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

特許第4133380号
(P4133380)

(45)発行日　平成20年8月13日(2008.8.13)　(24)登録日　平成20年6月6日(2008.6.6)

(51)Int.Cl.			F I		
H04Q	7/38	(2006.01)	H04B	7/26	109R
G09C	1/00	(2006.01)	G09C	1/00	640E
H04L	9/32	(2006.01)	H04L	9/00	675D
H04L	12/28	(2006.01)	H04L	9/00	675A
			H04L	9/00	675Z

請求項の数 13　(全 19 頁)　最終頁に続く

(21)出願番号　特願2003-23160(P2003-23160)
(22)出願日　平成15年1月31日(2003.1.31)
(65)公開番号　特開2004-236063(P2004-236063A)
(43)公開日　平成16年8月19日(2004.8.19)
審査請求日　平成17年7月12日(2005.7.12)

(73)特許権者　000006633
京セラ株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(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　福田　諭展
神奈川県横浜市都筑区加賀原二丁目１番１号　京セラ株式会社横浜事業所内

審査官　吉村　博之

最終頁に続く

(54)【発明の名称】通信システム、認証方法、無線通信装置及びデータ書込装置

(57)【特許請求の範囲】

【請求項１】

ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、によって構成される通信システムにおいて、

前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を表す前記基地局情報に対応して認証情報として記憶され、

前記認証装置は、前記無線通信装置が前記認証装置に送信する認証要求が経由した基地局を特定する基地局特定手段を有し、前記認証要求が経由した基地局を特定し、

該基地局の基地局情報に対応した前記期間情報と、前記無線通信装置が認証要求している時点との比較結果に基づいて、前記無線通信装置の前記ネットワークへの接続を認証する認証手段を有することを特徴とする通信システム。

【請求項２】

前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化する暗号化手段を有し、

前記無線通信装置の記憶部には、前記暗号化された認証情報を記憶する請求項１に記載

の通信システム。
【請求項３】
ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、によって構成される通信システムにおいて、
前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す期間情報が、前記無線通信装置が接続される基地局を表す前記基地局情報に対応して認証情報として記憶され、
前記無線通信装置は、前記認証要求を前記認証装置に送信する認証要求送信手段を有し、
前記認証装置は、前記無線通信装置が前記認証装置に送信した認証要求が経由した基地局を特定する基地局特定手段を有し、
特定された該基地局の情報を前記無線通信装置へ送信する基地局情報送信手段を有し、
前記無線通信装置は、前記記憶部に記憶された基地局情報と、前記基地局情報送信手段によって送信された基地局の情報との比較結果に基づいて、該基地局への接続可否を判定する接続可否判定手段を有し、
前記接続可否の判定の結果、該基地局への接続が可能と判定されると、前記無線通信装置は、該基地局の基地局情報に対応して前記記憶部に記憶された期間情報を送信する期間情報送信手段を有し、
前記認証装置は、前記無線通信装置が認証要求している時点と前記期間情報との比較結果に基づいて、前記無線通信装置の認証をする認証手段を有することを特徴とする通信システム。
【請求項４】
前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化する暗号化手段を有し、
前記無線通信装置の記憶部には、前記暗号化された認証情報を記憶する請求項３に記載の通信システム。
【請求項５】
ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されてデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、を備えた通信システムに用いられる認証方法において、
前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を示す基地局情報に対応して認証情報として記憶されており、
前記無線通信装置は、前記期間情報を、認証情報として、前記認証装置に送信し、
前記認証装置は、前記無線通信装置が前記認証装置に送信する認証要求が経由した基地局を特定し、
該基地局の基地局情報に対応した前記期間情報と、前記無線通信装置が認証要求している時点との比較結果に基づいて、前記無線通信装置の前記ネットワークへの接続の認証をすることを特徴とする認証方法。
【請求項６】
前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化し、暗号化された期間情報又は／及び基地局情報を前記無線通信装置に送出し、
前記無線通信装置は、暗号化された期間情報又は／及び基地局情報を前記記憶部に記憶

し、
前記認証装置は、前記無線通信装置から取得した暗号化された期間情報又は基地局情報を、前記データ書込装置と共通の暗号鍵によって復号化して、前記無線通信装置の認証をすることを特徴とする請求項５に記載の認証方法。
【請求項７】
ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されてデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、を備えた通信システムに用いられる認証方法において、
前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる、前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を示す基地局情報に対応して認証情報として記憶されており、
前記無線通信装置は、前記認証情報を前記認証装置に送信し、
前記認証装置は、前記無線通信装置が前記認証装置に送信した認証要求が経由した基地局を特定して、該基地局の情報を前記無線通信装置へ送信し、
前記無線通信装置は、前記記憶部に記憶された基地局情報と、前記認証装置によって特定された基地局の情報との比較結果に基づいて、該基地局への接続可否を判定し、
前記接続可否の判定の結果、該基地局への接続が可能と判定されると、前記無線通信装置は、該基地局の基地局情報に対応して前記記憶部に記憶された期間情報を送信し、
前記認証装置は、前記無線通信装置が認証要求している時点と前記期間情報との比較結果に基づいて、前記無線通信装置の認証をすることを特徴とする認証方法。
【請求項８】
前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化し、暗号化された期間情報又は／及び基地局情報を前記無線通信装置に送出し、
前記無線通信装置は、暗号化された期間情報又は／及び基地局情報を前記記憶部に記憶し、
前記認証装置は、前記無線通信装置から取得した暗号化された期間情報又は基地局情報を、前記データ書込装置と共通の暗号鍵によって復号化して、前記無線通信装置の認証をすることを特徴とする請求項７に記載の認証方法。
【請求項９】
前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化し、暗号化された基地局情報を前記無線通信装置に送出し、
前記無線通信装置は、暗号化された基地局情報を前記記憶部に記憶し、
前記無線通信装置は、前記暗号化された基地局情報を前記データ書込装置と共通の暗号鍵によって復号化して、前記特定された基地局情報との比較結果に基づいて、該基地局への接続可否を判定することを特徴とする請求項７に記載の認証方法。
【請求項１０】
無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置から送信される認証要求が経由した基地局を特定する基地局特定手段を有し、前記認証要求が経由した基地局を特定して前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、によって構成される通信システムに用いられ、ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されデータ通信を行う無線通信装置において、
無線通信装置の記憶部に認証情報を書き込むデータ書込装置が前記認証情報を前記記憶部に書き込むために接続される接続手段を有し、
前記記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を表す前記基地局情

報に対応して認証情報として記憶されることを特徴とする無線通信装置。
【請求項１１】
前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化する暗号化手段を有し、
前記無線通信装置の記憶部には、前記暗号化された認証情報を記憶する請求項１０に記載の無線通信装置。
【請求項１２】
ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置から送信される認証要求が経由した基地局を特定する基地局特定手段を有し、前記認証要求が経由した基地局を特定して前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、によって構成される通信システムに用いられる、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置であって、
前記無線通信装置の記憶部に、前記ネットワークへの接続可能期間を示す前記期間情報として書き込み、
前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を表す前記基地局情報に対応して認証情報として記憶されることを特徴とするデータ書込装置。
【請求項１３】
前記認証装置と共有する暗号鍵によって前記認証情報を暗号化する暗号化手段を有し、
前記無線通信装置の記憶部に、前記暗号化された認証情報を書き込む請求項１２に記載のデータ書込装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、公衆無線スポット等のいわゆるホットスポットを用いてインターネット接続業者との接続に用いる通信システム及び認証方法に関する。
【０００２】
【従来の技術】
従来のインターネット接続サービス業者（ＩＳＰ）に接続するための認証方式としてＩＤとパスワードを予めＩＳＰに登録し、登録されたＩＤ及びパスワードを用いて認証を行う方法が知られている。
【０００３】
ここで、例えば公衆無線スポット、いわゆるホットスポットを経由してＩＳＰと認証を行う場合にも同様に登録されたＩＤ及びパスワードを用いて認証を行う必要がある。例えば、特開２００２－１５２２７６号公報では、自宅で使用しているＩＳＰで用いるため、予め登録しているＩＤとパスワードとを公衆スポットで利用することができるような発明が開示されている。
【０００４】
【特許文献１】
特開２００２－１５２２７６号公報
【０００５】
【発明が解決しようとする課題】
しかしながら、従来のようにＩＤとパスワードを用いた認証は、定期的で繰り返してインターネット接続が利用される場合には有効な方法であるが、特定期間のみ、又は特定の場所でのみインターネット接続を利用可能とするような、一時的に提供されるホットスポットサービスにおいては、その都度ＩＤ及びパスワードを発行する必要があり、また、いつ利用するかわからないユーザのためにＩＤを管理することはサーバに負担を掛ける。
【０００６】

本発明は上記の不都合を鑑みてなされたものであり、ホットスポットを一時的に利用するユーザに対して、専用の無線カードと期間又はアクセスポイントを限定した認証ＩＤを発行することによって、ユーザの利用をより簡便にすることのできる通信システム及びサービス提供方法に関する。

【０００７】

【課題を解決するための手段】

第１の発明は、ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、によって構成される通信システムにおいて、前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を表す前記基地局情報に対応して認証情報として記憶され、前記認証装置は、前記無線通信装置が前記認証装置に送信する認証要求が経由した基地局を特定する基地局特定手段を有し、前記認証要求が経由した基地局を特定し、該基地局の基地局情報に対応した前記期間情報と、前記無線通信装置が認証要求している時点との比較結果に基づいて、前記無線通信装置の前記ネットワークへの接続を認証する認証手段を有することを特徴とする。

【０００８】

第２の発明は、第１の発明において、前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化する暗号化手段を有し、前記無線通信装置の記憶部には、前記暗号化された認証情報を記憶する。

【０００９】

第３の発明は、ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、によって構成される通信システムにおいて、前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す期間情報が、前記無線通信装置が接続される基地局を表す前記基地局情報に対応して認証情報として記憶され、前記無線通信装置は、前記認証要求を前記認証装置に送信する認証要求送信手段を有し、前記認証装置は、前記無線通信装置が前記認証装置に送信した認証要求が経由した基地局を特定する基地局特定手段を有し、特定された該基地局の情報を前記無線通信装置へ送信する基地局情報送信手段を有し、前記無線通信装置は、前記記憶部に記憶された基地局情報と、前記基地局情報送信手段によって送信された基地局の情報との比較結果に基づいて、該基地局への接続可否を判定する接続可否判定手段を有し、前記接続可否の判定の結果、該基地局への接続が可能と判定されると、前記無線通信装置は、該基地局の基地局情報に対応して前記記憶部に記憶された期間情報を送信する期間情報送信手段を有し、前記認証装置は、前記無線通信装置が認証要求している時点と前記期間情報との比較結果に基づいて、前記無線通信装置の認証をする認証手段を有することを特徴とする。

【００１０】

第４の発明は、第３の発明において、前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化する暗号化手段を有し、前記無線通信装置の記憶部には、前記暗号化された認証情報を記憶する。

【００１１】

第５の発明は、ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されてデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネット

ワークと、前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、を備えた通信システムに用いられる認証方法において、前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を示す基地局情報に対応して認証情報として記憶されており、前記無線通信装置は、前記期間情報を、認証情報として、前記認証装置に送信し、前記認証装置は、前記無線通信装置が前記認証装置に送信する認証要求が経由した基地局を特定し、該基地局の基地局情報に対応した前記期間情報と、前記無線通信装置が認証要求している時点との比較結果に基づいて、前記無線通信装置の前記ネットワークへの接続の認証をすることを特徴とする。

【００１２】

第６の発明は、第５の発明において、前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化し、暗号化された期間情報又は／及び基地局情報を前記無線通信装置に送出し、前記無線通信装置は、暗号化された期間情報又は／及び基地局情報を前記記憶部に記憶し、前記認証装置は、前記無線通信装置から取得した暗号化された期間情報又は基地局情報を、前記データ書込装置と共通の暗号鍵によって復号化して、前記無線通信装置の認証をすることを特徴とする。

【００１３】

第７の発明は、ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されてデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、を備えた通信システムに用いられる認証方法において、前記無線通信装置の記憶部には、前記データ書込装置により書き込まれる、前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を示す基地局情報に対応して認証情報として記憶されており、

前記無線通信装置は、前記認証情報を前記認証装置に送信し、前記認証装置は、前記無線通信装置が前記認証装置に送信した認証要求が経由した基地局を特定して、該基地局の情報を前記無線通信装置へ送信し、前記無線通信装置は、前記記憶部に記憶された基地局情報と、前記認証装置によって特定された基地局の情報との比較結果に基づいて、該基地局への接続可否を判定し、前記接続可否の判定の結果、該基地局への接続が可能と判定されると、前記無線通信装置は、該基地局の基地局情報に対応して前記記憶部に記憶された期間情報を送信し、前記認証装置は、前記無線通信装置が認証要求している時点と前記期間情報との比較結果に基づいて、前記無線通信装置の認証をすることを特徴とする。

【００１４】

第８の発明は、第７の発明において、前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化し、暗号化された期間情報又は／及び基地局情報を前記無線通信装置に送出し、前記無線通信装置は、暗号化された期間情報又は／及び基地局情報を前記記憶部に記憶し、前記認証装置は、前記無線通信装置から取得した暗号化された期間情報又は基地局情報を、前記データ書込装置と共通の暗号鍵によって復号化して、前記無線通信装置の認証をすることを特徴とする。

【００１５】

第９の発明は、第７の発明において、前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化し、暗号化された基地局情報を前記無線通信装置に送出し、前記無線通信装置は、暗号化された基地局情報を前記記憶部に記憶し、前記無線通信装置は、前記暗号化された基地局情報を前記データ書込装置と共通の暗号鍵によって復号化して、前記特定された基地局情報との比較結果に基づいて、該基地局への接続可否を判定することを特徴とする。

【００１６】

第１０の発明は、無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記

無線通信装置と接続される前記ネットワークと、前記無線通信装置から送信される認証要求が経由した基地局を特定する基地局特定手段を有し、前記認証要求が経由した基地局を特定して前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置と、によって構成される通信システムに用いられ、ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されデータ通信を行う無線通信装置において、無線通信装置の記憶部に認証情報を書き込むデータ書込装置が前記認証情報を前記記憶部に書き込むために接続される接続手段を有し、前記記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を表す前記基地局情報に対応して認証情報として記憶されることを特徴とする。

【００１７】

第１１の発明は、第１０の発明において、前記データ書込装置は、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化する暗号化手段を有し、前記無線通信装置の記憶部には、前記暗号化された認証情報を記憶する。

【００１８】

第１２の発明は、ネットワークへの接続時に使用する認証情報を記憶する記憶部を有し、前記ネットワークに接続されデータ通信を行う無線通信装置と、前記無線通信装置と無線通信を行う基地局と、前記基地局を経由して前記無線通信装置と接続される前記ネットワークと、前記無線通信装置から送信される認証要求が経由した基地局を特定する基地局特定手段を有し、前記認証要求が経由した基地局を特定して前記無線通信装置の前記ネットワークへの接続の認証をする認証装置と、によって構成される通信システムに用いられる、前記無線通信装置の記憶部に認証情報を書き込むデータ書込装置であって、前記無線通信装置の記憶部に、前記ネットワークへの接続可能期間を示す前記期間情報として書き込み、記無線通信装置の記憶部には、前記データ書込装置により書き込まれる前記ネットワークへの接続可能期間を示す前記期間情報が、前記無線通信装置が接続される基地局を表す前記基地局情報に対応して認証情報として記憶されることを特徴とする。

【００１９】

第１３の発明は、第１２の発明において、前記認証装置と共有する暗号鍵によって前記認証情報を暗号化する暗号化手段を有し、前記無線通信装置の記憶部に、前記暗号化された認証情報を書き込む。

【００２５】

【発明の実施の形態】

以下に、本発明の実施の形態について図面を参照して説明する。

【００２６】

図１は、本発明の実施の形態の通信システムの構成を表すブロック図である。

【００２７】

ユーザの端末１０には、無線通信装置としての無線ＬＡＮカード１００が接続されている。無線ＬＡＮカード１００はＰＣＭＣＩＡインターフェースを備えたＰＣカード形状であり、無線基地局としてのアクセスポイント３０と無線通信を行うことができ、端末１０は、無線ＬＡＮカード１００によって、アクセスポイント３０、ＩＳＰのネットワーク４０を介してインターネット５０と接続して、データ通信をすることができる。

【００２８】

アクセスポイント３０は無線基地局として機能し、無線ＬＡＮカード１００と通信をするための無線回路、変復調回路及びアンテナを有し、インターネット接続サービス業者（ＩＳＰ）のネットワーク４０と接続するインターフェースを有している。また、アクセスポイント３０には、無線ＬＡＮカード１００に対して認証情報を書き込むデータ書込装置としてのＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０が併設されている。

【００２９】

また、ＩＳＰのネットワーク４０は認証サーバを有し、無線ＬＡＮカード１００から送られてきた認証情報に基づいて、無線ＬＡＮカード１００（端末１０）からの接続要求が正

当なものであるか否かを判定する。また、ＩＳＰのネットワーク４０は複数のアクセスポイント（無線基地局）３０Ａ、３０Ｂ、３０Ｃと接続されており、各アクセスポイントの近傍にＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０Ａ、２０Ｂ、２０Ｃが設けられている。

【００３０】

図２は、無線ＬＡＮカード１００の構成を表したブロック図である。

【００３１】

ＰＣＭＣＩＡインターフェース１１０は、パーソナルコンピュータやＰＤＡ等のＰＣＭＣＩＡスロット又はＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０と接続するためのインターフェースであり、接続手段として機能する。

【００３２】

制御部１２０は、ＰＣＭＣＩＡインターフェース１１０、メモリ１３０、無線ＬＡＮ制御部１４０と接続し、各部の操作を制御して制御手段として機能する。

【００３３】

メモリ１３０は、ＩＳＰのネットワーク４０に接続するための認証に用いる認証情報として、接続するアクセスポイントを示すアクセスポイント情報及び接続する期間を示す期間情報を記憶して記憶部として機能する。メモリ１３０にはデータの読み書きを制限するアクセス制限手段が構成されている。すなわち、ユーザの端末１０からは読み書きができず、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０からのみ読み書きすることができるよう構成されている。例えば、ＰＣＭＣＩＡ規格の特定の空き端子をメモリへのアクセス制御用にして、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０から該端子に特定の信号を供給することによって、メモリ１３０を読み書き可能な状態にするように制御すれば、ユーザの端末１０からは該端子に特定の信号を供給することができず、メモリ１３０が読み書き可能状態にならない。また、ＩＳＰのネットワーク４０側（例えば、認証サーバ）からは無線ＬＡＮカード１００に予め搭載されているソフトウェアによって、無線通信回線を経由してメモリ１３０の内容を参照することができる。

【００３４】

無線ＬＡＮ制御部１４０は、無線回路及び変復調回路を有し、制御部１２０から送られたデータ信号を高周波信号に変換しアンテナ１５０に送り、またアンテナ１５０から送られた高周波信号をデータ信号に変換する。

【００３５】

アンテナ１５０は、無線ＬＡＮ制御部１４０から送られた高周波信号を電波に変換しアクセスポイント３０に送信し、またはアクセスポイント３０から受信した電波を高周波信号に変換し無線ＬＡＮ制御部１４０に送る。

【００３６】

なお、本実施の形態の無線ＬＡＮカード１００はＰＣＭＣＩＡカード形状であるが、これをコンパクトフラッシュ（登録商標）形状や他の形状としてもよいし、端末と一体型として端末側にＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０と接続するインターフェース（例えば、赤外線インターフェース）を備えるよう構成し、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０と接続されるインターフェースからのみメモリ１３０の内容を読み書き可能として、接続手段及びアクセス制限手段を構成してもよい。

【００３７】

図３は、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０の構成を説明する図である。

【００３８】

このＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０には、無線ＬＡＮカード１００を接続するためのインターフェースとしてＰＣＭＣＩＡスロット２０１が設けられている。また、アクセスポイントの場所の指定やアクセスポイントに接続する期間を指定する入力手段２０２、対価の支払いを受け入れる入金口２０３、釣り銭を排出する出金口２０４、購入した無線ＬＡＮカードを排出する排出口２０５、各種情報を表示するディスプレイ２０６が備えられている。

【００３９】

また、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０は、内部にＣＰＵ、メモリを有しており、入力手段２０２に入力された情報に基づいて、認証情報を生成、暗号化して、ＰＣＭＣＩＡスロット２０１に接続された無線ＬＡＮカード１００内のメモリ１３０に該認証情報を書き込む。

【００４０】

また、既に認証情報が書き込まれた無線ＬＡＮカード１００を販売する。

【００４１】

次に、上記のように構成された本発明の実施の形態の通信システムの動作を説明する。

【００４２】

本実施の形態の通信システムでは、従来のユーザＩＤやパスワードによる認証ではなく、接続するアクセスポイントを示すアクセスポイント情報と、接続する期間を示す期間情報とで構成される認証情報を用いてＩＳＰのネットワーク（認証サーバ）４０が無線ＬＡＮカード１００の認証を行うよう構成した。

【００４３】

図４に、メモリ１３０に記憶されている認証情報の例を示す。

【００４４】

例えば、図４では、番号１はアクセスポイント情報として「アクセスポイントＡ」（具体的には、アクセスポイントＡを示す番号）と、期間情報として「021101-021130」（２００２年１１月０１日から２００２年１１月３０日までの期間）とが第１認証情報として記録されており、該当する場所及び期間でネットワーク接続サービスが利用可能であることを示している。また、第２認証情報として、アクセスポイントＣにおける認証情報も記憶されており、複数のアクセスポイントでＩＳＰのネットワーク４０との接続が可能となっている。この認証情報は、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０をユーザが操作し、アクセスポイント情報と期間情報とを指定して代価と引き換えに（又は無償で）無線ＬＡＮカード１００に書き込むことができ、複数の認証情報をメモリ１３０に記憶することができる。

【００４５】

図５はこの認証情報の暗号化の説明図である。

【００４６】

ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０は、無線ＬＡＮカード１００に書き込む認証情報（アクセスポイント情報、期間情報）を、ＶｅｎｄｉｇＭａｃｈｉｎｅ２０とＩＳＰの認証サーバとで共有されている秘密鍵による秘密鍵方式によって暗号化して、無線ＬＡＮカード１００のメモリ１３０に書き込む。なお、本実施の形態では、秘密鍵を用いた共通鍵方式の暗号方式を用いたが、秘密鍵方式に代えて公開鍵方式を用いてもよいし、他の暗号方式を用いてもよい。このようにＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０のＣＰＵが動作することで認証情報を暗号化する暗号化手段が構成される。

【００４７】

無線ＬＡＮカード１００に記憶されている認証情報は、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０またはＩＳＰのネットワーク４０側からしか読み込むことはできないが、暗号化を行うことで認証情報のさらなる機密性が確保できる。なお、無線ＬＡＮカード１００の内部では暗号化された状態の認証情報で内容の検索等の処理を行う。

【００４８】

また、ＩＳＰのネットワーク（認証サーバ）４０では、無線ＬＡＮカード１００から認証要求として送信された暗号化された認証情報を、秘密鍵によって復号化して認証情報の内容を確認する。このように認証サーバに設けられたＣＰＵが動作することでＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０のＣＰＵが動作することで認証情報を復号化する復号化手段が構成される。

【００４９】

次に、図６の認証情報の書き込み手順のフローチャートを用いて、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０による無線ＬＡＮカード１００のメモリ１３０の書き込みの手順を説明する

。
【００５０】
ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０のＰＣＭＣＩＡスロット２０１に無線ＬＡＮカード１００が挿入されると、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０は、まず、無線ＬＡＮカード１００のメモリ１３０に認証情報として記憶されているアクセスポイント情報及び期間情報を読み出す（処理６０１）。
【００５１】
このメモリ１３０に保存されている認証情報は暗号化されているので、読み出した認証情報の復号化処理を行い、アクセスポイント情報と期間情報との内容が確認できる状態に変換する。（処理６０２）。
【００５２】
次に復号化した期間情報を参照し、既に期間が経過し期限切れとなっている認証情報があるか否かを判定する（処理６０３）。期限切れの認証情報がなければ処理６０５に移行し、期限切れとなっている認証情報があればその認証情報を削除する（処理６０４）。これは、メモリ１３０に書き込まれている認証情報はＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０でしか直接読み書きができないので、期限切れとなっている認証情報の削除もＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０から行うことが必要だからである。期限切れの認証情報の削除が完了すると処理６０５に移行する。
【００５３】
次に、ユーザの操作によって入力された、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０に接続するアクセスポイントのアクセスポイント情報、使用する期間情報を読み込み、相当する代価をユーザから受領する（処理６０５）。この操作によって、例えば、現在のアクセスポイント、他のアクセスポイント、全てのアクセスポイントといったアクセスポイント情報、本日から何日間、指定した日から何日間といった期間情報を指定することができる。指定を行うと場所及び期間に対して相当する対価の金額が表示され、ユーザは表示された対価を支払うことで操作が完了する。
【００５４】
代価の支払いが完了すると、ユーザによって入力されたアクセスポイント情報と期間情報とを、秘密鍵によって暗号化する（処理６０６）。
【００５５】
次に、暗号化されたアクセスポイント情報、期間情報を無線ＬＡＮカード１００のメモリ１３０に書き込む（処理６０７）。
【００５６】
以上の操作によって無線ＬＡＮカード１００への認証情報の書き込みが完了する。
【００５７】
図７は、無線ＬＡＮ１００に書き込まれた認証情報によってＩＳＰとの間で行われる第１の実施の形態としての認証処理のシーケンス図である。
【００５８】
まず、端末１０が認証を開始すると、無線ＬＡＮカード１００はＩＳＰのネットワーク（認証サーバ）４０に対して認証要求メッセージを送信する。
【００５９】
ＩＳＰの認証サーバは認証要求メッセージを受信すると、アクセスポイント情報応答処理を行う。この処理の詳細は図８において後述する。
【００６０】
ＩＳＰの認証サーバは、アクセスポイント情報応答メッセージとして、無線ＬＡＮカード１００からの認証情報が送信されてきた経路情報から特定されたアクセスポイントの情報を、アクセスポイント情報応答として無線ＬＡＮカード１００に送信する。
【００６１】
無線ＬＡＮカード１００は、アクセスポイント情報応答メッセージを受信すると、受信したアクセスポイントの情報を用いて期間情報検索処理を行う。この処理の詳細は図９にお

いて後述する。受信したアクセスポイントの情報と一致するアクセスポイント情報が検索されて期間情報検索処理が完了すると、無線ＬＡＮカード１００は期間情報提示メッセージをＩＳＰの認証サーバに送信する。

【００６２】

ＩＳＰの認証サーバは期間情報提示メッセージを受信すると、認証処理を行う。この処理の詳細は図１０において後述する。認証処理が完了すると、ＩＳＰの認証サーバは無線ＬＡＮカード１００に対して認証完了応答メッセージを送信する。無線ＬＡＮカード１００がこの認証完了応答メッセージを受信すると認証が成功し、端末１０とＩＳＰのネットワーク４０とが接続されて、端末１０が無線ＬＡＮカード１００を介したデータ通信が可能となる。

【００６３】

図８は、ＩＳＰの認証サーバにおけるアクセスポイント情報応答処理のフローチャートである。

【００６４】

まず、ＩＳＰの認証サーバが無線ＬＡＮカード１００より認証要求を受信すると（処理８０１）、該認証要求の経路情報を解析し、経路情報から該認証要求の送信元となっており、認証情報を送信した無線ＬＡＮカード１００が接続しているアクセスポイント３０を特定する（処理８０２）。

【００６５】

次に、特定したアクセスポイント情報（アクセスポイントの番号）を秘密鍵によって暗号化し、暗号化されたアクセスポイント情報を無線ＬＡＮカード１００に対して送信する（処理８０３）。この処理によって、特定したアクセスポイント情報によって無線ＬＡＮカード１００のメモリ１３０に記憶されている暗号化されたアクセスポイント情報を検索することができるようになり、認証情報の内容は他人にはわからないので、認証情報の機密性を確保できる。

【００６６】

図９は、無線ＬＡＮカード１００における期間情報検索処理のフローチャートである。

【００６７】

まず、無線ＬＡＮカード１００は、アクセスポイント情報応答メッセージとしてＩＳＰの認証サーバから送信されたアクセスポイント（基地局）の情報を受信する（処理９０１）。次に、受信したアクセスポイントの情報に基づいてメモリ１３０に記憶されているアクセスポイント情報を検索し（処理９０２）、アクセスポイント情報が一致する認証情報が記憶されているか否かを判定する（処理９０３）。

【００６８】

一致する認証情報が記憶されている場合には、該当する認証情報の期間情報（暗号化されて記憶されている）をＩＳＰの認証サーバに対して送信する（処理９０４）。メモリ１３０に記憶されているアクセスポイント情報とＩＳＰから送信された暗号化されたアクセスポイントの情報とは同一の秘密鍵によって暗号化されているので、暗号化されたアクセスポイントの情報が一致すれば暗号化前のアクセスポイント情報も一致する。

【００６９】

一方、アクセスポイントの情報が一致する認証情報が記憶されていない場合には、現在端末１０が接続しているアクセスポイント３０からはＩＳＰのネットワーク４０へ接続することができないので、無線ＬＡＮカード１００は端末１０に認証が失敗した旨を通知し、端末１０の表示画面にはアクセス不可である旨が表示される（処理９０５）。そして、無線ＬＡＮカード１００は、ＩＳＰの認証サーバに対して認証要求の中止を通知し認証の処理を終了する（処理９０６）。

【００７０】

このように、無線ＬＡＮカード１００において期間情報検索処理が行われることで、接続可否判定手段が構成される。

【００７１】

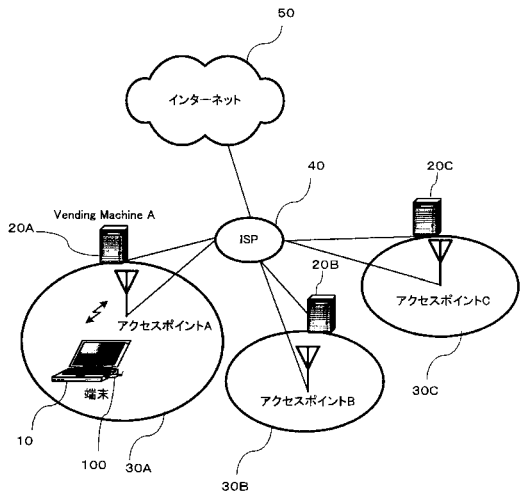
図１０は、図７におけるＩＳＰの認証サーバにおける認証処理のフローチャートである。
【００７２】
ＩＳＰの認証サーバが端末１０から送信された期間情報を受信すると（処理１００１）、この期間情報は暗号化されているので、秘密鍵によって期間情報を復号化する（処理１００２）。
【００７３】
次に、復号化した期間情報を参照し、期間情報が有効な情報であるか否か、すなわち、現在の日時は復号化された期間情報に規定される期間内に含まれているか否かを判定する（処理１００３）。現在の日時が期間情報に含まれており、期間情報が有効であると判定された場合には、認証成功とし、無線ＬＡＮカード１００との通信のセッションを確立し（処理１００４）、接続完了のメッセージを無線ＬＡＮカード１００に送信する（処理１００５）。セッション確立によって端末１０が、無線ＬＡＮカード１００、ＩＳＰのネットワーク４０を経由してインターネットに接続が可能となる。
【００７４】
一方、現在の日時が期間情報に含まれておらず、期間情報が有効でないと判定された場合には、無線ＬＡＮカード１００に対して接続不可である旨を通知し（処理１００６）、認証処理を終了する。
【００７５】
以上の処理によって、ＩＳＰの認証サーバによる無線ＬＡＮカード１００の認証が完了し、ＩＳＰのネットワーク４０と無線ＬＡＮカード１００との間のセッションが確立して、端末１０が、無線ＬＡＮカード１００とＩＳＰのネットワーク４０とを経由してインターネットに接続され、データ通信が行われる。
【００７６】
このように、ＩＳＰのネットワーク４０側（認証サーバ）において認証処理が行われることで、認証手段が構成される。
【００７７】
図１１は、本発明の第２の実施の形態としての認証情報のシーケンス図である。
【００７８】
まず、端末１０が認証を開始すると、無線ＬＡＮカード１００はＩＳＰのネットワーク（認証サーバ）４０に対して認証要求メッセージを送信する。
【００７９】
ＩＳＰの認証サーバは認証要求メッセージを受信すると、無線ＬＡＮカード１００からの認証情報が送信されてきた経路情報から特定されたアクセスポイントの情報を取得すると共に、無線ＬＡＮカード１００に対して認証情報を送信するよう要求する。（認証情報要求処理）。この認証情報要求処理によって無線ＬＡＮカード１０に対して認証情報要求メッセージが送信される。
【００８０】
無線ＬＡＮカード１００は、認証情報要求メッセージを受信すると、認証のための認証情報をメモリ１３０に保存されている期間情報及びアクセスポイント情報から取得しＩＳＰの認証サーバに対して送信する（認証情報送出処理）。この認証情報送出処理によってＩＰＳの認証サーバに対して認証情報送出メッセージが送信される。
【００８１】
ＩＳＰの認証サーバは認証情報送出メッセージを受信すると、受信した認証情報によって認証処理を行う。すなわち、受信したアクセスポイントの情報と認証情報要求処理によって特定したアクセスポイントの情報が一致するか否かを判定し、さらに、現在の日時が期間情報に含まれており、期間情報が有効であるか否かを判定する。前記の判定によって認証が可能であれば、認証処理が完了し、ＩＳＰの認証サーバは無線ＬＡＮカード１００に対して認証完了応答メッセージを送信する。無線ＬＡＮカード１００がこの認証完了応答メッセージを受信すると認証が成功し、端末１０とＩＳＰのネットワーク４０とが接続されて、端末１０が無線ＬＡＮカード１００を介したデータ通信が可能となる。

【００８２】
前述したように構成された本発明の実施の形態の通信システムでは、従来のように認証データベースに登録されたＩＤ及びパスワードによって認証を行うのではなく、無線ＬＡＮカードがアクセスするホットスポットの場所を示すアクセスポイント情報と、アクセスする期間を示す期間情報とによって認証を行うので、ホットスポットを利用するユーザが予めＩＤとパスワードとによる認証情報を登録しなくても、利用したいホットスポットでＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０を操作することで簡単に認証情報を入手することができ、ユーザの利便性が向上すると共に、ＩＳＰが認証用データベースによるユーザの認証情報を管理する必要がなくなり、ＩＳＰに備えられる認証サーバの管理がより簡便となる。
【００８３】
また、ユーザは、認証時にＩＤ及びパスワードを必要とせず、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０によって即座に認証情報を入手できるので迅速にサービスの提供を受けることができ、また、認証の処理は無線ＬＡＮカード１００とＩＳＰの認証サーバとの間で自動的に行われるので、キーボードを用いた煩わしい入力操作の必要がなくなり、ユーザの利便性が向上する。
【００８４】
また、ノートパソコンなどのユーザの端末１０に接続する無線ＬＡＮカード１００に、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０からのみ認証情報の読み書きが可能で、無線通信経由でＩＳＰのネットワーク４０（認証サーバ）側から読み込みが可能なメモリ１３０を備えたので、ユーザの端末１０からはアクセスポイント情報と期間情報とで構成される認証情報を参照することができないため、認証情報の機密性を高めることができる。
【００８５】
さらに、メモリ１３０に格納されるアクセスポイント情報と期間情報とで構成される認証情報は、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０とＩＳＰ４０とで共有する秘密鍵によって暗号化されているので、より高い機密性を確保することができる。
【００８６】
次に、本発明の実施の形態の通信システムの利用形態として、無線ＬＡＮを用いたインターネット接続サービスの提供方式の一例について説明する。
【００８７】
アクセスポイント３０は、例えば、喫茶店やファーストフード店などの店舗内に設け、ユーザの持参したノートパソコンやＰＤＡ等から利用できる方式や、町中の電信柱等に設置し電波伝搬範囲をアクセスポイントとし、路上、自宅、オフィスなどのパソコンなどから、無線ＬＡＮによるインターネット接続サービス利用できる方式などがある。
【００８８】
例えば、ファーストフード店をアクセスポイントとした場合には、店舗内にＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０を設置し、無線ＬＡＮカード１００の購入、アクセスポイント情報及び期間情報の購入を店舗内で行うことができる。なお、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０をユーザが直接操作できる場所には設置せず、店員との対話形式によって無線ＬＡＮカード１００の購入、アクセスポイント情報及び期間情報の購入を行い、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０の操作は店員が行ってもよい。
【００８９】
無線ＬＡＮカード１００は保証金込みで販売され、無線ＬＡＮカードが不要になった場合には、その返還時に保証金を返却する。
【００９０】
また、アクセスポイント情報及び期間情報の金額は、例えば１ヶ所のアクセスポイントのみを１日間のみ使用する場合には１００円、ＩＳＰのネットワーク４０に接続可能な全てのアクセスポイントを１年間使用する場合には１０、０００円、というように、アクセスポイントの場所の数や利用する期間に応じて段階的に適宜設定することができる。
【００９１】
このＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０における課金情報の生成の手順を図１２に示す。

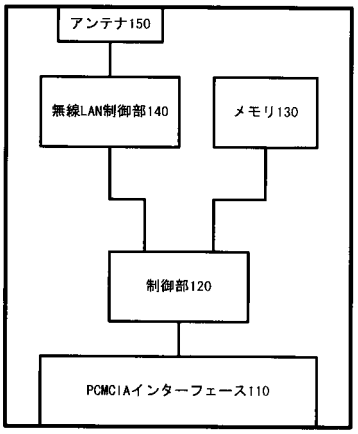
【００９２】
まず、ユーザの操作によって無線ＬＡＮカード１００によってアクセスを行いたいアクセスポイントを選択する（処理１２０１）。これは例えば、現在のアクセスポイントを指定したり、他のアクセスポイントや、ＩＳＰのネットワーク４０に接続可能な全てのアクセスポイントといった指定ができる。
【００９３】
次に、選択されたアクセスポイントの数に応じた金額を、予めＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０に設定し登録されたアクセスポイント金額テーブルより読み出し、取得する（処理１２０２）。本発明の実施の形態では、接続したいアクセスポイントの数に応じて金額が加算されるよう、予めアクセスポイント金額テーブルが登録されている。
【００９４】
次に、ユーザの操作によってアクセスしたい期間を入力する（処理１２０３）。これは例えば、１日、２日、１週間、１ヶ月、１年…と言った期間が指定できる。次に、ＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０は、選択された期間に応じた金額を予めＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０に設定し登録された期間金額テーブルより読み出し、取得する。（処理１２０４）本発明の実施の形態は、期間の長さによって金額が加算されるよう、予め金額テーブルに設定されている。
【００９５】
次に、処理１２０２及び１２０４にて取得した金額を加算し、合計金額を算出する（処理１２０５）。
【００９６】
以上の処理によって、アクセスポイント及びアクセスする期間から、課金情報が生成され、ユーザに対して必要な代価の支払いをユーザに通知することができる。
【００９７】
そして、購入した無線ＬＡＮカード１００、又は、期間情報及びアクセスポイント情報を書き込んだ無線ＬＡＮカード１００をユーザの持参したノートパソコンやＰＤＡなどに挿入することで、ホットスポットを介した通信によるインターネット接続が利用可能になる。
【００９８】
【発明の効果】
本発明によると、サービス提供業者は、無線通信装置（無線ＬＡＮカード）に記憶された期間情報及びアクセスポイント情報によって構成された認証情報によって無線通信装置を認証するので、予め認証情報を登録しておく必要がなく、ユーザの管理が簡便になる。
【００９９】
また、認証情報は、データ書換装置によってのみ書換可能で、サービス提供業者によってのみ読み出し可能なので、期間情報とアクセスポイント情報を第三者に知られる危険性が低くなる。さらに、この認証情報は、データ書換装置とサービス提供業者とで共有された暗号鍵によって暗合化されているので、認証情報の機密性をより高めることができる。
【図面の簡単な説明】
【図１】　本発明の実施の形態の通信システムの構成を表すブロック図である。
【図２】　本発明の実施の形態の無線ＬＡＮカード１００の構成を表したブロック図である。
【図３】　本発明の実施の形態のＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０の構成の説明図である。
【図４】　本発明の実施の形態の認証情報の説明図である。
【図５】　本発明の実施の形態の認証情報の暗号化の説明図である。
【図６】　本発明の実施の形態のＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０による無線ＬＡＮカード１００への認証情報の書き込み手順のフローチャートである。
【図７】　本発明の第１の実施の形態の無線ＬＡＮカード１００とＩＳＰとによって行われる認証処理のシーケンス図である。

【図８】　本発明の第１の実施の形態のＩＳＰの認証サーバにおける場所応答処理のフローチャートである。
【図９】　本発明の第１の実施の形態の無線ＬＡＮカード１００における期間情報検索処理のフローチャートである。
【図１０】　本発明の第１の実施の形態のＩＳＰの認証サーバにおける期間情報検索処理のフローチャートである。
【図１１】　本発明の第２の実施の形態の無線ＬＡＮカード１００とＩＳＰとによって行われる認証処理のシーケンス図である。
【図１２】　本発明の実施の形態のＶｅｎｄｉｎｇＭａｃｈｉｎｅ２０における課金情報の生成のフローチャートである。
【符号の説明】
１０　端末
２０Ａ、２０Ｂ、２０Ｃ　ＶｅｎｄｉｎｇＭａｃｈｉｎｅ
３０Ａ、３０Ｂ、３０Ｃ　アクセスポイント
４０　ＩＳＰのネットワーク
５０　インターネット
１００　無線ＬＡＮカード

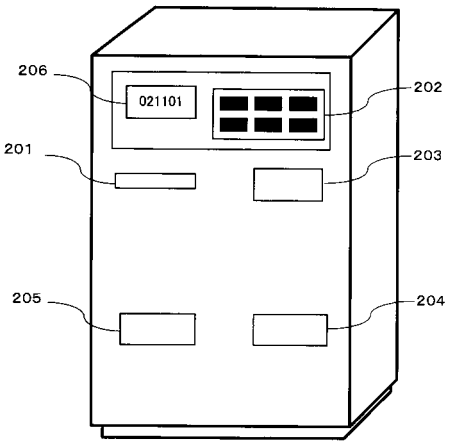
【図１】



【図２】



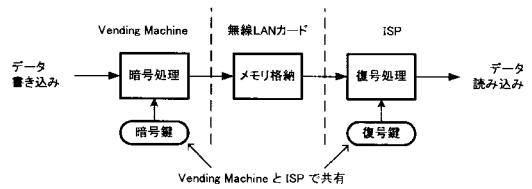
【図３】



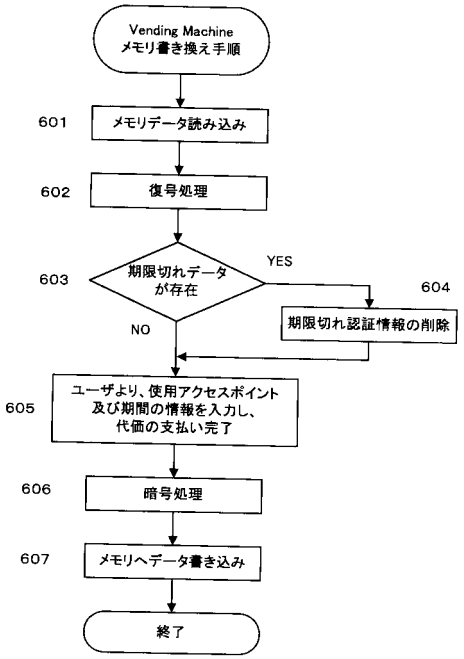
【図４】

番号	アクセスポイント情報	期間情報
1	アクセスポイントA	021101-021130
2	アクセスポイントC	021111-021111
…	…	…
…	…	…

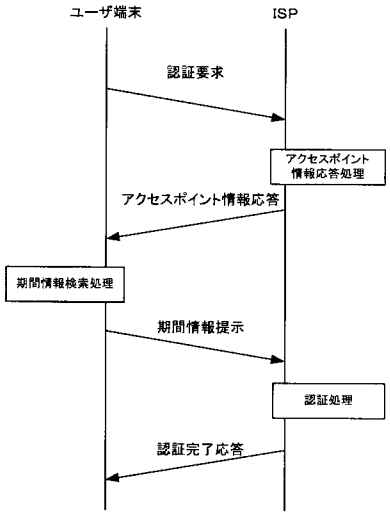
【図５】



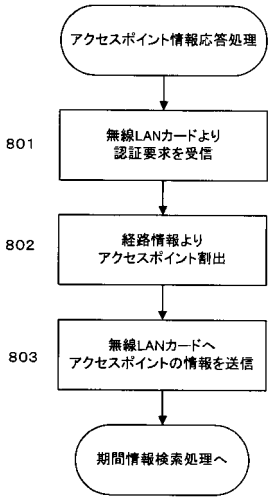
【図６】



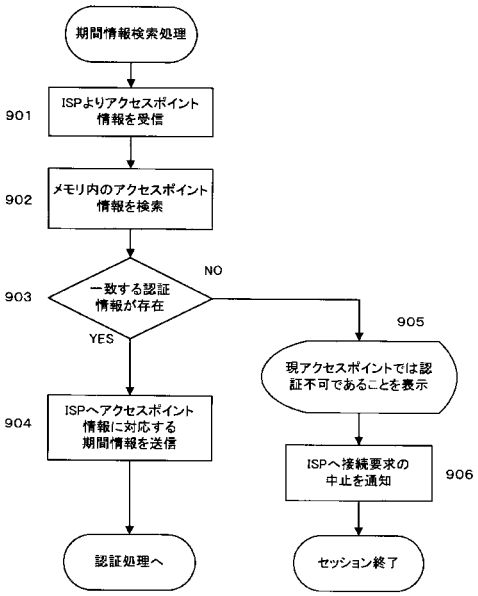
【図７】


ユーザ端末
ISP
認証要求
アクセスポイント
情報応答処理
アクセスポイント情報応答
期間情報検索処理
期間情報提示
認証処理
認証完了応答

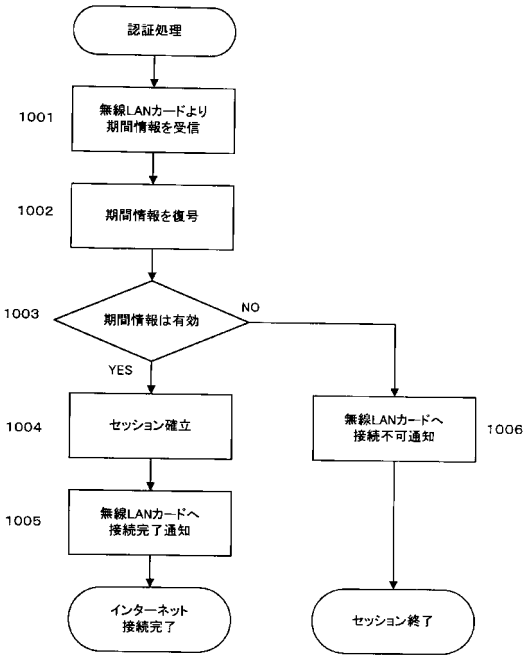
【図８】


アクセスポイント情報応答処理
801
無線LANカードより
認証要求を受信
802
経路情報より
アクセスポイント割出
803
無線LANカードへ
アクセスポイントの情報を送信
期間情報検索処理へ

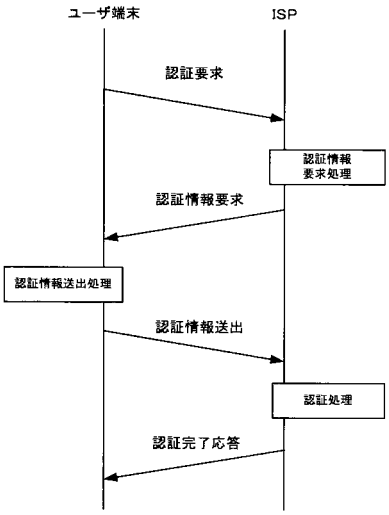
【図９】


期間情報検索処理
901
ISPよりアクセスポイント
情報を受信
902
メモリ内のアクセスポイント
情報を検索
903
一致する認証
情報が存在
NO
YES
905
現アクセスポイントでは認
証不可であることを表示
904
ISPへアクセスポイント
情報に対応する
期間情報を送信
ISPへ接続要求の
中止を通知
906
認証処理へ
セッション終了

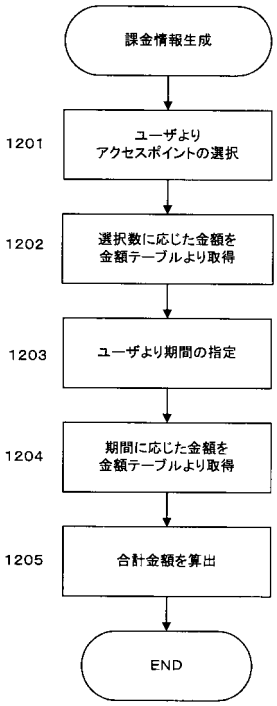
【図１０】


認証処理
1001
無線LANカードより
期間情報を受信
1002
期間情報を復号
1003
期間情報は有効
NO
YES
1004
セッション確立
1006
無線LANカードへ
接続不可通知
1005
無線LANカードへ
接続完了通知
インターネット
接続完了
セッション終了

【図１１】


ユーザ端末
ISP
認証要求
認証情報
要求処理
認証情報要求
認証情報送出処理
認証情報送出
認証処理
認証完了応答

【図１２】


課金情報生成
1201
ユーザより
アクセスポイントの選択
1202
選択数に応じた金額を
金額テーブルより取得
1203
ユーザより期間の指定
1204
期間に応じた金額を
金額テーブルより取得
1205
合計金額を算出
END

フロントページの続き

(51)Int.Cl. F I
H04L 12/28 300Z

(56)参考文献 特開平09－312708（JP，A）
特開2000－115417（JP，A）
特開2000－032177（JP，A）
国際公開第02／058326（WO，A1）
特開2002－315058（JP，A）
特開2001－189722（JP，A）

(58)調査した分野(Int.Cl.，DB名)
H04B 7/24/7/26
H04Q 7/00-7/38