(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6775683号
(P6775683)
(45)発行日　令和2年10月28日(2020.10.28)　(24)登録日　令和2年10月8日(2020.10.8)

(51)Int.Cl.　F I
H04W 12/06 (2009.01)　H04W 12/06
G06F 21/44 (2013.01)　G06F 21/44

請求項の数 17　(全 19 頁)

(21)出願番号　特願2019-521802(P2019-521802)
(86)(22)出願日　平成29年10月25日(2017.10.25)
(65)公表番号　特表2019-533951(P2019-533951A)
(43)公表日　令和1年11月21日(2019.11.21)
(86)国際出願番号　PCT/EP2017/077330
(87)国際公開番号　WO2018/077960
(87)国際公開日　平成30年5月3日(2018.5.3)
審査請求日　令和1年7月12日(2019.7.12)
(31)優先権主張番号　62/415,006
(32)優先日　平成28年10月31日(2016.10.31)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エルエム　エリクソン（パブル）
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100109726
弁理士　園田　吉隆
(74)代理人　100161470
弁理士　冨樫　義孝
(74)代理人　100194294
弁理士　石岡　利康
(74)代理人　100194320
弁理士　藤井　亮

最終頁に続く

(54)【発明の名称】次世代システムの認証

(57)【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、ネットワークにおける２次認証のための方法であって、
セキュリティアンカー機能（ＳＥＡＦ）との１次認証を確立すること（１００）と、
ユーザプレーン（ＵＰ）機能（ＵＰＦ）との、または前記ＵＰＦを介するユーザプレーン（ＵＰ）セッションまたは接続を確立すること（１１０）と、
前記ＵＰＦを介して拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信すること（１３０）と、
ＥＡＰベースの認証応答を前記ＵＰＦに送信すること（１４０）と、
ＥＡＰベースの認証結果を前記ＵＰＦを介して受信することであって、前記ＥＡＰベースの認証結果は、サードパーティドメインの認証、認可、アカウンティング（ＡＡＡ）サーバからの検証応答に基づく、受信することとを備える方法。
【請求項２】
前記ユーザ機器（ＵＥ）は次世代（ＮＧ）ＵＥである、請求項１に記載の方法。
【請求項３】
前記ユーザプレーン機能（ＵＰＦ）は次世代（ＮＧ）ＵＰＦである、請求項１に記載の方法。
【請求項４】
前記ＳＥＡＦは、認証サーバ機能（ＡＵＳＦ）にさらに接続される、請求項１に記載の

方法。
【請求項５】
ユーザプレーン（ＵＰ）機能（ＵＰＦ）によって実行される、ネットワークにおける２次認証のための方法であって、
ユーザ機器（ＵＥ）へのＵＰセッションまたは接続を確立すること（１１０）と、
拡張認証プロトコル（ＥＡＰ）ベースの認証要求を前記ＵＥに送信すること（１２０）と、
ＥＡＰベースの認証応答を前記ＵＥから受信すること（１５０）と、
前記受信されたＥＡＰベースの認証応答の検証要求を、サードパーティドメインの認証、認可、アカウンティング（ＡＡＡ）サーバに送信すること（１６０）と、
前記ＡＡＡサーバから検証応答を受信すること（１７０）と、
認証結果を前記ＵＥに送信することであって、前記認証は前記ＡＡＡサーバからの前記検証応答に基づくこととを備える方法。
【請求項６】
前記ユーザ機器（ＵＥ）は次世代（ＮＧ）ユーザ機器（ＵＥ）である、請求項５に記載の方法。
【請求項７】
前記ユーザプレーン機能（ＵＰＦ）は次世代（ＮＧ）ＵＰＦである、請求項５に記載の方法。
【請求項８】
ネットワークにおける動作のためのユーザ機器（ＵＥ）であって、
プロセッサ（１０）と、
前記プロセッサによって実行されるとき、前記ＵＥに、
セキュリティアンカー機能（ＳＥＡＦ）との１次認証を確立すること（１００）と、
ユーザプレーン（ＵＰ）機能（ＵＰＦ）との、または前記ＵＰＦを介するユーザプレーン（ＵＰ）セッションまたは接続を確立すること（１１０）と、
前記ＵＰＦを介して拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信すること（１３０）と、
ＥＡＰベースの認証応答を前記ＵＰＦに送信すること（１４０）と、
ＥＡＰベースの認証結果を前記ＵＰＦを介して受信することであって、前記ＥＡＰベースの認証結果は、サードパーティドメインの認証、認可、アカウンティング（ＡＡＡ）サーバからの検証応答に基づく、受信することとを行わせる命令を格納するコンピュータプログラム製品（１２、１３）とを備えるＵＥ。
【請求項９】
前記ユーザ機器（ＵＥ）は次世代（ＮＧ）ＵＥである、請求項８に記載のＵＥ。
【請求項１０】
前記ＵＰＦは次世代（ＮＧ）ＵＰＦである、請求項８に記載のユーザ機器（ＵＥ）。
【請求項１１】
前記ＳＥＡＦは、認証サーバ機能（ＡＵＳＦ）にさらに接続される、請求項８に記載のユーザ機器（ＵＥ）。
【請求項１２】
ネットワークにおいて動作可能なユーザプレーン（ＵＰ）機能（ＵＰＦ）であって、
プロセッサ（１０）と、
前記プロセッサによって実行されるとき、前記ＵＰＦに、
ユーザ機器（ＵＥ）とのＵＰセッションまたは接続を確立すること（１１０）と、
拡張認証プロトコル（ＥＡＰ）ベースの認証要求を前記ＵＥに送信すること（１２０）と、
ＥＡＰベースの認証応答を前記ＵＥから受信すること（１５０）と、
前記受信されたＥＡＰベースの認証応答の検証要求を、サードパーティドメインの認証、認可、アカウンティング（ＡＡＡ）サーバに送信すること（１６０）と、

前記ＡＡＡサーバから検証応答を受信すること（１７０）と、
認証結果を前記ＵＥに送信することであって、前記認証は前記ＡＡＡサーバからの前記検証応答に基づくこととを行わせる命令を格納するコンピュータプログラム製品（１２、１３）とを備えるＵＰＦ。
【請求項１３】
前記ＵＰＦは次世代（ＮＧ）ＵＰＦである、請求項１２に記載のＵＰＦ。
【請求項１４】
前記ＵＥは次世代（ＮＧ）ＵＥである、請求項１２に記載のＵＰＦ。
【請求項１５】
ネットワークにおける２次認証のためのコンピュータプログラム（１４、１５）であって、ユーザ機器（ＵＥ）において実行されるとき、前記ＵＥに、
セキュリティアンカー機能（ＳＥＡＦ）との１次認証を確立すること（１００）と、
ユーザプレーン（ＵＰ）機能（ＵＰＦ）との、または前記ＵＰＦを介するユーザプレーン（ＵＰ）セッションまたは接続を確立すること（１１０）と、
前記ＵＰＦを介して拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信すること（１３０）と、
ＥＡＰベースの認証応答を前記ＵＰＦに送信すること（１４０）と、
ＥＡＰベースの認証結果を前記ＵＰＦを介して受信することであって、前記ＥＡＰベースの認証結果は、サードパーティドメインの認証、認可、アカウンティング（ＡＡＡ）サーバからの検証応答に基づく、受信することとを行わせるコンピュータプログラムコードを備えるコンピュータプログラム。
【請求項１６】
ネットワークにおける２次認証のためのコンピュータプログラム（１４、１５）であって、ユーザプレーン（ＵＰ）機能（ＵＰＦ）において実行されるとき、前記ＵＰＦに、
ユーザ機器（ＵＥ）へのユーザプレーン（ＵＰ）セッションまたは接続を確立すること（１１０）と、
拡張認証プロトコル（ＥＡＰ）ベースの認証要求を前記ＵＥに送信すること（１２０）と、
ＥＡＰベースの認証応答を前記ＵＥから受信すること（１５０）と、
前記受信されたＥＡＰベースの認証応答の検証要求を、サードパーティドメインの認証、認可、アカウンティング（ＡＡＡ）サーバに送信すること（１６０）と、
前記ＡＡＡサーバから検証応答を受信すること（１７０）と、
認証結果を前記ＵＥに送信することであって、前記認証は前記ＡＡＡサーバからの前記検証応答に基づくこととを行わせるコンピュータプログラムコードを備えるコンピュータプログラム。
【請求項１７】
請求項１５または１６のいずれか一項に記載のコンピュータプログラム（１４、１５）と、前記コンピュータプログラム（１４、１５）が格納されているコンピュータ可読ストレージ手段とを備えるコンピュータプログラム製品（１２、１３）。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、ネットワークにおける２次認証のための方法および装置に関する。
【背景技術】
【０００２】
３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ（第３世代移動体通信システム標準化プロジェクト）（３ＧＰＰ）は現在、次世代（ＮＧ）システムとも称される、５Ｇの標準を開発している。５Ｇが多くの新しいシナリオおよびユースケースをサポートすること、およびモノのインターネット（ＩｏＴ）のイネーブラーとなることが期待されている。ＮＧシステムが、センサー、スマートウェアラブル、車両、機械

などのような広範にわたる新しいデバイスに接続をもたらすことが期待されている。したがって、柔軟性はＮＧシステムにおいて重要な特性である。これは、オペレータによって事前プロビジョンされ、ユニバーサル集積回路カード（ＵＩＣＣ）に安全に格納されている通常の認証および鍵合意（ＡＫＡ）資格情報と比較して、代替の認証方法およびさまざまなタイプの資格情報のサポートを義務づけるネットワークアクセスのセキュリティ要件に反映されている。これにより、工場所有者または企業は、認証およびアクセスネットワークセキュリティのために各自の識別および資格情報管理システムを活用できるようになる。

【０００３】

ＮＧシステムの新しい機能の中には、ネットワークスライシングの概念がある。ネットワークスライス（ＮＳ）は、基本的に、特定のサービスを提供することに専用のコアネットワークのインスタンスである。これにより、オペレータは、サービス品質（ＱｏＳ）に関して各々がさまざまなサービス要件を備える、多種多様な新しいユースケースを処理することができるようになる。たとえば、オペレータは、非常に低いレイテンシを必要とする（ミッションクリティカルプッシュツートーク（ＭＣＰＴＴ）のような）公共安全サービスのためのミッションクリティカルＮＳと並行して、さらには非常に低い帯域幅を伴う電気メーターのためのＩｏＴ　ＮＳと並行して、通常のモバイルブロードバンド（ＭＢＢ）サービスのためにＮＳを実行していることもある。

【０００４】

ネットワークスライシングに関連して研究されているトピックの中には、異なるＮＳにアクセスするための認証および認可の手順の分離がある。

【発明の概要】

【０００５】

本明細書において提示される実施形態の目的は、次世代システムにおいて認証の分離を可能にすることである。

【０００６】

第１の態様によれば、ネットワークにおける２次認証のための方法が提示される。方法は、ユーザ機器（ＵＥ）によって実行され、ユーザプレーン（ＵＰ）機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立することと、ＵＰＦから拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信することと、ＥＡＰベースの認証応答をＵＰＦに送信することとを備える。

【０００７】

方法は、セキュリティアンカー機能（ＳＥＡＦ）との１次認証を確立することをさらに備えることができる。

【０００８】

方法は、ＵＰＦからＥＡＰベースの認証結果を受信することをさらに備えることができる。

【０００９】

ＵＥはさらに、次世代（ＮＧ）ＵＥであってもよい。ＵＰＦはさらに、ＮＧ　ＵＰＦであってもよい。

【００１０】

第２の態様によれば、ネットワークにおける２次認証のための方法が提示される。方法は、ユーザプレーン（ＵＰ）機能（ＵＰＦ）によって実行され、ユーザ機器（ＵＥ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立することと、拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＵＥに送信することと、ＥＡＰベースの認証応答をＵＥから受信することとを備える。

【００１１】

方法は、受信されたＥＡＰベースの認証応答の検証要求を、認証、認可、アカウンティング（ＡＡＡ）サーバに送信することと、ＡＡＡサーバから検証応答を受信することとをさらに備えることができる。

【００１２】
方法は、認証結果をＵＥに送信することであって、認証はＡＡＡサーバからの検証応答に基づく、送信することをさらに備えることができる。
【００１３】
ＵＥはさらに、次世代（ＮＧ）ＵＥであってもよい。ＵＰＦはさらに、ＮＧ　ＵＰＦであってもよい。
【００１４】
第３の態様によれば、ネットワークにおける動作のためのユーザ機器（ＵＥ）が提示される。ＵＥは、プロセッサと、コンピュータプログラム製品とを備える。コンピュータプログラム製品は、プロセッサによって実行されるとき、ＵＥに、ＵＰ機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立することと、ＵＰＦから拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信することと、ＥＡＰベースの認証応答をＵＰＦに送信することとを行わせる命令を格納する。
【００１５】
ＵＥに、セキュリティアンカー機能（ＳＥＡＦ）との１次認証を確立することをさらに行わせてもよい。
【００１６】
ＵＥに、ＵＰＦからＥＡＰベースの認証結果を受信することをさらに行わせもよい。
【００１７】
ＵＥはさらに、次世代（ＮＧ）ＵＥであってもよい。ＵＰＦはさらに、ＮＧ　ＵＰＦであってもよい。
【００１８】
第４の態様によれば、ネットワークにおいて動作可能なユーザプレーン（ＵＰ）機能（ＵＰＦ）が提示される。ＵＰＦは、プロセッサと、コンピュータプログラム製品とを備える。コンピュータプログラム製品は、プロセッサによって実行されるとき、ＵＰＦに、ユーザ機器（ＵＥ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立することと、拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＵＥに送信することと、ＥＡＰベースの認証応答をＵＥから受信することとを行わせる命令を格納する。
【００１９】
ＵＰＦに、受信されたＥＡＰベースの認証応答の検証要求を、認証、認可、アカウンティング（ＡＡＡ）サーバに送信することと、ＡＡＡサーバから検証応答を受信することとをさらに行わせてもよい。
【００２０】
ＵＰＦに、認証結果をＵＥに送信することであって、認証はＡＡＡサーバからの検証応答に基づく、送信することをさらに行わせてもよい。
【００２１】
ＵＥはさらに、次世代（ＮＧ）ＵＥであってもよい。ＵＰＦはさらに、ＮＧ　ＵＰＦであってもよい。
【００２２】
第５の態様によれば、ネットワークにおける動作のためのユーザ機器（ＵＥ）が提示される。ＵＥは、ＵＰ機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立するための手段と、ＵＰＦから拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信するための手段と、ＥＡＰベースの認証応答をＵＰＦに送信するための手段とを備える。
【００２３】
ＵＥは、セキュリティアンカー機能（ＳＥＡＦ）との１次認証を確立するための手段をさらに備えることができる。
【００２４】
ＵＥは、ＵＰＦからＥＡＰベースの認証結果を受信するための手段をさらに備えることができる。

【００２５】
ＵＥはさらに、次世代（ＮＧ）ＵＥであってもよい。ＵＰＦはさらに、ＮＧ　ＵＰＦであってもよい。
【００２６】
第６の態様によれば、ネットワークにおいて動作可能なユーザプレーン（ＵＰ）機能（ＵＰＦ）が提示される。ＵＰＦは、ユーザ機器（ＵＥ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立するための手段と、拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＵＥに送信するための手段と、ＥＡＰベースの認証応答をＵＥから受信するための手段とを備える。
【００２７】
ＵＰＦは、受信されたＥＡＰベースの認証応答の検証要求を、認証、認可、アカウンティング（ＡＡＡ）サーバに送信するための手段と、ＡＡＡサーバから検証応答を受信する手段とをさらに備えることができる。
【００２８】
ＵＰＦは、認証結果をＵＥに送信するための手段であって、認証はＡＡＡサーバからの検証応答に基づく手段をさらに備えることができる。
【００２９】
ＵＥはさらに、次世代（ＮＧ）ＵＥであってもよい。ＵＰＦはさらに、ＮＧ　ＵＰＦであってもよい。
【００３０】
第７の態様によれば、ネットワークにおける２次認証のためのコンピュータプログラムが提示される。コンピュータプログラムは、ユーザ機器（ＵＥ）において実行されるとき、ＵＥに、ＵＰ機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立することと、ＵＰＦから拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信することと、ＥＡＰベースの認証応答をＵＰＦに送信することとを行わせるコンピュータプログラムコードを備える。
【００３１】
ＵＥはさらに、次世代（ＮＧ）ＵＥであってもよい。ＵＰＦはさらに、ＮＧ　ＵＰＦであってもよい。
【００３２】
第８の態様によれば、ネットワークにおける２次認証のためのコンピュータプログラムが提示される。コンピュータプログラムは、ユーザプレーン（ＵＰ）機能（ＵＰＦ）において実行されるとき、ＵＰＦに、ユーザ機器（ＵＥ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立することと、拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＵＥに送信することと、ＥＡＰベースの認証応答をＵＥから受信することとを行わせるコンピュータプログラムコードを備える。
【００３３】
ＵＥはさらに、次世代（ＮＧ）ＵＥであってもよい。ＵＰＦはさらに、ＮＧ　ＵＰＦであってもよい。
【００３４】
第９の態様によれば、コンピュータプログラム製品が提示される。コンピュータプログラム製品は、コンピュータプログラムと、コンピュータプログラムが格納されるコンピュータ可読ストレージ手段とを備える。概して、特許請求の範囲において使用されるすべての用語は、本明細書においてそうではないと明示的に規定されていない限り、当技術分野におけるそれらの通常の意味に従って解釈されるものとする。「（ａ／ａｎ／ｔｈｅ）要素、装置、コンポーネント、手段、ステップなど」のすべての参照は、そうではないと特に明記のない限り、要素、装置、コンポーネント、手段、ステップなどの少なくとも１つの例を参照するものとして広義に解釈されるものとする。本明細書において開示される任意の方法のステップは、特に明記のない限り、開示されている正確な順序で実行される必要はない。

【００３５】
これ以降、本発明の概念は、添付の図面を参照して、例証として説明される。
【図面の簡単な説明】
【００３６】
【図１】本明細書において提示される実施形態が適用され得る環境を示す概略図である。
【図２】ＬＴＥにおける２次認証のフローを概略的に示す図である。
【図３】次世代システムにおけるＥＡＰベースの２次認証のフローを概略的に示す図である。
【図４】本明細書において提示される実施形態のＥＡＰベースの２次認証のためのプロトコルアーキテクチャを概略的に示す図である。
【図５】本明細書において提示される実施形態のＥＡＰベースの２次認証のためのプロトコルアーキテクチャを概略的に示す図である。
【図６Ａ】本明細書において提示される実施形態の方法を示す流れ図である。
【図６Ｂ】本明細書において提示される実施形態の方法を示す流れ図である。
【図７】本明細書において提示されるデバイスの一部のコンポーネントを示す概略図である。
【図８】本明細書において提示されるデバイスの一部のコンポーネントを示す概略図である。
【図９】本明細書において提示されるデバイスの機能モジュールを示す概略図である。
【図１０】本明細書において提示されるデバイスの機能モジュールを示す概略図である。
【発明を実施するための形態】
【００３７】
これ以降、本発明の概念は、本発明の概念の特定の実施形態が示される添付の図面を参照して以下にさらに詳細に説明される。しかし、この発明の概念は、多数の異なる形態で具現化されてもよく、本明細書において記載される実施形態に限定されるものと解釈されるべきではなく、これらの実施形態は、この開示が綿密かつ完全なものとなり、本発明の概念の範囲を当業者に十分に伝達できるように、例証として提供されている。説明全体を通じて、類似する番号は類似する要素を示す。
【００３８】
異なるネットワークスライス（ＮＳ）にアクセスするための認証および認可の手順を分離する１つの可能なシナリオは次のとおりである。ＮＧユーザ機器（ＵＥ）が特定のＮＳにアクセスするために、オペレータは、２次ＮＳ固有の認証が後に続く、初期ネットワークアクセスのための１次（通常）認証を最初に実行することになる。２次ＮＳ固有の認証は、場合によっては、サードパーティの制御の下であってもよい。これは、サードパーティサービスプロバイダと、たとえば専用のＮＳインスタンスにおいてこのサードパーティにアクセスおよびトランスポートサービスを提供しているモバイルネットワークオペレータ（ＭＮＯ）との間の信頼を想定している。
【００３９】
Ｌｏｎｇ　Ｔｅｒｍ　Ｅｖｏｌｕｔｉｏｎ（ＬＴＥ）において、説明されるシナリオに関連し得るメカニズムがある。このメカニズムは、ＴＳ２３．４０１からの条項５．３．２において説明される。これは、いわゆる暗号化オプション要求に基づいており、プロトコル設定オプション（ＰＣＯ）と称される情報要素を使用する。
【００４０】
ＰＣＯは、非アクセス階層（ＮＡＳ）メッセージにおける情報要素の１つである。ＰＣＯは、モビリティ管理エンティティ（ＭＭＥ）およびサービングゲートウェイ（Ｓ－ＧＷ）を通じて情報をＰＤＮ－ＧＷに透過的に送信するためにパケットデータネットワーク（ＰＤＮ）接続要求のような複数のタイプのメッセージにおいて使用されることがある。たとえば、ＰＣＯは、ダイナミックホスト設定プロトコルバージョン４（ＤＨＣＰｖ４）を用いてデフォルトベアラアクティブ化の後に限りインターネットプロトコルバージョン４（ＩＰｖ４）アドレスを取得するようＵＥが選択することを指示するアドレス割り当てプ

リファレンスを含むことができる。

【００４１】

ＰＣＯの１つのユースケースは、パスワード認証プロトコル（ＰＡＰ）やチャレンジハンドシェーク認証プロトコル（ＣＨＡＰ）のユーザ名とパスワードのＰＤＮ－ＧＷへの転送であり、次いでアクセス認可のために認証、認可、アカウンティング（ＡＡＡ）サーバを通じてこれらを実行する。ＡＡＡサーバは、外部ドメインに配置されてもよい。ユーザ名およびパスワードは、機密事項であり、保護される必要があるため、ＵＥが暗号化を必要とするＰＣＯ（たとえば、ＰＡＰ／ＣＨＡＰユーザ名およびパスワード）を送信しようとする場合、ＵＥは、接続要求メッセージで暗号化オプション転送フラグを設定して、認証およびＮＡＳセキュリティセットアップが完了した後に限りＰＣＯを送信するものとする。

【００４２】

図２は、ＬＴＥにおいてＰＤＮ－ＧＷを通じてそのような追加の（つまり、２次の）認証手順を実行するために必要とされるメッセージフローを示す。後段において、ステップのさらに詳細な説明が提供される。

【００４３】

ＵＥは、ＵＥドメイン内にある。ＭＭＥ、Ｓ－ＧＷ、ホーム加入者サーバ（ＨＳＳ）、およびＰＤＮ－ＧＷは、ＭＮＯドメイン内にある。ＡＡＡサーバは、サードパーティドメイン内にある。

【００４４】

ステップ１において、ＵＥは、暗号化オプション転送フラグが設定された接続要求メッセージをＭＭＥに送信する。

【００４５】

ステップ２において、認証および鍵共有（ＡＫＡ）手順が、ＵＥとＨＳＳの間で実行される。認証に成功すると、次のステップが実行される。

【００４６】

ステップ３において、ＮＡＳセキュリティが、セキュアモードコマンド（ＳＭＣ）を使用してセットアップされる。ＮＡＳセキュリティがセットアップされた後、すべてのＮＡＳメッセージは機密性および保全性が保護される。

【００４７】

ステップ４において、ＭＭＥは、ＰＣＯの取得のために、暗号化オプション要求メッセージをＵＥに送信する。

【００４８】

ステップ５において、ＵＥは、ＰＣＯ情報要素にＰＡＰ／ＣＨＡＰユーザ名およびパスワードを含む暗号化オプション応答メッセージで応答する。ＵＥが複数のＰＤＮのサブスクリプションを有する場合、ＵＥは、メッセージにアクセスポイント名（ＡＰＮ）も含む。

【００４９】

ステップ６において、ＭＭＥは、受信されたデータを暗号化し、ＰＤＮ－ＧＷを識別するために可能な提供されたＡＰＮを使用して、作成セッション要求メッセージでＳ－ＧＷを通じてＰＣＯをターゲットＰＤＮ－ＧＷに転送する。

【００５０】

ステップ７において、ＰＤＮ－ＧＷは、ｄｉａｍｅｔｅｒ／ｒａｄｉｕｓアクセス要求メッセージで受信されたＰＡＰ／ＣＨＡＰ情報を外部ＡＡＡサーバに送信する。成功すると、セッション作成手順が通常どおりに進行する。

【００５１】

したがって、上記のステップ４～７は、ステップ２の第１の認証が完了した後に実行される２次認証を表す。しかし、ＮＧシステムにおいてこのメカニズムまたは拡張を使用することは、何らかの欠点をもたらすことになる。

【００５２】

第１に、メカニズムは、可能な認証方法に関して極めて限定されている。現在、ＰＡＰおよびＣＨＡＰのサポートしかない。しかし、今日のＰＡＰは、セキュリティの観点からは陳腐化しており、基本的に使用することが可能であるのはＣＨＡＰのみである。

【００５３】

第２に、その他の方法をサポートし、認証情報のトランスポートのためにＰＣＯ情報要素を使用するために、メカニズムは、この目的に専用のＭＭＥとＳ－ＧＷならびにＳ－ＧＷとＰＤＮ－ＧＷの間の特別メッセージを指定するように求められる。すなわち、単に１回だけにはとどまらない往復回数が要求される認証方法を処理することになる。

【００５４】

さらに、このメカニズムが、さらに細分化されるＮＧアーキテクチャにどのように適合するかを見極めることは困難である。実際に、新しいアーキテクチャの特徴（ＴＲ　２３．７９９）を考慮すると、たとえば、モビリティ管理機能（ＭＭＦ）およびセッション管理機能ＳＭＦへのＭＭＥの分離に関する進行中の取組み（ＴＲ　２３．７９９）、ならびに制御およびユーザプレーン分離のための制御とユーザプレーンの分離（ＣＵＰＳ）の取組み（ＴＲ　２３．７１４）に関して、ＵＥとＰＤＮ－ＧＷの間のパスのホップはおそらくはさらに多くなる。このことは、コアネットワーク（ＣＮ）におけるさらに多くの過負荷およびシグナリングを暗示する。

【００５５】

最後に、ＵＥとＰＤＮ－ＧＷとの間に直接プロトコルがないので、このメカニズムは次善策である。特に多くの方法がトランスポート層に厳しい勧告および要件を有するので、その他の認証方法をサポートするのに十分に汎用的なものにすることは技術的に困難となろう。

【００５６】

ユーザプレーン（ＵＰ）で２次認証を実行することは、これがセットアップされると提示される。ＰＤＮへの完全なアクセスを許可するのではなく、２次認証の手順に対して限定されたＵＰセッションが実行されてもよい。２次認証が完了すると、限定されたＵＰセッションは、データネットワークに完全アクセスを有するセッションにアップグレードされてもよい。ＲＦＣ３７４８において規定されているように、拡張認証プロトコル（ＥＡＰ）の使用もまた提示される。ＥＡＰは、ＵＥと潜在的に外部のＡＡＡサーバとの間の認証のために使用され、ここでＮＧ－ＵＰ機能（ＵＰＦ）は、ＬＴＥにおけるＰＤＮ－ＧＷの役割と類似する役割を果たし、ＥＡＰオーセンティケータの機能を保証する。ＥＡＰペイロードは、プロトコルがＩＰベースである、ＲＦＣ５１９１において規定されているように、ネットワークアクセスの認証を搬送するためのプロトコル（ＰＡＮＡ）によって搬送される。もう１つの代替は、ＮＧ－ＵＰＦがＥＡＰサーバの機能を保証するものである。

【００５７】

提示される解決策は、ＥＡＰを使用し、ＥＡＰは幅広く使用され、ＥＡＰトランスポート層セキュリティ（ＴＬＳ）、ＥＡＰ認証および鍵合意（ＡＫＡ）、ＥＡＰトンネル化ＴＬＳ（ＴＴＬＳ）、およびＥＡＰ保護拡張認証プロトコル（ＰＥＡＰ）のような多数の認証方法のサポートを提供する。提示される解決策は、ＩＰベースであり、したがってアクセスネットワーク（ＡＮ）のタイプに非依存である。さらに、解決策はＵＰベースであるため、２次認証は、たとえＮＧ－ＵＥが複数の、場合によっては同時のＮＳ接続をサポートするようなシナリオであっても、ＮＳ固有ベースで独立して実行され得る。ＥＡＰを使用することにより、解決策はまた、異なるタイプの資格情報および認証方法をサポートする。ＥＡＰ交換は、エアインターフェイスを介する保護から恩恵を受けることができる。

【００５８】

したがって、２次認証は、ＮＧ－ＵＥにＩＰアドレスが割り当てられた後のＵＰベアラの流れである。次いで、ＥＡＰは、ＮＧ－ＵＥと（潜在的に外部の）ＡＡＡサーバの間の認証に使用され、ここでＮＧ－ＵＰＦはＥＡＰオーセンティケータの機能を保証する。

【００５９】

ＮＧ－ＵＰＦがＥＡＰオーセンティケータの役割を果たす実施形態は、図３を参照して提示される。

【００６０】

図３は、ＵＰベースの２次認証が外部ＡＡＡサーバで実行されるフローを示す。ＮＧ－ＵＥは、ＵＥドメイン内にある。ＮＧモビリティ管理機能（ＭＭＦ）、ＮＧセッション管理機能（ＳＭＦ）、ＮＧセキュリティアンカー機能（ＳＥＡＦ）、およびＮＧ－ＵＰＦは、ＭＮＯドメイン内にある。ＮＧ－ＵＰＦは、ＬＴＥにおけるＰＤＮ－ＧＷに対応するＵＰＦである。ＡＡＡサーバは、サードパーティドメイン内にある。ＮＧ－ＵＰＦの要件は、場合によっては、ＳＧｉインターフェイスのサポートのようなＬＴＥにおけるＰＤＮ－ＧＷのすべての必要とされるＵＰ機能のサポートに加えて、ＰＡＮＡおよびＥＡＰのサポートを含めることである。一般に、ＮＧプレフィックスは、ＬＴＥ概念に対応するＮＧシステム機能に使用される。

【００６１】

ステップ１において、ＮＧ－ＵＥは、接続手順を開始する接続要求を送信する。本明細書において提示される解決策は、ネットワークスライシングがどのようにサポートされるか、たとえばＮＳインスタンスがどのように選択されるか、およびＮＧ－ＵＥがどのように適正なＮＳインスタンスに方向付けられるかには依存していない。

【００６２】

ステップ２において、ＮＧ－ＵＥは、ＮＧ　ＳＥＡＦとの１次認証を実行する。ＮＧ　ＳＥＡＦは、ＮＧ認証サーバ機能（ＡＵＳＦ）にさらに接続されてもよい。その後、２次認証は、ＮＧ　ＳＥＡＦおよびＮＧ　ＭＭＦがどのように配備されるか（つまり、連結されるかまたは分離されるか）にも、ＮＧＳＥＡＦの位置（ホームまたは訪問先の地上波公共移動通信ネットワーク（ＰＬＭＮ））にも依存することはない。

【００６３】

ステップ３において、制御プレーンセキュリティは、ＮＧ－ＵＥと、ＮＧ　ＮＡＳのエンドポイントの間で確立される。ＮＧ　ＮＡＳのエンドポイントは、たとえばＮＧ　ＭＭＦまたはＮＧ　ＳＭＦであってもよい。

【００６４】

ステップ４において、プロトコルデータユニット（ＰＤＵ）セッションは、それ以降、ＮＧ　ＵＰＦを介するＮＧ－ＵＥとデータネットワークの間のＵＰデータのトランスポートのために確立される。ステップ４は、２次認証手順を実行することのみを許容する限定されたセッションであってもよい。その後、２次認証は、ＮＧ－ＵＥとＮＧ－ＵＰＦの間のＩＰ接続を確立するので、セットアップされているＵＰに依存する。

【００６５】

ステップ５において、２次ＥＡＰベースの認証は、ＮＧ－ＵＥとＮＧ－ＵＰＦの間で実行され、ここでＥＡＰオーセンティケータの機能を保証し、バックエンドの外部ＡＡＡサーバに依存する。ＮＧ－ＵＥは、その後、この認証手順の結果に基づいてデータネットワークにおけるアクセスを許可される。

【００６６】

この提示される解決策は、非３ＧＰＰアクセスがどのように統合されるか、およびステップ１からステップ３がここで示されるとおり正確に、または異なるように実行されるかどうかには非依存である。ステップ４において達成されるＮＧ－ＵＥとＮＧ－ＵＰＦの間にＩＰ接続が確立される限り、ＥＡＰベースの認証は、ステップ５において実行され得る。無線アクセスネットワーク（ＲＡＮ）セキュリティが、ステップ５の前に確立されている場合は、ＥＡＰ交換はエアインターフェイス上でも保護される。

【００６７】

図４は、図３を参照して説明されるように、ＮＧ－ＵＰＦと、ＥＡＰオーセンティケータとしてのＮＧ－ＵＰＦを伴うＮＧ－ＵＥの間のＥＡＰベースの２次認証のプロトコルアーキテクチャを示す。図４に示されるアーキテクチャは、ＵＥとＰＤＮ－ＧＷの間のＵＰトラフィックのトランスポートに関しては、ＬＴＥのアーキテクチャと類似する。グレー

表示されたボックスは、上記で説明されるＥＡＰベースの２次認証を提供するために必要とされる追加のプロトコル層を強調する。

【００６８】

ＥＡＰサーバとしてのＵＧ－ＵＰＦとのＥＡＰベースの２次認証のプロトコルアーキテクチャによる実施形態は、図５を参照して提示される。

【００６９】

この実施形態において、ＮＧ－ＵＰＦはＥＡＰ交換を終了させ、完全なＥＡＰサーバの機能を保証する。したがって、この実施形態のメッセージフローは、ステップ５において外部ＡＡＡサーバがコンタクトされていないことを除いては、図３のメッセージフローと類似している。

【００７０】

ＮＧ－ＵＥと、コアネットワーク内のＵＰトラフィックを終了させ、場合によっては外部ＡＡＡサーバと対話するＮＧ－ＵＰＦとの間のＮＧシステムにおける追加または２次認証のメカニズムが提示された。ＮＧ－ＵＰＦは、ＬＴＥにおけるＰＤＮ－ＧＷに対応する。メカニズムは、ＮＧ－ＵＰＦがＥＡＰオーセンティケータの役割またはＥＡＰサーバの機能を保証するように、ＵＰトラフィック上のＩＰを介するＥＡＰに基づく。

【００７１】

本明細書において説明される実施形態が実施され得る通信ネットワーク４は、図１に提示される。ユーザ機器（ＵＥ）１は、基地局（ＢＳ）２に無線により接続可能である。ＢＳ２は、コアネットワーク（ＣＮ）３に接続される。

【００７２】

実施形態によれば、ネットワークにおける２次認証のための方法が、図６Ａを参照して提示される。方法は、次世代（ＮＧ）ユーザ機器（ＵＥ）によって実行され、ＮＧ－ＵＰ機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立すること１１０、拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＮＧ－ＵＰＦから受信すること１３０、およびＥＡＰベースの認証応答をＮＧ－ＵＰＦに送信すること１４０を備える。

【００７３】

方法は、ＮＧ　ＳＥＡＦとの１次認証を確立すること１００をさらに備えることができる。

【００７４】

方法は、ＵＰＦからＥＡＰベースの認証結果を受信することをさらに備えることができる。

【００７５】

実施形態によれば、コアネットワークにおける２次認証のための方法が、図６Ｂを参照して提示される。方法は、次世代（ＮＧ）ユーザプレーン（ＵＰ）機能（ＵＰＦ）によって実行され、ＮＧユーザ機器（ＵＥ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立すること１１０、拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＮＧ　ＵＥに送信すること１２０、およびＥＡＰベースの認証応答をＮＧ　ＵＥから受信すること１５０を備える。

【００７６】

方法は、受信されたＥＡＰベースの認証応答の検証要求を、認証、認可、アカウンティング（ＡＡＡ）サーバに送信すること１６０、および検証応答をＡＡＡサーバから受信すること１７０をさらに備えることができる。

【００７７】

方法は、認証結果をＵＥに送信することをさらに備えることができ、認証はＡＡＡサーバからの検証応答に基づく。

【００７８】

実施形態によれば、ネットワークにおける動作のためのＮＧ　ＵＥが、図７を参照して提示される。ＮＧ　ＵＥ１は、プロセッサ１０、およびコンピュータプログラム製品１２、１３を備える。コンピュータプログラム製品は、プロセッサによって実行されるとき、

ＮＧ　ＵＥに、ＮＧ－ＵＰＦとのＵＰセッションまたは接続を確立すること１１０、ＥＡＰベースの認証要求をＮＧ－ＵＰＦから受信すること１３０、およびＥＡＰベースの認証応答をＮＧ－ＵＰＦに送信すること１４０を行わせる命令を格納する。

【００７９】

実施形態によれば、コアネットワークにおいて動作可能なＮＧ－ＵＰＦが、図８を参照して提示される。ＵＧ－ＵＰＦは、プロセッサ１０、およびプロセッサによって実行されるとき、ＮＧ－ＵＰＦに、ＮＧ　ＵＥとのＵＰセッションまたは接続を確立すること１１０、ＥＡＰベースの認証要求をＮＧ－ＵＰＦに送信すること１２０、およびＥＡＰベースの認証応答をＮＧ　ＵＥから受信すること１５０を行わせる命令を格納するコンピュータプログラム製品１２、１３を備える。

【００８０】

実施形態によれば、ネットワークにおける動作のためのＮＧ　ＵＥが、図９を参照して提示される。ＮＧ　ＵＥは、ＮＧ－ＵＰＦとのＵＰセッションまたは接続を確立する１１０ため、ＥＡＰベースの認証要求をＮＧ－ＵＰＦから受信する１３０ため、およびＥＡＰベースの認証応答をＮＧ－ＵＰＦに送信する１４０ための通信マネージャ６１を備える。

【００８１】

実施形態によれば、ネットワークにおいて動作可能なＮＧ－ＵＰＦが、図１０を参照して提示される。ＮＧ－ＵＰＦは、ＮＧ　ＵＥとのＵＰセッションまたは接続を確立する１１０ため、ＥＡＰベースの認証要求をＮＧ　ＵＥに送信する１２０ため、およびＥＡＰベースの認証応答をＮＧ　ＵＥから受信する１５０ための通信マネージャ７１を備える。

【００８２】

実施形態によれば、ネットワークにおける２次認証のためのコンピュータプログラム１４、１５が提示される。コンピュータプログラムは、ＮＧ　ＵＥ上で実行されるとき、ＮＧ　ＵＥに、ＮＧ－ＵＰＦとのＵＰセッションまたは接続を確立すること１１０、ＥＡＰベースの認証要求をＮＧ－ＵＰＦから受信すること１３０、およびＥＡＰベースの認証応答をＮＧ－ＵＰＦに送信すること１４０を行わせるコンピュータプログラムコードを備える。

【００８３】

実施形態によれば、ネットワークにおける２次認証のためのコンピュータプログラム１４、１５が提示される。コンピュータプログラムは、ＮＧ－ＵＰＦ上で実行されるとき、ＮＧ－ＵＰＦに、ＮＧ　ＵＥとのＵＰセッションまたは接続を確立すること１１０、ＥＡＰベースの認証要求をＮＧ　ＵＥに送信すること１２０、およびＥＡＰベースの認証応答をＮＧ　ＵＥから受信すること１５０を行わせるコンピュータプログラムコードを備える。

【００８４】

実施形態によれば、コンピュータプログラム製品１２、１３が提示される。コンピュータプログラム製品は、上記で提示されるように、コンピュータプログラム１４、１５、およびコンピュータプログラム１４、１５が格納されているコンピュータ可読ストレージ手段を備える。

【００８５】

図７は、ＮＧ　ＵＥ１の一部のコンポーネントを示す概略図である。プロセッサ１０は、メモリに格納されているコンピュータプログラム１４のソフトウェア命令を実行することができる、適切な中央演算処理装置（ＣＰＵ）、マルチプロセッサ、マイクロコントローラ、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路などのうちの１つまたは複数の任意の組合せを使用して提供されてもよい。したがって、メモリは、コンピュータプログラム製品１２の一部であるか、または一部を形成するものと見なされてもよい。プロセッサ１０は、図１２および図１３を参照して本明細書において説明される方法を実行するように設定されてもよい。

【００８６】

メモリは、読取り書込みメモリおよび読取り専用メモリ（ＲＯＭ）の任意の組合せであ

ってもよい。メモリはまた、たとえば磁気メモリ、光メモリ、ソリッドステートメモリ、またはさらにリモートに搭載されたメモリの任意の１つまたは組合せであってもよい、永続ストレージを備えることもできる。

【００８７】

データメモリの形式の第２のコンピュータプログラム製品１３はまた、たとえば、プロセッサ１０でのソフトウェア命令の実行中にデータを読み取りおよび／または格納するために提供されてもよい。データメモリは、読取りおよび書込みメモリと読取り専用メモリ（ＲＯＭ）の任意の組合せであってもよく、また、たとえば磁気メモリ、光メモリ、ソリッドステートメモリ、またはリモートに搭載されたメモリの任意の１つまたは組合せであってもよい、永続ストレージを備えることもできる。データメモリは、たとえば、ＮＧ　ＵＥ１の機能を向上させるために、その他のソフトウェア命令１５を保留することができる。

【００８８】

ＮＧ　ＵＥ１は、たとえばユーザインターフェイスを含む、入出力（Ｉ／Ｏ）インターフェイス１１をさらに備えることができる。ＮＧ　ＵＥ１は、その他のノードからシグナリングを受信するように設定された受信機と、シグナリングをその他のノード（図示せず）に送信するように設定された送信機とをさらに備えることができる。ＮＧ　ＵＥ１のその他のコンポーネントは、本明細書において提示される概念を不明瞭にすることがないように省略される。

【００８９】

図９は、ＮＧ　ＵＥ１の機能ブロックを示す概略図である。モジュールは、キャッシュサーバで実行するコンピュータプログラムのような単独のソフトウェア命令として、または特殊用途向け集積回路、フィールドプログラマブルゲートアレイ、ディスクリート論理コンポーネント、送受信機などのような単独のハードウェアとして、またはその組合せとして実装されてもよい。代替の実施形態において、機能ブロックの一部はソフトウェアにより実装されてもよく、その他はハードウェアにより実装されてもよい。図６Ａに示される方法におけるステップに対応するモジュールは、通信マネージャユニット６１および決定モジュールユニット６０を備える。モジュールの１つまたは複数がコンピュータプログラムによって実装される実施形態において、これらのモジュールは必ずしもプロセスモジュールに対応するわけではないが、一部のプログラミング言語が通常はプロセスモジュールを含まないので、これらが実装されるプログラミング言語による命令として記述され得ることを理解されたい。

【００９０】

通信マネージャ６１は、ネットワークにおける動作のためのものである。このモジュールは、図６Ａの確立ＵＰステップ１１０、受信要求ステップ１３０、および送信応答ステップ１４０に対応する。このモジュールは、コンピュータプログラムを実行しているとき、たとえば、図７のプロセッサ１０によって実装されてもよい。

【００９１】

決定マネージャ６０は、ネットワークにおける動作のためのものである。このモジュールは、図６Ａの１次認証ステップ１００に対応する。このモジュールは、コンピュータプログラムを実行しているとき、たとえば、図７のプロセッサ１０によって実装されてもよい。

【００９２】

図８は、ＮＧ－ＵＰＦ３の一部のコンポーネントを示す概略図である。プロセッサ１０は、メモリに格納されているコンピュータプログラム１４のソフトウェア命令を実行することができる、適切な中央演算処理装置（ＣＰＵ）、マルチプロセッサ、マイクロコントローラ、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路などのなどの１つまたは複数の任意の組合せを使用して提供されてもよい。したがって、メモリは、コンピュータプログラム製品１２の一部であるか、または一部を形成するものと見なされてもよい。プロセッサ１０は、図６Ｂを参照して本明細書において説明される方法を実行するよう

に設定されてもよい。

【００９３】

メモリは、読取り書込みメモリ（ＲＡＭ）および読取り専用メモリ（ＲＯＭ）の任意の組合せであってもよい。メモリはまた、たとえば磁気メモリ、光メモリ、ソリッドステートメモリ、またはさらにリモートに搭載されたメモリの任意の１つまたは組合せであってもよい、永続ストレージを備えることもできる。

【００９４】

データメモリの形式の第２のコンピュータプログラム製品１３はまた、たとえば、プロセッサ１０でのソフトウェア命令の実行中にデータを読み取りおよび／または格納するために提供されてもよい。データメモリは、読取りおよび書込みメモリ（ＲＡＭ）と読取り専用メモリ（ＲＯＭ）の任意の組合せであってもよく、また、たとえば磁気メモリ、光メモリ、ソリッドステートメモリ、またはさらにリモートに搭載されたメモリの任意の１つまたは組合せであってもよい、永続ストレージを備えることもできる。データメモリは、たとえば、ＮＧ－ＵＰＦ３の機能を向上させるために、その他のソフトウェア命令１５を保留することができる。

【００９５】

ＮＧ－ＵＰＦ３は、たとえばユーザインターフェイスを含む、入出力（Ｉ／Ｏ）インターフェイス１１をさらに備えることができる。ＮＧ－ＵＰＦ３は、その他のノードからシグナリングを受信するように設定された受信機と、シグナリングをその他のノード（図示せず）に送信するように設定された送信機とをさらに備えることができる。ＮＧ－ＵＰＦ３のその他のコンポーネントは、本明細書において提示される概念を不明瞭にすることがないように省略される。

【００９６】

図１０は、ＮＧ－ＵＰＦ３の機能ブロックを示す概略図である。モジュールは、キャッシュサーバで実行するコンピュータプログラムのような単独のソフトウェア命令として、または特殊用途向け集積回路、フィールドプログラマブルゲートアレイ、ディスクリート論理コンポーネント、送受信機などのような単独のハードウェアとして、またはその組合せとして実装されてもよい。代替の実施形態において、機能ブロックの一部はソフトウェアにより実施されてもよく、その他はハードウェアにより実装されてもよい。図６Ｂに示される方法におけるステップに対応するモジュールは、通信マネージャユニット７１および決定マネージャユニット７０を備える。モジュールの１つまたは複数がコンピュータプログラムによって実装される実施形態において、これらのモジュールは必ずしもプロセスモジュールに対応するわけではないが、一部のプログラミング言語が通常はプロセスモジュールを含まないので、これらが実装されるであろうプログラミング言語による命令として記述され得ることを理解されたい。

【００９７】

通信マネージャ７１は、コアネットワークにおける動作のためのものである。このモジュールは、図６Ｂの確立ＵＰステップ１１０、送信要求ステップ１２０、および送信応答ステップ１５０に対応する。このモジュールは、コンピュータプログラムを実行しているとき、たとえば、図８のプロセッサ１０によって実装されてもよい。

【００９８】

決定マネージャユニット７０は、コアネットワークにおける動作のためのものである。このモジュールは、図６Ｂの検証要求ステップ１６０、および検証応答ステップ１７０に対応する。このモジュールは、コンピュータプログラムを実行しているとき、たとえば、図８のプロセッサ１０によって実装されてもよい。

【００９９】

本発明の概念は、主として、いくつかの実施形態を参照して上記で説明された。しかし、当業者によって容易に理解されるように、上記で開示されている実施形態以外の他の実施形態は、添付の特許請求の範囲によって規定されるように本発明の概念の範囲内で同等に可能である。

【０１００】
以下に示すのは、開示される主題のさまざまな態様をさらに示す特定の列挙される実施形態である。
１．　次世代（ＮＧ）ユーザ機器（ＵＥ）によって実行される、ネットワークにおける２次認証のための方法であって、
ＮＧ－ＵＰ機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立すること（１１０）と、
ＵＰ　ＮＧ－ＵＰＦから拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信すること（１３０）と、
ＥＡＰベースの認証応答をＵＰ　ＮＧ－ＵＰＦに送信すること（１４０）とを備える方法。
２．　ＮＧセキュリティアンカー機能（ＳＥＡＦ）との１次認証を確立すること（１００）をさらに備える１項に記載の方法。
３．　次世代（ＮＧ）ユーザプレーンＵＰ機能（ＵＰＦ）によって実行される、ネットワークにおける２次認証のための方法であって、
ＮＧユーザ機器（ＵＥ）へのＵＰセッションまたは接続を確立すること（１１０）と、
拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＮＧ　ＵＥに送信すること（１２０）と、
ＥＡＰベースの認証応答をＮＧ　ＵＥから受信すること（１５０）とを備える方法。
４．　受信されたＥＡＰベースの認証応答の検証要求を、認証、認可、アカウンティング（ＡＡＡ）サーバに送信すること（１６０）と、
ＡＡＡサーバから検証応答を受信すること（１７０）とをさらに備える３項に記載の方法。
５．　ネットワークにおける動作のための次世代（ＮＧ）ユーザ機器（ＵＥ）であって、
プロセッサ（１０）と、
プロセッサによって実行されるとき、ＮＧ　ＵＥに、
ＮＧ－ＵＰ機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立すること（１１０）と、
ＵＰ　ＮＧ－ＵＰＦから拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信すること（１３０）と、
ＥＡＰベースの認証応答をＮＧ－ＵＰＦに送信すること（１４０）とを行わせる命令を格納するコンピュータプログラム製品（１２、１３）とを備えるＮＧ　ＵＥ。
６．　ＮＧユーザ機器（ＵＥ）に、ＮＧセキュリティアンカー機能（ＳＥＡＦ）との１次認証を確立すること（１００）をさらに行わせる５項に記載のＮＧ　ＵＥ。
７．　ネットワークにおいて動作可能な次世代（ＮＧ）ユーザプレーン（ＵＰ）機能（ＵＰＦ）であって、
プロセッサ（１０）と、
プロセッサによって実行されるとき、ＮＧ－ＵＰＦに、
ＮＧユーザ機器（ＵＥ）とのＵＰセッションまたは接続を確立すること（１１０）と、
拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＮＧ　ＵＥに送信すること（１２０）と、
ＥＡＰベースの認証応答をＮＧ　ＵＥから受信すること（１５０）とを行わせる命令を格納するコンピュータプログラム製品（１２、１３）とを備えるＮＧ－ＵＰＦ。
８．　受信されたＥＡＰベースの認証応答の検証要求を、認証、認可、アカウンティング（ＡＡＡ）サーバに送信すること（１６０）と、
ＮＧユーザプレーン（ＵＰ）機能（ＵＰＦ）に、ＡＡＡサーバから検証応答を受信すること（１７０）とをさらに行わせる７項に記載のＮＧ－ＵＰＦ。
９．　ネットワークにおける動作のための次世代（ＮＧ）ユーザ機器（ＵＥ）であって、
ＮＧ－ＵＰ機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立す

る（１１０）ため、拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＮＧ－ＵＰＦから受信する（１３０）ため、およびＥＡＰベースの認証応答をＮＧ－ＵＰＦに送信する（１４０）ための通信マネージャ（６１）を備えるＮＧ　ＵＥ。

１０．ネットワークにおいて動作可能な次世代（ＮＧ）ユーザプレーン（ＵＰ）機能（ＵＰＦ）であって、

ＮＧユーザ機器（ＵＥ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立する（１１０）ため、拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＮＧ　ＵＥに送信する（１２０）ため、およびＥＡＰベースの認証応答をＮＧ　ＵＥから受信する（１５０）ための通信マネージャ（７１）を備えるＮＧ－ＵＰＦ。

１１．　ネットワークにおける２次認証のためのコンピュータプログラム（１４、１５）であって、次世代（ＮＧ）ユーザ機器（ＵＥ）において実行されるとき、ＮＧ　ＵＥに、

ＮＧ－ＵＰ機能（ＵＰＦ）とのユーザプレーン（ＵＰ）セッションまたは接続を確立すること（１１０）と、

ＵＰ　ＮＧ－ＵＰＦから拡張認証プロトコル（ＥＡＰ）ベースの認証要求を受信すること（１３０）と、

ＥＡＰベースの認証応答をＮＧ－ＵＰＦに送信すること（１４０）とを行わせるコンピュータプログラムコードを備えるコンピュータプログラム。

１２．　ネットワークにおける２次認証のためのコンピュータプログラム（１４、１５）であって、次世代（ＮＧ）ユーザプレーン（ＵＰ）機能（ＵＰＦ）において実行されるとき、ＮＧ－ＵＰＦに、

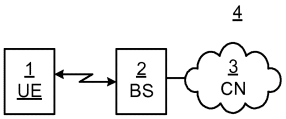
ＮＧユーザ機器（ＵＥ）へのユーザプレーン（ＵＰ）セッションまたは接続を確立すること（１１０）と、

拡張認証プロトコル（ＥＡＰ）ベースの認証要求をＮＧ　ＵＥに送信すること（１２０）と、

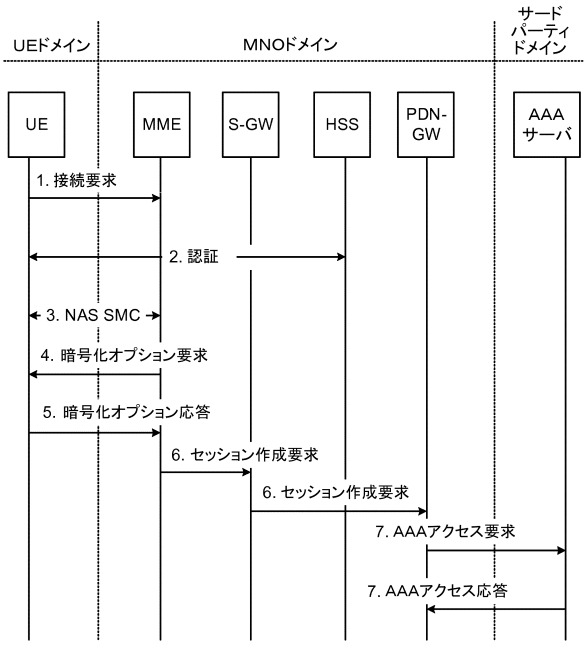
ＥＡＰベースの認証応答をＮＧ　ＵＥから受信すること（１５０）とを行わせるコンピュータプログラムコードを備えるコンピュータプログラム。

１３．　１１項または１２項のいずれか一項に記載のコンピュータプログラム（１４、１５）と、コンピュータプログラム（１４、１５）が格納されているコンピュータ可読ストレージ手段とを備えるコンピュータプログラム製品（１２、１３）。

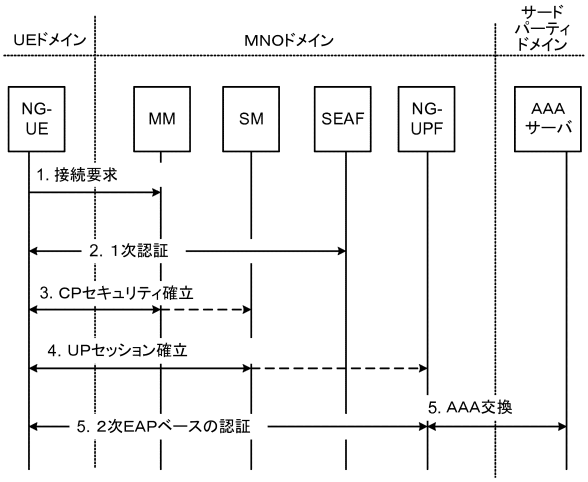
【図１】


4
1
UE
2
BS
3
CN

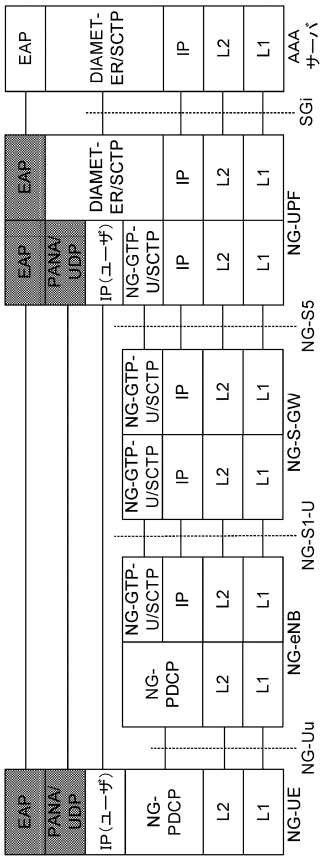
【図２】


UEドメイン
MNOドメイン
サード
パーティ
ドメイン
UE
MME
S-GW
HSS
PDN-
GW
AAA
サーバ
1. 接続要求
2. 認証
3. NAS SMC
4. 暗号化オプション要求
5. 暗号化オプション応答
6. セッション作成要求
6. セッション作成要求
7. AAAアクセス要求
7. AAAアクセス応答

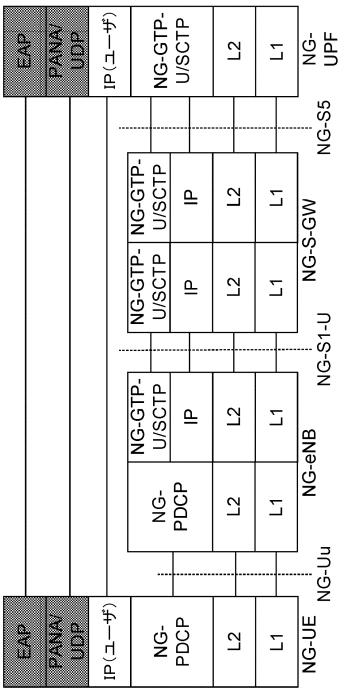
【図３】


UEドメイン
MNOドメイン
サード
パーティ
ドメイン
NG-
UE
MM
SM
SEAF
NG-
UPF
AAA
サーバ
1. 接続要求
2. 1次認証
3. CPセキュリティ確立
4. UPセッション確立
5. AAA交換
5. 2次EAPベースの認証

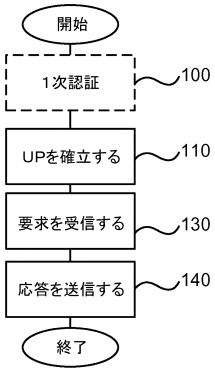
【図４】


EAP
DIAMET-
ER/SCTP
IP
L2
L1
AAA
サーバ
SGi
EAP
PANA/
UDP
IP(ユーザ)
NG-GTP-
U/SCTP
NG-UPF
NG-S5
NG-S-GW
NG-S1-U
NG-eNB
NG-Uu
NG-
PDCP
NG-UE

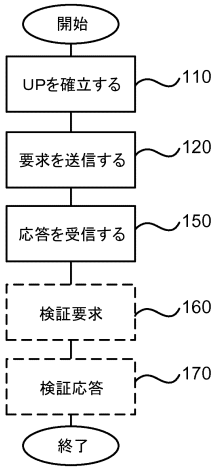
【図５】


EAP
PANA/
UDP
IP(ユーザ)
NG-GTP-
U/SCTP
IP
L2
L1
NG-
PDCP
NG-
UPF
NG-S5
NG-S-GW
NG-S1-U
NG-eNB
NG-Uu
NG-UE

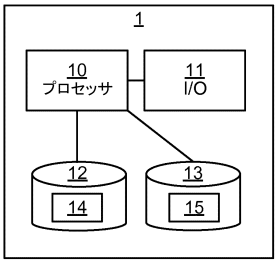
【図６Ａ】



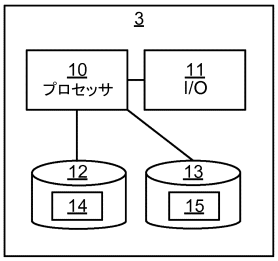
【図６Ｂ】



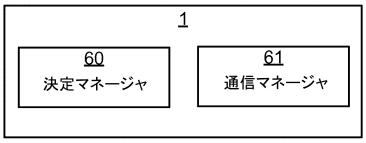
【図７】



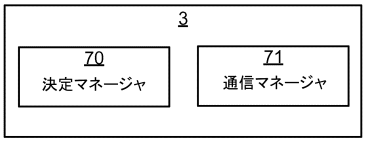
【図８】



【図９】



【図１０】



フロントページの続き

(72)発明者 ベン ヘンダ, ノアメン
スウェーデン国 １６２ ４７ ストックホルム, チューモルトグレン ２２８
(72)発明者 レフトヴィルタ, ヴェサ
フィンランド国 エフアイ－０２６２０ エスポー, ヴェイニンマキ １０ベー
(72)発明者 カステリャノス サモーラ, ダビド
スペイン国 ２８０４５ マドリード, カジェ エンバハドール ２５６, １階 ビー号室

審査官 倉本 敦史

(56)参考文献 米国特許出願公開第２０１２／０２６９１６２（ＵＳ，Ａ１）
Qualcomm Inc., LG Electronics, Way forward on support of non-3GPP access and update to solution 8.6 for support of untrusted non-3GPP access, 3GPP SA WG2 Meeting #117 S2-166283, ２０１６年１０月２４日, pp.1-10

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｗ ４／００－９９／００
Ｇ０６Ｆ ２１／４４