

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号  
特許第7613818号  
(P7613818)

(45)発行日 令和7年1月15日(2025.1.15)

(24)登録日 令和7年1月6日(2025.1.6)

(51)国際特許分類 F I  
H 0 4 W 12/062 (2021.01) H 0 4 W 12/062  
H 0 4 W 12/75 (2021.01) H 0 4 W 12/75

請求項の数 6 (全30頁)

|             |                             |          |                                                             |
|-------------|-----------------------------|----------|-------------------------------------------------------------|
| (21)出願番号    | 特願2023-506691(P2023-506691) | (73)特許権者 | 392026693<br>株式会社NTTドコモ<br>東京都千代田区永田町二丁目1番1号                |
| (86)(22)出願日 | 令和3年3月19日(2021.3.19)        | (74)代理人  | 100107766<br>弁理士 伊東 忠重                                      |
| (86)国際出願番号  | PCT/JP2021/011495           | (74)代理人  | 100070150<br>弁理士 伊東 忠彦                                      |
| (87)国際公開番号  | WO2022/195878               | (74)代理人  | 100124844<br>弁理士 石原 隆治                                      |
| (87)国際公開日   | 令和4年9月22日(2022.9.22)        | (72)発明者  | 鈴木 悠司<br>東京都千代田区永田町2丁目1番1号<br>山王パークタワー 株式会社NTTドコモ<br>知的財産部内 |
| 審査請求日       | 令和6年1月29日(2024.1.29)        | (72)発明者  | 巳之口 淳<br>東京都千代田区永田町2丁目1番1号<br>最終頁に続く                        |

(54)【発明の名称】 ネットワークノード及び通信方法

(57)【特許請求の範囲】

【請求項1】

端末を認証し暫定識別子を当該端末に送信する送信部と、  
前記暫定識別子を含む要求又は前記暫定識別子に基づく認証コードを受信する受信部と、  
前記暫定識別子を含む要求又は前記認証コードに基づいて、アクセストークンを発行する制御部とを有し、

前記送信部は、前記アクセストークンを前記端末又は外部アプリケーションに送信し、  
前記受信部は、前記アクセストークンに基づくAPI(Application Programming Interface)呼び出し要求を前記端末又は前記外部アプリケーションから受信し、

前記制御部は、前記アクセストークンを検証して前記API呼び出し要求が認可されたものであると判定した場合、前記API呼び出し要求に基づいて処理を実行するネットワークノード。

10

【請求項2】

前記受信部は、前記端末又は前記外部アプリケーションからAPI呼び出しに使用するセキュリティメソッドに係る要求を受信し、

前記制御部は、セキュリティメソッドを選択し、  
前記送信部は、前記選択したセキュリティメソッドを示す応答を前記端末又は外部アプリケーションに送信する請求項1記載のネットワークノード。

【請求項3】

前記送信部が前記アクセストークンを前記外部アプリケーションに送信する場合、前記

20

制御部は、前記外部アプリケーションを予め認証し登録している請求項 1 記載のネットワークノード。

【請求項 4】

前記送信部が前記アクセストークンを前記外部アプリケーションに送信する場合、前記制御部は、ユーザに A P I 利用可否の確認を実施した後、前記アクセストークンを発行する請求項 3 記載のネットワークノード。

【請求項 5】

前記制御部は、前記 A P I 呼び出し要求が認可されたものであるかを判定するとき、少なくともユーザごとのスコープが設定される、許可される A P I 及び許可されるメソッドを参照する請求項 1 記載のネットワークノード。

10

【請求項 6】

端末を認証し暫定識別子を当該端末に送信する送信手順と、  
前記暫定識別子を含む要求又は前記暫定識別子に基づく認証コードを受信する受信手順と、

前記暫定識別子を含む要求又は前記認証コードに基づいて、アクセストークンを発行する制御手順と、

前記アクセストークンを前記端末又は外部アプリケーションに送信する手順と、

前記アクセストークンに基づく A P I (Application Programming Interface) 呼び出し要求を前記端末又は前記外部アプリケーションから受信する手順と、

前記アクセストークンを検証して前記 A P I 呼び出し要求が認可されたものであると判定した場合、前記 A P I 呼び出し要求に基づいて処理を実行する手順とをネットワークノードが実行する通信方法。

20

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、通信システムにおけるネットワークノード及び通信方法に関する。

【背景技術】

【0002】

3 G P P (3rd Generation Partnership Project) では、システム容量の更なる大容量化、データ伝送速度の更なる高速化、無線区間における更なる低遅延化等を実現するために、5 G あるいは N R (New Radio) と呼ばれる無線通信方式 (以下、当該無線通信方式を「5 G」あるいは「N R」という。) の検討が進んでいる。5 G では、10 G b p s 以上のスループットを実現しつつ無線区間の遅延を 1 m s 以下にするという要求条件を満たすために、様々な無線技術の検討が行われている。

30

【0003】

N R では、L T E (Long Term Evolution) のネットワークアーキテクチャにおけるコアネットワークである E P C (Evolved Packet Core) に対応する 5 G C (5G Core Network) 及び L T E のネットワークアーキテクチャにおける R A N (Radio Access Network) である E - U T R A N (Evolved Universal Terrestrial Radio Access Network) に対応する N G - R A N (Next Generation - Radio Access Network) を含むネットワークアーキテクチャが検討されている (例えば非特許文献 1)。

40

【0004】

また、例えば、5 G システムにおける N E F (Network Exposure Function) と A F (Application Function) 間の N o r t h b o u n d インタフェースを C A P I F (Common API Framework) により構成するアーキテクチャが検討されている (例えば非特許文献 2 及び非特許文献 3)。

【先行技術文献】

【非特許文献】

【0005】

【文献】 3 G P P T S 23.501 V16.7.0 (2020-12)

50

【文献】3GPP TS 29.522 V16.6.0 (2020-12)

【文献】3GPP TS 23.222 V16.9.0 (2020-09)

【発明の概要】

【発明が解決しようとする課題】

【0006】

3GPPコアネットワークでは外部のアプリケーション向けにAPI (Application Programming Interface) を解放しており、サードパーティのアプリケーションからAPIを呼び出すことができる。ここで、サードパーティのアプリケーションからAPIを呼び出すとき、コアネットワークは、サードパーティのアプリケーションを利用するユーザを識別することが困難であるため、適切なサービスを提供することができなかった。

10

【0007】

本発明は上記の点に鑑みてなされたものであり、ネットワークにおいて加入者情報を識別可能とするインタフェースを提供することを目的とする。

【課題を解決するための手段】

【0008】

開示の技術によれば、端末を認証し暫定識別子を当該端末に送信する送信部と、前記暫定識別子を含む要求又は前記暫定識別子に基づく認証コードを受信する受信部と、前記暫定識別子を含む要求又は前記認証コードに基づいて、アクセストークンを発行する制御部とを有し、前記送信部は、前記アクセストークンを前記端末又は外部アプリケーションに送信し、前記受信部は、前記アクセストークンに基づくAPI (Application Programming Interface) 呼び出し要求を前記端末又は前記外部アプリケーションから受信し、前記制御部は、前記アクセストークンを検証して前記API呼び出し要求が認可されたものであると判定した場合、前記API呼び出し要求に基づいて処理を実行するネットワークノードが提供される。

20

【発明の効果】

【0009】

開示の技術によれば、ネットワークにおいて加入者情報を識別可能とするインタフェースを提供することができる。

【図面の簡単な説明】

【0010】

【図1】通信システムの例を説明するための図である。

【図2】ローミング環境下の通信システムの例を説明するための図である。

【図3】API呼び出しの例(1)を示す図である。

【図4】API呼び出しの例(2-1)を示す図である。

【図5】API呼び出しの例(2-2)を示す図である。

【図6】API呼び出しの例(3-1)を示す図である。

【図7】API呼び出しの例(3-2)を示す図である。

【図8】API呼び出しの例(4)を示す図である。

【図9】本発明の実施の形態におけるUEによるAPI呼び出しの例(1)を説明するための図である。

40

【図10】本発明の実施の形態におけるUEによるAPI呼び出しの例(2)を説明するための図である。

【図11】本発明の実施の形態におけるUEによるAPI呼び出しの例(3)を説明するための図である。

【図12】本発明の実施の形態におけるUE及びAFによるAPI呼び出しの例(1)を説明するための図である。

【図13】本発明の実施の形態におけるUE及びAFによるAPI呼び出しの例(2)を説明するための図である。

【図14】本発明の実施の形態におけるUE及びAFによるAPI呼び出しの例(3)を説明するための図である。

50

【図 15】本発明の実施の形態における UE 及び AF による API 呼び出しの例 (4) を説明するための図である。

【図 16】本発明の実施の形態における UE 及び AF による API 呼び出しの例 (5) を説明するための図である。

【図 17】本発明の実施の形態における API のスコープを説明するための図である。

【図 18】本発明の実施の形態における UE 及び AF を含むシステムの例を示す図である。

【図 19】本発明の実施の形態における UE を含むシステムの例を示す図である。

【図 20】本発明の実施の形態における UE による API 呼び出しの例を説明するためのシーケンス図である。

【図 21】本発明の実施の形態における UE 及び AF による API 呼び出しの例を説明するためのシーケンス (1) 図である。

10

【図 22】本発明の実施の形態における UE 及び AF による API 呼び出しの例を説明するためのシーケンス (2) 図である。

【図 23】本発明の実施の形態における基地局 10 の機能構成の一例を示す図である。

【図 24】本発明の実施の形態における端末 20 の機能構成の一例を示す図である。

【図 25】本発明の実施の形態における基地局 10 及び端末 20 のハードウェア構成の一例を示す図である。

【発明を実施するための形態】

【0011】

以下、図面を参照して本発明の実施の形態を説明する。なお、以下で説明する実施の形態は一例であり、本発明が適用される実施の形態は、以下の実施の形態に限られない。

20

【0012】

本発明の実施の形態の無線通信システムの動作にあたっては、適宜、既存技術が使用される。ただし、当該既存技術は、例えば既存の LTE であるが、既存の LTE に限られない。また、本明細書で使用する用語「LTE」は、特に断らない限り、LTE-Advanced、及び、LTE-Advanced 以降の方式 (例: NR)、又は無線 LAN (Local Area Network) を含む広い意味を有するものとする。

【0013】

また、本発明の実施の形態において、無線パラメータ等が「設定される (Configure)」とは、所定の値が予め設定 (Pre-configure) されることであってもよいし、ネットワークノード 30 又は端末 20 から通知される無線パラメータが設定されることであってもよい。

30

【0014】

図 1 は、通信システムの例を説明するための図である。図 1 に示されるように、通信システムは、端末 20 である UE、複数のネットワークノード 30 から構成される。以下、機能ごとに 1 つのネットワークノード 30 が対応するものとするが、複数の機能を 1 つのネットワークノード 30 が実現してもよいし、複数のネットワークノード 30 が 1 つの機能を実現してもよい。また、以下に記載する「接続」は、論理的な接続であってもよいし、物理的な接続であってもよい。

【0015】

40

RAN (Radio Access Network) は、無線アクセス機能を有するネットワークノード 30 であり、基地局 10 を含んでもよく、UE、AMF (Access and Mobility Management Function) 及び UPF (User plane function) と接続される。AMF は、RAN インタフェースの終端、NAS (Non-Access Stratum) の終端、登録管理、接続管理、到達性管理、モビリティ管理等の機能を有するネットワークノード 30 である。UPF は、DN (Data Network) と相互接続する外部に対する PDU (Protocol Data Unit) セッションポイント、パケットのルーティング及びフォワーディング、ユーザプレーンの QoS (Quality of Service) ハンドリング等の機能を有するネットワークノード 30 である。UPF 及び DN は、ネットワークスライスを構成する。本発明の実施の形態における無線通信ネットワークでは、複数のネットワークスライスが構築されている。

50

## 【 0 0 1 6 】

AMFは、UE、RAN、SMF (Session Management function)、NSSF (Network Slice Selection Function)、NEF (Network Exposure Function)、NRF (Network Repository Function)、UDM (Unified Data Management)、AUSF (Authentication Server Function)、PCF (Policy Control Function)、AF (Application Function)と接続される。AMF、SMF、NSSF、NEF、NRF、UDM、AUSF、PCF、AFは、各々のサービスに基づくインタフェース、Namf、Nsmf、Nnsf、Nnef、Nnrf、Nudm、Nausf、Npcf、Nafを介して相互に接続されるネットワークノード30である。

## 【 0 0 1 7 】

SMFは、セッション管理、UEのIP (Internet Protocol) アドレス割り当て及び管理、DHCP (Dynamic Host Configuration Protocol) 機能、ARP (Address Resolution Protocol) プロキシ、ローミング機能等の機能を有するネットワークノード30である。NEFは、他のNF (Network Function) に能力及びイベントを通知する機能を有するネットワークノード30である。NSSFは、UEが接続するネットワークスライスの選択、許可されるNSSAI (Network Slice Selection Assistance Information) の決定、設定されるNSSAIの決定、UEが接続するAMFセットの決定等の機能を有するネットワークノード30である。PCFは、ネットワークのポリシー制御を行う機能を有するネットワークノード30である。AFは、アプリケーションサーバを制御する機能を有するネットワークノード30である。NRFは、サービスを提供するNFインスタンスを発見する機能を有するネットワークノード30である。UDMは、加入者データ及び認証データを管理するネットワークノード30である。UDMは、当該データを保持するUDR (User Data Repository) と接続される。

## 【 0 0 1 8 】

図2は、ローミング環境下の通信システムの例を説明するための図である。図2に示されるように、ネットワークは、端末20であるUE、複数のネットワークノード30から構成される。以下、機能ごとに1つのネットワークノード30が対応するものとするが、複数の機能を1つのネットワークノード30が実現してもよいし、複数のネットワークノード30が1つの機能を実現してもよい。また、以下に記載する「接続」は、論理的な接続であってもよいし、物理的な接続であってもよい。

## 【 0 0 1 9 】

RANは、無線アクセス機能を有するネットワークノード30であり、UE、AMF及びUPFと接続される。AMFは、RANインタフェースの終端、NASの終端、登録管理、接続管理、到達性管理、モビリティ管理等の機能を有するネットワークノード30である。UPFは、DNと相互接続する外部に対するPDUセッションポイント、パケットのルーティング及びフォワーディング、ユーザプレーンのQoSハンドリング等の機能を有するネットワークノード30である。UPF及びDNは、ネットワークスライスを構成する。、本発明の実施の形態における無線通信ネットワークでは、複数のネットワークスライスが構築されている。

## 【 0 0 2 0 】

AMFは、UE、RAN、SMF、NSSF、NEF、NRF、UDM、AUSF、PCF、AF、SEPP (Security Edge Protection Proxy) と接続される。AMF、SMF、NSSF、NEF、NRF、UDM、AUSF、PCF、AFは、各々のサービスに基づくインタフェース、Namf、Nsmf、Nnsf、Nnef、Nnrf、Nudm、Nausf、Npcf、Nafを介して相互に接続されるネットワークノード30である。

## 【 0 0 2 1 】

SMFは、セッション管理、UEのIPアドレス割り当て及び管理、DHCP機能、ARPプロキシ、ローミング機能等の機能を有するネットワークノード30である。NEFは、他のNFに能力及びイベントを通知する機能を有するネットワークノード30である

10

20

30

40

50

。NSSFは、UEが接続するネットワークスライスの選択、許可されるNSSAIの決定、設定されるNSSAIの決定、UEが接続するAMFセットの決定等の機能を有するネットワークノード30である。PCFは、ネットワークのポリシー制御を行う機能を有するネットワークノード30である。AFは、アプリケーションサーバを制御する機能を有するネットワークノード30である。NRFは、サービスを提供するNFインスタンスを発見する機能を有するネットワークノード30である。SEPPは、非透過的なプロキシであり、PLMN (Public Land Mobile Network) 間のコントロールプレーンのメッセージをフィルタリングする。図2に示されるvSEPPは、visitedネットワークにおけるSEPPであり、hSEPPは、homeネットワークにおけるSEPPである。

10

#### 【0022】

図2に示されるように、UEは、VPLMN (Visited PLMN) においてRAN及びAMFと接続されているローミング環境にある。VPLMN及びHPLMN (Home PLMN) は、vSEPP及びhSEPPを経由して接続されている。UEは、例えば、VPLMNのAMFを介してHPLMNのUDMと通信が可能である。

#### 【0023】

上述のNEFは、AFから呼び出し可能であるAPI (Application Programming Interface) を、CAPIF (Common API Framework) アーキテクチャを適用して実装することが検討されている。CAPIFアーキテクチャは、サービスAPI運用をサポートするメカニズムを提供し、例えば、API呼び出し元 (invoker) にAPI提供者 (provider) から提供されるサービスAPIを発見させ、当該サービスAPIを使用する通信を可能とする。また、CAPIFアーキテクチャは、例えば、PLMNトラストドメインの外部からサービスAPIにアクセスするAPI呼び出し元から、PLMNトラストドメインの接続形態 (topology) を隠蔽するメカニズムを有する。

20

#### 【0024】

図3は、API呼び出しの例(1)を示す図である。3GPPコアネットワークでは外部のアプリケーション向けにAPIを解放しており、サードパーティのアプリケーションからAPIを呼び出すことができる。APIを呼び出すとき、コアネットワーク内にあるCAPIFコア機能 (CAPIF Core Function、CCFとも記載する。) によって、呼び出し元のアプリケーション (API invoker) を認証及び/又は認可し、いずれのアプリケーションがAPIを呼び出すことができるかを管理する。

30

#### 【0025】

図3に示されるように、API呼び出し元のアプリケーション30Aが、CAPIF-APIを利用してCAPIFコア機能30Bに事前登録される。CAPIFコア機能30Bでは、サードパーティのアプリケーション30Aを認証及び/又は認可する。また、図3に示されるように、API呼び出し元のアプリケーション30Aが、コアネットワークのAPIを呼び出すと、認証及び/又は認可された外部アプリケーション向けに、API提供機能 (API Exposing Function、AEFとも記載する。) 30CによってサービスAPIを解放する。

#### 【0026】

図4は、API呼び出しの例(2-1)を示す図である。図5は、API呼び出しの例(2-2)を示す図である。具体的なユースケースとして、QoS変更オプションを想定する。ユーザは、契約により所望のタイミングでQoS変更リクエストを送ることにより、快適な通信環境が得られるものとする。図4に示されるように、ユーザのアプリケーションからQoS変更リクエストが5GS (5G System) に含まれるNEFにコアネットワークのAPI呼び出しとして送信され、QoS変更が実行される。

40

#### 【0027】

しかしながら、従来技術では、いずれのユーザがいずれのユーザのQoSを変更できるのか判断することができず、適切でないユーザのQoSを変更することが可能となってしまう。例えば、図5に示されるように、CAPIFコア機能30Bでは、どのユーザのQ

50

oS 変更が許可されているかがわからず、API 提供機能 30C では、QoS 変更可の契約者が、QoS 変更不可ユーザの QoS を変更することを受け入れてしまう。また、QoS 以外のサービスであっても、いずれのユーザのリソースにアクセスできるかを判断することができない。なお、図 5 では、API 呼び出し元はエンドユーザのスマホ等である。

【0028】

以降、本実施例では QoS 変更を具体例として案を説明するが、ユーザが利用する API は QoS 制御に限られず、オペレータがユーザ向けに提供しているすべての API としてよい。例えば、特定のユーザの U-plane 通信路を変更する API があるが、エンドユーザが自ら当該 API を利用する際にも、本実施例で説明する方式を適用してよい。

【0029】

図 6 は、API 呼び出しの例 (3-1) を示す図である。図 7 は、API 呼び出しの例 (3-2) を示す図である。具体的なユースケースとして、サードパーティ社製のスマートフォンゲームをプレイする場合を想定する。ユーザは課金すなわち契約により所望のタイミングで QoS 変更リクエストを送ることにより、快適な通信環境が得られるものとする。図 6 に示されるように、ユーザのアプリケーションから QoS 変更リクエストが、ゲームサーバを介して 5G に含まれる NEF にコアネットワークの API 呼び出しとして送信され、QoS 変更が実行される。

【0030】

しかしながら、従来技術では、いずれのユーザがいずれのユーザの QoS を変更できるのか判断することができず、QoS 変更オプションのない (又は一般に適切な契約のない) ユーザからの QoS 変更リクエストを拒否することができない。例えば、図 7 に示されるように、CAPIF コア機能 30B では、どのユーザからの要求であるかがわからず、API 提供機能 30C では、ゲームサーバ自体が認証及び認可されていれば、API を呼び出すことが可能となってしまう。図 7 に示されるように、QoS 変更オプションありのゲームプレイヤーに対応する UE 20A からの QoS 変更リクエストを許容し、QoS 変更オプションなしのゲームプレイヤーに対応する UE 20B からの QoS 変更リクエストを拒否する動作が、ネットワーク側が意図する動作である。なお、図 7 では、API 呼び出し元はサードパーティのゲームサーバ等である。

【0031】

そこで、CAPIF コア機能 30B が、個々の端末を認証して API 利用を認可してもよい。また、個々の端末がいずれの API を呼び出してよいかを規定するスコープを管理してもよい。また、当該スコープ内で、指定した UE の QoS のみを変更できるようにしてもよい。

【0032】

図 8 は、API 呼び出しの例 (4) を示す図である。図 8 は従来技術において AF が API を呼び出す例を示す。図 8 に示されるように、API 呼び出し元 30A は、CAPIF コア機能 30B に onboarding する。「onboarding」とは、ここでは CAPIF コア機能 30B が API 呼び出し元 30A を認証しワンタイム登録して、API 呼び出し元 30A に CAPIF 及びサービス API にアクセスすることを許可する動作をいう。続いて、API 呼び出し元 30A と CAPIF コア機能 30B はセキュリティメソッドを合意する。続いて、API 呼び出し元 30A は、アクセストークンを CAPIF コア機能 30B に要求し、CAPIF コア機能 30B はアクセストークンを発行する。

【0033】

上記のセキュリティメソッドの合意は、OAuth 2.0 Client Credential 方式を用いており、リソースオーナーの許諾がなくてもクライアント (図 8 では API 呼び出し元) の認証のみで API 呼び出しが認可される。

【0034】

図 9 は、本発明の実施の形態における UE による API 呼び出しの例 (1) を説明するための図である。ステップ 1 において、BSF (Bootstrapping Server Function) 30F 及び UDM 30G は、Bootstrapping 手順の実行により UE 20 を認証

10

20

30

40

50

し、UE 20とCAPIFコア機能30Bが直接通信できるようにする。UE 20は、CCF 30Bから暫定識別子を受け取る。暫定識別子は、例えば、NA-GUTI (Northbound Access Globally Unique Temporary Identifier) であってもよい。続くステップ2において、UE 20とCCF 30Bとの間でセキュリティメソッドが合意される。

【0035】

図10は、本発明の実施の形態におけるUEによるAPI呼び出しの例(2)を説明するための図である。続くステップ3において、UE 20は、暫定識別子及び呼び出したいAPIを明示してCCF 30Bにアクセストークンの発行を要求する。なお、ステップ3の時点で、変更対象のユーザ情報等をCCF 30Bに送信し、当該ユーザ情報に基づいてアクセストークンがCCF 30Bから発行されてもよい。

10

【0036】

続くステップ4において、CCF 30Bは暫定識別子から加入者を特定し、UDM 30Gに加入者情報を確認する。続くステップ5において、UDM 30Gは、加入者情報を返却する。図10に示される許可API、メソッド及び対象ユーザが関連付けられたテーブルを、UDM 30Gは、加入者情報としてCCF 30Bに返却してもよい。

【0037】

続くステップ6において、CCF 30Bは、当該テーブルの許可API及びメソッドに基づいて、UE 20が目的のAPIを呼び出すことが許容されるとCCF 30Bが判定できた場合、CCF 30BはUEにアクセストークンを発行する。図10に示される例では、例えば、AssesssionWithQoSがUE 20から呼び出されている場合、許可されているAPIであるため、アクセストークンがCCF 30Bから発行される。

20

【0038】

続くステップ7において、UE 20は、受領したアクセストークンを用いて、AEF 30C宛にサービスAPIを呼び出す。例えば、図10に示されるように、アクセストークンが@@@@@、APIがAssesssionWithQoS及び変更対象ユーザのIPアドレスがxxx.xxx.xxx.xxxであることを示す情報をUE 20はAEF 30Cに送ることで、サービスAPIを呼び出してよい。

【0039】

図11は、本発明の実施の形態におけるUEによるAPI呼び出しの例(3)を説明するための図である。続くステップ8において、AEF 30Cは、CCF 30Bに対し、API要求を認可してよいか確認する。続くステップ9において、CCF 30Bは、UDM 30GにAPI呼び出し元の加入者の加入者情報を要求する。続くステップ10において、UDM 30Gは、加入者情報を返却する。図11に示される許可API、メソッド及び対象ユーザが関連付けられたテーブルを、UDM 30Gは、加入者情報としてCCF 30Bに返却してもよい。続くステップ11において、CCF 30Bは、加入者情報及びAPI要求に基づいて、認可してよいAPI要求が否かを判定し、結果をAEF 30Cに返却する。

30

【0040】

例えば、CCF 30Bは、「API: AssesssionWithQoS、変更対象ユーザのIPアドレスがxxx.xxx.xxx.xxx」という要求と、図11に示される加入者情報の「対象ユーザ」とを比較し、目的のユーザへのQoS変更が加入者情報にて許可されていれば、当該APIの利用を認可してよいと判定してもよい。続くステップ12において、CCF 30Bにおいて当該API利用が認可された場合、AEF 30Cは要求に従って処理を実行し、API利用可否の結果をUE 20に返却する。

40

【0041】

図12は、本発明の実施の形態におけるUE及びAFによるAPI呼び出しの例(1)を説明するための図である。ステップ1において、API呼び出し元30A(例えば、ゲームサーバ)は、CAPIFコア機能30BにOnboardingする。当該Onboardingは、従来技術と同様であってもよい。ステップ1において、ステップ1と並行して、BSF 30F及びUDM 30Gは、Bootstrapping手順の実行に

50

よりUE 20を認証し、UE 20とCAPIFコア機能30Bが直接通信できるようにする。UE 20は、CCF 30Bから暫定識別子を受け取る。暫定識別子は、例えば、NA-GUTIであってもよい。

【0042】

図13は、本発明の実施の形態におけるUE及びAFによるAPI呼び出しの例(2)を説明するための図である。続くステップ2において、API呼び出し元30Aは、UEトリガのAPI呼び出しが必要であることを、UE 20からの要求等により検知する。例えば、当該UEトリガは、UE 20からゲームサーバに対してQoSの変更要求を示す情報を送信することであってもよいし、ゲームサーバ側で当該ユーザに対してQoSを変更する必要があると判定されたことであってもよい。

10

【0043】

続くステップ3において、API呼び出し元30AとCCF 30Bとの間で、個々の契約者の契約内容に関わるAPIの呼び出しが必要な場合、API呼び出し元30AとCCF 30Bとの間で、セキュリティメソッドとしてOAuth 2.0 Authorization Code Flowを用いた認可を行うことが合意される。

【0044】

図14は、本発明の実施の形態におけるUE及びAFによるAPI呼び出しの例(3)を説明するための図である。続くステップ4において、API呼び出し元30Aは、APIを呼び出してよいかユーザに確認する。続くステップ5において、APIを呼び出す許可がユーザから得られた場合、UE 20の暫定識別子及び呼び出したいAPIを明示してCCF 30Bに認可リクエストを送信する。続くステップ6において、CCF 30Bは、暫定識別子から対象UE(契約者)を特定し、UDM 30Gに対して当該契約者の加入者情報を確認する。

20

【0045】

続くステップ7において、UDM 30Gは、加入者情報を返却する。図12に示される許可API、メソッド及び対象ユーザが関連付けられたテーブルを、UDM 30Gは、加入者情報としてCCF 30Bに返却してもよい。続くステップ8において、CCF 30Bは、加入者情報及に基づいて、当該契約書が目的のAPIを呼び出してよいか否かを判定し、結果をUE 20に通知する。ここで、UE 20は、必要に応じてパスワード入力等でAPI利用を許諾してもよい。続くステップ9において、CCF 30Bは、API呼び出し元30Aに対し、APIの利用が認可されたことを示すAuthorization Codeを発行する。

30

【0046】

図15は、本発明の実施の形態におけるUE及びAFによるAPI呼び出しの例(4)を説明するための図である。続くステップ10において、API呼び出し元30Aは、Authorization Codeを用いて、API呼び出しのアクセストークンを要求し、アクセストークンをCCF 30Bから受領する。続くステップ11において、API呼び出し元30Aは、アクセストークンを用いてサービスAPIにアクセスする。

【0047】

図16は、本発明の実施の形態におけるUE及びAFによるAPI呼び出しの例(5)を説明するための図である。続くステップ12において、AEF 30Cは、CCF 30Bに対し、API要求を認可してよいか確認する。続くステップ13において、CCF 30Bは、UDM 30GにAPI呼び出し元の加入者の加入者情報を要求する。続くステップ14において、UDM 30Gは、加入者情報を返却する。図16に示される許可API、メソッド及び対象ユーザが関連付けられたテーブルを、UDM 30Gは、加入者情報としてCCF 30Bに返却してもよい。

40

【0048】

続くステップ15において、CCF 30Bは、加入者情報及びAPI要求に基づいて、認可してよいAPI要求か否かを判定し、結果をAEF 30Cに返却する。続くステップ16において、CCF 30Bにおいて当該API利用が認可された場合、AEF 30Cは

50

要求に従って処理を実行し、API利用可否の結果をAPI呼び出し元30Aに返却する。  
【0049】

図17は、本発明の実施の形態におけるAPIの範囲を説明するための図である。図17に示されるように、CCF30Bからの加入者識別子に基づく契約者情報の問い合わせに対して、UDM30Gは、個々の加入者情報に対して、当該加入者が許可されているAPI及び許可されたメソッド、許可されたユーザを一覧としてCCF30Bに返却してもよい。例えば、UDM30Gは、図17に示されるオプション1のように、許可API、メソッド及び対象ユーザを関連付けて1エントリとしてCCF30に返却してもよい。  
【0050】

また、例えば、UDM30Gは、図17に示されるオプション2のように、Role対応表として、典型的なスコープの設定としてRole、メソッド及び対象ユーザを1エントリとして関連付けて予め定義し、許可APIといずれのRoleかを示す情報を、CCF30Bに返却してもよい。すなわち、CCF30Bは、個々の加入者とRoleを関連付けることで、各APIで許可された動作を特定してもよい。

10

【0051】

図18は、本発明の実施の形態におけるUE及びAFを含むシステムの例を示す図である。図18に示されるように、信頼済ドメインであるPLMN (PLMN Trust domain) には、CAPIF-APIを含むCCF30B、サービスAPIを含むAEF30C、APF (API Publishing Function) 30D、AMF (API Management Function) 30E、コアネットワーク及びアクセスネットワークが属する。一方、PLMN外には、API呼び出し元30A (例えばゲームサーバ)、UE20が存在する。

20

【0052】

図18に示されるように、API呼び出し元30Aは、コアネットワークを介してAEF30Cに接続されてもよいし、CAPIF-API及びサービスAPIを呼び出し可能であってもよい。UE20は、アクセスネットワーク及びコアネットワークを介して、API呼び出し元30A、AEF30Cと接続されてもよい。

【0053】

図19は、本発明の実施の形態におけるUEを含むシステムの例を示す図である。図18に示されるように、信頼済ドメインであるPLMNには、CAPIF-APIを含むCCF30B、サービスAPIを含むAEF30C、APF30D、AMF30E、コアネットワーク及びアクセスネットワークが属する。一方、PLMN外には、UE20が存在する。

30

【0054】

図18に示されるように、UE20は、アクセスネットワーク及びコアネットワークを介して、CCF30B、AEF30Cと接続されてもよいし、CAPIF-API及びサービスAPIを呼び出し可能であってもよい。

【0055】

なお、図18及び図19はシステム構成の一例を示すものであり、これに限られない。例えば、AEF30C、APF30D及びAMF30Eが信頼済PLMNドメイン外にあってもよい。

40

【0056】

図20は、本発明の実施の形態におけるUEによるAPI呼び出しの例を説明するためのシーケンス図である。図20を用いて、上述した図8から図11までのUEによるAPI呼び出しの例の詳細な動作を説明する。

【0057】

ステップS101において、UE20は、BSF30F及びUDM30GとBoostrapping手順を実行する。続くステップS102において、UE20は、CCF20Bとアプリケーション要求/応答を実行、CCF20Bは、BSF30Fと認証要求/応答を実行する。続くステップS103において、UE20はNA-GUTIを取得する。続くステップS104において、UE20はCCF30Bから必要な通知を受けられ

50

るよう CCF 30B に Subscribe する。続くステップ S 105 において、UE 20 と CCF 30B との間の TLS (Transport Layer Security) 接続が確立される。ステップ S 101 からステップ S 105 までの手順により、既存の Onboarding の代わりに、Bootstrapping にて端末 20 を認証してから UE - CCF 間で通信を行う。なお、ステップ S 104 は、実行されてもよいし、実行されなくてもよい。

【0058】

ステップ S 106 において、UE 20 は、セキュリティメソッド要求を CCF 30B に送信する。続くステップ S 107 において、CCF 30B は、セキュリティメソッドを選択する。続くステップ S 108 において、OAuth 2.0 Client Credential であるセキュリティメソッド応答が、CCF 30B から UE 20 に送信される。ステップ S 106 からステップ S 108 までの手順により、API 呼び出しに使用するセキュリティメソッドが決定される。

10

【0059】

ステップ S 109 において、UE 20 は、NA - GUTI を用いて、OAuth 2.0 に基づいたアクセストークン要求を CCF 30B に送信する。続くステップ S 110 において、CCF 30B は、加入者情報の確認を UDM 30G に対して行う。続くステップ S 111 において、CCF 30B は、アクセストークン要求を検証する。続くステップ S 112 において、CCF 30B は、OAuth 2.0 によるアクセストークンを UE 20 に応答する。ステップ S 109 からステップ S 112 までの手順により、NA - GUTI を用いてアクセストークンが発行され、API 呼び出しのためのアクセストークンを端末 20 は取得する。

20

【0060】

ステップ S 113 において、UE 20 と AEF 30C 間に TLS 接続が確立される。続くステップ S 114 において、UE 20 は、OAuth 2.0 によるアクセストークンによって、Northbound API を AEF 30C に対して呼び出す。続くステップ S 115 において、CCF 30B は、加入者情報の確認を UDM 30G に対して行う。続くステップ S 116 において、AEF 30C は、アクセストークンを検証する。続くステップ S 117 において、AEF 30C は、Northbound API 呼び出しに係る応答を UE 20 に送信する。ステップ S 113 からステップ S 117 までの手順で、API 呼び出しが実行される。

30

【0061】

図 21 は、本発明の実施の形態における UE 及び AF による API 呼び出しの例を説明するためのシーケンス (1) 図である。図 22 は、本発明の実施の形態における UE 及び AF による API 呼び出しの例を説明するためのシーケンス (2) 図である。図 21 及び図 22 を用いて、上述した図 12 から図 16 までの UE 及び AF による API 呼び出しの例の詳細な動作を説明する。

【0062】

ステップ S 201 において、AMF 30E は、Onboarding 登録情報 (CCF 情報、OAuth 2.0 アクセストークンを伴う) を AF 30A に送信する。ステップ S 201 は AF 30A がオフラインの何らかの手法で Onboarding 登録情報を取得することでもよい。ステップ S 202 において、AF 30A と CCF 30B との間に TLS 接続が確立される。続くステップ S 203 において、AF 30A は、Onboard API 呼び出し要求 (OAuth 2.0 アクセストークン、API 呼び出しパブリックキーを伴う) を CCF 30B に送信する。続くステップ S 204 において、CCF 30B は、Onboard API 呼び出し応答 (API 呼び出し ID、API 呼び出し証明書、Onboard シークレットを伴う) を AF 30A に送信する。ステップ S 201 からステップ S 204 までの動作で、AF の Onboarding (登録) が完了する。

40

【0063】

ステップ S 205 において、UE 20 は、BSF 30F 及び UDM 30G と Bootstrapping 手順を実行する。続くステップ S 206 において、UE 20 は、CCF

50

20Bとアプリケーション要求/応答を実行、CCF20Bは、BSF30Fと認証要求/応答を実行する。続くステップS207において、UE20はNA-GUTIを取得する。続くステップS208において、UE20はCCF30Bから必要な通知を受けられるようCCF30BにSubscribeする。ステップS205からステップS208までの手順により、Bootstrapping完了する。すなわち、AF30AはOnboardingを実施し、UE20はBootstrappingを実施する。

【0064】

ステップS209において、CCF30Bは、API呼び出しのトリガを検知する。続くステップS210において、AF30Aは、セキュリティメソッド要求をCCF30Bに送信する。続くステップS211において、CCF30Bは、セキュリティメソッドを選択する。続くステップS212において、CCF30Bは、OAuth2.0 Authorization Code Flowによるセキュリティメソッド応答をAF30Aに送信する。ステップS209からステップS212までの手順でAPI呼び出しに使用するセキュリティメソッドが決定される。

10

【0065】

ステップS213において、AF30Aは、ユーザにAPI利用可否の確認を行う。UE20は必要に応じて応答をAF30Aに送信する。続くステップS214において、AF30Aは、CAPIFセキュリティ要求及び認証要求(NA-GUTIを伴う)をCCF30Bに送信する。続くステップS215において、CCF30Bは、加入者情報の確認をUDM30Gに対して行う。続くステップS216において、UE20とCCF30Bとの間でTLS接続が確立される。続くステップS217において、UE20とCCF30Bとの間で、CAPIFセキュリティ要求及び認証通知要求/応答が実行される。続くステップS218において、CCF30Bは、Authorization Codeを発行し、AF30Aに送信する。ステップS213からステップS218までの手順により、ユーザからの許可取得及びAuthorization Codeの発行が実施される。

20

【0066】

ステップS219において、AF30Aは、Authorization CodeによるOAuth2.0によるアクセストークン要求をCCF30Bに送信する。続くステップS220において、CCF30Bは、アクセストークン要求を検証する。続くステップS221において、OAuth2.0によるアクセストークン(アクセストークン、有効期限、スコープを伴う)をAF30Aに返信する。ステップS219からステップS221までの手順によって、API呼び出しのためのアクセストークンが取得される。

30

【0067】

ステップS222において、AF30AとAEF30C間にTLS接続が確立される。続くステップS223において、AF30Aは、OAuth2.0によるアクセストークンによって、Northbound APIをAEF30Cに対して呼び出す。続くステップS224において、CCF30Bは、加入者情報の確認をUDM30Gに対して行う。続くステップS225において、AEF30Cは、アクセストークンを検証する。続くステップS226において、AEF30Cは、Northbound API呼び出しに係る応答をAF30Aに送信する。ステップS222からステップS226までの手順で、API呼び出しが実行される。

40

【0068】

上述の実施例により、回線利用者の立場においては、個々の契約者の契約情報に基づいて、エンドユーザ自身が端末からコアネットワークのAPIを利用し、ネットワークの制御ができるようになる。オペレータの立場においては、ネットワークが解放するAPIのうち、個々の契約者が利用できるAPIの粒度を加入者情報に基づいて管理することで、必要最低限のAPIのみを利用者に開放することができる。

【0069】

また、API呼び出しの事前準備として、既存のOnboardingに代替して、端

50

末のSIM情報を使って、個々の契約者を認証するBootstrappingを用いることにより、API呼び出しのトリガとなる個々の契約者を識別することができる。

【0070】

また、個々の契約者が利用できるAPIの範囲を加入者情報に保持しておき、当該加入者情報をチェックすることで、個人の粒度でAPI利用の権限を管理することができる。

【0071】

また、UE20及びAF30AによるAPI呼び出しの場合、OAuth 2.0のAuthorization Code Flow方式を利用することで、サードパーティのAF及びオペレータのネットワークノードが契約者の承諾を安全に取得しつつ、個々の契約者に許可されたAPIを利用することができる。

【0072】

すなわち、ネットワークにおいて加入者情報を識別可能とするインタフェースを提供することができる。

【0073】

(装置構成)

次に、これまでに説明した処理及び動作を実施する基地局10、ネットワークノード30及び端末20の機能構成例を説明する。基地局10、ネットワークノード30及び端末20は上述した実施例を実施する機能を含む。ただし、基地局10、ネットワークノード30及び端末20はそれぞれ、実施例の中の一部の機能のみを備えることとしてもよい。

【0074】

<基地局10及びネットワークノード30>

図23は、基地局10の機能構成の一例を示す図である。図23に示されるように、基地局10は、送信部110と、受信部120と、設定部130と、制御部140とを有する。図23に示される機能構成は一例に過ぎない。本発明の実施の形態に係る動作を実施できるのであれば、機能区分及び機能部の名称はどのようなものでもよい。なお、ネットワークノード30は、基地局10と同様の機能構成を有してもよい。また、システムアーキテクチャ上で複数の異なる機能を有するネットワークノード30は、機能ごとに分離された複数のネットワークノード30から構成されてもよい。また、ネットワークノード30は、コアネットワーク又はアクセスネットワークに存在するネットワークノードに限定されず、PLMNドメインに属するネットワークノードに対応してもよい。

【0075】

送信部110は、端末20又は他のネットワークノード30に送信する信号を生成し、当該信号を有線又は無線で送信する機能を含む。受信部120は、端末20又は他のネットワークノード30から送信された各種の信号を受信し、受信した信号から、例えばより上位のレイヤの情報を取得する機能を含む。

【0076】

設定部130は、予め設定される設定情報、及び、端末20に送信する各種の設定情報を記憶装置に格納し、必要に応じて記憶装置から読み出す。設定情報の内容は、例えば、ネットワークにおける加入者のプロファイル情報等である。

【0077】

制御部140は、実施例において説明したように、ネットワークにおける加入者のプロファイル情報の更新に係る処理を行う。また、制御部140は、端末20との通信に係る処理を行う。制御部140における信号送信に関する機能部を送信部110に含め、制御部140における信号受信に関する機能部を受信部120に含めてもよい。

【0078】

<端末20>

図24は、端末20の機能構成の一例を示す図である。図24に示されるように、端末20は、送信部210と、受信部220と、設定部230と、制御部240とを有する。図24に示される機能構成は一例に過ぎない。本発明の実施の形態に係る動作を実施できるのであれば、機能区分及び機能部の名称はどのようなものでもよい。

10

20

30

40

50

## 【 0 0 7 9 】

送信部 2 1 0 は、送信データから送信信号を作成し、当該送信信号を無線で送信する。受信部 2 2 0 は、各種の信号を無線受信し、受信した物理レイヤの信号からより上位のレイヤの信号を取得する。また、受信部 2 2 0 は、ネットワークノード 3 0 から送信される NR - P S S、NR - S S S、NR - P B C H、DL / U L 制御信号又は参照信号等を受信する機能を有する。

## 【 0 0 8 0 】

設定部 2 3 0 は、受信部 2 2 0 によりネットワークノード 3 0 から受信した各種の設定情報を記憶装置に格納し、必要に応じて記憶装置から読み出す。また、設定部 2 3 0 は、予め設定される設定情報も格納する。設定情報の内容は、例えば、接続が許可されるネットワークに係る情報等である。

10

## 【 0 0 8 1 】

制御部 2 4 0 は、実施例において説明したように、ネットワーク及びネットワークスライスへの接続制御に係る処理を行う。制御部 2 4 0 における信号送信に関する機能部を送信部 2 1 0 に含め、制御部 2 4 0 における信号受信に関する機能部を受信部 2 2 0 に含めてもよい。

## 【 0 0 8 2 】

(ハードウェア構成)

上記実施形態の説明に用いたブロック図(図 2 3 及び図 2 4)は、機能単位のブロックを示している。これらの機能ブロック(構成部)は、ハードウェア及びソフトウェアの少なくとも一方の任意の組み合わせによって実現される。また、各機能ブロックの実現方法は特に限定されない。すなわち、各機能ブロックは、物理的又は論理的に結合した 1 つの装置を用いて実現されてもよいし、物理的又は論理的に分離した 2 つ以上の装置を直接的又は間接的に(例えば、有線、無線などを用いて)接続し、これら複数の装置を用いて実現されてもよい。機能ブロックは、上記 1 つの装置又は上記複数の装置にソフトウェアを組み合わせて実現されてもよい。

20

## 【 0 0 8 3 】

機能には、判断、決定、判定、計算、算出、処理、導出、調査、探索、確認、受信、送信、出力、アクセス、解決、選択、選定、確立、比較、想定、期待、見做し、報知(broadcasting)、通知(notifying)、通信(communicating)、転送(forwarding)、構成(configuring)、再構成(reconfiguring)、割り当て(allocating、mapping)、割り振り(assigning)などがあるが、これらに限られない。たとえば、送信を機能させる機能ブロック(構成部)は、送信部(transmitting unit)や送信機(transmitter)と呼称される。いずれも、上述したとおり、実現方法は特に限定されない。

30

## 【 0 0 8 4 】

例えば、本開示の一実施の形態におけるネットワークノード 3 0、端末 2 0 等は、本開示の無線通信方法の処理を行うコンピュータとして機能してもよい。図 2 5 は、本開示の一実施の形態に係る基地局 1 0 及び端末 2 0 のハードウェア構成の一例を示す図である。ネットワークノード 3 0 は、基地局 1 0 と同様のハードウェア構成を有してもよい。上述の基地局 1 0 及び端末 2 0 は、物理的には、プロセッサ 1 0 0 1、記憶装置 1 0 0 2、補助記憶装置 1 0 0 3、通信装置 1 0 0 4、入力装置 1 0 0 5、出力装置 1 0 0 6、バス 1 0 0 7 などを含むコンピュータ装置として構成されてもよい。

40

## 【 0 0 8 5 】

なお、以下の説明では、「装置」という文言は、回路、デバイス、ユニット等に読み替えることができる。基地局 1 0 及び端末 2 0 のハードウェア構成は、図に示した各装置を 1 つ又は複数含むように構成されてもよいし、一部の装置を含まずに構成されてもよい。

## 【 0 0 8 6 】

基地局 1 0 及び端末 2 0 における各機能は、プロセッサ 1 0 0 1、記憶装置 1 0 0 2 等のハードウェア上に所定のソフトウェア(プログラム)を読み込ませることによって、プロセッサ 1 0 0 1 が演算を行い、通信装置 1 0 0 4 による通信を制御したり、記憶装置 1

50

002及び補助記憶装置1003におけるデータの読み出し及び書き込みの少なくとも一方を制御したりすることによって実現される。

【0087】

プロセッサ1001は、例えば、オペレーティングシステムを動作させてコンピュータ全体を制御する。プロセッサ1001は、周辺装置とのインタフェース、制御装置、演算装置、レジスタ等を含む中央処理装置(CPU: Central Processing Unit)で構成されてもよい。例えば、上述の制御部140、制御部240等は、プロセッサ1001によって実現されてもよい。

【0088】

また、プロセッサ1001は、プログラム(プログラムコード)、ソフトウェアモジュール又はデータ等を、補助記憶装置1003及び通信装置1004の少なくとも一方から記憶装置1002に読み出し、これらに従って各種の処理を実行する。プログラムとしては、上述の実施の形態において説明した動作の少なくとも一部をコンピュータに実行させるプログラムが用いられる。例えば、図23に示した基地局10の制御部140は、記憶装置1002に格納され、プロセッサ1001で動作する制御プログラムによって実現されてもよい。また、例えば、図24に示した端末20の制御部240は、記憶装置1002に格納され、プロセッサ1001で動作する制御プログラムによって実現されてもよい。上述の各種処理は、1つのプロセッサ1001によって実行される旨を説明してきたが、2以上のプロセッサ1001により同時又は逐次に実行されてもよい。プロセッサ1001は、1以上のチップによって実装されてもよい。なお、プログラムは、電気通信回線を介してネットワークから送信されてもよい。

【0089】

記憶装置1002は、コンピュータ読み取り可能な記録媒体であり、例えば、ROM(Read Only Memory)、EPROM(Erasable Programmable ROM)、EEPROM(Electrically Erasable Programmable ROM)、RAM(Random Access Memory)等の少なくとも1つによって構成されてもよい。記憶装置1002は、レジスタ、キャッシュ、メインメモリ(主記憶装置)等と呼ばれてもよい。記憶装置1002は、本開示の一実施の形態に係る通信方法を実施するために実行可能なプログラム(プログラムコード)、ソフトウェアモジュール等を保存することができる。

【0090】

補助記憶装置1003は、コンピュータ読み取り可能な記録媒体であり、例えば、CD-ROM(Compact Disc ROM)等の光ディスク、ハードディスクドライブ、フレキシブルディスク、光磁気ディスク(例えば、コンパクトディスク、デジタル多用途ディスク、Blu-ray(登録商標)ディスク)、スマートカード、フラッシュメモリ(例えば、カード、スティック、キードライブ)、フロッピー(登録商標)ディスク、磁気ストリップ等の少なくとも1つによって構成されてもよい。上述の記憶媒体は、例えば、記憶装置1002及び補助記憶装置1003の少なくとも一方を含むデータベース、サーバその他の適切な媒体であってもよい。

【0091】

通信装置1004は、有線ネットワーク及び無線ネットワークの少なくとも一方を介してコンピュータ間の通信を行うためのハードウェア(送受信デバイス)であり、例えばネットワークデバイス、ネットワークコントローラ、ネットワークカード、通信モジュールなどともいう。通信装置1004は、例えば周波数分割複信(FDD: Frequency Division Duplex)及び時分割複信(TDD: Time Division Duplex)の少なくとも一方を実現するために、高周波スイッチ、デュプレクサ、フィルタ、周波数シンセサイザなどを含んで構成されてもよい。例えば、送受信アンテナ、アンプ部、送受信部、伝送路インタフェース等は、通信装置1004によって実現されてもよい。送受信部は、送信部と受信部とで、物理的に、または論理的に分離された実装がなされてもよい。

【0092】

入力装置1005は、外部からの入力を受け付ける入力デバイス(例えば、キーボード

10

20

30

40

50

、マウス、マイクロフォン、スイッチ、ボタン、センサ等)である。出力装置1006は、外部への出力を実施する出力デバイス(例えば、ディスプレイ、スピーカー、LEDランプ等)である。なお、入力装置1005及び出力装置1006は、一体となった構成(例えば、タッチパネル)であってもよい。

#### 【0093】

また、プロセッサ1001及び記憶装置1002等の各装置は、情報を通信するためのバス1007によって接続される。バス1007は、単一のバスを用いて構成されてもよいし、装置間ごとに異なるバスを用いて構成されてもよい。

#### 【0094】

また、基地局10及び端末20は、マイクロプロセッサ、デジタル信号プロセッサ(DSP: Digital Signal Processor)、ASIC(Application Specific Integrated Circuit)、PLD(Programmable Logic Device)、FPGA(Field Programmable Gate Array)等のハードウェアを含んで構成されてもよく、当該ハードウェアにより、各機能ブロックの一部又は全てが実現されてもよい。例えば、プロセッサ1001は、これらのハードウェアの少なくとも1つを用いて実装されてもよい。

#### 【0095】

(実施の形態のまとめ)

以上、説明したように、本発明の実施の形態によれば、端末を認証し暫定識別子を当該端末に送信する送信部と、前記暫定識別子を含む要求又は前記暫定識別子に基づく認証コードを受信する受信部と、前記暫定識別子を含む要求又は前記認証コードに基づいて、アクセストークンを発行する制御部とを有し、前記送信部は、前記アクセストークンを前記端末又は外部アプリケーションに送信し、前記受信部は、前記アクセストークンに基づくAPI(Application Programming Interface)呼び出し要求を前記端末又は前記外部アプリケーションから受信し、前記制御部は、前記アクセストークンを検証して前記API呼び出し要求が認可されたものであると判定した場合、前記API呼び出し要求に基づいて処理を実行するネットワークノードが提供される。

#### 【0096】

上記の構成により、回線利用者の立場においては、個々の契約者の契約情報に基づいて、エンドユーザ自身が端末からコアネットワークのAPIを利用し、ネットワークの制御ができるようになる。オペレータの立場においては、ネットワークが解放するAPIのうち、個々の契約者が利用できるAPIの粒度を加入者情報に基づいて管理することで、必要最低限のAPIのみを利用者に開放することができる。また、API呼び出しの事前準備として、既存のOnboardingに代替して、端末のSIM情報を使って、個々の契約者を認証するBoostrappingを用いることにより、API呼び出しのトリガとなる個々の契約者を識別することができる。また、個々の契約者が利用できるAPIの範囲を加入者情報に保持しておき、当該加入者情報をチェックすることで、個人の粒度でAPI利用の権限を管理することができる。また、UE20及びAF30AによるAPI呼び出しの場合、OAuth 2.0のAuthorization Code Flow方式を利用することで、サードパーティのAF及びオペレータのネットワークノードが契約者の承諾を安全に取得しつつ、個々の契約者に許可されたAPIを利用することができる。すなわち、ネットワークにおいて加入者情報を識別可能とするインタフェースを提供することができる。

#### 【0097】

前記受信部は、前記端末又は前記外部アプリケーションからAPI呼び出しに使用するセキュリティメソッドに係る要求を受信し、前記制御部は、セキュリティメソッドを選択し、前記送信部は、前記選択したセキュリティメソッドを示す応答を前記端末又は外部アプリケーションに送信してもよい。当該構成により、ネットワークノードは、API呼び出しに使用するセキュリティメソッドを選択し設定することができる。

#### 【0098】

前記送信部が前記アクセストークンを前記外部アプリケーションに送信する場合、前記

制御部は、前記外部アプリケーションを予め認証し登録してもよい。当該構成により、ネットワークノードは、認証された外部アプリケーションから、UEに係るAPI呼び出しを受けることができる。

#### 【0099】

前記送信部が前記アクセストークンを前記外部アプリケーションに送信する場合、前記制御部は、ユーザにAPI利用可否の確認を実施した後、前記アクセストークンを発行してもよい。当該構成により、ネットワークノードは、外部アプリケーションがAPI呼び出しを実行する場合、事前にユーザの意図を確認してからAPI呼び出しを実行することができる。

#### 【0100】

前記制御部は、前記API呼び出し要求が認可されたものであるかを判定するとき、少なくともユーザごとのスコープが設定される、許可されるAPI及び許可されるメソッドを参照してもよい。当該構成により、ネットワークノードは、ユーザごとの粒度のスコープで、API呼び出しを制御することができる。

#### 【0101】

また、本発明の実施の形態によれば、端末を認証し暫定識別子を当該端末に送信する送信手順と、前記暫定識別子を含む要求又は前記暫定識別子に基づく認証コードを受信する受信手順と、前記暫定識別子を含む要求又は前記認証コードに基づいて、アクセストークンを発行する制御手順と、前記アクセストークンを前記端末又は外部アプリケーションに送信する手順と、前記アクセストークンに基づくAPI (Application Programming Interface) 呼び出し要求を前記端末又は前記外部アプリケーションから受信する手順と、前記アクセストークンを検証して前記API呼び出し要求が認可されたものであると判定した場合、前記API呼び出し要求に基づいて処理を実行する手順とをネットワークノードが実行する通信方法が提供される。

#### 【0102】

上記の構成により、回線利用者の立場においては、個々の契約者の契約情報に基づいて、エンドユーザ自身が端末からコアネットワークのAPIを利用し、ネットワークの制御ができるようになる。オペレータの立場においては、ネットワークが解放するAPIのうち、個々の契約者が利用できるAPIの粒度を加入者情報に基づいて管理することで、必要最低限のAPIのみを利用者に開放することができる。また、API呼び出しの事前準備として、既存のOnboardingに代替して、端末のSIM情報を使って、個々の契約者を認証するBootstrappingを用いることにより、API呼び出しのトリガとなる個々の契約者を識別することができる。また、個々の契約者が利用できるAPIの範囲を加入者情報に保持しておき、当該加入者情報をチェックすることで、個人の粒度でAPI利用の権限を管理することができる。また、UE20及びAF30AによるAPI呼び出しの場合、OAuth2.0のAuthorization Code Flow方式を利用することで、サードパーティのAF及びオペレータのネットワークノードが契約者の承諾を安全に取得しつつ、個々の契約者に許可されたAPIを利用することができる。すなわち、ネットワークにおいて加入者情報を識別可能とするインタフェースを提供することができる。

#### 【0103】

(実施形態の補足)

以上、本発明の実施の形態を説明してきたが、開示される発明はそのような実施形態に限定されず、当業者は様々な変形例、修正例、代替例、置換例等を理解するであろう。発明の理解を促すため具体的な数値例を用いて説明がなされたが、特に断りのない限り、それらの数値は単なる一例に過ぎず適切な如何なる値が使用されてもよい。上記の説明における項目の区分けは本発明に本質的ではなく、2以上の項目に記載された事項が必要に応じて組み合わせ使用されてよいし、ある項目に記載された事項が、別の項目に記載された事項に(矛盾しない限り)適用されてよい。機能ブロック図における機能部又は処理部の境界は必ずしも物理的な部品の境界に対応するとは限らない。複数の機能部の動作が物

10

20

30

40

50

理的には1つの部品で行われてもよいし、あるいは1つの機能部の動作が物理的には複数の部品により行われてもよい。実施の形態で述べた処理手順については、矛盾の無い限り処理の順序を入れ替えてもよい。処理説明の便宜上、ネットワークノード30及び端末20は機能的なブロック図を用いて説明されたが、そのような装置はハードウェアで、ソフトウェアで又はそれらの組み合わせで実現されてもよい。本発明の実施の形態に従ってネットワークノード30が有するプロセッサにより動作するソフトウェア及び本発明の実施の形態に従って端末20が有するプロセッサにより動作するソフトウェアはそれぞれ、ランダムアクセスメモリ(RAM)、フラッシュメモリ、読み取り専用メモリ(ROM)、EPROM、EEPROM、レジスタ、ハードディスク(HDD)、リムーバブルディスク、CD-ROM、データベース、サーバその他の適切な如何なる記憶媒体に保存されてもよい。

10

#### 【0104】

また、情報の通知は、本開示で説明した態様/実施形態に限られず、他の方法を用いて行われてもよい。例えば、情報の通知は、物理レイヤシグナリング(例えば、DCI(Downlink Control Information)、UCI(Uplink Control Information))、上位レイヤシグナリング(例えば、RRC(Radio Resource Control)シグナリング、MAC(Medium Access Control)シグナリング、報知情報(MIB(Master Information Block)、SIB(System Information Block))、その他の信号又はこれらの組み合わせによって実施されてもよい。また、RRCシグナリングは、RRCメッセージと呼ばれてもよく、例えば、RRC接続セットアップ(RRC Connection Setup)メッセージ、RRC接続再構成(RRC Connection Reconfiguration)メッセージ等であってもよい。

20

#### 【0105】

本開示において説明した各態様/実施形態は、LTE(Long Term Evolution)、LTE-A(LTE-Advanced)、SUPER 3G、IMT-Advanced、4G(4th generation mobile communication system)、5G(5th generation mobile communication system)、FRA(Future Radio Access)、NR(new Radio)、W-CDMA(登録商標)、GSM(登録商標)、CDMA2000、UMB(Ultra Mobile Broadband)、IEEE 802.11(Wi-Fi(登録商標))、IEEE 802.16(WiMAX(登録商標))、IEEE 802.20、UWB(Ultra-WideBand)、Bluetooth(登録商標)、その他の適切なシステムを利用するシステム及びこれらに基づいて拡張された次世代システムの少なくとも一つに適用されてもよい。また、複数のシステムが組み合わされて(例えば、LTE及びLTE-Aの少なくとも一方と5Gとの組み合わせ等)適用されてもよい。

30

#### 【0106】

本明細書で説明した各態様/実施形態の処理手順、シーケンス、フローチャート等は、矛盾の無い限り、順序を入れ替えてもよい。例えば、本開示において説明した方法については、例示的な順序を用いて様々なステップの要素を提示しており、提示した特定の順序に限定されない。

#### 【0107】

本明細書においてネットワークノード30によって行われるとした特定動作は、場合によってはその上位ノード(upper node)によって行われることもある。ネットワークノード30を有する1つ又は複数のネットワークノード(network nodes)からなるネットワークにおいて、端末20との通信のために行われる様々な動作は、ネットワークノード30及びネットワークノード30以外の他のネットワークノード(例えば、MME又はS-GW等が考えられるが、これらに限られない)の少なくとも一つによって行われ得ることは明らかである。上記においてネットワークノード30以外の他のネットワークノードが1つである場合を例示したが、他のネットワークノードは、複数の他のネットワークノードの組み合わせ(例えば、MME及びS-GW)であってもよい。

40

#### 【0108】

本開示において説明した情報又は信号等は、上位レイヤ(又は下位レイヤ)から下位レ

50

イヤ（又は上位レイヤ）へ出力され得る。複数のネットワークノードを介して入出力されてもよい。

【0109】

入出力された情報等は特定の場所（例えば、メモリ）に保存されてもよいし、管理テーブルを用いて管理してもよい。入出力される情報等は、上書き、更新、又は追記され得る。出力された情報等は削除されてもよい。入力された情報等は他の装置へ送信されてもよい。

【0110】

本開示における判定は、1ビットで表される値（0か1か）によって行われてもよいし、真偽値（Boolean：true又はfalse）によって行われてもよいし、数値の比較（例えば、所定の値との比較）によって行われてもよい。

10

【0111】

ソフトウェアは、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語と呼ばれるか、他の名称で呼ばれるかを問わず、命令、命令セット、コード、コードセグメント、プログラムコード、プログラム、サブプログラム、ソフトウェアモジュール、アプリケーション、ソフトウェアアプリケーション、ソフトウェアパッケージ、ルーチン、サブルーチン、オブジェクト、実行可能ファイル、実行スレッド、手順、機能などを意味するよう広く解釈されるべきである。

【0112】

また、ソフトウェア、命令、情報などは、伝送媒体を介して送受信されてもよい。例えば、ソフトウェアが、有線技術（同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線（DSL：Digital Subscriber Line）など）及び無線技術（赤外線、マイクロ波など）の少なくとも一方を使用してウェブサイト、サーバ、又は他のリモートソースから送信される場合、これらの有線技術及び無線技術の少なくとも一方は、伝送媒体の定義内に含まれる。

20

【0113】

本開示において説明した情報、信号などは、様々な異なる技術のいずれかを使用して表されてもよい。例えば、上記の説明全体に渡って言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、チップなどは、電圧、電流、電磁波、磁界若しくは磁性粒子、光場若しくは光子、又はこれらの任意の組み合わせによって表されてもよい。

30

【0114】

なお、本開示において説明した用語及び本開示の理解に必要な用語については、同一の又は類似する意味を有する用語と置き換えてもよい。例えば、チャンネル及びシンボルの少なくとも一方は信号（シグナリング）であってもよい。また、信号はメッセージであってもよい。また、コンポーネントキャリア（CC：Component Carrier）は、キャリア周波数、セル、周波数キャリアなどと呼ばれてもよい。

【0115】

本開示において使用する「システム」及び「ネットワーク」という用語は、互換的に使用される。

【0116】

また、本開示において説明した情報、パラメータなどは、絶対値を用いて表されてもよいし、所定の値からの相対値を用いて表されてもよいし、対応する別の情報を用いて表されてもよい。例えば、無線リソースはインデックスによって指示されるものであってもよい。

40

【0117】

上述したパラメータに使用する名称はいかなる点においても限定的な名称ではない。さらに、これらのパラメータを使用する数式等は、本開示で明示的に開示したものと異なる場合もある。様々なチャンネル（例えば、P U C C H、P D C C Hなど）及び情報要素は、あらゆる好適な名称によって識別できるので、これらの様々なチャンネル及び情報要素に割り当てている様々な名称は、いかなる点においても限定的な名称ではない。

50

## 【0118】

本開示においては、「基地局 (BS: Base Station)」、「無線基地局」、「基地局装置」、「固定局 (fixed station)」、「Node B」、「eNode B (eNB)」、「gNode B (gNB)」、「アクセスポイント (access point)」、「送信ポイント (transmission point)」、「受信ポイント (reception point)」、「送受信ポイント (transmission/reception point)」、「セル」、「セクタ」、「セルグループ」、「キャリア」、「コンポーネントキャリア」などの用語は、互換的に使用され得る。基地局は、マクロセル、スモールセル、フェムトセル、ピコセルなどの用語で呼ばれる場合もある。

## 【0119】

基地局は、1つ又は複数 (例えば、3つ) のセルを収容することができる。基地局が複数のセルを収容する場合、基地局のカバレッジエリア全体は複数のより小さいエリアに区分でき、各々のより小さいエリアは、基地局サブシステム (例えば、屋内用の小型基地局 (RRH: Remote Radio Head)) によって通信サービスを提供することもできる。「セル」又は「セクタ」という用語は、このカバレッジにおいて通信サービスを行う基地局及び基地局サブシステムの少なくとも一方のカバレッジエリアの一部又は全体を指す。

## 【0120】

本開示においては、「移動局 (MS: Mobile Station)」、「ユーザ端末 (user terminal)」、「ユーザ装置 (UE: User Equipment)」、「端末」などの用語は、互換的に使用され得る。

## 【0121】

移動局は、当業者によって、加入者局、モバイルユニット、加入者ユニット、ワイヤレスユニット、リモートユニット、モバイルデバイス、ワイヤレスデバイス、ワイヤレス通信デバイス、リモートデバイス、モバイル加入者局、アクセス端末、モバイル端末、ワイヤレス端末、リモート端末、ハンドセット、ユーザエージェント、モバイルクライアント、クライアント、又はいくつかの他の適切な用語で呼ばれる場合もある。

## 【0122】

基地局及び移動局の少なくとも一方は、送信装置、受信装置、通信装置などと呼ばれてもよい。なお、基地局及び移動局の少なくとも一方は、移動体に搭載されたデバイス、移動体自体などであってもよい。当該移動体は、乗り物 (例えば、車、飛行機など) であってもよいし、無人で動く移動体 (例えば、ドローン、自動運転車など) であってもよいし、ロボット (有人型又は無人型) であってもよい。なお、基地局及び移動局の少なくとも一方は、必ずしも通信動作時に移動しない装置も含む。例えば、基地局及び移動局の少なくとも一方は、センサなどのIoT (Internet of Things) 機器であってもよい。

## 【0123】

また、本開示における基地局は、ユーザ端末で読み替えてもよい。例えば、基地局及びユーザ端末間の通信を、複数の端末20間の通信 (例えば、D2D (Device-to-Device)、V2X (Vehicle-to-Everything) などと呼ばれてもよい) に置き換えた構成について、本開示の各態様/実施形態を適用してもよい。この場合、上述のネットワークノード30が有する機能を端末20が有する構成としてもよい。また、「上り」及び「下り」などの文言は、端末間通信に対応する文言 (例えば、「サイド (side) 」) で読み替えられてもよい。例えば、上りチャネル、下りチャネルなどは、サイドチャネルで読み替えられてもよい。

## 【0124】

同様に、本開示におけるユーザ端末は、基地局で読み替えてもよい。この場合、上述のユーザ端末が有する機能を基地局が有する構成としてもよい。

## 【0125】

本開示で使用する「判断 (determining)」、「決定 (determining)」という用語は、多種多様な動作を包含する場合がある。「判断」、「決定」は、例えば、判定 (judging)、

10

20

30

40

50

計算(calculating)、算出(computing)、処理(processing)、導出(deriving)、調査(investigating)、探索(looking up、search、inquiry) (例えば、テーブル、データベース又は別のデータ構造での探索)、確認(ascertaining)した事を「判断」「決定」したとみなす事などを含み得る。また、「判断」「決定」は、受信(receiving) (例えば、情報を受信すること)、送信(transmitting)(例えば、情報を送信すること)、入力(input)、出力(output)、アクセス(accessing) (例えば、メモリ中のデータにアクセスすること)した事を「判断」「決定」したとみなす事などを含み得る。また、「判断」「決定」は、解決(resolving)、選択(selecting)、選定(choosing)、確立(establishing)、比較(comparing)などした事を「判断」「決定」したとみなす事を含み得る。つまり、「判断」「決定」は、何らかの動作を「判断」「決定」したとみなす事を含み得る。また、「判断(決定)」は、「想定する(assuming)」、「期待する(expecting)」、「みなす(considering)」などで読み替えられてもよい。

10

## 【0126】

「接続された(connected)」、「結合された(coupled)」という用語、又はこれらのあらゆる変形は、2又はそれ以上の要素間の直接的又は間接的なあらゆる接続又は結合を意味し、互いに「接続」又は「結合」された2つの要素間に1又はそれ以上の中間要素が存在することを含むことができる。要素間の結合又は接続は、物理的なものであっても、論理的なものであっても、或いはこれらの組み合わせであってもよい。例えば、「接続」は「アクセス」で読み替えられてもよい。本開示で使用する場合、2つの要素は、1又はそれ以上の電線、ケーブル及びプリント電気接続の少なくとも一つを用いて、並びにいくつかの非限定的かつ非包括的な例として、無線周波数領域、マイクロ波領域及び光(可視及び不可視の両方)領域の波長を有する電磁エネルギーなどを用いて、互いに「接続」又は「結合」されると考えることができる。

20

## 【0127】

参照信号は、RS (Reference Signal) と略称することもでき、適用される標準によってパイロット(Pilot)と呼ばれてもよい。

## 【0128】

本開示において使用する「に基づいて」という記載は、別段に明記されていない限り、「のみに基づいて」を意味しない。言い換えれば、「に基づいて」という記載は、「のみに基づいて」と「に少なくとも基づいて」の両方を意味する。

30

## 【0129】

本開示において使用する「第1の」、「第2の」などの呼称を使用した要素へのいかなる参照も、それらの要素の量又は順序を全般的に限定しない。これらの呼称は、2つ以上の要素間を区別する便利な方法として本開示において使用され得る。したがって、第1及び第2の要素への参照は、2つの要素のみが採用され得ること、又は何らかの形で第1の要素が第2の要素に先行しなければならないことを意味しない。

## 【0130】

上記の各装置の構成における「手段」を、「部」、「回路」、「デバイス」等に置き換えてもよい。

## 【0131】

本開示において、「含む(include)」、「含んでいる(including)」及びそれらの変形が使用されている場合、これらの用語は、用語「備える(comprising)」と同様に、包括的であることが意図される。さらに、本開示において使用されている用語「又は(or)」は、排他的論理和ではないことが意図される。

40

## 【0132】

本開示において、例えば、英語でのa, an及びtheのように、翻訳により冠詞が追加された場合、本開示は、これらの冠詞の後に続く名詞が複数形であることを含んでもよい。

## 【0133】

本開示において、「AとBが異なる」という用語は、「AとBが互いに異なる」ことを意味してもよい。なお、当該用語は、「AとBがそれぞれCと異なる」ことを意味しても

50

よい。「離れる」、「結合される」などの用語も、「異なる」と同様に解釈されてもよい。

【0134】

本開示において説明した各態様／実施形態は単独で用いてもよいし、組み合わせて用いてもよいし、実行に伴って切り替えて用いてもよい。また、所定の情報の通知（例えば、「Xであること」の通知）は、明示的に行うものに限られず、暗黙的（例えば、当該所定の情報の通知を行わない）ことによって行われてもよい。

【0135】

なお、本開示におけるAFは、外部アプリケーションの一例である。NA-GUTIは、暫定識別子の一例である。

【0136】

以上、本開示について詳細に説明したが、当業者にとっては、本開示が本開示中に説明した実施形態に限定されるものではないということは明らかである。本開示は、請求の範囲の記載により定まる本開示の趣旨及び範囲を逸脱することなく修正及び変更態様として実施することができる。したがって、本開示の記載は、例示説明を目的とするものであり、本開示に対して何ら制限的な意味を有するものではない。

【符号の説明】

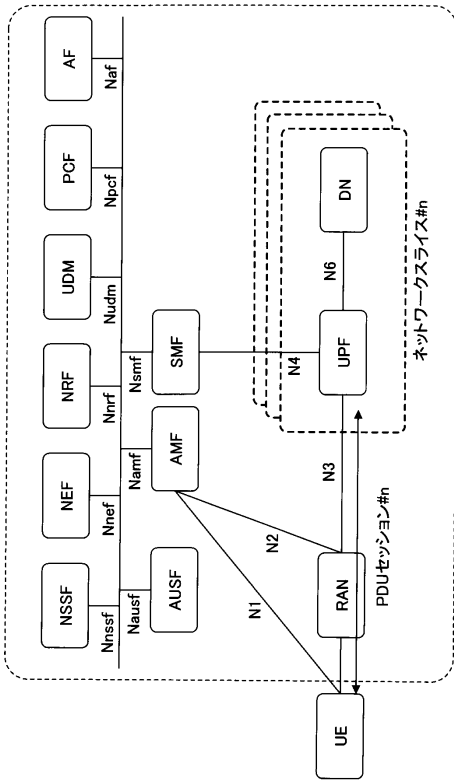
【0137】

|      |           |    |
|------|-----------|----|
| 10   | 基地局       |    |
| 110  | 送信部       |    |
| 120  | 受信部       | 20 |
| 130  | 設定部       |    |
| 140  | 制御部       |    |
| 20   | 端末        |    |
| 210  | 送信部       |    |
| 220  | 受信部       |    |
| 230  | 設定部       |    |
| 240  | 制御部       |    |
| 30   | ネットワークノード |    |
| 1001 | プロセッサ     |    |
| 1002 | 記憶装置      | 30 |
| 1003 | 補助記憶装置    |    |
| 1004 | 通信装置      |    |
| 1005 | 入力装置      |    |
| 1006 | 出力装置      |    |

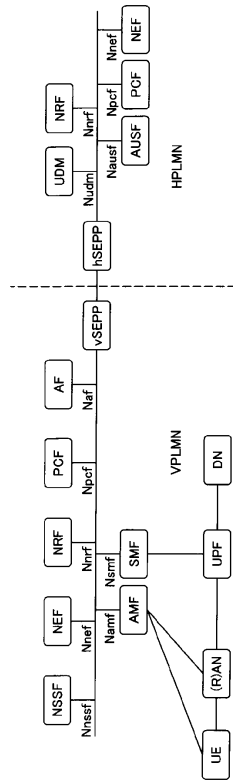
40

50

【図面】  
【図 1】



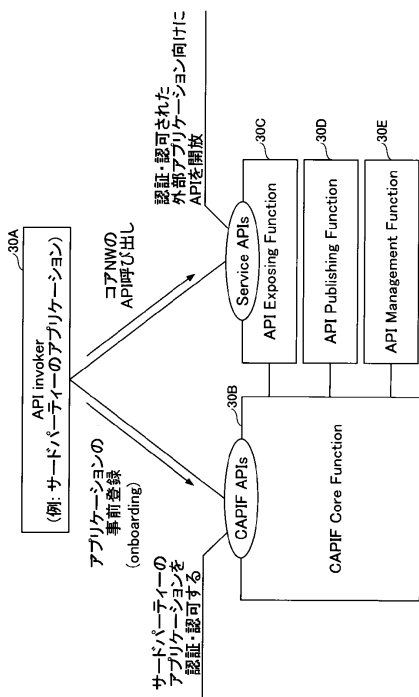
【図 2】



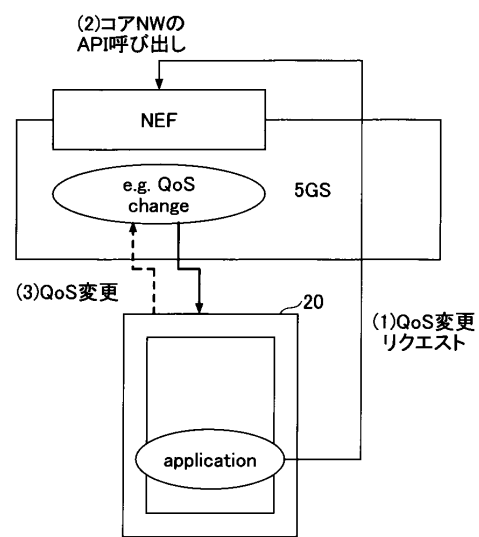
10

20

【図 3】



【図 4】

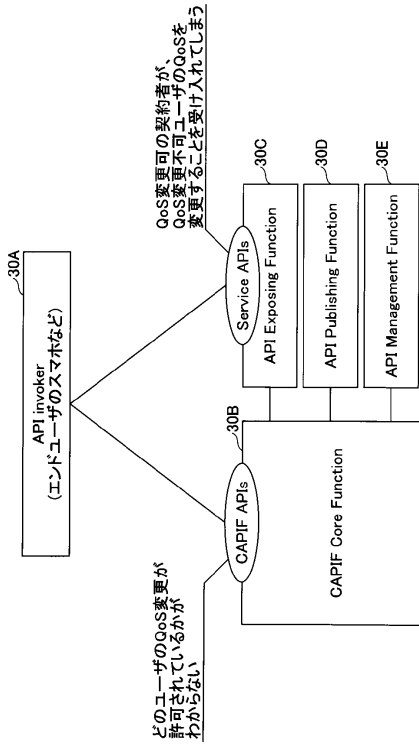


30

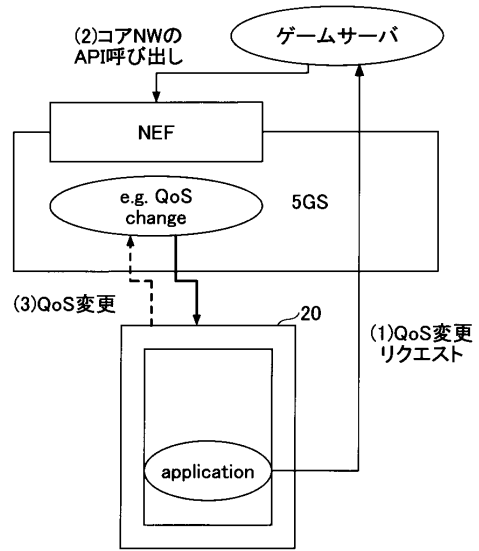
40

50

【 図 5 】



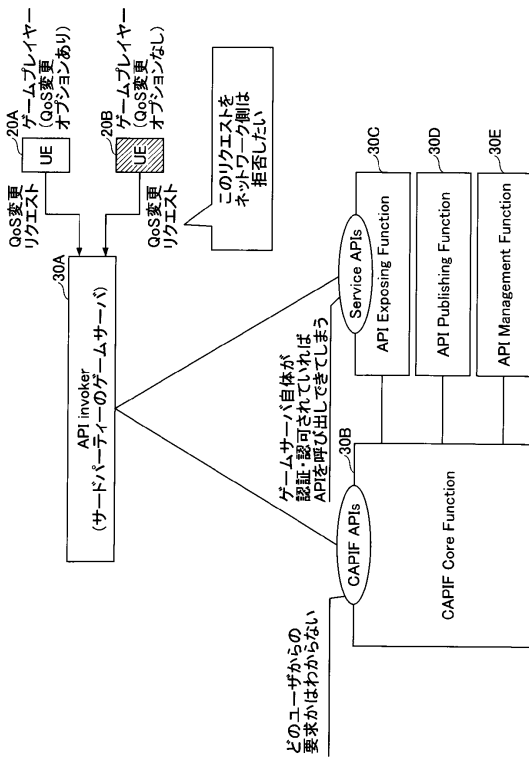
【 図 6 】



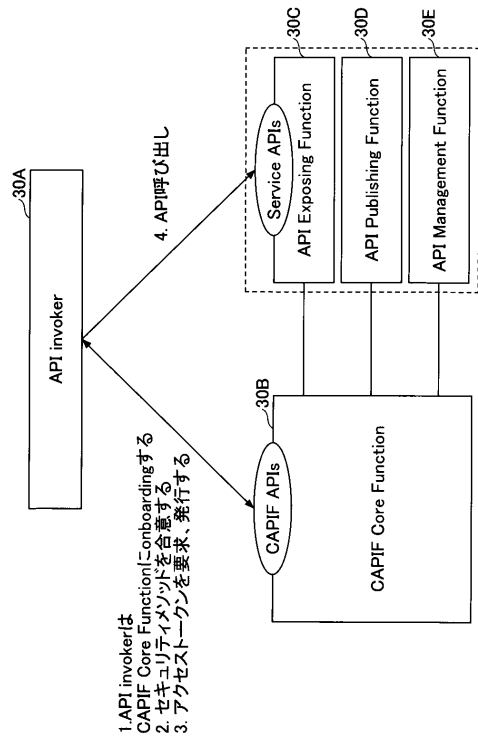
10

20

【 図 7 】



【 図 8 】

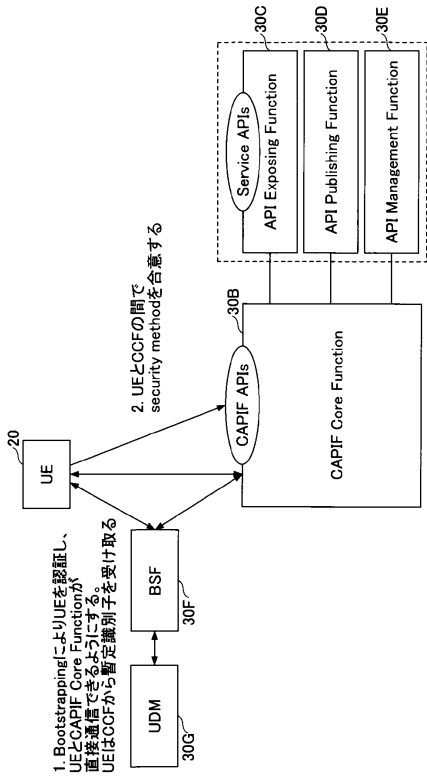


30

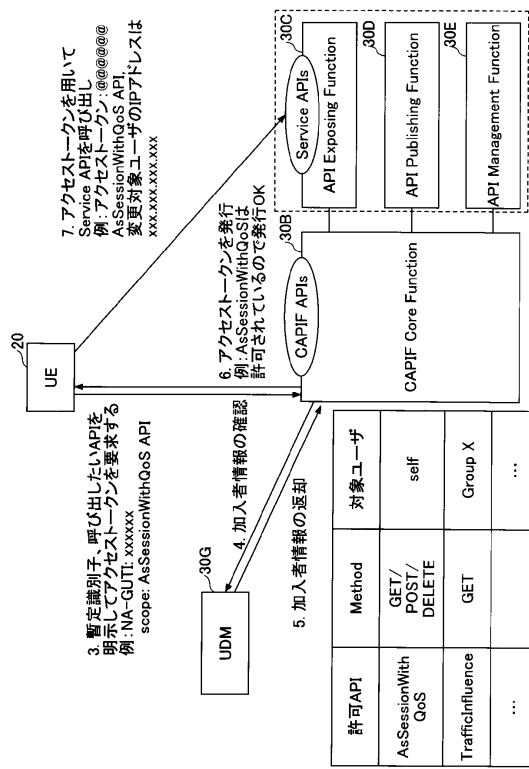
40

50

【図 9】



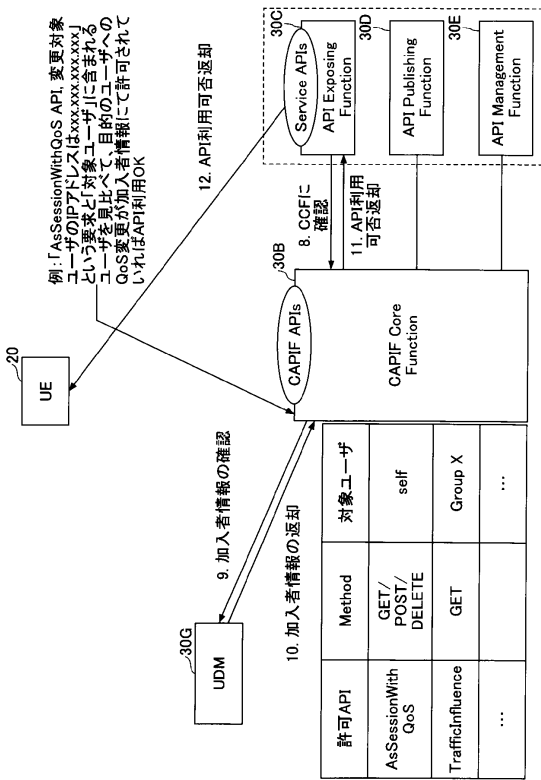
【図 10】



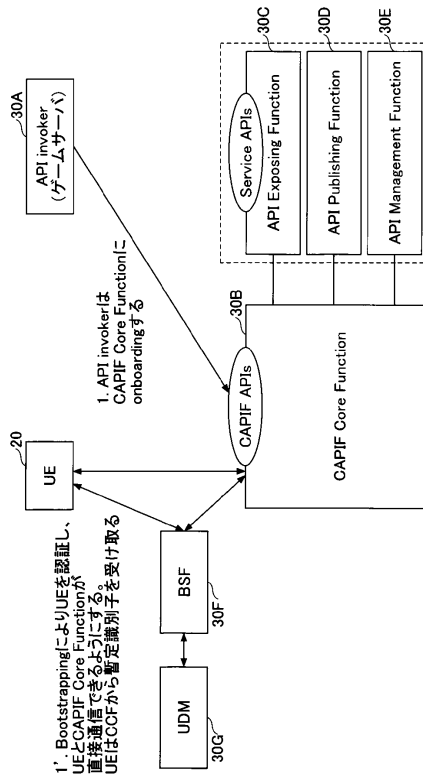
10

20

【図 11】



【図 12】

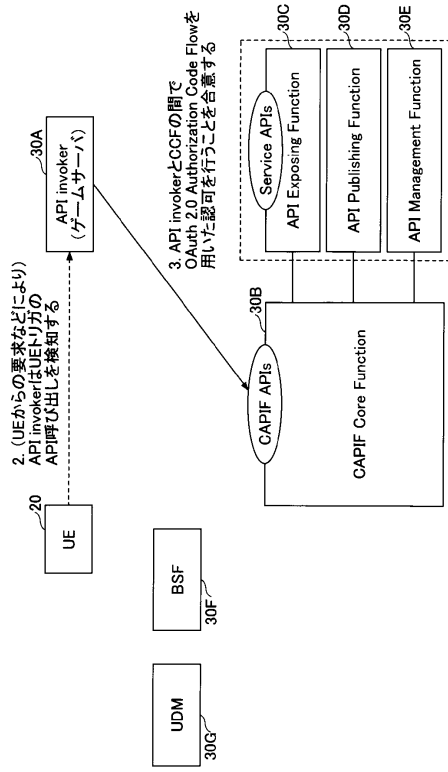


30

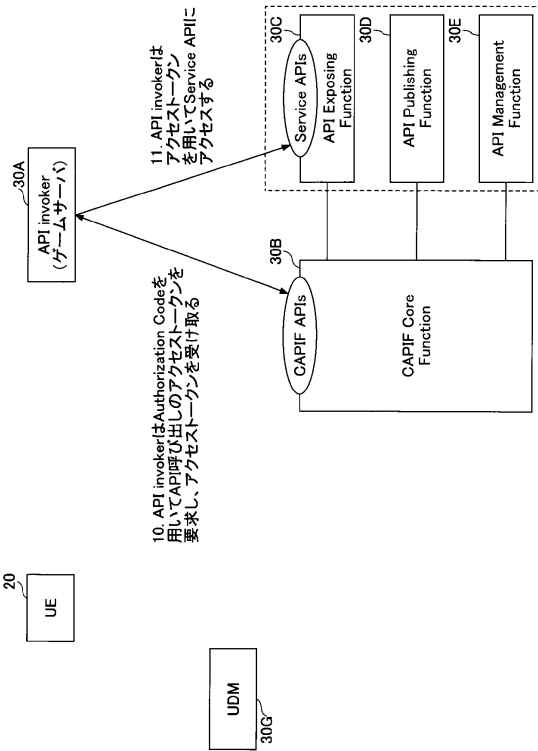
40

50

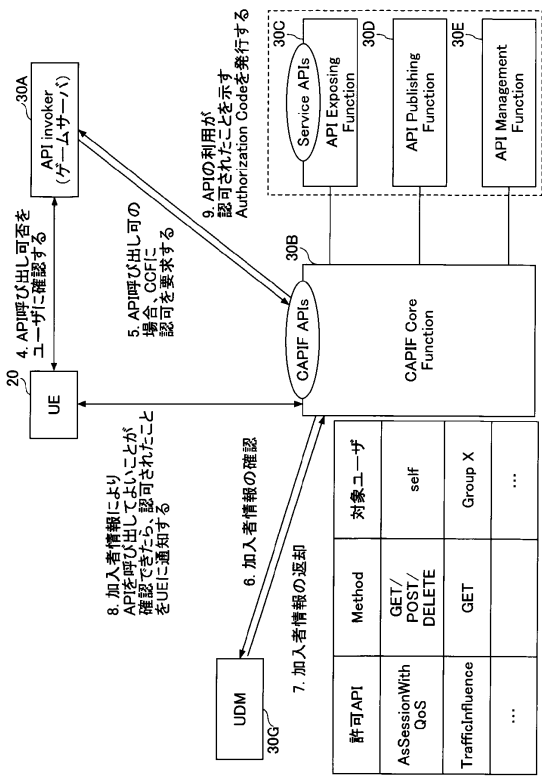
【図 1 3】



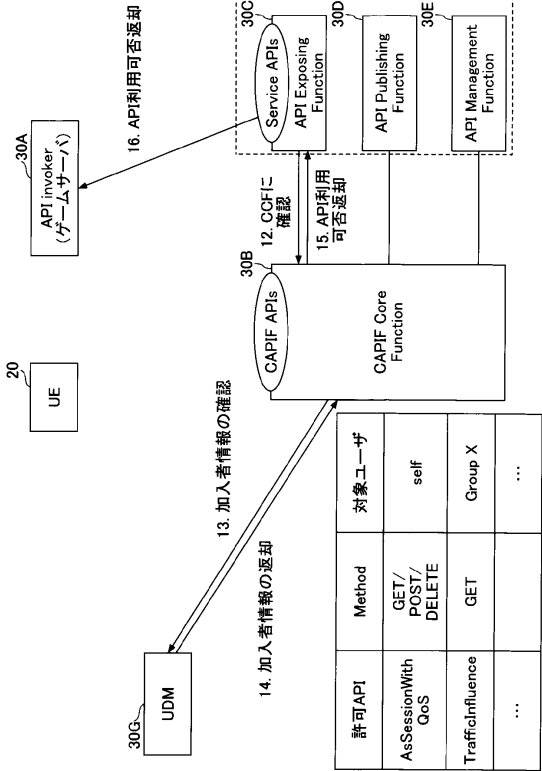
【図 1 5】



【図 1 4】



【図 1 6】



10

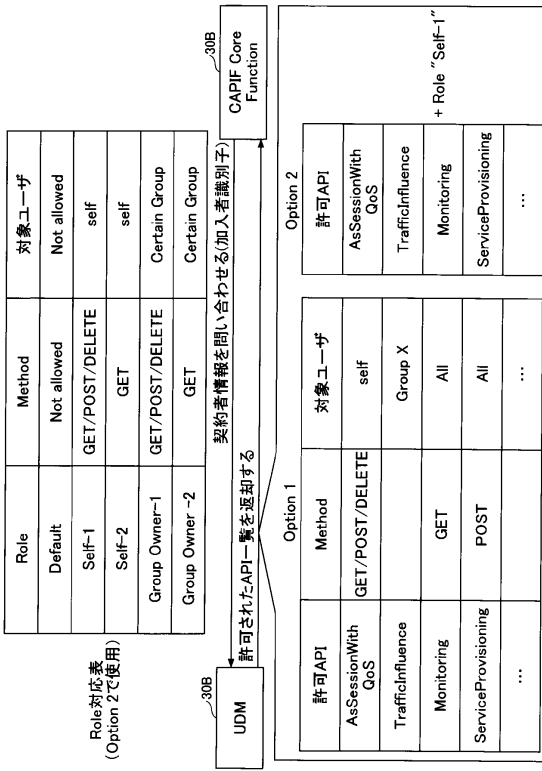
20

30

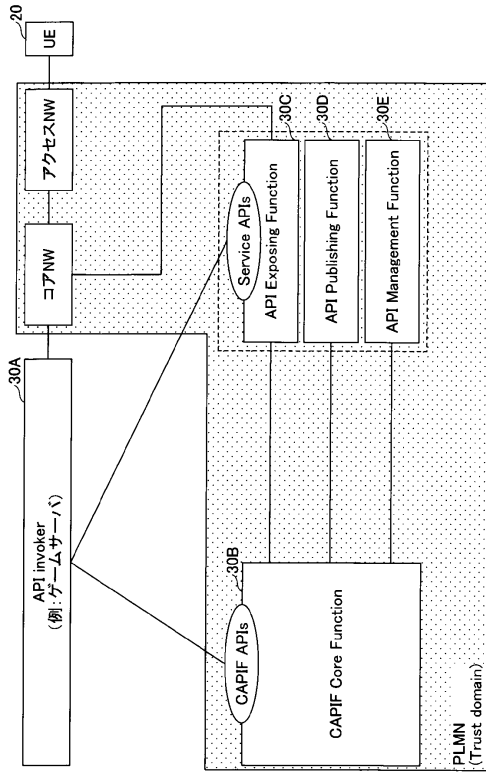
40

50

【図 17】



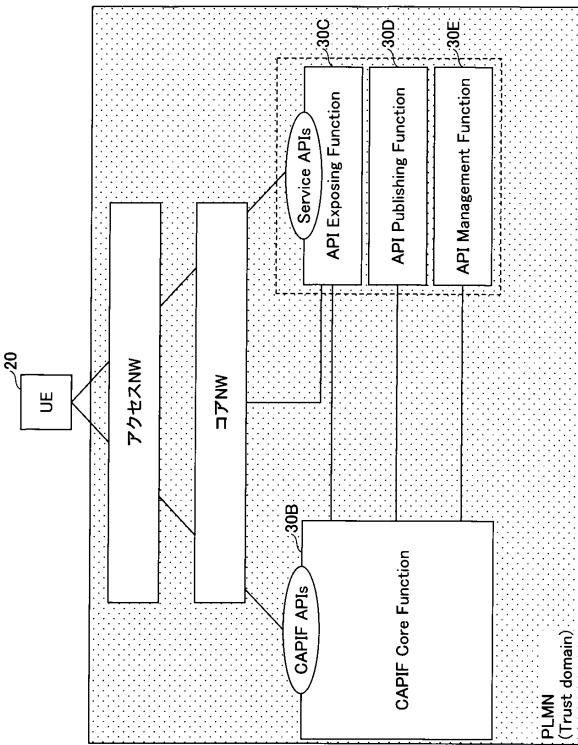
【図 18】



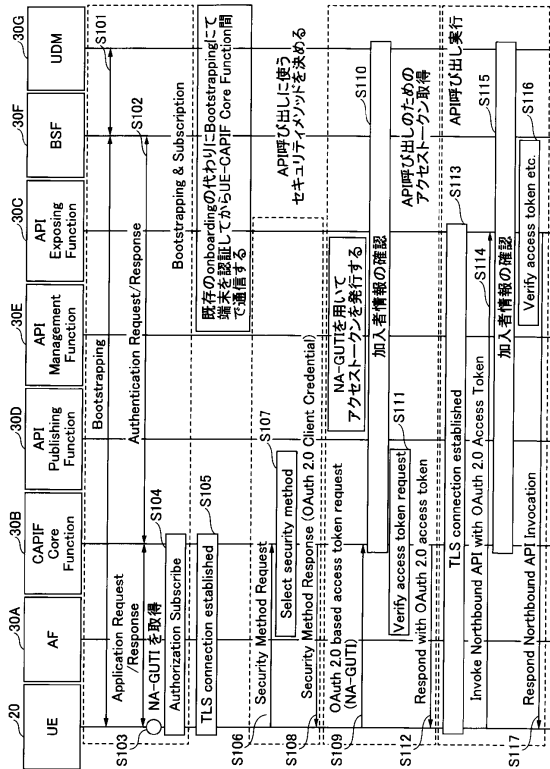
10

20

【図 19】



【図 20】

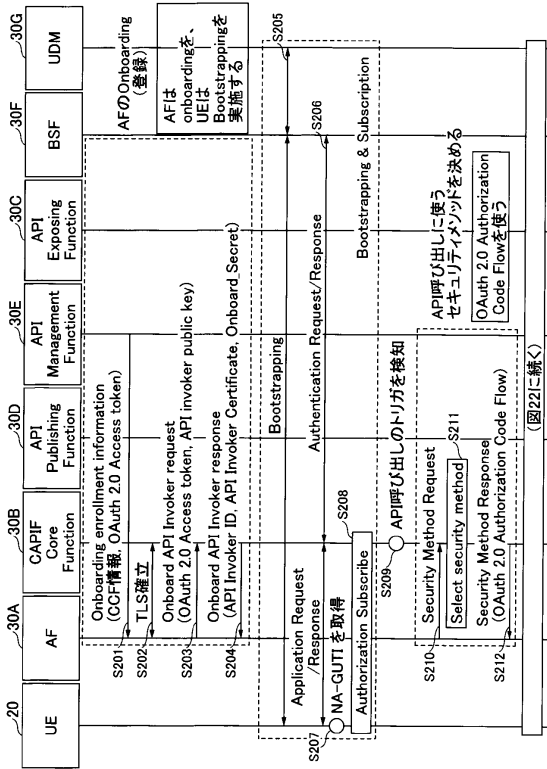


30

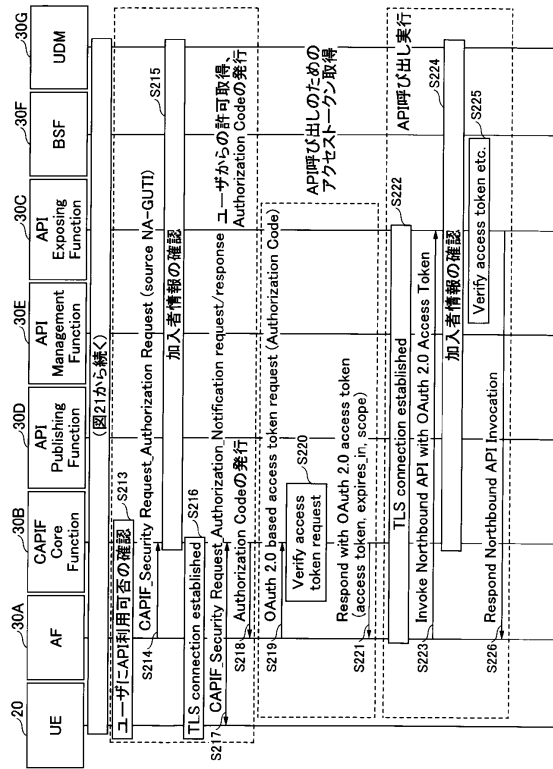
40

50

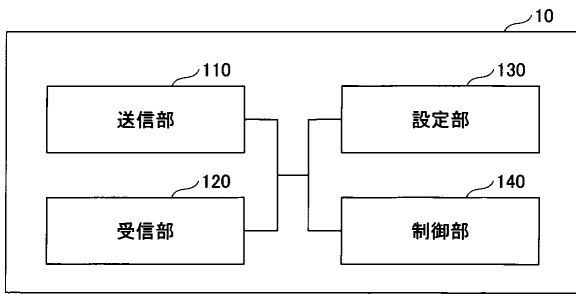
【図 2 1】



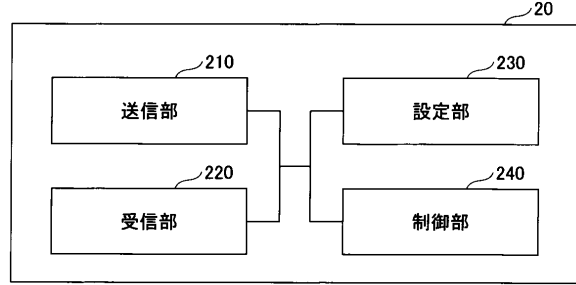
【図 2 2】



【図 2 3】



【図 2 4】



10

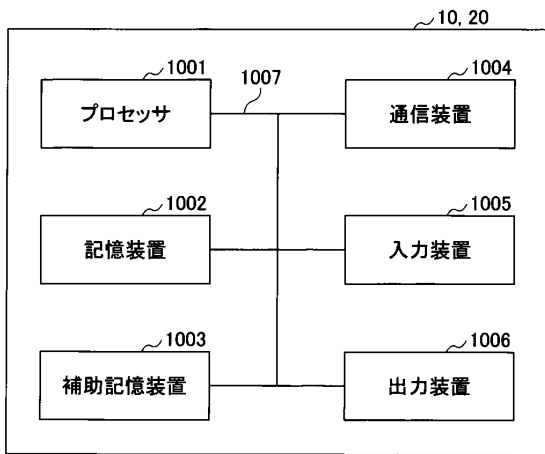
20

30

40

50

【図 25】



10

20

30

40

50

---

フロントページの続き

山王パークタワー 株式会社NTTドコモ 知的財産部内

審査官 伊東 和重

(56)参考文献 NEC, Correction/enhancement in CAPIF TS[online], 3GPP TSG SA WG3 #93, 3GPP, 2018年11月16日, S3-183341, [検索日 2024.11.19],インターネット: URL:[https://www.3gpp.org/ftp/tsg\\_sa/WG3\\_Security/TSGS3\\_93\\_Spokane/Docs/S3-183341.zip](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_93_Spokane/Docs/S3-183341.zip)

(58)調査した分野 (Int.Cl., DB名)

H 0 4 B 7 / 2 4 - 7 / 2 6

H 0 4 W 4 / 0 0 - 9 9 / 0 0

3 G P P T S G R A N W G 1 - 4

S A W G 1 - 4

C T W G 1 , 4