

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 6 月 20 日 (20.06.2002)

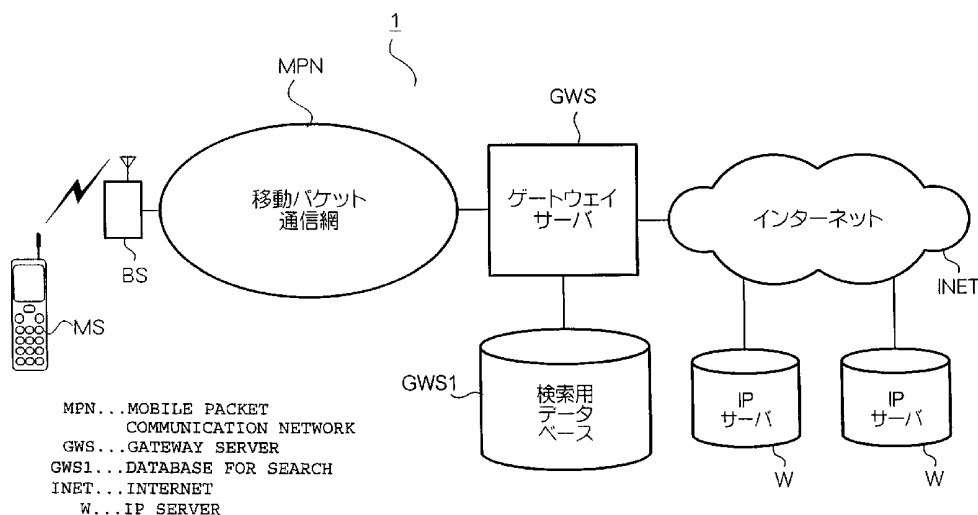
PCT

(10) 国際公開番号
WO 02/48893 A1

- (51) 国際特許分類: G06F 15/00, 17/60
- (21) 国際出願番号: PCT/JP01/10834
- (22) 国際出願日: 2001 年 12 月 11 日 (11.12.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特 願 2000-376630
2000 年 12 月 11 日 (11.12.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社
エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.)
[JP/JP]; 〒100-6150 東京都千代田区永田町二丁目 11
番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 山本正明 (YA-
MAMOTO, Masaaki) [JP/JP]; 〒235-0033 神奈川県横
浜市磯子区杉田九丁目 2-10-107 Kanagawa (JP). 平松孝
- (74) 代理人: 川崎研二 (KAWASAKI, Kenji); 〒103-0027 東
京都中央区日本橋一丁目 2 番 10 号 東洋ビルディング
7 階 朝日特許事務所 Tokyo (JP).
- (81) 指定国 (国内): AU, BR, CA, CN, JP, KR, NO, NZ, PL,
SG, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- 添付公開書類:
— 国際調査報告書
- 2 文字コード及び他の略語については、定期発行される
各 PCT ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(54) Title: METHOD AND DEVICE FOR AUTHENTICATING USER

(54) 発明の名称: ユーザ認証を行うための方法及び装置



(57) Abstract: An IP server (W) and a gateway server (GWS) transmit data of the HTML format in response to a request of a mobile station (MS). In the HTML data, an individual identification information request data sequence is added to the URL of a Web page concerning a service requiring user authentication. The HTML data is received by the mobile station (MS), and an image corresponding to the HTML data is displayed on a liquid crystal display unit. In this state, a user carries out an operation for designating the URL. Then the mobile station (MS) reads the individual identification information from a ROM to send it to a mobile packet communication network (MPN). Thus, the IP server (W) authenticates the user on the basis of the individual identification information sent from the mobile station (MS).

[続葉有]



(57) 要約:

I PサーバWやゲートウェイサーバGWSは、移動機MSからの要求に従ってHTML形式のデータを送信する。ここで、このHTMLデータ中において、ユーザ認証が必要なサービスに関連するページのURLには、個人識別情報要求データ列が付加されている。このHTMLデータが移動機MSに受信され、当該HTMLデータに対応した画面が液晶表示部に表示されている状態において、ユーザが当該URLを指定する入力操作を行う。すると、移動機MSは、個人識別情報をROMから読み出して移動パケット通信網MPNへと送出する。I PサーバWは、このようにして移動機MSから送出された個人識別情報に基づいてユーザ認証を行う。

明 細 書

ユーザ認証を行うための方法及び装置

5 技 術 分 野

本発明は、相異なるネットワーク間においてエンドトゥエンドのユーザ認証を行うための方法および装置に関する。

技 術 背 景

10 近年、携帯電話機等の移動機の高機能化に伴って、移動機にWWW（World Wide Web）のブラウザ（以下、「WWWブラウザ」という）を搭載し、移動機単体でWWWのブラウジングを可能とする製品が市販されている。かかる移動機を利用することにより、ユーザは、インターネット上のインフォメーションプロバイダ（以下、「IP」という）から各種サービスの提供を受けることが可能と
15 になっている。

ここで、IPが提供するサービスの中には、契約ユーザに対してのみ提供されるものや秘匿性を必要とするものが存在する。このため、この種のサービスを提供するIPは、第三者による不正使用を防止する観点から、サービスの提供時にユーザ認証を行っている。このユーザ認証方法として、従来、一般的に用いられて
20 いる方法が、パスワードを用いた方法である。しかし、パスワードによるユーザ認証方法では、パスワードが悪意の第三者に漏洩する危険性があり、また、パスワードが漏洩してしまうと、誰でも不正使用ができるようになってしまう。このため、例えば、ネットウェアを利用した銀行取引サービス（以下、「ネットバンキング」と言う）のように、セキュリティの確保が不可欠なサービスを提供す
25 るに当たっては、より信頼性の確保できるユーザ認証方法を利用することが必要となる。

そこで、かかるサービスを提供するIPにおいては、移動通信網の保有する発ID等の移動機を特定できるユニークな情報（以下、「個人識別情報」という）

を用いて、ユーザ認証を行っている。このユーザ認証方法について簡単に説明すると以下のとおりである。

i. 移動機のユーザにサービスを提供する場合、まず、I Pの保有するサーバ（以下、「I Pサーバ」という）は、移動通信網に対して個人識別情報の送信要求を送信する。

ii. この送信要求に基づいて、移動通信網が、個人識別情報をI Pサーバへと返信する。

iii. I Pサーバは、移動通信網から返信されてきた個人識別情報に基づいて、ユーザ認証を行う。

10 従来においては、以上説明したユーザ認証方法により、第三者による不正使用を有効に防止しているのである。

しかしながら、個人識別情報は、ユーザのプライバシーや財産に関わる重要な情報である。このため、移動通信事業者が、何らの制限なく、この個人識別情報をI Pに提供してしまうと、移動機のユーザに不測の不利益を与える危険性がある。移動通信事業者は、かかる不測の不利益を防止するため、自身の保有する個人識別情報の提供先となるI Pと事前に契約し、これにより、個人識別情報の提供先についての信頼性を確保している。このように、かかる方法では、事前の契約が必要となる結果、移動通信事業者と契約を結んでいないI Pがユーザ認証に個人識別情報を利用することは不可能であり、当該I Pにおいては個人識別情報を用いた認証を行うことができないという問題があった。

発明の開示

本発明の目的は、移動通信事業者と特別な契約を結ぶことなく、全てのI Pにおいて個人識別情報を利用したユーザ認証を行うことを可能とするユーザ認証方法及び通信システムを提供することである。

上記目的を達成するため、この発明は、第1のネットワークに収容された携帯端末が、前記第1のネットワークからデータを受信する受信過程と、前記携帯端末が前記受信過程において受信したデータ中に所定のデータ列が存在するか否か

を検出する検出過程と、前記検出過程において前記データ列が存在するものと検出された場合にのみ、前記携帯端末が、予め自端末に記憶されているユーザを一意に特定するための個人識別情報を送信する送信過程と、前記第1のネットワークと第2のネットワークとの間のデータの授受を中継する中継装置が、前記携帯
5 端末から送信された個人識別情報を前記第2のネットワークへと転送する転送過程と、前記第2のネットワークに接続されたサーバが、前記個人識別情報に基づいて前記携帯端末のユーザを認証する認証過程とを具備することを特徴とするユーザ認証方法を提供する。

かかる構成において、前記送信過程において前記携帯端末が送信する個人識別
10 情報は、前記サーバ以外の装置によって解読不能な形式により送信されるようにしても良い。この場合、前記認証過程において前記サーバは、前記携帯端末から送信された個人識別情報を解読し、当該個人識別情報に基づいて前記携帯端末のユーザを認証することとなる。

また、前記受信過程に先立ち、前記中継装置が、前記携帯端末からの要求に従
15 って、前記第2のネットワークにおける前記サーバのアドレスを検索する検索過程を設けるようにしても良い。この場合、前記受信過程において前記携帯端末が受信する前記データは、前記検索過程において、前記中継装置が検索した検索結果に対応したデータとなる。好ましい態様において、前記データをマークアップ言語により記述し、前記データ列を、前記データ内において所定の識別子により
20 マークアップするようにしても良い。

更に、前記送信過程に先立ち、前記検出過程において前記データ列が存在するものと検出された場合にのみ、前記携帯端末が自端末のユーザに対して、前記個人識別情報の送信の可否について判断を促す判断促進過程を更に設け、この過程においてユーザの許可が得られた場合にのみ、前記送信過程において、前記携帯
25 端末が前記個人識別情報を送信するようにしても良い。この場合、前記判断促進過程において、ユーザの判断を仰ぐための画像を表示するのみならず、ユーザに対して入力識別情報の入力を促し、ユーザが入力した入力識別情報を、前記送信過程において前記個人識別情報と共に送信するようにしても良い。

また、前記認証過程の後に、前記サーバが前記携帯端末に対して前記入力識別情報の入力を促す入力データを配信する配信過程と、前記配信過程において配信された前記入力データを受信した前記携帯端末が当該入力データに基づきユーザに対して入力識別情報の入力を促す過程と、前記入力を促す過程において入力された入力識別情報を送信する第2の送信過程と、前記第2の送信過程において送信された入力識別情報に基づいて前記携帯端末のユーザを認証する第2の認証過程とを更に設けるようにしても良い。

好ましくは、前記個人識別情報として、前記携帯端末の製造番号を用いると良い。この場合において、個人識別情報として、更に、前記携帯端末の製造番号と、前記携帯端末に接続されたユーザ識別モジュールに格納された情報との組み合わせを用いれば、認証の信頼性を高めることが可能となる。また、前記第1のネットワークとして、移動通信網を用いても良い。

この発明は、更に、第1のネットワークからデータを受信し、当該データ中に所定のデータ列が存在するか否かを検出して、前記データ列が存在するものと検出された場合にのみ、予め自端末に記憶されているユーザを一意に特定するための個人識別情報を前記第1のネットワークに送信する携帯端末と、前記第1のネットワークと中継装置を介して相互接続された第2のネットワークと、前記第2のネットワークに接続され、前記個人識別情報に基づいて認証を行うサーバとを具備することを特徴とする通信システムを提供する。

また、この発明は、第1のネットワークを介して他者との通信を行う通信部と、前記通信部により前記第1のネットワークおよびこれに接続された第2のネットワークを介して、該第2のネットワーク内のサーバと通信を行い、該サーバから所定のデータ列を含むデータを受け取ったとき、当該携帯端末に備えられたメモリまたは当該携帯端末に接続されたメモリから個人識別情報を読み出し、前記コネクションを介して前記サーバに送信する制御部とを具備することを特徴とする携帯端末を提供する。

また、この発明は、このような携帯端末としての機能を営むためのプログラムをネットワークを介してユーザに配布したり、CDやFDなどの記憶媒体に格納

してユーザに配布するという態様でも実施され得る。

図面の簡単な説明

図 1 は、実施形態にかかる通信システム 1 の全体構成を例示する図である。

5 図 2 は、同実施形態にかかる I P サーバ W の構成を例示するブロック図である。

図 3 は、同実施形態にかかる H T M L データのソース例を示す図である。

図 4 は、図 3 に示すデータに対応した画像の一例を示す図である。

10 図 5 は、同実施形態にかかる個人識別情報データベース 1 1 3 の記憶内容を例示する図である。

図 6 は、同実施形態にかかる検索用データベース G W S 1 の記憶内容を例示する図である。

図 7 は、同実施形態にかかる移動機 M S の構成を例示するブロック図である。

15 図 8 は、同実施形態にかかる履歴格納テーブル T B L の記憶内容を例示する図である。

図 9 は、同実施形態にかかる移動機 M S の液晶表示部 2 4 に表示される画面の一例を示す図である。

図 1 0 は、同実施形態にかかる移動機 M S の液晶表示部 2 4 に表示される画面の一例を示す図である。

20 図 1 1 は、同実施形態において移動機 M S の C P U 2 1 1 が行う処理を示すフローチャートである。

図 1 2 は、同実施形態にかかる移動機 M S の液晶表示部 2 4 に表示される画面の一例を示す図である。

25 図 1 3 は、同実施形態における通信システム 1 における信号の流れを示すシーケンスチャートである。

図 1 4 は、同実施形態における通信システム 1 における信号の流れを示すシーケンスチャートである。

図 1 5 は、同実施形態にかかる移動機 M S の液晶表示部 2 4 に表示される画面

の一例を示す図である。

図 1 6 は、同実施形態にかかる移動機 M S の液晶表示部 2 4 に表示される画面の一例を示す図である。

図 1 7 は、変形例 1 にかかる個人識別情報データベース 1 1 3 の記憶内容を例示する図である。

図 1 8 は、変形例 2 にかかる移動機 M S の液晶表示部 2 4 に表示される画面の一例を示す図である。

図 1 9 は、同変形例にかかる移動機 M S の液晶表示部 2 4 に表示される画面の一例を示す図である。

図 2 0 は、変形例 3 にかかる移動機 M S 2 の構成を例示するブロック図である。

図 2 1 は、同変形例にかかる U I M 2 0 0 0 の構成を例示するブロック図である。

図 2 2 は、同変形例にかかる個人識別情報データベース 1 1 3 の記憶内容を例示する図である。

発明を実施するための最良の形態

以下、図面を参照して、本発明の実施形態について説明する。本実施形態は、本発明をインターネットに接続された移動通信網に適用することによって実現されるものである。

< 1 - 1 . 実施形態の構成 >

< A . システム全体の構成 >

図 1 は、本実施形態にかかる通信システムの構成を示すブロック図である。

同図に示すように本実施形態にかかる通信システム 1 は、複数の移動機 M S と、複数の基地局 B S と、移動パケット通信網 M P N と、ゲートウェイサーバ G W S と、インターネット I N E T と、複数の I P サーバ W とを有する。なお、図 1 においては、図面が煩雑となることを防ぐため、通信システム 1 に收容された

移動機MS、基地局BS及びIPサーバWのうち所定の移動機、基地局及びIPサーバのみが示されている。

移動機MSは、携帯電話機等の携帯型の電子機器であって、図1に示す移動パケット通信網MPNを介してデータ通信が可能な他、図示しない移動電話網を介して音声通話を行う。移動機MSは、移動パケット通信網MPNを介したデータ通信により、当該IPサーバWから各種サービスの提供を受ける。また、移動機MSは、個人識別情報を記憶しており、ユーザ認証が必要なサービスの提供を受けるにあたり、IPサーバWに対して個人識別情報を送信する。ここで、個人識別情報には、ユーザを一意に特定することができるユニークな情報であれば如何なる情報を利用しても構わないが、本実施形態においては移動機MSの製造番号を用いるものとする。

IPサーバWは、IPが保有するWWW（World Wide Web）サーバであり、移動機MSに対して「ネットバンキング」（例えば、「銀行振込」や「残高照会」等）や会員制のサービス等の各種サービスを提供する。

図2は、IPサーバWの構成を示したブロック図である。同図に示すように、IPサーバWは、データ配信管理部111と、認証部112と、個人識別情報データベース113と、通信部114を有する。

データ配信管理部111は、例えば、CPU(Central Processing Unit)、ROM(Read Only Memory)、RAM(Random Access Memory)、ハードディスク（何れも図示は省略）を有する。ハードディスクには、ホームページやWebページ等のリソースに対応したHTML(Hyper Text markup Language)形式のデータ（以下、「HTMLデータ」という）が格納されており、その各々にはURLが設定されている。ROMには、移動機MSからGETメソッドを用いたHTTP(Hyper Text Transfer Protocol)やHTTPSのメッセージ（以下、「GET要求」という）を受けた場合に、当該GET要求に従ってデータを配信するための制御プログラムが格納されている。CPUは、これらプログラムに従って各種処理を実行する。RAMは、CPUのワークエリアとして用いられる。

ここで、本実施形態においてデータ配信管理部 1 1 1 からインターネット I N E T に送信される H T M L データには、従来にない特徴的な構成が存在する。

図 3 は、本実施形態にかかる H T M L データのソース例を示したものであり、図 4 は、図 3 に示すデータに対応した画像の一例を示す図である。図 3 において、`<A h e r f = "" ></A>` は、アンカータグであり、このアンカータグによって、I P サーバ W が移動機 M S に提供可能なサービスに関連するページに対応した U R L が指定されている。

この図 4 に示す「銀行振込」なるメニュー項目には、図 3 に示すアンカータグ `<A h e r f = "http://www.〇〇.co.jp/△△#utn" ></A>` が対応付けられているが、このアンカータグによって、指定されている U R L の末尾には、「utn」なるデータ列が付加されている。このデータ列「utn」は、I P サーバ W が個人識別情報の送信を要求していることを表すデータ列である（以下、この「utn」なる文字列を「個人識別情報要求データ列」と呼ぶ）。

上述したように、I P サーバ W が移動機 M S に提供するサービスには、「ネットバンキング」サービスや会員制のサービス等のユーザ認証が必要なものが存在する。上述の H T M L データ中には、この種のサービスに関連するページの U R L に対して個人識別情報要求データ列「utn」が付加されたものが含まれている。そして、個人識別情報要求データ列「utn」の付加された U R L を含む H T M L データが移動機 M S に受信され、移動機 M S において当該 U R L が指定されると、移動機 M S は、当該 U R L を含む G E T 要求に対して自らの記憶している個人識別情報を付加して送出する。このようにして、移動機 M S から個人識別情報を含む G E T 要求が送信されてくると、データ配信管理部 1 1 1 は、当該 G E T 要求に含まれている U R L を抽出して、認証部 1 1 2 へと送る。

認証部 1 1 2 は、データ配信管理部 1 1 1 から送られた個人識別情報と個人識別情報データベース 1 1 3 に格納された情報に基づいてユーザ認証を行う。

図 5 は、個人識別情報データベース 1 1 3 の記憶内容を例示する図である。同図に示すように個人識別情報データベース 1 1 3 には、各ユーザ I D に対応付けて個人識別情報が格納されている。ここで、個人識別情報データベース 1 1 3 に

格納されているユーザIDは、ユーザがIPサーバWに自らの個人識別情報を登録する際に、IPサーバWが各ユーザに対して払い出すIDである。IPサーバWがユーザに対して提供するサービスが、例えば、「ネットバンキング」サービスである場合、このユーザIDは、当該ユーザの銀行口座を特定するために用いられる。これに対して、IPサーバWが提供するサービスがコンテンツ配信である場合、ユーザIDは、課金の為の処理に用いられる。

また、個人識別情報データベース113に対する個人識別情報やユーザIDの登録は、種々の方法で実現可能である。例えば、ユーザがIPサーバWを保有するIPのサービス窓口に出向き、移動機MSの製造番号を窓口の従業者に提示することにより、登録を行う構成としても良い。また、IP側においてSSL (Secure Sockets Layer) による通信が可能なサイトを開設し、ユーザが移動機MSを用いて当該サイトへとアクセスして個人識別情報の登録を行う構成としても構わない。かかる方法を採用する場合、当該サイトのページに対応するHTMLデータ中に、個人情報要求データ列を記述して、移動機MSに記憶されている製造番号等の個人識別情報を送信させるようにすれば良い。

データ配信管理部111から個人識別情報が送られてくると、認証部112は、その個人識別情報に基づいて個人識別情報データベース113の検索を行う。そして、当該個人識別情報と一致する情報が個人識別情報データベース113に格納されている場合、当該個人識別情報に対応したユーザIDを読み出す。そして、当該ユーザIDに従って各種サービスを提供する。これに対して、当該個人識別情報に一致する情報が個人識別情報データベース113に存在しない場合、認証部112は、当該移動機MSのユーザが正当な権限を有するユーザではないものと判定して、サービスの提供を拒絶する。

通信部114は、インターネットINETとデータ配信管理部111との間のデータの授受を仲介する。具体的には、通信部114は、インターネットINETから送られてきたデータをデータ配信管理部111に送ると共に、データ配信管理部111から送られてきたデータをインターネットINETへと送出する。

次に、移動パケット通信網MPNは、移動機MSに対してパケット通信サービ

スを提供するための通信網であり、ゲートウェイサーバGWSや複数の基地局BSを収容する他、図示せぬパケット加入者処理装置を有する。

ゲートウェイサーバGWSは、インターネットINETと、移動パケット通信網MPNとを相互接続する移動パケット関門中継交換局に設けられたコンピュータシステムであり、相異なるネットワーク間のデータの授受を仲介する。具体的には、ゲートウェイサーバGWSは、移動パケット通信網MPN側の移動機MSから送られてきたデータに対し、インターネットINETが従うTCP/IP (Transmission Control Protocol/Internet Protocol) に適合させるためのプロトコル変換を施してインターネットINET側に送信する。また、ゲートウェイサーバGWSは、インターネットINET側から送信されてきたデータを移動パケット通信網MPN用の伝送プロトコルへと変換して移動パケット通信網MPN側に送信する。

また、ゲートウェイサーバGWSは、移動機MSから送信された、HTTPのGET要求を受信すると、当該GET要求に含まれるURLを調べ、そのURLがインターネットINET上の一般的なURLである場合には、当該GET要求をインターネットINET側へ転送する。そして、このGET要求に対してインターネットINET側から返信されてきたデータを移動パケット通信網MPNに転送する。

また、ゲートウェイサーバGWSは、移動機MSから、HTTPSのGET要求を受けると、当該GET要求に含まれるURLを調べ、そのURLに対応したSSLのサイトと移動機MSが直接通信をできるようにする。

更に、ゲートウェイサーバGWSは、移動機MSからの要求に従い、例えば、ホームページやWebページ等に対応したHTMLデータを生成する。ゲートウェイサーバGWSは、このHTMLデータを移動機MSに配信することにより、移動機MSに対して各種サービスを提供する。ゲートウェイサーバGWSが移動機MSに提供するサービスとしては、例えば、IPサーバWの検索サービス等がある。この検索サービスを提供するため、ゲートウェイサーバGWSは、検索用データベースGWS1を有する。

図6は、検索用データベースGWS1の記憶内容を例示する図である。同図に示すように、検索用データベースGWS1には、IPサーバWの有する各ページのタイトルに対応付けて、検索用のキーワードと、当該ページに対応したURLが格納されている。ここで、検索用データベースGWS1に格納されているURLのうち、ユーザ認証を必要とするサービスに関連するページのURLについては、個人識別情報データ列（すなわち、「utn」）が付加されている。例えば、同図に示す例において、「〇〇銀行」や「△△銀行」なるタイトルに対応付けて格納されているURL（すなわち、「<http://www.〇〇bank.co.jp/index.html#utn>」や「<http://www.△△bank.co.jp/index.html#utn>」）がこれにあたる。

- 10 ゲートウェイサーバGWSは、移動機MSからの要求に基づいて、検索用データベースGWS1の検索を行う。そして、その検索の結果ヒットしたURLをアンカータグにより指定したHTMLデータを生成して、インターネットINETへと送出する。例えば、図6に示す場合において、「〇〇銀行」なるタイトルがヒットした場合、ゲートウェイサーバGWSは、検索用データベースからURL
- 15 「<https://www.〇〇bank.co.jp/index.html#utn>」を読み出して当該URLを含むHTMLデータを生成して移動パケット通信網MPNへと送出する。

<B. 移動機MSの構成>

図7は、本実施形態にかかる移動機MSの構成を例示するブロック図である。

- 20 同図に示すように移動機MSは、制御部21と、送受信部22と、指示入力部23と、液晶表示部24と、各要素間におけるデータの授受を仲介するバス25を有する。

送受信部22は、移動パケット通信網MPNの基地局BSとの間において無線通信を行う。

- 25 指示入力部23は、PB（プッシュボタン）等の各種ボタン及びカーソルキーからなり、ユーザによって入力操作が行われると、その入力操作に対応した操作データを制御部22のCPU211に供給する。CPU211は、この操作データからユーザの入力コマンドを判定し、同コマンドに対応した制御を行う。

液晶表示部 2 4 は、液晶パネル等の表示装置から構成されており、制御部 2 1 の制御の下に、各種情報を表示する。

制御部 2 1 は、CPU 2 1 1 と、ROM 2 1 2 と、RAM 2 1 3 と、フラッシュメモリ 2 1 4 から構成されており、移動機 MS の各部を制御する。ROM 2 1 2 には、個人識別情報としての移動機 MS の製造番号や移動機 MS の全体を制御するための制御プログラム、各種制御情報の他、他の通信装置（例えば、IPサーバ W）から所望のデータを取得して、その取得したデータに対応した画像を表示するための WWW ブラウザが記憶されている。RAM 2 1 3 は、CPU 2 1 1 のワークエリアとして用いられる。

10 CPU 2 1 1 は、ROM 2 1 2 に記憶された各種制御プログラムに従って各種処理を実行する。例えば、CPU 2 1 1 が ROM 2 1 2 に記憶された WWW ブラウザを読み出して実行するとその実行過程において次の処理が行われる。すなわち、ユーザが指示入力部 2 3 に所望の URL を指定すると、CPU 2 1 1 は、指示入力部 2 3 からの入力コマンドに基づいて、当該 URL を含む HTTP や HT
15 T P S の G E T 要求を移動パケット通信網 M P N に送出するための処理を行う。

また、この際、指示入力部 2 3 から指定された URL に個人識別情報要求データ列「utn」が付加されていることがある。かかる場合に、CPU 2 1 1 は、ROM 2 1 2 に格納された個人識別情報（製造番号）を読み出して、この個人識別情報要求データ列「utn」を付加した G E T 要求を送信する。そして、当該 G E
20 T 要求に対応した HTML データが IP サーバ W やゲートウェイサーバ G W S から返信されてくると、CPU 2 1 1 は、当該 HTML データを RAM 2 1 3 に書き込むと共に、当該 HTML データに対応した画像を液晶表示部 2 4 に表示させる。

フラッシュメモリ 2 1 4 には、アクセス先の履歴を登録するため、図 8 に示す
25 ような履歴格納テーブル T B L が設けられている。同図に示すように、履歴格納テーブル T B L には、ユーザが移動機 M S を用いて実際にアクセスしたリソースの URL がアクセス履歴として格納されている（以下、このアクセス履歴としての URL を「履歴 URL」という）。また、各履歴 URL に対応付けて、当該 U

R Lに個人識別情報要求データ列「utn」が付加されていたか否かを示す要求データ列フラグFが格納されている。この要求データ列フラグFが“1”である場合には当該URLには要求データ列が付加されていたことを示し、“0”である場合には要求データ列が付加されていなかったことを示している。

- 5 移動機MSがIPサーバWからHTMLデータのダウンロードに失敗し、当該HTMLデータを再度ダウンロードすることがある。かかる場合に、移動機MSは、この履歴格納テーブルTBL中の要求データ列フラグFを読み出し、個人識別情報を送信するか否かを決定する。具体的には、再度読み込むページに対応したURLの要求データ列フラグFが“1”の場合、制御部21は、IPサーバW
10 に対して個人識別情報を付加してGET要求を送信する。これに対して、要求データ列フラグFが“0”である場合、制御部21は、個人識別情報を付加することなく、単に当該ページに対応したURLを含むGET要求を送信する。

<1-2. 実施形態の動作>

- 15 以下、図面を参照して、本実施形態にかかる通信システムの動作について説明する。なお、以下の説明においては、説明をより具体的なものとするため、個人識別情報データベース113及び検索用データベースGWS1の記憶内容は、図5及び図6に示したものと同一であるものとし、移動機MSの製造番号は「△△△△△△△△」であるものとする。

- 20 まず、外出先において自分のアパートの家賃の振り込みを忘れていたことに気がついたユーザは、ゲートウェイサーバGWSの検索サービスを利用して自分が口座を開設している「〇〇銀行」のホームページを検索し、「ネットバンキング」サービスを受けるべく、移動機MSの指示入力部23に対して、ブラウジングを行う旨の入力を行う。この指示入力部23に対する入力に従い、CPU21
25 1は、ROM212からWWWブラウザを読み出して、パケット加入者処理装置（図示は省略）に対してパケット登録を行う。このパケット登録とは、移動機MSが移動パケット通信網MPNとの間においてパケット交換を行うための登録手続きである。このようにして、パケット登録が行われると、移動機MSは、ゲー

トウェイサーバGWSとの間で、パケット交換を行うことが可能となる。

その後、ユーザが移動機MSの指示入力部23に対して、ゲートウェイサーバGWSの検索サービスに対応したURLを入力すると、移動機MSは、当該URLを含むGET要求を移動パケット通信網MPNへと送信する。ゲートウェイサーバGWSは、このGET要求を受信すると検索画面に対応したHTMLデータ
5 移動パケット通信網MPNに送出する。なお、この検索画面の構成は、任意であるが、本実施形態においては、図9に示すように、「キーワード」なる文字列の下にあるボックスの部分に検索用の文字列を入力する構成となっている。

次に、この検索画面に対応したHTMLデータは、移動機MSの送受信部22
10 によって受信され、CPU211へと送られる。この結果、当該HTMLデータに対応した検索画面（図9参照）が液晶表示部24に表示される。この状態において、ユーザは、移動機MSの指示入力部23に対して、自分の検索したいサービスに対応した検索用文字列（すなわち、「ネットバンキング」なる検索用文字列）を入力して、決定を行う旨の入力操作を行う。この結果、移動機MSのCPU211は、当該文字列を付加したGET要求を移動パケット通信網MPNに送出する。
15

そして、このGET要求がゲートウェイサーバGWSによって受信されると、ゲートウェイサーバGWSは、当該GET要求に含まれている検索用文字列（すなわち、「ネットバンキング」なる検索用文字列）を抽出する。ゲートウェイサーバGWSは、この「ネットバンキング」なる検索用文字列に基づき、検索用データベースGWS1の検索を行う。この結果、検索用データベースGWS1において「ネットバンキング」なるキーワードに基づいて「〇〇銀行」や「△△銀行」に対応したURLがヒットする（図6参照）。
20

次に、ゲートウェイサーバGWSは、これら「〇〇銀行」や「△△銀行」に対応するURL「https://www.〇〇bank.co.jp /index.html#utn」や「http://www.△△bank.co.jp /index.html#utn」を検索用データベースGWS1から読み出す。ここで、「ネットバンキング」は、上述したようにセキュリティを必要とするサービスであるため、これらのサービスに関連するページのURLには、個人
25

識別情報要求データ列「utn」が含まれている。そして、ゲートウェイサーバGWSは、検索用データベースGWS1から読み出した「〇〇銀行」や「△△銀行」に対応するURLをアンカータグにより指定したHTMLデータを生成して、移動パケット通信網MPNへと送出する。

- 5 次に、このHTMLデータは、移動機MSの送受信部22によって受信され、CPU211へと送られる。CPU211は、この送られてきたHTMLデータに対応した画像を液晶表示部24に表示させる。この結果、移動機MSの液晶表示部24には、図10に示すように、ゲートウェイサーバGWSにおける検索の結果、ヒットしたタイトル（例えば、「〇〇銀行」や「△△銀行」等）がメニュー項目として表示される。

この状態において、ユーザが移動機MSの指示入力部23に対して、自分が口座を有している銀行名に対応したメニュー項目（すなわち、「〇〇銀行」）を選択する入力操作を行うと、当該メニュー項目に対応した文字列が反転表示される。この反転表示されている状態において、ユーザが指示入力部23に決定を行う旨の入力操作を行うと、移動機MSのCPU211は、図11に示す処理を実行する。

この処理において、CPU211は、まず、選択されたメニュー項目「〇〇銀行」に対応したURL「<https://www.〇〇bank.co.jp/index.html#utn>」を抽出し、当該URLに個人識別情報要求データ列（すなわち、「utn」）が含まれているか否かを判定する（ステップS1、S2）。

そして、抽出したURLに個人情報要求データ列が含まれていない場合（ステップS2「No」）、CPU211は、当該URLがSSLによる通信を指定しているか否かを判断する（ステップS9）。この際、CPU211は、当該URLが「http」で始まるものか、「https」で始まるものかによって、当該URLがSSLによる通信を指定しているか否かを判定する。そして、当該URLがSSLによる通信を指定している場合（ステップS9「Yes」）、CPU211は、SSLによる通信を開始するための処理を実行し（ステップS10）、GET要求を送信する（ステップS11）。これに対して、当該URLがSSLによ

る通信を指定しない場合（ステップs 9「No」）、CPU 211は、SSLの
ハンドシェイクを確立することなくGET要求を送信する（ステップS 11）。
そして、CPU 211は、フラッシュメモリ 214の履歴格納テーブルTBLに
対して当該URLをアクセス履歴として格納すると共に、要求データ列フラグF
5 として“0”を格納する（ステップS 12）。

なお、この際における処理の違いについては、後に詳細に説明する。

一方、今の場合、メニュー項目「〇〇銀行」が選択されている。このため、C
PU 211によって抽出されるURLには、個人情報要求データ列が含まれてい
る（ステップS 2「Yes」）。かかる場合に、CPU 211は、図12に示す
10 ような画面を液晶表示部24上に表示させる（ステップS 3）。すなわち、移動
機MSの液晶表示部24上には、「個人識別情報が要求されています。送信しま
すか？」等のユーザの判断を促す文字と共に、「Yes」と「No」のボタンが
表示されるのである。この状態において、ユーザが「No」ボタンを選択した場
合、CPU 211は、ステップS 4において「No」と判定し、処理を終了す
15 る。

これに対して、ユーザが「Yes」を選択する入力操作を行うと、CPU 21
1は、ステップS 4において「Yes」と判定し、ステップS 1において抽出し
たURLがSSLによる通信を指定しているか否かを判定する（ステップS
5）。この際、CPU 211は、当該URLが「http」で始まるものか、「http
20 s」で始まるものかによって、当該URLがSSLによる通信を指定しているか
否かを判定する。そして、このステップS 5における判断の結果によって、通信
システム1においては、以下のような2つの異なる処理が実行される。

（i）処理1

この処理は、当該URLがSSLによる通信を指定しているものと判定された
25 場合（すなわち、ステップS 5「Yes」の場合）に行われる処理である。例え
ば、メニュー項目「〇〇銀行」に対応したURL「https://www.〇〇bank.co.jp
/index.html#utn」のように「https」から始まっているURLが指定された場
合には、この処理1が実行されることとなる。

この処理1においては、CPU 211によって、SSLによる通信を開始するための処理が実行される結果（ステップS6）、通信システム1においては、図13に示すようなデータの授受が行われる。この過程においては、まず、移動機MSのCPU 211が「connect」信号DS1を送受信部22を介してゲートウェイサーバGWSへと送信する。この信号DS1が受信されると、ゲートウェイサーバGWSは、IPサーバWに対して、「TCP Connect」信号DS2を送信する。このようにして、IPサーバWに対する信号DS2の送信が終了すると、ゲートウェイサーバGWSは、移動機MSに対して「Connection established」信号DS3を送信する。

10 一方、この「Connection established」信号DS3を受信すると、移動機MSのCPU 211は、IPサーバWに対して「Client hello」信号DS4を送信する。このようにして、移動機MSから送信された「Client hello」信号DS4がIPサーバWの通信部114によって受信されると、データ配信管理部111は、「Server hello」信号DS5を移動機MSに送信する。以上説明した信号DS1～DS5の授受が行われることにより、移動機MSとIPサーバWの間でSSLのハンドシェイクが行われ、移動機MSとIPサーバWとの間においてエンドトゥエンドのSSL通信が可能となる。

次に、移動機MSのCPU 211は、ステップS7を実行して、メニュー項目「〇〇銀行」に対応したURL「https://www.〇〇bank.co.jp /index.html」を含むGET要求DS6に対し、個人識別情報（すなわち、製造番号）「△△△△△△」を付加して移動パケット通信網MPNに送出する（ステップS7）。そして、CPU 211は、フラッシュメモリ214の履歴格納テーブルTBLに対して当該URL「http://www.〇〇bank.co.jp /index.html」をアクセス履歴として格納すると共に、要求データ列フラグFとして“1”を格納する（ステップS8）。

一方、移動機MSから送信されてきたGET要求DS6がIPサーバWの通信部114によって受信されると、データ配信管理部111は、このGET要求DS6に付加されているURL「https://www.〇〇bank.co.jp /index.html」を抽

出して、RAMに格納する。次に、データ配信管理部111は、RAMに格納したURLに基づいて、移動機MSのユーザの所望するサービスがユーザ認証を必要とするものであるか否かを判定する。そして、この判定の結果、ユーザ認証の必要がないと判定した場合、データ配信管理部111は、RAMに格納したURL
5 Lに対応するHTMLデータを返信して、処理を終了する。

これに対して、今の例の場合、移動機MSのユーザが所望しているサービスは、「ネットバンキング」サービスである。このため、かかる判定において、データ配信管理部111は、ユーザ認証が必要であるものと判定し、当該GET要求DS6に付加されてきた個人識別情報「△△△△△△」を抽出して、認証部1
10 12へと送る。このようにして、データ配信管理部111から個人識別情報が送られてくると、認証部112は、この個人識別情報「△△△△△△」を検索キーとして、個人識別情報データベース113を検索する。そして、この検索の結果、個人識別情報「△△△△△△」がヒットしない場合、認証部112は、GET要求DS6の送信元である移動機MSのユーザが正当なユーザではないものと
15 みなして、データ配信管理部111へと処理を終了する旨の命令を送る。

一方、図5に示す場合、個人識別情報データベース113には、個人識別情報「△△△△△△」が格納されている。かかる場合に、認証部112は、個人識別情報データベース113から個人識別情報「△△△△△△」に対応したユーザID「user.a」を読み出して、データ配信管理部111に送る。そして、データ配
20 信管理部111は、当該移動機MSのユーザが正当なユーザであるものと判定して、RAMに格納していたURL「https://www.〇〇bank.co.jp /index.html」に対応したHTMLデータDS7をインターネットINETへと送出するのである。

(ii) 処理2

25 この処理は、当該URLがSSLによる通信を指定していないと判定された場合（すなわち、ステップS5「No」の場合）に行われるものである。移動機MSのCPU221がこの処理2を実行すると、通信システム1においては、図14に示すようなデータの授受が行われる。例えば、メニュー項目「△△銀行」に

対応したURL「http://www.△△bank.co.jp /index.html#utn」のように「http」から始まっているURLが指定された場合には、この処理2が実行される。

この処理2において、CPU211は、メニュー項目「△△銀行」に対応したURL「http://www. △△bank.co.jp /index.html#utn」を含むGET要求D1
5 に対し、個人識別情報（すなわち、製造番号）「△△△△△△」を付加して移動
パケット通信網MPNに送出する（ステップS7）。次に、CPU211は、フ
ラッシュメモリ214の履歴格納テーブルTBLに対して当該URL「http://w
ww.△△bank.co.jp /index.html」をアクセス履歴として格納すると共に、要求
データ列フラグFとして“1”を格納する（ステップS8）。このようにして、
10 移動機MSから送出されたGET要求D1は、その後、ゲートウェイサーバGWS
によって受信され、プロトコル変換され、GET要求D2としてインターネッ
トINETへと転送される。

次に、GET要求D2が通信部114によって受信されると、データ配信管理
部111においては、上述した処理1と同様の処理が実行されて、URL「”htt
15 p://www.△△bank.co.jp /index.html”」に対応したHTMLデータD3がインター
ネットINETへと送出され、ゲートウェイサーバGWSによりHTMLデー
タD4として転送される。

以上説明した処理1或いは処理2を経て送信されたHTMLデータD4或いは
DS7が、移動機MSによって受信されると、移動機MSの液晶表示部24に
20 は、図15に示すような画面が表示される。ここで、同図に示す各メニュー項目
には、当該メニュー項目に対応したサービスの提供を受けるためのページへとジ
ャンプするためのURLが対応付けられている。なお、これら各メニュー項目に
対応付けられるURLとして、個人識別情報要求データ列「utn」の付加された
URLを利用するか否かは、任意である。更なるユーザ認証を必要とする場合に
25 は、個人識別情報要求データ列「utn」の付加されたURLを利用すれば良く、
ユーザ認証を必要としない場合には、個人識別情報要求データ列「utn」の付加
されていないURLを利用すれば良い。

この状態において、家賃を振り込もうとするユーザが移動機MSの指示入力部

2 3 に対して「銀行振込」を選択する入力操作を行う。すると、移動機MSにおいては、上述した図11と同様の処理が実行され、「銀行振込」に対応したURLを含むGET要求に対して、個人識別情報「△△△△△△」を付加して移動パケット通信網MPNに送出する。なお、この際、当該メニュー項目に対応したURLがSSLによる通信を指定しているか否かによって、上述した処理1 或いは

5 処理2の何れかの処理と同様の処理が実行される。

そして、IPサーバWから当該GET要求に対応したHTMLデータが送信されてくると、移動機MSの液晶表示部24には、図16に示すような銀行振込用の画面が表示される。その後、ユーザが振込先の口座番号と、家賃に対応した金額等を入力して決定を行う旨の入力操作を行う。すると、移動機MSは、これらの情報と、個人識別情報「△△△△△△」を含むGET要求を送信する。このようにして、移動機MSからGET要求が送信されてくると、IPサーバWは、受信したGET要求から各種情報を抽出して、銀行振込を行う。

これに対して、移動機MSが図16の画面に対応したHTMLデータのダウンロード中に通信状態が悪化し、当該HTMLデータのダウンロードに失敗した場合、移動機MSは、再度、図16の画面に対応したHTMLデータをダウンロードすることが必要となる。かかる場合に、移動機MSは、履歴格納テーブルTBL中の要求データ列フラグFを読み出す。そして、要求データ列フラグFが”0”であるか”1”であるかによって、以下のように処理を変更する。

20 (a) 要求データ列フラグF=”1”のとき

この場合、移動機MSのCPU211は、再読込を行う画面に対応したGET要求を送信するにあたり、当該GET要求に個人識別情報「△△△△△△」を付加して送信する。例えば、上述した図10のメニュー項目「〇〇銀行」や「△△銀行」に対応したURLのように、URLに個人情報送信要求データ列「utn」が付加されている場合、上述した図11ステップS8における処理の結果、移動機MSの履歴格納テーブルTBLには、要求データ列フラグFとして“1”が格納されている。この場合、当該画面に対応したHTMLデータの再読み込みの際、移動機MSのCPU211は、IPサーバWに対して個人識別情報を付加し

25

てGET要求を送信する。この結果、移動機MSの液晶表示部24には、図16に示す画面が表示される。そして、同様にして「銀行振込」等のサービスが提供される。

(b) 要求データ列フラグF="0" のとき

5 この場合、移動機MSのCPU211は、再読込を行う画面に対応したURLを含むGET要求を送信するにあたり、当該GET要求に個人識別情報「△△△△△△」を付加することはない。

以上、ユーザが銀行振込を行う場合を例に本実施形態の動作を説明したが、移動機MSのユーザがIPサーバWから登録制のサービスを受ける際も全く同様の
10 処理が通信システム1において行われることとなる。

このようにして、本実施形態にかかるユーザ認証方法によれば、HTMLデータ中のURLに個人識別情報要求データ列が付加されている場合に、移動機がユーザの承諾を得て個人識別情報をIPサーバへ送信し、IPサーバが個人識別情報に基づいてユーザ認証を行う構成となっている。このため、移動通信事業者と
15 の間において特別な契約を結ぶことなく、全てのIPにおいて個人識別情報を利用したユーザ認証を行うことが可能となる。

また、本実施形態にかかる移動機は、個人識別情報を送信するにあたり、ユーザの承認を得るための画像を液晶表示部に表示して、ユーザの承諾が得られた場合にのみ個人識別情報を送信する構成としている。このため、ユーザが意図しない
20 い場合にまで個人識別情報が送信されてしまい、当該個人識別情報が不正使用されてしまうことを有効に防止することが可能となる。

また、本実施形態においては、ゲートウェイサーバの検索サービスを利用した場合でも、ユーザ認証を必要とするサービスを提供するページのURLには個人識別情報要求データ列が付加されて送信される。このため、検索サービスを利用
25 して、IPサーバにアクセスした場合でも、確実に個人識別情報を付加したGET要求が送信されるため、より確実にユーザ認証を行うことが可能となる。

更には、本実施形態においては、IPサーバ等から送信されるデータの形式として、HTML形式のデータを用いているため、既存の設備を用いて、本発明の

効果を奏することが可能となる。

なお、本実施形態においては、個人識別情報に用いるユニークな情報として移動機MSの製造番号を用いる構成について説明したが、当然移動機MSの電話番号等の情報を用いても良い。

- 5 なお、本実施形態においては、個人識別情報として、データ列「utn」を用いたが、当然他のデータ列を用いるようにしても良い。

 なお、本実施形態においては、移動機MSが移動パケット通信網MPNを介して通信を行う場合について説明した。しかし、本発明は、これに限らず、固定電話網に収容された、パーソナルコンピュータ等の端末を用いて通信を行う場合に
10 も適用可能である。この場合、パーソナルコンピュータに上記実施形態の移動機MSと同様の機能を持たせることにより、上記実施形態と同様の処理を実行することが可能である。

 なお、本実施形態においてIPサーバWやゲートウェイサーバGWSから移動機MSに送信されるデータは、HTML形式のデータであるものとして説明を行っている。しかし、本発明は、これに限らず、XML (eXtensive Markup Language) 等の他のマークアップ言語を用いても構わない。
15

< 1 - 3. 変形例 >

< 変形例 1 >

- 20 本実施形態においては、ゲートウェイサーバGWSに検索機能を設けて、移動機MSに対して検索サービスを提供する構成としている。しかし、検索サービスの提供元は、ゲートウェイサーバGWSではなく、インターネットINET上の検索エンジンとしても良い。この場合、検索エンジンに検索用のデータベースを持たせることにより、本実施形態と同様の効果を奏することが可能となる。

25

< 変形例 2 >

 本実施形態においては、ゲートウェイサーバGWSが移動機MSから送られてきたキーワードに従って、検索用データベースの検索を行う構成としている。し

かし、ゲートウェイサーバGWSが移動機MSに対して各種サービスを紹介する方法は、他の方法であっても良い。例えば、ゲートウェイサーバGWSのホームページ上に「ネットバンキング」や「ゲーム」等の各種サービスに対応したメニュー項目を設け、各メニュー項目毎に対応したページを作成する構成としても良い。この場合、この各メニュー項目毎に対応したページ中に、例えば、「〇〇銀行」等のメニュー項目を設ける。そして、当該メニュー項目に対応したURLをアンカータグにより指定する際に個人識別情報要求データ列「utn」を付加する。このような構成とすれば、本実施形態と同様に移動機MSのユーザが、ゲートウェイサーバGWS上で所望のサイトを見つけだすことが可能となる。

10

＜変形例3＞

本実施形態においてIPサーバWは、移動機MSから送信されてきた個人識別情報のみに従って、ユーザ認証を行う構成となっている。しかし、より確実なユーザ認証を行うために他の情報を併用する構成としても構わない。例えば、以下

15

i) 方法a

この方法は、個人識別情報に基づいてユーザ認証を行った後に、ユーザにパスワードを入力させる方法である。

この方法を採用する場合、IPサーバWの個人識別情報データベース113の記憶内容を図17のように変更する。すなわち、各ユーザIDに対応付けて、個人識別情報と、パスワードを格納する。ここで、このパスワードは、IPと移動機MSのユーザがサービスの提供契約を結んだ際に、IPによって払い出されるパスワードである。

そして、IPサーバWのデータ配信管理部111は、移動機MSから個人識別情報を付加したGET要求DS6或いはD2（図13、図14）が送信されてくると、当該GET要求DS6或いはD2に付加されたURLを抽出してRAMに格納すると共に、当該GET要求DS6或いはD2から個人識別情報を抽出して認証部112に送る。認証部112は、この個人識別情報に基づいて個人識別情

25

報データベース 113 を検索し、当該個人識別情報に対応したユーザ ID を読み出して、データ配信管理部 111 に送る。

そして、認証部 112 からユーザ ID が送られてくると、データ配信管理部 111 は、当該ユーザ ID を RAM に格納すると共に、図 18 に示すようなパスワード等を入力するための画面（以下、「パスワード入力画面」という）に対応した HTML データをインターネット I N E T へと送出する。

この HTML データが移動機 MS によって受信され、液晶表示部 24 上に図 18 に示すパスワード入力画面が表示されている状況で、移動機 MS の指示入力部 23 にパスワードとユーザ ID を入力し、決定を行う旨の入力操作を行うと、移動機 MS の制御部 21 は、移動パケット通信網 MPN に対して、当該パスワード等を含む GET 要求を送出する。IP サーバ W のデータ配信管理部 111 は、この GET 要求を受信すると、当該 GET 要求からパスワードとユーザ ID を抽出し、認証部 112 へと送る。

認証部 112 は、データ配信管理部 111 から送られてきたユーザ ID に対応したパスワードを個人識別情報データベース 113 から読み出す。そして、認証部 112 は、読み出したパスワードと、データ配信管理部 111 から送信されてきたパスワードの一致を判定し、その認証結果をデータ配信管理部 111 に送る。次に、データ配信管理部 111 は、このユーザ認証の結果、当該ユーザが正当なユーザであるものと判断した場合にのみサービスを提供する。

なお、この場合、IP サーバ W が提供するサービス毎に、セキュリティを確保する必要性に従い、認証方法を変更しても構わないし、個人識別情報によるユーザ認証のみにしても構わない。また、パスワードの代わりに、指紋情報等のバイオメトリックス情報を送信する構成としても良い。

ii) 方法 b

この方法は、移動機 MS が個人識別情報を送信する際に、ユーザにユーザ ID の入力を促し、ユーザが入力したユーザ ID と個人識別情報を IP サーバ W に送信することにより、ユーザ認証を行う方法である。

この場合、上述した図 11 のステップ S3 において移動機 MS の液晶表示部 2

4に表示される画面（図12）に対して、ユーザIDを入力するボックスを追加する。図19は、この際に移動機MSの液晶表示部24に表示される画面の一例を示した図である。ここで、同図に示す画面が表示されている状態において、ユーザが自らのユーザIDを入力し、送信ボタンを選択する入力操作を行うと、移動機MSの制御部21は、入力されたユーザIDと個人識別情報を付加したGET要求DS6
5 あるいはD2（図13、図14）を移動パケット通信網MPNに送信する。

一方、IPサーバWにおいては、データ配信管理部111が当該GET要求DS6
10 あるいはD2から個人識別情報とユーザIDを抽出して認証部112へと送り、認証部112がこれらの情報に基づいてユーザ認証を行う。具体的には、認証部112は、データ配信管理部111から送られてきたユーザIDに対応した個人識別情報を個人識別情報データベース113から読み出し、当該個人識別情報と、データ配信管理部111から送られてきた個人識別情報の一致を判定する。そして、認証部112は、その認証結果をデータ配信管理部111に送る。
15 データ配信管理部111は、このユーザ認証の結果、当該ユーザが正当なユーザであるものと判断した場合にのみサービスを提供するのである。

このように、個人識別情報によるユーザ認証のみならず、他の認証方法を併用することにより、ユーザ認証の確実性を担保することが可能となる。特に、「ネットバンキング」のような、ユーザの財産に関するサービスについては、その提供にあたり、個人識別情報によるユーザ認証のみならず、他の認証方法を併用することによる効果は非常に大きなものとなる。
20

<変形例4>

図20は、本変形例にかかる移動機MS2の構成を示したブロック図である。
25 なお、同図において、上述した図7と同様の要素については、同一の符号を付してある。

本変形例において特徴的な構成として移動機MS2は、UIM（User Identity Module）2000を接続するためのUIMインターフェイス部26（以下、

「インターフェイス」を「I/F」と略称する)を有し、UIM2000と接続された状態で使用される。ここで、UIM2000は、ユーザの加入者番号等のユーザ固有の情報を有したモジュールである。移動機MS2の制御部21は、UIM I/F部26によりUIM2000とデータの授受を行い、移動パケット通信網MPNのパケット交換サービスを受ける。また、本変形例においては、移動パケット通信網MPNにおけるパケット交換サービスの提供を受ける際に、例えば、GSM(Global System for Mobile Communications)におけるSIMのように各UIM2000単位で加入者番号が発行され、課金も各UIM2000単位で行われる。

次に、UIM2000についてより詳細に説明を行う。図21は、UIM2000の構成を示すブロック図である。同図に示すように、UIM2000は、CPU2001と、外部I/F部2002と、ROM2003と、RAM2004と、EEPROM2005とを有する。

外部I/F部2002は、CPU2001と移動機MS2のUIM I/F部26との間のデータの授受を仲介する。ROM2003は、不揮発性のメモリであり、制御プログラムの他、移動機MS2から供給される制御コマンドの解析、実行、応答、データ管理等を行うためのプログラムが記憶されている。CPU2001は、ROM2003に格納されているプログラムを実行することによりUIM2000の各部を制御する。RAM2004は、CPU2001のワークエリアとして用いられる。EEPROM2005には、ユーザの加入者情報等のユーザ固有の情報、UIM2000の製造番号等の情報が格納されている。

ここで、IPサーバWが移動機MS2に対して提供するサービスの中には、キャラクターコンテンツや、音楽コンテンツ等を配信するものが存在する。これらのサービスにおいては、コンテンツ単位で課金が行われるため、再度同一のユーザからの配信要求がなされ場合に課金を行わないことが多い。このため、本変形例のようにUIM2000単位で課金を行う通信システムにおいては、同一のUIM2000を用いることにより、一回の課金で複数の移動機MS2に同一コンテンツをダウンロードするという不正使用が可能となってしまう。そこで、本変

形例においては、個人識別情報として、移動機MS 2の製造番号のみならず、UIM 2000に固有のユニークな情報（本変形例においては、「UIM 2000の製造番号」）を用いることによりユーザ認証を行う構成となっている。

以下、本変形例の動作において、上述した実施形態と異なる部分について説明する。

まず、本変形例において移動機MS 2においては、図11ステップS1～S6と同様の処理が実行される。そして、図11ステップS7において移動機MS 2がGET要求を送信する際に、CPU 211は、UIM 2000に対して、当該UIM 2000の製造番号の送信要求を行う。UIM 2000のCPU 2001は、移動機MS 2から、製造番号の送信要求が送られてくると、EEPROM 2005から自らの製造番号を読み出して、外部I/F部2002を介して移動機MS 2へと送る。

そして、移動機MS 2のCPU 211は、ROM 212から読み出した移動機MS 2の製造番号と共に、このUIM 2000から取得したUIMの製造番号を個人識別情報として付加したGET要求を移動パケット通信網MPNへと送出する。IPサーバWは、このGET要求に付加された移動機MS 2の製造番号と、UIM 2000の製造番号に基づいてユーザ認証を行う。

これに伴い、IPサーバWの個人識別情報データベース113は、図22に示すように、その記憶内容が変更されている。すなわち、各ユーザIDに対応付けて、個人識別情報としての移動機MS 2の製造番号とUIMの製造番号が格納されている。認証部112は、移動機MS 2から送られてきた2つの製造番号と、個人識別情報データベース113に格納されている情報との一致を判定し、一致する場合に認証成功とする。

このようにして、本変形例によれば、移動機の製造番号のみならずUIMの製造番号をも個人識別情報として用いてユーザ認証を行う構成としている。このため、移動機単位で課金が行われる場合のみならず、UIM等のモジュール単位で課金が行われるシステムにおいても、簡易かつ確実なユーザ認証を行うことが可能となると共に、認証の正当性を確保することが可能となる。

請 求 の 範 囲

1. 第1のネットワークに収容された携帯端末が、前記第1のネットワークからデータを受信する受信過程と、

5 前記携帯端末が前記受信過程において受信したデータ中に所定のデータ列が存在するか否かを検出する検出過程と、

前記検出過程において前記データ列が存在するものと検出された場合にのみ、前記携帯端末が、予め自端末に記憶されているユーザを一意に特定するための個人識別情報を送信する送信過程と、

10 前記第1のネットワークと第2のネットワークとの間のデータの授受を中継する中継装置が、前記携帯端末から送信された個人識別情報を前記第2のネットワークへと転送する転送過程と、

前記第2のネットワークに接続されたサーバが、前記個人識別情報に基づいて前記携帯端末のユーザを認証する認証過程と

15 を具備することを特徴とするユーザ認証方法。

2. 前記送信過程において前記携帯端末は、

前記サーバ以外の装置によって解読不能な形式により前記個人識別情報を送信し、

20 前記認証過程において前記サーバは、

前記個人識別情報を解読し、当該個人識別情報に基づいて前記携帯端末のユーザを認証する

ことを特徴とする請求項1に記載のユーザ認証方法。

25 3. 前記中継装置が前記携帯端末からの要求に従い、前記第2のネットワークにおける前記サーバのアドレスを検索する検索過程を更に有し、

前記受信過程において前記携帯端末が受信する前記データは、前記検索過程において、前記中継装置が検索した検索結果に対応したデータである

ことを特徴とする請求項 1 に記載のユーザ認証方法。

4. 前記データは、マークアップ言語により記述されており、
前記データ列は、前記データ内に含まれる所定の識別子である

5 ことを特徴とする請求項 1 に記載のユーザ認証方法。

5. 前記検出過程において前記データ列が存在するものと検出された場合にのみ、前記携帯端末が自端末のユーザに対して、前記個人識別情報の送信の可否について判断を促す判断促進過程を更に有し、

10 前記送信過程において前記携帯端末は、前記判断促進過程において該ユーザの許可が得られた場合にのみ、前記個人識別情報を送信する
ことを特徴とする請求項 1 に記載のユーザ認証方法。

6. 前記判断促進過程において前記携帯端末は、

15 ユーザの判断を仰ぐための画像を表示すると共に、ユーザに対して入力識別情報の入力を促し、

前記送信過程において前記携帯端末は、前記個人識別情報と共に、ユーザの入力した入力識別情報を送信し、

前記認証過程において前記サーバは、前記送信過程において送信された個人識別情報と、前記入力識別情報に基づいてユーザ認証を行う
20 ことを特徴とする請求項 5 に記載のユーザ認証方法。

7. 前記認証過程の後に、前記サーバが前記携帯端末に対して入力識別情報の入力を促す入力データを配信する配信過程と、

25 前記配信過程において配信された前記入力データを受信した前記携帯端末が当該入力データに基づきユーザに対して前記入力識別情報の入力を促す過程と、

前記入力を促す過程において入力された入力識別情報を送信する第 2 の送信過程と、

前記第 2 の送信過程において送信された前記入力識別情報に基づいて前記携帯端末のユーザを認証する第 2 の認証過程と

を更に有することを特徴とする請求項 1 に記載のユーザ認証方法。

5 8. 前記個人識別情報は、前記携帯端末の製造番号であることを特徴とする請求項 1 に記載のユーザ認証方法。

9. 前記個人識別情報は、前記携帯端末の製造番号と、前記携帯端末に接続されたユーザ識別モジュールに格納された情報との組み合わせにより構成されてい

10 ることを特徴とする請求項 1 に記載のユーザ認証方法。

10. 前記第 1 のネットワークは、移動通信網であり、

前記携帯端末は、前記移動通信網を介して通信を行う移動機である

ことを特徴とする請求項 1 に記載のユーザ認証方法。

15

11. 第 1 のネットワークからデータを受信し、当該データ中に所定のデータ列が存在するか否かを検出して、前記データ列が存在するものと検出された場合にのみ、予め自端末に記憶されているユーザを一意に特定するための個人識別情報を前記第 1 のネットワークに送信する携帯端末と、

20 前記第 1 のネットワークと中継装置を介して相互接続された第 2 のネットワークと、

前記第 2 のネットワークに接続され、前記個人識別情報に基づいて認証を行うサーバと

を具備することを特徴とする通信システム。

25

12. 第 1 のネットワークを介して他者との通信を行う通信部と、

前記通信部により前記第 1 のネットワークおよびこれに接続された第 2 のネットワークを介して、該第 2 のネットワーク内のサーバと通信を行い、該サーバか

ら所定のデータ列を含むデータを受け取ったとき、当該携帯端末に備えられたメモリまたは当該携帯端末に接続されたメモリから個人識別情報を読み出し、前記コネクションを介して前記サーバに送信する制御部と

を具備することを特徴とする携帯端末。

5

13. 通信部により第1のネットワークおよびこれに接続された第2のネットワークを介して、該第2のネットワーク内のサーバと通信を行い、該サーバから所定のデータ列を含むデータを受け取ったとき、携帯端末に備えられたメモリまたは当該携帯端末に接続されたメモリから個人識別情報を読み出し、前記通信部

10 により前記サーバに送信する処理をコンピュータに実行させるプログラム。

14. 通信部により第1のネットワークおよびこれに接続された第2のネットワークを介して、該第2のネットワーク内のサーバと通信を行い、該サーバから所定のデータ列を含むデータを受け取ったとき、携帯端末に備えられたメモリま

15 たは当該携帯端末に接続されたメモリから個人識別情報を読み出し、前記通信部により前記サーバに送信する処理をコンピュータに実行させるプログラムを記憶した記録媒体。

図 1

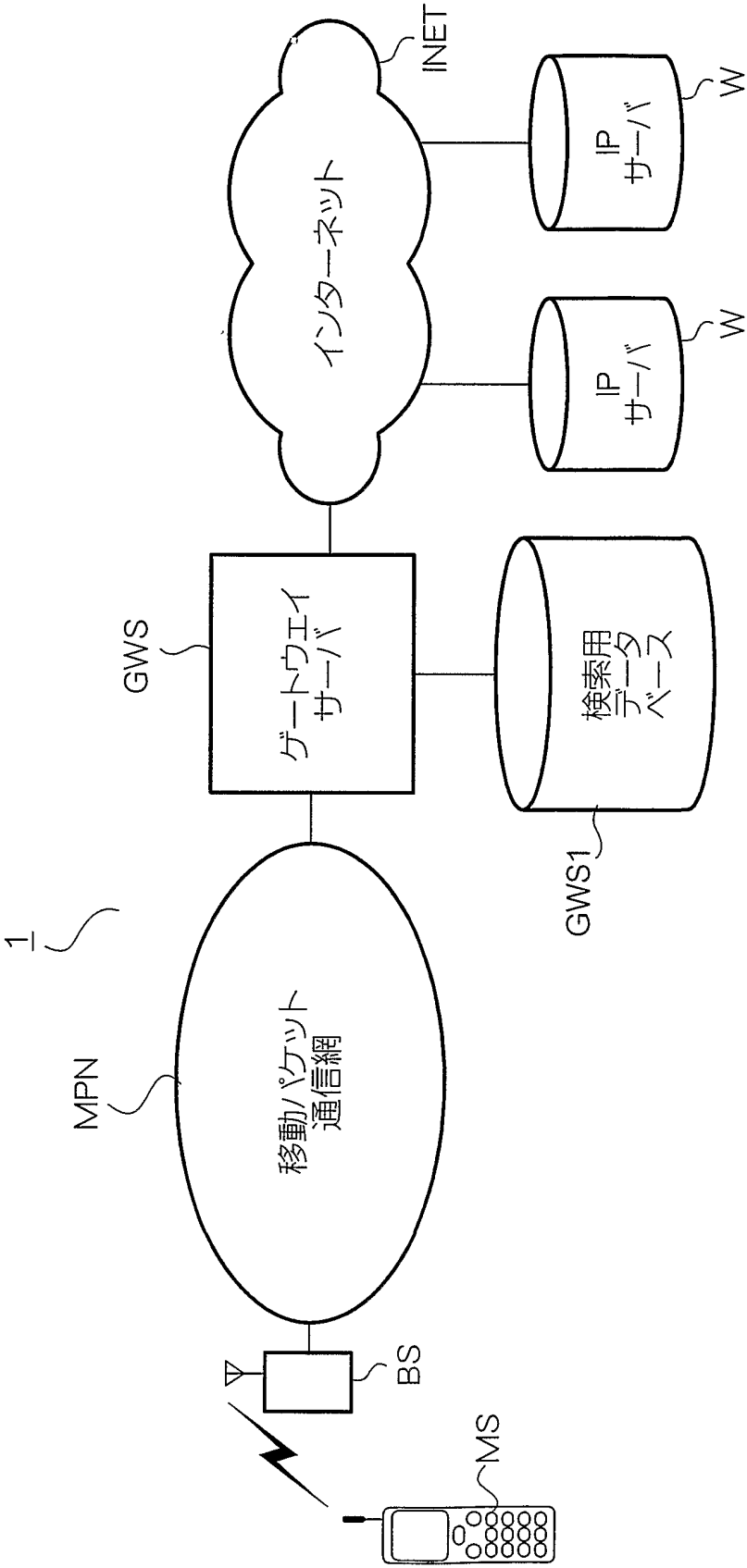
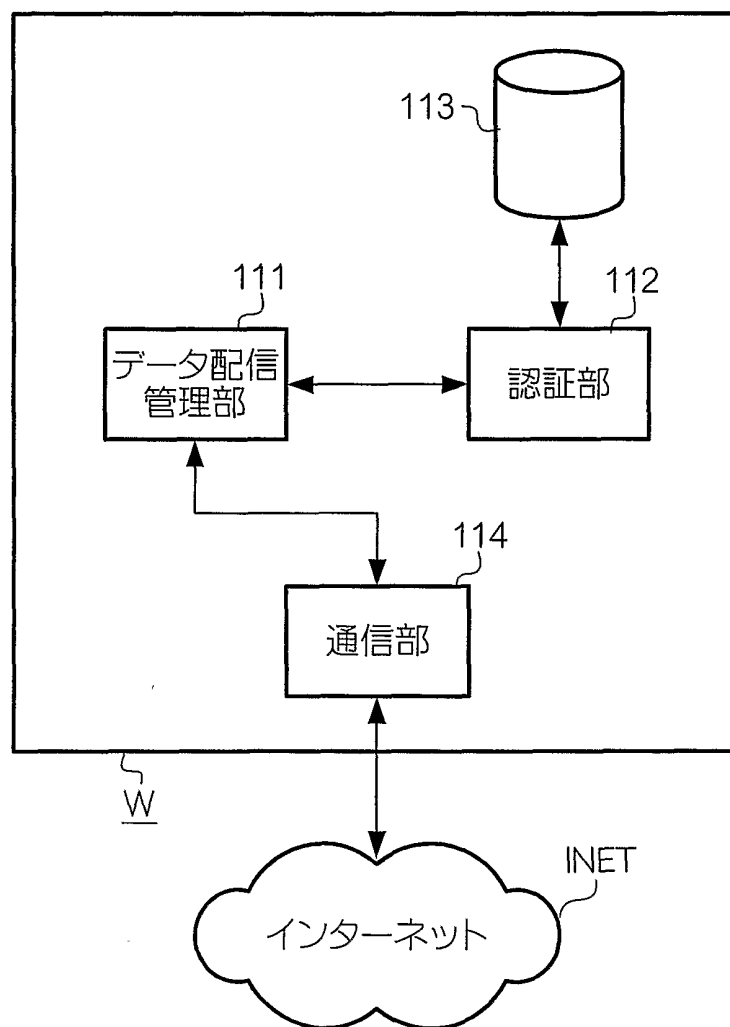


図 2



3/15

図 3

```
<HTML>
<HEAD>
<TITLE>〇〇銀行</TITLE>
<META name="△△" content="△△">
</HEAD>
<CETNTER>
<H2><IMG src="△△GIF" alt="〇〇銀行"
height="30" width="200"><FONT
color="#004000">
〇〇銀行</FONT></H2>
</CENTER>
<BODY>
<BR>
<A href="http://www.〇〇bank.co.jp/△△#utn">
1.銀行振込</A>
<FONT size="-1"><BR>
<BR>
<A href="http://www.〇〇bank.co.jp/××#utn">
2.残高照会</A>
<FONT size="-1"><BR>
</BODY>
```

図 4

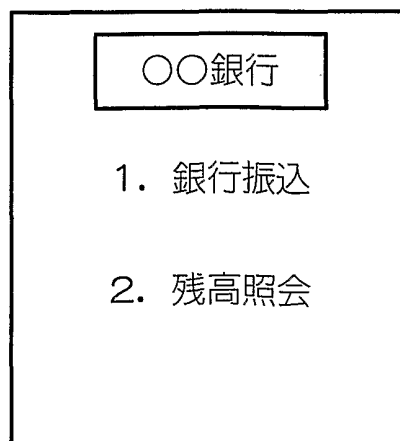


図 5

ユーザID	個人識別情報
user.a	△△△△△△
user.b	■■■■■■
...	...

図 6

タイトル	キーワード	URL
〇〇銀行	ネットバンキング	https://www.〇〇 bank.co.jp/index.html#utn
	...	
××商事	ネットオークション	http://www.××.co.jp
	...	
△△銀行	ネットバンキング	http://www.△△ bank.co.jp/index.html#utn
	...	
...	...	...

図 7

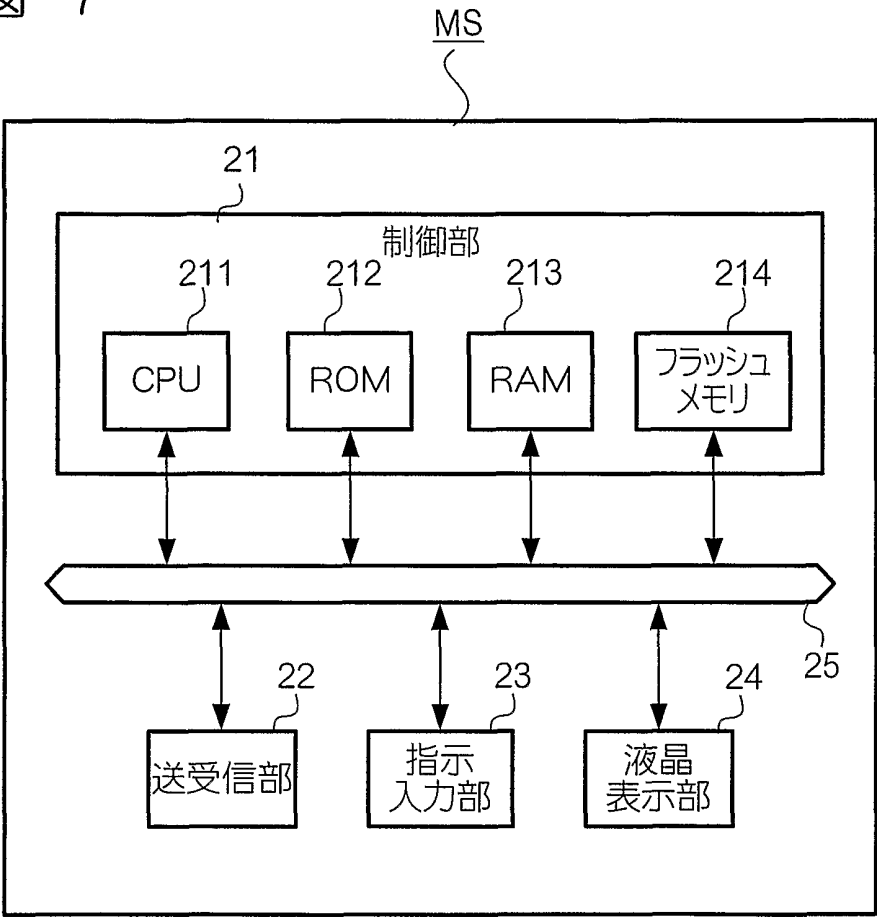


図 8

F

URL	要求データ列フラグ
http://:△△.co.jp	1
http://:■■■.co.jp	0
...	...

TBL

図 9

検索サービス

キーワード

図 10

検索結果

キーワード “ネットバンキング”

1

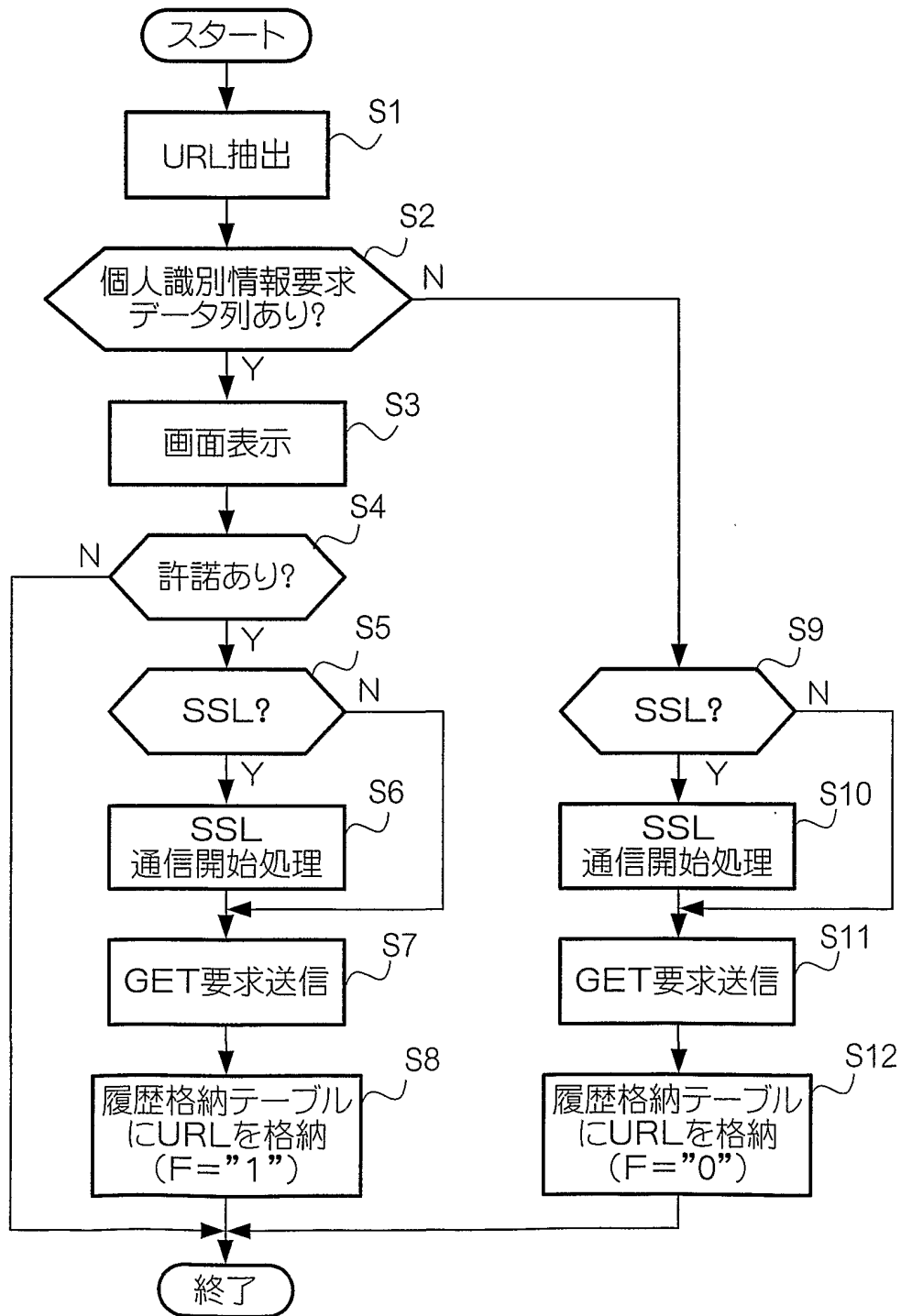
〇〇銀行

2

△△銀行

...

図 11



9/15

図 12

注意!

個人識別情報が要求
されています。
送信しますか?

Yes

No

図 13

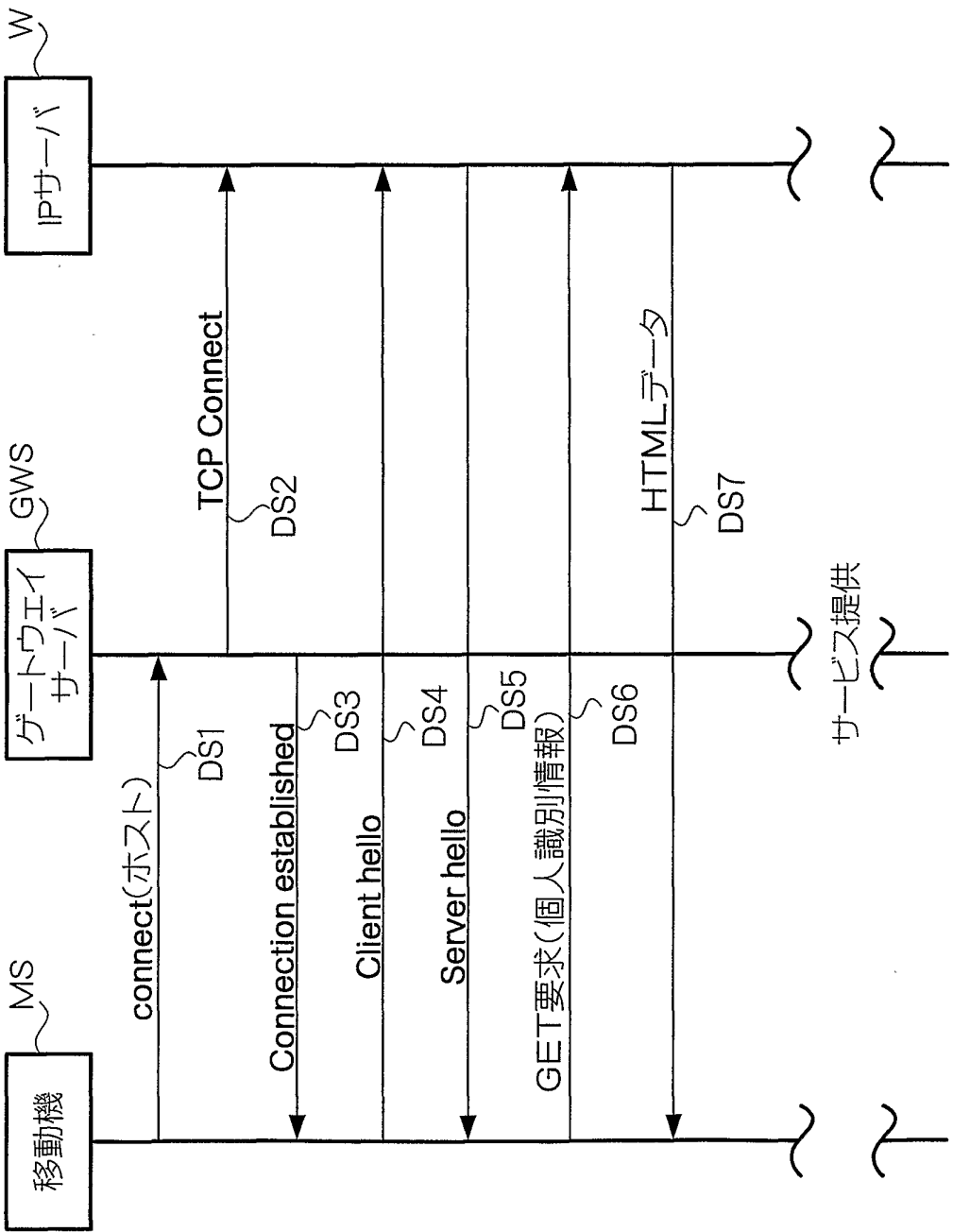


図 14

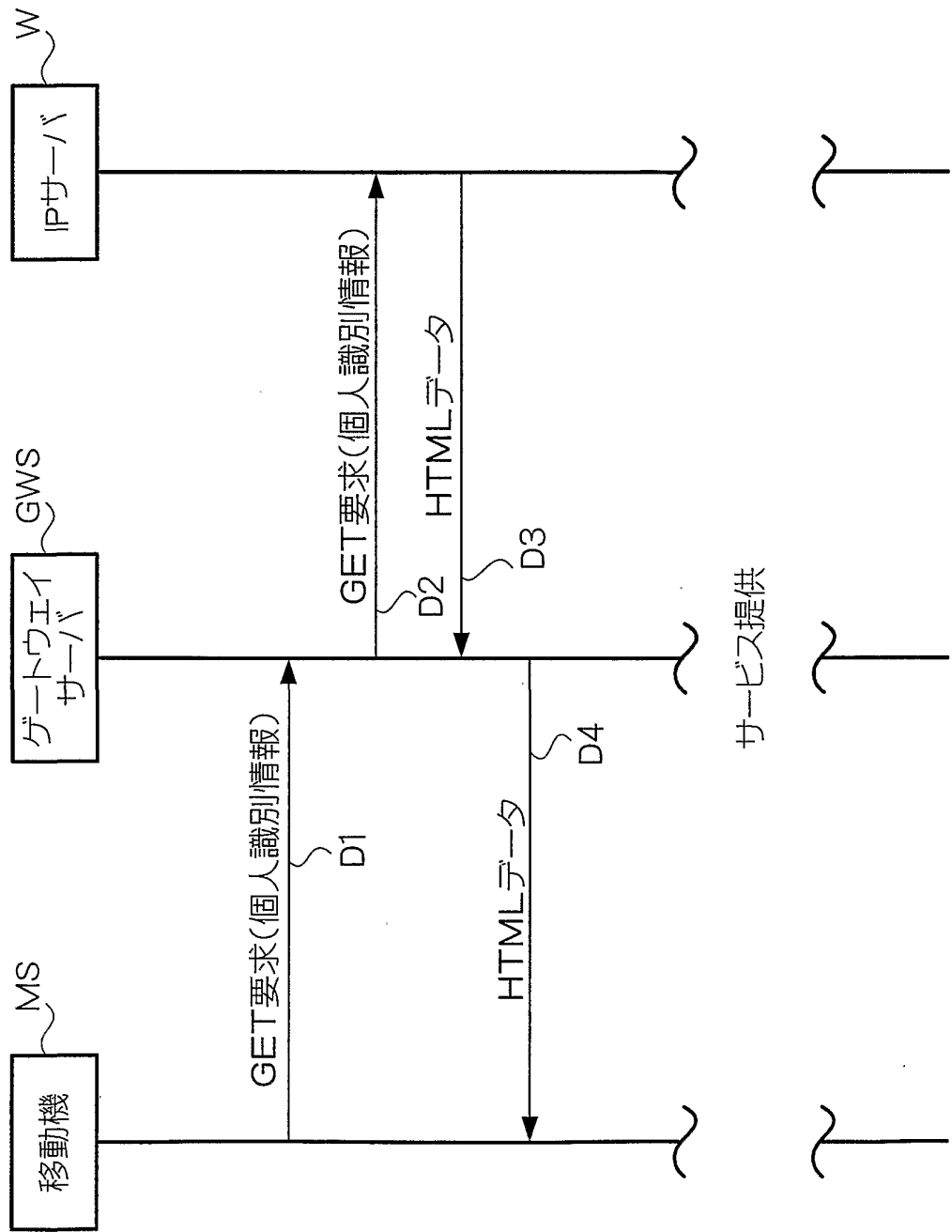


図 15

〇〇銀行

1 銀行振込

2 残高照会

...

図 16

銀行振込ページ

.....

.....

.....

.....

.....

.....

戻る

図 17

ユーザID	個人識別情報	パスワード
user.a	△△△△△△	△△△△
user.b	■■■■■■■■	■■■■■■
...	...	...

図 18

サービス
ログイン

ユーザID

パスワード

図 19

注意！

個人識別情報が要求されて
います。
送信する場合ユーザIDを入
力してください。

ユーザID

送信

図 20

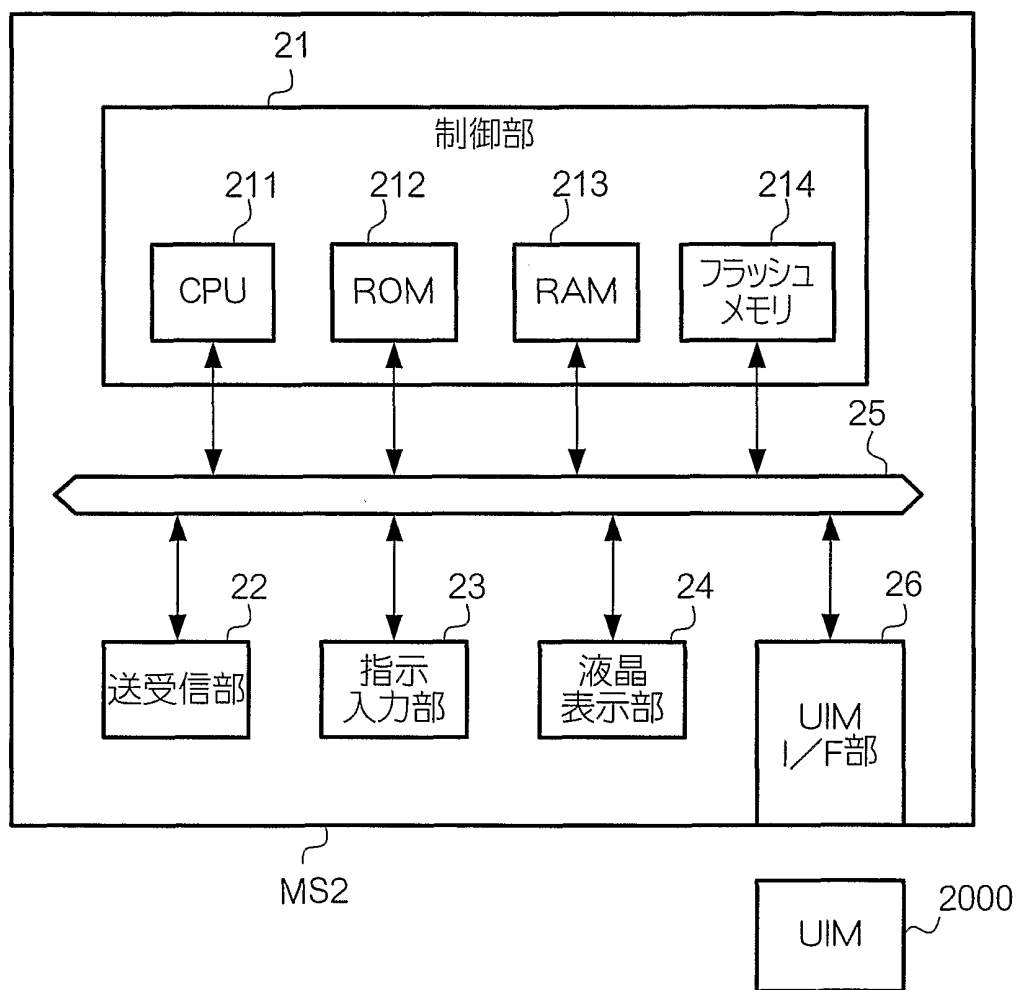


図 21

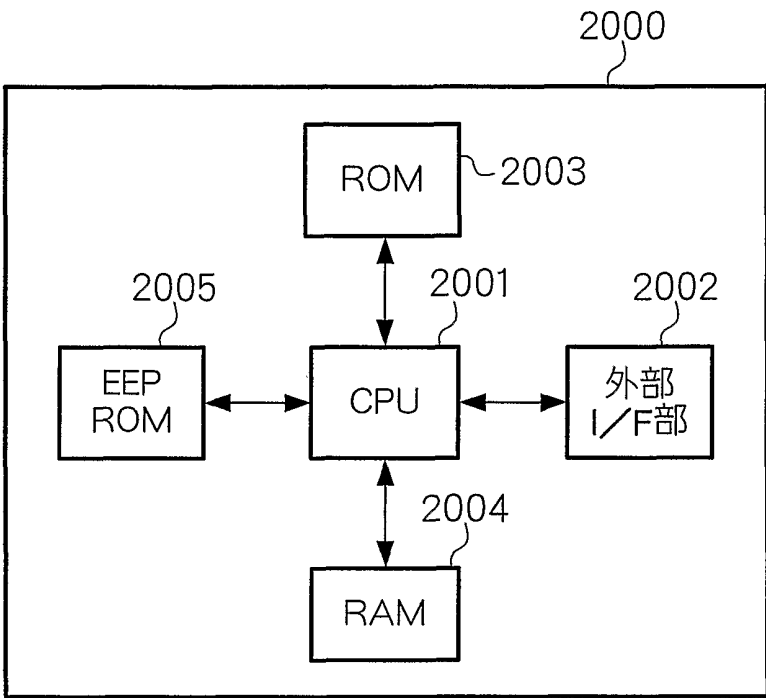


図 22

ユーザID	個人識別情報	
	移動機	UIM
user.a	△△△△△△	△△△△
user.b	■ ■ ■ ■ ■ ■ ■ ■	■ ■ ■ ■ ■
...	...	...

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/10834

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00, G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00, G06F17/60, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Toroku Jitsuyo Shinan Koho	1994-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP, 11-306171, A (Fujitsu Ltd.), 05 November, 1999 (05.11.99), Claims (Family: none)	12-14 1-11
Y A	JP, 10-11383, A (Unwired Planet Inc.), 16 January, 1998 (16.01.98), Claims & US 5809415 A & EP 779759 A2	12-14 1-11
A	JP, 2000-285078, A (NEC Corp.), 13 October, 2000 (13.10.00), Claims (Family: none)	1-14
A	JP, 11-168758, A (Sanyo Electric Co., Ltd.), 22 June, 1999 (22.06.99), Claims (Family: none)	1-14
A	JP, 11-25051, A (Hitachi, Ltd.), 29 January, 1999 (29.01.99), Claims (Family: none)	1-14

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
01 March, 2002 (01.03.02)Date of mailing of the international search report
12 March, 2002 (12.03.02)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/10834

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Hiroki EDA, "Pasocon ID Sengen Ninshogijutsu Part 2 Koyubango to Ninshokairo de Kobetsu no Tanmatsu o Kakujitsu ni Shikibetsu", Nikkei Electronics, 1999.04.05, No.740, pages 105 to 113	2, 8
A	JP, 10-260939, A (Fujitsu Ltd.), 29 September, 1998 (29.09.98), Claims (Family: none)	8

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, G06F17/60, H04L9/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
 日本国公開実用新案公報 1971-2002年
 日本国実用新案登録公報 1996-2002年
 日本国登録実用新案公報 1994-2002年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	JP 11-306171 A (富士通株式会社) 1999. 1 1. 05, 特許請求の範囲 (ファミリーなし)	12-14 1-11
Y A	JP 10-11383 A (アンワイアード・プラネット・イン コーポレイテッド) 1998. 01. 16, 特許請求の範囲 & US 5809415 A & EP 779759 A2	12-14 1-11
A	JP 2000-285078 A (日本電気株式会社) 200 0. 10. 13, 特許請求の範囲 (ファミリーなし)	1-14

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

01. 03. 02

国際調査報告の発送日

12.03.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

宮司 卓佳



5B

9555

電話番号 03-3581-1101 内線 3545

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P 11-168758 A (三洋電機株式会社) 1999. 06. 22, 特許請求の範囲 (ファミリーなし)	1-14
A	J P 11-25051 A (株式会社日立製作所) 1999. 01. 29, 特許請求の範囲 (ファミリーなし)	1-14
A	枝洋樹他, パソコンID宣言 認証技術 第2部 固有番号と認証回路で個別の端末を確実に識別, 日経エレクトロニクス, 1999. 04. 05, 第740号, p. 105-p. 113	2,8
A	J P 10-260939 A (富士通株式会社) 1998. 09. 29, 特許請求の範囲 (ファミリーなし)	8