(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7422193号
(P7422193)

(45)発行日　令和6年1月25日(2024.1.25)

(24)登録日　令和6年1月17日(2024.1.17)

(51)国際特許分類

Ｈ０４Ｗ　12/08　(2021.01)		Ｈ０４Ｗ	12/08
Ｈ０４Ｗ　12/37　(2021.01)		Ｈ０４Ｗ	12/37

ＦＩ

請求項の数　25　外国語出願　（全20頁）

(21)出願番号　特願2022-126838(P2022-126838)
(22)出願日　令和4年8月9日(2022.8.9)
(65)公開番号　特開2023-24967(P2023-24967A)
(43)公開日　令和5年2月21日(2023.2.21)
審査請求日　令和4年10月12日(2022.10.12)
(31)優先権主張番号　202141035928
(32)優先日　令和3年8月9日(2021.8.9)
(33)優先権主張国・地域又は機関
インド(IN)

(73)特許権者　515076873
ノキア テクノロジーズ オサケユイチア
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　100103610
弁理士　▲吉▼田 和彦
(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　100086771
弁理士　西島 孝喜
(74)代理人　100109335

最終頁に続く

(54)【発明の名称】　通信ネットワークにおけるユーザ機器のデータ伝送管理

(57)【特許請求の範囲】

【請求項１】

少なくとも１つのプロセッサと、

コンピュータプログラムコードを含む少なくとも１つのメモリと、

を備える装置であって、

前記少なくとも１つのメモリおよび前記コンピュータプログラムコードは、前記少なくとも１つのプロセッサによって、前記装置に少なくとも、

通信ネットワークを介したデータネットワークとの接続の確立を開始させることと、

前記データネットワークへのアップリンクデータ転送が許可されていないという第１の通知を前記通信ネットワークから受信することと、

前記データネットワークへのアップリンクデータ転送が許可されているという第２の通知を前記通信ネットワークから受信することであって、前記第２の通知は認証エンティティによる前記装置の検証の成功に対応する、前記受信することと、

を行わせるように構成される、装置。

【請求項２】

前記装置は、前記第１の通知の受信および前記第２の通知の受信の間、前記データネットワークへのアップリンクデータ転送の開始を控える、請求項１に記載の装置。

【請求項３】

前記装置は、前記通信ネットワークを介して前記データネットワークにアクセスするように構成されるユーザ機器の一部である、請求項１に記載の装置。

【請求項４】
前記ユーザ機器は無乗員航空機システム（ＵＡＳ）の一部である、請求項３に記載の装置。
【請求項５】
前記検証は、前記通信ネットワークにアクセスするために使用される識別子とは異なるデータネットワーク識別子に関して行われる前記装置の認証および認可を含む、請求項１に記載の装置。
【請求項６】
ユーザ機器によって、通信ネットワークを介したデータネットワークとの接続の確立を開始させることと、
前記ユーザ機器において、前記データネットワークへのアップリンクデータ転送が許可されていないという第１の通知を前記通信ネットワークから受信することと、
前記ユーザ機器において、前記データネットワークへのアップリンクデータ転送が許可されているという第２の通知を前記通信ネットワークから受信することであって、前記第２の通知は認証エンティティによる前記ユーザ機器の検証の成功に対応する、前記受信することと、
を含む、方法。
【請求項７】
前記ユーザ機器は、前記第１の通知の受信および前記第２の通知の受信の間、前記データネットワークへのアップリンクデータ転送の開始を控える、請求項６に記載の方法。
【請求項８】
前記ユーザ機器は無乗員航空機システム（ＵＡＳ）の一部である、請求項６に記載の方法。
【請求項９】
前記検証は、前記通信ネットワークにアクセスするために使用される識別子とは異なるデータネットワーク識別子に関して行われる前記ユーザ機器の認証および認可を含む、請求項６に記載の方法。
【請求項１０】
プロセッサによって実行された場合に、請求項６のステップを前記プロセッサに実行させる実行可能なプログラムコードが内部に具現化された非一時的なコンピュータ可読記憶媒体。
【請求項１１】
少なくとも１つのプロセッサと、
コンピュータプログラムコードを含む少なくとも１つのメモリと、
を備える装置であって、
前記少なくとも１つのメモリおよび前記コンピュータプログラムコードは、前記少なくとも１つのプロセッサによって、前記装置に少なくとも、
通信ネットワークを介したデータネットワークとの接続を確立する要求をユーザ機器から受信することと、
前記データネットワークへのアップリンクデータ転送が許可されていないという第１の通知を前記通信ネットワークから前記ユーザ機器に送信することと、
前記データネットワークへのアップリンクデータ転送が許可されているという第２の通知を前記通信ネットワークから前記ユーザ機器に送信することであって、前記第２の通知は認証エンティティによる前記ユーザ機器の検証の成功に対応する、前記送信することと、
を行わせるように構成される、装置。
【請求項１２】
前記検証は、前記通信ネットワークにアクセスするために使用される識別子とは異なるデータネットワーク識別子に関して行われる前記ユーザ機器の認証および認可を含む、請求項１１に記載の装置。
【請求項１３】

前記通信ネットワークは、４Ｇネットワークアーキテクチャおよび５Ｇネットワークアーキテクチャのうちの少なくとも１つを含む、請求項１１に記載の装置。
【請求項１４】
前記認証エンティティは、データネットワーク－認証、認可およびアカウンティング（ＤＮ－ＡＡＡ）サーバを含む、請求項１１に記載の装置。
【請求項１５】
前記認証エンティティは、ＵＡＳサービスサプライヤ（ＵＳＳ）サーバを含む、請求項１１に記載の装置。
【請求項１６】
前記第１の通知および前記第２の通知は、前記通信ネットワークのデータネットワークゲートウェイによって生成される、請求項１１に記載の装置。
【請求項１７】
前記第１の通知は、前記通信ネットワークを介した接続サービスの確立に関連する、請求項１１に記載の装置。
【請求項１８】
通信ネットワークを介したデータネットワークとの接続を確立する要求をユーザ機器から受信することと、
前記データネットワークへのアップリンクデータ転送が許可されていないという第１の通知を前記通信ネットワークから前記ユーザ機器に送信することと、
前記データネットワークへのアップリンクデータ転送が許可されているという第２の通知を前記通信ネットワークから前記ユーザ機器に送信することであって、前記第２の通知は認証エンティティによる前記ユーザ機器の検証の成功に対応する、前記送信することと、を含む、方法。
【請求項１９】
前記検証は、前記通信ネットワークにアクセスするために使用される識別子とは異なるデータネットワーク識別子に関して行われる前記ユーザ機器の認証および認可を含む、請求項１８に記載の方法。
【請求項２０】
前記通信ネットワークは、４Ｇネットワークアーキテクチャおよび５Ｇネットワークアーキテクチャのうちの少なくとも１つを含む、請求項１８に記載の方法。
【請求項２１】
前記認証エンティティは、データネットワーク－認証、認可およびアカウンティング（ＤＮ－ＡＡＡ）サーバを含む、請求項１８に記載の方法。
【請求項２２】
前記認証エンティティは、ＵＡＳサービスサプライヤ（ＵＳＳ）サーバを含む、請求項１８に記載の方法。
【請求項２３】
前記第１の通知および前記第２の通知は、前記通信ネットワークのデータネットワークゲートウェイによって生成される、請求項１８に記載の方法。
【請求項２４】
前記第１の通知は、前記通信ネットワークを介した接続サービスの確立に関連する、請求項１８に記載の方法。
【請求項２５】
プロセッサによって実行された場合に、請求項１８のステップを前記プロセッサに実行させる実行可能なプログラムコードが内部に具現化された非一時的なコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本分野は一般に通信システムに関し、より詳細には、排他的にではないが、そのような

システムにおけるセキュリティ管理に関する。
【背景技術】
【０００２】
本セクションでは、本発明をより理解しやすくするのに有益であり得る態様を紹介する。したがって、本セクションの記述はこの観点で読まれるべきであり、何が従来技術に含まれるか、または何が従来技術に含まれないかについて認めるものとして理解されるべきではない。
【０００３】
第４世代（４Ｇ）ワイヤレス移動体電気通信技術、別名ロングタームエボリューション（ＬＴＥ）技術は、特に人的交流のために高データレートの大容量モバイルマルチメディアを提供するように設計されていた。そのような４Ｇネットワークは、典型的には進化型パケットシステム（ＥＰＳ：Ｅｖｏｌｖｅｄ　Ｐａｃｋｅｔ　Ｓｙｓｔｅｍ）を利用し、そのアーキテクチャは２つのサブシステム、すなわち、進化型ユニバーサル地上無線アクセスネットワーク（Ｅ－ＵＴＲＡＮ：Ｅｖｏｌｖｅｄ　Ｕｎｉｖｅｒｓａｌ　Ｔｅｒｒｅｓｔｒｉａｌ　Ｒａｄｉｏ　Ａｃｃｅｓｓ　Ｎｅｔｗｏｒｋ）および進化型パケットコア（ＥＰＣ：Ｅｖｏｌｖｅｄ　Ｐａｃｋｅｔ　Ｃｏｒｅ）ネットワークを含む。
【０００４】
次世代または第５世代（５Ｇ）技術は、人的交流のみでなく、いわゆるモノのインターネット（ＩｏＴ）ネットワークにおけるマシンタイプ通信にも使用されることが意図されている。５Ｇネットワークは、大規模ＩｏＴサービス（たとえば、非常に多数の限られた能力のデバイス）およびミッションクリティカルなＩｏＴサービス（たとえば、高い信頼性を必要とするもの）を実現することが意図されているが、改善されたワイヤレスインターネットアクセスをモバイルデバイスに提供する拡張モバイルブロードバンド（ｅＭＢＢ：ｅｎｈａｎｃｅｄ　ｍｏｂｉｌｅ　ｂｒｏａｄｂａｎｄ）サービスの形態で、従来の移動通信サービスに対する改善がサポートされる。
【０００５】
例示的な通信システムでは、ユーザ機器（５Ｇネットワークにおける５Ｇ　ＵＥ、またはより広範にはＵＥ）は、５ＧネットワークではＮＧ－ＲＡＮと呼ばれるアクセスネットワークの基地局またはアクセスポイントとエアインターフェースを介して通信する。アクセスポイント（たとえば、ｇＮＢ）は、例示的には、通信システムのＮＧ－ＲＡＮの一部である。一般に、アクセスポイント（たとえば、ｇＮＢ）は、ＵＥにコアネットワーク（ＣＮまたは５ＧＣ）へのアクセスを提供し、コアネットワークは次いで、他のＵＥおよび／またはデータネットワーク、たとえば、パケットデータネットワークすなわちＰＤＮ（たとえば、インターネット）へのアクセスをＵＥに提供する。
【０００６】
ＵＥは一般的には移動局、加入者局と呼ばれ得、またはさらにいっそう一般的には通信デバイスと呼ばれ得、これには、ラップトップまたはスマートフォンなどの他の機器に挿入されるカードの組み合わせなどの例が含まれるが、いくつかの応用シナリオでは、ＵＥは無人／無乗員航空機システム（ＵＡＳ：Ｕｎｍａｎｎｅｄ／Ｕｎｃｒｅｗｅｄ　Ａｅｒｉａｌ　Ｓｙｓｔｅｍ）（無人／無乗員航空機（Ｕｎｍａｎｎｅｄ／Ｕｎｃｒｅｗｅｄ　Ａｅｒｉａｌ　Ｖｅｈｉｃｌｅ）すなわちＵＡＶとも呼ばれる）の一部（たとえば、これに挿入されるカード）である。
【０００７】
しかしながら、４Ｇ／５Ｇネットワークに関連するアーキテクチャおよびプロトコルのセキュリティを改善するための継続的な試みにより、データネットワーク接続の確立中のＵＥ認証／認可に関連する問題が大きな課題を提示し得る。
【発明の概要】
【０００８】
例示的な実施形態は、通信ネットワークを介したデータネットワーク接続を確立する場合のユーザ機器の認証／認可中のユーザ機器に関連するアップリンクデータ伝送を管理す

るための技術を提供する。
【０００９】
ユーザ機器の観点からの１つの例示的な実施形態では、方法は以下のステップを含む。ユーザ機器は、通信ネットワークを介したデータネットワークとの接続の確立を開始させる。データネットワークへのアップリンクデータ転送が許可されていないという第１の通知が、通信ネットワークからユーザ機器によって受信される。データネットワークへのアップリンクデータ転送が許可されているという第２の通知が、通信ネットワークからユーザ機器によって受信され、第２の通知は認証エンティティによるユーザ機器の検証の成功に対応する。
【００１０】
たとえば、ユーザ機器は、第１の通知の受信および第２の通知の受信の間、データネットワークへのアップリンクデータ転送の開始を控える。また、例として、検証は、通信ネットワークにアクセスするために使用される識別子（たとえば、加入者識別情報）とは異なるデータネットワーク識別子（たとえば、サービスレベル識別情報またはデータネットワーク固有の識別情報）に関して行われるユーザ機器の認証および認可を含む。
【００１１】
通信ネットワークの観点からの他の例示的な実施形態では、方法は以下のステップを含む。通信ネットワークは、通信ネットワークを介したデータネットワークとの接続を確立する要求をユーザ機器から受信する。通信ネットワークは、データネットワークへのアップリンクデータ転送が許可されていないという第１の通知をユーザ機器に送信する。通信ネットワークは、データネットワークへのアップリンクデータ転送が許可されているという第２の通知をユーザ機器に送信し、第２の通知は認証エンティティによるユーザ機器の検証の成功に対応する。この場合もやはり、例として、検証は、通信ネットワークにアクセスするために使用される識別子（たとえば、加入者識別情報）とは異なるデータネットワーク識別子（たとえば、サービスレベル識別情報またはデータネットワーク固有の識別情報）に関して行われるユーザ機器の認証および認可を含む。
【００１２】
さらなる例示的な実施形態は、プロセッサによって実行された場合に、上記のステップをプロセッサに実行させる実行可能なプログラムコードが内部に具現化された非一時的なコンピュータ可読記憶媒体の形態で提供される。さらに他の例示的な実施形態は、上記のステップを実行するように構成されるプロセッサおよびメモリを有する装置を含む。
【００１３】
有利なことに、例示的な実施形態は、ＵＡＳと共に使用されるＵＥのパケットデータネットワーク（ＰＤＮ）接続確立中のＵＡＳの認証および認可への強化を提供する。しかしながら、例示的な実施形態は、より一般的にはこれらの強化を、たとえば、任意のＵＥ（すなわち、必ずしもＵＡＳと共に使用されるものに限らない）に拡張して、データネットワーク接続確立中に認証エンティティが、ＵＥによって提示されたデータネットワーク固有の識別情報の認証および認可（すなわち、検証）を行うようにすることを理解されたい。たとえば、ＵＡＳシナリオでは、認証エンティティはＵＡＳサービスサプライヤ（ＵＳＳ）であり得、ＥＰＳのシナリオでは、認証エンティティは、データネットワークの認証、認可およびアカウンティングサーバ（ＤＮ－ＡＡＡサーバ：Ｄａｔａ　Ｎｅｔｗｏｒｋ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ，　Ａｕｔｈｏｒｉｚａｔｉｏｎ　ａｎｄ　Ａｃｃｏｕｎｔｉｎｇ　ｓｅｒｖｅｒ）であり得る。しかしながら、実施形態はこれらの例示的なシナリオに限定されない。
【００１４】
本明細書に記載した実施形態のこれらおよび他の特徴および利点は、添付の図面および以下の詳細な説明からより明らかになるであろう。
【図面の簡単な説明】
【００１５】
【図１Ａ】１つまたは複数の例示的な実施形態が実装され得る第１の通信ネットワークア

ーキテクチャを実装する通信システムを示す図である。
【図１Ｂ】１つまたは複数の例示的な実施形態が実装され得る第２の通信ネットワークアーキテクチャを実装する通信システムを示す図である。
【図２】１つまたは複数の例示的な実施形態が実装され得るユーザ機器および少なくとも１つのネットワークエンティティ／機能を示す図である。
【図３】１つまたは複数の例示的な実施形態が実装され得る、第１のタイプの通信ネットワークおよび第２のタイプの通信ネットワークの複合アーキテクチャを示す図である。
【図４】図３の複合アーキテクチャのさらなる詳細を示す図である。
【図５】例示的な実施形態による、データネットワーク接続確立中に実行される、無人／無乗員航空機システムに関連する認証／認可メッセージフローを示す図である。
【発明を実施するための形態】
【００１６】
通信システムにおけるセキュリティ管理のための実施形態を、例示的な通信システムおよび関連する技術と共に本明細書に示す。しかしながら、特許請求の範囲は、開示した特定のタイプの通信システムおよび／または処理に限定されないことを理解されたい。実施形態は、代替的なネットワーク、処理、および動作を使用する多種多様な他のタイプの通信システムで実装することができる。たとえば、４Ｇおよび／または５Ｇシステムなどの３ＧＰＰシステム要素を利用するワイヤレスセルラーベースのシステムのコンテキストで例示しているが、開示した実施形態は、簡単な方法で種々の他のタイプの通信システムに適合させることができる。
【００１７】
例示的な実施形態によれば、１つまたは複数の３ＧＰＰ技術仕様（ＴＳ：ｔｅｃｈｎｉｃａｌ　ｓｐｅｃｉｆｉｃａｔｉｏｎ）および／または技術レポート（ＴＲ：ｔｅｃｈｎｉｃａｌ　ｒｅｐｏｒｔ）は、本発明の解決策の各部とやりとりし得るネットワークエンティティおよび／または動作のさらなる説明を提供し得る。たとえば、ＥＰＳアーキテクチャにおけるＥ－ＵＴＲＡＮアクセスの詳細については、「General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access」と題されたＴＳ２３．４０１に記載されており、その開示全体が本明細書に引用により組み込まれている。５Ｇネットワークでは、アクセスネットワークについては、「Technical Specification Group Services and System Aspects; System Architecture for the 5G System」と題されたＴＳ２３．５０１に記載されており、その開示全体が本明細書に引用により組み込まれている。５Ｇコアネットワークについては、「Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS)」と題されたＴＳ２３．５０２に記載されており、その開示全体が本明細書に引用により組み込まれている。他の３ＧＰＰ　ＴＳ／ＴＲの文書には、当業者が理解する他の詳細が提供され得る。たとえば、ＵＡＳアプリケーションのコンテキストにおいて、「Support of Uncrewed Aerial Systems (UAS) Connectivity, Identification and Tracking; Stage 2」と題されたＴＳ２３．２５６、および「Unmanned Aerial System (UAS) Support in 3GPP; Stage 1」と題されたＴＳ２２．１２５は、それらの開示全体が本明細書に引用により組み込まれているが、本明細書でさらに説明する例示的な実施形態に適用可能であり得る。
【００１８】
しかしながら、実施形態は、４Ｇ関連および／または５Ｇ関連の３ＧＰＰ規格によく適しているが、必ずしも特定の規格に限定されることを意図しておらず、複数の規格およびアーキテクチャにわたる一般的な解決策を提供する。
【００１９】
さらに、本明細書で例示的に使用する場合、以下を含むがこれらに限定されない様々な略称を参照する。
３ＧＰＰ：第３世代パートナーシッププロジェクト
ＡＡＡ：認証、認可、およびアカウンティング

ＤＮ：データネットワーク
ＭＭＥ：モビリティ管理エンティティ
ＮＡＳ：非アクセス層
ＮＥＦ：ネットワーク公開機能
ＰＤＮ：パケットデータネットワーク
ＰＣＯ：プロトコル設定オプション
ＰＧＷ：ＰＤＮゲートウェイ
ＳＧＷ：サービングゲートウェイ
ＳＭＦ：セッション管理機能
ＴＰＡＥ：サードパーティ認可エンティティ
ＵＡＳ：無人／無乗員航空機システム
ＵＡＶ：無人／無乗員航空機
ＵＳＳ：ＵＡＳサービスサプライヤ
ＵＴＭ：ＵＡＳトラフィック管理
ＵＵＡＡ：ＵＳＳ　ＵＡＶ認可／認証

【００２０】

例示的な実施形態は、４Ｇおよび５Ｇネットワークにおける ＵＡＳ認証／認可に関する。そのような例示的な実施形態を説明する前に、４Ｇネットワーク（図１Ａ）および５Ｇネットワーク（図１Ｂ）の特定の主要なコンポーネントの概要を以下で説明する。

【００２１】

図１Ａは、例示的な実施形態が実装される４Ｇ通信システム１００の一部を示している。通信システム１００に示す要素は、そのシステム内に提供される特定の主要なエンティティ、たとえば、ＵＥアクセスエンティティ、モビリティ管理エンティティ、認証エンティティなどを表現することを意図しているということを理解されたい。そのため、図１Ａに示すブロックは、これらの主要なエンティティを提供する４Ｇネットワークにおける特定の要素を指す。しかしながら、表現した主要なエンティティの一部または全てを実装するために、他のネットワーク要素が使用され得る。また、４Ｇネットワークの全てのエンティティを図１Ａに示しているわけではないということを理解されたい。むしろ、例示的な実施形態の説明を容易にする少なくとも一部のエンティティを表現している。以降の図では、これらのエンティティおよび追加のエンティティ（すなわち、より一般的にはネットワークノードと呼ばれ得るもの）をさらに描写し得る。

【００２２】

したがって、図示のように、通信システム１００は、エアインターフェース１０３を介してアクセスポイント（ｅＮＢ）１０４と通信するユーザ機器（ＵＥ）１０２を含む。前述のように、例示的な実施形態では、ＵＥ１０２はＵＡＳの一部（たとえば、これに挿入されるカード）であり得る。「航空機対応ユーザ機器」という用語は、本明細書では、飛行しているＵＥ付きの種々の異なるタイプのＵＡＳ（およびＵＡＶ）、たとえば、限定はしないが、ドローンなどを包含するために使用し得る。

【００２３】

アクセスポイント１０４は、例示的には、通信システム１００のアクセスネットワークの一部である。そのようなアクセスネットワークは、たとえば、複数の基地局および１つまたは複数の関連する無線ネットワーク制御機能を有する４Ｇ　ＲＡＮ（Ｅ－ＵＴＲＡＮ）システムを含み得る。基地局および無線ネットワーク制御機能は、論理的に別々のエンティティであり得るが、所与の実施形態では、同一の物理ネットワーク要素に実装され得る。

【００２４】

この例示的な実施形態でのアクセスポイント１０４は、モビリティ管理エンティティ（ＭＭＥ）１０６に動作可能に結合される。通信システムのコアネットワーク部分におけるモビリティ管理エンティティは、ネットワーク動作の中でもとりわけ、（アクセスポイント１０４を介した）ＵＥに対するアクセスおよびモビリティ（認証／認可を含む）動作を

管理するかまたは別の方法でこれに参加する。ＭＭＥを本明細書ではより一般的に、アクセスおよびモビリティ管理ノードとも呼び得る。

【００２５】

この例示的な実施形態におけるＭＭＥ１０６は、追加のネットワークエンティティ１０８に動作可能に結合される。図示のように、これらのエンティティの一部には、ホーム加入者サーバ（ＨＳＳ：ｈｏｍｅ　ｓｕｂｓｃｒｉｂｅｒ　ｓｅｒｖｅｒ）ならびに認証センター（ＡｕＣ：ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｃｅｎｔｅｒ）が含まれる。ＨＳＳおよびＡｕＣを（個別にまたは集合的に）、本明細書ではより一般的に、認証ノードまたは複数の認証ノードとも呼び得る。また、追加のエンティティ１０８には、サービングゲートウェイ（ＳＧＷ）およびパケットデータネットワークゲートウェイ（ＰＧＷ）が含まれ得る。

【００２６】

ＵＥ１０２などのＵＥは、典型的には、エンティティ１０６および１０８の一部または全てが存在するホーム公衆地上移動ネットワーク（ＨＰＬＭＮ：Ｈｏｍｅ　Ｐｕｂｌｉｃ　Ｌａｎｄ　Ｍｏｂｉｌｅ　Ｎｅｔｗｏｒｋ）と呼ばれるものに加入していることに留意されたい。ＵＥがローミングしている（ＨＰＬＭＮにない）場合、典型的には、訪問先ネットワークとも呼ばれる訪問先公衆地上移動ネットワーク（ＶＰＬＭＮ：Ｖｉｓｉｔｅｄ　Ｐｕｂｌｉｃ　Ｌａｎｄ　Ｍｏｂｉｌｅ　Ｎｅｔｗｏｒｋ）に接続され、ＵＥに現在サービス提供しているネットワークはサービングネットワークと呼ばれる。ローミングしている場合、ネットワークエンティティ１０６および１０８の一部はＶＰＬＭＮに存在し得、その場合、ＶＰＬＭＮ内のエンティティは必要に応じてＨＰＬＭＮ内のエンティティと通信する。しかしながら、ローミングしていないシナリオでは、モビリティ管理エンティティ１０６および他のネットワークエンティティ１０８は同一の通信ネットワーク、すなわち、ＨＰＬＭＮに存在する。本明細書に記載の実施形態は、どのエンティティがどのＰＬＭＮ（すなわち、ＨＰＬＭＮまたはＶＰＬＭＮ）に存在するかによって制限されない。

【００２７】

４Ｇネットワークのさらなる典型的な動作およびエンティティについてはここでは説明せず、その理由は、それらが例示的な実施形態の焦点ではなく、適切な３ＧＰＰ　４Ｇ資料で見つかり得るためである。

【００２８】

システム要素のこの特定の配置は例にすぎず、他のタイプおよび配置の追加のまたは代替の要素を使用して、他の実施形態の通信システムを実装できることを理解されたい。たとえば、他の実施形態では、システム１００は、本明細書に明示的に示していない他のエンティティを含み得る。

【００２９】

したがって、図１Ａの配置は、ワイヤレスセルラーシステムの１つの例示的な構成にすぎず、システム要素の多数の代替的な構成が使用され得る。たとえば、図１Ａの実施形態では単一のエンティティのみを示し得るが、これは説明を簡単かつ明確にするためのものにすぎない。所与の代替的な実施形態は、当然ながら、より多数のそのようなシステム要素、ならびに従来のシステム実装に一般的に関連するタイプの追加のまたは代替の要素を含み得る。

【００３０】

図１Ｂは、例示的な実施形態が実装される５Ｇ通信システム１１０の一部を示している。通信システム１１０内に示す要素は、そのシステム内に提供される特定の主要な機能、たとえば、ＵＥアクセス機能、モビリティ管理機能、認証機能などを表現することを意図しているということを理解されたい。そのため、図１Ｂに示すブロックは、これらの主要な機能を提供する５Ｇネットワークにおける特定の要素を指す。しかしながら、表現した主要な機能の一部または全てを実装するために、他のネットワーク要素が使用され得る。また、５Ｇネットワークの全ての機能を図１Ｂに示しているわけではないということを理解されたい。むしろ、例示的な実施形態の説明を容易にする少なくとも一部の機能を表現

している。以降の図では、これらの機能および追加の機能（すなわち、より一般的にはネットワークノードと呼ばれるもの）をさらに描写し得る。

【００３１】

したがって、図示のように、通信システム１１０は、エアインターフェース１１３を介してアクセスポイント（ｇＮＢ）１１４と通信するユーザ機器（ＵＥ）１１２を含む。この場合も、ＵＥ１１２は例示的な実施形態ではＵＡＳを含む。

【００３２】

アクセスポイント１１４は、例示的には、通信システム１１０のアクセスネットワークの一部である。そのようなアクセスネットワークは、たとえば、複数の基地局および１つまたは複数の関連する無線ネットワーク制御機能を有するＮＧ－ＲＡＮシステムを含み得る。基地局および無線ネットワーク制御機能は、論理的に別々のエンティティであり得るが、所与の実施形態では、同一の物理ネットワーク要素に実装され得る。

【００３３】

この例示的な実施形態におけるアクセスポイント１１４は、モビリティ管理機能１１６に動作可能に結合される。５Ｇネットワークでは、モビリティ管理機能は、アクセスおよびモビリティ管理機能（ＡＭＦ：Ａｃｃｅｓｓ ａｎｄ Ｍｏｂｉｌｉｔｙ Ｍａｎａｇｅｍｅｎｔ Ｆｕｎｃｔｉｏｎ）によって実装される。セキュリティアンカー機能（ＳＥＡＦ：Ｓｅｃｕｒｉｔｙ Ａｎｃｈｏｒ Ｆｕｎｃｔｉｏｎ）をＡＭＦで実装して、ＵＥをモビリティ管理機能と接続することもできる。モビリティ管理機能とは、本明細書で使用する場合、ネットワーク動作の中でもとりわけ、（アクセスポイント１１４を介した）ＵＥに対するアクセスおよびモビリティ（認証／認可を含む）動作を管理するかまたは別の方法でこれに参加する通信システムのコアネットワーク（ＣＮ）部分における要素または機能（すなわち、エンティティ）である。ＡＭＦを本明細書ではより一般的に、アクセスおよびモビリティ管理ノードとも呼び得る。

【００３４】

この例示的な実施形態におけるＡＭＦ１１６は、追加の機能１１８に動作可能に結合される。図示のように、これらの機能の一部には、統合データ管理（ＵＤＭ：Ｕｎｉｆｉｅｄ Ｄａｔａ Ｍａｎａｇｅｍｅｎｔ）機能ならびに認証サーバ機能（ＡＵＳＦ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｓｅｒｖｅｒ Ｆｕｎｃｔｉｏｎ）が含まれる。ＡＵＳＦおよびＵＤＭを（個別にまたは集合的に）、本明細書ではより一般的に、認証ノードまたは複数の認証ノードとも呼び得る。追加の機能１１８には、セッション管理機能（ＳＭＦ）、ユーザプレーン機能（ＵＰＦ：Ｕｓｅｒ Ｐｌａｎｅ Ｆｕｎｃｔｉｏｎ）、ポリシー制御機能（ＰＣＦ：Ｐｏｌｉｃｙ Ｃｏｎｔｒｏｌ Ｆｕｎｃｔｉｏｎ）、およびネットワーク公開機能（ＮＥＦ）も含まれ得る。

【００３５】

ＵＥ１１２などのＵＥは、典型的には、機能１１６および１１８の一部または全てが存在するホーム公衆地上移動ネットワーク（ＨＰＬＭＮ）と呼ばれるものに加入していることに留意されたい。ＵＥがローミングしている（ＨＰＬＭＮにない）場合、典型的には、訪問先ネットワークとも呼ばれる訪問先公衆地上移動ネットワーク（ＶＰＬＭＮ）に接続され、ＵＥに現在サービス提供しているネットワークはサービングネットワークと呼ばれる。ローミングしている場合、ネットワーク機能１１６および１１８の一部はＶＰＬＭＮに存在し得、その場合、ＶＰＬＭＮ内の機能は必要に応じてＨＰＬＭＮ内の機能と通信する。しかしながら、ローミングしていないシナリオでは、モビリティ管理機能１１６および他のネットワーク機能１１８は同一の通信ネットワーク、すなわち、ＨＰＬＭＮに存在する。本明細書に記載の実施形態は、どの機能がどのＰＬＭＮ（すなわち、ＨＰＬＭＮまたはＶＰＬＭＮ）に存在するかによって制限されない。

【００３６】

そのようなネットワークのさらなる典型的な動作および機能についてはここでは説明せず、その理由は、それらが例示的な実施形態の焦点ではなく、適切な３ＧＰＰ ５Ｇ資料で見つかり得るためである。１１６および１１８に示す機能はネットワーク機能（ＮＦ：

ｎｅｔｗｏｒｋ　ｆｕｎｃｔｉｏｎ）の例であることに留意されたい。

【００３７】

システム要素のこの特定の配置は例にすぎず、他のタイプおよび配置の追加のまたは代替の要素を使用して、他の実施形態の通信システムを実装できることを理解されたい。たとえば、他の実施形態では、システム１１０は、本明細書に明示的に示していない他の要素／機能を含み得る。

【００３８】

したがって、図１Ｂの配置は、ワイヤレスセルラーシステムの１つの例示的な構成にすぎず、システム要素の多数の代替的な構成が使用され得る。たとえば、図１Ｂの実施形態では単一の機能のみを示しているが、これは説明を簡単かつ明確にするためのものにすぎない。所与の代替的な実施形態は、当然ながら、より多数のそのようなシステム要素、ならびに従来のシステム実装に一般的に関連するタイプの追加のまたは代替の要素を含み得る。

【００３９】

図１Ｂではシステム要素を単機能のブロックとして示しているが、５Ｇネットワークを構成する様々なサブネットワークがいわゆるネットワークスライスに分割されることにも留意されたい。ネットワークスライス（ネットワークパーティション）は、共通の物理インフラストラクチャ上でのネットワーク機能仮想化（ＮＦＶ：ｎｅｔｗｏｒｋ　ｆｕｎｃｔｉｏｎ　ｖｉｒｔｕａｌｉｚａｔｉｏｎ）を使用した対応するサービスタイプごとの一連のネットワーク機能（ＮＦ）セット（すなわち、機能チェーン）を含む。ネットワークスライスは、たとえば、ｅＭＢＢサービス、大規模ＩｏＴサービス、およびミッションクリティカルなＩｏＴサービスなどの所与のサービスのために必要に応じてインスタンス化される。このため、ネットワークスライスまたは機能は、そのネットワークスライスまたは機能のインスタンスが作成されるときに、インスタンス化される。いくつかの実施形態では、これには、基盤となる物理インフラストラクチャの１つまたは複数のホストデバイス上にネットワークスライスまたは機能をインストールするかまたは別の方法で動作させることが含まれる。ＵＥ１１２は、ｇＮＢ１１４を介してこれらのサービスのうちの１つまたは複数にアクセスするように構成される。

【００４０】

図２は、例示的な実施形態における、ユーザ機器（ＵＥ）と、通信システムにおいて認証／認可を提供するかまたは別の方法でこれに参加するためのネットワークノードとのブロック図である。ユーザ機器２０２およびネットワークノード２０４を含むシステム２００を示している。

【００４１】

ユーザ機器２０２は、例示的な実施形態ではＵＡＳを含むＵＥ１０２（図１Ａ）またはＵＥ１１２（図１Ｂ）の一例を表すことに留意されたい。ネットワークノード２０４は、セキュリティ管理および本明細書に記載の他の技術を提供するように構成される任意のネットワークエンティティおよび／または任意のネットワーク機能、ならびに他の任意のネットワークコンポーネント、要素、サービスなどを表し、たとえば、限定はしないが、ＳＢＡベースの５Ｇコアネットワーク（図１Ｂ）の一部であるようなＡＭＦ、ＳＥＡＦおよびＵＤＭ、またはＥＰＳベースの４Ｇコアネットワーク（図１Ａ）の一部であるようなＭＭＥ、ＨＳＳおよびＡｕＣを表すことをさらに理解されたい。

【００４２】

ネットワークノード２０４は、コアネットワークの外部の、すなわち、サードパーティの外部企業ネットワークのネットワークエンティティ、機能、ノード、コンポーネント、要素、サービスなどとすることもできる。さらに、ネットワークノード２０４は、コアネットワークまたは任意の通信ネットワークもしくはシステム内の１つまたは複数のネットワークエンティティまたは機能のインスタンス化を指揮および管理するように構成される１つまたは複数の処理デバイスを表すことができる。ネットワークノード２０４は、ＵＡＳの認証／認可に直接または間接的に関与する他の任意のエンティティ／機能とすること

ができ、これについては、たとえば、上記で参照したＴＳ２３．２５６およびＴＳ２２．１２５に記載され得、および／または以下で別途説明し得る。例として、ＤＮ－ＡＡＡによる二次ＤＮ認証／認可の場合、ネットワークノード２０４はＤＮ－ＡＡＡサーバとすることができる。

【００４３】

ユーザ機器２０２は、メモリ２１６およびインターフェース回路２１０に結合されたプロセッサ２１２を含む。ユーザ機器２０２のプロセッサ２１２は、プロセッサによって実行されるソフトウェアの形態で少なくとも部分的に実装され得るセキュリティ管理処理モジュール２１４を含む。処理モジュール２１４は、以降の図および本明細書の他の部分に関連して説明するセキュリティ管理に関連する動作を実行する。ユーザ機器２０２のメモリ２１６は、セキュリティ管理動作中に生成されるかまたは別の方法で使用されるデータを記憶するセキュリティ管理ストレージモジュール２１８を含む。

【００４４】

ネットワークノード２０４は、メモリ２２６およびインターフェース回路２２０に結合されたプロセッサ２２２を含む。ネットワークノード２０４のプロセッサ２２２は、プロセッサ２２２によって実行されるソフトウェアの形態で少なくとも部分的に実装され得るセキュリティ管理処理モジュール２２４を含む。処理モジュール２２４は、以降の図および本明細書の他の部分に関連して説明するセキュリティ管理に関連する動作を実行する。ネットワークノード２０４のメモリ２２６は、セキュリティ管理動作中に生成されるかまたは別の方法で使用されるデータを記憶するセキュリティ管理ストレージモジュール２２８を含む。

【００４５】

プロセッサ２１２および２２２は、たとえば、マイクロプロセッサ、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）、デジタル信号プロセッサ（ＤＳＰ）、または他のタイプの処理デバイスもしくは集積回路、ならびにそのような要素の一部または組み合わせを含み得る。そのような集積回路デバイス、ならびにその一部または組み合わせは、「回路」という用語を本明細書で使用する場合、「回路」の例である。ハードウェアおよび関連するソフトウェアまたはファームウェアの多種多様な他の配置が、例示的な実施形態を実装する際に使用され得る。また、例示的な実施形態は、様々なネットワーク機能をエミュレートするためにクラウドプラットフォーム上で動作するソフトウェアを使用する完全に仮想化された環境で実現され得る。

【００４６】

メモリ２１６および２２６は、本明細書に記載の機能の少なくとも一部を実装するためにそれぞれのプロセッサ２１２および２２２によって実行される１つまたは複数のソフトウェアプログラムを記憶するために使用され得る。たとえば、以降の図および本明細書の他の部分に関連して説明するセキュリティ管理動作および他の機能は、プロセッサ２１２および２２２によって実行されるソフトウェアコードを使用して簡単な方法で実装され得る。

【００４７】

そのため、メモリ２１６または２２６のうちの所与の１つは、より一般的にはコンピュータプログラム製品と呼ばれるもの、またはさらにより一般的には、実行可能なプログラムコードが内部に具現化されたプロセッサ可読記憶媒体と本明細書で呼ばれるものの一例とみなされ得る。プロセッサ可読記憶媒体の他の例には、任意の組み合わせでのディスクまたは他のタイプの磁気もしくは光学媒体が含まれ得る。例示的な実施形態は、そのようなコンピュータプログラム製品または他のプロセッサ可読記憶媒体を含む製造品を含むことができる。

【００４８】

メモリ２１６または２２６は、より詳細には、たとえば、スタティックＲＡＭ（ＳＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）などの電子ランダムアクセスメモリ（ＲＡＭ）、または他のタイプの揮発性もしくは不揮発性電子メモリを含み得る。後者には、たとえば

、フラッシュメモリ、磁気ＲＡＭ（ＭＲＡＭ）、相変化ＲＡＭ（ＰＣ－ＲＡＭ）、または強誘電体ＲＡＭ（ＦＲＡＭ）などの不揮発性メモリが含まれ得る。本明細書で使用する「メモリ」という用語は、広く解釈されることを意図しており、追加的または代替的には、たとえば、読み取り専用メモリ（ＲＯＭ）、ディスクベースのメモリ、または他のタイプのストレージデバイス、ならびにそのようなデバイスの一部または組み合わせを包含し得る。

【００４９】

インターフェース回路２１０および２２０は、例示的には、関連付けられたシステム要素が本明細書に記載のように相互に通信することを可能にする送受信器または他の通信ハードウェアもしくはファームウェアを含む。

【００５０】

ユーザ機器２０２がネットワークノード２０４とそれぞれのインターフェース回路２１０および２２０を介して通信するように構成され、逆も同様であることは図２から明らかである。この通信には、ユーザ機器２０２がネットワークノード２０４にデータを送信することと、ネットワークノード２０４がユーザ機器２０２にデータを送信することとが含まれる。しかしながら、代替的な実施形態では、他のネットワークノードが、ユーザ機器２０２およびネットワークノード２０４の間に動作可能に結合され得る。本明細書で使用する「データ」という用語は、ユーザ機器およびネットワークノードの間、ならびにネットワークエンティティ間で送信され得る任意のタイプの情報、たとえば、限定はしないが、メッセージ、識別子、キー、インジケータ、ユーザデータ、制御データなどを包含するように広く解釈されることを意図している。

【００５１】

図２に示すコンポーネントの特定の配置は一例にすぎず、他の実施形態では多数の代替的な構成が使用され得ることを理解されたい。たとえば、任意の所与のネットワークノードは、追加のまたは代替のコンポーネントを組み込み、他の通信プロトコルをサポートするように構成することができる。

【００５２】

ｅＮＢ１０４およびｇＮＢ１１４などの他のシステム要素のそれぞれも、プロセッサ、メモリおよびネットワークインターフェースなどのコンポーネントを含むように構成され得る。これらの要素は、別々のスタンドアローンの処理プラットフォーム上に実装される必要はなく、代わりに、単一の共通の処理プラットフォームの異なる機能的部分を表すことができる。

【００５３】

またさらに、図２はユーザ機器およびネットワークノードの間の例示的なアーキテクチャおよび相互接続を示しているが、図２は複数のネットワークノード間の例示的なアーキテクチャおよび相互接続を表すこともできる（たとえば２０２は、ネットワークノード２０４の形態の他のネットワークノードに動作可能に結合される、あるネットワークノードを表すことができる）。より一般的には、図２は、それぞれのセキュリティ管理機能を提供するように構成され、通信システムにおいて互いに動作可能に結合された２つの処理デバイスを表すものとみなすことができる。

【００５４】

上記のように、ＴＳ２３．２５６では、ＴＳ２２．１２５で規定されたユースケースおよびサービス要件に従う、ＵＡＳ接続、識別、および追跡をサポートするための４Ｇ／５Ｇネットワークへのアーキテクチャ拡張が示されている。

【００５５】

図３は、１つまたは複数の例示的な実施形態が実装され得る、ＴＳ２３．２５６に記載されているＵＡＳアプリケーションのための４Ｇおよび５Ｇ通信ネットワークの複合アーキテクチャ３００を示している。概略的に示しているように、ＵＥ（ＵＡＳ内）３０２は、５ＧＣ３０６（５Ｇコアネットワーク）にアクセスするためにＮＧ－ＲＡＮ３０４（５Ｇアクセスネットワーク）を介して複合アーキテクチャ３００に動作可能に結合され得る

。同様に、ＵＥ（ＵＡＳ内）３０２は、ＥＰＣ３１０（４Ｇコアネットワーク）にアクセスするためにＥ－ＵＴＲＡＮ（４Ｇアクセスネットワーク）などのＲＡＮ３０８を介して複合アーキテクチャ３００に動作可能に結合され得る。ＵＡＳ　ＮＦ／ＮＥＦ３１２は、５ＧＣ３０６および／またはＥＰＣ３１０に動作可能に結合されるか、または別の方法でそれらの一部として組み込まれる。ＵＡＳ　ＮＦ／ＮＥＦは、データネットワーク３１６（たとえば、ＰＤＮ）にアクセスするためにＵＳＳ３１４に動作可能に結合される。ＴＰＡＥ３１８はデータネットワーク３１６に動作可能に結合される。図３のＮ、ＳおよびＳＧの参照符号は、ネットワークノードを接続するために使用される特定の３ＧＰＰインターフェースに対応することに留意されたい。

【００５６】

図４は、図３の複合アーキテクチャ３００のさらなる詳細を示す複合アーキテクチャ４００を示している。図示のように、同じまたは異なるＵＥとすることができるＵＥ４０２－１およびＵＥ４０２－２は、それぞれＥ－ＵＴＲＡＮ４０４およびＮＧ－ＲＡＮ４０６を介して複合アーキテクチャ４００に接続する。複合アーキテクチャ４００は、４Ｇアクセスおよびモビリティコントローラ ＭＭＥ４０８、５Ｇアクセスおよびモビリティコントローラ ＡＭＦ４１０、ＳＧＷ４１２、ユーザプレーンコントローラ４１４（４Ｇ用のＰＧＷ－Ｕおよび５Ｇ用のＵＰＦ）、制御プレーンコントローラ４１６（４Ｇ用のＰＧＷ－Ｃおよび５Ｇ用のＳＭＦ）、ＰＣＦ４１８、認証コントローラ４２０（４Ｇ用のＨＳＳおよび５Ｇ用のＵＤＭ）、ならびにＵＡＳ　ＮＦ／ＮＥＦ４２２を含む。ＵＡＳネットワーク機能（ＵＡＳ　ＮＦ）は、ＮＥＦによってサポートされ、ＵＳＳ（すなわち、図３のＵＳＳ３１４）へのサービスの外部公開のために使用される。これらのおよび他のネットワークノードについては、以下で図５のコンテキストでさらに説明する。

【００５７】

ＴＳ２３．２５６によると、航空レベルで、ＵＡＳは民間航空局（ＣＡＡ：Ｃｉｖｉｌ Ａｖｉａｔｉｏｎ Ａｕｔｈｏｒｉｔｙ）レベルのＵＡＶ識別情報（ＩＤ）によって識別される。通常の／一次ＵＥ認証／認可に加えて、３ＧＰＰシステムはまた、ネットワーク内の航空機ＵＥへのあらゆるサービスを許可する前に、ＵＡＳサービスサプライヤ（ＵＳＳ）／ＵＡＳトラフィック管理（ＵＴＭ）によってＵＡＶ識別情報（ＣＡＡレベルのＵＡＶ　ＩＤ）の認証／認可を実行し得る。５ＧＳの場合、ＣＡＡレベルのＵＡＶ　ＩＤの認証／認可は、５ＧＳ登録時またはパケットデータユニット（ＰＤＵ）セッション確立中に実行され得る。ＥＰＳの場合、ＵＡＶ認証／認可は、ＰＤＮ接続確立中に実行される。

【００５８】

さらに、ＴＳ２３．２５６では、ＥＰＳアタッチ時のデフォルトＰＤＮ接続中のＵＳＳ ＵＡＶ認可／認証（ＵＵＡＡ）が定義されている。３ＧＰＰ　Ｒｅｌ－１７では、二次ＤＮ認証／認可もＴＳ２３．５０１に定義されている。

【００５９】

ＵＳＳ　ＵＡＶ認可／認証（ＵＵＡＡ）および二次ＤＮ認証／認可のそれぞれの間の認証／認可手順は、ＵＥおよび認証エンティティ（ＵＳＳ／ＵＴＭまたはＤＮ　ＡＡＡサーバ）の間での認証関連メッセージ交換の複数回の往復を必要とし得る。ＥＰＣを介して、ＵＥがＰＤＮ接続の確立を要求する場合、４Ｇ　ＮＡＳおよびＳ１１／Ｓ５／Ｓ８シグナリングは、ＵＥ要求およびＰＤＮ接続が確立された（ＮＡＳデフォルトベアラ有効化）というネットワーク回答以外の、ＵＥおよびＰＧＷ（ＰＤＮ　ＧＷ）の間の追加のシグナリングの交換を想定していない。

【００６０】

ＴＳ２３．２５６で定義された手順によると、デフォルトベアラ有効化後、認証エンティティ（ＵＡＳの場合はＵＳＳ／ＵＴＭ、または二次ＤＮ認証／認可の場合はＤＮ　ＡＡＡサーバ）から認証成功応答を取得するまで、デフォルトベアラ上のあらゆるトラフィックを停止するように、アクセス制御がＰＧＷ（ＰＤＮ　ＧＷ）で適用される。しかしながら、ＰＤＮ接続がアップリンクデータ転送に使用できないことにＵＥが気付かないということを本明細書で認識した。この状態により、ＵＥが意図するようにアップリンクデータ

をＰＤＮに転送できない場合でも、ＵＥはアップリンクデータ転送を実行しようとする。その結果、ＵＥの処理能力だけでなくネットワークリソースが浪費され、ＵＥアプリケーションは、データネットワークへのアクセスを開始できると誤って想定し得る。

【００６１】

例示的な実施形態は、上記および他の課題を克服するための解決策を提供する。ＰＤＮ接続（すなわち、ＥＰＣを介したもの）の確立時に二次ＤＮ認証／認可またはＳＭレベルＵＵＡＡが適用される場合、ネットワーク（ＰＧＷ）は、二次ＤＮ認証／認可またはＳＭレベルＵＵＡＡが成功するという条件でＰＤＮ接続が確立されることをＵＥに通知する。例示的な実施形態によれば、二次ＤＮ認証／認可またはＳＭレベルＵＵＡＡが成功したことをネットワーク（たとえば、ＰＧＷ）がＵＥに通知するまで、ＵＥはアップリンクデータをネットワークに送信することはない（またはそのようなデータを送信した場合、それらはネットワークによって破棄され得る）。

【００６２】

ＴＳ２３．２５６によれば、ＵＵＡＡ－ＭＭは、５ＧＳへの登録中に任意に実行されてもよいＵＵＡＡ手順を指し、ＵＵＡＡ－ＳＭは、（ＵＵＡＡ－ＭＭが実行されない場合に）ＰＤＵセッションの確立中に実行されてもよく、ＰＤＮ接続の確立中に実行されてもよいＵＵＡＡ手順を指す。

【００６３】

図５は、ＰＤＮ接続確立時に実行される（すなわち、ＥＰＣ用の）ＳＭレベルＵＵＡＡを実行するためのメッセージフロー５００を示している。図５にはＳＭレベルＵＵＡＡ手順のみを示しているが、例示的な実施形態は、ＤＮ－ＡＡＡによる二次ＤＮ認証／認可に等しく適用可能である（たとえば、ＥＡＰ／ＴＬＳを使用して、ＵＥがデータネットワーク上のＡＡＡサーバによって認証および認可されるようにする）。図示のように、メッセージフロー５００には、ＵＥ５０２、ＲＡＮ５０４、ＭＭＥ５０６、ＳＧＷ５０８、ＳＭＦ＋ＰＧＷ－Ｃ５１０およびＰＧＷ－Ｕ５１２として表されるＰＧＷ、ＵＡＳ　ＮＦ／ＮＥＦ５１４、ならびにＵＳＳ５１６が関与する。

【００６４】

一般に、ＵＥ５０２はまず、通信ネットワークの認証情報に基づいて（たとえば、汎用加入者識別モジュール（ＵＳＩＭ：Ｕｎｉｖｅｒｓａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）ベースの認証を使用して）通信ネットワークによって認証される（４ＧネットワークではＭＭＥ５０６によって行われる）。これが完了した場合、通信ネットワークは、データネットワークへの接続のＵＥ要求の検討を開始する（ここではデータネットワークに関連する他の認証情報が考慮され得る）。

【００６５】

ステップ１において、たとえば、ＴＳ２３．４０１の図５．３．２．１－１のステップ１～１３およびＴＳ２３．５０２図４．１１．１．５．２－１のステップ１～２またはＴＳ２３．５０２節４．１１．２．４．１のように、ＵＥ５０２がＥＰＳアタッチ手順を開始する。ＵＥ５０２はアタッチ要求内にサービスレベルデバイス識別情報（たとえば、ＵＡＶの場合はＣＡＡレベルのＵＡＶ　ＩＤ）を含め、認証エンティティ（すなわち、ＵＡＶの場合はＵＳＳ５１６、または二次ＤＮ認証／認可の場合はＤＮ－ＡＡＡサーバ）によって求められた場合には、認証データをプロトコル設定オプション（ＰＣＯ）内に含め得る。

【００６６】

ステップ２において、ＰＧＷ（５ＧＣ－ＥＰＣが相互接続する場合はＳＭＦ＋ＰＧＷ－Ｃ５１０）は、ＰＤＮ接続要求が認証エンティティ／サーバ（すなわち、ＵＡＶの場合はＵＳＳ５１６、または二次ＤＮ認証／認可の場合はＤＮ－ＡＡＡサーバ）によって認証／認可される必要があると判定し、デフォルトＰＤＮ接続を介したあらゆるトラフィックを停止するようにアクセス制御リスト（ＡＣＬ：Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ　Ｌｉｓｔ）を設定する。

【００６７】

ステップ３において、たとえば、ＴＳ２３．４０１図５．３．２．１－１のステップ１４～２２のように、アタッチ手順が完了し、その後、ＳＭレベルＵＵＡＡ（すなわち、ＵＵＡＡ－ＳＭ）手順（またはＤＮ－ＡＡＡによる二次ＤＮ認証／認可）が呼び出される。アタッチ手順中に、ＴＳ２３．４０１の図５．３．２．１－１のステップ１５のようにＰＧＷ（ＳＭＦ＋ＰＧＷ－Ｃ５１０）がセッション作成応答を返すときに、ＰＧＷは、ＰＤＮ接続上でアップリンクデータ伝送がまだ許可されていないというＵＥ５０２への表示（ｉｎｄｉｃａｔｉｏｎ）をＰＣＯ（プロトコル設定オプション）内に含める。これが行われた結果、ネットワークがアタッチアクセプトを送信する前にＭＭＥ５０６はＮＡＳ ＳＭトランスポートをＵＥ５０２と交換することができないので、ＵＥ５０２およびＵＥ５０２を認証する認証エンティティ／サーバ（ＵＳＳ５１６またはＤＮ ＡＡＡサーバ）の間で認証関連メッセージ交換の複数回の往復の可能性が実現される。アタッチ完了（およびデフォルトベアラ有効化）後、ＵＥ５０２が「アップリンクデータ伝送が許可されていない」という表示（すなわち、第１の通知）を受信した場合、ＵＥは、ＰＤＮ接続上で「アップリンクデータ伝送が許可されている」という表示（すなわち、第２の通知）をネットワークからさらに受信するまで、アップリンクデータをネットワークに送信しない（すなわち、送信を控える）。

【００６８】

ステップ４において、ＰＧＷ（ＳＭＦ＋ＰＧＷ－Ｃ５１０）は認証／認可手順を開始する。メッセージフロー５００（すなわち、ＵＵＡＡ－ＳＭ用）において、これは３ＧＰＰ ＴＳ２３．２５６の図５．２．３．２－１のステップ１～２に記載された認証／認可手順に従う。二次ＤＮ認証の場合、ＰＧＷは、ＤＮ－ＡＡＡによるＰＤＵセッション確立認証／認可のためのＴＳ２３．５０２図４．３．２．３－１のステップ２および３に従う。

【００６９】

ステップ５において、認証エンティティ／サーバ（たとえば、ＵＳＳ５１６またはＤＮ－ＡＡＡ）によって使用される認証方法によって必要とされる複数の往復メッセージが存在し得る。認証エンティティ／サーバ（たとえば、ＵＳＳ５１６またはＤＮ－ＡＡＡ）からの認証メッセージを含むＰＣＯが、ＰＧＷ（ＳＭＦ＋ＰＧＷ－Ｃ５１０）によってベアラ更新要求およびダウンリンクＮＡＳトランスポート内でＵＥ５０２に転送される（ステップ５ｂ～５ｄ）。ＵＥ５０２からの応答は、アップリンクＮＡＳトランスポートおよびベアラ更新応答内でＰＧＷ（ＳＭＦ＋ＰＧＷ－Ｃ５１０）に転送される（ステップ５ｅ～５ｇ）。ＰＣＯおよびベアラ更新手順を使用することにより、ＭＭＥ５０６への影響を最小限にすること、およびＳＧＷ５０８に影響を与えないことが可能になる。

【００７０】

ステップ６において、認証エンティティ／サーバによる認証／認可処理が完了し、認証／認可結果が受信される。メッセージフロー５００（すなわち、ＵＵＡＡ用）において、これは３ＧＰＰ ＴＳ２３．２５６の図５．２．３．２－１のステップ４～５に記載された認証／認可手順に従う。

【００７１】

ＵＵＡＡ－ＳＭ（またはＤＮ－ＡＡＡによる二次ＤＮ認証／認可）が成功した後、ステップ７において、ＰＧＷ（ＳＭＦ＋ＰＧＷ－Ｃ５１０）はＰＤＮ接続を介したトラフィックを許可するようにＡＣＬを更新する。

【００７２】

さらに、ステップ８において、ＰＧＷ（またはＳＭＦ＋ＰＧＷ－Ｃ５１０）は、ＰＤＮ接続上でアップリンクデータ伝送が現在許可されているというＵＥ５０２への表示をＰＣＯに含めて、ベアラ更新要求を送信する。ＰＧＷ（ＳＭＦ＋ＰＧＷ－Ｃ５１０）はまた、認証／認可結果と、ＵＥ５０２に転送される必要がある認可データとを含め得る。

【００７３】

有利なことに、本明細書に示したように、例示的な実施形態はまず、通信ネットワークの認証情報に基づいて（たとえば、ＵＳＩＭベースの認証を使用して）通信ネットワークによってＵＥが認証される（４Ｇネットワークではまず）ことを可能

にする。これが完了した場合、通信ネットワークは、データネットワークへの接続のＵＥ要求の検討を開始する。データネットワークへの接続のＵＥ要求の処理の一部として、通信ネットワークはデータネットワークへのアップリンクデータ転送が許可されていないという第１の通知を送信し、次いで、データネットワークによる認証がデータネットワーク識別子に基づいて行われ、その後、通信ネットワークはデータネットワークへのアップリンクデータ転送が許可されているという第２の通知を送信する。たとえば、ＵＡＳの場合、ＵＥはＣＡＡレベルのＩＤを提示し、これはサービスレベルのデバイス識別情報と呼ばれ得る。ＤＮ－ＡＡＡベースの二次ＤＮ認証／認可の場合、この識別情報はＤＮ固有の識別情報と呼ばれ得る。

【００７４】

本明細書における本発明の教示が与えられた場合、ＤＮ－ＡＡＡによる二次ＤＮ認証／認可のための類似のメッセージフローを簡単な方法で実現することができる。より詳細には、５ＧＳにおけるＰＤＵセッションの確立中のＤＮ－ＡＡＡサーバによる二次認証／認可の手順がＴＳ２３．５０１およびＴＳ２３．５０２に記載されている。ＥＰＣ（相互接続）の場合の二次ＤＮ認証および認可のサポートも現在、５ＧＣ－ＥＰＣ相互接続のための課題／ギャップと考えられている。そのため、例示的な実施形態は、より一般的に任意のＵＥに実装されることを意図している（すなわち、必ずしもＵＡＳに実装されるＵＥに限らない）。

【００７５】

本明細書に記載の図と共に説明した特定の処理動作および他のシステム機能は、説明用の例として提示しているにすぎず、いかなる方法でも本開示の範囲を限定するものと解釈されるべきではない。代替的な実施形態は、他のタイプの処理動作およびメッセージングプロトコルを使用することができる。たとえば、ステップの順序は他の実施形態では変更され得、または特定のステップは順次的にではなく少なくとも部分的に互いと同時に実行され得る。また、ステップのうちの１つまたは複数は定期的に繰り返され得、または方法の複数のインスタンスを互いと並行して実行することができる。

【００７６】

本明細書に記載の様々な実施形態は説明用の例として提示しているにすぎず、特許請求の範囲を限定するものとして解釈されるべきではないということを再度強調すべきである。たとえば、代替的な実施形態は、例示的な実施形態のコンテキストで上述したものとは異なる通信システム構成、ユーザ機器構成、基地局構成、プロビジョニングおよび使用プロセス、メッセージングプロトコルおよびメッセージフォーマットを利用することができる。添付の特許請求の範囲内のこれらおよび他の多数の代替的な実施形態は、当業者には容易に明らかになろう。

【符号の説明】

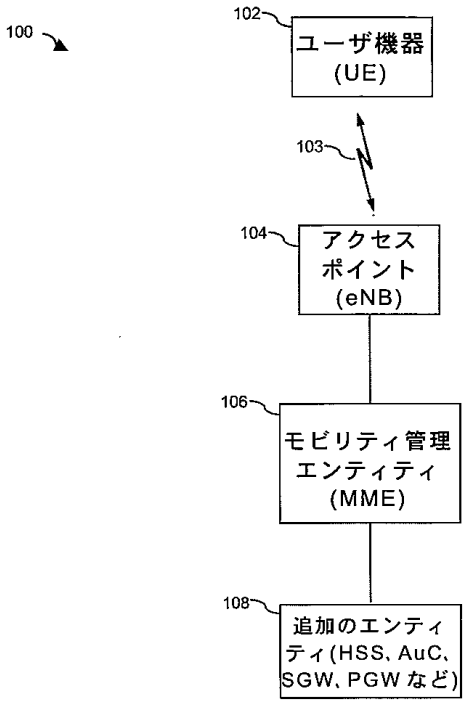
【００７７】

１００　４Ｇ通信システム
１０２　ユーザ機器（ＵＥ）
１０３　エアインターフェース
１０４　アクセスポイント（ｅＮＢ）
１０６　モビリティ管理エンティティ（ＭＭＥ）
１０８　追加のネットワークエンティティ
１１０　５Ｇ通信システム
１１２　ユーザ機器（ＵＥ）
１１３　エアインターフェース
１１４　アクセスポイント（ｇＮＢ）
１１６　モビリティ管理機能（ＡＭＦ／ＳＥＡＦ）
１１８　追加の機能
２００　システム
２０２　ユーザ機器

２１０　インターフェース回路
２１２　プロセッサ
２１４　セキュリティ管理処理
２１６　メモリ
２１８　セキュリティ管理ストレージ
２０４　ネットワークノード（エンティティ／機能）
２２０　インターフェース回路
２２２　プロセッサ
２２４　セキュリティ管理処理
２２６　メモリ
２２８　セキュリティ管理ストレージ
３００　複合アーキテクチャ
３０２　ＵＥ
３０４　ＮＧ－ＲＡＮ
３０８　（Ｒ）ＡＮ
３１２　ＵＡＳ　ＮＦ／ＮＥＦ
３０６　５ＧＣ
３１０　ＥＰＣ
３１４　ＵＳＳ
３１６　データネットワーク
３１８　ＴＰＡＥ
４００　複合アーキテクチャ
４０２－１　ＵＥ
４０４　Ｅ－ＵＴＲＡＮ
４０８　ＭＭＥ
４１２　ＳＧＷ
４１４　ＵＰＦ＋ＰＧＷ－Ｕ
４１６　ＳＭＦ＋ＰＧＷ－Ｃ
４１８　ＰＣＦ
４２０　ＨＳＳ＋ＵＤＭ
４２２　ＵＡＳ　ＮＦ／ＮＥＦ
４１０　ＡＭＦ
４０６　ＮＧ－ＲＡＮ
４０２－２　ＵＥ
５００　メッセージフロー
５０２　ＵＥ（ＵＡＶ）
５０４　（Ｒ）ＡＮ
５０６　ＭＭＥ
５０８　ＳＧＷ
５１０　ＳＭＦ＋ＰＧＷ－Ｃ
５１２　ＰＧＷｕ
５１４　ＵＡＳ　ＮＦ／ＮＥＦ
５１６　ＵＳＳ

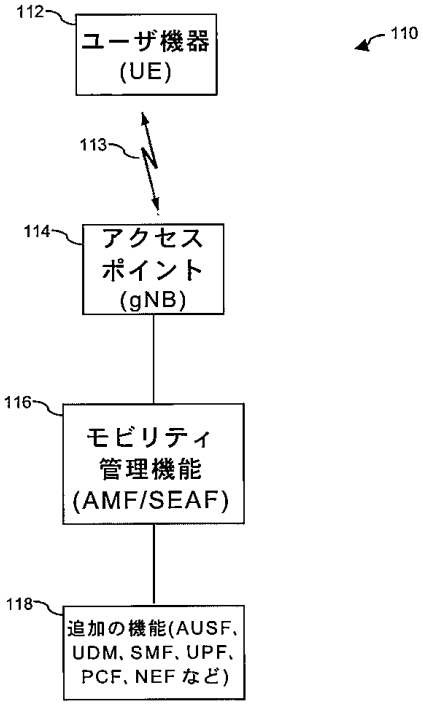
【図面】

【図１Ａ】



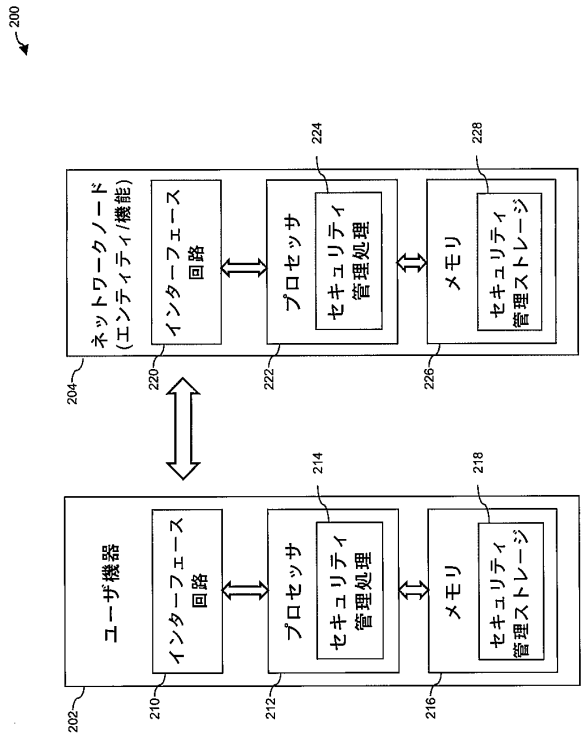
4G ネットワーク
の一部

【図１Ｂ】

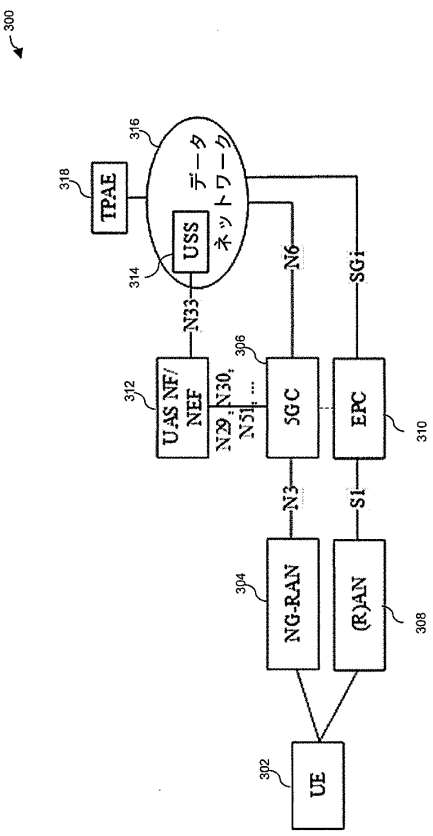


5G ネットワーク
の一部

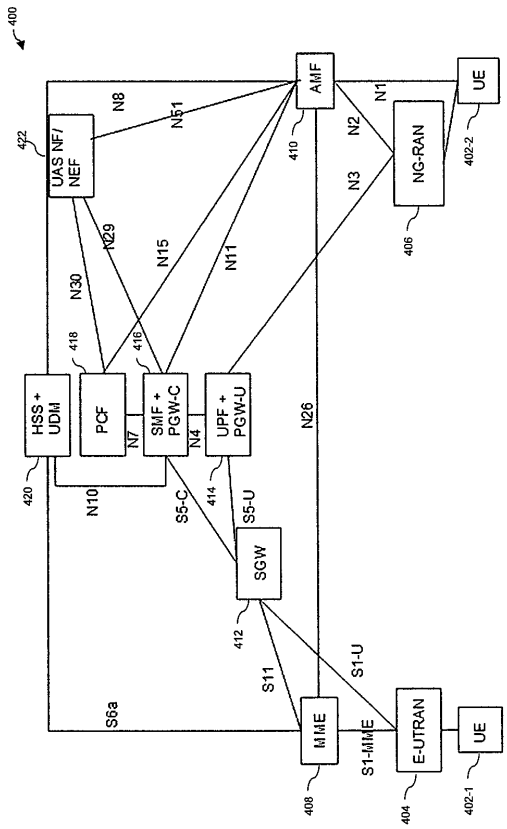
【図２】



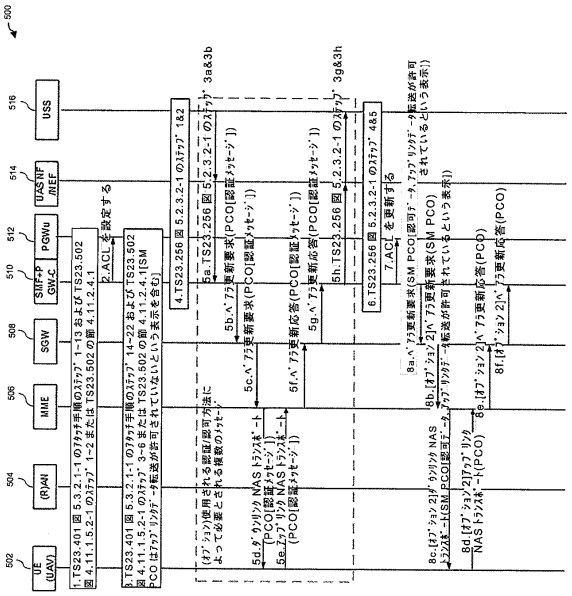
【図３】



【図４】


400
AMF
410
UE
402-2
NG-RAN
406
UAS NF/
NEF
422
N8
N51
N1
N2
N3
N29
N15
N11
N30
418
416
HSS +
UDM
PCF
SMF +
PGW-C
UPF +
PGW-U
N26
420
N7
N4
N10
S5-C
414
S5-U
SGW
412
S11
S1-U
S6a
MME
408
S1-MME
E-UTRAN
404
UE
402-1

【図５】


500
UE
(UAV)
502
(R)AN
504
MME
506
SGW
508
SMF+P
GW-C
510
PGWu
512
UAS NF
/NEF
514
USS
516
1. TS23.401 図 5.3.2.1-1 のステップ 1-13 および TS23.502 図 4.11.1.5.2-1 のステップ 1-2 または TS23.502 の節 4.11.2.4.1
2. ACL を設定する
3. TS23.401 図 5.3.2.1-1 のステップ 14-22 および TS23.502 図 4.11.1.5.2-1 のステップ 3-6 または TS23.502 の節 4.11.2.4.1 (SM PCO はアプリケーション転送が許可されている表示を含む)
4. TS23.256 図 5.2.3.2-1 のステップ 1&2
5a. TS23.256 図 5.2.3.2-1 のステップ 3a&3b
5b. ﾌﾗｲ更新要求(PCO[認証ﾒｯｾｰｼﾞ])
5c. ﾌﾗｲ更新要求(PCO[認証ﾒｯｾｰｼﾞ])
5d. ダウンリンク NAS トランスポート (PCO[認証ﾒｯｾｰｼﾞ])
5e. アップリンク NAS トランスポート (PCO[認証ﾒｯｾｰｼﾞ])
5f. ﾊﾞﾌﾗｲ更新応答(PCO[認証ﾒｯｾｰｼﾞ])
5g. ﾊﾞﾌﾗｲ更新応答(PCO[認証ﾒｯｾｰｼﾞ])
5h. TS23.256 図 5.2.3.2-1 のステップ 3g&3h
6. TS23.256 図 5.2.3.2-1 のステップ 4&5
7. ACL を更新する
8a. ﾊﾞﾌﾗｲ更新要求(SM PCO[認可ｿﾌﾄｳｪｱ・ｱﾌﾟﾘｹｰｼｮﾝ転送が許可されている表示])
8b. [ﾊﾞﾌﾟｼｮﾝ2] ﾊﾞﾌﾗｲ更新要求(SM PCO)
8c. [ﾊﾞﾌﾟｼｮﾝ2] ﾀﾞｳﾝﾘﾝｸ NAS ﾄﾗﾝｽﾎﾟｰﾄ(SM PCO[認可ｿﾌﾄｳｪｱ・ｱﾌﾟﾘｹｰｼｮﾝ転送が許可されている表示])
8d. [ﾊﾞﾌﾟｼｮﾝ2] ｱｯﾌﾟﾘﾝｸ NAS ﾄﾗﾝｽﾎﾟｰﾄ(PCO)
8e. [ﾊﾞﾌﾟｼｮﾝ2] ﾊﾞﾌﾗｲ更新応答(PCO)
8f. [ﾊﾞﾌﾟｼｮﾝ2] ﾊﾞﾌﾗｲ更新応答(PCO)

フロントページの続き

弁理士　上杉 浩
(74)代理人　100120525
弁理士　近藤 直樹
(74)代理人　100139712
弁理士　那須 威夫
(72)発明者　ロラン ティエボー
フランス ９２１６０ アントニー リュー ラシーヌ ３４
(72)発明者　パラブ グプタ
インド ５６００８７ バンガロール グンジュール プレステージ レイクサイド ハビタット ２２０８２

審査官　永田 義仁

(56)参考文献　特表２０２０－５０５８５８（ＪＰ，Ａ）
3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2 (Release 17)，3GPP TS 23.256 V1.0.0 (2021-06)，2021年06月07日，p.10-12,26-27，Internet〈URL:https://www.3gpp.org/ftp/Specs/archive/23_series/23.256/23256-100.zip〉，[検索日２０２３年９月２２日]
Nokia, Nokia Shanghai Bell，KI#2, Sol #23: Updates to clarify on interfacing with USS/UTM [online]，3GPP TSG SA WG2 #141e S2-2008265，Internet〈URL:https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_141e_Electronic/Docs/S2-2008265.zip〉，2020年10月23日

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ７／２４－７／２６
Ｈ０４Ｗ４／００－９９／００
３ＧＰＰ ＴＳＧ ＲＡＮ ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１、４