(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-135599
(P2017-135599A)
(43)公開日　平成29年8月3日(2017.8.3)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601D	5J104
H04W 12/02	(2009.01)	H04L	9/00	601E	5K067
H04W 12/04	(2009.01)	H04W	12/02		
H04W 12/06	(2009.01)	H04W	12/04		
		H04W	12/06		

審査請求 未請求　請求項の数 7　OL　（全 19 頁）

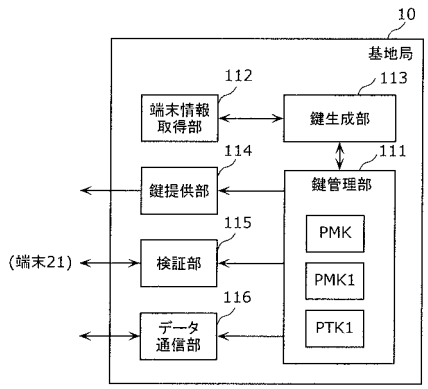
(21)出願番号　特願2016-14673(P2016-14673)
(22)出願日　平成28年1月28日(2016.1.28)

(71)出願人　500112146
サイレックス・テクノロジー株式会社
京都府相楽郡精華町光台二丁目３番地１
(74)代理人　100109210
弁理士　新居　広守
(72)発明者　呼元　文数
京都府相楽郡精華町光台二丁目３番地１サイレックス・テクノロジー株式会社内
(72)発明者　高田　悦子
京都府相楽郡精華町光台二丁目３番地１サイレックス・テクノロジー株式会社内

Ｆターム(参考)　5J104 AA07 AA16 EA26 KA02 KA03 NA02 NA03 NA11 NA12 NA37 PA01
5K067 AA35 BB04 BB21 DD17 EE02 EE10 HH22 HH23 HH36

(54)【発明の名称】無線基地局装置、無線通信システム、及び、無線基地局装置の制御方法

(57)【要約】　（修正有）
【課題】導入コストを抑えながら端末のなりすましを抑制する無線基地局装置を提供する。
【解決手段】基地局１０は、第一鍵情報ＰＭＫを保有する鍵管理部１１１と、無線端末から取得した、無線端末に固有の識別情報である第一識別情報と、第一鍵情報ＰＭＫとを用いた第一演算により第二鍵情報ＰＭＫ１を生成する鍵生成部１１３と、鍵生成部１１３が生成した第二鍵情報ＰＭＫ１が無線端末に提供されるよう制御する鍵提供部１１４と、基地局１０と無線データ通信しようとする通信端末に固有の識別情報を第二識別情報として通信端末から取得し、第二識別情報と第一鍵情報ＰＭＫとを用いた第一演算を利用して、通信端末が第二鍵情報ＰＭＫ１を保有していることの検証を行う検証部１１５と、検証部１１５による検証が成功したと判定したことを条件の１つとして、第二鍵情報ＰＭＫ１に基づいて暗号化されたデータ通信を通信端末と行うデータ通信部１１６とを備える。
【選択図】図６



【特許請求の範囲】
【請求項１】
無線端末との暗号化されたデータ通信を行うための無線基地局装置であって、
第一鍵情報を保有している鍵管理部と、
無線端末に固有の識別情報である第一識別情報を取得する端末情報取得部と、
前記端末情報取得部が取得した前記第一識別情報と、前記第一鍵情報とを用いた第一演算により第二鍵情報を生成する鍵生成部と、
前記鍵生成部が生成した前記第二鍵情報が前記無線端末に提供されるよう制御する鍵提供部と、
前記無線基地局との前記データ通信をしようとする無線端末である通信端末に固有の識別情報を第二識別情報として前記通信端末から取得し、前記第二識別情報と前記第一鍵情報とを用いた前記第一演算を利用して、前記通信端末が前記第二鍵情報を保有していることの検証を行う検証部と、
前記検証部による前記検証が成功したと判定したことを条件の１つとして、前記第二鍵情報に基づいて暗号化されたデータ通信を前記通信端末と行うデータ通信部とを備える
無線基地局装置。
【請求項２】
前記第一演算は、一方向関数による演算を含む
請求項１に記載の無線基地局装置。
【請求項３】
前記検証部は、（ａ）第一情報を前記通信端末に送信し、（ｂ）前記第一情報と、前記鍵生成部が前記通信端末に提供した前記第二鍵情報とに基づく第二演算を用いて前記通信端末により算出された第二情報を、前記第二識別情報とともに前記通信端末から取得し、（ｃ）前記第一鍵情報と、取得した前記第二識別情報とに基づく前記第二演算により算出された第三情報が、前記第二情報と一致するときに、前記検証が成功したと判定する
請求項１又は２に記載の無線基地局装置。
【請求項４】
前記検証部は、前記通信端末が送信した前記第二情報を含む通信フレームを取得し、取得した通信フレームに含まれる送信元アドレスフィールドから、前記第二識別情報を取得する
請求項３に記載の無線基地局装置。
【請求項５】
前記通信端末の前記第一識別情報及び前記第二識別情報は、それぞれ、前記通信端末のハードウェアアドレスを含む
請求項１～４のいずれか１項に記載の無線基地局装置。
【請求項６】
請求項１～５のいずれか１項に記載の無線基地局装置と、
前記無線基地局装置と無線通信を行う前記無線端末とを備える
無線通信システム。
【請求項７】
無線端末との暗号化されたデータ通信を行うための無線基地局装置の制御方法であって、
第一鍵情報を保有する鍵管理ステップと、
無線端末に固有の識別情報である第一識別情報を取得する端末情報取得ステップと、
前記端末情報取得ステップで取得した前記第一識別情報と、前記第一鍵情報とを用いた第一演算により第二鍵情報を生成し、生成した前記第二鍵情報が前記無線端末に提供されるよう制御する鍵生成ステップと、
前記無線基地局との前記データ通信をしようとする無線端末である通信端末に固有の識別情報を第二識別情報として前記通信端末から取得し、前記第二識別情報と前記第一鍵情報とを用いた前記第一演算を利用して、前記通信端末が前記第二鍵情報を保有しているこ

との検証を行う検証ステップと、
前記検証ステップで前記検証が成功したと判定したことを条件の１つとして、前記第二鍵情報に基づいて暗号化されたデータ通信を前記通信端末と行うデータ通信ステップとを含む
制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線端末との無線通信を行う無線基地局装置、無線通信システム、及び、無線基地局装置の制御方法に関する。
【背景技術】
【０００２】
従来、無線通信端末（以降、端末ともいう）と、無線通信リンク（以降、通信リンクともいう）を介して当該端末と通信する無線基地局装置（以降、基地局ともいう）とを用いたＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が利用されている。端末は、無線ＬＡＮを介して、当該無線ＬＡＮに接続されているネットワーク上の他の通信装置（Ｗｅｂサーバ又はメールサーバなど）と通信することができる。無線通信では、通信する装置間にケーブルなどによる有線接続がないので、盗聴又はなりすましのようなセキュリティ上のリスクが比較的大きい。盗聴又はなりすましを防止する施策として、通信信号を暗号化することが行われているが充分とはいえない。
【０００３】
特許文献１は、通信信号の暗号化に使用する鍵情報を、端末及び基地局それぞれが保有する情報に基づいて生成することで、端末のなりすましを防ぐ通信システムを開示している。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特許第４５５０７５９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１が開示する通信システムでは、従来の端末及び基地局が搭載していない機能を、端末及び基地局の両方が搭載している必要がある。そのため、特許文献１が開示する通信システムを機能させるためには、通信システムに含まれる端末及び基地局の両方を導入する必要があり、導入コストが高く、また、利便性が低い。
【０００６】
本発明は、上記問題を解決するためになされたものであり、導入コストを抑えながら端末のなりすましを抑制する無線基地局装置等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】
【０００７】
上記課題を解決するために、本発明の一態様に係る無線基地局装置は、無線端末との暗号化されたデータ通信を行うための無線基地局装置であって、第一鍵情報を保有している鍵管理部と、無線端末に固有の識別情報である第一識別情報を取得する端末情報取得部と、前記端末情報取得部が取得した前記第一識別情報と、前記第一鍵情報とを用いた第一演算により第二鍵情報を生成する鍵生成部と、前記鍵生成部が生成した前記第二鍵情報が前記無線端末に提供されるよう制御する鍵提供部と、前記無線基地局との前記データ通信をしようとする無線端末である通信端末に固有の識別情報を第二識別情報として前記通信端末から取得し、前記第二識別情報と前記第一鍵情報とを用いた前記第一演算を利用して、前記通信端末が前記第二鍵情報を保有していることの検証を行う検証部と、前記検証部による前記検証が成功したと判定したことを条件の１つとして、前記第二鍵情報に基づいて

暗号化されたデータ通信を前記通信端末と行うデータ通信部とを備える。

【０００８】

これによれば、無線基地局装置は、無線端末の識別情報に基づいて生成された第二鍵情報を用いて、無線端末の正当性を検証することができる。具体的には、無線基地局装置は、無線端末の識別情報を加味して第二鍵情報を生成し、また、当該無線基地局装置に接続しようとする無線端末が正当な鍵情報を有することを無線端末の識別情報を加味して行う。これにより、一の無線端末の識別情報を加味して生成された第二鍵情報を、他の無線端末が使用して無線基地局装置に接続することを禁止する。また、本発明の無線基地局装置に接続しようとする端末は、従来の端末の機能だけで十分であり、本発明の無線基地局装置に接続するための特別な機能を要しない。よって、本発明の無線基地局装置は、導入コストを抑えながら端末のなりすましを抑制することができる。

【０００９】

また、前記第一演算は、一方向関数による演算を含んでもよい。

【００１０】

これによれば、無線基地局装置は、第二鍵情報から、当該第二鍵情報を生成するために利用した第一鍵情報を得ることが実質的に不可能である。よって、第一鍵情報が無線基地局装置の外部に漏洩することが抑制される。これにより、端末のなりすましをより一層抑制することができる。

【００１１】

また、前記検証部は、（ａ）第一情報を前記通信端末に送信し、（ｂ）前記第一情報と、前記鍵生成部が前記通信端末に提供した前記第二鍵情報とに基づく第二演算を用いて前記通信端末により算出された第二情報を、前記第二識別情報とともに前記通信端末から取得し、（ｃ）前記第一鍵情報と、取得した前記第二識別情報とに基づく前記第二演算により算出された第三情報が、前記第二情報と一致するときに、前記検証が成功したと判定してもよい。

【００１２】

これによれば、無線基地局装置は、端末が第二鍵情報を保有していることを具体的に検証することができる。よって、無線基地局装置は、端末のなりすましの抑制をより具体的に実現することができる。

【００１３】

また、前記検証部は、前記通信端末が送信した前記第二情報を含む通信フレームを取得し、取得した通信フレームに含まれる送信元アドレスフィールドから、前記第二識別情報を取得してもよい。

【００１４】

これによれば、無線基地局装置は、端末が第二鍵情報を保有していることの検証に用いられる通信フレームのアドレスフィールドを用いて、より具体的かつ確実に、端末のなりすましを抑制することができる。

【００１５】

また、前記通信端末の前記第一識別情報及び前記第二識別情報は、それぞれ、前記通信端末のハードウェアアドレスを含んでもよい。

【００１６】

これによれば、無線基地局装置は、端末のハードウェアアドレスを用いてより具体的に端末のなりすましを抑制することができる。

【００１７】

上記課題を解決するために、本発明の一態様に係る無線通信システムは、上記の無線基地局装置と、前記無線基地局装置と無線通信を行う前記無線端末とを備える。

【００１８】

これにより、上記無線基地局装置と同様の効果を奏する。

【００１９】

上記課題を解決するために、本発明の一態様に係る無線基地局装置の制御方法は、無線

端末との暗号化されたデータ通信を行うための無線基地局装置の制御方法であって、第一鍵情報を保有する鍵管理ステップと、無線端末に固有の識別情報である第一識別情報を取得する端末情報取得ステップと、前記端末情報取得ステップで取得した前記第一識別情報と、前記第一鍵情報とを用いた第一演算により第二鍵情報を生成し、生成した前記第二鍵情報が前記無線端末に提供されるよう制御する鍵生成ステップと、前記無線基地局との前記データ通信をしようとする無線端末である通信端末に固有の識別情報を第二識別情報として前記通信端末から取得し、前記第二識別情報と前記第一鍵情報とを用いた前記第一演算を利用して、前記通信端末が前記第二鍵情報を保有していることの検証を行う検証ステップと、前記検証ステップで前記検証が成功したと判定したことを条件の１つとして、前記第二鍵情報に基づいて暗号化されたデータ通信を前記通信端末と行うデータ通信ステップとを含む。

【００２０】

これにより、上記無線基地局装置と同様の効果を奏する。

【００２１】

なお、本発明は、装置として実現できるだけでなく、その装置を構成する処理手段をステップとする方法として実現したり、それらステップをコンピュータに実行させるプログラムとして実現したり、そのプログラムを記録したコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体として実現したり、そのプログラムを示す情報、データ又は信号として実現したりすることもできる。そして、それらプログラム、情報、データ及び信号は、インターネット等の通信ネットワークを介して配信してもよい。

【発明の効果】

【００２２】

本発明に係る無線基地局装置は、導入コストを抑えながら端末のなりすましを抑制することができる。

【図面の簡単な説明】

【００２３】

【図１】図１は、実施の形態に係る無線通信システムの構成図である。

【図２】図２は、実施の形態に係る基地局のハードウェア構成を示すブロック図である。

【図３】図３は、関連技術に係る基地局の機能構成を示すブロック図である。

【図４】図４は、関連技術に係る基地局の鍵情報の導入に係る処理を示すフロー図である。

【図５】図５は、関連技術に係る通信システムにおける鍵情報の導入に係る処理を示すシーケンス図である。

【図６】図６は、実施の形態に係る基地局の機能構成を示すブロック図である。

【図７】図７は、実施の形態に係る基地局の鍵情報の導入に係る処理を示すフロー図である。

【図８】図８は、実施の形態に係る通信システムにおける鍵情報の導入に係る処理であって、ＭＩＣの検証処理が成功する場合を示すシーケンス図である。

【図９】図９は、実施の形態に係る通信システムにおける鍵情報の導入に係る処理であって、ＭＩＣの検証処理が失敗する場合を示すシーケンス図である。

【図１０】図１０は、実施の形態に係る無線通信システムにおける各装置が保有し又は使用する鍵情報とを示す説明図である。

【発明を実施するための形態】

【００２４】

以下、実施の形態について、図面を参照しながら具体的に説明する。

【００２５】

以下で説明する実施の形態は、いずれも本発明の好ましい一具体例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、本発明の最上位概念を示す独立請求項

に記載されていない構成要素については、より好ましい形態を構成する任意の構成要素として説明される。

【００２６】

なお、同一の構成要素には同一の符号を付し、説明を省略する場合がある。

【００２７】

（実施の形態）

本実施の形態において、導入コストを抑えながら端末のなりすましを抑制する無線基地局装置及び無線通信システムについて説明する。

【００２８】

図１は、本実施の形態に係る無線通信システム１の構成図である。

【００２９】

図１に示されるように、無線通信システム１は、基地局１０と、端末２１及び２２とを備える。無線通信システム１は、ＬＡＮ４０に通信可能に接続されており、端末２１及び２２は、ＬＡＮ４０を経由して外部のネットワーク（不図示）の通信装置と通信することができる。

【００３０】

基地局１０は、端末２１等と無線通信を行う無線基地局装置である。基地局１０は、無線通信インタフェース（以降、「無線ＩＦ」ともいう）を備えており、無線ＩＦにより端末２１との間で通信リンク３１を確立し、確立した通信リンク３１を通じて端末２１と通信フレームを送受信することで通信する。また、基地局１０は、有線通信インタフェース（以降、「有線ＩＦ」ともいう）を備えており、有線ＩＦによりＬＡＮ４０に接続されている。

【００３１】

端末２１及び２２は、無線ＩＦを有する無線端末である。端末２１及び２２は、それぞれ、基地局１０が有する無線ＩＦと通信リンク３１及び３２を確立し、確立した通信リンク３１及び３２を通じて無線通信を行う。端末２１及び２２は、基地局１０を介して、ＬＡＮ４０に接続された通信装置（不図示）、及び、ＬＡＮ４０に接続された他のネットワークに接続された通信装置（不図示）と通信することができる。端末２１及び２２それぞれは、基地局１０との間で暗号化された通信フレームをやりとりすることで無線通信を行う。この無線通信は、通信相手が正当な暗号鍵を有していることを例えばＩＥＥＥ８０２．１１ｉに規定される４ウェイハンドシェイクにより検証した上で行われる。なお、基地局１０との暗号化されたデータ通信をしようとする無線端末のことを通信端末ともいう。

【００３２】

なお、端末２１及び２２は、従来の端末と同じ機能を有するものである。なお、以降では、端末２１について主に説明するが、特に断らない限り、同様の説明が端末２２にも成立する。

【００３３】

ＬＡＮ４０は、基地局１０が接続された通信ネットワーク（ローカルエリアネットワーク）である。ＬＡＮ４０は、例えば、ＩＥＥＥ８０２．３規格などに適合する有線ＬＡＮにより実現される。ＬＡＮ４０には、基地局１０と異なる通信装置（端末、ルータ等）が接続されていてもよい。

【００３４】

無線通信システム１において、基地局１０は、基地局１０への接続を許可する端末を所定の端末だけに制限するように利用されることを想定する。例えば、無線通信システム１は、個人の宅内に設置される家庭内ネットワーク、又は、企業のオフィス内に設置される社内ネットワークに適用され得る。

【００３５】

このように構成された無線通信システム１における基地局１０のハードウェア構成及び機能構成について説明する。

【００３６】

図２は、本実施の形態に係る基地局１０のハードウェア構成を示すブロック図である。
【００３７】
図２に示されるように、基地局１０は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１０１と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１０２と、メインメモリ１０３と、ストレージ１０４と、有線ＩＦ１０５と、無線ＩＦ１０６とを備える。
【００３８】
ＣＰＵ１０１は、ＲＯＭ１０２又はストレージ１０４等に記憶された制御プログラムを実行するプロセッサである。
【００３９】
ＲＯＭ１０２は、制御プログラム等を保持する読み出し専用記憶領域である。
【００４０】
メインメモリ１０３は、ＣＰＵ１０１が制御プログラムを実行するときに使用するワークエリアとして用いられる揮発性の記憶領域である。
【００４１】
ストレージ１０４は、制御プログラム、及び、コンテンツなどを保持する不揮発性の記憶領域である。
【００４２】
有線ＩＦ１０５は、ＬＡＮ４０に通信可能に接続される有線通信インタフェースである。有線ＩＦ１０５は、ＬＡＮ４０に接続することができる通信規格に適合するものであればよく、例えば、ＩＥＥＥ８０２．３規格などに適合する有線ＬＡＮの通信インタフェースであり、有線通信信号の生成回路及び端子等を有する。
【００４３】
無線ＩＦ１０６は、端末２１との間で通信リンク３１を確立し、無線通信を行う無線通信インタフェースである。無線ＩＦ１０６は、例えば、ＩＥＥＥ８０２．１１ａ、ｂ、ｇ、ｎ規格等に適合する無線ＬＡＮの通信インタフェースであり、無線通信信号の生成回路及びアンテナ等を有する。
【００４４】
以降で説明する基地局１０の機能は、ＣＰＵ１０１がＲＯＭ１０２及びストレージ１０４等に記憶されたプログラムをメインメモリ１０３等を用いて実行する情報処理により実現される。その際、機能によっては、有線ＩＦ１０５又は無線ＩＦ１０６も適宜用いられる。
【００４５】
以降において、基地局１０について関連技術と対比しながら説明する。
【００４６】
図３は、関連技術に係る基地局５０の機能構成を示すブロック図である。ここで、関連技術とは、本実施の形態に係る基地局１０に関連する従来技術を指しており、基地局５０は、本実施の形態における基地局１０と同等の位置づけで配置されるものである。基地局５０のハードウェア構成は、図２に示される基地局１０のハードウェア構成と同じである。
【００４７】
図３に示されるように、基地局５０は、鍵管理部５１１と、鍵提供部５１２と、検証部５１３と、データ通信部５１４とを備える。
【００４８】
鍵管理部５１１は、基地局５０と端末２１との通信の暗号化に用いる鍵情報を保有している管理部である。鍵管理部５１１は、基地局５０と端末２１との通信の暗号化に用いる暗号鍵の元となる鍵情報であるＰＭＫ（Ｐａｉｒｗｉｓｅ Ｍａｓｔｅｒ Ｋｅｙ）を保有している。ＰＭＫは、基地局５０への接続を許可する端末だけに提供されることが想定される。基地局５０が、ＰＭＫを保有している端末による基地局５０への接続を許可し、ＰＭＫを保有していない端末による基地局５０への接続を拒否するためである。

【００４９】
また、鍵管理部５１１は、基地局５０と端末２１との通信の暗号化に用いる鍵情報であるＰＴＫ（Ｐａｉｒｗｉｓｅ Ｔｒａｎｓｉｅｎｔ Ｋｅｙ、Ｐａｉｒｗｉｓｅ Ｔｅｍｐｏｒａｌ Ｋｅｙ）をＰＭＫに基づいて生成して保有する。ＰＴＫは、ＰＭＫに基づいて所定の計算式を用いた演算により生成される。具体的には、鍵管理部５１１がＰＴＫを生成する演算は、関数ｆを用いて以下の（式１）のように表現され得る。
【００５０】
ＰＴＫ＝ｆ（ＰＭＫ，ＡＮｏｎｃｅ，ＳＮｏｎｃｅ，ＭＡＣ（５０），ＭＡＣ（２１））
（式１）
【００５１】
ここで、関数ｆは、括弧内の各変数に基づいてＰＴＫを算出するための関数である。ＡＮｏｎｃｅ及びＳＮｏｎｃｅは、それぞれ、基地局５０及び端末２１により一時的に生成される、ＰＴＫの生成のための乱数値である。また、ＭＡＣ（５０）は、基地局５０のＭＡＣアドレスを表し、ＭＡＣ（２１）は端末２１のＭＡＣアドレスを表している。なお、関数ｆは、例えばＩＥＥＥ８０２．１１ｉに定められたものを用いることができる。なお、鍵管理部５１１は、ＣＰＵ１０１等による情報処理により実現される。
【００５２】
鍵提供部５１２は、鍵管理部５１１が保有しているＰＭＫを取得し、取得したＰＭＫが端末２１に提供されるよう制御する処理部である。ＰＭＫは、端末２１と異なる通信装置にＰＭＫが取得されない通信方法により端末２１に提供される。この通信方法としては、例えば、ＷＰＳ（Ｗｉ－Ｆｉ Ｐｒｏｔｅｃｔｅｄ Ｓｅｔｕｐ）によりＰＭＫを送信する方法を用いることができ、以降ではこの場合を説明するが、本発明はこの場合に限定されない。例えば、ＷＰＳを用いる代わりに、基地局５０が表示画面（不図示）にＰＭＫを示す情報（英数字列）を表示し、基地局５０の管理者が端末２１の利用者に対して口頭又は書面により伝達し、利用者が端末２１に入力するようにしてもよい。なお、鍵提供部５１２は、ＣＰＵ１０１等、及び、無線ＩＦ１０６により実現される。
【００５３】
検証部５１３は、鍵提供部５１２が端末２１に提供したＰＭＫを端末２１が保有していることの検証を行う処理部である。この検証には、いわゆる４ウェイハンドシェイクによる方法が採用され得る。４ウェイハンドシェイクの詳細についてはＩＥＥＥ８０２．１１ｉに規定されている。以下では、本実施の形態に関連する特徴的な部分のみ説明する。
【００５４】
検証部５１３は、乱数値であるＡＮｏｎｃｅを生成し、生成したＡＮｏｎｃｅを端末２１に送信する。ＡＮｏｎｃｅを受信した端末２１は、乱数値であるＳＮｏｎｃｅを生成し、生成したＳＮｏｎｃｅと鍵提供部５１２から取得したＰＭＫとを用いて（式１）によりＰＴＫを生成する。そして、端末２１は、生成したＰＴＫ等を用いて改ざん検知のためのＭＩＣ（Ｍｅｓｓａｇｅ Ｉｎｔｅｇｒｉｔｙ Ｃｏｄｅ）を算出し、算出したＭＩＣ及びＳＮｏｎｃｅ等を検証部５１３に送信する。検証部５１３は、鍵管理部５１１が保有しているＰＭＫと、生成したＡＮｏｎｃｅと、端末２１から受信したＳＮｏｎｃｅ等から（式１）によりＰＴＫを生成し、生成したＰＴＫ等を用いてＭＩＣを算出する。そして、検証部５１３は、端末２１から受信したＭＩＣと、自身が算出したＭＩＣとが一致するか否かを判定し、一致すると判定すると、端末２１がＰＭＫを保有していることの検証が成功したと判定する。また、検証部５１３は、端末２１が行う、基地局５０がＰＭＫを保有していることの検証処理の結果を取得する。なお、検証部５１３は、ＣＰＵ１０１等による情報処理、及び、無線ＩＦ１０６により実現される。
【００５５】
データ通信部５１４は、検証部５１３による検証が成功したと判定したことを条件の１つとして、ＰＴＫに基づいて暗号化されたデータ通信を端末２１と行う処理部である。具体的には、データ通信部５１４は、検証部５１３による検証の結果、及び、端末２１によ

る検証処理の結果を取得し、これらの両方において検証が成功したことを条件としてデータ通信を行う。データ通信において、データ通信部５１４は、ＣＰＵ１０１による情報処理により生成される通信フレームを取得する。また、データ通信部５１４は、ＰＴＫを取得し、このＰＴＫの所定の一部であるＴＫ（Ｔｅｍｐｏｒａｌ　Ｋｅｙ）を取得し、取得したＴＫに基づいて通信フレームごとに異なる暗号鍵を生成し、生成した暗号鍵により通信フレームを暗号化して端末２１に送信する。また、データ通信部５１４は、端末２１が暗号化して送信した通信フレームを受信して、受信した通信フレームをＰＴＫに基づいて生成される暗号鍵により復号してＣＰＵ１０１による情報処理に提供する。なお、データ通信部５１４は、ＣＰＵ１０１等による情報処理、及び、無線ＩＦ１０６により実現される。

【００５６】

以上のように構成された基地局５０が行う処理について以降で説明する。

【００５７】

図４は、関連技術に係る基地局５０の鍵情報の導入に係る処理を示すフロー図である。図５は、関連技術に係る通信システムにおける鍵情報の導入に係る処理を示すシーケンス図である。これらを参照しながら基地局５０が行う処理について説明する。

【００５８】

まず、基地局５０は、ステップＳ５０１からＳ５０２までの処理により、同一のＰＭＫを端末２１と共有する。

【００５９】

ステップＳ５０１において、鍵提供部５１２は、鍵管理部５１１が保有しているＰＭＫを取得する。

【００６０】

ステップＳ５０２において、鍵提供部５１２は、ステップＳ５０１で取得したＰＭＫを端末２１にＷＰＳにより提供する。

【００６１】

以降、ステップＳ５０３からＳ５１０までの処理（４ウェイハンドシェイク）により、基地局５０及び端末２１が同一のＰＭＫ及びＰＴＫを保有していることが検証される。なお、基地局５０と端末２１との通信には、ＥＡＰＯＬ（Ｅｘｔｅｎｓｉｖｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ　ｏｖｅｒ　ＬＡＮ）のＥＡＰＯＬ－Ｋｅｙフレームが用いられる。

【００６２】

ステップＳ５０３において、検証部５１３は、乱数値であるＡＮｏｎｃｅを生成し、生成したＡＮｏｎｃｅを端末２１にメッセージＭ１として送信する。

【００６３】

ステップＳ５０３の後、端末２１は、上記ＡＮｏｎｃｅを受信すると、乱数値であるＳＮｏｎｃｅを生成し、ステップＳ５０２で取得したＰＭＫ、ステップＳ５０３で受信したＡＮｏｎｃｅ、生成したＳＮｏｎｃｅ、基地局５０のＭＡＣアドレス、端末２１のＭＡＣアドレスから（式１）によりＰＴＫを算出する。さらに、端末２１は、ＰＴＫに基づいてＭＩＣを算出し、ＳＮｏｎｃｅとＭＩＣとを基地局５０にメッセージＭ２として送信する（図５のステップＳ５０３Ａ）。

【００６４】

ステップＳ５０４において、検証部５１３は、端末２１がステップＳ５０３Ａで送信したＳＮｏｎｃｅとＭＩＣとを受信する。

【００６５】

ステップＳ５０５において、検証部５１３は、ステップＳ５０１で取得したＰＭＫ、ステップＳ５０３で生成したＡＮｏｎｃｅ、及び、ステップＳ５０４で受信したＳＮｏｎｃｅ等を用いて（式１）によりＰＴＫを生成する。なお、ここで生成されるＰＴＫは、端末２１のなりすまし等がなければ、端末２１で生成されるＰＴＫと同一となるものであり、この同一性が後の処理で検証される。端末２１がステップＳ５０３Ａで生成したＰＴＫと

区別するため、ステップＳ５０５で検証部５１３が生成したＰＴＫを「ＰＴＫ＿Ａ」と記載することとする。

【００６６】

ステップＳ５０６において、検証部５１３は、ステップＳ５０５で生成したＰＴＫ＿Ａを用いて、ステップＳ５０４で受信したＭＩＣの検証処理を行う。具体的には、検証部５１３は、ステップＳ５０５で算出したＰＴＫ＿Ａに基づいてＭＩＣ（上記と同様の理由からＭＩＣ＿Ａと記載する）を算出し、算出したＭＩＣ＿Ａが、ステップＳ５０４で受信したＭＩＣと同一であるか否かを判定する。ＭＩＣ＿ＡとＭＩＣとが同一であると判定した場合、ＭＩＣを算出した端末が確かに端末２１であること、及び、端末２１がＭＩＣの算出に使用したＰＴＫがＰＴＫ＿Ａと同一であることが確認され得る。

【００６７】

なお、上記検証処理において、ＭＩＣを算出した端末が確かに端末２１であり、かつ、端末２１が使用したＰＴＫがＰＴＫ＿Ａと同一であることが確認されたことを、「検証が成功した」と表現し、検証が成功しなかったことを「検証が失敗した」と表現する。

【００６８】

ステップＳ５０７において、検証部５１３は、ステップＳ５０６の検証処理において検証が成功したか否かを判定する。検証が成功した場合（ステップＳ５０７でＹｅｓ）、ステップＳ５０８に進む。一方、検証が失敗した場合（ステップＳ５０７でＮｏ）、ステップＳ５２１に進む。

【００６９】

ステップＳ５０８において、検証部５１３は、端末２１による基地局５０の認証のためのＭＩＣの検証処理の結果を取得する。検証部５１３は、ＰＭＫ、ＡＮｏｎｃｅ及びＳＮｏｎｃｅ等を用いてＰＴＫを生成し、生成したＰＴＫに基づいてＭＩＣを算出し、算出したＭＩＣを端末２１にメッセージＭ３として送信する。端末２１は、送信されたＭＩＣに対して、ステップＳ５０６で検証部５１３が行った検証処理と同様の検証処理を実行する（図５のステップＳ５０６Ａ）。端末２１は、検証処理の結果、つまり、検証が成功した、又は、検証が失敗したことを示す情報を検証部５１３にメッセージＭ４として送信する。このように端末２１が送信した検証処理の結果を、ステップＳ５０８で検証部５１３が取得する。

【００７０】

ステップＳ５０９において、検証部５１３は、ステップＳ５０８で取得した、端末２１による検証の結果が成功であるか否かを判定する。検証の結果が成功であると判定した場合（ステップＳ５０９でＹｅｓ）、ステップＳ５１０に進む。一方、検証の結果が成功でない（つまり失敗である）と判定した場合（ステップＳ５０９でＮｏ）、ステップＳ５２１に進む。

【００７１】

ステップＳ５１０において、検証部５１３は、ステップＳ５０５で生成したＰＴＫ（ＰＴＫ＿Ａ）に基づいて生成される暗号鍵をデータ通信部５１４に導入する、つまり、データ通信部５１４が上記暗号鍵をデータ通信に利用するよう制御する。このとき、端末２１は、端末２１によるＭＩＣの検証処理（図６のステップＳ５０６Ａ）で生成したＰＴＫを、端末２１のデータ通信部に導入する（図６のステップＳ５１０Ａ）。この後、基地局５０のデータ通信部５１４と端末２１のデータ通信部とは、ＰＴＫに基づいて生成される暗号鍵を用いた通信を行う（図６のステップＳ５１１）。

【００７２】

ステップＳ５２１において、検証部５１３は、４ウェイハンドシェイクを中断する。この場合、基地局５０と端末２１とは、暗号通信を行うことが禁止される。

【００７３】

上記一連の処理により、ステップＳ５０２で基地局５０が提供したＰＭＫを取得した端末２１だけが基地局５０に接続し暗号通信を行うことができる。しかしながら、ＰＭＫが漏洩し、端末２１とは異なる端末がＰＭＫを取得した場合、当該端末は、上記ステップＳ

５０３Ａ及びＳ５０６Ａの処理を、端末２１になりすまして行うことができ、その結果、基地局５０との暗号通信が可能となる。つまり、関連技術における鍵情報の導入に係る処理では、上記の手法による端末２１へのなりすましができてしまう。

【００７４】

図６は、本実施の形態に係る基地局１０の機能構成を示すブロック図である。

【００７５】

図６に示されるように、基地局１０は、鍵管理部１１１と、端末情報取得部１１２と、鍵生成部１１３と、鍵提供部１１４と、検証部１１５と、データ通信部１１６とを備える。なお、上記の各構成要素のうち、基地局５０の構成要素と同名のものは、類似の機能を有する。以下では、上記の各構成要素について、基地局５０における同名の構成要素と異なる点を主に説明する。

【００７６】

鍵管理部１１１は、鍵管理部５１１と同様、基地局１０と端末２１との通信の暗号化に用いる鍵情報を保有している管理部である。鍵管理部１１１は、ＰＭＫを保有している。このＰＭＫは、基地局５０の鍵管理部５１１が保有しているＰＭＫと同等のものであるが、端末２１に提供されることは想定されていない。

【００７７】

また、鍵管理部１１１は、後述する鍵生成部１１３がＰＭＫに基づいて生成する、基地局１０と端末２１との通信の暗号化に用いる暗号鍵の元となる鍵情報であるＰＭＫ１を保有しており、さらに、ＰＭＫ１に基づいて以下の（式２）を用いた演算により算出されるＰＴＫ１を保有する。

【００７８】

ＰＴＫ１＝ｆ（ＰＭＫ１，ＡＮｏｎｃｅ，ＳＮｏｎｃｅ，ＭＡＣ（１０），ＭＡＣ（２１））

（式２）

【００７９】

なお、（式２）における関数ｆは、（式１）における関数ｆと同じである。なお、ＰＭＫは、第一鍵情報に相当し、ＰＭＫ１は、第二鍵情報に相当する。

【００８０】

端末情報取得部１１２は、端末２１に固有の識別情報を取得する処理部である。識別情報は、仮に端末２１と同種の端末が複数存在する場合に、これらのうちから端末２１の個体を一意に特定し得る情報であり、例えば、端末２１のハードウェアアドレス（ＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレス）（以降、「ＭＡＣ（２１）」と記載）を用いることができる。なお、上記識別情報は、端末２１から受信する通信フレームのヘッダから取得してもよいし、端末２１のハードウェアアドレスとして管理されている情報が管理者により入力されることによって、取得してもよい。

【００８１】

鍵生成部１１３は、鍵管理部１１１が保有しているＰＭＫと、端末情報取得部１１２が取得した端末２１の識別情報とを用いた演算により、基地局１０と端末２１との通信の暗号化に用いる暗号鍵の元となる情報であるＰＭＫ１を生成する処理部である。ＰＭＫ１は、端末ごとに対応付けられたＰＭＫとしての役割を有する。鍵生成部１１３は、鍵管理部１１１からＰＭＫを取得し、端末情報取得部１１２から端末２１の識別情報を取得する。そして、所定のアルゴリズム、より具体的には、以下の（式３）に示される演算（第一演算に相当）によりＰＭＫ１を算出する。

【００８２】

ＰＭＫ１＝ｈ（ＰＭＫ，ＭＡＣ（２１））　　（式３）

【００８３】

ここで、関数ｈは、関数の値がＰＭＫとして用いられ得るものであれば、任意の関数を用いることができる。なお、関数ｈとして、演算結果つまり関数の値から引数を求めることがきわめて困難又は実質的に不可能である一方向関数、より具体的には、ハッシュ関数

を用いることも可能である。この場合、例えば、（式３）の代わりに、（式３）をより具体化した（式４）を用いてＰＭＫ１を算出することになる。

【００８４】

ＰＭＫ１＝ｈａｓｈ（ＰＭＫ＋ＭＡＣ（２１））　　（式４）

【００８５】

ここで、関数ｈａｓｈは、ハッシュ関数である。ハッシュ関数を用いれば、さらに、ＰＭＫ１からＰＭＫを導出することが実質的に不可能であることにより、ＰＭＫが外部に漏洩するリスクを低減することができる利点がある。以降では関数ｈがハッシュ関数である例を説明する。

【００８６】

鍵提供部１１４は、鍵管理部１１１が管理しているＰＭＫ１を取得し、ＰＭＫ１が端末２１に提供されるよう制御する処理部である。端末２１にＰＭＫ１が提供される方法は、関連技術において鍵提供部５１２により端末２１にＰＭＫが提供される方法と同様であり、例えばＷＰＳが用いられる。このように、鍵提供部１１４がＰＭＫではなくＰＭＫ１を端末２１に提供するので、基地局１０によりＰＭＫが外部に漏洩するリスクが低減されている。

【００８７】

検証部１１５は、端末２１がＰＭＫ１を保有していることの検証を行う処理部である。検証部１１５による検証の方法は、関連技術において端末２１がＰＭＫを保有していることを検証部５１３が検出する方法と類似しているが、ＭＩＣの検証処理において、ＭＩＣを含む通信フレームから得られる端末２１の識別情報を用いる点で異なる。

【００８８】

具体的には、検証部１１５は、乱数値であるＡＮｏｎｃｅを生成し、生成したＡＮｏｎｃｅを端末２１に送信する。ＡＮｏｎｃｅを受信した端末２１は、乱数値であるＳＮｏｎｃｅを生成し、生成したＳＮｏｎｃｅと、鍵提供部１１４から取得したＰＭＫ１とを用いて（式２）によりＰＴＫ１を生成する。そして、生成したＰＴＫ１と、検証部１１５から受信したＡＮｏｎｃｅとによりＭＩＣを算出し、算出したＭＩＣ及びＳＮｏｎｃｅ等を検証部１１５に送信する。なお、ＡＮｏｎｃｅは第一情報に相当し、ＭＩＣは第二情報に相当する。

【００８９】

検証部１１５は、端末２１が送信したＭＩＣ及びＳＮｏｎｃｅと、端末２１のＭＡＣアドレスを取得する。なお、ここで取得するＭＡＣアドレスのことを、端末情報取得部１１２が取得するものと区別するために、ＭＡＣ（２１）＿Ａと記載する。なお、検証部１１５は、端末２１が送信したＭＩＣ及びＳＮｏｎｃｅを含む通信フレームのヘッダに含まれる送信元アドレスフィールドから端末２１のＭＡＣアドレスを取得してもよい。このようにすると、端末２１がＰＭＫ１を保有していることの検証に用いられる通信フレームのアドレスフィールドを用いて、より具体的かつ確実に、端末のなりすましを抑制することができる利点がある。

【００９０】

検証部１１５は、鍵管理部１１１が保有しているＰＭＫ１と、検証部１１５が取得したＭＡＣ（２１）＿Ａとを用いて（式２）によりＰＴＫ１を生成し、生成したＰＴＫ１と、生成したＡＮｏｎｃｅとによりＭＩＣ（ＭＩＣ＿Ａ）を算出する。そして、検証部１１５は、ＭＩＣとＭＩＣ＿Ａとが一致するか否かを判定し、一致すると判定すると、端末２１がＰＭＫ１を保有していることの検証が成功したと判定する。なお、ＭＩＣ＿Ａは第三情報に相当する。

【００９１】

データ通信部１１６は、検証部１１５による検証が成功したと判定したことを条件の１つとして、ＰＴＫ１により暗号化されたデータ通信を端末２１と行う処理部である。具体的には、データ通信部１１６は、検証部１１５による検証の結果、及び、端末２１による検証処理の結果を取得し、これらの両方において検証が成功したことを条件としてデータ

通信を行う。
【００９２】
以上のように構成された基地局１０が行う処理について以降で説明する。
【００９３】
図７は、本実施の形態に係る基地局１０の鍵情報の導入に係る処理を示すフロー図である。図８は、本実施の形態に係る通信システムにおける鍵情報の導入に係る処理であって、ＭＩＣの検証処理が成功する場合を示すシーケンス図である。
【００９４】
まず、基地局１０は、ステップＳ１０１からＳ１０４までの処理により、端末２１との通信に用いる暗号鍵の元となる情報であるＰＭＫ１を端末２１と共有する。
【００９５】
ステップＳ１０１において、鍵提供部１１４は、鍵管理部１１１が保有しているＰＭＫを取得する。
【００９６】
ステップＳ１０２において、端末情報取得部１１２は、端末２１の識別情報であるＭＡＣ（２１）を取得する。
【００９７】
ステップＳ１０３において、鍵生成部１１３は、ＰＭＫとＭＡＣ（２１）とから（式３）によりＰＭＫ１を生成する。
【００９８】
ステップＳ１０４において、鍵提供部１１４は、ステップＳ１０３で鍵生成部１１３が生成したＰＭＫ１を端末２１にＷＰＳにより提供する。
【００９９】
以降、ステップＳ１０５からＳ１１２までの処理（４ウェイハンドシェイク）により、基地局１０及び端末２１が同一のＰＭＫ１及びＰＴＫ１を保有していることが検証される。
【０１００】
ステップＳ１０５において、検証部１１５は、乱数値であるＡＮｏｎｃｅを生成し、生成したＡＮｏｎｃｅを端末２１にメッセージＭ１として送信する。
【０１０１】
ステップＳ１０５の後、端末２１は、上記ＡＮｏｎｃｅを受信すると、乱数値であるＳＮｏｎｃｅを生成し、ＰＭＫ１、ＡＮｏｎｃｅ、ＳＮｏｎｃｅ、基地局１０のＭＡＣアドレス、自装置（端末２１）のＭＡＣアドレスから（式２）によりＰＴＫ１を算出する。さらに、端末２１は、ＰＴＫ１に基づいて改ざん防止のためのＭＩＣを算出し、ＳＮｏｎｃｅとＭＩＣとを基地局１０にメッセージＭ２として送信する（図８のステップＳ１０５Ａ）。
【０１０２】
ステップＳ１０６において、検証部１１５は、端末２１がステップＳ１０５Ａで送信したＳＮｏｎｃｅとＭＩＣとＭＡＣ（２１）＿Ａとを受信する。なお、検証部１１５は、ＭＡＣ（２１）＿Ａを、端末２１が送信した通信フレームのヘッダから取得することで受信し得る。ここで、ＭＡＣ（２１）＿Ａは、端末２１のＭＡＣアドレスであるが、前述のとおり、端末情報取得部１１２が取得するものと区別するために、ＭＡＣ（２１）＿Ａと記載している。
【０１０３】
ステップＳ１０７において、検証部１１５は、ステップＳ１０５で生成したＡＮｏｎｃｅ、ステップＳ１０６で受信したＳＮｏｎｃｅ及びＭＡＣ（２１）＿Ａ等に基づいて、ＰＴＫ１を生成する。なお、ここで生成するＰＴＫ１は、端末２１のなりすまし等がなければ、端末２１で生成されるＰＴＫ１と同一となるものであり、この同一性が後の処理で検証される。よって、ステップＳ１０７で生成されたＰＴＫ１を「ＰＴＫ１＿Ａ」と記載することとする。

【０１０４】
ステップＳ１０８において、検証部１１５は、ステップＳ１０７で生成したＰＴＫ１＿Ａを用いて、ステップＳ１０６で受信したＭＩＣの検証処理を行う。具体的には、検証部１１５は、検証処理において、（式３）を用いてＰＭＫ１＿Ａを算出し、（式２）を用いてＰＴＫ１＿Ａを算出し、算出したＰＴＫ１＿Ａに基づいて、ＭＩＣの演算を行ったのが端末２１であること、及び、端末２１が使用したＰＴＫ１がＰＴＫ１＿Ａと同一であることが確認され得る。
【０１０５】
ステップＳ１０９において、検証部１１５は、ステップＳ１０８の検証処理において検証が成功したか否かを判定する。検証が成功した場合（ステップＳ１０９でＹｅｓ）、ステップＳ１１０に進む。一方、検証が失敗した場合（ステップＳ１０９でＮｏ）、ステップＳ１２１に進む。
【０１０６】
ステップＳ１１０において、検証部１１５は、端末２１による基地局１０の認証のためのＭＩＣの検証処理の結果を取得する。検証部１１５は、ＡＮｏｎｃｅ及びＳＮｏｎｃｅを用いてＰＴＫ１を算出し、算出したＰＴＫ１に基づいてＭＩＣを算出し、算出したＭＩＣを端末２１にメッセージＭ３として送信する（図８のステップＳ１０８Ａ）。端末２１は、送信されたＭＩＣに対して、ステップＳ１０７で検証部１１５が行った検証処理と同様の検証処理を実行し、その結果（検証が成功した、又は、検証が失敗した）を検証部１１５にメッセージＭ４として送信する。このように端末２１が送信した、検証処理の結果を、ステップＳ１１０で検証部１１５が取得する。
【０１０７】
ステップＳ１１１において、検証部１１５は、ステップＳ１１０で取得した、端末２１による検証の結果が成功であるか否かを判定する。検証の結果が成功であると判定した場合（ステップＳ１１１でＹｅｓ）、ステップＳ１１２に進む。一方、検証の結果が成功でない（つまり失敗である）と判定した場合（ステップＳ１１１でＮｏ）、ステップＳ１２１に進む。
【０１０８】
ステップＳ１１２において、検証部１１５は、ステップＳ１０７で生成したＰＴＫ１（ＰＴＫ１＿Ａ）をデータ通信部１１６に導入する、つまり、データ通信部１１６がデータ通信に利用する暗号鍵としてＰＴＫ１を用いるよう制御する。このとき、端末２１は、端末２１によるＭＩＣの検証処理（図８のステップＳ１０８Ａ）で生成したＰＴＫ１を、端末２１のデータ通信部に導入する（図８のステップＳ１１２Ａ）。この後、基地局１０のデータ通信部１１６と端末２１のデータ通信部とは、ＰＴＫ１を暗号鍵として用いた通信を行う（図８のステップＳ１１３）。
【０１０９】
ステップＳ１２１において、検証部１１５は、４ウェイハンドシェイクを中断する。この場合、基地局１０と端末２１とは、暗号通信を行うことができない。
【０１１０】
上記一連の処理において、ステップＳ１０４で基地局１０が送信したＰＭＫ１を取得した端末２１が基地局１０に接続し暗号通信を行うことができる。一方、ステップＳ１０４で基地局１０が送信したＰＭＫ１を、端末２１とは異なる端末が何らかの方法で取得したとしても、この端末は、端末２１になりすまして基地局１０との暗号通信を行うことはできない。このことを以下で説明する。
【０１１１】
図９は、実施の形態に係る通信システムにおける鍵情報の導入に係る処理であって、ＭＩＣの検証が失敗する場合を示すシーケンス図である。図９は、端末２２が、端末２１に提供されるべきＰＭＫ１を取得して、端末２１になりすまして基地局１０に接続することを試みて失敗することを示した図である。
【０１１２】

ステップＳ１０４Ｂにおいて、端末２２は、ステップＳ１０２で基地局１０が生成したＰＭＫ１を何らかの方法で取得する。

【０１１３】

ステップＳ１０５Ｂにおいて、端末２２は、基地局１０がステップＳ１０５で送信したＡＮｏｎｃｅを受信すると、乱数値であるＳＮｏｎｃｅを生成し、ＰＭＫ１、ＡＮｏｎｃｅ、ＳＮｏｎｃｅ、基地局１０のＭＡＣアドレス、端末２２のＭＡＣアドレスから所定の計算式に基づいてＰＴＫ（以降、「ＰＴＫ２」と記載）を算出する。さらに、端末２２は、ＰＴＫ２に基づいて改ざん防止のためのＭＩＣを算出し、ＳＮｏｎｃｅとＭＩＣとを基地局１０にメッセージＭ２Ａとして送信する。

【０１１４】

ステップＳ１０８において、検証部１１５は、ステップＳ１０７で生成したＰＴＫ２＿Ａを用いて、ステップＳ１０５Ｂで端末２２が送信したＭＩＣの検証処理を行う。具体的には、検証部１１５は、検証処理において、（式３）を用いてＰＭＫ２＿Ａを算出し、（式２）を用いてＰＴＫ２＿Ａを算出し、算出したＰＴＫ２＿Ａに基づいて、端末２２が生成したＰＴＫ２がＰＴＫ２＿Ａと一致しないことを確認することで、検証が失敗する。その後、４ウェイハンドシェイクは中断される（ステップＳ１２１）。

【０１１５】

このように、端末２１の識別情報に基づいて生成されたＰＭＫ１を、端末２１と異なる端末である端末２２が取得したとしても、端末２２と基地局１０との４ウェイハンドシェイクにおいて検証が失敗し、端末２２は基地局１０との暗号通信を行うことができない。つまり、端末２２が、端末２１になりすまして基地局１０に接続することが禁止される。

【０１１６】

図１０は、本実施の形態に係る無線通信システム１における各装置が保有し又は使用する鍵情報とを示す説明図である。

【０１１７】

図１０に示されるように、基地局１０は、ＰＭＫと、ＰＭＫ１及びＰＭＫ２と、ＰＴＫ１及びＰＴＫ２を保有している。ＰＭＫは、通信の暗号鍵の元となる情報であり、基地局１０の外部に漏洩しないことが想定される情報である。ＰＭＫ１及びＰＭＫ２は、それぞれ、基地局１０と端末２１との間、及び、基地局１０と端末２２との間の通信の暗号鍵の元となる情報である。ＰＴＫ１及びＰＴＫ２は、ＰＭＫ１及びＰＭＫ２それぞれに基づいて４ウェイハンドシェイクにより生成されたものである。

【０１１８】

端末２１は、ＰＭＫ１及びＰＴＫ１を保有している。これらは、基地局１０が保有しているものと共通である。ＰＭＫ１は、例えばＷＰＳで基地局１０から提供されたものであり、ＰＴＫ１は、４ウェイハンドシェイクにより生成されたものである。

【０１１９】

端末２２は、ＰＭＫ２及びＰＴＫ２を保有している。これらは、基地局１０が保有しているものと共通である。ＰＭＫ２は、例えばＷＰＳで基地局１０から提供されたものであり、ＰＴＫ２は、４ウェイハンドシェイクにより生成されたものである。

【０１２０】

基地局１０と端末２１との間で確立される通信リンク３１では、ＰＴＫ１に基づく暗号通信が行われる。基地局１０と端末２２との間で確立される通信リンク３２では、ＰＴＫ２に基づく暗号通信が行われる。

【０１２１】

このようにして、端末２１と異なる端末が端末２１になりすまして基地局１０との間で暗号通信をすることが抑制される。このとき、たとえＰＭＫ１が外部に漏洩したとしてもＰＭＫ１を取得した端末が基地局１０との暗号通信を行うことはできない。基地局１０との暗号通信を行うためには、ＰＭＫ１と端末２１のＭＡＣアドレスとの両方が必要であるからである。

【０１２２】

また、仮にＰＭＫ１とＰＭＫ１の生成アルゴリズム（上記説明における関数ｈ）とが漏洩したとしても、生成アルゴリズムが一方向関数による演算を含む場合には、端末２１と異なる端末が端末２１になりすまして基地局１０との間で暗号通信をすることはできない。ＰＭＫ１とＰＭＫ１の生成アルゴリズムとを用いても、ＰＭＫを算出することが実質的に不可能であるので、端末２１と異なる端末が使用すべき暗号鍵を生成することが実質的に不可能であるからである。

【０１２３】

このようにして、基地局１０は、導入コストを抑えながら端末のなりすましを抑制することができる。

【０１２４】

以上のように、本実施の形態の基地局は、無線端末の識別情報に基づいて生成された第二鍵情報を用いて、無線端末の正当性を検証することができる。具体的には、無線基地局装置は、無線端末の識別情報を考慮して第二鍵情報を生成し、また、当該無線基地局装置に接続しようとする無線端末が正当な鍵情報を有することを無線端末の識別情報を考慮して行う。これにより、一の無線端末の識別情報を考慮して生成された第二鍵情報を、他の無線端末が使用して無線基地局装置に接続することができなくなる。また、本発明の無線基地局装置に接続しようとする端末は、従来の端末の機能だけで十分であり、本発明の無線基地局装置に接続するための特別な機能を要しない。よって、本発明の無線基地局装置は、導入コストを抑えながら端末のなりすましを抑制することができる。

【０１２５】

また、無線基地局装置は、第二鍵情報から、当該第二鍵情報を生成するために利用した第一鍵情報を得ることが実質的に不可能である。よって、第一鍵情報が無線基地局装置の外部に漏洩することが抑制される。これにより、端末のなりすましをより一層抑制することができる。

【０１２６】

また、無線基地局装置は、端末が第二鍵情報を保有していることを具体的に検証することができる。よって、無線基地局装置は、端末のなりすましの抑制をより具体的に実現することができる。

【０１２７】

また、無線基地局装置は、端末が第二鍵情報を保有していることの検証に用いられる通信フレームのアドレスフィールドを用いて、より具体的かつ確実に、端末のなりすましを抑制することができる。

【０１２８】

また、無線基地局装置は、端末のハードウェアアドレスを用いてより具体的に端末のなりすましを抑制することができる。

【０１２９】

以上、本発明の無線基地局装置について、実施の形態に基づいて説明したが、本発明は、この実施の形態に限定されるものではない。本発明の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、本発明の範囲内に含まれる。

【産業上の利用可能性】

【０１３０】

本発明は、導入コストを抑えながら端末のなりすましを抑制する基地局装置等に適用可能である。

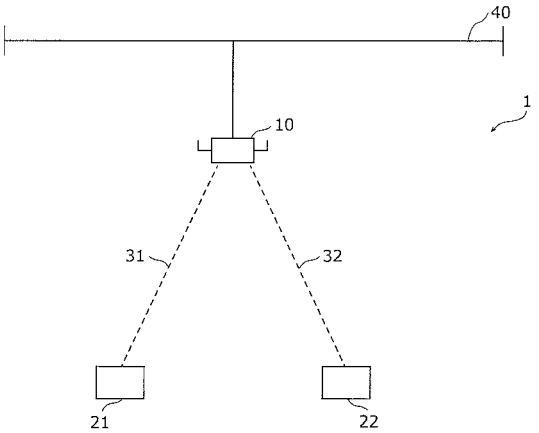
【符号の説明】

【０１３１】

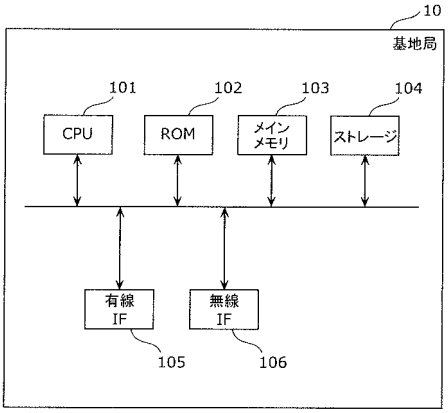
１　　無線通信システム
１０、５０　　基地局
２１、２２　　端末
３１、３２　　通信リンク

４０　　ＬＡＮ
１０１　　ＣＰＵ
１０２　　ＲＯＭ
１０３　　メインメモリ
１０４　　ストレージ
１０５　　有線ＩＦ
１０６　　無線ＩＦ
１１１、５１１　　鍵管理部
１１２　　端末情報取得部
１１３　　鍵生成部
１１４、５１２　　鍵提供部
１１５、５１３　　検証部
１１６、５１４　　データ通信部
Ｍ１、Ｍ２、Ｍ２Ａ、Ｍ３、Ｍ４　　メッセージ

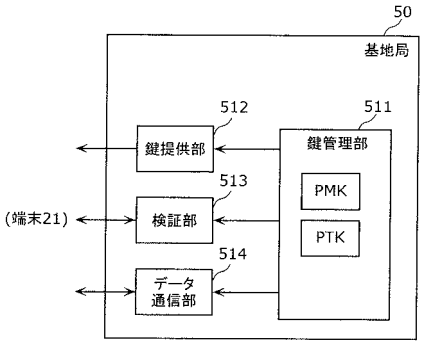
【図１】



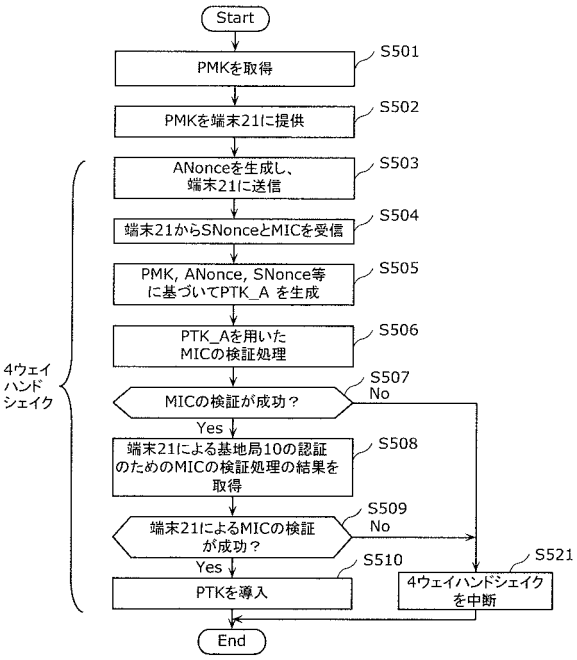
【図２】



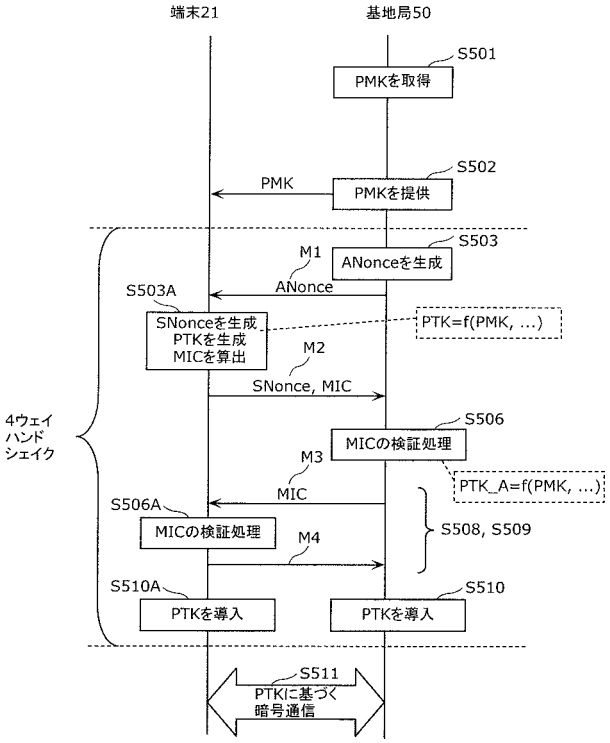
【図３】



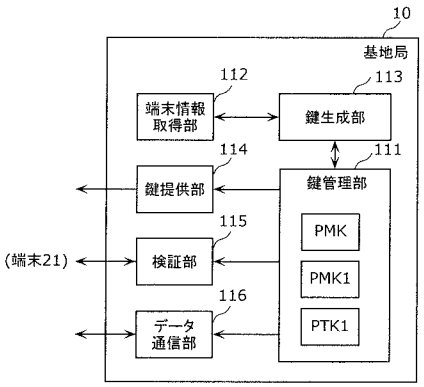
【図４】


Start
PMKを取得
S501
PMKを端末21に提供
S502
ANonceを生成し、
端末21に送信
S503
端末21からSNonceとMICを受信
S504
PMK, ANonce, SNonce等
に基づいてPTK_A を生成
S505
PTK_Aを用いた
MICの検証処理
S506
MICの検証が成功？
S507
No
Yes
端末21による基地局10の認証
のためのMICの検証処理の結果を
取得
S508
端末21によるMICの検証
が成功？
S509
No
Yes
PTKを導入
S510
4ウェイハンドシェイク
を中断
S521
End
4ウェイ
ハンド
シェイク

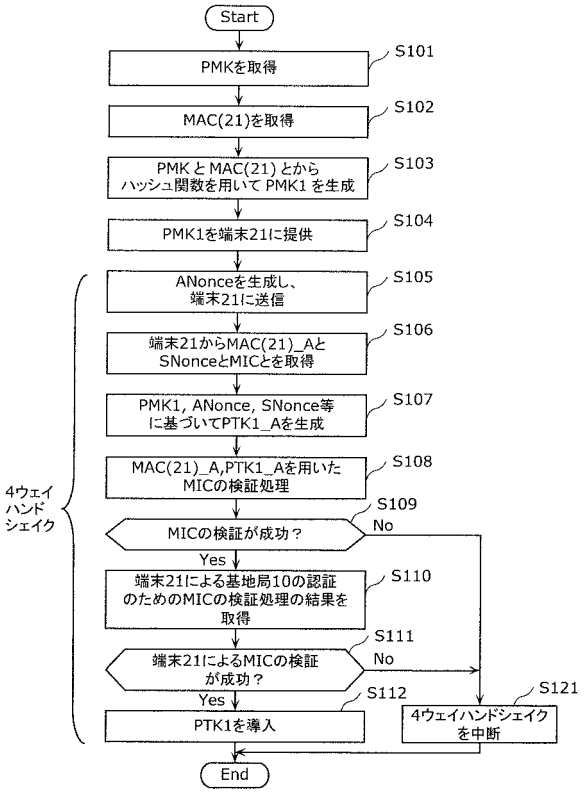
【図５】


端末21
基地局50
S501
PMKを取得
PMK
S502
PMKを提供
M1
S503
ANonceを生成
ANonce
S503A
SNonceを生成
PTKを生成
MICを算出
PTK=f(PMK, ...)
M2
SNonce, MIC
4ウェイ
ハンド
シェイク
S506
MICの検証処理
M3
PTK_A=f(PMK, ...)
MIC
S506A
MICの検証処理
S508, S509
M4
S510A
PTKを導入
S510
PTKを導入
S511
PTKに基づく
暗号通信

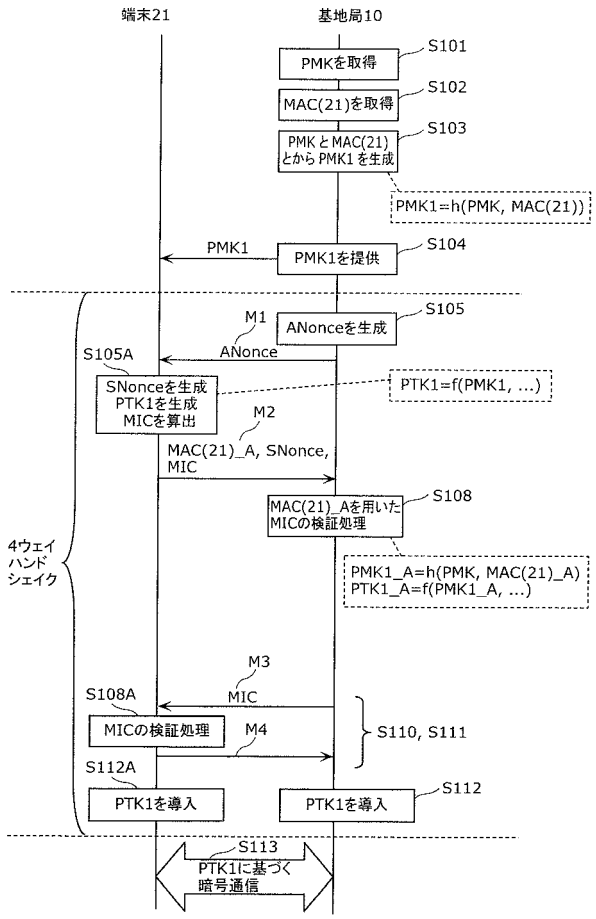
【図６】


10
基地局
112
端末情報
取得部
113
鍵生成部
114
鍵提供部
111
鍵管理部
115
検証部
PMK
PMK1
116
データ
通信部
PTK1
(端末21)

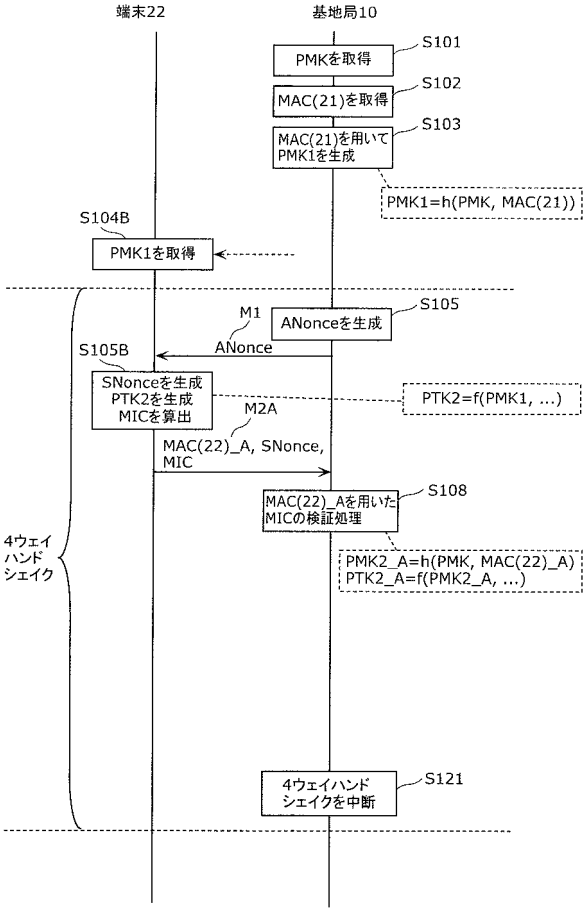
【図７】


Start
PMKを取得
S101
MAC(21)を取得
S102
PMKとMAC(21)とから
ハッシュ関数を用いて PMK1 を生成
S103
PMK1を端末21に提供
S104
ANonceを生成し、
端末21に送信
S105
端末21からMAC(21)_AとSNonceとMICとを取得
S106
PMK1, ANonce, SNonce等
に基づいてPTK1_Aを生成
S107
MAC(21)_A,PTK1_Aを用いた
MICの検証処理
S108
4ウェイ
ハンド
シェイク
MICの検証が成功？
S109
No
Yes
端末21による基地局10の認証
のためのMICの検証処理の結果を
取得
S110
端末21によるMICの検証
が成功？
S111
No
Yes
PTK1を導入
S112
4ウェイハンドシェイク
を中断
S121
End

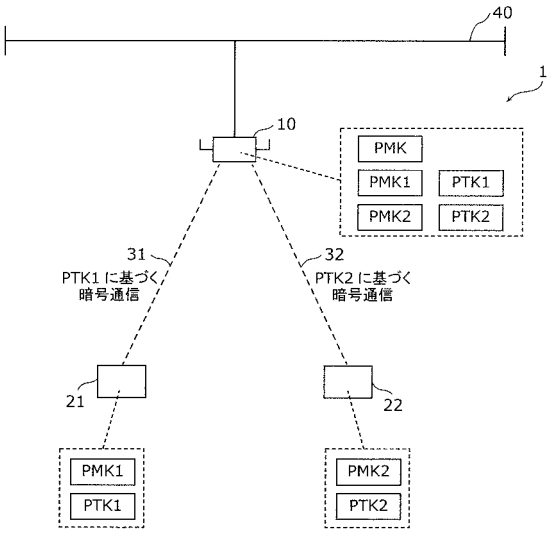
【図８】


端末21
基地局10
PMKを取得
S101
MAC(21)を取得
S102
PMKとMAC(21)とからPMK1を生成
S103
PMK1=h(PMK, MAC(21))
PMK1
PMK1を提供
S104
M1
ANonceを生成
S105
ANonce
S105A
SNonceを生成
PTK1を生成
MICを算出
PTK1=f(PMK1, ...)
M2
MAC(21)_A, SNonce, MIC
MAC(21)_Aを用いたMICの検証処理
S108
PMK1_A=h(PMK, MAC(21)_A)
PTK1_A=f(PMK1_A, ...)
4ウェイハンドシェイク
M3
MIC
S108A
MICの検証処理
M4
S110, S111
S112A
PTK1を導入
PTK1を導入
S112
S113
PTK1に基づく暗号通信

【図９】


端末22
基地局10
PMKを取得
S101
MAC(21)を取得
S102
MAC(21)を用いてPMK1を生成
S103
PMK1=h(PMK, MAC(21))
S104B
PMK1を取得
M1
ANonceを生成
S105
ANonce
S105B
SNonceを生成
PTK2を生成
MICを算出
PTK2=f(PMK1, ...)
M2A
MAC(22)_A, SNonce, MIC
MAC(22)_Aを用いたMICの検証処理
S108
PMK2_A=h(PMK, MAC(22)_A)
PTK2_A=f(PMK2_A, ...)
4ウェイハンドシェイク
4ウェイハンドシェイクを中断
S121

【図１０】


40
1
10
PMK
PMK1
PTK1
PMK2
PTK2
31
PTK1 に基づく暗号通信
32
PTK2 に基づく暗号通信
21
22
PMK1
PTK1
PMK2
PTK2