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

特許第4777512号
(P4777512)

(45)発行日　平成23年9月21日(2011.9.21)　(24)登録日　平成23年7月8日(2011.7.8)

(51)Int.Cl.		F I		
G06Q 30/00	(2006.01)	G06F	17/60	310E
G06Q 50/00	(2006.01)	G06F	17/60	ZEC
G06Q 40/00	(2006.01)	G06F	17/60	330
G06Q 20/00	(2006.01)	G06F	17/60	240
G06Q 10/00	(2006.01)	G06F	17/60	400

請求項の数 6　(全 14 頁)　最終頁に続く

(21)出願番号　特願2000-404056 (P2000-404056)
(22)出願日　平成12年12月12日 (2000.12.12)
(65)公開番号　特開2002-183596 (P2002-183596A)
(43)公開日　平成14年6月28日 (2002.6.28)
審査請求日　平成19年11月26日 (2007.11.26)

(73)特許権者　591071230
株式会社ソリトンシステムズ
東京都新宿区新宿２丁目４番３号
(74)代理人　100121083
弁理士　青木　宏義
(74)代理人　100138391
弁理士　天田　昌行
(74)代理人　100132067
弁理士　岡田　喜雅
(72)発明者　鎌田　信夫
東京都新宿区新宿２丁目４番３号　株式会社ソリトンシステムズ

審査官　岩間　直純

最終頁に続く

(54)【発明の名称】電子商取引のサーバシステム

(57)【特許請求の範囲】
【請求項１】
クライアントと接続し、公開サーバ、前記公開サーバと接続された認証エージェントサーバおよび決済サーバを含むＥＣサイトと、認証サーバを含む認証サイトと、を有する電子商取引のサーバシステムであって、
前記認証エージェントサーバは、
前記クライアントのＩＤおよびメールアドレスと、データベースに登録されたクライアント情報とから、前記クライアントが本人であるか否かを判断する手段と、
前記クライアントが本人であることが確認された場合に、前記認証サーバに対して、ＥＣサイトのＩＤ、仮想ＵＲＬ発行先メールアドレス、アクセス制限時間、および実際にアクセスさせるサーバのＩＰアドレスを送信する手段と、を有し、
前記認証サーバは、
前記認証エージェントサーバから、前記ＥＣサイトのＩＤ、前記仮想ＵＲＬ発行先メールアドレス、前記アクセス制限時間、および前記実際にアクセスさせるサーバのＩＰアドレスが送信された場合に、前記クライアントに対して仮想ＵＲＬを発行する手段と、
前記アクセス制限時間内に前記クライアントが仮想ＵＲＬをクリックした場合に、前記ＥＣサイトにメールを送信する手段と、を有し、
前記決済サーバは、
前記認証サーバから前記ＥＣサイトにメールが送信された場合に決済を行う手段を有する、

ことを特徴とする電子商取引のサーバシステム。
【請求項２】
前記認証エージェントサーバおよび前記決済サーバは、不正侵入を遮断する機能を有するファイヤーウォールサーバを介して前記公開サーバと接続されたことを特徴とする請求項１に記載の電子商取引のサーバシステム。
【請求項３】
前記ＥＣサイトは、前記認証エージェントサーバと接続された前記データベースを有することを特徴とする請求項１または２に記載の電子商取引のサーバシステム。
【請求項４】
前記認証サーバに対して、前記ＥＣサイトのＩＤ、前記仮想ＵＲＬ発行先メールアドレス、前記アクセス制限時間、および前記実際にアクセスさせるサーバのＩＰアドレスを送信する前記手段は、
前記認証サーバに対して、前記ＥＣサイトのＩＤ、前記仮想ＵＲＬ発行先メールアドレス、前記アクセス制限時間、および前記実際にアクセスさせるサーバのＩＰアドレスを暗号化して送信する手段であることを特徴とする請求項１から３のいずれか一に記載の電子商取引のサーバシステム。
【請求項５】
前記決済サーバは、専用線を介して金融機関と接続されたことを特徴とする請求項１から４のいずれか一に記載の電子商取引のサーバシステム。
【請求項６】
前記アクセス制限時間内に前記仮想ＵＲＬがクリックされなかった場合に前記仮想ＵＲＬを消滅させる手段を有することを特徴とする請求項１から５のいずれか一に記載の電子商取引のサーバシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、インターネット網を利用した電子商取引に係り、特に、ｗｗｗサーバ（公開サーバ）、個人認証サーバ、決済サーバ、データベースをインターネット公衆網、専用網を介して、機密性と安全性の程度に応じて結びつけて迅速に処理を行うのと、ユーザと企業とを効率よく結合したサーバシステムの最適化に関する。
【０００２】
【従来の技術】
ｗｗｗサーバと個人パスワードを用いて決済を行っていたが、情報の漏洩、不正使用、改ざん、誤りが多発しクレジットカード会社とのトラブルが絶えなかった。ユーザは安心して信頼して使用出来ないという不具合さがある故、高額な取引は実現していない。
【０００３】
現金の振り替え、手形等の従来からの決済は人手を要して、地球規模で広がったグローバル経済に適応しなくなった。
【０００４】
【発明が解決しようとする課題】
このため、多くのユーザは現状の決済に対する不満があり、瞬時に情報の交換が出来るインターネット時代に即応したｅコマース時代の決済方法を願望していた。
【０００５】
現在のサーバシステムでは、小口の取引では徐々に普及しているが、大口取引は従来の手順で行って来た。金融機関にたびたび足を運んでの決済であるため労力を要してかつ、極めて効率が悪かった。
【０００６】
【発明の目的】
本発明は、かかる従来例の不都合を改善し、特に、サーバシステムとネットワークを有効に組み合わせてユーザに信頼と信用という安心感を与えて効率が良く、迅速に決済処理を

行う事を目的とする。
【０００７】
新規サーバシステムを提案して、Ｗｅｂ上で時間、距離、空間を超越して、浮いた時間と人材をネット時代の、将来の進歩的なビジネスの創出をはかり、我が国の経済を強固なものにしたい。
【０００８】
【課題を解決するための手段】
上記目的を達成するため、サービス、物品の売買、企業イントラネットの活用、情報サイトのデータベースの有料、無料での使用、マーケティング調査、アンケート調査等のユーザへのアクセスに、その使用目的に応じたサーバシステムとインターネットを含む専用網を構成する。
【０００９】
サーバは公開サーバとしてｗｗｗサーバ、個人認証を行う認証エージェントサーバ、認証サーバ、それに取引の決済を行う決済サーバにより構成する。
【００１０】
ネットワークは地球規模に広がったインターネット網、ＰＨＳ等のモバイル・インターネット網、衛星網（ＧＭＰＣＳ：Ｇｌｏｂａｌ Ｍｏｂｉｌｅ ｐｅｒｓｏｎａｌ Ｃｏｍｍｕｎｉｃａｔｉｏｎ ｂｙ Ｓａｔｅｌｌｉｔｅ）を有機的に組み合わせて構成して使用する。
【００１１】
各種ネットワークはサーバシステムによって使用目的に応じて都度、構成する、例えば広く一般人に普及したＮＴＴドコモ社のｉモードサービスを有効に活用する。
【００１２】
発明者はこれらを Ｓｏｌｉｔｏｎ方式 と名付けた。この Ｓｏｌｉｔｏｎ方式 のサーバシステムによって、前述した目的を達成しようとするものである。
【００１３】
本発明では、各種目的に応じたサーバを用いる。小規模なネットワークの構築には、一般的なパソコンで用は足りる。ここで言うサーバは、ネットワーク上部に位置して、流通ネットワーク上にクライアント群（ＰＣ等）が接続されている。
【００１４】
クライアントとはサービスを受ける側（端末機器は、ＰＣ、携帯電話機、携帯情報端末機器等）、サーバとはクライアントにサービスを提供する側と定義する。
【００１５】
ｗｗｗサーバはインターネットにおける情報サービスの一つで、ＨＴＭＬ（Ｈｙｐｅｒ Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）言語で記述した情報を、ＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）によってやり取りする。ＨＴＭＬ等の情報をＨＴＴＰによってクライアントにサービスを提供するためのサーバと定義する。
【００１６】
クライアントはｗｗｗサーバから送信されたＨＴＭＬをｗｗｗブラウザソフト（ｗｗｗ検索、閲覧ソフト）が解析して画面上に表示する。
クライアントのブラウザは、ユーザの指定するホームページのＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｉｏｎ）に従ってｗｗｗサーバにＨＴＭＬの情報の転送を要求する。
【００１７】
本発明ではｗｗｗサーバを公開サーバとし、誰でもアクセス可能である。ｗｗｗサーバと接続してあるＦＷサーバ（ファイヤーウォール）によって、ネットワークを遮断して、不正侵入を防ぐ。ＦＷサーバの背後のネットワーク上に認証エージェントサーバ、データベース、決済サーバが接続されている。

【００１８】
マルチキャストサイトのように、ユーザにアンケートを求めたり、市場調査、クイズ等を提供してポイントを与えたりするサーバは公開サーバ、ｗｗｗサーバを使用する。ＦＷサーバ、認証サーバによって侵入を拒否する必要のない、開放した情報を提供するアプリケーションである事による。
【００１９】
【発明の実施の形態】
【第１実施形態】
【００２０】
以下、本発明の第１実施形態を図１から図５に基いて説明する。
図１はシステムの全体構成図である。本システムは、インターネット等の通信システム１に専用網２、３、さらにモバイル・インターネット網を通信手段に用いる。
【００２１】
これらの通信システムに電子商取引を行うＥＣサイト（Ｅｌｅｃｔｒｉｃ Ｃｏｍｍｅｒｃｅ）５、銀行、クレジット会社６、個人認証を行う認証サイト７、それにクライアント１９の端末機器１６を接続している。
【００２２】
５のＥＣサイトは２４の公開サーバ（ｗｗｗサーバ）と８のファイヤーウォールを介してＬＡＮ１７に認証エージェントサーバ９とデータベース１０、それに電子商取引の決済を行う決済サーバ１１より構成される。
【００２３】
８のファイヤーウォールサーバ、インターネットに常時接続している環境では、誰もがインターネットを介してアクセスすることが出来る利便性という特徴がある。反面、不正侵入をもくろむ悪意を持った第三者からのアクセスがある危険性を持っている。
【００２４】
ファイヤーウォールは、このような第三者からの不正侵入を遮断するために外部ネットワークと内部ネットワークとの中間に位置して門番の役割を果たす。
【００２５】
図１，５において２４の公開サーバにはルータ１２を介して誰でもアクセス出来る。しかし８のファイヤーウォールサーバ以降のネットワークにはアクセス出来ない。
【００２６】
インターネット網１から２４の公開サーバのＣＧＩ（Ｃｏｍｍｏｎ Ｇａｔｅｗａｙ Ｉｎｔｅｒｆａｃｅ）へアクセスする。ＣＧＩはクライアントのブラウザからの要求に対してｗｗｗサーバ（公開サーバ）側で対応するプログラムを起動し、このプログラムで得た結果をクライアント側に返送するインターフェースである。
【００２７】
インターネット上でのショッピング等の場合は、ｗｗｗサーバからクライアントに対して商品のＰＲをするだけでなく、その場で注文を受け付けたり、ユーザからのアンケートを収集してそれを集計するなどの必要がある場合も多い。
【００２８】
２４の公開サーバはクライアント１６の端末とＨＴＭＬ（Ｈｙｐｅｒ Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）で記述した情報をＨＴＴＰ（ＨｙｐｅｒＴｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）プロトコルによってやり取りする。
【００２９】
５の認証エージェントサーバはクライアントのＩＤ、メールアドレスを参照して、登録してあるクライアントの情報をデータベース１０より検索し、照合して本人であるか否かを判断する。
【００３０】
不正であれば認証サーバ９は何もアクションを起こさない。本人である事が確認出来たら９は、ＥＣサイト名（図１では５）、ＥＣサイトＩＤ、仮想ＵＲＬ発行先メールアドレス

、アクセス制御時間、実際にアクセスさせるサーバのＩＰアドレス、コメントをフォーマット化（フォーマット後、暗号化しても良い）して７の認証サイトへ送信する。

【００３１】

この場合図１において、２０のＩＰライン、１のＩＰ網、２１のＩＰラインのルートを経由して認証サイト７に送信される。

【００３２】

ＥＣサイト５の認証エージェント９から受信したクライアントからの要求を１８の認証サーバによって仮想ＵＲＬを発行する。１８はＬＡＮ１７、ルータ１２、ＩＰライン２１とインターネット１を経由してクライアントの端末１６に送信される。

【００３３】

受信したクライアント１９は、１６の端末機器のキー又はブラウザを所定時間内に発行された仮想ＵＲＬをクリックすると、専用線１、２を介してＩＰライン２２を介して認証サーバ１８が認知する。

【００３４】

認証サーバ１８はクライアントから受信した仮想ＵＲＬを暗号化して認証サイト７より２１のＩＰライン、１のＩＰ網、２０のＩＰラインを介してＥＣサイトにメールを送る。

【００３５】

ＥＣサイト１１の決済サーバはクライアントからの要求をただちに決済を行う。６は銀行、クレジット会社、その他の金融会社である。１３は銀行、１４はクレジット会社、１５はその他の金融、信託会社で、いずれも現金の決済を行う。

【００３６】

図１のシステム構成は、クライアント１９か端末機器１６でｉモード（ＮＴＴドコモ社のサービス名）メニューによって、欲するものを閲覧する。買いたいもの、欲しいサービスが見つかったら、１６のブラウザをクリックすると自動的にメールが発信して、アンテナ４を介してＥＣサイト５のｗｗｗサーバに入力される。

【００３７】

先に説明したように、本人である事が確認出来れば、仮想ＵＲＬを認証サイトの認証サーバ１８よりクライアントの端末機器１６に折り返し、発行される。

【００３８】

クライアントは所定時間内に発行された仮想ＵＲＬをクリックすると取引は成立して、決済される。所定時間経過してもブラウザのクリックがなければ、発行された仮想ＵＲＬは自然に消滅する。

【００３９】

図２はＥＣサイト５とクライアントの端末機器１６とのメールの更新を示すブロック図である。以下、図に基いて説明する。図中、▲１▼から▲７▼の記号は各ブロック間の流れを示すパスである。▲１▼はクライアントの端末機器１６よりインターネットに一般公開サーバのＣＧＩプログラムへアクセスする。例えばＮＴＴドコモ社のｉモードサーバがある。

【００４０】

▲２▼はＣＧＩで作成されたブラウザのフォーム内にユーザＩＤを送信する。１６が携帯電話機の場合、メールボックスを自動的に開く命令とともに、宛先アドレスを自動発信する。

【００４１】

▲３▼、▲４▼は、２４のｗｗｗサーバのＣＧＩプログラムによってユーザＩＤとユーザのメールアドレスをフォーマット化して、８のファイヤーウォールサーバを介して認証エージェントサーバ９に送られる。不正アクセスは８によって遮断される。

【００４２】

▲５▼は認証エージェントサーバ９よりクライアントからの要求を１０のデータベースを参照する。ユーザＩＤとメールアドレスのチェックを行う。１０のデータベースにはクライアントのあらかじめ登録してある個人情報を格納している。

【００４３】
ユーザＩＤ、メールアドレスが正しくなければ９の認証エージェントはクライアントの要求を無視する。何もアクションは起こさない。
【００４４】
正しいと判断した場合は認証エージェントサーバ９はＥＣサイトＩＤ、仮想ＵＲＬ発行メールアドレス、アクセス制限時間、実際にアクセスするサーバのＩＰアドレス、コメントをフォーマット化して、暗号化して、▲６▼のパスで１８の認証サーバへ送る。
【００４５】
▲６▼のパスはＩＰ網１を経由するので９の認証サーバで暗号化して認証サイト７の認証サーバ１８へ送信する。
【００４６】
▲７▼は決済サーバ１１との接続を示す。クライアントに発行した仮想ＵＲＬをクリックして決済の意志が表示された時に実際の現金の決済を行う。１１は図１に示す６の金融機関に接続している。
【００４７】
図１において決済サーバ１１と金融機関を結ぶ２３のラインは、不正アクセスを遮断する目的から、専用線もしくは暗号化して送信する。
【００４８】
図３は認証サイト７の認証サーバの構成要素を示すブロック図である。ＥＣサイト５の認証エージェント９から暗号化されたメールが入力される。図中▲１▼から▲１３▼の記号はブロック構成間の流れを示すパスである。
【００４９】
▲１▼のパスは暗号化フォーマットされたメールの入力部３１を示す。▲２▼は暗号フォーマットのデコード部３２に接続し、▲３▼のパスで３３のブロックで平文にもどされる。
【００５０】
▲４▼のパスでは平文化されたデータを３４のブロックでサイト名、メールアドレス、ＩＤをチェックする。不正があれば▲６▼のパスで排除され、アクションは起こさない。
【００５１】
正しければ▲５▼のパスで、仮想ＵＲＬ　ＰＲＯＸＹの設定を行う。実際に通信を行う相手はインターネットのように複数のネットワークやルータなどを介した場所に存在する。このために同一ネットワークの相手のＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを知るだけでは用は足りない。
【００５２】
そのため、ルータがその先にある端末にかわってＡＰＲ（Ａｄｄｒｅｓｓ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）レスポンスパケットを応答することをＰＲＯＸＹと称する。
【００５３】
▲７▼のパスで仮想ＵＲＬ　ＰＲＯＸＹは３９のブロックでＰＲＯＸＹを設定する。▲８▼のパスで実ＩＰアドレスが送られる。
【００５４】
▲９▼のパスでは仮想ＵＲＬの体制が整い、Ｒｅａｄｙ状態となる。３６のブロックはタイマー部で、発行した仮想ＵＲＬを所定時間可能にし、一定時間後に消滅させるためのカウントを行う。
【００５５】
▲１０▼のパスで、ブロック３７においてメールをフォーマット化して▲１１▼のパスでクライアントの端末機器１６に送信する。▲１２▼のパスは３６のタイマーのカウントによって所定時間経過後クライアントからのアクションが無かったり、不正使用が発覚した時に３９のＰＲＯＸＹの発信を遮断する。
【００５６】

パス▲１３▼はクライアント１６よりアクション、この場合発行した仮想ＵＲＬを１６の端末機器のブラウザ上をクリックした場合、クライアントの商取引の意志が表示して、成立する。

【００５７】

ブロック３８はウォッチドのプログラムで、不正を監視する。▲１４▼のパスで正しければ、ＰＲＯＸＹ設定ＯＫの信号を出し、不正があればＰＲＯＸＹの設定を遮断する。

【００５８】

▲７▼のパスでブロック３５より仮想ＵＲＬが設定された時、▲１２▼、▲１４▼のパスからの信号を待って３９のＰＲＯＸＹは設定される。

【００５９】

図４はクライアントの要求によって認証サーバ１８による仮想ＵＲＬの発行とＰＲＯＸＹの設定までを示したフロー図である。

【００６０】

Ｓ４０１はクライアントの端末機器よりＩＤメールが発信され、Ｓ４０２で公開サーバ２４にてメールフォーマットの処理が行われる。Ｓ４０３では認証エージェントサーバ９によって個人認証が行われる。不正アクセスされていたり、悪意がある事がわかれば遮断する。

【００６１】

Ｓ４０４では、ＩＤ、メールアドレスが正しく、本人である事が確認された。認証サイトの認証サーバに仮想ＵＲＬの発行を要求する。

【００６２】

Ｓ４０５は、仮想ＵＲＬの発行を認証エージェントサーバ９から認証サーバ１８に要求するのにインターネット網１を経由するため暗号化を行う。暗号化処理を行って認証サーバ１８に送る。

【００６３】

Ｓ４０６は認証サイトの認証サーバ１８にて暗号化されたデータを復号する。Ｓ４０７では平文にして解析を行う。

【００６４】

Ｓ４０８ではＩＤ、メールアドレスのチェックを行う。不正が発覚すれば直ちに遮断する。Ｓ４０９は、正しく本人認証が立証出来たので仮想ＵＲＬ　ＰＲＯＸＹの設定を行う。そしてＳ４１０でタイマーをスタートする。

【００６５】

Ｓ４１１で要求したクライアントに仮想ＵＲＬを発行する。タイマーは所定時間内に仮想ＵＲＬをクライアントがクリックして返信メールが到着するまで、所定時間内であるか否かをカウントする。

【００６６】

Ｓ４１２ではタイマーが設定した時間内に返信メールが到着しない場合は、発行した仮想ＵＲＬを消滅させて、以降の動作を遮断する。

【００６７】

Ｓ４１３では、所定時間内に返信があればＳ４１４に進み、さらにメールアドレス、ＩＤ（パスワード）等のチェックを行って不正があれば遮断する。

【００６８】

Ｓ４１５ではＰＲＯＸＹを設定する。ＰＲＯＸＹは実アドレスの設定を行う。仮想ＵＲＬはＰＲＯＸＹで設定する実アドレスをマスクしたものでバーチカルであって実際の使用者には見えない。

【００６９】

Ｓ４１６では仮想ＵＲＬの発行、クライアントからの応答によってＰＲＯＸＹが設定されて、全ての処理が終了する。

【００７０】

図５は、図１のシステムにおいてクライアント（ユーザ）がＥＣサイトにアクセスして、

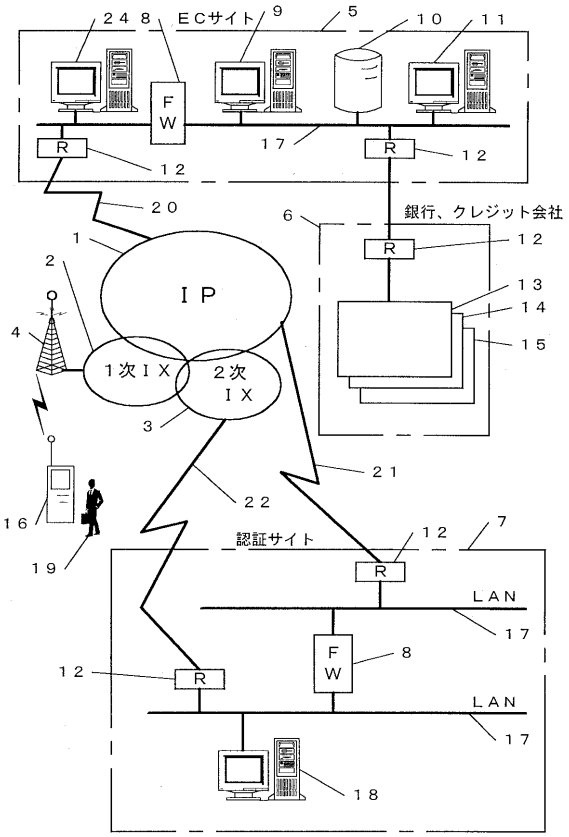
ＥＣサイトの公開サーバ２４よりメニューをＨＴＭＬによってクライアントのブラウザに表示する。
クライアントの物品、サービスの購入意志表示をＥＣサイトにメール発信して、物品、サービスの提供を受け、決済を行うシーケンスを示した。
【００７１】
図５において、公開サーバ（ｗｗｗサーバ）はｉモードサーバを使用して、メニューの閲覧は普通のＩＰ網で行う。
【００７２】
仮想ＵＲＬ、購入決定のメール等は機密保持上専用網図１、２、３を介して処理を行う。
【００７３】
次に、本発明の第２実施形態を図６と図７に基いて説明する。図６にシステムの全体構成を示す。
第１実施形態で示した図１とインターネット網１と専用網２、３は同一である。
【００７４】
本実施形態においては、企業内イントラネット６２とＳＯＨＯ（スモールオフィス、ホームオフィス）６１とクライアント１９の相互動作、遠隔処理を行う事に特徴がある。
【００７５】
本システムは、企業人が会社以外の場所、サテライトオフィス、ホームで、路上から、企業内のイントラネットに仮想ＵＲＬを発行して、機密性、安全性を高めて使用できる。
【００７６】
６２の企業内イントラネットは、２４の公開サーバとファイヤーウォール８で遮断されたＬＡＮ１７にアクセス出来る。
企業内データベース６７は、多彩な記憶手段により構成されており、営業用の顧客データ、取引先データ、購買データ、統計、開発データから、企業の経営、運営上必要なデータが格納してある。
【００７７】
普通社員は、社内でこれらのデータを必要に応じて収集して仕事の処理を行ってきた。
【００７８】
根まわし、稟議、決済等々、無駄な時間と労力を費やして来た。社内はもとより、社外のあらゆる場所からアクセスして今まで人力で行って来た作業を電子処理で行う事が可能である。
【００７９】
公開サーバ２４と社内のイントラネットは、ファイヤーウォール８によって完全にアイソレーションしている。まず社内においては、６４のサーバ、６５、６６のＰＣ、携帯端末機器１６を用いて電子処理が可能である。
【００８０】
社内ではフルートゥース、Ｉｒｄａを用いて端末間ネットワークをアクセス出来る。６８はこれら携帯端末機器、端末、ＰＣをワイヤレスで接続するためのアンテナである。
【００８１】
２４の公開サーバは外から誰でもインターネット１を介してアクセス出来る。企業のホームページ、企業の情報等があって、必要に応じて利用出来る。企業の受付とも言える。
【００８２】
６１のＳＯＨＯは、会社員が家庭から企業の機密情報を取り出して処理を行い、決済を行う。モバイル・インターネットを用いて街中でも行う事が出来る。
【００８３】
仮想ＵＲＬを、６４の認証サーバにて発行して本人認証を行う手順は、第１実施形態と同じである。
企業イントラネットシステムでは、認証エージェントサーバは使用していない。使用する人は、企業内の人、及びその関係者に限られ、ＩＤ、パスワード、メールアドレスが与えられる。

【００８４】
６３は物品、サービスを配送する輸送車で、決済に応じて客先、クライアント等を往来する。なお、最高機密を外部から、企業イントラネットよりとり出す場合、本人認証を複数回行ったり、複数のパスワードを使用して機密情報をとり出すようにする。２つ以上のパスワードは、企業が重要と認めたもののみ与える少数に限られる。
【００８５】
図７は、図５のシステム、企業内のイントラネットのプロセスシーケンス制御図を示す。第１実施形態と同様なので説明は省略する。公開サーバ２４へのアクセスはＩＰ（インターネット網）で行って、仮想ＵＲＬの発行はＶＰＮ（専用線、Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）で処理するのも同じである。
【００８６】
次に、本説明による第３実施形態について、図８、図９、図１０に基いて説明する。システム構成は、第１実施形態で説明した構成と同じ内容であるが、ここでは専用網を用いていない。
【００８７】
会員制の情報サイト、趣味、サークルのサイト、マーケティングリサーチ、調査、クイズ等の回答に幅広く用いる事が出来る。
【００８８】
図８において、８１は情報サイトである。ここには趣味、ゲームをはじめアミューズメント、スポーツ等々有料会員制で利用出来る。２４は公開サーバ、８のファイヤーウォールサーバでアイソレートされてＬＡＮ１７に接続した８４の非公開サーバ。８４は本人認証、仮想ＵＲＬの発行を行う。
【００８９】
８５はデータベース、構成は、図１のシステムとほぼ同様である。８２の家庭、６１のＳＯＨＯ、モバイル・インターネット１６でアクセス出来る。８３の車載端末機器からもドライブしながらアクセス可能である。
【００９０】
図９は、会員制情報サイトのプロセスシーケンス制御図を示す。第１実施例と仮想ＵＲＬの発行、メールの発信は同じであるが、機密性は低いため専用網を使っていない。
【００９１】
本実施例においては、無料で、お金を払わないで情報サイトへのアクセスを排除するだけでも良い。
【００９２】
図１０は、マーケティングリサーチ、アンケート、クイズ等に利用する事を目的としている。図８のシステム構成を使用した、プロセスシーケンス制御図である。
【００９３】
本実施例においては、機密性、安全性は全く必要ないし、ユーザがお金を払う必要もない。従って認証は行わず、公開サーバ（ｗｗｗサーバ）とデータベースのみで行う。
【００９４】
メニュー等については、ｉモードサービスを利用する。ユーザは、アンケートに答えてポイントを稼いで商品をもらったり、商品を安価に購入出来るというサービスを受けられる。
【００９５】
ポイントシステムは、カメラ、家電、量販店、外食産業まで波及し、消費者の購買意欲を向上させている。今後ポイントキャストは大いに利用されると考えられる。
【００９６】
以上説明した各実施形態によれば、公開サーバ（ｗｗｗ）と非公開サーバ（認証サーバ）と既存のｉモードサービスを利用して、安全、確実に電子商取引が出来るのと、社会活動の必要な情報を、素早く、安価に利用出来、かつ家でも、モバイルでも、企業の高度な機密性の高い仕事を行えるので、経済活動を活性化する最良のシステムである。

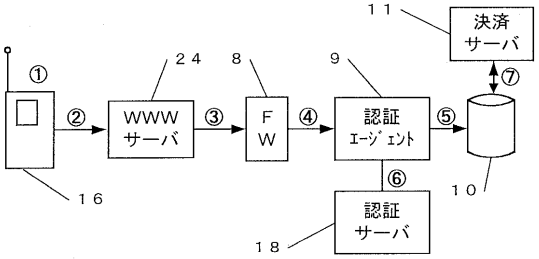
【００９７】
本発明は、以上のように構成され機能するので、クライアントがｉモードメニューによって検索出来、物品、サービスの購入の意志表示、決済は、実アドレスをマスクした仮想ＵＲＬによって行う。従って機密性、安全性は確保出来て、電子商取引を活性化するシステムを提供出来る。
【００９８】
公開サーバ、非公開サーバと認証、決済、インターネット公衆網、専用網を利用目的に応じて有機的に組み合わせて使用するから利便性が高く、ユーザは安価に使用出来る。
【００９９】
さらに情報サイトの活用によって、趣味、スポーツ、アミューズメントの輪が広がり、社会を活性化させ新規ビジネスの創出に寄与出来る。
【図面の簡単な説明】
【図１】第１実施形態を示すシステム構成図である。
【図２】ＥＣサイトを示すブロック構成図である。
【図３】認証サーバのブロック構成図である。
【図４】仮想ＵＲＬ発行のプロセスを示すフロー図である。
【図５】電子商取引のプロセスを示すシーケンス制御図である。
【図６】第２実施形態を示すシステム構成図である。
【図７】イントラネットのアクセスプロセスを示すシーケンス制御図である。
【図８】第３実施形態を示すシステム構成図である。
【図９】情報サイトへのアクセスプロセスを示すシーケンス制御図である。
【図１０】ポイントキャストのアクセスプロセスを示すシーケンス制御図である。
【符号の説明】
１．　インターネット網
２．　１次専用網
３．　２次専用網
４．　モバイルインターネット基地局
５．　ＥＣサイト
６．　金融機関
７．　認証サイト
８．　ファイヤーウォールサーバ
９．　認証エージェントサーバ
１０．　データベース
１１．　決済サーバ
１２．　ルータ
１３．　銀行
１４．　クレジット会社
１５．　信託会社、他の金融機関
１６．　携帯情報端末機器
１７．　ＬＡＮ
１８．　認証サーバ
１９．　クライアント
２０、２１、２２、２３．インターネットライン
２４．　ｗｗｗサーバ
３１．　暗号化フォーマット部
３２．　復号化器
３３．　平文解析
３４．　サイト、メール、ＩＤチェック部
３５．　仮想ＵＲＬ　ＰＲＯＸＹ設定部
３６．　タイマー部

３７．　メールフォーマット部
３８．　監視プログラム部
３９．　ＰＲＯＸＹ設定部
６１．　スモールオフィス・ホームオフィス
６２．　企業内イントラネット
６３．　配送車
６４．　企業内認証サーバ
６５．　ＰＣ
６６．　ノートＰＣ
６７．　企業内データベース
６８．　ブルートゥース／Ｉｒｄａアンテナ
６９．　電話機付ＦＡＸ
８１．　情報サイト
８２．　家族
８３．　乗用車
８４．　非公開サーバ
８５．　データベース

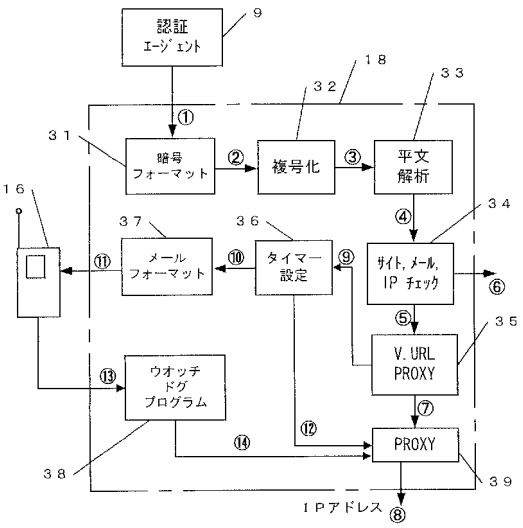
【図１】



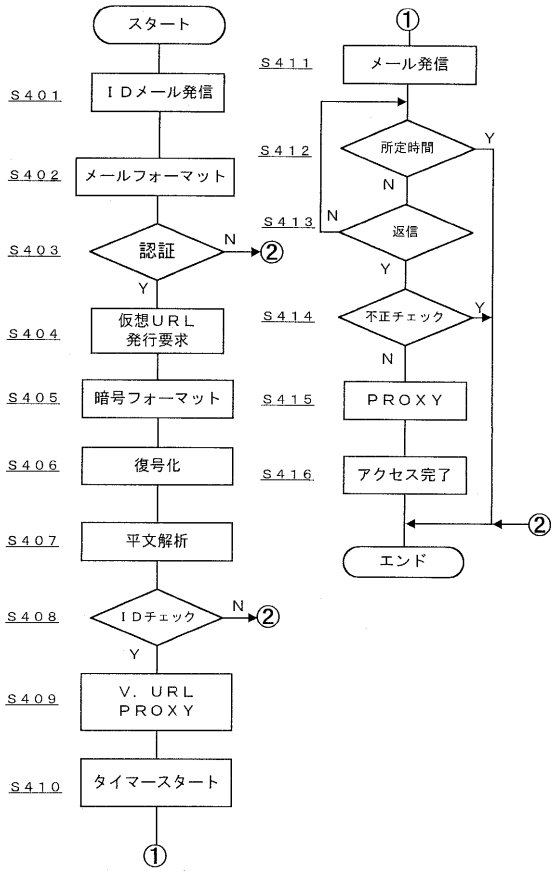
【図２】



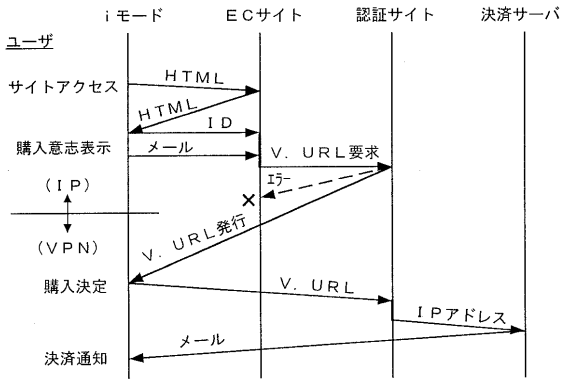
【図３】



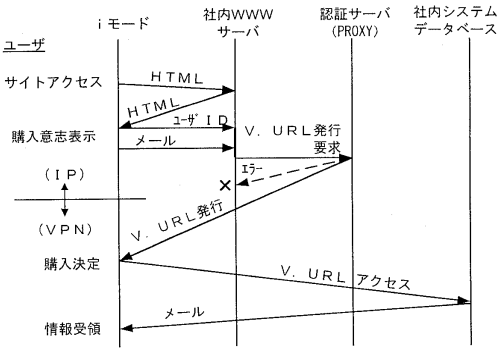
【図４】


スタート
S401
ＩＤメール発信
S402
メールフォーマット
S403
認証
N
②
Y
S404
仮想ＵＲＬ
発行要求
S405
暗号フォーマット
S406
復号化
S407
平文解析
S408
ＩＤチェック
N
②
Y
S409
Ｖ．ＵＲＬ
ＰＲＯＸＹ
S410
タイマースタート
①
①
S411
メール発信
S412
所定時間
Y
N
S413
返信
N
Y
S414
不正チェック
Y
N
S415
ＰＲＯＸＹ
S416
アクセス完了
②
エンド

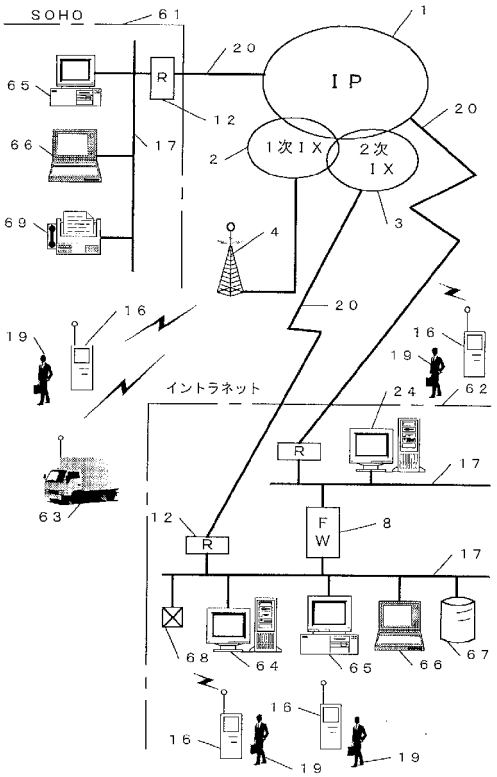
【図５】


ｉモード
ＥＣサイト
認証サイト
決済サーバ
ユーザ
サイトアクセス
HTML
HTML
ＩＤ
購入意志表示
メール
Ｖ．ＵＲＬ要求
（ＩＰ）
エラー
（ＶＰＮ）
Ｖ．ＵＲＬ発行
購入決定
Ｖ．ＵＲＬ
ＩＰアドレス
メール
決済通知

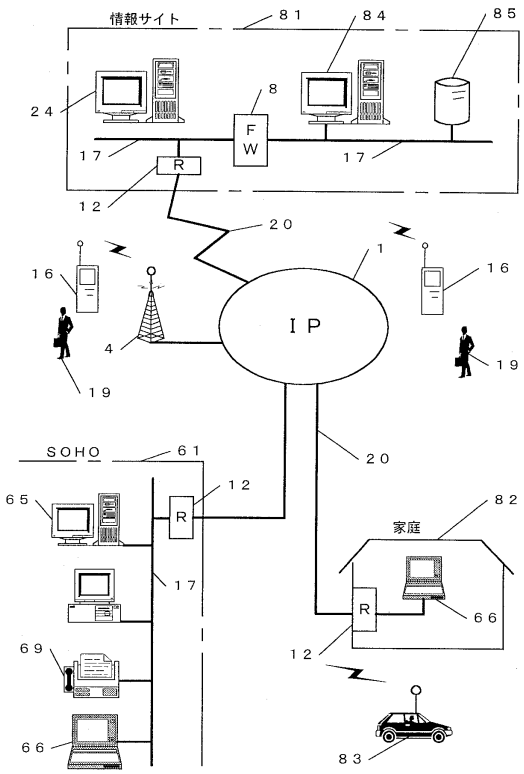
【図７】


ｉモード
社内WWW
サーバ
認証サーバ
(PROXY)
社内システム
データベース
ユーザ
サイトアクセス
HTML
HTML
ユーザ ＩＤ
購入意志表示
メール
Ｖ．ＵＲＬ発行
要求
（ＩＰ）
エラー
（ＶＰＮ）
Ｖ．ＵＲＬ発行
購入決定
Ｖ．ＵＲＬ アクセス
メール
情報受領

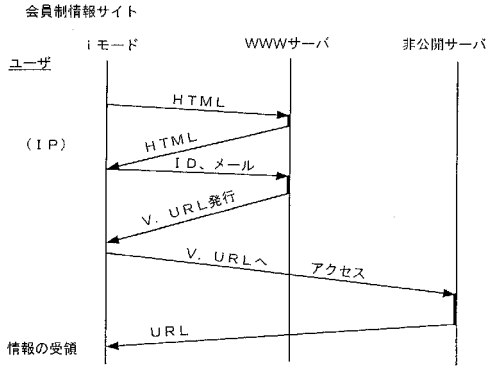
【図６】


SOHO
61
1
ＩＰ
20
65
R
12
66
17
2
1次ＩＸ
2次
ＩＸ
3
69
4
20
16
19
16
19
62
イントラネット
24
R
17
63
12
R
FW
8
17
68
64
65
66
67
16
16
19
19

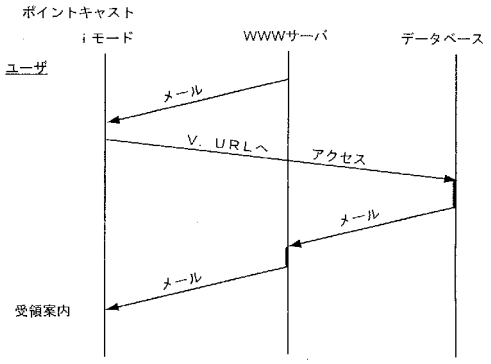
【図８】


情報サイト
81
84
85
24
8
FW
17
17
R
12
20
1
16
16
4
ＩＰ
19
19
SOHO
61
20
65
R
12
82
家庭
17
R
66
69
12
66
83

【図９】


会員制情報サイト
ｉモード
WWWサーバ
非公開サーバ
ユーザ
HTML
HTML
（ＩＰ）
ＩＤ、メール
Ｖ．URL発行
Ｖ．URLへ
アクセス
URL
情報の受領

【図１０】


ポイントキャスト
ｉモード
WWWサーバ
データベース
ユーザ
メール
Ｖ．URLへ
アクセス
メール
メール
受領案内

フロントページの続き

(51)Int.Cl. FI
G06F 17/60 512

(56)参考文献 特開平１０－２８９２６７（ＪＰ，Ａ）
特開２０００－２０７３００（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
G06Q 30/00
G06Q 10/00
G06Q 20/00
G06Q 40/00
G06Q 50/00