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

特許第5461563号
(P5461563)

(45)発行日　平成26年4月2日(2014.4.2)　(24)登録日　平成26年1月24日(2014.1.24)

(51)Int.Cl.		F I		
H04W 12/08	(2009.01)	H04W	12/08	
H04W 12/06	(2009.01)	H04W	12/06	
H04W 12/04	(2009.01)	H04W	12/04	
H04W 92/18	(2009.01)	H04W	92/18	
H04L 9/32	(2006.01)	H04L	9/00	675D

請求項の数 17　(全 43 頁)　最終頁に続く

(21)出願番号	特願2011-526905 (P2011-526905)
(86)(22)出願日	平成21年8月27日 (2009.8.27)
(65)公表番号	特表2012-502587 (P2012-502587A)
(43)公表日	平成24年1月26日 (2012.1.26)
(86)国際出願番号	PCT/US2009/055263
(87)国際公開番号	WO2010/030516
(87)国際公開日	平成22年3月18日 (2010.3.18)
審査請求日	平成23年5月16日 (2011.5.16)
(31)優先権主張番号	12/209,432
(32)優先日	平成20年9月12日 (2008.9.12)
(33)優先権主張国	米国(US)

(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　100159651
弁理士　高倉　成男
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】チケットベースのスペクトル認証およびアクセス制御

(57)【特許請求の範囲】

【請求項１】

第１のデバイスによって実行される、スペクトル認証およびアクセス制御のための方法であって、

信頼されるサードパーティによって発行された前記第１のデバイスに関する第１の認証チケットを獲得することであって、前記第１の認証チケットは、前記第１のデバイスによってアクセスされることが許されるサービスを備えることと、

前記第１の認証チケットを第２のデバイスに送信することと、

前記第２のデバイスから、前記信頼されるサードパーティ、または別の信頼されるパーティによって発行された、前記第２のデバイスに関する第２の認証チケットを受信することであって、前記第２の認証チケットは、前記第２のデバイスによってアクセスされることが許されるサービスを備えることと、

前記第２のデバイスとの有効にされた通信セッションを確立することと、

を備え、

前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成される方法。

【請求項２】

前記第２のデバイスと前記有効にされた通信セッションを確立する前に、前記第２のデバイスに関する前記第２の認証チケットを有効にすることをさらに備える、

請求項１に記載の方法。
【請求項３】
前記第２の認証チケットは、有効時間と、前記信頼されるサードパーティまたは前記別の信頼されるパーティの暗号署名とを含み、前記第２の認証チケットを有効にすることは、前記有効時間および前記暗号署名を検証することを含む、
請求項２に記載の方法。
【請求項４】
前記第２の認証チケットを有効にすることは、デジタル証明書の中に含まれる公開鍵とアイデンティティの両方に関連する秘密鍵の所有を検証することを備える、
請求項２に記載の方法。
【請求項５】
前記第２のデバイスに関する前記第２の認証チケットを有効にすることに失敗することは、前記第１のデバイスと前記第２のデバイスの間の通信リンクを解体することをもたらす、
請求項２に記載の方法。
【請求項６】
前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる情報に基づいて、前記有効にされた通信セッションをセキュリティで保護することをさらに備える、
請求項１に記載の方法。
【請求項７】
前記第１の認証チケットは、前記第１のデバイスの識別子と、前記信頼されるサードパーティの署名と、有効時間と、を備える、
請求項１に記載の方法。
【請求項８】
前記第１の認証チケットと前記第２の認証チケットの少なくともいずれかは、従来のデジタル証明書として実現される、
請求項１に記載の方法。
【請求項９】
信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得することであって、前記第１の認証チケットは、前記第１のデバイスによってアクセスされることが許されるサービスを備えることと、前記第１の認証チケットを第２のデバイスに送信することと、前記第２のデバイスから、前記第２のデバイスに関する第２の認証チケットを受信することであって、前記第２の認証チケットは、前記第２のデバイスによってアクセスされることが許されるサービスを備えることと、および前記第２のデバイスとの有効にされた通信セッションを確立すること、と関係する命令を保持するメモリと、なお、前記第２の認証チケットは、前記信頼されるサードパーティ、または別の信頼されるパーティによって発行され、前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成される
前記メモリに結合され、前記メモリの中に保持される前記命令を実行するように構成されるプロセッサと、
を備える無線通信装置。
【請求項１０】
前記メモリは、前記有効にされた通信セッションを確立する前に、前記第２のデバイスに関する前記第２の認証チケットを有効にすることと関係する命令をさらに保持し、前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成される、
請求項９に記載の無線通信装置。
【請求項１１】

前記第２のデバイスに関する前記第２の認証チケットを有効にすることに失敗することは、前記第１のデバイスと前記第２のデバイスの間の通信リンクを解体することをもたらす、

請求項１０に記載の無線通信装置。

【請求項１２】

前記第１の認証チケットは、前記第１のデバイスの識別子と、前記信頼されるサードパーティの署名と、有効時間とを備える、

請求項９に記載の無線通信装置。

【請求項１３】

スペクトル認証およびアクセス制御を円滑にする無線通信装置であって、

信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得するための手段であって、前記第１の認証チケットは、前記第１のデバイスによってアクセスされることが許されるサービスを備える手段と、

前記第１の認証チケットを第２のデバイスに伝送するための手段と、

前記第２のデバイスから、前記信頼されるサードパーティ、または別の信頼されるサードパーティによって発行された、前記第２のデバイスに関する第２の認証チケットを受信するための手段であって、前記第２の認証チケットは、前記第２のデバイスによってアクセスされることが許されるサービスを備える手段と、

前記第２のデバイスに関する前記第２の認証チケットを有効にするための手段と、

前記第２の認証チケットの前記有効確認が成功した場合、前記第２のデバイスとの有効にされた通信セッションを確立するための手段と、

を備え、

前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成される無線通信装置。

【請求項１４】

前記第１の認証チケットは、前記第１のデバイスの識別子と、前記信頼されるサードパーティの署名とを備え、前記第２の認証チケットは、前記第２のデバイスの識別子と、前記信頼されるサードパーティ、または前記別の信頼されるパーティの署名と、を備える、

請求項１３に記載の無線通信装置。

【請求項１５】

コンピュータに、信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得させるための第１のコードセットであって、前記第１の認証チケットは、前記第１のデバイスによってアクセスされることが許されるサービスを備える第１のコードセットと、

前記コンピュータに、前記第１の認証チケットを第２のデバイスに送信させるための第２のコードセットと、

前記コンピュータに、前記第２のデバイスから、前記信頼されるサードパーティ、または別の信頼されるパーティによって発行された、前記第２のデバイスに関する第２の認証チケットを受信させるための第３のコードセットであって、前記第２の認証チケットは、前記第２のデバイスによってアクセスされることが許されるサービスを備える第３のコードセットと、

前記コンピュータに、前記第２の認証チケットを有効にさせるための第４のコードセットと、

前記コンピュータに、前記第２の認証チケットが有効である場合、前記第２のデバイスとの有効にされた通信セッションを確立させるための第５のコードセットと、

を備え、

前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成されるコンピュータ可読記憶媒体。

【請求項１６】
スペクトル認証およびアクセス制御を提供するように構成された少なくとも１つのプロセッサであって、
信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得するための第１のモジュールであって、前記第１の認証チケットは、前記第１のデバイスによってアクセスされることが許されるサービスを備える第１のモジュールと、
前記第１の認証チケットを第２のデバイスに伝送するための第２のモジュールと、
前記第２のデバイスから、前記信頼されるサードパーティ、または別の信頼されるサードパーティによって発行された、前記第２のデバイスに関する第２の認証チケットを受信するための第３のモジュールであって、前記第２の認証チケットは、前記第２のデバイスによってアクセスされることが許されるサービスを備える第３のモジュールと、
前記第２のデバイスに関する前記第２の認証チケットを有効にするための第４のモジュールと、
前記第２の認証チケットの前記有効確認が成功した場合、前記第２のデバイスとの有効にされた通信セッションを確立するための第５のモジュールと、
を備え、
前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成されるプロセッサ。
【請求項１７】
前記第１の認証チケットは、前記第１のデバイスによってアクセスされることが許されるサービスを備え、前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成される、
請求項１６に記載の少なくとも１つのプロセッサ。
【発明の詳細な説明】
【技術分野】
【０００１】
以下の説明は、一般に、無線通信に関し、より詳細には、認可されたスペクトルを介する通信を認証することに関する。
【背景技術】
【０００２】
無線通信システムは、ユーザがどこに位置しているか（構造物の中または外）にかかわらず、さらにユーザが静止しているか、動いているか（例えば、車両内にいる、歩いている）にかかわらず、様々なタイプの通信を提供するように、さらに情報を転送するように広く展開される。例えば、音声、データ、ビデオなどが、無線通信システムを介して提供されることができる。通常の無線通信システム、または無線通信ネットワークは、複数のユーザに１つまたは複数の共有リソースへのアクセスを提供することができる。例えば、システムは、周波数分割多重化（ＦＤＭ）、時分割多重化（ＴＤＭ）、符号分割多重化（ＣＤＭ）、直交周波数分割多重化（ＯＦＤＭ）、その他などの様々な多元接続技術を使用することができる。
【０００３】
一般に、無線通信ネットワークは、基地局またはアクセスポイントと通信するデバイスを介して確立される。アクセスポイントは、或る地理的範囲、またはセルを範囲に含み、デバイスが動作させられる際、デバイスは、これらの地理的セルを出入りするように移動させられることができる。
【０００４】
また、ネットワークは、アクセスポイントを利用せずに、ピアツーピアデバイスだけを利用して構築されることも可能であり、あるいはネットワークは、アクセスポイントとピ

アツーピアデバイスをともに含むこともできる。これらのタイプのネットワークは、ときとして、アドホックネットワークと呼ばれる。アドホックネットワークは、或るデバイス（またはアクセスポイント）が別のデバイスから通信を受信すると、その別のデバイスがネットワークに追加される自己構成型であることができる。デバイスがその区域を離れる際、それらのデバイスは、ネットワークから動的に取り除かれる。このため、このネットワークのトポグラフィは、絶えず変化していることができる。

【０００５】

アドホックネットワークは、通信デバイスが、移動中に情報を送信する、さらに／または受信することを可能にする。通信は、複数のタイプのデータの伝送に利用される広い範囲の電磁無線周波数を備える貴重な、限られたリソースであるスペクトルを使用して確立される。アドホックネットワークは、デバイスへの情報の転送、およびデバイスからの情報の転送を可能にするために、例えば、有線アクセスポイントおよび／または無線アクセスポイントを介して、他の公共ネットワークまたはプライベートネットワークに通信するように結合されることができる。そのようなアドホックネットワークは、通常、ピアツーピアで通信する複数のデバイスを含む。また、アドホックネットワークは、デバイス間のピアツーピア通信を円滑にする強力な信号を発信するビーコンポイントを含むこともできる。例えば、発信されたビーコンは、そのようなデバイスのタイミング同期を助けるタイミング情報を含むことができる。これらのビーコンポイントは、デバイスが様々なカバレッジエリア内で、さらにそのようなカバレッジエリアをまたいで移動するので、広域カバレッジを提供するように配置される。

【０００６】

通信システムが、事業者所有のアクセスポイントを要求しないが、スペクトル所有者／ライセンス保持者／プロバイダに所属する認可されたスペクトルを利用する場合、認証されたデバイスだけが、そのスペクトルを使用できるようにされなければならない。スペクトル所有者／ライセンス保持者がスペクトルライセンス料の補償を受けるために、スペクトルの認証は、スペクトルプロバイダ、またはスペクトルプロバイダの仲介代理業者とビジネス関係を有するユーザまたは組織に関連付けられたデバイスに与えられる。

【０００７】

このため、スペクトルプロバイダは、サービス契約に従ってスペクトルを利用するようにデバイスを認証し、認証するために、ユーザサービス契約によって、またはスペクトルプロバイダ管理部門によって規定されたタイムラインで、またはそのようなイベントがあると、デバイスと通信するコアネットワークノードもしくはノードのセットである認証サーバを使用することによって、スペクトルの使用を制御することができる。

【０００８】

スペクトルを使用するアドホック通信に関連付けられているのが、そのようなリンクを適切に利用するのに必要な一連の構成パラメータである。これらのパラメータは、ＩＰ（インターネットプロトコル）アドレス、上位層識別子もしくはネットワーク層識別子、サービス識別子などである。これらのパラメータの構成の誤りは、セキュリティ侵害をもたらす可能性がある。例えば、（不正を行う）デバイスが、別のネットワークノードに属するＩＰアドレスを、その（盗まれた）ＩＰアドレスが、その不正を行うデバイスに属するかのように利用することができる場合、その不正を行うデバイスと通信するピアは、このネットワークノードに向けられたデータトラフィックが、その不正を行うデバイスにリダイレクトされることを意図せずに生じさせる可能性がある。

【発明の概要】

【０００９】

以下に、１つまたは複数の態様の簡略化された概要を、そのような態様の基本的理解をもたらすために提示する。この概要は、企図されるすべての態様の広範な概観ではなく、任意またはすべての態様の重要なエレメントもしくは不可欠なエレメントを特定することも、いずれか、もしくはすべての態様の範囲を線引きすることも意図していない。この概要の唯一の目的は、後段で提示されるより詳細な説明の前置きとして、１つまたは複数の

態様のいくつかの概念を簡略化された形態で提示することである。

【００１０】

１つまたは複数の態様、およびそれらの態様の対応する開示によれば、認可されたスペクトルを利用して他のデバイスと直接に通信するようにデバイスを認証することに関連する様々な態様が説明される。一部の態様によれば、この認証は、規定されたユーザ／サービス契約に基づく。スペクトルの正しい使用を可能にするように用いられる構成パラメータが、スペクトルプロバイダ認証サーバによって保証されることが可能であり、このため、ピアデバイスによって検証されることができる。そのようなピアデバイスは、スペクトル認証されていることが可能であり、さらに、そのスペクトルを利用するピアツーピア／アドホック通信のプロセスにおいて利用されることが可能な認証された構成パラメータを備える。

【００１１】

或る態様は、スペクトル認証およびアクセス制御のための方法に関する。この方法は、信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得することを含む。また、この方法は、第２のデバイスから、第２のデバイスに関する第２の認証チケットを受信することも含む。第２の認証チケットは、その信頼されるサードパーティ、または別の信頼されるパーティによって発行される。また、この方法は、第２のデバイスとの有効にされた通信セッションを確立することも含む。

【００１２】

別の態様は、メモリと、プロセッサとを含む無線通信装置に関する。このメモリは、信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得すること、および第２のデバイスから、第２のデバイスに関する第２の認証チケットを受信することと関係する命令を保持する。第２の認証チケットは、その信頼されるサードパーティ、または別の信頼されるパーティによって発行される。また、メモリは、第２のデバイスとの有効にされた通信セッションを確立することと関係する命令も保持する。プロセッサは、メモリに結合され、メモリの中に保持される命令を実行するように構成される。

【００１３】

さらなる態様は、スペクトル認証およびアクセス制御を円滑にする無線通信装置に関する。この装置は、信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得するための手段と、第１の認証チケットを第２のデバイスに伝送するための手段とを含む。また、この装置は、第２のデバイスから、第２のデバイスに関する第２の認証チケットを受信するための手段も含む。第２の認証チケットは、その信頼されるサードパーティ、または別の信頼されるサードパーティによって発行される。やはり、この装置に含まれるのが、第２のデバイスに関する第２の認証チケットを有効にするための手段、および第２の認証チケットの有効確認が成功した場合、第２のデバイスとの有効にされた通信セッションを確立するための手段である。

【００１４】

さらに別の態様は、信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットをコンピュータに獲得させるための第１のコードセットを含む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に関する。また、このコンピュータ可読媒体は、第２のデバイスから、第２のデバイスに関する第２の認証チケットをコンピュータに受信させるための第２のコードセットと、第２の認証チケットをコンピュータに有効にさせるための第３のコードセットとをさらに含む。第２の認証チケットは、信頼されるサードパーティ、または別の信頼されるパーティによって発行される。また、コンピュータ可読媒体は、第２の認証チケットが有効である場合、第２のデバイスとの有効にされた通信をコンピュータに確立させるための第４のコードセットも含む。

【００１５】

さらに別の態様は、スペクトル認証およびアクセス制御を提供するように構成された少なくとも１つのプロセッサに関する。このプロセッサは、信頼されるサードパーティによ

って発行される第１のデバイスに関する第１の認証チケットを獲得するための第１のモジュールと、第１の認証チケットを第２のデバイスに送信するための第２のモジュールとを含む。また、第２のデバイスから、第２のデバイスに関する第２の認証チケットを受信するための第３のモジュールもプロセッサに含まれる。第２の認証チケットは、その信頼されるサードパーティ、または別の信頼されるサードパーティによって発行される。さらに、プロセッサは、第２のデバイスに関する第２の認証チケットを有効にするための第４のモジュールと、第２の認証チケットの有効確認が成功した場合、第２のデバイスとの有効にされた通信セッションを確立するための第５のモジュールとを含む。

【００１６】

別の態様は、スペクトル認証およびアクセス制御のための方法に関する。この方法は、第１のデバイスからシステムアクセスを求める要求を受信すること、および第１のデバイスの認証を実行することを含む。また、この方法は、第１のデバイスに関するシステムアクセスを許すこと（認証すること）、および認証されたシステムアクセスに基づいて、第１のデバイスに関する認証チケットを作成することも含む。

【００１７】

さらなる態様は、メモリと、プロセッサとを含む無線通信装置に関する。プロセッサは、メモリに結合され、メモリの中に保持される命令を実行するように構成される。メモリは、少なくとも第１のデバイスからシステムアクセスを求める要求を受信すること、および少なくとも第１のデバイスの認証を実行することと関係する命令を保持する。また、メモリは、第１のデバイスにシステムアクセスを許すこと（認証すること）、および認証されたシステムアクセスに部分的に基づいて、少なくとも第１のデバイスに関する認証チケットを生成することと関係する命令も保持する。

【００１８】

さらに別の態様は、スペクトル認証を提供する無線通信装置に関する。この装置は、少なくとも第１のデバイスからシステムアクセスを求める要求を受信するための手段と、少なくとも第１のデバイスの認証を実行するための手段とを含む。また、この装置は、少なくとも第１のデバイスにシステムアクセスを許す（認証する）ための手段と、少なくとも第１のデバイスの認証されたシステムアクセスに部分的に基づいて、少なくとも第１のデバイスに関する認証チケットを生成するための手段とをさらに含む。

【００１９】

さらに別の態様は、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に関する。コンピュータ可読媒体は、第１のデバイスからシステムアクセスを求める要求をコンピュータに受信させるための第１のコードセットと、第１のデバイスの認証をコンピュータに実行させるための第２のコードセットとを含む。また、コンピュータ可読媒体は、第１のデバイスにシステムアクセスをコンピュータに許させる（認証させる）ための第３のコードセットと、認証されたシステムアクセスに基づいて、第１のデバイスに関する認証チケットをコンピュータに生成させるための第４のコードセットとをさらに含む。

【００２０】

さらなる態様は、スペクトル認証を提供するように構成された少なくとも１つのプロセッサに関する。このプロセッサは、少なくとも第１のデバイスからシステムアクセスを求める要求を受信するための第１のモジュールと、少なくとも第１のデバイスの認証を実行するための第２のモジュールとを含む。また、このプロセッサは、少なくとも第１のデバイスにシステムアクセスを許す／認証するための第３のモジュールと、少なくとも第１のデバイスに与えられた認証されたシステムアクセスに部分的に基づいて、少なくとも第１のデバイスに関する認証チケットを生成するための第４のモジュールとをさらに含む。この認証チケットは、少なくとも第１のデバイスのアイデンティティと、この認証チケットが有効である有効範囲（validity range）と、暗号署名とを備える。

【００２１】

以上、および関連する目的を達するのに、１つまたは複数の態様は、後段で完全に説明され、特許請求の範囲において特に指摘される特徴を備える。後段の説明、および添付の

図面は、１つまたは複数の態様のいくつかの例示的な特徴を詳細に説明する。しかし、これらの特徴は、様々な態様の原理が使用されることが可能な、様々な様態のいくつかを示すに過ぎない。他の利点、および新たな特徴は、後段の詳細な説明が図面と併せて考慮されると、明白となり、開示される態様は、すべてのそのような態様、および均等の態様を含むことを意図している。

【図面の簡単な説明】

【００２２】

【図１】様々な態様による無線通信システムを示す図。

【図２】スペクトル使用認証のためのシステムを示す図。

【図３】認証サーバから認証を獲得するデバイスの動作を示すフローチャート図。

【図４】開示される態様で利用され得る例示的な認証チケットを示す図。

【図５】本明細書で開示される様々な態様による、スペクトル使用認証および／または関連する構成パラメータを最初に有効にすることによって、有効にされた通信リンクを確立する２つのデバイスの動作を示すフローチャート図。

【図６】１つまたは複数の態様によるチケットベースのスペクトル認証およびアクセス制御のためのシステムを示す図。

【図７】スペクトル認証およびアクセス制御のためのシステムを示す図。

【図８】チケットベースの構成パラメータの有効確認のためのシステムを示す図。

【図９】チケットベースの構成パラメータの有効確認のための別のシステムを示す図。

【図１０】スペクトル認証およびアクセス制御のための方法を示す図。

【図１１】スペクトル認証およびアクセス制御のための方法を示す図。

【図１２】チケットベースの構成パラメータを有効にするための方法を示す図。

【図１３】チケットベースの構成パラメータを有効確認するための方法を示す図。

【図１４】開示される態様によるチケットベースの認証および有効確認を円滑にするシステムを示す図。

【図１５】アドホック（ピアツーピア）環境におけるスペクトル認証およびアクセス制御を円滑にする例示的なシステムを示す図。

【図１６】スペクトル認証を提供する例示的なシステムを示す図。

【図１７】通信環境においてチケットベースの構成パラメータを有効にする例示的なシステムを示す図。

【図１８】チケットベースの構成パラメータを有効にする例示的なシステムを示す図。

【発明を実施するための形態】

【００２３】

次に、図面を参照して様々な態様を説明する。以下の説明では、説明の目的で、１つまたは複数の態様の徹底的な理解をもたらすために多数の特定の詳細が示される。しかし、そのような態様（複数可）は、これらの特定の詳細なしに実施されてもよいことが明白であり得る。その他、よく知られた構造およびデバイスは、これらの態様を説明することを容易にするためにブロック図形態で示される。

【００２４】

本出願において使用される「コンポーネント」、「モジュール」、「システム」などの用語は、ハードウェア、ファームウェア、ハードウェアとソフトウェアの組み合わせ、ソフトウェア、または実行中のソフトウェアである、コンピュータ関連エンティティを指すことを意図している。例えば、コンポーネントは、プロセッサ上で実行されているプロセス、プロセッサ、オブジェクト、実行可能ファイル、実行のスレッド、プログラム、および／またはコンピュータであることができるが、以上には限定されない。例として、コンピューティングデバイス上で実行されているアプリケーションと、そのコンピューティングデバイスがともに、コンポーネントであり得る。１つまたは複数のコンポーネントが、プロセス内、および／または実行のスレッド内に存在することが可能であり、コンポーネントは、１つのコンピュータ上に局所化される、さらに／または２つ以上のコンピュータの間に分散されることができる。さらに、これらのコンポーネントは、様々なデータ構造

が格納されている様々なコンピュータ可読媒体から実行されることができる。これらのコンポーネントは、１つまたは複数のデータパケットを有する信号に従うなどして、ローカルプロセスおよび／または遠隔プロセスを介して通信することができる（例えば、１つのコンポーネントからのデータが、信号によってローカルシステムにおける別のコンポーネント、分散システムにおける別のコンポーネント、さらに／またはインターネットなどのネットワークを介する他のシステムと対話して）。

【００２５】

さらに、様々な態様が、デバイスに関連して本明細書で説明される。デバイスは、システム、加入者ユニット、加入者局、移動局、移動体、無線端末装置、デバイス、移動デバイス、遠隔局、遠隔端末装置、アクセス端末装置、ユーザ端末装置、端末装置、無線通信デバイス、無線通信装置、ユーザエージェント、ユーザデバイス、またはユーザ機器（ＵＥ）と呼ばれることも可能であり、以上の機能の一部またはすべてを含むことができる。移動デバイスは、セルラ電話機、コードレス電話機、セッション開始プロトコル（ＳＩＰ）電話機、スマートフォン、無線ローカルループ（ＷＬＬ）局、ＰＤＡ（携帯情報端末）、ラップトップ、ハンドヘルド通信デバイス、ハンドヘルドコンピューティングデバイス、衛星ラジオ、無線モデムカード、および／または無線システムを介して通信するための別の処理デバイスであることができる。さらに、様々な態様が、基地局に関連して本明細書で説明される。基地局は、無線端末装置（複数可）と通信するために利用されることが可能であり、さらにアクセスポイント、ノードＢ、または他の何らかのネットワークエンティティと呼ばれることが可能であり、以上の機能の一部またはすべてを含むことができる。

【００２６】

様々な態様または特徴が、いくつかのデバイス、コンポーネント、モジュールなどを含むことが可能なシステムに関連して提示される。様々なシステムは、さらなるデバイス、コンポーネント、モジュールなどを含むことが可能であり、さらに／または図に関連して説明されるデバイス、コンポーネント、モジュールなどのすべてを含むわけではないこともあり得ることを理解し、認識されたい。また、これらのアプローチの組み合わせが使用されることもできる。

【００２７】

次に図１を参照すると、例示されているのは、様々な態様による無線通信システム１００である。システム１００は、複数のアンテナグループを含むことが可能な基地局１０２を備える。例えば、１つのアンテナグループが、アンテナ１０４および１０６を含むことが可能であり、別のグループが、アンテナ１０８および１１０を備えることが可能であり、さらなるグループが、アンテナ１１２および１１４を含むことができる。各アンテナグループにつき２つのアンテナが例示されるが、各グループにつき、より多くの、またはより少ないアンテナが利用されることもできる。基地局１０２は、送信機チェーンと、受信機チェーンとをさらに含むことが可能であり、送信機チェーンおよび受信機チェーンのそれぞれは、当業者には認識されるとおり、信号送信および信号受信に関連する複数のコンポーネント（例えば、プロセッサ、変調器、多重化装置、復調器、逆多重化装置、アンテナなど）を備えることができる。さらに、基地局１０２は、ホーム基地局、フェムト基地局、および／または以上に類するものであることができる。

【００２８】

基地局１０２は、デバイス１１６などの１つまたは複数のデバイスと通信することができるが、基地局１０２は、デバイス１１６と同様の、実質的に任意の数のデバイスと通信することができることを認識されたい。図示されるとおり、デバイス１１６は、アンテナ１０４および１０６と通信状態にあり、ただし、アンテナ１０４および１０６は、順方向リンク１１８を介してデバイス１１６に情報を送信し、逆方向リンク１２０を介してデバイス１１６から情報を受信する。

【００２９】

例えば、周波数分割複信（ＦＤＤ）システムにおいて、順方向リンク１１８は、逆方向

リンク１２０によって使用されるのとは異なる周波数帯域を利用することができる。さらに、時分割複信（ＴＤＤ）システムにおいて、順方向リンク１１８と逆方向リンク１２０は、共通の周波数帯域を利用することができる。

【００３０】

さらに、デバイス１２２とデバイス１２４は、ピアツーピア構成などで、互いに通信していることができる。さらに、デバイス１２２は、リンク１２６および１２８を使用してデバイス１２４と通信状態にある。ピアツーピアアドホックネットワークにおいて、デバイス１２２および１２４などの、互いの範囲内にあるデバイスは、それらのデバイスの通信を中継する基地局１０２および／または有線インフラストラクチャなしに、互いに直接に通信する。さらに、ピアデバイスまたはピアノードは、トラフィックを中継することができる。ピアツーピア様態で通信するネットワーク内のデバイスは、基地局と同様に機能することができ、トラフィックが最終の宛先に到達するまで、基地局と同様に機能して、他のデバイスにトラフィックまたは通信を中継することができる。また、デバイスは、ピアデバイス間のデータ伝送を管理するのに利用されることが可能な情報を伝送する、制御チャネルを伝送することもできる。

【００３１】

通信ネットワークは、無線通信状態にある任意の数のデバイスまたはノードを含むことができる。各デバイスまたは各ノードは、他の１つまたは複数のデバイスまたはノードの範囲内にあることが可能であり、さらに、マルチホップトポグラフィなどにおいて、その他のデバイス／ノードと、またはその他のデバイス／ノードの利用を介して通信することができる（例えば、通信は、最終の宛先に到達するまで、ノードからノードへとホップすることができる）。例えば、送信側デバイスが、受信側デバイスと通信することを所望することができる。送信側デバイスと受信側デバイスの間でパケット転送を可能にするのに、１つまたは複数の中間デバイスが利用されることができる。任意のデバイスが送信側デバイスおよび／または受信側デバイスであることが可能であり、実質的に同時に情報を送信する、さらに／または受信する機能を実行することができる（例えば、情報を受信するのと実質的に同時に、さらに／または異なる時点で情報をブロードキャストする、または通信することができる）ことを理解されたい。

【００３２】

システム１００は、認証されたデバイスによるデータ通信のために或るスペクトルの使用を可能にするように構成されることが可能であり、認証されていないデバイス（例えば、従来のデバイス、もしくは一般的なデバイス）は、そのスペクトルを使用することができない。デバイスの証明書（credential）、およびそのデバイスが受ける権利があるサービスの有効確認の後、認証チケットが、信頼されるサードパーティによって配信されることができる。さらに、システム１００は、そのスペクトルを利用して無線リンクを構成するための条件として、デバイスによる認証チケットの交換および検証を義務付けることができる。

【００３３】

図２は、スペクトル使用認証のためのシステム２００を示す。システム２００は、デバイス間で（例えば、ピアツーピア様態で）、またはデバイスと基地局の間で、スペクトルプロバイダ（または信頼されるサードパーティ）によって認証された（または保証された）通信を可能にするように構成されることができる。

【００３４】

システム２００は、認証サーバ２０２と、構成パラメータデータベース２０４とを含む。認証サーバ２０２は、構成パラメータデータベース２０４と並置されること、または通信するように結合されることができる。やはり、システム２００に含まれるのが、デバイス$_1$２０６およびデバイス$_N$２０８というラベルが付けられたデバイスであり、ただし、Ｎは整数である。デバイス２０６、２０８は、開示される態様による移動デバイスと同様に動作する移動デバイスおよび／または基地局であることができる（例えば、基地局が、通常、他のネットワークまたはインフラストラクチャに接続されるという事実は、開示され

る態様に関係がない）。デバイス２０６、２０８は、無線で、互いに通信することができ（双方向通信リンク２１０によって図示される）、さらに他のデバイスと通信することができる。さらに、デバイス２０６、２０８は、認証サーバ２０２と無線で、または有線リンクを介して（双方向通信リンク２１２および２１４によって図示される）通信することができる。デバイス２０６、２０８と認証サーバ２０２の間の通信が無線である場合、この通信は、デバイス２０６、２０８によって互いに通信するのに使用される認可されたスペクトルなどの、認可されたスペクトルを介しても、介さなくてもよい。一部の態様によれば、デバイス間のリンク（リンク２１０）と、１つまたは複数のデバイス２０６、２０８と認証サーバ２０２の間のリンク（リンク２１２または２１４）は、同一のリンク、または同様のリンクであることができる。

【００３５】

認証サーバ２０２は、認可されたスペクトルなどのスペクトルの使用に関する認証を、１つまたは複数のデバイス２０６、２０８に選択的に配信することができる。この認証は、認証チケット$_1$２１６および認証チケット$_M$２１８として図示される認証チケットの形態で配信されることが可能であり、ただし、Ｍは整数である。認証チケット２１６、２１８は、デバイス識別子、有効期間（validity period）、認証するデバイス（例えば、認証サーバ２０２）の暗号署名、ならびに他の情報などの様々な情報を含むことができる。認証チケットと関係するさらなる情報は、後段で与えられる。

【００３６】

認証チケット２１６、２１８は、デバイス２０６、２０８によって、デバイス２０６、２０８間の通信を可能にするのに利用されることができる。一部の態様によれば、認証チケット２１６、２１８は、そのスペクトルの或る使用を認証する（例えば、サービスを認証する）のに利用されることができる。一部の態様によれば、認証チケット２１６、２１８は、ネットワーク層プロトコルを使用して１つまたは複数のデバイス２０６、２０８に配信されることができる。（認可された）スペクトルへの認証が与えられないデバイスは、認証チケットを受信しないことを理解されたい。

【００３７】

認証チケットを配信するのに、認証サーバ２０２は、１つまたは複数のデバイス２０６、２０８と定期的に（例えば、１ヶ月に１回、別の所定の間隔で）通信し、各デバイスに適切な認証チケットを個々に提供することができる。例えば、認証サーバ２０２は、デバイスに以前に送信された認証チケットとは異なる有効範囲を有する新たな認証チケットを送信することができる。各デバイス２０６、２０８は、別のデバイスに供給される認証チケットとは異なる認証チケットを受信する。例えば、認証サーバ２０２は、デバイス$_1$２０６に認証チケット$_1$２１６を送信し、デバイス$_N$２０８に認証チケット$_M$２１８を送信する。各デバイス２０６、２０８は、記憶媒体の中などに、そのデバイス２０６、２０８の認証チケットを保持することができる。

【００３８】

デバイス２０６、２０８は、認証チケットを交換して、互いの間で有効にされた通信リンク２１０を確立する。したがって、デバイス$_1$２０６は、デバイス$_N$２０８に認証チケット$_1$２１６を送信し、デバイス$_N$２０８は、デバイス$_1$２０６に認証チケット$_M$２１８を送信する。認証チケットの有効確認は、デバイス（例えば、２つの移動デバイス、移動デバイスとアクセスポイントなど）が、開示される態様に従ってピアツーピア様態で通信することを可能にする。デバイスが、そのデバイスが通信することを所望するデバイスの認証チケットを有効にすることができない場合、それらのデバイス間で有効にされた通信リンクは確立されない。

【００３９】

図３は、認証サーバから認証を獲得するデバイスの動作のフローチャート図３００を示す。認証サーバ２０２は、デバイス$_1$２０６などのデバイスに認証チケットを発行する信頼されるパーティであることができる。認証サーバ２０２は、実質的に同時に、または異なる時点で複数のデバイスに認証チケットを発行することができることを認識されたい。

しかし、簡明のため、１つだけのデバイスが図示される。

【００４０】

認証チケットの発行を開始するのに、デバイス２０６は、デバイスの少なくとも固有の識別子（例えば、Ｄｅｖｉｃｅ＿ＩＤ＿１）を含む認証要求メッセージ３０２を送信する。一部の態様によれば、認証要求メッセージ３０２は、公開鍵などの他の証明書情報を含むことができる。

【００４１】

デバイス２０６は、以前に獲得された認証チケット（例えば、デバイスが、他のデバイスと通信するのに現在、使用している認証チケット）の近づいている失効の検出に基づいて、認証要求メッセージ３０２を送信するようにトリガされることができる。一部の態様によれば、認証要求メッセージ３０２を送信することは、デバイスの中に（例えば、記憶媒体の中に）保持されている有効な認証チケットが存在しない間、無線リンクを可能にするようにというユーザアプリケーションへの命令によってトリガされることができる。

【００４２】

さらに、または代替として、デバイス２０６は、認証サーバ２０２から受信された要求に基づいて、認証要求メッセージ３０２を送信するようにトリガされることができる。認証サーバ２０２は、運営管理上の理由で、さらに／または以前の認証チケットの下で、そのデバイスによって送信／受信されることが認証されていたデータの量または割り当て量を超えた（または超える）ことが示されたことに基づいて、この要求を送信することができる。この代替の態様では、認証要求メッセージ３０２の送信に先立って、認証サーバ２０２からメッセージ（図示せず）が受信される。

【００４３】

認証要求メッセージ３０２を受信するのと実質的に同時に、認証サーバ２０２は、デバイス２０６のアイデンティティ、およびデバイス２０６が受ける権利があるサービス（例えば、購入されたサービス、現在のプランの下で許されるサービス、プロモーション期間中、費用なしで許されるサービスなど）を検証する。このことが、３０４における二重の双方向矢印（認証機構）によって図示される。この検証プロセスは、「認証」、「認証」、「アカウンティングプロトコル」、および／または「認証プロトコル」と呼ばれることができる。そのようなプロトコルの例には、ＴＬＳ（トランスポートレベルセキュリティ）、インターネット鍵交換（ＩＫＥ）、およびその他が含まれる。

【００４４】

一部の態様によれば、デバイス２０６は、メッセージ交換３０４の一環として認証サーバ２０２によって送信されたチャネルメッセージに応答して、証明書情報を送信する。他の態様によれば、デバイス２０６と認証サーバ２０２の両方が、相互認証手順を実行し、通常、デバイス２０６と認証サーバ２０２の間の通信チャネルをセキュリティで保護するため、それぞれの証明書情報を交換する。

【００４５】

デバイス２０６のアイデンティティが検証された場合、認証サーバ２０２は、構成パラメータを割り当て／生成し、さらに認証サーバ２０２によって作成される認証チケットの中に、この情報を含める。さらに、または代替として、認証サーバ２０２は、他の１つまたは複数のデータベースまたはサーバと連携して、これらの構成パラメータを割り当てる／生成することができる。

【００４６】

一部の態様によれば、この新たに作成された認証チケットは、デバイス２０６に供給された以前の認証チケットと実質的に同一である。しかし、この新たに作成された認証チケットは、異なる有効期間（開始時間／終了時間）、および異なる暗号署名を有することができる。一部の態様によれば、この新たに作成された認証チケットは、（例えば、より多くのサービス、より少ないサービス、異なるサービスなど）以前の認証チケットによって認証されたサービスと同一である、または異なるサービスの認証を含むことができる。この認証チケットと関係するさらなる情報は、図４を参照してさらに詳細に説明される。

【００４７】
この新たに作成された認証チケットは、認証応答メッセージ３０６の中でデバイス２０６に送信される。一部の態様によれば、この認証チケットは、このチケットが向けられたデバイス（例えば、デバイス２０６）によってだけ、このチケットが解読され得ることを意図して、暗号化されることができる。デバイス２０６は、他のデバイスとの有効にされた通信リンクを確立するのに後に使用するために、この認証チケットを記憶媒体の中に保持することができる。
【００４８】
図４は、開示される態様で利用され得る例示的な認証チケット４００を示す。図示され、説明される認証チケット４００は、この詳細な説明を理解することを容易にするように与えられ、他の認証チケットが利用されることもできることを理解されたい。
【００４９】
認証チケット４００の中に含まれるのが、デバイス識別子４０２、有効期間４０４、ならびにチケット４００データ全体を対象範囲とする、認証サーバの暗号署名４０６である。有効期間４０４は、開始時間（例えば、＜日付／時刻＞より前は無効）および終了時間（例えば、＜日付／時刻＞より後は無効）を含む。有効期間４０４は、認証チケットが、不正を行うデバイスによって不正に獲得された場合、期限切れになると、その認証チケットは、その不正を行うデバイスによってもはや使用可能でないため、或るレベルのセキュリティをもたらすことができる。
【００５０】
オプションの態様によれば、認証チケット４００は、チケット保持者（例えば、デバイス）を認証するのに利用され得る情報を含むことができる。４０８で破線によってオプションとして表される、この情報は、デジタル証明書、公開鍵、デバイス識別子４０２によって示されるデバイスに属する公開鍵のハッシュ、ならびにその他の認証手段の形態であることができる。
【００５１】
さらに、または代替として、認証チケット４００は、デバイス識別子４０２によって識別されるデバイスが、ピアツーピアで、またはグループ様態で、そのスペクトルを使用して消費することを許されるサービスのタイプのオプションの（破線によって表される）リスト（または表現）４１０（例えば、音声呼もしくはビデオ呼、最大速度または最小速度のデータ交換、特殊なブロードキャスト情報の受信など）を含むことができる。一部の態様によれば、許されるサービスに関する情報４１０は、チケット４００を有効にしている他のデバイスによって、それらの他のデバイス（複数可）が、有効にされた通信リンクを使用可能にするかどうか、およびどのように使用可能にするかを判定することができるように、考慮に入れられる。有効な通信リンクが使用可能にされる場合、それらの他のデバイス（複数可）は、許されたサービスのタイプのリストの中で指定されたデータのタイプおよび／またはデータ転送速度だけを伝送するように、そのリンクを構成することができる。
【００５２】
また、認証チケット４００は、他の構成情報または使用可能にする情報４１２を、オプションとして含む（破線によって表されるとおり）こともできる。この他の情報４１２は、認証されたすべてのデバイスに与えられ、物理チャネルまたは媒体アクセス制御チャネルを構成するようにアドホックネットワークにおいて利用されて、認証されたデバイスだけが、これらのチャネルを使用して通信できるようにされる、データを含むことができる。一部の態様によれば、その他の情報４１２は、構成情報および／または割り当てられたパラメータリストを含み、この情報および／または割り当てられたパラメータリストは、認証チケットを有効にしている他のデバイスによって、それらの他のデバイスがどのようにしてリンクを正しく構成すべきかを判定するために利用されることができる。
【００５３】
図５は、本明細書で開示される様々な態様による、スペクトル使用認証および／または

関連する構成パラメータを最初に有効にすることによって、有効にされた通信リンクを確立する２つのデバイスの動作のフローチャート図５００を示す。第１のデバイス（デバイス$_1$）２０６が、そのスペクトルを使用して、他の１つまたは複数のデバイス（デバイス$_N$）２０８と通信することを所望する場合、第１のデバイス２０６は、接続要求メッセージ５０２を送信する。接続要求メッセージ５０２は、第１のデバイス２０６の識別子（例えば、「ＩＤ－Ｄｅｖｉｃｅ－１」）を含む。一部の態様によれば、接続要求メッセージ５０２は、第１のデバイス２０６を識別する（さらにデバイス２０６に属する）認証チケットを含む。

【００５４】

第２のデバイス２０８は、接続要求メッセージ５０２に、第２のデバイス２０６の識別子（例えば、「ＩＤ－Ｄｅｖｉｃｅ－Ｎ」）を含む接続応答メッセージ５０４で応答することができる。一部の態様によれば、接続応答メッセージ５０４は、第２のデバイス２０８が第１のデバイス２０６から受信された認証チケットの内容を検証した後、送信されることができる。接続応答メッセージ５０４は、第２のデバイス２０８を識別する（さらにデバイス２０８に属する）認証チケットを含むことができる。接続応答メッセージ５０４を受信するのと実質的に同時に、第１のデバイス２０６は、第２のデバイス２０８から受信された認証チケットの内容を検証することができる。

【００５５】

接続要求メッセージ５０２と接続応答メッセージ５０４のいずれか、または両方が、そのメッセージを送信するデバイスに関連付けられた公開鍵（複数可）（例えば、「ｐｕｂｌｉｃ－ｋｅｙ－１」、「ｐｕｂｌｉｃ－ｋｅｙ－Ｎ」）を含むことができる。一部の態様によれば、いずれか、または両方のメッセージ５０２、５０４が、完全なデジタル証明書を含む。

【００５６】

破線５０６によって表されるオプションの態様において、他の１つまたは複数のメッセージが交換されることができる。これらの他のメッセージ５０６は、相互アイデンティティ認証を実現する目的で送信されることができる。例えば、第１のデバイス２０６が、第２のデバイス２０８のアイデンティティを認証する（例えば、アイデンティティ「ＩＤ－Ｄｅｖｉｃｅ－Ｎ」を検証する）ことが可能であり、第２のデバイス２０８が、第１のデバイス２０６のアイデンティティを認証する（例えば、アイデンティティ「ＩＤ－Ｄｅｖｉｃｅ－１」を検証する）ことができる。

【００５７】

メッセージ５０２、５０４、およびオプションとして、メッセージ５０６の目的は、相互アイデンティティティ認証を実現することである。相互アイデンティティティ認証は、認証検証プロセスとは異なる。一部の態様によれば、相互アイデンティティティ認証プロセスと認証検証プロセスはともに、実質的に同時に実行されることができる。

【００５８】

様々な態様によれば、アイデンティティティ認証は、デジタル証明書を使用することによって達せられることができる。例えば、２つのデバイス２０６、２０８が、各デバイスが、そのデバイスの証明書およびその他の情報（例えば、乱数またはナンス（nonce））を送信するプロトコルに参加することができる。この交換は、他方のデバイスが、提示された証明書に関連付けられた秘密鍵を実際に所有していることを検証するのを助けることができる。

【００５９】

一部の態様によれば、アイデンティティティ認証により、デバイス２０６とデバイス２０８の間の通信チャネルをセキュリティで保護するのに利用され得る共有秘密鍵が確立されることがもたらされることもできる。

【００６０】

他の態様によれば、アイデンティティティ認証、および通信チャネルセキュリティの確立のために利用されるデジタル証明書は、スペクトル認証チケットと同一であることができる

。この場合、アイデンティティ認証タスクと認証タスクは組み合わされる。

【００６１】

第１のデバイス２０６が第２のデバイス２０８に認証要求メッセージ５０８を送信する認証交換が行われる。認証要求メッセージ５０８は、第１のデバイス２０６の認証チケットを含むことができる。第２のデバイス２０８は、第２のデバイス２０８の認証チケットを含むことが可能な認証応答メッセージ５１０で応答することができる。

【００６２】

認証要求メッセージ５０８を受信するのと実質的に同時に、第２のデバイス２０８は、第１のデバイス２０６の受信された認証チケット（このメッセージの中に含まれる）を検証することができる。同様にして、認証応答メッセージ５１０を受信するのと実質的に同時に、第１のデバイス２０６は、第２のデバイス２０８の認証チケット（このメッセージの中に含まれる）を検証することができる。それぞれの認証チケットの検証は、そのチケットの中の識別子が、前述したとおり、相互アイデンティティ認証中に有効にされた識別子と同一であることを確認することを含む。

【００６３】

一部の態様によれば、認証チケットを検証することだけでは、適切な量のセキュリティを実現するのに十分でない可能性があることに留意されたい。したがって、検証プロセスは、デバイスアイデンティティ認証またはユーザアイデンティティ認証を含むこともできる。この態様によれば、「認証チケット検証」とは、サーバによって生成されたチケット（例えば、認証チケット）の検証、およびそのチケットが、そのチケットの中に含まれる識別子によって識別される、そのチケットを送信するデバイスに属することの検証を指す。さらに、または代替として、認証チケットは、デジタル証明書の形態を有する、またはデバイスデジタル証明書もしくはユーザデジタル証明書も含む。このため、この態様によれば、各デバイスは、そのデバイスが、提示される認証チケットの正当な所有者であることを証明する必要がある。一部の態様によれば、デジタル証明書の所有権は、その証明書の中に存在する公開鍵に関連する秘密鍵を所有していることの検証されたエンティティ証明を示すことによって検証されることができる。

【００６４】

破線５１２によって表されるオプションの態様では、別のセキュリティプロトコルおよび／または構成プロトコルが、セキュリティで保護された鍵導出、および場合により、他の構成の目的で、デバイス２０６とデバイス２０８の間で実施されることができる。

【００６５】

アイデンティティおよび認証チケットの相互検証が完了した後、交換された認証チケットの中に含まれる情報／割り当てられたパラメータを利用してリンクが構成される。有効なリンクの構成の後、５１４で、その有効にされた通信リンクを介してデバイス２０６とデバイス２０８の間でユーザデータが交換されることができる。

【００６６】

図５に関連して図示され、説明されるフローチャート図は、単に例示を目的とすることに留意されたい。例えば、アイデンティティおよび認証チケットの相互検証は、接続メッセージが受信された時点以外の時点で実行されることもできる。さらに、アイデンティティ検証および認証検証などのタスクは、組み合わされることもできる。さらに、認証チケット交換のプロトコル、および関連するセキュリティのプロトコルの一環として、エンティティが、後の時点で交換され、検証されることもできる。さらに、または代替として、第１のデバイス２０６によって送信されるメッセージが組み合わされて（例えば、メッセージ５０２および５０８、メッセージ５０２、５０６、５０８、および５１２）、１つまたはいくつかのメッセージにされることもできる。同様に、第２のデバイス２０８からのメッセージが組み合わされて（例えば、メッセージ５０４および５１０、メッセージ５０４、５０６、５１０、および５１２）、１つまたはいくつかのメッセージにされることもできる。

【００６７】

一部の態様によれば、認証チケットは、第２のデバイス２０８から直接にではなく、他の手段を介して、第１のデバイス２０６によって獲得されることができる。例えば、第２のデバイス２０８が、第２のデバイス２０８の（固有の）識別子を送信することが可能であり、第１のデバイス２０６は、この識別子を利用して、サーバまたはローカルデータベースから獲得されることが可能な、第２のデバイスの認証チケットを取り出し、検証する。

【００６８】

様々な態様によれば、デバイス２０６、２０８はともに、そのスペクトルを使用する共有無線リンク上でユーザデータまたはその他のプロトコルデータが、５１４で流れることを許すのに先立って、他方のデバイスのアイデンティティおよび認証チケットを検証する。また、３つ以上のデバイスによって同様のプロセスが行われることもできる（例えば、ブロードキャスト／マルチキャスト機構を使用してグループ無線通信が使用される場合に）ことをさらに理解されたい。マルチデバイスシナリオにおいて、各デバイスは、他のデータを伝送する無線リンクまたは複数の無線リンクを活性化するのに先立って、通信グループの中のその他のデバイスに与えられた認証チケットを有効にすることに成功しなければならない。

【００６９】

一部のオプションの態様によれば、本明細書で説明されるスペクトル使用認証有効確認と実質的に同時に、他の執行スキームが利用されることもできる。例えば、無線センサポイントが、或る地理的区域にわたって配置されることができる。これらのセンサポイントは、認証のない無線データ交換をリッスンすることができる。別の例では、チケットが明示的に交換されることをシステムが要求する場合に、有効な認証チケットの交換が先行して行われていない通信を、正当なノードが能動的にリッスンし、報告することができる。

【００７０】

別の態様によれば、第１のデバイス２０６は、タイプ「Ａ」だけのスペクトル使用サービス（例えば、音声呼だけ）を認証する認証チケットを（例えば、認証サーバから）獲得する。第１のデバイス２０６と別のデバイス（例えば、第２のデバイス２０８）の間の通信を確立する際、各デバイスは、そのデバイスの認証チケットを他方のデバイスに送信する。第２のデバイス２０８が、タイプ「Ａ」のサービスを受ける権利がある場合、リンクは、タイプ「Ａ」だけのデータを交換するために使用可能にされる。後の時点で、第１のデバイス２０６が、第２のデバイス２０８とタイプ「Ｂ」のデータ（例えば、ビデオ）を交換することを所望する場合、第２のデバイス２０８は、そのようなデータ（例えば、タイプ「Ｂ」）が送信される、さらに／または受信されることを許さないように構成されているため、第２のデバイス２０８は協力しない。

【００７１】

次に図６を参照すると、図示されているのは、１つまたは複数の態様によるチケットベースのスペクトル認証およびアクセス制御のためのシステム６００である。システム６００は、制御されたインフラストラクチャの必要なしに、スペクトルライセンス保持者／所有者が、アドホック様態で、またはピアツーピア様態で（無線周波数）スペクトルを利用して通信するデバイスから収益を引き出すことを可能にするように構成されることができる。システム６００は、ユーザデータ通信または制御データ通信を伝送する有効にされた無線リンクを使用可能にするために、認証チケットの配信を介した、認証されたデバイスによるデータ通信のためのスペクトルの使用、ならびにそれらのデバイス間の、これらの認証チケットの交換および検証を可能にすることができる。システム６００に含まれるのが、１つまたは複数のデバイス６０４と通信状態にあることが可能な無線通信装置６０２、およびノードであることが可能な１つまたは複数の信頼されるパーティ６０６である。

【００７２】

無線通信装置６００は、無線通信装置６０２に関して発行された認証チケットを獲得する認証チケット要求器（ticket requestor）６０８を含む。無線通信装置６０２に関する認証チケットは、信頼されるサードパーティ６０６によって発行される。一部の態様によ

れば、信頼されるパーティ６０６は、認証チケットを発行する認証サーバ（複数可）であることができる。

【００７３】

一部の態様によれば、信頼されるパーティ６０６（または認証サーバ（複数可））との通信は、セルラ無線インターフェース、デジタル加入者線（ＤＳＬ）ケーブルなどの有線インターフェースであることが可能なインターフェースを介して行われる。

【００７４】

やはり、無線通信装置６００に含まれるのが、関連するデバイス６０４（複数可）（例えば、通信が確立されるべきデバイス）から認証チケットを要求する、または受信するように構成された、関連デバイス認証チケット捕捉器（acquirer）６１０である。認証チケットは、無線通信装置６０２に関する認証チケットを発行した信頼されるサードパーティから、または別の信頼されるパーティから、１つまたは複数の関連するデバイス６０４に発行される。関連するデバイス６０４（複数可）の認証チケットは、有効時間（validity time）、またはそのチケットを発行した信頼されるパーティの暗号署名を含むことができる。

【００７５】

一部の態様によれば、無線通信装置６０２の認証チケット、および／または関連するデバイス６０４（複数可）の認証チケット（複数可）は、従来のデジタル証明書（例えば、Ｘ．５０９標準）として実現される。例えば、従来のデジタル証明書は、スペクトル使用に関する認証を示す拡張子を含むことが可能であり、さらに／または有効にされた通信リンクを確立することに関係がある他の情報を伝えることができる。

【００７６】

検証モジュール６１２が、無線通信装置６０２と、１つまたは複数の関連するデバイス６０４との間で有効な通信セッションを確立するように構成される。検証モジュール６１２は、関連するデバイス（複数可）に関する認証チケットを有効にすることができる。一部の態様によれば、有効にされた通信セッションは、無線通信装置６０２の認証チケット、および関連するデバイス６０４（複数可）の認証チケット（複数可）の中に含まれる情報に基づいて、セキュリティで保護されることができる。セキュリティで保護された通信セッションとは、暗号化／解読および完全性保護を有する通信セッションを指す。

【００７７】

一部の態様によれば、無線通信装置６０２に関して発行された認証チケットは、関連するデバイス（複数可）が無線通信装置６０２のアイデンティティを検証し、有効にされた通信セッションを確立するために、関連するデバイス６０４（複数可）に送信される。無線通信装置６０２と１つまたは複数のデバイス６０４の間のデータは、認証チケット交換が行われることに成功し、リンクが有効にされるまで、データを伝送するように使用できない。

【００７８】

一部の態様によれば、無線通信装置６０２、デバイス６０４（複数可）、および／または信頼されるパーティ６０６の間で通信を可能にするセルラインターフェースが、利用されることができる。このセルラインターフェースは、概ね、他のデバイス６０４（複数可）と通信することを目的とすることができるものの、このインターフェースは、アクセスポイント（または基地局）と通信するために利用されることもできる。例えば、セルラインターフェースは、無線通信装置６０２からアクセスポイントに、アクセスポイントから１つまたは複数の信頼されるサードパーティ６０６に無線でデータを伝送することができる。しかし、アクセスポイントの存在または関与は、必須でないことに留意されたい。また、データは、他の１つまたは複数のデバイスを介して中継されることも可能であり、それらのデバイスの１つが、信頼されるサードパーティ６０６が存在するネットワークに最終的に接続される。

【００７９】

一部の態様によれば、無線通信装置６０２と１つまたは複数の信頼されるサードパーテ

ィ６０６の間の通信は、無線インターフェースを介して実行される。この態様によれば、直接の通信ポイントは、別のデバイスまたはアクセスポイントであることが可能であり、そのデバイスまたはアクセスポイントが、信頼されるサードパーティ６０６との通信リンクを有する別のエンティティにデータを中継することができ、あるいは信頼されるサードパーティ６０６に直接に、そのデータを送信することができる。この態様を実施する際、認可されたスペクトルを使用するインターフェースを介する通信は、認証チケットが獲得された後（さらに検証される）まで、使用可能にされてはならないことに留意されたい。１つのアプローチでは、認証プロトコルは、別の利用可能なインターフェースが存在しない状況で、この通信リンクを使用して実行され、したがって、スペクトル使用の認証をブートストラップする手段が提供されなければならない。有効な認証チケットが存在しない場合、このインターフェースを介する通信は、構成により、信頼されるパーティ６０６との認証プロセス（例えば、認証チケットを獲得すること）に直接、関係があるプロトコルおよびデータだけに限られるものと理解される。

【００８０】

別のアプローチにおいて、認証プロトコルは、認証を求める無線通信装置６０２に代行して「ヘルパ（helper）」デバイスまたはアクセスポイントによって実行される。このため、無線通信装置６０２は、このインターフェースだけを使用して、別のアクセスポイントもしくはデバイスを探し出し、無線通信装置６０２に代行して信頼されるパーティ６０６との必要とされる認証／認証プロトコルを実行するよう、そのデバイスに要求する。このプロセスは、無線通信装置６０２とヘルパデバイスの間でデータを中継することを含むことができる。

【００８１】

システム６００は、無線通信装置６０２に動作上、結合されたメモリ６１４を含むことができる。メモリ６１４は、無線通信装置６０２の外部にあることが可能であり、あるいは無線通信装置６０２内に存在することができる。メモリ６１４は、無線通信装置６０２に関連付けられた第１の認証チケットを獲得することと関係する情報を格納することができる。第１の認証チケットは、信頼されるサードパーティによって発行されることができる。また、メモリ６１４は、第２のデバイスから、第２のデバイスに関する第２の認証チケットを受信することと関係する情報を格納することもできる。第２の認証チケットは、信頼されるサードパーティ、または別の信頼されるパーティによって発行されることができる。さらに、メモリ６１４は、第２のデバイス、または複数のデバイスとの有効にされた通信セッションを確立することと関係する命令を保持することもできる。

【００８２】

プロセッサ６１６は、ピアツーピア通信ネットワークまたはアドホック通信ネットワークにおけるスペクトル認証およびアクセス制御と関係する情報の解析を円滑にするように、無線通信装置６０２（および／またはメモリ６１４）に動作上、結合されることができる。プロセッサ６１６は、無線通信装置６０２によって受信される情報を解析すること、および／または生成することに専用のプロセッサ、システム６００の１つまたは複数のコンポーネントを制御するプロセッサ、および／または無線通信装置６０２によって受信される情報を解析し、生成するとともに、システム６００の１つまたは複数のコンポーネントを制御するプロセッサであることができる。

【００８３】

メモリ６１４は、システム６００が、本明細書で説明される無線ネットワークにおいて改良された通信を実現するのに、格納されたプロトコルおよび／またはアルゴリズムを使用することができるように、無線通信装置６０２、デバイス６０４（複数可）、および／または信頼されるパーティ６０６の間のスペクトル認証、アクセス制御に関連するプロトコルを格納することができる。メモリ６１４は、無線通信装置６０２および／または１つまたは複数のデバイス６０４に関連する認証チケットをさらに保持することができる。

【００８４】

メモリ６１４は、信頼されるサードパーティによって発行された第１のデバイスに関す

る第１の認証チケットを獲得すること、第２のデバイスから、その信頼されるサードパーティ、または別の信頼されるパーティによって発行された第２のデバイスに関する第２の認証チケットを受信すること、および第２のデバイスとの有効にされた通信セッションを確立することと関係する命令をさらに保持することができる。プロセッサ６１６は、メモリの中に保持される命令を実行するように構成される。

【００８５】

本明細書で説明されるデータストア（例えば、メモリ）コンポーネントは、揮発性メモリまたは不揮発性メモリであることが可能であり、あるいは揮発性メモリと不揮発性メモリをともに含むこともできることを認識されたい。例として、限定としてではなく、不揮発性メモリには、読み取り専用メモリ（ＲＯＭ）、プログラマブルＲＯＭ（ＰＲＯＭ）、電気的にプログラミング可能なＲＯＭ（ＥＰＲＯＭ）、電気的に消去可能なＲＯＭ（ＥＥＰＲＯＭ）、またはフラッシュメモリが含まれることができる。揮発性メモリには、外部キャッシュメモリの役割をするランダムアクセスメモリ（ＲＡＭ）が含まれることができる。例として、限定としてではなく、ＲＡＭは、シンクロナスＲＡＭ（ＤＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）、シンクロナスＤＲＡＭ（ＳＤＲＡＭ）、ダブルデータレートＳＤＲＡＭ（ＤＤＲ　ＳＤＲＡＭ）、拡張型ＳＤＲＡＭ（ＥＳＤＲＡＭ）、シンクリンクＤＲＡＭ（ＳＬＤＲＡＭ）、およびダイレクトラムバスＲＡＭ（ＤＲＲＡＭ）などの多くの形態で利用できる。開示される態様のメモリ６１４は、以上、およびその他の適切なタイプのメモリを、それらのメモリに限定されることなしに、備えることを意図している。

【００８６】

図７は、スペクトル認証およびアクセス制御のためのシステム７００を示す。システム７００は、図６のシステム６００と同様であり、他のデバイス７０４、ならびに無線通信装置７０６として示される１つまたは複数の信頼されるパーティと通信するデバイス７０２を含む。

【００８７】

信頼されるパーティ７０６は、デバイス７０２などの第１のデバイスから、システムアクセスを求める要求を受信するように構成された受信機７０８を含むことができる。また、受信機７０８は、第１のデバイス７０２から要求を受信するのと実質的に同時に、または異なる時点で、または以上の組み合わせで、その他のデバイス７０４の１つまたは複数から要求を受信することもできる。

【００８８】

その要求に基づいて、オーセンティケータ７１０が、第１のデバイス７０２（またはその要求を送信した別のデバイス）の認証を獲得するように構成されることができる。一部の態様によれば、第１のデバイス認証は、セキュリティで保護された通信リンクを介してネットワークデバイスからなど、外部ソースから、さらに／またはホームサーバから獲得される。例えば、この外部ソースは、第１のデバイス（例えば、デバイスを所有しているユーザ）とビジネス関係を有するサーバであることが可能であり、さらにこのサーバは、加入（例えば、ユーザが加入しているサービス）を検証することができる。

【００８９】

第１のデバイス７０２の認証に部分的に基づいて、アクセスオーソライザ７１２は、第１のデバイス７０２（または別のデバイス７０４）に関して認証され得るシステムアクセスを判定することができる。一部の態様によれば、アクセスオーソライザ７１２は、システムにアクセスすることを認証された複数のデバイスのリストを含む構成パラメータデータベースを調べて、第１のデバイスが権利を有するアクセスを判定することができる。また、構成パラメータデータベースは、各デバイスに関連付けられた１つまたは複数の構成パラメータ（例えば、構成パラメータのセット）を含むこともできる。第１のデバイスがリストの中に含まれる場合、第１のデバイスは、システムにアクセスすることを認証される。しかし、第１のデバイスがリストの中に含まれない場合、第１のデバイスは、システムにアクセスすることを認証されない。構成パラメータデータベースは、データベースに

変更があった際に、さらに／またはその他の基準に基づいてなど、動的に更新されることができる。

【００９０】

一部の態様によれば、オーセンティケータ７１０および／またはアクセスオーソライザ７１２は、第１のデバイス７０２（または別のデバイス７０４）に関連付けられた証明書を点検して、それぞれの判定を行うことができる。証明書は、共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の少なくとも１つ、または以上の組み合わせであることができる。

【００９１】

認証チケットジェネレータ７１４が、アクセスオーソライザ７１２によって特定された、認証されたシステムアクセスに基づいて、第１のデバイス７０２（および／またはその他のデバイス７０４）に関する認証チケットを作成することができる。認証チケット作成の一部は、認証チケットの有効性が依拠する暗号署名の生成を含むことができる。認証チケットは、第１のデバイスのアイデンティティ、認証チケットが有効である有効範囲、暗号署名、および／または他のパラメータを含むことができる。

【００９２】

システム７００は、無線通信装置７０６に動作上、接続された（または装置７０６内に含まれる）メモリ７１６を含むことができる。メモリ７１６は、少なくとも第１のデバイスからシステムアクセスを求める要求を受信すること、少なくとも第１のデバイスの認証を実行すること、第１のデバイスに関して認証され得るシステムアクセスを判定すること、認証されたシステムアクセスに部分的に基づいて、少なくとも第１のデバイスに関する認証チケットを生成することと関係する命令を格納することができる。プロセッサ７１８がメモリ７１６に結合されることが可能であり、メモリ７１６の中に保持される命令を実行するように構成されることができる。

【００９３】

次に図８を参照すると、図示されているのは、チケットベースの構成パラメータの有効確認のためのシステム８００である。システム８００は、認証されたデバイスが、認証チケットの利用を通じて、認可されたスペクトルを介して通信することを可能にするように構成されることができる。別のデバイスと通信することを所望するデバイスは、その別のデバイスによって主張されるリンク構成パラメータが、相互に信頼されるサードパーティによって認証されていることを検証することができる。

【００９４】

システム８００に含まれるのが、例えば、認証サーバなどの、信頼されるサードパーティであることが可能な、無線通信装置８０２である。無線通信装置８０２は、デバイス$_1$８０４からデバイス$_P$８０６というラベルが付けられた１つまたは複数のデバイスと通信するように構成され、ただし、Ｐは整数である。

【００９５】

無線通信装置８０２に含まれるのが、システムアクセスを求める要求に部分的に基づいて、各デバイス８０４、８０６を選択的に認識することができるデバイス識別子８０８である。例えば、各デバイス８０４、８０６は、ハードウェアアドレスなどの固有の識別子によって識別されることができる。さらに、デバイス識別子８０８は、各デバイス８０４、８０６に関連付けられた他の認証情報および／または認証情報を含むことができる。例えば、共有秘密鍵、公開鍵、認証情報、各デバイスが受ける権利があるサービスのリストなどの証明書、関連する料金請求／課金情報などが、デバイス識別子８０８によって保持される（またはアクセスされ得る）ことができる。

【００９６】

一部の態様によれば、デバイス識別子８０８は、そのスペクトルを使用することを認証されたデバイスのデータベースを含むことが可能な構成パラメータデータベースを含む。また、このデータベースは、各デバイスに関する構成情報および／または割り当てられたパラメータを含むこともできる。一部の態様によれば、デバイスから認証を求める要求が

受信された時点で、それらのパラメータのサブセットが生成されることができる。ＩＰアドレスなどの他のパラメータは、利用可能なアドレスのプールから割り当てられ、さらに／または別のサーバから獲得されることができる。一部の態様によれば、構成情報は、サービス契約などによって規定されるとおりに格納されることができる。

【００９７】

デバイス識別子８０８が、１つまたは複数のデバイス８０４、８０６に関する必要なすべての情報を有さない（または得ることができない）場合、その情報は、その必要とされる情報の全体または一部を保持する、またはそのような全体または一部にアクセスを有する別のサーバまたはネットワークデバイスから獲得されることができる。別のサーバまたはネットワークデバイスから情報を得ることは、セキュリティで保護された様態で行われることができる。この状況において、無線通信装置８０２は、通信インターフェースを利用して、すべての、または一部のデバイス８０４、８０６に関する認証／認証情報を保持する別のサーバと通信することができる。一部の態様によれば、一部の、またはすべてのデバイス８０４、８０６に関連する情報は、複数のネットワークノードに存在することができる。

【００９８】

データベースを調べる目的は、認証を求めているデバイスのアイデンティティを確認すること、およびユーザサービス契約などに従ってデバイスが受ける権利があるサービスを特定することである。データベースを調べることは、システムアクセスを求める各デバイス８０４、８０６に関して無線通信装置８０２が行うプロセスの一部である。

【００９９】

認証チケット配信器（authorization ticket distributor）８１０が、デバイス８０４、８０６に認証チケットを選択的に配信する。認証チケットの配信は、デバイスの証明書、ならびにそのデバイスがアクセスし、利用する権利を有するサービスを有効にしたことの結果であることができる。さらに、認証チケットは、デバイス間で交換され、そのスペクトルを使用してユーザデータ通信または制御データ通信を伝送する無線リンクを立ち上げる、または使用可能にする条件として、検証される。そのようにして、認証されたデバイスだけが、本明細書で提示される態様により、データ通信のためにそのスペクトルを使用することを可能にされる。一部の態様によれば、認証チケットは、ＩＰアドレスを含むことが可能な、Ｘ．５０９証明書などの従来のデジタル証明書として実施される。

【０１００】

さらに、メモリ８１２が、無線通信装置８０２に動作上、結合されることができる。メモリ８１２は、無線通信装置８０２の外部にあることが可能であり、あるいは無線通信装置８０２内に存在することができる。メモリ８１２は、デバイスを、１つまたは複数の有効にされた情報エレメントに関連付けること、および信頼されるパーティによって証明された認証チケットを、そのデバイスに送信することと関係する情報を格納することができる。このチケットは、その１つまたは複数の有効にされた情報エレメントのサブセットを含むことができる。

【０１０１】

メモリの中に認証チケットを保持することにより、有効にされた通信セッションが確立されるべき際に認証チケットを獲得する必要性が軽減されることができる。このため、認証チケットの認証サーバおよび／または認証ソースが利用可能でない（例えば、限られた接続）場合、メモリの中に保持される認証チケットが利用されることができる。一部の態様によれば、接続が復元されると、更新された認証チケットが獲得される。

【０１０２】

情報エレメントは、ユーザに提示されるべき表現、アドレス、電話番号、および／またはその他の情報（例えば、視覚情報、可聴情報など）であることができる。一部の態様によれば、情報エレメントは、構成パラメータおよび／またはＩＰアドレスであることができる。さらに、または代替として、情報エレメントは、ブロードキャストされている、さらに／または公示されている識別子であることができる。さらに、情報エレメントは、名

前、アイデンティティ、位置、ユーザ情報（例えば、ユーザが表現したい感情）、商標、および他の任意のデータであることができる。

【０１０３】

一部の態様によれば、利用可能な情報エレメントのサブセットだけが、認証チケットの中に含められる。例えば、認証チケットの中に含められることが可能な数百または数千の情報エレメントが存在する場合、それらの情報エレメントのサブセットだけが、認証チケットの中に含められることができる。いずれの情報エレメントを含めるべきかの決定は、それらの情報エレメント（および認証チケット）のソース、および／またはそれらの情報エレメント（および認証チケット）の宛先に応じることができる。

【０１０４】

それらの情報エレメントは、それらの情報エレメントにいくらかの信頼性を与えるために有効にされることができる。有効にされた情報エレメントは、それらの情報エレメントがサーバによって事前に有効にされるので、それらの情報エレメントを独立に有効にする必要性を軽減する（例えば、別のデバイス、別のデータベース、または他の任意のソースにアクセスする必要性がない）。

【０１０５】

プロセッサ８１４が、アドホック通信ネットワークにおけるスペクトル認証およびアクセス制御と関係する情報の解析を円滑にするように、無線通信装置８０２（および／またはメモリ８１２）に動作上、接続されることができる。プロセッサ８１４は、無線通信装置８０２によって受信される情報を解析すること、および／または生成することに専用のプロセッサ、システム８００の１つまたは複数のコンポーネントを制御するプロセッサ、および／または無線通信装置８０２によって受信される情報を解析し、生成するとともに、システム８００の１つまたは複数のコンポーネントを制御するプロセッサであることができる。

【０１０６】

メモリ８１２は、システム８００が、本明細書で説明される無線ネットワークにおいて改良された通信を実現するのに、格納されたプロトコルおよび／またはアルゴリズムを使用することができるように、無線通信装置８０２、デバイス８０４、８０６（複数可）、および／または信頼されるパーティの間のスペクトル認証、アクセス制御に関連するプロトコルを格納することができる。一部の態様によれば、メモリは、デバイスを、１つまたは複数の有効にされた情報エレメントに関連付けること、および無線通信装置によって証明された認証チケットを、そのデバイスに送信することと関係する命令を保持する。

【０１０７】

図９は、チケットベースの構成パラメータの有効確認のための別のシステム９００を示す。システム９００は、前出の図のシステムと同様であり、認証サーバ９０２、第１のデバイス９０４、および他の１つまたは複数のデバイス９０６を含む。

【０１０８】

デバイス９０４は、認証チケットを獲得するチケット捕捉器９０８を含むことができる。認証チケットは、別のデバイス（例えば、有効にされた通信セッションが確立されるべき相手のデバイス）に関連付けられた１つまたは複数の有効にされた情報エレメントを含むことが可能であり、このデバイスは、本明細書で第２のデバイス９０４と呼ばれる。有効にされた情報エレメントの少なくとも１つは、インターネットプロトコルアドレスである。一部の態様によれば、認証チケットは、第２のデバイス９０４の識別子、有効範囲、ならびに第２のデバイス９０４に認証チケットを発行した信頼されるパーティの署名を含む。やはり、デバイス９０４に含まれるのが、認証チケットを有効にする有効確認モジュール９１０である。

【０１０９】

通信確立器（communication establisher）９１２が、認証チケットを利用して、第２のデバイス９０４との有効にされた通信を確立する。この有効にされた通信は、ブロードキャストされる、またはマルチキャストされることができる。一部の態様によれば、有効

にされた通信は、ピアツーピア構成またはアドホック構成で第２のデバイス９０４とのものである。さらに、第２のデバイス９０４との通信は、セキュリティで保護された通信リンクを介することもできる。

【０１１０】

また、デバイス９０４は、１つまたは複数の有効にされた情報エレメントのサブセットを使用して、構成動作を実行する動作実行モジュール９１４も含む。この構成動作は、インターフェースを構成すること、および／またはルートを追加することを含むことができる。

【０１１１】

メモリ９１６が、デバイス９０４に動作上、接続され、第２のデバイスに関連付けられた１つまたは複数の有効にされた情報エレメントを含む認証チケットを獲得することと関係する命令を保持するように構成される。また、このメモリは、認証チケットを有効にすること、認証チケットを利用して、第２のデバイスとの有効にされた（さらに、場合により、セキュリティで保護された）通信を確立すること、および１つまたは複数の有効にされた情報エレメントのサブセットを使用して、構成動作を実行することと関係する命令も保持する。プロセッサ９１８がメモリ９１６に結合され、メモリ９１６の中に保持される命令を実行するように構成される。

【０１１２】

図示され、説明される例示的なシステムに鑑みて、開示される主題に従って実施されることが可能な方法は、本明細書で与えられるフローチャート図を参照して、よりよく理解されよう。説明を簡単にするため、これらの方法は、一連のブロックとして図示され、説明されることができるが、一部のブロックは、本明細書で図示され、説明される順序とは異なる順序で、さらに／または他のブロックと実質的に同時に行われることができるので、主張される主題は、ブロックの数または順序によって限定されないことを理解し、認識されたい。さらに、図示されるブロックのすべてが、本明細書で説明される方法を実施するのに要求されるわけではない可能性がある。ブロックに関連する機能は、ソフトウェア、ハードウェア、ソフトウェアとハードウェアの組み合わせ、または他の任意の適切な手段（例えば、デバイス、システム、プロセス、コンポーネント）によって実施されることができることを認識されたい。さらに、本明細書全体で開示される方法は、そのような方法を様々なデバイスにトランスポートし、移すことを円滑にするように製造品上に格納されることができることをさらに認識されたい。方法は、代替として、状態図における場合のように、一連の相互に関連する状態またはイベントとして表されることもできることが当業者には理解され、認識されよう。

【０１１３】

図１０は、スペクトル認証およびアクセス制御のための方法１０００を示す。方法１０００は、制御されたインフラストラクチャの必要なしに、アドホック様態またはピアツーピア様態で動作している認証されたデバイスによるスペクトルの利用を可能にすることができる。

【０１１４】

方法１０００は、１００２で、第１の認証チケットが信頼されるサードパーティから獲得されると、開始する。この信頼されるサードパーティは、例えば、認証サーバであることができる。認証チケットは、デバイスの識別子、および信頼されるサードパーティの署名を含むことができる。一部の態様によれば、第１の認証チケットは、第２のデバイスに送信される。

【０１１５】

１００４で、第２の認証チケットが、関連するデバイスから受信される。第２の認証チケットは、第１の認証チケットを発行した信頼されるサードパーティによって発行されることが可能であり、あるいは第２の認証チケットは、別の信頼されるパーティによって発行されることができる。第２の認証チケットは、有効時間、または第２の認証チケットを発行した信頼されるパーティ（例えば、その信頼されるサードパーティ、またはその別の

信頼されるパーティ）の暗号署名を含むことができる。一部の態様によれば、第１の認証チケットは、第１のデバイスによってアクセスされることが許されたサービスを備え、第２の認証チケットは、第２のデバイスによってアクセスされることが許されたサービスを備える。

【０１１６】

１００６で、関連するデバイスとの有効な通信セッションが確立される。この有効にされた通信セッションは、第１の認証チケットおよび第２の認証チケットの中に含まれる認証されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成されることができる。

【０１１７】

一部の態様によれば、有効な通信セッションを確立することは、第２の認証チケットを有効にすることを含むことができる。第２のデバイスに関する第２の認証チケットを有効にすることに失敗することにより、第１のデバイスと第２のデバイスの間の通信リンクが解体（tearing down）されることがもたらされることができる。第２の認証チケットを有効にすることは、有効時間および暗号署名を検証することを含むことができる。一部の態様によれば、第２の認証チケットを有効にすることは、第２の認証チケットの中で識別された第２のデバイスのアイデンティティを有効にすることを含む。さらに、または代替として、第２の認証チケットを有効確認することは、デジタル証明書の中に含まれるアイデンティティおよび公開鍵に関連する秘密鍵の所有を検証すること、および／またはそれらのデバイス間で過去の何らかの時点で行われた相互認証プロセスを介して導き出された共有鍵を検証することを含む。

【０１１８】

また、方法１０００は、第１の認証チケットおよび第２の認証チケットの中に含まれる情報に基づいて、有効にされた通信セッションをセキュリティで保護することを含むこともできる。有効にされた通信セッションをセキュリティで保護することは、暗号化／解読および完全性保護を含む。

【０１１９】

一部の態様によれば、第１の認証チケットおよび／または第２の認証チケットは、従来のデジタル証明書として実施される。例えば、従来のデジタル証明書は、スペクトル使用に関する認証を示す新たな拡張子を有するＸ．５０９標準であることが可能であり、さらに有効にされた通信リンクをセットアップすることに関係がある他の情報を伝えることができる。別の例において、従来のデジタル証明書は、ＩＰアドレスを含む新たな拡張子を含むＸ．５０９証明書であることができる。

【０１２０】

次に、図１１を参照すると、図示されているのは、スペクトル認証およびアクセス制御のための方法１１００である。１１０２で、少なくとも第１のデバイスからシステムアクセス（例えば、認可されたスペクトルへのアクセス）を求める要求が受信される。一部の態様によれば、いくつかのデバイスからの複数の要求が、実質的に同時に、異なる時点で、または以上の組み合わせで受信される。

【０１２１】

１１０４で、第１のデバイスの認証が、内部ソースから、外部ソースから、または内部ソースと外部ソースの組み合わせから獲得される。外部から獲得される場合、認証は、セキュリティで保護された通信リンクを介してネットワークノードから獲得されることができる。一部の態様によれば、この認証は、外部の別のサーバから獲得される。

【０１２２】

１１０６で、第１のデバイスに関して認証され得るシステムアクセスが特定される。一部の態様によれば、システムアクセスを判定することは、システムにアクセスすることを認証された複数のデバイスのリストを含む構成パラメータデータベースを調べることを含む。

【０１２３】

１１０４における第１のデバイスの認証、および／または１１０６における認証されたシステムアクセスは、第１のデバイスに関連付けられた証明書によって特定されることができる。これらの証明書は、共有秘密鍵、公開鍵、認証情報、およびサービスのリスト、または料金請求情報の１つまたは複数、あるいは以上の組み合わせであることができる。

【０１２４】

１１０８で、少なくとも第１のデバイスに関する認証チケットが、第１のデバイスが権利を有する認証されたシステムアクセスに基づいて、作成される。この認証チケットは、第１のデバイスのアイデンティティ、この認証チケットが有効である有効範囲、および／またはこの認証チケットを発行したパーティの暗号署名を含むことができる。

【０１２５】

図１２は、チケットベースの構成パラメータを有効にするための方法１２００を示す。方法１２００は、１２０２で、デバイスが１つまたは複数の有効にされた情報エレメントに関連付けられると、開始する。これらの情報エレメントには、そのデバイスに割り当てられたインターネットプロトコルアドレス、そのデバイスに割り当てられた電話番号、および／またはその他の情報が含まれることができる。

【０１２６】

一部の態様によれば、デバイスを１つまたは複数の情報エレメントに関連付けることに先立って、認証プロトコルを使用して、デバイスと通信が行われる。デバイスとの通信に部分的に基づいて、そのデバイスに関する認証チケットを構築すべきかどうか、その認証チケットの中に含められるべき情報エレメントの決定が行われる。

【０１２７】

一部の態様によれば、固有のデバイス識別子によって識別された認証されたデバイス、および関連するパラメータのデータベースが調べられて、そのデバイスをその情報エレメント（複数可）に関連付けるかどうかが判定される。このデータベースは、各デバイスが、認可されたスペクトルを使用して通信する際に利用することができる構成と関係する情報を含むことができる。

【０１２８】

１２０４で、認証チケットがデバイスに送信される。この認証チケットは、信頼されるパーティによって証明され、１つまたは複数の有効にされた情報エレメントのサブセットを含む。デバイスは、この認証チケットを使用して、別のデバイスとの通信リンクを確立する。一部の態様によれば、この認証チケットは、デバイスの識別子、有効範囲、および信頼されるパーティの署名を含む。

【０１２９】

一部の態様によれば、この認証チケットは、従来のデジタル証明書として実施される。例えば、従来のデジタル証明書は、スペクトル使用に関する認証を示す新たな拡張子を有するＸ．５０９標準であることが可能であり、さらに有効にされた通信リンクをセットアップすることに関係がある情報を伝えることができる。別の例において、従来のデジタル証明書は、ＩＰアドレスを含む新たな拡張子を含むＸ．５０９証明書であることができる。

【０１３０】

図１３は、チケットベースの構成パラメータの有効確認のための方法１３００を示す。１３０２で、或るデバイス（有効確認通信セッションが確立されるべき相手である）に関する認証チケットが獲得される。認証チケットは、そのデバイスに関連付けられた１つまたは複数の有効にされた情報エレメントを含むことができる。一部の態様によれば、この認証チケットは、そのデバイスの識別子、有効範囲、ならびにこの認証チケットを発行した信頼されるパーティの署名を含む。有効にされた情報エレメントの少なくとも１つは、インターネットプロトコルアドレスである。この認証チケットは、１３０４で有効にされる。

【０１３１】

１３０６で、この認証チケットを利用して、そのデバイスとの有効にされた（場合によ

り、セキュリティで保護された）通信が確立される。この通信は、ブロードキャストされる、またはマルチキャストされることができる。一部の態様によれば、そのデバイスとの有効にされた通信は、ピアツーピア構成である。

【０１３２】

１３０８で、その１つまたは複数の有効にされた情報エレメントのサブセットを使用して、構成動作が実行される。一部の態様によれば、この構成動作は、インターフェースを構成することを備える。一部の態様によれば、この構成動作は、ルートを追加することを備える。

【０１３３】

次に、図１４を参照すると、図示されているのは、開示される態様によるチケットベースの認証および有効確認を円滑にするシステム１４００である。システム１４００は、ユーザデバイス内に存在することができる。システム１４００は、例えば、受信機アンテナから信号を受信することができる受信機１４０２を備える。受信機１４０２は、受信された信号をフィルタリングする、増幅する、ダウンコンバートするなどの通常のアクションを信号に対して実行することができる。また、受信機１４０２は、調整された信号をデジタル化して、サンプルを得ることもできる。復調器１４０４が、各シンボル周期に関して受信されたシンボルを獲得すること、ならびに受信されたシンボルをプロセッサ１４０６に供給することができる。

【０１３４】

プロセッサ１４０６は、受信機コンポーネント１４０２によって受信された情報を解析すること、および／または送信機１４０８によって送信されるように情報を生成することに専用のプロセッサであることができる。さらに、または代替として、プロセッサ１４０６は、ユーザデバイス１４００の１つまたは複数のコンポーネントを制御し、受信機１４０２によって受信された情報を解析し、送信機１４０８によって送信されるように情報を生成し、さらに／またはユーザデバイス１４００の１つまたは複数のコンポーネントを制御することができる。プロセッサ１４０６は、さらなるユーザデバイスとの通信を調整することができるコントローラコンポーネントを含むことができる。ユーザデバイス１４００は、プロセッサ１４０６に動作上、結合され、通信を調整することと関係する情報、および他の任意の適切な情報を格納することができるメモリ１４０８をさらに備えることができる。

【０１３５】

図１５は、アドホック（ピアツーピア）環境におけるスペクトル認証およびアクセス制御を円滑にする例示的なシステム１５００を示す。システム１５００は、別々に、または連携して動作することができる電気コンポーネントの論理グループ化１５０２を含む。論理グループ化１５０２は、第１のデバイスに関する第１の認証チケットを獲得するための電気コンポーネント１５０４を含む。第１の認証チケットは、信頼されるサードパーティによって発行されることができる。一部の態様によれば、信頼されるサードパーティは、認証サーバである。

【０１３６】

やはり、論理グループ化１５０２に含まれるのが、第１の認証チケットを第２のデバイスに伝送するための電気コンポーネント１５０６である。第１の認証チケットは、第１のデバイスの識別子、および信頼されるサードパーティの署名を含む。第２のデバイスから、第２のデバイスに関する第２の認証チケットを受信するための電気コンポーネント１５０８も含まれる。

【０１３７】

また、論理グループ化１５０２は、第２のデバイスに関する第２の認証チケットを有効にするための電気コンポーネント１５１０も含む。第２の認証チケットは、有効時間、または第２の認証チケットの発行者（例えば、信頼されるサードパーティまたは別の信頼されるパーティ）の暗号署名を含むことができる。第２の認証チケットを有効にすることは、有効時間と暗号署名の両方を検証することを含む。一態様によれば、第２の認証チケッ

トを有効にすることは、第２の認証チケットの中で識別された第２のデバイスのアイデンティティを有効にすること、デジタル証明書の中に含まれるアイデンティティおよび公開鍵に関連する秘密鍵の所有を検証すること、または相互認証プロセスを介して導き出された共有鍵を検証すること、あるいは以上の組み合わせを含む。

【０１３８】

一部の態様によれば、第２のデバイスに関する第２の認証チケットを有効にしている間に失敗があった場合、第１のデバイスと第２のデバイスの間で確立されていた通信リンクは、解体される。解体される通信リンクは、それらのデバイスが、有効にされた通信が確立されるように認証チケットおよび／または他の情報を交換するのに利用した、有効にされていないリンクである。

【０１３９】

また、第２のデバイスとの有効にされた通信セッションを確立するための電気コンポーネント１５１２も論理グループ化１５０２の中に含まれる。有効にされた通信セッションは、第１の認証チケット、第２の認証チケット、または両方のチケットの中に含まれる、許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成されることができる。一部の態様によれば、第１の認証チケットは、第１のデバイスによってアクセスされることが許されたサービスを含み、第２の認証チケットは、第２のデバイスによってアクセスされることが許されたサービスを備える。

【０１４０】

さらに、システム１５００は、電気コンポーネント１５０４、１５０６、１５０８、１５１０、および１５１２、または他のコンポーネントに関連する機能を実行するための命令を保持するメモリ１５１４を含むことができる。メモリ１５１４の外部にあるものとして図示されるが、電気コンポーネント１５０４、１５０６、１５０８、１５１０、および１５１２の１つまたは複数は、メモリ１５１４内に存在してもよいことを理解されたい。

【０１４１】

図１６は、スペクトル認証を与える例示的なシステム１６００を示す。システムに含まれるのが、別々に、または連携して動作することができる電気コンポーネントの論理グループ化１６０２である。論理グループ化１６０２は、少なくとも第１のデバイスから或るスペクトルへのアクセスを求める要求を受信するための電気コンポーネント１６０４を含む。

【０１４２】

やはり、論理グループ化１６０２に含まれるのが、少なくとも第１のデバイスの認証を実行するための電気コンポーネント１６０６である。この認証は、内部ソースまたは外部ソースを使用して実行されることができる。一部の態様によれば、第１のデバイス認証は、セキュリティで保護された通信リンクを介して外部ネットワークデバイスの助けを借りて実行される。

【０１４３】

また、少なくとも第１のデバイスに提供されることが可能なシステムアクセスを判定するための電気コンポーネント１６０８も含まれる。一部の態様によれば、電気コンポーネント１６０８は、システムにアクセスすることを認証された複数のデバイスのリストを含む構成パラメータデータベースを調べることによって、システムアクセスを判定する。

【０１４４】

様々な態様によれば、電気コンポーネント１６０６は、認証を実行することができ、さらに／または電気コンポーネント１６０８は、第１のデバイスに関連付けられた証明書を点検することによって、スペクトルアクセスを判定することができる。これらの証明書は、１つまたは複数の共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報、または以上の組み合わせを含むことができる。

【０１４５】

論理グループ化１６０２は、少なくとも第１のデバイスに与えられることが可能なスペクトルアクセスに部分的に基づいて、少なくとも第１のデバイスに関する認証チケットを

生成するための電気コンポーネント１６１０をさらに含む。この認証チケットは、第１のデバイスのアイデンティティ、この認証チケットが有効である有効範囲、および／または暗号署名を含むことができる。

【０１４６】

一部の態様によれば、論理グループ化１６０２は、認証チケットを第１のデバイスに送信するための電気コンポーネント（図示せず）を含む。一部の態様によれば、複数の認証チケットは、複数の要求の受信に基づいて生成されることができる。各認証チケットは、各デバイスに対して固有であることができることが可能であり、各デバイスに個々に送信されることができる。

【０１４７】

また、システム１６００は、電気コンポーネント１６０４、１６０６、１６０８、および１６１０、または他のコンポーネントに関する機能を実行するための命令を保持するメモリ１６１２を含むこともできる。メモリ１６１２の外部にあるものとして示されるが、電気コンポーネント１６０４、１６０６、１６０８、および１６１０の１つまたは複数は、メモリ１６１２内に存在することもできる。

【０１４８】

図１７は、通信環境においてチケットベースの構成パラメータを有効にする例示的なシステム１７００を示す。この通信環境は、ピアツーピア構成またはアドホック構成になっていることができる。システム１７００に含まれるのが、別々に、または連携して動作することができる電気コンポーネントの論理グループ化１７０２である。論理グループ化１７０２に含まれるのが、デバイスを１つまたは複数の有効にされた情報エレメントに関連付けるための電気コンポーネント１７０４である。一部の態様によれば、これらの情報エレメントは、そのデバイスに割り当てられたインターネットプロトコルアドレス、および／またはそのデバイスに割り当てられた電話番号であることができる。

【０１４９】

また、論理グループ化１７０２は、信頼されるパーティによって保証された認証チケットをデバイスに送信するための電気コンポーネント１７０６も含む。この認証チケットは、信頼されるパーティの暗号署名、ならびに他の情報（例えば、デバイス識別子、デバイスがアクセスを得ることが可能なサービス、など）を含むことができる。

【０１５０】

情報エレメントを有効にするプロセスは、認証チケットの有効確認とは別個であり、異なることに留意されたい。信頼されるサードパーティは、事前に有効にされた情報エレメントを別のパーティから獲得することができ、あるいは他の何らかの別個のプロセスを介して自ら情報エレメントを有効にすることができる。

【０１５１】

一部の態様によれば、論理グループ化１７０２は、認証プロトコル（authentication protocol or authorization protocol）を使用して、デバイスと通信するための電気コンポーネント（図示せず）を含む。やはり含まれるのが、認証チケットを構築するかどうか、およびいずれの情報エレメントをその認証チケットの中に含めるべきかを決定するための電気コンポーネント（図示せず）であることができる。この決定は、デバイスとの通信に部分的に基づいて、行われることができる。

【０１５２】

一部の態様によれば、論理グループ化１７０２は、固有のデバイス識別子によって識別された認証されたデバイス、および関連するパラメータのデータベースを調べるための電気コンポーネント（図示せず）を含む。このデータベースは、各デバイスが、認可されたスペクトルを使用して通信する際に利用することができる構成と関係する情報を含むことができる。

【０１５３】

また、電気コンポーネント１７０４および１７０６、または他のコンポーネントに関連する機能を実行するための命令を保持するメモリ１７０８も、システムに含まれる。外部

メモリ１７０８が例示されるものの、一部の態様によれば、電気コンポーネント１７０４および１７０６の１つまたは複数は、メモリ１７０８内に存在してもよい。

【０１５４】

図１８を参照すると、図示されるのは、チケットベースの構成パラメータを有効にする例示的なシステム１８００である。システム１８００は、別のデバイスに関連付けられた１つまたは複数の有効にされた情報エレメントを含む認証チケットを獲得するための電気コンポーネント１８０４を含む論理グループ化１８０２を含む。一部の態様によれば、有効にされた情報エレメントの少なくとも１つは、インターネットプロトコルアドレスである。

【０１５５】

やはり論理グループ化１８０２に含まれるのが、認証チケットを有効にするための電気コンポーネント１８０６である。この認証チケットは、別のデバイスの識別子、有効範囲、ならびに認証チケットを発行した信頼されるパーティの署名を含むことができる。

【０１５６】

また、論理グループ化１８０２は、認証チケットに部分的に基づいて、別のデバイスとの有効にされた通信を確立するための電気コンポーネント１８０８も含む。有効にされた通信は、ブロードキャストされる、またはマルチキャストされることができる。別のデバイスとのした有効にされた通信は、ピアツーピア構成および／またはアドホック構成である。

【０１５７】

また、１つまたは複数の有効にされた情報エレメントのサブセットに対して構成動作を実行するための電気コンポーネント１８１０も含まれる。構成動作は、インターフェースを構成すること、および／またはルートを追加することを含むことができる。

【０１５８】

さらに、システム１８００は、電気コンポーネント１８０４、１８０６、１８０８、および１８１０、または他のコンポーネントに関連付けられた機能を実行するための命令を保持するメモリ１８１２を含むことができる。メモリ１８１２の外部に存在するものとして図示されるが、電気コンポーネント１８０４、１８０６、１８０８、および１８１０の１つまたは複数は、メモリ１８１２内に存在することもできることを理解されたい。

【０１５９】

前述した図１５、図１６、図１７、および図１８のシステム１５００、１６００、１７００、および１８００は、プロセッサ、ソフトウェア、またはプロトコルとソフトウェアの組み合わせ（例えば、ファームウェア）によって実施される機能を表す機能ブロックであることが可能な、機能ブロックを含むものとして表されることを認識されたい。

【０１６０】

本明細書で説明される態様は、ハードウェア、ソフトウェア、ファームウェア、またはハードウェアとソフトウェアとファームウェアの任意の組み合わせによって実施されることができることを理解されたい。ソフトウェアで実施される場合、これらの機能は、コンピュータ可読媒体上に格納される、またはコンピュータ可読媒体上の１つまたは複数の命令もしくはコードとして伝送されることができる。コンピュータ可読媒体には、１つの場所から別の場所にコンピュータプログラムを移すことを円滑にする任意の媒体を含むコンピュータ記憶媒体と通信媒体がともに含まれる。記憶媒体は、汎用コンピュータまたは専用コンピュータによってアクセスされることが可能な任意の利用可能な媒体であることができる。例として、限定としてではなく、そのようなコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭまたは他の光ディスクストレージ、磁気ディスクストレージまたは他の磁気ストレージデバイス、あるいは命令またはデータ構造の形態で所望されるプログラムコード手段を伝送する、または格納するのに使用されることが可能であり、さらに汎用コンピュータもしくは専用コンピュータ、または汎用プロセッサもしくは専用プロセッサによってアクセスされることが可能な他の任意の媒体を備えることができる。また、任意の接続もコンピュータ可読媒体と適切に呼ばれる。例えば、ソフトウェ

アが、同軸ケーブル、光ファイバケーブル、より対線、デジタル加入者線（ＤＳＬ）、あるいは赤外線、無線、およびマイクロ波などの無線技術を使用してウェブサイト、サーバ、または他の遠隔ソースから伝送される場合、その同軸ケーブル、光ファイバケーブル、より対線、ＤＳＬ、あるいは赤外線、無線、およびマイクロ波などの無線技術が、媒体の定義に含められる。本明細書で使用されるディスク（disk）およびディスク（disc）には、コンパクトディスク（ＣＤ）、レーザーディスク（登録商標）、光ディスク、デジタルバーサタイルディスク（ＤＶＤ）、フロッピー（登録商標）ディスク、およびブルーレイディスクが含まれ、ただし、ディスク（disk）は、通常、データを磁気的に再現するのに対して、ディスク（disc）は、レーザーを使用してデータを光学的に再現する。また、以上の媒体の組み合わせも、コンピュータ可読媒体の範囲内に含められるべきである。

【０１６１】

本明細書で開示される態様に関連して説明される様々な例示的なロジック、論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ（ＤＳＰ）、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ー（ＦＰＧＡ）もしくは他のプログラミング可能なロジックデバイス、ディスクリートのゲートもしくはトランジスタロジック、ディスクリートのハードウェアコンポーネント、あるいは本明細書で説明される機能を実行するように設計された以上の任意の組み合わせを使用して、実施される、または実行されることができる。汎用プロセッサは、マイクロプロセッサであることができるが、代替として、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態マシンであってもよい。また、プロセッサは、コンピューティングデバイスの組み合わせとして、例えば、ＤＳＰとマイクロプロセッサの組み合わせ、複数のマイクロプロセッサ、ＤＳＰコアと連携する１つまたは複数のマイクロプロセッサ、または他の任意のそのような構成として実施されることもできる。さらに、少なくとも１つのプロセッサは、前述したステップおよび／またはアクションの１つまたは複数を実行するように動作可能な１つまたは複数のモジュールを備えることができる。

【０１６２】

ソフトウェア実施形態の場合、本明細書で説明される技術は、本明細書で説明される機能を実行するモジュール（例えば、手順、関数など）で実施されることができる。ソフトウェアコードは、メモリユニットの中に格納されて、プロセッサによって実行されることができる。メモリユニットは、プロセッサ内に実装されても、プロセッサの外部に実装されてもよく、外部に実装される場合、メモリユニットは、当技術分野で知られている様々な手段を介してプロセッサに通信するように結合されることができる。さらに、少なくとも１つのプロセッサは、本明細書で説明される機能を実行するように動作可能な１つまたは複数のモジュールを含むことができる。

【０１６３】

本明細書で説明される技術は、ＣＤＭＡ、ＴＤＭＡ、ＦＤＭＡ、ＯＦＤＭＡ、ＳＣ－ＦＤＭＡ、およびその他のシステムなどの様々な無線通信システムに関して使用されることができる。「システム」という用語と「ネットワーク」という用語は、しばしば、互換的に使用される。ＣＤＭＡシステムは、ユニバーサル地上無線アクセス（ＵＴＲＡ）、ＣＤＭＡ２０００などの無線技術を実施することができる。ＵＴＲＡは、Ｗ－ＣＤＭＡ（広帯域ＣＤＭＡ）、ならびにＣＤＭＡの他の変種を含む。さらに、ＣＤＭＡ２０００は、ＩＳ－２０００標準、ＩＳ－９５標準、およびＩＳ－８５６標準を範囲に含む。ＴＤＭＡシステムは、グローバルシステムフォーモバイルコミュニケーションズ（ＧＳＭ（登録商標））などの無線技術を実施することができる。ＯＦＤＭＡシステムは、発展型ＵＴＲＡ（Ｅ－ＵＴＲＡ）、ウルトラモバイルブロードバンド（ＵＭＢ）、ＩＥＥＥ８０２．１１（Ｗｉ－Ｆｉ）、ＩＥＥＥ８０２．１６（ＷｉＭＡＸ）、ＩＥＥＥ８０２．２０、Ｆｌａｓｈ－ＯＦＤＭ（登録商標）などの無線技術を実施することができる。ＵＴＲＡおよびＥ－ＵＴＲＡは、ユニバーサル移動体通信システム（ＵＭＴＳ）の一部である。３ＧＰＰロングタームエボリューション（ＬＴＥ）は、ダウンリンクでＯＦＤＭＡを用い、アップリンク

でＳＣ－ＦＤＭＡを用いる、Ｅ－ＵＴＲＡを使用するＵＭＴＳのリリースである。ＵＴＲＡ、Ｅ－ＵＴＲＡ、ＵＭＴＳ、ＬＴＥ、およびＧＳＭは、「第３世代パートナーシッププロジェクト」（３ＧＰＰ）という名称の団体からの文書において説明される。さらに、ＣＤＭＡ２０００およびＵＭＢは、「第３世代パートナーシッププロジェクト２」（３ＧＰＰ２）という名称の団体からの文書において説明される。さらに、そのような無線通信システムは、しばしば、ペアになっていない無認可のスペクトル、８０２．ｘｘ無線ＬＡＮ、ＢＬＵＥＴＯＯＴＨ（登録商標）、および他の任意の短距離または長距離の無線通信技術を使用する、ピアツーピア（例えば、移動体－移動体）のアドホックネットワークシステムをさらに含むことができる。

【０１６４】

さらに、本明細書で説明される様々な態様または特徴は、標準のプログラミング技術および／またはエンジニアリング技術を使用して、方法、装置、または製品として実施されることができる。本明細書で使用される「製品」という用語は、任意のコンピュータ可読のデバイス、搬送波、または媒体からアクセス可能なコンピュータプログラムを包含することを意図している。例えば、コンピュータ可読媒体には、磁気ストレージデバイス（例えば、ハードディスク、フロッピーディスク、磁気帯など）、光ディスク（例えば、コンパクトディスク（ＣＤ）、デジタルバーサタイルディスク（ＤＶＤ）など）、スマートカード、およびフラッシュメモリデバイス（例えば、ＥＰＲＯＭ、カード、スティック、キードライブなど）が含まれるが、以上には限定されない。さらに、本明細書で説明される様々な記憶媒体は、情報を格納するための１つまたは複数のデバイスおよび／または他のマシン可読媒体を表すことができる。「マシン可読媒体」という用語には、命令（複数可）および／またはデータを格納する、包含する、さらに／または伝送することができる無線チャネル、および他の様々な媒体が含まれることができるが、以上には限定されない。さらに、コンピュータプログラム製品には、本明細書で説明される機能をコンピュータに実行させるように作用可能な１つまたは複数の命令またはコードを有するコンピュータ可読媒体が含まれることができる。

【０１６５】

さらに、本明細書で開示される態様に関連して説明される方法またはアルゴリズムのステップおよび／またはアクションは、ハードウェアにおいて直接に、プロセッサによって実行されるソフトウェアモジュールにおいて、またはハードウェアとそのようなソフトウェアモジュールの組み合わせにおいて実施されることができる。ソフトウェアモジュールは、ＲＡＭメモリ、フラッシュメモリ、ＲＯＭメモリ、ＥＰＲＯＭメモリ、ＥＥＰＲＯＭメモリ、レジスタ、ハードディスク、リムーバブルディスク、ＣＤ－ＲＯＭ、または当技術分野で知られている他の任意の形態の記憶媒体の中に存在することができる。例示的な記憶媒体は、プロセッサが、その記憶媒体から情報を読み取ること、およびその記憶媒体に情報を書き込むことができるように、プロセッサに結合されることができる。代替として、記憶媒体は、プロセッサと一体化していてもよい。さらに、一部の態様では、プロセッサおよび記憶媒体は、ＡＳＩＣの中に存在することができる。さらに、ＡＳＩＣは、ユーザデバイス内に存在することができる。代替として、プロセッサと記憶媒体は、ユーザデバイス内のディスクリートのコンポーネントとして存在してもよい。さらに、一部の態様では、方法またはアルゴリズムのステップは、コンピュータプログラム製品に組み込まれることが可能なマシン可読媒体および／またはコンピュータ可読媒体の上のコードセットおよび／または命令のいずれかとして、または任意の組み合わせもしくはセットとして存在することができる。

【０１６６】

以上の開示は、例示的な態様および／または態様を説明するが、説明される態様、および／または添付の特許請求の範囲によって規定される態様の範囲を逸脱することなく、様々な変更および変形が行われることもできることに留意されたい。したがって、説明される態様は、添付の特許請求の範囲に含まれるすべてのそのような代替、変形、および変種を包含することを意図している。さらに、説明される態様のエレメント、および／または

態様は、単数形で説明される、または主張されることができるものの、単数形への限定が明言されない限り、複数形も企図される。さらに、任意の態様のすべて、もしくは一部分、および／または態様が、特に明記しない限り、他の任意の態様のすべて、もしくは一部分、および／または態様とともに利用されることができる。

【０１６７】

「含む」という言葉が、詳細な説明または特許請求の範囲において使用される限りにおいて、そのような用語は、請求項におけるつなぎの語として使用される場合に解釈される「備える」という言葉と同様に、包含的であることが意図される。さらに、詳細な説明、または特許請求の範囲において使用される「または」という言葉は、「排他的でない「または」」であることが意図される。

以下に本願発明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］

スペクトル認証およびアクセス制御のための方法であって、

信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得することと、

第２のデバイスから、前記信頼されるサードパーティ、または別の信頼されるパーティによって発行された、前記第２のデバイスに関する第２の認証チケットを受信することと、

前記第２のデバイスとの有効にされた通信セッションを確立することと、

を備える方法。

［Ｃ２］

前記第２のデバイスと前記有効にされた通信セッションを確立する前に、前記第２のデバイスに関する前記第２の認証チケットを有効にすることをさらに備える、

Ｃ１に記載の方法。

［Ｃ３］

前記第２の認証チケットは、有効時間と、前記信頼されるサードパーティまたは前記別の信頼されるパーティの暗号署名とを含み、前記第２の認証チケットを有効にすることは、前記有効時間および前記暗号署名を検証することを含む、

Ｃ２に記載の方法。

［Ｃ４］

前記第２の認証チケットを有効にすることは、デジタル証明書の中に含まれる公開鍵とアイデンティティの両方に関連する秘密鍵の所有を検証することを備える、

Ｃ２に記載の方法。

［Ｃ５］

前記第２のデバイスに関する前記第２の認証チケットを有効にすることに失敗することは、前記第１のデバイスと前記第２のデバイスの間の通信リンクを解体することをもたらす、

Ｃ２に記載の方法。

［Ｃ６］

前記第２のデバイスと前記有効にされた通信セッションを確立する前に、前記第１の認証チケットを前記第２のデバイスに送信することをさらに備える、

Ｃ１に記載の方法。

［Ｃ７］

前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる情報に基づいて、前記有効にされた通信セッションをセキュリティで保護することをさらに備える、

Ｃ１に記載の方法。

［Ｃ８］

前記第１の認証チケットは、前記第１のデバイスの識別子と、前記信頼されるサードパーティの署名と、有効時間と、を備える、

Ｃ１に記載の方法。

［Ｃ９］
前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成される、
Ｃ１に記載の方法。
［Ｃ１０］
前記第１の認証チケットは、前記第１のデバイスによってアクセスされることが許されるサービスを備え、さらに前記第２の認証チケットは、前記第２のデバイスによってアクセスされることが許されるサービスを備える、
Ｃ１に記載の方法。
［Ｃ１１］
前記第１の認証チケットと前記第２の認証チケットの少なくともいずれかは、従来のデジタル証明書として実現される、
Ｃ１に記載の方法。
［Ｃ１２］
信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得すること、第２のデバイスから、前記第２のデバイスに関する第２の認証チケットを受信すること、および前記第２のデバイスとの有効にされた通信セッションを確立すること、と関係する命令を保持するメモリと、なお、前記第２の認証チケットは、前記信頼されるサードパーティ、または別の信頼されるパーティによって発行される、
前記メモリに結合され、前記メモリの中に保持される前記命令を実行するように構成されるプロセッサと、
を備える無線通信装置。
［Ｃ１３］
前記メモリは、前記有効にされた通信セッションを確立する前に、前記第２のデバイスに関する前記第２の認証チケットを有効にすることと関係する命令をさらに保持し、前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成される、
Ｃ１２に記載の無線通信装置。
［Ｃ１４］
前記第２のデバイスに関する前記第２の認証チケットを有効にすることに失敗することは、前記第１のデバイスと前記第２のデバイスの間の通信リンクを解体することをもたらす、
Ｃ１３に記載の無線通信装置。
［Ｃ１５］
前記メモリは、前記第２のデバイスと前記有効にされた通信セッションを確立することの前に、前記第１の認証チケットを前記第２のデバイスに伝送することに関係する命令をさらに保持し、前記第１の認証チケットは、前記第１のデバイスの識別子と、前記信頼されるサードパーティの署名と、有効時間とを備える、
Ｃ１２に記載の無線通信装置。
［Ｃ１６］
スペクトル認証およびアクセス制御を円滑にする無線通信装置であって、
信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得するための手段と、
前記第１の認証チケットを第２のデバイスに伝送するための手段と、
前記第２のデバイスから、前記信頼されるサードパーティ、または別の信頼されるサードパーティによって発行された、前記第２のデバイスに関する第２の認証チケットを受信するための手段と、
前記第２のデバイスに関する前記第２の認証チケットを有効にするための手段と、

前記第２の認証チケットの前記有効確認が成功した場合、前記第２のデバイスとの有効にされた通信セッションを確立するための手段と、
を備える無線通信装置。
［Ｃ１７］
前記第１の認証チケットは、前記第１のデバイスの識別子と、前記信頼されるサードパーティの署名とを備え、前記第２の認証チケットは、前記第２のデバイスの識別子と、前記信頼されるサードパーティ、または前記別の信頼されるパーティの署名と、を備える、
Ｃ１６に記載の無線通信装置。
［Ｃ１８］
コンピュータに、信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得させるための第１のコードセットと、
前記コンピュータに、第２のデバイスから、前記信頼されるサードパーティ、または別の信頼されるパーティによって発行された、前記第２のデバイスに関する第２の認証チケットを受信させるための第２のコードセットと、
前記コンピュータに、前記第２の認証チケットを有効にさせるための第３のコードセットと、
前記コンピュータに、前記第２の認証チケットが有効である場合、前記第２のデバイスとの有効にされた通信セッションを確立させるための第４のコードセットと、
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。
［Ｃ１９］
スペクトル認証およびアクセス制御を提供するように構成された少なくとも１つのプロセッサであって、
信頼されるサードパーティによって発行された第１のデバイスに関する第１の認証チケットを獲得するための第１のモジュールと、
前記第１の認証チケットを第２のデバイスに伝送するための第２のモジュールと、
前記第２のデバイスから、前記信頼されるサードパーティ、または別の信頼されるサードパーティによって発行された、前記第２のデバイスに関する第２の認証チケットを受信するための第３のモジュールと、
前記第２のデバイスに関する前記第２の認証チケットを有効にするための第４のモジュールと、
前記第２の認証チケットの前記有効確認が成功した場合、前記第２のデバイスとの有効にされた通信セッションを確立するための第５のモジュールと、
を備えるプロセッサ。
［Ｃ２０］
前記第１の認証チケットは、前記第１のデバイスによってアクセスされることが許されるサービスを備え、前記有効にされた通信セッションは、前記第１の認証チケットおよび前記第２の認証チケットの中に含まれる許されたサービスのリストの中で指定されるタイプおよび様態のデータを伝送するように構成される、
Ｃ１９に記載の少なくとも１つのプロセッサ。
［Ｃ２１］
スペクトル認証およびアクセス制御のための方法であって、
第１のデバイスからシステムアクセスを求める要求を受信することと、
前記第１のデバイスの認証を実行することと、
前記第１のデバイスに関して認証され得るシステムアクセスを判定することと、
前記認証されたシステムアクセスに基づいて、前記第１のデバイスに関する認証チケットを作成することと、
を備える方法。
［Ｃ２２］
前記第１のデバイス認証は、外部から、セキュリティで保護された通信リンクを介してネットワークデバイスから獲得される、

Ｃ２１に記載の方法。
［Ｃ２３］
システムアクセスを判定することは、前記システムにアクセスすることを認証された複数のデバイスのリストを含む構成パラメータデータベースを調べることを備える、
Ｃ２１に記載の方法。
［Ｃ２４］
前記認証または前記認証されたシステムアクセスは、前記第１のデバイスに関連付けられた証明書によって判定される、
Ｃ２１に記載の方法。
［Ｃ２５］
前記証明書は、共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の少なくとも１つ、または共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の組み合わせである、
Ｃ２４に記載の方法。
［Ｃ２６］
前記認証チケットは、前記第１のデバイスのアイデンティティを備える、
Ｃ２１に記載の方法。
［Ｃ２７］
前記認証チケットは、前記第１のデバイスのアイデンティティと、前記認証チケットが有効である有効範囲と、を備える、
Ｃ２１に記載の方法。
［Ｃ２８］
前記認証チケットは、前記第１のデバイスのアイデンティティと、前記認証チケットが有効である有効範囲と、暗号署名と、を備える、
Ｃ２１に記載の方法。
［Ｃ２９］
少なくとも第１のデバイスからシステムアクセスを求める要求を受信すること、前記少なくとも第１のデバイスの認証を実行すること、前記第１のデバイスに関して認証され得るシステムアクセスを判定すること、前記認証されたシステムアクセスに部分的に基づいて、前記少なくとも第１のデバイスに関する認証チケットを生成すること、と関係する命令を保持するメモリと、
前記メモリに結合された、前記メモリの中に保持される命令を実行するように構成されるプロセッサと、
を備える無線通信装置。
［Ｃ３０］
前記少なくとも第１のデバイスの認証は、ネットワークデバイスからセキュリティで保護された通信リンクを介して獲得される、
Ｃ２９に記載の無線通信装置。
［Ｃ３１］
システムアクセスを判定することは、前記システムにアクセスすることを認証された複数のデバイスのリストを含む構成パラメータデータベースを調べることを備える、
Ｃ２９に記載の無線通信装置。
［Ｃ３２］
前記認証または前記認証されたシステムアクセスは、前記第１のデバイスに関連付けられた証明書によって判定され、前記証明書は、共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の少なくとも１つ、または共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の組み合わせである、
Ｃ２９に記載の無線通信装置。
［Ｃ３３］
前記認証チケットは、前記第１のデバイスのアイデンティティと、前記認証チケットが

有効である有効期間と、暗号署名と、
を備えるＣ２９に記載の無線通信装置。
［Ｃ３４］
スペクトル認証を提供する無線通信装置であって、
少なくとも第１のデバイスからシステムアクセスを求める要求を受信するための手段と、
前記少なくとも第１のデバイスの認証を実行するための手段と、
前記少なくとも第１のデバイスに関して提供され得るシステムアクセスを判定するための手段と、
前記認証されたシステムアクセスに部分的に基づいて、前記少なくとも第１のデバイスに関する認証チケットを生成するための手段と、
を備える無線通信装置。
［Ｃ３５］
前記認証チケットは、前記第１のデバイスのアイデンティティと、前記認証チケットが有効である有効範囲と、暗号署名と、
を備えるＣ３４に記載の無線通信装置。
［Ｃ３６］
前記システムにアクセスすることを認証された複数のデバイスのリストを含む構成パラメータデータベースを調べるための手段をさらに備える、
Ｃ３４に記載の無線通信装置。
［Ｃ３７］
コンピュータに、第１のデバイスからシステムアクセスを求める要求を受信させるための第１のコードセットと、
前記コンピュータに、前記第１のデバイスの認証を実行させるための第２のコードセットと、
前記コンピュータに、前記第１のデバイスに関して認証され得るシステムアクセスを判定させるための第３のコードセットと、
前記コンピュータに、前記認証されたシステムアクセスに基づいて、前記第１のデバイスに関する認証チケットを生成させるための第４のコードセットと、
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。
［Ｃ３８］
システムアクセスを特定することは、前記システムにアクセスすることを認証された複数のデバイスのリストを含む構成パラメータデータベースを調べることを備え、さらに前記認証または前記認証されたシステムアクセスは、前記第１のデバイスに関連付けられた証明書に基づいて判定され、前記証明書は、共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の少なくとも１つ、または共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の組み合わせである、
Ｃ３７に記載のコンピュータプログラム製品。
［Ｃ３９］
スペクトル認証を提供するように構成された少なくとも１つのプロセッサであって、
少なくとも第１のデバイスからシステムアクセスを求める要求を受信するための第１のモジュールと、
前記少なくとも第１のデバイスの認証を実行するための第２のモジュールと、
前記少なくとも第１のデバイスに関して認証され得るシステムアクセスを判定するための第３のモジュールと、
前記認証されたシステムアクセスに部分的に基づいて、前記少なくとも第１のデバイスのアイデンティティと、認証チケットが有効である有効範囲と、暗号署名とを備える、前記少なくとも第１のデバイスに関する認証チケットを生成するための第４のモジュールと、
を備えるプロセッサ。

［Ｃ４０］

前記第４のモジュールは、前記第１のデバイスに関連付けられた証明書を利用して、認証され得る前記システムアクセスを判定し、前記証明書は、共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の少なくとも１つ、または共有秘密鍵、公開鍵、認証情報、サービスのリスト、料金請求情報の組み合わせである、

Ｃ３９に記載の少なくとも１つのプロセッサ。

【図１】

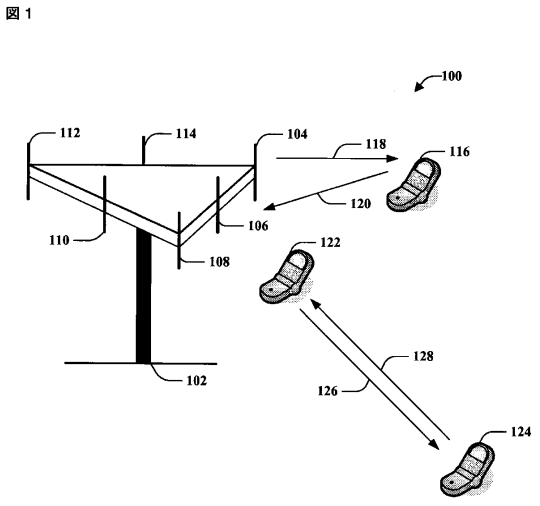

FIG. 1

【図２】

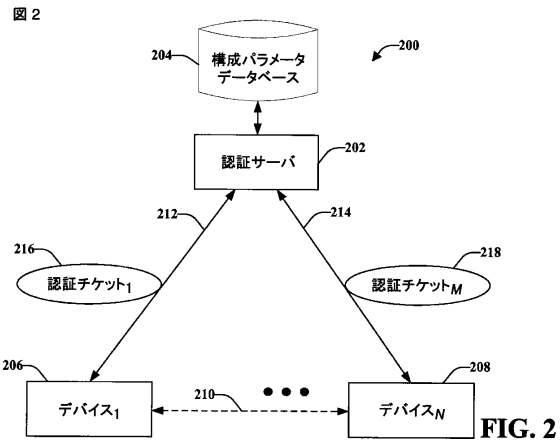

FIG. 2

【図３】

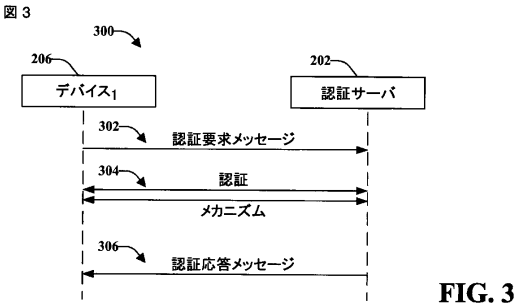

FIG. 3

【図４】

図４

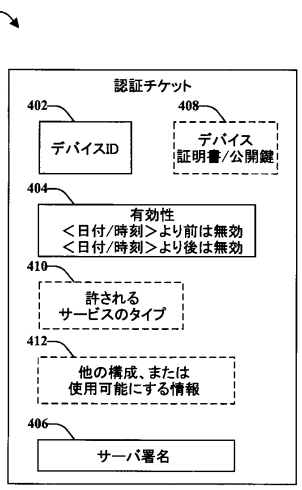

FIG. 4

【図５】

図５

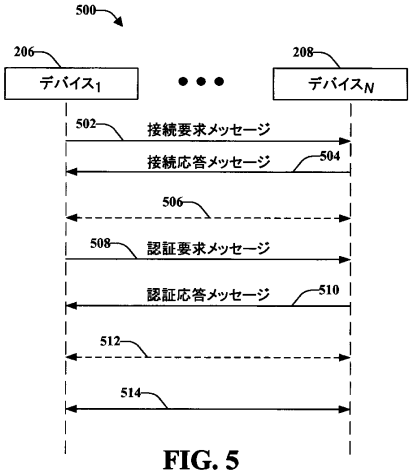

FIG. 5

【図６】

図６

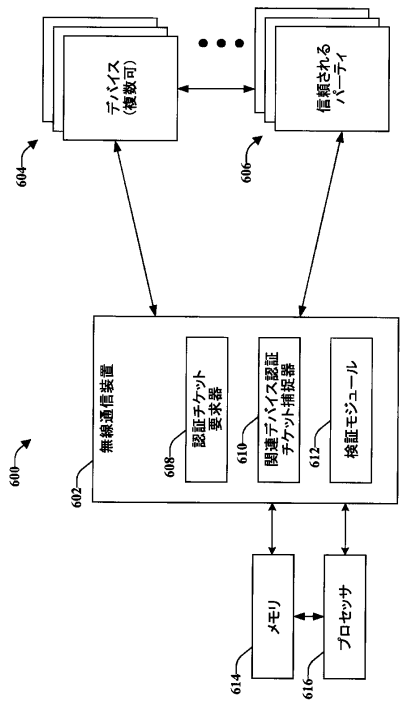

FIG. 6

【図７】

図７

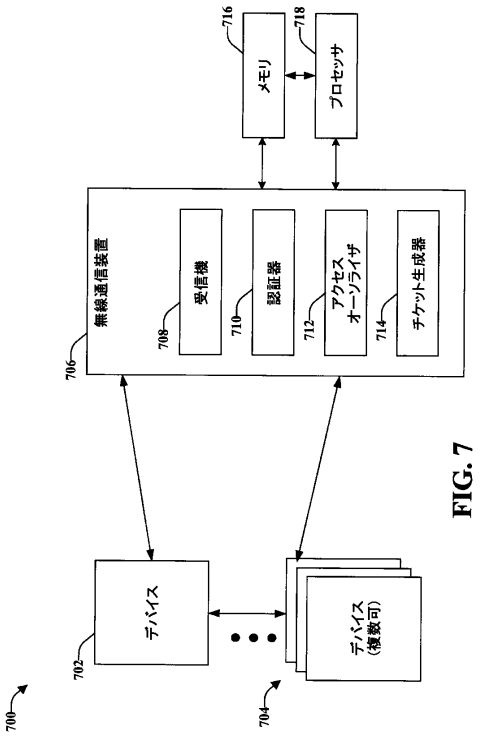

FIG. 7

【図８】

図 8

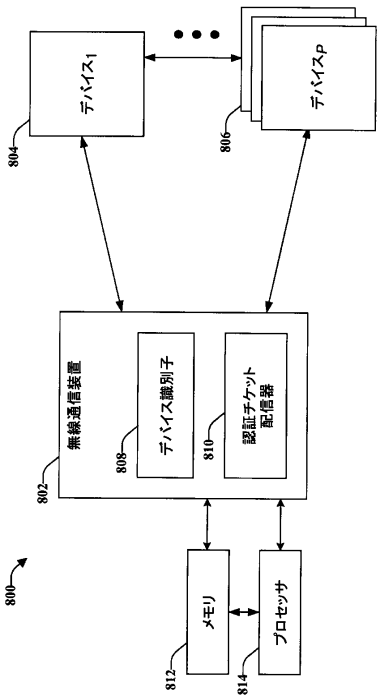

FIG. 8

【図９】

図 9

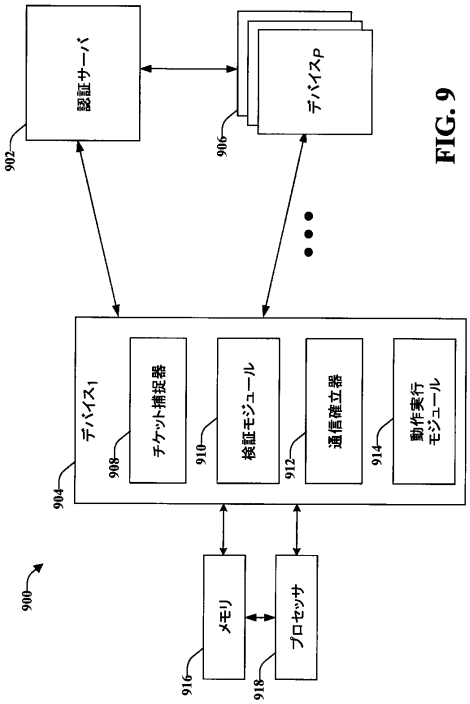

FIG. 9

【図１０】

図 10

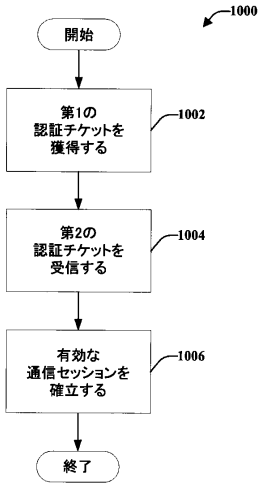

FIG. 10

【図１１】

図 11

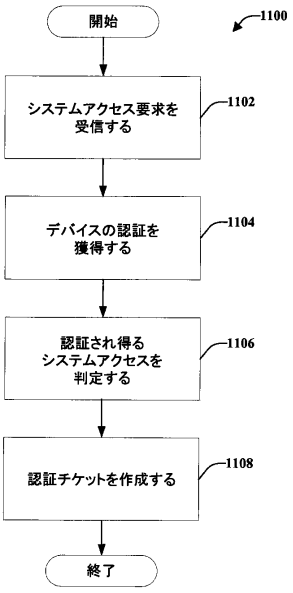

FIG. 11

【図１２】

図 12

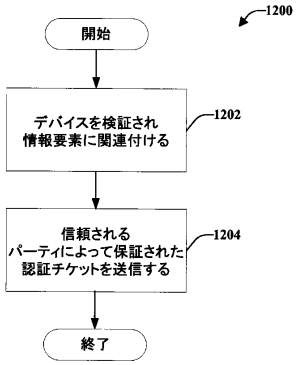

FIG. 12

【図１３】

図 13

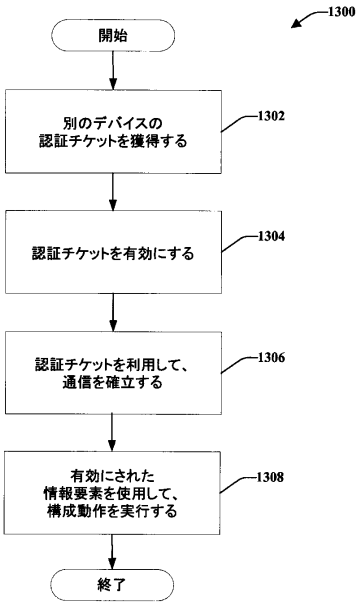

FIG. 13

【図１４】

図 14

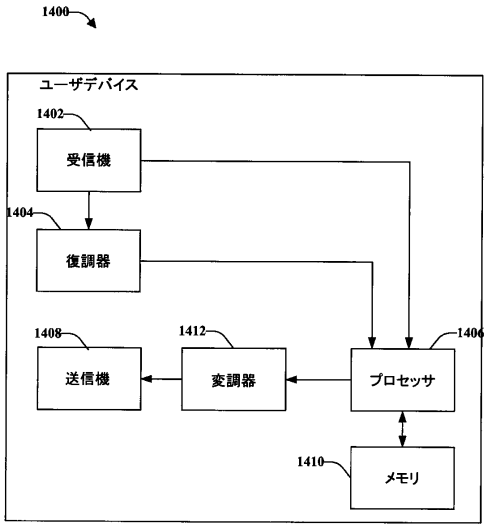

FIG. 14

【図１５】

図 15

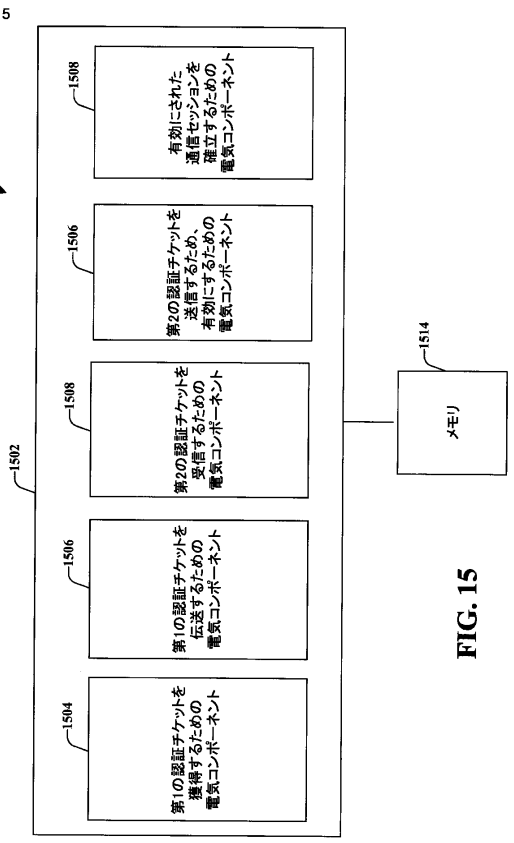

FIG. 15

【図１６】

図 16

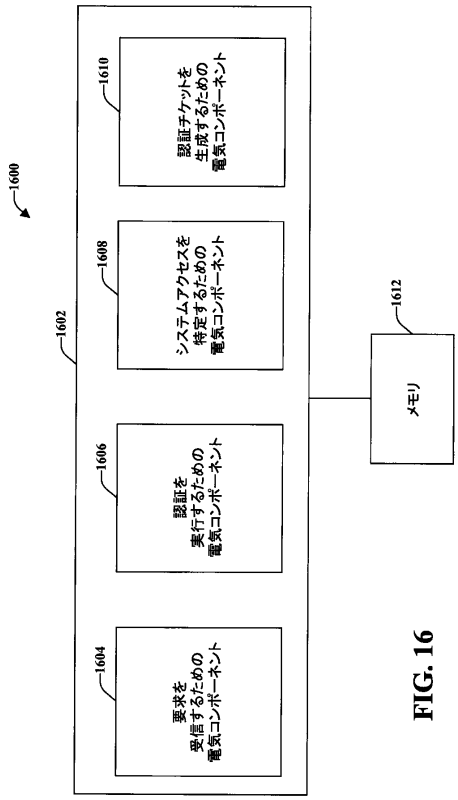

FIG. 16

【図１７】

図 17

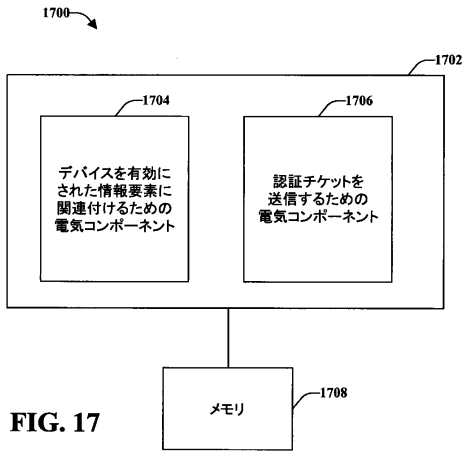

FIG. 17

【図１８】

図 18

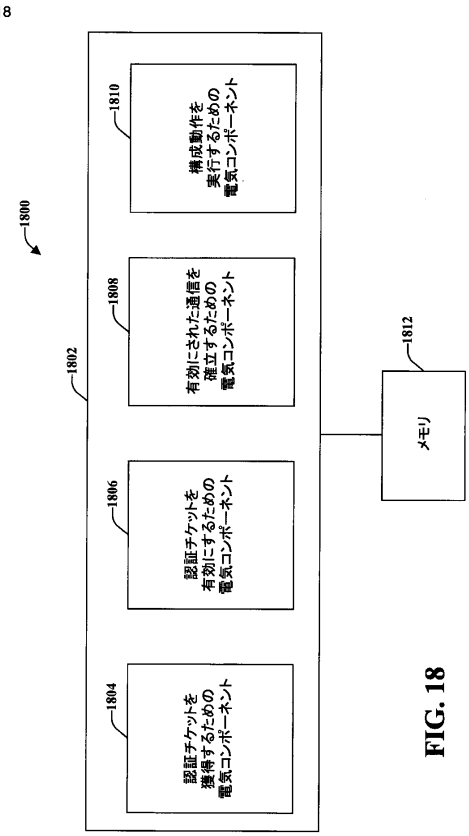

FIG. 18

フロントページの続き

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

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(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 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
(74)代理人 100134290
弁理士 竹内 将訓
(72)発明者 バンデルビーン・マイケラ
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
(72)発明者 シャオ、ル
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

審査官 石井 則之

(56)参考文献 特表２００９－５３３９８４（ＪＰ，Ａ）
特開２００５－１１０１１２（ＪＰ，Ａ）
特表２００３－５００９２３（ＪＰ，Ａ）
特開２００４－２７４１９３（ＪＰ，Ａ）
LOOTAH, TARP: TICKET-BASED ADDRESS RESOLUTION PROTOCOL, COMPUTER NETWORKS, NL, ELSEVIER SCIENCE PUBLISHERS B.V., ２００７年 ８月２３日, V51 N15, P4322-4337
BRIK V, DSAP: A PROTOCOL FOR COORDINATED SPECTRUM ACCESS, 2005 1ST IEEE INTERNATIONAL SYMPOSIUM ON NEW FRONTIERS IN DYNAMIC SPECTRUM ACCESS NETWORKS, ２００５年１１月 ８日, P611-614

YIHONG ZHOU, AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING FOR REAL-TIME SECONDARY MARKET SERVICES, IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC 2005), 米国, IEEE, ２００５年　５月１６日, V2, P1005-1009

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｂ　　７／２４－２６
Ｈ０４Ｗ　　４／００－９９／００