

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局
(43) 国際公開日
2021年7月1日(01.07.2021)



(10) 国際公開番号
WO 2021/131069 A1

- (51) 国際特許分類:
H04W 8/22 (2009.01)
- (21) 国際出願番号 : PCT/JP2019/051599
- (22) 国際出願日 : 2019年12月27日(27.12.2019)
- (25) 国際出願の言語 : 日本語
- (26) 国際公開の言語 : 日本語
- (71) 出願人:株式会社NTTドコモ(NTT DOCOMO, INC.) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目11番1号 Tokyo (JP).
- (72) 発明者:戸枝 輝朗(TOEDA Teruaki); 〒1006150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社NTTドコモ 知的財産部内 Tokyo (JP). 閔天楊(MIN Tianyang); 〒1006150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社NTTドコモ 知的財産部内 Tokyo (JP). 高橋 秀明(TAKAHASHI Hideaki); 〒1006150 東京都千代田区永田町二丁目11番1号 山王パークタワー 株式会社N

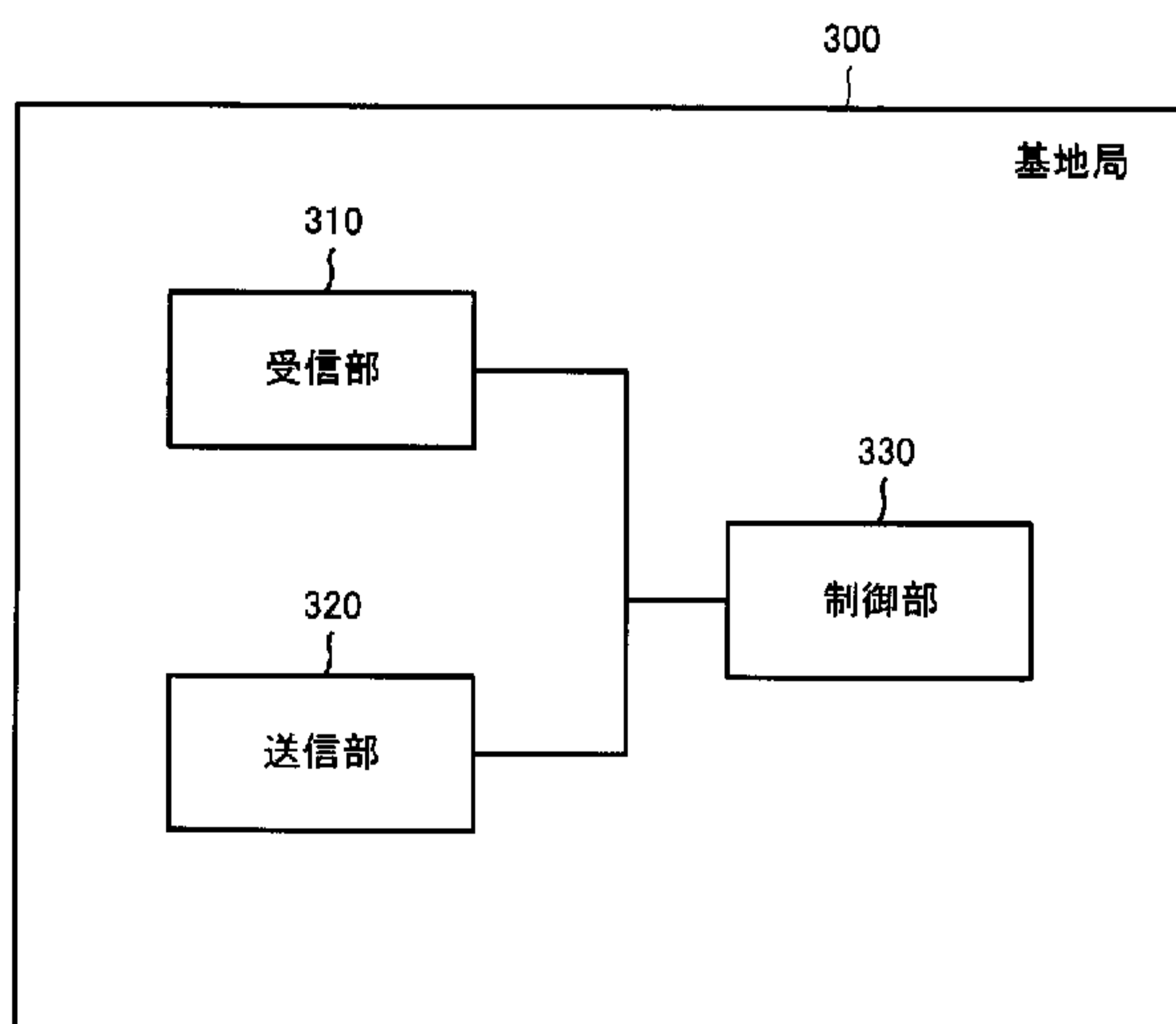
TTドコモ 知的財産部内 Tokyo (JP). ツーゲンマイヤー アルフ(ZUGENMAIER Alf); ミュンヘン市ロートストラッセ34 Munich (DE).

(74) 代理人: 三好 秀和, 外 (MIYOSHI Hidekazu et al.); 〒1050001 東京都港区虎ノ門一丁目2番8号 虎ノ門琴平タワー Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: BASE STATION AND WIRELESS COMMUNICATION METHOD

(54) 発明の名称 : 基地局及び無線通信方法



- 300 Base station
- 310 Reception unit
- 320 Transmission unit
- 330 Control unit

(57) Abstract: This base station is provided with: a reception unit that receives a terminal capability from a terminal before a security procedure; and a control unit that, in accordance with release of a terminal context regarding the terminal, deletes the terminal capability acquired before the security procedure.

(57) 要約: 基地局は、セキュリティ手順前に端末能力を端末から受信する受信部と、前記端末に関する端末コンテキストの解放に応じて、前記セキュリティ手順前に取得した前記端末能力を削除する制御部と、を備える。

WO 2021/131069 A1

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類 :

一 国際調査報告 (条約第21条(3))

明 細 書

発明の名称： 基地局及び無線通信方法

技術分野

[0001] 本発明は、セキュリティ手順前に取得した端末能力を処理する基地局及び無線通信方法に関する。

背景技術

[0002] 3rd Generation Partnership Project (3GPP) は、Long Term Evolution (LTE) を仕様化し、LTEのさらなる高速化を目的としてLTE-Advanced (以下、LTE-Advancedを含めてLTEという)、さらに、5th generation mobile communication system (以下、5G、New Radio (NR) 又はNext Generation (NG) とも呼ばれる) の仕様化も進められている。さらに、5G以降の移動通信方式の仕様化も進められている (6Gやbeyond 5Gなどと呼称される場合もあるが、これらの呼称に限られない)。

[0003] LTE及びNRでは、UEと基地局との間のセキュリティ手順の活性化前に取得したUE capabilityについて、コアネットワーク (例えば、EPC; Enhanced Packet Core、5GC; 5G Core) が取り扱う方法が合意された。具体的には、コアネットワークは、非認証緊急呼を除いて、セキュリティ手順前に取得したUE capabilityを後の利用のためにローカルに保存せず、他のネットワークエンティティ又はネットワークファンクションに送信しない旨が合意された (例えば、非特許文献1, 2)。

先行技術文献

非特許文献

[0004] 非特許文献1: “Security of RRC UE capability transfer procedure in EPS”, S3-192861, 3GPP TSG-SA WG3 Meeting #96, 2019年8月

非特許文献2: “Security of RRC UE capability transfer procedure in 5G S”, S3-192862, 3GPP TSG-SA WG3 Meeting #96, 2019年8月

発明の概要

[0005] 上述した技術では、コアネットワークにおける扱いが合意されたに過ぎず、このような合意を遵守するためのアクセスネットワーク（RAN; Radio Access Network又はAN; Access Network）の動作が明らかになっていない。従って、セキュリティ手順前に取得したUE capabilityを適切に扱うことができない可能性がある。

[0006] 第1の態様は、基地局は、セキュリティ手順前に端末能力を端末から受信する受信部と、前記端末に関する端末コンテキストの解放に応じて、前記セキュリティ手順前に取得した前記端末能力を削除する制御部と、を備えることを要旨とする。

[0007] 第2の態様は、無線通信方法であって、セキュリティ手順前に端末能力を端末から受信するステップと、前記端末に関する端末コンテキストの解放に応じて、前記セキュリティ手順前に取得した前記端末能力を削除するステップと、を備えることを要旨とする。

図面の簡単な説明

[0008] [図1]図1は、無線通信システム10の全体概略構成図である。

[図2]図2は、実施形態に係るUE200を示す図である。

[図3]図3は、実施形態に係る基地局300を示す図である。

[図4]図4は、実施形態に係るコアネットワークの動作を説明するための図である。

[図5]図5は、実施形態に係る前提動作を説明するための図である。

[図6]図6は、実施形態に係る動作例1を説明するための図である。

[図7]図7は、実施形態に係る動作例2-1を説明するための図である。

[図8]図8は、実施形態に係る動作例2-1を説明するための図である。

[図9]図9は、実施形態に係る動作例2-2を説明するための図である。

[図10]図10は、実施形態に係る動作例2-2を説明するための図である。

[図11]図11は、実施形態に係る動作例3を説明するための図である。

[図12]図12は、実施形態に係る動作例3を説明するための図である。

[図13]図13は、実施形態に係る動作例3を説明するための図である。

[図14]図14は、実施形態に係るUE200又は基地局300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

[0009] 以下、実施形態を図面に基づいて説明する。なお、同一の機能や構成には、同一又は類似の符号を付して、その説明を適宜省略する。

[0010] [実施形態]

(1) 無線通信システムの全体概略構成

図1は、実施形態に係る無線通信システム100の全体概略構成図である。無線通信システム100は、Long Term Evolution (LTE) 及び5G New Radio (NR) に従った無線通信システムである。なお、LTEは4Gと呼ばれてもよいし、NRは、5Gと呼ばれてもよい。LTE及びNRは、無線アクセス技術 (RAT) と解釈されてもよく、実施形態では、LTEは、第1無線アクセス技術と呼ばれ、NRは、第2無線アクセス技術と呼ばれてもよい。NRは、5G以降の無線アクセス技術も含まれると考えてもよい。

[0011] 無線通信システム100は、Evolved Universal Terrestrial Radio Access Network 110 (以下、E-UTRAN110)、Next Generation-Radio Access Network 120 (以下、NG RAN120)、及びコアネットワーク130を含む。無線通信システム100は、端末200を含む。

[0012] E-UTRAN110は、LTEに従った基地局であるeNB111を含む。eNB111は、1以上のセルを有する。E-UTRAN110は、2以上のeNB111を含んでもよい。

[0013] NG RAN120は、5G (NR) に従った基地局であるgNB121を含む。gNB121は、1以上のセルを有する。NG RAN120は、2以上のgNB121を含んでもよい。

[0014] 「セル」という用語は、eNB111又はgNB121が有する機能、すなわち、端末200と通信を行う機能の意味で用いられてもよい。「セル」という用語は、eNB111又はgNB121のカバレッジエリアの意味で用いられてもよい。各セルは、各セルで使用する周波数によって区別されてもよい。E-UTRAN110及びNG RAN120 (eNB111又はgNB121でもよい) は、単に無線アクセスネットワークと呼ばれてもよく、アクセスネットワークと呼ばれてもよい。

- [0015] eNB111、gNB121及び端末200は、複数のコンポーネントキャリア（CC）を用いるキャリアアグリゲーション（CA）に対応していてもよく、複数のNG-RAN Nodeと端末200との間においてコンポーネントキャリアを同時送信するデュアルコネクティビティ（DC）に対応してもよい。
- [0016] eNB111、gNB121及び端末200は、無線ベアラを介して無線通信を実行する。無線ベアラは、Signaling Radio Bearer（SRB）及びData Radio Bearer（DRB）を含んでもよい。
- [0017] 端末200は、特に限定されるものではないが、「移動局（Mobile Station：MS）」、「ユーザ端末（User Equipment：UE）」と呼ばれてもよい。以下においては、端末200についてUE200と称する。
- [0018] コアネットワーク130は、LTEに従ったEPC（Evolved Packet Core）及び5G（NR）に従った5G Coreを含む。EPCは、LTEに従ったネットワークノード131（例えば、MME；Mobility Management Entity）を含む。5G Coreは、5G（NR）に従ったネットワークノード132（例えば、AMF（Access and Mobility Management Function））を含む。MME及びAMFは、control planeに関する処理を実行するネットワークノードである。ノードは、ファンクションと称されてもよい。
- [0019] ここで、eNB111とMMEとの間のインタフェース及びgNB121とMMEとの間のインタフェースはS1インタフェースと称されてもよい。gNB121とAMFとの間のインタフェースは、NGインタフェース又はN2インタフェースと称されてもよい。eNB111とeNB111との間のインタフェース及びeNB111とgNB121との間のインタフェースは、X2インタフェースと称されてもよい。gNB121とgNB121との間のインタフェースは、Xnインタフェースと称されてもよい。MMEとAMFとの間のインタフェースは、N26インタフェースと称されてもよい。
- [0020] （2） 端末の機能ブロック構成

図2は、実施形態に係るUE200の機能ブロック構成を示す図である。図2に示すように、UE200は、受信部210と、送信部220と、制御部230と、を備える。

[0021] 受信部210は、ネットワーク（例えば、eNB111又はgNB121）から各種情報を受信する。例えば、受信部210は、RRCコネクションの設定手順で用いるメッセージ（例えば、RRC Connection Setup）、端末能力転送手順で用いるメッセージ（例えば、UE Capability Enquiry）、セキュリティ手順で用いるメッセージ（例えば、Security Mode Command）を受信してもよい。

[0022] ここでは、LTEに従ったメッセージについて例示しているが、受信部210は、5G（NR）に従ったメッセージを受信してもよい。このようなケースにおいて、LTEに従ったメッセージの名称は、必要に応じて5G（NR）に従ったメッセージの名称と読み替えられてもよい。

[0023] 送信部220は、ネットワーク（例えば、eNB111又はgNB121）に各種情報を送信する。例えば、送信部220は、RRCコネクションの設定手順で用いるメッセージ（例えば、RRC Connection Request）、端末能力転送手順で用いるメッセージ（例えば、UE Capability Information）、セキュリティ手順で用いるメッセージ（例えば、Security Mode Complete）を送信してもよい。

[0024] ここでは、LTEに従ったメッセージについて例示しているが、送信部220は、5G（NR）に従ったメッセージを受信してもよい。このようなケースにおいて、LTEに従ったメッセージの名称（例えば、RRC Connection Setupは、必要に応じて5G（NR）に従ったメッセージの名称（例えば、RRC Setup Request）と読み替えられてもよい。

[0025] 制御部230は、UE200の動作を制御する。例えば、制御部230は、セル（再）選択で用いる測定報告を実行してもよい。セル（再）選択は、基地局間のハンドオーバを伴ってもよい。制御部230は、セキュリティ手順前に実行される非認証緊急呼に関してもよい。

[0026] （3）基地局の機能ブロック構成

図3は、実施形態に係る基地局300の機能ブロック構成を示す図である。実施形態では、上述したeNB111及びgNB121は同様の構成を有し得る。従って、これらを区別せずに基地局300について説明する。図3に示すように、基地局300は、受信部310と、送信部320と、制御部330と、を備える。

- [0027] 受信部310は、UE200から各種情報を受信する。例えば、受信部310は、RRCコネクションの設定手順で用いるメッセージ（例えば、RRC Connection Request）、端末能力転送手順で用いるメッセージ（例えば、UE Capability Information）、セキュリティ手順で用いるメッセージ（例えば、Security Mode Complete）を受信してもよい。
- [0028] 受信部310は、上位ノードから各種情報を受信する。例えば、受信部310は、S1コネクション設定手順で用いるメッセージ（例えば、Initial context Setup Request）を受信してもよい。
- [0029] ここでは、LTEに従ったメッセージについて例示しているが、受信部310は、5G（NR）に従ったメッセージを受信してもよい。このようなケースにおいて、LTEに従ったメッセージの名称は、必要に応じて5G（NR）に従ったメッセージの名称と読み替えられてもよい。
- [0030] 送信部320は、UE200に各種情報を送信する。例えば、送信部320は、RRCコネクションの設定手順で用いるメッセージ（例えば、RRC Connection Setup）、端末能力転送手順で用いるメッセージ（例えば、UE Capability Enquiry）、セキュリティ手順で用いるメッセージ（例えば、Security Mode Command）を送信してもよい。
- [0031] 送信部320は、上位ノードに各種情報を送信する。上位ノードは、上述したMME及びAMFのいずれかを含む。例えば、送信部320は、S1コネクション設定手順で用いるメッセージ（例えば、UE Capability Info Indication）を送信してもよい。
- [0032] ここでは、LTEに従ったメッセージについて例示しているが、受信部310は、5G（NR）に従ったメッセージを受信してもよい。このようなケースにおいて、LTEに従ったメッセージの名称（例えば、UE Capability Info Indication）は、必要に応じて5G（NR）に従ったメッセージの名称（例えば、UE Radio Capability Info Indication）と読み替えられてもよい。
- [0033] 制御部330は、基地局300の動作を制御する。例えば、制御部330は、セル（再）選択及びハンドオーバーに関する制御を実行する。

[0034] 実施形態では、制御部330は、UE200の端末能力（以下、UE capability）の扱いに関するネットワークの動作に従ってUE capabilityを扱う。具体的には、UE capabilityに関するネットワークの動作としては、図4に示すバリエーションが考えられる。

[0035] 図4において、“Store”は、ネットワーク内においてUE capabilityを保持することを意味する。“Send”は、ネットワーク内においてUE capabilityを他ノードに送信することを意味する。“Secured”は、セキュリティ手順後にUE capabilityが基地局300によって取得されることを意味する。“Not secured”は、セキュリティ手順前にUE capabilityが基地局300によって取得されることを意味する。“Allowed”は、コアネットワークの上位ノードにおいて“Store”又は“Send”が許可されることを意味する。“Prohibited”は、コアネットワークの上位ノードにおいて“Store”又は“Send”が禁止されることを意味する。

[0036] このような背景下において、セキュリティ手順後に取得されたUE capabilityについては、“Store”及び“Send”の双方が許可されており、従来の手順に対して基地局300に特別な動作が要求されない。同様に、セキュリティ手順前に取得されたUE capabilityについて“Store”が許可される場合には、従来の手順に対して基地局300に特別な動作が要求されない。従って、これらの動作に関する説明については省略する。

[0037] すなわち、実施形態では、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityについて“Store”が禁止されるケースにおける基地局300の動作（動作例1）、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityについて“Send”が禁止されるケースにおける基地局300の動作（動作例2）、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityについて“Send”が許可されるケースにおける基地局300の動作（動作例3）について説明する。

[0038] （4）前提動作

以下において、上述した動作例1～3の前提動作について説明する。図5

は、実施形態に係る前提動作を示す図である。ここでは、LTEに従った動作について主として説明するが、5G (NR) に従った動作についても同様である。以下においては、上述したMME及びAMFを総称して上位ノード400と称する。

[0039] 図5に示すように、ステップS10において、UE200と基地局300との間でRACH procedureが実行される。RACH procedureは、UE200から基地局300に対するRACH preambleの送信によって、UE200と基地局300との間の同期などを確立する手順である。

[0040] ステップS11において、UE200は、RRC Connection Requestを基地局300に送信し、ステップS12において、基地局300は、RRC Connection SetupをUE200に送信し、ステップS13において、UE200は、RRC Connection Setup Completeを基地局300に送信する。これらの手順は、RRCコネクション設定手順と称されてもよい (TS36.331 v15.7.0 第5.3.3章又はTS36.331 v15.7.0 第5.3.3章を参照)。

[0041] ステップS14において、基地局300は、Initial UE messageを上位ノード400に送信する。ステップS15において、上位ノード400は、Initial Context Setup Requestを基地局300に送信する。ステップS15の動作は、S1コネクションの設定を開始する動作である (TS36.413 v15.7.1 第8.3章、TS38.413 v15.5.0 第8.3章)。

[0042] ステップS16において、基地局300は、UE Capability EnquiryをUE200に送信する。ステップS17において、UE200は、UE Capability Informationを基地局300に送信する。UE Capability Informationは、少なくともUE200のUE Capabilityを含む。これらの手順は、UE Capability転送手順と称されてもよい (TS36.331 v15.7.0 第5.6.3章又はTS36.331 v15.7.0 第5.6.1章を参照)。

[0043] ステップS18において、基地局300は、UE Capability Info Indicationを上位ノード400に送信する。UE Capability Info Indicationは、少なくともUE200のUE Capabilityを含む (TS36.413 v15.7.1 第8.9章、TS38.413 v15.5.0 第8.14.1章)。

[0044] ステップS19において、基地局300は、Security Mode CommandをUE200に送

信し、ステップS20において、基地局300は、RRC Connection ReconfigurationをUE200に送信する。ステップS21において、UE200は、Security Mode Completeを基地局300に送信し、ステップS22において、UE200は、RRC Connection Reconfiguration Completeを基地局300に送信する。ステップS19及びステップS20の処理は、セキュリティ手順と称されてもよい（TS36.331 v15.7.0 第5.3.4章又はTS36.331 v15.7.0 第5.3.4章を参照）。セキュリティ手順は、AS (Access-Stratum) セキュリティ手順と称されてもよい。

[0045] ステップS23において、基地局300は、Initial Context Setup Responseを上位ノード400に送信する。ステップS23の動作は、S1コネクションの設定を完了する動作である（TS36.413 v15.7.1 第8.3章、TS38.413 v15.5.0 第8.3章）。

[0046] このように、実施形態では、UE CapabilityがUE200と基地局300との間のセキュリティ手順前に取得されるケースを前提とする。

[0047] (5) 動作例1

以下において、実施形態に係る動作例1について説明する。上述したように、動作例1は、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityについて”Store”が禁止されるケースにおける基地局300の動作である。

[0048] 図6に示すように、ステップS30において、基地局300は、セキュリティ手順前にUE capabilityを送信したUE200に関するUE contextの解放を検出する。UE contextの解放は、セキュリティ手順前にUE capabilityを送信したUE200がRRC ConnectedからRRC Idle又はRRC Inactiveに遷移するときに検出されてもよい。UE contextの解放は、セキュリティ手順前にUE capabilityを送信したUE200がハンドオーバーを行うときに検出されてもよい。UE contextの解放は、セキュリティ手順前にUE capabilityを送信したUE200がセル再選択を行うときに検出されてもよい。UE contextの解放は、UE capabilityを送信したUE200の無線品質劣化時（UE200からRadio Link Failureが通知されたとき、若しくは基地局がUE200をRadio Link Failureと判定したときなど）を行うと

きに検出されてもよい

ステップS31において、基地局300は、セキュリティ手順前に取得したUE Capabilityを削除する。言い換えると、基地局300は、セキュリティ手順前にUE capabilityを送信したUE200がRRC Connectedである間においてUE capabilityを保持し、UE200がRRC Idle又はRRC Inactiveに遷移したときにUE capabilityを削除する。

[0049] ここで、セキュリティ手順前に取得されたUE capabilityは、非認証緊急呼以外の場合に取得したUE capabilityであってもよい。セキュリティ手順前に取得されたUE capabilityは、狭帯域を利用するUE200（例えば、NB（Narrow Band）IoT UE）に関するUE capabilityであってもよい。すなわち、基地局300は、セキュリティ手順前に取得されたUE capabilityが非認証緊急呼以外の場合に取得したものである場合に、S31の処理を実行してもよい。基地局300は、セキュリティ手順前に取得されたUE capabilityが狭帯域を利用するUE200（例えば、NB IoT UE）に関するUE capabilityである場合に、S31の処理を実行してもよい。

[0050] このような構成によれば、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityを後の利用のために保持することが禁止されているケースにおいて、基地局300がUE capabilityを保持し続けてしまう事態を抑制することができる。

[0051] なお、基地局300は、セキュリティ手順後にUE capabilityをUE200から受信してもよい。このようなケースにおいて、基地局300は、UE contextの解放された場合であっても、セキュリティ手順後に取得されたUE capabilityを削除せずに保持してもよい。

[0052] （6）動作例2

以下において、実施形態に係る動作例2について説明する。上述したように、動作例2は、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityについて” Send” が禁止されるケースにおける基地局300の動作である。このような基地局300の動作としては、以下に示す動作例2-1及び動

作例 2 - 2 が考えられる。

[0053] (動作例 2 - 1)

以下において、動作例 2 - 1 について説明する。動作例 2 - 1 では、セキュリティ手順前に UE capability を送信した UE200 がハンドオーバを行うケースについて例示する。

[0054] 図 7 に示すように、ステップ S41 において、基地局 300 は、ハンドオーバに関連するメッセージを上位ノード 400 に送信する。ハンドオーバに関連するメッセージは、Handover Preparation Information Message を含んでもよい。ここで、Handover Preparation Information Message は、セキュリティ手順前に取得された UE capability を含まない。すなわち、ステップ S41 において、基地局 300 は、セキュリティ手順前に取得された UE capability を含まないメッセージを上位ノード 400 に送信する。

[0055] ハンドオーバに関連するメッセージは、S1 インタフェースで用いる HANDOVER REQUIRED、HANDOVER REQUEST (TS36.413 v15.7.1 第 8.4 章を参照) を含んでもよく、N2 インタフェースで用いる HANDOVER REQUIRED、HANDOVER REQUEST (TS38.413 v15.5.0 第 8.4 章を参照) を含んでもよい。ハンドオーバに関連するメッセージは、X2 インタフェースで用いる HANDOVER REQUEST、RETRIEVE UE CONTEXT RESPONSE (TS36.423 v15.7.0 第 8.2 章、第 8.3 章) を含んでもよく、Xn インタフェースで用いる HANDOVER REQUEST、RETRIEVE UE CONTEXT RESPONSE (TS38.423 v15.5.0 第 8.2 章) を含んでもよい。

[0056] 例えば、Handover Preparation Information Message は、図 8 に示す UE-CapabilityRAT-ContainerList information element を含んでもよい。このようなケースにおいて、基地局 300 は、UE-CapabilityRAT-ContainerList のシーケンス長 (SIZE) に "0" をセットすることによって、セキュリティ手順前に取得された UE capability を含まないメッセージを上位ノード 400 に送信してもよい。このようなシーケンス長 (SIZE) が "0" に設定された情報要素は、セキュリティ手順前に取得された UE capability を含まない旨を示す情報要素の一例である。

[0057] ここで、セキュリティ手順前に取得されたUE capabilityは、非認証緊急呼以外の場合に取得したUE capabilityであってもよい。セキュリティ手順前に取得されたUE capabilityは、狭帯域を利用するUE200（例えば、NB IoT UE）に関するUE capabilityであってもよい。すなわち、基地局300は、セキュリティ手順前に取得されたUE capabilityが非認証緊急呼以外の場合に取得したものである場合に、S41の処理を実行してもよい。基地局300は、セキュリティ手順前に取得されたUE capabilityが狭帯域を利用するUE200（例えば、NB IoT UE）に関するUE capabilityである場合に、S41の処理を実行してもよい。

[0058] このような構成によれば、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityを送信することが禁止されているケースにおいて、セキュリティ手順前に取得されたUE capabilityが基地局300から送信される事態を回避することができる。

[0059] なお、基地局300は、セキュリティ手順後にUE capabilityをUE200から受信してもよい。このようなケースにおいて、基地局300は、セキュリティ手順後に取得されたUE capabilityを含むメッセージを上位ノード400に送信してもよい。

[0060] （動作例2-2）

以下において、動作例2-2について説明する。動作例2-2では、セキュリティ手順前にUE capabilityを送信したUE200がハンドオーバーを行うケースについて例示する。

[0061] 図9に示すように、ステップS42において、基地局300は、ハンドオーバーに関連するメッセージを上位ノード400に送信する。ハンドオーバーに関連するメッセージは、Handover Preparation Information Messageを含んでもよい。ここで、Handover Preparation Information Messageは、セキュリティ手順前に取得されたUE capabilityに加えて、UE capabilityが無効である旨を示す情報要素を含む。すなわち、ステップS42において、基地局300は、セキュリティ手順前に取得されたUE capabilityが無効である旨を示す情報要素と

もにUE capabilityを含むメッセージを上位ノード400に送信する。

[0062] 例えば、Handover Preparation Information Messageは、図10に示すように、“invalidUECapability”という情報要素を含んでもよい。“invalidUECapability”は、セキュリティ手順前に取得されたUE capabilityが無効である旨を示す情報要素の一例である。なお、図10では、NB IoT UEに関するHandover Preparation Information Messageが例示されている。

[0063] ここで、セキュリティ手順前に取得されたUE capabilityは、非認証緊急呼以外の場合に取得したUE capabilityであってもよい。セキュリティ手順前に取得されたUE capabilityは、狭帯域を利用するUE200（例えば、NB IoT UE）に関するUE capabilityであってもよい。すなわち、基地局300は、セキュリティ手順前に取得されたUE capabilityが非認証緊急呼以外の場合に取得したものである場合に、S42の処理を実行してもよい。基地局300は、セキュリティ手順前に取得されたUE capabilityが狭帯域を利用するUE200（例えば、NB IoT UE）に関するUE capabilityである場合に、S42の処理を実行してもよい。

[0064] このような構成によれば、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityを送信することが禁止されているケースにおいて、セキュリティ手順前に取得されたUE capabilityが基地局300から送信されたとしても、ネットワークでUE capabilityが無効であることを把握することができ、ネットワークにおいてUE capabilityを送信しない等の対応を実行することができる。

[0065] さらに、UE capabilityの送信が必須であると定められた既存のUEであっても、UE capabilityが無効である旨を示す情報要素を追加すればよいため、上述した動作例2-1と比べて既存のUEの動作変更に係る負荷を軽減することができる。

[0066] なお、基地局300は、セキュリティ手順後にUE capabilityをUE200から受信してもよい。このようなケースにおいて、基地局300は、セキュリティ手順後に取得されたUE capabilityを含むメッセージを上位ノード400に送信しても

よい。

[0067] (7) 動作例3

以下において、実施形態に係る動作例3について説明する。上述したように、動作例3は、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityについて” Send” が許可されるケースにおける基地局300の動作である。

[0068] 図11に示すように、ステップS50において、基地局300は、UE Capability Info Indicationを上位ノード400に送信する。このような処理は、図5で説明したステップS18と同様である。ここで、UE Capability Info Indicationは、UE capabilityがセキュリティ手順前に取得されたか否かを示す情報要素を含む。

[0069] 例えば、UE Capability Info Indicationは、図12に示す情報要素を含む(TS36.413 v15.7.1 第9.1.10章、TS38.413 v15.5.0 第9.2.13章)。ここで、UE Capability Info Indicationは、” Secured Capability Indication”を含む。” Secured Capability Indication”は、UE capabilityがセキュリティ手順前に取得されたか否かを示す情報要素の一例である。

[0070] ここで、セキュリティ手順前に取得されたUE capabilityは、非認証緊急呼の場合に取得したUE capabilityであってもよい。セキュリティ手順前に取得されたUE capabilityは、狭帯域を利用するUE200(例えば、NB IoT UE)に関するUE capabilityであってもよい。すなわち、基地局300は、セキュリティ手順前に取得されたUE capabilityが非認証緊急呼の場合に取得したものである場合に、S50の処理を実行してもよい。基地局300は、セキュリティ手順前に取得されたUE capabilityが狭帯域を利用するUE200(例えば、NB IoT UE)に関するUE capabilityである場合に、S50の処理を実行してもよい。

[0071] このような構成によれば、ネットワークにおいてセキュリティ手順前に取得されたUE capabilityについて” Send” が許可されるケースにおいて、ネットワークでUE capabilityがセキュリティ手順前に取得されたか否かを把握することができ、UE capabilityのその後の利用を適切に運用することができる

。

[0072] 図11及び図12に示す例では、UE Capability Info Indicationについて説明したが、動作例3はこれに限定されるものではない。UE capabilityがセキュリティ手順前に取得されたか否かを示す情報要素は、ハンドオーバに関連するメッセージに含まれてもよい。ハンドオーバに関連するメッセージは、Handover Preparation Information Messageを含んでもよい。

[0073] 例えば、Handover Preparation Information Messageは、図13に示すように、“ueCapabilitySecured”という情報要素を含んでもよい。“ueCapabilitySecured”は、UE capabilityがセキュリティ手順前に取得されたか否かを示す情報要素の一例である。

[0074] (8) 作用及び効果

実施形態では、基地局300の動作として動作例1～3を採用することによって、ネットワークの合意を遵守可能な基地局300を提供することができる。

[0075] [その他の実施形態]

以上、実施形態に沿って本発明の内容を説明したが、本発明はこれらの記載に限定されるものではなく、種々の変形及び改良が可能であることは、当業者には自明である。

[0076] 上述した動作例1～3では、基地局300と上位ノード400との間のインタフェース（特に、S1インタフェース）について例示した。しかしながら、実施形態はこれに限定されるものではない。動作例1～3は他のインタフェースについても適用可能である。例えば、上述した動作例1～3は、NG(N2)インタフェース、X2インタフェース、Xnインタフェース、N26インタフェースなどの中から選択された1以上のインタフェースに適用可能である。従って、メッセージの送信相手である他のノードは、MME又はAMFなどの上位ノード400に限定されるものではなく、他の基地局（例えば、eNB111及びgNB121）を含んでもよい。また、基地局300は基地局に限定されるものではなく、MME又はAMFなどを含んでもよい。

[0077] 上述した動作例2では、セキュリティ手順前にUE capabilityを送信したUE

200のハンドオーバにおける手順について例示した。このようなハンドオーバは、同一のアクセスネットワーク内におけるハンドオーバ（Intra-RAT handover）を含んでもよく、異なるアクセスネットワーク間におけるハンドオーバ（Inter-RAT handover）を含んでもよい。

また、ハンドオーバに限らず、上位ノード又は他の基地局からUE capabilityを取得する場合（RRC Connection ResumeやUE re-establishment時）を含んでもよい。

[0078] 上述した実施形態では、「セキュリティ手順前」又は「セキュリティ手順後」という用語を用いているが、実施形態はこれに限定されるものではない。これらの用語は「セキュリティ手順の活性化前」又は「セキュリティ手順の活性化後」という用語で読み替えられてもよい。

[0079] 上述した実施形態の説明に用いたブロック構成図（図2及び図3）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。

[0080] 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。例えば、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）と呼ばれる。何れも、上述したとおり、実現方法は特に限定されない。

[0081] さらに、上述したeNB111, gNB121及びUE200（当該装置）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14は、当該装置のハードウェア構成の一例を示す図である。図14に示すように、当該装置は、プロセッサ1001、メモリ1002、ストレージ1003、通信装置1004、入力装置1005、出力装置1006及びバス1007などを含むコンピュータ装置として構成されてもよい。

[0082] なお、以下の説明では、「装置」という文言は、回路、デバイス、ユニットなどに読み替えることができる。当該装置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。

[0083] 当該装置の各機能ブロック（図3参照）は、当該コンピュータ装置の何れかのハードウェア要素、又は当該ハードウェア要素の組み合わせによって実現される。

[0084] また、当該装置における各機能は、プロセッサ1001、メモリ1002など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1001が演算を行い、通信装置1004による通信を制御したり、メモリ1002及びストレージ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。

[0085] 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、レジスタなどを含む中央処理装置（CPU）によって構成されてもよい。

[0086] 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、データなどを、ストレージ1003及び通信装置1004の少なくとも一方からメモリ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。さらに、上述の各種処理は、1つのプロセッサ1001によって実行されてもよいし、2つ以上

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。

[0087] メモリ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、Read Only Memory (ROM)、Erasable Programmable ROM (EPROM)、Electrically Erasable Programmable ROM (EEPROM)、Random Access Memory (RAM)などの少なくとも1つによって構成されてもよい。メモリ1002は、レジスタ、キャッシュ、メインメモリ（主記憶装置）などと呼ばれてもよい。メモリ1002は、本開示の一実施形態に係る方法を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などを保存することができる。

[0088] ストレージ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、Compact Disc ROM (CD-ROM)などの光ディスク、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、磁気ストリップなどの少なくとも1つによって構成されてもよい。ストレージ1003は、補助記憶装置と呼ばれてもよい。上述の記録媒体は、例えば、メモリ1002及びストレージ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。

[0089] 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。

[0090] 通信装置1004は、例えば周波数分割複信（Frequency Division Duplex : FDD）及び時分割複信（Time Division Duplex : TDD）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。

[0091] 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、マウス、マイクロフォン、スイッチ、ボタン、センサなど）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ランプなど）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。

[0092] また、プロセッサ1001及びメモリ1002などの各装置は、情報を通信するためのバス1007で接続される。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。

[0093] さらに、当該装置は、マイクロプロセッサ、デジタル信号プロセッサ（Digital Signal Processor：DSP）、Application Specific Integrated Circuit（ASIC）、Programmable Logic Device（PLD）、Field Programmable Gate Array（FPGA）など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。

[0094] また、情報の通知は、本開示において説明した態様／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、Downlink Control Information（DCI）、Uplink Control Information（UCI）、上位レイヤシグナリング（例えば、RRCシグナリング、Medium Access Control（MAC）シグナリング、報知情報（Master Information Block（MIB）、System Information Block（SIB））、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）メッセージなどであってもよい。

[0095] 本開示において説明した各態様／実施形態は、Long Term Evolution（LTE）、LTE-Advanced（LTE-A）、SUPER 3G、IMT-Advanced、4th generation mobile communication system（4G）、5th generation mobile communication s

ystem (5G)、Future Radio Access (FRA)、New Radio (NR)、W-CDMA (登録商標)、GSM (登録商標)、CDMA2000、Ultra Mobile Broadband (UMB)、IEEE 802.11 (Wi-Fi (登録商標))、IEEE 802.16 (WiMAX (登録商標))、IEEE 802.20、Ultra-WideBand (UWB)、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との組み合わせなど) 適用されてもよい。

[0096] 本開示において説明した各態様／実施形態の処理手順、シーケンス、フローチャートなどは、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。

[0097] 本開示において基地局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。基地局を有する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、端末との通信のために行われる様々な動作は、基地局及び基地局以外の他のネットワークノード (例えば、MME又はS-GWなどが考えられるが、これらに限られない) の少なくとも1つによって行われ得ることは明らかである。上記において基地局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、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。

[0098] 情報、信号 (情報等) は、上位レイヤ (又は下位レイヤ) から下位レイヤ (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。

[0099] 入出力された情報は、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。入出力される情報は、上書き、更新、又は追記され得る。出力された情報は削除されてもよい。入力された情報は他の装置へ送信されてもよい。

- [0100] 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。
- [0101] 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。
- [0102] 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。
- [0103] 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（Digital Subscriber Line：DSL）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。
- [0104] 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何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。
- [0105] 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（Component Carrier：CC）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。

[0106] 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。

[0107] 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。

[0108] 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、PUCCH、PD CCH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ため、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。

[0109] 本開示においては、「基地局（Base Station：BS）」、「無線基地局」、「固定局（fixed station）」、「NodeB」、「eNodeB（eNB）」、「gNodeB（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。

[0110] 基地局は、1つ又は複数（例えば、3つ）のセル（セクタとも呼ばれる）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（Remote Radio Head : RRH）によって通信サービスを提供することもできる。

- [0111] 「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。
- [0112] 本開示においては、「移動局（Mobile Station : MS）」、「ユーザ端末（user terminal）」、「ユーザ装置（User Equipment : UE）」、「端末」などの用語は、互換的に使用され得る。
- [0113] 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。
- [0114] 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Internet of Things (IoT) 機器であってもよい。
- [0115] また、本開示における基地局は、移動局（ユーザ端末、以下同）として読み替えてもよい。例えば、基地局及び移動局間の通信を、複数の移動局間の通信（例えば、Device-to-Device (D2D)、Vehicle-to-Everything (V2X) 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、基地局が有する機能を移動局が有する構成

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。

[0116] 同様に、本開示における移動局は、基地局として読み替えてもよい。この場合、移動局が有する機能を基地局が有する構成としてもよい。

[0117] 無線フレームは時間領域において1つ又は複数のフレームによって構成されてもよい。時間領域において1つ又は複数の各フレームはサブフレームと呼ばれてもよい。

[0118] サブフレームはさらに時間領域において1つ又は複数のスロットによって構成されてもよい。サブフレームは、ニューメロロジー (numerology) に依存しない固定の時間長（例えば、1ms）であってもよい。

[0119] ニューメロロジーは、ある信号又はチャネルの送信及び受信の少なくとも一方に適用される通信パラメータであってもよい。ニューメロロジーは、例えば、サブキャリア間隔 (SubCarrier Spacing : SCS)、帯域幅、シンボル長、サイクリックプレフィックス長、送信時間間隔 (Transmission Time Interval : TTI)、TTIあたりのシンボル数、無線フレーム構成、送受信機が周波数領域において行う特定のフィルタリング処理、送受信機が時間領域において行う特定のウィンドウイング処理などの少なくとも1つを示してもよい。

[0120] スロットは、時間領域において1つ又は複数のシンボル (Orthogonal Frequency Division Multiplexing (OFDM) シンボル、Single Carrier Frequency Division Multiple Access (SC-FDMA) シンボルなど) で構成されてもよい。スロットは、ニューメロロジーに基づく時間単位であってもよい。

[0121] スロットは、複数のミニスロットを含んでもよい。各ミニスロットは、時間領域において1つ又は複数のシンボルによって構成されてもよい。また、ミニスロットは、サブスロットと呼ばれてもよい。ミニスロットは、スロットよりも少ない数のシンボルによって構成されてもよい。ミニスロットより大きい時間単位で送信されるPDSCH (又はPUSCH) は、PDSCH (又はPUSCH) マ

ッピングタイプAと呼ばれてもよい。ミニスロットを用いて送信されるPDSCH (又はPUSCH) は、PDSCH (又はPUSCH) マッピングタイプBと呼ばれてもよい。

- [0122] 無線フレーム、サブフレーム、スロット、ミニスロット及びシンボルは、何れも信号を伝送する際の時間単位を表す。無線フレーム、サブフレーム、スロット、ミニスロット及びシンボルは、それぞれに対応する別の呼称が用いられてもよい。
- [0123] 例えば、1サブフレームは送信時間間隔 (TTI) と呼ばれてもよいし、複数の連続したサブフレームがTTIと呼ばれてよいし、1スロット又は1ミニスロットがTTIと呼ばれてもよい。つまり、サブフレーム及びTTIの少なくとも一方は、既存のLTEにおけるサブフレーム (1ms) であってもよいし、1msより短い期間 (例えば、1-13シンボル) であってもよいし、1msより長い期間であってもよい。なお、TTIを表す単位は、サブフレームではなくスロット、ミニスロットなどと呼ばれてもよい。
- [0124] ここで、TTIは、例えば、無線通信におけるスケジューリングの最小時間単位のことをいう。例えば、LTEシステムでは、基地局が各ユーザ端末に対して、無線リソース (各ユーザ端末において使用することが可能な周波数帯域幅、送信電力など) を、TTI単位で割り当てるスケジューリングを行う。なお、TTIの定義はこれに限られない。
- [0125] TTIは、チャンネル符号化されたデータパケット (トランスポートブロック)、コードブロック、コードワードなどの送信時間単位であってもよいし、スケジューリング、リンクアダプテーションなどの処理単位となってもよい。なお、TTIが与えられたとき、実際にトランスポートブロック、コードブロック、コードワードなどがマッピングされる時間区間 (例えば、シンボル数) は、当該TTIよりも短くてもよい。
- [0126] なお、1スロット又は1ミニスロットがTTIと呼ばれる場合、1以上のTTI (すなわち、1以上のスロット又は1以上のミニスロット) が、スケジューリングの最小時間単位となってもよい。また、当該スケジューリングの最小

時間単位を構成するスロット数（ミニスロット数）は制御されてもよい。

[0127] 1msの時間長を有するTTIは、通常TTI（LTE Rel.8-12におけるTTI）、ノーマルTTI、ロングTTI、通常サブフレーム、ノーマルサブフレーム、ロングサブフレーム、スロットなどと呼ばれてもよい。通常TTIより短いTTIは、短縮TTI、ショートTTI、部分TTI（partial又はfractional TTI）、短縮サブフレーム、ショートサブフレーム、ミニスロット、サブスロット、スロットなどと呼ばれてもよい。

[0128] なお、ロングTTI（例えば、通常TTI、サブフレームなど）は、1msを超える時間長を有するTTIで読み替えてもよいし、ショートTTI（例えば、短縮TTIなど）は、ロングTTIのTTI長未満かつ1ms以上のTTI長を有するTTIで読み替えてもよい。

[0129] リソースブロック（RB）は、時間領域及び周波数領域のリソース割当単位であり、周波数領域において、1つ又は複数個の連続した副搬送波（subcarrier）を含んでもよい。RBに含まれるサブキャリアの数は、ニューメロロジーに関わらず同じであってもよく、例えば12であってもよい。RBに含まれるサブキャリアの数は、ニューメロロジーに基づいて決定されてもよい。

[0130] また、RBの時間領域は、1つ又は複数個のシンボルを含んでもよく、1スロット、1ミニスロット、1サブフレーム、又は1TTIの長さであってもよい。1TTI、1サブフレームなどは、それぞれ1つ又は複数のリソースブロックで構成されてもよい。

[0131] なお、1つ又は複数のRBは、物理リソースブロック（Physical RB：PRB）、サブキャリアグループ（Sub-Carrier Group：SCG）、リソースエレメントグループ（Resource Element Group：REG）、PRBペア、RBペアなどと呼ばれてもよい。

[0132] また、リソースブロックは、1つ又は複数のリソースエレメント（Resource Element：RE）によって構成されてもよい。例えば、1REは、1サブキャリア及び1シンボルの無線リソース領域であってもよい。

[0133] 帯域幅部分（Bandwidth Part：BWP）（部分帯域幅などと呼ばれてもよい）

は、あるキャリアにおいて、あるニューメロロジー用の連続する共通RB (common resource blocks) のサブセットのことを表してもよい。ここで、共通RBは、当該キャリアの共通参照ポイントを基準としたRBのインデックスによって特定されてもよい。PRBは、あるBWPで定義され、当該BWP内で番号付けされてもよい。

[0134] BWPには、UL用のBWP (UL BWP) と、DL用のBWP (DL BWP) とが含まれてもよい。UEに対して、1 キャリア内に1つ又は複数のBWPが設定されてもよい。

[0135] 設定されたBWPの少なくとも1つがアクティブであってもよく、UEは、アクティブなBWPの外で所定の信号／チャネルを送受信することを想定しなくてもよい。なお、本開示における「セル」、「キャリア」などは、「BWP」で読み替えられてもよい。

[0136] 上述した無線フレーム、サブフレーム、スロット、ミニスロット及びシンボルなどの構造は例示に過ぎない。例えば、無線フレームに含まれるサブフレームの数、サブフレーム又は無線フレームあたりのスロットの数、スロット内に含まれるミニスロットの数、スロット又はミニスロットに含まれるシンボル及びRBの数、RBに含まれるサブキャリアの数、並びにTTI内のシンボル数、シンボル長、サイクリックプレフィックス (Cyclic Prefix : CP) 長などの構成は、様々に変更することができる。

[0137] 「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

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。

参照信号は、Reference Signal (RS) 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。

[0138] 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。

[0139] 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。

[0140] 本開示において使用する「第1」、「第2」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つの要素のみがそこで採用され得ること、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。

[0141] 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。

[0142] 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。

[0143] 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)、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。

[0144] 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。

[0145] 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。

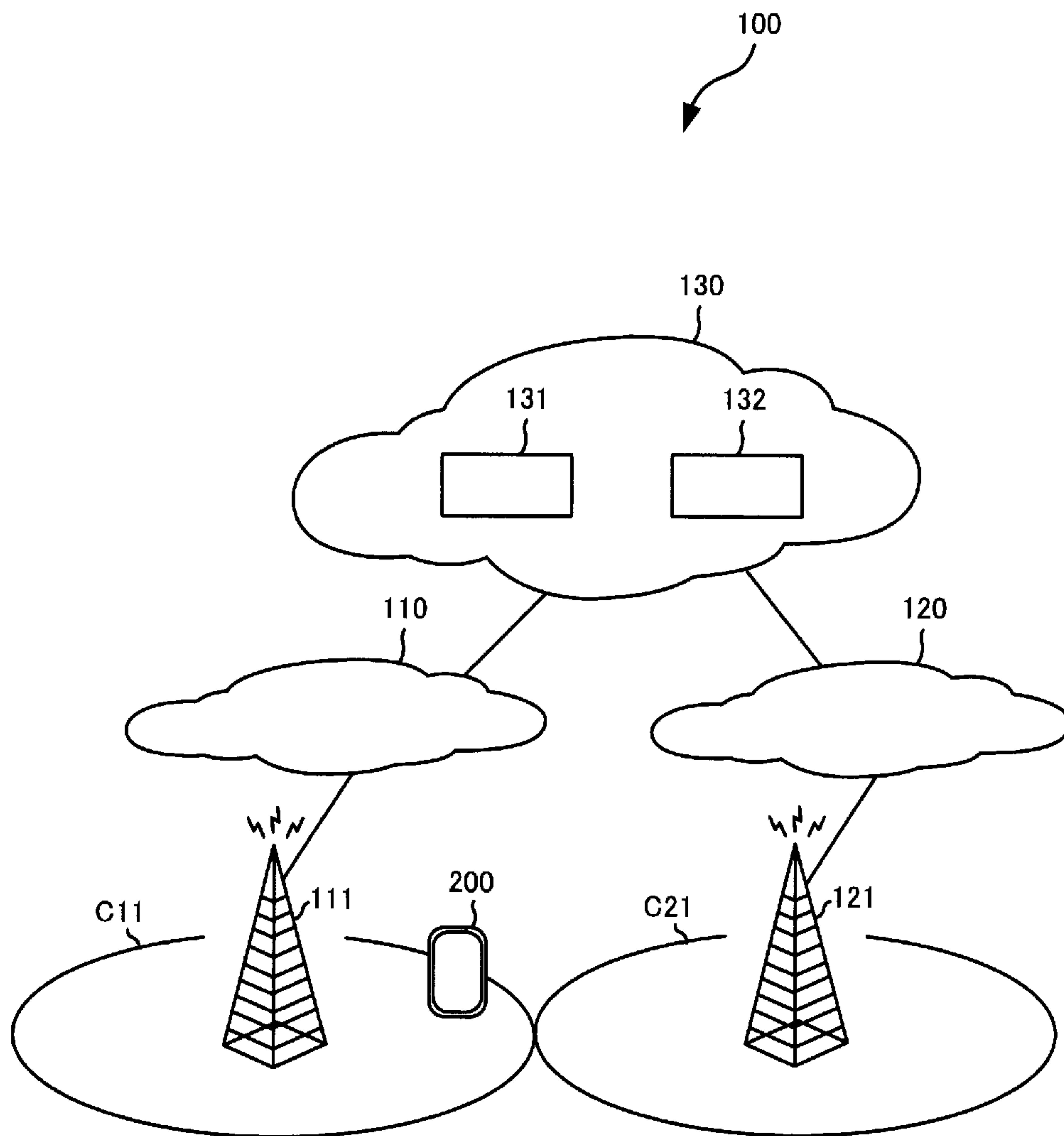
符号の説明

[0146] 100…無線通信システム、110…E-UTRAN、111…eNB、120…NG RAN、121…gNB121、130…コアネットワーク、200…UE、210…受信部、220…送信部、230…制御部、300…基地局、310…受信部、320…送信部、330…制御部、400…上位ノード、1001…プロセッサ、1002…メモリ、1003…ストレージ、1004…通信装置、1005…入力装置、1006…出力装置、1007…バス

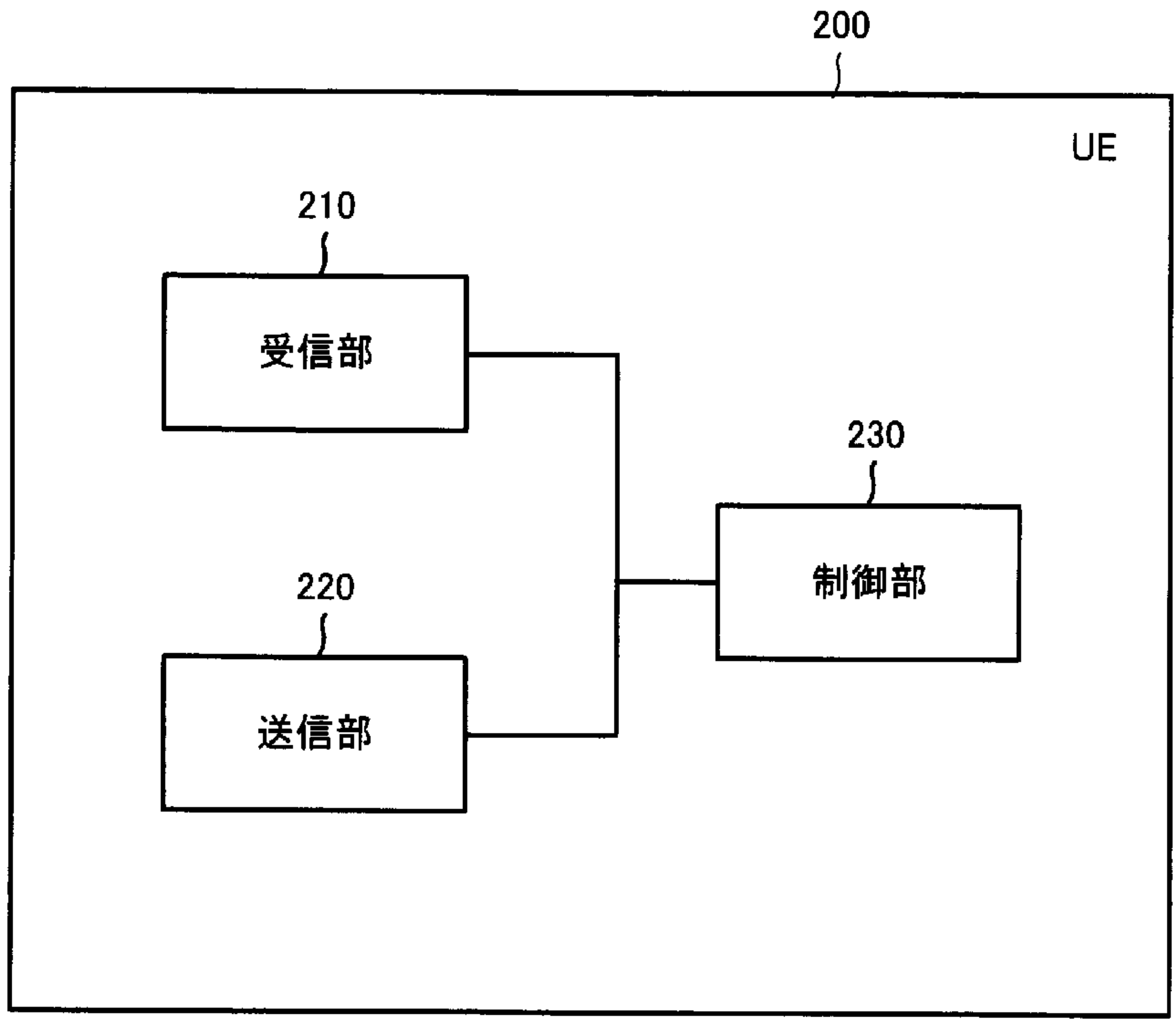
請求の範囲

- [請求項1] セキュリティ手順前に端末能力を端末から受信する受信部と、
前記端末に関する端末コンテキストの解放に応じて、前記セキュリティ手順前に取得した前記端末能力を削除する制御部と、を備える、
基地局。
- [請求項2] 前記受信部は、前記セキュリティ手順後に前記端末能力を前記端末
から受信し、
前記制御部は、前記端末に関する端末コンテキストが解放されても
、前記セキュリティ手順後に取得した前記端末能力を保持する制御を
実行する、請求項1に記載の基地局。
- [請求項3] 前記セキュリティ手順前に取得した前記端末能力は、非認証緊急呼
以外の場合に取得した端末能力、又は、狭帯域を利用する端末に関する
端末能力である、請求項1又は請求項2に記載の基地局。
- [請求項4] セキュリティ手順前に端末能力を端末から受信するステップと、
前記端末に関する端末コンテキストの解放に応じて、前記セキュリティ
手順前に取得した前記端末能力を削除するステップと、を備える
無線通信方法。

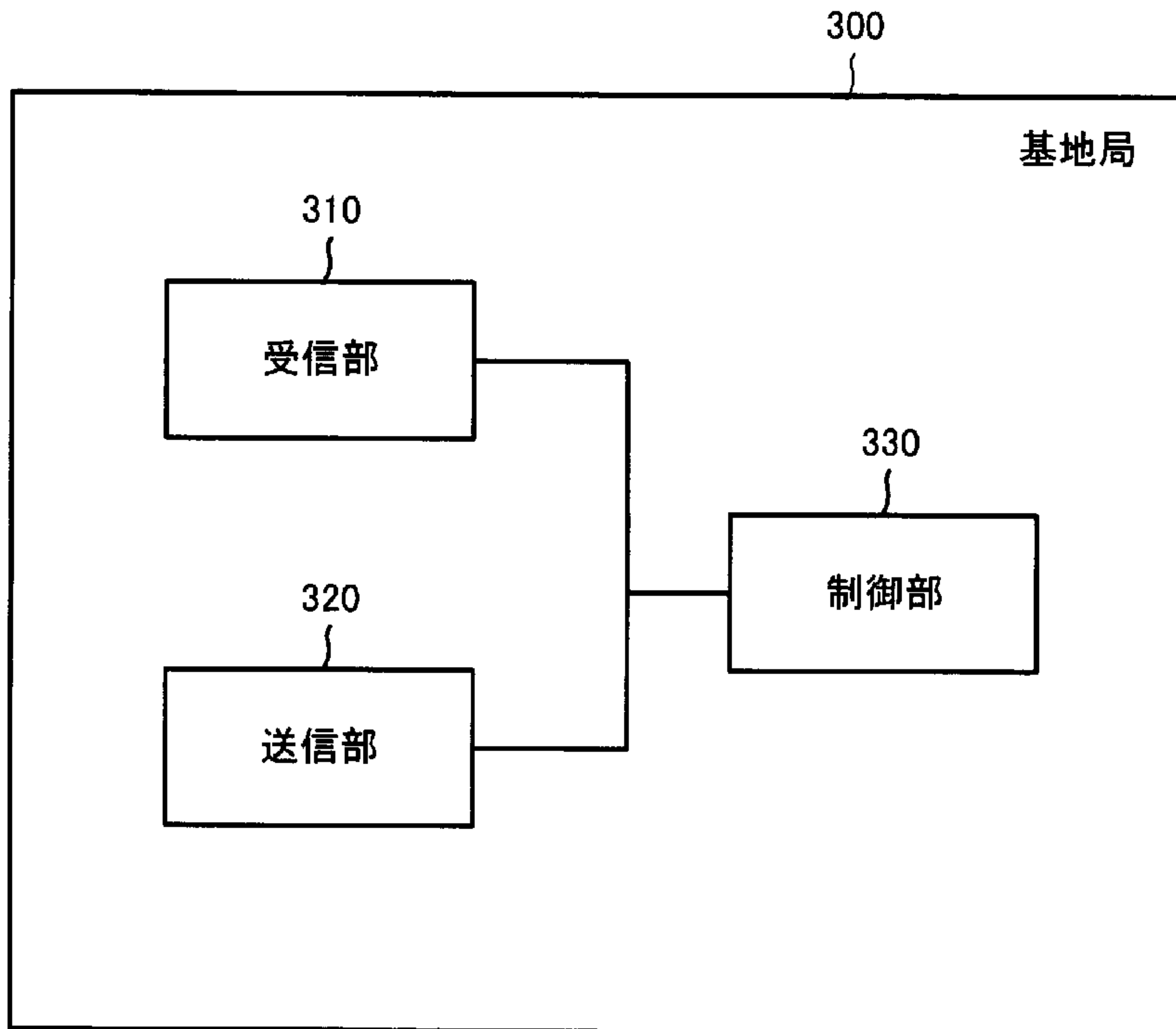
[図1]



[図2]



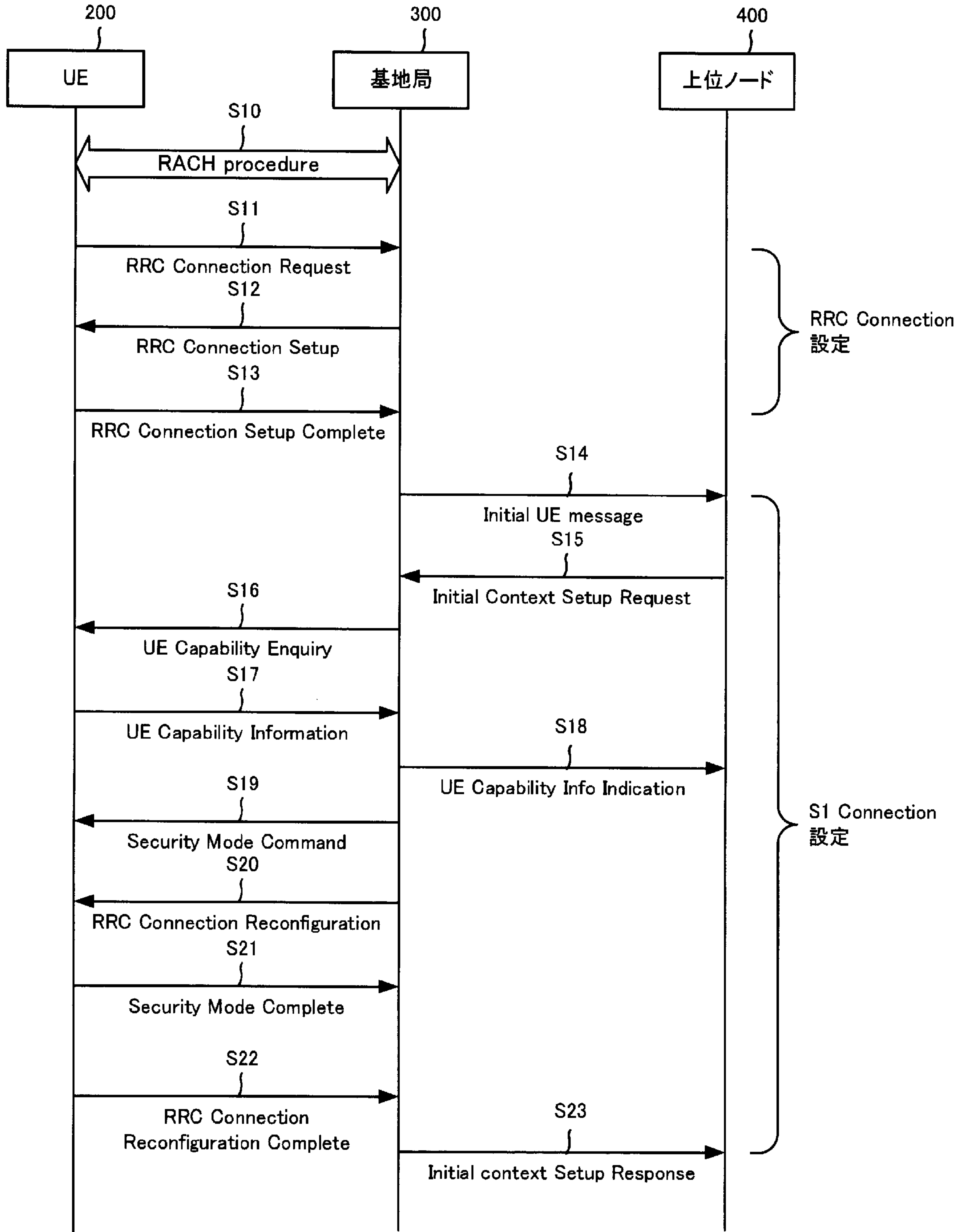
[図3]



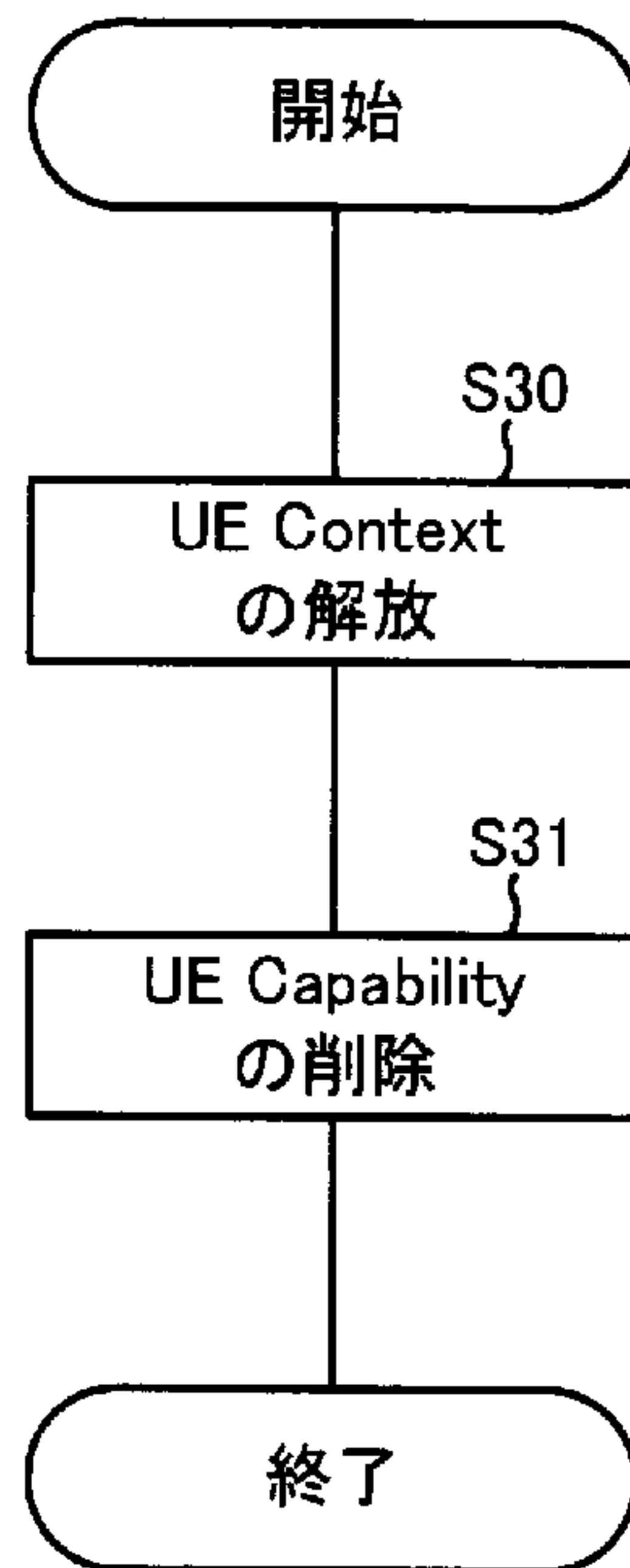
[図4]

UE Capability	Secured	Not Secured	
	Allowed	Allowed	Prohibited
Store	-	-	動作例1
Send	-	動作例3	動作例2

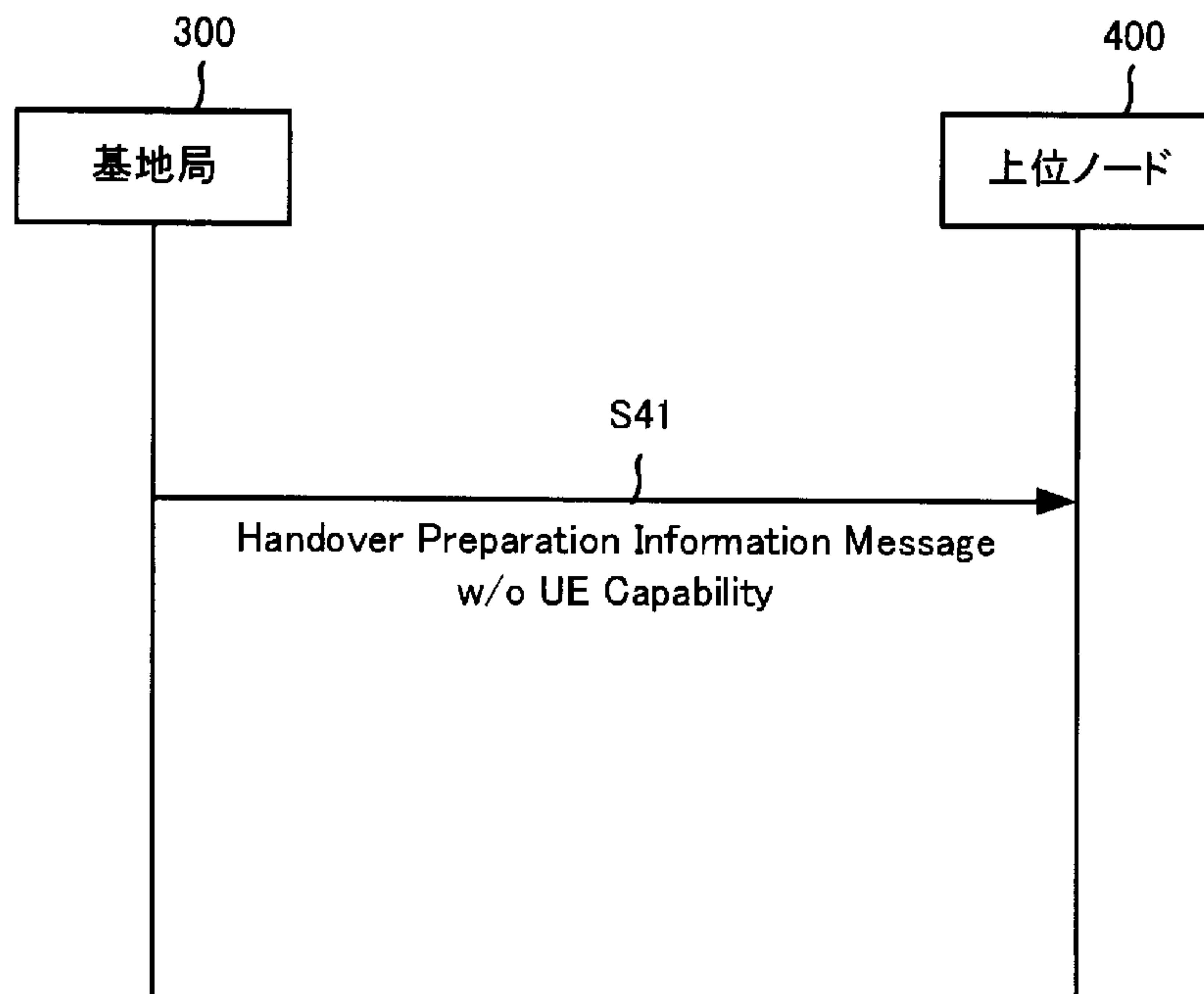
[図5]



[図6]



[図7]



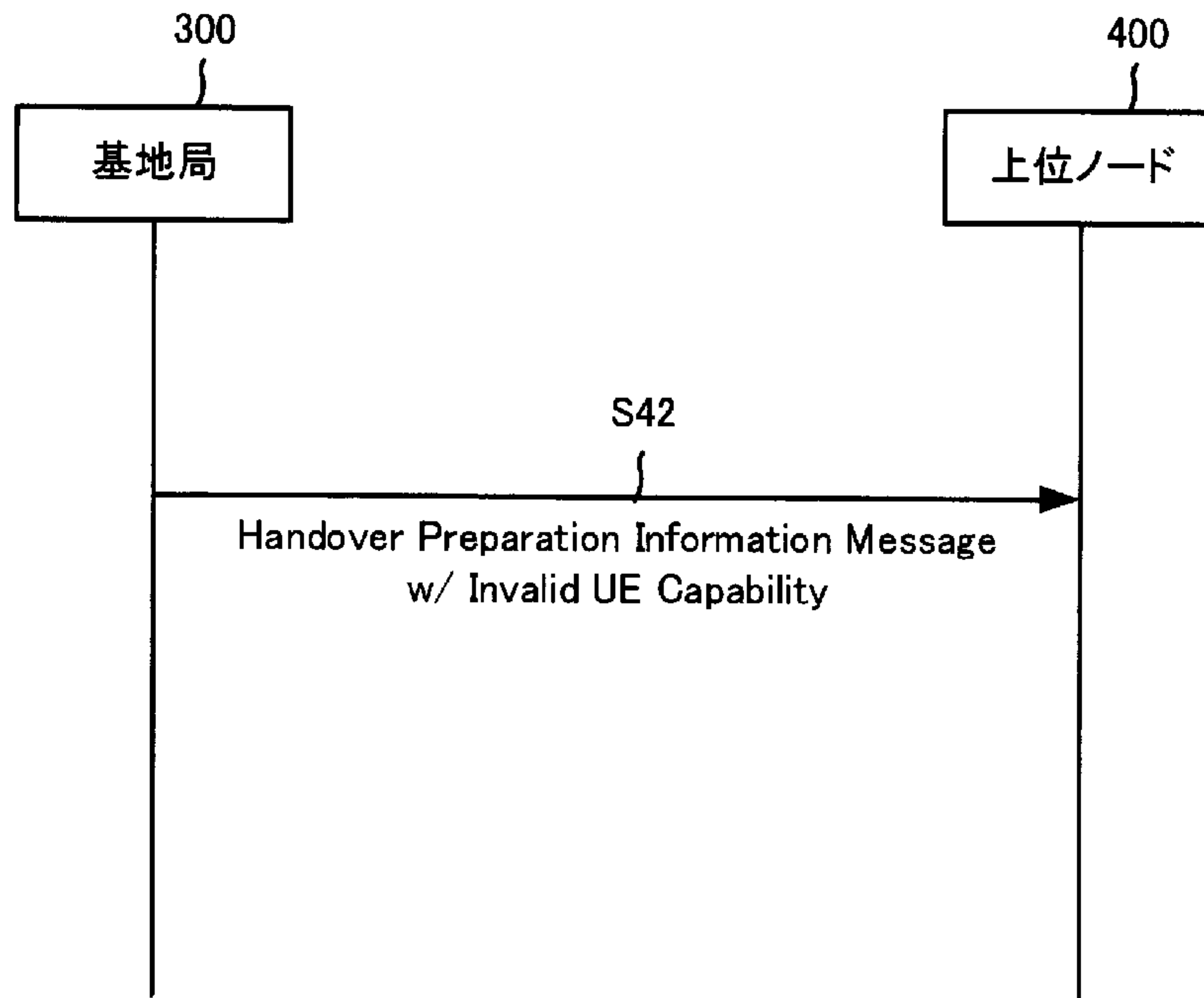
[図8]

UE-CapabilityRAT-ContainerList information element

```

-- ASN1START
UE-CapabilityRAT-ContainerList ::= SEQUENCE (SIZE (0..maxRAT-Capabilities)) OF UE-CapabilityRAT-Container
UE-CapabilityRAT-Container ::= SEQUENCE {
    rat-Type                                RAT-Type,
    ueCapabilityRAT-Container              OCTET STRING,
}
-- ASN1STOP
  
```

[図9]



[図10]

HandoverPreparationInformation-NB message

-- ASN1START

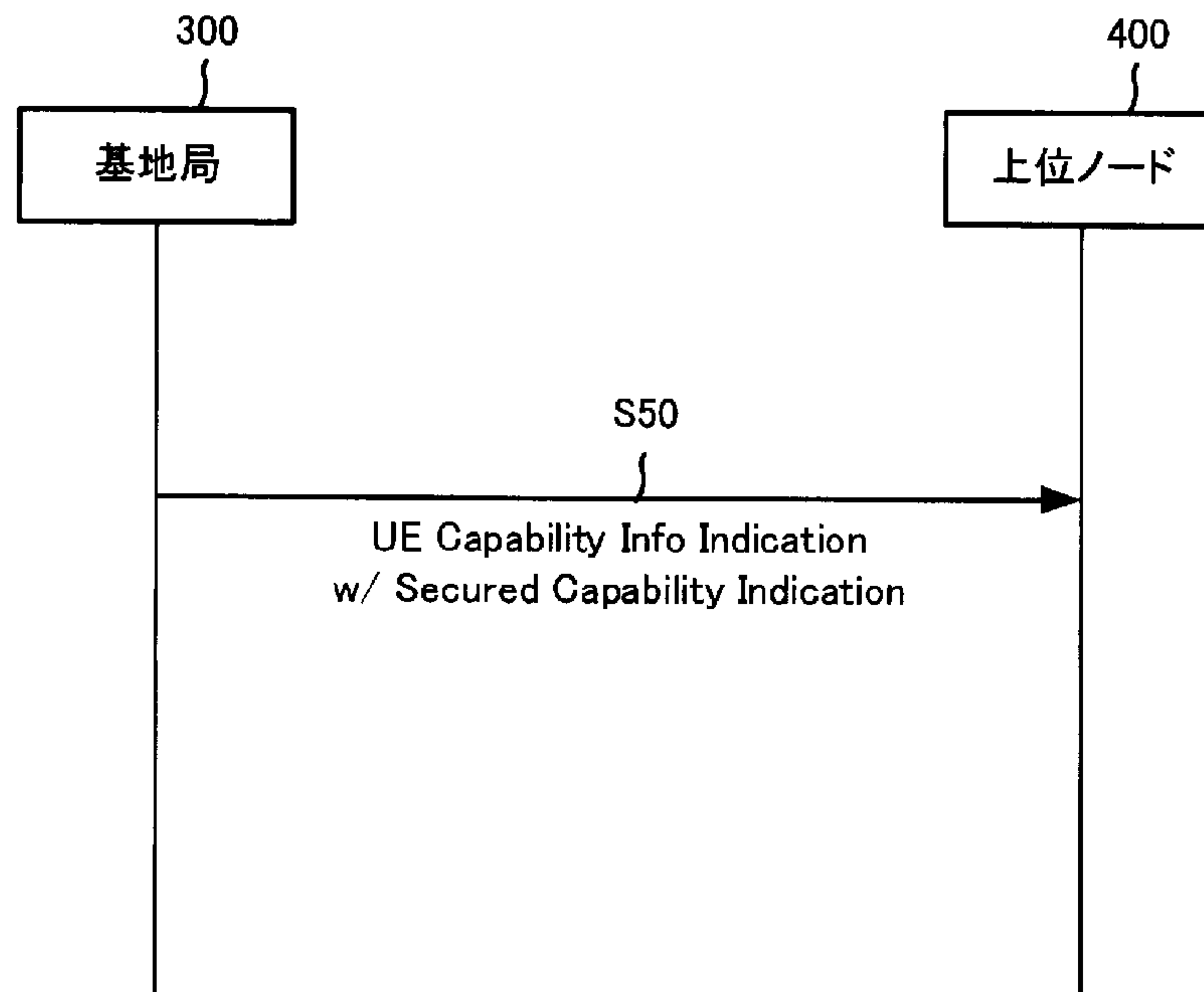
```

HandoverPreparationInformation-NB ::= SEQUENCE {
    criticalExtensions          CHOICE {
        c1
        CHOICE{
            handoverPreparationInformation-r13
            HandoverPreparationInformation-NB-IEs,
            spare3 NULL, spare2 NULL, spare1 NULL
        },
        criticalExtensionsFuture SEQUENCE {}
    }
}

HandoverPreparationInformation-NB-IEs ::= SEQUENCE {
    ue-RadioAccessCapabilityInfo-r13      UE-Capability-NB-r13,
    as-Config-r13                        AS-Config-NB,
    rrm-Config-r13                       RRM-Config-NB      OPTIONAL,
    as-Context-r13                       AS-Context-NB      OPTIONAL,
    nonCriticalExtension
    HandoverPreparationInformation-NB-v1380-IEs
    OPTIONAL
}
中略
HandoverPreparationInformation-NB-Ext-r14-IEs ::= SEQUENCE {
    ue-RadioAccessCapabilityInfoExt-r14    OCTET STRING (CONTAINING UE-
    Capability-NB-Ext-r14-IEs)      OPTIONAL,
    nonCriticalExtension
    HandoverPreparationInformation-NB-Ext-r15-IEs
    OPTIONAL
}
HandoverPreparationInformation-NB-Ext-r15-IEs ::= SEQUENCE {
    invalidUECapability          BOOLEAN,
    nonCriticalExtension        SEQUENCE {}          OPTIONAL
}

```

[図11]



[図12]

IE/Group Name	Presence	Range	IE type and reference	Semantics description	Criticality	Assigned Criticality
Message Type	M		9.2.1.1		YES	ignore
MME UE S1AP ID	M		9.2.3.3		YES	reject
eNB UE S1AP ID	M		9.2.3.4		YES	reject
UE Radio Capability	M		9.2.1.27		YES	ignore
UE Radio Capability for Paging	O		9.2.1.98		YES	ignore
UE Application Layer Measurement Capability	O		BIT STRING	省略	YES	ignore
LTE-M Indication	O		9.2.1.135		YES	ignore
<u>Secured Capability Indication</u>	O				YES	ignore

[図13]

HandoverPreparationInformation message

-- ASN1START

```

HandoverPreparationInformation ::= SEQUENCE {
    criticalExtensions          CHOICE {
        c1                     CHOICE{
            handoverPreparationInformation-r8  HandoverPreparationInformation-r8-IEs,
            spare7 NULL,
            spare6 NULL, spare5 NULL, spare4 NULL,
            spare3 NULL, spare2 NULL, spare1 NULL
        },
        criticalExtensionsFuture  SEQUENCE {}
    }
}

```

```

HandoverPreparationInformation-r8-IEs ::= SEQUENCE {
    ue-RadioAccessCapabilityInfo  UE-CapabilityRAT-ContainerList,
    as-Config                     AS-Config          OPTIONAL,  -- Cond HO
    rrm-Config                    RRM-Config         OPTIONAL,
    as-Context                    AS-Context         OPTIONAL,  -- Cond HO
    nonCriticalExtension          HandoverPreparationInformation-v920-IEs  OPTIONAL
}

```

中略

```

HandoverPreparationInformation-v1540-IEs ::= SEQUENCE {
    sourceRB-ConfigIntra5GC-r15  OCTET STRING    OPTIONAL, --Cond HO4
    nonCriticalExtension          HandoverPreparationInformation-v15xy-IEs
    OPTIONAL
}

```

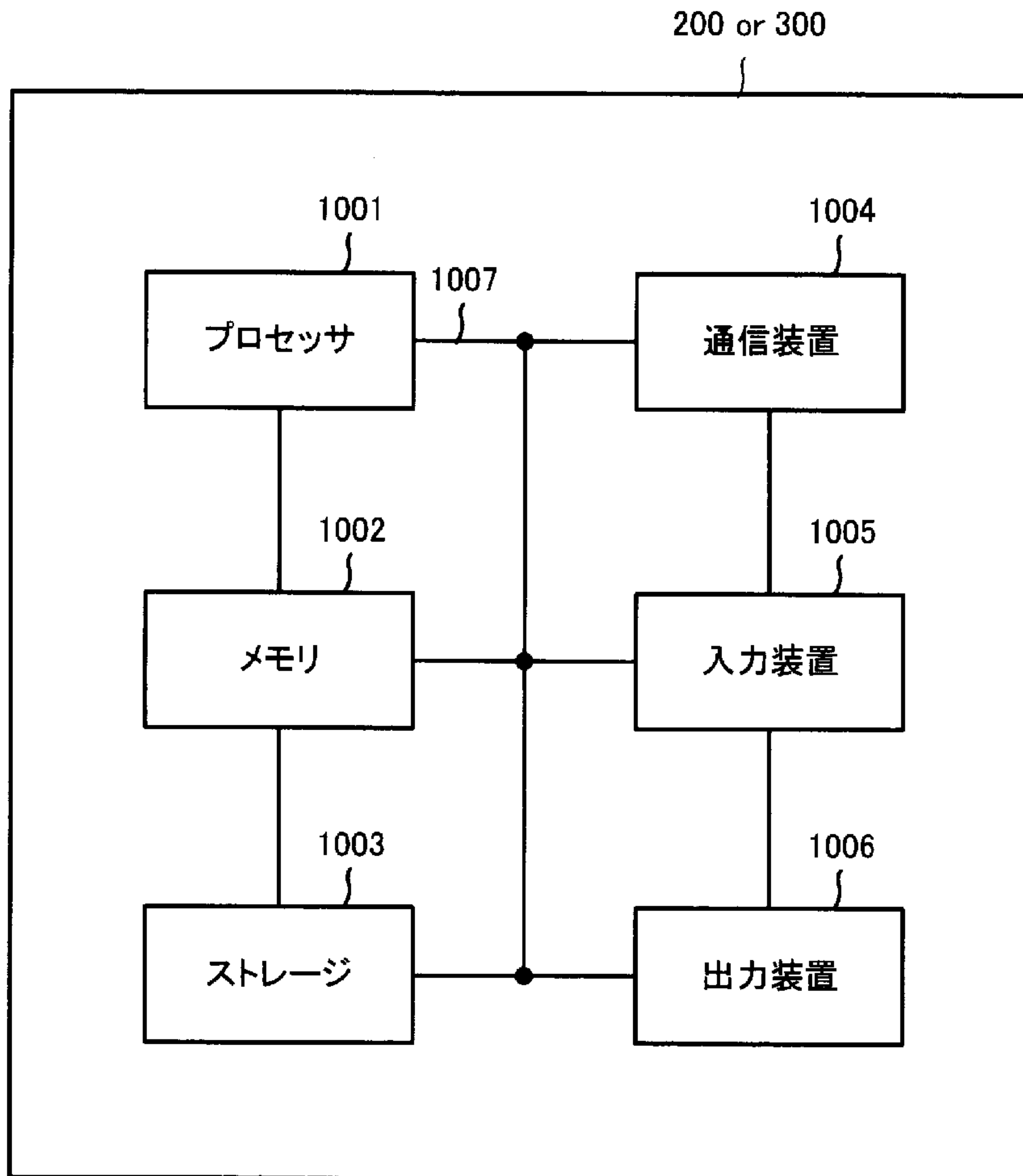
```

HandoverPreparationInformation-v15xy-IEs ::= SEQUENCE {
    ueCapabilitySecured-r15      BOOLEAN          OPTIONAL
    nonCriticalExtension          SEQUENCE {}          OPTIONAL
}


```

-- ASN1STOP

[図14]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/051599

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. H04W5/22 (2009.01) i

FI: H04W8/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. H04W8/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2020
 Registered utility model specifications of Japan 1996-2020
 Published registered utility model applications of Japan 1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ericsson, Security of RRC UE capability transfer procedure in EPS, 3GPP TSG-SA WG3 Meeting #96 S3-192861, 19 August 2019, pages 1, 2, [online], [retrieved on 10 July 2020], Retrieved from the Internet <URL: https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_96_Wroclaw/Does/53-192861.zip > pages 1, 2	1-4
A	Ericsson, Security of RRC UE capability transfer procedure in 5GS, 3GPP TSG-SA WG3 Meeting #96 S3-192862, 19 August 2019, pages 1, 2, [online], [retrieved on 10 July 2020], Retrieved from the Internet <URL: https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_96_Wroclaw/Does/S3-192862.zip > pages 1, 2	1-4

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search
16.07.2020

Date of mailing of the international search report
28.07.2020

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC）） H04W 8/22(2009.01)i FI: H04W8/22		
B. 調査を行った分野 調査を行った最小限資料（国際特許分類（IPC）） H04W8/22 最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922 - 1996年 日本国公開実用新案公報 1971 - 2020年 日本国実用新案登録公報 1996 - 2020年 日本国登録実用新案公報 1994 - 2020年		
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	Ericsson, Security of RRC UE capability transfer procedure in EPS, 3GPP TSG-SA WG3 Meeting #96 S3-192861, 2019.08.19, pages 1-2, [online], [retrieved on 2020-07-10], Retrieved from the Internet<URL:https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_96_Wroclaw/Docs/S3-192861.zip> page 1-2	1-4
A	Ericsson, Security of RRC UE capability transfer procedure in 5GS, 3GPP TSG-SA WG3 Meeting #96 S3-192862, 2019.08.19, pages 1-2, [online], [retrieved on 2020-07-10], Retrieved from the Internet<URL:https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_96_Wroclaw/Docs/S3-192862.zip> pages 1-2	1-4
<input type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技術水準を示すもの “E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの “L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） “O” 口頭による開示、使用、展示等に言及する文献 “P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献	“T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの “X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの “Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの “&” 同一パテントファミリー文献	
国際調査を完了した日 16.07.2020	国際調査報告の発送日 28.07.2020	
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 深津 始 5J 9383 電話番号 03-3581-1101 内線 3534	