

(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



(10) 国際公開番号

WO 2009/157172 A1

PCT

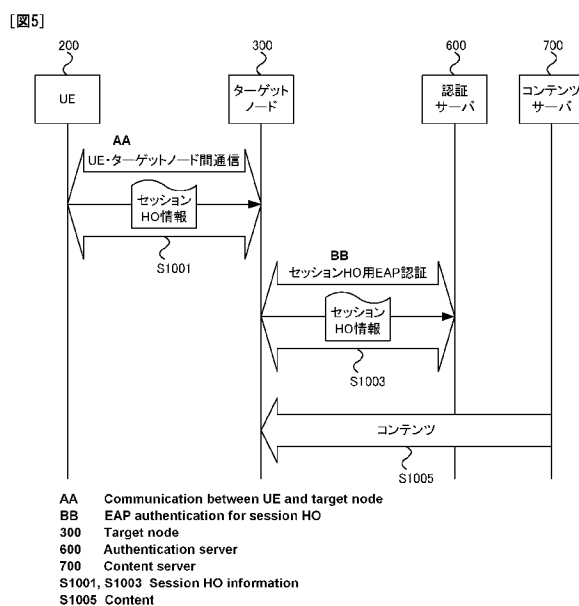
(43) 国際公開日
2009年12月30日(30.12.2009)

- (51) 国際特許分類:
H04W 36/14 (2009.01) H04W 12/06 (2009.01)
- (21) 国際出願番号: PCT/JP2009/002833
- (22) 国際出願日: 2009年6月22日(22.06.2009)
- (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 2008-168773 2008年6月27日(27.06.2008) JP
特願 2009-019217 2009年1月30日(30.01.2009) JP
- (71) 出願人(米国を除く全ての指定国について): パナソニック株式会社(PANASONIC CORPORATION) [JP/JP]; 〒5718501 大阪府門真市大字門真1006番地 Osaka (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 平野純(HIRANO, Jun). 荒牧隆(ARAMAKI, Takashi). 池田新吉(IKEDA, Shinkichi). 青山高久(AOYAMA, Takahisa).
- (74) 代理人: 二瓶正敬(NIHEI, Masayuki); 〒1600022 東京都新宿区新宿2-8-8とみん新宿ビル2F 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, JP, 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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, 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 (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) Title: COMMUNICATION SYSTEM, COMMUNICATION PROCESSING DEVICE AND AUTHENTICATION PROCESSING DEVICE

(54) 発明の名称: 通信システム及び通信処理装置並びに認証処理装置



(57) Abstract: Disclosed is technology to accomplish session handover between devices having different key generation functions in authentication protocol. With said technology, when a UE (200) hands over a session for receiving content from a content server (700) to a target node (300), first, the UE transfers information (session HO information) required for handover of said session to the target node (step S1001). The target node performs authentication processing with an authentication server 600 on the network to which the UE is connected and notifies the authentication server of the session HO information transferred from the UE (step S1003). The authentication server performs authentication for the session handover based on said session HO information, and if the authentication is successful, the session is handed over from the content server to the target node, and the content is distributed to the target node (step S1005).

(57) 要約: 認証プロトコルにおいて鍵生成機能が異なる装置間においてセッションハンドオーバーを行えるようにする技術が開示され、その技術によればUE 200がコンテンツサーバ700からコンテンツを受信するセッションをターゲットノード300へハンドオーバーさせる際、まずUEは、そのセッションをハンドオーバーさせるために必要な情報

(セッションHO情報)をターゲットノードへ渡す(ステップS1001)。ターゲットノードは、UEが接続しているネットワークの認証サーバ600との間で認証処理を行うと共に、UEから渡されたセッションHO情報を認証サーバへ通知する(ステップS1003)。認証サーバは、このセッションHO情報に基づいてセッションハンドオーバーのための認証を行い、認証に成功するとコンテンツサーバからターゲットノードへセッションがハンドオーバーされて、ターゲットノードへコンテンツが配信されるようになる(ステップS1005)。

WO 2009/157172 A1



添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：通信システム及び通信処理装置並びに認証処理装置 技術分野

[0001] 本発明は、パケット交換型データ通信ネットワークにおける通信技術に関し、特に、ユーザ端末（UE：User Equipment）がEAP（Extensible Authentication Protocol：拡張認証プロトコル）などの認証プロトコルを用いてネットワークへの接続を行う際の通信技術に関する。

背景技術

[0002] 現在、基地局1台あたりが中長距離のサービスエリアを包含するセルラ通信などの無線通信機能や、サービスエリアが比較的短距離な無線LAN（Local Area Network：ローカルエリアネットワーク）機能などを有し、複数の異種ネットワークで構成されるネットワークを用いて通信サービスを行うシステムや、これらのネットワークに接続可能な無線通信端末が存在している。

[0003] このような複数の異種ネットワークから構成されるネットワークとして、3GPP（Third Generation Partnership Project：第3世代パートナーシッププロジェクト）では、3GPPネットワーク（以下3Gネットワークと記載）に加えて、無線LAN、その他のセルラネットワーク（第2世代までのネットワーク、3GPP2ネットワークなどを含む）、WiMAX（Worldwide Interoperability for Microwave Access、IEEE 802.16）タイプの無線ワイドエリアネットワーク（WWAN：Wireless Wide Area Network）などの様々な異種ネットワークとの通信機能を有する無線通信端末及び関連する通信技術に関する議論が行われている。

[0004] 特に、このような異種ネットワークにおいて、シームレスなモビリティの実現や、リアルタイムビデオ、VoIP（Voice over Internet Protocol）などのセッションにモビリティサービスを付加することなどを目指した議論が行われている。例えば、下記の非特許文献1には、異種ネットワーク環境において、3Gネットワークと非3Gネットワークとの関係が検討されてお

り、主に、UEによる異種ネットワーク間の物理的なハンドオーバーに関して考察されている。

[0005] また、これらのネットワークにおいては、認証、アクセスコントロール、課金に関する規定も重要な要件となる。例えばセルラネットワークにおいてはUMTS (Universal Mobile Telecommunications System) でのAKA (Authentication and Key Agreement) やGSM (Global System for Mobile communications) でのSIM (GSM Subscriber Identification Module) の機能に基づいて認証を行うことが検討されている。

[0006] これらの機能の多くは、例えば、下記の非特許文献2や下記の非特許文献3に記載されているEAPを用いた通信方法で使用される。例えば、下記の非特許文献4に記載されているEAP-SIMにおいては、EAPのプロトコルに基づいて、SIMカード内の情報を用いて認証とセッション鍵の交換が行われる。また、下記の非特許文献5に記載されているEAP-AKAは、GSMでの認証との互換性を考慮して3Gネットワークで使えるよう拡張されたものである。また、LAN接続時に使用する認証規格であるIEEE (Institute of Electrical and Electronic Engineers) 802.1Xにおいても、EAP-MD5 (EAP - Message Digest version 5) やEAP-TLS (EAP - Transport Layer Security) など、様々なEAPを用いた認証が可能である。

[0007] 一方、下記の非特許文献6には、UEが行っている通信のセッションを他のUEへ移すセッションのモビリティに関する技術が記載されている。この非特許文献6に記載されている技術では、あるUEが利用しているセッションの一部又はすべてを別のUEへ移す際のセッションの連続性に関して検討されている。

[0008] また、下記の非特許文献7及び非特許文献8において、地震や津波などの災害情報を通知する仕組みに関する検討がなされている。非特許文献7に記載されているシステムは、地震や津波などの災害発生時に3GPPネットワークを利用して災害情報を通知するシステムであり、ETWS (Earthquake

Tsunami Warning System：地震津波警報システム）と呼ばれている。

[0009] このETWSは、端末（UE：User Equipment）に災害の発生を伝えるためのシステムであり、地震や津波などを始めとする100種類程度の災害の発生を知らせる第1報（以下、プライマリ通知：Primary Notificationと記載）と、災害の詳細な情報を知らせる第2報（以下、セカンダリ通知：Secondary Notificationと記載）を報知する。

[0010] 具体的には、例えば、災害発生時に3Gネットワーク側から基地局に対して災害発生が通知され、基地局から端末に対して緊急に報知情報として通知が行われる。基地局は、プライマリ通知を受信してから4秒以内に、第1報を端末に伝えることが要求されている。このプライマリ通知の端末への緊急通知には、システム情報として報知することが考えられている。また、このような災害の緊急通知以外においても、通信セル内のトラフィックの急激な増加などによる緊急のアクセスクラス制御などのシステム情報に関しても、特定の期間（Modification period）内で変更を通知することにより、より端末のアクセス制御が細かくできるようになると考えられる。

[0011] 少なくともプライマリ通知は最優先で端末に通知される必要があり、将来的にはMBMS（Multimedia Broadcast and Multicast Service：マルチメディアブロードキャスト／マルチキャストサービス）によってセカンダリ情報を通知することも検討されている。また、ETWSにおける災害情報の通知サービスはマクロ基地局（NE／eNB）だけではなく、よりローカルな基地局（HNB／HeNB）に対しても提供されるかどうかに関しては議論が行われているが、機能的にはローカルの基地局に対しても提供可能である。

先行技術文献

非特許文献

[0012] 非特許文献1：3GPP TS 23.402 V8.0.0、2007-12

非特許文献2：RFC2284、“PPP Extensible Authentication Protocol”、March 1998

非特許文献3：RFC3748、“Extensible Authentication Protocol (EAP)”、June 2004

非特許文献4：RFC4186、“Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”、January 2006

非特許文献5：RFC4187、“Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”、January 2006

非特許文献6：3GPP TR 23.893 V8.0.0、2008-06 (5.4章)

非特許文献7：3GPP TS22.168 V8.1.0、Earthquake and Tsunami Warning System (ETWS) requirements, 2008-06

非特許文献8：3GPP TS36.331 V8.4.0、Evolved Universal Terrestrial Radio Access (E-UTRA)；Radio Resource Control (RRC)；Protocol specification, 2008-12

[0013] しかしながら、利用者の利便性をより高めるために利用者の所有する装置間でセッションにモビリティサービスを付加した場合、オペレーションの要件によっては必ずしも自由にセッションのハンドオーバーが行えるとは限らないという問題がある。すなわち、例えば認証に必要な機能を持たない装置や認証の方式が異なる装置に対しては、機器間でのセッションハンドオーバーを行うことができない場合がある。

[0014] 例えば、図9において、利用者の端末（UE 200）が接続している3Gネットワーク400に存在するサービスネットワーク450からリアルタイムビデオの提供を受けている場合に、同一の接続基地局460（後述の図1のHeNB/Home-GW100に対応）の配下（若しくはネットワークを介して到達可能な状態）に存在するターゲットノード（TVセット）300へリアルタイムビデオのセッションをハンドオーバーし、ターゲットノード300においてリアルタイムビデオの視聴を行いたいとする。

[0015] このとき、ターゲットノード300もUE200と同様の3Gネットワー

ク４００に対する認証機能の要件（例えば、ターゲットノード３００がＳＩＭカードを有しており、３Ｇネットワーク４００のオペレータとの契約などの関係によって、ＳＩＭカード内の情報を利用した認証鍵が使用可能である場合など）を満たしていれば、３Ｇネットワーク４００のオペレータ側の何らかの操作によって、ターゲットノード３００が３Ｇネットワーク４００に認証されてセッションのハンドオーバが実現可能となるかもしれない。

- [0016] しかしながら、通常、ＴＶセットのようなターゲットノード３００には移動端末としての主要な機能が実装されていないことが多く、３Ｇネットワーク４００への接続に利用される認証機能（３Ｇネットワーク４００のオペレータが規定している認証方式）とは異なる認証機能しか有していない場合が多い。そのため、ターゲットノード３００が、たとえＵＥ２００の利用者本人が所有する機器であっても３Ｇネットワーク４００との間の認証が成功せず、３Ｇネットワーク４００への接続を行うことができないか、あるいは、３Ｇネットワーク４００からのセッションのセッション鍵を生成することができないために、セッションのハンドオーバが実現できないという問題がある。

発明の概要

- [0017] 上記の課題を解決するため、本発明は、認証プロトコルにおいて鍵生成機能が異なる装置間においてセッションハンドオーバを行えるようにする通信システム及び利用者端末並びに認証サーバを提供することを目的とする。
- [0018] 上記の目的を達成するため、本発明の通信システムは、第１ネットワークに属する第１ノードが保持している前記第１ネットワークとの間の認証用情報を利用して、前記第１ノードと前記第１ネットワークとの間の通信中のセッションを前記第１ネットワークとは異なる第２ネットワークに属する第２ノードへハンドオーバさせるための認証が行われるよう構成されている。

この構成により、認証プロトコルにおいて鍵生成機能が異なる装置間においてセッションハンドオーバを行うことが可能となる。

- [0019] また、上記の目的を達成するため、本発明の通信処理装置は、第１ネット

ワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第1ノードに実装される通信処理装置であって、

前記第2ノードが前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバーのための認証処理を行う際に前記認証サーバへ通知するための前記セッションのハンドオーバーのための認証に必要な情報を、前記第2ノードへ通知するよう構成されている。

この構成により、認証プロトコルにおいて鍵生成機能が異なる装置間において、セッションのハンドオーバー先となる第2ノードが認証処理を行うことによってセッションハンドオーバーを行うことが可能となる。

[0020] また、上記の目的を達成するため、本発明の通信処理装置は、第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第1ノードに実装される通信処理装置であって、

前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバーのための認証処理を行う際に、前記第2ノードの識別情報を前記認証サーバへ通知するよう構成されている。

この構成により、認証プロトコルにおいて鍵生成機能が異なる装置間において、セッションのハンドオーバー元となる第1ノードが認証処理を行うことによってセッションハンドオーバーを行うことが可能となる。

[0021] また、上記の目的を達成するため、本発明の通信処理装置は、第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属す

る第2ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第2ノードに実装される通信処理装置であって、

前記セッションのハンドオーバーのための認証に必要な情報を前記第1ノードから受信し、前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバーのための認証処理を行う際に、前記セッションのハンドオーバーのための認証に必要な情報に基づいて生成された情報を前記認証サーバへ通知するよう構成されている。

この構成により、認証プロトコルにおいて鍵生成機能が異なる装置間において、セッションのハンドオーバー先となる第2ノードが認証処理を行うことによってセッションハンドオーバーを行うことが可能となる。

[0022] また、上記の目的を達成するため、本発明の通信処理装置は、第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第2ノードに実装される通信処理装置であって、

前記第1ノードが前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバーのための認証処理を行う際に前記認証サーバへ通知するための前記第2ノードの識別情報を、前記第1ノードへ通知するよう構成されている。

この構成により、認証プロトコルにおいて鍵生成機能が異なる装置間において、セッションのハンドオーバー元となる第1ノードが認証処理を行うことによってセッションハンドオーバーを行うことが可能となる。

[0023] また、上記の目的を達成するため、本発明の認証処理装置は、第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバーさせるための認証が行われるよう構成されてい

る通信システムの前記第 1 ネットワークに属する認証サーバに実装される認証処理装置であって、

前記第 2 ノードとの間で前記セッションのハンドオーバーのための認証処理を行う際に、前記第 2 ノードが前記第 1 ノードから受信した前記セッションのハンドオーバーのための認証に必要な情報に基づいて生成した情報を前記第 2 ノードから受信し、前記セッションのハンドオーバーのための認証に必要な情報に基づいて生成された前記情報を利用して前記セッションのハンドオーバーのための認証を行うように構成されている。

この構成により、認証プロトコルにおいて鍵生成機能が異なる装置間において、セッションのハンドオーバー先となる第 2 ノードが認証処理を行うことによってセッションハンドオーバーを行うことが可能となる。

[0024] また、上記の目的を達成するため、本発明の認証処理装置は、第 1 ネットワークに属する第 1 ノードが保持している前記第 1 ネットワークとの間の認証用情報を利用して、前記第 1 ノードと前記第 1 ネットワークとの間の通信中のセッションを前記第 1 ネットワークとは異なる第 2 ネットワークに属する第 2 ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第 1 ネットワークに属する認証サーバに実装される認証処理装置であって、

前記第 1 ノードとの間で前記セッションのハンドオーバーのための認証処理を行う際に、前記第 2 ノードの識別情報を前記第 1 ノードから受信するように構成されている。

この構成により、認証プロトコルにおいて鍵生成機能が異なる装置間において、セッションのハンドオーバー元となる第 1 ノードが認証処理を行うことによってセッションハンドオーバーを行うことが可能となる。

[0025] 本発明は、上記の構成を有しており、認証プロトコルにおいて鍵生成機能が異なる装置間においてセッションハンドオーバーを行えるようになるという効果を有する。

図面の簡単な説明

[0026] [図1]本発明の第1及び第2の実施の形態におけるネットワークシステムの構成の一例を示す図

[図2]本発明の第1の実施の形態におけるUEの構成の一例を示す図

[図3]本発明の第1の実施の形態におけるターゲットノードの構成の一例を示す図

[図4]本発明の第1及び第2の実施の形態における認証サーバの構成の一例を示す図

[図5]本発明の第1の実施の形態における動作の一例を示すシーケンスチャート

[図6]本発明の第2の実施の形態におけるUEの構成の一例を示す図

[図7]本発明の第2の実施の形態におけるターゲットノードの構成の一例を示す図

[図8]本発明の第2の実施の形態における動作の一例を示すシーケンスチャート

[図9]本発明に係る課題を説明するための従来技術におけるネットワークシステム構成の一例を示す図

[図10]本発明の第3の実施の形態における認証サーバの構成の一例を示す図

[図11]本発明の第3の実施の形態におけるUEの構成の一例を示す図

[図12]本発明の第3の実施の形態における動作の一例を示すシーケンスチャート

[図13]本発明の第4の実施の形態における動作の一例を示すシーケンスチャート

発明を実施するための形態

[0027] 以下、図面を参照しながら、本発明の第1及び第2の実施の形態について説明する。まず、本発明の第1及び第2の実施の形態におけるネットワークシステムの構成について説明する。

[0028] 図1は、本発明の第1及び第2の実施の形態におけるネットワークシステムの構成の一例を示す図である。図1に図示されているネットワークシステ

ムにおいて、あるユーザのUE（例えば、3G通信可能な携帯電話機）200が、ユーザ自身の家屋に設置された小型の基地局（HeNB：Home eNB）を介して、第1ネットワークオペレータが管理する3Gネットワーク（第1ネットワーク）400に接続している。ここでは、UE200は、3Gネットワーク400を管理する第1ネットワークオペレータとの間でEAPを用いて認証を完了し、サービスネットワーク450のコンテンツサーバ（図1には不図示、後述のコンテンツサーバ700に対応）からコンテンツ（例えば、リアルタイムビデオ）の配信を受けているとする。

[0029] また、ターゲットノード（例えば、TVセット）300はホームゲートウェイ（Home-GW）経由で、第2ネットワークオペレータ（第1ネットワークオペレータとは異なるネットワークオペレータ）が管理するネットワーク500に接続している。なお、ここでは、HeNBとHome-GWとが同一の装置に実装されているとし、HeNB及びHome-GWを合わせてHeNB/Home-GW100と記載するが、HeNB及びHome-GWは分離されていてもよい。ターゲットノード300と第2ネットワークオペレータとの間においても認証が行われているが、UE200と第1ネットワークオペレータとの間とは異なる認証機能及び認証鍵を用いて行われているとする。すなわち、UE200は3Gネットワーク400での認証に利用可能なSIMカード（SIM）250を有している一方、ターゲットノード300は3Gネットワーク400での認証に利用可能なSIMカード250を有していない。なお、3Gネットワーク400へ接続する際に認証サーバとして機能する認証エンティティの機能の一部又はすべては、例えば、HeNB/Home-GW100に実装されていてもよく、あるいは、3Gネットワーク400内の他の任意のノードに実装されていてもよい。

[0030] <第1の実施の形態>

以下、本発明の第1の実施の形態について説明する。本発明の第1の実施の形態では、UE200が読み出し可能なSIMカード250内の情報（以下、SIM情報と呼ぶ）を利用して、ターゲットノード300が3Gネット

ワーク４００側からセッションハンドオーバを受ける方法について説明する。
。

[0031] 図２は、本発明の第１の実施の形態におけるＵＥの構成の一例を示す図である。図２に図示されているＵＥ２００は、通信部（下位レイヤ）２１１、ＳＩＭインタフェース２１２、セッションハンドオーバ情報準備部２１３、ＵＥ・ターゲットノード間通信部２１４、３Ｇネットワーク用通信部２１５を有しており、３Ｇネットワーク用通信部２１５はＥＡＰ認証機能部２１６を更に有している。

[0032] 通信部（下位レイヤ）２１１は、他のノードと通信を行うための通信機能を表すものであり、１つ又は複数のネットワークインタフェースを有している。ＵＥ２００が携帯電話機の場合には、通信部（下位レイヤ）２１１は無線通信機能を有している。この通信部（下位レイヤ）２１１の通信機能によって、ＵＥ２００は、３Ｇネットワーク４００やその他のネットワークに接続されているノードと通信を行うことが可能であるとともに、ターゲットノード３００と通信を行うことも可能である。

[0033] また、ＳＩＭインタフェース２１２は、ＵＥ２００に装着されているＳＩＭカード２５０（あるいは、ＵＳＩＭ（Universal Subscriber Identity Module）カード）に格納されているＳＩＭ情報を読み出す機能を有している。なお、ＳＩＭインタフェース２１２及びＳＩＭカード２５０は、特に３Ｇネットワーク４００に接続する場合（ＵＥ２００が携帯電話機である場合）の一例であり、ＵＥ２００が認証に用いる情報を保持、取得又は生成する機能と置き換え可能である。

[0034] また、セッションハンドオーバ情報準備部２１３は、ＳＩＭインタフェース２１２によりＳＩＭカード２５０から読み出せるＳＩＭ情報のうち、セッションハンドオーバの認証のために必要な情報（以下、セッションＨＯ（Handover：ハンドオーバ）情報と記載）を取り出して、そのセッションＨＯ情報をターゲットノード３００へ転送できるように準備する機能を有している。なお、セッションＨＯ情報の転送準備（あるいは、実際の転送）は、ユーザ

による入力指示、ターゲットノード300からの要求、ネットワーク側からの指示などを始めとして、任意のタイミングで実行可能である。

[0035] また、UE・ターゲットノード間通信部214は、UE200がターゲットノード300との間で通信を行うための機能を有している。UE・ターゲットノード間通信部214は、セッションハンドオーバー情報準備部213によって準備されたセッションHO情報をターゲットノード300へ送信することが可能である。なお、後述のように、UE200とターゲットノード300の間には信用関係が存在することが望ましく、UE・ターゲットノード間通信部214によってターゲットノード300へ送信されるセッションHO情報は、セキュアな状態で伝送されることが望ましい。

[0036] また、3Gネットワーク用通信部215は、UE200が3Gネットワーク400の任意のノードと通信を行うための機能を有している。3Gネットワーク用通信部215は、3Gネットワーク400に属するサービスネットワーク450のサーバ（例えば、後述のコンテンツサーバ700）からコンテンツ（例えば、リアルタイムビデオ）を受信することも可能である。なお、3Gネットワーク用通信部215は、セッションハンドオーバーの認証に成功した場合に、3Gネットワーク400内のノード（例えば、3Gネットワーク400の認証サーバ600）に対して、セッションをハンドオーバーさせるためのシグナリングを送信してもよく、あるいは、ターゲットノード300に対してセッションハンドオーバーの開始指示を送信し、セッションをハンドオーバーさせるためのシグナリングをターゲットノード300に送信させてもよい。

[0037] また、3Gネットワーク用通信部215のEAP認証機能部216は、UE200が3Gネットワーク400へ接続する際に、3Gネットワーク400（例えば、後述の認証サーバ600）との間でEAP認証を行う機能を有している。このEAP認証は、従来のUE200によって行われているEAP認証と同一であり、SIMインタフェース212によってSIMカード250から読み出されたSIM情報を用いて行われる。

[0038] また、図 3 は、本発明の第 1 の実施の形態におけるターゲットノードの構成の一例を示す図である。図 3 に図示されているターゲットノード 300 は、通信部（下位レイヤ）311、セッションハンドオーバー情報取得部 312、UE・ターゲットノード間通信部 313、セッションハンドオーバー用通信部 314、第 2 ネットワークオペレータ通信部 316 を有しており、セッションハンドオーバー用通信部 314 はセッションハンドオーバー用 EAP 認証拡張機能部 315 を更に有している。

[0039] 通信部（下位レイヤ）311 は、他のノードと通信を行うための通信機能を表すものであり、1 つ又は複数のネットワークインタフェースを有している。この通信部（下位レイヤ）311 の通信機能によって、ターゲットノード 300 は、第 2 ネットワーク 500 やその他のネットワークに接続されているノードと通信を行うことが可能であるとともに、UE 200 と通信を行うことも可能である。

[0040] また、セッションハンドオーバー情報取得部 312 は、UE・ターゲットノード間通信部 313 で UE 200 から受信したセッション H O 情報を取得し、必要であれば前処理を行った後、セッションハンドオーバー用 EAP 認証拡張機能部 315 へ渡す機能を有している。

[0041] また、UE・ターゲットノード間通信部 313 は、ターゲットノード 300 が UE 200 との間で通信を行うための機能を有している。UE・ターゲットノード間通信部 313 は、UE 200 から送信されたセッション H O 情報を受信することが可能である。なお、後述のように、UE 200 とターゲットノード 300 との間には信用関係が存在することが望ましく、UE・ターゲットノード間通信部 313 が UE 200 から受信するセッション H O 情報は、セキュアな状態で伝送されることが望ましい。

[0042] また、セッションハンドオーバー用通信部 314 は、UE 200 によって 3G ネットワーク 400 との間で保持されているセッションを譲り受けるための処理を行う機能を有している。セッションハンドオーバー用通信部 314 は、セッションハンドオーバー用 EAP 認証拡張機能部 315 におけるセッシ

ンハンドオーバの認証に成功した場合、3 Gネットワーク400内のノード（例えば、3 Gネットワーク400の認証サーバ600）に対して、セッションをハンドオーバさせるためのシグナリングを送信してもよく、あるいは、UE200からセッションハンドオーバの開始指示を受信してから、セッションをハンドオーバさせるためのシグナリングを送信してもよい。

[0043] また、セッションハンドオーバ用通信部314のセッションハンドオーバ用EAP認証拡張機能部315は、UE200によって3 Gネットワーク400との間で保持されているセッションを譲り受けるために、3 Gネットワーク400（例えば、認証サーバ600）との間でEAP認証を行う機能を有している。なお、セッションハンドオーバ用EAP認証拡張機能部315は、3 Gネットワーク400との間のEAP認証の過程で、セッションハンドオーバ情報取得部312から取得したセッションHO情報を利用して、認証を受けるとともに、ターゲットノード300が受信しようとしているセッションのセッション鍵の交換を行う。

[0044] また、第2ネットワークオペレータ通信部316は、ターゲットノード300が第2ネットワーク500の任意のノードと通信を行うための機能を有している。なお、ターゲットノード300が第2ネットワーク500に接続する際の認証処理も、この第2ネットワークオペレータ通信部316によって行われる。

[0045] また、図4は、本発明の第1の実施の形態における認証サーバの構成の一例を示す図である。図4に図示されている認証サーバ600は、通信部（下位レイヤ）611、セッションハンドオーバ処理部612、第2ネットワークオペレータ通信部613、3 Gネットワーク用通信部614を有しており、3 Gネットワーク用通信部614はEAP認証機能部615を更に有しており、EAP認証機能部615はセッションハンドオーバ用EAP認証拡張機能部616を更に有している。なお、図4に図示されている認証サーバ600の機能は、3 Gネットワーク400に属する任意のノード（例えば、HeNB/Home-GW100）に実装可能であり、また、複数のノードに

分散（例えば、認証エンティティが3 Gネットワーク400上で多段に構成）されていてもよい。

[0046] 通信部（下位レイヤ）611は、他のノードと通信を行うための通信機能を表すものであり、1つ又は複数のネットワークインタフェースを有している。この通信部（下位レイヤ）611の通信機能によって、第2ネットワーク500やその他のネットワークに接続されているノードと通信を行うことが可能であるとともに、UE200やターゲットノード300と通信を行うことも可能である。

[0047] また、セッションハンドオーバー処理部612は、セッションハンドオーバー用EAP認証拡張機能部616におけるEAP認証によって、UE200によって3 Gネットワーク400との間で保持されているセッションをターゲットノード300へ移すことが許可された場合に、そのセッションをUE200からターゲットノード300へハンドオーバーさせる機能を有している。なお、セッションハンドオーバー処理部612は、このセッションの送信元（例えば、コンテンツサーバ700）やセッションの通過点のノードに対して、セッションの送信先をUE200からターゲットノード300へ切り換える（第2ネットワーク経由となる場合も考えられる）よう指示してもよく、また、認証サーバ600がこのセッションの通過点のノードに実装されている場合（例えば、認証サーバ600がHeNB/Home-GW100に実装されている場合）には、自身のノード（例えば、HeNB/Home-GW100）でセッションの送信先をUE200からターゲットノード300へ切り換えてもよい。なお、セッションハンドオーバーのための認証と、実際のセッションハンドオーバーの処理が分離されている場合は、例えば、セッションハンドオーバー用EAP認証拡張機能部616におけるEAP認証が完了した後、認証サーバ600、UE200、ターゲットノード300、その他の3 Gネットワーク400内のノードが実際のセッションハンドオーバーの処理を開始し、セッションの送信先をUE200からターゲットノード300へ切り換えてもよい。特に、UE200及びターゲットノード300が上位

レイヤプロトコルとしてセッションの制御にSIP (Session Initiation Protocol) を使用している場合は、SIPで規定されているDIFFERメッセージ及びINVITEメッセージなどを用いてセッションの切り換えを行うことができる。

[0048] また、第2ネットワークオペレータ通信部613は、認証サーバ600が第2ネットワーク500に属する任意のノード（例えば、ターゲットノード300）と通信を行うための機能を有している。

[0049] また、3Gネットワーク用通信部614は、認証サーバ600が3Gネットワーク400の任意のノードと通信を行うための機能を有している。また、実際のセッションハンドオーバは、例えば、認証サーバ600からコンテンツサーバ700へセッションの切り換え指示が行われてコンテンツサーバ700がターゲットノード300に対してコンテンツを配信するなどのように、3Gネットワーク400内部で行われてもよく、また、HeNB/Home-GW100のような分岐点においてUE200からターゲットノード300へコンテンツの配信先を切り換えてもよい。なお、3Gネットワーク用通信部614は、セッションハンドオーバの認証に成功した場合に、セッションに係るデータを転送している装置（セッションを中継する装置、又は、セッションの送信元であるコンテンツサーバ700）に対して、セッションの転送先をUE200からターゲットノード300へ切り換えさせるシグナリングを送信してもよく、認証サーバ600自身がセッションを中継しているとき（例えば、HeNB/Home-GW100に認証サーバ600が実装されているとき）には、この装置自身が、セッションの転送先をUE200からターゲットノード300へ切り換えてもよい。

[0050] また、3Gネットワーク用通信部614のEAP認証機能部615は、UE200が3Gネットワーク400へ接続する際に、UE200との間でEAP認証を行う機能を有している。

[0051] また、EAP認証機能部615のセッションハンドオーバ用EAP認証拡張機能部616は、UE200によって3Gネットワーク400との間で保

持されているセッションを譲り受けようとしているターゲットノード300との間でEAP認証を行う機能を有している。なお、セッションハンドオーバー用EAP認証拡張機能部616は、ターゲットノード300との間のEAP認証の過程で、ターゲットノード300からセッションHO情報を受信することにより、ターゲットノード300が譲り受けようとしているセッションの保持者（UE200）の認証を行って、ターゲットノード300との間でターゲットノード300が受信しようとしているセッションのセッション鍵の交換を行う。

[0052] 次に、図1のネットワークシステム構成、及び、図2に図示されているUE200、図3に図示されているターゲットノード300、図4に図示されている認証サーバの各構成に基づいて、本発明の第1の実施の形態における動作について説明する。図5は、本発明の第1の実施の形態における動作の一例を示すシーケンスチャートである。

[0053] 図5において、UE200からターゲットノード300へのセッションハンドオーバーが開始されると、まず、UE200のセッションハンドオーバー情報準備部213は、UE200自身に取り付けられているSIMカード250から読み出すことが可能なSIM情報からセッションHO情報を取り出し、そのセッションHO情報をターゲットノード300に転送できるように準備する。セッションHO情報には、セッションハンドオーバーの認証のために必要な情報が含まれているが、特定のセッションのみをUE200からターゲットノード300へ移したい場合には、そのセッションを特定するための情報（あるいは、そのセッションをハンドオーバーさせるために必要な情報）が含まれていてもよい。

[0054] このとき、セッションHO情報は、あらかじめ3Gネットワーク400を管理する第1ネットワークオペレータとの間で取り決めがなされていることが望ましい。特に、時系列に関する情報（シリアルナンバーや時間情報など）と共に構成され、1回のみの使用（ワンタイム使用）に制限できるようになっていたり（リプレイ攻撃耐性を考慮）、ハッシュ関数などにより元の情

報要素を類推できないようになっていたり、通常の接続認証に用いる情報とは分離され、情報要素が万一漏洩した場合であっても他の通信のための接続には影響がないように構成されていたりすることが望ましい。

[0055] 次に、UE 200のUE・ターゲットノード間通信部214は、上記のように準備したセッションHO情報をターゲットノード300へ送信する（ステップS1001）。なお、UE 200とターゲットノード300との間には、信用関係が存在することが望ましい。例えば、ネットワークオペレータに接続する認証機能とは別の機器間の認証機能によって互いの装置の単一性や意図している装置であることが確認できているか、さらには第三者によって情報を収集されていないことや改ざんされていないことが確認できている（例えば、暗号化されている）ことが望ましい。このとき、例えばUE 200とターゲットノード300との間においてEAP認証が行われてもよい。

[0056] また、UE 200とターゲットノード300との間は、短距離無線通信などのような直接のリンク（有線接続を含む）で通信が行われてもよく、また、3Gネットワーク400又はターゲットノード300の属するネットワーク（第2ネットワークオペレータが管理する第2ネットワーク500）若しくはその両方のネットワークを介した通信経路によって通信が行われてもよく、さらには、HeNB/Home-GW100経由で通信が行われてもよい。

[0057] ステップS1001でUE 200からセッションHO情報を受信したターゲットノード300は、セッションハンドオーバー用EAP認証拡張機能部315において、UE 200から受信したセッションHO情報に基づいて生成された情報を利用して、3Gネットワーク400に対してEAP認証を行う（ステップS1003）。このとき、認証先となる認証サーバ600は、3Gネットワーク400側やUE 200から示されてもよく、また、HeNB/Home-GW100のように一体化された装置、若しくは情報転送の分岐点となる装置が認証サーバ600であってもよい。

[0058] この例では、ターゲットノード300が通常EAP認証を行っているHo

m e - G W と H e N B とは同一の装置（H e N B / H o m e - G W 1 0 0）であるため、ターゲットノード 3 0 0 は、3 G ネットワーク 4 0 0 に対する E A P 認証の際にセッション H O 情報（若しくは、この情報に基づいて認証鍵として生成できる情報）を使用し、セッション鍵などの情報を取得することでセッションハンドオーバーのための認証を完了することが可能である。なお、既に従来のアクセス認証の動作によってターゲットノード 3 0 0 と H o m e - G W との間におけるアクセス認証が完了している場合には、H e N B によってターゲットノード 3 0 0 の再認証や追加認証として行われてもよい。

[0059] 認証サーバ 6 0 0 は、セッションハンドオーバー用 E A P 認証拡張機能部 3 1 5 において、ターゲットノード 3 0 0 から受信したセッション H O 情報に基づいてセッションハンドオーバーのための認証を行い、セッションのハンドオーバー元の U E 2 0 0 を検証するとともに、セッションのハンドオーバー先のターゲットノード 3 0 0 を特定する。セッションハンドオーバーのための認証が完了すると、認証サーバ 6 0 0 のセッションハンドオーバー処理部 6 1 2 は、U E 2 0 0 からターゲットノード 3 0 0 へセッションをハンドオーバーさせる処理を開始する。これにより、3 G ネットワーク 4 0 0 側ではそれまで U E 2 0 0 に送信していたコンテンツ（リアルタイムビデオ）のセッションをターゲットノード 3 0 0 にハンドオーバーさせることによって、コンテンツ（リアルタイムビデオ）のセッションがターゲットノード 3 0 0 へ移り、サービスネットワーク 4 5 0 上のコンテンツサーバ 7 0 0 からターゲットノード 3 0 0 へコンテンツ（リアルタイムビデオ）が配信されるようになる（ステップ S 1 0 0 5）。

[0060] なお、特定のセッションのハンドオーバーが指定されている場合には、3 G ネットワーク 4 0 0 側はそのセッションのみハンドオーバーさせる。また、実際のセッションハンドオーバーは、例えば、認証サーバ 6 0 0 からコンテンツサーバ 7 0 0 へセッションの切り換え指示が行われてコンテンツサーバ 7 0 0 がターゲットノード 3 0 0 に対してコンテンツを配信するなどのように、

3 G ネットワーク 4 0 0 内部で行われてもよく、また、H e N B / H o m e - G W 1 0 0 のような分岐点において U E 2 0 0 からターゲットノード 3 0 0 へコンテンツの配信先を切り換えてもよい。また、認証サーバ 6 0 0 からコンテンツサーバ 7 0 0 への認証の成功に基づくセッションハンドオーバーの手続きは、任意の方法が利用可能である。図面においても、この 2 者間（若しくは仲介者が介在するかもしれない）の手続きについては不図示としている。

[0061] 以上のような認証方法により、ターゲットノード 3 0 0 は自身の認証情報（ターゲットノード 3 0 0 の I D など）では直接的に E A P 認証が不可能な場合であっても、セッションハンドオーバーのための認証を完了することができる。なお、ターゲットノード 3 0 0 へセッションのハンドオーバーが行われた場合であっても、そのセッションの権利（あるいは、課金などの責任）は U E 2 0 0 に残ることになる。

[0062] また、いったんターゲットノード 3 0 0 へ移されたセッションを元の U E 2 0 0 に戻すためのセッションハンドオーバーでは、本来の認証情報を U E 2 0 0 が持っているので、認証関係が維持されている場合はそのままの状態セッションハンドオーバーの準備が完了しており、また、認証関係が維持されていない場合であっても、再度認証を行うことによりセッションハンドオーバーの準備が完了する。この後、U E 2 0 0 若しくはセッションが移されていたターゲットノード 3 0 0 がセッションハンドオーバーの手順を開始すると、3 G ネットワーク 4 0 0 側ではそれまでターゲットノード 3 0 0 に送信していたコンテンツ（リアルタイムビデオ）のセッションを U E 2 0 0 にハンドオーバーさせることで、セッションが U E 2 0 0 に戻される。

[0063] なお、U E 2 0 0 やターゲットノード 3 0 0 からの 3 G ネットワークへの通信の一部又はすべてや、U E 2 0 0 からターゲットノード 3 0 0 へのハンドオーバー、ターゲットノード 3 0 0 から U E 2 0 0 へのハンドオーバーなどは、ネットワーク側からイニシエートされてもよい。また、ターゲットノード 3 0 0 へ移されたセッションを別のターゲットノードに更にハンドオーバーさ

せる場合は、元のターゲットノード 300 がセッションハンドオーバーに必要な情報を別のターゲットノード 300（次のターゲットノード 300）に転送することでセッションハンドオーバーが行われるようにしてもよいが、認証情報の性質上（若しくはリプレイ攻撃耐性機能を考慮した場合）、UE 200 が次のターゲットノード 300 に対して再び上述の手順を行うことが望ましい。また、単純に、いったん UE 200 にセッションを戻した後、上述の手順を行って別のターゲットノード 300 に対してセッションハンドオーバーを行うことも可能である。

[0064] <第 2 の実施の形態>

次に、本発明の第 2 の実施の形態について説明する。本発明の第 2 の実施の形態では、UE 200 が読み出し可能な SIM 情報とターゲットノードの情報とを利用して、UE 200 がセッションのハンドオーバーをターゲットノードに対して実行する方法について説明する。

[0065] 図 6 は、本発明の第 2 の実施の形態における UE の構成の一例を示す図である。図 6 に図示されている UE 200 は、通信部（下位レイヤ）221、SIM インタフェース 222、セッションハンドオーバー用 ID 取得部 223、UE・ターゲットノード間通信部 224、3G ネットワーク用通信部 225 を有しており、3G ネットワーク用通信部 225 は EAP 認証機能部 226 を更に有しており、EAP 認証機能部 226 はセッションハンドオーバー用 EAP 認証拡張機能部 227 を更に有している。

[0066] 通信部（下位レイヤ）221 は、他のノードと通信を行うための通信機能を表すものであり、1 つ又は複数のネットワークインタフェースを有している。UE 200 が携帯電話機の場合には、通信部（下位レイヤ）221 は無線通信機能を有している。この通信部（下位レイヤ）221 の通信機能によって、UE 200 は、3G ネットワーク 400 やその他のネットワークに接続されているノードと通信を行うことが可能であるとともに、ターゲットノード 300 と通信を行うことも可能である。

[0067] また、SIM インタフェース 222 は、UE 200 に装着されている S I

Mカード250（あるいは、USIMカード）に格納されているSIM情報を読み出す機能を有している。なお、SIMインタフェース222及びSIMカード250は、特に3Gネットワーク400に接続する場合（UE200が携帯電話機である場合）の一例であり、UE200が認証に用いる情報を保持、取得又は生成する機能と置き換え可能である。

[0068] また、セッションハンドオーバー用ID取得部223は、UE・ターゲットノード間通信部224でUE200から受信したターゲットノード300の識別情報（ターゲットノード300のID）を取得し、3Gネットワーク用通信部225のセッションハンドオーバー用EAP認証拡張機能部227へ渡す機能を有している。

[0069] また、UE・ターゲットノード間通信部224は、UE200がターゲットノード300との間で通信を行うための機能を有している。UE・ターゲットノード間通信部224は、ターゲットノード300から送信されたターゲットノード300の識別情報を受信することが可能である。なお、後述のように、UE200とターゲットノード300の間には信用関係が存在していてもよく、この場合には、UE・ターゲットノード間通信部224がターゲットノード300から受信するターゲットノード300の識別情報は、セキュアな状態で伝送可能となる。

[0070] また、3Gネットワーク用通信部225は、UE200が3Gネットワーク400の任意のノードと通信を行うための機能を有している。3Gネットワーク用通信部215は、3Gネットワーク400に属するサービスネットワーク450上のコンテンツサーバからコンテンツ（例えば、リアルタイムビデオ）を受信することも可能である。なお、3Gネットワーク用通信部215は、セッションハンドオーバーの認証に成功した場合に、3Gネットワーク400内のノード（例えば、3Gネットワーク400の認証サーバ600）に対して、セッションをハンドオーバーさせるためのシグナリングを送信してもよく、あるいは、ターゲットノード300に対してセッションハンドオーバーの開始指示を送信し、セッションをハンドオーバーさせるためのシグナリ

ングをターゲットノード300に送信させてもよい。

[0071] また、3Gネットワーク用通信部225のEAP認証機能部226は、UE200が3Gネットワーク400へ接続する際に、3Gネットワーク400（例えば、認証サーバ600）との間でEAP認証を行う機能を有している。このEAP認証は、SIMインタフェース222によってSIMカード250から読み出されたSIM情報を用いて行われる。

[0072] また、EAP認証機能部226のセッションハンドオーバ用EAP認証拡張機能部227は、UE200によって3Gネットワーク400との間で保持されているセッションをターゲットノード300へ譲り渡すために、3Gネットワーク400（例えば、認証サーバ600）との間でEAP認証を行う機能を有している。なお、セッションハンドオーバ用EAP認証拡張機能部227は、3Gネットワーク400との間のEAP認証の過程で、セッションハンドオーバ用ID取得部223から取得したターゲットノード300の識別情報を3Gネットワーク400へ通知することで、3Gネットワーク400がターゲットノード300を特定できるようにし、そのターゲットノード300へセッションを移すように要求する。

[0073] 図7は、本発明の第2の実施の形態におけるターゲットノードの構成の一例を示す図である。図7に図示されているターゲットノード300は、通信部（下位レイヤ）321、セッションハンドオーバ用ID生成部322、UE・ターゲットノード間通信部323、セッションハンドオーバ用通信部324、第2ネットワークオペレータ通信部325を有している。

[0074] 通信部（下位レイヤ）321は、他のノードと通信を行うための通信機能を表すものであり、1つ又は複数のネットワークインタフェースを有している。この通信部（下位レイヤ）321の通信機能によって、ターゲットノード300は、第2ネットワーク500やその他のネットワークに接続されているノードと通信を行うことが可能であるとともに、UE200と通信を行うことも可能である。

[0075] また、セッションハンドオーバ用ID生成部322は、UE200によっ

て3Gネットワーク400との間で保持されているセッションを譲り受けるために必要となるターゲットノード300の識別情報（3Gネットワーク400がターゲットノード300を特定するための情報）を生成する機能を有している。なお、UE200へのターゲットノード300の生成（あるいは、UE200への通知）は、事前に（セッションハンドオーバーが行われることが決定する前に）行われていてもよく、また、セッションハンドオーバーが行われることが決定してから行われてもよい。

[0076] UE・ターゲットノード間通信部323は、ターゲットノード300がUE200との間で通信を行うための機能を有している。UE・ターゲットノード間通信部323は、セッションハンドオーバー用ID生成部322によって生成されたターゲットノード300の識別情報をUE200へ送信することが可能である。なお、後述のように、UE200とターゲットノード300の間には信用関係が存在していてもよく、この場合には、UE・ターゲットノード間通信部323によってターゲットノード300へ送信されるターゲットノード300の識別情報は、セキュアな状態で伝送可能となる。

[0077] また、セッションハンドオーバー用通信部324は、UE200によって3Gネットワーク400との間で保持されているセッションを譲り受けるための処理を行う機能を有している。セッションハンドオーバー用通信部324は、セッションハンドオーバー用ID生成部322によって生成されたターゲットノード300の識別情報をUE200へ送信することが可能である。

[0078] また、第2ネットワークオペレータ通信部325は、ターゲットノード300が第2ネットワーク500の任意のノードと通信を行うための機能を有している。なお、ターゲットノード300が第2ネットワーク500に接続する際の認証処理も、この第2ネットワークオペレータ通信部325によって行われる。

[0079] また、本発明の第2の実施の形態における認証サーバ600は、図4に図示されている認証サーバ600と同様の構成を有しているが、上述の本発明の第1の実施の形態では、EAP認証に係る情報をターゲットノード300

から受信して処理する一方、本発明の第2の実施の形態では、EAP認証に係る情報をUE200から受信して処理する点で異なっている。

[0080] すなわち、本発明の第2の実施の形態における認証サーバ600のEAP認証機能部615のセッションハンドオーバー用EAP認証拡張機能部616は、3Gネットワーク400との間で保持されているセッションをターゲットノード300へ譲り渡そうとしているUE200との間でEAP認証を行う機能を有している。なお、セッションハンドオーバー用EAP認証拡張機能部616は、UE200との間のEAP認証の過程で、ターゲットノード300の識別情報をUE200から受信することにより、UE200がセッションを譲り渡そうとしているターゲットノード300を特定することができるようになる。なお、セッションハンドオーバーのための認証と、実際のセッションハンドオーバーの処理が分離されている場合は、例えば、セッションハンドオーバー用EAP認証拡張機能部616におけるEAP認証が完了した後、認証サーバ600、UE200、ターゲットノード300、その他の3Gネットワーク400内のノードが実際のセッションハンドオーバーの処理を開始し、セッションの送信先をUE200からターゲットノード300へ切り換えてもよい。特に、UE200が上位レイヤプロトコルとしてセッションの制御にSIPを使用している場合は、SIPで規定されているRE-INVITEメッセージなどを用いてセッションの切り換えを行うことができる。

[0081] 次に、図1のネットワークシステム構成、及び、図6に図示されているUE200、図7に図示されているターゲットノード300、図4に図示されている認証サーバの各構成に基づいて、本発明の第2の実施の形態における動作について説明する。図8は、本発明の第2の実施の形態における動作の一例を示すシーケンスチャートである。

[0082] 図8において、UE200からターゲットノード300へのセッションハンドオーバーが開始されると、まず、UE200は、セッションハンドオーバー用ID取得部223において、ターゲットノード300の識別情報を取得する（ステップS2001）。なお、ここでは、セッションハンドオーバーの開

始とともに、UE 200はターゲットノード300の識別情報をターゲットノード300から取得しているが、UE 200は、UE 200内部に事前に登録されているターゲットノード300の識別情報を利用してもよく、あるいは、必要に応じてターゲットノード300から取得するようにしてもよく、さらには、ターゲットノード300がセッションハンドオーバーの要求をUE 200に対して求める際にターゲットノード300の識別情報を通知するようにしてもよい。

[0083] ターゲットノード300の識別情報は、ターゲットノード300のIPアドレスや機器識別コードなど、ターゲットノード300を特定できる任意の情報をを用いることが可能である。このターゲットノード300の識別情報は、UE 200からターゲットノード300へセッションハンドオーバーを行う際の分岐点（例えば、HeNB/Home-GW100）や、セッションハンドオーバーのための認証サーバ600において認証時にターゲットノード300を特定し、認証できるようにする情報であることが望ましい。

[0084] なお、上述の本発明の第1の実施の形態と同様に、UE 200とターゲットノード300との間には、信用関係が存在することが望ましい。例えば、ネットワークオペレータに接続する認証機能とは別の機器間の認証機能によって互いの装置の単一性や意図している装置であることが確認できているか、さらには第3者によって情報を収集されていないことや改ざんされていないことが確認できている（例えば、暗号化されている）ことが望ましい。このとき、例えばUE 200とターゲットノード300との間においてEAP認証が行われてもよい。

[0085] また、UE 200とターゲットノード300との間は、短距離無線通信などのような直接のリンク（有線接続を含む）で通信が行われてもよく、また、3Gネットワーク400又はターゲットノード300の属するネットワーク（第2ネットワークオペレータが管理する第2ネットワーク500）若しくはその両方のネットワークを介した通信経路によって通信が行われてもよく、さらには、HeNB/Home-GW100経由で通信が行われてもよ

い。

[0086] なお、上述の本発明の第1の実施の形態ではUE 200からターゲットノード300へセッションHO情報が渡されたが、本発明の第2の実施の形態ではターゲットノード300からUE 200へターゲットノード300の識別情報が渡される。ターゲットノード300の識別情報は、ターゲットノード300への到達可能な（特定可能な）識別情報であり、UE 200がターゲットノード300を確認できればよい。したがって、セッションHO情報を通知する通信（すなわち、本発明の第1の実施の形態におけるセッションHO情報の伝送）に比べて、本発明の第2の実施の形態におけるターゲットノード300の識別情報の伝送では、処理負荷の低い暗号化や通信プロトコルを用いることができるかもしれないというメリットがある。

[0087] ステップS 2001でターゲットノード300の識別情報を取得したUE 200は、セッションハンドオーバー用EAP認証拡張機能部227において、UE 200自身の接続認証先である認証サーバ600に対して、ターゲットノード300の識別情報を追加情報として含んだ情報を送信してEAP認証を行う（ステップS 2003）。なお、UE 200が既に認証サーバ600との間におけるアクセス認証を完了している場合には、EAP再認証を行うことになる。また、特定のセッションのみをUE 200からターゲットノード300へ移したい場合には、そのセッションを特定するための情報が追加情報として含まれていてもよい。

[0088] なお、このステップS 2003におけるEAP認証において、コンテンツを受信するためのセッションがターゲットノード300あてに切り換えられる旨がサービスネットワーク450のエンティティ（コンテンツサーバ700など）に伝わるようになっていてもよい。ここでは、UE 200の接続ノードはHeNB/Home-GW100であり、UE 200は接続認証をHeNB/Home-GW100との間で行っていると考えられるので、セッションハンドオーバーのための認証もHeNB/Home-GW100との間のEAP認証（最終的な認証サーバ600は、3Gネットワーク400やサ

ービスネットワーク 450 に存在するかもしれない) で実行されることが考えられる。

[0089] 認証サーバ 600 は、セッションハンドオーバー用 EAP 認証拡張機能部 315 において、UE 200 との間のセッションハンドオーバーのための EAP 認証を行う。セッションハンドオーバーのための認証が完了すると、認証サーバ 600 のセッションハンドオーバー処理部 612 は、この認証過程で取得したターゲットノード 300 へセッションをハンドオーバーさせる処理を開始する。3G ネットワーク 400 側ではそれまで UE 200 に送信していたコンテンツ (リアルタイムビデオ) のセッションをターゲットノード 300 にハンドオーバーさせることによって、コンテンツ (リアルタイムビデオ) のセッションがターゲットノード 300 へ移り、サービスネットワーク 450 上のコンテンツサーバ 700 からターゲットノード 300 へコンテンツ (リアルタイムビデオ) が配信されるようになる (ステップ S1005)。

[0090] なお、特定のセッションのハンドオーバーが指定されている場合には、3G ネットワーク 400 側はそのセッションのみハンドオーバーさせる。また、実際のセッションハンドオーバーは、例えば、認証サーバ 600 からコンテンツサーバ 700 へセッションの切り換え指示が行われてコンテンツサーバ 700 がターゲットノード 300 に対してコンテンツを配信するなどのように、3G ネットワーク 400 内部で行われてもよく、また、HeNB/Home-GW 100 のような分岐点において UE 200 からターゲットノード 300 へコンテンツの配信先を切り換えてもよい。また、認証サーバ 600 からコンテンツサーバ 700 への認証の成功に基づくセッションハンドオーバーの手続きは、任意の方法が利用可能である。図面においてもこの 2 者間 (若しくは仲介者が介在するかもしれない) の手続きについては不図示としている。

[0091] 以上のような認証方法により、ターゲットノード 300 は自身の認証情報 (ターゲットノード 300 の識別情報など) では直接的に EAP 認証が不可能な場合であっても、セッションハンドオーバーのための認証を完了すること

ができる。なお、ターゲットノード300へセッションのハンドオーバーが行われた場合であっても、そのセッションの権利（あるいは、課金などの責任）はUE200に残ることになる。

[0092] また、いったんターゲットノード300へ移されたセッションを元のUE200に戻すためのセッションハンドオーバーでは、本来の認証情報をUE200が持っているので、認証関係が維持されている場合はそのままの状態ですessionハンドオーバーの準備が完了しており、また、認証関係が維持されていない場合であっても、再度認証を行うことによりセッションハンドオーバーの準備が完了する。この後、UE200若しくはセッションが移されていたターゲットノード300がハンドオーバーの手順を開始すると、3Gネットワーク400側ではそれまでターゲットノード300に送信していたコンテンツ（リアルタイムビデオ）のセッションをUE200にハンドオーバーさせることで、セッションがUE200に戻される。

[0093] なお、UE200やターゲットノード300からの3Gネットワークへの通信の一部又はすべてや、UE200からターゲットノード300へのハンドオーバー、ターゲットノード300からUE200へのハンドオーバーなどは、ネットワーク側からイニシエートされてもよい。また、ターゲットノード300へ移されたセッションを別のターゲットノードに更にハンドオーバーさせる場合は、元のターゲットノード300がセッションハンドオーバーに必要な情報を別のターゲットノード300（次のターゲットノード300）に転送することでセッションハンドオーバーが行われるようにしてもよいが、認証情報の性質上（若しくはリプレイ攻撃耐性機能を考慮した場合）、UE200が次のターゲットノード300に対して再び上述の手順を行うことが望ましい。また、単純に、いったんUE200にセッションを戻した後、上述の手順を行って別のターゲットノード300に対してセッションハンドオーバーを行うことも可能である。

[0094] なお、本発明に係るセッションハンドオーバーのための認証は、通常の接続認証や、対象となるコンテンツのセッションのための通常の認証とは区別さ

れていることが望ましい。本発明に係るセッションハンドオーバーのための認証が、通常の接続認証やセッションのための認証と区別されておらず、単一のものとして認証がなされている場合には、UE 200に対する他の通信（セッションハンドオーバーに係るセッション以外の通信）が止まったりUE 200の接続が解消されてしまったりする可能性もある。また、このような状況を回避するために単一のセッションを複数のセッションに分離したり、単一のセッションで使用されるデータを振り分けるようにしたりすることも可能である。

[0095] また、コンテンツにはリアルタイムビデオなどのような配信型（サービスネットワーク450から配信されるコンテンツデータがほとんどを占めており、コンテンツデータ受信側のノードからは制御用通信のみがなされる）のもののほかに、UE 200やターゲットノード300からデータをネットワーク側に送信するアップロード型や、双方向にやり取りされるコンテンツなども存在する。それぞれの形態に応じて、セッションハンドオーバーの際に通知すべき情報（例えば、受信用アドレスと送信用アドレスが異なる場合など）や詳細な認証手順などが異なることが考えられるが、こうした差異はセッションハンドオーバーを実行するうえでのパラメータの差異に過ぎないものであり、セッションの種類や方向などによらず、本発明を適用することが可能である。

[0096] また、上述の本発明の第1及び第2の実施の形態では、図1に図示されているように、同一家屋内に存在するUE 200からターゲットノード300へのセッションハンドオーバーを一例に挙げて説明を行ったが、UE 200及びターゲットノード300が異なるユーザによって所有されていてもよく、また、それぞれの設置場所（接続場所）が離れていてもよい。

[0097] また、本発明に係るセッションハンドオーバーによって、UE 200からターゲットノード300へ移るセッションの数は任意であり、1つのセッションのみが移されてもよく、複数のセッション（さらには、UE 200のすべてのセッション）が移されてもよい。また、セッションの移動ではなくセッ

ションを複製（分岐）し、UE 200からターゲットノード300へセッションを移すとともに、UE 200自体も依然としてそのセッションに係る通信が行えるようにしてもよい。この場合、UE 200は、セッションのハンドオーバーのための認証に必要な情報に、UE 200による通信中のセッションを残したままターゲットノード300と第1ネットワーク400との間のセッションを開始するセッション複製を要求する情報や、セッションをUE 200からターゲットノード300へ切り換えるセッション切り換えを要求する情報を挿入してもよい。

[0098] また、セッションの複製は第1ネットワークの管理上、UE 200の単独の判断のみで行うことには制限が設けられているほうが望ましい。この場合、セッションハンドオーバーのためのEAP認証のほかに（若しくはセッションハンドオーバーのためのEAP認証の中で）セッションの複製に関する追加の認証を行えるようにしてもよい。これにより、第1ネットワークの管理の下でセッションの複製が可能となる。

[0099] また、上述の本発明の第1及び第2の実施の形態では、UE 200が主にSIMカード250を有する携帯電話機であることを前提として説明を行ったが、UE 200は、例えばPC（Personal Computer）などを始めとする任意の通信装置であってもよく、さらには、UE 200によるネットワークへの接続は、無線接続あるいは有線接続のどちらであってもよい。また、上述のセッションHO情報は、各種通信装置に応じて任意の記憶媒体から読み出されるセッションハンドオーバーの認証に必要な情報が読み出されればよく、さらには、アクセス認証方式も上述のEAP認証方式に限定されるものではない。

[0100] また、上述の本発明の第1及び第2の実施の形態では、セッションハンドオーバー元であるUE 200とセッションハンドオーバー先であるターゲットノード300とが同一の認証サーバ（HeNB/Home-GW100）に接続している場合について説明しているが、それぞれが異なる装置で実現されていてもよく（すなわち、UE 200とターゲットノード300と、それぞれ

れ異なる認証サーバに接続していてもよい)、さらには、それぞれの認証サーバが遠く離れたところに存在していてもよい。この構成では、それぞれの認証サーバが情報交換(セキュアな状態であることが望ましい)を行う必要があるかもしれないが、そのセッションの権利(あるいは、課金などの責任)をUE 200に残した状態で、リモートに存在するターゲットノード300にコンテンツを提供できるようになる。このように、例えば、UE 200の所有者の提供で遠く離れた教育機関にコンテンツを寄贈するなど、UE 200の所有者とターゲットノード300の所有者とが異なる場合においても本発明が実施可能となる。

[0101] また、上述の本発明の第1及び第2の実施の形態では、1つのUE 200のセッションについて説明しているが、複数の異なるUE 200のセッションを一括してセッションハンドオーバーすることも可能である。この場合は、本発明の方法を複数回繰り返して(並行して)実施するほかに、代表となるUE 200(複数のUE 200のうちの1つ)が、他のUE 200のセッションハンドオーバーを一括して行うことで効率化が期待できる。このとき、他のUE 200は代表となるUE 200に対してあらかじめセッションハンドオーバーに必要な情報を通知しておくともよい。さらに、ターゲットノード300が複数であってもよい。

[0102] また、セッションハンドオーバーの対象となるセッションの使用に関して、ターゲットノード300において制限が設けられていてもよい。例えば、ターゲットノード300が利用できるセッションの持続時間や一定額の課金上限を設定し、この許可された範囲内でハンドオーバーされたセッションを使用できるようにしてもよい。このためには、UE 200と認証サーバ600若しくはコンテンツサーバ700があらかじめ上限を設定する手順を行ってもよく、あるいは、UE 200が独自に設定し、認証時(若しくは、認証に必要な情報の準備時)に認証情報として通知してもよい。

[0103] また、本発明の方法において、UE 200及びターゲットノード300がタイミングの同期を取ることで、セッションのシームレスな切り換えを行え

るようにすることも可能である。このとき、UE 200は、ターゲットノード300からのセッションの返還と、ターゲットノード300への新たなセッションハンドオーバとを同時に行えるよう、認証に必要な情報をまとめ、一括して認証できるようにする。これにより、1回の認証手順でセッションの交換が実現可能となる。これは、UE 200が両方のセッション（既にセッションハンドオーバによってターゲットノード300へ移されていたセッション、及び、これからセッションハンドオーバによってターゲットノード300へ移されるセッション）の権利を保持しているため、UE 200及びターゲットノード300のそれぞれが各セッションの権利を保持している場合に比べて、簡素な認証手順で実行できるというメリットがある。

[0104] <第3の実施の形態>

次に、本発明の第3の実施の形態について説明する。本発明の第3の実施の形態では、上述の本発明の第1又は第2の実施の形態に記載されている方法を、ETWSなどの災害情報通知システムに適用する場合について説明する。なお、本発明の第3の実施の形態においても、図1に図示されているネットワーク構成を参照しながら説明する。

[0105] 図10は、本発明の第3の実施の形態における認証サーバの構成の一例を示す図である。図10に図示されている認証サーバ600は、図4に図示されている認証サーバ600と同様の構成を有しているが、さらに、3Gネットワーク用通信部614が災害情報処理部651を有している。

[0106] 災害情報処理部651は、災害情報通知を取得し、その内容を処理する機能を有している。認証サーバ600は、例えば、3Gネットワークから各基地局へ向けて通知される災害情報を受信すると、災害情報処理部651が、災害情報の通知対象となる装置に対して災害情報の転送を行う。通知対象の装置に対して災害情報を通知する際には、その通知対象の装置に対して提供されているセッションに追加する形で災害情報の通知を行ってもよく、あるいは、通知対象の装置に対して提供されているセッションに混在させる形で災害情報の通知を行ってもよい。また、災害情報処理部651は、音声、映

像、制御信号など、通知対象の装置に適した形式に災害情報を抽出及び加工してもよい。

[0107] また、E T W Sなどの災害情報の通知は緊急時の通知であるという意味合いから、個別の詳細の認証によらず、ユーザの所有する通知可能な装置にできるだけ多く通知されることが望ましい。このため、E T W Sなどによる災害情報の通知に関する本発明の認証は、災害情報の通知においては通常と異なる動作をすることが必要となる。災害情報処理部 6 5 1 は、災害情報を受信した場合に、災害情報を通知するためのセッションに関しては、通常の認証と異なる認証（より迅速な認証）とするよう E A P 認証機能部 2 2 6 に通知したり、E A P 認証機能部 2 2 6 の処理を制御したりする機能を有している。

[0108] さらに、災害情報処理部 6 5 1 は、災害情報の通知を受けた場合に、所定の機器やシステムを制御する動作を開始してもよい。例えば、災害情報処理部 6 5 1 は、災害情報の通知を受けると、各機器の制御を行うことが可能なホームゲートウェイの機能（認証サーバ 6 0 0 と同一装置内に備わっていてもよく、別の装置に備わっていてもよい）に対して災害情報を受信した旨を通知する。これにより、ホームゲートウェイは、災害情報の取得／表示自体ができないような機器に対しても、災害に対する何らかの動作を指示し、例えば所定の機器やシステムに対して電源のオン／オフを制御したり、非常事態時のモード（非常モード）を開始させたりすることが可能となる。こうした非常事態時に行われる制御の一例としては、例えば、ガスコンロなどの火を使う器具の停止、給湯や空調（冷房／暖房）の停止、通常照明から非常照明への切り換え、セキュリティシステムの作動、放送受信機器の作動などが挙げられる。また、災害情報の表示はできるものの、その時点で電源が入っていないテレビなどにおいても、まずホームゲートウェイからテレビの電源を入れる処理を行い、その後に本発明に係るセッションハンドオーバーを行うことで、テレビから災害情報の報知を行うことが可能となる。

[0109] また、図 1 1 は、本発明の第 3 の実施の形態における U E の構成の一例を

示す図である。図 11 に図示されている UE 200 は、図 2 に図示されている UE 200 と同様の構成を有しているが、さらに、3G ネットワーク用通信部 215 が災害情報処理部 251 を有している。なお、図示省略するが、上述の本発明の第 2 の実施の形態に記載されている方法を ETWS に適用する場合には、図 6 に図示されている UE 200 の 3G ネットワーク用通信部 225 に災害情報処理部 251 が追加されればよい。

[0110] UE 200 の災害情報処理部 251 も、認証サーバ 600 の災害情報処理部 651 と同様に、ETWS などによる災害情報の通知に関する認証が迅速かつより多くの装置に通知されるようにするための機能を有している。すなわち、UE 200 の災害情報処理部 251 は、災害情報を通知するためのセッションに関しては、通常の認証と異なる認証（より迅速な簡易認証）とするよう EAP 認証機能部 216 に通知したり、EAP 認証機能部 216 の処理を制御したりする機能を有している。また、災害情報処理部 251 は、より多くの装置に災害情報が通知されるように、災害情報の通知対象となる新たな装置に災害情報に係るセッションが提供されるようにするための処理（例えば、新たなターゲットノードを認証サーバ 600 へ通知する処理）を行うことが可能である。また、UE 200 の災害情報処理部 251 が、災害情報の通知を受けた場合に所定の機器やシステムを制御する動作（例えば、災害情報を受信した旨をホームゲートウェイに通知）を行ってもよい。

[0111] また、本発明の第 3 の実施の形態におけるターゲットノード 300 の構成は、図 3 又は図 7 に図示されているターゲットノードと同様であるが、例えば図 3 に図示されているターゲットノード 300 のセッションハンドオーバー EAP 認証拡張機能部 315 が、災害情報の迅速な通知が行われるために簡素化された追加の認証処理（後述）に対応していることが望ましい。

[0112] 次に、図 1 のネットワークシステム構成、及び、図 10 に図示されている認証サーバ 600、図 11 に図示されている UE 200 の各構成に基づいて、本発明の第 3 の実施の形態における動作について説明する。図 12 は、本発明の第 3 の実施の形態における動作の一例を示すシーケンスチャートであ

る。

- [0113] 図 12において、初期状態として、例えばUE 200がサービスネットワーク 450から何らかのサービスに係るセッションを受けているとする。すなわち、UE 200は、認証サーバ600との間で認証処理を行い、サービスを受けることが適切な端末であることが承認され、その結果、所望のサービスに係るセッションを受けていることを前提とする。
- [0114] また、上述の本発明の第1又は第2の実施の形態に記載されている方法（図5又は図8に図示されている認証処理）によって、特定のターゲットノード300に対して任意のセッションのセッションハンドオーバーが行われているとする（ステップS3001）。
- [0115] ここで、何らかの災害が発生し、認証サーバ600（HeNB/Home-GW100のように一体化された装置、若しくは情報転送の分岐点となる装置が認証サーバ600であってもよい）が、3Gネットワーク400（例えば、コンテンツサーバ700に対応する災害情報通知サーバ750）からETWSなどの災害情報を通知する災害情報を受信したとする（ステップS3003）。
- [0116] 災害情報を受信した認証サーバ600の災害情報処理部651は、UE200に対して災害情報を通知する（ステップS3005）。この災害情報の通知は、通常の動作（例えばETWSで規定されている動作）によって行われる。
- [0117] また、並行して、認証サーバ600は、通知対象の装置が他に存在しないかどうかを判断する。このとき、上述の本発明の第1又は第2の実施の形態に記載されている方法によって、ターゲットノード300に対してセッションハンドオーバーが行われている状態の場合には、そのターゲットノード300は既に認証済みであり、認証サーバ600はそのターゲットノード300について把握している。この場合、認証サーバ600は、そのターゲットノード300に対して提供されているセッションに追加、若しくは混在させる形で災害情報を通知する処理を行う。

[0118] なお、特に災害情報を異なるセッションで通知する場合、認証サーバ600は、少なくとも認証サーバ自身が判断する認証部分に関しては、その認証レベルを低く（より多くの装置に対して災害情報を通知できるように）した追加の認証処理を行う必要がある（ステップS3007）。認証サーバ600は、既に認証済みのセッションハンドオーバー用EAP認証で用いられた情報を基に、ターゲットノード300との間で追加認証を行う。一方、ターゲットノード300側においてはこのセッション／災害情報を受けることに関する認証は通常通り必要となるかもしれない。すなわち、ターゲットノード300は、送られてくるセッションが正当なものであるかどうかを通常通り判断する必要があるかもしれない。

[0119] 災害情報の通知に係る追加の認証処理は、基本的に、上述の本発明の第1又は第2の実施の形態に記載されている方法に従って行われるものであり、これによって、本来は認証することができないターゲットノード300の認証処理が行われる。ただし、追加の認証処理は、迅速かつより多くの装置に対して通知されるように行われる必要があり、簡素化された認証処理であることが望ましい。例えば、追加の認証処理では、簡素化された認証情報が用いられたり、簡素化された認証手順が行われたりすることによって、迅速かつ認証レベルを低くすることが望ましい。また、認証サーバ600は、特に複雑な認証手順を必要とせずにセッション開始が可能であることのみを伝えたり、認証処理を行うことなく強制的に災害情報を伝達したりするようにしてもよい。

[0120] このように、認証サーバ600は、セッションハンドオーバーによって既に認証済みのターゲットノード300との間における追加の認証処理に成功すると、例えば、災害情報を通知するためのセッションを追加するか、若しくは既存のセッションに災害情報を混在させることで、ターゲットノード300に対して災害情報の通知を行う（ステップS3009）。

[0121] また、認証サーバ600は、セッションハンドオーバーによる認証が行われていない別の装置（3Gネットワーク400での認証に利用可能なSIM情

報を有していない装置、以下、新たなターゲットノード350と記載)に対して災害情報の通知を行うための認証処理を行う(ステップS3011)。このとき、災害情報を受信したUE200が災害情報に係るセッションH0情報を新たなターゲットノード350に対して送信することでセッションハンドオーバ(上述の本発明の第1の実施の形態に記載されている方法)が開始されてもよく、UE200が新たなターゲットノード350のID情報を認証サーバ600に送信する(あるいは、認証サーバ600が何らかの方法で事前に存在を把握している別の装置に係る認証処理を促す)ことで、セッションハンドオーバ(上述の本発明の第2の実施の形態に記載されている方法)が開始されてもよい。なお、この場合におけるセッションH0情報や認証手順も簡素化されており、認証レベルの低い認証が迅速に行われることが望ましい。また、認証サーバ600は、存在が特定された新たなターゲットノード350に対して、特に複雑な認証手順を必要とせずにセッション開始が可能であることのみを伝えたり、認証処理を行うことなく強制的に災害情報を伝達したりするようにしてもよい。そして、認証サーバ600は、新たなターゲットノード350の認証処理に成功すると、その装置に対して災害情報を通知する処理を行う(ステップS3013)。

[0122] なお、認証サーバ600は、UE200、セッションハンドオーバによる認証済みのターゲットノード300、セッションハンドオーバによる認証が行われていない新たなターゲットノード350のそれぞれに対して災害情報を通知するための処理を独立かつ並行して行うことが望ましい。また、認証サーバ600は、災害情報の初期情報(プライマリ情報)を所定時間内(4秒以内)に伝達する必要があるが、追加の認証処理を行うことで、第一報の通知が遅れてしまう可能性がある(特に、新たなターゲットノード350に対して)。このような遅延が発生しないようにするため、認証サーバ600は、例えば、認証処理中に並行して災害情報の初期情報(プライマリ情報)を通知し、認証処理に成功してから災害情報の詳細情報(セカンダリ情報)を通知するようにしてもよい。

[0123] また、図 1 2 には不図示であるが、認証サーバ 6 0 0 は、災害情報の通知を受けた場合に、所定の機器やシステムを制御する動作を開始してもよい。例えば、認証サーバ 6 0 0 は、災害情報の通知を受けると、各機器の制御を行うことが可能なホームゲートウェイの機能（認証サーバ 6 0 0 と同一装置内に備わっていてもよく、別の装置に備わっていてもよい）に対して災害情報を受信した旨を通知し、ホームゲートウェイが所定の機器やシステムの制御をすぐに開始できるようにしてもよい。

[0124] なお、UE 2 0 0、ターゲットノード 3 0 0／新たなターゲットノード 3 5 0、認証サーバ 6 0 0 に、災害情報を受信した場合に行われる処理をあらかじめ登録しておくことが望ましく、また、災害情報の通知に係る処理は、他の処理に比べて優先的に（あるいは、最優先に）行われることが望ましい。

[0125] <第 4 の実施の形態>

次に、本発明の第 4 の実施の形態について説明する。上述の本発明の第 3 の実施の形態では、認証サーバ 6 0 0 が 3 G ネットワーク 4 0 0 から災害情報の通知を受けて UE 2 0 0 に災害情報を通知する場合について説明しているが、UE 2 0 0 もマクロ基地局を通じて 3 G ネットワーク 4 0 0 に接続可能であり、UE 2 0 0 が認証サーバ 6 0 0 より先に 3 G ネットワーク 4 0 0 から災害情報を受信する可能性もある。本発明の第 4 の実施の形態では、UE 2 0 0 が 3 G ネットワーク 4 0 0 から災害情報の通知を受信した場合について説明する。

[0126] 例えば、UE 2 0 0 が災害情報通知サービスに参加しており、災害情報通知システム（例えば、ETWS）から災害情報を直接受信することが可能な場合がある。このような場合、認証サーバ 6 0 0（HeNB/Home-GW 1 0 0 のように一体化された装置、若しくは情報転送の分岐点となる装置が認証サーバ 6 0 0 であってもよい）からではなく、マクロ基地局から災害情報を先に受信する可能性がある。なお、このように UE 2 0 0 がマクロ基地局から災害情報を受信するためには、UE 2 0 0 がマクロ基地局に接続し

ている必要があり、このため、例えば、UE 200はアイドル状態である間には、よりETWSから災害情報を受信しやすいようにマクロ基地局に接続していてもよく、あるいは、例えばユーザが帰宅して、自分のセッションをTVセットなどのターゲットノード300に移し終わった時点でアイドル状態となってマクロ基地局に接続してもよい。

[0127] 本発明の第4の実施の形態におけるUE 200は、上述の本発明の第3の実施の形態に係る構成に加えて、さらに、災害情報を3Gネットワーク400側から受信した場合には、災害情報処理部251が、認証サーバ600に対して災害情報を転送する機能を有している。また、本発明の第4の実施の形態における認証サーバ600は、上述の本発明の第3の実施の形態に係る構成に加えて、さらに、3Gネットワーク400側からだけでなく、UE 200から災害情報の通知を受ける機能を有している。

[0128] 以下、本発明の第4の実施の形態における動作について説明する。図13は、本発明の第4の実施の形態における動作の一例を示すシーケンスチャートである。

[0129] 図13において、初期状態として、例えばUE 200がサービスネットワーク450から何らかのサービスに係るセッションを受けているとする。すなわち、UE 200は、認証サーバ600との間で認証処理を行い、サービスを受けることが適切な端末であることが承認され、その結果、所望のサービスに係るセッションを受けていることを前提とする。

[0130] また、上述の本発明の第1又は第2の実施の形態に記載されている方法（図5又は図8に図示されている認証処理）によって、特定のターゲットノード300に対して任意のセッションのセッションハンドオーバーが行われているとする（ステップS4001）。

[0131] ここで、何らかの災害が発生し、UE 200が、3Gネットワーク400（例えば、コンテンツサーバ700に対応する災害情報通知サーバ750）からマクロ基地局410経由でETWSなどの災害情報を通知する災害情報を受信したとする（ステップS4003）。このとき、UE 200の災害情

報処理部 251 は、災害情報を認証サーバ 600 へ転送する（ステップ S 4005）。

[0132] 以降の処理は、上述の本発明の第 3 の実施の形態における動作（図 12 のステップ S 3007～S 3013 の処理）とほぼ同様である。すなわち、認証サーバ 600 は、UE 200 から転送されてきた災害情報を受信し、ターゲットノード 300 及び新たなターゲットノード 350 へ災害情報を転送するための認証、及び災害情報の通知を行う。なお、認証サーバ 600 は、UE 200 から災害情報を受信したことから、UE 200 に対して災害情報を再度通知する必要はない。また、UE 200 は、3G ネットワーク 400 から災害情報を受信した時点で、認証サーバ 600 へ災害情報を転送するとともに、ターゲットノード 300 や新たなターゲットノード 350 へ災害情報を転送可能とするための処理（ターゲットノード 300 や新たなターゲットノード 350 と認証サーバ 600 との間における追加の認証処理のための準備）を自発的に開始することが望ましい。また、UE 200 自身が、3G ネットワーク 400 から災害情報を受信した時点で、ターゲットノード 300 や新たなターゲットノード 350、機器やシステムの制御を行うことが可能なホームゲートウェイなどに対して災害情報の転送を直接行ってもよく、UE 200 自身がホームゲートウェイの役割を果たして、機器やシステムの制御を行ってもよい。

[0133] <第 5 の実施の形態>

上述の本発明の各実施の形態では、HeNB/Home-GW 100 が固定設置されている場合について説明しているが、HeNB/Home-GW 100 に相当する移動体内ネットワークゲートウェイが移動体（車両や列車など）に搭載されている場合においても本発明の適用が可能である。この場合、移動体内ネットワークゲートウェイが 3G ネットワーク 400 と直接接続していてもよく、あるいは、3G ネットワーク 400 と接続可能な UE 200 が移動体内に存在しており、移動体内ネットワークゲートウェイが UE 200 を経由して（UE 200 がゲートウェイの役割を果たす）3G ネット

ワーク 400 と接続していてもよい。

[0134] このような構成において、例えば、SIM情報を有する機器（UE 200 やSIM情報を有するナビゲーションシステムなど）が受けることが可能なセッションを、SIM情報を有さない機器（移動体内に設置されたモニタや、SIM情報を有さないナビゲーションシステムなど）へハンドオーバーさせることが可能である。

[0135] この場合、移動体内ネットワークゲートウェイと3Gネットワーク400 との間の接続も無線接続である。例えば、状況によっては、この無線接続が切れてしまう場合も考えられるが、このような場合に、自動的にUE 200 へセッションを戻す（セッションハンドオーバー）ことが可能となり有用である。

[0136] また、移動体内ネットワークのコンテンツを3Gネットワーク400 を経由してUE 200 へ提供されるようにしてもよい。この場合、SIM情報を有さないターゲットノード（例えば、移動体内に設置されたカメラ）300 は、移動体内ネットワークゲートウェイのSIM情報に基づいて本発明に係る方法で認証された後、移動体内ネットワークゲートウェイの接続サービスを行っているネットワークへ移動体内ネットワークゲートウェイを経由してコンテンツ（例えば、カメラによって撮像された画像）を送信することが可能となり、UE 200 は、このコンテンツを3Gネットワーク400 から提供されているサービスとして受信することが可能となる。例えば、移動体内で移動体内ネットワークゲートウェイを経由してUE 200 がこのコンテンツサービスを受信している場合に、UE 200 が移動体内ネットワークゲートウェイからセッションHO情報を取得して、移動体内ネットワークゲートウェイの接続サービスを行っているネットワークの認証サーバとの間でセッションハンドオーバーに係る認証を行うことで、UE 200 は3Gネットワーク400 経由でコンテンツの受信を行うことが可能となる。これにより、UE 200 は3Gネットワーク400 経由でマクロ基地局からターゲットノードにより送信されるコンテンツを受信することが可能となり、例えば、UE

200のユーザが移動体を離れた場合であっても、移動体内のカメラによって撮像された画像を受信、閲覧することが可能となる。また、移動体に限らず、例えば、家屋に設置されたドアホンの映像をUE200で受信、閲覧することも同様にして可能となる。

[0137] <第6の実施の形態>

また、上述のように、UE200やターゲットノード300からデータをネットワーク側に送信するアップロード型のセッションに関しても、本発明に係る方法を適用することが可能である。例えば、UE200のカメラを用いてその撮像画像をアップロードするセッションを、ホームネットワークに接続しているビデオカメラにセッションハンドオーバーし、以降、UEの撮像画像からビデオカメラの撮像画像に切り換えてアップロードを行うことが可能である。また、上述の移動体の例の場合も同様に、UE200のカメラから移動体内に設置されているカメラにセッションハンドオーバーを行うことで、撮像主体をUE200のカメラから移動体内に設置されているカメラに切り換えるセッションハンドオーバーを行うことも可能である。なお、データのアップロードに関するセッションハンドオーバーを行うための動作は、データのダウンロードに関するセッションハンドオーバーのための動作と基本的に同一であり、コンテンツサーバとUE200（あるいはターゲットノード300）との間のコンテンツの転送方向が逆になるだけである。

[0138] また、図1、図9には不図示だが、HeNBを3Gネットワークに接続させるためのGW（以降HeNB-GW）が3Gネットワーク側（HeNBと3Gネットワークの間）に存在することが考えられる。このとき、HeNB-GWは複数のHeNBに対して3Gネットワークへのゲートウェイ装置として働き、いくつかの機能をHeNBと共有、分担することが考えられる。本発明の機能及び本発明に係る機能がどのようにHeNBとHeNB-GWとの間で分担されるかにかかわらず、上記の本発明の実施の形態は、実施可能である。

[0139] また、上記の本発明の実施の形態の説明で用いた各機能ブロックは、典型

的には集積回路であるＬＳＩ（Large Scale Integration）として実現される。これらは個別に１チップ化されてもよいし、一部又はすべてを含むように１チップ化されてもよい。なお、ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ（Integrated Circuit）、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

[0140] また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Field Programmable Gate Array）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。

[0141] さらに、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。例えば、バイオ技術の適応などが可能性としてあり得る。

産業上の利用可能性

[0142] 本発明は、認証プロトコルにおいて鍵生成機能が異なる装置間においてセッションハンドオーバを行えるようになるという効果を有しており、パケット交換型データ通信ネットワークにおける通信技術に適用可能であり、特に、ネットワーク接続のための認証技術やセッションのモビリティに関する技術に適用可能である。

請求の範囲

- [請求項1] 第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバさせるための認証が行われるよう構成されている通信システム。
- [請求項2] 前記第1ノードが、前記セッションのハンドオーバのための認証に必要な情報を前記第2ノードへ通知し、前記第2ノードが、前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバのための認証処理を行う際に、前記セッションのハンドオーバのための認証に必要な情報に基づいて生成された情報を前記認証サーバへ通知するよう構成されている請求項1に記載の通信システム。
- [請求項3] 前記第1ノードが、前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバのための認証処理を行う際に、前記第2ノードの識別情報を前記認証サーバへ通知するよう構成されている請求項1に記載の通信システム。
- [請求項4] 前記セッションが災害発生を通知する災害情報を送信するためのものである場合には、前記認証が、より迅速な認証を行うための簡易的な認証であるよう構成されている請求項1に記載の通信システム。
- [請求項5] 前記セッションが、前記第1ネットワークから前記第1ノードヘデータを送信するダウンロード型、又は、前記第1ノードから前記第1ネットワークヘデータを送信するアップロード型である請求項1に記載の通信システム。
- [請求項6] 第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバさせるための認証が行われるよう構成されている通信システムの前記第1ノ

ードに実装される通信処理装置であって、

前記第2ノードが前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバーのための認証処理を行う際に前記認証サーバへ通知するための前記セッションのハンドオーバーのための認証に必要な情報を、前記第2ノードへ通知するよう構成されている通信処理装置。

[請求項7] 前記セッションのハンドオーバーのための認証に必要な情報に、前記第1ノードによる通信中の前記セッションを残したまま前記第2ノードと前記第1ネットワークとの間の前記セッションを開始するセッション複製を要求する情報、又は、前記セッションを前記第1ノードから前記第2ノードへ切り換えるセッション切り換えを要求する情報が含まれている請求項6に記載の通信処理装置。

[請求項8] 前記第1ノードから前記第2ノードへハンドオーバーされた前記セッションの切断が検出された場合に、前記第2ノードから前記第1ノードへ前記セッションを戻す処理を行うよう構成されている請求項6に記載の通信処理装置。

[請求項9] 前記第1ノードから前記第2ノードへハンドオーバーされた前記セッションを前記第2ノードから前記第1ノードへ戻す際に、前記第1ネットワークの前記認証サーバとの間で前記セッションを戻すための認証を行うように構成されている請求項6に記載の通信処理装置。

[請求項10] 前記認証処理に成功した場合、前記セッションをハンドオーバーさせるためのシグナリングを前記第1ネットワークへ送信するように構成されている請求項6に記載の通信処理装置。

[請求項11] 前記認証処理に成功した後、前記セッションのハンドオーバーの開始指示を前記第2ノードへ送信するように構成されている請求項6に記載の通信処理装置。

[請求項12] 前記第1ノードから前記第2ノードへ第1のセッションをハンドオーバーさせる処理と、前記第1ノードから前記第2ノードへ既にハンド

オーバされていた第2のセッションを前記第2ノードから前記第1ノードへ戻す処理とを一括して行うために必要な情報を生成するように構成されている請求項6に記載の通信処理装置。

[請求項13] 災害発生を通知する災害情報に係るセッションのハンドオーバに関しては、前記セッションのハンドオーバのための認証に必要な情報として、より迅速な簡易的な認証を行うための情報を通知するよう構成されている請求項6に記載の通信処理装置。

[請求項14] 前記第1ネットワークの認証サーバを経由せずに災害発生を通知する災害情報を受信した場合には、前記第1ネットワークの認証サーバへ災害情報を転送するよう構成されている請求項6に記載の通信処理装置。

[請求項15] 第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバさせるための認証が行われるよう構成されている通信システムの前記第1ノードに実装される通信処理装置であって、

前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバのための認証処理を行う際に、前記第2ノードの識別情報を前記認証サーバへ通知するよう構成されている通信処理装置。

[請求項16] 前記第2ノードの識別情報を前記第2ノードから取得するよう構成されている請求項15に記載の通信処理装置。

[請求項17] 前記第1ノードから前記第2ノードへハンドオーバされた前記セッションの切断が検出された場合に、前記第2ノードから前記第1ノードへ前記セッションを戻す処理を行うよう構成されている請求項15に記載の通信処理装置。

[請求項18] 前記第1ノードから前記第2ノードへハンドオーバされた前記セッションを前記第2ノードから前記第1ノードへ戻す際に、前記第1ネ

ットワークの前記認証サーバとの間で前記セッションを戻すための認証を行うように構成されている請求項 15 に記載の通信処理装置。

[請求項19] 前記認証処理に成功した場合、前記セッションをハンドオーバーさせるためのシグナリングを前記第 1 ネットワークへ送信するように構成されている請求項 15 に記載の通信処理装置。

[請求項20] 前記認証処理に成功した後、前記セッションのハンドオーバーの開始指示を前記第 2 ノードへ送信するように構成されている請求項 15 に記載の通信処理装置。

[請求項21] 前記第 1 ノードから前記第 2 ノードへ第 1 のセッションをハンドオーバーさせる処理と、前記第 1 ノードから前記第 2 ノードへ既にハンドオーバーされていた第 2 のセッションを前記第 2 ノードから前記第 1 ノードへ戻す処理とを一括して行うために必要な情報を生成するように構成されている請求項 15 に記載の通信処理装置。

[請求項22] 前記第 1 ネットワークの認証サーバを経由せずに災害発生を通知する災害情報を受信した場合には、前記第 1 ネットワークの認証サーバへ災害情報を転送するよう構成されている請求項 15 に記載の通信処理装置。

[請求項23] 第 1 ネットワークに属する第 1 ノードが保持している前記第 1 ネットワークとの間の認証用情報を利用して、前記第 1 ノードと前記第 1 ネットワークとの間の通信中のセッションを前記第 1 ネットワークとは異なる第 2 ネットワークに属する第 2 ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第 2 ノードに実装される通信処理装置であって、

前記セッションのハンドオーバーのための認証に必要な情報を前記第 1 ノードから受信し、前記第 1 ネットワークの認証サーバとの間で前記セッションのハンドオーバーのための認証処理を行う際に、前記セッションのハンドオーバーのための認証に必要な情報に基づいて生成された情報を前記認証サーバへ通知するよう構成されている通信処理装置

。

[請求項24] 前記認証処理に成功した場合、前記セッションをハンドオーバーさせるためのシグナリングを前記第1ネットワークへ送信するように構成されている請求項23に記載の通信処理装置。

[請求項25] 前記認証処理に成功した後に前記セッションのハンドオーバーの開始指示を前記第1ノードから受信すると、前記セッションをハンドオーバーさせるためのシグナリングを前記第1ネットワークへ送信するように構成されている請求項23に記載の通信処理装置。

[請求項26] 災害発生を通知する災害情報に係るセッションのハンドオーバーに関しては、前記セッションのハンドオーバーのための認証に必要な情報に基づいて生成された情報として、より迅速な簡易的な認証を行うための情報を通知するよう構成されている請求項23に記載の通信処理装置。

[請求項27] 第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第2ノードに実装される通信処理装置であって、

前記第1ノードが前記第1ネットワークの認証サーバとの間で前記セッションのハンドオーバーのための認証処理を行う際に前記認証サーバへ通知するための前記第2ノードの識別情報を、前記第1ノードへ通知するよう構成されている通信処理装置。

[請求項28] 第1ネットワークに属する第1ノードが保持している前記第1ネットワークとの間の認証用情報を利用して、前記第1ノードと前記第1ネットワークとの間の通信中のセッションを前記第1ネットワークとは異なる第2ネットワークに属する第2ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第1ネ

ットワークに属する認証サーバに実装される認証処理装置であって、

前記第２ノードとの間で前記セッションのハンドオーバーのための認証処理を行う際に、前記第２ノードが前記第１ノードから受信した前記セッションのハンドオーバーのための認証に必要な情報に基づいて生成した情報を前記第２ノードから受信し、前記セッションのハンドオーバーのための認証に必要な情報に基づいて生成された前記情報を利用して前記セッションのハンドオーバーのための認証を行うように構成されている認証処理装置。

[請求項29] 前記セッションのハンドオーバーのための認証に必要な情報に基づいて生成された前記情報に基づいて、前記第１ノードを特定するとともに、前記第２ノードへの前記セッションのハンドオーバーの可否を認証するように構成されている請求項２８に記載の認証処理装置。

[請求項30] 前記認証処理に成功した場合、前記セッションに係るデータの転送先を前記第１ノードから前記第２ノードへ切り換えるように構成されている請求項２８に記載の認証処理装置。

[請求項31] 前記認証処理に成功した場合、前記セッションに係るデータを転送している装置に対して、前記データの転送先を前記第１ノードから前記第２ノードへ切り換えさせるシグナリングを送信するように構成されている請求項２８に記載の認証処理装置。

[請求項32] 前記第１ノードから前記第２ノードへハンドオーバーされた前記セッションの切断が検出された場合に、前記第２ノードから前記第１ノードへ前記セッションを戻す処理を行うよう構成されている請求項２８に記載の認証処理装置。

[請求項33] 前記セッションが災害発生を通知する災害情報を送信するためのものである場合には、より迅速な認証を行うための簡易的な認証を行うよう構成されている請求項２８に記載の認証処理装置。

[請求項34] 第１ネットワークに属する第１ノードが保持している前記第１ネットワークとの間の認証用情報を利用して、前記第１ノードと前記第１

ネットワークとの間の通信中のセッションを前記第 1 ネットワークとは異なる第 2 ネットワークに属する第 2 ノードへハンドオーバーさせるための認証が行われるよう構成されている通信システムの前記第 1 ネットワークに属する認証サーバに実装される認証処理装置であって、

前記第 1 ノードとの間で前記セッションのハンドオーバーのための認証処理を行う際に、前記第 2 ノードの識別情報を前記第 1 ノードから受信するように構成されている認証処理装置。

[請求項35] 前記第 2 ノードの識別情報を前記第 1 ノードから受信した場合、前記第 1 ノードの認証処理を行うとともに、前記第 2 ノードへの前記セッションのハンドオーバーの可否を認証するように構成されている請求項 3 4 に記載の認証処理装置。

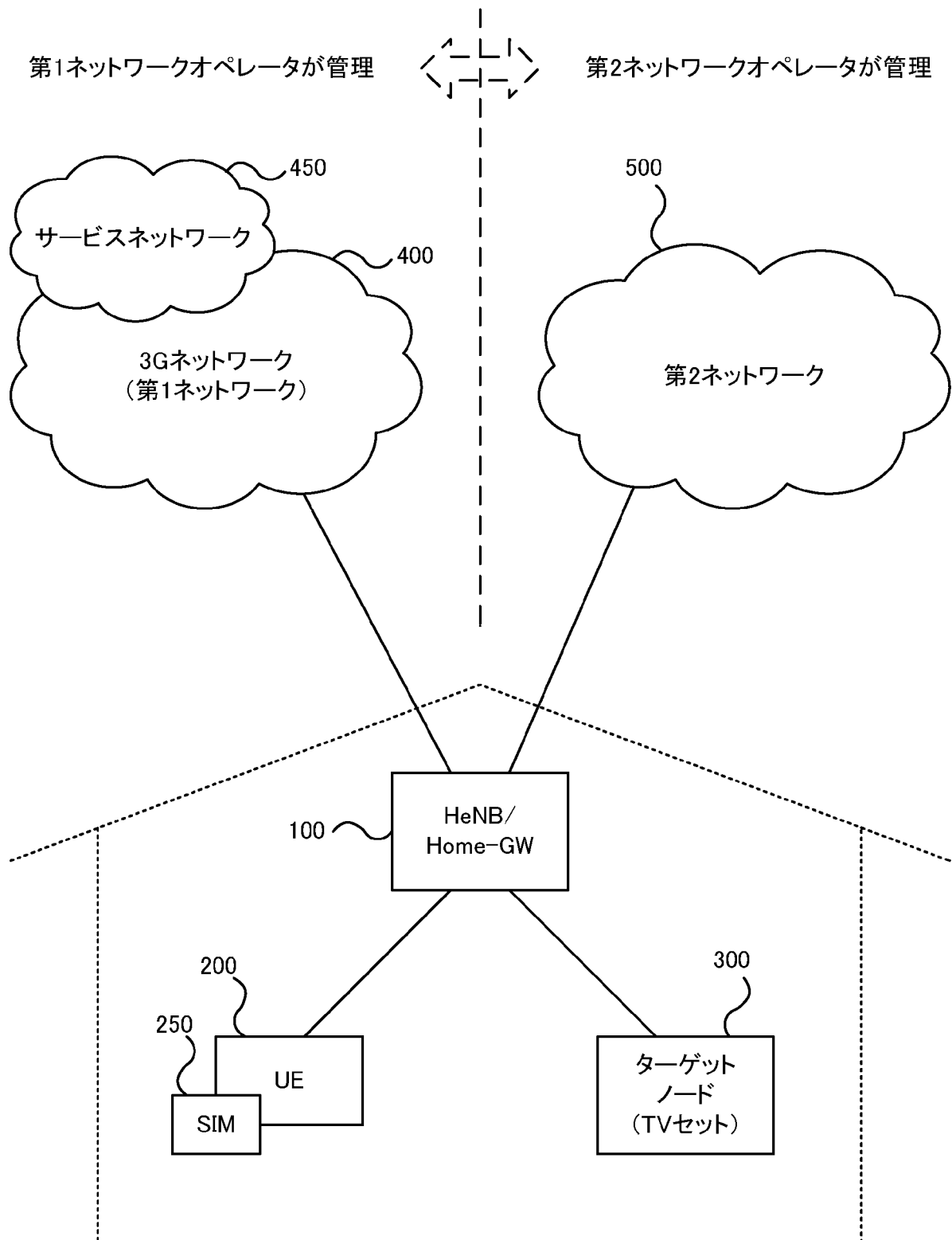
[請求項36] 前記認証処理に成功した場合、前記セッションに係るデータの転送先を前記第 1 ノードから前記第 2 ノードへ切り換えるように構成されている請求項 3 4 に記載の認証処理装置。

[請求項37] 前記認証処理に成功した場合、前記セッションに係るデータを転送している装置に対して、前記データの転送先を前記第 1 ノードから前記第 2 ノードへ切り換えさせるシグナリングを送信するように構成されている請求項 3 4 に記載の認証処理装置。

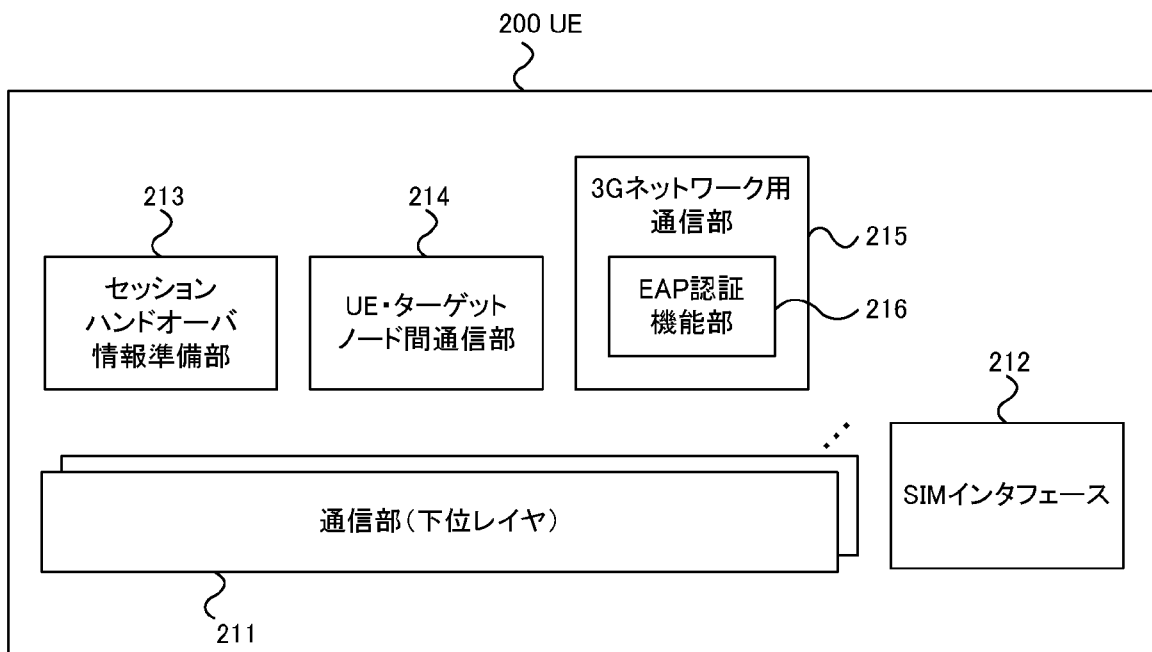
[請求項38] 前記第 1 ノードから前記第 2 ノードへハンドオーバーされた前記セッションの切断が検出された場合に、前記第 2 ノードから前記第 1 ノードへ前記セッションを戻す処理を行うよう構成されている請求項 3 4 に記載の認証処理装置。

[請求項39] 前記セッションが災害発生を通知する災害情報を送信するためのものである場合には、より迅速な認証を行うための簡易的な認証を行うよう構成されている請求項 3 4 に記載の認証処理装置。

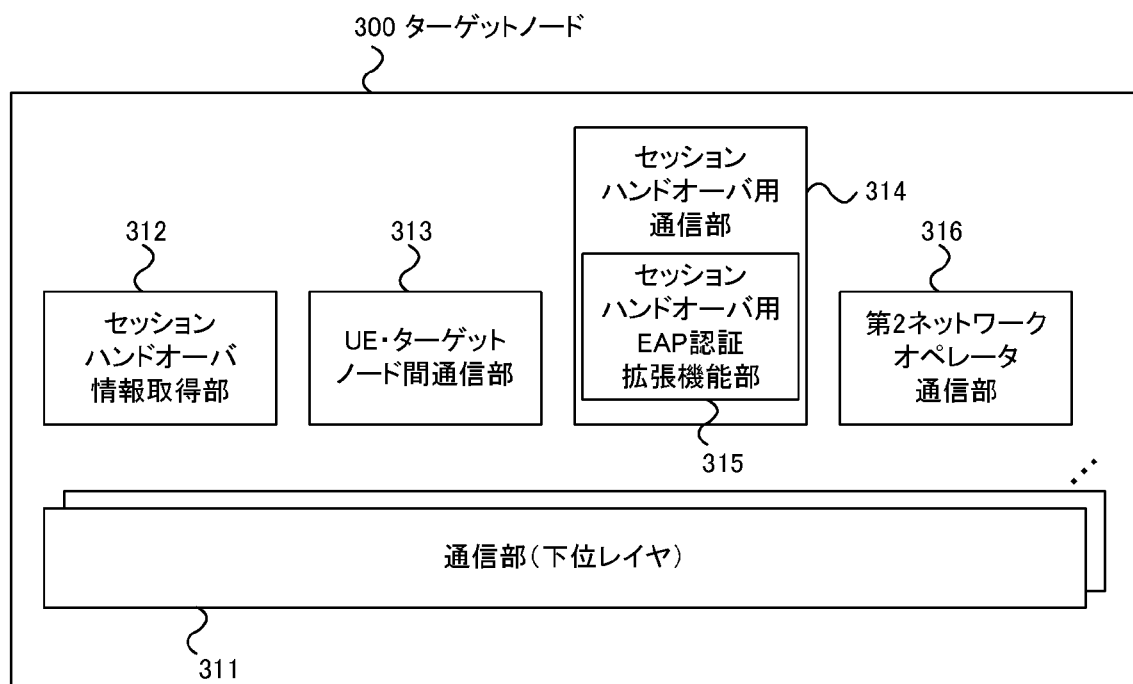
[図1]



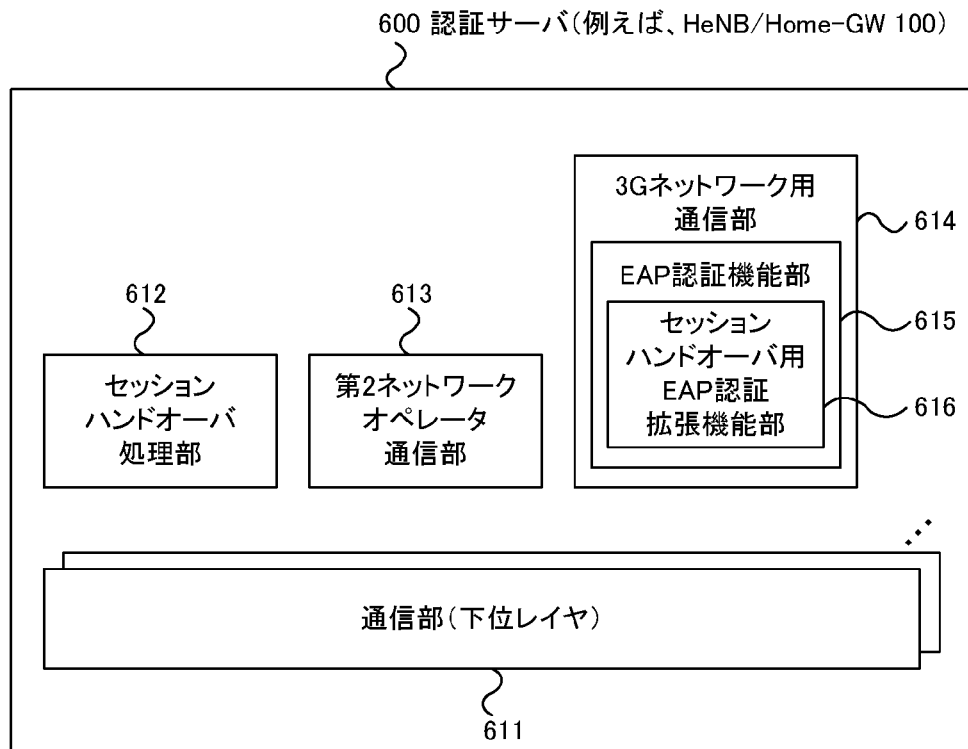
[図2]



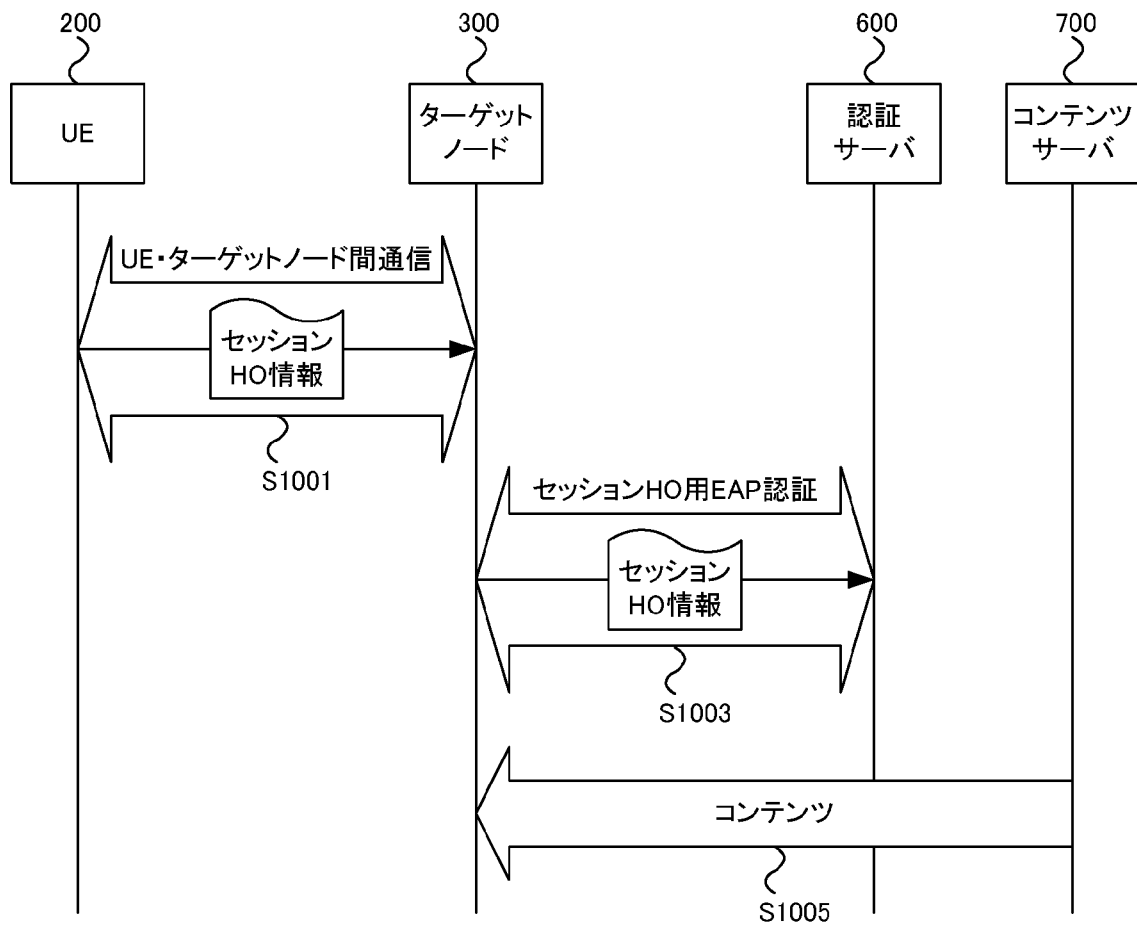
[図3]



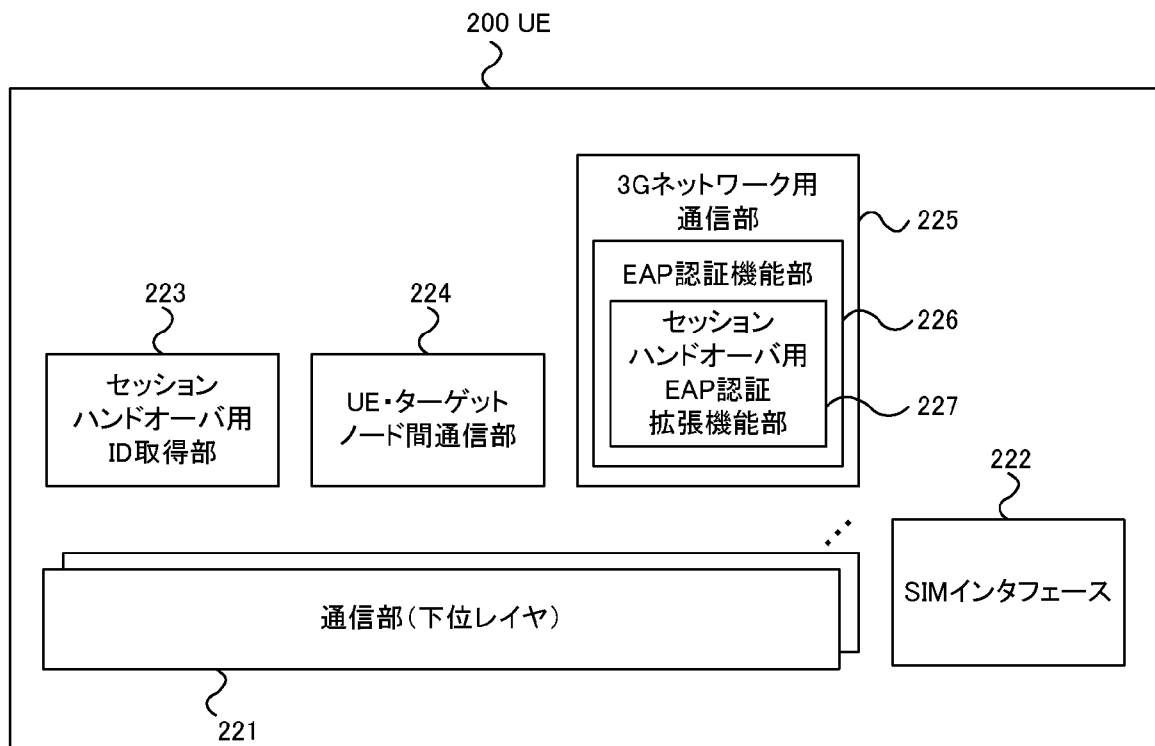
[図4]



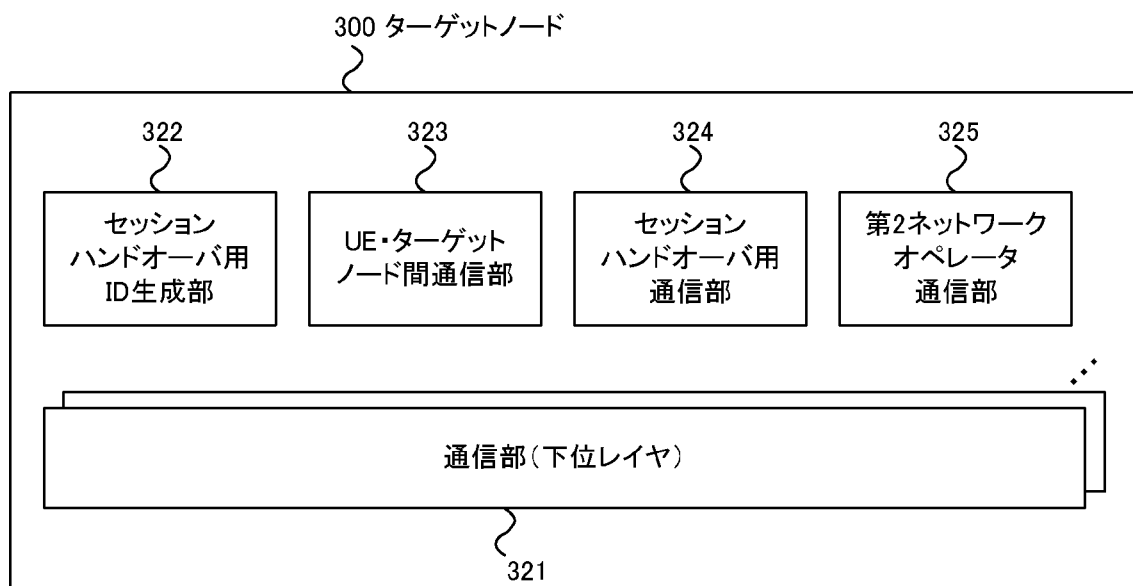
[図5]



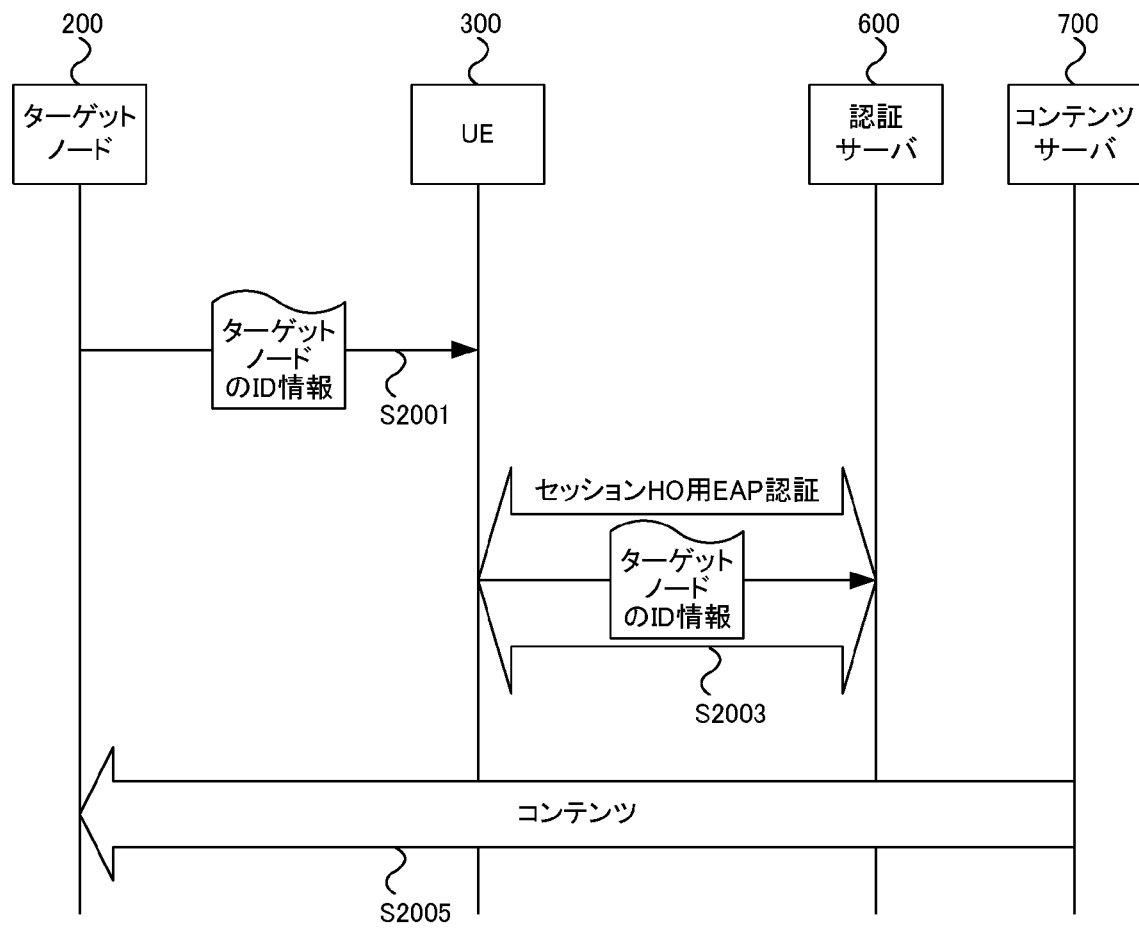
[図6]



[図7]

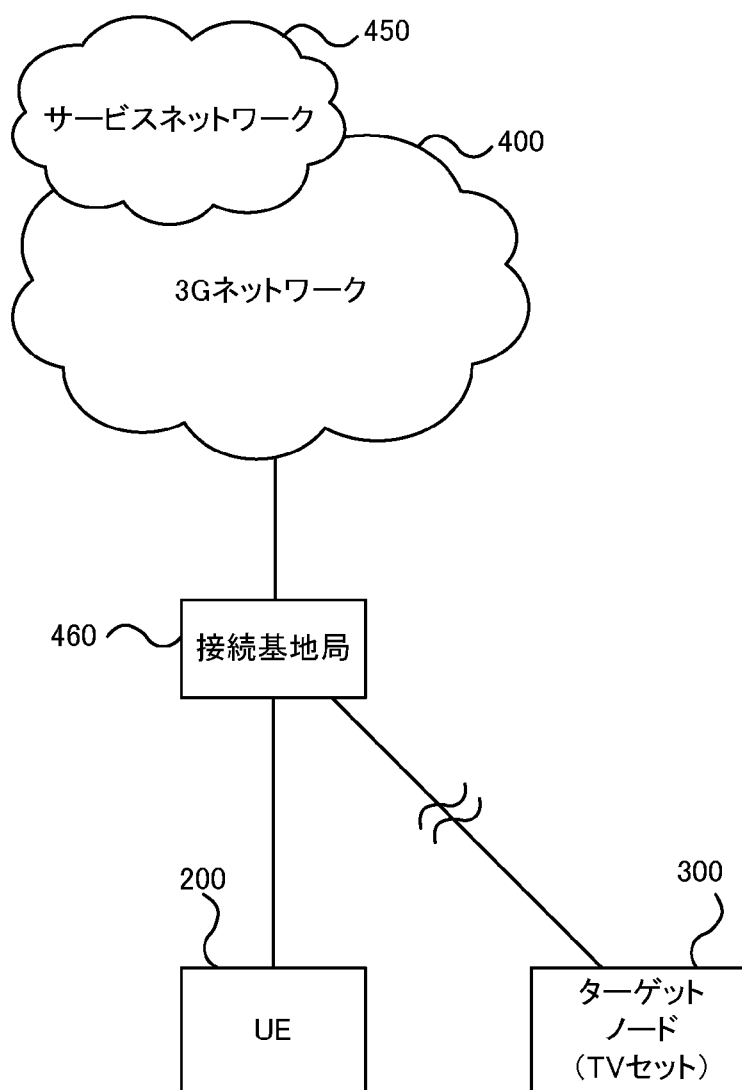


[図8]

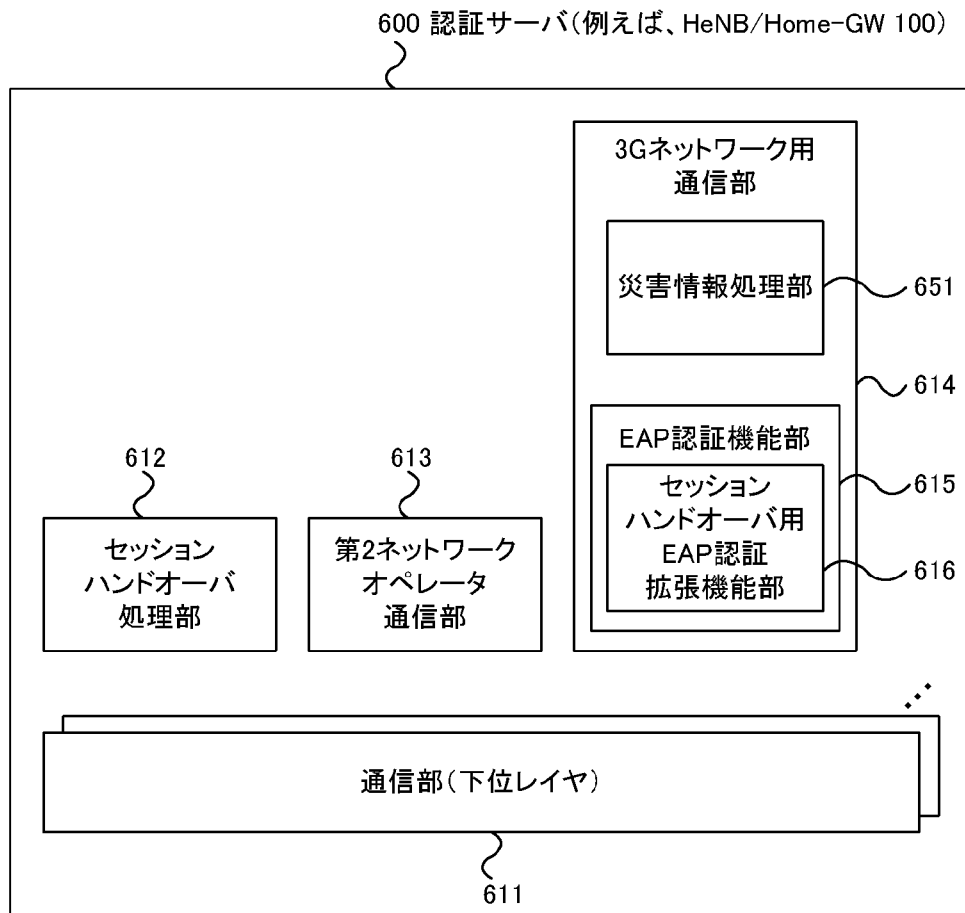


[図9]

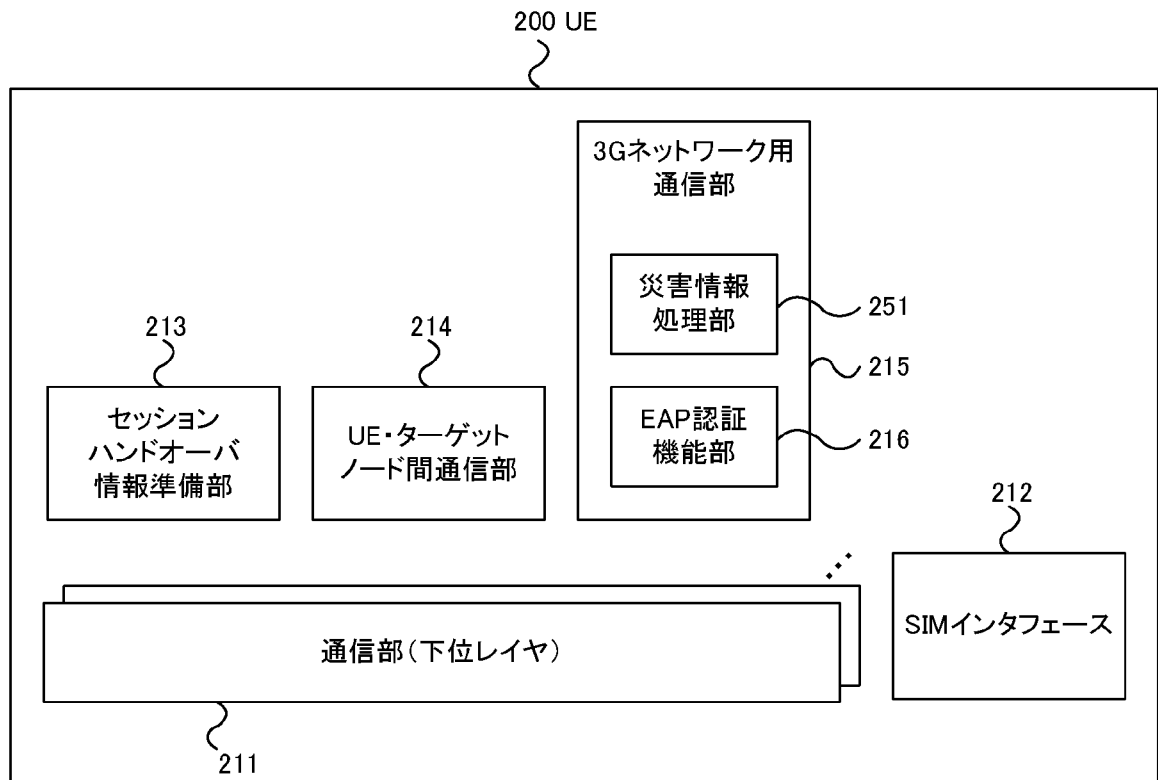
従来技術



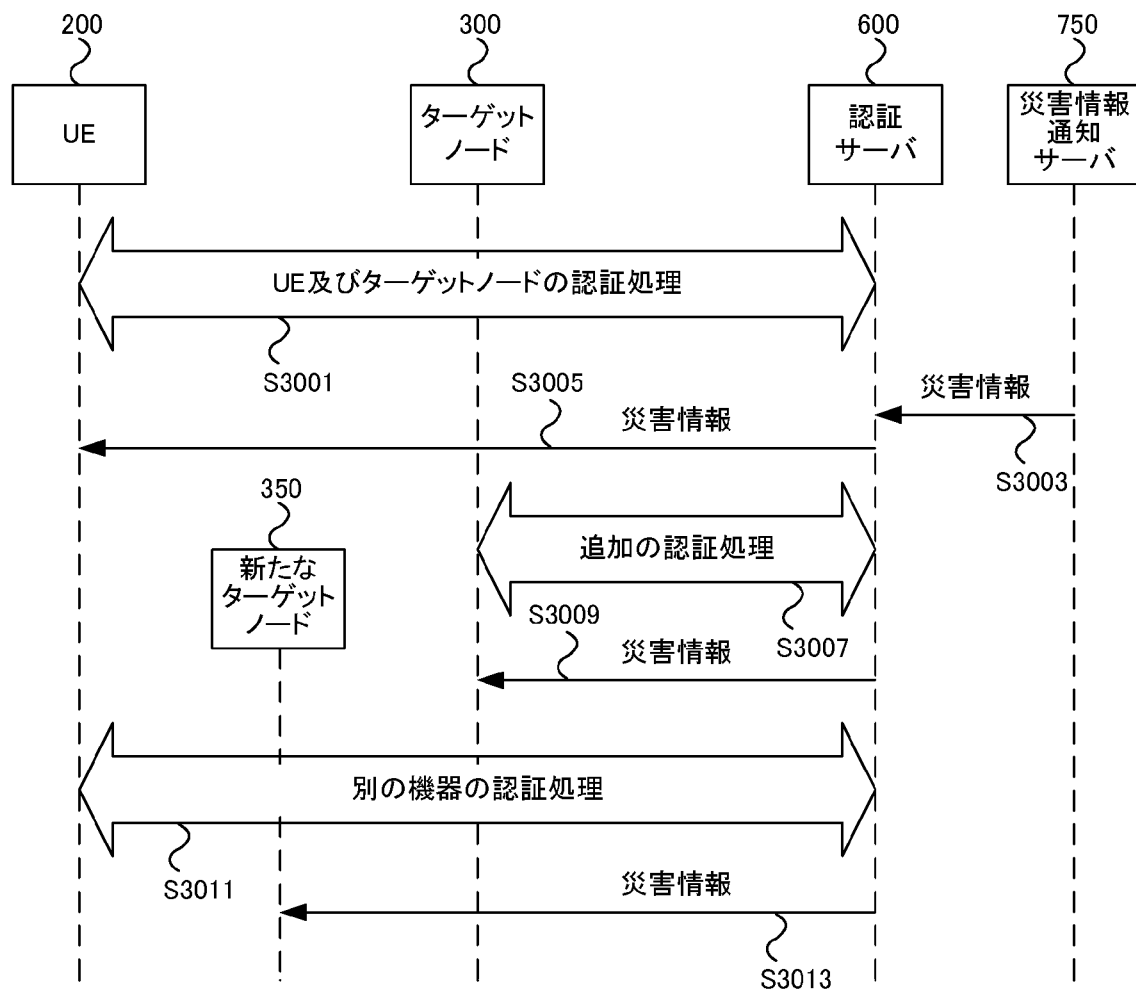
[図10]



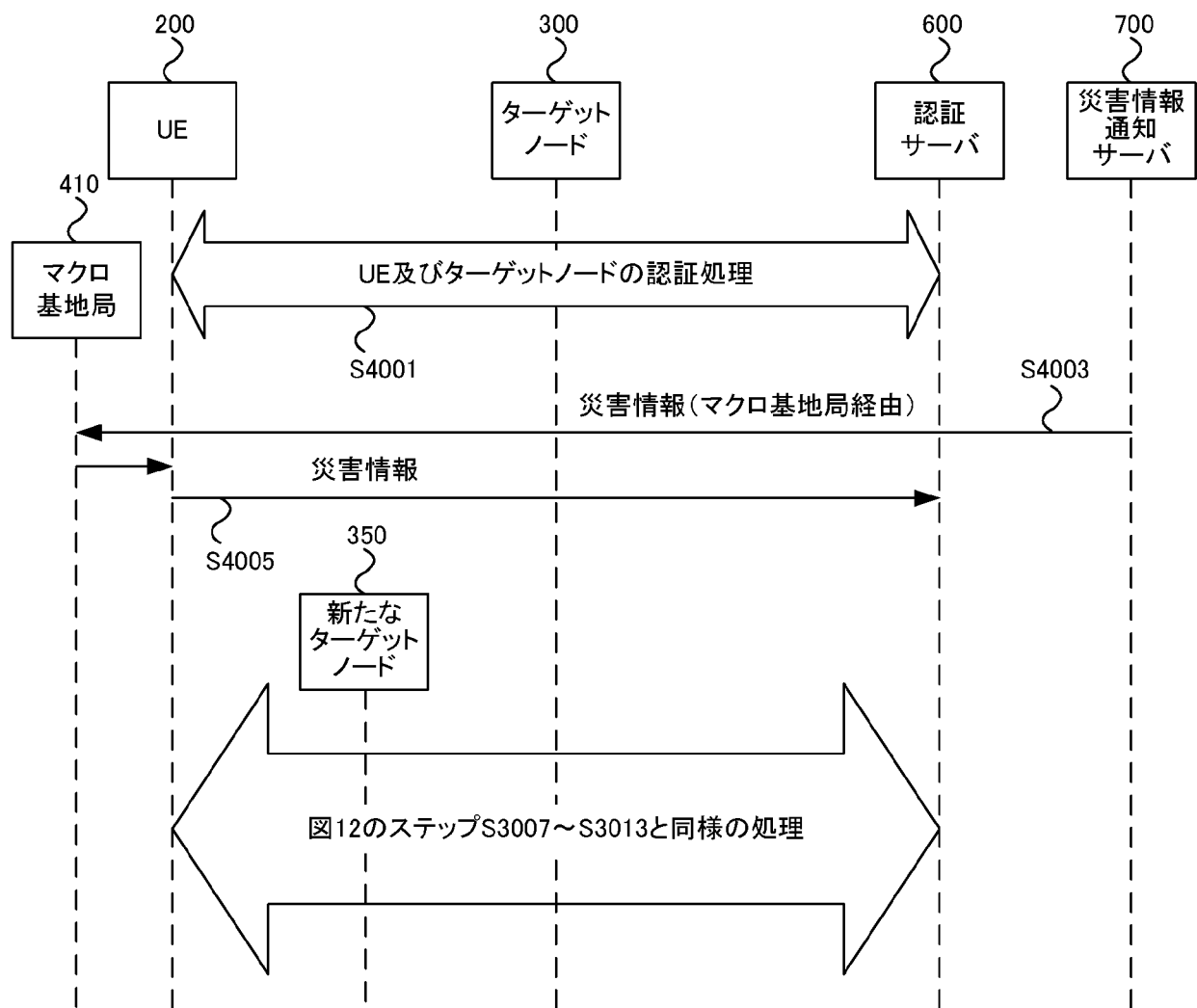
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/002833

A. CLASSIFICATION OF SUBJECT MATTER

H04W36/14 (2009.01) i, H04W12/06 (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)

H04W4/00-H04W99/00, H04B7/24-H04B7/26

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	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

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 Y	JP 2004-266331 A (Matsushita Electric Industrial Co., Ltd.), 24 September, 2004 (24.09.04), Par. Nos. [0050], [0056], [0057] & EP 1589777 A1 & US 2006/0135124 A1 & WO 2004/068887 A1	1 2-39
Y	WO 2007/005309 A1 (Lucent Technologies Inc.), 11 January, 2007 (11.01.07), Page 4, line 16 to page 6, line 17 & JP 2008-545337 & US 2007/0003062 A1 & EP 1897330 A1	2,3,6-39

☒ 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
13 August, 2009 (13.08.09)

Date of mailing of the international search report
25 August, 2009 (25.08.09)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/002833

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2007/103055 A2 (Interdigital Technology Corp.), 13 September, 2007 (13.09.07), Par. Nos. [0078], [0079] & JP 2009-528805 A & EP 1997340 A2	4, 13, 14, 22, 26, 33
Y	JP 2004-336256 A (NTT Docomo Inc.), 25 November, 2004 (25.11.04), Fig. 1 (Family: none)	5, 7
A	JP 2007-306312 A (Nippon Telegraph and Telephone East Corp.), 22 November, 2007 (22.11.07), Fig. 4 (Family: none)	1-39
A	JP 2007-515814 A (NTT Docomo Inc.), 14 June, 2007 (14.06.07), Claim 1 & WO 2005/015938 A1	1-39

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04W36/14(2009.01)i, H04W12/06(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. H04W4/00-H04W99/00, H04B7/24-H04B7/26

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 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 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	JP 2004-266331 A（松下電器産業株式会社）2004.09.24, [0050], [0056], [0057] & EP 1589777 A1 & US 2006/0135124 A1 & WO 2004/068887 A1	1 2-39
Y	WO 2007/005309 A1（ルーセント テクノロジーズ インコーポレイテッド）2007.01.11, 第4頁第16行-第6頁第17行 & JP 2008-545337 & US 2007/0003062 A1 & EP 1897330 A1	2, 3, 6-39

☒ 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 3 . 0 8 . 2 0 0 9

国際調査報告の発送日

2 5 . 0 8 . 2 0 0 9

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100-8915

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）

望月 章俊

5 J

4 1 0 1

電話番号 03-3581-1101 内線 3534

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
Y	WO 2007/103055 A2 (インターディジタル テクノロジー コーポレイション) 2007.09.13, [0078]、[0079] & JP 2009-528805 A & EP 1997340 A2	4, 13, 14, 22, 26, 33
Y	JP 2004-336256 A (株式会社エヌ・ティ・ティ・ドコモ) 2004.11.25, 図1 (ファミリーなし)	5, 7
A	JP 2007-306312 A (東日本電信電話株式会社) 2007.11.22, 図4 (ファミリーなし)	1-39
A	JP 2007-515814 A (株式会社エヌ・ティ・ティ・ドコモ) 2007.06.14, 請求項1 & WO 2005/015938 A1	1-39