平成２７年６月１１日判決言渡　同日原本領収　裁判所書記官

平成２６年（行ケ）第１０２１２号　審決取消請求事件

口頭弁論終結日　平成２７年５月１４日

判　　決

原　　告	テレフオンアクチーボラゲット エル エム エリクソン（パブル）
訴訟代理人弁護士	髙　梨　義　幸
訴訟代理人弁理士	稲　葉　良　幸
同	佐　藤　睦
同	笹　本　真　理　子
被　　告	特　許　庁　長　官　X
指　定　代　理　人	石　井　茂　和
同	木　村　貴　俊
同	相　崎　裕　恒
同	根　岸　克　弘

主　　文

１　原告の請求を棄却する。

２　訴訟費用は原告の負担とする。

３　この判決に対する上告及び上告受理の申立てのための付加期間を３０日と定める。

事実及び理由

第１　請求

特許庁が不服２０１２－１６３９１号事件について平成２６年４月３０日に

した審決を取り消す。

第２　事案の概要

１　特許庁における手続の経緯等

(1)　原告は，発明の名称を「電気通信システムにおける方法および構成」とする発明について，２００８年（平成２０年）５月２０日（優先権主張日２００７年（平成１９年）９月１７日，米国）を国際出願日とする特許出願（特願２０１０－５２４８２０号。以下「本願」という。）をした。

原告は，平成２４年４月１９日付けの拒絶査定（甲７）を受けたため，同年８月２３日，拒絶査定不服審判を請求した。

(2)　特許庁は，上記請求を不服２０１２－１６３９１号事件として審理を行い，平成２６年４月３０日，「本件審判の請求は，成り立たない。」との審決（出訴期間の付加期間９０日。以下「本件審決」という。）をし，同年５月１２日，その謄本が原告に送達された。

(3)　原告は，平成２６年９月９日，本件審決の取消しを求める本件訴訟を提起した。

２　特許請求の範囲の記載

本願の特許請求の範囲の請求項１の記載は，次のとおりである（以下，請求項１に係る発明を「本願発明」という。甲４）。

「【請求項１】　次世代パケットシステムＥＰＳのモビリティ管理エンティティ（１３）MMEにおいて，ユーザ装置（１１）ＵＥと前記ＵＥにサービスするｅＮｏｄｅＢ（１２）との間のＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーK__ｅＮＢを確立する方法であって，以下の

－　ＮＡＳサービス要求を前記ＵＥから受信するステップ（３２，５２）であって，前記要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ__U__ＳＥＱを示すステップと，

－　少なくとも前記受信されたＮＡＳ__U__ＳＥＱから，および前記ＵＥと

共有される，記憶されたアクセスセキュリティ管理エンティティキーK__ＡＳＭＥから，前記セキュリティキーK__ｅＮＢを導出するステップ（３３，５３）と，

－　前記導出されたK__ｅＮＢを，前記ＵＥにサービスする前記ｅＮｏｄｅＢ（１２）に転送するステップ（３４）と，を含む，ＭＭＥにおける方法。」

３　本件審決の理由の要旨

(1)　本件審決の理由は，別紙審決書（写し）記載のとおりである。要するに，本願発明は，本願の優先権主張日前に頒布された刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明，すなわち，「3GPP, Universal Mobile Telecommunications System (UMTS);Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN);Overall description;Stage 2(3GPP TS 36.300 version 8.1.0 Release 8), [online], ２００７年　６月，p.11-15, 58, 59；ＵＲＬ，http://www.etsi.org/deliver/etsi_ts/136300_136399/136300/08.01.00_60/ts_136300v080100p.pdf」（以下「引用刊行物１」又は「3GPP TS 36.300 version 8.1.0 Release 8」という。甲１）に掲載された発明等に基づいて当業者が容易に発明をすることができたものであって，特許法２９条２項の規定により特許を受けることができないから，本願は拒絶すべきものであるというものである。

(2)　本件審決が認定した引用刊行物１に記載された発明（以下「引用発明」という。），本願発明と引用発明の一致点及び相違点は，以下のとおりである。

ア　引用発明

「ＵＥと，ＵＥに対する資源の動的配置，ユーザ・データ・ストリームを暗号化するｅＮＢと，ｅＮＢへのページング・メッセージの分配，セキュリティ制御，及び，ＮＡＳ信号伝達の暗号化と完全性保護を行うＭＭＥとを有する無線通信システムにおいて，

ＵＥとMMEは，Ｋ＿ＡＳＭＥという名の基本鍵を共有し，前記Ｋ＿ＡＳＭＥからＫ＿ｅＮＢが得られ，

前記Ｋ＿ｅＮＢを得るために，シーケンス番号が使用され，

前記Ｋ＿ｅＮＢは，MMEから，ｅＮＢに送信される，方法。」

イ　本願発明と引用発明の一致点

「次世代パケットシステムＥＰＳのモビリティ管理エンティティMMEにおいて，ユーザ装置ＵＥと前記ＵＥにサービスするｅＮｏｄｅＢとの間のＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立する方法であって，

シーケンス番号と，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから，前記セキュリティキーＫ＿ｅＮＢを導出するステップと，

前記導出されたＫ＿ｅＮＢを，前記ＵＥにサービスする前記ｅＮｏｄｅＢに転送するステップ，とを含む方法。」である点。

ウ　本願発明と引用発明の相違点

“シーケンス番号”に関して，

本願発明においては，「ＮＡＳサービス要求を前記ＵＥから受信するステップ（３２，５２）であって，前記要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップ」において，「ＵＥ」側から「MME」側が受信する「アップリンクシーケンス番号」であるのに対して，

引用発明においては，「シーケンス番号」が，「ＵＥ」から，「MME」への「アップリンクシーケンス番号」であるか否かが明確でない点。

第３　当事者の主張

１　原告の主張

(1)　取消事由１（引用発明及び一致点の認定の誤り）

引用刊行物１（甲１）には，「K__ｅＮＢ」を得るために，「シーケンス番号」（sequence number）が使用される構成についての開示はないから，本件審決が認定した引用発明のうち，「前記K__ｅＮＢを得るために，シーケンス番号が使用され」との部分は誤りであり，本件審決が引用発明が上記部分の構成を有することを前提に，「シーケンス番号と，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーK__ＡＳＭＥから，前記セキュリティキーK__ｅＮＢを導出するステップ」を本願発明と引用発明の一致点と認定したことも誤りである。

ア　引用発明の認定の誤り

本件審決は，引用刊行物１（甲１）の「A given sequence number must only be used once for a given eNB key」との記載を「得られたシーケンス番号は，ｅＮＢ鍵を得るために使用されるのは，一度のみでなければならない」と和訳（以下「本件和訳」という場合がある。）した上で，上記記載箇所から「“ｅＮＢ鍵を得るために，シーケンス番号が使用される”ことが読み取れる。」と認定したが，以下のとおり誤りである。

(ア)　引用刊行物１の「A given sequence number must only be used once for a given eNB key」との記載は，「所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，一度のみでなければならない」と訳すべきである。上記記載中の「for a given eNB key」の部分を本件和訳のように「ｅＮＢ鍵を得るために」を意味すると解する余地はない。仮に「得るために」と英語表記するのであれば，「to get」，「to obtain」又は「to derive」などの語を用いるはずであるが，そのような語は用いられていない。

したがって，本件審決が上記記載箇所について本件和訳をし，上記記載箇所から「“ｅＮＢ鍵を得るために，シーケンス番号が使用される”ことが読み取れる。」と認定したのは誤りである。

(イ) 次に,「A given sequence number must only be used once for a given eNB key」との記載の前後の文脈からみても,本件和訳は誤りである。

a 引用刊行物１の「14 Security」の「14.1 Overview and Principles」(「１４ セキュリティ」の「１４．１ 概説及び原則」)には,以下のとおり,Ｅ－ＵＴＲＡＮのセキュリティに適用される６つの原則(「第１原則」ないし「第６原則」)が記載されており,「A given sequence number must only be used once for a given eNB key」との記載は,第５原則の第２文の一部である。

「- The eNB keys are cryptographically separated from the EPC keys used for NAS protection (making it impossible to use the eNB key to figure out an EPC key).」(以下「第１原則」という。)

「- The keys are derived in the EPC/UE from key material that was generated by a NAS (EPC/UE) level AKA procedure.」(以下「第２原則」という。)

「- The eNB keys are sent from the EPC to the eNB when the UE is entering LTE_ACTIVE state (i.e. during RRCconnection or S1 context setup).」(以下「第３原則」という。)

「- Key material for the eNB keys is sent between the eNBs during LTE_ACTIVE intra-E-UTRAN mobility.」(以下「第４原則」という。)

「- A sequence number is used as input to the ciphering and integrity protection. A given sequence number must only be used once for a given eNB key (except for identical re-transmission). The same sequence number can be used for both ciphering and integrity protection.」(以下「第５原則」という。)

「- A hyper frame number (HFN) (i.e. an overflow counter mechanism) is used in the eNB and UE in order to limit the actual number of sequence number bits that is needed to be sent over the radio. The HFN needs to be synchronized between the UE and eNB.」（以下「第６原則」という。）

b　引用刊行物１の「１４．１　概説及び原則」は，Ｅ－ＵＴＲＡＮのセキュリティ手続全体の概説及び原則を述べたものである。

「１４．１　概説及び原則」記載の第１原則ないし第４原則はｅＮＢ鍵の生成や配送について，第５原則は，鍵を用いて暗号化及び完全性保護を実現すること，当該手続にシーケンス番号を用いることについて，第６原則はＨＦＮの取り決めについてそれぞれ述べたものである。

第５原則は，第１文において「A sequence number is used as input to the ciphering and integrity protection.」（「シーケンス番号は，暗号化及び完全性保護のための入力として用いられる。」）と記載し，第３文において「The same sequence number can be used for both ciphering and integrity protection.」（「同一のシーケンス番号が，暗号化と完全性保護の両方に用いることができる。」）と記載しているように，暗号化及び完全性保護の手続，すなわち「鍵を用いる」手続について述べたものであるから，その第２文である「A given sequence number must only be used once for a given eNB key」についても，同様に暗号化及び完全性保護の手続について述べたものと理解すべきであり，これを「鍵の生成」について述べたものと理解することは極めて不自然であって，恣意的な解釈であるといわざるを得ない。

c　「１４．１　概説及び原則」の最終段落には，「From K_ASME, the NAS, (and indirectly) K_eNB keys are derived. The K_ASME never leaves the EPC, but the K_eNB key is transported to the eNB fr

om the EPC when the UE transitions to LTE_ACTIVE. From the K_eNB, the eNB and UE can derive the UP and RRC keys.」（「K__ＡＳＭＥから，ＮＡＳ（そして，間接的に），K__ｅＮＢが得られる。K__ＡＳＭＥは，決して，ＥＰＣから離れない。しかしながら，K__ｅＮＢ鍵は，ＵＥが，ＬＴＥ__ＡＣＴＩＶＥに移行すると，ＥＰＣからｅＮＢに運ばれる。K__ｅＮＢから，ｅＮＢ，及び，ＵＥは，ＵＰ，及び，ＲＲＣ鍵を得ることができる。」）との記載がある。この記載から，ＥＰＣにおいて得られたK__ｅＮＢがｅＮＢに運ばれ，ｅＮＢ及びＵＥにおいて，当該K__ｅＮＢを基にしてＵＰ鍵及びＲＲＣ鍵を得ていることが明らかである。

そして，ＵＥとｅＮＢ間のプロトコルで用いられる鍵は，引用刊行物１の「Figure 14.1-1」（別紙１参照）に示すとおり，K__ｅＮＢの下位の鍵である$K_{eNB-UP-enc}$（ＵＰ鍵），$K_{eNB-RRC-enc}$（ＲＲＣ鍵）及び$K_{eNB-RRC-int}$（ＲＲＣ鍵）であり，このうち，$K_{eNB-UP-enc}$及び$K_{eNB-RRC-enc}$は暗号化に用いられる鍵である。

また，引用刊行物１（3GPP TS 36.300 version 8.1.0 Release 8）の後のバージョンの甲８(3GPP TS 36.300 version 8.8.0 Release 8)に「A sequence number (COUNT) is used as input to the ciphering and integrity protection.」との記載があることからすると，第５原則の第２文中の「A given sequence number」にいう「sequence number」とは「ＣＯＵＮＴ」を意味する。

さらに，引用刊行物１の後のバージョンの甲９の１（3GPP TS 36.323 version 1.0.0 Release 8）には，シーケンス番号の一種である「ＣＯＵＮＴ」が，暗号化及び完全性保護のパラメータとして，K_{RRCenc}，K_{UPenc}及びK_{RRCint}のようなｅＮＢ鍵の下位の鍵と共に用いられることが示されている。

そうすると，第５原則は，第１文において，シーケンス番号が暗号化及び完全性保護の入力として用いられること，第２文において，ある所与のシーケンス番号が，（暗号化及び完全性保護に用いられる際に，）ある所与のｅＮＢ鍵を基にして得られたＵＰ鍵（$K_{eNB-UP-enc}$）及びＲＲＣ鍵（$K_{eNB-RRC-enc}$，$K_{eNB-RRC-int}$）のために用いられるのは一度でなければならないこと，第３文において，所与のｅＮＢ鍵（正確には，その下位のＵＰ鍵及びＲＲＣ鍵）が暗号化及び完全性保護の手続に用いられることを述べたものといえる。

ｄ　以上によれば，引用刊行物１の「A given sequence number must only be used once for a given eNB key」（第５原則第２文）との記載は，暗号化及び完全性保護の手続について述べたものであって，シーケンス番号がｅＮＢ鍵の生成のために用いられることを述べたものではないから，本件審決がした本件和訳は誤りである。

（ウ）　以上のとおり，本件審決が引用刊行物１の「A given sequence number must only be used once for a given eNB key」（第５原則第２文）との記載について本件和訳をし，上記記載箇所から「“ｅＮＢ鍵を得るために，シーケンス番号が使用される”ことが読み取れる。」と認定したのは誤りである。

引用刊行物１には，他に「K__ｅＮＢ」を導出する手法についての開示はないから，「K__ｅＮＢを得るために，シーケンス番号が使用され」る構成についての開示はない。

したがって，本件審決が認定した引用発明のうち，「前記K__ｅＮＢを得るために，シーケンス番号が使用され」との部分は誤りである。

イ　一致点の認定の誤り

本件審決が，「シーケンス番号と，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーK__ＡＳＭＥから，前

記セキュリティキーK＿ｅＮＢを導出するステップ」を本願発明と引用発明の一致点と認定したのは誤りである。

(ア)　前記ア(ウ)のとおり，引用刊行物１には，「K＿ｅＮＢを得るために，シーケンス番号が使用され」る構成についての開示はないから，引用発明は，「シーケンス番号と，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーK＿ＡＳＭＥから，前記セキュリティキーK＿ｅＮＢを導出するステップ」の構成を有するものとはいえない。

したがって，本件審決が上記構成を本願発明と引用発明の一致点と認定したのは誤りである。

(イ)ａ　本願の優先権主張日時点における当業者の技術常識によれば，引用発明における「シーケンス番号」には，本願発明の「ＮＡＳ＿Ｕ＿ＳＥＱ」は含まれない。

すなわち，前記ア(イ)ｃのとおり，引用刊行物１記載の第５原則の第２文中の「A given sequence number」にいう「sequence number」とは，「ＣＯＵＮＴ」を意味するものであり，「ＣＯＵＮＴ」はＨＦＮ及びＰＤＣＰシーケンス番号から構成されるものであるから，「ＮＡＳ＿Ｕ＿ＳＥＱ」とは異なるシーケンス番号である。

また，第５原則は，「Ｅ－ＵＴＲＡＮ」すなわち「ＵＥ」と「ｅＮＢ」間のネットワークのセキュリティについて述べたものであるのに対し（引用刊行物１のFigure4）（別紙１参照），「ＮＡＳ」は，「ＵＥ」と「MME」との間のプロトコルであり（同Figure4.3.2）（別紙１参照），本願発明と引用発明とは，「シーケンス番号」が用いられるプロトコルが異なるから，「シーケンス番号」の意味が異なることは，当業者にとって自明である。

したがって，引用発明における「シーケンス番号」には，本願発明

の「ＮＡＳ＿Ｕ＿ＳＥＱ」は含まれないから，本件審決が，「シーケンス番号と，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから，前記セキュリティキーＫ＿ｅＮＢを導出するステップ」を本願発明と引用発明の一致点と認定したのは誤りである。

b　被告は，これに対し，引用発明における「シーケンス番号」に「ＮＡＳ＿Ｕ＿ＳＥＱ」が含まれる旨主張する。

しかしながら，「シーケンス番号」という用語は，様々な場面で用いられるものであり，単に「シーケンス番号」といっても，その意味は一義的ではなく，一般的にシーケンス番号と整理されるものが全て引用発明における「シーケンス番号」に含まれるなどと解することはできない。

被告は，単に抽象論を述べるのみで，具体的な論証を一切行っていないから，被告の上記主張は失当である。

(2)　取消事由２（相違点の看過）

本願発明は，「ＮＡＳサービス要求を前記ＵＥから受信するステップ（３２，５２）であって，前記要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップ」の構成を有するが，本件審決は，引用発明が上記構成を有することを認定していないから，上記構成を本願発明と引用発明の相違点として認定すべきであったのに，この相違点の認定を看過した誤りがある。

そして，本件審決は，上記相違点の容易想到性について判断を示していない。

(3)　取消事由３（相違点の容易想到性の判断の誤り）

本件審決は，本件審決が認定した相違点について，引用発明，国際公開第２００６／１１６６２０号（２００６年１１月２日公開。以下「引用刊行物２」という。甲２の１）に記載の発明及び周知技術も共に，無線通信におけ

るパケット伝送のセキュリティに関するものであるから，「シーケンス番号」を「ＵＥ」側から「MME」に送信する必要がある場合に，「シーケンス番号」を「ＵＥ」から「MME」に送信するよう構成することは，当業者が適宜なし得る事項であり，本願発明と引用発明との相違点は格別のものではない旨判断したが，以下に述べるとおり，本件審決の上記判断は誤りである。

ア(ア)　前記(1)ア(ウ)のとおり，引用刊行物１（甲１）には，「Ｋ＿ｅＮＢを得るために，シーケンス番号が使用され」る構成についての開示はない。同様に，引用刊行物２（甲２の１）及び本件審決が認定した周知技術（「「ＵＥ」から，「MME」に対して「ＲＲＣ／ＮＡＳ信号」を送信する点」）のいずれにも，「Ｋ＿ｅＮＢを得るために，シーケンス番号が使用され」る構成についての開示も示唆もない。

また，仮に引用刊行物１に「Ｋ＿ｅＮＢを得るために，シーケンス番号が使用され」る構成の開示があるとしても，引用刊行物１には，Ｋ＿ｅＮＢを得るためにＮＡＳサービス要求で示される「ＮＡＳ＿Ｕ＿ＳＥＱ」をシーケンス番号として用いることの開示はない。同様に，引用刊行物２及び本件審決が認定した周知技術のいずれにおいても，ＮＡＳサービス要求で示される「ＮＡＳ＿Ｕ＿ＳＥＱ」をＫ＿ｅＮＢの生成のために用いることについての開示や示唆はない。

したがって，引用発明に引用刊行物２記載の発明及び本件審決が認定した構成を組み合わせても，当業者が相違点に係る本願発明の構成を容易に想到することができたものとはいえない。

（イ）　被告は，これに対し，乙２，４ないし７の記載を根拠として挙げて，シーケンス番号を使用して鍵を生成することによって効率的に鍵を共有することができることが，セキュリティの分野における技術常識であったこと，ＵＥからのアップリンクにシーケンス番号が含まれていることは広く知られていることからすると，このようなアップリンクに含まれるシーケ

ンス番号のうち，具体的に何を使用するかは，結局のところ，使用できるものの中から適宜選択すべきことにすぎないとして，当業者が相違点に係る本願発明の構成を容易に想到することができた旨主張する。

しかしながら，被告の上記主張は，引用刊行物１に全く記載のない事項について，乙２，４ないし７に記載されていることを理由に引用刊行物１に同じことが記載されている旨主張するに等しいものであり，また，公知の技術について，何らの論証もないまま殊更引用刊行物１に開示された構成を上位概念化するものであって不当である。

したがって，被告の上記主張は理由がない。

イ　本件審決は，本願発明と引用発明との相違点は格別のものではないと判断したが，その判断に際し，本願発明が引用発明と比べて顕著な効果を奏することを考慮していないから，上記判断は誤りである。

すなわち，前記ア(ア)のとおり，引用刊行物１には，Ｋ＿ｅＮＢを得るためにＮＡＳサービス要求で示される「ＮＡＳ＿Ｕ＿ＳＥＱ」をシーケンス番号として用いることの開示はない。

これに対し，本願の願書に添付した明細書（以下，図面を含めて「本願明細書」という。甲４）には，「ＮＡＳ＿Ｄ＿ＳＥＱ」を用いる場合には，「ＮＡＳメッセージ」の損失に起因する「ＵＥにおける誤ったＮＡＳ＿Ｄ＿ＳＥＱ」に基づく「Ｋ＿ｅＮＢ」生成が行われるおそれがあり（段落【０００７】），また，「別個のシーケンス番号」を用いる場合には，「再生攻撃を防ぐために，別個のシーケンス番号をＵＥおよびMMEの両方において保持しなければならない」といった「特別な複雑さ」を要するが（段落【０００８】），本願発明は，「Ｋ＿ｅＮＢ」の生成に「ＮＡＳ＿Ｕ＿ＳＥＱ」を使用することにより，「MMEからＵＥへの明示的なダウンリンクＮＡＳサービス受理メッセージまたはシーケンス番号が必要ではないこと，およびＮＡＳセキュリティコンテキストの再生保護機能が，ＲＲＣおよびＵＰセキュ

リティコンテキストにおいて再利用されること」（段落【００１１】）といった顕著な効果を奏することが開示されている。

しかるところ，本件審決は，本願発明の上記顕著な効果を考慮することなく，本願発明と引用発明との相違点は格別のものではないと判断したのであるから，本件審決の上記判断は誤りである。

ウ　以上によれば，本件審決における相違点の容易想到性の判断には誤りがある。

(4)　まとめ

以上によれば，本件審決には，引用発明及び一致点の認定の誤り，相違点の看過，相違点の容易想到性の判断の誤りがあり，その結果，本件審決は，本願発明は特許法２９条２項の規定により特許を受けることができないと誤った判断をしたものである。

したがって，本件審決は，違法であるから，取り消されるべきものである。

２　被告の主張

(1)　取消事由１（引用発明及び一致点の認定の誤り）に対し

ア　引用発明の認定について

(ア)　引用刊行物１がＬＴＥに関する規格として発行された技術文書であることに照らせば，本件審決が，第５原則の第１文と第３文については，逐語的な直訳を示す一方で，第２文については「ｅＮＢ鍵を得るために…が使用される」と訳し，逐語的な直訳を示さなかったことは不適切であったものといえる。

しかしながら，本件審決は，第５原則の第２文の「A given sequence number must only be used once for a given eNB key」の「for a given eNB key」との部分のみから「ｅＮＢ鍵を得るために」との訳を導いたわけではない。「use」の動詞は，「用いる」ないし「使用する」を意味するが，「use」の目的ないし態様は文脈によって異なる。第２文中の

「be used…for a given eNB key」の「ｅＮＢ鍵のために使用される」との記載が，引用刊行物１の「１４．１　概説及び原則」記載のｅＮＢ鍵の生成，共有，配送について主として述べている文脈中に存在しており，「ｅＮＢ鍵の生成のために」使用される趣旨を含むことから，このことを踏まえて意訳し，文脈に即して「ｅＮＢ鍵を得るために…が使用される」と訳したものであり，誤訳ではない。

すなわち，引用刊行物１の「１４．１　概説及び原則」には，「Ｅ－ＵＴＲＡＮのセキュリティに適用される」べき６つの「原則」（第１原則ないし第６原則）が記載されるとともに，ＡＫＡ（判決注:認証及び鍵共有のためのプロトコル）実行の結果としてＥＰＣとＵＥがＫ＿ＡＳＭＥという名称の基本鍵を共有する旨，Ｋ＿ＡＳＭＥからＫ＿ｅＮＢが得られる旨，Ｋ＿ＡＳＭＥはＥＰＣから離れないのに対して，Ｋ＿ｅＮＢは，（ＵＥがＬＴＥ＿ＡＣＴＩＶＥに移行すると）ＥＰＣからｅＮＢに運ばれる旨等が「概説」されている。そして，第１原則ないし第３原則は，「概説」された内容をさらに抽象化したものであり，第１原則には，（Ｅ－ＵＴＲＡＮ（ＵＥ／ｅＮＢ）のセキュリティにおいて用いられる）ｅＮＢ鍵は，ＮＡＳ保護のために用いられるＥＰＣ鍵から分離されることが，第２原則には，これらの「鍵」が「ＥＰＣ／ＵＥ」において「鍵素材」から得られる（つまりＥＰＣだけでなくＵＥにおいても鍵生成が行われる）とともに，その「鍵素材」は，「ＮＡＳレベルＡＫＡ手続」によって生成される旨が，第３原則には，ＵＥがＬＴＥ＿ＡＣＴＩＶＥ状態に入るとｅＮＢ鍵がＥＰＣからｅＮＢに送られる旨がそれぞれ示されており，また，第５原則には，「シーケンス番号」を用いることを前提として，第１文では「暗号化，及び，完全性保護のための入力」という最も抽象的なレベルでの目的ないし態様が示され，第２文では「あるｅＮＢ鍵」につき「一度のみ」しか用いることができない旨及び第３文

では同じシーケンス番号を暗号化と完全性保護の両方に用いることができる旨が示されているから，引用刊行物１の「１４．１　概説及び原則」は，ｅＮＢ鍵の生成，共有，配送について主として述べたものといえる。

また，第５原則は，Ｋ＿ｅＮＢとその派生鍵（ｅＮＢ鍵）が，ＮＡＳ保護のために用いられるＥＰＣ鍵から分離され，ＮＡＳレベルで行われる「認証及び鍵共有」のために用いられない旨を示した第１原則を受けて，Ｋ＿ｅＮＢが「認証及び鍵共有」の後の「暗号化」と「完全性保護」のために用いられる旨を述べたものである。要するに，第５原則は，第１原則の裏返しとして，Ｋ＿ｅＮＢが「認証及び鍵共有」のために用いられることはなく，「暗号化」と「完全性保護」のために用いられることを示すとともに，そのようなＫ＿ｅＮＢに関して，「暗号化」と「完全性保護」のために入力される「シーケンス番号」を本来独立であるべき複数の「鍵」間で共通に使用してはならないという原則（セキュリティの分野では当たり前のこと）を述べるとともに，「暗号化」のために用いた「シーケンス番号」を当該「暗号化」に用いた鍵と同じ鍵を用いてされる「完全性保護」においても用いることができることを述べたものである。

さらに，シーケンス番号を使用して鍵を生成することによって効率的に鍵を共有することができることは，本願の優先権主張日当時，セキュリティの分野における技術常識であったものである。例えば，①乙４（国際公開２００７／０４６３７６号）の段落【００２７】，【００２９】及び【００４７】には，「所定の契機でカウントアップされる「鍵更新カウンタ値（Ｎｃ）」というシーケンス番号を使用して送信の際の暗号化のための暗号鍵Ｋｃと受信の際の復号のための復号鍵Ｋｃを生成していること」が，②乙５（特表２００３－５２９２８８号公報）の段落【０００４】ないし【０００６】には，「暗号化送信に用いるキーを発

生するにあたって，カウンタのカウント値Ｒというシーケンス番号を用いていること」が，③乙６（特開平１１－１０９８５４号公報）の段落【００６８】，【００７２】，【００７３】，【００７７】，【００８０】及び【００９５】には，「発呼側装置と被呼側装置との間の暗号通信に使用される通信用暗号鍵の生成に用いられる乱数に限らず「シーケンス番号」を用いてもよいこと」が，④乙７（特表平４－５０５６９４号公報）の１１頁右上欄５行～１２行，１１頁左下欄２２行～１２頁左上欄１７行及び図４には，「暗号化のために用いられるキーストリームを発生するためにカウント２１３，２１４というシーケンス番号を用いていること」が記載されている。これらの文献は，シーケンス番号を使用して鍵を生成することによって効率的に鍵を共有することができることを示している。

以上の引用刊行物１の記載及び技術常識を踏まえれば，当業者であれば，第５原則第２文中の「be used…for a given eNB key」の「ｅＮＢ鍵のために使用される」との記載がｅＮＢ鍵の生成，共有，配送について主として述べている文脈中に存在しながら，「ｅＮＢ鍵の生成のために」使用される趣旨を含んでいないと解釈することはできず，むしろ，その趣旨を含むものと解釈するものである。

したがって，本件審決がした本件和訳は，逐語的な直訳を示さなかった点では不適切であったものの，誤訳とはいえないから，本件和訳に基づいてした本件審決の引用発明の認定にも誤りはない。

（イ） 原告は，これに対し，引用刊行物１の後のバージョンである甲８及び甲９の１を踏まえると，第５原則の第２文中の「A given sequence number」にいう「sequence number」とは「ＣＯＵＮＴ」を意味し，第２文は，ある所与のシーケンス番号（「ＣＯＵＮＴ」）が，（暗号化及び完全性保護に用いられる際に，）ある所与のｅＮＢ鍵を基にして得られたＵＰ

鍵（$K_{eNB-UP-enc}$）及びＲＲＣ鍵（$K_{eNB-RRC-enc}$，$K_{eNB-RRC-int}$）のために用いられるのは一度でなければならないことを述べたものであり，本件和訳は誤訳である旨主張する。

しかしながら，本願の優先権主張日前に発行された乙２（3GPP TS 33.102 version 7.1.0 Release 7）には，シーケンス番号には，部分的に時間を基にしたもの，時間を基にしていないもの，完全に時間を基にしたものが存在することが記載されており，上記記載によれば，「シーケンス番号」という用語は，「シーケンス番号」としての属性を有するこれらの様々なものを当該属性に即した上位概念として示す用語であることを理解することができる。

そうすると，「シーケンス番号」は，規格として定められた特定のパラメータを指すことが明示されているのであればともかく，そうでない限りは，規格とされた文献あるいは規格とされていない文献における特定のパラメータを示すものということはできない。

甲８及び甲９の１は，引用刊行物１の発行後にＬＴＥに関する規格として発行された技術文書であるが，引用刊行物１には「sequence number（シーケンス番号）」が「ＣＯＵＮＴ」である旨の記載はもちろん，「ＣＯＵＮＴ」というパラメータの定義自体が存在しないから，引用刊行物１の発行時点では，「ＣＯＵＮＴ」というパラメータやこのようなパラメータの利用方法が規格とされていなかったものといえるものであり,引用刊行物１に接した当業者が「sequence number(シーケンス番号)」が「ＣＯＵＮＴ」を意味し，他のシーケンス番号ではあり得ないと考えることはない。また，仮に原告が主張するように発行時点より後に規格とされた技術文書の内容を取り込む解釈が許容されることになれば，甲８において「特定的でない参照」として参照されている乙３（3GPP TS 33.401 version 8.3.1 Release 8）の図６．２－２（別紙２参照）には，

MMEにおいてK_{ASME}からK_{eNB}を生成するに当たって「ＮＡＳ　ＵＰＬＩＮＫ　ＣＯＵＮＴ」という「シーケンス番号」を用いることが図示されているから，引用刊行物１にその旨が記載されていると認定することすら可能であることになる。

したがって，原告の上記主張は，理由がない。

イ　一致点の認定について

(ア)　前記ア(ア)のとおり，引用刊行物１の記載からみて，第５原則の第２文がｅＮＢ鍵の生成，共有，配送について主として述べている文脈において「A given sequence number…be used for a given eNB keys…」（シーケンス番号は…ｅＮＢ鍵のために使用される…）と記載しているものであって，「ｅＮＢ鍵のために」使用される旨の記載がｅＮＢ鍵の生成，共有，配送について主として述べている文脈中に存在しながら「ｅＮＢ鍵の生成のために」使用される趣旨を含んでいないと解釈することはできない。本件審決は，このことを踏まえて，本件和訳をしたものであり，本件和訳に誤りはなく，本件審決の引用発明の認定に誤りはない。

したがって，本件審決が「シーケンス番号…から，前記セキュリティキーＫ＿ｅＮＢを導出する」点を本願発明と引用発明の一致点と認定したことに誤りはない。

(イ)　原告は，これに対し，引用刊行物１記載の第５原則の第２文中の「A given sequence number」にいう「sequence number」とは，「ＣＯＵＮＴ」を意味するものであり，「ＣＯＵＮＴ」はＨＦＮ及びＰＤＣＰシーケンス番号から構成されるものであるから，「ＮＡＳ＿Ｕ＿ＳＥＱ」とは異なるシーケンス番号である，第５原則は，「Ｅ－ＵＴＲＡＮ」すなわち「ＵＥ」と「ｅＮＢ」間のネットワークのセキュリティについて述べたものであるのに対し，「ＮＡＳ」は，「ＵＥ」と「MME」との間のプロト

コルであり，本願発明と引用発明とは，「シーケンス番号」が用いられるプロトコルが異なるから，「シーケンス番号」の意味が異なることは，当業者にとって自明であるとして，引用発明における「シーケンス番号」には，本願発明の「ＮＡＳ＿Ｕ＿ＳＥＱ」は含まれないから，本件審決の一致点の認定に誤りがある旨主張する。

しかしながら，前記ア(イ)のとおり，引用刊行物１の「シーケンス番号」は，「シーケンス番号」としての属性を有する様々なものを当該属性に即した上位概念を示す用語であり，本願発明の「ＮＡＳ＿Ｕ＿ＳＥＱ」が「シーケンス番号」としての属性を有する情報であれば，これが含まれないということはできない。本件審決は，相違点の判断において，「シーケンス番号」とその下位概念である「ＮＡＳ＿Ｕ＿ＳＥＱ」とが区別されることを前提として説示したが，この区別は，「ＮＡＳ＿Ｕ＿ＳＥＱ」がその上位概念である「シーケンス番号」としての属性を有することを前提としたものである。

また，前記ア(イ)のとおり，引用刊行物１の発行時点では，「ＣＯＵＮＴ」というパラメータやこのようなパラメータの利用方法が規格とされていなかったから，引用刊行物１に接した当業者が「sequence number（シーケンス番号）」が「ＣＯＵＮＴ」を意味し，他のシーケンス番号ではあり得ないと考えることはない。

さらに，本願発明の特許請求の範囲（請求項１）の「次世代パケットシステムＥＰＳのモビリティ管理エンティティ（１３）MMEにおいて，ユーザ装置（１１）ＵＥと前記ＵＥにサービスするｅＮｏｄｅＢ（１２）との間のＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立する方法」との記載によれば，本願発明は「ＵＥ」と「ｅＮＢ」間のセキュリティに係るものであるから，引用刊行物１が「ＵＥ」と「ｅＮＢ」間のセキュリティについて述べたものであることは，

本願発明と引用発明とが異なるプロトコルについて述べたものであることの根拠にならない。

したがって，原告の上記主張は理由がない。

ウ　小括

以上によれば，原告主張の取消事由１は理由がない。

(2)　取消事由２（相違点の看過）に対し

ア　本件審決は，引用刊行物１の摘記箇所において，本願発明の「ＮＡＳサービス要求を前記ＵＥから受信するステップ」に対応する構成が明記されていないことを踏まえて，これを一致点と認定せずに，相違点と認定した上で，相違点の判断を示している。

本件審決は，相違点の判断において，「ＵＥ」からのアップリンクに「シーケンス番号」を含ませることも，当業者には知られた技術であると判断している。「ＵＥ」からのアップリンクに「シーケンス番号」を含ませることは，「ＵＥ」から上位局（ＵＥより「網側」の局）が受信するアップリンクに「シーケンス番号」を含ませることを意味するものであり，「ＵＥ」から様々な「アップリンク」が上位局に送信され，これを上位局が受信することを前提とするものである。

したがって，「ＵＥ」からのアップリンクに「シーケンス番号」を含ませることも,当業者には知られた技術であるとの本件審決の上記判断には,「ＵＥ」からの「アップリンク」を上位局が受信する技術が当業者に知られた技術であるとの判断が前提に含まれている。

イ　また，引用刊行物１（甲１，乙１）には，「ＮＡＳダイレクト・メッセージ」が「ＵＥ」から「（MME中の）ＮＡＳ」へ転送する(transfer)こと（７．１），「初期直接転送(Initial Direct Transfer)」という「ＮＡＳメッセージ（NAS message）」が「ＲＲＣ接続要求（RRC connection request)に結びつけられる（concatenated)こと（７．３）が記載され，さら

に，ＲＲＣコネクション要求とＮＡＳサービス要求とがＵＥからｅＮＢに送られ，その後にｅＮＢからMMEへ送られた後にＳ１インターフェース（ｅＮＢとMMEとの間の通信）におけるコンテキストセットアップ手順が始まる様子（図１９．２．２．３）（別紙１参照）が図示されている。

これらによれば，「ＵＥ」から「ＲＲＣコネクション要求」とともに「ｅＮＢ」を経由して送られる「初期直接転送」という「ＮＡＳメッセージ」ないし「ＮＡＳサービス要求」を，MMEが受信するものと理解することができる。

そうすると，引用刊行物１の上記記載内容に照らせば，「ＮＡＳサービス要求をＵＥから受信するステップ」は，本願発明と引用発明との一致点であると整理することもできる。

ウ　以上によれば，本件審決の相違点の認定に誤りはなく，また，事実上，「ＮＡＳサービス要求を前記ＵＥから受信するステップ」に対応する構成を一致点と整理しても，本件審決の論旨の大枠が崩れることはなく，本件審決の結論にも影響しない。

したがって，原告主張の取消事由２は理由がない。

(3)　取消事由３（相違点の容易想到性の判断の誤り）に対し

ア　前記(1)ア(ア)のとおり，引用刊行物１には，第５原則第２文において，「ｅＮＢ鍵を得るためにシーケンス番号が使用される」構成が開示されている。

そして，前記(1)ア(ア)のとおり，シーケンス番号を使用して鍵を生成することによって効率的に鍵を共有することができることは，セキュリティの分野における技術常識であり，また，引用刊行物２（甲２の１）に示されているように，ＵＥからのアップリンクにシーケンス番号が含まれていることは広く知られている。

そうすると，このようなアップリンクに含まれるシーケンス番号のうち，

具体的に何を使用するかは，結局のところ，使用できるものの中から適宜選択すべきことにすぎない。

しかるところ，前記(2)のとおり，引用刊行物１には「ＮＡＳサービス要求をＵＥから受信するステップ」が事実上記載されているということができるところ，このＵＥからの「ＮＡＳサービス要求」は，ＵＥとｅＮＢとの暗号化等を用いた通信の前提となるＲＲＣコンテキストがセットアップされる前にＲＲＣコネクションリクエストとともに行われるから，ＮＡＳサービス要求に含まれるシーケンス番号は，暗号化等を用いた通信を開始することが可能となる前の段階で追加のコストを要せず必然的にＵＥとＭＭＥとの双方で利用可能となる。暗号化等に用いる鍵を生成するための情報は，暗号化等を用いた通信を開始する前の段階でＵＥとMMEの双方においてが利用可能である必要があるが，「ＮＡＳサービス要求」に含まれるシーケンス番号は，追加のコストを要せずこの要件を満たすものなのであって，その意味では，これを利用することが望ましいものといえる。

以上によれば，相違点は格別のものではなく，相違点に係る本願発明の構成は容易想到であるとした本件審決の判断に誤りはない。

イ　原告は，これに対し，本願明細書には，本願発明は，「Ｋ＿ｅＮＢ」の生成に「ＮＡＳ＿Ｕ＿ＳＥＱ」を使用することにより，「MMEからＵＥへの明示的なダウンリンクＮＡＳサービス受理メッセージまたはシーケンス番号が必要ではないこと，およびＮＡＳセキュリティコンテキストの再生保護機能が，ＲＲＣおよびＵＰセキュリティコンテキストにおいて再利用されること」（段落【００１１】）といった顕著な効果を奏することが開示されているが，本件審決が本願発明と引用発明との相違点は格別のものではないと判断するに際し，本願発明が引用発明と比べて顕著な効果を奏することを考慮していないから，上記判断は誤りである旨主張する。

しかしながら，MMEからＵＥへの明示的なダウンリンクＮＡＳサービ

ス受理メッセージが必要でないことは，本願明細書記載の従来技術及び引用刊行物１に記載された技術において既に達成されていた効果であって（本願明細書の段落【００２６】ないし【００２８】，図１，引用刊行物１の「１９．２．２．３」参照。），本願発明に特有のものではない。

また，「ユーザ装置（１１）ＵＥと前記ＵＥにサービスするｅＮｏｄｅＢ（１２）との間のＲＲＣ／ＵＰトラフィックを保護するため」の「セキュリティキーＫ＿ｅＮＢ」の「確立」のための「別個のシーケンス番号」の必要がなくなることは，シーケンス番号としてＮＡＳメッセージに含まれるシーケンス番号（ＮＡＳセキュリティコンテキストの再生保護機能）を用いたことによる予想どおりの効果にすぎず，格別なものでない。

したがって，原告の上記主張は，その前提を欠くものであり，理由がない。

(4)　まとめ

以上のとおり，原告主張の取消事由はいずれも理由がないから，本願発明は特許法２９条２項の規定により特許を受けることができないとした本件審決の判断に誤りはない。

第４　当裁判所の判断

１　取消事由１（引用発明及び一致点の認定の誤り）について

(1)　本願明細書の記載事項について

ア　本願発明の特許請求の範囲（請求項１）の記載は，前記第２の２のとおりである。

イ　本願明細書（甲４）の「発明の詳細な説明」には，次のような記載がある（下記記載中に引用する図面について別紙本願明細書図面を参照）。

(ア)　「【技術分野】

技術分野

本発明は，電気通信システムにおける方法および構成に関し，特に，

ＵＥによってトリガされたサービス要求のための，ＥＰＳ（次世代パケットシステム），すなわちＥ－ＵＴＲＡＮ（次世代UMTＳ地上無線アクセスネットワーク）およびＥＰＣ（次世代パケットコアネットワーク）におけるセキュリティソリューションに関する。より具体的には，本発明は，ＥＰＳ（次世代パケットシステム）用のMME（モビリティ管理エンティティ）およびＵＥ（ユーザ装置）において，ＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーを確立する方法および構成に関する。」（段落【０００１】）

（イ）「【背景技術】

背景

ＥＰＳアーキテクチャでは，加入者認証は，ＵＥとMME（モビリティ管理エンティティ）との間で実行され，かつMMEは，例えば，モビリティ，ＵＥ識別情報，およびセキュリティパラメータを管理する。ＥＰＳにおけるセキュリティ手順を定義するための基礎は，セキュリティキーK__ＡＳＭＥであり，このキーは，MMEとＵＥとの間で共有され，かつＵＥの認証において確立される。ＡＳＭＥ（アクセスセキュリティ管理エンティティ）と呼ばれる，ＥＰＳアーキテクチャの機能エンティティは，例えばMMEと同じ場所に配置してもよく，ＡＳＭＥは，ホームネットワークに制限されたＣＫ／ＩＫキーから導出されたセキュリティキーK__ＡＳＭＥを受信および記憶する。ＡＳＭＥは，セキュリティキーK__ＡＳＭＥから，ＮＡＳシグナリング，すなわち次世代パケットコア（ＥＰＣ）ネットワークのMMEとＵＥとの間の非アクセス層シグナリングを保護するために用いられるＮＡＳセキュリティコンテキストを導出する。ＮＡＳセキュリティコンテキストには，K__ＮＡＳ__ｅｎｃ，K__ＮＡＳ__ｉｎｔなど，ＮＡＳシグナリングの暗号化および完全性保護用のパラメータ，ならびにＮＡＳ__Ｕ__ＳＥＱおよびＮＡＳ__Ｄ

＿ＳＥＱなど，アップリンクおよびダウンリンクシーケンス番号が含まれ，シーケンス番号は，暗号化および完全性保護手順への入力だけでなく，古いメッセージの再生を防ぐために用いられる。ＡＳＭＥは，ＭＭＥにＮＡＳセキュリティコンテキストを提供し，１つのＮＡＳセキュリティコンテキストが，ＭＭＥに保持され，対応するＮＡＳセキュリティコンテキストが，ＵＥに保持され，再生保護，完全性保護および暗号化は，ＭＭＥおよびＵＥのＮＡＳセキュリティコンテキストのシーケンス番号が，再使用されないことに基づいている。」（段落【０００２】）

「ＵＥとサービスｅＮｏｄｅＢ（すなわち，ＥＰＳアーキテクチャにおける無線基地局）との間のＵＰ／ＲＲＣトラフィックを保護するためのセキュリティコンテキストもまた，前記セキュリティキーＫ＿ＡＳＭＥに基づくのが好ましい。ＵＰ／ＲＲＣセキュリティコンテキストを確立する手順には，Ｋ＿ｅＮＢと呼ばれるキーであって，これから，暗号化キーＫ＿ｅＮＢ＿ＵＰ＿ｅｎｃが，ＵＰ（ユーザ平面）すなわちＥＰＣおよびＥ－ＵＴＲＡＮ上で転送されるエンドユーザデータを保護するために導出されるキー，ならびにＲＲＣ（無線資源制御）を保護するための暗号化キーＫ＿ｅＮＢ＿ＲＲＣ＿ｅｎｃおよび完全性保護キーＫ＿ｅＮＢ＿ＲＲＣ＿ｉｎｔを導出することが含まれる。」（段落【０００３】）

「図１は，ＥＰＳアーキテクチャにおける，ＵＥが開始したアイドルからアクティブへの状態遷移のための従来の例示的なシグナリングフローを示す。アイドルＵＥは，ＥＰＳのＥＰＣ（次世代パケットコア）だけに認識されており，ＵＰ／ＲＲＣセキュリティコンテキストは，ｅＮｏｄｅＢとＵＥとの間には存在しない。アクティブ状態におけるＵＥは，ＥＰＣおよびＥＵＴＲＡＮの両方において認識されており，ＵＰ／ＲＲＣセキュリティコンテキストが，ＵＥとそのサービスｅＮｏｂｅＢとの

間でＵＰ／ＲＲＣトラフィックを保護するために確立された。」（段落【０００４】）

「図１は，ＵＥ１１，ｅＮｏｄｅＢ１２，MME１３，サービスGW（ゲートウェイ）１４，ＰＤＮゲートウェイ１５，およびＨＳＳ（ホーム加入者サーバ）１６を示す。サービスゲートウェイ１４は，ＥＵＴＲＡＮに向かってインタフェースを終端するＥＰＣのノードであり，ＰＤＮゲートウェイは，ＰＤＮ（パケットデータネットワーク）に向かってインタフェースを終端するＥＰＣのノードである。ＵＥが複数のＰＤＮにアクセスする場合には，そのＵＥのために複数のＰＤＮゲートウェイがあってもよい。信号Ｓ１および信号Ｓ２では，ＮＡＳサービス要求は，ＵＥからMMEへ透過的に転送され，かつＮＡＳサービス要求は，ＮＡＳ＿Ｕ＿ＳＥＱに基づいて，完全性が保護される。オプションの信号Ｓ３では，ＵＥは，MMEによって認証され，Ｋ＿ＡＳMEは，ＨＳＳ（ホーム加入者サーバ）に記憶された加入者データを用いて確立され，MMEは，Ｓ４で，初期コンテキストセットアップ要求をｅＮｏｄｅＢに送信する。信号Ｓ５およびＳ６では，ｅＮｏｄｅＢは，ＵＥとの無線ベアラを確立してアップリンクデータを転送し，信号Ｓ７で，初期コンテキストセットアップ完了メッセージをMMEへ返す。信号Ｓ８では，MMEは，更新ベアラ要求をサービスGWに送信し，サービスGWは，信号Ｓ９で応答する。」（段落【０００５】）

「従来のソリューションでは，ＲＲＣ／ＵＰセキュリティコンテキスト用の，ＵＥおよびMMEによるＫ＿ｅＮＢの導出は，例えば，MMEからＵＥに送信されたＮＡＳサービス受理メッセージまたは他の明示的な情報に基づいている。しかしながら，図１における例示的な従来のＥＰＳシグナリングフローに示されているように，MMEは，通常，ＥＰＳにおいて，ＵＥからＮＡＳサービス要求を受信しても，いかなるＮＡ

Ｓサービス受理も送信しない。したがって，ＮＡＳサービス受理メッセージにおける情報からＫ＿ｅＮＢを導出することは不可能である。」（段落【０００６】）

「例示的な公知のソリューションによれば，Ｋ＿ｅＮＢは，ＮＡＳサービス受理メッセージにおいてＭＭＥによって用いられるＫ＿ＡＳＭＥおよびＮＡＳ＿Ｄ＿ＳＥＱからＭＭＥによって導出され，ＵＥは，ＮＡＳサービス受理メッセージからシーケンス番号ＮＡＳ＿Ｄ＿ＳＥＱを検索し，かつＭＭＥと同じＫ＿ｅＮＢ導出を実行することによって，同じＫ＿ｅＮＢを導出する。ＭＭＥは，それがｅＮｏｄｅＢへのＳ１接続を設定する場合に，Ｋ＿ｅＮＢをｅＮｏｄｅＢに転送する。しかしながら，この公知のソリューションの欠点は，明示的なＮＡＳサービス受理メッセージがＭＭＥからＵＥに対して定義されない場合には，図１における例示的な従来のＥＰＳシグナリングフローにおけるように，ＵＥが，ＭＭＥと同じＫ＿ｅＮＢを導出することは不可能であることである。たとえＵＥが，現在のＮＡＳダウンリンクシーケンス番号ＮＡＳ＿Ｄ＿ＳＥＱを推定することが技術的に可能であっても，この推定は誤っている可能性がある。なぜなら，ＭＭＥは，損失してＵＥによって決して受信されなかったＮＡＳメッセージを送信したかもしれないからである。かかる場合には，ＭＭＥは，そのＮＡＳ＿Ｄ＿ＳＥＱを更新し，ＵＥが，この更新に気づくこともなく，ＵＥにおける誤ったＮＡＳ＿Ｄ＿ＳＥＱにつながることになろう。」（段落【０００７】）

「別の例示的な公知のソリューションによれば，Ｋ＿ｅＮＢの導出は，特にＫ＿ｅＮＢの導出のために保持される別個のシーケンス番号に基づき，このシーケンス番号は，ＵＥがそれをＭＭＥに送信するかまたはＭＭＥがそれをＵＥに送信することによって，ＮＡＳサービス要求手順の間に明示的に同期される。しかしながら，このソリューションの欠点は，

別個のシーケンス番号の特別な複雑さである。なぜなら，再生攻撃を防ぐために，別個のシーケンス番号をＵＥおよびMMEの両方において保持しなければならないからである。」（段落【０００８】）

（ウ）「【発明が解決しようとする課題】

概要

本発明の目的は，上記で概説した課題に取り組むことであり，この目的および他の目的は，独立請求項による方法および構成ならびに従属請求項による実施形態によって達成される。」（段落【０００９】）

（エ）「【課題を解決するための手段】

本発明の基本的な考えは，Ｋ＿ｅＮＢが，Ｋ＿ＡＳMEから，およびＵＥからMMEへのＮＡＳサービス要求メッセージのＮＡＳ＿Ｕ＿ＳＥＱから導出され，それによって，ｅＮｏｄｅＢにおけるＵＰ／ＲＲＣセキュリティコンテキストの確立をトリガするということである。」（段落【００１０】）

「MMEからＵＥへの明示的なダウンリンクＮＡＳサービス受理メッセージまたはシーケンス番号が必要ではないこと，およびＮＡＳセキュリティコンテキストの再生保護機能が，ＲＲＣおよびＵＰセキュリティコンテキストにおいて再利用されることが，本発明の利点である。」（段落【００１１】）

「一態様によれば，本発明は，次世代パケットシステムＥＰＳのモビリティ管理エンティティMMEにおいて，ユーザ装置ＵＥとＵＥにサービスするｅＮｏｄｅＢとの間のＲＲＣ／ＵＰトラフィックを保護するためにセキュリティキーＫ＿ｅＮＢを確立する方法を提供する。この方法には，ＵＥからＮＡＳサービス要求を受信するステップであって，この要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップと，少なくとも前記受信されたＮＡＳ＿Ｕ＿ＳＥＱから，およ

び前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥからセキュリティキーＫ＿ｅＮＢを導出するステップと，前記導出されたＫ＿ｅＮＢを，前記ＵＥにサービスするｅＮｏｄｅＢに転送するステップと，が含まれる。」（段落【００１２】）

「第２の態様によれば，本発明は，次世代パケットシステムＥＰＳ用のモビリティ管理エンティティＭＭＥを提供する。ＭＭＥは，ＵＥとＵＥにサービスするｅＮｏｄｅＢとの間のＲＲＣ／ＵＰトラフィックを保護するために，セキュリティキーＫ＿ｅＮＢを確立するように構成される。ＭＭＥには，ＵＥからＮＡＳサービス要求を受信するための手段であって，この要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示す手段と，少なくとも前記受信されたＮＡＳ＿Ｕ＿ＳＥＱから，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥからＫ＿ｅＮＢを導出するための手段と，ならびに，前記導出されたＫ＿ｅＮＢを，前記ＵＥにサービスするｅＮｏｄｅＢに送信するための手段と，が含まれる。」（段落【００１３】）

「第１および第２の態様は，さらに，方法および対応する手段を提供し，これらに従って，ＭＭＥが，擬似乱数関数ＰＲＦを用いてＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥからＫ＿ｅＮＢを導出可能になる。ＭＭＥは，さらに，受信された下位ビットから完全なＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを再構成し，ＵＥから受信されたＮＡＳサービス要求の完全性を検査してもよい。さらに，ＭＭＥは，受信されたＮＡＳ＿Ｕ＿ＳＥＱの通知をＵＥに返してもよく，ＮＡＳ＿Ｕ＿ＳＥＱは，Ｋ＿ｅＮＢをｅＮｏｄｅＢに転送するセットアップメッセージに含まれていてもよい。それによって，ＵＥは，ＭＭＥに送信されるＮＡＳ＿Ｕ＿ＳＥＱを覚えている必要がない。」（段落【００１４】）

（オ）「【発明を実施するための形態】

詳細な説明

以下の説明では，本発明の完全な理解を提供するために，特定のアーキテクチャおよびステップシーケンスなどの特定の詳細が記載される。しかしながら，本発明が，これらの特定の詳細から逸脱する可能性がある他の実施形態において実行し得ることは，当業者には明らかである。」（段落【００２０】）

「本発明の概念は，セキュリティキーＫ＿ｅＮＢが，アクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから，およびＵＥからＭＭＥに送信されるＮＡＳサービス要求メッセージのアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱから導出され，それによって，ｅＮｏｄｅＢにおいてＵＰ／ＲＲＣセキュリティコンテキストの確立をトリガするということである。」（段落【００２２】）

「ＵＥがアイドルモードにある場合には，ＮＡＳセキュリティコンテキストが，存在しかつ例えば，上記のＫ＿ＮＡＳ＿ｅｎｃ，Ｋ＿ＮＡＳ＿ｉｎｔ，ＮＡＳ＿Ｕ＿ＳＥＱ，およびＮＡＳ＿Ｄ＿ＳＥＱを含み，ＮＡＳメッセージは，完全性および場合により機密性を保護される。したがって，ＮＡＳセキュリティコンテキストにはまた，ＵＥのセキュリティ能力，特に暗号化および完全性アルゴリズムが含まれる。」（段落【００２３】）

「ＮＡＳメッセージの保護は，ＮＡＳセキュリティキーＫ＿ＮＡＳ＿ｅｎｃ，Ｋ＿ＮＡＳ＿ｉｎｔ，ならびにメッセージの方向についてアップリンクおよびダウンリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱまたはＮＡＳ＿Ｄ＿ＳＥＱに基づいている。完全なシーケンスカウンタは，通常，ＮＡＳメッセージと共に送信されず，下位ビットいくつかだけであり，完全なシーケンス番号は，上位ビットの局所推定および受信され

た下位ビットから，受信端で再構成される。」（段落【００２４】）

「図１における従来のシグナリング図のＳ１およびＳ２では，ＮＡＳサービス要求は，アップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱを含むが，ＵＥからMMEに転送され，ＮＡＳサービス要求メッセージは，前記ＮＡＳ＿Ｕ＿ＳＥＱに基づいて完全性が保護される。MMEは，メッセージの完全性を検査し，それが再生でない場合には，それを受理し，これによって，ＮＡＳ＿Ｕ＿ＳＥＱが，新しく以前に用いられなかったことが保証される。」（段落【００２６】）

「その後，本発明によれば，MMEは，少なくとも，受信されたアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱおよびＫ＿ＡＳＭＥに基づき，従来のキー導出関数を用いて，Ｋ＿ｅＮＢを導出するが，これは，図１に示す従来のシグナリング図には含まれない。したがって，シーケンスカウンタは，認証においてのみリセットしてもよい。MMEは，信号Ｓ４のメッセージ，初期コンテキストセットアップ要求（Ｓ１－ＡＰ）で，またはそこに相乗りして，導出されたＫ＿ｅＮＢをｅＮｏｄｅＢに送信する。」（段落【００２７】）

「信号Ｓ５では，ｅＮｏｄｅＢは，無線ベアラ確立およびセキュリティ構成メッセージ（セキュリティモードコマンド）をＵＥに送信する。図１におけるように，これらのメッセージは，２つの別個のメッセージとして，または１つのメッセージに組み合わせて送信してもよく，ＵＥによるこれらのメッセージの受信は，暗黙のうちに，信号Ｓ１におけるＵＥのＮＡＳサービス要求の確認になる。セキュリティモードコマンドは，例えば，保護がいつ開始すべきかおよびどのアルゴリズムを用いるべきかを決定する。」（段落【００２８】）

「本発明によれば，ＵＥは，信号Ｓ５でメッセージを受信すると，以前に実行されていない場合には，少なくともＮＡＳ＿Ｕ＿ＳＥＱおよび

K__ＡＳＭＥに基づき，従来のキー導出関数を用いて，K__ｅＮＢを導出する。その後，ｅＮｏｄｅＢおよびＵＥは，ＵＰ／ＲＲＣセキュリティコンテキストを確立するが，これは，図１における従来のシグナリング図には示されていない。」（段落【００２９】）

（カ）「図２は，本発明の第１の実施形態を示すが，この場合には，ＵＥは，信号Ｓ２４におけるK__ｅＮＢの導出のために，信号Ｓ２１における初期ＮＡＳサービス要求メッセージのＮＡＳ__Ｕ__ＳＥＱを保持する。MMEは，信号Ｓ２１でＵＥからＮＡＳ__Ｕ__ＳＥＱを受信するか，またはＮＡＳ__Ｕ__ＳＥＱを示す下位ビットだけを受信し，ＮＡＳ__Ｕ__ＳＥＱおよびK__ＡＳＭＥに基づいてＳ２２においてK__ｅＮＢを導出する。MMEは，導出されたK__ｅＮＢを信号Ｓ２３でｅＮｏｄｅＢに転送する。」（段落【００３２】）

「その後，図２には示していないが，ｅＮｏｄｅＢおよびＵＥは，K__ｅＮＢを用いてＵＰ／ＲＲＣセキュリティコンテキストを確立するが，ＵＰ／ＲＲＣセキュリティコンテキストには，ＵＰトラフィックを保護するための暗号化キーK__ｅＮＢ__ＵＰ__ｅｎｃ，ならびにＲＲＣトラフィックの保護のための暗号化キーおよび完全性保護キー，K__ｅＮＢ__ＲＲＣ__ｅｎｃおよびK__ｅＮＢ__ＲＲＣ__ｉｎｔがそれぞれ含まれ，それによって，信号Ｓ２５において安全なＵＰ／ＲＲＣトラフィックを可能にする。」（段落【００３３】）

「K__ｅＮＢの導出は，従来のキー導出関数によって，例えば擬似乱数関数K__ｅＮＢ＝ＰＲＦ（K__ＡＳＭＥ，ＮＡＳ__Ｕ__ＳＥＱ，．．．）によって，実行される。」（段落【００３４】）

（キ）「図３は，本発明による方法を示す流れ図であり，ステップ３１において，ＵＥ１１は，初期ＮＡＳサービス要求メッセージをMME１３に送信するが，このメッセージは，通常，カウンタの下位ビットだけを

送信することによって，ＮＡＳアップリンクシーケンスカウンタＮＡＳ＿Ｕ＿ＳＥＱを示す。ステップ３２において，ＭＭＥは，ＵＥからＮＡＳサービス要求メッセージを受信し，ＮＡＳ＿Ｕ＿ＳＥＱを取得し，受信された下位ビットから完全なシーケンスを再構成する。ステップ３３において，ＭＭＥは，適切なキー導出関数，例えば擬似乱数関数を用いて，少なくとも受信したＮＡＳ＿Ｕ＿ＳＥＱ，およびＡＳＭＥ（アクセスセキュリティモビリティエンティティ）からのＫ＿ＡＳＭＥから，セキュリティキーＫ＿ｅＮＢを導出する。」（段落【００３６】）

「その後，ＭＭＥは，ステップ３４において，ＵＥと共有される完全なＵＰ／ＲＲＣセキュリティコンテキストを確立するためにｅＮｏｄｅＢによって用いられるように，導出されたＫ＿ｅＮＢをｅＮｏｄｅＢ１２に転送する。ステップ３５において，前記ＵＥは，少なくとも記憶されたＫ＿ＡＳＭＥから，およびステップ３１においてＵＥからＭＭＥに送信された初期ＮＡＳサービス要求メッセージのＮＡＳ＿Ｕ＿ＳＥＱから，同じＫ＿ｅＮＢを導出し，導出されたＫ＿ｅＮＢからＵＰ／ＲＲＣセキュリティコンテキストを確立する。」（段落【００３７】）

「本発明の第１の実施形態では，ＵＥは，初期ＮＡＳサービス要求メッセージでＭＭＥに送信されたＮＡＳ＿Ｕ＿ＳＥＱを記憶し，記憶されたシーケンス番号を用いてＫ＿ｅＮＢを導出する。」（段落【００３８】）

（ク）　「図６ａは，本発明に従って，ＥＰＳ用のＭＭＥ１３（モビリティ管理エンティティ）を示すが，このＭＭＥ１３は，ＵＥとサービスｅＮｏｄｅＢとの間のＵＰ／ＲＲＣトラフィックを保護するためのセキュリティコンテキスト用のセキュリティキーＫ＿ｅＮＢを確立するようにさらに構成される。ＭＭＥには，図示していないが，ＥＰＳにおけるノードと，例えばＳ１－ＭＭＥインタフェースを介してｅＮｏｄｅＢｓと通

信するための従来の通信手段が設けられる。さらに，図１のMMEでは，ＡＳME（アクセスセキュリティ管理エンティティ）６１が，破線によって示されている。なぜなら，ＥＰＳのこの機能エンティティは，MMEと同じ場所に配置してもよいからである。」（段落【００４３】）

「セキュリティキーK__ｅＮＢを確立するための，図６ａに示すMME１３の手段には，（ＵＥのサービスｅＮｏｄｅＢを介した）ＵＥからのＮＡＳ__U__ＳＥＱを含むＮＡＳサービス要求メッセージを受信するために受信手段６２と，従来のキー導出関数を用い，少なくとも受信されたＮＡＳ__U__ＳＥＱおよび記憶されたK__ＡＳMEに基づいて，セキュリティキーK__ｅＮＢを導出するためのキー導出手段６３と，導出されたK__ｅＮＢを，ＵＥにサービスするｅＮｏｄｅＢに送信するための送信手段６４と，が含まれる。」（段落【００４４】）

「図６ｂは，本発明によるＵＥ１１（ユーザエンティティ）を示すが，ＵＥは，ＥＰＳ用に構成され，さらに，ＵＥのサービスｅＮｏｄｅＢと交換されるＵＰ／ＲＲＣトラフィックを保護するためのセキュリティコンテキスト用のセキュリティキーK__ｅＮＢを確立するように構成される。ＵＥには，そのサービスｅＮｏｄｅＢへのＬＴＥ－Ｕｕインタフェースを介してＥＰＳにおけるノードと通信するための従来の通信手段（図示せず）が設けられる。」（段落【００４５】）

「セキュリティキーK__ｅＮＢを確立するための，図６ｂに示すＵＥ１１の手段には，サービスｅＮｏｄｅＢを介して，ＮＡＳサービス要求メッセージをMMEに送信するための送信手段６６であって，この要求が，アップリンクシーケンス番号ＮＡＳ__U__ＳＥＱを示す手段が含まれ，セキュリティキーK__ｅＮＢを確立するための手段には，従来のキー導出関数を用い，少なくともＮＡＳ__U__ＳＥＱおよび記憶されたK__ＡＳMEに基づいて，セキュリティキーK__ｅＮＢを導出するための

キー導出手段６７が含まれる。」（段落【００４６】）

ウ　前記ア及びイによれば，本願明細書には，本願発明に関し，以下の点が開示されていることが認められる。

（ア）　ＥＰＳ（次世代パケットシステム）においてＵＥが開始したアイドルからアクティブへの状態遷移のための従来の例示的なシグナリングフロー（別紙本願明細書図面の図１参照）においては，ＭＭＥとＵＥとの間の非アクセス層シグナリングを保護するためにＮＡＳセキュリティコンテキストが用いられ，ＵＥとサービスｅＮｏｄｅＢとの間のＵＰ／ＲＲＣトラフィックを保護するためにＵＰ／ＲＲＣセキュリティコンテキストが用いられる（段落【０００２】ないし【０００４】）。ＵＰ／ＲＲＣセキュリティコンテキストを確立する手順には，Ｋ＿ｅＮＢと呼ばれるキーが導出され，Ｋ＿ｅＮＢから，エンドユーザデータを保護するための暗号化キーＫ＿ｅＮＢ＿ＵＰ＿ｅｎｃ，ＲＲＣ（無線資源制御）を保護するための暗号化キーＫ＿ｅＮＢ＿ＲＲＣ＿ｅｎｃ及び完全性保護キーＫ＿ｅＮＢ＿ＲＲＣ＿ｉｎｔを導出することが含まれる（段落【０００３】）。

従来のソリューションでは，ＲＲＣ／ＵＰセキュリティコンテキスト用のＵＥ及びＭＭＥによるＫ＿ｅＮＢの導出は，例えば，ＭＭＥからＵＥに送信されたＮＡＳサービス受理メッセージ又は他の明示的な情報に基づいているが，従来の例示的なシグナリングフローにおいては，ＭＭＥは，通常，ＥＰＳにおいて，ＵＥからＮＡＳサービス要求を受信しても，いかなるＮＡＳサービス受理も送信しないため，ＮＡＳサービス受理メッセージにおける情報からＫ＿ｅＮＢを導出することは不可能であった（段落【０００６】）。また，別の例示的な公知のソリューションによれば，Ｋ＿ｅＮＢの導出は，Ｋ＿ｅＮＢの導出のために保持される別個のシーケンス番号を，ＵＥがＭＭＥに送信するか，または，ＭＭＥ

がＵＥに送信することによって行われるが，別個のシーケンス番号をＵＥ及びMMＥの両方において保持しなければならないため，複雑であるという欠点があった（段落【０００８】）。

（イ） 本願発明のMMＥにおける方法は，従来のＲＲＣ／ＵＰセキュリティコンテキスト用のＵＥ及びMMＥによるＫ＿ｅＮＢの導出における上記課題を解決することを目的とし，Ｋ＿ｅＮＢが，アクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから，及びＵＥからMMＥに送信されるＮＡＳサービス要求メッセージのアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱから導出され，それによって，ｅＮｏｄｅＢにおいてＵＰ／ＲＲＣセキュリティコンテキストの確立をトリガするようにするため（段落【００２２】），ＮＡＳサービス要求を前記ＵＥから受信するステップ（３２）であって，前記要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップと，少なくとも前記受信されたＮＡＳ＿Ｕ＿ＳＥＱから，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから，前記セキュリティキーＫ＿ｅＮＢを導出するステップ（３３）と，前記導出されたＫ＿ｅＮＢを，前記ＵＥにサービスする前記ｅＮｏｄｅＢ（１２）に転送するステップ（３４）と，を含む構成を採用した。

（ウ） 本願発明は，MMＥからＵＥへの明示的なダウンリンクＮＡＳサービス受理メッセージ又はＫ＿ｅＮＢの導出のために保持される別個のシーケンス番号を必要とせず，また，ＮＡＳセキュリティコンテキストの再生保護機能が，ＲＲＣ及びＵＰセキュリティコンテキストにおいて再利用されるという利点を有する（段落【００１１】）。

(2) 引用刊行物１の記載事項について

引用刊行物１（甲１，乙１）には，次のような記載がある（「図面」については別紙１を参照）。

ア　「ＥＵＴＲＡＮのアーキテクチャを，以下の図４に示す。

４．１　機能の分割

ｅＮＢは，次の機能を実施する：

－　無線機能管理のための機能：無線ベアラ制御，無線アドミッション制御，接続モビリティ管理，アップリンクと，ダウンリンクの双方における，ＵＥのための資源の動的配置（スケジューリング）；

－　ＩＰヘッダの圧縮，及び，ユーザ・データ・ストリームの暗号化；

－　ＵＥ接続時の，ＭＭＥの選択；

注：　ＵＥ接続時，はじめにMMEは，含まれている，即ち，実質的には，MMEは選択されていると，仮定する。

－　サービス・ゲートウェイへのユーザ・プレーン・データのルーティング；

注：　どのノードがユーザ・プレーン・トンネルを実際に設立するかは，次の検討である。

注：　ユーザ・プレーン・トンネルの確立が，ＲＲＣ起動と共に起こるかどうかは，次の検討である。

－　（MMEからのものである）ページング・メッセージのスケジューリングと送信；

－　（MME，或いは，O&Mからのものである）ブロードキャスト情報のスケジューリングと送信；

－　モビリティ，及び，スケジューリングのための測定と，計測報告の設定.

MMEは，次の機能を実施する：

－　ｅＮＢへのページング・メッセージの分配；

－　セキュリティ制御；

－　アイドル状態モビリティ制御；

－　ＳＡＥベアラ制御；

－　ＮＡＳ信号伝達の暗号化と完全性保護.

サービス・ゲートウェイは次の機能を実施する：

－　ページング理由のための，Ｕ－プレーン・パケットの終端（次の検討である）；

－　ＵＥモビリティのサポートのためのＵ－プレーンの切替.」（甲１抄訳）

「４．３．２　制御プレーン

下の図（判決注・図４．３．２）は，制御プレーンのためのプロトコル・スタックを示している，それは，

－　（ネットワーク側のｅＮＢで終端される）ＰＤＣＰサブレイヤは，ユーザプレーンと同様のセキュリティ機能を実行するが，ヘッダの圧縮は実行しない；

－　（ネットワーク側のｅＮＢで終端される）ＲＬＣおよびＭＡＣサブレイヤは，ユーザプレーンと同様の機能を実行する；

－　（ネットワーク側のｅＮＢで終端される）ＲＲＣは，従属節７に一覧されている機能を実行する，たとえば：

－　ブロードキャスト；

－　ページング；

－　ＲＲＣ接続管理；

－　ＲＢ制御；

－　モビリティ機能；

－　ＵＥ測定報告および制御；

－　（ネットワーク側のMMEで終端されている）ＮＡＳ制御プロトコルは，とりわけ次を実行する。

－　ＳＡＥベアラ管理；

－　認証；

－　ＬＴＥ＿ＩＤＬＥ　モビリティ・ハンドリング；

－　ＬＴＥ＿ＩＤＬＥでのページングの開始；

－　セキュリティ制御

注：ＮＡＳ制御プロトコルは，このＴＳの範囲で取り扱われず，情報としてのみ言及される。」（乙１抄訳）

イ　「７　ＲＲＣ

この従属節は，ＲＲＣサブレイヤによって提供されるサービスと機能の概観を提供する。

７．１　サービスと機能

ＲＲＣサブレイヤの主なサービスと機能は，次を含む：

－非アクセス層（ＮＡＳ）に関連するシステム情報のブロードキャスト；

－　アクセス層（ＡＳ）に関連するシステム情報のブロードキャスト；

－　ページング；

－　以下を含む，ＵＥとＥ－ＵＴＲＡＮ間のRRC接続の確立，維持，及び，解除；

－　ＵＥとＥ－ＵＴＲＡＮ間の一時的な識別子の割当；

－　ＲＲＣ接続のための信号無線ベアラの設定：

－　低品位ＳＲＢと高品位ＳＲＢ

－　以下を含むセキュリティ機能：

－　ＲＲＣメッセージのための完全性保護

－　ポイントツーポイント無線ベアラの確立，維持，及び，解除；

－　以下を含むモビリティ機能

－　セル間，及び，ＲＡＴ間モビリティのためのＵＥ測定報告，及び，報告の制御；

－　セル間ハンドオーバ

－　ＵＥセル選択と再選択，及び，セルの選択と再選択の制御；

－　ｅＮＢ間のコンテキスト転送

－　ＭＢＭＳサービスのための通知（次の検討である）；

－　ＭＢＭＳサービスのための無線ベアラの確立，配置，維持，及び，解除（次の検討である）；

－　ＱｏＳ管理機能；

－　ＵＥ測定報告，及び，報告の制御；

－　ＭＢＭＳ制御（次の検討である）；

－　ＮＡＳダイレクト・メッセージのＵＥからＮＡＳへ／ＮＡＳからＵＥへの転送」

「７．３　ＮＡＳメッセージの転送

Ｅ－ＵＴＲＡＮ内で，ＮＡＳメッセージはＲＲＣメッセージに結びつけられるか，結びつけられることなく，ＲＲＣに入れられる。

初期直接転送は，もし転送ブロックサイズが許せば，ＲＲＣ接続要求に結びつけられる（次の検討である）。他のＮＡＳメッセージは，おそらく，（同期したＮＡＳ／ＲＲＣ手続のための）ＲＲＣメッセージ，に結びつけられる。

注：ＮＡＳによって実行された完全性保護と暗号化に加えて，ＮＡＳメッセージは，ＲＲＣによって完全性が保護され，ＰＤＣＰによって暗号化されている。」

（以上，乙１抄訳）

ウ　（原文）

「14 Security

14.1 Overview and Principles

The following principles apply to E-UTRAN security:」

「- The eNB keys are cryptographically separated from the EPC keys used for NAS protection (making it impossible to use the eNB key to figure out an EPC key).」（第１原則）

「- The keys are derived in the EPC/UE from key material that was generated by a NAS (EPC/UE) level AKA procedure.」（第２原則）

「- The eNB keys are sent from the EPC to the eNB when the UE is entering LTE_ACTIVE state (i.e. during RRCconnection or S1 context setup).」（第３原則）

「- Key material for the eNB keys is sent between the eNBs during LTE_ACTIVE intra-E-UTRAN mobility.」（第４原則）

「- A sequence number is used as input to the ciphering and integrity protection. A given sequence number must only be used once for a given eNB key (except for identical re-transmission). The same sequence number can be used for both ciphering and integrity protection.」（第５原則）

「- A hyper frame number (HFN) (i.e. an overflow counter mechanism) is used in the eNB and UE in order to limit the actual number of sequence number bits that is needed to be sent over the radio. The HFN needs to be synchronized between the UE and eNB.」（第６原則）

「As a result of an AKA run, the EPC and the UE share a base-key named K_ASME. From K_ASME, the NAS, (and indirectly) K_eNB keys are derived. The K_ASME never leaves the EPC, but the K_eNB key is transported to the eNB from the EPC when the UE transitions to LTE_ACTIVE. From the K_eNB, the eNB and UE can derive the UP and RRC keys. When the UE goes into LTE_IDLE or LTE_DETACHED, the K_e

NB, UP and RRC keys are deleted from the eNB. The key hierarchy is depicted on Figure 14.1-1 below:」（概説）

「１４　セキュリティ

１４．１　概説及び原則

次の原則は，Ｅ－ＵＴＲＡＮのセキュリティに適用される：

－　（ＥＰＣ鍵を見つけ出すためにｅＮＢ鍵を用いることが不可能なように）ｅＮＢ鍵は，暗号によって，ＮＡＳ保護のために用いられるＥＰＣ鍵から分離される．」（第１原則）

「－　その鍵は，ＥＰＣ／ＵＥにおいて，ＮＡＳ（ＥＰＣ／ＵＥ）レベルＡＫＡ手続によって生成された，鍵素材から得られる。」（第２原則）

「－　ｅＮＢ鍵は，ＵＥが，ＬＴＥ＿ＡＣＴＩＶＥ状態に入ると（即ち，ＲＲＣ接続，或いは，Ｓ１コンテキスト設定の間），ＥＰＣから，ｅＮＢに送られる。」（第３原則）

「－　ｅＮＢ鍵のための鍵素材は，ＬＴＥ＿ＡＣＴＩＶＥ　イントラ－Ｅ－ＵＴＲＡＮモビリティの間に，ｅＮＢの間に送られる。」（第４原則）

「－　シーケンス番号は，暗号化，及び，完全性保護のための入力として用いられる。所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，（同一の再送のためを除いて）一度のみでなければならない。同一のシーケンス番号が，暗号化と，完全性保護の両方に用いることができる。」（第５原則）

「－　ハイパー・フレーム番号（ＨＦＮ）（即ち，桁あふれ計数機構）は，無線上に送られるために必要な連続番号ビットの実数を制限するためにｅＮＢとＵＥの中で使用される。ＵＥとｅＮＢの間でＨＦＮを同期する必要がある。」（第６原則）

「ＡＫＡ（判決注:認証及び鍵共有のためのプロトコル）実行の結果として，ＥＰＣとＵＥは，Ｋ＿ＡＳＭＥという名の基本鍵を共有する。Ｋ＿Ａ

ＳＭＥから，ＮＡＳ（そして，間接的に），Ｋ＿ｅＮＢが得られる。Ｋ＿ＡＳＭＥは，決して，ＥＰＣから離れない。しかしながら，Ｋ＿ｅＮＢ鍵は，ＵＥが，ＬＴＥ＿ＡＣＴＩＶＥに移行すると，ＥＰＣからｅＮＢに運ばれる。Ｋ＿ｅＮＢから，ｅＮＢ，及び，ＵＥは，ＵＰ，及び，ＲＲＣ鍵を得ることができる。ＵＥが，ＬＴＥ＿ＩＤＬＥ，或いは，ＬＴＥ＿ＤＥＴＡＣＨＥＤの状態になると，Ｋ＿ｅＮＢ，ＵＰ，及び，ＲＲＣ鍵は，ｅＮＢから消去される。鍵階層は，下の図１４．１－１に描かれている。」

（概説）

（以上，甲１抄訳）

(3)　引用発明の認定の誤りの有無について

原告は，本件審決が，本件審決が引用刊行物１の「A given sequence number must only be used once for a given eNB key」（第５原則第２文）との記載について「得られたシーケンス番号は，ｅＮＢ鍵を得るために使用されるのは，一度のみでなければならない」と和訳（本件和訳）した上で，上記記載箇所から「“ｅＮＢ鍵を得るために，シーケンス番号が使用される”ことが読み取れる。」と認定したが，本件和訳は誤訳であり，引用刊行物１には，他に「Ｋ＿ｅＮＢ」を導出する手法についての開示はないから，「Ｋ＿ｅＮＢを得るために，シーケンス番号が使用され」る構成についての開示はないとして，本件審決が認定した引用発明のうち，「前記Ｋ＿ｅＮＢを得るために，シーケンス番号が使用され」との部分は誤りである旨主張するので，以下において判断する。

ア　まず，引用刊行物１記載の第５原則第２文の「 A given sequence number must only be used once for a given eNB key (except for identical re-transmission).」は，その文理からみて，「所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，（同一の再送のためを除いて）一度のみでなければならない。」（前記(2)ウ）と和訳するのが

自然である。

そこで，第５原則第２文の「所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，（同一の再送のためを除いて）一度のみでなければならない。」にいう「ｅＮＢ鍵のために使用される」との意義について検討する。

イ　前記(2)によれば，引用刊行物１の「１４．１　概説及び原則」には，第１原則としてｅＮＢ鍵（Ｋ＿ｅＮＢ）はＥＰＣ鍵から分離されること，第２原則としてｅＮＢ鍵はＥＰＣ／ＵＥにおいてＮＡＳ（ＥＰＣ／ＵＥ）レベルＡＫＡ手続によって生成された鍵素材から得られること，第３原則としてＵＥがＬＴＥ＿ＡＣＴＩＶＥ状態に入ると，ｅＮＢ鍵はＥＰＣからｅＮＢに送られること，第４原則としてｅＮＢ鍵のための鍵素材はｅＮＢ間で送られること，第６原則としてシーケンス番号を構成するハイパー・フレーム番号（ＨＦＮ）についての記載があり，また，これらの「原則」に引き続き記載されている「概説」には，ＥＰＣ及びＵＥが共有するＫ＿ＡＳＭＥという名称の基本鍵からＫ＿ｅＮＢが得られることや，ｅＮＢ及びＵＥにおいてＫ＿ｅＮＢからＵＰ及びＲＲＣ鍵を得られることが記載されている。

このように「１４．１　概説及び原則」には，第５原則の前後の文脈において，ｅＮＢ鍵（Ｋ＿ｅＮＢ）の「生成」及び「共有」（第２原則，概説），「転送」（第３原則，概説）に関する記載がある。

そして，第５原則には，ｅＮＢ鍵（Ｋ＿ｅＮＢ）と「シーケンス番号」との関係に関し，「所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，（同一の再送のためを除いて）一度のみでなければならない。」（第２文）との記載がある。

一方で，第５原則には，「シーケンス番号」に関し，「シーケンス番号」が暗号化及び完全性保護のための入力として用いられること（第１文），

同一の「シーケンス番号」が暗号化と完全性保護の両方に用いることができること（第３文）についての記載があるが，「１４．１　概説及び原則」には，第５原則第２文にいう「所与のあるシーケンス番号」が「ｅＮＢ鍵のために使用される」ことについて，その使用の具体的な態様を明示した記載はない。

ウ　被告は，この点に関し，シーケンス番号を使用して鍵を生成することによって効率的に鍵を共有することができることは，本願の優先権主張日当時，セキュリティの分野における技術常識であったことを踏まえると，シーケンス番号が「ｅＮＢ鍵のために使用される」とは，シーケンス番号が「ｅＮＢ鍵の生成のため」に使用されることを意味する旨主張するので，以下において，本願の優先権主張日当時におけるシーケンス番号に関する技術常識について検討する。

（ア）　乙６の記載事項

ａ　乙６には，図１，図５及び図６とともに，以下の記載がある（上記各図面については別紙３を参照）。

(a)　「【発明の属する技術分野】本発明は，通信の安全性を高めるために，暗号を用いて通信する暗号通信装置に関し，特に，暗号通信に先立って行われる暗号鍵伝送時の手間を簡略化できる暗号通信装置に関するものである。」（段落【０００１】）

(b)　「一方，本実施形態に係る暗号鍵生成部５２は，暗号通信に先立って，後述する手順で通信相手の暗号通信装置３ｂと通信してネゴシエーションする。これにより，暗号鍵生成部５２は，送信した暗号化乱数を，上記送信暗号化乱数領域４２へ格納すると共に，受信した暗号化乱数を，受信暗号化乱数領域４３へ格納する。さらに，暗号鍵生成部５２は，両暗号化乱数に基づき，暗号通信時に使用される通信用暗号化鍵および通信用復号化鍵を生成して暗号処理部５

１へ通知できる。」（段落【００６８】）

「両暗号通信装置３ａ・３ｂが通信可能になると，発呼側の暗号通信装置３ａは，図５に示すステップＳ１ａにて，乱数Ａ１を生成し，Ｓ２ａにて，通信相手の暗号通信装置３ｂへ当該乱数Ａ１を送出する。なお，以下では，発呼側の暗号通信装置３ａが実行するステップには，例えば，Ｓ１ａのように，符号の末尾にａを付して参照し，被呼側の暗号通信装置３ｂが実行するステップには，Ｓ１ｂのように，符号の末尾にｂを付して参照する。」（段落【００７２】）

「一方，被呼側の暗号通信装置３ｂは，Ｓ１ｂにて，暗号通信装置３ａから乱数Ａ１を受け取ると，Ｓ２ｂにおいて，予め共有された共有鍵Ｏを用いて，当該乱数Ａ１を暗号化する。これにより，暗号化乱数Ａ２が生成される。さらに，暗号通信装置３ｂは，Ｓ３ｂにおいて，発呼側の暗号通信装置３ａへ，生成した暗号化乱数Ａ２を送り返す。」（段落【００７３】）

「さらに，発呼側と被呼側とを入れ換えて，上記Ｓ１ａ～Ｓ５ａおよびＳ１ｂ～Ｓ３ｂと同様のステップが行われる（Ｓ１１ｂ～Ｓ１５ｂおよびＳ１１ａ～Ｓ１３ａ）。これらのステップでは，両暗号通信装置３ａ・３ｂは，被呼側の暗号通信装置３ｂが生成した乱数Ｂ１に基づいて，暗号化乱数Ｂ２・Ｂ３をそれぞれ生成する。これにより，被呼側の暗号通信装置３ｂは，発呼側の暗号通信装置３ａを認証できる。」（段落【００７７】）

「両暗号通信装置３ａ・３ｂが通信相手による認証に成功すると，図６に示すように，上記両暗号化乱数Ａ２・Ｂ２に基づいて，暗号通信に使用される通信用暗号鍵が生成される。すなわち，発呼側の暗号通信装置３ａは，Ｓ２１ａにおいて，自ら（発呼側）が生成し

た暗号化乱数Ｂ２を共有鍵Ｏで暗号化して，暗号化データＢ４を生成する。また，Ｓ２２ａにおいて，受け取った暗号化乱数Ａ２を共有鍵Ｏで暗号化して，暗号化データＡ５を生成する。」（段落【００８０】）

(c)　「また，本実施形態では，図５のステップＳ１ａ・Ｓ２ａ，および，Ｓ１１ｂ・Ｓ１２ｂに示すように，両暗号通信装置３ａ・３ｂが乱数を生成して送出する場合について説明したが，これに限るものではない。例えば，日付や時刻，あるいは，シーケンス番号などを用いてもよい。両暗号通信装置３ａ・３ｂが通信毎に異なるデータを送出すれば，本実施形態と同様の効果が得られる。」（段落【００９５】）

ｂ　前記ａの記載事項によれば，乙６には，暗号通信に使用される通信用暗号鍵の生成に，「乱数」や「シーケンス番号」が用いられることが開示されているものと認められる。

（イ）　乙７の記載事項

ａ　乙７には，第４図とともに，以下の記載がある（第４図については別紙４を参照）。

(a)　「発明の分野

本発明は，ディジタル領域式通信システムに関し，特にそのようなシステム内のデータ通信の暗号化用の方法および装置に関する。」（５頁左下欄４行～７行）

(b)　「本発明の特定な実施例の特定な説明をこれから行なう。上述の通り，かつ以下に使用される通り，「キーストリーム」という語は，未確認アクセス，例えばＲＦチャネルの影響を受けやすい媒体にある記憶を伝送する前に，ディジタル符号式メツセージまたはデータ信号を暗号化するのに用いられた２進ビットまたはビットのブロッ

クの擬似ランダム・シーケンスを意味する。」（１１頁右上欄５行～１２行）

(c) 「第４図を参照すると，従来技術の日毎定時刻駆動による暗号化システムの略ブロック図を見ることができる。第４図の上半分は，送信機部分を表わし，下半分はそのような暗号化システムの受信機部分を表わす。送信機部分では，タイム・クロックまたはブロック・カウンタ２０１はカウント２１３，例えばタイム・クロックまたはブロック・カウンタ２０１の入力に加えられる増分２１５に応じて，３２－ビットの出力を発生させる。カウント２１３は，結合式論理または混合工程２０２に第１入力として供給される。例えば，２進記法の値９６８１７３であるシークレット・キーは，第２入力２１１として，結合式論理または混合工程２０２の第２入力として供給される。カウント２１３に対して新しい値が生じるごとに，結合式論理または混合工程２０２は，シークレット・キー２１１をカウント２１３と結合させたり混合して，直列または並列出力２０９で複数の擬似ランダム・キーストリーム・ビットを発生させる。キーストリーム出力２０９は，同時に，モジュロ－２加算器２０３に入力として供給される。暗号化すべきデータは，モジュロ－２加算器２０３に第２入力２０７を形成する。各キーストリーム・ビットは，モジュロ－２加算機２０３によって特定のデータ・ビットに加えられるモジュロ－２であり，暗号式データは媒体を通して伝送する出力２１８に供給される。

受信機部分では，タイム・クロックまたはクロック・カウンタ２０４は，タイム・クロックまたはブロック・カウンタ２０１と構造が同じであり，増分２１５と同じ増分２１６を供給され，結合式論理または混合工程２０２と構造が同じである結合式論理または混合

工程２０５にカウント２１４を供給する。結合式論理または混合工程２０５は，カウント２１４を同一なシークレット・キー，すなわち入力２１２に供給される２進記法の９６８１７３と結合させたり混合したりするが，それによって出力２１０にキーストリームを作り，この出力は出力２０９で作られたキーストリームと同じである。キーストリーム出力２１０は，モジュロ－２加算器２０６によって伝送媒体で受信された暗号式データに少しずつ加えられるモジュロ－２である。モジュロ－２加算およびモジュロ－２減算は同じ操作であり，受信機における同一キー・ストリームのモジュロ－２加算は送信機におけるキーストリームの前の加算を打ち消して，出力２０８で原データの回復をもたらす。しかし，暗号式データのそのような打消しおよび正しい解読は，タイム・クロックまたはブロック・カウンタ２ｆ０１，２０４が相互に完全に同期機構２１７は，この目的で供給されなければならない。」（１１頁左下欄２２行～１２頁左上欄１７行）

ｂ　前記ａの記載事項によれば，乙７には，暗号鍵である「キーストリーム」の生成に，シーケンス番号である「カウント」が用いられることが開示されているものと認められる。

（ウ）　引用刊行物２の記載事項

引用刊行物２（甲２の１）のＦＩＧ．３Ａ（別紙５）によれば，引用刊行物２には，「Ｆｕｌｌ　Ｓｅｑｕｅｎｃｅ　Ｎｕｍｂｅｒ」（フルシーケンス番号）が「Ｋｅｙｓｔｒｅａｍ」（キーストリーム）の生成に用いられることが開示されているものと認められる。

（エ）　検討

以上によれば，本願の優先権主張日当時，暗号鍵の生成に，シーケンス番号が用いられることは，当業者の技術常識であったものと認められ

る。

エ　前記イのとおり，引用刊行物１の「１４．１　概説及び原則」には，第５原則第２文にいう「所与のあるシーケンス番号」が「ｅＮＢ鍵のために使用される」ことについて，その使用の具体的な態様を明示した記載はない。

しかるところ，「１４．１　概説及び原則」には，第５原則の前後の文脈において，ｅＮＢ鍵（K__ｅＮＢ）の「生成」及び「共有」（第２原則，概説），「転送」（第３原則，概説）に関する記載があり（前記イ），第５原則は，そのような一連の文脈の中で理解されるべきものであること，本願の優先権主張日当時，暗号鍵の生成に，シーケンス番号が用いられることは，当業者の技術常識であったこと（前記ウ(エ)）に鑑みると，引用刊行物１に接した当業者は，第５原則第２文の「所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，（同一の再送のためを除いて）一度のみでなければならない。」にいう「ｅＮＢ鍵のために使用される」とは，暗号鍵である「ｅＮＢ鍵の生成のために」使用されることを意味し，「第２文」は，「所与のあるｅＮＢ鍵」の生成のために一度使用された「所与のあるシーケンス番号」は，当該「所与のあるｅＮＢ鍵」の生成のために再度使用してはならないことを記載したものと理解するものと認められる。

そうすると，「シーケンス番号」が，「ｅＮＢ鍵の生成のために使用される」とは，本件審決が認定した引用発明の「K__ｅＮＢを得るために，シーケンス番号が使用され」ることと技術的に同じ意味であるといえるから，本件審決が認定した引用発明のうち，「前記K__ｅＮＢを得るために，シーケンス番号が使用され」との部分が誤りであるとはいえないというべきである。

オ　原告は，これに対し，①引用刊行物１（3GPP TS 36.300 version 8.1.0

Release 8）の後のバージョンの甲８（3GPP TS 36.300 version 8.8.0 Release 8）に「A sequence number (COUNT) is used as input to the ciphering and integrity protection.」との記載があることからすると，第５原則第２文中の「A given sequence number」にいう「sequence number」とは「ＣＯＵＮＴ」を意味すること，②引用刊行物１の後のバージョンの甲９の１（3GPP TS 36.323 version 1.0.0 Release 8）には，シーケンス番号の一種である「ＣＯＵＮＴ」が，暗号化及び完全性保護のパラメータとして，K_{RRCenc}，K_{UPenc}及びK_{RRCint}のようなｅＮＢ鍵の下位の鍵と共に用いられることが示されていることからすると，第５原則は，第１文において，シーケンス番号が暗号化及び完全性保護の入力として用いられること，第２文において，ある所与のシーケンス番号が，（暗号化及び完全性保護に用いられる際に，）ある所与のｅＮＢ鍵を基にして得られたＵＰ鍵（$K_{eNB-UP-enc}$）及びＲＲＣ鍵（$K_{eNB-RRC-enc}$，$K_{eNB-RRC-int}$）のために用いられるのは一度でなければならないこと，第３文において，所与のｅＮＢ鍵（正確には，その下位のＵＰ鍵及びＲＲＣ鍵）が暗号化及び完全性保護の手続に用いられることを述べたものであることからすると，第５原則第２文は，暗号化及び完全性保護の手続について述べたものであって，シーケンス番号がｅＮＢ鍵の生成のために用いられることを述べたものではない旨主張する。

しかしながら，原告の主張は，以下のとおり理由がない。

(ア)　上記①の点について

ａ　甲８には，「－　シーケンス番号（ＣＯＵＮＴ）は，暗号化，及び，完全性保護のための入力として用いられる。所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，同一方向における同一の無線ベアラにおいては（同一の再送のためを除いて）一度のみでなければならない。同一のシーケンス番号が，暗号化と，完全性保護の両方に用いることができる。」（原文７３頁下から９行～下か

ら７行の訳文）との記載がある。

甲８の上記記載と引用刊行物１の「１４．１　概説及び原則」の第５原則第２文とを対比すると，上記記載のうち，「シーケンス番号（ＣＯＵＮＴ）は，暗号化，及び，完全性保護のための入力として用いられる。」との記載箇所は，第５原則第１文の「シーケンス番号」を「シーケンス番号（ＣＯＵＮＴ）」としたほかは，第１文と同内容であること，「所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，同一方向における同一の無線ベアラにおいては（同一の再送のためを除いて）一度のみでなければならない。」との記載箇所は，第５原則第２文に「同一方向における同一の無線ベアラにおいては」の文言を付け加えたほかは，第２文と同内容であること，「同一のシーケンス番号が，暗号化と，完全性保護の両方に用いることができる。」との記載箇所は第３文と同内容であることが認められる。

b　上記認定事実によれば，引用刊行物１（3GPP TS 36.300 version 8.1.0 Release 8（2007-06））の公開時（２００７年（平成１９年）６月）には，第５原則第１文の「暗号化，及び，完全性保護のための入力」として「シーケンス番号」を用いること自体は決定されていたが，具体的にどのようなシーケンス番号を用いるのかについては決定されておらず，その後検討が進められた結果，引用刊行物１と同じ規格（「3GPP TS 36.300」）の後のバージョンである甲８（3GPP TS 36.300 version 8.8.0 Release 8（2009-03））の公開時（２００９年（平成２１年）３月）までに，第５原則第１文の「シーケンス番号」として「ＣＯＵＮＴ」を規格として採用することが決定されたものと推認される。このように引用刊行物１の公開時には，第５原則第１文の「シーケンス番号」として具体的にどのようなシーケンス番号を用いるの

かについては決定されていなかったことに照らすと，同様に，第５原則第２文の「所与のあるシーケンス番号」にいう「シーケンス番号」についても，具体的にどのようなシーケンス番号を用いるのかについては決定されていなかったと解するのが自然であるから，これが「ＣＯＵＮＴ」として特定されていた旨の原告の主張は採用することができない。

（イ）　上記②の点について

ａ　甲９の１には，次のような記載がある。

(a)　「５．３　暗号化及び復号化

暗号化機能はＰＤＣＰで実行される。暗号化されるデータユニットは，ヘッダ圧縮が構成される場合はその後のＰＤＣＰ　ＰＤＵのデータ部分（Ｕプレーンデータに関連するＰＤＣＰエンティティにのみ適用）（項目６．３．２を参照）及び，可能な場合，ＭＡＣフィールド（項目６．３．３を参照）である（ＦＦＳ（要検討））。

ユーザプレーン無線ベアラに関連するＰＤＣＰエンティティに使用される暗号化アルゴリズム及び鍵は，ＰＤＣＰ　ＰＤＵが受信／送信された時に上位層［３］によって構成され，［６］で明記した暗号化方法が適用される。ヘッダ圧縮を使用するように構成される場合，ＰＤＣＰ　ＳＤＵに関連する圧縮パケットのみが，関連するＣＯＵＮＴ値に基づいて暗号化／復号化される。

制御プレーン無線ベアラに関連するＰＤＣＰエンティティに使用される暗号化アルゴリズム及び鍵は，受信される各ＰＤＣＰ　ＰＤＵに対して上位層［３］によって構成され，［６］で明記した暗号化方法が適用される。

暗号化保護のためにＰＤＣＰに要求されるパラメータは［６］で定義され，暗号化アルゴリズムに入力される。上位層［３］によって

提供されるＰＤＣＰに要求されるパラメータを以下に記載する。

－　ＣＯＵＮＴ

－　ＢＥＡＲＥＲ（［５］で無線ベアラ識別子として定義される。［３］のように，値ＲＢアイデンティティ　１を使用する。）

－　ＤＩＲＥＣＴＩＯＮ（送信方向）

－　ＣＫ（暗号鍵）

－　ＩＢＳ（入力ビットストリーム）」

「５．４　完全性保護

完全性保護機能は，制御プレーン無線ベアラに関連するＰＤＣＰエンティティに対してＰＤＣＰで実行される。

ＰＤＣＰエンティティに使用される完全性保護アルゴリズム及び鍵は，受信される各ＰＤＣＰ　ＰＤＵに対して上位層［３］によって構成され，［６］で明記した完全性保護方法が適用される。完全性保護のためにＰＤＣＰに要求されるパラメータは［６］で定義され，完全性保護アルゴリズムに入力される。上位層［３］によって提供されるＰＤＣＰに要求されるパラメータを以下に記載する。

－　ＣＯＵＮＴ

－　ＢＥＡＲＥＲ（［６］で無線ベアラ識別子として定義される。［３］のように，値ＲＢアイデンティティ　１を使用する。）

－　ＤＩＲＥＣＴＩＯＮ（送信方向）

－　ＩＫ（完全性保護鍵）

－　ＩＢＳ（入力ビットストリーム：暗号化又は復号化されたデータユニット（ＦＦＳ（要検討））

－　ＦＲＥＳＨ

完全性保護を検証する場合，上記したように，ＵＥは，入力パラメータに基づいてＸ－ＭＡＣを計算する。計算したＸ－ＭＡＣがＭＡ

Ｃと一致する場合，完全性保護の検査は成功したことになる。Ｘ－ＭＡＣが受信したＭＡＣと一致しない場合，対応するパケットは廃棄される。」

（以上，原文１２頁１９行～１３頁１５行・訳文１頁～２頁）

(b)　「６．３．４　ＣＯＵＮＴ

暗号化と完全性保護のため，ＣＯＵＮＴ値は保持される。ＣＯＵＮＴ値は，ＨＦＮ及び当該ＰＤＣＰシーケンス番号から構成される。」

（原文１６頁３行～５行・訳文３頁）

b　上記ａの記載事項によれば，甲９の１には，暗号化機能は，「ＰＤＣＰ」（「ＮＡＳ」よりも下位の階層（サブレイヤ））で実行され，暗号化保護のためのパラメータが暗号化アルゴリズムに入力されること，完全性保護機能も，「ＰＤＣＰ」で実行され，完全性保護のためのパラメータが完全性保護アルゴリズムに入力されること，暗号化及び完全性保護のためのパラメータとして，ＨＦＮ及び当該ＰＤＣＰシーケンス番号から構成される「ＣＯＵＮＴ」が用いられることが開示されていることが認められる。

しかるところ，甲９の１は，引用刊行物１が公開（２００７年（平成１９年）６月）された後に公開（同年９月）されたこと（弁論の全趣旨）からすると，上記開示事項は，引用刊行物１の公開当時，「１４．１　概説及び原則」の第５原則第１文の「暗号化，及び，完全性保護のための入力」として「シーケンス番号」として，「ＣＯＵＮＴ」が有力候補の一つとして検討されていたことをうかがわせるものであるとしても，その公開時に，「ＣＯＵＮＴ」を採用することが決定していたことの根拠となるものではないし，同様に，第５原則第２文の「所与のあるシーケンス番号」にいう「シーケンス番号」として「Ｃ

ＯＵＮＴ」を採用することが決定していたことの根拠となるものでもない。

ましてや，甲９の１が，第５原則第２文が「ある所与のシーケンス番号が，（暗号化及び完全性保護に用いられる際に，）ある所与のｅＮＢ鍵を基にして得られたＵＰ鍵（$K_{eNB-UP-enc}$）及びＲＲＣ鍵（$K_{eNB-RRC-enc}$，$K_{eNB-RRC-int}$）のために用いられるのは一度でなければならないこと」を意味する旨の原告主張の裏付けとなるものではない。

（ウ） 小括

以上によれば，第５原則第２文は，暗号化及び完全性保護の手続について述べたものであり，シーケンス番号がｅＮＢ鍵の生成のために用いられることを述べたものではないとの原告の主張は，理由がない。

(4) 一致点の認定の誤りの有無について

原告は，引用発明における「シーケンス番号」には，本願発明の「ＮＡＳ＿Ｕ＿ＳＥＱ」は含まれないから，本件審決が，「シーケンス番号と，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから，前記セキュリティキーＫ＿ｅＮＢを導出するステップ」を本願発明と引用発明の一致点と認定したのは誤りである旨主張する。

ア 引用刊行物１の「１４．１ 概説及び原則」の第５原則第２文の「所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，（同一の再送のためを除いて）一度のみでなければならない。」にいう「ｅＮＢ鍵のために使用される」とは，「ｅＮＢ鍵の生成のために」使用されることを述べたものであることは，前記(3)エ認定のとおりである。

そして，引用刊行物１の公開時において，第５原則第１文の「シーケンス番号」及び第５原則第２文の「所与のあるシーケンス番号」にいう「シーケンス番号」として具体的にどのようなシーケンス番号を採用するかについて決定されていなかったことは，前記(3)オ(ア)及び(イ)のとおりであ

る。

イ　前記(2)アの引用刊行物１の記載事項（別紙１の図４．３．２を含む。）には，ＵＥ及びMME間の「ＮＡＳ」のサブレイヤ（レベル），ＵＥ及びｅＮＢ間の「ＲＲＣ」，「ＰＤＣＰ」，「ＲＬＣ」等のサブレイヤ（レベル）における「制御プレーン・プロトコル・スタック」についての記述がある。

しかるところ，上記各サブレイヤ（レベル）で送信又は受信されるパケットに，それぞれのサブレイヤ（レベル）に対応する「シーケンス番号」が含まれることは，本願の優先権主張日当時，技術常識であったものである。

上記技術常識に加えて，引用刊行物１には，「ｅＮＢ鍵」は，「ＥＰＣ／ＵＥにおいて，ＮＡＳ（ＥＰＣ／ＵＥ）レベルＡＫＡ手続によって生成された，鍵素材から得られる。」（第２原則）が記載されていること（前記(2)ウ）を踏まえると，引用刊行物１に接した当業者は，第５原則第２文の「ｅＮＢ鍵の生成のために」使用される「シーケンス番号」は，ＵＥ及びMME間の「ＮＡＳ」のサブレイヤ（レベル）で送信又は受信されるパケットに含まれるシーケンス番号を意味するものと理解するものと認められる。

そして，ＵＥからみて上流側であるｅＮＢやMMEへのパケット送信をアップリンク送信，逆に，MMEやｅＮＢからみて下流側であるＵＥへのパケット送信をダウンリンク送信と称することは，本願の優先権主張日当時，技術常識であったこと（例えば，引用刊行物２（甲２の１）の段落【００４３】，【００４４】，【００７４】）に照らすと，本願発明の「ＮＡＳ＿Ｕ＿ＳＥＱ」は，ＵＥ及びMME間の「ＮＡＳ」のサブレイヤ（レベル）で，ＵＥからMMEへの「ＮＡＳサービス要求」に係るパケットに含まれるアップリンクシーケンス番号であることは自明であるから，第５

原則第２文の「ｅＮＢ鍵の生成のために」使用される「シーケンス番号」に含まれるものと整理することも許されるというべきである。

そうすると，引用発明における「シーケンス番号」は，本願発明の「ＮＡＳ＿Ｕ＿ＳＥＱ」を含む上位概念として整理し，「シーケンス番号と，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから，前記セキュリティキーＫ＿ｅＮＢを導出するステップ」を本願発明と引用発明の一致点と認定したことに誤りはない。

ウ　原告は，これに対し，①引用刊行物１には，「Ｋ＿ｅＮＢを得るために，シーケンス番号が使用され」る構成についての開示はないから，引用発明は，「シーケンス番号と，および前記ＵＥと共有される，記憶されたアクセスセキュリティ管理エンティティキーＫ＿ＡＳＭＥから，前記セキュリティキーＫ＿ｅＮＢを導出するステップ」の構成を有するものとはいえない，②引用刊行物１記載の第５原則第２文中の「A given sequence number」にいう「sequence number」とは，「ＣＯＵＮＴ」を意味するから，「ＮＡＳ＿Ｕ＿ＳＥＱ」とは異なるシーケンス番号である，③第５原則は，「Ｅ－ＵＴＲＡＮ」すなわち「ＵＥ」と「ｅＮＢ」間のネットワークのセキュリティについて述べたものであるのに対し，「ＮＡＳ」は，「ＵＥ」と「ＭＭＥ」との間のプロトコルであり，本願発明と引用発明とは，「シーケンス番号」が用いられるプロトコルが異なるから，「シーケンス番号」の意味が異なることは，当業者にとって自明であり，引用発明における「シーケンス番号」には，本願発明の「ＮＡＳ＿Ｕ＿ＳＥＱ」は含まれない旨主張する。

しかしながら，引用刊行物１の第５原則第２文にシーケンス番号が「ｅＮＢ鍵の生成のために」使用されることについての開示があること，引用刊行物１の「シーケンス番号」が「ＣＯＵＮＴ」に特定又は限定されるものでないことは，前記(3)オで説示したとおりであるから，上記①及び②の点は

理由がない。

また，前記アのとおり，第５原則第２文の「ｅＮＢ鍵の生成のために」使用される「シーケンス番号」は，ＵＥ及びMME間の「ＮＡＳ」のサブレイヤ（レベル）で送信又は受信されるパケットに含まれるシーケンス番号を意味するものといえるから，上記③の点も理由がない。

したがって，原告の上記主張は，採用することができない。

(5)　まとめ

以上のとおり，本件審決がした引用発明及び一致点の認定に原告主張の誤りは認められないから，原告主張の取消事由１は理由がない。

２　取消事由２（相違点の看過）について

(1)　原告は，本願発明は，「ＮＡＳサービス要求を前記ＵＥから受信するステップ（３２，５２）であって，前記要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップ」の構成を有するが，本件審決は，引用発明が上記構成を有することを認定していないから，上記構成を本願発明と引用発明の相違点として認定すべきであったのに，この相違点の認定を看過した誤りがある旨主張する。

そこで検討するに，前記１(2)イの引用刊行物１の記載事項（「７．１　サービスと機能」，「７．３　ＮＡＳメッセージの転送）」）と図１９．２．２．３（別紙１参照）を総合すると，引用刊行物１には，①「ＮＡＳダイレクトメッセージ」が「ＵＥ」から「ＮＡＳ」へ又は「ＮＡＳ」から「ＵＥ」へ転送（初期直接転送）されること，②「ＮＡＳサービスリクエスト」（ＮＡＳサービス要求）が「ＵＥ」から「ＮＡＳ」によって「ｅＮＢ」を経て「MME」へ送信され，「MME」がこれを受信することが記載されていることが認められる。

そうすると，引用刊行物１には，「MME」が「ＮＡＳサービス要求を前記ＵＥから受信するステップ」が開示されているものといえる。

そして，「ＮＡＳサービス要求」のパケットにシーケンス番号（アップリンクシーケンス番号）含まれることは自明であるから，引用刊行物１には，「ＮＡＳサービス要求を前記ＵＥから受信するステップであって，前記要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップ」の構成が実質的に記載されているに等しいものと認められる。

そうすると，上記構成は，本願発明と引用刊行物１記載の方法との間の相違点ではなく，むしろ一致点と認定すべきであったものといえる。

したがって，原告の上記主張は理由がない。

(2)　以上によれば，本件審決に相違点の看過の誤りがあるものと認められないから，原告主張の取消事由２は理由がない。

なお，本件審決が，本願発明の「ＮＡＳサービス要求を前記ＵＥから受信するステップであって，前記要求が，ＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを示すステップ」の構成と引用刊行物１記載の方法との関係について明示的に認定判断を示さなかったことは，不適切であったものといわざるを得ないが，この点は，審決の結論に影響を及ぼすものではない。

３　取消事由３（相違点の容易想到性の判断の誤り）について

(1)　原告は，①引用刊行物１（甲１）には，「Ｋ＿ｅＮＢを得るために，シーケンス番号が使用され」る構成についての開示がなく，また，仮に引用刊行物１に上記構成の開示があるとしても，Ｋ＿ｅＮＢを得るためにＮＡＳサービス要求で示される「ＮＡＳ＿Ｕ＿ＳＥＱ」をシーケンス番号として用いることの開示はない，②同様に，引用刊行物２（甲２の１）及び本件審決が認定した周知技術（「「ＵＥ」から，「ＭＭＥ」に対して「ＲＲＣ／ＮＡＳ信号」を送信する点」）のいずれにおいても，ＮＡＳサービス要求で示される「ＮＡＳ＿Ｕ＿ＳＥＱ」をＫ＿ｅＮＢの生成のために用いることについての開示や示唆はないとして，引用発明に引用刊行物２記載の発明及び本件審決が認定した構成を組み合わせても，当業者が相違点に係る本願発明の構成を容易に

想到することができたものとはいえないから，本件審決における相違点の容易想到性の判断に誤りがある旨主張する。

ア　引用刊行物１の「１４．１　概説及び原則」の第５原則第２文の「所与のあるシーケンス番号は，所与のあるｅＮＢ鍵のために使用されるのは，（同一の再送のためを除いて）一度のみでなければならない。」にいう「ｅＮＢ鍵のために使用される」とは，「ｅＮＢ鍵の生成のために」使用されることを述べたものであることは，前記１(3)エ認定のとおりである。

そして，当業者においては，第５原則第２文の「ｅＮＢ鍵の生成のために」使用される「シーケンス番号」は，ＵＥ及びMME間の「ＮＡＳ」のサブレイヤ（レベル）で送信又は受信されるパケットに含まれるシーケンス番号を意味するものと理解するものと認められることは，前記１(4)イ認定のとおりである。

加えて，引用刊行物１に，「ＮＡＳサービスリクエスト」（ＮＡＳサービス要求）が「ＵＥ」から「ＮＡＳ」によって「ｅＮＢ」を経て「MME」へ送信され，「MME」がこれを受信することが記載されており，また，「ＮＡＳサービス要求」にパケットにシーケンス番号（アップリンクシーケンス番号）（「ＮＡＳ＿Ｕ＿ＳＥＱ」）が含まれることが自明であることは，前記２(1)認定のとおりである。

以上によれば，引用刊行物１に接した当業者は，第５原則第２文の「ｅＮＢ鍵の生成のために」使用される「シーケンス番号」は，ＵＥ及びMME間の「ＮＡＳ」のサブレイヤ（レベル）で送信又は受信されるパケットに含まれるシーケンス番号であることを理解し，そのようなシーケンス番号の中から，引用刊行物１記載の「ＮＡＳサービスリクエスト」（ＮＡＳサービス要求）に含まれるアップリンクシーケンス番号（「ＮＡＳ＿Ｕ＿ＳＥＱ」）を選択し，これを引用発明に採用することを容易に想到することができたものと認められる。

イ　原告は，この点に関し，本件審決は，本願発明と引用発明との相違点は格別のものではないと判断したが，その判断に際し，本願発明がＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱを採用して，セキュリティキーＫ＿ｅＮＢを生成するため，ＮＡＳダウンリンクシーケンス番号ＮＡＳ＿Ｄ＿ＳＥＱ等の別個のシーケンス番号が不要であり，特別な複雑さを回避することができるという顕著な効果を奏することを考慮していないから，上記判断は誤りである旨主張する。

しかしながら，前記ア認定のとおり，引用刊行物１に接した当業者であれば，引用発明において，「ｅＮＢ鍵の生成のために」使用される「シーケンス番号」としてＮＡＳアップリンクシーケンス番号ＮＡＳ＿Ｕ＿ＳＥＱの構成を採用することを容易に想到することができたものと認められ，この場合に，「ユーザ装置（１１）ＵＥと前記ＵＥにサービスするｅＮｏｄｅＢ（１２）との間のＲＲＣ／ＵＰトラフィックを保護するため」の「セキュリティキーＫ＿ｅＮＢ」の「確立」のために，ＮＡＳダウンリンクシーケンス番号ＮＡＳ＿Ｄ＿ＳＥＱ等の別個のシーケンス番号」を必要としないことは，上記構成を採用したことによる予想どおりの効果にすぎないものであり，格別なものではない。

したがって，原告の上記主張は，理由がない。

(2)　以上によれば，引用刊行物１に基づいて相違点に係る本願発明の構成を容易に想到することができたものと認められるから，本願発明と引用発明との相違点は格別のものではないとした本件審決における相違点の容易想到性の判断は，結論において誤りはない。

したがって，原告主張の取消事由３は理由がない。

４　結論

以上の次第であるから，原告主張の取消事由はいずれも理由がなく，本件審決にこれを取り消すべき違法は認められない。

したがって，原告の請求は棄却されるべきものである。

知的財産高等裁判所第４部

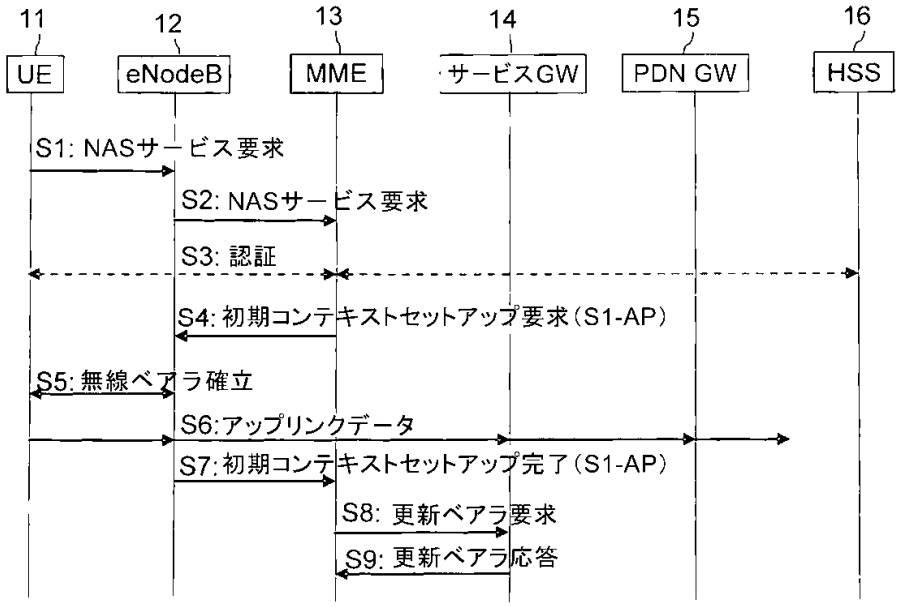
裁判長裁判官　　富　　田　　善　　範

裁判官　　大　　鷹　　一　　郎

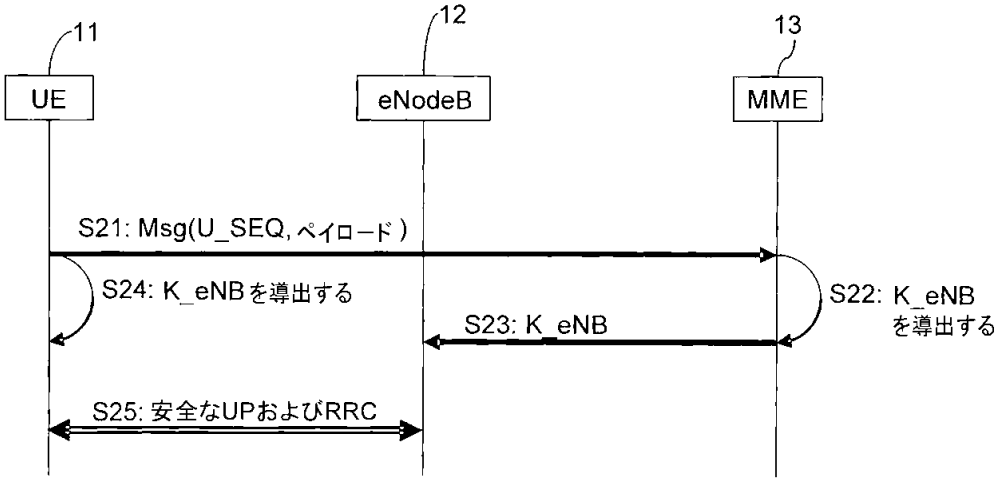
裁判官　　鈴　　木　　わ　か　な

（別紙）　　本願明細書図面

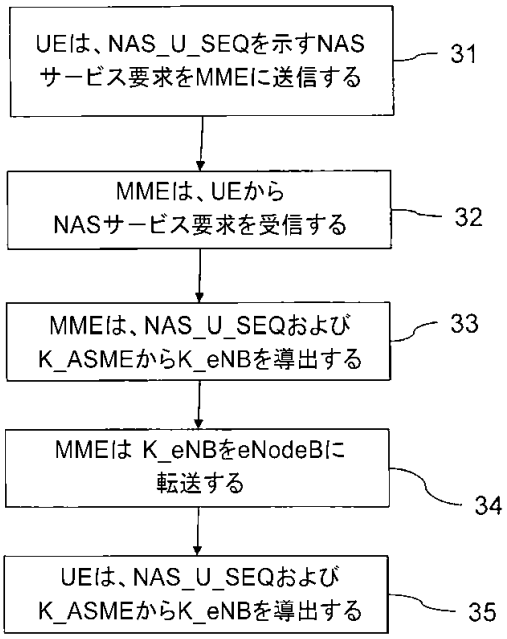
【図１】



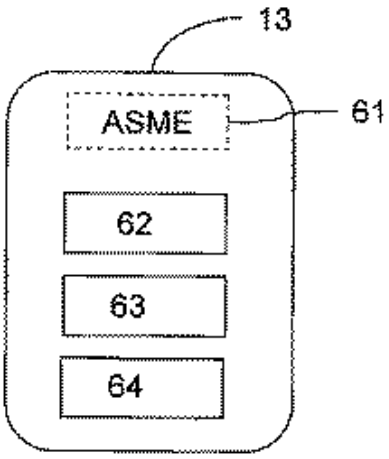
【図２】



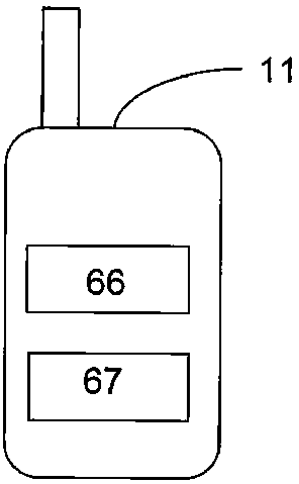
【図３】


UEは、NAS_U_SEQを示すNAS
サービス要求をMMEに送信する
31
MMEは、UEから
NASサービス要求を受信する
32
MMEは、NAS_U_SEQおよび
K_ASMEからK_eNBを導出する
33
MMEは K_eNBをeNodeBに
転送する
34
UEは、NAS_U_SEQおよび
K_ASMEからK_eNBを導出する
35

【図６ａ】


13
ASME
61
62
63
64

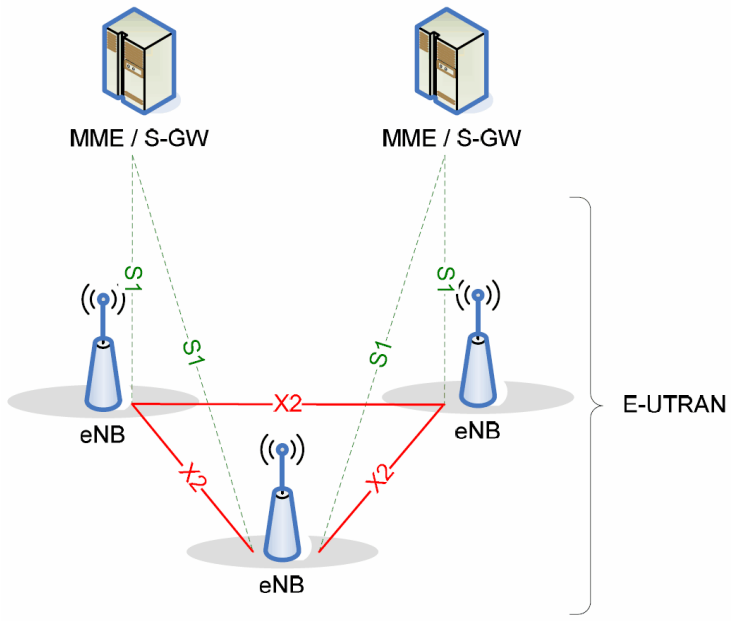
【図６ｂ】


11
66
67

（別紙１）

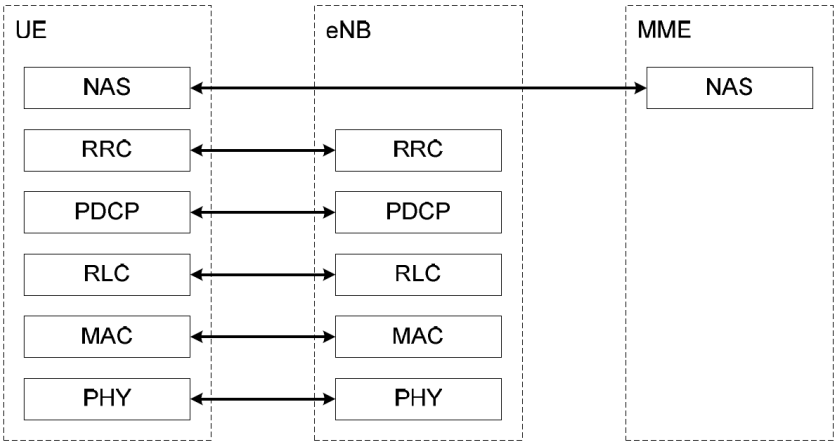
Ｆｉｇｕｒｅ　４

（図４）



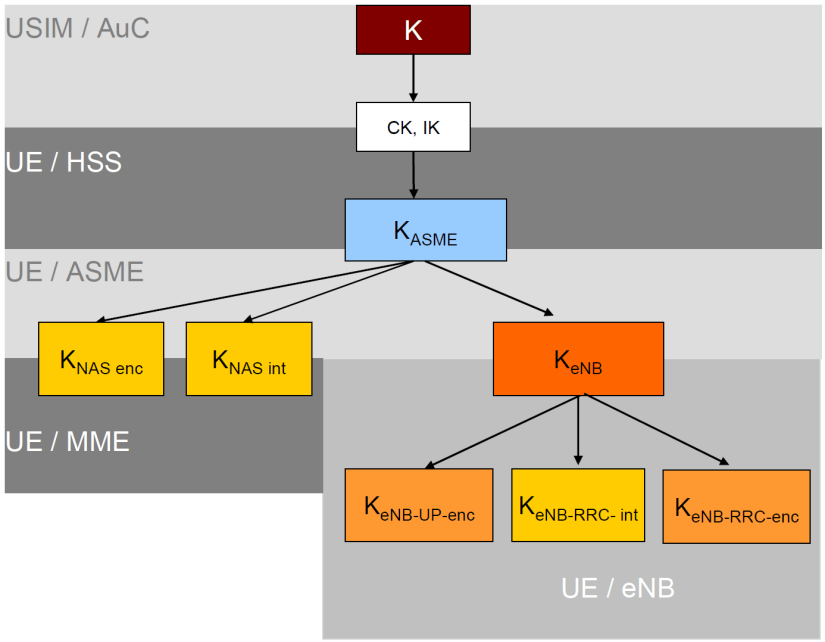
Ｆｉｇｕｒｅ　４．３．２

（図４．３．２）



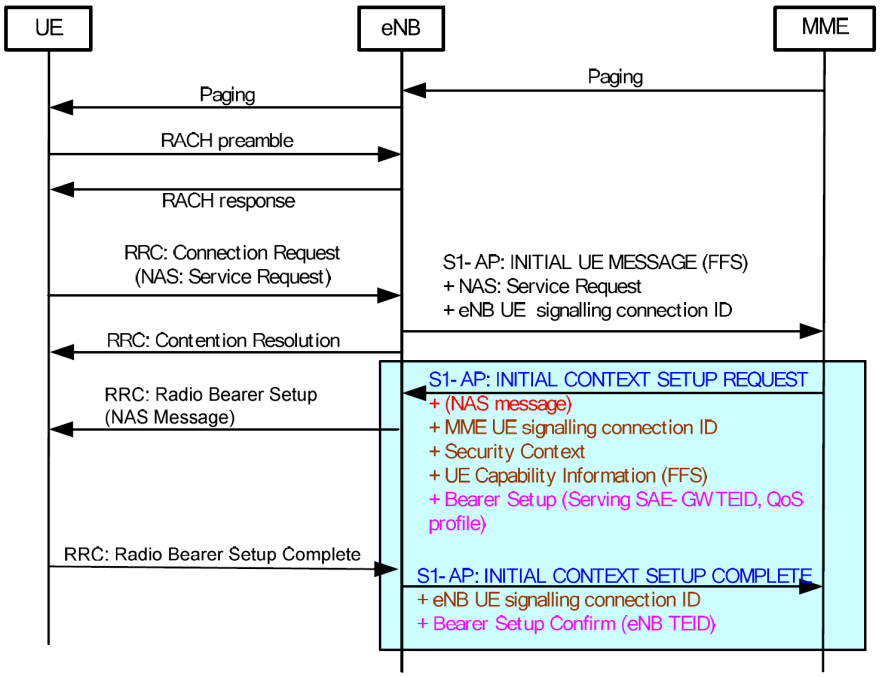
Ｆｉｇｕｒｅ １４．１－１

（図１４．１－１）

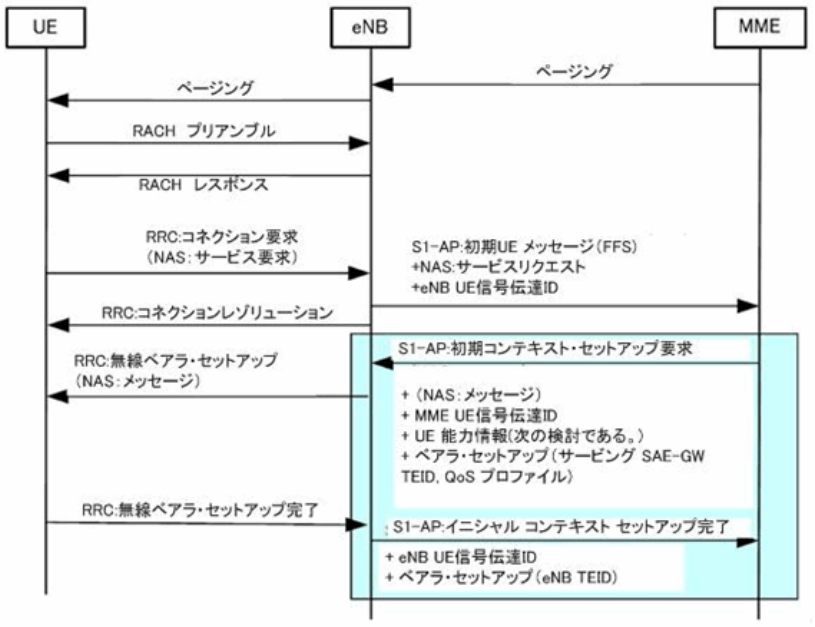


Ｆｉｇｕｒｅ １９．２．２．３

（図１９．２．２．３）



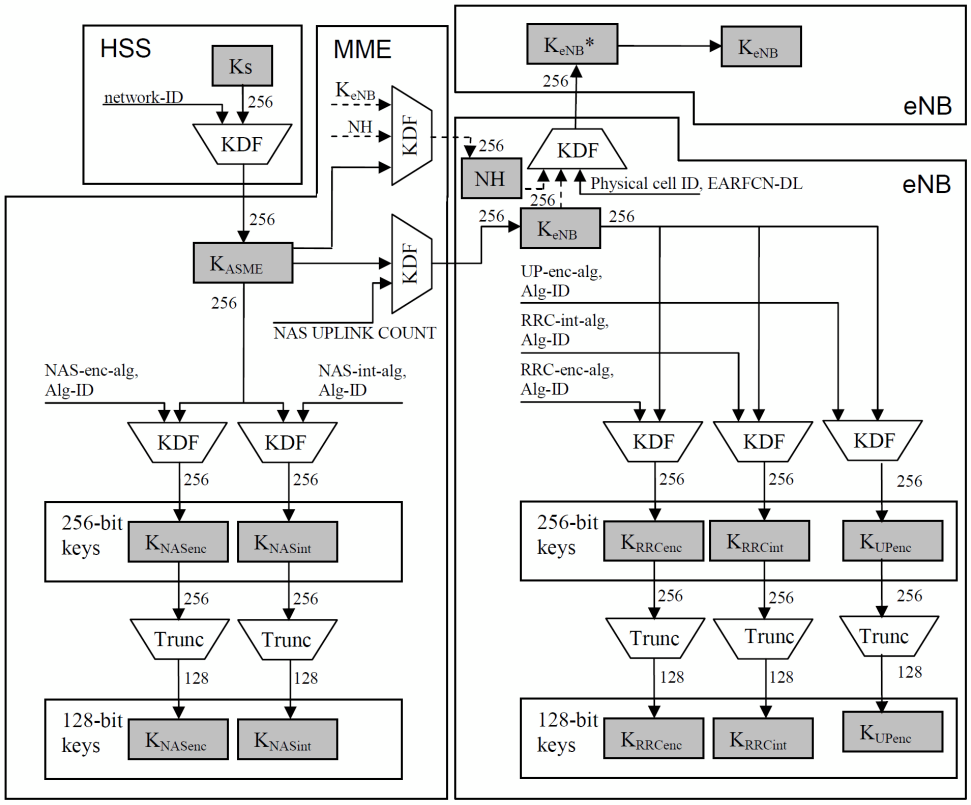
（訳文）



（別紙２）

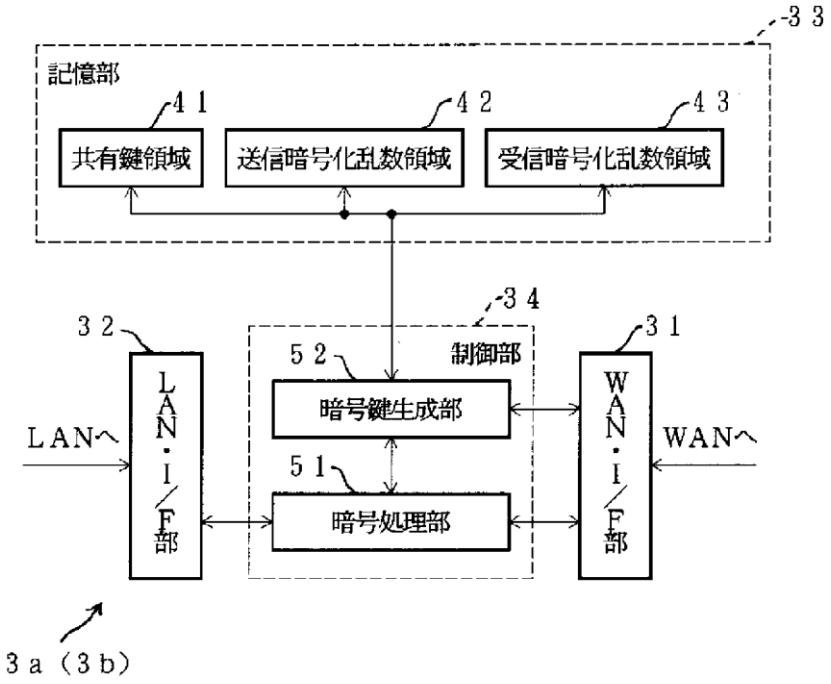
Ｆｉｇｕｒｅ　６．２．２．

（図６．２．２）

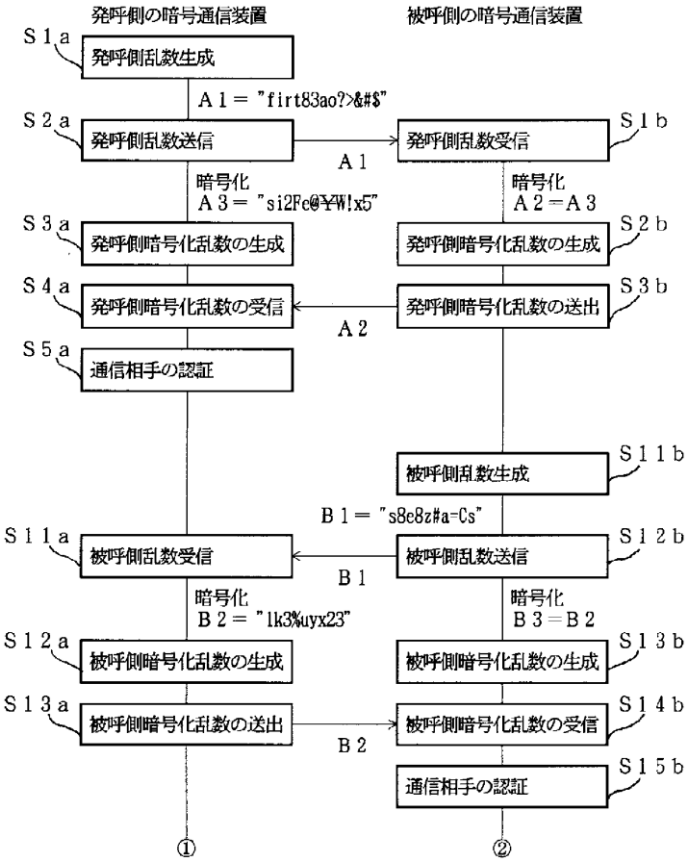


（別紙３）

【図１】


33
記憶部
41
42
43
共有鍵領域
送信暗号化乱数領域
受信暗号化乱数領域
34
32
52
制御部
31
LAN・I/F部
暗号鍵生成部
WAN・I/F部
LANへ
WANへ
51
暗号処理部
3a（3b）

【図５】


発呼側の暗号通信装置
被呼側の暗号通信装置
S1a
発呼側乱数生成
A1＝"firt83ao?>&#$"
S2a
発呼側乱数送信
A1
S1b
発呼側乱数受信
暗号化
A3＝"si2Fc@¥¥W!x5"
暗号化
A2＝A3
S3a
発呼側暗号化乱数の生成
S2b
発呼側暗号化乱数の生成
S4a
発呼側暗号化乱数の受信
A2
S3b
発呼側暗号化乱数の送出
S5a
通信相手の認証
S11b
被呼側乱数生成
B1＝"s8c8z#a-Cs"
S11a
被呼側乱数受信
B1
S12b
被呼側乱数送信
暗号化
B2＝"1k3%uyx23"
暗号化
B3＝B2
S12a
被呼側暗号化乱数の生成
S13b
被呼側暗号化乱数の生成
S13a
被呼側暗号化乱数の送出
B2
S14b
被呼側暗号化乱数の受信
S15b
通信相手の認証
①
②

【図６】

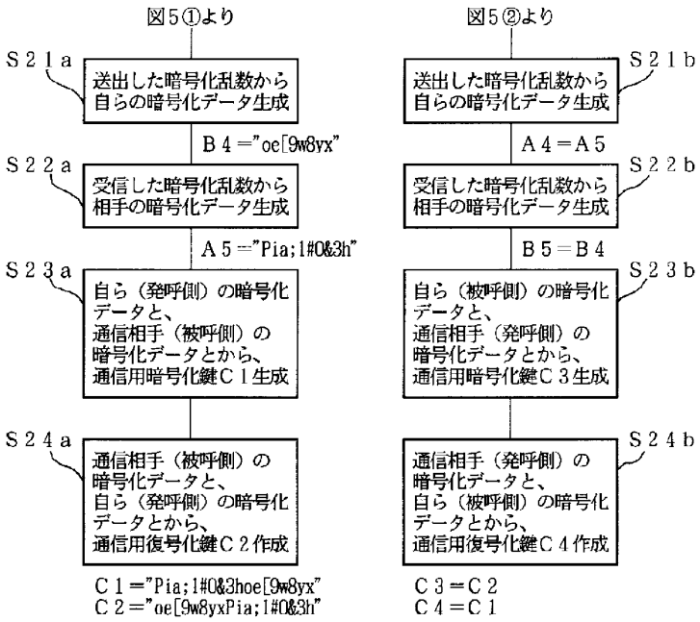
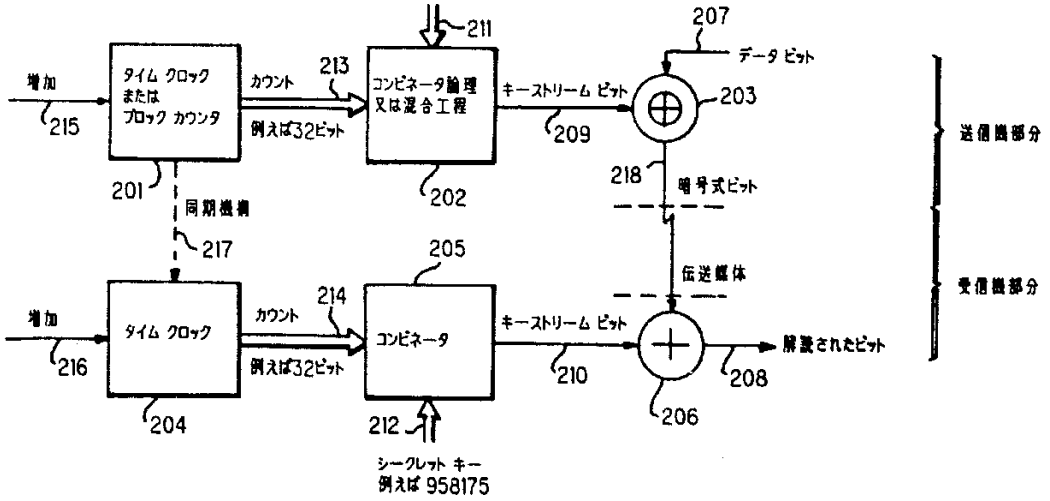


図5①より
図5②より
S21a
送出した暗号化乱数から
自らの暗号化データ生成
S21b
送出した暗号化乱数から
自らの暗号化データ生成
B4＝"oe[9w8yx"
A4＝A5
S22a
受信した暗号化乱数から
相手の暗号化データ生成
S22b
受信した暗号化乱数から
相手の暗号化データ生成
A5＝"Pia;1#O&3h"
B5＝B4
S23a
自ら（発呼側）の暗号化
データと、
通信相手（被呼側）の
暗号化データとから、
通信用暗号化鍵C1生成
S23b
自ら（被呼側）の暗号化
データと、
通信相手（発呼側）の
暗号化データとから、
通信用暗号化鍵C3生成
S24a
通信相手（被呼側）の
暗号化データと、
自ら（発呼側）の暗号化
データとから、
通信用復号化鍵C2作成
S24b
通信相手（発呼側）の
暗号化データと、
自ら（被呼側）の暗号化
データとから、
通信用復号化鍵C4作成
C1＝"Pia;1#O&3hoe[9w8yx"
C2＝"oe[9w8yxPia;1#O&3h"
C3＝C2
C4＝C1

（別紙４）

第４図


増加
215
タイム クロック
または
ブロック カウンタ
201
カウント
例えば32ビット
213
211
コンビネータ論理
又は混合工程
202
キーストリーム ビット
209
207
データ ビット
203
218
暗号式ビット
送信機部分
伝送媒体
受信機部分
同期機構
217
205
増加
216
タイム クロック
204
カウント
例えば32ビット
214
コンビネータ
212
シークレット キー
例えば 958175
キーストリーム ビット
210
解読されたビット
208
206

（別紙５）

ＦＩＧ ３Ａ

（図３Ａ）