

(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
2012 年 10 月 11 日(11.10.2012)



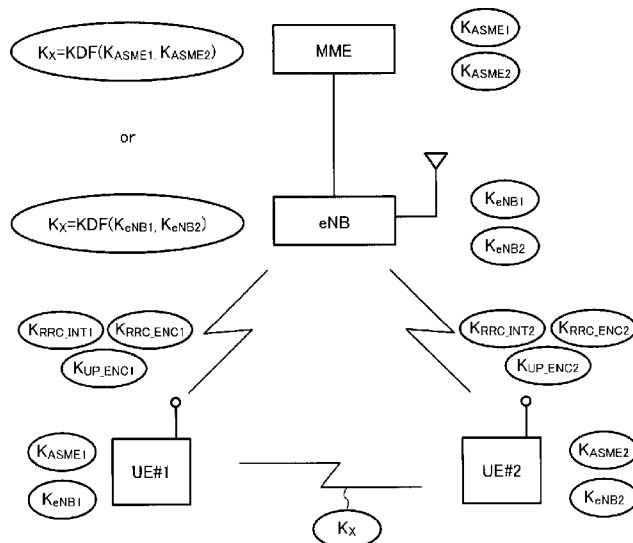
(10) 国際公開番号
WO 2012/137633 A1

- (51) 国際特許分類:
H04W 12/04 (2009.01) H04W 92/18 (2009.01)
- (21) 国際出願番号: PCT/JP2012/057982
- (22) 国際出願日: 2012 年 3 月 27 日(27.03.2012)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2011-082199 2011 年 4 月 1 日(01.04.2011) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒1006150 東京都千代田区永田町二丁目 1 1 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 岩村 幹生 (IWAMURA, Mikio) [JP/—]; 〒1006150 東京都千代田区永田町二丁目 1 1 番 1 号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). ハブサリ ウリ アンダルマワンティ (HAPSARI, Wuri Andarmawanti) [ID/—]; 〒1006150 東京都千代田区永田町二丁目 1 1 番 1 号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP).
- (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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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.
- (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, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).
- 添付公開書類:
— 国際調査報告 (条約第 21 条(3))

(54) Title: MOBILE COMMUNICATIONS METHOD, MOBILE MANAGEMENT NODE, AND WIRELESS BASE STATION

(54) 発明の名称: 移動通信方法、移動管理ノード及び無線基地局

【図3】



(57) Abstract: A mobile communications method pertaining to the present invention has: a step in which a mobile management node (MME) uses a key (K_{ASME1}) managed by the mobile management node (MME) and a mobile station (UE#1) only and a key (K_{ASME2}) managed by the mobile management node (MME) and a mobile station (UE2) only, and generates a key (K_X) used for the security of data signals sent and received via a Uu interface; a step in which the mobile management node (MME) sends the key (K_X) to the mobile station (UE#1) and the mobile station (UE#2); and a step in which the mobile station (UE#1) and the mobile station (UE#2) send and receive data signals via the Uu interface using the key (K_X).

(57) 要約: 本発明に係る移動通信方法は、移動管理ノードMMEが、移動管理ノードMMEと移動局UE#1のみで管理されている鍵 K_{ASME1} 及び移動管理ノードMMEと移動局UE2のみで管理されている鍵 K_{ASME2} を用いて、Uuインタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_X を生成する工程と、移動管理ノードMMEが、移動局UE#1及び移動局UE#2

に対して、鍵 K_X を送信する工程と、移動局UE#1及び移動局UE#2が、鍵 K_X を用いて、Uuインタフェースを介したデータ信号の送受信を行う工程とを有する。

明 細 書

発明の名称：移動通信方法、移動管理ノード及び無線基地局

技術分野

[0001] 本発明は、移動通信方法、移動管理ノード及び無線基地局に関する。

背景技術

[0002] W-CDMA (Wideband-Code Division Multiple Access) 方式やLTE (Long Term Evolution) の方式等のセルラー方式の移動通信システムでは、複数の移動局UE同士の通信は、無線アクセスネットワーク装置やコアネットワーク装置等を介して行われるように構成されている。

先行技術文献

非特許文献

[0003] 非特許文献1：3GPP TS 36.300

非特許文献2：3GPP TS 33.401

発明の概要

発明が解決しようとする課題

[0004] しかしながら、従来のセルラー方式の移動通信システムでは、複数の移動局UEが、同一セル（或いは、無線アクセスネットワーク装置配下のセル）内に配置されている場合であっても、データ信号及び制御信号の両方が、無線アクセスネットワーク装置を介して送受信されるように構成されているため、無線アクセスネットワーク装置の処理負荷が増大してしまうという問題点があった。

[0005] かかる問題点を解決するために、複数の移動局が、無線基地局との間で設定されているUuインタフェースを介することなく、移動局間インタフェース（以下、Udインタフェース）を介して、データ信号の送受信を行うことを想定することができる。

[0006] しかしながら、かかる場合、既存の移動通信システムの仕組みを利用して

、U d インタフェースを介して送受信されるデータ信号のセキュリティ（秘匿や改竄検出）に用いる移動局間通信用鍵について生成することができないという問題点があった。

[0007] そこで、本発明は、上述の課題に鑑みてなされたものであり、既存の移動通信システムの仕組みを利用して、U d インタフェースを介して送受信されるデータ信号のセキュリティ（秘匿や改竄検出）に用いる移動局間通信用鍵を生成することができる移動通信方法、移動管理ノード及び無線基地局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] 本発明の第1の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、移動管理ノードが、該移動管理ノードと前記第1移動局のみで管理されている第1アクセスセキュリティ管理鍵及び該移動管理ノードと前記第2移動局のみで管理されている第2アクセスセキュリティ管理鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成する工程と、前記移動管理ノードが、前記第1移動局及び前記第2移動局に対して、前記移動局間通信用鍵を送信する工程と、前記第1移動局及び前記第2移動局が、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行う工程とを有することを要旨とする。

[0009] 本発明の第2の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノードであって、前記移動管理ノードと前記第1移動局のみで管理されている第1アクセスセキュリティ管理鍵及び該移動

管理ノードと前記第2移動局のみで管理されている第2アクセスセキュリティ管理鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するように構成されている生成部と、前記第1移動局及び前記第2移動局に対して、前記移動局間通信用鍵を送信するように構成されている送信部とを具備することを要旨とする。

[0010] 本発明の第3の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、前記無線基地局が、該無線基地局と前記第1移動局のみで管理されている第1無線基地局鍵及び該無線基地局と前記第2移動局のみで管理されている第2無線基地局鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成する工程と、前記無線基地局が、前記第1移動局及び前記第2移動局に対して、前記移動局間通信用鍵を送信する工程と、前記第1移動局及び前記第2移動局が、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行う工程とを有することを要旨とする。

[0011] 本発明の第4の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる前記無線基地局であって、前記無線基地局と前記第1移動局のみで管理されている第1無線基地局鍵及び該無線基地局と前記第2移動局のみで管理されている第2無線基地局鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するように構成されている生成部と、前記第1移動局及び前記第2移動局に対して、前記移動局間通信用鍵を送信するように構成されて

いる送信部とを具備することを要旨とする。

[0012] 本発明の第5の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、移動管理ノードが、該移動管理ノードと前記第1移動局のみで管理されている第1アクセスセキュリティ管理鍵及び該移動管理ノードと前記第2移動局のみで管理されている第2アクセスセキュリティ管理鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するための第1パラメータ及び第2パラメータを生成する工程と、前記移動管理ノードが、前記第1移動局に対して、前記第1パラメータを送信し、前記第2移動局に対して、前記第2パラメータを送信する工程と、前記第1移動局が、前記第1パラメータを用いて、前記移動局間通信用鍵を生成する工程と、前記第2移動局が、前記第2パラメータを用いて、前記移動局間通信用鍵を生成する工程と、前記第1移動局及び前記第2移動局が、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行う工程とを有することを要旨とする。

[0013] 本発明の第6の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノードであって、前記移動管理ノードと前記第1移動局のみで管理されている第1アクセスセキュリティ管理鍵及び該移動管理ノードと前記第2移動局のみで管理されている第2アクセスセキュリティ管理鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するための第1パラメータ及び第2パラメータを生成するように構成されている生成部と、前記第1移動局に対して、前記第1パラメータを送信し、前記第2移動局に対し

て、前記第2パラメータを送信するように構成されている送信部とを具備することを要旨とする。

[0014] 本発明の第7の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、前記無線基地局が、該無線基地局と前記第1移動局のみで管理されている第1無線基地局鍵及び該無線基地局と前記第2移動局のみで管理されている第2無線基地局鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するための第1パラメータ及び第2パラメータを生成する工程と、前記無線基地局が、前記第1移動局に対して、前記第1パラメータを送信し、前記第2移動局に対して、前記第2パラメータを送信する工程と、前記第1移動局が、前記第1パラメータを用いて、前記移動局間通信用鍵を生成する工程と、前記第2移動局が、前記第2パラメータを用いて、前記移動局間通信用鍵を生成する工程と、前記第1移動局及び前記第2移動局が、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行う工程とを有することを要旨とする。

[0015] 本発明の第8の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる前記無線基地局であって、前記無線基地局と前記第1移動局のみで管理されている第1無線基地局鍵及び該無線基地局と前記第2移動局のみで管理されている第2無線基地局鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するための第1パラメータ及び第2パラメータを生成するように構成されている生成部と、前記第1移動局に対して、前記第1パラメー

タを送信し、前記第2移動局に対して、前記第2パラメータを送信するように構成されている送信部とを具備することを要旨とする。

[0016] 本発明の第9の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて該第1移動局として動作する移動局であって、前記無線基地局又は移動管理ノードから、移動局間通信用鍵を取得するように構成されている受信部と、前記第2移動局との間で、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行うように構成されている通信部とを具備することを要旨とする。

[0017] 本発明の第10の特徴は、第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて該第1移動局として動作する移動局であって、前記無線基地局又は移動管理ノードから、第1パラメータを取得するように構成されている受信部と、前記第1パラメータを用いて、移動局間通信用鍵を生成するように構成されている生成部と、前記第2移動局との間で、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行うように構成されている通信部とを具備することを要旨とする。

発明の効果

[0018] 以上説明したように、本発明によれば、既存の移動通信システムの仕組みを利用して、Udインタフェースを介して送受信するデータ信号のセキュリティ（秘匿や改竄検出）に用いる移動局間通信用鍵を生成することができる移動通信方法、移動管理ノード及び無線基地局を提供することができる。

図面の簡単な説明

[0019] [図1]図1は、本発明の第1の実施形態に係る移動通信システムの全体構成図

である。

[図2]図2は、本発明の第1の実施形態に係る移動管理ノード及び無線基地局の機能ブロック図である。

[図3]図3は、本発明の第1の実施形態に係る移動通信システムにおける鍵 K_x の生成方法について説明するための図である。

[図4]図4は、本発明の第2の実施形態に係る移動通信システムにおける鍵 K_x の生成方法について説明するための図である。

[図5]図5は、本発明の第2の実施形態に係る移動局の機能ブロック図である。

発明を実施するための形態

[0020] (本発明の第1の実施形態に係る移動通信システム)

図1乃至図3を参照して、本発明の第1の実施形態に係る移動通信システムについて説明する。

[0021] 本実施形態に係る移動通信システムは、LTE方式の移動通信システムであって、図1に示すように、移動管理ノードMME (Mobility Management Entity) と、移動管理ノードMME配下に接続されている無線基地局eNBとを具備している。なお、本発明は、LTE方式以外のセルラー方式の移動通信システムにも適用可能である。

[0022] ここで、無線基地局eNBと移動局UE#1/UE#2との間では、Uuインタフェースを介してデータ信号が送受信されるように構成されており、移動局UE#1と移動局UE#2との間では、Udインタフェースを介してデータ信号が送受信されるように構成されている。

[0023] すなわち、移動局UE#1は、移動局UE#2との間で、無線基地局eNBを介して (Uuインタフェースを介して) データ信号を送受信することもできるし、無線基地局eNBを介さないで (Udインタフェースを介して) データ信号を送受信することもできる。

[0024] 同様に、移動局UE#2は、移動局UE#1との間で、無線基地局eNBを介して (Uuインタフェースを介して) データ信号を送受信することもで

きるし、無線基地局 eNB を介さないで (Uu インタフェースを介して) データ信号を送受信することもできる。

[0025] ここで、Uu インタフェースや Uu インタフェースを介して送受信されるデータ信号には、セキュリティ (秘匿や改竄検出) が適用される。セキュリティを適用するために、送受信エンティティ間で、共通の鍵が用意される。

[0026] LTE 方式の Uu インタフェースにおける鍵の生成方法は、3GPP の TS 33.401 等に規定されている。本発明は、Uu インタフェースにおける鍵の生成方法に係るものである。

[0027] 図 2 に示すように、移動管理ノード MME は、管理部 11 と、生成部 12 と、送信部 13 とを具備している。

[0028] 管理部 11 は、3GPP の TS 33.401 に規定されている各移動局 UE 用の鍵 K_{ASME} (Access Security Management Entity) を管理するように構成されている。例えば、管理部 11 は、移動局 UE # 1 用の鍵 K_{ASME1} や移動局 UE # 2 用の鍵 K_{ASME2} を管理するように構成されている。

[0029] ここで、鍵 K_{ASME1} は、移動管理ノード MME と移動局 UE # 1 のみで管理されており、無線基地局 eNB や移動局 UE # 2 によって管理されていない。また、鍵 K_{ASME2} は、移動管理ノード MME と移動局 UE # 2 のみで管理されており、無線基地局 eNB や移動局 UE # 1 によって管理されていない。

[0030] 生成部 12 は、鍵 K_{ASME1} 及び鍵 K_{ASME2} を用いて、Uu インタフェースを介した移動局 UE # 1 と移動局 UE # 2 との間におけるデータ信号の送受信に用いる鍵 K_x を生成するように構成されている。

[0031] 例えば、図 3 に示すように、生成部 12 は、式「 $K_x = KDF(K_{ASME1}, K_{ASME2})$ 」によって、かかる鍵 K_x を生成するように構成されていてもよい。

[0032] なお、生成部 12 は、鍵 K_{ASME1} を用いて、Uu インタフェースを介した移動局 UE # 1 と無線基地局 eNB との間におけるデータ信号の送受信に用いる鍵 K_{RRC_INT1} や鍵 K_{RRC_ENC1} や鍵 K_{UP_ENC1} の生成に必要な鍵 K_{eNB1} の生成に必要なパラメータ NH1 (3GPP の TS 33.401 参照) を生成する

ように構成されていてもよい。

[0033] 同様に、生成部12は、鍵 K_{ASME2} を用いて、Uuインタフェースを介した移動局UE#2と無線基地局eNBとの間におけるデータ信号の送受信に用いる鍵 K_{RRC_INT2} や鍵 K_{RRC_ENC2} や鍵 K_{UP_ENC2} の生成に必要な鍵 K_{eNB2} の生成に必要なパラメータNH2（3GPPのTS33.401参照）を生成するように構成されていてもよい。

[0034] また、生成部12は、鍵 K_{ASME1} を用いて鍵 K_{eNB1} を生成し、鍵 K_{ASME2} を用いて鍵 K_{eNB2} を生成するように構成されていてもよい。

[0035] 送信部13は、移動局UE#1及び移動局UE#2に対して、上述の鍵 K_x を送信するように構成されている。

[0036] なお、送信部13は、無線基地局eNBに対して、上述のパラメータNH1及びNH2を送信するように構成されていてもよい。

[0037] また、送信部13は、無線基地局eNB及び移動局UE#1に対して、パラメータNH1のカウントNCC1を送信し、無線基地局eNB及び移動局UE#2に対して、パラメータNH2のカウントNCC2を送信するように構成されていてもよい。

[0038] また、送信部13は、無線基地局eNBに対して、鍵 K_{eNB1} 及び K_{eNB2} を送信するように構成されていてもよい。

[0039] ここで、移動局UE#1は、移動管理ノードMMEから受信した鍵 K_x を用いて、Udインタフェースを介して、移動局UE#2との間で、データ信号の送受信を行うように構成されている。

[0040] 同様に、移動局UE#2は、移動管理ノードMMEから受信した鍵 K_x を用いて、Udインタフェースを介して、移動局UE#1との間で、データ信号の送受信を行うように構成されている。

[0041] なお、移動局UE#1は、移動管理ノードMMEから受信したパラメータNH1及び自身が管理している鍵 K_{eNB1} を用いて、鍵 K_{RRC_INT1} や鍵 K_{RRC_ENC1} や鍵 K_{UP_ENC1} を生成し、鍵 K_{RRC_INT1} や鍵 K_{RRC_ENC1} や鍵 K_{UP_ENC1} を用いて、Uuインタフェースを介して、無線基地局eNBとの間で、データ

信号の送受信を行うように構成されている。

[0042] また、移動局UE # 2は、移動管理ノードMMEから受信したパラメータNH2及び自身が管理している鍵 K_{eNB2} を用いて、鍵 K_{RRC_INT2} や鍵 K_{RRC_ENC2} や鍵 K_{UP_ENC2} を生成し、鍵 K_{RRC_INT2} や鍵 K_{RRC_ENC2} や鍵 K_{UP_ENC2} を用いて、Uuインタフェースを介して、無線基地局eNBとの間で、データ信号の送受信を行うように構成されている。

[0043] 本発明の第1の実施形態に係る移動通信システムによれば、移動管理ノードMMEが、既存の移動通信システムで用いられていた鍵 K_{ASME1} 及び鍵 K_{ASME2} を用いて、Udインタフェースを介した移動局UE # 1と移動局UE # 2との間におけるデータ信号の送受信で用いられる鍵 K_x を生成して、移動局UE # 1及び移動局UE # 2に対して送信することができる。

[0044] (変更例1)

以下、本発明の第1の実施形態に係る移動通信システムの変更例1について、本発明の第1の実施形態に係る移動通信システムとの相違点に着目して説明する。

[0045] 本変更例1に係る移動通信システムでは、移動管理ノードMMEの代わりに、無線基地局eNBが、上述の鍵 K_x を生成して、移動局UE # 1及び移動局UE # 2に対して送信するように構成されている。

[0046] 具体的には、図2に示すように、移動管理ノードMMEの代わりに、無線基地局eNBが、管理部11と、生成部12と、送信部13とを具備している。

[0047] 管理部11は、3GPPのTS33.401に規定されている各移動局UE用の鍵 K_{eNB} を管理するように構成されている。例えば、管理部11は、移動局UE # 1用の鍵 K_{eNB1} や移動局UE # 2用の鍵 K_{eNB2} を管理するように構成されている。

[0048] ここで、鍵 K_{eNB1} は、無線基地局eNBと移動局UE # 1のみで管理されており、移動管理ノードMME（通信確立時にMMEが生成する初回の鍵 K_{NB1} を除く）や移動局UE # 2によって管理されていない。また、鍵 K_{eNB2}

は、無線基地局 eNB と移動局 $UE \# 2$ のみで管理されており、移動管理ノード MME （通信確立時に MME が生成する初回の鍵 K_{eNB2} を除く）や移動局 $UE \# 1$ によって管理されていない。

[0049] 生成部 12 は、鍵 K_{eNB1} 及び鍵 K_{eNB2} を用いて、 Ud インタフェースを介した移動局 $UE \# 1$ と移動局 $UE \# 2$ との間におけるデータ信号の送受信に用いる鍵 K_x を生成するように構成されている。

[0050] 例えば、図 3 に示すように、生成部 12 は、式「 $K_x = KDF(K_{eNB1}, K_{eNB2})$ 」によって、かかる鍵 K_x を生成するように構成されていてもよい。

[0051] なお、生成部 12 は、移動管理ノード MME から受信したパラメータ $NH1$ 及び自身が管理している鍵 K_{eNB1} を用いて、 Uu インタフェースを介した移動局 $UE \# 1$ と無線基地局 eNB との間におけるデータ信号の送受信に用いる鍵 K_{RRC_INT1} や鍵 K_{RRC_ENC1} や鍵 K_{UP_ENC1} を生成するように構成されていてもよい。

[0052] 同様に、生成部 12 は、移動管理ノード MME から受信したパラメータ $NH2$ 及び自身が管理している鍵 K_{eNB2} を用いて、 Uu インタフェースを介した移動局 $UE \# 2$ と無線基地局 eNB との間におけるデータ信号の送受信に用いる鍵 K_{RRC_INT2} や鍵 K_{RRC_ENC2} や鍵 K_{UP_ENC2} を生成するように構成されていてもよい。

[0053] 送信部 13 は、移動局 $UE \# 1$ 及び移動局 $UE \# 2$ に対して、上述の鍵 K_x を送信するように構成されている。

[0054] 本発明の第 1 の実施形態の変更例 1 に係る移動通信システムによれば、無線基地局 eNB が、既存の移動通信システムで用いられていた鍵 K_{eNB1} 及び鍵 K_{eNB2} を用いて、 Ud インタフェースを介した移動局 $UE \# 1$ と移動局 $UE \# 2$ との間におけるデータ信号の送受信で用いられる鍵 K_x を生成して、移動局 $UE \# 1$ 及び移動局 $UE \# 2$ に対して送信することができる。

[0055] （本発明の第 2 の実施形態）

図 4 及び図 5 を参照して、本発明の第 2 の実施形態に係る移動通信システムについて説明する。以下、本発明の第 2 の実施形態に係る移動通信システム

ムについて、上述の第 1 の実施形態に係る移動通信システムとの相違点に着目して説明する。

[0056] 移動管理ノードMMEの生成部12は、鍵 K_{ASME1} 及び鍵 K_{ASME2} を用いて、Udインタフェースを介した移動局UE#1と移動局UE#2との間のデータ信号の送受信に用いる鍵 K_x を生成するためのパラメータ K_{x1} 及びパラメータ K_{x2} を生成するように構成されている。

[0057] 例えば、図4に示すように、移動管理ノードMMEの生成部12は、式「 $K_{x1} = KDF(K_{ASME1}, K_{ASME2}, K_{ASME2})$ 」によって、かかるパラメータ K_{x1} を生成するように構成されていてもよい（代替として、式「 $K_{x1} = KDF(K_{ASME2})$ 」といった形式の式が用いられてもよい）。

[0058] また、図4に示すように、移動管理ノードMMEの生成部12は、式「 $K_{x2} = KDF(K_{ASME1}, K_{ASME1}, K_{ASME2})$ 」によって、かかるパラメータ K_{x2} を生成するように構成されていてもよい（代替として、式「 $K_{x2} = KDF(K_{ASME1})$ 」といった形式の式が用いられてもよい）。

[0059] 移動管理ノードMMEの送信部13は、移動局UE#1に対して、パラメータ K_{x1} を送信し、移動局UE#2に対して、パラメータ K_{x2} を送信するように構成されている。

[0060] 図5に示すように、移動局UE#1及び移動局UE#2は、管理部21と、受信部22と、生成部23と、通信部24とを具備している。

[0061] 移動局UE#1の管理部21は、上述の鍵 K_{ASME1} 及び鍵 K_{eNB1} を管理するように構成されている。また、移動局UE#2の管理部21は、上述の鍵 K_{ASME2} 及び鍵 K_{eNB2} を管理するように構成されている。

[0062] 移動局UE#1の受信部22は、移動管理ノードMMEから、パラメータNH1のカウンタNCC1やパラメータ K_{x1} を受信するように構成されている。また、移動局UE#2の受信部22は、移動管理ノードMMEから、パラメータNH2のカウンタNCC2やパラメータ K_{x2} を受信するように構成されている。

[0063] 移動局UE#1の生成部23は、パラメータ K_{x1} 及び自身が管理している

鍵 K_{ASME1} を用いて、Udインタフェースを介した移動局UE # 2 との間のデータ信号の送受信に用いる鍵 K_x を生成するように構成されている。

[0064] 例えば、図4に示すように、移動局UE # 1の生成部23は、式「 $K_x = KDF(K_{x1}, K_{ASME1})$ 」によって、かかる鍵 K_x を生成するように構成されていてもよい。

[0065] 同様に、移動局UE # 2の生成部23は、パラメータ K_{x2} 及び自身が管理している鍵 K_{ASME2} を用いて、Udインタフェースを介した移動局UE # 1との間のデータ信号の送受信に用いる鍵 K_x を生成するように構成されている。

[0066] 例えば、図4に示すように、移動局UE # 2の生成部23は、式「 $K_x = KDF(K_{x2}, K_{ASME2})$ 」によって、かかる鍵 K_x を生成するように構成されていてもよい。

[0067] また、移動局UE # 1の生成部23は、移動管理ノードMMEから受信したパラメータNH1及び自身が管理している鍵 K_{NB1} を用いて、鍵 K_{RRC_INT1} や鍵 K_{RRC_ENC1} や鍵 K_{UP_ENC1} を生成するように構成されている。

[0068] また、移動局UE # 2は、移動管理ノードMMEから受信したパラメータNH2及び自身が管理している鍵 K_{NB2} を用いて、鍵 K_{RRC_INT2} や鍵 K_{RRC_ENC2} や鍵 K_{UP_ENC2} を生成するように構成されている。

[0069] 移動局UE 1の通信部24は、かかる鍵 K_x を用いて、Udインタフェースを介して、移動局UE # 2との間で、データ信号の送受信を行うように構成されている。

[0070] 移動局UE 2の通信部24は、かかる鍵 K_x を用いて、Udインタフェースを介して、移動局UE # 1との間で、データ信号の送受信を行うように構成されている。

[0071] 本発明の第2の実施形態に係る移動通信システムによれば、移動管理ノードMMEが、既存の移動通信システムで用いられていた鍵 K_{ASME1} 及び鍵 K_{ASME2} を用いて、パラメータ K_{x1} 及びパラメータ K_{x2} を生成して、移動局UE # 1及び移動局UE # 2に対して送信し、移動局UE # 1及び移動局UE # 2が、かかるパラメータ K_{x1} 及びパラメータ K_{x2} を用いて、Udインタフェ

ースを介した移動局UE # 1と移動局UE # 2との間におけるデータ信号の送受信で用いられる鍵 K_x を生成することができる。

[0072] (変更例2)

以下、本発明の第2の実施形態に係る移動通信システムの変更例2について、本発明の第2の実施形態に係る移動通信システムとの相違点に着目して説明する。

[0073] 本変更例2に係る移動通信システムでは、移動管理ノードMMEの代わりに、無線基地局eNBが、上述のパラメータ K_{x1} 及びパラメータ K_{x2} を生成して、移動局UE # 1及び移動局UE # 2に対して送信するように構成されている。

[0074] 無線基地局eNBの生成部12は、鍵 K_{eNB1} 及び鍵 K_{eNB2} を用いて、Udインタフェースを介した移動局UE # 1と移動局UE # 2との間のデータ信号の送受信に用いる鍵 K_x を生成するためのパラメータ K_{x1} 及びパラメータ K_{x2} を生成するように構成されている。

[0075] 例えば、図4に示すように、無線基地局eNBの生成部12は、式「 $K_{x1} = KDF(K_{eNB1}, K_{eNB2}, K_{eNB2})$ 」によって、かかるパラメータ K_{x1} を生成するように構成されていてもよい（代替として、式「 $K_{x1} = KDF(K_{eNB2})$ 」といった形式の式が用いられてもよい）。

[0076] また、図4に示すように、無線基地局eNBの生成部12は、式「 $K_{x2} = KDF(K_{eNB1}, K_{eNB1}, K_{eNB2})$ 」によって、かかるパラメータ K_{x2} を生成するように構成されていてもよい（代替として、式「 $K_{x2} = KDF(K_{eNB1})$ 」といった形式の式が用いられてもよい）。

[0077] 無線基地局eNBの送信部13は、移動局UE # 1に対して、パラメータ K_{x1} を送信し、移動局UE # 2に対して、パラメータ K_{x2} を送信するように構成されている。

[0078] 移動局UE # 1の受信部22は、無線基地局eNBから、パラメータ K_{x1} を受信するように構成されている。また、移動局UE # 2の受信部22は、無線基地局eNBから、パラメータ K_{x2} を受信するように構成されている。

- [0079] 移動局UE # 1の生成部23は、パラメータ K_{x1} 及び自身が管理している鍵 K_{eNB1} を用いて、Udインタフェースを介した移動局UE # 2との間のデータ信号の送受信に用いる鍵 K_x を生成するように構成されている。
- [0080] 例えば、図4に示すように、移動局UE # 1の生成部23は、式「 $K_x = KDF(K_{x1}, K_{eNB1})$ 」によって、かかる鍵 K_x を生成するように構成されていてもよい。
- [0081] 同様に、移動局UE # 2の生成部23は、パラメータ K_{x2} 及び自身が管理している鍵 K_{eNB2} を用いて、Udインタフェースを介した移動局UE # 1との間のデータ信号の送受信に用いる鍵 K_x を生成するように構成されている。
- [0082] 例えば、図4に示すように、移動局UE # 2の生成部23は、式「 $K_x = KDF(K_{x2}, K_{eNB2})$ 」によって、かかる鍵 K_x を生成するように構成されていてもよい。
- [0083] 本発明の第2の実施形態の変更例2に係る移動通信システムによれば、無線基地局eNBが、既存の移動通信システムで用いられていた鍵 K_{eNB1} 及び鍵 K_{eNB2} を用いて、パラメータ K_{x1} 及びパラメータ K_{x2} を生成して、移動局UE # 1及び移動局UE # 2に対して送信し、移動局UE # 1及び移動局UE # 2が、かかるパラメータ K_{x1} 及びパラメータ K_{x2} を用いて、Udインタフェースを介した移動局UE # 1と移動局UE # 2との間におけるデータ信号の送受信で用いられる鍵 K_x を生成することができる。
- [0084] なお、以上の全ての実施形態において、実際にUdインタフェースを介したデータ送受信で用いられる鍵は、上述の鍵 K_x から派生した鍵であってもよい。
- [0085] 例えば、何らかのカウンタやベアラIDやベアラ種別や送受信方向等のパラメータに基づき、鍵 K_x から派生された鍵が用いられてもよい。
- [0086] 以上に述べた本実施形態の特徴は、以下のように表現されていてもよい。
- [0087] 本実施形態の第1の特徴は、移動局UE # 1（第1移動局）及び移動局UE # 2（第2移動局）が、無線基地局eNBとの間で設定されているUuインタフェース（無線基地局インタフェース）を介することなく、移動局UE

1 と移動局 UE # 2 との間で設定されている U d インタフェース（移動局間インタフェース）を介して、データ信号の送受信を行う移動通信方法であって、移動管理ノード MME が、移動管理ノード MME と移動局 UE # 1 のみで管理されている鍵 K_{ASME1} （第 1 アクセスセキュリティ管理鍵）及び移動管理ノード MME と移動局 UE 2 のみで管理されている鍵 K_{ASME2} （第 2 アクセスセキュリティ管理鍵）を用いて、U d インタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x （移動局間通信用鍵）を生成する工程と、移動管理ノード MME が、移動局 UE # 1 及び移動局 UE # 2 に対して、鍵 K_x を送信する工程と、移動局 UE # 1 及び移動局 UE # 2 が、鍵 K_x を用いて、U d インタフェースを介したデータ信号の送受信を行う工程とを有することを要旨とする。

[0088] 本実施形態の第 2 の特徴は、移動局 UE # 1 及び移動局 UE # 2 が、U u インタフェースを介することなく、U d インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノード MME であって、鍵 K_{ASME1} 及び鍵 K_{ASME2} を用いて、U d インタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x を生成するように構成されている生成部 12 と、移動局 UE # 1 及び移動局 UE # 2 に対して、鍵 K_x を送信するように構成されている送信部 13 とを具備することを要旨とする。

[0089] 本実施形態の第 3 の特徴は、移動局 UE # 1 及び移動局 UE # 2 が、U u インタフェースを介することなく、U d インタフェースを介して、データ信号の送受信を行う移動通信方法であって、無線基地局 eNB が、無線基地局 eNB と移動局 UE # 1 のみで管理されている鍵 K_{eNB1} （第 1 無線基地局鍵）及び無線基地局 eNB と移動局 UE # 2 のみで管理されている鍵 K_{eNB2} （第 2 無線基地局鍵）を用いて、U d インタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x を生成する工程と、無線基地局 eNB が、移動局 UE # 1 及び移動局 UE # 2 に対して、鍵 K_x を送信する工程と、移動局 UE # 1 及び移動局 UE # 2 が、鍵 K_x を用いて、U d インタフェース

を介したデータ信号の送受信を行う工程とを有することを要旨とする。

[0090] 本実施形態の第4の特徴は、移動局UE # 1及び移動局UE # 2が、Uuインタフェースを介することなく、Udインタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる無線基地局eNBであって、鍵 K_{eNB1} 及び鍵 K_{eNB2} を用いて、Udインタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x を生成するように構成されている生成部12と、移動局UE # 1及び移動局UE # 2に対して、鍵 K_x を送信するように構成されている送信部13とを具備することを要旨とする。

[0091] 本実施形態の第5の特徴は、移動局UE # 1及び移動局UE # 2が、Uuインタフェースを介することなく、Udインタフェースを介して、データ信号の送受信を行う移動通信方法であって、移動管理ノードMMEが、鍵 K_{ASME1} 及び鍵 K_{ASME2} を用いて、Udインタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x を生成するためのパラメータ K_{x1} （第1パラメータ）及びパラメータ K_{x2} （第2パラメータ）を生成する工程と、移動管理ノードMMEが、移動局UE # 1に対して、パラメータ K_{x1} を送信し、移動局UE # 2に対して、パラメータ K_{x2} を送信する工程と、移動局UE # 1が、パラメータ K_{x1} を用いて、鍵 K_x を生成する工程と、移動局UE # 2が、パラメータ K_{x2} を用いて、鍵 K_x を生成する工程と、移動局UE # 1及び移動局UE # 2が、鍵 K_x を用いて、Udインタフェースを介したデータ信号の送受信を行う工程とを有することを要旨とする。

[0092] 本実施形態の第6の特徴は、移動局UE # 1及び移動局UE # 2が、Uuインタフェースを介することなく、Udインタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノードMMEであって、鍵 K_{ASME1} 及び鍵 K_{ASME2} を用いて、Udインタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x を生成するためのパラメータ K_{x1} 及びパラメータ K_{x2} を生成するように構成されている生成部12と、移動局UE # 1に対して、パラメータ K_x

K_{x1} を送信し、移動局UE # 2に対して、パラメータ K_{x2} を送信するように構成されている送信部13とを具備することを要旨とする。

[0093] 本実施形態の第7の特徴は、移動局UE # 1及び移動局UE # 2が、Uuインタフェースを介することなく、Udインタフェースを介して、データ信号の送受信を行う移動通信方法であって、無線基地局eNBが、鍵 K_{eNB1} 及び鍵 K_{eNB2} を用いて、Udインタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x を生成するためのパラメータ K_{x1} 及びパラメータ K_{x2} を生成する工程と、無線基地局eNBが、移動局UE # 1に対して、パラメータ K_{x1} を送信し、移動局UE # 2に対して、パラメータ K_{x2} を送信する工程と、移動局UE # 1が、パラメータ K_{x1} を用いて、鍵 K_x を生成する工程と、移動局UE # 2が、パラメータ K_{x2} を用いて、鍵 K_x を生成する工程と、移動局UE # 1及び移動局UE # 2が、鍵 K_x を用いて、Udインタフェースを介したデータ信号の送受信を行う工程とを有することを要旨とする。

[0094] 本実施形態の第8の特徴は、移動局UE # 1及び移動局UE # 2が、Uuインタフェースを介することなく、Udインタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる無線基地局eNBであって、鍵 K_{eNB1} 及び鍵 K_{eNB2} を用いて、Udインタフェースを介して送受信されるデータ信号のセキュリティに用いる鍵 K_x を生成するためのパラメータ K_{x1} 及びパラメータ K_{x2} を生成するように構成されている生成部12と、移動局UE # 1に対して、パラメータ K_{x1} を送信し、移動局UE # 2に対して、パラメータ K_{x2} を送信するように構成されている送信部13とを具備することを要旨とする。

[0095] 本実施形態の第9の特徴は、移動局UE # 1及び移動局UE # 2が、Uuインタフェースを介することなく、Udインタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて移動局UE # 1として動作する移動局UEであって、無線基地局eNB又は移動管理ノードMMEから、鍵 K_x を取得するように構成されている受信部22と、移動局UE # 2との間で、鍵 K_x を用いて、Udインタフェースを

介したデータ信号の送受信を行うように構成されている通信部24とを具備することを要旨とする。

[0096] 本実施形態の第10の特徴は、移動局UE#1及び移動局UE#2が、Uuインタフェースを介することなく、Udインタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて移動局UE#1として動作する移動局UEであって、無線基地局eNB又は移動管理ノードMMEから、パラメータ K_{x1} を取得するように構成されている受信部22と、パラメータ K_{x1} を用いて、鍵 K_x を生成するように構成されている生成部23と、移動局UE#2との間で、鍵 K_x を用いて、Udインタフェースを介したデータ信号の送受信を行うように構成されている通信部24とを具備することを要旨とする。

[0097] なお、上述の移動管理ノードMMEや無線基地局eNBや移動局UE等の動作は、ハードウェアによって実施されてもよいし、プロセッサによって実行されるソフトウェアモジュールによって実施されてもよいし、両者の組み合わせによって実施されてもよい。

[0098] ソフトウェアモジュールは、RAM (Random Access Memory) や、フラッシュメモリや、ROM (Read Only Memory) や、EPROM (Erasable Programmable ROM) や、EEPROM (Electrically Erasable and Programmable ROM) や、レジスタや、ハードディスクや、リムーバブルディスクや、CD-ROMといった任意形式の記憶媒体内に設けられていてもよい。

[0099] かかる記憶媒体は、プロセッサが当該記憶媒体に情報を読み書きできるように、当該プロセッサに接続されている。また、かかる記憶媒体は、プロセッサに集積されていてもよい。また、かかる記憶媒体及びプロセッサは、ASIC内に設けられていてもよい。かかるASICは、移動管理ノードMMEや無線基地局eNBや移動局UE等内に設けられていてもよい。また、かかる記憶媒体及びプロセッサは、ディスクリートコンポーネントとして移動

管理ノードMMEや無線基地局eNBや移動局UE等内に設けられていてもよい。

[0100] 以上、上述の実施形態を用いて本発明について詳細に説明したが、当業者にとっては、本発明が本明細書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。本発明は、請求の範囲の記載により定まる本発明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。従って、本明細書の記載は、例示説明を目的とするものであり、本発明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

[0101] MME…移動管理ノード

eNB…無線基地局

UE…移動局

11、21…管理部

12、23…生成部

13…送信部

22…受信部

24…通信部

請求の範囲

[請求項1]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、

移動管理ノードが、該移動管理ノードと前記第1移動局のみで管理されている第1アクセスセキュリティ管理鍵及び該移動管理ノードと前記第2移動局のみで管理されている第2アクセスセキュリティ管理鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成する工程と、

前記移動管理ノードが、前記第1移動局及び前記第2移動局に対して、前記移動局間通信用鍵を送信する工程と、

前記第1移動局及び前記第2移動局が、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行う工程とを有することを特徴とする移動通信方法。

[請求項2]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノードであって、

前記移動管理ノードと前記第1移動局のみで管理されている第1アクセスセキュリティ管理鍵及び該移動管理ノードと前記第2移動局のみで管理されている第2アクセスセキュリティ管理鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するように構成されている生成部と、

前記第1移動局及び前記第2移動局に対して、前記移動局間通信用鍵を送信するように構成されている送信部とを具備することを特徴と

する移動管理ノード。

[請求項3]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、

前記無線基地局が、該無線基地局と前記第1移動局のみで管理されている第1無線基地局鍵及び該無線基地局と前記第2移動局のみで管理されている第2無線基地局鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成する工程と、

前記無線基地局が、前記第1移動局及び前記第2移動局に対して、前記移動局間通信用鍵を送信する工程と、

前記第1移動局及び前記第2移動局が、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行う工程とを有することを特徴とする移動通信方法。

[請求項4]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる前記無線基地局であって、

前記無線基地局と前記第1移動局のみで管理されている第1無線基地局鍵及び該無線基地局と前記第2移動局のみで管理されている第2無線基地局鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するように構成されている生成部と、

前記第1移動局及び前記第2移動局に対して、前記移動局間通信用鍵を送信するように構成されている送信部とを具備することを特徴とする無線基地局。

[請求項5]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、

移動管理ノードが、該移動管理ノードと前記第1移動局のみで管理されている第1アクセスセキュリティ管理鍵及び該移動管理ノードと前記第2移動局のみで管理されている第2アクセスセキュリティ管理鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するための第1パラメータ及び第2パラメータを生成する工程と、

前記移動管理ノードが、前記第1移動局に対して、前記第1パラメータを送信し、前記第2移動局に対して、前記第2パラメータを送信する工程と、

前記第1移動局が、前記第1パラメータを用いて、前記移動局間通信用鍵を生成する工程と、

前記第2移動局が、前記第2パラメータを用いて、前記移動局間通信用鍵を生成する工程と、

前記第1移動局及び前記第2移動局が、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行う工程とを有することを特徴とする移動通信方法。

[請求項6]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる移動管理ノードであって、

前記移動管理ノードと前記第1移動局のみで管理されている第1アクセスセキュリティ管理鍵及び該移動管理ノードと前記第2移動局のみで管理されている第2アクセスセキュリティ管理鍵を用いて、前記

移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するための第1パラメータ及び第2パラメータを生成するように構成されている生成部と、

前記第1移動局に対して、前記第1パラメータを送信し、前記第2移動局に対して、前記第2パラメータを送信するように構成されている送信部とを具備することを特徴とする移動管理ノード。

[請求項7]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行う移動通信方法であって、

前記無線基地局が、該無線基地局と前記第1移動局のみで管理されている第1無線基地局鍵及び該無線基地局と前記第2移動局のみで管理されている第2無線基地局鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するための第1パラメータ及び第2パラメータを生成する工程と、

前記無線基地局が、前記第1移動局に対して、前記第1パラメータを送信し、前記第2移動局に対して、前記第2パラメータを送信する工程と、

前記第1移動局が、前記第1パラメータを用いて、前記移動局間通信用鍵を生成する工程と、

前記第2移動局が、前記第2パラメータを用いて、前記移動局間通信用鍵を生成する工程と、

前記第1移動局及び前記第2移動局が、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行う工程とを有することを特徴とする移動通信方法。

[請求項8]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2

移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムで用いられる前記無線基地局であって、

前記無線基地局と前記第1移動局のみで管理されている第1無線基地局鍵及び該無線基地局と前記第2移動局のみで管理されている第2無線基地局鍵を用いて、前記移動局間インタフェースを介して送受信されるデータ信号のセキュリティに用いる移動局間通信用鍵を生成するための第1パラメータ及び第2パラメータを生成するように構成されている生成部と、

前記第1移動局に対して、前記第1パラメータを送信し、前記第2移動局に対して、前記第2パラメータを送信するように構成されている送信部とを具備することを特徴とする無線基地局。

[請求項9]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて該第1移動局として動作する移動局であって、

前記無線基地局又は移動管理ノードから、移動局間通信用鍵を取得するように構成されている受信部と、

前記第2移動局との間で、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行うように構成されている通信部とを具備することを特徴とする移動局。

[請求項10]

第1移動局及び第2移動局が、無線基地局との間で設定されている無線基地局インタフェースを介することなく、該第1移動局と該第2移動局との間で設定されている移動局間インタフェースを介して、データ信号の送受信を行うことができるように構成されている移動通信システムにおいて該第1移動局として動作する移動局であって、

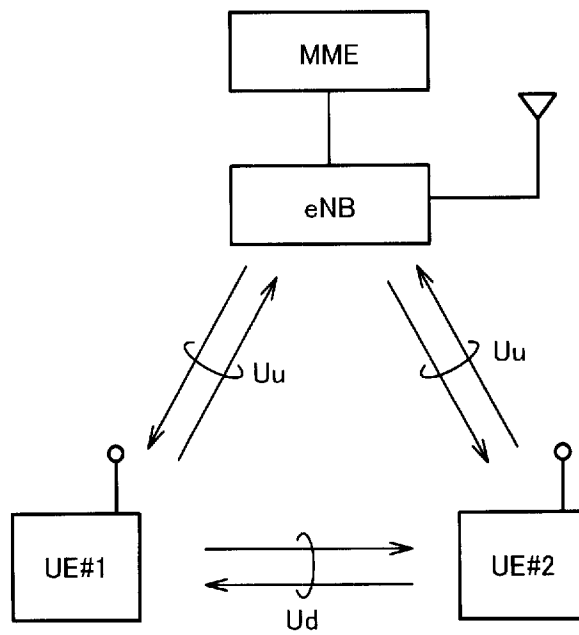
前記無線基地局又は移動管理ノードから、第1パラメータを取得す

るように構成されている受信部と、

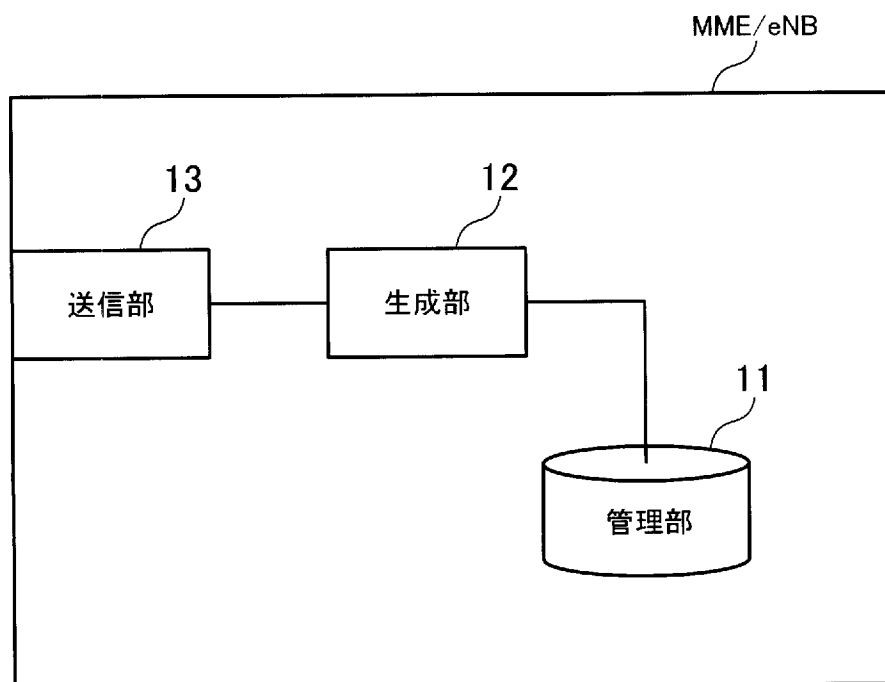
前記第 1 パラメータを用いて、移動局間通信用鍵を生成するように構成されている生成部と、

前記第 2 移動局との間で、前記移動局間通信用鍵を用いて、前記移動局間インタフェースを介したデータ信号の送受信を行うように構成されている通信部とを具備することを特徴とする移動局。

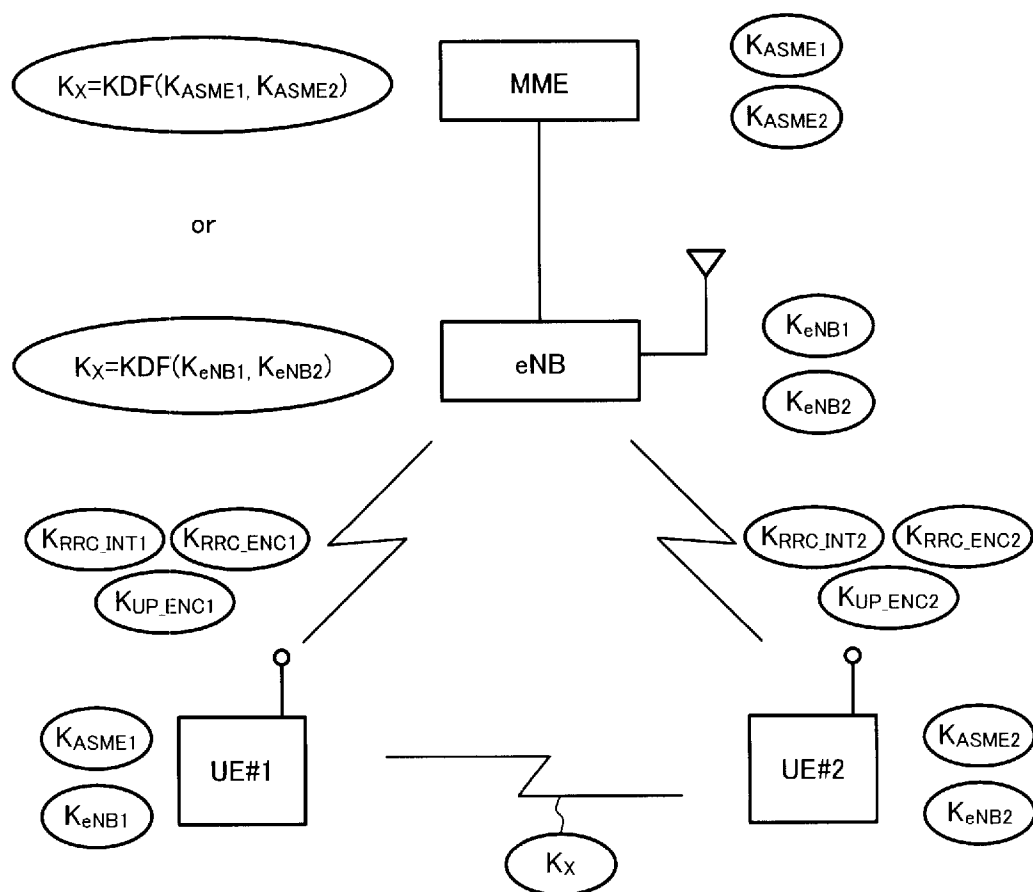
[図1]



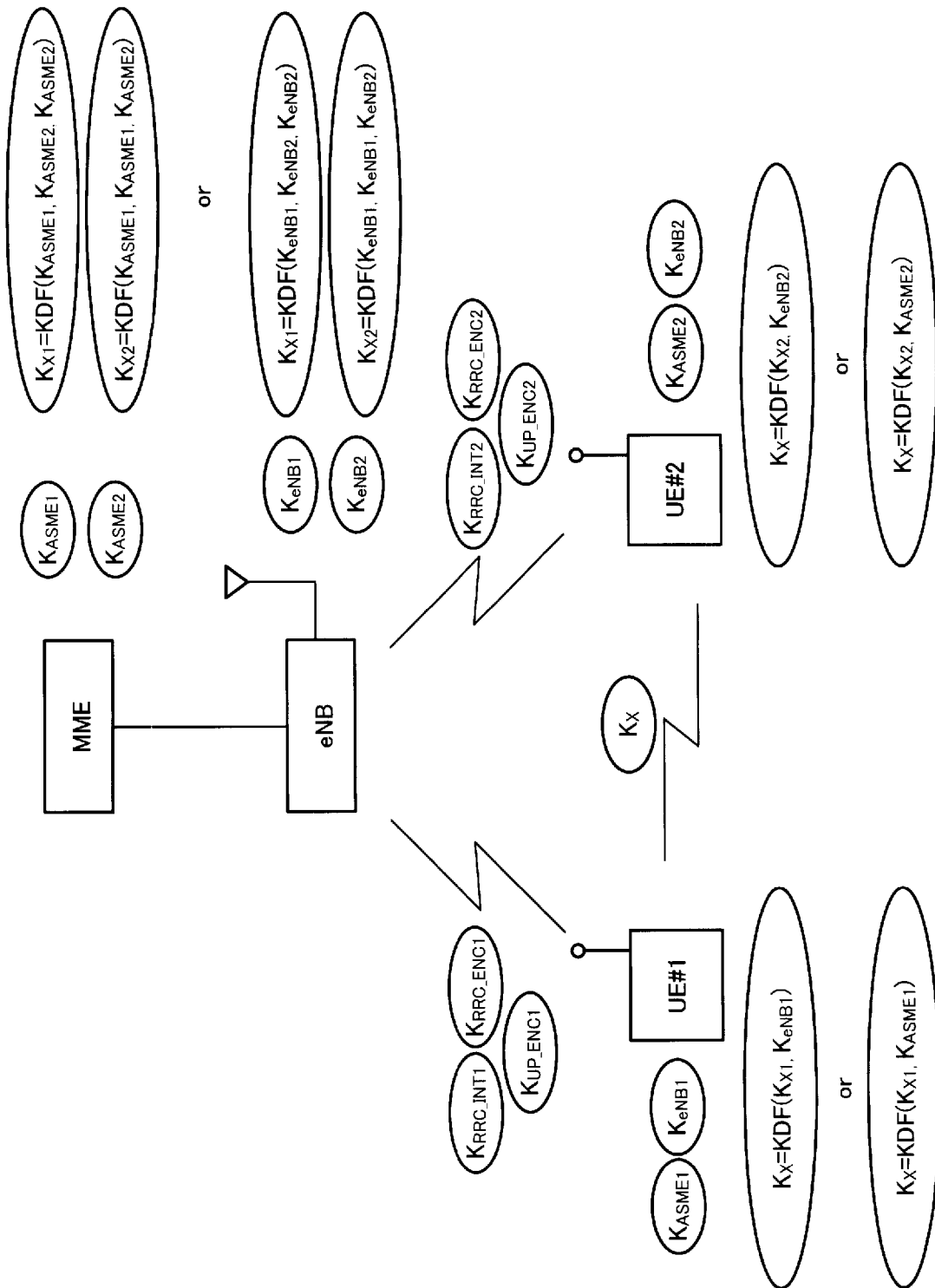
[図2]



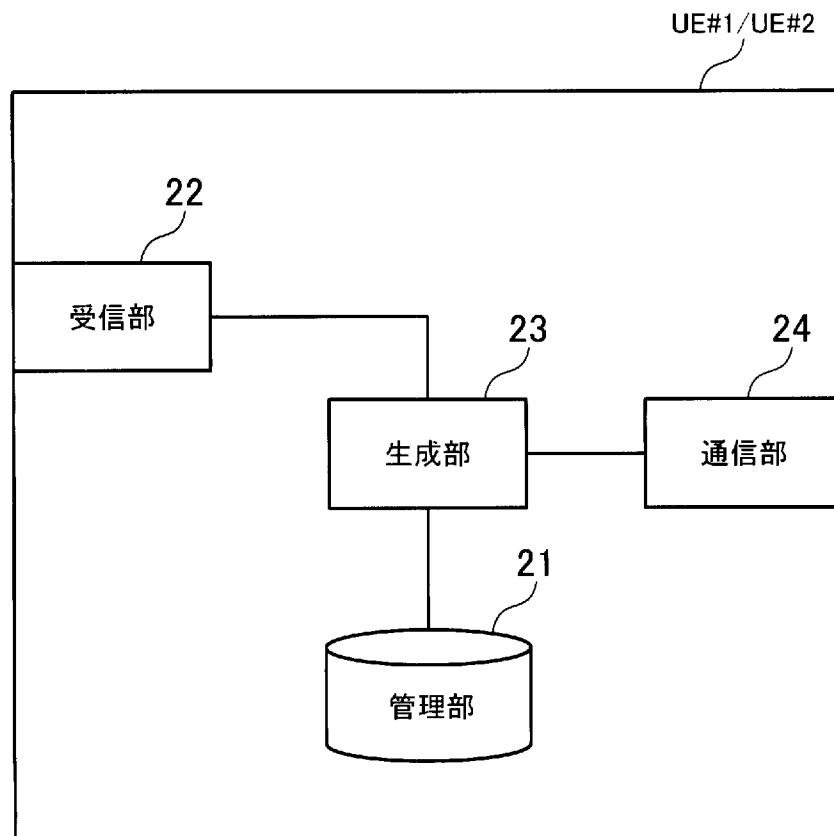
[図3]



[図4]



[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/057982

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/04(2009.01)i, H04W92/18(2009.01)i

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)

H04B7/24-7/26, H04W4/00-99/00

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

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.
X	JP 2005-303449 A (Buffalo Inc.),	9
Y	27 October 2005 (27.10.2005),	10
A	paragraphs [0002], [0003], [0035], [0037], [0038], [0040], [0041], [0044] (Family: none)	1-8
Y	JP 2008-227846 A (Ricoh Co., Ltd.), 25 September 2008 (25.09.2008), paragraphs [0017], [0032] (Family: none)	10
A	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 10), 3GPP TS 33.401 V10.0.0 (2011-03), 2011.03, P.23-26	1-8



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
19 April, 2012 (19.04.12)

Date of mailing of the international search report
01 May, 2012 (01.05.12)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04W12/04(2009.01)i, H04W92/18(2009.01)i

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（I P C））

Int.Cl. H04B7/24-7/26, H04W4/00-99/00

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 2 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 2 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 2 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
X Y A	JP 2005-303449 A（株式会社バッファロー） 2005. 10. 27, 段落 2, 3, 35, 37, 38, 40, 41, 44（ファミリーなし）	9 10 1-8
Y	JP 2008-227846 A（株式会社リコー） 2008. 09. 25, 段落 17, 32（ファミリーなし）	10

☒ C 欄の続きにも文献が列挙されている。☐ 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矛盾するものではなく、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

1 9 . 0 4 . 2 0 1 2

国際調査報告の発送日

0 1 . 0 5 . 2 0 1 2

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

中村 信也

5 J

4 0 5 8

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 3 4

C (続き) . 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	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution(SAE); Security architecture (Release 10), 3GPP TS 33.401 V10.0.0(2011-03), 2011.03, P.23-26	1-8