(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7612286号
(P7612286)

(45)発行日　令和7年1月14日(2025.1.14)

(24)登録日　令和6年12月27日(2024.12.27)

(51)国際特許分類

		FI	
H04W	*12/062 (2021.01)*	H04W	12/062
H04W	*12/0471(2021.01)*	H04W	12/0471
H04W	*92/12 (2009.01)*	H04W	92/12
H04W	*88/14 (2009.01)*	H04W	88/14

請求項の数　13　外国語出願　（全37頁）

(21)出願番号　特願2023-116614(P2023-116614)
(22)出願日　令和5年7月18日(2023.7.18)
(62)分割の表示　特願2020-573395(P2020-573395)の分割
原出願日　令和1年6月28日(2019.6.28)
(65)公開番号　特開2023-156302(P2023-156302A)
(43)公開日　令和5年10月24日(2023.10.24)
審査請求日　令和5年8月16日(2023.8.16)
(31)優先権主張番号　62/692,722
(32)優先日　平成30年6月30日(2018.6.30)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　513311642
ノキア ソリューションズ アンド ネットワークス オサケユキチュア
フィンランド国，０２６１０ エスプー，カラカーリ ７
(74)代理人　100094569
弁理士　田中 伸一郎
(74)代理人　100109070
弁理士　須田 洋之
(74)代理人　100067013
弁理士　大塚 文昭
(74)代理人　100120525
弁理士　近藤 直樹
(74)代理人　100167911
弁理士　豊島 匠二

最終頁に続く

(54)【発明の名称】　５ＧＣＮへの非３ＧＰＰアクセスが許可されない失敗の対処

(57)【特許請求の範囲】

【請求項１】

信頼されていない非第３世代パートナシッププロジェクト（非３ＧＰＰ）アクセスネットワークを介した第５世代コアネットワーク（５ＧＣＮ）へのネットワーク接続を管理するためのインターワーキング機能ノード（Ｎ３ＩＷＦ）であって、前記Ｎ３ＩＷＦは、

前記信頼されていない非３ＧＰＰアクセスネットワークを介してユーザ機器（ＵＥ）と通信するように構成された第１のネットワークインタフェースと、

前記５ＧＣＮ内のアクセス及びモビリティ管理機能（ＡＭＦ）と通信するように構成された第２のネットワークインタフェースと、

処理デバイスであって、

前記信頼されていない非３ＧＰＰアクセスネットワークを介して前記ＵＥから受信された、前記５ＧＣＮへの安全な接続を確立するための要求を処理して、前記５ＧＣＮの前記ＡＭＦへの要求を生成することと、

前記第２のネットワークインタフェースを介して、前記５ＧＣＮ内の前記ＡＭＦに、認証及び安全な接続確立要求を提供することと、

前記認証及び安全な接続確立要求に応答する前記５ＧＣＮ内の前記ＡＭＦからのレスポンスに基づいて、信頼されていない非３ＧＰＰアクセスネットワークを介した安全な接続の確立が前記５ＧＣＮによって許可されないと判定することと、

いずれの信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮへのアクセスも前記５ＧＣＮが許可しないことを示す５Ｇモビリティ管理（５ＧＭＭ）原因

値を含むレスポンスメッセージを前記ＵＥに提供することと、
　前記レスポンスメッセージに応答して、前記ＵＥから、前記信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮへの前記安全な接続を確立するための前記要求を終了するストップメッセージを受信することであって、前記ストップメッセージは、メッセージ識別子フィールドを含み、前記メッセージ識別子フィールドは、前記信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮへの前記安全な接続を確立するための前記要求を前記ＵＥが終了するつもりであることを示す５Ｇ－Ｓｔｏｐ識別子を含む、前記受信することと、
　を前記Ｎ３１ＷＦに実行させるように構成されている、処理デバイスと
を備える、Ｎ３ＩＷＦ。
【請求項２】
　前記処理デバイスは、さらに、
　前記ＵＥから、前記信頼されていない非３ＧＰＰアクセスネットワークを介して、前記第１のネットワークインタフェースを通じて、前記５ＧＣＮへの前記安全な接続を確立するための前記要求を受信することと、
　前記５ＧＣＮの前記ＡＭＦから、前記第２のネットワークインタフェースを通じて、認証及びサブスクリプションチェックのための要求に対する前記レスポンスを受信することと、
　いずれの信頼されていない非３ＧＰＰアクセスネットワークを介した安全な接続確立も前記５ＧＣＮが許可しないことを示す前記５ＧＭＭ原因値を含む非アクセス層（ＮＡＳ）ペイロードを有するインターネット鍵交換（ＩＫＥ）レスポンスメッセージを前記ＵＥに対して生成することと、
を前記Ｎ３１ＷＦに実行させるように構成されている、請求項１に記載のＮ３ＩＷＦ。
【請求項３】
　前記処理デバイスは、さらに、
　前記５ＧＣＮの前記ＡＭＦから、いずれの信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮへの安全な接続確立も前記５ＧＣＮが許可しない旨のインディケーションを含む登録拒否メッセージをカプセル化しているレスポンスを受信することと、
　信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮとの安全な接続確立を前記５ＧＣＮが許可しないことを示すメッセージタイプを含むペイロードを有する前記ＩＫＥレスポンスメッセージを生成することと、
を前記Ｎ３１ＷＦに実行させるように構成されている、請求項２に記載のＮ３ＩＷＦ。
【請求項４】
　前記処理デバイスは、さらに、
　失敗理由を示すプライベート通知メッセージタイプを含む通知ペイロードを有する前記ＩＫＥレスポンスメッセージを生成すること、または
　信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮとの接続確立及び接続が前記５ＧＣＮによって許可されないことを示す前記プライベート通知メッセージタイプを含む前記通知ペイロードを有する前記ＩＫＥレスポンスメッセージを生成すること、
のいずれかによって前記Ｎ３１ＷＦに前記ＩＫＥレスポンスメッセージを生成させるように構成されている、請求項２に記載のＮ３ＩＷＦ。
【請求項５】
　前記処理デバイスは、さらに、
　前記ＵＥから前記ストップメッセージを受信したことに応答して、前記ＵＥに対して失敗メッセージを生成することと、
　前記ＵＥから受信された前記ストップメッセージを処理することであって、前記ストップメッセージはメッセージ識別子フィールドを有する５Ｇ－Ｓｔｏｐメッセージ形式を含み、前記メッセージ識別子フィールドは５Ｇ－Ｓｔｏｐ識別子を含む、前記処理すること

と、
を前記Ｎ３１ＷＦに実行させるように構成されている、請求項１に記載のＮ３ＩＷＦ。
【請求項６】
前記信頼されていない非３ＧＰＰアクセスネットワークを介して前記ＵＥから受信された安全な接続確立のための登録要求が、前記５ＧＣＮとのＩＰｓｅｃセキュリティアソシエーション（ＳＡ）を開始するためのＩＫＥ要求メッセージを含む、請求項１に記載のＮ３ＩＷＦ。
【請求項７】
第５世代コアネットワーク（５ＧＣＮ）のインターワーキング機能ノード（Ｎ３ＩＷＦ）からのネットワーク接続要求に対処するためのアクセス及びモビリティ管理機能（ＡＭＦ）デバイスであって、前記ＡＭＦデバイスは、
前記５ＧＣＮ内の前記Ｎ３ＩＷＦ並びに認証及びサブスクリプション機能（ＡＵＳＦ）と通信するように構成されたネットワークインタフェースと、
処理デバイスであって、
前記Ｎ３ＩＷＦがユーザ機器（ＵＥ）から受信した、信頼されていない非第３世代パートナシッププロジェクト（非３ＧＰＰ）アクセスネットワークを介した前記５ＧＣＮとの安全な接続を確立するための登録要求に関連する認証及び安全な接続確立要求を、前記Ｎ３ＩＷＦから前記ネットワークインタフェースを介して受信することと、
前記認証及び安全な接続確立要求を受信したことに応答して、前記５ＧＣＮの前記ＡＵＳＦに、認証及びサブスクリプションチェックのための要求を提供することと、
前記ＡＵＳＦによる前記認証及びサブスクリプションチェックが失敗したと判定したことに応答して、いずれの信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮへのアクセスも前記５ＧＣＮが許可しない旨のインディケーションをレスポンスメッセージにカプセル化することにより、前記Ｎ３ＩＷＦから受信された前記認証及び安全な接続確立要求に応答して前記レスポンスメッセージを生成することと、
前記レスポンスメッセージを前記Ｎ３ＩＷＦに提供することと、
を前記ＡＭＦデバイスに実行させるように構成されている、処理デバイスと
を備える、ＡＭＦ。
【請求項８】
前記処理デバイスは、さらに、
いずれの信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮとの安全な接続確立も前記５ＧＣＮが許可しない旨の前記インディケーションを含む登録拒否メッセージを前記レスポンスメッセージにカプセル化することを前記ＡＭＦデバイスに実行させるように構成されている、請求項７に記載のＡＭＦデバイス。
【請求項９】
前記処理デバイスは、さらに、
前記レスポンスメッセージに、拡張認証プロトコル（ＥＡＰ）失敗インディケーションを生成することを前記ＡＭＦデバイスに実行させるように構成されている、請求項８に記載のＡＭＦデバイス。
【請求項１０】
ユーザ機器（ＵＥ）であって、
信頼されていない非第３世代パートナシッププロジェクト（非３ＧＰＰ）アクセスネットワークを介して第５世代コアネットワーク（５ＧＣＮ）のインターワーキング機能ノード（Ｎ３ＩＷＦ）と通信するように構成されたネットワークインタフェースと、
処理デバイスであって、
前記５ＧＣＮとの安全な接続確立のための登録要求を生成することと、
前記信頼されていない非３ＧＰＰネットワークを介して、前記５ＧＣＮの前記Ｎ３ＩＷＦに、前記５ＧＣＮとの安全な接続確立のための前記要求を含むメッセージを送信することと、
前記要求に応答して、前記５ＧＣＮの前記Ｎ３ＩＷＦから、いずれの信頼されていな

い非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮとの安全な接続確立も前記５ＧＣＮが許可しないことを示す５Ｇモビリティ管理（５ＧＭＭ）原因値を含むレスポンスメッセージを受信することと、

前記レスポンスメッセージから、いずれの信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮとの安全な接続確立も前記５ＧＣＮが許可しないと判定することと、

いずれの信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮとの安全な接続確立も前記５ＧＣＮが許可しない場合、ストップメッセージを生成することであって、前記ストップメッセージは、メッセージ識別子フィールドを含み、前記メッセージ識別子フィールドは、前記信頼されていない非３ＧＰＰアクセスネットワークを介した前記５ＧＣＮへの前記安全な接続を確立するための前記要求を前記ＵＥが終了するつもりであることを示す５Ｇ－Ｓｔｏｐ識別子を含む、前記生成することと、

前記ストップメッセージの前記メッセージ識別子フィールド内の前記５Ｇストップ識別子を５Ｇ－Ｓｔｏｐに設定することと、

前記信頼されていない非３ＧＰＰネットワークを介した前記５ＧＣＮとの前記安全な接続確立のための前記登録要求を終了するために、前記ストップメッセージを前記５ＧＣＮの前記Ｎ３ＩＷＦに向けて送信することと、

を前記ＵＥに実行させるように構成されている、処理デバイスと

を備える、ＵＥ。

【請求項１１】

前記処理デバイスは、さらに、

前記５ＧＣＮへの安全な接続確立のための前記登録要求の終了を示す前記ストップメッセージを生成することと、

前記信頼されていない非３ＧＰＰネットワークを介して前記５ＧＣＮの前記Ｎ３ＩＷＦに前記ストップメッセージを送信することと、

を前記ＵＥに実行させるように構成されている、請求項１０に記載のＵＥ。

【請求項１２】

前記処理デバイスは、さらに、

５Ｇ－Ｓｔｏｐに設定されたメッセージ識別子フィールドを含む拡張認証プロトコル（ＥＡＰ）－Ｒｅｓｐｏｎｓｅ形式のメッセージとして前記ストップメッセージを生成することを前記ＵＥに実行させるように構成されている、請求項１１に記載のＵＥ。

【請求項１３】

前記処理デバイスは、さらに、

前記Ｎ３ＩＷＦからのＥＡＰ失敗メッセージを処理することと、

セキュリティアソシエーション（ＳＡ）の削除手順を実行することと、

を前記ＵＥに実行させるように構成されている、請求項１２に記載のＵＥ。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本出願は、「Ｍｅｔｈｏｄ ａｎｄ Ａｐｐａｒａｔｕｓ Ｆｏｒ Ｈａｎｄｌｉｎｇ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆａｉｌｕｒｅ Ｄｕｒｉｎｇ Ｓｅｃｕｒｉｔｙ Ａｓｓｏｃｉａｔｉｏｎ Ｅｓｔａｂｌｉｓｈｍｅｎｔ」と題する２０１８年6月３０日に出願された、参照により本明細書に明示的に組み込まれる米国仮出願第６２／６９２，７２２号に対する優先権を米国特許法第１１９条の下で主張する。

【０００２】

本出願は、一般にアクセスネットワークに関し、より詳細には、セキュリティアソシエーションの確立が承認されない場合のアクセスネットワークにおけるユーザ機器によるセッション確立に関する。

【０００３】

関連技術の説明

本節の記載は、関連技術の説明を与えるものであり、先行技術を認めるものではない。スマートフォン、スマートタブレット、ラップトップ、コンピュータ、スマートウォッチなどのユーザ機器（ＵＥ）は、多くの場合、ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）接続性（ＩＥＥＥ　８０２．１１ｘ準拠のＷＬＡＮ接続性など）と無線アクセスネットワーク接続性（ＥＶＤＯ、ＵＭＴＳ、ＨＳＰＡ、及びＬＴＥを含む第３世代パートナシッププロジェクト（３ＧＰＰ）との規格セットに、全面的に、または部分的に準拠しているテクノロジなど）の両方の機能を含む。したがって、ＵＥは、３ＧＰＰアクセスネットワークと非３ＧＰＰアクセスネットワークとで構成される２種類のアクセス技術を使用して、３ＧＰＰ発展型パケットコア（ＥＰＣ）ネットワークに接続することができる。

【０００４】

一般に、３ＧＰＰアクセスネットワークは、例えば、ＧＰＲＳ、ＵＭＴＳ、ＥＤＧＥ、ＨＳＰＡ、ＬＴＥ、及びＬＴＥ　Ａｄｖａｎｃｅｄを含む３ＧＰＰの規格セットによって指定された技術に、全面的に、または部分的に準拠している。非３ＧＰＰアクセスネットワークは、３ＧＰＰの規格セットによって指定されない技術に、全面的に、または部分的に準拠している。それらには、ｃｄｍａ２０００、ＷＬＡＮ（ＩＥＥＥ　８０２．１１ｘ準拠のＷＬＡＮなど）、または固定ネットワークなどの技術が含まれる。

【０００５】

３ＧＰＰの規格セットは、様々なセキュリティ機構を備えた「非３ＧＰＰ」アクセス技術を指定している。信頼されていないアクセスネットワークと信頼されたアクセスネットワークである。信頼されていないアクセスネットワークには、セキュリティリスクを高め得るアクセスネットワーク（例えば、公衆ＷＬＡＮまたはフェムトセルアクセスネットワーク）が含まれる。信頼されたアクセスネットワークには、セキュリティの観点から一定の信頼度を有し、ＥＰＣネットワークと直接インタフェースすることができるとネットワークオペレータが認めるアクセスネットワークが含まれる。

【０００６】

新たな５Ｇ規格のセットでは、非３ＧＰＰアクセスネットワーク（Ｎ３ＡＮ）は、５Ｇアクセスネットワークとして扱われ、かつ５Ｇシステム（５ＧＳ）の一部として扱われる。信頼されていない非３ＧＰＰアクセスの場合、非３ＧＰＰインターワーキング機能（Ｎ３ＩＷＦ）が、ＮＧ－ＲＡＮノードと同様に、制御プレーン及びユーザプレーンに対して、それぞれシグナリングインタフェースの終端を提供する。したがって、５Ｇ対応のＵＥは、Ｎ３ＩＷＦを介して、５Ｇアクセスネットワークとして非３ＧＰＰアクセスネットワークに接続することによって、５Ｇコアネットワーク（５ＧＣＮ）にアクセスすることができる。Ｎ３ＩＷＦは、ＵＥと５ＧＣＮとの間でアップリンク及びダウンリンクの制御プレーンシグナリングを中継する。さらに、Ｎ３ＩＷＦは、非３ＧＰＰアクセスネットワークを介したセッションのために、ＵＥと５ＧＣＮとの間にユーザプレーン接続を提供する。

【０００７】

現在、ＵＥとＮ３ＩＷＦとの間のシグナリング手順は、特定のセキュリティ認証の確立がネットワークによって承認されたときに指定される。ただし、セキュリティアソシエーションの確立がネットワークによって承認されないときに対処するために利用できる方法はない。同様に、ユーザプレーン接続の場合、ユーザプレーンセキュリティアソシエーションの確立がネットワークによって承認されないときに対処するための方法が指定される必要がある。

【０００８】

したがって、非３ＧＰＰアクセスネットワークを介した５ＧＣＮへのアクセスのためのセキュリティアソシエーション確立中の障害対処を支援するシステム及び方法を提供する必要性がある。他の必要性及び利点もまた、本明細書に記載された実施形態でもって提供される。

【発明の概要】

【０００９】

以下では、開示された主題のいくつかの態様への基本的な理解を提供するために、開示された主題の概要が示される。本概要は、開示された主題の網羅的な全体像ではない。開示された主題の主要素もしくは決定的要素を特定すること、または開示された主題の範囲を明確化することを意図したものではない。その唯一の目的は、後述するさらに詳細な説明の前置きとして、いくつかの概念を簡略化した形で提示することである。

【００１０】

一態様では、信頼されていないアクセスネットワークを介したコアネットワークへのネットワーク接続を管理するためのインターワーキング機能ノードが、信頼されていないアクセスネットワークを介してユーザ機器（ＵＥ）と通信するように構成された第１のネットワークインタフェースと、コアネットワーク内の１つ以上のノードと通信するように構成された第２のネットワークインタフェースとを含む。本インターワーキング機能ノードは、信頼されていないアクセスネットワーク内のＵＥからのコアネットワークへの接続確立の要求を処理し、コアネットワークへの要求を生成することと、接続確立がコアネットワークによって承認されないと判定することと、ＵＥへのレスポンスメッセージを生成することとを行うように構成され、レスポンスメッセージが、信頼されていないアクセスネットワークを介した接続確立がコアネットワークによって許可されないことを示すエラーを含む、処理デバイスを備える。

【００１１】

別の態様では、インターワーキング機能ノードからのネットワーク接続要求に対処するためのアクセス及びモビリティ管理機能（ＡＭＦ）が、コアネットワーク内のインターワーキング機能ノード及び認証機能と通信するように構成されたネットワークインタフェースを含む。本ＡＭＦはまた、信頼されていないアクセスネットワークを介したＵＥの認証及び安全な接続確立の要求を処理することと、認証サーバ機能（ＡＵＳＦ）に対する認証及びサブスクリプションチェックの要求を生成することと、認証及びサブスクリプションチェックに対するレスポンスが、認証の失敗を示すことを判定することと、認証及び安全な接続確立のレスポンスメッセージを、信頼されていないアクセスネットワークを介したコアネットワークへのアクセスが許可されないことを示す原因値をレスポンスメッセージに含むことによって生成することとを行うように構成されている処理デバイスを含む。

【００１２】

別の態様では、ユーザ機器（ＵＥ）が、信頼されていないアクセスネットワークを介して、インターワーキング機能ノードと通信するように構成されたネットワークインタフェースを含む。本ＵＥは、コアネットワークへの安全なセッション確立のための登録要求を生成することと、インターワーキング機能ノードからのレスポンスメッセージを処理することと、レスポンスメッセージから、信頼されていないアクセスネットワークを介した接続確立が、コアネットワークによって許可されないことを判定することとを行うように構成されている処理デバイスを含む。

【００１３】

上記の態様の１つ以上において、インターワーキング機能ノード内の処理デバイスは、信頼されていないアクセスネットワークを介したＵＥからの認証及び安全な接続確立の要求を受信することと、認証及びサブスクリプションチェックの要求を生成し、認証及びサブスクリプションチェックの要求を、第２のインタフェースを介して、アクセス及びモビリティ管理機能（ＡＭＦ）に対して送信することと、ＡＭＦからの認証及びサブスクリプションチェックのレスポンスを受信することと、信頼されていないアクセスネットワークを介した接続確立がコアネットワークによって許可されないことを示すエラーを含むＮＡＳペイロードを有するＵＥへのインターネット鍵交換（ＩＫＥ）レスポンスメッセージを生成することとを行うように構成されている。

【００１４】

上記の態様の１つ以上において、インターワーキング機能ノード内の処理デバイスは、５ＧＣＮへの非３ＧＰＰアクセスが許可されていないことを示す５ＧＭＭ原因値を含む登録拒否メッセージをカプセル化するアクセス及びモビリティ管理機能からのレスポンスを

受信することと、接続確立がコアネットワークによって承認されないことを示すメッセージタイプを含むペイロードを有するインターネット鍵交換（ＩＫＥ）レスポンスメッセージを生成することとを行うように構成されている。

【００１５】

上記の態様の１つ以上において、インターワーキング機能ノード内の処理デバイスは、失敗理由を示すプライベート通知メッセージタイプを含む通知ペイロードを有するインターネット鍵交換（ＩＫＥ）レスポンスメッセージを生成するように構成されている。

【００１６】

上記の態様の１つ以上において、インターワーキング機能ノード内の処理デバイスは、５ＧＣＮへの信頼されていない非３ＧＰＰアクセスが許可されないことを示すプライベート通知メッセージタイプを含む通知ペイロードを有するＩＫＥレスポンスメッセージを生成することにより、ＩＫＥレスポンスメッセージを生成するように構成されている。

【００１７】

上記の態様の１つ以上において、インターワーキング機能ノード内の処理デバイスは、ＵＥにレスポンスメッセージを送信することであって、レスポンスメッセージは、接続確立がコアネットワークによって承認されないことを示す、送信することと、ＵＥからストップメッセージを受信することと、ＵＥへの失敗メッセージを生成することとを行うように構成されている。

【００１８】

上記の態様の１つ以上において、インターワーキング機能ノード内の処理デバイスは、ＵＥからのストップメッセージを処理するように構成されており、ストップメッセージは、メッセージ識別子フィールドを有する５Ｇ－Ｓｔｏｐメッセージ形式を含み、メッセージ識別子フィールドは、５Ｇ－Ｓｔｏｐ識別子を含む。

【００１９】

上記の態様の１つ以上において、信頼されていないアクセスネットワーク内のＵＥからの接続確立の要求が、コアネットワークとのＩＰｓｅｃセキュリティアソシエーション（ＳＡ）を開始するためのＩＫＥ要求メッセージを含む。

【００２０】

上記の態様の１つ以上において、コアネットワークが５ＧＣＮであり、信頼されていないアクセスネットワークが非３ＧＰＰアクセスネットワークである。

【００２１】

上記の態様の１つ以上において、ＡＭＦの処理デバイスは、原因値を含む登録拒否メッセージをレスポンスメッセージにカプセル化するように構成されており、原因値は、５ＧＣＮへの非３ＧＰＰアクセスが許可されないことを示す５ＧＭＭ原因値を含む。

【００２２】

上記の態様の１つ以上において、ＡＭＦの処理デバイスは、レスポンスメッセージに、拡張認証プロトコル（ＥＡＰ）の失敗インディケーションを生成するように構成されている。

【００２３】

上記の態様の１つ以上において、ユーザ機器の処理デバイスは、５ＧＣＮへの安全なセッション確立のための登録要求の終了を示すストップメッセージを生成することと、非３ＧＰＰアクセスネットワークを介してインターワーキング機能ノードにストップメッセージを送信することとを行うように構成されている。

【００２４】

上記の態様の１つ以上において、ユーザ機器の処理デバイスは、５Ｇ－Ｓｔｏｐに設定されたメッセージ識別子フィールドを含むＥＡＰ－Ｒｅｓｐｏｎｓｅ形式のメッセージとしてストップメッセージを生成するように構成されている。

【００２５】

上記の態様の１つ以上において、ユーザ機器の処理デバイスは、インターワーキング機能ノードからのＥＡＰ失敗メッセージを処理することと、セキュリティアソシエーション

の削除手順を実行することとを行うように構成されている。
【００２６】
上記の態様の１つ以上において、ユーザ機器の処理デバイスは、５ＧＣＮへの安全なセッション確立のための第２の登録要求を生成することにより、５ＧＣＮへの登録を再試行することと、インターワーキング機能ノードからの第２のレスポンスメッセージから、信頼されていないアクセスネットワークを介した接続確立が成功したことを判定することとを行うように構成されている。
【００２７】
上記の態様の１つ以上において、ユーザ機器の処理デバイスは、更新されたパラメータで、５ＧＣＮへの安全なセッション確立のための第２の登録要求を生成するように構成されている。
【００２８】
以下の詳細な説明、図、及びいずれかの特許請求の範囲では、部分的に、更なる態様が述べられており、一部はその詳細な説明から得られる。上記の概説と以下の詳細な説明とはいずれも、例示及び説明のためのものにすぎず、特許請求の範囲は、開示された実施形態に限定されないことを理解されたい。
【００２９】
次に、本開示の実施形態による装置及び／または方法のいくつかの実施形態を、ほんの一例として、添付の図面を参照して説明する。
【図面の簡単な説明】
【００３０】
【図１】アクセスネットワークの種類の実施形態の概略ブロック図を示す。
【図２】非３ＧＰＰアクセスのための５Ｇシステムアーキテクチャの実施形態の概略ブロック図を示す。
【図３】信頼されていない非３ＧＰＰアクセスネットワークを介してＵＥを５ＧＣＮに登録するための方法の実施形態を示す論理フロー図を示す。
【図４】ＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が承認されない実施形態に対処するための方法の実施形態の論理フロー図を示す。
【図５】修復可能なエラーによる認証失敗後のＥＡＰ－５Ｇセッション手順の方法の実施形態の論理フロー図を示す。
【図６】修復不能なエラー障害による登録拒否のＥＡＰ－５Ｇセッション手順の実施形態を示す論理フロー図を示す。
【図７】ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージの実施形態の概略ブロック図を示す。
【図８】非３ＧＰＰアクセスを介したＵＥ登録のためのＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が承認されないときのネットワーク機能間のメッセージフローのための方法の実施形態の論理フロー図を示す。
【図９】非３ＧＰＰアクセスを介したＵＥ登録のためのＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が、サブスクリプション制限のために承認されないときのネットワーク機能間のメッセージフローのための方法の実施形態の論理フロー図を示す。
【図１０】ユーザプレーンＩＰｓｅｃセキュリティアソシエーションの確立が承認されないときのネットワーク機能間のメッセージフローのための方法の実施形態の論理フロー図を示す。
【図１１】５ＧＭＭ原因情報要素１１００の実施形態の概略ブロック図を示す。
【図１２】５ＧＭＭ原因情報要素の値の実施形態の概略ブロック図を示す。
【図１３】Ｎ３ＩＷＦの方法の実施形態の論理フロー図を示す。
【図１４】修復可能なエラーによる認証失敗を伴う、信頼されていないアクセスネットワークを介したコアネットワークへの登録要求の方法の実施形態の論理フロー図を示す。
【図１５】修復不能なエラーによる認証失敗を伴う、信頼されていないアクセスネットワークを介したコアネットワークへの登録要求の方法の実施形態の論理フロー図を示す。

【図１６】例示的なユーザ機器の実施形態の概略ブロック図を示す。
【図１７】ＡＭＦノードの実施形態の概略ブロック図を示す。
【図１８】Ｎ３ＩＷＦの実施形態の概略ブロック図を示す。
【発明を実施するための形態】
【００３１】
説明及び図面は、単に様々な実施形態の原理を例示しているにすぎない。したがって、当業者であれば、本明細書に明示的に記載されず、または示されないが、本明細書及び特許請求の範囲に記載されている原理を具体化し、本開示の趣旨及び範囲の内に含まれる様々な構成を考案できるであろうことが理解されよう。さらに、本明細書で説明された全ての実施例は、主として、読者が、本実施形態の原理と、本発明者が本技術をさらに発展させるのに貢献した概念とを理解するのを補助するための教育的目的のものであるにすぎないことが明示的に意図されており、そのような具体的に説明された実施例及び条件に限定されるものではないと解釈されるべきである。さらに、本明細書では、原理、態様、及び実施形態、ならびにそれらの具体例を説明する全ての記載は、それらの均等物を包含することが意図されている。
【００３２】
本明細書に記載された略語のいくつかが、便宜のため、以下に展開されている。
５ＧＣ　５Ｇコア
５ＧＣＮ　５Ｇコアネットワーク
５ＧＳ　５Ｇシステム
５Ｇ－ＡＮ　５Ｇアクセスネットワーク
５ＧＭＭ　５ＧＳモビリティ管理
５Ｇ－ＧＵＴＩ　５Ｇグローバル固有テンポラリ識別子
５Ｇ－Ｓ－ＴＭＳＩ　５Ｇ　Ｓ－テンポラリモバイルサブスクリプション識別子
５ＱＩ　５Ｇ　ＱｏＳ識別子
ＡＭＦ　アクセス及びモビリティ管理機能
ＡＵＳＦ　認証サーバ機能
ＥＡＰ　拡張認証プロトコル
ＨＰＬＭＮ　家庭用公衆陸上モバイルネットワーク
ＩＫＥｖ２　インターネット鍵交換ｖ２
ＩＭＳＩ　国際モバイル加入者識別番号
ＩＭＥＩ　国際モバイル機器識別番号
ＩＰｓｅｃ　インターネットプロトコルセキュリティ
ＭＣＭ　マルチ接続モード
Ｎ３ＩＷＦ　非３ＧＰＰインターワーキング機能
ＮＡＳ　非アクセス層
ＰＤＮ　パケットデータネットワーク
ＰＬＭＮ　公衆陸上モバイルネットワーク
ＱｏＳ　サービス品質
ＳＡ　セキュリティアソシエーション
ＳＣＭ　シングル接続モード
ＵＤＭ　統合データ管理
ＵＥ　ユーザ機器
ＵＩＣＣ　ユニバーサル集積回路カード
ＵＳＩＭ　ＵＭＴＳ加入者識別モジュール
【００３３】
本明細書には、認証されていないユーザ機器にネットワークサービスを提供するためのシステム及び方法を提供する１つ以上の実施形態が説明されている。例えば、非３ＧＰＰアクセスネットワークにおいて、認証されていないＵＥのセッションを確立するための様々な方法が説明されている。

【００３４】
図１は、技術仕様（ＴＳ）２３．５０１「Ｓｙｓｔｅｍ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ ｔｈｅ ５Ｇ Ｓｙｓｔｅｍ」、５Ｇシステムの手順を定める技術仕様（ＴＳ）２３．５０２、ならびに５Ｇシステムのポリシー及び課金制御フレームワークを定める技術仕様（ＴＳ）２３．５０３など、５Ｇシステム向けの第３世代パートナーシッププロジェクト（３ＧＰＰ）の規格セットに、全面的にまたは部分的に準拠した５Ｇコアネットワーク（５ＧＣＮ）１００のためのアクセスネットワークの種類の実施形態の概略ブロック図を示す。
【００３５】
５ＧＣＮ１００は、１つ以上のアクセスネットワーク１０２に通信可能に結合されている。実施形態では、アクセスネットワーク１０２には、１つ以上の３ＧＰＰアクセスネットワーク１０４、または１つ以上の非３ＧＰＰアクセスネットワーク１０６が含まれ得る。３ＧＰＰアクセスネットワーク１０４は、３ＧＰＰの規格セットによって指定された技術に、全面的に、または部分的に準拠しており、例えば、ＧＰＲＳ、ＵＭＴＳ、ＥＤＧＥ、ＨＳＰＡ、ＬＴＥ、及びＬＴＥ Ａｄｖａｎｃｅｄを含む。非３ＧＰＰアクセスネットワーク１０６は、３ＧＰＰの規格セットによって指定されない技術に、全面的に、または部分的に準拠している。非３ＧＰＰアクセスネットワーク１０６は、３ＧＰＰの規格セットでそのように指定され得る。非３ＧＰＰアクセスネットワーク１０６には、１つ以上の信頼された非３ＧＰＰアクセスネットワーク１０８、または１つ以上の信頼されていない非３ＧＰＰアクセスネットワーク１１０が含まれ得る。
【００３６】
信頼された非３ＧＰＰアクセスネットワーク１０８は、ＩＥＥＥ８０２．１１ｘ準拠のＷＬＡＮネットワークなど、暗号化及びセキュアな認証方法を用いた、オペレータによって構築される、またはオペレータによってサポートされる、ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）である。一実施形態では、信頼された非３ＧＰＰアクセスネットワーク１０８は、以下の例示的な特徴をサポートする。無線アクセスネットワーク（ＲＡＮ）の暗号化をも要求する８０２．１ｘベースの認証、認証にＥＡＰ方式を使用する３ＧＰＰベースのネットワークアクセス、及びＩＰｖ４及び／またはＩＰｖ６プロトコルである。また一方、セキュリティタイプの異なる他種の非３ＧＰＰアクセスネットワークが信頼されたと認められるとオペレータが判断する場合もある。信頼されていない非３ＧＰＰアクセスネットワーク１１０には、オペレータに知られていない非３ＧＰＰアクセスネットワーク、またはサポートされた認証規格を含まない非３ＧＰＰアクセスネットワークが含まれる。例えば、信頼されていない非３ＧＰＰアクセスネットワークには、一般に公開されるＩＥＥＥ８０２．１１ｘ準拠のＷＬＡＮネットワーク、家庭用ＷＬＡＮ、または他の非オペレータによって創設され管理されるものなど、家庭用または公衆用のＷＬＡＮが含まれ得る。
【００３７】
図２は、非３ＧＰＰアクセスのための５Ｇシステムアーキテクチャの実施形態の概略ブロック図を示す。このアーキテクチャは、参照により本明細書に組み込まれる「Ｓｙｓｔｅｍ Ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ ｔｈｅ ５Ｇ Ｓｙｓｔｅｍ」と題する技術規格３ＧＰＰ ＴＳ ２３．５０１，Ｒｅｌｅａｓｅ １５ （２０１７年１２月）にさらに詳細に説明されている。
【００３８】
非３ＧＰＰアクセスネットワークは、非３ＧＰＰインターワーキング機能（Ｎ３ＩＷＦ）を介して５ＧＣＮ１００に接続されている。Ｎ３ＩＷＦ２０４は、５ＧＣＮ１００の制御プレーン（ＣＰ）機能及びユーザプレーン（ＵＰ）機能を、それぞれＮ２インタフェース及びＮ３インタフェースを介してインタフェース接続する。ＵＥ２００は、Ｎ３ＩＷＦ２０４とのＩＰセキュリティ（ＩＰＳｅｃ）トンネルを確立して、信頼されていない非３ＧＰＰアクセスネットワーク１１０を介して５ＧＣＮ１００にアタッチする。ＵＥ２００は、ＩＰＳｅｃトンネルの確立手順を通じて、５ＧＣＮ１００によって認証されて、５Ｇ

ＣＮ１００にアタッチされる。信頼されていない非３ＧＰＰアクセス１１０を介した５ＧＣＮ１００へのＵＥ２００のアタッチに関する更なる詳細が、参照により本明細書に組み込まれる「Ｐｒｏｃｅｄｕｒｅｓ ｆｏｒ ｔｈｅ ５Ｇ Ｓｙｓｔｅｍ」と題する３ＧＰＰ ＴＳ ２３．５０２，Ｒｅｌｅａｓｅ １５（２０１７年１２月）に説明されている。

【００３９】

５ＧＣＮ１００は、アクセス及びモビリティ管理機能（ＡＭＦ）２０２を含む家庭用公衆陸上モバイルネットワークまたは同等の家庭用ＰＬＭＮ（ＨＰＬＭＮ）を含む。ＡＭＦ２０２は、制御プレーンインタフェース（Ｎ２）の終端及びＮＡＳ（Ｎ１）プロトコルセットの終端と、ＮＡＳの暗号化及び整合性の保護とを提供する。ＡＭＦ２０２はまた、登録及び接続の管理を提供する。ＡＭＦ２０２は、非３ＧＰＰアクセスネットワーク１１０をサポートするために様々な機能性を含み得る。例えば、ＡＭＦ２０２は、Ｎ３ＩＷＦ２０４を用いたＮ２インタフェース制御プロトコルのサポートと、Ｎ３ＩＷＦ２０４を介したＵＥ２００とのＮＡＳシグナリングのサポートとを提供し得る。さらに、ＡＭＦ２０２は、Ｎ３ＩＷＦ２０４を介して接続されたＵＥ２００の認証のサポートと、非３ＧＰＰアクセスを介して接続された、または３ＧＰＰアクセス及び非３ＧＰＰアクセスを介して同時に接続されたＵＥ２００のモビリティ、認証、及び別個のセキュリティコンテキスト状態（複数可）の管理を提供し得る。非アクセス層（ＮＡＳ）は、５Ｇ規格のプロトコルセットである。５Ｇ ＮＡＳ（非アクセス層）は、５ＧＳ（５Ｇシステム）での５ＧＭＭ（５ＧＳモビリティ管理）及び５ＧＳＭ（５Ｇセッション管理）に関連した手順を含む。ＮＡＳは、ユーザ機器（ＵＥ）と５ＧＣＮ機能との間で制御シグナリングを伝達するのに用いられる。５ＧＮＡＳプロトコルのバージョンが、参照により本明細書に組み込まれる３ＧＰＰ ＴＳ ２４．５０１：「Ａｃｃｅｓｓ－Ｓｔｒａｔｕｍ（ＮＡＳ） ｐｒｏｔｏｃｏｌ ｆｏｒ ５Ｇ Ｓｙｓｔｅｍ（５ＧＳ）」 Ｖｅｒｓｉｏｎ １．１（２０１８年５月９日）で定義されている。

【００４０】

セッション管理機能（ＳＭＦ）２０６は、セッション管理機能性、例えば、ＵＰＦ２０８とＡＮノードとの間のトンネル維持を含む、セッションの確立、変更、及び解除を含む。ＳＭＦ２０６はまた、ＵＥのＩＰアドレスの割り当て及び管理（任意選択の認可を含む）と、ＤＨＣＰｖ４（サーバ及びクライアント）及びＤＨＣＰｖ６（サーバ及びクライアント）の機能とを提供する。

【００４１】

ユーザプレーン機能（ＵＰＦ）２０８は、データネットワークとパケットルーティング及びパケットフォワーディングとに外部ＰＤＵセッションの相互接続ポイントを提供する。ＵＰＦ２０８はまた、ポリシールール施行のユーザプレーン部分、例えば、ゲーティング、リダイレクト、トラフィックステアリングなどをサポートする。

【００４２】

ポリシー制御機能（ＰＣＦ）２１４は、ネットワークの挙動を統御するための統合されたポリシーフレームワークをサポートする。統合データ管理（ＵＤＭ）２１２は、３ＧＰＰ ＡＫＡ認証証明書の生成、サブスクリプションデータに基づくアクセス認可（例えば、ローミング制限）、及びＵＥのサービングＮＦ登録管理（例えば、ＵＥのためのサービングＡＭＦを保存する、ＵＥのＰＤＵセッションのためのサービングＳＭＦを保存する）のサポートを含む。ＵＤＭ２１２はまた、ＳＭＳ及びサブスクリプションの管理を提供する。この機能性を提供するために、ＵＤＭ２１２は、ＵＤＲに格納され得るサブスクリプションデータ（認証データを含む）を使用する。別のモジュールが、認証サーバ機能（ＡＵＳＦ）２１０を提供する。

【００４３】

信頼されていない非３ＧＰＰアクセス１１０の場合のＮ３ＩＷＦ２０４の機能性は、ＵＥ２００とのＩＰｓｅｃトンネル確立のサポートを含む。Ｎ３ＩＷＦ２０４は、ＮＷｕインタフェースを介したＵＥ２００とのＩＫＥｖ２／ＩＰｓｅｃプロトコルを終端し、Ｎ３ＩＷＦ２０４は、ＵＥ２００を認証して、その５ＧＣＮ１００へのアクセスを認可するた

めに必要な情報を、Ｎ２インタフェースを介して中継する。Ｎ３ＩＷＦ２０４は、Ｎ２及びＮ３インタフェースの終端を、それぞれ制御プレーン及びユーザプレーンを関して、５ＧＣＮ１００に提供する。Ｎ３ＩＷＦ２０４は、ＵＥ２００とＡＭＦ２０２との間で、アップリンク及びダウンリンクの制御プレーンＮＡＳ（Ｎ１）シグナリングを中継する。Ｎ３ＩＷＦ２０４は、ＰＤＵセッション及びＱｏＳに関連するＳＭＦ２０６からの（ＡＭＦ２０２によって中継される）Ｎ２シグナリングの対処を提供する。Ｎ３ＩＷＦ２０４は、ＰＤＵセッショントラフィックをサポートするためのＩＰｓｅｃセキュリティアソシエーション（ＩＰｓｅｃ　ＳＡ）の確立をさらに提供する。Ｎ３ＩＷＦ２０４はまた、ＵＥ２００とＵＰＦ２０８との間で、アップリンク及びダウンリンクのユーザプレーンパケットを中継することを提供する。

【００４４】

図３は、信頼されていない非３ＧＰＰアクセス１１０を介してＵＥ２００を５ＧＣＮ１００に登録するための方法の実施形態を示す論理フロー図を示す。本方法は、「ＥＡＰ－５Ｇ」と呼ばれるベンダー固有の拡張認証プロトコル（ＥＡＰ）を含む。ＥＡＰは、２００４年６月付けのＩＥＴＦ　ＲＦＣ　３７４８：「Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（ＥＡＰ）」で定義されている。ＥＡＰ－５Ｇは、ＵＥ２００とＮ３ＩＷＦ２０４との間でＮＡＳメッセージをカプセル化するのに用いられるベンダー固有の５ＧＳ用ＥＡＰ（ＥＡＰ－５Ｇ）である。ＥＡＰ－５Ｇパケットは、「拡張」ＥＡＰタイプと、ＳＭＩプライベートエンタープライズコードレジストリ（すなわち１０４１５）の下でＩＡＮＡに登録された既存の３ＧＰＰベンダーＩＤとを利用する。実施形態では、ＥＡＰ－５Ｇは、ＮＡＳメッセージをカプセル化するためにのみ利用される（認証のためではない）。

【００４５】

ＵＥ２００を認証する必要がある場合、以下に本明細書で説明するように、ＵＥ２００とＡＵＳＦ２１０との間でＥＡＰ－ＡＫＡ’相互認証が実行される。信頼されていない非３ＧＰＰアクセスネットワーク１１０を介した登録と、その後の登録手順とでは、ＮＡＳメッセージがＵＥ２００とＡＭＦ２０２との間で交換される。

【００４６】

ステップ１において、ＵＥ２００は、３ＧＰＰの範囲外の手順（ＩＥＥＥ　８０２．１１ＷＬＡＮプロトコルで指定される手順など）で、信頼されていない非３ＧＰＰアクセスネットワーク１１０に接続し、ＩＰアドレスが割り当てられる。任意の非３ＧＰＰ認証方法、例えば、認証なし（無料ＷＬＡＮの場合）や、事前共有鍵、ユーザ名／パスワードなどを用いる拡張認証プロトコル（ＥＡＰ）が使用され得る。ＵＥ２００が５ＧＣＮ１００にアタッチすることを決定すると、ＵＥ２００は、５Ｇ　ＰＬＭＮ内のＮ３ＩＷＦ２０４を選択する。

【００４７】

ステップ２において、ＵＥ２００は、例えば、ＩＥＴＦ　ＲＦＣ　７２９６，「Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ　Ｐｒｏｔｏｃｏｌ　Ｖｅｒｓｉｏｎ　２（ＩＫＥｖ２）」（２０１４年１０月）に記載されているように、インターネット鍵交換（ＩＫＥ）プロトコルの初期交換を開始することで、選択したＮ３ＩＷＦ２０４とのＩＰｓｅｃセキュリティアソシエーション（ＳＡ）の確立を進める。ステップ２の後、以降のＩＫＥメッセージは、このステップで確立されたＩＫＥ　ＳＡを使用することによって、暗号化され、整合性が保護される。

【００４８】

ステップ３において、ＵＥ２００は、ＩＫＥ＿ＡＵＴＨ要求メッセージを送信することにより、ＩＫＥ＿ＡＵＴＨ交換を開始するものとする。ＡＵＴＨペイロードはＩＫＥ＿ＡＵＴＨ要求メッセージに含まれず、このことは、ＩＫＥ＿ＡＵＴＨ交換が、拡張認証プロトコル（ＥＡＰ）シグナリングプロトコル、例えば、ＥＡＰ－５Ｇシグナリング（ＩＥＴＦ　ＲＦＣ　５４４８，「Ｉｍｐｒｏｖｅｄ　Ｅｘｔｅｎｓｉｂｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ　Ｍｅｔｈｏｄ　ｆｏｒ　３ｒｄ　Ｇｅｎｅｒａｔｉｏｎ

Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ （ＥＡＰ－ＡＫＡ’）」（２０１８年３月５日）に記載され、参照により本明細書に組み込まれるＥＡＰ－ＡＫＡ’など）を使用することを示す。

【００４９】

ステップ４において、Ｎ３ＩＷＦ２０４は、ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔパケットを含むＩＫＥ＿ＡＵＴＨレスポンスメッセージで応答する。ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔパケットは、ＵＥ２００に、ＥＡＰ－５Ｇセッションを開始するよう通知する、つまり、ＥＡＰ－５Ｇパケットの中にカプセル化されたＮＡＳメッセージの送信を開始するよう通知する。

【００５０】

ステップ５において、ＵＥ２００は、５ＧＣＮ１００に対する登録要求、例えば、アクセスネットワークパラメータ（ＡＮ－Ｐａｒａｍｓ）を含むＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳパケットとＮＡＳ登録要求メッセージとを含むＩＫＥ＿ＡＵＴＨ要求を生成して送信する。したがって、ＵＥは、例えば、ａ）ＮＡＳメッセージ、例えば、登録要求メッセージを包含するＮＡＳ－ＰＤＵフィールドと、ｂ）ＳＵＰＩまたは５Ｇ－ＧＵＴＩ、選択されたネットワーク及びＳ－ＮＳＳＡＩなどのアクセスネットワークパラメータを包含するＡＮパラメータフィールド（３ＧＰＰ ＴＳ ２３．５０２を参照）とを含むＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳパケットを送信することにより、ＥＡＰ－５Ｇセッションの開始を確認する。ＡＮパラメータ（ＡＮ－Ｐａｒａｍｓ）は、５ＧＣＮ１００でのＡＭＦ２０２を選択するためにＮ３ＩＷＦ２０４によって使用される。

【００５１】

ステップ６ａにおいて、Ｎ３ＩＷＦ２０４は、受信したＡＮパラメータ及びローカルポリシーに基づいて、５ＧＣＮ１００内のＡＭＦ２０２を選択する。次に、Ｎ３ＩＷＦ２０４は、ステップ６ｂにおいて、ＵＥ２００から受信した登録要求を、選択したＡＭＦ２０２に転送する。Ｎ３ＩＷＦ２０４は、ＡＭＦ２０２からのＮＡＳメッセージの受信時に、ＵＥ２００へのＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－ＮＡＳメッセージ内にＮＡＳメッセージを含む。ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－ＮＡＳメッセージは、ＮＡＳメッセージを包含するＮＡＳ－ＰＤＵフィールドを含む。Ｎ３ＩＷＦ２０４を介したＵＥ２００とＡＭＦ２０２との間の更なるＮＡＳメッセージは、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージ（ＵＥからＮ３ＩＷＦへの向き）及びＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－ＮＡＳメッセージ（Ｎ３ＩＷＦからＵＥへの向き）のＮＡＳ－ＰＤＵフィールドに挿入される。

【００５２】

ステップ７ａ及び７ｂにおいて、選択したＡＭＦ２０２は、Ｎ３ＩＷＦ２０４を介してＵＥ２００にＮＡＳ ＩＤ要求メッセージを送信することにより、ＵＥの永続的ＩＤ（ＳＵＰＩ）を要求することを決定することができる。このＮＡＳメッセージと、それに続く全てのＮＡＳメッセージとは、ＥＡＰ／５Ｇ－ＮＡＳパケット内にカプセル化されて、Ｎ３ＩＷＦ２０４によってＵＥ２００に送信される。

【００５３】

ステップ８において、ＡＭＦ２０２は、ＵＥ２００を認証することを決定することができる。この場合、ＡＭＦ２０２は、ＵＥ２００のＳＵＰＩまたは暗号化されたＳＵＰＩを使用することによりＡＵＳＦ２１０を選択するものとし、ステップ８ａでは、選択したＡＵＳＦ２１０に鍵要求を送信するものとする。ＡＵＳＦ２１０は、参照により本明細書に組み込まれるＴＳ ３ＧＰＰ ＴＳ ３３．５０１：「ＳｅｃｕｒｉｔｙＡｒｃｈｉｔｅｃｔｕｒｅ ａｎｄ Ｐｒｏｃｅｄｕｒｅｓ ｆｏｒ ５Ｇ Ｓｙｓｔｅｍ」（Ｒｅｌｅａｓｅ １５（２０１８年３月２６日））に指定されるように、ステップ８ｂにおいてＥＡＰ－ＡＫＡ’認証を開始し得る。ＥＡＰ－ＡＫＡ’チャレンジパケットは、ステップ８ｃでＮ３ＩＷＦへのＮＡＳ認証メッセージ内にカプセル化され、このＮＡＳ認証メッセージは、ステップ８ｄでＥＡＰ／５Ｇ－ＮＡＳパケット内にカプセル化される。ＵＥ２００は、ステップ８ｅでＥＡＰ－ＡＫＡチャレンジに対する認証レスポンスを生成し、この認証レスポンスは、ステップ８ｆでＮ３ＩＷＦ２０４によってＡＭＦに転送される。次に、ＡＵＳＦ

２１０は、ステップ８ｇでＡＭＦから認証レスポンスを受信する。

【００５４】

ＵＥ２００の認証が成功した後、ステップ８ｈにおいて、ＡＵＳＦ２１０は、ＮＡＳのセキュリティ鍵とＮ３ＩＷＦ２０４用のセキュリティ鍵（Ｎ３ＩＷＦ鍵）とを導出するためにＡＭＦ２０２によって使用されるアンカー鍵（ＳＥＡＦ鍵）をＡＭＦ２０２に送信する。ＵＥ２００はまた、アンカー鍵（ＳＥＡＦ鍵）を導出し、その鍵からＮＡＳのセキュリティ鍵とＮ３ＩＷＦ２０４用のセキュリティ鍵（Ｎ３ＩＷＦ鍵）とを導出する。Ｎ３ＩＷＦ鍵は、（ステップ１１において）ＩＰｓｅｃセキュリティアソシエーションを確立するために、ＵＥ２００及びＮ３ＩＷＦ２０４によって使用される。ＡＵＳＦ２１０は、ステップ８ａにおいて、ＡＭＦ２０２が、暗号化されたＳＵＰＩをＡＵＳＦ２１０に提供した場合には、ＳＵＰＩ（暗号化されていない）を含む。

【００５５】

ステップ９ａ及び９ｂで、ＡＭＦ２０２は、セキュリティモードコマンド（ＳＭＣ）要求をＵＥ２００に送信して、ＮＡＳセキュリティをアクティブ化する。（Ｎ２メッセージ内の）この要求は、最初にＮ３ＩＷＦ鍵とともにＮ３ＩＷＦ２０４に送信される。ステップ８においてＥＡＰ－ＡＫＡ’認証が正常に実行された場合、ステップ９ａにおいてＡＭＦ２０２は、ＡＵＳＦ２１０から受信したＥＡＰ－ＳｕｃｃｅｓｓをＳＭＣ要求メッセージ内にカプセル化する。

【００５６】

ステップ１０ａにおいて、ＵＥ２００は、（ステップ８で開始された場合）ＥＡＰ－ＡＫＡ’認証を完了し、ＮＡＳセキュリティコンテキスト及びＮ３ＩＷＦ鍵を作成する。Ｎ３ＩＷＦ鍵がＵＥ２００で作成された後、ＵＥ２００は、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｃｏｍｐｌｅｔｅパケットを送信することによって、ＥＡＰ－５Ｇセッションの完了を要求する。それによって、Ｎ３ＩＷＦ２０４がＡＭＦ２０２からＮ３ＩＷＦ鍵も受信していると仮定して、ステップ１０ｂにおいて、Ｎ３ＩＷＦ２０４がＵＥ２００にＥＡＰ－Ｓｕｃｃｅｓｓを送信することをトリガする。これでＥＡＰ－５Ｇセッションは完了し、それ以上ＥＡＰ－５Ｇパケットを交換することはできない。Ｎ３ＩＷＦ２０４がＡＭＦ２０２からＮ３ＩＷＦ鍵を受信していない場合は、Ｎ３ＩＷＦ２０４はＥＡＰ－Ｆａｉｌｕｒｅで応答する。

【００５７】

ステップ１１では、ＵＥ２００で作成されて、ステップ９ａにおいてＮ３ＩＷＦ２０４によって受信された共通のＮ３ＩＷＦ鍵を用いることにより、ＵＥ２００とＮ３ＩＷＦ２０４との間にＩＰｓｅｃ　ＳＡが確立される。このＩＰｓｅｃ　ＳＡは、「シグナリングＩＰｓｅｃ　ＳＡ」と呼ばれる。シグナリングＩＰｓｅｃ　ＳＡの確立後、ＵＥ２００とＮ３ＩＷＦ２０４との間の全てのＮＡＳメッセージは、このＩＰｓｅｃ　ＳＡを介して交換される。シグナリングＩＰｓｅｃ　ＳＡは、トランスポートモードで動作するように構成されるものとする。ＳＰＩ値は、ＩＰｓｅｃパケットがＮＡＳメッセージを搬送するかどうかを判定するのに用いられる。

【００５８】

ステップ１２で、ＵＥ２００は、確立されたシグナリングＩＰｓｅｃ　ＳＡを介してＳＭＣ完了メッセージを送信し、その後の全てのＮＡＳメッセージは、このＩＰｓｅｃ　ＳＡを介して、ＵＥ２００とＡＭＦ２０２との間で交換される。

【００５９】

上記のように、ＵＥ２００及びＮ３ＩＷＦ２０４は、非３ＧＰＰアクセスネットワーク１１０を介したＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が５ＧＣＮ１００によって承認されたときの方法を定めている。しかし、ＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が５ＧＣＮ１００によって承認されないときに対処するのに利用できるシステムまたは方法はない。さらに、ユーザプレーンについては、ユーザプレーンのＩＰｓｅｃ　ＳＡの確立が５ＧＣＮ１００によって承認されないときに対処するためのシステム及び方法を指定する必要がある。一般に、５ＧＣＮ１００への非３ＧＰＰアクセスの

拒否に対処するための方法及びシステムを確立する必要がある。
【００６０】
実施形態 － 非３ＧＰＰアクセスネットワークを介したＵＥ登録が５Ｇコアネットワークによって承認されないときに対処するためのプロセス及びプロトコルの高度化
図４は、ＩＫＥ ＳＡ及びシグナリングＩＰｓｅｃ ＳＡの確立が承認されないときに対処するための方法４００の実施形態の論理フロー図を示す。ステップ４０２において、ＵＥ２００は、選択したＮ３ＩＷＦ２０４とのＩＰｓｅｃセキュリティアソシエーション（ＳＡ）の確立の要求を進める。ＵＥ２００は、ＩＥＴＦ ＲＦＣ ７２９６「Ｉｎｔｅｒｎｅｔ Ｋｅｙ Ｅｘｃｈａｎｇｅ Ｐｒｏｔｏｃｏｌ Ｖｅｒｓｉｏｎ ２（ＩＫＥｖ２）」，（２０１４年１０月）に記載されているインターネット鍵交換（ＩＫＥ）プロトコルを使用してＩＰｓｅｃ ＳＡの確立を開始する。ＵＥ２００は、ステップ４０４において、ＩＫＥ＿ＡＵＴＨ要求メッセージを送信する。ステップ４０６において、Ｎ３ＩＷＦ２０４は、ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔパケットを含むＩＫＥ＿ＡＵＴＨレスポンスメッセージで応答する。ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔパケットは、ＵＥ２００に、ＥＡＰ－５Ｇセッションを開始するよう通知する、つまり、ＥＡＰ－５ＧパケットのカプセルされたＮＡＳメッセージの送信を開始するよう通知する。
【００６１】
ステップ４０８において、ＵＥ２００は、５ＧＣＮ１００に対する登録要求、例えば、アクセスネットワークパラメータ（ＡＮ－Ｐａｒａｍｓ）を含むＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳパケットとＮＡＳ登録要求メッセージとを含むＩＫＥ＿ＡＵＴＨ要求を生成する。ＡＮ－Ｐａｒａｍｓは、５ＧＣＮ１００でＡＭＦ２０２を選択するためのＮ３ＩＷＦ２０４によって使用される情報（例えば、ＳＵＰＩまたは５Ｇ－ＧＵＴＩ、選択したネットワーク及びＮＳＳＡＩなど）を含む。
【００６２】
場合によっては、例えばＥＡＰ－ＡＫＡ’認証が成功しなかったなどの認証の失敗が原因で、非３ＧＰＰアクセスを介したＵＥ登録が拒否される。その場合、ＩＫＥ ＳＡ及びシグナリングＩＰｓｅｃ ＳＡの確立は、５ＧＣＮ１００によって承認されない。実施形態では、ＡＭＦ２０２は、登録拒否（ＲＥＧＩＳＴＲＡＴＩＯＮ ＲＥＪＥＣＴ）メッセージを生成し、Ｎ３ＩＷＦ２０４は、ステップ４１０において、その登録拒否メッセージを包含するＮＡＳ－ＰＤＵフィールドを含むＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージをＵＥに送信する。
【００６３】
登録拒否メッセージを受信すると、ＵＥ２００は、ステップ４１２において、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージ（ＩＫＥ＿Ａｕｔｈ要求にカプセル化される）を生成して送信することにより、登録要求を終了する。ＵＥ２００は、ステップ４１４において、Ｎ３ＩＷＦ２０４からＥＡＰ失敗メッセージ付きのＩＫＥ＿ＡＵＴＨレスポンスを受信する。Ｎ３ＩＷＦ２０４からＥＡＰ－Ｆａｉｌｕｒｅメッセージを受信すると、ＵＥ２００は、ＩＫＥｖ２ ＳＡ削除手順を実行する。ＵＥ２００は、スイッチを切るか、またはＵＳＩＭを含むＵＩＣＣが除去されるまで、同じＰＬＭＮからＮ３ＩＷＦ２０４へのＩＫＥ ＳＡ及びシグナリングＩＰｓｅｃ ＳＡの確立を再開始しない。
【００６４】
非３ＧＰＰアクセスネットワーク１１０を介したＵＥ２００の登録が拒否されると、ＡＭＦ２０２は、登録拒否メッセージをＮ３ＩＷＦ２０４に送信する。それに応答して、Ｎ３ＩＷＦ２０４は、登録拒否メッセージを含むＮＡＳ－ＰＤＵフィールドを含むＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージをＵＥ２００に送信する。その後のＵＥ２００のレスポンスは、登録拒否の理由に応じて異なり得る。構文エラーまたは特定の一時的な拒否理由など、修復可能なエラーの場合、ＵＥ２００は、有効なパラメータを用いて登録を再び開始しようと試みることができる。他の拒否の理由では、ＵＥ２００はＥＡＰ－５Ｇ手順を停止し、ＩＫＥ ＳＡ及びＥＡＰスタック関連のリソースを復元する。ＥＡＰ－５Ｇ手順の停止には、５Ｇ－Ｓｔｏｐ表示が必要とされる。これらの手順はいずれも、

本明細書でさらに詳細に説明されている。

【００６５】

実施形態　－　修復可能なエラーによる登録失敗後のＥＡＰ－５Ｇ手順の完了

図５は、修復可能なエラーによる認証失敗後のＥＡＰ－５Ｇセッション手順の方法５００の実施形態の論理フロー図を示す。本実施形態では、信頼されていない非３ＧＰＰアクセスネットワーク１１０を介した５ＧＣＮ１００へのＵＥ２００登録要求は拒否される。

【００６６】

Ｎ３ＩＷＦ２０４は、ステップ５０２において、ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔメッセージを ＵＥ２００に送信する。この５Ｇ開始メッセージは、ＵＥ２００に、ＥＡＰ－５Ｇセッションを開始するよう要求する、つまり、ＥＡＰ－５Ｇパケットの中にカプセル化されたＮＡＳメッセージの送信を開始するよう要求する。ＵＥ２００は、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージ内に、５ＧＣＮ１００への登録要求を生成しており、このＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージは、ＡＮパラメータと、ステップ５０４でのその登録要求を含むＮＡＳ－ＰＤＵフィールドとを含む。本実施形態では、５ＧＣＮ１００へのＵＥ２００登録は、ＡＭＦ２０２によって拒否される。ＡＭＦ２０２は、登録拒否メッセージをＮ３ＩＷＦ２０４に送信する。それに応答して、Ｎ３ＩＷＦ２０４は、ＮＡＳ登録拒否メッセージを含むＮＡＳ－ＰＤＵフィールドを含むＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－ＮＡＳメッセージを、ステップ５０６でＵＥ２００に送信する。

【００６７】

登録を再試行することは必須ではないが、ＵＥ２００は、５ＧＣＮへの登録を再び開始することを試みることができる。構文エラーまたは特定の一時的な拒否理由などの修復可能なエラーの場合、ＵＥ２００は、更新されたパラメータで登録要求メッセージを変更し、登録を再試行し得る。あるいは、ＵＥ２００は、パラメータを更新せずに、後で登録を再試行してもよい。

【００６８】

ＵＥ２００は、必要に応じて更新されたＡＮパラメータと、ステップ５０８での登録要求を含むＮＡＳ－ＰＤＵフィールドとを含むＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージとしてフォーマットされた第２の登録要求を送信する。次に、ＵＥ２００及びＮ３ＩＷＦ２０４は、ＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立を行って、ＮＡＳセキュリティコンテキスト及びＮ３ＩＷＦ鍵を作成する（図示せず）。

【００６９】

Ｎ３ＩＷＦ鍵がＵＥ２００で作成された後、Ｎ３ＩＷＦ２０４は、５１０でのＥＡＰ－ｓｕｃｃｅｓｓを示すセキュリティモードコマンド（ＳＥＣＵＲＩＴＹ　ＭＯＤＥ　ＣＯＭＭＡＮＤ）メッセージを有したＮＡＳ　ＰＤＵを含むＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ　ＮＡＳメッセージを送信する。ＵＥ２００は、５１２でのセキュリティモード完了（ＳＥＣＵＲＩＴＹ　ＭＯＤＥ　ＣＯＭＰＬＥＴＥ）メッセージを含むＮＡＳ　ＰＤＵを備えたＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージを生成して送信することにより、ＥＡＰ－５Ｇセッションの完了を要求する。それによって、Ｎ３ＩＷＦ２０４がＡＭＦ２０２からＮ３ＩＷＦ鍵も受信していると仮定して、Ｎ３ＩＷＦ２０４がＵＥ２００にＥＡＰ－Ｓｕｃｃｅｓｓを送信することをトリガする。これでＥＡＰ－５Ｇセッションは完了し、それ以上ＥＡＰ－５Ｇパケットを交換することはできない。

【００７０】

このようにして、ＵＥ２００は、拒否されたときに、非３ＧＰＰアクセスネットワーク１１０を介して５ＧＣＮ１００への登録要求を再試行することができる。拒否は、構文エラーまたはＡＮパラメータのエラーなど、修復可能なエラーが原因である場合がある。このような修復可能なエラーが修正されたときに、２回目の登録試行は成功する可能性がある。別の実施形態では、拒否は一時的な拒否理由によるものである。その後、ＵＥ２００は、同じパラメータで登録を再試行し、ＥＡＰ－５Ｇセッションを完了することができる。

【００７１】

実施形態 － 修復不能なエラーによる登録失敗後のＥＡＰ－５Ｇ手順の完了

図６は、修復不能なエラーまたは永続的な障害による登録拒否のＥＡＰ－５Ｇセッション手順の実施形態を示す論理フロー図を示す。本実施形態では、信頼されていない非３ＧＰＰアクセスネットワーク１１０を介した５ＧＣＮ１００へのＵＥ２００登録要求は再び拒否される。

【００７２】

Ｎ３ＩＷＦ２０４は、ステップ６０２において、非３ＧＰＰアクセスネットワーク１１０を介した５ＧＣＮ１００への登録を開始するために、ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔメッセージを ＵＥ２００に送信する。ＵＥ２００は、登録要求、例えば、ＡＮパラメータと、ステップ６０４での登録要求を含むＮＡＳ－ＰＤＵフィールドとを含むＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージで応答する。

【００７３】

ＥＡＰ－ＡＫＡ’認証が成功しなかったなど、修復不能なエラーが原因で認証が失敗した場合、Ｎ３ＩＷＦ２０４はＡＭＦ２０２（図示せず）から登録拒否メッセージを受信する。ＡＭＦ２０２からの登録拒否メッセージの受信に応答して、Ｎ３ＩＷＦ２０４は、６０６でＵＥ２００へのＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－ＮＡＳメッセージを生成する。ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－ＮＡＳメッセージは、ＥＡＰ－Ｆａｉｌｕｒｅフィールドを有するＮＡＳ登録拒否メッセージを含むＮＡＳ－ＰＤＵフィールドを含む。

【００７４】

ＵＥ２００は、ステップ６０８において、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージを生成して送信することにより、登録手順を終了する。５Ｇ－ｓｔｏｐメッセージは、非３ＧＰＰアクセスネットワーク１１０を介した５ＧＣＮ１００への登録のためのＥＡＰセッションが終了したことを示す。ＵＥ２００からＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージを受信した後、Ｎ３ＩＷＦ２０４は、ステップ６１０において、ＥＡＰ－ＦａｉｌｕｒｅメッセージをＵＥ２００に送信することにより、ＥＡＰ－５Ｇの手順を終了する。本実施形態では、ＵＥ２００は、登録時に再試行することなく、ＥＡＰ－５Ｇセッションを停止する。

【００７５】

図７は、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージ７００の実施形態の概略ブロック図を示す。ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージ７００は、コード７０２、識別子７０４、長さ７０６、タイプ７０８、ベンダーＩＤ７１０、ベンダータイプ７１２、メッセージ識別子（メッセージＩＤ）７１４、スペア７１６、及び拡張子７１８を含む例示的なフィールドを有する様々なＥＡＰパケットを含む。ＥＡＰパケットのメッセージＩＤフィールド７１４は、５Ｇ－Ｓｔｏｐメッセージを示すための識別子を含む。ＥＡＰパケット内のフィールドの値の例を以下の表１に示す。

コードフィールドは、ＩＥＴＦ　ＲＦＣ　３７４８［９］　４．１項で指定された１（１０進数）に設定され、要求を示す。

識別子フィールドは、ＩＥＴＦ　ＲＦＣ　３７４８［９］　４．１項の指定に応じて設定される。

長さフィールドは、ＩＥＴＦ　ＲＦＣ　３７４８［９］　４．１項の指定に応じて設定され、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージの長さをオクテットで示す。

タイプフィールドは、ＩＥＴＦ　ＲＦＣ　３７４８［９］　５．７項で指定された２５４（１０進数）に設定され、拡張タイプを示す。

ベンダーＩＤフィールドは、ＳＭＩプライベートエンタープライズコードレジストリの下でＩＡＮＡに登録された１０４１５（１０進数）の３ＧＰＰベンダーＩＤに設定される。

ベンダータイプフィールドは、３ＧＰＰ　ＴＳ　３３．４０２［１０］　付録Ｃの指定に応じて、３（１０進数）のＥＡＰ－５Ｇメソッド識別子に設定される。

メッセージＩＤフィールドは、４（１０進数）の５Ｇ－Ｓｔｏｐ－ＩＤに設定される。

スペアフィールドはスペアビットで構成される。

拡張子フィールドはオプションのフィールドであり、スペアビットで構成される。

表１
ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージのフィールド例

【００７６】

ＥＡＰメッセージ内のメッセージ識別子（メッセージＩＤ）フィールド７１４は、５ＧＳｔｏｐ識別子または値を含む。ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージ７００のフィールド及び値は例にすぎず、登録停止の同様の意味を示す他のフィールド／値またはプロトコルパケットが実装されてもよい。

【００７７】

実施形態　－　認証失敗のためにＩＰｓｅｃ　ＳＡの確立が承認されないときに対処するための方法及びプロトコルの高度化

図８は、認証失敗により、非３ＧＰＰアクセスネットワーク１１０を介したＵＥ２００登録のためのＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が承認されないときのネットワークノード機能間のメッセージフローのための方法８００の実施形態の論理フロー図を示す。例えば、ＡＫＡ－ＣｈａｌｌｅｎｇｅまたはＡＫＡ’－ｃｈａｌｌｅｎｇｅなどの認証手順の失敗により、ＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が承認されない場合がある。方法８００は、ＵＥ２００に障害を伝えるための新たなプライベートＩＫＥｖ２通知メッセージタイプと、５ＧＣＮ１００へのアクセスが非３ＧＰＰアクセスネットワーク１１０によって許可されないことを指摘するための新たな原因値とを含む。

【００７８】
ＵＥ２００は、ステップ８０２において、信頼されていない非３ＧＰＰアクセスネットワーク（Ｎ３ＡＮ）１１０、例えば、パブリックＷＬＡＮに、８０２．１ｘプロトコルを使用して接続する。ＵＥ２００が５ＧＣＮ１００にアタッチすることを決定すると、ＵＥ２００は、ステップ８０４において、５Ｇ　ＰＬＭＮ内のＮ３ＩＷＦ２０４を選択する。ＵＥ２００は、例えば、ステップ８０６において、ＩＥＴＦ　ＲＦＣ　７２９６「Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ　Ｐｒｏｔｏｃｏｌ　Ｖｅｒｓｉｏｎ　２（ＩＫＥｖ２）」（２０１４年１０月）に記載されているように、ＩＫＥの初期交換を開始することで、選択したＮ３ＩＷＦ２０４とのＩＰｓｅｃセキュリティアソシエーション（ＳＡ）の確立を進める。ＩＫＥ　ＳＡの確立後、後続のＩＫＥメッセージは暗号化され、このステップ８０６で確立されたＩＫＥ　ＳＡを使用することによって整合性が保護される。

【００７９】
次に、ＵＥ２００は、ステップ８０８において、ＩＫＥ＿ＡＵＴＨ要求メッセージを送信することにより、ＩＫＥ＿ＡＵＴＨ交換を開始する。ＡＵＴＨペイロードはＩＫＥ＿ＡＵＴＨ要求メッセージに含まれず、このことは、ＩＫＥ＿ＡＵＴＨ交換が、ＥＡＰシグナリング（この場合はＥＡＰ－５Ｇシグナリング）を使用しなければならないことを示す。ＵＥ２００は、このメッセージのＵＥ　ＩＤフィールドを任意の乱数に等しく設定することになる。Ｎ３ＩＷＦ２０４は、ステップ８１０において、ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔパケットを含むＩＫＥ＿ＡＵＴＨレスポンスメッセージで応答する。ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔパケットは、ＵＥ２００に、ＥＡＰ－５Ｇセッションを開始するよう通知する、つまり、ＥＡＰ－５Ｇパケットの中にカプセル化されたＮＡＳメッセージの送信を開始するよう通知する。

【００８０】
ＵＥ２００はまた、Ｎ３ＩＷＦ証明書を有効にし、Ｎ３ＩＷＦ２０４のＩＤがＵＥ２００によって選択されたＮ３ＩＷＦ２０４と一致することを確認し得る。Ｎ３ＩＷＦ２０４からの証明書がないか、またはＩＤ確認に失敗すると、接続に失敗する可能性がある。次に、ＵＥ２００は、ステップ８１２で、５ＧＣＮ１００への登録を要求するために、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳパケットを含むＩＫＥ＿ＡＵＴＨ要求を送信する。ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージは、ＡＮパラメータ（例えば、ＧＵＡＭＩ、選択されたＰＬＭＮ　ＩＤ、要求されたＮＳＳＡＩ）と、登録要求を含むＮＡＳ－ＰＤＵフィールドとを含む。

【００８１】
次に、Ｎ３ＩＷＦ２０４は、ＡＮパラメータを使用してＡＭＦ２０２を選択し、ステップ８１４において、ＵＥ２００から受信した登録要求をＮ２　ＮＡＳトランスポートメッセージでＡＭＦ２０２に転送する。

【００８２】
ＡＭＦ２０２は、ＵＥ２００を認証することを決定することができる。この場合、ＡＭＦ２０２は、ステップ８１６でＡＵＳＦ２１０を選択し、そのＡＵＳＦ２１０に鍵要求を送信する。次に、ＡＵＳＦ２１０は、ステップ８１８で、ＡＫＡ－ＣｈａｌｌｅｎｇｅまたはＡＫＡ’－ｃｈａｌｌｅｎｇｅなどの認証手順を開始することができる。ＡＭＦ２０２とＵＥ２００との間で、認証パケットはＮＡＳ認証メッセージ内にカプセル化され、このＮＡＳ認証メッセージはＥＡＰ－５Ｇ／５Ｇ－ＮＡＳパケット内にカプセル化される。ステップ８２０及び８２２では、ＮＡＳメッセージの認証要求メッセージ内のＥＡＰ－Ｒｅｑｕｅｓｔ／ＡＫＡ’－Ｃｈａｌｌｅｎｇｅメッセージが、Ｎ３ＩＷＦ２０４を介してＵＥ２００へ送信される。このメッセージは、認証が成功した場合に作成される部分的ネイティブセキュリティコンテキストを識別するためにＵＥ２００及びＡＭＦ２０２によって使用されるｎｇＫＳＩを含み得る。ＵＥ２００は、ＥＡＰ－Ｒｅｑｕｅｓｔ／ＡＫＡ’－Ｃｈａｌｌｅｎｇｅメッセージで受信したＲＡＮＤ及びＡＵＴＮをＵＳＩＭに転送する。

【００８３】
ＲＡＮＤ及びＡＵＴＮを受信すると、ＵＳＩＭは、ＡＵＴＮを承認することができるか

どうかを確認することにより、認証ベクトルを検証する。その場合、ＵＳＩＭはステップ８２３でレスポンスＲＥＳを計算する。ＵＥ２００は、ステップ８２４において、ＮＡＳメッセージのＡｕｔｈ－Ｒｅｓｐメッセージ内のＥＡＰ－Ｒｅｓｐｏｎｓｅ／ＡＫＡ’－Ｃｈａｌｌｅｎｇｅメッセージを送信する。ＥＡＰ－Ｒｅｓｐｏｎｓｅ／ＡＫＡ’－Ｃｈａｌｌｅｎｇｅメッセージは、ステップ８２６及び８２８において、ＡＭＦ２０２を介してＡＵＳＦ２１０に送信される。次に、ＡＵＳＦ２１０は、メッセージの検証を試みることになる。ＡＵＳＦ２１０は、このメッセージを成功裏に検証した場合、認証を続行する。

【００８４】

先行する既知のシステムでは、ＡＵＳＦ２１０は、ステップ８３０での認証失敗のために、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されていないと判定した場合に、エラーを返す。新しく改良されたシステム及び方法では、ＡＭＦ２０２は、例えば認証の失敗のために５ＧＣネットワークへの非３ＧＰＰアクセスが許可されないことを伝えるために、新たなプライベートＩＫＥｖ２通知メッセージタイプを生成する。

【００８５】

ステップ８３２において、ＡＵＳＦ２１０は、ＥＡＰ失敗（ＥＡＰ－Ｆａｉｌｕｒｅ）のＥＡＰペイロード（ＥａｐＰａｙｌｏａｄ）と、認証失敗（ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ＿ＦＡＩＬＵＲＥ）の認証結果（ａｕｔｈｅｎＲｅｓｕｌｔ）とを含むＨＴＴＰ　ＥＡＰセッション（ＥＡＰ－ｓｅｓｓｉｏｎ）メッセージを送信する。ＡＭＦ２０２は、５ＧＣＮ１００の非３ＧＰＰアクセスが許可されていないことを示す新たな５Ｇモビリティ管理（５ＧＭＭ）の原因（ｃａｕｓｅ）を生成する。ＡＭＦ２０２は、ステップ８３４で、登録拒否とＥＡＰ失敗を示すＥＡＰメッセージ（ＥＡＰ　ｍｅｓｓａｇｅ）とを含み、５ＧＭＭ原因を含むＮ２　ＮＡＳトランスポートメッセージを生成する。５ＧＭＭ原因（５ＧＭＭ＿ｃａｕｓｅ）は、エラータイプが、例えばこの場合は、「５ＧＣＮの非３ＧＰＰアクセスは許可されていない」であることを示している。

【００８６】

ＵＥ２００は、ステップ８３６において、Ｎ３ＩＷＦ２０４から、プライベート通知メッセージタイプ（例えば、８１９２．．．１６３８３などの事前定義された範囲内の任意のプライベート通知メッセージタイプ）を有する通知ペイロードを含むＩＫＥ＿ＡＵＴＨレスポンスメッセージを受信する。プライベートＩＫＥｖ２通知メッセージには、「５ＧＣへの非３ＧＰＰアクセスは許可されない（ＮＯＮ＿３ＧＰＰ＿ＡＣＣＥＳＳ＿ＴＯ＿５ＧＣＮ＿ＮＯＴ＿ＡＬＬＯＷＥＤ）」の５ＧＭＭ原因による登録拒否と、ＥＡＰ－ＦａｉｌｕｒｅのＥＡＰメッセージタイプとを含むＥＡＰレスポンス／５Ｇ－ＮＡＳ　ＰＤＵが含まれる。

【００８７】

したがって、方法８００は、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されないという登録要求の失敗をＵＥに通知するために、新たなプライベートＩＫＥｖ２通知メッセージタイプと新たな５ＧＭＭ原因値とを含む。新たなプライベートＩＫＥｖ２通知メッセージが実装されるが、５ＧＣネットワークへの非３ＧＰＰアクセスが許可されないか、または拒否されたことをＵＥ２００に通知するために、他のタイプのメッセージ、またはフォーマット、またはフィールド、またはエラータイプが実装されてもよい。

【００８８】

ＮＯＮ＿３ＧＰＰ＿ＡＣＣＥＳＳ＿ＴＯ＿５ＧＣＮ＿ＮＯＴ＿ＡＬＬＯＷＥＤの５ＧＭＭ原因を伴うプライベート通知メッセージを受信すると、ＵＥ２００は、ステップ８３８において、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージを送信することにより、ＥＡＰ－５Ｇセッションを終了する。ＵＥ２００は、ステップ８４０において、Ｎ３ＩＷＦ２０４から、ＥＡＰ失敗メッセージ付きのＩＫＥ＿ＡＵＴＨレスポンスメッセージを受信する。

【００８９】

Ｎ３ＩＷＦ２０４からＥＡＰ失敗メッセージを受信すると、ＵＥ２００は、ＩＫＥｖ２ＳＡ削除手順を実行し、ステップ８４２でＩＫＥ　ＳＡを閉じる。ＵＥ２００は、スイッ

チを切るか、またはＵＳＩＭを含むＵＩＣＣが除去されるまで、同じＰＬＭＮからＮ３ＩＷＦ２０４へのＩＫＥ　ＳＡ及びＩＰｓｅｃ　ＳＡの確立を再開始しない。ＵＥ２００は、ステップ８４４で、ＩＫＥｖ２　ＳＡ削除の情報（ＩＮＦＯＲＭＡＴＩＯＮＡＬ）メッセージを送信してもよい。その後、Ｎ３ＩＷＦ２０４は、ステップ８４６でＩＫＥｖ２　ＳＡを閉じることができる。

【００９０】

実施形態　－　サブスクリプション制限のためにＩＰｓｅｃ　ＳＡの確立が承認されないときに対処するための方法及びプロトコルの高度化

図９は、非３ＧＰＰアクセスを介したＵＥ２００登録のためのＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が、サブスクリプション制限のために承認されないときのネットワーク機能間のメッセージフローのための方法９００の実施形態の論理フロー図を示す。例えば、サブスクリプション制限により、ＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡの確立が承認されない場合がある。方法９００は、ＵＥ２００に障害を伝えるための新たなプライベートＩＫＥｖ２通知メッセージタイプと、５ＧＣＮ１００へのアクセスが非３ＧＰＰアクセスネットワーク１１０によって許可されないことを指摘するための新たな原因値とを含む。

【００９１】

ＵＥ２００は、ステップ９０２において、信頼されていない非３ＧＰＰアクセスネットワーク（Ｎ３ＡＮ）１１０、例えば、パブリックＷＬＡＮに、８０２．１ｘプロトコルを使用して接続する。ＵＥ２００が５ＧＣＮ１００にアタッチすることを決定すると、ＵＥ２００は、ステップ９０４において、５Ｇ　ＰＬＭＮ内のＮ３ＩＷＦ２０４を選択する。ＵＥ２００は、例えば、ステップ９０６において、ＩＥＴＦ　ＲＦＣ　７２９６「Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ　Ｐｒｏｔｏｃｏｌ　Ｖｅｒｓｉｏｎ　２（ＩＫＥｖ２）」（２０１４年１０月）に記載されているように、ＩＫＥの初期交換を開始することで、選択したＮ３ＩＷＦ２０４とのＩＰｓｅｃセキュリティアソシエーション（ＳＡ）の確立を進める。ＩＫＥ　ＳＡの確立後、後続のＩＫＥメッセージは暗号化され、このＩＫＥ　ＳＡで確立された鍵を使用して整合性が保護される。

【００９２】

次に、ＵＥ２００は、ステップ９０８において、ＩＫＥ＿ＡＵＴＨ要求メッセージを送信することにより、ＩＫＥ＿ＡＵＴＨ交換を開始する。ＡＵＴＨペイロードはＩＫＥ＿ＡＵＴＨ要求メッセージに含まれず、このことは、ＩＫＥ＿ＡＵＴＨ交換が、ＥＡＰシグナリング（この場合はＥＡＰ－５Ｇシグナリング）を使用しなければならないことを示す。ＵＥ２００は、このメッセージのＵＥ　ＩＤフィールドを任意の乱数に等しく設定する。Ｎ３ＩＷＦ２０４は、ステップ９１０において、ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔパケットを含むＩＫＥ＿ＡＵＴＨレスポンスメッセージで応答する。ＥＡＰ－Ｒｅｑｕｅｓｔ／５Ｇ－Ｓｔａｒｔパケットは、ＵＥ２００に、ＥＡＰ－５Ｇセッションを開始するよう通知する、つまり、ＥＡＰ－５Ｇパケットの中にカプセル化されたＮＡＳメッセージの送信を開始するよう通知する。

【００９３】

ＵＥ２００はまた、Ｎ３ＩＷＦ証明書を有効にし、Ｎ３ＩＷＦ２０４のＩＤがＵＥによって選択されたＮ３ＩＷＦ２０４と一致することを確認し得る。Ｎ３ＩＷＦ２０４からの証明書がないか、またはＩＤ確認に失敗すると、接続に失敗する可能性がある。次に、ＵＥ２００は、ステップ９１２において、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳパケットを含むＩＫＥ＿ＡＵＴＨ要求の中の登録要求を送信する。ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳパケットは、ＧＵＡＭＩ、選択されたＰＬＭＮ　ＩＤ、要求されたＮＳＳＡＩなどのＡＮパラメータと、登録要求を有するＮＡＳ　ＰＤＵとを含む。次に、Ｎ３ＩＷＦ２０４は、ステップ９１４において、ＡＭＦ２０２を選択し、ＵＥ２００から受信したＮＡＳ　ＰＤＵ内の登録要求をＡＭＦ２０２に転送する。

【００９４】

ＡＭＦ２０２は、ＵＥ２００を認証することを決定することができる。この場合、ＡＭ

Ｆ２０２は、ステップ９１６でＡＵＳＦ２１０を選択し、そのＡＵＳＦ２１０に鍵要求を送信する。次に、ＡＵＳＦ２１０は、ステップ９１８で、ＡＫＡ－ＣｈａｌｌｅｎｇｅまたはＡＫＡ’－ｃｈａｌｌｅｎｇｅなどの認証手順を開始することができる。ＡＭＦ２０２とＵＥ２００との間で、認証パケットはＮＡＳ認証メッセージ内にカプセル化され、このＮＡＳ認証メッセージはＥＡＰ－５Ｇ／５Ｇ－ＮＡＳパケット内にカプセル化される。ＮＡＳメッセージの認証要求メッセージ内のＥＡＰ－Ｒｅｑｕｅｓｔ／ＡＫＡ’－Ｃｈａｌｌｅｎｇｅメッセージが、ステップ９２０でＡＭＦによってＵＥ２００に送信され、ステップ９２２でＮ３ＩＷＦによって転送される。このメッセージは、認証が成功した場合に作成される部分的ネイティブセキュリティコンテキストを識別するためにＵＥ２００及びＡＭＦ２０２によって使用されるｎｇＫＳＩを含み得る。ＵＥ２００は、ＥＡＰ－Ｒｅｑｕｅｓｔ／ＡＫＡ’－Ｃｈａｌｌｅｎｇｅメッセージで受信したＲＡＮＤ及びＡＵＴＮを、ＵＥ２００のＵＳＩＭに転送する。

【００９５】

ＲＡＮＤ及びＡＵＴＮを受信すると、ＵＳＩＭは、ＡＵＴＮを承認することができるかどうかを確認することにより、認証ベクトルを検証する。その場合、ＵＳＩＭはステップ９２３で認証レスポンスを計算する。ＵＥ２００は、ステップ９２４において、ＮＡＳメッセージのＡｕｔｈ－Ｒｅｓｐメッセージ内のＥＡＰ－Ｒｅｓｐｏｎｓｅ／ＡＫＡ’－Ｃｈａｌｌｅｎｇｅメッセージを送信する。ＥＡＰ－Ｒｅｓｐｏｎｓｅ／ＡＫＡ’－Ｃｈａｌｌｅｎｇｅメッセージは、ステップ９２６でＮ３ＩＷＦによってＡＭＦに送信され、次にステップ９２８でＡＵＳＦ２１０に送信される。次に、ＡＵＳＦ２１０は、メッセージの検証を試みることになる。ＡＵＳＦ２１０は、このメッセージを成功裏に検証した場合、認証を続行する。しかしながら、ＡＵＳＦ２１０は、ステップ９３０において、認証を拒否し、非３ＧＰＰの５ＧＣＮ１００へのアクセスを許可しない場合がある。

【００９６】

先行する既知のシステムでは、ＡＵＳＦ２１０が認証失敗を判定すると、ＡＵＳＦ２１０はエラーを返す。新しく改良された方法では、ＡＭＦ２０２は、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されないことを伝えるために、新たな原因を生成する。例えば、ＡＭＦ２０２は、例えば、サブスクリプションまたはネットワークの制限のために、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されないことをＵＥ２００に伝えるために、新たなプライベートＩＫＥｖ２通知メッセージタイプを生成することができる。

【００９７】

ステップ９３２において、ＡＵＳＦ２１０は、ＥＡＰ失敗（ＥＡＰ－Ｆａｉｌｕｒｅ）のＥＡＰペイロード（ＥａｐＰａｙｌｏａｄ）と、認証失敗（ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ＿ＦＡＩＬＵＲＥ）の認証結果（ａｕｔｈｅｎＲｅｓｕｌｔ）とを含むＨＴＴＰ ＥＡＰセッション（ＥＡＰ－ｓｅｓｓｉｏｎ）メッセージを原因とともに送信する。ＡＭＦ２０２は、ステップ９３４で、登録拒否とＥＡＰ失敗のＥＡＰメッセージ（ＥＡＰ ｍｅｓｓａｇｅ）とを有する、５ＧＭＭ原因を含むＮ２ ＮＡＳトランスポートメッセージを生成する。５ＧＭＭ原因（５ＧＭＭ＿ｃａｕｓｅ）は、エラータイプがＮＯＮ＿３ＧＰＰ＿ＡＣＣＥＳＳ＿ＴＯ＿５ＧＣＮ＿ＮＯＴ＿ＡＬＬＯＷＥＤであることを示している。

【００９８】

Ｎ３ＩＷＦ２０４は、５ＧＣＮへの非３ＧＰＰアクセスが許可されていないことを示す５ＧＭＭ原因値と、ＥＡＰ－Ｆａｉｌｕｒｅタイプメッセージとを含む登録拒否メッセージをカプセル化したＡＭＦ２０２からのレスポンスを受信する。Ｎ３ＩＷＦ２０４は、ステップ９３６において、プライベート通知メッセージタイプ（例えば、８１９２．．．１６３８３などの事前定義された範囲内の任意のプライベート通知メッセージタイプ）を有する通知（Ｎｏｔｉｆｙ）ペイロードを含むＩＫＥ＿ＡＵＴＨレスポンスメッセージを生成する。プライベートＩＫＥｖ２通知メッセージには、「５ＧＣへの非３ＧＰＰアクセスは許可されない（ＮＯＮ＿３ＧＰＰ＿ＡＣＣＥＳＳ＿ＴＯ＿５ＧＣＮ＿ＮＯＴ＿ＡＬＬＯＷＥＤ）」の５ＧＭＭ原因による登録拒否と、ＥＡＰ－ＦａｉｌｕｒｅのＥＡＰメッセージタイプとを含むＥＡＰレスポンス／５Ｇ－ＮＡＳ ＰＤＵが含まれる。

【００９９】
このように、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されていないことをＵＥ２００に伝えるために、新たな５ＧＭＭ原因コードが実装される。この５ＧＭＭ原因は、ＡＭＦ２０２によって生成され、ＵＥ２００がサブスクリプションまたはネットワークの制限により、非３ＧＰＰアクセスネットワーク１１０を介して５ＧＣＮ１００にアクセスすることが許可されていないＰＬＭＮでは、ＵＥ２００が非３ＧＰＰアクセスを介してサービスを要求した場合に、この５ＧＭＭ原因がＵＥ２００に送信される。したがって、ＵＥ２００は、非３ＧＰＰアクセスネットワーク１１０を介して５ＧＣＮ１００へアクセスすることが拒否されたことを通知される。

【０１００】
ＵＥ２００は、ステップ９３６において、Ｎ３ＩＷＦ２０４から、プライベート通知メッセージタイプを有する通知ペイロードと、ＥＡＰ－ＦａｉｌｕｒｅのＥＡＰメッセージと、ＮＯＮ＿３ＧＰＰ＿ＡＣＣＥＳＳ＿ＴＯ＿５ＧＣＮ＿ＮＯＴ＿ＡＬＬＯＷＥＤの５ＧＭＭ原因とを含むＩＫＥ＿ＡＵＴＨレスポンスメッセージを受信する。この結果として、ＵＥ２００は、単にエラーメッセージを受信するのではなく、理由付きの登録拒否通知を受信する。

【０１０１】
次に、ＵＥ２００は、ステップ９３８において、Ｎ３ＩＷＦ２０４へのＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージを生成することにより、登録要求を終了する。ＵＥ２００は、ステップ９４０において、Ｎ３ＩＷＦ２０４から、ＥＡＰ失敗メッセージ付きのＩＫＥ＿ＡＵＴＨレスポンスメッセージを受信する。

【０１０２】
Ｎ３ＩＷＦ２０４からＥＡＰ失敗メッセージを受信すると、ＵＥ２００は、ＩＫＥｖ２ＳＡ削除手順を実行し、ステップ９４２でＩＫＥ　ＳＡを閉じる。本例では、サブスクリプションまたはネットワークの制限という修正不能なエラーのため、ＵＥ２００は、スイッチを切るか、またはＵＳＩＭを含むＵＩＣＣが除去されるまで、同じＰＬＭＮからＮ３ＩＷＦ２０４へのＩＫＥ　ＳＡ及びＩＰｓｅｃ　ＳＡの確立を再開始しない。ＵＥ２００は、ステップ９４４で、ＩＫＥｖ２　ＳＡ削除の情報（ＩＮＦＯＲＭＡＴＩＯＮＡＬ）メッセージを送信してもよい。その後、Ｎ３ＩＷＦ２０４は、ステップ９４６でＩＫＥｖ２ＳＡを閉じることができる。

【０１０３】
実施形態　－　ユーザプレーンのＩＰｓｅｃ　ＳＡの確立が承認されないときに対処するための方法及びプロトコルの高度化
図１０は、ユーザプレーンＩＰｓｅｃセキュリティアソシエーション（ＳＡ）の確立が承認されないときのネットワークノード機能間のメッセージフローのための方法の実施形態の論理フロー図を示す。ＵＥ２００は、ステップ１００２において、信頼されていない非３ＧＰＰアクセスネットワーク（Ｎ３ＡＮ）１１０、例えば、パブリックＷＬＡＮに、８０２．１ｘプロトコルを使用して接続する。ＵＥ２００が５ＧＣＮ１００にアタッチすることを決定すると、ＵＥ２００は、ステップ１００４において、５Ｇ　ＰＬＭＮ内のＮ３ＩＷＦ２０４を選択する。ＵＥ２００は、ステップ１００６でＩＫＥ初期交換を開始することにより、選択されたＮ３ＩＷＦ２０４とのＩＰｓｅｃセキュリティアソシエーション（ＳＡ）の確立を進める。本実施形態では、ＵＥ２００は、１００８で、選択されたＮ３ＩＷＦ２０４に対してＩＫＥ　ＳＡ及びシグナリングＩＰｓｅｃ　ＳＡを正常に確立する。例えば、図３に示すように、例えば、ＥＡＰ－ＡＫＡ’手順などのＵＥ２００の認証が成功し、ＥＡＰ－５Ｇが完了する。

【０１０４】
次に、ＵＥ２００は、１０１０でＰＤＵセッション確立要求メッセージをＡＭＦ２０２に送信して、ユーザプレーンＩＰｓｅｃ　ＳＡを確立する。このＰＤＵセッション確立要求メッセージは、シグナリングＩＰｓｅｃ　ＳＡを介してＮ３ＩＷＦ２０４に送信され、Ｎ３ＩＷＦ２０４は、このメッセージを、ステップ１０１２で、５ＧＣＮ１００のＡＭＦ

２０２に透過的に転送する。ＡＭＦ２０２は、ステップ１０１４で、ＳＭＦ２０６とのセッション管理（ＳＭ）コンテキストを作成することができる。ＡＭＦ２０２は、ＮＡＳ　Ｎ２インタフェースＰＤＵセッション要求メッセージをＮ３ＩＷＦ２０４に送信して、例えば、ステップ１０１６で、Ｎ２　ＰＤＵセッションリソースセットアップ要求において、このＰＤＵセッションのためのアクセスリソースを確立する。ＰＤＵセッション要求は、ＰＤＵセッションＩＤ、ＰＤＵセッション確立承認、ＱＦＩ、ＱｏＳプロファイルなどを含み得る。

【０１０５】

独自のポリシー及び構成に基づいて、かつＮ２　ＰＤＵセッション要求で受信したＱｏＳプロファイルに基づいて、Ｎ３ＩＷＦ２０４は、確立するユーザプレーンＩＰｓｅｃ　ＳＡの数と、各ユーザプレーンＩＰｓｅｃ　ＳＡに関連付けられたＱｏＳプロファイルとを判定する。例えば、Ｎ３ＩＷＦ２０４は、１つのユーザプレーンＩＰｓｅｃ　ＳＡを確立し、全てのＱｏＳプロファイルをこのユーザプレーンＩＰｓｅｃ　ＳＡに関連付けることを決定することができる。本例では、ＰＤＵセッションの全てのＱｏＳフローは、１つのユーザプレーンＩＰｓｅｃ　ＳＡを介して転送される。別の例では、Ｎ３ＩＷＦ２０４は、複数のユーザプレーンＩＰｓｅｃチャイルドＳＡを確立し、特定のＱｏＳプロファイルを、複数のユーザプレーンＩＰｓｅｃチャイルドＳＡのうちの種々のユーザプレーンＩＰｓｅｃチャイルドＳＡに関連付けることを決定し得る。

【０１０６】

Ｎ３ＩＷＦ２０４は、ステップ１０１８で、ＰＤＵセッションのための第１のユーザプレーンＩＰｓｅｃチャイルドＳＡを確立するために、ＩＫＥ　Ｃｒｅａｔ＿Ｃｈｉｌｄ＿ＳＡ要求をＵＥ２００に送信する。ＩＫＥ　Ｃｒｅａｔｅ＿Ｃｈｉｌｄ＿ＳＡ要求は、ＳＡｕｐ１のＩＤを持つ第１のユーザプレーンＩＰｓｅｃチャイルドＳＡを示す。この要求には、（ａ）チャイルドＳＡに関連付けられたＱＦＩ（複数可）、（ｂ）このチャイルドＳＡに関連付けられたＰＤＵセッションのＩＤ、（ｃ）任意選択で、チャイルドＳＡに関連付けられたＤＳＣＰ値、及び（ｄ）ＵＰ＿ＩＰ＿ＡＤＤＲＥＳＳを含む３ＧＰＰ固有の通知（Ｎｏｔｉｆｙ）ペイロードが含まれ得る。ＩＫＥ　Ｃｒｅａｔｅ＿Ｃｈｉｌｄ＿ＳＡ要求は、ＳＡペイロード、Ｎ３ＩＷＦ２０４及びＵＥ２００のトラフィックセレクタ（Ｔｒａｆｆｉｃ　Ｓｅｌｅｃｔｏｒ）（ＴＳ）などの他の情報を含む場合もある。

【０１０７】

ＵＥ２００が新たなＩＰｓｅｃチャイルドＳＡを承認すると、ＵＥ２００は、ステップ１０２０で、ＩＫＥ　Ｃｒｅａｔｅ＿Ｃｈｉｌｄ＿ＳＡレスポンスを送信する。ＵＥ２００及びＮ３ＩＷＦ２０４は、ステップ１０２２で、複数のＩＰｓｅｃチャイルドＳＡを確立するために、ＩＫＥ　Ｃｒｅａｔｅ＿Ｃｈｉｌｄ＿ＳＡ要求及びレスポンスの複数回の繰り返しをやり取りし得る。追加のＩＰｓｅｃチャイルドＳＡが確立され、それぞれが１つ以上のＱＦＩ（複数可）とＵＰ＿ＩＰ＿ＡＤＤＲＥＳＳとに関連付けられる。

【０１０８】

ステップ１０２４でのユーザプレーンＩＰｓｅｃ　ＳＡ要求が、ステップ１０２６でのように、ＵＥ２００によって承認されない場合、ＵＥ２００は、ステップ１０２６で、エラータイプの通知ペイロードを有するＣＲＥＡＴＥ＿ＣＨＩＬＤ＿ＳＡレスポンスメッセージをＮ３ＩＷＦ２０４に送信する。通知メッセージのタイプは「エラー」であり得る。「エラー」の通知メッセージタイプは、ＩＰｓｅｃチャイルドＳＡがＵＥ２００によって承認されないことを示す。

【０１０９】

エラータイプの通知ペイロードを含むＣＲＥＡＴＥ＿ＣＨＩＬＤ＿ＳＡレスポンスメッセージを受信すると、Ｎ３ＩＷＦ２０４は、非３ＧＰＰアクセスを介したＰＤＵセッション確立の拒否をトリガするために、ステップ１０３２でＮ２　ＰＤＵセッションリソースセットアップレスポンスメッセージを介して、ＡＭＦ２０２に、失敗と、セットアップに失敗したＰＤＵセッションリソースのリストとを示す。あるいは、Ｎ３ＩＷＦ２０４が、以前にＰＤＵセッションのＱｏＳフロー識別子（ＱＦＩ）用に、複数のユーザプレーンＩ

Ｐｓｅｃ　ＳＡを作成することを決定し、ＰＤＵセッションの１つ以上のユーザプレーンＩＰｓｅｃ　ＳＡがすでにアクティブである場合、ネットワークは、ステップ１０２８及び１０３０に示すように、障害が発生したユーザプレーンＩＰｓｅｃ　ＳＡのＱＦＩ（複数可）を、すでに確立されているユーザプレーンＩＰｓｅｃ　ＳＡにマッピングすることにより、ＰＤＵセッションの確立を完了することを選択することができる。

【０１１０】

ステップ１０３４で、ＰＤＵセッション確立拒否メッセージを示すＮＡＳ　ＰＤＵを含むＮ２　ＰＤＵセッションリソース解放コマンドを受信すると、Ｎ３ＩＷＦ２０４は、ステップ１０３６で、このＰＤＵセッション確立拒否をＵＥ２００へ透過的に転送する。専用の５Ｇセッション管理（５ＧＳＭ）原因（５ＧＳＭ＿ｃａｕｓｅ）「ＩＰｓｅｃ　ＳＡ障害」が、ＰＤＵセッション拒否の理由を示すために定められている。

【０１１１】

実施形態 － 非３ＧＰＰアクセスのためのプライベートＩＫＥｖ２通知メッセージタイプ

以下の表２に、非３ＧＰＰアクセス用の通知メッセージのタイプを示す。本例では、プライベートＩＫＥｖ２通知メッセージ及びプライベートエラータイプを説明しているが、他のメッセージプロトコル、値、及びエラータイプを、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されないときに、ＵＥ２００へ理由またはエラーの通知を提供するのに使用してもよい。

【０１１２】

本例では、プライベートＩＫＥｖ２通知メッセージタイプが非３ＧＰＰアクセス使用のために定義されている。８１９２～１６３８３の値（１０進数）を持つ通知メッセージタイプが、プライベートエラー使用のために予約されているが、他の値やフィールドが実装されている場合もある。４０９６０～６５５３５の値（１０進数）を持つ通知メッセージタイプが、プライベートステータスでの使用のために予約されている。本明細書では、本明細書で使用されるプライベートＩＫＥｖ２通知メッセージタイプのみを説明する。表２で定義されているプライベート通知メッセージのエラータイプは、５ＧＣＮ１００への非３ＧＰＰアクセスのネゴシエーション中のエラーを示すエラー通知である。例えば、エラータイプは、５ＧＣＮ１００への非３ＧＰＰアクセスのためのＩＫＥｖ２　ＳＡまたはＩＰｓｅｃ　ＳＡのネゴシエーションに応答して生成され得る。プライベート通知メッセージタイプのフィールド及び値は例にすぎず、同様の意味を示す他のフィールド／値を実装してもよい。

通知メッセージ	値 (10進数)	説明
AUTHORIZATION_REJECTED	9003	エラータイプは、UEがこのサービスの使用を許可されていないために、要求されたサービスが拒否されたことを示すのに使用される。
ILLEGAL_ME	9006	エラータイプは、要求されたサービスが認証失敗のために拒否されたか、UE のアイデンティティがネットワークに受け入れられないために拒否されたことを示すのに使用される。
RAT_TYPE_NOT_ALLOWED	11001	エラータイプは、要求されたサービスが拒否されたことを示すのに使用される。使用された RAT タイプは PLMN によって許可されていない。
PEI_NOT_ACCEPTED	11005	エラータイプは、ネットワークがPEIを使用した緊急サービス要求を受け入れないため、緊急PDUセッション要求が拒否されたことを示すのに使用される。
PLMN_NOT_ALLOWED	11011	エラータイプは、サブスクリプションまたはオペレーターが決定した規制により、要求されたサービスが拒否されたことを示すのに使用される。
NETWORK_FAILURE	10500	エラータイプは、要求されたサービスがネットワーク障害のために拒否されたことを示すのに使用される。
CONGESTION	12005	エラータイプは、要求されたサービスがネットワークの輻輳のために拒否されたことを示すのに使用される。
5GS_SERVICEs_NOT_ALLOWED	12007	エラータイプは、5GSサービスが許可されていないため、要求されたサービスが拒否されたことを示すのに使用される。
NON_3GPP_ACCESS_TO_5GC_NOT_ALLOWED	12071	エラータイプは、UE が 5GC への非 3GPP アクセスの使用を許可されていないため、要求されたサービスが拒否されたことを示すのに使用される。

表２
非３ＧＰＰアクセス用の通知メッセージのタイプ
【０１１３】
ＵＥ２００は、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されていないことを示すエラータイプを伴うメッセージを受信することができる。この結果として、ＵＥ２００は、非３ＧＰＰアクセスネットワーク１１０を介して５ＧＣＮ１００へアクセスすることが拒否されたことを通知される。
【０１１４】
実施形態 － ５ＧＣネットワークへの非３ＧＰＰアクセスのためのサブスクリプションがないために認証失敗を通知するための原因コード
図１１は、５ＧＭＭ原因情報要素１１００の実施形態の概略ブロック図を示す。５ＧＭＭ原因情報要素１１００は、５ＧＭＭ原因情報要素インディケータ（ＩＥＩ）１１０４及び原因値１１０６を含む。原因値１１０６は、ＵＥ２００から５ＧＣＮ１００へのアクセスを求める５ＧＭＭ要求がネットワークによって拒否される理由を示す。本実施形態においては、「５ＧＣＮへの非３ＧＰＰアクセスは許可されていない」に新たな原因コードが対応する。この５ＧＭＭ原因は、サブスクリプション、ネットワーク制限、またはその他の認証失敗により、ＵＥ２００が非３ＧＰＰアクセスを介して５ＧＣＮ１００にアクセスすることを許可されていないＰＬＭＮにおいて、ＵＥ２００が非３ＧＰＰアクセスを介してサービスを要求した場合に、ＵＥ２００に送信される。
【０１１５】
図１２は、５ＧＭＭ原因情報要素の値の実施形態の概略ブロック図を示す。この例では、所定の値が「５ＧＣＮへの非３ＧＰＰアクセスは許可されていない」に対応する。ＵＥ２００によって受信される他の値が、「プロトコルエラー、詳細不明」として扱われる。ネットワークが受信したその他の何らかの値も「プロトコルエラー、詳細不明」として扱われる。５ＧＭＭ原因情報要素のフィールド及び値は例にすぎず、同様の意味を示す他の

フィールド／値を実装してもよい。
【０１１６】
図１３は、Ｎ３ＩＷＦ２０４の方法１３００の実施形態の論理フロー図を示す。Ｎ３ＩＷＦ２０４は、ステップ１３０２で１つ以上のプロトコルを使用して、５ＧＣＮ１００内のノードと第１のインタフェースを使用して通信する。Ｎ３ＩＷＦ２０４は、ステップ１３０４で、ＩＥＥＥ　８０２．１ｘ　ＷＬＡＮプロトコルに準拠したＷＬＡＮトランシーバなどの少なくとも第２のインタフェースを使用して、非３ＧＰＰアクセスネットワークを介してＵＥと通信する。
【０１１７】
Ｎ３ＩＷＦ２０４は、ステップ１３０６で、信頼されていないアクセスネットワーク内のＵＥ２００からコアネットワークへ安全な接続を確立するための登録要求を処理する。例えば、Ｎ３ＩＷＦ２０４は、ＵＥ２００からのＡＮパラメータ及び登録要求を含むＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージを受信する。Ｎ３ＩＷＦ２０４は、ＵＥ２００の認証及びサブスクリプションチェックのために、メッセージを５ＧＣＮ１００に転送する。例えば、Ｎ３ＩＷＦ２０４は、認証及びサブスクリプションチェックの要求を生成し、この認証及びサブスクリプションチェックの要求を、ＡＭＦ２０２に向けて、第２のインタフェースを介して送信する。
【０１１８】
Ｎ３ＩＷＦ２０４は、例えば、修復不能なエラーのために、ステップ１３０８で、接続の確立がコアネットワークによって承認されないと判定する。例えば、ＡＭＦ２０２は、ＡＵＳＦ２１０から認証失敗のレスポンスを受信する。ＡＭＦ２０２は、登録拒否を有するＮＡＳトランスポートメッセージと、５ＧＭＭ原因を含むＥＡＰ失敗のＥＡＰメッセージとを生成する。５ＧＭＭ原因（５ＧＭＭ＿ｃａｕｓｅ）は、エラータイプがＮＯＮ＿３ＧＰＰ＿ＡＣＣＥＳＳ＿ＴＯ＿５ＧＣＮ＿ＮＯＴ＿ＡＬＬＯＷＥＤであることを示している。Ｎ３ＩＷＦ２０４は、５ＧＣＮへの非３ＧＰＰアクセスが許可されていないことを示す５ＧＭＭ原因値を含む登録拒否メッセージをカプセル化したＡＭＦ２０２からのレスポンスを受信する。
【０１１９】
Ｎ３ＩＷＦ２０４は、ＵＥへのレスポンスメッセージを生成し、このレスポンスメッセージは、ステップ１３１０において、信頼されていないネットワークアクセスを介した接続の確立が、コアネットワークによって許可されていないことを示す原因値を含む。例えば、Ｎ３ＩＷＦ２０４は、接続の確立が５ＧＣＮ１００によって承認されないことを示すメッセージタイプまたはＥＡＰ－Ｆａｉｌｕｒｅを含むペイロードと、５ＧＭＭ原因とを有するインターネット鍵交換（ＩＫＥ）レスポンスメッセージを生成する。ＵＥ２００へのＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＮＡＳメッセージには、ＥＡＰ－Ｆａｉｌｕｒｅフィールドと５ＧＭＭ原因とを含む登録拒否メッセージが含まれる。登録拒否メッセージの５ＧＭＭ原因は、非３ＧＰＰアクセスが５ＧＣＮ１００によって許可されないことを示す。
【０１２０】
実施形態では、ＵＥへのＩＫＥレスポンスメッセージは、プライベート通知メッセージタイプ（例えば、８１９２．．．１６３８３などの事前定義された範囲内の任意のプライベート通知メッセージタイプ）を有する通知（Ｎｏｔｉｆｙ）ペイロードを含むＩＫＥ＿ＡＵＴＨレスポンスメッセージを含み得る。プライベートＩＫＥｖ２通知メッセージには、「５ＧＣへの非３ＧＰＰアクセスは許可されない（ＮＯＮ＿３ＧＰＰ＿ＡＣＣＥＳＳ＿ＴＯ＿５ＧＣＮ＿ＮＯＴ＿ＡＬＬＯＷＥＤ）」の５ＧＭＭ原因による登録拒否と、ＥＡＰ－ＦａｉｌｕｒｅのＥＡＰメッセージタイプとを含むＥＡＰレスポンス／５Ｇ－ＮＡＳ　ＰＤＵが含まれる。
【０１２１】
Ｎ３ＩＷＦ２０４は、ストップメッセージを含むＵＥ２００からのレスポンスを処理し、それに応答してＵＥ２００への失敗メッセージを生成する。例えば、ＵＥ２００は、ＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－ＳｔｏｐメッセージをＮ３ＩＷＦ２０４に送信して、５

ＧＣＮ１００との安全なセッション確立のための登録要求の終了を示す。ＥＡＰ－ｒｅｓｐｏｎｓｅパケットには、５Ｇ停止のメッセージタイプ識別子が含まれている。ＵＥ２００からＥＡＰ－Ｒｅｓｐｏｎｓｅ／５Ｇ－Ｓｔｏｐメッセージを受信した後、Ｎ３ＩＷＦ２０４は、ＥＡＰ－Ｆａｉｌｕｒｅメッセージを２００に送信することにより、ＥＡＰ－５Ｇの手順を終了する。Ｎ３ＩＷＦ２０４は、方法１３００でこれらのステップを実行するものとして説明されているが、ＵＥ及びコアネットワークと通信する他のノードまたはモジュールが、本明細書で説明されるステップのうちの１つ以上を行ってもよい。

【０１２２】

図１４は、修復可能なエラーによる認証失敗を伴う、信頼されていないアクセスネットワークを介したコアネットワークへの登録要求の方法１４００の実施形態の論理フロー図を示す。ＵＥ２００は、ステップ１４０２で、非３ＧＰＰアクセスネットワークを介して５ＧＣＮ１００内のインターワーキング機能（Ｎ３ＩＷＦ２０４など）へ通信するように構成される。ＵＥ２００は、１４０４で、非３ＧＰＰアクセスネットワークを介した５ＧＣＮ１００への登録を要求し得る。ＵＥ２００は、１４０６で、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されていないという通知を含むレスポンスメッセージを処理する。ＵＥ２００は、ステップ１４０８において、エラーまたは拒否理由が修復可能であると判定する。ＵＥ２００は、この第２の登録要求におけるパラメータを第１の試行から修正することができる。あるいは、ＵＥは、同じパラメータを用いて後で登録を再試行することを決定することができる。次に、ＵＥ２００は、１４１０で、非３ＧＰＰアクセスネットワークを介して、第２の登録要求を５ＧＣＮ１００に送信する。次に、ＵＥ２００は、ステップ１４１２で、セッションの確立が成功したというレスポンスを処理する。

【０１２３】

図１５は、修復不能なエラーによる認証失敗を伴う、信頼されていないアクセスネットワークを介したコアネットワークへの登録要求の方法１５００の実施形態の論理フロー図を示す。ＵＥ２００は、ステップ１５０２で、非３ＧＰＰアクセスネットワークを介して５ＧＣＮ１００内のインターワーキング機能（Ｎ３ＩＷＦ２０４など）へ通信するように構成される。ＵＥ２００は、１５０４で、非３ＧＰＰアクセスネットワークを介した５ＧＣＮ１００への登録を要求し得る。ＵＥ２００は、１５０６で、５ＧＣＮ１００への非３ＧＰＰアクセスが許可されていないという通知を含むレスポンスメッセージを処理する。ＵＥ２００は、ステップ１５０８において、エラーまたは拒否理由が修復可能ではないと判定する。ＵＥ２００は、ステップ１５１０において、セッションを終了し、ストップメッセージを含むレスポンスを生成する。ＵＥ２００は、ステップ１５１２において、失敗メッセージを受信し、削除手順を実行して、セッションを閉じる。

【０１２４】

図１６は、例示的なユーザ機器２００の実施形態の概略ブロック図を示す。ユーザ機器（ＵＥ）２００は、非３ＧＰＰアクセスネットワーク１１０を介して通信するように動作可能なスマートフォン、スマートタブレット、ラップトップ、スマートウォッチ、ＰＣ、テレビまたは他のデバイスを含み得る。追加または代替の構成要素及び機能が、ＵＥ２００内に含まれてもよい。さらに、本明細書に示す機能及び構成要素のうちの１つ以上は、存在しない場合があり、または他の構成要素もしくは機能と組み合わされない場合がある。

【０１２５】

ＵＥ２００は、ＵＥ２００に関して本明細書で説明される機能のうちの１つ以上を実行するように構成された処理デバイス１６００及びメモリデバイス１６０２を含む。メモリデバイス１６０２は、本明細書で説明される様々な機能を実行するように処理デバイス１６００を制御するアプリケーション及び動作命令を格納する管理対象オブジェクト１６０４を含み得る。ＵＥ２００はまた、ＩＭＳＩの記憶のためのＵＳＩＭ１６０８を含むＵＩＣＣ１６０６を含み得る。他の実施形態では、例えば、ＵＥ２００はＵＩＣＣ１６０６を有さない、ＵＥ２００は動作不能なＵＩＣＣ１６０６を有するなど、ＵＥ２００はＵＩＣＣ機能を有さない。

【０１２６】

ＵＥ２００は、ブルートゥーストランシーバ１６１０、ＷＬＡＮ（ＩＥＥＥ　８０２．１１ｘ準拠）トランシーバ１６１２、モバイルＲＦ（３Ｇ／４Ｇ）トランシーバ１６１４、及びＧＰＳ１６１６をさらに含み得る。ＷＬＡＮトランシーバ１６１２は、ＷＬＡＮネットワークへの非３ＧＰＰアクセスインタフェースとして動作し得る。ＵＥ２００は、ユーザインタフェース１６１８、ＡＣアダプタ１６２０、バッテリモジュール１６２２、ＵＳＢトランシーバ１６２４、及びイーサネットポート１６２８をさらに含み得る。

【０１２７】

ＵＥ２００は、デジタルカメラ１６３０、タッチスクリーンコントローラ１６３２、スピーカ１６３４、及びマイクロフォン１６３６をさらに含み得る。ＵＥ２００はまた、電力管理ユニット１６３８を含み得る。１つ以上の内部通信バス（図示せず）が、ＵＥ２００の構成要素のうちの１つ以上を通信可能に結合し得る。

【０１２８】

図１７は、例示的なＡＭＦ２０２の実施形態の概略ブロック図を示す。ＡＭＦ２０２は、ＡＭＦ２０２の機能性を備えた任意の１つ以上のノードを含む。ＡＭＦ２０２は、５ＧＣＮ１００内の他のノードと統合され得る。追加または代替の構成要素及び機能が、ＡＭＦ２０２内に含まれてもよい。さらに、本明細書に示す機能及び構成要素のうちの１つ以上は、存在しない場合があり、あるいは他の構成要素または機能もしくはノードと組み合わされない場合がある。ＡＭＦ２０２は、ＡＭＦ２０２に関して本明細書で説明される機能のうちの１つ以上を実行するように構成された処理デバイス１７００及びメモリデバイス１７０２を含む。ＡＭＦ２０２は、５ＧＣＮ１００内の他のネットワークノードとインタフェースするためのポートを含むネットワークインタフェース１７０４を含み得る。

【０１２９】

図１８は、例示的なＮ３ＩＷＦ２０４の実施形態の概略ブロック図を示す。Ｎ３ＩＷＦ２０４は、ワイヤレスローカルエリアネットワーク内のアクセスポイント、ローカルエリアネットワーク内のゲートウェイ、または本明細書で説明されるインターワーキング機能を含む他のタイプのノードであり得る。Ｎ３ＩＷＦ２０４は、アクセスネットワークまたは５ＧＣＮ１００内の他のノードと統合させてもよい。追加または代替の構成要素及び機能が、Ｎ３ＩＷＦ２０４内に含まれてもよい。さらに、本明細書に示す機能及び構成要素のうちの１つ以上は、存在しない場合があり、または他の構成要素もしくは機能と組み合わされない場合がある。

【０１３０】

Ｎ３ＩＷＦ２０４は、本明細書で説明される機能のうちの１つ以上を実行するように構成された処理デバイス１８００及びメモリデバイス１８０２を含む。Ｎ３ＩＷＦ２０４は、５ＧＣＮ１００内の他のネットワークノードとインタフェースするための第１のネットワークインタフェース１８０４（例えば、イーサネットポート、ＩＰポート）を含み得る。Ｎ３ＩＷＦ２０４はまた、ＷＬＡＮトランシーバ１８０６（例えば、ＩＥＥＥ　８０２．１ｘ　ＷＬＡＮタイプのネットワークに準拠）など、ＵＥと通信するための１つ以上の他のタイプのインタフェースを含み得る。Ｎ３ＩＷＦ２０４はまた、セルラエアインタフェースに準拠したモバイルＲＦトランシーバ１８０８を含み得る。ＵＥ２００は、ＷＬＡＮトランシーバ１８０６またはモバイルＲＦトランシーバ１８０８のうちの１つ以上を使用して、Ｎ３ＩＷＦ２０４と通信し得る。

【０１３１】

実施形態では、処理デバイスは、信頼されていない非３ＧＰＰアクセスネットワークを介してＵＥ２００からＩＰｓｅｃセキュリティアソシエーション（ＳＡ）要求を受信し、ＩＫＥプロトコルなど、信頼されていない非３ＧＰＰアクセスネットワーク内のＵＥ２００の認証プロトコルを実行するように構成される。次に、Ｎ３ＩＷＦ２０４は、ＩＰｓｅｃ　ＳＡ要求がコアネットワークによって承認されないことを示す認証レスポンスを取得することができる。その後、Ｎ３ＩＷＦ２０４は、ＵＥ２００への認証レスポンスを生成することができ、この認証レスポンスは、信頼されていないアクセスネットワークを介したＵＥ２００によるコアネットワークへのアクセスが拒否されることを示す。

【０１３２】
本明細書に記載の処理デバイスは、マイクロプロセッサ、マイクロコントローラ、デジタルシグナルプロセッサ、マイクロコンピュータ、中央処理装置、フィールドプログラマブルゲートアレイ、プログラマブルロジックデバイス、ステートマシン、ロジック回路、アナログ回路、デジタル回路、及び／または回路のハードコーディング及び／または動作命令に基づいて信号（アナログ及び／またはデジタル）を操作する任意のデバイスなどの少なくとも１つの処理デバイスを含む。メモリデバイスは、非一時的メモリデバイスであり、内部メモリまたは外部メモリであり得、メモリは、単一のメモリデバイスまたは複数のメモリデバイスであり得る。メモリデバイスは、読み出し専用メモリ、ランダムアクセスメモリ、揮発性メモリ、不揮発性メモリ、静的メモリ、動的メモリ、フラッシュメモリ、キャッシュメモリ、及び／またはデジタル情報を格納する任意の非一時的メモリデバイスであり得る。用語「モジュール」は、本明細書の要素の１つ以上の実施形態の説明で使用される。モジュールは、本明細書で説明され得るように、１つ以上の機能を実行するように動作可能な１つ以上の処理デバイス及び／または１つ以上の非一時的メモリデバイスを含む。モジュールは、独立して及び／または他のモジュールと組み合わせて動作し得、他のモジュールの処理デバイス及び／またはメモリ及び／または他のモジュールの動作命令を利用し得る。本明細書でも使用されるように、モジュールは、１つ以上のサブモジュールを含み得、そのそれぞれは、１つ以上のモジュールであり得る。

【０１３３】
本明細書で使用され得るように、「動作可能な」または「構成可能な」という用語は、要素が、記載された、または必要な対応する機能のうちの１つ以上を実行するための回路、命令、モジュール、データ、入力（複数可）、出力（複数可）などのうちの１つ以上を含むことを示し、記載された、または必要な対応する機能を実行するために、１つ以上の他のアイテムへの推論的結合をさらに含み得る。本明細書でも使用されることがあるように、用語（複数可）「結合された」、「～に結合された」、「～に接続された」及び／または「接続している」または「相互に接続される」は、ノード／デバイス間の直接的な接続またはリンク、及び／またはノード／デバイス間の間接的な接続を、介在するアイテム（例えば、アイテムは、構成要素、要素、回路、モジュール、ノード、デバイス、ネットワーク要素などを含むが、これらに限定されない）を介して含む。本明細書でさらに使用され得るように、推論的接続（すなわち、１つの要素が推論によって別の要素に接続されている場合）は、「接続されている」と同様に、２つのアイテム間の直接的及び間接的な接続を含む。

【０１３４】
本開示の態様は、本明細書では、概略図、フローチャート、流れ図、構造図、またはブロック図として示されるプロセスとして説明され得ることに留意されたい。フローチャートは動作を順序プロセスとして説明する場合があるが、動作の多くは並行してまたは同時に実行することができる。さらに、動作の順序を再整理する場合がある。プロセスは、その動作が完了した時点で終了する。プロセスは、方法、関数、プロシージャ、サブルーチン、サブプログラムなどに対応し得る。プロセスが関数に対応する場合、その終了は、呼び出し元の関数、またはメイン関数への関数の戻りに対応する。

【０１３５】
本明細書に記載された本開示の様々な特徴は、本開示から逸脱することなく、様々なシステム及びデバイスに実装することができる。本開示の上記の態様は単なる例にすぎず、本開示を限定するものとして解釈されるべきではないことに留意すべきである。本開示の態様の説明は、例示を意図するものであり、特許請求の範囲を限定するものではない。したがって、本教示は、他のタイプの装置に容易に適用することができ、多くの代替、修正、及び変形が当業者には明らかであろう。

【０１３６】
上記の明細書では、本発明の特定の代表的な態様が、特定の例を参照して説明されている。しかしながら、特許請求の範囲に記載されている本発明の範囲から逸脱することなく

、様々な修正及び変更を行い得る。本明細書及び図は、限定的ではなく例示的なものであり、修正は、本発明の範囲内に含まれることが意図されている。したがって、本発明の範囲は、単に記載された例によってではなく、特許請求の範囲及びそれらの法的同等物によって決定されるべきである。例えば、任意の装置請求項に記載された構成要素及び／または要素は、組み立てられ得、または別の方法で、様々な組み合わせで作動的に構成され得、したがって、請求項に記載された特定の構成に限定されない。

【０１３７】

さらに、特定の実施形態に関して、特定の利益、他の利点、及び問題に対する解決策が上記で説明されているが、任意の特定の利益、利点、問題に対する解決策、あるいは任意の特定の利益、利点、または解決策を発生させる、もしくはより顕著になる可能性のある要素は、請求項のいずれかまたは全ての特許請求の範囲の重要な、必須の、または本質的な特徴もしくは構成要素として解釈されるべきではない。

【０１３８】

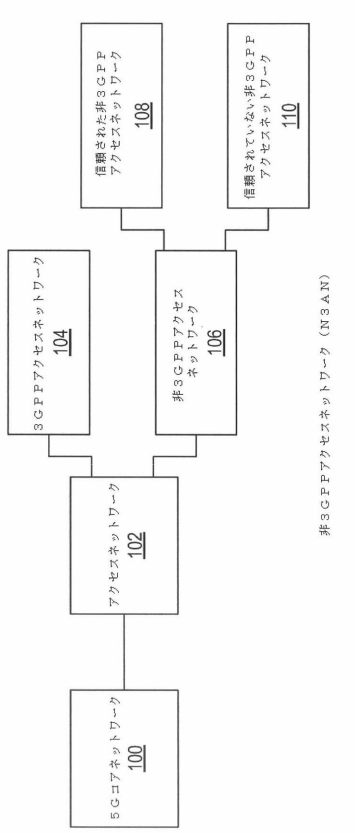
本明細書で使用するとき、用語「備える（ｃｏｍｐｒｉｓｅ）」、「備える（ｃｏｍｐｒｉｓｅｓ）」、「備えている（ｃｏｍｐｒｉｓｉｎｇ）」、「有している（ｈａｖｉｎｇ）」、「含んでいる（ｉｎｃｌｕｄｉｎｇ）」、「含む（ｉｎｃｌｕｄｅｓ）」またはそれらの任意の変形は、要素のリストを構成するプロセス、方法、成形品、組成物または装置が、引用された要素のみを含むのではなく、明示的にリストされていない他の要素またはそのようなプロセス、方法、成形品、組成物もしくは装置に固有の要素を含むことができるように、非排他的な包含を参照することを意図している。本発明の実施において使用される上記の構造、配置、用途、割合、要素、材料、または構成要素の他の組み合わせ及び／または変更は、特に言及されていないものに加えて、同様の一般原則から逸脱することなく、特定の環境、製造仕様、設計パラメータ、または他の動作要件に変化させるか、または別の方法で特別に適合させることができる。

【０１３９】

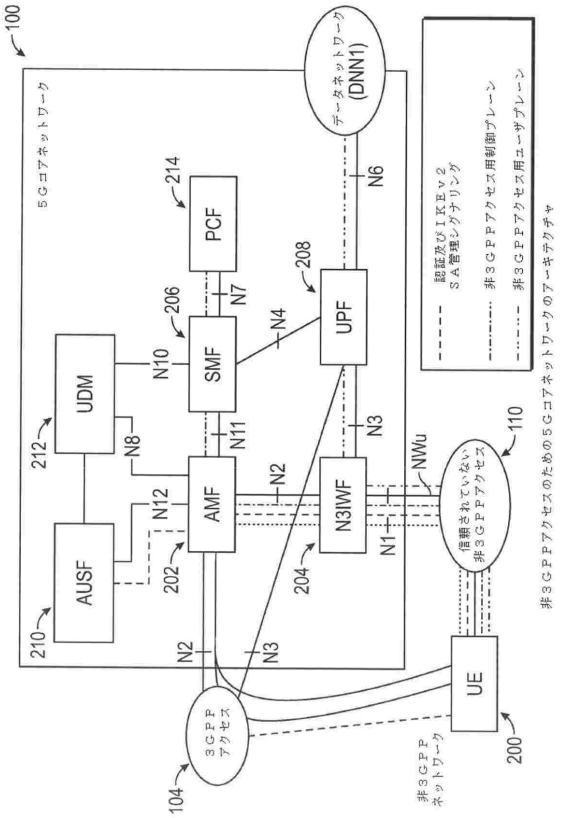
さらに、単数形の要素への言及は、特に明記されていない限り、「１つだけ（ｏｎｅ　ａｎｄ　ｏｎｌｙ　ｏｎｅ）」を意味するのではなく、「１つ以上（ｏｎｅ　ｏｒ　ｍｏｒｅ）」を意味することが意図されている。特に明記されていない限り、「一部」という用語は、１つまたは複数のものを指す。当業者に知られている、または後に知られるようになる、本開示を通して記載された様々な態様の要素に対する全ての構造的及び機能的均等物は、参照により本明細書に明示的に組み込まれ、特許請求の範囲に包含されることが意図されている。さらに、本明細書に開示されているものは、そのような開示が特許請求の範囲に明示的に記載されているかどうかにかかわらず、公衆に提供されることを意図していない。いかなる特許請求の要素も、その要素が明示的に「手段」（ｍｅａｎｓ　ｆｏｒ）という語句を用いて記載されているか、または方法クレームの場合には、その要素が「ステップ」（ｓｔｅｐ　ｆｏｒ）という語句を用いて記載されているかでない限り、米国特許法第１１２条（ｆ）の定めにより、「ミーンズプラスファンクション」（ｍｅａｎｓ－ｐｌｕｓ－ｆｕｎｃｔｉｏｎ）タイプの要素として解釈されることを意図していない。

【図面】

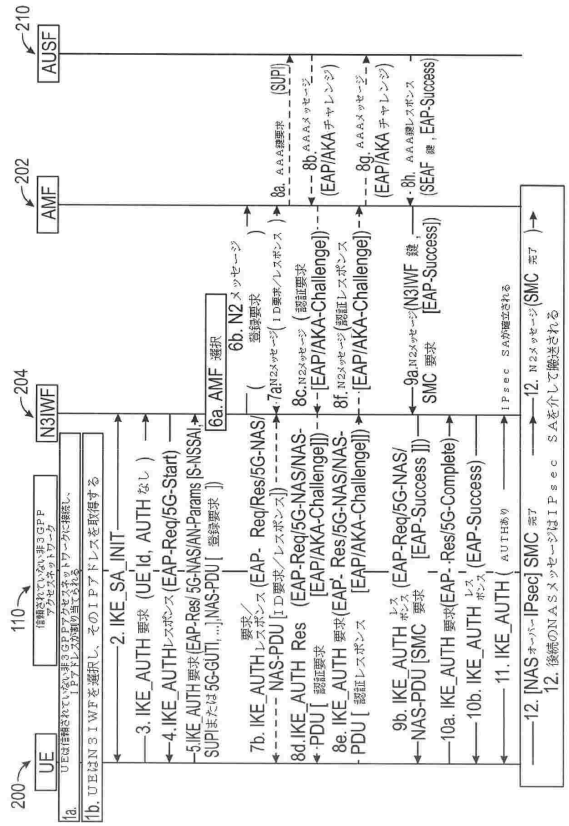
【図１】


信頼された非３ＧＰＰアクセスネットワーク
108
信頼されていない非３ＧＰＰアクセスネットワーク
110
３ＧＰＰアクセスネットワーク
104
非３ＧＰＰアクセスネットワーク
106
アクセスネットワーク
102
５Ｇコアネットワーク
100
非３ＧＰＰアクセスネットワーク（Ｎ３ＡＮ）

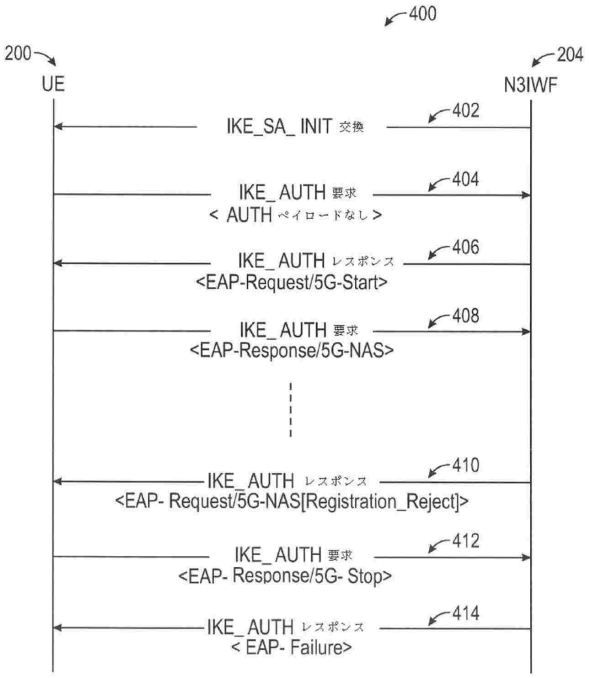
【図２】


100
５Ｇコアネットワーク
データネットワーク
(DNN1)
N6
214
PCF
N7
208
UPF
206
SMF
N4
N10
212
UDM
N8
N11
N3
NWu
110
信頼されていない非３ＧＰＰアクセス
N2
AMF
N12
N1
N3IWF
202
204
AUSF
210
N2
N3
UE
200
３ＧＰＰアクセス
104
非３ＧＰＰネットワーク
認証及びＩＫＥｖ２ＳＡ管理シグナリング
非３ＧＰＰアクセス用制御プレーン
非３ＧＰＰアクセス用ユーザプレーン
非３ＧＰＰアクセスのための５Ｇコアネットワークのアーキテクチャ

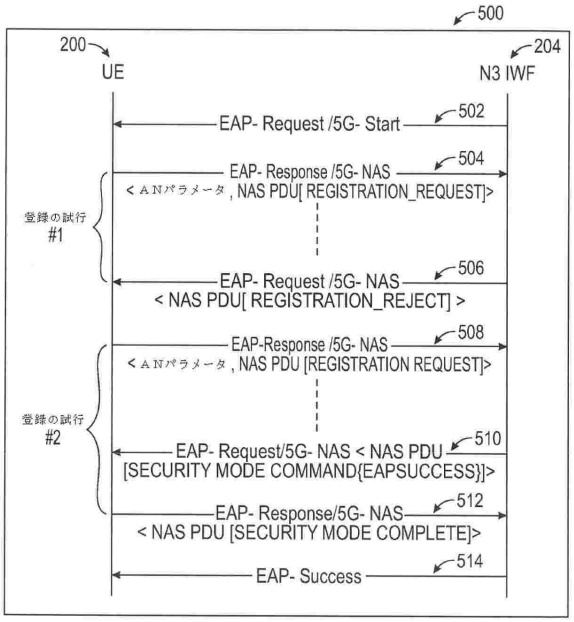
【図３】


210
AUSF
202
AMF
204
N3IWF
110
信頼されていない非３GPPアクセスネットワークに接続。IPアドレスが割り当てられる
200
UE
1a. UEはN3IWFを選択し、そのIPアドレスを取得する
1b.
2. IKE_SA_INIT
3. IKE_AUTH 要求 (UE Id, AUTH なし)
4. IKE_AUTH レスポンス (EAP-Req/5G-Start)
5.IKE_AUTH要求 (EAP-Res/ 5G-NAS/AN-Params [S-NSSAI, SUPIまたは5G-GUTI,...],NAS-PDU [登録要求])
6a. AMF 選択
6b. N2 メッセージ (登録要求)
7a.N2メッセージ (ID要求レスポンス)
7b. IKE_AUTH 要求/レスポンス (EAP- Req/Res/5G-NAS/ NAS-PDU [ID要求/レスポンス])
8a. AAA要求 ... [SUPI]
8b. AAAメッセージ (EAP/AKAチャレンジ)
8c.N2メッセージ (認証要求 [EAP/AKA-Challenge])
8d.IKE_AUTH Res (EAP-Req/5G-NAS/NAS-PDU [認証要求 [EAP/AKA-Challenge]])
8e. IKE_AUTH 要求(EAP- Res/5G-NAS/NAS-PDU [認証レスポンス [EAP/AKA-Challenge]])
8f. N2メッセージ(認証レスポンス [EAP/AKA-Challenge])
8g. AAAメッセージ (EAP/AKA チャレンジ)
8h. AAA確立レスポンス (SEAF 鍵, EAP-Success)
9a.N2メッセージ(N3IWF 鍵, SMC 要求 [EAP-Success])
9b. IKE_AUTH レスポンス (EAP-Req/5G-NAS/ NAS-PDU [SMC 要求 [EAP-Success]])
10a. IKE_AUTH 要求(EAP- -Res/5G-Complete)
10b. IKE_AUTH レスポンス (EAP-Success)
11. IKE_AUTH (AUTH あり)
IPsec SA が確立される
12. [NASキー, IPsec] SMC 完了
12. N2メッセージ(SMC 完了)
12. 後続のNASメッセージはIPsec SAを介して搬送される

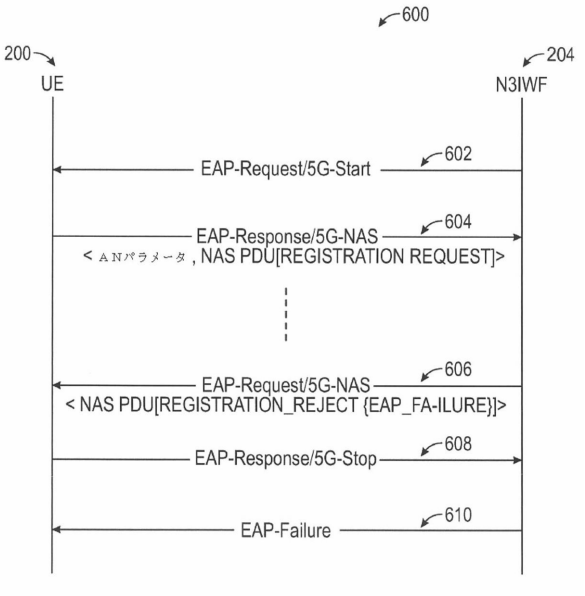
【図４】


400
200
UE
204
N3IWF
IKE_SA_ INIT 交換
402
IKE_ AUTH 要求
< AUTH ペイロードなし >
404
IKE_ AUTH レスポンス
<EAP-Request/5G-Start>
406
IKE_ AUTH 要求
<EAP-Response/5G-NAS>
408
IKE_ AUTH レスポンス
<EAP- Request/5G-NAS[Registration_Reject]>
410
IKE_ AUTH 要求
<EAP- Response/5G- Stop>
412
IKE_ AUTH レスポンス
< EAP- Failure>
414

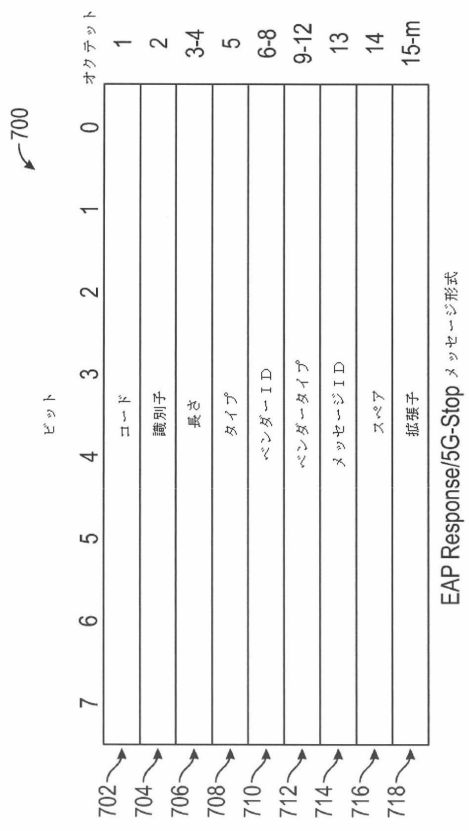
【図５】


500
200
UE
204
N3 IWF
EAP- Request /5G- Start
502
EAP- Response /5G- NAS
504
< ANパラメータ , NAS PDU[REGISTRATION_REQUEST]>
登録の試行 #1
EAP- Request /5G- NAS
506
< NAS PDU[REGISTRATION_REJECT] >
EAP-Response /5G- NAS
508
< ANパラメータ , NAS PDU [REGISTRATION REQUEST]>
登録の試行 #2
EAP- Request/5G- NAS < NAS PDU
510
[SECURITY MODE COMMAND{EAPSUCCESS}]>
EAP- Response/5G- NAS
512
< NAS PDU [SECURITY MODE COMPLETE]>
EAP- Success
514

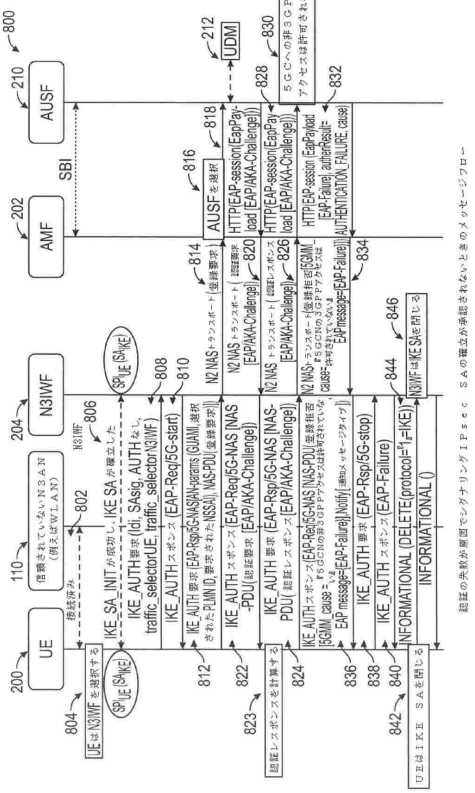
【図６】


600
200
UE
204
N3IWF
EAP-Request/5G-Start
602
EAP-Response/5G-NAS
604
< ANパラメータ , NAS PDU[REGISTRATION REQUEST]>
EAP-Request/5G-NAS
606
< NAS PDU[REGISTRATION_REJECT {EAP_FA-ILURE}]>
EAP-Response/5G-Stop
608
EAP-Failure
610

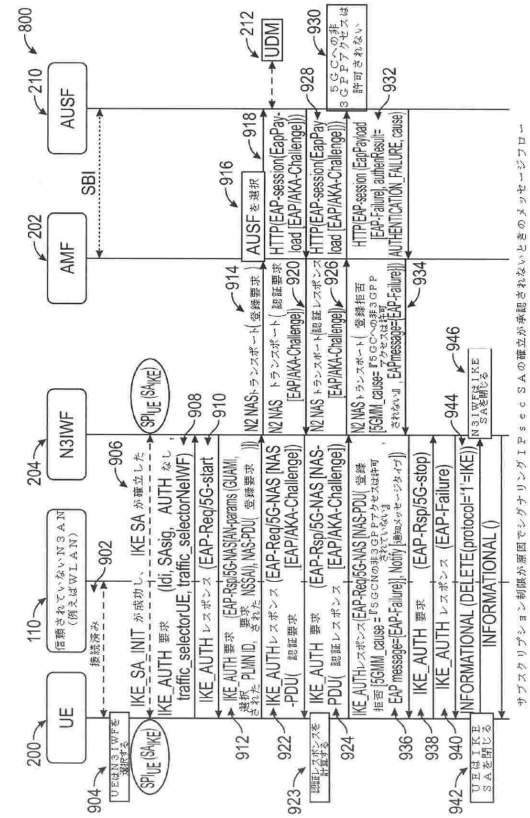
【図７】


700
ビット
オクテット
1
2
3-4
5
6-8
9-12
13
14
15-m
0
1
2
3
4
5
6
7
コード
識別子
長さ
タイプ
ベンダーＩＤ
ベンダータイプ
メッセージＩＤ
スペア
拡張子
EAP Response/5G-Stop メッセージ形式
702
704
706
708
710
712
714
716
718

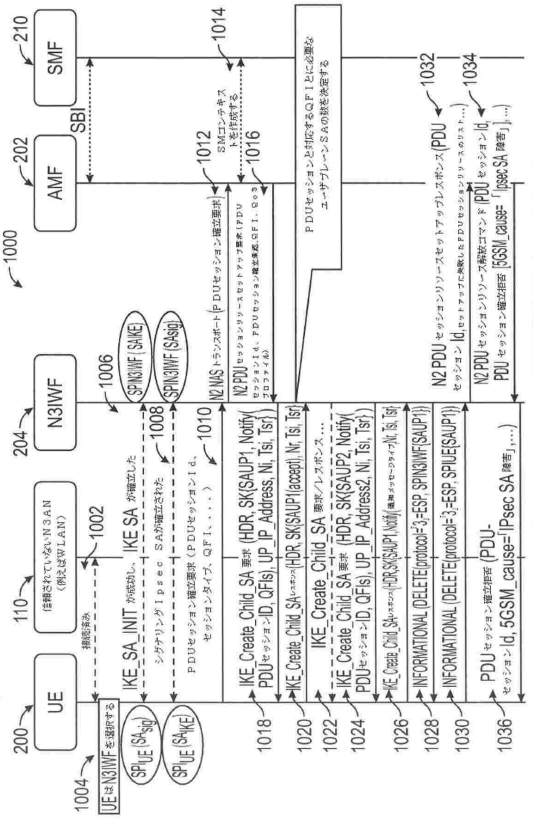
【図８】


800
210
AUSF
212
UDM
SBI
202
AMF
204
N3IWF
200
UE
110
信頼されていないN3AN（非3GPPアクセスN3AN）
802
806
808
810
812
814
816
818
820
822
823
824
826
828
830
832
834
836
838
840
842
844
846
IKE_SA_INIT が成功し、IKE SA が確立した
IKE_AUTH 要求 [idi, SAsig, AUTH など, traffic_selectorUE, traffic_selectorN3IWF]
IKE_AUTH レスポンス [EAP-Req/5G-start]
IKE_AUTH 要求 [EAP-Rsp(5G-NAS(PA-reserns (GUAMI,選択された PLMN ID, 要求された NSSAI), NAS-PDU (登録要求))]
N2 NAS トランスポート [登録要求]
HTTP(EAP-session(EapPayload [EAP/AKA-Challenge]))
IKE_AUTH レスポンス [EAP-Req/5G-NAS (NAS-PDU [EAP/AKA-Challenge])]
IKE_AUTH 要求 [EAP-Rsp/5G-NAS (NAS-PDU [認証レスポンス [EAP/AKA-Challenge]])]
N2 NAS トランスポート [認証レスポンス [EAP/AKA-Challenge]]
HTTP(EAP-session (EapPayload [EAP-Failure], authenResult= AUTHENTICATION_FAILURE cause))
IKE_AUTH レスポンス [EAP-Req(5GMM_cause = 5GCへの非3GPPアクセスは許可されていない EAP message=[EAP-Failure])]
N2 NAS トランスポート [登録拒否(5GMM_cause= 5GCへの非3GPPアクセスは許可されていない) EAP message=[EAP-Failure]]
IKE_AUTH 要求 [EAP-Rsp/5G-stop)]
IKE_AUTH レスポンス [EAP-Failure]
INFORMATIONAL (DELETE[protocol=1, =IKE])
INFORMATIONAL ()
5GCへの非3GPPアクセスは許可されない
AUSFを選択
UEはN3IWFを選択する
SPI UE (SMc)
SPI UE (SMc)
N3IWF
認証レスポンスを計算する
UEはIKE SAを閉じる
N3IWFはIKE SAを閉じる
認証の失敗が原因でシグナリングIPsec SAの確立が承認されないときのメッセージフロー

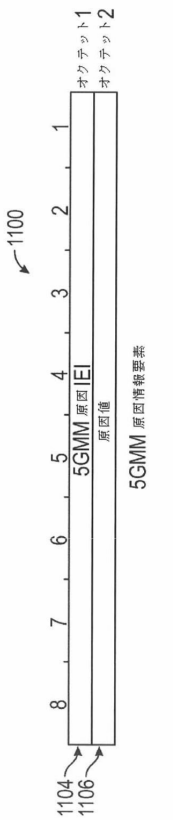
【図９】



【図１０】



【図１１】



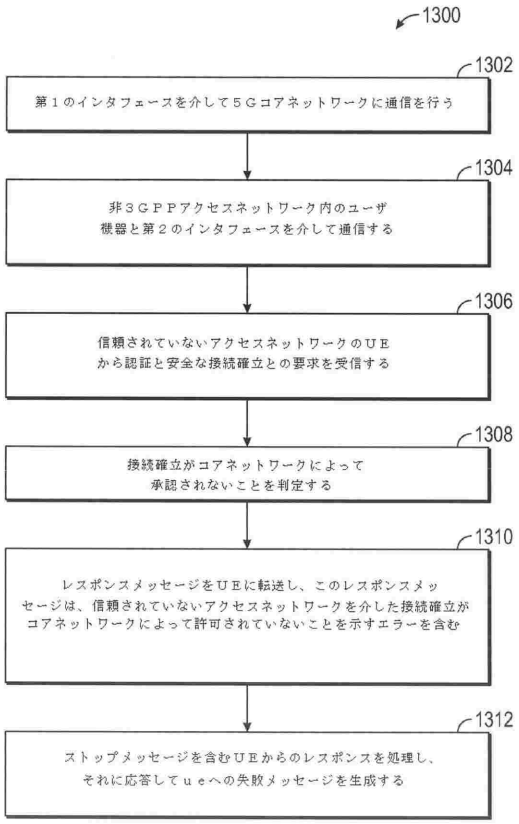
【図１２】

原因値（オクテット2）	
ビット 8 7 6 5 4 3 2 1	
0 1 0 0 0 0 1 1	....
0 1 0 0 0 1 0 1	....
0 1 0 0 0 1 1 1	....
0 1 0 0 1 0 0 0	５ＧＣＮへの非３ＧＰＰアクセスは許可されていない
0 1 0 0 1 0 0 1	....
0 1 0 1 0 1 1 0	....

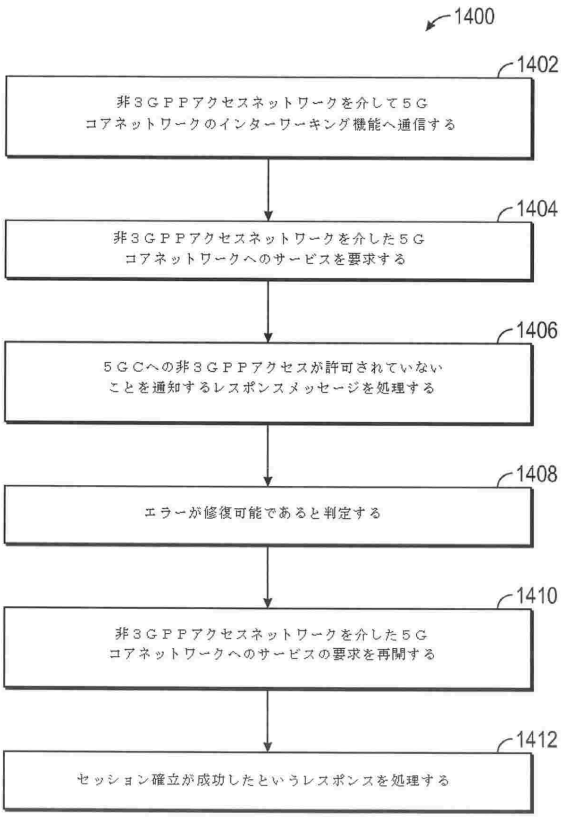
移動局が受信した他の何らかの値は、０１１０　１１１１、「プロトコルエラー、詳細不明」として扱われる。ネットワークが受信した他の何らかの値は、０１１０　１１１１、「プロトコルエラー、詳細不明」として扱われる。

5GMM 原因情報要素の値

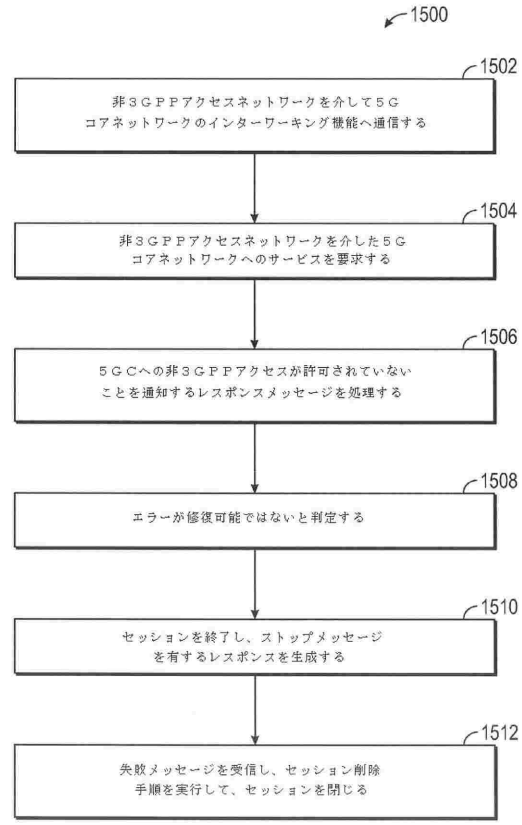
【図１３】



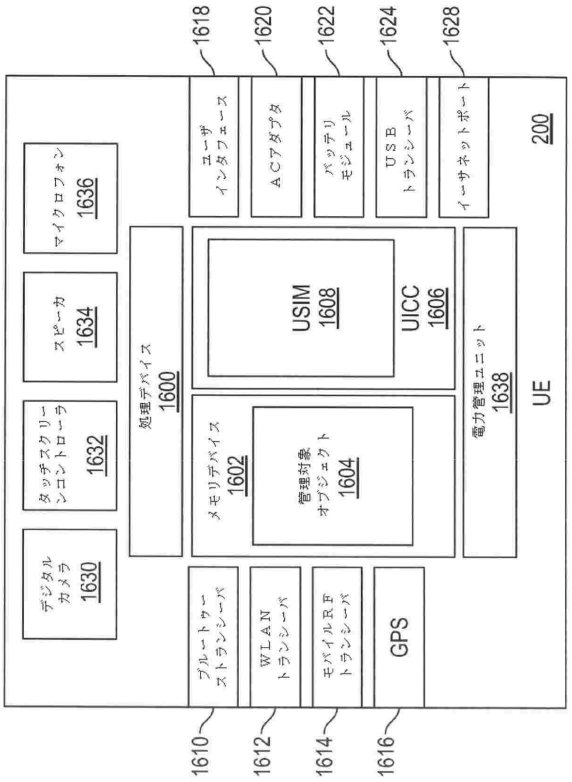
【図１４】



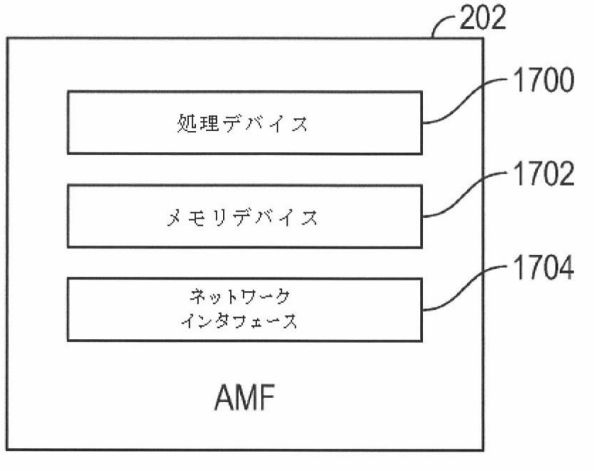
【図１５】



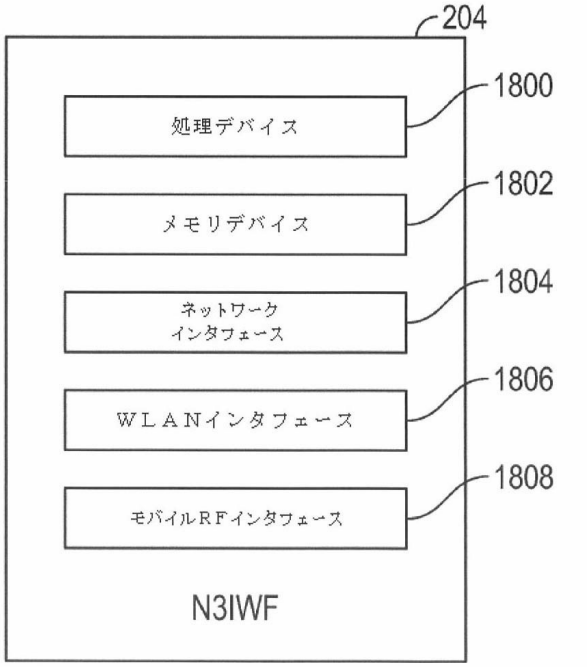
【図１６】



【図１７】


202
1700
処理デバイス
1702
メモリデバイス
1704
ネットワーク
インタフェース
AMF

【図１８】


204
1800
処理デバイス
1802
メモリデバイス
1804
ネットワーク
インタフェース
1806
ＷＬＡＮインタフェース
1808
モバイルＲＦインタフェース
N3IWF

フロントページの続き

(72)発明者　リウ，ジェニファー
アメリカ合衆国，テキサス州　７５０２５，プラノ，３１０４　オーク　スプリングス　ドライブ

審査官　米倉　明日香

(56)参考文献　Motorola Mobility, Lenovo, Broadcom, Brocade, Rogers Wireless, Samsung, ITRI, CMCC, CATT, Cisco, NEC，Details of EAP-5G Solution for registration via untrusted non-3GPP access，3GPP TSG SA WG3 #88Bis S3-172511，2017年10月13日
Nokia，Observations on the solution for untrusted non-3GPP access in S2-174885，3GPP TSG SA WG3 #88 S3-171943，2017年07月31日
Samsung R & D Institute UK, Nokia, Nokia Shanghai Bell, Intel，Change "N1 mode radio capability" to "N1 mode capability for 3GPP access"，3GPP TSG CT WG1 #111 C1-183524，2018年05月28日

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　７／２４－　７／２６
Ｈ０４Ｗ　４／００－９９／００
３ＧＰＰ　ＴＳＧ　ＲＡＮ　ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１、４