(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6276417号
(P6276417)
(45)発行日　平成30年2月7日(2018.2.7)　(24)登録日　平成30年1月19日(2018.1.19)

(51)Int.Cl.　F I
H04L 12/24 (2006.01)　H04L 12/24

請求項の数 23　(全 51 頁)

(21)出願番号	特願2016-552245 (P2016-552245)
(86)(22)出願日	平成26年10月30日 (2014.10.30)
(65)公表番号	特表2016-540463 (P2016-540463A)
(43)公表日	平成28年12月22日 (2016.12.22)
(86)国際出願番号	PCT/US2014/063239
(87)国際公開番号	WO2015/066369
(87)国際公開日	平成27年5月7日 (2015.5.7)
審査請求日	平成29年9月4日 (2017.9.4)
(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	62/066,835
(32)優先日	平成26年10月21日 (2014.10.21)
(33)優先権主張国	米国(US)

早期審査対象出願

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

最終頁に続く

(54)【発明の名称】ラベルベースのアクセス制御ルールの自動生成

(57)【特許請求の範囲】

【請求項１】

管理ドメイン内で複数の管理対象サーバ間の通信を許可するアクセス制御ルールを判定する方法であって、

前記複数の管理対象サーバ間の過去の通信を記述した通信情報を取得するステップと、

前記取得された通信情報に基づいて、前記複数の管理対象サーバをグループ化することによって、前記複数の管理対象サーバから管理対象サーバのサブセットを各々が含むサーバグループを識別するステップと、

各サーバグループにおける前記管理対象サーバのサブセットにグループレベルラベルセットを割り当てるステップであって、前記グループレベルラベルセットは、前記サーバグループにおける前記管理対象サーバを記述した１つまたは複数のグループレベルラベルを含む、ステップと、

各サーバグループ内の個々の管理対象サーバにロールラベルを割り当てるステップであって、個々の管理対象サーバに割り当てられるロールラベルは、前記個々の管理対象サーバに関する情報に基づいて判定される、ステップと、

前記通信情報において、第１の管理対象サーバと第２の管理対象サーバとの間の通信を識別するステップであって、前記第１の管理対象サーバは、第１のグループレベルラベルおよびロールラベルのペアを割り当てられ、前記第２の管理対象サーバは、第２のグループレベルラベルおよびロールラベルのペアを割り当てられる、ステップと、

前記第１の管理対象サーバと前記第２の管理対象サーバとの間の通信を許可するアクセ

ス制御ルールを生成するステップであって、前記生成されたアクセス制御ルールは、前記第１のグループレベルラベルおよびロールラベルのペアを割り当てられた他の管理対象サーバと前記第２のグループレベルラベルおよびロールラベルのペアを割り当てられた他の管理対象サーバとの間の通信をさらに許可する、ステップと、

管理ドメイン全体管理ポリシの一部として前記アクセス制御ルールを記憶するステップと

を備えたことを特徴とする方法。

【請求項２】

前記第１の管理対象サーバと前記第２の管理対象サーバとの間の前記通信を識別するステップは、前記第１の管理対象サーバによって提供され、および前記第２の管理対象サーバによって使用されるサービスを識別するステップを含み、

前記アクセス制御ルールを生成するステップは、前記サービスを指定する前記アクセス制御ルールを生成するステップを含み、前記アクセス制御ルールは、前記第１のグループレベルラベルおよびロールラベルのペアを指定する提供側部分、ならびに前記第２のグループレベルラベルおよびロールラベルのペアを指定する使用側部分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】

前記識別された通信は、前記第１の管理対象サーバと前記第２の管理対象サーバとの間の過去の許可されていない通信であり、前記管理ドメイン全体管理ポリシは、前記許可されていない通信を記述するアクセス制御ルールを有してなく、前記アクセス制御ルールを生成するステップは、

前記許可されていない通信を記述した情報、前記第１の管理対象サーバの前記第１のグループレベルラベルおよびロールラベルのペア、ならびに前記第２の管理対象サーバの前記第２のグループレベルラベルおよびロールラベルのペアに基づいて、前記許可されていない通信が許可可能であるべきと判定するステップと、

前に許可されていない通信を許可する前記アクセス制御ルールを生成するステップと

含むことを特徴とする請求項１に記載の方法。

【請求項４】

第１の管理対象サーバと前記管理ドメインの外部のデバイスとの間の別の通信を識別するステップと、

前記第１の管理対象サーバと前記外部デバイスとの間の通信を許可する第２のアクセス制御ルールを生成するステップであって、前記第２のアクセス制御ルールは、前記外部デバイスと前記第１のグループレベルラベルおよびロールラベルのペアを有する他のデバイスとの間の通信をさらに許可するステップと

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】

前記取得された通信情報は、前記複数の管理対象サーバの間で前に転送されたデータの特性を記述し、前記特性は、前記前に転送されたデータのタイミング、期間、頻度、プロトコルタイプ、データサイズ、またはデータ速度のうちの１つまたは複数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】

前記取得された通信情報は、前記管理対象サーバのサブセットによって実行される処理を記述し、前記ロールラベルを割り当てるステップは、

前記管理対象サーバによって実行される１つまたは複数の処理に基づいて管理対象サーバに対するロールラベルを判定するステップを含む

ことを特徴とする請求項１に記載の方法。

【請求項７】

前記取得された通信情報は、前記管理対象サーバのサブセットのハードウェアリソースを記述し、

前記ロールラベルを割り当てるステップは、

前記管理対象サーバのハードウェアリソースに基づいて、管理対象サーバに対するロールラベルを判定するステップを含む
ことを特徴とする請求項１に記載の方法。
【請求項８】
前記割り当てられたグループレベルラベルセットおよび前記割り当てられたロールラベルのうちの少なくとも１つを管理者が確認することを要求するステップと、
前記管理者からの訂正に応じて前記グループレベルラベルセットおよび前記ロールラベルのうちの少なくとも１つを修正するステップと
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９】
前記サーバグループを識別するステップは、
前記複数の管理対象サーバのうちの管理対象サーバを表すノード、および前記管理対象サーバ間の通信を表す前記ノード間のエッジを有するグラフを構築するステップと、
前記グラフを前記識別されたサーバグループに対応するサブグラフに区分化するステップと
を含むことを特徴とする請求項１に記載の方法。
【請求項１０】
前記グループにおける前記管理対象サーバのサブセットに前記グループレベルラベルセットを割り当てるステップは、
前記サーバグループにおける管理対象サーバを記述した複数の次元を有する前記グループレベルラベルを割り当てるステップであって、前記複数の次元は、前記サーバグループにおける前記管理対象サーバの論理アプリケーションを記述したアプリケーションの次元、または前記サーバグループにおける前記管理対象サーバのライフサイクルステージを記述した環境の次元のうちの少なくとも１つを含む、ステップと、
前記管理対象サーバに条件付きヒューリスティックを適用して、前記アプリケーションの次元または前記環境の次元のうちの少なくとも１つに対する値を判定するステップと
を含み、
前記グループレベルラベルセットは、前記アプリケーションの次元または前記環境の次元のうちの少なくとも１つに対する前記判定された値に応じて、前記グループにおける前記管理対象サーバのサブセットに割り当てられる
ことを特徴とする請求項１に記載の方法。
【請求項１１】
前記取得された通信情報は、前記複数の管理対象サーバ間の前に転送されたデータのルーティング情報を記述することを特徴とする請求項１に記載の方法。
【請求項１２】
管理ドメイン内で複数の管理対象サーバ間の通信を許可するアクセス制御ルールを判定するためのステップを実行するよう１つまたは複数のプロセッサによって実行可能なコンピュータプログラムモジュールを記憶した非一時的コンピュータ可読記憶媒体であって、前記ステップは、
前記複数の管理対象サーバ間の過去の通信を記述した通信情報を取得するステップと、
前記取得された通信情報に基づいて、前記複数の管理対象サーバをグループ化することによって、前記複数の管理対象サーバから管理対象サーバのサブセットを各々が含むサーバグループ識別するステップと、
各サーバグループにおける前記管理対象サーバのサブセットにグループレベルラベルセットを割り当てるステップであって、前記グループレベルラベルセットは、前記サーバグループにおける前記管理対象サーバを記述した１つまたは複数のグループレベルラベルを含む、ステップと、
各サーバグループ内の個々の管理対象サーバにロールラベルを割り当てるステップであって、個々の管理対象サーバに割り当てられるロールラベルは、前記個々の管理対象サーバに関する情報に基づいて判定される、ステップと、

前記通信情報において、第１の管理対象サーバと第２の管理対象サーバとの間の通信を識別するステップであって、前記第１の管理対象サーバは、第１のグループレベルラベルおよびロールラベルのペアを割り当てられ、前記第２の管理対象サーバは、第２のグループレベルラベルおよびロールラベルのペアを割り当てられる、ステップと、

前記第１の管理対象サーバと前記第２の管理対象サーバとの間の通信を許可するアクセス制御ルールを生成するステップであって、前記生成されたアクセス制御ルールは、前記第１のグループレベルラベルおよびロールラベルのペアを割り当てられた他の管理対象サーバと前記第２のグループレベルラベルおよびロールラベルのペアを割り当てられた他の管理対象サーバとの間の通信をさらに許可する、ステップと、

管理ドメイン全体管理ポリシの一部として前記アクセス制御ルールを記憶するステップと

を備えた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１３】

前記第１の管理対象サーバと前記第２の管理対象サーバとの間の前記通信を識別するステップは、前記第１の管理対象サーバによって提供され、および前記第２の管理対象サーバによって使用されるサービスを識別するステップを含み、

前記アクセス制御ルールを生成するステップは、前記サービスを指定する前記アクセス制御ルールを生成するステップを含み、前記アクセス制御ルールは、前記第１のグループレベルラベルおよびロールラベルのペアを指定する提供側部分、ならびに前記第２のグループレベルラベルおよびロールラベルのペアを指定する使用側部分を含むことを特徴とする請求項１２に記載のコンピュータ可読記憶媒体。

【請求項１４】

前記識別された通信は、前記第１の管理対象サーバと前記第２の管理対象サーバとの間の過去の許可されていない通信であり、前記管理ドメイン全体管理ポリシは、前記許可されていない通信を記述するアクセス制御ルールを有してなく、前記アクセス制御ルールを生成するステップは、

前記許可されていない通信を記述した情報、前記第１の管理対象サーバの前記第１のグループレベルラベルおよびロールラベルのペア、ならびに前記第２の管理対象サーバの前記第２のグループレベルラベルおよびロールラベルのペアに基づいて、前記許可されていない通信が許可可能であるべきと判定するステップと、

前に許可されていない通信を許可する前記アクセス制御ルールを生成するステップと

含むことを特徴とする請求項１２に記載のコンピュータ可読記憶媒体。

【請求項１５】

前記ステップは、

第１の管理対象サーバと前記管理ドメインの外部のデバイスとの間の別の通信を識別するステップと、

前記第１の管理対象サーバと前記外部デバイスとの間の通信を許可する第２のアクセス制御ルールを生成するステップであって、前記第２のアクセス制御ルールは、前記外部デバイスと前記第１のグループレベルラベルおよびロールラベルのペアを有する他のデバイスとの間の通信をさらに許可するステップと

さらに備えたことを特徴とする請求項１２に記載のコンピュータ可読記憶媒体。

【請求項１６】

前記取得された通信情報は、前記管理対象サーバのサブセットによって実行される処理を記述し、前記ロールラベルを割り当てるステップは、

前記管理対象サーバによって実行される１つまたは複数の処理に基づいて管理対象サーバに対するロールラベルを判定するステップを含む

ことを特徴とする請求項１２に記載のコンピュータ可読記憶媒体。

【請求項１７】

前記取得された通信情報は、前記管理対象サーバのサブセットのハードウェアリソースを記述し、

前記ロールラベルを割り当てるステップは、
前記管理対象サーバのハードウェアリソースに基づいて、管理対象サーバに対するロールラベルを判定するステップを含む
ことを特徴とする請求項１２に記載のコンピュータ可読記憶媒体。
【請求項１８】
前記グループにおける前記管理対象サーバのサブセットに前記グループレベルラベルセットを割り当てるステップは、
前記サーバグループにおける管理対象サーバを記述した複数の次元を有する前記グループレベルラベルを割り当てるステップであって、前記複数の次元は、前記サーバグループにおける前記管理対象サーバの論理アプリケーションを記述したアプリケーションの次元、または前記サーバグループにおける前記管理対象サーバのライフサイクルステージを記述した環境の次元のうちの少なくとも１つを含む、ステップと、
前記管理対象サーバに条件付きヒューリスティックを適用して、前記アプリケーションの次元または前記環境の次元のうちの少なくとも１つに対する値を判定するステップと
を含み、
前記グループレベルラベルセットは、前記アプリケーションの次元または前記環境の次元のうちの少なくとも１つに対する前記判定された値に応じて、前記グループにおける前記管理対象サーバのサブセットに割り当てられる
ことを特徴とする請求項１に記載の方法。
【請求項１９】
管理ドメイン内で複数の管理対象サーバ間の通信を許可するアクセス制御ルールを判定する方法であって、
前記複数の管理対象サーバ間の過去の通信を記述した通信情報を取得するステップと、
前記取得された通信情報に基づいて、前記複数の管理対象サーバをグループ化することによって、前記複数の管理対象サーバから管理対象サーバのサブセットを各々が含むサーバグループを識別するステップと、
各サーバグループにおける前記管理対象サーバのサブセットにグループレベルラベルセットを割り当てるステップであって、前記グループレベルラベルセットは、前記サーバグループにおける前記管理対象サーバを記述した複数の次元を有し、前記複数の次元は、前記サーバグループにおける前記管理対象サーバの論理アプリケーションを記述したアプリケーションの次元を含み、前記アプリケーションは、前記サーバグループにおける前記管理対象サーバに条件付きヒューリスティックを適用することによって判定される、ステップと、
各サーバグループ内の個々の管理対象サーバにロールラベルを割り当てるステップであって、個々の管理対象サーバに割り当てられるロールラベルは、前記個々の管理対象サーバに関する情報に基づいて判定される、ステップと、
前記通信情報、グループレベルラベルセット、およびロールラベルに基づいて、前記複数の管理対象サーバ間の通信を許可するアクセス制御ルールを生成するステップと、
管理ドメイン全体管理ポリシの一部として前記アクセス制御ルールを記憶するステップと
を備えたことを特徴とする方法。
【請求項２０】
前記アクセス制御ルールを生成するステップは、
前記通信情報から、第１の管理対象サーバによって提供され、および第２の管理対象サーバによって使用されるサービスを識別するステップと、
アクセス制御ルールを生成するステップであって、前記アクセス制御ルールは、前記第１の管理対象サーバに割り当てられる１つまたは複数のラベルを指定する提供側部分を含み、前記アクセス制御ルールはさらに、前記第２の管理対象サーバに割り当てられる１つまたは複数のラベルを指定する使用側部分を含むことを特徴とする請求項１９に記載の方法。

【請求項２１】
管理ドメイン内で複数の管理対象サーバ間の通信を許可するアクセス制御ルールを判定するためのステップを実行するよう１つまたは複数のプロセッサによって実行可能なコンピュータプログラムモジュールを記憶した非一時的コンピュータ可読記憶媒体であって、前記ステップは、
前記複数の管理対象サーバ間の過去の通信を記述した通信情報を取得するステップと、
前記取得された通信情報に基づいて、前記複数の管理対象サーバをグループ化することによって、前記複数の管理対象サーバから管理対象サーバのサブセットを各々が含むサーバグループを識別するステップと、
各サーバグループにおける前記管理対象サーバのサブセットにグループレベルラベルセットを割り当てるステップであって、前記グループレベルラベルセットは、前記サーバグループにおける前記管理対象サーバを記述した複数の次元を有し、前記複数の次元は、前記サーバグループにおける前記管理対象サーバの論理アプリケーションを記述したアプリケーションの次元を含み、前記アプリケーションは、前記サーバグループにおける前記管理対象サーバに条件付きヒューリスティックを適用することによって判定される、ステップと、
各サーバグループ内の個々の管理対象サーバにロールラベルを割り当てるステップであって、個々の管理対象サーバに割り当てられるロールラベルは、前記個々の管理対象サーバに関する情報に基づいて判定される、ステップと、
前記通信情報、グループレベルラベルセット、およびロールラベルに基づいて、前記複数の管理対象サーバ間の通信を許可するアクセス制御ルールを生成するステップと、
管理ドメイン全体管理ポリシの一部として前記アクセス制御ルールを記憶するステップと
を備えた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２２】
前記アクセス制御ルールを生成するステップは、
前記通信情報から、第１の管理対象サーバによって提供され、および第２の管理対象サーバによって使用されるサービスを識別するステップと、
アクセス制御ルールを生成するステップであって、前記アクセス制御ルールは、前記第１の管理対象サーバに割り当てられる１つまたは複数のラベルを指定する提供側部分を含み、前記アクセス制御ルールはさらに、前記第２の管理対象サーバに割り当てられる１つまたは複数のラベルを指定する使用側部分を含むことを特徴とする請求項２１に記載のコンピュータ可読記憶媒体。
【請求項２３】
管理ドメイン内で複数の管理対象サーバ間の通信を許可するアクセス制御ルールを判定するためのシステムであって、
プロセッサと、
非一時的コンピュータ可読記憶媒体と
を備え、前記非一時的コンピュータ可読記憶媒体は、
前記複数の管理対象サーバ間の過去の通信を記述した通信情報を取得するステップと、
前記取得された通信情報に基づいて、前記複数の管理対象サーバをグループ化することによって、前記複数の管理対象サーバから管理対象サーバのサブセットを各々が含むサーバグループを識別するステップと、
各サーバグループにおける前記管理対象サーバの前記サブセットにグループレベルラベルセットを割り当てるステップであって、前記グループレベルラベルセットは、前記サーバグループにおける前記管理対象サーバを記述した１つまたは複数のグループレベルラベルセットを含む、ステップと、
各サーバグループ内の個々の管理対象サーバにロールラベルを割り当てるステップであって、個々の管理対象サーバに割り当てられるロールラベルは、前記個々の管理対象サーバに関する情報に基づいて判定される、ステップと、

前記通信情報、グループレベルラベルセット、およびロールラベルに基づいて、前記複数の管理対象サーバ間の通信を許可するアクセス制御ルールを生成するステップと、

管理ドメイン全体管理ポリシの一部として前記アクセス制御ルールを記憶するステップと

を備えたステップを実行するように前記プロセッサによって実行可能なコンピュータプログラム命令を記憶し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】

本明細書において説明される主題は、一般に、管理ドメインのサーバ（物理または仮想）を管理する分野に関し、特に、論理多次元ラベルベースのポリシモデルに準拠する管理ドメイン全域にわたるポリシに従ってサーバを管理することに関する。

【背景技術】

【０００２】

管理ドメインのサーバ（物理または仮想）は、ポリシに従って管理される。たとえば、セキュリティポリシは、アクセス制御および／またはセキュア接続性を指定してよいが、リソース使用ポリシは、管理ドメインのコンピューティングリソース（たとえば、ディスクおよび／または周辺機器）の使用を指定してよい。従来のポリシは、物理デバイスを参照し、インターネットプロトコル（ＩＰ）アドレス、ＩＰアドレス範囲、サブネットワーク、およびネットワークインタフェースのような、低レベルの構成概念（construct）に関して表現される。これらの低レベルの構成概念は、抽象的かつ自然な方法で細分化された（fine-grained）ポリシを記述することを困難にしている。

【発明の概要】

【０００３】

上記およびその他の課題は、管理ドメイン内の複数の管理対象サーバの間の通信を許可するアクセス制御ルールを判定するための方法、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。方法の実施形態は、複数の管理対象サーバの間の過去の通信を記述する通信情報を取得するステップを備える。方法は、取得された通信情報に基づいて複数の管理対象サーバをグループ化することによって、複数の管理対象サーバから管理対象サーバのサブセットを識別するステップをさらに備える。方法は、管理対象サーバのサブセットに関連付けるようにグループレベルラベルセットを判定するステップをさらに備える。方法は、管理対象サーバのサブセット内の管理対象サーバに対するロールラベルを判定するステップであって、管理対象サーバは１つのロールラベルに関連付けられる、ステップをさらに備える。方法は、グループレベルラベルセットおよびロールラベルに基づいて、管理対象サーバのサブセットの第１の管理対象サーバと第２の管理対象サーバとの間の通信を許可するアクセス制御ルールを生成するステップをさらに備える。方法は、アクセス制御ルールを、管理ドメイン全体管理ポリシの一部として記憶するステップをさらに備える。

【０００４】

媒体の実施形態は、ステップを実行するために１または複数のプロセッサによって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。ステップは、複数の管理対象サーバの間の過去の通信を記述する通信情報を取得するステップを備える。ステップは、取得された通信情報に基づいて複数の管理対象サーバをグループ化することによって、複数の管理対象サーバから管理対象サーバのサブセットを識別するステップをさらに備える。ステップは、管理対象サーバのサブセットに関連付けるようにグループレベルラベルセットを判定するステップをさらに備える。ステップは、管理対象サーバのサブセット内の管理対象サーバに対するロールラベルを判定するステップであって、管理対象サーバは１つのロールラベルに関連付けられるステップをさらに備える。ステップは、グループレベルラベルセットおよびロールラベルに基づいて、管理対象サーバのサブセットの第１の管理対象サーバと第２の管理対象サーバとの間の通信を許可するアクセス制御ルールを生成する

ステップをさらに備える。ステップは、アクセス制御ルールを、管理ドメイン全体管理ポリシの一部として記憶するステップをさらに備える。

【０００５】

システムの実施形態は、１または複数のプロセッサと、ステップを実行するために１または複数のプロセッサによって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とを備える。ステップは、複数の管理対象サーバの間の過去の通信を記述する通信情報を取得するステップを備える。ステップは、取得された通信情報に基づいて複数の管理対象サーバをグループ化することによって、複数の管理対象サーバから管理対象サーバのサブセットを識別するステップをさらに備える。ステップは、管理対象サーバのサブセットに関連付けるようにグループレベルラベルセットを判定するステップをさらに備える。ステップは、管理対象サーバのサブセット内の管理対象サーバにロールラベルを判定するステップであって、管理対象サーバは１つのロールラベルに関連付けられるステップをさらに備える。ステップは、グループレベルラベルセットおよびロールラベルに基づいて、管理対象サーバのサブセットの第１の管理対象サーバと第２の管理対象サーバとの間の通信を許可するアクセス制御ルールを生成するステップをさらに備える。ステップは、アクセス制御ルールを、管理ドメイン全体管理ポリシの一部として記憶するステップをさらに備える。

【０００６】

上記およびその他の課題は、１または複数のアクセス制御ルールを実施する管理対象サーバからのアラート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。方法の実施形態は、第２の管理対象サーバとの過去の通信に応じてアラートを生成するように構成された第１の管理対象サーバからアラートを取得し、第１の管理対象サーバに応答して、１または複数のアクセス制御ルールが第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を許可しないことを判定するステップを備える。方法は、第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を記述する通信情報を含むコンテキスト情報を取得するステップをさらに備える。方法は、通信情報に基づいて、過去の通信を正当なもの、または悪意あるものとして分類するステップをさらに備える。方法は、過去の通信を正当なものとして分類したことに応答して、第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を許可するアクセス制御ルールを生成するステップをさらに備える。方法は、アクセス制御ルールを、管理ドメイン全体管理ポリシの一部として記憶するステップをさらに備える。

【０００７】

媒体の実施形態は、ステップを実行するために１または複数のプロセッサによって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。ステップは、第２の管理対象サーバとの過去の通信に応じてアラートを生成するように構成された第１の管理対象サーバからアラートを取得し、第１の管理対象サーバに応答して、１または複数のアクセス制御ルールが第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を許可しないことを判定するステップを備える。ステップは、第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を記述する通信情報を含むコンテキスト情報を取得するステップをさらに備える。ステップは、通信情報に基づいて、過去の通信を正当なもの、または悪意あるものとして分類するステップをさらに備える。ステップは、過去の通信を正当なものとして分類したことに応答して、第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を許可するアクセス制御ルールを生成するステップをさらに備える。ステップは、アクセス制御ルールを、管理ドメイン全体管理ポリシの一部として記憶するステップをさらに備える。

【０００８】

システムの実施形態は、１または複数のプロセッサと、ステップを実行するために１または複数のプロセッサによって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とを備える。ステップは、第２の管理対象サーバとの過去の通信に応じてアラートを生成するように構成された第１の管理対象サーバからアラ

ートを取得し、第１の管理対象サーバに応答して、１または複数のアクセス制御ルールが第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を許可しないと判定するステップを備える。ステップは、第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を記述する通信情報を含むコンテキスト情報を取得するステップをさらに備える。ステップは、通信情報に基づいて、過去の通信を正当なもの、または悪意あるものとして分類するステップをさらに備える。ステップは、過去の通信を正当なものとして分類したことに応答して、第１の管理対象サーバと第２の管理対象サーバとの間の過去の通信を許可するアクセス制御ルールを生成するステップをさらに備える。ステップは、アクセス制御ルールを、管理ドメイン全体管理ポリシの一部として記憶するステップをさらに備える。

【図面の簡単な説明】

【０００９】

【図１】１つの実施形態に従った、管理ドメインのサーバ（物理または仮想）を管理するための環境を示す高レベルブロック図である。

【図２】１つの実施形態に従った、図１に示されるエンティティの１または複数として使用するコンピュータの例を示す高レベルブロック図である。

【図３】１つの実施形態に従った、グローバルマネージャの詳細な表示を示す高レベルブロック図である。

【図４】１つの実施形態に従った、管理対象サーバのポリシ実施モジュールの詳細な表示を示す高レベルブロック図である。

【図５】１つの実施形態に従った、特定の管理対象サーバの管理命令を生成する方法を示すフローチャートである。

【図６】１つの実施形態に従った、管理対象サーバの管理モジュールの構成を生成する方法を示すフローチャートである。

【図７】１つの実施形態に従った、管理対象サーバ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に送信する方法を示すフローチャートである。

【図８】１つの実施形態に従った、管理ドメインのコンピュータネットワークインフラストラクチャの状態への変更を処理する方法を示すフローチャートである。

【図９】１つの実施形態に従った、グローバルマネージャのアクセス制御ルール作成モジュールの詳細な表示を示す高レベルブロック図である。

【図１０】１つの実施形態に従った、複数の管理対象サーバの間の通信を許可するアクセス制御ルールを生成する方法を示すフローチャートである。

【図１１】１つの実施形態に従った、１または複数のアクセス制御ルールを実施する管理対象サーバからのアラートを処理する方法を示すフローチャートである。

【発明を実施するための形態】

【００１０】

図面および以下の説明は、単に例示として特定の実施形態を説明する。本明細書において示される構造および方法の代替的な実施形態が、本明細書において説明される原理を逸脱することなく採用されてよいことを、当業者は以下の説明から容易に理解するであろう。これ以降、いくつかの実施形態に参照が行われ、実施形態の例は添付の図面に示される。実施可能な限り、類似するかまたは同様の参照番号は、図面において使用されてよく、類似するかまたは同様の機能を示してよいことに留意されたい。

【００１１】

図１は、１つの実施形態に従った、管理ドメイン１５０のサーバ（物理または仮想）１３０を管理するための環境１００を示す高レベルブロック図である。管理ドメイン１５０は、たとえば、サービスプロバイダ、法人、大学、または政府機関のような、企業に対応することができる。環境１００は、企業自身によって、または企業によるそのサーバ１３０の管理を支援する第三者（たとえば、第２の企業）によって維持されてよい。図示されているように、環境１００は、ネットワーク１１０、グローバルマネージャ１２０、複数の管理対象サーバ１３０、および複数の非管理対象デバイス１４０を含む。複数の管理対

象サーバ１３０および複数の非管理対象デバイス１４０は、管理ドメイン１５０に関連付けられている。たとえば、これらは、企業によって、または企業の代行として第三者（たとえば、パブリッククラウドサービスプロバイダ）によって運用される。１つのグローバルマネージャ１２０、２つの管理対象サーバ１３０、および２つの非管理対象デバイス１４０は、明確にするために図１に示される実施形態において図示されるが、その他の実施形態は、異なる数のグローバルマネージャ１２０、管理対象サーバ１３０、および／または非管理対象デバイス１４０を有することができる。

【００１２】

ネットワーク１１０は、グローバルマネージャ１２０と、管理対象サーバ１３０と、非管理対象デバイス１４０との間の通信経路を表す。１つの実施形態において、ネットワーク１１０は、標準通信技術および／またはプロトコルを使用し、インターネットを含むことができる。もう１つ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。

【００１３】

管理対象サーバ１３０は、管理ドメイン全体管理ポリシ３３０（図３に図示される）を実施するマシン（物理または仮想）である。１つの実施形態において、サーバは、オペレーティングシステムレベルの仮想化に従った仮想サーバ（場合によっては、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（jail）と称されることもある）のユーザスペースインスタンスであり、これ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（isolated）ユーザスペースインスタンスを可能にするサーバ仮想化の方法である。管理対象サーバ１３０が物理マシンである場合、管理対象サーバ１３０は、コンピュータまたはコンピュータの集合である。管理対象サーバ１３０が仮想マシンである場合、管理対象サーバ１３０は、コンピュータまたはコンピュータの集合上で実行する。管理ドメイン全体管理ポリシ３３０は、管理ドメイン１５０に関連付けられているエンティティがその他のエンティティにアクセスする（もしくはその他のエンティティによってアクセスされる）こと、またはサービスを消費（もしくは提供）することを許可されるかどうか、および／またはどのように許可されるかを指定する。たとえば、管理ドメイン全体管理ポリシ３３０は、セキュリティまたはリソース使用を指定する。セキュリティポリシは、アクセス制御、セキュア接続性、ディスク暗号化、および／または実行可能処理の制御を指定してよいが、リソース使用ポリシは、管理ドメインのコンピューティングリソース（たとえば、ディスク、周辺機器、および／または帯域幅）の使用を指定してよい。

【００１４】

管理対象サーバ１３０は、管理モジュール１３２、管理モジュール構成１３４、およびポリシ実施モジュール１３６を含む。管理モジュール１３２は、管理ドメイン全体管理ポリシ３３０を実施する。たとえば、セキュリティの場合、管理モジュール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、もしくはネットワークトラフィックフィルタリングエンジン（たとえば、Ｗｉｎｄｏｗｓ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）のような低レベルのネットワークまたはセキュリティエンジンであってもよい。リソース使用の場合、管理モジュール１３２は、ディスク使用エンジンまたは周辺機器使用エンジンであってもよい。

【００１５】

管理モジュール構成１３４は、管理モジュール１３２の動作に影響を及ぼす。たとえば、セキュリティの場合、管理モジュール構成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（たとえば、Ｌｉｎｕｘ（登録商標）オペレーティングシステムでｉｐｔａｂｌｅｓエントリおよびｉｐｓｅｔエントリとして具体化されている）によって適用されるセキュア接続性ポリシ、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であってもよい。リソース使用の場合、管理モジュール構成１３４は、ディスク使用エンジンによって適用されるディスク使用ポリシ

、または周辺機器使用エンジンによって適用される周辺機器使用ポリシであってもよい。
【００１６】
ポリシ実施モジュール１３６は、ａ）グローバルマネージャ１２０から受信した管理命令、およびｂ）管理対象サーバ１３０の状態に基づいて、管理モジュール構成１３４を生成する。管理命令は、部分的に、管理ドメイン全体管理ポリシ３３０に基づいて生成される。ポリシ実施モジュール１３６によって生成された管理モジュール構成１３４は、管理ドメイン全体管理ポリシ３３０を（ポリシが管理対象サーバ１３０に関与する範囲において）実施する。この２段階の処理（管理命令を生成するステップ、および管理モジュール構成１３４を生成するステップ）は、管理ポリシの「インスタンス化」と称される。ポリシ実施モジュール１３６はまた、管理対象サーバ１３０のローカル状態を監視し、グローバルマネージャ１２０にローカル状態情報を送信する。
【００１７】
１つの実施形態において、ポリシ実施モジュール１３６は、より大規模な専有（proprietary）モジュール（図示せず）の一部である。専有モジュールは、管理モジュール１３２および管理モジュール構成１３４を既に有するデバイス（または仮想デバイス）上にロードされて、それによりデバイス（または仮想デバイス）を非管理対象デバイス１４０から管理対象サーバ１３０に変換する。ポリシ実施モジュール１３６は、図４、図６、および図７を参照して以下においてさらに説明される。
【００１８】
非管理対象デバイス１４０は、ポリシ実施モジュール１３６を含まないコンピュータ（またはコンピュータの集合）である。非管理デバイス１４０は、管理ドメイン全体管理ポリシ３３０を実施しない。しかし、管理対象サーバ１３０と非管理対象デバイス１４０との間の対話は、管理ドメイン全体管理ポリシ３３０（管理対象サーバ１３０によって実施された）の影響を受けることがある。非管理対象デバイス１４０の１つの例は、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。非管理対象デバイス１４０のもう１つの例は、個人によって使用されて管理ドメイン１５０に自身を認証させるデバイスである（たとえば、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）。
【００１９】
グローバルマネージャ１２０は、管理対象サーバ１３０に対して管理命令を生成し、生成された管理命令をサーバに送信するコンピュータ（またはコンピュータの集合）である。管理命令は、ａ）管理ドメインのコンピュータネットワークインフラストラクチャ３２０の状態、およびｂ）管理ドメイン全体管理ポリシ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ストラクチャ３２０の状態は、管理対象サーバ１３０の記述（descriptions）、および（オプションで）非管理対象デバイス１４０の記述を含む。グローバルマネージャ１２０はまた、管理対象サーバ１３０から受信したローカル状態情報を処理する。
【００２０】
管理ドメイン全体管理ポリシ３３０は、本明細書において「ラベル」と称されるそれらの高レベル特性に基づいて管理対象サーバ１３０を参照することができる論理管理モデルに基づく。ラベルは、「次元」（高レベル特性）および「値」（その高レベル特性の値）を含むペアである。この多次元スペースにおいて構築された管理ポリシは、単一特性のネットワーク／ＩＰアドレスベースのポリシモデルに従って構築された管理ポリシよりもさらに意味を有する（expressive）。特に、「ラベル」の高レベル抽象概念（abstraction）を使用して管理ポリシを表現することで、人々は、管理ポリシをより深く理解し、視覚化し、かつ修正することができる。
【００２１】
論理管理モデル（たとえば、使用可能な次元の数およびタイプ、ならびにそれらの次元の取り得る値）は、構成可能である。１つの実施形態において、論理管理モデルは、表１に示されるように、後段の次元および値を含む。

【００２２】
【表１】

次元	意味（Ｍ）、値（Ｖ）
ロール	Ｍ：管理ドメイン内の管理対象サーバのロール Ｖ：Ｗｅｂ、ＡＰＩ、データベース
環境	Ｍ：管理対象サーバのライフサイクルステージ Ｖ：製作、ステージング、開発
アプリケーション	Ｍ：管理対象サーバが属する論理アプリケーション（管理対象サーバの高レベルのグループ化） Ｖ：取引、人材
業種	Ｍ：管理対象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
位置	Ｍ：管理対象サーバの位置。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。物理的な位置は、特に地理的順守要件を表すのに有効である。 Ｖ：ＵＳまたはＥＵ（物理的）、ＵＳ－ＷＥＳＴ－１またはＵＳ－ＷＥＳＴ－２（論理的）

表１　論理管理モデルの例

【００２３】
論理管理モデルは、複数の管理対象サーバ１３０が、グループ内のすべての管理対象サーバ１３０を記述する１または複数のラベル（本明細書において「ラベルセット」と称される）を指定することによってグループ化されるようにすることができる。ラベルセットは、論理管理モデル内の次元に対してゼロの値または１の値のいずれかを含む。ラベルセットは、論理管理モデル内のすべての次元に対してラベルを含む必要はない。このようにして、論理管理モデルは、管理ドメインの管理対象サーバ１３０のセグメント化および分離、ならびに管理対象サーバ１３０の任意のグループ化の作成を可能にする。論理管理モデルはまた、単一の管理対象サーバ１３０が、複数の重複する集合（つまり、管理対象サーバの複数の重複するグループ）に存在することを許可する。論理管理モデルは、単一の管理対象サーバ１３０が、ネスト化された（nested）集合の階層に存在するよう限定することはない。
【００２４】
たとえば、セキュリティの場合、セグメント化は、特定のポリシの影響を受ける管理対象サーバ１３０のグループを定義するためにアクセス制御ポリシと共に使用されてもよい。同様に、セグメント化は、管理対象サーバ１３０のグループを定義するためのセキュア接続性ポリシ、ならびにグループ内通信およびグループ間通信に適用するポリシと共に使用されてもよい。したがって、管理対象サーバ１３０の第１のグループ（第１のラベルセットによって指定された）間の通信は、第１のセキュア接続設定（たとえば、セキュア接続は要求されない）に制限されることがあり、および管理対象サーバの第１のグループと管理対象サーバの第２のグループ（第２のラベルセットによって指定された）との間の通信は、第２のセキュア接続設定（たとえば、ＩＰｓｅｃカプセル化セキュリティペイロード（Encapsulating Security Payload）（ＥＳＰ）／認証ヘッダ（Authentication Header）（ＡＨ）高度暗号化標準（Advanced Encryption Standard）（ＡＥＳ）／セキュアハッシュアルゴリズム－２（Secure Hash Algorithm-2）（ＳＨＡ－２））に制限されることがある。
【００２５】
環境１００内の各管理対象サーバ１３０は、管理ドメイン全体管理ポリシ３３０を（ポリシが管理対象サーバ１３０に関与する範囲において）実施する。その結果、管理ドメイン全体管理ポリシ３３０は、管理ドメイン１５０全体にわたって分散方式で適用され、チ

ョークポイントは存在しない。また、管理ドメイン全体管理ポリシ３３０は、管理ドメインの物理ネットワークトポロジーおよびネットワークアドレス指定スキームにはかかわりなく、論理レベルにおいて適用される。

【００２６】

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ストラクチャ３２０の状態、および管理ドメイン全体管理ポリシ３３０については、図３、図５、および図８～図１１を参照して、以下においてさらに説明される。

【００２７】

＜コンピュータ＞

図２は、１つの実施形態に従った、図１に示されるエンティティの１または複数として使用するコンピュータ２００の例を示す高レベルブロック図である。示されているのは、チップセット２０４に結合された少なくとも１つのプロセッサ２０２である。チップセット２０４は、メモリコントローラハブ２２０、および入出力（Ｉ／Ｏ）コントローラハブ２２２を含む。メモリ２０６およびグラフィックスアダプタ２１２は、メモリコントローラハブ２２０に結合され、ディスプレイデバイス２１８は、グラフィックスアダプタ２１２に結合される。ストレージデバイス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は、入出力コントローラハブ２２２に結合される。コンピュータ２００のその他の実施形態は、さまざまなアーキテクチャを有する。たとえば、メモリ２０６は、一部の実施形態において、プロセッサ２０２に直接結合される。

【００２８】

ストレージデバイス２０８は、ハードドライブ、コンパクトディスクリードオンリメモリ（ＣＤ－ＲＯＭ）、ＤＶＤ、またはソリッドステートメモリデバイスのような、１または複数の非一時的コンピュータ可読記憶媒体を含む。メモリ２０６は、プロセッサ２０２によって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、データをコンピュータシステム２００に入力するために、キーボード２１０と組み合わせて使用される。グラフィックスアダプタ２１２は、ディスプレイデバイス２１８上に画像およびその他の情報を表示する。一部の実施態様において、ディスプレイデバイス２１８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機能を含む。ネットワークアダプタ２１６は、コンピュータシステム２００をネットワーク１１０に結合する。コンピュータ２００の一部の実施形態は、図２に図示される実施形態とは異なるコンポーネントおよび／またはその他のコンポーネントを有する。たとえば、グローバルマネージャ１２０および／または管理対象サーバ１３０は、複数のブレードサーバで形成されて、ディスプレイデバイス、キーボード、およびその他のコンポーネントを備えていない場合もあり、非管理対象デバイス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もよい。

【００２９】

コンピュータ２００は、本明細書において説明される機能を提供するためにコンピュータプログラムモジュールを実行するように適合される。本明細書において使用されるように、「モジュール」という用語は、指定された機能を提供するために使用されるコンピュータプログラム命令および／またはその他の論理を指す。したがって、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において実施され得る。１つの実施形態において、実行可能コンピュータプログラム命令で形成されるプログラムモジュールは、ストレージデバイス２０８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。

【００３０】

＜グローバルマネージャ＞

図３は、１つの実施形態に従った、グローバルマネージャ１２０の詳細な表示を示す高レベルブロック図である。グローバルマネージャ１２０は、リポジトリ３００、および処理サーバ３１０を含む。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

インフラストラクチャ３２０の状態、および管理ドメイン全体管理ポリシ３３０を記憶するコンピュータ（またはコンピュータの集合）である。１つの実施形態において、リポジトリ３００は、要求に応じて、処理サーバ３１０に、管理ドメイン状態３２０および管理ポリシ３３０へのアクセスを提供するサーバを含む。

【００３１】

＜管理ドメイン状態＞

管理ドメインのコンピュータネットワークインフラストラクチャ３２０の状態は、管理対象サーバ１３０の記述、および（オプションで）非管理対象デバイス１４０の記述を含む。管理対象サーバ１３０の記述は、たとえば、一意の識別子（ＵＩＤ）、オンライン／オフラインインジケータ、１または複数の構成済み特性（オプション）、ネットワーク公開情報、サービス情報、および管理対象サーバ１３０を記述する１または複数のラベル（ラベルセット）を含む。

【００３２】

ＵＩＤは、管理対象サーバ１３０を一意に識別する。オンライン／オフラインインジケータは、管理対象サーバ１３０がオンラインまたはオフラインのいずれであるかを示す。「構成済み特性」は、管理対象サーバ１３０に関連付けられている値を記憶し、任意のタイプの情報であってもよい（たとえば、どのオペレーティングシステムが管理対象サーバ上で稼働しているかのインジケーション）。構成済み特性は、（以下において説明される）ルールの条件部分と併せて使用される。

【００３３】

ネットワーク公開情報は、管理対象サーバのネットワークインタフェースに関する。１つの実施形態において、ネットワーク公開情報は、管理対象サーバのネットワークインタフェースの各々について、ネットワークインタフェースが取り付けられる「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内で動作するために使用されるゼロまたは１以上のＩＰアドレス（およびそれらのサブネット）を含む。ＢＲＮは、組織内または組織全体にわたるサブネットの集合であり、ＢＲＮ内の任意のノードは、ＢＲＮの任意の他のノードとの通信を確立することができる。たとえば、ＢＲＮ内のすべてのノードは、一意のＩＰアドレスを有する。言い換えれば、ＢＲＮは、ＮＡＴを含んではいない。ネットワーク公開情報（たとえば、ネットワークインタフェースのＢＲＮ識別子）は、ルールの条件部分と併せて使用されてもよい。

【００３４】

もう１つの実施形態において、ネットワーク公開情報は、ルーティング情報および／または管理対象サーバがネットワークアドレストランスレータ（ＮＡＴ）の後方にあるかどうか（さらにそれがＮＡＴの後方にある場合、ＮＡＴのどのタイプ、１：１または１：Ｎであるか）を含む。グローバルマネージャ１２０は、管理対象サーバ１３０がネットワークアドレストランスレータ（ＮＡＴ）の後方にあるかどうか（さらにそれがＮＡＴの後方にある場合、ＮＡＴのどのタイプ、１：１または１：Ｎであるか）を判定することができる。たとえば、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接続に従ったサーバのＩＰアドレスと、（ｂ）サーバから受信したローカル状態情報に従ったサーバのＩＰアドレスとを比較することによって、グローバルマネージャ１２０と管理対象サーバ１３０との間にＮＡＴが存在するかどうかを判定する。（ａ）と（ｂ）が異なる場合、グローバルマネージャ１２０と管理対象サーバ１３０との間にＮＡＴが存在する。ＮＡＴが存在しない場合、グローバルマネージャ１２０は、データセンタ検出を実行することによって、ＮＡＴのタイプ（１：１または１：Ｎ）を判定する。たとえば、グローバルマネージャ１２０は、データセンタのパブリックＩＰアドレスによりサーバのデータセンタを識別する。（あるいは、管理対象サーバは、サーバの外部であるがデータセンタの内部である情報にクエリを実行することによってデータセンタ検出を実行する。次いで、サーバは、その情報をローカルステータスの一部としてグローバルマネージャに送信する。）構成情報は、どのタイプのＮＡＴがどのデータセンタによって使用されるかを示す。ＮＡＴ情報が特定のデータセンタに関連付けられていない場合、グロー

バルマネージャ１２０は、ＮＡＴのタイプが１：Ｎであると仮定する。

【００３５】

サービス情報は、たとえば、処理情報および／またはパッケージ情報を含む。処理情報は、たとえば、管理対象サーバ１３０が稼働している処理の名前、それらの処理がリスンしているネットワークポートおよびネットワークインタフェース、それらの処理を開始したユーザ、それらの処理の構成、それらの処理のコマンドライン開始引数、およびそれらの処理の従属性（たとえば、それらの処理がリンクする共有オブジェクト）を含む。（それらの処理は、サービスを提供するか、またはサービスを使用する管理対象サーバ１３０に対応する。）パッケージ情報は、たとえば、どのパッケージ（実行可能ファイル、ライブラリ、またはその他のコンポーネント）が管理対象サーバ１３０にインストールされているか、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を含む。

【００３６】

非管理対象デバイス１４０の記述は、たとえば、ネットワーク公開情報（たとえば、非管理対象デバイス１４０のＩＰアドレス、および非管理対象デバイス１４０が接続されているＢＲＮの識別子）を含む。非管理対象デバイス１４０は、「非管理対象デバイスグループ」（ＵＤＧ）の一部である。ＵＤＧは、１または複数の非管理対象デバイス１４０を含む。たとえば、「Ｈｅａｄｑｕａｒｔｅｒｓ　ＵＤＧ」は、一次回路および管理ドメインの本部によって使用されるバックアップ回路を含む場合もあり、各回路はＩＰアドレスに関連付けられている。ＵＤＧは、一意の識別子（ＵＩＤ）に関連付けられている。ＵＤＧに関して管理ドメイン状態３２０に記憶されている情報は、ＵＤＧのＵＩＤ、およびＵＤＧ内の非管理対象デバイス１４０に関する情報（たとえば、それらのネットワーク公開情報）を含む。

【００３７】

管理対象サーバ１３０および非管理対象デバイス１４０の記述は、グラフィカルユーザインタフェース（ＧＵＩ）またはアプリケーションプログラミングインタフェース（ＡＰＩ）を介してグローバルマネージャ１２０と対話することによってなど、さまざまな方法で管理ドメイン状態３２０にロードされてもよい。管理対象サーバ１３０の記述はまた、管理対象サーバから受信したローカルステータス情報に基づいて管理ドメイン状態３２０にロードされてもよい（以下において説明される）。

【００３８】

特に管理対象サーバのラベル（および、ある場合は構成済み特性）に関して、次元の値の割り当て（もしくは再割り当て）（または構成済み特性の値の設定）は、さらに多くの方法で実行されてもよい。たとえば、割り当て／設定は、管理対象サーバ１３０のプロビジョニング（provisioning）の一部として配備および構成ツールを使用して実行されてもよい。既成のサードパーティツール（たとえば、Ｐｕｐｐｅｔ　ＬａｂｓのＰｕｐｐｅｔソフトウェア、ＯｐｓｃｏｄｅのＣｈｅｆソフトウェア、またはＣＦＥｎｇｉｎｅ　ＡＳのＣＦＥｎｇｉｎｅソフトウェア）、および管理ドメイン１５０が有する場合もあるカスタムツールを含む、任意のそのようなツールが使用されてもよい。

【００３９】

もう１つの例として、割り当て／設定は、ラベルおよび／または構成済み特性（「ＣＣ」）値を算出する「ラベル／構成済み特性エンジン」（図示せず）によって実行されてもよい。１つの実施形態において、ラベル／ＣＣエンジンは、ラベル／ＣＣ割り当てルールに基づいて、ラベル／ＣＣ値を算出する。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（またはラベルもしくはＣＣ値の割り当てを提案する）機能である。ラベル／ＣＣ割り当てルールは、事前設定またはユーザ構成可能であってもよい。たとえば、グローバルマネージャ１２０は、事前定義済みルールのセットを含むが、エンドユーザは、それらのルールを修正および／または削除し、ユーザの各自のカスタム要件に基づいて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、初期化処理の間に、管理対象サーバ１３０に対し

て評価されてもよい。次いで、ラベル／ＣＣ値提案（suggestion）は、任意の次元／ＣＣについて実行されてもよく、エンドユーザは、それらの提案を受諾または拒否することができる。たとえば、管理対象サーバ１３０がＰｏｓｔｇｒｅｓデータベースまたはＭｙＳＱＬデータベースを実行している場合、提案されるラベルは＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞であってもよい。管理対象サーバがＬｉｎｕｘオペレーティングシステムを実行している場合、オペレーティングシステムＣＣについて提案される値は、「Ｌｉｎｕｘ」であってもよい。

【００４０】

もう１つ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いて、ラベル／ＣＣ値を算出する。たとえば、ラベル／ＣＣエンジンは、連結グラフの、最小カット（min-cut）およびＫ平均法（K-means）アルゴリズムの組合せを、追加のヒューリスティックと共に使用して、高度に接続された管理対象サーバ１３０のクラスタを自動的に識別する。管理対象サーバ１３０のクラスタは、管理ドメイン１５０内の「アプリケーション」に対応してよい（表１を参照）。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）の値を、それらの管理対象サーバ１３０に全体として適用するよう選択することができる。

【００４１】

＜管理ドメイン全体管理ポリシ＞

管理ドメイン全体管理ポリシ３３０は、１または複数のルールを含む。大まかに言うと、「ルール」は、サービスの１または複数の提供者と、そのサービスの１または複数の消費者との間の関係を指定する。

【００４２】

ルール機能（rule function）：関係は「ルール機能」に従い、これはルールの実質的な影響である。たとえば、セキュリティの場合、ルール機能は、アクセス制御、セキュア接続性、ディスク暗号化、または実行可能処理の制御であってもよい。アクセス制御機能を伴うルールは、消費者が提供者のサービスを使用してよいかどうかを指定する。１つの実施形態において、アクセス制御機能は、純粋な「ホワイトリスト」モデルを使用するが、これは許可可能な関係のみが表現され、すべての他の関係はデフォルトでブロックされることを意味する。セキュア接続性機能を伴うルールは、どのセキュアチャネル（たとえば、ポイントツーポイントのデータ暗号化を使用する暗号化ネットワークセッション）を介して消費者が提供者のサービスを使用してよいかを指定する。たとえば、セキュア接続性機能を伴うルールは、提供者がＵＳに位置し、消費者がＥＵに位置している場合に、提供者のサービスの使用が暗号化される必要があることを指定することができる。ディスク暗号化機能を伴うルールは、提供者がそのデータを暗号化ファイルシステム上に記憶する必要があるかどうかを指定する。実行可能処理制御機能を伴うルールは、処理が実行を許可されるかどうかを指定する。

【００４３】

リソース使用の場合、ルール機能は、ディスク使用または周辺機器使用であってもよい。ディスク使用機能を伴うルールは、消費者が提供者に記憶することができるデータの量を指定する。ルールが、アクセス制御、セキュア接続性、ディスク暗号化、実行可能処理の制御、ディスク使用、および周辺機器使用のみにとどまらず、その他のルール機能も指定できることに留意されたい。たとえば、ルール機能は、ネットワークトラフィックに適用する開放型システム間相互接続（ＯＳＩ：Open Systems Interconnection）モデルレイヤ７サービス、セキュリティ分析のために収集するメタデータの量、または完全なネットワークパケットを取得ためのトリガを指定することができる。管理ポリシモデルは、適用され得るルール機能の任意の数をサポートする。

【００４４】

ルール機能は、ルールの実質的な影響に関する詳細を指定する１または複数の設定（本明細書において「機能プロファイル」と称される）に関連付けられてもよい。たとえば、セキュア接続性ルール機能に関連付けられている設定は、ネットワークトラフィックを暗

号化するために使用される暗号アルゴリズムのリストであってもよい。１つの実施形態において、ルール機能は、複数の機能プロファイルに関連付けられ、機能プロファイルは優先順位を含む。この優先順位は、以下において説明されるように、機能レベル命令生成モジュール３６０によって使用される。

【００４５】

サービス：一般に、「サービス」は、固有のネットワークプロトコルを使用して固有のネットワークポートで実行する任意の処理である。管理ポリシ３３０内のルールのサービスは、（管理ドメイン状態３２０内の管理対象サーバ１３０の記述に関して上記で説明される）処理情報および／またはパッケージ情報のような、ポート／プロトコルのペアおよび（オプションで）追加の資格（qualification）によって指定される。管理対象サーバ１３０が複数のネットワークインタフェースを有する場合、サービスは、すべてのネットワークで公開されるか、またはそれらのネットワークのサブセットのみで公開されてもよい。エンドユーザは、サービスが公開されるネットワークを指定する。ルール機能に応じて、サービスがネットワークリソースを使用しなくてよい場合もあることに留意されたい。たとえば、実行可能処理制御ルール機能のサービスは、ネットワークプロトコルを使用してネットワークポートでは実行しない。

【００４６】

提供者／消費者－サービスの１または複数の提供者およびサービスの１または複数の消費者（つまりユーザ）は、管理対象サーバ１３０および／または非管理対象デバイス１４０である。

【００４７】

１つの実施形態において、ルールは、ルール機能部分（rule function portion）、サービス部分（service portion）、提供側部分（provided-by portion）、使用側部分（used-by portion）、およびオプションのルール条件部分（rule condition portion）を含む情報のセットを使用して、管理ドメイン全体管理ポリシ３３０内で表される。ルール機能部分は、ルールの実質的な影響を記述し、１または複数の設定（機能プロファイル）に関連付けられてもよい。サービス部分は、ルールが適用するサービスを記述する。サービス部分が「Ａｌｌ（すべて）」を示す場合、ルールはすべてのサービスに適用する。

【００４８】

提供側（ＰＢ）部分は、どの管理対象サーバ１３０および／または非管理対象デバイス１４０がサービスを提供することができるか（つまり、誰が「提供者」であるか）を記述する。ＰＢ部分が「Ａｎｙｂｏｄｙ（誰でも）」を示す場合、誰でも（たとえば、任意の管理対象サーバ１３０または非管理対象デバイス１４０）がサービスを提供することができる。ＰＢ部分が「Ａｎｙ　ｍａｎａｇｅｄ　ｓｅｒｖｅｒ（任意の管理対象サーバ）」を示す場合、任意の管理対象サーバ１３０がサービスを提供することができる。（「任意の管理対象サーバ」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、それによりすべての管理対象サーバ１３０を一致する。）使用側（ＵＢ）部分は、どの管理対象サーバ１３０および／または非管理対象デバイス１４０がサービスを使用することができるか（つまり、誰が「消費者」であるか）を記述する。ＰＢ部分と同様に、ＵＢ部分もまた、「Ａｎｙｂｏｄｙ（誰でも）」または「Ａｎｙ　ｍａｎａｇｅｄ　ｓｅｒｖｅｒ（任意の管理対象サーバ）」を示すことができる。

【００４９】

ＰＢ部分およびＵＢ部分内で、管理対象サーバ１３０は、ラベルセットつまり、管理対象サーバを記述する１または複数のラベル）またはＵＩＤを使用することによって指定される。ラベルセットを使用して管理対象サーバ１３０を指定することができる能力は、論理管理モデルに起因するが、これは管理対象サーバをそれらの次元および値（ラベル）に基づいて参照する。非管理対象デバイス１４０は、非管理対象デバイスグループ（ＵＤＧ）のＵＩＤを使用することによって指定される。ルールがＵＤＧを指定する場合、ルールは、そのグループ内の非管理対象デバイス１４０に関する追加情報（たとえば、デバイスのネットワーク公開情報）を含む。ルールのＰＢ部分および／またはルールのＵＢ部分は

、（管理対象サーバ１３０を指定するための）ラベルセット、管理対象サーバＵＩＤ、および／またはＵＤＧ　ＵＩＤを含む複数の項目を含むことができる。

【００５０】

オプションであるルール条件部分は、ルールが、特定の管理対象サーバ１３０および／またはその管理対象サーバの特定のネットワークインタフェースに適用するかどうかを指定する。ルール条件部分は、１または複数の構成済み特性（「ＣＣ」、管理ドメイン状態３２０の管理対象サーバの記述の一部）および／またはネットワーク公開情報（たとえば、ネットワークインタフェースのＢＲ識別子、また管理ドメイン状態３２０の管理対象サーバの記述の一部）を含むブール表現である。表現のＣＣ部分は、ルールが、特定の管理対象サーバに適用するかどうかを指定するが、表現のネットワーク公開情報部分は、ルールが、その管理対象サーバの特定のネットワークインタフェースに適用するかどうかを指定する。表現が、特定の管理対象サーバの構成済み特性（具体的に、その管理対象サーバの構成済み特性の値に対して）および特定のネットワークインタフェースの情報に対して「真」であると評価する場合、ルールは、その管理対象サーバおよびその管理対象サーバの関連するネットワークインタフェースに適用する。表現が「偽」であると評価する場合、ルールは、その管理対象サーバおよびその管理対象サーバの関連するネットワークインタフェースに適用しない。たとえば、構成済み特性が、どのオペレーティングシステムが管理対象サーバ上で稼働しているかのインジケーションを記憶する場合、その構成済み特性を含むルール条件部分は、ルールが、そのサーバのオペレーティングシステムに基づいて特定の管理対象サーバに適用するかどうかを制御することができる。

【００５１】

管理ドメイン全体管理ポリシ３３０内のルールは、ルールリストに構成される。具体的には、管理ポリシ３３０は、１または複数のルールリストを含み、ルールリストは、１または複数のルールおよび（オプションで）１または複数のスコープ（scope）を含む。「スコープ」は、どこに（つまり、どの管理対象サーバ１３０に）ルールが適用されるかを制約する。スコープは、ルールリスト内のルールの適用を限定する提供側（ＰＢ）部分および使用側（ＵＢ）部分を含む。スコープのＰＢ部分は、ルールのＰＢ部分を限定し、スコープのＵＢ部分は、ルールのＵＢ部分を限定する。スコープのＰＢ部分およびＵＢ部分は、ラベルセットを使用することによって、管理対象サーバ１３０のグループを指定することができる。ラベルセットが、固有の次元に対するラベルを含まない場合、その結果もたらされる管理対象サーバ１３０のグループに対してその次元のスコープは存在しない。ルールリストがスコープを含まない場合、そのルールは全体に適用される。

【００５２】

異なるスコープが、単一のルールリストに適用されてもよい。たとえば、エンドユーザは、Ｗｅｂサービスレイヤ（＜Ｒｏｌｅ，Ｗｅｂ＞ラベルを備える管理対象サーバ１３０）がどのようにデータベースレイヤ（＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞ラベルを備える管理対象サーバ）からのサービスを消費するか、ロードバランシングレイヤがどのようにＷｅｂサービス層からのサービスを消費するか、以下同様、を表現するルールのセットを構築することができる。次いで、エンドユーザが、このルールリストを自身の製作環境（＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞ラベルを備える管理対象サーバ１３０）、および自身のステージング環境（＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｓｔａｇｉｎｇ＞ラベルを備える管理対象サーバ）に適用しようとする場合、エンドユーザは、ルールリストをコピーまたは複製する必要はない。代わりに、エンドユーザは、単一のルールリストに複数のスコープを適用する（ＰＢ部分およびＵＢ部分が＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞ラベルを含む第１のスコープ、およびＰＢ部分およびＵＢ部分が＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｓｔａｇｉｎｇ＞ラベルを含む第２のスコープ）。スコープ抽象化は、ユーザビリティの観点および計算の観点のいずれからも、ルールリストを基準化させる。

【００５３】

管理ドメイン全体管理ポリシ３３０が記述されたので、これ以降、いくつかの例を扱う

ことが有用となる。ユーザデバイスがＷｅｂサーバにアクセスし（第１のレイヤ）、Ｗｅｂサーバがデータベースサーバにアクセスする（第２のレイヤ）２レイヤアプリケーションを備える管理ドメイン１５０を検討する。第１のレイヤにおいて、ユーザデバイスは消費者であり、Ｗｅｂサーバは提供者である。第２のレイヤにおいて、Ｗｅｂサーバは消費者であり、データベースは提供者である。管理ドメイン１５０は、このアプリケーションの２つのインスタンス、つまり製作環境におけるインスタンスとステージング環境におけるインスタンスとを含む。

【００５４】

Ｗｅｂサーバおよびデータベースサーバは、管理対象サーバ１３０であり、これらの記述（たとえば、ラベルセット）は、管理ドメイン状態３２０内に存在する。たとえば、これらのラベルセットは、以下のとおりである。

製作におけるＷｅｂサーバ：＜Ｒｏｌｅ，Ｗｅｂ＞および＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞

製作におけるデータベースサーバ：＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞および＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞

ステージングにおけるＷｅｂサーバ：＜Ｒｏｌｅ，Ｗｅｂ＞および＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｓｔａｇｉｎｇ＞

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

（アプリケーション次元、業種次元、および位置次元はこの例に関連しないので、これらのラベルは省略される。）

【００５５】

これ以降、アクセス制御およびセキュア接続性を指定するセキュリティポリシである、後段の管理ドメイン全体管理ポリシ３３０を検討する。

ルールリスト＃１

－スコープ

・＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞

・＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｓｔａｇｉｎｇ＞

－ルール

・＃１

機能：アクセス制御

サービス：Ａｐａｃｈｅ

ＰＢ：＜Ｒｏｌｅ，Ｗｅｂ＞

ＵＢ：Ａｎｙｂｏｄｙ

・＃２

機能：アクセス制御

サービス：ＰｏｓｔｇｒｅＳＱＬ

ＰＢ：＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞

ＵＢ：＜Ｒｏｌｅ，Ｗｅｂ＞

ルールリスト＃２

－スコープｓ：Ｎｏｎｅ

－ルール

・＃１

機能：セキュア

サービス：Ａｌｌ

ＰＢ：＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞

ＵＢ：Ａｎｙ ｍａｎａｇｅｄ ｓｅｒｖｅｒ

【００５６】

上記のルールが、明確にするために、サービスを単に「Ａｐａｃｈｅ」および「ＰｏｓｔｇｒｅＳＱＬ」と称することに留意されたい。サービスは、処理であり、（管理ドメイ

ン状態３２０内の管理対象サーバ１３０の記述に関して上記で説明される）処理情報および／またはパッケージ情報のような、ポート／プロトコルのペアおよび（オプションで）追加の資格によって指定される。

【００５７】

ルールリスト＃１／ルール＃１は、任意のデバイス（たとえば、ユーザデバイス）が、Ｗｅｂサーバに接続してＡｐａｃｈｅサービスを使用することを許可する。具体的には、接続の許可は、機能部分（Function portion）において「アクセス制御」により指定される。「任意のデバイス」は、ＵＢ部分において「誰でも」により指定される。「Ｗｅｂサーバ」は、ＰＢ部分において「＜Ｒｏｌｅ，Ｗｅｂ＞」（１つのラベルのみを含むラベルセット）により指定される。Ａｐａｃｈｅサービスは、サービス部分において「Ａｐａｃｈｅ」により指定される。

【００５８】

ルールリスト＃１／ルール＃２は、Ｗｅｂサーバが、データベースサーバ上のＰｏｓｔｇｒｅＳＱＬに接続することを許可する。具体的には、接続の許可は、機能部分において「アクセス制御」により指定される。「Ｗｅｂサーバ」は、ＵＢ部分において「＜Ｒｏｌｅ，Ｗｅｂ＞」により指定される。「ＰｏｓｔｇｒｅＳＱＬ」は、サービス部分において「ＰｏｓｔｇｒｅＳＱＬ」により指定される。「データベースサーバ」は、ＰＢ部分において「＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞」（１つのラベルのみを含むラベルセット）により指定される。

【００５９】

ルールリスト＃１はまた、環境間の接続を回避する。たとえば、Ｗｅｂサーバは、Ｗｅｂサーバとデータベースサーバがいずれも同じ環境内にある場合（たとえば、共に製作環境にあるか、または共にステージング環境にある）、データベースサーバ上でＰｏｓｔｇｒｅＳＱＬに接続することが許可される。製作環境にある両サーバは、スコープ部分（Scope portion）において「＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞」（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が、ステージング環境にある両サーバは、スコープ部分において「＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｓｔａｇｉｎｇ＞」（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。（この例のスコープは、ＰＢ部分とＵＢ部分を区別しないので、それぞれのスコープのラベルセットは、ＰＢ部分およびＵＢ部分の両方に適用される。）その結果、Ｗｅｂサーバは、サーバが異なる環境内にある場合（たとえば、Ｗｅｂサーバがステージング環境にあり、データベースサーバが製作環境にある場合）データベースサーバ上でＰｏｓｔｇｒｅＳＱＬに接続することが許可されない。

【００６０】

ルールリスト＃２は、任意の管理対象サーバがデータベースサーバに接続する場合には必ず、その接続は暗号化チャネルを通じて行われる必要があることを記載している。具体的には、「データベースサーバ」は、ＰＢ部分において「＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞」により指定される。「暗号化チャネル」は、機能部分において「セキュア接続性」により指定される。「任意の管理対象サーバ」は、ＵＢ部分において「任意の管理対象サーバ」により指定される。「いつでも」は、サービス部分において「すべて」により指定される。

【００６１】

上記の例を離れ、後段の２つの管理対象サーバ１３０を検討するが、サーバ１は、製作の一部であり、ａｐｐ１の一部であって、カリフォルニアのエンジニアリングによって所有されているＷｅｂサーバである。これは、以下のようにラベル付けされる。

＜Ｒｏｌｅ，Ｗｅｂ＞
＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞
＜Ａｐｐｌｉｃａｔｉｏｎ，ａｐｐ１＞
＜ＬＢ，Ｅｎｇｉｎｅｅｒｉｎｇ＞
＜ロケーション、ＵＳ＞

サーバ２は、製作の一部であり、同様にａｐｐ１の一部であって、ドイツのエンジニアリングに所有されているデータベースサーバである。これは、以下のようにラベル付けされる。
＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ　Ｓｅｒｖｅｒ＞
＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞
＜Ａｐｐｌｉｃａｔｉｏｎ，ａｐｐ１＞
＜ＬＢ，Ｅｎｇｉｎｅｅｒｉｎｇ＞
＜Ｌｏｃａｔｉｏｎ，ＥＵ＞
【００６２】
アクセス制御ルールが、すべてのアクセスを、ａｐｐ１の一部であるすべての管理対象サーバ１３０に許可することを仮定する。このルールは、サーバ１およびサーバ２が相互に通信することを許可し、ａｐｐ２の一部であるドイツの管理対象サーバ１３０が、サーバ１またはサーバ２と通信することを許可しない。これ以降、セキュア接続性ルールが、ＥＵとＵＳとの間のすべてのネットワークトラフィックが暗号化される必要があることを指定すると仮定する。ルール機能は、独立して適用される。言い換えれば、セキュア接続性ルールは、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は、（アクセス制御ルールを所与として）許容され、（セキュア接続性ルールを所与として）暗号化される。
【００６３】
＜アクセス制御ルール＞
図３に戻ると、管理ドメイン全体管理ポリシ３３０は、アクセス制御ルールのセット３３５を含み、これについては以下の「アクセス制御ルール」と題するセクションにおいて説明される。
【００６４】
＜処理サーバ＞
処理サーバ３１０は、管理対象サーバ１３０の管理命令を生成し、生成された管理命令をサーバに送信する。処理サーバ３１０はまた、管理対象サーバ１３０から受信したローカル状態情報を処理する。処理サーバ３１０は、ポリシ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、アクタ列挙モジュール（actor enumeration module）３７０、関連アクタモジュール３８０、管理ドメイン状態更新モジュール３８５、およびアクセス制御ルール作成モジュール３９０のようなさまざまなモジュールを含む。１つの実施形態において、処理サーバ３１０は、リポジトリ３００と通信するコンピュータ（またはコンピュータの集合）を含み、（たとえば、ポリシ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、アクタ列挙モジュール３７０、関連アクタモジュール３８０、管理ドメイン状態更新モジュール３８５、およびアクセス制御ルール作成モジュール３９０を実行することによって）データを処理する。
【００６５】
関連ルールモジュール３５０は、管理ドメイン全体管理ポリシ３３０、および特定の管理対象サーバ１３０のインジケーション（たとえば、そのサーバのＵＩＤ）を入力として取得し、そのサーバに関連するルールのセットを生成して、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が管理ポリシ３３０を検査して、所与の管理対象サーバ１３０に対して関連するルールのみを抽出する、フィルタリング処理である。関連ルールモジュール３５０は、管理ポリシ３３０内のルールリストのすべてを反復し、各ルールリストのスコープを分析してスコープがこの管理対象サーバ１３０に適用するかどうかを判定し、（スコープがこの管理対象サーバ１３０に適用する場合）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管理対象サーバ１３０に適用するかどうかを判定することによって、フィルタリングを実行する。ルールは、ａ）ルールのＰＢ部分および／またはルールのＵＢ部分が管理対象サーバを指定する、およびｂ）ルールの条件部分が（もしあれば）その管理対象サーバに対して（具体的には、その管理対象サーバの構成済み

特性の値およびネットワーク公開情報に対して）「真」であると評価する場合、管理対象サーバ１３０に適用する。最終結果（本明細書において「管理ポリシパースペクティブ（management policy perspective）」と称される）は、この管理対象サーバ１３０がサービスを提供する場合のルール、およびこの管理対象サーバ１３０がサービスを消費する場合のルール、というルールの２つのセットの集合である。

【００６６】

機能レベル命令生成モジュール３６０は、ルールのセット（たとえば、関連ルールモジュール３５０によって生成された管理ポリシパースペクティブ）を入力として取得し、機能レベル命令を生成して、機能レベル命令を出力する。機能レベル命令は、後に、管理命令の一部として管理対象サーバ１３０に送信される。機能レベル命令は、各々がルール機能部分、サービス部分、ＰＢ部分、およびＵＢ部分を含むという点において、ルールと類似している。しかし、ルールは、そのＰＢ部分および／またはＵＢ部分内に（ラベルセット、管理対象サーバＵＩＤ、および／またはＵＤＧ　ＵＩＤを含む）複数の項目を含むことができるが、機能レベル命令は、そのＰＢ部分内に１つの項目のみ、およびそのＵＢ部分内に１つの項目のみを含む。また、ルールは、そのＰＢ部分および／またはＵＢ部分内に（その複数のネットワークインタフェースを含む）管理対象サーバを指定することができるが、機能レベル命令は、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フェースのみを含む。

【００６７】

機能レベル命令生成モジュール３６０は、ルールを分析し、そのルールに基づいて１または複数の機能レベル命令を生成する。ルールのＰＢ部分が複数の項目を含む場合、ルールのＵＢ部分は複数の項目を含むか、または（ＰＢ部分またはＵＢ部分内の）ルールによって参照される管理対象サーバが複数のネットワークインタ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、複数の機能レベル命令を生成する（たとえば、ＰＢ項目、ＵＢ項目、および特定のネットワークインタフェースの取り得る組合せごとに１つの機能レベル命令）。

【００６８】

ルールのＰＢ部分に２つの項目（ＡおよびＢ）を含み、ルールのＵＢ部分に２つの項目（ＣおよびＤ）を含むルールを検討する。機能レベル命令生成モジュール３６０は、１）ＰＢ＝Ａ、ＵＢ＝Ｃ、２）ＰＢ＝Ａ、ＵＢ＝Ｄ、３）ＰＢ＝Ｂ、ＵＢ＝Ｃ、４）ＰＢ＝Ｂ、ＵＢ＝Ｄ、のようなＰＢ部分およびＵＢ部分を伴う４つの機能レベル命令を生成する。これ以降、（たとえば、ＵＩＤまたはラベルセットを指定することによって）ルールのＰＢ部分またはＵＢ部分で管理対象サーバをカバーし、その管理対象サーバが複数のネットワークインタフェースを有するルールを検討する。機能レベル命令生成モジュール３６０は、複数の機能レベル命令を生成する（たとえば、管理対象サーバのネットワークインタフェースごとに１つの機能レベル命令）。

【００６９】

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って参照される機能プロファイルを分析する。ルールリストが複数のスコープを含む場合、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複数回、反復してルールリストに適用する（それにより、各スコープについて機能レベル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もよく、機能プロファイルは優先順位を含むことができることを想起されたい。機能レベル命令生成モジュール３６０は、最高の優先順位を備える機能プロファイルが使用されるように、さまざまな機能プロファイルの優先順位に基づいてルールを順序付ける。機能レベル命令生成モジュール３６０は、順序付けられたルールを、管理対象サーバ１３０が実行するように機能レベル命令に解釈する。機能レベル命令は、ルールに関連付けられているサービスのネットワーク公開の詳細を考慮して、適切な管理対象サーバ１３０および／または非管理対象デバイス１４０（たとえば、入力ルールで参照された管理対象サーバ１３０および／または非管理対象デバイス１４０）。

【００７０】
機能レベル命令生成モジュール３６０は、特定の管理対象サーバ１３０に対して、そのサーバには無関係であると判明する機能レベル命令を生成することができることに留意されたい。たとえば、その管理対象サーバはルールの提供側（ＰＢ）部分によってカバーされているので、機能レベル命令生成モジュール３６０は、対応する機能レベル命令を生成する。しかし、ルールはまた、管理対象サーバのローカル状態を指定する部分（たとえば、提供されるサービスを記述するサービス部分）も含む。グローバルマネージャ１２０は管理対象サーバのローカル状態（たとえば、管理対象サーバが実際にそのサービスを提供しているのかどうか）を認識していないので、生成される機能レベル命令は管理対象サーバに送信される。管理対象サーバは、そのローカル状態（たとえば、管理対象サーバがそのサービスを提供しているかどうか）を確認し、ポリシコンパイルモジュール４１０を参照して以下において説明されるように、それに応じて機能レベル命令を処理する。
【００７１】
アクタ列挙モジュール３７０は、管理対象サーバ１３０および非管理対象デバイスグループ（ＵＤＧ）の記述（たとえば、管理ドメインのコンピュータネットワークインフラストラクチャ３２０の状態）の集合を入力として取得し、サーバおよびＵＤＧのそれらの記述の表示を（「アクタセット」と称される）列挙型形式で生成して、アクタセットを出力する。たとえば、アクタ列挙モジュール３７０は、管理ドメイン状態３２０内の管理対象サーバ１３０およびＵＤＧ、および取り得るラベルセットを列挙して、各々に一意の識別子（ＵＩＤ）を割り当てる。次いで、これらのアクタセットは、管理対象サーバＵＩＤ、ＵＤＧ　ＵＩＤ、および／またはラベルセットを使用してアクタを指定するルールおよびスコープのＰＢ部分およびＵＢ部分と併せて使用されてもよい。
【００７２】
Ｎの次元D_i（ｉ＝１、．．．、Ｎ）の集合を含み、各次元D_iが可能な値V_j（ｊ＝１、．．．、M_i）のセットＳｉを含む（ただし、ワイルドカード「＊」は取り得る値のうちの１つである）論理管理モデルを検討する。１つの実施形態において、アクタ列挙モジュール３７０は、論理管理モデルに基づいて取り得るすべてのラベルセットを列挙するが、これは$S_1 \times S_2 \times . . . S_N$によって与えられるデカルト積と等しい。このセットの大きさは、$M_1 \times M_2 \times . . . \times M_N$である。列挙処理は、管理対象サーバ１３０の多次元ラベルスペースを、単純な列挙型形式に縮小する。
【００７３】
もう１つの実施形態において、アクタ列挙モジュール３７０は、管理ドメイン状態３２０に基づいて（たとえば、管理ドメイン１５０内の管理対象サーバ１３０の記述に基づいて）取り得るラベルセットのみを列挙する。たとえば、２つの次元（ＸおよびＹ）を含み、各次元が３つの取り得る値（Ａ、Ｂ、および＊）を含む論理管理モデルを検討する。ラベルセット「＜Ｘ＝Ａ＞、＜Ｙ＝Ｂ＞」を備える管理対象サーバは、１）「＜Ｘ＝Ａ＞、＜Ｙ＝Ｂ＞」、２）「＜Ｘ＝Ａ＞、＜Ｙ＝＊＞」、３）「＜Ｘ＝＊＞、＜Ｙ＝Ｂ＞」、および４）「＜Ｘ＝＊＞、＜Ｙ＝＊＞」、という４つの取り得るラベルセットの要素であってもよい。管理対象サーバのラベルセットは２次元スペース（ＸおよびＹ）に存在するが、取り得るラベルセット２、３、および４は、管理対象サーバのラベルセットの下位次元スペースへの射影である（ラベルセット２は１次元スペース（Ｘ）、ラベルセット３は１次元スペース（Ｙ）、およびラベルセット４は０次元スペース）。したがって、アクタ列挙モジュール３７０は、それらの４つの可能なラベルセットを列挙する。ラベルセット「＜Ｘ＝Ａ＞、＜Ｙ＝Ｂ＞」を備える管理対象サーバは、ラベルセット「＜Ｘ＝Ａ＞、＜Ｙ＝Ａ＞」の要素とはなり得ないので、アクタ列挙モジュール３７０は、そのラベルセットを列挙しない。
【００７４】
さらにもう１つの実施形態において、アクタ列挙モジュール３７０は、管理ドメイン全体管理ポリシ３３０において（たとえば、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列挙する。

【００７５】
アクタセットは、ＵＩＤ、およびゼロまたは１以上のアクタセットレコードを含む。アクタセットレコードは、ＵＩＤ（管理対象サーバＵＩＤまたはＵＤＧ　ＵＩＤのいずれか）、アクタのオペレーティングシステムの識別子、および固有のＢＲＮを所与とするアクタ（管理対象サーバ１３０または非管理対象デバイス１４０）のＩＰアドレスを含む。たとえば、アクタセットは、ＩＰアドレスが、＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞および＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞のラベルセットによりカバーされる管理対象サーバ１３０のすべてに対応するアクタセットレコードを含んでもよい。もう１つの例として、アクタセットは、ＩＰアドレスが、本部ＵＤＧの非管理対象デバイス１４０のすべてに対応するアクタセットレコードを含んでもよい。単一のアクタ（たとえば、管理対象サーバ１３０または非管理対象デバイス１４０）は、複数のアクタセットに出現することができる。
【００７６】
アクタセットの計算におけるもう１つの要因は、複数のネットワークインタフェースを備えるアクタに加えて、ネットワークアドレス変換（ＮＡＴ）のようなネットワークトポロジーの包含である。したがって、＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ＞および＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞のラベルセットについて、管理対象サーバ１３０のインターネット接続の（つまり、第１のＢＲＮに関連付けられている）ＩＰアドレスを備える１つのアクタセット、およびそれらの管理対象サーバのプライベートネットワーク接続の（つまり、第２のＢＲＮに関連付けられている）ＩＰアドレスを備える同じ管理対象サーバの別のアクタセット、という、２つのアクタセットがあってもよい。
【００７７】
１つの実施形態において、アクタ列挙モジュール３７０はまた、管理ドメイン状態３２０への変更に基づいてアクタセットを更新することもできる。たとえば、アクタ列挙モジュール３７０は、（アクタ列挙モジュールによって以前出力された）アクタセット、および（管理ドメイン状態３２０内の）管理対象サーバの記述の変更を入力として取得し、（変更されたサーバの記述と一貫する）更新済みのアクタセットを生成して、更新済みのアクタセットを出力する。アクタ列挙モジュール３７０は、管理対象サーバの記述への変更のタイプに応じて、さまざまな方法で更新済みのアクタセットを生成する。
【００７８】
オンライン／オフライン変更：記述の変更が、オンラインからオフラインにサーバが推移したことを示す場合、アクタ列挙モジュール３７０は、サーバが要素であったすべての入力アクタセットからサーバのアクタセットレコードを除去することによって更新済みのアクタセットを生成する。記述の変更が、オフラインからオンラインにサーバが推移したことを示す場合、アクタ列挙モジュール３７０は、サーバのアクタセットレコードを任意の関連する入力アクタセットに追加することによって更新済みのアクタセットを生成する。（必要な場合、アクタ列挙モジュール３７０は、新しいアクタセットを作成して、サーバのアクタセットレコードをその新しいアクタセットに追加する）。
【００７９】
ラベルセットの変更：記述の変更が、サーバのラベルセットが変更されたことを示す場合、アクタ列挙モジュール３７０は、これを第１のサーバ（古いラベルセットを備える）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備える）がオンラインになるかのように処理する。
【００８０】
ネットワーク公開情報の変更：記述の変更が、ネットワークインタフェースをサーバが除去したことを示す場合、アクタ列挙モジュール３７０は、サーバが要素であったすべての入力アクタセット（ネットワークインタフェースのＢＲＮに関連付けられている）からサーバのアクタセットレコードを除去することによって更新済みのアクタセットを生成する。記述の変更が、ネットワークインタフェースをサーバが追加したことを示す場合、アクタ列挙モジュール３７０は、サーバのアクタセットレコードを（そのネットワークイン

タフェースのＢＲＮに関連付けられている）任意の関連する入力アクタセットに追加することによって更新済みのアクタセットを生成する。（必要な場合、アクタ列挙モジュール３７０は、（そのネットワークインタフェースのＢＲＮに関連付けられている）新しいアクタセットを作成して、サーバのアクタセットレコードをその新しいアクタセットに追加する）。記述の変更が、ネットワークインタフェースのＢＲＮをサーバが変更したことを示す場合、アクタ列挙モジュール３７０は、これを第１のネットワークインタフェース（古いＢＲＮを備える）が除去され、第２のネットワークインタフェース（新しいＢＲＮを備える）が追加されるかのように処理する。記述の変更が、ネットワークインタフェースのＩＰアドレス（ただしＢＲＮではない）をサーバが変更したことを示す場合、アクタ列挙モジュール３７０は、サーバが要素であったすべての（そのネットワークインタフェースのＢＲＮに関連付けられている）入力アクタセット内のサーバのアクタセットレコードを修正することによって更新済みのアクタセットを生成する。

【００８１】

関連アクタモジュール３８０は、１または複数のアクタセット（たとえば、列挙型形式の管理ドメイン状態３２０内の管理対象サーバ１３０およびＵＤＧ）およびルールのセット（たとえば、管理ポリシパースペクティブ）を入力として取得し、どのアクタセットがそのルールに関連するかを判定して、それらのアクタセットのみを出力する。これは、関連アクタモジュール３８０がアクタセットを検査して、所与のルールのセットに対して関連するアクタセットのみを抽出する、フィルタリング処理である。関連アクタモジュール３８０は、入力アクタセットのすべてを反復し、入力ルールのＰＢ部分およびＵＢ部分を分析して特定のアクタセットがルールの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フィルタリングを実行する。最終結果（本明細書において「アクタパースペクティブ」と称される）は、アクタセットの集合である。アクタパースペクティブは、後に、管理命令の一部として管理対象サーバ１３０に送信される。

【００８２】

１つの実施形態において、関連アクタモジュール３８０は、ルールの入力セットを使用して「アクタセットフィルタ」を生成する。アクタセットフィルタは、入力アクタセットから、入力ルールに関連するアクタセットのみを選択する。言い換えれば、関連アクタモジュール３８０は、アクタセットフィルタを使用して、入力アクタセットを関連アクタセットにフィルタリングする。

【００８３】

ポリシエンジンモジュール３４０は、管理対象サーバ１３０の管理命令を生成し、生成された管理命令をサーバに送信する。ポリシ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ストラクチャ３２０の状態、およびｂ）管理ドメイン全体管理ポリシ３３０に基づいて、（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、アクタ列挙モジュール３７０、および関連アクタモジュール３８０を使用して）管理命令を生成する。

【００８４】

たとえば、ポリシエンジンモジュール３４０は、管理ドメイン全体管理ポリシ３３０および特定の管理対象サーバ１３０のＵＩＤを入力として提供し、関連ルールモジュール３５０を実行する。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（「管理ポリシパースペクティブ」）を出力する。ポリシエンジンモジュール３４０は、管理ドメイン状態３２０を入力として提供し、アクタ列挙モジュール３７０を実行する。アクタ列挙モジュール３７０は、列挙型形式の管理ドメイン状態３２０内の管理対象サーバ１３０および非管理対象デバイスグループ（ＵＤＧ）の記述の表示（「アクタセット」）を出力する。ポリシエンジンモジュール３４０は、（関連ルールモジュール３５０によって出力された）管理ポリシパースペクティブを入力として提供し、機能レベル命令生成モジュール３６０を実行する。機能レベル命令生成モジュール３６０は、機能レベル命令を出力する。ポリシエンジンモジュール３４０は、（列挙モジュール３７０によって出力

された）アクタセットおよび（関連ルールモジュール３５０によって出力された）管理ポリシパースペクティブを入力として提供して、関連アクタモジュール３８０を実行する。関連アクタモジュール３８０は、そのルールに関連するアクタセット（「関連アクタセット」）のみを出力する。ポリシ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によって出力された）機能レベル命令および（関連アクタモジュール３８０によって出力された）関連アクタセットを特定の管理対象サーバ１３０に送信する。

【００８５】

１つの実施形態において、ポリシエンジンモジュール３４０は、上記の処理の間に生成された情報をキャッシュに入れる。たとえば、ポリシエンジンモジュール３４０は、特定の管理対象サーバ１３０に関連して、管理ポリシパースペクティブ、機能レベル命令、アクタセットフィルタ、および／または関連アクタセットをキャッシュに入れる。もう１つの例として、ポリシエンジンモジュール３４０は、管理ドメインのアクタセット（特定の管理対象サーバ１３０に固有ではない）をキャッシュに入れる。

【００８６】

管理ドメインのアクタセットは管理ドメイン状態３２０に基づいているので、管理ドメイン状態３２０への変更は、管理ドメインのアクタセットへの変更を必要とする可能性がある。同様に、管理対象サーバの管理命令は、管理ドメイン状態３２０および管理ドメイン全体管理ポリシ３３０に基づいているので、管理ドメイン状態３２０への変更および／または管理ドメイン全体管理ポリシ３３０への変更は、管理対象サーバの管理命令への変更を必要とする可能性がある。１つの実施形態において、ポリシエンジンモジュール３４０は、管理ドメインのアクタセットを更新、および／または管理対象サーバの管理命令を更新し、次いでそれらの変更を（必要な場合）管理対象サーバ１３０に配布することができる。前述のキャッシュに入れられた情報は、ポリシエンジンモジュール３４０が、管理ドメインのアクタセットおよび／または管理対象サーバの管理命令をより効率的に更新して、変更を配布する上で役立つ。

【００８７】

１つの実施形態において、ポリシエンジンモジュール３４０は、（管理ドメイン状態３２０への変更に基づいて）管理ドメインのアクタセットを更新し、管理対象サーバ１３０への変更を、次のように配布する。ポリシエンジンモジュール３４０は、（アクタ列挙モジュールによって以前出力された）キャッシュに入れられているアクタセットおよび（たとえば、変更済みのサーバの記述など）管理ドメイン状態３２０の変更済み部分を入力として提供して、アクタ列挙モジュール３７０を実行する。アクタ列挙モジュール３７０は、更新済みのアクタセットを出力する。１つの実施形態において、ポリシエンジンモジュール３４０は、次いで、更新済みのアクタセットのすべてを、管理ドメイン１５０内の管理対象サーバ１３０のすべてに送信する。しかし、すべての管理対象サーバが、すべてのアクタセットへの変更の影響を受けるわけではないので、その実施形態は非効率的である。

【００８８】

もう１つの実施形態において、選択されたアクタセットのみが、選択されたサーバに送信される。たとえば、特定の管理対象サーバが、ａ）そのサーバに以前送信された、およびｂ）変更された、アクタセットのみを送信される。キャッシュに入れられている関連アクタセットは、どのアクタセットが以前そのサーバに送信されたかを示す（上記（ａ）を参照）。ポリシエンジンモジュール３４０は、どのアクタセットが変更されているかを判定するため、キャッシュに入れられているアクタセットを、更新済みのアクタセットと比較する（上記（ｂ）を参照）。次いで、ポリシエンジンモジュール３４０は、（ａ）と（ｂ）の論理積を計算する。その論理積内のアクタセットは、特定の管理対象サーバに送信される。１つの実施形態において、さらに一層効率を高めるために、アクタセットは、キャッシュに入れられているアクタセットと更新済みのアクタセットとの間の差を記述する「ｄｉｆｆ」フォーマットで送信される。たとえば、ｄｉｆｆフォーマットは、アクタセット識別子、アクタ識別子（たとえば、管理対象サーバＵＩＤまたはＵＤＧ　ＵＩＤ）、

およびアクタがアクタセット内で追加されるべきか、除去されるべきか、または修正されるべきかどうかのインジケーションを指定する。

【００８９】

さらにもう１つの実施形態において、２つのテーブルが保持されて、効率を高めるために使用される。第１のテーブルは、管理対象サーバ１３０を、その管理対象サーバが要素であるアクタセットに関連付ける。第２のテーブルは、管理対象サーバ１３０を、（たとえば、関連アクタモジュール３８０によって判定された）その管理対象サーバに関連するアクタセットに関連付ける。これらのテーブルにおいて、管理対象サーバ１３０は、たとえばその管理対象サーバのＵＩＤによって表され、アクタセットは、たとえばそのアクタセットのＵＩＤによって表される。ポリシエンジンモジュール３４０は、管理ドメイン状態３２０の変更済み部分（たとえば、変更済みのサーバの記述）を使用して、どの管理対象サーバの記述が変更されたかを判定する。ポリシエンジンモジュール３４０は、第１のテーブルを使用して、その管理対象サーバが要素であったアクタセットを判定する。それらのアクタセットは、変更済みのサーバの記述の結果として変更してもよい。したがって、ポリシエンジンモジュール３４０は、第２のテーブルを使用して、それらのアクタセットが関連する管理対象サーバを判定する。ポリシエンジンモジュール３４０は、上記で説明された論理積計算を、それらの管理対象サーバについてのみ実行する。

【００９０】

１つの実施形態において、ポリシエンジンモジュール３４０は、（管理ドメイン状態３２０への変更に基づいて）管理対象サーバの管理命令を更新し、更新済みの管理命令を管理対象サーバに、次のように送信する。ポリシエンジンモジュール３４０は、管理ドメイン全体管理ポリシ３３０および管理対象サーバ１３０のＵＩＤを入力として提供し、関連ルールモジュール３５０を実行する。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（「管理ポリシパースペクティブ」）を出力する。ポリシエンジンモジュール３４０は、先ほど出力された管理ポリシパースペクティブを、キャッシュに入れられている管理ポリシパースペクティブと比較して、これらが異なっているかどうかを判定する。先ほど出力された管理ポリシパースペクティブおよびキャッシュに入れられている管理ポリシパースペクティブが同一である場合、ポリシエンジンモジュール３４０は、さらにアクションを実行することはない。この状況において、以前生成された管理対象サーバの管理命令（具体的には、機能レベル命令および関連アクタセット）は、管理ドメイン状態３２０への変更と一貫しており、再生成されて管理対象サーバに再送信される必要はない。

【００９１】

先ほど出力された（just-output）管理ポリシパースペクティブおよびキャッシュに入れられている管理ポリシパースペクティブが異なる場合、ポリシエンジンモジュール３４０は、どのルールがキャッシュに入れられているパースペクティブに追加されるべきか、およびどのルールがキャッシュに入れられているパースペクティブから除去されるべきかを判定する。ポリシエンジンモジュール３４０は、追加すべきルールおよび除去すべきルールを入力として提供し、機能レベル命令生成モジュール３６０を実行する。機能レベル命令生成モジュール３６０は、（以前管理対象サーバに送信された、キャッシュに入れられている機能レベル命令に関して）追加すべき機能レベル命令および除去すべき機能レベル命令を出力する。ポリシエンジンモジュール３４０は、管理対象サーバに、必要に応じて、さまざまな機能レベル命令を追加または除去するよう命令する。１つの実施形態において、さらに一層効率を高めるために、機能レベル命令は、キャッシュに入れられている機能レベル命令と更新済みの機能レベル命令との間の差を記述する「ｄｉｆｆ」フォーマットで送信される。たとえば、ｄｉｆｆフォーマットは、機能レベル命令識別子、および機能レベル命令が以前送信された機能レベル命令に追加されるべきか、または除去されるべきかどうかのインジケーションを指定する。

【００９２】

ポリシエンジンモジュール３４０はまた、キャッシュに入れられているアクタセットお

よび（たとえば、変更済みのサーバの記述など）管理ドメイン状態３２０の変更済み部分を入力として提供して、アクタ列挙モジュール３７０を実行する。アクタ列挙モジュール３７０は、更新済みのアクタセットを出力する。ポリシエンジンモジュール３４０は、更新済みのアクタセットおよび先ほど出力された管理ポリシパースペクティブを入力として提供し、関連アクタモジュール３８０を実行する。関連アクタモジュール３８０は、そのルールに関連する更新済みのアクタセット（「更新済みの関連アクタセット」）のみを出力する。

【００９３】

ポリシエンジンモジュール３４０は、更新済みの関連アクタセットを、キャッシュに入れられている関連アクタセットと比較して、これらが異なっているかどうかを判定する。更新済みの関連アクタセットおよびキャッシュに入れられている関連アクタセットが同一である場合、ポリシエンジンモジュール３４０は、アクタセットを管理対象サーバに送信しない。この状況において、以前生成された関連アクタセットは、管理ドメイン状態３２０への変更と一貫しており、管理対象サーバに再送信される必要はない。更新済みの関連アクタセットおよびキャッシュに入れられている関連アクタセットが異なる場合、ポリシエンジンモジュール３４０は、キャッシュに入れられている関連アクタセットに関してどのアクタセットが追加されるべきか、除去されるべきか、または修正されるべきかを判定する。ポリシエンジンモジュール３４０は、管理対象サーバに、必要に応じて、さまざまなアクタセットを追加、除去、または修正するよう命令する。１つの実施形態において、さらに効率を高めるために、アクタセットは、キャッシュに入れられている関連アクタセットと更新済みの関連アクタセットとの間の差を記述する「ｄｉｆｆ」フォーマットで送信される。たとえば、ｄｉｆｆフォーマットは、アクタセット識別子、およびそのアクタセットが以前送信されたアクタセットに関して追加まされるべきか、除去されるべきか、または修正されるべきかどうかのインジケーションを指定する。

【００９４】

ポリシエンジンモジュール３４０が、（管理ドメイン全体管理ポリシ３３０への変更に基づいて）管理対象サーバの管理命令を更新し、更新済みの管理命令を管理対象サーバに送信できることを想起されたい。管理ポリシ３３０への変更は、たとえば、ルールもしくはルールセットの追加、除去、または修正である。１つの実施形態において、管理ポリシ３３０への変更は、ＧＵＩまたはＡＰＩを介するグローバルマネージャ１２０との対話によって生成される。もう１つの実施形態において、管理ポリシ３３０への変更は、（たとえば、グローバルマネージャによって検出されたセキュリティ脅威に応じて）グローバルマネージャ１２０内の自動化処理によって生成される。ポリシエンジンモジュール３４０は、管理対象サーバの管理命令を更新し、管理ポリシ３３０への変更または管理ドメイン状態３２０への変更があったかどうかにはかかわりなく、同様の方法で更新済みの管理命令を管理対象サーバに送信する。しかし、わずかな差がある。

【００９５】

管理ポリシ３３０への変更の場合、ポリシエンジンモジュール３４０は、必ずしも、すべての管理対象サーバ１３０の管理命令を更新するわけではない。代わりに、ポリシエンジンモジュール３４０は、以前の管理ポリシ３３０を、新しい管理ポリシ３３０と比較して、以前の管理ポリシ３３０に関してルールが追加されるべきか、除去されるべきか、または修正されるべきかどうかを判定する。ポリシエンジンモジュール３４０は、どの管理対象サーバ１３０が、変更済みのルールの影響を受けるか（たとえば、どの管理対象サーバが、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、ならびにｂ）ルールの条件部分（ある場合は）によってカバーされるか）を判定する。ポリシエンジンモジュール３４０は、（新しい管理ポリシ３３０全体ではなく）変更済みのルール、および（変更済みのルールの影響を受けるサーバのみについて）管理対象サーバ１３０のＵＩＤを入力として提供し、関連ルールモジュール３５０を実行する。

【００９６】

管理ドメイン状態更新（ＡＤＳＵ）モジュール３８５は、管理ドメイン状態３２０への

変更を受信し、それらの変更を処理する。管理ドメイン状態３２０への変更は、たとえば、（管理対象サーバのラベルセットまたは構成済み特性の修正を含む）管理対象サーバ１３０の記述、または非管理対象デバイスもしくは非管理対象デバイスグループの記述の追加、除去、または修正である。１つの実施形態において管理ドメイン状態３２０への変更は、特定の管理対象サーバ１３０から受信したローカル状態情報に由来する。もう１つの実施形態において、管理ドメイン状態３２０への変更は、ＧＵＩまたはＡＰＩを介するグローバルマネージャ１２０との対話によって生成される。さらにもう１つの実施形態において、管理ドメイン状態３２０への変更は、（たとえば、グローバルマネージャによって検出されたセキュリティ脅威に応じて）グローバルマネージャ１２０内の自動化処理によって生成される。

【００９７】

たとえば、ＡＤＳＵモジュール３８５は、特定の非管理対象デバイス１４０に関する変更を受信する。ＡＤＳＵモジュール３８５は、（たとえば、その特定の非管理対象デバイスが要素である非管理対象デバイスグループの一部として）管理ドメイン状態３２０に新しい情報を記憶する。次いで、ＡＤＳＵモジュール３８５は、非管理対象デバイスグループの変更に基づいて、管理ドメインのアクタセットを更新する。具体的には、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に、管理ドメインのアクタセットを更新するよう命令する。１つの実施形態において、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に管理ドメインのアクタセットを更新するよう命令する前に、イベントが発生するのを待つ。このイベントは、たとえば、ユーザコマンドの受信、または指定された保守ウィンドウの発生であってもよい。

【００９８】

もう１つの例として、ＡＤＳＵモジュール３８５は、特定の管理対象サーバ１３０に関する変更を受信する。ＡＤＳＵモジュール３８５は、特定の管理対象サーバ１３０の記述の一部として管理ドメイン状態３２０に新しい情報を記憶する。次いで、ＡＤＳＵモジュール３８５は、その管理対象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、その情報を記述に記憶する。次いで、ＡＤＳＵモジュール３８５は、管理対象サーバの記述への変更に基づいて、管理ドメインのアクタセットおよび／または管理対象サーバの管理命令を更新するかどうかを判定する。ＡＤＳＵモジュール３８５が管理ドメインのアクタセットを更新すると判定する場合、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に、管理ドメインのアクタセットを更新するよう命令する。１つの実施形態において、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に管理ドメインのアクタセットを更新するよう命令する前に、イベントが発生するのを待つ。ＡＤＳＵモジュール３８５が管理対象サーバの管理命令を更新すると判定する場合、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に、管理対象サーバの管理命令を更新するよう命令する。１つの実施形態において、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に管理対象サーバの管理命令を更新するよう命令する前に、イベントが発生するのを待つ。前述のイベントは、たとえば、ユーザコマンドの受信、または指定された保守ウィンドウの発生であってもよい。

【００９９】

ＡＤＳＵモジュール３８５が、管理ドメインのアクタセットおよび／または管理対象サーバの管理命令を更新するよう判定するかどうかは、管理対象サーバの記述への変更のタイプに依存する。１つの実施形態において、ＡＤＳＵモジュール３８５は、この判定を表２に図示されるように実行する。

【０１００】

【表２】

変更のタイプ	更新するか
オンライン－オフライン	管理ドメインのアクタセット：Ｙｅｓ 管理対象サーバの管理命令：Ｎｏ
オンライン－オフライン	管理ドメインのアクタセット：Ｙｅｓ 管理対象サーバの管理命令：Ｙｅｓ
ラベルセット	管理ドメインのアクタセット：Ｙｅｓ 管理対象サーバの管理命令：Ｙｅｓ
構成済み特性	管理ドメインのアクタセット：Ｙｅｓ 管理対象サーバの管理命令：Ｙｅｓ
ネットワーク公開情報	管理ドメインのアクタセット：Ｙｅｓ 管理対象サーバの管理命令：Ｙｅｓ（ＩＰアドレスが単なる変更でない限り）
サービス情報	管理ドメインのアクタセット：Ｎｏ 管理対象サーバの管理命令：Ｙｅｓ（指定された状況でのみ）

表２　サーバの記述の変更のタイプに基づく管理ドメインのアクタセットおよび／または管理対象サーバの管理命令

【０１０１】

１つの実施形態において、ＡＤＳＵモジュール３８５は、ラベル／構成済み特性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、サーバの記述およびラベル／ＣＣ割り当てルールに基づいて、サーバのラベル／ＣＣ値を算出する。もう１つ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トランスレータ（ＮＡＴ）の後方にあるかどうか（さらにサーバがＮＡＴの後方にある場合、ＮＡＴのどのタイプ、１：１または１：Ｎであるか）を判定する。

【０１０２】

アクセス制御ルール作成モジュール３９０については、以下の「アクセス制御ルール」と題するセクションにおいて記述される。

【０１０３】

＜ポリシ実施モジュール＞

図４は、１つの実施形態に従った、管理対象サーバ１３０のポリシ実施モジュール１３６の詳細なビューを示す高レベルブロック図である。ポリシ実施モジュール１３６は、ローカル状態リポジトリ４００、ポリシ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、およびアラート生成モジュール４３０を含む。ローカル状態リポジトリ４００は、管理対象サーバ１３０のローカル状態に関する情報を記憶する。１つの実施形態において、ローカル状態リポジトリ４００は、管理対象サーバ１３０のオペレーティングシステム（ＯＳ）、ネットワーク公開、およびサービスに関する情報を記憶する。ＯＳ情報は、たとえば、どのＯＳが稼働しているかのインジケーションを含む。ネットワーク公開情報およびサービス情報は、管理ドメイン状態３２０内の管理対象サーバ１３０の記述に関して上記で説明されている。

【０１０４】

ポリシコンパイルモジュール４１０は、管理命令および管理対象サーバ１３０の状態を入力として取得し、管理モジュール構成１３４を生成する。たとえば、管理命令は、グローバルマネージャ１２０から受信され、（機能レベル命令生成モジュール３６０によって生成された）機能レベル命令および（関連アクタモジュール３８０によって出力された）関連アクタセットを含む。管理対象サーバ１３０の状態は、ローカル状態リポジトリ４００から取り出される。１つの実施形態において、ポリシコンパイルモジュール４１０の実行は、ａ）管理対象サーバの電源投入またはオンライン状態、ｂ）管理対象サーバの管理

命令受信、および／またはｃ）ローカル状態リポジトリ４００の内容の変化によってトリガされる。

【０１０５】

ポリシコンパイルモジュール４１０は、機能レベル命令および関連アクタセットを管理モジュール構成１３４にマップする。たとえば、ポリシコンパイルモジュール４１０は、（ポートおよびアクタセット参照を含む）アクセス制御機能レベル命令を、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、またはＷｉｎｄｏｗｓオペレーティングシステムのＷｉｎｄｏｗｓフィルタリングプラットフォーム（ＷＦＰ）ルールにマップする。

【０１０６】

管理対象サーバ１３０における管理ポリシの適用は、そのサーバのローカル状態の影響を受ける可能性がある。１つの実施形態において、ポリシコンパイルモジュール４１０は、受信した機能レベル命令に関連付けられている条件を評価し、その評価の結果に基づいて管理モジュール構成１３４を生成する。たとえば、ポリシコンパイルモジュール４１０は、管理対象サーバのピア（つまり、関係内の他のアクタ）のオペレーティングシステムを参照する条件を評価して、その評価の結果に基づいて機能プロファイル属性を選択するが、選択される機能プロファイル属性は管理モジュール構成１３４で表現される。

【０１０７】

もう１つの例として、管理対象サーバ１３０が、そのサーバには無関係であると判明する機能レベル命令を受信できることを想起されたい。たとえば、ルールは、管理対象サーバのローカル状態を指定する部分（たとえば、提供されるサービスを記述するサービス部分）も含む。グローバルマネージャ１２０は管理対象サーバのローカル状態（たとえば、管理対象サーバが実際にそのサービスを提供しているのかどうか）を認識していないので、生成される機能レベル命令は管理対象サーバに送信される。ポリシコンパイルモジュール４１０は、管理対象サーバのローカル状態（たとえば、管理対象サーバがそのサービスを提供しているかどうか）を確認する。この判定は、管理対象サーバのローカル状態を参照する条件を評価することになる。ポリシコンパイルモジュール４１０は、それに応じて機能レベル命令を処理する。ポリシコンパイルモジュール４１０が、条件が「真」であると評価する（たとえば、管理対象サーバがそのサービスを提供している）と判定する場合、ポリシコンパイルモジュール４１０は、その機能レベル命令を管理モジュール構成１３４に組み入れる。具体的には、ポリシコンパイルモジュール４１０は、（そのサーバのローカル状態に関与する）関連条件を評価した後に限り、機能レベル命令を管理モジュール構成１３４に組み入れる。条件の評価が偽である場合、ポリシコンパイルモジュール４１０は、機能レベル命令を管理モジュール構成１３４で表現しない。固有の条件（たとえば、それらの本質および特定の値）は、拡張可能である。１つの実施形態において、条件は、「サービス」の定義に関連し、（管理ドメイン状態３２０内の管理対象サーバ１３０の記述に関して上記で説明される）処理情報および／またはパッケージ情報を含む。

【０１０８】

たとえば、ポート８０のＡｐａｃｈｅサービスインバウンドのみへのアクセスを許容する（つまり、管理対象サーバ１３０が「提供者」またはエンドポイントである場合）機能レベル命令を検討する。管理対象サーバ１３０は、この機能レベル命令を管理モジュール構成１３４で表現して、ポート８０でリスンしている（そのサーバで実行中の）アプリケーションが実際にＡｐａｃｈｅであって、他のアプリケーション（ローグまたはそれ以外）ではないかどうかに関与する、関連条件を評価した後に限り、ポート８０でのアクセスを許容する。管理対象サーバ１３０は、関連条件が「真」であると評価することを判定した後に限り、機能レベル命令を管理モジュール構成１３４で表現する。関連条件が「偽」であると評価する場合、管理対象サーバ１３０は、この機能レベル命令を管理モジュール構成１３４で表現しない。その結果、ネットワークトラフィックはブロックされる。

【０１０９】

１つの実施形態において、管理対象サーバ１３０は、そのアウトバウンド接続を監視す

る。管理対象サーバ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処理がそれらのアウトバウンド接続を確立しているかを判定する。管理対象サーバ１３０は、アウトバウンド接続を確立するために（上記で「処理情報」として言及される、要件のセットを所与として）特定の処理のみを許容するルールを強行することができる。

【０１１０】

１つの実施形態（図示せず）において、ポリシコンパイルモジュール４１０は、管理対象サーバ１３０ではなく、グローバルマネージャ１２０に位置する。その実施形態において、グローバルマネージャ１２０は、管理命令を管理対象サーバ１３０に送信しない。その代わり、管理対象サーバ１３０は、そのローカル状態をグローバルマネージャ１２０に送信する。ポリシコンパイルモジュール４１０が（グローバルマネージャ１２０において）管理モジュール構成１３４を生成した後、管理モジュール構成１３４は、グローバルマネージャ１２０から管理対象サーバ１３０に送信される。

【０１１１】

ローカル状態更新（ＬＳＵ）モジュール４２０は、管理対象サーバ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に送信する。１つの実施形態において、ＬＳＵモジュール４２０は、管理対象サーバ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に記憶して、そのローカル状態情報をグローバルマネージャ１２０に送信する。ＬＳＵモジュール４２０は、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さまざまな部分を検査することによって、管理対象サーバ１３０のローカル状態を判定する。たとえば、ＬＳＵモジュール４２０は、ＯＳのカーネルテーブルから（ネットワーキング情報）、ＯＳのシステムテーブルから（パッケージ情報）、およびファイルシステムから（ファイルおよびハッシュ値）、サービス情報を取得する。ＬＳＵモジュール４２０は、ＯＳのカーネルおよび／またはＯＳレベルのデータ構造からネットワーク公開情報を取得する。

【０１１２】

ＬＳＵモジュール４２０が初期ローカル状態情報をグローバルマネージャ１２０に送信した後、ＬＳＵモジュールは、ローカル状態への変更を監視する。ＬＳＵモジュールは、たとえば、ポーリング（たとえば、定期的に検査を実行する）、またはリスニング（たとえば、イベントストリームにサブスクライブする）によって変更を監視する。ＬＳＵモジュール４２０は、最近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にすでに記憶されている情報と比較する。情報が一致する場合、ＬＳＵモジュール４２０は、（ローカル状態情報が再度取得されるまで）さらにアクションを実行することはない。情報が異なる場合、ＬＳＵモジュール４２０は、最近取得された情報をローカル状態リポジトリ４００に記憶し、管理モジュール構成１３４を再生成（およびそれに応じて管理モジュール１３２を再構成）するためにポリシコンパイルモジュール４１０を実行して、グローバルマネージャ１２０に変更を通知する。１つの実施形態において、ＬＳＵモジュール４２０は、ローカル状態情報への変更を、以前ローカル状態リポジトリ４００に記憶され（したがって、以前グローバルマネージャ１２０に送信された）ローカル状態情報と最近取得されたローカル状態情報との間の差を記述する、「ｄｉｆｆ」フォーマットで、グローバルマネージャ１２０に送信する。たとえば、ｄｉｆｆフォーマットは、ローカル状態情報のタイプ（たとえば、オペレーティングシステム）、およびその情報タイプの新しい値を指定する。もう１つ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の内容全体をグローバルマネージャ１２０に送信する。

【０１１３】

アラート生成モジュール４３０については、以下において「アクセス制御ルール」と題するセクションにおいて説明される。

【０１１４】

＜管理命令の生成＞

図５は、１つの実施形態に従った、特定の管理対象サーバ１３０の管理命令を生成する

方法５００を示すフローチャートである。その他の実施形態は、異なる順序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、ステップの一部または全部は、図１に図示されているエンティティ以外のエンティティによって実行されてもよい。１つの実施形態において、方法５００は、複数回（たとえば、管理ドメイン１５０内の各管理対象サーバ１３０ごとに１回）実行される。

【０１１５】

方法５００が始動するとき、管理ドメインのコンピュータネットワークインフラストラクチャ３２０の状態、および管理ドメイン全体管理ポリシ３３０は、グローバルマネージャ１２０のリポジトリ３００にすでに記憶されている。この時点において、方法５００は開始する。

【０１１６】

ステップ５１０において、管理ドメイン状態３２０および管理ドメイン全体管理ポリシ３３０がアクセスされる。たとえば、ポリシエンジンモジュール３４０は、リポジトリ３００に要求を送信し、それに応じて、管理ドメイン状態３２０および管理ドメイン全体管理ポリシ３３０を受信する。

【０１１７】

ステップ５２０において、１または複数の関連ルールが判定される。たとえば、ポリシエンジンモジュール３４０は、管理ドメイン全体管理ポリシ３３０および特定の管理対象サーバ１３０のＵＩＤを入力として提供し、関連ルールモジュール３５０を実行する。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（管理ポリシパースペクティブ）を出力する。

【０１１８】

ステップ５３０において、アクタが列挙される。たとえば、ポリシエンジンモジュール３４０は、管理ドメイン状態３２０を入力として提供し、アクタ列挙モジュール３７０を実行する。アクタ列挙モジュール３７０は、列挙型形式の管理ドメイン状態３２０内の管理対象サーバ１３０および非管理対象デバイスグループ（ＵＤＧ）の表示（アクタセット）を生成する。

【０１１９】

ステップ５４０において、１または複数の機能レベル命令が生成される。たとえば、ポリシエンジンモジュール３４０は、（ステップ５２０において生成された）管理ポリシパースペクティブを入力として提供し、機能レベル命令生成モジュール３６０を実行する。機能レベル命令生成モジュール３６０は、機能レベル命令を生成する。

【０１２０】

ステップ５５０において、１または複数の関連アクタが判定される。たとえば、ポリシエンジンモジュール３４０は、（ステップ５３０において生成された）アクタセットおよび（ステップ５２０において生成された）管理ポリシパースペクティブを入力として提供し、関連アクタモジュール３８０を実行する。関連アクタモジュール３８０は、そのルールに関連するアクタセット（関連アクタセット）のみを出力する。

【０１２１】

ステップ５６０において、管理命令は、特定の管理対象サーバ１３０に送信される。たとえば、ポリシエンジンモジュール３４０は、（ステップ５４０において生成された）機能レベル命令および（ステップ５５０において生成された）関連アクタセットを特定の管理対象サーバ１３０に送信する。

【０１２２】

ステップ５２０およびステップ５４０は、特定の管理対象サーバ１３０の管理ポリシパースペクティブ（およびその結果もたらされる機能レベル命令）を生成することに関与しているが、ステップ５３０およびステップ５５０は、その管理対象サーバのアクタパースペクティブを生成することに関与していることに留意されたい。ステップ５２０が、ステップ５５０によって使用されるルールのセットを生成するので、管理ポリシパースペクティブの生成およびアクタパースペクティブの生成は、最低限に相互に依存している。そう

であっても、管理ポリシの計算（つまり、ステップ５２０およびステップ５４０）ならびにアクタセットの計算（つまり、ステップ５３０およびステップ５５０）を別々にしておくことで、ポリシエンジンモジュールのスケーラビリティを強化する。管理ポリシの計算およびアクタセットの計算はほとんどの場合別々にされているので、これらは（たとえば同じ管理対象サーバ１３０に対してであっても）並行して実行されてもよい。加えて、異なる管理対象サーバ１３０に対するパースペクティブの計算もまた、並列に実行されてもよい。さらに、アクタが変更する場合、再計算される必要があるのはアクタセットだけである。（機能レベル命令は再計算される必要はない。）ルールが変更する場合、再計算される必要があるのは機能レベル命令および関連アクタセットだけである。（アクタは再列挙される必要はない。）

【０１２３】

＜管理モジュールの構成＞

図６は、１つの実施形態に従った、管理対象サーバ１３０の管理モジュール１３２のための構成１３４を生成する方法６００を示すフローチャートである。その他の実施形態は、異なる順序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、ステップの一部または全部は、図１に図示されているエンティティ以外のエンティティによって実行されてもよい。

【０１２４】

方法６００が始動するとき、管理対象サーバ１３０のローカル状態に関する情報は、すでに管理対象サーバ１３０内のポリシ実施モジュール１３６のローカル状態リポジトリ４００に記憶されている。この時点において、方法６００は開始する。

【０１２５】

ステップ６１０において、管理命令がグローバルマネージャ１２０から受信される。たとえば、ポリシコンパイルモジュール４１０は、機能レベル命令および関連アクタセットをグローバルマネージャ１２０から受信する。

【０１２６】

ステップ６２０において、ローカル状態がアクセスされる。たとえば、ポリシコンパイルモジュール４１０は、ローカル状態リポジトリ４００に記憶されている管理対象サーバ１３０のローカル状態に関する情報にアクセスする。

【０１２７】

ステップ６３０において、管理モジュール構成１３４が生成される。たとえば、ポリシコンパイルモジュール４１０は、（ステップ６１０において受信した）管理命令および（ステップ６２０においてアクセスされた）ローカル状態を入力として取得し、管理モジュール構成１３４を生成する。

【０１２８】

ステップ６４０において、管理モジュール構成１３２が構成される。たとえば、ポリシコンパイルモジュール４１０は、（ステップ６３０において生成された）管理モジュール構成１３４に従って動作するように管理モジュール１３２を構成する。

【０１２９】

＜管理対象サーバの監視＞

図７は、１つの実施形態に従った、管理対象サーバ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に送信する方法７００を示すフローチャートである。その他の実施形態は、異なる順序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、ステップの一部または全部は、図１に図示されているエンティティ以外のエンティティによって実行されてもよい。

【０１３０】

方法７００が始動するとき、管理対象サーバ１３０のローカル状態に関する情報は、すでに管理対象サーバ１３０のローカル状態リポジトリ４００に記憶されている。この時点において、方法７００は開始する。

【０１３１】

ステップ７１０において、管理対象サーバ１３０の現在のローカル状態に関する情報が判定される。たとえば、ＬＳＵモジュール４２０は、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さまざまな部分を検査することによって、管理対象サーバ１３０のローカル状態を判定する。

【０１３２】

ステップ７２０において、判定は、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に記憶されている情報と異なるかどうかに関して実行される。たとえば、ＬＳＵモジュール４２０は、この判定を実行する。情報が異なっていない場合、方法はステップ７３０に進み、終了する。情報が異なっている場合、方法は、ステップ７４０に進む。

【０１３３】

ステップ７４０において、異なる情報は、ローカル状態リポジトリ４００に記憶される。たとえば、ＬＳＵモジュール４２０は、このステップを実行する。

【０１３４】

ステップ７５０において、管理モジュール構成１３４は、（ローカル状態リポジトリ４００の内容が変更したので）再生成され、それに応じて管理モジュール１３２は再構成される。たとえば、ＬＳＵモジュール４２０は、管理モジュール構成１３４を再構成するポリシコンパイルモジュール４１０を実行する。

【０１３５】

ステップ７６０において、異なる情報は、グローバルマネージャ１２０に送信される。たとえば、ＬＳＵモジュール４２０は、このステップを実行する。

【０１３６】

＜管理ドメイン状態の更新＞

図８は、１つの実施形態に従った、管理ドメインのコンピュータネットワークインフラストラクチャ３２０の状態への変更を処理する方法８００を示すフローチャートである。その他の実施形態は、異なる順序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、ステップの一部または全部は、図１に示されているエンティティ以外のエンティティによって実行されてもよい。

【０１３７】

ステップ８１０において、特定の管理対象サーバ１３０に関する変更が受信される。たとえば、管理ドメイン状態更新（ＡＤＳＵ）モジュール３８５は、ローカル状態情報の一部として管理対象サーバ１３０から、オンライン／オフラインインジケータ、オペレーティングシステムインジケータ、ネットワーク公開情報、および／またはサービス情報を受信する。

【０１３８】

ステップ８２０において、受信された情報が記憶される。たとえば、ＡＤＳＵモジュール３８５は、受信したオンライン／オフラインインジケータ、ネットワーク公開情報、および／またはサービス情報を管理ドメイン状態３２０に（具体的には、情報が関連する管理対象サーバ１３０の記述に）記憶する。

【０１３９】

ステップ８３０において、サーバに関する追加情報を判定するために、サーバの記述は分析される。たとえば、ＡＤＳＵモジュール３８５は、サーバのラベル／ＣＣ値を算出するためにラベル／構成済み特性エンジンを使用する、および／またはサーバがネットワークアドレストランスレータ（ＮＡＴ）の後方にあるかどうか（さらにサーバがＮＡＴの後方にある場合、ＮＡＴのどのタイプ、１：１または１：Ｎであるか）を判定して、その情報をサーバの記述に記憶する。ステップ８３０はオプションである。

【０１４０】

ステップ８４０において、判定は、管理ドメインのアクタセットを更新するかどうかに関して実行される。たとえば、ＡＤＳＵモジュール３８５は、管理対象サーバの記述への変更に基づいて、管理ドメインのアクタセットを更新するかどうかを判定する。管理ドメ

インのアクタセットを更新するよう判定が実行される場合、方法はステップ８５０に進む。管理ドメインのアクタセットを更新しないよう判定が実行される場合、方法はステップ８６０に進む。

【０１４１】

ステップ８５０において、管理ドメインのアクタセットが更新される。たとえば、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に、管理ドメインのアクタセットを更新し、それに応じて、影響を受ける管理対象サーバ１３０に通知するよう命令する。１つの実施形態（図示せず）において、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に管理ドメインのアクタセットを更新するよう命令する前に、イベントが発生するのを待つ。

【０１４２】

ステップ８６０において、判定は、管理対象サーバの管理命令を更新するかどうかに関して実行される。たとえば、ＡＤＳＵモジュール３８５は、管理対象サーバの記述への変更に基づいて、管理対象サーバの管理命令を更新するかどうかを判定する。管理対象サーバの管理命令を更新するよう判定が実行される場合、方法はステップ８７０に進む。管理対象サーバの管理命令を更新しないよう判定が実行される場合、方法はステップ８８０に進む。

【０１４３】

ステップ８７０において、管理対象サーバの管理命令は更新される。たとえば、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に、管理対象サーバの管理命令を更新するよう命令する。１つの実施形態（図示せず）において、ＡＤＳＵモジュール３８５は、ポリシエンジンモジュール３４０に管理対象サーバの管理命令を更新するよう命令する前に、イベントが発生するのを待つ。

【０１４４】

ステップ８８０において、方法は終了する。

【０１４５】

＜アクセス制御ルール＞

グローバルマネージャ１２０の管理ドメイン全体管理ポリシ３３０が、アクセス制御ルールのセット３３５を含むことを想起されたい。アクセス制御ルールのセット３３５は、アクセス制御ルール機能を伴うルールである１または複数のアクセス制御ルールを含む。概して、アクセス制御ルールは、第１の管理対象サーバ１３０と、第２の管理対象サーバ１３０または非管理対象デバイス１４０または管理ドメイン１５０外部のデバイスとの間の通信を許可する。１つの実施形態において、アクセス制御ルールは、消費者が提供者のサービスを使用してよいかどうかを指定する。そのようなアクセス制御ルールは、提供側（ＰＢ）部分、使用側（ＵＢ）部分、およびサービスを指定する。１つの実施形態において、アクセス制御ルールは、アクセス制御ルールのセット３３５が一致するＰＢ、ＵＢ、およびサービス部分を伴うアクセス制御ルールを含む場合に限り、消費者が提供者のサービスにアクセスしてよい、純粋な「ホワイトリスト」モデルに使用される。

【０１４６】

アクセス制御ルールは、１または複数の部分の代わりにワイルドカードを使用することによって、ＰＢ、ＵＢ、およびサービス部分を一部分だけ指定してよい。たとえば、アクセス制御ルールが、ワイルドカードを指定するＵＢ部分を有する場合、任意の管理対象サーバ１３０、非管理対象デバイス１４０、または管理ドメイン１５０外部の他のデバイスはサービスにアクセスしてよい。ＰＢ部分およびＵＢ部分は、（たとえば、管理対象サーバＵＩＤまたはＵＤＧ　ＵＩＤを使用して）１または複数の特定のアクタ、１または複数のラベルセット、またはそれらの組合せを指定してよい。例示のアクセス制御ルールは、特定の管理対象サーバ１３０を示すＰＢ部分、ならびにラベルセット＜Ｒｏｌｅ，Ｄａｔａｂａｓｅ　Ｓｅｒｖｅｒ＞および＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞を示すＵＢ部分を有する。例示のアクセス制御ルールは、「データベースサーバ」ロールを有し、「製作」環境に属する管理対象サーバ１３０が、特定の管理対象サーバ１３０に

おいてサービスにアクセスすることを許容する。

【０１４７】

管理対象サーバ１３０のポリシ実施モジュール１３６は、アラート生成モジュール４３０を含むことを想起されたい。アラート生成モジュール４３０は、管理モジュール構成１３４に含まれるアクセス制御ルールを順守するために、管理対象サーバ１３０とその他のアクタ（管理対象サーバ１３０、非管理対象デバイス１４０、または管理ドメイン１５０外部のデバイス）との間の通信（「ネットワークトラフィック」とも称される）を監視する。アラート生成モジュール４３０は、アクセス制御ルールに適合しない通信（「無許可の通信」と称される）を検出したことに応じてアラートを生成し、アラートをグローバルマネージャ１２０に送信するが、アラートはアクセス制御ルール作成モジュール３９０によって（具体的には、アラート処理モジュール９５０によって）処理される。無許可の通信は、管理対象サーバ１３０によって提供されるサービスを使用しようとする消費者による試行、および別のアクタによって提供されるサービスを使用しようとする管理対象サーバ１３０による試行を含む。たとえば、サービスに関連付けられているポートとの間でネットワークトラフィックを送信または受信しようとする試行は、無許可の通信となる可能性がある。アクセス制御ルールが容認可能なアクティビティのホワイトリストとしての役割を果たす１つの実施形態において、管理モジュール１３２は、アクセス制御ルールと一致する試行された通信を許容し、アクセス制御ルールと一致しない試行された通信を拒否する。

【０１４８】

管理モジュール１３２が管理対象サーバ１３０との間の通信を拒否またはブロックする場合、アラート生成モジュール４３０はアラートを生成する。アラートは、通信に対応するサービス、サービスの提供者、およびサービスの消費者を記述する。アラートは、サービスについての関連サービス情報、ならびに提供者および消費者についてのネットワーク公開情報を含んでよい。アラートは、通信の特性を記述する通信情報を含んでよい。通信情報は、タイミング、期間、頻度、プロトコルタイプ、データサイズ（たとえば、合計サイズ、パケットサイズ）、または試行された通信のデータ転送速度を含んでよい。たとえば、通信情報は、サービスにアクセスしようとする単一の試行と、サービスにアクセスしようとする繰り返しの試行とを区別する。通信情報はまた、ソースアドレス、宛先アドレス、およびパス情報（たとえば、無許可の通信をルーティングするロードバランサおよびＮＡＴデバイス）のような通信のルーティング情報も記述してよい。

【０１４９】

＜アクセス制御ルール作成モジュール＞

グローバルマネージャ１２０の処理サーバ３１０が、アクセス制御ルール作成モジュール３９０を含むことを想起されたい。図９は、１つの実施形態による、グローバルマネージャ１２０のアクセス制御ルール（ＡＣＲ）作成モジュール３９０の詳細なビューを示す高レベルブロック図である。ＡＣＲ作成モジュール３９０は、コンテキスト情報収集モジュール９１０、管理対象サーバグルーピングモジュール９２０、ラベリングエンジン９３０、フロー処理モジュール９４０、アラート処理モジュール９５０、およびアクセス制御ルール（ＡＣＲ）作成インタフェース９６０を含む。

【０１５０】

コンテキスト情報収集モジュール９１０は、管理ドメイン１５０内のアクタ（管理対象サーバ１３０または非管理対象デバイス１４０）を記述し、管理ドメイン１５０内のアクタによって送信または受信された通信を記述するコンテキスト情報を取得する。コンテキスト情報は、管理対象サーバ情報、非管理対象デバイス情報、外部デバイス情報、通信情報、および管理ドメイン情報を含む。

【０１５１】

管理対象サーバ情報は、管理対象サーバ１３０の特性を記述する。管理対象サーバ情報は、管理ドメイン状態３２０に関して上記で説明されるように、処理情報およびパッケージ情報のようなサービス情報を含む。管理対象サーバ情報は、識別子（たとえば、ＵＩＤ

、インターネットプロトコル（ＩＰ）アドレス、メディアアクセス制御（ＭＡＣ）アドレス、ホスト名）、ハードウェアリソース（たとえば、プロセッサタイプ、プロセッサスループット、プロセッサロード、合計メモリ、使用可能メモリ、ネットワークインタフェースデバイス、ストレージデバイスタイプ）、または管理対象サーバのタイプ（たとえば、物理デバイス、クラウド提供の仮想デバイス、仮想マシン、Ｌｉｎｕｘコンテナ）を記述してよい。管理対象サーバ情報は、処理情報およびパッケージ情報によって記述されるオペレーティングシステムおよびその他のソフトウェアのような、ソフトウェアリソースを記述してよい。

【０１５２】

仮想またはクラウドベースの管理対象サーバ１３０はまた、環境情報に関連付けられており、この情報は、管理対象サーバ１３０の提供者（たとえば、専有のデータセンタ、サードパーティプライベートデータセンタ、クラウド提供者）および提供者と通信するための通信プロトコル（たとえば、カプセル化情報、ネットワークアドレス、ネットワークアドレス変換）を記述する。管理対象サーバ１３０に関する管理対象サーバ情報は、管理対象サーバのローカル状態リポジトリ４００に記憶され、コンテキスト情報収集モジュール９１０により処理するためにグローバルマネージャ１２０に送信される。管理対象サーバ情報を仮想またはクラウドベースの管理対象サーバ１３０から取り出すため、コンテキスト情報収集モジュール９１０は、管理対象サーバ情報またはその他のコンテキスト情報を送信するようクラウドサービス提供者または仮想サーバを提供するソフトウェアにクエリを行ってよい。

【０１５３】

非管理対象デバイス情報は、管理ドメイン状態３２０に関して上記で説明されるように、ネットワーク公開情報のような、非管理対象デバイス１４０の特定を記述する。非管理対象デバイス情報は、非管理対象デバイス１４０の識別子（たとえば、ＵＤＧ　ＵＩＤ、ＩＰアドレス、ＭＡＣアドレス、デバイス名）、ハードウェアリソース、ソフトウェアリソース、またはネットワーク接続性（たとえば、使用可能なポート、ポートとサービスとの間のマッピング）を含んでよい。管理対象サーバ１３０は、管理対象サーバ１３０と通信する非管理対象デバイス１４０についての非管理対象デバイス情報を収集して、コンテキスト情報収集モジュール９１０により処理するために非管理対象デバイス情報をグローバルマネージャ１２０に送信してよい。あるいは、または加えて、グローバルマネージャ１２０は、非管理対象デバイス情報を収集するように管理ドメイン１５０内の非管理対象デバイス１４０にクエリを実行する。非管理対象デバイス１４０は、非管理対象デバイスのローカル状態をレポートするポリシ実施モジュール１３６を含まないので、非管理対象デバイス情報は、管理対象サーバ情報に比べて不完全であるかまたはあまり詳細ではなくてよい。

【０１５４】

外部デバイス情報は、管理対象サーバ１３０と通信する管理ドメインに外部のデバイスの特性を記述する。外部デバイス情報は、外部デバイスの識別子（たとえば、ＩＰアドレス、ユニフォームリソースロケータ（ＵＲＬ）、その他のＷｅｂアドレス）、ハードウェアリソース、ソフトウェアリソース、またはネットワーク接続性を含んでよい。管理対象サーバ１３０は、外部デバイス情報を収集し、コンテキスト情報収集モジュール９１０により処理するために情報をグローバルマネージャ１２０に送信してよいが、外部デバイス情報の多くは管理対象サーバ１３０に対して可視でなくてもよい。加えて、外部デバイス情報は、外部デバイスの信頼性を示す、外部デバイスの信用情報を記述する。１つの実施形態において、コンテキスト情報収集モジュール９１０は、外部デバイスの識別子と一致する信用情報を取得する。信用情報を使用して、コンテキスト情報収集モジュール９１０は、外部デバイスを、安全、不正、または中間として分類する。信用情報は、２進インジケータ（たとえば、外部デバイスの識別子がブラックリストにあるかどうか）またはスコア（たとえば、識別子に関連付けられている危険の相対的判定）であってよい。

【０１５５】

通信情報は、アラート生成モジュール４３０に関連して上記で説明されている。管理対象サーバ１３０は、管理対象サーバ１３０によって送信または受信された通信を記述するグローバルマネージャ１２０に、通信情報を送信する。１つの実施形態において、管理対象サーバ１３０は、通信が許可されているか、または許可されていないかを評価することにはかかわりなく、通信についての通信情報を送信する。コンテキスト情報収集モジュール９１０が同一の通信を記述する重複通信情報を受信したとき、コンテキスト情報収集モジュール９１０は、重複通信情報を結合または非重複化してよい。たとえば、コンテキスト情報収集モジュール９１０は、サービスを提供する管理対象サーバおよびサービスを消費する管理対象サーバという、２つの管理対象サーバ１３０から受信した通信情報を非重複化する。

【０１５６】

コンテキスト情報収集モジュール９１０は、管理対象サーバ１３０から受信したコンテキスト情報に基づいて、管理ドメイン情報を生成する。管理ドメイン情報は、管理ドメイン１５０にわたり、または管理ドメイン１５０内のアクタのサブセットにわたり、コンテキスト情報を集約する。管理ドメイン内のアクタのサブセットは、ラベルセットによって記述される管理対象サーバ１３０であってよい。１つの実施形態において、管理ドメイン情報は、少なくとも１つの共通する特性を有する通信を記述する。共通する特性は、特定のポート、処理、プロトコル、またはアクタ（たとえば、管理対象サーバ１３０、非管理対象デバイス１４０、外部デバイス）であってよい。たとえば、コンテキスト情報収集モジュール９１０は、特定のサービスに関連付けられている破損した２進数を有する管理対象サーバ１３０の数を示す管理ドメイン情報を生成する。もう１つの例として、コンテキスト情報収集モジュール９１０は、特定のアクタによってスキャンされた管理対象サーバ１３０の数を示す管理ドメイン情報を生成する。「スキャニング」は、管理対象サーバ１３０に要求（たとえば、プローブ）を送信すること、および管理対象サーバの応答（またはその欠如）を使用して、管理対象サーバ１３０の構成および管理対象サーバ１３０上で実行中の処理を取得または自動的に判定することを指す。

【０１５７】

１つの実施形態において、コンテキスト情報収集モジュール９１０は、管理ドメイン１５０内の異常なアクティビティを示す管理ドメイン情報を生成する。コンテキスト情報収集モジュール９１０は、特定のアクタ、（たとえば、共通のラベルセットによって特徴付けられる）管理対象サーバ１３０のグループ、共通のサービス、またはその他の特性に関連付けられているコンテキスト情報を識別する。コンテキスト情報収集モジュール９１０は、数量（たとえば、通信の量、破損したファイルの数）を使用してコンテキスト情報を要約し、数量を、しきい値数量と比較する。しきい値数量は、事前構成済みの設定に基づいてもよいか、または数量の以前の履歴の標準に基づいて動的に判定されてよい。たとえば、しきい値数量は、数量について週単位の移動平均を上回る２つの標準偏差である。しきい値数量との比較に応じて、コンテキスト情報収集モジュール９１０は、要約されたコンテキスト情報が異常であるかどうかを判定する。たとえば、コンテキスト情報収集モジュール９１０は、管理対象サーバ１３０がアクセスしたサービスに関連付けられていないポートの数がしきい値数を超える場合、管理対象サーバ１３０がサービスに関連付けられていない異常な数のポートにアクセスしようと試行していると判定する。

【０１５８】

管理対象サーバグルーピングモジュール９２０は、管理ドメイン１５０内のアクタの間の通信を記述する通信情報を取得する。通信情報に基づいて、管理対象サーバグルーピングモジュール９２０は、管理対象サーバ１３０をアプリケーショングループにグループ化する。アプリケーショングループは、グループに外部のアクタとの通信の量と比較して著しい量の通信をグループ内に有する管理対象サーバ１３０のセットである。１つの実施形態において、管理対象サーバグルーピングモジュール９２０は、グラフを構築し、ここでノードは管理ドメイン１５０の管理対象サーバ１３０を表し、エッジは管理対象サーバ１３０の間の通信を表す。エッジは、ノードの間の通信の存在／不在を示す２進値を有する

か、または通信の量を定量化する非２進値（たとえば、頻度、データサイズ、期間）を有する。たとえば、２つのノードを接続するエッジの値は、２つのノードに対応する管理対象サーバ１３０の間で交換されるデータの日次量である。グラフは、通信の方向を無視するエッジで方向付けられていなくてもよいか、または通信の方向に従って有向エッジで方向付けられてよい。たとえば、ノードから逸れて指し示す方向性エッジは、対応する管理対象サーバ１３０がサービスの消費者であることを示し、ノードの方向を指し示す方向性エッジは、管理対象サーバ１３０がサービスの提供者であることを示す。管理対象サーバグルーピングモジュール９２０は、グラフを、各々アプリケーショングループに対応するサブグラフに区分化する。たとえば、管理対象サーバグルーピングモジュール９２０は、縦型検索、Ｋ平均クラスタ、またはグラフを区分化する最小カットアルゴリズムを適用する。言い換えれば、管理対象サーバグルーピングモジュール９２０は、管理対象サーバ１３０を、コンテキスト情報収集モジュール９１０によって集められた通信情報に基づいてアプリケーショングループにグループ化する。

【０１５９】

ラベリングエンジン９３０は、管理対象サーバ情報を取得し、管理対象サーバ情報に少なくとも部分的に基づいて、管理対象サーバ１３０のラベルを判定する。ラベリングエンジン９３０は、ラベリング／ＣＣエンジンと類似しているが、構成済み特性を判定することはない。１つの実施形態において、ラベリングエンジン９３０は、アプリケーショングループ内の管理対象サーバ１３０に関連付けるようにグループレベルラベルセット（つまり、１または複数のグループレベルラベル）を判定する。１つの実施形態において、グループレベルラベルセットは、管理対象サーバ１３０の環境、アプリケーション、およびロケーションに対応する次元を伴うラベルを含む。ラベルは、表１および管理ドメイン全体管理ポリシ３３０に関してさらに記述される。

【０１６０】

ラベリングエンジン９３０は、管理対象サーバ１３０に関連付けられているＷｅｂアドレス（たとえば、ＩＰアドレスおよび／またはＵＲＬ）のロケーションに基づいて、管理対象サーバのロケーション次元の値を判定してよい。ラベリングエンジン９３０は、コンテキスト情報（および／またはコンテキスト情報から派生した情報）を使用する条件付きヒューリスティックに基づいて管理対象サーバのラベルの値を判定してよい。条件付きヒューリスティックは、管理者によって作成され得るか、または事前構成され得る。たとえば、条件付きヒューリスティックは、管理対象サーバ１３０が特定のクラウドサービス提供者によって提供されるか、または特定のデータセンタに位置する場合に、ラベリングエンジン９３０が、管理対象サーバの環境次元に特定の値を判定することを指定する。もう１つの例として、条件付きヒューリスティックは、管理対象サーバ１３０が特定のファイルもしくは処理（またはファイルもしくは処理の特定のセット）を含む場合に、ラベリングエンジン９３０が、管理対象サーバのアプリケーション次元に特定の値を判定することを指定する。ラベリングエンジン９３０は、管理者に、グループレベルラベルセットを示すか、または自動的に生成されたグループレベルラベルセットを確認するよう要求してよい。ラベリングエンジン９３０は、管理者によるインジケーションまたは訂正に応じて、グループレベルラベルセットを修正する。

【０１６１】

アプリケーショングループに適用可能なグループレベルラベルセットに加えて、ラベリングエンジン９３０は、アプリケーショングループ内の個々の管理対象サーバ１３０のロールラベル（つまり、ロール次元を伴うラベル）を判定する。１つの実施形態において、ラベリングエンジン９３０は、ハードウェアリソース、サービス情報、またはその他の管理対象サーバ情報に基づいて、管理対象サーバ１３０のロールラベルを判定する。たとえば、ラベリングエンジン９３０は、合計使用可能メモリがしきい値を超える場合、管理対象サーバ１３０がデータベースであると判定する。もう１つの例として、ラベリングエンジン９３０は、ネットワークインタフェースの数に基づいて、管理対象サーバ１３０がロードバランサであると判定する。１つの実施形態において、ラベリングエンジン９３０は

、管理対象サーバ１３０上で実行中の処理に関する情報を管理対象サーバ情報から取得し、処理に基づいてロール次元値を判定する。表３は、処理とロール次元値との間の例示のマッピングを示す。

【０１６２】

【表３】

処理	ロール次元値
Ｐｏｓｔｇｒｅｓ	データベース
Ｏｒａｃｌｅ	データベース
ＳＱＬＳｅｒｖｅｒ	データベース
Ａｐａｃｈｅ	ＨＴＴＰサーバ
ＮＧＩＮＸ	ＨＴＴＰサーバ
ＨＡＰｒｏｘｙ	ロードバランサ

表３　処理とロール次元値との間のマッピング

【０１６３】

フロー処理モジュール９４０は、管理ドメイン１５０内のアクタの間の通信情報を取得し、通信情報に対応するアクセス制御ルールを生成する。１つの実施形態において、フロー処理モジュール９４０は、アクセス制御ルールによって許可されていない通信を識別し、通信を許可するアクセス制御ルールを生成する。アクセス制御ルールを生成するため、フロー処理モジュール９４０は、通信を生成するサービス、サービスの提供者、およびサービスの消費者を識別する。フロー処理モジュール９４０は、識別されたサービスを示すサービス部分、識別された提供者を示すＰＢ部分、および識別された消費者を示すＵＢ部分を備えるアクセス制御ルールを生成する。１つの実施形態において、フロー処理モジュール９４０は、管理ドメイン１５０には異常または悪意のある通信がないと仮定し、それに応じて、管理ドメイン１５０に存在する任意の通信を許可するアクセス制御ルールを生成する。

【０１６４】

１つの実施形態において、フロー処理モジュール９４０は、管理対象サーバ１３０のグループレベルラベルセットおよびロールラベルに基づいて、アクセス制御ルールを生成する。フロー処理モジュール９４０は、ターゲットアクセス制御ルールを判定する。たとえば、ターゲットアクセス制御ルールは、（たとえば、管理対象サーバグルーピングモジュール９２０によって生成されたグラフに対応する表示されたグラフの特定の境界を示すことによって）ＧＵＩを通じて管理者によって指定される。生成されたアクセス制御ルールは、サービス、サービスの提供者としての第１の管理対象サーバ１３０、およびサービスの消費者としての第２の管理対象サーバ１３０を指定する。フロー処理モジュール９４０は、ラベリングエンジン９３０によって生成された第１および第２の管理対象サーバ１３０のロールラベルおよびグループレベルラベルセットを識別する。次いで、フロー処理モジュール９４０は、（表示されたグラフの特定のエッジに対応する）指定されたサービスを使用して、管理対象サーバ１３０のその他の消費者－提供者ペアに適用する追加のアクセス制御ルールを生成する。サービスの提供者である識別された管理対象サーバ１３０は、第１の管理対象サーバ１３０のグループレベルラベルセットおよびロールラベルと一致するグループレベルラベルセットおよびロールラベルを有する。サービスの消費者である識別された管理対象サーバ１３０は、第２の管理対象サーバ１３０のグループレベルラベルセットおよびロールラベルと一致するグループレベルラベルセットおよびロールラベルを有する。あるいは、または管理対象サーバ１３０の識別された消費者－提供者ペアをカバーする追加のアクセス制御ルールを生成することに加えて、フロー処理モジュール９４０は、管理対象サーバ１３０の識別された消費者－提供者ペアを含むようにターゲットアクセス制御ルールを拡大する。たとえば、拡大されたアクセス制御ルールのＰＢ部分およびＵＢ部分は、特定の管理対象サーバ１３０の識別子に関してではなく、ロールラベルお

よびグループレベルラベルセットを含むラベルセットに関して指定される。

【０１６５】

１つの実施形態において、フロー処理モジュール９４０は、第１の管理対象サーバ１３０と、別のアクタ（たとえば、非管理対象デバイス１４０、管理ドメイン１５０の外側の外部デバイス）との間の通信を制御するアクセス制御ルールを生成する。フロー処理モジュール９４０は、サービス、第１の管理対象サーバ１３０、およびその他のアクタを指定する既存のアクセス制御ルールを識別する。フロー処理モジュール９４０は、第１の管理対象サーバ１３０と同じラベル（ロールラベルおよびグループレベルラベルセットを含む）を有する第２の管理対象サーバ１３０を識別する。第１および第２の管理対象サーバ１３０は、共に指定されたサービスの消費者であるか、または共に指定されたサービスの提供者であるかのいずれかである。フロー処理モジュール９４０は、第２の管理対象サーバ１３０と他のアクタとの間のサービス関連の通信を許可する別のアクセス制御ルールを生成する。あるいは、または追加のアクセス制御ルールを生成することに加えて、フロー処理モジュール９４０は、第１の管理対象サーバ１３０の識別子に関してではなく、第１の管理対象サーバのラベルセット（ロールラベルおよびグループレベルラベルセットを含む）に関してアクセス制御ルールのＰＢ部分またはＵＢ部分を指定することによって、既存のアクセス制御ルールを拡大する。

【０１６６】

１つの実施形態において、フロー処理モジュール９４０は、管理ドメイン１５０内の管理対象サーバ１３０のサーバ状態を修正するルールを生成する。サーバ状態は、どの程度まで管理モジュール１３２がアクセス制御ルールを実施するかを判定する。実施状態において、管理モジュール１３２は、アクセス制御ルールに従って無許可である通信をブロックまたは終了する。たとえば、純粋なホワイトリストポリシにおいて、管理モジュール１３２は、少なくとも１つのアクセス制御ルールと一致しない通信をブロックまたは終了する。サーバ状態はまた、ビルド状態およびテスト状態を含み、ここで管理モジュール１３２は、通信がアクセス制御ルールによって許可されない場合であっても、通信を認可する。ビルド状態またはテスト状態を始めるため、フロー処理モジュール９４０は、ワイルドカードを指定するＰＢ、ＵＢ、およびサービス部分を伴う無制限のアクセス制御ルールを生成する。言い換えれば、さまざまなサービスまたはアクタへのアクセス制御ルールの適用可能性に全く制限がないので、無制限のアクセス制御ルールは、すべての通信を許可する。ビルド状態またはテスト状態から実施状態に移行するため、フロー処理モジュール９４０は、無制限のアクセス制御ルールを除去する。

【０１６７】

アラート処理モジュール９５０は、管理対象サーバ１３０からアラートを取得し、アラートを処理して、（適切な場合）取得したアラートに基づいてアクセス制御ルールを生成する。１つの実施形態において、アラート処理モジュール９５０は、管理対象サーバ１３０が実施状態またはテスト状態にある場合、管理対象サーバ１３０からアラートを取得する。管理対象サーバ１３０がビルド状態にある場合、アラート処理モジュール９５０は、管理対象サーバ１３０に、アクセス制御ルールによって許可されない通信を検出したことに応じてアラートを生成しないように命令する。管理対象サーバ１３０がテスト状態にある場合、アラート生成モジュール４３０は、たとえ管理モジュール１３２が無許可のトラフィックをブロックするためのアクセス制御ルールを強行していなくても、無許可のトラフィックを示すアラートを生成する。

【０１６８】

アラートに応じてアクセス制御ルールを生成する前に、アラート処理モジュール９５０は、アラートに関連する取得したコンテキスト情報を使用して、アラートをトリガした通信を分類する。コンテキスト情報は、通信を記述する通信情報、通信を送信もしくは受信している管理対象サーバ１３０に関する管理対象サーバ情報、または管理ドメイン情報を含む。アラートが外部デバイスとの通信に応じて生成される場合、コンテキスト情報は、外部デバイス情報を含む。アラートが非管理対象デバイス１４０との通信に応じて生成さ

れる場合、コンテキスト情報は、非管理対象デバイス情報を含む。アラート処理モジュール９５０は、取得したコンテキスト情報に基づいて、アラートをトリガする通信を正当なもの、または悪意あるものとして分類する。たとえば、外部デバイス情報が、外部デバイスは悪意あるものであることを示す場合、通信は悪意あるものとして分類される。

【０１６９】

１つの実施形態において、アラート処理モジュール９５０は、通信を始めるアクタが異常なアクティビティに関連付けられていることを管理ドメイン情報が示す場合、通信を悪意あるものとして分類する。コンテキスト情報収集モジュール９１０は、共通のアクタ、処理、ポート、またはプロトコルのような、共通の特性に関連付けられているアラートの数を要約する管理ドメイン情報を生成してよい。共通の特性に関連付けられているアラートの数がしきい値数を超える場合、コンテキスト情報収集モジュール９１０は、通信を悪意あるものとして分類する。たとえば、管理対象サーバ１３０によって始められたトラフィックに応じて生成されたアラートの数がしきい値数を超える場合、管理対象サーバ１３０によって始められた通信は悪意あるものとして分類される。

【０１７０】

アラート処理モジュール９５０は、取得した管理ドメイン情報が進行性の感染の存在を示すことを判定してよい。進行性の感性において、悪意あるソフトウェアは、時間の経過に伴って管理ドメイン１５０にわたり拡散する。管理ドメイン情報が、第１の管理対象サーバ１３０からのアラートの数がしきい値を超えることを示す場合、および第１の管理対象サーバ１３０と通信する第２の管理対象サーバ１３０がアラートの生成を開始する場合、アラート処理モジュール９５０は、アラートが進行性の感染に関連付けられていることを判定する。したがって、アラート処理モジュール９５０は、アラートをトリガする通信を悪意あるものとして分類する。

【０１７１】

あるいは、またはコンテキスト情報に従ってアラートを分類することに加えて、アラート処理モジュール９５０は、アラートを受信したことに応じて管理者に通知する。管理者に通知することは、アラートをトリガする通信に関連するコンテキスト情報をレポートすることを含んでよい。アラート処理モジュール９５０は、対応する通信が正当なもの、または悪意あるものであるかどうかを示す分類を管理者から受信してよい。

【０１７２】

アラート処理モジュール９５０は、対応する通信の分類に従ってアラートを処理する。対応する通信が悪意あるものとして分類されている場合、アラート処理モジュール９５０は、対応する通信を許可するアクセス制御ルールを生成しない。一部の実施形態において、アラート処理モジュール９５０は、アラートをトリガする通信を開始した発信元アクタとの通信を停止するよう管理対象サーバ１３０に命令する。言い換えれば、発信元アクタは通信遮断される。アラート処理モジュール９５０は、対応する通信を悪意あるものとして分類したことに応じて、アラートについて管理者に通知する。あるいは、または加えて、アラート処理モジュール９５０は、アラートの分類にはかかわりなく、アラートについて管理者に通知する。対応する通信が正当なものとして分類されている場合、アラート処理モジュール９５０は、通信を許可するアクセス制御ルールを生成するようフロー処理モジュール９４０に命令してよい。一部の実施形態において、アラート処理モジュール９５０は、アクセス制御ルールをアクセス制御ルールのセット３３５に追加する前に、アクセス制御ルールの承認を管理者に要求してよい。

【０１７３】

アクセス制御ルール（ＡＣＲ）作成インタフェース９６０は、コンテキスト情報、アプリケーショングループ、管理対象サーバ１３０に割り当てられているラベルセット（たとえば、ロールラベルおよび／またはグループレベルラベルセットを含む）、ならびにアクセス制御ルールを検討するためのインタフェースを管理者に提供する。ＡＣＲ作成インタフェース９６０は、管理対象サーバ１３０の訂正済みのアプリケーショングループを管理者から受信してよい。これに応答して、管理対象サーバグルーピングモジュール９２０は

、管理対象サーバのアプリケーショングループを、訂正済みのアプリケーショングループと一致するように更新する。加えて、ラベリングエンジン９３０は、管理対象サーバ１３０のグループレベルラベルセットを、新たに選択されたアプリケーショングループのグループレベルラベルセットと一致するように更新する。ＡＣＲ作成インタフェース９６０は、管理対象サーバ１３０の訂正済みのラベルセットを受信してよく、ラベリングエンジン９３０は、訂正に従って管理対象サーバのラベルセットを更新する。管理者がアプリケーションのグループレベルラベルセットを修正したことに応じて、ラベリングエンジン９３０は、アプリケーショングループ内の他の管理対象サーバ１３０のグループレベルラベルセットを、訂正済みのグループレベルラベルセットと一致するように修正する。

【０１７４】

ＡＣＲ作成インタフェース９６０は、（たとえば、表示されるグラフの特定のエッジを管理者が示すことによって）ターゲットアクセス制御ルールを管理者から受信してよい。たとえば、管理者のターゲットアクセス制御ルールは、サービス、サービスの提供者、およびサービスの消費者を示す。フロー処理モジュール９４０は、管理者の命令に従ってアクセス制御ルールを生成し、場合によっては、サービスならびに提供者および消費者のラベルセットに基づいて、追加のアクセス制御ルールを生成する（または、生成されたアクセス制御ルールを拡大する）。

【０１７５】

ＡＣＲ作成インタフェース９６０は、アラート処理モジュール９５０によって取得されたアラートについて管理者に通知してよい。ＡＣＲ作成インタフェース９６０は、アラートをトリガする通信の分類を受信してよく、フロー処理モジュール９４０は、分類に従ってアクセス制御ルールを生成してよい。１つの実施形態において、ＡＣＲ作成インタフェース９６０は、フロー処理モジュール９４０によって自動的に生成されたアクセス制御ルールを管理者に提示する。ＡＣＲ作成インタフェース９６０は、管理者の承認、修正、または自動生成のアクセス制御ルールの拒否を受信してよい。フロー処理モジュール９４０は、管理者から承認または修正を受信したことに応じて、アクセス制御ルールのセット３３５に、（場合によっては修正された）自動生成のアクセス制御ルールを追加する。

【０１７６】

＜アクセス制御ルールの生成＞

図１０は、１つの実施形態に従った、複数の管理対象サーバ１３０の間の通信を許可するアクセス制御ルールを生成する方法１０００を示すフローチャートである。その他の実施形態は、異なる順序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、ステップの一部または全部は、図１に図示されているエンティティ以外のエンティティによって実行されてもよい。

【０１７７】

ステップ１０１０において、複数の管理対象サーバ１３０の間の過去の通信を記述する通信情報が取得される。たとえば、通信情報は、管理対象サーバ１３０の各ペアの間で転送されたデータの日次量を記述する。ステップ１０１０は、たとえば、コンテキスト情報収集モジュール９１０によって実行される。

【０１７８】

ステップ１０２０において、管理対象サーバ１３０のサブセットは、取得された通信情報に基づいて複数の管理対象サーバ１３０をグループ化することによって、複数の管理対象サーバ１３０から識別される。たとえば、サブセットは、管理対象サーバ１３０を表すノード、および管理対象サーバ１３０のペアの間で転送されたデータの日次量を反映する値を有するエッジによるグラフに、Ｋ平均クラスタリングアルゴリズムを適用することによって判定される。ステップ１０２０は、たとえば、管理対象サーバグルーピングモジュール９２０によって実行される。

【０１７９】

ステップ１０３０において、グループレベルラベルセットは、管理対象サーバ１３０のサブセットに関連付けるように判定される。たとえば、ラベルセットは、アプリケーショ

ンラベル（たとえば、＜アプリケーション、人的資源＞）、ロケーションラベル（たとえば、＜ロケーション、北米＞）、および環境ラベル（たとえば、＜Ｅｎｖｉｒｏｎｍｅｎｔ，Ｐｒｏｄｕｃｔｉｏｎ＞）を含む。ステップ１０３０は、たとえば、ラベリングエンジン９３０によって実行される。

【０１８０】

ステップ１０４０において、ロールラベルは、管理対象サーバのサブセット内の管理対象サーバ１３０に対して判定される。管理対象サーバ１３０は、１つのロールラベルに関連付けられている。たとえば、それぞれの管理対象サーバ１３０で実行中の処理に基づいて、第１の管理対象サーバ１３０は、「データベース」値を有するロールラベルに関連付けられており、第２の管理対象サーバ１３０は、「Ｗｅｂサーバ」値を有するロールラベルに関連付けられている。ステップ１０４０は、たとえば、ラベリングエンジン９３０によって実行される。

【０１８１】

ステップ１０５０において、管理対象サーバ１３０のサブセットの第１の管理対象サーバと第２の管理対象サーバ１３０との間の通信を許可するアクセス制御ルールは、グループレベルラベルセットおよびロールラベルに基づいて生成される。第２のサーバ１３０は、管理対象サーバ１３０のサブセットの一部、または管理対象サーバ１３０の別のサブセットの一部であってよい。たとえば、アクセス制御ルールのＰＢ部分は、第１の管理対象サーバ１３０が「ｓｓｈｄ」（ｓｓｈデーモン）サービスの提供者であることを示し、アクセス制御ルールのＵＢ部分は、第２の管理対象サーバ１３０が「ｓｓｈｄ」サービスの消費者であることを示す。ステップ１０５０は、たとえば、フロー処理モジュール９４０によって実行される。

【０１８２】

ステップ１０６０において、アクセス制御ルールは、アクセス制御ルールのセット３３５の一部として記憶される。ステップ１０６０は、たとえば、フロー処理モジュール９４０によって実行される。

【０１８３】

ステップ１０７０において、方法は終了する。後に、ポリシエンジンモジュール３４０は、管理ドメイン全体管理ポリシ３３０への変更を処理する。処理は、結果として、アクセス制御ルールを１または複数の関連管理対象サーバ１３０の機能レベル命令に変換して、アクセス制御ルールを実施すること、および機能レベル命令を関連管理対象サーバ１３０に送信することをもたらす。

【０１８４】

あるいは、またはアクセス制御ルールを生成すること加えて、本明細書において説明される方法は、管理ドメイン全体管理ポリシ３３０の一部としてさまざまなルール機能を伴う他のルールの作成を容易にするために使用されてよい。一部のルールは、サービスの提供者およびサービスの消費者を共に指定する。そのような例示のルールの１つは、サービスのための通信と共に使用されるプロトコル、暗号化、またはチャネルを指定するセキュア接続性機能を有する。これらのルールに対して、グローバルマネージャ１２０は、ターゲットルールを取得し、提供者を記述するラベルセット（たとえば、ロールラベルおよび／またはグループレベルラベルを含む）および消費者を記述するラベルセットを識別する。次いで、グローバルマネージャ１２０は、識別されたラベルセットのペアと一致するそれぞれのラベルセットのペアを伴う提供者－消費者ペアに適用する追加のルールを生成する（または既存のルールを拡大する）。追加の（または拡大された）ルールは、同じサービスに適用し、ターゲットルールと同じ機能プロファイル（たとえば、暗号化プロトコル、通信プロトコルタイプ）を有する。

【０１８５】

一部のルールは、サービスの提供者のみ、またはサービスの消費者のみを指定する。消費者または提供者のうちの１つを指定する例示のルールは、記憶済みデータ暗号化、ディスク使用、周辺機器使用、またはプロセッサ使用を調整するルール機能を有してよい。こ

れらのルールに対して、グローバルマネージャ１２０は、ターゲットルールを取得し、提供者または消費者に対応するラベルセットを識別する。提供者を指定するルールに対して、グローバルマネージャ１２０は、識別されたラベルセットと一致するラベルセットを有するサービスの提供者に適用する追加のルールを生成する（または既存のルールを拡大する）。消費者を指定するルールに対して、グローバルマネージャ１２０は、識別されたラベルセットと一致するラベルセットを有するサービスの消費者に適用する追加のルールを生成する（または既存のルールを拡大する）。追加の（または拡大された）ルールは、同じサービスに適用し、ターゲットルールと同じ機能プロファイル（たとえば、暗号化プロトコル、リソース使用制限）を有する。

【０１８６】

一部のルールは、管理対象サーバ１３０によって提供されたサービス、または管理対象サーバ１３０によって消費されたサービスであるかにはかかわりなく、管理対象サーバ１３０に影響を及ぼす。例示のルールは、どの処理が管理対象サーバ１３０上で実行してよいか、汎用ディスク暗号化設定、またはいつセキュリティ分析のためにネットワークパケットを取得するかを調整する。グローバルマネージャ１２０は、ターゲットルールを取得し、ターゲットルールからラベルセットを識別し、識別されたラベルセットと一致するラベルセットを伴う追加の管理対象サーバ１３０に適用するルールを生成する（または拡大する）。追加の（または拡大された）ルールは、ターゲットルールと同じ機能プロファイルを有する。この処理は、生成されたルールがサービスを指定しないことを除いては、前に記述されたものと類似している。

【０１８７】

一部の実施形態において、フロー処理モジュール９４０は、その他のルール（たとえば、アクセス制御ルール）に使用されるものとは異なるラベルのクラスに基づいて、ルールを生成する。そのようなルールは、管理対象サーバ１３０によって提供されるかまたは使用されるサービスに影響を及ぼし、管理対象サーバの１または複数の代替もしくは追加のラベルに基づいて生成されてよい。ラベリングエンジン９３０は、管理対象サーバ１３０の処理に適用する複数の処理固有のロールラベルを判定してよい。１つの実施形態において、フロー処理モジュール９４０は、サービスの提供者または消費者の代替のロールラベルに基づいて、ルールを生成する。代替のロールラベルは、ルールによって指定されたサービスを提供または消費するために管理対象サーバ１３０によって使用される１または複数の処理に関連付けられている処理固有のロールラベルである。

【０１８８】

＜管理対象サーバからのアラートの処理＞

図１１は、１つの実施形態に従った、１または複数のアクセス制御ルールを実施する管理対象サーバ１３０からのアラートを処理する方法１１００を示すフローチャートである。その他の実施形態は、異なる順序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、ステップの一部または全部は、図１に図示されているエンティティ以外のエンティティによって実行されてもよい。

【０１８９】

ステップ１１１０において、第２の管理対象サーバ１３０との通信に応じてアラートを生成するように構成されている第１の管理対象サーバ１３０から、アラートが取得される。アラートは、第１の管理対象サーバによって実施された１または複数のアクセス制御ルールが第１の管理対象サーバ１３０と第２の管理対象サーバ１３０との間の通信を許可しないことを判定する、第１の管理対象サーバ１３０に応じて生成される。

【０１９０】

ステップ１１２０において、第１の管理対象サーバ１３０の少なくとも１つ、第２の管理対象サーバ１３０、およびアラートに関連するコンテキスト情報が取得される。たとえば、コンテキスト情報は、第１の管理対象サーバ１３０が第２の管理対象サーバ１３０において接続するよう要求したポートの数を示す管理ドメイン情報であり、ここで第２の管理対象サーバ１３０はポートをリスンする処理を有していない。もう１つの例として、コ

ンテキスト情報は、第１の管理対象サーバ１３０と第２の管理対象サーバ１３０との間の通信の頻度を示す通信情報である。

【０１９１】

ステップ１１３０において、アラートに対応する通信は、正当なもの、または悪意あるものとして分類される。たとえば、管理ドメイン情報で識別されたポートの数がポートのしきい値数を超えたことに応じて、通信は悪意あるものとして分類される。もう１つの例として、通信の頻度が、サービスに関連付けられている通信の予想頻度のしきい値差を超えていないことに応じて、通信は正当なものとして分類される。

【０１９２】

ステップ１１４０において、通信が正当なものとして分類されるかどうかについて判定が実行される。通信が正当なものである場合、方法１１００は、ステップ１１５０に進む。通信が正当なものでない場合、方法１１００は、ステップ１１７０に進む。

【０１９３】

ステップ１１５０において、第１の管理対象サーバ１３０と第２の管理対象サーバ１３０との間の通信を認可するアクセス制御ルールが生成される。

【０１９４】

ステップ１１６０において、アクセス制御ルールは、アクセス制御ルールのセット３３５の一部として記憶される。

【０１９５】

ステップ１１７０において、管理者がアラートについて通知される。管理者にアラートについて通知することは、通信が正当なものとして分類される場合、アラートに対応する通信を許可するように生成されたアクセス制御ルールを承認するよう管理者に要求することを含んでよい。管理者に通知することはまた、通信が悪意あるものとして分類される場合、第１または第２の管理対象サーバ１３０を通信遮断するよう求めるプロンプトを管理者に表示することを含んでよい。

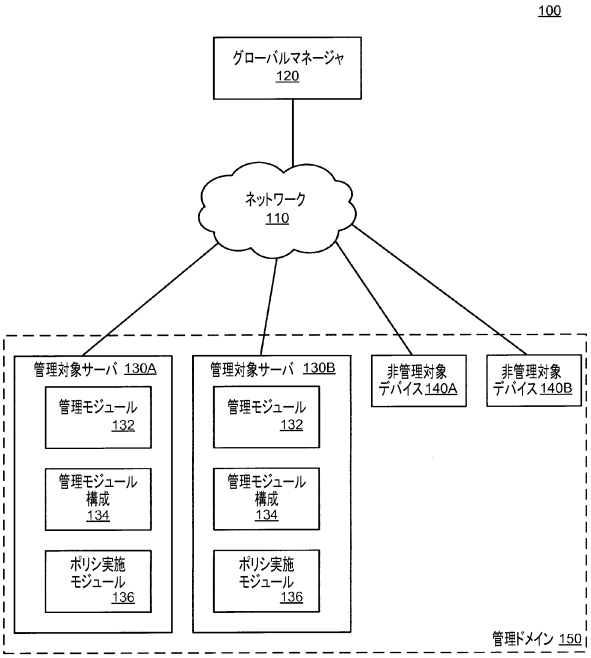
【０１９６】

ステップ１１８０において、方法は終了する。後に、ポリシエンジンモジュール３４０は、管理ドメイン全体管理ポリシ３３０への変更を処理する。処理は、結果として、アクセス制御ルールを１または複数の関連管理対象サーバ１３０の機能レベル命令に変換してアクセス制御ルールを実施すること、および機能レベル命令を関連管理対象サーバ１３０に送信することをもたらす。

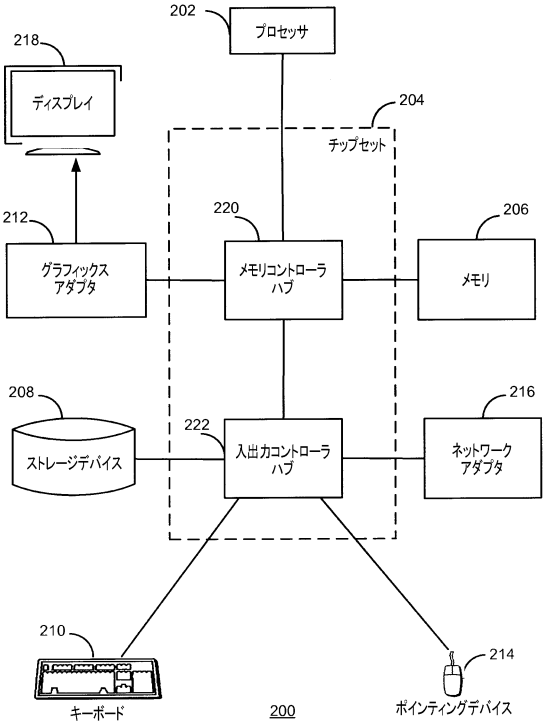
【０１９７】

上記の説明は、特定の実施形態の操作を示すために含まれており、本発明の範囲を限定することを意図されてはいない。本発明の範囲は、後段の特許請求の範囲によってのみ限定されるものとする。上記の説明から、当業者には、多くの変形が明らかとなるが、それらは本発明の精神および範囲により引き続き包含されるであろう。

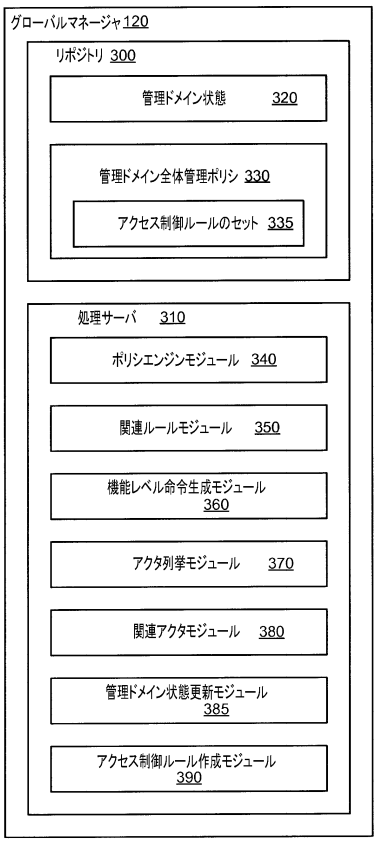
【図１】


100
グローバルマネージャ
120
ネットワーク
110
管理対象サーバ 130A
管理モジュール
132
管理モジュール
構成
134
ポリシ実施
モジュール
136
管理対象サーバ 130B
管理モジュール
132
管理モジュール
構成
134
ポリシ実施
モジュール
136
非管理対象
デバイス140A
非管理対象
デバイス140B
管理ドメイン 150

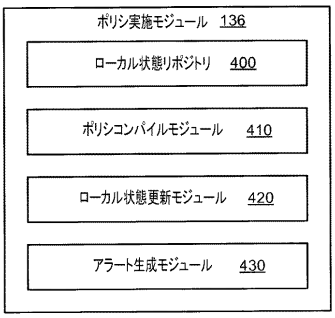
【図２】


202
プロセッサ
218
ディスプレイ
204
チップセット
212
220
206
グラフィックス
アダプタ
メモリコントローラ
ハブ
メモリ
208
222
216
ストレージデバイス
入出力コントローラ
ハブ
ネットワーク
アダプタ
210
214
キーボード
200
ポインティングデバイス

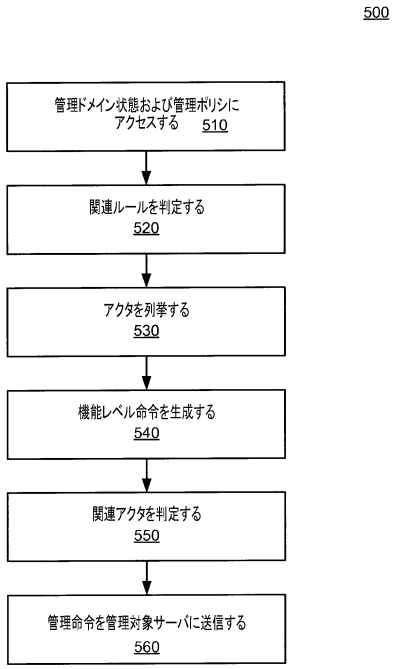
【図３】


グローバルマネージャ120
リポジトリ 300
管理ドメイン状態 320
管理ドメイン全体管理ポリシ 330
アクセス制御ルールのセット 335
処理サーバ 310
ポリシ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
アクタ列挙モジュール 370
関連アクタモジュール 380
管理ドメイン状態更新モジュール
385
アクセス制御ルール作成モジュール
390

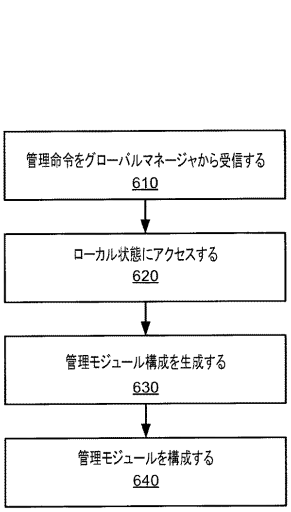
【図４】


ポリシ実施モジュール 136
ローカル状態リポジトリ 400
ポリシ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
アラート生成モジュール 430

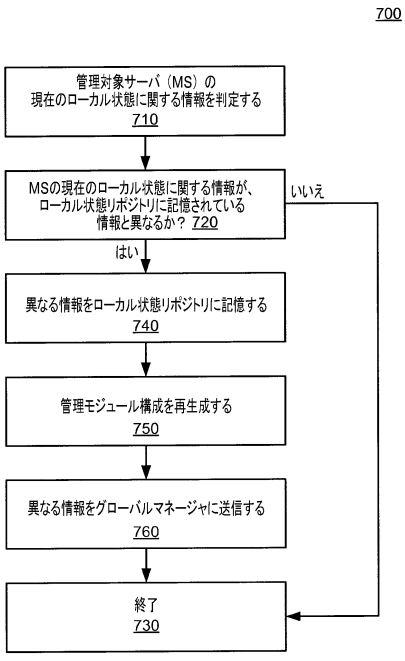
【図５】


500
管理ドメイン状態および管理ポリシにアクセスする 510
関連ルールを判定する 520
アクタを列挙する 530
機能レベル命令を生成する 540
関連アクタを判定する 550
管理命令を管理対象サーバに送信する 560

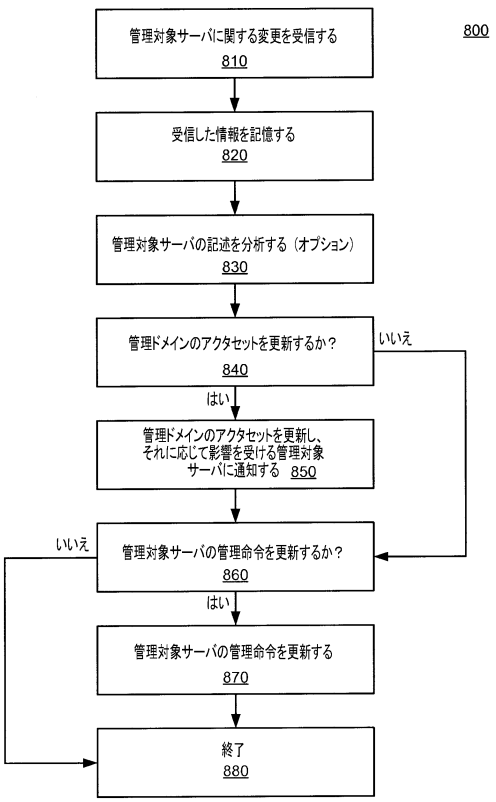
【図６】


600
管理命令をグローバルマネージャから受信する 610
ローカル状態にアクセスする 620
管理モジュール構成を生成する 630
管理モジュールを構成する 640

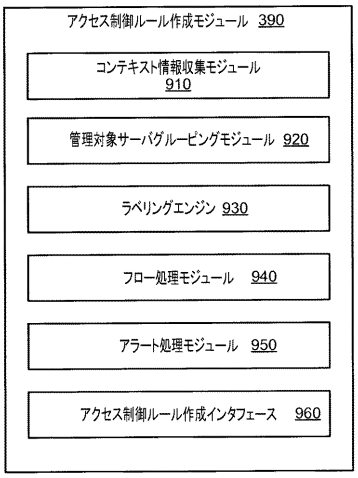
【図７】


700
管理対象サーバ（MS）の現在のローカル状態に関する情報を判定する 710
MSの現在のローカル状態に関する情報が、ローカル状態リポジトリに記憶されている情報と異なるか？ 720
いいえ
はい
異なる情報をローカル状態リポジトリに記憶する 740
管理モジュール構成を再生成する 750
異なる情報をグローバルマネージャに送信する 760
終了 730

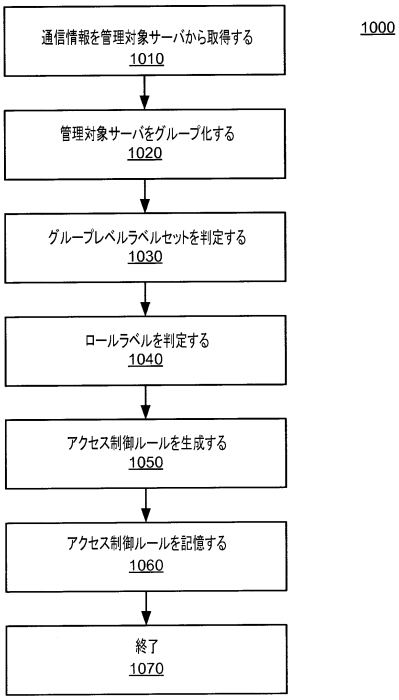
【図８】


800
管理対象サーバに関する変更を受信する 810
受信した情報を記憶する 820
管理対象サーバの記述を分析する（オプション）830
管理ドメインのアクタセットを更新するか？ 840
いいえ
はい
管理ドメインのアクタセットを更新し、それに応じて影響を受ける管理対象サーバに通知する 850
管理対象サーバの管理命令を更新するか？ 860
いいえ
はい
管理対象サーバの管理命令を更新する 870
終了 880

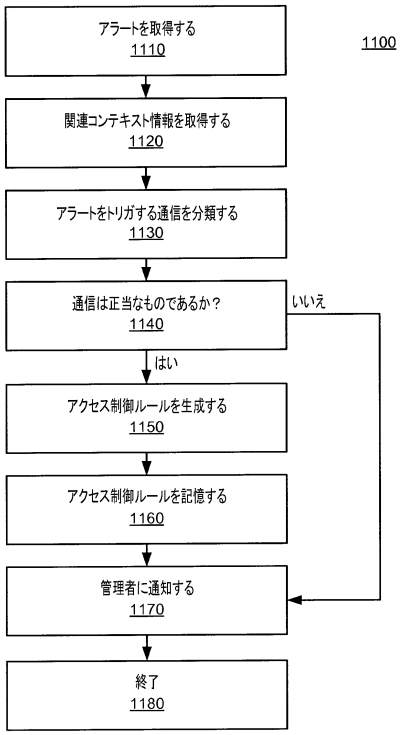
【図９】


アクセス制御ルール作成モジュール 390
コンテキスト情報収集モジュール 910
管理対象サーバグルーピングモジュール 920
ラベリングエンジン 930
フロー処理モジュール 940
アラート処理モジュール 950
アクセス制御ルール作成インタフェース 960

【図１０】


1000
通信情報を管理対象サーバから取得する 1010
管理対象サーバをグループ化する 1020
グループレベルラベルセットを判定する 1030
ロールラベルを判定する 1040
アクセス制御ルールを生成する 1050
アクセス制御ルールを記憶する 1060
終了 1070

【図１１】


1100
アラートを取得する 1110
関連コンテキスト情報を取得する 1120
アラートをトリガする通信を分類する 1130
通信は正当なものであるか？ 1140
いいえ
はい
アクセス制御ルールを生成する 1150
アクセス制御ルールを記憶する 1160
管理者に通知する 1170
終了 1180

フロントページの続き

(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　ロイ　エヌ．ナカシマ
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

審査官　速水　雄太

(56)参考文献　米国特許出願公開第２０１１／０２０９１９５（ＵＳ，Ａ１）
米国特許出願公開第２００４／０１９９７９２（ＵＳ，Ａ１）
古川諒，中江政行，小川隆一，権限集合の類似度を用いたアクセスルールのクラスタリングに基づくロール抽出方式，コンピュータセキュリティシンポジウム２００９　論文集　［第一分冊］，日本，社団法人情報処理学会，２００９年１０月１９日，第４６９－４７４頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　１２／２４