(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5932137号
(P5932137)

(45)発行日　平成28年6月8日(2016.6.8)　(24)登録日　平成28年5月13日(2016.5.13)

(51)Int.Cl.			F I		
H04L	***9/32***	***(2006.01)***	H04L	9/00	675A
H04L	***9/08***	***(2006.01)***	H04L	9/00	601F

請求項の数 25　(全 35 頁)

(21)出願番号	特願2015-505724 (P2015-505724)
(86)(22)出願日	平成25年3月11日 (2013.3.11)
(65)公表番号	特表2015-514380 (P2015-514380A)
(43)公表日	平成27年5月18日 (2015.5.18)
(86)国際出願番号	PCT/US2013/030277
(87)国際公開番号	WO2013/154714
(87)国際公開日	平成25年10月17日 (2013.10.17)
審査請求日	平成27年9月17日 (2015.9.17)
(31)優先権主張番号	61/622,434
(32)優先日	平成24年4月10日 (2012.4.10)
(33)優先権主張国	米国(US)
(31)優先権主張番号	13/791,879
(32)優先日	平成25年3月8日 (2013.3.8)
(33)優先権主張国	米国(US)

早期審査対象出願

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

最終頁に続く

(54)【発明の名称】安全なＭＢＭＳ受信報告のための方法およびデバイス

(57)【特許請求の範囲】

【請求項１】

ユーザ機器（ＵＥ）のワイヤレス通信の方法であって、

サービスプロバイダから、認証局リストを受信することと、前記認証局リストは、前記ＵＥおよび前記サービスプロバイダによって知られ、かつ前記ＵＥにおけるスマートカード上に記憶された認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われている、

サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信することと、

前記サーバとの安全な接続をセットアップすることと、

前記受信された認証局リストを使用して前記サーバを認証することと、

前記アドレスおよび前記受信報告構成に基づいて前記安全な接続を通じて前記サーバに受信報告を送ることと、を備える、方法。

【請求項２】

前記認証局リストは、信頼される認証局の証明書を含む、請求項１に記載の方法。

【請求項３】

前記サーバの証明書を受信することと、

前記サーバを認証する際に前記サーバとの前記安全な接続をセットアップすることを決定することと、

をさらに備え、

前記認証することは、前記受信された証明書と前記認証局リストとの比較に基づいて、前記受信された証明書が信頼される認証局からのものであることを決定すること、を備える、
請求項１に記載の方法。
【請求項４】
前記認証情報は、前記ＵＥおよび前記サービスプロバイダによって知られている共有キーである、請求項１に記載の方法。
【請求項５】
前記共有キーは、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）、ＭＢＭＳユーザキー（ＭＵＫ）、または前記ＭＲＫまたは前記ＭＵＫのうちの１つから導出されたキーに基づく、請求項４に記載の方法。
【請求項６】
前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じたものである、請求項１に記載の方法。
【請求項７】
前記ユーザサービス発見／アナウンスメントは、前記ＵＥおよびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、請求項１に記載の方法。
【請求項８】
前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づく、請求項７に記載の方法。
【請求項９】
ワイヤレス通信のための装置であって、
サービスプロバイダから、認証局リストを受信するための手段と、前記認証局リストは、前記装置および前記サービスプロバイダによって知られ、かつ前記装置におけるスマートカード上に記憶された認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われている、
サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信するための手段と、
前記サーバとの安全な接続をセットアップするための手段と、
前記受信された認証局リストを使用して前記サーバを認証するための手段と、
前記アドレスおよび前記受信報告構成に基づいて前記安全な接続を通じて前記サーバに受信報告を送るための手段と、を備える、装置。
【請求項１０】
前記認証局リストは、信頼される認証局の証明書を含む、請求項９に記載の装置。
【請求項１１】
前記サーバの証明書を受信するための手段と、
前記サーバを認証する際に前記サーバとの前記安全な接続をセットアップすることを決定するための手段と、
をさらに備え、
前記認証するための手段は、前記受信された証明書と前記認証局リストとの比較に基づいて、前記受信された証明書が信頼される認証局からのものであることを決定することによって前記サーバを認証する、請求項９に記載の装置。
【請求項１２】
前記認証情報は、前記装置および前記サービスプロバイダによって知られている共有キーである、請求項９に記載の装置。
【請求項１３】
前記共有キーは、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）、ＭＢＭＳユーザキー（ＭＵＫ）、もしくは前記ＭＲＫまたは前記ＭＵＫのうちの１つから導出されたキーに基づく、請求項１２に記載の装置。

【請求項１４】
前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じたものである、請求項９に記載の装置。
【請求項１５】
前記ユーザサービス発見／アナウンスメントは、前記装置およびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、請求項９に記載の装置。
【請求項１６】
前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づく、請求項１５に記載の装置。
【請求項１７】
ワイヤレス通信のための装置であって、
メモリと、
前記メモリに結合された少なくとも１つのプロセッサであって、
サービスプロバイダから、認証局リストを受信し、前記認証局リストは、前記装置および前記サービスプロバイダによって知られ、かつ前記装置におけるスマートカード上に記憶された認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われている、
サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信し、
前記サーバとの安全な接続をセットアップし、
前記受信された認証局リストを使用して前記サーバを認証し、
前記アドレスおよび前記受信報告構成に基づいて前記安全な接続を通じて前記サーバに受信報告を送る、ように構成された少なくとも１つのプロセッサと、を備える、装置。
【請求項１８】
前記認証局リストは、信頼される認証局の証明書を含む、請求項１７に記載の装置。
【請求項１９】
前記少なくとも１つのプロセッサは、
前記サーバの証明書を受信し、
前記サーバを認証する際に、前記サーバとの前記安全な接続をセットアップすることを決定する、ようにさらに構成され、
前記少なくとも１つのプロセッサは、前記受信された証明書と前記認証局リストとの比較に基づいて、前記受信された証明書が信頼される認証局からのものであることを決定することによって認証する、請求項１７に記載の装置。
【請求項２０】
前記認証情報は、前記装置および前記サービスプロバイダによって知られている共有キーである、請求項１７に記載の装置。
【請求項２１】
前記共有キーは、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）、ＭＢＭＳユーザキー（ＭＵＫ）、もしくは前記ＭＲＫまたは前記ＭＵＫのうちの１つから導出されたキーに基づく、請求項２０に記載の装置。
【請求項２２】
前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じたものである、請求項１７に記載の装置。
【請求項２３】
前記ユーザサービス発見／アナウンスメントは、前記装置およびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、請求項１７に記載の装置。
【請求項２４】
前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）

サービスキー（ＭＳＫ）に基づく、請求項２３に記載の装置。
【請求項２５】
サービスプロバイダから、認証局リストを受信することと、前記認証局リストは、ユーザ機器（ＵＥ）および前記サービスプロバイダによって知られ、かつ前記ＵＥにおけるスマートカード上に記憶された認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われている、
サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信することと、
前記サーバとの安全な接続をセットアップすることと、
前記受信された認証局リストを使用して前記サーバを認証することと、
前記アドレスおよび前記受信報告構成に基づいて前記安全な接続を通じて前記サーバに受信報告を送ることと、のためのワイヤレス通信のためのコンピュータ実行可能なコードを記憶したコンピュータ可読媒体。
【発明の詳細な説明】
【関連出願の相互参照】
【０００１】
[0001] 本出願は、２０１２年４月１０日に出願された、「Ｓｅｃｕｒｅ　Ｒｅｃｅｐｔｉｏｎ　Ｒｅｐｏｒｔｉｎｇ」という名称の、米国仮出願番号第６１／６２２４３４号、および２０１３年３月８日に出願された、「Ｓｅｃｕｒｅ　Ｒｅｓｏｕｒｃｅ　Ｒｅｐｏｒｔｉｎｇ」という名称の、米国特許出願第１３／７９１８７９号の利益を主張し、それらはその全体でここに参照により明示的に組み込まれている。
【技術分野】
【０００２】
[0002] 本開示は、概して通信システムに関し、より具体的には、安全な受信報告に関する。
【背景技術】
【０００３】
[0003] ワイヤレス通信システムは、電話通信、ビデオ、データ、メッセージング、およびブロードキャストのような様々な電気通信サービスを提供するために広く展開されている。典型的なワイヤレス通信システムは、利用可能なシステムリソース（例えば、帯域幅、送信電力）を共有することによって複数のユーザとの通信をサポートすることができる多元接続技術を用いることができる。このような多元接続技術の例は、符号分割多元接続（ＣＤＭＡ）システム、時分割多元接続（ＴＤＭＡ）システム、周波数分割多元接続（ＦＤＭＡ）システム、直交周波数分割多元接続（ＯＦＤＭＡ）システム、シングルキャリア周波数分割多元接続（ＳＣ－ＦＤＭＡ）システム、および時分割同期符号分割多元接続（ＴＤ－ＳＣＤＭＡ）システムを含む。
【０００４】
[0004] これらの多元接続技術は、異なる無線デバイスが、市区町村レベル、国レベル、地方レベル、さらにグローバルなレベルでさえ通信できるようにする、共通のプロトコルを提供するために、様々な電気通信規格に採用されてきた。台頭してきた電気通信規格の例は、ロングタームエボリューション（ＬＴＥ）である。ＬＴＥは、第３世代パートナーシッププロジェクト（３ＧＰＰ）によって発表されたユニバーサルモバイル電気通信システム（ＵＭＴＳ）のモバイル規格の強化したもの（ｅｎｈａｎｃｅｍｅｎｔ）のセットである。それは、スペクトル効率を改善すること、コストを下げること、サービスを向上させること、新たなスペクトルを利用すること、および、ダウンリンク（ＤＬ）にＯＦＤＭＡを使用し、アップリンク（ＵＬ）にＳＣ－ＦＤＭＡを使用し、かつ多入力多出力（ＭＩＭＯ）アンテナ技術を使用して、より良好に他のオープン規格と統合することによって、モバイルブロードバンドインターネットアクセスをより良好にサポートするように設計されている。しかしながら、モバイルブロードバンドアクセスを求める需要が増加し続けるのに伴い、ＬＴＥ技術にはさらなる改善の必要性が存在する。望ましくは、これらの改善

は、これらの技術を用いる電気通信規格および他の多元接続技術に適用可能であるべきである。

【発明の概要】

【０００５】

[0005] 本開示の態様では、方法、コンピュータプログラム製品、および装置ＵＥが提供されている。ＵＥは、サービスプロバイダから、認証局リストを受信する。認証局リストは、ＵＥおよびサービスプロバイダによって知られ、かつＵＥにおけるスマートカード上に記憶された認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる。加えて、ＵＥは、受信された認証局リストを使用してサーバを認証する。

【０００６】

[0006] 本開示の態様では、方法、コンピュータプログラム製品、および装置が提供されている。装置は、サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信する。加えて、装置は、受信報告構成に基づいて、サーバに保護された受信報告を送る。

【０００７】

[0007] 本開示の態様では、方法、コンピュータプログラム製品、および装置が提供されている。装置は、ＵＥでありうる。ＵＥは、保護されたブロードキャストアナウンスメントを受信する。ブロードキャストアナウンスメントは、ＵＥによって知られ、かつＵＥにおけるスマートカード上に記憶された認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる。加えて、ＵＥは、ブロードキャストアナウンスメントに基づいて通信する。

【図面の簡単な説明】

【０００８】

【図１】ネットワークアーキテクチャの例を例示する図である。

【図２】アクセスネットワークの例を例示する図である。

【図３】ＬＴＥにおけるＤＬフレーム構造の例を例示する図である。

【図４】ＬＴＥにおけるＵＬフレーム構造の例を例示する図である。

【図５】ユーザおよび制御プレーンのための無線プロトコルアーキテクチャの例を例示する図である。

【図６】アクセスネットワークにおける発展型ノードＢおよびユーザ機器の例を例示する図である。

【図７Ａ】マルチキャストブロードキャスト単一周波数ネットワークにおける発展型マルチメディアブロードキャストマルチキャストサービスチャネル構成の例を例示する図である。

【図７Ｂ】マルチキャストチャネルスケジューリング情報メディアアクセス制御の制御要素のフォーマットを例示する図である。

【図８】安全な受信報告を送るための第１の実例となる方法を例示する図である。

【図９】安全な受信報告を送るための第２の実例となる方法を例示する図である。

【図１０】安全なユーザサービス発見／アナウンスメントを受信および処理するための実例となる方法を例示する図である。

【図１１】ワイヤレス通信の第１の方法のフローチャートである。

【図１２】ワイヤレス通信の第２の方法のフローチャートである。

【図１３】ワイヤレス通信の第３の方法のフローチャートである。

【図１４】実例となる装置において異なるモジュール／手段／コンポーネント間のデータフローを例示する概略的なデータフロー図である。

【図１５】処理システムを用いる装置のためのハードウェアインプリメンテーションの例を例示する図である。

【詳細な説明】

【０００９】

[0024] 添付の図面に関係して以下に述べられる詳細な説明は、様々な構成の説明として

意図されており、ここで説明される概念が実現されうる、唯一の構成を表すように意図されていない。詳細な説明は、様々な概念の徹底的な理解を提供する目的で、具体的な詳細を含む。しかしながら、これらの概念がこれらの具体的な詳細なしに実現されうることは当業者には明らかになるだろう。いくつかの事例では、周知の構造およびコンポーネントが、そのような概念を曖昧にすることを避けるためにブロック図の形態で図示されている。

【００１０】

[0025] 電気通信システムのいくつかの態様は、ここでは、様々な装置および方法を参照して表されることになる。これらの装置および方法は、様々なブロック、モジュール、コンポーネント、回路、ステップ、処理、アルゴリズム等（集合的には「要素」と称される）により、以下の詳細な説明において説明され、添付の図面において例示されることになる。これらの要素は、電子ハードウェア、コンピュータソフトウェア、またはそれらのあらゆる組み合わせを使用してインプリメントされうる。そのような要素がハードウェアとしてインプリメントされるかソフトウェアとしてインプリメントされるかは、システム全体に課された設計の制約および特定のアプリケーションに依存する。

【００１１】

[0026] 例として、要素、または要素のいずれか一部、または要素のあらゆる組み合わせは、１つまたは複数のプロセッサを含む「処理システム」を用いてインプリメントされうる。プロセッサの例は、本開示全体を通して説明される様々な機能を行うように構成された、マイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ（ＤＳＰ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、プログラマブル論理デバイス（ＰＬＤ）、ステートマシン、ゲート論理、ディスクリートハードウェア回路、および他の適したハードウェアを含む。処理システムにおける１つまたは複数のプロセッサは、ソフトウェアを行うことができる。ソフトウェアは、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語、あるいは別の方法で称されようと、命令、命令セット、コード、コードセグメント、プログラムコード、プログラム、サブプログラム、ソフトウェアモジュール、アプリケーション、ソフトウェアアプリケーション、ソフトウェアパッケージ、ルーチン、サブルーチン、オブジェクト、実行ファイル、実行スレッド、プロシージャ、関数、等を意味するように広く解釈されるだろう。

【００１２】

[0027] したがって、１つまたは複数の実例となる実施形態では、説明される機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらのあらゆる組み合わせでインプリメントされうる。ソフトウェアでインプリメントされる場合、機能は、コンピュータ可読媒体上に、１つまたは複数の命令またはコードとして記憶されるか、あるいは１つまたは複数の命令またはコードとして符号化されうる。コンピュータ可読媒体は、コンピュータ記憶媒体を含む。記憶媒体は、コンピュータによってアクセスされうるあらゆる利用可能な媒体でありうる。限定ではなく例として、このようなコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭまたは他の光学ディスク記憶装置、磁気ディスク記憶装置またはその他の磁気記憶デバイス、あるいは、データ構造または命令の形態で所望のプログラムコードを搬送または記憶するために使用されることができ、かつコンピュータによってアクセスされうるあらゆる他の媒体を備えることができる。ここで使用される、ディスク（Ｄｉｓｋ）とディスク（ｄｉｓｃ）は、コンパクトディスク（ＣＤ）、レーザディスク（登録商標）、光学ディスク、デジタルバーサタイルディスク（ＤＶＤ）、およびフロッピー（登録商標）ディスクを含み、ディスク（Ｄｉｓｋ）は大抵、データを磁気的に再生し、その一方でディスク（ｄｉｓｃ）は、データをレーザで光学的に再生する。上記の組み合わせは、また、コンピュータ可読媒体の範囲内に含まれるべきである。

【００１３】

[0028] 図１は、ＬＴＥネットワークアーキテクチャ１００を例示する図である。ＬＴＥネットワークアーキテクチャ１００は、発展型パケットシステム（ＥＰＳ）１００として

称されうる。ＥＰＳ１００は、１つまたは複数のユーザ機器（ＵＥ）１０２、発展型ＵＭＴＳ地上無線アクセスネットワーク（Ｅ－ＵＴＲＡＮ）１０４、発展型パケットコア（ＥＰＣ）１１０、ホーム加入者サーバ（ＨＳＳ）１２０、およびオペレータのインターネットプロトコル（ＩＰ）サービス１２２を含むことができる。ＥＰＳは、他のアクセスネットワークと相互接続することができるけれども、簡潔化のために、それらのエンティティ／インターフェースは図示されていない。図示されているように、ＥＰＳはパケット交換サービスを提供するけれども、当業者が容易に認識するように、本開示全体を通して示されている様々な概念が、回路交換サービスを提供するネットワークに拡張されることができる。

【００１４】

[0029] Ｅ－ＵＴＲＡＮは、発展型ノードＢ（ｅＮＢ）１０６および他のｅＮＢ１０８を含む。ｅＮＢ１０６は、ＵＥ１０２に対するユーザおよび制御プレーンプロトコル終端を提供する。ｅＮＢ１０６は、バックホール（例えば、Ｘ２インターフェース）を介して、他のｅＮＢ１０８に接続されることができる。ｅＮＢ１０６はまた、基地局、ノードＢ、アクセスポイント、基地トランシーバ局、無線基地局、無線トランシーバ、トランシーバ機能、ベーシックサービスセット（ＢＳＳ）、拡張サービスセット（ＥＳＳ）、または何らかの他の適した専門用語として称されうる。ｅＮＢ１０６は、ＵＥ１０２のためのＥＰＣ１１０へのアクセスポイントを提供する。ＵＥ１０２の例は、セルラ式電話、スマートフォン、セッション開始プロトコル（ＳＩＰ）電話、ラップトップ、携帯情報端末（ＰＤＡ）、衛星ラジオ、全地球測位システム、マルチメディアデバイス、ビデオデバイス、デジタルオーディオプレイヤ（例えば、ＭＰ３プレイヤ）、カメラ、ゲーム機、タブレット、またはあらゆる他の同様に機能するデバイスを含む。ＵＥ１０２はまた、モバイル局、加入者局、モバイルユニット、加入者ユニット、ワイヤレスユニット、遠隔ユニット、モバイルデバイス、ワイヤレスデバイス、ワイヤレス通信デバイス、遠隔デバイス、モバイル加入者局、アクセス端末、モバイル端末、ワイヤレス端末、遠隔端末、ハンドセット、ユーザエージェント、モバイルクライアント、クライアント、または何らかの他の適した専門用語としても当業者によって称されうる。

【００１５】

[0030] ｅＮＢ１０６は、ＥＰＣ１１０に接続される。ＥＰＣ１１０は、モビリティ管理エンティティ（ＭＭＥ）１１２、他のＭＭＥ１１４、サービングゲートウェイ１１６、マルチメディアブロードキャストマルチキャストサービス（ＭＢＭＳ）ゲートウェイ１２４、ブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）１２６、およびパケットデータネットワーク（ＰＤＮ）ゲートウェイ１１８を含む。ＭＭＥ１１２は、ＵＥ１０２とＥＰＣ１１０との間のシグナリングを処理する制御ノードである。概して、ＭＭＥ１１２はベアラおよび接続管理を提供する。全てのユーザＩＰパケットは、自身がＰＤＮゲートウェイ１１８に接続されているサービングゲートウェイ１１６を通って転送される。ＰＤＮゲートウェイ１１８は、ＵＥ　ＩＰアドレス割り振り、ならびに他の機能を提供する。ＰＤＮゲートウェイ１１８は、オペレータのＩＰサービス１２２に接続される。オペレータのＩＰサービス１２２は、インターネット、イントラネット、ＩＰマルチメディアサブシステム（ＩＭＳ）、およびＰＳストリーミングサービス（ＰＳＳ）を含むことができる。ＢＳ－ＳＣ１２６は、ＭＢＭＳユーザサービスプロビジョニングおよび配信のための機能を提供することができる。ＢＭ－ＳＣ１２６は、コンテンツプロバイダＭＢＭＳ送信のためのエントリポイントとして役目をし、ＰＬＭＮ内のＭＢＭＳベアラサービスを認証および開始するために使用され、ＭＢＭＳ送信をスケジュールおよび配信するために使用されうる。ＭＢＭＳゲートウェイ１２４は、特定のサービスをブロードキャストするマルチキャストブロードキャスト単一周波数ネットワーク（ＭＢＳＦＮ）エリアに属するｅＮＢ（例えば、１０６、１０８）にＭＢＭＳトラフィックを分配するために使用され、セッション管理（開始／停止）およびｅＭＢＭＳ関連課金情報を集めることを担いうる。

【００１６】

[0031] 図２は、ＬＴＥネットワークアーキテクチャにおけるアクセスネットワーク２０

０の例を例示する図である。この例では、アクセスネットワーク２００が、多数のセルラ領域（セル）２０２に分割されている。１つまたは複数のより低い電力クラスのｅＮＢ２０８は、セル２０２のうちの１つまたは複数と重複するセルラ領域２１０を有することができる。より低い電力クラスｅＮＢ２０８は、フェムトセル（例えば、ホームｅＮＢ（ＨｅＮＢ））、ピコセル、マクロセル、または遠隔無線ヘッド（ＲＲＨ）でありうる。マクロｅＮＢ２０４は、それぞれ、各セル２０２に割り当てられ、セル２０２内の全てのＵＥ２０６にＥＰＣ１１０へのアクセスポイントを提供するように構成されている。アクセスネットワーク２００のこの例には中央コントローラ（ｃｅｎｔｒａｌｉｚｅｄ ｃｏｎｔｒｏｌｌｅｒ）が存在しないけれども、代わりの構成では、中央コントローラが使用されうる。ｅＮＢ２０４は、無線ベアラ制御、アドミッション制御、モビリティ制御、スケジューリング、安全性、およびサービングゲートウェイ１１６への接続を含む、全ての無線関連機能を担う。ｅＮＢは、（セクタとしても称される）１つまたは複数（例えば、３つ）のセルをサポートすることができる。「セル」という用語は、ｅＮＢの最も小さいカバレッジエリアを称し、ならびに／もしくは、ｅＮＢサブシステムサービング（ｅＮＢ ｓｕｂｓｙｓｔｅｍ ｓｅｒｖｉｎｇ）は、特定のカバレッジエリアである。さらに、用語「ｅＮＢ」、「基地局」および「セル」は、ここで交換可能に使用されることができる。

【００１７】

[0032] アクセスネットワーク２００によって用いられる変調および多元接続スキームは、展開されている特定の電気通信規格に依存して異なりうる。ＬＴＥアプリケーションでは、周波数分割デュプレックス（ＦＤＤ）および時分割デュプレックス（ＴＤＤ）の両方をサポートするために、ＯＦＤＭはＤＬ上で使用され、ＳＣ－ＦＤＭＡはＵＬ上で使用される。以下に続く詳細な説明から当業者が容易に認識することになるように、ここで示される様々な概念はＬＴＥアプリケーションに良好に適合される。しかしながら、これらの概念は、他の変調および複数のアクセス技法を用いる他の電気通信標準規格に容易に拡張されうる。例として、これらの概念は、エボリューションデータオプティマイズド（ＥＶ－ＤＯ）またはウルトラモバイルブロードバンド（ＵＭＢ）に拡張されることができる。ＥＶ－ＤＯおよびＵＭＢは、ＣＤＭＡ２０００ファミリの規格の一部として第３世代パートナーシッププロジェクト２（３ＧＰＰ２）によって発表されたエアインターフェース規格であり、モバイル局にブロードバンドインターネットアクセスを提供するためにＣＤＭＡを用いる。これらの概念はまた、広帯域ＣＤＭＡ（Ｗ－ＣＤＭＡ（登録商標））、およびＴＤ－ＳＣＤＭＡのようなＣＤＭＡの他の変形例を用いるユニバーサル地上無線アクセス（ＵＴＲＡ）、ＴＤＭＡを用いる移動体通信のための全世界システム（ＧＳＭ（登録商標））、ＯＦＤＭＡを用いる、発展型ＵＴＲＡ（Ｅ－ＵＴＲＡ）、ＩＥＥＥ８０２．１１（Ｗｉ－Ｆｉ）、ＩＥＥＥ８０２．１６（ＷｉＭＡＸ）、ＩＥＥＥ８０２．２０、およびフラッシュＯＦＤＭに拡張されることもできる。ＵＴＲＡ、Ｅ－ＵＴＲＡ、ＵＭＴＳ、ＬＴＥ、およびＧＳＭは、３ＧＰＰの組織による文書において説明されている。ＣＤＭＡ２０００およびＵＭＢは、３ＧＰＰ２の組織による文書において説明されている。用いられる実際のワイヤレス通信規格および多元接続技術は、システムに課された全体的な設計の制約および指定のアプリケーションに依存するだろう。

【００１８】

[0033] ｅＮＢ２０４は、ＭＩＭＯ技術をサポートする複数のアンテナを有することができる。ＭＩＭＯ技術の使用は、ｅＮＢ２０４が、空間多重化、ビームフォーミング、および送信ダイバーシティをサポートするために空間領域を利用できるようにする。空間多重化は、同じ周波数上で同時にデータの異なるストリームを送信するために使用されうる。データストリームは、データレートを増加させるために単一のＵＥ２０６に、または、全体的なシステム容量を増加させるために複数のＵＥ２０６に、送信されうる。これはそれぞれのデータストリームを空間的にプリコーディングし（つまり、振幅および位相のスケーリングを適用し）、その後ＤＬ上の複数の送信アンテナを通じてそれぞれの空間的にプリコーディングされたストリームを送信することによって達成される。空間的にプリコーディングされたデータストリームは、異なる空間シグネチャとともに（１つまたは複数の

）ＵＥ２０６に到達し、このことは、（１つまたは複数の）ＵＥ２０６のそれぞれが、そのＵＥ２０６に宛てられた１つまたは複数のデータストリームを復元できるようにする。ＵＬ上では、それぞれのＵＥ２０６は、空間的にプリコーディングされたデータストリームを送信し、このことは、ｅＮＢ２０４が、それぞれの空間的にプリコーティングされたデータストリームのソースを識別できるようにする。

【００１９】

[0034] 空間多重化は概して、チャネル状況が良好なときに使用される。チャネル状況がさほど好ましくないときには、１つまたは複数の方向に送信エネルギーの焦点を当てるためにビームフォーミングが使用されうる。これは、複数のアンテナを通じた送信のためにデータを空間的にプリコーディングすることによって、達成されることができる。セルの端で良好なカバレッジを達成するために、単一のストリームのビームフォーミング送信が送信ダイバーシティと組み合わせて使用されうる。

【００２０】

[0035] 以下に続く詳細な説明では、アクセスネットワークの様々な態様は、ＤＬ上でＯＦＤＭをサポートするＭＩＭＯシステムを参照して説明されることになる。ＯＦＤＭは、ＯＦＤＭシンボル内の多数のサブキャリアにわたってデータを変調する拡散スペクトル技法である。サブキャリアは、精確な周波数で間隔が空けられている。間隔を空けることは、受信機がサブキャリアからデータを復元できるようにする、「直交性」を提供する。時間ドメインでは、ＯＦＤＭシンボル間干渉を抑制するために、それぞれのＯＦＤＭシンボルにガードインターバル（例えば、サイクリックプリフィクス）が追加されうる。ＵＬは、高いピーク対平均電力比（ＰＡＰＲ）を補償するために、ＤＦＴ拡散ＯＦＤＭ信号の形態でＳＣ－ＦＤＭＡを使用することができる。

【００２１】

[0036] 図３は、ＬＴＥにおけるＤＬフレーム構造の例を例示する図３００である。フレーム（１０ｍｓ）は、１０つの等しいサイズのサブフレームに分割されうる。それぞれのサブフレームは、２つの連続するタイムスロットを含むことができる。リソースグリッドが２つのタイムスロットを表すために使用されることができ、それぞれのタイムスロットは、リソースブロックを含む。リソースグリッドは、複数のリソース要素に分割される。ＬＴＥでは、リソースブロックは、周波数ドメインにおいて１２つの連続するサブキャリア、およびそれぞれのＯＦＤＭシンボルにおける通常のサイクリックプリフィクスでは、時間ドメインにおいて７つの連続するＯＦＤＭシンボルを含み、すなわち、８４つのリソース要素を含む。拡張されたサイクリックプリフィックスでは、リソースブロックは、時間ドメインにおいて６つの連続するＯＦＤＭシンボルを含み、７２つのリソース要素を有する。Ｒ３０２、３０４として表示されている、リソース要素のいくつかは、ＤＬ基準信号（ＤＬ－ＲＳ）を含む。ＤＬ－ＲＳは、セル固有のＲＳ（ＣＲＳ）（時折共通ＲＳとも呼ばれる）３０２、およびＵＥ固有のＲＳ（ＵＥ－ＲＳ）３０４を含む。ＵＥ－ＲＳ３０４は、対応する物理ＤＬ共有チャネル（ＰＤＳＣＨ）がマッピングされているリソースブロック上のみで送信される。それぞれのリソース要素によって搬送されるビットの数は、変調スキームに依存する。したがって、ＵＥが受信するリソースブロックが多いほど、また、変調スキームが高度であるほど、そのＵＥのためのデータレートは高くなる。

【００２２】

[0037] 図４は、ＬＴＥにおけるＵＬフレーム構造の例を例示する図４００である。ＵＬのための利用可能なリソースブロックは、データセクションおよび制御セクションに区分されることができる。制御セクションは、システム帯域幅の両端に形成されることができ、設定可能なサイズを有することができる。制御セクションにおけるリソースブロックは、制御情報の送信のためにＵＥに割り当てられることができる。データセクションは、制御セクションに含まれない全てのリソースブロックを含むことができる。ＵＬフレーム構造は、結果として連続するサブキャリアを含むデータセクションをもたらし、このことは、単一のＵＥがデータセクションにおける連続するサブキャリアの全てを割り当てられることを可能にしうる。

【００２３】
[0038] ＵＥは、ｅＮＢに制御情報を送信するために、制御セクションにおけるリソースブロック４１０ａ、４１０ｂを割り当てられうる。ＵＥはまた、ｅＮＢにデータを送信するために、データセクションにおけるリソースブロック４２０ａ、４２０ｂを割り当てられうる。ＵＥは、制御セクションにおける割り当てられたリソースブロック上で、物理ＵＬ制御チャネル（ＰＵＣＣＨ）において、制御情報を送信することができる。ＵＥは、データセクションにおける割り当てられたリソースブロック上で、物理ＵＬ共有チャネル（ＰＵＳＣＨ）において、データのみ、またはデータと制御情報の両方を送信することができる。ＵＬ送信は、サブフレームの両方のスロットにわたることができ、周波数にわたってホッピングする（ｈｏｐ）ことができる。

【００２４】
[0039] リソースブロックのセットは、物理ランダムアクセスチャネル（ＰＲＡＣＨ）４３０において、初期システムアクセスを行い、ＵＬ同期を達成するために使用されうる。ＰＲＡＣＨ４３０は、ランダムシーケンスを搬送し、いずれのＵＬデータ／シグナリングも搬送することはできない。それぞれのランダムアクセスプリアンブルは、６つの連続するリソースブロックに対応する帯域幅を占有する。始めの周波数は、ネットワークによって指定される。つまり、ランダムアクセスプリアンブルの送信は、ある特定の時間および周波数リソースに制限される。ＰＲＡＣＨのためにホッピングする周波数は存在しない。ＰＲＡＣＨの試みは、単一のサブフレーム（１ｍｓ）において、またはいくつかの連続するサブフレームのシーケンスにおいて搬送され、ＵＥは、フレーム（１０ｍｓ）毎に単一のＰＲＡＣＨの試みのみを行うことができる。

【００２５】
[0040] 図５は、ＬＴＥにおけるユーザおよび制御プレーンのための無線プロトコルアーキテクチャの例を示す図５００である。ＵＥおよびｅＮＢのための無線プロトコルアーキテクチャは、レイヤ１、レイヤ２、およびレイヤ３の３つのレイヤで図示されている。レイヤ１（Ｌ１レイヤ）は、最下位のレイヤであり、様々な物理レイヤの信号処理機能をインプリメントする。Ｌ１レイヤは、ここでは物理レイヤ５０６として称されることになる。レイヤ２（Ｌ２レイヤ）５０８は、物理レイヤ５０６よりも上位であり、物理レイヤ５０６をわたったＵＥとｅＮＢとの間のリンクを担う。

【００２６】
[0041] ユーザプレーンでは、Ｌ２レイヤ５０８は、媒体アクセス制御（ＭＡＣ）サブレイヤ５１０、無線リンク制御（ＲＬＣ）サブレイヤ５１２、およびパケットデータコンバージェンスプロトコル（ＰＤＣＰ）５１４サブレイヤを含み、それらは、ネットワーク側のｅＮＢで終端とされる。図示されていないけれども、ＵＥは、ネットワーク側のＰＤＮゲートウェイ１１８で終端とされるネットワークレイヤ（例えば、ＩＰレイヤ）、および接続のもう一方の端（例えば、遠端のＵＥ、サーバ、等）で終端とされるアプリケーションレイヤを含む、Ｌ２レイヤ５０８よりも上の、いくつかの上位レイヤを有することができる。

【００２７】
[0042] ＰＤＣＰサブレイヤ５１４は、異なる無線ベアラと論理チャネルとの間での多重化を提供する。ＰＤＣＰサブレイヤ５１４はまた、無線送信のオーバーヘッドを減じるための上位レイヤのデータパケットに関するヘッダ圧縮、データパケットを暗号化することによる安全性、ｅＮＢ間でのＵＥのためのハンドオーバーサポートを提供する。ＲＬＣサブレイヤ５１２は、上位レイヤのデータパケットのセグメンテーションおよびリアセンブリ、損失データパケットの再送、およびハイブリッド自動再送要求（ＨＡＲＱ）による、順序が乱れた受信を補償するためのデータパケットの並び替えを提供する。ＭＡＣサブレイヤ５１０は、論理チャネルとトランスポートチャネルの間で多重化を提供する。ＭＡＣサブレイヤ５１０はまた、１つのセルにおける様々な無線リソース（例えば、リソースブロック）をＵＥの間で割り振ることを担う。ＭＡＣサブレイヤ５１０はまた、ＨＡＲＱ演算を担う。

【００２８】
[0043] 制御プレーンにおいて、ＵＥおよびｅＮＢのための無線プロトコルアーキテクチャは、制御プレーンではヘッダ圧縮機能が存在しないという点を除き、物理レイヤ５０６およびＬ２レイヤ５０８に関しては実質的に同一である。制御プレーンはまた、レイヤ３（Ｌ３　レイヤ）において無線リソース制御（ＲＲＣ）サブレイヤ５１６を含む。ＲＲＣサブレイヤ５１６は、無線リソース（例えば、無線ベアラ）を得ること、およびｅＮＢとＵＥとの間でのＲＲＣシグナリングを使用してより下位のレイヤを構成することとを担う。
【００２９】
[0044] 図６は、アクセスネットワークにおいてＵＥ６５０と通信するｅＮＢ６１０のブロック図である。ＤＬでは、コアネットワークから、上位レイヤのパケットが、コントローラ／プロセッサ６７５に提供される。コントローラ／プロセッサ６７５は、Ｌ２レイヤの機能をインプリメントする。ＤＬにおいて、コントローラ／プロセッサ６７５は、ヘッダ圧縮、暗号化、パケットセグメンテーションおよび並び替え、論理チャネルとトランスポートチャネルとの間での多重化、ならびに様々な優先順位メトリックに基づいたＵＥ６５０への無線リソース割り振りを提供する。コントローラ／プロセッサ６７５はまた、ＨＡＲＱ演算、損失パケットの再送、ＵＥ６５０へのシグナリングを担う。
【００３０】
[0045] 送信（ＴＸ）プロセッサ６１６は、Ｌ１レイヤ（つまり、物理レイヤ）のための様々な信号処理機能をインプリメントする。信号処理機能は、ＵＥ６５０における前方誤り訂正（ＦＥＣ）を容易にするようにコード化およびインターリーブすること、ならびに様々な変調スキーム（例えば、２相位相変調（ＢＰＳＫ）、４相位相変調（ＱＰＳＫ）、Ｍ相位相変調（Ｍ－ＰＳＫ）、Ｍ値直交振幅変調（Ｍ－ＱＡＭ））に基づいて信号コンステレーションにマッピングすることを含む。コード化および変調されたシンボルは、その後、並行なストリームに分けられる。それぞれのストリームは、その後、時間ドメインのＯＦＤＭシンボルストリームを搬送する物理チャネルを作り出すために、ＯＦＤＭサブキャリアにマッピングされ、時間および／または周波数ドメインにおいて基準信号（例えば、パイロット）とともに多重化され、そして、逆高速フーリエ変換（ＩＦＦＴ）を使用してともに合成される。ＯＦＤＭストリームは、複数の空間ストリームを作り出すために空間的にプリコーディングされる。チャネル推定器６７４からのチャネル推定値は、コード化および変調スキームを決定するために、さらには空間処理のために、使用されうる。チャネル推定値は、ＵＥ６５０によって送信された基準信号および／またはチャネル状況フィードバックから導出されうる。それぞれの空間ストリームは、その後、別個の送信機６１８ＴＸを介して異なるアンテナ６２０に提供されうる。それぞれの送信機６１８ＴＸは、ＲＦキャリアを、送信のために各空間ストリームで変調することができる。
【００３１】
[0046] ＵＥ６５０において、それぞれの受信機６５４ＲＸは、その各アンテナ６５２を通じて、信号を受信する。それぞれの受信機６５４ＲＸは、ＲＦキャリア上に変調された情報を復元し、受信（ＲＸ）プロセッサ６５６に情報を提供する。ＲＸプロセッサ６５６はＬ１レイヤの様々な信号処理機能をインプリメントする。ＲＸプロセッサ６５６は、ＵＥ６５０に宛てられた任意の空間ストリームを復元するために、情報に対して空間処理を行うことができる。複数の空間ストリームがＵＥ６５０に宛てられている場合、それらは、ＲＸプロセッサ６５６によって単一のＯＦＤＭシンボルストリームに合成されうる。ＲＸプロセッサ６５６は、その後、高速フーリエ変換（ＦＦＴ）を使用して、ＯＦＤＭシンボルストリームを時間ドメインから周波数ドメインに変換する。周波数ドメイン信号は、ＯＦＤＭ信号のサブキャリア毎に別個のＯＦＤＭシンボルストリームを備える。それぞれのサブキャリア上のシンボル、および基準信号は、ｅＮＢ６１０によって送信された最も確からしい信号コンステレーションポイントを決定することによって、復元および復調される。軟判定は、チャネル推定器６５８によって計算されたチャネル推定値に基づきうる。これらの軟判定は、その後、物理チャネル上でｅＮＢ６１０によって元々送信されたデ

ータおよび制御信号を復元するために、復号およびデインターリーブされる。データおよび制御信号は、その後、コントローラ／プロセッサ６５９に提供される。

【００３２】

[0047] コントローラ／プロセッサ６５９は、Ｌ２レイヤをインプリメントする。コントローラ／プロセッサは、プログラムコードおよびデータを記憶するメモリ６６０に関連付けられうる。メモリ６６０は、コンピュータ可読媒体として称されうる。ＵＬにおいて、コントローラ／プロセッサ６５９は、コアネットワークからの上位レイヤパケットを復元するためにトランスポートチャネルと論理チャネルとの間での逆多重化、パケットリアセンブリ、解読、ヘッダ圧縮解除（ｄｅｃｏｍｐｒｅｓｓｉｏｎ）、制御信号処理を提供する。上位レイヤパケットは、その後、データシンク６６２に提供され、それは、Ｌ２レイヤより上位の全てのプロトコルレイヤを表す。様々な制御信号もまた、Ｌ３処理のために、データシンク６６２に提供されることができる。コントローラ／プロセッサ６５９はまた、ＨＡＲＱ演算をサポートするための肯定応答（ＡＣＫ）および／または否定応答（ＮＡＣＫ）プロトコルを使用する誤り検出も担う。

【００３３】

[0048] ＵＬでは、データソース６６７は、コントローラ／プロセッサ６５９に上位レイヤパケットを提供するために使用される。データソース６６７は、Ｌ２レイヤより上位の全てのプロトコルレイヤを表す。ｅＮＢ６１０によるＤＬ送信に関係して説明された機能と同様に、コントローラ／プロセッサ６５９は、ヘッダ圧縮、暗号化、パケットセグメンテーションおよび並び替え、ならびにｅＮＢ６１０による無線リソースの割り当てに基づいた論理チャネルとトランスポートチャネルとの間での多重化を提供することによって、ユーザプレーンおよび制御プレーンのためのＬ２レイヤを実現する。コントローラ／プロセッサ６５９はまた、ＨＡＲＱ演算、損失パケットの再送、ｅＮＢ６１０へのシグナリングを担う。

【００３４】

[0049] ｅＮＢ６１０によって送信された基準信号またはフィードバックからチャネル推定器６５８によって導出されたチャネル推定値は、適切なコード化および変調スキームを選択し、空間処理を容易にするために、ＴＸプロセッサ６６８によって使用されうる。ＴＸプロセッサ６６８によって生成された空間ストリームは、別個の送信機６５４ＴＸを介して異なるアンテナ６５２に提供されうる。それぞれの送信機６５４ＴＸは、ＲＦキャリアを、送信のために各空間ストリームで変調することができる。

【００３５】

[0050] ＵＬ送信は、ＵＥ６５０における受信機機能に関係して説明された手法と同様の手法で、ｅＮＢ６１０において処理される。それぞれの受信機６１８ＲＸは、その各アンテナ６２０を通じて、信号を受信する。それぞれの受信機６１８ＲＸは、ＲＦキャリア上に変調された情報を復元し、ＲＸプロセッサ６７０に情報を提供する。ＲＸプロセッサ６７０は、Ｌ１レイヤをインプリメントすることができる。

【００３６】

[0051] コントローラ／プロセッサ６７５は、Ｌ２レイヤをインプリメントする。コントローラ／プロセッサ６７５は、プログラムコードおよびデータを記憶するメモリ６７６に関係付けられることができる。メモリ６７６は、コンピュータ可読媒体として称されうる。ＵＬにおいて、制御／プロセッサ６７５は、ＵＥ６５０から上部レイヤパケットを復元するためにトランスポートチャネルと論理チャネルとの間の逆多重化、パケットリアセンブリ、解読、ヘッダ圧縮解除、制御信号処理を提供する。コントローラ／プロセッサ６７５からの上部レイヤパケットはコアネットワークに提供されうる。コントローラ／プロセッサ６７５はまた、ＨＡＲＱ動作をサポートするためのＡＣＫ、および／またはＮＡＣＫプロトコルを使用する誤り検出を担う。

【００３７】

[0052] 図７Ａは、ＭＢＳＦＮにおける発展型ＭＢＭＳ（ｅＭＢＭＳ）チャネル構成の例を例示する図７５０である。セル７５２’におけるｅＮＢ７５２は、第１のＭＢＳＦＮエ

リアを形成することができ、セル７５４’におけるｅＮＢ７５４は、第２のＭＢＳＦＮエリアを形成することができる。ｅＮＢ７５２、７５４はそれぞれ、例えば合計８つのＭＢＳＦＮエリアまで、他のＭＢＳＦＮエリアに関連付けられうる。ＭＢＳＦＮエリア内のセルは、未使用のセルと指示されうる。未使用のセルは、マルチキャスト／ブロードキャストコンテンツを提供しないけれども、セル７５２’、７５４’に時間同期され、ＭＢＳＦＮエリアへの干渉を限定するためにＭＢＳＦＮリソース上に制限された電力を有する。ＭＢＳＦＮエリアにおけるそれぞれのｅＮＢは、同じｅＭＢＭＳ制御情報およびデータを同時に送信する。それぞれのエリアは、ブロードキャスト、マルチキャスト、およびユニキャストサービスをサポートすることができる。ユニキャストサービスは、指定のユーザを対象としたサービス、例えばボイスコール、である。マルチキャストサービスは、ユーザのグループによって受信されうるサービス、例えば加入者ビデオサービス、である。ブロードキャストサービスは、全てのユーザによって受信されうるサービス、例えばニュースブロードキャスト、である。図７Ａを参照すると、第１のＭＢＳＦＮエリアは、例えばＵＥ７７０に特定のニュースブロードキャストを提供することによって、第１のｅＭＢＭＳブロードキャストサービスをサポートすることができる。第２のＭＢＳＦＮエリアは、例えばＵＥ７６０に異なるニュースブロードキャストを提供することによって、第２のｅＭＢＭＳブロードキャストサービスをサポートすることができる。それぞれのＭＢＳＦＮエリアは、複数の物理マルチキャストチャネル（ＰＭＣＨ）（例えば、１５つのＰＭＣＨ）をサポートする。それぞれのＰＭＣＨは、マルチキャストチャネル（ＭＣＨ）に対応する。それぞれのＭＣＨは、複数（例えば２９つ）のマルチキャスト論理チャネルを多重化することができる。それぞれのＭＢＳＦＮエリアは、１つのマルチキャスト制御チャネル（ＭＣＣＨ）を有することができる。このように、１つのＭＣＨは、１つのＭＣＣＨおよび複数のマルチキャストトラフィックチャネル（ＭＴＣＨ）を多重化することができ、残りのＭＣＨは複数のＭＴＣＨを多重化することができる。

【００３８】

[0053] ＵＥは、ｅＭＢＭＳサービスアクセスの利用可能性および対応するアクセス層構成を発見するためのＬＴＥセルにキャンプオンする（ｃａｍｐ　ｏｎ）ことができる。第１のステップでは、ＵＥは、システム情報ブロック（ＳＩＢ）１３（ＳＩＢ１３）を獲得することができる。第２のステップでは、ＳＩＢ１３に基づいて、ＵＥは、ＭＣＣＨ上でＭＢＳＦＮエリア構成メッセージを獲得することができる。第３のステップでは、ＭＢＳＦＮエリア構成メッセージに基づいて、ＵＥは、ＭＣＨスケジューリング情報（ＭＳＩ）ＭＡＣ制御要素を獲得することができる。ＳＩＢ１３は、（１）セルによってサポートされるそれぞれのＭＢＳＦＮエリアのＭＢＳＦＮエリア識別子、（２）ＭＣＣＨ繰り返し周期（例えば、３２、６４、…２５６フレーム）、ＭＣＣＨオフセット（例えば、０、１、…１０フレーム）、ＭＣＣＨ変更周期（例えば、５１２、１０２４フレーム）、シグナリング変調およびコード化スキーム（ＭＣＳ）、繰り返し周期およびオフセットによって表示されているような無線フレームのどのサブフレームがＭＣＣＨを送信することができるかを表示するサブフレーム割り当て情報、のようなＭＣＣＨを獲得するための情報、および（３）ＭＣＣＨ変化通知構成を表示する。ＭＢＳＦＮエリア毎に１つのＭＢＳＦＮエリア構成メッセージが存在する。ＭＢＳＦＮエリア構成メッセージは、（１）ＰＭＣＨ内の論理チャネル識別子によって識別されるそれぞれのＭＴＣＨの一時的なモバイルグループ識別子（ｔｅｍｐｏｒａｔｙ　ｍｏｂｉｌｅ　ｇｒｏｕｐ　ｉｄｅｎｔｉｆｙ（ＴＭＧＩ））および任意のセッション識別子、（２）ＭＢＳＦＮエリアのそれぞれのＰＭＣＨを送信するための割り当てられたリソース（つまり、無線フレームおよびサブフレーム）およびエリア内の全てのＰＭＣＨのための割当てられたリソースの割り当て周期（例えば、４、８、…２５６フレーム）、ならびに（３）ＭＳＩ　ＭＡＣ制御要素が送信されるＭＣＨスケジューリング周期（ＭＳＰ）（例えば、８、１６、３２、…または１０２４無線フレーム）を表示する。

【００３９】

[0054] 図７Ｂは、ＭＳＩ　ＭＡＣ制御要素のフォーマットを例示する図７９０である。

ＭＳＩ　ＭＡＣ制御要素はＭＳＰ毎に一度送られうる。ＭＳＩ　ＭＡＣ制御要素は、ＰＭＣＨの各スケジューリング周期の第１のサブフレームで送られうる。ＭＳＩ　ＭＡＣ制御要素は、ＰＭＣＨ内の各ＭＴＣＨの停止フレームおよびサブフレームを表示することができる。ＭＢＳＦＮエリア毎のＰＭＣＨ毎に１つのＭＳＩが存在しうる。

【００４０】

[0055] ＵＥ（つまり、ＭＢＭＳ受信機）は、ＭＢＭＳユーザサービス発見／アナウンスメントを受信することができる。ユーザサービス発見／アナウンスメントは、サービス説明情報および受信報告構成を含む。受信報告構成は、ＵＥがＭＢＭＳ受信報告を送ることができる１つまたは複数のサーバユニフォームリソースロケータ（ＵＲＬ）を含むことができる。ＭＢＭＳダウンロード配信では、受信報告が、１つまたは複数のファイルの完全な受信を報告する、および／またはダウンロード配信上で統計を報告するために使用される。ＭＢＭＳストリーミング配信では、受信報告は、ストリーミング配信上で統計を報告するために使用される。ＵＥは、報告タイプに基づく受信報告における情報を含む。報告タイプは、受信肯定応答（ＲＡｃｋ）、成功した受信に関する統計報告（ＳｔａＲ）、全てのコンテンツ受信に関する統計報告（ＳｔａＲ－ａｌｌ）、および受信肯定応答を有さない統計報告（ＳｔａＲ－ｏｎｌｙ）を含む。ＵＥが、コンテンツ項目の完全な受信、またはセッションの完了を識別するとき、ＵＥは、受信報告が必要とされるかどうかを決定する。ＵＥは、受信報告構成における受信されたサンプル割合属性に基づいて受信報告を送るべきかどうかを決定することができる。ＵＥは、受信報告を含む受信報告要求を送るべき時間を選択し、受信報告要求を送るべきリストからサーバを選択する。ＵＥは、ランダムに、ならびに均等に分配されたサーバおよび時間を選択する。ＵＥはその後、ハイパーテキストトランスファープロトコル（ＨＴＴＰ）ポスト動作を通じてサーバに受信報告要求を送る。ＵＥは続いて、ＨＴＴＰ応答動作を通じてサーバから受信報告応答を受信する。

【００４１】

[0056] 現在、受信報告およびユーザサービス発見／アナウンスメントは保護されていない。受信報告は、ユーザまたはネットワークに関連する感知情報を含むことができる。例えば、受信報告は、ＵＥが受信するコンテンツ、およびＵＥがコンテンツを受信するロケーションを識別する情報を含むことができる。別の例では、受信報告は、ネットワークトポロジ情報（例えば、セルＩＤ等）、および無線リンク情報（例えば、ＭＢＳＦＮ基準信号受信電力（ＲＳＲＰ）、基準信号受信品質（ＲＳＲＱ）、および／または信号対干渉プラス雑音比（ＳＩＮＲ）情報）を含むことができる。さらに、ユーザサービス発見／アナウンスメントは、感知データフィールドを含むことができ、および／または、不正サーバ（ｒｏｇｕｅ　ｓｅｖｅｒ）（例えば、サービスプロバイダに関連付けられていないサーバ）に受信報告を送ることをＵＥに行わせる不正ユーザサービス発見／アナウンスメントをＵＥに受信させることを通じた改ざんを被りうる。安全な受信報告およびユーザサービス発見／アナウンスメントの安全な受信のための方法、コンピュータプログラム製品、装置が以下で提供される。

【００４２】

[0057] 図８は、安全な受信報告を送るための第１の実例となる方法を例示する図８００である。図８で図示されているように、ステップ８１０では、ＵＥ８０２は、サービスプロバイダ８０８から、信頼される認証局リストを受信することができる。別の構成では、ステップ８１０は行われず、ステップ８１１において、ＵＥ８０２が、ブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）８０６から信頼される認証局リストを受信することができる。信頼される認証局リストは、信頼される認証局の証明書を含む。信頼される認証局は、証明書を提供したサーバとの安全な接続をセットアップするための証明書をＵＥ８０２が信頼することができる局（ａｕｔｈｏｒｉｔｙ）である。信頼される認証局リストは、ＵＥ８０２およびサービスプロバイダ８０８／ＢＭ－ＳＣ８０６によって知られている認証情報に基づいて暗号化および／または完全性保護されうる。認証情報は、ＵＥ８０２におけるスマートカード上に記憶されうる。認証情報は、ＵＥ８０２および

サービスプロバイダ８０８／ＢＭ－ＳＣ８０６にのみ知られている共有キーでありうる。そのような共有キーの例は、（例えば、ユニバーサル集積回路カード（ＵＩＣＣ）スマートカード上のユニバーサル加入者識別モジュール（ＵＳＩＭ）アプリケーション上の）サービスプロバイダへのＵＥの加入に基づいてサービスプロバイダ８０８／ＢＭ－ＳＣ８０６およびＵＥ８０２に知られているルートキー（例えば、ワイヤレスアクセス認証のために使用されるルートキーである、Ｋｉ）から導出されるあらゆるキーを含む。そのような導出されるキーの例は、ＭＢＭＳユーザキー（ＭＵＫ）、ＭＢＭＳ要求キー（ＭＲＫ）、ＭＵＫまたはＭＲＫから導出されるキー、または共有キーから導出されるあらゆる他のキーに限定されないけれども、含む。信頼される認証局リストを完全性保護するために、信頼される認証局リストは、（ハッシュコード、ハッシュサム、チェックコード、またはハッシュとしても知られる）ハッシュ値を得るために、（ＭＵＫまたはＭＲＫのような共有キーの関数でありうる）ハッシュベースメッセージ認証コード（ＨＭＡＣ）のようなキーのある（keyed）ハッシュ関数を通じて認証情報を使用してハッシュされることができ、ハッシュ値は、ＵＥ８０２が、信頼される認証局リスト内のフィールドが完全性保護から変更されているかどうかをチェックすることができるように、信頼される認証局リスト内に含まれうる。

【００４３】

[0058] ステップ８１２では、ＵＥ８０２は、ＢＭ－ＳＣ８０６からユーザサービス発見／アナウンスメントを受信することができる。ユーザサービス発見／アナウンスメントは、１つまたは複数の受信報告構成およびＵＥが受信報告を送ることができるサーバの１つまたは複数のアドレスを含むことができる。１つの例では、ユーザサービス発見／アナウンスメントは、第１の受信報告構成と安全でない受信報告を送るための保証されていないサーバＵＲＬ、および第２の受信報告構成および安全な受信報告を送るための保証されたサーバＵＲＬを含む。保証されていないサーバＵＲＬは、ＨＴＴＰを通じて受信報告を送るためのＵＲＬでありうる。保証されたサーバＵＲＬは、ＨＴＴＰセキュア（ＨＴＴＰＳ）（例えば、トランスポートレイヤセキュリティ（ＴＬＳ）プロトコルを用いたＨＴＴＰ）を通じて受信報告を送るためのＵＲＬでありうる。ユーザサービス発見／アナウンスメントはそれ自体が、ＵＥ８０２およびＢＭ－ＳＣ８０６によって知られている認証情報に基づいて、完全性保護および／または暗号化されうる。認証情報は、ＵＥ８０２におけるスマートカード上に記憶されうる。認証情報は、ユーザサービス発見／アナウンスメントを受信するように認証されているＵＥのセットに知られているＭＢＭＳサービスキー（ＭＳＫ）またはＭＳＫから導出されたキーのようなグループ共有キーでありうる。代わりとして、グループ共有キーは、（例えば、オーバージエア（ｏｖｅｒ－ｔｈｅ－ａｉｒ）（ＯＴＡ）構成またはオープンモバイルアライアンスデバイス管理（ＯＭＡ－ＤＭ）構成プロトコルのようなあらゆる構成メカニズムを使用して、）ＵＥ上で予め構成されうる。

【００４４】

[0059] ステップ８１４では、ＵＥ８０２は、受信報告を送るべきかどうか、ならびに感知受信報告情報が受信報告に含まれうるかどうかを決定する。ステップ８１４は、ＵＥ８０２が、ＭＢＭＳコンテンツ項目の完全な受信またはＭＢＭＳセッションの完了を識別した後に生じうる。ステップ８１６では、ＵＥ８０２は報告時間およびサーバを選択する。ＵＥ８０２が、感知受信報告情報が受信報告に含まれないだろうことを決定する場合、ＵＥ８０２は、保証されていないサーバＵＲＬへの保証されていない接続を通じて受信報告を送ることを選択しうる。ＵＥ８０２が、感知受信報告情報が受信報告に含まれるだろうことを決定する場合、ＵＥ８０２は、保証されたサーバＵＲＬへの保証された接続を通じて受信報告を送ることを選択しうる。

【００４５】

[0060] ＵＥ８０２がサーバ８０４への保証された接続を通じて受信報告を送ることを選択することを仮定すると、ステップ８１８では、ＵＥ８０２はＨＴＴＰＳのセットアップを開始する。ステップ８１８で、ＵＥ８０２は、サーバ８０４の証明書を受信する。証明書は、Ｘ．５０９サーバ証明書でありうる。ＵＥ８０２が信頼される認証局リストを受信

していなかった（ステップ８１０またはステップ８１１が生じていなかった）場合、ステップ８２０で、ＵＥ８０２はサービスプロバイダ８０８から信頼される認証局リストを得る、あるいはステップ８２１でＵＥ８０２はＢＭ－ＳＣ８０６から信頼される認証局リストを得る。ステップ８２２では、ＵＥ８０２は、証明書が、（例えば、Ｘ．５０９サーバ証明書におけるｓｕｂｊｅｃｔＡｌｔＮａｍｅがユーザサービス発見／アナウンスメントにおけるサーバアドレスと同じであることを証明することによって）保証されたサーバＵＲＬによって識別されたサーバに属していることを証明し、受信された証明書が信頼される認証局リストに含まれているルート証明書に基づいて発行されたかどうかをチェックすることによって証明書を使用してサーバを認証する。サーバ認証は、ＵＥ８０２に、安全なサーバアドレスが改ざんされておらず、ＵＥが接続しているサーバが信頼を置けるものであるという保証を提供する。ステップ８２４では、ＵＥ８０２がサーバ８０４を認証することができる場合、ＵＥ８０２はサーバ８０４との安全な接続のセットアップを完了することを決定する。ＵＥ８０２はその後、サーバ８０４とのＨＴＴＰＳを通じた安全な接続のセットアップを完了する。ステップ８２６では、ＵＥ８０２は、対応する受信報告構成に基づいてＨＴＴＰＳ接続を通じて受信報告を送る。

【００４６】

[0061] ステップ８１８は、ステップ８１６の後に生じると図示されている。しかしながらステップ８１８はステップ８１４の前に生じることができる。ステップ８１０、８２０では、ＵＥは、サービスプロバイダ８０８から信頼される認証局リストを受信する。しかしながらステップ８１１、８２１では、信頼される認証局リストは、ＵＥ　ｅＭＢＭＳ登録手順の一部として、ＢＭ－ＳＣから、あるいはＵＥとサービスプロバイダとの間の別のユニキャストメカニズムを通じて、受信されうる。ＵＥ　ｅＭＢＭＳサービス登録手順の一部として信頼される認証局リストを得るために、ＵＥは、ＢＭ－ＳＣ８０６にＨＴＴＰポストメッセージを送ることができる。メッセージは、登録指示、ＭＢＭＳユーザサービスＩＤ、および認証局リストを求める要求を含むことができる。ＢＭ－ＳＣ８０６は、応答し、認証局リストを送ることができる。ＢＭ－ＳＣ８０６は、ＭＲＫ、ＭＵＫ、あるいはＭＲＫまたはＭＵＫのうちの１つから導出されたキーに基づいて認証局リストを完全性保護および／または暗号化することができる。別の構成では、信頼される認証局リストは、ＵＥ８０２上に予め構成されうる。例えば、予めの構成は、ｅＭＢＭＳ　ＯＴＡ構成またはデバイス管理の一部であることができ、あるいはサービスプロバイダ８０８の代わりに相手先商標製品製造会社（ｏｒｉｇｉｎａｌ　ｅｑｕｉｐｍｅｎｔ　ｍａｎｕｆａｃｔｕｒｅｒｓ）（ＯＥＭ）によって行われうる。

【００４７】

[0062] 図９は、安全な受信報告を送るための第２の実例となる方法を例示する図９００である。ステップ９０８では、サーバ９０４は、ＭＵＫまたはＭＲＫ、あるいはＭＵＫまたはＭＲＫから導出されたキーを、ＢＭ－ＳＣ９０６から受信する。ステップ９１０で、ＵＥ９０２は、ユーザサービス発見／アナウンスメントを受信する。ユーザサービス発見／アナウンスメントは、ＭＳＫまたは類似のグループキーに基づいて、完全性保護および／または暗号化されうる。ステップ９１２では、ＵＥ９０２は、受信報告を送るべきかどうか、ならびに受信報告が感知情報を含みうるかどうかを決定する。ステップ９１４では、ＵＥ９０２は受信報告を送るための報告時間を選択する。ステップ９１６では、ＵＥは、ＭＵＫまたはＭＲＫ、あるいはその導出されたキーに基づいて受信報告を完全性保護および／または暗号化する。ステップ９１８では、ＵＥは、サーバ９０４に保護された受信報告を送る。ユーザサービス発見／アナウンスメントを保護する判定が、受信報告を保護する判定から独立していることは留意されるべきである。

【００４８】

[0063] ＵＥ９０２は、ハッシュ値を得るためのハッシュ関数を通じて、受信報告または受信報告における１つまたは複数のフィールドをハッシュすることによって、受信報告を完全性保護することができる。ハッシュ関数はそれ自体、ＭＵＫまたはＭＲＫ、あるいはその導出されたキーの関数でありうる。ＵＥ９０２は、サーバ９０４に、受信報告でハッ

シュ値を送ることができる。代わりとして、あるいは加えて、ＵＥ９０２は、ＭＵＫまたはＭＲＫに基づいて（例えば、ＭＵＫまたはＭＲＫ、あるいはＭＵＫまたはＭＲＫから導出されたキーを使用して）、全体の受信報告、または受信報告における１つまたは複数のフィールドを暗号化することによって受信報告を暗号化することができる。

【００４９】

[0064] 図１０は、安全なユーザサービス発見／アナウンスメントを受信および処理するための実例となる方法を例示する図１０００である。ステップ１００８では、ＢＭ－ＳＣ１００６は、ユーザサービス発見／アナウンスメントを完全性保護および／または暗号化する。ＢＭ－ＳＣ１００６は、完全なユーザサービス発見／アナウンスメント、またはユーザサービス発見／アナウンスメントの１つまたは複数のフィールドを完全性保護および／または暗号化することができる。例えば、ＢＭ－ＳＣ１００６は、ユーザサービス発見／アナウンスメント内の受信報告構成のみ、またはサーバＵＲＬフィールドのみを完全性保護および／または暗号化することができる。ＢＭ－ＳＣ１００６は、ハッシュ値を得るためのハッシュ関数を通じて、ユーザサービス発見／アナウンスメントまたはユーザサービス発見／アナウンスメントにおける１つまたは複数のフィールドをハッシュすることによって、ユーザサービス発見／アナウンスメントを完全性保護することができる。ハッシュ関数はそれ自体、ＵＥのグループおよびサービスプロバイダに知られている、ＭＳＫまたは類似のグループキーの関数でありうる。ＢＭ－ＳＣ１００６は、ＵＥ１００２に、ユーザサービス発見／アナウンスメントでハッシュ値を送ることができる。代わりとして、あるいは加えて、ＢＭ－ＳＣ１００６は、ＭＳＫに基づいて（例えば、ＭＳＫ、またはＭＳＫから導出されたキーを使用して）、全体のユーザサービス発見／アナウンスメント、またはユーザサービス発見／アナウンスメントにおける１つまたは複数のフィールドを暗号化することによってユーザサービス発見／アナウンスメントを暗号化することができる。ＢＭ－ＳＣ１００６が、ユーザサービス発見／アナウンスメントにおける１つまたは複数のフィールドのみを保護することを判定する場合、ＢＭ－ＳＣ１００６は、ユーザサービス発見／アナウンスメントで送られるフィールドタイプを通じてＵＥ１００２にその判定を表示することができる。フィールドタイプはまた、完全性保護されうる。ＵＥは、ＯＴＡ構成またはデバイス管理手順を通じて保護されることになるフィールドで予め構成されうる、あるいはＵＥは、どのフィールドが保護されるべきかを知る前にプログラムされうる。

【００５０】

[0065] ステップ１０１０では、ＢＭ－ＳＣ１００６は、ＵＥ１００２にユーザサービス発見／アナウンスメントを送る。ステップ１０１２では、ユーザサービス発見／アナウンスメントが完全性保護される場合、ＵＥ１００２はＭＳＫに基づいてユーザサービス発見／アナウンスメントの完全性を証明する。加えて、ユーザサービス発見／アナウンスメントが暗号化される場合、ＵＥ１００２はＭＳＫに基づいてユーザサービス発見／アナウンスメントを解読する。ステップ１０１４では、ＵＥ１００２は、受信報告を送るべきかどうか、ならびに受信報告が感知情報を含むことができるかどうかを決定する。ステップ１０１６では、ＵＥ１００２は受信報告を送るための時間を選択する。ステップ１０１８では、ＵＥ１００２は、サーバ１００４に受信報告を送る。１つの構成では、ＵＥ１００２は、安全な接続（例えば、ＨＴＴＰＳ）を通じてサーバ１００４に受信報告を送る。別の構成では、ＵＥ１００２は、サーバ１００４に受信報告を送る前に受信報告を完全性保護および／または暗号化する。

【００５１】

[0066] 図１１は、無線通信の第１の方法のフローチャート１１００である。方法は、ＵＥによって行われうる。ステップ１１０２では、ＵＥは、サービスプロバイダから、認証局リストを受信する。認証局リストは、信頼される認証局の証明書を含む。認証局リストは、ＵＥおよびサービスプロバイダによって知られている認証情報に基づいて完全性保護および／または暗号化される。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。認証情報は、ＭＵＫまたはＭＲＫ、あるいはＭＵＫまたはＭＲＫから導出されたキー

のような、ＵＥおよびサービスプロバイダに知られているいずれかの共有キーに基づきうる。ステップ１１０４では、ＵＥは、サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信する。全体のユーザサービス発見／アナウンスメント、またはユーザサービス発見／アナウンスメント内の１つまたは複数のフィールドは、ＵＥおよびＢＭ－ＳＣによって知られている認証情報に基づいて完全性保護および／または暗号化されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。認証情報は、ＭＳＫ、またはＭＳＫから導出されたキーのような共有キーでありうる。ステップ１１０４の後に、ＵＥがコンテンツ項目の完全な受信またはセッションの完了を識別し、受信報告が必要とされることを決定する場合、ステップ１１０６では、ＵＥは受信報告が感知受信報告情報を含むかどうかを決定する。ステップ１１０６における決定は、受信報告のための報告タイプＲＡｃｋ、ＳｔａＲ、ＳｔａＲ－ａｌｌ、またはＳｔａＲ－ｏｎｌｙに基づきうる、あるいは他の情報に基づきうる。受信報告が感知情報を含まない場合、ステップ１１０８では、ＵＥは、受信されたサーバアドレスおよび受信報告構成に基づいて、保証されていない接続を通じてサーバに受信報告を送る。受信報告が感知情報を含む場合、ステップ１１１０では、ＵＥは安全な接続セットアップ（例えば、ＨＴＴＰＳ）を開始し、サーバの証明書を受信する。ステップ１１１２では、ＵＥは、受信された認証局リストおよび証明書を使用してサーバを認証する。ＵＥは、証明書が受信されたサーバＵＲＬと同じサーバアドレスに属することを証明することによって、ならびに受信された証明書が、受信された認証局リスト内のルート証明書に基づいて発行されたことを証明するために、その証明書を認証局リストと比較することによってサーバを認証することができる。ステップ１１１４では、ＵＥは、サーバを認証する際にサーバとの安全な接続をセットアップすることを決定し、サーバとの安全な接続をセットアップする。ステップ１１１６では、ＵＥは、受信されたサーバアドレスおよび受信報告構成に基づいて、安全な接続を通じてサーバに受信報告を送る。

【００５２】

[0067] 図１２は、無線通信の第２の方法のフローチャート１２００である。方法は、ＵＥによって行われうる。ステップ１２０２では、ＵＥは、サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信する。全体のユーザサービス発見／アナウンスメント、またはユーザサービス発見／アナウンスメントの一部は、完全性保護および／または暗号化されうる。ステップ１２０２の後に、ＵＥがコンテンツ項目の完全な受信またはセッションの完了を識別し、受信報告が必要とされることを決定する場合、ステップ１２０４では、ＵＥは受信報告が感知受信報告情報を含むかどうかを決定する。ステップ１２０４における決定は、受信報告のための報告タイプＲＡｃｋ、ＳｔａＲ、ＳｔａＲ－ａｌｌ、またはＳｔａＲ－ｏｎｌｙに基づきうる、あるいは他の情報に基づきうる。受信報告が感知情報を含まない場合、ステップ１２０８では、ＵＥは、受信されたサーバアドレスおよび受信報告構成に基づいて、サーバに保護されていない受信報告を送る。受信報告が感知情報を含む場合、ステップ１２０６では、ＵＥが受信報告を完全性保護および暗号化すること、ならびに／もしくは受信報告を送るために安全な接続をセットアップすることによって受信報告を保護する。ステップ１２１０では、ＵＥは、受信報告構成に基づいて、サーバに保護された受信報告を送る。

【００５３】

[0068] 図１３は、無線通信の第３の方法のフローチャート１３００である。方法は、ＵＥによって行われうる。ステップ１３０２では、ＵＥは、保護されたブロードキャストアナウンスメントを受信する。ブロードキャストアナウンスメントは、完全性保護および／または暗号化される。ブロードキャストアナウンスメントは、ＵＥおよびＢＭ－ＳＣに知られている認証情報に基づいて、完全性保護および／または暗号化されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。ブロードキャストアナウンスメントが完全性保護されるとき、認証情報は、チェックサムまたはハッシュサムを含むことができる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。認証情報は、ＭＳＫ、またはＭＳＫから導き出されたキーのような共有キーでありうる。ステップ１３０４では

、ＵＥは、ブロードキャストアナウンスメントが暗号化されたときに、認証情報／共有キー／ＭＳＫに基づいてブロードキャストアナウンスメントを解読する、ならびに／もしくは、ブロードキャストアナウンスメントが完全性保護されるときに、認証情報／共有キー／ＭＳＫに基づいてブロードキャストアナウンスメントの完全性を証明する。ＵＥは、チェックサム／ハッシュサムを再計算すること、および再計算されたチェックサム／ハッシュサムを認証情報で提供されるチェックサム／ハッシュサムと比較することによってブロードキャストアナウンスメントの完全性を証明する。再計算されたチェックサム／ハッシュサムが認証情報におけるチェックサム／ハッシュサムと一致するとき、完全性チェックは通過する。そうでなければ完全性チェックは失敗する。ステップ１３０６では、ＵＥはブロードキャストアナウンスメントが首尾よく解読されたか、および／または完全性チェックは通過したかどうかを決定する。ＵＥがブロードキャストアナウンスメントを解読すること、および／またはブロードキャストアナウンスメントの完全性を証明することができた場合、ステップ１３０８では、ＵＥは、ブロードキャストアナウンスメントに基づいて通信（例えば、受信報告を送る）ことができる。

【００５４】

[0069] 図１４は、実例となる装置１４０２において異なるモジュール／手段／コンポーネント間のデータフローを例示している概略的なデータフロー図１４００である。装置は、ＵＥでありうる。装置は、ｅＮＢ１４５０を介してサービスプロバイダから、認証局リストを受信するように構成されうる通信モジュール１４０４を含む。認証局リストは、信頼される認証局の証明書を含みうる。認証局リストは、ＵＥおよびサービスプロバイダによって知られている認証情報に基づいて完全性保護または暗号化されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。認証情報は、共有キーでありうる。共有キーは、ＭＵＫまたはＭＲＫ、あるいはＭＵＫまたはＭＲＫから導出されたキーのような、ＵＥおよびサービスプロバイダに知られているいずれかの共有キーでありうる。通信モジュール１４０４は、サーバ認証モジュール１４１０に認証局リストを提供するように構成されうる。サーバ認証モジュール１４１０は、暗号化／解読モジュール１４０８を通じて認証局リストを解読するように構成され、完全性保護モジュール１４１２を通じて認証局リストの完全性を証明するように構成されうる。暗号化／解読モジュール１４０８は、共有キー（例えば、ＭＵＫ／ＭＲＫ、またはＭＵＫ／ＭＲＫから導出されたキー）のような、ＵＥおよびサーバに知られている認証情報に基づいて、認証局リストを解読するように構成されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。完全性保護モジュール１４１２は、共有キー（例えば、ＭＵＫ／ＭＲＫ、またはＭＵＫ／ＭＲＫから導出されたキー）のような、ＵＥおよびサーバに知られている認証情報に基づいて、認証局リストの完全性を証明するように構成されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。

【００５５】

[0070] 通信モジュール１４０４は、サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信するように構成されうる。ユーザサービス発見／アナウンスメントは、ＵＥおよびＢＭ－ＳＣによって知られている認証情報に基づいて、完全性保護および／または暗号化されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。認証情報は、共有キーでありうる。共有キーは、ＭＳＫ、またはＭＳＫから導出されたキーでありうる。通信モジュール１４０４は、受信報告処理モジュール１４０６に受信されたユーザサービス発見／アナウンスメントを提供するように構成されうる。受信報告処理モジュール１４０６は、暗号化／解読モジュール１４０８を通じてユーザサービス発見／アナウンスメントを解読するように構成され、完全性保護モジュール１４１２を通じてユーザサービス発見／アナウンスメントの完全性を証明するように構成されうる。暗号化／解読モジュール１４０８は、共有キー（例えば、ＭＳＫ、またはＭＳＫから導出されたキー）のような、ＵＥおよびＢＭ－ＳＣに知られている認証情報に基づいて、ユーザサービス発見／アナウンスメントを解読するように構成されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。完全性保護モジュール１４１２は、共

有キー（例えば、ＭＳＫ、またはＭＳＫから導出されたキー）のような、ＵＥおよびＢＭ－ＳＣに知られている認証情報に基づいて、ユーザサービス発見／アナウンスメントの完全性を証明するように構成されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。

【００５６】

[0071] 通信モジュール１４０４は、サーバとの安全な接続を開始する際に、サーバの証明書を受信するように構成されうる。通信モジュール１４０４は、サーバ認証モジュール１４１０に証明書を提供するように構成されうる。サーバ認証モジュール１４１０は、受信された認証局リストおよび受信された証明書を使用してサーバを認証するように構成されうる。サーバ認証モジュール１４１０は、サーバを認証する際に、サーバとの安全な接続（例えば、ＨＴＴＰＳ）をセットアップすることを決定するように構成されうる。サーバ認証モジュール１４１０は、通信モジュール１４０４がサーバとの安全な接続をセットアップするように、通信モジュール１４０４と通信するように構成されうる。通信モジュール１４０４は、コンテンツ項目の完全な受信またはセッションの完了が存在するときに、受信報告処理モジュール１４０６に通信することができる。受信報告プロセスモジュール１４０６は、受信報告が必要とされるかどうかを決定し、受信報告が必要とされる場合、受信報告を生成することができる。受信報告処理モジュール１４０６は、暗号化／解読モジュール１４０８を通じて受信報告を暗号化するように構成されうる。暗号化／解読モジュール１４０８は、共有キー（例えば、ＭＵＫ／ＭＲＫ、またはＭＵＫ／ＭＲＫから導出されたキー）のような、ＵＥおよびサーバに知られている認証情報に基づいて、受信報告を暗号化するように構成されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。受信報告処理モジュール１４０６は、完全性保護モジュール１４１２を通じて受信報告を完全性保護するように構成されうる。完全性保護モジュール１４１２は、共有キー（例えば、ＭＵＫ／ＭＲＫ、またはＭＵＫ／ＭＲＫから導き出されたキー）のような、ＵＥおよびサーバに知られている認証情報に基づいて、受信報告を完全性保護するように構成されうる。認証情報は、ＵＥにおけるスマートカード上に記憶されうる。受信報告処理モジュール１４０６は、サーバに受信報告を送るように構成されうる、通信モジュール１４０４に生成された受信報告を提供することができる。通信モジュール１４０４は、サーバとの安全な接続をセットアップしている場合、通信モジュール１４０４は、安全な接続を通じてサーバに受信報告を送るように構成されうる。

【００５７】

[0072] 装置は、図８－１０の上述の図、および図１１－１３のフローチャートにおけるアルゴリズムのステップの各々を行う追加のモジュールを含むことができる。このように、図８－１０の上述の図、および図１１－１３のフローチャートにおける各ステップはモジュールによって行われ、装置はこれらのモジュールのうちの１つまたは複数を含むことができる。モジュールは、述べられたプロセス／アルゴリズムを実施するように特に構成され、述べられたプロセス／アルゴリズムを行うように構成されたプロセッサによってインプリメントされ、プロセッサによるインプリメンテーションのためにコンピュータ可読媒体内に記憶された、あるいはそれらのいくつかの組み合わせの、１つまたは複数のハードウェアコンポーネントでありうる。

【００５８】

[0073] 図１５は、処理システム１５１４を用いる装置１４０２‘のためのハードウェアインプリメンテーションの例を示す図である。処理システム１５１４は、バス１５２４により一般的に表されるバスアーキテクチャでインプリメントされうる。バス１５２４は、処理システム１５１４の指定のアプリケーションと全体的な設計の制約に依存して、任意の数の相互接続バスおよびブリッジを含むことができる。バス１５２４は、プロセッサ１５０４、モジュール１４０４、１４０６、１４０８、１４１０、１４１２、およびコンピュータ可読媒体１５０６によって表されている１つまたは複数のプロセッサおよび／またはハードウェアモジュールを含む様々な回路とリンクする。バス１５２４はまた、タイミングソース、周辺機器、電圧レギュレータ、および電力管理回路のような様々な他の回路

とリンクすることができ、これらは、当該技術分野で周知であるので、これ以上説明されない。

【００５９】

[0074] 処理システム１５１４は、トランシーバ１５１０に結合されうる。トランシーバ１５１０は、１つまたは複数のアンテナ１５２０に結合される。トランシーバ１５１０は、送信媒体をわたって様々な他の装置と通信するための手段を提供する。処理システム１５１４は、コンピュータ可読媒体１５０６に結合されたプロセッサ１５０４を含む。プロセッサ１５０４は、コンピュータ可読媒体１５０６上に記憶されたソフトウェアの実行を含む、一般的な処理を担う。ソフトウェアは、プロセッサ１５０４によって実行されると、処理システム１５１４に、あらゆる特定の装置に関して上で説明された様々な機能を行わせる。コンピュータ可読媒体１５０６はまた、ソフトウェアを実行するときにプロセッサ１５０４によって操作されるデータを記憶するために使用されることもできる。処理システムはさらに、モジュール１４０４、１４０６、１４０８、１４１０、および１４１２のうちの少なくとも１つを含む。モジュールは、プロセッサ１５０４において稼働し、コンピュータ可読媒体１５０６に内在し／記憶されたソフトウェアモジュール、プロセッサ１５０４に結合された１つまたは複数のハードウェアモジュール、またはそれらの何らかの組み合わせでありうる。処理システム１５１４は、ＵＥ６５０のコンポーネントであり、メモリ６６０ならびに／もしくは、ＴＸプロセッサ６６８、ＲＸプロセッサ６５６、およびコントローラ／プロセッサ６５９のうちの少なくとも１つを含むことができる。

【００６０】

[0075] １つの構成では、ワイヤレス通信のための装置１４０２／１４０２’は、サービスプロバイダから認証局リストを受信するための手段を含む。認証局リストは、装置およびサービスプロバイダによって知られている認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる。認証情報は、装置におけるスマートカード上に記憶されうる。装置はさらに、受信された認証局リストを使用してサーバを認証するための手段を含む。装置はさらに、サーバの証明書を受信するための手段、およびサーバを認証する際にサーバとの安全な接続をセットアップすることを決定するための手段を含むことができる。装置はさらに、サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信するための手段、サーバとの安全な接続をセットアップするための手段、およびアドレスおよび受信報告構成に基づいて安全な接続を通じてサーバに受信報告を送るための手段を含むことができる。

【００６１】

[0076] 上述の手段は、装置１４０２の上述のモジュールのうちの１つまたは複数、および／または上述の手段によって記載された機能を行うように構成された装置１４０２’の処理システム１５１４でありうる。上で説明されているように、処理システム１５１４は、ＴＸプロセッサ６６８、ＲＸプロセッサ６５６、およびコントローラ／プロセッサ６５９を含むことができる。このように、１つの構成において上述の手段は、上述の手段によって記載された機能を行うように構成されたＴＸプロセッサ６６８、ＲＸプロセッサ６５６、コントローラ／プロセッサ６５９でありうる。

【００６２】

[0077] １つの構成では、ワイヤレス通信のための装置１４０２／１４０２’は、サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信するための手段、および受信報告構成に基づいてサーバに保護された受信報告を送るために手段を含む。装置はさらに、サーバとの安全な接続をセットアップするための手段を含むことができる。装置はさらに、サービスプロバイダから認証局リストを受信するための手段、サーバの証明書を受信するための手段、および受信された認証局リストおよび証明書を使用してサーバを認証するための手段をさらに含むことができる。装置はさらに、受信報告を完全性保護および／または暗号化するための手段を含むことができる。

【００６３】

[0078] 上述の手段は、装置１４０２の上述のモジュールのうちの１つまたは複数、およ

び／または上述の手段によって記載された機能を行うように構成された装置１４０２’の処理システム１５１４でありうる。上で説明されているように、処理システム１５１４は、ＴＸプロセッサ６６８、ＲＸプロセッサ６５６、およびコントローラ／プロセッサ６５９を含むことができる。このように、１つの構成において上述の手段は、上述の手段によって記載された機能を行うように構成されたＴＸプロセッサ６６８、ＲＸプロセッサ６５６、コントローラ／プロセッサ６５９でありうる。

【００６４】

[0079] １つの構成では、無線通信のための装置１４０２／１４０２’は、保護されたブロードキャストアナウンスメントを受信するための手段を含む。ブロードキャストアナウンスメントは、装置によって知られ、かつ装置におけるスマートカード上に記憶された認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる。装置はさらに、ブロードキャストアナウンスメントに基づいて通信するための手段を含む。装置はさらに、ブロードキャストアナウンスメントが暗号化されるとき、ＭＳＫに基づいてブロードキャストアナウンスメントを解読するための手段を含むことができる。装置はさらに、ブロードキャストアナウンスメントが完全性保護されるとき、ＭＳＫに基づいてブロードキャストアナウンスメントの完全性を証明するための手段を含むことができる。

【００６５】

[0080] 上述の手段は、装置１４０２の上述のモジュールのうちの１または複数、および／または上述の手段によって記載された機能を行うように構成された装置１４０２’の処理システム１５１４でありうる。上で説明されているように、処理システム１５１４は、ＴＸプロセッサ６６８、ＲＸプロセッサ６５６、およびコントローラ／プロセッサ６５９を含むことができる。このように、１つの構成において上述の手段は、上述の手段によって記載された機能を行うように構成されたＴＸプロセッサ６６８、ＲＸプロセッサ６５６、コントローラ／プロセッサ６５９でありうる。

【００６６】

[0081] 開示されたプロセスにおけるステップの指定の順序または階層は、実例となる手法の例示のであることが理解される。設計選好に基づいて、プロセスにおけるステップの指定の順序または階層は並べ替えられうるということが理解される。さらにいくつかのステップが組み合わされる、または省略されることができる。添付の方法の請求項は、サンプルの順序で様々なステップの要素を示し、示された指定の順序または階層に限定されるようには意図されない。

【００６７】

[0082] 先の説明は、当業者が、ここで説明された様々な態様を実現できるように提供されている。これらの態様への様々な変更は当業者には容易に明らかになり、ここで定義される包括的な本質は他の態様に適用されうる。このように、特許請求の範囲は、ここで提示された態様を限定されるように意図されておらず、特許請求の範囲の用語と一貫した最大範囲であると認められるべきであり、ここにおいて、単数の要素に対する言及は、そうと特別に述べられない限りは「１つおよび１つだけ」を意味するのではなく、むしろ「１または複数」を意味することが意図されている。他の方法で特別に述べられていない限り、「いくつか」という用語は、１つまたは複数を称する。「Ａ、Ｂ、またはＣのうちの少なくとも１つ」、「Ａ、Ｂ、およびＣのうちの少なくとも１つ」、および「Ａ、Ｂ、Ｃ、またはそれらのあらゆる組み合わせ」のような組み合わせは、Ａ、Ｂ、および／またはＣのいずれの組み合わせも含み、複数のＡ、複数のＢ、または、複数のＣを含むことができる。特に、「Ａ、Ｂ、またはＣのうちの少なくとも１つ」、「Ａ、Ｂ、およびＣのうちの少なくとも１つ」、および「Ａ、Ｂ、Ｃ、またはそれらのあらゆる組み合わせ」のような組み合わせは、Ａのみ、Ｂのみ、Ｃのみ、ＡとＢ、ＡとＣ、ＢとＣ、またはＡとＢとＣであることができ、ここにおいてそのようなあらゆる組み合わせが、Ａ、Ｂ、またはＣの１つまたは複数のメンバーを含むことができる。当業者に知られている、あるいは後に知られることになる本開示全体で説明された様々な態様の要素に対する全ての構造的および機能的な均等物は、参照によってここに明確に組み込まれ、特許請求の範囲に包含されるよ

うに意図されている。さらに、ここで開示されたものはどれも、そのような開示が特許請求の範囲において明示的に記載されているかどうかに関わらず公共に寄与されるようには意図されていない。どの特許請求の範囲の要素も、要素が明確に「ための手段」という表現を使用して明確に記載されていない限り、ミーンズプラスファンクション（ｍｅａｎｓ　ｐｌｕｓ　ｆｕｎｃｔｉｏｎ）として解釈されるべきではない。

以下に、本願出願の当初の特許請求の範囲に記載された発明を付記する。

［Ｃ１］

ユーザ機器（ＵＥ）のワイヤレス通信の方法であって、

サービスプロバイダから、認証局リストを受信することと、前記認証局リストは、前記ＵＥおよび前記サービスプロバイダによって知られ、かつ前記ＵＥにおけるスマートカード上に記憶された認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、

前記受信された認証局リストを使用してサーバを認証することと、

を備える、方法。

［Ｃ２］

前記認証局リストは、信頼される認証局の証明書を含む、Ｃ１に記載の方法。

［Ｃ３］

サーバの証明書を受信することと、

前記サーバを認証する際に前記サーバとの安全な接続をセットアップすることを決定することと、

をさらに備え、

前記認証することは、前記受信された証明書と前記認証局リストとの比較に基づいて、前記受信された証明書が信頼される認証局からのものであることを決定すること、を備える、

Ｃ１に記載の方法。

［Ｃ４］

前記認証情報は、前記ＵＥおよび前記サービスプロバイダによって知られている共有キーである、Ｃ１に記載の方法。

［Ｃ５］

前記共有キーは、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）、ＭＢＭＳユーザキー（ＭＵＫ）、または前記ＭＲＫまたは前記ＭＵＫのうちの１つから導出されたキーに基づく、Ｃ４に記載の方法。

［Ｃ６］

前記サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信することと、

前記サーバとの安全な接続をセットアップすることと、

前記アドレスおよび前記受信報告構成に基づいて前記安全な接続を通じて前記サーバに受信報告を送ることと、

をさらに備える、Ｃ１に記載の方法。

［Ｃ７］

前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じたものである、Ｃ６に記載の方法。

［Ｃ８］

前記ユーザサービス発見／アナウンスメントは、前記ＵＥおよびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ６に記載の方法。

［Ｃ９］

前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づく、Ｃ８に記載の方法。

［Ｃ１０］

ワイヤレス通信の方法であって、
サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信することと、
前記受信報告構成に基づいて前記サーバに保護された受信報告を送ることと、
を備える、方法。
［Ｃ１１］
前記サーバとの安全な接続をセットアップすることをさらに備え、ここにおいて前記保護された受信報告は、前記安全な接続を通じて送られる、Ｃ１０に記載の方法。
［Ｃ１２］
前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じたものである、Ｃ１１に記載の方法。
［Ｃ１３］
サービスプロバイダから、認証局リストを受信することと、
前記サーバの証明書を受信することと、
前記受信された認証局リストおよび前記証明書を使用して前記サーバを認証することと、
をさらに備える、Ｃ１０に記載の方法。
［Ｃ１４］
前記認証局リストは、前記ＵＥおよび前記サービスプロバイダによって知られている認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ１３に記載の方法。
［Ｃ１５］
前記認証局リストは、信頼される認証局の証明書を含む、Ｃ１３に記載の方法。
［Ｃ１６］
前記受信報告を完全性保護および／または暗号化すること、をさらに備える、Ｃ１０に記載の方法。
［Ｃ１７］
前記完全性保護および／または暗号化することは、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）登録キー（ＭＲＫ）に基づく、Ｃ１６に記載の方法。
［Ｃ１８］
前記ユーザサービス発見／アナウンスメントは、前記ＵＥおよびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ１０に記載の方法。
［Ｃ１９］
前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づく、Ｃ１８に記載の方法。
［Ｃ２０］
ユーザ機器（ＵＥ）のワイヤレス通信の方法であって、
保護されたブロードキャストアナウンスメントを受信することと、前記ブロードキャストアナウンスメントは、前記ＵＥによって知られ、かつ前記ＵＥにおけるスマートカード上に記憶された認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、
前記ブロードキャストアナウンスメントに基づいて通信することと、
を備える、方法。
［Ｃ２１］
前記ブロードキャストアナウンスメントが暗号化されるとき、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づいて前記ブロードキャストアナウンスメントを解読すること、をさらに備える、Ｃ２０に記載の方法。
［Ｃ２２］
前記ブロードキャストアナウンスメントが完全性保護されるとき、マルチメディアブロ

ードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づいて、前記ブロードキャストアナウンスメントの完全性を証明することをさらに備え、前記通信することは、前記ブロードキャストアナウンスメントの前記完全性が証明されるとき、前記ブロードキャストアナウンスメントに基づいて生じる、Ｃ２０に記載の方法。

［Ｃ２３］

前記ブロードキャストアナウンスメントは、サーバのアドレスおよび受信報告構成を備えるユーザサービス発見／アナウンスメントであり、前記ブロードキャストアナウンスメントに基づいて前記通信することは、前記アドレスおよび前記受信報告構成に基づいて前記サーバに受信報告を送ることを備える、Ｃ２０に記載の方法。

［Ｃ２４］

前記受信報告は、安全な接続を通じて送られる、Ｃ２３に記載の方法。

［Ｃ２５］

前記受信報告は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）登録キー（ＭＲＫ）に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ２３に記載の方法。

［Ｃ２６］

ワイヤレス通信のための装置であって、

サービスプロバイダから、認証局リストを受信するための手段と、前記認証局リストは、前記装置および前記サービスプロバイダによって知られ、かつ前記装置におけるスマートカード上に記憶された認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、

前記受信された認証局リストを使用してサーバを認証するための手段と、

を備える、装置。

［Ｃ２７］

前記認証局リストは、信頼される認証局の証明書を含む、Ｃ２６に記載の装置。

［Ｃ２８］

サーバの証明書を受信するための手段と、

前記サーバを認証する際に前記サーバとの安全な接続をセットアップすることを決定するための手段と、

をさらに備え、

前記認証するための手段は、前記受信された証明書と前記認証局リストとの比較に基づいて、前記受信された証明書が信頼される認証局からのものであることを決定することによって前記サーバを認証する、

Ｃ２６に記載の装置。

［Ｃ２９］

前記認証情報は、前記装置および前記サービスプロバイダによって知られている共有キーである、Ｃ２６に記載の装置。

［Ｃ３０］

前記共有キーは、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）、ＭＢＭＳユーザキー（ＭＵＫ）、もしくは前記ＭＲＫまたは前記ＭＵＫのうちの１つから導出されたキーに基づく、Ｃ２９に記載の装置。

［Ｃ３１］

前記サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信するための手段と、

前記サーバとの安全な接続をセットアップするための手段と、

前記アドレスおよび前記受信報告構成に基づいて前記安全な接続を通じて前記サーバに受信報告を送るための手段と、

をさらに備える、Ｃ２６に記載の装置。

［Ｃ３２］

前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じた

ものである、Ｃ３１に記載の装置。
［Ｃ３３］
前記ユーザサービス発見／アナウンスメントは、前記装置およびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ３１に記載の装置。
［Ｃ３４］
前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づく、Ｃ３３に記載の装置。
［Ｃ３５］
ワイヤレス通信のための装置であって、
サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信するための手段と、
前記受信報告構成に基づいて前記サーバに保護された受信報告を送るための手段と、
を備える、装置。
［Ｃ３６］
前記サーバとの安全な接続をセットアップするための手段をさらに備え、ここにおいて前記保護された受信報告は、前記安全な接続を通じて送られる、Ｃ３５に記載の装置。
［Ｃ３７］
前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じたものである、Ｃ３６に記載の装置。
［Ｃ３８］
サービスプロバイダから、認証局リストを受信するための手段と、
前記サーバの証明書を受信するための手段と、
前記受信された認証局リストおよび前記証明書を使用して前記サーバを認証するための手段と、
をさらに備える、Ｃ３５に記載の装置。
［Ｃ３９］
前記認証局リストは、前記装置および前記サービスプロバイダによって知られている認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ３８に記載の装置。
［Ｃ４０］
前記認証局リストは、信頼される認証局の証明書を含む、Ｃ３８に記載の装置。
［Ｃ４１］
前記受信報告を完全性保護および／または暗号化するための手段、をさらに備える、Ｃ３５に記載の装置。
［Ｃ４２］
前記完全性保護および／または暗号化するための手段は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）またはＭＢＭＳユーザキー（ＭＵＫ）に基づいて、完全性保護および／または暗号化する、Ｃ４１に記載の装置。
［Ｃ４３］
前記ユーザサービス発見／アナウンスメントは、前記装置およびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ３５に記載の装置。
［Ｃ４４］
前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づく、Ｃ４３に記載の装置。
［Ｃ４５］
ユーザ機器（ＵＥ）のワイヤレス通信のための装置であって、
保護されたブロードキャストアナウンスメントを受信するための手段と、前記ブロードキャストアナウンスメントは、前記ＵＥによって知られ、かつ前記ＵＥにおけるスマート

カード上に記憶された認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、
前記ブロードキャストアナウンスメントに基づいて通信するための手段と、
を備える、装置。
［Ｃ４６］
前記ブロードキャストアナウンスメントが暗号化されるとき、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づいて前記ブロードキャストアナウンスメントを解読するための手段、をさらに備える、Ｃ４５に記載の装置。
［Ｃ４７］
前記ブロードキャストアナウンスメントが完全性保護されるとき、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づいて、前記ブロードキャストアナウンスメントの完全性を証明するための手段をさらに備え、前記通信するための手段は、前記ブロードキャストアナウンスメントの前記完全性が証明されるとき、前記ブロードキャストアナウンスメントに基づいて通信する、Ｃ４５に記載の装置。
［Ｃ４８］
前記ブロードキャストアナウンスメントは、サーバのアドレスおよび受信報告構成を備えるユーザサービス発見／アナウンスメントであり、前記通信するための手段は、前記アドレスおよび前記受信報告構成に基づいて前記サーバに受信報告を送ることによって、前記ブロードキャストアナウンスメントに基づいて通信する、Ｃ４５に記載の装置。
［Ｃ４９］
前記受信報告は、安全な接続を通じて送られる、Ｃ４８に記載の装置。
［Ｃ５０］
前記受信報告は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）またはＭＢＭＳユーザキー（ＭＵＫ）に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ４８に記載の装置。
［Ｃ５１］
ワイヤレス通信のための装置であって、
サービスプロバイダから、認証局リストを受信し、前記認証局リストは、前記装置および前記サービスプロバイダによって知られ、かつ前記装置におけるスマートカード上に記憶された認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、
前記受信された認証局リストを使用してサーバを認証する、
ように構成された処理システム、
を備える、装置。
［Ｃ５２］
前記認証局リストは、信頼される認証局の証明書を含む、Ｃ５１に記載の装置。
［Ｃ５３］
前記処理システムは、
サーバの証明書を受信し、
前記サーバを認証する際に、前記サーバとの安全な接続をセットアップすることを決定する、
ようにさらに構成され、
前記処理システムは、前記受信された証明書と前記認証局リストとの比較に基づいて、前記受信された証明書が信頼される認証局からのものであることを決定することによって認証する、
Ｃ５１に記載の装置。
［Ｃ５４］
前記認証情報は、前記装置および前記サービスプロバイダによって知られている共有キ

ーである、Ｃ５１に記載の装置。
［Ｃ５５］
前記共有キーは、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）、ＭＢＭＳユーザキー（ＭＵＫ）、もしくは前記ＭＲＫまたは前記ＭＵＫのうちの１つから導出されたキーに基づく、Ｃ５４に記載の装置。
［Ｃ５６］
前記処理システムは、
前記サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信し、
前記サーバとの安全な接続をセットアップし、
前記アドレスおよび前記受信報告構成に基づいて前記安全な接続を通じて前記サーバに受信報告を送る、
ようにさらに構成される、Ｃ５１に記載の装置。
［Ｃ５７］
前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じたものである、Ｃ５６に記載の装置。
［Ｃ５８］
前記ユーザサービス発見／アナウンスメントは、前記装置およびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ５６に記載の装置。
［Ｃ５９］
前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づく、Ｃ５８に記載の装置。
［Ｃ６０］
ワイヤレス通信のための装置であって、
サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信し、
前記受信報告構成に基づいて前記サーバに保護された受信報告を送る、
ように構成された処理システム、
を備える、装置。
［Ｃ６１］
前記処理システムは、前記サーバとの安全な接続をセットアップするようにさらに構成され、ここにおいて前記保護された受信報告は、前記安全な接続を通じて送られる、Ｃ６０に記載の装置。
［Ｃ６２］
前記安全な接続は、ハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）を通じたものである、Ｃ６１に記載の装置。
［Ｃ６３］
前記処理システムは、
サービスプロバイダから、認証局リストを受信し、
前記サーバの証明書を受信し、
前記受信された認証局リストおよび前記証明書を使用して前記サーバを認証する、
ようにさらに構成される、Ｃ６０に記載の装置。
［Ｃ６４］
前記認証局リストは、前記装置および前記サービスプロバイダによって知られている認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ６３に記載の装置。
［Ｃ６５］
前記認証局リストは、信頼される認証局の証明書を含む、Ｃ６３に記載の装置。
［Ｃ６６］

前記処理システムは、前記受信報告を完全性保護および／または暗号化するようにさらに構成される、Ｃ６０に記載の装置。

［Ｃ６７］

前記処理システムは、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）要求キー（ＭＲＫ）ＭＢＭＳユーザキー（ＭＵＫ）に基づいて、完全性保護および／または暗号化する、Ｃ６６に記載の装置。

［Ｃ６８］

前記ユーザサービス発見／アナウンスメントは、前記装置およびブロードキャストマルチキャストサービスセンタ（ＢＭ－ＳＣ）によって知られている認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ６０に記載の装置。

［Ｃ６９］

前記認証情報は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づく、Ｃ６８に記載の装置。

［Ｃ７０］

ユーザ機器（ＵＥ）のワイヤレス通信ための装置であって、

保護されたブロードキャストアナウンスメントを受信し、前記ブロードキャストアナウンスメントは、前記ＵＥによって知られ、かつ前記ＵＥにおけるスマートカード上に記憶された認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、

前記ブロードキャストアナウンスメントに基づいて通信する、

ように構成された処理システム、

を備える、装置。

［Ｃ７１］

前記処理システムは、前記ブロードキャストアナウンスメントが暗号化されるとき、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づいて前記ブロードキャストアナウンスメントを解読するようにさらに構成される、Ｃ７０に記載の装置。

［Ｃ７２］

前記処理システムは、前記ブロードキャストアナウンスメントが完全性保護されるとき、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）サービスキー（ＭＳＫ）に基づいて、前記ブロードキャストアナウンスメントの完全性を証明するようにさらに構成され、ここにおいて前記処理システムは、前記ブロードキャストアナウンスメントの前記完全性が証明されるとき、前記ブロードキャストアナウンスメントに基づいて通信する、Ｃ７０に記載の装置。

［Ｃ７３］

前記ブロードキャストアナウンスメントは、サーバのアドレスおよび受信報告構成を備えるユーザサービス発見／アナウンスメントであり、前記処理システムは、前記アドレスおよび前記受信報告構成に基づいて前記サーバに受信報告を送ることによって、前記ブロードキャストアナウンスメントに基づいて通信する、Ｃ７０に記載の装置。

［Ｃ７４］

前記受信報告は、安全な接続を通じて送られる、Ｃ７３に記載の装置。

［Ｃ７５］

前記受信報告は、マルチメディアブロードキャストマルチキャストサーバ（ＭＢＭＳ）登録キー（ＭＲＫ）に基づいて完全性保護または暗号化のうちの少なくとも１つが行われる、Ｃ７３に記載の装置。

［Ｃ７６］

ユーザ機器（ＵＥ）内のコンピュータプログラム製品であって、

サービスプロバイダから、認証局リストを受信することと、前記認証局リストは、前記ＵＥおよび前記サービスプロバイダによって知られ、かつ前記ＵＥにおけるスマートカード上に記憶された認証情報に基づいて、完全性保護または暗号化のうちの少なくとも１つが行われる、

前記受信された認証局リストを使用してサーバを認証することと、
のためのコードを備えるコンピュータ可読媒体、
を備える、コンピュータプログラム製品。
［Ｃ７７］
コンピュータプログラム製品であって、
サーバのアドレスおよび受信報告構成を含むユーザサービス発見／アナウンスメントを受信することと、
前記受信報告構成に基づいて前記サーバに保護された受信報告を送ることと、
のためのコードを備えるコンピュータ可読媒体、
を備える、コンピュータプログラム製品。
［Ｃ７８］
ユーザ機器（ＵＥ）のコンピュータプログラム製品であって、
保護されたブロードキャストアナウンスメントを受信することと、前記ブロードキャストアナウンスメントは、前記ＵＥによって知られ、かつ前記ＵＥにおけるスマートカード上に記憶された認証情報に基づいて完全性保護または暗号化のうちの少なくとも１つが行われ、
前記ブロードキャストアナウンスメントに基づいて通信することと、
のためのコードを備えるコンピュータ可読媒体、
を備える、コンピュータプログラム製品。

【図１】

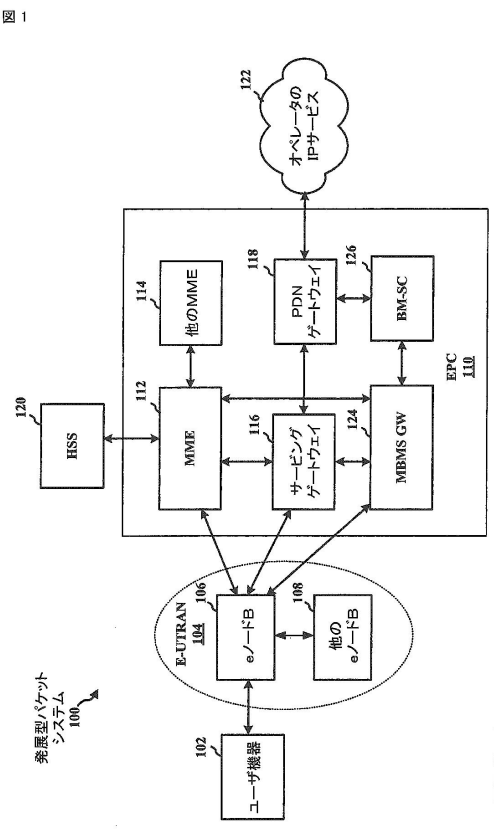

FIG. 1

【図２】

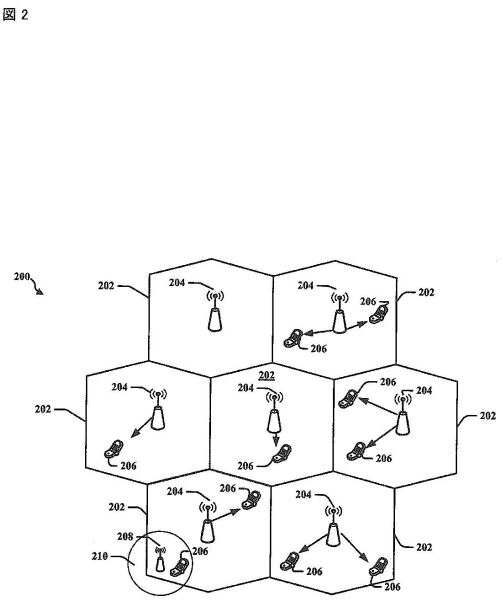

FIG. 2

【図３】

図３

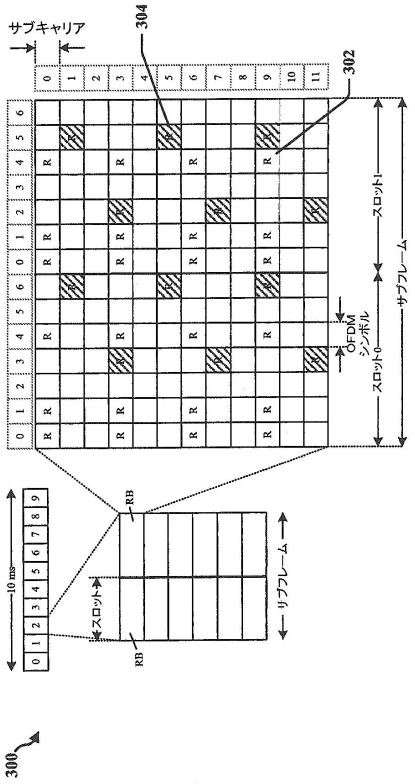

FIG. 3

【図４】

図４

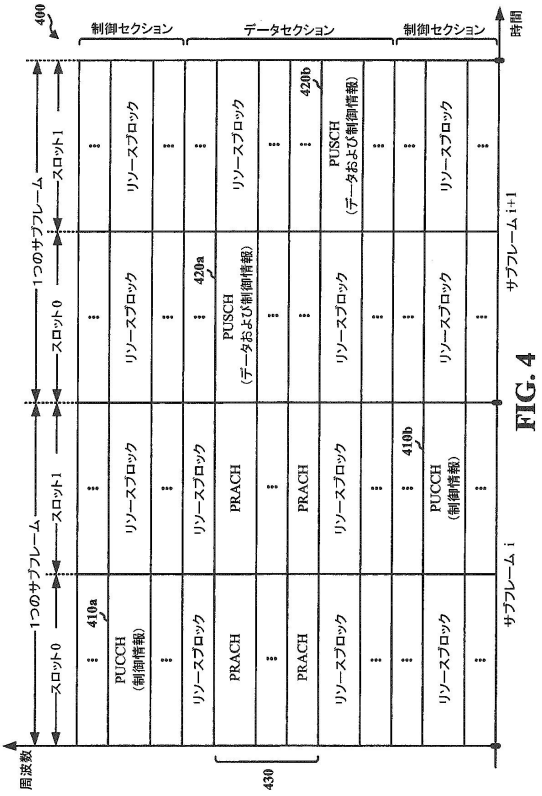

FIG. 4

【図５】

図５

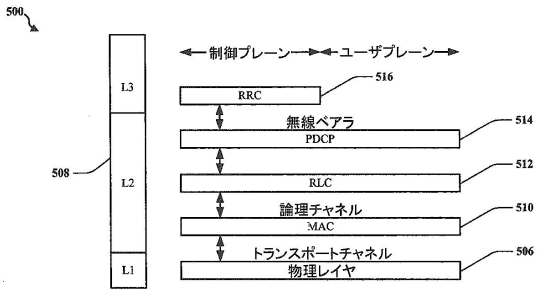

FIG. 5

【図６】

図６

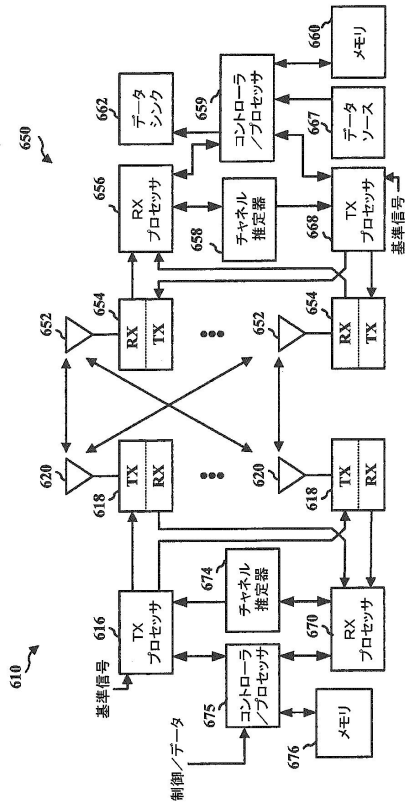

FIG. 6

【図７Ａ】

図 7A

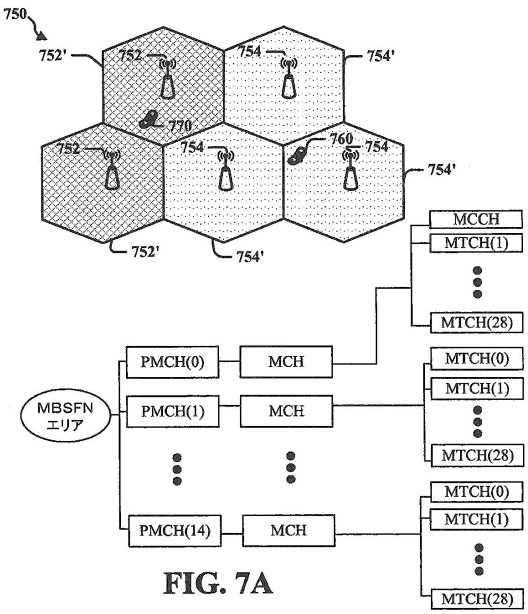

FIG. 7A

【図７Ｂ】

図 7B

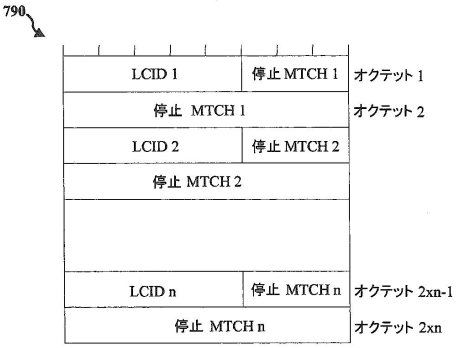

FIG. 7B

【図８】

図 8

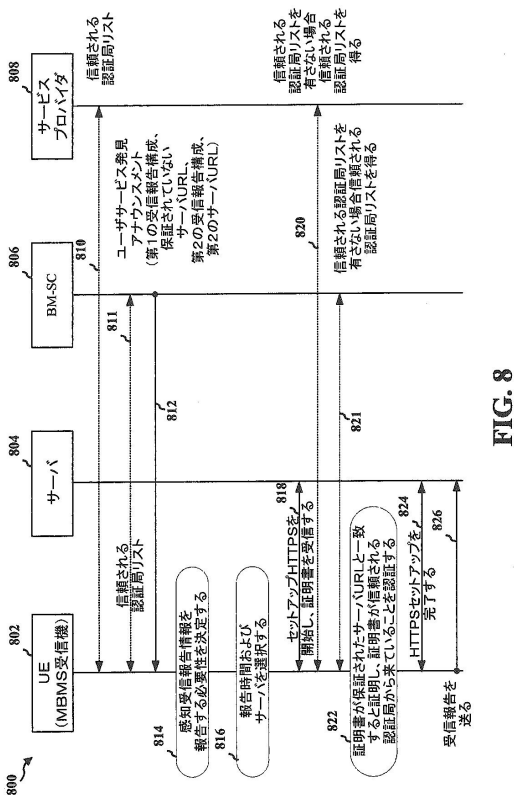

FIG. 8

【図９】

図 9

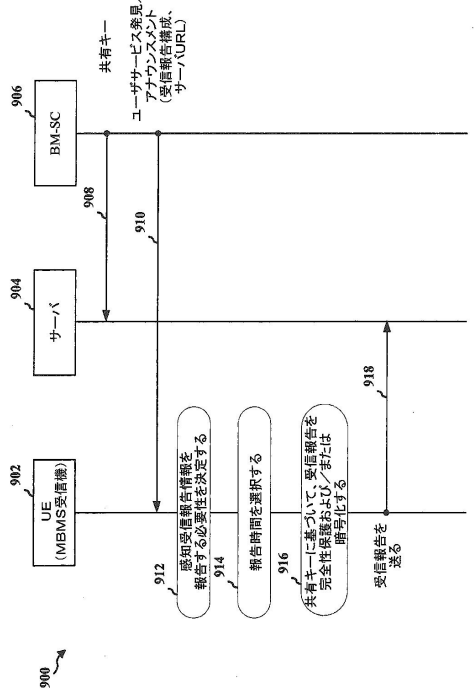

FIG. 9

【図１０】

図 10

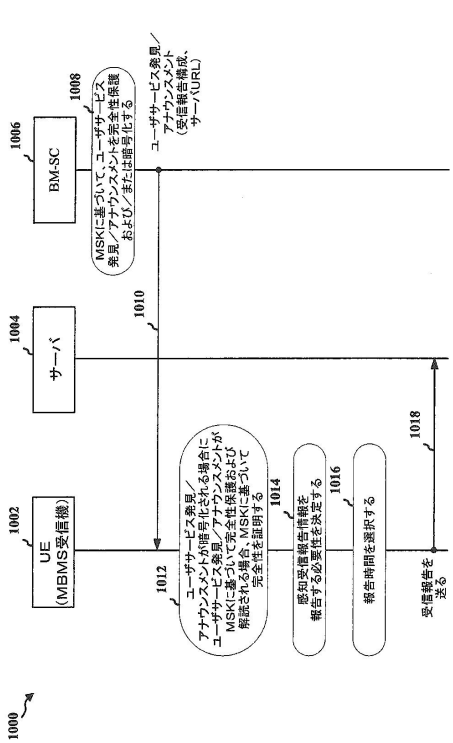

FIG. 10

【図１１】

図 11

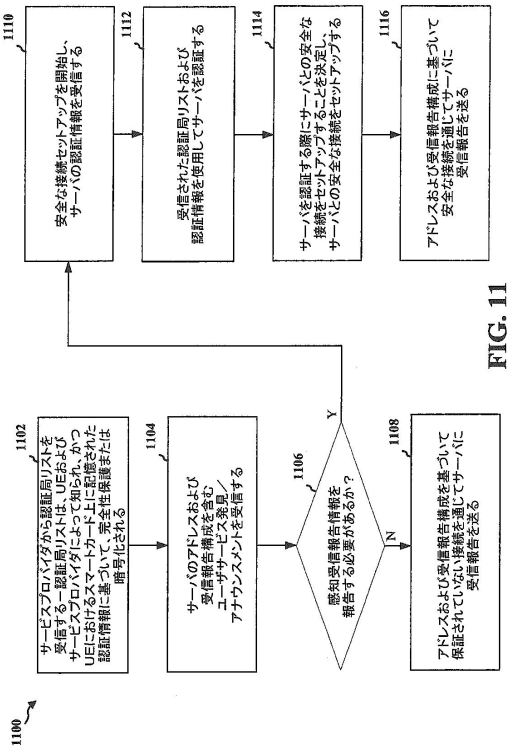

FIG. 11

【図１２】

図 12

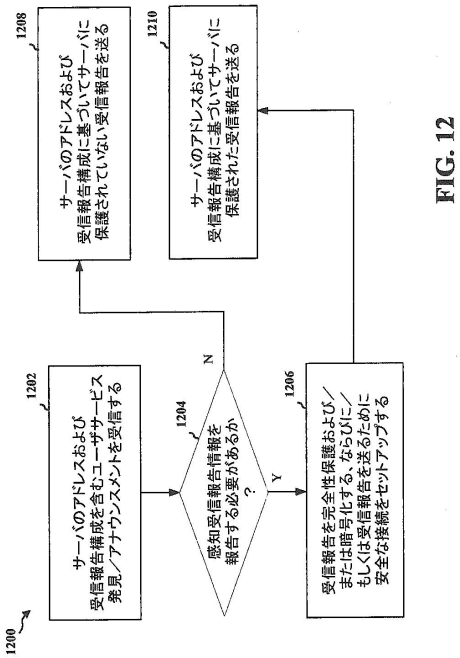

FIG. 12

【図１３】

図 13

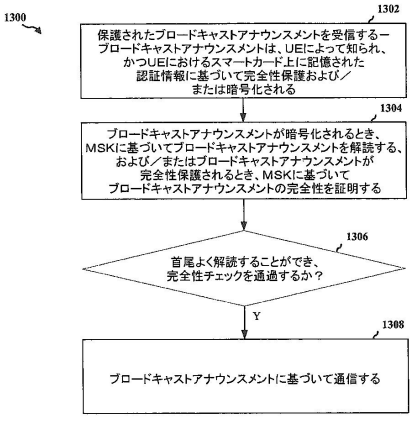

FIG. 13

【図１４】

図 14

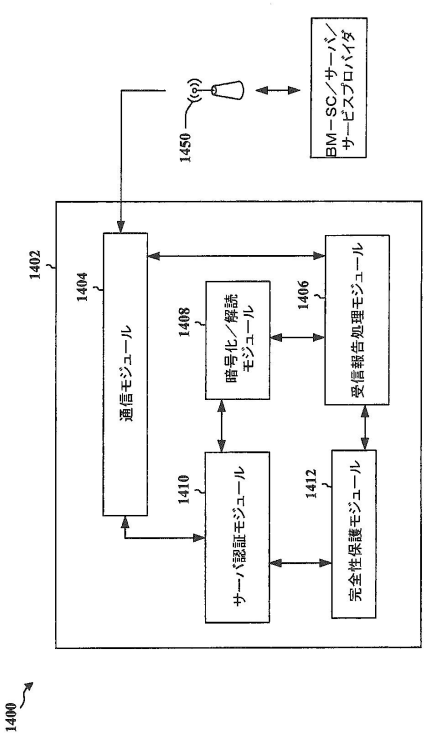

FIG. 14

【図１５】

図 15

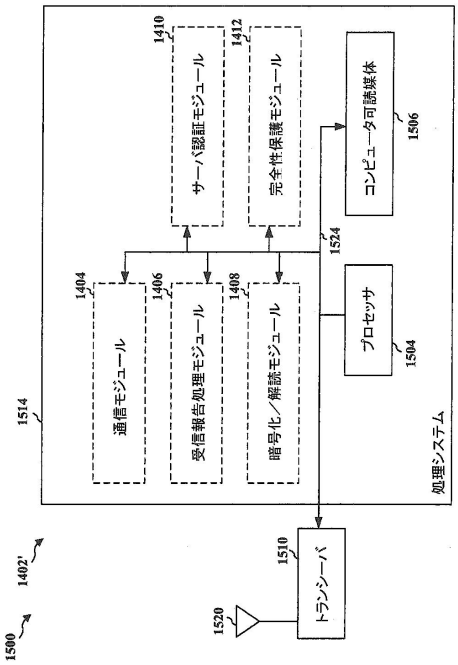

FIG. 15

フロントページの続き

(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100158805
弁理士 井関 守三
(74)代理人 100179062
弁理士 井上 正
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(72)発明者 パラニゴウンダー、アナンド
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５、クゥアルコム・インコーポレイテッド気付
(72)発明者 ワン、ジュン
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５、クゥアルコム・インコーポレイテッド気付
(72)発明者 ジャン、シャオシャ
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５、クゥアルコム・インコーポレイテッド気付
(72)発明者 ウォーカー、ゴードン・ケント
アメリカ合衆国、カリフォルニア州 ９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５、クゥアルコム・インコーポレイテッド気付

審査官 打出 義尚

(56)参考文献 特表２００９－５１２３２０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｈ０４Ｌ ９／０８