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

特許第4713955号
(P4713955)

(45)発行日　平成23年6月29日(2011.6.29)　(24)登録日　平成23年4月1日(2011.4.1)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
H04W 12/06	(2009.01)	H04Q	7/00	183
H04W 76/02	(2009.01)	H04Q	7/00	581
H04W 92/10	(2009.01)	H04Q	7/00	686

請求項の数 10　(全 19 頁)

(21)出願番号　特願2005-172146 (P2005-172146)
(22)出願日　平成17年6月13日 (2005.6.13)
(65)公開番号　特開2006-352225 (P2006-352225A)
(43)公開日　平成18年12月28日 (2006.12.28)
審査請求日　平成19年10月30日 (2007.10.30)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100075513
弁理士　後藤　政喜
(74)代理人　100084537
弁理士　松田　嘉夫
(74)代理人　100114236
弁理士　藤井　正弘
(72)発明者　大河内　俊夫
東京都国分寺市東恋ヶ窪一丁目２８０番地
株式会社日立製作所　中央研究所内

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】認証システム、無線通信端末及び無線基地局

(57)【特許請求の範囲】

【請求項１】

無線通信端末と、前記無線通信端末と無線通信を行う基地局と、前記無線通信端末と前記基地局との間の通信を管理する管理サーバと、を備える認証システムにおいて、

前記無線通信端末は、前記基地局と情報を送受信する端末側送受信部と、前記基地局との間で認証処理を行う端末側認証処理部と、クーポン公開部とクーポン秘密部とを含む電子クーポンを記録する端末側記録部と、を備え、

前記基地局は、前記無線通信端末と情報を送受信する基地局側送受信部と、基地局側記録部と、前記無線通信端末との間で認証処理を行う基地局側認証処理部と、を備え、

前記管理サーバは、

乱数ｓを生成し、生成されたｓを端末秘密鍵とし、

$v = g^{-s} \bmod p$によって端末公開鍵ｖを計算し、この値ｇ及びｐはクーポン生成用のパラメータであって、

乱数ｘを生成し、生成されたｘを前記クーポン秘密部とし、$t = g^{x} \bmod p$によって前記クーポン公開部ｔを計算し、前記電子クーポンを生成し、

前記計算された端末公開鍵ｖを前記基地局に送信し、

前記生成された端末秘密鍵ｓ及び前記生成された電子クーポンを前記無線通信端末に送信し、

前記基地局側記録部は、端末公開鍵ｖを記録し、

前記端末側記録部は、複数の電子クーポンを記録し、

前記端末側送受信部は、前記複数の電子クーポンのうち一のクーポン公開部を前記基地局に送信し、当該クーポン公開部の電子クーポンを無効と設定し、
前記端末側送受信部は、一つの端末認証鍵ＩＤ及び一つのクーポン公開部ｔを含む接続要求を、前記基地局に送信し、
前記基地局側認証処理部は、接続要求を受信すると乱数ｃを生成し、生成した乱数ｃを前記無線通信端末に送信し、
前記端末側認証処理部は、受信した乱数ｃ、クーポン秘密部ｘ及び端末秘密鍵ｓに基づいて、応答値ｙ＝ｘ＋ｓｃを計算し、計算された応答値ｙを前記無線基地局に送信し、
前記基地局側認証処理部は、受信した応答値ｙ、乱数ｃ及び端末公開鍵ｖに基づいて、$g^{y}v^{c}$ｍｏｄ　ｐを計算し、前記計算結果がクーポン公開部ｔと一致するか否かを判定することを特徴とする認証システム。
【請求項２】
前記端末側記録部は、複数の端末秘密鍵を記録し、
前記端末側認証処理部は、前記複数の端末秘密鍵から一の端末秘密鍵を選択して認証処理を行うことを特徴とする請求項１に記載の認証システム。
【請求項３】
前記管理サーバは、
前記端末側記録部に記録された前記電子クーポンの数が所定の数以下になると新たな電子クーポンを生成し、
前記生成された新たな電子クーポンを前記無線通信端末に送信し、
前記無線通信端末は、受信した前記電子クーポンを前記端末側記録部に記録することを特徴とする請求項１又は２に記載の認証システム。
【請求項４】
前記無線通信端末が予め定められた前記基地局と接続している場合に、前記新たな電子クーポンが生成されることを特徴とする請求項３に記載の認証システム。
【請求項５】
前記管理サーバは、前記新たな電子クーポンにメッセージ認証コードを付加して前記無線通信端末に送信し、
前記無線通信端末は、受信した前記電子クーポンのメッセージ認証コードが、予め有するメッセージ認証鍵によって生成したメッセージ認証コードと一致するか否かを判定することを特徴とする請求項３に記載の認証システム。
【請求項６】
前記無線通信端末は、起動時に前記管理サーバに登録を要求し、
前記管理サーバは、
前記登録の要求を受信すると、前記無線通信端末の固有の識別情報及び前記認証用秘密鍵を生成し、
当該無線通信端末の固有の識別情報及び当該端末秘密鍵を前記無線通信端末に送信し、
前記無線通信端末は、前記無線通信端末の固有の識別情報及び前記端末秘密鍵を受信すると、当該無線通信端末の固有の識別情報及び当該端末秘密鍵を前記端末側記録部に記録することを特徴とする請求項１又は２に記載の認証システム。
【請求項７】
請求項１に記載の認証システムの無線通信端末。
【請求項８】
前記無線通信端末の前記記録部に記録された有効な電子クーポンの数を表示する情報表示画面を備えることを特徴とする請求項７に記載の無線通信端末。
【請求項９】
請求項１に記載の認証システムの基地局。
【請求項１０】
前記管理サーバは、予め定められた桁数の任意の素数ｐ、及び、ｐよりも小さい素数であってｐ－１の素因数となる素数ｑを、クーポン生成のためのパラメータとして生成する

ことを特徴とする請求項１に記載の認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線基地局による無線通信端末の認証システムに関し、特に、使い捨て型認証情報を用いる認証システムに関する。
【背景技術】
【０００２】
近年、多数の無線通信端末が近距離無線通信によって接続されるセンサネットが普及している。このセンサネットでは、偽造された無線通信端末による不正なデータの流入や、通信資源の占有による稼働妨害が問題となっている（例えば、非特許文献１参照）。
【０００３】
これらの不正なアクセスを排除するためには、無線基地局が無線通信端末の認証を厳格に行い、不正な端末がネットワークに接続要求してきた段階でこれを排除する必要がある。
【０００４】
そこで、認証の度にパスワードが変更されるワンタイム・パスワード認証方式を用いた無線通信端末の認証システムが提案されている（例えば、特許文献１参照）。
【０００５】
また、繰り返して使用することができない使い捨て型の電子クーポンを、交通チケット等において利用する技術が提案されている（例えば、非特許文献２参照）。
【特許文献１】特開２００４－２８２２９５号公報
【非特許文献１】James Newsome and Elaine Shi and Dawn Song and Adrian Perrig "The sybil attack in sensor networks: analysis & defenses", IPSN'04: Proceedings of the third international symposium on Information processing in sensor networks, Berkeley, California, USA, 2004, ISBN1-58113-846-6, p.259-268, ACM Press
【非特許文献２】Poupard and J.Stern “Security analysis of a practical ‘on the fly' authentication and signature generation, Advances in cryptology - Eurocrypt '98, Lecture Notes in Computer Science 1403, Springer-Verlag” 1998, p.422-436
【発明の開示】
【発明が解決しようとする課題】
【０００６】
ワンタイム・パスワード認証方式の基本的なものとして、チャレンジ－レスポンス型が挙げられる。チャレンジ－レスポンス型の認証方式では、無線通信端末が固有の暗号鍵を所持していることを確認することで、端末の個体識別及び認証を行う。
【０００７】
このチャレンジ－レスポンス型は、秘密鍵暗号を用いる方法と公開鍵暗号を用いる方法とに分けられる。
【０００８】
秘密鍵暗号を用いる方法では、無線通信端末の秘密鍵を予め無線基地局が所持していなければならない。しかし、車載センサ等を用いた広域のセンサネットにおいては、無線通信端末が複数の無線基地局を跨って移動する。このような運用形態では、多数の無線基地局に端末の秘密鍵を予め配布しなければならず、秘密鍵の漏洩の危険性が高くなるという問題がある。
【０００９】
一方、公開鍵暗号を用いる方法は、予め無線通信端末と無線基地局との間で秘密鍵を共有する必要がない。よって、無線通信端末は、移動先のいずれの無線基地局とも通信が可能である。
【００１０】
しかし、公開鍵暗号を用いる方法では、認証の際の暗号処理が複雑化して端末が実行す

べき計算量が大きくなる。そうすると、小型バッテリや太陽電池、発電素子で稼働する小型無線通信端末では処理が実行しきれず、適用が困難という問題がある。よって、広域を移動する小型無線通信端末に適用可能であって、当該端末がいずれの無線基地局とも通信可能な認証システムが望まれている。

【００１１】

そこで、本発明は、使い捨て型認証情報を用いた運用の安全性の高い無線通信端末の認証システム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】

【００１２】

本発明は、無線通信端末と、前記無線通信端末と無線通信を行う基地局と、前記無線通信端末と前記基地局との間の通信を管理する管理サーバと、を備える認証システムにおいて、前記無線通信端末は、前記基地局と情報を送受信する端末側送受信部と、前記基地局との間で認証処理を行う端末側認証処理部と、クーポン公開部とクーポン秘密部とを含む電子クーポンを記録する端末側記録部と、を備える。基地局は、前記無線通信端末と情報を送受信する基地局側送受信部と、前記無線通信端末との間で認証処理を行う基地局側認証処理部と、を備える。前記管理サーバは、乱数ｓを生成し、生成されたｓを端末秘密鍵とし、$v = g^{-s} \bmod p$によって端末公開鍵ｖを計算し、この値ｇ及びｐはクーポン生成用のパラメータであって、乱数ｘを生成し、生成されたｘをクーポン秘密部とし、$t = g^{x} \bmod p$によってクーポン公開部ｔを計算し、前記電子クーポンを生成し、前記計算された端末公開鍵ｖを前記基地局に送信し、前記生成された端末秘密鍵ｓ及び前記生成された電子クーポンを前記無線通信端末に送信する。前記基地局側記録部は、端末公開鍵ｖを記録する。前記端末側記録部は、複数の電子クーポンを記録し、前記端末側送受信部は、前記複数の電子クーポンのうち一のクーポン公開部を前記基地局に送信し、当該クーポン公開部の電子クーポンを無効と設定し、前記端末側送受信部は、一つの端末認証鍵ＩＤ及び一つのクーポン公開部ｔを含む接続要求を、前記基地局に送信し、前記基地局側認証処理部は、接続要求を受信すると乱数ｃを生成し、生成した乱数ｃを前記無線通信端末に送信し、前記端末側認証処理部は、受信した乱数ｃ、クーポン秘密部ｘ及び端末秘密鍵ｓに基づいて、応答値$y = x + sc$を計算し、計算された応答値ｙを前記無線基地局に送信し、前記基地局側認証処理部は、受信した応答値ｙ、乱数ｃ及び端末公開鍵ｖに基づいて、$g^{y} v^{c} \bmod p$を計算し、前記計算結果がクーポン公開部ｔと一致するか否かを判定することを特徴とする。

【発明の効果】

【００１３】

本発明の認証システムによれば、無線通信端末側の計算量が少ないので、演算資源及び電力供給能力の小さい小型無線通信端末でも個体識別又は認証を行うことができる。また、無線基地局が無線通信端末を認証するための情報は全て公開情報であるため、情報漏洩の危険性がなく、安全性の高い運用ができる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の実施の形態を図面を参照して説明する。

【００１５】

図１は、本発明の実施の形態の認証システムのブロック図である。

【００１６】

認証システムは、通信網３及び複数の無線通信網（ローカルネットワーク）５を備える。通信網３は、複数のローカルネットワーク５を接続する。

【００１７】

各ローカルネットワーク５は、管理サーバ４、無線基地局（アクセスポイント）２及び複数の無線通信端末１を備える。無線基地局２は、ローカルネットワーク５内に少なくとも一つ含まれる。

【００１８】

管理サーバ４は、ネットワークを通じて無線基地局２に接続されており、無線基地局２を経由して無線通信端末１と通信する。なお、管理サーバ４が、無線通信端末１との間に無線又は有線の通信手段を備え、無線基地局２を経由しないで直接に通信してもよい。

【００１９】

管理サーバ４は、無線通信端末１を初期設定し、また、ローカルネットワーク５内の無線基地局２と無線通信端末１との通信を管理する。管理サーバ４は、無線通信端末１の初期設定時に、暗号化鍵及び認証用の鍵を無線通信端末１の記憶媒体に書き込む。また、管理サーバ４は、同一のローカルネットワーク５内の無線基地局２と、当該暗号化鍵及び認証用の鍵を共有する。そして、無線通信端末１は、ホームネットワーク内の無線基地局２と、この暗号化鍵及び認証用の鍵を用いて安全に通信することができる。

【００２０】

無線基地局２は、無線通信端末１と無線で通信する。また、無線基地局２は、通信網３に接続されており、無線通信端末１から受信した情報を収集して通信網３に送信する。

【００２１】

無線通信端末１は、電源、センサ１１（図２）及び無線通信機を有する。無線通信端末１は、初回の起動時に、いずれかのローカルネットワーク５で管理サーバ４によって初期設定される。この初期設定時に接続されているローカルネットワーク５を、ホームネットワークと呼ぶ。

【００２２】

無線通信端末１は、ホームネットワーク以外のローカルネットワーク５と接続して通信することもできる。このホームネットワーク以外のローカルネットワークを訪問先ネットワークと呼ぶ。

【００２３】

無線通信端末１の物理的な位置移動によって、無線通信端末１がローカルネットワーク５から訪問先ネットワークに移動して接続を要求した場合、又は、訪問先ネットワークからさらに別の訪問先ネットワークに移動して接続を要求した場合、各訪問先ネットワークは、当該無線通信端末１が認証システムに登録された正当な無線通信端末１であることを確認する。そして、正当な無線通信端末１であることが確認できると接続を許可する。なお、無線通信端末１が認証システムに登録された正当な無線通信端末１であるか否かの認証方法は、図３で後述する。

【００２４】

図２は、本発明の実施の形態の無線通信端末１、無線基地局２及び管理サーバ４の構成を示すブロック図である。

【００２５】

無線通信端末１は、センサ１１、コントローラ１２、不揮発性メモリ１３、ＲＦ回路１４、アンテナ１５、表示部１０２及び操作部１０３を備える。センサ１１、コントローラ１２、不揮発性メモリ１３、表示部１０２及び操作部１０３は、バス１０によって接続されている。

【００２６】

センサ１１は、例えば、温度、湿度、照度、加速度、赤外線を感知するセンサである。なお、センサ１１は、無線通信端末１に必須の構成ではない。

【００２７】

コントローラ１２は、通信を制御するＣＰＵ及び通信時にワークエリアとして利用されるＲＡＭを備える。また、無線通信端末１は、コントローラ１２に外付けされる不揮発性メモリ１３を備える。

【００２８】

不揮発性メモリ１３は、認証処理に用いる情報を記憶するメモリであって、例えば、ＥＥＰＲＯＭが用いられる。不揮発性メモリ１３は、認証処理プログラム１６、端末認証鍵ＩＤ１７、端末秘密鍵１８及びクーポンリスト１９が記憶されている。

【００２９】

認証処理プログラム１６は、認証処理時の応答値を計算する（図３）。コントローラ１２が認証処理プログラム１６を実行することで、無線通信端末１側の認証処理部が構成される。

【００３０】

端末認証鍵ＩＤ１７は、初期設定時に管理サーバ４によって生成される。端末認証鍵ＩＤ１７は、無線通信端末１が有する端末認証用鍵の特定に用いられる。

【００３１】

端末秘密鍵１８は、初期設定時に管理サーバ４によって生成される。端末秘密鍵１８は、認証処理時の応答値の算出に用いられる。

【００３２】

クーポンリスト１９は、管理サーバ４によって発行された電子クーポンの一覧である。認証処理で一度使用された電子クーポンは無効化される。また、管理サーバ４によって新たな電子クーポンが発行されると、クーポンリスト１９に記録されていた無効となった電子クーポンは、新たな電子クーポンに更新される。なお、クーポンリスト１９については、図４で後述する。

【００３３】

表示部１０２は、無線基地局２との通信状態や、電子クーポンの残数を表示するディスプレイを備える。また、操作部１０３は、無線通信端末１の各種操作のための装置（スイッチ、ボタン等）を備える。操作部１０３の操作により入力された信号は、コントローラ１２に送信されて所定の処理がされる。なお、表示部１０２及び／又は操作部１０３は、無線通信端末１に必須の構成ではない。

【００３４】

アンテナ１５は、無線基地局２と情報を送受信する。送受信される情報は、ＲＦ回路１４を介してコントローラ１２に入出力される。

【００３５】

無線基地局２は、無線Ｉ／Ｆ２２、コントローラ２１、不揮発性メモリ２４及び通信Ｉ／Ｆ２３を備える。無線Ｉ／Ｆ２２、コントローラ２１、不揮発性メモリ２４及び通信Ｉ／Ｆ２３は、バス２０によって接続されている。

【００３６】

無線Ｉ／Ｆ２２は、アンテナを有し、無線通信端末１と情報を送受信する。コントローラ２１は、通信制御を司るＣＰＵ及び通信時にワークエリアとして利用されるＲＡＭを内蔵する。また、無線基地局２は、コントローラ２１に外付けされる不揮発性メモリ２４を備える。

【００３７】

不揮発性メモリ２４は、認証処理に用いる情報を記憶するメモリであって、例えば、ＥＥＰＲＯＭが用いられる。不揮発性メモリ２４は、端末認証鍵リスト２５及び認証処理プログラム２６が記憶されている。

【００３８】

端末認証鍵リスト２５は、無線通信端末１に付与された端末認証用鍵に関するリストである。この場合の無線通信端末１は、端末認証鍵リスト２５が記憶された無線基地局２に接続する可能性のある全ての無線通信端末１である。なお、無線通信端末１が接続する可能性がある無線基地局２とは、当該無線通信端末１のホームネットワーク内の無線基地局２のほか、例えば、当該ホームネットワークの近隣のローカルネットワーク５内の無線基地局２、及び、当該無線通信端末１が移動する可能性のある所定範囲のローカルネットワーク５内の無線基地局２である。

【００３９】

認証処理プログラム２６は、無線通信端末１に送信する乱数を生成し、受信した応答値を検証する（図３）。コントローラ２１が認証処理プログラム２６を実行することで、無線基地局２側の認証処理部が構成される。

【００４０】

通信Ｉ／Ｆ２３は、通信網３にネットワーク（例えば、Ethernet（登録商標、以下同じ））で接続されている。そして、通信網３に接続されている管理サーバ４と、情報の送受信を行う。

【００４１】

管理サーバ４は、コントローラ４３、通信Ｉ／Ｆ４４及び記憶装置（ＨＤＤ）４１を備える。コントローラ４３、通信Ｉ／Ｆ４４及び記憶装置４１は、バス４０によって接続されている。

【００４２】

コントローラ４３は、ＣＰＵ、プログラム等を予め格納したＲＯＭ、ＣＰＵの動作時にワークエリアとして使用されるメモリであるＲＡＭが設けられている。

【００４３】

記憶装置４１には、クーポン生成用パラメータ４２、端末認証鍵リスト４３及び発行済みクーポンリスト４４が記憶されている。

【００４４】

クーポン生成用パラメータ４２は、管理サーバ４で複数生成される。そして、無線通信端末１の初期設定時に、選択された一つのクーポン生成用パラメータ４２を用いて電子クーポンが発行される。電子クーポンは、一度の認証処理についてのみ使用が可能であって、既に使用された電子クーポンは使用済みクーポンとして無効になる点が本発明の特徴である。

【００４５】

端末認証鍵リスト４３は、管理サーバ４が初期設定を行った無線通信端末１の端末認証用鍵に関するリストである。管理サーバ４は、無線通信端末１から登録要求があると当該無線通信端末１に対して初期設定を行う。そして、初期設定が完了すると、端末認証鍵リスト４３に生成した端末認証用鍵に関する情報を追加する。

【００４６】

発行済みクーポンリスト４４は、管理サーバ４が発行した電子クーポンのリストである。複数の無線通信端末１に複数の電子クーポンを発行した場合であっても、全ての電子クーポンについての情報が一つの発行済みクーポンリスト４４に記憶される。

【００４７】

図３は、本発明の実施の形態の初期設定処理及び認証処理のフローチャートである。

【００４８】

管理サーバ４は、無線通信端末１の登録及び当該無線通信端末１に対して電子クーポンの発行を含む初期設定をする。クーポン発行処理は、登録処理の後に行ってもよく、登録処理と同時に行ってもよい。なお、無線通信端末１は、起動時に初期設定を行わなければ正しく使用することができない。

【００４９】

まず、無線通信端末１の登録処理（５００～５０６）について説明する。

【００５０】

無線通信端末１が起動すると、無線通信端末１は、管理サーバ４に登録を要求する（５００）。管理サーバ４は、受信した登録要求に端末ＩＤが含まれていなかったら、登録要求を送信する当該無線通信端末１は初めて電源が投入されたものと判定し、無線通信端末１を識別する端末ＩＤを生成する。管理サーバ４は、生成した端末ＩＤを端末認証鍵リスト４３に登録する。そして、管理サーバ４は、無線通信端末１に当該端末ＩＤを送信する（５０１）。

【００５１】

なお、各無線通信端末１に、予め端末ＩＤが設定されていてもよい。この場合、無線通信端末１は、起動とともに端末ＩＤを管理サーバ４に送信して登録を要求する（５００）。管理サーバ４は、無線通信端末１から端末ＩＤを含む登録要求を受信すると、当該端末ＩＤを端末認証鍵リスト４３に登録する。そして、後述するように、管理サーバ４は、当該端末ＩＤに対応させて端末認証用鍵及び電子クーポンを生成する。

【００５２】
この、端末ＩＤの端末認証鍵リスト４３への登録によって、無線通信端末１のホームネットワークが決定する。
【００５３】
次に、管理サーバ４は、無線通信端末１に固有の端末認証用鍵を生成する（５０２）。また同時に、端末認証用鍵を識別するための端末認証鍵ＩＤを生成する。生成した端末認証用鍵及び端末認証鍵ＩＤは、端末ＩＤと関連付けられて端末認証鍵リスト４３（図６）に登録される。
【００５４】
端末認証用鍵は、端末認証鍵秘密部４３３と端末認証鍵公開部４３４とを含む。管理サーバ４は、乱数ｓを生成して端末認証鍵秘密部４３３とし、選択された乱数ｓを用いてｖ＝g^{-s} ｍｏｄ ｐを計算する。その結果、算出されたｖを、対応する端末認証鍵公開部４３４とする。なお、値ｇ、ｐはクーポン生成用パラメータ４２であり、詳細は後述する。
【００５５】
この端末認証鍵秘密部４３３は端末秘密鍵１８に用いられ、端末認証鍵公開部４３４は端末公開鍵２５４に用いられる。
【００５６】
なお、使い捨て型の電子クーポンを実現するためのアルゴリズムは、本実施の形態に示す方法に限られない。個体認証アルゴリズムであって、認証処理で無線通信端末１が行う処理のうち計算量の大きい部分を事前に計算しておくことが可能な方法であれば、例えば、Okamoto-identificationスキームを用いてもよい。Okamoto-identificationスキームについては、T. Okamoto "Provably secure and practical identification schemes and corresponding signature schemes", Advances in cryptology - Crypt'92, Lecture Notes in Computer Science 740, Springer-Verlag” 1993, p.31-53に記載されている。
【００５７】
次に、管理サーバ４は、生成した端末認証鍵ＩＤ及び端末認証鍵の秘密部（端末秘密鍵）１８を無線通信端末１に送信する（５０３）。無線通信端末１は、これらの情報を不揮発性メモリ１３に記録する（５０４）。また、管理サーバ４は、生成した端末認証鍵ＩＤ及び端末認証鍵の公開部（端末公開鍵）２５４を、当該端末公開鍵２５４を有する無線通信端末１が接続する可能性のある無線基地局２に送信する（５０５）。無線基地局２は、これらの情報を不揮発性メモリ２４の端末認証鍵リスト２５（図５）に記録する（５０６）。
【００５８】
なお、無線基地局２への端末公開鍵２５４の送信は、後述する無線通信端末１から接続要求を受信したときでもよい。この場合、接続要求を受信した無線基地局２は、当該無線通信端末１のホームネットワークの管理サーバ４へ要求することによって端末公開鍵２５４を取得する。
【００５９】
次に、クーポン発行処理（５０７～５０９）について説明する。
【００６０】
管理サーバ４は、クーポン生成用パラメータ４２を生成する。そして、クーポン生成用パラメータ４２を用いて、無線通信端末１の電子クーポンを生成する（５０７）。なお、登録処理によって決定したホームネットワークの管理サーバ４が有するクーポン生成用パラメータ４２が、当該無線通信端末１のクーポン発行処理に用いられる。
【００６１】
クーポン生成用パラメータ４２は、まず、予め定められた桁数の任意の素数ｐと、ｐよりも小さい素数であってｐ－１の素因数となる素数ｑを生成する。次に、０＜ｇ＜ｐとなる整数で、ｇのｐによる剰余系での位数がｑとなるものを生成する。このような条件を満たす整数の組は、例えば、Alfred J. Menezes、Paul C. van Oorschot、Scott A. Vansto

ne “Handbook of Applied Cryptography”, CRC Press, 1996, ISBN: 0-8493-8523-7 chapter4に記載されているような技術を用いて生成する。

【００６２】

なお、クーポン生成用パラメータ４２は、予め複数生成したパラメータのうちの一つを使用してもよく、一つのパラメータを繰り返し使用してもよい。また、クーポン生成用パラメータ４２は、秘密性及び安全性を保つことができれば、管理サーバ４で生成してもよく、管理サーバ４が外部で生成したパラメータを取得してクーポン生成用パラメータ４２として用いてもよい。

【００６３】

電子クーポンは、クーポン公開部１９１及びクーポン秘密部１９２を含む。管理サーバ４は、乱数ｘを生成して、$t = g^x \bmod p$を計算する。このｘがクーポン秘密部１９１、ｔがクーポン公開部１９２となる。管理サーバ４は、無線通信端末１に複数の使い捨て型電子クーポンを発行する。なお、使い捨て型電子クーポンの方式は限定されないが、例えば、非特許文献１に記載されている方式を用いることができる。

【００６４】

管理サーバ４は、発行した電子クーポンを、無線通信端末１に送信する（５０８）。無線通信端末１は、受信した電子クーポンを不揮発性メモリ１３のクーポンリスト１９に登録する（５０９）。

【００６５】

次に、無線基地局２による無線通信端末１の認証処理（６２１～６２６）について説明する。

【００６６】

認証処理は、初期設定処理とは異なる段階で実行される。つまり、初期設定処理が実行されるのは、無線通信端末１の初回の起動時のみであるが、認証処理が実行されるのは、無線通信端末１が他のネットワークに移動し、無線基地局２への接続を要求した場合である。例えば、無線通信端末１がローカルネットワーク５から訪問先ネットワークに移動した場合や、訪問先ネットワークからさらに別の訪問先ネットワークに移動した場合である。

【００６７】

無線通信端末１は、他のローカルネットワーク５へ移動すると、通信可能な無線基地局２を探す。

【００６８】

無線通信端末１は、通信可能な無線基地局２を検出すると、使用する一の電子クーポンをクーポンリスト１９に記録されている電子クーポンの中から選択する。そして、当該電子クーポンの状態１９３に”０”を書き込み、当該電子クーポンが使用済みであって無効であることを記録する（６２０）。

【００６９】

次に、検出した無線基地局２に接続要求を送信する。接続要求には、一つの端末認証鍵ＩＤ１７及び一つのクーポン公開部４４２が含まれる（６２１）。

【００７０】

無線基地局２は、接続要求を受信すると、端末認証鍵リスト２５の状態２５５（図５）を参照して、受信した端末認証鍵ＩＤ１７に対応する端末公開鍵２５４が有効か否かを判定する。

【００７１】

受信した端末認証鍵ＩＤ１７自体が存在しないか、又は対応する端末公開鍵２５４が無効の場合は、無線基地局２は接続拒否を無線通信端末１に通知する。なお、端末公開鍵２５４が無効な場合は、図５で説明する。

【００７２】

一方、端末公開鍵２５４が有効であれば、無線基地局２は乱数ｃを生成する（６２２）。そして、生成した乱数ｃを無線通信端末１に送信する（６２３）。

【００７３】
無線通信端末１は、受信した乱数ｃ、クーポン秘密部１９１（ｘ）及び端末秘密鍵１８（ｓ）に基づいて応答値ｙ＝ｘ＋ｓｃを算出する（６２４）。そして、算出した応答値ｙを無線基地局２に送信する（６２５）。
【００７４】
無線基地局２は、受信した応答値ｙ、乱数ｃ及び端末公開鍵２５４（ｖ）を用いて、$g^{y}v^{c}$ ｍｏｄ ｐを算出する。その結果が、ステップＳ６２１で受信したクーポン公開部４４２（ｔ）と一致するか否かを判定する（６２６）。値が一致すれば、受信した応答値ｙが本認証システムに登録された無線通信端末１からのものであると判断して、接続許可を通知する。一方、値が一致しなければ、無線通信端末１は本認証システムに登録されていないと判断して、端末に接続拒否を通知する（６２７）。
【００７５】
以上の処理によって、無線通信端末１が認証される。
【００７６】
このように、認証処理に使い捨て型の電子クーポンを用いることによって、無線通信端末１側の計算量が公開鍵暗号を用いた方式の１０００分の１程度になるため、演算資源及び電力供給能力の小さい小型の無線通信端末１でも個体識別又は認証を行うことができる。また、無線基地局２が無線通信端末１を認証するための情報は全て公開情報であるため、情報漏洩の危険性がなく、安全性の高い運用ができる。
【００７７】
なお、無線通信端末１の認証が成功し、接続が許可されると、無線通信における情報の秘匿性の維持及び改竄防止のために、無線基地局２は、暗号化通信又はメッセージ認証コードを用いて通信してもよい。このために、無線基地局２は、無線通信端末１と、暗号化鍵又はメッセージ認証コード鍵を共有する。メッセージ認証コード鍵は、メッセージ認証コード生成及び認証に用いる。
【００７８】
これらの鍵は、Diffie-Hellman鍵交換プロトコルにより共有する。又は、無線通信端末１の初期設定時に、管理サーバ４が暗号化鍵又はメッセージ認証コード用鍵を生成する。そして、無線通信端末１が無線基地局２に接続した際に、管理サーバ４が当該無線基地局２に暗号化鍵又はメッセージ認証コード用鍵を送信してもよい。
【００７９】
また、以下に示す方法でこれらの鍵を生成してもよい。
【００８０】
まず、管理サーバ４は、秘密パラメータｕ及び乱数ｚを生成する。そして、$t＝g^{z}$ ｍｏｄ ｐ、$k＝g^{zu}$ ｍｏｄ ｐを計算する。
【００８１】
管理サーバ４は、算出した（ｔ，ｋ）を無線通信端末１に送信する。無線通信端末１は、受信した（ｔ，ｋ）を不揮発性メモリ１３に記録する。
【００８２】
また、管理サーバ４は、ｕを無線基地局２に送信する。無線基地局２は、受信したｕを不揮発性メモリ２４に記憶する。
【００８３】
次に、無線通信端末１は、不揮発性メモリ１３に記録されたｔを、無線基地局２に送信する。無線基地局２は、受信したｔに基づいてt^{u}を計算する。この値t^{u}が、暗号化鍵又はメッセージ認証コード用鍵となる。これにより、無線通信端末１と無線基地局２との間で鍵が共有される。
【００８４】
図４は、本発明の実施の形態のクーポンリスト１９の構成図であり、無線通信端末１の不揮発性メモリ１３に記憶されている。
【００８５】

クーポンリスト１９は、クーポン秘密部１９１、クーポン公開部１９２、状態１９３を含む。

【００８６】

クーポン秘密部１９１は、クーポン発行処理時に管理サーバ４によって選択された乱数ｘが記録される。乱数ｘは、正の整数（例えば、１６進法の１０桁の整数）で構成される。

【００８７】

クーポン公開部１９２は、乱数ｘを用いて算出された値ｔが記録される。ｔは、正の整数（例えば、１６進法の１０桁の整数）で構成される。

【００８８】

状態１９３は、該当する電子クーポンが有効であるか否かの情報が記録される。該当する電子クーポンが既に使用されている場合は、当該電子クーポンは無効であり、状態１９３には”０”が記録される。該当する電子クーポンが未だ使用されていない場合は、当該電子クーポンは有効であり、状態１９３には”１”が記録される。

【００８９】

クーポンリスト１９に記録されたデータは、後述する追加クーポン発行処理によって、追加された電子クーポンのデータに更新される。

【００９０】

図５は、本発明の実施の形態の無線基地局２に設けられた端末認証鍵リスト２５の構成図であり、無線基地局２の不揮発性メモリ２４に記憶されている。

【００９１】

端末認証鍵リスト２５は、端末認証鍵ＩＤ２５３、端末公開鍵２５４及び状態２５５を含む。

【００９２】

端末認証鍵ＩＤ２５３は、端末認証用鍵ごとに割り当てられた一意な識別番号である。端末認証鍵ＩＤ２５３には、無線基地局２に接続する可能性のある全ての無線通信端末１に付与された端末認証鍵ＩＤ２５３が記録される。

【００９３】

端末公開鍵２５４は、算出された値ｖが記録される。ｖは、正の整数（例えば、１６進法の２０桁の整数）で構成される。

【００９４】

状態２５５は、該当する端末認証用鍵を有する無線通信端末１が有効に稼動している否かの情報が記録される。該当する無線通信端末１が有効に稼動している場合は、状態２５５には”１”が記録される。一方、該当する無線通信端末１が無効である場合は、状態２５５には”０”が記録される。

【００９５】

無線通信端末１が無効である場合とは、例えば、無線通信端末１を紛失した場合である。無線通信端末１の紛失や盗難があった場合は、利用者の申告によって当該無線通信端末１を無効とする。また、無線通信端末１の破損や不具合によって無線通信端末１が稼動できなくなった場合も、無効である。

【００９６】

無線基地局２は、無線通信端末１から接続要求を受信すると、当該接続要求に含まれる端末認証鍵ＩＤ２５３が端末認証鍵リスト２５に記録されているか否かを判定する。例えば、初期設定処理がされていない無線通信端末１は、端末認証鍵ＩＤ２５３が付与されていないため、端末認証鍵リスト２５に記録されていない。この場合、無線基地局２は、無線通信端末１に接続拒否を通知する。

【００９７】

受信した端末認証鍵ＩＤ２５３が端末認証鍵リスト２５に記録されている場合は、対応する状態２５５を参照して、接続要求を送信した無線通信端末１が有効に稼動しているか否かを判定する。例えば、無線通信端末１が盗まれた場合は、当該無線通信端末１の状態

２５５には”０”が記録されているので、当該無線通信端末１は無効であると判断される。この場合、無線基地局２は、接続拒否を無線通信端末１に通知する。

【００９８】

無線信端末１が有効に稼動している場合は、対応する端末公開鍵２５４を用いて認証する。認証の結果、無線通信端末１が本認証システムに登録されていると判断した場合は、当該無線通信端末１との通信を開始する。

【００９９】

図６は、本発明の実施の形態の管理サーバ４に設けられた端末認証鍵リスト４３の構成図であり、管理サーバ４の記憶装置４１に記憶されている。

【０１００】

端末認証鍵リスト４３は、端末ＩＤ４３１、端末認証鍵ＩＤ４３２、端末認証鍵秘密部４３３、端末認証鍵公開部４３４及び状態４３５を含む。

【０１０１】

端末ＩＤ４３１は、本端末認証鍵リスト４３を有する管理サーバ４が属するローカルネットワーク５をホームネットワークとする無線通信端末１の端末ＩＤ４３１が記録される。端末ＩＤ４３１は、無線通信端末１に割り当てられた一意な識別番号である。

【０１０２】

端末認証鍵ＩＤ４３２は、端末ＩＤ４３１の無線通信端末１に付与された端末認証用鍵の端末認証鍵ＩＤ４３２が記録される。なお、端末認証鍵ＩＤ４３２は、各無線基地局２に記憶された端末認証鍵リスト２５の端末認証鍵ＩＤ２５３と同一である。ただし、端末認証鍵リスト２５には、無線基地局２に接続する可能性のある全ての無線通信端末１の端末認証鍵ＩＤが記録されるが、端末認証鍵リスト４３には、管理サーバ４が含まれるローカルネットワーク５をホームネットワークとする無線通信端末１のみの端末認証鍵ＩＤが記録される。

【０１０３】

端末認証鍵秘密部４３３は、登録処理時に管理サーバ４によって選択された乱数ｓが記録される。乱数ｓは、正の整数（例えば、１６進法の２０桁の整数）で構成される。

【０１０４】

端末認証鍵公開部４３４は、乱数ｓを用いて算出された値ｖが記録される。ｖは、正の整数（例えば、１６進法の２０桁の整数）で構成される。

【０１０５】

なお、端末認証鍵秘密部４３３は、各無線基地局２に記憶された端末認証鍵リスト２５の端末秘密部２５３と同一である。また、端末認証鍵公開部４３４は、各無線基地局２に記憶された端末認証鍵リスト２５の端末公開部２５４と同一である。ただし、端末認証鍵リスト２５には、無線基地局２に接続する可能性のある全ての無線通信端末１の端末秘密部及び端末公開部が記録されるが、端末認証鍵リスト４３には、管理サーバ４が含まれるローカルネットワーク５をホームネットワークとする無線通信端末１のみの端末認証鍵秘密部４３３及び端末認証鍵公開部４３４が記録される。

【０１０６】

状態４３５は、該当する無線通信端末１が有効に稼動している否かの情報が記録される。該当する無線通信端末１が有効に稼動している場合は、状態４３５には”１”が記録される。該当する無線通信端末１が無効である場合は、状態４３５には”０”が記録される。

【０１０７】

無線通信端末１が無効である場合とは、例えば、無線通信端末１を紛失した場合や、破損や不具合によって無線通信端末１が稼動できなくなった場合である。

【０１０８】

図７は、本発明の実施の形態の発行済みクーポンリスト４４の構成図であり、管理サーバ４の記憶装置４１に記憶されている。

【０１０９】

発行済みクーポンリスト４４は、クーポン秘密部４４１、クーポン公開部４４２、端末ＩＤ４４３及び状態４４４を含み、いずれの無線通信端末１にいずれの電子クーポンが発行されたかが記録される。

【０１１０】

クーポン秘密部４４１は、クーポン発行処理時に選択された乱数ｘが記録される。乱数ｘは、正の整数（例えば、１６進法の１０桁の整数）で構成される。なお、クーポン秘密部４４１は、各無線通信端末１に記憶されたクーポンリスト１９のクーポン秘密部１９１と同一である。

【０１１１】

クーポン公開部４４２は、乱数ｘを用いて算出された値ｔが記録される。ｔは、正の整数（例えば、１６進法の１０桁の整数）で構成される。なお、クーポン公開部４４２は、各無線通信端末１に記憶されたクーポンリスト１９のクーポン公開部１９２と同一である。

【０１１２】

端末ＩＤ４４３は、該当する電子クーポンが発行された無線通信端末１の端末ＩＤ４４３が記録される。なお、端末ＩＤ４４３は、各無線通信端末１に記憶されたクーポンリスト１９の端末ＩＤ４３１と同一である。

【０１１３】

また、図７では便宜上、各無線通信端末１に対してそれぞれ２つの電子クーポンに関する情報が記録されている。つまり、一度のクーポン発行処理によって各無線通信端末１に対して電子クーポンが２個ずつ発行されている。しかし、一度のクーポン発行処理によって発行される電子クーポンの数は２個に限られず、他の数であってもよい。

【０１１４】

状態４４４は、対応する発行済み電子クーポンが有効であるか否かの情報が記録される。各電子クーポンが有効であるか否かの情報は、各無線通信端末１から所定のタイミングで受信して記録される。該当する電子クーポンが既に使用されている場合は、当該電子クーポンは無効であり、状態４４４には”０”が記録される。該当する電子クーポンが未だ使用されていない場合は、当該電子クーポンは有効であり、状態４４４には”１”が記録される。

【０１１５】

なお、状態４４４は、必須の構成ではない。ただし、状態４４４を設けることによって、管理サーバ４において、各無線通信端末１が有する電子クーポンの使用状態を管理することができる。

【０１１６】

発行済みクーポンリスト４４には、いずれかの無線通信端末１に対して電子クーポンが発行される度に、発行された電子クーポンに関する情報が追加される。

【０１１７】

図８は、本発明の実施の形態の無線通信端末１の概略図である。

【０１１８】

無線通信端末１は、表示画面１０１、操作ボタン（操作部）１０３を有する。

【０１１９】

表示画面１０１は、ＬＣＤ（液晶表示器）で構成されている。表示画面１０１には、無線基地局２との通信状態や、インジケータ１０２が表示される。

【０１２０】

インジケータ１０２は、電子クーポンの残数（無線通信端末１が現在保持している有効な電子クーポンの数）を表示する。これにより、無線通信端末１の利用者に電子クーポンの残数を知らせることができる。図８では、インジケータ１０２内のバー（図の斜線部）によって電子クーポンの残量を示している。インジケータ１０２内に目盛りを付して電子クーポンの残数を示してもよい。また、電子クーポンの残数を数値で表示してもよい。

【０１２１】

また、インジケータ１０２に、電子クーポンの残数を電池の残量として表示してもよい。これにより、広域を移動して多数の電子クーポンが使用された場合に、無線通信端末１の電池の残量が減少したように見せることができる。そして利用者に、無線通信端末１の充電（電子クーポンの追加発行）を促すことができる。

【０１２２】

操作ボタン１０３は、管理サーバ４に電子クーポンの追加発行の要求を通知する。利用者は、インジケータ１０２に表示される電子クーポンの数が残り僅かになると、操作ボタン１０３を操作して、管理サーバ４に電子クーポンの追加発行を要求する。

【０１２３】

なお、表示画面１０１、インジケータ１０２及び／又は操作ボタン１０３は、無線通信端末１に必須の構成ではない。

【０１２４】

ここで、電子クーポンの追加発行処理について説明する。

【０１２５】

無線通信端末１は、クーポンリスト１９に記録された有効な電子クーポンが一定数を下回ると、管理サーバ４に新しい電子クーポンの追加発行を要求する。電子クーポンの残数が一定数を下回ると、自動的に新たな電子クーポンの追加発行が要求されてもよく、利用者による操作ボタン１０３の操作によって追加発行が要求されてもよい。

【０１２６】

管理サーバ４は無線通信端末１からの要求を受信すると、クーポン生成用パラメータ４２を用いて電子クーポンを生成する。そして、生成した電子クーポンを、通信網３及び無線基地局２を経由して無線通信端末１に送信する。

【０１２７】

電子クーポンの不正使用を防止するために、電子クーポンは、無線通信端末１がホームネットワーク内にある場合にのみ追加発行される。つまり、無線通信端末１がホームネットワーク内の無線基地局２に接続している場合に限られる。この場合、管理サーバ４は、クーポン追加発行の要求を受け付けると、当該要求をした無線通信端末１が接続されている無線基地局２のアドレスを確認する。その結果、当該無線通信端末１のホームネットワーク内の無線基地局２であることを確認した場合にのみ、クーポン追加発行の要求に応じる。

【０１２８】

また、発行される電子クーポンの内容の安全性を保証するため、初期設定時に管理サーバ４がメッセージ認証コード用の鍵を生成してもよい。当該鍵は、無線通信端末１と管理サーバ４とで共有する。そして、クーポン発行処理時に、管理サーバ４は、発行した電子クーポンにメッセージ認証コードを付加する。当該電子クーポンを受信すると、無線通信端末１は、予め所有するメッセージ認証コード用の鍵を用いて受信した電子クーポンのメッセージ認証コードを生成する。そして、受信した電子クーポンに付されたメッセージ認証コードと比較する。このときにメッセージ認証コードが一致した場合のみ、受信した電子クーポンをクーポンリスト１９に記録する。これにより、無線通信端末１は不正な電子クーポンの受信を防ぐことができる。

【０１２９】

次に、利用者のプライバシーを保護する無線通信端末１の認証方法について説明する。

【０１３０】

無線通信端末１は、例えば健康管理の目的で、人間の身体の一部に装着して利用される場合がある。この場合、利用者の行動履歴等の個人情報が、ネットワークを通じて収集され、ネットワーク管理者に知られる。このネットワーク管理者と本認証システムの管理者が異なる場合には、無線通信端末１の利用者のプライバシーを保護する必要がある。

【０１３１】

従来の認証方法としては、仮の名前を利用した匿名認証技術が知られている。しかし、この方法では、前述の公開鍵暗号を用いる方法以上に、無線通信端末１側の認証処理が大

きくなる。よって、小型バッテリや太陽電池で稼働する小型の無線通信端末１で用いるのは困難である。

【０１３２】

そこで、複数の無線通信端末１に同一の端末認証用鍵を付与したり、複数の無線通信端末１に共通する複数の端末認証用鍵を付与する。これによって、端末認証用鍵からの個々の無線通信端末１の特定が困難になる。そのため、無線通信端末１の利用者のプライバシーを保護することができる。

【０１３３】

各無線通信端末１が複数の端末認証鍵を有するようにしてもよい。このようにすれば、漏洩した端末公開鍵が無効化されても、無効化された端末認証用鍵以外の端末認証用鍵を使用することができる。つまり、一つの端末認証用鍵が無効化されても、無線通信端末の有する全ての端末認証用鍵が無効化されない限りは通信を継続することができ、無線通信端末１の稼働率が向上し、保守コストが低減される。

【０１３４】

例えば、複数の無線通信端末１が複数の端末認証用鍵を共有する。そして、無線基地局２は、これらの複数の端末秘密鍵１８の中から任意の一つの端末秘密鍵１８を選択して認証を行う。

【０１３５】

この方法により、無線基地局２は、認証した無線通信端末１が、管理サーバ４により発行された端末認証用鍵を有する無線通信端末１のうちの一つであることを確認できる。しかし、無線通信端末１を特定することはできない。ただし、ホームネットワークの管理サーバ４は、認証に使用された電子クーポンを、発行済みクーポンリスト４４と照合することにで、無線通信端末１を特定することができる。

【図面の簡単な説明】

【０１３６】

【図１】本発明の実施の形態の認証システムのブロック図である。

【図２】本発明の実施の形態の無線通信端末、無線基地局及び管理サーバの構成を示すブロック図である。

【図３】本発明の実施の形態の初期設定処理及び認証処理のフローチャートである。

【図４】本発明の実施の形態のクーポンリストの構成図である。

【図５】本発明の実施の形態の無線基地局に設けられた端末認証鍵リストの構成図である。

【図６】本発明の実施の形態の管理サーバに設けられた端末認証鍵リストの構成図である。

【図７】本発明の実施の形態の発行済みクーポンリストの構成図である。

【図８】本発明の実施の形態の無線通信端末の概略図である。

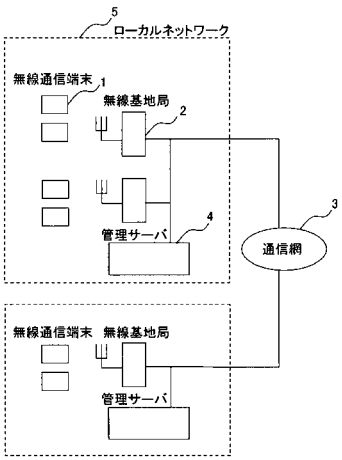
【符号の説明】

【０１３７】

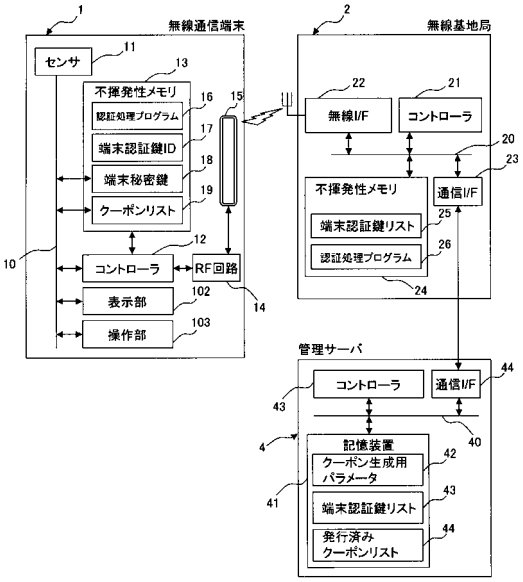
１　無線通信端末
２　無線基地局
３　通信網
４　管理サーバ
５　ローカルネットワーク
１１　センサ
１６、２６　認証処理プログラム
１７、２５３、４３２　端末認証鍵ＩＤ
１８　端末秘密鍵
１０１　表示部
１９１、４４１　クーポン秘密部
１９２、４４２　クーポン公開部

２５４　端末公開鍵
４３３　端末認証鍵秘密部
４３４　端末認証鍵公開部

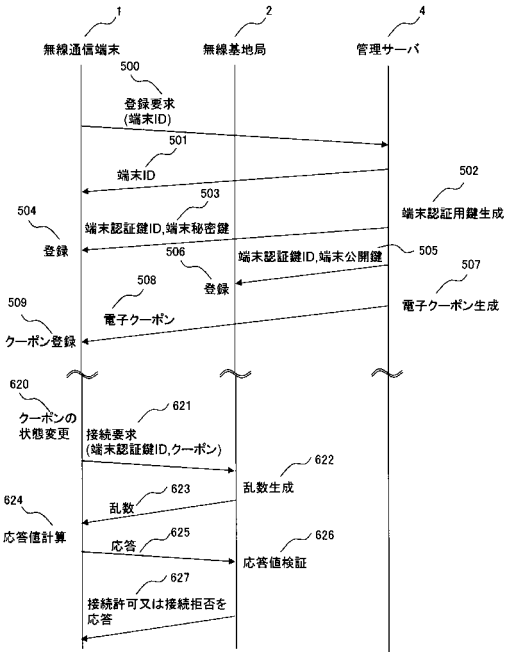
【図１】



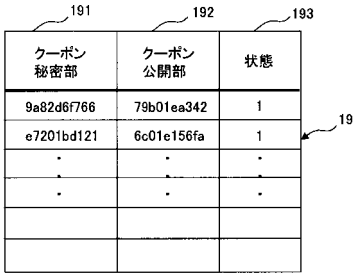
【図２】



【図３】



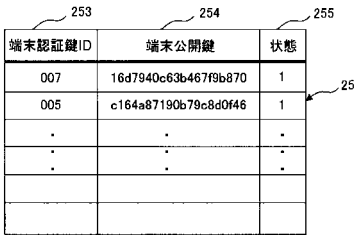
【図４】



クーポン秘密部 (191)	クーポン公開部 (192)	状態 (193)
9a82d6f766	79b01ea342	1
e7201bd121	6c01e156fa	1
・	・	・
・	・	・
・	・	・

19

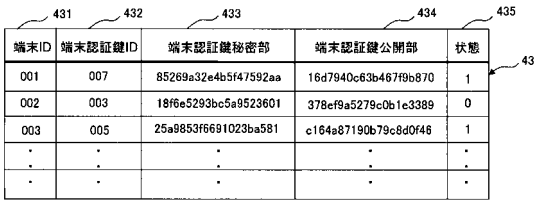
【図５】



端末認証鍵ID (253)	端末公開鍵 (254)	状態 (255)
007	16d7940c63b467f9b870	1
005	c164a87190b79c8d0f46	1
・	・	・
・	・	・
・	・	・

25

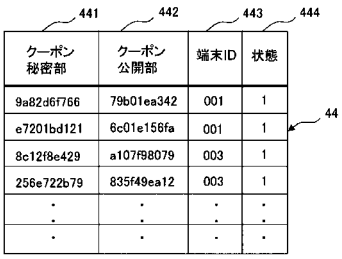
【図６】



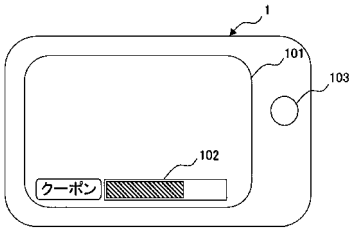
端末ID (431)	端末認証鍵ID (432)	端末認証鍵秘密部 (433)	端末認証鍵公開部 (434)	状態 (435)
001	007	85269a32e4b5f47592aa	16d7940c63b467f9b870	1
002	003	18f6e5293bc5a9523601	378ef9a5279c0b1e3389	0
003	005	25a9853f6691023ba581	c164a87190b79c8d0f46	1
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

43

【図７】


441
442
443
444
クーポン秘密部
クーポン公開部
端末ID
状態
9a82d6f766
79b01ea342
001
1
e7201bd121
6c01e156fa
001
1
8c12f8e429
a107f98079
003
1
256e722b79
835f49ea12
003
1
44

【図８】


1
101
103
102
クーポン

フロントページの続き

(56)参考文献 特開平１０－３３６１６９（ＪＰ，Ａ）
特開２００３－１８６８３８（ＪＰ，Ａ）
特開２００４－０１５７２５（ＪＰ，Ａ）
特開２００３－２８３４８０（ＪＰ，Ａ）
特開２００３－２６３４１４（ＪＰ，Ａ）
特開２０００－０７８１２４（ＪＰ，Ａ）
特開２００４－２０８０７３（ＪＰ，Ａ）
特開２００３－１８８８８５（ＪＰ，Ａ）
特表２００４－５０１４６０（ＪＰ，Ａ）
朴美娘、馬場義昌、妹尾尚一郎、岡崎直宣，ワイヤレスネットワークシステムにおける高速ユーザ認証プロトコルに関する考察，コンピュータセキュリティシンポジウム２００４論文集，日本，社団法人情報処理学会，２００４年１０月２０日，Vol.2004、No.11，pp.313-318，情報処理学会シンポジウムシリーズ

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１４，　９／３２
Ｈ０４Ｗ　　４／００－９９／００