

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2009-530921
(P2009-530921A)

(43) 公表日 平成21年8月27日(2009.8.27)

(51) Int.Cl. HO4M 11/00 HO4W 8/08	F 1 (2006.01) (2009.01)	HO4M 11/00 HO4Q 7/00	302 144	テーマコード (参考) 5K067 5K201
---	---	-------------------------	------------	-------------------------------

審査請求 未請求 予備審査請求 未請求 (全 19 頁)

(21) 出願番号 (86) (22) 出願日 (85) 翻訳文提出日 (86) 國際出願番号 (87) 國際公開番号 (87) 國際公開日 (31) 優先権主張番号 (32) 優先日 (33) 優先権主張国 (31) 優先権主張番号 (32) 優先日 (33) 優先権主張国	特願2009-500626 (P2009-500626) 平成19年3月16日 (2007.3.16) 平成20年11月10日 (2008.11.10) PCT/US2007/064164 W02007/133844 平成19年11月22日 (2007.11.22) 60/783,230 平成18年3月17日 (2006.3.17) 米国(US) 60/783,232 平成18年3月17日 (2006.3.17) 米国(US)	(71) 出願人 キャミアント、インク。 アメリカ合衆国 マサチューセッツ州 O 1752, マールボロ, セカンド フロア -, ニッカーソン ロード 200
		(74) 代理人 110000659
		(72) 発明者 リレイ, ユスン, キム。 アメリカ合衆国 マサチューセッツ州 O 1762, マールボロ, ヘミンウェイ ス トリート 630
		F ターム (参考) 5K067 AA22 EE02 EE10 EE16 FF02 FF03 JJ51 5K201 BA05 CA02 CB11 CB12 CC04 DA01 EA07 EC08
		最終頁に続く

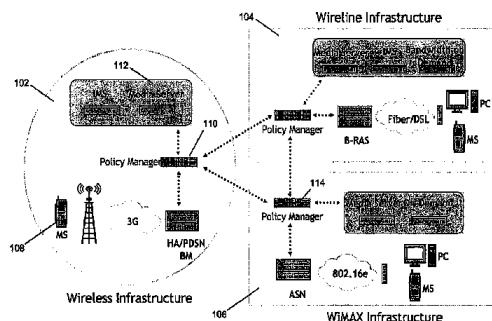
(54) 【発明の名称】移動及び遊動ネットワークで利用する配信ポリシーサービス

(57) 【要約】

【課題】 それぞれがアクセデバイスとポリシーファンクションを有している1以上のネットワークを有したシステム内でサブスクライバに関するトポロジー情報を配信する方法を提供する。

【解決手段】 1以上のネットワーク102を有したシステム内でサブスクライバ108に関するトポロジー情報を配信する方法であって、それぞれのネットワーク102はアクセデバイスとポリシーファンクション110とを有しており、利用ポリシーファンクションによってサブスクライバの現行位置を特定するステップを含んでいる。方法は、利用ポリシーファンクション110からサブスクライバ108に関係するアンカーポリシーファンクションにその現行位置に関する情報を転送するステップをさらに含んでいる。

【選択図】図2



【特許請求の範囲】**【請求項 1】**

1以上のネットワークを有したシステム内でサブスクライバに関するトポロジー情報を配信する方法であって、

利用ポリシーファンクションによってサブスクライバの現行位置を特定するステップと

、
前記利用ポリシーファンクションからサブスクライバに関するアンカーポリシーファンクションに前記現行位置に関する情報を転送するステップと、
を含んでいることを特徴とする方法。

【請求項 2】

サブスクライバが異なる利用ポリシーファンクションに移動するたびに特定ステップと転送ステップとを実行するステップをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 3】

サブスクライバに関するポリシー情報をアンカーポリシーファンクションから利用ポリシーファンクションにルート付けするためにサブスクライバの現行位置に関する情報を利用するステップをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 4】

サブスクライバに関するポリシー情報と、該ポリシー情報のリクエストとをプッシュモデルを実行することでルート付けするステップをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 5】

サブスクライバに関するポリシー情報と、該ポリシー情報のリクエストとをプルモデルを実行することでルート付けするステップをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 6】

サブスクライバと関する状況情報をアンカーポリシーファンクションによって維持するステップと、該状況情報に従ってポリシールールを実行するステップとをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 7】

利用ポリシーファンクションとアンカーポリシーファンクションとは異なるサービスプロバイダのネットワーク内に存在しており、現行位置に関する情報を転送するステップは該現行位置に関する情報を少なくとも1つのサービスプロバイダのネットワークバウンドリを越えて伝達するステップをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 8】

利用ポリシーサーバがリソースコントロールを監視するネットワーク内のリソース消費に基づいてサブスクライバに関するポリシーディジョンを制限またはコントロールするために1以上のリソースレベルポリシールールを実行する利用ポリシーファンクションをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 9】

利用ポリシーファンクションをアンカーポリシーファンクションから脱カップリングするステップをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 10】

サブスクライバの現行位置に関する情報をシステム内の1以上の他のポリシーファンクションに配信するステップをさらに含んでいることを特徴とする請求項1記載の方法。

【請求項 11】

1以上のサブネットワークを有したネットワーク内でサブスクライバに関するトポロジー情報を配信するシステムであって、それぞれのサブネットワークはアクセスデバイスとポリシーファンクションとを有しており、本システムは、サブスクライバの現行位置を特定するための利用ポリシーファンクションと、

10

20

30

40

50

前記利用ポリシーファンクションから前記現行位置に関する情報を受領するためのサブスクライバに関するアンカーポリシーファンクションと、
を含んでいることを特徴とするシステム。

【請求項 1 2】

サブスクライバが異なる利用ポリシーファンクションに移動するたびに該異なる利用ポリシーファンクションはサブスクライバの現行位置を特定し、該現行位置をアンカーポリシーファンクションに転送することを特徴とする請求項 1 1 記載のシステム。

【請求項 1 3】

サブスクライバに関するポリシー情報をサブスクライバの現行位置に関する情報を利用してアンカーポリシーファンクションから利用ポリシーファンクションにルート付けすることを特徴とする請求項 1 1 記載のシステム。 10

【請求項 1 4】

ネットワークはサブスクライバに関するポリシー情報と、該ポリシー情報のリクエストとをプッシュモデルを実行することでルート付けすることを特徴とする請求項 1 1 記載のシステム。

【請求項 1 5】

ネットワークはサブスクライバに関するポリシー情報と、該ポリシー情報のリクエストとをプルモデルを実行することでルート付けすることを特徴とする請求項 1 1 記載のシステム。

【請求項 1 6】

アンカーポリシーファンクションはサブスクライバと関する状況情報を維持し、該状況情報に従ってポリシールールを実行することを特徴とする請求項 1 1 記載のシステム。 20

【請求項 1 7】

利用ポリシーファンクションとアンカーポリシーファンクションとは異なるサービスプロバイダのネットワーク内に存在しており、現行位置に関する情報を少なくとも 1 つのサービスプロバイダのネットワークバウンダリを越えて伝達することを特徴とする請求項 1 1 記載のシステム。

【請求項 1 8】

利用ポリシーファンクションは、利用ポリシーサーバがリソースコントロールを監視するサブネットワーク内でのリソース消費に基づいてサブスクライバに関するポリシーディジョンを制限またはコントロールするために 1 以上のリソースレベルポリシールールを実行することを特徴とする請求項 1 1 記載のシステム。 30

【請求項 1 9】

利用ポリシーファンクションはアンカーポリシーファンクションから脱カップリングされることを特徴とする請求項 1 1 記載のシステム。

【請求項 2 0】

ネットワーク内に 1 以上の他のポリシーファンクションをさらに含んでおり、サブスクライバの現行位置に関する情報は該 1 以上の他のポリシーファンクションに配信されることを特徴とする請求項 1 1 記載のシステム。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

本発明はデジタルコンテンツを配信するための通信システムおよび通信サービスに関する。特にサブスクライバの物理的所在地とは無関係にサブスクライバを該当ポリシーサービスと適切に関連させる技術に関する。

【背景技術】

【0 0 0 2】

図 1 は複数のサブスクライバに対してデジタルコンテンツを送る従来技術によるシステム 10 を図示する。アプリケーションファンクション 1 2 (本例では P - C S C F (プロキシコールセッションコントロールファンクション)) はサブスクライバに V o I P コー

ルを実行させるようにセッションセットアップファンクションを提供する。あるいはアプリケーションファンクションはサーバとして作用することもできる。このサーバは複数のサブスクリーバ14のうちの1サブスクリーバにビデオストリームのごときデジタルコンテンツを提供する。サブスクリーバには電話またはパソコン等の電子装置が含まれる。これら電子装置は無線装置であっても、ローカルな有線ネットワークに接続することもできる。

【0003】

セッション時にアプリケーションサーバ12がサブスクリーバ14に提供するデジタルコンテンツはいくつかのネットワークコンポーネントを通過する。このデジタルコンテンツは実施ポイントを通過するが、ポリシーをリクエストするシグナルは図のポリシー要素(ポリシールータ16とポリシーサーバ18並びに実施ポイント)間で伝達される。10

【0004】

実施ポイント20はケーブルモデムターミネーションシステム(CMTS)、GPRSゲートウェイサポートノード(GGSN)、パケットデータサービスノード(PDSN)等であるエッジデバイスである。一般的に実施ポイントはサブスクリーバのセッション中にパケットがトラバースするネットワーク内のどのようなエンティティであってもよい。実施ポイント20はどの特定アプリケーションサーバ12の専用ではないが、その代わりに実施ポイントのリソースはネットワーク内のポリシーファンクション(例えば本例ではポリシーサーバ18)によってサブスクリーバのアプリケーションセッションに割り当てられる。20

【0005】

“ポリシーファンクション”とはポリシーを実施しているネットワーク内のエンティティを表す一般用語である。ポリシーファンクションの主要目的はセッションのために適したサービスクオリティを提供し、加えてセッションと関連する情報の料金請求および決算を管理することである。ポリシーファンクションは実施ポイント20に対してポリシーディジョンを伝達すなわち“ブッシュ”し、サブスクリーバのために正確なポリシーセットが設定されていることを確認する役目を担っている。よってポリシーファンクションはアプリケーションサーバ12に成り代わって実施ポイント20を制御する。

【0006】

図示のポリシールータ16はポリシーファンクションであり、ポリシーリクエストを下流のポリシーファンクションに発送あるいは転送する。図1の例ではアプリケーションサーバ12はポリシールータ16を介してポリシーリクエストをポリシーサーバ20に送る。30

【0007】

一般的に図1は複数のアプリケーション、複数のサブスクリーバおよび複数のサブスクリーバエッジデバイスをサポートするサービスプロバイダのポリシー環境を示す。サブスクリーバエッジデバイス20はサービスクオリティ、バンド幅マネージメントおよびアドミッションコントロールに関連するオペレータポリシーのためのポリシー実施ポイントとして機能する。

【発明の開示】

【発明が解決しようとする課題】

【0008】

以下は解説されている実施例によって提供されるポリシー環境の重要な目的の一部である。

【0009】

アプリケーションはネットワーキングあるいはネットワーケンジニアリングの知識を必要とすべきではない。アプリケーションがトポロジーの知識を必要とせずにいられるようにネットワーク内のポリシーサーバがトポロジーアブストラクションの面倒を見るべきである。

【0010】

10

20

30

40

50

ポリシー環境は全国規模での利用スケールに合わせるべきである。

【0011】

実際のネットワークトポロジーは動的であるべきである。ネットワークサブスクライバ、ポリシーサーバ、実施ポイントおよびそれらの相互接続は追加、変更または削除が可能であるべきである。管理規定は最少限度に留めるべきである。

【0012】

サブスクライバは異なるネットワークと異なるサービスプロバイダからアプリケーションにアクセスできるべきである。このタイプのローミングの振る舞いはサブスクライバと関連する実施ポイントが時間と共に変化することを意味する。またサブスクライバは潜在的には同時的に異なるネットワークおよび異なるサービスプロバイダからサービスとアプリケーションとに潜在的にアクセスできるべきである。

10

【0013】

ネットワークサブスクライバは異なる時間に異なるサブスクライバエッジデバイスからネットワークにアクセス可能（すなわちサブスクライバは遊動性）であるか、同一セッション中に1つのサブスクライバエッジデバイスおよび別エッジデバイスとの間で移動可能（すなわちサブスクライバは移動性）であるべきである。

【0014】

サブスクライバがどこからアタッチしているかには無関係にサブスクライバには一貫したセットのポリシーが提供されるべきである。ポリシーは以下タイプのサブスクライバサービスの属性を管理する。

20

【0015】

サブスクライバの受益資格（どのようなサービスおよびコンテンツにアクセス可能およびアクセス不能か）。

【0016】

サブスクライバのためのサービスクオリティ（サービスのユーザー体験の品質またはサービスを得るためにサブスクライバが認可されているバンド幅）。

【0017】

特定サービスまたは特定アプリケーションでサブスクライバが幾ら請求されるべきか。

【0018】

カスタマーに一貫したセットのポリシーを提供するため、実施ポイントをコントロールする役割を負うネットワーク（典型的には“来訪”ネットワーク）と呼称）内のポリシーファンクションが、サブスクライバポリシーに関する全情報を含む“ホーム”ポリシーファンクションと交信できるようにするメカニズムが存在すべきである。

30

【0019】

[関連出願]

本願は2006年3月17日出願の米国仮特許願60/783232および2006年3月17日出願の米国仮特許願60/783230の優先権を主張する。

【0020】

1特徴によれば本発明は、それぞれがアクセスデバイスとポリシーファンクションをしている1以上のネットワークを有したシステム内でサブスクライバに関係するテポロジー情報を配信する方法を提供する。

40

【課題を解決するための手段】

【0021】

この方法は利用ポリシーファンクションによってサブスクライバの現行位置を特定するステップを含む。この方法はさらに利用ポリシーファンクションからサブスクライバに関係するアンカーポリシーファンクションにまでその現行位置に関する情報を転送するステップをさらに含む。

【0022】

本発明の1実施例によればサブスクライバが異なる利用ポリシーファンクションに移動するごとにその特定ステップと転送ステップとを実行するステップも含まれる。別実施例

50

ではサブスクライバに関するポリシー情報をアンカーポリシーファンクションから利用ポリシーファンクションへとルート付けするためにサブスクライバの現行位置に関する情報を使用するステップがさらに含まれる。

【0023】

1実施例によればサブスクライバに関するポリシー情報をルート付けし、プッシュモデルを実行してポリシー情報をリクエストするステップがさらに含まれる。別実施例ではサブスクライバに関するポリシー情報をルート付けするステップをさらに含み、プルモデルを実行してポリシー情報をリクエストする。

【0024】

1実施例ではアンカーポリシーファンクションによってサブスクライバに関する状況情報を維持し、その状況情報に従ってポリシールールを実行するステップがさらに含まれる。

【0025】

別実施例では利用ポリシーファンクションおよびアンカーポリシーファンクションは異なるサービスプロバイダネットワーク内に存在しており、現行位置に情報を転送するステップは現行位置に関する情報を少なくとも1つのサービスプロバイダネットワークバウンダリに送るステップをさらに含む。

【0026】

1実施例では利用ポリシーサーバがリソースコントロールを監督するネットワーク内のリソース消費に基づいてサブスクライバに関するポリシーディジョンを制限または制御する1以上のリソースレベルポリシールールを実行する利用ポリシーファンクションをさらに含む。

【0027】

さらに別実施例ではアンカーポリシーファンクションから利用ポリシーファンクションを脱カップリングするステップがさらに含まれる。1実施例ではサブスクライバの現行位置に関する情報をシステム内の1以上の他のポリシーファンクションに配信するステップがさらに含まれる。

【0028】

別特徴ではそれぞれアクセスデバイスとポリシーファンクションとを有した1以上のサブネットワークを有するネットワーク内のサブスクライバに関するトポロジー情報を配信するシステムが提供される。このシステムはサブスクライバの現行位置を特定する利用ポリシーファンクションと、その利用ポリシーファンクションから現行位置に関する情報を受領するためのサブスクライバに関するアンカーポリシーファンクションとを含む。

【0029】

1実施例ではサブスクライバが異なる利用ポリシーファンクションに移動するたびに異なる利用ポリシーファンクションがサブスクライバの現行位置を特定し、アンカーポリシーファンクションにその現行位置を転送する。

【0030】

別実施例ではネットワークはサブスクライバに関するポリシー情報をサブスクライバの現行位置に関する情報をを利用してアンカーポリシーファンクションから利用ポリシーファンクションにルート付けする。

【0031】

1実施例ではネットワークはサブスクライバに関するポリシー情報をルート付けし、プッシュモデルを実行することでそのポリシー情報をリクエストする。別実施例ではネットワークはサブスクライバに関するポリシー情報をルート付けし、プルモデルを実行することでそのポリシー情報をリクエストする。

【0032】

1実施例ではアンカーポリシーファンクションはサブスクライバに関する状況情報を維持し、その状況情報に従ってポリシールールを実行する。別実施例では利用ポリシーファンクションとアンカーポリシーファンクションは異なるサービスプロバイダネットワー

10

20

30

40

50

ク内に存在し、その現行位置に関する情報は少なくとも1つのサービスプロバイダネットワークバウンダリを越えて送られる。

【0033】

別実施例では利用ポリシーファンクションは1以上のリソースレベルポリシールールを実行し、利用ポリシーサーバがリソースコントロールを監督するサブネットワーク内のリソース消費に基づいてサブスクライバに関するポリシーディジョンを制限又はコントロールする。

【0034】

1実施例では利用ポリシーファンクションはアンカーポリシーファンクションから脱カップリングされる。

【0035】

別実施例ではネットワーク内に1以上のポリシーファンクションがさらに含まれる。サブスクライバの現行位置に関する情報はその1以上の他のポリシーファンクションに配信される。

【発明を実施するための最良の形態】

【0036】

図2は本発明に従って構築された1例示的実施例によるシステム構造を図示する。図2で図示されている例示システムは無線ネットワーク102、有線ネットワーク104およびWiMAX(IEEE802.16)ネットワーク106を含む。

【0037】

無線ネットワーク102においてサブスクライバ108は無線ネットワーク102にアクセスするためにモバイル装置(MS)を使用する。サブスクライバ108は、例えばSprintである特定アクセスプロバイダと契約する。サブスクライバのポリシーファンクションはSprintの無線ネットワーク102内に位置する。

【0038】

サブスクライバ108が別アクセスプロバイダネットワークに“ローミング”すると仮定する。この例ではSprintネットワーク102はサブスクライバの“ホームネットワーク”であると考えられる。Sprintネットワーク内のポリシーファンクション110(この場合はポリシーマネージャ)はサブスクライバの“ホームポリシーファンクション”すなわち“アンカーポリシーファンクション”である。

【0039】

サブスクライバが例えばWiMAX無線ネットワーク106である異なるタイプのネットワークをサポートするアクセスプロバイダにローミングすると仮定する。サブスクライバ108がWiMAXネットワークに接続されるとサブスクライバはそのホームネットワーク(Sprintネットワーク102)内に位置するアプリケーション112にアクセスを願うかも知れない。このことを実現するためには、そのホームポリシーファンクション110内に存在するサブスクライバ108のポリシーはサブスクライバが訪問しているネットワーク(WiMAXネットワーク106)内で究極的に実行される必要がある。

【0040】

しかし、無線ネットワーク102からのホーム/アンカーポリシーファンクション110はWiMAXネットワーク106(サブスクライバがローミングした先のネットワーク)をコントロールしないし、直接的にコントロールすることはできない。いくつかの警備理由によりネットワークプロバイダは典型的にはポリシーの実施のためにそのネットワーク機器を外部エンティティに直接的にコントロールさせることはない。

【0041】

よってホーム/アンカーポリシーファンクションは、必要なネットワークアセットを配信させるために本例においてはWiMAXネットワーク106内のポリシーマネージャ114である“来訪”ポリシーファンクションと通信および協調しなければならない。この来訪ポリシーファンクションは本明細書では“利用”ポリシーファンクションとも呼称されている。なぜならそれは来訪ネットワーク内のサブスクライバに利用されるためのポリ

シーファンクションだからである。

【0042】

上記で解説された実施例は以下の目的を達成するための技術と機構を含んでいる。

【0043】

1. サブスクライバが移動形態または遊動形態でネットワークにアクセスしようと、任意サブスクライバを特定のポリシーサーバと関連させる。従ってそのサブスクライバは適した来訪ポリシーファンクションおよび適性ホーム/アンカーポリシーファンクションと関連付けが可能である。

【0044】

2. サブスクライバが移動形態または遊動形態でネットワークにアクセスしようと、どのポリシーサーバにポリシーを任意アプリケーションにアクセスさせるかを決定する任務からアプリケーションを開放する。

10

【0045】

3. ポリシーサーバにアプリケーションアドレス処理（典型的には5個組であるIPソースアドレス、IPデスティネーションアドレス、ソースポート、デスティネーションポートおよびプロトコール）およびMACアドレス並びにEメールID（インバリアントサブスクライバアイデンティファイア（ISI））のごとき他のサブスクライバアイデンティファイアを現在特定のサブスクライバをサポートしているネットワークエッジデバイスにマップ処理させる。

【0046】

アクセスネットワーク内のそれぞれのサブスクライバステーションはサブスクライバが使用する特定アクセス技術に依存するインバリアントサブスクライバアイデンティファイア（ISI）と関連している。ISIの例には電子連番、電話番号、モバイルステーションインテグレーテドサービスデジタルネットワーク番号（MS-ISDN）、インターナショナルモバイルサブスクライバアイデンティファイア、エータネットメディアアクセスコントロール（MAC）アドレス等がある。

20

【0047】

サブスクライバが異なるアクセスデバイスからネットワークにアクセスするたびに変動するIPアドレスレンジとは異なり、あるいはサブスクライバが異なるサブスクライバアクセスデバイスを介してネットワークにアクセスするとき、ISIはサブスクライバに関連しており、アクセスごとに変化することはない。(i) ISI番号が、サブスクライバがネットワークにアクセスする“典型的な”位置をコード化し、(ii)連続的アイデンティファイアが同一位置から支給されるこの技術的特徴はマッピング操作をさらに効率的にするが、ここで解説した実施例では特に必要とされない。

30

【0048】

ポリシーサーバ（以降“PS”）は“学習”するか、典型的にはどのISIにそれらがサービスを提供するかを特定する情報が支給される。このように特定PSは任意セットのサブスクライバの“アンカー”PSとなる。“アンカー”PSであるということは、どこでサブスクライバがネットワークに現在アクセスしているかには関係なくPSが常に関連サブスクライバのための最終的ポリシーディジョンメーカーであることを意味する。

40

【0049】

[状況認識]

特定のサブスクライバのアンカーPSはサブスクライバを状況認識している。この“状況認識”とはサブスクライバがネットワーク上に存在するときは常にアンカーPSはサブスクライバの状況を認識している（すなわち状況に関する情報を有している）ということであり、その意味ではアプリケーションはサブスクライバが行使したポリシーを必要とする。サブスクライバが、例えばそれ自身のポリシーサーバを有するネットワークの別領域にネットワーク内で移動するときでさえもポリシーリクエストはそのサブスクライバのために最終的にはアンカーPSとの相互作用を必要とする。アンカーPSはサブスクライバを認識しているため、サブスクライバを中心としたパラメータ（すなわちそのサブスクライバ）を状況認識する。

50

イバ特有のパラメータ)に基づいてポリシーディジョンをすることができる。

【0050】

例えば、アンカーPSは、サブスクライバは誰であるか、どのサービス段階またはパッケージをサブスクライバが購入したか、または享受できるか、並びにいくつのそのようなセッションを享受できるか等々に基づいてサブスクライバが何をすることができ、何をすることができないかを決定するポリシールールを実行することができる。

【0051】

アンカーPSはサブスクライバとそのポリシーパラメータの状況認識をするものの、そのアンカーPSはどのようなネットワークリソースをサブスクライバが利用しているかに関しては情報を持っていないかも知れない。例としてサブスクライバがローミングしていればそのアンカーPSは利用PSではないかも知れないからである。そのアンカーPSがホームネットワークであり、もしサブスクライバが別PS(サブスクライバはネットワークの別部分あるいは別プロバイダにローミングしているため、来訪PSまたは利用PS)によって利用されている位置に存在するならば、それはただサブスクライバが利用しているネットワークリソースを認識する来訪PSまたは利用PSである。その結果、利用PSまたは来訪PSはネットワークリソースを中心とするポリシー(それらネットワークリソースに特有なポリシー)を監督することができる。

10

【0052】

来訪または利用PSはリソース消費のためにセッティング閾値に焦点を合わせるポリシールールを実行することができる。利用PSは実施ポイントとインターフェースするPSであり、それがコントロールする実施ポイントで承認された全セッションを認識しているため、それは利用されているリソースを認識している。その結果、利用PSは実施ポイントで承認できるリソース量(例えばバンド幅あるいはセッション数)をコントロールするポリシールールを実施できる。

20

【0053】

よってアンカーPSはサブスクライバを中心とするポリシーを実行する役割を担い、来訪または利用PSはリソースを中心とするポリシーを実行する役割を担う。サブスクライバセッションを状況認識する別アンカーポリシーサーバはサブスクライバが何をすることができるかコントロールするためにサブスクライバが認識するポリシールールを実行できる。例えばアンカーPSは、サブスクライバが既に2つのセッションを同時的に実行状態にしているなら3番目のセッションを拒絶することができる。またはアンカーPSはサブスクライバが音声アプリケーションを実行状態にしているならビデオのリクエストを拒絶することができる。同一シナリオでも、サブスクライバがエリート(“ゴールド”)サービス階層であれば音声アプリケーションが既に実行状態であろうともアンカーPSはビデオのリクエストを認可することができる。

30

【0054】

[ネットワークを介したトポロジーのパーコレーション]

サブスクライバがネットワークに登録するときには常にサブスクライバのアタッチメントポイントに関する情報(トポロジー)はネットワークの当該ポリシーファンクションを介してパーコレーション処理する必要がある。この処理によってアプリケーションが行使されたときにはローミングしているサブスクライバのために正確なセットのポリシーファンクションがそのポリシー活動に参加するであろう。その結果、サブスクライバを中心とするポリシーおよびリソースを中心とするポリシーが適正に実行および実施される。

40

【0055】

このトポロジー情報が配信可能ないくつかの方法が存在する。図3と図4にて図示するように利用ポリシーサーバ150は登録情報152をネットワーク内の指定ポリシールータ154に転送できる(この指定情報は利用ポリシーサーバで支給できるか、利用ポリシーサーバによってアルゴリズム的に導き出せる)。

【0056】

その後、ポリシールータはサブスクライバのために指定されたアンカーPSにその登録

50

情報を転送する役割を担うことができる。ポリシールータは、例えば以下のような複数の異なる方法で特定サブスクライバのためにどのアンカー PS が指定されたかに関する情報を取得することができる。

【0057】

ポリシールータにその情報を支給することができる。

【0058】

ポリシールータは外部データベースルックアップを介してその情報をリトリーブすることができる。

【0059】

ポリシールータはアルゴリズム的にその情報を導き出すことができる（例えばサブスクライバが使用している装置の電話番号に基づき、アンカーの位置を確認させるエリアコードを使用する）。 10

【0060】

アンカー PS はポリシールータにトポロジー情報をパーコレーション処理することができる。

【0061】

ポリシールータが登録情報を指定されたアンカー PS に送ると、ポリシールータとアンカー PS の両方はどのサーバまたは来訪 PS がサブスクライバと現在関連するかを知る。もしサブスクライバが物理的に移動すれば、新サービス PS がサブスクライバと関連するであろう。そうなると登録プロセスは再現され、アンカーおよびポリシールータは上述のように新関連性を“発見”または“学習”する。 20

【0062】

あるいは利用 PS は上記と同様な機構を利用してアンカー PS にもトポロジー情報を送るであろう。例えば、サブスクライバが登録するとき利用 PS は登録のレルム情報をを利用して、どのアンカーポリシーサーバが登録/トポロジー情報を受領するか決定することができる。

【0063】

[登録およびトポロジー学習]

サブスクライバは典型的にはサブスクライバステーションに動的 IP ネットワークアドレスを割り当てるケーブルモデムターミネーションシステム (CMTS) 、パケットデータサービスノード (PDSN) 、ゲートウェイ GPRS サービスノード (GGSN) 、またはブロードバンドリモートアクセスサーバ (B-RAS) デバイス等のサブスクライバアクセス装置によってネットワークにアクセスする。PS はサブスクライバアクセス装置を介してネットワークアプリケーションからサブスクライバに流れるアプリケーションデータストリームのためのポリシーディジョンファンクション ((PDF) サービスクオリティ、アドミッションコントロールおよびパケットプロセスディシプリン並びに特定セッションをどのように請求するかを決定する) を提供する。 30

【0064】

サブスクライバがネットワークに登録すると、そのサブスクライバはアプリケーションファンクションと共に信号発信することでアプリケーションを使用できる。このアプリケーションファンクションは中心化された位置に存在できる。このアプリケーションファンクションはネットワークに関してサブスクライバの物理的位置は認識していない。 40

【0065】

サブスクライバがアプリケーションサーバからのセッションのリクエストを開始するとアプリケーションファンクション/サーバはポリシーディジョンのために PS に対してリクエストを発給する。これで最終的にポリシー (QoS 処理と特定セッション並びに潜在的には資格に関連する請求ルール) が決定される。この PS は PS に支給されているルールに照らしてリクエストを評価し (ルールはサブスクライバの階層、時間帯およびネットワーク利用のごとき情報に基づいて決定することができる) 、ポリシーディジョン (QoS ポリシーディジョンおよび請求処理) をサブスクライバアクセス装置、すなわち実施ポ 50

イントまでプッシュダウンする。

【0066】

ネットワークが大きくなると、一般的にはそれぞれサブスクライバアクセス装置のセットに信号発信する複数のPSにPDFを分配することが望ましい。ポリシールータはネットワークを通じてアプリケーションにポリシーディジョンのための1つのコンタクトポイントを持たせ、アプリケーションをネットワークトポロジーまたはサブスクライバ位置の認識負担から開放する。ポリシールータはどのサブスクライバアクセスデバイスがサブスクライバに利用されているか、およびどのPS（サービスおよびアンカー）がサブスクライバに関するポリシーディジョンを実行できるかの認識を維持する。

【0067】

モバイルネットワークにおいては、サブスクライバが最初にシステムにアクセスするときサブスクライバアクセス装置はネットワークIPアドレスとISIをその関連PSに信号発信する。非モバイルネットワークでは、SNMPのごとき他の手段または支給によってサブスクライバ関連性を学習することができる。これでポリシールータはそのポリシールート付けファンクションを実行するためにその情報を使用することができる。すなわちアプリケーションがポリシールータにリクエストを発行するとき、サブスクライバIPアドレスまたはISIのいずれかに基づいてどのPSにリクエストをルート付けさせるのかを知ることができる。

【0068】

PSは特定サブスクライバのための“アンカー”PSとしても支給することができ、サブスクライバが物理的にどこに存在しようと（サブスクライバは異なる実施ポイント間を移動できる）ポリシーリクエストは常に別PSにルート付けされる。よってサブスクライバが関連している特定実施ポイントを利用させる任務を担う利用PSにリクエストをルート付けすることはアンカーPSの任務となる。ポリシールータはリクエストをアンカーPSにルート付けするためにISIを利用することができ、アンカーPSはISIまたはサブスクライバIPアドレスを使用して利用PSへルート付けすることができる。

【0069】

このアンカー技術は、スケール変動性であることによりネットワークにポリシーファンクションの分布が存在するとき、並びにサブスクライバがネットワークとネットワークプロバイダとの間をローミングしているときには有用である。

【0070】

図5と図6はポリシールータからアンカーへ、続いて利用PSへのポリシーリクエストのルート付けを図示する。各PSは登録プロセス中に学習したトポロジー情報に基づいて適正にルート付けができる。

【0071】

1実施例ではアプリケーションファンクション並びにポリシールータは第三者のネットワークまたはアプリケーションプロバイダのドメインに存在する。別実施例では全ポリシーコンポーネントは異なるネットワークまたはプロバイダドメインに存在する。

【0072】

上記のシナリオではサブスクライバはネットワークの中心部に位置するアプリケーションにアクセスする。アプリケーションファンクションはポリシーリクエストをそのデフォルト（休止）PSに発行する。本例の場合これはポリシールータである。その後にこのポリシールータは、アンカーPSにサブスクライバを中心とするポリシーを実行させるためにポリシーリクエストを関連アンカーPSに転送する任務を負う。アンカーPSはその関連ポリシールールを実行し、続いてリクエストを利用PSに転送する。

【0073】

[プッシュモデル]

これまで解説したポリシー相互間作用はポリシー配信の“プッシュモデル”を実行するものである。アプリケーションファンクションはリクエストをポリシールータに“プッシュ”し、ポリシールータはリクエストをアンカーPSに“プッシュ”し、アンカーはサー

10

20

30

40

50

ビス PS にリクエストを “ プッシュ ” する。

【 0074 】

トポロジー学習プロセスはポリシーのプッシュモデルを実行するのに重要である。サブスクライバが QoS を必要とするアプリケーションにアクセスするとき、アプリケーションはリクエストをポリシールータに信号発信する。ポリシールータは、サブスクライバのためにアンカー PS を検索し、評価のために QoS リクエストをそのアンカー PS に転送する前に特定グローバルまたはアプリケーション専用ポリシールールを評価することができる。

【 0075 】

ポリシールータとアンカー PS はサブスクライバの “ ホームネットワーク ” ドメイン内に存在できる（例えば、もしこれが S print サブスクライバであり、サブスクライバが別ネットワークからの S print サービスにアクセスしていれば、相互間作用に関与するアプリケーション、ポリシールータおよびアンカー PS は全て S print ドメイン内に存在するであろう）。

10

【 0076 】

アンカー PS はサブスクライバポリシールール（本例では “ サブスクライバを中心とするルール ” と呼称；例えば特定サブスクライバがいくつのセッションを同時利用可能か、またはサブスクライバがどのようなアプリケーションおよびサービスを利用可能か、あるいはサブスクライバが利用限度を超えたか、等々）に関して QoS リクエストを評価する。もし QoS リクエストが承認可能と評価されたらアンカー PS はそのリクエストをサブスクライバに現在利用されているサブスクライバアクセスデバイスにインターフェースしている “ 利用 ” PS に送る。

20

【 0077 】

必要であれば（例えばもしサブスクライバが別運用ドメインでローミングしていたら）アンカー PS は運用ポリシールールに基づいて QoS リクエストも評価する。最終的には利用 PS は QoS 指示をサブスクライバアクセス装置に送り、サブスクライバのためにその QoS を実行する。利用 PS は来訪ネットワーク内に存在できる。利用 PS はリソース利用（アクセスネットワークで消費されるリソース量をコントロールすること）に関してポリシールールを実行するであろう。

30

【 0078 】

例えば、（来訪 / 利用ポリシーサーバのドメイン範囲内で）サブスクライバがサービスを受けているアクセスネットワークにおいて消費される全バンド幅が設定閾値 X を超えれば利用 PS はサブスクライバによるリソースのリクエストを拒絶することができる。別例では、（利用 / 来訪ポリシーサーバのコントロール下で）特定実施ポイントで全ビデオアプリケーションのために消費されるバンド幅が設定閾値 Y を超えれば利用 PS はサブスクライバからのビデオリクエストを拒絶することができる。あるいは利用 PS は特定実施ポイントで搬送中の音声セッションの総数が別設定閾値 Z を超えるならビデオの上記リクエストを拒絶することができる。

【 0079 】

あるいはアプリケーションファンクションはアンカー PS と同一のドメイン / ネットワークに存在できる。この場合にはアプリケーションファンクションはアンカー PS に直接的に信号発信し、アンカーをアプリケーションファンクションのデフォルト PS として扱うであろう。アンカー PS は両方のポリシールート付けファンクションを実行し（利用 PS にルート付けしている理由による）、サブスクライバを中心とするポリシールールを実行する任務を担う PS をも実行する。アンカーポリシーサーバはアプリケーションファンクションにも直接的にインターフェースしている。

40

【 0080 】

図 7 はアプリケーションファンクションの位置がアンカー PS と同一のネットワーク内に存在し、アプリケーションファンクションのデフォルト PS としてアンカー PS を使用している実施例を図示する。

50

【 0 0 8 1 】

図 7 で示すシステムではサブスクライバの利用 PS は来訪ネットワーク（例えば T e l u s ）でも構わないがサブスクライバは V e r i z o n のカスタマーであり、そのアンカーポリシーサーバは V e r i z o n ネットワーク内に、サブスクライバがアクセスを願うアプリケーションと共に存在する。実施例によっては異なる商業エンティティにより運用されるネットワークは本例では“ポリシーピアリング”と呼称されるものを介して協調作用する。サブスクライバに関連するローミング情報をを利用して利用およびアンカーポリシーサーバはポリシーのインター-オペレータサービスレベルアグリーメント（ S L A ）並びに他のビジネスアグリーメントを実行することができる。

【 0 0 8 2 】

アプリケーションリクエストはネットワーク内またはアンカー PS が存在するネットワークとは異なるプロバイダ内に物理的に存在するサブスクライバで発生する。ポリシーリクエストは利用 PS または来訪 PS に最終的に転送される。このシナリオでは第三者のアプリケーションが来訪ネットワークにリクエストするものを規制するのに来訪 PS が利用可能である。例えば 2 者（アクセスネットワークプロバイダおよびコンテンツプロバイダ）間で合意したビジネスアレンジに基づいて来訪ポリシーサーバは第三者のコンテンツ/アプリケーションプロバイダにより実行されるコンテンツ/アプリケーションのためにネットワークへの進入が承認されたものを追跡調査することができる。

【 0 0 8 3 】

展開スケールによっては論理ポリシーファンクション（ルート付け、アンカー、利用、その他）は構造の複雑性を低減するように共同配置することができる。

【 0 0 8 4 】

無線の世界ではサブスクライバがサブスクライバアクセス装置から脱登録すると、その脱登録メッセージは利用 PS に送られ、さらにポリシールータに転送される。図 8 は 1 実施例による例示的メッセージフロー図である。ポリシールータは脱登録の事実をアンカー PS に転送し、サブスクライバがネットワークではこれ以上アクセスすることも、利用 PS と関係することもできないことを表示する。あるいは脱登録メッセージを利用 PS から別のアンカー PS に直接的に転送することもできる。

【 0 0 8 5 】

一般的にサブスクライバは特定アンカー PS と関係するが、この関係はほとんどの場合に一貫しているべきである。しかしサブスクライバのアンカー PS がいずれ変更される場合がある。管理セット時間に基づいて定期的にポリシールータとアンカー PS は利用されている I S I の範囲から I S I を派生させることができる。これは典型的に使用されるサブスクライバアクセス装置に基づいてサブスクライバに利用されるさらに効率的な PS が存在する場合に該当する。

【 0 0 8 6 】**[プルモデル]**

ポリシー配信の別方法は“プル”モデルによって実行される。プルモデルではクライアント/サブスクライバはアプリケーションファンクションからのリクエストの代わりにポリシーリクエストを直接的に行使する。クライアントは R S V P のごときメッセージを使用してアクセス装置（実施ポイント）からのリクエストを作動させる。アクセス装置はその指定した利用 PS からのポリシーリクエストを始動する。利用ポリシーサーバはアンカー PS からサブスクライバのために適正なセットのポリシーを回収する必要があるであろう。

【 0 0 8 7 】

トポロジー発見/配信フェーズ中に使用されたものと同じタイプの機構を使用して利用 PS はその適正セットのポリシーのためにアンカー PS から“プル”操作することができる。大型スケール展開の場合においてはネットワークではプッシュモデル並びにプルモデルの両方が実行される。

【 0 0 8 8 】

10

20

30

40

50

図9はサブスクライバがポリシーリクエストを作動させるポリシー普及のためのプルモデル”を図示する。アクセスネットワーク装置は利用PSからのポリシーのためにプル操作することができる。利用PSはトポロジー情報の配信に利用されるものと同一タイプの方法でアンカーPSからサブスクライバのためのポリシーを得るためにプル操作することができる。プル操作対象のポリシータイプには、サブスクライバの受益権利（どのようなサービス/アプリケーションにサブスクライバがアクセス可能か）、どのサービスにも適応するQoS処理、サービス対価請求方法（定額料金請求またはバイト単位請求またはタイムチャージ、等々）が含まれる。

【0089】

サブスクライバが初めてネットワークに登録するとき利用PSはそのサブスクライバがローミングしているか否かを承知している。アンカーPSもサブスクライバのローミング状況を承知している。ローミング情報はサブスクライバが最初にネットワークにアタッチした際にアクセスネットワーク装置からのメッセージから推察可能である。当初アタッチメントメッセージに存在するサブスクライバレルム情報はサブスクライバに関する情報を提供できる。

10

【0090】

例えばサブスクライバはTelsネットワークにローミングしているVerizon無線サブスクライバであろう。サブスクライバ/クライエントからの情報はサブスクライバがVerizon無線サブスクライバであることを表示するであろう。利用PSはこの情報をを利用してどのアンカーPSまたはポリシールータがトポロジー情報（利用PSからのブッシュ内）を受領し、ポリシー情報（利用PSによるプル内）を提供するかを決定する。

20

【0091】

様々なポリシーサーバもサブスクライバレルム情報をを利用してサブスクライバに対するポリシールールを実行できる。例えばサブスクライバが他のサービスプロバイダのサブスクライバではなく、VerizonのサブスクライバであればTelsネットワーク内の利用PSは異なるレベルの処理を提供するルールを有することができる。TelsとVerizonとの間に配置されたサービスレベルアグリーメントまたはビジネスアグリーメントが存在すると、Telsの利用PSは、音声、ビデオまたはデータサービスのために増強QoSの提供のごときビジネスルールの実行に使用することができる。実施例によっては、特定レルムのファンクションとして様々なアプリケーションに対してサブスクライバが異なる様式で料金請求されるような異なる請求形態の提供のためにもレルム情報が使用される。

30

【0092】

本発明はその精神または本質的な特徴から逸脱せずに他の実施形態であっても同様に実施可能である。従ってそれら実施例は本発明の説明のためだけに提供されており、本発明の限定は意図されておらず、本発明の範囲はそれら実施例ではなく本明細書の「請求の範囲」において定義されており、請求範囲内の全ての変更および均等物は本発明に含まれる。

40

【図面の簡単な説明】

【0093】

【図1】図1はデジタルコンテンツを複数のサブスクライバに送るための従来技術システム10を図示する。

50

【図2】図2は本発明に従って構築されたシステム構造の例示的実施例を図示する。

【図3】図3は指定されたポリシールータに登録情報を転送する利用PS150を図示する。

【図4】図4は指定されたポリシールータに登録情報を転送する利用PS150を図示する。

【図5】図5はポリシールータからアンカーへ、そしてその後に利用PSへのポリシーリクエストのルート付けするステップを図示する。

【図 6】図 6 はポリシールータからアンカーへ、そしてその後に利用 PSへのポリシーリクエストのルート付けするステップを図示する。

【図 7】図 7 はアプリケーションファンクションの位置がアンカー PSと同じネットワーク内に存在している実施例を図示する。

【図 8】図 8 は図 2 で示すシステムの 1 実施例の例示的メッセージ工程図を図示する。

【図 9】図 9 はポリシーを配信するための“プル”モデルを図示する。

【符号の説明】

【0 0 9 4】

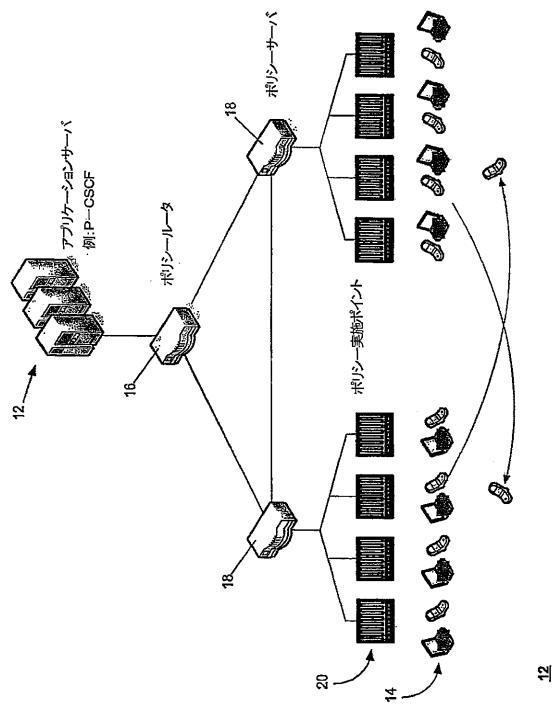
1 0 2 ネットワーク

1 0 8 サブスクリイブ

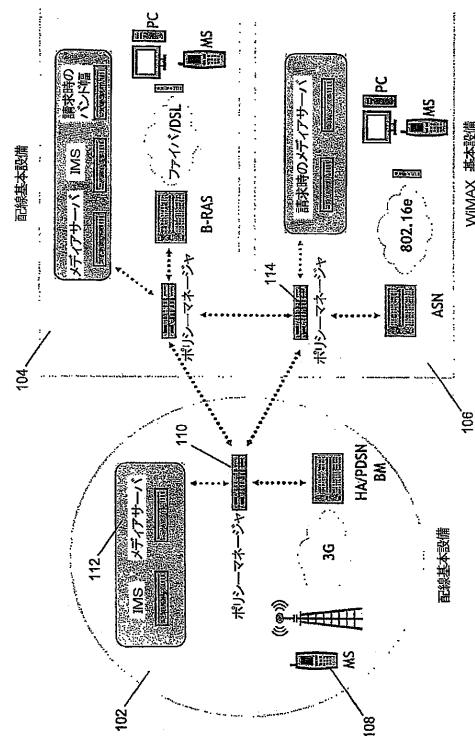
1 1 0 ポリシーファンクション

10

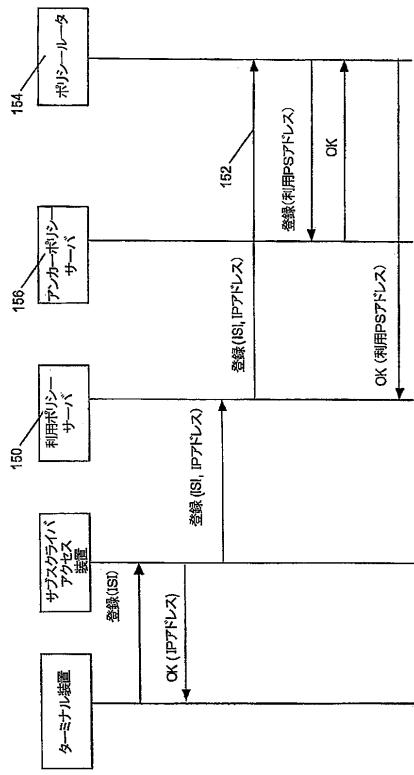
【図 1】



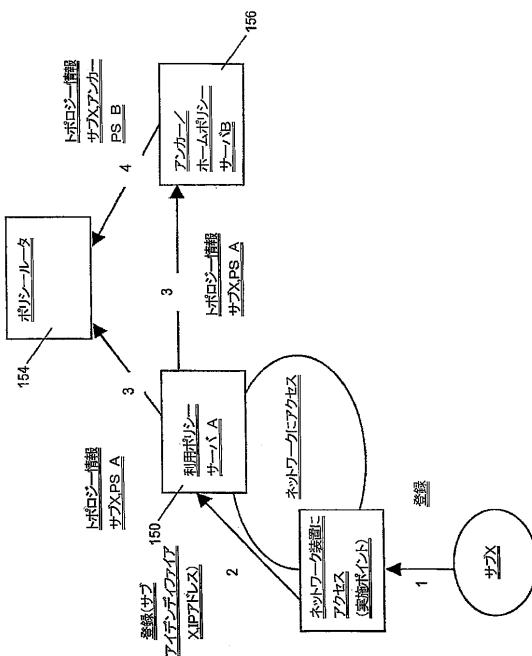
【図 2】



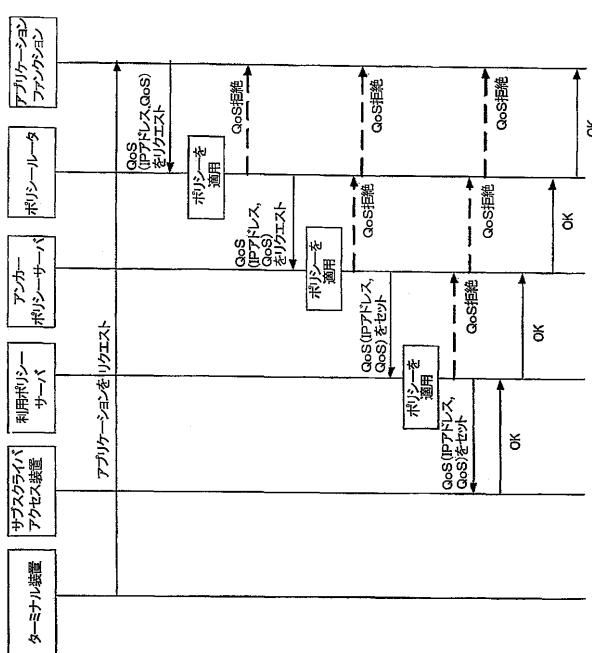
【図3】



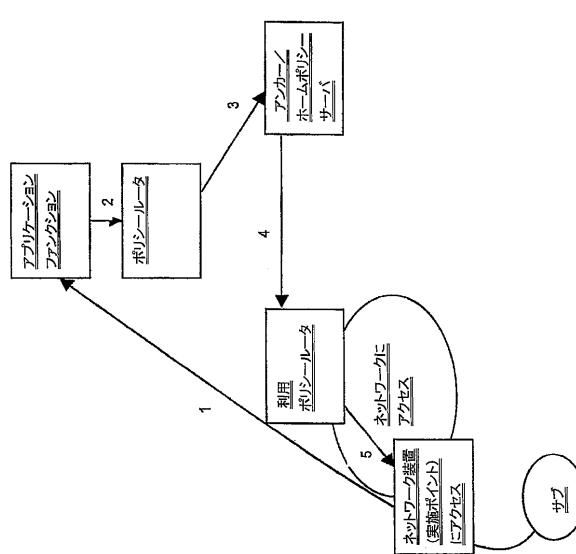
【図4】



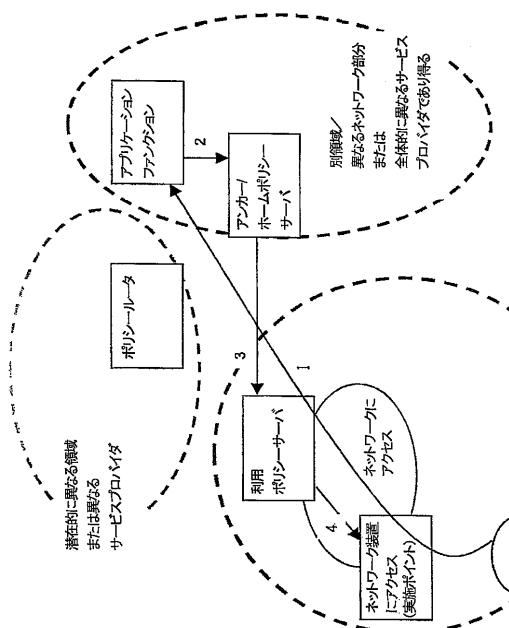
【図5】



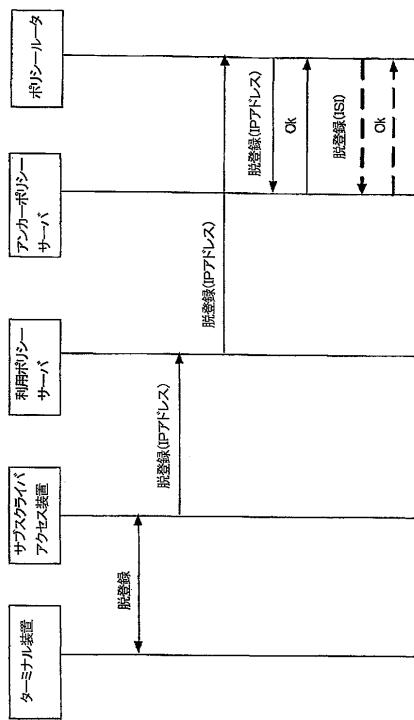
【図6】



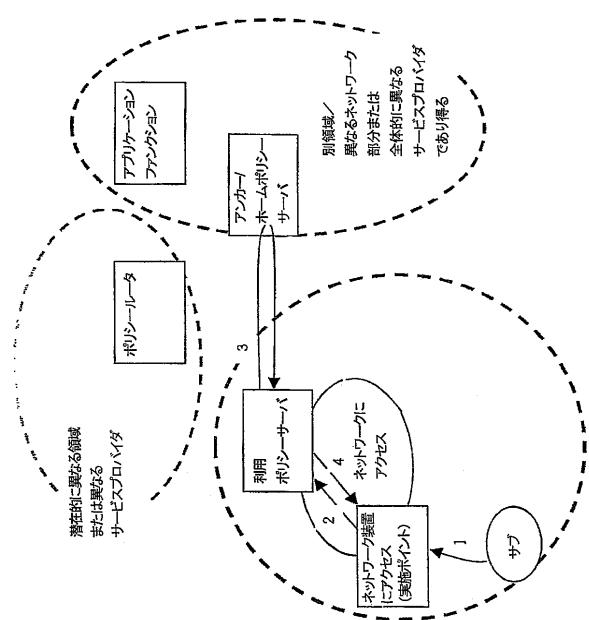
【図7】



【図8】



【図9】



【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application No. PCT/US07/64164						
A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - H04L 12/26 (2007.01) USPC - 370/230.1 According to International Patent Classification (IPC) or to both national classification and IPC								
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC(8) - H04L 12/26 (2007.01) USPC - 370/230.1								
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched								
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) PatBase, MicroPatent, IP.com, DialogPro, Google Patent								
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Category*</th> <th style="text-align: left; padding: 2px;">Citation of document, with indication, where appropriate, of the relevant passages</th> <th style="text-align: left; padding: 2px;">Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;">X</td> <td style="padding: 2px;">US 2002/0036983 A1 (WIDEGREEN et al) 28 March 2002 (28.03.2002) entire document</td> <td style="padding: 2px;">1-20</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	US 2002/0036983 A1 (WIDEGREEN et al) 28 March 2002 (28.03.2002) entire document	1-20
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.						
X	US 2002/0036983 A1 (WIDEGREEN et al) 28 March 2002 (28.03.2002) entire document	1-20						
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/>								
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed								
Date of the actual completion of the international search 11 October 2007	Date of mailing of the international search report 15 NOV 2007							
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774							

フロントページの続き

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