(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2016-136724
(P2016-136724A)
(43)公開日　平成28年7月28日(2016.7.28)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
H04L 9/32	(2006.01)	H04L	9/00	675A	5K067
H04W 12/08	(2009.01)	H04W	12/06		
H04W 48/16	(2009.01)	H04W	48/16	110	

審査請求 有　請求項の数 30　ＯＬ　外国語出願　（全 60 頁）

(21)出願番号　特願2016-8945 (P2016-8945)
(22)出願日　平成28年1月20日 (2016.1.20)
(62)分割の表示　特願2014-530755 (P2014-530755)の分割
原出願日　平成24年9月12日 (2012.9.12)
(31)優先権主張番号　61/533,627
(32)優先日　平成23年9月12日 (2011.9.12)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/535,234
(32)優先日　平成23年9月15日 (2011.9.15)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/583,052
(32)優先日　平成24年1月4日 (2012.1.4)
(33)優先権主張国　米国 (US)

(71)出願人　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　100158805
弁理士　井関　守三
(74)代理人　100194814
弁理士　奥村　元宏

最終頁に続く

(54)【発明の名称】リンク設定および認証を実行するシステムおよび方法

(57)【要約】　（修正有）
【課題】無線通信におけるリンク設定処理および認証処理において、認証レベルを維持し、通信されるメッセージの数を低減する。
【解決手段】第１の方法は、保護されていない関連付け要求と、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を含む関連付け応答とを利用する。第２の方法は、第１のＡＮｏｎｃｅを用いる第１のリンク設定中に、第２のリンク設定において用いるための第２のＡＮｏｎｃｅを受信することを含む。第３の方法は、関連付け要求を保護するために、テンポラリ鍵を利用する。第４の方法は、アクセス・ポイントから受信したＡＮｏｎｃｅシードに基づいて、モバイル・デバイスにおいて、ＡＮｏｎｃｅを生成することを含む。
【選択図】図１７

図17

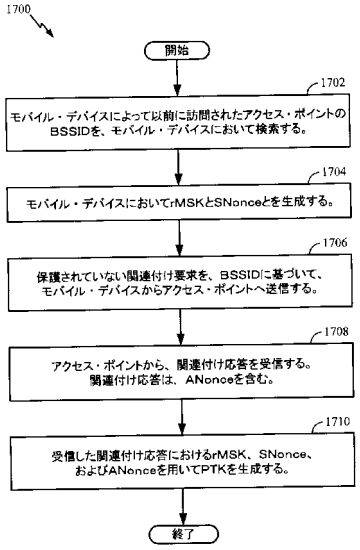

FIG. 17

【特許請求の範囲】
【請求項１】
方法であって、
モバイル・デバイスからアクセス・ポイントへ、保護されていない関連付け要求を送信することと、
前記アクセス・ポイントから、関連付け応答を受信することと、ここで、前記関連付け応答は、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を含む、
前記モバイル・デバイスにおいて、前記ＡＮｏｎｃｅを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
を備える方法。
【請求項２】
前記モバイル・デバイスにおいて、前記保護されていない関連付け要求を前記アクセス・ポイントへ送信する前に、再認証マスタ・セッション鍵（ｒＭＳＫ）および局ノンス（ＳＮｏｎｃｅ）を生成することをさらに備え、
前記ＰＴＫは、前記ｒＭＳＫおよび前記ＳＮｏｎｃｅを用いて生成される、請求項１に記載の方法。
【請求項３】
前記モバイル・デバイスのメモリから、前記アクセス・ポイントの基本サービス・セット識別子（ＢＳＳＩＤ）を検索することをさらに備え、
前記保護されていない関連付け要求は、前記ＢＳＳＩＤに基づいて前記アクセス・ポイントへ送信される、請求項１に記載の方法。
【請求項４】
前記モバイル・デバイスにおいて位置情報が決定されることに応じて、前記保護されていない関連付け要求が送信される、請求項１に記載の方法。
【請求項５】
前記ＡＮｏｎｃｅ以外の、前記関連付け要求における情報要素が、前記ＡＮｏｎｃｅを用いて保護され、
前記方法はさらに、前記ＰＴＫを用いて、前記関連付け応答の保全性を検証すること、
を備える請求項１に記載の方法。
【請求項６】
装置であって、
プロセッサと、
アクセス・ポイントへ、保護されていない関連付け要求を送信することと、
前記アクセス・ポイントから、関連付け応答を受信することと、ここで、前記関連付け応答は、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を含む、
前記ＡＮｏｎｃｅを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項７】
前記命令群はさらに、前記保護されていない関連付け要求を前記アクセス・ポイントへ送信する前に、再認証マスタ・セッション鍵（ｒＭＳＫ）および局ノンス（ＳＮｏｎｃｅ）を生成することのために前記プロセッサによって実行可能であり、
前記ＰＴＫは、前記ｒＭＳＫおよび前記ＳＮｏｎｃｅを用いて生成される、請求項６に記載の装置。
【請求項８】
前記メモリはさらに、前記アクセス・ポイントの基本サービス・セット識別子（ＢＳＳＩＤ）を格納し、
前記命令群はさらに、前記メモリから前記アクセス・ポイントのＢＳＳＩＤを検索することのために前記プロセッサによって実行可能であり、

前記保護されていない関連付け要求は、前記ＢＳＳＩＤに基づいて前記アクセス・ポイントへ送信される、請求項６に記載の装置。
【請求項９】
装置であって、
モバイル・デバイスからアクセス・ポイントへ、保護されていない関連付け要求を送信する手段と、
前記アクセス・ポイントから関連付け応答を受信する手段と、ここで、前記関連付け応答は、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を含む、
前記モバイル・デバイスにおいて、前記ＡＮｏｎｃｅを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成する手段と、
を備える装置。
【請求項１０】
プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスによってアクセス・ポイントへ送信されるべき、保護されていない関連付け要求を生成することと、
前記アクセス・ポイントからの関連付け応答から検索されたアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
【請求項１１】
方法であって、
アクセス・ポイントにおいて、モバイル・デバイスから、保護されていない関連付け要求を受信することと、
前記保護されていない関連付け要求から、開始メッセージを抽出することと、
前記開始メッセージを、認証サーバへ送信することと、
前記認証サーバから、回答メッセージを受信することと、ここで、前記回答メッセージは、再認証マスタ・セッション鍵（ｒＭＳＫ）を含む、
アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスへ、関連付け応答を送信することと、ここで、前記関連付け応答は、前記ＡＮｏｎｃｅを含む、
を備える方法。
【請求項１２】
前記アクセス・ポイントにおいて、前記保護されていない関連付け要求に含まれる局ノンス（ＳＮｏｎｃｅ）、前記ＡＮｏｎｃｅ、および前記ｒＭＳＫを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することをさらに備え、
前記関連付け応答は、前記ＰＴＫを用いて保護されている、請求項１１に記載の方法。
【請求項１３】
装置であって、
プロセッサと、
モバイル・デバイスから、保護されていない関連付け要求を受信することと、
前記保護されていない関連付け要求から、開始メッセージを抽出することと、
前記開始メッセージを、認証サーバへ送信することと、
前記認証サーバから、回答メッセージを受信することと、ここで、前記回答メッセージは、再認証マスタ・セッション鍵（ｒＭＳＫ）を含む、
アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスへ関連付け応答を送信することと、ここで、前記関連付け応答は、前記ＡＮｏｎｃｅを含む、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項１４】

前記命令群はさらに、前記保護されていない関連付け要求に含まれる局ノンス（ＳＮｏｎｃｅ）、前記ＡＮｏｎｃｅ、および前記ｒＭＳＫを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することのために前記プロセッサによって実行可能であり、
前記関連付け応答は、前記ＰＴＫを用いて保護されている、請求項１３に記載の装置。
【請求項１５】
装置であって、
アクセス・ポイントにおいて、モバイル・デバイスから、保護されていない関連付け要求を受信する手段と、
前記保護されていない関連付け要求から、開始メッセージを抽出する手段と、
前記開始メッセージを、認証サーバへ送信する手段と、
前記認証サーバから、回答メッセージを受信する手段と、ここで、前記回答メッセージは、再認証マスタ・セッション鍵（ｒＭＳＫ）を含む、
アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成する手段と、
前記アクセス・ポイントから前記モバイル・デバイスへ、関連付け応答を送信する手段と、ここで、前記関連付け応答は、前記ＡＮｏｎｃｅを含む、
を備える装置。
【請求項１６】
プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスから受信された、保護されていない関連付け要求から、開始メッセージを抽出することと、
前記開始メッセージに応じて、認証サーバから受信された回答メッセージから再認証マスタ・セッション鍵（ｒＭＳＫ）を抽出することと、
アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスへ送信されるべき関連付け応答を生成することと、ここで、前記関連付け応答は、前記ＡＮｏｎｃｅを含む、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
【請求項１７】
方法であって、
モバイル・デバイスにおいて、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、アクセス・ポイントとの第１のリンク設定を開始することと、
前記アクセス・ポイントとの第１のリンク設定中、前記第１のリンク設定に後続する、前記アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信することと、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
を備える方法。
【請求項１８】
前記第１のＡＮｏｎｃｅは、前記モバイル・デバイスのメモリから検索されるか、前記アクセス・ポイントからビーコンまたはプローブ応答で受信されるか、これら任意の組み合わせで取得される、請求項１７に記載の方法。
【請求項１９】
前記第２のＡＮｏｎｃｅは、関連付け応答で、拡張可能認証プロトコル（ＥＡＰ）オーバ・ローカル・エリア・ネットワーク（ＬＡＮ）（ＥＡＰＯＬ）メッセージで、または、これら任意の組み合わせで受信される、請求項１７に記載の方法。
【請求項２０】
前記第２のＡＮｏｎｃｅは、有効性寿命を有する、請求項１７に記載の方法。
【請求項２１】
前記後続するリンク設定の開始前に、前記第２のＡＮｏｎｃｅの有効性寿命が終了した場合、
ビーコンまたはプローブ応答で第３のＡＮｏｎｃｅを受信することと、
前記第３のＡＮｏｎｃｅを用いて前記第２のリンク設定を開始することと、
前記第２のリンク設定中、前記アクセス・ポイントとの第３のリンク設定に用いるため

の第４のＡＮｏｎｃｅを受信することと、
をさらに備える請求項２０に記載の方法。
【請求項２２】
前記モバイル・デバイスにおいて、前記第２のＡＮｏｎｃｅを用いて、前記アクセス・ポイントとの第２のリンク設定を開始することと、
前記アクセス・ポイントとの第２のリンク設定中、前記アクセス・ポイントとの、後続する第３のリンク設定において用いるための第３のＡＮｏｎｃｅを受信することと、
をさらに備える請求項１７に記載の方法。
【請求項２３】
装置であって、
プロセッサと、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、アクセス・ポイントとの第１のリンク設定を開始することと、
前記アクセス・ポイントとの第１のリンク設定中、前記第１のリンク設定に後続する、前記アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信することと、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項２４】
前記第１のＡＮｏｎｃｅは、前記メモリから検索されるか、前記アクセス・ポイントからビーコンまたはプローブ応答で受信されるか、これら任意の組み合わせで取得され、
前記第２のＡＮｏｎｃｅは、関連付け応答で、拡張可能認証プロトコル（ＥＡＰ）オーバ・ローカル・エリア・ネットワーク（ＬＡＮ）（ＥＡＰＯＬ）メッセージで、または、これら任意の組み合わせで受信される、請求項２３に記載の装置。
【請求項２５】
前記第２のＡＮｏｎｃｅは、有効性寿命を有する、請求項２３に記載の装置。
【請求項２６】
前記命令群はさらに、
前記後続するリンク設定の開始前に、前記第２のＡＮｏｎｃｅの有効性寿命が終了した場合、
ビーコンまたはプローブ応答で第３のＡＮｏｎｃｅを受信することと、
前記第３のＡＮｏｎｃｅを用いて前記第２のリンク設定を開始することと、
前記第２のリンク設定中、前記アクセス・ポイントとの第３のリンク設定に用いるための第４のＡＮｏｎｃｅを受信することと、
のために前記プロセッサによって実行可能である、請求項２５に記載の装置。
【請求項２７】
前記命令群はさらに、
前記第２のＡＮｏｎｃｅを用いて、前記アクセス・ポイントとの第２のリンク設定を開始することと、
前記アクセス・ポイントとの第２のリンク設定中、前記アクセス・ポイントとの、後続する第３のリンク設定に用いるための第３のＡＮｏｎｃｅを受信することと、
のために前記プロセッサによって実行可能である、請求項２３に記載の装置。
【請求項２８】
装置であって、
モバイル・デバイスにおいて、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、アクセス・ポイントとの第１のリンク設定を開始する手段と、
前記アクセス・ポイントとの第１のリンク設定中、前記第１のリンク設定に後続する、前記アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信する手段と、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、

を備える装置。
【請求項２９】
プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスにおいて、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、アクセス・ポイントとの第１のリンク設定を開始することと、
前記アクセス・ポイントとの第１のリンク設定中、前記第１のリンク設定に後続する、前記アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信することと、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
【請求項３０】
方法であって、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いる第１のリンク設定中に、アクセス・ポイントからモバイル・デバイスへ、前記第１のリンク設定に後続する、前記モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを送信することを備え、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、方法。
【請求項３１】
前記第１のリンク設定の開始前に、前記第１のＡＮｏｎｃｅを、ビーコンまたはプローブ応答で、前記モバイル・デバイスへ送信すること、をさらに備える請求項３０に記載の方法。
【請求項３２】
前記第２のＡＮｏｎｃｅは、前記モバイル・デバイスへ、関連付け応答で、拡張可能認証プロトコル（ＥＡＰ）オーバ・ローカル・エリア・ネットワーク（ＬＡＮ）（ＥＡＰＯＬ）メッセージで、または、これら任意の組み合わせで送信される、請求項３０に記載の方法。
【請求項３３】
前記第２のＡＮｏｎｃｅは、有効性寿命に関連付けられる、請求項３０に記載の方法。
【請求項３４】
装置であって、
プロセッサと、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いる第１のリンク設定中、前記第１のリンク設定に後続する、前記モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅをモバイル・デバイスへ送信すること、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項３５】
前記命令群は、前記第１のリンク設定の開始前に、前記第１のＡＮｏｎｃｅをビーコンまたはプローブ応答によって前記モバイル・デバイスへ送信することのために前記プロセッサによってさらに実行可能である、請求項３４に記載の装置。
【請求項３６】
前記第２のＡＮｏｎｃｅは、前記モバイル・デバイスへ、関連付け応答で、拡張可能認証プロトコル（ＥＡＰ）オーバ・ローカル・エリア・ネットワーク（ＬＡＮ）（ＥＡＰＯＬ）メッセージで、または、これら任意の組み合わせで送信される、請求項３４に記載の装置。
【請求項３７】
前記第２のＡＮｏｎｃｅは、有効性寿命に関連付けられる、請求項３４に記載の装置。
【請求項３８】
装置であって、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いる第１のリンク設定中に、

アクセス・ポイントからモバイル・デバイスへ、前記第１のリンク設定に後続する、前記モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを送信する手段と、
前記第１のリンク設定の開始前に、前記第１のＡＮｏｎｃｅを、ビーコンまたはプローブ応答で、前記モバイル・デバイスへ送信する手段と、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
を備える装置。
【請求項３９】
プロセッサによって実行された場合、前記プロセッサに対して、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いる第１のリンク設定中に、アクセス・ポイントからモバイル・デバイスへ、前記第１のリンク設定に後続する、前記モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを送信させる命令群を備え、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、非一時的なプロセッサ読取可能な媒体。
【請求項４０】
方法であって、
モバイル・デバイスにおいて、アクセス・ポイントから、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を受信することと、
前記第１のＡＮｏｎｃｅを用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
前記アクセス・ポイントへ、関連付け要求を送信することと、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記アクセス・ポイントから関連付け応答を受信することと、ここで、前記関連付け応答は、第２のＡＮｏｎｃｅを含み、第２のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅを用いて、前記第２のＰＴＫを生成することと、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いることと、
を備える方法。
【請求項４１】
方法であって、
アクセス・ポイントからモバイル・デバイスへ第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を送信することと、
前記モバイル・デバイスから、関連付け要求を受信することと、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を用いて保護されている、
前記アクセス・ポイントにおいて、前記第１のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて、前記第１のＰＴＫを生成することと、
第２のＡＮｏｎｃｅを生成することと、
前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて、第２のＰＴＫを生成することと、
前記モバイル・デバイスへ、関連付け応答を送信することと、ここで、前記関連付け応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
を備える方法。
【請求項４２】
装置であって、
プロセッサと、
モバイル・デバイスにおいて、アクセス・ポイントから受信された第１のアクセス・

ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき関連付け要求を生成することと、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
前記アクセス・ポイントから、関連付け応答によって受信された第２のＡＮｏｎｃｅおよび前記ＳＮｏｎｃｅを用いて第２のＰＴＫを生成することと、ここで、前記関連付け応答は、前記第２のＰＴＫを用いて保護されている、
前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いることと、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項４３】
装置であって、
プロセッサと、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべき第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスからの関連付け要求によって受信された局ノンス（ＳＮｏｎｃｅ）および前記第１のＡＮｏｎｃｅに基づいて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、ここで、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
第２のＡＮｏｎｃｅを生成することと、
前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて第２のＰＴＫを生成することと、
前記モバイル・デバイスへ送信されるべき関連付け応答を生成することと、ここで、前記関連付け応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項４４】
プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスにおいて、アクセス・ポイントから受信された第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき関連付け要求を生成することと、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、
前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
前記アクセス・ポイントから、関連付け応答によって受信された第２のＡＮｏｎｃｅおよび前記ＳＮｏｎｃｅを用いて第２のＰＴＫを生成することと、ここで、前記関連付け応答は、前記第２のＰＴＫを用いて保護されている、
前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いることと、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
【請求項４５】
プロセッサによって実行された場合、前記プロセッサに対して、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべき第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスからの関連付け要求によって受信された前記第１のＡＮｏｎｃｅおよび局ノンス（ＳＮｏｎｃｅ）に基づいて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、ここで、前記関連付け要求は、前記第１のＰＴＫを用いて保

護されている、
第２のＡＮｏｎｃｅを生成することと、
前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて第２のＰＴＫを生成することと、
前記モバイル・デバイスへ送信されるべき関連付け応答を生成することと、ここで、前記関連付け応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
【請求項４６】
装置であって、
モバイル・デバイスにおいて、アクセス・ポイントから、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を受信する手段と、
前記第１のＡＮｏｎｃｅを用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成する手段と、
関連付け要求を前記アクセス・ポイントへ送信する手段と、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記アクセス・ポイントから関連付け応答を受信する手段と、ここで、前記関連付け応答は、第２のＡＮｏｎｃｅを含み、第２のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅを用いて、前記第２のＰＴＫを生成する手段と、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いる手段と、
を備える装置。
【請求項４７】
装置であって、
アクセス・ポイントから、モバイル・デバイスへ、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を送信する手段と、
前記モバイル・デバイスから、関連付け要求を受信する手段と、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を用いて保護されている、
前記アクセス・ポイントにおいて、前記第１のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて、前記第１のＰＴＫを生成する手段と、
第２のＡＮｏｎｃｅを生成する手段と、
前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて第２のＰＴＫを生成する手段と、
前記モバイル・デバイスへ、関連付け応答を送信する手段と、ここで、前記関連付け応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
を備える装置。
【請求項４８】
方法であって、
モバイル・デバイスにおいて、アクセス・ポイントから、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を受信することと、
前記モバイル・デバイスにおいて、前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスおよび前記ＡＮｏｎｃｅシードに基づいて、ＡＮｏｎｃｅを生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記アクセス・ポイントとのリンク設定を実行することと、
を備える方法。

【請求項４９】
方法であって、
アクセス・ポイントから、モバイル・デバイスへ、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を送信することと、
前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスを受信することと、
前記モバイル・デバイスのＭＡＣアドレスおよび前記ＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記モバイル・デバイスとのリンク設定を実行することと、
を備える方法。
【請求項５０】
装置であって、
プロセッサと、
モバイル・デバイスにおいて、アクセス・ポイントから受信したアクセス・ポイント・ノンス・シード（ＡＮｏｎｃｅシード）および前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスに基づいて、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記アクセス・ポイントとのリンク設定を実行することと
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項５１】
装置であって、
プロセッサと、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべきアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を生成することと、
前記モバイル・デバイスから受信された前記モバイル・デバイスのＭＡＣアドレスおよび前記ＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記モバイル・デバイスとのリンク設定を実行することと、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項５２】
プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスにおいて、アクセス・ポイントから受信したアクセス・ポイント・ノンス・シード（ＡＮｏｎｃｅシード）および前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスに基づいて、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記アクセス・ポイントとのリンク設定を実行することと、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
【請求項５３】
プロセッサによって実行された場合、前記プロセッサに対して、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべきアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を生成することと、
前記モバイル・デバイスから受信された前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスおよび前記ＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記モバイル・デバイスとのリンク設定を実行することと、

をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
【請求項５４】
装置であって、
モバイル・デバイスにおいて、アクセス・ポイントからアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を受信する手段と、
前記モバイル・デバイスにおいて、前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスおよび前記ＡＮｏｎｃｅシードに基づいて、ＡＮｏｎｃｅを生成する手段と、
前記生成されたＡＮｏｎｃｅに基づいて、前記アクセス・ポイントとのリンク設定を実行する手段と、
を備える装置。
【請求項５５】
装置であって、
アクセス・ポイントから、モバイル・デバイスへ、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を送信する手段と、
前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスを受信する手段と、
前記モバイル・デバイスのＭＡＣアドレスおよび前記ＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを生成する手段と、
前記生成されたＡＮｏｎｃｅに基づいて、前記モバイル・デバイスとのリンク設定を実行する手段と、
を備える装置。
【発明の詳細な説明】
【関連出願に対する相互参照】
【０００１】
本特許出願は、共同所有されている、２０１１年９月１２日出願の米国仮出願６１／５３３，６２７（クゥオルコム整理番号１１３３４６Ｐ１）、２０１１年９月１５日出願の米国仮出願６１／５３５，２３４（クゥオルコム整理番号１１３３４６Ｐ２）、２０１２年１月４日出願の米国仮出願６１／５８３，０５２（クゥオルコム整理番号１１３３４６Ｐ３）、２０１２年３月５日出願の米国仮出願６１／６０６，７９４（クゥオルコム整理番号１２１５８５Ｐ１）、２０１２年５月１１日出願の米国仮出願６１／６４５，９８７（クゥオルコム整理番号１２１５８５Ｐ２）、および２０１２年３月１５日出願の米国仮出願６１／６１１，５５３（クゥオルコム整理番号１２１６０２Ｐ１）からの優先権を主張する。これらの内容は、その全体における参照によって、本明細書に明確に組み込まれている。さらに、２０１２年９月１１日に出願され、並列的な再認証および接続設定を用いた無線通信（WIRELESS COMMUNICATION USING CONCURRENT RE-AUTHENTICATION AND CONNECTION SETUP）と題された、クゥオルコム整理番号１１３３４６の仮出願と、２０１２年９月１１日に出願され、共有された暫定鍵データのセットとの交換をエンコードするためのシステムおよび方法（SYSTEMS AND METHODS FOR ENCODING EXCHANGES WITH A SET OF SHARED EPHEMERAL KEY DATA）と題された、クゥオルコム整理番号１２１６０２の仮出願との内容が、本明細書において参照によって組み込まれている。
【技術分野】
【０００２】
以下は、一般に、無線通信に関し、さらに詳しくは、無線通信におけるリンク設定処理および認証処理に関する。
【背景技術】
【０００３】
技術の進歩の結果、より小型で、よりパワフルなコンピューティング・デバイスが出現した。
【０００４】
例えば、現在、ポータブル無線電話、情報携帯端末（ＰＤＡ）、およびページング・デバ

イスのように、小型で、軽量で、ユーザによって容易に携帯される無線コンピューティング・デバイスを含む、さまざまなポータブル・パーソナル・コンピューティング・デバイスが存在する。

【０００５】

さらに詳しくは、例えば、セルラ電話およびインターネット・プロトコル（ＩＰ）電話のようなポータブル無線電話は、無線ネットワークを介して音声パケットおよびデータ・パケットを通信しうる。

【０００６】

さらに、そのような多くの無線電話は、組み込まれたその他のタイプのデバイスを含んでいる。

【０００７】

例えば、無線電話はまた、デジタル静止カメラ、デジタル・ビデオ・カメラ、デジタル・レコーダ、およびオーディオ・ファイル・プレーヤを含みうる。

【０００８】

また、そのような無線電話は、例えばウェブ・ブラウザ・アプリケーションのように、インターネットにアクセスするために使用されうるソフトウェア・アプリケーションを含む、実行可能な命令群を処理しうる。

【０００９】

このため、これらの無線電話は、著しいコンピューティング能力を含みうる。

【００１０】

無線通信ネットワークによって、通信デバイスは、移動中に、情報を送信および／または受信できるようになった。

【００１１】

これらの無線通信ネットワークは、モバイル・アクセス端末への、および、モバイル・アクセス端末からの情報の転送を可能にするために、その他のパブリック・ネットワークまたはプライベート・ネットワークに通信可能に接続されうる。

【００１２】

そのような通信ネットワークは、
アクセス端末（例えば、モバイル通信デバイス、モバイル電話、無線ユーザ端末）へ無線通信リンクを提供する複数のアクセス・ポイント（ＡＰ）を含む。

【００１３】

アクセス・ポイントは、据置式（例えば、陸上に固定されている）か、または、モバイル（例えば、車両、衛星等の搭載されている）であり、アクセス端末は有効通信範囲エリア内を移動するので、広いエリアの有効通信範囲を提供するように配置されうる。

【００１４】

ポータブル・デバイスは、これら無線ネットワークを経由してデータを通信するように構成されうる。

【００１５】

例えば、多くのデバイスが、アクセス・ポイントを経由したデータの無線交換を可能にする電気電子学会（ＩＥＥＥ）８０２．１１仕様にしたがって動作するように構成される。

【００１６】

いくつかの通信システムでは、モバイル・アクセス端末が、アクセス・ポイントを介して通信ネットワークに接続する場合、アクセス・ポイントは、ネットワーク・アクセス認証を行なう。

【００１７】

モバイル・アクセス端末が異なるアクセス・ポイントへ接続する毎に、認証処理が繰り返される必要がありうる。

【００１８】

しかしながら、この認証処理の繰り返しは、著しい設定遅れをもたらしうる。

【００１９】

多くの通信デバイスが、初期接続段階と、１または複数の再接続段階との両方においてリンク設定を実行するように構成される。

【００２０】

現在のシステムは、ＩＰアドレス割当を保護するために、認証後に、ＡＰ　ＩＰアドレス割当に対して事前に共有された鍵を仮定する。

【００２１】

システム内の２またはそれ以上のメッセージ処理ポイント間で通信されている複数のメッセージを利用することが、リンク設定を可能にする一方、
この通信の必要とされている認証レベルを維持することが高く要求されている間、通信されるメッセージの数が低減される。

【００２２】

さらに、モバイル通信デバイスは、リンク設定が実行されうる前に、近くのアクセス・ポイントを求めてスキャンしうる。

【００２３】

このスキャンは、「パッシブ」または「アクティブ」でありうる。

【００２４】

「パッシブ」なスキャンでは、デバイスは、アクセス・ポイント（例えば、制御メッセージ）を求めてアクティブにリスンしうる。

【００２５】

「アクティブ」なスキャンでは、デバイスは、クエリをブロードキャストし、その後、近くのアクセス・ポイントからの応答を待ちうる。

【００２６】

したがって、「パッシブ」なスキャンは、時間がかかり、「アクティブ」なスキャンは、時間のみならず、モバイル通信デバイスにおける電力をも消費しうる。

【図面の簡単な説明】

【００２７】

同一の参照符号が、全体を通じて類似の要素を特定している図面とともに考慮された場合、さまざまな特徴、特性、および利点が、以下に記載する詳細な記載からより明らかになりうる。

【図１】図１は、無線ネットワークの例を例示する概念図である。

【図２】図２は、典型的なユーザ・デバイスを例示するブロック図である。

【図３】図３は、従来の接続設定において実行されうるメッセージングを例示するフロー図である。

【図４】図４は、本開示の１または複数の態様にしたがって実行されうるメッセージングを例示するフロー図である。

【図５】図５は、リンク設定および認証を実行する際に実行されうるメッセージングを例示するフロー図である。

【図６】図６は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。

【図７】図７は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。

【図８】図８は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。

【図９】図９は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。

【図１０】図１０は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。

【図１１】図１１は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。

【図１２】図１２は、再認証プロトコル中に実行されうるメッセージングを例示するフロ

ー図である。
【図１３】図１３は、再認証プロトコルのために用いられうる鍵階層を例示する。
【図１４】図１４は、再認証要求と発見要求とを生成し、関連付け要求へバンドルするための典型的な処理を示すフロー図である。
【図１５】図１５は、局／端末によって送信された関連付け要求を受信し、この関連付け要求から、再認証要求および上部レイヤ・メッセージを抽出するために基地局において動作可能な典型的な処理を示すフロー図である。
【図１６】図１６は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。
【図１７】図１７は、リンク設定および認証を実行するために図１６の局において動作可能な典型的な処理を示すフロー図である。
【図１８】図１８は、リンク設定および認証を実行するために図１６のアクセス・ポイントにおいて動作可能な典型的な処理を図示するフロー図である。
【図１９】図１９は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。
【図２０】図２０は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。
【図２１】図２１は、リンク設定および認証を実行するために図１９－２０の局において動作可能な典型的な処理を図示するフロー図である。
【図２２】図２２は、リンク設定および認証を実行するために図１９－２０のアクセス・ポイントにおいて動作可能な典型的な処理を図示するフロー図である。
【図２３】図２３は、リンク設定および認証の別の態様によって実行されうるメッセージングを例示する図解である。
【図２４】図２４は、図２３において図示されるようなリンク設定および認証を実行するために局において動作可能な典型的な処理を図示するフロー図である。
【図２５】図２５は、図２３において図示されるようなリンク設定および認証を実行するためにアクセス・ポイントにおいて動作可能な典型的な処理を図示するフロー図である。
【図２６】図２６は、リンク設定および認証の別の態様によって実行されうるメッセージングを例示する図解である。
【図２７】図２７は、図２６において図示されるようなリンク設定および認証を実行するために局において動作可能な典型的な処理を図示するフロー図である。
【図２８】図２８は、図２６において図示されるようなリンク設定および認証を実行するためにアクセス・ポイントにおいて動作可能な典型的な処理を図示するフロー図である。
【発明を実施するための形態】
【００２８】
以下の記載では、本開示が実現されうる具体的な実施形態が例示によって図示されている添付図面に対する参照がなされる。これら実施形態は、当業者が本発明を実施できるように十分詳細な開示の態様を記述することが意図されている。その他の実施形態が利用され、本開示の範囲から逸脱することなく、開示された実施形態に対する変更がなされうる。以下の詳細記載は、限定する意味でなされているのではなく、本発明の範囲は、特許請求の範囲によってのみ定義される。
【００２９】
本明細書に記載された特徴および態様は、接続設定の再認証処理中における速い設定時間のためのデバイスおよび方法を提供する。例えば、記載された技術によって、モバイル・デバイス（例えば、局（ＳＴＡ））は、先ずビーコンを求めてリスンすることも、または、アクセス・ポイントからのプローブ応答を要求することもなく、アクセス・ポイント（ＡＰ）に関するリンク設定を実行できるようになりうる。ビーコンまたはプローブ応答は、一般に、リンク設定中に用いられるべきアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を含みうる。したがって、記載された技術によって、ＳＴＡは、以前に受信したＡＮｏｎｃｅを有することなく、リンク設定を実行できるようになりうる。「修正４方式ハンド

シェイク」技術にしたがって、ＳＴＡは、保護されていない関連付け要求をＡＰへ送信し、関連付け応答で、ＡＴからＡＮｏｎｃｅを受信しうる。受信されたＡＮｏｎｃｅは、その後、鍵導出のために用いられうる。「次のＡＮｏｎｃｅ」技術にしたがって、ＳＴＡは、第１のＡＮｏｎｃｅを用いて開始された第１のリンク設定中に、第１のリンク設定に後続する第２のリンク設定において用いるための第２のＡＮｏｎｃｅを受信しうる。

【００３０】

記載された技術はまた、上部レイヤ・シグナリング保護のためのテンポラリ鍵の使用をも可能にしうる。例えば、ＳＴＡは、保護されていない関連付け要求を送信する代わりに、ビーコンまたはプローブ応答によって、ＡＰから第１のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ１）を受信し、第１のＡＮｏｎｃｅに基づいて第１の鍵（例えば、第１のペアワイズ・トランジェント鍵（ＰＴＫ））を導出しうる。第１の鍵は、ＳＴＡによってＡＰへ送信された関連付け要求を保護するために用いられうる。この関連付け要求を受信することに応じて、ＡＰは、第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ２）を生成し、第２のＡＮｏｎｃｅに基づいて、第２の鍵（例えば、第２のＰＴＫ）を導出しうる。ＡＰは、ＳＴＡへ関連付け応答を送信しうる。関連付け応答は、第２のＡＮｏｎｃｅを含んでおり、第２の鍵を用いて保護される。ＳＴＡは、第２のＡＮｏｎｃｅに基づいて第２の鍵を導出し、この第２の鍵を用いて、関連付け応答を処理し、リンク設定を完了する。第２の鍵はまた、ＳＴＡとＡＰとの間で通信される、後続するメッセージ（例えば、データ・メッセージ）を保護するためにも用いられうる。

【００３１】

あるいは、ＳＴＡは、ビーコンまたはプローブ応答によってＡＰからＡＮｏｎｃｅを受信するのではなく、ビーコンまたはプローブ応答でＡＮｏｎｃｅシードを受信しうる。ＡＮｏｎｃｅシードは、ＡＰによって頻繁に更新される暗号シード値でありうる。ＳＴＡは、ＡＮｏｎｃｅシードを、ＳＴＡの媒体アクセス制御（ＭＡＣ）アドレスを用いてハッシュすることによって、ＡＮｏｎｃｅを生成しうる。したがって、ビーコン・メッセージによって複数のＳＴＡへブロードキャストされるＡＮｏｎｃｅとは異なり、ＡＮｏｎｃｅシードおよびＳＴＡのＭＡＣアドレスに基づいてＳＴＡにおいて生成されるＡＮｏｎｃｅは、ＳＴＡにユニークでありうる。生成されたＡＮｏｎｃｅは、ＡＰとのリンク設定を開始するためにＳＴＡによって用いられうる。ＡＰは、リンク設定中、ＳＴＡからのリンク設定メッセージ（例えば、関連付け要求）に含まれうるＳＴＡのＭＡＣアドレスおよびＡＮｏｎｃｅシードに基づいて、ＡＮｏｎｃｅを生成しうる。その他のハンドシェイク技術とは対照的に、この技術は、ＡＰの前にＳＴＡがＡＮｏｎｃｅを生成することを含みうる。有利なことに、ＡＮｏｎｃｅは、ＳＴＡにユニークでありうり、「クリアに」（すなわち、暗号化されずに）送信されうる。そして、ＡＰによる送信前に、許可されていないデバイスによって予測可能ではないことがありうる。

【００３２】

特定の実施形態では、方法は、保護されていない関連付け要求を、モバイル・デバイスからアクセス・ポイントへ送信することを含む。この方法はまた、アクセス・ポイントから関連付け応答を受信することを含む。関連付け応答は、ＡＮｏｎｃｅを含む。この方法は、モバイル・デバイスにおいて、ＡＮｏｎｃｅを用いてペアワイズ・トランジェント鍵（ＰＴＫ）を生成することを含む。

【００３３】

別の特定の実施形態では、装置は、プロセッサとメモリとを含む。このメモリは、保護されていない関連付け要求をアクセス・ポイントへ送信し、アクセス・ポイントから、関連付け応答を受信するために、プロセッサによって実行可能な命令群を格納している。関連付け応答は、ＡＮｏｎｃｅを含む。これら命令群はまた、ＡＮｏｎｃｅを用いてＰＴＫを生成するためにプロセッサによって実行可能である。

【００３４】

別の特定の実施形態では、方法は、保護されていない関連付け要求を、アクセス・ポイントにおいて、モバイル・デバイスから受信することを含む。この方法はまた、保護され

ていない関連付け要求から開始メッセージを抽出することと、開始メッセージを、認証サーバへ送信することと、を含む。この方法はさらに、認証サーバから回答メッセージを受信することを含む。回答メッセージは、再認証マスタ・セッション鍵（ｒＭＳＫ）を含む。この方法は、ＡＮｏｎｃｅを生成することと、関連付け応答をモバイル・デバイスへ送信することとを含む。関連付け応答は、ＡＮｏｎｃｅを含む。

【００３５】

別の特定の実施形態では、装置は、プロセッサとメモリとを含む。メモリは、保護されていない関連付け要求をモバイル・デバイスから受信するためにプロセッサによって実行可能な命令群を格納している。これら命令群はまた、保護されていない関連付け要求から開始メッセージを抽出し、開始メッセージを認証サーバへ送信するためにプロセッサによって実行可能である。これら命令群はさらに、認証サーバから回答メッセージを受信するためにプロセッサによって実行可能である。回答メッセージは、ｒＭＳＫを含む。これら命令群は、ＡＮｏｎｃｅを生成するため、および、モバイル・デバイスへ関連付け応答を送信するためにプロセッサによって実行可能である。関連付け応答は、ＡＮｏｎｃｅを含む。

【００３６】

別の特定の実施形態では、方法は、モバイル・デバイスにおいて、第１のＡＮｏｎｃｅを用いて、アクセス・ポイントとの第１のリンク設定を開始することを含む。この方法はまた、アクセス・ポイントとの第１のリンク設定中、第１のリンク設定に後続する、アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信することを含む。第２のＡＮｏｎｃｅは、第１のＡＮｏｎｃｅとは異なる。

【００３７】

別の特定の実施形態では、装置は、プロセッサとメモリとを含む。メモリは、第１のＡＮｏｎｃｅを用いて、アクセス・ポイントとの第１のリンク設定を開始するために、プロセッサによって実行可能な命令群を格納する。これら命令群はまた、アクセス・ポイントとの第１のリンク設定中、第１のリンク設定に後続する、アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信するためにプロセッサによって実行可能である。第２のＡＮｏｎｃｅは、第１のＡＮｏｎｃｅとは異なる。

【００３８】

別の特定の実施形態では、第１のリンク設定に後続する、モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを、第１のＡＮｏｎｃｅを用いる第１のリンク設定中に、アクセス・ポイントからモバイル・デバイスへ送信することを含む。第２のＡＮｏｎｃｅは、第１のＡＮｏｎｃｅとは異なる。

【００３９】

別の特定の実施形態では、装置は、プロセッサとメモリとを含む。メモリは、第１のリンク設定に後続する、モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを、第１のＡＮｏｎｃｅを用いる第１のリンク設定中に、モバイル・デバイスへ送信するためにプロセッサによって実行可能である。第２のＡＮｏｎｃｅは、第１のＡＮｏｎｃｅとは異なる。

【００４０】

別の特定の実施形態では、方法は、モバイル・デバイスにおいて、アクセス・ポイントから第１のＡＮｏｎｃｅを受信することを含む。この方法はまた、第１のＡＮｏｎｃｅを用いて第１のＰＴＫを生成することを含む。この方法はさらに、関連付け要求をアクセス・ポイントへ送信することを含む。関連付け要求は、ＳＮｏｎｃｅを含んでおり、第１のＰＴＫを用いて保護されている。この方法は、アクセス・ポイントから関連付け応答を受信することを含む。関連付け応答は、第２のＡＮｏｎｃｅを含んでおり、第２のＰＴＫを用いて保護されている。この方法はまた、第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅを用いて第２のＰＴＫを生成することを含む。この方法はさらに、アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために、第２のＰＴＫを用いることを含む。

【００４１】
別の特定の実施形態では、装置は、プロセッサとメモリとを含む。メモリは、モバイル・デバイスへ送信されるべきＡＮｏｎｃｅシードを、アクセス・ポイントにおいて生成するためにプロセッサによって実行可能な命令群を格納する。これら命令群はまた、モバイル・デバイスから受信されたモバイル・デバイスのＭＡＣアドレスおよびＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを生成するためにプロセッサによって実行可能である。これら命令群はさらに、生成されたＡＮｏｎｃｅに基づいて、モバイル・デバイスとのリンク設定を実行するためにプロセッサによって実行可能である。
【００４２】
例えば８０２．１１（ＷｉＦｉ）ネットワークのような無線ネットワークでは、モバイル・ユーザは、１つのネットワークから別のネットワークへ移動しうる。いくつかの場合には、これらネットワークは、同じネットワーク・キャリアまたはエンティティによって管理されうる。
【００４３】
このような用途の場合のいくつかの限定しない例を以下に示す。
１．ホット・スポット・パス・スルー
（Ａ）ユーザは、（いくつかの、オーバラップしない）公的にアクセス可能なＷｉＦｉホット・スポット（例えば、コーヒー・ショップまたはその他の公共的な場所）を通過しうる。接続を有している間、ユーザ端末は、例えば、電子メール、ソーシャル・ネットワーキング・メッセージ等のような情報をアップロードおよびダウンロードしうる。別の例は、ＷｉＦｉアクセス・ポイントを備えた多くの列車駅を通過する列車に乗った乗客である。
２．列車
（Ｂ）ユーザは、ＷｉＦｉサービスがローカル・アクセス・ポイント（ＡＰ）を介して顧客に提供される列車に乗車しうる。このＡＰは、トラック側インフラストラクチャに接続するために、無線の８０２．１１ベースのバックボーンを用いうる。トラックに沿った連続的な有効通信範囲を提供するために、指向性アンテナが用いられうる。
３．運転中の料金／重量検査所
（Ｃ）料金所を通り抜けるか、または、重量検査所を通過する、高速道路上の車両は、料金所または重量検査所において、ＡＰにアクセスすることが可能でありうる。運転中（または重量がかけられている間）、例えば、貨物情報の交換または料金を顧客に課すことのような情報が提供されうる。
【００４４】
これらオーバラップしていないが関連する接続のためのアプリケーションをイネーブルすることは、安全なリンクを確立するために、標準的なＩＰプロトコル・スイートに依存し、根本となる無線技術を潜在的に信頼しうる。
【００４５】
インターネット・プロトコル（ＩＰ）接続の設定のためのいくつかの提案されたシステムでは、ビーコンの受信後、アクセス端末のための安全なリンクを確立するために、往復１６回の交換（アクセス端末へ、および、アクセス端末からの３２のメッセージ）が存在しうる。
【００４６】
本明細書に記載された提案されたシステムの選択された実施形態では、高速なリンク設定が実行されうる。ここでは、ビーコンの受信後に、ＩＰ接続および安全なリンクを設定するためのメッセージの数が、以前の往復１６回の交換（３２のメッセージ）から、往復１回の交換（２つのメッセージ）へ低減される。拡張可能認証プロトコル／再認証プロトコル（ＥＡＰ／ＥＲＰ：Extensible Authentication Protocol/Re-authentication Protocol）が、高速なリンク設定の一部として用いられうる。
【００４７】
図１は、１または複数の端末と、アクセス・ポイントとの間でデータを通信するための

無線ネットワーク構成の例を例示する概念図である。図１のネットワーク構成１００は、１または複数の端末と、アクセス・ポイントとの間でデータを通信するために用いられうる。ネットワーク構成１００は、ネットワーク１０４に接続されたアクセス・ポイント１０２を含んでいる。アクセス・ポイント１０２は、例えば（ここでは、局（ＳＴＡ）およびアクセス端末（ＡＴ）１０６，１０８，１１０とも称されうる）無線デバイスのようなさまざまな通信デバイスへ無線通信を提供するように構成されうる。限定しない例として、アクセス・ポイント１０２は、基地局でありうる。限定しない例として、局／端末１０６，１０８，１１０は、パーソナル・コンピュータ（ＰＣ）、ラップトップ・コンピュータ、タブレット・コンピュータ、モバイル電話、携帯情報端末（ＰＤＡ）、および／または、データを無線で送信および／または受信するように構成された任意のデバイス、または、これら任意の組み合わせでありうる。ネットワーク１０４は、例えば、送信制御プロトコル／インターネット・プロトコル（ＴＣＰ／ＩＰ）ネットワークのような分散型コンピュータ・ネットワークを含みうる。

【００４８】

アクセス・ポイント１０２は、限定される訳ではないが、ワイヤレス・フィデリティ（ＷｉＦｉ）サービス、ワールドワイド・インタオペラビリティ・フォー・マイクロウェーブ・アクセス（ＷｉＭＡＸ）サービス、および無線セッション開始プロトコル（ＳＩＰ）サービスを含むさまざまな無線通信サービスを提供するように構成されうる。局／端末１０６，１０８，１１０は、（限定される訳ではないが、電気電子学会（ＩＥＥＥ）によって開発された８０２．１１、８０２．１１－２００７、および８０２．１１ｘ仕様ファミリに準拠した通信を含む）無線通信のために構成されうる。さらに、局／端末１０６，１０８，１１０は、アクセス・ポイント１０２へデータを送信し、アクセス・ポイント１０２からデータを受信するように構成されうる。

【００４９】

図２は、典型的な局／端末２００を例示するブロック図である。プロセッサ２１０（例えば、デジタル信号プロセッサ（ＤＳＰ））は、プロセッサ２１０における実行のための命令群２６０および送信を処理するためのデータのような情報を格納するためのメモリ２３２に接続されている。これら命令群は、本明細書に記載されるように、局／端末のさまざまな方法および機能を実行するためにプロセッサ２１０によって実行可能でありうる。さらに、アクセス・ポイント（ＡＰ）、認証サーバ（ＡＳ）、およびダイナミック・ホスト・コンフィギュレーション・プロトコル（ＤＨＣＰ）サーバも同様に、プロセッサおよびメモリを含みうる。メモリは、本明細書で記載されたように、ＡＰ、ＡＳ、およびＤＨＣＰサーバそれぞれのさまざまな方法および機能を実行するためにプロセッサによって実行可能な命令群を格納している。

【００５０】

ディスプレイ・コントローラ２２６は、プロセッサ２１０およびディスプレイ・デバイス２２８へ接続されうる。コーダ／デコーダ（ＣＯＤＥＣ）２３４も、プロセッサ２１０に接続されうる。ユーザ・インタフェース・デバイスの限定しない例として、スピーカ２３６およびマイクロホン２３８が、ＣＯＤＥＣ２３４に接続されうる。無線コントローラ２４０が、プロセッサ２１０およびアンテナ２４２に接続されうる。特定の例では、プロセッサ２１０、ディスプレイ・コントローラ２２６、メモリ２３２、ＣＯＤＥＣ２３４、および無線コントローラ２４０は、システム・イン・パッケージまたはシステム・オン・チップ・デバイス２２２に含まれうる。特定の例では、入力デバイス２３０および電源２４４が、システム・オン・チップ・デバイス２２２に接続されうる。さらに、特定の例では、例示されるように、ディスプレイ・デバイス２２８、入力デバイス２３０、スピーカ２３６、マイクロホン２３８、アンテナ２４２、および電源２４４は、システム・オン・チップ・デバイス２２２の外側にありうる。しかしながら、ディスプレイ・デバイス２２８、入力デバイス２３０、スピーカ２３６、マイクロホン２３８、無線アンテナ２４２、および電源２４４の各々は、インタフェースまたはコントローラのようなシステム・オン・チップ・デバイス２２２の構成要素に接続されうる。

【００５１】
図３は、従来の接続設定において実行されうるメッセージングを例示するフロー図である。局／端末３０２とアクセス・ポイント３０４の間に示されているメッセージは、プローブと認証要求とを含みうる。拡張可能認証プロトコル(ＥＡＰ：Extensible Authentication Protocol) オーバ・ローカル・エリア・ネットワーク(ＬＡＮ)（ＥＡＰＯＬ）処理は、識別フェーズ、保護ＥＡＰ（ＰＥＡＰ）フェーズ、およびＥＡＰ－マイクロソフト・チャレンジ・ハンドシェイク認証プロトコル（ＥＡＰ－ＭＳＣＨＡＰｖ２）を開始および含みうる。ＥＡＰが成功すると、ＥＡＰＯＬ鍵が確立されうる。したがって、リンク設定および認証を確立するために、少なくとも１６のメッセージが、局／端末３０２へ通信されうるか、または、局／端末３０２から通信されうる。

【００５２】
本明細書に記載された提案されたシステムの特定の実施形態では、（ビーコン受信後）ＩＰ接続を設定するためのメッセージの数が、（１６のメッセージから）２つのメッセージへ低減される。拡張可能認証プロトコル再認証プロトコル（ＥＲＰ）は、図１２および１３に関して以下により十分に記載されているような再認証の一部として使用され、以下の最適化を含みうる。局／端末（ＳＴＡ）３０２は、フルなＥＡＰ認証を実行すると、その後、高速な初期リンク設定のためのＥＲＰ高速再認証を用いて、ＥＡＰ認証を維持する。

【００５３】
関連付け要求を送信する前に、ネットワークからのチャレンジを取得することなく、再認証マスタ・セッション鍵（ｒＭＳＫ）が局／端末３０２によって生成される。ｒＭＳＫから、局（ＳＴＡ）３０２によって、ペアワイズ・トランジェント鍵（ＰＴＫ）が生成される。ペアワイズ・トランジェント鍵（ＰＴＫ）は、鍵確認鍵（ＫＣＫ）、鍵暗号鍵（ＫＥＫ）、およびトランジェント鍵（ＴＫ）を含む。

【００５４】
この関連付け要求は、局３０２によって送信され、ＥＡＰ再認証要求を、ダイナミック・ホスト・コンフィギュレーション・プロトコル（ＤＨＣＰ）－Ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－Ｒａｐｉｄ－Ｃｏｍｍｉｔと、ＳＮｏｎｃｅとバンドルする（例えば、ＳＮｏｎｃｅは、局３０２によってピック・アップされる。すなわち、局ノンス）。バンドルされたメッセージは、１または複数の情報要素（ＩＥ）として含まれうる。ＥＡＰ再認可要求は、再認証保全鍵（ｒＩＫ）を用いて認証サーバ（Ａｕｔｈサーバ）３０８によって認証される。ＤＨＣＰ－Ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－Ｒａｐｉｄ－Ｃｏｍｍｉｔ と、ＳＮｏｎｃｅとは、再認証マスタ・セッション鍵（ｒＭＳＫ）を用いて、または、ｒＭＳＫから導出されたペアワイズ・トランジェント鍵（ＰＴＫ）を用いて保護される。ＤＨＣＰ－Ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－Ｒａｐｉｄ－Ｃｏｍｍｉｔが暗号化され、ＭＩＣ（メッセージ保全符号）化されるか、または、暗号化されずにＭＩＣ化される。本明細書に記載された例のいくつかは、効率的な再認証概念を例示するために、発見要求（例えば、Ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－Ｒａｐｉｄ－Ｃｏｍｍｉｔ）を利用するが、ＩＰアドレスを割り当てるために（プロトコル・スタックの）上部レイヤにおいて用いられる任意のメッセージが、代わりに用いられうることが理解されるべきである。

【００５５】
ＤＨＣＰメッセージが暗号化されているのであれば、アクセス・ポイント３０４は、ＥＡＰ再認証要求が認証サーバ３０８によって検証されるまで、Ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－Ｒａｐｉｄ－Ｃｏｍｍｉｔメッセージとを保持しうる。メッセージを検証にするために、アクセス・ポイント（ＡＰ）３０４は、認証サーバ３０８からｒＭＳＫを受信し、ペアワイズ・トランジェント鍵（ＰＴＫ）を導出するまで待つ。認証サーバ３０８から取得したｒＭＳＫに基づいて、アクセス・ポイント３０４は、ＭＩＣ（メッセージ保全符号）のために用いられるのみならず、メッセージを解読するためにも用いられるＰＴＫを導出する。

【００５６】

ＤＨＣＰメッセージが暗号化されていないのであれば、アクセス・ポイント３０４は、多くのケースにおいて、メッセージが、正しいデバイスから到来したとの予測の下、Ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－Ｒａｐｉｄ－ＣｏｍｍｉｔをＤＨＣＰサーバへ転送しうる（が、ＥＡＰ再認証要求が認証サーバ３０８によって検証されるまでＳＮｏｎｃｅメッセージを保持する）。アクセス・ポイント３０４は、Ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－Ｒａｐｉｄ－ＣｏｍｍｉｔがＤＨＣＰサーバへ送信されても、認証サーバ３０８から取得されたｒＭＳＫに基づいてＤＨＣＰディスカバ・メッセージを有効にし、ＰＴＫを導出するまで、ＤＨＣＰアクノレッジを保持するだろう。

【００５７】

その後、アクセス・ポイント（ＡＰ）３０４は、ＰＴＫで保護されたＧＴＫ／ＩＧＴＫ＋ＤＣＨＰアクノレッジを送信する。言い換えれば、ＤＨＣＰアクノレッジが暗号化され、メッセージ保全性が保護される。

【００５８】

限定しない態様は、リンク設定および認証のための処理における以下のステップのうちの１または複数を含みうる。

【００５９】

第１に、ユーザは、局／端末３０２を取得し、特定のネットワーク（例えば、特定のＷｉＦｉネットワーク）との初期設定の一部として、フルＥＰＡ認証を実行しうる。限定しない例として、恐らく、例えば１年のような特定の認証期間、フルＥＰＡ認証が維持されうる。

【００６０】

第２に、認証期間中、ユーザは、（いくつかの、オーバラップしない）公的にアクセス可能なＷｉＦｉホット・スポット（例えば、コーヒー・ショップおよびその他の公共的な場所）を通り過ぎる。言い換えれば、このステップは、認証期間中に、複数回、かつ、設定ネットワークの一部である複数のアクセス・ポイント３０４と実行されうる。局／端末３０２は、ＥＲＰを用いてネットワークと高速初期リンク設定（ＦＩＬＳ：Fast Initial Link Setup）を実行するだろう。関連付け要求メッセージを用いてＥＲＰをＤＨＣＰ-Ｒａｐｉｄ－Ｄｉｓｃｏｖｅｒｙとバンドルすることは、以下により詳しく説明されるように、関連付け要求のためのシグナリングを、１往復に減少させるだろう。認証期間中、ユーザの局／端末３０２は、ネットワークと接続している場合に、高速初期リンク設定（ＦＩＬＳ）を求めてＥＲＰを実行し続けうる。

【００６１】

第３に、認証期間アプローチが終了すると、ユーザは、（例えば、２週間のような）所与の期間内、ネットワークへの「フル・アタッチメント」を実行するように再度警告されうる。この期間中、ユーザは、早期のフルＥＡＰ認証が終了するまで、または、フル・アタッチメントが実行されるまで、早期のフルＥＡＰ認証に基づいて、高速認証を用いることが可能であり続けるだろう。フル・アタッチメント通知は、ネットワークから発行されうるか、または、局／端末３０２においてローカルに設定されうる。

【００６２】

第４に、ユーザが、フル・アタッチメントを実行しないのであれば、１年後に、ネットワークは、ＥＲＰに失敗し、ステップ１において概説されるように、別の年のために、フルＥＡＰ認証を開始するだろう。

【００６３】

図４－１１は、２つのメッセージ・リンク設定および認証を実行するためのさまざまな別のシナリオを例示する。

【００６４】

図４は、クライアント局のための効率的なリンク設定および認証を実行する第１の例を例示するフロー図である。ステップ０ａおよび０ｂでは、局／端末（ＳＴＡ）３０２は、第１のアクセス・ポイントＡＰ１　３０４Ａに通信可能に接続されている間、フルＥＡＰ認証を実行しうる。局／端末３０２は、第２のアクセス・ポイントＡＰ２　３０４Ｂに接

近し（ステップ１）、そのビーコンを検出する（ステップ２）と、第２のアクセス・ポイントＡＰ２　３０４Ｂを介して、自己を再認証するように努めうる。この処理では、アクセス・ポイント３０４Ｂは、高速初期リンク設定（ＦＩＬＳ）のための能力インジケータを含むビーコン／プローブを送信する。能力インジケータは、バンドルされたＥＲＰおよびＤＣＨＰ－Ｒａｐｉｄ－Ｄｉｓｃｏｖｅｒｙを伴う関連付け要求を取り扱うための能力を示しうる。ステップ３では、局／端末３０２は、関連付け要求を送信する前に、ＥＲＰを用いて、再認証マスタ・セッション鍵（ｒＭＳＫ）（図１３参照）を生成する。ここで、

ｒＭＳＫ＝ＫＤＦ（Ｋ、Ｓ）；

Ｋ＝ｒＲＫ；および、

Ｓ＝ｒＭＳＫ　ｌａｂｅｌ　｜“＼０”｜ＳＥＱ｜　ｌｅｎｇｔｈ

である。

【００６５】

局／端末３０２は、１または複数のメッセージを、関連付け要求の情報要素（ＩＥ）（または、パラメータ／ペイロード）としてパックする。例えば、このような関連付け要求は、１）ＥＡＰ再認証開始（ｒＩＫを用いたメッセージ保全）；２）ＤＨＣＰ－Ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－Ｒａｐｉｄ－Ｃｏｍｍｉｔ（ＫＣＫ／ＫＥＫを用いた暗号化＆メッセージ保全）；および／または、３）ＥＡＰＯＬ鍵（ＳＮｏｎｃｅ，ＡＮｏｎｃｅ）（ＫＣＫを用いたメッセージ保全）を含みうる。ＥＡＰＯＬ鍵は、フレーム全体またはサブセットとして構成されうる。ＡＮｏｎｃｅ（すなわち、アクセス・ポイント・ノンス）は、局／端末３０２によって選択され、アクセス・ポイントＡＰ２　３０４Ｂへ送信されうる。アクセス・ポイント（ＡＰ２）３０４Ｂは、局／端末３０２が、例えば、過去の数秒／ミリ秒で送信されたＡＮｏｎｃｅ（例えば、ＡＰ２のため、ビーコンから取得された最近のＡＮｏｎｃｅ）を用いていることを保証しうる。アクセス・ポイントＡＰ２　３０４Ｂは、認証サーバ３０８からルート・マスタ・セッション鍵（ｒＭＳＫ）を受信するまで、ＤＨＣＰ＆ＥＡＰＯＬ鍵メッセージを保持する。アクセス・ポイントＡＰ２　３０４Ｂは、ｒＭＳＫからＰＴＫを生成する。アクセス・ポイントＡＰ２　３０４Ｂは、ＤＨＣＰ＆ＥＡＰＯＬ鍵メッセージのためのメッセージ保全符号（ＭＩＣ）交換を実行し、ＤＨＣＰを解読する。アクセス・ポイントＡＰ２　３０４Ｂは、ＫＣＫ／ＫＥＫを導出するためにｒＭＳＫを用い、ＤＨＣＰアクノレッジとＥＡＰＯＬ鍵メッセージとを、局／端末３０２へ送信する前に保護する。

【００６６】

さまざまな例において、ＡＮｏｎｃｅは、局がパッシブ・スキャンを用いることを可能にするビーコンを用いて、または、アクティブ・スキャンが用いられる場合、プローブ応答メッセージで、ＡＰ２　３０４Ｂによって送信されうる。ビーコンを用いてＡＮｏｎｃｅがＡＰ２　３０４Ｂによって送信される場合、ＡＮｏｎｃｅは、ビーコン毎に、または、複数のビーコンにおいて変更されうる。局３０２は、局３０２からＡＰ２　３０４Ｂへ送信される関連付け要求メッセージに、局３０２によって取得されたＡＮｏｎｃｅを含めうる。

【００６７】

図５は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。この処理は、オプション１ａと称されうる。図５において実行される処理は、関連付け要求メッセージにカプセル化されたＤＨＣＰ発見メッセージおよびＥＡＰＯＬ鍵メッセージを認証するために（ＰＴＫのＫＣＫ／ＫＥＫの代わりに）ｒＭＳＫが用いられることを除いて、図４（オプション１）で実行されるものに類似している。

【００６８】

図６は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。この処理はオプション１ｂと称されうる。図６において実行される処理は、次のようなありうる相違点を除いて、図４（オプション１）で実行されるも

のに類似している。図６に図示されるステップ２では、アクセス・ポイント３０４は、ＤＨＣＰ要求が暗号化されうるという能力を通知しうる。図６に図示されるステップ４では、局／端末３０２は、ＤＨＣＰメッセージが暗号化されるべきであるか否かを決定しうる。例えば、ＤＣＨＰ発見要求が、何らかのプライベート情報等を含んでいるのであれば、いくつかの要因が、局／端末３０２によって考慮されうる。局／端末が、ＤＨＣＰ発見要求を暗号化すると決定すると、アクセス・ポイント３０４は、（図４および５に図示されるように）このメッセージを保持しうる。

【００６９】

局／端末が、ＤＨＣＰ発見要求を暗号化しないと決定すると、以下のステップが実行されうる。図６に図示されるステップ４では、ＤＨＣＰ発見要求情報要素（ＩＥ）またはパラメータは、メッセージ保全性のみが保護される。ステップＳ４に基づいて、アクセス・ポイント３０４は、ＥＡＰ再認証開始要求に対する応答（ステップ９）を待つことなく、ＤＨＣＰ－Ｄｉｓｃｏｖｅｒ－Ｒａｐｉｄ－Ｃｏｍｍｉｔを送信する（ステップ６）。この処理によって、ＥＡＰ再認証手順と並行して、ＩＰアドレス割当がなされる。図６に図示されるステップ７ａでは、アクセス・ポイントは、ＤＨＣＰサーバから到来したＤＨＣＰアクノレッジを、ＤＨＣＰ発見が検証されるステップ１０ｂまで保持する。メッセージ保全に失敗すると、アクセス・ポイント３０４は、ＤＨＣＰアクノレッジを用いて、割り当てられたＩＰアドレスを削除するための手順を開始する。

【００７０】

図７は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。この処理は、オプション２と称されうる。図７において実行される処理は、次のようなありうる相違点を除いて、図４（オプション１）で実行されるものに類似している。ＤＨＣＰメッセージとＥＡＰＯＬ鍵メッセージとを独立して認証する代わりに、ＥＡＰ再認証、ＤＨＣＰ発見、およびＥＡＰＯＬ鍵を含む結合されたペイロードが、ＫＣＫ／ＫＥＫを用いて認証されうる。アクセス・ポイント３０４は、ＥＡＰ再認証開始メッセージを抽出し、ＫＣＫ／ＫＥＫを用いて認証されたメッセージ全体を検証することなく認証サーバ３０８へ転送する。アクセス・ポイント３０４は、認証サーバ３０８からｒＭＳＫを受信した後、メッセージ全体を認証する。

【００７１】

図８は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。この処理は、オプション２ａと称されうる。図８において実行される処理は、次のようなありうる相違点を除いて、図５（オプション１ａ）で実行されるものに類似している。ＤＨＣＰメッセージとＥＡＰＯＬ鍵メッセージとを独立して認証する代わりに、ＥＡＰ再認証、ＤＨＣＰ発見、およびＥＡＰＯＬ鍵とを含む結合されたペイロードが、ｒＭＳＫを用いて認証されうる。アクセス・ポイント３０４は、ＥＡＰ再認証開始メッセージを抽出し、ｒＭＳＫを用いて認証されたメッセージ全体を検証することなく認証サーバ３０８へ転送する。アクセス・ポイント３０４は、認証サーバ３０８からｒＭＳＫを受信した後、メッセージ全体を認証する。ＤＨＣＰ発見メッセージ（ステップ９）が、ステップ５の前に送信されうる。このケースでは、認証が成功しなかったのであれば、割り当てられたＩＰアドレスは無視される。

【００７２】

図９は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。この処理は、オプション２ｂと称されうる。図９において実行される処理は、次のようなありうる相違点を除いて、図４で実行されるものに類似している。ステップ２では、アクセス・ポイントは、ＤＨＣＰ要求が暗号化されうるとの能力を通知しうる。ステップ４では、局／端末３０２は、ＤＨＣＰメッセージが暗号化されるべきか否かを決定する。例えば、ＤＣＨＰ発見要求が、何らかのプライベート情報等を含んでいるのであれば、いくつかの要因が、局／端末３０２によって考慮されうる。局／端末３０２が、ＤＨＣＰ発見要求を暗号化すると決定すると、アクセス・ポイント３０４は、オプション２およびオプション２ａにおいて前述したようにメッセージを保持しうる。局

／端末３０２が、ＤＨＣＰ発見要求を暗号化しないことを決定すると、以下のステップが実行されうる。ステップ４では、メッセージ保全性のみが保護される。ステップＳ４に基づいて、アクセス・ポイント３０４は、ＥＡＰ再認証開始要求に対する応答（ステップ９）を待つことなく、ＤＨＣＰ－Ｄｉｓｃｏｖｅｒ－Ｗｉｔｈ－Ｒａｐｉｄ－Ｃｏｍｍｉｔを送信する（ステップ６）。この処理によって、ＥＡＰ再認証手順と並行して、ＩＰアドレス割当がなされる。ステップ７ａでは、アクセス・ポイント３０４は、ＤＨＣＰサーバから到来したＤＨＣＰアクノレッジを、ＤＨＣＰ発見が検証されるステップ１０ｂまで保持する。メッセージ保全に失敗すると、アクセス・ポイント３０４は、ＤＨＣＰアクノレッジ・メッセージを用いて、割り当てられたＩＰアドレスを削除するための手順を開始する。

【００７３】

図１０は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。この処理は、オプション３と称されうる。図１０において実行される処理は、次のようなありうる相違点を除いて、図４および５（オプション１および１ａ）で実行されるものに類似している。ＡＮｏｎｃｅは、「インストールＰＴＫ，ＧＴＫ，ＩＧＴＫ」メッセージとともに関連付け応答で送信されうる。図１０におけるステップ９および１１は、オプション１ｂおよびオプション２ｂに記載されるようなステップ５－７と並行して実行されうる。

【００７４】

オプション４はまた、次のようなありうる相違点を除いて、オプション１および２から導出されうる。関連付け要求は、ステップ４における単一のメッセージ（すなわち、関連付け要求）ではなく、メッセージ１（Ｍ１）として分離されうる。メッセージ１（Ｍ１）は、ＤＨＣＰ発見メッセージおよびメッセージ２（Ｍ２）をカプセル化し、メッセージ２（Ｍ２）は、ＥＡＰ再認証開始メッセージおよびＳＮｏｎｃｅをカプセル化する。アクセス・ポイント３０４は、ＥＡＰＯＬ鍵を受信するまで、ＤＨＣＰ発見メッセージに作用しないだろう。これら２つのメッセージ（Ｍ１＆Ｍ２）は、ＳＩＦＳ期間によって分離されうる。このオプション４は、ＥＡＰＯＬ構造が再使用されうるという利点を有しうる。

【００７５】

図１１は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。この処理は、オプション５と称されうる。図１１において実行される処理は、次のようなありうる相違点を除いて、図４（オプション１）で実行されるものに類似している。アクセス・ポイント３０４は、ビーコン／プローブ応答を送信する。これは、同時ＥＲＰおよび／またはＩＰアドレス割当のための高速初期リンク設定（ＦＩＬＳ）能力インジケータを含む。このシナリオでは、アクセス・ポイント３０４によって割り当てられたＩＰアドレスのリース・タイマは終了しない。局／端末３０２は、このＩＰアドレスを使用し続けることができるか否かを確認するために、第２のアクセス・ポイント３０４に送信されたＤＨＣＰ要求において、第１のアクセス・ポイント３０４Ａによって割り当てられたＩＰアドレスを用いる。ＩＰアドレスが終了すると、ＤＨＣＰサーバ３０６は、ＤＨＣＰ－ＮＡＫを送信する。

【００７６】

図１２は、再認証プロトコル中に実行されうるメッセージングを例示するフロー図である。局／端末３０２は、初めてネットワークにアタッチした時に、認証サーバ３０８とのフルＥＡＰ交換を実行する。その結果、マスタ・セッション・キー（ＭＳＫ）が、ＥＡＰ認証部に配信される。その後、必要に応じて、トランジェント・セッション鍵（ＴＳＫ）を確立するために、マスタ・セッション鍵（ＭＳＫ）が認証部および局／端末３０２によって用いられる。局／端末３０２および認証サーバ３０８はまた、最初のＥＡＰ交換時に、ＥＭＳＫを導出する。これは、再認証ルート鍵（ｒＲＫ）を導出するために用いられる。さらに詳しくは、再認証ルート鍵（ｒＲＫ）が、拡張ＭＳＫ（ＥＭＳＫ）から、または、ドメイン特有ルート鍵（ＤＳＲＫ）から導出されうる。ドメイン特有ルート鍵（ＤＳＲＫ）自身も、ＥＭＳＫから導出される。再認証ルート鍵（ｒＲＫ）は、局／端末３０２と

認証サーバ３０８とに対してのみ利用可能でありうる。そして、一般には、その他の何れのエンティティにも配信されない。さらに、再認証保全鍵（ｒＩＫ）が、再認証ルート鍵（ｒＲＫ）から導出されうる。局／端末３０２および認証サーバ３０８は、ＥＲＰ交換を実行している間、所有の証拠を提供するために、再認証保全鍵（ｒＩＫ）を用いうる。再認証保全鍵（ｒＩＫ）はまた、一般に、その他のどのエンティティへ渡されず、一般には、局／端末３０２と認証サーバ３０８に対してのみ利用可能である。

【００７７】

２つの新たなＥＡＰ符号、すなわち、ＥＡＰ開始およびＥＰＡ終了が、ＥＡＰ再認証のために定義される。局／端末３０２は、ＥＲＰを要求した場合、図１２の下の箱に図示されるように、ＥＲＰ交換を実行する。

【００７８】

図１３は、再認証プロトコルのために用いられうる鍵階層を例示する。マスタ・セッション鍵（ＭＳＫ）が、ルート・キーから導出され、ペアワイズ・マスタ鍵（ＰＭＫ）が、マスタ・セッション鍵（ＭＳＫ）から導出されうる。拡張ＭＳＫ（ＥＭＳＫ）が、ルート鍵から導出されうる。ＥＲＰ交換のために、追加のさまざまな鍵が、拡張ＭＳＫ（ＥＭＳＫ）から導出されうる。ＤＳＲＫ１－ＤＳＲＫｎが導出される。ドメイン特有ルート鍵（ＤＳＲＫ）のおのおのは、ｒＲＫを含みうる。再認証ルート鍵（ｒＲＫ）から、再認証保全鍵（ｒＩＫ）および再認証マスタ・セッション鍵（ｒＭＳＫ１・・・ｒＭＳＫｎ）が導出されうる。ｒＭＳＫのおのおのは、ペアワイズ・マスタ鍵（ＰＭＫ）を含みうる。（鍵確認鍵（ＫＣＫ）、鍵暗号鍵（ＫＥＫ）、およびトランジェント鍵（ＴＫ）を含みうる）ペアワイズ・トランジェント鍵（ＰＴＫ）が、ＰＭＫから導出されうる。

【００７９】

図１４は、再認証要求と上部レイヤ・メッセージ（例えば、発見要求）を生成し、関連付け要求へバンドルするために局／端末において動作可能な典型的な処理１４００を図示するフロー図である。動作ブロック１４０２は、乱数またはノンス（例えば、ＡＮｏｎｃｅ）を含むビーコンが、アクセス端末から受信されたことを示す。動作ブロック１４０４では、端末は、乱数またはノンスを用いて、暗号鍵から、拡張可能な認証プロトコルを備える再認証要求を生成する。動作ブロック１４０６では、端末は、上部レイヤ・メッセージを生成する。例えば、このような上部レイヤ・メッセージは、発見要求、ダイナミック・ホスト・コンフィギュレーション・プロトコル（ＤＨＣＰ）ｄｉｓｃｏｖｅｒ－ｗｉｔｈ－ｒａｐｉｄ－ｃｏｍｍｉｔ要求、および／または、インターネット・プロトコル（ＩＰ）アドレス割当メッセージでありうる。

【００８０】

動作ブロック１４０８において、いくつかの態様では、端末は、以前の認証処理の結果に応じて、再認証マスタ・セッション鍵（ｒＭＳＫ）を生成しうる。動作ブロック１４１０において、いくつかの態様では、端末は、ｒＭＳＫ、乱数（ＡＮｏｎｃｅ）、および／または、ローカルに生成された乱数（ＳＮｏｎｃｅ）から、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成しうる。

【００８１】

動作ブロック１４１２は、いくつかの態様では、端末が、ｒＭＳＫを用いて上部レイヤ・メッセージを暗号化しうることを示す。動作ブロック１４１４は、いくつかの態様では、端末が、ＰＴＫを用いて、または、ＫＣＫとＫＥＫとの組み合わせを用いて、上部レイヤ・メッセージを暗号化しうることを示す。別の態様では、上部レイヤ・メッセージは、解読されうる。

【００８２】

動作ブロック１４１６は、いくつかの態様では、端末は、ＤＨＣＰ発見メッセージをカプセル化する第１のメッセージ、および、ＥＡＰＯＬ再認証開始メッセージをカプセル化する第２のメッセージとして、関連付け要求を生成しうる。

【００８３】

動作ブロック１４１８は、端末が、上部レイヤ・メッセージと再認証要求とを、関連付

け要求としてバンドルすることを示す。動作ブロック１４２０は、いくつかの態様では、端末が、第１のメッセージおよび第２のメッセージを個別に送信しうることを示す。

【００８４】

図１５は、基地局において、局／端末から送信された関連付け要求から再認証要求および上部レイヤ・メッセージを受信し抽出するように動作可能な典型的な処理１５００を図示するフロー図である。動作ブロック１５０２は、いくつかの態様では、アクセス・ポイントが、乱数を生成し、乱数を含むビーコンを送信しうることを示す。

【００８５】

動作ブロック１５０４は、アクセス・ポイントが、上部レイヤ・メッセージと、ともにバンドルされた再認証要求とを含む関連付け要求を端末から受信することを示す。動作ブロック１５０６は、アクセス・ポイントが、関連付け要求から上部レイヤ・メッセージを抽出し、コンフィギュレーション・サーバへ転送することを示す。動作ブロック１５０８は、アクセス・ポイントが、関連付け要求から再認証要求を抽出し、認証サーバへ転送することを示す。

【００８６】

動作ブロック１５１０は、いくつかの態様では、アクセス・ポイントが、認証サーバから暗号鍵を受信しうることを示す。動作ブロック１５１２は、いくつかの態様では、アクセス・ポイントが、暗号鍵、乱数、および、端末から受信した乱数からＰＴＫを生成しうることを示す。動作ブロック１５１４は、いくつかの態様では、アクセス・ポイントが、ＰＴＫ内のＫＣＫとＫＥＫとの組み合わせを用いて、上部レイヤ・メッセージを検証しうる。この組み合わせは、拡張可能認証プロトコル・オーバＬＡＮ（ＥＡＰＯＬ）鍵確認鍵（ＫＣＫ）およびＥＡＰＯＬ鍵暗号鍵（ＫＥＫ）を含む。

【００８７】

図４－１５に関して記述された特定の実施形態は、高速初期リンク設定のための４方式ハンドシェイクを含みうることが注目されるだろう。一般に、４方式ハンドシェイクは、１）ＳＴＡにＡＮｏｎｃｅを送信するＡＰ、２）ＡＰにＳＮｏｎｃｅを送信するＳＴＡ、３）ＳＴＡにＰＴＫを送信するＡＰ、および４）ハンドシェイクの完了を確認するＳＴＡ、を含みうる。

【００８８】

したがって、４方式ハンドシェイクの第１の部分は、ＳＴＡが、アクセス・ポイントとのリンク設定を開始する前に、アクセス・ポイントからのプローブ応答を要求するか、または、ビーコンを求めてリスンすることを含みうる。例えば、ビーコンまたはプローブ応答は、暗号目的および／またはメッセージ保全目的のためにＳＴＡによって用いられるであろうＡＮｏｎｃｅを含みうる。しかしながら、ビーコンを求めてリスンすることは、時間を浪費しうるし、プローブ応答を要求することは、時間及び電力を消費しうる。したがって、ＳＴＡにおける時間および電力は、ＳＴＡが、最初に、アクセス・ポイントからのプローブ応答を要求したり、または、ビーコンを求めてリンスしたりすることなく、リンク設定を実行することを可能にすることによって節約されうる。

【００８９】

図１６は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。特に、図１６は、最初に、アクセス・ポイントからプローブ応答を要求することも、または、ビーコンを求めることもなくリンク設定を可能にする、修正４方式ハンドシェイクを例示する。

【００９０】

図１６において例示された選択されたメッセージおよび動作は、以下の修正を伴って、図４－１１に例示されたメッセージおよび動作に対応しうる。ＳＴＡ３０２は、ステップ２において、ｒＭＳＫおよびＳＮｏｎｃｅを生成し、ステップ３において、保護されていない関連付け要求をＡＰ３０４へ送信しうる。保護されていない関連付け要求は、ＳＮｏｎｃｅを含みうる。図４の実施形態とは対照的に、ＳＴＡ３０２は、ＡＮｏｎｃｅを受信しＰＴＫを導出する前に、これらの動作を実行しうる。ＳＴＡ３０２は、ＡＮｏｎｃｅを

受信しＰＴＫを導出する前に、関連付け要求を送信するので、ＡＰ３０４は、図４に記載されたＡＮｏｎｃｅ有効化を実行することなく、ステップ４において示されるように、関連付け要求のＥＡＰ再認証開始部分を抽出し、ＡＳ３０８へ転送しうる。その代わりに、ＡＰ３０４は、ＳＴＡ３０２のための認証として、ＡＳ３０８が、導出されたｒＭＳＫ（ステップ７）とともに回答メッセージを送信することに依存しうる。

【００９１】

ＡＰ３０４は、ｒＭＳＫを受信した後、ステップ９においてＡＮｏｎｃｅを生成し、ステップ１０ａにおいて、ＡＮｏｎｃｅ、ｒＭＳＫ、およびＳＮｏｎｃｅに基づいてＰＴＫを導出しうる。したがって、ＰＴＫは、ＳＴＡ３０２において導出される前に、ＡＰ３０４において導出されうる。ＡＰ３０４は、ステップ１２において、ＡＮｏｎｃｅを含む関連付け応答を、ＳＴＡ３０２へ送信しうる。この関連付け応答は、ＰＴＫのＫＣＫおよびＫＥＫを用いて保護されている。ＳＴＡ３０２は、ＡＰ３０４から関連付け応答を受信した後、ステップ１２ａにおいて、関連付け応答におけるｒＭＳＫ、ＳＮｏｎｃｅ、およびＡＮｏｎｃｅを用いてＰＴＫを生成しうる。

【００９２】

ＡＰ３０４から送信された関連付け応答（ＡＮｏｎｃｅを含む）は、ＡＮｏｎｃｅを用いて保全保護される。関連付け応答におけるＡＮｏｎｃｅ以外の情報要素もまた暗号化されうる。したがって、関連付け要求においてＳＴＡ３０２から取得されたＳＮｏｎｃｅを用いてＡＴ３０４において生成されたＰＴＫ、ＡＳ３０８から取得されたｒＭＳＫ、および、まだＳＴＡ３０２へ送信されていないローカルに生成されたＡＮｏｎｃｅを用いて、関連付け応答を「事前保護」（すなわち、事前暗号化／事前保全保護）しうる。ＳＴＡ３０２は、関連付け応答を受信すると、関連付け応答からＡＮｏｎｃｅを抽出し、ＰＴＫを生成し、このメッセージの保全保護を有効にする。したがって、ＳＴＡ３０２は、メッセージから取得された鍵に基づいてメッセージを「事後検証」する。このような事前保護および事後検証によって、先ず鍵を確認し、次に、鍵を用いてデータを保護する、従来のハンドシェイク・スキームよりも高速なリンク設定を可能としうる。

【００９３】

したがって、図１６の実施形態によって、ＳＴＡ３０２は、先ず、ビーコンを求めてリスンすることも、プローブ応答を要求することもなく、リンク設定のために、修正４方式ハンドシェイクを実行できるようになりうる。これはリンク設定時間を短縮し、ＳＴＡ３０２における電力を節約しうる。ＳＴＡ３０２は、ビーコン／プローブ応答を待たないので、保護されていない関連付け要求のために、代替のアドレシング・メカニズムを用いうる。例えば、ＡＰ３０４が、ＳＴＡ３０２に「知られている」場合、ＳＴＡ３０２は、ＳＴＡ３０２のメモリに、ＡＰ３０４の基本サービス・セット識別子（ＢＳＳＩＣ）を既に格納しているかもしれない。ＳＴＡ３０２は、リンク設定を開始するために、格納されたＢＳＳＩＤを検索し、保護されていない関連付け要求を、ＢＳＳＩＤに基づいてＡＰ３０４へ送信しうる。ＡＰ３０４がＳＴＡ３０２に「知られうる」状況は、ＡＰ３０４が、以前にＳＴＡ３０２によって訪問されている場合（例えば、「ホーム」ＡＰまたは「オフィス」ＡＰ）と、（例えば、ＳＴＡ３０２のセルラおよび／またはグローバル・ポジショニング・システム（ＧＰＳ）機能によって決定されたように）ＳＴＡ３０２が最近移動していない場合とを含む。したがって、特定の実施形態では、ＳＴＡ３０２は、（例えば、ＳＴＡ３０２が、ターゲットＡＰ３０４がＳＴＡ３０２の近傍にあることを「知っている」場合、）ＳＴＡ３０２において決定された位置情報に応じて、関連付け要求を送信しうる。

【００９４】

図１７は、リンク設定および認証を実行するために図１６のＳＴＡ３０２において動作可能な典型的な処理１７００を図示するフロー図である。１７０２では、モバイル・デバイス（例えば、ＳＴＡ３０２）が、モバイル・デバイスによって以前に訪問されたアクセス・ポイントのＢＳＳＩＤを検索しうる。１７０４に進んで、モバイル・デバイスはｒＭＳＫとＳＮｏｎｃｅとを生成しうる。１７０６に進んで、モバイル・デバイスは、保護さ

れていない関連付け要求を、ＢＳＳＩＤに基づいて、アクセス・ポイントへ送信しうる。例えば、図１６に示すように、ＳＴＡ３０２は、ステップ３において、保護されていない関連付け要求を、ＡＰ３０４へ送信しうる。

【００９５】

１７０８へ進んで、モバイル・デバイスは、アクセス・ポイントから、関連付け応答を受信しうる。関連付け応答は，ＡＮｏｎｃｅを含む。１７１０では、モバイル・デバイスは、受信した関連付け応答におけるｒＭＳＫ、ＳＮｏｎｃｅ、およびＡＮｏｎｃｅを用いてＰＴＫを生成しうる。例えば、図１６に示すように、ＳＴＡ３０２は、ステップ１２において、ＡＰ３０４から関連付け応答を受信し、ステップ１２ａにおいて、ＰＴＫを導出しうる。

【００９６】

図１８は、リンク設定および認証を実行するために、図１６のＡＰ３０４において動作可能な典型的な処理１８００を図示するフロー図である。１８０２において、アクセス・ポイントは、モバイル・デバイスから、保護されていない関連付け要求を受信しうる。保護されていない関連付け要求は、ＳＮｏｎｃｅを含む。１８０４に進んで、アクセス・ポイントは、保護されていない関連付け要求から、開始メッセージを抽出しうる。１８０６に進んで、アクセス・ポイントは、認証サーバへ開始メッセージを送信し、認証サーバから回答メッセージを受信しうる。回答メッセージは、ｒＭＳＫを含む。例えば、図１６に示すように、ＡＰ３０４は、ステップ３において、ＳＴＡ３０２から、保護されていない関連付け要求を受信し、ステップ８において、ＡＳ３０８から、ｒＭＳＫを受信しうる。

【００９７】

１８０８に進んで、アクセス・ポイントは、ＡＮｏｎｃｅを生成しうる。アクセス・ポイントはまた、１８１０において、ｒＭＳＫ、ＡＮｏｎｃｅ、およびＳＮｏｎｃｅを用いてＰＴＫを生成しうる。１８１２に進んで、アクセス・ポイントは、関連付け応答をモバイル・デバイスへ送信しうる。関連付け応答は、ＡＮｏｎｃｅを含み、ＰＴＫを用いて保護されている。例えば、図１６に示すように、ＡＰ３０４は、ステップ９においてＡＮｏｎｃｅを生成し、ステップ１０ａにおいてＰＴＫを導出し、ステップ１２において、関連付け応答をＳＴＡ３０２へ送信しうる。

【００９８】

図１９は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示するフロー図である。特に、図１９は、第１のリンク設定中に、第１のリンク設定に後続する第２のリンク設定中に用いられうる「次の」ＡＮｏｎｃｅを提供することを例示する。

【００９９】

図１６に例示された選択されたメッセージおよび動作は、以下の修正を伴い、図４－１１に例示されるメッセージおよび動作に対応しうる。ＳＴＡ３０２は、第１のＡＮｏｃｅ（例えば、ＡＮｏｎｃｅ　第１のリンク設定１９０２中、ＳＴＡ３０２は、第１のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ］）を用いて、ＡＰ３０４へ、関連付け要求を送信しうる。ＡＰ３０４は、第１のリンク設定１９０２中、ＳＴＡ３０２へ第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ＋１］）を提供しうる。第２のＡＮｏｎｃｅは、ＡＰ３０４との、後続する第２のリンク設定１９０４における使用のためのものでありうる。例えば、第２のＡＮｏｎｃｅは、（例えば、図４ａに図示されるような）関連付け応答で、（例えば、図４ｂにおいて図示されるような）ＥＡＰＯＬメッセージで、またはこれら任意の組み合わせで提供されうる。

【０１００】

ＳＴＡ３０２がＡＰ３０４との第２のリンク設定を開始した場合、ＳＴＡ３０２は、ビーコンを待つ代わりに、または、プローブ応答を要求する代わりに、第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ＋１］）を用いうる。特定の実施形態では、第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ＋１］）が、ＡＰ３０４によって設定された有効性寿命を有しうる。そして、ＳＴＡ３０２は、ステップ５ａにおいて、第２のリンク設定１９０

４を開始する前に、第２のＡＮｏｎｃｅが有効であると判定しうる。第２のＡＮｏｎｃｅが無効であると判定されると、ＳＴＡ３０２は、図２０を参照して記載したように続けうる。

【０１０１】

第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ＋１］）が有効であると判定されると、ＳＴＡは、第２のＡＮｏｎｃｅを用いて、第２のリンク設定１９０４を開始しうる。第２のリンク設定１９０４中、ＳＴＡ３０２は、ステップ６に図示されるように、第２のＡＮｏｎｃｅを用いて、第２の関連付け要求を送信しうる。ＳＴＡ３０２はまた、ステップ７ａまたはステップ７ｂに図示されるように、後続する第３のリンク設定において用いられるべき第３のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ＋２］）を受信しうる。

【０１０２】

図２０は、リンク設定および認証の他の態様にしたがって実行されうるメッセージを例示するフロー図である。図２０において例示されるメッセージおよび動作は、以下の修正を伴い、図１９に図示されるものに相当しうる。

【０１０３】

ステップ５ａにおいて、ＳＴＡ３０２は、（例えば、有効期間の終了によって、）第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ　したがって、図１９－２０に記載される実施形態は、「次のＡＮｏｎｃｅ」をモバイル・デバイスへ提供しうる。これによって、後続するリンク設定は、より高速に実行され、より少ない電力しか消費しないようになりうる。さらに、例示を容易にするために、図１９－２０の実施形態は、リンク設定に含まれるすべてのメッセージングを必ずしも含むものではないことが注目されるべきである。例えば、ＤＨＣＰ動作に関連するメッセージングと、ＡＰ３０４とＡＳ３０８との間のメッセージングとは図示されていない。

【０１０４】

図２１は、リンク設定および認証を実行するために、図１９－２０のＳＴＡ３０２において動作可能な典型的な処理２１００を図示するフロー図である。２１０２において、モバイル・デバイスは、第１のＡＮｏｎｃｅを用いて、アクセス・ポイントとの第１のリンク設定を開始しうる。第１のＡＮｏｎｃｅが、メモリから検索されうるか、および／または、ビーコンまたはプローブ応答によってアクセス・ポイントから受信されうる。２１０４に進んで、モバイル・デバイスは、アクセス・ポイントとの第１のリンク設定中に、アクセス・ポイントとの、後続する第２のリンク設定において用いられるための第２のＡＮｏｎｃｅを受信しうる。第２のＡＮｏｎｃｅは、関連付け応答および／またはＥＡＰＯＬメッセージで受信されうる。例えば、図１９－２０に示すように、ＳＴＡ３０２は、第１のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ］）を用いて第１のリンク設定１９０２を開始し、第１のリンク設定１９０２中に、第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ＋１］）を受信しうる。

【０１０５】

２１０６へ進んで、モバイル・デバイスは、第２のＡＮｏｎｃｅが有効であるか否かを判定しうる。例えば、モバイル・デバイスは、第２のリンク設定を開始する前に、このような判定を行いうる。例示するために、モバイル・デバイスは、第２のＡＮｏｎｃｅとともに送信されたタイマを用いうるか、または、第２のＡＮｏｎｃｅが有効であるか否かを判定するために予め設定されたタイマを用いうる。第２のＡＮｏｎｃｅが有効であると判定された場合、モバイル・デバイスは、２１０８において、第２のＡＮｏｎｃｅを用いて、第２のリンク設定を開始しうる。例えば、図１９に示すように、ＳＴＡ３０２は、第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｘ＋１］）を用いて第２のリンク設定１９０４を開始しうる。

【０１０６】

第２のＡＮｏｎｃｅが、無効であると判定された場合、モバイル・デバイスは、２１１０において、アクセス・ポイントから新たなＡＮｏｎｃｅを受信しうる。新たなＡＮｏｎｃｅは、ビーコンまたはプローブ応答で受信されうる。２１１２へ進んで、モバイル・デ

バイスは、新たなＡＮｏｎｃｅを用いて、アクセス・ポイントとのリンク設定を開始しうる。例えば、図２０に示すように、モバイル・デバイスは、リンク設定のために、この新たなＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ［ｙ］）を用いうる。

【０１０７】

図２２は、リンク設定および認証を実行するために、図１９－２０のＡＰ３０４において動作可能な典型的な処理２２００を図示するフロー図である。２２０２において、アクセス・ポイントは、モバイル・デバイスへ第１のＡＮｏｎｃｅを送信しうる。第１のＡＮｏｎｃｅは、第１のＡＮｏｎｃｅを用いる第１のリンク設定の開始前に送信されうる。２２０４へ進んで、アクセス・ポイントは、第１のリンク設定中、モバイル・デバイスとの、後続する第２のリンク設定において用いるために、第２のＡＮｏｎｃｅをモバイル・デイバスへ送信しうる。例えば、図１９－２０に示すように、ＡＰ３０４は、第１のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ　図２３は、リンク設定および認証の別の態様にしたがって実行されうるメッセージングを例示する図解である。特に、図２３は、リンク設定中の上部レイヤ・シグナリング保護のため、「テンポラリ」鍵（例えば、ＰＴＫ）を使用を例示する。上部レイヤ・シグナリング・メッセージは、（ＳＴＡ３０２と認証サーバ３０８との間に）内蔵型セキュリティ保護を有しているので、上部レイヤ・シグナリング・メッセージは、「より弱い」ＡＮｏｎｃｅ（例えば、より低いセキュリティ特性を有するＡＮｏｎｃｅ）を用いて保護されうる。これは、関連付けのためのより高速なシグナリング手順を可能にしうる。本明細書に記載されるように、「より強い」ＡＮｏｎｃｅが上部レイヤ・シグナリングと並行して導出され、さらなるデータ転送のために用いられる。

【０１０８】

図２３に例示された、選択されたメッセージおよび動作は、以下の修正を伴って、図４－１１に例示されたメッセージおよび動作に相当しうる。ステップ２において図示されるように、ＡＰ３０４はＳＴＡ３０２に第１のＡＮｏｎｃｅ（例えばＡＮｏｎｃｅ１）を送信しうる。ステップ３ａにおいて図示されるように、ＳＴＡ３０２は、ＳＴＡ３０２のＳＮｏｎｃｅおよびＡＮｏｎｃｅ１に基づいて、第１のＰＴＫ（例えば、ＰＴＫ１）を導出しうる。ステップ４において、ＳＴＡ３０２は、ＡＰ３０４に関連付け要求を送信しうる。関連付け要求は、ＳＮｏｎｃｅを含みうる。そして、ＰＴＫ１を用いて保護されうる。例示するために、関連付け要求は、ＰＫＴ１から導出された第１の鍵確認鍵（ＫＣＫ１）を用いて保護されうる。

【０１０９】

ステップ８ａにおいて、ＡＰ３０４は、関連付け要求に含まれるＳＮｏｎｃｅおよびＡＮｏｎｃｅ１に基づいてＰＴＫ１を導出しうる。ステップ１２において、ＡＰは、第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ２）を生成しうる。そして、ＳＮｏｎｃｅおよびＡＮｏｎｃｅ２に基づいて、第２のＰＴＫ（例えば、ＰＴＫ２）を導出しうる。ステップ１３において、ＡＰ３０４は、ＳＴＡ３０２へ、関連付け応答を送信しうる。関連付け要求は、ＡＮｏｎｃｅ２を含んでおり、ＰＴＫ２を用いて保護される。例示するために、関連付け応答は、ＰＴＫ２に基づいて導出された鍵暗号鍵（ＫＥＫ）とＫＣＫを用いて保護されうる。ＳＴＡ３０２は、リンク設定を完了するために、ステップ１４において、ＳＮｏｎｃｅに基づいてＰＴＫ２を生成しうる。ＰＴＫ２は、ＳＴＡ３０２とＡＰ３０４との間で通信される後続するメッセージ（例えば、データ・メッセージ）を保護するために、ＳＴＡ３０２およびＡＰ３０４によって用いられうる。

【０１１０】

したがって、保護されていない関連付け要求の送信を含む、図１６に例示されるメッセージ・フローとは異なり、図２３のメッセージ・フローは、「テンポラリ」ＰＴＫ１を用いて、関連付け要求を保護する。ＰＴＫ１は、複数のＳＴＡに知られうるＡＮｏｎｃｅを用いて生成される（例えば、ＡＮｏｎｃｅ１は、ビーコンによって複数のＳＴＡへブロードキャストされうる）が、「テンポラリ」鍵ＰＴＫ１を用いて、１つのメッセージ（関連付け要求）しか保護されないことが注目されるだろう。ＳＴＡ３０２とＳＴＡ３０４との間のデータ・メッセージおよび関連付け応答を含む後続するメッセージは、異なる鍵ＰＴ

Ｋ２を用いて保護される。図２３のメッセージ・フローは、例えば公衆アクセス・エリアのように、ＡＰが「知られている」または「信頼されている」状況においては、望ましいことでありうる。

【０１１１】

図２４は、リンク設定および認証を実行するために、図２３によって例示されているようにメッセージを通信し処理するＳＴＡ３０２のような局において動作可能な典型的な処理２４００を図示するフロー図である。２４０２において、モバイル・デバイス（例えば、ＳＴＡ３０２）は、アクセス・ポイント（例えば、ＡＰ３０４）から、第１のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ１）を受信しうる。２４０４に進んで、モバイル・デバイスは、第１のＡＮｏｎｃｅを用いて第１のＰＴＫ（例えば、ＰＴＫ１）を生成しうる。２４０６に進んで、モバイル・デバイスはアクセス・ポイントへ関連付け要求を送信しうる。関連付け要求は、ＳＮｏｎｃｅを含みうる。そして、第１のＰＴＫを用いて保護されうる。

【０１１２】

２４０８において、モバイル・デバイスは、アクセス・ポイントから、関連付け応答を受信しうる。関連付け応答は、第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ２）を含みうる。そして、第２のＰＴＫ（例えば、ＰＴＫ２）を用いて保護されうる。２４１０に進んで、モバイル・デバイスは、第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅを用いて第２のＰＴＫを生成しうる。２４１２に進んで、モバイル・デバイスは、アクセス・ポイントへ送信されるべき１または複数の後続するメッセージを保護するために、第２のＰＴＫを用いうる。

【０１１３】

図２５は、リンク設定および認証を実行するために、図２３によって例示されているようにメッセージを通信し処理するＡＰ３０４のようなアクセス・ポイントにおいて動作可能な典型的な処理２５００を図示するフロー図である。２５０２において、アクセス・ポイント（例えば、ＡＰ３０４）は、モバイル・デバイス（例えば、ＳＴＡ３０２）へ、第１のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ１）を送信しうる。例えば、第１のＡＮｏｎｃｅは、ユニキャスト・プローブ応答またはブロードキャスト・ビーコンによって送信されうる。２５０４に進んで、アクセス・ポイントは、モバイル・デバイスから関連付け要求を受信しうる。関連付け要求は、ＳＮｏｎｃｅを含みうる。そして、第１のＰＴＫ（例えば、ＰＴＫ１）を用いて保護されうる。２５０６において、アクセス・ポイントは、第１のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて、第１のＰＴＫを生成しうる。

【０１１４】

２５０８に進んで、アクセス・ポイントは、第２のＡＮｏｎｃｅ（例えば、ＡＮｏｎｃｅ２）を生成し、第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて、第２のＰＴＫ（例えば、ＰＴＫ２）を生成しうる。２５１０において、アクセス・ポイントは、モバイル・デバイスへ、関連付け応答を送信しうる。関連付け応答は、第２のＡＮｏｎｃｅを含みうる。そして、第２のＰＴＫを用いて保護されうる。

【０１１５】

図２６は、リンク設定および認証の別の態様によって実行されうるメッセージングを例示する図解である。特に、図２６は、ＡＮｏｎｃｅを生成するためにＡＮｏｎｃｅシードを用いることを例示する。

【０１１６】

図２６に例示された、選択されたメッセージおよび動作は、以下の修正を伴い、図４－１１において例示されたメッセージおよび動作に相当しうる。ステップ２において図示されるように、ＡＰ３０４は、ビーコンまたはプローブ応答で、ＳＴＡ３０２にＡＮｏｎｃｅシードを送信しうる。特定の実施形態では、ＡＮｏｎｃｅシードは、ＡＰ３０４によって頻繁に更新される６４ビットの暗号シード値である。特定の実施形態では、ＡＮｏｎｃｅシードは、複数のＳＴＡへ（例えば、ビーコンで）ブロードキャストされる。ステップ３に図示されるように、ＳＴＡ３０２は、デバイス特定のＡＮｏｎｃｅを生成するために

ＡＮｏｎｃｅシードを用いうる。特定の実施形態では、ＡＮｏｎｃｅは、ＳＴＡ３０２を記述する、および／または、（例えば、ＳＴＡ３０２のＭＡＣアドレス、または、ＳＴＡ３０２に関連付けられたその他いくつかの値のような）ＳＴＡ３０２にユニークな値およびＡＮｏｎｃｅシードに関数（例えば、ハッシュ関数）を実行することによって生成されうる。複数のＳＴＡへブロードキャストされたＡＮｏｎｃｅとは異なり、ステップ３で生成されたＡＮｏｎｃｅは、ＳＴＡ３０２にユニークでありうることが認識されるだろう。ＳＴＡ３０２は、生成されたＡＮｏｎｃｅに基づいて、ＡＰ３０４とのリンク設定を実行しうる。

【０１１７】

ステップ８ａにおいて、ＡＰ３０４は、ＳＴＡ３０２のＭＡＣアドレスおよびＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを導出しうる。例えば、ＳＴＡ３０２のＭＡＣアドレスは、ステップ４において送信された関連付け応答からＡＰ３０４によって検索されうる。ＡＰ３０４は、ＡＮｏｎｃｅを生成した後、ＳＴＡ３０２とのリンク設定を実行し、完了しうる。

【０１１８】

他のハンドシェイク技術とは異なり、図２６の実施形態は、ＡＰ３０４の前にＳＴＡ３０２がＡＮｏｎｃｅを生成することを含むことが注目されるだろう。しかしながら、後方互換性を保つために、図２６のＡＮｏｎｃｅシード技術にしたがって生成されたＡＮｏｎｃｅは、ハンドシェイク技術で、類似の特性をＡＮｏｎｃｅへ共有しうる。例えば、ＡＮｏｎｃｅは、ＳＴＡ３０２へユニークであり、ＡＮｏｎｃｅおよび／またはＡＮｏｎｃｅシードは、（例えば、ステップ２において図示されるようなビーコンまたはプローブ応答メッセージ、または、ステップ４において図示されるようなＥＡＰＯＬ鍵メッセージを用いて）「クリアに」送信されうる。そして、ＡＮｏｎｃｅは、ＡＰ３０４による送信前に、認証されていないデバイスによって予測可能ではないことがありうる。

【０１１９】

図２７は、リンク設定および認証を実行するために、図２６によって例示されているようにメッセージを通信し処理するＳＴＡ３０２のような局において動作可能な典型的な処理２７００を図示するフロー図である。２７０２において、モバイル・デバイス（例えば、ＳＴＡ３０２）は、アクセス・ポイント（例えば、ＡＰ３０４）から、ＡＮｏｎｃｅシードを受信しうる。２７０４に進んで、モバイル・デバイスは、モバイル・デバイスのＭＡＣアドレスおよびＡＮｏｎｃｅシードに基づいて、ＡＮｏｎｃｅを生成しうる。２７０６に進んで、モバイル・デバイスは、生成されたＡＮｏｎｃｅに基づいて、アクセス・ポイントとのリンク設定を実行しうる。

【０１２０】

図２８は、リンク設定および認証を実行するために、図２６によって例示されているようにメッセージを通信し処理するＡＰ３０４のようなアクセス・ポイントにおいて動作可能な典型的な処理２８００を図示するフロー図である。２８０２において、アクセス・ポイント（例えば、ＡＰ３０４）は、モバイル・デバイス（例えば、ＳＴＡ３０２）へ、ＡＮｏｎｃｅシードを送信しうる。２８０４に進んで、アクセス・ポイントは、モバイル・デバイスのＭＡＣアドレスを受信しうる。例えば、ＭＡＣアドレスは、モバイル・デバイスからの、例えば関連付け要求のようなメッセージに含まれうる。２８０６に進んで、アクセス・ポイントは、モバイル・デバイスのＭＡＣアドレスおよびＡＮｏｎｃｅシードに基づいて、ＡＮｏｎｃｅを生成しうる。２８０８において、アクセス・ポイントは、モバイル・デバイスによってレポートされたＡＮｏｎｃｅを、アクセス・ポイントによって計算されたモバイル・デバイスと比較することにより、モバイル・デバイスの認証性を検証しうる。モバイル・デバイスが検証に合格すると、アクセス・ポイントは、生成されたＡＮｏｎｃｅに基づいて、モバイル・デバイスとのリンク設定を実行しうる。

【０１２１】

さまざまな実施形態およびオプションが、本明細書において代案として記載されているが、別の実施形態およびオプションとは異なる特性が、リンク設定および認証を実行する

ために結合されうることが注目されるべきである。

【０１２２】

本明細書に記載されたさまざまな技術は、プル・ベースおよびプッシュ・ベースのデータ・シナリオに適用されうる。例えば、図１６－１８を参照して記載された修正４方式ハンドシェイクと、図１９－２２を参照して記載された「次の」ＡＮｏｎｃｅ技術が、プル・ベースおよびプッシュ・ベースのデータ・シナリオに適用されうる。例えば、電子メールおよびソーシャル・ネットワーク・アプリケーションのように、モバイル・デバイスによって実行される１または複数のアプリケーションは、データ更新を求めて定期的にチェックしうる。修正４方式ハンドシェイクまたは「次の」ＡＮｏｎｃｅ技術によって、このようなデータ更新プルは、より高速に、かつ、モバイル・デバイスのおけるバッテリ消費量を低減して実行できるようになりうる。別の例として、モバイル・デバイスにおけるアプリケーション（単数または複数）は、（例えば、サーバから）プッシュされたデータ更新を受信するように構成されうる。データ更新の最初の部分は、セル接続で受信されうる。しかしながら、データ更新の残りは、（例えば、ＷｉＦｉによって）より高速に、および／または、バッテリ消費量を低減して受信されうる。なぜなら、データ更新の最初の部分は、本明細書に記載されたように、修正４方式ハンドシェイクまたは「次の」ＡＮｏｎｃｅ技術を用いて、高速初期リンク設定をトリガするからである。図２３－２５を参照して記載されたテンポラリＰＴＫ技術と、図２６－２８を参照して記載されたＡＮｏｎｃｅシード技術とはまた、このようなプル・ベースおよびプッシュ・ベースのデータ・シナリオで用いられうる。

【０１２３】

記載された実施形態と連携して、第１の装置は、保護されていない関連付け要求をモバイル・デバイスからアクセス・ポイントへ送信する手段を含みうる。例えば、この送信する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、無線コントローラ２４０、アンテナ２４２、ＳＴＡ３０２の１または複数の構成要素、保護されていない関連付け要求を送信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。第１の装置はまた、アクセス・ポイントから関連付け応答を受信する手段を含みうる。関連付け応答は、ＡＮｏｎｃｅを含む。例えば、受信する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、無線コントローラ２４０、アンテナ２４２、ＳＴＡ３０２の１または複数の構成要素、関連付け応答を受信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。第１の装置はさらに、モバイル・デバイスにおいて、ＡＮｏｎｃｅを用いてＰＴＫを生成する手段を含みうる。例えば、生成する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、プロセッサ２１０、ＳＴＡ３０２の１または複数の構成要素、ＰＴＫを生成するように構成された１または複数の他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１２４】

第２の装置は、モバイル・デバイスから、保護されていない関連付け要求を、アクセス・ポイントにおいて受信する手段を含みうる。例えば、保護されていない関連付け要求を受信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、保護されていない関連付け要求を受信するように構成された１または複数の他のデバイス（例えば、無線コントローラおよび／またはＡＰのアンテナ）、またはこれら任意の組み合わせを含みうる。第２の装置はまた、保護されていない関連付け要求から、開始メッセージを抽出する手段を含みうる。例えば、抽出する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、開始メッセージを抽出するように構成された１または複数の他のデバイス（例えば、ＡＰのプロセッサ）、またはこれら任意の組み合わせを含みうる。第２の装置はさらに、ＡＳに開始メッセージを送信する手段を含みうる。例えば、開始メッセージを送信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、開始メッセージを送信するように構成された１または複数の他のデバイス（例えば、無線コントローラおよび／またはＡＰのアンテナ）、またはこれら任意の組み合わせを含みうる。

【０１２５】
第２の装置は、ＡＳから回答メッセージを受信する手段を含みうる。回答メッセージは、ｒＭＳＫを含む。例えば、回答メッセージを受信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、回答メッセージを受信するように構成された１または複数の他のデバイス（例えば、無線コントローラおよび／またはＡＰのアンテナ）またはこれら任意の組み合わせを含みうる。第２の装置はまた、ＡＮｏｎｃｅを生成する手段を含みうる。例えば、生成する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＡＮｏｎｃｅを生成するように構成された１または複数の他のデバイス（例えば、ＡＰのプロセッサ）、またはこれら任意の組み合わせを含みうる。第２の装置はさらに、アクセス・ポイントからモバイル・デバイスへ関連付け応答を送信する手段を含みうる。関連付け応答は、ＡＮｏｎｃｅを含む。例えば、関連付け応答を送信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、関連付け応答を送信するように構成された１または複数の他のデバイス（例えば、無線コントローラおよび／またはＡＰのアンテナ）、またはこれら任意の組み合わせを含みうる。

【０１２６】
第３の装置は、モバイル・デバイスにおいて、第１のＡＮｏｎｃｅを用いてアクセス・ポイントとの第１のリンク設定を開始する手段を含みうる。例えば、開始する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、プロセッサ２１０、ＳＴＡ３０２の１または複数の構成要素、リンク設定を開始するように構成された１または複数の他のデバイス、またはこれら任意の組み合わせを含みうる。第３の装置はまた、アクセス・ポイントとの第１のリンク設定中、第１のリンク設定に後続する、アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信する手段を含みうる。例えば、受信する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、無線コントローラ２４０、アンテナ２４２、ＳＴＡ３０２の１または複数の構成要素、ＡＮｏｎｃｅを受信するように構成された１または複数の他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１２７】
第４の装置は、第１のＡＮｏｎｃｅを用いる第１のリンク設定中に、アクセス・ポイントからモバイル・デバイスへ、第１のリンク設定に後続する、モバイル・デバイスとの第２のリンク設定のために用いる第２のＡＮｏｎｃｅを送信する手段を含みうる。例えば、第２のＡＮｏｎｃｅを送信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＡＮｏｎｃｅを送信するように構成された１または複数のその他のデバイス（例えば、無線コントローラおよび／またはＡＰのアンテナ）、またはこれら任意の組み合わせを含みうる。第４の装置はまた、第１のリンク設定の開始前に、ビーコンまたはプローブ応答で、モバイル・デバイスへ第１のＡＮｏｎｃｅを送信する手段を含みうる。第２のＡＮｏｎｃｅは、第１のＡＮｏｎｃｅとは異なる。例えば、第１のＡＮｏｎｃｅを送信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＡＮｏｎｃｅを送信するように構成された１または複数のその他のデバイス（例えば、無線コントローラおよび／またはＡＰのアンテナ）、またはこれら任意の組み合わせを含みうる。

【０１２８】
第５の装置は、モバイル・デバイスにおいて、アクセス・ポイントから第１のＡＮｏｎｃｅを受信する手段を含みうる。例えば、受信する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、無線コントローラ２４０、アンテナ２４２、ＳＴＡ３０２の１または複数の構成要素、ＡＮｏｎｃｅを受信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。この装置はまた、第１のＡＮｏｎｃｅを用いて第１のＰＴＫを生成する手段を含みうる。例えば、生成する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、プロセッサ２１０、ＳＴＡ３０２の１または複数の構成要素、ＰＴＫを生成するように構成された１または複数のその他のデバイス、ま

たはこれら任意の組み合わせを含みうる。第１のＡＮｏｎｃｅは、例えば、ビーコンで複数のＳＴＡへブロードキャストされる、または、値が予測可能であることによって、「弱い」ＡＮｏｎｃｅであると考えられうる。しかしながら、上部レイヤ・シグナリング・メッセージに埋め込まれた暗黙的なセキュリティによって、そのような「弱い」ＡＮｏｎｃｅを用いることは許容可能でありうる。さらに、本明細書に記載されるように、第２の、「より強い」ＡＮｏｎｃｅが導出され、さらなるデータ転送のために用いられうる。

【０１２９】

装置はさらに、関連付け要求をアクセス・ポイントへ送信する手段を含みうる。関連付け要求は、ＳＮｏｎｃｅを含み、第１のＰＴＫを用いて保護される。例えば、送信する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、無線コントローラ２４０、アンテナ２４２、ＳＴＡ３０２の１または複数の構成要素、関連付け要求を送信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３０】

装置は、アクセス・ポイントからの関連付け応答を、モバイル・デバイスにおいて受信する手段を含みうる。関連付け応答は、第２のＡＮｏｎｃｅを含み、第２のＰＴＫを用いて保護される。例えば、受信する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、無線コントローラ２４０、アンテナ２４２、ＳＴＡ３０２の１または複数の構成要素、関連付け応答を受信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。第２のＡＮｏｎｃｅは、「強い」ＡＮｏｎｃｅと考えられうる。

【０１３１】

装置はまた、モバイル・デバイスにおいて、第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅを用いて第２のＰＴＫを生成する手段を含みうる。例えば、生成する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、プロセッサ２１０、ＳＴＡ３０２の１または複数の構成要素、ＰＴＫを生成するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。この装置はさらに、モバイル・デバイスからアクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために、第２のＰＴＫを用いる手段を含みうる。例えば、用いる手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、プロセッサ２１０、ＳＴＡ３０２の１または複数の構成要素、メッセージを保護するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３２】

第６の装置は、アクセス・ポイントからモバイル・デバイスへ第１のＡＮｏｎｃｅを送信する手段を含みうる。例えば、送信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＡＮｏｎｃｅを送信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。この装置はまた、モバイル・デバイスから関連付け要求を受信する手段を含みうる。関連付け要求は、ＳＮｏｎｃｅを含んでおり、第１のＰＴＫを用いて保護される。例えば、受信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、関連付け要求を受信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３３】

この装置はさらに、アクセス・ポイントにおいて、第１のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて第１のＰＴＫを生成する手段を含みうる。例えば、生成する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＰＴＫを生成するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。この装置は、第２のＡＮｏｎｃｅを生成する手段を含みうる。例えば、第２のＡＮｏｎｃｅを生成する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＡＮｏｎｃｅを生成するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。この装置はまた、第２のＡＮ

ｏｎｃｅおよびＳＮｏｎｃｅに基づいて第２のＰＴＫを生成する手段を含みうる。例えば、生成する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＰＴＫを生成するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３４】

この装置はさらに、関連付け応答をモバイル・デバイスへ送信する手段を含みうる。関連付け応答は、第２のＡＮｏｎｃｅを含み、第２のＰＴＫを用いて保護される。例えば、送信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、関連付け応答を送信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３５】

第７の装置は、モバイル・デバイスにおいて、アクセス・ポイントからＡＮｏｎｃｅシードを受信する手段を含みうる。ＡＮｏｎｃｅシードは、（例えば、ビーコンによって）複数のデバイスへブロードキャストされうる。例えば、ＡＮｏｎｃｅシードを受信する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、無線コントローラ２４０、アンテナ２４２、ＳＴＡ３０２の１または複数の構成要素、ＡＮｏｎｃｅシードを受信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。装置はまた、モバイル・デバイスのＭＡＣアドレスおよびＡＮｏｎｃｅシードに基づいて、モバイル・デバイスにおいて、ＡＮｏｎｃｅを生成する手段を含みうる。例えば、生成する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、プロセッサ２１０、ＳＴＡ３０２の１または複数の構成要素、ＡＮｏｎｃｅを生成するように構成された１または複数のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３６】

装置はさらに、生成されたＡＮｏｎｃｅに基づいて、アクセス・ポイントとのリンク設定を実行する手段を含みうる。例えば、実行する手段は、ＳＴＡ１０６－１１０の１または複数の構成要素、プロセッサ２１０、ＳＴＡ３０２の１または複数の構成要素、リンク設定を実行するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３７】

第８の装置は、アクセス・ポイントからモバイル・デバイスへＡＮｏｎｃｅシードを送信する手段を含みうる。例えば、送信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＡＮｏｎｃｅシードを送信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３８】

装置はまた、モバイル・デバイスのＭＡＣアドレスを受信する手段を含みうる。例えば、受信する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＭＡＣアドレスを受信するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。この装置はまた、モバイル・デバイスのＭＡＣアドレスおよびＡＮｏｎｃｅシードに基づいて、ＡＮｏｎｃｅを生成する手段を含みうる。例えば、生成する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、ＡＮｏｎｃｅを生成するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１３９】

装置は、生成されたＡＮｏｎｃｅに基づいて、モバイル・デバイスとのリンク設定を実行する手段を含みうる。例えば、実行する手段は、ＡＰ１０２の１または複数の構成要素、ＡＰ３０４の１または複数の構成要素、リンク設定を実行するように構成された１または複数のその他のデバイス、またはこれら任意の組み合わせを含みうる。

【０１４０】

開示された実施形態の上記記載は、当業者が、開示された実施形態の製造または利用を可能とするように提供される。これら実施形態に対するさまざまな変形例もまた、当業者

に明らかであって、本明細書で定義された原理は、本開示の範囲から逸脱することなく他の例にも適用されうる。したがって、本開示は、本明細書で開示された実施形態に限定されるものではなく、後述する特許請求の範囲によって定義されたような原理および新規な特徴に一致することが可能な最も広い範囲に相当することが意図されている。

【０１４１】

本明細書において記載された要素は、同じ要素の複数の実例を含みうる。これらの要素は、一般に、数字指定（例えば、１１０）によって示され、特に、アルファベットが後続する数字表示（例えば、１１０Ａ）、または、「ダッシュ」が先行する数字表示（例えば、１１０－１）によって示されうる。以下の記載を容易にするために、大部分は、要素番号指定は、これら要素が導入または最も十分に記載されている図面の番号とともに始まる。

【０１４２】

本明細書において、例えば、「第１の」、「第２の」等のような要素に対するいずれの参照も、明示的に限定されていないのであれば、これら要素の数も順序も限定しないことが理解されるべきである。むしろ、これら指定は、本明細書において、複数の要素または要素の事例を区別する従来の方法として使用されうる。したがって、第１の要素および第２の要素への参照は、２つのみの要素しか適用されていないことも、第１の要素が、ある方式において、第２の要素に先行することも意味していない。さらに、特に述べられていないのであれば、これら要素のセットは、１または複数の要素を備えうる。

【０１４３】

図示および記載された特定の実施例は、単なる例であり、本明細書において指定されていないのであれば、本開示を実現するための唯一の方法であると解釈されるべきではない。本開示におけるさまざまな例は、その他多くの分割システムによって実現されうることが当業者に容易に明らかである。

【０１４４】

当業者であれば、情報および信号は、さまざまな異なる技術および技法のうちの何れかを用いて表されうることを理解するであろう。例えば、本記載を通じて参照されたデータ、命令群、指示、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場または磁気粒子、光場または光粒子、またはこれらの任意の組み合わせによって表されうる。いくつかの図面は、表示および記載の明瞭化のために、複数の信号を、単一の信号として例示しうる。信号は、複数の信号のバスを表しうることが当業者によって理解されるだろう。ここで、バスは、さまざまなビット幅を有し、本開示は、単一のデータ信号を含む任意の数のデータ信号で実現されうる。

【０１４５】

この記載では、本開示を不必要に詳細に不明確にしないために、要素、回路、および機能が、ブロック図形式で示されうる。逆に、図示および記載された特定の実施は、単なる典型例であって、本明細書において指定されていないのであれば、本開示を実現するための唯一の方法であると解釈されるべきではない。さらに、ブロック定義や、さまざまなブロック間のロジックの分割は、特定の実施例の典型例である。本開示は、その他多くの分割システムによって実現されうることが当業者に容易に明らかである。ほとんどの部分において、タイミング考慮等に関する詳細は、それが本開示の完全な理解を得るために必ずしも必要ではなく、かつ、当業者の能力内である場合には、省略されている。

【０１４６】

本明細書に記載され、図面に例示されている構成要素、動作、および／または、機能のうちの１または複数は、単一の構成要素、動作、特徴、または機能に再構成および／または結合されうるか、または、いくつかの構成要素、動作、特徴、または機能に組み込まれうる。さらなる要素、構成要素、動作、および／または、機能も、本発明から逸脱することなく追加されうる。本明細書に記載されたアルゴリズムはまた、効率的に、ソフトウェアで実現されうるか、および／または、ハードウェアに組み込まれうる。

【０１４７】

さらに、実施形態は、フローチャート、フロー図、構成図、またはブロック図として図示される処理として記述されうることが注目される。フローチャートは、動作をシーケンシャルな処理として記述しうるが、これら動作の多くは並行して、または、同時に実行されうる。さらに、これら動作の順序は、再構成されうる。動作が完了した場合、処理が終了する。処理は、方法、機能、手順、サブルーチン、サブプログラム等に相当しうる。処理が機能に相当する場合、その終了は、コール元機能またはメイン機能へ機能を戻すことに相当する。

【０１４８】

さらに、記憶媒体は、読取専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、磁気ディスク記憶媒体、光記憶媒体、フラッシュ・メモリ・デバイスおよび／またはその他の機械読取可能媒体、およびプロセッサ読取可能媒体、および／または、情報を格納するためのコンピュータ読取可能媒体を含む、データ格納のための１または複数のデバイスを表しうる。用語「機械読取可能媒体」、「コンピュータ読取可能媒体」、および／または、「プロセッサ読取可能媒体」は、限定される訳ではないが、例えば、ポータブルまたは据置式記憶デバイス、光記憶デバイス、および、命令群（単数または複数）および／またはデータを格納、包含、または搬送することが可能なその他さまざまな媒体のような非一時的な媒体を含みうる。したがって、本明細書に記載されたさまざまな方法は、「機械読取可能媒体」、「コンピュータ読取可能媒体」、および／または、「プロセッサ読取媒体」に格納されうる命令群および／またはデータによって完全にまたは部分的に実現され、１または複数のプロセッサ、機械および／またはデバイスによって実行されうる。

【０１４９】

さらに、実施形態は、ハードウェア、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、またはこれらの任意の組み合わせによって実現されうる。ソフトウェア、ファームウェア、ミドルウェア、またはマイクロコードにおいて実現される場合、必要なタスクを実行するためのコード・セグメントまたはプログラム・コードは、例えば記憶媒体またはその他の記憶装置（単数または複数）のような機械読取可能媒体に格納されうる。プロセッサは、必要なタスクを実行しうる。コード・セグメントは、手順、機能、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェア・パッケージ、クラス、あるいは命令群、データ構造、あるいはプログラム文の任意の組み合わせを示しうる。コード・セグメントは、情報、データ、引数、パラメータ、あるいはメモリ・コンテンツの引き渡しおよび／または受け取りを行うことによって、他のコード・セグメントあるいはハードウェア回路に接続されうる。情報、引数、パラメータ、データ等は、メモリ共有、メッセージ引き渡し、トークン引き渡し、ネットワーク送信等を含む任意の適切な手段によって引き渡し、転送、または送信されうる。

【０１５０】

本明細書で開示された例に関連して記述されたさまざまな例示的な論理ブロック、モジュール、回路、要素、および／または、構成要素は、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・アレイ（ＦＰＧＡ）、あるいはその他のプログラマブル論理構成要素、ディスクリート・ゲートあるいはトランジスタ・ロジック、ディスクリート・ハードウェア構成要素、または上述された機能を実現するために設計された上記何れかの組み合わせを用いて実現または実施されうる。汎用プロセッサは、マイクロ・プロセッサでありうるが、代替例では、このプロセッサは、従来のプロセッサ、コントローラ、マイクロ・コントローラ、またはステート・マシンでありうる。プロセッサは、例えばＤＳＰとマイクロ・プロセッサとの組み合わせ、多くのマイクロ・プロセッサ、ＤＳＰコアと連携する１または複数のマイクロ・プロセッサ、またはその他任意のこのような構成であるコンピューティング構成要素の組み合わせとして実現されうる。本明細書に記載された実施形態を実行するように構成された汎用プロセッサは、このような実施形態を実行するための専用プロセッサと考えられる。同様に、汎用コンピュータは、本明細書に記載された実施形態を実行する

ように構成されている場合、専用コンピュータであると考えられる。

【０１５１】

本明細書の開示された例に関連して記載された方法またはアルゴリズムは、処理ユニット、プログラミング命令群、またはその他の指示の形態で、直接的にハードウェアで、プロセッサによって実行可能なソフトウェア・モジュールで、または、これら両方の組み合わせで具体化されうる。そして、単一のデバイスに含まれうるか、または、複数のデバイスに分散されうる。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（登録商標）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、あるいは当該技術分野で知られているその他の型式の記憶媒体に存在しうる。記憶媒体は、プロセッサが記憶媒体から情報を読み取ったり、記憶媒体へ情報を書き込んだりできるように、プロセッサに接続されうる。あるいは、この記憶媒体は、プロセッサに統合されうる。

【０１５２】

例えば、ＳＴＡ機能は、プロセッサ読取可能な媒体に格納された命令群を用いて実施されうる。特定の媒体は、モバイル・デバイスによってアクセス・ポイントへ送信されるべき保護されていない関連付け要求を、プロセッサに対して生成させるように実行可能な命令群を格納しうる。これら命令群はまた、アクセス・ポイントからの関連付け応答から検索されたＡＮｏｎｃｅを用いてＰＴＫを、プロセッサに対して生成させるように実行可能でありうる。別の特定の媒体は、モバイル・デバイスにおいて、第１のＡＮｏｎｃｅを用いてアクセス・ポイントとの第１のリンク設定を開始するためにプロセッサによって実行可能な命令群を格納しうる。これら命令群はまた、アクセス・ポイントとの第１のリンク設定中に、第１のリンク設定に後続する、アクセス・ポイントとの第２のリンク設定のために用いる第２のＡＮｏｎｃｅをプロセッサに対して受信させるように実行可能でありうる。

【０１５３】

別の例として、ＡＰ機能は、プロセッサ読取可能な媒体に格納された命令群を用いて実施されうる。例えば、特定の媒体は、プロセッサに対して、モバイル・デバイスから受信した、保護されていない関連付け要求から、開始メッセージを抽出させるように実行可能な命令群を格納しうる。これら命令群はまた、プロセッサに対して、開始メッセージに応じて、認証サーバから受信した回答メッセージから、ｒＭＳＫを抽出させるように実行可能でもありうる。これら命令群はさらに、プロセッサに対して、ＡＮｏｎｃｅを生成させ、さらに、モバイル・デバイスへ送信されるべき関連付け応答を生成させるように実行可能でありうる。ここで、関連付け応答は、ＡＮｏｎｃｅを含む。別の特定の媒体は、第１のＡＮｏｎｃｅを用いる第１のリンク設定中に、アクセス・ポイントからモバイル・デバイスへ、第１のリンク設定に後続する、モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを送信するようにプロセッサによって実行可能な命令群を格納しうる。

【０１５４】

当業者であればさらに、本明細書で開示された実施形態に関連して記載されたさまざまな例示的な論理ブロック、モジュール、回路、およびアルゴリズム・ステップが、電子工学ハードウェア、コンピュータ・ソフトウェア、あるいはこれらの組み合わせとして実現されることを理解するであろう。ハードウェアとソフトウェアとの相互置換性を明確に説明するために、さまざまな例示的な構成要素、ブロック、モジュール、回路、およびステップが、これらの機能の観点から一般的に記載された。これら機能がハードウェアとして、ソフトウェアとして、またはこれらの組み合わせとして実現されるかは、システム全体に課せられている設計選択および特定のアプリケーションに依存する。

【０１５５】

本明細書に記載された発明のさまざまな特徴は、本発明から逸脱することなく、別のシステムにおいて実現されうる。前述した実施形態は、単なる例であり、本発明を限定するものとして解釈されるべきではないことが注目されるべきである。実施形態の記載は、例

示であって、請求項の範囲を制限するものではことが意図されている。そのため、本教示は、その他のタイプの装置および多くの代替例、修正、および変更が、当業者に明らかになるだろう。

【図１】

図1

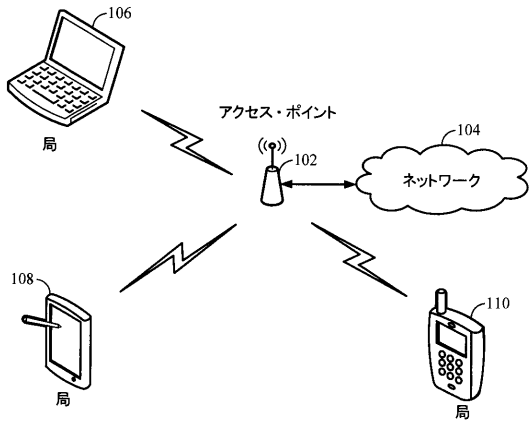

FIG. 1

【図２】

図2

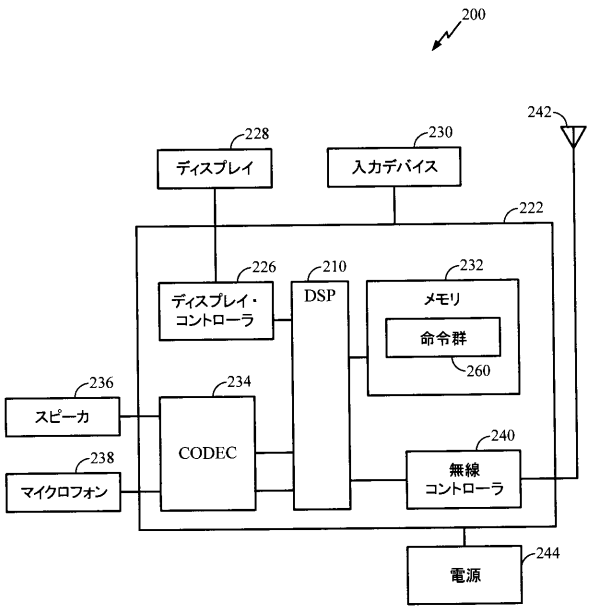

FIG. 2

【図３】

図３

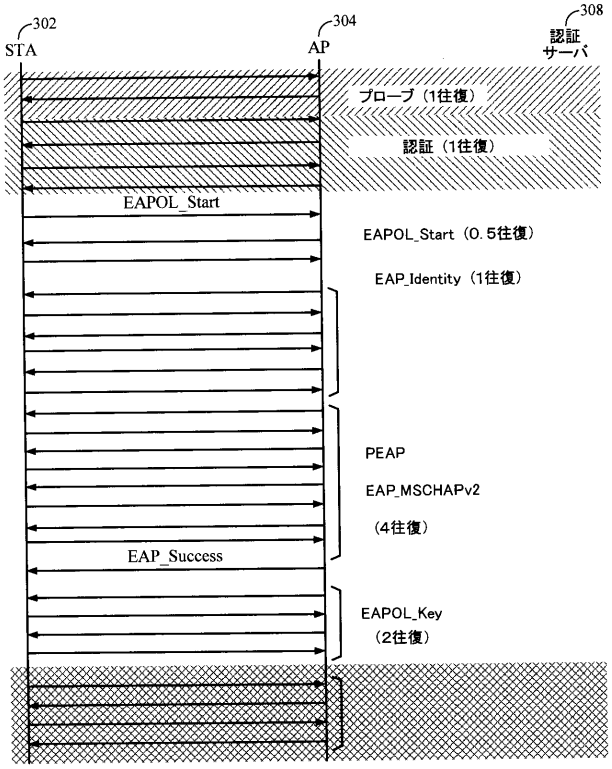

FIG. 3

【図４】

図４（オプション１）

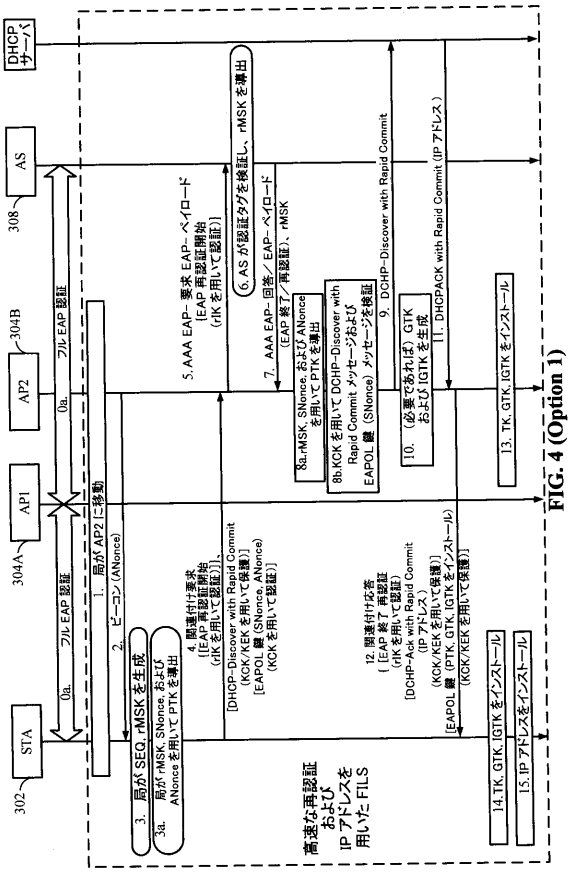

FIG. 4 (Option 1)

【図５】

図５（オプション１ａ）

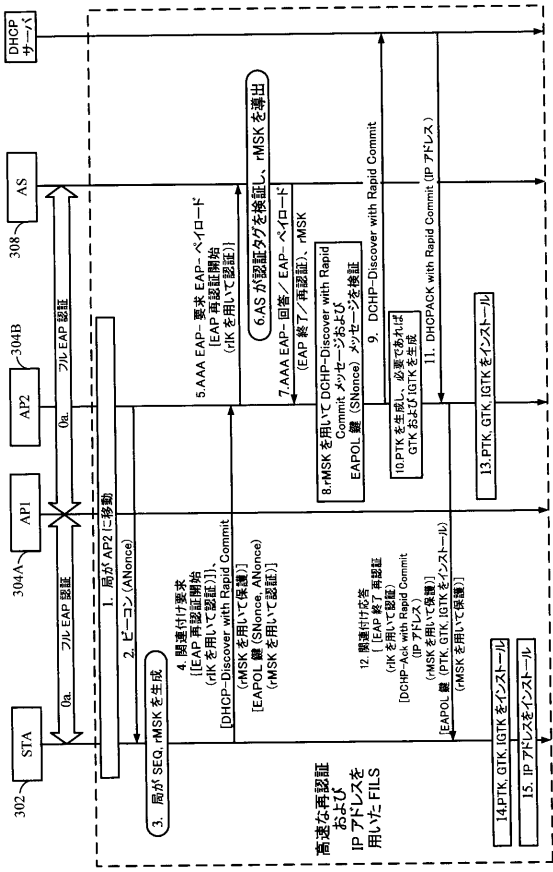

FIG. 5 (Option 1a)

【図６】

図６（オプション１ｂ）

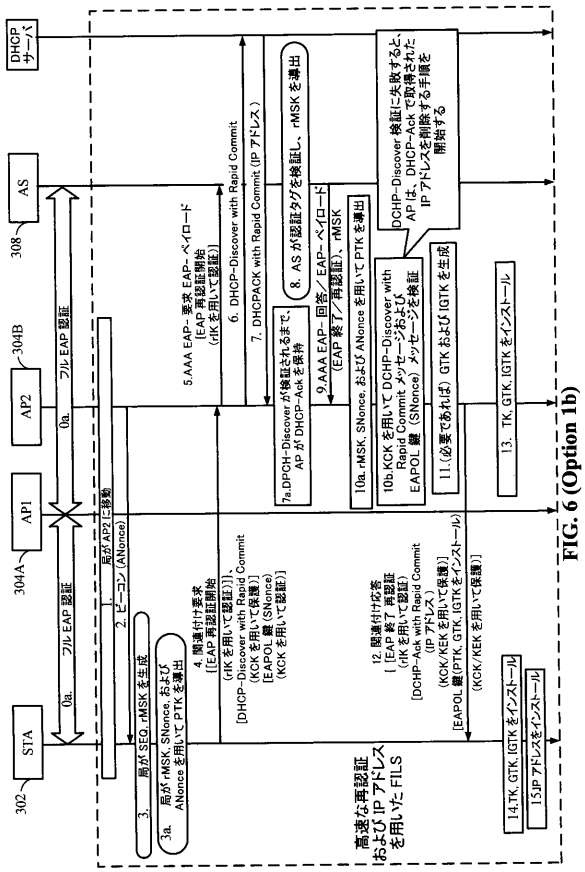

FIG. 6 (Option 1b)

【図７】

図7(オプション2)

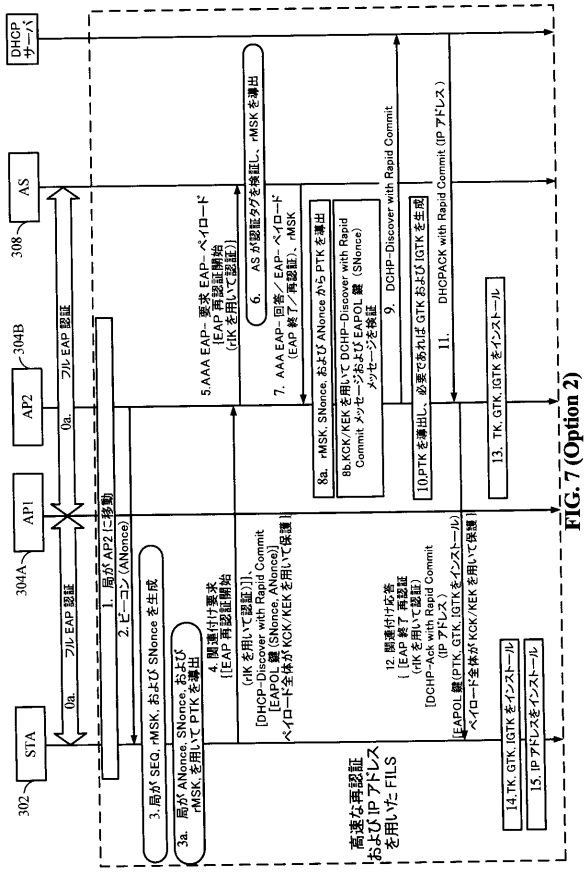

FIG. 7 (Option 2)

【図８】

図8(オプション2a)

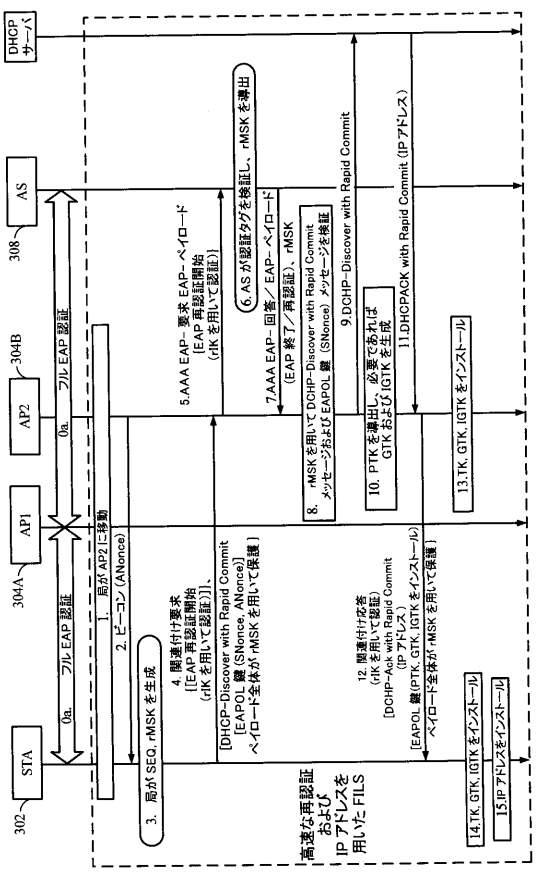

FIG. 8 (Option 2a)

【図９】

図9(オプション2b)

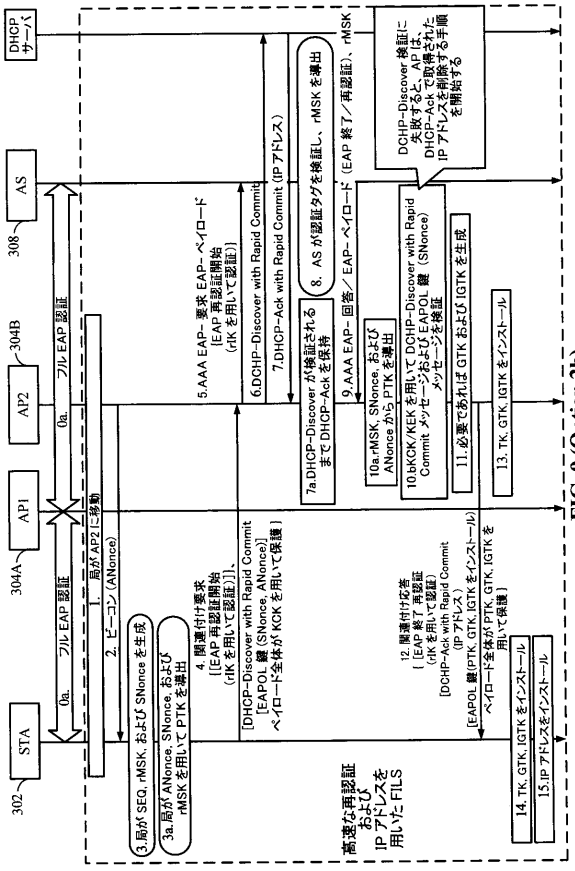

FIG. 9 (Option 2b)

【図１０】

図10(オプション3)

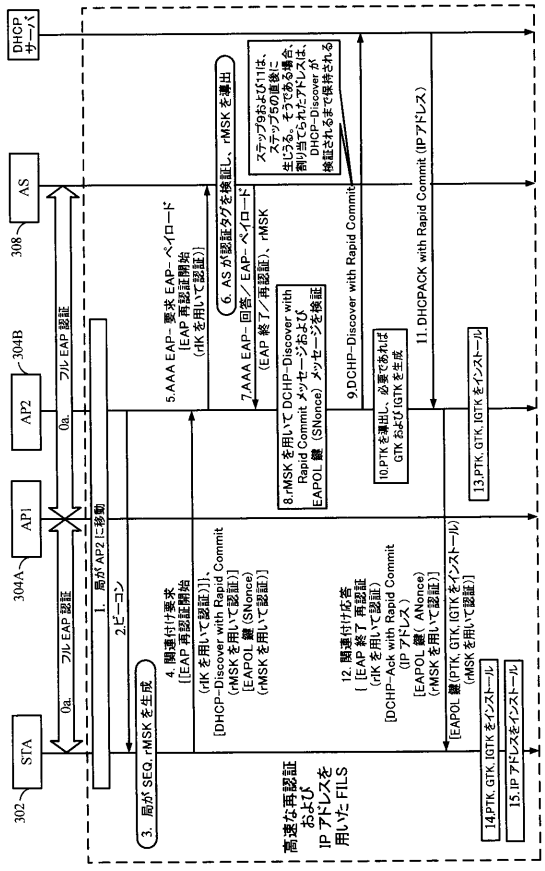

FIG. 10 (Option 3)

【図１１】

図 11(オプション 5)

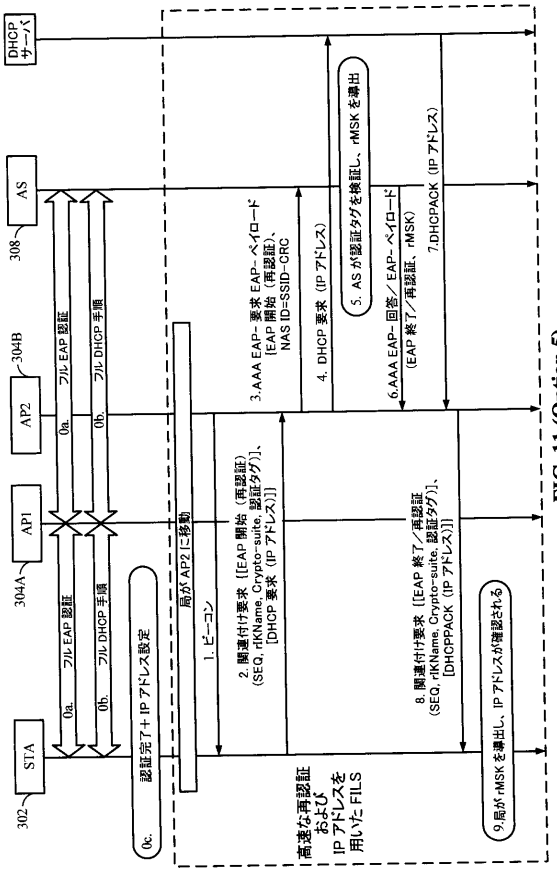

FIG. 11 (Option 5)

【図１２】

図 12

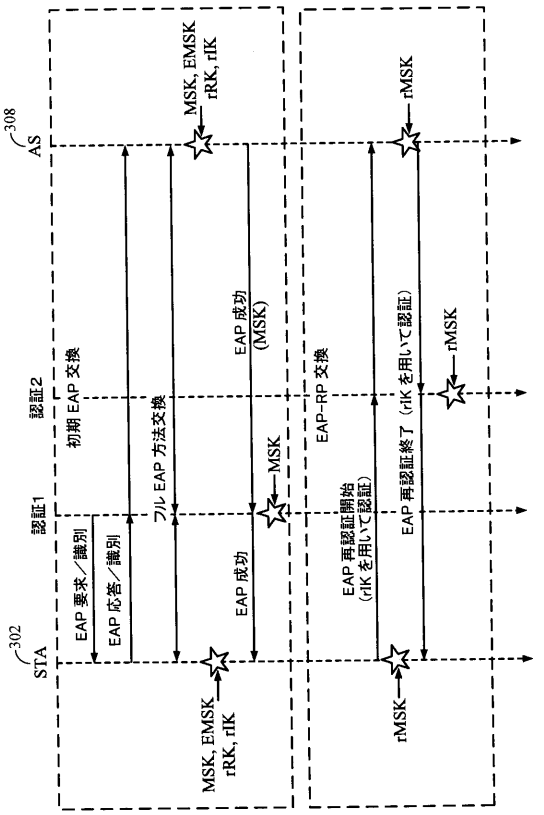

FIG. 12

【図１３】

図 13

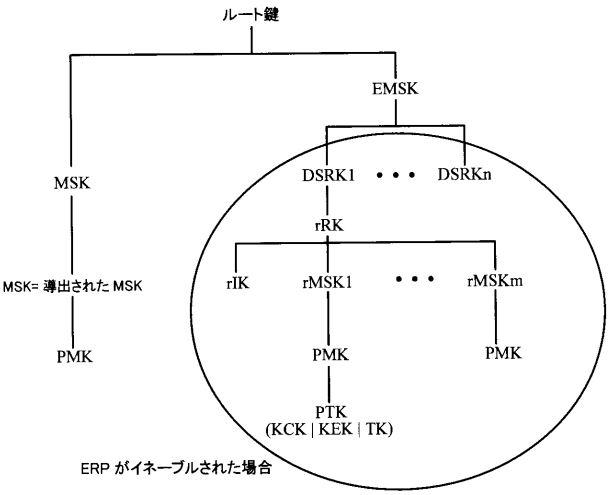

FIG. 13

【図１４】

図 14

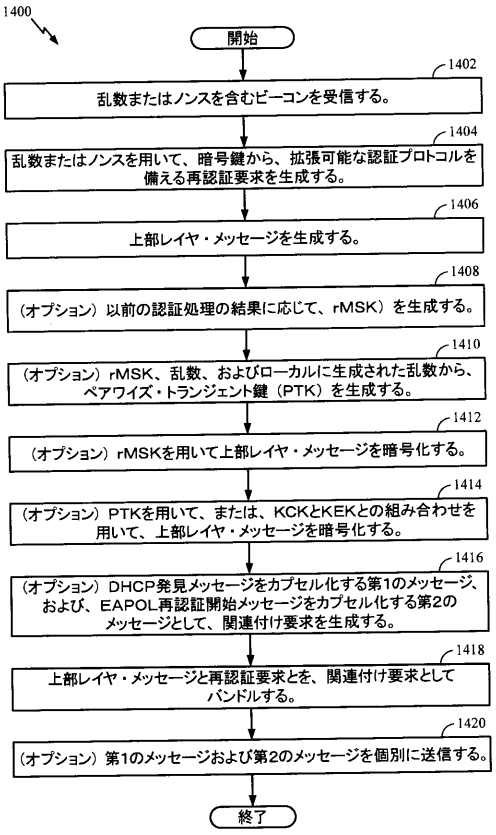

FIG. 14

【図１５】

図15

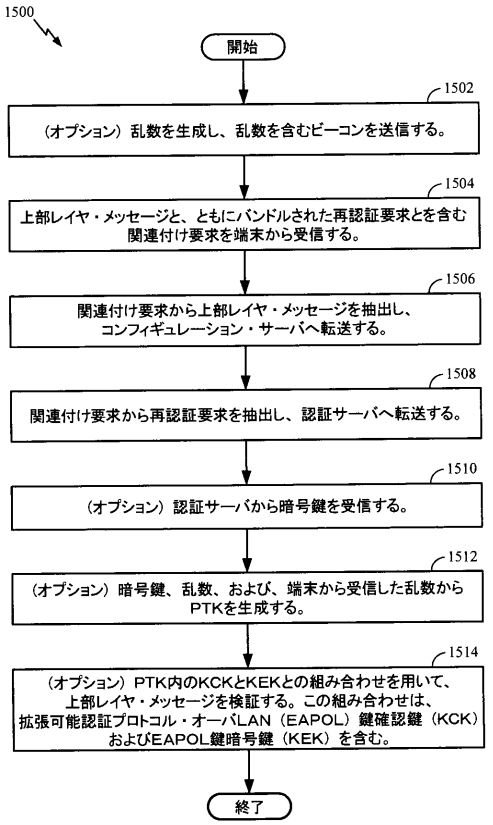

FIG. 15

【図１６】

図16

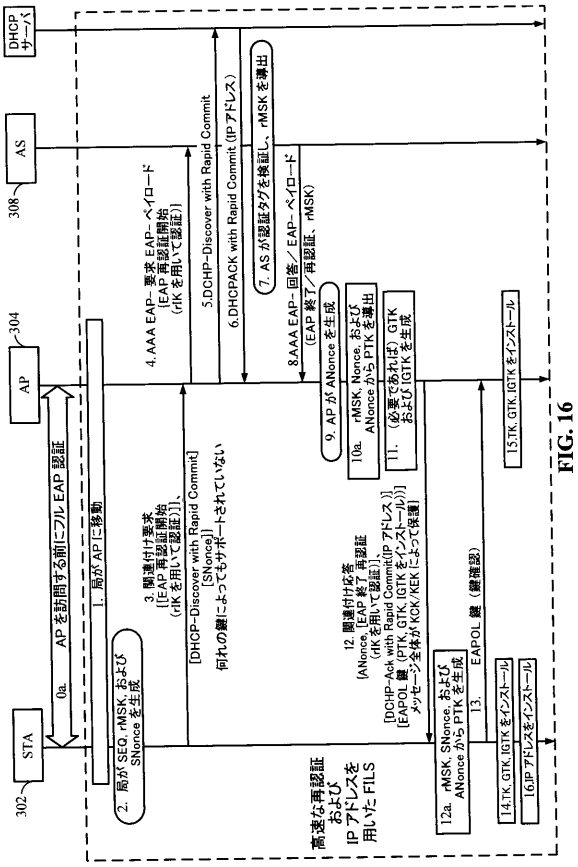

FIG. 16

【図１７】

図17

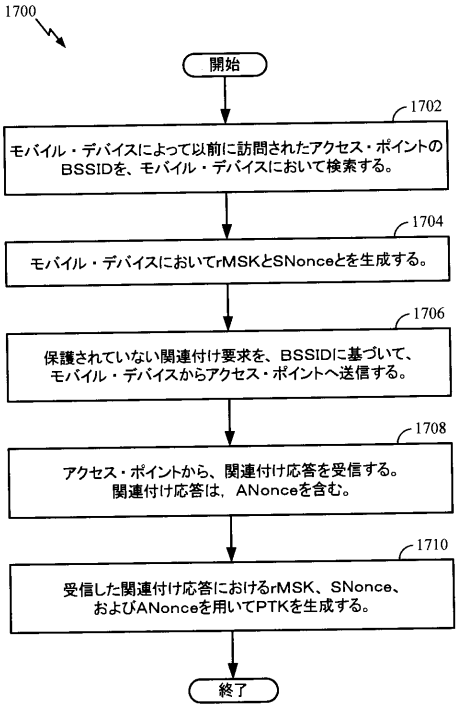

FIG. 17

【図１８】

図18

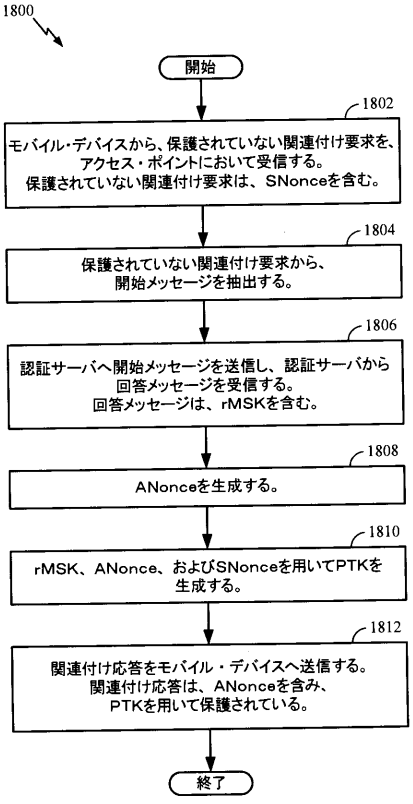

FIG. 18

【図１９】

図 19

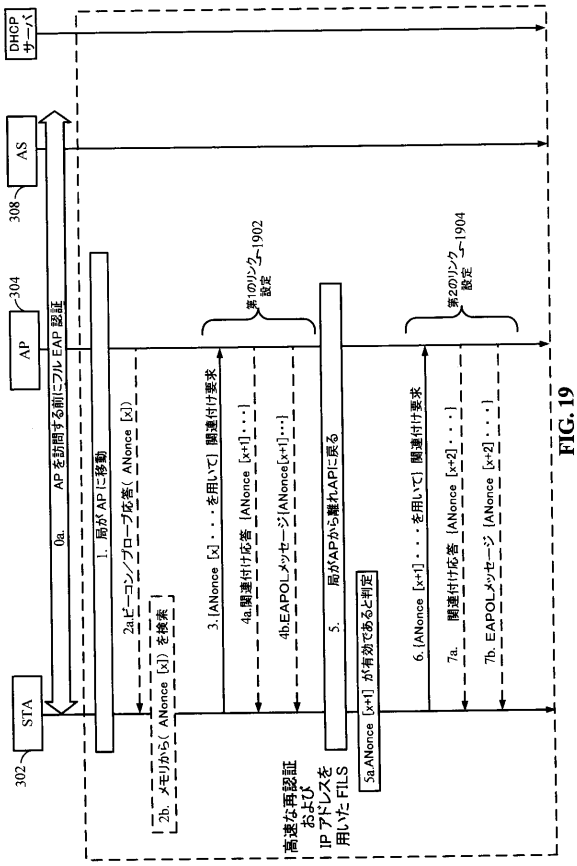

FIG. 19

【図２０】

図 20

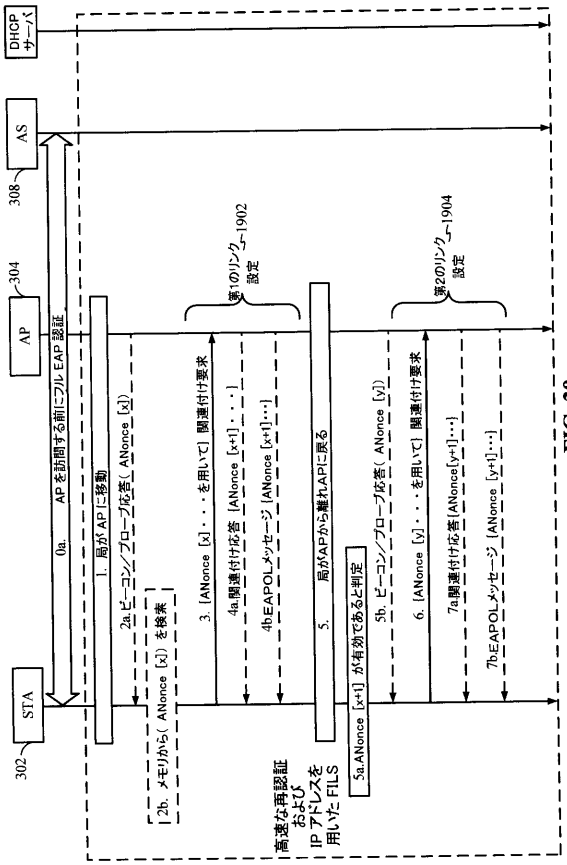

FIG. 20

【図２１】

図 21

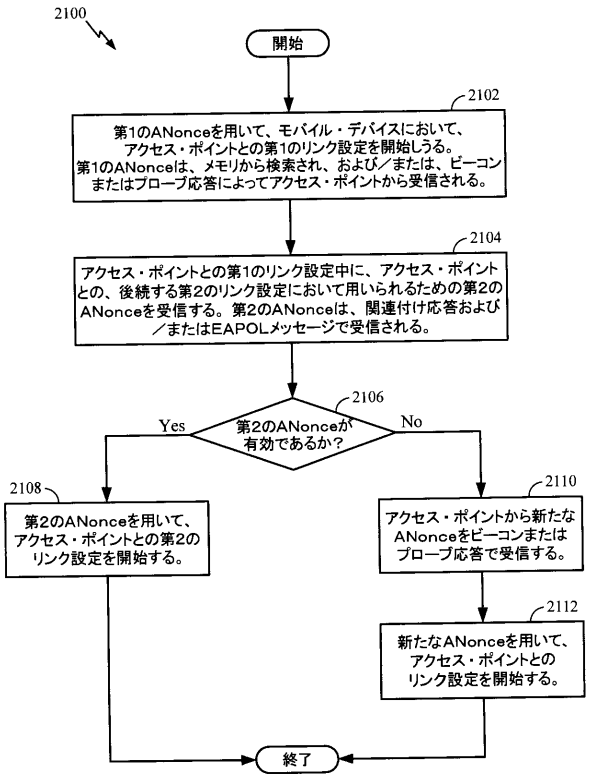

FIG. 21

【図２２】

図 22

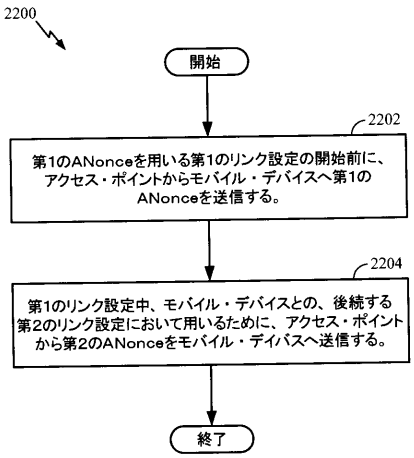

FIG. 22

【図２３】

図 23

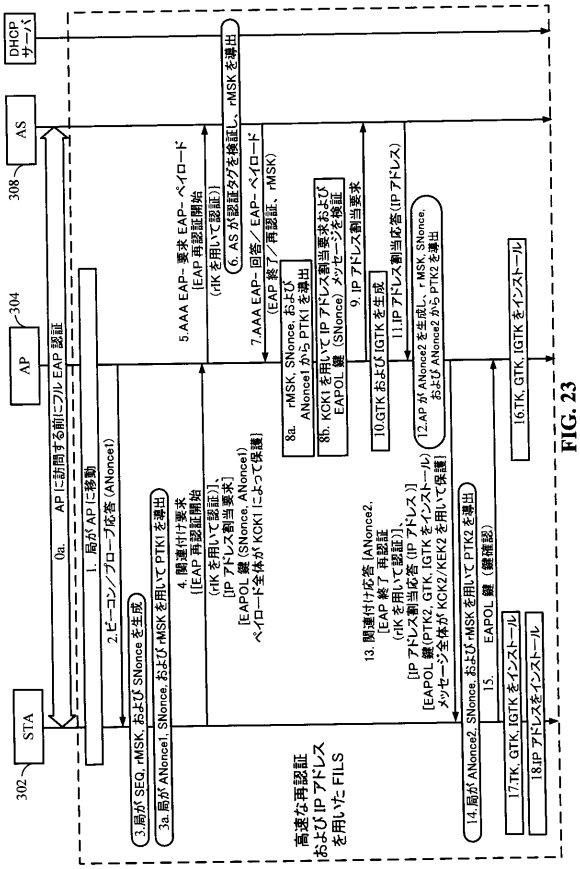

FIG. 23

【図２４】

図 24

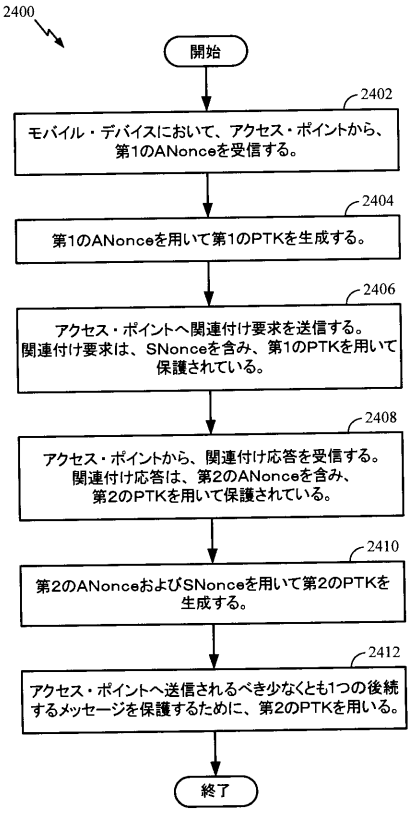

FIG. 24

【図２５】

図 25

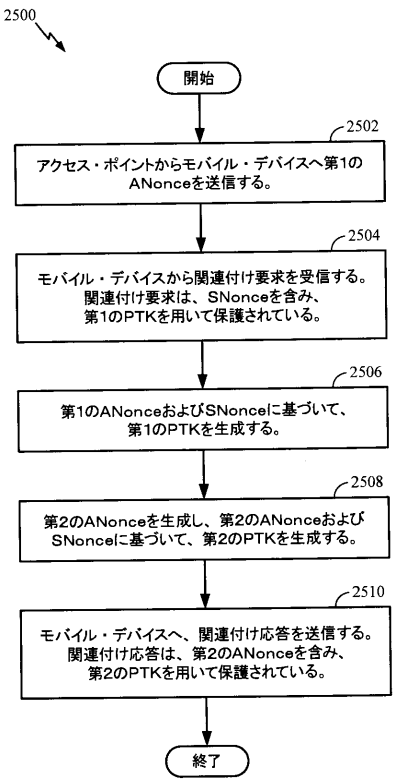

FIG. 25

【図２６】

図 26

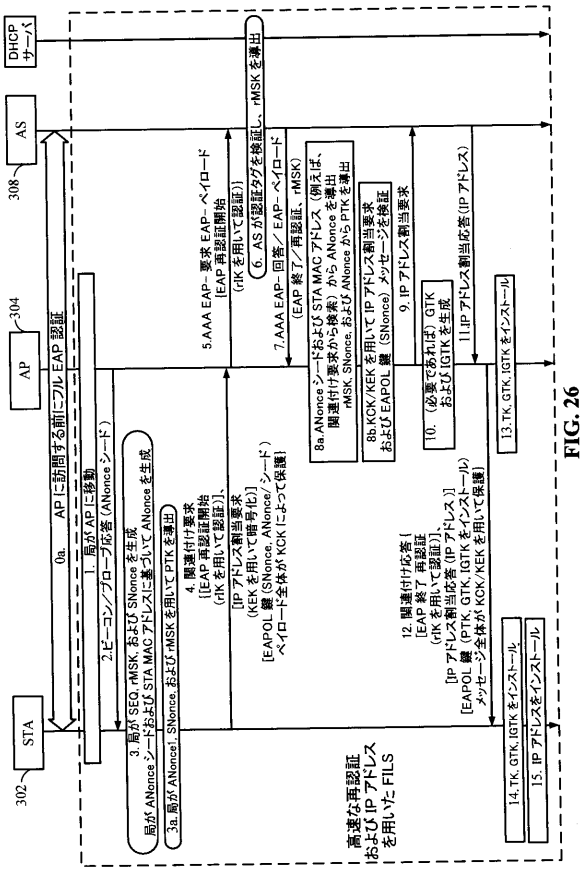

FIG. 26

【図２７】

図 27

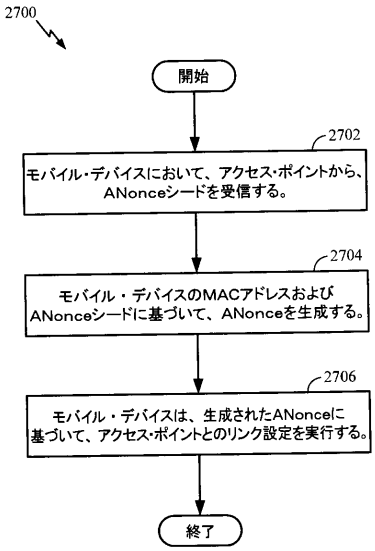

FIG. 27

【図２８】

図 28

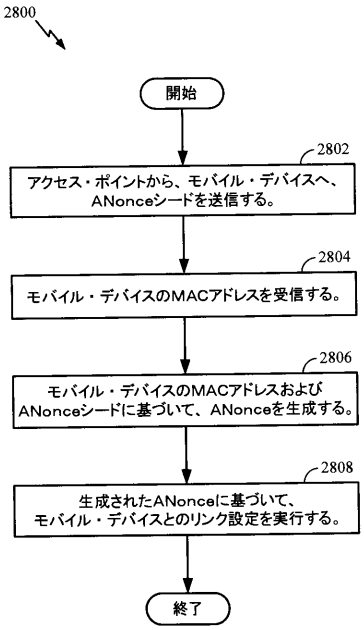

FIG. 28

【手続補正書】
【提出日】平成28年2月10日(2016.2.10)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
方法であって、
モバイル・デバイスにおいて、アクセス・ポイントから、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を受信することと、
前記第１のＡＮｏｎｃｅを用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
前記アクセス・ポイントへ、認証要求を送信することと、ここで、前記認証要求は、局ノンス（ＳＮｏｎｃｅ）を含み、前記認証要求は、前記第１のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記アクセス・ポイントから認証応答を受信することと、ここで、前記認証応答は、第２のＡＮｏｎｃｅを含み、第２のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記第２のＡＮｏｎｃｅおよび前記ＳＮｏｎｃｅを用いて、前記第２のＰＴＫを生成することと、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いることと、
を備える方法。

【請求項２】
前記第１のＡＮｏｎｃｅは、ビーコンによって受信される、請求項１記載の方法。
【請求項３】
前記第１のＡＮｏｎｃｅは、プローブ応答によって受信される、請求項１記載の方法。
【請求項４】
前記第１のＰＴＫは、前記第１のＡＮｏｎｃｅ、前記ＳＮｏｎｃｅ、および再認証マスタ・セッション鍵（ｒＭＳＫ）を用いて生成される、請求項１記載の方法。
【請求項５】
前記ｒＭＳＫは、前記モバイル・デバイスにおいて生成される、請求項４記載の方法。
【請求項６】
前記認証要求は、前記第１のＡＮｏｎｃｅをさらに含む、請求項１記載の方法。
【請求項７】
前記第２のＰＴＫは、前記第２のＡＮｏｎｃｅ、前記ＳＮｏｎｃｅ、および再認証マスタ・セッション鍵（ｒＭＳＫ）を用いて生成される、請求項１記載の方法。
【請求項８】
前記ｒＭＳＫは、前記モバイル・デバイスにおいて生成される、請求項７記載の方法。
【請求項９】
前記認証要求は、前記第１のＰＴＫのうちの少なくとも鍵確認鍵（ＫＣＫ）部分を用いて保護されている、請求項１記載の方法。
【請求項１０】
、
前記認証応答は、少なくとも前記第２のＰＴＫの鍵確認鍵（ＫＣＫ）部分、前記第２のＰＴＫの鍵暗号鍵（ＫＥＫ）部分、またはこれらの組み合わせを用いて保護されている、請求項１記載の方法。
【請求項１１】
装置であって、
プロセッサと、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべき第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスからの認証要求によって受信された局ノンス（ＳＮｏｎｃｅ）および前記第１のＡＮｏｎｃｅに基づいて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、ここで、前記認証要求は、前記第１のＰＴＫを用いて保護されている、
第２のＡＮｏｎｃｅを生成することと、
前記第２のＡＮｏｎｃｅおよび前記ＳＮｏｎｃｅに基づいて第２のＰＴＫを生成することと、
前記モバイル・デバイスへ送信されるべき認証応答を生成することと、ここで、前記認証応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
【請求項１２】
前記第１のＡＮｏｎｃｅは、ビーコンによって前記モバイル・デバイスに送信される、請求項１１記載の装置。
【請求項１３】
前記第１のＡＮｏｎｃｅは、プローブ応答によって前記モバイル・デバイスに送信される、請求項１１記載の装置。
【請求項１４】
前記認証要求は、前記第１のＰＴＫのうちの少なくとも鍵確認鍵（ＫＣＫ）部分を用いて保護されている、請求項１１記載の装置。

【請求項１５】
前記第２のＰＴＫは、前記第２のＡＮｏｎｃｅ、前記ＳＮｏｎｃｅ、および再認証マスタ・セッション鍵（ｒＭＳＫ）に基づいて生成される、請求項１１記載の装置。
【請求項１６】
、
前記認証応答は、少なくとも前記第２のＰＴＫの鍵確認鍵（ＫＣＫ）部分、前記第２のＰＴＫの鍵暗号鍵（ＫＥＫ）部分、またはこれらの組み合わせを用いて保護されている、請求項１１記載の装置。
【請求項１７】
装置であって、
モバイル・デバイスにおいて、アクセス・ポイントから、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を受信する手段と、
前記第１のＡＮｏｎｃｅを用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成する手段と、
認証要求を前記アクセス・ポイントへ送信する手段と、ここで、前記認証要求は、局ノンス（ＳＮｏｎｃｅ）を含み、前記認証要求は、前記第１のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記アクセス・ポイントから認証応答を受信する手段と、ここで、前記認証応答は、第２のＡＮｏｎｃｅを含み、第２のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記第２のＡＮｏｎｃｅおよび前記ＳＮｏｎｃｅを用いて、前記第２のＰＴＫを生成する手段と、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いる手段と、
を備える装置。
【請求項１８】
前記第１のＡＮｏｎｃｅは、ビーコンによって受信される、請求項１７記載の装置。
【請求項１９】
前記第１のＡＮｏｎｃｅは、プローブ応答によって受信される、請求項１７記載の装置。
【請求項２０】
前記第１のＰＴＫは、前記第１のＡＮｏｎｃｅ、前記ＳＮｏｎｃｅ、および再認証マスタ・セッション鍵（ｒＭＳＫ）を用いて生成される、請求項１７記載の装置。
【請求項２１】
前記認証要求は、前記第１のＡＮｏｎｃｅをさらに含む、請求項１７記載の装置。
【請求項２２】
前記第２のＰＴＫは、前記第２のＡＮｏｎｃｅ、前記ＳＮｏｎｃｅ、および再認証マスタ・セッション鍵（ｒＭＳＫ）を用いて生成される、請求項１７記載の装置。
【請求項２３】
前記認証要求は、前記第１のＰＴＫのうちの少なくとも鍵確認鍵（ＫＣＫ）部分を用いて保護されている、請求項１７記載の装置。
【請求項２４】
前記認証応答は、少なくとも前記第２のＰＴＫの鍵確認鍵（ＫＣＫ）部分、前記第２のＰＴＫの鍵暗号鍵（ＫＥＫ）部分、またはこれらの組み合わせを用いて保護されている、請求項１７記載の装置。
【請求項２５】
プロセッサによって実行された場合、前記プロセッサに対して、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべき第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスからの認証要求によって受信された前記第１のＡＮｏｎｃｅお

よび局ノンス（ＳＮｏｎｃｅ）に基づいて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、ここで、前記認証要求は、前記第１のＰＴＫを用いて保護されている、

第２のＡＮｏｎｃｅを生成することと、

前記第２のＡＮｏｎｃｅおよび前記ＳＮｏｎｃｅに基づいて第２のＰＴＫを生成することと、

前記モバイル・デバイスへ送信されるべき認証応答を生成することと、ここで、前記認証応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。

【請求項２６】

前記第１のＡＮｏｎｃｅは、ビーコンによって前記モバイル・デバイスに送信される、請求項２５記載の非一時的なプロセッサ読取可能な媒体。

【請求項２７】

前記第１のＡＮｏｎｃｅは、プローブ応答によって前記モバイル・デバイスに送信される、請求項２５記載の非一時的なプロセッサ読取可能な媒体。

【請求項２８】

前記認証要求は、前記第１のＰＴＫのうちの少なくとも鍵確認鍵（ＫＣＫ）部分を用いて保護されている、請求項２５記載の非一時的なプロセッサ読取可能な媒体。

【請求項２９】

前記第２のＰＴＫは、前記第２のＡＮｏｎｃｅ、前記ＳＮｏｎｃｅ、および再認証マスタ・セッション鍵（ｒＭＳＫ）に基づいて生成される、請求項２５記載の非一時的なプロセッサ読取可能な媒体。

【請求項３０】

、

前記認証応答は、少なくとも前記第２のＰＴＫの鍵確認鍵（ＫＣＫ）部分、前記第２のＰＴＫの鍵暗号鍵（ＫＥＫ）部分、またはこれらの組み合わせを用いて保護されている、請求項２５記載の非一時的なプロセッサ読取可能な媒体。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】０１５５

【補正方法】変更

【補正の内容】

【０１５５】

本明細書に記載された発明のさまざまな特徴は、本発明から逸脱することなく、別のシステムにおいて実現されうる。前述した実施形態は、単なる例であり、本発明を限定するものとして解釈されるべきではないことが注目されるべきである。実施形態の記載は、例示であって、請求項の範囲を制限するものではことが意図されている。そのため、本教示は、その他のタイプの装置および多くの代替例、修正、および変更が、当業者に明らかになるだろう。

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。

［１］　方法であって、

モバイル・デバイスからアクセス・ポイントへ、保護されていない関連付け要求を送信することと、

前記アクセス・ポイントから、関連付け応答を受信することと、ここで、前記関連付け応答は、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を含む、

前記モバイル・デバイスにおいて、前記ＡＮｏｎｃｅを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、

を備える方法。

［２］　前記モバイル・デバイスにおいて、前記保護されていない関連付け要求を前記アクセス・ポイントへ送信する前に、再認証マスタ・セッション鍵（ｒＭＳＫ）および局

ノンス（ＳＮｏｎｃｅ）を生成することをさらに備え、
前記ＰＴＫは、前記ｒＭＳＫおよび前記ＳＮｏｎｃｅを用いて生成される、［１］に記載の方法。
［３］ 前記モバイル・デバイスのメモリから、前記アクセス・ポイントの基本サービス・セット識別子（ＢＳＳＩＤ）を検索することをさらに備え、
前記保護されていない関連付け要求は、前記ＢＳＳＩＤに基づいて前記アクセス・ポイントへ送信される、［１］に記載の方法。
［４］ 前記モバイル・デバイスにおいて位置情報が決定されることに応じて、前記保護されていない関連付け要求が送信される、［１］に記載の方法。
［５］ 前記ＡＮｏｎｃｅ以外の、前記関連付け要求における情報要素が、前記ＡＮｏｎｃｅを用いて保護され、
前記方法はさらに、前記ＰＴＫを用いて、前記関連付け応答の保全性を検証すること、を備える［１］に記載の方法。
［６］ 装置であって、
プロセッサと、
アクセス・ポイントへ、保護されていない関連付け要求を送信することと、
前記アクセス・ポイントから、関連付け応答を受信することと、ここで、前記関連付け応答は、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を含む、
前記ＡＮｏｎｃｅを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
［７］ 前記命令群はさらに、前記保護されていない関連付け要求を前記アクセス・ポイントへ送信する前に、再認証マスタ・セッション鍵（ｒＭＳＫ）および局ノンス（ＳＮｏｎｃｅ）を生成することのために前記プロセッサによって実行可能であり、
前記ＰＴＫは、前記ｒＭＳＫおよび前記ＳＮｏｎｃｅを用いて生成される、［６］に記載の装置。
［８］ 前記メモリはさらに、前記アクセス・ポイントの基本サービス・セット識別子（ＢＳＳＩＤ）を格納し、
前記命令群はさらに、前記メモリから前記アクセス・ポイントのＢＳＳＩＤを検索することのために前記プロセッサによって実行可能であり、
前記保護されていない関連付け要求は、前記ＢＳＳＩＤに基づいて前記アクセス・ポイントへ送信される、［６］に記載の装置。
［９］ 装置であって、
モバイル・デバイスからアクセス・ポイントへ、保護されていない関連付け要求を送信する手段と、
前記アクセス・ポイントから関連付け応答を受信する手段と、ここで、前記関連付け応答は、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を含む、
前記モバイル・デバイスにおいて、前記ＡＮｏｎｃｅを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成する手段と、
を備える装置。
［１０］ プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスによってアクセス・ポイントへ送信されるべき、保護されていない関連付け要求を生成することと、
前記アクセス・ポイントからの関連付け応答から検索されたアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
［１１］ 方法であって、
アクセス・ポイントにおいて、モバイル・デバイスから、保護されていない関連付け要

求を受信することと、
前記保護されていない関連付け要求から、開始メッセージを抽出することと、
前記開始メッセージを、認証サーバへ送信することと、
前記認証サーバから、回答メッセージを受信することと、ここで、前記回答メッセージは、再認証マスタ・セッション鍵（ｒＭＳＫ）を含む、
アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスへ、関連付け応答を送信することと、ここで、前記関連付け応答は、前記ＡＮｏｎｃｅを含む、
を備える方法。
［１２］　前記アクセス・ポイントにおいて、前記保護されていない関連付け要求に含まれる局ノンス（ＳＮｏｎｃｅ）、前記ＡＮｏｎｃｅ、および前記ｒＭＳＫを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することをさらに備え、
前記関連付け応答は、前記ＰＴＫを用いて保護されている、［１１］に記載の方法。
［１３］　装置であって、
プロセッサと、
モバイル・デバイスから、保護されていない関連付け要求を受信することと、
前記保護されていない関連付け要求から、開始メッセージを抽出することと、
前記開始メッセージを、認証サーバへ送信することと、
前記認証サーバから、回答メッセージを受信することと、ここで、前記回答メッセージは、再認証マスタ・セッション鍵（ｒＭＳＫ）を含む、
アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスへ関連付け応答を送信することと、ここで、前記関連付け応答は、前記ＡＮｏｎｃｅを含む、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
［１４］　前記命令群はさらに、前記保護されていない関連付け要求に含まれる局ノンス（ＳＮｏｎｃｅ）、前記ＡＮｏｎｃｅ、および前記ｒＭＳＫを用いて、ペアワイズ・トランジェント鍵（ＰＴＫ）を生成することのために前記プロセッサによって実行可能であり、
前記関連付け応答は、前記ＰＴＫを用いて保護されている、［１３］に記載の装置。
［１５］　装置であって、
アクセス・ポイントにおいて、モバイル・デバイスから、保護されていない関連付け要求を受信する手段と、
前記保護されていない関連付け要求から、開始メッセージを抽出する手段と、
前記開始メッセージを、認証サーバへ送信する手段と、
前記認証サーバから、回答メッセージを受信する手段と、ここで、前記回答メッセージは、再認証マスタ・セッション鍵（ｒＭＳＫ）を含む、
アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成する手段と、
前記アクセス・ポイントから前記モバイル・デバイスへ、関連付け応答を送信する手段と、ここで、前記関連付け応答は、前記ＡＮｏｎｃｅを含む、
を備える装置。
［１６］　プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスから受信された、保護されていない関連付け要求から、開始メッセージを抽出することと、
前記開始メッセージに応じて、認証サーバから受信された回答メッセージから再認証マスタ・セッション鍵（ｒＭＳＫ）を抽出することと、
アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスへ送信されるべき関連付け応答を生成することと、ここで、前記関連付け応答は、前記ＡＮｏｎｃｅを含む、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。

［１７］　方法であって、
モバイル・デバイスにおいて、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、アクセス・ポイントとの第１のリンク設定を開始することと、
前記アクセス・ポイントとの第１のリンク設定中、前記第１のリンク設定に後続する、前記アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信することと、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
を備える方法。
［１８］　前記第１のＡＮｏｎｃｅは、前記モバイル・デバイスのメモリから検索されるか、前記アクセス・ポイントからビーコンまたはプローブ応答で受信されるか、これら任意の組み合わせで取得される、［１７］に記載の方法。
［１９］　前記第２のＡＮｏｎｃｅは、関連付け応答で、拡張可能認証プロトコル（ＥＡＰ）オーバ・ローカル・エリア・ネットワーク（ＬＡＮ）（ＥＡＰＯＬ）メッセージで、または、これら任意の組み合わせで受信される、［１７］に記載の方法。
［２０］　前記第２のＡＮｏｎｃｅは、有効性寿命を有する、［１７］に記載の方法。
［２１］　前記後続するリンク設定の開始前に、前記第２のＡＮｏｎｃｅの有効性寿命が終了した場合、
ビーコンまたはプローブ応答で第３のＡＮｏｎｃｅを受信することと、
前記第３のＡＮｏｎｃｅを用いて前記第２のリンク設定を開始することと、
前記第２のリンク設定中、前記アクセス・ポイントとの第３のリンク設定に用いるための第４のＡＮｏｎｃｅを受信することと、
をさらに備える［２０］に記載の方法。
［２２］　前記モバイル・デバイスにおいて、前記第２のＡＮｏｎｃｅを用いて、前記アクセス・ポイントとの第２のリンク設定を開始することと、
前記アクセス・ポイントとの第２のリンク設定中、前記アクセス・ポイントとの、後続する第３のリンク設定において用いるための第３のＡＮｏｎｃｅを受信することと、
をさらに備える［１７］に記載の方法。
［２３］　装置であって、
プロセッサと、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、アクセス・ポイントとの第１のリンク設定を開始することと、
前記アクセス・ポイントとの第１のリンク設定中、前記第１のリンク設定に後続する、前記アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信することと、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
［２４］　前記第１のＡＮｏｎｃｅは、前記メモリから検索されるか、前記アクセス・ポイントからビーコンまたはプローブ応答で受信されるか、これら任意の組み合わせで取得され、
前記第２のＡＮｏｎｃｅは、関連付け応答で、拡張可能認証プロトコル（ＥＡＰ）オーバ・ローカル・エリア・ネットワーク（ＬＡＮ）（ＥＡＰＯＬ）メッセージで、または、これら任意の組み合わせで受信される、［２３］に記載の装置。
［２５］　前記第２のＡＮｏｎｃｅは、有効性寿命を有する、［２３］に記載の装置。
［２６］　前記命令群はさらに、
前記後続するリンク設定の開始前に、前記第２のＡＮｏｎｃｅの有効性寿命が終了した場合、
ビーコンまたはプローブ応答で第３のＡＮｏｎｃｅを受信することと、
前記第３のＡＮｏｎｃｅを用いて前記第２のリンク設定を開始することと、
前記第２のリンク設定中、前記アクセス・ポイントとの第３のリンク設定に用いるための第４のＡＮｏｎｃｅを受信することと、

のために前記プロセッサによって実行可能である、［２５］に記載の装置。
［２７］　前記命令群はさらに、
前記第２のＡＮｏｎｃｅを用いて、前記アクセス・ポイントとの第２のリンク設定を開始することと、
前記アクセス・ポイントとの第２のリンク設定中、前記アクセス・ポイントとの、後続する第３のリンク設定に用いるための第３のＡＮｏｎｃｅを受信することと、
のために前記プロセッサによって実行可能である、［２３］に記載の装置。
［２８］　装置であって、
モバイル・デバイスにおいて、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、アクセス・ポイントとの第１のリンク設定を開始する手段と、
前記アクセス・ポイントとの第１のリンク設定中、前記第１のリンク設定に後続する、前記アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信する手段と、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
を備える装置。
［２９］　プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスにおいて、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、アクセス・ポイントとの第１のリンク設定を開始することと、
前記アクセス・ポイントとの第１のリンク設定中、前記第１のリンク設定に後続する、前記アクセス・ポイントとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを受信することと、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
［３０］　方法であって、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いる第１のリンク設定中に、アクセス・ポイントからモバイル・デバイスへ、前記第１のリンク設定に後続する、前記モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを送信することを備え、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
方法。
［３１］　前記第１のリンク設定の開始前に、前記第１のＡＮｏｎｃｅを、ビーコンまたはプローブ応答で、前記モバイル・デバイスへ送信すること、をさらに備える［３０］に記載の方法。
［３２］　前記第２のＡＮｏｎｃｅは、前記モバイル・デバイスへ、関連付け応答で、拡張可能認証プロトコル（ＥＡＰ）オーバ・ローカル・エリア・ネットワーク（ＬＡＮ）（ＥＡＰＯＬ）メッセージで、または、これら任意の組み合わせで送信される、［３０］に記載の方法。
［３３］　前記第２のＡＮｏｎｃｅは、有効性寿命に関連付けられる、［３０］に記載の方法。
［３４］　装置であって、
プロセッサと、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いる第１のリンク設定中、前記第１のリンク設定に後続する、前記モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅをモバイル・デバイスへ送信すること、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
［３５］　前記命令群は、前記第１のリンク設定の開始前に、前記第１のＡＮｏｎｃｅをビーコンまたはプローブ応答によって前記モバイル・デバイスへ送信することのために前記プロセッサによってさらに実行可能である、［３４］に記載の装置。
［３６］　前記第２のＡＮｏｎｃｅは、前記モバイル・デバイスへ、関連付け応答で、拡張可能認証プロトコル（ＥＡＰ）オーバ・ローカル・エリア・ネットワーク（ＬＡＮ）（ＥＡＰＯＬ）メッセージで、または、これら任意の組み合わせで送信される、［３４］

に記載の装置。
［３７］　前記第２のＡＮｏｎｃｅは、有効性寿命に関連付けられる、［３４］に記載の装置。
［３８］　装置であって、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いる第１のリンク設定中に、アクセス・ポイントからモバイル・デバイスへ、前記第１のリンク設定に後続する、前記モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを送信する手段と、
前記第１のリンク設定の開始前に、前記第１のＡＮｏｎｃｅを、ビーコンまたはプローブ応答で、前記モバイル・デバイスへ送信する手段と、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、
を備える装置。
［３９］　プロセッサによって実行された場合、前記プロセッサに対して、
第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いる第１のリンク設定中に、アクセス・ポイントからモバイル・デバイスへ、前記第１のリンク設定に後続する、前記モバイル・デバイスとの第２のリンク設定に用いるための第２のＡＮｏｎｃｅを送信させる命令群を備え、ここで、前記第２のＡＮｏｎｃｅは、前記第１のＡＮｏｎｃｅとは異なる、非一時的なプロセッサ読取可能な媒体。
［４０］　方法であって、
モバイル・デバイスにおいて、アクセス・ポイントから、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を受信することと、
前記第１のＡＮｏｎｃｅを用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
前記アクセス・ポイントへ、関連付け要求を送信することと、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記アクセス・ポイントから関連付け応答を受信することと、ここで、前記関連付け応答は、第２のＡＮｏｎｃｅを含み、第２のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅを用いて、前記第２のＰＴＫを生成することと、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いることと、
を備える方法。
［４１］　方法であって、
アクセス・ポイントからモバイル・デバイスへ第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を送信することと、
前記モバイル・デバイスから、関連付け要求を受信することと、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を用いて保護されている、
前記アクセス・ポイントにおいて、前記第１のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて、前記第１のＰＴＫを生成することと、
第２のＡＮｏｎｃｅを生成することと、
前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて、第２のＰＴＫを生成することと、
前記モバイル・デバイスへ、関連付け応答を送信することと、ここで、前記関連付け応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
を備える方法。
［４２］　装置であって、
プロセッサと、

モバイル・デバイスにおいて、アクセス・ポイントから受信された第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき関連付け要求を生成することと、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
前記アクセス・ポイントから、関連付け応答によって受信された第２のＡＮｏｎｃｅおよび前記ＳＮｏｎｃｅを用いて第２のＰＴＫを生成することと、ここで、前記関連付け応答は、前記第２のＰＴＫを用いて保護されている、
前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いることと、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
［４３］　装置であって、
プロセッサと、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべき第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスからの関連付け要求によって受信された局ノンス（ＳＮｏｎｃｅ）および前記第１のＡＮｏｎｃｅに基づいて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、ここで、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
第２のＡＮｏｎｃｅを生成することと、
前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて第２のＰＴＫを生成することと、
前記モバイル・デバイスへ送信されるべき関連付け応答を生成することと、ここで、前記関連付け応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
［４４］　プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスにおいて、アクセス・ポイントから受信された第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき関連付け要求を生成することと、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、
前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
前記アクセス・ポイントから、関連付け応答によって受信された第２のＡＮｏｎｃｅおよび前記ＳＮｏｎｃｅを用いて第２のＰＴＫを生成することと、ここで、前記関連付け応答は、前記第２のＰＴＫを用いて保護されている、
前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いることと、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
［４５］　プロセッサによって実行された場合、前記プロセッサに対して、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべき第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記モバイル・デバイスからの関連付け要求によって受信された前記第１のＡＮｏｎｃｅおよび局ノンス（ＳＮｏｎｃｅ）に基づいて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成することと、ここで、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
第２のＡＮｏｎｃｅを生成することと、

前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて第２のＰＴＫを生成することと、
前記モバイル・デバイスへ送信されるべき関連付け応答を生成することと、ここで、前記関連付け応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
［４６］　装置であって、
モバイル・デバイスにおいて、アクセス・ポイントから、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を受信する手段と、
前記第１のＡＮｏｎｃｅを用いて、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を生成する手段と、
関連付け要求を前記アクセス・ポイントへ送信する手段と、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、前記関連付け要求は、前記第１のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記アクセス・ポイントから関連付け応答を受信する手段と、ここで、前記関連付け応答は、第２のＡＮｏｎｃｅを含み、第２のＰＴＫを用いて保護されている、
前記モバイル・デバイスにおいて、前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅを用いて、前記第２のＰＴＫを生成する手段と、
前記モバイル・デバイスから前記アクセス・ポイントへ送信されるべき少なくとも１つの後続するメッセージを保護するために前記第２のＰＴＫを用いる手段と、
を備える装置。
［４７］　装置であって、
アクセス・ポイントから、モバイル・デバイスへ、第１のアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を送信する手段と、
前記モバイル・デバイスから、関連付け要求を受信する手段と、ここで、前記関連付け要求は、局ノンス（ＳＮｏｎｃｅ）を含み、第１のペアワイズ・トランジェント鍵（ＰＴＫ）を用いて保護されている、
前記アクセス・ポイントにおいて、前記第１のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて、前記第１のＰＴＫを生成する手段と、
第２のＡＮｏｎｃｅを生成する手段と、
前記第２のＡＮｏｎｃｅおよびＳＮｏｎｃｅに基づいて第２のＰＴＫを生成する手段と、
前記モバイル・デバイスへ、関連付け応答を送信する手段と、ここで、前記関連付け応答は、前記第２のＡＮｏｎｃｅを含み、前記第２のＰＴＫを用いて保護されている、
を備える装置。
［４８］　方法であって、
モバイル・デバイスにおいて、アクセス・ポイントから、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を受信することと、
前記モバイル・デバイスにおいて、前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスおよび前記ＡＮｏｎｃｅシードに基づいて、ＡＮｏｎｃｅを生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記アクセス・ポイントとのリンク設定を実行することと、
を備える方法。
［４９］　方法であって、
アクセス・ポイントから、モバイル・デバイスへ、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を送信することと、
前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスを受信することと、
前記モバイル・デバイスのＭＡＣアドレスおよび前記ＡＮｏｎｃｅシードに基づいてＡ

Ｎｏｎｃｅを生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記モバイル・デバイスとのリンク設定を実行することと、
を備える方法。
［５０］　装置であって、
プロセッサと、
モバイル・デバイスにおいて、アクセス・ポイントから受信したアクセス・ポイント・ノンス・シード（ＡＮｏｎｃｅシード）および前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスに基づいて、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記アクセス・ポイントとのリンク設定を実行することと
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
［５１］　装置であって、
プロセッサと、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべきアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を生成することと、
前記モバイル・デバイスから受信された前記モバイル・デバイスのＭＡＣアドレスおよび前記ＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記モバイル・デバイスとのリンク設定を実行することと、
のために前記プロセッサによって実行可能な命令群を格納するメモリと、
を備える装置。
［５２］　プロセッサによって実行された場合、前記プロセッサに対して、
モバイル・デバイスにおいて、アクセス・ポイントから受信したアクセス・ポイント・ノンス・シード（ＡＮｏｎｃｅシード）および前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスに基づいて、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）を生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記アクセス・ポイントとのリンク設定を実行することと、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
［５３］　プロセッサによって実行された場合、前記プロセッサに対して、
アクセス・ポイントにおいて、モバイル・デバイスへ送信されるべきアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を生成することと、
前記モバイル・デバイスから受信された前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスおよび前記ＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを生成することと、
前記生成されたＡＮｏｎｃｅに基づいて、前記モバイル・デバイスとのリンク設定を実行することと、
をさせる命令群を備える非一時的なプロセッサ読取可能な媒体。
［５４］　装置であって、
モバイル・デバイスにおいて、アクセス・ポイントからアクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を受信する手段と、
前記モバイル・デバイスにおいて、前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスおよび前記ＡＮｏｎｃｅシードに基づいて、ＡＮｏｎｃｅを生成する手段と、
前記生成されたＡＮｏｎｃｅに基づいて、前記アクセス・ポイントとのリンク設定を実行する手段と、
を備える装置。

［５５］　装置であって、
アクセス・ポイントから、モバイル・デバイスへ、アクセス・ポイント・ノンス（ＡＮｏｎｃｅ）シード（ＡＮｏｎｃｅシード）を送信する手段と、
前記モバイル・デバイスの媒体アクセス制御（ＭＡＣ）アドレスを受信する手段と、
前記モバイル・デバイスのＭＡＣアドレスおよび前記ＡＮｏｎｃｅシードに基づいてＡＮｏｎｃｅを生成する手段と、
前記生成されたＡＮｏｎｃｅに基づいて、前記モバイル・デバイスとのリンク設定を実行する手段と、
を備える装置。

フロントページの続き

(31)優先権主張番号 61/606,794
(32)優先日 平成24年3月5日(2012.3.5)
(33)優先権主張国 米国(US)
(31)優先権主張番号 61/611,553
(32)優先日 平成24年3月15日(2012.3.15)
(33)優先権主張国 米国(US)
(31)優先権主張番号 61/645,987
(32)優先日 平成24年5月11日(2012.5.11)
(33)優先権主張国 米国(US)
(31)優先権主張番号 13/610,730
(32)優先日 平成24年9月11日(2012.9.11)
(33)優先権主張国 米国(US)

(72)発明者 ジョージ・シェリアン
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
(72)発明者 フィリップ・マイケル・ホークス
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 サントシュ・ポール・アブラハム
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 ヘマンス・サンパス
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

Ｆターム(参考) 5J104 AA07 AA16 AA32 EA04 EA18 JA03 KA02 NA02 NA12 NA36
NA37 NA38 PA01
5K067 DD17 EE02 EE10

【外国語明細書】
2016136724000001.pdf