(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2006-166315
(P2006-166315A)
(43)公開日　平成18年6月22日(2006.6.22)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/56	(2006.01)	H04L 12/56	B	5K030

審査請求 未請求　請求項の数 4　OL　（全 14 頁）

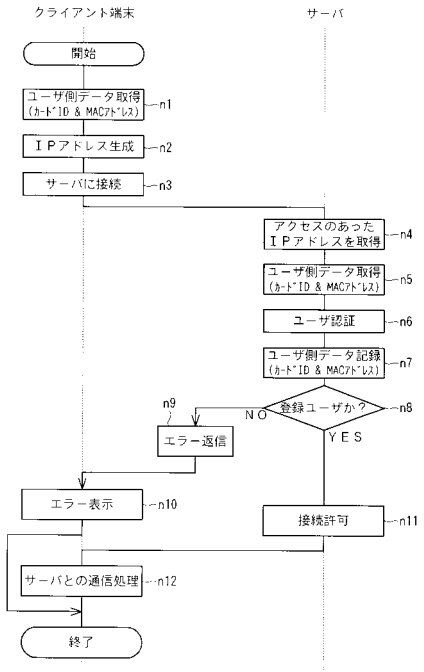
(21)出願番号　特願2004-358074 (P2004-358074)
(22)出願日　平成16年12月10日 (2004.12.10)

(71)出願人　504456145
株式会社ＺＥＲＯ
東京都大田区仲池上１丁目２６番１５－５０４号
(74)代理人　100067747
弁理士　永田　良昭
(74)代理人　100121603
弁理士　永田　元昭
(72)発明者　調子　友一
兵庫県尼崎市築地北浜２－１７－５０５

Ｆターム(参考)　5K030 HC01　KA06

(54)【発明の名称】ユーザ識別システム及びＩＰアドレス生成方法

(57)【要約】
【課題】
接続してきたクライアント端末３０とユーザとを確実に識別できるユーザ識別システム１及びＩＰアドレス生成方法を提案し、ネットワーク接続の利便性と安全性を高めて利用者の満足度を向上する。
【解決手段】
サーバ１０にアクセスするユーザを識別するユーザ識別システムを、ユーザが所持するＲＦ－ＩＤカード５０に記憶しているカードＩＤとクライアント端末３０に記憶しているＭＡＣアドレスとに基づいてクライアント端末３０がＩＰアドレスを生成し、該ＩＰアドレスを使用してクライアント端末３０が前記サーバ１０にアクセスすると、サーバ１０が、そのＩＰアドレスに基づいて前記カードＩＤ及び前記ＭＡＣアドレスを取得してユーザを識別する構成とした。
【選択図】　図９



【特許請求の範囲】
【請求項１】
管理装置とクライアント装置とを電気通信回線を通じて接続し、前記管理装置が前記クライアント装置からアクセスしてくるユーザを識別するユーザ識別システムであって、
前記クライアント装置を、ユーザが所持する媒体に記憶している媒体情報とクライアント装置に記憶しているクライアント情報とに基づいてＩＰアドレスを生成するＩＰアドレス生成処理と、該ＩＰアドレスを使用して前記管理装置にアクセスするアクセス処理とを実行する構成とし、
前記管理装置を、前記クライアント装置がアクセスに使用したＩＰアドレスに基づいて前記媒体情報及び前記クライアント情報を取得するユーザ識別処理を実行する構成としたユーザ識別システム。
【請求項２】
前記媒体に、ＩＣとアンテナとを備えて該アンテナにより非接触で通信する非接触ＩＣ媒体を使用する構成とした
請求項１記載のユーザ識別システム。
【請求項３】
前記ユーザ識別処理を、前記ＩＰアドレスから前記媒体情報及び前記クライアント情報を取得する処理で構成した
請求項１又は２記載のユーザ識別システム。
【請求項４】
非接触ＩＣ媒体に記憶した情報と、クライアント装置に記憶した情報とに基づいてＩＰアドレスを生成する
ＩＰアドレス生成方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、例えば管理装置がクライアント装置からアクセスするユーザを認識するようなユーザ認識システム、及びこれに使用するＩＰアドレス生成方法に関する。
【背景技術】
【０００２】
従来、インターネットやイントラネットやＬＡＮ等、電気通信回線を使用してコンピュータを接続する方法として、ＩＰアドレスを用いる方法が利用されている。このＩＰアドレスは、コンピュータ毎に異なるＩＰアドレスを手動で割当てて使用するか、ＤＨＣＰ（Dynamic Host Configuration Protocol）を利用して自動で割当てて使用されている。
【０００３】
一方、接続したユーザの識別や認証には、コンピュータにログインした際のユーザ名とパスワードによって行われることが一般的となっており、この他にも指紋や虹彩等を利用するものも提案されている。
【０００４】
しかし、これらの従来の方法では、ＩＰアドレスは単に複数のコンピュータ間のデータ通信を混乱無く適切に行うに使用され、ユーザ認証はユーザ名とパスワード等の別途の方法で行うために、手続が煩雑で時間がかかることとなっていた。
【０００５】
一方、ログインユーザ名とアプリケーション名からＩＰアドレスを生成する情報処理システムが提案されている（特許文献１参照）。
【０００６】
また、機器タイプデータとＭＡＣアドレスとルータから受信したプレフィックスからＩＰアドレスを生成するＩＰアドレス作成装置が提案されている（特許文献２参照）。
【０００７】
また、ＭＡＣアドレスに基づくインタフェースＩＤと設置位置情報に基づくプレフィッ

クスからＩＰアドレスを生成するＩＰアドレス作成装置が提案されている（特許文献３参照）。

【０００８】

また、適当なＩＰアドレスを生成し、生成したＩＰアドレスに重複があればＩＰアドレスの生成を再実行することで、一意性を確保したＩＰアドレスの生成を行うＩＰアドレス生成方法が提案されている（特許文献４参照）。

【０００９】

また、ユーザが所有するＩＣカードにＩＰアドレスを格納しておき、このＩＰアドレスを用いて通信を行う健康情報管理サーバが提案されている（特許文献５参照）。

【００１０】

これらの方法や装置により、ＩＰアドレスにログインユーザ名等の情報を含めることや、ＩＰアドレスからユーザ情報を取得することが可能とされている。

【００１１】

しかし、ログインユーザ名でユーザを識別する場合には、成りすましが容易に行えるため、ユーザ認証での成りすましを防止するためにはクライアント装置へのログイン時のパスワード管理等を適切に行なう必要がある。またこの方法では、ユーザがどのようなクライアント端末を使用したかは識別できない。

【００１２】

また、ＭＡＣアドレスを利用する場合には、クライアント装置は特定できてもユーザを特定できないため、クライアント装置を不正使用することで誰でも不正アクセスができてしまう。

【００１３】

また、ユーザが所有するＩＣカードにＩＰアドレスを格納しておく方法では、ＩＣカードの記憶しているＩＰアドレスを変更できる問題がある。またこの方法では、ユーザがどのようなクライアント端末を使用したかは識別できない。

【００１４】

このように、従来の方法ではユーザ側の識別を行うには不十分であるという問題があった。

【００１５】

【特許文献１】特開２００３－３３３０６７号公報
【特許文献２】特開２００３－２９８６１９号公報
【特許文献３】特開２００３－３０４２４６号公報
【特許文献４】特開２００３－３１８９４３号公報
【特許文献５】特開２００４－５４８１７号公報

【発明の開示】

【発明が解決しようとする課題】

【００１６】

この発明は、上述の問題に鑑み、接続してきたクライアント装置とユーザとを確実に識別できるユーザ識別システム及びＩＰアドレス生成方法を提案し、ネットワーク接続の利便性と安全性を高めて利用者の満足度を向上することを目的とする。

【課題を解決するための手段】

【００１７】

この発明は、管理装置とクライアント装置とを電気通信回線を通じて接続し、前記管理装置が前記クライアント装置からアクセスしてくるユーザを識別するユーザ識別システムであって、前記クライアント装置を、ユーザが所持する媒体に記憶している媒体情報とクライアント装置に記憶しているクライアント情報とに基づいてＩＰアドレスを生成するＩＰアドレス生成処理と、該ＩＰアドレスを使用して前記管理装置にアクセスするアクセス処理とを実行する構成とし、前記管理装置を、前記クライアント装置がアクセスに使用したＩＰアドレスに基づいて前記媒体情報及び前記クライアント情報を取得するユーザ識別処理を実行する構成としたユーザ識別システムであることを特徴とする。

【００１８】
前記クライアント装置は、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistance）、又はインターネット接続機能を有する携帯電話等、電気通信回線を通じた通信が可能な装置で構成することを含む。
【００１９】
前記管理装置は、サーバ又はルータ等、複数のクライアント装置からＩＰアドレスを利用した接続を許容する装置で構成することを含む。
前記電気通信回線は、インターネット等の公衆回線、又はＬＡＮ（Local Area Network）等、双方向に通信を行う回線で構成することを含む。
【００２０】
前記媒体は、ＩＣに情報を記憶しておき非接触で通信する非接触ＩＣタグや非接触ＩＣカード等の非接触ＩＣ媒体、ＩＣに情報を記憶しておき接触して通信する接触ＩＣカード等の接触ＩＣ媒体、又は、磁気テープ部に情報を記憶した磁気カード等の磁気媒体等、情報を記憶する媒体で構成することを含む。
【００２１】
前記媒体情報は、非接触ＩＣ媒体のユニークなＩＤ（ＵＩＤ）等の媒体固有の識別情報、又はユーザに付与して媒体に記憶させたユーザＩＤ等、媒体に記憶している情報で構成することを含む。
【００２２】
前記クライアント情報は、クライアント装置の通信手段が記憶しているＭＡＣアドレス等、クライアント装置を特定可能な情報で構成することを含む。
前記ＩＰアドレスは、ＩＰｖ６（Internet Protocol Version 6）又はＩＰｖ４といったプロトコルで用いられる識別番号で構成することを含む。
【００２３】
前記構成により、通信に用いられるＩＰアドレスから、ユーザとクライアント装置とを確実に識別することができる。従って、従来のように一端接続してからユーザ認証を行うといった２段階の処理が不要であり、ユーザとクライアント装置の識別を高速に行うことができる。
【００２４】
またこの発明の態様として、前記媒体に、ＩＣとアンテナとを備えて該アンテナにより非接触で通信する非接触ＩＣ媒体を使用するすることができる。
前記非接触ＩＣ媒体は、リーダライタが発生する磁界をアンテナで受けてこれにより起電力を得て駆動するタイプ、あるいは電池等の電源を備えてこの電源の電力で駆動するタイプで構成することを含む。
【００２５】
前記構成により、磁気カード等のようにユーザが媒体をリーダライタに挿入する手間が防止でき、非接触ＩＣ媒体を置くあるいはかざすといった簡単な操作で非接触ＩＣ媒体に記憶した情報をクライアント装置に読取らせることができる。
【００２６】
また非接触ＩＣ媒体は記憶容量が大きいため、データ長の長いＩＤを記憶させてこれを媒体情報とすることが可能となり、また非接触ＩＣ媒体の固有識別情報であるＵＩＤを媒体情報とすることも可能となる。
【００２７】
またこの発明の態様として、前記ユーザ識別処理を、前記ＩＰアドレスから前記媒体情報及び前記クライアント情報を取得する処理で構成することができる。
この処理は、クライアント装置がＩＰアドレスを生成した逆の手順で前記媒体情報及び前記クライアント情報を取得する処理で構成することを含む。
【００２８】
前記構成により、クライアント装置が管理装置へのアクセスに使用するＩＰアドレスから即座に前記媒体情報及び前記クライアント情報を取得することができ、ユーザ側の識別

を高速に行うことができる。
【００２９】
またこの発明は、非接触ＩＣ媒体に記憶した情報と、クライアント装置に記憶した情報とに基づいてＩＰアドレスを生成するＩＰアドレス生成方法とすることができる。
【００３０】
これにより、クライアント装置でそのユーザ用のＩＰアドレスを自動生成することができる。また、クライアント装置を利用するユーザによってＩＰアドレスを変更することができ、例えばクライアント装置のログオフや電源ＯＦＦ等を行わずに、非接触ＩＣ媒体の切り替えによって切り替えたユーザ用のＩＰアドレスで管理装置と接続するといったことも可能となる。
【発明の効果】
【００３１】
この発明により、通信に用いられるＩＰアドレスから、ユーザとクライアント装置とを確実に識別することができる。
【発明を実施するための最良の形態】
【００３２】
この発明の一実施形態を以下図面と共に説明する。
まず、図１に示すシステム構成図、及び図２に示す部分拡大斜視図と共に、ユーザ識別システム１の全体構成について説明する。
ユーザ識別システム１には、インターネット３に接続して、１台のサーバ１０と、複数台のクライアント端末３０を備えている。
【００３３】
前記サーバ１０には、管理データベース（ＤＢ）１９を備えており、アクセスを許容するクライアント端末３０を管理している。
前記クライアント端末３０には、図２に示すようにＲＦ－ＩＤカードリーダライタ３２を備えており、ＲＦ－ＩＤカード５０と非接触で通信してデータの読書きを行う。
【００３４】
ここで、ＲＦ－ＩＤカード５０は制御部と記憶部とを有するＩＣチップ５２と、非接触通信を行うアンテナコイル５１とを備えて構成しており、ＲＦ－ＩＤカードリーダライタ３２が発生させる磁界によって起電力を得て応答処理を実行する。記憶部には、メーカーにて固有の識別番号として記録されたユニークなＩＤ（ＵＩＤ）と、ユーザの氏名や所属等の必要な情報とを格納している。
また、ＲＦ－ＩＤカードリーダライタ３２には、ＲＦ－ＩＤカード５０と通信するためのアンテナコイルを備えている。
【００３５】
以上のシステム構成により、クライアント端末３０はＲＦ－ＩＤカード５０のデータを読み取ることができ、インターネット３を介してサーバ１０にアクセスすることができる。
【００３６】
次に、図３に示すブロック図、及び図４～図６に示すデータ説明図と共に、サーバ１０の構成について説明する。
サーバ１０は、デスクトップＰＣで構成しており、制御装置１１に接続して、記録媒体処理装置１２、入力装置１３、表示装置１４、通信装置１５、及び記憶装置１６を備えている。
【００３７】
記録媒体処理装置１２は、ＣＤ－ＲＯＭドライブやフレキシブルディスクドライブ等、記録媒体にデータを読書きする装置であり、読取った情報を制御装置１１に送信し、制御装置１１から受信した情報を記録媒体に書き込む。
【００３８】
入力装置１３は、マウスやキーボード等、座標入力やキー入力といった入力を受け付け

る装置であり、入力された入力信号を制御装置１１に送信する。
表示装置１４は、液晶モニタ等の文字や画像を表示する装置であり、制御装置１１から受信する表示信号に従って表示を行う。
【００３９】
通信装置１５は、ＬＡＮボード等の通信可能な装置であり、制御装置１１に制御に従って、インターネット３を介したデータの送信や受信を実行する。
記憶装置１６には、ハードディスク等のデータを記憶する装置であり、各種データやプログラムを格納する。プログラムとしては、ユーザ側の情報を復元するユーザ側情報復元プログラム１７、及びユーザ認証を行うユーザ認証プログラム１８等を格納している。またデータとしては、アクセス許可するユーザやクライアント端末に関する各種データを記録する管理データベース１９等を格納している。
【００４０】
ここで、管理データベース１９は、図４～図６のデータ説明図に示すように、登録ユーザテーブル１９ａ、登録機器テーブル１９ｂ、及びアクセス履歴テーブル１９ｃといったテーブルデータで構成している。
【００４１】
登録ユーザテーブル１９ａは、図４に示すように、カードＩＤ、ユーザ名、更新日（若しくは登録日）、及び有効期限等の項目（フィールド）で構成する。
【００４２】
カードＩＤには、ユーザが保有するＲＦ－ＩＤカード５０のＵＩＤを格納する。このＵＩＤは、メーカーナンバーと製品ナンバーとからユニークに決定されている６４ｂｉｔのＩＤであり、後述するようにＩＰアドレスの生成に使用する。
【００４３】
なお、前記カードＩＤは、書換不可能な領域に格納しておくことが望ましい。また、このカードＩＤの替わりに、ユーザに付与したユーザＩＤをＲＦ－ＩＤカード５０に格納し、このユーザＩＤを使用する構成としても良い。
【００４４】
ユーザ名には、ユーザの氏名を格納する。
更新日には、そのユーザの登録データ内容を最後に更新した年月日を格納する。
有効期限には、登録したユーザに対して登録内容での利用を許可する期限の年月日を格納する。
【００４５】
登録機器テーブル１９ｂは、図５に示すように、ＭＡＣアドレス、機器名称、更新日、有効期限、及び使用可能ユーザ等の項目で構成する。
ＭＡＣアドレスは、クライアント端末３０の通信装置３６（後述の図６）に書換え不可能に記憶している機器固有のユニークなアドレスである。
【００４６】
機器名称には、クライアント端末３０の名称を示し、運用にて適宜定めた名称を格納する。
更新日には、そのクライアント端末３０の登録データ内容を最後に更新した年月日を格納する。
【００４７】
有効期限には、登録したユーザに対して登録内容での利用を許可する期限の年月日を格納する。
使用可能ユーザには、そのクライアント端末３０を使用してのサーバ１０へのアクセスを許容するユーザのカードＩＤをユーザＩＤとして格納する。
【００４８】
アクセス履歴テーブル１９ｃは、図６に示すように、履歴ナンバー、ＭＡＣアドレス、カードＩＤ、任意データ、アクセス可否、アクセス日、及びアクセス時刻等の項目で構成する。

【００４９】
履歴ナンバーは、履歴を記憶する毎に採番して記憶する履歴の順番を格納する。
ＭＡＣアドレスには、アクセスしたクライアント端末３０の通信装置のＭＡＣアドレスを格納する。
【００５０】
カードＩＤには、アクセスしたクライアント端末３０のＲＦ－ＩＤカードリーダライタ３２（図２）で読取ったカードＩＤ、すなわち利用しているユーザが所持するＲＦ－ＩＤカード５０のカードＩＤを格納する。
【００５１】
任意データには、後述する生成したＩＰアドレスに使用した任意データを格納する。なお、この任意データの項目は設けず、任意データを記録しない構成としても良い。
【００５２】
アクセス可否には、クライアント端末３０によるサーバ１０へのアクセスを最終的に許可したか否かを格納する。
アクセス日には、そのアクセスがあった年月日を格納する。
アクセス時刻には、そのアクセスがあった時刻を格納する。
【００５３】
以上の構成により、通信装置１５でインターネット３を介してクライアント端末３０からのアクセスを許容することができる。また、アクセスの際には、登録ユーザテーブル１９ａ及び登録機器テーブル１９ｂのデータからユーザとクライアント端末３０とを識別して認証することができ、アクセス履歴テーブル１９ｃにアクセス履歴を蓄積することができる。
【００５４】
次に、図７に示すブロック図と共に、クライアント端末３０の構成について説明する。

クライアント端末３０は、デスクトップＰＣで構成しており、制御装置３１に接続して、ＲＦ－ＩＤカードリーダライタ３２、記録媒体処理装置３３、入力装置３４、表示装置３５、通信装置３６、及び記憶装置３７を備えている。
【００５５】
ＲＦ－ＩＤカードリーダライタ３２は、誘導電磁界を利用してＲＦ－ＩＤカード５０（図２）と非接触で通信し、ＲＦ－ＩＤカード５０に記憶するデータの読書きを実行する。
【００５６】
記録媒体処理装置３３は、ＣＤ－ＲＯＭドライブやフレキシブルディスクドライブ等、記録媒体にデータを読書きする装置であり、読取った情報を制御装置３１に送信し、制御装置３１から受信した情報を記録媒体に書き込む。
入力装置３４は、マウスやキーボード等、座標入力やキー入力といった入力を受け付ける装置であり、入力された入力信号を制御装置３１に送信する。
【００５７】
表示装置３５は、液晶モニタ等の文字や画像を表示する装置であり、制御装置３１から受信する表示信号に従って表示を行う。
通信装置３６は、ＬＡＮボード等の通信可能な装置であり、制御装置３１に制御に従って、インターネット３を介したデータの送信や受信を実行する。
【００５８】
記憶装置３７には、ハードディスク等のデータを記憶する装置であり、各種データやプログラムを格納する。プログラムとしては、ＩＰアドレスを生成するＩＰアドレス生成プログラム３８や、サーバ１０にアクセスするサーバアクセスプログラム３９等を格納する。
【００５９】
以上の構成により、クライアント端末３０はＲＦ－ＩＤカードリーダライタ３２によりユーザが所持するＲＦ－ＩＤカード５０に記憶しているデータ、特にカードＩＤを読取る

ことができる。

【００６０】

この読み取りは、図２に示したようにＲＦ－ＩＤカードリーダライタ３２にＲＦ－ＩＤカード５０を載せた場合だけでなく、ＲＦ－ＩＤカードリーダライタ３２の上方にある通信領域内にＲＦ－ＩＤカード５０が入るようにかざした場合にも行うことができる。

【００６１】

また、クライアント端末３０はＩＰアドレスを生成し、このＩＰアドレスを利用して通信装置３６でインターネット３を介してサーバ１０に接続することができる。

【００６２】

次に図８に示す説明図と共に、クライアント端末３０で自動生成するＩＰアドレスと、ＲＦ－ＩＤカード５０のカードＩＤ及びクライアント端末３０の通信装置３６のＭＡＣアドレスの関係について説明する。

【００６３】

図８の（Ａ）の表に示すように、ＩＰアドレスは１２８ｂｉｔのデータ長を有している。このＩＰアドレスには、インターネットプロトコルとしてＩＰｖ６を使用している。

【００６４】

クライアント端末３０の固有ナンバーとなる通信装置３６のＭＡＣアドレスは、４８ｂｉｔのデータ長を有している。

またＲＦ－ＩＤカードの固有ナンバーであるカードＩＤは、６４ｂｉｔのデータ長を有している。

【００６５】

クライアント端末３０のＩＰアドレス生成プログラムは、ＭＡＣアドレスの次にカードＩＤを続け、残りに任意データを付加して（Ｂ）に示すようにＩＰアドレスを生成する。

【００６６】

ここで、前記ＭＡＣアドレスとカードＩＤを加えても１１２ｂｉｔであり、ＩＰアドレスのデータ長である１２８ｂｉｔより短くなる。このため、ＭＡＣアドレスとカードＩＤを復元可能な状態のＩＰアドレスを生成することができる。このとき、１６ｂｉｔ分の余りが生じるが、この余り部分にはパリティチェックによる誤り検出を行うために誤り検出用符号を当てはめる。

【００６７】

以上に説明するように、クライアント端末３０にてＭＡＣアドレスとカードＩＤからＩＰアドレスを生成することができる。ＭＡＣアドレスとカードＩＤはいずれもユニークなＩＤであるため、重複のないＩＰアドレスを容易に作成することができる。

【００６８】

次に、図９に示す処理フロー図と共に、ユーザ識別システム１の全体動作について説明する。

まず、ユーザがクライアント端末３０でブラウザ等のソフトウェアを立ち上げてサーバ１０にアクセスしようとすると、クライアント端末３０の制御装置３１はユーザ側データの取得を実行する（ステップｎ１）。

【００６９】

このユーザ側データはカードＩＤとＭＡＣアドレスであり、制御装置３１はＲＦ－ＩＤカードリーダライタ３２により通信可能領域内にあるＲＦ－ＩＤカード５０と通信してカードＩＤを取得する。

【００７０】

カードＩＤが取得できれば、通信装置３６からＭＡＣアドレスも取得してＩＰアドレス生成プログラムを実行し、カードＩＤとＭＡＣアドレスからＩＰアドレスを生成する（ステップｎ２）。

【００７１】

制御装置３１は、生成したＩＰアドレスを使用してサーバ１０にアクセスする（ステップｎ３）。

サーバ１０の制御装置１１は、通信装置１５から他のコンピュータ（この説明ではクライアント端末３０）からのアクセスを検知すると、アクセスのあったＩＰアドレスを取得する（ステップｎ４）。

【００７２】

制御装置１１は、このＩＰアドレスを分解して、ＭＡＣアドレスとカードＩＤを取得し（ステップｎ５）、このＭＡＣアドレスとカードＩＤによるユーザ認証を実行する（ステップｎ６）。

【００７３】

ユーザ認証では、登録機器テーブル１９ｂに取得したＭＡＣアドレスが登録されているか判定し、登録されていれば、そのＭＡＣアドレスを有する機器の使用可能ユーザに、取得したカードＩＤが登録されているか判定する。

カードＩＤも登録されていると判定できれば登録ユーザであると判定し、いずれか一方でも登録されていないと判定すれば登録ユーザでないと判定する。

【００７４】

なお、ＭＡＣアドレスは登録機器テーブル１９ｂで、カードＩＤは登録ユーザテーブル１９ａで、それぞれ個別に登録されているか判定し、両方が登録されていればアクセス許可する構成としても良い。この場合は、ユーザ毎に使用可能なクライアント端末３０を登録する手間を省くことができる。

【００７５】

前記ユーザ認証の際に、制御装置１１は任意データ（図８）部分の誤り検出用符号を用いて誤り検出も実行し、ＩＰアドレスのデータ欠損や成りすましが行われていればアクセスできないようにしている。

【００７６】

ここで、誤りが検出された場合には、クライアント端末３０に前記ＩＰアドレスを使用した再アクセスを要求し、これが規定回数繰り返された場合には、そのＩＰアドレスに含まれているカードＩＤ又は／及びＭＡＣアドレスについてはアクセス拒否する設定としている。これにより、成りすましによる不正アクセスを防止している。

【００７７】

このようにしてユーザ認証を行った後に、制御装置１１は、ユーザ側データとして前記ステップｎ５で取得したカードＩＤとＭＡＣアドレス、アクセス可否、及びアクセス日時等を管理データベース１９（図３）内のアクセス履歴テーブル１９ｃ（図６）に記録する（ステップｎ７）。

【００７８】

前記ステップｎ６でのユーザ認証で、登録ユーザでないと判定したか、誤りが検出されてアクセス拒否する対象と判定した場合は（ステップｎ８）、制御装置１１はクライアント端末３０へエラー信号を返信する（ステップｎ９）。

クライアント端末３０は、このエラー信号を受信して表示装置３５（図７）にエラー表示を行ない（ステップｎ１０）、処理を終了する。

【００７９】

前記ステップｎ８で、誤りの検出もない正規の登録ユーザのアクセスであると判定した場合には、制御装置１１は、クライアント端末３０に対して接続許可を行う（ステップｎ１１）。

クライアント端末３０は、サーバ１０との通信処理を実行し、ユーザ操作による情報処理等の要求された処理を実行し（ステップｎ１２）、処理を終了する。

【００８０】

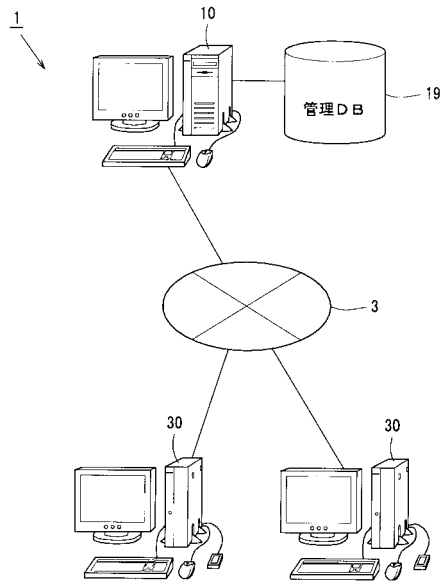
以上の動作により、クライアント端末３０はＲＦ－ＩＤカード５０のカードＩＤと通信装置３６のＭＡＣアドレスからＩＰアドレスを生成することができ、このＩＰアドレスでサーバ１０と通信することができる。

従って、クライアント端末３０はグローバルＩＰアドレスを容易に作成してネットワーク接続ができる。

【００８１】
　また、サーバ１０は、クライアント端末３０が使用するＩＰアドレスからユーザ認証やクライアント端末認証を行うことができると共に、アクセスを試みたユーザのカードＩＤとＭＡＣアドレスとをアクセス履歴として記録することができる。従って、後に不正利用が発覚したような場合に、このアクセス履歴を用いて不正利用者とそれに使用されたクライアント端末３０とを特定することも可能となる。
【００８２】
　なお、上述した実施形態ではＭＡＣアドレスを用いたが、このＭＡＣアドレスの変わりに、クライアント端末３０が記憶しているクライアント端末３０の製造ナンバー等によって構成するクライアント端末番号を使用する構成としても良い。
【００８３】
　また、誤り検出を行わない構成としても良い。この場合は、任意データ部分に他の適宜のデータを格納してデータ長を調整すると良い。
　また、インターネット3の替わりにＬＡＮを使用するローカルエリアでのシステムで構成しても良く、サーバ１０の替わりにルータを用いても良い。この場合は、グローバルＩＰアドレスではなく、ローカルＩＰアドレスを生成して使用すると良い。
【００８４】
　また、カードＩＤとＭＡＣアドレスとを２つ並べてＩＰアドレスの一部を構成したが、クライアント端末３０がカードＩＤとＭＡＣアドレスに適宜の変換処理を適用してＩＰアドレスを生成し、サーバ１０が前記変換処理を逆に適用する復元処理を行ってＩＰアドレスからカードＩＤとＭＡＣアドレスとを取得構成としても良い。
【００８５】
　変換処理の具体的としては、例えば８ｂｉｔ単位等の所定単位ずつにカードＩＤとＭＡＣアドレスをそれぞれ分割し、その分割単位で交互に並べてカードＩＤとＭＡＣアドレスが混ざり合ったコードを作成し、これをＩＰアドレスの一部を構成するといった変換が利用できる。
　これにより、カードＩＤ及びＭＡＣアドレスが通信経路を平文では流れないこととなり、通信系路上の盗聴でカードＩＤ及びＭＡＣアドレスが他人に漏洩することを防止することができる。
【００８６】
　また、ステップｎ４～ｎ１１（図９）で説明したサーバの処理は、そのＩＰアドレスを用いた最後の接続から所定時間（例えば6時間など）が経過していなければ、そのＩＰアドレスについては実行しない構成としても良い。これにより、認証回数と履歴データのデータ数を削減し、システム負荷の軽減を図ることができる。
【００８７】
　また、インターネットプロトコルにＩＰｖ６を使用したが、ＩＰｖ４を使用する構成としても良い。この場合は、ＩＰアドレスのデータ長が３２ｂｉｔとなるため、カードＩＤとＭＡＣアドレスを並べたデータ長１１２ｂｉｔより短くなる。
【００８８】
　従って、ハッシュ関数を用いて圧縮するなど、適宜の方式によってカードＩＤとＭＡＣアドレスとのそれぞれのデータを圧縮し、３２ｂｉｔに収まるように変換すると良い。
【００８９】
　この場合、データ量が減少しているため復元することはできないが、サーバ１０でも同一のデータ圧縮をする、あるいはデータ圧縮後の縮小カードＩＤと縮小ＭＡＣアドレスを格納しておく等の方法により、ユーザとクライアント端末３０とを認証することができる。
【００９０】
　なお、カードＩＤとＭＡＣアドレスを圧縮する際には、メーカーや商品の型番を指定する部分より、個別に割り与えられる識別番号部分を多く使用して圧縮することが望ましい。このように多数の物品で同一ナンバーとなるメーカー指定部分や型番部分を避けること

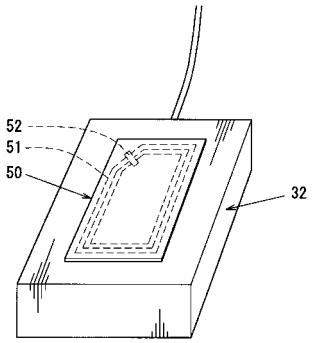
で、圧縮後のデータが同一となるケースを少なくすることができる。
【００９１】
この発明の構成と、上述の実施形態との対応において、
この発明の電気通信回線は、実施形態のインターネット３に対応し、
以下同様に、
管理装置は、サーバ１０に対応し、
クライアント装置は、クライアント端末３０に対応し、
媒体及び非接触ＩＣ媒体は、ＲＦ－ＩＤカード５０に対応し、
アンテナは、アンテナコイル５１に対応し、
ＩＣは、ＩＣチップ５２に対応し、
ＩＰアドレス生成処理は、ステップｎ２に対応し、
アクセス処理は、ステップｎ３に対応し、
ユーザ識別処理は、ステップｎ５～ｎ６に対応し、
媒体情報は、カードＩＤに対応し、
クライアント情報は、ＭＡＣアドレスに対応するも、
この発明は、上述の実施形態の構成のみに限定されるものではなく、多くの実施の形態を得ることができる。
【図面の簡単な説明】
【００９２】
【図１】ユーザ識別システムのシステム構成図。
【図２】ＲＦ－ＩＤカードリーダライタ部分の拡大斜視図。
【図３】サーバの構成を示すブロック図。
【図４】登録ユーザテーブルのデータ説明図。
【図５】登録機器テーブルのデータ説明図。
【図６】アクセス履歴テーブルのデータ説明図。
【図７】クライアント端末の構成を示すブロック図。
【図８】ＩＰアドレスとカードＩＤとＭＡＣアドレスの関係の説明図。
【図９】ユーザ識別システムの全体動作を示す処理フロー図。
【符号の説明】
【００９３】
１…ユーザ識別システム
３…インターネット
１０…サーバ
３０…クライアント端末
５０…ＲＦ－ＩＤカード
５１…アンテナコイル
５２…ＩＣチップ

【図１】



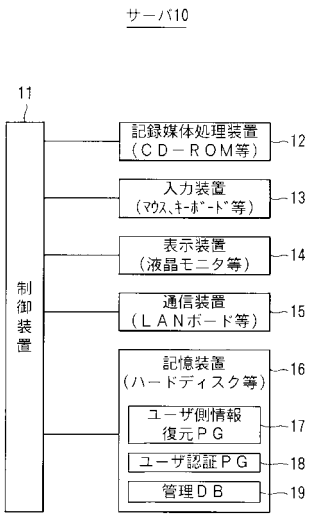
1…ユーザ識別システム　10…サーバ
3…インターネット　30…クライアント端末

【図２】



32…ＲＦ－ＩＤカードリーダライタ
50…ＲＦ－ＩＤカード
51…アンテナコイル
52…ＩＣチップ

【図３】



【図４】

登録ユーザテーブル19a

タグID	ユーザ名	更新日	有効期限	…
--**-**-**-**-**-06	○○ 太郎	2004.8.2	2005.2.2	
--**-**-**-**-**-92	△△ 花子	2004.8.9	2005.8.9	
--**-**-**-**-**-42	×× 次郎	2004.8.10	2005.8.10	
	⋮			

【図５】

登録機器テーブル19b

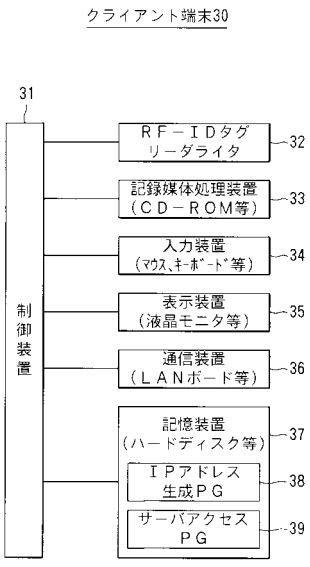
MACアドレス	機器名称	更新日	有効期限	使用可能ユーザ（タグID）	…
--**-63	○○㈱102	2004.8.4	2005.8.4	**-**-**-**-**-**-**-**-06	
--**-08	○○㈱005	2004.8.11	2006.8.11	**-**-**-**-**-**-**-**-06, **-**-**-**-**-**-**-**-92	
--**-86	大阪個人000036	2004.8.13	2005.8.13	**-**-**-**-**-**-**-**-42	
		⋮			

【図６】

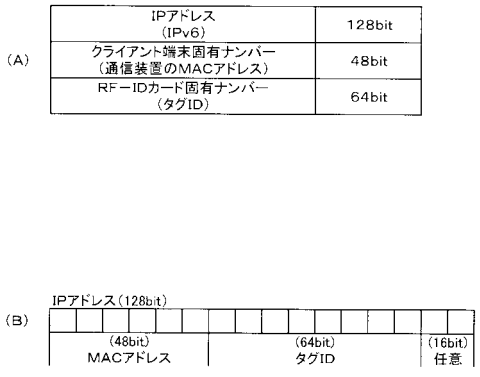
アクセス履歴テーブル19c

履歴No.	MACアドレス	タグID	任意データ	アクセス可否	アクセス日	アクセス時刻
1	**-**-**-63	**-**-**-**-**-**-**-**-06	**	○	2004.9.1	10:15:23
2	**-**-**-08	**-**-**-**-**-**-**-**-92	**	○	2004.9.1	11:52:01
3	**-**-**-27	**-**-**-**-**-**-**-**-35	**	×	2004.9.1	12:44:30
		⋮				

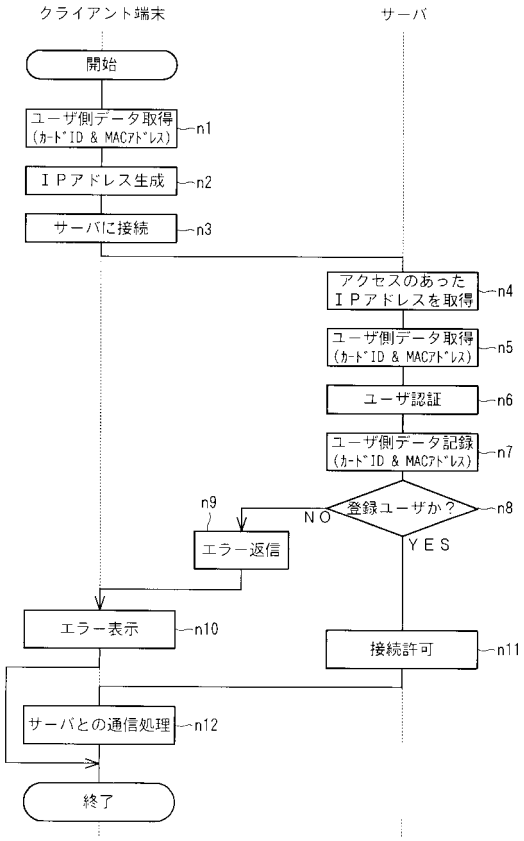
【図７】



【図８】



【図９】


クライアント端末
サーバ
開始
ユーザ側データ取得
(ｶｰﾄﾞID & MACｱﾄﾞﾚｽ)
n1
ＩＰアドレス生成
n2
サーバに接続
n3
アクセスのあった
ＩＰアドレスを取得
n4
ユーザ側データ取得
(ｶｰﾄﾞID & MACｱﾄﾞﾚｽ)
n5
ユーザ認証
n6
ユーザ側データ記録
(ｶｰﾄﾞID & MACｱﾄﾞﾚｽ)
n7
登録ユーザか？
n8
ＮＯ
ＹＥＳ
n9
エラー返信
エラー表示
n10
接続許可
n11
サーバとの通信処理
n12
終了