(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7533671号
(P7533671)

(45)発行日　令和6年8月14日(2024.8.14)

(24)登録日　令和6年8月5日(2024.8.5)

(51)国際特許分類

| | | | |
|---|---|---|---|
| *H04W 12/06 (2021.01)* | | H04W | 12/06 |
| *H04W 76/20 (2018.01)* | | H04W | 76/20 |

FI

請求項の数　8　（全47頁）

(21)出願番号　特願2023-65476(P2023-65476)
(22)出願日　令和5年4月13日(2023.4.13)
(62)分割の表示　特願2021-567405(P2021-567405)の分割
原出願日　令和2年12月18日(2020.12.18)
(65)公開番号　特開2023-80266(P2023-80266A)
(43)公開日　令和5年6月8日(2023.6.8)
審査請求日　令和5年4月13日(2023.4.13)
(31)優先権主張番号　特願2019-237391(P2019-237391)
(32)優先日　令和1年12月26日(2019.12.26)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103894
弁理士　家入 健
(72)発明者　田村 利之
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　高倉 強
東京都台東区竜泉二丁目７番７号 株式会社クラップアンドクランク内
審査官　望月 章俊

最終頁に続く

(54)【発明の名称】　モビリティ管理ノード、ユーザ機器、及びこれらの方法

(57)【特許請求の範囲】

【請求項１】

コアネットワークにおけるモビリティ管理ノードであって、

S-NSSAI（Single-Network Slice Selection Assistance Information）に対する再NSSAA（Network Slice Specific Authentication and Authorization）手順をトリガーする手段と、

前記再NSSAA手順において、タイマーを起動する手段と、

前記タイマーが満了したことに基づいて、前記再NSSAA手順における認証が失敗したと判断する手段と、

前記NSSAAが失敗した場合に、前記S-NSSAIに関するPDU（Protocol Data Unit）SessionのRelease手続きを起動する手段と、

を有する、

モビリティ管理ノード。

【請求項２】

ユーザー機器（UE）であって、

コアネットワークにおけるモビリティ管理ノードと、S-NSSAI（Single-Network Slice Selection Assistance Information）に対する再NSSAA（Network Slice Specific Authentication and Authorization）手順を実行する手段と、

前記NSSAA手順中に起動されたタイマーの満了に基づいて前記NSSAAが失敗したと判断され、かつ前記S-NSSAIに関するPDU（Protocol Data Unit）Sessionがある場合に、

前記モビリティ管理ノードから、前記NSSAA手順の認証が失敗したことを示す原因値を含むNAS（Non-Access Stratum）メッセージを受信する手段と、
を備えるUE。
【請求項３】
前記NASメッセージを受信したことに応じて、前記PDU Sessionを解放する手段を備える、請求項２に記載のUE。
【請求項４】
コアネットワークにおけるモビリティ管理ノードにおける方法であって、
S-NSSAI（Single-Network Slice Selection Assistance Information）に対する再NSSAA（Network Slice Specific Authentication and Authorization）手順をトリガーし、
前記再NSSAA手順において、タイマーを起動し、
前記タイマーが満了したことに基づいて、前記再NSSAA手順における認証が失敗したと判断し、
前記NSSAAが失敗したと判断した場合に、前記S-NSSAIに関するPDU（Protocol Data Unit）SessionのRelease手続きを起動する、
方法。
【請求項５】
ユーザー機器（UE）における方法であって、
コアネットワークにおけるモビリティ管理ノードと、S-NSSAI（Single-Network Slice Selection Assistance Information）に対する再NSSAA（Network Slice Specific Authentication and Authorization）手順を実行し、
前記NSSAA手順中に起動されたタイマーの満了に基づいて前記NSSAAが失敗したと判断され、かつ前記S-NSSAIに関する（Protocol Data Unit）Sessionがある場合に、前記モビリティ管理ノードから、前記NSSAA手順の認証が失敗したことを示す原因値を含むNAS（Non-Access Stratum）メッセージを受信する、
方法。
【請求項６】
前記NASメッセージを受信したことに応じて、前記PDU Sessionを解放することを備える、請求項５に記載の方法。
【請求項７】
Configuration Update Commandメッセージを、ユーザー機器（UE）に送信する手段をさらに備え、
前記Configuration Update Commandメッセージは、前記S－NSSAIがRejected NSSAI（Network Slice Selection Assistance Information）に含まれることを示す、
請求項１に記載のモビリティ管理ノード。
【請求項８】
前記NASメッセージは、Configuration Update Commandメッセージであり、
前記Configuration Update Commandメッセージは、前記S－NSSAIがRejected NSSAI（Network Slice Selection Assistance Information）に含まれることを示す、
請求項２に記載のUE。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、セルラーネットワークに関し、特に無線端末に許可されるネットワークスライスの管理に関する。
【背景技術】
【０００２】
5G system（5GS）は、無線端末（user equipment（UE））をデータネットワーク（Data Network（DN））に接続する。5Gアーキテクチャでは、UEとDNとの間の接続（c

onnectivity）サービスは、１又はそれ以上のProtocol Data Unit（PDU）セッション（sessions）によってサポートされる（例えば、非特許文献１～３を参照）。PDUセッションは、UEとDNとの間のアソシエーション、セッション、又はコネクションである。PDUセッションは、PDU connectivity service（つまり、UEとDNとの間のPDUsの交換（exchange of PDUs））を提供するために使用される。PDUセッションは、UEとDNが接続されているUser Plane Function（UPF）（i.e., PDU session anchor）との間に確立される。データ転送の観点では、PDUセッションは、5Gコアネットワーク（5G core network（5GC））内のトンネル（N9トンネル）、5GCとアクセスネットワーク（Access Network（AN））との間のトンネル（N3トンネル）、及び１又はそれ以上の無線ベアラによって構成される。

【０００３】

非特許文献２（3GPP（登録商標） TS 23.502）及び非特許文献３（3GPP TS 24.501）は、PDUセッション確立（establishment）手順及びPDUセッション解放（release）手順を規定している。より具体的には、PDUセッション確立手順は、例えば、非特許文献１の第4.3.2.2章及び非特許文献２の第6.4.1章に記載されている。PDUセッション解放手順は、例えば、非特許文献１の第4.3.4.2章、並びに非特許文献２の第6.3.3章及び第6.4.3章に記載されている。

【０００４】

5GSは、さらに、network slicingをサポートする（例えば非特許文献１～３、特に非特許文献１の第5.15節を参照）。Network slicingは、Network Function Virtualization（NFV）技術及びsoftware-defined networking（SDN）技術を使用し、複数の仮想化された論理的なネットワークを物理的なネットワークの上に作り出すことを可能にする。各々の仮想化された論理的なネットワークは、ネットワークスライス（network slice）と呼ばれる。ネットワークスライスは、特定のネットワーク能力及びネットワーク特性（specific network capabilities and network characteristics）を提供する。ネットワークスライス・インスタンス（network slice instance（NSI））は、１つのネットワークスライスを形成するためにネットワーク機能（Network Function(NF））インスタンスと、リソース（resources）(e.g., computer processing resources、storage、及びnetworking resources)と、アクセスネットワーク（AN）（Next Generation Radio Access Network（NG-RAN）及びNon-3GPP InterWorking Function （N3IWF）の少なくともいずれか）と、のセットとして定義される。

【０００５】

ネットワークスライスは、Single Network Slice Selection Assistance Information（S-NSSAI）として知られる識別子によって特定される。S-NSSAIは、Slice/Service type (SST)及びSlice Differentiator (SD)から成る。SSTは、特性及びサービス（features and services）に関して期待されるネットワークスライスの振る舞い（expected network slice behaviour）を意味する（refers to）。SDは、任意の情報（optional information）であり、同じSlice/Service typeの複数（multiple）ネットワークスライスを区別するためにSSTを補完（complements）する。

【０００６】

S-NSSAIは、標準値（standard values）又は非標準値（non-standard values）を持つことができる。現時点では、Standard SST valuesの１、２、３、及び４は、enhanced Mobile Broad Band (eMBB)、Ultra Reliable and Low Latency Communication (URLLC)、Massive Internet of Things (MIoT)、及びVehicle to Everything (V2X)スライスタイプ（slice types）に関連付けられている。S-NSSAIのnon-standard valueは、特定のPublic Land Mobile Network（PLMN）内の１つのネットワークスライスを特定する。すなわち、non-standard SST valuesは、PLMN-specific valuesであり、これらをアサインしたPLMNのPLMN IDに関連付けられる。各S-NSSAIは、特定の（particular）NSIを選択する点でネットワークを支援する。同じNSIは、異なるS-NSSAIsを介して選択されてもよい。同じS-NSSAIは、異なるNSIに関連付けられてもよい。各

ネットワークスライスはS-NSSAIによってユニークに特定されてもよい。

【０００７】

S-NSSAIには二つの種類があり、これらはS-NSSAI及びMapped S-NSSAIとして知られている。S-NSSAIは、UEが登録されているPublic Land Mobile Network（PLMN）が提供するネットワークスライスを識別する。Mapped S-NSSAIは、UEがローミングしている際に、ローミング網のネットワークスライスを識別するS-NSSAIにマッピングされる（関連付けられる、または該当する）Home PLMN(HPLMN)のS-NSSAIであってもよく、さらにその中でUEユーザーの加入者情報に含まれるS-NSSAIであってもよい。以降、本明細書において、S-NSSAI及びMapped S-NSSAIを総称して単にS-NSSAIと呼ぶ場合がある。

【０００８】

一方、Network Slice Selection Assistance Information（NSSAI）は、S-NSSAIsのセットを意味する。したがって、１又はそれ以上のS-NSSAIsが１つのNSSAIに含まれることができる。NSSAIには複数のタイプがあり、これらはConfigured NSSAI、Requested NSSAI、Allowed NSSAI、Rejected NSSAI、及びPending NSSAIとして知られている。

【０００９】

Configured NSSAIは、各々が１又はそれ以上のPLMNsに適用可能(applicable)な１又はそれ以上のS-NSSAIsを含む。Configured NSSAIは、例えば、Serving PLMNによって設定され、当該Serving PLMNに適用される。あるいは、Configured NSSAIは、Default Configured NSSAIであってもよい。Default Configured NSSAIは、Home PLMN（HPLMN）によって設定され、特定の（specific）Configured NSSAIが提供されていない任意の（any）PLMNsに適用される。Default Configured NSSAIは、例えば、HPLMNのUnified Data Management（UDM）からAccess and Mobility Management Function（AMF）を介して無線端末（User Equipment（UE））にプロビジョンされる。

【００１０】

Requested NSSAIは、例えば登録手順（registration procedure）において、UEによってネットワークにシグナルされ、当該UEのためのServing AMF、１又はそれ以上のネットワークスライス、及び１又はそれ以上のNSIsを決定することをネットワークに可能にする。

【００１１】

Allowed NSSAIは、Serving PLMNによってUEに提供され、当該Serving PLMNの現在の（current）Registration Areaにおいて当該UEが使用することができる１又はそれ以上のS-NSSAIsを示す。Allowed NSSAIは、Serving PLMNのAMFによって、例えば登録手順（registration procedure）の間に決定される。したがって、Allowed NSSAIは、ネットワーク（i.e., AMF）によってUEにシグナルされ、AMF及びUEのぞれぞれの（non-volatile）メモリに格納される。

【００１２】

Rejected NSSAIは、現在の（current）PLMNによって拒絶された１又はそれ以上のS-NSSAIsを含む。Rejected NSSAIは、rejected S-NSSAIsと呼ばれることもある。S-NSSAIは、現在のPLMN全体で拒絶されるか、又は現在の（current）registration areaで拒絶される。AMFは、例えばUEの登録手順（registration procedure）において、Requested NSSAIに含まれる１又はそれ以上のS-NSSAIsのうちいずれかを拒絶したなら、これらをRejected NSSAIに含める。Rejected NSSAIは、ネットワーク（i.e., AMF）によってUEにシグナルされ、AMF及びUEのぞれぞれの（non-volatile）メモリに格納される。

【００１３】

Pending NSSAIは、3rd Generation Partnership Project（3GPP）において新たに合意された（非特許文献４を参照）。Pending NSSAIは、ネットワークスライスに特化し

た認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））が保留中である１又はそれ以上のS-NSSAIsを示す。Serving PLMNは、加入者情報（subscription informationに基づいてNSSAAを課されたHPLMNのS-NSSAIsに対してNSSAAを行わなければならない。NSSAAを行うために、AMFは、Extensible Authentication Protocol(EAP)-based authorization procedureを実施（invoke）する。EAP-based authentication procedureはその結果（outcome）を得るまでに比較的長い時間を要する。したがって、AMFは、UEの登録手順（registration procedure）において上述のようにAllowed NSSAIを決定するが、NSSAAを課されたS-NSSAIsを当該Allowed NSSAIに含めず、これらを代わりにPending NSSAIに含める。Pending NSSAIは、ネットワーク（i.e., AMF）によってUEにシグナルされ、AMF及びUEのぞれぞれの（non-volatile）メモリに格納される。

【００１４】

AMFは、Registration Management (RM)-REGISTERED状態のUEのUEコンテキストを管理する。UEコンテキストは、これに限らないが、Mobility Management（MM）コンテキストと呼ばれてもよい。UEコンテキストは、上述のAllowed NSSAI、Rejected NSSAI、及びPending NSSAIのいずれか一つ以上を含んでよい。一方、UEは、UE NSSAI設定（configuration）を管理する。UE NSSAI設定は、上述のConfigured NSSAI、Allowed NSSAI、Rejected NSSAI、及びPending NSSAIを含む。UE NSSAI設定は、UE（Universal Subscriber Identity Module（USIM）を除くMobile Equipment（ME））内のnon-volatileメモリにストアされる。UE NSSAI設定がストアされたメモリ又はメモリ領域は、NSSAI storageと呼ばれる。

【００１５】

非特許文献１（3GPP TS 23.501）の第5.15.10節及び非特許文献２（3GPP TS 23.502）の第4.2.9節は、Network Slice-Specific Authentication and Authorization（NSSAA）を規定している。より具体的には、非特許文献１の第5.15.10節及び非特許文献２の第4.2.9.2節は、NSSAAを記載している。非特許文献１の第5.15.10節及び非特許文献２の第4.2.9.3節は、Authentication, Authorization and Accounting（AAA）サーバ（AAA-S）によりトリガーされる再認証及び再認可（re-authentication and re-authorization）を記載している。非特許文献１の第5.15.10節及び非特許文献２の第4.2.9.4節は、AAAサーバ（AAA-S）によりトリガーされるSlice-Specific Authorizationの取り消し（revocation）を記載している。さらに非特許文献５には、非特許文献２の第4.2.9.4節に記載のSlice-Specific Authorizationの取り消し（revocation）の修正案が記載されている。

【先行技術文献】

【非特許文献】

【００１６】

【文献】3GPP TS 23.501 V16.2.0 (2019-09) “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Architecture for the 5G System (5GS); Stage 2(Release 16)”, September 2019

【文献】3GPP TS 23.502 V16.2.0 (2019-09) “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS); Stage 2 (Release 16)”, September 2019

【文献】3GPP TS 24.501 V16.2.0 (2019-09) “3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (Release 16)”, September 2019

【文献】InterDigital, ZTE, vivo, NEC, “Introduction of pending NSSAI for network slice-specific authentication and authorization”, C1-199044, 3GPP TSG-CT WG1 Meeting #121, Reno (NV), USA, 11-15 November 2019

【文献】China Mobile, Nokia, Ericsson, Telecom Italia, “Service used for slice-specific re-authentication and revocation”, S2-1912488, 3GPP TSG-SA WG2 M

eeting #136, Reno NV, USA, 18-22 November 2019
【発明の概要】
【発明が解決しようとする課題】
【００１７】
AMFは、UEの１又はそれ以上の現在許可された（current Allowed）S-NSSAIsに関するNetwork Slice-Specific Authentication and Authorization（NSSAA）を再度行う場合がある（例えば、非特許文献２の第4.2.9節を参照）。より具体的には、AMFは、Authentication, Authorization and Accounting（AAA）サーバが１又はそれ以上の現在許可されたS-NSSAIsの再認証（re-authentication）をトリガーした場合に、これらのS-NSSAIsのためのNSSAAの開始をトリガーする。さらに、AMFは、UEの加入者情報（subscription information）の変更に基づいて、当該UEの１又はそれ以上の現在許可されたS-NSSAIsのための再認証が必要であると判定することができる。さらにまた、AMFは、Mobility Registration Update又はPeriodic Registration UpdateのためのRegistration Requestメッセージを UEから受信した際に、例えばオペレータポリシーに基づいて、１又はそれ以上の現在許可されたS-NSSAIsのための再認証が必要であると判定することができる。さらに、AMFは、これらの条件に限らず、例えばオペレータポリシーに基づいて、１又はそれ以上の現在許可されたS-NSSAIsのための再認証が必要であると判定することができる。これらの場合、AMFは、再認証が必要とされるS-NSSAIsのためのNSSAAの開始をトリガーする。
【００１８】
発明者等は、UEに現在許可されたS-NSSAIのための再認証及び再認可手順に関して検討し、様々な課題を見出した。第１に、UEに現在許可された特定のS-NSSAIのための再認証及び再認可手順（i.e., NSSAA）の開始をトリガーする場合に、UEに格納されているUE NSSAI設定（NSSAI storage）をAMFがどのように扱うかが明確でない。より具体的には、AMFは、（ａ）UE NSSAI設定内のAllowed NSSAIに当該特定のS-NSSAIを格納したまま維持するべきか否かが明確でない。加えて、現在の3GPP仕様書では、UE NSSAI設定内のAllowed NSSAIからPending NSSAIにS-NSSAIを移すこと、すなわちUE NSSAI設定内のAllowed NSSAIに格納されているS-NSSAIを削除してこれをUE NSSAI設定内のPending NSSAIに格納することは規定されていない。
【００１９】
第２に、例えば、UEに現在許可されたS-NSSAIのための再認証及び再認可手順が行われている間に、UEが当該S-NSSAIに関連付けられた新たなPDUセッション確立手順を開始する可能性がある。この場合、S-NSSAIのための再認証及び再認可手順とPDUセッション確立手順とが衝突（抵触、conflict、collision）するおそれがある。
【００２０】
第３に、S-NSSAIのための再認証及び再認可手順が失敗した場合、当該S-NSSAIに関連付けられた既存のPDUセッションをネットワーク（e.g., AMF及びSMF）がどのように扱うか明確でない。
【００２１】
第４に、S-NSSAIのための再認証及び再認可手順が失敗した場合、当該S-NSSAIに関連付けられた進行中の（ongoing）PDUセッション確立手順をネットワーク（e.g., AMF及びSMF）がどのように扱うか明確でない。
【００２２】
ここに開示される実施形態が達成しようとする目的の１つは、UEに格納されているネットワークスライス設定（e.g., UE NSSAI設定）を適切に管理することをAMFに可能にすることに寄与する装置、方法、及びプログラムを提供することである。なお、この目的は、ここに開示される複数の実施形態が達成しようとする複数の目的の１つに過ぎないことに留意されるべきである。その他の目的又は課題と新規な特徴は、本明細書の記述又は添付図面から明らかにされる。
【課題を解決するための手段】

【００２３】
第１の態様では、AMFは、少なくとも１つのメモリと、前記少なくとも１つのメモリに結合された少なくとも１つのプロセッサとを備える。前記少なくとも１つのプロセッサは、UE設定の更新をUEに引き起こす第１のNon-Access Stratum（NAS）メッセージを前記UEに送信するよう構成される。前記UE設定は、前記UEに保持され、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含む。前記第１のNASメッセージは、前記UEに現在許可された第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納することを前記UEに引き起こす。
【００２４】
第２の態様では、AMFにおける方法は、UEに現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の開始をトリガーする場合に、UE設定の更新を前記UEに引き起こす第１のNon-Access Stratum（NAS）メッセージを前記UEに送信することを含む。前記UE設定は、前記UEに保持され、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含む。前記第１のNASメッセージは、前記UEに現在許可された第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納することを前記UEに引き起こす。
【００２５】
第３の態様では、UEは、少なくとも１つのメモリと、前記少なくとも１つのメモリに結合された少なくとも１つのプロセッサとを備える。前記少なくとも１つのプロセッサは、UE設定を管理するよう構成される。前記UE設定は、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含む。前記少なくとも１つのプロセッサは、さらに第１のNon-Access Stratum（NAS）メッセージをAMFから受信したことに応答して、前記UEに現在許可された第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納するよう構成される。
【００２６】
第４の態様では、UEにおける方法は、以下のステップを含む：
（ａ）UE設定を管理すること、ここで前記UE設定は、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含む；及び
第１のNon-Access Stratum（NAS）メッセージをAccess and Mobility Management Function（AMF）から受信したことに応答して、前記UEに現在許可された第１のネッ

トワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納すること。

【００２７】

第５の態様では、プログラムは、コンピュータに読み込まれた場合に、上述の第２又は第４の態様に係る方法をコンピュータに行わせるための命令群（ソフトウェアコード）を含む。

【発明の効果】

【００２８】

上述の態様によれば、UEに格納されているネットワークスライス設定（e.g., UE NSSAI設定）を適切に管理することをAMFに可能にすることに寄与する装置、方法、及びプログラムを提供できる。

【図面の簡単な説明】

【００２９】

【図１】実施形態に係るセルラーネットワークの構成例を示す図である。
【図２】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図３】実施形態に係るUE及びAMFの動作の一例を示すシーケンス図である。
【図４】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図５】実施形態に係るUE、AMF、及びAUSFの動作の一例を示すシーケンス図である。
【図６】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図７】実施形態に係るUE、AMF、及びAUSFの動作の一例を示すシーケンス図である。
【図８】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図９】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図１０】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図１１】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図１２】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図１３】実施形態に係るUE、AMF、及びAUSFの動作の一例を示すシーケンス図である。
【図１４】実施形態に係るUE、AMF、及びAUSFの動作の一例を示すシーケンス図である。
【図１５】実施形態に係るUE、AMF、及びSMFの動作の一例を示すシーケンス図である。
【図１６】実施形態に係るAMFの動作の一例を示すフローチャートである。
【図１７】実施形態に係るUEの動作の一例を示すフローチャートである。
【図１８】実施形態に係るUE、AMF、及びAUSFの動作の一例を示すシーケンス図である。
【図１９】実施形態に係るUEの構成例を示すブロック図である。
【図２０】実施形態に係るAMFの構成例を示すブロック図である。

【発明を実施するための形態】

【００３０】

以下では、具体的な実施形態について、図面を参照しながら詳細に説明する。各図面において、同一又は対応する要素には同一の符号が付されており、説明の明確化のため、必要に応じて重複説明は省略される。

【００３１】

以下に説明される複数の実施形態は、独立に実施されることもできるし、適宜組み合わせて実施されることもできる。これら複数の実施形態は、互いに異なる新規な特徴を有している。したがって、これら複数の実施形態は、互いに異なる目的又は課題を解決することに寄与し、互いに異なる効果を奏することに寄与する。

【００３２】

以下に示される複数の実施形態は、3GPP第5世代移動通信システム（5G system（5GS））を主な対象として説明される。しかしながら、これらの実施形態は、5GSと類似のネ

ットワークスライシングをサポートする他のセルラー通信システムに適用されてもよい。

【００３３】

＜第１の実施形態＞

図１は、本実施形態に係るセルラーネットワーク（i.e., 5GS）の構成例を示している。図１に示された要素の各々はネットワーク機能であり、3rd Generation Partnership Project（3GPP）により定義されたインタフェースを提供する。図１に示された各要素（ネットワーク機能）は、例えば、専用ハードウェア（dedicated hardware）上のネットワークエレメントとして、専用ハードウェア上で動作する（running）ソフトウェア・インスタンスとして、又はアプリケーション・プラットフォーム上にインスタンス化（instantiated）された仮想化機能として実装されることができる。

【００３４】

図１に示されたセルラーネットワークは、Mobile Network Operator（MNO）によって提供されてもよいし、MNO以外によって提供されるNon-Public Network (NPN)であってもよい。図１に示されたセルラーネットワークがNPNである場合、これはStand-alone Non-Public Network（SNPN）と表される独立したネットワークでもよいし、Public network integrated NPNと表されるMNOネットワークと連動したNPNであってもよい。

【００３５】

無線端末（i.e., UE）１は、5G接続（connectivity）サービスを利用し、データネットワーク（DN）７と通信する。より具体的には、UE１は、アクセスネットワーク（i.e., 5G Access Network（5GAN））５に接続され、コアネットワーク（i.e., 5G core network（5GC））内のUser Plane Function（UPF）６を介してデータネットワーク（DN）７と通信する。AN５は、Next Generation Radio Access Network（NG-RAN）若しくはnon-3GPP AN又は両方を含む。Non-3GPP ANは、無線LAN（WiFi）通信を扱うネットワークであってもよいし、Wireline 5G Access Network（W-5GAN）と表される有線通信を扱うネットワークであってもよい。UPF６は、相互に接続された複数のUPFを含んでもよい。

【００３６】

5Gアーキテクチャでは、UE１とDN７との間の接続（connectivity）サービスは、1又はそれ以上のProtocol Data Unit（PDU）セッションによってサポートされる。PDUセッションは、UE１とDN７との間のアソシエーション、セッション、又はコネクションである。PDUセッションは、PDU connectivity service（つまり、UE１とDN７との間のPDUsの交換（exchange of PDUs））を提供するために使用される。UE１は、UE１とDN７が接続されているUPF６（i.e., PDU session anchor）との間に１又はそれ以上のPDUセッションを確立する。データ転送の観点では、PDUセッションは、5GC内のトンネル（N9トンネル）、5GCとAN５との間のトンネル（N3トンネル）、及び１又はそれ以上の無線ベアラによって構成される。図１には示されていないが、UE１は、複数のDNs７に同時に（concurrently）アクセスするために、複数のUPFs（PDU session anchors）６それぞれとの複数のPDUセッションを確立してもよい。

【００３７】

AMF２は、5GC Control Plane内のネットワーク機能の１つである。AMF２は、RAN Control Plane（CP）インタフェース（i.e., N2インタフェース）の終端を提供する。AMF２は、UE１との１つの（single）シグナリングコネクション（i.e., N1 NAS signalling connection）を終端し、registration management、connection management、及びmobility managementを提供する。AMF２は、サービス・ベースド・インタフェース（i.e., Namfインタフェース）上でNFサービス（services）をNFコンシューマ（consumers）（e.g. 他のAMF、Session Management Function（SMF）３、及びAuthentication Server Function（AUSF）４）に提供する。AMF２により提供されるNFサービスは、通信サービス（Namf_Communication）を含む。当該通信サービスは、NFコンシューマ（e.g., SMF３）にAMF２を介してUE１又はAN５と通信することを可能にする。

【００３８】
SMF３は、5GC Control Plane内のネットワーク機能の１つである。SMF３は、PDUセッションを管理する。SMF３は、AMF２により提供される通信サービスを介して、UE１のNon-Access-Stratum (NAS) Session Management (SM)レイヤとの間でSMシグナリングメッセージ（messages）（NAS-SM messages、N1 SM messages）を送受信する。SMF３は、サービス・ベースド・インタフェース（i.e., Nsmfインタフェース）上でNFサービス（services）をNFコンシューマ（consumers）（e.g. AMF２、他のSMF）に提供する。SMF３により提供されるNFサービスは、PDUセッション管理サービス（Nsmf_PDUSession）を含む。当該NFサービスは、NFコンシューマ（e.g., AMF２）にPDUセッション(sessions)を操作する（handle）ことを可能にする。SMF３は、Intermediate SMF（I-SMF）であってもよい。I-SMFは、UPF６が異なるSMFサービスエリアに属しており、オリジナルSMFによる制御ができない場合に、必要に応じてAMF２とオリジナルSMF３の間に挿入される。
【００３９】
AUSF４は、5GC Control Plane内のネットワーク機能の１つである。AUSF４は、サービス・ベースド・インタフェース（i.e., Nausfインタフェース）上でNFサービス（services）をNFコンシューマ（consumers）（e.g. AMF２、UDM８）に提供する。AUSF４により提供されるNFサービスは、UE authentication service（e.g. Nausf_UEAuthentication及びNausf_NSSAA_Authenticate）を含む。Nausf_UEAuthenticationサービスは、UEの認証及び関係する鍵情報（keying material）をNFコンシューマ（i.e., AMF）に提供する。より具体的には、AUSF４は、UDM８及びAuthentication credential Repository and Processing Function（ARPF）と連携し、5GSでサポートされる２つの認証方法（i.e., 5G-Authentication and Key Agreement (AKA)及びEAP-based authentication）のいずれかを用いた認証を実行する。認証を実行した後に、AUSF４は、AMF２に、認証結果ともし成功ならマスターキーを返信する。マスターキーは、NAS security keys及びその他のsecurity key(s)を導出するためにAMF２により使用される。UEの認証のために、AUSF４は、UDM８と密接に連携する。Nausf_NSSAA_Authenticateサービスは、NFコンシューマ（e.g., AMF２）にAUSF４を介してUE１とAAAサーバ間のネットワークスライスに特化した認証及び認可サービスを提供する。
【００４０】
UDM８は、5GC Control Plane内のネットワーク機能の１つである。UDM８は、加入者データ（加入者情報（subscription information））が格納されたデータベース（i.e., User Data Repository（UDR））へのアクセスを提供する。UDM８は、サービス・ベースド・インタフェース（i.e., Nudmインタフェース）上でNFサービス（services）をNFコンシューマ（consumers）（e.g. AMF２、AUSF４、SMF３）に提供する。UDM８により提供されるNFサービスは、加入者データ管理サービスを含む。当該NFサービスは、NFコンシューマ（e.g., AMF）に加入者データを取得（retrieve）することを可能にし、更新された加入者データをNFコンシューマに提供する。
【００４１】
図１の構成例は、説明の便宜のために、代表的なNFsのみを示している。本実施形態に係るセルラーネットワークは、図１に示されていない他のNFs、例えばNetwork Slice Selection Function（NSSF）及びPolicy Control Function（PCF）を含んでもよい。
【００４２】
図２は、本実施形態に係るAMF２の動作の一例を示すフローチャートである。ステップ２０１では、AMF２は、UE１に格納されるUE NSSAI設定（NSSAI storage）を管理する。具体的には、AMF２は、UE１のUE NSSAI設定（NSSAI storage）に格納されるべきAllowed NSSAI、Rejected NSSAI、若しくはPending NSSAI又はこれらの任意の組み合わせを作成し、NASメッセージを介してこれをUE１に提供する。また、AMF２は、RM-REGISTERED状態であるUE１のUEコンテキストを管理する。当該UEコンテキストは、Allowed NSSAI、Rejected NSSAI若しくはPending NSSAI又はこれらの任意の組み

合わせを含む。

【００４３】

ステップ２０２では、AMF２は、特定のS-NSSAIをUE NSSAI設定内のAllowed NSSAIから削除しこれをUE NSSAI設定内のPending NSSAIに格納することをUE１に引き起こすNASメッセージをUE１に送信する。言い換えると、AMF２は、当該特定のS-NSSAIをUE NSSAI設定内のAllowed NSSAIからPending NSSAIに移すことをUE１に引き起こすNASメッセージをUE１に送信してもよい。具体的には、AMF２は、当該特定のS-NSSAIをPending NSSAI IEに含めて、これをNASメッセージを介してUE１に供給する。他の例として、AMF２は、特定のS-NSSAIがそれから削除された更新後の（updated）Allowed NSSAI及び当該特定のS-NSSAIがそれに追加された更新後のPending NSSAIを共に作成し、これをNASメッセージを介してUE１に供給してもよい。当該NASメッセージは、例えば、UE Configuration Update Commandメッセージであってもよい。当該NASメッセージの受信に応答して、UE１は、UE１の（non-volatile）メモリに格納されているUE NSSAI設定（NSSAI storage）を更新する。具体的には、UE１は、当該NASメッセージを介して受信したPending NSSAI IEに含まれる当該特定のS-NSSAIがUE NSSAI設定（NSSAI storage）内のAllowed NSSAIに含まれる場合、これをAllowed NSSAIから削除し、Pending NSSAIに格納する。または、UE１は、当該特定のS-NSSAIをUE NSSAI設定（NSSAI storage）内のAllowed NSSAIからPending NSSAIに移動してもよい。

【００４４】

UE NSSAI設定（NSSAI storage）は、Allowed NSSAI、Rejected NSSAI、及びPending NSSAIのうち一つ以上に含まれるS-NSSAIsそれぞれのNSSAAによる許可ステータスを示すステータス情報を含んでもよい。S-NSSAIsのステータス情報は、各S-NSSAIについてNSSAAによる現在の許可(permission)が再認証及び再認可中にもavailable（allowed to use, 又はpermitted）であるか、それともunavailable（not allowed to use, 又はnot permitted）であるかを示してもよい。

【００４５】

幾つかの実装では、UE１は、Allowed NSSAIに含まれるS-NSSAIsに関してステータス情報を管理してもよい。言い換えると、ステータス情報は、Allowed NSSAIと関連付けられてもよい。他の実装では、UE１は、Allowed NSSAI、Rejected NSSAI、及びPending NSSAIとは独立に、NSSAAを課される（subjected to）S-NSSAIsそれぞれの現在の許可(permission)ステータスを管理してもよい。

【００４６】

幾つかの実装では、特定のS-NSSAIについてNSSAAによる現在の許可(permission)が再認証及び再認可中にもavailableであること示すために、ステータス情報は、それがactivateされていること(activate状態)、valid状態であること、認証済みであること（previously authorized）、又は（再）認証中であること（under (re-)authorization）を示してもよい。一方、特定のS-NSSAIについてNSSAAによる現在の許可(permission)が再認証及び再認可中にunavailableであること示すために、ステータス情報は、それがdeactivateされていること(deactivate状態)、invalid状態であること、（再）認証中であること（under (re-)authorization）、又は未認証であること（not (yet) authorized）を示してもよい。

【００４７】

すなわち、現在許可されている特定のS-NSSAIのステータス情報が（再）認証中を示す場合、幾つかの実装ではこれは特定のS-NSSAIのための現在の許可が再認証及び再認可中にも「有効」であることを意味してもよいし、他の実装ではこれは特定のS-NSSAIのための現在の許可が再認証及び再認可中には「無効」であることを意味してもよい。

【００４８】

したがって、幾つかの実装では、available状態は、複数の状態（サブ状態）、例えば「認証済み」および「再認証及び再認可中」を含んでもよい。他の実装では、unavailable状態は、複数の状態（サブ状態）、例えば「未認証」および「再認証及び再認可中」を含

んでもよい。
【００４９】
特定のS-NSSAIについてNSSAAによる現在の許可が認証済みである（previously authorized）か、それとも（再）認証中である（under (re-)authorization）か、又は未認証である（not (yet) authorized）か、を示すステータス情報は、S-NSSAIsに関してNSSAAの動作を管理するために使用されるデータに含まれてもよい。当該データは、“S-NSSAIs subject to Network Slice-Specific Authentication and Authorization”と称されてもよい。
【００５０】
ステータス情報は、特定のS-NSSAIについてNSSAAによる現在の許可が（再）認証中であることを示すために、既に認証されている当該S-NSSAIが念の為再認証されることを示してもよい。
【００５１】
ステータス情報は、特定のS-NSSAIについてNSSAAによる現在の許可が未認証であることを示すために、既に認証されている当該S-NSSAIが疑義があるために再認証及び再認可（追加認証及び認可）されることを示してもよい。
【００５２】
AMF２は、上述のAllowed NSSAI、Rejected NSSAI、及びPending NSSAIのうち一つ以上に含まれるS-NSSAIsのステータス情報を更新することをUE１に引き起こすための情報を前述のNASメッセージに含めてもよい。UE１は、受信した当該情報に基づいて、上述のAllowed NSSAI、Rejected NSSAI、及びPending NSSAIのうち一つ以上に含まれるS-NSSAIsのステータス情報を更新してもよい。
【００５３】
図３は、UE NSSAI設定の更新のためのUE Configuration Update手順の一例を示している。ステップ３０１では、特定のS-NSSAI（ここではS-NSSAI #1）がUE１に許可されている。したがって、UE１に格納されているUE NSSAI設定（３０２）では、S-NSSAI #1がAllowed NSSAIに含まれる。同様に、AMF２によって管理されているUE１のUEコンテキストでは、S-NSSAI #1がAllowed NSSAIに含まれる。
【００５４】
ステップ３０３では、AMF２は、特定のS-NSSAIがAllowed NSSAIから削除されPending NSSAIに含まれることを示すUE Configuration Update CommandメッセージをUE１に送信する。当該UE Configuration Update Commandメッセージの受信に応答して、UE１は、UE１の（non-volatile）メモリに格納されているUE NSSAI設定（NSSAI storage）を更新する（ステップ３０４）。具体的には、UE１は、UE Configuration Update Commandメッセージを介して受信したPending NSSAI IEに含まれる当該特定のS-NSSAIがUE NSSAI設定（NSSAI storage）内のAllowed NSSAIに含まれる場合、これをAllowed NSSAIから削除し、Pending NSSAIに格納する。
【００５５】
図３に示されたUE Configuration Update Commandメッセージは、UE NSSAI設定の更新をUE１に引き起こすために使用されることができるメッセージの典型的な例の１つである。しかしながら、AMF２は、他のNASメッセージを介して、UE NSSAI設定の更新をUE１に指示又は要求してもよい。例えば、AMF２は、特定のS-NSSAIのための再認証及び再認可手順の間にAMF２からUE１に送られるNASメッセージ（e.g., Network Slice-Specific Authentication Command）を使用してもよい。他のNASメッセージはNetwork Slice-Specific Authentication Commandであってもよく、AMF２は当該特定のS-NSSAIをNetwork Slice-Specific Authentication Commandに含めてよい。このとき、当該特定のS-NSSAIは、S-NSSAI IEに含まれていてもよい。
【００５６】
図２及び図３を用いて説明されたAMF２の動作によれば、AMF２は、特定のS-NSSAIがAllowed NSSAIからPending NSSAIに移されることをUE１に通知できる。例えば、UE

１は、S-NSSAIsそれぞれについてのNSSAAによる許可に関するステータスを示す情報に基づいて、PDUセッション確立要求を禁止されてもよいし、PDUセッション確立手順を中止または中断（suspend）してもよい。より具体的には、UE１は、特定のS-NSSAIについて現在のNSSAAによる許可が再認証及び再認可中にunavailableであること（not allowed to use, not permitted）を示す情報に関連付けられている、あるいはそのように更新された場合、そのS-NSSAIに関連付けられたPDUセッションの確立を禁止されてもよいし、当該PDUセッションの確立の手順を中止または中断(suspend、またはrefrain)するよう動作してもよい。

【００５７】

図２及び図３を用いて説明した手順は、以下のように変形されてもよい。図３のステップ３０１において、特定のS-NSSAI（ここではS-NSSAI #1）が現時点でUE１に対して許可されていなくてもよい。例えば、特定のS-NSSAIが過去にUE１に対して許可されていたが、現時点で何らかの理由（又は特定の理由）により許可されていない又は拒絶されていてもよい。

【００５８】

この場合、AAA-S、AMF２、およびUE１は、過去にUE１に対して許可されていたが現時点で何らかの理由（又は特定の理由）により許可されていない又は拒絶されているS-NSSAIを、当該理由を示すcause IEとともに又はこれと関連付けて記憶してもよい。この理由を示すcause IEは、例えば、S-NSSAI is not available due to the failed or revoked network slice-specific authorization and authenticationであってもよい。このとき、ステップ３０１において、AMF２は、特定のS-NSSAIをRejected NSSAIに含めることを示すUE Configuration Update CommandメッセージをUE１に送信してもよく、このメッセージに当該理由を示すcause IEを特定のS-NSSAIと対応付けて含めてもよい。

【００５９】

この場合、UE１に格納されているUE NSSAI設定（３０２）では、S-NSSAI #1がRejected NSSAIに含まれる。同様に、AMF２によって管理されているUE１のUEコンテキストでは、S-NSSAI #1がRejected NSSAIに含まれる。この動作は、AAA-Sが特定のS-NSSAIに対して一度Revocationの手続を実施した後に、AAA-Sが当該特定のS-NSSAIのための再認証及び再認可手順を起動した場合に起こりうる。

【００６０】

AAA-Sが特定のS-NSSAIに対して一度Revocationの手続を実施した後、（例えば、図３のステップ３０２とステップ３０３の間で）実行された再認証及び再認可手順が成功した場合、UE１およびAMF２は、Rejected NSSAIとして管理されていたS-NSSAI #1をAllowed NSSAIに移動してもよい。この動作により、UE１は、当該S-NSSAIが提供するサービスの利用が可能となる。

【００６１】

特定のS-NSSAIがRejected NSSAIに格納されていた場合、ステップ３０３において、AMF２は、特定のS-NSSAIをPending NSSAI又はAllowed NSSAIに含めることを示すUE Configuration Update CommandメッセージをUE１に送信してもよい。この場合、UE１に格納されているUE NSSAI設定（３０２）およびAMF２が管理するUEコンテキストでは、S-NSSAI #1がRejected NSSAIに含まれたまま維持されてもよいし、S-NSSAI #1がRejected NSSAIからPending NSSAI又はAllowed NSSAIへ移されてもよい。AMF２からUE１に送信されるUE Configuration Update Commandメッセージは、Access Type毎に送信されてもよい。

【００６２】

図４は、AMF２の動作の他の例を示すフローチャートである。ステップ４０１は、図２のステップ２０１と同様である。ステップ４０２では、AMF２は、UE１に現在許可された特定のS-NSSAIのための再認証及び再認可手順（再度又は追加のNSSAA）をトリガーする。NSSAA手順は、既存のそれと同様であってもよい。既存のNSSAA手順は、非特許文献２の第4.2.9.1節に規定されている。

【００６３】
既に説明したように、ＡＭＦ２は、ＵＥ１の１又はそれ以上の現在許可されたS-NSSAIsに関するNetwork Slice-Specific Authentication and Authorization（NSSAA）を再度行う場合がある。より具体的には、AMFは、AAAサーバ(AAA-S)が１又はそれ以上の現在許可されたS-NSSAIの再認証（re-authentication）をトリガーした場合に、これらのS-NSSAIsのためのNSSAAの開始をトリガーする。さらに、ＡＭＦ２は、ＵＥ１の加入者情報の変更に基づいて、ＵＥ１の１又はそれ以上の現在許可されたS-NSSAIsのための再認証が必要であると判定することができる。さらにまた、ＡＭＦ２は、Mobility Registration Update又はPeriodic Registration UpdateのためのRegistration RequestメッセージをＵＥ１から受信した際に、例えばオペレータポリシーに基づいて、１又はそれ以上の現在許可されたS-NSSAIsのための再認証が必要であると判定することができる。さらに、ＡＭＦ２は、これらの条件に限らず、例えばオペレータポリシーに基づいて、１又はそれ以上の現在許可されたS-NSSAIsのための再認証が必要であると判定することができる。これらの場合、ＡＭＦ２は、再認証が必要とされるS-NSSAI(s)のためのNSSAAの開始をトリガーする。
【００６４】
ＡＭＦ２は、再認証及び再認可手順を開始する（又は開始をトリガーする）ために、ＡＵＳＦ４に認証要求メッセージを送信してもよい。当該メッセージは、例えば、Nausf_Communication_EAPMessage_Transferメッセージ、又はNausf_NSSAA_Authenticate Requestメッセージであってもよい。ＡＭＦ２は、（再）認証が必要とされるS-NSSAIを、上記メッセージに含めてＡＵＳＦ４に送信してもよいし、別のメッセージによりＡＵＳＦ４に送信してもよい。ＡＭＦ２は、（再）認証が必要とされるS-NSSAIのためのUE User ID for EAP authentication (EAP ID) を、上記メッセージに含めてＡＵＳＦ４に送信してもよいし、別のメッセージによりＡＵＳＦ４に送信してもよい。ＡＭＦ２は、ＵＥ１のGeneric Public Subscription Identifier (GPSI)を、上記メッセージに含めてＡＵＳＦ４に送信してもよいし、別のメッセージによりＡＵＳＦ４に送信してもよい。ＡＭＦ２は、AAA-Ｓ９のアドレスを上記メッセージに含めてＡＵＳＦ４に送信してもよいし、別のメッセージによりＡＵＳＦ４に送信してもよい。これに先立って、ＡＭＦ２は、当該S-NSSAIのためのEAP IDをＵＥ１に要求してもよい。
【００６５】
ステップ４０３では、特定のS-NSSAIのための再認証及び再認可手順の開始に応答して、ＡＭＦ２は、図２のステップ２０２と同様のNASメッセージをＵＥ１に送信する。より具体的には、ＡＭＦ２は特定のS-NSSAIをUE NSSAI設定内のAllowed NSSAIから削除しこれをUE NSSAI設定内のPending NSSAIに格納することをＵＥ１に引き起こすNASメッセージをＵＥ１に送信する。
【００６６】
上述のように、UE1のUE NSSAI設定は、S-NSSAIsのNSSAAによる許可ステータスを示すステータス情報を含んでもよい。S-NSSAIsのステータス情報は、各S-NSSAIについてNSSAAによる現在の許可(permission)が再認証及び再認可中にもavailable（allowed to use, 又はpermitted）であるか、それともunavailable（not allowed to use, 又はnot permitted）であるかを示してもよい。この場合、ステップ４０３においてＡＭＦ２は、S-NSSAI #1のステータスをavailable状態からunavailable状態に変更することをＵＥ１に引き起こすための情報を当該NASメッセージに含めてもよい。これに代えて、ＡＭＦ２は、S-NSSAI #1のステータスがavailable状態のまま維持されることをＵＥ１に指示するための情報を当該NASメッセージに含めてもよい。ＵＥ１は、受け取った当該情報に基づいて、S-NSSAI #1のステータス情報を更新する。
【００６７】
ステップ４０３は、、ＡＭＦ２からＡＵＳＦ４へのNSSAAのための認証要求メッセージの送信の前に行われてもよいし、これの後に行われてもよい。例えば、ＡＭＦ２は、特定のS-NSSAIのための再認証イベントが発生したことをAAA-Ｓ９からＡＵＳＦ４を介して通知されたこ

とに応答して、ステップ４０３を行ってもよい。例えば、AMF２は、特定のS-NSSAIのための再認証が必要であることをオペレータポリシーに基づいて判定したことに応答してステップ２０２を行ってもよい。AMF２は、特定のS-NSSAIのための再認証が必要であることをオペレータポリシーの変更に基づいて判定したことに応答してステップ２０２を行ってもよい。AMF２は、特定のS-NSSAIのための再認証が必要であることを加入者情報の変更に基づいて判定したことに応答して、ステップ４０３を行ってもよい。例えば、AMF２は、AUSF４へNausf_Communication_EAPMessage_Transferメッセージを送信したことに応答して、ステップ４０３を行ってもよい。例えば、AMF２は、当該S-NSSAIのためのEAP IDをUE１に要求したことに応答して、ステップ４０３を行ってもよい。

【００６８】

図４に示された動作は、例えば、セキュリティの向上に寄与できる。具体的には、UE１は、Pending NSSAIに含まれている特定のS-NSSAIに関連付けられたPDUセッションの確立を要求できない。したがって、AMF２は、特定のS-NSSAIのための再認証及び再認可手順が行われているときに当該特定のS-NSSAIに関連付けられた新たなPDUセッションの確立をUE１が要求することを抑止できる。

【００６９】

例えば、UE１は、S-NSSAIsそれぞれについてのNSSAAによる許可に関するステータスを示す情報に基づいて、PDUセッション確立要求を禁止されてもよいし、PDUセッション確立手順を中止または中断（suspend）してもよい。より具体的には、UE１は、特定のS-NSSAIについて現在のNSSAAによる許可が再認証及び再認可中にunavailableであること（not allowed to use, not permitted）を示す情報に関連付けられている、あるいはそのように更新された場合、そのS-NSSAIに関連付けられたPDUセッションの確立を禁止されてもよいし、当該PDUセッションの確立の手順を中止または中断(suspend、またはrefrain)するよう動作してもよい。

【００７０】

図５は、AAA-Sによって開始（又はトリガー）される再認証及び再認可手順の一例を示している。ステップ５０１では、特定のS-NSSAI（ここではS-NSSAI #1）がUE１に許可されている。したがって、UE１に格納されているUE NSSAI設定（５０２）では、S-NSSAI #1がAllowed NSSAIに含まれる。同様に、AMF２によって管理されているUE１のUEコンテキストでは、S-NSSAI #1がAllowed NSSAIに含まれる。

【００７１】

ステップ５０３では、AAA-S９は、S-NSSAI #1によって特定されるネットワークスライスのための再認証及び再認可を要求する。具体的には、AAA-S９は、再認証及び再認可要求メッセージをAUSF４に送信してもよい。当該メッセージは、例えば、Nausf_Re-Auth Requestメッセージ又はAAA Protocol Re-Auth Requestメッセージであってもよい。当該メッセージは、S-NSSAI #1を示し、UE１のGeneric Public Subscription Identifier（GPSI）をさらに示す。当該メッセージは、AAA-S９からAUSF４に直接的に送られてもよいし、図示されていないAAA Proxy（AAA-P）を介してAUSF４に送られてもよい。

【００７２】

ステップ５０４では、AUSF４は、AUSF４が提供するNFサービスを介して、S-NSSAI #1をUE１のために再認証及び再認可するイベントが発生したことをAMF２に通知する。当該通知は、例えば、Namf_Re-Auth Requestメッセージ又はNAusf_NSSAA_Notifyメッセージであってもよい。当該通知は、S-NSSAI #1を示し、UE１のGPSIをさらに示す。

【００７３】

ステップ５０５では、AMF２は、特定のS-NSSAIがAllowed NSSAIから削除されPending NSSAIに含まれることを示すUE Configuration Update Commandメッセージを UE１に送信する。当該UE Configuration Update Commandメッセージの受信に応答して、UE１は、UE１の（non-volatile）メモリに格納されているUE NSSAI設定（NSSAI storage）を更新する（ステップ５０６）。具体的には、UE１は、当該UE Configuration

Update Commandメッセージを介して受信したPending NSSAI IEに含まれる当該特定のS-NSSAIがUE NSSAI設定（NSSAI storage）内のAllowed NSSAIに含まれる場合、これをAllowed NSSAIから削除し、Pending NSSAIに格納する。また、AMF２は、UE１のためのUEコンテキスト内のAllowed NSSAIからS-NSSAI #1を削除し、UE１のUEコンテキスト内のPending NSSAIにS-NSSAI #1を格納する（追加する）。言い換えると、AMF２は、S-NSSAI #1をAllowed NSSAIからPending NSSAIに移動（変更）してもよい。

【００７４】

上述のように、UE1のUE NSSAI設定は、S-NSSAIsのNSSAAによる許可ステータスを示すステータス情報を含んでもよい。S-NSSAIsのステータス情報は、各S-NSSAIについてNSSAAによる現在の許可(permission)が再認証及び再認可中にもavailable（allowed to use, 又はpermitted）であるか、それともunavailable（not allowed to use, 又はnot permitted）であるかを示してもよい。この場合、ステップ５０６においてAMF２は、S-NSSAI #1のステータスをavailable状態からunavailable状態に変更することをUE１に引き起こすための情報を当該NASメッセージに含めてもよい。これに代えて、AMF２は、S-NSSAI #1のステータスがavailable状態のまま維持されることをUE１に指示するための情報を当該NASメッセージに含めてもよい。UE１は、受け取った当該情報に基づいて、S-NSSAI #1のステータス情報を更新する。

【００７５】

ステップ５０７では、AMF２は、Network Slice-Specific Authentication and Authorization（NSSAA）手順をトリガーする。NSSAA手順は、既存のそれと同様であってもよい。既存のNSSAA手順は、非特許文献２の第4.2.9.1節に規定されている。

【００７６】

図５の手順は、適宜変形されることができる。例えば、ステップ５０５（及び５０６）は、ステップ５０７が開始された後（つまり、NSSAA手順の実行中）に行われてもよい。

【００７７】

図６は、AMF２の動作の他の例を示すフローチャートである。ステップ６０１及び６０２は、図４のステップ４０１及び４０２と同様である。ステップ６０２の再認証及び再認可手順は、上述の理由又は他の理由のためにAMF２によって開始される。

【００７８】

ステップ６０３では、AMF２は、再認証及び再認可手順（NSSAA手順）が実行中である（ongoing）特定のS-NSSAIに関連付けられた新たなPDUセッション確立の要求をUE１から受信する。言い換えると、AMF２は、再認証及び再認可手順の開始をトリガーした後に特定のS-NSSAIに関連付けられた新たなPDUセッション確立の要求をUE１から受信する。より具体的には、AMF２は、NASメッセージ（e.g., UL NAS Transportメッセージ）をUE１から受信する。当該NASメッセージは、特定のS-NSSAI、新たなPDU session ID、及びN1 SMコンテナ (PDU Session Establishment Request)を包含する。

【００７９】

ステップ６０４では、再認証及び再認可手順が実行中である特定のS-NSSAIに関連付けられた新たなPDUセッション確立の要求をUE１から受信したことに応答して、図２のステップ２０２と同様のNASメッセージをUE１に送信する。この場合、AMF２は、図２のステップ２０２と同様のNASメッセージをUE１に送信する。より具体的には、AMF２は、特定のS-NSSAIをUE NSSAI設定内のAllowed NSSAIから削除しこれをUE NSSAI設定内のPending NSSAIに格納することをUE１に引き起こすNASメッセージをUE１に送信する。なお、AMF２は、AMF２は、ステップ６０３で受信したNASメッセージが、特定のS-NSSAI及び新たなPDU session IDを含むことに基づいて、特定のS-NSSAIに関連付けられた新たなPDUセッション確立要求の受信を判断してもよい。

【００８０】

一例では、ステップ６０４のNASメッセージは、UE Configuration Update Commandメッセージであってもよい。具体的には、AMF２は、当該特定のS-NSSAIをPending NSSAI IEに含めて、これをUE Configuration Update Commandメッセージを介してUE

１に供給してもよい。他の例として、ＡＭＦ２は、特定のS-NSSAIがそれから削除された更新後の（updated）Allowed NSSAI及び当該特定のS-NSSAIがそれに追加された更新後のPending NSSAIを共に作成し、これをUE Configuration Update Commandメッセージを介してＵＥ１に供給してもよい。

【００８１】

他の例では、当該NASメッセージは、ＵＥ１から受信したPDUセッション確立要求が拒絶されることを示すメッセージであってもよい。当該メッセージは、再認証及び再認可手順が実行中であることを示すcause情報要素（Information Element（IE））を包含してもよい。より具体的には、ＡＭＦ２は、PDU Session Establishment Rejectメッセージを生成し、これを包含するN1 SMコンテナを運ぶNASメッセージ（e.g., DL NAS Transportメッセージ）をＵＥ１に送信してもよい。当該NASメッセージは、当該特定のS-NSSAIを含んだPending NSSAI IEを含んでもよい。他の例として、当該NASメッセージは、特定のS-NSSAIがそれから削除された更新後のAllowed NSSAI及び特定のS-NSSAIがそれに追加された更新後のPending NSSAIを含んでもよい。さらに又はこれに代えて、当該NASメッセージ（e.g., DL NAS Transportメッセージ）は、再認証及び再認可手順が実行中であることを示す新たなcause IE（e.g., 5GMM Cause IE）を包含してもよい。さらに又はこれに代えて、ＡＭＦ２により生成されるPDU Session Establishment Rejectメッセージは、再認証及び再認可手順が実行中であることを示す新たなcause IE（e.g., 5GSM Cause IE）を含んでもよい。

【００８２】

上述のように、UE1のUE NSSAI設定は、S-NSSAIsのNSSAAによる許可ステータスを示すステータス情報を含んでもよい。S-NSSAIsのステータス情報は、各S-NSSAIについてNSSAAによる現在の許可(permission)が再認証及び再認可中にもavailable（allowed to use, 又はpermitted）であるか、それともunavailable（not allowed to use, 又はnot permitted）であるかを示してもよい。この場合、ステップ６０４においてＡＭＦ２は、S-NSSAI #1のステータスをavailable状態からunavailable状態に変更することをＵＥ１に引き起こすための情報を当該NASメッセージに含めてもよい。これに代えて、ＡＭＦ２は、S-NSSAI #1のステータスがavailable状態のまま維持されることをＵＥ１に指示するための情報を当該NASメッセージに含めてもよい。ＵＥ１は、受け取った当該情報に基づいて、S-NSSAI #1のステータス情報を更新する。

【００８３】

ＡＭＦ２は、ステップ６０３で受信したPDUセッション確立要求を拒絶してもよい。これに代えて、ＡＭＦ２は、ステップ６０３で受信したPDUセッション確立要求、または当該PDUセッション確立要求への応答（acceptまたはreject）を少なくともNSSAA手順の結果が得られるまで中断（suspendまたはrefrain）してもよい。ＡＭＦ２は、NSSAA手順が成功したなら、中断されていたPDUセッション確立手順を再開してもよい。

【００８４】

図６に示された動作は、例えば、セキュリティの向上に寄与できる。具体的には、ＵＥ１は、Pending NSSAIに含まれている特定のS-NSSAIに関連付けられたPDUセッションの確立を要求できない。したがって、ＡＭＦ２は、再認証及び再認可手順が実行中であるS-NSSAIに関連付けられた新たなPDUセッション確立をＵＥ１がさらに要求することを抑止できる。

【００８５】

図７は、AAA-Sによって開始（又はトリガー）される再認証及び再認可手順の一例を示している。図７のステップ７０１～７０４は図５のステップ５０１～５０４と同様である。ステップ７０５では、ＡＭＦ２は、再認証及び再認可イベント通知メッセージの受信に応答して、ＵＥ１に現在許可された特定のS-NSSAIのための再認証及び再認可手順（再度又は追加のNSSAA）をトリガーする。より具体的には、ＡＭＦ２は、再認証及び再認可手順を開始する（又は開始をトリガーする）ために、ＡＵＳＦ４に認証要求メッセージを送信する。当該認証要求メッセージは、例えば、Nausf_Communication_EAPMessage_Transfer

メッセージ、又はNausf_NSSAA_Authenticate Requestメッセージであってもよい。AMF２は、（再）認証が必要とされるS-NSSAIを、上記メッセージに含めてAUSF４に送信してもよいし、別のメッセージによりAUSF４に送信してもよい。AMF２は、（再）認証が必要とされるS-NSSAIのためのUE User ID for EAP authentication（EAP ID）を、上記メッセージに含めてAUSF４に送信してもよいし、別のメッセージによりAUSF４に送信してもよい。AMF２は、UE１のGeneric Public Subscription Identifier (GPSI)を、上記メッセージに含めてAUSF４に送信してもよいし、別のメッセージによりAUSF４に送信してもよい。AMF２は、AAA-S９のアドレスを上記メッセージに含めてAUSF４に送信してもよいし、別のメッセージによりAUSF４に送信してもよい。

【００８６】

ステップ７０６では、AMF２は、再認証及び再認可手順が実行中であるS-NSSAI #1に関連付けられた新たなPDUセッションの確立の要求をUE１から受信する。より具体的には、AMF２は、NASメッセージ（e.g., UL NAS Transportメッセージ）をUE１から受信する。当該NASメッセージは、S-NSSAI #1、新たなPDU session ID、及びN1 SMコンテナ (PDU Session Establishment Request)を包含する。

【００８７】

ステップ７０７では、AMF２は、再認証及び再認可手順が実行中であるS-NSSAI #1に関連付けられた新たなPDUセッション確立要求を受信したことを判定する。例えば、AMF２は、ステップ７０６で受信したNASメッセージが、S-NSSAI #1及び新たなPDU session IDを含むことに基づいて、S-NSSAI #1に関連付けられた新たなPDUセッション確立要求の受信を判断してもよい。この場合、AMF２は、新たなPDUセッションの確立の拒絶を示すNASメッセージによってUE１に応答する。具体的には、AMF２は、PDU Session Establishment Rejectメッセージを生成し、これをUE１に送信してもよい。当該PDU Session Establishment Rejectメッセージは、再認証及び再認可手順が実行中であることを示す新たな5GSM causeを包含してもよい。さらに又はこれに代えて、AMF２は、PDU Session Establishment Rejectメッセージを含むN1 SMコンテナと再認証及び再認可手順が実行中であることを示す新たな5GMM causeとを含むNASメッセージ（e.g., DL NAS Transportメッセージ）をUE１に送信してもよい。当該NASメッセージは、S-NSSAI #1を含んだPending NSSAI IEを含んでもよい。他の例として、当該NASメッセージは、S-NSSAI #1がそれから削除された更新後の（updated）Allowed NSSAI及びS-NSSAI #1がそれに追加された更新後のPending NSSAIを含んでもよい。

【００８８】

さらに、AMF２は、UE１のためのUEコンテキスト内のAllowed NSSAIからS-NSSAI #1を削除し、UE１のUEコンテキスト内のPending NSSAIにS-NSSAI #1を格納する（追加する）。ステップ７０８では、UE１は、UE１の（non-volatile）メモリに格納されているUE NSSAI設定（NSSAI storage）を更新する。具体的には、UE１は、当該NASメッセージを介して受信したPending NSSAI IEに含まれるS-NSSAI#1がUE NSSAI設定（NSSAI storage）内のAllowed NSSAIに含まれる場合、これをAllowed NSSAIから削除し、Pending NSSAIに格納する。

【００８９】

図８は、AMF２の動作の他の例を示すフローチャートである。ステップ８０１～８０３は、図４のステップ４０１～４０３と同様である。ステップ８０２の再認証及び再認可手順は、上述の理由又は他の理由のためにAMF２によって開始される。

【００９０】

ステップ８０４では、AMF２は、特定のS-NSSAIのための再認証及び再認可手順の失敗を検出する。例えば、AMF２は、特定のS-NSSAIのためのEAP-based authentication procedureの失敗を示すメッセージをAUSF４から受信したか否かを判定してもよい。特定のS-NSSAIのための再認証及び再認可手順の失敗に応答して、AMF２は、UE１のためのUEコンテキスト内のPending NSSAIから当該特定のS-NSSAIを削除し、これをRejected NSSAIに格納してもよい。

【００９１】
ステップ８０５では、AMF２は、特定のS-NSSAIをUE NSSAI設定内のPending NSSAIから削除しこれをUE NSSAI設定内のRejected NSSAIに格納することをUE１に引き起こすNASメッセージをUE１に送信する。具体的には、AMF２は、当該特定のS-NSSAIをRejected NSSAI IEに含めて、これをNASメッセージを介してUE１に供給する。他の例として、AMF２は、特定のS-NSSAIがそれから削除された更新後の（updated）Pending NSSAI及び当該特定のS-NSSAIがそれに追加された更新後のRejected NSSAIを共に作成し、これをNASメッセージを介してUE１に供給してもよい。当該NASメッセージは、例えば、UE Configuration Update Commandメッセージであってもよい。これに代えて、当該NASメッセージは、EAP失敗を示すNAS MM transportメッセージであってもよい。当該NASメッセージは、再認証及び再認可手順の失敗を示すcause IEを含んでもよい。言い換えると、当該NASメッセージに含まれる当該特定のS-NSSAIは、再認証及び再認可手順の失敗を示すcause IEに関連付けられてもよい。当該Cause IEは、例えば、S-NSSAI is not available due to the failed or revoked network slice-specific authorization and authenticationであってもよい。
【００９２】
さらに、AMF２は、特定のS-NSSAIに関連付けられた新たなセッションの確立手順が行われている又は中断されているなら、当該PDUセッションの確立の拒絶を示すNASメッセージをUE１に送信してもよい。具体的には、AMF２は、PDU Session Establishment Rejectメッセージを生成し、これをUE１に送信してもよい。当該PDU Session Establishment Rejectメッセージは、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示す新たな5GSM causeを包含してもよい。さらに又はこれに代えて、AMF２は、PDU Session Establishment Rejectメッセージを含むN1 SMコンテナと再認証及び再認可手順の失敗を示す新たな5GMM causeとを含むNASメッセージ（e.g., DL NAS Transportメッセージ）をUE１に送信してもよい。当該NASメッセージは、S-NSSAI#1を含んだRejected NSSAI IEを含んでもよい。他の例として、当該NASメッセージは、S-NSSAI #1がそれから削除された更新後の（updated）Pending NSSAI及びS-NSSAI #1がそれに追加された更新後のRejected NSSAIを含んでもよい。当該NASメッセージは、再認証及び再認可手順の失敗を示すcause IEを含んでもよい。言い換えると、当該NASメッセージに含まれる当該特定のS-NSSAIは、再認証及び再認可手順の失敗を示すcause IEに関連付けられてもよい。当該Cause IEは、例えば、S-NSSAI is not available due to the failed or revoked network slice-specific authorization and authenticationであってもよい。
【００９３】
＜第２の実施形態＞
本実施形態は、ネットワークスライスのための再認証及び再認可手順と新たなPDUセッションの確立と衝突を回避するための解決策を提供する。本実施形態に係るセルラーネットワークの構成例は、図１に示された例と同様であってもよい。
【００９４】
図９は、本実施形態に係るAMF２の動作の一例を示すフローチャートである。ステップ９０１では、AMF２は、UE１に現在許可された特定のS-NSSAIのための再認証及び再認可手順（再度又は追加のNSSAA）をトリガーする。NSSAA手順は、既存のそれと同様であってもよい。既存のNSSAA手順は、非特許文献２の第4.2.9.1節に規定されている。
【００９５】
ステップ９０２では、AMF２は、再認証及び再認可手順（NSSAA手順）が実行中である特定のS-NSSAIに関連付けられた新たなPDUセッション確立の要求をUE１から受信する。より具体的には、AMF２は、NASメッセージ（e.g., UL NAS Transportメッセージ）をUE１から受信する。当該NASメッセージは、特定のS-NSSAI、新たなPDU session ID、及びN1 SMコンテナ (PDU Session Establishment Request)を包含する。例えば、AMF２は、ステップ９０２で受信したNASメッセージが、特定のS-NSSAI及び新たなPDU session IDを含むことに基づいて、特定のS-NSSAIに関連付けられた新たなPDUセッション

確立要求の受信を判断してもよい。

【００９６】

ステップ９０３では、AMF２は、少なくともNSSAA手順の結果が得られるまでPDUセッション確立手順、または当該PDUセッション確立要求への応答（acceptまたはreject）を中断（suspendまたはrefrain）する。例えば、AMF２は、UE１のためのUEコンテキストを参照し、特定のS-NSSAIがPending NSSAIに格納されているなら、少なくともNSSAA手順の結果が得られるまでPDUセッション確立手順を中断（suspendまたはrefrain）してもよい。

【００９７】

図９に示された動作によれば、AMF２は、再認証及び再認可手順が実行されているネットワークスライスに関連付けられた新たなPDUセッションの確立を妨げることができる。

【００９８】

なお、第１の実施形態（図６のステップ６０４）で説明されたように、AMF２は、特定のS-NSSAIをUE NSSAI設定内のAllowed NSSAIから削除しこれをUE NSSAI設定内のPending NSSAIに格納することをUE１に引き起こすNASメッセージをUE１に送信してもよい。これにより、AMF２は、再認証及び再認可手順が実行中であるS-NSSAIに関連付けられた新たなPDUセッション確立をUE１がさらに要求することを抑止できる。

【００９９】

上述のように、UE1のUE NSSAI設定は、S-NSSAIsのNSSAAによる許可ステータスを示すステータス情報を含んでもよい。S-NSSAIsのステータス情報は、各S-NSSAIについてNSSAAによる現在の許可(permission)が再認証及び再認可中にもavailable（allowed to use, 又はpermitted）であるか、それともunavailable（not allowed to use, 又はnot permitted）であるかを示してもよい。この場合、AMF２は、S-NSSAI #1のステータスをavailable状態からunavailable状態に変更することをUE１に引き起こすための情報を当該NASメッセージに含めてもよい。これに代えて、AMF２は、S-NSSAI #1のステータスがavailable状態のまま維持されることをUE１に指示するための情報を当該NASメッセージに含めてもよい。UE１は、受け取った当該情報に基づいて、S-NSSAI #1のステータス情報を更新する。

【０１００】

例えば、UE１は、S-NSSAIsそれぞれについてのNSSAAによる許可に関するステータスを示す情報に基づいて、PDUセッション確立要求を禁止されてもよいし、PDUセッション確立手順を中止または中断（suspend）してもよい。より具体的には、UE１は、特定のS-NSSAIについて現在のNSSAAによる許可が再認証及び再認可中にunavailableであること（not allowed to use, not permitted）を示す情報に関連付けられている、あるいはそのように更新された場合、そのS-NSSAIに関連付けられたPDUセッションの確立を禁止されてもよいし、当該PDUセッションの確立の手順を中止または中断(suspend、またはrefrain)するよう動作してもよい。

【０１０１】

AMF２は、再認証のためのNSSAA手順が成功したなら、中断されていたPDUセッション確立手順を再開してもよい。

【０１０２】

一方、AMF２は、再認証のためのNSSAA手順が失敗したなら中断されていたPDUセッション確立手順を拒絶してもよい。図１０は、特定のS-NSSAIのための再認証及び再認可手順（NSSAA手順）が失敗したときのAMF２の動作の一例を示すフローチャートである。図１０に記載された動作は、図９のステップ９０３の後に行われる。

【０１０３】

ステップ１００１では、AMF２は、特定のS-NSSAIのための再認証及び再認可手順の失敗を検出（又は認識）する。AMF２は、NSSAA手順（EAP認証）の失敗を示す通知をAUSF４から受信することで、再認証のためのNSSAA手順の失敗を検出してもよい。より具体的には、AMF２は、特定のS-NSSAIのためのEAP-based authentication procedureの

失敗を示すメッセージをAUSF４から受信したか否かを判定してもよい。さらに又はこれに代えて、AMF２は、再認証及び再認可手順（NSSAA手順）をトリガーする際にタイマを開始し、再認証及び再認可手順の結果（成功又は失敗）をAUSF４から受信する前に当該タイマが満了したなら、再認証及び再認可手順が失敗したと判断してもよい。

【０１０４】

ステップ１００２では、AMF２は、中断されていたPDUセッション確立手順の拒絶を示すNASメッセージをUE１に送信する。具体的には、AMF２は、PDU Session Establishment Rejectメッセージを生成し、これをUE１に送信してもよい。当該PDU Session Establishment Rejectメッセージは、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示す新たな5GSM causeを包含してもよい。さらに又はこれに代えて、AMF２は、PDU Session Establishment Rejectメッセージを含むN1 SMコンテナと再認証及び再認可手順の失敗を示す新たな5GMM causeとを含むNASメッセージ（e.g., DL NAS Transportメッセージ）をUE１に送信してもよい。当該NASメッセージは、特定のS-NSSAIを含んだRejected NSSAI IEを含んでもよい。他の例として、当該NASメッセージは、特定のS-NSSAIがそれから削除された更新後のAllowed NSSAI（又はPending NSSAI）及び特定のS-NSSAIがそれに追加された更新後のRejected NSSAIを含んでもよい。当該NASメッセージは、再認証及び再認可手順の失敗を示すcause IEを含んでもよい。言い換えると、当該NASメッセージに含まれる特定のS-NSSAIは、再認証及び再認可手順の失敗を示すcause IEに関連付けられてもよい。当該Cause IEは、例えば、S-NSSAI is not available due to the failed or revoked network slice-specific authorization and authenticationであってもよい。

【０１０５】

＜第３の実施形態＞

本実施形態は、ネットワークスライスのための再認証及び再認可手順と新たなPDUセッションの確立と衝突を回避するための他の解決策を提供する。本実施形態に係るセルラーネットワークの構成例は、図１に示された例と同様であってもよい。

【０１０６】

図１１は、本実施形態に係るAMF２の動作の一例を示すフローチャートである。ステップ１１０１及び１１０２は、図９のステップ９０１及び９０２と同様である。すなわち、ステップ１１０１では、AMF２は、UE１に現在許可された特定のS-NSSAIのための再認証及び再認可手順（再度又は追加のNSSAA）をトリガーする。ステップ１１０２では、AMF２は、再認証及び再認可手順（NSSAA手順）が実行中である特定のS-NSSAIに関連付けられた新たなPDUセッション確立の要求をUE１から受信する。

【０１０７】

ステップ１１０３では、AMF２は、ステップ１１０２で受信したPDUセッション確立要求を拒絶する。具体的には、PDUセッション確立要求が拒絶されることを示すNASメッセージによりUE１に応答する。当該メッセージは、再認証及び再認可手順が実行中であることを示すcause IEを包含してもよい。より具体的には、AMF２は、PDU Session Establishment Rejectメッセージを生成し、これを包含するN1 SMコンテナを運ぶNASメッセージ（e.g., DL NAS Transportメッセージ）をUE１に送信してもよい。当該NASメッセージは、特定のS-NSSAIを含んだPending NSSAI IEを含んでもよい。他の例として、当該NASメッセージは、特定のS-NSSAIがそれから削除された更新後のAllowed NSSAI及び特定のS-NSSAIがそれに追加された更新後のPending NSSAIを含んでもよい。さらに又はこれに代えて、当該NASメッセージ（e.g., DL NAS Transportメッセージ）は、再認証及び再認可手順が実行中であることを示す新たなcause IE（e.g., 5GMM Cause IE）を包含してもよい。さらに又はこれに代えて、AMF２により生成されるPDU Session Establishment Rejectメッセージは、再認証及び再認可手順が実行中であることを示す新たなcause IE（e.g., 5GSM Cause IE）を含んでもよい。

【０１０８】

図１１に示された動作によれば、AMF２は、再認証及び再認可手順が実行されているネ

ットワークスライスに関連付けられた新たなPDUセッションの確立を妨げることができる。

【０１０９】

＜第４の実施形態＞

本実施形態は、ネットワークスライスの再認証及び再認可が失敗したときのAMF２の動作の例を提供する。

【０１１０】

図１２は、本実施形態に係るAMF２の動作の一例を示すフローチャートである。ステップ１２０１では、AMF２は、特定のS-NSSAIのための再認証及び再認可手順（NSSAA手順）の失敗を検出（又は認識）する。AMF２は、NSSAA手順（EAP認証）の失敗を示す通知をAUSF４から受信することで、再認証のためのNSSAA手順の失敗を検出してもよい。より具体的には、AMF２は、特定のS-NSSAIのためのEAP-based authentication procedureの失敗を示すメッセージをAUSF４から受信したか否かを判定してもよい。さらに又はこれに代えて、AMF２は、再認証及び再認可手順（NSSAA手順）をトリガーする際にタイマを開始し、再認証及び再認可手順の結果（成功又は失敗）をAUSF４から受信する前に当該タイマが満了したなら、再認証及び再認可手順が失敗したと判断してもよい。

【０１１１】

ステップ１２０２では、AMF２は、特定のS-NSSAIのための再認証及び再認可手順の失敗に応答して、当該特定のS-NSSAIに関連付けられた全てのPDUセッションを解放するための解放手順を開始する。AMF２は、EAP-based authentication procedureの失敗を示すメッセージのAUSF４からの受信に応答して、PDUセッション解放手順を開始してもよい。

【０１１２】

AMF２は、非特許文献２の第4.3.4.2章に記載されたPDUセッション解放手順に従って、特定のS-NSSAIに関連付けられた１又はそれ以上のPDUセッションを解放するためにNsmf_PDUSession_UpdateSMContext（又はNsmf_PDUSession_ReleaseSMContext）service operationを実施（invoke）してもよい。より具体的には、AMF２は、Release Indicationを含むメッセージ（例えば、Nsmf_PDUSession_UpdateSMContextメッセージ）をSMF３に送信してもよい。AMF２は、network-requested PDU session release procedureを起動するために、当該S-NSSAIに関連付けられた１又はそれ以上のPDUセッションのPDUセッションIDをSMF３に通知してもよい。AMF２は、これらのPDUセッションIDを上記メッセージに含めてもよいし、別のメッセージによりこれらのPDUセッションIDをSMF３に通知してもよい。またAMF２は、当該特定のS-NSSAIを上記メッセージに含めてもよいし、別のメッセージにより当該S-NSSAIをSMF３に通知してもよい。これに代えて、AMF２は、Nsmf_PDUSession_ReleaseSMContextメッセージをSMF３に送信してもよい。AMF２は、Nsmf_PDUSession_ReleaseSMContextメッセージに、当該S-NSSAIに関連付けられた１又はそれ以上のPDUセッションのPDUセッションIDを含めてもよい。AMF２は、Nsmf_PDUSession_ReleaseSMContextメッセージに、当該S-NSSAIを含めてもよい。

【０１１３】

AMF２は、PDUセッション解放手順において、UE１のための特定のS-NSSAIのための再認証及び再認可手順（NSSAA手順）の失敗をSMF３に通知してもよい。具体的には、AMF２は、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示すcause IEを包含するメッセージをSMF３に送信してもよい。当該メッセージは、例えば、Nsmf_PDUSession_UpdateSMContextメッセージ（又はNsmf_PDUSession_ReleaseSMContextメッセージ）であってもよい。

【０１１４】

図１２に示された動作によれば、AMF２は、再認証及び再認可手順に失敗したネットワークスライスに関連付けられたPDUセッションを速やかに解放できる。

【０１１５】

図１３は、ネットワークスライスの再認証及び再認可手順に失敗したときのUE１、AMF２、及びSMF３の動作の一例を示している。ステップ１３０１では、AAA-S９は、特定のS-NSSAI（ここではS-NSSAI #1）によって特定されるネットワークスライスのためのEAP認証の失敗をAUSF４に通知する。具体的には、AAA-S９は、EAP認証失敗を示すAAAプロトコルメッセージをAUSF４に送信してもよい。当該メッセージは、S-NSSAI #1及びEAP認証失敗を示し、UE１のGPSIをさらに示す。当該メッセージは、AAA-S９からAUSF４に直接的に送られてもよいし、図示されていないAAA Proxy（AAA-P）を介してAUSF４に送られてもよい。

【０１１６】

ステップ１３０２では、AUSF４は、S-NSSAI #1のためのEAP認証の失敗をAMF２に通知する。具体的には、AUSF４は、Nausf_NSSAA_Authenticate Responseメッセージを AMF２に送信してもよい。当該メッセージは、S-NSSAI #1及びEAP認証失敗を示し、UE１のGPSIをさらに示す。

【０１１７】

ステップ１３０３では、再認証に失敗したS-NSSAI #1に関連付けられているUE１のPDUセッションが存在する場合、AMF２は、S-NSSAI #1に関連付けられたUE１の全てのPDUセッションを解放するための手続き（例えば、Nsmf_PDUSession_UpdateSMContext（又はNsmf_PDUSession_ReleaseSMContext） service operation）を実施（invoke）する。この手続において、AMF２は、Release Indicationを含むメッセージ（例えば、Nsmf_PDUSession_UpdateSMContextメッセージ）をSMF３に送信する。AMF２は、network-requested PDU session release procedureを起動するために、S-NSSAI #1に関連付けられた１又はそれ以上のPDUセッションのPDUセッションIDをSMF３に通知してもよい。AMF２は、これらのPDUセッションIDを上記メッセージに含めてもよいし、別個のメッセージによりこれらのPDUセッションIDをSMF３に通知してもよい。またAMF２は、S-NSSAI #1を上記メッセージに含めてもよいし、別個のメッセージによりS-NSSAI #1をSMF３に通知してもよい。これに代えて、AMF２は、Nsmf_PDUSession_ReleaseSMContextメッセージをSMF３に送信してもよい。AMF２は、Nsmf_PDUSession_ReleaseSMContextメッセージに、S-NSSAI #1に関連付けられた１又はそれ以上のPDUセッションのPDUセッションIDを含めてもよい。AMF２は、Nsmf_PDUSession_ReleaseSMContextメッセージに、S-NSSAI #1を含めてもよい。上述のように、当該メッセージは、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示すcause IEを包含してもよい。

【０１１８】

ステップ１３０４では、AMF２は、再認証に失敗したS-NSSAI #1をAllowed NSSAI（又はPending NSSAI）から削除するために、UE１とシグナルしてUE NSSAI設定（NSSAI storage）を更新する。具体的には、AMF２は、S-NSSAI #1がAllowed NSSAI（又はPending NSSAI）から削除され、これがRejected NSSAIに含まれることを示すUE Configuration Update CommandメッセージをUE１に送信する。当該UE Configuration Update Commandメッセージの受信に応答して、UE１は、UE１の（non-volatile）メモリに格納されているUE NSSAI設定（NSSAI storage）を更新する。具体的には、UE１は、UE NSSAI設定（NSSAI storage）内のAllowed NSSAI（又はPending NSSAI）からS-NSSAI #1を削除し、これをRejected NSSAIに格納する。当該UE Configuration Update Commandメッセージは、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示すcause IEを包含してもよい。言い換えると、当該UE Configuration Update CommandメッセージにS-NSSAI #1は、再認証及び再認可手順の失敗を示すcause IEに関連付けられてもよい。当該Cause IEは、例えば、S-NSSAI is not available due to the failed or revoked network slice-specific authorization and authentication であってもよい。

【０１１９】

図１３の手順は、適宜変形されることができる。例えば、AMF２は、UE Configuratio

n Update手順（ステップ１３０４）の後に、PDUセッションの解放をSMF３に要求してもよい。

【０１２０】

図１４は、ネットワークスライスの再認証及び再認可手順に失敗したときのUE１、AMF２、及びSMF３の動作の他の例を示している。図１４では、AMF２は、UE Configuration Update手順（ステップ１４０３）の後に、PDUセッションの解放をSMF３に要求する（ステップ１４０５）。

【０１２１】

図１４のステップ１４０１及び１４０２は、図１３のステップ１３０１及び１３０２と同様である。ステップ１４０３では、AMF２は、再認証に失敗したS-NSSAI #1をAllowed NSSAI（又はPending NSSAI）から削除するために、UE Configuration Update手順を実行する。UE Configuration Update手順では、AMF２は、S-NSSAI #1がAllowed NSSAI（又はPending NSSAI）から削除され、これがRejected NSSAIに含まれることを示すUE Configuration Update Commandメッセージを UE１に送信する。当該UE Configuration Update Commandメッセージは、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示すcause IEを包含してもよい。言い換えると、当該UE Configuration Update Commandメッセージに含まれるS-NSSAI #1は、再認証及び再認可手順の失敗を示すcause IEに関連付けられてもよい。当該Cause IEは、例えば、S-NSSAI is not available due to the failed or revoked network slice-specific authorization and authenticationであってもよい。

【０１２２】

S-NSSAI #1に関連付けられているUE１の１又はそれ以上のPDUセッションが存在する場合、AMF２は、これらPDUセッションが解放されるまでの猶予期間を示す情報要素をUE Configuration Update Commandメッセージに含める。当該情報要素は、猶予期間の満了を判定するために使用されるタイマの値であってもよい。AMF２は、UE Configuration Update Commandメッセージの送信をトリガーとして当該タイマを開始してもよい。これに代えて、AMF２は、UE Configuration Update Commandメッセージに対するレスポンスメッセージ（例えば UE Configuration Update Completeメッセージ）の受信をトリガーとして当該タイマを開始してもよい。

【０１２３】

猶予期間を測定するためのタイマが満了した場合（ステップ１４０４）、AMF２は、S-NSSAI #1に関連付けられたUE１の全てのPDUセッションを解放するためにNsmf_PDUSession_UpdateSMContext（又はNsmf_PDUSession_ReleaseSMContext） service operationを実施（invoke）する（ステップ１４０５）。より具体的には、AMF２は、Nsmf_PDUSession_UpdateSMContextメッセージ（又はNsmf_PDUSession_ReleaseSMContextメッセージ）をSMF３に送信する。上述のように、当該メッセージは、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示すcause IEを包含してもよい。AMF２は、猶予期間を測定するためのタイマが満了する前に、UE１より、当該PDU sessionをReleaseするプロシージャの開始を受けた場合、当該タイマを停止して、network-requested PDU session release procedureを終了してもよい。

【０１２４】

図１４の手順によれば、AMF２は、認可を取り消されたネットワークスライスに関連付けられたPDUセッションが猶予期間の経過後に解放されることをUE１に通知することができる。

【０１２５】

図１５は、PDUセッション解放手順の一例を示している。ステップ１５０１では、AMF２は、再認証に失敗したネットワークスライス（S-NSSAI）に関連付けられたPDUセッションの解放を要求するために、メッセージ（例えば、Nsmf_PDUSession_UpdateSMContextメッセージ、又はNsmf_PDUSession_ReleaseSMContextメッセージ）をSMF３に送信する。当該メッセージは、Release Indicationを包含し、さらに再認証及び再認可

手順の失敗（e.g., NSSAA failure）を示すcause IEを包含する。AMF２は、network-requested PDU session release procedureを起動するために、当該S-NSSAIに関連付けられた１又はそれ以上のPDUセッションのPDUセッションIDをSMF３に通知してもよい。AMF２は、これらのPDUセッションIDを上記メッセージに含めてもよいし、別のメッセージによりこれらのPDUセッションIDをSMF３に通知してもよい。またAMF２は、当該S-NSSAIを上記メッセージに含めてもよいし、別個のメッセージにより当該S-NSSAIをSMF３に通知してもよい。ステップ１５０１は、図１３のステップ１３０３、又は図１４のステップ１４０５に対応する。

【０１２６】

ステップ１５０２では、SMF３は、応答メッセージをAMF２に送信する。例えば、SMF３は、Nsmf_PDUSession_UpdateSMContext Responseメッセージ又はNsmf_PDUSession_ReleaseSMContext ResponseメッセージによってAMF２に応答してもよい。当該メッセージは、PDU Session Release Commandを包含するN1 SMコンテナを含む。当該メッセージは、さらに、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示すcause IEを包含してもよい。さらに又はこれに代えて、PDU Session Release Commandは、再認証及び再認可手順の失敗（e.g., NSSAA failure）（又は当該S-NSSAIがnot availableであること）を示す5GSM Cause IEを包含してもよい。

【０１２７】

ステップ１５０３では、AMF２は、PDU Session Release Commandを包含するN1 SMコンテナを含むNASメッセージをUE１にAN５を介して送信する。PDU Session Release Commandは、再認証及び再認可手順の失敗（e.g., NSSAA failure）（又は当該S-NSSAIがnot availableであること）を示す5GSM Cause IEを包含してもよい。

【０１２８】

ステップ１５０４では、UE１は、PDU Session Release Commandを承認（acknowledge）するために、PDU Session Release Complete を包含するNASメッセージをAMF２に送信する。PDU Session Release Completeは、再認証及び再認可手順の失敗（e.g., NSSAA failure）を示す5GSM Cause IEを包含してもよい。

【０１２９】

ステップ１５０５では、AMF２は、Nsmf_PDUSession_UpdateSMContext service operationを実施（invoke）し、SMF３にN1 SMコンテナ（PDU Session Release Complete）をフォワードする。

【０１３０】

＜第５の実施形態＞

本実施形態に係るセルラーネットワークの構成例は、図１に示された例と同様であってもよい。本実施形態は、ネットワークスライスの再認証及び再認可が失敗したときのAMF２の動作の他の例を提供する。

【０１３１】

図１６は、本実施形態に係るAMF２の動作の一例を示すフローチャートである。ステップ１６０１は、図１２のステップ１２０１と同様である。すなわち、AMF２は、AMF２は、特定のS-NSSAIのための再認証及び再認可手順（NSSAA手順）の失敗を検出する。ステップ１６０２では、AMF２は、特定のS-NSSAIのための再認証及び再認可手順の失敗をSMF３に通知する。AMF２から通知メッセージ（ステップ１６０２）を受信したなら、SMF３は、当該特定のS-NSSAIに関連付けられたPDUセッションの解放を決定する。

【０１３２】

図１６に示された動作によれば、AMF２は、特定のS-NSSAIのための再認証及び再認可手順の失敗をSMF３に通知し、これにより再認証に失敗した特定のS-NSSAI（又はこれにより特定されるネットワークスライス）に関連付けられたPDUセッションを解放するようSMF３を支援できる。

【０１３３】

＜第６の実施形態＞

本実施形態に係るセルラーネットワークの構成例は、図１に示された例と同様であってもよい。本実施形態は、ネットワークスライスの再認証及び再認可が失敗したときのUE１の動作の一例を提供する。

【０１３４】

図１７は、本実施形態に係るUE１の動作の一例を示すフローチャートである。ステップ１７０１では、UE１は、特定のS-NSSAIのための再認証及び再認可手順の失敗を検出（又は認識）する。例えば、UE１は、特定のS-NSSAIがAllowed NSSAI（又はPending NSSAI）から削除され、これがRejected NSSAIに含まれることを示すUE Configuration Update Commandメッセージを AMF２から受信したなら、当該特定のS-NSSAIの再認証及び再認可手順の失敗を検出（又は認識）してもよい。さらに又はこれに代えて、UE１は、特定のS-NSSAIのための再認証の失敗を示す情報要素を包含するNASメッセージをAMF２から受信したなら、当該特定のS-NSSAIのための再認証及び再認可手順の失敗を検出（又は認識）してもよい。

【０１３５】

ステップ１７０２では、UE１のための特定のS-NSSAIの再認証の失敗に応答して、UE１は、当該特定のS-NSSAIに関連付けられたPDUセッションの解放をネットワークに要求する。具体的には、UE１は、当該特定のS-NSSAIに関連付けられたPDUセッションの解放を要求するためのNASメッセージをAMF２に送信する。より具体的には、UE１のNAS-MMレイヤは、特定のS-NSSAIの再認証の失敗をUE１のNAS-SMレイヤに通知する。UE１のNAS-SMレイヤは、下位レイヤ（NAS-MMレイヤ）からの通知に応答して、再認証に失敗した特定のS-NSSAIに関連付けられたPDUセッションに関するPDU Session Release Requestを生成する。UE１のNAS-SMレイヤは、生成したPDU Session Release Requestを、PDU Session IDと共にNAS-MMレイヤに渡す。UE１のNAS-MMレイヤは、PDU Session IDとN1 SMコンテナ（PDU Session Release Request）とを包含するNASメッセージ（e.g., UL NAS Transportメッセージ）をAMF２に送信する。当該NASメッセージ及び当該PDU Session Release Requestの一方又は両方は、再認証及び再認可手順の失敗の取り消しを示すcause情報要素を含んでもよい。

【０１３６】

図１７に示された動作によれば、UE１は、再認証に失敗したネットワークスライスに関連付けられたPDUセッションを速やかに解放できる。

【０１３７】

図１８は、ネットワークスライスの再認証及び再認可手順に失敗したときのUE１、AMF２、及びSMF３の動作の一例を示している。ステップ１８０１及び１８０２は、図１３のステップ１３０１及び１３０２と同様である。すなわち、AAA-S９は、特定のS-NSSAI（ここではS-NSSAI #1）のためのEAP認証の失敗をAMF２にAUSF４を介して通知する。

【０１３８】

ステップ１８０３では、AMF２は、再認証に失敗したS-NSSAI #1をAllowed NSSAI（又はPending NSSAI）から削除するために、UE１とシグナルしてUE NSSAI設定（NSSAI storage）を更新する。具体的には、AMF２は、S-NSSAI #1がAllowed NSSAI（又はPending NSSAI）から削除され、これがRejected NSSAIに含まれることを示すUE Configuration Update CommandメッセージをUE１に送信する。当該UE Configuration Update Commandメッセージの受信に応答して、UE１は、UE１の（non-volatile）メモリに格納されているUE NSSAI設定（NSSAI storage）を更新する。具体的には、UE１は、UE NSSAI設定（NSSAI storage）内のAllowed NSSAI（又はPending NSSAI）からS-NSSAI #1を削除し、これをRejected NSSAIに格納する。当該UE Configuration Update Commandメッセージは、再認証及び再認可手順の失敗を示すcause IEを包含してもよい。言い換えると、当該UE Configuration Update Commandメッセージに含まれる特定のS-NSSAIは、再認証及び再認可手順の失敗を示すcause IEに関連付けられてもよい。当該Cause IEは、例えば、S-NSSAI is not available due to the failed or revoked network slice-specific authorization and authenticationであってもよい。

【０１３９】
ステップ１８０４では、UE１は、S-NSSAI #1のための再認証の失敗を検出したことに応答して、S-NSSAI #1に関連付けられたPDUセッションの解放をネットワークに要求する。具体的には、UE１は、S-NSSAI #1に関連付けられたPDUセッションのPDU Session IDとN1 SMコンテナ（PDU Session Release Request）とを包含するNASメッセージをAMF２に送信する。上述のように、当該NASメッセージ及び当該PDU Session Release Requestの一方又は両方は、再認証及び再認可手順の失敗を示すcause IEを含んでもよい。
【０１４０】
ステップ１８０５では、AMF２は、Nsmf_PDUSession_UpdateSMContext service operationを実施（invoke）し、SMF３にN1 SMコンテナ（PDU Session Release Request）をフォワードする。
【０１４１】
続いて以下では、上述の複数の実施形態に係るUE１、AMF２、及びSMF３の構成例について説明する。図１９は、UE１の構成例を示すブロック図である。Radio Frequency（RF）トランシーバ１９０１は、NG-RAN nodesと通信するためにアナログRF信号処理を行う。RFトランシーバ１９０１は、複数のトランシーバを含んでもよい。RFトランシーバ１９０１により行われるアナログRF信号処理は、周波数アップコンバージョン、周波数ダウンコンバージョン、及び増幅を含む。RFトランシーバ１９０１は、アンテナアレイ１９０２及びベースバンドプロセッサ１９０３と結合される。RFトランシーバ１９０１は、変調シンボルデータ（又はOFDMシンボルデータ）をベースバンドプロセッサ１９０３から受信し、送信RF信号を生成し、送信RF信号をアンテナアレイ１９０２に供給する。また、RFトランシーバ１９０１は、アンテナアレイ１９０２によって受信された受信ＲＦ信号に基づいてベースバンド受信信号を生成し、これをベースバンドプロセッサ１９０３に供給する。RFトランシーバ１９０１は、ビームフォーミングのためのアナログビームフォーマ回路を含んでもよい。アナログビームフォーマ回路は、例えば複数の移相器及び複数の電力増幅器を含む。
【０１４２】
ベースバンドプロセッサ１９０３は、無線通信のためのデジタルベースバンド信号処理（データプレーン処理）とコントロールプレーン処理を行う。デジタルベースバンド信号処理は、(a) データ圧縮／復元、(b) データのセグメンテーション／コンカテネーション、(c) 伝送フォーマット（伝送フレーム）の生成／分解、(d) 伝送路符号化／復号化、(e) 変調（シンボルマッピング）／復調、及び(f) Inverse Fast Fourier Transform（IFFT）によるOFDMシンボルデータ（ベースバンドOFDM信号）の生成などを含む。一方、コントロールプレーン処理は、レイヤ１（e.g., 送信電力制御）、レイヤ２（e.g., 無線リソース管理、及びhybrid automatic repeat request（HARQ）処理）、及びレイヤ３（e.g., アタッチ、モビリティ、及び通話管理に関するシグナリング）の通信管理を含む。
【０１４３】
例えば、ベースバンドプロセッサ１９０３によるデジタルベースバンド信号処理は、Service Data Adaptation Protocol（SDAP）レイヤ、Packet Data Convergence Protocol（PDCP）レイヤ、Radio Link Control（RLC）レイヤ、Medium Access Control（MAC）レイヤ、およびPhysical（PHY）レイヤの信号処理を含んでもよい。また、ベースバンドプロセッサ１９０３によるコントロールプレーン処理は、Non-Access Stratum（NAS）プロトコル、Radio Resource Control（RRC）プロトコル、及びMAC Control Elements（CEs）の処理を含んでもよい。
【０１４４】
ベースバンドプロセッサ１９０３は、ビームフォーミングのためのMultiple Input Multiple Output（MIMO）エンコーディング及びプリコーディングを行ってもよい。
【０１４５】
ベースバンドプロセッサ１９０３は、デジタルベースバンド信号処理を行うモデム・プ

ロセッサ（e.g., Digital Signal Processor（DSP））とコントロールプレーン処理を行うプロトコルスタック・プロセッサ（e.g., Central Processing Unit（CPU）又はMicro Processing Unit（MPU））を含んでもよい。この場合、コントロールプレーン処理を行うプロトコルスタック・プロセッサは、後述するアプリケーションプロセッサ１９０４と共通化されてもよい。

【０１４６】

アプリケーションプロセッサ１９０４は、CPU、MPU、マイクロプロセッサ、又はプロセッサコアとも呼ばれる。アプリケーションプロセッサ１９０４は、複数のプロセッサ（複数のプロセッサコア）を含んでもよい。アプリケーションプロセッサ１９０４は、メモリ１９０６又は図示されていないメモリから読み出されたシステムソフトウェアプログラム（Operating System（OS））及び様々なアプリケーションプログラム（例えば、通話アプリケーション、WEBブラウザ、メーラ、カメラ操作アプリケーション、音楽再生アプリケーション）を実行することによって、UE１の各種機能を実現する。

【０１４７】

幾つかの実装において、図１９に破線（１９０５）で示されているように、ベースバンドプロセッサ１９０３及びアプリケーションプロセッサ１９０４は、１つのチップ上に集積されてもよい。言い換えると、ベースバンドプロセッサ１９０３及びアプリケーションプロセッサ１９０４は、１つのSystem on Chip（SoC）デバイス１９０５として実装されてもよい。SoCデバイスは、システムLarge Scale Integration（LSI）またはチップセットと呼ばれることもある。

【０１４８】

メモリ１９０６は、揮発性メモリ若しくは不揮発性メモリ又はこれらの組合せである。メモリ１９０６は、物理的に独立した複数のメモリデバイスを含んでもよい。揮発性メモリは、例えば、Static Random Access Memory（SRAM）若しくはDynamic RAM（DRAM）又はこれらの組み合わせである。不揮発性メモリは、マスクRead Only Memory（MROM）、Electrically Erasable Programmable ROM（EEPROM）、フラッシュメモリ、若しくはハードディスクドライブ、又はこれらの任意の組合せである。例えば、メモリ１９０６は、ベースバンドプロセッサ１９０３、アプリケーションプロセッサ１９０４、及びSoC１９０５からアクセス可能な外部メモリデバイスを含んでもよい。メモリ１９０６は、ベースバンドプロセッサ１９０３内、アプリケーションプロセッサ１９０４内、又はSoC１９０５内に集積された内蔵メモリデバイスを含んでもよい。さらに、メモリ１９０６は、Universal Integrated Circuit Card（UICC）内のメモリを含んでもよい。

【０１４９】

メモリ１９０６は、上述の複数の実施形態で説明されたUE１による処理を行うための命令群およびデータを含む１又はそれ以上のソフトウェアモジュール（コンピュータプログラム）１９０７を格納してもよい。幾つかの実装において、ベースバンドプロセッサ１９０３又はアプリケーションプロセッサ１９０４は、当該ソフトウェアモジュール１９０７をメモリ１９０６から読み出して実行することで、上述の実施形態で図面を用いて説明されたUE１の処理を行うよう構成されてもよい。

【０１５０】

なお、上述の実施形態で説明されたUE１によって行われるコントロールプレーン処理及び動作は、RFトランシーバ１９０１及びアンテナアレイ１９０２を除く他の要素、すなわちベースバンドプロセッサ１９０３及びアプリケーションプロセッサ１９０４の少なくとも一方とソフトウェアモジュール１９０７を格納したメモリ１９０６とによって実現されることができる。

【０１５１】

図２０は、AMF２の構成例を示している。SMF３も図２０に示されるように構成されてもよい。図２０を参照すると、AMF２は、ネットワークインターフェース２００１、プロセッサ２００２、及びメモリ２００３を含む。ネットワークインターフェース２００１は

、例えば、RAN nodesと通信するため、並びに5GC内の他のネットワーク機能（NFs）又はノードと通信するために使用される。5GC内の他のNFs又はノードは、例えば、UDM、AUSF、SMF、及びPCFを含む。ネットワークインターフェース２００１は、例えば、IEEE 802.3 seriesに準拠したネットワークインタフェースカード（NIC）を含んでもよい。

【０１５２】

プロセッサ２００２は、例えば、マイクロプロセッサ、Micro Processing Unit（MPU）、又はCentral Processing Unit（CPU）であってもよい。プロセッサ２００２は、複数のプロセッサを含んでもよい。

【０１５３】

メモリ２００３は、揮発性メモリ及び不揮発性メモリによって構成される。メモリ２００３は、物理的に独立した複数のメモリデバイスを含んでもよい。揮発性メモリは、例えば、Static Random Access Memory（SRAM）若しくはDynamic RAM（DRAM）又はこれらの組み合わせである。不揮発性メモリは、マスクRead Only Memory（MROM）、Electrically Erasable Programmable ROM（EEPROM）、フラッシュメモリ、若しくはハードディスクドライブ、又はこれらの任意の組合せである。メモリ２００３は、プロセッサ２００２から離れて配置されたストレージを含んでもよい。この場合、プロセッサ２００２は、ネットワークインターフェース２００１又は図示されていないI/Oインタフェースを介してメモリ２００３にアクセスしてもよい。

【０１５４】

メモリ２００３は、上述の複数の実施形態で説明されたAMF２による処理を行うための命令群およびデータを含む１又はそれ以上のソフトウェアモジュール（コンピュータプログラム）２００４を格納してもよい。いくつかの実装において、プロセッサ２００２は、当該ソフトウェアモジュール２００４をメモリ２００３から読み出して実行することで、上述の実施形態で説明されたAMF２の処理を行うよう構成されてもよい。

【０１５５】

図１９及び図２０を用いて説明したように、上述の実施形態に係るUE１、AMF２、及びSMF３が有するプロセッサの各々は、図面を用いて説明されたアルゴリズムをコンピュータに行わせるための命令群を含む１又は複数のプログラムを実行する。このプログラムは、様々なタイプの非一時的なコンピュータ可読媒体（non-transitory computer readable medium）を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体（tangible storage medium）を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えばフレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば光磁気ディスク）、Compact Disc Read Only Memory（CD-ROM）、CD-R、CD-R/W、半導体メモリ（例えば、マスクROM、Programmable ROM（PROM）、Erasable PROM（EPROM）、フラッシュROM、Random Access Memory（RAM））を含む。また、プログラムは、様々なタイプの一時的なコンピュータ可読媒体（transitory computer readable medium）によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

【０１５６】

本明細書における無線端末（User Equipment（UE））は、無線インタフェースを介して、ネットワークに接続されたエンティティである。本明細書の無線端末（UE）は、専用の通信装置に限定されるものではなく、本明細書中に記載された無線端末（UE）の通信機能を有する次のような任意の機器であってもよい。

【０１５７】

「（3GPPで使われる単語としての）ユーザー端末（User Equipment（UE））」、「移動局（mobile station）」、「移動端末（mobile terminal）」、「モバイルデバイス（mobile device）」、及び「無線端末（wireless device）」との用語は、一般的に

互いに同義であることが意図されている。UEは、ターミナル、携帯電話、スマートフォン、タブレット、セルラーIoT端末、IoTデバイス、などのスタンドアローン移動局であってもよい。「UE」及び「無線端末」との用語は、長期間にわたって静止している装置も包含する。

【０１５８】

UEは、例えば、生産設備・製造設備および／またはエネルギー関連機械（一例として、ボイラー、機関、タービン、ソーラーパネル、風力発電機、水力発電機、火力発電機、原子力発電機、蓄電池、原子力システム、原子力関連機器、重電機器、真空ポンプなどを含むポンプ、圧縮機、ファン、送風機、油圧機器、空気圧機器、金属加工機械、マニピュレータ、ロボット、ロボット応用システム、工具、金型、ロール、搬送装置、昇降装置、貨物取扱装置、繊維機械、縫製機械、印刷機、印刷関連機械、紙工機械、化学機械、鉱山機械、鉱山関連機械、建設機械、建設関連機械、農業用機械および／または器具、林業用機械および／または器具、漁業用機械および／または器具、安全および／または環境保全器具、トラクター、軸受、精密ベアリング、チェーン、歯車（ギアー）、動力伝動装置、潤滑装置、弁、管継手、および／または上記で述べた任意の機器又は機械のアプリケーションシステムなど）であってもよい。

【０１５９】

UEは、例えば、輸送用装置（一例として、車両、自動車、二輪自動車、自転車、列車、バス、リヤカー、人力車、船舶（ship and other watercraft）、飛行機、ロケット、人工衛星、ドローン、気球など）であってもよい。

【０１６０】

UEは、例えば、情報通信用装置（一例として、電子計算機及び関連装置、通信装置及び関連装置、電子部品など）であってもよい。

【０１６１】

UEは、例えば、冷凍機、冷凍機応用製品および装置、商業およびサービス用機器、自動販売機、自動サービス機、事務用機械及び装置、民生用電気・電子機械器具（一例として音声機器、スピーカー、ラジオ、映像機器、テレビ、オーブンレンジ、炊飯器、コーヒーメーカー、食洗機、洗濯機、乾燥機、扇風機、換気扇及び関連製品、掃除機など）であってもよい。

【０１６２】

UEは、例えば、電子応用システムまたは電子応用装置（一例として、X線装置、粒子加速装置、放射性物質応用装置、音波応用装置、電磁応用装置、電力応用装置など）であってもよい。

【０１６３】

UEは、例えば、電球、照明、計量機、分析機器、試験機及び計測機械（一例として、煙報知器、対人警報センサ、動きセンサ、無線タグなど）、時計（watchまたはclock）、理化学機械、光学機械、医療用機器および／または医療用システム、武器、利器工匠具、または手道具であってもよい。

【０１６４】

UEは、例えば、無線通信機能を備えたパーソナルデジタルアシスタントまたは装置（一例として、無線カードや無線モジュールなどを取り付けられる、もしくは挿入するよう構成された電子装置（例えば、パーソナルコンピュータや電子計測器など））であってもよい。

【０１６５】

UEは、例えば、有線や無線通信技術を使用した「あらゆるモノのインターネット（IoT：Internet of Things）」において、以下のアプリケーション、サービス、ソリューションを提供する装置またはその一部であってもよい。IoTデバイス（もしくはモノ）は、デバイスが互いに、および他の通信デバイスとの間で、データ収集およびデータ交換することを可能にする適切な電子機器、ソフトウェア、センサ、ネットワーク接続、などを備える。IoTデバイスは、内部メモリの格納されたソフトウェア指令に従う自動化された機器

であってもよい。IoTデバイスは、人間による監督または対応を必要とすることなく動作してもよい。IoTデバイスは、長期間にわたって備え付けられている装置および／または、長期間に渡って非活性状態（inactive）状態のままであってもよい。IoTデバイスは、据え置き型な装置の一部として実装され得る。IoTデバイスは、非据え置き型の装置（例えば車両など）に埋め込まれ得る、または監視される／追跡される動物や人に取り付けられ得る。IoT技術は、人間の入力による制御またはメモリに格納されるソフトウェア命令に関係なくデータを送受信する通信ネットワークに接続されることができる任意の通信デバイス上に実装されることができる。IoTデバイスは、機械型通信（Machine Type Communication、MTC）デバイス、またはマシンツーマシン（Machine to Machine、M2M）通信デバイス、Narrow Band-IoT (NB-IoT) UEと呼ばれることもある。

【０１６６】

UEは、１つまたは複数のIoTまたはMTCアプリケーションをサポートしてもよい。

【０１６７】

MTCアプリケーションのいくつかの例は、3GPP TS22.368 V13.2.0(2017-01-13) Annex B（その内容は参照により本明細書に組み込まれる）に示されたリストに列挙されている。このリストは、網羅的ではなく、一例としてのMTCアプリケーションを示すものである。このリストでは、MTCアプリケーションのサービス範囲 (Service Area)は、セキュリティ (Security)、追跡及びトレース (Tracking & Tracing)、支払い (Payment)、健康 (Health)、リモートメンテナンス／制御 (Remote Maintenance/Control)、計量 (Metering)、及び民生機器 (Consumer Devices)を含む。

【０１６８】

セキュリティに関するMTCアプリケーションの例は、監視システム (Surveillance systems)、固定電話のバックアップ (Backup for landline)、物理アクセスの制御（例えば建物へのアクセス） (Control of physical access (e.g. to buildings))、及び車／運転手のセキュリティ (Car/driver security)を含む。

【０１６９】

追跡及びトレースに関するMTCアプリケーションの例は、フリート管理 (Fleet Management)、注文管理 (Order Management)、テレマティクス保険：走行に応じた課金 (Pay as you drive (PAYD))、資産追跡 (Asset Tracking)、ナビゲーション (Navigation)、交通情報 (Traffic information)、道路料金徴収 (Road tolling)、及び道路通行最適化／誘導 (Road traffic optimisation/steering)を含む。

【０１７０】

支払いに関するMTCアプリケーションの例は、販売時点情報管理 (Point of sales (POS))、自動販売機 (Vending machines)、及び遊戯機 (Gaming machines)を含む。

【０１７１】

健康に関するMTCアプリケーションの例は、生命徴候の監視 (Monitoring vital signs)、高齢者又は障害者支援 (Supporting the aged or handicapped)、ウェブアクセス遠隔医療 (Web Access Telemedicine points)、及びリモート診断 (Remote diagnostics)を含む。

【０１７２】

リモートメンテナンス／制御に関するMTCアプリケーションの例は、センサ (Sensors)、明かり (Lighting)、ポンプ (Pumps)、バルブ (Valves)、エレベータ制御 (Elevator control)、自動販売機制御 (Vending machine control)、及び車両診断 (Vehicle diagnostics)を含む。

【０１７３】

計量に関するMTCアプリケーションの例は、パワー (Power)、ガス (Gas)
水 (Water)、暖房 (Heating)、グリッド制御 (Grid control)、及び産業用メータリング (Industrial metering)を含む。

【０１７４】

民生機器に関するMTCアプリケーションの例は、デジタルフォトフレーム、デジタルカ

メラ、及び電子ブック (ebook)を含む。
【０１７５】
アプリケーション、サービス、及びソリューションは、一例として、MVNO（Mobile Virtual Network Operator：仮想移動体通信事業者）サービス/システム、防災無線サービス/システム、構内無線電話（PBX（Private Branch eXchange：構内交換機））サービス/システム、PHS/デジタルコードレス電話サービス/システム、Point of sales（POS）システム、広告発信サービス/システム、マルチキャスト（Multimedia Broadcast and Multicast Service（MBMS））サービス/システム、V2X（Vehicle to Everything：車車間通信および路車間・歩車間通信）サービス/システム、列車内移動無線サービス/システム、位置情報関連サービス/システム、災害/緊急時無線通信サービス/システム、IoT（Internet of Things：モノのインターネット）サービス/システム、コミュニティーサービス/システム、映像配信サービス/システム、Femtoセル応用サービス/システム、VoLTE（Voice over LTE）サービス/システム、無線タグ・サービス/システム、課金サービス/システム、ラジオオンデマンドサービス/システム、ローミングサービス/システム、ユーザー行動監視サービス/システム、通信キャリア/通信NW選択サービス/システム、機能制限サービス/システム、PoC（Proof of Concept）サービス/システム、端末向け個人情報管理サービス/システム、端末向け表示・映像サービス/システム、端末向け非通信サービス/システム、アドホックNW/DTN（Delay Tolerant Networking）サービス/システムなどであってもよい。
【０１７６】
上述したUEのカテゴリは、本明細書に記載された技術思想及び実施形態の応用例に過ぎない。本明細書のUEは、これらの例に限定されるものではなく、当業者は種々の変更をこれに行うことができる。
【０１７７】
上述した実施形態は本件発明者により得られた技術思想の適用に関する例に過ぎない。すなわち、当該技術思想は上述の実施形態に限定されるものではなく、種々の変更がこれらに対して行われることができる。
【０１７８】
例えば、上記の実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。
【０１７９】
（付記Ａ１）
User Equipment（UE）であって、
少なくとも１つのメモリと、
前記少なくとも１つのメモリに結合された少なくとも１つのプロセッサと、
を備え、
前記少なくとも１つのプロセッサは、UE設定を管理するよう構成され、ここで前記UE設定は、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含み、
前記少なくとも１つのプロセッサは、第１のNon-Access Stratum（NAS）メッセージをAccess and Mobility Management Function（AMF）から受信したことに応答して、前記UEに現在許可された第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納（store）するよう構成される、
UE。
（付記Ａ２）
前記第１のNASメッセージは、前記第１のネットワークスライス識別子に関する前記UE

設定の更新を明示的に示すUE CONFIGURATION UPDATE COMMANDメッセージである、
付記Ａ１に記載のUE。
（付記Ａ３）
前記第１のNASメッセージは、前記第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の間に前記UEに送られるメッセージである、
付記Ａ１に記載のUE。
（付記Ａ４）
前記第１のNASメッセージは、前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立の要求を前記第１のネットワークスライス識別子のための再認証及び再認可手順が行われている間に前記AMFが前記UEから受信した場合に前記AMFによって送られるメッセージである、
付記Ａ１に記載のUE。
（付記Ａ５）
前記第１のNASメッセージは、前記要求の拒絶を示し、前記再認証及び再認可手順が行われていることを示すcause情報要素を包含する、
付記Ａ４に記載のUE。
（付記Ａ６）
前記UE設定は、ｃ）前記AMFにより拒絶され且つそれにより前記UEが利用できない１又はそれ以上のネットワークスライス識別子を示す拒絶されたネットワークスライス識別子のセットを含み、
前記少なくとも１つのプロセッサは、前記第１のネットワークスライス識別子が前記保留中のネットワークスライス識別子のセットから削除され、前記第１のネットワークスライス識別子が前記拒絶されたネットワークスライス識別子のセットに格納されるべきことを示す第２のNASメッセージを前記AMFから受信するよう構成され、
前記少なくとも１つのプロセッサは、前記第２のNASメッセージの受信に応答して、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記拒絶されたネットワークスライス識別子のセットに格納するよう構成される、
付記Ａ１～Ａ５のいずれか１項に記載のUE。
（付記Ａ７）
前記第１のネットワークスライス識別子は、Single Network Slice Selection Assistance Information（S-NSSAI）であり、
前記許可されたネットワークスライス識別子のセットは、前記UEに現在許可された１又はそれ以上のS-NSSAIsを示すAllowed Network Slice Selection Assistance Information（NSSAI）であり、
前記保留中のネットワークスライス識別子のセットは、前記NSSAAが保留中である１又はそれ以上のS-NSSAIsを示すPending NSSAIである、
付記Ａ１～Ａ６のいずれか１項に記載のUE。
（付記Ａ８）
User Equipment（UE）における方法であって、
UE設定を管理すること、ここで前記UE設定は、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含む；及び
第１のNon-Access Stratum（NAS）メッセージをAccess and Mobility Management Function（AMF）から受信したことに応答して、前記UEに現在許可された第１のネッ

トワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納すること、
を備える方法。
（付記Ａ９）
User Equipment（UE）における方法をコンピュータに行わせるためのプログラムであって、
前記方法は、
UE設定を管理すること、ここで前記UE設定は、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含む；
第１のNon-Access Stratum（NAS）メッセージをAccess and Mobility Management Function（AMF）から受信したことに応答して、前記UEに現在許可された第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納すること、
を備える、プログラム。
（付記Ａ１０）
少なくとも１つのメモリと、
前記少なくとも１つのメモリに結合された少なくとも１つのプロセッサと、
を備え、
前記少なくとも１つのプロセッサは、User Equipment（UE）設定の更新をUEに引き起こす第１のNon-Access Stratum（NAS）メッセージを前記UEに送信するよう構成され、
前記UE設定は、前記UEに保持され、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含み、
前記第１のNASメッセージは、前記UEに現在許可された第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納することを前記UEに引き起こす、
Access and Mobility Management Function（AMF）ノード。
（付記Ａ１１）
前記少なくとも１つのプロセッサは、前記第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の開始をトリガーする場合に、前記第１のNASメッセージを前記UEに送信するよう構成される、
付記Ａ１０に記載のAMFノード。
（付記Ａ１２）
前記少なくとも１つのプロセッサは、
前記第１のネットワークスライス識別子のための再認証及び再認可手順の開始をトリガーした後に前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立の要求を前記UEから受信した場合に、前記第１のNASメッセージを前記UEに送信するよう構成される、
付記Ａ１０に記載のAMFノード。

（付記Ａ１３）
前記第１のNASメッセージは、前記第１のネットワークスライス識別子に関する前記UE設定の更新を明示的に示すUE CONFIGURATION UPDATE COMMANDメッセージである、
付記Ａ１０～Ａ１２のいずれか１項に記載のAMFノード。
（付記Ａ１４）
前記第１のNASメッセージは、前記再認証及び再認可手順の間に前記UEに送られるメッセージである、
付記Ａ１１に記載のAMFノード。
（付記Ａ１５）
前記第１のNASメッセージは、前記要求の拒絶を示し、前記再認証及び再認可手順が行われていることを示すcause情報要素を包含する、
付記Ａ１２に記載のAMFノード。
（付記Ａ１６）
前記UE設定は、ｃ）前記AMFノードにより拒絶され故に前記UEが利用できない１又はそれ以上のネットワークスライス識別子を示す拒絶されたネットワークスライス識別子のセットを含み、
前記少なくとも１つのプロセッサは、前記再認証及び再認可手順の失敗に応答して、前記UE設定の更新を前記UEに引き起こす第２のNASメッセージを前記UEに送信するよう構成され、
前記第２のNASメッセージは、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記拒絶されたネットワークスライス識別子のセットに格納することを前記UEに引き起こす、
付記Ａ１１又はＡ１２に記載のAMFノード。
（付記Ａ１７）
前記少なくとも１つのプロセッサは、前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立手順が行われている又は中断されているなら、前記確立手順を拒絶するよう構成され、
前記第２のNASメッセージは、前記確立手順の拒絶を示し、且つ前記再認証及び再認可手順の失敗を示すcause情報要素を包含する、
付記Ａ１６に記載のAMFノード。
（付記Ａ１８）
前記少なくとも１つのプロセッサは、ａ）前記第１のネットワークスライス識別子を許可したAuthentication, Authorization and Accounting（AAA）サーバが再認証を要求した場合、又はｂ）前記AMFノードが、オペレータポリシー又は前記UEの加入者情報（subscription information）の変更に基づいて、前記第１のネットワークスライス識別子のための再認証が必要とされることを判定した場合に、前記第１のネットワークスライス識別子のための前記再認証及び再認可手順の開始をトリガーするよう構成される、
付記Ａ１１に記載のAMFノード。
（付記Ａ１９）
前記第１のネットワークスライス識別子は、Single Network Slice Selection Assistance Information（S-NSSAI）であり、
前記許可されたネットワークスライス識別子のセットは、前記UEに現在許可された１又はそれ以上のS-NSSAIsを示すAllowed Network Slice Selection Assistance Information（NSSAI）であり、
前記保留中のネットワークスライス識別子のセットは、前記NSSAAが保留中である１又はそれ以上のS-NSSAIsを示すPending NSSAIである、
付記Ａ１０～Ａ１８のいずれか１項に記載のAMFノード。
（付記Ａ２０）

User Equipment（UE）設定の更新をUEに引き起こす第１のNon-Access Stratum（NAS）メッセージを前記UEに送信することを備え、
前記UE設定は、前記UEに保持され、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含み、
前記第１のNASメッセージは、前記UEに現在許可された第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納することを前記UEに引き起こす、
Access and Mobility Management Function（AMF）ノードにおける方法。
（付記Ａ２１）
Access and Mobility Management Function（AMF）ノードにおける方法をコンピュータに行わせるためのプログラムであって、
前記方法は、 User Equipment（UE）設定の更新をUEに引き起こす第１のNon-Access Stratum（NAS）メッセージを前記UEに送信することを備え、
前記UE設定は、前記UEに保持され、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含み、
前記第１のNASメッセージは、前記UEに現在許可された第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納することを前記UEに引き起こす、
プログラム。
【０１８０】
（付記Ｂ１）
少なくとも１つのメモリと、
前記少なくとも１つのメモリに結合された少なくとも１つのプロセッサと、
を備え、
前記少なくとも１つのプロセッサは、
User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の開始をトリガーするよう構成され、
前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立の要求を前記UEから前記再認証及び再認可手順の開始をトリガーした後に受信したなら、少なくとも前記再認証及び再認可の結果が得られるまで前記要求によりトリガーされたセッション確立手順を中断するよう構成される、
Access and Mobility Management Function（AMF）ノード。
（付記Ｂ２）
前記少なくとも１つのプロセッサは、前記要求の受信に応答して、UE設定の更新を前記UEに引き起こすNon-Access Stratum（NAS）メッセージを前記UEに送信するよう構成され、
前記UE設定は、前記UEに保持され、ａ）前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセット、及びｂ）ネットワークスライスに特化した認証及び認可（Network Slice-Specific Authenti

cation and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットを含み、
前記NASメッセージは、前記第１のネットワークスライス識別子を前記許可されたネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットに格納することを前記UEに引き起こす、
付記Ｂ１に記載のAMFノード。
（付記Ｂ３）
前記少なくとも１つのプロセッサは、前記再認証及び再認可手順の失敗に応答して、前記要求の拒絶を示す拒絶メッセージを前記UEに送信するよう構成される、
付記Ｂ２に記載のAMFノード。
（付記Ｂ４）
前記少なくとも１つのプロセッサは、前記再認証及び再認可手順の失敗を示すcause情報要素を、前記拒絶メッセージと共に前記UEに送信する、
付記Ｂ３に記載のAMFノード。
（付記Ｂ５）
前記UE設定は、ｃ）前記AMFノードにより拒絶され故に前記UEが利用できない１又はそれ以上のネットワークスライス識別子を示す拒絶されたネットワークスライス識別子のセットを含み、
前記拒絶メッセージは、前記第１のネットワークスライス識別子を前記保留中のネットワークスライス識別子のセットから削除し、前記第１のネットワークスライス識別子を前記拒絶されたネットワークスライス識別子のセットに格納することを前記UEに引き起こす、
付記Ｂ３又はＢ４に記載のAMFノード。
（付記Ｂ６）
User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の開始をトリガーすること、及び
前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立の要求を前記UEから前記再認証及び再認可手順の開始をトリガーした後に受信したなら、少なくとも前記再認証及び再認可の結果が得られるまで前記要求によりトリガーされたセッション確立手順を中断すること、
を備えるAccess and Mobility Management Function（AMF）ノードにおける方法。
（付記Ｂ７）
Access and Mobility Management Function（AMF）ノードにおける方法をコンピュータに行わせるためのプログラムであって、
前記方法は、
User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の開始をトリガーすること、及び
前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立の要求を前記UEから前記再認証及び再認可手順の開始をトリガーした後に受信したなら、少なくとも前記再認証及び再認可の結果が得られるまで前記要求によりトリガーされたセッション確立手順を中断すること、
を備える、プログラム。
（付記Ｂ８）
少なくとも１つのメモリと、
前記少なくとも１つのメモリに結合された少なくとも１つのプロセッサと、
を備え、

前記少なくとも１つのプロセッサは、
User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の開始をトリガーするよう構成され、
前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立の要求を前記UEから前記再認証及び再認可手順の開始をトリガーした後に受信したなら、前記要求を拒絶するよう構成される、
Access and Mobility Management Function（AMF）ノード。
（付記Ｂ９）
前記少なくとも１つのプロセッサは、前記要求の拒絶を示すNon-Access Stratum（NAS）メッセージを前記UEに送信するよう構成され、
前記NASメッセージは、前記再認証及び再認可手順が行われていることを示すcause情報要素を包含する、
付記Ｂ８に記載のAMFノード。
（付記Ｂ１０）
前記NASメッセージは、前記UEに現在許可された１又はそれ以上のネットワークスライス識別子を示す許可されたネットワークスライス識別子のセットから前記第１のネットワークスライス識別子が削除され、且つネットワークスライスに特化した認証及び認可（Network Slice-Specific Authentication and Authorization（NSSAA））手順が保留中（pending）である１又はそれ以上のネットワークスライス識別子を示す保留中のネットワークスライス識別子のセットに前記第１のネットワークスライス識別子が格納されるようにUE設定を更新することを前記UEに引き起こす、
付記Ｂ９に記載のAMFノード。
（付記Ｂ１１）
User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の開始をトリガーすること、及び
前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立の要求を前記UEから前記再認証及び再認可手順の開始をトリガーした後に受信したなら、前記要求を拒絶すること、
を備えるAccess and Mobility Management Function（AMF）ノードにおける方法。
（付記Ｂ１２）
Access and Mobility Management Function（AMF）ノードにおける方法をコンピュータに行わせるためのプログラムであって、
前記方法は、
User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の開始をトリガーすること、及び
前記第１のネットワークスライス識別子に関連付けられた新たなセッションの確立の要求を前記UEから前記再認証及び再認可手順の開始をトリガーした後に受信したなら、前記要求を拒絶すること、
を備える、プログラム。
【０１８１】
（付記Ｃ１）
少なくとも１つのメモリと、
前記少なくとも１つのメモリに結合された少なくとも１つのプロセッサと、
を備え、
前記少なくとも１つのプロセッサは、User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の失敗に応答して、前記第１のネットワークスライス識別子に関連付

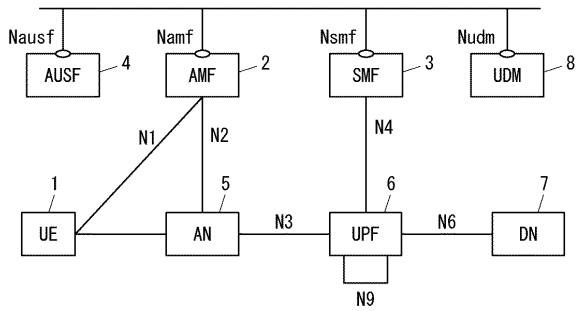
けられたProtocol Data Unit（PDU）セッションを解放するための解放手順を開始するよう構成される、
Access and Mobility Management Function（AMF）ノード。
（付記Ｃ２）
前記少なくとも１つのプロセッサは、前記解放手順において、前記UEのための前記第１のネットワークスライス識別子のための前記再認証及び再認可の失敗をSession Management Function（SMF）に通知するよう構成される、
付記Ｃ１に記載のAMFノード。
（付記Ｃ３）
前記少なくとも１つのプロセッサは、前記解放手順において、前記PDUセッションのためのSession Management（SM）コンテキストの解放を要求するためのメッセージを前記SMFに送信するよう構成され、
前記メッセージは、前記再認証及び再認可の失敗を示すcause情報要素を包含する、
付記Ｃ２に記載のAMFノード。
（付記Ｃ４）
前記少なくとも１つのプロセッサは、前記再認証及び再認可の前記失敗に応答して、UE設定の更新を指示するNon-Access Stratum（NAS）メッセージを前記UEに送信するよう構成され、
前記NASメッセージは、拒絶されたネットワークスライス識別子のセットに前記第１のネットワークスライス識別子が含まれることを示し、
前記NASメッセージは、さらに、前記PDUセッションが解放されるまでの猶予期間を示す、
付記Ｃ１～Ｃ３のいずれか１項に記載のAMFノード。
（付記Ｃ５）
前記少なくとも１つのプロセッサは、前記猶予期間の経過後に前記解放手順を開始するよう構成される、
付記Ｃ４に記載のAMFノード。
（付記Ｃ６）
前記少なくとも１つのプロセッサは、前記再認証及び再認可の失敗を示すメッセージをAuthentication Server Function（AUSF）から受信したことに応答して、前記解放手順を開始するよう構成される、
付記Ｃ１～Ｃ５のいずれか１項に記載のAMFノード。
（付記Ｃ７）
前記第１のネットワークスライス識別子は、Single Network Slice Selection Assistance Information（S-NSSAI）である、
付記Ｃ１～Ｃ６のいずれか１項に記載のAMFノード。
（付記Ｃ８）
User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の失敗に応答して、前記第１のネットワークスライス識別子に関連付けられたProtocol Data Unit（PDU）セッションを解放するための解放手順を開始することを備える、
Access and Mobility Management Function（AMF）ノードにおける方法。
（付記Ｃ９）
Access and Mobility Management Function（AMF）ノードにおける方法をコンピュータに行わせるためのプログラムであって、
前記方法は、User Equipment（UE）に現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の失敗に応答して、前記第１のネットワークスライス識別子に関連付けられたProtocol Data Unit（PDU）セッションを解放するための解放手順を開始することを備える、
プログラム。

（付記Ｃ１０）
User Equipment（UE）であって、
少なくとも１つのメモリと、
前記少なくとも１つのメモリに結合された少なくとも１つのプロセッサと、
を備え、
前記少なくとも１つのプロセッサは、前記UEに現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の失敗に応答して、前記第１のネットワークスライス識別子に関連付けられたProtocol Data Unit（PDU）セッションの解放をネットワークに要求するよう構成される、
UE。
（付記Ｃ１１）
前記少なくとも１つのプロセッサは、前記PDUセッションの解放を要求するための第１のNon-Access Stratum（NAS）メッセージをAccess and Mobility Management Function（AMF）に送信するよう構成され、
前記第１のNASメッセージは、前記再認証及び再認可の失敗を示すcause情報要素を包含する、
付記Ｃ１０に記載のUE。
（付記Ｃ１２）
前記少なくとも１つのプロセッサは、UE設定の更新を指示する第２のNon-Access Stratum（NAS）メッセージをAccess and Mobility Management Function（AMF）から受信するよう構成され、
前記第２のNASメッセージは、拒絶されたネットワークスライス識別子のセットに前記第１のネットワークスライス識別子が含まれることを示し、
前記少なくとも１つのプロセッサは、前記第２のNASメッセージの受信に応答して、前記PDUセッションの解放を前記ネットワークに要求するよう構成される、
付記Ｃ１０又はＣ１１に記載のUE。
（付記Ｃ１３）
前記少なくとも１つのプロセッサは、前記再認証及び再認可の失敗を示す第３のNon-Access Stratum（NAS）メッセージをAccess and Mobility Management Function（AMF）から受信するよう構成され、
前記少なくとも１つのプロセッサは、前記第３のNASメッセージの受信に応答して、前記PDUセッションの解放を前記ネットワークに要求するよう構成される、
付記Ｃ１０又はＣ１１に記載のUE。
（付記Ｃ１４）
User Equipment（UE）における方法であって、
前記UEに現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の失敗に応答して、前記第１のネットワークスライス識別子に関連付けられたProtocol Data Unit（PDU）セッションの解放をネットワークに要求することを備える、
方法。
（付記Ｃ１５）
User Equipment（UE）における方法をコンピュータに行わせるためのプログラムであって、
前記方法は、前記UEに現在許可された第１のネットワークスライス識別子のための再認証及び再認可（re-authentication and re-authorization）手順の失敗に応答して、前記第１のネットワークスライス識別子に関連付けられたProtocol Data Unit（PDU）セッションの解放をネットワークに要求することを備える、
プログラム。
【０１８２】
この出願は、２０１９年１２月２６日に出願された日本出願特願２０１９－２３７３９

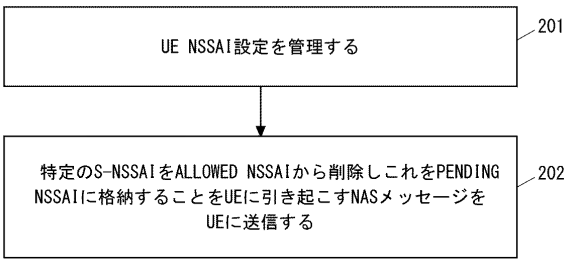
１を基礎とする優先権を主張し、その開示の全てをここに取り込む。
【符号の説明】
【０１８３】
１　ＵＥ
２　ＡＭＦ
３　ＳＭＦ
４　ＡＵＳＦ
５　ＡＮ
６　ＵＰＦ
７　ＤＮ
８　ＵＤＭ
９　ＡＡＡ-Ｓ
１９０３　ベースバンドプロセッサ
１９０４　アプリケーションプロセッサ
１９０６　メモリ
１９０７　モジュール（ｍｏｄｕｌｅｓ）
２００２　プロセッサ
２００３　メモリ
２００４　モジュール（ｍｏｄｕｌｅｓ）

【図面】

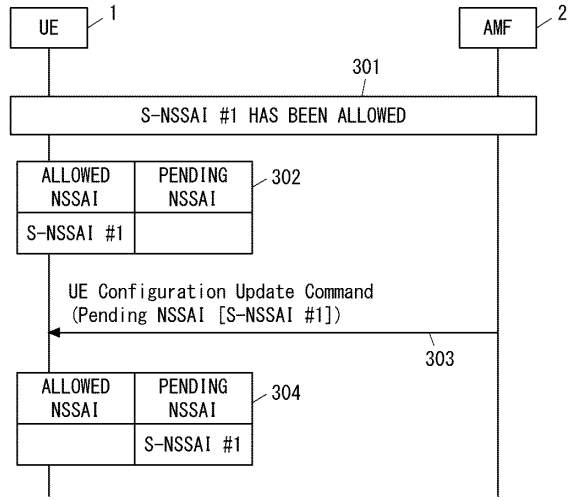
【図１】


Nausf
Namf
Nsmf
Nudm
AUSF
AMF
SMF
UDM
4
2
3
8
N1
N2
N4
1
5
6
7
UE
AN
N3
UPF
N6
DN
N9

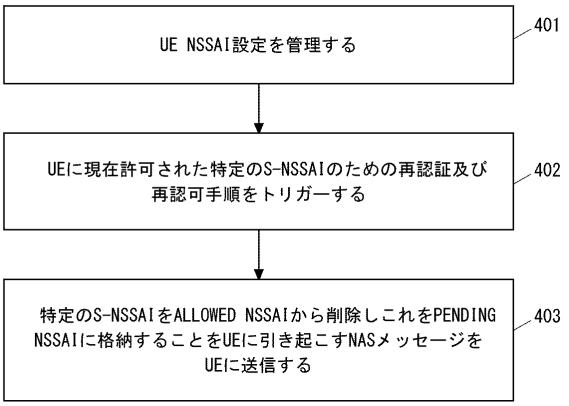
【図２】


UE NSSAI設定を管理する
201
特定のS-NSSAIをALLOWED NSSAIから削除しこれをPENDING NSSAIに格納することをUEに引き起こすNASメッセージをUEに送信する
202

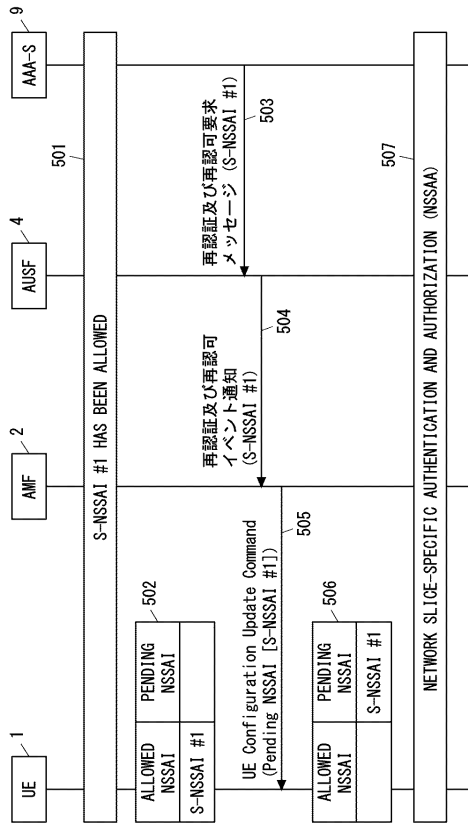
【図３】


UE
1
AMF
2
301
S-NSSAI #1 HAS BEEN ALLOWED
ALLOWED NSSAI
PENDING NSSAI
302
S-NSSAI #1
UE Configuration Update Command
(Pending NSSAI [S-NSSAI #1])
303
ALLOWED NSSAI
PENDING NSSAI
304
S-NSSAI #1

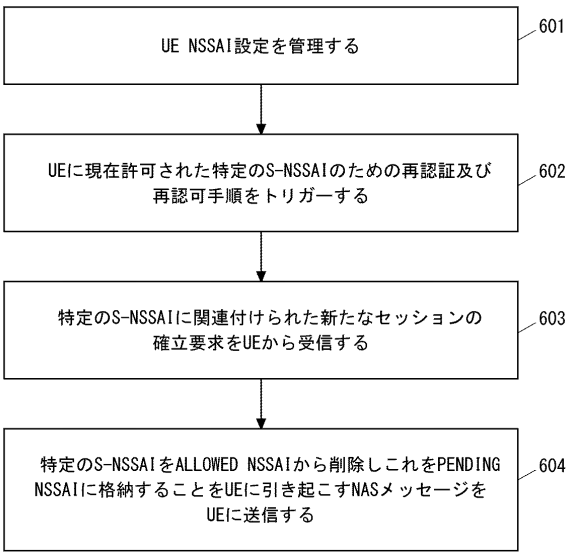
【図４】


UE NSSAI設定を管理する
401
UEに現在許可された特定のS-NSSAIのための再認証及び再認可手順をトリガーする
402
特定のS-NSSAIをALLOWED NSSAIから削除しこれをPENDING NSSAIに格納することをUEに引き起こすNASメッセージをUEに送信する
403

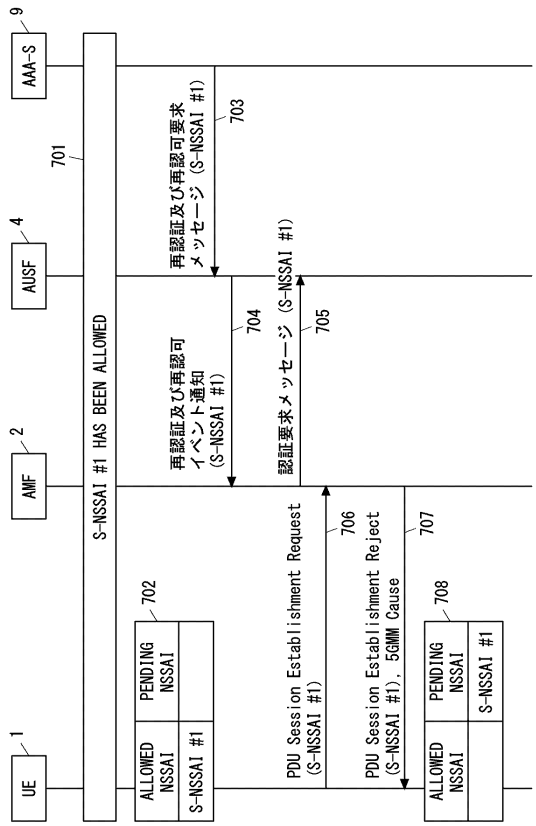
【図５】


AAA-S
9
AUSF
4
AMF
2
UE
1
S-NSSAI #1 HAS BEEN ALLOWED
501
再認証及び再認可要求
メッセージ (S-NSSAI #1)
503
再認証及び再認可
イベント通知
(S-NSSAI #1)
504
UE Configuration Update Command
(Pending NSSAI [S-NSSAI #1])
505
NETWORK SLICE-SPECIFIC AUTHENTICATION AND AUTHORIZATION (NSSAA)
507
502
PENDING NSSAI
ALLOWED NSSAI
S-NSSAI #1
506
PENDING NSSAI
S-NSSAI #1
ALLOWED NSSAI

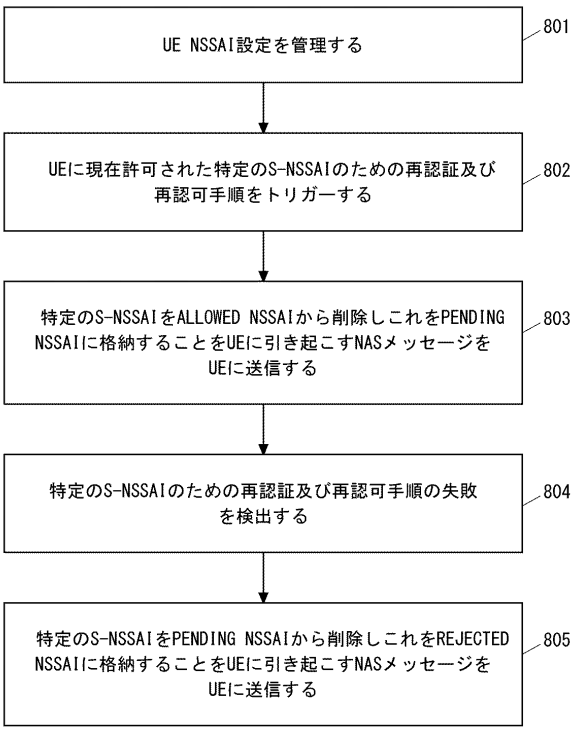
【図６】


UE NSSAI設定を管理する
601
UEに現在許可された特定のS-NSSAIのための再認証及び
再認可手順をトリガーする
602
特定のS-NSSAIに関連付けられた新たなセッションの
確立要求をUEから受信する
603
特定のS-NSSAIをALLOWED NSSAIから削除しこれをPENDING
NSSAIに格納することをUEに引き起こすNASメッセージを
UEに送信する
604

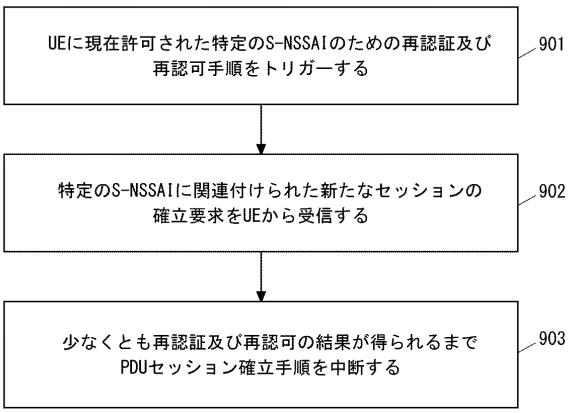
【図７】


AAA-S
9
AUSF
4
AMF
2
UE
1
S-NSSAI #1 HAS BEEN ALLOWED
701
再認証及び再認可要求
メッセージ (S-NSSAI #1)
703
再認証及び再認可
イベント通知
(S-NSSAI #1)
704
認証要求メッセージ (S-NSSAI #1)
705
PDU Session Establishment Request
(S-NSSAI #1)
706
PDU Session Establishment Reject
(S-NSSAI #1), 5GMM Cause
707
702
PENDING NSSAI
ALLOWED NSSAI
S-NSSAI #1
708
PENDING NSSAI
S-NSSAI #1
ALLOWED NSSAI

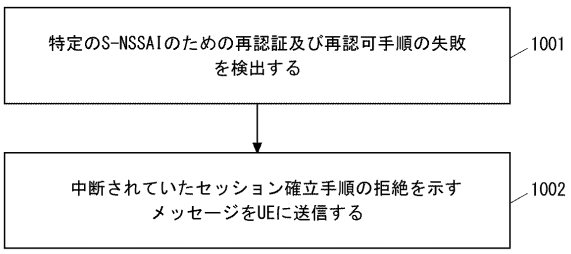
【図８】


UE NSSAI設定を管理する
801
UEに現在許可された特定のS-NSSAIのための再認証及び
再認可手順をトリガーする
802
特定のS-NSSAIをALLOWED NSSAIから削除しこれをPENDING
NSSAIに格納することをUEに引き起こすNASメッセージを
UEに送信する
803
特定のS-NSSAIのための再認証及び再認可手順の失敗
を検出する
804
特定のS-NSSAIをPENDING NSSAIから削除しこれをREJECTED
NSSAIに格納することをUEに引き起こすNASメッセージを
UEに送信する
805

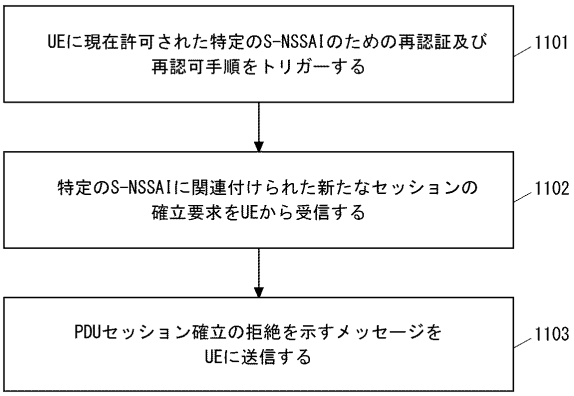
【図９】



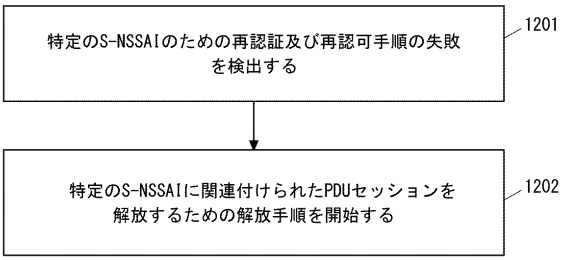

【図１０】



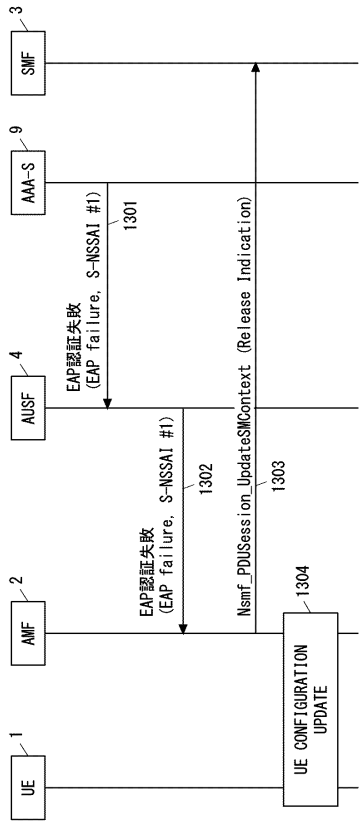

【図１１】



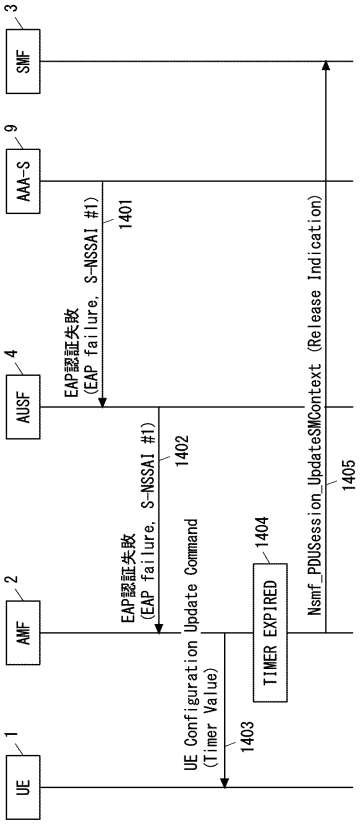

【図１２】



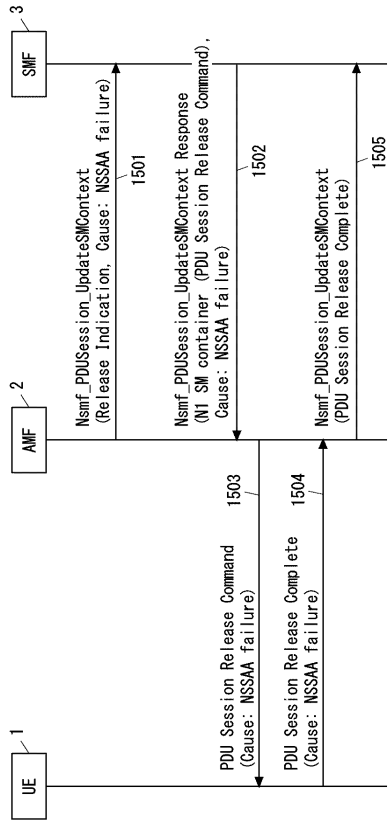
【図１３】



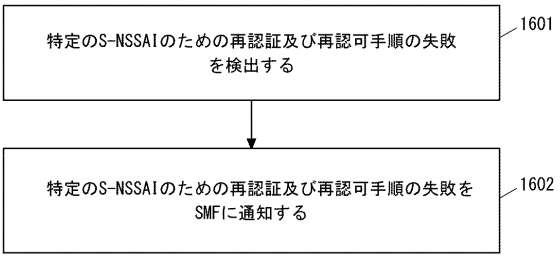

【図１４】



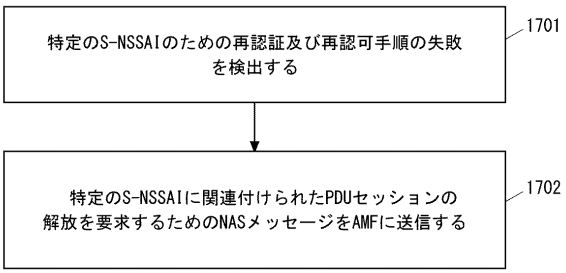

【図１５】



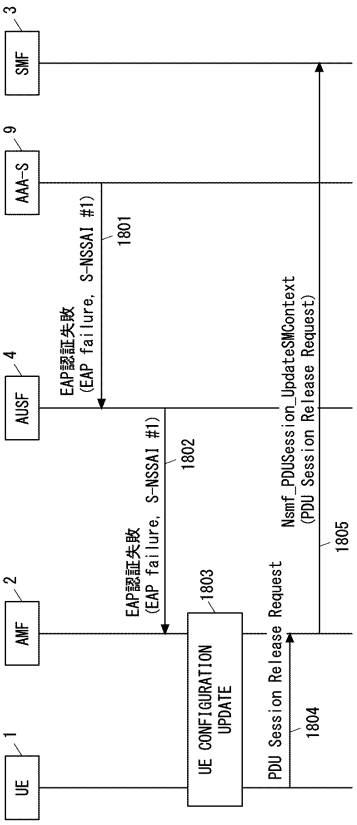

【図１６】



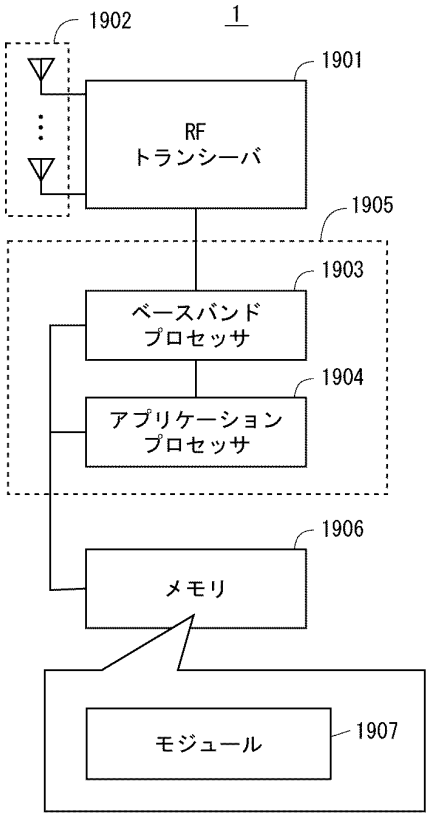
【図１７】



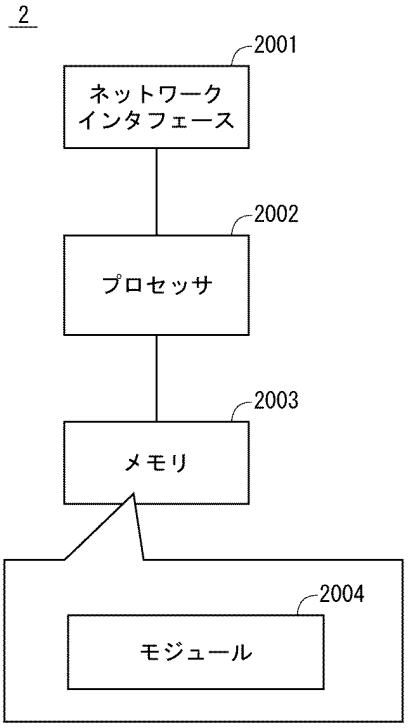

【図１８】




【図１９】




【図２０】



フロントページの続き

(56)参考文献 3GPP TS 24.501 V16.3.0 (2019-12)，フランス，2019年12月20日，第77ページ, 第174ページ-第181ページ，[検索日 2024.03.26]
Nokia, Nokia Shanghai Bell, Ericsson, Huawei, HiSilicon, InterDigital，Draft for network slice specific authentication procedures'[online]，3GPP TSG SA WG3 #97 S3-194541，フランス， Internet〈URL:https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_97_Reno/Docs/S3-194541.zip〉，2019年11月22日，[検索日 2024.03.26]
Motorola Mobility, Lenovo，KI#3: Update to Solution 3.3 on (re-)authentication after failure/revocation[online]，3GPP TSG SA WG2 #129BIS S2-1812403，フランス，Internet〈URL:https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_129BIS_West_Palm_Beach/Docs/S2-1812403.zip〉 ，2018年11月20日，[検索日 2024.03.26]
NEC，Preventing UE waiting for completion of NSSAA indefinitely - Atl1 NW timer[online]，3GPP TSG CT WG1 #121 C1-198368，フランス，Internet〈URL:https://www.3gpp.org/ftp/tsg_ct/WG1_mm-cc-sm_ex-CN1/TSGC1_121_Reno/Docs/C1-198368.zip〉，2019年11月04日，[検索日 2024.03.26]

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｗ４／００－Ｈ０４Ｗ９９／００
Ｈ０４Ｂ７／２４－Ｈ０４Ｂ７／２６
３ＧＰＰ ＴＳＧ ＲＡＮ ＷＧ１－４
ＳＡ ＷＧ１－４
ＣＴ ＷＧ１、４