(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5286360号
(P5286360)

(45)発行日　平成25年9月11日(2013.9.11)　(24)登録日　平成25年6月7日(2013.6.7)

(51)Int.Cl.		F I		
H04W 36/14	(2009.01)	H04W	36/14	
H04W 12/06	(2009.01)	H04W	12/06	
H04M 11/00	(2006.01)	H04M	11/00	302

請求項の数 23　(全 38 頁)

(21)出願番号	特願2010-517748 (P2010-517748)
(86)(22)出願日	平成21年6月22日 (2009.6.22)
(86)国際出願番号	PCT/JP2009/002833
(87)国際公開番号	WO2009/157172
(87)国際公開日	平成21年12月30日 (2009.12.30)
審査請求日	平成24年5月25日 (2012.5.25)
(31)優先権主張番号	特願2008-168773 (P2008-168773)
(32)優先日	平成20年6月27日 (2008.6.27)
(33)優先権主張国	日本国(JP)
(31)優先権主張番号	特願2009-19217 (P2009-19217)
(32)優先日	平成21年1月30日 (2009.1.30)
(33)優先権主張国	日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100093067
弁理士　二瓶　正敬
(72)発明者　平野　純
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　荒牧　隆
大阪府門真市大字門真１００６番地　パナソニック株式会社内
(72)発明者　池田　新吉
大阪府門真市大字門真１００６番地　パナソニック株式会社内

最終頁に続く

(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)【特許請求の範囲】

【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であって、

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通信システム。

【請求項２】

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３】
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、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２に記載の通信処理装置。
【請求項４】
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２に記載の通信処理装置。
【請求項５】
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２に記載の通信処理装置。
【請求項６】
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２に記載の通信処理装置。
【請求項７】
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２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ノードへ第１のセッションをハンドオーバさせる処理と、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２に記載の通信処理装置。
【請求項９】
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２に記載の通信処理装置。
【請求項１０】
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２に記載の通信処理装置。
【請求項１１】
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１２】
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に構成されている請求項１１に記載の通信処理装置。
【請求項１３】
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通信処理装置。

【請求項１４】

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１３に記載の通信処理装置。

【請求項１５】

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１３に記載の通信処理装置。

【請求項１６】

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１３に記載の通信処理装置。

【請求項１７】

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１８】

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のための認証を行うように構成されており、

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の可否を認証するように構成されている認証処理装置。

【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１８に記載の認証処理装置。

【請求項２０】

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１８に記載の認証処理装置。
【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１８に記載の認証処理装置。
【請求項２２】
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１８に記載の認証処理装置。
【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おり、
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の可否を認証するように構成されている認証処理装置。
【発明の詳細な説明】
【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、ＩＥＥＥ８０２．１６）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

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ネットワークで使用でき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（ＵＥ２００）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】
【発明が解決しようとする課題】
【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。

【課題を解決するための手段】
【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。
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。
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の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の開始指示を送信し、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用通信部３１４はセッションハンドオーバ用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、ＵＥ２００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情報取得部３１２は、ＵＥ・ターゲットノード間通信部３１３でＵＥ２００から受信したセッションＨＯ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３１３は、ＵＥ２００から送信されたセッションＨＯ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ＵＥ２００から受信するセッションＨＯ情報は、セキュアな状態で伝送されることが望ましい。

【００４２】

また、セッションハンドオーバ用通信部３１４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用通信部３１４は、セッションハンドオーバ用ＥＡＰ認証拡張機能部３１５におけるセッションハンドオーバの認証に成功した場合、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、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３１５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、３Ｇネットワーク用通信部６１４を有しており、３Ｇ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、３Ｇ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３Ｇ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処理部６１２は、セッションハンドオーバ用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へハンドオーバさせる機能を有している。なお、セッションハンドオーバ処理部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のための認証と、実際のセッションハンドオーバ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が開始されると、まず、ＵＥ２００のセッションハンドオーバ情報準備部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、ＵＥ２００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、ＵＥ２００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ＵＥ２００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、ＵＥ２００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ＵＥ２００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用ＥＡＰ認証拡張機能部３１５において、ＵＥ２００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ＵＥ２００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Ｈｏｍｅ－ＧＷとＨｅＮＢとは同一の装置（ＨｅＮＢ／Ｈｏｍｅ－ＧＷ１００）であるため、ターゲットノード３００は、３Ｇネットワーク４００に対するＥＡＰ認証の際にセッションＨＯ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３００とＨｏｍｅ－ＧＷとの間におけるアクセス認証が完了している場合には、ＨｅＮＢによってターゲットノード３００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６００は、セッションハンドオーバ用ＥＡＰ認証拡張機能部３１５において、ターゲットノード３００から受信したセッションＨＯ情報に基づいてセッションハンドオーバのための認証を行い、セッションのハンドオーバ元のＵＥ２００を検証するとともに、セッションのハンドオーバ先のターゲットノード３００を特定する。セッションハンドオーバ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処理部６１２は、ＵＥ２００からターゲットノード３００へセッションをハンドオーバさせる処理を開始する。これにより、３Ｇネットワーク４００側ではそれまでＵＥ２００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）。

【００６０】

なお、特定のセッションのハンドオーバ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させる。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。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３００は自身の認証情報（ターゲットノード３００のＩＤ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。

【００６２】

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セッションハンドオーバ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がセッションハンドオーバ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にハンドオーバさせることで、セッションがＵＥ２００に戻される。

【００６３】

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、ターゲットノード３００からＵＥ２００へのハンドオーバなどは、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、ＵＥ２００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、ＵＥ２００がセッションのハンドオーバ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ＵＥ２００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。ＵＥ２００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、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。

【００６７】

また、ＳＩＭインタフェース２２２は、ＵＥ２００に装着されているＳＩＭ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と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２２５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２２５は、セッションハンドオーバ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の開始指示を送信し、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の識別情報の生成（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と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用通信部３２４は、セッションハンドオーバ用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のための認証と、実際のセッションハンドオーバ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が開始されると、まず、ＵＥ２００は、セッションハンドオーバ用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の開始とともに、ＵＥ２００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、ＵＥ２００は、ＵＥ２００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の要求をＵＥ２００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、ＵＥ２００からターゲットノード３００へセッションハンドオーバを行う際の分岐点（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、ＵＥ２００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ＵＥ２００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、ＵＥ２００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ＵＥ２００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ＵＥ２００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、ＵＥ２００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Ｓ２００１でターゲットノード３００の識別情報を取得したＵＥ２００は、セッションハンドオーバ用ＥＡＰ認証拡張機能部２２７において、ＵＥ２００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Ｓ２００３）。なお、ＵＥ２００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Ｓ２００３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、ＵＥ２００の接続ノードはＨｅＮＢ／Ｈｏｍｅ－ＧＷ１００であり、ＵＥ２００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用ＥＡＰ認証拡張機能部３１５において、ＵＥ２００との間のセッションハンドオーバのためのＥＡＰ認証を行う。セッションハンドオーバ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ＵＥ２００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させる。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。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セッションハンドオーバ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、ターゲットノード３００からＵＥ２００へのハンドオーバなどは、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、ＵＥ２００に対する他の通信（セッションハンドオーバに係るセッション以外の通信）が止まったりＵＥ２００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、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を一例に挙げて説明を行ったが、ＵＥ２００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によって、ＵＥ２００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、ＵＥ２００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、ＵＥ２００からターゲットノード３００へセッションを移すとともに、ＵＥ２００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、ＵＥ２００は、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、ＵＥ２００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ＵＥ２００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、ＵＥ２００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、ＵＥ２００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、ＵＥ２００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、ＵＥ２００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元であるＵＥ２００とセッションハンドオーバ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、ＵＥ２００とターゲットノード３００と、それぞ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ＵＥ２００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、ＵＥ２００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、ＵＥ２００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ＵＥ２００のセッションについて説明しているが、複数の異なるＵＥ２００のセッションを一括してセッションハンドオーバ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ＵＥ２００（複数のＵＥ２００のうちの１つ）が、他のＵＥ２００のセッションハンドオーバ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ＵＥ２００は代表となるＵＥ２００に対してあらかじめセッションハンドオーバに必要な情報を通知しておくとよい。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、ＵＥ２００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、ＵＥ２００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、ＵＥ２００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、ＵＥ２００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

必要となる情報をまとめ、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、ＵＥ２００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、ＵＥ２００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、ＥＴＷＳ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、ＥＴＷＳ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６５１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ＥＡＰ認証機能部２２６に通知したり、ＥＡＰ認証機能部２２６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６５１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６５１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６００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１１は、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である。図１１に図示されているＵＥ２００は、図２に図示されているＵＥ２００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ＵＥ２００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】
ＵＥ２００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、ＵＥ２００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、ＵＥ２００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用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ＵＥ２００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ＵＥ２００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、ＵＥ２００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ＨＯ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ＨＯ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１２には不図示であるが、認証サーバ６００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６００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６００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、ＵＥ２００、ターゲットノード３００／新たなターゲットノード３５０、認証サーバ６００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６００が３Ｇネットワーク４００から災害情報の通知を受けてＵＥ２００に災害情報を通知する場合について説明しているが、ＵＥ２００もマクロ基地局を通じて３Ｇネットワーク４００に接続可能であり、ＵＥ２００が認証サーバ６００より先に３Ｇネットワーク４００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、ＵＥ２００が３Ｇネットワーク４００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、ＵＥ２００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）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ＵＥ２００がマクロ基地局から災害情報を受信するためには、ＵＥ２００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、ＵＥ２００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ＵＥ２００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側からだけではなく、ＵＥ２００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ＵＥ２００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、ＵＥ２００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、ＵＥ２００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、ＵＥ２００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Ｓ４００５）。
【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Ｓ３００７～Ｓ３０１３の処理）とほぼ同様である。すなわち、認証サーバ６００は、ＵＥ２００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、ＵＥ２００から災害情報を受信したことから、ＵＥ２００に対して災害情報を再度通知する必要はない。また、ＵＥ２００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、ＵＥ２００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、ＵＥ２００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－ＧＷ１００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－ＧＷ１００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ＵＥ２００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ＵＥ２００を経由して（ＵＥ２００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（ＵＥ２００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ＵＥ２００へセッションを戻す（セッションハンドオーバ）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ＵＥ２００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、ＵＥ２００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ＵＥ２００がこのコンテンツサービスを受信している場合に、ＵＥ２００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に係る認証を行うことで、ＵＥ２００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、ＵＥ２００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、ＵＥ２００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Ｌ

ＳＩ、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】

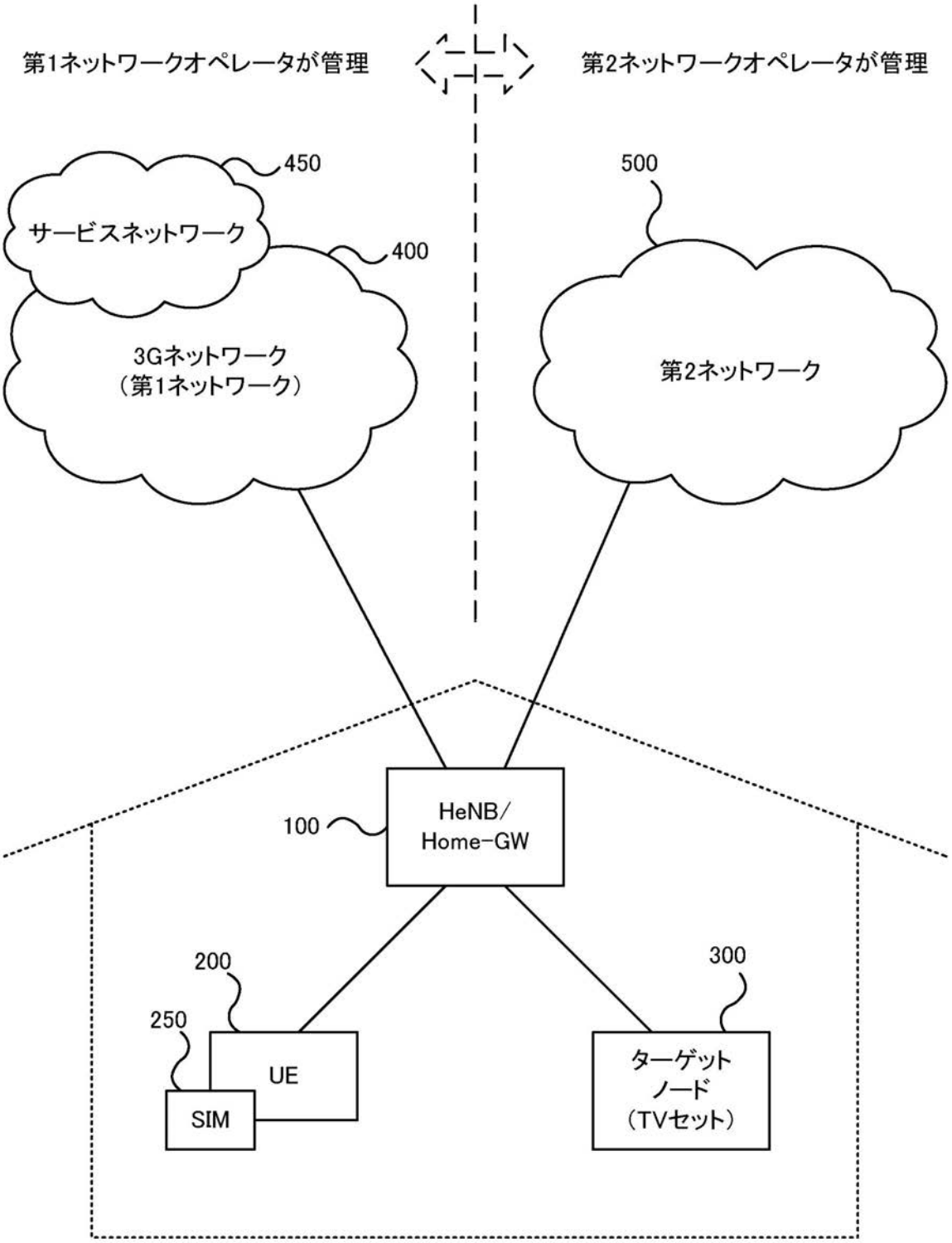
さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。例えば、バイオ技術の適応などが可能性としてあり得る。

【産業上の利用可能性】

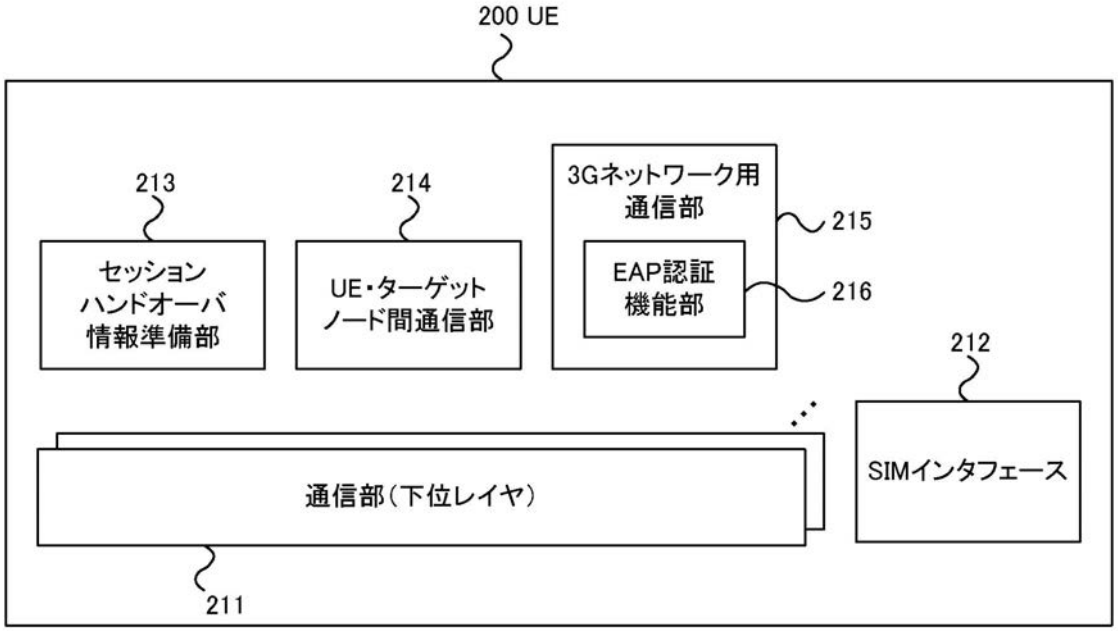
【０１４２】

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。

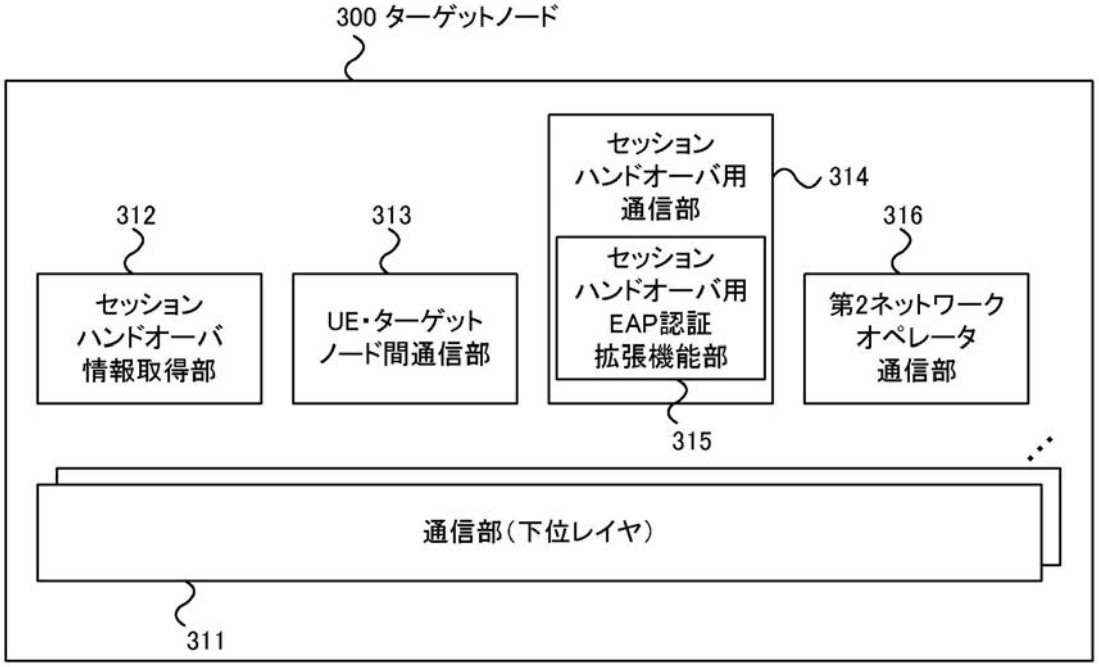
【図１】


第1ネットワークオペレータが管理
第2ネットワークオペレータが管理
450
サービスネットワーク
400
3Gネットワーク
（第1ネットワーク）
500
第2ネットワーク
100
HeNB/
Home-GW
200
250
UE
SIM
300
ターゲット
ノード
（TVセット）

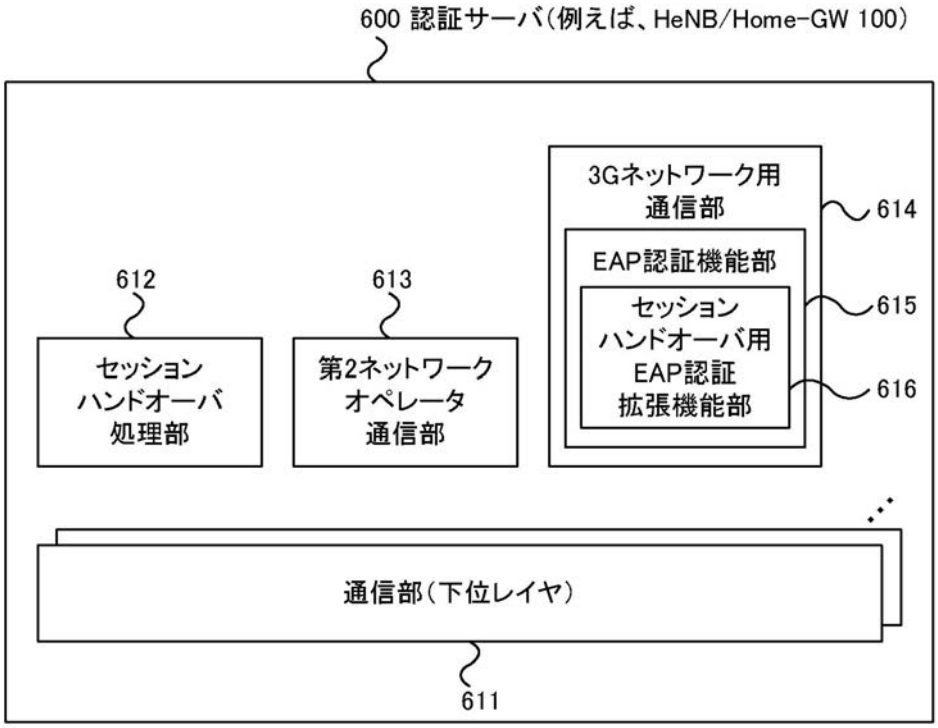
【図２】


200 UE
213
セッション
ハンドオーバ
情報準備部
214
UE・ターゲット
ノード間通信部
3Gネットワーク用
通信部
215
EAP認証
機能部
216
212
SIMインタフェース
通信部（下位レイヤ）
211

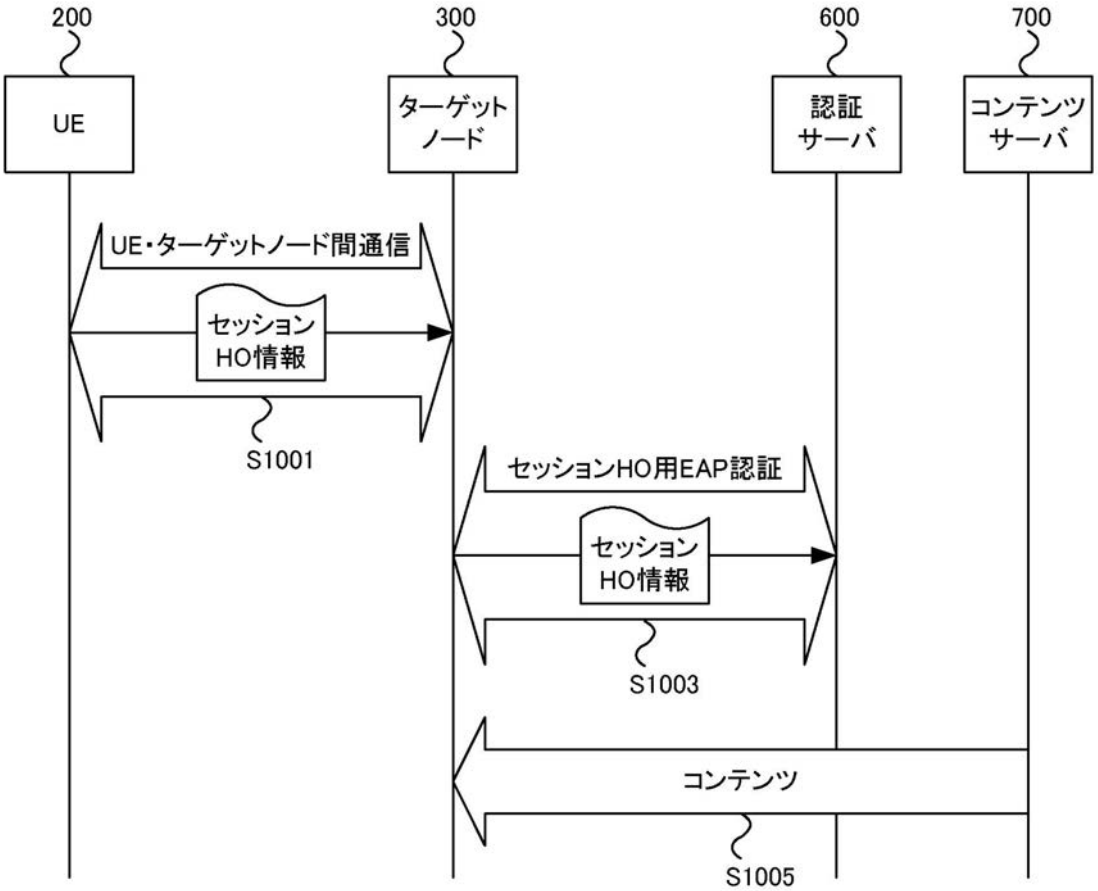
【図３】


300 ターゲットノード
312
セッション
ハンドオーバ
情報取得部
313
UE・ターゲット
ノード間通信部
セッション
ハンドオーバ用
通信部
314
セッション
ハンドオーバ用
EAP認証
拡張機能部
315
316
第2ネットワーク
オペレータ
通信部
通信部（下位レイヤ）
311

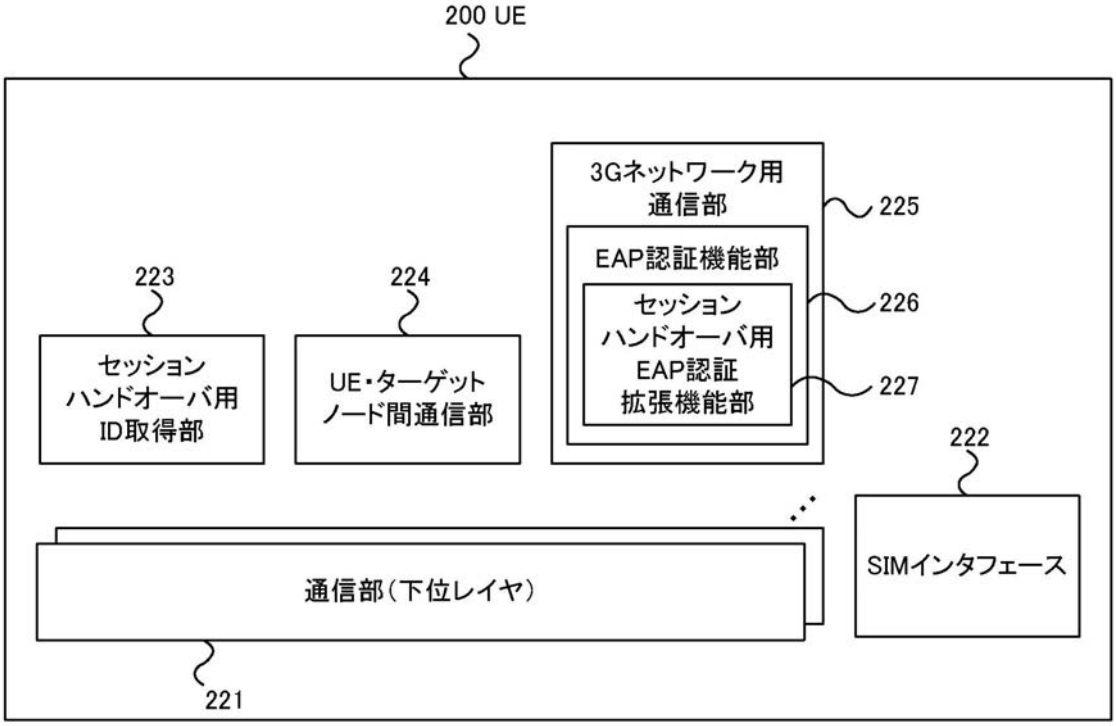
【図４】


600 認証サーバ（例えば、HeNB/Home-GW 100）
3Gネットワーク用
通信部
614
EAP認証機能部
セッション
ハンドオーバ用
EAP認証
拡張機能部
615
616
612
セッション
ハンドオーバ
処理部
613
第2ネットワーク
オペレータ
通信部
通信部（下位レイヤ）
611

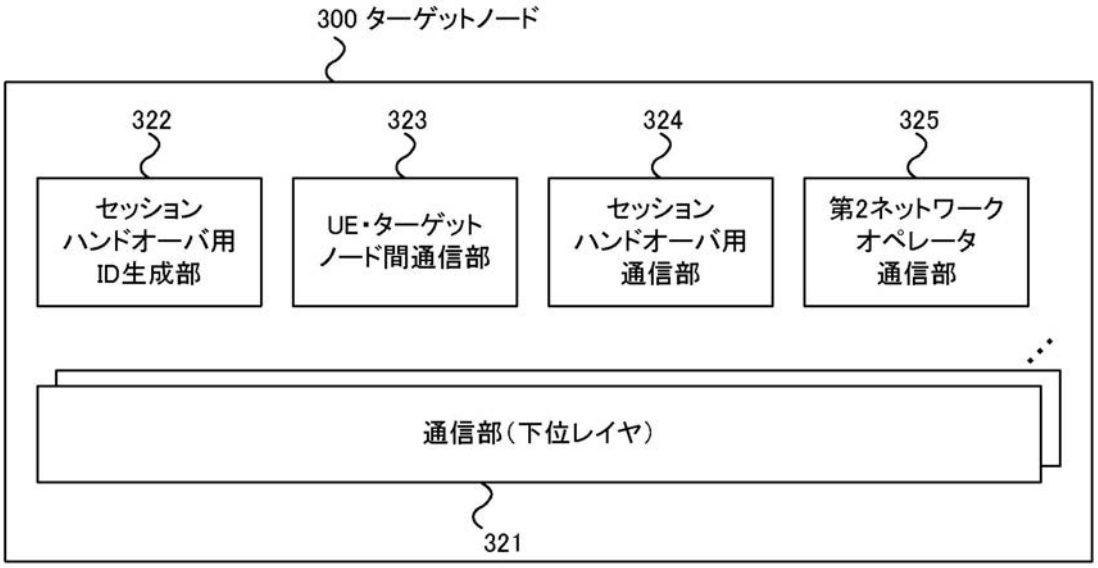
【図５】


200
UE
300
ターゲット
ノード
600
認証
サーバ
700
コンテンツ
サーバ
UE・ターゲットノード間通信
セッション
HO情報
S1001
セッションHO用EAP認証
セッション
HO情報
S1003
コンテンツ
S1005

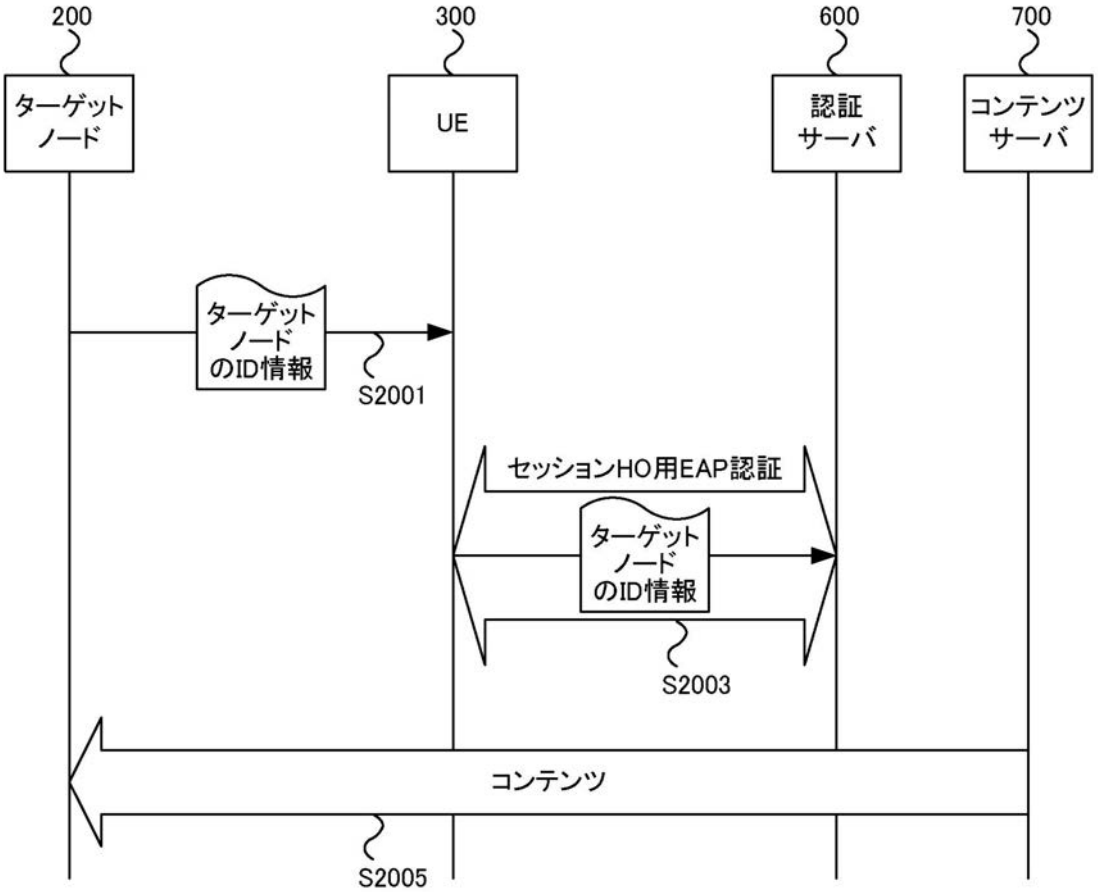
【図６】


200 UE
3Gネットワーク用
通信部
225
EAP認証機能部
セッション
ハンドオーバ用
EAP認証
拡張機能部
226
227
223
セッション
ハンドオーバ用
ID取得部
224
UE・ターゲット
ノード間通信部
222
SIMインタフェース
通信部（下位レイヤ）
221

【図７】

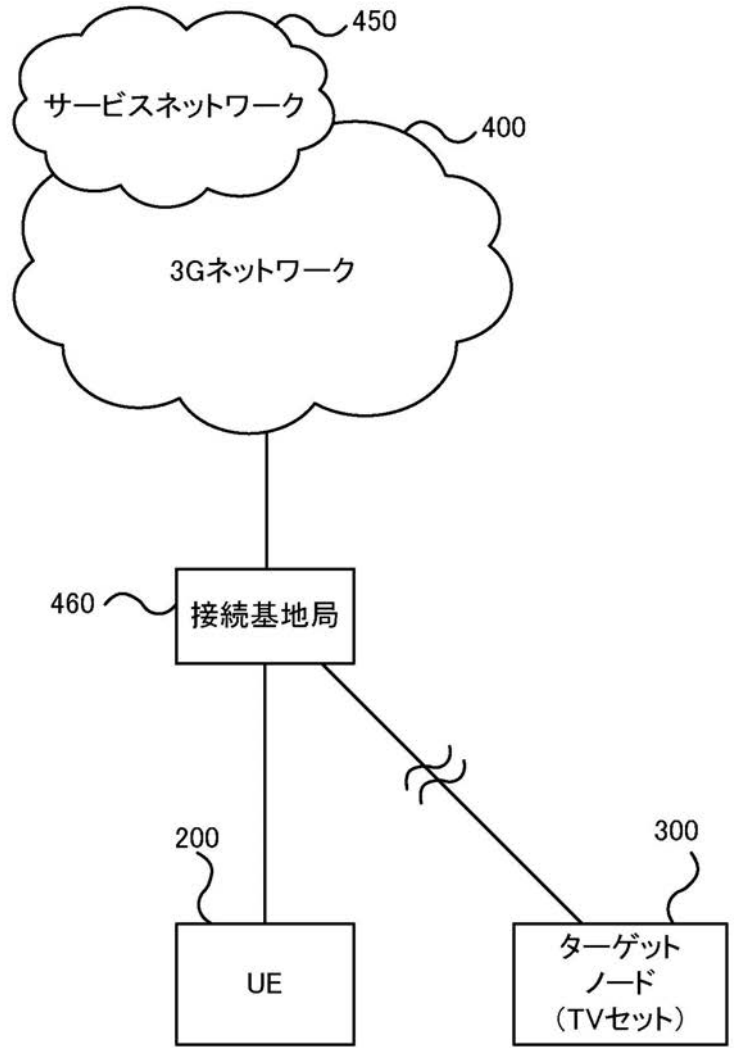

300 ターゲットノード
322
セッション
ハンドオーバ用
ID生成部
323
UE・ターゲット
ノード間通信部
324
セッション
ハンドオーバ用
通信部
325
第2ネットワーク
オペレータ
通信部
通信部（下位レイヤ）
321

【図８】

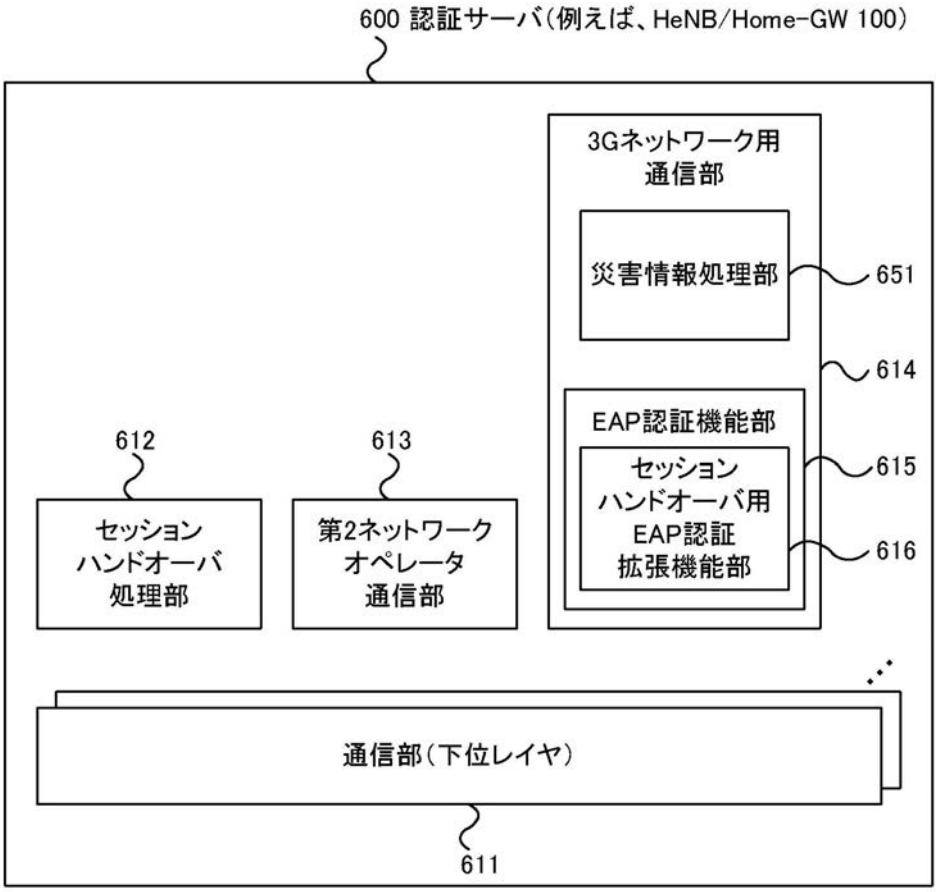

200
300
600
700
ターゲット
ノード
UE
認証
サーバ
コンテンツ
サーバ
ターゲット
ノード
のID情報
S2001
セッションHO用EAP認証
ターゲット
ノード
のID情報
S2003
コンテンツ
S2005

【図９】

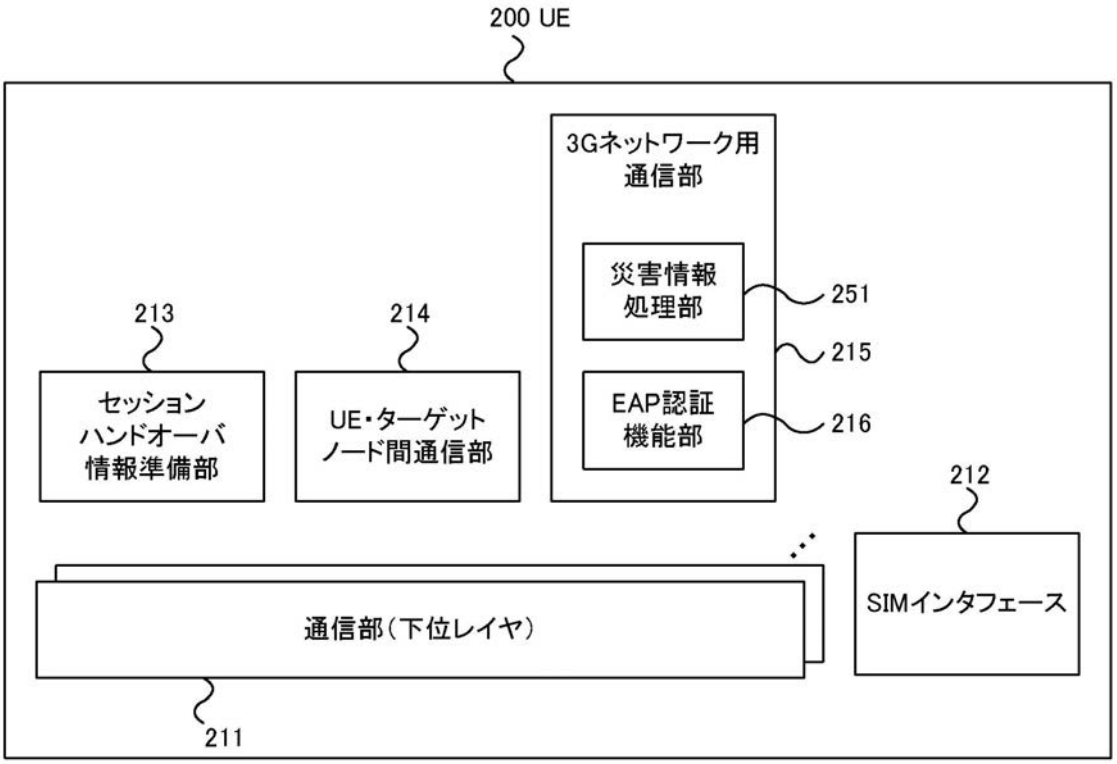
従来技術


450
サービスネットワーク
400
3Gネットワーク
460
接続基地局
200
UE
300
ターゲット
ノード
（TVセット）

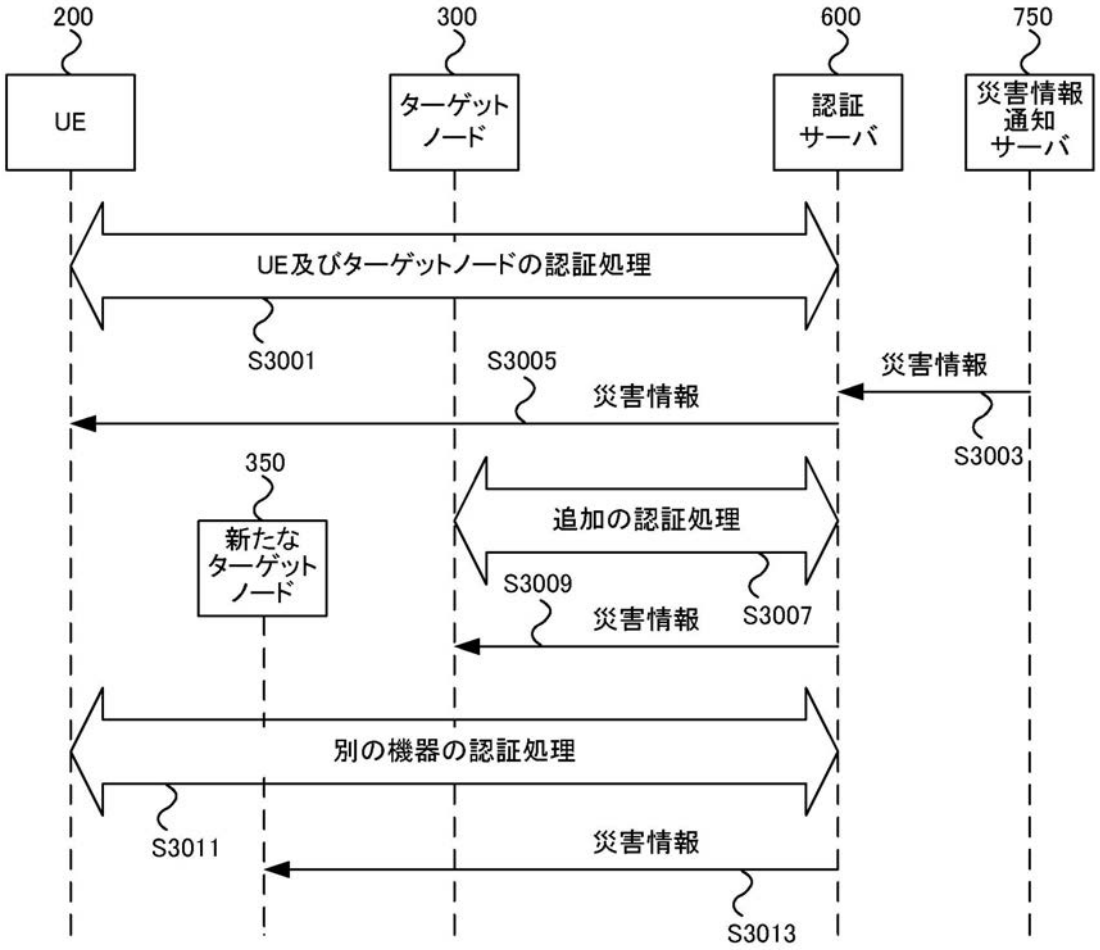
【図１０】


600 認証サーバ（例えば、HeNB/Home-GW 100）
3Gネットワーク用
通信部
災害情報処理部
651
614
EAP認証機能部
セッション
ハンドオーバ用
EAP認証
拡張機能部
615
616
612
セッション
ハンドオーバ
処理部
613
第2ネットワーク
オペレータ
通信部
通信部（下位レイヤ）
611

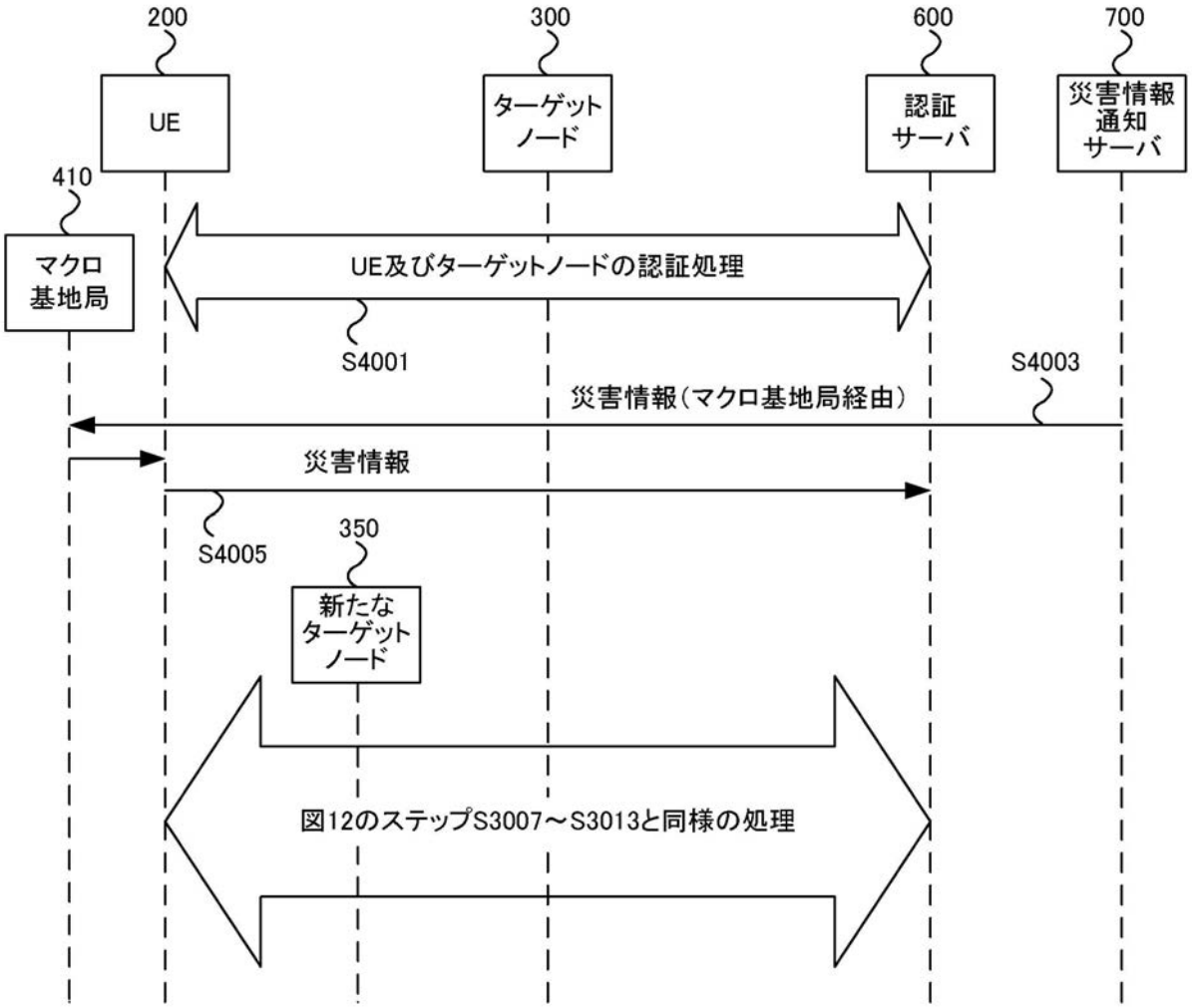
【図１１】


200 UE
3Gネットワーク用
通信部
災害情報
処理部
251
215
EAP認証
機能部
216
213
セッション
ハンドオーバ
情報準備部
214
UE・ターゲット
ノード間通信部
212
SIMインタフェース
通信部（下位レイヤ）
211

【図１２】


200
300
600
750
UE
ターゲット
ノード
認証
サーバ
災害情報
通知
サーバ
UE及びターゲットノードの認証処理
S3001
S3005
災害情報
災害情報
S3003
350
新たな
ターゲット
ノード
追加の認証処理
S3009
災害情報
S3007
別の機器の認証処理
S3011
災害情報
S3013

【図１３】


200
UE
300
ターゲット
ノード
600
認証
サーバ
700
災害情報
通知
サーバ
410
マクロ
基地局
UE及びターゲットノードの認証処理
S4001
S4003
災害情報（マクロ基地局経由）
災害情報
S4005
350
新たな
ターゲット
ノード
図12のステップS3007～S3013と同様の処理

フロントページの続き

(72)発明者　青山　高久
大阪府門真市大字門真１００６番地　パナソニック株式会社内

審査官　望月　章俊

(56)参考文献　特開２００４－２６６３３１（ＪＰ，Ａ）
国際公開第２００７／００５３０９（WO，Ａ１）
国際公開第２００７／１０３０５５（WO，Ａ２）
特開２００４－３３６２５６（ＪＰ，Ａ）
特開２００７－３０６３１２（ＪＰ，Ａ）
特表２００７－５１５８１４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｗ４／００－Ｈ０４Ｗ９９／００
Ｈ０４Ｂ７／２４－Ｈ０４Ｂ７／２６
Ｈ０４Ｍ１１／００