(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7511030号
(P7511030)

(45)発行日　令和6年7月4日(2024.7.4)

(24)登録日　令和6年6月26日(2024.6.26)

(51)国際特許分類

Ｈ０４Ｌ	*43/04*	*(2022.01)*	Ｈ０４Ｌ	43/04
Ｈ０４Ｗ	*88/18*	*(2009.01)*	Ｈ０４Ｗ	88/18
Ｈ０４Ｗ	*92/24*	*(2009.01)*	Ｈ０４Ｗ	92/24

ＦＩ

請求項の数　28　（全27頁）

(21)出願番号　特願2022-576820(P2022-576820)
(86)(22)出願日　令和2年6月16日(2020.6.16)
(65)公表番号　特表2023-530118(P2023-530118A)
(43)公表日　令和5年7月13日(2023.7.13)
(86)国際出願番号　PCT/EP2020/066597
(87)国際公開番号　WO2021/254600
(87)国際公開日　令和3年12月23日(2021.12.23)
審査請求日　令和5年2月6日(2023.2.6)

(73)特許権者　598036300
テレフオンアクチーボラゲット エルエム エリクソン（パブル）
スウェーデン国 ストックホルム エス－１６４ ８３
(74)代理人　100109726
弁理士　園田 吉隆
(74)代理人　100150670
弁理士　小梶 晴美
(74)代理人　100194294
弁理士　石岡 利康
(72)発明者　テスレンコ， マキシム
スウェーデン国 エスエー－１９２ ７４ ソーレントゥーナ， リリーズ ヴェーグ ８０

最終頁に続く

(54)【発明の名称】　ネットワークトラフィックアクティビティを報告するための技法

(57)【特許請求の範囲】

【請求項１】

複数のモバイルデバイス（１０８）のネットワークトラフィックアクティビティについて生成されたデータレコード中に含まれる情報を報告する方法であって、各データレコードが、モバイルデバイス（１０８）のトラフィックアクティビティのトラフィックタイプと、前記トラフィックアクティビティのタイムスタンプと、前記モバイルデバイス（１０８）の識別子と、前記モバイルデバイスに関連付けられた地理的エリアと、を含み、前記方法は、

監視タイプを指定する監視要求を受信すること（３０２）と、

所与の監視期間内に、以下の条件、

ｉ）　前記トラフィックアクティビティのトラフィックタイプが前記監視タイプに一致する、

ｉｉ）　前記トラフィックアクティビティのタイムスタンプが前記監視期間内に入る、ならびに

ｉｉｉ）　同じ識別子および同じトラフィックアクティビティに関連付けられたトラフィックアクティビティが監視期間ごとに１回のみ考慮される、

ｉｖ）　前記トラフィックアクティビティの地理的ロケーションが前記地理的エリア内に入る、

を満たすトラフィックアクティビティを有するモバイルデバイス（１０８）の数を前記データレコードから計算すること（３０４）と、

前記監視要求に応答して、モバイルデバイス（１０８）について計算された前記数に基づく監視報告を返すこと（３０６）と
を含み、
前記モバイルデバイスの各々に関する識別情報が前記監視報告において匿名化されている、方法。
【請求項２】
条件ｉｉｉ）を満たすために、条件ｉ）と条件ｉｉ）とを同時に満たす複数のデータレコードが所与のモバイルデバイス（１０８）について１回のみ考慮される、
請求項１に記載の方法。
【請求項３】
各トラフィックアクティビティが、一連のプロトコルデータユニット（ＰＤＵ）の送信を含み、１つのデータレコードが１つのＰＤＵから生成されている、
請求項１または２に記載の方法。
【請求項４】
各ＰＤＵが、ＰＤＵヘッダとＰＤＵペイロードとを有し、特定のデータレコード中に含まれるトラフィックタイプが、ＰＤＵヘッダ検査とＰＤＵペイロード検査とのうちの少なくとも１つから決定される、
請求項３に記載の方法。
【請求項５】
前記ＰＤＵが、インターネットプロトコル（ＩＰ）ＰＤＵとハイパーテキスト転送プロトコル（ＨＴＴＰ）ＰＤＵとから選択される、
請求項３または４に記載の方法。
【請求項６】
前記データレコードのうちの個々の１つを生成することが、
特定のモバイルデバイス（１０８）の現在のトラフィックアクティビティについて、前記トラフィックアクティビティのトラフィックタイプと前記モバイルデバイス（１０８）の識別子とを指示する、測定報告を受信することと、
前記モバイルデバイス（１０８）の前記識別子に基づいて、前記トラフィックアクティビティの前記地理的ロケーションを要求することと、
前記トラフィックアクティビティの前記地理的ロケーションを受信することと、
前記地理的ロケーションを前記トラフィックタイプと前記特定のモバイルデバイスの前記識別子とに関連付けるデータレコードを生成することと、
前記データレコードにタイムスタンプを提供することと
を含む、
請求項１から５のいずれか一項に記載の方法。
【請求項７】
前記データレコードが、前記現在のトラフィックアクティビティとともに実質的にリアルタイムで生成される、
請求項６に記載の方法。
【請求項８】
前記監視報告が、
－　モバイルデバイス（１０８）のＮ個の数を取得するように前記監視期間中に前記計算をＮ回実施することと、
－　このようにして取得されたモバイルデバイスの前記Ｎ個の数を平均化することと
によって導出されたモバイルデバイス（１０８）の平均数を含む
請求項１から７のいずれか一項に記載の方法。
【請求項９】
個々の前記計算が、前記監視期間にわたって時間的に等間隔である、
請求項８に記載の方法。
【請求項１０】

個々の前記計算の各々が前記監視期間の専用サブ期間について実施される、
請求項８または９に記載の方法。
【請求項１１】
前記監視報告が、前記条件を満たす前記データレコードから導出された値を含む、
請求項１から１０のいずれか一項に記載の方法。
【請求項１２】
前記値が、トラフィックタイプと、下位階層レベルにおける複数のトラフィックタイプを包含する一般トラフィックタイプと、前記条件を満たす前記データレコードに基づいて機械学習アルゴリズムによって行われた予測と、前記予測の時間的有効性と、平均トラフィック持続時間とのうちの１つまたは複数を指示する、
請求項１１に記載の方法。
【請求項１３】
前記監視期間が前記監視要求中で指定される、
請求項１から１２のいずれか一項に記載の方法。
【請求項１４】
前記監視期間が、１つまたは複数の可変ネットワークパラメータの関数である、
請求項１から１３のいずれか一項に記載の方法。
【請求項１５】
前記トラフィックタイプが、ネットワークトラフィックに関与するアプリケーション（１０２Ｂ）のアプリケーション識別子と、前記ネットワークトラフィックの宛先の宛先ドメイン名とのうちの少なくとも１つを指示するかまたはこれらのうち少なくとも１つから導出される、
請求項１から１４のいずれか一項に記載の方法。
【請求項１６】
匿名化のために、下位階層レベルにおける２つまたはそれ以上のトラフィックタイプが、前記計算において、上位階層レベルにおける単一の一般トラフィックタイプにマッピングされる、
請求項１から１５のいずれか一項に記載の方法。
【請求項１７】
異なるアプリケーション識別子と異なる宛先ドメイン名との一方または両方が、下位レベルトラフィックタイプとして、前記上位階層レベルにおける単一の一般トラフィックタイプにマッピングされる、
請求項１６に記載の方法。
【請求項１８】
前記監視要求が、監視されるべき地理的エリアをさらに指定する、
請求項１から１７のいずれか一項に記載の方法。
【請求項１９】
前記地理的ロケーションがセル識別子によって規定される、
請求項１８に記載の方法。
【請求項２０】
前記トラフィックアクティビティの前記地理的ロケーションが前記地理的エリア内に入るかどうかを決定するために、セル識別子と地理的エリアとの間のマッピングを調べることを含む、請求項１９に記載の方法。
【請求項２１】
コンピュータプログラム製品であって、前記コンピュータプログラム製品がプロセッサ上で実行されたとき、請求項１から２０のいずれか一項に記載の方法のステップを実施するように設定されたプログラムコード部分を含む、コンピュータプログラム製品。
【請求項２２】
コンピュータ可読記録媒体に記憶された、請求項２１に記載のコンピュータプログラム製品。

【請求項２３】
複数のモバイルデバイス（１０８）のネットワークトラフィックアクティビティについて生成されたデータレコード中に含まれる情報を報告するように設定されたネットワーク装置（１１２）であって、各データレコードが、モバイルデバイス（１０８）のトラフィックアクティビティのトラフィックタイプと、前記トラフィックアクティビティのタイムスタンプと、前記モバイルデバイスの識別子と、前記モバイルデバイスに関連付けられた地理的エリアとを含み、前記ネットワーク装置は、
監視タイプを指定する監視要求を受信することと、
所与の監視期間内に、以下の条件、
ｉ） 前記トラフィックアクティビティのトラフィックタイプが前記監視タイプに一致する、
ｉｉ） 前記トラフィックアクティビティのタイムスタンプが前記監視期間内に入る、ならびに
ｉｉｉ） 同じ識別子および同じトラフィックアクティビティに関連付けられたトラフィックアクティビティが監視期間ごとに１回のみ考慮される、
ｉｖ） 前記トラフィックアクティビティの地理的ロケーションが前記地理的エリア内に入る、
を満たすトラフィックアクティビティを有する、モバイルデバイス（１０８）の数を前記データレコードから計算することと、
前記監視要求に応答して、モバイルデバイス（１０８）について計算された前記数に基づく監視報告を返すことと
を行うように設定され、
前記モバイルデバイスの各々に関する識別情報が前記監視報告において匿名化されている、ネットワーク装置（１１２）。
【請求項２４】
第４世代モバイル通信ネットワーク（１００）のパケットゲートウェイノードとして設定されるかまたは前記パケットゲートウェイノード上に位置する、請求項２３に記載のネットワーク装置。
【請求項２５】
第５世代のモバイル通信ネットワーク（１００）のネットワークデータ分析機能として設定されるかまたは前記ネットワークデータ分析機能とコロケートされた、請求項２３に記載のネットワーク装置。
【請求項２６】
請求項２３から２５のいずれか一項に記載のネットワーク装置（１１２）と、
そのネットワークトラフィックアクティビティに関する情報が報告されるべきである、モバイルデバイス（１０８）の第１のセットについてのネットワークトラフィックをルーティングするように設定された第１のゲートウェイノードと、
そのネットワークトラフィックアクティビティに関する情報が報告されるべきでない、モバイルデバイス（１０８）の第２のセットについてのネットワークトラフィックをルーティングするように設定された第２のゲートウェイノードと
を備える、ネットワークシステム（１０００）。
【請求項２７】
請求項２３から２５のいずれか一項に記載のネットワーク装置（１１２）と、
そのネットワークトラフィックアクティビティに関する情報が報告されるべきである、モバイルデバイス（１０８）についてのネットワークトラフィックをルーティングするように設定された第１のゲートウェイノードであって、前記第１のゲートウェイノードは、再ルーティング条件が満たされるまで、ルーティングすることを実施する、第１のゲートウェイノードと、
前記再ルーティング条件が満たされた後にモバイルデバイス（１０８）のセットについてのネットワークトラフィックをルーティングするように設定された第２のゲートウェイ

ノードと
を備える、ネットワークシステム（１０００）。
【請求項２８】
前記再ルーティング条件が、モバイルデバイス（１０８）ごとに個々に開始されたあらかじめ規定された時間期間の経過である、
請求項２７に記載のネットワークシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、一般に、モバイルデバイスのネットワークトラフィックアクティビティを報告することを目的として通信ネットワークにおいて集められた情報を処理する分野に関する。本明細書で提示される技法は、方法、コンピュータプログラム製品、ネットワーク装置、およびネットワークシステムの形態で実装され得る。
【背景技術】
【０００２】
現在のモバイル通信ネットワークでは、モバイルデバイスのネットワークトラフィックパターンが、主に、サービス品質保証と、課金契約と、アドミッション制御とを含む、トラフィックハンドリングポリシおよび他のネットワーク関係ポリシを施行するために分析される。いくつかの実装形態では、関連するトラフィック分析が、ポリシ制御および課金ルール機能（ＰＣＲＦ）によってコアネットワークドメインにおいて行われる。ＰＣＲＦベースポリシ施行のためにネットワークトラフィックアクティビティに関する情報を公開することに加えて、第４世代（４Ｇ）／Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ（ＬＴＥ）通信ネットワークにおけるサービス能力公開機能（ＳＣＥＦ）と第５世代（５Ｇ）通信ネットワークにおけるネットワーク公開機能（ＮＥＦ）とを含む、サービス公開機能による何らかのさらなる情報公開がある。この場合、公開される情報は、主に、コネクティビティの側面（たとえば、ローミングステータス、通信障害、ダウンリンクデータ障害の後の利用可能性、ある地理的エリア中のモバイルデバイスの数、無線アクセスネットワーク輻輳の検出、コネクティビティの喪失、および到達可能性）に関する。
【０００３】
その上、５Ｇ通信ネットワークのために新たに導入されたネットワークデータ分析機能（ＮＷＤＡＦ）も分析サービスを提供する。これらのサービスは、ＳＣＥＦおよびＮＥＦと同様のサブスクライブ／通知モデルを使用して提供される。ＮＷＤＡＦの目的は、トラフィック監視インサイト（ｉｎｓｉｇｈｔ）を提供することである。そのようなインサイトの例は、アクティブネットワークスライスの負荷ステータス、アプリケーション性能、または、モバイルデバイスの挙動を予測／分析することを含む。
【０００４】
上記で説明されたネットワーク機能は、サービス品質監視の目的でネットワークトラフィック情報を公開すること、モバイルインフラストラクチャステータスの監視、またはモバイルデバイスステータスの監視を目標としており、監視される情報は、主に、それぞれのアセットの所有者、たとえば、ネットワークオペレータおよび／またはデバイス所有者を対象とする。したがって、公開される情報は、典型的に、モバイルデバイスの識別情報、またはモバイルデバイスのグループの識別情報のいずれかを含む。しかしながら、いくつかの場合には、モバイルデバイスのネットワークトラフィックアクティビティに関するインサイトを匿名で報告することが望まれる。
【０００５】
この点についての１つのソリューションは、たとえば、関連付けられたデバイス識別子を開示することなしに、いくつかのフィルタ処理基準を満たすモバイルデバイスの数を報告することによる、情報アグリゲーションである。しかしながら、その報告が、特に、監視期間が、拡張された時間期間をカバーし得るとき、（たとえば、プロトコルデータユニット（ＰＤＵ）レベルにおける）高度に粒度の細かい情報から生成されるべきである場合

、様々な課題が存在する。
【発明の概要】
【０００６】
モバイルデバイスのネットワークトラフィックアクティビティについて集められた情報を効率的に報告するための技法が必要である。
【０００７】
第１の態様によれば、複数のモバイルデバイスのネットワークトラフィックアクティビティについて生成されたデータレコード中に含まれる情報を報告する方法が提供される。各データレコードが、モバイルデバイスのトラフィックアクティビティのトラフィックタイプと、トラフィックアクティビティのタイムスタンプと、モバイルデバイスの識別子とを含む。本方法は、監視タイプを指定する監視要求を受信することと、所与の監視期間内に、以下の条件、
ｉ） トラフィックアクティビティのトラフィックタイプが監視タイプに一致する、
ｉｉ） トラフィックアクティビティのタイムスタンプが監視期間内に入る、ならびに
ｉｉｉ） 同じ識別子および同じトラフィックアクティビティに関連付けられたトラフィックアクティビティが監視期間ごとに１回のみ考慮される、
を満たすトラフィックアクティビティを有するモバイルデバイスの数をデータレコードから計算することとを含む。
第１の態様の方法は、監視要求に応答して、モバイルデバイスの計算された数に基づく監視報告を返すことをさらに含む。
【０００８】
監視報告は、モバイルデバイスの計算された数に基づき、監視タイプおよび監視期間に関連付けられたトラフィックアクティビティのモバイルデバイスにわたる範囲（ｅｘｔｅｎｔ）を指示する、パラメータを含み得る。いくつかの変形態では、パラメータは、（たとえば、監視期間に対応する特定の時間的ポイントについての）そのようなものとしてのモバイルデバイスの計算された数であり得る。他の変形態では、パラメータは、（たとえば、監視期間内の異なる時間的ポイントについての）デバイスの２つまたはそれ以上の個々に計算された数を平均化することによって導出されたモバイルデバイスの平均化された数であり得る。したがって、監視期間は、時間的ポイントであるように規定され得るか、または（たとえば、秒、分、時間、または日の）より長い時間的拡張を有し得る。
【０００９】
監視報告は、匿名化された情報のみを含み得る。たとえば、その報告は、モバイルデバイスの計算された数中に含まれる特定のモバイルデバイスまたは特定のデバイスグループを識別することを可能にする情報を含まないことがある。特に、その報告は、モバイルデバイス識別子を含まないことがある。
【００１０】
いくつかの変形態では、モバイルデバイスごとに複数回、同じトラフィックアクティビティおよび同じトラフィックタイプに関連付けられた複数のデータレコードをカウントし、したがって、モバイルデバイスの実際の数の計算を偽る（ｆａｌｓｉｆｙ）ことを回避するために、同じ識別子および同じトラフィックアクティビティに関連付けられたトラフィックアクティビティが監視期間ごとに１回のみ考慮される。一実装形態では、条件ｉｉｉ）を満たすために、条件ｉ）と条件ｉｉ）とを同時に満たすモバイルデバイスごとの複数のデータレコードが１回のみ考慮される。たとえば、所与のモバイルデバイスについての、条件ｉ）と条件ｉｉ）とを満たすデータレコードのセットのうち、１つのデータレコード（たとえば、監視期間内の第１のもの）のみが実際に考慮されて、デバイスの数の現在のカウントを増分し、他のデータレコードは（さらなる）増分をもたらさない。
【００１１】
各トラフィックアクティビティが、一連のプロトコルデータユニット（ＰＤＵ）の送信を含み得る。ＰＤＵは、オープンシステムインターコネクション（ＯＳＩ）モデルの任意の特定のレイヤ上の特定の通信プロトコルに関連付けられ得る。そのレイヤに応じて、そ

のようなＰＤＵは、たとえば、セグメントまたはデータグラム（レイヤ４）、データパケット（レイヤ３）、およびフレーム（レイヤ２）と呼ばれる。

【００１２】

一連のＰＤＵは、特定のモバイルデバイスのために確立されたセッションのコンテキストなどにおいて送信され得る。いくつかの場合には、１つのデータレコードが１つのＰＤＵから生成された。

【００１３】

各ＰＤＵが、ＰＤＵヘッダとＰＤＵペイロードとを有し得る。特定のデータレコード中に含まれるトラフィックタイプが、ＰＤＵヘッダ検査とＰＤＵペイロード検査とのうちの少なくとも１つによって（たとえば、データレコード生成時に）決定され得る。たとえば、ＰＤＵは、インターネットプロトコル（ＩＰ）ＰＤＵおよびハイパーテキスト転送プロトコル（ＨＴＴＰ）ＰＤＵから選択され得、次いで、対応するヘッダまたはペイロードが検査され得る。

【００１４】

データレコードのうちの個々の１つを生成することは、特定のモバイルデバイスの現在のトラフィックアクティビティについて、トラフィックアクティビティのトラフィックタイプとモバイルデバイスの識別子とを指示する、測定報告を受信することを含み得る。測定報告は、専用ＰＤＵ、または専用の一連のＰＤＵに関係し得る。測定報告は、ＰＤＵヘッダ検査とＰＤＵペイロード検査の一方または両方によって生成され得る。測定報告は、モバイル通信システムの無線アクセスネットワークドメインにおいてまたはコアネットワークドメインにおいて生成され得る。

【００１５】

第１の変形態によれば、データレコードのうちの個々の１つを生成することは、トラフィックタイプと特定のモバイルデバイスの識別子とを関連付けるデータレコードを生成することと、データレコードにタイムスタンプを提供することとをさらに含み得る。第２の変形態によれば、データレコードのうちの個々の１つを生成することは、モバイルデバイスの識別子に基づいて、トラフィックアクティビティの地理的ロケーションを要求することと、トラフィックアクティビティの地理的ロケーションを受信することと、地理的ロケーションをトラフィックタイプと特定のモバイルデバイスの識別子とに関連付けるデータレコードを生成することと、データレコードにタイムスタンプを提供することとをさらに含み得る。

【００１６】

これらの変形態では、データレコードは、現在のトラフィックアクティビティとともに実質的にリアルタイムで生成され得る。このようにして、タイムスタンプが、現在のトラフィックアクティビティが行われる時間を実際に指示することが保証され得る。

【００１７】

上記のように、監視報告は、モバイルデバイスの平均数を含み得る。この平均数は、モバイルデバイスのＮ個の数を取得するように監視期間中に計算をＮ回実施することと、このようにして取得されたモバイルデバイスのＮ個の数を（たとえば、加算された数をＮで除算することによって）平均化することとによって導出され得る。個々の計算が、監視期間にわたって時間的に等間隔であり得る。個々の計算の各々が、監視期間の（専用の時間的ポイントを含む）専用サブ期間について実施され得る。たとえば、ネットワーク負荷など、１つまたは複数のネットワークパラメータに応じて、計算の頻度が可変であり得る。

【００１８】

監視報告は、条件を満たすデータレコードから導出された値を含み得る。たとえば、監視報告は、＜タイプ，値＞データ構造中にその値を含め得る。このデータ構造中のタイプは、監視要求中で指定された監視タイプに対応し得る。値は、トラフィックタイプと、下位階層レベルにおける複数のトラフィックタイプを包含する一般トラフィックタイプと、条件を満たすデータレコードに基づいて機械学習アルゴリズムによって行われた予測と、予測の時間的有効性と、平均トラフィック持続時間とのうちの１つまたは複数を指示し得

る。監視タイプは、いくつかの変形態では、同じ階層レベルまたは一般トラフィックタイプよりも上位の階層レベルにおけるものであり得る。監視要求は、＜タイプ，値＞データ構造のリストを含み得、各値について、モバイルデバイスの関連する（場合によっては、平均化された）数が報告され得る。いくつかの変形態では、監視報告は、随意に、少なくとも１つの＜タイプ，値＞データ構造中に、モバイルデバイスの数を含めないが、少なくとも１つまたは複数の値を含める。

【００１９】

監視期間は、いくつかの変形態では、監視要求中で指定され得る。他の変形態では、監視期間は、ネットワークオペレータなどによって規定され得る。監視期間は、１つまたは複数の可変ネットワークパラメータの関数であり得る。一例として、監視期間は、ネットワーク負荷が増加するにつれて減少し得る。

【００２０】

トラフィックタイプは、トラフィックアクティビティを生じる、ネットワークトラフィックに関与するアプリケーションのアプリケーション識別子と、ネットワークトラフィックの宛先の宛先ドメイン名とのうちの少なくとも１つを指示するかまたは少なくとも１つから導出され得る。アプリケーションは、モバイル通信ネットワークの外部のアプリケーションサーバ上で稼働していることがある。宛先ドメイン名は、ユニバーサルリソース識別子（ＵＲＩ）の形態をとり得る。

【００２１】

匿名化のために、下位階層レベルの２つまたはそれ以上のトラフィックタイプが、計算において、上位階層レベルにおける単一の一般トラフィックタイプにマッピングされ得る。次いで、モバイルデバイスの数が、一般トラフィック指示にマッピングされた下位階層レベルのすべてのトラフィックタイプにわたって計算される。監視要求中で指定された監視タイプは、同じ階層レベルまたは各一般トラフィックタイプよりも上位の階層レベルに位置し得る。

【００２２】

たとえば、ＹｏｕＴｕｂｅトラフィックアクティビティとＮｅｔｆｌｉｘトラフィックアクティビティとが、両方とも、一般トラフィックタイプ「ビデオストリーミングトラフィック」にマッピングされ得る。したがって、監視要求が、監視タイプとして「ストリーミングトラフィック」（または「ビデオストリーミングトラフィック」）を指定したとき、ＹｏｕＴｕｂｅトラフィックアクティビティとＮｅｔｆｌｉｘトラフィックアクティビティのいずれか一方を有するモバイルデバイスがカウントされ、これは、報告される情報の匿名化を高める。もちろん、これは、監視要求中で指定された監視タイプが、そのようなものとしてトラフィックタイプ（たとえば、「Ｎｅｔｆｌｉｘトラフィック」）をも指示することができることを除外しない。

【００２３】

たとえば、異なるアプリケーション識別子と異なる宛先ドメイン名との一方または両方が、例示的な下位レベルトラフィックタイプとして、上位階層レベルにおける単一の一般トラフィックタイプにマッピングされ得る。一般トラフィックタイプは、次いで、一般トラフィックタイプにわたってフィルタ処理条件を満たすモバイルデバイスの（場合によっては、平均化された）数に加えて、監視報告中に値として含められ得る。

【００２４】

各データレコードは、トラフィックアクティビティ中のモバイルデバイスの地理的ロケーションをさらに含み得る。そのような場合、監視要求は、監視されるべき地理的エリアをさらに指定し得、モバイルデバイスの数を計算するとき、以下のさらなる条件、

ｉｖ） トラフィックアクティビティの地理的ロケーションが地理的エリア内に入る、

が考慮され得る。

【００２５】

地理的ロケーションは、一変形態では、セル識別子によって規定される。したがって、本方法は、トラフィックアクティビティの地理的ロケーションが地理的エリア内に入るか

どうかを決定するために、セル識別子と地理的エリアとの間のマッピングを調べることをさらに含み得る。

【００２６】

コンピュータプログラム製品であって、コンピュータプログラム製品がプロセッサ上で実行されたとき、本明細書で提示される方法のステップを実施するように設定されたプログラムコード部分を含む、コンピュータプログラム製品も提供される。本コンピュータプログラム製品は、コンピュータ可読記録媒体に記憶され得る。

【００２７】

さらなる態様によれば、複数のモバイルデバイスのネットワークトラフィックアクティビティについて生成されたデータレコード中に含まれる情報を報告するように設定されたネットワーク装置が提示され、各データレコードが、モバイルデバイスのトラフィックアクティビティのトラフィックタイプと、トラフィックアクティビティのタイムスタンプと、モバイルデバイスの識別子とを含む。本ネットワーク装置は、監視タイプを指定する監視要求を受信することと、所与の監視期間内に、以下の条件、

ｉ）　トラフィックアクティビティのトラフィックタイプが監視タイプに一致する、

ｉｉ）　トラフィックアクティビティのタイムスタンプが監視期間内に入る、ならびに

ｉｉｉ）　同じ識別子および同じトラフィックアクティビティに関連付けられたトラフィックアクティビティが監視期間ごとに１回のみ考慮される、

を満たすトラフィックアクティビティを有するモバイルデバイスの数をデータレコードから計算することとを行うように設定される。

本ネットワーク装置は、監視要求に応答して、モバイルデバイスの計算された数に基づく監視報告を返すようにさらに設定される。

【００２８】

本ネットワーク装置は、たとえば、無線アクセスネットワークドメインまたはコアネットワークドメイン中の、ネットワークノードとして設定されるかまたはネットワークノード上に位置し得る。したがって、本ネットワーク装置は、第４世代モバイル通信ネットワークのパケットゲートウェイノードとして設定されるかまたはパケットゲートウェイノード上に位置し得る。代替的に、本ネットワーク装置は、第５世代モバイル通信ネットワークのネットワークデータ分析機能として設定されるかまたはネットワークデータ分析機能とコロケートされ得る。

【００２９】

本明細書で提示されるネットワーク装置と、そのネットワークトラフィックアクティビティに関する情報が報告されるべきである、モバイルデバイスの第１のセットについてのネットワークトラフィックをルーティングするように設定された第１のゲートウェイノードと、そのネットワークトラフィックアクティビティに関する情報が報告されるべきでない、モバイルデバイスの第２のセットについてのネットワークトラフィックをルーティングするように設定された第２のゲートウェイノードとを備える、ネットワークシステムも提供される。

【００３０】

またさらに、本明細書で提示されるネットワーク装置と、そのネットワークトラフィックアクティビティに関する情報が報告されるべきである、モバイルデバイスについてのネットワークトラフィックをルーティングするように設定された第１のゲートウェイノードであって、第１のゲートウェイノードは、再ルーティング条件が満たされるまで、ルーティングすることを実施する、第１のゲートウェイノードとを備え、再ルーティング条件が満たされ後にモバイルデバイスのセットについてのネットワークトラフィックをルーティングするように設定された第２のゲートウェイノードをさらに備える、ネットワークシステムが提供される。いくつかの実装形態では、再ルーティング条件は、モバイルデバイスごとに個々に開始されたあらかじめ規定された時間期間の経過である。

【００３１】

本開示のさらなる態様、詳細および利点は、以下の例示的な実施形態の詳細な説明から

、および図面から明らかになろう。
【図面の簡単な説明】
【００３２】
【図１】本開示のネットワークシステム実施形態を示す図である。
【図２】本開示による、報告装置の一実施形態を示すブロック図である。
【図３】本開示の方法実施形態の流れ図である。
【図４】階層トラフィックタイプ構成を示す図である。
【図５】本明細書で提示される技法のための入力データのソースを示す表である。
【図６】本開示のＬＴＥ／４Ｇネットワークシステム実施形態を示す図である。
【図７】入力データについてのフィルタ処理ルールを示す表である。
【図８】ＬＴＥ／４Ｇおよび５Ｇネットワークアーキテクチャのコンテキストにおける本開示のさらなる実施形態を示す概略シグナリング図である。
【図９Ａ】ＬＴＥ／４Ｇおよび５Ｇネットワークアーキテクチャのコンテキストにおける本開示のさらなる実施形態を示す概略シグナリング図である。
【図９Ｂ】ＬＴＥ／４Ｇおよび５Ｇネットワークアーキテクチャのコンテキストにおける本開示のさらなる実施形態を示す概略シグナリング図である。
【図１０】ＬＴＥ／４Ｇおよび５Ｇネットワークアーキテクチャのコンテキストにおける本開示のさらなる実施形態を示す概略シグナリング図である。
【発明を実施するための形態】
【００３３】
以下の説明では、限定ではなく説明の目的で、本開示の完全な理解を提供するために、具体的な詳細が記載される。本開示が、これらの具体的な詳細から逸脱する他の実施形態において実践され得ることが、当業者には明らかであろう。
【００３４】
たとえば、以下の説明のいくつかの実施形態は、特定の４Ｇおよび５Ｇ仕様による例示的なコアネットワーク設定に焦点を当てるが、本開示はこの点について限定されない。本開示はまた、他のセルラまたは非セルラ無線通信ネットワークにおいて実装され得る。
【００３５】
さらに、本明細書で説明されるステップ、サービスおよび機能は、個々のハードウェア回路を使用して、プログラムされたマイクロプロセッサまたは汎用コンピュータとともに機能するソフトウェアを使用して、１つまたは複数の特定用途向け集積回路（ＡＳＩＣ）を使用して、および／あるいは１つまたは複数のデジタル信号プロセッサ（ＤＳＰ）を使用して、実装され得ることを当業者は諒解されよう。本開示が方法に関して説明されるとき、それがまた、１つまたは複数のプロセッサと、１つまたは複数のプロセッサに結合された１つまたは複数のメモリとにおいて具現され得、１つまたは複数のメモリが、１つまたは複数のプロセッサによって実行されたとき、本明細書で開示されるステップ、サービスおよび機能を実施する、１つまたは複数のコンピュータプログラムを記憶することも諒解されよう。
【００３６】
例示的な実施形態の以下の説明では、同じ参照番号は、同じまたは同様の構成要素を示す。
【００３７】
図１は、本開示が実装され得るネットワークシステム１０００の一実施形態を示す。図１に示されているように、ネットワークシステム１０００は、特定のネットワークオペレータによって動作されるモバイル通信ネットワーク１００を備える。ネットワークシステム１０００は、モバイル通信ネットワーク１００の外部のドメイン１０２をさらに備える。この外部ドメイン１０２は、モバイル通信ネットワーク１００と通信するように設定された１つまたは複数の外部ネットワーク、システムまたは構成要素を備え得る。例示的な外部ネットワークがインターネット１０２Ａであり、例示的な外部構成要素がアプリケーションサーバ１０２Ｂである。

【００３８】
いくつかの実施形態におけるアプリケーションサーバ１０２Ｂは、（サービスプロバイダと呼ばれることもある）コンテンツプロバイダによって動作されるコンテンツプロバイダシステムに属する。コンテンツプロバイダシステムは、場合によってはインターネット１０２Ａを介して、（インスタントメッセージング（ＩＭ）サービス、あるいはビデオまたはオーディオストリーミングサービスなどの）アプリケーションサービスを提供し得る。いくつかの変形態では、アプリケーションサーバ１０２Ｂは、オーバーザトップ（ＯＴＴ）アプリケーションサービスを提供するように設定される。そのようなＯＴＴアプリケーションサービスは、（典型的にセッションコンテキストにおいて）ビデオコンテンツまたはオーディオコンテンツをトランスポートするためにＯＴＴネットワークトラフィックを生成する。
【００３９】
図１に示されているように、モバイル通信ネットワーク１００は、コアネットワークドメイン１０４と無線アクセスネットワークドメイン１０６とを備える。モバイル通信ネットワーク１００は、複数のモバイルデバイス１０８をさらに備える。モバイルデバイス１０８は、ユーザ機器（ＵＥ）タイプのモバイルデバイス（たとえば、スマートフォンまたはタブレットコンピュータ）、およびモノのインターネット（ＩｏＴ）タイプのモバイルデバイス（たとえば、車およびウェアラブルデバイス）の形態をとり得る。
【００４０】
２つのドメイン１０４、１０６の各々は、アプリケーショントラフィックをトランスポートするためのユーザプレーンと、制御シグナリングをトランスポートするための制御プレーンとを備える。アクセスネットワークドメイン１０６は、セルラ設定または非セルラ設定を有し得る。いくつかの変形態では、アクセスネットワークドメイン１０６は、複数の基地局または無線アクセスポイントを備える。コアネットワークドメイン１０２によって提供されるサービスは、アクセスネットワークドメイン１０６を介して、外部ドメイン１０２とモバイルデバイス１０８との間で交換されるネットワークトラフィックのためのコアネットワーク処理機能１１０を含む。例示的なコアネットワーク処理機能１１０は、サービス品質施行、課金、モビリティ関係サービスなどを含む。
【００４１】
コアネットワークドメイン１０４によって、報告機能１１２も提供される。報告機能１１２は、論理エンティティまたはハードウェアエンティティであり得る。報告機能１１２は、５Ｇ通信ネットワークにおけるＮＷＤＡＦネットワーク機能（ＮＦ）の一部、またはＬＴＥ／４Ｇ通信ネットワークにおけるパケットゲートウェイ（ＰＧＷ）ノードの一部であり得る。
【００４２】
報告機能１１２は、モバイルデバイス１０８のネットワークトラフィックアクティビティについて生成されたデータレコード中に含まれる情報を報告するように設定される。そのようなネットワークトラフィックアクティビティは、特定のモバイルデバイス１０８が、特定のアプリケーションサーバ１０２Ａからビデオコンテンツをストリーミングすること、インターネット１０２を介して、別のアプリケーションサーバ１０２Ａ上のオンラインショッピングまたはニュースウェブサイトを訪問することなどを含み得る。
【００４３】
報告されるべき情報をフィルタ処理および分析するために報告機能１１２によってアクセスされるデータレコードは、一変形態では、コアネットワーク処理機能１１０から受信される。別の変形態では、これらのデータレコードは、コアネットワーク処理機能１１０から受信された情報に基づいて報告機能１１２によってローカルに生成される。図１に示されている実施形態では、データレコードは、報告機能のローカルデータベース１１２Ａに記憶されるが、データレコードは、コアネットワークドメイン１０４内のリモートデータベース（図示せず）にも記憶され得る。報告生成のために報告機能１１２によってアクセスされるデータレコードは、履歴データレコード、または進行中のネットワークトラフ

ィックアクティビティに関係するデータレコードであり得る。後者の場合、報告は、実質的に、進行中のトラフィックアクティビティとともにリアルタイムで行われ得る。

【００４４】

報告機能１１２は、専用監視要求に応答して報告機能１１２の報告を生成するように設定される。図１に示されているように、これらの監視要求は、モバイル通信ネットワーク１００中に内部的に位置するか、または外部的に（すなわち、外部ドメイン１０２中に）位置する、装置または機能１１４から受信される。いくつかの実装形態では、監視要求はアプリケーションサーバ１１４Ａによって生成され、要求された監視報告がアプリケーションサーバ１１４Ａに返される。

【００４５】

以下で、図１の報告機能１１２の装置実施形態が、図２を参照しながら説明され、報告機能１１２の動作が、図３の流れ図３００に示されている方法実施形態を参照しながら説明される。

【００４６】

図２Ａに示されている装置実施形態では、報告機能１１２は、プロセッサ２０２と、プロセッサ２０２に結合されたメモリ２０４とを備える。メモリ２０４は、プロセッサ２０２の動作を制御するプログラムコードを記憶する。本明細書において理解されるように、プロセッサ２０２などのプロセッサが、任意の処理回路を使用して実装され得、たとえば、単一の処理コアに限定されないが、また、（たとえば、クラウドコンピューティングリソースを使用して）分散トポロジーを有し得る。

【００４７】

報告機能１１２は、入力インターフェース２０６と出力インターフェース２０８とをさらに備える。２つのインターフェース２０６、２０８は、一方ではコアネットワーク処理機能１１０との通信のために設定され、他方では機能または装置１１４との通信のために設定される。

【００４８】

報告機能１１２のプロセッサ２０２は、データレコード中に含まれる情報を報告するように設定され、データレコードは、複数のモバイルデバイス１０８のネットワークトラフィックアクティビティについて生成される。各データレコードが、特定のモバイルデバイス１０８の特定のネットワークトラフィックアクティビティに関係する。特定のトラフィックアクティビティ（たとえば、特定のコンテンツストリーミングセッション）について、複数のデータレコードが生成され得る（およびデータベース１１２Ａに記憶され得る）。たとえば、各データレコードは、特定のトラフィックアクティビティのコンテキストにおいて、コアネットワークドメイン１０４とアクセスネットワークドメイン１０６とを介した外部ドメイン１０２から特定のモバイルデバイス１０８への（またはその逆の）送信のために生成された特定のＰＤＵに対応し得る。

【００４９】

各トラフィックアクティビティは、少なくとも１つのトラフィックタイプに関連付けられる。（１つまたは複数の）トラフィックタイプは、特定のトラフィックアクティビティに関与する特定のアプリケーションサーバ１０２Ｂによって提供されるコンテンツによって規定され得る。たとえば、アプリケーションサーバ１０２ＢがＮｅｔｆｌｉｘによって動作される場合、トラフィックタイプは、（論理階層の降順で）コンテンツストリーミング、ビデオストリーミング、およびＮｅｔｆｌｉｘトラフィックのうちの１つ（または複数）であり得る。

【００５０】

報告コンテキストにおいてプロセッサ２０２によって分析される各データレコードは、特定のモバイルデバイス１０８の特定のトラフィックアクティビティのトラフィックタイプ（または複数のそのようなタイプ）と、トラフィックアクティビティのタイムスタンプと、モバイルデバイス１０８の識別子とを含む。識別子は、たとえば、国際モバイル加入者識別情報（ＩＭＳＩ）の形態をとり得る。データレコードは、トラフィックアクティビ

ティ中のモバイルデバイス１０８の地理的ロケーションなど、さらなる情報を含み得る。この地理的ロケーションは、トラフィックアクティビティ中にモバイルデバイス１０８をサーブするアクセスネットワークドメイン１０６の特定のセルのセル識別子を介して、データレコード中で指示され得る。

【００５１】

次に、図３の流れ図３００を参照すると、報告機能１１２の動作は、監視要求を受信するステップ３０２を含む。監視要求は、報告機能１１２によってアプリケーションサーバ１１４Ａ、あるいは任意の他の機能または装置１１４、図１参照、から受信される（たとえば、入力インターフェース２０６を介してプロセッサ２０２によって受信される、図２参照）。監視要求は、（少なくとも）監視タイプを指定する。監視タイプは、報告機能１１２とアプリケーションサーバ１１４Ａの両方に知られている監視タイプのあらかじめ規定されたセットから選択され得る。監視要求中で指定された監視タイプは、（コンテンツストリーミング、ビデオストリーミング、またはＮｅｔｆｌｉｘトラフィックなど、任意の階層レベルにおける）特定のトラフィックタイプに対応し得る。監視タイプは、監視タイプが、報告機能１１２によって、１つまたは複数のトラフィックタイプの特定のセット上にマッピングされ得るように、規定され得る。

【００５２】

いくつかの変形態では、監視要求は、あらかじめ規定された時間期間（監視期間）など、報告機能１１２によって生成されるべき監視報告についての１つまたは複数のさらなるフィルタ処理基準を含む。時間期間は、相対的フォーマット（たとえば、日、週、月）でまたは絶対的フォーマット（たとえば、２０２０年５月１２日１６：００～１７：００、または今日、または今、または昨日）で指示され得る。特に、相対的フォーマットで指示されたときの、あらかじめ規定された時間期間は、報告頻度を規定し得る。あらかじめ規定された時間期間は、瞬間であり得る。監視要求中で規定されないとき、監視期間は、報告機能１１２のデフォルトセッティングであり得るか、または（たとえば、より高いネットワーク負荷が、より頻繁な報告、したがって、より短い監視期間をもたらす、ネットワーク負荷に基づいて）動的に規定され得る。

【００５３】

そのようなまたは代替変形態では、監視要求は、随意に、監視されるべき（すなわち、その（１つまたは複数の）報告が生成されるべきである）地理的エリアを指定し得る。地理的エリアの指定は、以下のパラメータ、すなわち、１つまたは複数の郵便番号、１つまたは複数のセル識別子、および地理的エリアの名前（たとえば、町名）のうちの少なくとも１つを含み得る。

【００５４】

方法は、プロセッサ２０２によって、所与の監視期間内に、いくつかの条件を満たすトラフィックアクティビティを有するモバイルデバイス１０８の数をデータレコードから計算すること（図３中のステップ３０４）をさらに含む。一変形態では、これらの条件は、

ｉ） トラフィックアクティビティのトラフィックタイプが、監視要求中で指定された監視タイプに一致する、

ｉｉ） トラフィックアクティビティのタイムスタンプが、監視要求中で指定されたまたは他の方法で規定された監視期間内に入る、ならびに

ｉｉｉ） 同じ識別子および同じトラフィックアクティビティに関連付けられたトラフィックアクティビティが監視期間ごとに１回のみ考慮される、

を含む。

【００５５】

条件ｉｉｉ）は、特定のモバイルデバイス１０８と特定の監視期間とについて、複数回、同じトラフィックアクティビティ（および同じトラフィックタイプ）に関連付けられた複数のデータレコードをカウントし、したがって、モバイルデバイス１０８の実際の数の計算を偽ることを回避するのを助ける。そのような偽りは、特に、データレコードが、高度に粒度の細かい性質のものである（たとえば、ＰＤＵごとに生成される）が、監視期間

が、時間的に瞬時でないが、実際の持続時間を有する場合、生じ得る。したがって、条件ｉ）と条件ｉｉ）とを同時に満たす複数のデータレコードが、監視期間ごとにおよびモバイルデバイス１０８ごとに１回のみ考慮される。たとえば、条件ｉ）と条件ｉｉ）とを満たすデータレコードのセットのうち、１つのデータレコード（たとえば、監視期間内の第１のもの）のみが実際に考慮されて、モバイルデバイス１０８の数の現在のカウントを増分し、他のデータレコードは、無視され、したがって、その数の（さらなる）増分をもたらさない。

【００５６】

監視要求が、監視されるべき地理的エリアをさらに指定した場合、ステップ３０４においてモバイルデバイス１０８の数を計算するとき、以下のさらなる条件、

ｉｖ） トラフィックアクティビティの地理的ロケーションが地理的エリア内に入る、

が考慮される。

【００５７】

地理的ロケーションが、データレコード中のセル識別子を介して指示された場合、プロセッサ２０２は、条件ｉｖ）をテストするためにセル識別子と地理的エリアとの間のマッピングを調べ得る。

【００５８】

方法は、監視要求に応答して、モバイルデバイス１０８の計算された数に基づく監視報告を返すこと（図３中のステップ３０６参照）をさらに含む。たとえば、その報告は、プロセッサ２０２によって出力インターフェース２０８を介して機能または装置１１４に出力される（図１および図２参照）。匿名化を必要とする実施形態では、監視報告は、モバイルデバイス１０８の報告された数中に含まれる特定のモバイルデバイス１０８またはモバイルデバイスグループを識別することを可能にする情報を含まないことになる。特に、その報告は、モバイルデバイス識別子を含まないことになり、したがって、この点について匿名化された。言い換えれば、その報告は、いくつかのフィルタ処理条件を満たすトラフィックアクティビティをもつモバイルデバイスの特定のグループに関係し、そのようなものとしてモバイルデバイス１０８を機能または装置１１４に開示しない（したがって、機能または装置１１４は、プライバシーまたはセキュリティ問題を生じずに、外部ドメイン１０２中に位置し得る）。

【００５９】

一例では、報告機能１１２は、監視要求中で指示された監視タイプによって分類された現在の（「瞬間の」）需要を報告する。別の例では、報告機能１１２は、（たとえば、時系列分析の使用によって）将来の需要を予測するために履歴データレコードを使用する。需要は、いくつかの実装形態では、指示された監視タイプに準拠する特定のデジタルコンテンツについての「興味」として規定され得る。上記で説明されたように、「興味」は、随意に、特定の地理的エリアにおける、特定の時間期間についてのモバイルデバイス１０８の（たとえば、平均化された）数によって定量化される。

【００６０】

いくつかの変形態では、アクティブモバイルデバイス１０８のみがカウントされる。アクティブモバイルデバイス１０８は、無線リソース制御（ＲＲＣ）接続を確立し、データをアクティブに送信および受信するモバイルデバイス１０８である。５Ｇ通信ネットワーク１００の場合、モバイルデバイス１０８はＲＲＣ＿ＡＣＴＩＶＥ状態によって特徴づけられる。ＬＴＥ／４Ｇ通信ネットワーク１００の場合、モバイルデバイス１０８は、ＲＲＣ＿ＣＯＮＮＥＣＴＥＤ状態にあり、ユーザデータトランザクションを受けている。モバイルデバイス１０８がある状態に関する情報は、アクセスネットワークドメイン１０６から取得された情報から知られる。諒解されるように、アクティブモバイルデバイス１０８のみがセッションを確立し、データトラフィックを作り出すことができる。アクティブモバイルデバイス１０８に限定されるそのようなタイプのカウンティングは、少なくとも、それらのユーザによって忘れられ、データを送信する立場にないアイドルモバイルデバイス１０８をカウンティングすることを回避することを望むいくつかの使用事例について、

実施される。

【００６１】

したがって、（たとえば、監視要求中で指示された）所与の監視持続期間（ｐｅｒｉｏｄ　ｏｆ　ｄｕｒａｔｉｏｎ）t_dについて、特定の監視タイプについてのおよび特定の地理的エリアにおける興味Ｉが、Ｉ＝｛ロケーション，UE_{num}｝として表され（および報告され）得、ここで、ロケーション（随意）は地理的エリアであり、UE_{num}は、（モバイルデバイス１０８が、t_d内にロケーションに入り、ロケーションを出得るので）その地理的エリア中のモバイルデバイス１０８の（場合によっては、平均化された）数である。

【００６２】

地理的エリアは、モバイルデバイス１０８がアタッチされたアクセスネットワークドメイン１０６のセルの実際のロケーション、またはそのセルのロケーションと近似カバレッジエリアとを含むバウンディングボックスであり得る。また、実装形態に応じて、地理的エリアは、複数のセルを含むことができ、その場合、中心ポイントが選定されるか、またはより大きいバウンディングボックスが選定される。オペレータ固有の「セル識別子」または「セルＩＤ」によって識別される、モバイルデバイス１０８をサーブするセルのいわゆるジオロケーションが、ネットワークオペレータシステムが、セルのロケーションに関する情報と、そのセルにアタッチされたモバイルデバイス１０８に関する情報の両方を保持するので、そのシステムに知られている。例示的な４Ｇ通信ネットワーク１００としてのＬＴＥにおける担当するノードが、モビリティ管理エンティティ（ＭＭＥ）であり、担当するノードは、５Ｇ通信ネットワーク１００ではアクセスおよびモビリティ機能（ＡＭＦ）である。

【００６３】

報告について有効であるために、モバイルデバイスグループは、t_dの少なくとも一部分について、監視要求において規定された（１つまたは複数の）フィルタ処理条件を満たす少なくとも１つのモバイルデバイス１０８を含まなければならない。モバイルデバイス１０８の平均数を報告するために、モバイルデバイス１０８は、t_d内に周期的にサンプリングされ得る（たとえば、１００個のデータポイントのサンプルの場合、t_d／１００ごとの周期的サンプリングが実装され得る）。

【００６４】

監視報告において、興味Ｉは、１つまたは複数のいわゆるインサイトでオーグメントされ得、すなわち、Ｉ＝｛ロケーション，UE_{num}，インサイト｝であり、ここで、インサイト＝リスト＜タイプ，値＞である。インサイトは、監視要求中で指定された監視タイプによって少なくとも暗黙的に規定され得る（たとえば、データ構造＜タイプ，値＞中のパラメータ「タイプ」は、監視要求中で指定された監視タイプに対応し得る）。いくつかの変形態では、UE_{num}は、データ構造＜タイプ，値＞ごとに報告される。

【００６５】

インサイトの例示的な非限定的なタイプ、したがって、監視タイプが、以下で説明される。

【００６６】

第１のインサイト／監視タイプは、「人気がある宛先」と呼ばれる。この目的で、報告機能１１２は、ＰＤＵ中の宛先ドメイン名を（トラフィックタイプとして）識別するためにＰＤＵヘッダを分析する。報告機能は、さらに、図４において、一般的な＜タイプ，値＞データ構造について概略的に示されているように、上位レベルの一般トラフィックタイプの下で宛先ドメイン名をグループ化し得る。

【００６７】

この第１のインサイトは、人気があるＰＤＵ宛先（たとえば、アプリケーションサーバ１０２Ｂのどの（１つまたは複数の）一般のまたは特定のタイプがモバイルデバイス１０８によって実際に接触されるか）に関するものである。この分析は、アプリケーションレイヤＰＤＵ分析に基づき、特に、（たとえば、ＨＴＴＰ　ＰＤＵヘッダの分析による）宛先のドメイン名に基づき得る。その分析は、ユーザ興味を確立するために、ドメイン名カ

テゴリーのシソーラスを使用することができる（たとえば、ｈｔｔｐｓ：／／ｔｏｏｌｓ．ｚｖｅｌｏ．ｃｏｍ参照、カテゴリーは、ソーシャルメディア、ニュースサイト、車両製造業者、企業ウェブサイトなどであり得る）。

【００６８】

以下の例を考慮する。

・ あるモバイルデバイス１０８のユーザＡが、ｔ$_d$中の少なくともある時間の間ｈｔｔｐ：／／ｗｗｗ．ｔｅｃｈｒａｄａｒ．ｃｏｍを訪問する

・ 別のモバイルデバイス１０８のユーザＢが、ｔ$_d$中の少なくともある時間の間ｈｔｔｐ：／／ｗｗｗ．ｅｎｄａｄｇｅｔ．ｃｏｍを訪問する

・ またさらなるモバイルデバイス１０８のユーザＣが、ｔ$_d$中に少なくともある時間の間ｈｔｔｐ：／／ｗｗｗ．ｇｉｚｍｏｄｏ．ｃｏｍを訪問する

【００６９】

ユーザＡ、Ｂ、Ｃは、上記の規定通りに、同じ興味を共有するので、関連付けられたグループは、タイプ「人気がある宛先」と値「技術ウェブサイト」とのインサイトを有する。対応する監視報告が、報告タイプ「人気がある宛先」について複数の値を含み得、各報告タイプについて、モバイルデバイス１０８の専用の（たとえば、平均化された）数が報告されることに留意されたい。ユーザＡとユーザＢとユーザＣとを識別するために使用され得る、モバイルデバイス１０８の識別子（たとえば、ＩＭＳＩ）と明示的ウェブサイト名とが、監視報告中に含まれないことにさらに留意されたい。

【００７０】

第２のインサイト／監視タイプは、「人気があるアプリケーションカテゴリー」と呼ばれる。ここで、ＰＤＵヘッダは、関連付けられたトラフィックアクティビティを生成するアプリケーションを識別するために分析され、値としての、１つまたは複数の一般トラフィックアクティビティの下でのアプリケーションのグループ化に対するものである。このインサイトは、「人気がある宛先」アイデアの前の例と同様に、一般トラフィックアクティビティに関してアプリケーションを分類するためにアプリケーション識別子をトラフィックタイプとして使用する。この場合も、実際のアプリケーションと、そのアプリケーションを使用する実際のモバイルデバイス１０８とは、監視報告中で開示される必要がない。経時的に、このインサイトは、どんなタイプのアプリケーションが特定のエリアおよび／または時間において人気があるかの推定を与えることができる。場合によっては、暗号化されたＰＤＵからアプリケーション識別子を抽出することが行われ得、ｈｔｔｐｓ：／／ｗｗｗ．ｃａｉｄ　ａ．ｏｒｇ／ｒｅｓｅａｒｃｈ／ｔｒａｆｆｉｃ－ａｎａｌｙｓｉｓ／ｃｌａｓｓｉｆｉｃａｔｉｏｎ－ｏｖｅｒｖｉｅｗ／において指定した。

【００７１】

以下の例を考慮する。

・ あるモバイルデバイス１０８のユーザＡが、ｔ$_d$中の少なくともある時間の間Ｇｍａｉｌアプリを使用する

・ 別のモバイルデバイス１０８のユーザＢが、ｔ$_d$中の少なくともある時間の間Ｏｕｔｌｏｏｋアプリを使用する

・ またさらなるモバイルデバイス１０８のユーザＣが、ｔ$_d$中の少なくともある時間の間Ａｐｐｌｅ　Ｍａｉｌアプリを使用する

【００７２】

ユーザＡ、Ｂ、Ｃは、上記の規定により、同じ興味を共有するので、グループは、タイプ「人気があるアプリケーション」と値「電子メール」とのインサイトを有する。この場合も、モバイルデバイスユーザを識別するために使用され得る、モバイルデバイス識別子（たとえば、ＩＭＳＩ）と明示的アプリケーション名とが、公開されない。

【００７３】

第３のインサイト／監視タイプは、「短期グループ性向」と呼ばれる。ここで、モバイルデバイス１０８からの／への生成されたトラフィックが分析される。たとえば、モバイルデバイス１０８のユーザが、ＹｏｕＴｕｂｅからビデオをストリーミングしている場合

、そのユーザは、将来においてある時間期間の間さらなるビデオトラフィックを要求し続けることになる可能性が高い。ユーザがＮｅｔｆｌｉｘコンテンツをストリーミングしている場合、そのユーザは、ビデオトラフィックを要求するが、Ｎｅｔｆｌｉｘ上のビデオストリームがより長くなる傾向があるので、より長い時間期間の間そのビデオトラフィックを要求することになる可能性もある。さらに、モバイルデバイス１０８が、ビデオをストリーミングすることを停止した場合でも、そのユーザは、完全にアイドルであったモバイルデバイス１０８、またはウェブブラウジングのために使用されたモバイルデバイス１０８と比較して、何かをストリーミングすることを再び開始する可能性が高い。時間的相関のほかに、同じ地理的エリア中の同じモバイルデバイス１０８がデータ消費の典型的なパターンを有し得る。たとえば、ユーザが通勤しているとき、そのユーザは、典型的に、あるテレビ番組を見ていることがある。

【００７４】

以下の例を考慮する。

・ あるモバイルデバイス１０８のユーザＡが、t_d中の少なくともある時間の間Ｎｅｔｆｌｉｘ上でビデオを見た

・ 別のモバイルデバイス１０８のユーザＢが、t_d中の少なくともある時間の間Ｙｏｕｔｕｂｅ上でビデオを見た

・ さらなるモバイルデバイス１０８のユーザＣが、t_d中の少なくともある時間の間Ａｍａｚｏｎ上でビデオを見た

【００７５】

ユーザＡ、Ｂ、Ｃは、上記の規定により、同じ興味を共有するので、グループは、タイプ「グループ性向」と３つの値「ビデオ消費、８８％、１０分」とのインサイトを有し、ここで、割合は、予測についての機械学習アルゴリズムの信頼性レベルを示し、時間は、モバイルデバイスの所与のグループについて予測がどのくらいの時間の間有効であるかを示す。この場合も、モバイルデバイスユーザを識別するために使用され得る、モバイルデバイス識別子（たとえば、ＩＭＳＩ）と明示的アプリケーション名とが、得られた監視報告中で公開されない。

【００７６】

第４のインサイト／監視タイプは、「関与アウェアグループプロファイル（Ｅｎｇａｇｅｍｅｎｔ Ａｗａｒｅ Ｇｒｏｕｐ Ｐｒｏｆｉｌｅ）」と呼ばれる。ここで、関与アウェアグループプロファイルは、所与のセルに接続されたモバイルデバイス１０８のグループのアグリゲートされた選好を報告することができる高度分析サービスである。すべての接続されたモバイルデバイス１０８の選好および興味をもつプロファイルが、グループプロファイルを作成するために組み合わせられる。プロファイルを組み合わせるとき、ユーザのモバイルデバイス１０８とのユーザの対話のレベルに基づいて、異なるモバイルデバイス１０８のプロファイルを重み付けすることができる。通話中であるか、ビデオを見るか、またはアクティブブラウジングを行うユーザが、自分のモバイルデバイス１０８をアイドルに保つユーザと比較して、自分の周りで何が起きているかに関してほとんど関与しておらず、さらには、ほとんど気づいていないことになる。自分のモバイルデバイス１０８のインタラクティブなユーザは、エリア中のグループプロファイルにあまり寄与しないことになる。このタイプの関与アウェアグループプロファイル情報は、オンスクリーンターゲット広告のプロバイダにとって興味があるものであり得る。このタイプの広告は、バス、列車、駅、停留所などのような公共輸送エリアにおいて一般的になっている。そこの人々は、密に集結しており、広告メディアに対して静的なままでいる。また、ピコセルのような極小セルが、公共輸送エリア中に設置され、ＵＥ位置特定を極めて正確にすることが、一般的になっている。

【００７７】

以下の例を考慮する。

・ ユーザＡが、t_d中の少なくともある時間の間多くの通話を行った

・ ユーザＢが、t_d中の少なくともある時間の間多くのビデオを見た

・ ユーザＣが、すべての時間ｔｄの間インターネット１０２Ａをブラウズした

【００７８】

ユーザＡ、Ｂ、Ｃは、上記の規定により、同じ興味を共有するので、得られたモバイルデバイスグループは、タイプ「関与アウェアグループプロファイル」と値「１２％、１０分」とのインサイトを有し、ここで、割合は、グループ中のユーザがどのくらい関与することになるかに関する機械学習アルゴリズムの信頼性を示し、時間は、所与のモバイルデバイスグループについて予測がどのくらいの時間の間有効であるかを指示する。この場合も、モバイルデバイスユーザを識別するために使用され得る、モバイルデバイス識別子（たとえば、ＩＭＳＩ）と明示的アプリケーション名とが、得られた監視報告中で公開されない。

【００７９】

最後の２つの例から明らかになったように、監視報告は、いくつかの条件を満たす選択されたデータレコードに基づいて機械学習アルゴリズムによって行われた予測を指示する１つの値を含み得る。監視報告は、予測の時間的有効性を指示するさらなる値を含み得る。

【００８０】

図５の表５００は、モバイル通信ネットワーク１００の例示的なＬＴＥ／４Ｇおよび５Ｇ実装形態における報告機能１１２のための、ならびに上記で説明されたインサイト／監視タイプの４つの使用事例のための、入力データを提供するノードおよび機能を示す。その上、次に、ＬＴＥ／４Ｇおよび５Ｇ通信ネットワーク１００における図１のネットワークシステム１０００の例示的な実装形態がより詳細に説明される。この点について、図６は、ネットワークシステムのＬＴＥ／４Ｇ実装形態を示す。

【００８１】

図６の図は、動作中の典型的なＬＴＥ／４Ｇ通信ネットワーク１００を示す。そのような実装形態では、アクセスネットワークドメイン１０６は、複数のｅノードＢを含むことになり、コアネットワークドメイン１０４は、ＭＭＥ１０４Ａと、サービングゲートウェイ（ＳＧＦ）１０４Ｂと、ＳＣＥＦ１０４Ｃと、パケットフロー記述機能（ＰＦＤＦ：Ｐａｃｋｅｔ Ｆｌｏｗ Ｄｅｓｃｒｉｐｔｉｏｎ Ｆｕｎｃｔｉｏｎ）１０４Ｄと、ＰＧＷ（ＰＣＥＦ）１０４Ｅとを含むことになる。機能１０４Ａ～１０４Ｅは、図１に示されているコアネットワーク処理機能１１０に少なくとも部分的に対応し得る。同様の機能が５Ｇネットワークについて存在し、たとえば、ＭＭＥ１０４Ａの代わりにＡＭＦ、ＳＣＥＦ１０４Ｃの代わりにＮＥＦ、ＳＧＷ１０４ＢおよびＰＧＷ１０４Ｅは、それぞれ、ユーザプレーンおよび制御プレーントラフィックをハンドリングするＳＧＷ－Ｕ／ＳＧＷ－ＣおよびＰＧＷ－Ｕ／ＰＧＷ－Ｃにスプリットされる。

【００８２】

図６に示されているように、ＰＧＷ１０４ＥはＰＣＥＦを含んでおり、ＰＣＥＦは、ＳＧＷ１０４Ｂから受信された／ＳＧＷ１０４Ｂのほうへ送られたネットワークデータトラフィックに対してポリシ制御および課金（ＰＣＣ）ルールを施行し、ＳＧＷ１０４Ｂは、（ｅノードＢをもつ）無線アクセスネットワーク（ＲＡＮ）ドメイン１０６および（ＬＴＥ／４Ｇのコンテキストにおいて ＵＥとも呼ばれる）モバイルデバイス１０８から受信する／それらのほうへネットワークデータを送る。これは、ＰＣＥＦ（および、したがって、ＰＧＷ１０４Ｅ）が、あらゆる着信ＰＤＵ（ここでは、ＩＰデータパケット）のヘッダを、このＰＤＵをそのＰＤＵの対応するサービスクラスにマッピングするために検査することを意味する。このマッピングは、サービスデータフロー（ＳＤＦ）を使用して行われ、検査は、ＩＰ（ネットワーク）レイヤ上で行われ、随意に、トランスポートレイヤ上でも行われる。一例が、図７の表において示されている。

【００８３】

図７の表は、特定のモバイルデバイス１０８についてのすべてのユーザデータグラムプロトコル（ＵＤＰ）／リアルタイムトランスポートプロトコル（ＲＴＰ）トラフィック（すなわち、そのデバイス１０８から受信されたおよびそのデバイス１０８によって送られたトラフィック）が、フィルタ処理され、保証された１００Ｋｂｐｓアップリンク／ダウ

ンリンクをもつ高優先度データトンネル（３ＧＰＰ用語では「ＥＰＳベアラ」）を割り振られることを例示的に示す。ＳＤＦに加えて、また、アプリケーション識別子が提供される場合（アプリケーション識別子は、ＨＴＴＰなどのアプリケーションレイヤプロトコル、あるいはＹｏｕＴｕｂｅまたはＮｅｔｆｌｉｘなど、アプリケーションレイヤプロトコルを稼働する特定のアプリケーションを示すかまたはそれらから導出され得る）、アプリケーションフィルタをＰＣＣルールに供給し、ＳＤＦに適用する同じＱｏＳ、課金などのポリシを適用することが可能である。

【００８４】

各アプリケーションについて、このアプリケーションＩＤ（たとえば、サーバ側ＩＰアドレスおよびポート番号、またはＵＲＩ／ＵＲＬ、またはドメイン名など）の下でＩＰトラフィックをどこにルーティングすべきかに関する情報を含んでいるパケットフロー記述（ＰＦＤ）が存在する。ＰＦＤＦ１０４Ｄは、ＰＦＤを記憶および施行することを可能にするノードである。ＰＦＤＦ１０４Ｄは、ＳＣＥＦ１０４ＣへのノースバウンドインターフェースとＰＧＷ（ＰＣＥＦ）１０４Ｅへのサウスバウンドインターフェースとを有する。

【００８５】

一方、ＳＣＥＦ１０４Ｃは、モバイルネットワークオペレータのアドミニストレーティブドメイン内にあることもないこともある機能である、アプリケーションサーバ（ＡＳ）１１４Ａ（たとえば、ＡＳ１１４Ａは、外部ドメイン１０２中の企業サーバ上に位置し得る）が、（導入において述べられたものなどの）ＵＥコネクティビティの側面を中心として監視イベントにセキュアにサブスクライブすることを可能にする。そのプロセスは、ＡＳ１１４ＡによってＳＣＥＦ１０４Ｃにサブミットされる「監視要求」メッセージを含み、その後、ＳＣＥＦ１０４Ｃは、要求された情報を取り出すために、ＭＭＥ１０４ＡおよびＰＣＲＦ（図示せず）などのノードを内部的にポーリングする。イベントについて、新しい情報が利用可能であるとき、ＳＣＥＦ１０４Ｃは、「監視報告」メッセージを使用してＡＳ１１４Ａにその情報を報告する。そのようなものとしての「監視要求」メッセージおよび「監視報告」メッセージは、適用可能な規格において規定されている（たとえば、３ＧＰＰ　ＴＳ２３．６８２、第３世代パートナーシッププロジェクト、技術仕様グループサービスおよびシステム態様、パケットデータネットワークおよびアプリケーションとの通信を容易にするためのアーキテクチャ拡張（リリース１３）参照）。また、同じプロセスが、５Ｇ通信ネットワークおよびＮＥＦにおいて利用可能である。

【００８６】

したがって、図６のＬＴＥ／４Ｇ通信ネットワーク１００における技術手段は、ネットワークデータトラフィックをキャプチャし、フィルタ処理することを許可する。しかしながら、このネットワークデータトラフィックに関する情報を（たとえば、外部ドメイン１０２中の）サードパーティに公開するための現在の機構は、そのトラフィックについてのポリシ管理に限定され、トラフィックパターン自体の分析を実施していない。

【００８７】

これらの限定を克服するために、ユーザデータインサイト生成器機能（ＵＤＩＧＦ：Ｕｓｅｒ　Ｄａｔａ　Ｉｎｓｉｇｈｔ　Ｇｅｎｅｒａｔｏｒ　Ｆｕｎｃｔｉｏｎ）と呼ばれる新しい機能がコアネットワークドメイン１０４に追加されることが提案される。ＵＤＩＧＦは、上記で説明された報告機能１１２の動作の一部または全部を実装し得、したがって、以下で、シグナリング図８、シグナリング図９Ａおよびシグナリング図９Ｂでは、同じ参照番号によって示される。ＵＤＧＩＦ１１２は、ユーザデータフローからインサイトを生成することと、これらのインサイトを匿名化することと、それらのインサイトを、たとえばＳＣＥＦ１０４Ｃを介して、興味があるサードパーティに公開することとを担当する。ＵＤＩＧＦ１１２は、ＰＧＷ（ＰＣＥＦ）１０４ＥとＳＣＥＦ１０４Ｃとの間に配置され、たとえば、ＰＦＤＦ１０４Ｄとコロケートされ得る。

【００８８】

ＵＤＩＧＦ１１２は、図８に示されているように、５つのエレメント、またはサブ機能、１１２Ａ～１１２Ｅを備える。

【００８９】
解析サブ機能１１２Ｂが、ＰＧＷ１０４Ｅ上のＰＣＥＦからポリシルール施行アクションを取り出す。モバイルデバイス１０８またはインターネット１０２Ａからの（すなわち、モバイルデバイス１０８のほうへの）ＰＤＵ（たとえば、ＩＰパケット）が到着したときはいつでも、ＰＣＥＦはポリシアクションをトリガする。これは、たとえば、図７の表に示されているように、ＳＤＦからトリガされるポリシであり得、ここで、ＩＰパケットヘッダが走査され、または、これは、トリガされるＰＦＤであり得、ここで、アプリケーションヘッダが走査される。いずれの場合も、パケットヘッダと、アプリケーションの場合、パケットがどのアプリケーションに属するかに関する情報とに加えて、発信元（ｏｒｉｇｉｎａｔｉｎｇ）が送られる。

【００９０】
（たとえば、図１に示されているデータベース１１２Ａの形態で実現される）記憶サブ機能１１２Ａが、前に説明されたポリシルール施行要求を記憶するが、（以下で、図９Ａおよび図９Ｂを参照しながら説明されるように）生成されたインサイトに関する情報をも記憶する。

【００９１】
分析サブ機能１１２Ｃが、記憶サブ機能１１２Ａによって記憶された、生成されたポリシルールを分析し、インサイトを作り出す。作り出されたインサイトは、次いで、ＳＣＥＦ１０４Ｃへの、およびその後、ＡＳ１１４Ａへのディスパッチ（ｄｉｓｐａｔｃｈｍｅｎｔ）のために、公開サブ機能１１２Ｄに提供される。公開サブ機能１１２Ｄは、（たとえば、３ＧＰＰ　ＴＳ２３．６８２において説明されているＴ６ａにおける機能と同様の）監視要求／監視報告インターフェースを実装する。特に、公開サブ機能１１２Ｄは、分析インサイトを取り出し、それらの分析インサイトを要求元ＡＳ１１４Ａに報告する。

【００９２】
地理的データベースサブ機能１１２Ｅが、セル識別子と（たとえば、郵便番号、地名などによって規定される）地理的ロケーションとの間のマッピングを提供する。

【００９３】
図８のシグナリング図に示されているように、ＰＧＷ１０４Ｅ上のＰＣＥＦは、ＰＤＵ（たとえば、ＩＰデータパケット）が受信されるたびに、解析サブ機能１１２Ｂにポリシルール施行メッセージを送ることになる。このメッセージは、（１つまたは複数の）ＰＤＵヘッダと（１つまたは複数の）アプリケーション識別子の一方または両方、ならびに、ＰＤＵがそれに宛てられる、またはＰＤＵがそれによって送られた、モバイルデバイス１０８の識別子（たとえば、ＩＭＳＩ）を含むことになる。（１つまたは複数の）トラフィックタイプを指示する、（１つまたは複数の）ＰＤＵヘッダおよび（１つまたは複数の）アプリケーション識別子が、（たとえば、上記で説明されたディープパケット検査を使用して）測定される。したがって、ポリシルール施行メッセージはまた、測定報告をなすと見なされ得る。

【００９４】
その後、解析サブ機能１１２Ｂは、ポリシルール施行メッセージ中で指示されたモバイルデバイス１０８の識別子に関連付けられたセル識別子（セルＩＤ）に関してＭＭＥ１０４Ａ（５ＧにおけるＡＭＦ）に尋ねる。この情報は、モバイルデバイス１０８が、ＲＡＮドメイン１０６にアタッチし、および／または別のセルからハンドオーバするときはいつでも、この情報が、認証プロセス（ＬＴＥアタッチ）の一部であり、ＭＭＥ１０４Ａによって記憶されることになるので、ＭＭＥ１０４Ａに知られている。セル識別子のオープンソースデータベースについては、ｈｔｔｐｓ：／ｏｐｅｎｃｅｌｌｉｄ．ｏｒｇを参照されたい、そのアイデアは、セル識別子がまた、（ある粒度をもつ）モバイルデバイス１０８の地理的ロケーションの指示子であることである。セル識別子が取り出されると、次いで、ＰＣＥＦによって提供された情報と、セル識別子とは、現在の日付および時間でタイムスタンプを付けられ、記憶サブ機能１１２Ａにデータレコードとして記憶される。モバイルデバイス１０８の地理的ロケーションが重要でない使用事例では、ポリシルール施行

メッセージ（または、その中に含まれる情報）は、タイムスタンプに直接関連付けられ、記憶サブ機能１１２Ａにデータレコードとして記憶され得る。

【００９５】

図８に示されているデータ収集プロセスと並行して、ＵＤＩＧＦ１１２は、（たとえば、サードパーティ、またはＵＤＩＧＦ１１２を負うネットワークオペレータから）監視要求を受け付け、記憶サブ機能１１２Ａにデータレコードとして記憶された情報に関する匿名のインサイトを生成する。そのプロセスは、図９Ａおよび図９Ｂのシグナリング図に示されている。

【００９６】

ＵＤＩＧＦ１１２の公開サブ機能１１２Ｄは、３ＧＰＰ　ＴＳ２３．６８２において規定されている、監視要求／監視応答および監視報告発行／サブスクライブインターフェースを完全に実装する。ＭＭＥ１０４Ａも、同じタイプのインターフェースを実装する。

【００９７】

図９Ａに示されているように、プロセスは、ＡＳ１１４Ａが監視要求をＳＣＥＦ１０４Ｃに送ることから開始し、ＳＣＥＦ１０４Ｃはその監視要求を公開サブ機能１１２Ｄにフォワーディングする（図３中の受信ステップ３０２参照）。監視要求は、少なくとも、監視タイプを指定し、望まれる報告の最大数、（たとえば、１週間でなど、監視プロセスの終了を規定する）監視持続時間、地理的エリア（たとえば、ベルリンまたはある郵便番号）、および（監視粒度、たとえば、１分、２時間または３日など、単一の監視報告によってカバーされるべき監視時間の期間を規定し得る）監視期間など、さらなるパラメータを規定し得る。望まれる報告の最大数、および監視持続時間は、以下で、これ以上考察されない。

【００９８】

公開サブ機能１１２Ｄは、インサイト生成（Ｇｅｎｅｒａｔｅ　Ｉｎｓｉｇｈｔ）メッセージにより（随意のパラメータ、監視期間および地理的エリアとともに）監視タイプを分析サブ機能１１２Ｃにフォワーディングする。分析サブ機能１１２Ｃは、そのメッセージをＳＣＥＦ１０４Ｃに確認応答し、ＳＣＥＦ１０４Ｃは、要求元ＡＳ１１４Ａに確認応答をフォワーディングする。

【００９９】

上記で説明されたように、監視要求中でコードとして指示された監視タイプは、生成されたインサイトに対応する。この実施形態においてサポートされる例示的なインサイトは、（説明－引用符中の監視タイプコード）

－　人気がある要求宛先：「ｎｒ－ｒｅｑｕｅｓｔｓ」

－　人気があるアプリケーションカテゴリー：「ｕｅ－ｃｏｎｔｅｘｔｐｏｐｕｌａｒｉｔｙ」

－　短期グループ性向：「ｕｅ－ｓｈｏｒｔｔｅｒｍｐｒｏｐｅｎｓｉｔｙ」

－　関与アウェアグループプロファイル：「ｕｅ－ｇｒｏｕｐｐｒｏｆｉｌｅ」

である。

【０１００】

このポイント以降、分析サブ機能１１２Ｃは、インサイトを生成するために、着信（現在の）データと履歴データの一方または両方に対して分析を実施する。このプロセスは監視要求に対して非同期であり得、これは、新しいデータレコードが記憶サブ機能１１２Ａにとって利用可能であるときはいつでも、または周期的に（たとえば、監視要求などにおいて指定された監視期間に応じて、２分ごとに）分析が行われ得ることを意味する。上記のように、監視要求はまた、（たとえば、時間または日で）監視の持続時間を指定し得る。

【０１０１】

分析の一部として、分析サブ機能１１２Ｃは、記憶サブ機能１１２Ａから、分析されるべきデータレコードを取り出す。取り出されるべきデータレコードは、とりわけ、監視期間によって規定され得る。図９Ａの最後のシグナリングステップにおいて指示されているように、データレコードは、リストの形態で取り出され、各リストエントリが、特定のト

ラフィックアクティビティの（１つまたは複数の）ＰＤＵヘッダおよび／または（１つまたは複数の）アプリケーション識別子（すなわち、（１つまたは複数の）トラフィックタイプ）、モバイルデバイス識別子（「ＵＥ　ＩＤ」）、およびそのトラフィックアクティビティ中のモバイルデバイス１０８の地理的ロケーション（「セルＩＤ」）を関連付ける、データレコードを規定し得る。

【０１０２】

次に、図９Ｂのシグナリング図への参照が行われる。このシグナリング図は、本質的に、図３のステップ３０４および３０６のＬＴＥ／４Ｇ実装形態について説明する。

【０１０３】

地理的エリアが監視要求中で指定された場合、分析サブ機能１１２Ｃは、各データレコード（リストエントリ）について、地理的データベースサブ機能１１２Ｅを調べて、データレコード中のセル識別子について、関連付けられた地理的ロケーションを決定する。分析サブ機能１１２Ｃは、次いで、このようにして決定された地理的ロケーションを、監視要求中で指定された地理的エリアと比較し、データレコードが、地理的エリア中に含まれる地理的ロケーション上にマッピングするセル識別子を有することのみに基づいて、（上記で説明された）インサイトを生成する。インサイト生成は、上記で説明されたように、指定された監視タイプに従って実施されることになる（図３中のステップ３０４も参照）。次いで、１つまたは複数のインサイトの得られたリストが公開サブ機能１１２Ｄに中継されることになり、公開サブ機能１１２Ｄは、監視報告中でそのリストをＳＣＥＦ１０４Ｃに中継する。ＳＣＥＦ１０４Ｃは、要求元ＡＳ１１４Ａにその監視報告をフォワーディングすることになる（図３中のステップ３０６も参照）。明白に、インサイト生成は、データレコードが、監視要求中で指示された地理的エリアに一致しない場合、実施され得ない。その上、地理的エリアが監視要求中で指定されない場合、インサイト生成は、（たとえば、特定のネットワークオペレータの完全なネットワークを介して）すべての利用可能なデータレコードについて実施される。

【０１０４】

上記のアイデアは、ＵＤＩＧＦ１１２を導入することと、ＰＣＥＦによってフィルタ処理されたあらゆるＰＤＵに関する情報を報告するためのＰＧＷ報告能力を拡張することとについて説明した。明白に、この種類のフィルタ処理および報告は、ＰＧＷ１０４Ｅに計算オーバーヘッドを課し、ＰＧＷ１０４Ｅの性能に影響を及ぼし、したがって、潜在的に、データプレーン上のネットワークトラフィックフローに影響を及ぼすことがある。この問題に対処するため１つのアイデアは、２つのＰＧＷ１０４Ｅ、すなわち、「通常の」ネットワークデータトラフィックのための１つと、本明細書で説明されるトラフィック分析およびインサイト生成（図８参照）のための別の１つとを使用することである。たとえば、いくつかのモバイルデバイス１０８（たとえば、いくつかのカテゴリーのＩＭＳＩ）についてのネットワークデータトラフィックが、後者のゲートウェイを通してルーティングされることになり、残りのモバイルデバイス１０８（残りのＩＭＳＩ）が、それが今日標準的な実践であるので、前者のゲートウェイによってサーブされ得る。上述のカテゴリーのＩＭＳＩは、たとえば、何らかの報酬（たとえば、特定のモバイルオペレータネットワーク１００からの無料データ、ＳＭＳおよび／または通話）と引き換えに、自分のネットワークデータトラフィックを分析させるための自分の承諾を与えた私人を含むことができる。

【０１０５】

別のアイデアは、特定のモバイルオペレータネットワーク１００へのモバイルデバイス１０８の初期アタッチ中に猶予期間（ｇｒａｃｅ　ｐｅｒｉｏｄ）を追加することであろう。この猶予期間は、すべてのモバイルデバイス１０８に適用され得、たとえば、数分から数時間の間の任意のあらかじめ規定された時間期間であり得る。この猶予期間中に、特定のモバイルデバイス１０８のトラフィックが、図８に示されているように、フィルタ処理されたネットワークデータトラフィックを報告するＰＧＷ１０４Ｅを通してルーティングされ、猶予期間が終了するとすぐに、ネットワークデータトラフィックは「通常」ＰＧ

Ｗを通して再ルーティングされる。このようにして、あらゆるモバイルデバイス１０８が、そのモバイルデバイス１０８のトラフィックアクティビティを供給することによってデータ分析に参加するための変更を与えられる。猶予期間は、周期的に、または別のセルへのハンドオーバの後に（たとえば、２回目のハンドオーバまたは３回目のハンドオーバごとに）繰り返され得る。猶予期間の代わりに、再ルーティングはまた、ネットワークトラフィック負荷など、別の条件に応じて実施され得る（再ルーティングは、あらかじめ規定された負荷しきい値が超えられたとき、行われる）。

【０１０６】

図１０は、上記で説明されたＬＴＥ／４Ｇ通信ネットワークのための実装形態と同様の５Ｇ通信ネットワーク１００のための一実装形態を示す。アイデアは、（ユーザ１１４Ａとして示されている）サードパーティが、ＮＥＦ１２０への、関連するイベントの更新にサブスクライブし、ＮＥＦ１２０はＮＷＤＡＦ１２４にサブスクライブし、ＮＷＤＡＦ１２４は、関連のあるネットワーク機能（ＮＦ）１２４にデータレコードを要求する（図５の表５００参照）。

【０１０７】

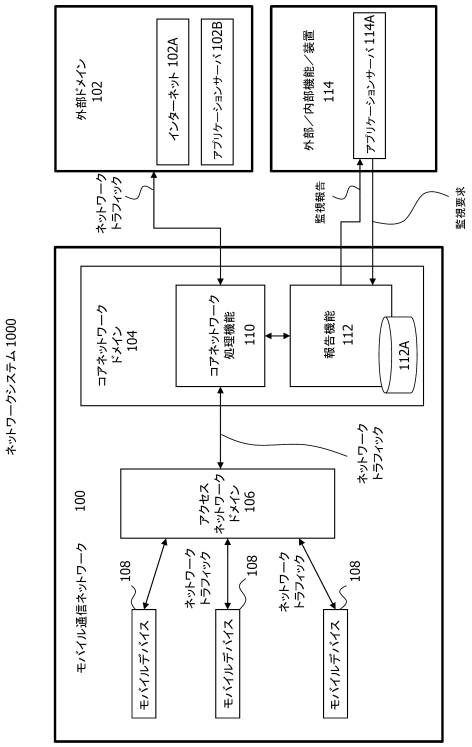
データレコードは、利用可能なとき、非同期的に提供される。ＮＷＤＡＦ１２４が、（上記で略述したような）t_dに等しい時間期間の間すべてのデータレコードを受信したとき、ＮＷＤＡＦ１２４は、上記で説明された使用事例（インサイト／監視タイプ）に従ってそれらのデータレコードを処理し、ＳＣＥＦ（図示せず）に報告し、ＳＣＥＦは、次いで、ユーザ１１４Ａに通知する。通知ペイロードが、インサイトに関する情報と、関連付けられた値とを含む。２つ以上のインサイトにサブスクライブすることが可能であることに留意されたい。

【０１０８】

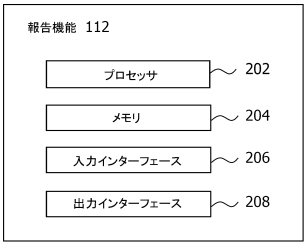
本開示が、多くの側面において変更され得る例示的な実施形態を参照しながら説明されたことが諒解されよう。したがって、本発明は、以下の特許請求の範囲によってのみ限定される。

【図面】

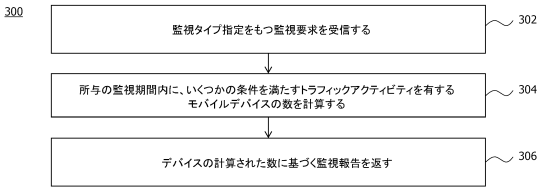
【図１】


外部ドメイン
102
インターネット 102A
アプリケーションサーバ 102B
外部／内部機能／装置
114
アプリケーションサーバ 114A
ネットワーク
トラフィック
監視報告
監視要求
ネットワークシステム 1000
コアネットワーク
ドメイン
104
コアネットワーク
処理機能
110
報告機能
112
112A
ネットワーク
トラフィック
100
アクセス
ネットワーク
ドメイン
106
モバイル通信ネットワーク
108
ネットワーク
トラフィック
108
ネットワーク
トラフィック
108
モバイルデバイス
モバイルデバイス
モバイルデバイス

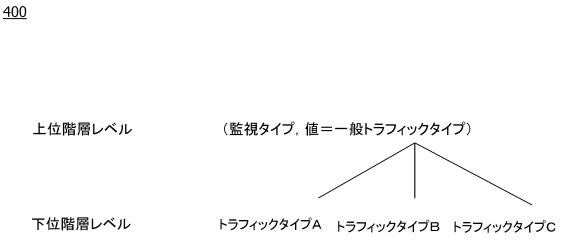
【図２】


報告機能 112
プロセッサ
202
メモリ
204
入力インターフェース
206
出力インターフェース
208

【図３】


300
監視タイプ指定をもつ監視要求を受信する
302
所与の監視期間内に、いくつかの条件を満たすトラフィックアクティビティを有する
モバイルデバイスの数を計算する
304
デバイスの計算された数に基づく監視報告を返す
306

【図４】

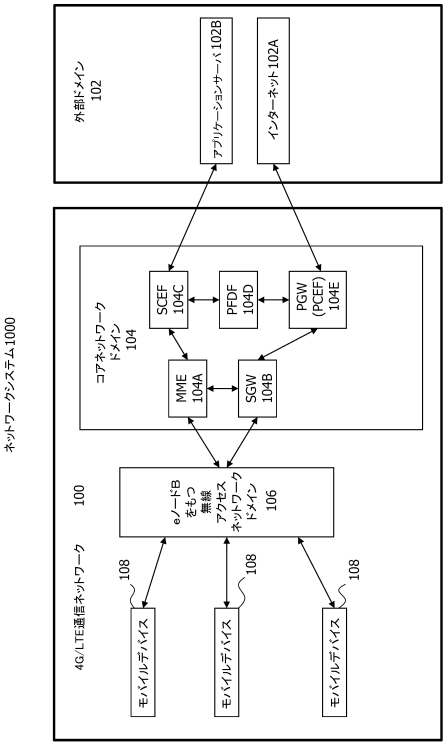

400
上位階層レベル
（監視タイプ，値＝一般トラフィックタイプ）
下位階層レベル
トラフィックタイプA
トラフィックタイプB
トラフィックタイプC

【図５】

入力データ	入力ノードLTE	入力ノード5G
アクティブモバイルデバイス(のデバイス識別子)	eNB	gNB
地理的ロケーション	MME(cellID-IMSI結合)、HSS(IMSIについてのジオロケーション)	AMF(cellID-IMSI結合)、UDM(IMSIについてのジオロケーション)
使用事例、人気がある宛先についてのデータ		
使用事例、人気があるアプリケーションカテゴリーについてのデータ	ディープパケット/PDU検査のためのPGW(PCEF)	ディープパケット/PDU検査のためのUPF(ユーザプレーン機能)
使用事例、短期グループ性向についてのデータ		
使用事例、関与アウェアグループプロファイルについてのデータ	キーワードーカテゴリー分類のための外部主題データベース(たとえば、https://tools.zvelo.com)	キーワードーカテゴリー分類のための外部主題データベース(たとえば、https://tools.zvelo.com)

500

【図６】

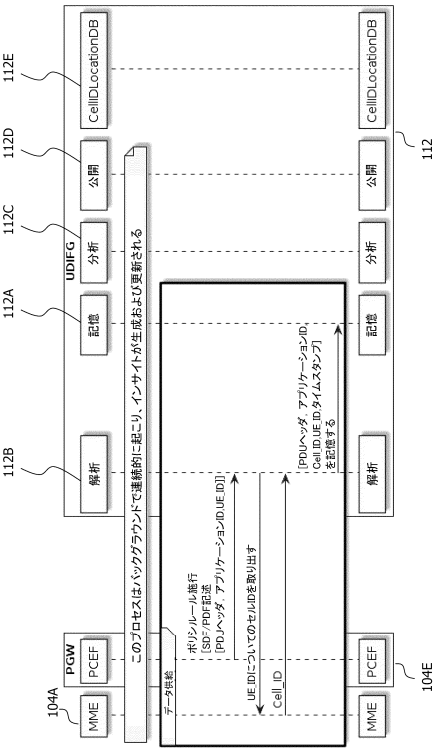


【図７】

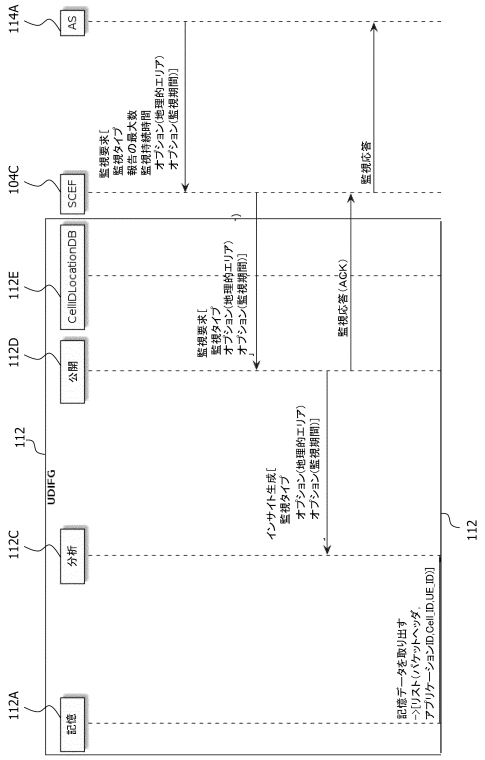
EPSベアラQoS	ポリシールール名	SDFテンプレート	SDF GBR	SDF MBR	SDF QCI/ARP	SDF ゲーティングステータス	SDF 課金
デディケーテッドベアラ(APN:IMS) QCI=1, ARP=7, GBR/MBR(UL)=100Kbps, GBR/MBR(DL)=100Kbps	ボイスU	UL:{UE IP, *, RTP, *, UDP} DL:{*, UE IP, RTP, *, UDP}	UL: 100Kbps DL: 100Kbps	UL: 100Kbps DL: 100Kbps	QCI=1, ARO=7	開(許可する)	オフライン

700

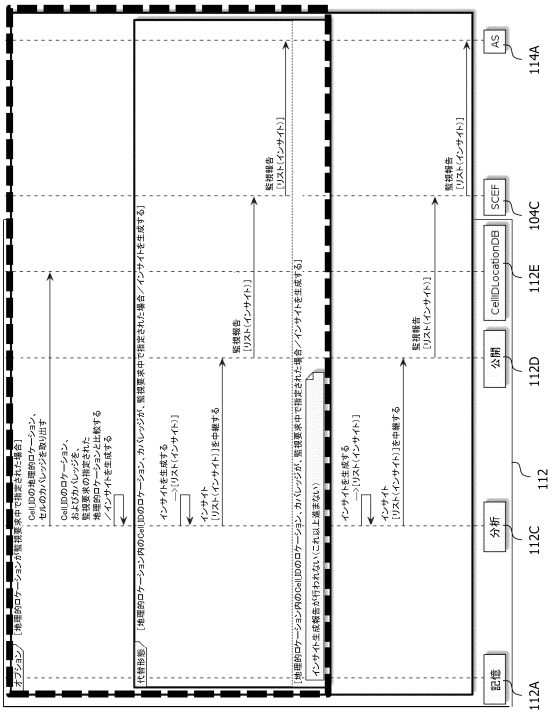
【図８】



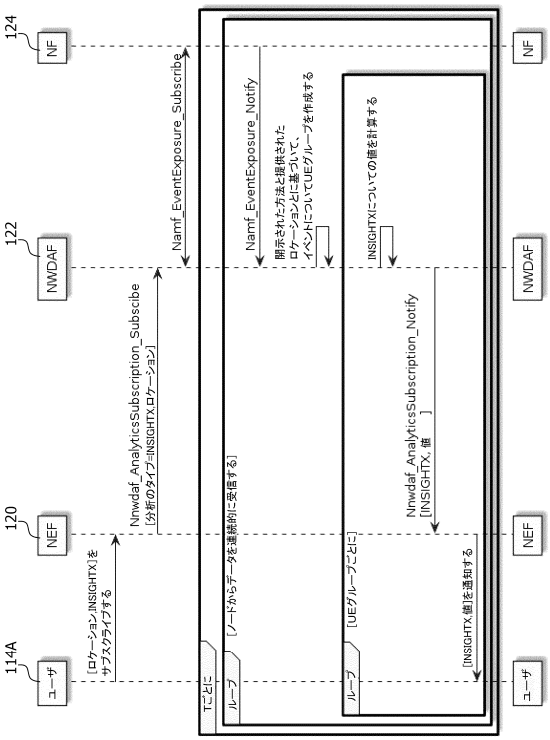
【図９Ａ】


114A
AS
104C
SCEF
112E
CellIDLocationDB
112D
公開
112
UDIFG
112C
分析
112A
記憶
監視要求[
監視タイプ
報告の最大数
監視持続時間
オプション(地理的エリア)
オプション(監視期間)]
監視応答
監視応答(ACK)
インサイト生成[
監視タイプ
オプション(地理的エリア)
オプション(監視期間)]
記憶データを取り出す
->リスト(パケットヘッダ,
アプリケーションID,Cell_ID,UE_ID)]
112

【図９Ｂ】


オプション
[地理的ロケーションが監視要求中で指定された場合]
CellIDの地理的ロケーション、
セルのカバレッジを取り出す
CellIDのロケーション、
およびカバレッジを、
監視要求の指定された
地理的ロケーションと比較する
/インサイトを生成する
代替形態
[地理的ロケーション内のCellIDのロケーション、カバレッジが、監視要求中で指定された場合/インサイトを生成する]
インサイトを生成する
->[リスト(インサイト)]
インサイト
[リスト(インサイト)]を中継する
監視報告
[リスト(インサイト)]
[地理的ロケーション内のCellIDのロケーション、カバレッジが、監視要求中で指定された場合/インサイトを生成する]
インサイトが生成要件が行われないこれ以上基づかない
インサイトを生成する
->[リスト(インサイト)]
インサイト
[リスト(インサイト)]を中継する
監視報告
[リスト(インサイト)]
AS
114A
SCEF
104C
CellIDLocationDB
112E
公開
112D
112
分析
112C
記憶
112A

【図１０】


124
NF
122
NWDAF
120
NEF
114A
ユーザ
[ロケーション/INSIGHTX]を
サブスクライブする
Nnwdaf_AnalyticsSubscription_Subscribe
[分析のタイプ=INSIGHTX,ロケーション]
Namf_EventExposure_Subscribe
Namf_EventExposure_Notify
開示された方法と提供された
ロケーションとに基づいて、
イベントについてUEグループを作成する
INSIGHTXについての値を計算する
Nnwdaf_AnalyticsSubscription_Notify
[INSIGHTX, 値]
[INSIGHTX,値]を通知する
Tごとに
ループ
[ノードからデータを連続的に受信する]
ループ
[UEグループごとに]

フロントページの続き

(72)発明者　フェルスマン， エレーナ
スウェーデン国 エスエー－１１１２３ ストックホルム， ダラガータン ６ベー
(72)発明者　カラパンテラキス， アタナシオス
スウェーデン国 エスエー－１６９ ７９ ソルナ， エヴェネマングスガータン １２
(72)発明者　ヴァルガラキス フェルヤン， アネタ
スウェーデン国 エスエー－１１２ １６ ストックホルム， フランゼンガータン ３４

審査官　和平 悠希

(56)参考文献　国際公開第２０１２／０１６３２７（WO，Ａ１）
特開２０１６－０９６５１４（ＪＰ，Ａ）
特開２０１５－１０３９７９（ＪＰ，Ａ）
米国特許第１０４１１９７８（ＵＳ，Ｂ１）
米国特許出願公開第２０１４／０３７０８４３（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／００－１２／６６
Ｈ０４Ｌ　４１／００－１０１／６９５
Ｈ０４Ｗ　８８／１８
Ｈ０４Ｗ　９２／２４