

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3648159号
(P3648159)

(45) 発行日 平成17年5月18日(2005.5.18)

(24) 登録日 平成17年2月18日(2005.2.18)

(51) Int. Cl.⁷

F I

G06F 17/60
G06F 15/00

G06F 17/60 140
G06F 17/60 414
G06F 17/60 504
G06F 17/60 512
G06F 15/00 330A

請求項の数 2 (全 11 頁)

(21) 出願番号 特願2000-404978 (P2000-404978)
(22) 出願日 平成12年12月29日(2000.12.29)
(65) 公開番号 特開2002-207946 (P2002-207946A)
(43) 公開日 平成14年7月26日(2002.7.26)
審査請求日 平成14年5月10日(2002.5.10)

(73) 特許権者 592018320
あいおい損害保険株式会社
東京都渋谷区恵比寿一丁目28番1号
(74) 代理人 100081271
弁理士 吉田 芳春
(72) 発明者 西辻 徹
東京都渋谷区代々木3丁目25番3号 大
東京火災海上保険株式会社内

審査官 関 博文

最終頁に続く

(54) 【発明の名称】 認証システム

(57) 【特許請求の範囲】

【請求項1】

サービス提供者のサービス提供者サーバと認証者の認証者サーバとクライアントのクライアント端末とがネットワークを介して接続され、前記クライアント端末は、前記サービス提供者サーバの提供するサービスに関する取扱情報を画面に表示する取扱情報表示手段と、前記サービス提供者サーバが前記認証者サーバに認証されたことを示す認証情報を、前記取扱情報と同一の表示画面内の別々の表示領域で表示する認証情報表示手段とを備え、

前記サービス提供者サーバは、前記取扱情報を記憶する記憶手段と、前記クライアント端末へ前記取扱情報を送信する取扱情報送信手段と、前記取扱情報を更新した日付時刻である更新日時と認証を受けたサービス提供者を特定する認証番号とを前記認証者サーバに送信して認証情報を要求する認証情報要求手段と、前記認証者サーバから受信した認証情報を前記クライアント端末の表示画面内で前記取扱情報と別々の表示領域で表示させるよう送信する認証情報送信手段とを備え、

前記認証者サーバは、前記サービス提供者サーバが前記認証者サーバに認証された日付時刻を示す認証日時、及び前記認証番号を含み前記サービス提供者サーバの認証状態を記録した認証登録情報を格納する認証登録情報データベースと、前記サービス提供者サーバから送信された前記認証番号と前記更新日時を受信するとともに、受信した前記認証番号を基に前記認証登録情報データベースに格納されている認証登録情報を検索し、該当する認証登録情報に含まれる認証日時と前記更新日時との日付日時を比較する認証登録情報手

10

20

エック手段と、前記認証日時が前記更新日時よりも後の日付時刻であった場合に前記サービス提供者に対応する前記認証情報を前記サービス提供者サーバに送信する送信手段とを備える認証システム。

【請求項2】

サービス提供者のサービス提供者サーバと認証者の認証者サーバとクライアントのクライアント端末とがネットワークを介して接続され、前記クライアント端末は、前記サービス提供者サーバの提供するサービスに関する取扱情報を画面に表示する取扱情報表示手段と、前記サービス提供者サーバが前記認証者サーバに認証されたことを示す認証情報を、前記取扱情報と同一の表示画面内の別々の表示領域で表示する認証情報表示手段とを備え、

10

前記サービス提供者サーバは、前記取扱情報を記憶する記憶手段と、前記クライアント端末の要求に応じて前記クライアント端末へ前記取扱情報を送信する取扱情報送信手段と、前記取扱情報を更新した日付時刻である更新日時と認証を受けたサービス提供者を特定する認証番号とを前記認証者サーバに送信して認証情報を要求する認証情報要求手段と、前記認証者サーバから受信した認証情報を前記クライアント端末の表示画面内で前記取扱情報と別々の表示領域で表示させるよう送信する認証情報送信手段とを備え、

前記認証者サーバは、前記サービス提供者サーバが前記認証者サーバに認証された日付時刻を示す認証日時、及び前記認証番号を含み前記サービス提供者サーバの認証状態を記録した認証登録情報を格納する認証登録情報データベースと、前記サービス提供者サーバから送信された前記認証番号と前記更新日時を受信するとともに、受信した前記認証番号を基に前記認証登録情報データベースに格納されている認証登録情報を検索し、該当する認証登録情報に含まれる認証日時と前記更新日時との日付日時を比較する認証登録情報チェック手段と、前記認証日時が前記更新日時よりも後の日付時刻であった場合に前記サービス提供者に対応する前記認証情報を前記サービス提供者サーバに送信する送信手段とを備え、

20

前記サービス提供者サーバは、前記認証情報を前記クライアント端末の要求に関係なく、自動的に前記クライアント端末へ送信する認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークを利用した認証システムに関する。

30

【0002】

【従来の技術】

近年、インターネット等に代表される情報通信関連の技術は高度化の一途を辿っている。それに伴いインターネットを利用したビジネスも様々なものが考え出されている。インターネットを利用した取引である電子取引もその一つであり、多くの企業、団体によって活用されている。インターネットを利用した電子取引は当事者の地理的制約や時間的制約を受けることが少なく、その取引形態も個人と個人、個人と企業、企業と企業等の取引者に応じた様々な形態が生み出され、尚も増加中である。しかし、インターネットを利用した電子取引は匿名性が強く、取引先の信用が得られないことが多かった。

40

【0003】

【発明が解決しようとする課題】

そのため利用者の側から見ると、現実知っている相手との取引や著名な相手との取引であれば安心して行えたものの、直接の面識のない相手との取引は相手の信用度がわからないために、安心して行うことができなかった。

【0004】

また、取引を行う相手に信用してもらうために、信用のおける第三者からの認証を得ることで、信用を高める方法がある。しかし、第三者からの認証を証明する文章や記号を自己のホームページに記載しておいても、相手が気付かず、結局信用が得られないことが多かった。

50

【0005】

また、第三者が認証を行う際には、認証する対象が膨大な数になることが多く、認証自体にも時間がかかり、一旦認証を行った相手がある後も認証条件を満たしているかのチェックを行えなかった。

【0006】

このような従来の課題を考慮して、本発明は、ネットワークに於いてサービスや情報を提供する者の認証情報を迅速かつ確実に利用者に公開するシステムを提供することを課題とするものである。

【0007】

【課題を解決するための手段】

上記課題を解決するため、本発明に係る認証システムは以下のような手段を採用する。

【0008】

即ち、請求項1では、サービス提供者のサービス提供者サーバと認証者の認証者サーバとクライアントのクライアント端末とがネットワークを介して接続され、前記クライアント端末は、前記サービス提供者サーバの提供するサービスに関する取扱情報を画面に表示する取扱情報表示手段と、前記サービス提供者サーバが前記認証者サーバに認証されたことを示す認証情報を、前記取扱情報と同一の表示画面内の別々の表示領域で表示する認証情報表示手段とを備え、前記サービス提供者サーバは、前記取扱情報を記憶する記憶手段と、前記クライアント端末へ前記取扱情報を送信する取扱情報送信手段と、前記取扱情報を更新した日付時刻である更新日時と認証を受けたサービス提供者を特定する認証番号とを前記認証者サーバに送信して認証情報を要求する認証情報要求手段と、前記認証者サーバから受信した認証情報を前記クライアント端末の表示画面内で前記取扱情報と別々の表示領域で表示させるよう送信する認証情報送信手段とを備え、前記認証者サーバは、前記サービス提供者サーバが前記認証者サーバに認証された日付時刻を示す認証日時、及び前記認証番号を含み前記サービス提供者サーバの認証状態を記録した認証登録情報を格納する認証登録情報データベースと、前記サービス提供者サーバから送信された前記認証番号と前記更新日時を受信するとともに、受信した前記認証番号を基に前記認証登録情報データベースに格納されている認証登録情報を検索し、該当する認証登録情報に含まれる認証日時と前記更新日時との日付日時を比較する認証登録情報チェック手段と、前記認証日時が前記更新日時よりも後の日付時刻であった場合に前記サービス提供者に対応する前記認証情報を前記サービス提供者サーバに送信する送信手段とを備える。

【0009】

上記手段では、利用者であるクライアント端末がサービス提供者であるサービス提供者サーバに接続すると、前記サービス提供者サーバは認証番号と更新日時を含む取扱情報を前記クライアント端末に送信して認証情報を要求し、前記認証者サーバは、サービス提供者に該当する認証日時と認証番号を含む認証登録情報を認証登録情報データベースから検索し、該当する認証登録情報に含まれる認証日時と前記更新日時との日付日時を比較して、サービス提供者サーバを認証した日付時刻から後にサービス提供者サーバが取扱情報を更新していないかをチェックしてから、認証情報を前記サービス提供者サーバに送信し、サービス提供者サーバは受信した認証情報を前記クライアント端末に送信する。クライアント端末は受信した取扱情報と認証情報を同一画面上の別々の表示領域に表示する。

【0010】

また、請求項2では、サービス提供者のサービス提供者サーバと認証者の認証者サーバとクライアントのクライアント端末とがネットワークを介して接続され、前記クライアント端末は、前記サービス提供者サーバの提供するサービスに関する取扱情報を画面に表示する取扱情報表示手段と、前記サービス提供者サーバが前記認証者サーバに認証されたことを示す認証情報を、前記取扱情報と同一の表示画面内の別々の表示領域で表示する認証情報表示手段とを備え、前記サービス提供者サーバは、前記取扱情報を記憶する記憶手段と、前記クライアント端末の要求に応じて前記クライアント端末へ前記取扱情報を送信する取扱情報送信手段と、前記取扱情報を更新した日付時刻である更新日時と認証を受けた

10

20

30

40

50

サービス提供者を特定する認証番号とを前記認証者サーバに送信して認証情報を要求する認証情報要求手段と、前記認証者サーバから受信した認証情報を前記クライアント端末の表示画面内で前記取扱情報と別々の表示領域で表示させるよう送信する認証情報送信手段とを備え、前記認証者サーバは、前記サービス提供者サーバが前記認証者サーバに認証された日付時刻を示す認証日時、及び前記認証番号を含み前記サービス提供者サーバの認証状態を記録した認証登録情報を格納する認証登録情報データベースと、前記サービス提供者サーバから送信された前記認証番号と前記更新日時を受信するとともに、受信した前記認証番号を基に前記認証登録情報データベースに格納されている認証登録情報を検索し、該当する認証登録情報に含まれる認証日時と前記更新日時との日付時刻を比較する認証登録情報チェック手段と、前記認証日時が前記更新日時よりも後の日付時刻であった場合に前記サービス提供者に対応する前記認証情報を前記サービス提供者サーバに送信する送信手段とを備え、前記サービス提供者サーバは、前記認証情報を前記クライアント端末の要求に関係なく、自動的に前記クライアント端末へ送信する。

10

【0011】

上記手段では、前記サービス提供者サーバは、取扱情報を前記クライアント端末の要求に応じて前記クライアント端末に送信し、前記クライアント端末の要求に関係なく認証情報を認証者サーバに要求する。サービス提供者サーバは認証者サーバから認証情報を受信し、クライアント端末に送信する。

【0012】**【発明の実施の形態】**

以下、本発明にかかる認証システムの実施の形態(1)を図1~図7により説明する。図1は本発明に係る認証システムの全体構成を示す図である。図2は認証確認手順を示すブロック部である。図3は取扱情報、認証情報の表示形態を示す図である。図4は認証確認手順を示すフローチャート図である。図5は本発明の認証登録手順を示すブロック図である。図6は認証依頼情報、認証登録情報を示す図である。図7は認証登録手順を示すフローチャート図である。

20

【0013】

図1に示すように本発明の認証システム1は少なくとも1つのサービス提供者サーバ2、認証者サーバ3、少なくとも1つのクライアント端末4がネットワーク5を介して接続されて構成されている。

30

【0014】

サービス提供者サーバ2及び認証者サーバ3は入出力部、記録部、通信部、演算部を備え、他のコンピュータからの依頼に応える機能を持つメインフレームやワークステーション、パーソナルコンピュータ等である。クライアント端末4は表示ディスプレイ等の入出力部や記録機能、通信機能、演算機能を備えるワークステーションやパーソナルコンピュータ、携帯端末等であり、ネットワーク接続してWebブラウザ等により情報を得ることができる。ネットワーク5はインターネットやLAN等から成る既存のネットワークである。

【0015】

なお、本発明でサービス提供者とは認証者の認証する事柄についてサービスを提供する者又は団体であり、認証者とはサービス提供者の扱う情報やサービスについて認証を与える者又は団体である。認証者とサービス提供者の関係には、例えば自動車メーカーと自動車ディーラー、保険会社と保険代理店、英語能力資格認定者と被認定者等がある。

40

【0016】

以下、本発明を実施例の一つである認証者としての自動車メーカーとサービス提供者としての自動車ディーラーを例に説明する。なお、これにより本発明が限定されるものではない。

【0017】

以下、図2、図3、図4を用いて、本発明の認証確認手順を説明する。図2に示すように、自動車ディーラーであるディーラーサーバ20は取扱情報を利用者端末40に送信す

50

る取扱情報送信手段 2 1 と、認証情報をメーカーサーバ 3 0 に要求する認証情報要求手段 2 2 と、メーカーサーバ 3 0 から認証情報又は認証不可情報を受信する認証情報受信手段 2 3 と、利用者端末 4 0 に認証情報又は認証不可情報を送信する認証情報送信手段 2 4 を備える。

【 0 0 1 8 】

取扱情報、認証情報及び認証不可情報は、利用者端末 4 0 が Web ブラウザを介して画面上で Web ページとして表示できるように、サービス提供者サーバから送信される。

【 0 0 1 9 】

自動車メーカーであるメーカーサーバ 3 0 は認証登録情報データベース 3 2 と、認証情報要求受付手段 3 1、認証登録情報をチェックする認証チェック手段 3 3、ディーラーサーバ 2 0 に認証情報又は認証不可情報を送信する送信手段 3 4 を備える。

10

【 0 0 2 0 】

利用者である利用者端末 4 0 は表示画面 4 6 と、ディーラーサーバ 3 0 へ取扱情報を要求する取扱情報要求手段 4 1 とディーラーサーバ 3 0 から取扱情報を受信する取扱情報受信手段 4 2 と、表示画面 4 6 に取扱情報を表示する取扱情報表示手段 4 3 と、ディーラーサーバ 3 0 から認証情報又は認証不可情報を受信する認証情報受信手段 4 4 と、表示画面 4 6 に認証情報又は認証不可情報を表示する認証情報表示手段 4 5 とを備える。

【 0 0 2 1 】

取扱情報表示手段 4 3 及び認証情報表示手段 4 5 はそれぞれ受信した取扱情報、認証情報又は認証不可情報を Web ブラウザを介して表示画面 4 6 に Web ページとして表示する。

20

【 0 0 2 2 】

図 3 は取扱情報を示す Web ページ 4 3 1、認証情報を示す Web ページ 4 5 1、認証不可情報を示す Web ページ 4 5 2 である。図に示すように、自動車販売情報表示ウィンドウ 4 3 1 には自動車ディーラーの取扱情報である自動車販売に関する情報が記載される。認証情報 Web ページ 4 5 1 には該当の自動車ディーラーが自動車メーカーにより認証されている旨を示す情報が表示される。認証不可情報 Web ページ 4 5 2 には該当の自動車ディーラーが自動車メーカーに認証されていない旨を示す情報が表示される。

【 0 0 2 3 】

次に図 4 のフローチャート図を用いて、認証確認方法を説明する。利用者端末 4 0 はディーラーサーバ 2 0 へ接続し、取扱情報を要求する (S 1 0 0 1)。ディーラーサーバ 2 0 は利用者端末 4 0 の要求に応じて取扱情報を利用者端末 4 0 へ取扱情報送信手段 4 1 により送信する (S 1 0 0 2) 一方で、メーカーサーバ 3 0 に認証情報を要求する (S 1 0 0 3)。ディーラーサーバ 2 0 が認証情報を要求する際には認証情報要求手段 2 2 により、取扱情報である Web ページを更新した日付時刻を示す更新日時と、予めメーカーサーバ 3 0 に認証された際に記憶していた認証番号をメーカーサーバ 3 0 に送信する。

30

【 0 0 2 4 】

一方、利用者端末 4 0 は取扱情報受信手段 4 2 により取扱情報を受信し (S 1 0 0 4)、取扱情報表示手段 4 3 により Web ブラウザを介して受信した取扱情報を取扱情報 Web ページ 4 3 1 として表示画面 4 6 に表示する (S 1 0 0 5)。

40

【 0 0 2 5 】

また、メーカーサーバ 3 0 はディーラーサーバ 2 0 の要求に応じて、認証情報要求受付手段 3 1 によりディーラーサーバ 2 0 の要求を受け、認証登録情報を認証登録情報データベース 3 2 から検索する (S 1 0 0 6)。検索はディーラーサーバ 2 0 から認証チェック要求の際に送信された認証番号を用いて、認証登録情報データベース 3 2 に格納している認証登録情報から該当する認証番号をもつものを検索する方法で行う。検索の結果、該当する認証登録情報が見つかり、認証登録情報に含まれる認証日時と更新日時を比較する。認証日時が更新日時よりも後の日付時刻であった場合 (S 1 0 0 7 - Y E S)、メーカーサーバ 3 0 は認証したことを示す認証情報を、送信手段 3 4 により、ディーラーサーバ 2 0 へ送信する (S 1 0 0 8)。また認証日時が更新日時よりも前の日付時刻であった

50

場合 (S 1 0 0 7 - N O)、メーカーサーバ 3 0 は認証不可を示す認証不可情報を、送信手段 3 4 によりディーラーサーバ 2 0 へ送信する (S 1 0 0 9)。

【 0 0 2 6 】

ディーラーサーバ 2 0 は認証情報受信手段 2 3 により認証情報、又は認証不可情報を受信し (S 1 0 1 0)、認証情報又は認証不可情報を予め定めた形式で利用者端末 4 0 へ認証情報送信手段 2 4 により送信する (S 1 0 1 1)。

【 0 0 2 7 】

利用者端末 4 0 は認証情報受信手段 4 4 により認証情報、又は認証不可情報を受信し (S 1 0 1 2)、認証結果表示手段 4 5 により取扱情報 Web ページ 4 3 1 とは別の Web ページとして、認証情報 Web ページ 4 5 1、又は認証不可情報 Web ページとして Web ブラウザを介して表示画面 4 6 に表示する (S 1 0 1 3)。図 3 に於いては認証情報 Web ページ 4 5 1 が示されているが、認証不可情報 4 5 2 も同様の手順で表示される。

10

【 0 0 2 8 】

次に図 5、図 6、図 7 を用いて認証登録手順を説明する。図 5 に示すように、ディーラーサーバ 2 0 は認証情報を送信する依頼情報送信手段 2 5、審査結果を受信する審査結果受信手段 2 6、審査結果に含まれる認証番号を記憶する記憶手段 2 7 を備える。メーカーサーバ 3 0 は依頼情報を受信する依頼受信手段 3 5、認証依頼情報を審査する審査手段 3 6、認証情報を格納する認証登録情報データベース 3 2、審査結果を送信する審査結果送信手段 3 7 を備える。

【 0 0 2 9 】

20

図 6 は認証依頼情報 2 5 0、認証登録情報 3 2 0 を示す図である。認証依頼情報 2 5 0 は自動車メーカーが定めた形式に則り、例えばサービス提供者名 2 5 1、所在地 2 5 2、電話番号 2 5 3、Web ページファイル 2 5 4、更新日時 2 5 5 等から成る。Web ページファイル 2 5 4 はディーラーサーバ 3 0 の取扱情報である Web ページのソースをファイルにしたものである。更新日時 2 5 5 は、Web ページを作成又は更新した日時が記録され、図では 2 0 0 0 年 1 2 月 5 日 1 1 時 9 分を示す「 2 0 0 0 1 2 0 5 1 1 0 9 」という値が記録されている。

【 0 0 3 0 】

認証登録情報 3 2 0 は自動車メーカーが定めた形式に則り、メーカーサーバ 3 0 により作成され、認証登録情報データベース 3 2 に格納される。認証登録情報は認証依頼情報に、認証者名と認証日時と認証番号を加えた形式で作成される。認証登録情報には例えば認証対象であるディーラーのサービス提供者名 3 2 1、所在地 3 2 2、電話番号 3 2 3、Web ページファイル 3 2 4、また認証者である認証者名 3 2 5、認証を行った日時である認証日時 3 2 6、認証番号 3 2 7 等から成る。認証日時 3 2 6 は、審査に合格し認証された日時が記録され、図では 2 0 0 0 年 1 2 月 1 0 日 9 時 5 0 分を示す「 2 0 0 0 1 2 1 0 0 9 5 0 」という値が記録されている。

30

【 0 0 3 1 】

次に図 7 のフローチャート図を用いて、認証登録手順について説明を行う。サービス提供者である自動車ディーラーが認証者である自動車メーカーからの認証を希望する場合、自動車ディーラーであるディーラーサーバ 2 0 は認証依頼情報 2 5 0 を依頼送信手段 2 5 により自動車メーカーであるメーカーサーバ 3 0 へ送信する (S 2 0 0 1)。メーカーサーバ 3 0 は依頼受信手段 3 5 により認証依頼情報 2 5 0 を受信し (S 2 0 0 2)、審査手段 3 6 により審査する (S 2 0 0 3)。

40

【 0 0 3 2 】

審査の結果、認証可の場合 (S 2 0 0 4 - Y E S)、認証依頼情報 2 5 0 に認証者名 3 2 5、認証日時 3 2 6、認証番号 3 2 7 を加え、認証登録情報 3 2 0 として認証登録情報データベース 3 2 へ格納し (S 2 0 0 5)、認証番号 3 2 1 を含む審査合格通知をディーラーサーバ 2 0 へ送信する (S 2 0 0 6)。一方、審査して不合格の場合 (S 2 0 0 4 - N O)、審査不合格通知をディーラーサーバ 2 0 へ送信する (S 2 0 0 7)。

【 0 0 3 3 】

50

ディーラーサーバ20は審査合格通知又は、審査不合格通知を審査結果受信手段26により受信し(S2008)、審査結果が認証可の場合(S2009 - YES)、審査合格通知の中に含まれる認証番号327を記憶手段27により記憶する(S2010)。

【0034】

【発明の効果】

本発明によれば、クライアント端末がサービス提供者サーバへアクセスしたと同時にサービス提供者サーバが自動的に認証者サーバへ認証チェックの要求を行う。この認証チェックはサービス提供者がWebページを更新した日付時刻と最後にサービス提供者が認証された日付時刻を比較する処理だけであるので、迅速に行われる。

【0035】

また、クライアント端末がサービス提供者サーバへアクセスするたびに自動的にサービス提供者サーバの認証チェックが行われるので、最新の認証状態を確認することができ、安全かつ信頼性の高いサービスを提供することができる。

【0036】

また、サービス提供者が提供する取扱情報を表示するWebページとは別にサービス提供者の認証状態をWebページとして表示するので、利用者は画面上で認証情報を見逃すことがなくなり、サービス提供者の信頼度を高めることができる。

【図面の簡単な説明】

【図1】本発明の認証システムの全体構成を示す図である。

【図2】認証状態確認手順を示すブロック図である。

【図3】取扱情報Webページ、認証合格情報Webページ、認証不合格情報Webページを示す図である。

【図4】認証状態確認手順を示すフローチャート図である。

【図5】自動車メーカーと自動車ディーラーによる認証登録手順を示すブロック図である。

【図6】登録依頼情報及び認証情報を示す図である。

【図7】認証登録手順を示すフローチャート図である。

【符号の説明】

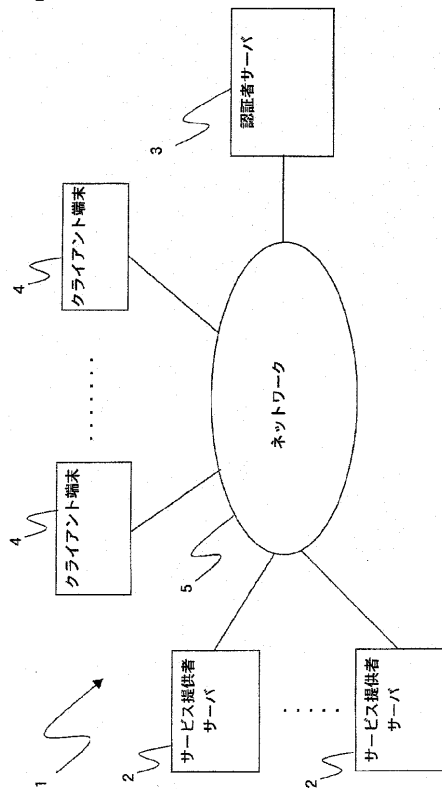
- 1 認証システム
- 2 サービス提供者サーバ
- 3 認証者サーバ
- 4 クライアント端末
- 5 ネットワーク
- 20 ディーラーサーバ
- 30 メーカーサーバ
- 40 利用者端末
- 21 取扱情報送信手段
- 22 認証情報要求手段
- 23 認証情報受信手段
- 24 認証情報送信手段
- 25 依頼送信手段
- 26 審査結果受信手段
- 27 記憶手段
- 31 認証情報要求受付手段
- 32 認証登録情報データベース
- 33 認証チェック手段
- 34 送信手段
- 35 依頼受信手段
- 36 審査手段
- 37 審査結果送信手段

- 4 1 取扱情報要求手段
- 4 2 取扱情報受信手段
- 4 3 取扱情報表示手段
- 4 4 認証情報受信手段
- 4 5 認証情報表示手段
- 2 5 0 認証依頼情報
- 2 5 1 ディーラー名
- 2 5 2 ディーラー所在地
- 2 5 3 ディーラー電話番号
- 2 5 4 取扱情報Webページファイル
- 2 5 5 更新日時
- 3 2 0 認証登録情報
- 3 2 1 ディーラー名
- 3 2 2 ディーラー所在地
- 3 2 3 ディーラー電話番号
- 3 2 4 取扱情報Webページファイル
- 3 2 5 自動車メーカー名
- 3 2 6 認証日時
- 3 2 7 認証番号
- 4 3 1 取扱情報Webページ
- 4 5 1 認証情報Webページ
- 4 5 2 認証不可情報Webページ

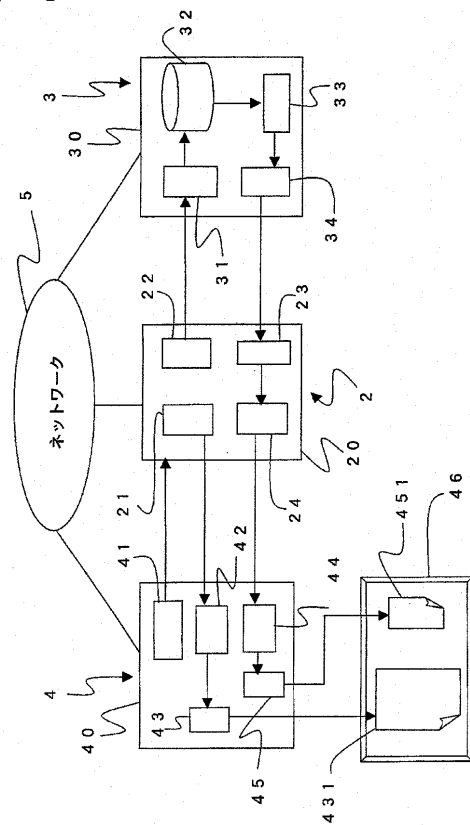
10

20

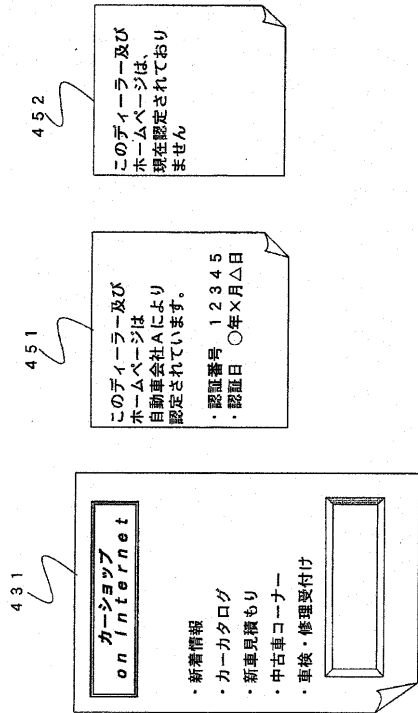
【 図 1 】



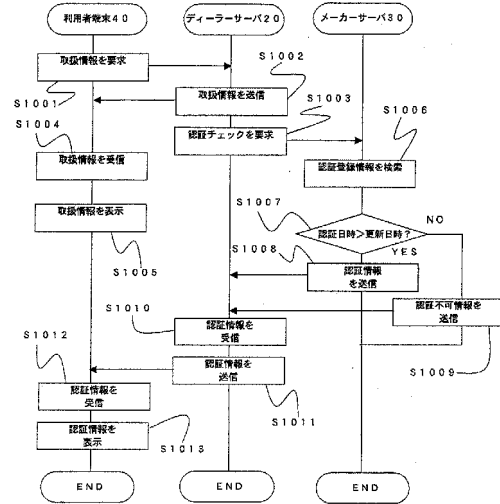
【 図 2 】



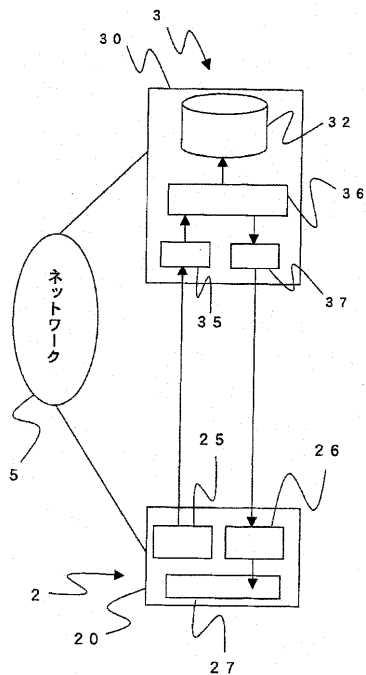
【 図 3 】



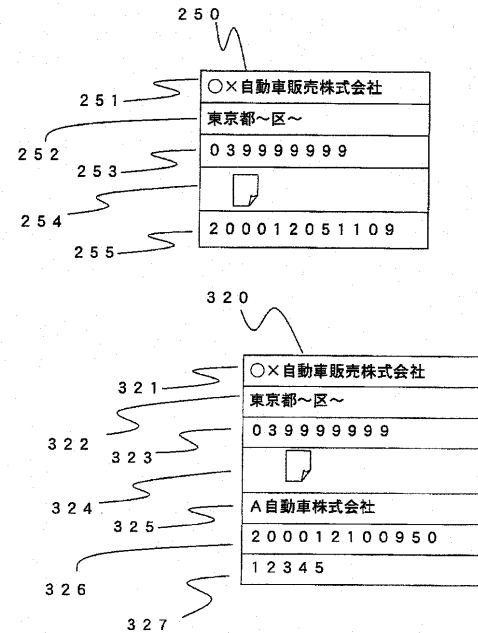
【 図 4 】



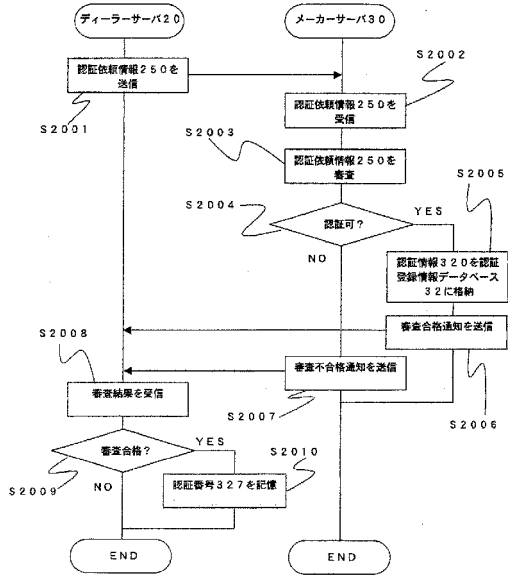
【 図 5 】



【 図 6 】



【 図 7 】



フロントページの続き

- (56)参考文献 特開2000-331088(JP,A)
特開平10-313308(JP,A)
特開2000-353194(JP,A)
特開2001-306514(JP,A)
特開平11-154139(JP,A)
ネットビジネスの本格始動の必須条件 「セキュリティ事情」を探る ネットビジネス成功のための最新セキュ, 日経ネットビジネス, 日本, 日経BP社, 1999年11月15日, 第53号, 第109-130頁
ネットビジネスに、新しい価値を - 日立のネットビジネスブランド Cubium インターネット・マーク, はいたっく, 日本, 株式会社日立製作所, 2000年11月 1日, 第24頁
森側真一他, 発展編 利用拡大に伴う4つの関門を, ツールやサービスの利用で乗り越える, 日経オープンシステム, 日本, 日経BP社, 1999年10月15日, 第79号, 第124-133頁
可部孝二他, ホームページ改竄パトロール方式, 情報処理学会研究会報告, 日本, 社団法人情報処理学会, 2000年 3月22日, 第2000巻, 第30号, 第173-178頁

(58)調査した分野(Int.Cl.⁷, DB名)

G06F 17/60

G06F 15/00

JICSTファイル(JOIS)