(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-541831
(P2024-541831A)
(43)公表日　令和6年11月13日(2024.11.13)

(51)国際特許分類		FI		テーマコード（参考）
H04W 12/043(2021.01)		H04W	12/043	5K067
H04W 12/041(2021.01)		H04W	12/041	

審査請求　未請求　予備審査請求　未請求　（全44頁）

(21)出願番号　特願2024-521794(P2024-521794)
(86)(22)出願日　令和4年10月28日(2022.10.28)
(85)翻訳文提出日　令和6年4月10日(2024.4.10)
(86)国際出願番号　PCT/US2022/048150
(87)国際公開番号　WO2023/076545
(87)国際公開日　令和5年5月4日(2023.5.4)
(31)優先権主張番号　63/273,997
(32)優先日　令和3年10月31日(2021.10.31)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　18/050,028
(32)優先日　令和4年10月26日(2022.10.26)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA
最終頁に続く

(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　110003708
弁理士法人鈴榮特許綜合事務所
(72)発明者　エスコット、エイドリアン・エドワード
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(72)発明者　パラニゴウンダー、アナンド
アメリカ合衆国、カリフォルニア州　９
最終頁に続く

(54)【発明の名称】　鍵の再ネゴシエーションの必要性を示すための汎用ブートストラッピングアーキテクチャ（ＧＢＡ）シグナリング

(57)【要約】
事前共有鍵（ＰＳＫ）再ネゴシエーションをサポートするための実施形態の方法において、ユーザ機器（ＵＥ）は、第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、を含む要求メッセージを生成し、その要求メッセージをネットワークデバイスに送信することができる。ネットワークデバイスは、ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定したことに応答して、第１の相関ＰＳＫ名前空間のためのＰＳＫ再ネゴシエーションの表示を決定し、第１の相関ＰＳＫ名前空間のためのＰＳＫ再ネゴシエーションの表示を含む応答メッセージを生成し、その応答メッセージをＵＥに送信することができる。それに応答して、ＵＥは、第２のＢ－ＴＩＤ及び第２の（すなわち、新しい）セッション鍵（Ｋｓ）を取得するために、ブートストラッピング手順を実行することができる。

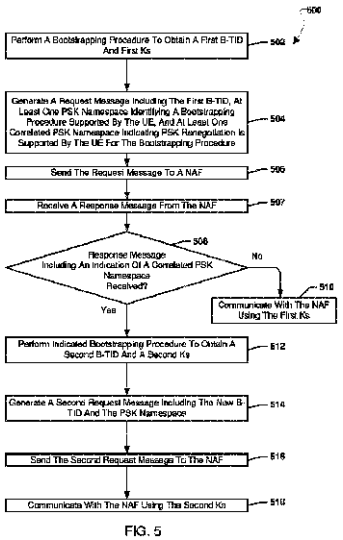


FIG. 5

【特許請求の範囲】
【請求項１】
ユーザ機器（ＵＥ）によって実行される方法であって、
第１の要求メッセージを生成することであって、前記第１の要求メッセージが、
第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、
前記ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１の事前共有鍵（ＰＳＫ）名前空間と、
前記第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、
を含む、生成することと、
前記第１の要求メッセージをネットワークアプリケーション機能（ＮＡＦ）に送信することと、
を含む、方法。
【請求項２】
前記第１の相関ＰＳＫ名前空間の表示を含む応答メッセージを前記ＮＡＦから受信することと、
前記応答メッセージを受信することに基づいて、第２のＢ－ＴＩＤ及びセッション鍵（Ｋｓ）を取得するためにブートストラッピング手順を実行することと、
を更に含む、請求項１に記載の方法。
【請求項３】
前記ブートストラッピング手順を実行することが、前記第２のＢ－ＴＩＤ及び第２のセッション鍵（Ｋｓ）を取得するために前記第１のブートストラッピング手順を再実行することを含む、請求項２に記載の方法。
【請求項４】
前記第２のＢ－ＴＩＤと前記第１の相関ＰＳＫ名前空間とを含む第２の要求メッセージを生成することと、
前記第２の要求メッセージを前記ＮＡＦに送信することと、
を更に含む、請求項２に記載の方法。
【請求項５】
前記第１の相関ＰＳＫ名前空間の前記表示が、前記第１の相関ＰＳＫ名前空間である、請求項２に記載の方法。
【請求項６】
前記第１の相関ＰＳＫ名前空間の前記表示が、前記第１の相関ＰＳＫ名前空間のインデックスである、又はリスト内の前記第１の相関ＰＳＫ名前空間の位置である、請求項２に記載の方法。
【請求項７】
前記第２のＫｓを使用して前記ＮＡＦと通信すること、
を更に含む、請求項２に記載の方法。
【請求項８】
前記第１の要求メッセージが、
前記ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、
前記第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間と、
を更に含む、請求項１に記載の方法。
【請求項９】
前記第１の要求メッセージが、クライアントが開始するハローメッセージである、請求項１に記載の方法。
【請求項１０】
ネットワークデバイスによって実行される方法であって、

前記ネットワークデバイスによって、ユーザ機器（ＵＥ）から、第１の要求メッセージを受信することであって、前記第１の要求メッセージが、
第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、
前記ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１の事前共有鍵（ＰＳＫ）名前空間と、
前記第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、
を含む、受信することと、
前記第１の要求メッセージを受信した後に、前記ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定することと、
前記ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定したことに応答して、前記第１の相関ＰＳＫ名前空間の表示を決定することと、
前記第１の相関ＰＳＫ名前空間の前記表示を含む応答メッセージを生成することと、
前記応答メッセージを前記ＵＥに送信することと、
を含む、方法。
【請求項１１】
前記第１の相関ＰＳＫ名前空間の前記表示が、前記第１の相関ＰＳＫ名前空間である、請求項１０に記載の方法。
【請求項１２】
前記第１の相関ＰＳＫ名前空間の前記表示が、前記第１の相関ＰＳＫ名前空間のインデックスである、又はリスト内の前記第１の相関ＰＳＫ名前空間の位置である、請求項１０に記載の方法。
【請求項１３】
第２のＢ－ＴＩＤ及び前記第１の相関ＰＳＫ名前空間のみを含む第２の要求メッセージを、前記ＵＥから前記ネットワークデバイスによって受信すること、
を更に含む、請求項１０に記載の方法。
【請求項１４】
前記第２のＢ－ＴＩＤを使用してブートストラッピングセキュリティ機能（ＢＳＦ）から取得されたセッション鍵（Ｋｓ）を使用して前記ＵＥと通信すること、
を更に含む、請求項１３に記載の方法。
【請求項１５】
前記第１の要求メッセージが、
前記ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、
前記第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間と、を更に含み、
前記第１の要求メッセージを受信した後に前記ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定することが、
前記ＵＥによってサポートされる前記第１のブートストラッピング手順及び前記ＵＥによってサポートされる前記第２のブートストラッピング手順の選択肢から、前記ＵＥによってサポートされる前記第１のブートストラッピング手順を選択することと、
前記第１のブートストラッピング手順のために再ネゴシエーションが必要であると判定することと、
前記ＵＥによってサポートされる前記第１のブートストラッピング手順を選択したことに応答して、前記第１の相関ＰＳＫ名前空間の前記表示を決定することと、
を含む、
請求項１０に記載の方法。
【請求項１６】
前記応答メッセージが、サーバが開始するハローメッセージである、請求項１０に記載の方法。

【請求項１７】
前記ネットワークデバイスがネットワークアプリケーション機能（ＮＡＦ）サーバである、請求項１０に記載の方法。
【請求項１８】
ユーザ機器（ＵＥ）であって、
トランシーバと、
前記トランシーバに結合されたプロセッサと、
を備え、前記プロセッサが、
第１の要求メッセージであって、
第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、
前記ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１の事前共有鍵（ＰＳＫ）名前空間と、
前記第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、
を含む、第１の要求メッセージを生成し、
前記トランシーバを介してネットワークアプリケーション機能（ＮＡＦ）に前記第１の要求メッセージを送信する、
ように構成されている、
ユーザ機器（ＵＥ）。
【請求項１９】
前記プロセッサが、
前記第１の相関ＰＳＫ名前空間の表示を含む応答メッセージを前記ＮＡＦから受信し、
前記応答メッセージを受信することに基づいて、第２のＢ－ＴＩＤ及びセッション鍵（Ｋｓ）を取得するためにブートストラッピング手順を実行する、
ように更に構成されている、
請求項１８に記載のＵＥ。
【請求項２０】
前記プロセッサが、前記第２のＢ－ＴＩＤ及び第２のセッション鍵（Ｋｓ）を取得するために前記第１のブートストラッピング手順を再実行することによって、別のブートストラッピング手順を実行するように更に構成されている、請求項１９に記載のＵＥ。
【請求項２１】
前記プロセッサが、
前記第２のＢ－ＴＩＤと前記第１の相関ＰＳＫ名前空間とを含む第２の要求メッセージを生成し、
前記トランシーバを介して前記ＮＡＦに前記第２の要求メッセージを送信する、
ように更に構成されている、
請求項１９に記載のＵＥ。
【請求項２２】
前記第１の相関ＰＳＫ名前空間の前記表示が、前記第１の相関ＰＳＫ名前空間である、請求項１９に記載のＵＥ。
【請求項２３】
前記第１の相関ＰＳＫ名前空間の前記表示が、前記第１の相関ＰＳＫ名前空間のインデックスである、又はリスト内の前記第１の相関ＰＳＫ名前空間の位置である、請求項１９に記載のＵＥ。
【請求項２４】
前記プロセッサが、
前記第２のＫｓを使用して前記ＮＡＦと通信する、
ように更に構成されている、請求項１９に記載のＵＥ。
【請求項２５】
前記第１の要求メッセージが、

前記ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、
前記第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間と、
を更に含む、請求項１８に記載のＵＥ。
【請求項２６】
前記第１の要求メッセージが、クライアントが開始するハローメッセージである、請求項１８に記載のＵＥ。
【請求項２７】
ネットワークデバイスであって、
プロセッサを備え、前記プロセッサが、
ユーザ機器（ＵＥ）から、第１の要求メッセージであって、
第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、
前記ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１の事前共有鍵（ＰＳＫ）名前空間と、
前記第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、
を含む、第１の要求メッセージを受信し、
前記第１の要求メッセージを受信した後に、前記ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定し、
前記ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定したことに応答して、前記第１の相関ＰＳＫ名前空間のためのＰＳＫ再ネゴシエーションの表示を決定し、
前記第１の相関ＰＳＫ名前空間の前記表示を含む応答メッセージを生成し、
前記応答メッセージを前記ＵＥに送信する、
ための動作を実行するように構成されている、
ネットワークデバイス。
【請求項２８】
前記第１の相関ＰＳＫ名前空間の前記表示が、前記第１の相関ＰＳＫ名前空間である、請求項２７に記載のネットワークデバイス。
【請求項２９】
前記第１の相関ＰＳＫ名前空間の前記表示が、前記第１の相関ＰＳＫ名前空間のインデックスである、又はリスト内の前記第１の相関ＰＳＫ名前空間の位置である、請求項２７に記載のネットワークデバイス。
【請求項３０】
前記プロセッサが、
第２のＢ－ＴＩＤ及び前記第１の相関ＰＳＫ名前空間のみを含む第２の要求メッセージを前記ＵＥから受信する、
ように更に構成されている、
請求項２７に記載のネットワークデバイス。
【請求項３１】
前記第２のＢ－ＴＩＤを使用してブートストラッピングセキュリティ機能（ＢＳＦ）から取得されたセッション鍵（Ｋｓ）を使用して前記ＵＥと通信すること、
を更に含む、請求項３０に記載のネットワークデバイス。
【請求項３２】
前記第１の要求メッセージが、
前記ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、
前記第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間と、
を更に含み、

前記プロセッサが、
前記ＵＥによってサポートされる前記第１のブートストラッピング手順及び前記ＵＥによってサポートされる前記第２のブートストラッピング手順の選択肢から、前記ＵＥによってサポートされる前記第１のブートストラッピング手順を選択し、
前記第１のブートストラッピング手順のために再ネゴシエーションが必要であると判定し、
前記ＵＥによってサポートされる前記第１のブートストラッピング手順を選択したことに応答して、前記第１の相関ＰＳＫ名前空間の前記表示を決定する、
ことによって、前記第１の要求メッセージを受信した後に、前記ＵＥのためにＰＳＫ再ネゴシエーションが必要であると決定するように更に構成されている、
請求項２７に記載のネットワークデバイス。
【請求項３３】
前記応答メッセージが、サーバが開始するハローメッセージである、請求項２７に記載のネットワークデバイス。
【請求項３４】
前記ネットワークデバイスがネットワークアプリケーション機能（ＮＡＦ）サーバである、請求項２７に記載のネットワークデバイス。
【請求項３５】
ユーザ機器（ＵＥ）のプロセッサに動作を実行させるように構成されたプロセッサ実行可能命令を記憶した非一時的プロセッサ可読記憶媒体であって、前記動作が、
第１の要求メッセージを生成することであって、前記第１の要求メッセージが、
第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、
前記ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１の事前共有鍵（ＰＳＫ）名前空間と、
前記第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが前記ＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、
を含む、生成することと、
前記第１の要求メッセージをネットワークアプリケーション機能（ＮＡＦ）に送信することと、
を含む、
非一時的プロセッサ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
[0001] 本出願は、２０２１年１０月３１日に出願された「Ｇｅｎｅｒｉｃ Ｂｏｏｔｓｔｒａｐｐｉｎｇ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＧＢＡ）Ｓｉｇｎａｌｉｎｇ Ｔｏ Ｉｎｄｉｃａｔｅ Ｎｅｅｄ Ｆｏｒ Ｋｅｙ Ｒｅｎｅｇｏｔｉａｔｉｏｎ」と題する米国特許出願第６３／２７３，９９７号の優先権の利益を主張し、この文書の内容全体はあらゆる目的のために参照により本明細書に組み込まれている。
【背景技術】
【０００２】
[0002] 第５世代（５Ｇ）の新無線（ＮＲ）及び他の通信技術により、ワイヤレスデバイスなどのユーザ機器（ＵＥ）との超高信頼性の低レイテンシ通信が可能になる。そのような通信システムの１つの用途は、ＵＥに様々なサービスを提供することである。いくつかのアプリケーション及びサービスは、１つ又は複数の機能を提供するために通信セキュリティを採用する、又は必要とすることがある。
【発明の概要】
【０００３】
[0003] 様々な態様は、通信をセキュアにするためにユーザ機器（ＵＥ）のプロセッ

サによって実行される方法を含む。様々な態様は、鍵の再ネゴシエーションをサポートするために汎用ブートストラッピングアーキテクチャ（ＧＢＡ）を提供するための、ＵＥのプロセッサによって実行される方法を含み得る。様々な態様は、ＵＥのプロセッサによって実行される、事前共有鍵（ＰＳＫ）再ネゴシエーションをサポートするための方法を含み得る。様々な態様は、第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、を含む、第１の要求メッセージを生成することと、第１の要求メッセージをネットワークアプリケーション機能（ＮＡＦ）に送信することと、を含むことができる。

【０００４】

［0004］ 様々な態様は、第１の相関ＰＳＫ名前空間を示す応答メッセージをＮＡＦから受信することと、応答メッセージを受信したことに基づいて、第２のＢ－ＴＩＤ及びセッション鍵（Ｋｓ）を取得するためにブートストラッピング手順を実行することと、を更に含むことができる。いくつかの態様では、ブートストラッピング手順を実行することは、第２のＢ－ＴＩＤ及び第２のセッション鍵（Ｋｓ）を取得するために第１のブートストラッピング手順を再実行することを含むことができる。いくつかの態様は、第２のＢ－ＴＩＤ及び第１の相関ＰＳＫ名前空間を含む第２の要求メッセージを生成することと、第２の要求メッセージをＮＡＦに送信することと、を更に含むことができる。いくつかの態様では、第１の相関ＰＳＫ名前空間の表示は、第１の相関ＰＳＫ名前空間であり得る。いくつかの態様では、第１の相関ＰＳＫ名前空間の表示は、第１の相関ＰＳＫ名前空間のインデックス、又はリスト内の第１の相関ＰＳＫ名前空間の位置であり得る。

【０００５】

［0005］ 様々な態様は、第２のＫｓを使用してＮＡＦと通信することを更に含むことができる。

【０００６】

［0006］ いくつかの態様では、第１の要求メッセージは、ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間と、を更に含むことができる。

【０００７】

［0007］ いくつかの態様では、第１の要求メッセージは、クライアントが開始するハローメッセージとすることができる。

【０００８】

［0008］ 更なる態様は、上記で要約した方法のうちのいずれかの１つ又は複数の動作を実行するように構成されたプロセッサを有するＵＥを含む。更なる態様は、上記で要約した方法のうちのいずれかの動作を実行するためのプロセッサ実行可能命令で構成された、ＵＥにおいて使用される処理デバイスを含む。更なる態様は、上記で要約した方法のうちのいずれかの動作をＵＥのプロセッサに実行させるように構成されたプロセッサ実行可能命令を記憶している非一時的プロセッサ可読記憶媒体を含む。更なる態様は、上記で要約した方法のうちのいずれかの機能を実行するための手段を有するＵＥを含む。更なる態様は、上記で要約した方法のうちのいずれかの１つ又は複数の動作を実行するように構成されたプロセッサを含む、ＵＥにおいて使用するためのシステムオンチップを含む。

【０００９】

［0009］ 様々な態様は、通信をセキュアにするためにネットワークデバイスのプロセッサによって実行される方法を含む。様々な態様は、鍵の再ネゴシエーションをサポートするためにＧＢＡを提供するための、ネットワークデバイスのプロセッサによって実行される方法を含むことができる。様々な態様は、ネットワークデバイスのプロセッサによって実行される、事前共有鍵（ＰＳＫ）再ネゴシエーションをサポートするための方法を含むことができる。いくつかの態様では、ネットワークデバイスは、ネットワークアプリケ

ーション機能（ＮＡＦ）サーバとすることができる。様々な態様は、第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、を含む第１の要求メッセージを、ユーザ機器（ＵＥ）からネットワークデバイスによって受信することと、第１の要求メッセージを受信した後に、ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定することと、ＰＳＫ再ネゴシエーションがＵＥのために必要であると判定したことに応答して、第１の相関ＰＳＫ名前空間のためのＰＳＫ再ネゴシエーションの表示を決定することと、第１の相関ＰＳＫ名前空間のためのＰＳＫ再ネゴシエーションの表示を含む応答メッセージを生成することと、応答メッセージをＵＥに送信することと、を含むことができる。いくつかの態様では、第１の相関ＰＳＫ名前空間の表示は、第１の相関ＰＳＫ名前空間の表示であり得る。いくつかの態様では、第１の相関ＰＳＫ名前空間の表示は、第１の相関ＰＳＫ名前空間のインデックス、又はリスト内の第１の相関ＰＳＫ名前空間の位置であり得る。

【００１０】

［0010］ 様々な態様は、第２のＢ－ＴＩＤ及び第１の相関ＰＳＫ名前空間を含む第２の要求メッセージを、ネットワークデバイスによってＵＥから受信することを更に含むことができる。

【００１１】

［0011］ 様々な態様は、第２のＢ－ＴＩＤを使用してブートストラッピングセキュリティ機能（ＢＳＦ）から取得されたセッション鍵（Ｋｓ）を使用してＵＥと通信することを更に含み得る。

【００１２】

［0012］ いくつかの態様では、第１の要求メッセージは、ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間と、を更に含むことができる。いくつかの態様では、第１の要求メッセージを受信した後に、ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定することは、ＵＥによってサポートされる第１のブートストラッピング手順を、ＵＥによってサポートされる第１のブートストラッピング手順及びＵＥによってサポートされる第２のブートストラッピング手順の選択肢から選択することと、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションが必要であると判定することと、ＵＥによってサポートされる第１のブートストラッピング手順を選択することに応答して、第１の相関ＰＳＫ名前空間の表示を決定することと、を含むことができる。いくつかの態様では、第１の相関ＰＳＫ名前空間の表示は、第１の相関ＰＳＫ名前空間であり得る。いくつかの態様では、第１の相関ＰＳＫ名前空間の表示は、第１の相関ＰＳＫ名前空間のインデックス、又はリスト内の第１の相関ＰＳＫ名前空間の位置であり得る。

【００１３】

［0013］ いくつかの態様では、応答メッセージは、サーバが開始するハローメッセージであり得る。

【００１４】

［0014］ 更なる態様は、上記で要約した方法のうちのいずれかの１つ又は複数の動作を実行するように構成されたプロセッサを有するネットワークデバイスを含む。更なる態様は、上記で要約した方法のうちのいずれかの動作を実行するためのプロセッサ実行可能命令で構成された、ネットワークデバイスにおいて使用される処理デバイスを含む。更なる態様は、上記で要約した方法のうちのいずれかの動作をネットワークデバイスのプロセッサに実行させるように構成されたプロセッサ実行可能命令を記憶した、非一時的プロセッサ可読記憶媒体を含む。更なる態様は、上記で要約した方法のうちのいずれかの機能を実行するための手段を有するネットワークデバイスを含む。更なる態様は、上記で要約した方法のうちのいずれかの１つ又は複数の動作を実行するように構成されたプロセッサを

含む、ネットワークデバイスにおいて使用されるシステムオンチップを含む。
【図面の簡単な説明】
【００１５】
［0015］ 本明細書に組み込まれるとともに本明細書の一部を構成する添付の図面は、例示的な実施形態を示し、上記で与えられた概略的な説明及び以下に与えられる詳細な説明とともに、様々な実施形態の特徴を説明するのに役立つ。
【図１Ａ】［0016］ 様々な実施形態のいずれかを実装するのに好適な、例示的な通信システムを示すシステムブロック図である。
【図１Ｂ】［0017］ 様々な実施形態のいずれかを実装するのに好適な、ワイヤレス通信システムのための例示的な分離型基地局アーキテクチャを示すシステムブロック図である。
【図２】［0018］ 様々な実施形態のいずれかを実装するのに好適な、例示的なコンピューティング及びワイヤレスモデムシステムを示す構成要素ブロック図である。
【図３】［0019］ 様々な実施形態のいずれかを実装するのに好適な、ワイヤレス通信におけるユーザ及び制御プレーンのための無線プロトコルスタックを含むソフトウェアアーキテクチャを示す構成要素ブロック図である。
【図４】［0020］ 様々な実施形態とともに使用するのに好適な、ブートストラップアプリケーションセキュリティのための例示的なシステムを示すシステムブロック図である。
【図５】［0021］ 様々な実施形態による、ＰＳＫ再ネゴシエーションをサポートするための、ＵＥのプロセッサによって実行される方法を示すプロセスフロー図である。
【図６】［0022］ 様々な実施形態による、ＰＳＫ再ネゴシエーションをサポートするための、ネットワークデバイスのプロセッサによって実行される方法を示すプロセスフロー図である。
【図７】［0023］ 様々な実施形態において使用するのに好適な、ネットワークデバイスの構成要素ブロック図である。
【図８】［0024］ 様々な実施形態において使用するのに好適な、ＵＥの構成要素ブロック図である。
【発明を実施するための形態】
【００１６】
［0025］ 添付の図面を参照しながら、様々な実施形態について詳細に説明する。可能な場合はどこでも、同じか又は同様の部分を指すために、図面全体にわたって同じ参照番号が使用される。特定の例及び実装形態に対してなされる参照は、例示を目的としており、特許請求の範囲を限定するものではない。
【００１７】
［0026］ 様々な実施形態は、汎用ブートストラッピングアーキテクチャ（ＧＢＡ）における事前共有鍵（ＰＳＫ）の再ネゴシエーションを可能にする。様々な実施形態では、ユーザ機器（ＵＥ）、及びネットワークアプリケーション機能（ＮＡＦ）サーバなどのネットワークデバイスは、１つ又は複数のＧＢＡ方法、例えば、モバイル機器（ＭＥ）ベースのＧＢＡ（ＧＢＡ＿ＭＥ）、ユニバーサル集積回路カード（ＵＩＣＣ）ベースの拡張を用いるＧＢＡ（ＧＢＡ＿Ｕ）、第２世代（２Ｇ）ＧＢＡ、ＧＢＡ＿Ｄｉｇｅｓｔ（ＧＢＡのためのセッション情報プロトコル（ＳＩＰ）ダイジェストクレデンシャルを使用する方法）など、ブートストラッピング手順のためにＰＳＫ再ネゴシエーションがいつ必要とされるかをＮＡＦが示すことを可能にする情報を通信することができる。
【００１８】
［0027］ ＵＥは、ＮＡＦサーバなどのネットワークデバイスに送信される要求メッセージ内に、ＰＳＫ名前空間と相関付けられたＰＳＫ識別情報を含めることができ、ＰＳＫ識別情報は、ＮＡＦによって選択された場合、ＮＡＦとのＧＢＡ手順を完了する前にセッション鍵を更新するためにブートストラッピング手順がＵＥによって再実行されるべきであることを示す。ブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによって実行されるべきであることを示すＰＳＫ名前空間を要求メッセージに含めることに

より、ＮＡＦサーバなどのネットワークデバイスが、セキュアな通信リンクを確立するためにＵＥと使用するブートストラッピング手順を選択することが可能になり得る。更に、ブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによって実行されるべきであることを示すＰＳＫ名前空間を要求メッセージに含めることにより、ＰＳＫ名前空間自体のコピー、ＰＳＫ名前空間のインデックス、ＰＳＫ名前空間のリスト内のＰＳＫ名前空間の位置など、ＰＳＫ名前空間の表示を単に返すことによってＰＳＫ再ネゴシエーションが実行される必要があることが示され得る。

【００１９】

［0028］ 様々な実施形態では、ＮＡＦサーバなどのネットワークデバイスは、ＧＢＡ方法（例えば、ＧＢＡ＿ＭＥ、ＧＢＡ＿Ｕ、２Ｇ ＧＢＡ、ＧＢＡ＿Ｄｉｇｅｓｔ等）など、選択されたブートストラッピング手順に関連するＰＳＫ名前空間と相関付けられたＰＳＫ再ネゴシエーションの表示を含む応答メッセージを送信することによって、新しいブートストラッピングが必要であることをユーザ機器（ＵＥ）に示すことができる。選択されたブートストラッピング手順に関連するＰＳＫ名前空間に相関付けられたＰＳＫ再ネゴシエーションの表示は、選択されたブートストラッピング手順自体に関連するＰＳＫ名前空間の表示であってもよい。選択されたブートストラッピング手順に関連するＰＳＫ名前空間に相関付けられたＰＳＫ再ネゴシエーションの表示は、選択されたブートストラッピング手順に関連するＰＳＫ名前空間のインデックスであってもよい。選択されたブートストラッピング手順に関連するＰＳＫ名前空間に相関付けられたＰＳＫ再ネゴシエーションの表示は、ＰＳＫ名前空間のリストなどのリスト内の選択されたブートストラッピング手順に関連するＰＳＫ名前空間の位置であってもよい。

【００２０】

［0029］ ブートストラッピング手順に関連するＰＳＫ名前空間と相関付けられたＰＳＫ再ネゴシエーションの表示を応答メッセージに含めることにより、ＵＥに、表示によって示される選択されたブートストラッピング手順のための新しいブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）及び新しいセッション鍵（Ｋｓ）を取得するためにブートストラッピングネゴシエーションを実行し、次いで、セキュアな通信を確立するために、新しいＢ－ＴＩＤ及び新しいＫｓを使用して、ＮＡＦサーバなどのネットワークデバイスとのブートストラッピング手順を実行するように促すことができる。特定のＧＢＡ方法を使用する鍵の再ネゴシエーションの必要性をＵＥに示す、ＮＡＦサーバなどのネットワークデバイスは、ネットワークデバイスが、ＵＥによって使用されるＫｓがフレッシュであることを保証することを可能にし得る。特定のＧＢＡ方法を使用する鍵の再ネゴシエーションの必要性をＵＥに示す、ＮＡＦサーバなどのネットワークデバイスは、ネットワークデバイスが、有効なスマートカードなどの有効なクレデンシャルがＵＥに利用可能であることを確認することを可能にし得る。

【００２１】

［0030］ 「ユーザ機器」及び「ＵＥ」という用語は、本明細書では、ワイヤレスデバイス、ワイヤレスルータデバイス、ワイヤレスアプライアンス、セルラー電話、スマートフォン、ポータブルコンピューティングデバイス、パーソナル又はモバイルマルチメディアプレーヤ、ラップトップコンピュータ、タブレットコンピュータ、スマートブック、ウルトラブック、パームトップコンピュータ、ワイヤレス電子メール受信機、マルチメディアインターネット対応セルラー電話、医療デバイス及び機器、生体センサ／デバイス、拡張現実（ＸＲ）ヘッドセット（例えば仮想現実（ＶＲ）、複合現実（ＭＲ）、又は拡張現実（ＡＲ）ヘッドセット）、スマートウォッチ、スマート衣類、スマートグラス、スマートリストバンド、スマートジュエリー（例えば、スマートリング及びスマートブレスレット）を含むウェアラブルデバイス、エンターテインメントデバイス（例えば、ワイヤレスゲームコントローラ、音楽及びビデオプレーヤ、衛星ラジオなど）、スマートメーター／センサを含むワイヤレスネットワーク対応のモノのインターネット（ＩｏＴ）デバイス、工業用製造機器、自宅又は企業使用のための大型及び小型の機械器具、自律及び半自律車両内のワイヤレス通信要素、様々なモバイルプラットフォームに固定されたか又は組み込

まれたワイヤレスデバイス、全地球測位システムデバイス、並びにメモリとワイヤレス通信構成要素とプログラマブルプロセッサとを含む同様の電子デバイスを含む、エンドポイント又はユーザデバイスのいずれか１つ又はすべてを指すために使用される。

【００２２】

［0031］「システムオンチップ」（ＳＯＣ）という用語は、単一の基板上に統合された複数のリソース又はプロセッサを含む、単一の集積回路（ＩＣ）チップを指すために、本明細書で使用される。単一のＳＯＣは、デジタル、アナログ、混合信号、及び無線周波数機能のための回路を含んでもよい。単一のＳＯＣはまた、任意の数の汎用又は専用プロセッサ（デジタル信号プロセッサ、モデムプロセッサ、ビデオプロセッサなど）、メモリブロック（ＲＯＭ、ＲＡＭ、フラッシュなど）、及びリソース（タイマー、電圧調節器、発振器など）を含み得る。ＳＯＣはまた、統合されたリソース及びプロセッサを制御するため、並びに周辺デバイスを制御するためのソフトウェアを含み得る。

【００２３】

［0032］「システムインパッケージ」（ＳＩＰ）という用語は、２つ以上のＩＣチップ、基板、又はＳＯＣ上で複数のリソース、計算ユニット、コア、又はプロセッサを含む、単一のモジュール又はパッケージを指すために、本明細書で使用され得る。例えば、ＳＩＰは、その上で複数のＩＣチップ又は半導体ダイが垂直構成で積層される、単一の基板を含み得る。同様に、ＳＩＰは、その上で複数のＩＣ又は半導体ダイが単一化基板にパッケージングされる、１つ以上のマルチチップモジュール（multi-chip module、ＭＣＭ）を含み得る。ＳＩＰはまた、単一のマザーボード上、又は単一のワイヤレスデバイス内などで、高速通信回路を介して互いに結合され、極めて近接してパッケージングされた、複数の独立したＳＯＣを含み得る。ＳＯＣの近接性によって、高速通信、並びにメモリ及びリソースの共有が容易になる。

【００２４】

［0033］本明細書で使用される「ネットワーク」、「システム」、「ワイヤレスネットワーク」、「セルラーネットワーク」、及び「ワイヤレス通信ネットワーク」という用語は、ワイヤレスデバイスに関連するキャリア及び／又はワイヤレスデバイス上のサブスクリプションのワイヤレスネットワークの一部又は全部を互換的に指し得る。本明細書で説明される技法は、符号分割多元接続（ＣＤＭＡ）、時分割多元接続（ＴＤＭＡ）、ＦＤＭＡ、直交ＦＤＭＡ（ＯＦＤＭＡ）、シングルキャリアＦＤＭＡ（ＳＣ－ＦＤＭＡ）、及び他のネットワークなど、様々なワイヤレス通信ネットワークについて使用され得る。一般に、任意の数のワイヤレスネットワークを所与の地理的エリアにおいて展開することができる。各ワイヤレスネットワークは、１つ又は複数の周波数又は周波数の範囲上で動作し得る、少なくとも１つの無線アクセス技術をサポートし得る。例えば、ＣＤＭＡネットワークは、ユニバーサル地上無線アクセス（ＵＴＲＡ）（広帯域符号分割多元接続（ＷＣＤＭＡ）規格を含む）、ＣＤＭＡ２０００（ＩＳ－２０００、ＩＳ－９５及び／又はＩＳ－８５６規格を含む）などを実装することができる。別の例では、ＴＤＭＡネットワークは、ＧＳＭエボリューションのためのＧＳＭ拡張データレート（ＥＤＧＥ）を実装することができる。別の例では、ＯＦＤＭＡネットワークは、発展型ＵＴＲＡ（Ｅ－ＵＴＲＡ）（ＬＴＥ規格を含む）、米国電気電子技術者協会（ＩＥＥＥ）８０２．１１（Ｗｉ－Ｆｉ）、ＩＥＥＥ　８０２．１６（ＷｉＭＡＸ）、ＩＥＥＥ　８０２．２０、Ｆｌａｓｈ－ＯＦＤＭ（登録商標）などを実装し得る。ＬＴＥ規格を使用するワイヤレスネットワークが参照され得、従って、「ユニバーサル地上無線アクセス」、「Ｅ－ＵＴＲＡＮ」、及び「ｅＮｏｄｅＢ」という用語はまた、ワイヤレスネットワークを指すために本明細書で互換的に使用され得る。しかしながら、そのような言及は例として提供されるにすぎず、他の通信規格を使用するワイヤレスネットワークを除外するものではない。例えば、様々な第３世代（３Ｇ）システム、第４世代（４Ｇ）システム、及び第５世代（５Ｇ）システムが本明細書で説明されるが、それらのシステムは例として言及されるにすぎず、将来の世代システム（例えば、第６世代（６Ｇ）又はより上位のシステム）が様々な例で代わりに使用され得る。

【００２５】
［0034］ いくつかのアプリケーション及びサービスは、１つ又は複数の機能を提供するために通信セキュリティを使用する、又は必要とすることがある。例えば、汎用ブートストラッピングアーキテクチャ（ＧＢＡ）は、ＵＥとネットワークデバイスとの間の共有シークレットを設定するために、第３世代パートナーシッププロジェクト（３ＧＰＰ）の認証及び鍵合意（ＡＫＡ）などのプロトコルを使用するメカニズムを提供することができる。いくつかの手法では、ＵＥ及びネットワークデバイスは、すべてのサービス及びアプリケーションによるすべての通信用に単一の共有シークレットを共有する。
【００２６】
［0035］ 様々な実施形態は、鍵の再ネゴシエーションをサポートするためにＧＢＡを提供することによって、ＵＥとネットワークデバイスとの間の通信をセキュアにするための方法を実行するように構成された方法及びコンピューティングデバイスを含む。様々な実施形態は、ＰＳＫ再ネゴシエーションをサポートするＵＥとネットワークデバイスとの間の通信をセキュアにするように構成された方法及びコンピューティングデバイスを含む。
【００２７】
［0036］ ＧＢＡブートストラッピング手順は、アプリケーションレベルでのセキュリティを提供するために、モバイル加入セキュリティ材料を使用してＵＥのための鍵を導出することを可能にする。例えば、ＧＢＡアーキテクチャでは、ブートストラッピングサーバ機能（ＢＳＦ）は、Ｕｂインターフェースを介してＵＥと通信し、Ｚｎインターフェースを介してＮＡＦと通信し得る。本明細書で使用される場合、「Ｕｂ」は、ブートストラッピングのためのＵＥ－ＢＳＦインターフェースを指す。本明細書で使用される場合、「Ｚｎ」は、汎用認証アーキテクチャ（ＧＡＡ）アプリケーションのためのＢＳＦ－ＮＡＦインターフェースを指す。ＢＳＦは、ＵＥを認証してＮＡＦに鍵を提供する、事業者のネットワーク内のネットワークエンティティであり得る。ＮＡＦは、インターネット技術タスクフォース（ＩＥＴＦ：Internet Engineering Task Force）Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ（ＲＦＣ）８４４６において定義されるトランスポート層セキュリティ（ＴＬＳ）プロトコルバージョン１．３（ＴＬＳ １．３）に従うセキュア通信など、ＵＥがセキュア通信を確立する、又は確立を試みるアプリケーションであり得る。ＢＳＦは、ＵＥ認証を可能にする加入者データを保持することができるホーム加入者サーバ（ＨＳＳ）を利用してＵＥを認証することができる。例示的なブートストラッピング手順では、ＵＥは、ＢＳＦとダイジェストＡＫＡプロトコルを実行することができる。ブートストラッピング手順は、ＵＥ及びＢＳＦが共通のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）及び鍵（Ｋｓ）を有することをもたらし得る。Ｂ－ＴＩＤは、Ｋｓを識別し得る。
【００２８】
［0037］ ＵＥは、ＢＳＦとブートストラッピング手順を実行した後、クライアント開始ハローメッセージ（例えば、本明細書で使用される場合、ＣｌｉｅｎｔＨｅｌｌｏメッセージ）などの要求メッセージの中でＢ－ＴＩＤをＮＡＦに送ることができる。ＮＡＦは、ＵＥから受信されたＢ－ＴＩＤを使用してＢＳＦに鍵を要求することができる。ＢＳＦは、ＵＥとのブートストラッピング手順中に生成されたＫｓから、ＮＡＦ固有鍵（例えば、本明細書で使用されるＫｓ＿ＮＡＦ）を生成し、ＮＡＦ固有鍵をＮＡＦに送ることができる。Ｋｓ＿ＮＡＦの導出では、ＮＡＦの完全修飾ドメイン名（ＦＱＤＮ）とＵａセキュリティプロトコル識別子とから構成され得るＮＡＦ識別子（ＩＤ）を使用することができる。Ｕａセキュリティプロトコル識別子は、異なるプロトコルのために異なる鍵が生成され、各鍵が正確に１回しか使用されないようにすることができる。本明細書で使用される場合、「Ｕａ」は、ＧＡＡアプリケーションのためのＵＥ－ＮＡＦインターフェースを指す。ＦＱＤＮは、鍵がＮＡＦに固有であることを保証することができる。
【００２９】
［0038］ いくつかのＮＡＦは、例えばＰＳＫ再ネゴシエーションを実行するために、

ブートストラッピング再ネゴシエーションをサポートするように構成され得る。ＵＥは、ＢＳＦとのブートストラッピング手順を既に実行した後、初期（又は現在の）Ｂ－ＴＩＤをＮＡＦに送信することができる。ＮＡＦは、Ｂ－ＴＩＤをＢＳＦに転送して、ＵＥとのセキュア通信を行うためのＫｓを取得することができる。しかしながら、状況によっては、ＮＡＦは、ＢＳＦから受信された鍵がセキュア通信における使用に適切でないと判定することがある。例えば、ＮＡＦは、Ｂ－ＴＩＤが古くなっていると判定することができ、ＮＡＦは、常に最初に再ネゴシエーションを要求するように構成されることができ、又はＮＡＦは、任意の他の理由でブートストラッピング再ネゴシエーションが必要であると判定することができる。従来のシステム、特にＧＢＡ鍵を使用するＴＬＳ　１．３を採用する従来のシステムでは、ＮＡＦが、新しい鍵の必要性、従ってＵＥがＢＳＦから更新された鍵を取得する必要性を、ＵＥに示す方法がない。

【００３０】

［0039］ 様々な実施形態は、ＵＥがＧＢＡ手順を使用してＮＡＦとのセキュアな通信リンクを確立する前に、ＰＳＫ再ネゴシエーションが必要であることをＮＡＦがＵＥに効率的に通知することができるメカニズムを提供する。様々な実施形態では、ＵＥは、ＮＡＦなどのネットワークデバイスに、１つ若しくは複数のＧＢＡ方法（例えば、ＧＢＡ＿ＭＥ、ＧＢＡ＿Ｕ、２Ｇ　ＧＢＡ、ＧＢＡ＿Ｄｉｇｅｓｔ等）などの１つ若しくは複数のブートストラッピング手順及び／又は１つ若しくは複数の他のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを、リストされたブートストラッピング手順に、鍵をリフレッシュする必要があるサポートされる手順に相関付けられる追加された手順を含めることによって、示すことができる。言い換えれば、サポートされるブートストラッピング手順のうちの少なくとも１つ（又は各々）について、対応するブートストラッピング再ネゴシエーション手順を、（サポートされる）ブートストラッピング手順のリストに含めることができる。

【００３１】

［0040］ 様々な実施形態では、ＮＡＦは、選択されたブートストラッピング手順と、ＮＡＦとのセキュアな通信リンクを確立するための動作を実行する前にＵＥが鍵をリフレッシュする必要性との両方について、ＵＥに通知するために、ブートストラッピング手順のリストを参照することができる。例えば、ＮＡＦは、選択されたブートストラッピング方法を示すために、ブートストラッピング手順を名前によって選択することができ、又はＮＡＦは、ブートストラッピング手順のインデックス値を選択することができ、又はＮＡＦは、リスト内のブートストラッピング手順の位置を選択することができる。これにより、ＮＡＦサーバなどのネットワークデバイスが、対応する表示（例えば、選択されたブートストラッピング方法に相関付けられる新しい鍵の必要性を示す手順の名前空間、選択されたブートストラッピング方法に相関付けられる新しい鍵の必要性を示す手順のインデックス番号、又は選択されたブートストラッピング方法に相関付けられる新しい鍵の必要性を示す手順のリスト内の位置）を単に提供するだけで、ＮＡＦが選択されたブートストラッピング方法の使用を望むこと、及びＵＥがその方法の鍵をリフレッシュする必要があることを、ＵＥに示すことが可能になる。

【００３２】

［0041］ 様々な実施形態では、ＵＥは、サポートされるブートストラッピング手順を示すＰＳＫ名前空間を、それぞれのサポートされるブートストラッピング手順のためのＰＳＫ再ネゴシエーションを示す関連付けられたＢ－ＴＩＤ及び（相関）ＰＳＫ名前空間とともに含む要求メッセージを、ＮＡＦサーバなどのネットワークデバイスに送信することができる。（追加の又は相関）ＰＳＫ名前空間及びＢ－ＴＩＤを含めることにより、ＮＡＦサーバなどのネットワークデバイスが、ＵＥとともに使用するためのＰＳＫ再ネゴシエーションのためのブートストラッピング手順を選択することが可能になり得、また、選択されたブートストラッピング手順のためにフレッシュな鍵が使用されるように、ＵＥが鍵を再ネゴシエートする必要があることが示され得る。

【００３３】

[0042] 様々な実施形態では、ＮＡＦサーバなどのネットワークデバイスは、ＧＢＡ方法（例えば、ＧＢＡ＿ＭＥ、ＧＢＡ＿Ｕ、２Ｇ ＧＢＡ、ＧＢＡ＿Ｄｉｇｅｓｔ等）など、選択されたブートストラッピング手順に関連するＰＳＫ名前空間に相関付けられる（又は対応する）ＰＳＫ再ネゴシエーションの表示を含む応答メッセージを送信することによって、新しいブートストラッピングが必要であることをＵＥに示すことができる。例えば、表示は、ＰＳＫ名前空間自体、ＰＳＫ名前空間のインデックス、又はリスト内のＰＳＫ名前空間の位置であり得る。選択されたブートストラッピング手順に関連するＰＳＫ名前空間と相関付けられるＰＳＫ再ネゴシエーションを示すことにより、ＵＥが、示されたブートストラッピング手順を実行し、ネットワークデバイスとのセキュア通信を確立するための新しいＢ－ＴＩＤ及び新しいセッション鍵（Ｋｓ）を取得することが可能になり得る。

【００３４】

[0043] 様々な実施形態では、ＵＥは、サポートされるＧＢＡ方法ごとに（相関）ＰＳＫ識別情報を示して、そのＧＢＡ方法のための再ネゴシエーションを示すことができる。例えば、ＰＳＫ識別情報（又は相関ＰＳＫ名前空間）「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」がサポートされるものとしてＵＥによって示されるとき、表示「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」が、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」方法を使用するブートストラッピングのために新しいセッション鍵（Ｋｓ）が必要とされることを示す相関ＰＳＫ識別情報として含まれ得る。同様の相関ＰＳＫ識別情報（又は名前空間）が、他のＧＢＡ方法のために含まれ得る。

【００３５】

[0044] ブートストラッピング再ネゴシエーションのために複数のＧＢＡ方法がＵＥによってサポートされるものとして示される実施形態では、以前のブートストラッピング手順（例えば、初期ブートストラッピング手順、直近のブートストラッピング手順など）において最初に使用されたものとは異なるＧＢＡ方法が、ブートストラッピング再ネゴシエーションのために利用可能であり得る。ＵＥは、ＮＡＦに送信される要求メッセージにおいて、最初に使用された以前のブートストラッピング手順のためのＰＳＫ識別情報（又はＰＳＫ名前空間）の表示に加えて、以前のブートストラッピング手順のために最初に使用されたものとは異なる１つ又は複数のＧＢＡ方法のためのそのような追加の（又は相関）ＰＳＫ識別情報（又は相関ＰＳＫ名前空間）の表示を提供することによって、以前のブートストラッピング手順のために最初に使用されたものとは異なるそのような１つ又は複数のＧＢＡ方法を示すことができる。

【００３６】

[0045] 様々な実施形態では、ＮＡＦは、この特定の選択されたＧＢＡキーイング方法を使用するために（例えば、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」を使用するために）新しいブートストラッピングの実行が必要とされることを示すために、相関ＰＳＫ識別情報（例えば、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」）など、追加の（又は相関）ＰＳＫ識別情報の表示（例えば、追加のＰＳＫ識別情報自体、追加のＰＳＫ識別情報のインデックス、リスト内の追加のＰＳＫ識別情報の位置など）を選択することができる。キーイングの選択されたＧＢＡ方法が、以前のブートストラッピング手順（例えば、初期ブートストラッピング手順、直近のブートストラッピング手順など）のために最初に使用されたものとは異なっていてもよいため、ＵＥによってＢＳＦと実行される新しいブートストラッピングは、選択されたＧＢＡ方法において使用するためのフレッシュなセッション鍵を取得するために必要とされ得る。ＮＡＦなどのネットワークデバイスは、（例えば、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」を使用するために）ＵＥとのセキュア通信を確立する選択されたＧＢＡ方法において使用されるフレッシュなセッション鍵を取得するために、ＵＥによってＢＳＦと実行される新しいブートストラッピングが必要であることを示す目的で、相関ＰＳＫ識別情報（例えば、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」）など、追加のＰＳＫ識別情報の表示（例えば、名前空間、インデックス、位置など）を含む、サーバが開始

するハローメッセージ（本明細書ではＳｅｒｖｅｒＨｅｌｌｏメッセージと呼ばれる）などの応答メッセージをＵＥに送信することができる。このようにして、ネットワークデバイスは、（フレッシュな）鍵自体を示すのではなく、特定のＧＢＡ方法など、選択されたブートストラッピング手順とともに使用するための鍵の再生成の必要性を示す鍵識別子をＵＥに送信することができる。

【００３７】

［0046］ 様々な実施形態では、この特定のＧＢＡキーイング方法を使用するために（例えば、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」を使用するために）新しいブートストラッピングの実行が必要であることを示すための相関ＰＳＫ識別情報（例えば、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」）などの追加のＰＳＫ識別情報の表示（例えば、名前空間、インデックス、位置など）を含むＳｅｒｖｅｒＨｅｌｌｏメッセージなどの応答メッセージを受信したことに応答して、ＵＥは、１つ又は複数の鍵を、ＢＳＦと再ネゴシエートして、ＮＡＦサーバなどのネットワークデバイスとの識別されたＧＢＡ手順で使用するための新しいＢ－ＴＩＤと新しいセッション鍵（Ｋｓ）とを取得することができる。様々な実施形態では、ＵＥは、セキュアな通信セッションの確立を要求する要求メッセージにおいて、ＧＢＡ方法に関連するＰＳＫ識別情報と新しいＢ－ＴＩＤとを、ＮＡＦサーバなどのネットワークデバイスに再送信することができる。

【００３８】

［0047］ 様々な実施形態では、ＵＥが、ＣｌｉｅｎｔＨｅｌｌｏメッセージなど、セキュアな通信セッションのための要求メッセージを送信することによってＮＡＦにコンタクトするとき、ＵＥは、ＵＥがＰＳＫ認証を用いたＴＬＳをサポートすることをＮＡＦに示すことができる。ＵＥは、ＣｌｉｅｎｔＨｅｌｌｏメッセージにおいて、ＰＳＫ以外の認証方法をサポートすることを示すことができる。ＵＥは、サーバ名表示（ＴＬＳ拡張によるＣｌｉｅｎｔＨｅｌｌｏメッセージへのｓｅｒｖｅｒ＿ｎａｍｅ拡張など）を使用して、ＮＡＦのホスト名を送信することができる。ＵＥは、ＣｌｉｅｎｔＨｅｌｌｏメッセージ内でＢ－ＴＩＤをＮＡＦに提供することによって、ＰＳＫ認証を伴うＴＬＳのためのＧＢＡベースの共有シークレットを使用することができる。ＵＥが有効なＧＢＡベースの共有シークレットを有していない場合、ＵＥは、まず、Ｕｂ基準点を介してＢＳＦとブートストラッピング手順を実行することによって、ＧＢＡベースの共有シークレットを取得する。

【００３９】

［0048］ ＣｌｉｅｎｔＨｅｌｌｏ内のＰＳＫ識別情報は、ＰＳＫ識別情報名前空間（「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」、及び／又は「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」など）を示すプレフィックスと、そのブートストラッピング方法に関連付けられた関連Ｂ－ＴＩＤとを含むことができる。様々な実施形態では、これらの含まれる識別子（例えば、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」、及び／又は「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」などのＰＳＫ識別情報名前空間）の各々について、フレッシュなセッション鍵の要求を可能にするために、追加のＰＳＫ識別情報名前空間を含めることができる。例えば、ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」が含まれる場合、相関ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」を含めることができ、ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」が含まれる場合、ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」を含めることができ、及び／又は、ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」が含まれる場合、ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」を含めることができる。同様に、相関付けられる実際の鍵のＰＳＫ識別情報名前空間と、ＰＳＫ識別情報名前空間ペアを示す再ネゴシ

エーションサポートとが、他の認証方法のために含まれ得る。プレフィックス（又は名前空間）「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」は、ＴＬＳセッション鍵を確立するためにＡＫＡベースのＫｓ＿（ｅｘｔ）＿ＮＡＦが使用されることをＵＥが受け入れることを示すために、ＰＳＫ識別情報において使用することができる。プレフィックス（又は名前空間）「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」は、ＴＬＳセッション鍵を確立するためにＫｓ＿ｉｎｔ＿ＮＡＦが使用されることをＵＥが受け入れることを示すために、ＰＳＫ識別情報において使用することができる。プレフィックス（又は名前空間）「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」は、ＴＬＳセッション鍵を確立するためにＧＢＡ＿ＤｉｇｅｓｔベースのＫｓ＿ＮＡＦが使用されることをＵＥが受け入れることを示すために、ＰＳＫ識別情報において使用される。同様に、付加された「ｒｅｎｅｇｏｔｉａｔｉｏｎ」又は何らかの他の付加された表示を使用する相関プレフィックス（又は名前空間）は、相関ＧＢＡ方法のために再ネゴシエーションがサポートされることを示すために、ＰＳＫ識別情報において使用することができる。ＣｌｉｅｎｔＨｅｌｌｏメッセージは、ＵＥがサポートする認証方法のためのプレフィックスを含むことができる。

【００４０】

［0049］ 様々な実施形態では、ＮＡＦなどのネットワークデバイスは、特定の方法のための新しいブートストラッピング手順をＵＥに実行させるべきかどうかを判定することができる。ＵＥが特定のＧＢＡ方法のためのフレッシュなセッション鍵を取得するために新しいブートストラッピングを実行すべきであるとネットワークデバイスが判定したことに応答して、ネットワークデバイスは、ＵＥに応答するＳｅｒｖｅｒＨｅｌｌｏメッセージにおいて、選択されたＰＳＫ識別情報（又はブートストラッピング手順）の再ネゴシエーションの表示（例えば、名前空間、インデックス、位置など）を返すことができる。選択されたＰＳＫ識別情報（又はブートストラッピング手順）の再ネゴシエーションの表示（例えば、名前空間、インデックス、位置など）を受信したことに応答して、ＵＥは、このＳｅｒｖｅｒＨｅｌｌｏメッセージを、ブートストラッピング動作を再試行する要求として（例えば、ＨｅｌｌｏＲｅｔｒｙＲｅｑｕｅｓｔとして）扱い、示されたブートストラッピング方法のためのフレッシュなセッション鍵（Ｋｓ）並びにフレッシュなＢ－ＴＩＤを取得するために、ＢＳＦと新しいブートストラッピング動作を実行することができる。ブートストラッピングが完了すると、ＵＥは、選択されたブートストラッピング方法のＰＳＫ識別情報名前空間及び新しいＢ－ＴＩＤのみを含む新しいＣｌｉｅｎｔＨｅｌｌｏメッセージを、ＮＡＦに送信することができる。ＮＡＦが、（元のＣｌｉｅｎｔＨｅｌｌｏ又はフレッシュなブートストラッピング後に送信されたＣｌｉｅｎｔＨｅｌｌｏのいずれかに応答して）ＰＳＫ認証を使用してＴＬＳトンネルを確立しようとする場合、ＮＡＦは、ＰＳＫ識別情報のうちの１つを選択し、例えば、選択されたＰＳＫ識別情報の名前空間、インデックス、又はリスト内の位置を示すことによって、ＳｅｒｖｅｒＨｅｌｌｏメッセージにおいて選択されたＰＳＫ識別情報を示すことができる。ＵＥがＦｉｎｉｓｈｅｄメッセージを送信し、ＮＡＦがＵＥからＦｉｎｉｓｈｅｄメッセージを受信した後、ＵＥ及びＮＡＦは、フレッシュなセッション鍵を使用して、ＴＬＳトンネルを介してのアプリケーションレベルの通信を使用することができる。

【００４１】

［0050］ 様々な実施形態は、ＵＥ及びネットワークデバイスが、秘密鍵などの秘密情報又はセキュア情報を交換することなく、ＵＥのための各アプリケーション又はサービスのための一意の鍵について合意することを可能にする。結果として、様々な実施形態は、ＵＥとネットワークデバイスとの間の通信のセキュリティを改善することによって、ＵＥ、ネットワークデバイス、及び通信システムの動作を改善する。

【００４２】

［0051］ 図１Ａは、例示的な通信システム１００を示すシステムブロック図である。通信システム１００は、５Ｇ新無線（ＮＲ）ネットワーク、又はロングタームエボリューション（ＬＴＥ）ネットワークなどの任意の他の好適なネットワークであり得る。図１Ａ

は５Ｇネットワークを示すが、後世代ネットワークは同じ又は同様の要素を含み得る。従って、以下の説明における５Ｇネットワーク又は５Ｇネットワーク要素の言及は、例示のためであり、限定的であることを意図しない。

【００４３】

［0052］ 通信システム１００は、コアネットワーク１４０と、様々なＵＥ（図１Ａにおいて ＵＥ１２０ａ～１２０ｅとして示される）とを含む、異種ネットワークアーキテクチャを含み得る。通信システム１００はまた、ＮＡＦサーバ、ＢＳＦ、ＨＳＳ、加入者ロケータ機能（ＳＬＦ）サーバなどを含む様々なネットワークサーバなど、様々なネットワークデバイス１４２ａを含み得る。通信システム１００はまた、いくつかの基地局（ＢＳ １１０ａ、ＢＳ １１０ｂ、ＢＳ １１０ｃ、及びＢＳ １１０ｄとして示される）と他のネットワークエンティティとを含み得る。基地局は、ＵＥと通信するエンティティであり、また、ノードＢ（ＮｏｄｅＢ）、ＬＴＥ発展型ノードＢ（ｅＮｏｄｅＢ又はｅＮＢ）、アクセスポイント（ＡＰ）、無線ヘッド、送受信ポイント（ＴＲＰ）、新無線基地局（ＮＲ ＢＳ）、５ＧノードＢ（ＮＢ）、次世代ノードＢ（ｇＮｏｄｅＢ又はｇＮＢ）などと呼ばれることもある。各基地局は、特定の地理的エリアに通信カバレッジを提供し得る。３ＧＰＰでは、「セル」という用語は、この用語が使用される文脈に応じて、基地局のカバレッジエリア、このカバレッジエリアにサービスする基地局サブシステム、又はそれらの組合せを指すことがある。コアネットワーク１４０は、ＬＴＥコアネットワーク（例えば、発展型パケットコア（ＥＰＣ）ネットワーク）、５Ｇコアネットワークなど、任意のタイプのコアネットワークであり得る。

【００４４】

［0053］ 基地局１１０ａ～１１０ｄは、マクロセル、ピコセル、フェムトセル、別のタイプのセル、又はそれらの組合せに通信カバレッジを提供し得る。マクロセルは、比較的大きい地理的エリア（例えば、半径数キロメートル）をカバーすることができ、サービスに加入しているＵＥによる無制限アクセスを可能にし得る。ピコセルは、比較的小さい地理的エリアをカバーすることができ、サービスに加入しているＵＥによる無制限アクセスを可能にすることができる。フェムトセルは、比較的小さい地理的エリア（例えば、自宅）をカバーすることができ、フェムトセルとの関連付けを有するＵＥ（例えば、限定加入者グループ（ＣＳＧ）内のＵＥ）による制限付きアクセスを可能にし得る。マクロセルのための基地局は、マクロＢＳと呼ばれることがある。ピコセルのための基地局は、ピコＢＳと呼ばれることがある。フェムトセルのための基地局は、フェムトＢＳ又はホームＢＳと呼ばれることがある。図１に示す例では、基地局１１０ａは、マクロセル１０２ａのためのマクロＢＳであってもよく、基地局１１０ｂは、ピコセル１０２ｂのためのピコＢＳであってもよく、基地局１１０ｃは、フェムトセル１０２ｃのためのフェムトＢＳであってもよい。基地局１１０ａ～１１０ｄは、１つ又は複数（例えば、３つ）のセルをサポートし得る。「ｅＮＢ」、「基地局」、「ＮＲ ＢＳ」、「ｇＮＢ」、「ＴＲＰ」、「ＡＰ」、「ｎｏｄｅ Ｂ」、「５Ｇ ＮＢ」、及び「セル」という用語は、本明細書では互換的に使用され得る。

【００４５】

［0054］ いくつかの例では、セルは静止していないことがあり、セルの地理的エリアは、モバイル基地局のロケーションに従って移動し得る。いくつかの例では、基地局１１０ａ～１１０ｄは、任意の好適なトランスポートネットワークを使用して、直接物理接続、仮想ネットワーク、又はそれらの組合せなど、様々なタイプのバックホールインターフェースを通して、通信システム１００において互いに、並びに、１つ又は複数の他の基地局又はネットワークノード（図示せず）に相互接続され得る。

【００４６】

［0055］ 基地局１１０ａ～１１０ｄは、ワイヤード又はワイヤレス通信リンク１２６上で、コアネットワーク１４０と通信し得る。ＵＥ１２０ａ～１２０ｅは、ワイヤレス通信リンク１２２上で、基地局１１０ａ～１１０ｄと通信し得る。

【００４７】

［0056］ワイヤード通信リンク１２６は、イーサネット（登録商標）、ポイントツーポイントプロトコル、ハイレベルデータリンク制御（ＨＤＬＣ）、アドバンストデータ通信制御プロトコル（ＡＤＣＣＰ）、及び伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）など、１つ又は複数のワイヤード通信プロトコルを使用し得る様々なワイヤードネットワーク（イーサネット、ＴＶケーブル、電話、光ファイバー、及び他の形態の物理ネットワーク接続など）を使用し得る。

【００４８】

［0057］通信システム１００はまた、中継局（中継ＢＳ１１０ｄなど）を含み得る。中継局は、上流局（例えば、基地局又はＵＥ）からデータの送信を受信し、データの送信を下流局（例えば、ＵＥ又は基地局）に送ることができるエンティティである。中継局はまた、他のＵＥのための送信を中継することができるワイヤレスデバイス（例えばＵＥ）であり得る。図１に示す例では、中継局１１０ｄは、基地局１１０ａとＵＥ１２０ｄとの間の通信を容易にするために、基地局１１０ａ及びＵＥ１２０ｄと通信し得る。中継局はまた、中継基地局、中継基地局、中継器などと呼ばれることもある。

【００４９】

［0058］通信システム１００は、異なるタイプの基地局、例えば、マクロ基地局、ピコ基地局、フェムト基地局、中継基地局などを含む異種ネットワークであり得る。これらの異なるタイプの基地局は、異なる送信電力レベル、異なるカバレッジエリアを有することがあり、通信システム１００における干渉に異なる影響を及ぼすことがある。例えば、マクロ基地局は、高い送信電力レベル（例えば、５～４０ワット）を有し得るのに対して、ピコ基地局、フェムト基地局、及び中継基地局は、より低い送信電力レベル（例えば、０．１～２ワット）を有し得る。

【００５０】

［0059］ネットワークコントローラ１３０は、基地局のセットに結合し得、これらの基地局のための協調及び制御を提供し得る。ネットワークコントローラ１３０は、バックホールを介して、基地局と通信し得る。基地局はまた、例えば、ワイヤレス又はワイヤラインバックホールを介して、直接又は間接的に互いと通信し得る。

【００５１】

［0060］ＵＥ１２０ａ、１２０ｂ、１２０ｃは、通信システム１００全体にわたって分散され得、各ＵＥは固定又は移動であり得る。ＵＥは、アクセス端末、端末、移動局、加入者ユニット、局、ワイヤレスデバイスなどと呼ばれることもある。

【００５２】

［0061］マクロ基地局１１０ａは、ワイヤード又はワイヤレス通信リンク１２６上で、コアネットワーク１４０と通信し得る。ＵＥ　１２０ａ、１２０ｂ、１２０ｃは、ワイヤレス通信リンク１２２上で、基地局１１０ａ～１１０ｄと通信し得る。

【００５３】

［0062］ワイヤレス通信リンク１２２及び１２４は、複数のキャリア信号、周波数、又は周波数帯域を含むことがあり、これらの各々が複数の論理チャネルを含むことがある。ワイヤレス通信リンク１２２及び１２４は、１つ又は複数の無線アクセス技術（ＲＡＴ）を使用し得る。ワイヤレス通信リンクにおいて使用され得るＲＡＴの例としては、３ＧＰＰ　ＬＴＥ、３Ｇ、４Ｇ、５Ｇ（ＮＲなど）、ＧＳＭ、符号分割多元接続（ＣＤＭＡ）、広帯域符号分割多元接続（ＷＣＤＭＡ）、ワールドワイドインターオペラビリティフォーマイクロウェーブアクセス（ＷｉＭＡＸ）、時分割多元接続（ＴＤＭＡ）、及び他のモバイルテレフォニー通信技術セルラーＲＡＴが挙げられる。通信システム１００内の様々なワイヤレス通信リンクのうちの１つ又は複数において使用され得るＲＡＴの更なる例は、Ｗｉ－Ｆｉ、ＬＴＥ－Ｕ、ＬＴＥ－Ｄｉｒｅｃｔ、ＬＡＡ、ＭｕＬＴＥｆｉｒｅなどの中距離プロトコル、並びに、ＺｉｇＢｅｅ、Ｂｌｕｅｔｏｏｔｈ、及びＢｌｕｅｔｏｏｔｈ低エネルギー（ＬＥ）などの比較的短距離のＲＡＴを含む。

【００５４】

［0063］いくつかのワイヤレスネットワーク（例えば、ＬＴＥ）は、ダウンリンク上

で直交周波数分割多重化（ＯＦＤＭ）を、またアップリンク上でシングルキャリア周波数分割多重化（ＳＣ－ＦＤＭ）を使用する。ＯＦＤＭ及びＳＣ－ＦＤＭは、システム帯域幅を、一般にトーン、ビンなどとも呼ばれる複数（Ｋ）の直交サブキャリアに区分する。各サブキャリアは、データで変調され得る。一般に、変調シンボルは、周波数領域においてＯＦＤＭを用いて、また時間領域においてＳＣ－ＦＤＭを用いて送られる。隣接するサブキャリアの間の間隔は、固定されていてもよく、サブキャリアの総数（Ｋ）は、システム帯域幅に依存してもよい。例えば、サブキャリアの間隔は、１５ｋＨｚであり得、最小リソース割振り（「リソースブロック」と呼ばれる）は、１２個のサブキャリア（又は、１８０ｋＨｚ）であり得る。従って、公称の高速ファイル転送（ＦＦＴ）サイズは、１．２５、２．５、５、１０、又は２０メガヘルツ（ＭＨｚ）のシステム帯域幅に対して、それぞれ、１２８、２５６、５１２、１０２４、又は２０４８に等しくなり得る。システム帯域幅はまた、サブバンドに区分され得る。例えば、サブバンドは、１．０８ＭＨｚ（すなわち、６個のリソースブロック）をカバーし得、１．２５、２．５、５、１０又は２０ＭＨｚのシステム帯域幅に対して、それぞれ、１、２、４、８又は１６個のサブバンドが存在し得る。

【００５５】

［0064］ いくつかの実装形態の説明は、ＬＴＥ技術に関連する専門用語及び例を使用し得るが、いくつかの実装形態は、新無線（ＮＲ）又は５Ｇネットワークなど、他のワイヤレス通信システムに適用可能であり得る。ＮＲは、アップリンク（ＵＬ）及びダウンリンク（ＤＬ）上でサイクリックプレフィックス（ＣＰ）を用いてＯＦＤＭを利用し得、時分割複信（ＴＤＤ）を使用する半二重動作のためのサポートを含み得る。１００ＭＨｚの単一のコンポーネントキャリア帯域幅がサポートされてもよい。ＮＲリソースブロックは、０．１ミリ秒（ｍｓ）の持続時間にわたって、７５ｋＨｚのサブキャリア帯域幅を有する１２個のサブキャリアにまたがり得る。各無線フレームは、１０ｍｓの長さを有する５０個のサブフレームで構成され得る。従って、各サブフレームは長さが０．２ｍｓであってよい。各サブフレームはデータ送信のためのリンク方向（すなわち、ＤＬ又はＵＬ）を示し得、サブフレームごとのリンク方向は動的に切り替えられてよい。各サブフレームは、ＤＬ／ＵＬデータ並びにＤＬ／ＵＬ制御データを含んでよい。ビームフォーミングがサポートされてよく、ビーム方向は動的に構成され得る。プリコーディングを用いた多入力多出力（ＭＩＭＯ）送信もまた、サポートされ得る。ＤＬにおけるＭＩＭＯ構成は、最大８つのストリーム及びＵＥごとに最大２つのストリームのマルチレイヤＤＬ送信とともに、最大８つの送信アンテナをサポートし得る。ＵＥ当り最大２ストリームを用いるマルチレイヤ送信がサポートされてよい。

【００５６】

［0065］ 複数のセルのアグリゲーションは、最大８つのサービングセルとともにサポートされ得る。代替として、ＮＲは、ＯＦＤＭベースのエアインターフェースとは異なるエアインターフェースをサポートし得る。

【００５７】

［0066］ いくつかのＵＥは、マシンタイプ通信（ＭＴＣ：machine-type communication）ＵＥ、又は発展型若しくは拡張マシンタイプ通信（ｅＭＴＣ：evolved or enhanced machine-type communication）ＵＥと見なされてよい。ＭＴＣ　ＵＥ及びｅＭＴＣ　ＵＥは、例えば、基地局、別のデバイス（例えば、リモートデバイス）、又は何らかの他のエンティティと通信し得る、ロボット、ドローン、リモートデバイス、センサ、メーター、モニタ、ロケーションタグなどを含む。ワイヤレスコンピューティングプラットフォームは、例えば、ワイヤード又はワイヤレス通信リンクを介した、ネットワーク（例えば、インターネット又はセルラーネットワークなどのワイドエリアネットワーク）のための、又はネットワークへの接続性を提供し得る。いくつかのＵＥは、モノのインターネット（ＩｏＴ）デバイスと見なされてもよく、又はＮＢ－ＩｏＴ（狭帯域のモノのインターネット）デバイスとして実装されてもよい。ＵＥ１２０ａ～１２０ｅは、プロセッサ構成要素、メモリ構成要素、同様の構成要素、又はそれらの組合せなどの、ＵＥ１２

０ａ～１２０ｅの構成要素を収容するハウジングの内部に含まれてもよい。
【００５８】
［0067］ 一般に、任意の数の通信システム及び任意の数のワイヤレスネットワークが、所与の地理的エリアにおいて展開され得る。各通信システム及びワイヤレスネットワークは、特定の無線アクセス技術（ＲＡＴ）をサポートしてよく、１つ又は複数の周波数上で動作し得る。ＲＡＴは、無線技術、エアインターフェースなどと呼ばれることもある。周波数は、キャリア、周波数チャネルなどと呼ばれることもある。各周波数は、異なるＲＡＴの通信システム間の干渉を回避するために、所与の地理的エリアにおいて単一のＲＡＴをサポートし得る。場合によっては、４Ｇ／ＬＴＥ及び／又は５Ｇ／ＮＲ ＲＡＴネットワークが展開されることがある。例えば、５Ｇ非スタンドアロン（ＮＳＡ）ネットワークは、５Ｇ ＮＳＡネットワークの４Ｇ／ＬＴＥ ＲＡＮサイドで４Ｇ／ＬＴＥ ＲＡＴと、５Ｇ ＮＳＡネットワークの５Ｇ／ＮＲ ＲＡＮサイドで５Ｇ／ＮＲ ＲＡＴとの両方を利用し得る。４Ｇ／ＬＴＥ ＲＡＮと５Ｇ／ＮＲ ＲＡＮは両方とも、互いに、また５Ｇ ＮＳＡネットワーク内で４Ｇ／ＬＴＥコアネットワーク（例えば、発展型パケットコア（ＥＰＣ）ネットワーク）に接続し得る。他の例示的なネットワーク構成は、５Ｇ／ＮＲ ＲＡＮが５Ｇコアネットワークに接続する５Ｇスタンドアロン（ＳＡ）ネットワークを含み得る。
【００５９】
［0068］ いくつかの実装形態では、（例えば、ＵＥ１２０ａ及びＵＥ１２０ｅとして示されている）２つ以上のＵＥは、（例えば、互いに通信するための媒介として基地局１１０ａ～１１０ｄを使用せずに）１つ又は複数のサイドリンクチャネルを使用して直接通信し得る。例えば、ＵＥ １２０ａ～１２０ｅは、ピアツーピア（Ｐ２Ｐ）通信、デバイス間（Ｄ２Ｄ）通信、（車車間（Ｖ２Ｖ）プロトコル、路車間（Ｖ２Ｉ）プロトコル、若しくは同様のプロトコルを含み得る）ビークルツーエブリシング（Ｖ２Ｘ）プロトコル、メッシュネットワーク、又は同様のネットワーク、あるいはそれらの組合せを使用して通信し得る。この場合、ＵＥ１２０ａ～１２０ｅは、スケジューリング動作、リソース選択動作、及び本明細書の他の箇所で基地局１１０ａ～１１０ｄによって実行されるものとして説明する他の動作を実行し得る。
【００６０】
［0069］ 図１Ｂは、様々な実施形態のいずれかを実装するのに好適な、５Ｇ（又は後世代）ネットワークなどの通信システム（例えば、通信システム１００）の一部であり得る例示的な分離型基地局１６０アーキテクチャを示すシステムブロック図である。図１Ａ及び図１Ｂを参照すると、分離型基地局１６０アーキテクチャは、バックホールリンクを介してコアネットワーク１８０と直接通信することのできる、あるいは、１つ又は複数の分離型基地局ユニット（Ｅ２リンクを介した準リアルタイム（準ＲＴ）ＲＡＮインテリジェントコントローラ（ＲＩＣ）１６４、又は、サービス管理及びオーケストレーション（ＳＭＯ）フレームワーク１６６に関連付けられている非リアルタイム（非ＲＴ）ＲＩＣ１６８、若しくはその双方など）を通じて、コアネットワーク１８０と間接的に通信することのできる、１つ又は複数の中央ユニット（ＣＵ）１６２を含み得る。ＣＵ１６２は、Ｆ１インターフェースなどのそれぞれのミッドホールリンクを介して、１つ又は複数の分散ユニット（ＤＵ）１７０と通信することができる。ＤＵ１７０は、それぞれのフロントホールリンクを介して、１つ又は複数の無線ユニット（ＲＵ）１７２と通信することができる。ＲＵ１７２は、１つ又は複数の無線周波数（ＲＦ）アクセスリンクを介してそれぞれのＵＥ１２０と通信し得る。いくつかの実装形態では、ＵＥは、複数のＲＵ１７２によって同時にサービスされてもよい。
【００６１】
［0070］ ユニットの各々（すなわち、ＣＵ１６２、ＤＵ１７０、ＲＵ１７２）、並びに近ＲＴ ＲＩＣ１６４、非ＲＴ ＲＩＣ１６８、及びＳＭＯフレームワーク１６６は、ワイヤード又はワイヤレス伝送媒体を介して信号、データ、又は情報（集合的に信号）を受信又は送信するように構成された１つ若しくは複数のインターフェースを含むか、又は

１つ若しくは複数のインターフェースに結合され得る。ユニットの各々、又はユニットの通信インターフェースに命令を提供する関連付けられたプロセッサ若しくはコントローラは、伝送媒体を介して他のユニットのうちの１つ以上と通信するように構成され得る。例えば、ユニットは、ワイヤード伝送媒体を介して他のユニットのうちの１つ以上に信号を受信又は送信するように構成されたワイヤードインターフェースを含むことができる。更には、それらのユニットは、他のユニットのうちの１つ以上に対するワイヤレス伝送媒体を介して、信号を受信若しくは送信又は送受信するように構成されている、受信機、送信機、又はトランシーバ（無線周波数（ＲＦ）トランシーバなど）を含み得る、ワイヤレスインタフェースを含み得る。

【００６２】

［0071］ いくつかの態様では、ＣＵ１６２は、１つ又は複数の上位レイヤの制御機能をホストすることができる。そのような制御機能としては、無線リソース制御（ＲＲＣ）、パケットデータコンバージェンスプロトコル（ＰＤＣＰ）、サービスデータアダプテーションプロトコル（ＳＤＡＰ）などを挙げることができる。各制御機能は、ＣＵ１６２によってホストされる他の制御機能と信号を通信するように構成されたインターフェースを用いて実装され得る。ＣＵ１６２は、ユーザプレーン機能（すなわち、中央ユニット－ユーザプレーン（ＣＵ－ＵＰ））、制御プレーン機能（すなわち、中央ユニット－制御プレーン（ＣＵ－ＣＰ））、又はそれらの組合せを扱うように構成され得る。いくつかの実装形態では、ＣＵ１６２は、１つ又は複数のＣＵ－ＵＰユニットと１つ又は複数のＣＵ－ＣＰユニットとに論理的に分割することができる。ＣＵ－ＵＰユニットは、Ｏ－ＲＡＮ構成で実装されるとき、Ｅ１インターフェースなどのインターフェースを介してＣＵ－ＣＰユニットと双方向に通信することができる。ＣＵ１６２は、ネットワーク制御及びシグナリングのために、必要に応じて、ＤＵ１７０と通信するように実装することができる。

【００６３】

［0072］ ＤＵ１７０は、１つ又は複数のＲＵ１７２の動作を制御するための１つ又は複数の基地局機能を含む論理ユニットに対応し得る。いくつかの態様では、ＤＵ１７０は、第３世代パートナーシッププロジェクト（３ＧＰＰ）によって定義されているものなどの機能分割に少なくとも部分的に応じて、無線リンク制御（ＲＬＣ）レイヤ、媒体アクセス制御（ＭＡＣ）レイヤ、及び１つ又は複数の上位物理（ＰＨＹ）レイヤ（前方誤り訂正（ＦＥＣ）符号化及び復号化、スクランブル化、変調及び復調などに関するモジュールなど）のうちの、１つ又は複数をホストすることができる。いくつかの態様では、ＤＵ１７０は更に、１つ又は複数の低ＰＨＹレイヤをホストし得る。各レイヤ（又はモジュール）は、ＤＵ１７０によってホストされる他のレイヤ（及びモジュール）と、又はＣＵ１６２によってホストされる制御機能と、信号を通信するように構成されたインターフェースを用いて実装され得る。

【００６４】

［0073］ 下位レイヤ機能は、１つ又は複数のＲＵ１７２によって実装され得る。いくつかの配備では、ＤＵ１７０によって制御されるＲＵ１７２は、下位レイヤ機能分割などの機能分割に少なくとも部分的に基づいて、ＲＦ処理機能、又は低ＰＨＹレイヤ機能（高速フーリエ変換（ＦＦＴ）、逆ＦＦＴ（ｉＦＦＴ）、デジタルビームフォーミング、物理ランダムアクセスチャネル（ＰＲＡＣＨ）抽出及びフィルタリングなどを実行するなど）、あるいはその両方をホストする論理ノードに対応し得る。そのようなアーキテクチャでは、ＲＵ（単数又は複数）１７２は、１つ又は複数のＵＥ１２０との地上波（ＯＴＡ）通信を扱うように実装され得る。いくつかの実装形態では、ＲＵ（単数又は複数）１７２との制御及びユーザプレーン通信のリアルタイム態様及び非リアルタイム態様は、対応するＤＵ１７０によって制御され得る。いくつかのシナリオでは、この構成は、ＤＵ（単数又は複数）１７０及びＣＵ１６２が、ｖＲＡＮアーキテクチャなどのクラウドベースの無線アクセスネットワーク（ＲＡＮ）アーキテクチャにおいて実装されることを可能にすることができる。

【００６５】

［0074］ ＳＭＯフレームワーク１６６は、非仮想化及び仮想化ネットワーク要素のＲＡＮ配備及びプロビジョニングをサポートするように構成され得る。非仮想化ネットワーク要素の場合、ＳＭＯフレームワーク１６６は、ＲＡＮカバレッジ要件のための専用の物理リソースの配備をサポートするように構成することができ、これは、動作及び保守インターフェース（Ｏ１インターフェースなど）を介して管理することができる。仮想化ネットワーク要素の場合、ＳＭＯフレームワーク１６６は、クラウドコンピューティングプラットフォーム（オープンクラウド（Ｏ－クラウド）１７６など）と対話して、クラウドコンピューティングプラットフォームインターフェース（Ｏ２インターフェースなど）を介してネットワーク要素ライフサイクル管理を実行する（仮想化ネットワーク要素をインスタンス化するなど）ように構成されてもよい。そのような仮想化されたネットワーク要素は、ＣＵ１６２、ＤＵ１７０、ＲＵ１７２及び近ＲＴ　ＲＩＣ１６４を含むことができるが、これらに限定されない。いくつかの実装形態では、ＳＭＯフレームワーク１６６は、Ｏ１インターフェースを介して、オープンｅＮＢ（Ｏ－ｅＮＢ）１７４などの４Ｇ　ＲＡＮのハードウェア態様と通信することができる。加えて、いくつかの実装形態では、ＳＭＯフレームワーク１６６は、Ｏ１インターフェースを介して１つ又は複数のＲＵ１７２と直接通信することができる。ＳＭＯフレームワーク１６６はまた、ＳＭＯフレームワーク１６６の機能をサポートするように構成された非ＲＴ　ＲＩＣ１６８を含み得る。

【００６６】

［0075］ 非ＲＴ　ＲＩＣ１６８は、ＲＡＮ要素及びリソースの非リアルタイム制御及び最適化、モデルトレーニング及び更新を含む人工知能／機械学習（ＡＩ／ＭＬ）ワークフロー、又は近ＲＴ　ＲＩＣ１６４におけるアプリケーション／特徴のポリシーベースのガイダンスを可能にする論理機能を含むように構成されてもよい。非ＲＴ　ＲＩＣ１６８は、近ＲＴ　ＲＩＣ１２５に結合されてもよく、又は（Ａ１インターフェースなどを介して）近ＲＴ　ＲＩＣ１６４と通信してもよい。近ＲＴ　ＲＩＣ１６４は、１つ又は複数のＣＵ１６２、１つ又は複数のＤＵ１７０、又はその両方、並びにＯ－ｅＮＢを近ＲＴ　ＲＩＣ１６４に接続するインターフェースを介した（Ｅ２インターフェースを介するなど）データ収集及びアクションを介して、ＲＡＮ要素及びリソースの近リアルタイム制御及び最適化を可能にする論理機能を含むように構成され得る。

【００６７】

［0076］ いくつかの実装形態では、近ＲＴ　ＲＩＣ１６４に展開されるＡＩ／ＭＬモデルを生成するために、非ＲＴ　ＲＩＣ１６８は、外部サーバからパラメータ又は外部エンリッチメント情報を受信してもよい。そのような情報は、近ＲＴ　ＲＩＣ１６４によって利用されてもよく、非ネットワークデータソースから又はネットワーク機能からＳＭＯフレームワーク１６６又は非ＲＴ　ＲＩＣ１６８において受信されてもよい。いくつかの例では、非ＲＴ　ＲＩＣ１６８又は近ＲＴ　ＲＩＣ１６４は、ＲＡＮ挙動又は性能を調整するように構成され得る。例えば、非ＲＴ　ＲＩＣ　１６８は、性能に関する長期の傾向及びパターンを監視し、ＳＭＯフレームワーク１６６を通じて（Ｏ１を介した再構成など）又はＲＡＮ管理ポリシー（Ａ１ポリシーなど）の作成を介して是正措置を実行するためにＡＩ／ＭＬモデルを採用してもよい。

【００６８】

［0077］ 図２は、様々な実施形態のいずれかを実装するのに好適な、例示的なコンピューティング及びワイヤレスモデムシステム２００を示す構成要素ブロック図である。様々な実施形態は、システムオンチップ（ＳＯＣ）又はシステムインパッケージ（ＳＩＰ）を含む、いくつかのシングルプロセッサ及びマルチプロセッサコンピュータシステム上で実装され得る。

【００６９】

［0078］ 図１Ａ～図２を参照すると、示される例示的なコンピューティングシステム２００（いくつかの実施形態ではＳＩＰであってよい）は、クロック２０６と、電圧調整器２０８と、アンテナ（図示せず）を介してワイヤレス通信を、基地局１１０ａなどのＵＥへ送信し、ＵＥから受信するように構成されたワイヤレストランシーバ２６６と、に結

合された２つのＳＯＣ２０２、２０４を含む。いくつかの実装形態では、第１のＳＯＣ２０２は、命令によって指定された算術、論理、制御及び入出力（Ｉ／Ｏ）演算を実施することによってソフトウェアアプリケーションプログラムの命令を実行するＵＥの中央処理装置（ＣＰＵ）として動作し得る。いくつかの実装形態では、第２のＳＯＣ２０４は、専用処理ユニットとして動作し得る。例えば、第２のＳＯＣ２０４は、高ボリューム、高速度（５Ｇｂｐｓなど）、又は超高周波短波長（２８ＧＨｚ　ｍｍＷａｖｅスペクトルなど）通信を管理することを担当する専用５Ｇ処理ユニットとして動作し得る。

【００７０】

[0079] 第１のＳＯＣ２０２は、デジタル信号プロセッサ（ＤＳＰ）２１０と、モデムプロセッサ２１２と、グラフィックスプロセッサ２１４と、アプリケーションプロセッサ２１６と、プロセッサのうちの１つ又は複数に接続された１つ又は複数のコプロセッサ２１８（ベクトルコプロセッサなど）と、メモリ２２０と、カスタム回路構成２２２と、システム構成要素及びリソース２２４と、相互接続／バスモジュール２２６と、１つ又は複数の温度センサ２３０と、熱管理ユニット２３２と、熱電力エンベロープ（ＴＰＥ：thermal power envelope）構成要素２３４とを含み得る。第２のＳＯＣ２０４は、５Ｇモデムプロセッサ２５２と、電力管理ユニット２５４と、相互接続／バスモジュール２６４と、複数のｍｍＷａｖｅトランシーバ２５６と、メモリ２５８と、アプリケーションプロセッサ、パケットプロセッサなど様々な追加のプロセッサ２６０とを含んでもよい。

【００７１】

[0080] 各プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０は、１つ又は複数のコアを含んでもよく、各プロセッサ／コアは、他のプロセッサ／コアとは無関係の動作を実行してもよい。例えば、第１のＳＯＣ２０２は、第１のタイプのオペレーティングシステム（ＦｒｅｅＢＳＤ、ＬＩＮＵＸ、ＯＳ　Ｘなど）を実行するプロセッサと、第２のタイプのオペレーティングシステム（ＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ　１０など）を実行するプロセッサとを含み得る。加えて、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０のいずれか又はすべては、プロセッサクラスタアーキテクチャ（同期プロセッサクラスタアーキテクチャ、非同期又は異種プロセッサクラスタアーキテクチャなど）の一部として含まれ得る。

【００７２】

[0081] 第１のＳＯＣ２０２及び第２のＳＯＣ２０４は、センサデータ、アナログデジタル変換、ワイヤレスデータ送信を管理するため、並びに、データパケットを復号すること、及びウェブブラウザにおいてレンダリングするために、符号化されたオーディオ及びビデオ信号を処理することなど、他の専用動作を実行するための、様々なシステム構成要素、リソース、及びカスタム回路を含んでもよい。例えば、第１のＳＯＣ２０２のシステム構成要素及びリソース２２４は、電力増幅器、電圧調節器、発振器、位相ロックループ、周辺ブリッジ、データコントローラ、メモリコントローラ、システムコントローラ、アクセスポート、タイマー、並びに、ＵＥ上で実行しているプロセッサ及びソフトウェアクライアントをサポートするために使用される他の同様の構成要素を含んでもよい。システム構成要素及びリソース２２４、又はカスタム回路２２２はまた、カメラ、電子ディスプレイ、ワイヤレス通信デバイス、外部メモリチップなど、周辺デバイスとインターフェースするための回路を含み得る。

【００７３】

[0082] 第１のＳＯＣ２０２及び第２のＳＯＣ２０４は、相互接続／バスモジュール２５０を介して通信してもよい。様々なプロセッサ２１０、２１２、２１４、２１６、２１８は、相互接続／バスモジュール２２６を介して、１つ又は複数のメモリ要素２２０、システム構成要素及びリソース２２４、並びにカスタム回路２２２、並びに熱管理ユニット２３２に相互接続されてもよい。同様に、プロセッサ２５２は、相互接続／バスモジュール２６４を介して、電力管理ユニット２５４、ｍｍＷａｖｅトランシーバ２５６、メモリ２５８、及び様々な追加のプロセッサ２６０に相互接続されてもよい。相互接続／バスモジュール２２６、２５０、２６４は、再構成可能な論理ゲートのアレイを含むか、又は

バスアーキテクチャ（ＣｏｒｅＣｏｎｎｅｃｔ、ＡＭＢＡなど）を実装し得る。通信は、高性能ネットワークオンチップ（ＮｏＣ）などの高度な相互接続部によって行われてもよい。

【００７４】

［0083］ 第１のＳＯＣ２０２又は第２のＳＯＣ２０４は、クロック２０６及び電圧調節器２０８など、ＳＯＣの外部にあるリソースと通信するための入出力モジュール（図示せず）を更に含み得る。ＳＯＣの外部にあるリソース（クロック２０６、電圧調節器２０８など）は、内部ＳＯＣプロセッサ／コアのうちの２つ以上によって共有され得る。

【００７５】

［0084］ 上記した例示的なＳＩＰ２００に加えて、いくつかの実装形態が、単一のプロセッサ、複数のプロセッサ、マルチコアプロセッサ、又はそれらの任意の組合せを含み得る、多種多様なコンピューティングシステムにおいて実装され得る。

【００７６】

［0085］ 図３は、様々な実施形態のいずれかを実装するのに好適な、ワイヤレス通信におけるユーザ及び制御プレーンのための無線プロトコルスタックを含むソフトウェアアーキテクチャ３００を示す構成要素ブロック図である。図１Ａ～図３を参照すると、ＵＥ３２０は、通信システム（例えば、１００）のＵＥ３２０（例えば、ＵＥ１２０ａ～１２０ｅ、２００）とネットワークデバイス３５０（例えば、ネットワークデバイス１４２ａ）との間の通信を容易にするためにソフトウェアアーキテクチャ３００を実装し得る。様々な実施形態では、ソフトウェアアーキテクチャ３００におけるレイヤは、ネットワークデバイス３５０のソフトウェアにおける対応するレイヤとの論理接続を形成し得る。ソフトウェアアーキテクチャ３００は、１つ又は複数のプロセッサ（プロセッサ２１２、２１４、２１６、２１８、２５２、２６０など）の間に分散され得る。マルチＳＩＭ（加入者識別モジュール）ＵＥにおける、１つの無線プロトコルスタックに関して示されているが、ソフトウェアアーキテクチャ３００は、複数のプロトコルスタックを含んでよく、複数のプロトコルスタックの各々が、異なるＳＩＭに関連付けられ得る（デュアルＳＩＭワイヤレス通信デバイスにおける、それぞれ２つのＳＩＭに関連付けられた２つのプロトコルスタックなど）。ＬＴＥ通信レイヤに関して以下で説明するが、ソフトウェアアーキテクチャ３００は、ワイヤレス通信のための様々な規格及びプロトコルのいずれかをサポートし得るか、並びに／又は、ワイヤレス通信のための様々な規格及びプロトコルのいずれかをサポートする追加のプロトコルスタックを含み得る。

【００７７】

［0086］ ソフトウェアアーキテクチャ３００は、非アクセス層（ＮＡＳ）３０２とアクセス層（ＡＳ）３０４とを含み得る。ＮＡＳ３０２は、ＵＥのＳＯＣ（ＳＯＣ２０４など）とそれのコアネットワーク１４０との間のパケットフィルタリングと、セキュリティ管理と、モビリティ制御と、セッション管理と、トラフィック及びシグナリングとをサポートするための機能とプロトコルとを含み得る。ＡＳ３０４は、ＳＯＣ（ＳＯＣ２０４など）と、サポートされたアクセスネットワークのエンティティ（基地局など）との間の通信をサポートする、機能及びプロトコルを含み得る。具体的には、ＡＳ３０４は、少なくとも３つのレイヤ（レイヤ１、レイヤ２、及びレイヤ３）を含み得、その各々が様々なサブレイヤを含み得る。

【００７８】

［0087］ ユーザ及び制御プレーンにおいて、ＡＳ３０４のレイヤ１（Ｌ１）は、物理レイヤ（ＰＨＹ）３０６であってよく、物理レイヤ（ＰＨＹ）３０６は、ワイヤレストランシーバ（例えば、２６６）を介してエアインターフェース上の送信又は受信を可能にする機能を監督し得る。そのような物理レイヤ３０６機能の例には、巡回冗長検査（ＣＲＣ）アタッチメント、コーディングブロック、スクランブリング及びデスクランブリング、変調及び復調、信号測定、ＭＩＭＯなどが含まれ得る。物理レイヤは、物理ダウンリンク制御チャネル（ＰＤＣＣＨ）及び物理ダウンリンク共有チャネル（ＰＤＳＣＨ）を含む、様々な論理チャネルを含み得る。

【００７９】
［0088］ユーザプレーン及び制御プレーンにおいて、ＡＳ３０４のレイヤ２（Ｌ２）は、物理レイヤ３０６上のＵＥ３２０とネットワークデバイス３５０との間のリンクを担い得る。いくつかの実装形態では、レイヤ２は、媒体アクセス制御（ＭＡＣ）サブレイヤ３０８と、無線リンク制御（ＲＬＣ）サブレイヤ３１０と、パケットデータコンバージェンスプロトコル（ＰＤＣＰ）サブレイヤ３１２と、サービスデータアダプテーションプロトコル（ＳＤＡＰ）３１７サブレイヤとを含み得、それらの各々が、ネットワークデバイス３５０において終端する論理接続を形成する。
【００８０】
［0089］制御プレーンにおいて、ＡＳ３０４のレイヤ３（Ｌ３）は、無線リソース制御（ＲＲＣ）サブレイヤ３を含み得る。示されていないが、ソフトウェアアーキテクチャ３００は、追加のレイヤ３サブレイヤ、並びにレイヤ３の上の様々な上位レイヤを含み得る。いくつかの実装形態では、ＲＲＣサブレイヤ３１３は、システム情報をブロードキャストすること、ページングすること、並びにＵＥ３２０とネットワークデバイス３５０との間のＲＲＣシグナリング接続を確立及び解放することを含む機能を提供し得る。
【００８１】
［0090］様々な実施形態では、ＳＤＡＰサブレイヤ３１７は、サービス品質（ＱｏＳ）フローとデータ無線ベアラ（ＤＲＢ）との間のマッピングを提供し得る。様々な実装形態では、ＰＤＣＰサブレイヤ３１２は、異なる無線ベアラと論理チャネルとの間の多重化、シーケンス番号付加、ハンドオーバデータ処理、完全性保護、暗号化、及びヘッダ圧縮を含む、アップリンク機能を提供し得る。ダウンリンクにおいて、ＰＤＣＰサブレイヤ３１２は、データパケットの順序配信、重複データパケット検出、完全性検証、解読、及びヘッダ復元を含む機能を提供し得る。
【００８２】
［0091］アップリンクにおいて、ＲＬＣサブレイヤ３１０は、上位レイヤデータパケットのセグメント化及び連結、損失したデータパケットの再送信、並びに自動再送要求（ＡＲＱ）を提供し得る。ダウンリンクにおいて、ＲＬＣサブレイヤ３１０機能は、順序が狂った受信を補償するためのデータパケットの並べ替え、上位レイヤデータパケットの再アセンブリ、及びＡＲＱを含み得る。
【００８３】
［0092］アップリンクにおいて、ＭＡＣサブレイヤ３０８は、論理チャネルとトランスポートチャネルとの間の多重化、ランダムアクセス手順、論理チャネル優先度、及びハイブリッドＡＲＱ（ＨＡＲＱ）動作を含む機能を提供し得る。ダウンリンクにおいて、ＭＡＣレイヤ機能は、セル内でのチャネルマッピング、逆多重化、間欠受信（ＤＲＸ）、及びＨＡＲＱ動作を含み得る。
【００８４】
［0093］ソフトウェアアーキテクチャ３００は、物理媒体を通して、データを送信するための機能を提供し得るが、ソフトウェアアーキテクチャ３００は、ＵＥ３２０における様々なアプリケーションへのデータ転送サービスを提供するための少なくとも１つのホストレイヤ３１４を更に含み得る。いくつかの実装形態では、少なくとも１つのホストレイヤ３１４によって提供されるアプリケーション固有機能は、ソフトウェアアーキテクチャと汎用プロセッサとの間のインターフェース２０６を提供し得る。
【００８５】
［0094］他の実装形態では、ソフトウェアアーキテクチャ３００は、ホストレイヤ機能を提供する１つ又は複数の上位論理レイヤ（トランスポート、セッション、プレゼンテーション、アプリケーションなど）を含み得る。例えば、いくつかの実装形態では、ソフトウェアアーキテクチャ３００は、それにおいて論理接続がパケットデータネットワーク（ＰＤＮ）ゲートウェイ（ＰＧＷ）において終端するネットワークレイヤ（インターネットプロトコル（ＩＰ）レイヤなど）を含み得る。いくつかの実装形態では、ソフトウェアアーキテクチャ３００は、それにおいて論理接続が別のデバイス（エンドユーザデバイス

、サーバなど）において終端するアプリケーションレイヤを含み得る。いくつかの実装形態では、ソフトウェアアーキテクチャ３００は、ＡＳ３０４中に、物理レイヤ３０６と通信ハードウェア（１つ又は複数の無線周波数（ＲＦ）トランシーバなど）との間のハードウェアインターフェース３１６を更に含み得る。

【００８６】

［0095］ 図４は、様々な実施形態において使用するのに好適な、ブートストラッピングアプリケーションセキュリティのための例示的なシステム４００ａを示すシステムブロック図である。図１Ａ～図４を参照すると、システム４００ａは、ＵＥ４０２、ＮＡＦ４０４、ＢＳＦ４０６、ホーム加入者サーバ（ＨＳＳ）４０８、及び加入者ロケータ機能（ＳＬＦ）４１０を含むことができる。

【００８７】

［0096］ 様々な実施形態では、ＵＥ４０２及びＢＳＦ４０６は、ＵＥをＢＳＦに対して認証するために認証動作を実行することができる。いくつかの実施形態では、ＢＳＦ４０６とＵＥ４０２との間のネゴシエーションは、Ｕｂインターフェースを介して認証動作を実行することができ、ＡＫＡなどのプロトコルを使用することができる。ＵＥ４０２は、Ｕａインターフェースを介してＮＡＦ４０４と通信することができる。様々な実施形態では、ＵＥ４０２及びＮＡＦ４０４は、事前のセキュリティアソシエーションを有していなくてもよい。ＵＥ４０２は、第１のセッション鍵、例えば、Ｋｓ＿ＮＡＦを生成することができる。ＮＡＦ４０４は、Ｚｎインターフェースを介してＢＳＦ４０６から第１のセッション鍵（例えば、Ｋｓ＿ＮＡＦ）を受信することができる。

【００８８】

［0097］ ＨＳＳ４０８は、ユーザセキュリティ設定（ＵＳＳ）（例えば、ＧＢＡユーザセキュリティ設定（ＧＵＳＳ））など、ＵＥ４０２のためのユーザ認証クレデンシャルを記憶し得るデータベース又は他の好適なデータストレージの役割を果たすことができる。いくつかの実施形態では、ＨＳＳ４０８は、ユーザ認証クレデンシャルを、ＩＰマルチメディアプライベート識別情報（ＩＭＰＩ）などのプライベート識別情報にマッピングすることができる。ＨＳＳ４０８は、Ｚｈインターフェースを介してこの情報及び他の情報をＢＳＦ４０６に通信することができる。ＳＬＦ４１０は、ＵＥ４０２に関する（すなわち、特定のＵＥに関する）情報を記憶するＨＳＳ４０８を識別するための情報を記憶し、提供することができる。ＢＳＦ４０６及びＳＬＦ４１０は、Ｄｚインターフェースを介して通信することができる。

【００８９】

［0098］ いくつかの実施形態では、ＵＥ４０２は、Ｕｂインターフェースを介して、様々なＧＢＡ方法（例えば、ＧＢＡ＿ＭＥ、ＧＢＡ＿Ｕ、２Ｇ ＧＢＡ、ＧＢＡ＿Ｄｉｇｅｓｔ等）など、ＢＳＦ４０６とのブートストラッピング動作を実行することができる。ＵＥ４０２によるブートストラッピング手順は、ＡＫＡベースのＫｓ＿（ｅｘｔ）＿ＮＡＦが生成される手順（例えば、ＰＳＫ識別情報（名前空間）「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」によって識別されるＧＢＡベースの認証）と、Ｋｓ＿ｉｎｔ＿ＮＡＦが生成される手順（例えば、ＰＳＫ識別情報（名前空間）「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」によって識別されるＧＢＡベースの認証）と、ＧＢＡ＿ＤｉｇｅｓｔベースのＫｓ＿ＮＡＦが生成される手順（例えば、ＰＳＫ識別情報（名前空間）「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」によって識別されるＧＢＡベースの認証）とを含み得る。いくつかの実施形態では、ＵＥ４０２によって実行されるブートストラッピング手順は、初期（又は第１の）Ｂ－ＴＩＤ及び初期（又は第１の）鍵（Ｋｓ）を取得するための元の（又は初期の）ブートストラッピング手順であり得るか、又は新しい（又はフレッシュな）Ｂ－ＴＩＤ及び新しい（又はフレッシュな）Ｋｓを取得するためのフレッシュな（例えば、再ネゴシエーション関連の）ブートストラッピング手順であり得る。

【００９０】

［0099］ 図５は、様々な実施形態による、ＰＳＫ再ネゴシエーションをサポートする

ための、ＵＥのプロセッサによって実行され得る方法５００を示すプロセスフロー図である。図１Ａ～図５を参照すると、方法５００の動作は、ＵＥ（例えば、１２０ａ～１２０ｅ、３２０、４０２）のプロセッサ（プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０など）によって実行され得る。図１Ａ～図５を参照すると、方法５００の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０のうちの１つ又は複数など、ＵＥ（例えば、１２０ａ～１２０ｅ、３２０、４０２）の１つ若しくは複数のプロセッサ、及び／又はトランシーバ２５６、２６６など、１つ若しくは複数のトランシーバであり得る。

【００９１】

［0100］ ブロック５０２において、プロセッサは、第１のＢ－ＴＩＤ及び第１のＫｓを取得するために、ＢＳＦとブートストラッピング手順を実行することを含む動作を実行することができる。例えば、実行されるブートストラッピング手順は、第１のＢ－ＴＩＤ及び第１のＫｓを取得するための元の（又は初期）ブートストラッピング手順であり得る。例えば、ブロック５０２の動作は、図４を参照しながら説明したブートストラッピング及び／又は他の認証手順を含み得る。ブロック５０２の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【００９２】

［0101］ ブロック５０４において、プロセッサは、第１のＢ－ＴＩＤと、ＵＥによってサポートされるブートストラッピング手順（第１のＢ－ＴＩＤに関連付けられた鍵（Ｋｓ）を生成するために使用されたブートストラッピング手順など）を識別する少なくとも１つのＰＳＫ名前空間と、そのブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す少なくとも１つの相関ＰＳＫ名前空間とを含む要求メッセージを生成することを含む動作を実行することができる。ブロック５０４における動作の一例として、第１の要求メッセージは、第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、を含み得る。ブロック５０４の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【００９３】

［0102］ 任意選択で、ブロック５０４において生成される第１の要求メッセージは、ＵＥによってサポートされる１つ、２つ、又はそれ以上の更なるブートストラッピング手順など、ＵＥによってサポートされる更なるブートストラッピング手順を識別する更なるＰＳＫ名前空間を含むことができる。任意選択で、ブロック５０４において生成される第１の要求メッセージは、任意の更なるブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す、１つ、２つ、又はそれ以上の更なる相関ＰＳＫ名前空間など、更なる相関ＰＳＫ名前空間を含み得る。示された各ＰＳＫ名前空間は、示されたＰＳＫ名前空間のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされるとき、それ自体のそれぞれの相関ＰＳＫ名前空間を有し得る。一例として、第１の要求メッセージは、第１のＢ－ＴＩＤと、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間と、その第２のブートストラッピング方法に関連付けられた第２のＢ－ＴＩＤと、を含み得る。

【００９４】

[0103] いくつかの実施形態では、ブロック５０４において生成される第１の要求メッセージは、ＣｌｉｅｎｔＨｅｌｌｏメッセージであり得る。ＣｌｉｅｎｔＨｅｌｌｏメッセージ内のＰＳＫ識別情報は、それぞれのＰＳＫ識別情報名前空間及びＢ－ＴＩＤを示すプレフィックスを含むことができる。プレフィックスの非限定的な例としては、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」、及び／又は「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」が挙げられる。プレフィックス「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」は、ＴＬＳセッション鍵を確立するためにＡＫＡベースのＫｓ＿（ｅｘｔ）＿ＮＡＦが使用されることをＵＥが受け入れることを示すために、ＰＳＫ識別情報において使用され得る。プレフィックス「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」は、ＴＬＳセッション鍵を確立するためにＫｓ＿ｉｎｔ＿ＮＡＦが使用されることをＵＥが受け入れることを示すために、ＰＳＫ識別情報において使用され得る。プレフィックス「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」は、ＴＬＳセッション鍵を確立するためにＧＢＡ＿ＤｉｇｅｓｔベースのＫｓ＿ＮＡＦが使用されることをＵＥが受け入れることを示すために、ＰＳＫ識別情報において使用される。様々な実施形態では、これらの含まれる識別子（例えば、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」、及び／又は「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」などのＰＳＫ識別情報名前空間）の各々に加えて、ＮＡＦがフレッシュなブートストラッピングを要求することを可能にするために、少なくとも１つの追加の（又は相関）ＰＳＫ識別情報名前空間を含めることができる。例えば、ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」が含まれる場合、相関ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」を含めることができ、ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」が含まれる場合、相関ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」を含めることができ、及び／又は、ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」が含まれる場合、相関ＰＳＫ識別情報名前空間「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」を含めることができる。同様に、相関付けられた実際の鍵のＰＳＫ識別情報名前空間と、ＰＳＫ識別情報名前空間ペアを示す再ネゴシエーションサポートとを、他のブートストラッピング方法のために含めることができる。

【００９５】

[0104] ブロック５０６において、プロセッサは、ＮＡＦサーバなどのネットワークエンティティに要求メッセージを送信することを含む動作を実行することができる。例えば、要求メッセージは、ネットワークエンティティへのＴＬＳトンネルの確立を試みるために送信され得る。ブロック５０６の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【００９６】

[0105] ブロック５０７において、プロセッサは、任意選択で、ＮＡＦサーバなどのネットワークエンティティから応答メッセージを受信することを含む動作を実行することができる。例えば、応答メッセージは、ＮＡＦからのＳｅｒｖｅｒＨｅｌｌｏメッセージであってもよい。ブロック５０７の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【００９７】

[0106] 判定ブロック５０８において、プロセッサは、（ＰＳＫ再ネゴシエーションに相関付けられる）相関ＰＳＫ名前空間の表示が、受信された応答メッセージ中に含まれるかどうかを判定することを含む動作を実行することができる。例えば、応答メッセージは、ＮＡＦからのＳｅｒｖｅｒＨｅｌｌｏメッセージであってもよい。相関ＰＳＫ名前空間の表示は、受信された応答メッセージに含まれる相関ＰＳＫ名前空間自体であってもよ

い。相関ＰＳＫ名前空間の表示は、受信された応答メッセージに含まれる相関ＰＳＫ名前空間のインデックスであってもよい。相関ＰＳＫ名前空間の表示は、リスト内の相関ＰＳＫ名前空間の位置であってもよい。プロセッサは、応答メッセージ中の表示（例えば、名前空間、インデックス、位置など）が、（ＰＳＫ再ネゴシエーションに相関付けられる）相関ＰＳＫ名前空間の表示であるか、又は選択されたＰＳＫ名前空間（選択されたサポートされるブートストラッピング手順）の表示であるかどうかを判定するために、応答メッセージをパースすることができる。相関ＰＳＫ名前空間の表示である表示（例えば、名前空間、インデックス、位置など）は、相関ＰＳＫ名前空間の表示を含む応答メッセージが受信されたことを示すことができる。選択されたＰＳＫ名前空間の表示である表示（例えば、名前空間、インデックス、位置など）は、相関ＰＳＫ名前空間の表示を含む応答メッセージが受信されなかったことを示すことができる。判定ブロック５０８の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【００９８】

［0107］ 応答メッセージが相関ＰＳＫ名前空間の表示（例えば、名前空間、インデックス、位置など）を含まないと判定したこと（すなわち、判定ブロック５０８＝「いいえ」）に応答して、プロセッサは、ブロック５１０において、第１のセッション鍵Ｋｓを使用してネットワーク要素（例えば、ＮＡＦサーバ）と通信することを含む動作を実行することができる。例えば、応答メッセージが（ＰＳＫ名前空間ではなく）ＰＳＫのインデックスを含む場合、これは、セキュア通信が現在の鍵を使用して進行し得ることを示し得る。ブロック５１０の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【００９９】

［0108］ 応答メッセージが相関ＰＳＫ名前空間の表示（例えば、名前空間、インデックス、位置など）を含むと判定したこと（すなわち、判定ブロック５０８＝「はい」）に応答して、プロセッサは、ブロック５１２において第２の（すなわち、新しい又はフレッシュな）Ｂ－ＴＩＤ及び第２の（すなわち、新しい又はフレッシュな）Ｋｓを取得するために、示されたブートストラッピング手順（すなわち、相関ＰＳＫ名前空間に関連するサポートされたブートストラッピング手順）をＢＳＦと実行することを含む動作を実行することができる。プロセッサは、応答メッセージを受信したことに基づいて、第２の（すなわち、新しい）Ｂ－ＴＩＤ及び第２の（すなわち、新しい）Ｋｓを取得するために、示されたブートストラッピング手順をＢＳＦと実行することを含む動作を実行することができる。例えば、実行されるブートストラッピング手順は、第２の（すなわち、新しい）Ｂ－ＴＩＤ及び第２の（すなわち、新しい）Ｋｓを取得するための新しい（又はフレッシュな）ブートストラッピング手順であり得る。例えば、ブロック５１２の動作は、ＰＳＫ再ネゴシエーションと、ＵＥにおける第２の（すなわち、新しい）Ｂ－ＴＩＤ及び第２の（すなわち、新しい）Ｋｓをもたらすために、後続の時間において実行される、図４を参照しながら説明したブートストラッピング手順及び／又は他の認証手順を含み得る。ブロック５１２の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０及びトランシーバ２５６、２６６を含み得る。

【０１００】

［0109］ ブロック５１４において、プロセッサは、第２の（すなわち、新しい）Ｂ－ＴＩＤ及びＰＳＫ名前空間を含む第２の要求メッセージを生成することを含む動作を実行することができる。一例として、ＰＳＫ名前空間は、第２の（すなわち、新しい）Ｂ－ＴＩＤ及び第２の（すなわち、新しい）Ｋｓをもたらすｇｂａ方法に対応するＰＳＫ名前空間であり得る。別の例として、ＰＳＫ名前空間は、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間であり得る。別の例として、第２の要求メッセージは、第２のＣｌｉｅｎｔＨｅｌｌｏメッセージであり得る。ブロック５０４の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びワイヤレストランシーバ２６６を含み得る。

【０１０１】
［0110］ ブロック５１６において、プロセッサは、第２の要求メッセージをネットワークエンティティ（例えば、ＮＡＦサーバ）に送信することを含む動作を実行することができる。例えば、第２の要求メッセージは、ＮＡＦへのＴＬＳトンネルを確立することを試みるために送信され得る。ブロック５１６の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。
【０１０２】
［0111］ ブロック５１８において、プロセッサは、第２の（すなわち、新しい）Ｋｓを使用して、セキュアな通信セッションを介してネットワークエンティティ（例えば、ＮＡＦサーバ）と通信することを含む動作を実行することができる。ブロック５１８の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０及びトランシーバ２５６、２６６を含み得る。
【０１０３】
［0112］ 図６は、様々な実施形態による、ＵＥとの通信をセキュアにするための、ネットワークエンティティ（例えば、ＮＡＦサーバ）のプロセッサによって実行され得る方法６００を示すプロセスフロー図である。図１Ａ～図６を参照すると、方法６００の動作は、ネットワークデバイス（例えば、１４２ａ、３５０）のプロセッサ（プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、４３２など）によって実行され得る。様々な実施形態では、方法６００の動作は、方法５００（図５Ａ）の動作と組み合わせて実行され得る。）。図１Ａ～図６を参照すると、方法６００の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０のうちの１つ若しくは複数などのネットワークデバイス（例えば、１４２ａ、３５０）の１つ若しくは複数のプロセッサ、及び／又はトランシーバ２５６、２６６などの１つ若しくは複数のトランシーバであってもよい。
【０１０４】
［0113］ ブロック６０２において、プロセッサは、Ｂ－ＴＩＤと、ＵＥによってサポートされるブートストラッピング手順を識別する少なくとも１つのＰＳＫ名前空間と、ブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す少なくとも１つの相関ＰＳＫ名前空間と、を含む要求メッセージを、ＵＥから受信することを含む動作を実行することができる。例えば、第１の要求メッセージは、第１のＢ－ＴＩＤと、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、を含み得る。ブロック６０２の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びワイヤレストランシーバ２６６を含み得る。
【０１０５】
［0114］ 任意選択で、ブロック６０２において受信される第１の要求メッセージは、ＵＥによってサポートされる１つ、２つ、又はそれ以上の更なるブートストラッピング手順など、ＵＥによってサポートされる更なるブートストラッピング手順を識別する更なるＰＳＫ名前空間を含み得る。任意選択で、ブロック６０２において受信される第１の要求メッセージは、任意の更なるブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す、１つ、２つ、又はそれ以上の更なる相関ＰＳＫ名前空間など、更なる相関ＰＳＫ名前空間を含み得る。示された各ＰＳＫ名前空間は、示されたＰＳＫ名前空間のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされるとき、それ自体のそれぞれの相関ＰＳＫ名前空間を有し得る。一例として、第１の要求メッセージは、第１のＢ－ＴＩＤと、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、ＵＥによってサポートされる第２のブートス

トラッピング手順を識別する第２のＰＳＫ名前空間と、第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間とを含み得る。

【０１０６】

［0115］ いくつかの実施形態では、ブロック６０２において受信される第１の要求メッセージは、ＣｌｉｅｎｔＨｅｌｌｏメッセージであり得る。ＣｌｉｅｎｔＨｅｌｌｏ内のＰＳＫ識別子は、方法５００（図５）のブロック５０４を参照して説明したように、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ」、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ」、及び／又は「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ」などのそれぞれのＰＳＫ識別情報名前空間を示すプレフィックス、並びに「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｕｉｃｃ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」、「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｄｉｇｅｓｔ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」、及び／又は「３ＧＰＰ－ｂｏｏｔｓｔｒａｐｐｉｎｇ－ｒｅｎｅｇｏｔｉａｔｉｏｎ」などの追加の（又は相関）ＰＳＫ識別情報名前空間を示すプレフィックスを含むことができる。

【０１０７】

［0116］ 判定ブロック６０４において、プロセッサは、ＵＥのためにＰＳＫ再ネゴシエーションが必要かどうかを判定することを含む動作を実行し得る。例えば、プロセッサは、ＰＳＫ再ネゴシエーションが必要かどうかを判定するために、Ｂ－ＴＩＤに関連付けられた鍵が規定時間を過ぎている（ｏｖｅｒａｇｅｄ）かどうかを判定することができる（例えば、規定時間を過ぎている鍵は、ＰＳＫ再ネゴシエーションが必要であることを示すことができる）。別の例として、プロセッサは、ＵＥが再ネゴシエーションをサポートするためのセキュリティクレデンシャルにアクセスできることを保証するためのセキュリティ対策として、デフォルトでＰＳＫ再ネゴシエーションを要求することができる。ブロック６０２の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【０１０８】

［0117］ ＰＳＫ再ネゴシエーションが必要でないという判定（すなわち、判定ブロック６０４＝「いいえ」）に応答して、プロセッサは、ブロック６０６において、ＧＢＡ手順を完了してＢＳＦから第１のセッション鍵Ｋｓを取得し、（例えば、ＳｅｒｖｅｒＨｅｌｌｏメッセージで）ＵＥに応答して、選択されたＧＢＡ方法を示し、第１のセッション鍵Ｋｓを使用してＵＥとの通信を開始することを含む動作を実行することができる。例えば、ＰＳＫ再ネゴシエーションは必要でないことがあり、ＵＥとの通信は現在の鍵を使用して進行し得る。ブロック６０６の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０及びトランシーバ２５６、２６６を含み得る。

【０１０９】

［0118］ ＰＳＫ再ネゴシエーションが必要であるという判定（すなわち、判定ブロック６０４＝「はい」）に応答して、プロセッサは、ブロック６０８において、選択されたＰＳＫ名前空間に相関付けられる（又は対応する）（ＰＳＫ再ネゴシエーションに相関付けられる）相関ＰＳＫ名前空間の表示を決定することを含む動作を実行することができる。選択されたＰＳＫ名前空間に相関付けられた相関ＰＳＫ名前空間の表示は、相関ＰＳＫ名前空間自体の表示であってもよい。相関ＰＳＫ名前空間の表示は、相関ＰＳＫ名前空間のインデックスであってもよい。相関ＰＳＫ名前空間の表示は、ＰＳＫ名前空間のリスト内の相関ＰＳＫ名前空間の位置であってもよい。例えば、ＮＡＦは、ＮＡＦがサポートしており、かつＵＥがサポートする（選択されたＰＳＫ名前空間によって識別される）ブートストラッピング手順に相関付けられた相関ＰＳＫ名前空間のインデックスを決定し得る。ブロック６０８の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【０１１０】

［0119］ ブロック６１０において、プロセッサは、相関ＰＳＫ名前空間の表示（例えば、名前空間、インデックス、位置など）を含む応答メッセージを生成することを含む動

作を実行することができる。例えば、応答メッセージは、相関ＰＳＫ名前空間のインデックスを含むＳｅｒｖｅｒＨｅｌｌｏメッセージとすることができる。ブロック６１０の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【０１１１】

［0120］ ブロック６１２において、プロセッサは、応答メッセージをＵＥに送信することを含む動作を実行することができる。ブロック６１２の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【０１１２】

［0121］ ブロック６１４において、プロセッサは、ＵＥから第２の要求メッセージを受信することを含む動作を実行することができる。例えば、第２の要求メッセージは、ＮＡＦへのＴＬＳトンネルを確立することを試みるために送信され得る。一例として、ＵＥからの第２の要求メッセージは、第２の（すなわち、新しい）Ｂ－ＴＩＤとともに、選択されたＧＢＡ方法に対応するＰＳＫ名前空間を含むＣｌｉｅｎｔＨｅｌｌｏメッセージであり得る。ブロック６１４の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【０１１３】

［0122］ ブロック６１６において、プロセッサは、ＧＢＡ手順を完了して、新しいＢ－ＴＩＤに基づいてＢＳＦから第２の（すなわち新しい）セッション鍵Ｋｓを取得することと、（例えばＳｅｒｖｅｒＨｅｌｌｏメッセージを用いて）ＵＥに応答して、選択されたＧＢＡ方法を示すことと、新しいＫｓを使用してＵＥとの通信を開始することと、を含む動作を実行することができる。ブロック６１６の動作を実行する手段は、プロセッサ２１０、２１２、２１４、２１６、２１８、２５２、２６０、及びトランシーバ２５６、２６６を含み得る。

【０１１４】

［0123］ 図７は、様々な実施形態において使用するのに好適なネットワークデバイス７００（例えばＮＡＦサーバ）の構成要素ブロック図である。そのようなネットワークデバイス（例えば、ネットワークデバイス１４２ａ、３５０）は、少なくとも図７に示す構成要素を含み得る。図１Ａ～図７を参照すると、ネットワークデバイス７００は、典型的には、揮発性メモリ７０２と、ディスクドライブ７０８などの大容量不揮発性メモリとに結合されたプロセッサ７０１を含むことができる。ネットワークデバイス７００はまた、プロセッサ７０１に結合されたフロッピーディスクドライブ、コンパクトディスク（ＣＤ）ドライブ、又はデジタルビデオディスク（ＤＶＤ）ドライブなどの周辺メモリアクセスデバイス７０６を含むことができる。ネットワークデバイス７００はまた、インターネット、又は他のシステムコンピュータ及びサーバに結合されたローカルエリアネットワークなどのネットワークとのデータ接続を確立するために、プロセッサ７０１に結合されたネットワークアクセスポート７０４（又はインターフェース）を含むことができる。ネットワークデバイス７００は、ワイヤレス通信リンクに接続され得る、電磁放射を送受信するための１つ又は複数のアンテナ７０７を含み得る。ネットワークデバイス７００は、周辺機器、外部メモリ、又は他のデバイスに結合するためのＵＳＢ、Ｆｉｒｅｗｉｒｅ、Ｔｈｕｎｄｅｒｂｏｌｔなどの追加のアクセスポートを含むことができる。

【０１１５】

［0124］ 図８は、様々な実施形態において使用するのに好適なＵＥ８００の構成要素ブロック図である。図１Ａ～図８を参照すると、様々な実施形態が、様々なＵＥ８００（例えば、ＵＥ１２０ａ～１２０ｅ、３２０、４０２）に実装され得、その一例が、スマートフォンの形態で図８に図示されている。ＵＥ８００は、第２のＳＯＣ２０４（例えば、５Ｇ対応ＳＯＣ）に結合された第１のＳＯＣ２０２（例えば、ＳＯＣ－ＣＰＵ）を含み得る。第１のＳＯＣ２０２及び第２のＳＯＣ２０４は、内部メモリ８１６、ディスプレイ８１２、及びスピーカ８１４に結合され得る。更に、ＵＥ８００は、第１のＳＯＣ２０２及

び／又は第２のＳＯＣ２０４内の１つ又は複数のプロセッサに結合されたワイヤレストランシーバ２６６に接続され得る、電磁放射を送受信するためのアンテナ８０４を含み得る。ＵＥ８００は、ユーザ入力を受信するためのメニュー選択ボタン又はロッカースイッチ８２０を含むことができる。

【０１１６】

［0125］ ＵＥ８００は、音声符号化／復号化（ＣＯＤＥＣ）回路８１０を含んでもよく、この回路８１０は、マイクロフォンから受信した音声をワイヤレス伝送に好適なデータパケットにデジタル化し、受信した音声データパケットを復号して、音声を生成するためにスピーカに提供されるアナログ信号を生成する。第１のＳＯＣ２０２及び第２のＳＯＣ２０４におけるプロセッサ、ワイヤレストランシーバ２６６、及びコーデック８１０のうちの１つ又は複数は、デジタル信号プロセッサ（ＤＳＰ）回路（個別に図示せず）を含み得る。

【０１１７】

［0126］ ネットワークデバイス７００及びＵＥ８００のプロセッサは、以下で説明されるいくつかの実装形態の機能を含む、様々な機能を実行するようにソフトウェア命令（アプリケーション）によって構成され得る任意のプログラマブルマイクロプロセッサ、マイクロコンピュータ、あるいは１つ又は複数のマルチプルプロセッサチップであり得る。いくつかのＵＥでは、ワイヤレス通信機能専用のＳＯＣ２０４内の１つのプロセッサ、及び他のアプリケーションの実行専用のＳＯＣ２０２内の１つのプロセッサなど、複数のプロセッサが設けられ得る。ソフトウェアアプリケーションは、それらがアクセスされプロセッサにロードされる前に、メモリ７０２、８１６に記憶され得る。プロセッサは、アプリケーションソフトウェア命令を記憶するのに十分な内部メモリを含み得る。

【０１１８】

［0127］ 本出願で使用する場合、「構成要素」、「モジュール」、「システム」などの用語は、限定はしないが、特定の動作又は機能を実行するように構成される、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合せ、ソフトウェア、又は実行中のソフトウェアなど、コンピュータ関連エンティティを含むものとする。例えば、構成要素は、限定はしないが、プロセッサ上で実行しているプロセス、プロセッサ、オブジェクト、実行ファイル、実行スレッド、プログラム、又はコンピュータであり得る。例として、ＵＥ上で実行されているアプリケーションとＵＥの両方は、構成要素と呼ばれる場合がある。１つ以上の構成要素は、プロセス又は実行スレッド内に存在することがあり、構成要素は、１つのプロセッサ若しくはコアに局在し得るか、又は２つ以上のプロセッサ若しくはコアの間で分散され得る。加えて、これらの構成要素は、様々な命令又はデータ構造がその上に記憶されている様々な非一時的コンピュータ可読媒体から実行し得る。構成要素は、ローカルプロセス又はリモートプロセス、関数呼出し又はプロシージャ呼出し、電子信号、データパケット、メモリ読み出し／書き込み、及び他の知られているネットワーク、コンピュータ、プロセッサ、又はプロセス関連の通信方法によって通信し得る。

【０１１９】

［0128］ いくつかの異なるセルラー通信及びモバイル通信のサービス及び規格が利用可能であるか、又は将来において企図され、それらのすべてが様々な実施形態を実装し、様々な実施形態から利益を得ることができる。そのようなサービス及び規格は、例えば、第３世代パートナーシッププロジェクト（３ＧＰＰ）、ロングタームエボリューション（ＬＴＥ）システム、第３世代ワイヤレスモバイル通信技術（３Ｇ）、第４世代ワイヤレスモバイル通信技術（４Ｇ）、第５世代ワイヤレスモバイル通信技術（５Ｇ）、更に後の世代の３ＧＰＰ技術、モバイル通信用グローバルシステム（ＧＳＭ）、ユニバーサル移動体通信システム（ＵＭＴＳ）、３ＧＳＭ、汎用パケット無線サービス（ＧＰＲＳ）、符号分割多元接続（ＣＤＭＡ）システム（例えばｃｄｍａＯｎｅ、ＣＤＭＡ１０２０（登録商標））、ＧＳＭ進化型高速データレート（ＥＤＧＥ）、高度モバイルフォンシステム（ＡＭＰＳ）、デジタルＡＭＰＳ（ＩＳ－１３６／ＴＤＭＡ）、エボリューションデータオプティマイズド（ＥＶ－ＤＯ）、デジタル強化コードレス電気通信（ＤＥＣＴ：digital en

hanced cordless telecommunications）、ワールドワイドインターオペラビリティフォーマイクロウェーブアクセス（ＷｉＭＡＸ）、ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）、Ｗｉ－Ｆｉ保護アクセスＩ　＆　ＩＩ（ＷＰＡ、ＷＰＡ２）、及び統合デジタル拡張ネットワーク（ｉＤＥＮ）を含む。これらの技術の各々は、例えば、音声、データ、シグナリング、及び／又はコンテンツメッセージの送信及び受信を伴う。個々の電気通信の規格又は技術に関係する用語及び／又は技術的詳細に対するいかなる言及も例示目的にすぎず、請求項の文言に具体的に記載されない限り、特許請求の範囲の範囲を特定の通信システム又は通信技術に限定するものではないことを理解されたい。

【０１２０】

［0129］図示及び説明する様々な実施形態は、特許請求の範囲の様々な特徴を示すための例として提供されるにすぎない。しかしながら、任意の所与の実施形態に関して図示及び説明される特徴は、必ずしも関連する実施形態に限定されるとは限らず、図示及び説明される他の実施形態とともに使用されてよく、又はそれらと組み合わせられてもよい。更に、特許請求の範囲は、いかなる例示的な一実施形態によっても限定されるものでない。例えば、本明細書に記載された方法及び動作の１つ又は複数を、方法及び動作の１つ又は複数の動作に置き換えるか、又はそれらと組み合わせることができる。

【０１２１】

［0130］実装例について、以下の段落において説明する。以下の実施例のうちのいくつかは、例示的な方法に関して説明されるが、更なる例示的な実装は、以下の実施例の方法の動作を実行するためのプロセッサ実行可能命令で構成されたプロセッサを含むＵＥ又はネットワークデバイスによって実装される以下の段落で説明される例示的な方法、以下の実施例の方法の機能を実行するための手段を含む、ＵＥ又はネットワークデバイスによって実装される、以下の段落に記載される例示的な方法、を含み得る。以下の段落で説明する例示的な方法は、以下の実施例の方法の動作をＵＥ又はネットワークデバイスのプロセッサに実行させるように構成されたプロセッサ実行可能命令を記憶する非一時的プロセッサ可読記憶媒体として実装することができる。

【０１２２】

［0131］実施例１．ユーザ機器（ＵＥ）のプロセッサによって実行される事前共有鍵（ＰＳＫ）再ネゴシエーションをサポートするための方法など、ＵＥによって実行される方法であって、第１の要求メッセージを生成することであって、第１の要求メッセージが、第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、を含む、生成することと、第１の要求メッセージをネットワークアプリケーション機能（ＮＡＦ）に送信することと、

を含む、方法。

【０１２３】

［0132］実施例２．第１の相関ＰＳＫ名前空間の表示を含む応答メッセージをＮＡＦから受信することと、応答メッセージを受信することに基づいて、第２のＢ－ＴＩＤ及びセッション鍵（Ｋｓ）を取得するためにブートストラッピング手順を実行することと、を更に含む、実施例１に記載の方法。

【０１２４】

［0133］実施例３．ブートストラッピング手順を実行することが、第２のＢ－ＴＩＤ及び第２のセッション鍵（Ｋｓ）を取得するために第１のブートストラッピング手順を再実行することを含む、実施例２に記載の方法。

【０１２５】

［0134］実施例４．第２のＢ－ＴＩＤと第１の相関ＰＳＫ名前空間とを含む第２の要求メッセージを生成することと、第２の要求メッセージをＮＡＦに送信することと、を更に含む、実施例２又は３のいずれかに記載の方法。

【０１２６】

［0135］実施例５．第１の相関ＰＳＫ名前空間の表示が、応答メッセージ内の第１の相関ＰＳＫ名前空間である、実施例２から４のいずれか一項に記載の方法。
【０１２７】
［0136］実施例６．第１の相関ＰＳＫ名前空間の表示が、第１の相関ＰＳＫ名前空間のインデックス又はリスト内の第１の相関ＰＳＫ名前空間の位置である、実施例２から５のいずれか一項に記載の方法。
【０１２８】
［0137］実施例７．第２のＫｓを使用してＮＡＦと通信することを更に含む、実施例１から６のいずれか一項に記載の方法。
【０１２９】
［0138］実施例８．第１の要求メッセージが、ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第２の相関ＰＳＫ名前空間と、を更に含む、実施例１から７のいずれか一項に記載の方法。
【０１３０】
［0139］実施例９．第１の要求メッセージが、クライアントが開始するハローメッセージである、実施例１から８のいずれか一項に記載の方法。
【０１３１】
［0140］実施例１０．ネットワークデバイスのプロセッサによって実行される事前共有鍵（ＰＳＫ）再ネゴシエーションをサポートするためにネットワークデバイスによって実行される方法など、ネットワークデバイスによって実行される方法であって、ネットワークデバイスによって、ユーザ機器（ＵＥ）から、第１の要求メッセージを受信することであって、第１の要求メッセージが、第１のブートストラッピングトランザクション識別子（Ｂ－ＴＩＤ）と、ＵＥによってサポートされる第１のブートストラッピング手順を識別する第１のＰＳＫ名前空間と、第１のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第１の相関ＰＳＫ名前空間と、を含む、受信することと、第１の要求メッセージを受信した後に、ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定することと、ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定したことに応答して、第１の相関ＰＳＫ名前空間のためのＰＳＫ再ネゴシエーションの表示を決定することと、第１の相関ＰＳＫ名前空間の表示を含む応答メッセージを生成することと、応答メッセージをＵＥに送信することと、を含む、方法。
【０１３２】
［0141］実施例１１．第１の相関ＰＳＫ名前空間の表示が、第１の相関ＰＳＫ名前空間である、実施例１０に記載の方法。
【０１３３】
［0142］実施例１２．第１の相関ＰＳＫ名前空間の表示が、第１の相関ＰＳＫ名前空間のインデックスである、又はリスト内の第１の相関ＰＳＫ名前空間の位置である、実施例１０に記載の方法。
【０１３４】
［0143］実施例１３．第２のＢ－ＴＩＤ及び第１の相関ＰＳＫ名前空間のみを含む第２の要求メッセージを、ＵＥからネットワークデバイスによって受信すること、を更に含む、実施例１０から１２のいずれか一項に記載の方法。
【０１３５】
［0144］実施例１４．第２のＢ－ＴＩＤを使用してブートストラッピングセキュリティ機能（ＢＳＦ）から取得されたセッション鍵（Ｋｓ）を使用してＵＥと通信すること、を更に含む、実施例１３に記載の方法。
【０１３６】
［0145］実施例１５．第１の要求メッセージが、ＵＥによってサポートされる第２のブートストラッピング手順を識別する第２のＰＳＫ名前空間と、第２のブートストラッピング手順のためにＰＳＫ再ネゴシエーションがＵＥによってサポートされることを示す第

２の相関ＰＳＫ名前空間と、を更に含み、第１の要求メッセージを受信した後に、ＵＥのためにＰＳＫ再ネゴシエーションが必要であると判定することが、ＵＥによってサポートされる第１のブートストラッピング手順及びＵＥによってサポートされる第２のブートストラッピング手順の選択肢から、ＵＥによってサポートされる第１のブートストラッピング手順を選択することと、第１のブートストラッピング手順のために再ネゴシエーションが必要であると判定することと、ＵＥによってサポートされる第１のブートストラッピング手順を選択したことに応答して、第１の相関ＰＳＫ名前空間の表示を決定することと、を含む、

実施例１０から１４のいずれか一項に記載の方法。

【０１３７】

[0146] 実施例１６．応答メッセージが、サーバが開始するハローメッセージである、実施例１０から１５のいずれか一項に記載の方法。

【０１３８】

[0147] 実施例１７．ネットワークデバイスがネットワークアプリケーション機能（ＮＡＦ）サーバである、実施例１０から１６のいずれか一項に記載の方法。

【０１３９】

[0148] 上記の方法の説明及びプロセスフロー図は、例示的な例として提供されるにすぎず、様々な実施形態の動作が、提示された順序で実行されなければならないことを要求又は暗示するものではない。当業者によって諒解されるように、上述の実施形態における動作の順序は、任意の順序で実施されてもよい。「その後（thereafter）」、「次いで（then）」、「次に（next）」などの語は、動作の順序を限定するものではない。これらの語は、方法の説明を通じて読み手を導くために使用される。更に、例えば、冠詞「ａ」、「ａｎ」又は「ｔｈｅ」を使用する単数形での請求項要素へのいかなる言及も、要素を単数形に限定するものとして解釈されるべきではない。

【０１４０】

[0149] 本明細書で開示する実施形態に関して説明する様々な例示的な論理ブロック、モジュール、構成要素、回路、及びアルゴリズム動作は、電子ハードウェア、コンピュータソフトウェア、又はその両方の組合せとして実装され得る。ハードウェア及びソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路及び動作について、概してそれらの機能性に関して上記してきた。そのような機能がハードウェアとして実装されるのか又はソフトウェアとして実装されるのかは、特定の適用例及びシステム全体に課される設計上の制約に依存する。当業者は、説明した機能性を特定の適用例ごとに様々な方法で実装してよいが、そのような実施形態の決定は、特許請求の範囲からの逸脱を引き起こすものとして解釈されるべきではない。

【０１４１】

[0150] 本明細書で開示する実施形態に関して説明する様々な例示的な論理、論理ブロック、モジュール、及び回路を実装するために使用されるハードウェアは、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）若しくは他のプログラマブル論理デバイス、個別ゲート若しくはトランジスタ論理、個別ハードウェア構成要素、又は本明細書で説明する機能を実行するように設計されたそれらの任意の組合せを用いて実装又は実行され得る。汎用プロセッサはマイクロプロセッサであってもよいが、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、又は状態機械であってもよい。プロセッサはまた、受信機スマートオブジェクトの組合せ、例えば、ＤＳＰとマイクロプロセッサの組合せ、複数のマイクロプロセッサ、ＤＳＰコアと連携する１つ若しくは複数のマイクロプロセッサ、又は任意の他のそのような構成として実装されてもよい。代替的に、いくつかの動作又は方法は、所与の機能に固有の回路によって実行されてもよい。

【０１４２】

[0151] １つ又は複数の実施形態では、説明した機能は、ハードウェア、ソフトウェ

ア、ファームウェア、又はそれらの任意の組合せで実装されてもよい。ソフトウェアにおいて実装される場合、機能は、非一時的コンピュータ可読記憶媒体又は非一時的プロセッサ可読記憶媒体上に１つ又は複数の命令又はコードとして記憶されてもよい。本明細書で開示する方法又はアルゴリズムの動作は、非一時的コンピュータ可読又はプロセッサ可読記憶媒体に存在し得るプロセッサ実行可能ソフトウェアモジュール又はプロセッサ実行可能命令において具現化されてもよい。非一時的コンピュータ可読又はプロセッサ可読記憶媒体は、コンピュータ又はプロセッサによってアクセスされ得る任意の記憶媒体であってもよい。限定ではなく例として、そのような非一時的コンピュータ可読又はプロセッサ可読記憶媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、ＦＬＡＳＨメモリ、ＣＤ－ＲＯＭ若しくは他の光ディスクストレージ、磁気ディスクストレージ若しくは他の磁気ストレージスマートオブジェクト、又は命令若しくはデータ構造の形態で所望のプログラムコードを記憶するために使用される場合があり、コンピュータによってアクセスされる場合がある任意の他の媒体を含んでもよい。本明細書で使用するディスク（Disk）及びディスク（disc）は、コンパクトディスク（disc）（ＣＤ）、レーザーディスク（disc）、光ディスク（disc）、デジタル多用途ディスク（disc）（ＤＶＤ）、フロッピーディスク（disk）、及びＢｌｕ－ｒａｙディスク（disc）を含み、ここで、ディスク（disk）は、通常、データを磁気的に再生し、ディスク（disc）は、レーザーを用いてデータを光学的に再生する。上記の組合せも、非一時的コンピュータ可読及びプロセッサ可読媒体の範囲内に含まれる。更に、方法又はアルゴリズムの動作は、非一時的プロセッサ可読記憶媒体及び／又は非一時的コンピュータ可読記憶媒体上のコード及び／又は命令の１つ又は任意の組合せ又はセットとして存在してもよく、これらの記憶媒体は、コンピュータプログラム製品内に組み込まれてもよい。

【０１４３】

［0152］ 開示する実施形態の前述の説明は、任意の当業者が特許請求の範囲を製作又は使用することを可能にするために提供される。これらの実施形態への様々な修正が当業者には容易に明らかになり、本明細書で定義される一般原理は、特許請求の範囲から逸脱することなく他の実施形態に適用されてよい。従って、本開示は、本明細書で示される実施形態に限定されるように意図されるものではなく、以下の特許請求の範囲並びに本明細書において開示する原理及び新規の特徴に一致する最も広い範囲を与えられるべきである。

【図面】

【図１Ａ】

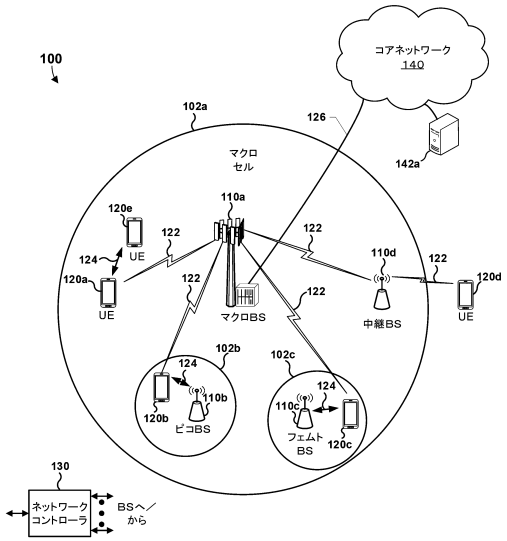


FIG. 1A

【図１Ｂ】

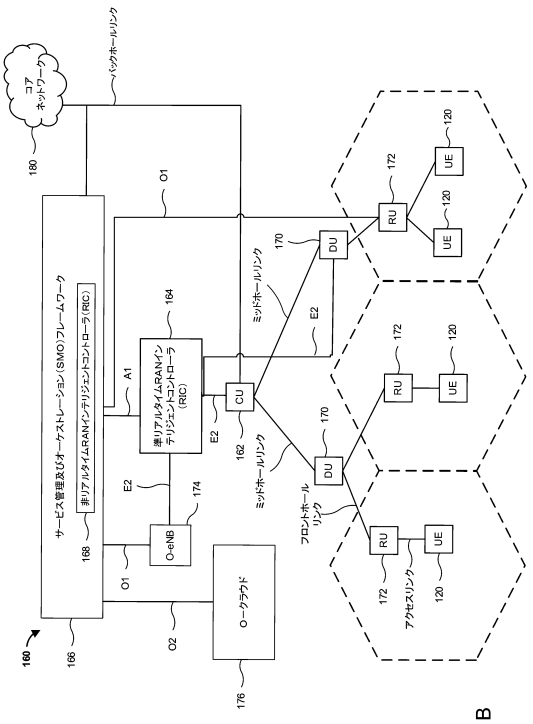


FIG. 1B

【図２】

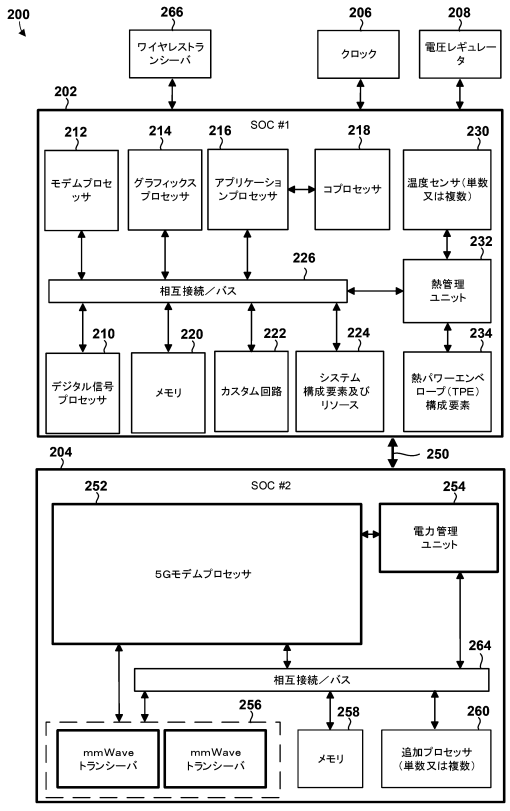


FIG. 2

【図３】

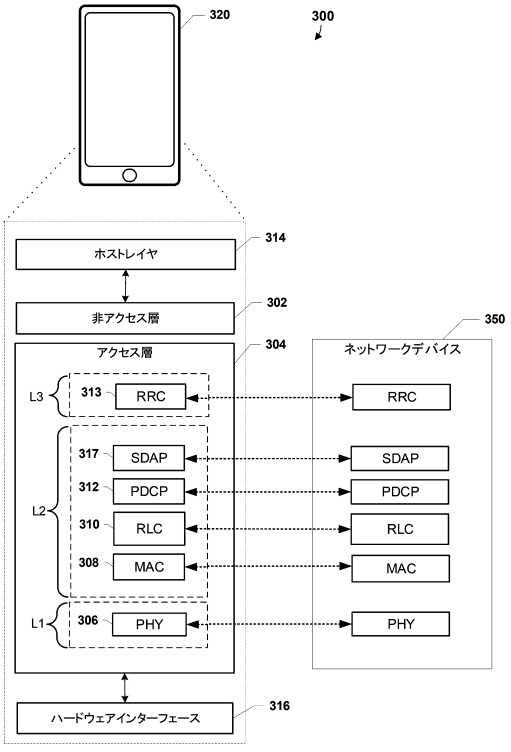


FIG. 3

【図４】

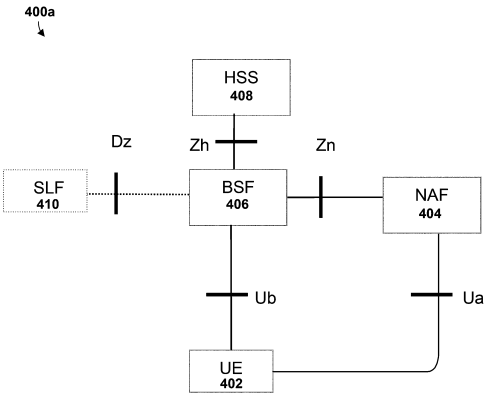


FIG. 4

【図５】

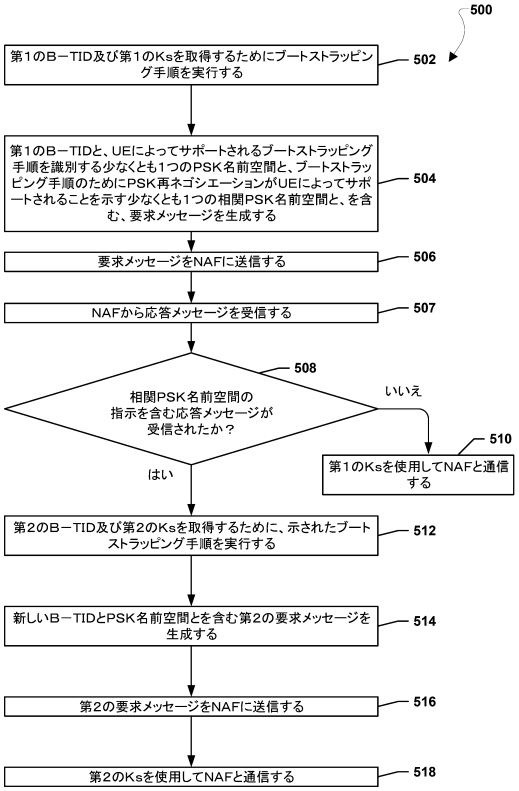


FIG. 5

【図６】

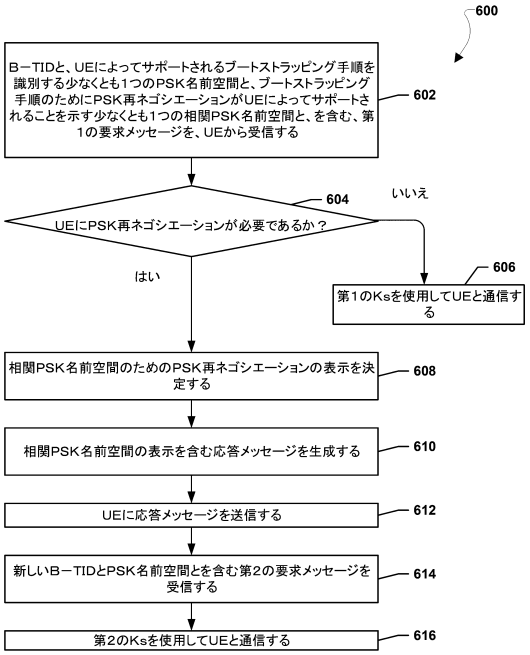


FIG. 6

【図７】

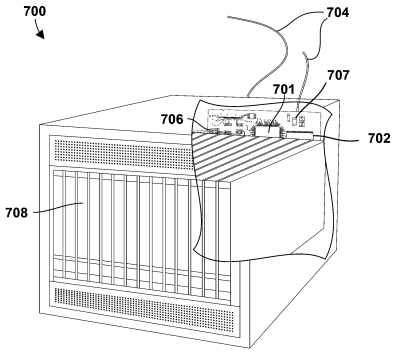


FIG. 7

【図８】

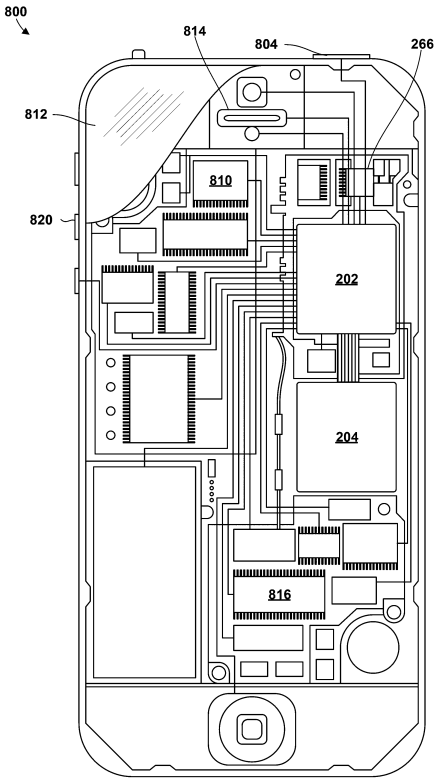


FIG. 8

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/048150

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/041 H04W12/043 H04W12/06
ADD. H04L9/40

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/389788 A1 (SMEETS BERNARD [SE] ET AL) 10 December 2020 (2020-12-10)	1-4, 7-10, 13-21, 24-27, 30-35
A	paragraphs [0050] - [0053], [0061] - [0063], [0068], [0131], [0139] - [0144]; figure 5	5,6,11, 12,22, 23,28,29
X	US 2013/067552 A1 (HAWKES PHILIP MICHAEL [AU] ET AL) 14 March 2013 (2013-03-14)	1-4,7,9, 10, 13-21, 24-27, 30-35
A	paragraphs [0078] - [0080], [0091] - [0093], [0504] - [0515], [0978] - [0981] paragraphs [1048] - [1055], [1185] - [1189], [1380] - [1384]	5,6,8, 11,12, 22,23, 28,29

-/--

[x] Further documents are listed in the continuation of Box C. [x] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 February 2023	20/02/2023

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Betz, Sebastian

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/048150

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	CN 114 726 520 A (H3C HOLDING LTD) 8 July 2022 (2022-07-08) paragraphs [0006] - [0014], [0120] - [0132]	1-35

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2022/048150

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020389788 A1	10-12-2020	EP 3718330 A1	07-10-2020
		US 2020389788 A1	10-12-2020
		WO 2019108100 A1	06-06-2019
US 2013067552 A1	14-03-2013	CN 103370915 A	23-10-2013
		CN 105491070 A	13-04-2016
		EP 2636203 A1	11-09-2013
		JP 5876063 B2	02-03-2016
		JP 6185017 B2	23-08-2017
		JP 2013546260 A	26-12-2013
		JP 2016007004 A	14-01-2016
		KR 20130089655 A	12-08-2013
		KR 20140137454 A	02-12-2014
		US 2013067552 A1	14-03-2013
		US 2014093081 A1	03-04-2014
		US 2014094147 A1	03-04-2014
		US 2016337861 A1	17-11-2016
		WO 2012087435 A1	28-06-2012
CN 114726520 A	08-07-2022	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

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

（特許庁注：以下のものは登録商標）
１．ＷＣＤＭＡ
２．３ＧＰＰ
３．ＺＩＧＢＥＥ
４．ＢＬＵＥＴＯＯＴＨ
５．Ｌｉｎｕｘ
６．ＯＳ Ｘ
７．ＦＩＲＥＷＩＲＥ
８．ＴＨＵＮＤＥＲＢＯＬＴ
９．Ｂｌｕ－ｒａｙ

２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 リ、ス・ボム
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 キム、ホンギル
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

Ｆターム（参考） 5K067 AA30 DD23 DD24 EE02 EE10 EE16 HH36