(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5937221号
(P5937221)
(45)発行日　平成28年6月22日(2016.6.22)　(24)登録日　平成28年5月20日(2016.5.20)

(51)Int.Cl.　　F I
H04L 12/813 (2013.01)　H04L 12/813
H04L 12/66 (2006.01)　H04L 12/66　A
H04L 12/70 (2013.01)　H04L 12/70　100Z

請求項の数 18　(全 29 頁)

(21)出願番号　特願2014-537342 (P2014-537342)
(86)(22)出願日　平成24年10月19日 (2012.10.19)
(65)公表番号　特表2014-534723 (P2014-534723A)
(43)公表日　平成26年12月18日 (2014.12.18)
(86)国際出願番号　PCT/US2012/061216
(87)国際公開番号　WO2013/059744
(87)国際公開日　平成25年4月25日 (2013.4.25)
審査請求日　平成27年9月25日 (2015.9.25)
(31)優先権主張番号　61/550,344
(32)優先日　平成23年10月21日 (2011.10.21)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　13/655,399
(32)優先日　平成24年10月18日 (2012.10.18)
(33)優先権主張国　米国 (US)

早期審査対象出願

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100103034
弁理士　野河　信久
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】通信ネットワークのためのクラウドコンピューティングエンハンストゲートウェイ

(57)【特許請求の範囲】
【請求項１】
第１のネットワークのネットワークトラフィックを監視することと、
前記ネットワークトラフィックの前記監視に基づいて、前記第１のネットワークに関連するネットワークイベントを検出することと、
第２のネットワークのサーバに前記ネットワークイベントを報告することと、
前記サーバから前記第１のネットワークのためのネットワークポリシー更新を受信することであって、前記ネットワークポリシー更新が、前記サーバに報告された前記ネットワークイベントのイベントタイプに少なくとも部分的に基づく、受信することと、
前記第１のネットワークにおいて前記ネットワークポリシー更新を実装することとを備える方法。
【請求項２】
前記第１のネットワークに関連するネットワークアクティビティを検出することと、
前記サーバに、前記ネットワークアクティビティを報告することと、
前記第２のネットワークから前記第１のネットワークにおいてネットワークアラートを受信することとをさらに備える、請求項１に記載の方法。
【請求項３】
前記監視することと、前記検出することと、前記報告することと、前記受信することと、前記実装することとが、前記第１のネットワークの管理ノードによって実行される、請求項１または２に記載の方法。

【請求項４】
前記管理ノードが前記第１のネットワークのルータを備える、請求項３に記載の方法。
【請求項５】
前記管理ノードが、前記第１のネットワークのルータと、アクセスポイントと、ケーブルモデムと、ネットワークスイッチとから成るグループのうちの少なくとも１メンバを含むコンピュータシステムを備える、請求項３に記載の方法。
【請求項６】
前記第１のネットワークに関連する前記ネットワークイベントを前記検出することが、前記第１のネットワークにおいてオーバーサブスクリプションイベントを検出することと、前記第１のネットワークにおいて未知のパケットストリームを検出することと、前記第１のネットワークにおいてネットワーク障害イベントを検出することと、から成るグループのうちの少なくとも１メンバを備える、請求項１または２に記載の方法。
【請求項７】
前記ネットワークポリシー更新を前記実装することが、前記ネットワークイベントを処理し、解決するために前記第１のネットワークの管理ノードを構成した後に前記ネットワークポリシー更新を実装することを備える、請求項１または２に記載の方法。
【請求項８】
前記ネットワークトラフィックを前記監視することが、前記第１のネットワークの複数のデバイスからワイドエリアネットワークに送られた前記ネットワークトラフィックを監視することと、前記ワイドエリアネットワークのリモートネットワークノードから前記第１のネットワークの前記複数のデバイスに送られた前記ネットワークトラフィックを監視することとを備える、請求項１または２に記載の方法。
【請求項９】
前記ネットワークポリシー更新が、前記イベントタイプおよび第３のネットワークからの前記第２のネットワークにおいて収集された前記イベントタイプに関連するアグリゲートデータの分析に少なくとも部分的に基づき、ここで、前記第１のネットワークおよび前記第３のネットワークは、ローカルエリアネットワークである、請求項１または２に記載の方法。
【請求項１０】
第２のネットワークの第１のルータから、前記第１のルータにおいて前記第２のネットワークのネットワークトラフィックの監視に基づいて検出された第１のネットワークイベントを示す報告メッセージを第１のネットワークのサーバにおいて受信することと、
前記第１のネットワークイベントのイベントタイプを判断することと、
前記イベントタイプに関連するデータを、前記イベントタイプの第２のネットワークイベントを検出した第２のルータからの前に受信されたデータとアグリゲートすることと、
前記アグリゲートされたデータを分析することと、
前記アグリゲートされたデータを分析した結果に基づいて前記イベントタイプに関連するネットワークポリシー更新を判断することと、
前記ネットワークポリシー更新で前記第１のルータを構成するために前記第１のルータに前記ネットワークポリシー更新を送ることとを備える方法。
【請求項１１】
前記イベントタイプを前記判断することは、前記イベントタイプが、前記第２のネットワークにおけるオーバーサブスクリプションイベントと、前記第１のルータにおける未知のパケットストリームの検出と、前記第１のルータからのネットワーク分析報告の受信と、前記第２のネットワークにおけるネットワーク障害イベントの検出と、から成るグループのうちの少なくとも１メンバであると判断することを備える、請求項１０に記載の方法。
【請求項１２】
前記アグリゲートされたデータを分析した前記結果に少なくとも部分的に基づいて前記第１のルータにおいて前記イベントタイプに関連するコンテンツの一時記憶を要求するこ

とをさらに備える、請求項１０に記載の方法。
【請求項１３】
前記ネットワークポリシー更新が、前記第１のルータにおいて検出された前記イベントタイプのネットワークイベントを処理および解決するための動作を示す、請求項１０に記載の方法。
【請求項１４】
ネットワークルータであって、
プロセッサと、
命令を記憶するように構成されたメモリユニットであって、前記命令は、前記プロセッサによって実行されたとき、
第１のネットワークのネットワークトラフィックを監視することと、
前記ネットワークトラフィックの前記監視に基づいて、前記第１のネットワークに関連するネットワークイベントを検出することと、
第２のネットワークのサーバに前記ネットワークイベントを報告することと、
前記サーバから前記ネットワークルータのためのネットワークポリシー更新を受信することであって、前記ネットワークポリシー更新が、前記ネットワークイベントのイベントタイプに少なくとも部分的に基づく、受信することと、
前記ネットワークルータにおいて前記ネットワークポリシー更新を実装することと
を前記ネットワークルータに実行させる、ユニットとを備えるネットワークルータ。
【請求項１５】
前記プロセッサによって実行される前記命令が、
前記第１のネットワークに関連するネットワークアクティビティを検出することと、
前記サーバに、前記ネットワークアクティビティを報告することと、
前記第２のネットワークからネットワークアラートを受信することとを前記ネットワークルータにさらに実行させる、請求項１４に記載のネットワークルータ。
【請求項１６】
前記ネットワークイベントが、前記第１のネットワークにおけるオーバーサブスクリプションイベントと、前記ネットワークルータにおいて受信された未知のパケットストリームと、前記第１のネットワークにおけるネットワーク障害イベントとから成るグループのうちの少なくとも１メンバを備える、請求項１４または１５に記載のネットワークルータ。
【請求項１７】
前記プロセッサによって実行される前記命令が、前記ネットワークルータを構成した後に前記ネットワークポリシー更新を実装することによって前記ネットワークイベントを処理および解決することを前記ネットワークルータにさらに実行させる、請求項１４または１５に記載のネットワークルータ。
【請求項１８】
前記ネットワークトラフィックを監視するための、前記プロセッサによって実行される前記命令が、
前記第１のネットワークの複数のデバイスからワイドエリアネットワークに送られた前記ネットワークトラフィックを監視することと、
前記ワイドエリアネットワークのリモートネットワークノードから前記複数のデバイスに送られた前記ネットワークトラフィックを監視することとを前記ネットワークルータにさらに実行させる、請求項１４または１５に記載のネットワークルータ。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願
[0001]本出願は、２０１１年１０月２１日に出願された米国仮出願第６１／５５０，３４４号、および２０１２年１０月１８日に出願された米国出願第１３／６５５，３９９号

の優先権の利益を主張する。

【０００２】

[0002]本発明の主題の実施形態は、一般に通信ネットワークの分野に関し、より詳細には、通信ネットワークのためのクラウドコンピューティングエンハンストゲートウェイに関する。

【背景技術】

【０００３】

[0003]ホームネットワークまたはオフィスネットワークなど、ローカルエリアネットワーク（ＬＡＮ）は、一般に、ＬＡＮをワイドエリアネットワーク（ＷＡＮ）に接続し、２つのネットワーク間でパケットをルーティングするルータ（またはゲートウェイ）を含む。ＬＡＮ中の様々なネットワークデバイスが、ルータを介してインターネットからの情報にアクセスし、ダウンロードすることができ、ルータは、インターネットにアクセスしている異なるネットワークデバイスからの様々なパケットストリームを管理することができる。ＬＡＮのルータはまた、ルータの動作を構成およびカスタマイズするための様々なネットワーク管理者オプションを提供することができる。しかしながら、ネットワーク管理者は、一般に、ネットワークトラフィックとネットワーク状態とに関してネットワーク管理者に知られている限られた情報に基づいてルータを手動で構成しなければならない。

【発明の概要】

【０００４】

[0004]いくつかの実施形態では、方法は、ローカルエリアネットワーク（ＬＡＮ）のネットワークトラフィックを監視することと、ＬＡＮに関連するネットワークイベントを検出することと、クラウドベースコンピューティングネットワークの１つまたは複数のサーバにネットワークイベントを報告することと、クラウドベースコンピューティングネットワークの１つまたは複数のサーバからＬＡＮのためのネットワークポリシー更新を受信することであって、ネットワークポリシー更新が、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに報告されたネットワークイベントのタイプに少なくとも部分的に基づく、受信することと、ＬＡＮにおいてネットワークポリシー更新を実装することとを備える。

【０００５】

[0005]いくつかの実施形態では、前記監視することと、前記検出することと、前記報告することと、前記受信することと、前記実装することとは、ＬＡＮのネットワークトラフィック管理ノードによって実行される。

【０００６】

[0006]いくつかの実施形態では、ネットワークトラフィック管理ノードはＬＡＮのルータを備える。

【０００７】

[0007]いくつかの実施形態では、ネットワークトラフィック管理ノードは、ＬＡＮのルータと、アクセスポイントと、ケーブルモデムと、ネットワークスイッチとのうちの１つまたは複数を含むコンピュータシステムを備える。

【０００８】

[0008]いくつかの実施形態では、ＬＡＮに関連するネットワークイベントを前記検出することは、ＬＡＮにおいてオーバーサブスクリプションイベントを検出することと、ＬＡＮにおいて未知のパケットストリームを検出することと、ＬＡＮにおいてネットワーク障害イベントを検出することとのうちの少なくとも１つを備える。

【０００９】

[0009]いくつかの実施形態では、ネットワークポリシー更新を前記実装することは、ネットワークイベントを処理し、解決するためにＬＡＮのネットワークトラフィック管理ノードの構成の後にネットワークポリシー更新を実装することを備える。

【００１０】

[0010]いくつかの実施形態では、ＬＡＮのネットワークトラフィックを前記監視するこ

とは、ＬＡＮの複数のネットワークデバイスのうちの１つまたは複数からワイドエリアネットワークに送られたネットワークトラフィックを監視することと、ワイドエリアネットワークのリモートネットワークノードからＬＡＮの複数のネットワークデバイスのうちの１つまたは複数に送られたネットワークトラフィックを監視することとを備える。

【００１１】

[0011]いくつかの実施形態では、クラウドベースコンピューティングネットワークの１つまたは複数のサーバから受信されたネットワークポリシー更新は、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに報告されたネットワークイベントのタイプに基づき、および複数の追加のローカルエリアネットワークからクラウドベースコンピューティングネットワークにおいて収集されたネットワークイベントのタイプに関連するアグリゲート（aggregate）データの分析に基づく。

【００１２】

[0012]いくつかの実施形態では、本方法は、ＬＡＮに関連するネットワークアクティビティを検出することと、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、ＬＡＮに関連するネットワークアクティビティを報告することと、クラウドベースコンピューティングネットワークからＬＡＮにおいてネットワークアラートを受信することとをさらに備える。

【００１３】

[0013]いくつかの実施形態では、方法は、ローカルエリアネットワーク（ＬＡＮ）のネットワークトラフィック管理ノードにおいて検出された複数のパケットストリームを分類することと、ネットワークトラフィック管理ノードにおいて未知のパケットストリームを検出することと、未知のパケットストリームのためのデフォルト分類を選択することと、ネットワークトラフィック管理ノードからクラウドベースコンピューティングネットワークの１つまたは複数のサーバに、未知のパケットストリームに関連する情報を報告することと、クラウドベースコンピューティングネットワークから未知のパケットストリームのためのパケットストリーム検出ポリシー更新をネットワークトラフィック管理ノードにおいて受信することと、未知のパケットストリームを後で検出し、分類するためにネットワークトラフィック管理ノードにおいてパケットストリーム検出ポリシー更新を実装することとを備える。

【００１４】

[0014]いくつかの実施形態では、ネットワークトラフィック管理ノードにおいて検出された複数のパケットストリームを前記分類することは、複数のパケットストリームに関連するパケットストリーム特性を検出することと、対応するパケットストリーム特性に少なくとも部分的に基づいて複数のパケットストリームの各々に関連するアプリケーションを判断することと、パケットストリームの各々に関連するアプリケーションに少なくとも部分的に基づいて複数のパケットストリームの各々を分類することとを備える。

【００１５】

[0015]いくつかの実施形態では、ネットワークトラフィック管理ノードにおいて検出された複数のパケットストリームを前記分類することは、複数のパケットストリームの各々に関連するアプリケーションと、複数のパケットストリームの各々に関連するアプリケーションタイプとのうちの少なくとも１つに基づいて複数のパケットストリームを分類することを備える。

【００１６】

[0016]いくつかの実施形態では、ネットワークトラフィック管理ノードにおいて未知のパケットストリームを前記検出することと、未知のパケットストリームのためのデフォルト分類を前記選択することとは、ネットワークトラフィック管理ノードにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、アプリケーションが未知であると判断したことに応答して未知のパケットストリームのためのデフォルト分類を選択することとを備える。

【００１７】

[0017]いくつかの実施形態では、ネットワークトラフィック管理ノードにおいて未知のパケットストリームを前記検出することと、未知のパケットストリームのためのデフォルト分類を前記選択することとは、ネットワークトラフィック管理ノードにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、未知のパケットストリームに関連するアプリケーションタイプを判断することと、未知のパケットストリームに関連するアプリケーションタイプに基づいて未知のパケットストリームのためのデフォルト分類を選択することとを備える。

【００１８】

[0018]いくつかの実施形態では、ネットワークトラフィック管理ノードからクラウドベースコンピューティングネットワークの１つまたは複数のサーバに未知のパケットストリームに関連する情報を前記報告することは、未知のパケットストリームに関連するパケットストリーム特性を報告することを備える。

【００１９】

[0019]いくつかの実施形態では、本方法は、パケットストリーム検出ポリシー更新を受信することに加えて、未知のパケットストリームに関連するアプリケーションと、未知のパケットストリームの分類とを示す情報を受信することをさらに備える。

【００２０】

[0020]いくつかの実施形態では、未知のパケットストリームを後で検出し、分類するためにネットワークトラフィック管理ノードにおいてパケットストリーム検出ポリシー更新を前記実装することは、パケットストリーム検出ポリシー更新に従って前に未知であったパケットストリームに関連するパケットストリーム特性をネットワークトラフィック管理ノードにおいて検出することと、パケットストリーム検出ポリシー更新に従ってパケットストリーム特性に関連するアプリケーションを判断することと、パケットストリーム特性に関連するアプリケーションに基づいて前に未知であったパケットストリームのための分類を選択することとを備える。

【００２１】

[0021]いくつかの実施形態では、方法は、ローカルエリアネットワーク（ＬＡＮ）のルータから、そのルータにおいて検出されたネットワークイベントを示す報告メッセージをクラウドベースコンピューティングネットワークの１つまたは複数のサーバにおいて受信することと、ＬＡＮにおいてルータによって検出されたネットワークイベントのタイプを判断することと、ルータによって報告されたネットワークイベントのタイプに関連するデータを、ネットワークイベントのタイプを同じく検出した他のルータからの前に受信されたデータとアグリゲートすることと、ネットワークイベントのタイプに関連するアグリゲートデータを分析することと、ネットワークイベントのタイプに関連するアグリゲートデータの分析の結果に基づいてネットワークイベントのタイプに関連するネットワークポリシー更新を判断することと、ネットワークイベントのタイプに関連するネットワークポリシー更新でルータを構成するためにＬＡＮのルータにネットワークポリシー更新を送ることとを備える。

【００２２】

[0022]いくつかの実施形態では、ＬＡＮにおいてルータによって検出されたネットワークイベントのタイプを前記判断することは、ネットワークイベントのタイプが、ＬＡＮにおけるオーバーサブスクリプションイベントと、ルータにおける未知のパケットストリームの検出と、ルータからのネットワーク分析報告の受信と、ＬＡＮにおけるネットワーク障害イベントの検出とのうちの１つであると判断することを備える。

【００２３】

[0023]いくつかの実施形態では、本方法は、ルータにおけるコンテンツの一時記憶を要求するためにネットワークイベントのタイプに関連するアグリゲートデータの分析の結果に基づいてＬＡＮのルータにコマンドを送ることをさらに備える。

【００２４】

[0024]いくつかの実施形態では、ネットワークイベントのタイプに関連するアグリゲー

トデータの分析の結果に基づいてネットワークイベントのタイプに関連するネットワークポリシー更新を前記判断することは、ルータにおいて検出されたネットワークイベントのタイプを処理し、解決するためにネットワークポリシー更新を判断することを備える。

【００２５】

[0025]いくつかの実施形態では、ネットワークルータは、１つまたは複数のプロセッサと、１つまたは複数の命令を記憶するように構成された１つまたは複数のメモリユニットであって、命令は、１つまたは複数のプロセッサによって実行されたとき、ローカルエリアネットワーク（ＬＡＮ）のネットワークトラフィックを監視することと、ＬＡＮに関連するネットワークイベントを検出することと、クラウドベースコンピューティングネットワークの１つまたは複数のサーバにネットワークイベントを報告することと、クラウドベースコンピューティングネットワークの１つまたは複数のサーバからネットワークルータのためのネットワークポリシー更新を受信することであって、ネットワークポリシー更新が、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに報告されたネットワークイベントのタイプに少なくとも部分的に基づく、受信することと、ネットワークルータにおいてネットワークポリシー更新を実装することとを備える動作をネットワークルータに実行させる、１つまたは複数のメモリユニットとを備える。

【００２６】

[0026]いくつかの実施形態では、ＬＡＮに関連するネットワークイベントは、ＬＡＮにおけるオーバーサブスクリプションイベントと、ネットワークルータにおいて受信された未知のパケットストリームと、ＬＡＮにおけるネットワーク障害イベントとのうちの１つを備える。

【００２７】

[0027]いくつかの実施形態では、１つまたは複数のプロセッサによって実行される１つまたは複数の命令は、ネットワークルータの構成の後にネットワークポリシー更新を実装することによってネットワークイベントを処理し、解決することをさらに備える動作をネットワークルータに実行させる。

【００２８】

[0028]いくつかの実施形態では、１つまたは複数のプロセッサによって実行される１つまたは複数の命令は、ＬＡＮに関連するネットワークアクティビティを検出することと、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、ＬＡＮに関連するネットワークアクティビティを報告することと、クラウドベースコンピューティングネットワークからネットワークルータにおいてネットワークアラートを受信することとをさらに備える動作をネットワークルータに実行させる。

【００２９】

[0029]いくつかの実施形態では、ネットワークルータは、プロセッサと、プロセッサに結合されたネットワーク監視ユニットであって、ローカルエリアネットワーク（ＬＡＮ）のネットワークルータにおいて検出された複数のパケットストリームを分類することと、ネットワークルータにおいて受信された未知のパケットストリームを検出することと、未知のパケットストリームのためのデフォルト分類を選択することと、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、未知のパケットストリームに関連する情報を報告することと、未知のパケットストリームのためのパケットストリーム検出ポリシー更新をクラウドベースコンピューティングネットワークから受信することと、未知のパケットストリームを後で検出し、分類するためにネットワークルータにおいてパケットストリーム検出ポリシー更新を実装することとを行うように構成されたネットワーク監視ユニットとを備える。

【００３０】

[0030]いくつかの実施形態では、ネットワークルータにおいて検出された複数のパケットストリームを分類するように構成されたネットワーク監視ユニットは、複数のパケットストリームに関連するパケットストリーム特性を検出することと、対応するパケットストリーム特性に少なくとも部分的に基づいて複数のパケットストリームの各々に関連するア

プリケーションを判断することと、パケットストリームの各々に関連するアプリケーションに少なくとも部分的に基づいて複数のパケットストリームの各々を分類することとを行うように構成されたネットワーク監視ユニットを備える。

【００３１】

[0031]いくつかの実施形態では、ネットワークルータにおいて検出された複数のパケットストリームを分類するように構成されたネットワーク監視ユニットは、複数のパケットストリームの各々に関連するアプリケーションと、複数のパケットストリームの各々に関連するアプリケーションタイプとのうちの少なくとも１つに基づいて複数のパケットストリームを分類するように構成されたネットワーク監視ユニットを備える。

【００３２】

[0032]いくつかの実施形態では、ネットワークトラフィック管理ノードにおいて未知のパケットストリームを検出することと、未知のパケットストリームのためのデフォルト分類を選択することとを行うように構成されたネットワーク監視ユニットは、ネットワークルータにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、アプリケーションが未知であると判断したことに応答して未知のパケットストリームのためのデフォルト分類を選択することとを行うように構成されたネットワーク監視ユニットを備える。

【００３３】

[0033]いくつかの実施形態では、ネットワークルータにおいて未知のパケットストリームを検出することと、未知のパケットストリームのためのデフォルト分類を選択することとを行うように構成されたネットワーク監視ユニットは、ネットワークルータにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、未知のパケットストリームに関連するアプリケーションタイプを判断することと、未知のパケットストリームに関連するアプリケーションタイプに基づいて未知のパケットストリームのためのデフォルト分類を選択することとを行うように構成されたネットワーク監視ユニットを備える。

【００３４】

[0034]いくつかの実施形態では、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、未知のパケットストリームに関連する情報を報告するように構成されたネットワーク監視ユニットは、未知のパケットストリームに関連するパケットストリーム特性を報告するように構成されたネットワーク監視ユニットを備える。

【００３５】

[0035]いくつかの実施形態では、未知のパケットストリームの後での検出および分類のためにネットワークルータにおいてパケットストリーム検出ポリシー更新を実装するように構成されたネットワーク監視ユニットは、パケットストリーム検出ポリシー更新に従って前に未知であったパケットストリームに関連するパケットストリーム特性を検出することと、パケットストリーム検出ポリシー更新に従ってパケットストリーム特性に関連するアプリケーションを判断することと、パケットストリーム特性に関連するアプリケーションに基づいて前に未知であったパケットストリームのための分類を選択することとを行うように構成されたネットワーク監視ユニットを備える。

【００３６】

[0036]いくつかの実施形態では、命令を記憶した１つまたは複数の機械可読記憶媒体であって、命令は、１つまたは複数のプロセッサによって実行されたとき、ローカルエリアネットワーク（ＬＡＮ）において検出された複数のパケットストリームを分類することと、ＬＡＮにおいて未知のパケットストリームを検出することと、未知のパケットストリームのためのデフォルト分類を選択することと、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、未知のパケットストリームに関連する情報を報告することと、クラウドベースコンピューティングネットワークから未知のパケットストリームのためのパケットストリーム検出ポリシー更新を受信することと、未知のパケットストリームを後で検出し、分類するためにパケットストリーム検出ポリシー更新を実装するこ

ととを備える動作を１つまたは複数のプロセッサに実行させる、１つまたは複数の機械可読記憶媒体が提供される。

【００３７】

[0037]いくつかの実施形態では、ＬＡＮにおいて検出された複数のパケットストリームを分類する前記動作は、複数のパケットストリームの各々に関連するアプリケーションと、複数のパケットストリームの各々に関連するアプリケーションタイプとのうちの少なくとも１つに基づいて複数のパケットストリームを分類することを備える。

【００３８】

[0038]いくつかの実施形態では、未知のパケットストリームを検出することと、未知のパケットストリームのためのデフォルト分類を選択することとの前記動作は、ＬＡＮにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、アプリケーションが未知であると判断したことに応答して未知のパケットストリームのためのデフォルト分類を選択することとを備える。

【００３９】

[0039]いくつかの実施形態では、未知のパケットストリームを検出することと、未知のパケットストリームのためのデフォルト分類を選択することとの前記動作は、ＬＡＮにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、未知のパケットストリームに関連するアプリケーションタイプを判断することと、未知のパケットストリームに関連するアプリケーションタイプに基づいて未知のパケットストリームのためのデフォルト分類を選択することとを備える。

【００４０】

[0040]添付の図面を参照することによって、本実施形態はより良く理解され得、多数の目的、特徴、および利点が当業者に明らかになり得る。

【図面の簡単な説明】

【００４１】

【図１】[0041]いくつかの実施形態による、通信ネットワークのためのクラウドコンピューティングエンハンストルータを示す例示的なブロック図。

【図２】[0042]いくつかの実施形態による、図１に示したローカルエリアネットワークのためのクラウドコンピューティングエンハンストルータを実装するための例示的な動作を示す流れ図。

【図３】[0043]いくつかの実施形態による、図１に示したクラウドコンピューティングエンハンストルータシステムを実装するための例示的な動作を示す流れ図。

【図４】[0044]いくつかの実施形態による、図１～図３に記載したクラウドコンピューティングエンハンストルータにおいてパケットストリーム検出を実装するための例示的な動作を示す流れ図。

【図５】[0045]いくつかの実施形態による、ローカルエリアネットワークルーティング、監視およびクラウドベースサポートのための機構を含むネットワークデバイスの一実施形態のブロック図。

【発明を実施するための形態】

【００４２】

[0046]以下の説明は、本発明の主題の技法を実施する例示的なシステム、方法、技法、命令シーケンスおよびコンピュータプログラム製品を含む。ただし、説明する実施形態は、これらの具体的な詳細なしに実施され得ることを理解されたい。たとえば、例では、クラウドコンピューティングエンハンストルータをホームローカルエリアネットワーク（ＬＡＮ）中で利用することに言及するが、他の例では、クラウドコンピューティングエンハンストルータは、オフィスネットワーク、集合住宅ネットワーク、大学ネットワークなど、任意の好適なタイプのネットワークにおいて使用され得る。他の例では、説明を不明瞭にしないために、よく知られている命令インスタンス、プロトコル、構造および技法を詳細に図示していない。

【００４３】

[0047]通信ネットワークのためのルータ（またはゲートウェイ）はますます複雑になっている。同時に、ルータのコストを低減するために競争が進んでいる。その結果、性能の観点と機能の観点の両方から、今日のホームＬＡＮルータの処理能力は、ルータの能力を向上させ得る高性能なアルゴリズムを活用するのに十分でない。さらに、すべてのルータは、本質的に、処理能力、ストレージ、ソフトウェア、および他の機能など、利用可能なリソースの量が限られている。

【００４４】

[0048]図１は、いくつかの実施形態による、通信ネットワークのためのクラウドコンピューティングエンハンストルータを示す例示的なブロック図である。ＬＡＮ１００は、複数のネットワークデバイス１０２と、ルータ１１０とを備える。複数のネットワークデバイス１０２は、ノートブックコンピュータ、タブレットコンピュータ、モバイルフォン、デスクトップコンピュータ、デジタルカメラ、テレビジョン、ゲーミングコンソール、スマートアプライアンス、および他の好適なデバイスなど、様々なタイプのワイヤードネットワーキングデバイスおよびワイヤレスネットワーキングデバイスを含み得る。ルータ１１０（またはゲートウェイ）は、通信ネットワークとの間でパケットを受信し、ルーティングする通信ネットワーク中のノードである。ルータ１１０は、２つ以上のネットワークに関連するパケットを受信し、処理し、ルーティングするネットワーク間のネットワークトラフィック管理ノードである。ただし、他の実施形態では、ＬＡＮ１００は、（１つまたは複数の）ネットワークのための様々な機能を実行するように構成された他のタイプのネットワークトラフィック管理ノードおよび／またはネットワークトラフィック管理ノード、たとえば、図１～図５に関して本明細書で説明する機能をも実装し得る、ケーブルモデム、ゲートウェイ／ルータ、ワイヤレスアクセスポイント、ブリッジ、スイッチおよび／またはストレージのうちの１つまたは複数を組み込むサーバコンピュータシステムを含み得ることに留意されたい。図１に示すように、ルータ１１０は、ＬＡＮ１００のネットワークデバイス１０２が、ＷＡＮ１４０にアクセスし、ＷＡＮ１４０からコンテンツを受信することを可能にする。ＬＡＮ１００は、インターネット１２０と概して呼ばれることがあるＷＡＮ１４０を形成する多くのＬＡＮのうちの１つである。図示のように、ＷＡＮ１４０は、サーバ（ならびに他のネットワークデバイスおよびソフトウェア）の様々なネットワークをも含み得る。一例では、サーバのネットワークは、本明細書ではクラウドコンピューティングネットワーク１５０（またはクラウド１５０）として参照する、インターネット１２０上のクラウドコンピューティングを実装することができる。ルータ１１０は、ＬＡＮ１００が、インターネット１２０を介してクラウド１５０によって与えられる様々なサービスの利益を得ることを可能にし得る。他のＬＡＮをサービスする様々な他のルータ（たとえば、ルータ１８５および１９５）もクラウド１５０に接続し得る。すべてのルータがインターネットに接続されるので、クラウド１５０において利用可能なクラウドコンピューティングリソースを使用してルータを増強することにより、より高性能なルータが得られ、またルータのコストが低減し得る。

【００４５】

[0049]クラウド１５０は、インターネット１２０に接続された様々なルータから統計値を収集し、ルータ中で動作するネットワーク管理アルゴリズムを改良するためにクラウドソーシングの概念を使用するように構成され得、それにより、クラウド１５０に接続されたすべての他のルータの経験を活用するよりスマートな「学習」ルータが得られ得る。いくつかの実施形態では、ルータ１１０（また、ルータ１８５および１９５など、様々なルータ）は、様々なタイプのネットワークイベント、統計的情報および他のネットワークアクティビティをクラウド１５０に報告することができる。たとえば、以下でさらに説明するように、ルータ１１０は、未知であるルータにおいて受信されたパケットストリームと、ルータによって検出されたＬＡＮ１００中のオーバーサブスクリプションイベントとに関連する情報を報告し得る。クラウド１５０は、様々なルータによって報告されたネットワークイベントに関連するデータをアグリゲートし、そのデータを分析してルータポリシーおよびプロシージャを改善し、更新する（たとえば、ルータに記憶されたネットワーク

管理アルゴリズムを更新する）ことができる。ルータ１１０はまた、クラウドがＬＡＮ１００上でネットワーク分析を実行し、ルータにネットワークアラートを送ることを可能にするために、ネットワークアクティビティ報告をクラウド１５０に送ることができる。ルータ１１０がネットワークアクティビティを報告することに加えて、ルータ１１０はクラウド１５０におけるストレージを利用することができる。クラウド１５０は、サービスを個人化し、ＬＡＮ１００とＬＡＮ１００のユーザとに示唆を与える（たとえば、オフピーク夜間時間中に一般的なファイルおよびソフトウェアダウンロードを実行する）ために、ネットワークアクティビティとストレージ利用とを監視することができる。

【００４６】

[0050]いくつかの実装形態では、ルータ１１０は、ルータ１１０を通してＷＡＮ１４０との間でパケットストリームを生成し、処理しているアプリケーションをインテリジェントに検出するように構成され得る。たとえば、ルータ１１０は、ルータ１１０を通してパケットをアクティブに送っている、（たとえば、第１のネットワークデバイス１０２中に実装された）Ｎｅｔｆｌｉｘ（登録商標）ビデオストリーミングアプリケーションからのパケットストリームと、ファイルダウンロードアプリケーション（たとえば、第２のネットワークデバイス１０２中に実装されたビットトレント（bit torrent））からのパケットストリームとを検出し得る。いくつかの例では、ビデオストリーミングサービス（または他のコンテンツ）を提供したサーバは、ビデオコンテンツを、ルータ１１０を介してＬＡＮ１００に、およびネットワークデバイス１０２のうちの１つにおいて実行されているクライアントアプリケーションにストリーミングし得る。ただし、場合によっては、ルータ１１０は、未知のパケットストリームを検出するか、またはパケットストリームが認識不可能であると判断し得る。他の場合には、知られているストリーム「フィンガープリント（fingerprints）」またはストリーム特性をもつ、知られているアプリケーションは、それが生成するパケットストリームを変更し得（すなわち、ストリーム特性を変更し得）、それにより、前に検出可能であったパケットストリームが検出不可能になり得る。一実装形態では、ルータ１１０は、クラウドコンピューティングネットワーク１５０の１つまたは複数のサーバにすべての未知のパケットストリームに関する情報（たとえば、ストリーム特性）を送るように構成され得る。クラウド１５０は、未知のパケットストリームに関する様々な他のルータから収集された関係するアグリゲートデータにアクセスすることができる。関係するアグリゲートデータに対してパケット検査および／または統計的分析を実行することに基づいて、またインターネット１２０上の様々なサービスプロバイダからのパケットストリームを連続的に監視することに基づいて、クラウド１５０は、未知のパケットストリームをインテリジェントに識別することができる。次いで、クラウド１５０は、新しい検出規則をルータ１１０に（また、ルータ１８５および１９５などの他のルータに）ダウンロードすることができる。

【００４７】

[0051]いくつかの実装形態では、ルータ１１０は、インターネットを介して送られる最も一般的なアプリケーションパケットストリーム（たとえば、トップ１００のアプリケーション）を検出するようにアルゴリズムで構成され得る。ルータ１００を通過した他の未知のパケットストリームは、検出および識別のためにクラウド１５０に送られ得る。一例では、未知のパケット情報がさらなる分析のためにクラウド１５０に送られた後、ルータ１１０は、未知のパケットストリームにデフォルト分類を一時的に割り当て得る。たとえば、ルータ１１０は、パケットストリームに関連する特定のアプリケーションを検出することが可能でないことがあるが、ルータ１１０は、パケットストリームがストリーミングビデオであると判断し、ビデオトラフィックのためのデフォルト分類を一時的に割り当てることができる。言い換えれば、ルータ１１０は、特定のアプリケーションを検出することが可能でないことがあるが、ルータ１１０は、アプリケーションタイプ（たとえば、ビデオトラフィック）を検出し、アプリケーションタイプに基づいて未知のパケットストリームのためのデフォルト分類を選択し得る。クラウド１５０が新しい検出規則を判断した後に、その結果はルータ１１０に返送され得、ルータ１１０は、新しい検出規則を実装し

てパケットストリームを適切に識別し、処理することができる。これは自己帰還ループを生じ、ルータ１１０は、検出アルゴリズムを実行し、クラウド１５０に送られた統計値を収集し、様々なルータからの統計値はクラウド１５０においてアグリゲートされ、分析され、新しい検出アルゴリズムがその後に判断され、すべてのルータに送出される。

【００４８】

[0052]いくつかの実装形態では、ルータ１１０はまた、ＬＡＮ１００中のオーバーサブスクリプションイベントを報告することができる。ルータ１１０は、ルータがＬＡＮ１００中の様々なタイプのオーバーサブスクリプションイベントをどのように処理したかを報告することができる。一例では、ＬＡＮ１００の何人かのユーザが、ＷＡＮ１４０からルータ１１０を通してＬＡＮの異なるネットワークデバイス１０２に５つの映画を同時にストリーミングするために５つの異なるビデオストリーミングアプリケーションを開始し得る。この状況では、ネットワークは、５つの異なるビデオストリーミングアプリケーションのための５つの異なるパケットストリームをサポートするのに十分な帯域幅をおそらく有さず、したがって、ルータはオーバーサブスクリプションイベントを検出する。ルータ１１０は、オーバーサブスクリプションイベントを解決するために１つの技法を実装し、使用された技法および結果をクラウド１５０に報告することができる。たとえば、ルータ１１０は、すべてのビデオストリームの帯域幅をある割合（たとえば、１０～２０％）だけ減少させることを判断することができる。クラウド１５０中のサーバは、同様のシナリオについて他のルータから収集されたアグリゲートデータを使用し、分析を実行し、ルータ１１０が遭遇したオーバーサブスクリプションイベントを処理するためのより良い技法があると判断することができる。クラウド１５０中のサーバは、次いで、新しいオーバーサブスクリプション解決技法に関する詳細をルータ１１０に与えることができ、すなわち、クラウド１５０の１つまたは複数のサーバが、そのタイプのオーバーサブスクリプションイベントを解決するための新しいアルゴリズムを用いてルータ１１０をプログラムすることができる。たとえば、すべての５つのビデオストリームの帯域幅を１５％だけ低減する代わりに、ルータ１１０は、ビデオストリームのうちの４つのために最適な帯域幅を維持し、ビデオストリームのうちの１つの帯域幅を最小許容レベルに低減すべきであると、クラウド１５０は判断し得る。

【００４９】

[0053]いくつかの実装形態では、ルータ１１０はまた、ネットワークアクティビティの一部または全部をクラウド１５０に報告し、データの大部分またはすべてをクラウド１５０に記憶することができる。ルータ１１０から報告を検出し、データを収集したことに応答して、クラウド１５０は、ＬＡＮ１００上でネットワーク分析を実行し、またネットワークアラートを送ることができる。クラウド１５０は、限られたリソースおよびストレージなど、ローカルネットワークルータまたは他のデバイスが本質的に有し得る制限なしに、数週間、数か月間、および数年間にわたってネットワーク分析を実行することができる。一例では、ネットワークアクティビティ報告に基づいて、クラウド１５０は、あるデバイスまたはデバイスの種類が、デバイスがアクティブである（たとえば、デバイスが連続的に送信する）ときに不相応な量の帯域幅を使用していると判断することができる。クラウド１５０は、ＬＡＮ１００を監視し、デバイスがアクティブであり、そのような挙動を示すことをクラウド１５０が検出したとき、クラウド１５０はネットワークアラートを送ることができる。別の例では、クラウド１５０は、アップストリームトラフィックが過負荷をかけられていることを検出し、アップストリームトラフィックを低減し潜在的により良いパフォーマンスを得るために、ルータ１１０が広告された利用可能な帯域幅を半分に（たとえば、１０ｍｂｐｓから５ｍｂｐｓに）低減すべきことを示唆するネットワークアラートをルータ１１０に送ることができる。ルータ１１０は他のタイプのネットワークイベントを報告することができることに留意されたい。場合によっては、ルータ１１０はクラウド１５０にネットワーク障害を報告することができ、クラウド１５０は、アグリゲートデータに基づいて解決プロシージャを判断し、ルータ１１０に解決策（たとえば、構成更新または新しい解決プロシージャステップ）を報告することができる。いくつかの実装

形態では、クラウド１５０はＬＡＮ１００に関連するネットワークアクティビティおよびネットワークイベントの大部分またはすべてをルータ１１０から受信しているので、クラウド１５０は、他の個人化されたサービスをもＬＡＮ１００に与えることができる。たとえば、クラウド１５０は、ネットワークデバイス１０２のうちの１つまたは複数中のソフトウェアプログラム（たとえば、Ａｄｏｂｅ（登録商標）Ａｃｒｏｂａｔ（登録商標））が自動更新のために構成されている（またはユーザが更新を定期的に確認する）ことを検出することができる。ユーザが更新をダウンロードしているという情報をクラウド１５０が別のルータから受信したとき、クラウド１５０は、過去にアプリケーションを更新したことがある他のルータに、更新が利用可能であり、トラフィックが軽いとき（たとえば、オフピーク時）にルータが更新をダウンロードすべきである（たとえば、更新をキャッシュに一時的に記憶する）ことを通知することができる。別の例では、クラウド１５０は、ある著者からの電子ブックがリリースされたとき、ユーザの１人がその電子ブックをダウンロードすることを検出することができる。このアクティビティに基づいて、クラウド１５０は、著者が新しい電子ブックをリリースしたとき、ユーザがＷＡＮリンクを使用せずにローカルに電子ブックにアクセスし、ダウンロードすることができるように、電子ブックをルータ１１０のローカルストレージに自動的にダウンロードすることができる。

【００５０】

[0054]図１に示すように、いくつかの実施形態では、ルータ１１０は、ネットワーク監視ユニット１１２と、１つまたは複数のプロセッサ１１５と、メモリユニット１１８とを含み得る。ルータ１１０のネットワーク監視ユニット１１２と、１つまたは複数のプロセッサ１１５と、メモリユニット１１８とは、クラウドコンピューティングネットワーク１５０と連携してする、本明細書で説明するネットワークイベント監視および報告動作を実装するように構成され得る。いくつかの実施形態では、ルータ１１０の１つまたは複数のプロセッサ１１５は、クラウド１５０への未知のパケットストリームとオーバーサブスクリプションイベントとの報告、およびクラウド１５０から取得された情報に基づく新しい検出および解決ポリシーの実装など、本明細書で説明するネットワークイベント監視および報告技法を実装するためにネットワーク監視ユニット１１２に関連する（たとえば、メモリユニット１１８に記憶された）プログラム命令を実行することができる。いくつかの実装形態では、ルータ１１０はネットワークインターフェースカード（またはモジュール）１１１を含み得る。ネットワークインターフェースカード１１１は、（たとえば、１つまたは複数の集積回路中に）ネットワーク監視ユニット１１２と、１つまたは複数のプロセッサ１１５と、メモリユニット１１８とを実装し得る。他の実装形態では、ルータ１１０は、（ネットワークインターフェースカード１１１を含む）複数のネットワークインターフェースカードおよび回路板を含み得、複数のネットワークインターフェースカードは、ネットワーク監視ユニット１１２と、１つまたは複数のプロセッサ１１５と、メモリユニット１１８とを実装し得る。図１には示されていないが、いくつかの実装形態では、ルータ１１０は、（１つまたは複数の）プロセッサ１１５およびメモリユニット１１８のほかに１つまたは複数の追加のプロセッサおよびメモリユニット（および他の構成要素）を含み得る。たとえば、ルータ１１０は、１つまたは複数の追加の回路板中に１つまたは複数のプロセッサと１つまたは複数のメモリユニットとを含み得る。

【００５１】

[0055]図２は、いくつかの実施形態による、図１に示したローカルエリアネットワークのためのクラウドコンピューティングエンハンストルータを実装するための例示的な動作を示す流れ図（「フロー」）２００である。フローは図２のブロック２０２から開始する。

【００５２】

[0056]ブロック２０２において、ルータを使用してローカルエリアネットワークのネットワークトラフィックを監視する。たとえば、（図１に示した）ルータ１１０のネットワーク監視ユニット１１２は、１つまたは複数のネットワークデバイス１０２からＷＡＮ１４０に送られたネットワークトラフィック（たとえばファイルアップロード）と、ＷＡＮ

からＬＡＮ１００において受信されたネットワークトラフィック（たとえば、ビデオストリーミング）とを監視する。さらに、ネットワーク監視ユニット１１２は、ＬＡＮ１００中のネットワークデバイス１０２間で送られたネットワークトラフィックを監視することができる。ブロック２０２の後に、フローはブロック２０４に進む。

【００５３】

[0057]ブロック２０４において、ルータを使用してローカルエリアネットワークに関連する１つまたは複数のネットワークイベントを検出する。いくつかの実装形態では、ネットワーク監視ユニット１１２は、ＬＡＮ１００のネットワークトラフィックに基づいて１つまたは複数のネットワークイベントを検出する。上記で説明したように、いくつかの例では、ネットワーク監視ユニット１１２は、ルータ１１０を介してルーティングされた未知のパケットストリームを検出し、および／またはＬＡＮ１００においてオーバーサブスクリプションイベントを検出し得る。ネットワーク監視ユニット１１２はまた、ネットワーク障害またはネットワーク帯域幅の不相応な使用など、他のネットワークイベントを検出し得る。ブロック２０４の後に、フローはブロック２０６に進む。

【００５４】

[0058]ブロック２０６において、ルータからクラウドコンピューティングネットワークに１つまたは複数のネットワークイベントを報告する。いくつかの実装形態では、ネットワーク監視ユニット１１２は、ルータ１１０からクラウドコンピューティングネットワーク１５０の１つまたは複数のサーバに１つまたは複数のネットワークイベントを報告し得る。いくつかの実装形態では、すべてのネットワークイベントまたはネットワークアクティビティをクラウドコンピューティングネットワーク１５０に報告する代わりに、ルータ１１０は、いくつかのネットワークイベント（「あらかじめ定義されたネットワークイベント」）を報告するように構成され得る。たとえば、ルータ１１０は、オーバーサブスクリプションイベントおよび未知のパケットストリームのみをクラウド１５０に報告するように構成され得る。ブロック２０６の後に、フローはブロック２０８に進む。

【００５５】

[0059]ブロック２０８において、クラウドベースコンピューティングネットワークの１つまたは複数のサーバからルータのためのネットワークポリシー更新を受信する。ネットワークポリシー更新は、クラウドベースコンピューティングネットワークの１つまたは複数のサーバに報告されたネットワークイベントのタイプに少なくとも部分的に基づく。いくつかの実装形態では、ルータ１１０は、クラウド１５０からネットワークポリシー更新を受信する。受信されたネットワークポリシー更新は、クラウド１５０に報告されたネットワークイベントのタイプに少なくとも部分的に基づく。たとえば、クラウド１５０は、報告されたネットワークイベントのタイプに基づいて、および、図３に関して以下でさらに説明するように、ＷＡＮ１４０の複数のローカルエリアネットワークから収集された同じタイプのネットワークイベントに関連するアグリゲートデータに対して実行された分析の結果に基づいて、ネットワークポリシー更新を判断し得る。たとえば、ルータ１１０によって報告されたネットワークイベントが、ルータ１１０において検出された未知のパケットストリームである場合、クラウド１５０は、ＬＡＮ１００から、および未知のパケットストリーム中の同じパケットストリーム特性のいくつかを同じく検出したＷＡＮ１４０中の他のローカルエリアネットワークから収集されたアグリゲートデータに対して分析を実行する。アグリゲートデータから、クラウド１５０は、未知のパケットストリームの将来の検出および識別のために未知のパケットストリームの特性に基づいて新しいパケットストリーム検出ポリシーを判断することができる。クラウド１５０は、次いで、ルータ１１０に実装されているストリーム検出ポリシーを更新するためにルータ１１０に新しいパケットストリーム検出ポリシーを送ることができる。ブロック２０８の後に、フローはブロック２１０に進む。

【００５６】

[0060]ブロック２１０において、構成の後にネットワークトラフィック管理ノードにおいてネットワークポリシー更新を実装する。いくつかの実装形態では、ネットワーク監視

ユニット１１２は、ネットワークポリシー更新で構成され、次いで、ＬＡＮ１００のネットワークイベントを検出し、処理するときにルータ１１０においてネットワークポリシー更新を実装する。たとえば、未知のパケットストリームの例では、ネットワーク監視ユニット１１２は更新されて、パケットストリーム検出および識別のためにクラウド１５０から受信された新しいパケットストリーム検出ポリシーが実装され得る。ブロック２１０の後に、フローは終了する。

【００５７】

[0061]図３は、いくつかの実施形態による、図１に示したクラウドコンピューティングエンハンストルータシステムを実装するための例示的な動作を示す流れ図（「フロー」）３００である。フローは図３のブロック３０２から開始する。

【００５８】

[0062]ブロック３０２において、クラウドコンピューティングネットワーク１５０の１つまたは複数のサーバが、ＬＡＮ１００において検出されたネットワークイベントを示す報告メッセージをルータ１１０から受信する。たとえば、上記で前に説明したように、ルータ１１０は、ルーティングされているパケットストリームのうちの１つが未知であると判断し、未知のパケットストリームに関連する情報をクラウド１５０に送ることができる。別の例として、ルータ１１０は、ＬＡＮ１００においてオーバーサブスクリプションイベントを検出し、オーバーサブスクリプションイベントを解決することを試みるために実装された技法を示す報告をクラウド１５０に送ることができる。報告において、ルータ１１０はまた、その特定の技法がオーバーサブスクリプションイベントを解決するのに成功したかどうかと、技法の特定の結果とを示すことができる。ブロック３０２の後に、フローはブロック３０４に進む。

【００５９】

[0063]ブロック３０４において、クラウドコンピューティングネットワーク１５０は、ルータ１１０から受信された報告メッセージに関連するネットワークイベントのタイプを判断する。たとえば、クラウド１５０は、報告メッセージが、ルータ１１０において受信された未知のパケットストリームに関連すると判断するか、または、報告メッセージが、ＬＡＮ１００において検出されたオーバーサブスクリプションイベントに関連すると判断する。ただし、報告メッセージは、図１を参照しながら上記で説明したもの（たとえば、ネットワーク障害報告）など、様々な他のネットワークイベントを示し得ることに留意されたい。ブロック３０４の後に、フローはブロック３０６に進む。

【００６０】

[0064]ブロック３０６において、クラウドコンピューティングネットワーク１５０は、報告されたネットワークイベントに関連するデータを、同じまたは同様のタイプの検出されたネットワークイベントについて他のローカルエリアネットワーク中の他のルータから前に受信されたデータとアグリゲートする。たとえば、クラウド１５０は、様々なルータによって報告された未知のパケットストリームに関連するすべての情報（たとえば、パケットストリーム特性）をアグリゲートする。別の例として、クラウド１５０は、様々なルータによって報告された同じまたは同様のタイプのオーバーサブスクリプションイベントに関連するすべてのデータ（たとえば、使用された解決技法および結果）をアグリゲートする。ブロック３０６の後に、フローはブロック３０８に進む。

【００６１】

[0065]ブロック３０８において、クラウドコンピューティングネットワーク１５０は、同じまたは同様のタイプの報告されたネットワークイベントに関連するアグリゲートデータを分析する。たとえば、クラウド１５０は、他のローカルエリアネットワーク中の様々なルータによって報告された未知のパケットストリームに関連するアグリゲートデータを分析する。一例では、クラウド１５０は、未知のパケットストリームに関連するアグリゲートデータに対してディープパケット検査（deep packet inspection）および統計的分析を実行し、未知のパケットストリームに関連する様々なストリーム特性を分析することができる。同時に、クラウド１５０は、未知のパケットストリームを識別するのを助けるた

めに、インターネット１２０上の様々なサービスプロバイダからのパケットストリームを連続的に監視し、対応するパケットストリームの変化を識別することができる。別の例では、クラウド１５０は、様々なルータによって報告された様々なオーバーサブスクリプションイベントに関連するアグリゲートデータを分析することができる。クラウド１５０は、オーバーサブスクリプションイベントを解決するために使用される様々な技法を検査し、異なる技法を実装した結果を比較することができる。ブロック３０８の後に、フローはブロック３１０に進む。

【００６２】

[0066]ブロック３１０において、クラウドコンピューティングネットワーク１５０は、検出されたネットワークイベントを処理するための改善されたネットワークポリシーまたはプロシージャを判断し、ルータ構成を更新するために更新されたネットワークポリシーまたはプロシージャをＬＡＮ１００のルータ１１０に送る。たとえば、上記のブロック３０８において実行された分析に基づいて、クラウド１５０は、パケットストリームを検出するための改善されたパケットストリーム検出ポリシー（たとえば、更新されたストリーム特性基準）を判断するか、またはオーバーサブスクリプションイベントを処理するための改善された解決ポリシーを判断することができる。ブロック３１０の後に、フローは終了する。

【００６３】

[0067]いくつかの実装形態では、クラウドコンピューティングネットワーク１５０は、リアルタイムでネットワークポリシー更新を判断し、ルータ１１０に送る。たとえば、クラウドコンピューティングネットワーク１５０が、ＷＡＮ１４０中の様々なルータからの十分なデータをアグリゲートし、アグリゲートデータの分析を実行した場合、クラウドコンピューティングネットワーク１５０は、ルータ１１０がネットワークイベントを報告したときにリアルタイムでネットワークポリシー更新をルータ１１０に送ることができる。その結果、ルータ１１０は、報告されたネットワークイベントをリアルタイムで処理および／または解決するためにネットワークポリシー更新をリアルタイムで実装することができる。いくつかの実装形態では、ルータ１１０からネットワークイベントに関連する（１つまたは複数の）報告メッセージを受信した後に、クラウドコンピューティングネットワーク１５０は、ＷＡＮ１４０中の他のルータからのネットワークイベントに関連する追加のデータをアグリゲートし続けることができ、および／またはアグリゲートデータに対して追加の分析を実行し得る。たとえば、クラウドコンピューティングネットワーク１５０は、ネットワークイベントについて改善されたネットワークポリシーを判断するために、クラウドコンピューティングネットワーク１５０が追加のデータをクラウドソースするおよび／または追加の分析を実行する必要があると判断し得る。この例では、クラウドコンピューティングネットワーク１５０は、ルータ１１０にネットワークポリシー更新をリアルタイムで送らないであろう。代わりに、クラウドコンピューティングネットワーク１５０はネットワークポリシー更新を後で送り得、ルータ１１０は、ネットワークイベントの次の発生を処理および／または解決するためにネットワークポリシー更新を実装するであろう。

【００６４】

[0068]図４は、いくつかの実施形態による、図１～図３に記載したクラウドコンピューティングエンハンストルータにおいてパケットストリーム検出を実装するための例示的な動作を示す流れ図（「フロー」）４００である。フローは図４のブロック４０２から開始する。

【００６５】

[0069]ブロック４０２において、ローカルエリアネットワークのルータにおいて検出された複数のパケットストリームを分類する。いくつかの実装形態では、（図１に示す）ルータ１１０のネットワーク監視ユニット１１２は、ネットワークトラフィックを監視し、複数のパケットストリームを検出し、パケットストリームを分類する。たとえば、（たとえば、ディープパケット検査を使用して）パケットストリームの特性および統計値を検出

した後に、ネットワーク監視ユニット１１２は、パケットストリームに関連するアプリケーションを判断し、関連するアプリケーションに基づいてパケットストリームを分類することができる。一例では、パケットストリーム特性および統計値はパケットストリームがＮｅｔｆｌｉｘ（登録商標）ビデオストリーミングサービスから配信されていることを示す場合、ネットワーク監視ユニット１１２は、パケットストリームをＮｅｔｆｌｉｘ（登録商標）アプリケーションパケットストリームとして分類する。ブロック４０２の後に、フローはブロック４０４に進む。

【００６６】

[0070]ブロック４０４において、ルータにおいて未知のパケットストリームを検出する。いくつかの実装形態では、ネットワーク監視ユニット１１２は、パケットストリーム特性および統計値を検出し、パケットストリーム特性および統計値を既知のパケットストリームと比較し、パケットストリームが未知のパケットストリーム特性および統計値をもつ未知のパケットストリームであると判断する。ブロック４０４の後に、フローはブロック４０６に進む。

【００６７】

[0071]ブロック４０６において、未知のパケットストリームのためのデフォルト分類を選択する。いくつかの実装形態では、ネットワーク監視ユニット１１２は未知のパケットストリームに関連する特定のアプリケーションを判断することができないが、ネットワーク監視ユニット１１２は、未知のパケットストリームに関連するアプリケーションタイプ（たとえば、ストリーミングビデオまたはオーディオ）に基づいてデフォルト分類を選択し得る。たとえば、未知のパケットストリームのアプリケーションタイプはストリーミングビデオまたはストリーミングオーディオとして判断され得、アプリケーションタイプに基づいて未知のパケットストリームにデフォルト分類が割り当てられ得る。いくつかの実装形態では、ネットワーク監視ユニット１１２は、未知のパケットストリームに関連する特定のアプリケーションとアプリケーションタイプの両方を判断することが可能でないことがあり、したがって、未知のアプリケーションとアプリケーションタイプとをもつパケットストリームのためのデフォルト分類を一時的に選択し得る。特定のアプリケーションが判断され得るまで未知のパケットストリームがルータ１１０によって処理されることを可能にするために、デフォルト分類は一時的に割り当てられ得る。たとえば、デフォルト分類は、未知のパケットストリームに、最小および最大帯域幅要件と、場合によっては優先度値とを割り当て得る。一例では、アプリケーションタイプとしてビデオストリーミングに基づいて未知のパケットストリームのためのデフォルト分類が選択された場合、デフォルト分類は、ビデオストリーミングアプリケーションにとって典型的である最小および最大帯域幅要件（たとえば、ビデオストリーミングアプリケーションの平均帯域幅数）を割り当てる。ブロック４０６の後に、フローはブロック４０８に進む。

【００６８】

[0072]ブロック４０８において、クラウドコンピューティングネットワークの１つまたは複数のサーバに、未知のパケットストリームに関連する情報を報告する。いくつかの実装形態では、ネットワーク監視ユニット１１２は、未知のパケットストリームに関連するパケットストリーム特性および統計値を示す報告メッセージをインターネットを介してルータ１１０からクラウド１５０に送ることができる。ブロック４０８の後に、フローはブロック４１０に進む。

【００６９】

[0073]ブロック４１０において、クラウドコンピューティングネットワークから、更新されたパケットストリーム検出ポリシーを受信する。いくつかの実装形態では、ネットワーク監視ユニット１１２は、前に未知であったパケットストリームを検出し、分類するために使用され得る、更新されたパケットストリーム検出ポリシーをクラウド１５０から受信することができる。一例では、クラウド１５０は、ルータ１１０から、および未知のパケットストリーム中の同じパケットストリーム特性および統計値のいくつかを同じく検出したＷＡＮ１４０中の他のローカルエリアネットワークから収集されたアグリゲートデー

タに対して分析を実行する。クラウドはまた、インターネットにおいてサービスプロバイダおよびアプリケーションからパケットストリーム特性および統計値を収集し続ける。アグリゲートデータから、クラウド１５０は、未知のパケットストリームの将来の識別および分類のために未知のパケットストリームの特性および統計値に基づいて新しいパケットストリーム検出ポリシーを判断することができる。たとえば、クラウド１５０は、新しいオーディオストリーミングサービスからのパケットストリーム特性および統計値を、クラウド１５０によってアグリゲートされたパケットストリーム特性および統計値と比較した後に、未知のパケットストリームが、最近オンラインに持ってこられた新しいオーディオストリーミングサービスから来たと判断することができる。別の例では、クラウド１５０は、既存のビデオストリーミングサービスが、それのサービスおよびアプリケーションに関連するパケットストリーム特性および統計値を変化させたと判断することができる。ブロック４１０の後に、フローはブロック４１２に進む。

【００７０】

[0074]ブロック４１２において、更新されたパケットストリーム検出ポリシーは、ルータにおいて実装される。いくつかの実装形態では、ネットワーク監視ユニット１１２は、ルータ１１０が新しいポリシーで構成された後に、更新されたパケットストリーム検出ポリシーを実装する。更新されたパケットストリーム検出ポリシーは、前に未知であったパケットストリームの後での検出および分類のために使用され得る。フロー４１２の後に、フローは終了する。

【００７１】

[0075]図１～図５および本明細書で説明する動作は、実施形態を理解するのを助けるための例であり、実施形態を限定したり、特許請求の範囲を限定したりするために使用されるべきでないことを理解されたい。実施形態は、追加の動作を実行し、より少ない動作を実行し、動作を異なる順序で実行し、動作を並行して実行し、いくつかの動作を別様に実行し得る。

【００７２】

[0076]当業者なら諒解するように、本発明の主題の態様は、システム、方法、またはコンピュータプログラム製品として具現化され得る。したがって、本発明の主題の態様は、完全にハードウェアの実施形態、（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）ソフトウェアの実施形態、またはソフトウェアの態様とハードウェアの態様とを組み合わせた実施形態の形態をとり得、本明細書では、それらすべてを全般的に「回路」、「モジュール」または「システム」と呼ぶことがある。さらに、本発明の主題の態様は、コンピュータ可読プログラムコードを組み込む１つまたは複数のコンピュータ可読媒体中で具現化されたコンピュータプログラム製品の形態をとり得る。

【００７３】

[0077]１つまたは複数のコンピュータ可読媒体の任意の組合せが利用され得る。コンピュータ可読媒体は、コンピュータ可読信号媒体またはコンピュータ可読記憶媒体であり得る。コンピュータ可読記憶媒体は、限定はしないが、たとえば、電子、磁気、光、電磁、赤外線、または半導体のシステム、装置、またはデバイス、あるいは上記の任意の適切な組合せであり得る。コンピュータ可読記憶媒体のより具体的な例（非網羅的なリスト）としては、１つまたは複数のワイヤを有する電気的接続、ポータブルコンピュータディスケット、ハードディスク、ランダムアクセスメモリ（ＲＡＭ）、読取り専用メモリ（ＲＯＭ）、消去可能プログラマブル読取り専用メモリ（ＥＰＲＯＭまたはフラッシュメモリ）、光ファイバー、ポータブルコンパクトディスク読取り専用メモリ（ＣＤ－ＲＯＭ）、光学記憶デバイス、磁気記憶デバイス、または上記の任意の好適な組合せがあり得る。本明細書のコンテキストでは、コンピュータ可読記憶媒体は、命令実行システム、装置、またはデバイスによってあるいはそれらに関連して使用するためのプログラムを包含または記憶することができる任意の有形媒体であり得る。コンピュータ可読信号媒体は、たとえばベースバンド内に、または搬送波の一部として、コンピュータ可読プログラムコードが組み込まれた伝搬データ信号を含み得る。そのような伝搬信号は、限定はしないが、電磁気、

光、またはそれらの任意の好適な組合せを含む、様々な形態のうちのいずれかをとり得る。コンピュータ可読信号媒体は、コンピュータ可読記憶媒体ではなく、命令実行システム、装置、またはデバイスによってあるいはそれらに関連して使用するためのプログラムを通信、伝搬、またはトランスポートすることができる任意のコンピュータ可読媒体であり得る。コンピュータ可読媒体上で実施されるプログラムコードは、限定はしないが、ワイヤレス、ワイヤライン、光ファイバーケーブル、ＲＦなど、または上記の任意の好適な組合せを含む、任意の好適な媒体を使用して送信され得る。

【００７４】

[0078]本発明の主題の態様のための動作を実行するためのコンピュータプログラムコードは、Ｊａｖａ（登録商標）、Ｓｍａｌｌｔａｌｋ、Ｃ＋＋などのオブジェクト指向プログラミング言語、および「Ｃ」プログラミング言語または同様のプログラミング言語などの従来の手続き型プログラミング言語を含む、１つまたは複数のプログラミング言語の任意の組合せで書かれ得る。プログラムコードは、完全にユーザのコンピュータ上で実行されるか、部分的にユーザのコンピュータ上で実行されるか、スタンドアロンソフトウェアパッケージとして実行されるか、部分的にユーザのコンピュータ上と部分的にリモートコンピュータ上とで実行されるか、あるいは完全にリモートコンピュータまたはサーバ上で実行され得る。後者のシナリオでは、リモートコンピュータは、ローカルエリアネットワーク（ＬＡＮ）または広域ネットワーク（ＷＡＮ）を含む、任意のタイプのネットワークを介してユーザのコンピュータに接続され得、または接続が（たとえば、インターネットサービスプロバイダを使用してインターネットを介して）外部コンピュータに行われ得る。

【００７５】

[0079]本発明の主題の態様は、本発明の主題の実施形態に従って、方法、装置（システム）およびコンピュータプログラム製品のフローチャート図および／またはブロック図を参照しながら説明している。フローチャート図および／またはブロック図の各ブロック、ならびにフローチャート図および／またはブロック図におけるブロックの組合せはコンピュータプログラム命令によって実装され得ることを理解されよう。これらのコンピュータプログラム命令は、機械を製造するために、汎用コンピュータ、専用コンピュータ、または他のプログラマブルデータ処理装置のプロセッサに与えられ得、その結果、コンピュータまたは他のプログラマブルデータ処理装置のプロセッサを介して実行される命令は、フローチャートおよび／またはブロック図の１つまたは複数のブロック中で指定された機能／動作を実装するための手段を作成する。

【００７６】

[0080]これらのコンピュータプログラム命令はまた、コンピュータ、他のプログラマブルデータ処理装置、または他のデバイスに、特定の方法で機能するように命令することができるコンピュータ可読媒体に記憶され得、その結果、コンピュータ可読媒体に記憶された命令は、フローチャートおよび／またはブロック図の１つまたは複数のブロック中で指定された機能／動作を実装する命令を含む製造品を製造する。

【００７７】

[0081]コンピュータプログラム命令はまた、コンピュータ、他のプログラマブルデータ処理装置、または他のデバイスにロードされて、一連の動作ステップをコンピュータ、他のプログラマブル装置または他のデバイス上で実行されるようにさせて、コンピュータ実装プロセスを作成し得、その結果、コンピュータまたは他のプログラマブル装置上で実行される命令は、フローチャートおよび／またはブロック図の１つまたは複数のブロック中で指定された機能／動作を実装するためのプロセスを提供する。

【００７８】

[0082]図５は、いくつかの実施形態による、ローカルエリアネットワーク監視およびワイドエリアネットワークにおけるクラウドベースサポートのための機構を含むネットワークデバイス５００の一実施形態のブロック図である。いくつかの実装形態では、ネットワークデバイス５００は、ネットワークに関連するパケットを受信し、処理し、ルーティン

グする、２つ以上のネットワーク（たとえば、ＬＡＮとＷＡＮ）間のネットワークトラフィック管理ノードであり、たとえば、ネットワークトラフィック管理ノードはＬＡＮのルータ／ゲートウェイ（たとえば、図１に示したＬＡＮ１００）であり得る。ただし、他の実装形態では、ネットワークデバイス５００は、ケーブルモデム、ワイヤレスアクセスポイント、ネットワークブリッジ、ネットワークスイッチ、デスクトップコンピュータ、ゲーミングコンソール、モバイルコンピューティングデバイスなど、図１～図４を参照しながら上記で説明した機能を実装するように構成され得る他の好適なタイプのネットワークデバイスであり得ることに留意されたい。ネットワーク５００は、（場合によっては、複数のプロセッサ、複数のコア、複数のノードを含む、および／またはマルチスレッドを実装するなどの）プロセッサユニット５０２を含む。ネットワークデバイス５００はメモリユニット５０６を含む。メモリユニット５０６は、システムメモリ（たとえば、キャッシュ、ＳＲＡＭ、ＤＲＡＭ、ゼロキャパシタＲＡＭ、ツイントランジスタＲＡＭ、ｅＤＲＡＭ、ＥＤＯ　ＲＡＭ、ＤＤＲ　ＲＡＭ、ＥＥＰＲＯＭ（登録商標）、ＮＲＡＭ、ＲＲＡＭ（登録商標）、ＳＯＮＯＳ、ＰＲＡＭなどのうちの１つまたは複数）あるいは上記ですでに説明した、機械可読記憶媒体の可能な実現形態のうちのいずれか１つまたは複数であり得る。ネットワークデバイス５００はまた、バス５１０（たとえば、ＰＣＩ、ＩＳＡ、ＰＣＩ－Ｅｘｐｒｅｓｓ、ＨｙｐｅｒＴｒａｎｓｐｏｒｔ（登録商標）、ＩｎｆｉｎｉＢａｎｄ（登録商標）、ＮｕＢｕｓ、ＡＨＢ、ＡＸＩなど）と、ワイヤレスネットワークインターフェース（たとえば、Ｂｌｕｅｔｏｏｔｈ（登録商標）インターフェース、ＷＬＡＮ８０２．１１インターフェース、ＷｉＭＡＸ（登録商標）インターフェース、ＺｉｇＢｅｅ（登録商標）インターフェース、ワイヤレスＵＳＢインターフェースなど）、およびワイヤードネットワークインターフェース（たとえば、イーサネット（登録商標）インターフェース、電力線通信インターフェースなど）のうちの少なくとも１つを含む、（１つまたは複数の）ネットワークインターフェース５０８とを含む。図示のように、（１つまたは複数の）ネットワークインターフェース５０８はまた、ネットワーク監視ユニット５１２を含む。たとえば、ネットワーク監視ユニット５１２は、（１つまたは複数の）ネットワークインターフェース５０８のネットワークインターフェースカードまたはネットワークインターフェースモジュール内に実装され得る。ネットワーク監視ユニット５１２は、図１～図４を参照しながら上記で説明したように、ネットワークデバイス５００のために（特徴の中でも）ネットワークトラフィック監視、ネットワークイベント検出、ならびにクラウドベースアクセスおよびサポートのための機構を実装するように動作可能であり得る。

【００７９】

[0083]これらの機能のうちの任意の１つは、ハードウェアでおよび／またはプロセッサユニット５０２上に部分的に（または完全に）実装され得る。たとえば、機能は、１つまたは複数の特定用途向け集積回路、１つまたは複数のシステムオンチップ（ＳｏＣ）、あるいは他のタイプの（１つまたは複数の）集積回路で、プロセッサユニット５０２中に実装された論理で、周辺デバイスまたはカード上のコプロセッサで、ネットワークインターフェース５０８内に実装された別個のプロセッサおよび／またはメモリなどで実装され得る。さらに、実現形態は、より少ない構成要素、または図５に示さない追加の構成要素（たとえば、ビデオカード、オーディオカード、追加のネットワークインターフェース、周辺デバイスなど）を含み得る。プロセッサユニット５０２、メモリユニット５０６、およびネットワークインターフェース５０８は、バス５１０に結合される。バス５１０に結合されるものとして示されているが、メモリユニット５０６はプロセッサユニット５０２に結合され得る。

【００８０】

[0084]本実施形態について、様々な実装形態および活用を参照しながら説明したが、これらの実施形態は例示的なものであり、本発明の主題の範囲はそれらに限定されないことを理解されよう。概して、本明細書で説明した通信ネットワークのためのクラウドコンピューティングエンハンストルータを実装するための技法は、任意の１つまたは複数のハー

ドウェアシステムに一致する設備で実装され得る。多くの変形、修正、追加、および改善が可能である。

【００８１】

[0085]単一の事例として本明細書で説明した構成要素、動作、または構造について、複数の事例が与えられ得る。最後に、様々な構成要素と、動作と、データストアとの間の境界はいくぶん恣意的であり、特定の動作が、特定の例示的な構成のコンテキストで示されている。機能の他の割振りが想定され、本発明の主題の範囲内に入り得る。概して、例示的な構成において別個の構成要素として提示された構造および機能は、組み合わされた構造または構成要素として実装され得る。同様に、単一の構成要素として提示された構造および機能は、別個の構成要素として実装され得る。これらおよび他の変形、修正、追加、および改善は、本発明の主題の範囲内に入り得る。

以下に、本願出願の当初の特許請求の範囲に記載された発明を付記する。

［Ｃ１］

ローカルエリアネットワーク（ＬＡＮ）のネットワークトラフィックを監視することと、

前記ＬＡＮに関連するネットワークイベントを検出することと、

クラウドベースコンピューティングネットワークの１つまたは複数のサーバに前記ネットワークイベントを報告することと、

前記クラウドベースコンピューティングネットワークの前記１つまたは複数のサーバから前記ＬＡＮのためのネットワークポリシー更新を受信することと、ここで、前記ネットワークポリシー更新が、前記クラウドベースコンピューティングネットワークの前記１つまたは複数のサーバに報告されたネットワークイベントのタイプに少なくとも部分的に基づく、

前記ＬＡＮにおいて前記ネットワークポリシー更新を実装することと

を備える方法。

［Ｃ２］

前記監視することと、前記検出することと、前記報告することと、前記受信することと、前記実装することとが、前記ＬＡＮのネットワークトラフィック管理ノードによって実行される、［Ｃ１］に記載の方法。

［Ｃ３］

前記ネットワークトラフィック管理ノードが前記ＬＡＮのルータを備える、［Ｃ２］に記載の方法。

［Ｃ４］

前記ネットワークトラフィック管理ノードが、前記ＬＡＮのルータと、アクセスポイントと、ケーブルモデムと、ネットワークスイッチとのうちの１つまたは複数を含むコンピュータシステムを備える、［Ｃ２］に記載の方法。

［Ｃ５］

前記ＬＡＮに関連する前記ネットワークイベントを前記検出することが、前記ＬＡＮにおいてオーバーサブスクリプションイベントを検出することと、前記ＬＡＮにおいて未知のパケットストリームを検出することと、前記ＬＡＮにおいてネットワーク障害イベントを検出することとのうちの少なくとも１つを備える、［Ｃ１］に記載の方法。

［Ｃ６］

前記ネットワークポリシー更新を前記実装することが、前記ネットワークイベントを処理し、解決するために前記ＬＡＮのネットワークトラフィック管理ノードの構成の後に前記ネットワークポリシー更新を実装することを備える、［Ｃ１］に記載の方法。

［Ｃ７］

前記ＬＡＮのネットワークトラフィックを前記監視することが、前記ＬＡＮの複数のネットワークデバイスのうちの１つまたは複数からワイドエリアネットワークに送られたネットワークトラフィックを監視することと、前記ワイドエリアネットワークのリモートネットワークノードから前記ＬＡＮの前記複数のネットワークデバイスのうちの１つまたは

複数に送られたネットワークトラフィックを監視することとを備える、［Ｃ１］に記載の方法。

［Ｃ８］

前記クラウドベースコンピューティングネットワークの前記１つまたは複数のサーバから受信された前記ネットワークポリシー更新が、前記クラウドベースコンピューティングネットワークの前記１つまたは複数のサーバに報告されたネットワークイベントの前記タイプに基づき、および複数の追加のローカルエリアネットワークから前記クラウドベースコンピューティングネットワークにおいて収集されたネットワークイベントの前記タイプに関連するアグリゲートデータの分析に基づく、［Ｃ１］に記載の方法。

［Ｃ９］

前記ＬＡＮに関連するネットワークアクティビティを検出することと、

クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、前記ＬＡＮに関連する前記ネットワークアクティビティを報告することと、

前記クラウドベースコンピューティングネットワークから前記ＬＡＮにおいてネットワークアラートを受信することと

をさらに備える、［Ｃ１］に記載の方法。

［Ｃ１０］

ローカルエリアネットワーク（ＬＡＮ）のネットワークトラフィック管理ノードにおいて検出された複数のパケットストリームを分類することと、

前記ネットワークトラフィック管理ノードにおいて未知のパケットストリームを検出することと、

前記未知のパケットストリームのためのデフォルト分類を選択することと、

前記ネットワークトラフィック管理ノードからクラウドベースコンピューティングネットワークの１つまたは複数のサーバに、前記未知のパケットストリームに関連する情報を報告することと、

前記クラウドベースコンピューティングネットワークから前記未知のパケットストリームのためのパケットストリーム検出ポリシー更新を前記ネットワークトラフィック管理ノードにおいて受信することと、

前記未知のパケットストリームを後で検出し、分類するために前記ネットワークトラフィック管理ノードにおいて前記パケットストリーム検出ポリシー更新を実装することと

を備える方法。

［Ｃ１１］

前記ネットワークトラフィック管理ノードにおいて検出された前記複数のパケットストリームを前記分類することが、

前記複数のパケットストリームに関連するパケットストリーム特性を検出することと、

前記対応するパケットストリーム特性に少なくとも部分的に基づいて前記複数のパケットストリームの各々に関連するアプリケーションを判断することと、

前記パケットストリームの各々に関連する前記アプリケーションに少なくとも部分的に基づいて前記複数のパケットストリームの各々を分類することと

を備える、［Ｃ１０］に記載の方法。

［Ｃ１２］

前記ネットワークトラフィック管理ノードにおいて検出された前記複数のパケットストリームを前記分類することが、前記複数のパケットストリームの各々に関連するアプリケーションと、前記複数のパケットストリームの各々に関連するアプリケーションタイプとのうちの少なくとも１つに基づいて前記複数のパケットストリームを分類することを備える、［Ｃ１０］に記載の方法。

［Ｃ１３］

前記ネットワークトラフィック管理ノードにおいて前記未知のパケットストリームを前記検出することと、前記未知のパケットストリームのための前記デフォルト分類を前記選択することとは、

前記ネットワークトラフィック管理ノードにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、
前記アプリケーションが未知であると判断したことに応答して前記未知のパケットストリームのための前記デフォルト分類を選択することと
を備える、［Ｃ１０］に記載の方法。
［Ｃ１４］
前記ネットワークトラフィック管理ノードにおいて前記未知のパケットストリームを前記検出することと、前記未知のパケットストリームのための前記デフォルト分類を前記選択することとは、
前記ネットワークトラフィック管理ノードにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、
前記未知のパケットストリームに関連するアプリケーションタイプを判断することと、
前記未知のパケットストリームに関連する前記アプリケーションタイプに基づいて前記未知のパケットストリームのための前記デフォルト分類を選択することと
を備える、［Ｃ１０］に記載の方法。
［Ｃ１５］
前記ネットワークトラフィック管理ノードからクラウドベースコンピューティングネットワークの１つまたは複数のサーバに前記未知のパケットストリームに関連する情報を前記報告することが、前記未知のパケットストリームに関連するパケットストリーム特性を報告することを備える、［Ｃ１０］に記載の方法。
［Ｃ１６］
前記パケットストリーム検出ポリシー更新を受信することに加えて、前記未知のパケットストリームに関連するアプリケーションと、前記未知のパケットストリームの分類とを示す情報を受信することをさらに備える、［Ｃ１０］に記載の方法。
［Ｃ１７］
前記未知のパケットストリームを後で検出し、分類するために前記ネットワークトラフィック管理ノードにおいて前記パケットストリーム検出ポリシー更新を前記実装することが、
前記パケットストリーム検出ポリシー更新に従って前に未知であったパケットストリームに関連するパケットストリーム特性を前記ネットワークトラフィック管理ノードにおいて検出することと、
前記パケットストリーム検出ポリシー更新に従って前記パケットストリーム特性に関連するアプリケーションを判断することと、
前記パケットストリーム特性に関連する前記アプリケーションに基づいて前記前に未知であったパケットストリームのための分類を選択することと
を備える、［Ｃ１０］に記載の方法。
［Ｃ１８］
ローカルエリアネットワーク（ＬＡＮ）のルータから、前記ルータにおいて検出されたネットワークイベントを示す報告メッセージをクラウドベースコンピューティングネットワークの１つまたは複数のサーバにおいて受信することと、
前記ＬＡＮにおいて前記ルータによって検出されたネットワークイベントのタイプを判断することと、
前記ルータによって報告されたネットワークイベントの前記タイプに関連するデータを、ネットワークイベントの前記タイプを同じく検出した他のルータからの前に受信されたデータとアグリゲートすることと、
ネットワークイベントの前記タイプに関連する前記アグリゲートデータを分析することと、
ネットワークイベントの前記タイプに関連する前記アグリゲートデータの前記分析の結果に基づいてネットワークイベントの前記タイプに関連するネットワークポリシー更新を判断することと、

ネットワークイベントの前記タイプに関連する前記ネットワークポリシー更新で前記ルータを構成するために前記ＬＡＮの前記ルータに前記ネットワークポリシー更新を送ることと
を備える方法。
［Ｃ１９］
前記ＬＡＮにおいて前記ルータによって検出されたネットワークイベントの前記タイプを前記判断することは、ネットワークイベントの前記タイプが、前記ＬＡＮにおけるオーバーサブスクリプションイベントと、前記ルータにおける未知のパケットストリームの検出と、前記ルータからのネットワーク分析報告の受信と、前記ＬＡＮにおけるネットワーク障害イベントの検出とのうちの１つであると判断することを備える、［Ｃ１８］に記載の方法。
［Ｃ２０］
前記ルータにおけるコンテンツの一時記憶を要求するためにネットワークイベントの前記タイプに関連する前記アグリゲートデータの前記分析の結果に基づいて前記ＬＡＮの前記ルータにコマンドを送ることをさらに備える、［Ｃ１８］に記載の方法。
［Ｃ２１］
ネットワークイベントの前記タイプに関連する前記アグリゲートデータの前記分析の結果に基づいてネットワークイベントの前記タイプに関連するネットワークポリシー更新を前記判断することが、前記ルータにおいて検出されたネットワークイベントの前記タイプを処理し、解決するためにネットワークポリシー更新を判断することを備える、［Ｃ１８］に記載の方法。
［Ｃ２２］
ネットワークルータであって、
１つまたは複数のプロセッサと、
１つまたは複数の命令を記憶するように構成された１つまたは複数のメモリユニットであって、前記命令は、前記１つまたは複数のプロセッサによって実行されたとき、
ローカルエリアネットワーク（ＬＡＮ）のネットワークトラフィックを監視することと、
前記ＬＡＮに関連するネットワークイベントを検出することと、
クラウドベースコンピューティングネットワークの１つまたは複数のサーバに前記ネットワークイベントを報告することと、
前記クラウドベースコンピューティングネットワークの前記１つまたは複数のサーバから前記ネットワークルータのためのネットワークポリシー更新を受信することであって、前記ネットワークポリシー更新が、前記クラウドベースコンピューティングネットワークの前記１つまたは複数のサーバに報告されたネットワークイベントのタイプに少なくとも部分的に基づく、受信することと、
前記ネットワークルータにおいて前記ネットワークポリシー更新を実装することと
を備える動作を前記ネットワークルータに実行させる、１つまたは複数のメモリユニットと
を備えるネットワークルータ。
［Ｃ２３］
前記ＬＡＮに関連する前記ネットワークイベントが、前記ＬＡＮにおけるオーバーサブスクリプションイベントと、前記ネットワークルータにおいて受信された未知のパケットストリームと、前記ＬＡＮにおけるネットワーク障害イベントとのうちの１つを備える、［Ｃ２２］に記載のネットワークルータ。
［Ｃ２４］
前記１つまたは複数のプロセッサによって実行される前記１つまたは複数の命令が、前記ネットワークルータの構成の後に前記ネットワークポリシー更新を実装することによって前記ネットワークイベントを処理し、解決することをさらに備える動作を前記ネットワークルータに実行させる、［Ｃ２２］に記載のネットワークルータ。

［Ｃ２５］
前記１つまたは複数のプロセッサによって実行される前記１つまたは複数の命令が、
前記ＬＡＮに関連するネットワークアクティビティを検出することと、
クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、前記ＬＡＮに関連する前記ネットワークアクティビティを報告することと、
前記クラウドベースコンピューティングネットワークから前記ネットワークルータにおいてネットワークアラートを受信することと
をさらに備える動作を前記ネットワークルータに実行させる、［Ｃ２２］に記載のネットワークルータ。
［Ｃ２６］
ネットワークルータであって、
プロセッサと、
前記プロセッサに結合されたネットワーク監視ユニットであって、
ローカルエリアネットワーク（ＬＡＮ）の前記ネットワークルータにおいて検出された複数のパケットストリームを分類することと、
前記ネットワークルータにおいて受信された未知のパケットストリームを検出することと、
前記未知のパケットストリームのためのデフォルト分類を選択することと、
クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、前記未知のパケットストリームに関連する情報を報告することと、
前記未知のパケットストリームのためのパケットストリーム検出ポリシー更新を前記クラウドベースコンピューティングネットワークから受信することと、
前記未知のパケットストリームを後で検出し、分類するために前記ネットワークルータにおいて前記パケットストリーム検出ポリシー更新を実装することと
を行うように構成されたネットワーク監視ユニットと
を備えるネットワークルータ。
［Ｃ２７］
前記ネットワークルータにおいて検出された前記複数のパケットストリームを分類するように構成された前記ネットワーク監視ユニットが、
前記複数のパケットストリームに関連するパケットストリーム特性を検出することと、
前記対応するパケットストリーム特性に少なくとも部分的に基づいて前記複数のパケットストリームの各々に関連するアプリケーションを判断することと、
前記パケットストリームの各々に関連する前記アプリケーションに少なくとも部分的に基づいて前記複数のパケットストリームの各々を分類することと
を行うように構成された前記ネットワーク監視ユニットを備える、［Ｃ２６］に記載のネットワークルータ。
［Ｃ２８］
前記ネットワークルータにおいて検出された前記複数のパケットストリームを分類するように構成された前記ネットワーク監視ユニットが、前記複数のパケットストリームの各々に関連するアプリケーションと、前記複数のパケットストリームの各々に関連するアプリケーションタイプとのうちの少なくとも１つに基づいて前記複数のパケットストリームを分類するように構成された前記ネットワーク監視ユニットを備える、［Ｃ２６］に記載のネットワークルータ。
［Ｃ２９］
前記ネットワークトラフィック管理ノードにおいて前記未知のパケットストリームを検出することと、前記未知のパケットストリームのための前記デフォルト分類を選択することとを行うように構成された前記ネットワーク監視ユニットは、
前記ネットワークルータにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、
前記アプリケーションが未知であると判断したことに応答して前記未知のパケットスト

リームのための前記デフォルト分類を選択することと
を行うように構成された前記ネットワーク監視ユニットを備える、［Ｃ２６］に記載のネットワークルータ。
［Ｃ３０］
前記ネットワークルータにおいて前記未知のパケットストリームを検出することと、前記未知のパケットストリームのための前記デフォルト分類を選択することとを行うように構成された前記ネットワーク監視ユニットは、
前記ネットワークルータにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、
前記未知のパケットストリームに関連するアプリケーションタイプを判断することと、
前記未知のパケットストリームに関連する前記アプリケーションタイプに基づいて前記未知のパケットストリームのための前記デフォルト分類を選択することと
を行うように構成された前記ネットワーク監視ユニットを備える、［Ｃ２６］に記載のネットワークルータ。
［Ｃ３１］
クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、前記未知のパケットストリームに関連する情報を報告するように構成された前記ネットワーク監視ユニットが、前記未知のパケットストリームに関連するパケットストリーム特性を報告するように構成された前記ネットワーク監視ユニットを備える、［Ｃ２６］に記載のネットワークルータ。
［Ｃ３２］
前記未知のパケットストリームの後での検出および分類のために前記ネットワークルータにおいて前記パケットストリーム検出ポリシー更新を実装するように構成された前記ネットワーク監視ユニットが、
前記パケットストリーム検出ポリシー更新に従って前に未知であったパケットストリームに関連するパケットストリーム特性を検出することと、
前記パケットストリーム検出ポリシー更新に従って前記パケットストリーム特性に関連するアプリケーションを判断することと、
前記パケットストリーム特性に関連する前記アプリケーションに基づいて前記前に未知であったパケットストリームのための分類を選択することと
を行うように構成された前記ネットワーク監視ユニットを備える、［Ｃ２６］に記載のネットワークルータ。
［Ｃ３３］
命令を記憶した１つまたは複数の機械可読記憶媒体であって、前記命令が、１つまたは複数のプロセッサによって実行されたとき、
ローカルエリアネットワーク（ＬＡＮ）において検出された複数のパケットストリームを分類することと、
前記ＬＡＮにおいて未知のパケットストリームを検出することと、
前記未知のパケットストリームのためのデフォルト分類を選択することと、
クラウドベースコンピューティングネットワークの１つまたは複数のサーバに、前記未知のパケットストリームに関連する情報を報告することと、
前記クラウドベースコンピューティングネットワークから前記未知のパケットストリームのためのパケットストリーム検出ポリシー更新を受信することと、
前記未知のパケットストリームを後で検出し、分類するために前記パケットストリーム検出ポリシー更新を実装することと
を備える動作を前記１つまたは複数のプロセッサに実行させる、１つまたは複数の機械可読記憶媒体。
［Ｃ３４］
前記ＬＡＮにおいて検出された前記複数のパケットストリームを分類する前記動作が、前記複数のパケットストリームの各々に関連するアプリケーションと、前記複数のパケッ

トストリームの各々に関連するアプリケーションタイプとのうちの少なくとも１つに基づいて前記複数のパケットストリームを分類することを備える、［Ｃ３３］に記載の機械可読記憶媒体。

［Ｃ３５］

前記未知のパケットストリームを検出することと、前記未知のパケットストリームのための前記デフォルト分類を選択することとの前記動作は、

ＬＡＮにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、

前記アプリケーションが未知であると判断したことに応答して前記未知のパケットストリームのための前記デフォルト分類を選択することと

を備える、［Ｃ３３］に記載の機械可読記憶媒体。

［Ｃ３６］

前記未知のパケットストリームを検出することと、前記未知のパケットストリームのための前記デフォルト分類を選択することとの前記動作は、

前記ＬＡＮにおいて受信されたパケットストリームに関連するアプリケーションが未知であると判断することと、

前記未知のパケットストリームに関連するアプリケーションタイプを判断することと、

前記未知のパケットストリームに関連する前記アプリケーションタイプに基づいて前記未知のパケットストリームのための前記デフォルト分類を選択することと

を備える、［Ｃ３３］に記載の機械可読記憶媒体。

【図１】

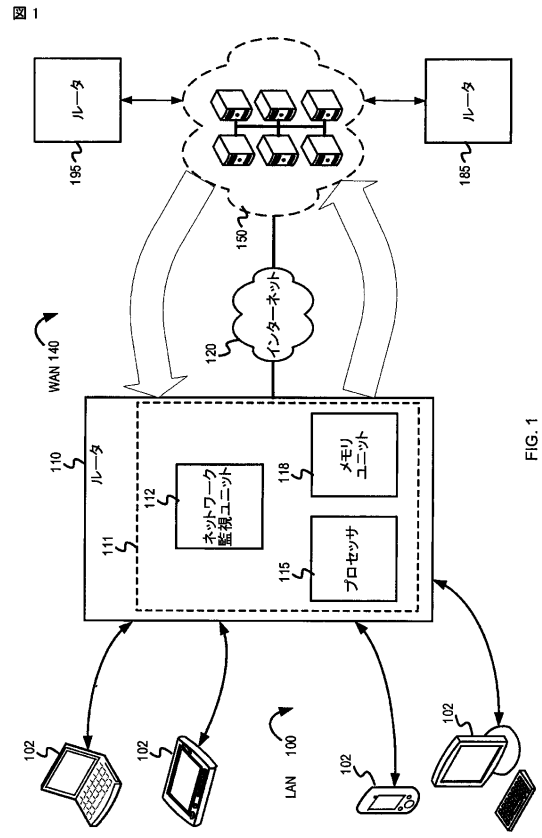

FIG. 1

【図２】

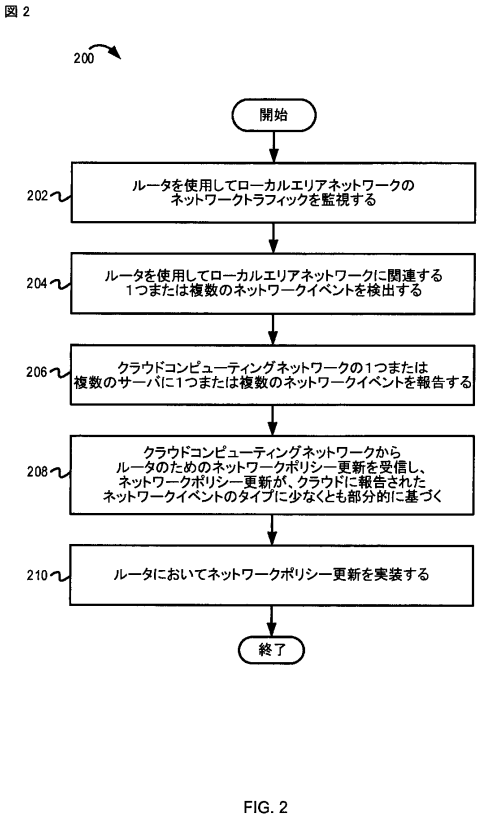

FIG. 2

【図３】

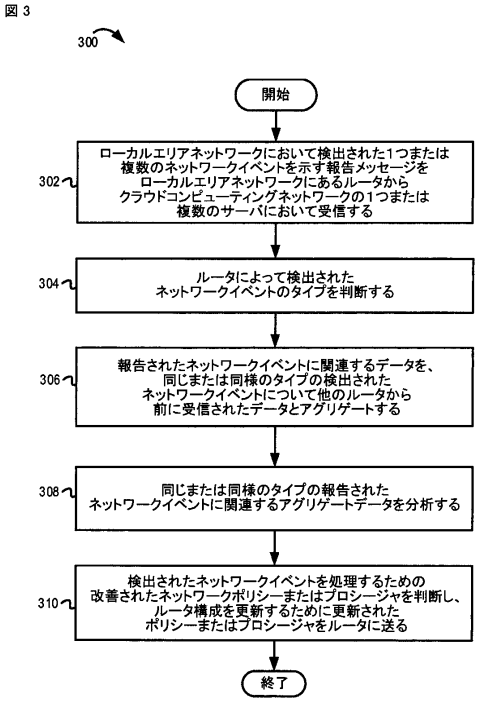

FIG. 3

【図４】

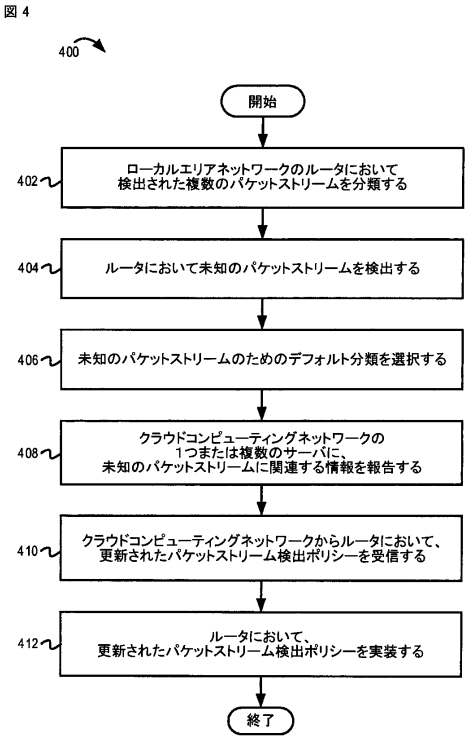

FIG. 4

【図５】

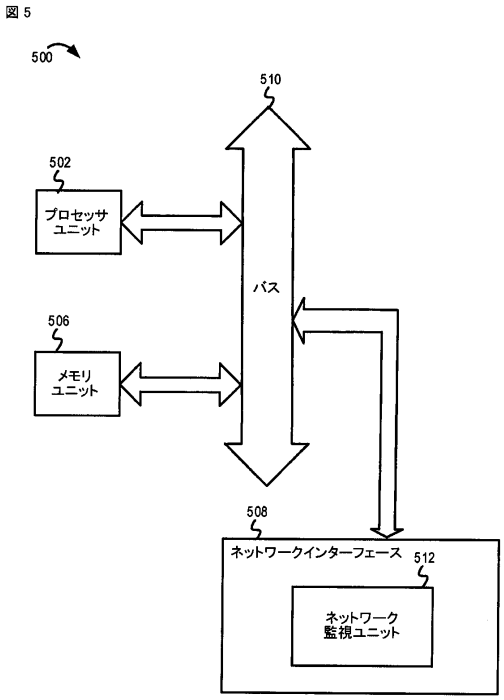

FIG. 5

フロントページの続き

(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100158805
弁理士 井関 守三
(74)代理人 100179062
弁理士 井上 正
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(72)発明者 ダンラップ、ウェイン・ジー.
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５、クゥアルコム・インコーポレイテッド気付
(72)発明者 メンチャカ、ベンジャミン・エム.
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５、クゥアルコム・インコーポレイテッド気付
(72)発明者 ノワコフスキー、ライアン・エー.
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５、クゥアルコム・インコーポレイテッド気付

審査官 宮島 郁美

(56)参考文献 特開２００１－２３７８９０（ＪＰ，Ａ）
特開２００２－２５２６１４（ＪＰ，Ａ）
特開２００１－２３７８３１（ＪＰ，Ａ）
国際公開第２０１１／０６１８０４（WO，Ａ１）
特開２００４－１８６７５３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ１２／００－１２／２６，１２／５０－１２／９５５