジトリ 335 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 335 と、グローバルセキュリティデータリポジトリ 335 と、へのアクセスを提供するサーバが含まれる。

【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、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）、ネットワーク露出情報、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。

【0029】

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 がオンラインであるのかオフラインであるのかを示す。「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）と併せて使用される。

【0030】

ネットワーク露出情報は、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、ネットワーク露出情報には、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。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 内の全てのノードが一意的な 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

10

20

30

40

50

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】

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、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。グローバルマネージャ120は、マネージドサーバ130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）、を判定することができる。例えば、グローバルマネージャ120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、グローバルマネージャ120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、グローバルマネージャ120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、グローバルマネージャ120は、NATのタイプが1：Nであると想定する。

【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ッスンしているのか、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、それらのプロセスのコマンドラインlaunch引数、および、それらのプロセスの依存関係（例えば、それらのプロセスがリンクする共有オブジェクト）、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、ネットワーク露出情報（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露出情報）、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。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、それらのルールを変更および／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について作成することができ、エンドユーザは、それらの示唆を受け入れること、または拒否することができる。

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つまたは複数のコンシューマとの間のリレーションシップを指定する。

【0039】

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、実行可能プロセスの制御、であってよい。アクセス制御機能でのルールは、コンシューマが、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、純粹な「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、コンシューマ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、コンシューマが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ければならないかどうか、を指定する。実行可能プロセスの制御機能でのルールは、プロセスが実行を許可されるかどうかを指定する。

10

【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、コンシューマ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、実行可能プロセスの制御、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獲得するためのトリガー、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。

20

【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）追加の適格性と、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、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ことができる。なお、ルール機能によっては、サービスは、いずれのネットワークリソースも使用しなくてもよい。例えば、実行可能プロセスの制御のルール機能のサービスでは、ネットワークプロトコルを使用したネットワークポート上での実行をしない。

30

40

【0043】

プロバイダ／コンシューマサービスの1つまたは複数のプロバイダ、および、サービスの1つまたは複数のコンシューマ（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

50

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「A l l（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（P B）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。P B部分が「A n y b o d y（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。P B部分が「A n y m a n a g e d s e r v e r（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。（「A n y m a n a g e d s e r v e r」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にマッチングする）。使用元（U B）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「コンシューマ」であるのか）を記述する。P B部分と同様に、U B部分は、「A n y b o d y」または「A n y m a n a g e d s e r v e r」を示すこともできる。

10

【0046】

P B部分およびU B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U I D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を指定する能力は、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（U D G）のU I Dを使用することにより指定される。ルールがU D G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露出情報）が含まれる。ルールのP B部分および／またはルールのU B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U I D、および／またはU D GのU I D、を含む複数の項目が含まれてよい。

20

【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（「C C」、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、ネットワーク露出情報（例えば、ネットワークインターフェースのB R N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である）、を含む、ブール式である。式のC C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、ネットワーク露出情報部分は、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。

30

40

【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

50

複数のスコープと、が含まれる。A「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、ウェブサービスティア（＜役割，Web＞ラベルのマネージドサーバ130）が、データベースティア（＜役割，データベース＞ラベルのマネージドサーバ）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（＜環境，プロダクション＞ラベルのマネージドサーバ）および自分のステージング環境（＜環境，ステージング＞ラベルのマネージドサーバ）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（PB部分とUB部分とに、＜環境，プロダクション＞ラベルが含まれる第1のスコープ、および、PB部分とUB部分とに、＜環境，ステージング＞ラベルが含まれる第2のスコープ）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は記述済みであり、これは、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、ユーザデバイスはコンシューマであり、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、ウェブサーバはコンシューマであり、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。

【0053】

ルールリスト#1

10

20

30

40

50

● 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

・ P B：<役割, ウェブ>

・ U B：Anybody

○ # 2

・ 機能：アクセス制御

・ サービス：PostgreSQL

・ P B：<役割, データベース>

・ U B：<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

・ P B：<役割, データベース>

・ U B：Any managed server

【0054】

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）追加の適格性、によって指定されるということを、思い出されたい。

【0055】

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、U B部分の「Anybody」によって指定される。「ウェブサーバ」が、P B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。

【0056】

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、U B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、P B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。

【0057】

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「

10

20

30

40

50

＜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。（本例のスコープは、PB部分とUB部分との間を区別しないため、それぞれのスコープのラベルセットが、PB部分およびUB部分の両方に適用される。）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。

【0058】

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。

10

【0059】

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＞

20

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＞

30

【0060】

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、お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）。

40

【0061】

図3に戻って、グローバルセキュリティデータリポジトリ335については、「追加的なセキュリティの態様」と題する章において以下で説明する。

【0062】

プロセッシングサーバ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。プロセッシングサーバ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、管理ドメイン状態更新モジュール385、および、グローバル

50

セキュリティモジュール 390、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、およびグローバルセキュリティモジュール 390、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。

【0063】

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 U I D）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 P B 部分および／またはルールの U B 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。

【0064】

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、P B 部分、および U B 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 P B 部分および／または U B 部分内に複数の項目（ラベルセット、マネージドサーバ U I D、および／または、U D G の U I D 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 P B 部分内に 1 項目のみ、およびその U B 部分に 1 項目のみ、しか含まない。また、ルールが、その P B 部分および／または U B 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 P B 部分および U B 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。

【0065】

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 P B 部分が、複数の項目を含む場合、ルールの U B 部分が、複数の項目を含む場合、または、ルール（P B 部分または U B 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を生成する（例えば、P B 項目、U B 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）。

【0066】

P B 部分に 2 つの項目（A および B）、ならびに、U B 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 P B

部分およびU B部分を用いて4つの機能レベルの命令を生成する1) P B = A、U B = C ; 2) P B = A、U B = D ; 3) P B = B、U B = C ; 4) P B = B、U B = D。ここで、P B部分またはU B部分でマネージドサーバをカバーするルール(例えば、U I D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を生成する(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)。

【0067】

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、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露出の詳細を考慮に入れる。

【0068】

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(P B)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。

【0069】

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(U D G)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U D G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U D G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(U I D)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、U B部分およびP B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U I D、U D GのU I D、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。

【0070】

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, . . . , 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、マネージドサーバ 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。

【0071】

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）「 $\langle X=A \rangle$ 、 $\langle Y=B \rangle$ 」、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、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「 $\langle X=A \rangle$ 、 $\langle Y=B \rangle$ 」を持つマネージドサーバが、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。

【0072】

さらに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、管理ドメイン規模のマネージメントポリシー 330 において（例えば、ルールおよびスコープのUB部分およびPB部分において）使用されるラベルセットのみをエニユメレートする。

【0073】

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、 $\langle$ 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。

【0074】

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。

【0075】

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、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、

アクターエニユメレーションモジュール370は、アクターセット（以前、アクターエニユ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。アクターエニユ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。

【0076】

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、アクターエニユ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、アクターエニユ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、アクターエニユ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。）

【0077】

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、アクターエニユ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。

【0078】

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、アクターエニユ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、アクターエニユ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、アクターエニユ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、アクターエニユ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、アクターエニユ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変更することにより、更新されたアクターセットを生成する。

【0079】

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

10

20

30

40

50

およびU B部分を分析して、特定のアクターセットが、ルールのP B部分またはU B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。

【0080】

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。

10

【0081】

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、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）。

【0082】

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、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、特定のマネージドサーバ130に送る。

20

30

【0083】

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）管理ドメインのアクターセットをキャッシュする。

40

【0084】

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

50

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に分散させることができる。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、変更を分散させることに、役立つ。

10

【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、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に分散させる。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、キャッシュしたアクターセット（以前、アクターエニュメレーションモジュールにより出力された）と、管理ドメイン状態320の変更された部分（例えば、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。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。

20

【0086】

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、そのサーバに送ったアクターセット、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、キャッシュし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、これは、キャッシュしたアクターセットと更新されたアクターセットとの間の差を記述するものである。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、アクターセットに追加、アクターセットから削除、または、アクターセット内で変更、されるべきかどうかの指標、を指定する。

30

【0087】

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（例えば、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

40

50

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。

【0088】

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、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U I D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、それ以上何のアクションも取らない。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。

【0089】

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、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、さらに効率を上げるために、機能レベルの命令が「d i f f」形式で送られ、これは、キャッシュされた機能レベルの命令と更新された機能レベルの命令との間の差を記述するものである。例えば、d i f f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、該機能レベルの命令から削除、されるべきかどうかの指標、を指定する。

【0090】

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、キャッシュし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（例えば、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。

【0091】

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

ル 3 4 0 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、または変更されるべきか、を判定する。ポリシーエンジンモジュール 3 4 0 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、または変更する。一実施形態において、効率を上げるために、アクターセットが「d i f f」形式で送られ、これは、キャッシュされた関連アクターセットと更新された関連アクターセットとの間の差を記述するものである。例えば、d i f f 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、以前送ったアクターセットに追加、該アクターセットから削除、またはアクターセットと比較して変更、されるべきかどうかの指標、を指定する。

【0092】

ポリシーエンジンモジュール 3 4 0 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 3 3 0 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 3 3 0 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、または変更、である。一実施形態において、マネージメントポリシー 3 3 0 に対する変更が、G U I または A P I を介したグローバルマネージャ 1 2 0 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 3 3 0 に対する変更が、グローバルマネージャ 1 2 0 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 3 4 0 は、マネージメントポリシー 3 3 0 に対する変更または管理ドメイン状態 3 2 0 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。

【0093】

マネージメントポリシー 3 3 0 に対する変更の場合、ポリシーエンジンモジュール 3 4 0 は、必ずしも全てのマネージドサーバ 1 3 0 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 3 4 0 は、以前のマネージメントポリシー 3 3 0 を、新しいマネージメントポリシー 3 3 0 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 3 3 0 と比較して、追加、削除、または変更されるべきか、を判定する。ポリシーエンジンモジュール 3 4 0 は、どのマネージドサーバ 1 3 0 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、P B 部分および／または U B 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 3 4 0 は、関連ルールモジュール 3 5 0 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 3 3 0 全体の代わりに）と、マネージドサーバ 1 3 0 の U I D（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。

【0094】

管理ドメイン状態更新（A D S U）モジュール 3 8 5 は、管理ドメイン状態 3 2 0 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 3 2 0 に対する変更は、例えば、マネージドサーバ 1 3 0 の記述の、追加、削除、もしくは変更（マネージドサーバのラベルセットまたは構成特徴の変更を含む）、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、もしくは変更、である。一実施形態において、管理ドメイン状態 3 2 0 に対する変更が、特定のマネージドサーバ 1 3 0 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 3 2 0 に対する変更が、G U I または A P I を介したグローバルマネージャ 1 2 0 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 3 2 0 に対する変更が、グローバルマネージャ 1 2 0 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）。

【0095】

例えば、A D S U モジュール 3 8 5 は、特定のアンマネージドサーバ 1 4 0 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、管理ドメイン状態320内に記憶する（例えば、その特定のアンマネージドデバイスがメンバーであるアンマネージドデバイスグループの一部として）。次に、A D S Uモジュール385は、アンマネージドデバイスグループの変更に基つき、管理ドメインのアクターセットを更新する。

詳細には、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。このイベントとは、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。

【0096】

別の例として、A D S U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。A D S Uモジュール385は、新しい情報を、その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、A D S U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、A D S U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。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ことを判定する場合、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、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を判定する場合、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、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、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。

【0097】

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を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、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。

【0098】

10

20

30

【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：はい マネージドサーバのマネージメント命令：はい
ネットワーク露出情報	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）

10

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

20

【0099】

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。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。

【0100】

グローバルセキュリティモジュール390については、「追加的なセキュリティの態様」と題する章において以下で説明する。

30

【0101】

図4は、一実施形態に係る、マネージドサーバ130のポリシー実行モジュール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。ポリシー実行モジュール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、ローカル状態更新モジュール420、およびローカルセキュリティモジュール430、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）、ネットワーク露出、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。ネットワーク露出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。

40

【0102】

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。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）マネージドサーバが電源が入るか

50

、オンラインになる、b) マネージドサーバがマネージメント命令を受け取る、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。

【0103】

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。

10

【0104】

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。

20

【0105】

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、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）。

30

40

【0106】

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 上でリッスンしている（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

50

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。

【0107】

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「プロセス情報」として言及した、要件のセットが与えられた）特定のプロセスのみに、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。

10

【0108】

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。

【0109】

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（ネットワーク情報）、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。

20

30

【0110】

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、それ以上何のアクションも取らない（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」形式で送り、これは、以前ローカル状態リポジトリ400に記憶された（かつ、従って、以前グローバルマネージャ120に送られた）ローカル状態情報と、直近に取得されたローカル状態情報と、の間の差を記述するものである。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。

40

50

【0111】

ローカルセキュリティモジュール430については、「追加的なセキュリティの態様」と題する章において以下で説明する。

【0112】

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）。

10

【0113】

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。

【0114】

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。

20

【0115】

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、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。

【0116】

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、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。

30

【0117】

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。

【0118】

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。

40

【0119】

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。

【0120】

50

なお、ステップ 5 2 0 および 5 4 0 は、特定のマネージドサーバ 1 3 0 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 5 3 0 および 5 5 0 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 5 2 0 で、ステップ 5 5 0 によって使用されるルール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、アクター観点的生成とは、最小限に相互に依存する。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 5 2 0 および 5 4 0）と、アクターセットの計算（すなわち、ステップ 5 3 0 および 5 5 0）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 3 4 0 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、同じマネージドサーバ 1 3 0 についてであっても）。加えて、異なるマネージドサーバ 1 3 0 についての観点的計算も、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。）

10

【0 1 2 1】

図 6 は、一実施形態に係る、マネージドサーバ 1 3 0 のマネージメントモジュール 1 3 2 の構成 1 3 4 を生成する方法 6 0 0 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 に示されるものの以外のエンティティによって実行されてよい。

20

【0 1 2 2】

方法 6 0 0 が開始されるとき、マネージドサーバ 1 3 0 のローカル状態に関する情報が、マネージドサーバ 1 3 0 のポリシー実行モジュール 1 3 6 のローカル状態リポジトリ 4 0 0 内に既に記憶されてある。この時点で、方法 6 0 0 が開始される。

【0 1 2 3】

ステップ 6 1 0 にて、マネージメント命令が、グローバルマネージャ 1 2 0 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 4 1 0 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 1 2 0 から受け取る。

【0 1 2 4】

ステップ 6 2 0 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 4 1 0 は、ローカル状態リポジトリ 4 0 0 内に記憶される、マネージドサーバ 1 3 0 のローカル状態に関する情報にアクセスする。

30

【0 1 2 5】

ステップ 6 3 0 にて、マネージメントモジュール構成 1 3 4 が生成される。例えば、ポリシーコンパイルモジュール 4 1 0 は、マネージメント命令（ステップ 6 1 0 にて受け取られた）と、ローカル状態（ステップ 6 2 0 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 1 3 4 を生成する。

【0 1 2 6】

ステップ 6 4 0 にて、マネージメントモジュール 1 3 2 が構成される。例えば、ポリシーコンパイルモジュール 4 1 0 は、マネージメントモジュール 1 3 2 を、マネージメントモジュール構成 1 3 4（ステップ 6 3 0 にて生成された）に従って動作するべく、構成する。

40

【0 1 2 7】

図 7 は、一実施形態に係る、マネージドサーバ 1 3 0 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 1 2 0 に送る、方法 7 0 0 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 に示されるものの以外のエンティティによって実行されてよい。

【0 1 2 8】

50

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。

【0129】

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。

【0130】

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。

【0131】

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。

【0132】

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。

【0133】

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。

【0134】

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 に対する変更を処理する、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。

【0135】

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、ネットワーク露出情報、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。

【0136】

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、情報が関連するマネージドサーバ 130 の記述内) に記憶する。

【0137】

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 は選択的なものである。

【0138】

10

20

30

40

50

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、A D S U 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。

【0139】

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、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、かつ、それに従って、影響を受けるマネージドサーバ 130 に通知する。一実施形態（図示せず）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。

10

【0140】

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、A D S U 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。マネージド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。

20

【0141】

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、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、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 に命令してマネージドサーバのマネージメント命令を更新させる。

【0142】

ステップ 880 にて、方法が終了する。

追加的なセキュリティの態様

【0143】

マネージドサーバ 130 のポリシー実行モジュール 136 には、ローカルセキュリティモジュール 430 が含まれることを思い出されたい。ローカルセキュリティモジュール 430 は、マネージドサーバ 130 からセキュリティ関連情報（「セキュリティメタデータ」）を収集し、収集した情報をグローバルマネージャ 120 に送る。ローカルセキュリティモジュール 430 は、マネージドサーバ 130 が、管理ドメイン 150 において、分散された検出ノードまたはプローブのように作動することを可能にする。一実施形態において、ローカルセキュリティモジュール 430 は、以下のセキュリティ関連情報のうちのいずれかまたは全てを収集して送る。

30

【0144】

a) 不正プロセスおよび／または不正アクションの識別—ローカルセキュリティモジュール 430 が、マネージドサーバ 130 上で実行されている「不正プロセス」を検出する。不正プロセスとは、不適切なアクション（「不正アクション」）、例えば、マネージメントモジュール構成 134 により実行されるマネージメントポリシーに反するアクション、を行う（または試みる）プロセスである。例えば、マネージメントポリシーに、許容可能なネットワーク接続を指定するアクセス制御ルールが含まれる場合、リッスンされないデバイスへの接続を試みる（例えば、ネットワーク接続を開始する）ことは、不正アクションであろう。詳細には、プロバイダがデータベースサーバであり、かつコンシューマがウェブサーバである場合に接続が許可される、ということをアクセス制御ルールが提示する場合、ウェブサーバがプロバイダとして作動する状態で、データベースサーバがコンシューマとして作動することを試みることは、不正アクションであろう。一実施形態におい

40

50

て、ローカルセキュリティモジュール430は、許可されたアクションについてのマネージメントポリシーを記述する命令にアクセスする。そのポリシーに不適合なものはいずれも、不正アクションとなる。

【0145】

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ッスンしているのか、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、それらのプロセスのコマンドライン `launch` 引数、および、それらのプロセスの依存関係、が含まれる。不正アクションは、いずれのタイプのプロセス情報にも関与することが可能である。例えば、「不当」なネットワークポートまたはネットワークインターフェース（例えば、マネージメントポリシーにより許可されるものとして指定されない、ネットワークポートまたはネットワークインターフェース）をリッスンすることは、不正アクションであり得る。別の例として、「不当」なユーザ（単数または複数）（例えば、マネージメントポリシーにより許可されるものとして指定されないユーザ）のコンテキストで実行することは、不正アクションであり得る。さらに別の例として、通常のものではない、または無許可の共有オブジェクトをロードすることは、不正アクションであり得る。

10

【0146】

一実施形態において、ローカルセキュリティモジュール430が不正プロセス／アクションを検出すると、ローカルセキュリティモジュールは、不正アクション（例えば、不正プロセスにより行われる）に関する情報、不正プロセスそのものに関する情報（例えば、プロセス情報）、および／または、不正プロセスにより行われる追加のアクション、例えば、要求されたDNS（`domain name system`（ドメイン名システム））ルックアップや、試みられたおよび／または行われたネットワーク接続など、をグローバルマネージャ120に送る。不正アクションに関する情報には、例えば、不正アクションのタイプ（例えば、不当ネットワークポートもしくはインターフェース上でのリッスン、または、不当ユーザのコンテキストでの実行）、そのタイプに基づく不正アクションの詳細（例えば、リッスンが行われる不当ネットワークポートもしくはインターフェース、または、プロセスが実行されたコンテキストの不当ユーザ）、および／または、不正アクションがいつ発生したのかを示すタイムスタンプ、が含まれる。DNSルックアップに関する情報には、例えば、ルックアップのためにDNSに送られた情報が含まれる。ネットワーク接続に関する情報には、例えば、送信先デバイスのIPアドレスおよび／またはポート番号が含まれる。不正プロセス／アクション情報は、「不良」なマネージドサーバ130の識別に使用することができ、マネージドサーバが、マネージメントモジュール構成134により実行されるマネージメントポリシーに反するアクション、を行う（または試みる）場合は、そのマネージドサーバは「不良」である。

20

30

【0147】

図9は、一実施形態に係る、不正プロセスを検出して報告する方法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。

40

【0148】

方法900が開始されるとき、マネージドサーバ130内のマネージメントモジュール132は、マネージメントモジュール構成134に従って、すでに構成済みである。マネージドサーバ130が、グローバルマネージャ120から受け取った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132を構成した。構成された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を実行する。この時点で、方法900が開始される。

【0149】

ステップ910にて、アクションの実行を求める要求が、マネージドサーバ130上で

50

実行されるプロセスから受け取られる。例えば、ローカルセキュリティモジュール 430 がその要求を受け取る。

【0150】

ステップ 920 にて、マネージドサーバ 130 内の構成されたマネージメントモジュール 132 に従って、アクションが不適切であるという判定がなされる。例えば、ローカルセキュリティモジュール 430 が、マネージメントモジュール 132 に要求を送り、マネージメントモジュール 132 が要求を分析して、要求が、管理ドメイン規模のマネージメントポリシー 330 を順守しているかどうかを判定する。ローカルセキュリティモジュール 430 は、要求が管理ドメイン規模のマネージメントポリシー 330 を順守していないことを示す応答を、マネージメントモジュール 132 から受け取る。受け取った応答に基づき、ローカルセキュリティモジュール 430 が、アクションは不適切であることを判定する。

10

【0151】

ステップ 930 にて、不適切なアクションに関する、または、プロセスに関する情報が、グローバルマネージャに送られる。例えば、ローカルセキュリティモジュール 430 が、不適切なアクションに関する情報（例えば、不適切なアクションのタイプ、不適切なアクションのタイプに基づく不適切なアクションの詳細、不適切なアクションがいつ発生したのかを示すタイムスタンプ）、または、アクションの実行を要求したプロセスに関する情報（例えば、プロセスの名称、プロセスがリッスンを行っているネットワークポート、プロセスがリッスンを行っているネットワークインターフェース、プロセスを起動したユーザ、プロセスの構成、プロセスのコマンドライン `launch` 引数、またはプロセスの依存関係）、をグローバルマネージャに送る。

20

【0152】

b) オペレーティングシステムレベルのタンパリングの識別—ローカルセキュリティモジュール 430 が、オペレーティングシステムレベルのタンパリング（例えば、マネージメントモジュール構成 134 に対する変更）を検出する。

【0153】

c) ログ—ローカルセキュリティモジュール 430 が、マネージドサーバ 130 からログを取得し、そのログをグローバルマネージャ 120 に送る。ログには、例えば、ファイアウォールのログ（例えば、ウェブアプリケーションファイアウォール（WAF）エンジンにより報告されるウェブベースの L7 ルールおよびシグネチャベースの攻撃）、侵入検知システム（IDS）ログ（例えば、IDS エンジンからの従来の L7 シグネチャベースの侵入検知イベント）、および、認証ログ（例えば、セキュアシェル（SSH）認証ログ）、が含まれる。一実施形態において、これらのログは、より簡単に分析されるように、標準の形式に正規化される。正規化は、マネージドサーバ 130 および／またはグローバルマネージャ 120 にて行うことができる。

30

【0154】

d) 検出された侵入の識別—ローカルセキュリティモジュール 430 が、種々の技術を使用して侵入を検出する。例えば、ローカルセキュリティモジュール 430 は、いくつかの基本侵入シグネチャを、`iptables` と併せて使用する。別の例として、ローカルセキュリティモジュール 430 が、IP アドレスに関連付けられたいくつかのアクティビティをトラッキングし、トラッキングしたアクティビティの量をいくつかの閾値と比較する（例えば、SSH 総当たり攻撃を検出する）。

40

【0155】

e) 「不良アクター」の識別—ローカルセキュリティモジュール 430 が、既知の「不良アクター」（例えば、低レピュテーションおよび／またはセキュリティ脅威に関連付けられた IP アドレスを持つデバイス）を、マネージドサーバ 130 によりブロックされる IP アドレスと比較する。不良アクターが典型的にはアンマネージドデバイス 140 であるのに対し、不良アクターはマネージドサーバ 130 であることがある。一実施形態において、不良アクターの識別は、ログストリームの形式でグローバルマネージャ 120 に提

50

供される。

【0156】

一実施形態において、ローカルセキュリティモジュール430はまた、自身のセキュリティ機能を実行する。例えば、ローカルセキュリティモジュール430は、マネージドサーバ130上のプロセスが、いつ新しいアウトバウンド接続を作成するのかを検出する。ローカルセキュリティモジュール430は、既知の不良アクター（アンマネージドデバイス140および／またはマネージドサーバ130）のリストにアクセスし、アウトバウンド接続の送信先デバイスがリスト上にあるかどうかを判定する。送信先デバイスがリスト上にある場合、ローカルセキュリティモジュール430は、侵入を防ぐためにアウトバウンド接続をブロックする。別の実施形態において、ローカルセキュリティモジュール430が、ローカル攻撃の閾値および発見的問題解決法を使用して、ブロッキングポリシーをローカルに適用する。

10

【0157】

グローバルマネージャ120のリポジトリ300には、グローバルセキュリティデータリポジトリ335が含まれることを思い出されたい。グローバルセキュリティデータリポジトリ335は、セキュリティ関連情報（「セキュリティメタデータ」）を記憶する。この情報には、例えば、不正プロセスおよび／または不正アクション、オペレーティングシステムレベルのタンパリング、ログ、検出された侵入、および不良アクター、が含まれる。

【0158】

グローバルマネージャ120のプロセッシングサーバ310には、グローバルセキュリティモジュール390が含まれることを思い出されたい。グローバルセキュリティモジュール390が、セキュリティ関連情報（「セキュリティメタデータ」）をマネージドサーバ130から受け取り、その情報をグローバルセキュリティデータリポジトリ335に記憶する。この情報には、例えば、不正プロセスおよび／または不正アクション、オペレーティングシステムレベルのタンパリング、ログ、検出された侵入、および不良アクター、が含まれる。

20

【0159】

グローバルセキュリティモジュール390はまた、グローバルセキュリティデータリポジトリ335に記憶される情報を分析し、必要に応じて、その分析の結果に基づき、管理ドメイン状態320および／または管理ドメイン規模のマネジメントポリシー330を変更する。グローバルセキュリティデータリポジトリ335に記憶される情報の分析により、攻撃および／または脆弱性が検出される。グローバルセキュリティモジュール390は、単一のマネージドサーバ130上、のみならず、管理ドメイン150全体に渡って、攻撃または脆弱性を検出することができる。

30

【0160】

管理ドメイン状態320および／またはマネジメントポリシー330の変更は、グローバルに実施される。管理ドメイン状態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、ことを思い出されたい。一実施形態において、管理ドメイン状態320が、マネージドサーバ130のポリシー違反に関する情報を記憶する。例えば、グローバルセキュリティモジュール390は、特定のマネージドサーバ130について、グローバルセキュリティデータリポジトリ335に記憶される不正プロセス／アクション情報を分析する。そして、グローバルセキュリティモジュール390は、そのマネージドサーバの、ポリシー違反固有に構成された特徴を、特定の値、例えば、行われたまたは試みられた違反の数（1、2、3など）に設定する。別の実施形態において、管理ドメイン状態320が、マネージドサーバ130をタンパリングすることに関する情報を記憶する。例えば、グローバルセキュリティモジュール390は、特定のマネージドサーバ130について、グローバルセキュリティデータリポジトリ335に記憶されるオペレーティングシステムレベルのタンパリング情報を分析する。そして、グローバルセキュリティモジュール390は、そのマネージドサーバの、タ

40

50

ンパリング固有に構成された特徴を、特定の値、例えば、タンパリングの有無を示すブール値、に設定する。

【0161】

別の実施形態において、管理ドメイン状態320が、1つまたは複数のアンマネージドデバイスグループ(UDG)に関する情報を記憶する。第1のUDGのメンバーは、既知の攻撃または不良アクター(例えば、セキュリティ脅威をもたらすアンマネージドデバイス140)である。グローバルセキュリティモジュール390は、必要に応じて、攻撃者/不良アクターを追加または削除することにより、この不良アクターUDGを維持する。例えば、グローバルセキュリティモジュール390は、グローバルセキュリティデータリポジトリ335に記憶されるログ情報、検出された侵入情報、および/または不良アクター情報を使用して、「不良」アンマネージドデバイス140を識別する。グローバルセキュリティモジュール390が、特定の攻撃者または不良アクターを識別すると、グローバルセキュリティモジュールは、そのアクターを不良アクターUDGに追加する。一実施形態において、不良アクターUDGを使用して、以下で説明するように、(マネージドサーバ130との間の)ネットワーク接続がブロックされるべきアンマネージドデバイス140を識別する。別の実施形態において、不良アクターUDGが、管理ドメイン規模のマネージメントポリシー330(例えば、ルールの提供元または使用元部分内)において使用される。

10

【0162】

他のUDGのメンバーは、「危険」であり、かつ、関連付けられた「リスクスコア」を持つ、ということが分かっている。例えば、第1の危険UDGのメンバーが、リスクスコア「1」を持ち、第2の危険UDGが、リスクスコア「2」を持つ、などである。グローバルセキュリティモジュール390は、必要に応じて、アンマネージドデバイス140を追加または削除することにより、危険UDGを維持する。例えば、グローバルセキュリティモジュール390は、グローバルセキュリティデータリポジトリ335に記憶されるログ情報、検出された侵入情報、および/または不良アクター情報を使用して、危険なアンマネージドデバイス140およびそのデバイスの危険スコアを識別する。グローバルセキュリティモジュール390が、特定の危険アンマネージドデバイス140を識別すると、グローバルセキュリティモジュールは、そのアンマネージドデバイスを、適切な危険UDGに(アンマネージドデバイスのリスクスコアに基づき)追加する。一実施形態において、危険UDGを使用して、以下で説明するように、ローカルセキュリティモジュール430の動作を、微調整、調整、改良、または改善する。別の実施形態において、危険UDGが、管理ドメイン規模のマネージメントポリシー330(例えば、ルールの提供元または使用元部分内)において使用される。

20

30

【0163】

管理ドメイン状態更新モジュール385は、上記で説明したように、管理ドメイン状態320に対する変更を受け取り、それに従って、それらの変更を処理する。これにより、1つのマネージドサーバ130への攻撃の検出が、動的な実施ポリシーとして、他のマネージドサーバに分散されることが可能となるため、該他のマネージドサーバが保護される。換言すると、フィードバックループが存在し、そこでは、マネージドサーバ130がセ

40

【0164】

特に、更新された関連アクターセット(例えば、変更されたUDGまたは変更されたマネージドサーバに関連付けられたアクターセット)は、種々のマネージドサーバ130に送られてもよい。一実施形態において、更新された関連アクターセットを受け取ることに起因して、それらのマネージドサーバが、自身のマネージメントモジュール132を再構成する。例えば、再構成されたマネージメントモジュール132は、第1のUDGのメンバーであるアンマネージドデバイス140への、および/またはアンマネージドデバイス

50

140からの、通信を許可することを中止してもよい（それによって、これら通信の全てをブロックする）。別の実施形態において、更新された関連アクターセットを受け取ることに起因して、それらマネージドサーバ内のローカルセキュリティモジュール430は、異なって動作する。例えば、ローカルセキュリティモジュール430は、モジュール430の分析を変更または調整して、データが、アンマネージドデバイス140のリスクスコアに基づき、異なって分析されるようにすることができる。特定のアンマネージドデバイス140に関するセキュリティ情報を報告するための閾値は、デバイスのリスクスコアが高い場合に、低くてもよい。別の例として、ローカルセキュリティモジュール430は、更新された不良アクターUDGに基づき、異なるアウトバウンド接続をブロックしてもよい。

10

【0165】

なお、攻撃を分散させることができるため、任意の1つのマネージドサーバ130は、自身が攻撃下にはないということを知らないかもしれない。マネージドサーバ130が、セキュリティ関連情報を、グローバルマネージャ120に送るので、グローバルセキュリティモジュール390は、ドメインのうちのいずれの1つの部分における、1つのプローブにも分離してとらえることができない、管理ドメイン150に渡る攻撃パターンを検出することができる。ドメイン規模の攻撃が、グローバルセキュリティモジュール390により検出されると、グローバルセキュリティモジュールは、上記で説明したものと同一機構（すなわち、管理ドメイン状態320の変更）の後に続き、動的な実施ポリシーを他のマネージドサーバ130に分散して、該他のマネージドサーバが保護されるようにする。

20

【0166】

グローバルセキュリティモジュール390は、アプリケーションベースの異常およびネットワークベースの異常の両方へのアクセスを有するので、グローバルセキュリティデータリポジトリ335に記憶される情報のモジュール390の分析は、さらに正確である。グローバルセキュリティモジュール390はまた、より早く作動することができ、実施のアクション（例えば、管理ドメイン状態320の変更）を取る前に、長い時間待つ必要が無い。また、グローバルセキュリティモジュール390は、特定の管理ドメイン150に一意的な攻撃を識別することができる。その攻撃は、そのドメインのみを標的にしていることができ、攻撃は、他のインターネットスケールのセキュリティシステム上の「ノイズの中」にある。また、管理ドメイン150におけるマネージドサーバ130（詳細には、そのポリシー実行モジュール136）の配置のため、グローバルセキュリティモジュール390はまた、内部関係者からの、ドメイン内からの内部の脅威、または、代替えとして、ドメインの境界防御を通り抜け、今度はドメイン内に横に移動しようとするボットネット、をキャッシュすることができる。

30

【0167】

一実施形態において、グローバルセキュリティモジュール390はまた、1つまたは複数の以下の機能を実行する。

【0168】

a) グローバルセキュリティデータリポジトリ335に記憶される情報の統計的分析—グローバルセキュリティモジュール390が、グローバルセキュリティデータリポジトリ335に記憶される情報を分析して、異なるカテゴリ内の上位の「N」個の項目を判定する。カテゴリは、例えば、通信している上位の個々のノード、通信している上位の対のノード、マネージドサーバ130によりブロックされる上位のIPアドレス、および、マネージドサーバにより高いリスクスコアで許可される上位のIPアドレス、とすることができる。統計値は、複数のレベルで、例えば、マネージドサーバごと、データセンターごと、事業単位ごと、および、管理ドメイン150ごと、に計算されてよい。

40

【0169】

b) 「不良アクター」の識別—グローバルセキュリティモジュール390が、アクティビティの構成された閾値を使用して、不良アクターを識別する。

【0170】

50

一実施形態において、グローバルセキュリティモジュール390は拡張可能であり、および／または、セキュリティ分析機能を実行して、異なる脅威および攻撃のタイプに基づき、グローバルな警告と動的な実施の両方を提供することができる。

【0171】

ここで、グローバルセキュリティモジュール390は記述済みであり、これは、いくつかの例に対処することに役立つ。環境100（特に、グローバルマネージャ120およびマネージドサーバ130）は、マネージドサーバが、「隔離モード」におかれることを可能にする。隔離モードは、特定のマネージドサーバ130を他のマネージドサーバから分離する。例えば、感染したまたは不良な挙動をするマネージドサーバ130が、他の「健全」なマネージドサーバから分離される。

10

【0172】

マネージドサーバ130が隔離中のときは、他のマネージドサーバ（詳細には、そのマネージメントモジュール132）が、隔離されたサーバから生じたインバウンドのネットワークトラフィックをブロックする。加えて、隔離されたサーバにインストールされたマネージメントモジュール132が、自身を構成可能なセルフ隔離モードにし、それにおいては、（デフォルトで）アウトバウンドのネットワークトラフィックがブロックされ、管理のインバウンドのネットワークトラフィックのみが許可される。隔離されたサーバがルーティングされており、かつ、攻撃者が十分に高性能である場合、セルフ隔離モードは回避され得る。しかし、それほど洗練されていないウィルスの多くの場合（および、感染したシステムが、まだ悪意のあるペイロードを有しておらず、単に偵察を行っているだけ場合）、セルフ隔離モードは、追加の予防策の提供を助ける。非常に進歩した脅威の場合でさえも、他のマネージドサーバ130が、隔離されたサーバからの分離を提供する。

20

【0173】

一実施形態において、隔離モードが、以下のように実行される。まず、グローバルセキュリティモジュール390が、特定のマネージドサーバ130を隔離することを判定する。例えば、グローバルセキュリティモジュール390は、ネットワーク攻撃が特定のマネージドサーバ130から生じた、または、特定のマネージドサーバ130が脆弱性を有することを判定する。この判定は、例えば、グローバルマネージャ120が行ったアクション（例えば、グローバルセキュリティデータリポジトリ335に記憶される情報の分析）および／またはグローバルマネージャが外部ソースから受け取る通知（例えば、マネージドサーバ130、サードパーティの脆弱性スキャナ、またはユーザコマンド）に基づくものとすることができる。マネージドサーバ130からの通知は、例えば、不正プロセス／アクションまたはオペレーティングシステムレベルのタンバリング、に關与するものとすることができる。脆弱性スキャナから受け取る通知は、例えば、脆弱性を有するデバイスに關与するものとすることができる。ユーザコマンドから受け取る通知は、例えば、任意の可能性のある手段を使用して人により識別された不良アクターに關与するものとすることができる。

30

【0174】

そして、グローバルセキュリティモジュール390は、管理ドメイン状態320を変更して、特定のマネージドサーバ130が隔離されることを示す。例えば、グローバルセキュリティモジュール390は、特定のマネージドサーバ130を、特別の隔離アクターセット（本明細書では、アクターセットQまたは「ASQ」と称する）に追加する。管理ドメイン状態320は、アクターセットQに関する情報を記憶し、アクターセットQのメンバーは隔離される。グローバルセキュリティモジュール390は、必要に応じてマネージドサーバ130を追加または削除することにより、アクターセットQを維持する。

40

【0175】

別の例において、グローバルセキュリティモジュール390は、隔離固有に構成された特徴（本明細書では、「CC_Q」と称する）を、特定の値、例えば、脅威レベル（1、2、3、など）、に設定する。CC_Qを使用して、アクターセットQを条件付きで定義することができ、ここで、アクターセットQの各メンバーは、ゼロより大きいCC_Q値を持つ

50

(「 $CC_Q > 0$ 」)。 CC_Q を使用して、複数の隔離アクターセットを条件付きで定義することもでき（例えば、各脅威レベルに1つの隔離アクターセット、ここで、そのアクターセットの各メンバーは、同じ CC_Q 値を持つ）。 CC_Q を、ルールの条件部分（ブール式）と併せて使用して、ルールが特定のマネージドサーバ130に適用されるかどうかを指定することもできる。例えば、条件部分「 $CC_Q = 0$ 」では、全ての隔離されたサーバが、その脅威レベルに関わらず除外される。この条件部分を、ホワイトリストモデルルールと共に使用して、隔離されたサーバがプロバイダまたはコンシューマとして作動することを防ぐことができる。

【0176】

隔離アクターセットは、条件付きで定義されようと、明示的に割り当てられたメンバーにより定義されようと、管理ドメイン規模のマネジメントポリシー330において、使用元（UB）部分または提供元（PB）部分内で、使用されてよいものとする。詳細には、隔離アクターセットを、セット差計算の一部として使用することができる（例えば、共通セット（集合）のメンバーの減算）。例えば、UB部分「 $* < \text{隔離アクターセット} >$ 」は、隔離アクターセットのメンバーを除く誰（どれ）でも、サービスを使用することができる、ことを指定するもので、ここで、ワイルドカード記号「 $*$ 」は、誰でも、を示し、減算記号「 $-$ 」は、「除く」を示し、「 $< \text{隔離アクターセット} >$ 」は、任意のタイプの隔離アクターセットを示す（この隔離アクターセットのメンバーは、例えば、全ての隔離したマネージドサーバ、または、特定の CC_Q 値（例えば、 $CC_Q > 2$ または $CC_Q < 5$ ）を持つマネージドサーバのみ、とすることができる）。隔離アクターセットを使用して、プロバイダまたはコンシューマを、積極的に示すこともできる。例えば、PB部分「 $< \text{隔離アクターセット} >$ 」は、隔離アクターセットのメンバーがサービス、例えば、管理セキュリティ対応チームの一部であるデバイスからの接続を許可すること、を提供する、ことを指定する。

【0177】

なお、ルールの条件部分において CC_Q を使用することは、ルールのUB部分またはPB部分においてセット差計算に隔離アクターセットを使用すること、と論理的に等価である。例えば、第1位のルール $< UB = \text{ウェブ}, PB = \text{データベース}, \text{条件} = 「CC_Q = 0」 >$ は、第2のルール $< UB = \text{ウェブ} - ASQ, PB = \text{データベース} - ASQ >$ 、ここで、 CC_Q は、ASQを条件付き（ $CC_Q > 0$ ）で定義する）、と論理的に等価である。

【0178】

管理ドメイン状態更新モジュール385は、上記で説明したように、管理ドメイン状態320に対するこの変更を受け取り、それに従って、この変更を処理する。特に、更新されたマネジメント命令（例えば、関連アクターセットおよび／または機能レベル命令）が、マネージドサーバ130に送られる。更新されたマネジメント命令を受け取ることに起因して、それらマネージドサーバ（詳細には、そのポリシーコンパイルモジュール410）は、新しいマネジメントモジュール構成134を生成し、それに従って、そのマネジメントモジュール132を再構成する。新しいマネジメントモジュール構成134は、更新されたマネジメント命令に基づき生成される。

【0179】

隔離したマネージドサーバ130については、受け取った更新されたマネジメント命令に起因して、該サーバは、セルフ隔離モードに入る。例えば、機能レベル命令がホワイトリスト型モデルに従う場合（例えば、サーバが行うことができることの完全なリストを提供する）、更新された機能レベル命令は、以前受け取られた機能レベル命令のサブセット（部分集合）であってもよい。その結果、隔離したマネージドサーバ130は、隔離されていなかったときには行ったような多くのタスクを、行うことが許可されない。

【0180】

隔離されないマネージドサーバ130については、受け取った更新されたマネジメント命令（詳細には、任意の隔離アクターセットおよび／または隔離機能レベル命令）に起因して、該サーバは、隔離されたサーバを分離する。（なお、隔離機能レベル命令は、以

10

20

30

40

50

前送られており変更がない場合には、グローバルマネージャ 1 2 0 からマネージドサーバ 1 3 0 に再度送られる必要はない。) 特に、ポリシーコンパイルモジュール 4 1 0 は、隔離機能レベル命令を、隔離アクターセットのメンバーに適用し、標準の機能レベル命令を、それらメンバーに適用しない。マネージメントモジュール 1 3 2 の再構成に起因して、該マネージメントモジュールは、隔離アクターセットのメンバー (すなわち、隔離したマネージドサーバ 1 3 0) からのインバウンドのトラフィックをブロックする。

【0 1 8 1】

ある時点で、隔離したマネージドサーバ 1 3 0 の「隔離を解除する」 (すなわち、サーバを隔離モードから解放する) ことが適切であることがある。例えば、隔離したマネージドサーバ 1 3 0 が安全になった場合 (例えば、悪意のあるソフトウェアまたは脆弱性を取り除くことにより)、そのサーバの隔離を解除することは適切であることがある。マネージドサーバ 1 3 0 は、一旦隔離を解除されると、それ以上他のマネージドサーバからは分離されず、セルフ隔離モードから解放される。

10

【0 1 8 2】

一実施形態において、隔離したマネージドサーバ 1 3 0 の隔離モードからの解放は、以下のように実行される。まず、グローバルセキュリティモジュール 3 9 0 が、特定のマネージドサーバ 1 3 0 を隔離から解放することを判定する。例えば、グローバルセキュリティモジュール 3 9 0 は、マネージドサーバ 1 3 0 がこれ以上セキュリティ脅威をもたらすことはないことを判定するこの判定は、例えば、グローバルマネージャ 1 2 0 が行ったアクション (例えば、グローバルセキュリティデータリポジトリ 3 3 5 に記憶される情報の分析) および/またはグローバルマネージャが外部ソースから受け取る通知 (例えば、サードパーティの脆弱性スキャナ、またはユーザコマンド) に基づくものとすることができる。

20

【0 1 8 3】

脆弱性スキャナから受け取る通知は、例えば、脆弱性を有するデバイスに關与するものとすることができる。一実施形態において、脆弱性の通知には、以前脆弱性を有していたが、もう有していないデバイス、がリストアップされている。別の実施形態において、脆弱性の通知には、現在脆弱性を有するデバイスがリストアップされている。その実施形態において、グローバルセキュリティモジュール 3 9 0 が、最近の脆弱性の通知を、古い脆弱性の通知と比較して、以前脆弱性を有していたがもう有していないデバイス、を判定することができる。ユーザコマンドから受け取る通知は、例えば、セキュリティ脅威をこれ以上もたらすことはない、と人により識別されたマネージドサーバ 1 3 0 に關与するものとすることができる。

30

【0 1 8 4】

そして、グローバルセキュリティモジュール 3 9 0 は、管理ドメイン状態 3 2 0 を変更して、特定のマネージドサーバ 1 3 0 が隔離から解放されることを示す。例えば、グローバルセキュリティモジュール 3 9 0 は、特定のマネージドサーバ 1 3 0 を、特別の隔離アクターセットから削除する。別の例において、グローバルセキュリティモジュール 3 9 0 は、隔離固有に構成された特徴を、特定の値、例えば、脅威レベル (例えば、脅威無しとして 0)、に設定する。

40

【0 1 8 5】

管理ドメイン状態更新モジュール 3 8 5 は、上記で説明したように、管理ドメイン状態 3 2 0 に対するこの変更を受け取り、それに従って、この変更を処理する。特に、更新されたマネージメント命令 (例えば、関連アクターセットおよび/または機能レベル命令) が、マネージドサーバ 1 3 0 に送られる。更新されたマネージメント命令を受け取ることに起因して、それらマネージドサーバ (詳細には、そのポリシーコンパイルモジュール 4 1 0) は、新しいマネージメントモジュール構成 1 3 4 を生成し、それに従って、そのマネージメントモジュール 1 3 2 を再構成する。新しいマネージメントモジュール構成 1 3 4 は、更新されたマネージメント命令に基づき生成される。

【0 1 8 6】

50

隔離から解放されたマネージドサーバ130については、受け取った更新されたマネージメント命令に起因して、該サーバは、セルフ隔離モードから出る。例えば、機能レベル命令がホワイトリスト型モデルに従う場合（例えば、サーバが行うことができることの完全なリストを提供する）、更新された機能レベル命令は、以前受け取られた機能レベル命令の上位セット（上位集合）であってもよい。その結果、隔離を解除されたマネージドサーバ130は、隔離されていたときに行ったよりも多くのタスクを、行うことが許可される。

【0187】

異なるマネージドサーバ130については、受け取った更新されたマネージメント命令（詳細には、任意の隔離アクターセットおよび／または隔離機能レベル命令）に起因して、該サーバは、新しく隔離を解除されたサーバの分離を中止する。特に、ポリシーコンパイルモジュール410は、隔離機能レベル命令を、隔離アクターセットのメンバー（新しく隔離を解除されたサーバはもはや含まれない）に適用し、標準の機能レベル命令を、それらメンバーに適用しない。マネージメントモジュール132の再構成に起因して、該マネージメントモジュールは、隔離アクターセットのメンバーからのインバウンドのトラフィックをブロックする。

【0188】

図10は、一実施形態に係る、管理ドメイン内のマネージドサーバ130を隔離する方法1000を説明するフローチャートである。管理ドメインに150には、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132を構成する複数のマネージドサーバ130が含まれ、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行するようにされ、隔離したマネージドサーバが、複数のマネージドサーバのうちの他のマネージドサーバから、分離されるようにする。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。

【0189】

方法1000が開始されるとき、マネージドサーバ130（隔離されるであろうマネージドサーバ）の記述は、グローバルマネージャ120の管理ドメイン状態320に既に記憶されてある。また、管理ドメインのアクターセットも、グローバルマネージャ120に既にキャッシュ済みである。最後に、マネージメントポリシー観点および関連アクターセットが、別のマネージドサーバ130（隔離したマネージドサーバとは異なる）に関連して、既にキャッシュ済みである。この時点で、方法1000が開始される。

【0190】

ステップ1010にて、マネージドサーバ130の記述が変更されて、マネージドサーバが隔離されることが示される。例えば、グローバルセキュリティモジュール390が、マネージドサーバ130の隔離固有に構成された特徴を、特定の値に設定することにより、管理ドメイン状態320を変更し、それによって、隔離したマネージドサーバの記述を指定する。

【0191】

ステップ1020にて、キャッシュしたアクターセットが更新されて、隔離したマネージドサーバの変更後状態が示される。例えば、グローバルセキュリティモジュール390が、アクターエニユメレーションモジュール370を使用して、管理ドメインのキャッシュしたアクターセットを更新し、それによって、更新されたアクターセットを指定する。

【0192】

ステップ1030にて、更新されたアクターセットのどれが他のマネージドサーバ130に関連するのか、に関して判定が行われる。例えば、グローバルセキュリティモジュール390が、関連アクターモジュール380を使用して、更新されたアクターセットのどれが他のマネージドサーバ130に関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定する。

10

20

30

40

50

【0193】

ステップ1040にて、現在関連する更新後アクターセットが、他のマネージドサーバ130に以前送ったアクターセットと異なるかどうか、に関して判定が行われる。例えば、グローバルセキュリティモジュール390が、現在関連する更新後アクターセットを、他のマネージドサーバ130に以前送ったアクターセット（他のマネージドサーバに関連して、「関連アクターセット」としてキャッシュしたアクターセット）と比較する。現在関連する更新後アクターセットが、以前送ったアクターセットと異なる（例えば、同一である）という判定に応じて、方法1000はステップ1050に進む。現在関連する更新後アクターセットが、以前送ったアクターセットと異なる、という判定に応じて、方法1000はステップ1060に進む。

10

【0194】

ステップ1050にて、それ以上アクションは取らない。例えば、グローバルセキュリティモジュール390は、それ以上アクションを取らない。

【0195】

ステップ1060にて、以前送ったアクターセットと比較して、追加、削除または変更されるべきである、更新されたアクターセットが、判定される。例えば、グローバルセキュリティモジュール390が、現在関連する更新後アクターセットを、他のマネージドサーバ130に以前送ったアクターセットと比較する。

【0196】

ステップ1070にて、更新されたアクターセットと、更新されたアクターセットを追加、削除、または変更するための命令と、が他のマネージドサーバに送られる。例えば、グローバルセキュリティモジュール390が、更新されたアクターセットと、命令とを、他のマネージドサーバに送る。

20

【0197】

図11は、一実施形態に係る、管理ドメイン150内のアンマネージドデバイス140のグループの状態に対する変更を処理する方法1100を説明するフローチャートである。管理ドメイン150には、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132を構成する複数のマネージドサーバ130が含まれ、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行するようにされる。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に示されるものの以外のエンティティによって実行されてよい。

30

【0198】

方法1100が開始されるとき、アンマネージドデバイスグループ（状態が変更されるアンマネージドデバイスグループ）の記述は、グローバルマネージャ120の管理ドメイン状態320に既に記憶されてある。また、管理ドメインのアクターセットも、グローバルマネージャ120に既にキャッシュ済みである。最後に、マネージメントポリシー観点および関連アクターセットが、マネージドサーバ130に関連して、既にキャッシュ済みである。この時点で、方法1100が開始される。

40

【0199】

ステップ1110にて、アンマネージドデバイスグループの記述が変更されて、アンマネージドデバイスがアンマネージドデバイスグループに追加される。例えば、グローバルセキュリティモジュール390が、アンマネージドデバイスをアンマネージドデバイスグループに追加することにより、管理ドメイン状態320を変更する。

【0200】

ステップ1120にて、キャッシュしたアクターセットが更新されて、アンマネージドデバイスグループの変更後状態が示される。例えば、グローバルセキュリティモジュール390が、アクターエニユメレーションモジュール370を使用して、管理ドメインのキャッシュしたアクターセットを更新し、それによって、更新されたアクターセットを指定

50

する。

【0201】

ステップ1130にて、更新されたアクターセットのどれがマネージドサーバ130に関連するのか、に関して判定が行われる。例えば、グローバルセキュリティモジュール390が、関連アクターモジュール380を使用して、更新されたアクターセットのどれがマネージドサーバ130に関連するのかを判定し、それによって、現在関連する更新後アクターセットを指定する。

【0202】

ステップ1140にて、現在関連する更新後アクターセットが、マネージドサーバ130に以前送ったアクターセットと異なるかどうか、に関して判定が行われる。例えば、グローバルセキュリティモジュール390が、現在関連する更新後アクターセットを、マネージドサーバ130に以前送ったアクターセット（マネージドサーバに関連して、「関連アクターセット」としてキャッシュしたアクターセット）と比較する。現在関連する更新後アクターセットが、以前送ったアクターセットと異なる（例えば、同一である）という判定に応じて、方法1100はステップ1150に進む。現在関連する更新後アクターセットが、以前送ったアクターセットと異なる、という判定に応じて、方法1100はステップ1160に進む。

【0203】

ステップ1150にて、それ以上アクションは取らない。例えば、グローバルセキュリティモジュール390は、それ以上アクションを取らない。

【0204】

ステップ1160にて、以前送ったアクターセットと比較して、追加、削除または変更されるべきである、更新されたアクターセットが、判定される。例えば、グローバルセキュリティモジュール390が、現在関連する更新後アクターセットを、マネージドサーバ130に以前送ったアクターセットと比較する。

【0205】

ステップ1170にて、更新されたアクターセットと、更新されたアクターセットを追加、削除、または変更するための命令と、がマネージドサーバに送られる。例えば、グローバルセキュリティモジュール390が、更新されたアクターセットと、命令とを、マネージドサーバに送る。

【0206】

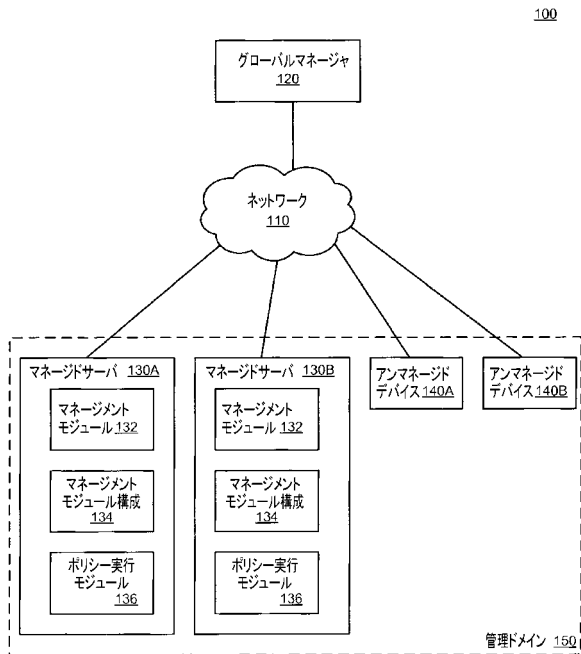
上記の説明は、特定の実施形態の動作を説明するために含まれ、本発明の範囲を制限することは意図されない。本発明の範囲は、以下の請求項によってのみ、制限されるべきである。上記の検討から、当業者には、本発明の精神および範囲によってさらに網羅されるであろう多くの変形が明らかとなるであろう。

10

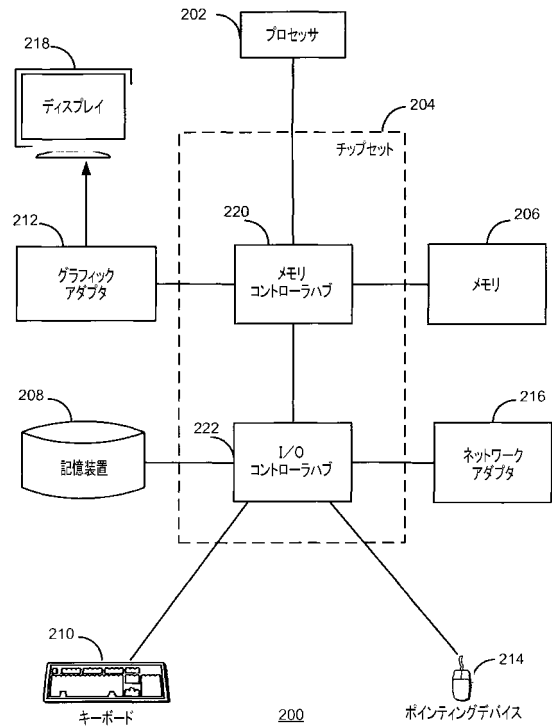
20

30

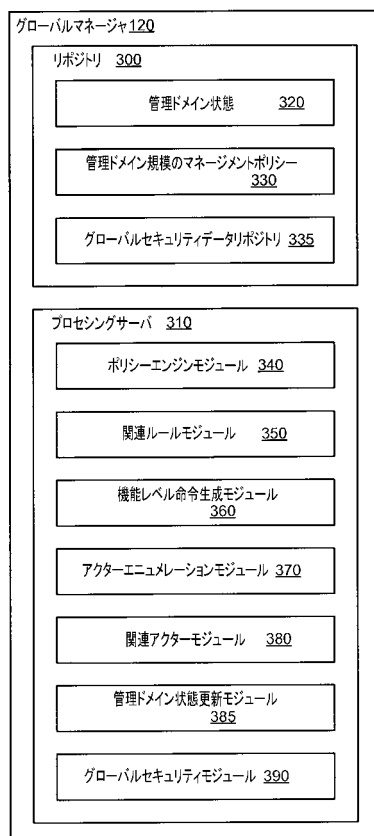
【図 1】



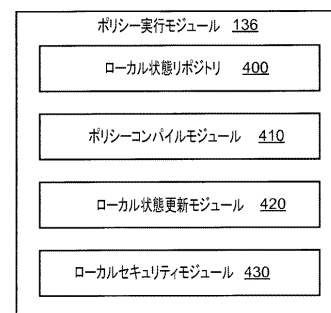
【図 2】



【図 3】

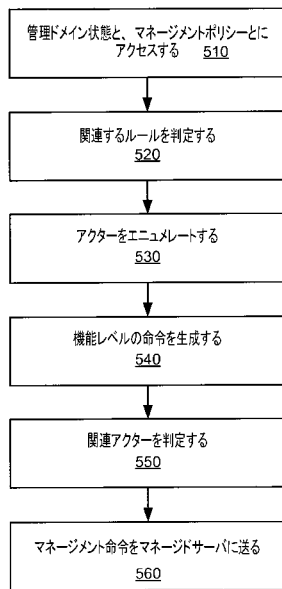


【図 4】



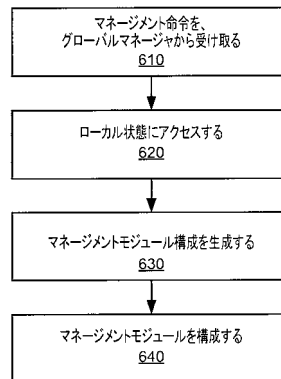
【図 5】

500



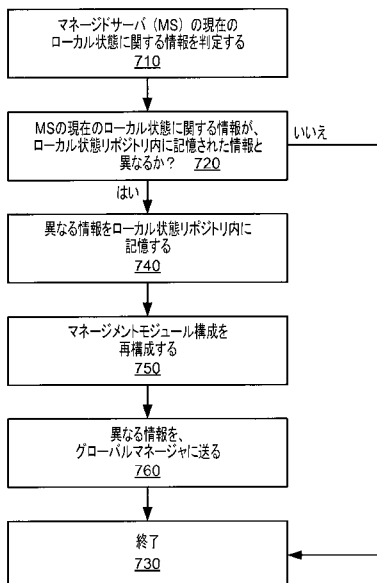
【図 6】

600



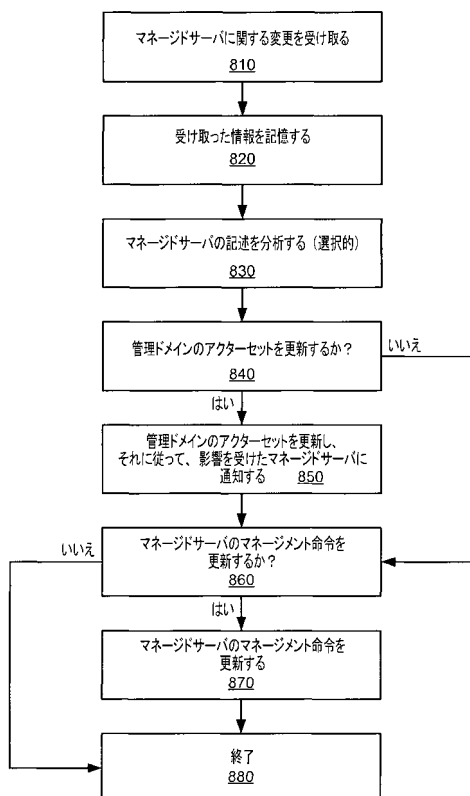
【図 7】

700



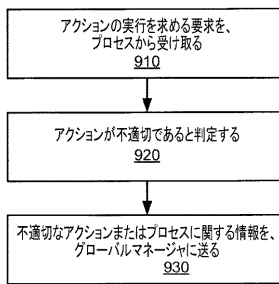
【図 8】

800



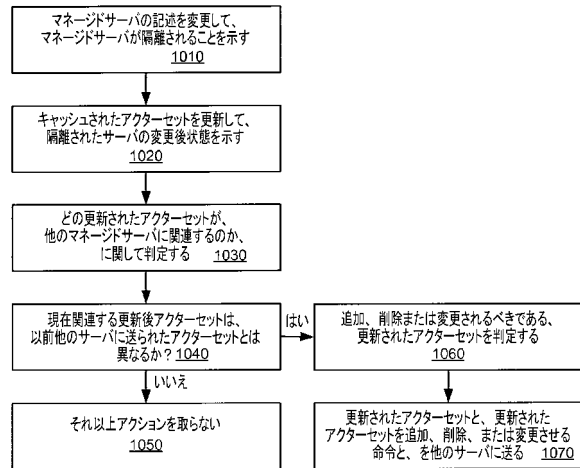
【図 9】

900



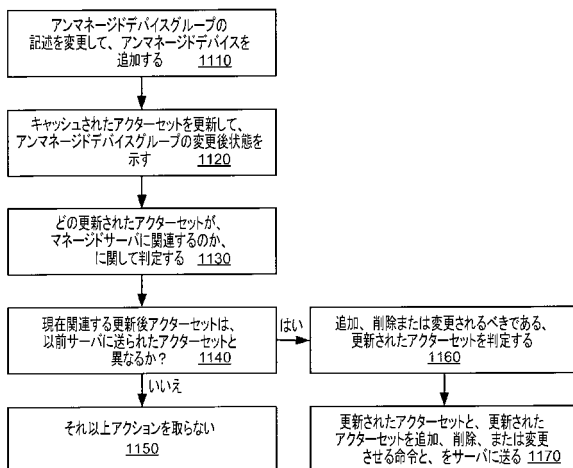
【図 10】

1000



【図 11】

1100



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 14/54505

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 17/00 (2015.01); H04L 29/06 (2015.01)

CPC - H04L63/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
CPC: H04L63/20; IPC(8): G06F 17/00 (2015.01); H04L 29/06 (2015.01); USPC: 726/1Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC: H04L63/20, H04L63/102, G06F21/6218, G06F21/604, H04L63/0227; USPC: 726/1, 709/223, 709/224, 709/225 (keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PatBase, Google Scholar

Search Terms: rogue, anomaly, virus, worm, trojan, hack, malware, spam, detect, monitor, track, report, manage, admin, policy, rule, global, domain-wide, server, central

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/0078309 A1 (BLOCH et al.) 31 March 2011 (31.03.2011), entire document, especially abstract and para [0053], [0058], [0062], [0064]-[0066], [0068]-[0071], [0074], [0085], [0090]-[0095], [0147], [0150], [0153], [0159]-[0160], [0177], [0184]-[0188], [0210], [0242], [0328], [0344], [0350]-[0351], [0353], [0402], Fig. 2, Fig. 4A.	1-10
A	US 2011/0296005 A1 (LABOVITZ et al.) 01 December 2011 (01.12.2011), entire document.	1-10
A	US 2012/0210425 A1 (PORRAS et al.) 16 August 2012 (16.08.2012), entire document.	1-10

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

01 June 2015 (01.06.2015)

Date of mailing of the international search report

26 JUN 2015

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-8300

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 14/54505

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1.

Group I: Claims 1-10, directed to detecting and reporting of rogue processes in a managed domain utilizing managed servers and instructions received from a global manager.

Group II: Claims 11-22 and 28-29, directed to quarantining a managed server within an administrative domain utilizing cached actor-sets to indicate changes in a server's state.

Group III: Claims 23-27, directed to processing a change to a state of a group of unmanaged devices within an administrative domain utilizing an administrative domain-wide management policy to categorize such unmanaged devices as security threats.
-- Continued on extra sheet --

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-10

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 14/54505

Continuation of Box No. III, Observations where unity of invention is lacking:

The groups of inventions listed above do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical feature of the Group I invention is detecting and reporting of rogue processes in a managed domain utilizing managed servers and instructions received from a global manager, not required by Group II or III. (See Fig. 9 for example).

The special technical feature of the Group II invention is quarantining a managed server within an administrative domain utilizing cached actor-sets to indicate changes in a server's state, not required by Group I or III. (See Fig. 10 for example).

The special technical feature of the Group III invention is processing a change to a state of a group of unmanaged devices within an administrative domain utilizing an administrative domain-wide management policy to categorize such unmanaged devices as security threats, not required by Group I or II. (See Fig. 11 for example).

Groups I-III share the technical features of, in various combination, managed servers that use management instructions to implement an administrative domain-wide policy.

However, these shared technical features fail to represent a contribution over the prior art of US 2012/0131164 A1 to Bryan et al. (hereinafter 'Bryan'), which discloses managed servers (para [0056], [0060] - "a scope 'domain=D1' specifies the management domain named D1, which includes the servers, applications, and other entities that are members of domain D1") that use management instructions to implement an administrative domain-wide policy (para [0048]-[0053] - "the policy manager 106, in response to instructions from the policy manager user interface 134 or other interface, creates, modifies, and deletes policies"; "a global policy attachment 160 that attaches a security policy 112 to all Web service endpoints in a domain").

Thus, the inventions listed as Groups I-III lack unity of invention because they do not share a same or corresponding special technical feature providing a contribution over the prior art.

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(特許庁注：以下のものは登録商標)

1. ウィンドウズ
2. L i n u x
3. M y S Q L

- (72)発明者 ダニエル アール. クック
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 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, 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 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, 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 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, 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 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, 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 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, 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 イルミオ, インコーポレイテッド内
- (72)発明者 スカラン ブイ. ヴァルギース
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 イルミオ, インコーポレイテッド内

Fターム(参考) 5K030 HD09 KA05 LB07 MD07