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

特許第6471039号
(P6471039)

(45)発行日　平成31年2月13日(2019.2.13)　(24)登録日　平成31年1月25日(2019.1.25)

(51)Int.Cl.		F I	
H04W 12/06	(2009.01)	H04W	12/06
H04W 12/04	(2009.01)	H04W	12/04
H04W 84/12	(2009.01)	H04W	84/12
H04W 92/18	(2009.01)	H04W	92/18

請求項の数 10　(全 28 頁)

(21)出願番号　特願2015-101181(P2015-101181)
(22)出願日　平成27年5月18日(2015.5.18)
(65)公開番号　特開2016-219955(P2016-219955A)
(43)公開日　平成28年12月22日(2016.12.22)
審査請求日　平成30年2月7日(2018.2.7)

(73)特許権者　392026693
株式会社ＮＴＴドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100125689
弁理士　大林　章
(74)代理人　100128598
弁理士　高田　聖一
(74)代理人　100121108
弁理士　高橋　太朗
(72)発明者　森岡　康史
東京都千代田区永田町二丁目１１番１号
株式会社ＮＴＴドコモ内
(72)発明者　森広　芳文
東京都千代田区永田町二丁目１１番１号
株式会社ＮＴＴドコモ内

最終頁に続く

(54)【発明の名称】無線通信システムおよび無線端末

(57)【特許請求の範囲】
【請求項１】
移動体通信網における加入者識別情報を有する第１無線端末と、
前記移動体通信網における加入者識別情報を有さない第２無線端末と
を含む複数の無線端末と、
前記第１無線端末と前記移動体通信網との通信を中継するアクセスポイントと、
前記移動体通信網における加入者識別情報を有する無線端末を認証する認証装置と
を備え、
前記第２無線端末は、
前記第１無線端末との通信を実行する第２端末通信部と、
前記第２無線端末が前記アクセスポイントへ接続するために用いる認証情報を前記第１無線端末が代理で取得するよう要求する第１認証要求を、前記第２端末通信部を通じて前記第１無線端末へ送信する代理認証要求部とを備え、
前記第１無線端末は、
前記第２無線端末との通信を実行する第１端末通信部と、
前記第１認証要求を受信すると、前記認証装置に対し、前記認証情報を、前記加入者識別情報を用いて要求する認証情報要求部と、
前記認証情報要求部の要求に応じて取得された前記認証情報を、前記第１端末通信部を通じて前記第２無線端末へ送信する認証情報送信部と
を備える

無線通信システム。
【請求項２】
前記第１無線端末は、
前記第１無線端末の前記加入者識別情報と対応する加入者登録情報を有し、
前記移動体通信網は、
前記認証装置と
前記第１無線端末の前記加入者識別情報と前記第１無線端末の前記加入者登録情報とを対応付けて記憶する加入者情報管理装置とを備え、
前記加入者情報管理装置は、
前記加入者識別情報に対応する、前記加入者識別情報を有する前記第１無線端末を認証するための情報であり、マスター鍵の生成に用いられる鍵情報を含む認証用パラメタを、前記加入者登録情報を用いて生成し、
前記第１無線端末の前記認証情報要求部は、
前記代理認証要求部から受信した前記第１認証要求に応じて、前記第１無線端末の前記加入者識別情報を搭載し、当該加入者識別情報を有する当該第１無線端末を認証するよう要求する第２認証要求を、前記アクセスポイントを介して前記認証装置へ送信し、
前記認証装置は、
前記第２認証要求に搭載された前記加入者識別情報に対応する前記認証用パラメタを前記加入者情報管理装置から取得する認証用パラメタ取得部と、
前記加入者情報管理装置から取得した前記認証用パラメタに含まれる前記鍵情報を用いて、アクセスポイントマスター鍵を生成するマスター鍵生成部と、
前記アクセスポイントマスター鍵を用いて生成した第１メッセージ認証コードを含むチャレンジメッセージを、前記アクセスポイントを介して前記第１無線端末へ送信するチャレンジ送信部とを備え、
前記第１無線端末はさらに、
前記第１無線端末が有する前記加入者登録情報に基づいて、前記アクセスポイントマスター鍵と一致する端末マスター鍵を生成するマスター鍵生成部と、
前記端末マスター鍵を記憶する記憶部と、
前記チャレンジメッセージを受信した後、前記端末マスター鍵を用いて生成した第２メッセージ認証コードを含むレスポンスメッセージを、前記アクセスポイントを介して前記認証装置へ送信するレスポンス送信部とを備え、
前記認証装置はさらに、
前記アクセスポイントマスター鍵を前記アクセスポイントへ送信するマスター鍵送信部を備え、
前記アクセスポイントは、
受信した前記アクセスポイントマスター鍵を記憶する記憶部を備え、
前記第１無線端末はさらに、
当該第１無線端末の前記記憶部に記憶された前記端末マスター鍵を用いて、端末一時鍵を生成する一時鍵生成部を備え、
前記アクセスポイントはさらに、
当該アクセスポイントの前記記憶部に記憶された前記アクセスポイントマスター鍵を用いて、前記端末一時鍵と一致するアクセスポイント一時鍵を生成する一時鍵生成部を備え、
前記第１無線端末の前記認証情報送信部は、
前記端末一時鍵を前記認証情報として前記第２無線端末へ送信する
請求項１の無線通信システム。
【請求項３】
前記第１無線端末は、
前記第１無線端末の前記加入者識別情報と対応する加入者登録情報を有し、
前記移動体通信網は、

前記認証装置と
前記第１無線端末の前記加入者識別情報と前記第１無線端末の前記加入者登録情報とを対応付けて記憶する加入者情報管理装置とを備え、
前記加入者情報管理装置は、
前記加入者識別情報に対応する、前記加入者識別情報を有する前記第１無線端末を認証するための情報であり、マスター鍵の生成に用いられる鍵情報を含む認証用パラメタを、前記加入者登録情報を用いて生成し、
前記第１無線端末の前記認証情報要求部は、
前記代理認証要求部から受信した前記第１認証要求に応じて、前記第１無線端末の前記加入者識別情報を搭載し、当該加入者識別情報を有する当該第１無線端末を認証するよう要求する第２認証要求を、前記アクセスポイントを介して前記認証装置へ送信し、
前記認証装置は、
前記第２認証要求に搭載された前記加入者識別情報に対応する前記認証用パラメタを前記加入者情報管理装置から取得する認証用パラメタ取得部と、
前記加入者情報管理装置から取得した前記認証用パラメタに含まれる前記鍵情報を用いて、アクセスポイントマスター鍵を生成するマスター鍵生成部と、
前記アクセスポイントマスター鍵を用いて生成した第１メッセージ認証コードを含むチャレンジメッセージを、前記アクセスポイントを介して前記第１無線端末へ送信するチャレンジ送信部とを備え、
前記第１無線端末はさらに、
前記第１無線端末が有する前記加入者登録情報に基づいて、前記アクセスポイントマスター鍵と一致する端末マスター鍵を生成するマスター鍵生成部と、
前記端末マスター鍵を記憶する記憶部と、
前記チャレンジメッセージを受信した後、前記端末マスター鍵を用いて生成した第２メッセージ認証コードを含むレスポンスメッセージを、前記アクセスポイントを介して前記認証装置へ送信するレスポンス送信部とを備え、
前記認証装置はさらに、
前記アクセスポイントマスター鍵を前記アクセスポイントへ送信するマスター鍵送信部を備え、
前記アクセスポイントは、
受信した前記アクセスポイントマスター鍵を記憶する記憶部を備え、
前記第１無線端末の前記認証情報送信部は、
前記端末マスター鍵を前記認証情報として前記第２無線端末へ送信し、
前記第２無線端末はさらに、
受信した前記端末マスター鍵を記憶する記憶部と、
当該第２無線端末の前記記憶部に記憶された前記端末マスター鍵を用いて、端末一時鍵を生成する一時鍵生成部とを備え、
前記アクセスポイントはさらに、
当該アクセスポイントの前記記憶部に記憶された前記アクセスポイントマスター鍵を用いて、前記端末一時鍵と一致するアクセスポイント一時鍵を生成する一時鍵生成部を備える
請求項１の無線通信システム。
【請求項４】
前記第１無線端末の前記一時鍵生成部は、
前記第１無線端末の前記記憶部に記憶された前記端末マスター鍵を用いて、間欠的に新たに端末一時鍵を生成し、
前記アクセスポイントの前記一時鍵生成部は、
前記アクセスポイントの前記記憶部に記憶された前記アクセスポイントマスター鍵を用いて、新たに生成された前記端末一時鍵と一致するアクセスポイント一時鍵を新たに生成し、

前記第１無線端末の前記認証情報送信部は、
端末一時鍵が新たに生成される度に、当該端末一時鍵を前記認証情報として前記第２無線端末へ送信する
請求項２の無線通信システム。
【請求項５】
前記第２端末通信部と前記第１端末通信部との間に確立される接続は、
前記第２無線端末が前記第１認証要求を送信してから、前記第２無線端末と前記アクセスポイントとの接続が切断されるまで維持される
請求項１から４のいずれかに記載の無線通信システム。
【請求項６】
前記第２端末通信部と前記第１端末通信部との間に確立される接続は、
前記第２無線端末が前記第１認証要求を送信してから、前記第１無線端末の前記認証情報送信部による、前記端末マスター鍵の前記第２無線端末への送信が完了するまで維持される
請求項３の無線通信システム。
【請求項７】
前記第２無線端末はさらに、
前記第１無線端末と前記第２無線端末との通信を暗号化するための端末間暗号鍵と、前記端末間暗号鍵で暗号化された通信を復号化するための端末間復号鍵とを生成する端末間鍵生成部と、
前記端末間暗号鍵を前記第１無線端末に送信する端末間鍵送信部とを備え、
前記第１無線端末はさらに、
前記認証情報要求部の要求に応じて取得された前記認証情報を、前記端末間鍵送信部から受信した前記端末間暗号鍵を用いて暗号化する端末間通信暗号化部を備え、
前記第１無線端末の前記認証情報送信部は、
前記端末間暗号鍵を用いて暗号化された前記認証情報を前記第２無線端末へ送信する
請求項１から６のいずれかに記載の無線通信システム。
【請求項８】
前記第１無線端末はさらに、
前記第１無線端末と前記第２無線端末との通信を暗号化するための第２端末間暗号鍵と、前記第２端末間暗号鍵で暗号化された通信を復号化するための第２端末間復号鍵とを生成する端末間鍵生成部と、
前記第２端末間暗号鍵を前記第２無線端末に送信する端末間鍵送信部とを備え、
前記第２無線端末はさらに、
受信した前記第２端末間暗号鍵で前記第１認証要求を暗号化する端末間通信暗号化部を備え、
前記代理認証要求部は、暗号化された前記第１認証要求を前記第１無線端末へ送信する
請求項７に記載の無線通信システム。
【請求項９】
移動体通信網における加入者識別情報を有する第１無線端末と、
前記移動体通信網における加入者識別情報を有さない第２無線端末と
を含む複数の無線端末と、
前記第１無線端末と前記移動体通信網との通信を中継するアクセスポイントと、
前記移動体通信網における加入者識別情報を有する無線端末を認証する認証装置と
を備える無線通信システムにおける前記第１無線端末であって、
前記第２無線端末との通信を実行する第１端末通信部と、
前記第２無線端末から、前記第２無線端末が前記アクセスポイントへ接続するために用いる認証情報を前記第１無線端末が代理で取得するよう要求する第１認証要求を受信した後、前記認証装置に対し、前記認証情報を、前記加入者識別情報を用いて要求する認証情報要求部と、

前記認証情報要求部の要求に応じて取得された前記認証情報を、前記第１端末通信部を通じて前記第２無線端末へ送信する認証情報送信部と
を備える
無線端末。
【請求項１０】
移動体通信網における加入者識別情報を有する第１無線端末と、
前記移動体通信網における加入者識別情報を有さない第２無線端末と
を含む複数の無線端末と、
前記第１無線端末と前記移動体通信網との通信を中継するアクセスポイントと、
前記移動体通信網における加入者識別情報を有する無線端末を認証する認証装置と
を備える無線通信システムにおける前記第２無線端末であって、
前記第１無線端末との通信を実行する第２端末通信部と、
前記第２無線端末が前記アクセスポイントへ接続するために用いる認証情報を前記第１無線端末が代理で取得するよう要求する第１認証要求を、前記第２端末通信部を通じて前記第１無線端末へ送信する代理認証要求部と
を備え、
前記第２端末通信部は、
前記第１認証要求に応じて前記第１無線端末が前記認証装置から取得し、送信する前記認証情報を受信する
無線端末。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信システムおよび無線端末に関する。
【背景技術】
【０００２】
現在、移動体通信網と無線LAN（Local Area Network）とのいずれを通じても通信を行える機能を持つ無線端末（例えば、スマートフォン）と、移動体通信網には接続しないが無線LANを通じて通信を行う機能を有する無線端末（例えば、タブレット端末、携帯ゲーム機）との両方を所持するユーザが存在する。一般的に、これらの無線端末が、移動体通信事業者が設置した公衆無線LANのアクセスポイントへ接続する場合、認証動作（ユーザ認証）が行われる。
【０００３】
認証方法には、SIM（subscriber identity module）を用いる方法（例えば、特許文献１）とSIMを用いない方法とが存在する。SIMは、スマートフォン等、移動体通信網を通じて通信が可能な無線端末に搭載されており、ユーザが移動体通信事業者と契約する際に割り当てられる固有の情報である加入者識別情報を含む。SIMを用いる認証方法には、例えばEAP-SIM、EAP-AKAがあり、SIMを用いない認証方法には、例えばWPA2-PSKがある。
【０００４】
SIMを用いる認証方法（以下、「SIM認証方法」と称する場合がある）では、無線端末のSIMの加入者識別情報に対応付けられた情報を用いて、当該無線端末とアクセスポイントとの通信を暗号化する暗号化鍵が生成される。一方、SIMを用いない認証方法（以下、「パスワード認証方法」と称する場合がある）では、事前にアクセスポイントに設定されたパスワードを用いて、当該アクセスポイントと無線端末との通信を暗号化する暗号化鍵が生成される。
【０００５】
不特定のユーザが利用するアクセスポイント（例えば、公衆無線LANのアクセスポイント）に設定されたパスワードは、そのアクセスポイントを利用する複数のユーザに共通する（複数のユーザが同じパスワードを使用する）。すなわち、無線端末がパスワード認証方法を用いた認証動作によりアクセスポイントに接続する場合、そのアクセスポイントと

無線端末との通信の暗号化には、その無線端末のユーザ以外にも知られている共有のパスワードを用いて生成される暗号化鍵が用いられる。そのため、無線端末のSIMに固有な加入者識別情報に対応付けられた情報を用いるSIM認証方法により生成された暗号化鍵に比べ、パスワード認証方法により作成された暗号化鍵は容易に特定される可能性がある。結果として、パスワード認証方法を用いた認証動作により接続したアクセスポイントと無線端末との通信は、SIM認証方法を用いた認証動作により接続したアクセスポイントと無線端末との通信よりも、機密性が損なわれる可能性が高いと理解される。

【０００６】

また、パスワード認証方法を用いてアクセスポイントに接続する場合、無線端末のユーザは、異なるSSID（service set ID）を持つアクセスポイントごとに、パスワードを手動で入力して認証動作を行う必要がある。一方、SIM認証方法を用いてアクセスポイントに接続する場合には、無線端末が有するSIMの情報を用いて認証動作が行われるため、無線端末のユーザはパスワードを入力する必要が無い。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開2014-155038号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

上述のように、パスワード認証方法に比べ、SIM認証方法は、高い安全性と利便性といった利点をユーザに提供し得る。しかし、タブレット端末等、SIMを有さない（すなわち、移動体通信網における加入者識別情報を有さない）無線端末は、SIM認証方法による認証動作を行うことができない。

【０００９】

本発明は、上記の課題に鑑みてなされたものであり、移動体通信網における加入者識別情報を有さない無線端末についても、加入者識別情報を用いる認証方法を使用できるようにすることを目的とする。

【課題を解決するための手段】

【００１０】

本発明の無線通信システムは、移動体通信網における加入者識別情報を有する第１無線端末と、前記移動体通信網における加入者識別情報を有さない第２無線端末とを含む複数の無線端末と、前記第１無線端末と前記移動体通信網との通信を中継するアクセスポイントとを備え、前記第２無線端末は、前記第１無線端末との通信を実行する第２端末通信部と、前記第２無線端末が前記アクセスポイントへ接続するために用いる認証情報を前記第１無線端末が代理で取得するよう要求する第１認証要求を、前記第２端末通信部を通じて前記第１無線端末へ送信する代理認証要求部とを備え、前記第１無線端末は、前記第２無線端末との通信を実行する第１端末通信部と、前記第１認証要求を受信すると、前記認証情報を、前記加入者識別情報を用いて要求する認証情報要求部と、前記認証情報要求部の要求に応じて取得された前記認証情報を、前記第１端末通信部を通じて前記第２無線端末へ送信する認証情報送信部とを備える。

【００１１】

本発明の無線端末は、移動体通信網における加入者識別情報を有する第１無線端末と、前記移動体通信網における加入者識別情報を有さない第２無線端末とを含む複数の無線端末と、前記第１無線端末と前記移動体通信網との通信を中継するアクセスポイントとを備える無線通信システムにおける前記第１無線端末であって、前記第２無線端末との通信を実行する第１端末通信部と、前記第２無線端末から、前記第２無線端末が前記アクセスポイントへ接続するために用いる認証情報を前記第１無線端末が代理で取得するよう要求する第１認証要求を受信した後、前記認証情報を、前記加入者識別情報を用いて要求する認証情報要求部と、前記認証情報要求部の要求に応じて取得された前記認証情報を、前記第

１端末通信部を通じて前記第２無線端末へ送信する認証情報送信部とを備える。
【００１２】
本発明の別の無線端末は、移動体通信網における加入者識別情報を有する第１無線端末と、前記移動体通信網における加入者識別情報を有さない第２無線端末とを含む複数の無線端末と、前記第１無線端末と前記移動体通信網との通信を中継するアクセスポイントとを備える無線通信システムにおける前記第２無線端末であって、前記第１無線端末との通信を実行する第２端末通信部と、前記第２無線端末が前記アクセスポイントへ接続するために用いる認証情報を前記第１無線端末が代理で取得するよう要求する第１認証要求を、前記第２端末通信部を通じて前記第１無線端末へ送信する代理認証要求部とを備え、前記第２端末通信部は、前記第１認証要求に応じて前記第１無線端末から送信される前記認証情報を受信する。
【発明の効果】
【００１３】
本発明によれば、移動体通信網における加入者識別情報を有さない無線端末についても、加入者識別情報を用いる認証方法を使用できる。
【図面の簡単な説明】
【００１４】
【図１】本発明の第１実施形態に係る無線通信システムの構成を示すブロック図である。
【図２】第１実施形態の代理認証動作の一例を示すフロー図である。
【図３】第１実施形態の代理認証動作の一例を示すフロー図である。
【図４】第１実施形態に係る第１無線端末の構成を示すブロック図である。
【図５】第１実施形態に係る第２無線端末の構成を示すブロック図である。
【図６】第１実施形態に係るアクセスポイントの構成を示すブロック図である。
【図７】第１実施形態に係る認証装置の構成を示すブロック図である。
【図８】第２実施形態の代理認証動作の一例を示すフロー図である。
【図９】第２実施形態の代理認証動作の一例を示すフロー図である。
【図１０】第２実施形態に係る第１無線端末の構成を示すブロック図である。
【図１１】第２実施形態に係る第２無線端末の構成を示すブロック図である。
【図１２】代理認証動作の変形例の一部を示すフロー図である。
【図１３】変形例に係る第１実施形態の第１無線端末の構成を示すブロック図である。
【図１４】変形例に係る第２実施形態の第１無線端末の構成を示すブロック図である。
【図１５】変形例に係る第１実施形態の第２無線端末の構成を示すブロック図である。
【図１６】変形例に係る第２実施形態の第２無線端末の構成を示すブロック図である。
【発明を実施するための形態】
【００１５】
以下、添付の図面を参照しながら本発明に係る様々な実施の形態を説明する。
【００１６】
１．第１実施形態
本実施形態では、移動体通信網ＭＮＷにおける加入者識別情報ＳＩＤを有する第１無線端末ＳＴＡ１が、加入者識別情報ＳＩＤを有さない第２無線端末ＳＴＡ２の代理として、自らの加入者識別情報ＳＩＤを用いて認証動作（ユーザ認証）を行う。第１無線端末ＳＴＡ１は、認証動作の結果として得た、アクセスポイントＡＰとの通信を暗号化する一時的な暗号化鍵である一時鍵ＰＴＫ（pairwise transient key）を、第２無線端末ＳＴＡ２へ送信する。
【００１７】
１－１．無線通信システムの構成
図１は、本発明の第１実施形態に係る無線通信システムＣＳの構成を示す。無線通信システムＣＳは、第１無線端末ＳＴＡ１と、第２無線端末ＳＴＡ２と、アクセスポイントＡＰと、認証装置ＡＡＡと、加入者情報管理装置ＨＳＳとを備える。また、移動体通信網ＭＮＷは、以上の要素のうち、認証装置ＡＡＡと加入者情報管理装置ＨＳＳとを備える。以

上の各要素は、無線通信システムＣＳ内にそれぞれ複数存在し得る。

【００１８】

第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とは、相互に無線通信が可能である。第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信には、所定の無線通信技術、例えば、Bluetooth（登録商標）、NFC（Near Field Communication）等が用いられる。

【００１９】

第１無線端末ＳＴＡ１は、移動体通信網ＭＮＷにおける加入者識別情報ＳＩＤと加入者識別情報ＳＩＤに対応付けられた加入者登録情報Ｋとを有する。第１無線端末ＳＴＡ１は、移動体通信網ＭＮＷ内の認証装置ＡＡＡに対して、加入者識別情報ＳＩＤを用いる認証方法で自端末を認証するよう、自らの加入者識別情報ＳＩＤを用いて要求することができる。

一方で、第２無線端末ＳＴＡ２は移動体通信網ＭＮＷにおける加入者識別情報ＳＩＤを有さない。そのため、第２無線端末ＳＴＡ２は、認証装置ＡＡＡに対し、加入者識別情報ＳＩＤを用いる認証方法で自端末を認証するよう要求することができない。

【００２０】

加入者情報管理装置ＨＳＳは、第１無線端末ＳＴＡ１の加入者識別情報ＳＩＤと加入者登録情報Ｋとを対応付けて記憶している。すなわち、第１無線端末ＳＴＡ１と加入者情報管理装置ＨＳＳとのそれぞれが、加入者識別情報ＳＩＤと加入者識別情報ＳＩＤに対応する加入者登録情報Ｋとを有している。

【００２１】

加入者情報管理装置ＨＳＳは、有線または無線にて認証装置ＡＡＡに接続される。認証装置ＡＡＡと加入者情報管理装置ＨＳＳとの通信と、認証装置ＡＡＡと第１無線端末ＳＴＡ１との通信とは、所定のアクセス技術（Radio Access Technology）、例えば３ＧＰＰ規格（Third Generation Partnership Project）に規定されるＬＴＥ／ＳＡＥ（Long Term Evolution / System Architecture Evolution）に従って実行される。

【００２２】

アクセスポイントＡＰは、認証装置ＡＡＡと、無線通信システムＣＳの外部ネットワークであるインターネットＩＮとに接続される。以上の接続の形態は有線でも無線でもよい。アクセスポイントＡＰは、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とのそれぞれと無線通信を実行する基地局として機能する。具体的に、アクセスポイントＡＰは、第１無線端末ＳＴＡ１と認証装置ＡＡＡとの通信と、第１無線端末ＳＴＡ１とインターネットＩＮとの通信とを中継する。また、アクセスポイントＡＰは、第２無線端末ＳＴＡ２とインターネットＩＮとの通信を中継する。

【００２３】

アクセスポイントＡＰと各無線端末（第１無線端末ＳＴＡ１、第２無線端末ＳＴＡ２）とは、所定の無線アクセス技術、例えば無線LAN規格（例えば、IEEE 802.11n、IEEE802.11ac）に従って無線通信を行う。以下では、アクセスポイントＡＰと各無線端末とが無線LAN規格に従って無線通信を行う形態を例示して説明するが、本発明の技術的範囲を限定する趣旨ではない。本発明は、必要な設計上の変形を施した上で、他の無線アクセス技術（例えば、IEEE 802.16-2004およびIEEE 802.16eに規定されるWiMAX）にも適用可能である。

【００２４】

１－２．代理認証動作

１－２－１．代理認証動作の概要

以下、図２および図３を参照して、本実施形態の代理認証動作の一例を説明する。なお、本明細書内において、「代理認証動作」とは、加入者識別情報ＳＩＤを有する第１無線端末ＳＴＡ１が、加入者識別情報ＳＩＤを有さない第２無線端末ＳＴＡ２の代理で、自らの加入者識別情報ＳＩＤを用いて認証動作を実行し、その結果として得られる認証情報（例えば、通信暗号化鍵）を第２無線端末ＳＴＡ２へ送信する一連の動作を指すものとする。

【００２５】
概略的には、アクセスポイントＡＰを介してインターネットＩＮとの通信を開始する第２無線端末ＳＴＡ２は、第１無線端末ＳＴＡ１に対し、第２無線端末ＳＴＡ２の代理として認証動作を実行するよう要求する。第２無線端末ＳＴＡ２の要求に応じて、第１無線端末ＳＴＡ１は自らの加入者識別情報ＳＩＤを用いて認証動作を行い、認証動作により生成される一時鍵ＰＴＫを第２無線端末ＳＴＡ２へ送信する。
【００２６】
以下の各実施形態では、無線端末とアクセスポイントＡＰとが共有するマスター鍵ＰＭＫ（pairwise master key）がEAP-AKAに従って生成され、無線端末とアクセスポイントＡＰとが共有する一時鍵ＰＴＫが４ウェイハンドシェイク（4-way handshake）に従って生成される様子を説明するが、本願の発明の技術的範囲を限定する意図ではない。必要な設計上の変形を施した上で、他の認証プロトコル（例えば、EAP-SIM）が使用されてもよい。
【００２７】
１－２－２．代理認証動作の一例
図２および図３は、代理認証動作の一例を示すフロー図である。図２および図３の例では、第１無線端末ＳＴＡ１と加入者情報管理装置ＨＳＳとのそれぞれが、予め第１無線端末ＳＴＡ１の加入者識別情報ＳＩＤと当該加入者識別情報ＳＩＤに対応する加入者登録情報Ｋとを有していると想定する。
【００２８】
第２無線端末ＳＴＡ２がアクセスポイントＡＰを介して外部ネットワークであるインターネットＩＮと通信を開始する場合、第２無線端末ＳＴＡ２はまず第１無線端末ＳＴＡ１との接続を確立する（S100）。第１無線端末ＳＴＡ１との接続を確立した後、第２無線端末ＳＴＡ２は、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信を暗号化する端末間暗号鍵ＴＥＫと、端末間暗号鍵ＴＥＫで暗号化された通信を復号化する端末間復号鍵ＴＤＫとを生成し（S110）、端末間暗号鍵ＴＥＫを第１無線端末ＳＴＡ１に送信する（S120）。
【００２９】
第２無線端末ＳＴＡ２は、当該第２無線端末ＳＴＡ２がアクセスポイントＡＰと接続および通信するために用いられる認証情報である一時鍵ＰＴＫを、第１無線端末ＳＴＡ１が代理で取得するよう要求する第１認証要求を、第１無線端末ＳＴＡ１へ送信する（S130）。第１認証要求には、第１認証要求を送信する無線端末ＳＴＡ（すなわち、第２無線端末ＳＴＡ２）の宛先情報（例えば、MACアドレス）が含まれてよい。
【００３０】
第１認証要求を受信した後、第１無線端末ＳＴＡ１は、マスター鍵ＰＭＫを生成する。マスター鍵ＰＭＫは、アクセスポイントＡＰと第１無線端末ＳＴＡ１との通信の暗号化に使用する通信暗号化鍵である一時鍵ＰＴＫに先立って生成される暗号化鍵であり、一時鍵ＰＴＫはマスター鍵ＰＭＫに基づいて生成される。以下にマスター鍵ＰＭＫ生成の手順（ステップS140からS230）を説明する。
【００３１】
第１認証要求を受信すると、第１無線端末ＳＴＡ１は、自らの加入者識別情報ＳＩＤを搭載した第２認証要求を、アクセスポイントＡＰを介して認証装置ＡＡＡへ送信する（S140）。第２認証要求は、搭載した加入者識別情報ＳＩＤを有する無線端末ＳＴＡ（すなわち、第１無線端末ＳＴＡ１）を認証装置ＡＡＡが認証するよう要求するメッセージである。
【００３２】
第２認証要求を受信すると、認証装置ＡＡＡは、認証用パラメタ要求メッセージを加入者情報管理装置ＨＳＳへ送信する（S150）。認証用パラメタ要求メッセージは、認証用パラメタを要求するメッセージであり、第２認証要求に搭載された加入者識別情報ＳＩＤを含む。認証用パラメタは、当該加入者識別情報ＳＩＤに対応する情報であり、当該加入者

識別情報ＳＩＤを有する無線端末ＳＴＡ（すなわち、第１無線端末ＳＴＡ１）を認証するための情報である。

【００３３】

認証用パラメタ要求メッセージを受信すると、加入者情報管理装置ＨＳＳは、認証用パラメタ要求メッセージに含まれる加入者識別情報ＳＩＤに対応する加入者登録情報Ｋを検索する。そして、当該加入者登録情報Ｋを用いて加入者識別情報ＳＩＤに対応する認証用パラメタを生成し（S160）、認証装置ＡＡＡへ送信する（S170）。認証用パラメタは、マスター鍵ＰＭＫの生成に用いられる鍵情報ＫＭと、第１無線端末ＳＴＡ１が移動体通信網ＭＮＷを検証するために用いられるネットワーク認証トークンＡＵＴＮと、認証装置ＡＡＡが第１無線端末ＳＴＡ１を検証するために用いられる端末検証用パラメタＸＲＥＳとを含む。

【００３４】

認証用パラメタを受信すると、認証装置ＡＡＡは、受信した認証用パラメタに含まれる鍵情報ＫＭを用いてアクセスポイントマスター鍵ＡＰＭＫを生成する（S180）。そして、アクセスポイントマスター鍵ＡＰＭＫを用いて生成した第１メッセージ認証コード（message authentication code）ＭＡＣ１と、ネットワーク認証トークンＡＵＴＮとを含むチャレンジメッセージを、アクセスポイントＡＰを介して第１無線端末ＳＴＡ１へ送信する（S190）。

【００３５】

チャレンジメッセージを受信すると、第１無線端末ＳＴＡ１はチャレンジメッセージに含まれるネットワーク認証トークンＡＵＴＮに基づき、通信している相手が正当な移動体通信網ＭＮＷであることを検証する。続いて、第１無線端末ＳＴＡ１は自らが有する加入者登録情報Ｋを用いて鍵情報ＫＭを生成し、鍵情報ＫＭを用いて端末マスター鍵ＳＰＭＫを生成する（S200）。そして、チャレンジメッセージに含まれる第１メッセージ認証コードＭＡＣ１に基づき、第１無線端末ＳＴＡ１が生成した端末マスター鍵ＳＰＭＫと認証装置ＡＡＡが生成したアクセスポイントマスター鍵ＡＰＭＫとが一致することを検証する。その後、第１無線端末ＳＴＡ１は、認証装置ＡＡＡが第１無線端末ＳＴＡ１を検証するために用いる端末検証用パラメタＲＥＳと、端末マスター鍵ＳＰＭＫを用いて生成した第２メッセージ認証コードＭＡＣ２とを含むレスポンスメッセージを、アクセスポイントＡＰを介して認証装置ＡＡＡへ送信する（S210）。端末検証用パラメタＲＥＳは、第１無線端末ＳＴＡ１が自らの加入者登録情報Ｋを用いて生成するパラメタである。

【００３６】

レスポンスメッセージを受信すると、認証装置ＡＡＡは、レスポンスメッセージに含まれる端末検証用パラメタＲＥＳと、加入者情報管理装置ＨＳＳから受信した認証用パラメタに含まれる端末検証用パラメタＸＲＥＳとに基づき、通信している相手が正当な第１無線端末ＳＴＡ１であることを検証する。また、レスポンスメッセージに含まれる第２メッセージ認証コードＭＡＣ２に基づき、第１無線端末ＳＴＡ１が生成した端末マスター鍵ＳＰＭＫと認証装置ＡＡＡが生成したアクセスポイントマスター鍵ＡＰＭＫとが一致することを検証する。これら、端末検証用パラメタＲＥＳと第２メッセージ認証コードＭＡＣ２との検証の後、認証装置ＡＡＡは、第１無線端末ＳＴＡ１を認証する判定を下し（S220）、アクセスポイントＡＰを介して、当該判定（認証成功）を第１無線端末ＳＴＡ１へ通知する（S230）。また、認証装置ＡＡＡは、アクセスポイントマスター鍵ＡＰＭＫをアクセスポイントＡＰへ送信する（S240）。

【００３７】

認証成功が通知された後、第１無線端末ＳＴＡ１は、アクセスポイントＡＰとの通信の暗号化に使用する通信暗号化鍵である一時鍵ＰＴＫを生成する。一時鍵ＰＴＫは、第１無線端末ＳＴＡ１とアクセスポイントＡＰとで共通のマスター鍵ＰＭＫ（端末マスター鍵ＳＰＭＫ、アクセスポイントマスター鍵ＡＰＭＫ）に基づいて生成される。以下に一時鍵ＰＴＫ生成の手順（ステップS250からS300）を説明する。

【００３８】

アクセスポイントマスター鍵ＡＰＭＫの受信後、アクセスポイントＡＰはアクセスポイント乱数ＡＮＯＮＣＥを生成し、アクセスポイント乱数ＡＮＯＮＣＥを含む第１メッセージフレームを第１無線端末ＳＴＡ１へ送信する（S250）。

【００３９】

第１メッセージフレームの受信後、第１無線端末ＳＴＡ１は、端末乱数ＳＮＯＮＣＥを生成する。そして、端末乱数ＳＮＯＮＣＥと、受信した第１メッセージフレームに含まれるアクセスポイント乱数ＡＮＯＮＣＥと、端末マスター鍵ＳＰＭＫとに基づいて、端末一時鍵ＳＰＴＫを生成する（S260）。続いて、端末一時鍵ＳＰＴＫに基づいて生成した第１メッセージ完全性コード（message integrity code）ＭＩＣ１と、端末乱数ＳＮＯＮＣＥとを含む第２メッセージフレームをアクセスポイントＡＰへ送信する（S270）。

【００４０】

第２メッセージフレームは、第１無線端末ＳＴＡ１が生成した端末一時鍵ＳＰＴＫと、アクセスポイントＡＰが第２メッセージフレームに基づいて生成する一時鍵ＰＴＫとが、第１無線端末ＳＴＡ１が代理する無線端末ＳＴＡ（すなわち、第２無線端末ＳＴＡ２）との通信に用いられることをアクセスポイントＡＰに知らせる端末情報通知を含む。端末情報通知には、第２無線端末ＳＴＡ２の宛先情報（例えば、第２無線端末ＳＴＡ２のMACアドレス）が含まれる。

【００４１】

第２メッセージフレームを受信すると、アクセスポイントＡＰは第２メッセージフレームに含まれる端末乱数ＳＮＯＮＣＥと、アクセスポイント乱数ＡＮＯＮＣＥと、アクセスポイントマスター鍵ＡＰＭＫとに基づいて、アクセスポイント一時鍵ＡＰＴＫを生成する（S280）。そして、端末一時鍵ＳＰＴＫに基づいて生成された第１メッセージ完全性コードＭＩＣ１と一致するメッセージ完全性コードＭＩＣを、アクセスポイントＡＰが生成したアクセスポイント一時鍵ＡＰＴＫを用いて生成できることを検証する。その後、アクセスポイントＡＰは、アクセスポイント一時鍵ＡＰＴＫに基づいて生成した第２メッセージ完全性コードＭＩＣ２を含む第３メッセージフレームを第１無線端末ＳＴＡ１へ送信する（S290）。

【００４２】

第３メッセージフレームを受信すると、第１無線端末ＳＴＡ１は、アクセスポイント一時鍵ＡＰＴＫに基づいて生成された第２メッセージ完全性コードＭＩＣ２と一致するメッセージ完全性コードＭＩＣを、第１無線端末ＳＴＡ１が生成した端末一時鍵ＳＰＴＫを用いて生成できることを検証する。その後、端末一時鍵ＳＰＴＫに基づいて生成した第３メッセージ完全性コードＭＩＣ３を含む第４メッセージフレームが第１無線端末ＳＴＡ１からアクセスポイントＡＰへ送信される（S300）。

【００４３】

第４メッセージフレームの受信後、アクセスポイントＡＰは上述と同様の手順で第４メッセージフレームに含まれる第３メッセージ完全性コードＭＩＣ３を検証する。その後、アクセスポイントＡＰは、端末情報通知により通知された無線端末ＳＴＡ（すなわち、第２無線端末ＳＴＡ２）との通信に、アクセスポイント一時鍵ＡＰＴＫを使用するよう、自身を設定する。

【００４４】

第４メッセージフレームをアクセスポイントＡＰへ送信後、第１無線端末ＳＴＡ１は、生成した端末一時鍵ＳＰＴＫを、ステップS120で第２無線端末ＳＴＡ２から受信した端末間暗号鍵ＴＥＫで暗号化し、第２無線端末ＳＴＡ２へ送信する（S310）。なお、端末一時鍵ＳＰＴＫは、端末情報通知の送信後に送信されればよく、第４メッセージフレームの送信前に送信されてもよい。

【００４５】

暗号化された端末一時鍵ＳＰＴＫを第１無線端末ＳＴＡ１から受信した後、第２無線端末ＳＴＡ２はステップS110で生成した端末間復号鍵ＴＤＫを用いて復号化し、端末一時鍵ＳＰＴＫを用いてアクセスポイントＡＰへ接続し、通信を開始する（S320）。

【００４６】
第２無線端末ＳＴＡ２とアクセスポイントＡＰとの接続が維持されている間、アクセスポイントＡＰと第１無線端末ＳＴＡ１とは間欠的に上述の共通一時鍵ＰＴＫ生成手順（S250からS300）を実行する（S330からS380）。なお、端末情報通知は、共通一時鍵ＰＴＫ生成手順が実行される度に送信されて（ステップS270およびS350の第２メッセージフレームに含まれて）もよいし、初回の共通一時鍵ＰＴＫ生成手順のみで送信されて（ステップS270の第２メッセージフレームのみに含まれて）もよい。
【００４７】
端末一時鍵ＳＰＴＫが新たに生成される度に、第１無線端末ＳＴＡ１は新たな端末一時鍵ＳＰＴＫを端末間暗号鍵ＴＥＫで暗号化して第２無線端末ＳＴＡ２へ送信する（S390）。すなわち、第２無線端末ＳＴＡ２が第１認証要求を送信した後（S130）、第２無線端末ＳＴＡ２とアクセスポイントＡＰとの接続が切断されるまで、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との接続は維持される。
【００４８】
第２無線端末ＳＴＡ２とアクセスポイントＡＰとの接続が切断された後（S400）、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との接続が切断される（S410）。
【００４９】
以上に説明した代理認証動作によれば、移動体通信網ＭＮＷにおける加入者識別情報ＳＩＤを有さない第２無線端末ＳＴＡ２についても、加入者識別情報ＳＩＤを用いる認証方法を適用し得る。
【００５０】
１－３．各要素の構成
１－３－１．第１無線端末の構成
図４は、第１実施形態に係る第１無線端末ＳＴＡ１の構成を示すブロック図である。第１無線端末ＳＴＡ１は、無線通信部１１０と、端末通信部１２０と、記憶部１３０と、制御部１４０とを備える。なお、音声及び映像等を出力する出力装置およびユーザからの指示を受け付ける入力装置等の図示は、便宜的に省略されている。
【００５１】
無線通信部１１０は、アクセスポイントＡＰと無線通信を実行するための要素であり、無線信号を受信する受信回路と無線信号を送信する送信回路とを含む。端末通信部１２０は、第２無線端末ＳＴＡ２と無線通信を実行するための要素であり、無線信号を受信する受信回路と無線信号を送信する送信回路とを含む。なお、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とがWi-Fi Direct等の無線LAN規格に従って無線通信を行う場合、第１無線端末ＳＴＡ１は端末通信部１２０を含まずに無線通信部１１０によって第２無線端末ＳＴＡ２との無線通信を行ってもよい。
【００５２】
記憶部１３０は、第１無線端末ＳＴＡ１の制御に関連するコンピュータプログラムと認証動作に関わる情報（例えば、端末マスター鍵ＳＰＭＫ、端末間暗号鍵ＴＥＫ）とを格納する。制御部１４０は、認証情報要求部１４２と、マスター鍵生成部１４４と、レスポンス送信部１４６と、端末乱数生成部１４８と、一時鍵生成部１５０と、フレーム送信部１５２と、端末間通信暗号化部１５４と、認証情報送信部１５６とを要素として含む。
【００５３】
認証情報要求部１４２は、第２無線端末ＳＴＡ２から第１認証要求を受信すると、アクセスポイントＡＰへ接続するために用いる認証情報を第１無線端末ＳＴＡ１が有する加入者識別情報ＳＩＤを用いて要求する要素であり、アクセスポイントＡＰを介して、第２認証要求を認証装置ＡＡＡへ送信する。マスター鍵生成部１４４は、加入者登録情報Ｋに基づいて、端末マスター鍵ＳＰＭＫを生成する。レスポンス送信部１４６は、チャレンジメッセージを受信した後、第２メッセージ認証コードＭＡＣ２等を含むレスポンスメッセージを認証装置ＡＡＡへ送信する。端末乱数生成部１４８は、端末乱数ＳＮＯＮＣＥを生成する。一時鍵生成部１５０は、アクセスポイント乱数ＡＮＯＮＣＥと端末乱数ＳＮＯＮＣ

Ｅと端末マスター鍵ＳＰＭＫとに基づいて、端末一時鍵ＳＰＴＫを生成する。フレーム送信部１５２は、メッセージフレーム（第２メッセージフレーム、第４メッセージフレーム）をアクセスポイントＡＰへ送信する。端末間通信暗号化部１５４は、端末間暗号鍵ＴＥＫを用いて、第２無線端末ＳＴＡ２へ送信する端末一時鍵ＳＰＴＫを暗号化する。認証情報送信部１５６は、端末通信部１２０を通じて、暗号化された端末一時鍵ＳＰＴＫを第２無線端末ＳＴＡ２へ送信する。

【００５４】

制御部１４０および制御部１４０に含まれる各要素は、第１無線端末ＳＴＡ１内の不図示のCPU（Central Processing Unit）が、記憶部１３０に記憶されたコンピュータプログラムを実行し、そのコンピュータプログラムに従って機能することにより実現される機能ブロックである。

【００５５】

１－３－２．第２無線端末の構成

図５は、第１実施形態に係る第２無線端末ＳＴＡ２の構成を示すブロック図である。第２無線端末ＳＴＡ２は、無線通信部２１０と、端末通信部２２０と、記憶部２３０と、制御部２４０とを備える。なお、音声及び映像等を出力する出力装置およびユーザからの指示を受け付ける入力装置等の図示は、便宜的に省略されている。

【００５６】

無線通信部２１０は、アクセスポイントＡＰと無線通信を実行するための要素であり、第１無線端末ＳＴＡ１の無線通信部１１０と同様の構成を有する。端末通信部２２０は、第２無線端末ＳＴＡ２と無線通信を実行するための要素であり、第１無線端末ＳＴＡ１の端末通信部１２０と同様の構成を有する。なお、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とがWi-Fi Direct等の無線LAN規格に従って無線通信を行う場合、第２無線端末ＳＴＡ２は端末通信部２２０を含まずに無線通信部２１０によって第１無線端末ＳＴＡ１との無線通信を行ってもよい。

【００５７】

記憶部２３０は、第２無線端末ＳＴＡ２の制御に関連するコンピュータプログラムと認証に関わる情報（例えば、端末一時鍵ＳＰＴＫ、端末間復号鍵ＴＤＫ）とを格納する。制御部２４０は、代理認証要求部２４２と、端末間鍵生成部２５０と、端末間鍵送信部２５２とを要素として含む。

【００５８】

代理認証要求部２４２は、端末通信部２２０を通じて、第１認証要求を第１無線端末ＳＴＡ１へ送信する。端末間鍵生成部２５０は、端末間暗号鍵ＴＥＫと端末間復号鍵ＴＤＫとを生成する。端末間鍵送信部２５２は、端末間鍵生成部２５０が生成した端末間暗号鍵ＴＥＫを第１無線端末ＳＴＡ１へ送信する。

【００５９】

制御部２４０および制御部２４０に含まれる各要素は、第２無線端末ＳＴＡ２内の不図示のCPUが、記憶部２３０に記憶されたコンピュータプログラムを実行し、そのコンピュータプログラムに従って機能することにより実現される機能ブロックである。

【００６０】

１－３－３．アクセスポイントの構成

図６は、第１実施形態に係るアクセスポイントＡＰの構成を示すブロック図である。アクセスポイントＡＰは、無線通信部３１０と、ネットワーク通信部３２０と、外部ネットワーク通信部３３０と、記憶部３４０と、制御部３５０とを備える。

【００６１】

無線通信部３１０は、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とのそれぞれと無線通信を実行するための要素であり、無線信号を受信する受信回路と無線信号を送信する送信回路とを含む。ネットワーク通信部３２０は、認証装置ＡＡＡと通信を実行するための要素であり、有線または無線で電気信号を送受信する。外部ネットワーク通信部３３０は、インターネットＩＮと通信を実行するための要素であり、有線または無線で電気信号

を送受信する。また、外部ネットワーク通信部３３０は必要に応じて信号のプロトコル変換を実行する。記憶部３４０はアクセスポイントＡＰの制御に関連するコンピュータプログラムと認証に関わる情報（例えば、アクセスポイントマスター鍵ＡＰＭＫ）とを格納する。制御部３５０は、アクセスポイント乱数生成部３５２と、フレーム送信部３５４と、一時鍵生成部３５６とを備える。

【００６２】

アクセスポイント乱数生成部３５２は、アクセスポイント乱数ＡＮＯＮＣＥを生成する。フレーム送信部３５４は、メッセージフレーム（第１メッセージフレーム、第３メッセージフレーム）を第１無線端末ＳＴＡ１へ送信する。一時鍵生成部３５６は、アクセスポイント乱数ＡＮＯＮＣＥと端末乱数ＳＮＯＮＣＥとアクセスポイントマスター鍵ＡＰＭＫとに基づいて、アクセスポイント一時鍵ＡＰＴＫを生成する。

【００６３】

制御部３５０および制御部３５０に含まれる各要素は、アクセスポイントＡＰ内の不図示のCPUが、記憶部３４０に記憶されたコンピュータプログラムを実行し、そのコンピュータプログラムに従って機能することにより実現される機能ブロックである。

【００６４】

１－３－４．認証装置の構成

図７は、第１実施形態に係る認証装置ＡＡＡの構成を示すブロック図である。認証装置ＡＡＡは、ネットワーク通信部４１０と、記憶部４２０と、制御部４３０とを備える。

【００６５】

ネットワーク通信部４１０は、加入者情報管理装置ＨＳＳおよびアクセスポイントＡＰと通信を実行するための要素であり、アクセスポイントＡＰのネットワーク通信部３２０と同様の構成を有する。記憶部４２０は認証装置ＡＡＡの制御に関連するコンピュータプログラムと認証動作に関わる情報（例えば、認証用パラメタ）とを格納する。制御部４３０は、認証用パラメタ取得部４３２と、マスター鍵生成部４３４と、チャレンジ送信部４３６と、認証判定部４３８と、判定結果通知部４４０と、マスター鍵送信部４４２とを備える。

【００６６】

認証用パラメタ取得部４３２は、第２認証要求に含まれる加入者識別情報ＳＩＤに対応する認証用パラメタを、加入者情報管理装置ＨＳＳから取得する要素であり、認証用パラメタ要求メッセージを送信する。マスター鍵生成部４３４は、取得した認証用パラメタに含まれる情報を用いて、アクセスポイントマスター鍵ＡＰＭＫを生成する。チャレンジ送信部４３６は、第１メッセージ認証コードＭＡＣ１等を含むチャレンジメッセージを第１無線端末ＳＴＡ１へ送信する。認証判定部４３８は、第１無線端末ＳＴＡ１から受信したレスポンスメッセージに含まれる情報に基づき、第１無線端末ＳＴＡ１を認証する判定を下す。判定結果通知部４４０は、認証判定部４３８が下した判定（例えば、認証成功）を、アクセスポイントＡＰを介して第１無線端末ＳＴＡ１へ通知する。マスター鍵送信部４４２は、マスター鍵生成部４３４が生成したアクセスポイントマスター鍵ＡＰＭＫをアクセスポイントＡＰへ送信する。

【００６７】

制御部４３０および制御部４３０に含まれる各要素は、認証装置ＡＡＡ内の不図示のCPUが、記憶部４２０に記憶されたコンピュータプログラムを実行し、そのコンピュータプログラムに従って機能することにより実現される機能ブロックである。

【００６８】

１－４．本実施形態の効果

以上の構成によれば、移動体通信網ＭＮＷにおける加入者識別情報ＳＩＤを有さない第２無線端末ＳＴＡ２についても、加入者識別情報ＳＩＤを用いる認証方法を使用し得る。具体的に、第２無線端末ＳＴＡ２は、加入者識別情報ＳＩＤを用いる認証方法による認証動作で生成される認証情報である通信暗号化鍵（一時鍵ＰＴＫ）を用いて、アクセスポイントＡＰとの通信を暗号化し得る。上述のように、加入者識別情報ＳＩＤを用いる認証方

法により生成された通信暗号化鍵は、加入者識別情報ＳＩＤを用いない認証方法により生成された通信暗号化鍵よりも、より特定されにくい場合があると理解される。したがって、本実施形態の例では、加入者識別情報ＳＩＤを用いない認証方法による認証動作を行ってアクセスポイントＡＰに接続する構成に比べ、第２無線端末ＳＴＡ２とアクセスポイントＡＰとがより機密性の高い通信を実行し得る。

【００６９】

さらに、以上の構成によれば、第１無線端末ＳＴＡ１が有する加入者識別情報ＳＩＤを用いて認証動作が実行されるため、第２無線端末ＳＴＡ２のユーザはパスワード等の認証情報を入力する必要がない。そのため、第２無線端末ＳＴＡ２のユーザがより容易にアクセスポイントＡＰへ接続し得る。

【００７０】

２．第２実施形態

本発明の第２実施形態を以下に説明する。以下に例示する各実施形態において、作用、機能が第１実施形態と同等である要素については、以上の説明で参照した符号を流用して各々の説明を適宜に省略する。

【００７１】

２－１．代理認証動作の一例

第１実施形態では、一時鍵ＰＴＫ（端末一時鍵ＳＰＴＫ）が第１無線端末ＳＴＡ１から第２無線端末ＳＴＡ２へ送信される。第２実施形態では、マスター鍵ＰＭＫが第１無線端末ＳＴＡ１から第２無線端末ＳＴＡ２へ送信される。

【００７２】

図８および図９を参照して、本実施形態の代理認証動作の一例を説明する。この例では、第１実施形態（図２および図３）と同様、第１無線端末ＳＴＡ１と加入者情報管理装置ＨＳＳとのそれぞれが、予め第１無線端末ＳＴＡ１の加入者識別情報ＳＩＤと当該加入者識別情報ＳＩＤに対応する加入者登録情報Ｋとを有していると想定する。

【００７３】

第２無線端末ＳＴＡ２による第１無線端末ＳＴＡ１との接続の確立（S500）から、認証装置ＡＡＡからアクセスポイントＡＰへのアクセスポイントマスター鍵ＡＰＭＫの送信（S640）は、第１実施形態のステップS100からS240までと同様であるから、説明を省略する。

【００７４】

第１無線端末ＳＴＡ１の認証成功が認証装置ＡＡＡから通知された後（S630）、第１無線端末ＳＴＡ１は、第１無線端末ＳＴＡ１とアクセスポイントＡＰとがそれぞれ生成したマスター鍵ＰＭＫ（端末マスター鍵ＳＰＭＫ、アクセスポイントマスター鍵ＡＰＭＫ）が、第１無線端末ＳＴＡ１が代理する無線端末ＳＴＡ（すなわち、第２無線端末ＳＴＡ２）との通信に用いられることを知らせる端末情報通知をアクセスポイントＡＰへ送信する（S650）。端末情報通知には、第２無線端末ＳＴＡ２の宛先情報（例えば、第２無線端末ＳＴＡ２のMACアドレス）が含まれる。その後、第１無線端末ＳＴＡ１は、ステップS520で第２無線端末ＳＴＡ２から受信した端末間暗号鍵ＴＥＫで端末マスター鍵ＳＰＭＫを暗号化し、第２無線端末ＳＴＡ２へ送信する（S660）。送信が完了した後、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との接続が切断される（S670）。

【００７５】

アクセスポイントマスター鍵ＡＰＭＫの受信後、アクセスポイントＡＰはアクセスポイント乱数ＡＮＯＮＣＥを生成し、アクセスポイント乱数ＡＮＯＮＣＥを含む第１メッセージフレームを、端末情報通知により通知された無線端末ＳＴＡ（すなわち、第２無線端末ＳＴＡ２）へ送信する（S680）。

【００７６】

第１メッセージフレームの受信後、第２無線端末ＳＴＡ２は、端末乱数ＳＮＯＮＣＥを生成する。そして、端末乱数ＳＮＯＮＣＥと、受信した第１メッセージフレームに含まれるアクセスポイント乱数ＡＮＯＮＣＥと、ステップS510で生成した端末間復号鍵ＴＤＫを

用いて復号化された端末マスター鍵ＳＰＭＫとに基づいて、端末一時鍵ＳＰＴＫを生成する（S690）。続いて、第２無線端末ＳＴＡ２は、端末一時鍵ＳＰＴＫに基づいて生成した第１メッセージ完全性コード（message integrity code）ＭＩＣ１と、端末乱数ＳＮＯＮＣＥとを含む第２メッセージフレームをアクセスポイントＡＰへ送信する（S700）。

【００７７】

第２メッセージフレームを受信すると、アクセスポイントＡＰは、第２メッセージフレームに含まれる端末乱数ＳＮＯＮＣＥと、アクセスポイント乱数ＡＮＯＮＣＥと、アクセスポイントマスター鍵ＡＰＭＫとに基づいて、アクセスポイント一時鍵ＡＰＴＫを生成する（S710）。そして、端末一時鍵ＳＰＴＫに基づいて生成された第１メッセージ完全性コードＭＩＣ１と一致するメッセージ完全性コードＭＩＣを、アクセスポイントＡＰが生成したアクセスポイント一時鍵ＡＰＴＫを用いて生成できることを検証する。その後、アクセスポイントＡＰは、アクセスポイント一時鍵ＡＰＴＫに基づいて生成した第２メッセージ完全性コードＭＩＣ２を含む第３メッセージフレームを第２無線端末ＳＴＡ２へ送信する（S720）。

【００７８】

第３メッセージフレームを受信すると、第２無線端末ＳＴＡ２は、アクセスポイント一時鍵ＡＰＴＫに基づいて生成された第２メッセージ完全性コードＭＩＣ２と一致するメッセージ完全性コードＭＩＣを、第２無線端末ＳＴＡ２が生成した端末一時鍵ＳＰＴＫを用いて生成できることを検証する。その後、第２無線端末ＳＴＡ２は、端末一時鍵ＳＰＴＫに基づいて生成した第３メッセージ完全性コードＭＩＣ３を含む第４メッセージフレームを第２無線端末ＳＴＡ２はアクセスポイントＡＰへ送信する（S730）。

【００７９】

第４メッセージフレームの受信後、アクセスポイントＡＰは上述と同様の手順で第４メッセージフレームに含まれる第３メッセージ完全性コードＭＩＣ３を検証する。その後、アクセスポイントＡＰは、第２無線端末ＳＴＡ２との通信にアクセスポイント一時鍵ＡＰＴＫを使用するよう、自身を設定する。

【００８０】

第４メッセージフレームをアクセスポイントＡＰへ送信後、第２無線端末ＳＴＡ２は、生成した端末一時鍵ＳＰＴＫを用いてアクセスポイントＡＰへ接続し、通信を開始する（S740）。

【００８１】

第２無線端末ＳＴＡ２がアクセスポイントＡＰと接続した後、第２無線端末ＳＴＡ２とアクセスポイントＡＰとの接続が切断される（S810）までの間（すなわち、第２無線端末ＳＴＡ２とアクセスポイントＡＰとの接続が維持されている間）、アクセスポイントＡＰと第２無線端末ＳＴＡ２とは間欠的に上述の共通一時鍵ＰＴＫ生成手順（S680からS730）を実行する（S750からS800）。

【００８２】

なお、本実施形態では、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との接続が、端末マスター鍵ＳＰＭＫの送信（S660）後に切断される（S670）例を示す。しかし、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との接続は、第１認証要求の送信（S530）から端末マスター鍵ＳＰＭＫの送信完了（S660）まで維持されればよく、例示したタイミング以外で切断されてもよい。例えば、第１実施形態（S410）と同様に、第２無線端末ＳＴＡ２とアクセスポイントＡＰとの接続が切断（S810）された後に、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との接続が切断されてもよい。

【００８３】

以上に説明した代理認証動作によれば、移動体通信網ＭＮＷにおける加入者識別情報ＳＩＤを有さない第２無線端末ＳＴＡ２についても、加入者識別情報ＳＩＤを用いる認証方法を適用し得る。

【００８４】

２－２．各要素の構成

２－２－１．第１無線端末の構成

図１０は、第２実施形態に係る第１無線端末ＳＴＡ１の構成を示すブロック図である。第１無線端末ＳＴＡ１は、無線通信部１１０と、端末通信部１２０と、記憶部１３０と、制御部１４０とを備える。なお、音声及び映像等を出力する出力装置およびユーザからの指示を受け付ける入力装置等の図示は、便宜的に省略されている。

【００８５】

無線通信部１１０と端末通信部１２０とは、それぞれ第１実施形態の第１無線端末ＳＴＡ１が有する無線通信部１１０と端末通信部１２０と同様の構成を有するため、説明を省略する。

【００８６】

記憶部１３０は、第１無線端末ＳＴＡ１の制御に関連するコンピュータプログラムと認証動作に関わる情報（例えば、端末マスター鍵ＳＰＭＫ、端末間暗号鍵ＴＥＫ）とを格納する。制御部１４０は、認証情報要求部１４２と、マスター鍵生成部１４４と、レスポンス送信部１４６と、端末間通信暗号化部１５４と、認証情報送信部１５６とを要素として含む。

【００８７】

認証情報要求部１４２は、第２無線端末ＳＴＡ２から第１認証要求を受信すると、アクセスポイントＡＰへ接続するための認証情報を第１無線端末ＳＴＡ１が有する加入者識別情報ＳＩＤを用いて要求する要素であり、アクセスポイントＡＰを介して、第２認証要求を認証装置ＡＡＡへ送信する。マスター鍵生成部１４４は、加入者登録情報Ｋに基づいて、端末マスター鍵ＳＰＭＫを生成する。レスポンス送信部１４６は、チャレンジメッセージを受信した後、第２メッセージ認証コードＭＡＣ２等を含むレスポンスメッセージを認証装置ＡＡＡへ送信する。端末間通信暗号化部１５４は、端末間暗号鍵ＴＥＫを用いて、第２無線端末ＳＴＡ２へ送信する端末マスター鍵ＳＰＭＫを暗号化する。認証情報送信部１５６は、端末通信部１２０を通じて、暗号化された端末マスター鍵ＳＰＭＫを第２無線端末ＳＴＡ２へ送信する。

【００８８】

制御部１４０および制御部１４０に含まれる各要素は、第１無線端末ＳＴＡ１内の不図示のCPUが、記憶部１３０に記憶されたコンピュータプログラムを実行し、そのコンピュータプログラムに従って機能することにより実現される機能ブロックである。

【００８９】

２－２－２．第２無線端末の構成

図１１は、第２実施形態に係る第２無線端末ＳＴＡ２の構成の一例を示すブロック図である。第２無線端末ＳＴＡ２は、無線通信部２１０と、端末通信部２２０と、記憶部２３０と、制御部２４０とを備える。なお、音声及び映像等を出力する出力装置およびユーザからの指示を受け付ける入力装置等の図示は、便宜的に省略されている。

【００９０】

無線通信部２１０と端末通信部２２０とは、それぞれ第１実施形態の第２無線端末ＳＴＡ２が有する無線通信部２１０と端末通信部２２０と同様の構成を有するため、説明を省略する。

【００９１】

記憶部２３０は、第２無線端末ＳＴＡ２の制御に関連するコンピュータプログラムと認証に関わる情報（例えば、端末マスター鍵ＳＰＭＫ、端末間復号鍵ＴＤＫ）とを格納する。制御部２４０は、代理認証要求部２４２と、端末乱数生成部２４４と、一時鍵生成部２４６と、フレーム送信部２４８と、端末間鍵生成部２５０と、端末間鍵送信部２５２とを要素として含む。

【００９２】

代理認証要求部２４２は、端末通信部２２０を通じて、第１認証要求を第１無線端末ＳＴＡ１へ送信する。端末乱数生成部２４４は、端末乱数ＳＮＯＮＣＥを生成する。一時鍵生成部２４６は、アクセスポイント乱数ＡＮＯＮＣＥと端末乱数ＳＮＯＮＣＥと端末マス

ター鍵ＳＰＭＫとに基づいて、端末一時鍵ＳＰＴＫを生成する。フレーム送信部２４８は、メッセージフレーム（第２メッセージフレーム、第４メッセージフレーム）をアクセスポイントＡＰへ送信する。端末間鍵生成部２５０は、端末間暗号鍵ＴＥＫと端末間復号鍵ＴＤＫとを生成する。端末間鍵送信部２５２は、端末間鍵生成部２５０が生成した端末間暗号鍵ＴＥＫを第１無線端末ＳＴＡ１へ送信する。

【００９３】

制御部２４０および制御部２４０に含まれる各要素は、第２無線端末ＳＴＡ２内の不図示のCPUが、記憶部２３０に記憶されたコンピュータプログラムを実行し、そのコンピュータプログラムに従って機能することにより実現される機能ブロックである。

【００９４】

２－２－３．アクセスポイントの構成

第２実施形態のアクセスポイントＡＰは、第１実施形態のアクセスポイントＡＰと同様の構成を有するため、説明を省略する。ただし、フレーム送信部３５４は、第１無線端末ＳＴＡ１の代わりに、端末情報通知（S650）により通知された無線端末ＳＴＡ（すなわち、第２無線端末ＳＴＡ２）へ、メッセージフレーム（第１メッセージフレーム、第３メッセージフレーム）を送信する。

【００９５】

２－２－４．認証装置の構成

第２実施形態の認証装置ＡＡＡは、第１実施形態の認証装置ＡＡＡと同様の構成を有するため、説明を省略する。

【００９６】

２－３．本実施形態の効果

以上の構成によれば、移動体通信網ＭＮＷにおける加入者識別情報ＳＩＤを有さない第２無線端末ＳＴＡ２についても、加入者識別情報ＳＩＤを用いる認証方法を使用し得る。具体的に、第２無線端末ＳＴＡ２は、加入者識別情報ＳＩＤを用いる認証方法による認証動作で生成される認証情報であるマスター鍵ＰＭＫを用いて、アクセスポイントＡＰとの通信を暗号化する通信暗号化鍵（一時鍵ＰＴＫ）を生成し、アクセスポイントＡＰとの通信の暗号化に用い得る。上述のように、加入者識別情報ＳＩＤを用いる認証方法により生成された認証情報に基づく通信暗号化鍵は、加入者識別情報ＳＩＤを用いない認証方法により生成された通信暗号化鍵よりも、より特定されにくい場合があると理解される。したがって、本実施形態の例では、加入者識別情報ＳＩＤを用いない認証方法による認証動作を行ってアクセスポイントＡＰに接続する構成に比べ、第２無線端末ＳＴＡ２とアクセスポイントＡＰとがより機密性の高い通信を実行し得る。

【００９７】

さらに、以上の構成によれば、第１無線端末ＳＴＡ１が有する加入者識別情報ＳＩＤを用いてユーザ認証を実行するため、第２無線端末ＳＴＡ２のユーザがパスワード等の認証情報を入力する必要がない。そのため、第２無線端末ＳＴＡ２のユーザがより容易にアクセスポイントＡＰへ接続し得る。

【００９８】

３．変形例

以上の実施の形態は多様に変形される。具体的な変形の態様を以下に例示する。以下の例示から任意に選択された２以上の態様は相互に矛盾しない限り適宜に併合され得る。

【００９９】

３－１．変形例１

以上の各実施形態において、第１無線端末ＳＴＡ１から送信される認証情報は、第２無線端末ＳＴＡ２の端末間鍵生成部２５０により生成される端末間暗号鍵ＴＥＫを用いて暗号化される。同様に、第１無線端末ＳＴＡ１が端末間暗号鍵を生成し、当該端末間暗号鍵を用いて、第２無線端末ＳＴＡ２から第１無線端末ＳＴＡ１への通信（例えば、第１認証要求）が暗号化されてもよい。

【０１００】

３－１－１．変形例１（１）
図１２を参照して、本変形例の動作フローを説明する。この動作フローは、図２のステップS100からS130、および図８のステップS500からS530に代えて実行され得る。
【０１０１】
第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とが接続を確立する（S900）のは、上述の各実施形態と同様である。その後、第１無線端末ＳＴＡ１は、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信を暗号化する第２端末間暗号鍵ＴＥＫ２と、第２端末間暗号鍵ＴＥＫ２で暗号化された通信を復号化する第２端末間復号鍵ＴＤＫ２とを生成し（S910）、第２端末間暗号鍵ＴＥＫ２を第２無線端末ＳＴＡ２に送信する（S920）。上述の各実施形態と同様に、第２無線端末ＳＴＡ２は、端末間暗号鍵ＴＥＫを生成し（S930）、第１無線端末ＳＴＡ１へ送信する（S940）。第２無線端末ＳＴＡ２は、受信した第２端末間暗号鍵ＴＥＫ２を用いて第１認証要求を暗号化し、第１無線端末ＳＴＡ１へ送信する（S950）。
【０１０２】
図１３は、本変形例を適用した第１実施形態の第１無線端末ＳＴＡ１の構成例を示すブロック図であり、図１４は、本変形例を適用した第２実施形態の第１無線端末ＳＴＡ１の構成例を示すブロック図である。図１３および図１４のそれぞれにおいて、第１無線端末ＳＴＡ１は、各実施形態で上述した要素に加え、端末間鍵生成部１５８と、端末間鍵送信部１６０とを含む。端末間鍵生成部１５８は、第２端末間暗号鍵ＴＥＫ２と第２端末間復号鍵ＴＤＫ２とを生成する。端末間鍵送信部１６０は、第２端末間暗号鍵ＴＥＫ２を第２無線端末ＳＴＡ２へ送信する。
【０１０３】
図１５は、本変形例を適用した第１実施形態の第２無線端末ＳＴＡ２の構成例を示すブロック図であり、図１６は、本変形例を適用した第２実施形態の第２無線端末ＳＴＡ２の構成例を示すブロック図である。図１５および図１６のそれぞれにおいて、第２無線端末ＳＴＡ２は、各実施形態で上述した要素に加え、端末間通信暗号化部２５４を含む。端末間通信暗号化部２５４は、第１無線端末ＳＴＡ１から受信した第２端末間暗号鍵ＴＥＫ２を用いて、第１認証要求を暗号化する。暗号化された第１認証要求は、代理認証要求部２４２により第１無線端末ＳＴＡ１へ送信される。
【０１０４】
本変形例によれば、第２無線端末ＳＴＡ２から送信される第１認証要求が暗号化されて送信される。結果として、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の機密性、ひいては第２無線端末ＳＴＡ２とアクセスポイントＡＰとの通信の機密性がより高く保たれ得るという効果を奏し得る。
【０１０５】
なお、図１２では、端末間暗号鍵ＴＥＫが第２無線端末ＳＴＡ２から送信される（S940）前に、第２端末間暗号鍵ＴＥＫ２が第１無線端末ＳＴＡ１から送信される（S920）例が示されるが、端末間暗号鍵ＴＥＫが第２無線端末ＳＴＡ２から送信された後に、第２端末間暗号鍵ＴＥＫ２が第１無線端末ＳＴＡ１から送信されてもよい。この場合にも、上述と同様の効果を奏し得る。
【０１０６】
３－１－２．変形例１（２）
以上に説明した変形例では、第２端末間暗号鍵ＴＥＫ２を用いて第１認証要求が暗号化される。第２端末間暗号鍵ＴＥＫ２が端末間暗号鍵ＴＥＫより前に送信される構成において、第２無線端末ＳＴＡ２は、第１認証要求に加え、端末間暗号鍵ＴＥＫも第２端末間暗号鍵ＴＥＫ２を用いて暗号化し、送信してもよい。
【０１０７】
本変形例によれば、端末間暗号鍵ＴＥＫが暗号化されて送信されるため、端末間暗号鍵ＴＥＫが盗聴される危険性が低くなると理解される。そのため、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の機密性、ひいては第２無線端末ＳＴＡ２とアクセスポイ

ントＡＰとの通信の機密性がさらにより高く保たれるという効果を奏し得る。この効果は、端末間暗号鍵ＴＥＫと端末間復号鍵ＴＤＫとが一致する暗号方式（例えば、共通鍵暗号方式）が用いられる場合、特に顕著であると理解される。

【０１０８】

３－２．変形例２

第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の暗号方式には、共通鍵暗号方式が用いられ得る。この場合、第２無線端末ＳＴＡ２の端末間鍵生成部２５０は、端末間暗号鍵ＴＥＫと端末間復号鍵ＴＤＫとの両方を兼ねる共通鍵を生成する（S110、S510）。第２無線端末ＳＴＡ２の端末間鍵送信部２５２は、当該共通鍵を第１無線端末ＳＴＡ１へ送信する（S120、S520）。第１無線端末ＳＴＡ１の端末間通信暗号化部１５４は、受信した共通鍵を用いて認証情報（端末一時鍵ＳＰＴＫ、端末マスター鍵ＳＰＭＫ）を暗号化する。第２無線端末ＳＴＡ２は、端末間鍵送信部２５２が送信した共通鍵と同一の共通鍵を用いて、暗号化された認証情報を復号化する。

【０１０９】

３－３．変形例３

第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の暗号方式には、公開鍵暗号方式が用いられ得る。この場合、第２無線端末ＳＴＡ２の端末間鍵生成部２５０は、端末間暗号鍵ＴＥＫとして公開鍵を生成し、端末間復号鍵ＴＤＫとして秘密鍵を生成する（S110、S510）。第２無線端末ＳＴＡ２の端末間鍵送信部２５２は、公開鍵を第１無線端末ＳＴＡ１へ送信する（S120、S520）。第１無線端末ＳＴＡ１の端末間通信暗号化部１５４は、受信した公開鍵を用いて認証情報（端末一時鍵ＳＰＴＫ、端末マスター鍵ＳＰＭＫ）を暗号化する。第２無線端末ＳＴＡ２は、秘密鍵を用いて、公開鍵で暗号化された認証情報を復号化する。

【０１１０】

本変形例を採用する場合、端末間復号鍵ＴＤＫである秘密鍵は、第２無線端末ＳＴＡ２のみが有し、第１無線端末ＳＴＡ１へ送信されない。そのため、端末間復号鍵ＴＤＫと一致する端末間暗号鍵ＴＥＫが送信される構成（例えば、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の暗号方式に共通鍵暗号方式を用いる構成）と比べ、端末間復号鍵ＴＤＫが盗聴等により特定されにくいと理解される。結果として、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の機密性、ひいては第２無線端末ＳＴＡ２とアクセスポイントＡＰとの通信の機密性がより高く保たれるという効果を奏し得る。

【０１１１】

３－４．変形例４

第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の暗号方式には、公開鍵暗号方式と秘密鍵暗号方式との両方を用いた暗号方式（例えば、TLS（transport layer security）暗号方式）が用いられ得る。この場合、第１無線端末ＳＴＡ１が、変形例１で上述した構成を有すると好適である。

【０１１２】

具体的に、第１無線端末ＳＴＡ１の端末間鍵生成部１５８は、第２端末間暗号鍵ＴＥＫ２として公開鍵を生成し、第２端末間復号鍵ＴＤＫ２として秘密鍵を生成する（S910）。端末間鍵送信部１６０は、公開鍵（第２端末間暗号鍵ＴＥＫ２）を第２無線端末ＳＴＡ２へ送信する（S920）。第２無線端末ＳＴＡ２の端末間鍵生成部２５０は、端末間暗号鍵ＴＥＫと端末間復号鍵ＴＤＫとの両方を兼ねる共通鍵を生成する（S110、S510、S930）。第２無線端末ＳＴＡ２の端末間通信暗号化部２５４は、第１無線端末ＳＴＡ１から受信した公開鍵（第２端末間暗号鍵ＴＥＫ２）で共通鍵（端末間暗号鍵ＴＥＫ）を暗号化し、第１無線端末ＳＴＡ１へ送信する（S120、S520、S940）。第１無線端末ＳＴＡ１は、秘密鍵（第２端末間復号鍵ＴＤＫ２）を用いて、暗号化された共通鍵（端末間暗号鍵ＴＥＫ）を復号化する。第１無線端末ＳＴＡ１の端末間通信暗号化部１５４は、復号化した共通鍵（端末間暗号鍵ＴＥＫ）を用いて認証情報（端末一時鍵ＳＰＴＫ、端末マスター鍵ＳＰＭＫ）を暗号化する。第２無線端末ＳＴＡ２は、共通鍵（端末間復号鍵ＴＤＫ）を用いて、共通

鍵（端末間暗号鍵ＴＥＫ）で暗号化された認証情報を復号化する。

【０１１３】

本変形例を採用する場合、端末間暗号鍵ＴＥＫである共通鍵が、第１無線端末ＳＴＡ１の端末間鍵生成部１５８が生成した公開鍵（第２端末間暗号鍵ＴＥＫ２）で暗号化された状態で（すなわち、第１無線端末ＳＴＡ１の端末間鍵生成部１５８が生成した秘密鍵（第２端末間復号鍵ＴＤＫ２）のみが復号化できる状態で）送信される。そのため、共通鍵が盗聴等により特定される危険性が低いと理解される。結果として、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の機密性、ひいては第２無線端末ＳＴＡ２とアクセスポイントＡＰとの通信の機密性がより高く保たれるという効果を奏し得る。

【０１１４】

３－５．変形例５

以上の例では、第２無線端末ＳＴＡ２へ送信される認証情報（端末一時鍵ＳＰＴＫ、端末マスター鍵ＳＰＭＫ）等の、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信が、端末間暗号鍵ＴＥＫまたは端末間暗号鍵ＴＥＫと第２端末間暗号鍵ＴＥＫ２との両方によって暗号化される。しかし、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信が暗号化されなくてもよい。この場合、端末間鍵を生成するステップ（S110、S510、S910、S930）および端末間鍵を送信するステップ（S120、S520、S920、S940）は不要である。さらに、第１無線端末ＳＴＡ１は、端末間通信暗号化部１５４と、端末間鍵生成部１５８と、端末間鍵送信部１６０とのうち、少なくともいずれか１要素を含まなくともよい。第２無線端末ＳＴＡ２は、端末間鍵生成部２５０と、端末間鍵送信部２５２と、端末間通信暗号化部２５４とのうち、少なくともいずれか１要素を含まなくともよい。

【０１１５】

３－６．変形例６

以上に説明した第１実施形態の例（第１実施形態の変形例も含む）において、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信に用いる無線通信技術として、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とが至近距離（例えば、10センチメートル以内）に位置していなくても通信が可能（例えば、数メートルから数十メートル以内に位置していれば通信が可能）である無線通信技術（例えばBluetooth（登録商標）、Wi-Fi Direct）（以下、「非近接型無線通信技術」と称する場合がある）を用いると好適である。

【０１１６】

第１実施形態の例では、第２無線端末ＳＴＡ２とアクセスポイントＡＰとの接続が維持されている間、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との接続も維持される。第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信に非近接型無線通信技術が用いられる場合、ユーザは、当該非近接型無線通信技術において通信が可能な範囲において、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とを離して使用できる。したがって、第２無線端末ＳＴＡ２とアクセスポイントＡＰとの接続が維持されている間（すなわち、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との接続が維持されている間）においても、ユーザが第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との両方の無線端末ＳＴＡを使用しやすくなるという効果を奏し得る。

【０１１７】

３－７．変形例７

以上に説明した第２実施形態の例（第２実施形態の変形例も含む）において、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信に用いる無線通信技術として、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とが至近距離（例えば、10センチメートル以内）に位置する必要がある無線通信技術（例えば、NFC）（以下、「近接型無線通信技術」と称する場合がある）を用いると好適である。

【０１１８】

第２実施形態の例では、第１無線端末ＳＴＡ１から第２無線端末ＳＴＡ２へ端末マスター鍵ＳＰＭＫが送信される。無線端末ＳＴＡとアクセスポイントＡＰとの通信を暗号化する一時鍵ＰＴＫ（端末一時鍵ＳＰＴＫ、アクセスポイント一時鍵ＡＰＴＫ）はマスター鍵

ＰＭＫ（端末マスター鍵ＳＰＭＫ、アクセスポイントマスター鍵ＡＰＭＫ）に基づいて生成されるため、マスター鍵ＰＭＫが盗聴されると、一時鍵ＰＴＫが特定される危険性が高まる可能性がある。そのため、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信にはより盗聴されにくい無線通信技術を用いると好適と理解される。

【０１１９】

第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２とが近接型無線通信技術を用いて通信する場合、近接型無線通信技術よりも広い通信可能範囲（例えば、数十メートル以内）を持つ無線通信技術を用いる場合と比べて、その通信可能範囲内に、通信する端末同士以外の第３の機器が入り込む余地が少ないと理解される。結果として、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信が第３の機器に盗聴されにくい。したがって、近接型無線通信技術を用いて通信する場合、第１無線端末ＳＴＡ１と第２無線端末ＳＴＡ２との通信の機密性、ひいては第２無線端末ＳＴＡ２とアクセスポイントＡＰとの通信の機密性がより高く保たれるという効果を奏し得る。

【０１２０】

３－８．変形例８

以上に説明した第１実施形態の例では、第１無線端末ＳＴＡ１が生成する端末一時鍵ＳＰＴＫと、アクセスポイントＡＰが生成するアクセスポイント一時鍵ＡＰＴＫとが、第１無線端末ＳＴＡ１が代理する第２無線端末ＳＴＡ２との通信に用いられることを知らせる端末情報通知が、第２メッセージフレームに含まれてアクセスポイントＡＰへ送信される。

【０１２１】

しかし、端末情報通知は、認証装置ＡＡＡがアクセスポイントＡＰへアクセスポイントマスター鍵ＡＰＭＫを送信してから、第１無線端末ＳＴＡ１が端末一時鍵ＳＰＴＫを第２無線端末ＳＴＡ２へ送信するまでの間にアクセスポイントＡＰへ送信されればよい。また、第２実施形態で例示したように（S650）、独立したメッセージとして端末情報通知が送信されてもよい。例えば、端末情報通知は第４メッセージフレームに含まれて送信されてもよいし、第４メッセージフレームが送信された後、端末一時鍵ＳＰＴＫが送信される前に、個別のメッセージとして送信されてもよい。

【０１２２】

３－９．変形例９

無線通信システムＣＳ内の各要素（第１無線端末ＳＴＡ１、第２無線端末ＳＴＡ２、アクセスポイントＡＰ、認証装置ＡＡＡ、加入者情報管理装置ＨＳＳ）において、ＣＰＵが実行する各機能は、ＣＰＵの代わりに、ハードウェアで実行してもよいし、例えばＦＰＧＡ（Field Programmable Gate Array）、ＤＳＰ（Digital Signal Processor）等のプログラマブルロジックデバイスで実行してもよい。

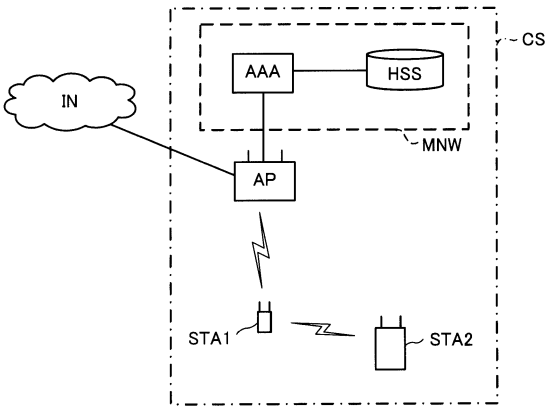
【符号の説明】

【０１２３】

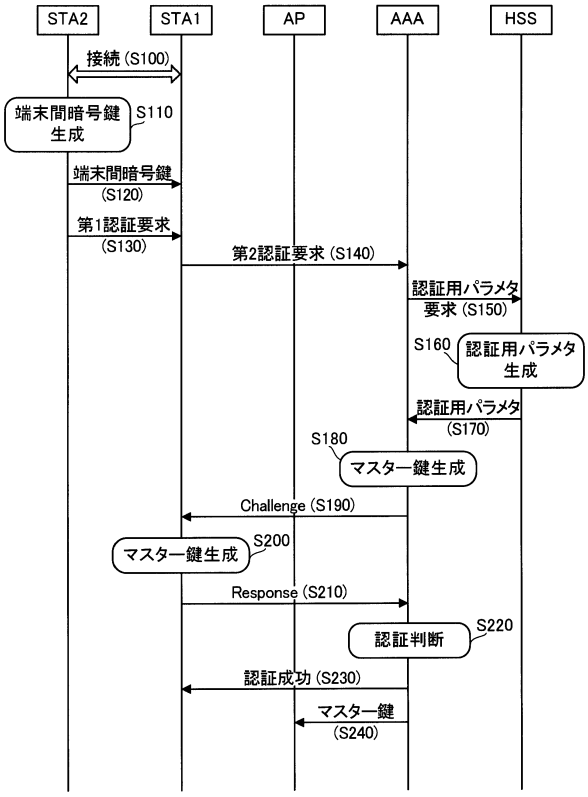
ＡＡＡ……認証装置、ＡＮＯＮＣＥ……アクセスポイント乱数、ＡＰ……アクセスポイント、ＡＰＭＫ……アクセスポイントマスター鍵、ＡＰＴＫ……アクセスポイント一時鍵、ＣＳ……無線通信システム、ＨＳＳ……加入者情報管理装置、Ｋ……加入者登録情報、ＫＭ……鍵情報、ＩＮ……インターネット、ＭＡＣ……メッセージ認証コード、ＭＩＣ（ＭＩＣ１、ＭＩＣ２、ＭＩＣ３）……メッセージ完全性コード、ＭＮＷ……移動体通信網、ＰＭＫ……マスター鍵、ＰＴＫ……一時鍵、ＳＩＤ……加入者識別情報、ＳＮＯＮＣＥ……端末乱数、ＳＰＭＫ……端末マスター鍵、ＳＰＴＫ……端末一時鍵、ＳＴＡ１……第１無線端末、ＳＴＡ２……第２無線端末、ＴＤＫ……端末間復号鍵、ＴＤＫ２……第２端末間復号鍵、ＴＥＫ……端末間暗号鍵、ＴＥＫ２……第２端末間暗号鍵、１２０……端末通信部、１３０……記憶部、１４２……認証情報要求部、１４４……マスター鍵生成部、１４６……レスポンス送信部、１４８……端末乱数生成部、１５０……一時鍵生成部、１５２……フレーム送信部、１５４……端末間通信暗号化部、１５６……認証情報送信部、１５８……端末間鍵生成部、１６０……端末間鍵送信部、２２０……端末通信部、２３０

……記憶部、２４２……代理認証要求部、２４４……端末乱数生成部、２４６……一時鍵生成部、２４８……フレーム送信部、２５０……端末間鍵生成部、２５２……端末間鍵送信部、２５４……端末間通信暗号化部、３４０……記憶部、３５２……アクセスポイント乱数生成部、３５４……フレーム送信部、３５６……一時鍵生成部、４２０……記憶部、４３２……認証用パラメタ取得部、４３４……マスター鍵生成部、４３６……チャレンジ送信部、４３８……認証判定部、４４０……判定結果通知部、４４２……マスター鍵送信部。

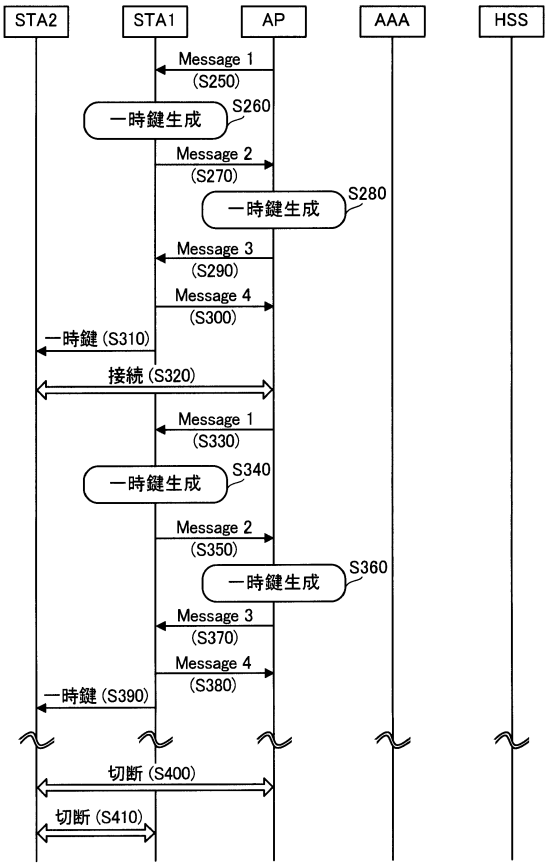
【図１】



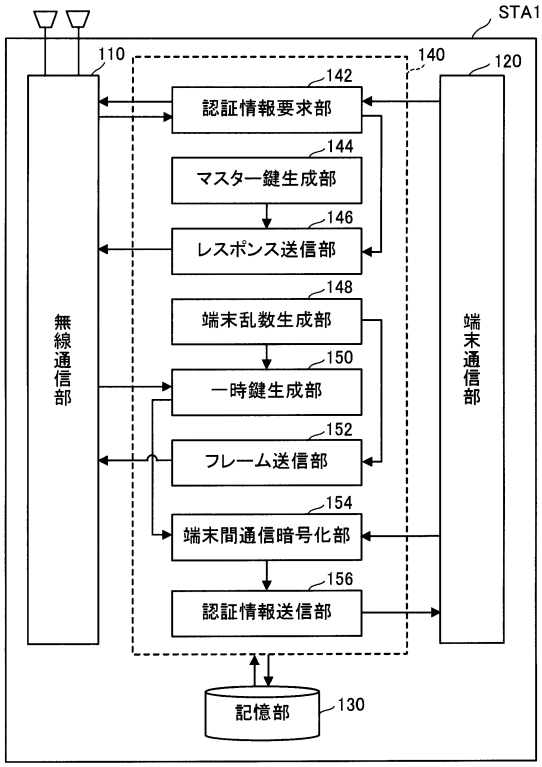
【図２】



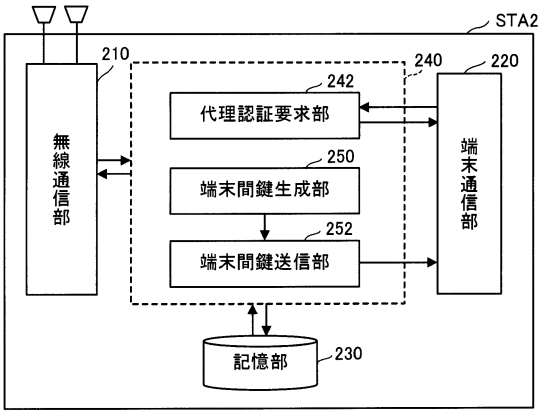
【図３】


STA2
STA1
AP
AAA
HSS
Message 1
(S250)
一時鍵生成
S260
Message 2
(S270)
一時鍵生成
S280
Message 3
(S290)
Message 4
(S300)
一時鍵 (S310)
接続 (S320)
Message 1
(S330)
一時鍵生成
S340
Message 2
(S350)
一時鍵生成
S360
Message 3
(S370)
Message 4
(S380)
一時鍵 (S390)
切断 (S400)
切断 (S410)

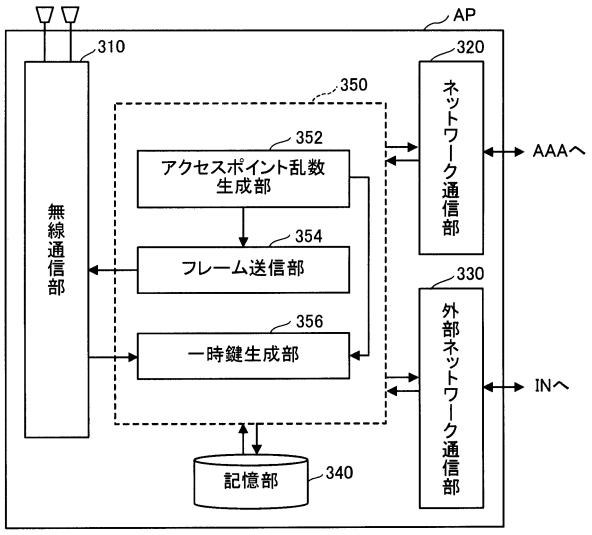
【図４】


STA1
110
140
120
142
認証情報要求部
144
マスター鍵生成部
146
レスポンス送信部
148
端末乱数生成部
150
一時鍵生成部
152
フレーム送信部
154
端末間通信暗号化部
156
認証情報送信部
無線通信部
端末通信部
記憶部
130

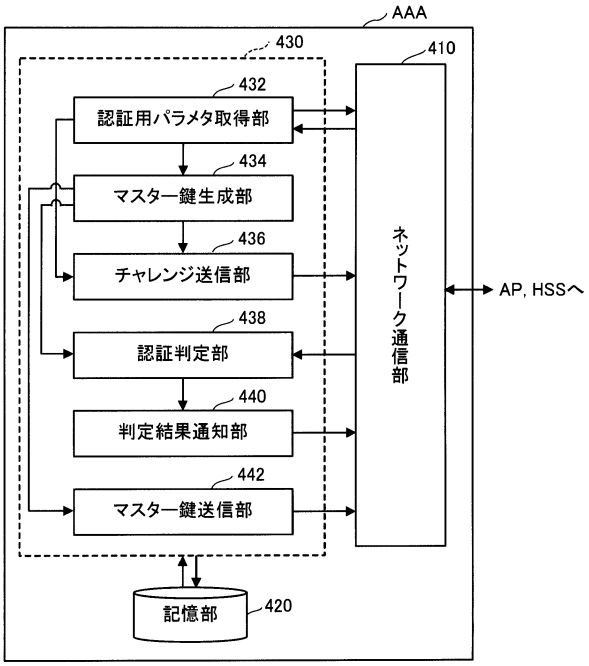
【図５】


STA2
210
240
220
242
代理認証要求部
250
端末間鍵生成部
252
端末間鍵送信部
無線通信部
端末通信部
記憶部
230

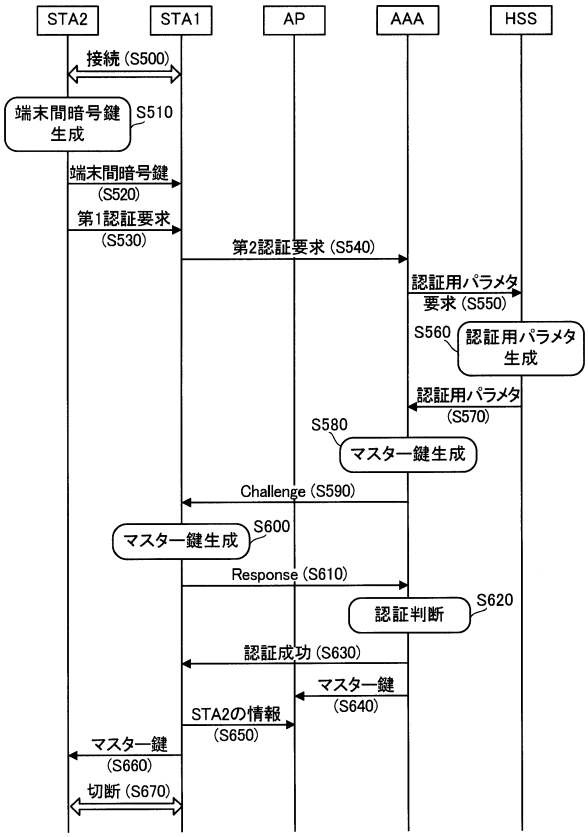
【図６】


AP
310
320
350
352
アクセスポイント乱数生成部
354
フレーム送信部
356
一時鍵生成部
330
無線通信部
ネットワーク通信部
外部ネットワーク通信部
AAAへ
INへ
記憶部
340

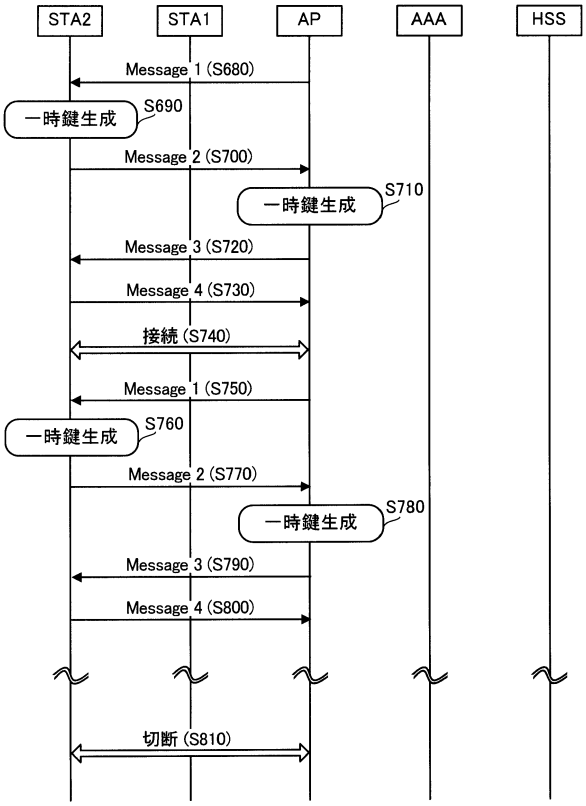
【図７】


AAA
430
410
432
認証用パラメタ取得部
434
マスター鍵生成部
436
チャレンジ送信部
438
認証判定部
440
判定結果通知部
442
マスター鍵送信部
ネットワーク通信部
AP, HSSへ
記憶部
420

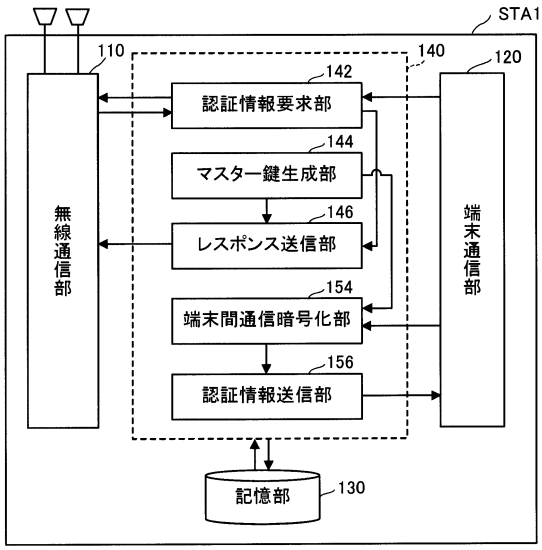
【図８】


STA2
STA1
AP
AAA
HSS
接続 (S500)
端末間暗号鍵生成
S510
端末間暗号鍵 (S520)
第1認証要求 (S530)
第2認証要求 (S540)
認証用パラメタ要求 (S550)
S560
認証用パラメタ生成
認証用パラメタ (S570)
S580
マスター鍵生成
Challenge (S590)
マスター鍵生成
S600
Response (S610)
認証判断
S620
認証成功 (S630)
マスター鍵 (S640)
STA2の情報 (S650)
マスター鍵 (S660)
切断 (S670)

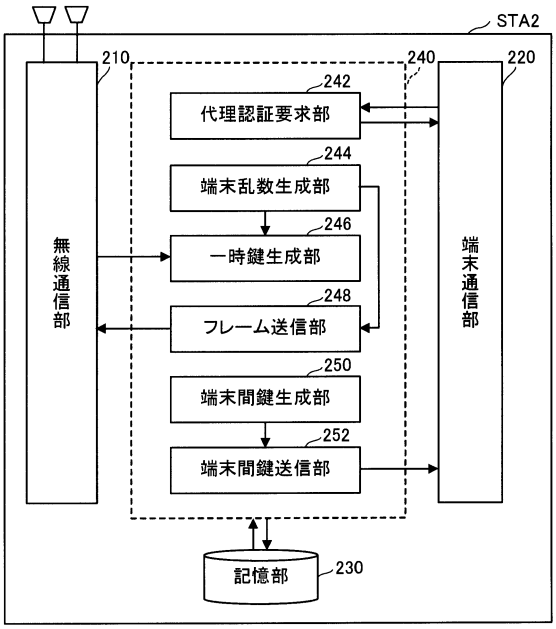
【図９】


STA2
STA1
AP
AAA
HSS
Message 1 (S680)
一時鍵生成
S690
Message 2 (S700)
一時鍵生成
S710
Message 3 (S720)
Message 4 (S730)
接続 (S740)
Message 1 (S750)
一時鍵生成
S760
Message 2 (S770)
一時鍵生成
S780
Message 3 (S790)
Message 4 (S800)
切断 (S810)

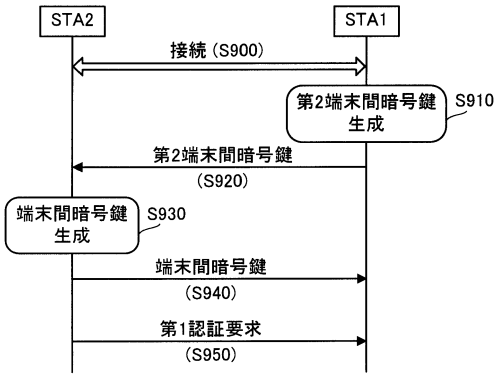
【図１０】


STA1
110
140
120
142
認証情報要求部
144
マスター鍵生成部
146
レスポンス送信部
154
端末間通信暗号化部
156
認証情報送信部
無線通信部
端末通信部
記憶部
130

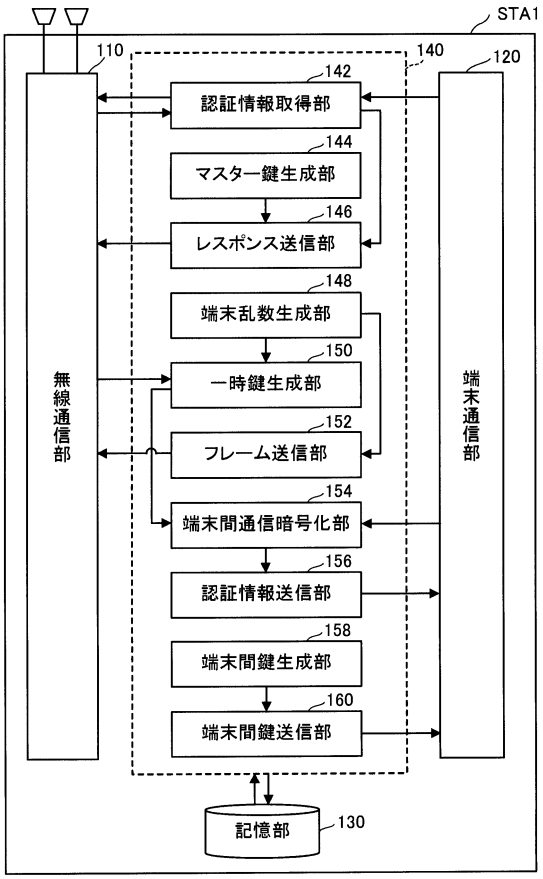
【図１１】



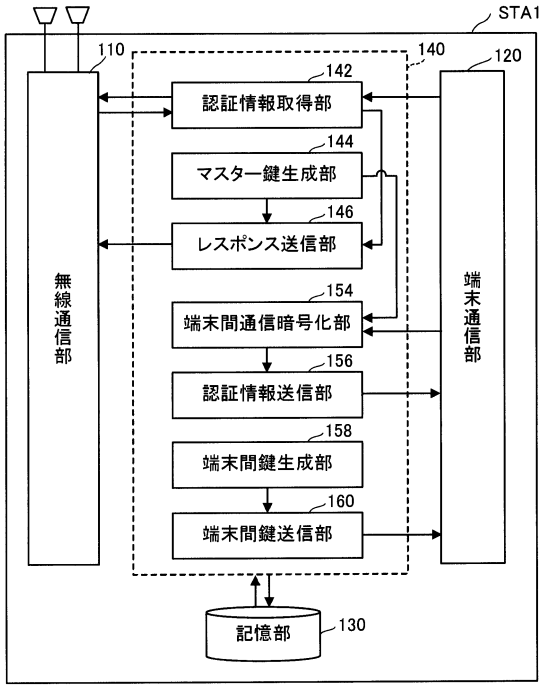
【図１２】



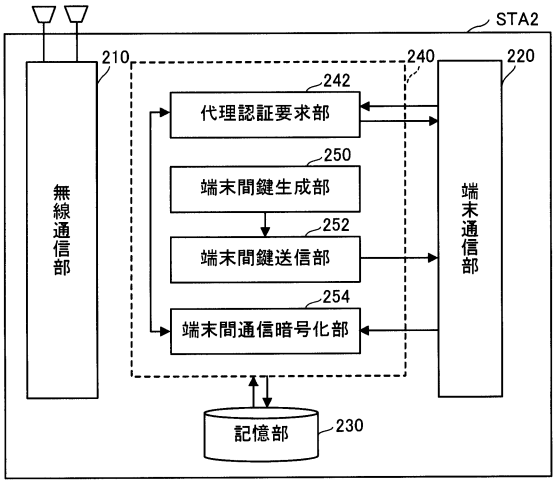
【図１３】



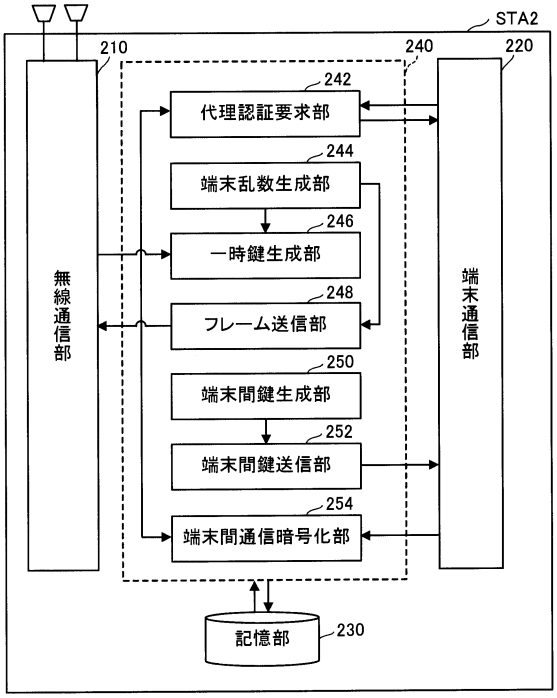
【図１４】



【図１５】


STA2
210
240
220
242
代理認証要求部
250
端末間鍵生成部
252
端末間鍵送信部
254
端末間通信暗号化部
無線通信部
端末通信部
記憶部
230

【図１６】


STA2
210
240
220
242
代理認証要求部
244
端末乱数生成部
246
一時鍵生成部
248
フレーム送信部
250
端末間鍵生成部
252
端末間鍵送信部
254
端末間通信暗号化部
無線通信部
端末通信部
記憶部
230

フロントページの続き

(72)発明者　安田　浩人
東京都千代田区永田町二丁目１１番１号　株式会社ＮＴＴドコモ内
(72)発明者　浅井　孝浩
東京都千代田区永田町二丁目１１番１号　株式会社ＮＴＴドコモ内

審査官　吉村　真治▲郎▼

(56)参考文献　特開２００９－３０３１８８（ＪＰ，Ａ）
特開２０１４－２３８６６４（ＪＰ，Ａ）
特表２０１３－５０９０８９（ＪＰ，Ａ）
特開２００４－２０８０７３（ＪＰ，Ａ）
特開２０１３－０９００４６（ＪＰ，Ａ）
特開２０１３－０４８３３０（ＪＰ，Ａ）
特開２００７－０１３３４８（ＪＰ，Ａ）
特開２００８－２０３８０３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　　７／２４－　７／２６
Ｈ０４Ｗ　　４／００－９９／００