(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5813252号
(P5813252)
(45)発行日　平成27年11月17日(2015.11.17)　(24)登録日　平成27年10月2日(2015.10.2)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00 351Z
H04L 12/70 (2013.01)　　H04L 12/70 Z

請求項の数 17　(全 27 頁)

(21)出願番号　特願2014-550617(P2014-550617)
(86)(22)出願日　平成24年12月3日(2012.12.3)
(65)公表番号　特表2015-508538(P2015-508538A)
(43)公表日　平成27年3月19日(2015.3.19)
(86)国際出願番号　PCT/CN2012/085721
(87)国際公開番号　WO2014/085952
(87)国際公開日　平成26年6月12日(2014.6.12)
審査請求日　平成25年12月20日(2013.12.20)

(73)特許権者　504277388
▲ホア▼▲ウェイ▼技術有限公司
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル
(74)代理人　100146835
弁理士　佐伯　義文
(74)代理人　100140534
弁理士　木内　敬二
(72)発明者　▲劉▼　赫▲偉▼
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル
(72)発明者　史　云▲龍▼
中華人民共和国５１８１２９広東省深▲セン▼市龍岡区坂田華為本社ビル

最終頁に続く

(54)【発明の名称】ポリシー処理方法およびネットワークデバイス

(57)【特許請求の範囲】
【請求項１】
混合オーケストレータ、条件照合器、およびルール照合器を備えるネットワークデバイスであって、
前記混合オーケストレータが、前記ネットワークデバイス上で動作する複数のサービスアプリケーションに対応するすべてのサービスルールの条件を抽出するために、すべての前記サービスルールに対して混合オーケストレーションを遂行するように構成されており、各サービスルールが条件およびアクションを含み、前記混合オーケストレータが、前記抽出された条件を各特徴毎に分類することによって、同一の特徴に関する少なくとも１つの条件を有する少なくとも1つの条件セットを構成し、各サービスルールと前記条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成するように構成されており、
前記条件照合器が、前記混合オーケストレータによって構成された条件セットのそれぞれに、前記ネットワークデバイスが受け取ったネットワークデータパケットのパケット特徴情報を照合のために入力することによって、前記条件セット内のそれぞれの条件に対する条件照合を遂行し、成功裏に照合された条件を記録するのに用いられる条件照合の結果セットを出力するように構成されており、
前記ルール照合器が、前記条件照合の結果セットと、前記混合オーケストレータが生成した前記マッピング関係データとに従って、成功裏に照合されたサービスルールを求め、前記成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して

、前記成功裏に照合されたサービスルールに対応するアクションを実行させるように構成されているネットワークデバイス。
【請求項２】
前記混合オーケストレータが、
すべての前記サービスルールのそれぞれを、条件とアクションとに分割するように構成されたルール分割ユニットと、
前記ルール分割ユニットが分割することによって得られた前記条件を抽出し複製条件を除去するように構成された、複製条件フィルタリング/除去ユニットと、
少なくとも1つのタイプの条件セットを取得するために、前記複製条件フィルタリング/除去ユニットによって前記複製条件が除去された後に残った条件を分類するように構成されている条件分類ユニットと、
各サービスルールと前記条件セットの中の1つの条件との間のマッピング関係を記録するための前記マッピング関係データを生成するように構成されているマッピングユニットと
を特に備える、請求項1に記載のネットワークデバイス。
【請求項３】
前記マッピングユニットが、各サービスルールと前記条件セットの中の1つの条件との間の前記マッピング関係を確立するために、前記条件セットの中の各条件を、前記条件を含むすべてのサービスルールに対応付け、前記マッピング関係を記録するためのマッピング関係データを生成するように特に構成されている、あるいは、前記マッピングユニットは、前記ルール分割ユニットがすべての前記サービスルールのそれぞれを条件とアクションに分割するとき、各サービスルールと前記サービスルールの前記条件との間のマッピング関係を記録し、前記複製条件フィルタリング/除去ユニットによって前記複製条件が除去された後に、前記条件セットの中の各条件が、前記条件を含むすべてのサービスルールに対応付けられるように、前記記録されたマッピング関係を調整し、前記調整されたマッピング関係を記録するためのマッピング関係データを生成するように特に構成されている、請求項2に記載のネットワークデバイス。
【請求項４】
前記混合オーケストレータが、前記条件分類ユニットによる統一フォーマットへの分類によって形成されたすべてのタイプの条件セットのそれぞれを編集するように構成された編集ユニットをさらに備え、前記統一フォーマットが前記条件照合器によってサポートされているフォーマットであり、前記条件照合器が、前記編集ユニットによって編集された前記統一フォーマットの前記条件セットに従って、前記ネットワークデバイスが受け取った前記ネットワークデータパケットの前記パケット特徴情報に対する条件照合を遂行し、前記条件照合の結果セットを出力するように特に構成されている請求項2または3に記載のネットワークデバイス。
【請求項５】
前記条件照合器が、
前記ネットワークデバイスが受け取った前記ネットワークデータパケットの前記パケット特徴情報を、条件セットのそれぞれの中の前記条件と照合し、成功裏に照合された条件の識別子を、前記条件照合の結果セットの中に記録する
ように特に構成されている請求項1から4のいずれか一項に記載のネットワークデバイス。
【請求項６】
前記ネットワークデータパケットの前記パケット特徴情報を収集するために、前記ネットワークデバイスが受け取った前記ネットワークデータパケットを検査するように構成されたインスペクタをさらに備え、前記条件照合器が、前記混合オーケストレータによって構成された条件セットのそれぞれに従って、前記インスペクタが収集した前記ネットワークデータパケットの前記パケット特徴情報に対する条件照合を遂行し、前記条件照合の結果セットを出力するように特に構成されている請求項5に記載のネットワークデバイス。
【請求項７】

前記インスペクタが、複数のパケット処理ユニットを備え、前記複数のパケット処理ユニットが、前記複数のサービスアプリケーションに必要なすべてのパケット特徴情報を、前記ネットワークデータパケットから重複することなく独立して収集し取得するように構成されている請求項6に記載のネットワークデバイス。

【請求項８】

前記条件照合器が、前記複数の処理ユニットに分散するやり方で配置されている請求項7に記載のネットワークデバイス。

【請求項９】

すべての前記サービスルールの中で、少なくとも1つのサービスルールが、複数の条件を含むサービスルールである複合ルールであり、

前記混合オーケストレータが、前記複合ルールの中の前記条件間の論理的関係を記録するようにさらに構成されており、

前記ルール照合器が、前記条件照合の結果セットと、前記混合オーケストレータが記録した前記マッピング関係と、前記条件間の前記論理的関係とに従って、成功裏に照合されたサービスルールを求め、前記成功裏に照合されたサービスルールが属するサービスアプリケーションを呼び出して、前記成功裏に照合されたサービスルールに対応するアクションを実行させるように、または、前記成功裏に照合されたサービスルールに対応するサービスアプリケーションに、ルールがヒットしたとのメッセージを送って、前記サービスアプリケーションが前記成功裏に照合されたサービスルールに対応するアクションを前記ルールがヒットしたとのメッセージに従って実行させるように特に構成されている、

請求項1から8のいずれか一項に記載のネットワークデバイス。

【請求項１０】

複合サービスポリシーの処理方法であって、

複数のサービスアプリケーションに対応するすべてのサービスルールの条件を抽出するために、条件およびアクションをそれぞれが含むすべての前記サービスルールに対して混合オーケストレーションを遂行し、前記抽出された条件を各特徴毎に分類することによって、同一の特徴に関する少なくとも１つの条件を有する少なくとも1つの条件セットを構成し、各サービスルールと前記条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成するステップと、

それぞれの構成された条件セットに、受け取ったネットワークデータパケットのパケット特徴情報を照合のために入力することによって、前記条件セット内のそれぞれの条件に対する条件照合を遂行し、成功裏に照合された条件を記録するのに用いられる条件照合の結果セットを出力するステップと、

前記条件照合の結果セットと、前記生成されたマッピング関係データとに従って、成功裏に照合されたサービスルールを求め、前記成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、前記成功裏に照合されたサービスルールに対応するアクションを実行させるステップと

を含む、方法。

【請求項１１】

複数のサービスアプリケーションに対応するすべてのサービスルールに対する混合オーケストレーションを遂行する前記ステップが、

すべての前記サービスルールのそれぞれを条件とアクションに分割し、各サービスルールと、前記サービスルールの中の前記条件との間のマッピング関係を記録するためのマッピング関係データを生成するステップと、

分割することによって得られた前記条件を抽出し、複製条件を除去するステップと、

少なくとも1つのタイプの条件セットを取得するために、前記複製条件が除去された後に残っている条件を分類するステップと、

前記条件セットの中の条件と各サービスルールの間の前記マッピング関係データを取得するために、前記条件セットの中の各条件が、前記条件を含むすべてのサービスルールに対応付けられるように、前記マッピング関係データを調整するステップと

を含む請求項10に記載の方法。
【請求項１２】
複数のサービスアプリケーションに対応するすべてのサービスルールに対する混合オーケストレーションを遂行する前記ステップが、
すべての前記サービスルールのそれぞれを、条件とアクションに分割するステップと、
分割することによって得られた前記条件を抽出し、複製条件を除去するステップと、
少なくとも1つのタイプの条件セットを取得するために、前記複製条件が除去された後に残っている条件を分類するステップと、
前記条件セットの中の条件と各サービスルールの間の前記マッピング関係データを取得するために、前記条件セットの中の各条件を、前記条件を含むすべてのサービスルールに対応付けるステップと
を含む請求項10に記載の方法。
【請求項１３】
それぞれの構成された条件セットに従って、受け取ったネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し条件照合の結果セットを出力する前記ステップが、
前記複数のサービスアプリケーションが必要とするパケット特徴情報をすべて取得するために、前記受け取ったネットワークデータパケットに対してパケット検査を遂行するステップと、
前記抽出されたパケット特徴情報を条件セットのそれぞれの前記条件と照合し、成功裏に照合された条件の識別子を、前記条件照合の結果セットの中に記録するステップと
を含む請求項10から12のいずれか一項に記載の方法。
【請求項１４】
すべての前記サービスルールの中で、少なくとも1つのサービスルールが、複数の条件を含むサービスルールである複合ルールであり、
前記方法が、すべての前記サービスルールのそれぞれを条件とアクションに分割する前記ステップの後に、前記複合ルールの中の前記条件間の論理的関係を記録するステップをさらに含み、
前記条件照合の結果セットと、前記生成されたマッピング関係データとに従って、成功裏に照合されたサービスルールを求める前記ステップが、前記条件照合の結果セットと、前記マッピング関係と、前記条件間の前記論理的関係とに従って、成功裏に照合されたサービスルールを求め、前記成功裏に照合されたサービスルールが属するサービスアプリケーションを呼び出して、対応するアクションを実行させるステップとを特に含む、
請求項10から13のいずれか一項に記載の方法。
【請求項１５】
前記成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、前記成功裏に照合されたサービスルールに対応するアクションを実行させる前記ステップが、
前記成功裏に照合されたサービスルールが属するサービスアプリケーションを呼び出して、前記成功裏に照合されたサービスルールに対応するアクションを実行させるステップ、または、前記成功裏に照合されたサービスルールに対応するサービスアプリケーションに、ルールがヒットしたとのメッセージを送って、前記サービスアプリケーションが前記成功裏に照合されたサービスルールに対応するアクションを前記ルールがヒットしたとのメッセージに従って実行させるステップ
を含む、請求項10から13のいずれか一項に記載の方法。
【請求項１６】
プロセッサおよびメモリを備えるネットワークデバイスであって、前記プロセッサと前記メモリがバスによって接続されており、前記メモリが、実行可能プログラムコードを格納するように構成されており、前記プロセッサが、前記メモリの中に格納されている前記実行可能プログラムコードを読み取り、前記実行可能プログラムコードに対応するプログ

ラムを実行して、
複数のサービスアプリケーションに対応するすべてのサービスルールの条件を抽出するために、条件およびアクションをそれぞれが含むすべての前記サービスルールに対して混合オーケストレーションを遂行し、前記抽出された条件を各特徴毎に分類することによって、同一の特徴に関する少なくとも１つの条件を有する少なくとも1つの条件セットを構成し、各サービスルールと前記条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成し、
それぞれの構成された条件セットに、受け取ったネットワークデータパケットのパケット特徴情報を照合のために入力することによって、前記条件セット内のそれぞれの条件に対する条件照合を遂行して、成功裏に照合された条件を記録するのに用いられる条件照合の結果セットを出力し、
前記条件照合の結果セットと、前記生成されたマッピング関係データとに従って、成功裏に照合されたサービスルールを求め、前記成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、前記成功裏に照合されたサービスルールに対応するアクションを実行させる
ように構成されているネットワークデバイス。
【請求項１７】
格納している動作を含んだ非一時的コンピュータ可読媒体であって、前記動作は少なくとも1つの処理ユニットによって処理されたとき、システムに、
複数のサービスアプリケーションに対応するすべてのサービスルールの条件を抽出するために、条件およびアクションをそれぞれが含むすべての前記サービスルールに対して混合オーケストレーションを遂行し、前記抽出された条件を各特徴毎に分類することによって、同一の特徴に関する少なくとも１つの条件を有する少なくとも1つの条件セットを構成し、各サービスルールと前記条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成する動作と、
それぞれの構成された条件セットに、受け取ったネットワークデータパケットのパケット特徴情報を照合のために入力することによって、前記条件セット内のそれぞれの条件に対する条件照合を遂行し、条件照合の結果セットを出力する動作であって、前記条件照合の結果セットが、成功裏に照合された条件を記録するのに用いられる、動作と、
前記条件照合の結果セットと、前記生成されたマッピング関係データとに従って、成功裏に照合されたサービスルールを求め、前記成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、前記成功裏に照合されたサービスルールに対応するアクションを実行させる動作とを遂行させる、
非一時的コンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信技術の分野に関し、詳細には、ポリシー処理方法およびネットワークデバイスに関する。
【背景技術】
【０００２】
通信システムでは、ポリシー制御は、種々のコアネットワークデバイス(ルータ、スイッチ、およびゲートウェイなど)の必須機能である。図1に示されるように、ユーザは、構成インターフェースもしくは特定のポリシースクリプトを用いることにより、または他の手段により、複数のポリシールールを構成し、ポリシールールをデバイスに配送し、デバイスは、ポリシールールに基づいて、デバイス上の複数のサービスを処理する。
【０００３】
現行のネットワークデバイスには、特にルータ、スイッチ、およびゲートウェイなどのデバイスには、例えば、アプリケーション配送制御(Application Delivery Controller、ADC)のサービスアプリケーション、広域ネットワークの最適化制御(WAN Optimization Co

ntroller、WOC)のサービスアプリケーション、ディープパケットインスペクション(Deep Packet Inspection、DPI)のサービスアプリケーション、侵入防止システム(Intrusion Prevention System、IPS)のサービスアプリケーション、およびユニフォームリソースロケータフィルタ(Uniform/Universal Resource Locator Filter、URLF)のサービスアプリケーションといった、ますます多くのサービスアプリケーションが存在する。各種サービスアプリケーションに対応するポリシールールの数およびタイプも、継続的に増加している。サービスルールの複雑さが増すことにより、ポリシー処理方法は、デバイスの性能および信頼性といった課題に直面している。

【０００４】

図2に示されるように、従来技術のポリシールールの実行には、パケットデータを処理するステップ(ポリシー関連の情報を収集するステップ)と、条件を照合するステップと、ルールを検証するステップと、アクションを実行するステップとが含まれる。デバイスは、パケットデータを受け取った後に、先ず、受け取ったパケットデータに対して、レイヤ1からレイヤ7のデータ処理を遂行し、この処理には、一般に、パケットを分解するステップと、種々のレイヤのパケットのヘッダ情報を抽出するステップと、レイヤ7のプロトコルのフィールド情報を抽出するステップとが含まれており、次いで、デバイスは、収集した情報をポリシー条件に従って検証し、条件が満たされた場合には、ルール検証モジュールを起動してルール照合を遂行し、ポリシールールが一致すると、対応するサービスアクションを実行する。別々のサービスが別々のパケット処理を必要とする場合には、パケットの一部分の特別な処理が含まれてもよい。

【０００５】

従来技術では、パケット情報の中に、各種サービスが必要とする複製の情報が存在するときには、複製のサービス処理プロシージャが存在する。例えば、IPS、URLF、およびADCはすべて、URL(Uniform/Universal Resource Locator、ユニフォームリソースロケータ)情報に対する条件照合の遂行を要求する。この場合、各サービスにおいて、条件照合プロセスは複製であり、ルール検証プロセスも複製である。それに加えて、パケット処理の中に、複製の冗長なプロセスが存在することもある。例えば、IPSがパケット全体のデータの走査を必要とし、URLFがURLフィールドのみの走査を必要とする一方で、ADCが必要とするのは、HTTP(Hyper Text Transfer Protocol、ハイパーテキスト転送プロトコル)パケットのヘッダデータの走査のみであるとき、パケットは、一般に、従来技術のIPS、URLF、およびADCサービスにおいて独立して処理され、これは、パケットが複数回にわたって走査されることを意味する。従来技術が用いられても、パケット処理、条件照合、およびルール照合のステップには、複製の動作が存在することがある。複雑なポリシーおよび複数のサービスを有するデバイスでは、多くの複製の動作が存在するので、サービスの性能が劣化する。

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本発明の実施形態は、ポリシーの実行プロセスにおける冗長な複製の動作を低減し、ネットワークデバイスのポリシー実行性能を改善するために、ポリシー処理方法およびネットワークデバイスを提供するものである。

【課題を解決するための手段】

【０００７】

第1の態様では、本発明の一実施形態は、混合オーケストレータ(mixed orchestrator)、条件照合器(condition matcher)、およびルール照合器(rule matcher)を含むネットワークデバイスを提供するものであり、

混合オーケストレータは、ネットワークデバイス上で動作している複数のサービスアプリケーションに対応するすべてのサービスルール(それぞれのサービスルールが条件およびアクションの2つの部分を含んでいる)の条件を抽出するために、すべてのサービスルールに対して混合オーケストレーション(mixed orchestration)を遂行し、抽出された条件

を用いて少なくとも1つの条件セットを構成し、かつ各サービスルールと条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成するように構成されており、
条件照合器は、混合オーケストレータによって構成された条件セットのそれぞれに従って、ネットワークデバイスが受け取ったネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し、成功裏に照合された条件を記録するのに用いられる条件照合の結果セットを出力するように構成されており、
ルール照合器は、条件照合の結果セットと、混合オーケストレータが生成したマッピング関係データとに従って、成功裏に照合されたサービスルールを求め、成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、成功裏に照合されたサービスルールに対応するアクションを実行させるように構成されている。

【０００８】

第1の態様の第1の可能な実装形態では、混合オーケストレータは、
すべてのサービスルールのそれぞれを、条件とアクションとに分割するように構成されたルール分割ユニットと、
分割ユニットが分割することによって得られた条件を抽出し複製条件を除去するように構成された、複製条件フィルタリング/除去ユニットと、
少なくとも1つのタイプの条件セットを取得するために、複製条件フィルタリング/除去ユニットによって複製条件が除去された後に残った条件を分類するように構成されている条件分類ユニットと、
各サービスルールと条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成するように構成されているマッピングユニットと
を特に含む。

【０００９】

第1の態様の第1の可能な実装形態によれば、第2の可能な実装形態では、マッピングユニットは、各サービスルールと条件セットの中の1つの条件との間のマッピング関係を確立するために、条件セットの中の各条件を、その条件を含むすべてのサービスルールに対応付け、マッピング関係を記録するためのマッピング関係データを生成するように特に構成されており、あるいは、マッピングユニットは、ルール分割ユニットが、すべてのサービスルールのそれぞれを条件とアクションに分割するとき、各サービスルールとサービスルールの条件との間のマッピング関係を記録し、複製条件フィルタリング/除去ユニットによって複製条件が除去された後に、条件セットの中の各条件が、その条件を含むすべてのサービスルールに対応付けられるように、記録されたマッピング関係を調整し、調整されたマッピング関係を記録するためのマッピング関係データを生成するように特に構成されている。

【００１０】

第1の態様または第1の態様の第1もしくは第2の可能な実装形態によれば、第3の可能な実装形態では、条件照合器は、ネットワークデバイスが受け取ったネットワークデータパケットのパケット特徴情報を、条件セットのそれぞれの中の条件と照合し、成功裏に照合された条件の識別子を、条件照合の結果セットの中に記録するように特に構成されている。

【００１１】

第1の態様または第1の態様の第1、第2、もしくは第3の可能な実装形態によれば、第4の可能な実装形態では、ネットワークデバイスは、ネットワークデータパケットのパケット特徴情報を収集するために、ネットワークデバイスが受け取ったネットワークデータパケットに対するパケット検査を遂行するように構成されたインスペクタをさらに含み、条件照合器は、混合オーケストレータによって構成された条件セットのそれぞれに従って、インスペクタが収集したネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し、条件照合の結果セットを出力するように特に構成されている。

【００１２】

第1の態様または第1の態様の第1、第2、第3、もしくは第4の可能な実装形態によれば、第5の可能な実装形態では、ネットワークデバイスのすべてのサービスルールの中で、少なくとも1つのサービスルールは、複数の条件を含むサービスルールである複合ルールであり、

混合オーケストレータは、複合ルールの中の各条件間の論理的関係を記録するようにさらに構成されており、

ルール照合器は、条件照合の結果セットと、混合オーケストレータが生成したマッピング関係データと、各条件間の論理的関係とに従って、成功裏に照合されたサービスルールを求め、成功裏に照合されたサービスルールが属するサービスアプリケーションを呼び出して、成功裏に照合されたサービスルールに対応するアクションを実行させるように、または、成功裏に照合されたサービスルールに対応するサービスアプリケーションに、ルールがヒットしたとのメッセージ(rule hit message)を送って、サービスアプリケーションが成功裏に照合されたサービスルールに対応するアクションをルールがヒットしたとのメッセージに従って実行させるように特に構成されている。

【００１３】

第2の態様では、本発明の一実施形態は、複合サービスポリシーの処理方法を提供し、この方法は、

複数のサービスアプリケーションに対応するすべてのサービスルールの条件を抽出するために、条件およびアクションの2つの部分をそれぞれが含むすべてのサービスルールに対して混合オーケストレーションを遂行し、抽出された条件を用いて、少なくとも1つの条件セットを構成し、各サービスルールと条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成するステップと、

それぞれの構成された条件セットに従って、受け取ったネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し、成功裏に照合された条件を記録するのに用いられる条件照合の結果セットを出力するステップと、

条件照合の結果セットと、生成されたマッピング関係データとに従って、成功裏に照合されたサービスルールを求め、成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、成功裏に照合されたサービスルールに対応するアクションを実行させるステップと

を含む。

【００１４】

第2の態様の第1の可能な実装形態では、複数のサービスアプリケーションに対応するすべてのサービスルールに対する混合オーケストレーションを遂行するステップは、

すべてのサービスルールのそれぞれを条件とアクションに分割し、各サービスルールと、サービスルールの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成するステップと、

分割することによって得られた条件を抽出し、複製条件を除去するステップと、

少なくとも1つのタイプの条件セットを取得するために、複製条件が除去された後に残っている条件を分類するステップと、

条件セットの中の各条件が、その条件を含む1つまたは複数のサービスルールに対応付けられるように、マッピング関係データを調整することによって、条件セットの中の条件と各サービスルールの間のマッピング関係データを取得するステップと

を含む。

【００１５】

第2の態様の第2の可能な実装形態では、複数のサービスアプリケーションに対応するすべてのサービスルールに対する混合オーケストレーションを遂行するステップは、

すべてのサービスルールのそれぞれを、条件とアクションに分割するステップと、

分割することによって得られた条件を抽出し、複製条件を除去するステップと、

少なくとも1つのタイプの条件セットを取得するために、複製条件が除去された後に残っている条件を分類するステップと、

条件セットの中の条件と各サービスルールとの間のマッピング関係データを取得するために、条件セットの中の各条件を、その条件を含むすべてのサービスルールに対応付けるステップと
を含む。
【００１６】
第2の態様または第2の態様の第1もしくは第2の可能な実装形態によれば、第3の可能な実装形態では、すべてのサービスルールの中で、少なくとも1つのサービスルールは、複数の条件を含むサービスルールである複合ルールであり、
この方法は、すべてのサービスルールのそれぞれを条件とアクションに分割するステップの後に、複合ルールの中の各条件間の論理的関係を記録するステップをさらに含み、
条件照合の結果セットと、生成されたマッピング関係データとに従って、成功裏に照合されたサービスルールを求めるステップは、条件照合の結果セットに従って、条件セットの中の条件と各サービスルールの間のマッピング関係データ、各条件間の論理的関係、および成功裏に照合されたサービスルールを求めるステップと、成功裏に照合されたサービスルールが属するサービスアプリケーションを呼び出して、対応するアクションを実行させるステップとを特に含む。
【００１７】
上記の技術的解決策から分かるように、本発明の実施形態のポリシー処理方法およびネットワークデバイスを用いて、複合サービスアプリケーションのポリシールールに対して混合オーケストレーションを遂行することにより、すべてのサービスが必要とする情報が、1つのパケットデータ走査プロセスで抽出され、統合条件照合とルール照合が、複数のサービスに対して遂行される。それによって、複数のサービス間の冗長な動作が低減され、単一デバイス上の複数のサービスを集中させるのが容易になって、デバイスの集積化および性能が改善され、それに加えて、サービス展開およびデバイスハードウェアのコストが低減され、ネットワークデバイスの競争上の優位性が改善される。
【００１８】
本発明の技術的解決策をより明瞭に説明するために、以下は、各実施形態および従来技術を説明するための添付図面について簡単に紹介する。明らかに、以下の説明における添付図面が示すのは、本発明のいくつかの実施形態のみであり、当業者なら、創造的な努力をしなくても、依然としてこれらの添付図面から他の図面を導出し得る。
【図面の簡単な説明】
【００１９】
【図１】従来技術による複合サービスポリシー制御の階層化された配置モードの概略図である。
【図２】従来技術の一実施形態による、ポリシールールの実行の概略流れ図である。
【図３】本発明の一実施形態による、企業の私設クラウドネットワークの概略図である。
【図４】本発明の一実施形態によるポリシー処理方法の概略流れ図である。
【図５】本発明の一実施形態によるポリシー処理方法の流れ図である。
【図６】本発明の一実施形態による、複合サービスルールの混合オーケストレーションのための方法の概略図である。
【図７】本発明の一実施形態によるネットワークデバイスの概略図である。
【図８】本発明の一実施形態による混合オーケストレータの概略図である。
【図９】本発明の一実施形態による条件照合器の概略処理の流れ図である。
【図１０】本発明の一実施形態による条件照合器の概略処理の流れ図である。
【図１１】本発明の一実施形態によるルール照合器の概略処理の流れ図である。
【図１２】本発明の一実施形態によるポリシー処理方法の概略流れ図である。
【図１３】本発明の一実施形態によるネットワークデバイスの概略図である。
【発明を実施するための形態】
【００２０】
本発明の目的、技術的解決策、および利点をより分かりやすくするために、以下は、本

発明の技術的解決策を、本発明の実施形態の添付図面を参照しながら明確に説明するものである。明らかに、説明される実施形態は、本発明の実施形態の一部分でしかない。本発明の技術的問題を解決し、本発明の技術的効果を達成することができる他の実施形態が、当業者によれば、創造的努力をしなくても、本発明の説明された実施形態に基づいて、技術的特徴のいくつかまたはすべてに対して等価な変更を加えることにより導出され得て、このような変更から導出された実施形態は、明らかに、本発明によって開示された範囲の中に入るものとする。

【００２１】

本発明の実施形態によって提供される技術的解決策が、当業者によってよりよく理解されるように、最初に、本発明の実施形態の技術的解決策の適用のシナリオが簡単に説明され、本発明の実施形態によって提供される技術的解決策は、例えばホームネットワーク、アクセスネットワーク、輻輳ネットワーク、バックボーンネットワーク、企業ネットワーク、キャリアネットワーク、種々の私設/公共クラウドといった複数のサービスアプリケーションがあるポリシー制御のシナリオに適用可能である。以下は、簡単な説明のために、一般的な適用のシナリオとして、企業の私設クラウドを用いる。

【００２２】

図3は、本発明の一実施形態による、企業の私設クラウドのシナリオにおけるネットワークの概略図である。図3に示されるように、企業の私設クラウドのシナリオでは、支店(Branch Offices)は、ローカルエリアネットワークのスイッチ(LAN SW)およびルータ(Router)によってローカルエリアネットワークを形成し、一方、支店によって形成されたローカルエリアネットワークは、WAN(Wide Area Network、広域ネットワーク)を通じてデータセンタ(Data Center)と相互接続されており、また、複数のルータ、ゲートウェイ、および複数のタイプのサーバ(ウェブサーバおよびデータベースサーバなど)もデータセンタに配置されており、通常、ファイアウォール、WOC、IPS、およびURLFなどのサービスは、支店のルータおよびスイッチにおいて一体化され、ファイアウォール、WOC、ADC、およびIPSなどの複数のサービスアプリケーションは、データセンタのルータおよびスイッチにおいて一体化されている。この状況では、ルータおよびスイッチは、すべて複数のタイプのポリシー処理を必要とする。

【００２３】

企業の私設クラウドのシナリオは、本発明の技術的解決策の一般的な適用のシナリオにすぎず、本発明の適用のシナリオに対する制限を構成するものではなく、他の適用のシナリオでは、本発明の実施形態の技術的解決策は、複数のタイプのポリシー処理が必要とされている限り適用可能であることに留意されたい。

【００２４】

本発明の一実施形態によって提供されるポリシー処理方法に対する全体的な紹介がもたらされる。図4に示されるように、この方法は、主としてパケット走査、混合オーケストレーション、統合条件照合、および統合ルール検証の処理ステップを含む。

【００２５】

パケット走査のステップでは、例えばレイヤ2からレイヤ7のDPI(Deep Packet Inspection、ディープパケットインスペクション)のパケット検査を遂行することにより、受け取ったネットワークデータパケットから、複数のサービスアプリケーションが必要とする、例えばURL、5つのタプル、およびプロトコルタイプといったすべてのパケット特徴情報が、主として抽出される。それに加えて、パケット走査プロセスでは、冗長な動作は遂行されず、現行のネットワークデバイス上で動作しているサービスアプリケーション(WOC、ADC、およびIPSなど)が必要するパケット特徴情報だけが抽出される。

【００２６】

混合オーケストレーションは、具体的には、すべてのサービスアプリケーションのサービスルールの混合オーケストレーションであり、主に、(1)関連したパケット情報の間の相違のみに関して、同じタイプの条件を抽出し、複数のタイプの条件セットを構築するステップと、(2)条件とルールの間のマッピング関係を生成するステップとを含む。

【００２７】
本発明の実施形態のサービスルールは、サービスアプリケーションの実行ポリシーであり、ルールには、条件およびアクションの2つの部分が含まれることに留意されたい。具体的には、1つのルールが、1つまたは複数の条件を含んでもよく、また、1つまたは複数のアクションを含んでもよく、同一のサービスルールの中の複数の条件が、別々のレイヤのパケット情報に由来してもよい。ルールでは、例えば「if (IP=1.1.1.1 && HTTP.host=www.huawei.com) then drop packet((IP=1.1.1.1 && HTTP.host=www.huawei.com)ならば、パケットをドロップする)」と、「IP=1.1.1.1」および、「HTTP.host=www.huawei.com」とは2つの並列の条件であり、前者はL3の条件であり、後者はL7の条件であって、これら2つは論理的「AND」の関係にあり、また、「drop packet(パケットをドロップする)」は、条件が照合されたとき、サービスアプリケーションが実行する必要のあるアクションである。

【００２８】
統合条件照合は、混合オーケストレーションの後の複数の条件セットに対する統合条件照合である。

【００２９】
統合ルール検証は、混合オーケストレーションを受けたルールセットに対して、統合ルール照合を遂行し、どのサービスルールが成功裏に照合されるか調べる。

【００３０】
統合条件照合および統合検証の目的は、単一の条件およびルールを照合するアクションを遂行する代わりに、パケット走査を遂行することによって収集された複数のタイプのパケット特徴情報と、混合オーケストレーションを受けた複数の条件セットとに対して、統合条件検証およびルール照合を遂行することである。例えば、上記のルール「if (IP=1.1.1.1 && HTTP.host=www.huawei.com) then drop packet((IP=1.1.1.1 && HTTP.host=www.huawei.com)ならば、パケットをドロップする)」を、引き続き例として用いると、最初にパケット識別を遂行することにより、各レイヤのパケット特徴情報が収集され、次いで、条件検証のために、この情報がそれぞれの対応する条件データセットに入力され、次に、ヒットしたルールを取得するために、条件検証結果が、統合ルール照合用のルール照合モジュールに報告されて、最後に、ヒットしたルールに対応するサービスアクションが実行される。

【００３１】
上記の方法に基づいて、以下は特定の実施形態を説明する。図5に示されるように、本発明の一実施形態によって提供される複合サービスポリシーの処理方法は、次のステップを含む。

【００３２】
S501。複数のサービスアプリケーションに対応するすべてのサービスルールの条件を抽出するために、すべてのサービスルールに対して混合オーケストレーションを遂行し、抽出された条件を用いて少なくとも1つの条件セットを構成し、各サービスルールと条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成する。

【００３３】
サービスルールには、通常、以下のように簡単に記述され得る2つの部分、条件およびアクションが含まれることに留意されたい。

ルール:「if (condition set) then (action set)」(「(条件セット)ならば、(アクションセット)」)、ここで条件セットは、条件と、通常はANDおよびORを含む各条件間の論理的関係とを含み、アクションセットは、1つのルールに対応する複数の逐次または並列のサービスアクションを含み、通常は、例えばアクション1およびアクション2といった具合に、順番に示されてもよく、簡潔にするために、本発明の実施形態では、ルール1:「if (condition 1) then action 1」(「(条件1)ならば、(アクション1)」)は、条件を1つだけ含み、1つのアクションが説明のために用いられており、ここで、ルール1は、条件1が

満たされると、対応するアクション1が実行されることを示す。

【００３４】

具体的には、一実施形態では、複数のサービスアプリケーションに対応するすべてのサービスルールに対して混合オーケストレーションを遂行するステップは、特に次のステップを含む。

【００３５】

S5011。各サービスルールを条件とアクションに分割し、各サービスルールと、サービスルールの中の条件との間のマッピング関係を記録するためのマッピング関係データを生成する。

【００３６】

すべてのサービスルールがルール1のような「単一条件のルール」であれば、マッピング関係データに記録する必要があるのは、各サービスルールの中の条件とサービスルールの間のマッピング関係のみであることに留意されたい。このようなサービスルールについては、条件が成功裏に検証されると、条件に対応するサービスルールが照合されたことを示し、サービスルールに含まれているアクションを起動して実行することもできる。一実施形態では、複数の条件を含む複合ルールが存在する場合には、条件がルールに対して一意的に対応し得ないので、各サービスルールとサービスルールの条件との間のマッピング関係を記録するだけでは不十分であり、したがって、各サービスルールとサービスルールの中の条件との間のマッピング関係を記録することに加えて、同一ルールの中の各条件間の論理的関係を記録する必要があり、この場合、ルールが成功裏に照合されたかかどうかということは、その同一のルールの中に含まれている各条件の照合結果と、各条件間の論理的関係によってのみ判断され得る。最後に、マッピング関係データは、単なる機能名であって、特定の実装形態のデータテーブルおよびデータファイルなどの、データを格納するための担体であり得ることに留意されたい。

【００３７】

S5012。分割することによって得られたすべてのサービスルールの条件を抽出し、複製条件を除去する。

【００３８】

S5013。少なくとも1つのタイプの条件セットを取得するために、複製条件が除去された後に残っている条件を分類する。

【００３９】

具体的には、複製条件を除去した後に残った条件を分類するステップは、同一の特徴を含む条件を1つのタイプに分類するものであり、例えば、IPアドレスを照合するための条件を1つのタイプに分類し、URLを照合するための条件を1つのタイプに分類する。確かに、分類は照合モードに従って遂行されてもよく、例えば、照合のための条件が、正規表現モードに従って1つのタイプに分類され、また、分類はパケット情報レイヤに従って遂行されてもよく、例えば、L3の条件が1つのタイプに分類され、L7の条件が1つのタイプに分類される。それに加えて、別の実装形態では、サービスルールの中に含まれている条件は、L1からL7のパケットデータの特徴情報に関連した条件ばかりでなく、あるタイプのサービスアクションを実行するかどうか判断するのに用いられ得る、サービス事象、プロトコルタイプ、およびサービス結果などのポリシー条件をさらに含んでいる可能性があることに留意されたい。

【００４０】

S5014。条件セットの中の各条件が、その条件を含むすべてのサービスルールに対応付けられるように、マッピング関係データを調整することによって、条件セットの中の条件と各サービスルールの間のマッピング関係データを取得する。

【００４１】

ステップS5012において、抽出されたすべての条件から複製条件が除去されているので、分類の後に得られた条件セットのそれぞれの中の条件は、すべて固有のものである。しかし、複製条件が除去される一方で、以前に生成されたマッピング関係データが損なわれ

る。したがって、マッピング関係データを調整する必要がある。調整後には、同一の条件を含むサービスルールのすべてが、条件セットの中の対応する同一の条件に対応付けられ、すなわち、条件セットの中の各条件が、その条件を含む1つまたは複数のサービスルールに対応付けられる。

【００４２】

確かに、別の実施形態では、上記のステップは、最初にマッピング関係データを生成し、次いで、複製条件を除去した後にマッピング関係データを調整するというモードを用いるのでなく、すべてのサービスルールの条件を抽出し複製条件を除去し、分類することによって条件セットを形成した後に、条件セットの中の条件と各サービスルールの間のマッピング関係データを取得するように、条件セットのそれぞれの中の各条件を、その条件を含むすべてのサービスルールに直接対応付けることにすれば、さらに簡易化され得ることは理解し得る。

【００４３】

さらに、別の実施形態では、ステップS5014の後に次のステップを含んでもよい。

【００４４】

S5015。分類の後に得られた条件セットのそれぞれを、統一フォーマットへと編集する。

【００４５】

具体的には、複製条件を除去した後の条件分類の結果に従って、分類された条件セットのそれぞれを、タイプに応じて、条件照合エンジンがサポートしているフォーマットへと編集する。さらに、サービスルールとサービスルールの条件との間のマッピング関係を記録するためのマッピング関係データを、ルール照合エンジンが必要とするフォーマットへと編集してもよく、それに加えて、上記の複合ルールが存在する場合には、さらに、各複合ルールの中の条件間の論理的関係(またはルール照合エンジンがサポートするフォーマットへと編集した後の論理的関係)をルール照合エンジンに格納する必要がある。条件照合エンジンは、主に種々の条件の統合された検証、すなわちサービスルールが成功裏に照合された条件データの検証に関与することに留意されたい。当業者なら、条件照合エンジンがソフトウェアまたはハードウェア論理によって実現され得ることを理解するはずであり、本明細書でさらに説明することはない。

【００４６】

以下で、上記のステップが特定の例を用いて説明される。図6に示されるように、現行のネットワークデバイスは、以下のサービスルールを有する(ここでは、実例として上記の「単一の条件」が説明に用いられる)。

IPSのルール1:「if (URL="url-1") alert threat 1 (alert process 1)」(「(URL="url-1")ならば、脅威1を警告する(プロセス1を警告する)」)

IPSのルール2:「if (IP="128.1.1.1") alert threat 2 (alert process 2)」(「(IP="128.1.1.1")ならば、脅威2を警告する(プロセス2を警告する)」)

URLFのルール1:「if (URL="url-2") block」(「(URL="url-2")ならば、ブロックする」)

WOCのルール1:「if (IP="128.1.1.1") read cache (read cache)」(「(IP="128.1.1.1")ならば、キャッシュを読み取る(read cache)」)

ADCのルール1:「if (URL="url-2") block」(「(URL="url-2")ならば、ブロックする」)

【００４７】

最初に、各サービスルールを分割し、すなわち各サービスルールを条件とアクションに分割して、ルールと条件との間のマッピング関係を記録し、図6において、「URL="url-1"」、「URL="url-2"」、「IP="128.1.1.1"」などはすべて条件であり、「alert threat 1」(「脅威1を警告する」)、「block」(「ブロックする」)、および「alert threat 2」(「脅威2を警告する」)はすべてアクションであり、次いで、分割することによって得られたすべての条件から複製条件を除去し、例えば、IPSのルール2の条件とWOCのルール1の条件は複製であり、また、URLFのルール1の条件とADCのルール1の条件は複製であって、複

製条件を除去した後に、条件とルールの間のマッピング関係をさらに調整する必要があり、例えば、図6に示された条件「IP="128.1.1.1"」は、複製条件を除去した後に、IPSのルール2およびWOCのルール1の2つのルールに対応付ける必要があり、また、条件「URL="url-2"」をURLFのルール1およびADCのルール1に対応付ける必要があり、次いで、複製条件を除去した後に残っている条件を図6に示されるように分類し、URL関連の条件を1つのタイプに分類し、IP関連の条件を1つのタイプに分類して、URL条件セットおよびIP条件セットを形成する。

【００４８】

S502。それぞれの構成された条件セットに従って、受け取ったネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し、成功裏に照合された条件を記録するのに用いられる条件照合の結果セットを出力する。

【００４９】

具体的には、ネットワークデータパケットのパケット特徴情報は、各サービスアプリケーションのサービスルールに関連するすべてのパケット特徴、すなわち各サービスルールの条件が照合されるかどうか検証するときに用いる必要のあるパケット特徴の情報を特に含んでおり、これらの情報は、例えばURLFルールの条件に関連するURL情報およびIPSルールの条件に関連する5つのタプル情報といった、特にネットワークデータパケットのL1～L7の情報であり得る。ネットワークデータパケットのパケット特徴情報は、あるタイプのサービスアクションを実行するかどうか判断するための、例えばサービス事象、プロトコルタイプ、サービス結果などといった条件に関連するパケット特徴情報をさらに含んでもよい。

【００５０】

各サービスルールの条件が分類され、編集されて、複製条件が除去された後に、例えばURL条件セット、IP条件セット、およびアプリケーションレイヤのプロトコルタイプ条件セットといった複数の条件セットが形成されると想定して、抽出されたパケット特徴情報に対して、統合条件照合が遂行され、これには、ネットワークデータパケットのURLを、照合のために、URL条件セットに入力するステップと、ネットワークデータパケットのIPアドレスを、照合のために、IPアドレス条件セットに入力するステップと、ネットワークデータパケットのアプリケーションレイヤのプロトコルタイプを、照合のために、アプリケーションレイヤのプロトコルタイプ条件セットに入力するステップとが特に含まれ、特定の照合プロセスでは、ネットワークデータパケットの特徴情報が、条件セットのそれぞれの条件と整合するか、または条件の要件を満たすかどうか、比較される。条件セットのすべてを照合した結果が、「条件照合の結果セット」に要約されて、最終的にはルール照合エンジンに報告され、条件照合の結果セットは、どの条件が成功裏に照合されたか(ヒットしたか)示すのに用いられる。具体的には、成功裏に照合された条件は、識別子を用いて、条件照合の結果セットの中に含まれてもよい。

【００５１】

特定の実装形態では、ステップS502は、特に次のステップを含む。

【００５２】

S5021。複数のサービスアプリケーションが必要とするパケット特徴情報をすべて抽出するために、受け取ったネットワークデータパケットに対してパケット検査を遂行する。

【００５３】

複数のサービスが必要とする、例えばURL、5つのタプル、およびプロトコルタイプといったすべてのパケット特徴情報が、例えばレイヤ2からレイヤ7のDPI(Deep Packet Inspection、ディープパケットインスペクション)といったパケット検査を遂行することにより、受け取ったネットワークデータパケットから抽出され得る。それに加えて、パケット走査プロセスでは、冗長な動作は遂行されず、現行のネットワークデバイス上で動作しているサービスアプリケーション(WOC、ADC、およびIPSなど)が必要するパケット特徴情報だけが抽出される。サービスアプリケーションが必要とするパケット特徴情報は、特に、サービスアプリケーションに対応するサービスルールに関連するパケット特徴情報を指す、

より具体的には、サービスルールの条件に対応するパケット特徴情報、すなわちサービスルールの中に含まれている条件が満たされているがどうか検証するときに用いる必要のあるパケット特徴情報を指すことに留意されたい。

【００５４】

S5022。抽出されたパケット特徴情報を条件セットのそれぞれの条件と照合し、成功裏に照合された条件の識別子を、条件照合の結果セットの中に記録する。

【００５５】

S503。条件照合の結果セットと、生成されたマッピング関係データとに従って、成功裏に照合されたサービスルールを求め、成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、成功裏に照合されたサービスルールに対応するアクションを実行させる。

【００５６】

特定の実施形態では、サービスルールが、条件を1つしか含まない「単一条件のルール」であると、ルール照合エンジンは、条件と、マッピング関係データの中に記録されたサービスルールの間のマッピング関係とに従って、どのサービスルールが成功裏に照合されているか、すなわち、どのルールがヒットしているか、判断することができ、サービスルールが、複数の条件を含む複合ルールであると、ルール照合エンジンは、各サービスルールと条件との間のマッピング関係、および各サービスルールの各条件間の論理的関係に従って、ルールがヒットしているかどうか判断する必要があり、最終的に、成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、サービスルールに対応するアクションを実行させる。アクションの実行を起動するプロセスは、成功裏に照合されたサービスルールが属するサービスアプリケーションを呼び出して、成功裏に照合されたサービスルールに対応するアクションを実行させる、または、成功裏に照合されたサービスルールに対応するサービスアプリケーションに、ルールがヒットしたとのメッセージを送って、サービスアプリケーションが成功裏に照合されたサービスルールに対応するアクションをルールがヒットしたとのメッセージに従って実行させる、または各サービスルールの照合結果を、対応するサービスアプリケーションに報告して、同サービスアプリケーションに、そのサービスのサービスルールの照合に従って、ルールに対応するアクションを実行するべきかどうか判断させるものであることが理解され得る。

【００５７】

上記の技術的解決策から分かるように、本発明の実施形態のポリシー処理方法を用いて、複合サービスのルールに対して混合オーケストレーションを遂行することにより、すべてのサービスルールが、統合やり方で構成され、すべてのサービスが必要とする情報が、1つのパケットデータ走査プロセスで抽出され、必要とされるのは、1つの条件照合およびルールの検証プロセスのみである。それによって、複数のサービス間の冗長な動作が低減され、単一デバイス上の複数のサービスを集中させるのが容易になって、デバイスの集積化および性能が改善され、それに加えて、サービス展開およびデバイスハードウェアのコストが低減され、ネットワークデバイスの競争上の優位性が改善される。

【００５８】

以下で、上記の方法を実施するための装置の実施形態が説明される。図7に示されるように、本発明の一実施形態は、ネットワークデバイスを提供するものである。図7によれば、ネットワークデバイス70は、混合オーケストレータ720、条件照合器730、およびルール照合器740を含み、各サービスルールは、条件およびアクションの2つの部分を含む。

【００５９】

混合オーケストレータ720は、ネットワークデバイス70上で動作している複数のサービスアプリケーションに対応するすべてのサービスルールの条件を抽出するために、すべてのサービスルールに対して混合オーケストレーションを遂行し、抽出された条件を用いて少なくとも1つの条件セットを構成し、かつ各サービスルールと条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成するように構成されている。

【００６０】
条件照合器730は、混合オーケストレータ720によって構成された条件セットのそれぞれに従って、ネットワークデバイス70が受け取ったネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し、成功裏に照合された条件を記録するのに用いられる条件照合の結果セットを出力するように構成されている。
【００６１】
ルール照合器740は、条件照合器730が出力した条件照合の結果セットと、混合オーケストレータ720が生成したマッピング関係データとに従って、成功裏に照合されたサービスルールを求め、成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、成功裏に照合されたサービスルールに対応するアクションを実行させるように構成されている。
【００６２】
具体的には、一実装形態では、図8に示されるように、混合オーケストレータ720は、ルール分割ユニット7201、複製条件フィルタリング/除去ユニット7202、条件分類ユニット7203、およびマッピングユニット7204を特に含んでいる。
【００６３】
ルール分割ユニット7201は、主として、複合サービスルールセットの中の各サービスルールを、条件とアクションに分割するように構成されており、複合サービスルールセットは、ネットワークデバイス70上で動作している、ネットワークデバイス70に配置された1つまたは複数のサービスアプリケーションに対応するサービスルールをすべて含んでいる。
【００６４】
複製条件フィルタリング/除去ユニット7202は、ルール分割ユニット7201が分割することによって得られた条件を抽出し複製条件を除去するように構成されている。
【００６５】
条件分類ユニット7203は、少なくとも1つのタイプの条件セットを取得するために、複製条件フィルタリング/除去ユニット7202によって複製条件が除去された後に残った条件を分類するように構成されている。
【００６６】
具体的には、条件分類ユニット7203は、同一の特徴を有する条件を1つのタイプに分類し、例えばIPアドレス照合用の条件を1つのタイプに分類し、URL照合用の条件を1つのタイプに分類するように構成されている。確かに、分類は照合モードに従って遂行されてもよく、例えば、照合のための条件が、正規表現モードに従って1つのタイプに分類され、また、分類はパケット情報レイヤに従って遂行されてもよく、例えば、L3の条件が1つのタイプに分類され、L7の条件が1つのタイプに分類される。それに加えて、別の実装形態では、サービスルールの中に含まれている条件は、L1からL7のパケットデータの特徴情報に関連した条件ばかりでなく、あるタイプのサービスアクションを実行するかどうか判断するのに用いられ得る、サービス事象、プロトコルタイプ、およびサービス結果などのポリシー条件をさらに含んでいる可能性があることに留意されたい。
【００６７】
マッピングユニット7204は、条件セットの中の条件と各サービスルールの間のマッピング関係データを生成するように構成されている。
【００６８】
具体的には、マッピングユニット7204は、条件セットの中の条件と各サービスルールの間のマッピング関係データを取得するために、条件セットの中の各条件を、その条件を含むすべてのサービスルールに直接対応付けてもよい。別の実施形態では、マッピングユニット7204は、ルール分割ユニット7201が、すべてのサービスルールのそれぞれを条件とアクションに分割するとき、各サービスルールとそのサービスルールの中の条件との間のマッピング関係を記録するためのマッピング関係データを生成して、複製条件フィルタリング/除去ユニット7202によって複製条件が除去された後に、条件セットの中の各条件が、

その条件を含む1つまたは複数のサービスルールに対応付けられるように、マッピング関係データを調整し、それによって、サービスルールの条件と各サービスルールの間のマッピング関係データを取得するように構成されてもよい。

【００６９】

さらに、一実施形態では、混合オーケストレータ720は、分類することによって得られたすべてのタイプの条件セットのそれぞれを、そのタイプに従って、条件照合器730がサポートする統一フォーマットに編集するように構成された編集ユニット7205をさらに含み、対応して、条件照合器730は、編集ユニット7205によって編集された統一フォーマットの条件セットに従って、ネットワークデバイス70が受け取ったネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し、条件照合の結果セットを出力するように特に構成されている。

【００７０】

さらに、編集ユニット7205は、マッピングユニット7204が生成したマッピング関係データを、ルール照合器740がサポートするフォーマットへと編集し、それに加えて、上記のルールのような複合ルールが存在する場合には、各サービスルールの中の各条件間の論理的関係を、ルール照合器740にさらに格納する(または、マッピング関係データを、ルール照合器がサポートするフォーマットに編集してから格納する)ように構成されてもよい。

【００７１】

特定の実装形態では、条件照合器730は、ネットワークデバイス70が受け取ったネットワークデータパケットのパケット特徴情報を、条件セットのそれぞれの中の条件と照合し、成功裏に照合された条件の識別子を、条件照合の結果セットの中に記録するように特に構成されている。ここで、照合に用いられるネットワークデータパケットの特徴情報は、ネットワークデバイス70上で動作しているサービスアプリケーションのサービスルールに関連するすべてのパケット特徴情報、すなわち各サービスルールの中の条件に対応するパケット特徴情報を特に含んでおり、条件の識別子は、条件を一意的に示すのに用いられ、具体的には数、文字、または文字列などでもよい。

【００７２】

条件照合器730は、特徴のタイプおよび条件に対応するパケット特徴情報などに従って、各タイプの条件セットにおいて統合条件照合を遂行するように特に構成されている。条件セットは、L1～L7のパケットデータの特徴情報に関連する条件セットに限定されず、あるタイプのサービスアクションを実行するかどうか判断するための、例えばサービス事象、プロトコルタイプ、サービス結果などといった他の条件セットをさらに含み得ることに留意されたい。

【００７３】

一実装形態では、図9に示されるように、条件照合器730の処理プロシージャは以下の通りである。

【００７４】

最初に、ネットワークデータパケットは、1つまたは複数の処理ユニットによって(図9のL3～L7の処理および他の処理に示されるように)処理され、かつ解析され、複数のサービスが必要とするすべてのパケット特徴情報が抽出されて、統合照合のために条件照合器に提示され、次いで、条件照合器が、混合オーケストレータによって生成された条件セットのそれぞれに従って、抽出されたパケット特徴情報に対して対応するマルチモード照合を遂行する。この照合モードは、集中型条件照合であって、条件照合器の出力結果は、条件照合の結果セット、すなわち、成功裏に照合された条件の識別子セットであり、各条件識別子が条件を一意的に示す。

【００７５】

別の実施形態では、ネットワークデバイス70は、ネットワークデバイス上で動作している複数のサービスアプリケーションが必要とするパケット特徴情報をすべて収集するために、受け取ったネットワークデータパケットに対してパケット検査を遂行するように構成されたインスペクタ710をさらに含んでもよく、対応して、条件照合器730は、混合オーケ

ストレータ720によって構成された条件セットのそれぞれに従って、インスペクタ710が収集したネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し、条件照合の結果セットを出力するように特に構成されている。

【００７６】

実際の適用では、インスペクタ710は、複数のパケット処理ユニットでもよく、例えばL3の処理専用の処理ユニット、L7の処理専用の処理ユニットなど、各パケット処理ユニットが、1つのタイプのパケット走査に独立して関与し、すべてのパケット処理ユニットが、複数のサービスによって必要とされるすべてのパケット特徴情報を連帯で抽出することに留意するべきであり、サービスが必要とするパケット特徴情報は、特に、ネットワークデバイス上のサービスアプリケーションに対応するすべてのサービスルールに関連するパケット特徴情報、または、より具体的には、サービスルールの中に含まれている各条件が照合されるかどうか検証するときに用いる必要のあるパケット特徴情報を指すことに留意するべきである。別の実装形態では、インスペクタは、例えばDPIモジュールといった、L3～L7の処理またはさらに他のタイプのパケット処理機能を組み込んだ多機能のプロセッサでもよい。それに加えて、実際の適用では、インスペクタ710は、ネットワークデバイスに配置されるばかりでなく、独立したサービスモジュールとして用いられてネットワークデバイスの外部にも配置され、バスを通じて、または他の通信方式で、ネットワークデバイスと相互に接続されてもよいことが、当業者には理解され得る。

【００７７】

適用のシナリオの1つでは、条件照合器は独立した照合エンジンでもよく、照合エンジンは、ソフトウェアアルゴリズムまたはハードウェア論理によって実現されてもよい。

【００７８】

別の適用のシナリオでは、図10に示されるように、インスペクタ710が複数のパケット処理ユニットを含む場合には、条件照合器も、複数の論理的機能ユニットに分割され得て、分散するやり方で各パケット処理ユニットに配置され、このシナリオでは、特徴分類に従って、混合オーケストレータが、分類後に取得された条件セットを、対応するパケット処理ユニットに配送し、各パケット処理ユニットには条件照合器が配置され、パケット処理ユニットがパケット特徴情報を抽出した後に、抽出されたパケット特徴情報は、パケット処理ユニットの条件照合器に直接報告され、条件が成功裏に照合されると、その結果が条件照合の結果セットに報告される。

【００７９】

図11に示されるように、ルール照合器740は、条件照合の結果セットと、各サービスルールとマッピング関係データの中に記録されたサービスルールの条件との間のマッピング関係とに従って、成功裏に照合されたサービスルールを求め、次いで、サービスアプリケーションを呼び出して、サービスルールに対応するアクションを実行させるように特に構成されている。サービスルールが、条件を1つしか含まない「単一条件のルール」であると、ルール照合器740は、条件照合の結果セットと、各サービスルールとマッピング関係データの中に記録されたサービスルールの条件との間のマッピング関係とに従って、どのサービスルールが成功裏に照合されたか、すなわち、どのルールがヒットしたか判断することができ、次いで、サービスアプリケーションを起動して、ヒットしたルールに対応するアクションを実行させ、サービスルールの中に複数の条件を含む複合ルールが存在する場合には、ルール照合器740は、条件照合の結果セットと、マッピング関係データに記録されている各サービスルールとサービスルールの条件との間のマッピング関係と、各サービスルールの各条件間の論理的関係とに従って、どのルールがヒットしたか、特に判断してもよく、最終的に、成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、サービスルールに対応するアクションを実行させることに留意されたい。具体的には、ルール照合器740は、プロセス/関数を呼ぶことにより、成功裏に照合されたサービスルールが属するサービスアプリケーションを直接呼び出してもよく、成功裏に照合されたサービスルールに対応するアクションを実行させ、または、成功裏に照合されたサービスルールに対応するサービスアプリケーションに、ルールがヒットしたとのメ

ッセージを送って、サービスアプリケーションが成功裏に照合されサービスルールに対応するアクションをルールがヒットしたとのメッセージに従って実行させるものであり、ルールがヒットしたとのメッセージは、サービスルールが成功裏に照合されたことを示すのに用いられる。

【００８０】

以下は、ネットワークデバイスによって遂行されるポリシー実行プロセスを説明するために特定の例を用いる。図12は、本発明の一実施形態に従ってネットワークデバイスによってHTTPパケットのURL情報に関して実行される複数サービスのポリシーの実行方法を示す。図12によれば、最初に、混合オーケストレータは、すべてのサービスルール(図12は3つのサービスルールを示す)に対して混合オーケストレーションを遂行し、次いで、URLの照合条件をすべて抽出し、URL条件照合器に配送し、また、条件とポリシールールの間のマッピング関係およびポリシーアクションをルール照合器に配送し、ポリシーの実行中に、パケットに対するDPI処理が遂行された後に取得されたURL情報が、統合条件照合のためにURL条件照合器に送られ、また、取得された照合結果がルール照合器に送られる。このときADCルールがヒットすると仮定すれば、対応するアクションを実行するためにADCサービスユニットが直接呼び出される。明らかに、本発明の実施形態では、URLに対して必要なのは1つの照合プロセスだけであり、サービスユニットに必要なのは、1つのルール検証プロセスおよび1つの呼出しプロセスだけであって、複数のサービスの間の冗長な動作が解消される。

【００８１】

最後に、前述の方法の実施形態は、本発明の実施形態によって提供されるネットワークデバイスの特定の動作原理および動作プロセスに関して参照されてもよく、このことは、本明細書にはさらなる説明がないことに留意されたい。

【００８２】

本発明の実施形態のネットワークデバイスを用いて、複合サービスのルールに対して混合オーケストレーションを遂行することにより、すべてのサービスルールが、統合やり方で構成され、すべてのサービスが必要とする情報が、1つのパケットデータ走査プロセスで抽出され、必要とされるのは、1つの条件照合およびルールの検証プロセスのみである。それによって、複数のサービス間の冗長な動作が低減され、単一デバイス上の複数のサービスを集中させるのが容易になって、デバイスの集積化および性能が改善され、それに加えて、サービス展開およびデバイスハードウェアのコストが低減され、ネットワークデバイスの競争上の優位性が改善される。

【００８３】

図13は、本発明の一実施形態による別のネットワークデバイスの概略図である。図13に示されるように、ネットワークデバイスは、少なくとも1つのプロセッサ1001、メモリ1002、通信インターフェース1003、およびバスを含む。プロセッサ1001、メモリ1002、および通信インターフェース1003は、バスによって接続されており、相互に通信する。バスは、業界標準アーキテクチャ(Industry Standard Architecture、ISA)バス、周辺装置相互接続(Peripheral Component Interconnect、PCI)バス、またはイーサ(Extended Industry Standard Architecture、EISA)バスなどでもよい。バスは、アドレスバス、データバス、制御バスなどに分類され得る。図示を容易にするために、バスは実線のみによって示されているが、これは、1つのバスまたは1つのタイプのバスしか存在しないことを意味するものではない。

【００８４】

メモリ1002は、実行可能プログラムコードを格納するように構成されており、プログラムコードにはコンピュータ動作指令が含まれる。メモリ1002は、高速RAMを含んでもよく、例えば少なくとも1つの磁気ディスク装置といった不揮発性メモリ(non-volatile memory)も含んでもよい。

【００８５】

一実施形態では、プロセッサ1001は、メモリ1002の中に格納された実行可能プログラム

コードを読み取って、
複数のサービスアプリケーションに対応するすべてのサービスルール(それぞれが条件およびアクションの2つの部分を含んでいる)の条件を抽出するために、すべてのサービスルールに対して混合オーケストレーションを遂行し、抽出された条件を用いて少なくとも1つの条件セットを構成し、各サービスルールと条件セットの中の1つの条件との間のマッピング関係を記録するためのマッピング関係データを生成し、
それぞれの構成された条件セットに従って、受け取ったネットワークデータパケットのパケット特徴情報に対する条件照合を遂行し、成功裏に照合された条件を記録するのに用いられる条件照合の結果セットを出力し、
条件照合の結果セットと、生成されたマッピング関係データとに従って、成功裏に照合されたサービスルールを求め、成功裏に照合されたサービスルールに対応するサービスアプリケーションを起動して、成功裏に照合されたサービスルールに対応するアクションを実行させるように、
実行可能プログラムコードに対応するプログラムを実行する。

【００８６】
上記のプロシージャは、本明細書ではさらには説明されない。詳細については、上記の方法および装置の実施形態が参照されてもよい。

【００８７】
プロセッサ1001は、中央処理装置(Central Processing Unit、CPU)もしくは特定用途向け集積回路(Application Specific Integrated Circuit、ASIC)でもよく、あるいは、本発明の実施形態を実現するための1つまたは複数の集積回路として構成されている。

【００８８】
上記のプロセッサ1001は、上記の機能を有するばかりでなく、これらの方法の実施形態の他のプロシージャを実行するようにも構成され得て、このことは、本明細書にはさらなる説明がないことに留意されたい。

【００８９】
通信インターフェース1003は、主として、この実施形態のネットワークデバイスと他のデバイスまたは装置の間の通信を実施するように構成されている。本発明の実施形態では、開示されたシステム、装置、および方法が他のやり方で実現されてもよいことが理解され得る。例えば、上記で説明された装置の実施形態は、単なる例示である。

【００９０】
個別の部分として説明されたユニットは、物理的に分離していても分離していなくてもよく、また、ユニットとして示された部分は、物理的ユニットであってもそうでなくてもよく、1つの位置に配置されても、複数のネットワークユニット上に分散されてもよい。実施形態の解決策の目的を達成するための実際の必要性に応じて、ユニットの一部分または全体を選択してもよい。

【００９１】
それに加えて、本発明の実施形態におけるネットワークデバイスの機能ユニットは、1つの処理ユニットに一体化されてもよく、またはユニットのそれぞれが単独で物理的に存在してもよく、または2つ以上のユニットが1つのユニットに一体化されてもよい。一体化されたユニットは、ハードウェアの形態で実現されてもよく、またはソフトウェアの機能ユニットの形態で実現されてもよい。

【００９２】
一体化されたユニットが、ソフトウェア機能ユニットの形態で実施されて、販売される、または独立した製品として用いられる場合には、一体化されたユニットは、コンピュータ可読記憶媒体の中に格納されてもよい。このような理解に基づいて、本発明の技術的解決策が、基本的に、または従来技術に寄与する部分が、または技術的解決策のすべてもしくは一部分が、ソフトウェア製品の形態で実現されてもよい。コンピュータソフトウェア製品は、記憶媒体に格納され、本発明の実施形態において説明された方法のステップのすべてまたは一部分を遂行するように、コンピュータ機器(パーソナルコンピュータ、サー

バ、またはネットワークデバイスでもよい)に指示するためのいくつかの指令を含んでいる。前述の記憶媒体には、USBフラッシュディスク、着脱式ハードディスク、読取り専用メモリ(Read-Only Memory、ROM)、ランダムアクセスメモリ(Random Access Memory、RAM)、磁気ディスク、または光ディスクなど、プログラムコードを格納することができる任意の媒体が含まれる。

【００９３】

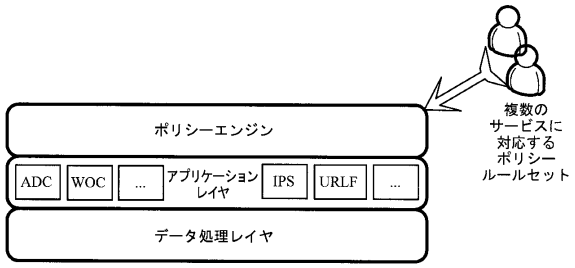
最後に、前述の実施形態は、本発明を限定するのでなく、単に本発明の技術的解決策を説明するように意図されていることに留意されたい。本発明が、前述の実施形態を参照しながら詳細に説明されているが、当業者なら、本発明の実施形態の技術的解決策の趣旨および範囲から逸脱することなく、前述の実施形態において説明された技術的解決策に対する修正形態またはそのいくつかの技術的特徴に対する等価な置換形態をさらに作成することができることを理解するはずである。

【符号の説明】

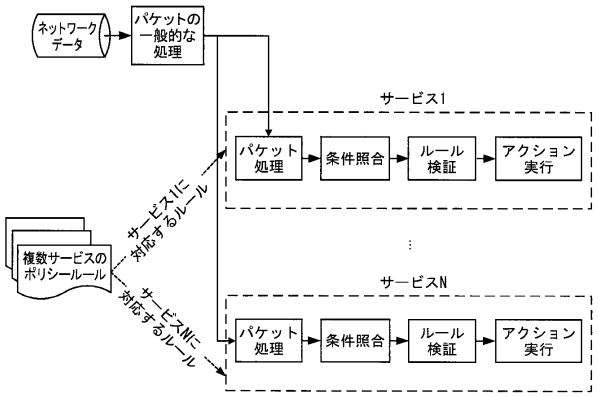
【００９４】

70　ネットワークデバイス
710　インスペクタ
720　混合オーケストレータ
730　条件照合器
740　ルール照合器
1001　プロセッサ
1002　メモリ
1003　通信インターフェース
7201　ルール分割ユニット
7202　複製条件フィルタリング/除去ユニット
7203　条件分類ユニット
7204　マッピングユニット
7205　編集ユニット

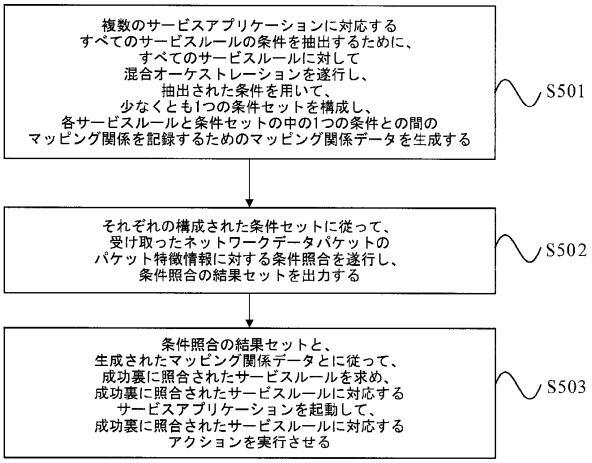
【図１】



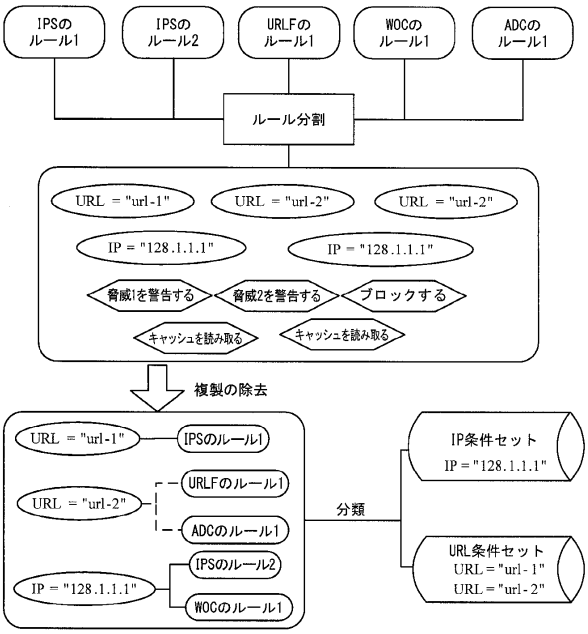
【図２】



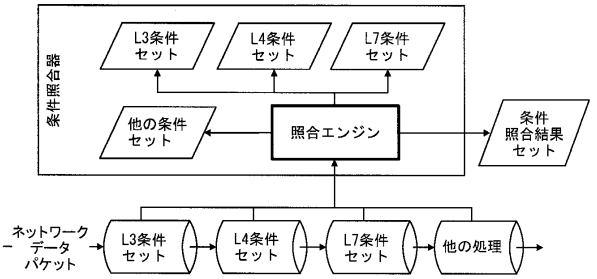
【図５】



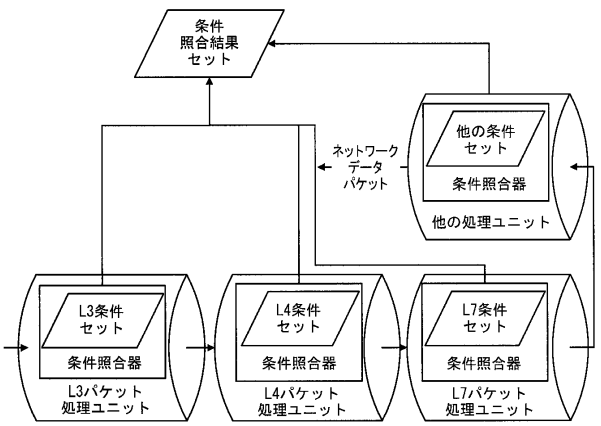
【図６】



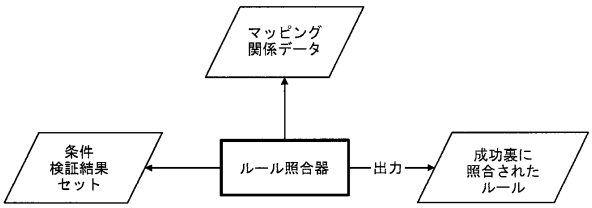
【図９】



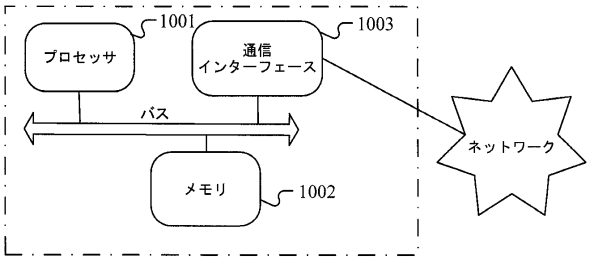
【図１０】



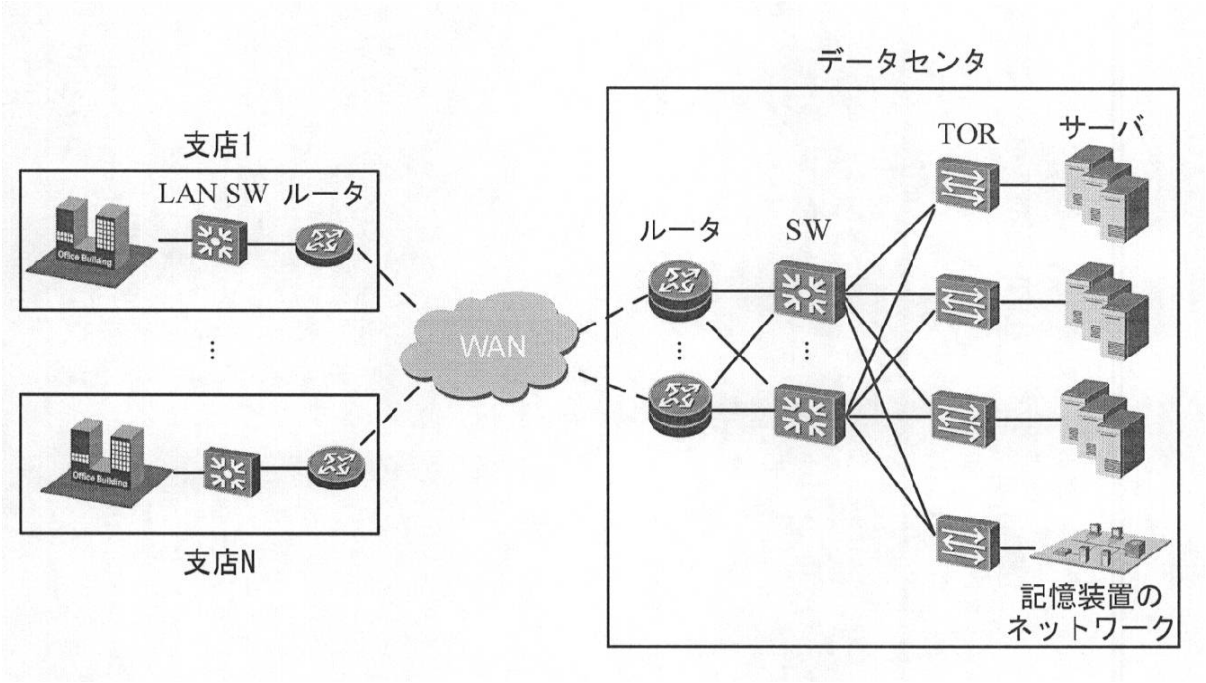
【図１１】


マッピング
関係データ
条件
検証結果
セット
ルール照合器
出力
成功裏に
照合された
ルール

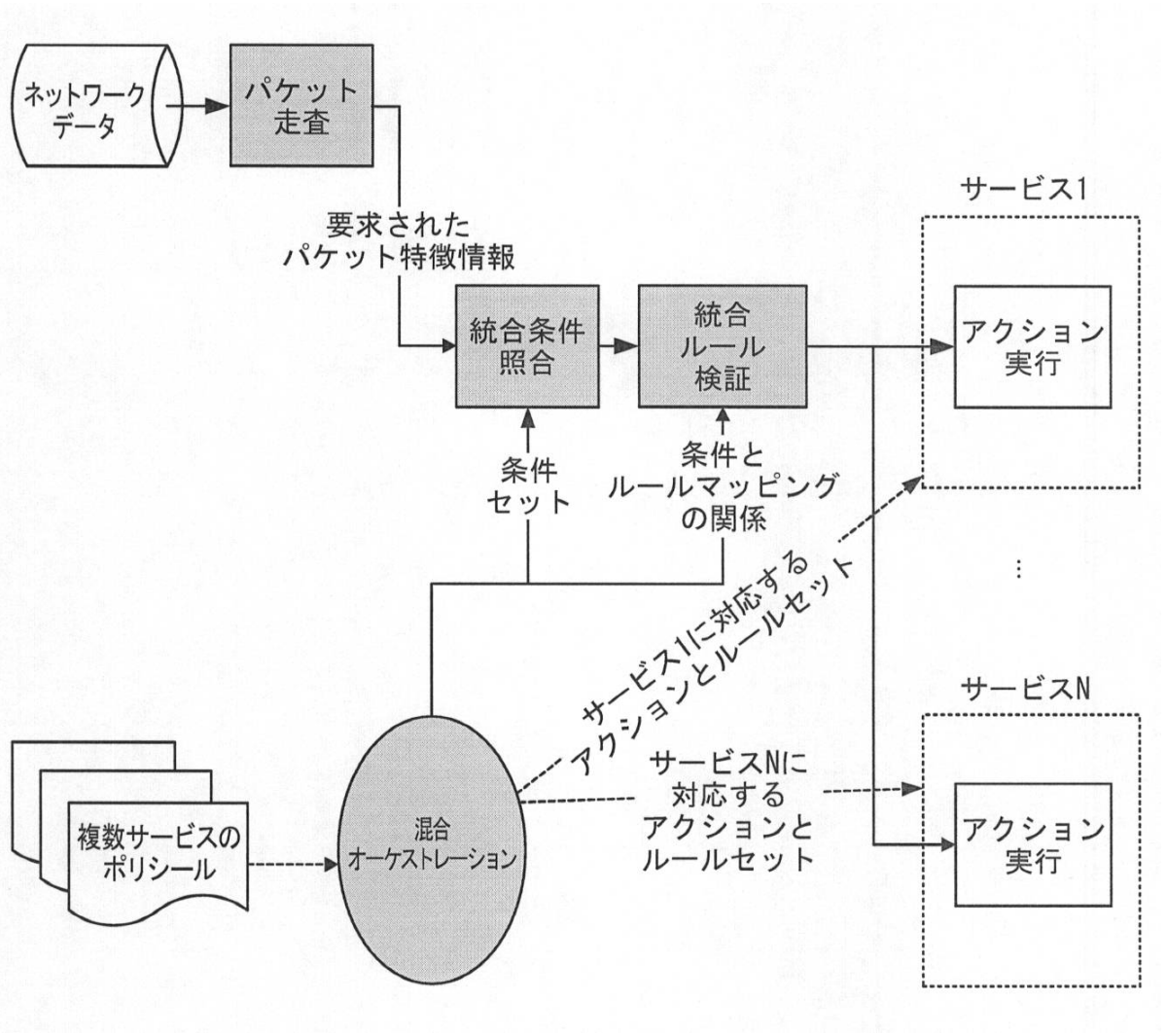
【図１３】


1001
プロセッサ
1003
通信
インターフェース
バス
ネットワーク
メモリ
1002

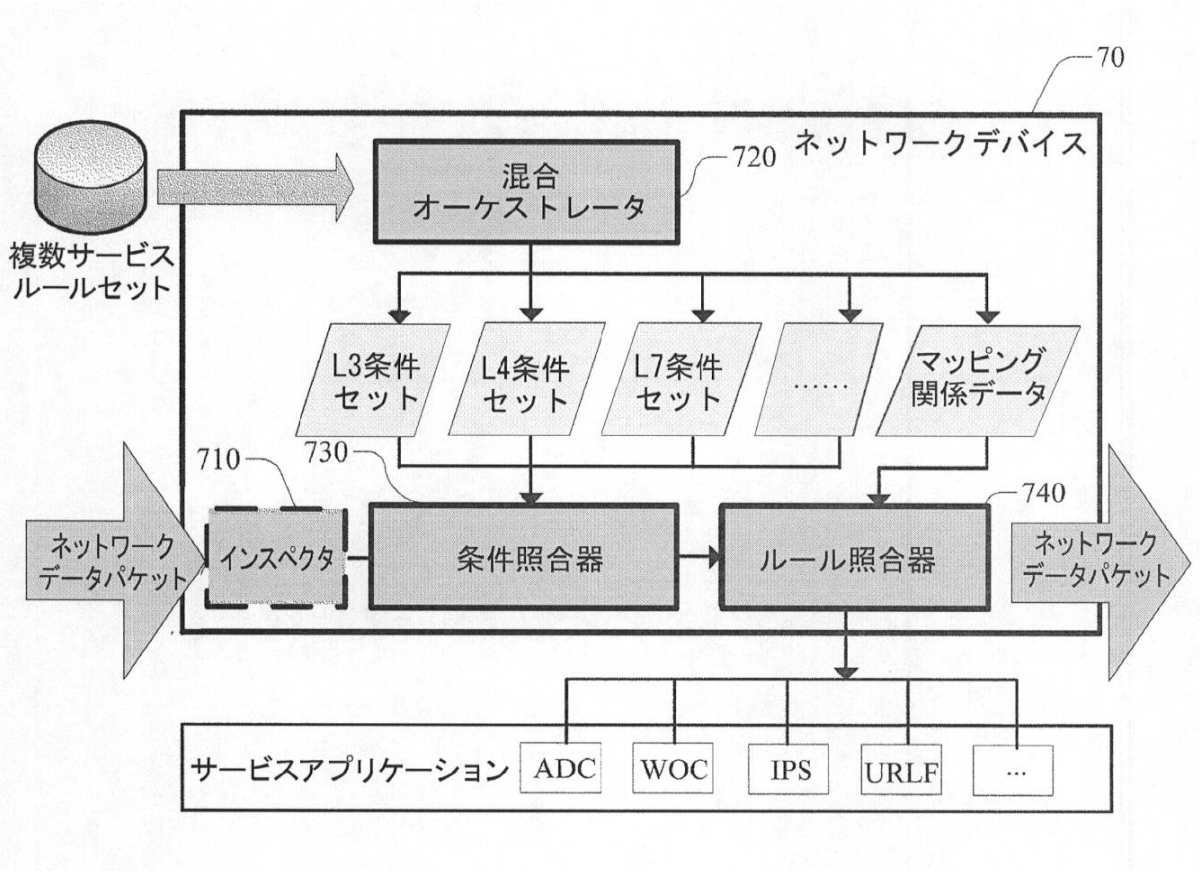
【図３】


データセンタ
支店1
LAN SW ルータ
TOR
サーバ
ルータ
SW
WAN
支店N
記憶装置の
ネットワーク

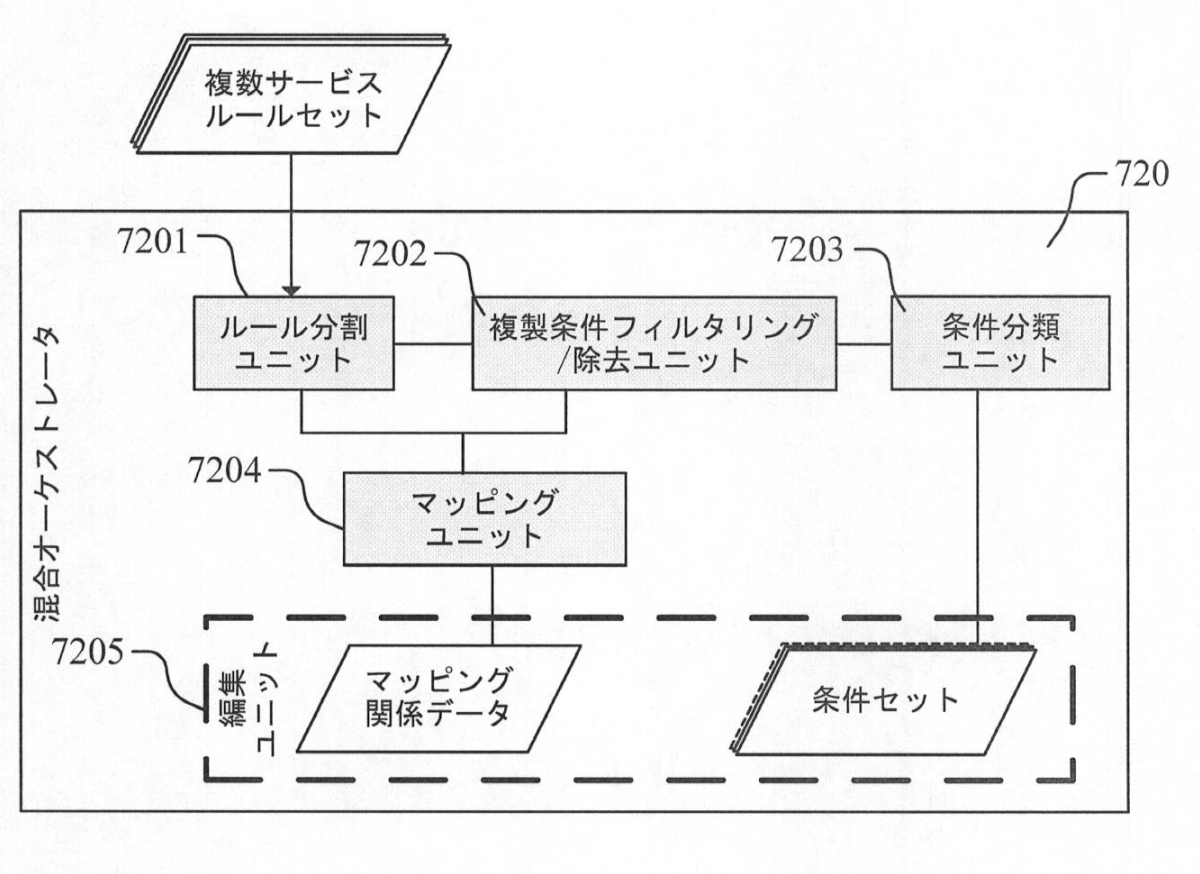
【図４】


ネットワーク
データ
パケット
走査
要求された
パケット特徴情報
統合条件
照合
統合
ルール
検証
サービス1
アクション
実行
条件
セット
条件と
ルールマッピング
の関係
サービス1に対応する
アクションとルールセット
サービスN
サービスNに
対応する
アクションと
ルールセット
複数サービスの
ポリシール
混合
オーケストレーション
アクション
実行

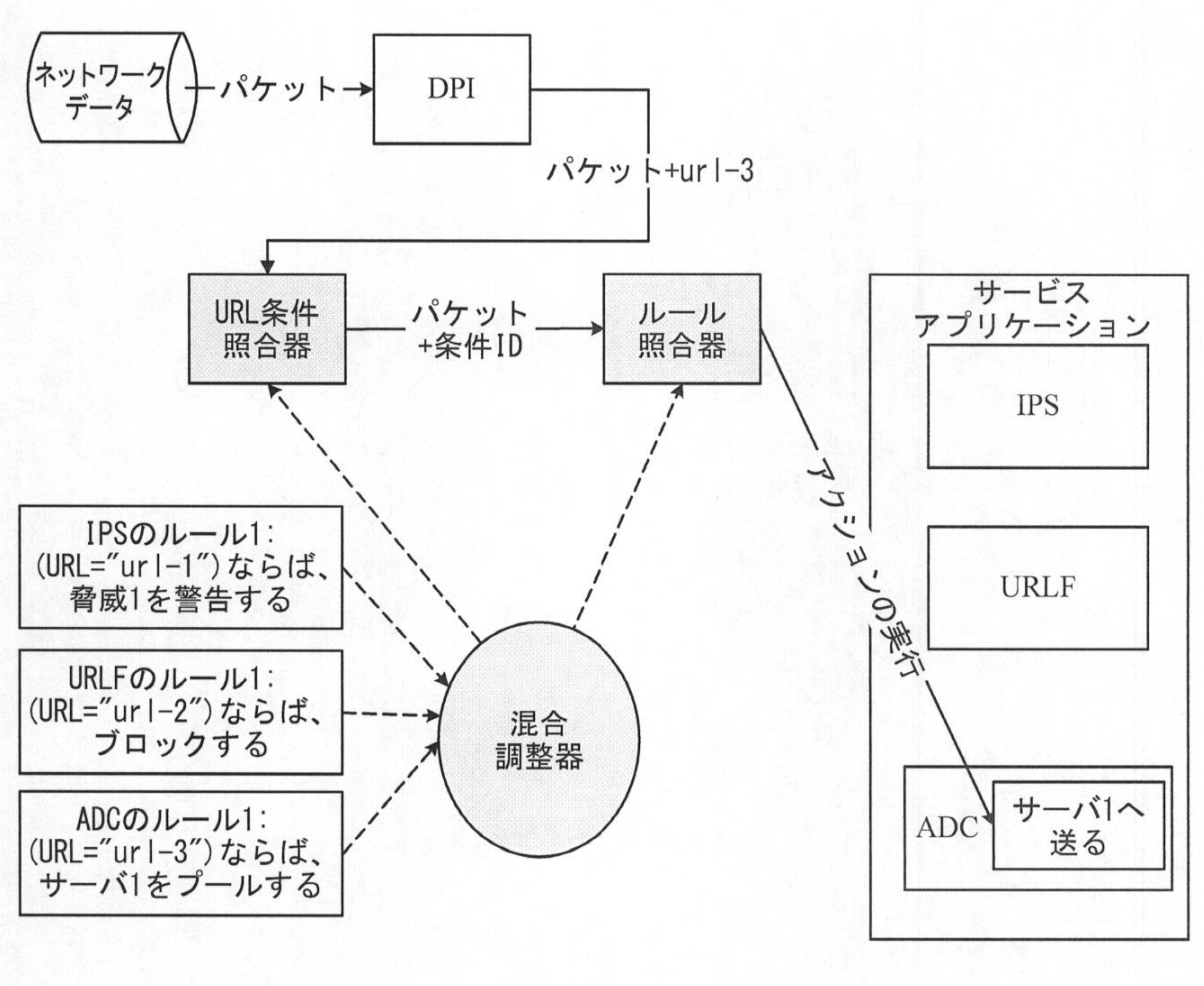
【図７】


70
ネットワークデバイス
720
混合
オーケストレータ
複数サービス
ルールセット
L3条件
セット
L4条件
セット
L7条件
セット
……
マッピング
関係データ
710
730
740
ネットワーク
データパケット
インスペクタ
条件照合器
ルール照合器
ネットワーク
データパケット
サービスアプリケーション
ADC
WOC
IPS
URLF
…

【図８】


複数サービス
ルールセット
720
7201
7202
7203
ルール分割
ユニット
複製条件フィルタリング
/除去ユニット
条件分類
ユニット
7204
マッピング
ユニット
混合オーケストレータ
7205
編集ユニット
マッピング
関係データ
条件セット

【図１２】


ネットワーク
データ
パケット
DPI
パケット+url-3
URL条件
照合器
パケット
+条件ID
ルール
照合器
サービス
アプリケーション
IPS
URLF
ADC
サーバ1へ
送る
アクションの実行
IPSのルール1:
(URL="url-1")ならば、
脅威1を警告する
URLFのルール1:
(URL="url-2")ならば、
ブロックする
ADCのルール1:
(URL="url-3")ならば、
サーバ1をプールする
混合
調整器

フロントページの続き

審査官　木村　雅也

(56)参考文献　米国特許第０７２５７８３３（ＵＳ，Ｂ１）
中国特許出願公開第１８２９１６０（ＣＮ，Ａ）
中国特許出願公開第１０１１９２９６７（ＣＮ，Ａ）
中国特許出願公開第１０２１３０９６５（ＣＮ，Ａ）
中国特許出願公開第１０１８７６９９４（ＣＮ，Ａ）
中国特許出願公開第１０１１４１２９５（ＣＮ，Ａ）
米国特許第８０６５７２１（ＵＳ，Ｂ１）
国際公開第２００６／０９０７８１（ＷＯ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｈ０４Ｌ　１２／７０