(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-233078
(P2014-233078A)
(43)公開日　平成26年12月11日(2014.12.11)

(51)Int.Cl.		F I		テーマコード（参考）
H04W 88/06	***(2009.01)***	H04W	88/06	5K067
H04W 92/08	***(2009.01)***	H04W	92/08	5K201
H04W 12/08	***(2009.01)***	H04W	12/08	
H04M 3/00	***(2006.01)***	H04M	3/00　B	

審査請求 有　請求項の数 3　ＯＬ　（全 38 頁）

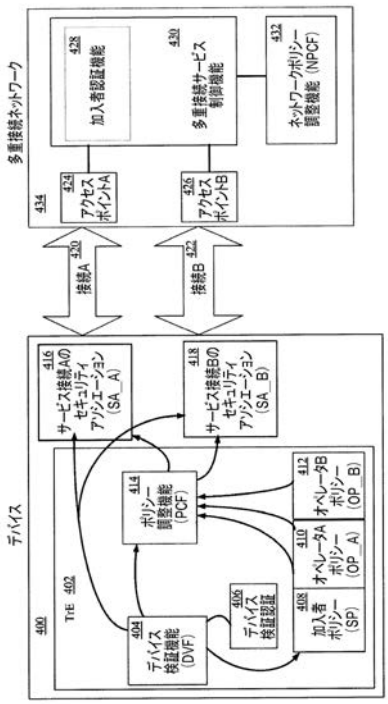
(21)出願番号　特願2014-149193 (P2014-149193)
(22)出願日　平成26年7月22日 (2014.7.22)
(62)分割の表示　特願2013-502897 (P2013-502897)の分割
原出願日　平成23年4月1日 (2011.4.1)
(31)優先権主張番号　61/320,665
(32)優先日　平成22年4月2日 (2010.4.2)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/320,910
(32)優先日　平成22年4月5日 (2010.4.5)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/362,597
(32)優先日　平成22年7月8日 (2010.7.8)
(33)優先権主張国　米国 (US)

(71)出願人　510030995
インターデイジタル　パテント　ホールディングス　インコーポレイテッド
アメリカ合衆国　１９８０９　デラウェア州　ウィルミントン　ベルビュー　パークウェイ　２００　スイート　３００
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　アレクサンダー　レズニック
アメリカ合衆国　０８５６０　ニュージャージー州　タイタスビル　リバー　ロード　１２１２

最終頁に続く

(54)【発明の名称】ポリシー管理のための方法

(57)【要約】
【課題】ネットワークおよび／またはワイヤレス送信／受信ユニット上でのポリシーの施行を調整するためのシステム、方法、および装置が開示される。
【解決手段】ポリシーは、ユーザ機器上でサービスを提供する１つまたは複数のステークホルダのステークホルダ固有のポリシーを含むことができる。ステークホルダ固有のポリシーの施行は、ポリシー調整機能を使用して、安全に調整され得る。サービス制御ポリシーおよびアクセス制御ポリシーを調整するネットワークポリシー調整機能（ＮＰＣＦ）を含むシステム、方法、および装置も開示される。ＮＰＣＦは、１つまたは複数のサービス制御エンティティのサービス制御ポリシーおよび１つまたは複数のアクセス制御エンティティのアクセス制御ポリシーの施行を調整することができる。
【選択図】図４



【特許請求の範囲】
【請求項１】
１つまたは複数のステークホルダの代わりにサービスを提供することができるユーザ機器であって、前記サービスの前記提供は前記１つまたは複数のステークホルダによって管理されることができ、前記ユーザ機器は前記１つまたは複数のステークホルダと通信し、
少なくとも１つのプロセッサと、
前記１つまたは複数のステークホルダの１つまたは複数のステークホルダ固有のポリシーが安全に記憶されるメモリであって、それぞれのステークホルダ固有のポリシーは異なるステークホルダ固有のポリシーであり、それぞれのステークホルダは異なるステークホルダである、メモリと、
前記１つまたは複数のステークホルダの前記１つまたは複数のステークホルダ固有のポリシーの安全な施行を調整する、前記プロセッサ上で実行するように構成されたポリシー調整機能（ＰＣＦ）と
を備えることを特徴とするユーザ機器。
【請求項２】
前記ＰＣＦは、自機器内の安全な環境内で実行するように構成されることを特徴とする請求項１に記載のユーザ機器。
【請求項３】
前記安全な環境は、信頼できる環境（ＴｒＥ：ｔｒｕｓｔｅｄ　ｅｎｖｉｒｏｎｍｅｎｔ）またはスマートカードであることを特徴とする請求項２に記載のユーザ機器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ワイヤレス通信に関する。
【０００２】
関連出願の相互参照
本出願は、２０１０年４月２日に出願された米国特許仮出願第６１／３２０，６６５号明細書、２０１０年４月５日に出願された米国特許仮出願第６１／３２０，９１０号明細書、および２０１０年７月８日に出願された米国特許仮出願第６１／３６２，５９７号明細書の利益を主張するものであり、これらの内容はその全体が参照により本明細書に組み込まれる。
【背景技術】
【０００３】
ワイヤレス送信／受信ユニット（ＷＴＲＵ）および／または多重接続ネットワークは、１つもしくは複数のエンティティもしくはステークホルダ（ｓｔａｋｅｈｏｌｄｅｒ）とともに、および／またはそれらの代わりに機能および／または通信を実行することが可能である。例えば、モバイルデバイスは、インターネットへの常時接続などの多重接続サービスを提供するとともに、高品質の音声サービスを提供し続けることができる。そのような多重接続サービスは、異なるネットワークオペレータなど異なるステークホルダによって、またはそれらの代わりに提供され得る。それぞれのステークホルダは、そのステークホルダの１つまたは複数のポリシーに従って、そのような機能または通信を実行することを望む場合がある。異なるステークホルダのポリシーは、競合しているか、無料である場合がある。
【発明の概要】
【０００４】
通信デバイス上でのおよび／または通信ネットワークにおけるポリシーの施行の管理および／または調整のためのシステム、方法、および装置が開示される。一実施形態によれば、１つまたは複数のステークホルダの代わりにサービスを提供することができるユーザ機器が記載される。ユーザ機器は、１つまたは複数のステークホルダと通信することができ、ステークホルダは、ユーザ機器上でのサービスの提供を管理することができる。ユー

ザ機器は、少なくとも１つのプロセッサ、メモリ、およびポリシー調整機能を含むことができる。１つまたは複数のステークホルダの１つまたは複数のステークホルダ固有のポリシーを、メモリ上で安全に記憶することができる。それぞれのステークホルダ固有のポリシーは、異なるステークホルダ固有のポリシーであってもよく、それぞれのステークホルダは、異なるステークホルダであってもよい。ポリシー調整機能は、プロセッサ上の安全な環境内で実行することなどによって、１つまたは複数のステークホルダの１つまたは複数のステークホルダ固有のポリシーの安全な管理および／または施行を調整することができる。

【０００５】

別の実施形態によれば、複数のアクセスポイントを有する１つまたは複数のネットワークに対してサービス制御ポリシーおよびアクセス制御ポリシーを調整するように構成されたシステムが記載される。それぞれのアクセスポイントを、１つまたは複数のアクセス制御エンティティによって管理することができ、それぞれのアクセス制御エンティティを、１つまたは複数のサービス制御エンティティによって管理することができる。システムは、ポリシー記憶機能およびネットワークポリシー調整機能（ＮＰＣＦ：ｎｅｔｗｏｒｋ ｐｏｌｉｃｙ ｃｏｏｒｄｉｎａｔｉｏｎ ｆｕｎｃｔｉｏｎ）を含むことができる。サービス制御ポリシーおよびアクセス制御ポリシーを、ポリシー記憶機能に記憶することができる。サービス制御ポリシーおよびアクセス制御ポリシーの施行を、ＮＰＣＦによって調整することができる。ＮＰＣＦは、１つまたは複数のアクセス制御エンティティに対するアクセス制御ポリシーの施行を調整することができる。ＮＰＣＦは、１つまたは複数のサービス制御エンティティに対するサービス制御ポリシーの施行を調整することができる。

【０００６】

本明細書に記載される方法、システム、および装置の他の特徴および態様は、以下の詳細な説明および関連する図面から明らかとなろう。

【図面の簡単な説明】

【０００７】

添付の図面とともに例として与えられた以下の説明から、より詳細な理解を得ることができる。

【０００８】

【図１Ａ】１つまたは複数の開示された実施形態を実施することができる例示的な通信システムのシステム図である。

【図１Ｂ】図１Ａに示す通信システム内で使用することができる例示的なワイヤレス送信／受信ユニット（ＷＴＲＵ）のシステム図である。

【図１Ｃ】図１Ａに示す通信システム内で使用することができる例示的な無線アクセスネットワークおよび例示的なコアネットワークのシステム図である。

【図２】いくつかのアグリゲーションシナリオの例を示す図である。

【図３】高レベルな性質のレイヤのやり取りを示すネットワークアーキテクチャの図である。

【図４】多重接続ネットワークにおける通信に使用されるポリシー調整エンティティの一例を示す図である。

【図５】ネットワークポリシーエンティティを示す機能アーキテクチャの図である。

【図６】開示された実施形態の１つまたは複数を実施することができる例示的なワイヤレス通信システムの別のシステム図である。

【図７】図６のワイヤレス通信システムのワイヤレス送信／受信ユニット（ＷＴＲＵ）およびノードＢの機能ブロック図である。

【図８】ＩＥＥＥ８０２．１９システムにおける例示的なセキュリティ手順の流れ図である。

【図９】初期アクセスの信頼の連鎖を示す図である。

【図１０】初回の接続（ａｔｔａｃｈｍｅｎｔ）および／または通常の動作の例示的なプ

ロセスを示す図である。

【発明を実施するための形態】

【０００９】

以下で参照されるとき、「ワイヤレス送信／受信ユニット（ＷＴＲＵ）」という用語は、ユーザ機器（ＵＥ）、移動局、固定もしくは移動加入者ユニット、ページャ、セルラ電話、携帯情報端末（ＰＤＡ）、コンピュータ、またはワイヤレス環境で動作することが可能な任意の他のタイプのデバイスを含むことができるが、これらに限定されない。以下で参照されるとき、「基地局」という用語は、ノードＢ、サイトコントローラ、アクセスポイント（ＡＰ）、またはワイヤレス環境で動作することが可能な任意の他のタイプのインターフェースデバイスを含むことができるが、これらに限定されない。以下で参照されるとき、「ノードＢ」という用語は、ホームノードＢ（ＨＮＢ）、ｅノードＢ（ｅＮＢ）またはホームｅノードＢ（ＨｅＮＢ）を含むことができるが、これらに限定されない。また、「ネットワーク」という語へのいかなる参照も、例えば、本明細書に記載される無線ネットワークコントローラ（ＲＮＣ）、コントローリングＲＮＣ（ＣＲＮＣ）、ドリフトＲＮＣ、または任意の他の通信ネットワークを参照し得る。

【００１０】

ポリシー制御管理のためのシステム、方法、および装置が本明細書に記載される。ポリシー制御管理は、例えば、ＷＴＲＵおよび／またはネットワークエンティティに含むことができるポリシー制御エンティティによって実行され得る。ポリシー制御エンティティは、ＷＴＲＵおよび／またはネットワークと関連する１つまたは複数のステークホルダと関連するポリシーを調整することができる。一例によれば、ポリシー制御は、例えば、次世代ネットワーク（ＮＧＮ）アーキテクチャなどにおける、多重無線アクセス技術（ＲＡＴ）における多重接続通信に対して実行され得る。

【００１１】

一実施形態によれば、１つまたは複数のステークホルダの代わりにサービスを提供することができるユーザ機器が記載される。ユーザ機器は、１つまたは複数のステークホルダと通信することができ、ステークホルダは、ユーザ機器上でのサービスの提供を管理することができる。ユーザ機器は、少なくとも１つのプロセッサ、メモリ、および／またはポリシー調整機能を含むことができる。１つまたは複数のステークホルダの１つまたは複数のステークホルダ固有のポリシーを、ユーザ機器のメモリ上で安全に記憶することができる。それぞれのステークホルダ固有のポリシーは、異なるステークホルダ固有のポリシーであってもよく、それぞれのステークホルダは、異なるステークホルダであってもよい。ポリシー調整機能は、プロセッサ上の安全な環境内で実行することなどによって、１つまたは複数のステークホルダの１つまたは複数のステークホルダ固有のポリシーの安全な施行を調整することができる。

【００１２】

別の実施形態によれば、複数のアクセスポイントを有する１つまたは複数のネットワークに対してサービス制御ポリシーおよびアクセス制御ポリシーを調整するように構成されたシステムが記載される。それぞれのアクセスポイントを、１つまたは複数のアクセス制御エンティティによって管理することができ、それぞれのアクセス制御エンティティを、１つまたは複数のサービス制御エンティティによって管理することができる。システムは、ポリシー記憶機能およびネットワークポリシー調整機能（ＮＰＣＦ）を含むことができる。サービス制御ポリシーおよびアクセス制御ポリシーを、ポリシー記憶機能に記憶することができる。サービス制御ポリシーおよびアクセス制御ポリシーの施行を、ＮＰＣＦによって調整することができる。ＮＰＣＦは、１つまたは複数のアクセス制御エンティティでのアクセス制御ポリシーの施行を調整することができる。ＮＰＣＦは、１つまたは複数のサービス制御エンティティでのサービス制御ポリシーの施行を調整することができる。

【００１３】

図１Ａは、１つまたは複数の開示された実施形態を実施することができる例示的な通信システム１００の図である。通信システム１００は、音声、データ、映像、メッセージン

グ、ブロードキャストなどのコンテンツを複数のワイヤレスユーザに提供する多重アクセスシステムであってもよい。通信システム１００により、複数のワイヤレスユーザは、ワイヤレス帯域幅を含むシステムリソースを共有することによって、そのようなコンテンツにアクセスすることができる。例えば、通信システム１００は、符号分割多元接続（ＣＤＭＡ）、時分割多元接続（ＴＤＭＡ）、周波数分割多元接続（ＦＤＭＡ）、直交ＦＤＭＡ（ＯＦＤＭＡ）、シングルキャリアＦＤＭＡ（ＳＣ－ＦＤＭＡ）などの１つまたは複数のチャネルアクセス方法を用いることができる。

【００１４】

図１Ａに示すように、通信システム１００は、ワイヤレス送信／受信ユニット（ＷＴＲＵ）１０２ａ、１０２ｂ、１０２ｃ、１０２ｄ、無線アクセスネットワーク（ＲＡＮ）１０４、コアネットワーク１０６、公衆交換電話網（ＰＳＴＮ）１０８、インターネット１１０、および他のネットワーク１１２を含むことができるが、開示された実施形態は、任意の数のＷＴＲＵ、基地局、ネットワーク、および／またはネットワーク要素を企図することを理解されたい。ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄのそれぞれは、ワイヤレス環境で動作するおよび／または通信するように構成された任意のタイプのデバイスであってもよい。例として、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄを、ワイヤレス信号を送信するおよび／または受信するように構成することができ、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄは、ユーザ機器（ＵＥ）、移動局、固定または移動加入者ユニット、ページャ、セルラ電話、携帯情報端末（ＰＤＡ）、スマートフォン、ラップトップ、ネットブック、パーソナルコンピュータ、ワイヤレスセンサ、コンシューマ向け電子機器などを含むことができる。

【００１５】

通信システム１００は、基地局１１４ａおよび基地局１１４ｂを含むこともできる。基地局１１４ａ、１１４ｂのそれぞれは、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄのうちの少なくとも１つとワイヤレスにインターフェースして、コアネットワーク１０６、インターネット１１０、および／またはネットワーク１１２などの１つまたは複数の通信ネットワークへのアクセスを容易にするように構成された任意のタイプのデバイスであってもよい。例として、基地局１１４ａ、１１４ｂは、トランシーバ基地局（ＢＴＳ）、ノードＢ、ｅノードＢ、ホームノードＢ、ホームｅノードＢ、サイトコントローラ、アクセスポイント（ＡＰ）、ワイヤレスルータなどであってもよい。基地局１１４ａ、１１４ｂはそれぞれ単一の要素として表されているが、基地局１１４ａ、１１４ｂは任意の数の相互接続された基地局および／またはネットワーク要素を含むことができることを理解されたい。

【００１６】

基地局１１４ａはＲＡＮ１０４の一部であってもよく、ＲＡＮ１０４は他の基地局および／または基地局コントローラ（ＢＳＣ）、無線ネットワークコントローラ（ＲＮＣ）、中継ノードなどのネットワーク要素（図示せず）を含むこともできる。基地局１１４ａおよび／または基地局１１４ｂは、セル（図示せず）と呼ぶことができる特定の地理的な領域内でワイヤレス信号を送信するおよび／または受信するように構成され得る。セルは、セルセクタにさらに分割され得る。例えば、基地局１１４ａと関連するセルは、３つのセクタに分割され得る。したがって、一実施形態では、基地局１１４は、３つのトランシーバ、すなわち、セルのそれぞれのセクタに１つのトランシーバを含むことができる。別の実施形態では、基地局１１４ａは、多入力多出力（ＭＩＭＯ）技術を用いることができ、したがって、セルのそれぞれのセクタに複数のトランシーバを利用することができる。

【００１７】

基地局１１４ａ、１１４ｂは、無線インターフェース１１６を介してＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄの１つまたは複数と通信することができ、無線インターフェース１１６は、任意の適切なワイヤレス通信リンク（例えば、無線周波数（ＲＦ）、マイクロ波、赤外線（ＩＲ）、紫外線（ＵＶ）、可視光など）であってもよい。任意の適切な無線アクセス技術（ＲＡＴ）を使用して、無線インターフェース１１６を確立するこ

とができる。
【００１８】
より具体的には、上記に述べたように、通信システム１００は多重アクセスシステムであってもよく、ＣＤＭＡ、ＴＤＭＡ、ＦＤＭＡ、ＯＦＤＭＡ、ＳＣ－ＦＤＭＡなどの１つまたは複数のチャネルアクセス方式を用いることができる。例えば、ＲＡＮ１０４における基地局１１４ａおよびＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃは、広帯域ＣＤＭＡ（ＷＣＤＭＡ（登録商標））を使用して無線インターフェース１１６を確立することができるユニバーサル移動体通信システム（ＵＭＴＳ）地上無線アクセス（ＵＴＲＡ）などの無線技術を実施することができる。ＷＣＤＭＡは、高速パケットアクセス（ＨＳＰＡ）および／または進化型ＨＳＰＡ（ＨＳＰＡ＋）などの通信プロトコルを含むことができる。ＨＳＰＡは、高速ダウンリンクパケットアクセス（ＨＳＤＰＡ）および／または高速アップリンクパケットアクセス（ＨＳＵＰＡ）を含むことができる。
【００１９】
別の実施形態では、基地局１１４ａおよびＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃは、ロングタームエボリューション（ＬＴＥ）および／またはＬＴＥアドバンスト（ＬＴＥ－Ａ）を使用して無線インターフェース１１６を確立することができる進化型ＵＭＴＳ地上無線アクセス（Ｅ－ＵＴＲＡ）などの無線技術を実施することができる。
【００２０】
他の実施形態では、基地局１１４ａおよびＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃは、ＩＥＥＥ８０２．１６（すなわち、ＷｉＭＡＸ（Ｗｏｒｌｄｗｉｄｅ Ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ ｆｏｒ Ｍｉｃｒｏｗａｖｅ Ａｃｃｅｓｓ））、ＣＤＭＡ２０００、ＣＤＭＡ２０００ ＩＸ、ＣＤＭＡ２０００ ＥＶ－ＤＯ、ＩＳ－２０００（Ｉｎｔｅｒｉｍ Ｓｔａｎｄａｒｄ ２０００）、ＩＳ－９５（Ｉｎｔｅｒｉｍ Ｓｔａｎｄａｒｄ ９５）、ＩＳ－８５６（Ｉｎｔｅｒｉｍ Ｓｔａｎｄａｒｄ ８５６）、ＧＳＭ（登録商標）（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）、ＥＤＧＥ（Ｅｎｈａｎｃｅｄ Ｄａｔａ ｒａｔｅｓ ｆｏｒ ＧＳＭ Ｅｖｏｌｕｔｉｏｎ）、ＧＥＲＡＮ（ＧＳＭ ＥＤＧＥ）などの無線技術を実施することができる。
【００２１】
図１Ａにおける基地局１１４ｂは、例えば、ワイヤレスルータ、ホームノードＢ、ホームｅノードＢ、またはアクセスポイントであってもよく、事業所、家庭、車両、キャンパスなどの局所的な区域におけるワイヤレス接続を容易にするために任意の適切なＲＡＴを利用することができる。一実施形態では、基地局１１４ｂおよびＷＴＲＵ１０２ｃ、１０２ｄは、ＩＥＥＥ８０２．１１などの無線技術を実施して、ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）を確立することができる。別の実施形態では、基地局１１４ｂおよびＷＴＲＵ１０２ｃ、１０２ｄは、ＩＥＥＥ８０２．１５などの無線技術を実施して、ワイヤレスパーソナルエリアネットワーク（ＷＰＡＮ）を確立することができる。さらに別の実施形態では、基地局１１４ｂおよびＷＴＲＵ１０２ｃ、１０２ｄは、セルラベースのＲＡＴ（例えば、ＷＣＤＭＡ、ＣＤＭＡ２０００、ＧＳＭ、ＬＴＥ、ＬＴＥ－Ａなど）を利用して、ピコセルまたはフェムトセルを確立することができる。図１Ａに示すように、基地局１１４ｂは、インターネット１１０に対する直接接続を有することができる。したがって、基地局１１４ｂは、コアネットワーク１０６を介してインターネット１１０にアクセスする必要がない場合がある。
【００２２】
ＲＡＮ１０４は、コアネットワーク１０６と通信することができ、コアネットワーク１０６は、音声、データ、アプリケーション、および／またはボイスオーバーインターネットプロトコル（ＶｏＩＰ）サービスをＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄの１つまたは複数に提供するように構成された任意のタイプのネットワークであってもよい。例えば、コアネットワーク１０６は、呼制御、請求サービス、モバイル位置ベースのサービス、プリペイドコール、インターネット接続、映像配信などを提供するおよび／ま

たはユーザ認証などの高レベルのセキュリティ機能を実行することができる。図１Ａには示されていないが、ＲＡＮ１０４および／またはコアネットワーク１０６は、ＲＡＮ１０４と同じＲＡＴまたは異なるＲＡＴを用いる他のＲＡＮと直接通信または間接通信することができることを理解されたい。例えば、Ｅ－ＵＴＲＡ無線技術を利用してもよいＲＡＮ１０４に接続されることに加えて、コアネットワーク１０６はＧＳＭ無線技術を用いる別のＲＡＮ（図示せず）とも通信することができる。

【００２３】

コアネットワーク１０６は、ＰＳＴＮ１０８、インターネット１１０、および／または他のネットワーク１１２にアクセスするための、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄのゲートウェイとしても機能する。ＰＳＴＮ１０８は、基本電話サービス（ＰＯＴＳ）を提供する回線交換電話網を含むことができる。インターネット１１０は、ＴＣＰ／ＩＰインターネットプロトコルスイートにおける伝送制御プロトコル（ＴＣＰ）、ユーザデータグラムプロトコル（ＵＤＰ）およびインターネットプロトコル（ＩＰ）などの一般的な通信プロトコルを使用する相互接続されたコンピュータネットワークおよびデバイスのグローバルシステムを含むことができる。ネットワーク１１２は、他のサービスプロバイダによって所有されるおよび／または操作される有線またはワイヤレス通信ネットワークを含むことができる。例えば、ネットワーク１１２は、ＲＡＮ１０４と同じＲＡＴまたは異なるＲＡＴを用いることができる１つまたは複数のＲＡＮに接続された別のコアネットワークを含むことができる。

【００２４】

通信システム１００におけるＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄのいくつかまたは全ては、マルチモード機能を含むことができる、すなわち、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃ、１０２ｄは、異なるワイヤレスリンクを介して異なるワイヤレスネットワークと通信するための複数のトランシーバを含むことができる。例えば、図１Ａに示すＷＴＲＵ１０２ｃは、セルラベースの無線技術を用いることができる基地局１１４ａ、およびＩＥＥＥ８０２無線技術を用いることができる基地局１１４ｂと通信するように構成され得る。

【００２５】

図１Ｂは、例示的なＷＴＲＵ１０２のシステム図である。図１Ｂに示すように、ＷＴＲＵ１０２は、プロセッサ１１８、トランシーバ１２０、送信／受信要素１２２、スピーカ／マイクロフォン１２４、キーパッド１２６、ディスプレイ／タッチパッド１２８、非リムーバブルメモリ１３０、リムーバブルメモリ１３２、電源１３４、全地球測位システム（ＧＰＳ）チップセット１３６、および他の周辺装置１３８を含むことができる。ＷＴＲＵ１０２は、上記の要素の任意の副組合せを含むとともに、一実施形態と一致したままであることができることを理解されたい。

【００２６】

プロセッサ１１８は、汎用プロセッサ、特殊用途プロセッサ、従来のプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、複数のマイクロプロセッサ、ＤＳＰコアに関連した１つまたは複数のマイクロプロセッサ、コントローラ、マイクロコントローラ、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）回路、任意の他のタイプの集積回路（ＩＣ）、状態機械などであってもよい。プロセッサ１１８は、信号符号化、データ処理、電力制御、入力／出力処理、および／またはＷＴＲＵ１０２がワイヤレス環境で動作することを可能にする任意の他の機能を実行することができる。プロセッサ１１８をトランシーバ１２０に結合することができ、トランシーバ１２０を送信／受信要素１２２に結合することができる。図１Ｂはプロセッサ１１８およびトランシーバ１２０を別個の構成要素として表しているが、プロセッサ１１８およびトランシーバ１２０を、電子パッケージまたはチップに一緒に組み込むことができることを理解されたい。

【００２７】

送信／受信要素１２２は、無線インターフェース１１６を介して基地局（例えば、基地

局１１４ａ）に信号を送信する、または基地局（例えば、基地局１１４ａ）から信号を受信するように構成され得る。例えば、一実施形態では、送信／受信要素１２２は、ＲＦ信号を送信するおよび／または受信するように構成されたアンテナであってもよい。別の実施形態では、送信／受信要素１２２は、例えば、ＩＲ信号、ＵＶ信号、または可視光信号を送信するおよび／または受信するように構成されたエミッタ／検出器であってもよい。さらに別の実施形態では、送信／受信要素１２２は、ＲＦ信号と光信号の両方を送信し、受信するように構成され得る。送信／受信要素１２２は、ワイヤレス信号の任意の組合せを送信するおよび／または受信するように構成され得ることを理解されたい。

【００２８】

加えて、送信／受信要素１２２は図１Ｂで単一の要素として表されているが、ＷＴＲＵ１０２は、任意の数の送信／受信要素１２２を含むことができる。より具体的には、ＷＴＲＵ１０２は、ＭＩＭＯ技術を用いることができる。したがって、一実施形態では、ＷＴＲＵ１０２は、無線インターフェース１１６を介してワイヤレス信号を送信し、受信するための２つ以上の送信／受信要素１２２（例えば、複数のアンテナ）を含むことができる。

【００２９】

トランシーバ１２０は、送信／受信要素１２２によって送信されるべき信号を変調し、送信／受信要素１２２によって受信された信号を復調するように構成され得る。上記に述べたように、ＷＴＲＵ１０２は、マルチモード機能を有することができる。したがって、トランシーバ１２０は、ＷＴＲＵ１０２が、例えば、ＵＴＲＡおよびＩＥＥＥ８０２．１１などの複数のＲＡＴを介して通信することを可能にするための複数のトランシーバを含むことができる。

【００３０】

ＷＴＲＵ１０２のプロセッサ１１８をスピーカ／マイクロフォン１２４、キーパッド１２６、および／またはディスプレイ／タッチパッド１２８（例えば、液晶ディスプレイ（ＬＣＤ）ディスプレイユニットまたは有機発光ダイオード（ＯＬＥＤ）ディスプレイユニット）に結合することができ、ＷＴＲＵ１０２のプロセッサ１１８はこれらからユーザ入力データを受信することができる。プロセッサ１１８は、ユーザデータをスピーカ／マイクロフォン１２４、キーパッド１２６、および／またはディスプレイ／タッチパッド１２８に出力することもできる。加えて、プロセッサ１１８は、非リムーバブルメモリ１３０および／またはリムーバブルメモリ１３２などの任意のタイプの適切なメモリから情報にアクセスし、このメモリにデータを記憶することができる。非リムーバブルメモリ１３０としては、ランダムアクセスメモリ（ＲＡＭ）、読取り専用メモリ（ＲＯＭ）、ハードディスク、または任意の他のタイプのメモリ記憶デバイスを挙げることができる。リムーバブルメモリ１３２としては、加入者識別モジュール（ＳＩＭ）カード、メモリスティック、セキュアデジタル（ＳＤ）メモリカードなどを挙げることができる。他の実施形態では、プロセッサ１１８は、サーバまたはホームコンピュータ（図示せず）上などの、ＷＴＲＵ１０２上に物理的に配置されていないメモリから情報にアクセスし、このメモリにデータを記憶することができる。

【００３１】

プロセッサ１１８は、電源１３４から電力を受信することができ、ＷＴＲＵ１０２における他の構成要素に電力を分配するおよび／または電力を制御するように構成され得る。電源１３４は、ＷＴＲＵ１０２に電力供給するための任意の適切なデバイスであってもよい。例えば、電源１３４は、１つまたは複数の乾電池（例えば、ニッケルカドミウム（ＮｉＣｄ）、ニッケル亜鉛（ＮｉＺｎ）、ニッケル水素（ＮｉＭＨ）、リチウムイオン（Ｌｉ－ｉｏｎ）など）、太陽電池、燃料電池などを含むことができる。

【００３２】

プロセッサ１１８をＧＰＳチップセット１３６に結合することもでき、ＧＰＳチップセット１３６は、ＷＴＲＵ１０２の現在の位置に関する位置情報（例えば、緯度および経度）を提供するように構成され得る。ＧＰＳチップセット１３６からの情報に加えて、また

はその代わりに、ＷＴＲＵ１０２は、無線インターフェース１１６を介して基地局（例えば、基地局１１４ａ、１１４ｂ）から位置情報を受信するおよび／または２つ以上の近くの基地局から受信されている信号のタイミングに基づいてその位置を判定することができる。ＷＴＲＵ１０２は、任意の適切な位置判定方法によって位置情報を取得するとともに、一実施形態と一致したままであることができることを理解されたい。

【００３３】

プロセッサ１１８を他の周辺装置１３８とさらに結合することができ、他の周辺装置１３８は、追加の特徴、機能および／または有線もしくはワイヤレス接続を提供する１つまたは複数のソフトウェアモジュールおよび／またはハードウェアモジュールを含むことができる。例えば、周辺装置１３８は、加速計、ｅコンパス、衛星トランシーバ、デジタルカメラ（写真または映像用）、ユニバーサルシリアルバス（ＵＳＢ）ポート、振動デバイス、テレビジョントランシーバ、ハンズフリーヘッドセット、Ｂｌｕｅｔｏｏｔｈ（登録商標）モジュール、周波数変調（ＦＭ）無線ユニット、デジタル音楽プレーヤ、メディアプレーヤ、ビデオゲームプレーヤモジュール、インターネットブラウザなどを含むことができる。

【００３４】

図１Ｃは、一実施形態によるＲＡＮ１０４およびコアネットワーク１０６のシステム図である。上記に述べたように、ＲＡＮ１０４はＵＴＲＡ無線技術を用いて、無線インターフェース１１６を介してＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃと通信することができる。また、ＲＡＮ１０４は、コアネットワーク１０６と通信することができる。図１Ｃに示すように、ＲＡＮ１０４はノードＢ１４０ａ、１４０ｂ、１４０ｃを含むことができ、ノードＢ１４０ａ、１４０ｂ、１４０ｃはそれぞれ、無線インターフェース１１６を介してＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃと通信するための１つまたは複数のトランシーバを含むことができる。ノードＢ１４０ａ、１４０ｂ、１４０ｃはそれぞれ、ＲＡＮ１０４内で特定のセル（図示せず）と関連してもよい。ＲＡＮ１０４は、ＲＮＣ１４２ａ、１４２ｂも含むことができる。ＲＡＮ１０４は、任意の数のノードＢおよびＲＮＣを含むとともに、一実施形態と一致したままであることができることを理解されたい。

【００３５】

図１Ｃに示すように、ノードＢ１４０ａ、１４０ｂは、ＲＮＣ１４２ａと通信することができる。さらに、ノードＢ１４０ｃは、ＲＮＣ１４２ｂと通信することができる。ノードＢ１４０ａ、１４０ｂ、１４０ｃは、Ｉｕｂインターフェースを介してそれぞれのＲＮＣ１４２ａ、１４２ｂと通信することができる。ＲＮＣ１４２ａ、１４２ｂは、Ｉｕｒインターフェースを介して互いに通信することができる。ＲＮＣ１４２ａ、１４２ｂのそれぞれは、ＲＮＣ１４２ａ、１４２ｂが接続された、それぞれのノードＢ１４０ａ、１４０ｂ、１４０ｃを制御するように構成され得る。加えて、ＲＮＣ１４２ａ、１４２ｂのそれぞれは、外側ループ電力制御、負荷制御、アドミッション制御、パケットスケジューリング、ハンドオーバ制御、マクロダイバーシチ、セキュリティ機能、データ暗号化などの他の機能を実行するまたはサポートするように構成され得る。

【００３６】

図１Ｃに示すコアネットワーク１０６は、メディアゲートウェイ（ＭＧＷ）１４４、モバイル交換センタ（ＭＳＣ）１４６、サービングＧＰＲＳサポートノード（ＳＧＳＮ）１４８、および／またはゲートウェイＧＰＲＳサポートノード（ＧＧＳＮ）１５０を含むことができる。上記の要素のそれぞれはコアネットワーク１０６の一部として表されているが、これらの要素のいずれか１つは、コアネットワークオペレータ以外のエンティティによって所有され得るおよび／または操作され得ることを理解されたい。

【００３７】

ＲＡＮ１０４におけるＲＮＣ１４２ａは、ＩｕＣＳインターフェースを介して、コアネットワーク１０６におけるＭＳＣ１４６に接続され得る。ＭＳＣ１４６は、ＭＧＷ１４４に接続され得る。ＭＳＣ１４６およびＭＧＷ１４４は、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃと従来の固定電話線通信デバイスとの間の通信を容易にするために、ＷＴＲＵ１０

２ａ、１０２ｂ、１０２ｃにＰＳＴＮ１０８などの回線交換網へのアクセスを提供することができる。

【００３８】

ＲＡＮ１０４におけるＲＮＣ１４２ａは、ＩｕＰＳインターフェースを介して、コアネットワーク１０６におけるＳＧＳＮ１４８にも接続され得る。ＳＧＳＮ１４８は、ＧＧＳＮ１５０に接続され得る。ＳＧＳＮ１４８およびＧＧＳＮ１５０は、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃとＩＰ対応デバイスとの間の通信を容易にするために、ＷＴＲＵ１０２ａ、１０２ｂ、１０２ｃにインターネット１１０などのパケット交換網へのアクセスを提供することができる。

【００３９】

上記に述べたように、コアネットワーク１０６をネットワーク１１２に接続することもでき、ネットワーク１１２は、他のサービスプロバイダによって所有されるおよび／または操作される他の有線またはワイヤレスネットワークを含むことができる。

【００４０】

本明細書に記載されるＷＴＲＵおよび／またはネットワークエンティティ上でポリシー管理機能を実行するとき、上記の通信システム、またはその部分を使用することができる。一例では、ＷＴＲＵおよび／または多重接続ネットワーク上での多重接続動作に対してポリシー管理機能を実行することができる。

【００４１】

本明細書に記載されるように、１つまたは複数の通信ネットワーク内で多重接続動作を利用可能とすることができる。例えば、セルラおよび／または非セルラ無線アクセス技術（ＲＡＴ）における多重接続動作を、モバイルオペレータの通信ネットワーク内で可能にすることができる。一例によれば、次世代ネットワーク（ＮＧＮ）／将来のネットワークに関する国際電気通信連合電気通信標準化部門（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ Ｕｎｉｏｎ Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ Ｓｅｃｔｏｒ）（ＩＴＵ－Ｔ ＳＧ１３１Ｑ９）は、モバイルオペレータの通信ネットワークの範囲内でセルラおよび／または非セルラＲＡＴにおける多重接続動作を可能にするための仕様（要件、アーキテクチャ、および／または技術）を策定中である。モバイルネットワークにおける様々な段階での多重接続アグリゲーション（ａｇｇｒｅｇａｔｉｏｎ）を実行することもできる。

【００４２】

図２は、モバイルネットワーク上でのいくつかのアグリゲーションシナリオを示す図である。この図は、モバイルネットワークの高レベルのプロトコルアーキテクチャを暗黙的に説明している（例えば、これはＯＳＩ７レイヤプロトコルアーキテクチャおよび／またはインターネットの４レイヤＴＣＰ／ＩＰアーキテクチャの次世代ネットワーク実装を示すことができる）。例えば、１つまたは複数のネットワーク内でおよび／または１つまたは複数のネットワークと関連してポリシー管理機能を実行するとき、図２に示すシナリオの１つまたは複数を実施することができる。

【００４３】

図２に示すシナリオを参照すると、シナリオＥは、２つの個別の無線アクセス技術（ＲＡＴ）、アクセス制御２６２およびアクセス制御２６４を介した、２つの個別のアプリケーション、アプリケーション２５４およびアプリケーション２５６の動作を示す。シナリオＥなどのシナリオのもとで動作しているネットワークは、アグリゲーションを実行することができない。例えば、ＷＴＲＵ２７０は、それぞれアクセスポイント２６６およびアクセスポイント２６８を介して、アクセス制御２６２およびアクセス制御２６４で通信することができる。アクセス制御２６２およびアクセス制御２６４は、サービス制御２５８およびサービス制御２６０を介して、それぞれアプリケーション２５４およびアプリケーション２５６と通信することができる。

【００４４】

シナリオＤはアグリゲーションをアプリケーション２３８に委ねることができ、アプリ

ケーション２３８は、例えば、モバイルネットワークの外側にあってもよい。アプリケーション２３８は、ネットワークとの一定の量のやり取りを有することができる。例えば、ＷＴＲＵ２５２は、それぞれアクセスポイント２４８およびアクセスポイント２５０を介して、アクセス制御２４４およびアクセス制御２４６で通信することができる。アクセス制御２４４およびアクセス制御２４６は、それぞれサービス制御２４０およびサービス制御２４２を介して、アプリケーション２３８と通信することができる。

【００４５】

シナリオＣは、ネットワークにおける接続アグリゲーションの一例を示す。シナリオＣに示すように、ＷＴＲＵ２３６は、それぞれアクセスポイント２３２およびアクセスポイント２３４を介して、アクセス制御２２８およびアクセス制御２３０で通信することができる。アクセス制御２２８およびアクセス制御２３０は、サービス制御２２６を介して、アプリケーション２２４と通信することができる。シナリオＣに示すように、それぞれの接続は専用のアクセス制御機構を保持してもよく、アグリゲーションはサービス制御２２６で行われてもよい。サービス制御２２６はアプリケーション２２４のサービスニーズに対処することができるので、シナリオＣは「サービスフロー」（例えば、ＩＰデータフロー）のレベルでほぼ動作することができる。シナリオＣは、例えば、独自のアクセス制御機能を保存することができる、異種の基本的な無線アクセス技術（ＲＡＴ）に対処することができる。シナリオＣにより、サービス制御２２６が少なくとも以下の機能、すなわち、例えば、より良いアグリゲートＱｏＳをもたらすために提供されるサービス品質（ＱｏＳ）機能などの、アプリケーションのための基本的なアクセス技術および／もしくはポリシー機能のアグリゲーションならびに／または異種アプリケーションデータトラフィックのポリシー固有のサブフロー（例えば、ＱｏＳ固有のサブフロー）への分割（サブフローは、次いで、それぞれのサブフローについて要求されたポリシー（例えば、ＱｏＳ）を満たすのに最も適した技術にアクセスするように適合される）について、これらの様々な技術をアグリゲートすることが可能になり得る。これの一例は、ハイパーテキスト転送プロトコル（ＨＴＴＰ）アクセスをデータ転送サブフロー、映像サブフローおよび音声サブフローに分割すること、ならびに／またはそれぞれのサブフローをそのサブフローを処理するのに最も適したアクセス手段にマップすることであってもよい。

【００４６】

シナリオＢは、例えば、協調マルチポイント送信（ＣｏＭＰ）などのマルチアンテナシステムの場合のように、アクセス制御２１６などの単一のアクセス技術が複数のアクセスポイントにまたがって使用される一例を示す。単一の技術の定義は、本明細書では「同じ系統の技術」として広く理解されてもよい。シナリオＢに示すように、ＷＴＲＵ２２２は、アクセスポイント２１８およびアクセスポイント２２０を介して、アクセス制御２１６で通信することができる。アクセス制御２１６は、サービス制御２１４を介して、アプリケーション２１２と通信することができる。シナリオＢは、複数のスペクトルにまたがる同じ系統の技術（例えば、認可されたセルラスペクトルにおけるセルラアクセス技術およびＴＶ帯域などライトリィライセンスド（ｌｉｇｈｔｌｙ　ｌｉｃｅｎｓｅｄ）スペクトルを対象とするその派生物）の動作に適用可能であってもよい。

【００４７】

シナリオＡは、多重アクセスアクセスポイントがネットワーク内で動作している一例を示す。例えば、ＷＴＲＵ２１０は、アクセスポイント２０８を介して、アクセス制御２０６と通信することができる。アクセス制御２０６は、サービス制御２０４を介して、アプリケーション２０２と通信することができる。

【００４８】

１つの例示的なアーキテクチャによれば、単一のポリシー制御エンティティは、サービス制御レイヤとアクセス制御レイヤとの間に配置されてもよい。しかし、このアーキテクチャには欠陥があり得る。構造上、ポリシー機能を、サービス制御レイヤとアクセス制御レイヤとの間に位置することができるレイヤとすることができない（例えば、データまたは情報がポリシーを通過することができない）。コントローラは、データ上でどのように

作用するかをサービス制御レイヤおよび／またはアクセス制御レイヤに伝えることができる。サービス制御（例えば、ＱｏＳ一致）およびアクセス制御（例えば、アクセス技術マッピング）によって行われる決定の性質は異なり得る。両方を同時に制御する単一の協同意思決定エンティティを有することは、不必要に複雑になる場合があるおよび／または例えば１つの多重接続シナリオをサポートするシステムなどのいくつかのシステムでは不要である場合がある。サービス制御およびアクセス制御のための専用のポリシーサービスをサポートするおよび／またはサービス制御とアクセス制御との間の緩やかな調整をもたらすことができる１つの手法を実施することができる。そのような手法は、ポリシー定義の設計、ならびに結果として生じるシステムの試験を簡易化することができる。例えばＱｏＳルール、コスト機能、および／またはアクセス権などの一連のポリシールールは、無料でおよび／または相反して同時に作用し得るいくつかの潜在的なポリシーエンジンを定義することができる。

【００４９】

これらのポリシールールは、プロトコルアーキテクチャに結び付けられない場合があるおよび／または場合によっては不適切である場合がある。例えば、アプリケーションポリシーで作用するように設計されたアグリゲーションポリシーは、アプリケーションポリシールールが利用可能でないことがあるので、アクセス制御エンティティで作用していない場合がある。ポリシーが「アグリゲーションポリシー」であるとき、図２に示すシナリオＣではアグリゲーションがサービス制御２２６によって行われ得るので、そのようなポリシーはシナリオＣでは適切であり得る。

【００５０】

どのようにポリシーエンティティがこのアーキテクチャに適合するかが本明細書に記載される。本明細書に記載されるポリシーエンティティを含むシステムを実施するとき、一連のポリシールールを定義することができるおよび／または一連のルールを例えばＱｏＳルールなどのポリシーに結び付けることができる。

【００５１】

図３は、図２の暗黙のアーキテクチャのいくつかのレイヤ、および高レベルな性質のレイヤのやり取りを示す。例えば、図３は、アプリケーションレイヤ３０２、サービス制御レイヤ３０６、アクセス制御レイヤ３１０、およびアクセスポイントレイヤ３１４を示す。アプリケーションレイヤ３０２は、サービス制御レイヤ３０６と通信することができ、ネットワークの内側および／または外側にあってもよい。アプリケーションレイヤ３０２は、例えば、アプリケーションＱｏＳ３０４を介して、サービス制御レイヤ３０６と通信することができる。アプリケーションレイヤ３０２は、データペイロードを送信するおよび／または受信するためのネットワークを使用して、ネットワークと通信することができる。

【００５２】

サービス制御レイヤ３０６は、アプリケーションレイヤ３０２および／またはアクセス制御レイヤ３１０と通信することができる。サービス制御レイヤ３０６は、アプリケーションレイヤ３０２とやり取りして、その通信ルール（例えば、ＱｏＳルールおよび／または他のポリシールール）を理解することができる。サービス制御レイヤ３０６は、アクセス制御３１０とやり取りして、通信ルール（例えば、ＱｏＳルールおよび／または他のポリシールール）が満たされていることを保証することができる。

【００５３】

アクセス制御レイヤ３１０は、アクセスポイントレイヤ３１４および／またはサービス制御レイヤ３０６と通信することができる。アクセス制御レイヤ３１０は、様々なアクセス方法（例えば、ＲＡＴ）を構成するおよび／または管理することに関与して、サービス制御レイヤ３０６によって要求されたポリシールール（例えば、ＱｏＳルールおよび／または他のポリシールール）が満たされていることを保証することができる。アクセス制御レイヤ３１０は、例えば、サービスＱｏＳ３０８を介して、サービス制御レイヤ３０６と通信することができる。アクセス制御レイヤ３１０は、例えば、アクセス構成３１２を介

して、アクセスポイントレイヤ３１４と通信することができる。
【００５４】
アクセスポイントレイヤ３１４は、ＷＴＲＵ３１６および／またはアクセス制御レイヤ３１０と通信することができるエンティティを含むことができる。アクセスポイントレイヤ３１４におけるエンティティは、物理媒体（例えば、基地局、Ｗｉ－Ｆｉ　ＡＰなど）によってＷＴＲＵ３１６と通信することができる。これらのエンティティは、アクセス制御レイヤ３１０によって作成されたＲＡＴ構成ルールを実施することができる。
【００５５】
上述したように、複数のアクセスポイントを有する多重接続ネットワークは、例えば、ＷＴＲＵなどのデバイスと通信することができる。多重接続ネットワークとデバイスとの間でそのような通信を実行する際、１つまたは複数のポリシーは、デバイスおよび／または多重接続ネットワークで実施することができる。複数のポリシーが存在するとき、デバイス上および／またはネットワーク上の様々なポリシー間で競合が存在する場合がある。例えば、１つまたは複数の異なるポリシーは、異なるステークホルダに対応し得る。ステークホルダは、例えば、１つまたは複数のネットワークならびに／またはアプリケーションサービスプロバイダ、デバイスの製造業者、デバイスユーザ、および／もしくは加入者を含むことができる。そのような競合を解決するために、デバイス上および／またはネットワーク上でポリシー調整エンティティを実施することができる。
【００５６】
図４は、多重接続ネットワークにおけるネットワーク通信に関して関連してもよいポリシーを調整する際に使用することができるエンティティを含む、例示的なシステムを示す。例えば、図４は、デバイス４００上の複数のポリシーを調整する際に使用するためのデバイスポリシー調整機能（ＰＣＦ）４１４を示す。ＰＣＦ４１４は、デバイス４００に含まれてもよい。デバイス４００は、例えば、多重接続ネットワーク４３４などのネットワークと通信する通信デバイスであってもよい。図４は、デバイス４００上および／または多重接続ネットワーク４３４上の複数のポリシーを調整する際に使用するためのネットワークポリシー調整機能（ＮＰＣＦ）４３２も示す。ＮＰＣＦ４３２は、例えば、多重接続ネットワーク４３４に含まれてもよい。
【００５７】
ＰＣＦ４１４に関して、デバイス４００は、通信を実行するときに関連するポリシーを調整するためのＰＣＦ４１４を含む。ＰＣＦ４１４は、デバイス４００の異なるステークホルダのポリシーを調整する機能を実行することができる。例えば、それぞれのステークホルダは、異なるアプリケーション、スマートカード、ならびに／またはデバイス４００にインストールされたおよび／もしくはデバイス４００と関連するＵＩＣＣと関連してもよい。ポリシーは、１つまたは複数のステークホルダの代わりに調整され得る。ＰＣＦ４１４は、デバイス４００の効率的な動作のために、多くの機能にまたがってもよい。例えば、セキュリティポリシー処理、通信ＱｏＳ処理、複数の通信リンクの処理、または他のポリシーパラメータなどのポリシー調整で使用するための１つまたは複数のパラメータがＰＣＦ４１４に含まれ得る。
【００５８】
デバイス４００は、ポリシーのインストール、構成、更新、調整などを安全に実行するための信頼できる安全な実行環境を提供することができる。例えば、デバイス４００は、信頼できる環境（ＴｒＥ：Ｔｒｕｓｔｅｄ　Ｅｎｖｉｒｏｎｍｅｎｔ）４０２を含むことができる。ＴｒＥ４０２は、機密機能の実行および機密データの記憶のための信頼できる環境を提供する論理エンティティを指してもよい。ＴｒＥ４０２内で機能を実行することによって生成されたデータは、無許可の外部エンティティに知られないようにすることができる。例えば、ＴｒＥ４０２は、外部エンティティに対するデータの無許可の開示を防ぐように構成され得る。ＴｒＥ４０２は、例えば、デバイス整合性チェックおよび／またはデバイス検証を実行するために使用することができる機密機能（秘密鍵の記憶、これらの秘密鍵を使用した暗号化計算の提供、およびセキュリティポリシーの実行など）を実行

することができる。ＴｒＥ４０２を、改ざんすることができない不変のハードウェアの信頼のルートに固定することができる。例えば、ＴｒＥ４０２は、デバイス４００のスレーブであってもよい。例えば、ＴｒＥ４０２は、例えば、ＧＳＭデバイスで使用することができるものなどのＳＩＭカードを含むことができる。ＴｒＥ４０２の実施は、例えば、アプリケーションおよび／または要求されるセキュリティのレベルに依存し得る。

【００５９】

ＴｒＥ４０２は、ＰＣＦ４１４を実行することができる安全な環境であってもよい。デバイス４００のＰＣＦ４１４は、異なるステークホルダからのポリシーを実行することができる。ＰＣＦ４１４は、複数のステークホルダからのポリシー間の競合を解決することもできる。ＰＣＦ４１４の構成要素は、ファームウェア、ハードウェア、および／またはソフトウェアにあってもよい。高レベルのＰＣＦ４１４機能を変更する許可は、ルート権限に属することができる。この権限の委任は、信頼できる環境（ＴｒＥ）４０２によって保証された信頼の連鎖によって達成され得る。それぞれの非ルートステークホルダが一部の結果には優先し得るが、他の結果には優先し得ないように、特定のＰＣＦ４１４解決機能における優先順位付けを、相互に排他的なおよび／または相互に特権的な（例えば、同等であるが異なる）方法で、ステークホルダに割り当てることができる。

【００６０】

ＰＣＦ４１４は、手順を開始することができるおよび／または動的な条件に対応することができる。ＰＣＦ４１４は、入力における変更がアクションまたはアクションのセットにおける変更となり得るように、ステータスおよび／または測定値をリアルタイムで受信することができる。アクションまたはアクションのセットにおけるそのような変更は、例えば、入力における変更の直後に、または制御された時間遅延を伴って行われ得る。

【００６１】

ＰＣＦ４１４は、ＮＰＣＦ４３２のプロキシとして作用することができる。例えば、デバイス４００上のＰＣＦ４１４は、ＮＰＣＦ４３２によって実施されたポリシーに対する「ピア」であるポリシーを実施することができる。これらのピアポリシーは、ＮＰＣＦ４３２によって実施されたマスターポリシーから生成されたサブポリシーであってもよい。ＮＰＣＦ４３２は、計算集約的な動作を処理することができるおよび／またはデバイス４００のＰＣＦ４１４機能を最適化するための管理特権を有することができる。ＮＰＣＦ４３２は、ステークホルダのうちの１つの代わりにサービスを提供するおよび／またはＰＣＦ４１４のある側面を制御することができる。場合によっては、ＰＣＦ４１４は、例えば、ネットワークにおけるその位置により、変化する条件を検出するおよび／またはそれに応じてネットワーク規模のポリシーを施行するのにより適していることがある。ＮＰＣＦ４３２は、ＮＰＣＦ４３２が受信する入力に基づいて自立的に作用することができる、またはＮＰＣＦ４３２は、ネットワーク側でのいくつかの命令および／または決定といくつかの局所的に行われた決定との間で半自立的に作用することができる。あるいは、ＮＰＣＦ４３２は、ネットワークからの命令および／または決定のみに作用することができる。

【００６２】

セキュリティポリシー処理では、ＰＣＦ４１４は、デバイス整合性検証が失敗した場合にどのように進めるかについての命令を示唆することができる。ポリシーベースの施行の例としては、デバイス検証を事前共有秘密ベースのクライアント認証に結合すること、デバイス検証を証明書ベースのデバイス認証に結合すること、および／またはデバイス整合性検証を他のデバイス機能に結合することを含む機構を挙げることができるが、これらに限定されない。セキュリティポリシーは、１つまたは複数のセキュリティパラメータを示すことができる。例えば、セキュリティポリシーは、使用されるべきアルゴリズムスイート、使用されるべき鍵の強度（例えば、長さ）、使用されるべき複数のセキュリティプロトコル、使用されるべき１つのセキュリティプロトコル、保持ポリシー（例えば、持続時間、鍵の有効性および／または鍵の存続期間を検証するエンティティ、例外条項）、暗号鍵の非推奨（ｄｅｐｒｅｃａｔｉｏｎ）、削除、および／または更新を示すことができる。例えば、ステークホルダ、および／またはステークホルダを対象としたサービスもしく

はアプリケーションに対して、セキュリティポリシーを示すことができる。異なるステークホルダ、および／または異なるステークホルダを対象とした異なるサービスもしくはアプリケーションに対して、異なるセキュリティポリシーを示すことができる。一例によれば、ＱｏＳが複数の接続のそれぞれの通信に提供されたセキュリティの強度の観点から定義される場合、セキュリティ固有のＱｏＳポリシーが適用され得る。

【００６３】

ＰＣＦ４１４は、サービスを利用するために複数のステークホルダによって定められたルールを考慮することができる。例えば、ＰＣＦ４１４は、その調整機能を用いてステークホルダポリシー間の競合を解決することができる。加入者は、施行ルールを伴う加入者ポリシー（ＳＰ）４０８を有してもよい。例えば、ＳＰ４０８は、ビジネス電話に対する最小のセキュリティ強度（例えば、暗号強度）および利用可能な最も安い電話サービスの選好を要求することができる。ＰＣＦ４１４はデバイスを起動して、例えばサービス接続Ａのセキュリティアソシエーション（ＳＡ＿Ａ）４１６などの、最も安いサービスのセキュリティアソシエーションを交渉することができる。デバイス４００は、例えば、接続Ａ４２０を介して、アクセスポイントＡ４２４でネットワーク４３４との接続を確立するよう試みることができる。ＳＰ４０８によって要求されたセキュリティのレベルで接続を達成することができない場合、この情報をＰＣＦ４１４にフィードバックすることができる。ＰＣＦ４１４は、ステータスを組み込むおよび／または例えば、サービス接続Ｂのセキュリティアソシエーション（ＳＡ＿Ｂ）４１８などの別のオペレータを高いコストで使用して第２の安全な呼を開始することができる。次いで、デバイス４００は、例えば、接続Ｂ４２２を介して、アクセスポイントＢ４２６で多重接続ネットワーク４３４との接続を確立することができる。示すように、ＳＰ４０８によって要求されたセキュリティのレベルで、デバイス４００と多重接続ネットワーク４３４との間で接続Ｂ４２２を確立することができる。

【００６４】

アクセスポイントＡ４２４およびアクセスポイントＢ４２６は、多重接続サービス制御機能４３０と通信することができる。多重接続サービス制御機能４３０は、加入者情報を認証するための加入者認証機能４２８を含むことができる。ＮＰＣＦ４３２は、多重接続サービス制御機能４３０と関連するポリシーを調整することができる。

【００６５】

別の例によれば、加入者は、データファイルを企業ネットワークからワイヤレスデバイスに転送することを望む場合がある。加入者は、伝送速度を達成するために複数のサービスを同時に使用して、多重接続通信を要求することができる。ＰＣＦ４１４は、同等のセキュリティ鍵強度の使用を施行して、様々なステークホルダ（例えば、企業）ポリシーに従って、複数の接続の間で転送されるデータの最小のセキュリティレベルを維持することができる。この場合、複数のチャネルにもかかわらず、宣伝通りに伝送速度が達成されない場合、加入者は、おそらくはＰＣＦ４１４によって、ＴｒＥ４０２内の信頼できるエンティティによって、および／またはＴｒＥ４０２自体によって署名された、これの記録を取っておきたいと思うことがある。別の例では、加入者は高速度が達成されたことを否定することがあり、サービスプロバイダは、例えば、ＰＣＦ４１４によって、または他の考えられる署名エンティティによって署名されてもよい、これの写しを求めることがある。したがって、ＰＣＦ４１４は、サービスの拒絶を防ぐための署名機能を有することができる。ＰＣＦ４１４の整合性チェックが失敗した場合、ＴｒＥ４０２はＰＣＦ４１４署名鍵へのアクセスを防ぐことができる。あるいは、ＴｒＥ４０２内の別の信頼できるエンティティが、ＰＣＦ４１４によって生成されたデータに署名することができる。ＰＣＦ４１４の整合性チェックが失敗した際、ＴｒＥ４０２は、ＰＣＦ４１４によって生成されたデータに署名するその他の信頼できるエンティティによって保持された署名鍵へのアクセスを防ぐことができる。

【００６６】

ＰＣＦ４１４は、デバイスの異なるステークホルダに対する鍵の生成、導出、および／

またはブートストラッピングに関するポリシーを調整することもできる。例えば、図４を参照すると、高レベルの鍵は、加入者ステークホルダとプライマリオペレータＡとの間の共有秘密によって生成され得る。ＳＰ４０８、オペレータＡポリシー（ＯＰ＿Ａ）４１０、および／またはオペレータＢポリシー（ＯＰ＿Ｂ）４１２に応じて、デバイス４００とオペレータＢとの間で使用することができるさらなる子レベルの共有鍵を、加入者とオペレータＡとの間で生成された鍵から導出することができる。これらの鍵を生成するために、ブートストラップ機構を使用することができる。

【００６７】

別の実施形態によれば、デバイス４００のＰＣＦ４１４は、デバイス４００の統合されたＴｒＥ４０２内ではなく、デバイス４００にプラグ接続されたまたは接続されたエンティティまたはモジュール内で実施することができる。エンティティまたはモジュールは、デバイス４００に取付け可能および／またはデバイス４００から取外し可能であってもよい。そのようなエンティティの一例は、高度なバージョンのスマートカードまたはＵＩＣＣであってもよい。

【００６８】

デバイス４００における特定の構成要素の整合性は、デバイス検証機能（ＤＶＦ）４０４によって保護され得る。ＤＶＦ４０４は、ＴｒＥ４０２の内部に含まれ得るおよび／またはデバイス４００の構成要素の整合性が保たれているかどうかを検証するためのデバイス整合性チェックを実行することができる。例えば、ＤＶＦ４０４は、デバイス４００の構成要素の整合性をチェックすることができる。ＤＶＦ４０４は、例えば、デバイス検証認証情報４０６を使用して、デバイス整合性チェックを実行することができる。ネットワークおよび／またはデバイス自体によって、デバイス検証のために整合性情報を使用することができる。例えば、デバイス４００の構成要素の整合性がチェックされると、ＤＶＦ４０４は、検証目的で整合性データを他のエンティティに転送する前に、ＴｒＥ４０２の秘密鍵を使用して、整合性データおよび／または任意の追加の関連した補足データに署名することができる。

【００６９】

ＤＶＦ４０４は、適切な権限を有するステークホルダは、その権限の制御下においてＰＣＦ４１４機能を変更することができるという保証を提供することができる。ＤＶＦ４０４によって提供される保証は、デバイス検証認証情報４０６を含むことができる。高レベルのＰＣＦ４１４機能は、管理ＰＣＦ権限下にあってもよい。管理ＰＣＦ権限は、例えば、加入者、オペレータ、アプリケーションサービスプロバイダ、および／またはデバイス製造業者であってもよい。管理ＰＣＦは、製造業者によって構成されてもよく、または例えばオペレータ、アプリケーションサービスプロバイダ、または加入者などの場合は後で構成されてもよい。ＴｒＥ４０２は、ＰＣＦ４１４機能に対する無許可の更新および／または変更を防ぐおよび／または例えば、ポリシー機能を互いに切り離すことを含め、デバイス上のステークホルダポリシーを保護することができる。

【００７０】

ＴｒＥ４０２は、ＤＶＦ４０４を使用して、デバイス上のポリシーを保護することができる。例えば、ＴｒＥ４０２は、ＤＶＦ４０４を使用して、１つまたは複数のアプリケーション、機能、および／または例えば、デバイス検証認証情報４０６などのＴｒＥ４０２内に保持されたデータに対するアクセスを制御する（ｇａｔｅ）ことができる「ゲーティング」手順を実行することができる。ゲーティング手順は、デバイス整合性検証結果のステータスに依存し得る。ゲーティング手順は「カスケード」することができる。例えば、ＤＶＦ４０４は、１つの機能またはアプリケーションに対するアクセスを制御することができるが、その機能またはアプリケーションは、例えば、別の機能、アプリケーション、またはデータに対するアクセスを制御することができる。ＤＶＦ４０４は、複数の手順またはデータを制御することができ、複数の手順またはデータの一部または全ては、因果関係または対応関係を有することができる。

【００７１】

図５は、ＮＰＣＦによって実行することができるポリシー調整機能を示す。図５は、存在しているポリシーエンティティを示すシステム／プロトコルアーキテクチャを示す。図５に示す機能アーキテクチャは、ネットワークエンティティによって果たされる様々な役割を示すためのコアネットワークの境界を表している。任意の所与のシステムでは、示されたエンティティの一部または全てが存在し得る。例えば、１つまたは複数の示されたエンティティの存在は、図２に記載されたシナリオのうちのどれが使用可能であるかに依存し得る。

【００７２】

ネットワークポリシー調整機能（ＮＰＣＦ）５０６は、コア多重接続ネットワーク５０１における機能エンティティであってもよい。ＮＰＣＦ５０６は、多重接続制御機能を有することができる。ＮＰＣＦ５０６は、多重接続登録エンティティから接続情報を受信するおよび／またはＷＴＲＵ毎にオペレータポリシー記憶エンティティからのオペレータポリシーを要求することができる。図５に示すように、ＮＰＣＦ５０６は、アプリケーションポリシーエンティティ５０２と通信することができ、アプリケーションポリシーエンティティ５０２は、例えば、多重接続アプリケーションポリシーエンティティであってもよい。アプリケーションポリシーエンティティ５０２は、アプリケーションレイヤ３０２に含まれ得るおよび／またはアプリケーションポリシーインターフェース５０４を介してアプリケーションレイヤ３０２と関連し得る。ＷＴＲＵ３１６に対するＩＰフローがあるとき、ＮＰＣＦ５０６はポリシーを実行して、そのＩＰフローを多重接続のなかで最も適切なネットワークにルーティングすることができる。

【００７３】

ＮＰＣＦ５０６は、コア多重接続ネットワーク５０１における様々なポリシーエンティティの動作を調整することができる。複数のポリシーが存在するとき、ＮＰＣＦ５０６は、様々なポリシー間の競合を解決することができる。ＮＰＣＦ５０６の適用可能性は、長期間にわたることができる、すなわち、特定のポリシーを同時に使用することを防ぐとともに、より多くの当座のポリシー実行を個々のポリシーエンティティに委ねることができる。

【００７４】

ＮＰＣＦ５０６は、サービス転送ポリシー機能を実施することができる。ＮＰＣＦ５０６は、１つまたは複数のレイヤにわたって一緒に実行されるべき機能を含むことができる。したがって、ＮＰＣＦ５０６は、例えば、図２に示すように、多重接続登録機能および／または多重接続制御機能を含むことができる。

【００７５】

ＮＰＣＦ５０６は、ＷＴＲＵ３１６とインターフェースすることができる。このインターフェースは、図５におけるＮＰＣＦ５０６とＷＴＲＵ３１６との間の点線５１４によって示される。ＷＴＲＵ３１６は、ネットワークにおけるポリシーに対する「ピア」であるポリシーを実施することができる。例えば、これらのピアポリシーは、サービス品質（ＱｏＳ）ポリシーエンティティ５０８、アクセスポリシーエンティティ５１０におけるおよび／またはＮＰＣＦ５０６自体内のマスターポリシーから生成されたサブポリシーであってもよい。ピアポリシーは、例えば、ＱｏＳ機能、コスト機能、データへのアクセス権、または他のポリシー機能を含むことができる。サブポリシーをＷＴＲＵ３１６に伝えることができ、次いで、ＷＴＲＵ３１６はそのサブポリシーに従うことができる。マスターポリシーは、ＷＴＲＵ３１６の挙動、コア多重接続ネットワーク５０１の状態、および／または無線インターフェースの状態に基づいて変更され得る複数のＷＴＲＵ３１６サブポリシーを含んでもよい。

【００７６】

図５の機能アーキテクチャは、図２に示すシナリオＤの機能アーキテクチャを認識することができる。アプリケーション３０２は、多重接続の決定を行うことができ、アプリケーションポリシーエンティティ５０２を所有することができる。アプリケーションレイヤ３０２およびアプリケーションポリシーエンティティ５０２は、破線５１６で示すように

、コア多重接続ネットワーク５０１の外部にあってもよい。コア多重接続ネットワーク５０１は、アプリケーションポリシーエンティティ５０２へのインターフェースを所有することができる。したがって、アプリケーションポリシーインターフェース５０４は、コア多重接続ネットワーク５０１とアプリケーションレイヤ３０２との間で分割された、コア多重接続ネットワーク５０１におけるＮＰＣＦ５０６とアプリケーションポリシーエンティティ５０２との間のインターフェースを提供することができる。

【００７７】

アプリケーションポリシーインターフェース５０４は、アプリケーションポリシーエンティティ５０２およびコア多重接続ネットワーク５０１がアグリゲーションおよび／またはポリシー競合回避に使用されるポリシーの性質に関する情報を交換するための手段を提供することができる。例えば、アプリケーション３０２が、特定のデータサブフローを特定の接続に配置するように要求することができるポリシーを適用した場合、ＮＰＣＦ５０６は、アプリケーションポリシーインターフェース５０４を介してこのポリシーを伝えて、例えば、別のアクセスポイントの取得などの別の多重接続動作がデータを異なる接続に移動しないことを保証することができる。

【００７８】

図５に示すように、ＱｏＳポリシーエンティティ５０８および／またはアクセスポリシーエンティティ５１０をポリシー記憶機能５１２に埋め込むことができる。ポリシー記憶機能５１２は、２つ以上の記憶機能を実行することができる。ポリシー記憶機能５１２は、例えば、ＱｏＳポリシーなどのいくつかのポリシー間でポリシー決定および／または比較を実行して、ポリシー間の競合を回避することができる。

【００７９】

サービス制御レイヤ３０６は、アプリケーション３０２のポリシーのニーズを利用可能なアクセスポリシーに適合させることによって、アプリケーション３０２のポリシーのニーズを満たすことができる。例えば、そのようなポリシーは、ＱｏＳポリシーを含むことができる。ＱｏＳポリシーエンティティ５０８は、サービス制御レイヤ３０６で含まれてもよい。例えば、図２に示すシナリオＣでは、多重接続の決定をサービス制御レイヤ３０６によって行うことができ、サービス制御レイヤ３０６はアプリケーションのＱｏＳニーズによって影響され得る。ＱｏＳポリシーエンティティ５０８は例示的なものであり、サービス制御レイヤ３０６によって使用することができる任意のポリシーエンティティを代表するものであってもよい。

【００８０】

図５に示すように、ＱｏＳポリシーエンティティ５０８は、ＱｏＳポリシーを実施することができる。さらに、ＱｏＳポリシーエンティティ５０８は、図２に示すように、多重接続シナリオＣが、サービス転送のために多重接続の最初および／または最後の混在した対象を使用するケースを包含する場合、サービス転送ポリシーを実行することができる。アクセスの変更および／または更新は、アクセス制御エンティティとサービス制御エンティティとの間の多重接続を対象とすることができる。

【００８１】

シナリオＢでは、図２に示すように、多重接続アクセス制御機能２１６によって多重接続を管理することができ、多重接続アクセス制御機能２１６は、同種の一連のアクセス技術を利用することができるアクセスポイント２１８およびアクセスポイント２２０などの一連のアクセスポイントにまたがって接続を管理することができる。図５に示すように、アクセスポリシーエンティティ５１０は、様々なアクセスポイントの使用を提供することができる。

【００８２】

アクセスポリシーエンティティ５１０は、アクセスネットワーク選択ポリシーを実施することができる。アクセスポリシーエンティティ５１０は、図２に示すように、多重接続シナリオＢがサービス転送のために多重接続の最初および最後の混在した対象を使用するケースを包含し得る場合、サービス転送ポリシーを実行することができる。アクセスの変

更は、アクセスポイントエンティティとアクセス制御エンティティとの間の多重接続を対象とすることができる。

【００８３】

いくつかのタイプのポリシー要求を以下に記載する。図２に示す５つのモデル、シナリオＡ、Ｂ、Ｃ、Ｄ、およびＥは、関与する無線アクセス技術、アクセス制御、サービス制御、および／またはアプリケーションのニーズに従って、異なるポリシー機能を伴うことができる。

【００８４】

シナリオに関する手法について、異なるポリシー要求を以下に記載する。

【００８５】

例えば、図２に示すようにシナリオＢをサポートするネットワークは、図５に示すアクセスポリシーエンティティ５１０を含むことができる。アクセスポリシーエンティティ５１０は、例えば、複数の利用可能なアクセスポイントのアグリゲーションによって、アクセス技術によってポリシー要求（例えば、ＱｏＳ要求）を満たすためのポリシーをサポートすることができる。アクセスポリシーは、アクセス方法がどのように構成されるかを制御することができる。例えば、セルラネットワークでは、アクセスポリシーはＱｏＳクラスを含むことができ、Ｗｉ－Ｆｉネットワークでは、アクセスポリシーは、トラフィック優先順位を含むことができる。アクセスポリシーは、使用されるべきスペクトル、使用されるべきアクセスポイント、アグリゲートされるべきチャネルの数、および／またはピアツーピア接続を使用することができるかどうか（例えば、Ｂｌｕｅｔｏｏｔｈ技術を介して別のデバイスにテザリングすることによって、インターネットにアクセスする）を含むこともできる。

【００８６】

別の例によれば、図２に示すようにシナリオＣをサポートするネットワークは、図５に示すＱｏＳポリシーエンティティ５０８を含むことができる。図５に示すように、ＱｏＳポリシーエンティティ５０８は、例えば、様々な利用可能なアクセス技術によって提供されたＱｏＳを適切に使用することによって、アプリケーションＱｏＳを満たすためのポリシーをサポートすることができる。ＱｏＳポリシーは、高レベルの問題に対処することができる。例えば、ＱｏＳポリシーは、使用されるべき１つまたは複数のアクセスネットワーク、どのように接続がセットアップされ得るか（例えば、どのプロトコルおよび／またはストリーミング方法を使用することができるか）、および／または接続の優先順位を示すことができる。ＱｏＳポリシーは、例えば、ＱｏＳの観点からの遅延、スループット、忠実度、コストなどの重要度を示すこともできる。

【００８７】

別の例によれば、図２に示すシナリオＤをサポートするネットワークは、図５に示すアプリケーションポリシーインターフェース５０４を含むことができる。図５に示すように、アプリケーションポリシーインターフェース５０４は、アプリケーションポリシーエンティティ５０２へのインターフェースを提供することができ、アプリケーションポリシーエンティティ５０２は、例えば、多重接続ポリシーエンティティであってもよい。アプリケーションポリシーインターフェース５０４は、詳細をアプリケーションレイヤ３０２に提供して、例えば、シナリオＣにおけるネットワーク上で行われるように、シナリオＤなどの構成において同じまたは類似したＱｏＳレベルの決定を行うことができる。

【００８８】

いくつかのポリシーは、図２に示す５つシナリオの１つまたは複数と共通であってもよい。例えば、ネットワークは、サービス制御レイヤ３０６を介してポリシーをＷＴＲＵ３１６に伝えることができてもよい。例えば、コア多重接続ネットワーク５０１などの多重接続ネットワークは、ネットワーク内に存在する複数のポリシーエンティティの調整のためのＮＰＣＦ５０６を含むことができる。

【００８９】

例えば、２つの独立したエンティティとして、ＰＣＦおよびＮＰＣＦを本明細書に記載

し、図４および５に示すことができるが、ポリシー調整をデバイスＰＣＦ、ＮＰＣＦ上で実行するか、デバイスＰＣＦおよびＮＰＣＦによって共有することができる。したがって、デバイスＰＣＦによって実行されるものとして本明細書に記載される任意の機能をＮＰＣＦによって実行することができ、ＮＰＣＦによって実行されるものとして本明細書に記載される任意の機能をデバイスＰＣＦによって実行することができ、および／または本明細書に記載される任意のポリシー調整機能をデバイスＰＣＦおよびＮＰＣＦによって一緒に実行することができる。

【００９０】

上記の記載に基づいて、例えば、ＱｏＳ管理要求などの一連のポリシー管理要求について以下に記載する。

【００９１】

多重接続ネットワークでは、ＷＴＲＵおよびネットワークは、アプリケーションおよび／または関連するＱｏＳに提供されたいくつかの同時アクセスによって作成されたやり取りを認識することができる。組合せまたは結果として生じたＱｏＳは、特定のサービスに関与する組み合わされたＱｏＳを表し得る。

【００９２】

以下に提供される記載は、多重接続ＱｏＳ要求のいくつかを含む。

【００９３】

例えば、シナリオＡ、Ｂ、およびＣでは、図２に示すように、サービス制御レイヤは、個々のアクセス技術自体によって提供されたＱｏＳと少なくとも同程度に良い結果として生じたＱｏＳをアプリケーションに提供することができる。

【００９４】

別の例によれば、シナリオＡおよびＢでは、図２に示すように、アクセス制御レイヤは、任意の個々のアクセスリンク自体によって提供されたＱｏＳと少なくとも同程度に良いアクセス技術ＱｏＳをサービス制御に提供することができる。

【００９５】

別の例によれば、シナリオＡでは、図２に示すように、アクセスポイント２０８は、その制御下にある任意の個々のアクセスリンクのＱｏＳと少なくとも同程度に良いＱｏＳをアクセス制御２０６に提供することができる。

【００９６】

図６は、本明細書に記載されるポリシー調整を実行する際に実施することができる例示的なワイヤレス通信システム６００を示す。ワイヤレス通信システム６００は、複数のＷＴＲＵ６１０、ノードＢ６２０、コントローリング無線ネットワークコントローラ（ＣＲＮＣ）６３０、サービング無線ネットワークコントローラ（ＳＲＮＣ）６４０、およびコアネットワーク６５０を含むことができる。ノードＢ６２０およびＣＲＮＣ６３０を総称してＵＴＲＡＮと呼ぶことができる。

【００９７】

図６に示すように、ＷＴＲＵ６１０はノードＢ６２０と通信しており、ノードＢ６２０はＣＲＮＣ６３０およびＳＲＮＣ６４０と通信している。３つのＷＴＲＵ６１０、１つのノードＢ６２０、１つのＣＲＮＣ６３０、および１つのＳＲＮＣ６４０が図６に示されているが、ワイヤレスおよび／または有線デバイスの任意の組合せがワイヤレス通信システム６００に含まれ得る。

【００９８】

図７は、図６のワイヤレス通信システム６００のＷＴＲＵ７１０およびノードＢ７２０の機能ブロック図７００である。図７に示すように、ＷＴＲＵ７１０はノードＢ７２０と通信しており、ＷＴＲＵ７１０とノードＢ７２０の両方は、例えば、マルチＲＡＴ　ＮＧＮアーキテクチャなどにおいて、多重接続通信に対するＱｏＳおよびポリシー管理のための方法を実行するように構成される。

【００９９】

ＷＴＲＵに見出され得る構成要素に加えて、ＷＴＲＵ７１０は、プロセッサ７１５、受

信機７１６、送信機７１７、メモリ７１８、およびアンテナ７１９を含む。メモリ７１８は、オペレーティングシステム、アプリケーションなどを含むソフトウェアを記憶することができる。プロセッサ７１５は、単独でまたはソフトウェアと関連して、例えば、マルチＲＡＴ　ＮＧＮアーキテクチャなどにおいて、多重接続通信に対するＱｏＳおよび／またはポリシー管理のための方法を実行することができる。受信機７１６および送信機７１７は、プロセッサ７１５と通信している。アンテナ７１９は、受信機７１６と送信機７１７の両方と通信して、ワイヤレスデータの送信および受信を容易にする。

【０１００】

ノードＢに見出され得る構成要素に加えて、ノードＢ７２０は、プロセッサ７２５、受信機７２６、送信機７２７、メモリ７２８、およびアンテナ７２９を含む。プロセッサ７２５は、例えば、マルチＲＡＴ　ＮＧＮアーキテクチャなどにおいて、多重接続通信に対するＱｏＳおよび／またはポリシー管理のための方法を実行するように構成される。受信機７２６および送信機７２７は、プロセッサ７２５と通信している。アンテナ７２９は、受信機７２６と送信機７２７の両方と通信して、ワイヤレスデータの送信および／または受信を容易にする。

【０１０１】

適切なプロセッサとしては、例として、汎用プロセッサ、特殊用途プロセッサ、従来のプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、複数のマイクロプロセッサ、ＤＳＰコアに関連した１つまたは複数のマイクロプロセッサ、コントローラ、マイクロコントローラ、特定用途向け集積回路（ＡＳＩＣ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）回路、任意の他のタイプの集積回路（ＩＣ）、および／または状態機械を挙げることができる。

【０１０２】

ソフトウェアに関連したプロセッサを使用して、ワイヤレス送信／受信ユニット（ＷＴＲＵ）、ユーザ機器（ＵＥ）、端末、基地局、無線ネットワークコントローラ（ＲＮＣ）、または任意のホストコンピュータで使用するための無線周波数トランシーバを実施することができる。ＷＴＲＵは、カメラ、ビデオカメラモジュール、ビデオ電話、スピーカフォン、振動デバイス、スピーカ、マイクロフォン、テレビジョントランシーバ、ハンズフリーヘッドセット、キーボード、Ｂｌｕｅｔｏｏｔｈモジュール、周波数変調（ＦＭ）無線ユニット、液晶ディスプレイ（ＬＣＤ）ディスプレイユニット、有機発光ダイオード（ＯＬＥＤ）ディスプレイユニット、デジタル音楽プレーヤ、メディアプレーヤ、ビデオゲームプレーヤモジュール、インターネットブラウザ、および／または任意のワイヤレスローカルエリアネットワーク（ＷＬＡＮ）もしくは超広帯域（ＵＷＢ）モジュールなどのハードウェアおよび／またはソフトウェアで実施されるモジュールとともに使用され得る。

【０１０３】

一実施形態によれば、本明細書に記載されるポリシー調整のためのシステム、方法、および装置を、ＴＶホワイトスペース（ＴＶＷＳ）を使用するシステムにおいて実施することができる。例えば、独立して操作されるＴＶ帯域デバイス（ＴＶＢＤ）ネットワークおよび異なるＴＶ帯域デバイスの間の共存をサポートするシステムにおけるセキュリティ手順の調整および／または実行のためのシステム、方法および装置が記載される。例えば、ＩＥＥＥ８０２．１９規格は、異なるまたは独立して操作されるＴＶＢＤネットワークおよび異なるＴＶＢＤの間の共存のための無線技術に依存しない方法を規定している。システムへの新規参加者は、８０２．１９システムを発見するおよび／または参加要求を送ることができる。次いで、認証手順とともにアクセス交渉を実行することができる。システムは、コミットされ得るシステムポリシーを提供することができる。新規参加者は、例えば、リストに供給され得るシステムポリシーの少なくとも一部をコミットすることができる。システムポリシーは更新されてもよい。新規参加者は、システムポリシーまたは更新されたシステムポリシーの少なくとも一部をコミット解除することができる。認証手順について、新規参加者は、ＴｒＥを使用して信頼状態の局所的な整合性チェックを実行して、プラットフォーム整合性の証明または測定値を生成し、信頼の検証のために測定または

証明データを送ることができる。

【０１０４】

一例によれば、異なるまたは独立して操作されるＴＶＢＤネットワークおよび異なるＴＶＢＤの間の共存のための無線技術に依存しない方法を指定することができる。例えば、ＩＥＥＥ８０２．１９規格、または他の類似の規格は、そのような無線技術に依存しない方法を指定することができる。８０２．１９規格は、ＩＥＥＥ８０２ワイヤレス規格のファミリーを使用可能にして、異なるまたは独立して操作されるＴＶＢＤネットワークおよび異なるＴＶＢＤの間に規格共存方法を提供することによって、ＴＶホワイトスペース（ＴＶＷＳ）を効率的に使用することができる。８０２．１９規格は、ＩＥＥＥ８０２ネットワークおよびデバイスの共存に対処することができ、非ＩＥＥＥ８０２ネットワークおよびＴＶＢＤにも有用であり得る。

【０１０５】

コアネットワーク１０６は、図１Ａおよび１Ｃに示すように、共存発見および情報サーバ（ＣＤＩＳ）、共存マネージャ、ＴＶＷＳデータベースなどを含むが、これらに限定されない、ＩＥＥＥ８０２．１９をサポートするネットワークエンティティを含むことができる。ＣＤＩＳは、ＴＶＷＳ共存に関する情報を収集することができ、共存に関する情報を提供し、共存マネージャの発見をサポートすることができるエンティティである。共存マネージャは、共存の決定を行うおよび／または共存要求およびコマンドならびに制御情報を生成し、提供するエンティティであってもよい。ＴＶＷＳ　ＤＢは、プライマリユーザによって占有されるチャネルのリストを提供することができる。

【０１０６】

（例えば、ＩＥＥＥ８０２．１９システムにおける）セキュリティ手順の実施形態を以下に開示する。一実施形態によれば、ＷＴＲＵおよび／またはネットワーク（例えば、ＴＶ帯域デバイスおよび／またはＴＶ帯域デバイスネットワーク）ならびに８０２．１９システムは、発見、アクセス制御、ポリシー交渉、および／またはポリシー施行手順を実行することができる。動作中に実行される手順は、ポリシー更新および／または変更ならびに他の共存機構（例えば、チャネル選択、電力制御、時分割など）を含むことができる。本明細書に記載される実施形態は、例えば、ＩＥＥＥ８０２．１９システムを使用することができるが、実施形態は、異なるまたは独立して操作されるＴＶ帯域デバイス（ＴＶＢＤ）ネットワークおよび異なるＴＶＢＤの間の共存をサポートするための任意の他のシステムに適用され得る。

【０１０７】

８０２．１９システムは、全ての人が参加しなければならないわけではない、または（多くの人が招待され得るが）全ての人が参加することを許可され得るわけではないクラブである。クラブのルールは多くてもよいが、任意選択であってもよい。このクラブのメンバーではないエンティティが周囲に存在し得る。このクラブに参加するために、新規参加者は発見および／またはアクセス制御手順を実行することができる。新規参加者は、ルール（共存ポリシー）のリストを取得するおよび／または新規参加者がどのルール（１つまたは複数）に従おうとしているかを宣言する（すなわち、共存ポリシーの交渉）ことができる。新規参加者は、新規参加者がコミットするポリシーに従ってもよい。

【０１０８】

新規参加者は、新規参加者がどのポリシーに従おうとしているかまたは従おうとしていないかを自由に宣言することができる。このことは、新規参加者がどのように扱われるかを決定し得る（例えば、新規参加者がより柔軟であろうとするほど、より多くの他者が新規参加者と連携する）。ポリシーコミットメントが行われると、新規参加者は、そのポリシーコミットメントに対して誠実であり続けることができる。クラブのルールは変更され得る。用いられている一連のポリシーは、どのネットワーク／デバイスがアクティブであるかに依存し得る。したがって、ネットワークおよびデバイスの入口および出口は、そのポリシーのセットに影響を及ぼし得る。ネットワークおよびデバイスはノマディック（ｎｏｍａｄｉｃ）であってもよい。クラブからクラブへ移動することはかなり簡単であり得

るが、接続継続性を維持することができない（すなわち、ハンドオーバがない）。

【０１０９】

図８は、ＩＥＥＥ８０２．１９システムにおける例示的なセキュリティ手順の流れ図を示す。新規参加者８０２および８０２．１９システム８０４は、発見プロトコル８０６を実行する。新規参加者は、参加要求８０８を８０２．１９システム８０４に送ることによって、８０２．１９システム８０４にアクセスする。８０２．１９システム８０４は、共存のために協調することを決定した他の８０２．１９対応ネットワークデバイスを備える。認証および／またはアクセス交渉８１０は、新規参加者８０２と８０２．１９システム８０４との間で実行され得る。

【０１１０】

８０２．１９システム８０４は、システムポリシー（共存ポリシー）リストを新規参加者に提供し、新規参加者は、ポリシーコミットメント８１４またはコミットメント解除を実行する（すなわち、共存ポリシーを交渉する）。全てのネットワークデバイスが、全てのことを行うことができる、または全てのことを行おうとするわけではない。ポリシーに従うことができるという「証拠」を、８０２．１９システム８０４に送ることができる。システムポリシーコミットメント８１４の後、通常の動作８１６が新規参加者８０２と８０２．１９システム８０４との間で実行され得る。新規参加者８０２は、「共存ヘルプ」を要求することができるまたは共存要求を受信し、実行することができる。新規参加者８０２は、システム脱退通知８１８を８０２．１９システム８０４に送ることによって、システムを離れることができる。新規参加者８０２と８０２．１９システム８０４との間の全てのやり取りは、標準的な整合性および機密性保護を使用してもよく、使用される伝送手段によって提供された機構を活用してもよい。

【０１１１】

アクセス交渉８１０中に実行される認証手順について、中央集中型アーキテクチャまたは分散型アーキテクチャを実施することができる。中央集中型アーキテクチャでは、例えば、標準的な手法（例えば、８０２．１Ｘ）を認証に使用することができる。共存発見および情報サーバ（ＣＤＩＳ）は、認証サーバを提供するエンティティであってもよい。

【０１１２】

分散型アーキテクチャでは、全ての「マスター」デバイスは、それ自体をＴＶＷＳデータベース（ＤＢ）に対して認証することができるという事実を使用することができる。ＴＶＢＤまたはＴＶＢＤネットワークは、ブロードキャストＴＶスペクトルが認可されたサービスによって使用されていない位置での、そのスペクトルにおける無認可の動作を管理することができる。ＴＶＷＳ　ＤＢは、プライマリユーザによって占有されるチャネルのリストを提供することができる。ＴＶＷＳ　ＤＢは、新規参加者の認証成功の証拠をＴＶＷＳ　ＤＢに提供するために使用され得る。この方式を中央集中型アーキテクチャにも使用することができ、このことにより、ＣＤＩＳ内に認証サーバを有することを回避することができる。これは、本明細書に記載される認証手順を実行するときに使用され得る。

【０１１３】

ＴｒＥは、新規参加者における機能の信頼性の測定値を提供して、期待されたやり方で振る舞うことができる。ＴｒＥは、新規参加者の信頼状態の内部セルフチェック（すなわち、新規参加者におけるソフトウェア構成要素の整合性測定値に基づいたハードウェア、ソフトウェア、およびデータのセルフチェック）を実行することができる。（局所的な）整合性チェックの結果のＴｒＥからの署名されたトークンは、新規参加者から８０２．１９システムへのメッセージに含まれ得る。８０２．１９システムは、トークン（および新規参加者）におけるＴｒＥの識別情報に基づいて、信頼できる第三者機関（ＴＴＰ）ベリファイヤを参照して、トークンを検証することができる。ＴＴＰベリファイヤは、その識別情報に基づいて、新規参加者に関するセキュリティアーキテクチャ、プロファイル、および／または機能の情報を提供することができる。

【０１１４】

新規参加者におけるＴｒＥの整合性を、ハードウェアに固定された信頼のルート（Ｒｏ

Ｔ：Ｒｏｏｔ　ｏｆ　Ｔｒｕｓｔ）によってチェックすることができる。ＲｏＴおよびＴｒＥは、その公開鍵ならびにそのセキュリティアーキテクチャ、プロファイル、および／または機能の情報についてのＴＴＰへの追跡可能性によって、信頼できるものとすることができる。新規参加者において、ＴｒＥが読み込まれ、実行され得る。ＴｒＥは、モジュールおよび／または検証し読み込むべき新規参加者の構成要素のグループの読込み順序のリストを用意することができる。ＴｒＥは、その信頼できる状態を証明するために、トークンを作成しおよび／またはトークンに署名して、８０２．１９システムに配布することができる。トークンは、ＴｒＥの秘密鍵によって署名され得る。ＴＴＰを参照することによって、デバイスおよびトークンにおけるＴｒＥの信頼性を検証することができる。８０２．１９システムは、整合性検証情報に基づいてアクセス許可を決定し、新規参加者を確認し、および／または独自の認証情報を用いてトークンに署名することができる。８０２．１９システムは、相互認証を実行した後、トークンを新規参加者に転送してもよい。認証後、新規参加者におけるＴｒＥは、その信頼できる状態を他の８０２．１９システムエンティティに保証するために、８０２．１９システムが署名したトークンをこれらのエンティティに自由に配布することができる。

【０１１５】

分散設定での信頼ベースの認証における課題に含まれるのは、認証用の中央集中型サーバおよび８０２．１９システムが新規参加者の識別情報を知ることができる方法がないということであり得る。信頼システムの存在ならびに規制ＴＶＷＳデータベースを用いた安全な認証および／または登録を前提として、利用可能なリソースを使用することによって、この課題に対処することができる。

【０１１６】

分散設定での信頼ベースの認証手順が本明細書に開示される。新規参加者は、内部セルフチェックを実行することができるおよび／またはプラットフォーム整合性の測定値もしくは証明を生成する。新規参加者は、ＴＶＷＳ　ＤＢにアクセスすることができる。このアクセスは安全なものであり得る。新規参加者は、安全な信頼できるプロセスを使用して、特定のデータベースＩＤを使用する規制データベースを用いて登録成功のトークンを生成することができる。例えば、トークンは、電子証明書または簡易証明書などの証明書であってもよい。例えば、トークンを信頼できる第三者機関に伝送するおよび／またはさかのぼることができる。

【０１１７】

新規参加者は、８０２．１９認証手順を実行することができる。新規参加者は、８０２．１９システムにおいてアクセスおよび／または参加を要求してもよい。新規参加者は、そのプラットフォーム整合性の検証可能なトークンを生成することができる。新規参加者は、規制ＤＢに登録するために使用され、ＤＢ登録成功のトークンを用いて署名された同じＩＤを使用して、８０２．１９システムに対して自分の身元を明らかにすることができる。

【０１１８】

８０２．１９システムは、以下のように新規参加者における信頼を評価することができる。システムは、新規参加者のプラットフォーム整合性を検証することができる。プラットフォーム整合性は、新規参加者の規制者ＤＢ　ＩＤが誠実に生成されることを保証することができる。データベースＩＤは、公開鍵基盤（ＰＫＩ）鍵ペアと関連して、ＴｒＥの秘密鍵を用いたトークンの署名を可能にすることができる。プラットフォーム整合性は、ＤＢ登録成功のトークンが誠実に生成されることを保証することができる。これらの全てをクリアすると、８０２．１９システムは、新規参加者が（知られている）規制ＤＢへの登録に実際に成功したことを信頼することができ、その事実を信頼および認証の根拠として使用することができる。このプロセスは、提供することが要求されるサービス以外の任意のサービスを提供するために規制ＤＢを必要としなくてもよい。

【０１１９】

図９は、初期アクセスの信頼の連鎖を示す。図９に示すように、８０２．１９システム

は、信頼のルート（ＲｏＴ）９０２をチェックすることができる。次いで、８０２．１９システムは、新規参加者のベースラインプラットフォーム整合性９０４をチェックすることができる。これは、例えば、ポリシーおよび／または８０２．１９機能を組み込むことができる。次いで、８０２．１９システムは、９０６で、登録されたデータベース識別情報が誠実なものであることをチェックすることができる。これは、例えば、新規参加者を認証するために実行され得る。８０２．１９システムは、８０２．１９システムに記憶された、データベース内の登録されたデータベース識別情報をチェックすることができる。９０８で、登録されたデータベース識別情報がＯＫである場合、新規参加者を８０２．１９システムに登録することができる。８０２．１９システムは、新規参加者が８０２．１９システムで通信するために使用するトークンを生成することができる。新規参加者は、９１０で、アクセス要求を開始することができる。例えば、新規参加者は、８０２．１９システムをローミングするおよび／または生成されたトークンを使用して他の８０２．１９デバイスと通信することができる。一実施形態では、８０２．１９デバイスは、真正性に関して８０２．１９システムによって生成されたトークンに依存し、独立して新規参加者を認証することができない。

【０１２０】

デバイスの改ざんが行われることがある（すなわち、デバイスがポリシーをコミットしたが、そのポリシーを実施することを意図していない場合、またはデバイスがポリシーをコミットし、そのポリシーを実施しようとしたが、デバイスが改ざんされたために実施できない場合）。例えば、ＴｒＥなどのセキュリティ機構を使用して、デバイスの改ざんの脅威に対処することができる。

【０１２１】

デバイスが改ざんされていないことを示す情報を提供することができる。これは、アクセスおよび／または登録手順の一部として、一度行われ得る。他の８０２．１９エンティティに回覧することができるトークンを生成することができる。それぞれのポリシーコミットメント（および／またはコミットメント解除）を用いたＴｒＥベースの誠実さの証明（ａｔｔｅｓｔａｔｉｏｎ　ｏｆ　ｈｏｎｅｓｔｙ）を使用することができる。ＴｒＥベースの誠実さの証明は、断続的におよび／またはまれにＴｒＥ機能を使用してもよい。これは、プラットフォーム整合性の証拠（トークン生成および／または通過）によって、コミットされたポリシーに従うことができることを証明することができる。

【０１２２】

図１０は、初回の接続の例示的なプロセスを示す。図１０に示すように、新規参加者１１０２は、システム構成要素の整合性を測定するおよび／またはチェックすることによって、安全な起動を実行することができる。新規参加者は、セルフチェック測定値またはデータおよびセキュリティプロファイル／機能の情報に関するレポート１０４を８０２．１９システム１１０８に送る（トークンを生成する）ことができる。８０２．１９システム１１０８は、レポート内の情報を解析して、信頼性を評価することができる。８０２．１９システム１１０８は、アクセスを許可することによって応答してもよく、またはレポートで供給された情報に基づいてデバイスが信頼できないと思われる場合はアクセスを許可しなくてもよい。アクセス制御決定１１０６を介して、アクセス情報を新規参加者１１０２に送ることができる。

【０１２３】

新規参加者１１０２は、ＴＶＢＤネットワークの領域内をローミングすることができ、ポリシー交渉を実行することができる。新規参加者１１０２は、ポリシーコミットメントをブロードキャストすることができる。新規参加者１１０２は、共存機構を実行することができる。

【０１２４】

ポリシー変更、ポリシー交渉、および／または認証の後、新規参加者１１０２は、セルフチェック（トークン）および／またはセキュリティプロファイル情報に関するレポートを８０２．１９システム１１０８に送ることができ、ポリシー更新メッセージを監視する

および／またはポリシー再交渉を実行するおよび／または更新されたポリシーコミットメントをブロードキャストすることができる。新規参加者１１０２は、共存機構を実行してもよい。

【０１２５】

本明細書に記載されるように、８０２．１９システムはシステムポリシー更新を新規参加者に送ることができ、新規参加者はシステムポリシーコミットメントで応答することができる。それぞれのネットワークおよび／またはデバイスは、それが従うことができるまたは従おうとするポリシーを自由に選んでもよい。ネットワークおよび／またはデバイスが、それが従うことができるまたは従おうとするポリシーを宣言すると、ネットワークおよび／またはデバイスはそのポリシーに従うことをコミットする。ポリシーコミットメントの後に、共存機構を実行することができる。新規参加者は、ポリシーコミットメント解除を宣言してもよい。

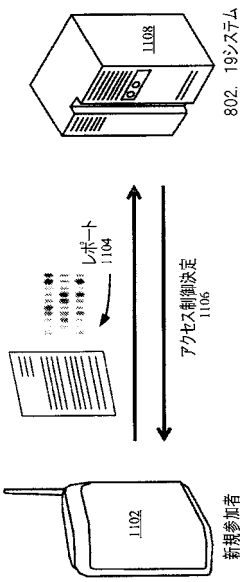
【０１２６】

本明細書に記載されるシステム、方法、および装置を３ＧＰＰ　ＵＭＴＳワイヤレス通信システムの文脈内で記載することができるが、これらは任意のワイヤレス技術に適用され得る。例えば、本明細書に記載される実施形態は、制御チャネル監視セットが使用される（例えば、ＬＴＥ、ＬＴＥ－Ａ、および／またはＷｉＭａｘ）場合、ワイヤレス技術に適用され得る。例えば、ＰＤＣＣＨ監視セットについて、解決策をＬＴＥに拡張することができる。

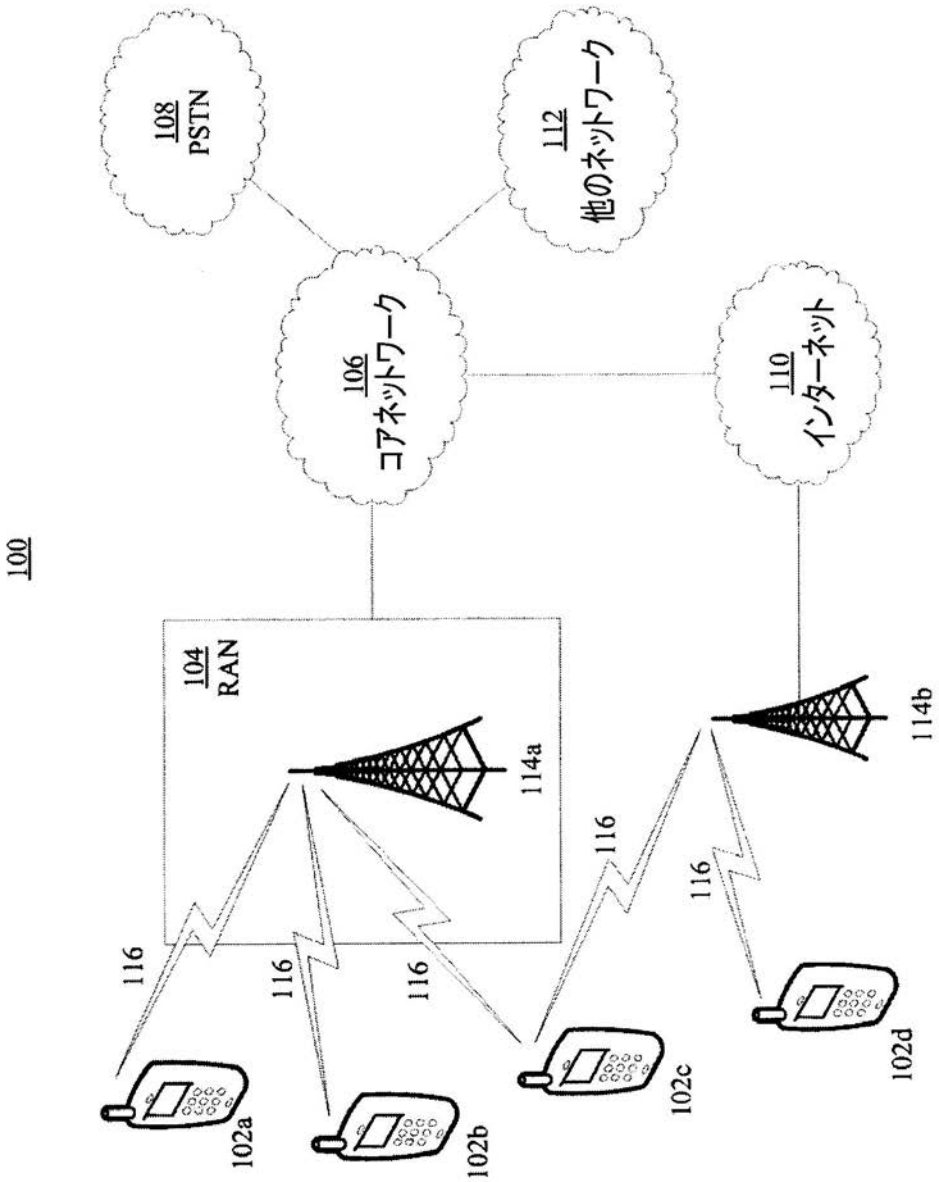
【０１２７】

特徴および要素が特定の組合せにおいて上記に記載されているが、当業者であれば、それぞれの特徴または要素を、単独でまたは他の特徴および要素との任意の組合せで使用することができることを理解されよう。加えて、本明細書に記載される方法を、コンピュータまたはプロセッサによって実行するためにコンピュータ可読媒体に組み込まれたコンピュータプログラム、ソフトウェア、またはファームウェアで実施することができる。コンピュータ可読媒体の例としては、（有線またはワイヤレス接続を介して送信される）電子信号およびコンピュータ可読記憶媒体が挙げられる。コンピュータ可読記憶媒体の例としては、読取り専用メモリ（ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、レジスタ、キャッシュメモリ、半導体メモリデバイス、内部ハードディスクおよびリムーバブルディスクなどの磁気媒体、磁気光学媒体、ならびにＣＤ－ＲＯＭディスク、およびデジタル多用途ディスク（ＤＶＤ）などの光学媒体が挙げられるが、これらに限定されない。ソフトウェアに関連したプロセッサを使用して、ＷＴＲＵ、ＵＥ、端末、基地局、ＲＮＣ、または任意のホストコンピュータで使用するための無線周波数トランシーバを実施することができる。

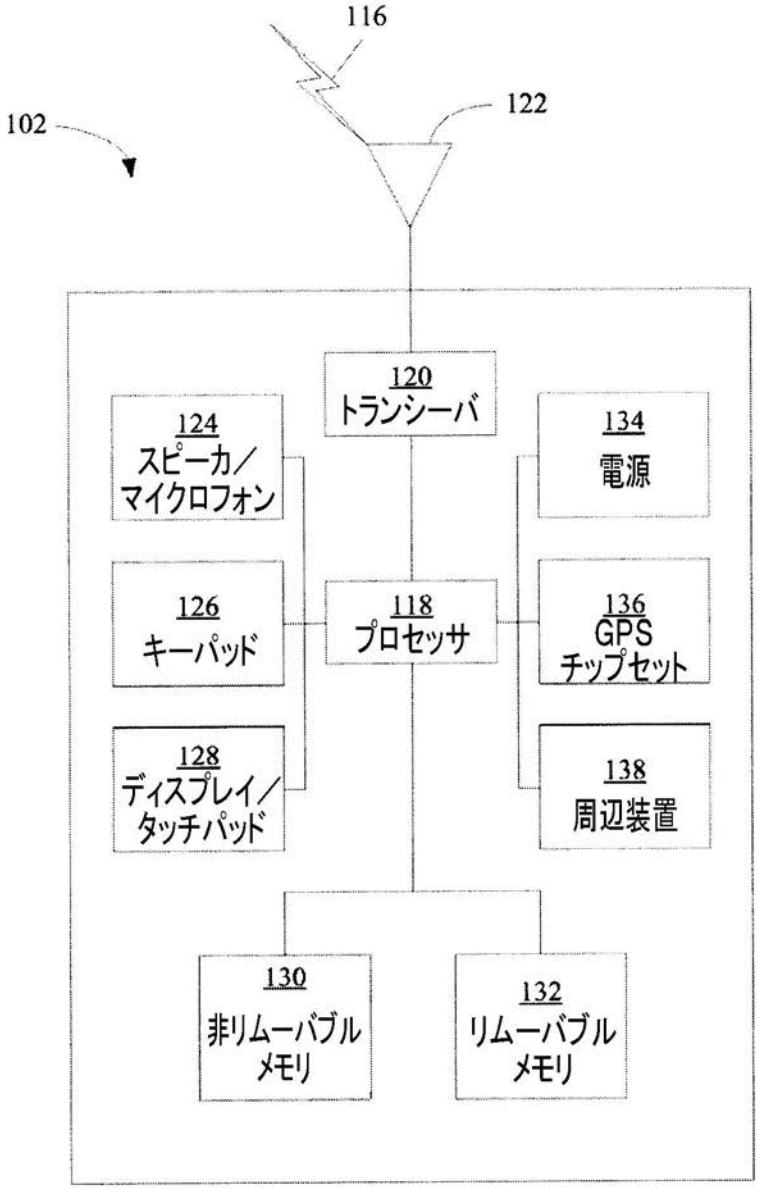
【図１０】



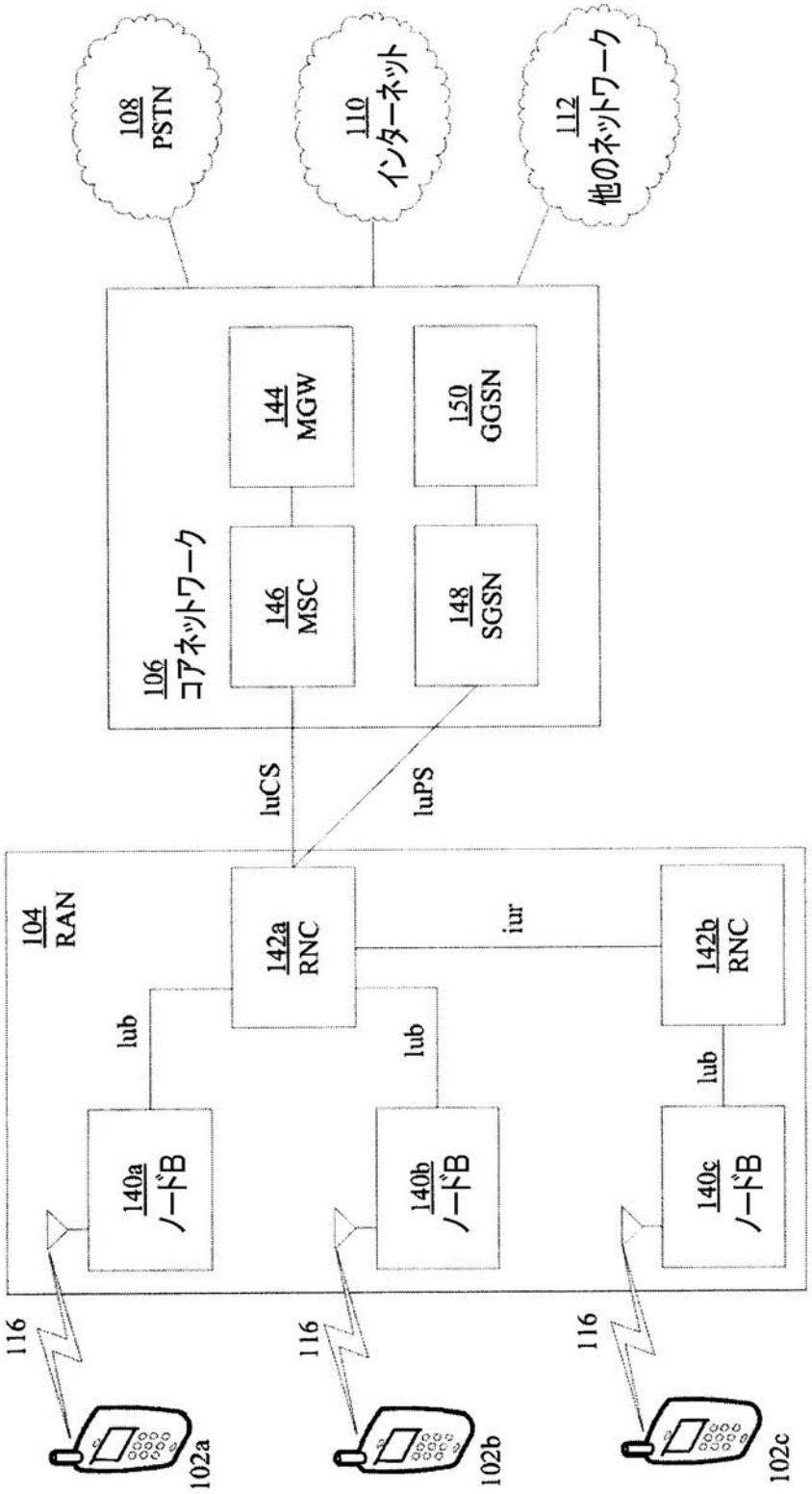
【図１Ａ】


100
108
PSTN
112
他のネットワーク
106
コアネットワーク
110
インターネット
104
RAN
114a
114b
116
116
116
116
116
102a
102b
102c
102d

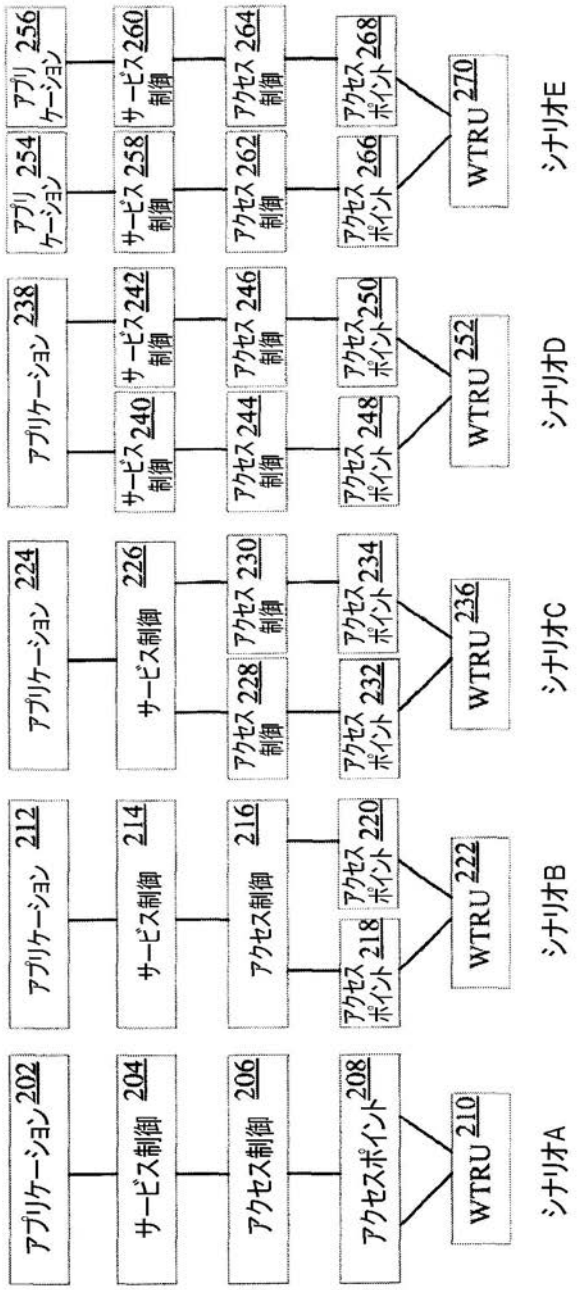
【図１Ｂ】


116
122
102
120
トランシーバ
124
スピーカ／
マイクロフォン
126
キーパッド
128
ディスプレイ／
タッチパッド
118
プロセッサ
134
電源
136
GPS
チップセット
138
周辺装置
130
非リムーバブル
メモリ
132
リムーバブル
メモリ

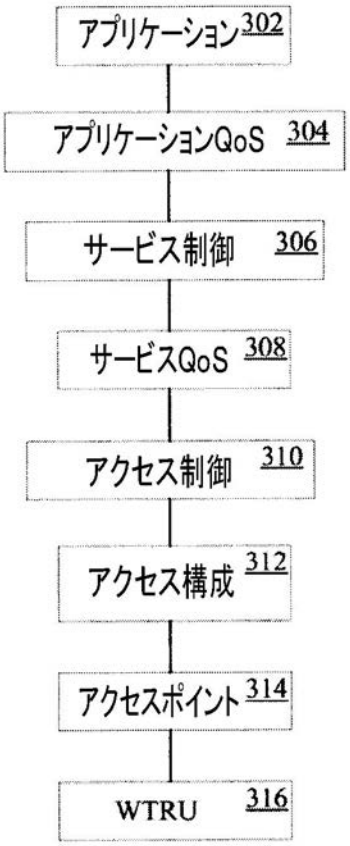
【図１Ｃ】


108
PSTN
110
インターネット
112
他のネットワーク
106
コアネットワーク
144
MGW
146
MSC
150
GGSN
148
SGSN
luCS
luPS
104
RAN
142a
RNC
142b
RNC
iur
lub
lub
lub
140a
ノードB
140b
ノードB
140c
ノードB
116
116
116
102a
102b
102c

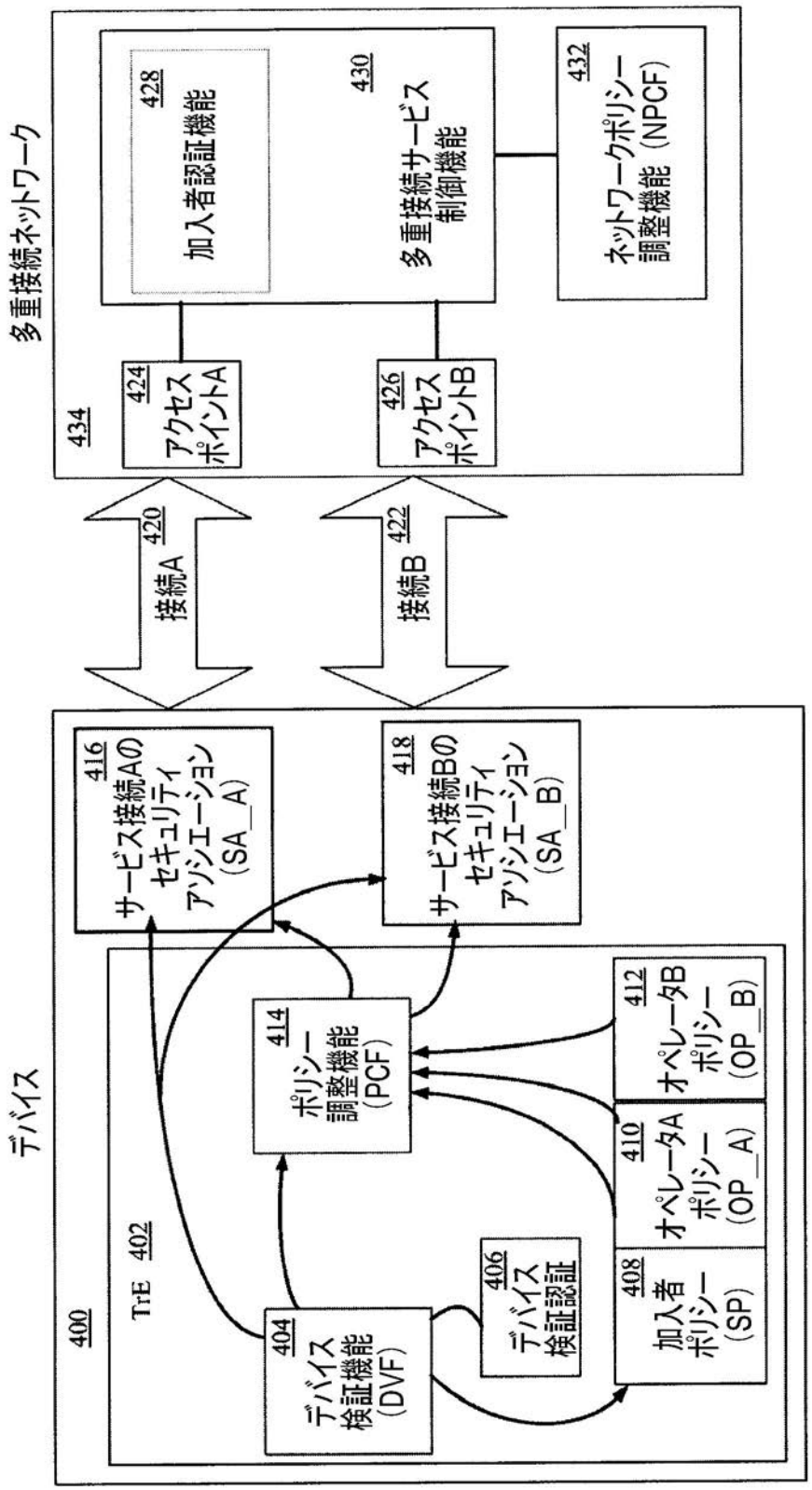
【図２】


アプリケーション 202
サービス制御 204
アクセス制御 206
アクセスポイント 208
WTRU 210
シナリオA
アプリケーション 212
サービス制御 214
アクセス制御 216
アクセス ポイント 218
アクセス ポイント 220
WTRU 222
シナリオB
アプリケーション 224
サービス制御 226
アクセス 制御 228
アクセス 制御 230
アクセス ポイント 232
アクセス ポイント 234
WTRU 236
シナリオC
アプリケーション 238
サービス 制御 240
サービス 制御 242
アクセス 制御 244
アクセス 制御 246
アクセス ポイント 248
アクセス ポイント 250
WTRU 252
シナリオD
アプリ ケーション 254
アプリ ケーション 256
サービス 制御 258
サービス 制御 260
アクセス 制御 262
アクセス 制御 264
アクセス ポイント 266
アクセス ポイント 268
WTRU 270
シナリオE

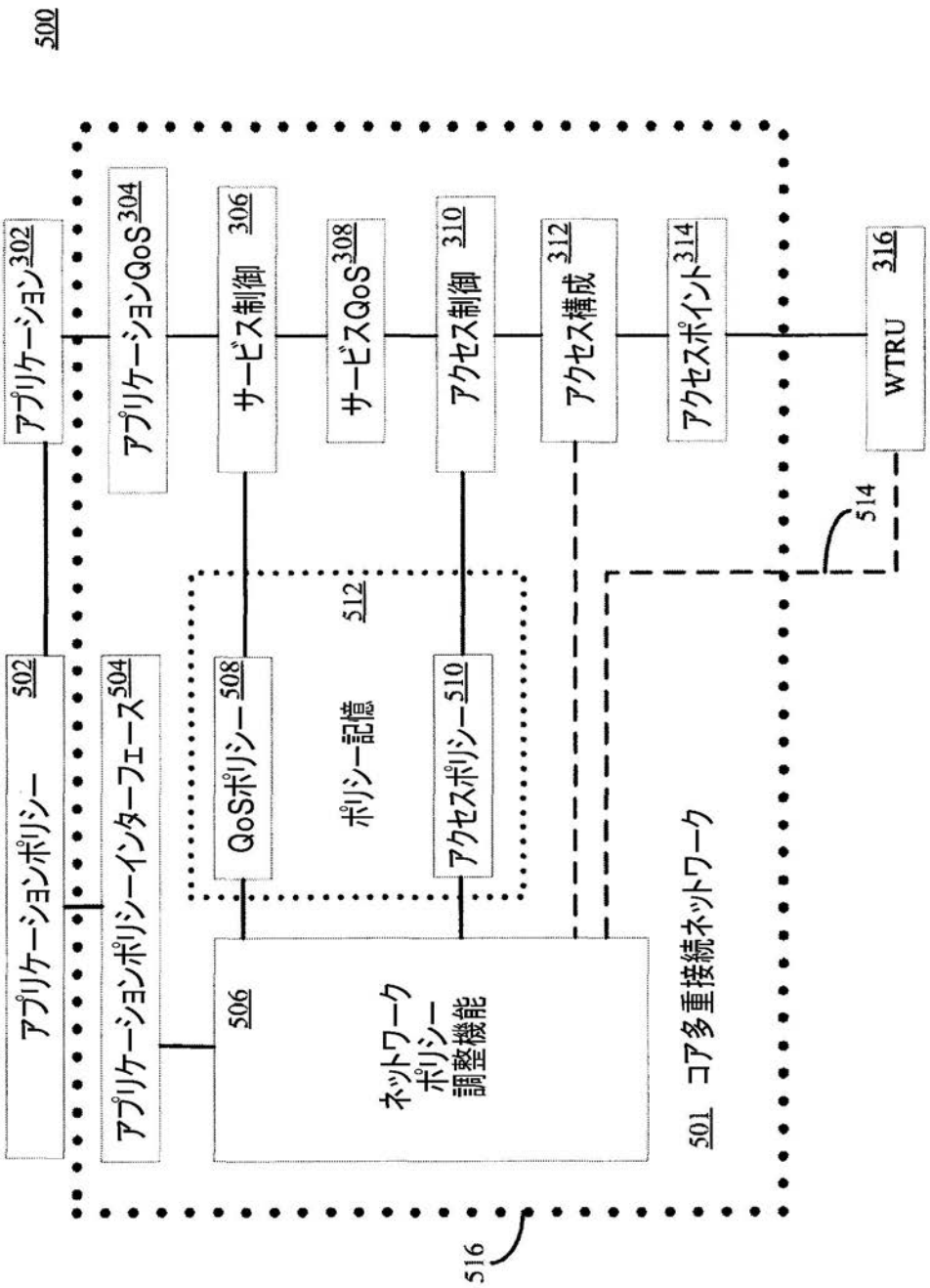
【図３】


アプリケーション 302
アプリケーションQoS 304
サービス制御 306
サービスQoS 308
アクセス制御 310
アクセス構成 312
アクセスポイント 314
WTRU 316

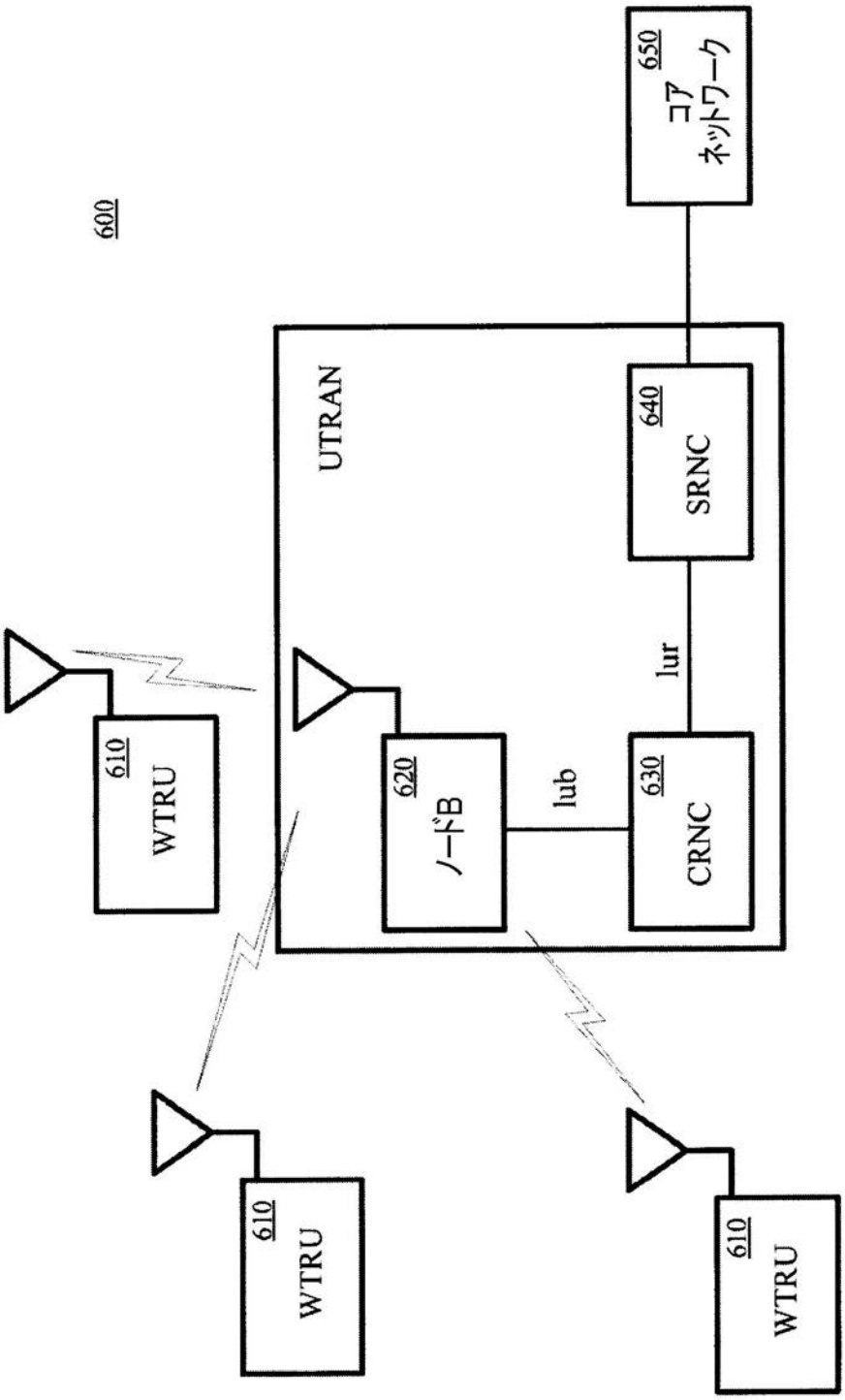
【図４】


多重接続ネットワーク
428
加入者認証機能
430
多重接続サービス
制御機能
432
ネットワークポリシー
調整機能（NPCF）
434
424
アクセス
ポイントA
426
アクセス
ポイントB
420
接続A
422
接続B
デバイス
400
TrE 402
416
サービス接続Aの
セキュリティ
アソシエーション
（SA_A）
418
サービス接続Bの
セキュリティ
アソシエーション
（SA_B）
414
ポリシー
調整機能
（PCF）
412
オペレータB
ポリシー
（OP_B）
410
オペレータA
ポリシー
（OP_A）
406
デバイス
検証認証
404
デバイス
検証機能
（DVF）
408
加入者
ポリシー
（SP）

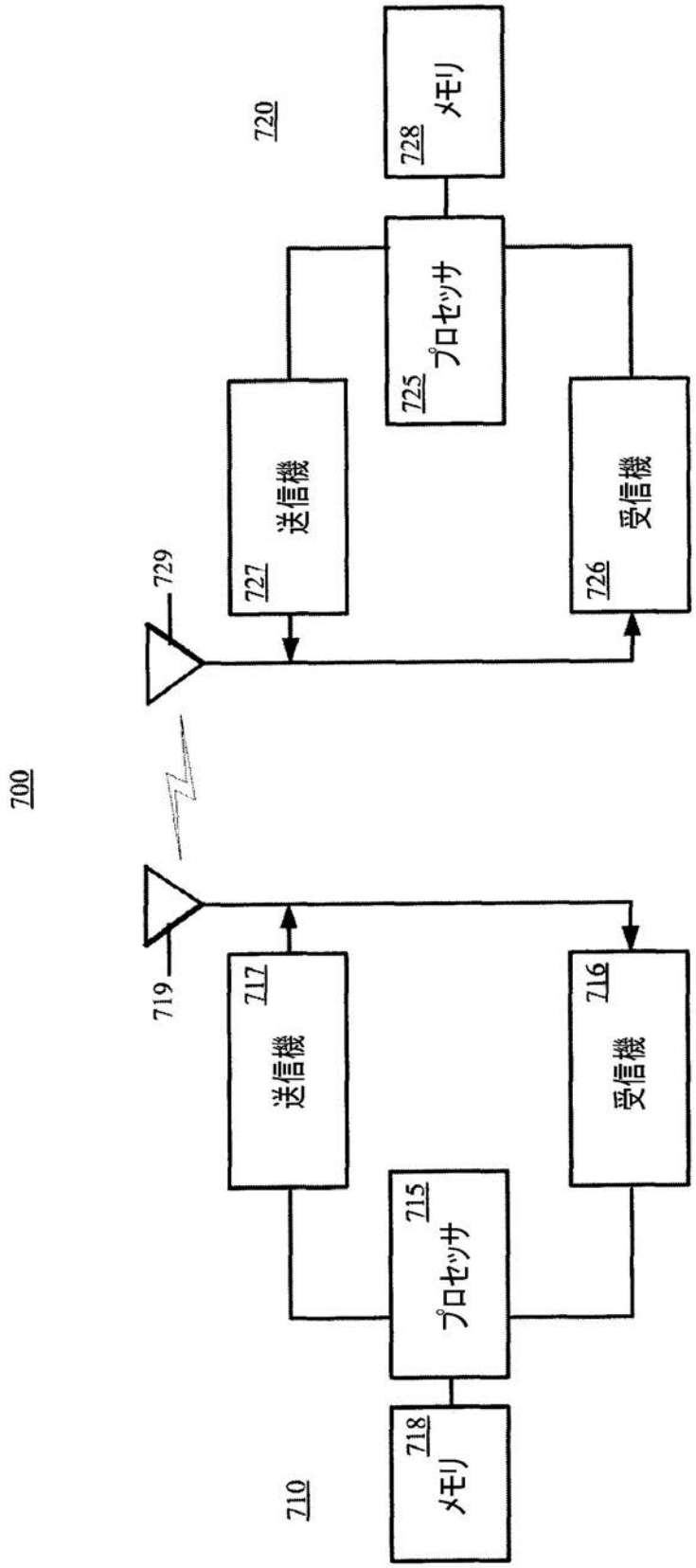
【図５】


500
アプリケーション 302
アプリケーションQoS 304
サービス制御 306
サービスQoS 308
アクセス制御 310
アクセス構成 312
アクセスポイント 314
WTRU 316
514
アプリケーションポリシー 502
アプリケーションポリシーインターフェース 504
QoSポリシー 508
ポリシー記憶 512
アクセスポリシー 510
506
ネットワーク
ポリシー
調整機能
501 コア多重接続ネットワーク
516

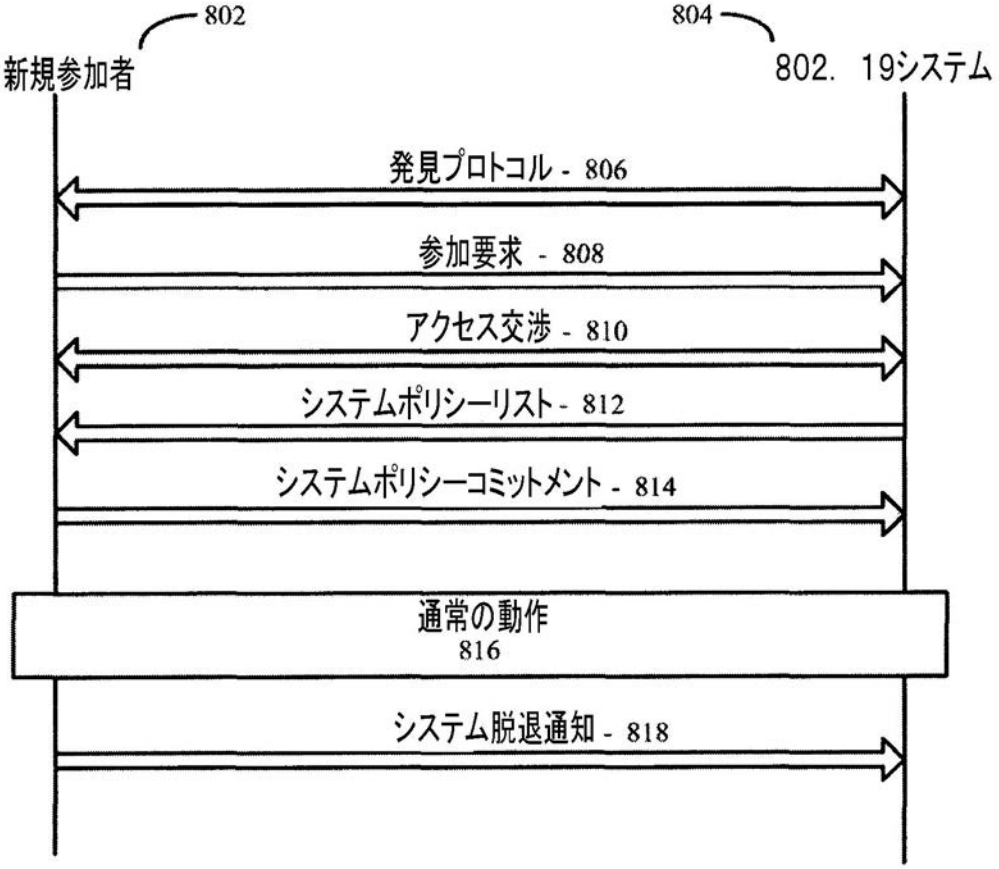
【図６】


600
650
コア
ネットワーク
UTRAN
640
SRNC
lur
620
ノードB
lub
630
CRNC
610
WTRU
610
WTRU
610
WTRU

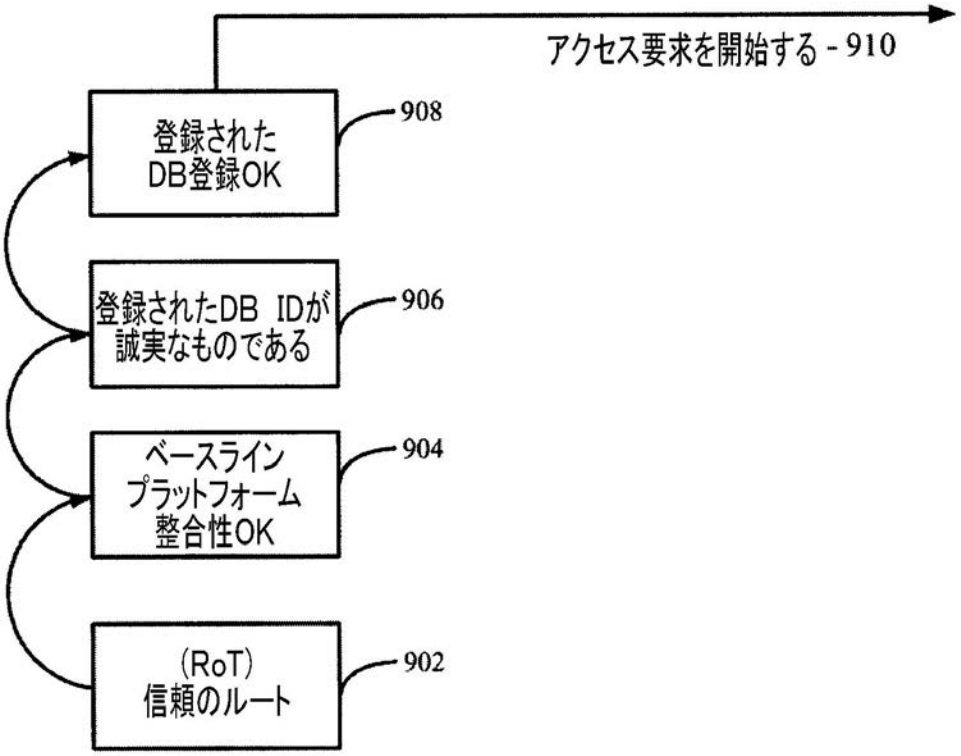
【図７】


700
710
715
プロセッサ
716
受信機
717
送信機
718
メモリ
719
720
725
プロセッサ
726
受信機
727
送信機
728
メモリ
729

【図８】


802
新規参加者
804
802. 19システム
発見プロトコル - 806
参加要求 - 808
アクセス交渉 - 810
システムポリシーリスト - 812
システムポリシーコミットメント - 814
通常の動作
816
システム脱退通知 - 818

【図９】


アクセス要求を開始する - 910
登録された
DB登録OK
908
登録されたDB IDが
誠実なものである
906
ベースライン
プラットフォーム
整合性OK
904
(RoT)
信頼のルート
902

フロントページの続き

(72)発明者　オスカー　ロペス－トーレス
アメリカ合衆国　７８２３９　テキサス州　サン　アントニオ　セリーヌ　リッジ　ドライブ　８５２３
(72)発明者　インヒョク　チャ
大韓民国　ソウル　カンナム－ク　２０２－ホ　１０２－ドン　ジュン－アン　ハイツ　ヴィレッジ
(72)発明者　ローレンス　ケース
アメリカ合衆国　７８７３４　テキサス州　オースティン　ティモシー　サークル　５００２
(72)発明者　ヨゲンドラ　シー．シャー
アメリカ合衆国　１９３４１　ペンシルベニア州　エクストン　リージェンシー　コート　１０

Ｆターム(参考) 5K067 AA30 AA32 BB04 EE04
5K201 AA07 BC23 EA07 ED05 EE05 FA01 FB01 FB06