

transaction by depressing the start key of WCD 120 when the user (carrying WCD 120) is within a wireless communication range of parking meter 115. In response, WCD 120 requests parking meter specific information from parking meter 115. Parking meter 115 responds with an exemplary message:

METER202398981:

THIS METER COSTS \$0.25 an hour, PAY?

This message, once received by WCD 120, is displayed to user 105 via the WCD display device. User 105 responds by depressing a WCD key indicating "YES ", the user wishes to pay for an hour of parking. In response to the "YES" key being depressed, WCD 120 transmits an encrypted request to ESP 125 for approval to transfer \$0.25 from user bank account 110 to the parking meter. Assuming a bank account balance of greater than \$0.25 in bank account 110, bank facility 135 approves the transfer, and in turn, ESP 125 transmits an encrypted approval message to WCD 120. After receiving the approval message, WCD 120 transmits a message including a \$0.25 monetary transfer to parking meter 115 to complete the transaction and to pay for one hour of parking. After the transaction is complete, ESP 125 reestablishes communication with facility 135 to thereby debit bank account 110 by \$.25.

In the following exemplary "restaurant-based" e-commerce transaction, POT terminal 115 resides in a restaurant and stores restaurant specific information such as a food and beverage menu with associated prices. In this example, user 105 again initiates the e-commerce transaction by depressing the start key of WCD 120 when in communication range of POT terminal 115. In response to the request transmitted by WCD 120, restaurant POT terminal 115 transmits a response message to the WCD 120. The response message includes the food and beverage menu and associated prices. This information is displayed to user 105 at

WCD 120. User 105 selects desired items from the displayed menu via input device 123 of WCD 120. WCD 120 automatically calculates a total cost of the selected items (including a designated tip if the user so desires), and transmits an encrypted message to ESP computer 125 for approval of this total cost amount. If ESP computer 120 approves the transaction, WCD 120 transmits an electronic payment to POT terminal 115 at the restaurant.

The e-commerce transactions described above each involve an electronic transfer of assets, such as money, from WCD 120 to POT terminal 115 at the POT. However, it should be appreciated that POT terminal 115 can be a second WCD, whereby assets are transferred electronically from WCD 120 to the second WCD. FIG. 6 is a block diagram of an arrangement 600 for such an electronic transfer of assets from WCD 120 to a WCD 605. Arrangement 600 is similar to the arrangement described in connection with system 100, except WCD 605 replaces POT terminal 115. Arrangement 600 also includes ESP computer 610 and an e-commerce facility 612, for supporting an e-commerce transaction effected using WCD 605. A user 615 owns assets in an asset account 620 held by e-commerce facility 612. WCD 605, ESP 610 and e-commerce facility 612 inter-communicate in the same manner that WCD 120, ESP 125, and e-commerce facility 135 inter-communicate.

In arrangement 600, user 615 can initiate and control an electronic transfer of assets from asset account 620 to asset account 110 using WCD 605. An exemplary transfer, wherein asset accounts 620 and 110 are bank accounts, includes the electronic transfer of money from bank account 620 to bank account 110, as now described. When user 615 initiates such a transaction at WCD 605, WCD 605 transmits an initial request to WCD 120. In response, e-commerce server application 325 of WCD 120 (see FIG. 3) generates a response message identifying WCD 120. Next,

at WCD 605, user 615 enters a dollar amount that is to be transferred from account 620 to account 110. Next a transfer of this amount is verified/validated by ESP 610 and e-commerce facility 612 in the same manner as described above in connection with FIG. 4. After such validation, WCD 605 transmits a message to WCD 120 electronically transferring the entered dollar amount to WCD 120. Finally, the account balances of asset accounts 620 and 110 are respectively debited and credited by the dollar amount transferred between the accounts to reflect the e-commerce transaction.

FIG. 7 is a block diagram of another arrangement 700 of the present invention for effecting an e-commerce transaction using a WCD 705 capable of scanning a merchandise bar code associated with a merchandise item 710. WCD 705 is interconnected with an ESP computer and bank facility as described above, but not shown in FIG. 7. The first wireless interface of WCD 705, that is, the short range wireless interface, includes a known bar code reader 715. Bar code reader 715 is any known bar code reader capable of reading or scanning a bar code 720, such as a UPC label, associated with merchandise item 710. When the user of WCD 705 scans UPC label 720 with reader 715, WCD 705 acquires a purchase price and an identification code corresponding to merchandise item 710, and stores this information to a memory buffer of WCD 705. As the user scans additional merchandise items while shopping, WCD 705 accumulates a total purchase price in, and adds additional identification codes to, the memory buffer. When the user is done shopping and wishes to pay for the scanned items, the user carries WCD 705 to a POT terminal capable of receiving an electronic transfer of money from WCD 705. The user then initiates a payment process as described in connection with FIG. 4 to pay for the scanned merchandise items at the POT terminal.

In the exemplary e-commerce transactions described above, asset account 110 is a bank account holding money, and money is electronically transferred to/from the bank account. However, asset account 110 can hold other, electronically transferrable, non-monetary assets. For example, asset account 110 can hold electronic coupons, credit points or bonus points cumulatively earned whenever user 105 makes a purchase either in accordance with the present invention, or that is not necessarily in accordance with the present invention. Such coupons, credit points or bonus points can then be applied to subsequent purchases made in accordance with the present invention, wherein the non-monetary assets are electronically transferred to a POT terminal, instead of money. Also, these non-monetary assets can be held in a second or third asset account owned by user 105 in addition to asset account 110. Asset account 110 can also be a credit account, such as a credit card account, for transferring credit to the POT terminal in the e-commerce transaction, thereby obviating the need for a credit card in a credit transaction.

FIG. 8 is a block diagram of an embodiment of WCD 120. WCD 120 has a compact, hand-held form factor similar to that of a personal digital assistant or cellular telephone. The functionality of WCD 120 can be integrated with the functionality of a wireless or cellular telephone so that WCD 120 can be used as both a cellular phone and to effect e-commerce transactions. WCD 120 includes a bus 802 or other communication mechanism for communicating information, and a processor 804 coupled with the bus 802 for processing information. WCD 120 also includes a main memory 806, such as a random access memory (RAM) or other dynamic storage device, coupled to the bus 802 for storing information and instructions to be executed by processor 804. Main memory 806 also may be used for storing temporary variables or other intermediate information during execution of

instructions to be executed by processor 804. WCD 120 further includes a read only memory (ROM) 808 or other static storage device coupled to the bus 802 for storing static information and instructions for the processor 804. A storage device 810, such as a magnetic disk or optical disk, is provided and coupled to the bus 802 for storing information and instructions.

WCD 120 includes display 124, such as a flat panel display, for displaying information to a user. Display 124 is coupled to bus 802. Input device 123, including alphanumeric and other keys, is coupled to bus 802 for communicating information and command selections to the processor 804. Another type of user input device is a cursor control 816, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 804 and for controlling cursor movement on display 124.

Initiation and control of the e-commerce transaction is provided by WCD 120 in response to processor 804 executing sequences of instructions contained in main memory 806. Such instructions may be read into main memory 806 from another computer-readable medium, such as a storage device 810. Execution of the sequences of instructions contained in the main memory 806 causes the processor 804 to perform the process steps described above in connection with FIG. 4 and the exemplary e-commerce transactions described above. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with computer software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.

WCD 120 includes a short range, wireless communication interface (I/F) 820 coupled to bus 802. Communication I/F 820 corresponds to the "first interface" mentioned in connection with FIGs. 1 and 7. As described above, communication I/F 820

provides bi-directional wireless data communication with the compatible wireless communication I/F of POT terminal 115, over wireless communication link 137. Communication I/F 820 includes a transceiver for transmitting and receiving data over wireless communication link 137, and a micro-controller for controlling the communication interface. The micro-controller can be integrated with processor 804, and executes program instructions or the like to implement the functionality of the communication I/F including any required data communication protocols. To support alternative arrangement 700 described in connection with FIG. 7, communication I/F 820 can optionally include a known bar code reader.

In the present invention, wireless communication I/F 820 supports digital data packet exchanges between WCD 120 and POT terminal 115, and as such, can be implemented in accordance with exemplary specifications for short-range wireless communications, such as "Bluetooth" and/or Infrared Data Association (IrDA) specifications, or any other suitable specification, so long as a compact communication I/F 820 can comply with the specification requirements. Bluetooth is a proposed radio frequency (RF) specification for short-range, point-to-multipoint data transfer. Bluetooth radio links, operating in the 2.4 gigahertz Industrial-Scientific-Medical (ISM) frequency band, have a nominal communication range between 10 centimeters and 10 meters. However, this nominal range can be extended to 100 meters by increasing the transmit power of a Bluetooth transmitter in communication I/F 820. The IrDA specification provides for wireless data exchanges using a short-range infrared wireless link. Accordingly, a typical distance between WCD 120 and POT terminal 115 during an e-commerce transaction is ten meters or less, unless an extended range transmitter is used in each device.

WCD 120 also includes a wireless network communication I/F 822. Network communication I/F 822 corresponds to the "second interface" mentioned in connection with FIG. 1, and supports the wireless exchange of digital data packets between WCD 120 and network access device 145, as described above. Wireless network communication I/F 822 incorporates a wireless transceiver and a micro-controller similar to the type used in cellular telephony devices for communicating between a cellular telephone and a distant base station. In the preferred embodiment, network communication I/F 822 communicates with network access device 145 using a code division multiple access (CDMA) communication protocol.

It should be understood that POT terminal 115 includes a wireless I/F compatible with wireless I/F 820 of WCD 120. POT terminal 115 also includes a processor and memory sufficient to host and execute server application 345.

While various embodiment of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments and arrangements, but should be defined only in accordance with the following claims and their equivalents.

25

CLAIMS

1. A method of effecting a wireless electronic commerce (e-commerce) transaction between a wireless communication device and a point-of-transaction (POT) terminal, comprising:
- (a) associating unique identifying information with the wireless communications device;
 - (b) wirelessly transmitting first e-commerce transaction data between the wireless communications device and the POT terminal; and
 - (c) wirelessly transmitting second e-commerce transaction data generated as a function of the unique identifying information and the first e-commerce transaction data, from the wireless communications device to a service provider.
2. The method of claim 1, wherein the service provider provides an e-commerce support service to a subscriber having a subscriber asset account electronically accessible to the service provider and remote from both the wireless communications device and the POT terminal, further comprising
- effecting a transfer of assets between the subscriber asset account and the POT terminal via the first e-commerce transaction data, the second e-commerce transaction data, and the wireless communications device; and
 - increasing and decreasing assets in the asset account to reflect the transfer of assets in the e-commerce transaction.
3. The method of claim 2, wherein the subscriber asset account is a subscriber bank account, further comprising
- electronically transferring a monetary fund amount from the bank account to the POT terminal; and

6 determining the monetary fund amount as a function of the
first e-commerce transaction data and transaction control
8 commands entered via the wireless communications device to
control the transaction.

4. The method of claim 1, wherein step (b) includes
2 transmitting a request message from the wireless
communications device to the POT terminal requesting
4 transaction information from the POT terminal; and
receiving a response message from the POT terminal at the
6 wireless communication device, the response message including
the transaction information requested from the POT terminal.

5. The method of claim 4, wherein step (b) further includes
2 transmitting the first e-commerce transaction data over a short-
range, wireless communication link in accordance with one of a
4 Bluetooth data transmission protocol, an IrDA data transmission
protocol, and a proprietary data transmission protocol.

6. The method of claim 1, further comprising
2 establishing a wireless network link between the wireless
communications device and the service provider in response to
4 receipt of the first e-commerce transaction data at the wireless
communications device; and
6 transmitting the second e-commerce transaction data over
the wireless network link using a packet data protocol compatible
8 with an Internet packet data protocol.

7. The method of claim 1, wherein the unique identification
2 information includes at least one of a subscriber personal
identification number, a mobile subscriber number, and an
4 electronic serial number, and wherein step (c) includes encrypting

6 e-commerce transaction data at the wireless communication
device using the unique identification information to generate the
second e-commerce transaction data.

8. The method of claim 1, further comprising
2 displaying information relating to the first transaction data
at the wireless communications device; and
4 entering commands via the wireless communications
device to initiate and control the e-commerce transaction.

9. A system for effecting a wireless electronic commerce (e-
2 commerce) transaction, comprising:
a wireless communications device having unique
4 identifying information;
a local wireless interface in said wireless communications
6 device for communicating with a wireless interface at a point-of-
transaction (POT) terminal;
8 means for transmitting first e-commerce transaction data
between the wireless interfaces; and
10 means for transmitting second e-commerce transaction data
generated as a function of the unique identifying information and
12 the first e-commerce transaction data from said wireless
communications device to a service provider.

10. The system of claim 9, further comprising a support
2 computer at the service provider for providing an e-commerce
support service to a subscriber having a subscriber asset account
4 electronically accessible to the support computer and remote from
both the wireless communications device and the POT terminal,
6 wherein assets are transferred between the subscriber asset
account and the POT terminal via the first e-commerce transaction
8 data, the second e-commerce transaction data, and the wireless

10 communications device, the support computer including means
for increasing and decreasing assets in the asset account to reflect
the transfer of assets in the e-commerce transaction.

11. The system of claim 10, further comprising
2 means for electronically transferring a monetary fund
amount from a subscriber bank account to the POT terminal; and
4 means for determining the monetary fund amount
transferred based on the e-commerce first transaction data and
6 transaction control commands entered via the wireless
communications device to control the transaction.

12. The system of claim 9, wherein said means for transmitting
2 first e-commerce transaction includes
means in the wireless communication device for
4 transmitting a request message from the wireless communications
device to the POT terminal requesting transaction information
6 from the POT terminal; and
means in the wireless communication device for receiving a
8 response message including the requested transaction information
from the POT terminal.

13. The system of claim 12, wherein said wireless interfaces
2 include means for transmitting the first e-commerce transaction
data over a short-range, wireless communication link in
4 accordance with one of a Bluetooth, an IrDA, and a proprietary
data packet transmission protocols.

14. The system of claim 9, wherein the wireless communication
2 device further comprises

4 means for establishing a wireless network link with the
service provider in response to receipt of the first e-commerce
transaction data at the wireless communications device; and
6 means for transmitting the second transaction data over the
wireless network link using a packet data protocol compatible
8 with an Internet packet data protocol.

15. The system of claim 9, wherein the wireless communication
2 device further comprises means for encrypting e-commerce
transaction data as a function of the personal identification
4 number to generate the second transaction data, wherein the
unique identification information includes at least one of a
6 subscriber personal identification number, a mobile subscriber
number, and an electronic serial number of the wireless
8 communication device.

16. The system of claim 9, wherein the wireless communication
2 device further comprises
means for displaying information relating to the first
4 transaction data; and
means for entering commands to initiate and control the e-
6 commerce transaction.

17. A system for effecting a wireless electronic commerce (e-
2 commerce) transaction, comprising:
an e-commerce support computer at a service provider for
4 providing an e-commerce support service to at least one
subscriber having a subscriber asset account electronically
6 accessible to the e-commerce support computer;
a point-of-transaction (POT) terminal having a wireless
8 interface;
a wireless communications device having

10 unique identifying information, and including
 a wireless interface for communicating with the first
12 wireless interface of the POT terminal,
 means for transmitting first e-commerce transaction
14 data between the wireless interfaces of the wireless
 communication device and the POT terminal; and
16 means for transmitting second e-commerce
 transaction data generated as a function of the unique identifying
18 information and the first e-commerce transaction data between
 the wireless communications device and the e-commerce support
20 computer.

18. The system of claim 17, wherein the subscriber asset
2 account is remote from both the wireless communications device
 and the POT terminal, and wherein assets are transferred between
4 the subscriber asset account and the POT terminal via the first e-
 commerce transaction data, the second e-commerce transaction
6 data, and the wireless communications device, the e-commerce
 support computer including means for increasing and decreasing
8 assets in the asset account to reflect the transfer of assets in the e-
 commerce transaction.

19. The system of claim 17, wherein said means for
2 transmitting first e-commerce transaction in the wireless
 communication device includes
4 means for transmitting a request message from the wireless
 communications device to the POT terminal requesting
6 transaction information from the POT terminal; and
 means in the wireless communication device for receiving a
8 response message including the requested transaction information
 from the POT terminal, and wherein

10 said POT terminal includes means for receiving the request
message and means for formulating and transmitting the response
12 message.

20. The system of claim 17, wherein both the wireless
2 communication device and the e-commerce support computer
further comprise means for encrypting e-commerce transaction
4 data as a function of unique identification information to generate
the second transaction data, wherein the unique identification
6 information includes at least one of a subscriber personal
identification number, a mobile subscriber number, and an
8 electronic serial number of the wireless communication device.

21. A computer program product comprising computer usable
2 media having computer readable program code means embodied
in said media for causing application programs to execute on
4 computer processors in a wireless communication device, in a
point-of-transaction terminal, and in an electronic commerce (e-
6 commerce) support computer at a service provider, to effect an e-
commerce transaction, said computer readable program code
8 means comprising:

 a first computer readable program code means for causing
10 the processor to associate unique identifying information with the
wireless communications device;

12 a second computer readable program code means for
causing the processor to wirelessly transmit first e-commerce
14 transaction data between the wireless communications device and
the POT terminal; and

16 a third computer readable program code means for causing
the processor to wirelessly transmit second e-commerce
18 transaction data generated as a function of the unique identifying
information and the first e-commerce transaction data, from the

20 wireless communications device to the e-commerce support
computer.

22. The computer program product of claim 21, wherein the
2 second program code means includes computer readable program
code means for causing the processor to encrypt e-commerce
4 transaction data as a function of the personal identification
number to generate the second transaction data, wherein the
6 unique identification information includes at least one of a
subscriber personal identification number, a mobile subscriber
8 number, and an electronic serial number of the wireless
communication device.

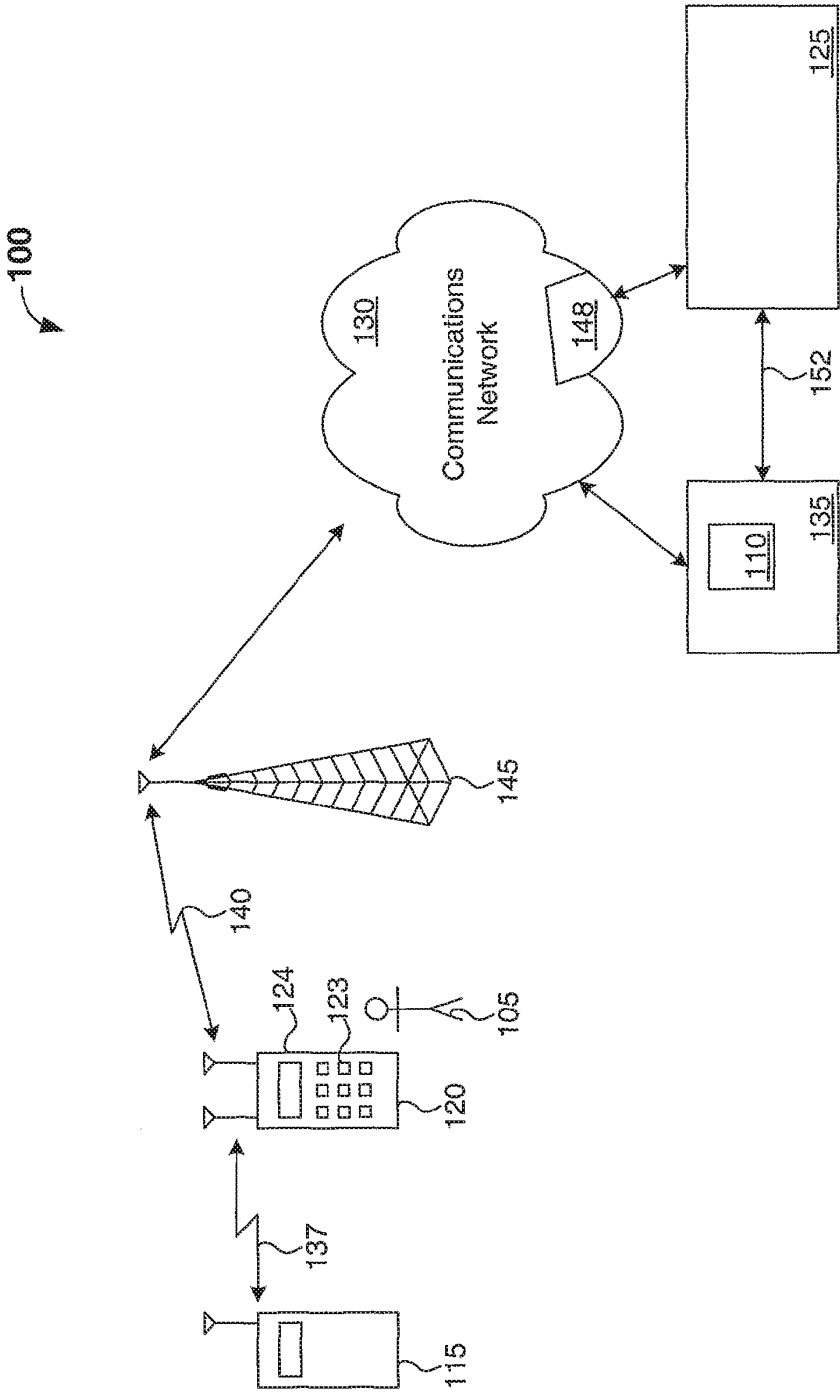


FIG. 1

200

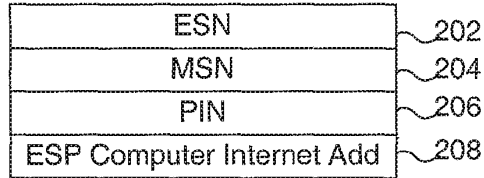


FIG. 2A

220

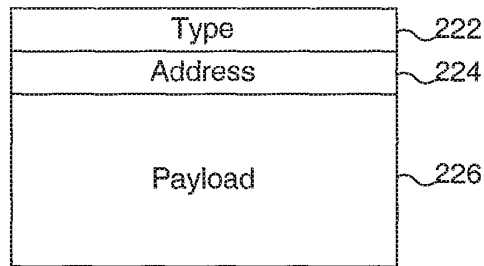


FIG. 2B

230

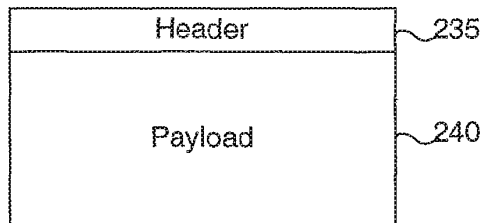


FIG. 2C

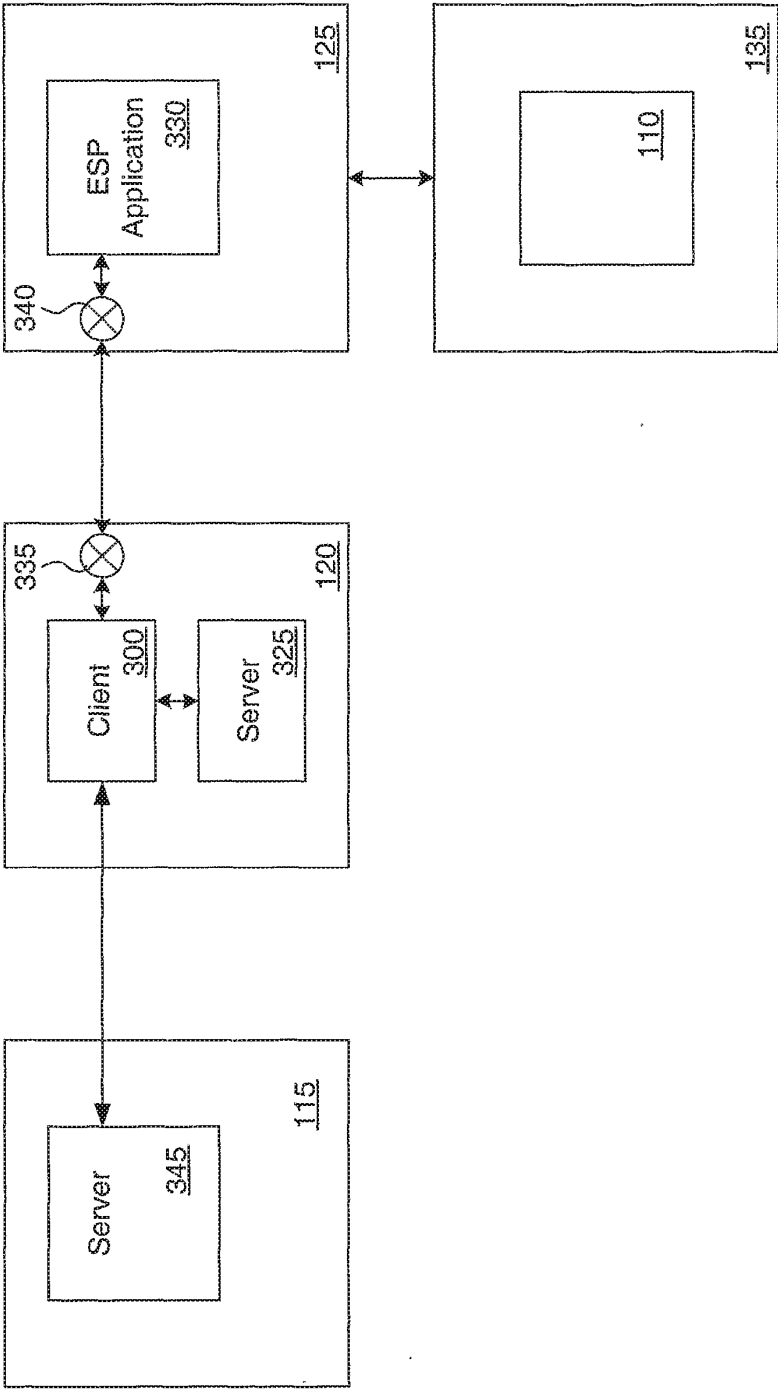


FIG. 3

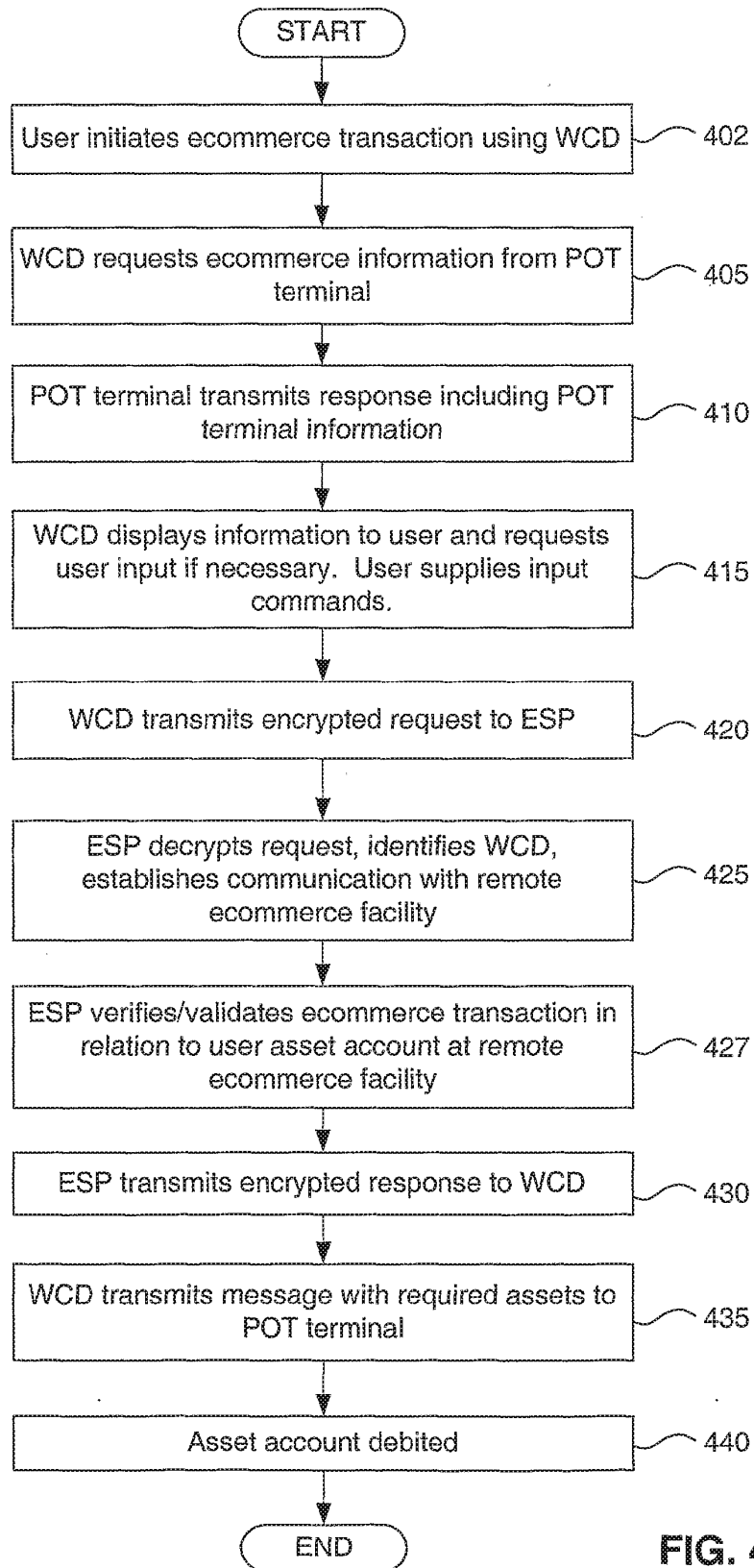


FIG. 4

SUBSTITUTE SHEET (RULE 26)

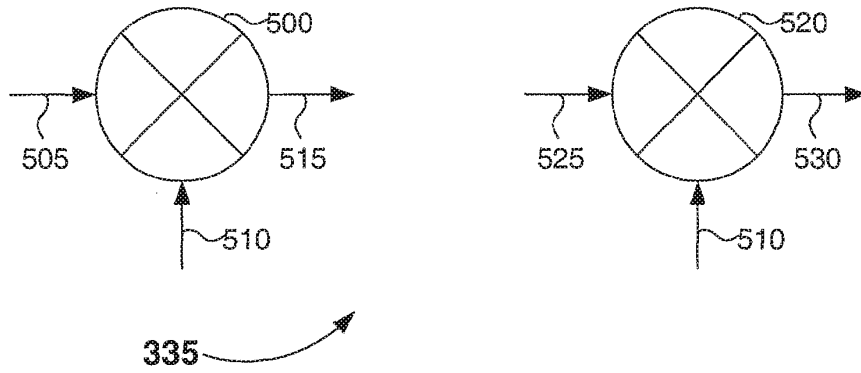


FIG. 5

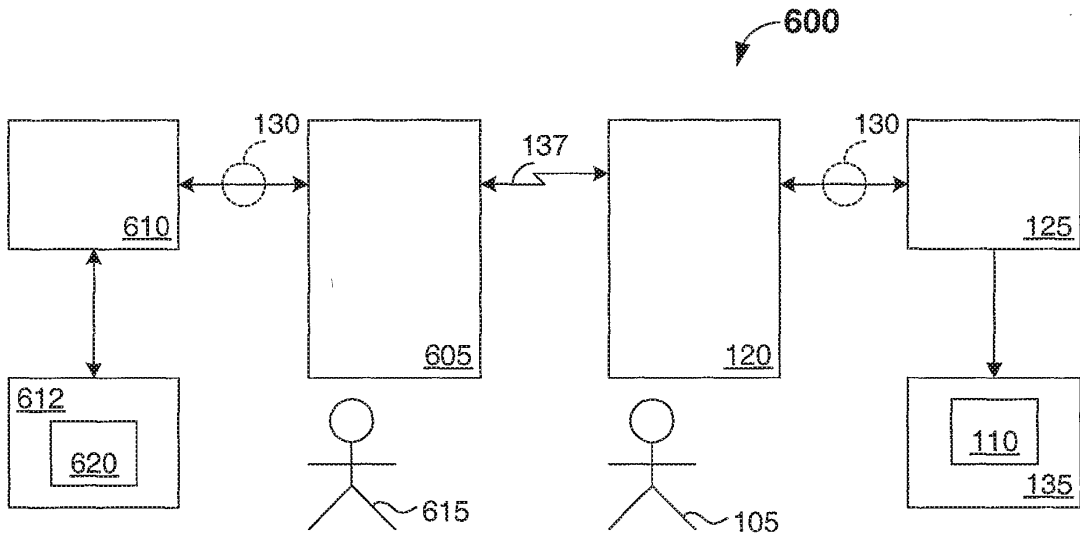


FIG. 6

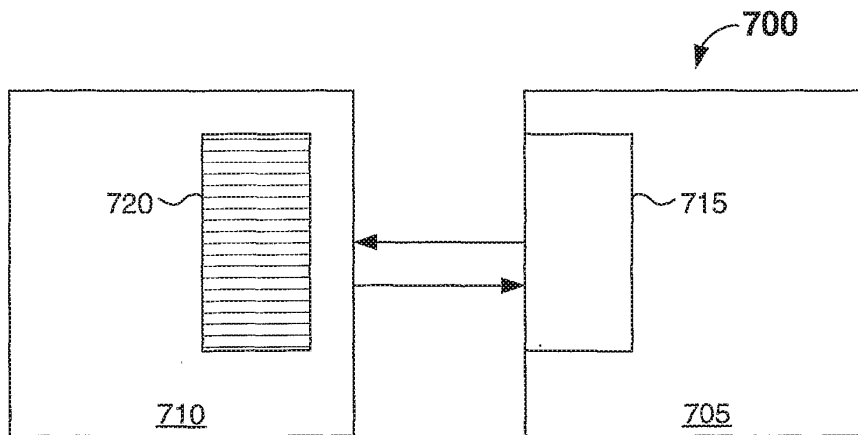


FIG. 7

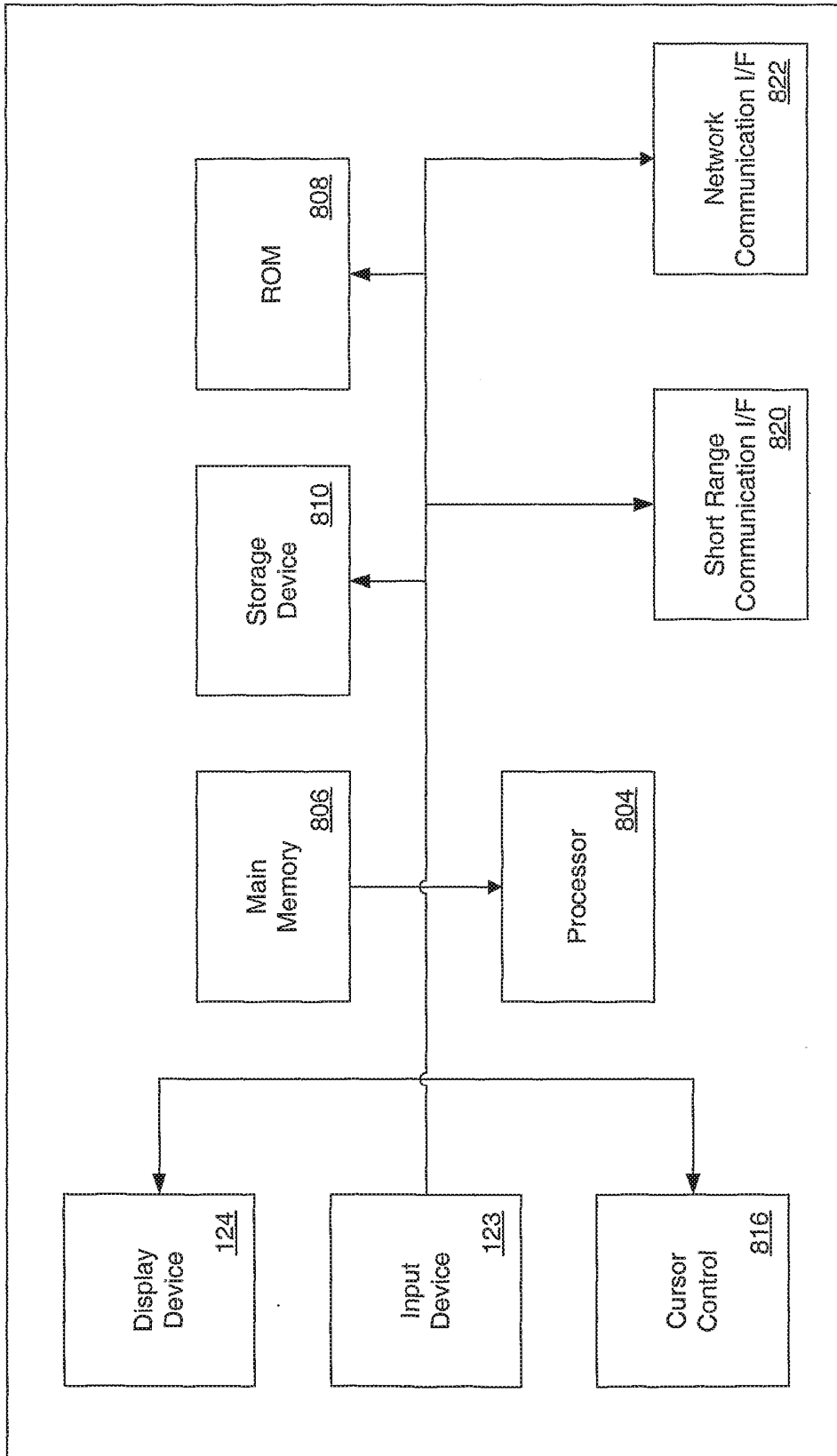


FIG. 8

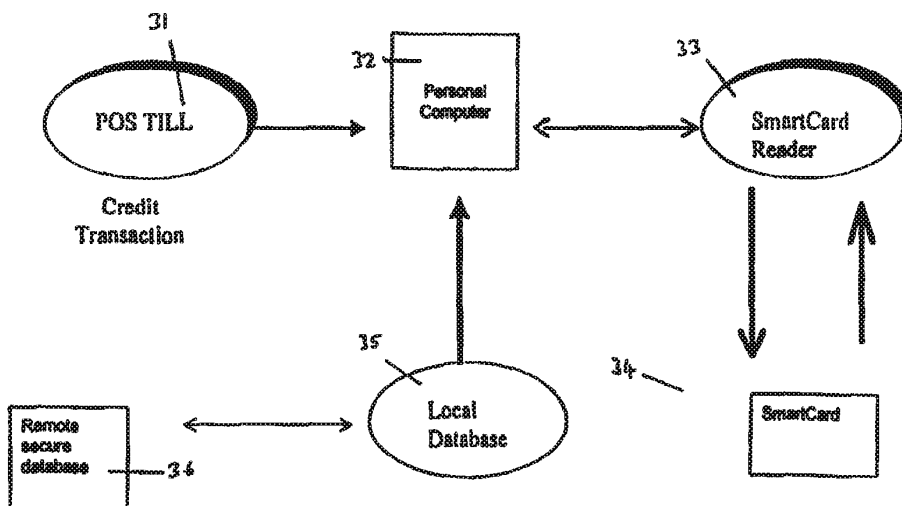


INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : H04M 17/00, H04Q 7/32</p>	<p>A1</p>	<p>(11) International Publication Number: WO 99/13636 (43) International Publication Date: 18 March 1999 (18.03.99)</p>
<p>(21) International Application Number: PCT/GB98/02729 (22) International Filing Date: 10 September 1998 (10.09.98) (30) Priority Data: 9719100.1 10 September 1997 (10.09.97) GB (71) Applicant (for all designated States except US): TEKTON COMMUNICATIONS LIMITED [GB/GB]; Marsh House, 500 Montagu Road, London N9 0UR (GB). (72) Inventors; and (75) Inventors/Applicants (for US only): BISWELL, Anthony, James [GB/FR]; Villa Mas Souleou, Boulevard Plan des Abeilles, F-06230 Saint Jean Cap Ferrat (FR). CASTLE, Derek, Keith [GB/GB]; 4 Tavern Road, Wooley Bridge, Glossop, Derbyshire SK13 2RB (GB). (74) Agent: COATES, Ian, Harold; Sommerville & Rushton, 45 Grosvenor Road, St. Albans, Herts AL1 3AW (GB).</p>		<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report.</i></p>

(54) Title: A PRE-PAYABLE COMMUNICATION DEVICE

Pre Paid credit Charging



(57) Abstract

A portable radio communications apparatus comprising: (i) a portable handset; (ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit; (iii) a recess in the handset adapted to accept the removable module; (iv) a reading device in the handset adapted to determine a content of the electronic purse; (v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse; and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

A Pre-payable Communication Device

Field of Invention

The present invention relates to pre-payable communication devices and more particularly to pre-payable communication devices which are suitable for use in radio
5 communication networks.

Background to the invention

One problem with radio communication devices such as mobile telephones is that they are relatively expensive both to purchase and to run. This represents a problem both for the subscriber and for the service provider. For example, the service
10 provider needs to rely on the creditworthiness of the mobile phone subscriber and both the service provider and the subscriber are at risk from fraudulent use of the subscriber's terminal. Many people who would otherwise benefit from the occasional use of a mobile phone are prevented from having this benefit because either the cost is too high and/or the service provider is unable to rely on their creditworthiness. For
15 occasional users the monthly line rental charge is often prohibitively expensive.

There are many situations in which the use of conventional mobile telephones is problematic. For example, an employee may be given a mobile telephone by his employer to use only in essential circumstances. The employer would like to ensure that the employee does not run up additional costs by using the phone for personal use.
20 However, this is difficult to do until after the event when the employer is able to check the telephone bill.

Another problem relates to the fact that in different geographic locations, different communication protocol systems are in operation. An example of a protocol system is Global system for Mobile Communications (GSM) which is a European
25 protocol system. Typically, mobile telephone handsets are operable with only one, or perhaps two different communication protocol systems. This means that when the user

moves to a different geographical area, he may be unable to operate his mobile telephone, if the communication protocol system for that area is incompatible with his handset. This is often a problem for travellers and yet travellers often only have access to mobile communications devices and need them most when they are on the move.

5 Some attempts have been made to overcome these problems using SmartCard technology. A conventional SmartCard is typically a rectangular piece of plastics material, of a similar size and shape to a credit card, which contains integrated circuits, microprocessors and/or read write memory. The use of SmartCards in radio telephones is known, for example, as described in UK patent application number 2267794 in the
10 name of Alan Kilpatrick Conroy. This application describes a pre-payable mobile cellular phone. However, the specification gives no details on how the pre-payment is achieved.

 UK Patent 2266798 in the name of Motorola Inc. describes an apparatus for accepting, retaining and making electrical contact between a SmartCard and a radio
15 telephone handset. The SmartCards used in radio telephones have been limited to subscriber identification module (SIM) cards for use in the European market. SIM cards are available in two sizes; a full size card and a chip card. SIM cards for GSM currently provide subscriber information (e.g. subscriber phone number, service provider) and plug into a GSM compatible mobile telephone handset to configure that handset for a
20 particular subscriber. These cards only reference the subscriber data and do not include radio frequency circuitry or protocol information. If the SIM card is removed from the handset incoming calls cannot be received.

 International patent application number WO/97/05729 in the name of Telecom Italia Mobile S. P. A. describes a radio mobile terminal that is provided with two SIM
25 card readers. One of the SIM cards is described as a prepaid card and this can be loaded into the additional reader. This system is disadvantageous because the mobile

telephone handset needs to contain two SIM card readers which increases the cost and bulk of the terminal. Also the design of the handset is complex because two SIM card readers must be allowed for.

None of the above prior art provides either communications equipment or a method of operation which enables every would-be subscriber, regardless of creditworthiness to have access to a mobile phone on a pay-as-you-use basis.

It is accordingly an object of the present invention to provide a pre-payable communication device for use with radio communication networks and a method of using such equipment which overcomes or at least mitigates one or more of the problems noted above.

Summary of invention

According to the present invention, there is provided a portable radio communications apparatus comprising:

- (i) a portable handset;
 - 15 (ii) a removable module comprising a rechargeable electronic purse and a subscriber identification unit;
 - (iii) a recess in the handset adapted to accept the removable module;
 - (iv) a reading device in the handset adapted to determine a content of the electronic purse;
 - 20 (v) an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse;
- and wherein said module is adapted such that in use the communications apparatus is substantially inoperable when the module is removed. This gives the advantage that every would-be subscriber, regardless of creditworthiness can have access to a mobile phone on a pay-as-you-use basis. When the module is removed from the device, the communications apparatus is inoperable which helps to prevent fraud. The subscriber

identification unit in the removable module provides "identification" for a particular subscriber, so that one subscriber can use several different handsets and configure these for his own use simply by adding the removable module. This helps subscribers when they travel between areas covered by different protocol systems. Such a traveller
5 would be able to retain his or her removable module and simply insert this into a different handset that is operable with the new protocol system.

Preferably, the removable module comprises a SmartCard. This provides the advantage that the removable module is conveniently sized and shaped and can easily be stored and transported.

10 In one embodiment of the invention the subscriber identification unit comprises a conventional subscriber identification module. This provides the advantage that the subscriber identification unit can easily be obtained and is compatible with other known systems. Preferably the subscriber identification unit is adapted to be compatible with the Global System for Mobile Communications Protocol. This enables the
15 communications apparatus to be used with a widely used European protocol system.

According to another aspect of the present invention there is provided a removable module suitable for use with a portable radio communications handset said module comprising an electronic purse and a subscriber identification unit, said module being adapted to be received in a recess in said handset, and wherein said module is
20 adapted such that in use the handset is substantially inoperable when the module is removed from the communications apparatus. This provides the advantage that removable modules are provided which contain an electronic purse. Would-be subscribers can obtain a removable module, regardless of their creditworthiness, and use this to gain access to a mobile phone on a pay-as-you-use basis.

According to another aspect of the present invention there is provided a method of communicating using a portable radio communications apparatus said method comprising the steps of :

- (i) purchasing air time from an air time provider or suitable intermediary;
- 5 (ii) charging said electronic purse with units equivalent to purchased air time;
- (iii) inserting the removable module incorporating the electronic purse into the recess in the handset;
- (iv) determining a content of the electronic purse;
- (v) allowing substantial operation of the communications apparatus on the basis of the
10 content of the electronic purse;
- (vi) operating the communications apparatus and updating the content of the electronic purse on the basis of said operation. This provides the advantage that a service provider or air-time provider no longer needs to be responsible for the creditworthiness of all its subscribers. Individual subscribers may purchase air-time units using cash and
15 "charge" a removable module in this way. The "charged" module can then be used to communicate using the mobile phone handset. The subscriber is then able to use the handset on a pay-as-you-use basis.

The present invention is intended to encompass both the removable module and the handset together and individually. The invention also encompasses a method for
20 using the removable module and handset as well as a charging station for charging the removable module.

Description of the drawings

The invention will be further described, by way of example, with reference to the accompanying drawings in which:

- 25 Figure 1 is a flow diagram indicating a method of using the prepayable portable radio communications apparatus.

Figure 2 is a schematic diagram of a handset and removable module.

Figure 3 is a flow diagram showing a method of recharging a removable module.

Figure 4 is a flow diagram of actions and screen messages in a method of recharging a removable module.

5 Figure 5 is a flow diagram of actions and screen messages in a method of initialising a removable module.

Figure 6 is a schematic diagram of an external fraud detection system.

Figure 7 is a schematic diagram of an alternative external fraud detection system.

Description of preferred embodiments

10 Embodiments of the present invention are described below by way of example only. These examples represent the best ways of putting the invention into practice that are currently known to the Applicant although they are not the only ways in which this could be achieved.

Figure 2 is a schematic diagram of a portable radio communications apparatus
15 20 comprising a portable handset 21 and a removable module 22. The portable handset is shown as being similar to a conventional mobile telephone handset although any suitable type of handset may be used. In the example shown the handset comprises a display area 23, an aerial 24, a key pad 25 and a recess 26. The recess 26 is adapted to receive the removable module 22 as shown in figure 2. The handset
20 may also comprise a microphone and a loudspeaker (not shown) as well as other elements typically contained in a conventional radio telephone handset. However, in one embodiment of the present invention, some components that would typically be contained in a conventional radio telephone handset are removed from the handset 21 and replaced by equivalent or alternative devices and circuitry in the removable module.
25 This is explained further below.

The removable module 22 is shown as being generally rectangular in shape although any shape can be used. Preferably the removable module is a SmartCard and has a shape similar to that of a conventional credit card. The removable module comprises an electronic purse. The term "electronic purse" is used to refer to any form of memory that is capable of being read and updated, and which is capable of storing information about units of "air-time". Preferably, the electronic purse is rechargeable, that is once the units of "air time" that it contains have been used up, they can be replaced. However, this is not essential. The removable modules can be disposable, so that once the units are used up the module is simply replaced. Units of "air-time" are units of time for which a communications service is provided by a communications network service provider. The removable module 22 can be inserted into and removed from the recess 26 in the handset.

The removable module 22 also comprises a subscriber identification unit (not shown) which is preferably a conventional subscriber identification module (SIM). For example, the removable module 22 can be a SIM card which further comprises an electronic purse. When the removable module 22 is removed from the handset the SIM is also removed and this means that the communications apparatus 20 cannot be used to transmit or receive information. When the SIM is removed from the apparatus 20 there is no information in the handset about which subscriber is using the apparatus, for example, the user's telephone number. This means that the communications apparatus is substantially inoperable when the module is removed.

Figure 1 is a flow diagram indicating a method of using the prepayable portable radio communications apparatus. This represents one example of a method for using the prepayable portable radio communications apparatus; other methods may also be used. The user first obtains a removable module 22 and inserts this into the handset 22 and then a card validity check process 1 is carried out. The card validity check process

involves checking whether the removable module is in anyway "data corrupt" or is not in credit. The handset contains a reading device adapted to determine a content of the electronic purse and also an enabling means arranged to allow substantial operation of the communications apparatus on the basis of the content of the electronic purse. At
5 this stage it is also possible for the subscriber to key in a personal identification number (PIN) to the key pad of the handset in order to allow use of the removable module. This provides extra security for the subscriber because it prevents unauthorised use of the removable module and/or the handset. However, use of a PIN number in this way is optional.

10 The next stage 2 involves a network authentication check by the airtime provider. This involves a check of the information provided in the subscriber identification unit or SIM (if a SIM is used). By making this check the service provider can help to prevent use of fraudulent removable modules. If the result of stage 2 is a "fail" i.e. the check is unsuccessful for any reason then the communications apparatus is
15 not enabled as shown in box 3 in figure 1. That is, the enabling means prevents use of the communications apparatus. A warning message and instructions to the subscriber can be displayed on the display panel to indicate that access to the communications network by the service provider has not been granted.

If the result of stage 2 is successful then full functionality and dial facilities are
20 granted by the service provider as indicated in box 4 of figure 1. The subscriber is then able to use the portable radio communications apparatus and as information is transmitted or received from the apparatus (indicated by box 7 in figure 1) the electronic purse is updated (as indicated by arrow 10 in figure 1). For example, as units of "air time" are used by the subscriber these are decremented from the electronic purse
25 contents. Once the reading device determines that the electronic purse is empty the result of the airtime credit box 5 is a "fail" and the user is advised (box 6) and the

enabling device prevents use of the communications apparatus. At this point the user may remove the removable module from the handset and use a charging station to recharge the module. That is, the user may purchase more "air-time" units and store these in the electronic purse on the removable module.

5 This method provides the advantage that the service provider is not responsible for the creditworthiness of the subscriber. Also, the subscriber is able to use a mobile phone on a pay-as-you-use basis and is fully in control of his or her expenditure at any one time. It is not necessary for the whole mobile telephone to be configured for use specifically by one subscriber i.e. the telephone does not have to be configured for one
10 telephone number. This is because the telephone number effectively "travels with" the subscriber within his removable module. When the subscriber moves between geographical regions over which different communications protocols are used the subscriber can simply obtain a new handset, that is preconfigured for the protocol of that area, and insert his removable module into the handset in order to configure that
15 handset for his own personal use. For example, travellers could hire a telephone handset when they enter a new area.

The charging station comprises a recess which is able to accept a removable module and also means for entering "air-time" units onto the electronic purse on the module.

20 As described above, in one embodiment of the invention, some of the functionality from the handset is removed and placed onto the removable module. That is, the handset will typically contain electronic apparatus which will enable the handset to function as a radio communications apparatus when the electronic purse is "charged" and the subscriber identification unit is provided. This means that the handset is hugely
25 more expensive relative to the removable module. However, in one embodiment of the invention, some of the functionality from the handset is removed and instead

incorporated into the removable module or SmartCard. This increases the value of the removable module relative to the handset and may also ensure that the handset will not function without the removable module. Examples of functions that could be removed from the handset include the enabling means, the reading device and other features
5 such as circuitry for converting the speech signal from the user into digital form. These are only examples of functions that could be incorporated into the removable module. Other functions could also be incorporated by making use of conventional circuit design techniques such as would be know to the skilled person in the art.

By making the removable module more expensive with respect to the handset
10 itself, the risk of theft of the handset is reduced and the consequences of theft of the handset are less severe.

In one example, the present invention is made available as an integral component of a customer loyalty programme. The pre-pay mobile telephone is made available to loyalty card holders as an extension of any existing loyalty scheme, on the
15 basis of reward for tenure and spend within the loyalty scheme. Users are able to earn loyalty points on airtime and also to redeem loyalty points against purchase of airtime.

In this example of the invention, the SmartCard for use with the pre-pay mobile telephone handset is also functional as a customer loyalty card. The SmartCard contains an amount of airtime included at the time of purchase and subsequent
20 recharging of the card is possible upon each visit to the loyalty scheme provider's premises.

A number of advantages are provided to the loyalty scheme provider including:

- provision of an "added value" service to existing customers
- ability to attract new customers
- 25 • broad customer availability - no credit rating checks
- rechargeable only at loyalty scheme provider's retail outlet

- minimal overheads and capital expenditure
- use of airtime derives gross revenues prior to month end settlement
- information about customers behaviour patterns is gained

Recharging the removable module

5 Figures 3 and 4 are flow diagrams which illustrate the process of recharging the removable module or SmartCard. When the user needs to recharge his or her SmartCard 34 he or she visits the loyalty provider's premises and at a point of sale till 31 carries out a credit transaction 41, 42 to pay for airtime units to be charged onto the SmartCard 34. After removal from the handset 43 the SmartCard 34 is then inserted
10 44, 45 into a SmartCard reader 33 that is connected to or integral with a secure personal computer 32. The personal computer 32 is connected to a local database 35 which contains information about the user's loyalty card and SmartCard 34. The local database 35 is in turn connected to a remote secure database 36.

 A message 46 is displayed on the screen of the personal computer 32 which
15 indicates the amount of pre-paid air time units that remain on the SmartCard 34. The amount of air time units that are to be credited to the card 34 is then entered onto the personal computer 46 and the personal computer updates the electronic purse in the SmartCard 34 accordingly using an encrypted transaction. The amount of units to be credited to the card can either be entered manually or can be transferred electronically
20 from the till 31 to the computer. The updated amount of pre-paid air time units on the SmartCard 34 is displayed on the computer screen 47 and the SmartCard 34 is then returned to the user or customer 47. Finally the handset is returned to the customer 48.

The encrypted transaction involves the following steps:

1. The secure personal computer obtains secret data that is specific to the
25 SmartCard from the SmartCard itself and/or the local and remote databases and builds an encrypted update command.

2. The software within the card deciphers the encrypted command and updates the airtime counter or electronic purse within the SmartCard.

Such an encrypted transaction is recorded by the personal computer and when a batch of such records are obtained this batch is sent to the remote secure database 36
5 for storage and to update that database.

Initialising the removable module

Each SmartCard contains secure key information which is stored on the card during the manufacturing process. Information about these secure keys is held on the main database 36 and is accessible by the local database 35.

10 When a user first obtains a removable module or SmartCard 34 this is initialised by placing the SmartCard 34 into the card reader 33. Information from the card 34 which identifies the card and provides security information (i.e. the secure key) is read by the card reader 33 and checked by the personal computer 32 using information from the local and/or remote databases 35, 36.

15 If this check is successful the card is authenticated 55 and a screen message asking for loyalty card details to be entered is displayed 55. The loyalty card details are entered 52 to the personal computer 32 and then the card is initialised by the personal computer 53. Details linking the loyalty card details and the secure key are stored on the local and/or remote database 35, 36 and an initial amount of airtime credit is
20 charged to the card. The card is then removed from the reader and returned to the customer 57 in order to be inserted into the customer handset 54.

External fraud detection system

A fraud detection system is provided that is external to the handset and removable module. This is provided in addition to any fraud detection system provided
25 by the network operator. This system monitors traffic made on the pre-paid mobile telephone network and compares this traffic against information about recharging of

SmartCards on the system. For a particular SmartCard, if more traffic is being created than is justified by the amount of credit on that SmartCard then possible fraud is identified. After checks have been made, if it is found that fraud is occurring then the SmartCard is prevented from accessing the network.

5 Figures 6 and 7 show two examples of an external fraud detection system. Pre-paid mobile phone handsets 62 are used to communicate over an operator or service provider's communications network 61. Each time a call is made a call detail record (CDR) is created and stored by the operator 61, as is known in the art. A call detail record contains information about the calling party, the called party, the duration of the
10 call, the time when the call was made and other information about the call. At the end of a certain period of time, for example 12 hours, the call detail records for that 12 hour period are downloaded to database 66,71 in the fraud management system.

 A SmartCard reader 64 or other removable module reader is provided that is connected to a till 63 such that the card reader 64 and till 63 are uniquely matched for
15 security reasons. When a SmartCard or removable module is recharged using the card reader 64 and till or PC 63 information about the recharge is downloaded to a database 65, 71 in the fraud management system. Information about new users from the card initialisation process can also be downloaded. The information can be stored within the local database 35 before being downloaded in batches.

20 In the example shown in figure 6 the fraud detection system comprises two separate databases 65 and 66. One database 66 stores the call detail records and the other 65 stores information about credit data and new users. The information from these two databases is accessed and compared by a processor 67 in order to identify potential fraud cases. The processor 67 generates action requests and reports of
25 fraudulent activity. These outputs can be provided directly to a human operator 69 or

can be sent to the network operator 61. Information from the databases 65, 66 and processor 67 can also be provided to the clubcard database 68.

In the example shown in figure 7 a single database 71 is used which stores information about both call detail records and credit data. The network operator 61 has
5 access to information from this database 71 as shown in figure 7. The database 71 also comprises a processor for analysing the data and producing management reports 73. Real time access 72 to the database 71 can also be provided.

Because there is a time delay whilst data enters the database(s) 71, 65, 66 then the database may state that no credit remains on a particular SmartCard, when in fact
10 the user has recently recharged the SmartCard. Allowance is made for this in order to avoid detecting this situation as a case of fraud. This is described below.

The processor 71, 67 in the fraud management system is arranged to detect a potential case of fraud in situations such as:

- the total number of calls made for a particular SmartCard in a predetermined
15 period exceed a threshold level;
- the total number of units used in a single call exceed a threshold level;
- the number of calls to a free helpline number exceed a threshold level;
- calls have been made by a user who has been barred or for whom a tamper alert has been generated by "in store" card reader systems;
- 20 • if a barred type of call set up is detected such as a call transfer;
- if the number of a certain type of outbound call events generated by a user or group of users exceeds a threshold;
- if the number of inbound verses outbound call events, in a given period, by a user or group of users falls within a certain range.
- 25 • if multiple use of a handset or SmartCard is detected from CDR data; and

- if geographically improbable use of a handset or SmartCard is detected from CDR data.

The interfaces to and from the fraud management system are now described.

Interfaces

- 5 • Imports of Call Detail Records (CDR) data from the network operator are performed on either a chronological push or pull basis at intervals that are viable by the system owner.
- Imports of "credit accumulated" data are performed on either a chronological push or pull basis at intervals that are variable by the system owner.
- 10 • Import of tamper alerts or "excess credit accumulated" general action requests for termination to the network operator.
- Export of management information reports and action requests to external systems located at the operator or at the system owners premises are performed on either a chronological push or pull basis at intervals that are
- 15 variable by the system owner.

The fraud detection system itself is protected from unauthorised access by Firewall Security on call External Data Communications.

Security

- 20 • The fraud detection system is protected from unauthorised access by firewall security on all external data communications.
- Physical access to the system is only possible by authorised personnel who are required to pass security vetting procedures.
- Back up of the system data is performed at regular intervals and back up data is stored at a secure off site location.

Use of handset and removable module to monitor the duration of calls

Because the CDRs are downloaded to the fraud detection system at intervals, such as 12 hourly or 2 hourly intervals, then a time window is present during which fraudulent use of "unpaid for" airtime may occur. In order to reduce this problem the handset and removable module combination is able to monitor call durations during this time window. If more than a threshold level of total call duration is exceeded during this time window than a potential fraud is detected. In this event the communications apparatus is either shut down until the time window has passed or the network operator or security staff are alerted.

This is implemented by incorporating a timer mechanism into the removable module or SmartCard. At the start of a call a pulse signal is sent from the handset to the module and this activates the timer mechanism. At the end of a call another pulse signal is sent from the handset to the module to deactivate the timer. The timer thus monitors total call duration for all calls during a time window, after which it is reset to zero. A processor in the removable module or SmartCard compares the call duration value from the timer against a predetermined threshold and if the threshold is exceeded all outgoing calls are barred for the duration of the time window.

The time window, or exclusion time is set from within the handset/SmartCard combination. At the end of this time normal outgoing call usage is restored and the process counters are reset to zero time.

If the total call duration time as monitored by the handset and module is less than the prescribed threshold then no action is taken to terminate outgoing calls.

Emulation of advice of charging signals

In the situation that no pulses or signals are provided by the network operator which contain information about the current charging rates then the handset and

SmartCard combination is able to emulate these signals. For example, this is required when charging signals are blocked, disrupted or not provided.

A timer mechanism is provided in the handset or in the removable module in order to emulate the charging signals. This timer may be the same as the timer
5 described in the section headed "use of handset and removable module to monitor duration of calls" above. This timer mechanism is activated by signals from the handset which are provided at the start and end of a call. Information about tariff rates is stored in the handset or removable module. For example, this information can be stored in the form of a look up table. Time information from the timer mechanism is then used in
10 conjunction with the tariff information in order to determine the cost of the call. The electronic purse is then decremented accordingly.

Other security features

- The handset is provided with two personal identification number accesses. A first PIN access allows the handset to be activated and a second provides access to sub
15 routings which can change values such as the value of charges or amount of charge time.
- Certain types of call, such as those to 0891 numbers may simply be barred to help prevent fraud.
- A particular handset and removable module or SmartCard are electronically "locked"
20 together during the manufacturing process so that they may only be used in conjunction with each other. This is done by storing a secure key in either or both of the handset and the removable module or SmartCard. The secure key is a cryptogram or other encrypted code. Means for checking that this secure key is present and correct are provided in the handset or removable module. Each
25 handset and module pair is given a unique key so that they will only function fully together. The term "key" is used to refer to stored cryptograms, encoded

information and other electronic keys as well as physical apparatus which ensures that a particular handset can only be used with a module which is able to operate the key.

SmartCard

5 Details about the SmartCard are described below:

Functionality

The SmartCard provides the means for storing an amount of credit in agreed currencies or units of time up to predetermined maximum values, which are variable by secure communication to a SmartCard reader. The credit is debited by the operation of
10 a mobile telephone or by a card reader in a point of sale terminal.

The SmartCard provides control over the mobile Handset functions of:

- Network authentication per the GSM protocols.
- Phone book directory per Handset implementation.
- Short message service.
- 15 • Handset welcome and permanent message display
- Confirm that the credit remaining prior to call set up is above a pre-set threshold value held on the SmartCard, and prevent call set up if below this value.
- Monitor credit remaining for a call in progress, decrement the credit at specific usage rates derived from an advice of charge, (AOC) trigger signal on the signalling
20 channel and interrogate the tariff information stored on the SmartCard. The network operator sends out signals which provide information about the charging rate. Examples of these signals are AOC or CAI (charging advice information). Any such type of signal can be used to enable the credit to be decremented correctly.
- Monitor total duration of calls made in a period and prevent additional calls until this
25 period is expired, excluding all zero rated calls.

- Monitor call in progress duration, provide user warning and tear down when threshold reached.
- Holding pre-determined call limits and monitoring all calls made over a given period, and of a given duration, to allow for call barring should these pre-determined thresholds be exceeded. This is described in detail in the section headed "use of
5 handset and module to monitor the duration of calls"
- The SmartCard is able to place restrictions that allow single language selection only.
- Provide advice of charge (AOC) charging information to the handset, when AOC emulation is used in the handset firmware for those instances where AOC is not
10 presented or supported by the network.
- The SmartCard is able to hold a secure electronic purse function that is capable of managing and controlling units of currency that are stored within it.
- The SmartCard is capable of storing loyalty or other retailer defined units as "points" which may have no monetary value placed upon them. These "points" are
15 redeemable via the SmartCard reader as units to be used in Prepay systems.

Interfaces

- A set of interface protocols are defined for secure transactions between the Handset and the SmartCard, to prevent fraud either through spoofing, or tamper of either the Handset or the SmartCard.
- 20 • A set of interface protocols are also defined for secure transactions between the card reader and the SmartCard, to prevent fraud either through spoofing, or tamper of either the card or the card reader.

Security

- No information generated by the SmartCard to the Handset relating to prepay usage
25 is transmitted to the network by the radio interface or by any other means.

- The SmartCard is capable of detecting unauthorised tampering and ceases to function until returned to a card reader and reactivated. For example, if the wrong personal identification number is entered three times during the card validity check process.
- 5 • The SmartCard protocols prevent no more than 3 unauthorised actions to access any secure area before complete termination of the SmartCard functions.
- A limited number of master SmartCards may be provided for use by point of sale operators, issued under strict controls in store.
- A number of secure access modules (SAM's) for use in the card readers at point of
10 sale can be provided. A SAM is a fixed SIM which contains cryptograms for accessing the identity or secure key information from the SmartCards.

The SmartCard:

- Allows remote disablement of the Handset and SmartCard upon authenticated request by the network or by the card reader.
- 15 • Allows remote enabling of the Handset and SmartCard upon authenticated request by the network or by the card reader in combination with user PIN entry.
- Does not allow re-enablement of the SmartCard once it has been disabled.
- Allows remote individual update of the threshold values held in the SmartCard, either by the card reader or over the network.
- 20 • Does not allow manual user reset of the Advice of charge indicators via the Handset, or access to PIN2 of the handset.
- Does not suffer any electrical or physical damage if withdrawn from the Handset or Card reader, while power is applied. The SmartCard retaining unit, in one embodiment, has retaining pins that are close together. The retaining unit is
25 specially designed such that these pins do not flex and contact each other, so creating a short circuit.

- Is delivered pre-registered with the network operator but not activated for use. Activation is only possible via the Card Reader.
- Permits Incoming calls when the credit has expired.

Standard Functions NOT required on the Card

5 Standard functions that are not required on the SmartCard, such as phone book options can be removed in order to make room for extra filters or algorithms for coding or decoding encrypted information.

- Phone Book Options

Form factor

- 10 • The SmartCard can be a full size SIM, mini SIM adapter based alternatives are also possible.
- The SmartCard can be delivered with a surface finish or other orientation mark to assist in identification of its correct insertion for visually impaired users.

Appearance

- 15 • The SmartCard can be capable of accepting various finishes e.g. silk screen printing for branding.
- In one embodiment each SmartCard is individually marked with a machine readable bar code and human readable serial number. Records of all SmartCard serial numbers and their distribution can then be kept.

20 SmartCard Reader

Functionality

The SmartCard reader:

- 25 • Allows SmartCards to be activated for first use and recharged with credit on a periodic basis. Allows SmartCards to be deactivated by the operator or automatically upon detection of tampering within the SmartCard by the SmartCard reader system.

- Allows the operator to read from a SmartCard remaining credit on a card inserted in the reader.
 - Captures and temporarily stores the credit held on the card and the subscriber phone number to allow transfer to a replacement card.
- 5
- Allows transfer of credit remaining on the SmartCard to a new card or to a secure external system for point of sale transactions.
 - Is intuitive to use by semiskilled checkout operators with a minimum of training, and employs the use of icons to indicate functions where possible.
 - Is easily serviced by trained personnel, with a good supply of replacement parts and
- 10
- spares.
 - The SmartCard reader allows a secure sign-on process at power on, user log on and log off. This process involves the use of master SmartCards coupled to PIN number entry.
 - The SmartCard reader is capable of maintaining the system clock function to allow
- 15
- for daylight saving.
 - The SmartCard reader is capable of recording the operator name and sign on/off date/times.
 - The SmartCard reader has a supervisor login password for password administration.
 - The SmartCard reader is able to hold a secure terminal key to identify each Card
- 20
- reader to the database to show where credit records have been generated.
 - The SmartCard reader does not allow any new transactions to be made whilst, data is being transferred to the fraud detection system or remote database.
 - The SmartCard reader is capable of creating batches of credit records with incrementing batch numbers.
- 25
- The SmartCard reader is capable of holding the previous 20 batches of credit records.

- Is capable of displaying simple text messages to prompt actions from operators to perform the following tasks:

1. Authenticate new Card
2. Apply credit to card
- 5 3. Transfer credit between authenticated Cards
4. Terminate Card after Credit transfer or discovery of fraudulent use.

Interfaces

- The card reader shall allow interaction to a PC or Point of Sale terminals via either a serial RS232 or other industry standard data transfer interface. The data transferred
10 is encrypted according to a predetermined protocol.
- The card reader system allows remote polling of the system by an external data device, such as the fraud detection system, via modem dial up communications or network connection. This modem can be internal to the card reader system.
- The card reader system initiates communications with the external data device upon
15 command by the program contained in the card reader system.
- The SmartCard reader is dismountable from a host PC if supplied as a separate unit, with minimal requirement for special tools or specialist knowledge by service personnel.
- The card reader is capable of arithmetically deriving SmartCard self identification or
20 SRES based on algorithms held on a mini SmartCard held within the unit.
- The card reader unit is capable of supporting internal readers for plug-in SmartCards conforming to current industry standards.
- The card reader is capable of supporting a main card reader that takes full size cards. This reader has the following characteristics:
25
 - Push-pull reader with landing contacts;
 - MTBF of 250,000 insertion cycles (minimum);

- Interface deactivation according to ISO 7816/3;
- Active short circuit protection for the SmartCard;
- The unit is capable of supporting industry standard protocols, for communication between the SmartCard and the reader, including Asynchronous protocols: T=0,
5 T=1;
- The unit has sufficient memory capabilities to support the requirements of the data capture and transfer routines.
- The unit is capable of supporting industry standard programming languages that are downloadable over an RS232 interface.
- 10 • The card reader system is capable of supporting common point of sale (POS) protocols to accept data transfer from POS systems to allow for updating of the values to the SmartCard.

Security

- The SmartCard reader communications with any external data device are encrypted.
- 15 • The SmartCard reader is capable of providing PIN controlled access to all of its functionality including initial access to the screen prompts prior to any form of authentication or credit related actions.
- The SmartCard reader protocols allow no more than 3 unauthorised actions to access any secure area before complete termination of the SmartCard functions.
- 20 • The SmartCard reader can detect unauthorised tampering of the SmartCard and causes the SmartCard to cease to function, in this situation.
- The SmartCard reader system software is protected from unauthorised access by either the use of PIN protection only or by the use of PIN protection and a system specific mini SmartCard being read before access to the program is granted.
- 25 • Data held on the card reader system is only transferable to other systems or devices upon the entry of security codes or devices as described previously.

Form factor

- The SmartCard reader is capable of accepting full size SmartCards and/or mini SIM's held within full size card adapters.
- 5
- Secondary card readers are provided to accept mini SIM
 - The SmartCard reader has an integral display capable of displaying either text or icons to prompt the operator.
 - The SmartCard reader is of a compact size, suitable for co-location with a POS terminal or PC on a customer services desk within a retail store.
- 10
- If the SmartCard reader system consists of a PC and card reader, the overall footprint (or size of the system on the desk) does not exceed that of a standard desktop PC. Any screen used in this configuration is not larger than 12" and ideally forms a single unit with the card reader and processor.

Environmental

- 15
- The SmartCard reader system supports dual voltage input and is suitable for installation in a number of European countries, with conformance to all relevant environmental requirements e.g. EMC, Noise, Operator ergonomics etc.
 - The unit is capable of being hard wired to power supply units (including UPS systems)
- 20
- All data, power, telephony communications, and internal SAM connections are capable of being secured in place to prevent unauthorised disconnection of any service.
 - The unit can have battery back-up capabilities.

Handset

Functionality

The Handsets used in this project provide the following functionality:

- 5 • Be driven by a SmartCard developed for the Handset so as to provide feedback to a user of the service of the credit remaining on the SmartCard, via the Handset display.
- The Handset display shows the amount of credit available at the start of each call, the end of each call, and by quick access via a hot key sequence. This display is in
10 minutes, viz "Time remaining =? Minutes".
- The Handset is capable of emulating AOC information when none is presented by the network for reference by the SmartCard for charging information purposes.
- Allow calls to predefined numbers held on the card, eg Emergency services and help line number(s) without debiting the credit on the card. The help line number(s)
15 may be allowed a pre-set number of transactions per period at which point additional use is denied until the period is expired.
- The extended menu option which gives access to PIN2 is set to the "OFF" position.
- Allow remote enabling of the Handset and SmartCard upon authenticated request by the network, in combination with user PIN entry.
- 20 • Allow remote individual update to the threshold values held in the SmartCard over the network.
- Provide speed dial access to the network operator's voice mail system.
- Call waiting, call swap (in which a call is transferred to another number) and call hold are allowed as long as any outbound call in progress continues to decrement the
25 credit on the SmartCard. The SmartCard allows the barring of calls by Calling Party Category (CPC).

- The Handset does not allow manual user reset of the Advice of charge indicators via the Handset, or access to PIN2.
- Roaming is not allowed by the Handset.
- The language default, ie the ability to access other network providers original is set to "English".
- The display is capable of displaying an alternating message in the style of "Emergency/Hotline Calls ONLY" and "Operator Name" when credit has expired.
- The display is capable of displaying the operator PLMN code rather than the operator name.
- Line 2 (ie a second line in a call swap) is not supported by the Handset.
- The Handset has the menu functions and associated GSM instruction sets removed or deleted, prior to despatch, for the following call types and menus:
 - Call Transfer;
 - Call forwarding (except Voice Mail);
 - Conference/Multiparty call set up;
 - Roaming facilities;
 - Restricted Dial lists;
 - Sub menu "Bar all incoming calls when roaming";
 - Call divert and sub menus;
 - Select phone line;
 - Call Charge settings;
- The purpose of this is to reduce fraud and costs. Also the space in the Handset that is otherwise used for these functions can be used for other things.
- In addition, the following call types and menus are removed because they cannot be provided by the pre-paid mobile phone system.
 - Change Greeting;

- All access to SIM memory for:
 - SMS;
 - Phonebook;
 - Capacity add or delete;
 - 5 • Copy functions;
 - One touch dialling;
 - Fixed Dialling;
 - Phone Status;
 - Network Selection;
 - 10 • Call Meters;

Also:

- The Master Reset or Clear functions are not able to reset or enable any features barred from use.
- Emergency 999/112 calls are allowed without a SmartCard being inserted into the
15 Handset or when credit has expired.
- The Handset is capable of providing a user configurable decrement warning to indicate unit usage, in both visual and audible formats.
- The Handset is capable of providing a "Credit nearing expiry, please recharge" warning to the user in both visual and audible formats.
- 20 • The Handset is capable of providing a user warning and also of "tearing down the call" when credit is expired or when a threshold configurable via the card reader or over the radio interface is reached.
- The Handset is capable of providing a "Credit expired, please recharge", warning to the user in both visual and audible formats, and prevent call set up being activated
25 except for emergency and helpline calls.

- The Handset supports voice calls and the Short Message Service. It supports restricted dialling, phone book, and diverts to voice mail.
- The default Caller line Identifier condition is set to "Present".
- The Handset is capable of being locked to a single network operator and to the SmartCard. These locks are not user addressable under any circumstances.
- The Handset has good standby battery life, in excess of 40 hours and talk time in excess of 90 minutes.
- The Handset supports one number dialling to the network voice mail service.
- The Handset display is easy to read and supports icons as well as text.
- The Handset is capable of supporting calls to pre-determined help line numbers on a toll free basis.
- The Handset manufacturer is able to unlock a SmartCard from its Handset in the repair centre. This is necessary if, for example, the Handset breaks when there is a large amount of credit on the SmartCard.
- The Handset permits Incoming calls when credit has expired.

Interfaces

- The Handset user interface is intuitive to the novice user and presents information in a logical and clear fashion. The use of multiple level menu access for the most common activities is avoided. Integral context sensitive user help is desirable.
- The Handset can support interfaces to data cards for connection from modem or laptop for example, and may have a connection for external power supplies.
- The Handset supports full size SIM cards and ideally contains a SIM release mechanism such that the user does not need to disassemble the Handset or battery to remove the SIM for recharging.
- The SIM does not suffer any harm due to withdrawal of the SIM while the Handset is switched on.

- The SIM to Handset interface supports insertion of the card with a duty cycle in excess of 5000 insertions before any degradation of the interface to the SIM is observed.

Security

- 5 • The Handset allows the suppression of access to PIN2 and other Handset menu functions by means of instruction from the SmartCard.
- The access control features are not addressable by the user from the Handset user interface, except for PIN1.
- The Handset has intrinsically good security to prevent unauthorised access to the data transfer between the SmartCard and the Handset.
- 10 • The physical design of the Handset is arranged to deter tamper or access to the contacts of the SIM. Ideally any attempt at access to the interior of the Handset leads to the destruction of the Handset.
- Preferably SIM card extenders which enable manipulation of a SIM card by keeping it outside the Handset cannot be with the Handset, when in operation.
- 15

Form factor

- The Handset supports full size SIM cards.
- The Handset is of a compact design and subject to evaluation on the basis of appearance, layout, clarity of markings, innovative features, user friendliness, audio quality etc.
- 20
- The Handset is of robust construction and provides good ergonomic operation to the user both in call set up and during a call.

Environmental

- The Handset is capable of being marked with branding marks, on the front or on the keypad cover as appropriate.
- 25

Accessories

- A full range of accessories including car kits, desk top chargers, desktop hands free kits, data cards (if appropriate) and a range of battery options, can be used with the Handset.
- 5 • The Handset is supported by a manufacturer's User Guide, Frequently asked Question and Answer sheets.

Operational requirements

- The network supports advice of charge (AOC) or other suitable systems which can be used to decrement credit held on the prepay SmartCards.
- 10 • The network is capable of setting the AOC decrement interval to 10 seconds at delivery and can allow this interval to be configurable over the radio interface to the Handset.
- The network supports remote enabling and disabling of the Handset and SmartCard via authenticated request by the network to the Handset in combination with user
- 15 PIN entry.
- The network is capable of monitoring the destinations of calls initiated and restrict calls to predefined destinations by National Number Group.
 - The network is capable of barring all calls to premium or international destinations.
 - The network is capable of preventing call transfer, call forwarding (except to voice
- 20 mail), conference calls or any non standard or basic call types from being initiated.

The network is capable of allowing Data calls and Short Message Service (SMS) calls on the basis that these are charged at the same rate as voice calls. If this is not possible inbound data and SMS calls only are allowed. The network should be capable of barring these outbound calls if charging on the above basis is not possible.

Rating and tariff requirements

- A tariff or look up table to be stored in the SmartCard to generate AOC information to the Handset on the basis of flat rate charging is required from the operator.
- The network operator provides the facility to zero rate calls to specified numbers
5 such as helpdesk numbers and emergency calls.
- Over time other tariffs may be introduced, and the network operator is able to support the introduction of new tariff plans via AOC in reasonable time scales.
- Call Detail Records (CDR) produced within the network by use of the present
10 invention are segregated from the operator's other traffic and moved to a secure area for export to the fraud detection system. The frequency of the collation and export of the CDR data shall not exceed 12 hours and may be as frequent as hourly.

15

Claims

1. A portable radio communications apparatus comprising:
 - (i) a portable handset;
 - (ii) a removable module comprising a rechargeable electronic purse and a subscriber
5 identification unit;
 - (iii) a recess in the handset adapted to accept the removable module;
 - (iv) a reading device in the handset adapted to determine a content of the electronic
purse;
 - (v) an enabling means arranged to allow substantial operation of the communications
10 apparatus on the basis of the content of the electronic purse;
and wherein said module is adapted such that in use the communications apparatus is
substantially inoperable when the module is removed.
2. A portable radio communications apparatus as claimed in claim 1 wherein the
removable module comprises a SmartCard.
- 15 3. A portable radio communications apparatus as claimed in claim 1 or claim 2
wherein the subscriber identification unit comprises a conventional subscriber
identification module.
4. A portable radio communications apparatus as claimed in any preceding claim
wherein said handset and said removable module are electronically locked such that a
20 particular handset and module pair only function fully together.
5. A portable radio communications apparatus as claimed in claim 4 wherein said
handset and said removable module contain information about a secure key that is
unique to a particular handset and removable module pair.
6. A portable radio communications apparatus as claimed in any preceding claim
25 which further comprises a timer mechanism adapted to monitor call duration, said timer

mechanism being adapted to be activated by signals from the handset at the start of a call.

7. A portable radio communications apparatus as claimed in claim 6 which further comprises a store of information about costs and a processor adapted to decrement the
- 5 electronic purse on the basis of the cost information and the monitored call duration.
8. A portable radio communications apparatus as claimed in claim 6 which further comprises a processor adapted to compare the monitored call duration with a prespecified threshold value and to bar outgoing calls in the event that the threshold value is exceeded.
- 10 9. A communications network comprising at least one portable radio communications apparatus as claimed in any preceding claim.
10. A communications network as claimed in claim 9 comprising a fraud detection system, said fraud detection system comprising database means for storing information about calls made from the handset over the communications network, and information
- 15 concerning the number of airtime units credited to the electronic purse associated with said portable radio communications apparatus.
11. A communications network as claimed in claim 10 wherein said fraud detection system further comprises a processor adapted to compare the information about calls and the information about electronic purse contents.
- 20 12. A removable module suitable for use with a portable radio communications handset said module comprising a rechargeable electronic purse and a subscriber identification unit, said module being adapted to be received in a recess in said handset, and wherein said module is adapted such that in use the handset is substantially inoperable when the module is removed from the communications apparatus.
- 25 13. A removable module as claimed in claim 12 which contains information about a secure key that is unique to the particular removable module and its handset pair.

14. A removable module as claimed in claim 12 or claim 13 which comprises a timer mechanism adapted to monitor call duration said timer mechanism being adapted to be activated by signals from the handset at the start of a call.
15. A removable module as claimed in any of claims 12 to claim 14 which further
5 comprises a store of information about costs and a processor adapted to decrement the electronic purse on the basis of the cost information and the monitored call duration.
16. A removable module as claimed in any of claims 12 to claim 15 which further comprises a processor adapted to compare the monitored call duration with a prespecified threshold value and to bar outgoing calls in the event that the threshold
10 value is exceeded.
17. A recharging system adapted to recharge an electronic purse of a removable module as claimed in any of claims 12 to 16.
18. A recharging system as claimed in claim 17 comprising a reader adapted to read the contents of the electronic purse and means for sending an encrypted update
15 message to the removable module in order to update the electronic purse.
19. A recharging system as claimed in claim 17 or claim 18 comprising at least one database of stored subscriber information and means for comparing the subscriber identification unit with said stored information.
20. A recharging system as claimed in claim 19 comprising at least one local
20 database and at least one remote database.
21. A recharging system as claimed in any of claims 17 to 20 wherein said reader and means for sending an encrypted update message to the removable module are connected to a point of sale apparatus.
22. A recharging system as claimed in claim 21 wherein said reader and said means
25 for sending an encrypted update message to the removable module are electronically locked to the point of sale apparatus.

23. A portable radio communications handset adapted for use with a removable module as claimed in any of claims 12 to 16, said handset comprising a recess adapted to accept the removable module; and a reading device adapted to determine a content of an electronic purse in the removable module.
- 5 24. A portable radio communications handset as claimed in claim 23 wherein said handset is adapted to send a signal to the removable module at the start and end of a call.
25. A portable radio communications handset as claimed in claim 23 or claim 24 wherein said handset contains information about a secure key that is unique to the
10 particular handset and its removable module pair.
26. A method of communicating using a portable radio communications apparatus as claimed in any of claims 1 to 8 said method comprising the steps of :
- (i) purchasing air time from an air time provider or suitable intermediary;
- (ii) charging said electronic purse with units equivalent to purchased air time;
- 15 (iii) inserting the removable module incorporating the electronic purse into the recess in the handset;
- (iv) determining a content of the electronic purse;
- (v) allowing substantial operation of the communications apparatus on the basis of the content of the electronic purse;
- 20 (vi) operating the communications apparatus and updating the content of the electronic purse on the basis of said operation.
27. A method as claimed in claim 26 wherein said step of updating the content of the electronic purse involves transmission of encrypted messages between the handset and removable module.

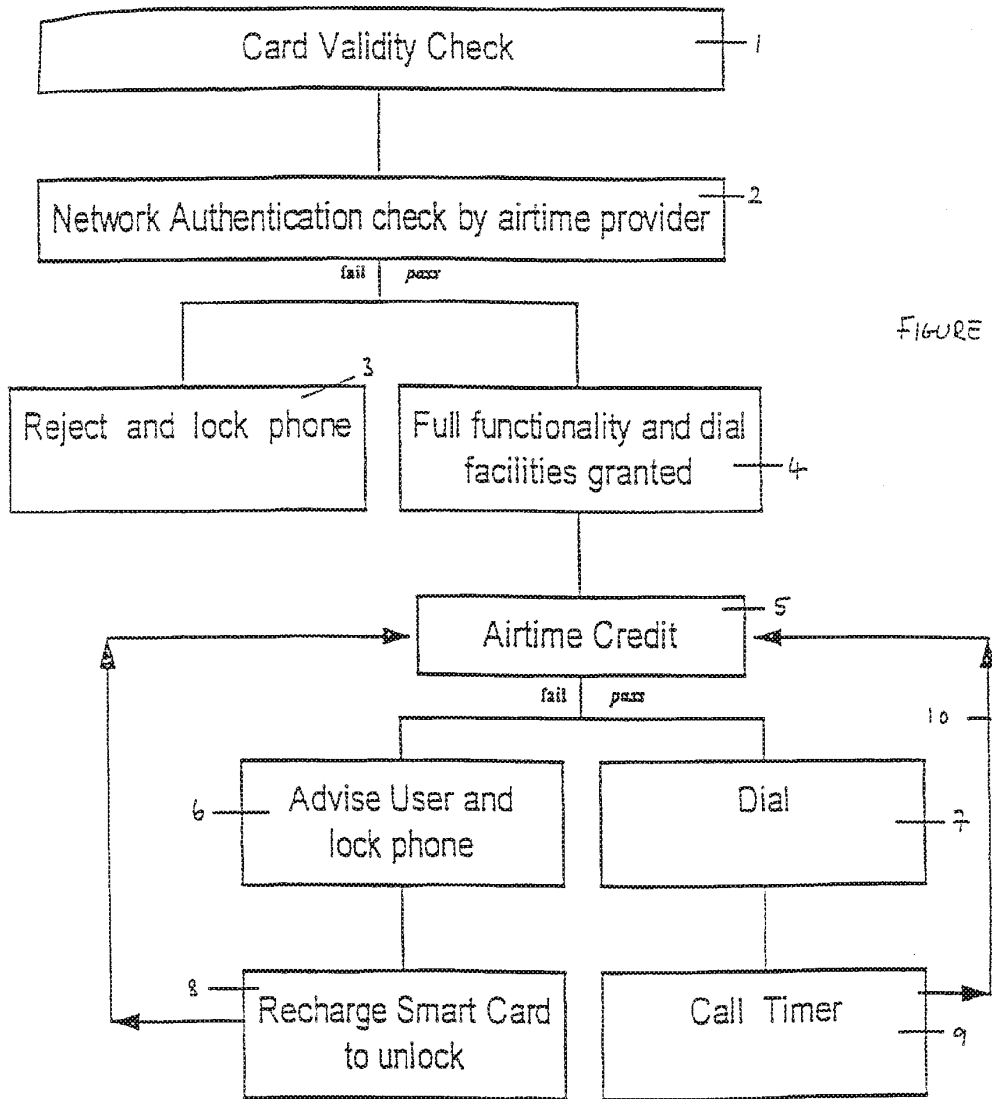


FIGURE 1

2/7

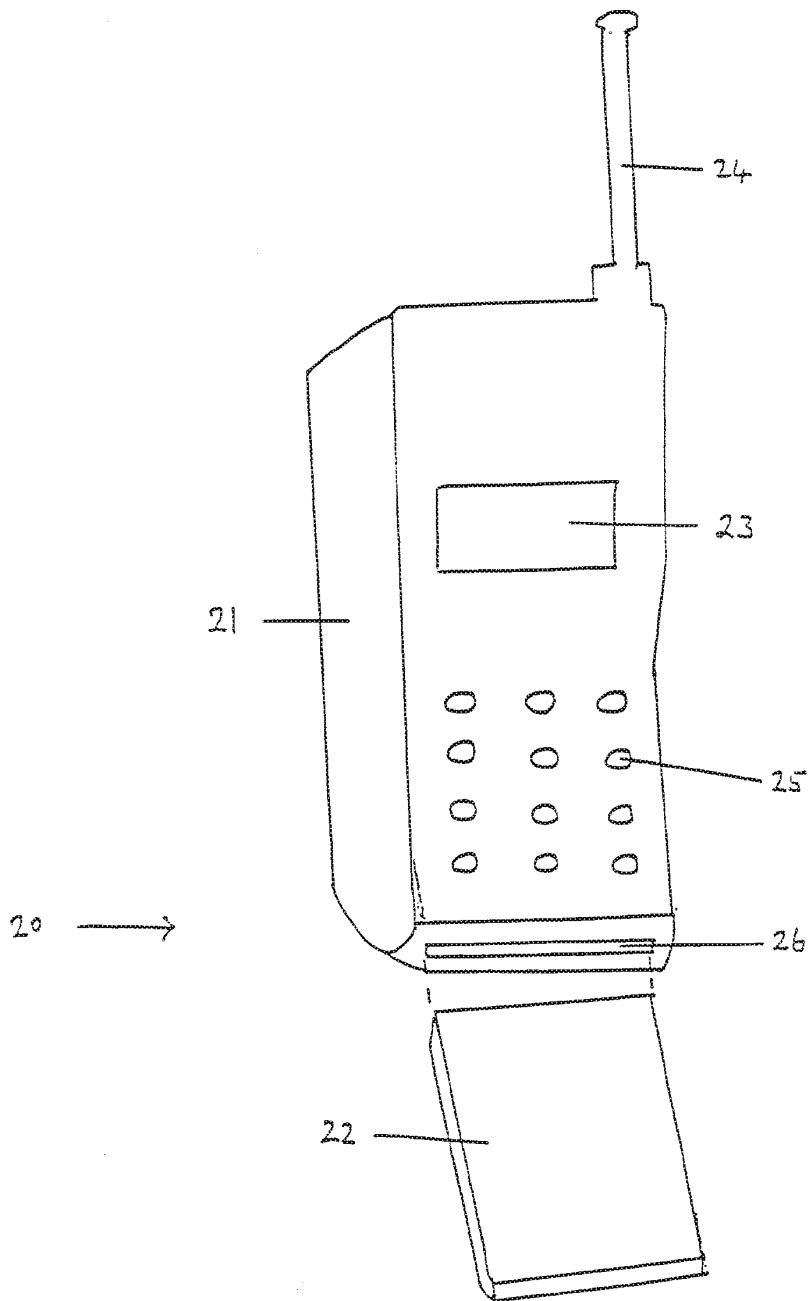


FIGURE 2

SUBSTITUTE SHEET (RULE 26)

Pre Paid credit Charging

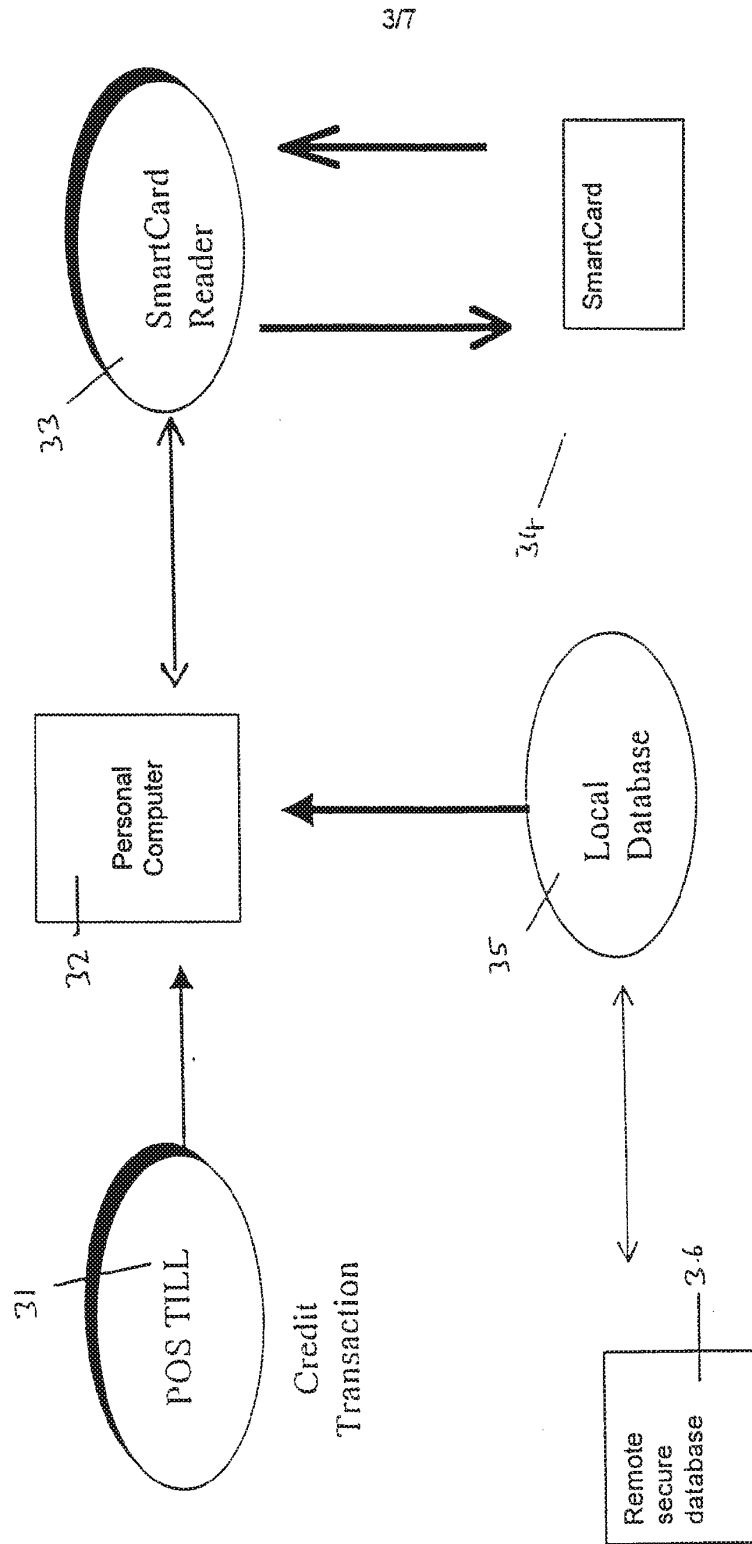


FIGURE 3

Credit Recharge

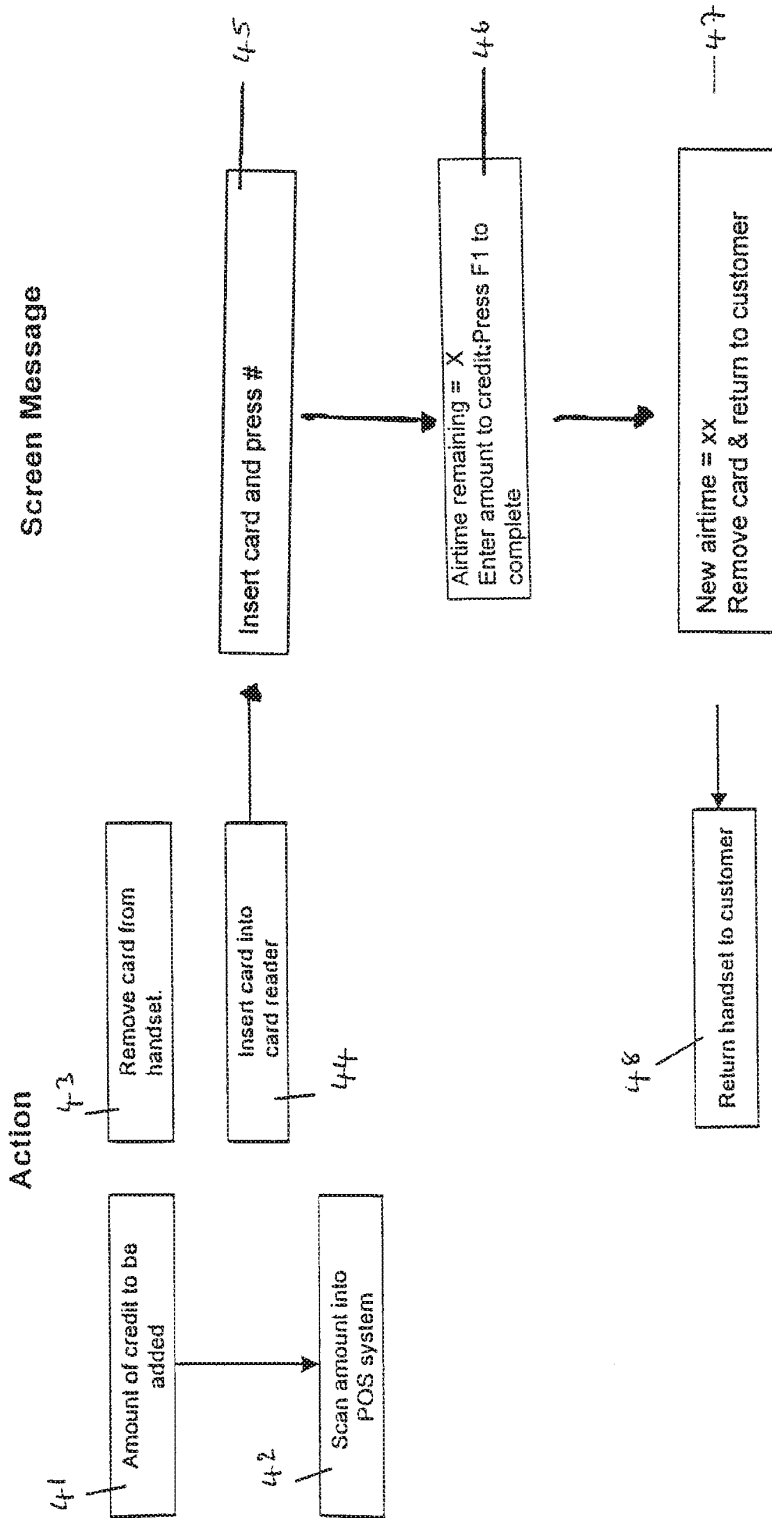


FIGURE 4

Card Initialisation

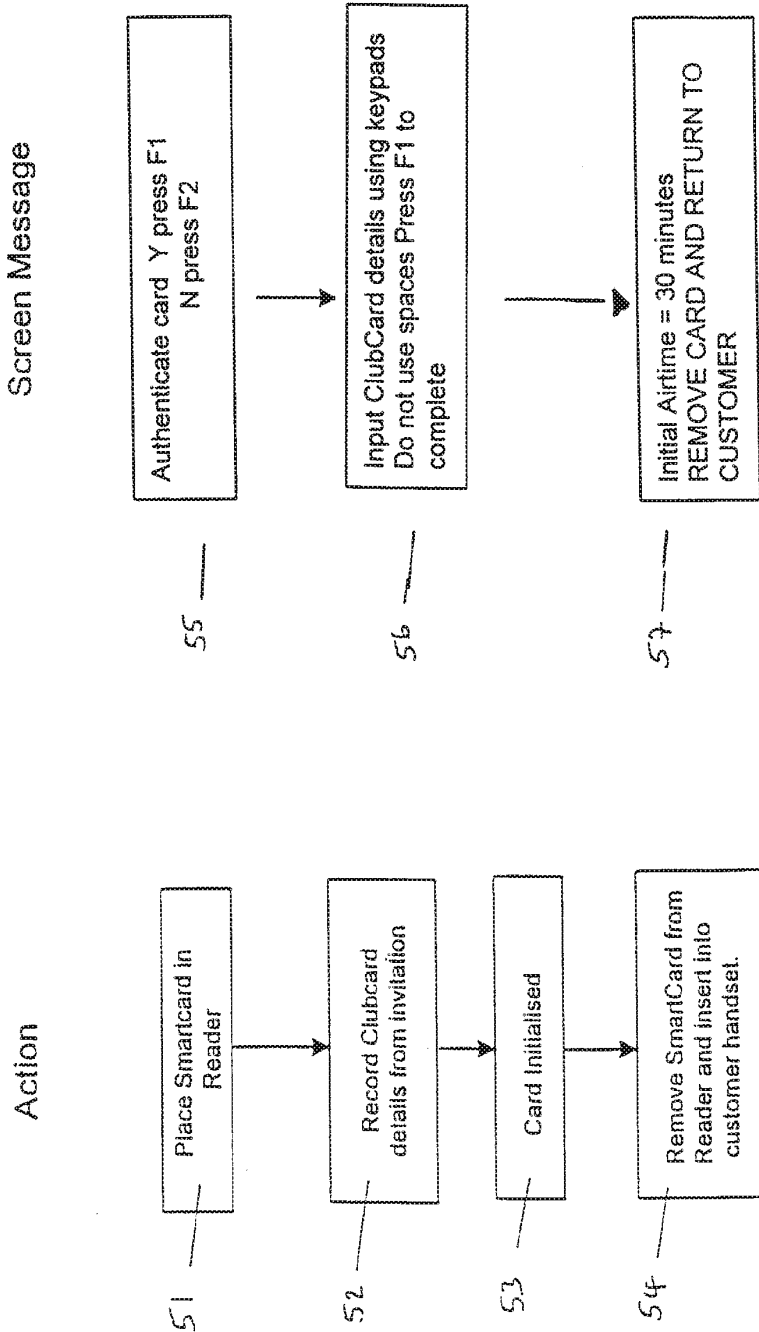


FIGURE 5

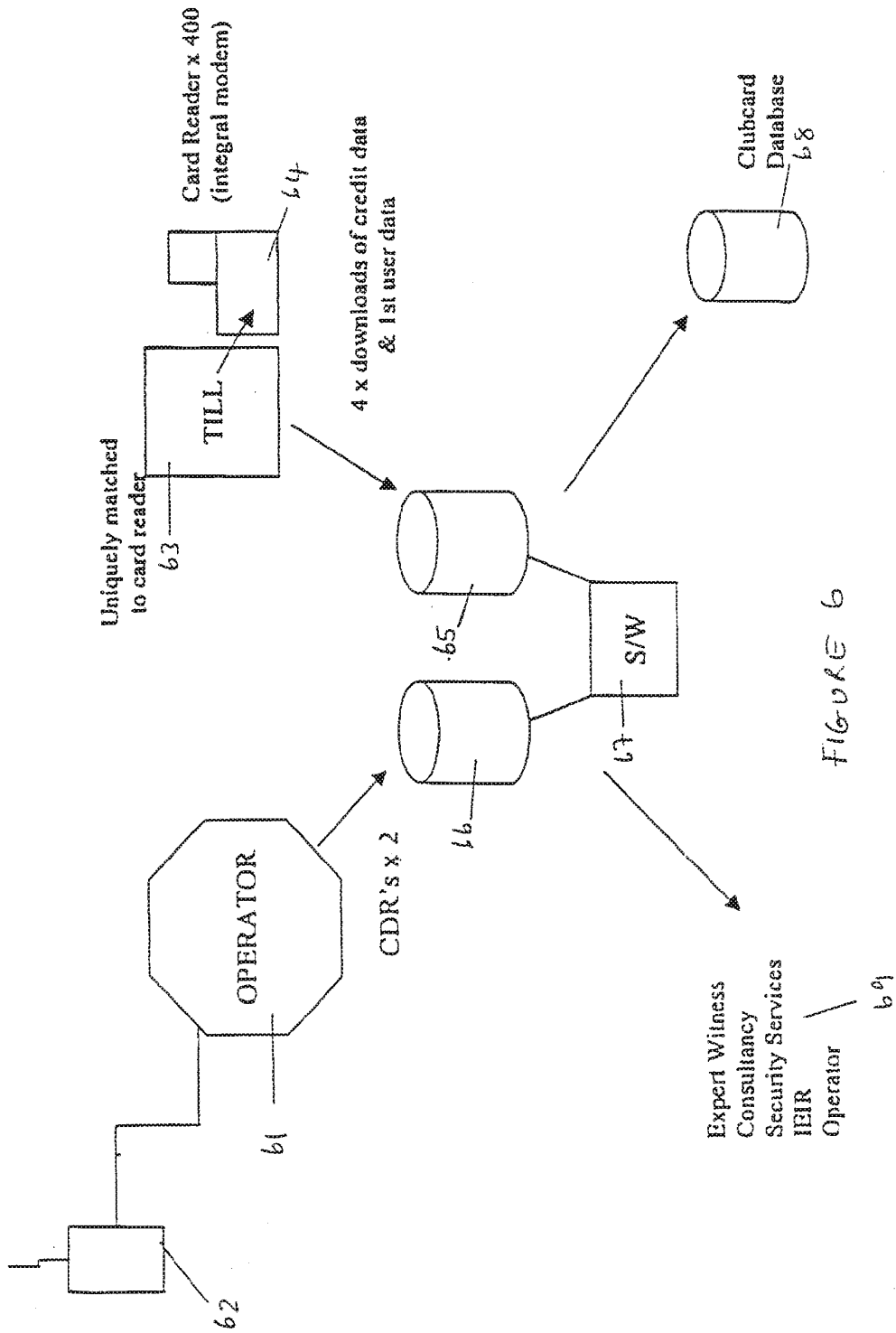


FIGURE 6

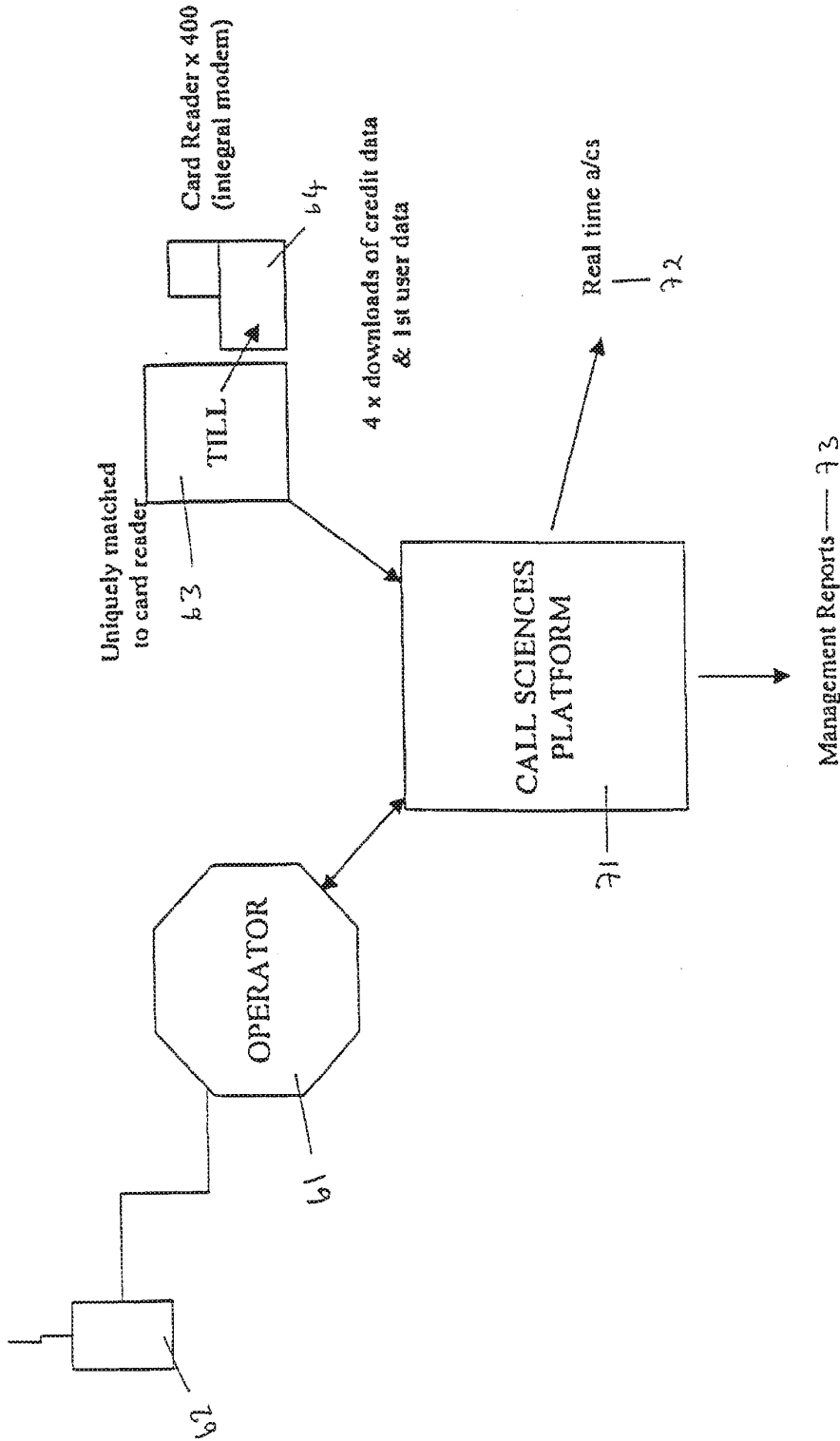


FIGURE 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 98/02729

A. CLASSIFICATION OF SUBJECT MATTER IPC 6 H04M17/00 H04Q7/32				
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) IPC 6 H04M H04Q				
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched				
Electronic data base consulted during the international search (name of data base and, where practical, 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.		
X	EP 0 790 587 A (PHILIPS ELECTRONICS NV) 20 August 1997	1-3, 6-9, 12, 14-17, 23, 24, 26, 27		
A	see column 3, line 26 - column 4, line 21	10		
X	WO 95 28062 A (NOKIA TELECOMMUNICATIONS OY) 19 October 1995 see page 3, line 1 - page 4, line 5 see page 8, line 24 - page 10, line 3 see page 11, line 35 - page 13, line 16 ----- -/--	1-3, 6-9, 12, 14-17, 23, 24, 26		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.				
<input checked="" type="checkbox"/> Patent family members are listed in annex.				
* Special categories of cited documents :				
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none; vertical-align: top;"> "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "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) "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 </td> <td style="width: 50%; border: none; vertical-align: top;"> "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 "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 "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. "&" document member of the same patent family </td> </tr> </table>			"A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "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) "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	"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 "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 "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. "&" document member of the same patent family
"A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "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) "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	"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 "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 "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. "&" document member of the same patent family			
Date of the actual completion of the international search <p style="text-align: center;">16 December 1998</p>		Date of mailing of the international search report <p style="text-align: center;">29/12/1998</p>		
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer <p style="text-align: center;">Neves Appelt, D</p>		

1

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 98/02729

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
X	<p>GB 2 308 528 A (KARAGOEZLUE IBRAHIM MURAT ;RAMIS HARRY (GB)) 25 June 1997</p> <p>see abstract see page 4, line 1 - page 6, line 27 see page 11, line 26 - page 12, line 22 see page 14</p>	<p>1-9, 12-17, 23-27</p>
A	<p>US 5 577 109 A (STIMSON CHARLES J ET AL) 19 November 1996 see column 1, line 59 - column 3, line 6</p>	<p>17-22</p>
A	<p>GB 2 267 794 A (CONROY ALAN KILPATRICK) 15 December 1993 cited in the application</p> <p>see page 3</p>	<p>1,2,5,9, 12,13, 17,23, 25,26</p>
A	<p>WO 97 05729 A (TELECOM ITALIA MOBILE S P A ;SENTINELLI MAURO (IT)) 13 February 1997 cited in the application see page 6 - page 7</p>	<p>1-3,6,7, 9,12,14, 15,23,26</p>

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/GB 98/02729

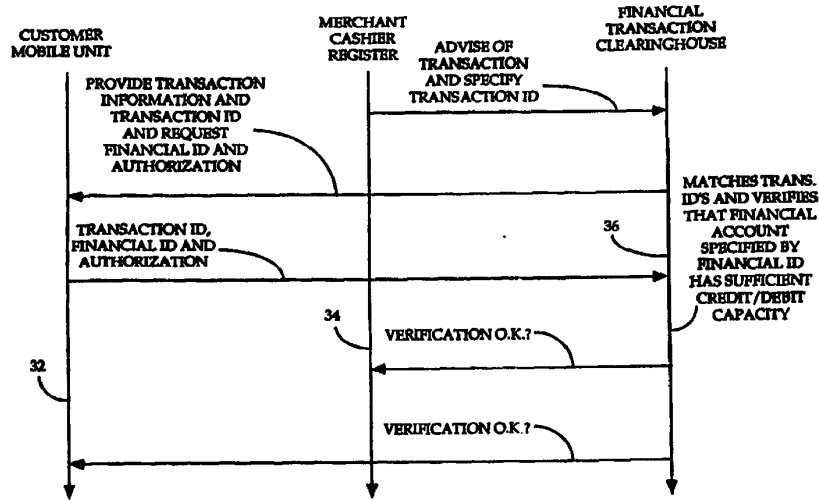
Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0790587 A	20-08-1997	FR 2744822 A CN 1168609 A JP 9233541 A	14-08-1997 24-12-1997 05-09-1997
WO 9528062 A	19-10-1995	AU 691604 B AU 2216795 A CN 1151240 A EP 0754394 A FI 963996 A JP 10501931 T US 5748720 A	21-05-1998 30-10-1995 04-06-1997 22-01-1997 05-12-1996 17-02-1998 05-05-1998
GB 2308528 A	25-06-1997	NONE	
US 5577109 A	19-11-1996	US 5511114 A AU 2770795 A CA 2192310 A WO 9534161 A US 5721768 A	23-04-1996 04-01-1996 14-12-1995 14-12-1995 24-02-1998
GB 2267794 A	15-12-1993	NONE	
WO 9705729 A	13-02-1997	IT RM950521 A AU 6667896 A CA 2227340 A CN 1192308 A CZ 9800233 A EP 0840973 A NO 980341 A PL 324646 A	27-01-1997 26-02-1997 13-02-1997 02-09-1998 15-07-1998 13-05-1998 26-03-1998 08-06-1998



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : G07F 19/00, H04M 17/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 98/34203 (43) International Publication Date: 6 August 1998 (06.08.98)</p>
<p>(21) International Application Number: PCT/US98/01391 (22) International Filing Date: 27 January 1998 (27.01.98) (30) Priority Data: 791,530 30 January 1997 (30.01.97) US (71) Applicant: QUALCOMM INCORPORATED [US/US]; 6455 Lusk Boulevard, San Diego, CA 92121 (US). (72) Inventors: JACOBS, Paul, E.; 9075 La Jolla Shores Lane, La Jolla, CA 92037 (US). BELK, Jeffrey, K.; 13967 Arbolitos Drive, Poway, CA 92064 (US). (74) Agents: OGROD, Gregory, D. et al.; Qualcomm Incorporated, 6455 Lusk Boulevard, San Diego, CA 92121 (US).</p>		<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>

(54) Title: METHOD AND APPARATUS FOR PERFORMING FINANCIAL TRANSACTIONS USING A MOBILE COMMUNICATION UNIT



(57) Abstract

Financial identification codes (ID's) are stored directly within a mobile communications unit (12) such as a mobile telephone or other device provided with wireless telephony capability such as a personal data assistant, a laptop computer, a dedicated Internet access device, or electronic organizer. The financial ID's represent credit or debit accounts, digital money or other financial entities. Storage of financial ID's within such devices allows the various financial ID's of credit (28) and debit accounts (30) of a customer or of digital money to be consolidated and used efficiently. The ID's are transmitted by radio or infrared signals to a merchant (14) or other party to enable quick and efficient transactions such as purchase transactions. Radio transmission is particularly advantageous for conducting transactions during a mobile telephone call which might otherwise require verbally reciting the financial ID of a credit or debit account.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

METHOD AND APPARATUS FOR PERFORMING FINANCIAL TRANSACTIONS USING A MOBILE COMMUNICATION UNIT

BACKGROUND OF THE INVENTION

I. Field of the Invention

The invention generally relates to mobile communication units such as mobile telephones and to devices for implementing financial transactions.

II. Description of the Related Art

Consumers increasingly use credit cards, debit cards (such as automated teller machine (ATM) cards), and the like for performing financial transactions with merchants to purchase goods or services. Typically, the consumer provides the credit or debit card to the merchant who runs it through a card scanner to read out a financial identification (ID) associated with the card. The financial ID and the cost of the goods or services are forwarded over a telephone network (such as the public switched telephone network PSTN) to the bank or other entity providing the credit for the credit card or maintaining the money associated with the debit card. The bank verifies that there is sufficient credit or debit capacity for the transaction and forwards verification to the merchant. The consumer then is typically asked to sign a receipt for the purchase and the transaction is thereby completed and the goods or services are conveyed to the consumer.

Among the advantages of this common type of financial transaction is that the consumer need not carry significant amounts of cash for making purchases and may take advantage of any credit granted to him or her. Disadvantages, however, remain. Consumers typically carry numerous credit and debit cards which can be lost or stolen and are often left accidentally with the merchant. Moreover, the financial ID associated with the card is typically recorded on a magnetic strip on the back of the card which can be accidentally erased or otherwise rendered unreadable. Often, purchases are made using credit or debit accounts over the telephone. In such case, the customer must read the financial ID for the account aloud and the merchant must transcribe the financial ID. This is, at best, a tedious and time consuming process and frequent errors occur in reading or transcribing the financial ID's. Moreover, the financial ID may be captured by

unauthorized parties by eavesdropping. Indeed, the party representing itself as the merchant may merely be fraudulently obtaining financial ID's without intending to provide any goods or services. If the purchase is initiated over the Internet, the financial ID is typically conveyed over the Internet via computer transmission signals which again are subject to eavesdropping.

Accordingly, it would be desirable to consolidate all of the financial ID's associated with all of the credit and debit cards of a consumer in a single device not subject to magnetic erasure thereby minimizing the likelihood of misplacing one of the cards and eliminating the risk of having the financial ID accidentally erased. It would also be desirable to consolidate the financial ID's in a device allowing the ID's to be transmitted efficiently such that the financial ID need not be read and transcribed verbally and allowing the financial ID's to be transmitted in an encrypted or otherwise protected form to minimize the risk that the financial ID's may be captured by eavesdropping. Aspects of the invention are directed to solving these and other problems.

To partially address some of these problems, it has been proposed to store the financial ID of a particular credit or debit account on a Smart Card. A Smart Card is similar to a credit card in size and shape but includes electronic circuitry, perhaps in the form of a small microprocessor, for controlling operation of devices receiving the Smart Card and for storing information such as financial ID's. In one possible implementation, the Smart Card is configured to enable telephony operations of the mobile telephone and is also configured to store the financial ID of a single credit or debit account. To effectuate a financial transaction, the Smart Card is removed from the mobile telephone and provided to a merchant for insertion into a Smart Card reader for reading the financial ID therefrom. Although, the use of such a Smart Card has the advantages that the financial ID cannot be easily erased and may be output subject to appropriate encryption, many of the other disadvantages of conventional credit and debit cards remain. For example, depending upon the implementation, a separate Smart Card may be required for each separate credit and debit account and the separate cards are thereby subject to being lost or stolen. Moreover, the consumer may need to terminate a telephone call to allow the Smart Card to be removed from mobile telephone to effectuate the transaction. Finally, because the Smart Card must be inserted into a reader provided by the merchant, no clear advantages are gained for financial transactions conducted over the telephone or using the Internet.

Accordingly, it would be desirable to provide a more effective integration of mobile telephony and financial ID transactions and it is to that end that further aspects of the invention are drawn.

Finally, there is an movement toward enabling the use of digital money for purchase transactions. Digital money constitutes packets of data containing financial ID's defining certain quantities of money that can be transferred from computer to computer. Digital money differs from credit or debit money in that it is not tied to any external real world account. Rather, digital money is the cyberspace equivalent of cash. It would be desirable to provide the aforementioned integration of mobile telephony and financial ID transactions in a manner that enables and facilitates digital money transactions and it is to that end that still further aspects of the invention are drawn.

SUMMARY OF THE INVENTION

In accordance with one aspect of the invention, financial ID's are stored directly within a mobile communications unit such as a mobile telephone or other device provided with wireless telephony capability such as a personal data assistant (PDA), a laptop computer, a dedicated Internet access device, or an electronic organizer. The financial ID's represent credit or debit accounts, digital money or other financial instruments. Storage of financial ID's within such devices allows the various financial ID's of credit and debit accounts of a customer or of digital money to be consolidated and used efficiently. The ID's are transmitted by radio or infrared signals to a merchant or other party to enable quick and efficient transactions such as purchase transactions. Radio transmission is particularly advantageous for conducting transactions during a mobile telephone call which might otherwise require verbally conveying the financial ID of a credit or debit account. Moreover, by storing the financial ID's in the mobile communications unit, the ID's are therefore not as easily subject to inadvertent magnetic erasure as with magnetic strip cards, and the risks associated with misplacing individual credit or debit cards are avoided. The financial ID's may be transmitted in an encrypted form to minimize the risk of unauthorized capture. Almost any form of transaction otherwise conventionally handled with credit or debit accounts or digital money may be performed.

In one embodiment, the invention is implemented within a mobile communications unit by a providing a means for storing a financial

identification code and a means for transmitting the financial identification code to effectuate a financial transaction. A means for receiving a signal representative of a requested financial transaction is also provided along with means for retrieving the financial ID in response to the received request signal. To receive selections from the customer, the mobile communications unit is further provided with a means for providing an indication representative of the financial identification codes to a customer and for requesting selection of one to effectuate transaction; and a means for receiving a selection signal representative of one of the financial identification codes. To receive authorization from the customer to complete a transaction, the mobile communications unit further includes a means for providing an indication of the requested financial transaction to a customer and for requesting approval to effectuate the transaction; a means for receiving an authorization signal representative of whether approval is granted for effectuating the transaction; and a means for transmitting the authorization signal.

Depending upon the implementation, the means for receiving signals and the means for transmitting signals may be an infrared receiver/transmitter, a cellular telephone receiver/transmitter for communicating with a cellular base station, or a mobile telephone receiver/transmitter for communicating with a satellite. Means for encrypting signals prior to transmission and for decrypting received signals may also be employed.

In other embodiments, the invention is implemented as a method.

BRIEF DESCRIPTION OF THE DRAWINGS

The features, objects, and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference characters identify correspondingly throughout and wherein:

FIG. 1 is a block diagram of a financial transaction system configured in accordance with an exemplary implementation of the invention wherein the mobile telephone of a customer has financial ID's stored therein and wherein signals relevant to a purchase transaction are transmitted between the mobile telephone and a merchant cashier register via a cellular telephone system;

FIG. 2 is a flowchart illustrating the steps performed by the system of **FIG. 1** to effectuate a financial transaction in accordance with a first method

wherein a financial ID is transmitted from the mobile telephone to a financial transaction clearinghouse;

FIG. 3 is a block diagram illustrating the mobile telephone of **FIG. 1** and showing a financial ID selection display;

FIG. 4 is a block diagram illustrating the mobile telephone of **FIG. 1** and showing an authorization display;

FIG. 5 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 1**;

FIG. 6 is a timing diagram summarizing, at a high level, a second method wherein the financial ID is transmitted from the mobile telephone to the merchant cashier register;

FIG. 7 is a block diagram of a financial transaction system configured in accordance with a first alternative implementation of the invention wherein signals relevant to the financial transaction are transmitted between the mobile telephone and the merchant cashier register via a satellite-based mobile telephone system;

FIG. 8 is a block diagram of a financial transaction system configured in accordance with a second alternative implementation wherein signals relevant to the transaction are transmitted between the mobile telephone and the merchant cashier register via infrared signals;

FIG. 9 is a block diagram of a financial transaction system configured in accordance with a third alternative implementation and wherein signals relevant to a transaction initiated during a telephone call are transmitted between the mobile telephone and the merchant cashier register via a cellular telephone system;

FIG. 10 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 9** to effectuate a financial transaction in accordance with a first method wherein a credit or debit account is accessed;

FIG. 11 is a timing diagram illustrating, at a high level, steps performed by the system of **FIG. 9** to effectuate a financial transaction in accordance with a second method wherein digital money is transferred;

FIG. 12 is a block diagram of a financial transaction system configured in accordance with a fourth alternative implementation of the invention wherein signals relevant to a transaction initiated via the Internet are transmitted between the mobile telephone and a merchant computer via a cellular telephone system connected to the Internet;

FIG. 13 is a timing diagram summarizing, at a high level, steps performed by the system of **FIG. 12** to effectuate a financial transaction in

accordance with a method wherein digital money is transferred via the Internet.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to the figures, preferred and exemplary implementations of the invention will now be described. Initially, techniques of the invention will be described with reference to **FIGS. 1 - 5** which illustrate a system employing a mobile telephone wherein signals appropriate for implementing an in-person purchase via a credit or debit account are transmitted between a mobile unit and a merchant cashier register or other point of sale unit via a cellular telephone. The transaction is coordinated by a financial transaction clearinghouse with the financial ID of a credit or debit account selected by the customer being transmitted from the mobile telephone to the clearinghouse, rather than to the merchant cashier register. An alternative method for in-person purchases wherein the financial ID is transmitted from the mobile telephone to the merchant cashier register will be described with reference to **FIG. 6**. Then, alternative systems employing satellite-fleet mobile communications or direct infrared communications between the mobile unit and the merchant cashier register for in-person purchases will be described with reference to **FIGS. 7 - 8**. Next, with reference to **FIGS. 9 - 11**, a system for implementing a purchase wherein the purchaser and merchant are remote from one another will be described both for a credit or debit account purchase and for a digital money purchase. Finally, with reference to **FIGS. 12 - 13** a system for implementing a digital money purchase via the Internet using a lap-top computer with mobile telephony capability will be described.

FIG. 1 shows a system **10** for performing a purchase based upon a credit or debit account between a customer (not shown) using a mobile telephone unit **12** and a merchant (also not shown) using a point of sale cashier register **14**. **FIG. 2** illustrates a method performed by the system of **FIG. 1**. **FIGS. 1** and **2** will be described together with the steps of **FIG. 2** provided in parentheses. After the customer verbally indicates a desire to purchase goods or services, the merchant enters purchase transaction information including the amount of the purchase and the telephone number (provided by the customer) of mobile unit **12** into cashier register **14** (**FIG. 2**, step **102**). The cashier register generates a transaction ID and transmits transaction information and the mobile unit telephone number

over a land line 16 connected to the PSTN 17 to a financial transaction clearinghouse (clearinghouse) 18 (FIG. 2, step 104). The transaction information includes, for example, a transaction ID, the identity and cost of the goods or services and an identification of the merchant. Clearinghouse 18 receives and records the information (FIG. 2, step 106), then calls mobile unit 12 using the provided telephone number via a cellular system 20 having a base station 22 in the vicinity of the mobile unit 12 (FIG. 2, step 108).

The purchaser answers the incoming telephone call to mobile unit 12 and thereby allows the mobile unit 12 to receive signals transmitted by the clearinghouse 18 (FIG. 2, step 110). Depending upon the implementation, clearinghouse 18 may transmit signals to the mobile unit 12 via the cellular system specifying the amount of the transaction, the identity of the goods or services, and the identity of the merchant. Clearinghouse 18 also transmits a request for either digital money or a financial ID specifying a credit or debit account and approval to charge the account. The mobile unit 12 receives the signals and presents appropriate displays to the customer to display information received from clearinghouse 18 and to request selection of a credit or debit account or digital money (FIG. 2, step 112). To this end, mobile unit 12 retrieves pre-stored financial information from a memory unit (not shown) within the mobile unit identifying the credit and debit accounts of the customer of mobile unit 12 and any digital money stored therein.

An exemplary display is provided in FIG. 3 within a display screen 24 of mobile unit 12. As can be seen, the exemplary display identifies the merchant, the goods or services and the amount of the purchase and provides three credit card accounts and two ATM (debit) accounts for selection. The credit card accounts may be, for example, VISA, MASTER CHARGE, and AMERICAN EXPRESS accounts and may be identified by appropriate icons in display screen 24. (VISA, MASTER CHARGE and AMERICAN EXPRESS are trademarks of their respective companies.) The ATM debit card accounts may be checking accounts maintained at different banks and may be identified by the bank name or other appropriate icons in display screen 24. The display also shows that the purchase may be made using digital money and specifies the amount of digital money available. Examples involving a digital money purchase will be described below with reference to FIGS. 11 - 13.

The customer enters a selection by, for example, pressing the appropriate button on keypad 26 corresponding to the number of the

selected account (FIG. 2, step 114). In the present example the customer selects credit card no. 2 and is presented with the display of FIG. 4 requesting authorization to bill the amount of the purchase to the selected credit account (FIG. 2, step 116). The customer responds by pressing the appropriate buttons, such as by pressing 1 for YES or 2 for NO. If NO, an appropriate refusal signal is sent to clearinghouse 18 (FIG. 1) via cellular system 20 refusing authorization. The refusal is forwarded to the cashier register and the transaction is terminated. Assuming however, that the customer grants approval by selecting YES, the mobile unit retrieves the financial ID for the selected credit account from an internal memory and forwards the financial ID and an authorization signal to the clearinghouse along with transaction ID (FIG. 2, step 120) via cellular system 20. Although not separately shown, the customer may be required to first enter a personal identification number (PIN) before authorizing the transaction. Also, depending upon the implementation the financial ID may be encrypted, perhaps using a public key encryption system, the details of which are well known to those skilled in the art and will accordingly not be described herein.

Clearinghouse 18 receives the authorization and the selected financial ID from mobile unit 12 along with the transaction ID and contacts the appropriate bank or credit card company to verify that the selected account has sufficient capacity to cover the purchase (FIG. 2, step 122). In FIG. 1, an exemplary set of credit card companies 28 and debit card companies 30 are shown. Communications between clearinghouse 18 and the credit and debit card companies may be via PSTN 17 or any other appropriate communications medium. Assuming that the selected account has sufficient capacity for the purchase, the selected credit account company records the amount of the purchase and the transaction ID and sends a verification signal to clearinghouse 18 for forwarding to the cashier register 14 and to mobile unit 12 (FIG. 2, step 124). Hence, both the customer and the merchant are advised simultaneously of the verification (FIG. 2, steps 126 and 128). Both mobile unit 12 and the cashier register 14 provide an appropriate verification display. The telephone call between clearinghouse 18 and the mobile unit 12 is then terminated. The merchant then conveys the goods or services to the customer and the transaction is completed. Ultimately, the credit card company forwards a bill to the customer for the amount of the purchase and forwards funds to the merchant to cover the purchase.

Thus, the system of FIG. 1 allows for a purchase transaction using, for example, a credit or debit account to be completed easily without requiring the financial ID of the purchasers account to be provided to the merchant and without the use of conventional credit or debit cards which, as noted above, are subject to being lost, stolen or damaged. All of the financial ID's for all of the customers accounts are consolidated in within mobile unit 12 for easy access. Depending upon the implementation, the memory unit of the mobile unit may additionally store the amount of credit or debit remaining, i.e. the account balance, for each credit and debit account. This information may be updated following each transaction. Assuming that all purchases are handled using mobile unit 12, the account balance information stored therein thereby remains correct. If purchases are made separately perhaps using a conventional credit or debit card, the information for a particular account can be updated following each transaction involving that account by transmitting the current account balance from the appropriate credit or debit card company to the mobile unit via the financial transaction clearinghouse. Additions to the amount of money available in a debit account as a result of a deposit may be tracked in much the same manner.

Depending upon the implementation, the signals transmitted to and from mobile unit 12 may be entirely digital and may be embedded in any on-going voice conversation the purchaser may be having using the mobile unit. For example, for cellular telephone systems employing Code Division Multiple Access (CDMA) technology, which encodes all voice signals digitally, the appropriate digital financial transaction signals may be embedded or interleaved in data packets along with voice signals. In this manner, the purchaser need not terminate an on-going voice telephone call. Rather, the purchaser merely pauses briefly during the conversation to review the information displayed regarding the transaction and to press the appropriate buttons for selecting the credit/debit account and for authorizing the purchase.

Also, depending upon the implementation, no financial transaction clearinghouse is required. Rather, merchant cashier register 14 may communicate directly with the appropriate credit card and debit card companies 28 and 30.

The messages exchanged during the performance of the steps of the method implemented by the system of FIG. 1 are summarized at a high level as shown in FIG. 5 which provides separate time lines 32, 34 and 36 showing, respectively, the steps performed by mobile unit 12, merchant

cashier register **14** and financial transaction clearinghouse **18** of **FIG. 1**. The steps performed during the generation of the messages shown in **FIG. 5** have already been described with reference to **FIGS. 1** and **2**, and will not be re-described.

With the system and method thus far described, the selected financial ID is transmitted directly from the mobile unit to the financial transaction clearinghouse. Hence the merchant never receives the financial ID. This helps maintain the privacy of the financial ID, particularly from unauthorized use by possible unscrupulous merchants. **FIG. 6** summarizes a somewhat simpler, alternative method wherein the financial ID is transmitted to the merchant cashier register **14**. After the customer indicates a desire to purchase goods or services and provides the telephone number of the mobile unit, the cashier register **14** calls the mobile unit using the telephone number and transmits signals to mobile unit **12** via the cellular system of **FIG. 1**, at step **20**, advising of the transaction and requesting either the financial ID of a credit/debit account or digital money and requesting authorization to complete the transaction. The advice of transaction information includes an identification of the goods or service to be purchased and the cost thereof.

Mobile unit **12** provides appropriate displays such as those illustrated in **FIGS. 3 - 4**, inputs the appropriate selections from the customer and then, assuming that a credit or debit account is selected, transmits the financial ID of the credit or debit account and an authorization signal to the merchant cashier register, step **202**. The cashier register then transmits signals to the financial transaction clearinghouse, step **204**, perhaps using land lines as illustrated in **FIG. 1**, advising of the transaction and providing the financial ID and the authorization signal received from the mobile unit. Again the advice of transaction information includes the cost of the goods or services to be purchased. Clearinghouse **18** forwards the financial ID to the appropriate credit account or debit account company and requests verification that the selected account has the capacity to cover the purchase. Assuming that the selected account has sufficient capacity, a verification signal is received by clearinghouse **18** and then forwarded to the cashier register **14** for completion of the transaction. One particular advantage of performing the method of **FIG. 6** is that the telephone number of the mobile unit need not be provided to the merchant for inputting into the cashier register because no telephone calls are made to the mobile unit.

What has been described thus far is a system wherein communication between the cashier and the financial transaction clearinghouse is

performed using the PSTN and wherein communications between the mobile unit and clearinghouse is performed using a cellular telephone system. In general, however, any appropriate forms of communication may alternatively be employed. For example, communication between the cashier register and the clearinghouse may also be via a cellular telephone system. Alternatively, communications may be performed using a satellite-based mobile communications system. Also, communications between the mobile unit and cashier may be performed using an infrared system.

FIG. 7 illustrates a satellite-based system **310** having a mobile unit **312**, a cashier register **314**, a financial transaction clearinghouse **318**, and credit account and debit account companies **320** and **322** all interconnected via a satellite mobile communications system represented by a single satellite **324**. The satellite system may include ground stations not separately shown. All communications between the various units are performed using the satellite system thereby eliminating the need for any land line communications. Any of the transaction methods described above with respect to **FIGS. 1 - 6** may be performed using the system of **FIG. 7** and the methods will not be re-described.

FIG. 8 illustrates an infrared-based system **410** having a mobile unit **412**, a cashier register **414**, PSTN **417**, a financial transaction clearinghouse **418**, and credit account and debit account companies **428** and **430**. As with the system of **FIG. 1** the cashier register, the clearinghouse and the credit and debit account companies are interconnected via the PSTN. However, communication between the mobile unit and the cashier is performed using infrared signals. More specifically, mobile unit **412** has an infrared receiver/transmitter **424** and cashier register **414** has an infrared receiver/transmitter **426**.

In an exemplary transaction performed in accordance with the method of **FIG. 6**, the cashier transmits to the mobile unit via infrared signals the amount of the transaction and an identification of the goods or services. The mobile unit inputs the customer's selection of a credit or debit account, receives explicit authorization from the customer, then transmits the financial ID of the selected account and an authorization signal to the cashier register **414** via infrared signals. Transmission and reception of the infrared signals may be entirely in accordance with conventional infrared techniques which are well understood by those skilled in the art and will not be described herein. In an alternative embodiment of the invention, the method of **FIG. 2** is performed using the system of **FIG. 8** whereby the telephone number of mobile unit **12** is exchanged using the infrared link.

Thus far, in-person transaction methods have been described wherein the customer with mobile unit is in the vicinity of the merchant cashier register. In the following, transactions are described wherein the customer is remote from the merchant and initiates the transaction either via a mobile telephone call to the merchant or via an Internet or similar computer network connection. Also, transactions are described wherein digital money is conveyed.

FIG. 9 illustrates a system 510 having a customer mobile unit 512 and a merchant cashier register 514 with telephone 515. The mobile unit is located remote from the cashier and telephone as indicated by a dashed line interposed between them. Cashier register 514 and telephone 515 are connected via a land line 516 to PSTN 517 which, in turn, is connected to a financial transaction clearinghouse 518, cellular system 520 having base station 522, and credit and debit account companies 528 and 530. The customer initiates a purchase transaction by calling the merchant telephone 515 using mobile unit 512 and indicates a desire to purchase goods or services. The merchant enters the selected transaction into cashier register 514 which communicates directly with mobile unit 512 via the open mobile telephone call connection to digitally provide the amount and nature of the transaction to the mobile unit and to digitally requests a financial ID and an authorization signal for completing the transaction. This assumes that a mobile system is employed that allows embedding of digital signals within voice telephone conversation signals such as the aforementioned CDMA system. The customer pauses briefly during his conversation with the merchant to select a credit or debit account and to authorize the transaction in the same manner as described above with reference to FIGS. 3 - 4. Mobile unit 512 retrieves the financial ID of the selected account and transmits the financial ID and an authorization signal digitally to cashier register 514 again via the same mobile telephone call. Cashier register 514 immediately forwards the financial ID and authorization signal to the financial transaction clearinghouse over a second PSTN line (not separately shown). Clearinghouse 518 operates in the same manner as described above to obtain verification that the selected account has sufficient capacity of the purchase. A verification signal is forwarded back to the cashier 514 which displays the verification to the merchant who verbally conveys the verification to the customer using telephone 515. Verification may additionally be transmitted from the cashier register to the mobile unit via the open mobile telephone call. The telephone call is then terminated and the transaction is thereafter completed by providing the goods or services to the customer.

The steps of the method implemented by the system of FIG. 9 are summarized at a high level within FIG. 10 which provides separate time lines 532, 534 and 536 showing, respectively, the steps performed by the mobile unit 512, the cashier register 514 and the financial transaction clearinghouse 518 of FIG. 9.

Hence, a system is provided wherein digital signals pertaining to a purchase transaction are transmitted between a customer mobile unit and a merchant cashier register during a voice mobile telephone conversation between the customer and merchant. This is similar to otherwise conventional telephone purchase transactions using credit or debit accounts, but with the system of FIG. 9 - 10 the customer need not verbally convey the financial ID of a credit/debit account to the merchant during the telephone call. This has the advantage of speeding up the transaction because the customer need not read aloud the financial ID, name and expiration date from a credit card and the merchant need not record that information. Also, mistakes that can commonly occur in reading and transcribing the digits of the financial ID are avoided. Moreover, the unauthorized capture of the financial ID by eavesdropping is minimized. As with previous embodiments, the financial ID may be encrypted to further reduce the risk of unauthorized access.

Thus far, all example transactions described have involved the purchase of goods or services using a credit or debit account selected by the customer. As noted above, however, any of the various transaction methods and systems also allow payment for the goods or services using digital money stored within the mobile unit.

FIG. 11 summarizes a digital money transaction using the system of FIG. 9. FIG. 11 provides separate time lines 632 and 634 showing, respectively, the steps performed by the mobile unit 512 and the point of sale cashier register 514 of FIG. 9. No time line is provided for the financial transaction clearinghouse because no credit or debit account is used and hence account verification is required. Rather digital money is conveyed for the customer mobile unit to the merchant cashier register.

The customer initiates a purchase transaction with the merchant during a voice mobile telephone call from the mobile unit to the merchant telephone, step 636. The merchant enters the purchase transaction information into the cashier register and, in the same manner as described above without reference to FIG. 9, the cashier register transmits digital signals to the mobile unit advising of the transaction and requesting a financial ID and an authorization signal, step 638. The customer is then

presented with a display such as is shown in FIG 3. However, rather than selecting a credit or debit account, the customer presses the appropriate buttons to select the digital money option and to authorize the purchase. Assuming the customer has sufficient digital money stored within the mobile telephone to cover the purchase, the financial ID or ID's of the digital money is transmitted to the cashier register as digital signals embedded within the mobile telephone voice conversation signals, step 640. The cashier register receives and stores the digital money. Hence, the digital money account of the mobile unit is decreased and the digital money account of the cashier register is increased. The completion of the digital money transaction is confirmed by transmitting appropriate verification and receipt signals from the cashier register back to the mobile unit, step 642. The telephone call is then ended and the goods or services are ultimately conveyed to the customer. If the goods or services are for some reason not conveyed, the verification and receipt signals received by the mobile unit of the customer provide proof of the transaction.

Thus far all transactions have been described with reference to systems employing mobile telephones capable of voice conversation telephone calls. As noted above however, purchase transactions can be performed in accordance with the invention using other types of mobile communications units such as laptop computers and PDA's configured with mobile transmitter/receivers. FIG. 12 provides an example of a system employing a laptop computer wherein a purchase transaction is performed over the Internet. FIG. 13 illustrates a method using the system of FIG. 12 wherein the purchase is made with digital money.

FIG. 12 illustrates a system 710 having a mobile laptop computer unit 712 and a merchant computer 714 located remote from one another. Merchant computer 714 is connected via a land line 716 to a PSTN 717 which is in turn connected to a financial transaction clearinghouse 718, the Internet 719 and a cellular system 720 having a base station 722. The clearinghouse is additionally connected to various credit account and debit account companies 728 and 730.

The customer initiates a purchase transaction by contacting the merchant computer via the cellular system and the Internet. In this regard, the laptop computer employs a modem (not separately shown) in connection with a mobile receiver/transmitter (also not separately shown) to contact the merchant computer via base station 722, cellular system 720, Internet 719 and PSTN 717 perhaps to access World Wide Web page maintained by the merchant. In any case, the customer selects goods or

services to be purchased by entering the appropriate commands into laptop 712 for transmission to merchant computer 714.

The merchant computer receives the customers purchase selection and transmits appropriate signals confirming the purchase selection and requesting a financial ID and an authorization signal. As with the other embodiments described above, the customer may select a credit or debit account or a quantity of digital money. If the former, the financial ID of the account is transmitted via the Internet, preferably encrypted, to the merchant computer for forwarding to the financial transaction clearinghouse, perhaps also via the Internet, for verification of adequate credit or debit account capacity. Appropriate, verification signals are sent to the merchant computer and forwarded to the customers laptop computer. If the purchase is via digital money, the financial ID defining the needed quantity of digital money is transmitted over the Internet to the merchant computer, again preferably encoded in some manner to prevent unauthorized capture, and appropriate verification and receipt signals are sent back to the customer. With the digital money transaction, no signal need be sent to the clearinghouse.

FIG. 13 summarizes the digital money transaction using the system of FIG. 12. FIG. 13 provides separate time lines 732 and 734 showing, respectively, the steps performed by the laptop 712 and merchant computer 714 of FIG. 12. Again, no time line is provided for the financial transaction clearinghouse because no credit or debit account is used and hence account verification is required.

Various exemplary systems and methods for performing financial transactions such as purchase transactions using a mobile telephone or other mobile communications unit configured to store the financial ID's of various credit and debit accounts and/or quantities of digital money have been described. In accordance with the principles of the invention, a wide variety of other financial transactions may be performed as well including, in general, almost any transaction otherwise handled with credit or debit cards or digital money. Although the examples provided wherein relate to mobile telephone or laptops computers, principles of the invention can be applied to almost any type of mobile communications unit including, the aforementioned PDA's, mobile Internet access devices, etc.

The exemplary embodiments have been primarily described with reference to block diagrams illustrating apparatus elements and timing diagrams and flow charts primarily illustrating method steps. As to the timing diagrams and flowcharts, each block or step therein represents both a

method step and an apparatus element for performing the recited step. Depending upon the implementation, each apparatus element, or portions thereof, may be configured in hardware, software, firmware or combinations thereof. It should be appreciated that not all components necessary for a complete implementation of a practical system are illustrated or described in detail. Rather, only those components necessary for a thorough understanding of the invention have been illustrated and described.

Moreover, the previous description of the preferred embodiments is provided to enable any person skilled in the art to make or use the present invention. The various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of the inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WE CLAIM:

CLAIMS

1. In a mobile communications unit, a system for performing a
2 financial transaction comprising:
means for storing a financial identification code; and
4 means for transmitting said financial identification code to
effectuate a financial transaction.

2. The system of claim 1 further including
2 means for receiving a signal representative of a requested financial
transaction; and
4 means for retrieving the stored financial identification code in
response to reception of the signal representative of the requested financial
6 transaction.

3. The system of claim 1 wherein said mobile communications
2 unit is selected from a group consisting of a mobile telephone, a personal
data assistant with mobile telephony capability, a laptop computer with
4 mobile telephony capability, an Internet access device with mobile telephony
capability, and an electronic organizer with mobile telephony capability.

4. The system of claim 1 wherein said financial identification code
2 is representative of digital money.

5. The system of claim 1 wherein said financial identification code
2 is representative of a debit account.

6. The system of claim 1 wherein said financial identification code
2 is representative of a credit account.

7. The system of claim 1 wherein said means for storing a
2 financial identification code stores a plurality of financial identification
codes.

2 8. The system of claim 7 wherein said system further includes --
2 means for providing an indication representative of said
4 financial identification codes and for requesting selection of one to effectuate
4 transaction; and
6 means for receiving a selection signal representative of one of
6 said financial identification codes.

2 9. The system of claim 2 further comprising:
2 means for providing an indication of said requested financial
4 transaction and for requesting approval to effectuate transaction;
4 means for receiving an authorization signal representative of
6 whether approval is granted for effectuating said requested transaction; and
6 means for transmitting said authorization signal.

2 10. The system of claim 9 wherein said means for receiving an
2 authorization signal operates to receive a personal identification number
code.

2 11. The system of claim 4 further including
2 means for receiving a signal indicative of a completed financial
4 transaction; and
4 means for modifying said digital money financial identification
code to reflect the completed financial transaction.

2 12. The system of claim 2
2 wherein said means for receiving the signal representative of the
requested financial transaction includes an infrared receiver.

2 13. The system of claim 1
2 wherein said means for transmitting said financial identification code
includes an infrared transmitter.

2 14. The system of claim 2
2 wherein said means for receiving the signal representative of the
requested financial transaction includes a cellular telephone receiver.

2 15. The system of claim 1
2 wherein said means for transmitting said financial identification code
includes a cellular telephone transmitter.

16. The system of claim 2
2 wherein said means for receiving the signal representative of the
requested financial transaction includes a wireless telephone receiver for
4 receiving signals from a satellite.

17. The system of claim 1
2 wherein said means for transmitting said financial identification code
includes a wireless telephone transmitter for transmitting signals to a
4 satellite.

18. The system of claim 1 wherein said means for transmitting said
2 financial identification code includes a means for encrypting the financial
identification code prior to transmission.

19. In a mobile communications unit, a system for performing a
2 financial transaction comprising:
a memory unit storing a financial identification code;
4 a receive unit receiving a signal representative of a requested
financial transaction;
6 a control unit retrieving the financial identification code in
response the received signal; and
8 a transmit unit transmitting said financial identification code
to effectuate said requested financial transaction.

20. A system for performing a financial transaction comprising:
2 a point of sale unit comprising
means for transmitting a signal representative of a
4 requested financial transaction, and
means for receiving a financial identification code for
6 effectuating said requested financial transaction;
a mobile communications unit comprising
8 means for storing a financial identification code,
means for receiving the signal representative of the
10 requested financial transaction, and
means for transmitting said financial identification code
12 to effectuate said requested financial transaction.

21. In a mobile communications unit, a method for performing a
2 financial transaction comprising the steps of:
storing a financial identification code; and
4 transmitting said financial identification code to effectuate a
financial transaction.

22. The method of claim 21 further including the steps of
2 receiving a signal representative of a requested financial
transaction; and
4 retrieving the stored financial identification code for
transmission in response to reception of the signal representative of a
6 requested financial transaction.

23. The method of claim 21 wherein said mobile communications
2 unit is selected from a group consisting of a mobile telephone, a personal
data assistant with mobile telephony capability, a laptop computer with
4 mobile telephony capability, an Internet access device with mobile telephony
capability, and an electronic organizer with mobile telephony capability.

24. The method of claim 21 wherein said financial identification
2 code is representative of digital money.

25. The method of claim 21 wherein said financial identification
2 code is representative of a debit account.

26. The method of claim 21 wherein said financial identification
2 code is representative of a credit account.

27. The method of claim 21 wherein said step of storing a financial
2 identification code is performed to store a plurality of financial identification
codes.

28. The method of claim 27 wherein said method further includes
2 the steps of
providing an indication representative of said financial
4 identification codes and for requesting selection of one to effectuate said
transaction; and
6 receiving a selection signal representative of one of said
financial identification codes.

29. The method of claim 23 further comprising the steps of: -
2 providing an indication of said requested financial transaction
and for requesting approval to effectuate said transaction;
4 receiving an authorization signal representative of whether
approval is granted for effectuating said transaction; and
6 transmitting said authorization signal.

30. The method of claim 21 wherein said step of receiving a
2 authorization signal is performed to receive a personal identification
number code.

31. The method of claim 24 further including the steps of
2 receiving a signal indicative of a completed financial
transaction; and
4 modifying said digital money financial identification code to
reflect the completed financial transaction.

32. The method of claim 22
2 wherein said step of receiving the signal representative of the
requested financial transaction includes the step of receiving an infrared
4 signal.

33. The method of claim 21
2 wherein said step of transmitting said financial identification code
includes the step of transmitting an infrared signal.

34. The method of claim 22
2 wherein said step of receiving the signal representative of the
requested financial transaction includes the step of receiving a cellular
4 telephone signal.

35. The method of claim 21
2 wherein said step of transmitting said financial identification
code includes the step of transmitting a cellular telephone signal.

36. The method of claim 22
2 wherein said step of receiving the signal representative of the
requested financial transaction includes the step receiving signals from a
4 satellite.

37. The method of claim 21
2 wherein said step of transmitting said financial identification code
includes the step of transmitting signals to a satellite.

38. The method of claim 21 wherein said step of transmitting said
2 financial identification code includes the step of encrypting the financial
identification code prior to transmission.

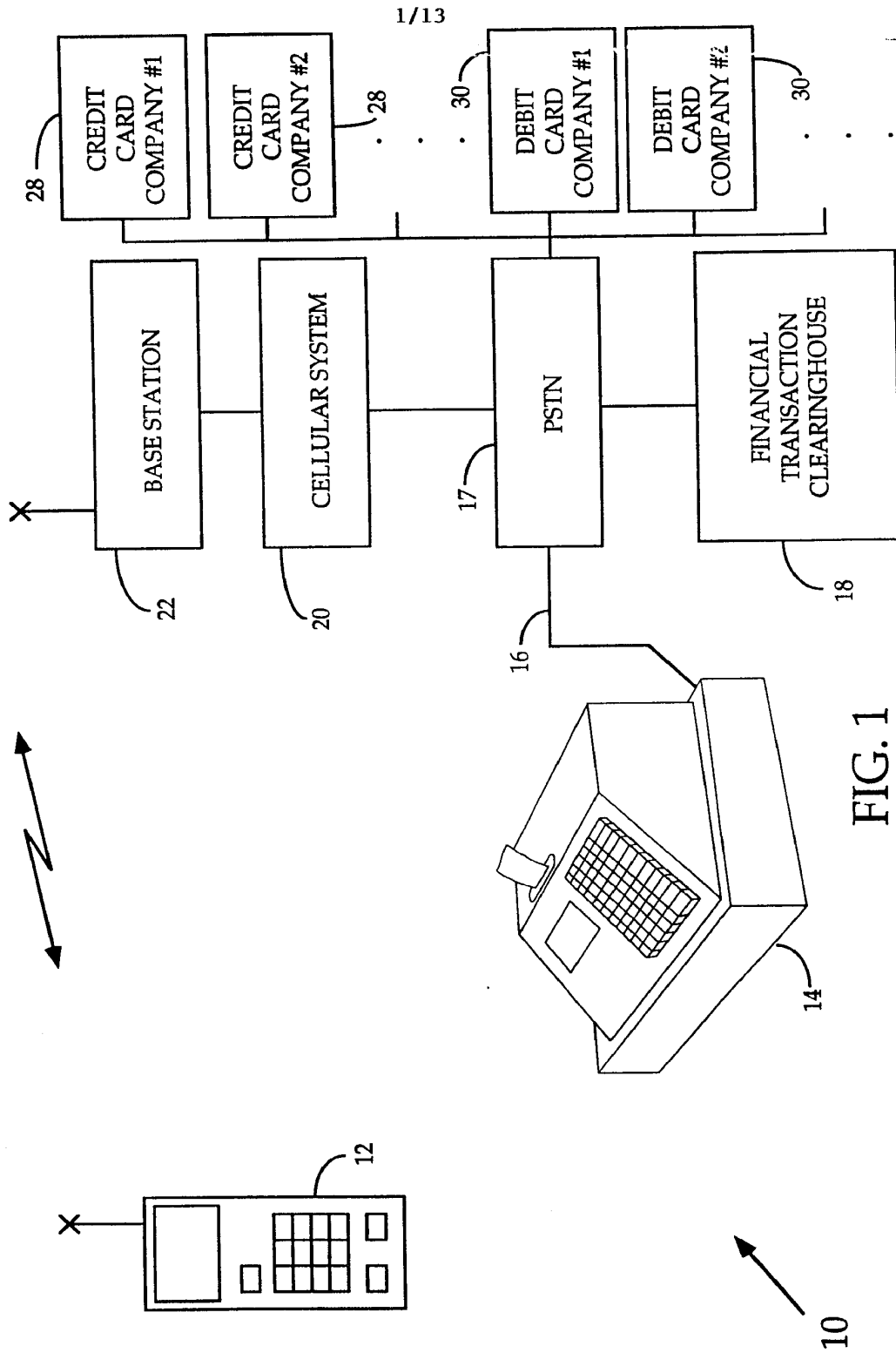


FIG. 1

2/13

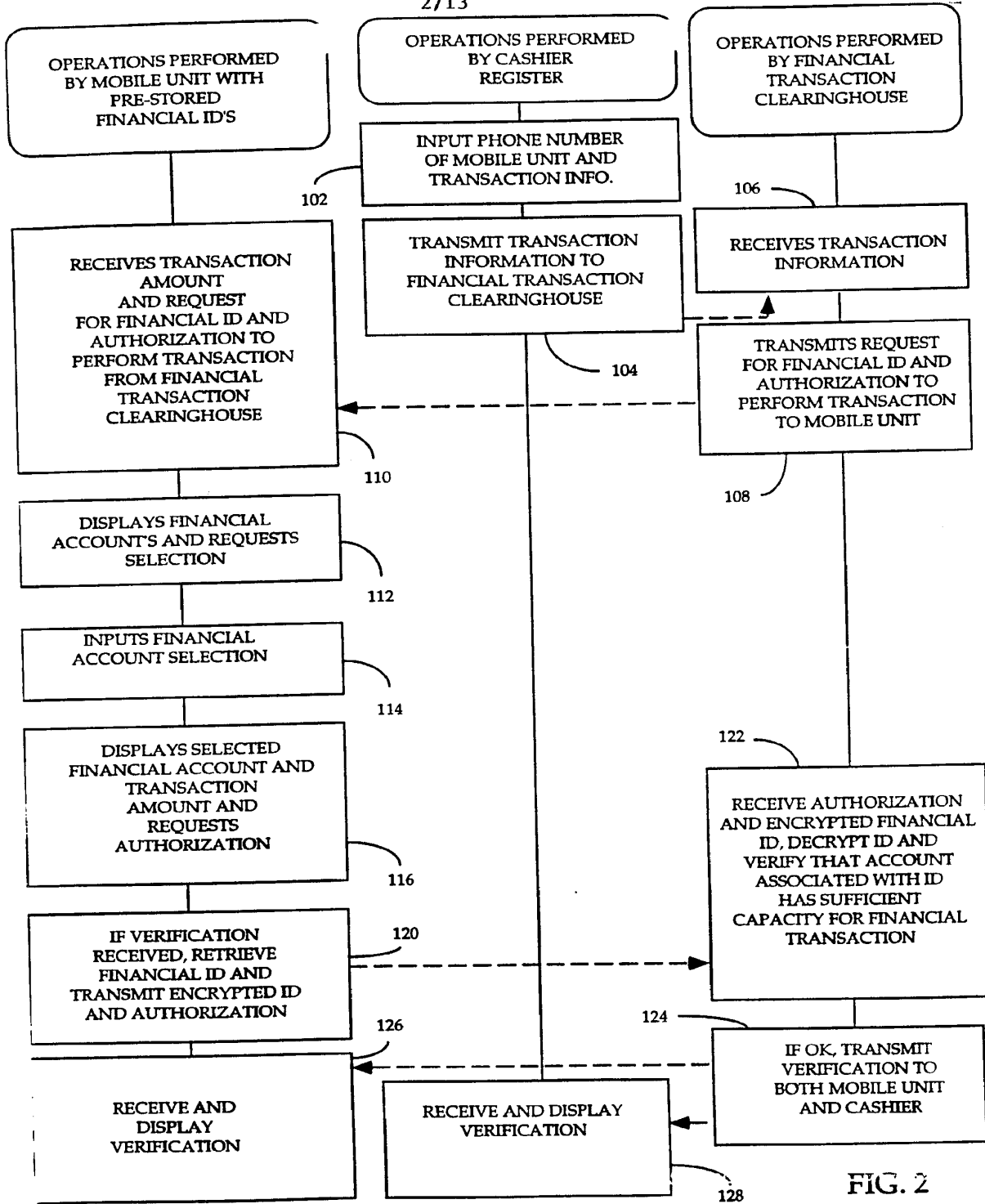


FIG. 2

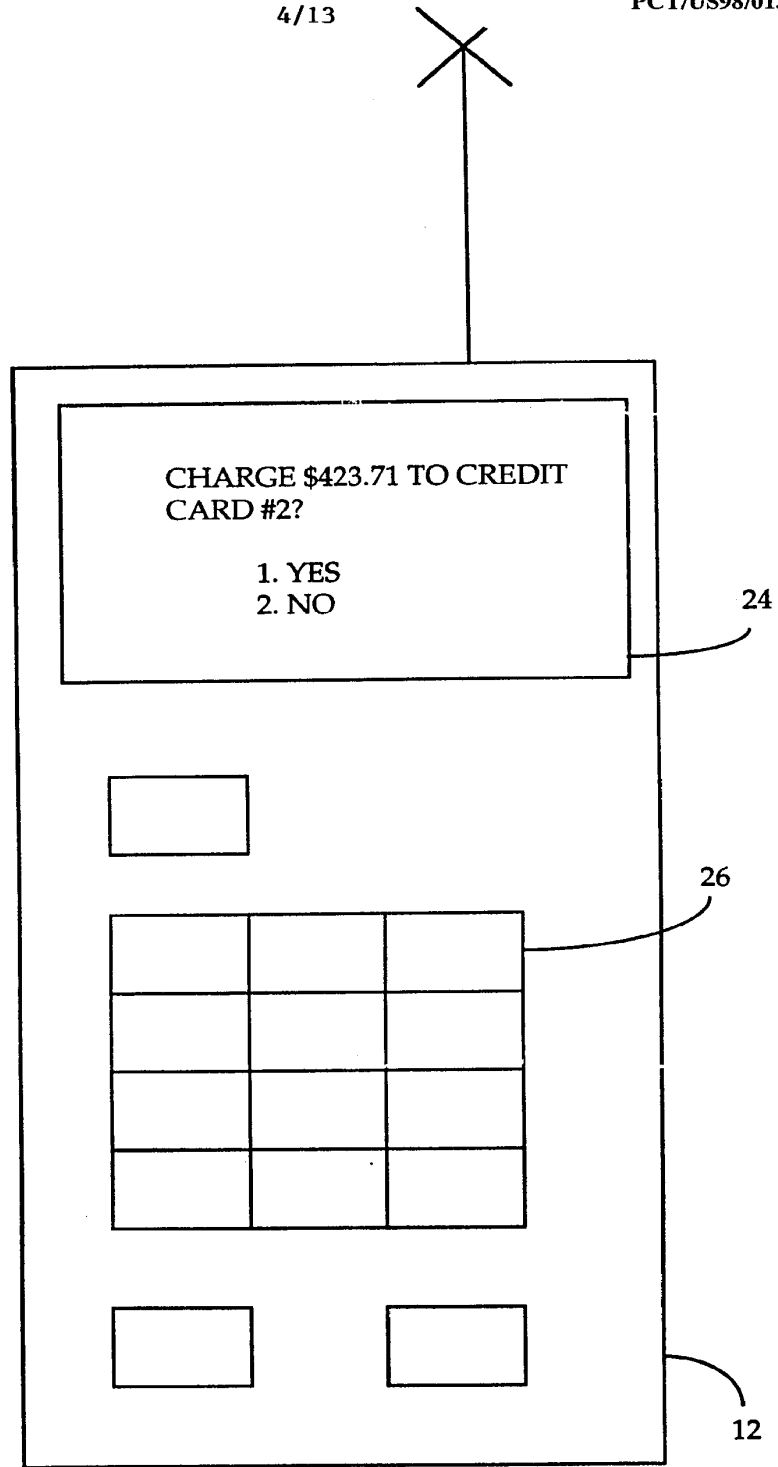


FIG. 4

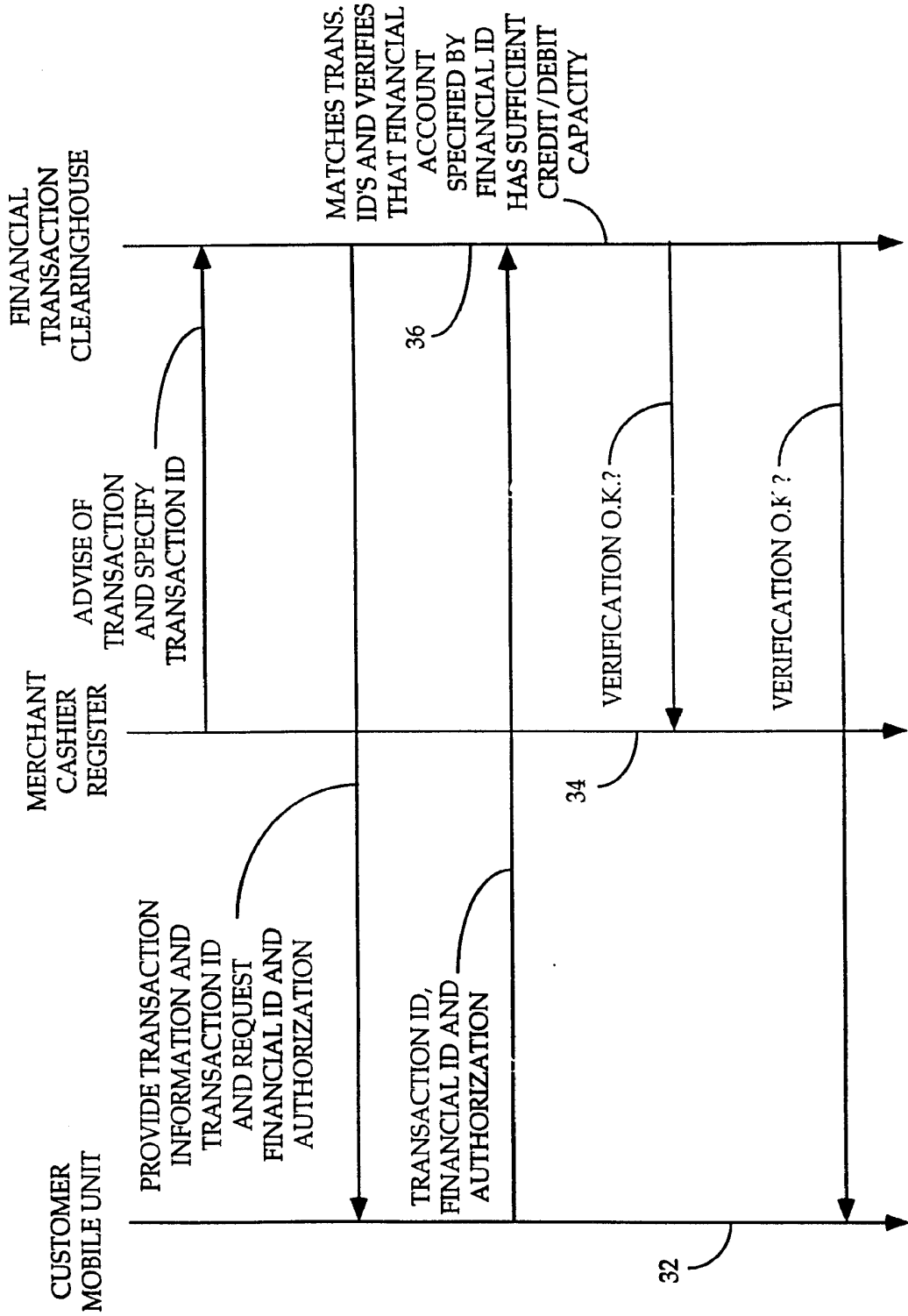


FIG. 5

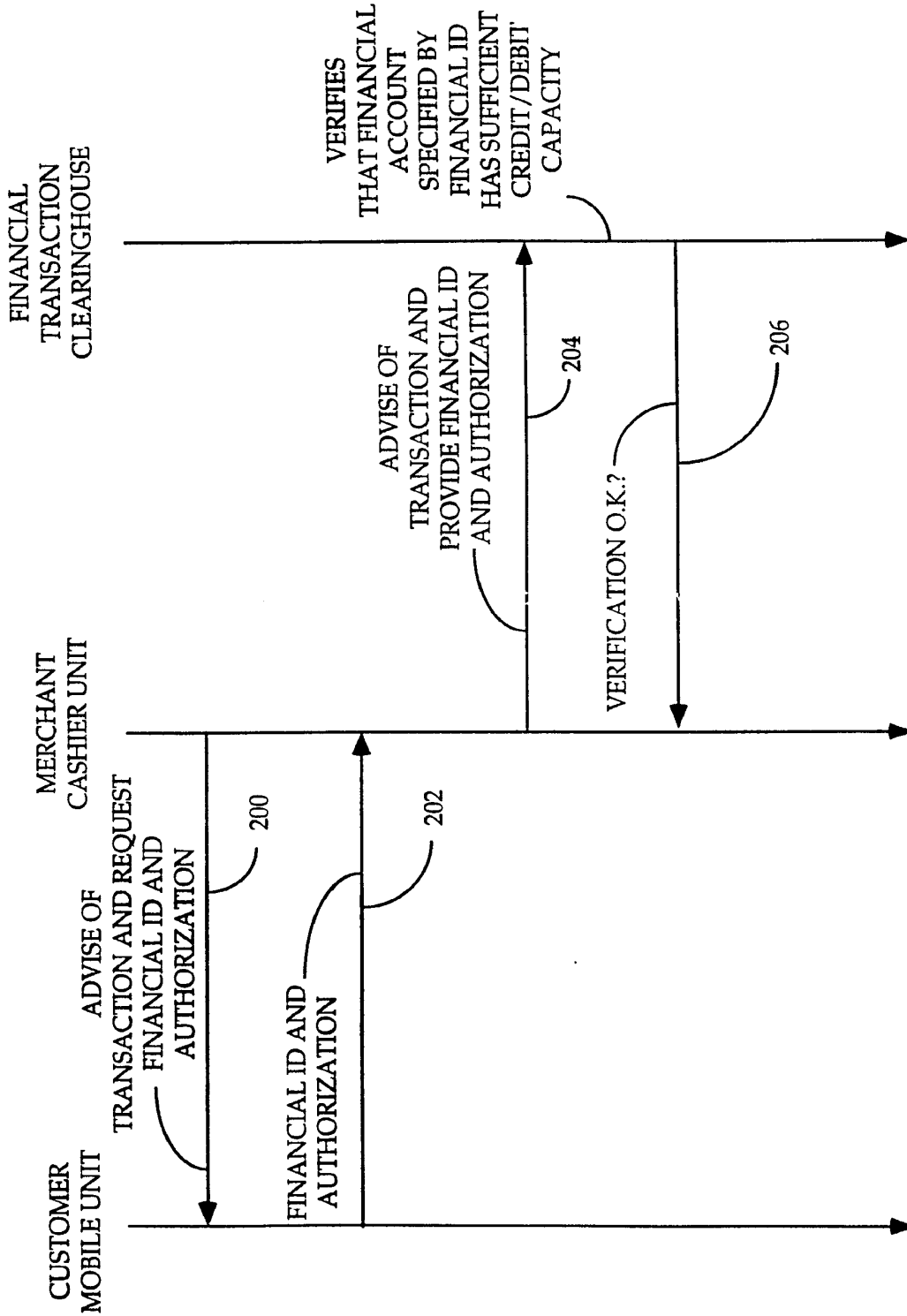


FIG. 6

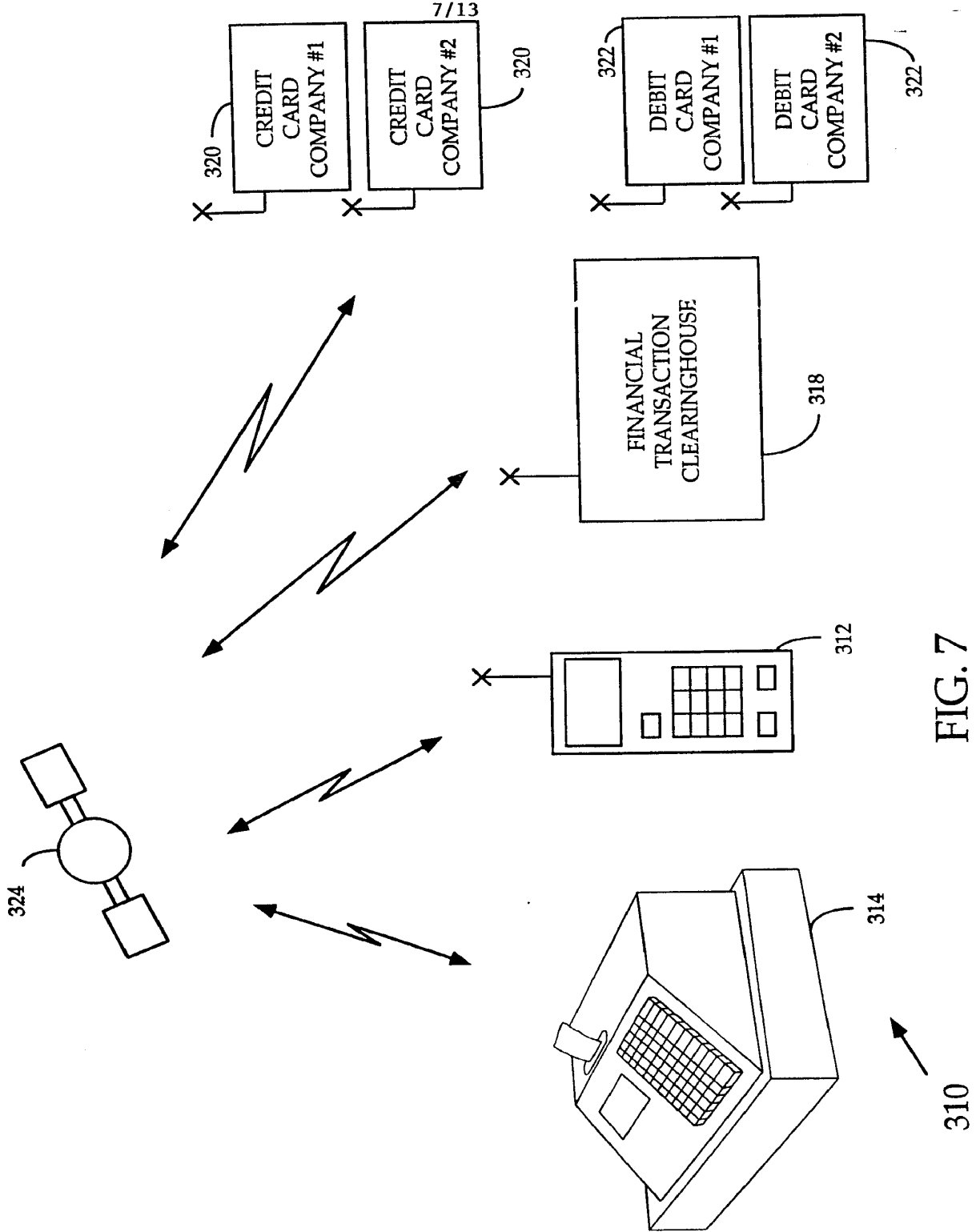


FIG. 7

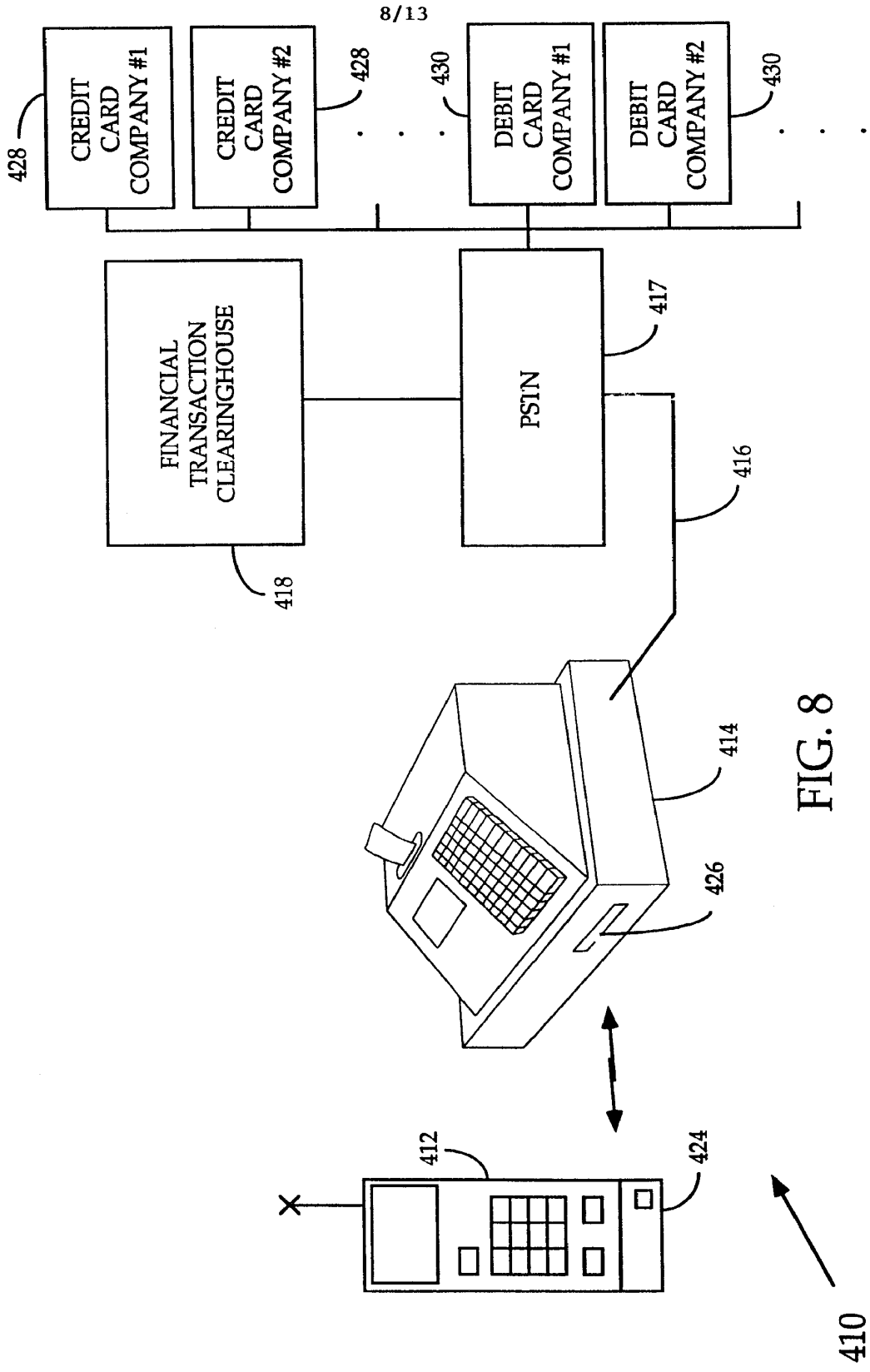


FIG. 8

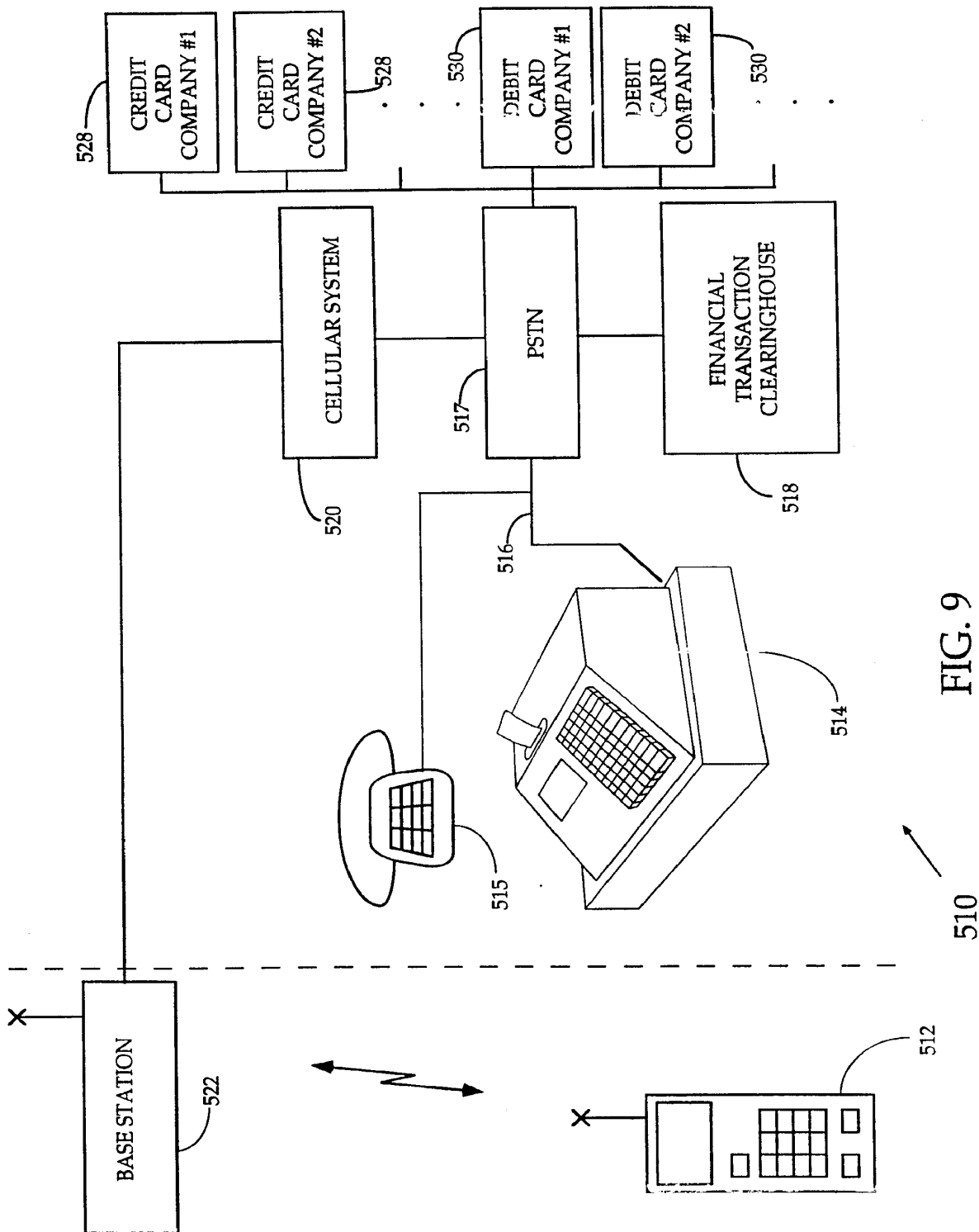


FIG. 9

510

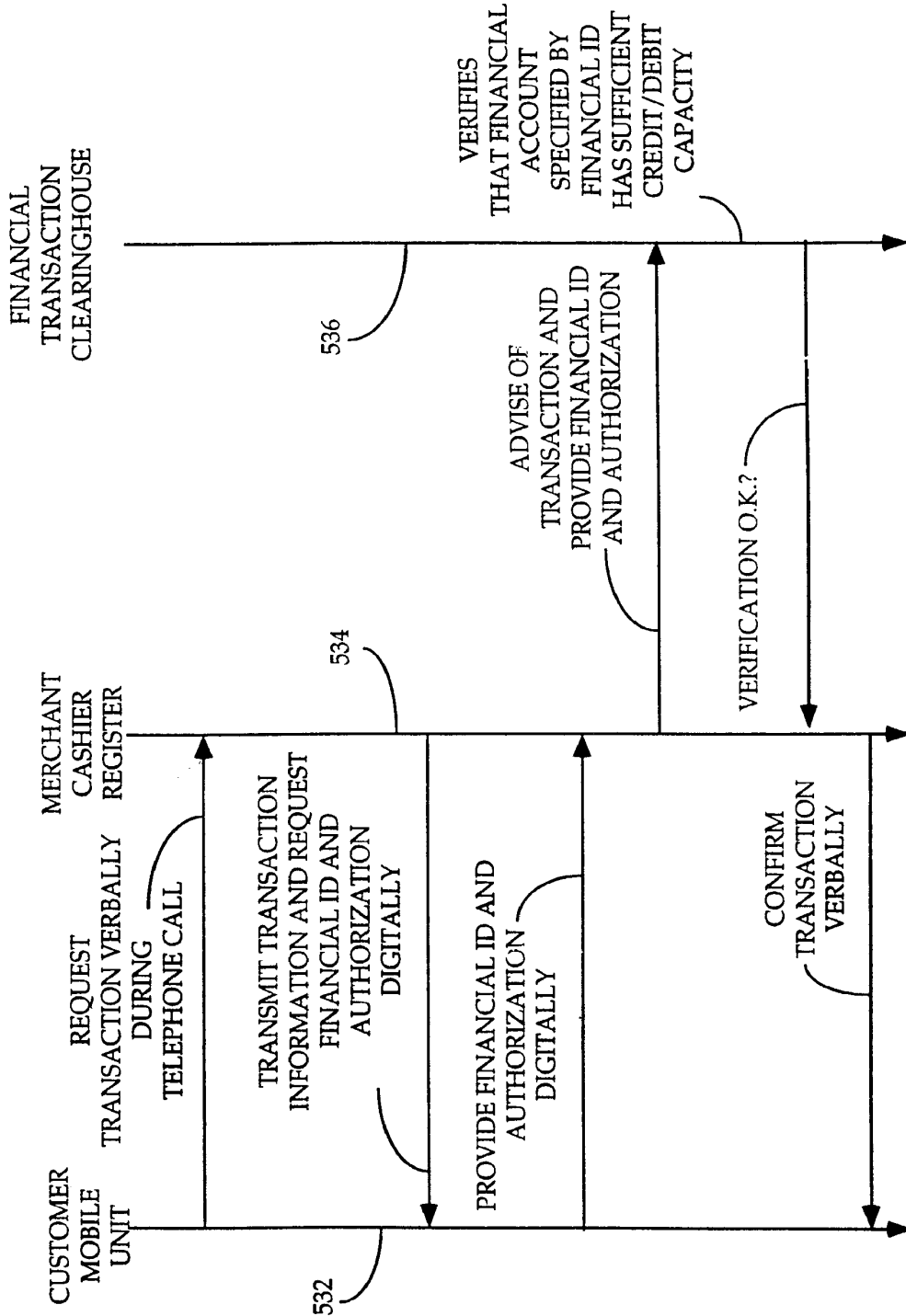


FIG. 10

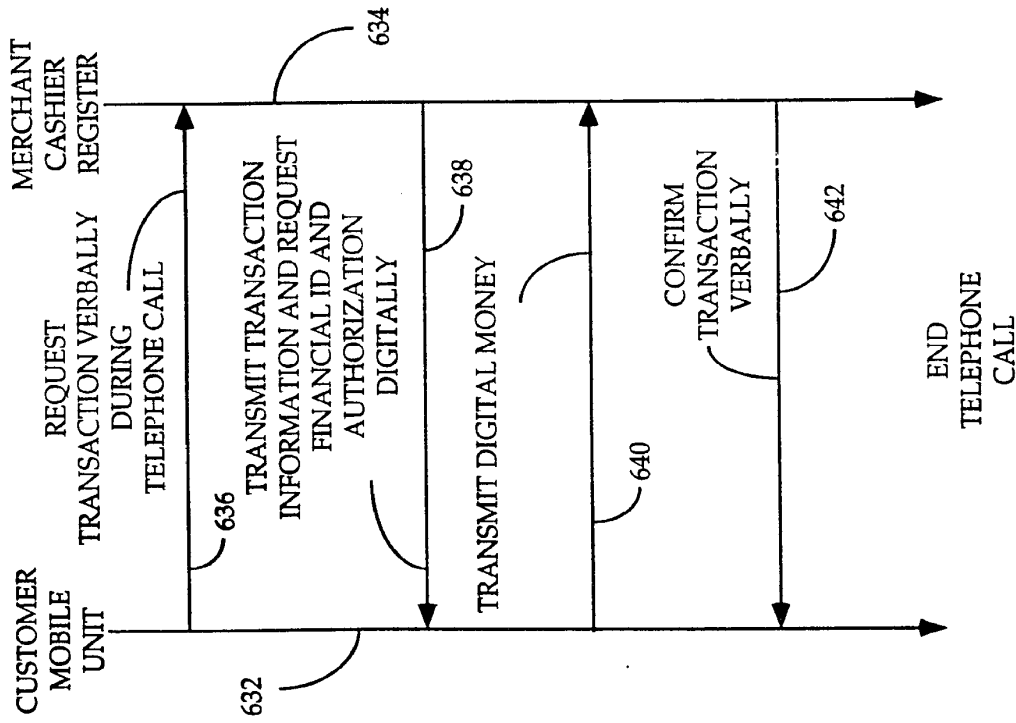


FIG. 11

12/13

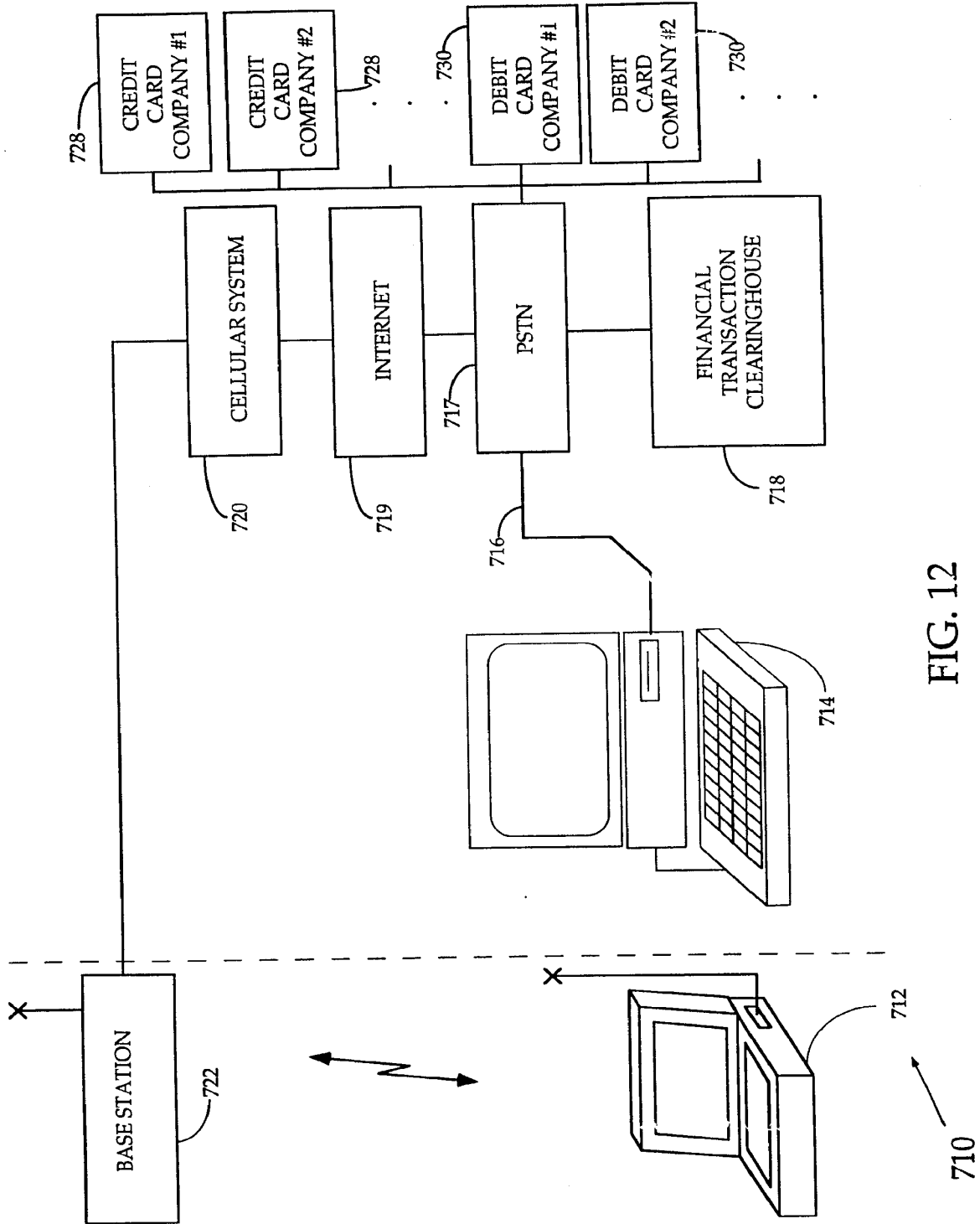


FIG. 12

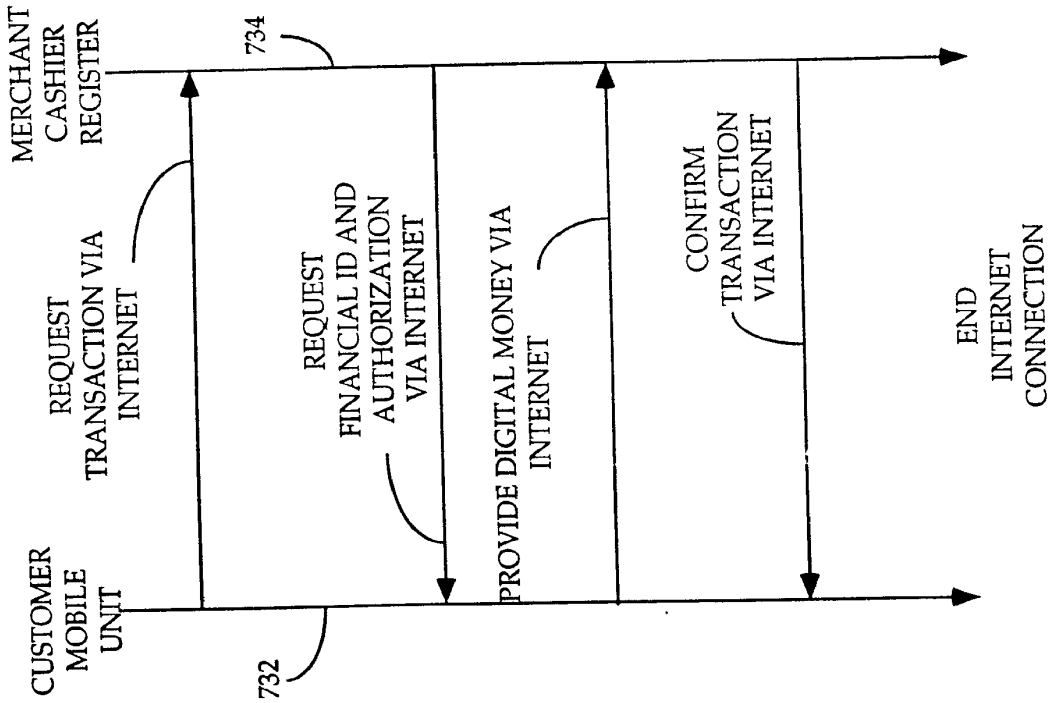


FIG. 13

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/01391

A. CLASSIFICATION OF SUBJECT MATTER IPC 6 G07F19/00 H04M17/00		
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) IPC 6 G07F H04M		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, 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.
X A	WO 96 25828 A (NOKIA MOBILE PHONES) 22 August 1996 see abstract; claims; figures 1,6,7 see page 13, line 3 - page 19, line 28 ---	1,3-7, 21,23-27 8,10-15, 19,20, 28,30-35
A	WO 94 11849 A (H.T. VATANEN) 26 May 1994 see abstract; claims; figures see page 5, line 36 - page 11, line 10 ---	1,3,5,6, 9,10, 12-15, 19-21, 23,25, 26,29, 30,32-35
A	EP 0 708 547 A (AT & T) 24 April 1996 --- -/--	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents :		
"A" document defining the general state of the art which is not considered to be of particular relevance	"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	
"E" earlier document but published on or after the international filing date	"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	
"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)	"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.	
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family	
"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	Date of mailing of the international search report	
7 July 1998	15/07/1998	
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer David, J	

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/01391

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No. --
A	WO 96 13814 A (B. VAZVAN) 9 May 1996 -----	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No PCT/US 98/01391

Patent document cited in search report	A	Publication date	Patent family member(s)	Publication date
WO 9625828	A	22-08-1996	FI 950685 A	16-08-1996
			AU 4624796 A	04-09-1996
			EP 0809916 A	03-12-1997
WO 9411849	A	26-05-1994	FI 925135 A	12-05-1994
			FI 934995 A	12-05-1994
			AT 159602 T	15-11-1997
			DE 69314804 D	27-11-1997
			EP 0669031 A	30-08-1995
			ES 2107689 T	01-12-1997
			NO 951814 A	09-05-1995
EP 0708547	A	24-04-1996	US 5608778 A	04-03-1997
			CA 2156206 A	23-03-1996
			JP 8096043 A	12-04-1996
WO 9613814	A	09-05-1996	FI 945075 A	29-04-1996
			EP 0739526 A	30-10-1996
			FI 962553 A	25-11-1997
			FI 962961 A	28-08-1996
			FI 971009 A	26-04-1997
			FI 971248 A	26-04-1997
			FI 971848 A	30-04-1997



Espacenet

- [About Espacenet](#)
- [Other EPO online services](#)
 - [Searching for patents](#)
 - [Open patent services](#)
 - [European Patent Register](#)
 - [European publication server](#)
 - [Global patent index](#)
- [Search](#)
- [Result list](#)
- [My patents list \(0\)](#)
- [Query history](#)
- [Settings](#)
- [Help](#)
- [Refine search](#)
- [Results](#)
- [WO0197118 \(A1\)](#)

Bibliographic data: WO0197118 (A1) — 2001-12-20

- |
-
- [In my patents list](#)
- |
- [EP Register](#)
- |
- [Report data error](#)
- |
- [Print](#)

SETTLING METHOD USING MOBILE PHONE AND MOBILE PHONE

Page bookmark: [WO0197118 \(A1\) - SETTLING METHOD USING MOBILE PHONE AND MOBILE PHONE](#)

Inventor(s): JOGU TAKAKO [JP]; ATAE SADAYUKI [JP] ± (JOGU, TAKAKO, ; ATAE, SADAYUKI)

Applicant(s): JOGU TAKAKO [JP]; ATAE SADAYUKI [JP] ± (JOGU, TAKAKO, ; ATAE, SADAYUKI)

Classification: **international:** [G06Q20/00](#); [G06Q30/00](#); [H04M17/00](#); [H04M17/02](#); (IPC1-7): [G06F17/60](#); [G06F19/00](#)
- cooperative: [G06Q20/02](#); [G06Q20/04](#); [G06Q20/12](#); [G06Q20/16](#); [G06Q20/32](#); [G06Q20/322](#); [G06Q30/04](#); [H04M15/68](#); [H04M17/00](#); [H04M17/02](#); [H04M17/10](#); [H04M22/15/01](#); [H04M22/15/02](#); [H04M22/15/03](#)

Application number: WO2001JP05039 20010613

Priority number(s): [JP20000178138 20000614](#) ; [JP20000221240 20000721](#) ; [JP20000402918 20001228](#)

Also published as: [JP4901953 \(B2\)](#) ; [AU6427491 \(A\)](#)

Abstract of WO0197118 (A1)

Translate this text into Tooltip

Albanian          

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年12月20日 (20.12.2001)

PCT

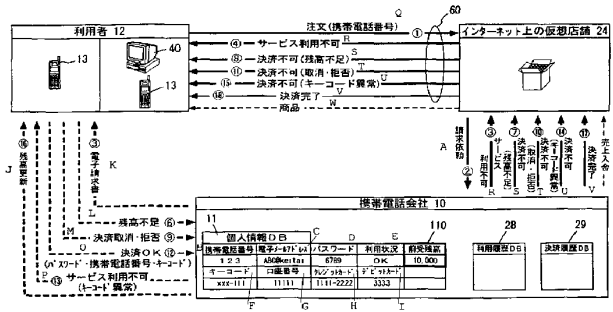
(10) 国際公開番号
WO 01/97118 A1

- (51) 国際特許分類: G06F 17/60, 19/00
 - (21) 国際出願番号: PCT/JP01/05039
 - (22) 国際出願日: 2001年6月13日 (13.06.2001)
 - (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2000-178188 2000年6月14日 (14.06.2000) JP
 - 特願2000-221240 2000年7月21日 (21.07.2000) JP
 - 特願2000-402918 2000年12月28日 (28.12.2000) JP
 - (71) 出願人 および
 - (72) 発明者: 浄弘 貴子 (JOGU, Takako) [JP/JP]; 〒631-0036 奈良県奈良市学園北1丁目8番4号 Nara (JP). 與 貞行 (ATAE, Sadayuki) [JP/JP]; 〒815-0071 福岡県福岡市南区平和2-4-10-402 Fukuoka (JP).
 - (74) 代理人: 深見 久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 三井住友銀行南森町ビル Osaka (JP).
 - (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
 - (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 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), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- 添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: SETTLING METHOD USING MOBILE PHONE AND MOBILE PHONE

(54) 発明の名称: 携帯電話機を用いた決済方法および携帯電話機



- 12...USER
- Q...ORDER (MOBILE PHONE NUMBER)
- R...SERVICE USE NOT PERMITTED
- S...SETTLEMENT NOT PERMITTED (BALANCE IN THE RED)
- T...SETTLEMENT NOT PERMITTED (CANCELLED, REJECTED)
- U...SETTLEMENT NOT PERMITTED (ABNORMAL KEYCODE)
- V...SETTLEMENT COMPLETED
- W...COMMODITY
- 24...VIRTUAL STORE ON INTERNET
- A...BILLING REQUEST
- X...SALES PAYMENT CREDITED
- 11...PERSONAL INFORMATION DB
- 10...MOBILE PHONE FIRM
- B...MOBILE PHONE NUMBER
- C...E-MAIL ADDRESS
- D...PASSWORD
- E...USAGE STATUS
- 110...ADVANCE PAYMENT BALANCE
- 28...USAGE HISTORY DB
- 29...SETTLEMENT HISTORY DB
- F...KEYCODE
- G...ACCOUNT NUMBER
- H...CREDIT CARD
- I...DEBIT CARD
- J...BALANCE UPDATING
- K...ELECTRONIC BILLING
- L...BALANCE IN THE RED
- M...SETTLEMENT CANCELED/REJECTED
- O...SETTLEMENT OK (PASSWORD/MOBILE PHONE NUMBER/KEYCODE)
- P...SERVICE USE NOT PERMITTED (ABNORMAL KEYCODE)

(57) Abstract: A virtual account (110) is opened in a mobile phone firm (10) for each user (12) of a mobile phone (13). A user (12) deposits advance payment in a virtual account (110) using a mobile phone (13). Advance payment is paid in combination with telephone charges or by means of a credit card or a debit card. A balance of a virtual account is stored in

[続葉有]

WO 01/97118 A1



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。

a mobile phone (13). When shopping at a virtual store on the Internet, the phone number of a mobile phone (13) is transmitted, and , when shopping at a real store, the phone number is sent to a POS terminal. Each store bills a settlement amount to a mobile phone firm. Therefore, settlement can be made with high security and simplicity by using a mobile phone.

(57) 要約:

携帯電話機（13）の利用者（12）ごとに携帯電話会社（10）内に仮想口座（110）を設ける。利用者（12）は携帯電話機（13）を用いて仮想口座（110）に前払金を入金しておく。前払金は、通話料と合せて支払ったり、クレジットカードやデビットカードで支払う。携帯電話機（13）には仮想口座（110）の残高が記憶されている。インターネット上の仮想店舗で買物をする場合は携帯電話機（13）の電話番号を送信し、実店舗で買物をする場合は電話番号をPOS端末に送信する。各店舗は、携帯電話会社（10）に決済金額を請求する。したがって、高いセキュリティで簡単に携帯電話機を用いて決済することができる。

明細書

携帯電話機を用いた決済方法および携帯電話機

5 技術分野

この発明は、携帯電話機およびその携帯電話機を用いた決済方法に関し、さらに詳しくは、インターネット上の仮想店舗や実店舗における決済を仲介するサービスに関する。

10 背景技術

現在、携帯電話機を用いた種々の決済方法が提案されている。日経エレクトロニクス「携帯で決済」第769号、日経BP社(2000年5月8日)発行、109～129頁には、ICカードを搭載した携帯電話機が記載されている。この携帯電話機では、ICカードにクレジットカード番号をセキュアな状態で予め記録しておき、決済時にクレジットカード番号を暗号化して送信するようにしている。また、非接触型ICカード用のリーダ/ライタを搭載した携帯電話機も記載されている。この携帯電話機では、プリペイドカードの度数のような電子バリューをダウンロードし、これをリーダ/ライタにより非接触型ICカードに無線経由で転送するようにしている。利用者はこの非接触型ICカードを使って決済を行なう。

上記ICカードを搭載した携帯電話機ではクレジットカード番号を暗号化しているが、クレジットカード番号を送信していることに変わりはないので、インターネット上の電子商取引では十分なセキュリティとは言えない。

一方、上記リーダ/ライタを搭載した携帯電話機では、利用者は携帯電話機とともに非接触型ICカードを持ち歩かなければならない。また、リーダ/ライタはサイズが大きく、コストも高いなど、問題も多い。

この他、携帯電話機を用いた種々の決済方法が提案されているが、いずれも決済時に与信照会が必要であったり、決済データの送信が必要なため、決済時に電波を飛ばす必要があり、電波圏外では使用することができず、また、決済に時間

がかかるとい問題がある。

発明の開示

この発明は、上記のような問題を解決するためになされたもので、セキュリティが高く使い勝手のよい携帯電話機およびその携帯電話機を用いた決済方法を提
5 供することを目的とする。

この発明による携帯電話機を用いた決済方法は、売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であって、利用者の金銭を蓄積するための口座を利用者ごとに設けたサーバコンピュータにおいて、携帯電話機から送信
10 された金額を受信するステップと、受信した金額を利用者の口座に入金してその口座の残高を更新するステップと、更新した口座の残高を携帯電話機に送信するステップと、決済金額を受信するステップと、受信した決済金額を口座の残高から減じるステップと、受信した決済金額を売り主に支払うステップとを含む。ここでのサーバコンピュータは、携帯電話局（会社）、金融機関（会社）、決済機
15 関（会社）などに設置され得るが、その位置は特に限定されない。

一方、この発明による携帯電話機は、売り主と携帯電話機の利用者たる買い主との間の決済に用いられる携帯電話機であって、利用者の金銭を蓄積するための口座がサーバコンピュータに利用者ごとに設けられ、利用者の操作に応じて口座
20 に入金される所望の金額を入力する手段と、入力された金額を携帯電話局のコンピュータに送信し、サーバコンピュータから送信された仮想口座の残高を受信する送受信手段と、受信した口座の残高を記憶する手段とを備える。

この決済方法または携帯電話機によれば、利用者は携帯電話機を用いて所望の金額を携帯電話局または携帯電話局を通じて金融機関もしくは決済機関に送信する。携帯電話局、金融機関または決済機関は、携帯電話機から送信された金額を受
25 信し、その金額を利用者の口座に入金してその口座の残高を更新して携帯電話機に送信する。携帯電話機は、携帯電話局から送信された口座の残高を受信して記憶する。したがって、利用者は携帯電話機を財布のように使って決済を行なうことができる。ここでは、クレジット番号などを送信する必要がないので、セキュリティが高い。また、ICカードなどを持ち歩く必要もないので、使い勝手が

よい。

図面の簡単な説明

図 1 は、この発明の第 1 の実施の形態に従って仮想口座に入金する前払金額を
5 通話料と併せて支払う場合の資金移動を示す概略図である。

図 2 は、この発明の第 1 の実施の形態に従って仮想口座に入金する前払金額を
クレジットカードで支払う場合の資金移動を示す概略図である。

図 3 は、この発明の第 1 の実施の形態に従って仮想口座に入金する前払金額を
デビットカードで支払う場合の資金移動を示す概略図である。

10 図 4 は、この発明の第 1 の実施の形態に従って仮想口座に入金する前払金額を
銀行口座から自動引落しする場合の資金移動を示す概略図である。

図 5 は、この発明の第 1 の実施の形態に従って携帯電話機を用いてインターネ
ット上の仮想店舗で決済する方法を示す概略図である。

15 図 6 は、この発明の第 1 の実施の形態に従って携帯電話機を用いて実在店舗で
決済する方法を示す概略図である。

図 7 は、図 1 ～図 4 に示したように仮想口座に前払金を入金するために用いら
れる、携帯電話機および携帯電話会社のサーバのハードウェア構成を示すブロッ
ク図である。

20 図 8 は、図 1 に示した場合における、図 7 に示した携帯電話機および携帯電
話会社のサーバの動作を示すフローチャートである。

図 9 は、図 8 に示した携帯電話機の動作中に表示される画面の遷移図である。

図 10 は、図 2 に示した場合における、図 7 に示した携帯電話機および携帯電
話会社のサーバの動作を示すフローチャートである。

25 図 11 は、図 10 に示した携帯電話機の動作中に表示される画面の遷移図であ
る。

図 12 は、図 3 に示した場合における、図 7 に示した携帯電話機および携帯電
話会社のサーバの動作を示すフローチャートである。

図 13 は、図 12 に示した携帯電話機の動作中に表示される画面の遷移図であ
る。

図 1 4 は、図 4 に示した場合における、図 7 に示した携帯電話機および携帯電話会社のサーバの動作を示すフローチャートである。

図 1 5 は、図 1 4 に示した携帯電話の動作中に表示される画面の遷移図である。

5 図 1 6 は、この発明の第 1 の実施の形態に従ってインターネット上の仮想店舗で携帯電話機を用いて決済する場合に用いられる、携帯電話機、携帯電話会社のサーバ、パーソナルコンピュータ、および仮想店舗のサーバのハードウェア構成を示すブロック図である。

10 図 1 7 は、図 5 に示した場合における図 1 6 に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

図 1 8 は、図 1 7 に続くフローチャートである。

図 1 9 は、図 1 7 および図 1 8 に示した携帯電話機の動作中に表示される画面の遷移図である。

15 図 2 0 は、図 6 に示した場合に用いられる、携帯電話機、携帯電話会社のサーバ、および実在店舗の P O S 端末のハードウェア構成を示すブロック図である。

図 2 1 は、図 2 0 に示した携帯電話機、実在店舗の P O S 端末、および携帯電話会社のサーバの動作を示すフローチャートである。

図 2 2 は、図 2 1 に続くフローチャートである。

20 図 2 3 は、図 2 1 および図 2 2 に示した携帯電話機の動作中に表示される画面の遷移図である。

図 2 4 は、携帯電話機の R A M および R O M に記憶される情報を示す図である。

図 2 5 は、この発明の第 2 の実施の形態に従って実在口座から仮想口座に振替える場合の資金移動を示す概略図である。

25 図 2 6 は、図 2 5 に示したように実在口座から仮想口座への振替に用いられる携帯電話機、携帯電話会社のサーバおよび金融機関のサーバのハードウェア構成を示すブロック図である。

図 2 7 は、図 2 5 に示した場合における、図 2 6 に示した携帯電話機、携帯電話会社のサーバ、および金融機関のサーバの動作を示すフローチャートである。

図 2 8 は、図 2 7 に続くフローチャートである。

図 29 は、図 27 および図 28 に示した携帯電話機の動作中に表示される画面の遷移図である。

図 30 は、この発明の第 2 の実施例に従って携帯電話機を用いてインターネット上の仮想店舗で決済する方法を示す概略図である。

5 図 31 は、図 30 に示した場合に用いられるパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、金融機関のサーバ、決済機関のサーバ、および仮想店舗のサーバのハードウェア構成を示すブロック図である。

10 図 32 は、図 30 に示した場合における、図 31 に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、仮想店舗のサーバ、および金融機関サーバの動作を示すフローチャートである。

図 33 は、図 32 に続くフローチャートである。

図 34 は、図 33 に続くフローチャートである。

図 35 は、図 32 ~ 図 34 に示した携帯電話機の動作中に表示される画面の遷移図である。

15 図 36 は、この発明の第 2 の実施の形態に従って携帯電話機を用いて実在店舗で決済する方法を示す概略図である。

図 37 は、図 36 に示した場合に用いられる、携帯電話機、実在店舗の POS 端末、携帯電話会社のサーバ、金融機関のサーバ、および決済機関のサーバのハードウェア構成を示すブロック図である。

20 図 38 は、図 36 に示した場合における、図 37 に示した携帯電話機、POS 端末、携帯電話会社のサーバ、金融機関のサーバの動作を示すフローチャートである。

図 39 は、図 38 に続くフローチャートである。

図 40 は、図 39 に続くフローチャートである。

25 図 41 は、この発明の第 3 の実施の形態に従ってサービスの利用者情報を登録する方法を示す概略図である。

図 42 は、この発明の第 3 の実施の形態に従って仮想口座に前払金額を入金する場合の資金移動を示す概略図である。

図 43 は、この発明の第 3 の実施の形態に従って携帯電話機を用いてインター

ネット上の仮想店舗で決済する方法を示す概略図である。

図 4 4 は、この発明の第 3 の実施の形態に従って携帯電話機を用いて実在店舗で決済する方法を示す概略図である。

5 図 4 5 は、この発明の第 3 の実施の形態に従って決済機関が利用者に対して携帯電話機に蓄積されている未通知データを要求する方法を示す概略図である。

図 4 6 は、この発明の第 3 の実施の形態に従って携帯電話機を用いてインターネット上の仮想店舗で決済する場合において決済機関が金融機関に対する請求を代行する方法を示す概略図である。

10 図 4 7 は、図 4 1 に示した利用登録に用いられる、携帯電話機、携帯電話会社のサーバおよび決済機関のサーバのハードウェア構成を示すブロック図である。

図 4 8 は、図 4 1 に示した場合における、図 4 7 に示した携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

15 図 4 9 は、図 4 2 に示した仮想口座への資金移動に用いられる、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび金融機関のサーバのハードウェア構成を示すブロック図である。

図 5 0 は、図 4 2 に示した場合における、図 4 9 に示した携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

図 5 1 は、図 5 0 に続くフローチャートである。

図 5 2 は、図 5 1 に続くフローチャートである。

20 図 5 3 は、図 4 3 に示した仮想店舗での決済に用いられる、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび仮想店舗のサーバのハードウェア構成を示すブロック図である。

25 図 5 4 は、図 4 3 に示した場合における、図 5 3 に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバおよび仮想店舗のサーバの動作を示すフローチャートである。

図 5 5 は、図 5 4 に続くフローチャートである。

図 5 6 は、図 5 5 に続くフローチャートである。

図 5 7 は、図 4 4 に示した実在店舗での決済に用いられる、携帯電話機、POS 端末、携帯電話会社のサーバおよび決済機関のサーバのハードウェア構成を示

すブロック図である。

図 58 は、図 44 に示した場合における、図 57 に示した携帯電話機、POS 端末、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

5 図 59 は、図 58 に続くフローチャートである。

図 60 は、図 59 に続くフローチャートである。

図 61 は、図 45 に示した未通知データの要求の場合における、携帯電話機、携帯電話会社のサーバおよび決済機関のサーバの動作を示すフローチャートである。

10 図 62 は、図 46 に示した請求代行に用いられる、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、金融機関のサーバおよび仮想店舗のサーバのハードウェア構成を示すブロック図である。

図 63 は、図 46 に示した場合における、図 62 に示したパーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、金融機関のサーバおよび仮想店舗のサーバの動作を示すフローチャートである。

15 図 64 は、図 63 に続くフローチャートである。

図 65 は、この発明の第 4 の実施の形態に従う前払方法を示す概略図である。

図 66 は、図 65 に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

20 図 67 は、図 66 に続くフローチャートである。

図 68 は、この発明の第 4 の実施の形態に従う第 1 の送金方法を示す概念図である。

図 69 は、図 68 に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

25 図 70 は、図 69 に続くフローチャートである。

図 71 は、この発明の第 4 の実施の形態に従う第 2 の送金方法を示す概念図です。

図 72 は、図 71 に示した場合における、パーソナルコンピュータ、携帯電話

機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

図 7 3 は、図 7 2 に続くフローチャートである。

5 図 7 4 は、この発明の第 4 の実施の形態に従って、小口決済履歴がない場合におけるワンタイム ID の発行方法を示す概念図である。

図 7 5 は、この発明の第 4 の実施の形態に従って、小口決済履歴がある場合におけるワンタイム ID の発行方法を示す概念図である。

図 7 6 は、図 7 4 および図 7 5 に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

10 図 7 7 は、図 7 6 に続くフローチャートである。

図 7 8 は、この発明の第 4 の実施の形態に従い、ワンタイム ID を使用して実在店舗で決済する方法を示す概念図である。

図 7 9 は、図 7 8 に示した場合における、携帯電話機、実在店舗の POS 端末、および決済機関のサーバの動作を示すフローチャートである。

15

発明を実施するための最良の形態

以下、この発明の実施の形態を図面を参照して詳しく説明する。図中同一または相当部分には同一符号を付してその説明は繰返さない。

[第 1 の実施の形態]

20 1. サービスの概要

この発明の実施の形態は、携帯電話会社が提供する新規サービス（「お財布サービス」と呼び、以下単に「本サービス」という）を実現するためのコンピュータシステムに関するものである。本サービスは、携帯電話機を財布のように使用できるようにするものである。以下、本サービスの概要を説明する。

25 携帯電話機購入の際、通話料金を引落す銀行口座以外に、クレジットカード番号やキャッシュカード番号などを携帯電話会社に登録する。携帯電話会社は、携帯電話機の利用者ごとに仮想口座を設ける。利用者は、決済の前に、仮想口座に前払金を入金するように、携帯電話機を用いて携帯電話会社に要請する。携帯電話会社は、予め登録されている銀行口座、クレジットカード番号、キャッシュカ

ード番号などを用い、利用者に対して前払金の請求を行なう。前払金の支払方法は、利用者が選択することができる。前払金の請求後、携帯電話会社は、仮想口座に前払金を入金したうえで仮想口座の残高を携帯電話機に送信する。携帯電話機は、送信された仮想口座の残高を記憶する。利用者は、この携帯電話機を財布
5 代わりに使ってインターネット上の仮想店舗や実店舗で決済を行なう。店舗は、携帯電話会社に対して請求を行なう。

2. 前払金の支払方法

次に、4通りの前払金の支払方法について説明する。

2-1. 通話料と併せて支払う場合

10 図1は、前払金を通話料と併せて支払う場合の資金移動を示す概略図である。図1に示すように、携帯電話会社（携帯電話局）10には、個人情報データベース11が設けられている。個人情報データベース11には、各利用者12の個人情報が登録されている。具体的には、前払金（携帯電話会社にとっては前受金）を蓄積するための仮想口座110が設けられ、携帯電話機13の電話番号の他、
15 電子メールアドレス、パスワード、利用状況、キーコード、口座番号、クレジットカード番号、デビットカード番号などが予め登録されている。

まず、利用者12は携帯電話機13を用いて所望の前払金額とその支払方法（ここでは「通話料に加算」）とを携帯電話会社10に送信する。このとき、携帯電話機13の電話番号も併せて送信する。

20 携帯電話会社10は、送信された携帯電話番号に基づいて個人情報データベース11を検索し、利用者12の仮想口座110の利用状況を照会する。利用者12に問題がなければ（利用状況が「OK」であれば）、携帯電話会社10は送信された前払金額を仮想口座110の前受残高に加算し、更新した最新の前受残高を送信する。一方、利用者12の支払いが滞っていたり、本サービスの利用が停
25 止されている場合、利用状況は「NG」となっている。この場合、携帯電話会社10は携帯電話機13を通じて本サービスを利用できない旨を利用者12に通知する。

上記のように利用者12が支払方法として「通話料に加算」を選択した場合、携帯電話会社10は、基本料金と通話料金の請求書14と併せて本サービスの利

用明細書 1 5 を利用者 1 2 に送付する。

携帯電話会社 1 0 は、個人情報データベース 1 1 に登録されている口座番号に基づいて利用者 1 2 の取引銀行 1 7 に利用料金の引落しを依頼する。これに応じて銀行 1 7 は、利用者 1 2 の口座 1 6 から、銀行 1 8 に開設されている携帯電話会社 1 0 の口座 1 9 に資金を振替える。

2-2. クレジットカードで支払う場合

図 2 は、前払金をクレジットカードで支払う場合の資金移動を示す概略図である。この場合、図 2 に示すように、利用者 1 2 は携帯電話機 1 3 を用いて前払金額とその支払方法（ここでは「クレジットカード」）とを携帯電話会社 1 0 に送信する。

携帯電話会社 1 0 は、利用者 1 2 の利用状況に問題がなければ、予め登録されているクレジットカード番号に基づいて信販会社 2 0 に承認を依頼する。信販会社 2 0 は、承認できる場合はその旨を携帯電話会社 1 0 に通知する。これに応じて、携帯電話会社 1 0 は仮想口座 1 1 0 の前受残高を更新し、その最新の前受残高を携帯電話機 1 3 に送信する。一方、承認できない場合は、信販会社 2 0 はその旨を携帯電話会社 1 0 に通知する。これに応じて、携帯電話会社 1 0 は前受残高を更新することなく、クレジットカードによる支払いができない旨を利用者 1 2 に通知する。

支払いを承認した場合、信販会社 2 0 は、利用者 1 2 が所望した前払金額を携帯電話会社 1 0 の口座 1 9 に振込む。次いで信販会社 2 0 は、銀行 1 7 に対して利用者 1 2 の口座 1 6 から前払金額を引落すように依頼する。これに応じて銀行 1 7 は、利用者 1 2 の口座 1 6 から信販会社 2 0 に資金を振替える。

2-3. デビットカードで支払う場合

図 3 は、前払金をデビットカードで支払う場合の資金移動を示す概略図である。この場合、図 3 に示すように、利用者 1 2 は携帯電話機 1 3 を用いて前払金額とその決済方法（ここでは「デビットカード」）とを携帯電話会社 1 0 に送信する。

携帯電話会社 1 0 は、利用者 1 2 の利用状況に問題がなければ、予め登録されているデビットカード番号に基づいてそのデビットカードを発行した銀行 1 7 に資金の振替えを依頼する。振替え依頼を承認した場合、銀行 1 7 はその振替えデ

ータをクリアリングセンター 21 に送信するとともに、振替えの完了を携帯電話会社 10 に通知する。これに応じて携帯電話会社 10 は、前受残高を更新し、その最新の前受残高を携帯電話機 13 に送信する。一方、銀行 17 が振替え依頼を承認しない場合、振替えできない旨を携帯電話会社 10 に通知する。これに応じて携帯電話会社 10 は、前受残高を更新することなく、デビットカードで支払いできない旨を利用者 12 に通知する。

クリアリングセンター 21 は、銀行 17 の他、多数の銀行から送信された振替えデータに基づいて振替えの相殺および集計を行ない、銀行間の決済尻データを決済銀行 22 に送信する。これに応じて決済銀行 22 は、銀行 17 から加盟店銀行 23 に資金を振替える。これに応じて加盟店銀行 23 は、その資金を携帯電話会社 10 の口座 19 に入金する。

2-4. 自動引落しで支払う場合

図 4 は、前受金を銀行口座から自動引落しで支払う場合の資金移動を示す概略図である。この場合、図 4 に示すように、利用者 12 は携帯電話機 13 を用いて前払金額とその支払方法（ここでは「自動引落」とを携帯電話会社 10 に送信する。携帯電話会社 10 は、利用者 12 の利用状況に問題がなければ、予め登録されている口座番号に基づいて銀行 17 に資金の引落しを依頼する。引落しが可能な場合、銀行 17 はその旨を携帯電話会社 10 に通知する。これに応じて携帯電話会社 10 は、前受残高を更新し、最新の前受残高を携帯電話機 13 に送信する。引落しが不可能な場合、銀行 17 はその旨を携帯電話会社 10 に通知する。これに応じて携帯電話会社 10 は、支払いできない旨を利用者 12 に通知する。携帯電話会社 10 から引落し依頼を受けた銀行 17 は直ちに、利用者 12 の口座 16 から携帯電話会社 10 の口座 19 に資金を振替える。これとは別に、利用明細書 15 は請求書 14 と併せて利用者 12 に送付される。

3. 決済

次に、携帯電話機 13 を使って上述した前払金で決済を行なう方法について説明する。

3-1. インターネット上の仮想店舗での決済

図 5 は、インターネット上の仮想店舗で携帯電話機を使って決済する方法を示

す概略図である。図 5 に示すように、まず、利用者 1 2 は携帯電話機 1 3 または
パーソナルコンピュータ 4 0 でインターネット上の仮想店舗 2 4 に商品やサー
ビスを注文し、その決済方法（ここでは「携帯電話決済」）を選択する。パー
ソナルコンピュータ 4 0 を用いる場合、利用者 1 2 は携帯電話機 1 3 の電話番号をパ
5 パーソナルコンピュータ 4 0 に手で入力し、インターネット 6 0 を通じて仮想店舗
2 4 に送信する。

注文を受けた仮想店舗 2 4 は、送信された携帯電話番号に基づいて携帯電話会
社 1 0 に決済金額の請求を依頼する。

請求依頼を受けた携帯電話会社 1 0 は、利用者 1 2 の利用状況に問題があれば
10 本サービスが利用できない旨を仮想店舗 2 4 に通知する。これに応じて仮想店舗
2 4 は、本サービスが利用できない旨を利用者 1 2 に通知する。利用者 1 2 の利
用状況に問題がなければ、携帯電話会社 1 0 は予め登録されている利用者 1 2 の
電子メールアドレスに基づいて利用者 1 2 の携帯電話機 1 3 に電子メールで電子
請求書を送信する。電子請求書は、仮想口座 1 1 0 からの支払いを利用者 1 2 に
15 確認するためのものである。

また、電子請求書を受取った利用者 1 2 は、その決済を承認するか否かを選択
する。利用者 1 2 が決済を承認した場合、電子請求書を受信した携帯電話機 1 3
は、前払残高を検証し、前払残高が決済金額を下回っている場合、携帯電話機 1
3 は残高不足として決済ができない旨を携帯電話会社 1 0 に通知する。これに
20 応じて携帯電話会社 1 0 は、残高が不足しているから決済できない旨を仮想店舗 2
4 を通じて利用者 1 2 に通知する。利用者 1 2 が決済を取消しまたは拒否した場
合、決済取消しまたは決済拒否を携帯電話会社 1 0 に通知する。これに応じて携
帯電話会社 1 0 は、決済が取消しまたは拒否されたから決済できない旨を仮想店
舗 2 4 に通知する。これに応じて仮想店舗 2 4 は、決済できない旨を利用者 1 2
25 に通知する。

また、利用者 1 2 が決済を承認した場合において、前払残高の検証の結果、決
済金額が前払残高以内のとき、その決済を了承する旨を携帯電話会社 1 0 に通知
する。このとき、予め携帯電話会社 1 0 に登録されているパスワード、携帯電話
番号、キーコードなどを併せて送信する。携帯電話会社 1 0 は、送信された携帯

電話番号に基づいて個人情報データベース 11 を検索し、送信されたパスワードおよびキーコードが予め登録されているパスワードおよびキーコードとそれぞれ一致するか否かを判別する。キーコードが一致しない場合、携帯電話会社 10 はキーコードが異常であるから本サービスを利用できない旨を利用者 12 に通知するとともに、決済できない旨を仮想店舗 24 を通じて利用者 12 に通知する。両者とも一致する場合、携帯電話会社 10 は仮想口座 110 の前受残高から決済金額を減算して前受残高を更新するとともに、その更新した前受残高を携帯電話機 13 に送信する。これに応じて携帯電話機 13 は内部の前受残高を更新する。また、携帯電話会社 10 は決済完了を仮想店舗 24 に通知する。これに応じて仮想店舗 24 は決済完了を利用者 12 に通知する。

その後、仮想店舗 24 は注文を受けた商品を利用者 12 に届けたり、注文を受けたサービスを利用者 12 に提供する。携帯電話会社 10 は、上記決済金額を仮想店舗 24 に入金する。仮想店舗 24 は、本サービスを利用した手数料を携帯電話会社 10 に支払う。

15 3-2. 実在店舗での決済

図 6 は、実在店舗で携帯電話機を使って決済する方法を示す概略図である。図 6 に示すように、実在店舗において、利用者 12 は携帯電話機 13 を POS 端末 27 に接続された読取装置 270 にセットする。店員は商品の金額を POS 端末 27 に打ち込み、決済金額を計算する。この決済金額は POS 端末 27 から読取装置 270 を通じて携帯電話機 13 に送信される。携帯電話機 13 は、内部に記憶されている残高と決済金額とを比較し、決済が不可能であればエラーを POS 端末 27 に送信する。一方、決済が可能であれば、携帯電話機 13 は携帯電話番号とキーコードとを POS 端末 27 に送信する。携帯電話番号は、POS 端末 27 に手で直接入力することはできない。

25 携帯電話番号とキーコードとを受信した POS 端末 27 は決済を完了して、その旨を携帯電話機 13 に通知する。決済完了を受けて、携帯電話機 13 はその決済金額を内部メモリに記憶し、決済モードがオフになる。その後、利用者 12 は携帯電話機 13 を読取装置 270 から取り除く。

次に、決済金額とともに携帯電話番号およびキーコードを携帯電話会社 10 に

送信する。これに応じて携帯電話会社10は、仮想口座110の前受残高から決済金額を減算して前受残高を更新するとともに、決済完了をPOS端末27に通知する。

4. ハードウェア構成

5 図7は、携帯電話機13、および携帯電話会社10に設置されるサーバコンピュータ（以下、単にサーバという）30のハードウェア構成を示すブロック図である。

図7に示すように、携帯電話機13は、CPUからなるデータ処理部131と、RAM132と、EEPROMのようなROM133と、アンテナ134と、送受信部135と、テンキーやカーソルキーのような入力装置136と、液晶ディスプレイのような表示装置137と、バッテリー138と、インターフェイス（I/F）部139とを備える。この携帯電話機13は電源アダプタ140に装着され、電源アダプタ140からI/F部139を通じてバッテリー138に電流が供給され、バッテリー138が充電される。データ処理部131は、RAM132、ROM133、送受信部135、入力装置136、表示装置137およびI/F部139を用いて通常の携帯電話機能を実行する他、後述する決済機能を実行する。

携帯電話会社10に設置されているサーバ30は、CPUからなるデータ処理部301と、データベース302とを備える。データベース302は、個人情報データベース11と、利用履歴データベース28と、決済履歴データベース29とを含む。データ処理部301はデータベース302を用いて後述する決済機能を実行する。データ処理部301は無線基地局303に接続されている。無線基地局303のアンテナ304と携帯電話機13のアンテナ134との間で電波が送受信される。利用履歴データベース28は、携帯電話機13とのデータの取引内容を記録するためのログファイルである。具体的には、仮想口座110の入出金日時、入出金額、残高などが記録される。決済履歴データベース29は、店舗とのデータの取引内容を記録するためのログファイルである。具体的には、決済日時、決済金額などが記録される。

5. 前払い時の処理動作

5-1. 通話料と併せて支払う場合

図8は、図1に示した前払金を通話料と併せて支払う場合における携帯電話機13およびサーバ30の動作を示すフローチャートである。図9は、この場合に携帯電話機13の表示装置137に表示される表示画面の遷移図である。

5 まず、携帯電話機13のデータ処理部131は、表示装置137上に図9に示した画面D1を表示し、利用者12に対してパスワードの入力を促す。利用者12が入力装置136を操作してパスワードを入力すると、入力装置136はその入力されたパスワードをデータ処理部131に与える（S101）。

10 続いて、データ処理部131はその入力されたパスワードをRAM132またはROM133に予め登録されているパスワードと比較することにより入力されたパスワードの検証を行なう（S102）。入力されたパスワードが誤っている場合、データ処理部131は表示装置137上に図9に示した画面D2を表示する（S103）。一方、入力されたパスワードが正しい場合、データ処理部131は表示装置137上に図9に示した画面D3を表示し、利用者12に対し、「①お金を払う」、「②お財布の中を見る」、「③お財布にお金を入れる」の中から1つを選択するよう促す。利用者12が入力装置136を操作し、「③お財布にお金を入れる」を選択すると、データ処理部131は表示装置137上に画面D4を表示し、利用者12に対して前払金額の入力を促す。このとき、未通知データ（詳細は後述する）がない場合はRAM132に記憶されている前払残高を現在の残高として表示し、未通知データがある場合はRAM132に記憶されている前払残高から未通知の決済金額を減算して真の前払残高を計算し、それを現在の残高として表示する。利用者12が入力装置136を操作して所望の前払金額を入力すると、入力装置136がその入力された前払金額をデータ処理部131に与える（S104）。

25 続いて、データ処理部131は表示装置137上に画面D5を表示し、利用者12に対して前払金額の支払方法を選択するよう促す。利用者12が入力装置136を操作すると、「通話料に加算」という支払方法の他、「クレジット」、「デビットカード」、「自動引落」といういくつかの支払方法が表示される。ここでは利用者12が「通話料に加算」という支払方法を選択するものとする。こ

れに応じて、入力装置 136 は「通話料に加算」という支払方法の選択をデータ処理部 131 に与える (S105)。

続いて、データ処理部 131 は選択された支払方法および入力された前払金額を送受信部 135 に与え、送受信部 135 はこれらを携帯電話会社 10 に送信する (S106)。このとき、ROM133 に予め記憶されている利用者 12 に固有の携帯電話番号と、ROM133 に予め記憶されている携帯電話機 13 に固有のキーコードと、RAM132 に記憶されている未通知データとを併せて送信する。携帯電話番号は、携帯電話会社 10 が携帯電話機 13 を販売する際に EEPROM のような ROM133 に予めプログラムする。キーコードは、携帯電話機メーカーが携帯電話機を製造する際に製造番号や各携帯電話機固有の管理番号 (サブスライバ ID (識別子)、機体 ID、端末 ID などと呼ばれる) などを EEPROM のような ROM133 に予めプログラムする。したがって、携帯電話番号は利用者 12 に固有のもので、携帯電話機 13 を買い換えた場合でも同じ携帯電話番号を登録することができる。ただし、利用者 12 自身は携帯電話番号を書き換えることはできず、利用者 12 の依頼に応じて携帯電話会社 10 が書き換えることになる。これに対し、キーコードは携帯電話機 13 に固有のものである。キーコードに製造番号を用いた場合、利用者 12 はもちろん、携帯電話会社 10 さえも書き換えることができない。キーコードに上述したサブスライバ ID のような管理番号を用いた場合、携帯電話会社 10 は書き換えることができるが、利用者 12 は書き換えることができない。

続いて、データ処理部 131 はこれまでの処理が正常に終了したか否かを判別し (S107)、正常に終了していない場合はその旨を表示装置 137 に表示し (S108)、接続を切断する (S109)。一方、正常に終了した場合は異常終了の表示をすることなく接続を一旦切断する (S109)。

一方、携帯電話会社 10 に設置されているサーバ 30 において、データ処理部 301 は、携帯電話機 13 から送信された前払金額、支払方法、携帯電話番号およびキーコードを無線基地局 303 を通じて受信する (S201)。

続いて、データ処理部 301 は受信した携帯電話番号に基づいて個人情報データベース 11 を検索する (S202)。

続いて、データ処理部 301 は受信したキーコードを検索した個人情報データベース 11 のキーコードと比較し、キーコードが一致するか否か確認する (S203)。キーコードが一致した場合、データ処理部 301 は個人情報データベース 11 の利用状況を確認し、問題があるか否か判別する (S204)。上記ステップ S202 でキーコードが一致しない場合、またはこのステップ S204 で利用状況に問題がある場合、データ処理部 301 は本サービス利用不可の情報を携帯電話機 13 に送信する (S205)。

携帯電話機 13 においては、送受信部 135 が携帯電話機 13 から送信された本サービス利用不可能の情報を受信する (S110)。

10 続いて、データ処理部 131 は図 9 に示した画面 D6 を表示装置 137 上に表示し、本サービスを利用できない旨を利用者 12 に通知する (S111)。そして、データ処理部 131 は表示装置 137 上に異常に終了した旨を表示する (S112)。

一方、上記ステップ S204 で利用状況に問題がなければ、利用履歴データベース 28 を更新する (S206)。具体的には、現在の日時と、今回の前受金額 (利用者 12 にとっては前払金額) と、現在の前受残高と、未通知データ (未通知の決済金額) とを利用履歴データベース 28 に記録する。

続いて、データ処理部 301 は現在の前受残高を携帯電話機 13 に送信する (S207)。

20 続いて、データ処理部 301 はこの前受金額について請求データを作成する (S208)。

続いて、データ処理部 301 は作成した請求データを毎月一括して通話料に加算し、図 1 に示すように請求書 14 とともに本サービスの利用明細書 15 を発行する。

25 以降の処理は既存の処理と同じで、利用者 12 の個人情報データベース 11 に登録されている口座番号に基づき利用者 12 の取引銀行 17 に対して料金の引落しを依頼する (S209)。これに応じて、本サービスの利用料金が通話料と併せて利用者の口座 16 から携帯電話会社の口座 19 に振替えられる。

携帯電話機 13 においては、上記ステップ S207 でサーバ 30 から送信され

た前受残高を送受信部 135 が受信する (S 113)。

続いて、データ処理部 131 は受信した前受残高を前払残高として RAM 132 に格納し、これにより前受残高を更新する (S 116)。

5 続いて、データ処理部 131 は図 9 に示した画面 D7 を表示装置 137 に表示する (S 117)。具体的には、これまでの前払処理が完了した旨と現在の前払残高とを表示する。

5-2. クレジットカードで支払う場合

10 図 10 は、図 2 に示した前払金額をクレジットカードで支払う場合における携帯電話機 13 およびサーバ 30 の動作を示すフローチャートである。図 11 は、この場合に携帯電話機 13 の表示装置 137 に表示される画面の遷移図である。

上記と異なり前払金額をクレジットカードで支払う場合は、図 11 に示した画面 D5 で利用者 12 は「クレジット (一括)」を選択する。これに応じて、入力装置 136 はクレジットカードによる支払いという支払方法の選択をデータ処理部 131 に与える (図 10, S 105)。

15 また、携帯電話会社 10 のサーバ 30 においては、利用状況に問題がない場合、個人情報データベース 11 に予め登録されているクレジットカード番号に基づいて信販会社 20 に利用者 12 の与信照会を行なう (S 210)。

続いて、データ処理部 301 は信販会社 20 からの返信に基づいて信販会社 20 がクレジットカードによる支払いを承認したか否かを判別する (S 211)。

20 非承認の場合、データ処理部 301 は支払できない旨を携帯電話機 13 に送信する (S 212)。承認の場合は、利用履歴データベース 28 を更新する (S 205)。

25 一方、携帯電話機 13 においては、送受信部 135 がサーバ 30 からクレジットカードによる支払いは不可能な旨を受信した場合、図 12 に示した画面 D8 を表示装置 137 に表示し、クレジットカードによる支払いが不可能な旨を利用者 12 に通知する (S 120)。

5-3. デビットカードで支払う場合

図 12 は、前払金額をデビットカードで支払う場合の携帯電話機 13 およびサーバ 30 の動作を示すフローチャートである。図 13 は、この場合に携帯電話機

1 3 の表示装置 1 3 7 に表示される画面の遷移図である。

上記と異なり前払金額をデビットカードで支払う場合、図 1 3 に示した表示画面 D 5 において利用者 1 2 は「デビットカード」を選択する。これに応じて、入力装置 1 3 6 はその選択情報をデータ処理部 1 3 1 に与える (S 1 0 5)。

5 一方、携帯電話会社 1 0 のサーバ 3 0 においては、利用状況に問題がない場合、データ処理部 3 0 1 は個人情報データベース 1 1 に予め登録されているデビットカード番号に基づいてそのデビットカードの発行銀行 1 7 に引落とし (承認) 依頼を送信する (S 2 2 0)。これに応じて、既存のデビットカード処理が実行される (S 2 2 1)。

10 続いて、データ処理部 3 0 1 はデビットカードの発行銀行 1 7 から送信された振替結果に基づいて振替が完了したか否かを判別する (S 2 2 2)。振替ができなかった場合、データ処理部 3 0 1 はその旨を携帯電話機 1 3 に送信する (S 2 1 2)。

これに応じて携帯電話機 1 3 のデータ処理部 1 3 1 は、図 1 3 に示した画面 D 15 9 を表示装置 1 3 7 に表示し (S 1 2 0)、デビットカードによる支払いができない旨を利用者 1 2 に通知する。

5-4. 自動引落で即時支払う場合

図 1 4 は、図 4 に示した前払金額を利用者の口座 1 6 から自動的に引落とす場合における携帯電話機 1 3 およびサーバ 3 0 の動作を示すフローチャートである。

20 図 1 5 は、この場合に携帯電話機 1 3 の表示装置 1 3 7 に表示される画面の遷移図である。

上記と異なり自動引落の場合、図 1 5 に示した画面 D 5 で利用者 1 2 は「自動引落」を選択し、この利用者 1 2 の操作に応じて入力装置 1 3 6 はデータ処理部 1 3 1 にその選択情報を与える (S 1 0 5)。

25 一方、サーバ 3 0 においては、利用状況に問題がない場合、データ処理部 3 0 1 は受信した前払金額が引落とし可能か否かを利用者 1 2 の取引銀行 1 7 に照会する (S 2 3 0)。

続いて、データ処理部 3 0 1 は銀行 1 7 から返信された照会結果に基づいて引落としが可能か否かを判別する (S 2 3 1)。引落としが不可能な場合、データ処理

部 3 0 1 はその旨を携帯電話機 1 3 に送信する (S 2 3 2)。

これに応じて携帯電話機 1 3 のデータ処理部 1 3 1 は、図 1 5 に示した画面 D 1 0 を表示し (S 1 2 0)、利用者の口座 1 6 からは所望の前払金額を引落すことができない旨を利用者 1 2 に通知する。

5 一方、引落しが可能な場合、携帯電話会社 1 0 は既存の方法で銀行 1 7 に引落しを依頼する (S 2 2 3)。

6. 決済時の処理動作

次に、携帯電話機 1 3 を用いてインターネット上の仮想店舗および実店舗で決済を行なう場合の動作について説明する。

10 6-1. 仮想店舗で決済する場合

図 1 6 は、仮想店舗で決済を行なう場合に用いられる利用者のパーソナルコンピュータ (P C) 4 0 および携帯電話機 1 3、携帯電話会社のサーバ 3 0、ならびに仮想店舗のサーバコンピュータ (以下、単にサーバという) 5 0 のハードウェア構成を示すブロック図である。

15 図 1 6 に示すように、利用者 1 2 のパーソナルコンピュータ 4 0 は、CPU のようなデータ処理部 4 0 1 と、ROM や RAM のようなメモリ 4 0 2 と、ハードディスク (H D) 4 0 3 と、モデム 4 0 4 と、キーボードやマウスのような入力装置 4 0 5 と、C R T ディスプレイや液晶ディスプレイのような表示装置 4 0 6 とを備える。仮想店舗 2 4 のサーバ 5 0 も同様に、データ処理部 5 0 1 と、メモリ 5 0 2 と、ハードディスク 5 0 3 と、モデム 5 0 4 と、入力装置 5 0 5 と、表示装置 5 0 6 とを備える。パーソナルコンピュータ 4 0 はモデム 4 0 4 を通じて
20 インターネット 6 0 に接続される。サーバ 5 0 もモデム 5 0 4 を通じてインターネット 6 0 に接続される。携帯電話会社 1 0 のサーバ 3 0 もモデム 3 0 3 を通じてインターネット 6 0 に接続される。

25 図 1 7 および図 1 8 は、図 1 6 に示したパーソナルコンピュータ 4 0、携帯電話機 1 3、サーバ 3 0 および 5 0 の動作を示すフローチャートである。

利用者 1 2 はパーソナルコンピュータ 4 0 の入力装置 4 0 5 を操作して仮想店舗 2 4 に商品やサービスの注文を行ない、その決済方法として携帯電話決済を選択する。これに応じて、パーソナルコンピュータ 4 0 のデータ処理部 4 0 1 は入

力された注文情報および携帯電話番号をインターネット 60 を通じて仮想店舗 24 のサーバ 50 に送信する (S301)。

サーバ 50 のデータ処理部 501 は、送信された注文情報および携帯電話番号を受信する (S601)。

- 5 続いて、データ処理部 501 は、店舗名、決済金額、携帯電話番号などの請求情報をインターネット 60 を通じて携帯電話会社 10 のサーバ 30 に送信することにより、携帯電話会社 10 に利用者 12 の決済金額を請求する (S602)。

サーバ 30 のデータ処理部 301 は、送信された請求情報を受信する (S501)。

- 10 続いて、データ処理部 301 は受信した携帯電話番号に基づいて個人情報データベース 11 を検索する (S502)。

続いて、データ処理部 301 は検索した利用者 12 の個人情報の中から利用状況を照会し、問題がないか否か確認する (S503)。問題がある場合、データ

- 15 処理部 301 は本サービス利用不可の情報をサーバ 50 に送信する。これにより、本サービスを利用できない旨を仮想店舗 24 に通知する (S504)。一方、利用状況に問題がない場合、データ処理部 301 は検索した個人情報の中から利用者 12 の電子メールアドレスを特定し、電子メールで請求データを携帯電話機 13 に送信する (S505)。これは、携帯電話会社 10 が仮想店舗 24 に代わっ

て利用者 12 に請求書を発行することを意味する。利用者 12 の携帯電話機 13

20 においては、送受信部 135 が携帯電話会社 10 のサーバ 30 から送信された請求データを受信する (S401)。

- 利用者 12 が携帯電話機 13 の入力装置 136 を操作して「受信メール一覧」を選択すると、携帯電話機 13 のデータ処理部 131 は図 19 に示した画面 D11 を表示装置 137 上に表示する。利用者 12 が入力装置 136 を操作して請求
- 25 データの電子メールを選択すると、データ処理部 131 は画面 D12 を表示装置 137 上に表示する。これは電子請求書であり、注文日、注文者（通常は利用者 12 と同じ）、請求者（通常は仮想店舗 24 と同じ）、請求額（通常は決済金額と同じ）が表示されている。

利用者 12 が請求内容を確認し、同意できれば「支払」を選択し、同意できな

ければ「拒否」を選択する。携帯電話機 1 3 の入力装置 1 3 6 はこのような利用者 1 2 の操作に応じて選択情報をデータ処理部 1 3 1 に入力する。データ処理部 1 3 1 は入力された選択情報に基づいて決済が承認されたか否かを判別する（S 4 0 2）。決済が承認されなかった場合、送受信部 1 3 5 は決済取消・拒否の情報を携帯電話機 1 0 のサーバ 3 0 に送信する（S 4 0 3）。この場合、データ処理部 1 3 1 は、図 1 9 に示した画面 D 1 3 を表示装置 1 3 7 上に表示する（S 4 0 4）。

携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が携帯電話機 1 3 から送信された決済取消・拒否の情報を受信し（S 5 0 6）、さらにその情報を仮想店舗 2 4 のサーバ 5 0 に送信する（S 5 0 7）。

仮想店舗 2 4 のサーバ 5 0 においては、データ処理部 5 0 1 が携帯電話会社 1 0 のサーバ 3 0 から送信された決済取消・拒否の情報を受信する（S 6 0 5）。

続いて、データ処理部 5 0 1 は受信した決済取消・拒否の情報をインターネット 6 0 を通じて利用者 1 2 のパーソナルコンピュータ 4 0 に送信し、これにより仮想店舗 2 4 は利用者 1 2 に決済が取消しまたは拒否された旨を利用者 1 2 に通知する（S 6 0 6）。

利用者 1 2 のパーソナルコンピュータ 4 0 においては、データ処理部 4 0 1 が仮想店舗 2 4 のサーバ 5 0 から送信された決済取消・拒否の情報を受信し（S 3 0 4）、決済が取消しまたは拒否された旨を表示装置 4 0 6 上に表示する。

上記ステップ S 4 0 2 で決済が承認された場合、携帯電話機 1 3 のデータ処理部 1 3 1 は、RAM 1 3 2 内に未通知データ（電波圏外の店舗で決済したために携帯電話会社 1 0 に未だ通知できていない決済日時、決済金額などで、その詳細は後述する。）が存在しないか否かを判別する（S 4 0 5）。未通知データがある場合、データ処理部 1 3 1 は未通知の決済金額を合計して累計未通知金額を計算し（S 4 0 6）、続いて RAM 1 3 2 に記憶されている前払残高から累計未通知金額を減算して現時点における真の前払金額を計算する（S 4 0 7）。

上記ステップ S 4 0 5 で未通知データがない場合、または上記ステップ S 4 0 7 の後、データ処理部 1 3 1 は前払残高を検証し、決済金額が前受残高以内か否かを判別する（S 4 0 8）。決済金額が前受残高を超えている場合、データ処理

部 1 3 1 は図 1 9 に示した画面 D 1 4 を表示装置 1 3 7 上に表示して残高不足を利用者 1 2 に通知し (S 4 0 9)、続いて残高不足の情報を電波で携帯電話会社 1 0 のサーバ 3 0 に送信する (S 4 1 0)。

5 これに応じて携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が携帯電話機 1 3 から送信された残高不足の情報を受信し (S 5 0 8)、続いてこの残高不足の情報をインターネット 6 0 を通じて仮想店舗 2 4 のサーバ 5 0 に送信する (S 5 0 9)。

10 仮想店舗 2 4 のサーバ 5 0 においては、データ処理部 5 0 1 が携帯電話会社 1 0 のサーバ 3 0 から送信された残高不足の情報を受信し (S 6 0 7)、続いてこの残高不足の情報をインターネット 6 0 を通じて利用者 1 2 のパーソナルコンピュータ 4 0 に送信する (S 6 0 8)。利用者 1 2 のパーソナルコンピュータ 4 0 はこの残高不足の情報を受信し、その旨を表示装置 4 0 6 上に表示する (S 3 0 5)。

15 一方、携帯電話機 1 3 において、上記ステップ S 4 0 8 で決済金額が前払残高以内の場合、データ処理部 1 3 1 は図 1 9 に示した画面 D 1 を表示し、利用者 1 2 にパスワードの入力を促す。利用者 1 2 がパスワードを入力すると、入力装置 1 3 6 は入力されたパスワードをデータ処理部 1 3 1 に与える (S 4 1 1)。

20 続いて、送受信部 1 3 5 は、決済承認の情報および未通知データを携帯電話会社 1 0 のサーバ 3 0 に電波で送信する (S 4 1 2)。具体的には、携帯電話機 1 3 の電話番号、ROM 1 3 3 に予めハード的に登録されているキーコード、上記ステップ S 4 1 1 で入力されたパスワード、未通知の決済金額を送信する。

携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が携帯電話機 1 3 から送信された決済承認の情報を受信する (S 5 1 0)。

25 続いて、データ処理部 3 0 1 は個人情報データベース 1 1 を検索し、受信した携帯電話番号に基づいて利用者 1 2 の個人情報を特定する。データ処理部 3 0 1 はさらに、受信したキーコードを利用者 1 2 の個人情報として予め登録されているキーコードと比較し、キーコードが一致するか否かを判別する (S 5 1 1)。キーコードが一致した場合、データ処理部 3 0 1 は、受信したパスワードを利用者 1 2 の個人情報として予め登録されているパスワードと比較し、パスワードが

一致するか否かを判別する（S 5 1 2）。

キーコードが一致しない場合、またはパスワードが一致しない場合、データ処理部 3 0 1 は本サービス利用不可の情報を携帯電話機 1 3 に電波で送信し、これにより携帯電話会社 1 0 は利用者 1 2 に本サービスが利用できない旨を通知する（S 5 1 3）。

利用者の携帯電話機 1 3 においては、送受信部 1 3 5 が携帯電話会社 1 0 のサーバ 3 0 から送信された本サービス利用不可の情報を受信する（S 4 1 3）。

続いて、データ処理部 1 3 1 は本サービスが利用できない旨を表示装置 1 3 7 上に表示する（S 4 1 4）。

続いて、データ処理部 1 3 1 は本サービス手続が異常に終了した旨を表示装置 1 3 7 上に表示する（S 4 1 5）。

一方、携帯電話会社 1 0 の携帯電話機 1 3 において、データ処理部 3 0 1 は決済不可の情報をインターネット 6 0 を通じて仮想店舗 2 4 のサーバ 5 0 に送信する（S 5 1 4）。

仮想店舗 2 4 のサーバ 5 0 においては、データ処理部 5 0 1 が携帯電話会社 1 0 のサーバ 3 0 から送信された決済不可の情報を受信する（S 6 0 9）。

これに応じて、データ処理部 5 0 1 は決済不可の情報をインターネット 6 0 を通じて利用者 1 2 のパーソナルコンピュータ 4 0 に送信し、これにより仮想店舗 2 4 は利用者 1 2 に決済ができない旨を通知する（S 6 1 0）。

利用者 1 2 のパーソナルコンピュータ 4 0 においては、データ処理部 4 0 1 が仮想店舗 2 1 のサーバ 5 0 から送信された決済不可の情報を受信し（S 3 0 6）、決済ができない旨を表示装置 4 0 6 上に表示する。

一方、携帯電話会社 1 0 のサーバ 3 0 においては、上記ステップ S 5 1 2 でパスワードが一致した場合、データ処理部 3 0 1 は利用履歴データベース 2 8 を更新し、利用者 1 2 の仮想口座 1 1 0 の前受残高を更新する（S 5 1 5）。利用履歴データベース 2 8 には具体的には、決済日時、決済金額などを記録する。

続いて、データ処理部 3 0 1 は更新した前受残高を電波で携帯電話機 1 3 に送信する（S 5 1 6）。

携帯電話機 1 3 においては、データ処理部 1 3 1 が携帯電話会社 1 0 のサーバ

30から送信された仮想口座110の前受残高を受信する(S416)。

続いて、データ処理部131は受信した仮想口座の前受残高と同じになるようにRAM132に記憶されている前払残高を更新し、さらにRAM132に記憶されている未通知データをクリアする(S417)。これにより、携帯電話機13内の前払残高と携帯電話会社内の仮想口座110の前受残高とが同期する。

そして、データ処理部131は図19に示した画面D15を表示装置137上に表示し、決済が完了した旨を利用者12に通知する。

携帯電話会社10のサーバ30においては、上記ステップS516の後、決済完了の情報をインターネット60を通じて仮想店舗24のサーバ50に送信し、これにより携帯電話会社10は決済が完了した旨を仮想店舗24に通知する(S517)。そして、携帯電話会社10は既存の方法で仮想店舗24に決済金額を支払う(S518)。

一方、仮想店舗24のサーバ50においては、データ処理部501は携帯電話会社10のサーバ30から送信された決済完了の情報を受信する(S611)。

続いて、データ処理部501は受注明細および決済完了の情報をインターネット60を通じて利用者12のパーソナルコンピュータ40に送信する(S612)。

利用者12のパーソナルコンピュータ40においては、データ処理部401が仮想店舗24のサーバ50から送信された受注明細および決済完了の情報を受信する(S307)。

6-2. 実在店舗で決済する場合

図20は、実在店舗で決済する場合に用いられる携帯電話機13、POS端末37およびサーバ30のハードウェア構成を示すブロック図である。

図20に示すように、POS端末27も同様に、データ処理部271と、RAM272と、ハードディスク273と、入力装置274と、表示装置275と、インターフェイス(I/F)部276とを備える。決済時に携帯電話機13がセットされる読取装置270はインターフェイス276に接続される。商品バーコードを読取るためのスキャナもインターフェイス部276に接続される。現金引出し部278もインターフェイス部276に接続される。

図 2 1 および図 2 2 は、図 6 に示したように実在店舗で決済する場合における携帯電話機 1 3、POS 端末 2 7 およびサーバ 3 0 の動作を示すフローチャートである。

5 まず利用者 1 2 は実在店舗 2 6 で買物する前に、図 2 3 に示した画面 D 1 で携帯電話機 1 3 の入力装置 1 3 6 を操作してパスワードを入力し、これに応じて入力装置 1 3 6 は入力されたパスワードをデータ処理部 1 3 1 に与える (S 7 0 1)。

10 続いて、データ処理部 1 3 1 は入力されたパスワードを、図 2 4 に示すように RAM 1 3 2 に予め登録されているパスワードと比較し、パスワードの検証を行なう (S 7 0 2)。パスワードが一致しない場合、データ処理部 1 3 1 は図 2 3 に示した画面 D 2 を表示装置 1 3 7 上に表示する (S 7 0 3)。

15 一方、パスワードが一致した場合、データ処理部 1 3 1 は図 2 3 に示したメニュー画面 D 3 を表示する。利用者 1 2 が「①お金を払う」を選択すると、データ処理部 1 3 1 は未通知データがあるか否かを判別する (S 7 0 4)。未通知データは、電波圏外の店舗で決済した場合に、その決済金額、決済日時、決済店舗など
20 d が図 2 4 に示すように RAM 1 3 2 に累積的に格納されたものである。未通知データがある場合、データ処理部 1 3 1 は電波圏内か否かを判別し (S 7 0 5)、電波圏内の場合、送受信部 1 3 5 は電波で携帯電話会社 1 0 のサーバ 3 0 に未通知データを図 2 4 に示すように ROM 1 3 3 に予め登録されたキーコードとともに送信する (S 7 0 6)。電波圏外の場合、RAM 1 3 2 に記憶されている未通知の決済金額を合計して累計未通知金額を計算し (S 7 0 7)、続いて RAM 1 3 2 に記憶されている前払残高からその累計未通知金額を減算し、現在の真の前
25 払残高を計算する (S 7 0 8)。携帯電話機 1 3 内の前払残高は、携帯電話会社 1 0 から仮想口座 1 1 0 の前受残高が送信されて来ない限り更新されない。したがって、電波圏外の実在店舗で連続して携帯電話機 1 3 で決済を行なった場合などは、その各決済金額を未通知データとして RAM 1 3 2 に記憶しておく。

一方、携帯電話会社 1 0 のサーバ 3 0 においては、上記ステップ S 7 0 6 で利用者 1 2 の携帯電話機 1 3 から送信された未通知データをデータ処理部 3 0 1 が受信する (S 9 0 1)。

続いて、データ処理部 301 は、携帯電話機 13 から送信されたキーコードを、個人情報データベース 11 に予め登録されているキーコードと比較し、キーコードが一致するか否かを確認する (S902)。キーコードが一致しない場合、データ処理部 301 は本サービス利用不可の情報を携帯電話機 13 に電波で送信し、
5 これにより携帯電話会社 10 は利用者 12 に本サービスが利用できない旨を通知する (S903)。キーコードが一致する場合、データ処理部 301 は受信した未通知データに基づいて利用履歴データベース 28 を更新し、仮想口座 110 の前受残高を更新する (S904)。続いて、データ処理部 301 は更新した最新の前受残高を携帯端末機 13 に送信する (S905)。

10 携帯電話機 13 においては、上記ステップ S903 で携帯電話会社 10 のサーバ 30 から送信された本サービス利用不可の情報を送受信部 135 が受信する (S709)。続いて、データ処理部 131 は本サービスが利用できない旨を表示装置 137 上に表示し (S710)、さらに本サービス手続が異常に終了した旨を表示装置 137 上に表示する (S711)。

15 また、上記ステップ S905 で携帯電話会社 10 のサーバ 30 から送信された前受残高を送受信部 135 が受信する (S712)。続いて、データ処理部 131 は受信した前受残高と同じになるように RAM 132 に記憶されている前払残高を更新し、さらに未通知データをクリアする (S713)。

上記ステップ S704 で未通知データがない場合、または上記ステップ S708 もしくは S713 の後、データ処理部 103 は図 23 に示した画面 D16 のように現在利用可能な残高を表示する (S714)。

続いて、携帯電話機 13 の決済モードがオンになり、データ処理部 131 は図 23 に示した画面 D17 を表示装置 137 上に表示する (S715)。

25 続いて、利用者 12 は携帯電話機 13 を読取装置 270 にセットする (S716)。これにより、データ処理部 131 は図 23 に示した画面 D18 を表示装置 137 上に表示する。このとき、実在店舗の POS 端末 27 においては、データ処理部 271 が読取装置 28 を通じて携帯電話機 13 に決済金額を送信する (S801)。

携帯電話機 13 においては、データ処理部 131 は POS 端末 27 から送信さ

れた決済金額を受信する（S 7 1 7）。

続いて、データ処理部 1 3 1 は受信した決済金額が現在の残高内か否かを判別する（S 7 1 8）。決済金額が残高を超えている場合、データ処理部 1 3 1 は図 2 3 に示した画面 D 1 9 を表示装置 1 3 7 上に表示し、残高不足を利用者 1 2 に通知する（S 7 1 9）。

決済金額が残高内の場合、データ処理部 1 3 1 は携帯電話機 1 3 の電話番号および ROM 1 3 3 に予めハード的に登録されているキーコードを読取装置 2 8 を通じて POS 端末 2 7 に送信する（S 7 2 0）。

POS 端末 2 7 においては、データ処理部 2 7 1 が携帯端末機 1 3 から送信された携帯電話番号およびキーコードを受信する（S 8 0 2）。

続いて、データ処理部 2 7 1 は受信した携帯電話番号およびキーコードならびに決済内容をハードディスク 2 7 3 に記録する（S 8 0 3）。

続いて、データ処理部 2 7 1 は決済完了の情報を読取装置 2 7 0 を通じて携帯電話機 1 3 に送信する（S 8 0 4）。

携帯電話機 1 3 においては、データ処理部 1 3 1 が POS 端末 2 7 から送信された決済完了の情報を受信し、取引完了を確認する（S 7 2 1）。

続いて、データ処理部 1 3 1 はこのときの決済金額などを含む決済内容を未通知データとして RAM 1 3 2 に記憶する（S 7 2 2）。

上記ステップ S 7 1 6 ~ S 7 2 2 の間、データ処理部 1 3 1 は図 2 3 に示した画面 D 1 8 を表示装置 1 3 7 上に表示する。また、携帯電話機 1 3 が途中で読取装置 2 7 0 から取外された場合は異常終了となる。上記ステップ S 7 2 2 で決済内容を RAM 1 3 2 に記憶した後、データ処理部 1 3 1 は図 2 3 に示した画面 D 2 0 を表示装置 1 3 7 上に表示する。そして、上記決済モードはオフになる（S 7 2 3）。

続いて、データ処理部 1 3 1 は電波圏内か否かを判別し（S 7 2 4）、電波圏内の場合、RAM 1 3 2 に蓄積されている未通知データを ROM 1 3 3 にプログラムされているキーコードとともに携帯電話会社 1 0 のサーバ 3 0 に送信する（S 7 2 5）。

携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が携帯電話機

1 3 から送信された未通知データをキーコードとともに受信する (S 9 0 9)。

続いて、データ処理部 3 0 1 は、携帯電話機 1 3 から送信されたキーコードを、個人情報データベース 1 1 に予め登録されているキーコードと比較し、キーコードが一致するか否かを確認する (S 9 1 0)。キーコードが一致しない場合、データ処理部 3 0 1 は本サービス利用不可の情報を携帯電話機 1 3 に電波で送信する (S 9 1 1)。携帯電話機 1 3 は、この情報を受信し (S 7 2 6)、続いて本サービスが利用できない旨を表示装置 1 3 7 上に表示し (S 7 2 7)、そして本サービス手続が異常に終了した旨を表示装置 1 3 7 上に表示する (S 7 2 8)。

上記ステップ S 9 1 0 でキーコードが一致する場合、データ処理部 3 0 1 は受信した未通知データに基づいて利用履歴データベース 2 8 を更新し、仮想口座 1 1 0 の前受残高を更新する (S 9 1 2)。

続いて、データ処理部 3 0 1 は最新の前受残高を携帯電話機 1 3 に送信する (S 9 1 3)。

携帯電話機 1 3 においては、携帯電話会社 1 0 のサーバ 3 0 から送信された前受残高を受信し、この受信した前受残高と同じになるように RAM 1 3 2 に記憶されている前払残高を更新し、さらに未通知データをクリアする (S 7 2 9)。

一方、実在店舗 2 6 の POS 端末 2 7 においては、データ処理部 2 7 1 が上記決済内容を携帯電話会社 1 0 のサーバ 3 0 に送信する (S 8 0 5)。決済内容の送信は取引ごと、つまりリアルタイムで行なうのが望ましいが、営業終了後に一括してバッチ処理で行なってもよい。

携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 は POS 端末 2 7 から送信された決済内容を受信する (S 9 0 6)。

続いて、データ処理部 3 0 1 は決済完了の情報を POS 端末 2 7 に送信する (S 9 0 7)。そして、携帯電話会社 1 0 は決済内容に基づいて実在店舗 2 6 に対して支払処理を行なう (S 9 0 8)。

POS 端末 2 7 においては、データ処理部 2 7 1 が携帯電話会社 1 0 のサーバ 3 0 から送信された決済完了の情報を受信する (S 8 0 6)。

上記第 1 の実施の形態では POS 端末 2 7 から決済金額を携帯電話機 1 3 に送信し、携帯電話機 1 3 が決済の可否を判定しているが、携帯電話機 1 3 から仮想

口座の残高をPOS端末27に送信し、POS端末27が決済の可否を判定するようにしてもよい。また、上記第1の実施の形態では携帯電話機13を読取装置270を用いてPOS端末27に電氣的に接続しているが、近距離無線（たとえばブルートゥース(Bluetooth)、無線LAN(Local Area Network)またはIrDA (Infrared Data Association)で接続したり、あるいはバーコードリーダーを用いて光学的に接続してもよい。バーコードリーダーを用いる場合、携帯電話機13からPOS端末27に送信するデータをバーコードで表示装置137に表示し、これをバーコードリーダーで読取るようにすればよい。これらの変更は後述する実施の形態でも適用可能である。

10 7. 本サービスの利点

7-1. クレジットカード番号、キャッシュカード番号、口座番号がインターネット上に流れない。

クレジットによる決済の場合、クレジットカード番号さえあれば決済可能な場合があり、特にインターネット上の決済においては、利用者はクレジットカード番号を入力することに強い不安と抵抗を感じることになり、事実、第三者にクレジットカード番号を知られると決済されてしまう危険性や、店頭においてもカード番号が盗まれる危険性は否定できない。しかしながら、この実施の形態ではインターネット上に流れる決済取引データにクレジットカード番号は含まれておらず、携帯電話番号がその役目を果たすものである。また、携帯電話番号はその利用目的上、広く第三者に知られているが、第三者が他人の携帯電話番号のみを知っていても携帯電話機そのものを持っていないと、実在店舗でもインターネット上の仮想店舗でも決済を完了できないうえ、決済限度額が仮想口座内の残高に限定されるため、安全性は高い。

7-2. 決済の際に信用照会および承認が不要である。

25 利用者が携帯電話会社の仮想口座に資金を預ける（前払）する際に、その支払方法ごとに必要とされる信用照会および承認が行なわれるので、利用者がインターネット上の仮想店舗や実在店頭で決済するときには、決済金額が前払残高以内であるか否かを確認するだけでよい。現在、店頭決済時に必要とされている承認番号の取得や本人の署名などの手続が不要となる。

7-3. 店頭決済時に電波を飛ばす必要がない（電波圏外でもよい）。

この実施の形態では、店頭決済時に携帯電話機から必ずしも電波を飛ばす必要はない。したがって、店頭決済を行なう場所が電波圏内であるかどうかを意識する必要がない。よって、電波圏外の多い都市圏の地下街やビル内部、地下鉄構内、
5 地下に設置されている自動販売機や券売機などでも決済することが可能である。携帯電話機が電波圏外にあり、決済金額が携帯電話会社に未通知状態になっていても、携帯電話機の内部メモリに未通知金額が記憶された状態で残り、次回取引発生時には未通知データが必ず送信され、仮想口座の残高が携帯電話機と携帯電話会社との間で同期がとれている状態になってから次の決済処理に入る。

10 7-4. 24時間仮想口座への振替が可能である。

インターネット上の仮想店舗または実店舗での決済時に仮想口座の残高が不足しても、原則としてその場で24時間いつでも仮想口座への資金の振替（前払）をすることが可能であるので、時間を問わず買物ができる。

7-5. 決済の際に与信枠や残高を意識する必要がない。

15 従来、店頭でクレジットカードによる決済をする際に利用限度額を超過するため、クレジットカードによる決済を拒否されることがあり、現金の持ち合せが十分でないときには決済そのものが不可能になることもある。そのため、複数のクレジットカードを使い分けている利用者も多く、かといって利用者が各社クレジットカードごとにその限度額を認識しておくことは現実的には困難である。これ
20 に対し、この実施の形態では利用者がいつでも携帯電話会社内の仮想口座に振替済である金額、つまり前払残高を携帯電話機で確認することが可能であり、その上その残高内であれば常に決済可能であることが保証されている。

7-6. 利用者は、クレジットカードやデビットカードなどの既存決済手段を提供している売り手から提供されている各サービスプログラムを継続して利用可能
25 である。

利用者は、クレジットカードなどの既存決済手段等を利用して携帯電話会社の仮想口座に資金を振込むことで、信販会社などが提供しているサービスを継続して受けることができる。

7-7. クレジットカードを持たない世代でも後払が可能である。

利用者が携帯電話会社内の仮想口座に「通話料に加算」という支払方法で資金の振替を指定する場合、実際に利用者の口座から資金が引落されるのは通話料金の引落し時点である。よって、クレジットカードを持ってない世代でも通話料の引落し時に口座に資金があればよいことになり、クレジットカードのような「擬似
5 翌月一括払」が可能となる。

7-8. 宅配業者が提供する「代金引換え」において利用可能となれば、利用者は予め現金を準備しておく必要がなくなる。

宅配業者は、商品配達時に代金を回収する手段として、携帯電話機による決済を導入することにより、利用者は現金を予め用意する必要がなくなり、宅配業者は配達員に釣銭を持たせる必要が軽減する。店頭でのPOS端末のように携帯電話会社のサーバと決済ごとにデータの送受信を行わず、一括してその日の業務終了後に送信する方法や、その都度無線で送受信する方法等が考えられる。また、
10 こういった移動先での決済を可能とする端末は、小規模店舗等でも流用可能であるうえ、導入が容易である。

7-9. 銀行振込やコンビニエンスストアでの決済と比較して手数料が割安である。

携帯電話会社内の仮想口座への資金の振替を「通話料に加算」という支払方法で行なう場合、利用者は100円～200円程度の月額使用料を支払う。少額決済を同じ月内に繰返し行なう場合等は、銀行振込みやコンビニエンスストアでの決済を利用する場合よりも利用者が負担する手数料が安く済むことになる。
20

7-10. 手数料負担が公平である。

現行のクレジットカードやデビットカードによる決済では、手数料を加盟店が負担しており、その課金方法では少額決済では売上利益を圧迫するため、クレジットカードやデビットカードによる決済を採用していない（加盟していない）店舗がある。一方、この実施の形態では携帯電話会社への資金振込みの際にクレジットカードやデビットカードを利用する場合、極端な少額を振替える例は少ないと想定され、必要に応じて携帯電話会社が資金振替の際の最低金額やその単位を
25 予め設定することにより、携帯電話会社が負担する信販会社等に支払う手数料と収入金額のバランスを取ることが可能である。一方、携帯電話会社から加盟店へ

資金を振替える際には、その振替金額の一定期間中の合計に対して手数料が計算され、課金される。つまり、利用者が決済するごとに、その決済金額に対して手数料が加盟店に課金される現状のクレジットカードやデビットカードによる決済方法とは違い、加盟店は携帯電話会社からその合計金額に対する手数料を課金されることになり、少額決済の多い店舗（企業）であっても導入しやすく、個々の取引決済金額の大小にかかわらず、手数料負担が公平である。つまり、従来の決済システムでは、少額決済が大半を占める店舗、企業（たとえばコンビニエンスストア）でも、利益率を圧迫されることがない。

7-11. 少額取引に適した決済システムである。

10 上記7-10のとおり、手数料負担が公平であることから、少額決済が大半を占める店舗や企業（たとえばコンビニエンスストア）でも、売上利益を圧迫されることはない。また、クレジットカードやデビットカードによる決済方法を導入している店舗や企業でも、負担する手数料の売上金額に対する割合を考慮し、利用可能な最低決済金額（たとえば3000円以上）が設けられていることが多いが、この実施の形態では手数料は一定期間中の合計決済金額に対して課金されるので、限度額設定の必要がない。

7-12. 携帯電話機に金銭的な価値を付加するものではない。

20 現在、進行中の電子マネー計画では携帯電話機に金銭情報そのものをダウンロードして利用することを目的としているが、この実施の形態では仮想口座から振込を実現するための道具として携帯電話機を使用するものであり、電子マネーを仮想口座に振込む資金として利用することも可能である。商取引に携帯電話会社および決済サイトを介在させることにより、その安全性と利便性を高めることが目的であり、携帯電話機に金銭価値を付加するものではない。したがって、電子マネーは紛失したら現金を紛失することと同じであるが、この実施の形態では携帯電話機を落としても金銭的価値が消失するものではない。

7-13. 端末の不正使用に対する安全性

25 紛失や盗難の際も携帯電話会社にサービス停止を依頼することが可能であり、サービス停止になるまでに店頭で悪用されたとしても、利用できる金額は仮想口座内の残高内である。また、本人が携帯電話機を所有しているにもかかわらず、

その携帯電話番号がインターネット上で第三者に悪用された場合でも、他の決済手段では決済が完了するまでまたは利用明細書が届くまで本人が認識することが困難であるのに対し、この実施の形態では決済確認がすべて携帯電話機に送信されることから、決済が完了する前に本人が認識し、未然に防ぐことが可能である。

5 なお、携帯電話機の利用契約者が本サービスの停止を携帯電話会社に申告している場合は、インターネット上での決済の場合は携帯電話機の利用状況の確認の際に、実在店舗での決済の場合は決済モードをオンにする際にサービスの利用不可として通知される。

7-14. 携帯電話機と携帯電話会社のサーバ間での取引の安全性が高い。

10 携帯電話機から携帯電話会社のサーバには携帯電話番号とキーコードとがペアで送信され、携帯電話会社はこの両者を用いて認証を行なっている。携帯電話番号は利用者に固有で、キーコードは携帯電話機に固有であるから、利用者12の携帯電話番号を知っている第三者であっても、利用者12自身の携帯電話機13以外の携帯電話機を使って上述した取引を行なうことはできない。

15 7-15. 短時間で決済が完了する。

上記7-2のとおり、与信照会は前払い時に行ない、決済時には行なう必要がないので、決済にかかる時間は短い。この時間は、現在実在店舗で行なわれているクレジットカードやデビットカードによる決済にかかる時間よりも短い。

[第2の実施の形態]

20 以上、本発明の実施の形態を説明したが、本発明はその他の形態でも実施可能なものである。たとえば上記実施の形態では携帯電話会社に仮想口座を設けているが、銀行のような金融機関に仮想口座を設けてもよく、要するに携帯電話機と直接または間接的に通信可能なサーバに仮想口座を設ければよい。以下、本発明の第2の実施の形態を上記第1の実施の形態との相違点を中心に説明する。

25 1. 資金移動

図25は、この発明の第2の実施の形態における資金移動を示す概略図である。図1に示した第1の実施の形態と異なり、この第2の実施の形態では図25に示すように、利用者12の仮想口座110が銀行などの金融機関70のサーバコンピュータに設けられる。この仮想口座110には残高の他、実在口座番号、仮想

口座番号、携帯電話会社、および携帯電話番号が記憶される。実在口座番号としては、利用者 1 2 が金融機関 7 0 に実際に開設している口座の番号が登録される。仮想口座番号としては、この仮想口座 1 1 0 を特定するための番号が登録される。携帯電話会社としては、利用者 1 2 が契約している携帯電話会社 1 0 の名称が登録される。携帯電話番号としては、利用者 1 2 の携帯電話機 1 3 の携帯電話番号が登録される。

金融機関 7 0 には仮想口座 1 1 0 の他、利用者 1 2 の実在口座 7 1 0、仮想口座 1 1 0 の入出金履歴データベース 7 1 2、および仮想口座 1 1 0 の決済履歴データベース 7 1 4 が設けられる。利用者 1 2 の実在口座 7 1 0 には、実在口座番号および口座残高が記憶される。入出金履歴データベース 7 1 2 には、仮想口座 1 1 0 の口座番号と、仮想口座 1 1 0 の入出金の日付と、その入出金額とが記憶される。決済履歴データベース 7 1 4 には、仮想口座 1 1 0 の口座番号と、仮想口座 1 1 0 の入出金の日付と、決済金額と、携帯電話機 1 3 にその時点での仮想口座残高を携帯電話機 1 3 に通知したか否かを示す状態とが記憶される。一方、携帯電話会社 1 0 のサーバコンピュータにおける個人情報データベース 1 1 には利用者 1 2 が取引している金融機関 7 0 の名称が記憶される。

図 2 6 は、資金移動に用いられる携帯電話機、携帯電話会社のサーバ、および金融機関のサーバのハードウェア構成を示すブロック図である。上記図 7 に示した第 1 の実施の形態と異なり、この第 2 の実施の形態では図 2 6 に示すように携帯電話会社 1 0 のサーバ 3 0 のデータベース 3 0 2 には前受け履歴や決済履歴は記録されない。また、この個人情報データベース 1 1 には仮想口座情報は記録されない。その代わりに、金融機関 7 0 のサーバ 7 2 にはデータベース 7 0 2 が設けられ、このデータベース 7 0 2 に仮想口座情報 1 1 0、仮想口座入出金履歴 7 1 2、および仮想口座決済履歴 7 1 4 が記録される。サーバ 7 2 のデータ処理部 7 0 1 はサーバ 3 0 のデータ処理部 3 0 1 と通信し、データベース 7 0 2 を用いて決済処理を行なう。

図 2 7 および図 2 8 は、金融機関 7 0 の仮想口座 1 1 0 に資金を振替える場合における携帯電話機 1 3、携帯電話会社のサーバ 3 0、および金融機関のサーバ 7 2 の動作を示すフローチャートである。図 2 9 は、この場合に携帯電話機 1 3

に表示される画面の遷移図である。

図 27 に示すようにこの第 2 の実施の形態では、ステップ S 104 において、利用者 12 は携帯電話機 13 の入力装置 136 を操作して所望の振替金額を入力する。これにより、入力装置 136 はその入力された振替金額をデータ処理部 131 に与える。

続いて、携帯電話機 13 の送受信部 135 は、携帯電話番号、キーコードおよび未通知データとともに、その入力された振替金額を携帯電話会社 10 のサーバ 30 に送信する。

携帯電話会社 10 のサーバ 30 においては、上記第 1 の実施の形態と同様に、受信した携帯電話番号およびキーコードを用いて認証を行なった後 (S 202, S 203)、図 28 に示すように利用者 12 の取引銀行へ振替依頼を送信する (S 240)。具体的には、利用者 12 の個人情報データベース 11 から利用者 12 の取引銀行の名称 (ここでは B 銀行) を読み出し、B 銀行のサーバ 72 に利用者 12 の携帯電話番号および振替金額を送信し、これにより利用者 12 の実在口座 710 から仮想口座 110 にその送信した金額を振替えるよう依頼する。

金融機関 70 のサーバ 72 においては、データ処理部 701 が携帯電話会社 10 から送信された上記振替依頼を受信する (S 1000)。

続いて、データ処理部 701 は利用者 12 の実在口座 710 を参照して振替が可能か否かを判定する (S 1001)。依頼のあった振替金額が実在口座 710 の残高を超えている場合、データ処理部 701 は振替不可の情報を携帯電話会社 10 のサーバ 30 に送信する (S 1002)。

携帯電話会社 10 のサーバ 30 においては、データ処理部 301 が金融機関 70 から送信された振替不可の情報を受信し (S 241)、引続きこれを利用者 12 の携帯電話機 13 に送信する (S 242)。

利用者 12 の携帯電話機 13 においては、送受信部 135 が携帯電話会社 10 から送信された振替不可の情報を受信する (S 140)。

続いて、データ処理部 131 は表示装置 137 上に図 29 に示した画面 D 21 を表示し (S 141)、残高不足のために振替ができない旨を利用者 12 に通知する。

続いて、データ処理部 131 は表示装置 137 上に異常終了を表示する (S142)。

上記ステップ S1001 において依頼のあった振替金額が実在口座 710 の残高以内の場合、データ処理部 701 はその依頼のあった金額を実在口座 710 から仮想口座 110 に振替える (S1004)。

続いて、データ処理部 701 は上記振替金額に基づいて入出金履歴データベース 712 を更新する (S1005)。

続いて、上記ステップ S1000 で受信した情報の中に未通知データがあるか否かをデータ処理部 701 が判別する (S1005)。上記ステップ S704 で未通知データが存在し、上記ステップ S1006 で携帯電話機 13 から携帯電話会社 10 に未通知データを送信し、さらに上記ステップ S240 で携帯電話会社 10 から金融機関 70 に未通知データを送信している場合、データ処理部 701 はその未通知データに基づいて決済履歴データベース 714 を更新する (S1006)。未通知データが存在しない場合、データ処理部 701 は仮想口座 110 の残高を携帯電話会社 10 に送信する (S1007)。

携帯電話会社 10 のサーバ 30 においては、データ処理部 301 が金融機関 70 から送信された仮想口座 110 の残高を受信し (S243)、引続きこれを利用者 12 の携帯電話機 13 に送信する (S207)。

携帯電話機 13 においては、上記第 1 の実施の形態と同様に送受信部 135 が携帯電話会社 10 から送信された仮想口座 110 の残高を受信し (S113)、データ処理部 131 が RAM 132 に記録されている仮想口座の残高を更新し (S114)、最後に表示装置 137 上に振替が完了した旨を表示する (S115)。ここで、未通知データが存在する場合はその未通知データをクリアする (S143)。

25 2. 仮想店舗での決済

図 30 は、この発明の第 2 の実施の形態による仮想店舗での決済を示す概略図である。図 30 に示すように、ここではインターネット上の仮想店舗 24 と金融機関 70 との間に決済機関 80 が設けられる。決済機関 80 は本サービスが利用される度に決済情報 810 を蓄積し、蓄積した多数の決済情報 810 に基づいて

仮想店舗 24 に対して利用代金を一括して支払う。決済情報 810 には、銀行名として金融機関 70 の名称、支払者名として利用者 12 の氏名または名称、振替金額、仮想口座 110 の仮想口座番号、および支払先としてインターネット上の仮想店舗 24 の名称が含まれている。

5 図 31 は、仮想店舗での決済に用いられるパーソナルコンピュータ 40、携帯電話機 13、携帯電話会社 10 のサーバ 30、金融機関 70 のサーバ 72、決済機関 80 のサーバ 82、および仮想店舗 24 のサーバ 50 のハードウェア構成を示すブロック図である。図 31 に示すように、決済機関 80 のサーバ 82 には、
10 データ処理部 801 と、データベース 802 とが設けられる。データベース 802 には決済情報 810 が蓄積される。データ処理部 801 はサーバ 72 のデータ処理部 701 と通信し、データベース 802 に蓄積した決済情報 810 に従って仮想店舗 24 に対して支払処理を行なう。

図 32～図 34 は、仮想店舗 24 で決済を行なう場合におけるパーソナルコンピュータ 40、携帯電話機 13、携帯電話会社 10 のサーバ 30、仮想店舗 24
15 のサーバ 50、および金融機関 70 のサーバ 72 の動作を示すフローチャートである。ここでは説明を簡単にするために、決済機関 80 のサーバ 82 の動作を省略する。

図 17 に示した第 1 の実施の形態と同様に、携帯電話会社 10 のサーバ 30 は仮想店舗 24 からの請求データを携帯電話機 13 に送信する (S505)。

20 携帯電話機 13 においては、送受信部 135 がその請求データを受信する (S401)。

続いて、その電子メールで送られてきた電子請求書を開封する (S420)。

25 続いて、上記第 1 の実施の形態と同様に未通知データを処理した後 (S405～S407)、データ処理部 131 が表示装置 137 上に請求内容および利用可能残高 (たとえば図 35 に示した画面 D22 または D23) を表示する (S421)。

続いて、データ処理部 131 は請求額が利用可能残高以内か否かを検証する (S422)。請求額が利用可能残高以内の場合、図 35 の画面 D22 のように「支払」のボタンが表示される。請求額が利用可能残高を超えている場合、図 3

5の画面D23のように「お財布にお金を入れる」のボタンが表示される。

請求額が利用可能残高を超えている場合、データ処理部131は利用者12の操作に応じて追加資金を振替えるか否かを判別する(S423)。追加資金を振替える場合は上述した資金振替を行ない(S424)、追加資金を振替えない場合はステップS403に移る。

上記ステップS422で請求額が利用可能残高以内の場合、上記第1の実施の形態と同様に利用者12が決済を承認したか否かを判別する(S402)。

また、携帯電話会社10のサーバ30において、パスワードを確認した後(S512)、データ処理部301は金融機関70に対して決済依頼の情報を送信するとともに、未通知データが存在する場合はその未通知データを送信する(S520)。

金融機関70のサーバ72においては、データ処理部701が携帯電話会社10から送信された決済依頼の情報を受信する(S1100)。

続いて、データ処理部701は受信した決済金額を利用者12の仮想口座110から振替える(S1101)。未通知データを受信している場合、その未通知の決済金額も利用者12の仮想口座110から振替える。ここでは、仮想店舗24への決済金額の振替を決済機関80に依頼する。決済機関80は依頼のたびにその決済金額を仮想店舗24に支払うのではなく、たとえば所定の月度単位で複数の決済金額をまとめて仮想店舗24に支払う。このような決済機関80は必ずしも必要なく、金融機関70が決済金額を直接仮想店舗24に支払うようにしてもよい。ただし、決済機関80を設けた方が振替の度に発生する手数料を抑えることができる。

続いて、データ処理部701はその決済金額に基づいて入出金履歴データベース712を更新する。(S1102)。

25 続いて、データ処理部701はその決済金額に基づいて決済履歴データベース714を更新する。(S1103)。

続いて、データ処理部701は仮想口座110の残高を讀出して携帯電話会社10に送信する(S1104)。

携帯電話会社10のサーバ30においては、データ処理部301が金融機関7

0から送信された仮想口座残高を受信し（S 5 2 1）、引続きこれを利用者 1 2の携帯電話機 1 3に送信する（S 5 1 6）。

3. 実在店舗での決済

5 図 3 6 は、この発明の第 2 の実施の形態による実在店舗での決済を示す概略図である。図 3 6 に示すように、実在店舗で決済する場合も決済機関 8 0 が金融機関 7 0 からの振替依頼を一括して実在店舗 2 6 に対して支払を行なう。

図 3 7 は、実在店舗での決済に設けられる携帯電話機 1 3、POS 端末 2 7、携帯電話会社 1 0 のサーバ 3 0、金融機関 7 0 のサーバ 7 2、および決済機関 8 0 のサーバ 8 2 のハードウェア構成を示すブロック図である。

10 図 3 7 に示すように、決済機関 8 0 のサーバ 8 2 におけるデータ処理部 8 0 1 はサーバ 7 2 のデータ処理部 7 0 1 と通信し、決済情報 8 1 0 に従って実在店舗 2 6 に対する支払を行なう。

15 図 3 8 ~ 図 4 0 は、実在店舗で決済する場合における携帯電話機 1 3、POS 端末 2 7、携帯電話会社 1 0 のサーバ 3 0、および金融機関 7 0 のサーバ 7 2 の動作を示すフローチャートである。

上記図 2 1 に示した第 1 の実施の形態と異なり、この第 2 の実施の形態では図 3 8 に示したステップ S 7 0 7 において、携帯電話機 1 3 のデータ処理部 1 3 1 は RAM 1 3 2 に記録されている仮想口座残高からステップ S 7 0 7 で計算した累計未通知金額を減算する。

20 また、携帯電話会社 1 0 のサーバ 3 0 において、ステップ S 9 0 2 でキーコードの一致を確認した場合、データ処理部 3 0 1 は未通知データを金融機関 7 0 のサーバ 7 2 に送信する（S 9 2 0）。

金融機関 7 0 のサーバ 7 2 においては、データ処理部 7 0 1 が携帯電話会社 1 0 から送信された未通知データを受信する（S 1 2 0 0）。

25 続いて、データ処理部 7 0 1 は受信した未通知データに基づいて決済履歴データベース 7 1 4 を更新する（S 1 2 0 1）。

続いて、データ処理部 7 0 1 は仮想口座 1 1 0 の仮想口座残高を携帯電話会社 1 0 のサーバ 3 0 に送信する（S 1 2 0 2）。

携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が金融機関 7

0から送信された仮想口座残高を受信し（S 9 2 1）、引続きこれを利用者1 2の携帯電話機1 3に送信する（S 1 0 5）。

携帯電話機1 3においては、送受信部1 3 5が携帯電話会社1 0から送信された仮想口座残高を受信し（S 7 1 2）、さらにデータ処理部1 3 1はその受信した仮想口座残高に基づいてRAM 1 3 2に記録されている仮想口座残高を更新し
5 かつ未通知データをクリアする（S 7 1 3）。

また、携帯電話会社1 0のサーバ3 0においては、ステップS 9 0 6で実在店舗2 6から送信された決済内容を受信した後、データ処理部3 0 1がその受信した決済内容を金融機関7 0のサーバ7 2に送信する（S 9 2 2）。金融機関7 0
10 のサーバ7 2においては、データ処理部7 0 1が携帯電話会社1 0から送信された決済内容を受信する（S 1 2 0 3）。

続いて、データ処理部7 0 1はその受信した決済内容に基づいて決済履歴データベース7 1 4を更新する（S 1 2 0 4）。

続いて、データ処理部7 0 1は決済完了の情報を携帯電話会社1 0のサーバ3 0
15 0に送信する（S 1 2 0 5）。そして、金融機関7 0は上記仮想店舗の場合と同様に決済機関8 0を通じて実在店舗2 6に対する支払処理を行なう（S 1 2 0 6）。

携帯電話会社1 0のサーバ3 0においては、データ処理部3 0 1が金融機関7 0から送信された決済完了の情報を受信し（S 9 2 3）、引続きこれを実在店舗2 6のPOS端末2 7に送信する（S 9 0 7）。

また、携帯電話会社1 0のサーバ3 0においては、ステップS 9 0 9でキーワードの一致を確認した場合、データ処理部3 0 1はステップS 9 0 9で受信した未通知データを金融機関7 0のサーバ7 2に送信する（S 9 2 4）。

金融機関7 0のサーバ7 2においては、データ処理部7 0 1が携帯電話会社1
25 0から送信された未通知データを受信しする（S 1 2 0 7）。

続いて、データ処理部7 0 1はその受信した未通知データに基づいて決済履歴データベース7 1 4を更新する（S 1 2 0 8）

続いて、データ処理部7 0 1は仮想口座1 1 0の仮想口座残高を讀出して携帯電話会社1 0のサーバ3 0に送信する（S 1 2 0 9）。

携帯電話会社10のサーバ30においては、データ処理部301が金融機関70から送信された仮想口座残高を受信し(S925)、引続きこれを利用者12の携帯電話機13に送信する(S913)。

5 利用者12の携帯電話機13においては、送受信部135が携帯電話会社10から送信された仮想口座残高を受信し(S730)、さらにその受信した仮想口座残高に基づいてRAM132に記録されている仮想口座残高を更新しかつ未通知データをクリアする(S729)。

10 以上のようにこの発明の第2の実施の形態によれば、仮想口座110を金融機関70に設けているため、仮想口座110への資金移動が上記第1の実施の形態に比べて簡単になる。

上記第2の実施の形態では金融機関70に実在口座710とは別に仮想口座110を設けているが、実在口座710をそのまま仮想口座110として取扱うようにしてもよい。この場合、実在口座710から仮想口座110への資金移動が不要となるため、処理手続はさらに簡単になる。

15 上記実施の形態のインターネット上の仮想店舗での決済では利用者はパーソナルコンピュータを用いて注文をしているが、携帯電話機を用いて注文をする場合もある。この場合、携帯電話機がパーソナルコンピュータの代わりの機能を果たす。

[第3の実施の形態]

20 仮想口座を上記第1の実施の形態では携帯電話会社に設け、上記第2の実施の形態では金融機関に設けているが、以下に述べる第3の実施の形態では携帯電話会社や金融機関とは別個の決済機関に仮想口座を設ける。

1. サービスの概要

25 この第3の実施の形態によるサービスの利用を希望する利用者は、仮想口座に前払金を入金するために必要な銀行の口座番号や信販会社のクレジットカード番号などを決済機関に予め登録しておく。利用者は、決済の前に、仮想口座に前払金を入金するように、携帯電話機を用いて携帯電話会社を通じて決済機関に要請する。決済機関は、予め登録されている銀行の口座番号や信販会社のクレジットカード番号などを用い、利用者に対して前払金の請求を行なう。決済機関は、前

払金の請求後、前払金を仮想口座に入金した上で仮想口座の残高を携帯電話会社を介して携帯電話機に送信する。仮想店舗や実店舗は、上記第1および第2の実施の形態のように携帯電話会社や金融機関ではなく、決済機関に対して請求を行なう。

5 1-1. 利用登録

図4-1は、携帯電話機1-3の利用者1-2が本サービスの利用を希望する場合に最初に行なう利用登録の方法を示す概略図である。図4-1に示すように、本サービスの利用を希望する利用者1-2は、加入している携帯電話会社、携帯電話番号、および前払金を引落すための銀行の口座番号や信販会社のクレジットカード番号
10 といった決済情報を所定の引落口座登録用紙2-5に記入して決済機関9-0に郵送する。決済機関9-0は、引落口座登録用紙2-5に基づいて利用者情報9-1-0をデータベースに登録する。

続いて、決済機関9-0は、利用者1-2に付与した会員番号（利用者情報9-1-0中の顧客番号）を携帯電話会社1-0を通じて利用者1-2に通知する。利用者1-2
15 はその通知内容を確認し、問題がなければ携帯電話会社1-0を通じて決済機関9-0に対して本サービスの申込を承認する。これに応じて決済機関9-0は、仮想口座1-1-0を開設するとともに、仮想口座の入出金履歴9-1-2や決済履歴9-1-4を記録するための領域をデータベース内に開設する。

なお、決済機関9-0のデータベースには、本サービスの利用が可能な加盟店
20 （仮想店舗および実店舗を含む）とその加盟店における利用金額を振込むための振込口座などの加盟店情報9-1-6が登録されている。

続いて、決済機関9-0は、本サービスの開始を携帯電話会社1-0を通じて利用者1-2の携帯電話機1-3に通知する。このとき、携帯電話会社1-0は個人情報1-1の利用状況を「未登録」から「利用可」に変更する。利用者1-2の携帯電話機
25 1-3が携帯電話会社1-0から本サービス開始の通知を受けると、携帯電話機1-3の利用状況を「利用不可」から「利用可」に変更する。

上記手続により、利用者1-2は本サービスの利用が可能となる。

1-2. 仮想口座への資金移動

図4-2は、決済機関9-0に設けた仮想口座1-1-0に入金する前払金を金融機関

の口座から引落しする場合の資金移動を示す概略図である。図 4 2 に示すように、利用者 1 2 は携帯電話機 1 3 を用い、携帯電話会社 1 0 を通じて決済機関 9 0 に対して所望の前払金を仮想口座 1 1 0 に入金するよう要請する。ここでは仮想口座 1 1 0 に 5 0 0 0 円を入金する場合を例示している。決済機関 9 0 は仮想口座 1 1 0 への前払の要請を受けると、利用者情報 9 1 0 に基づき、利用者 1 2 の口座 1 6 0 が開設されている銀行や信販会社のような金融機関 1 7 0 に対して前払金の引落しを依頼する。引落し依頼を受けた金融機関 1 7 0 は引落しが可能か否かを確認し、可能な場合は振替データを決済機関 9 0 に送り、前払金を決済機関 9 0 に支払う。引落しが不可能な場合はその旨決済機関 9 0 に通知する。決済機関 9 0 は金融機関 1 7 0 から振替データを受けると、入出金履歴 9 1 2 を更新し、さらに仮想口座 1 1 0 を更新する。続いて、決済機関 9 0 はその更新した仮想口座 1 1 0 の残高を携帯電話会社 1 0 に通知する。携帯電話会社 1 0 では、携帯電話番号や仮想口座残高などの送信データ 1 0 2 が作成される。携帯電話会社 1 0 はこの送信データ 1 0 2 に基づいて利用者 1 2 に仮想口座残高を通知する。この通知に応じて利用者 1 2 の携帯電話機 1 3 は仮想口座残高を更新する。携帯電話会社 1 0 から利用者 1 2 の携帯電話機 1 3 への送信データ 1 0 2 の送信が完了すると、送信データ 1 0 2 はクリアされる。利用者 1 2 が電波圏外にいる場合など、送信データ 1 0 2 の送信が不可能な場合、送信データ 1 0 2 はクリアされずにそのまま保持される。

20 1-3. 仮想店舗での決済

図 4 3 は、携帯電話機 1 3 を用いてインターネット上の仮想店舗 2 4 で決済する方法を示す概略図である。図 4 3 に示すように、利用者 1 2 は携帯電話機 1 3 またはパーソナルコンピュータ 4 0 を用いて仮想店舗 2 4 に対して注文を出す。注文を受けた仮想店舗 2 4 は、利用者 1 2 の顧客番号や請求内容などを記載した電子請求書を決済機関 9 0 および携帯電話会社 1 0 を通じて利用者 1 2 の携帯電話機 1 3 に送信する。利用者 1 2 はその送信された電子請求書を携帯電話機 1 3 で確認し、その請求内容が自らの注文内容と一致する場合は決済の承認を携帯電話会社 1 0 を通じて決済機関 9 0 に通知する。決済機関 9 0 は決済の承認を得ると、その請求内容に応じて入出金履歴 9 1 2 および決済履歴 9 1 4 を更新すると

ともに、仮想口座 110 の残高も更新する。ここでは B 店という仮想店舗 24 で 3000 円の商品を購入した場合を例示している。

続いて、決済機関 90 はその更新した仮想口座残高を携帯電話会社 10 に通知する。携帯電話会社 10 はその仮想口座残高を送信データ 102 とし、さらに利用者 12 の携帯電話機 13 に送信する。これに応じて携帯電話機 13 の仮想口座残高が更新される。携帯電話会社 10 から利用者 12 への仮想口座残高の送信が完了すると、送信データ 102 はクリアされる。

一方、決済機関 90 は仮想口座残高の更新を終えると、決済の完了を仮想店舗 24 を通じて利用者 12 に通知する。また、決済機関 90 は加盟店情報 916 に基づいてその決済金額を加盟店の振込口座に入金する。

1-4. 実店舗での決済

図 44 は、携帯電話機 13 を用いて実店舗 26 で決済する方法を示す概略図である。図 44 に示すように、実店舗 26 に設置されている POS 端末 27 に携帯電話機 13 が装着されると、POS 端末 27 は決済金額を携帯電話機 13 に送信する。決済金額が仮想口座残高以内の場合、携帯電話機 13 は決済内容を未通知データに記録するとともに、携帯電話番号、キーコードおよびパスワードを POS 端末 27 に送信する。これに応じて、POS 端末 27 は決済の完了を携帯電話機 13 に通知する。

その後、POS 端末 27 は、携帯電話番号、キーコードおよびパスワードとともに決済内容を決済機関 90 に通知する。決済機関 90 は、受信した携帯電話番号、キーコードおよびパスワードを携帯電話会社 10 に送信することにより認証を依頼する。認証依頼を受けた携帯電話会社 10 は、個人情報 11 の未通知を「無」から「有」に変更する。受信した携帯電話番号、キーコードおよびパスワードが個人情報 11 として登録されている携帯電話番号、キーコードおよびパスワードと一致しない場合、携帯電話会社 10 は個人情報 11 の利用状況を「認証異常」に変更し、その旨を利用者 12 および決済機関 90 に通知する。この通知に応じて、携帯電話機 13 は利用状況を「認証異常」に変更する。

一方、受信した携帯電話番号、キーコードおよびパスワードが個人情報 11 として登録されている携帯電話番号、キーコードおよびパスワードと一致した場合、

携帯電話会社 10 は認証が正常に完了した旨を決済機関 90 に通知する。この通知に応じて、決済機関 90 は入出金履歴 912 および決済履歴 914 を更新する。決済機関 90 はさらに、仮想口座 110 の残高を更新するとともに、未通知を「無」から「有」に変更する。ここでは、D店という実在店舗 26 で 1000 円の商品を購入した場合を例示している。

続いて、決済機関 90 は決済が完了した旨を実在店舗 26 に通知する。また、決済機関 90 は加盟店情報 916 に基づいて加盟店の振込口座にその決済金額を入金する。

1-5. 未通知データの要求

図 45 は、利用者 12 が実在店舗 26 で決済をしたために携帯電話機 13 内に未通知データが発生して携帯電話機 13 の仮想口座残高が決済機関 90 の仮想口座残高と一致しなくなった場合に決済機関 90 が仮想口座残高の同期をとるために携帯電話機 13 に対して未通知データの送信を要求する方法を示す概略図である。図 45 に示すように、決済機関 90 は携帯電話会社 10 を通じて利用者 12 の携帯電話機 13 に未通知データを要求する。これに応じて、携帯電話機 13 は携帯電話会社 10 を通じて未通知データを決済機関 90 に送信する。決済機関 90 は、受信した未通知データに基づいて決済履歴 914 のうち該当の決済の状態を「未通知」から「通知済」に変更する。

続いて、決済機関 90 は仮想口座 110 の残高を携帯電話会社 10 に送信する。携帯電話会社 10 は受信した仮想口座残高を送信データ 102 とするとともに、個人情報 11 中の未通知を「有」から「無」に変更する。携帯電話会社 10 は仮想口座残高を携帯電話機 13 に送信する。これに応じて、携帯電話機 13 は仮想口座残高を更新するとともに、未通知データをクリアする。携帯電話会社 10 は仮想口座残高の送信を完了すると、送信データ 102 をクリアする。

1-6. 請求代行

図 46 は、仮想店舗 24 に代わって決済機関 90 が利用者 12 による仮想店舗 24 での決済金額を信販会社 20 に請求する方法を示す概略図である。この請求代行は、決済機関 90 に設けた仮想口座 110 を利用するものではなく、利用者情報 910 として登録されている銀行の口座番号や信販会社のクレジットカード

番号を利用してデビット決済やカード決済を行なうものである。

図 4 6 に示すように、利用者 1 2 が携帯電話機 1 3 またはパーソナルコンピュータ 4 0 を用いて仮想店舗 2 4 に対して注文をすると、仮想店舗 2 4 は顧客番号や請求内容などからなる電子請求書を決済機関 9 0 および携帯電話会社 1 0 を通じて利用者 1 2 に発行する。利用者 1 2 は携帯電話機 1 3 に送信された電子請求書を確認し、決済を承認する場合はその旨を携帯電話会社 1 0 を通じて決済機関 9 0 に通知する。その際に、予め登録している決済方法の中から 1 つを選択する。ここでは、信販会社 E 社のクレジットカードによる決済を選択した場合を例示している。

10 決済機関 9 0 は決済の承認を仮想店舗 2 4 に通知するとともに、利用者情報 9 1 0 を用いてクレジットカード番号や決済金額などの決済内容を信販会社 2 0 に通知する。これに応じて信販会社 2 0 は仮想店舗 2 4 に対して決済金額の支払処理を行ない、決済が完了した旨を仮想店舗 2 4 に通知する。

15 利用者 1 2 が決済方法としてデビットカードによる決済を選択した場合、決済機関 9 0 は利用者情報 9 1 0 を用いて口座番号や決済金額などの決済内容を銀行 1 7 に通知する。銀行 1 7 はその決済金額を利用者 1 2 の口座から引落とし、さらに仮想店舗 2 4 に対してその決済金額の支払処理を行なう。

上記請求代行サービスでは、銀行の口座番号や信販会社のクレジットカード番号といった重要な決済情報は予め決済機関 9 0 に登録されており、携帯電話機 1 3 やパーソナルコンピュータ 4 0 から送信されることはない。認証は携帯電話番号、キーコードおよびパスワードを用いて携帯電話会社 1 0 で行なわれ、認証が得られた場合だけ予め登録されている口座番号やクレジットカード番号が決済機関 9 0 から金融機関 1 7 0 や信販会社 2 0 に通知される。したがって、高い安全性を確保することができる。

25 2. システム構成およびその動作

次に、上記サービスを実現するためのシステム構成およびその動作について説明する。

2-1. 利用登録

図 4 7 は、図 4 1 に示した利用登録のためのハードウェア構成を示すブロック

図である。上記第1および第2の実施の形態と異なり、この第3の実施の形態では、携帯電話会社10のサーバ30には、送信データ102を記憶するためのメモリ303が設けられる。また、決済機関90のサーバ92には、データ処理部921と、データベース922とが設けられる。データベース922には、利用者情報910、仮想口座の入出金履歴912、仮想口座の決済履歴914および加盟店情報916が蓄積される。データ処理部921は、携帯電話会社10に設置されているサーバ30のデータ処理部301と接続され、データベース922に対して所定のデータ処理を行なう。

図48は、利用登録を行なう場合における利用者12の携帯電話機13、携帯電話会社10のサーバ30および決済機関90のサーバ92の動作を示すフローチャートである。

まず、利用者12は携帯電話機13の入力装置136を操作して本サービスの利用申込を携帯電話機13から携帯電話会社10に送信する(S11)。携帯電話会社10のサーバ30においては、データ処理部301が携帯電話機13から送信された利用申込を受信し(S21)、これを決済機関90に送信する(S22)。決済機関90のサーバ92においては、データ処理部921が携帯電話会社10から送信された利用申込を受信する(S1301)。これに応じて、決済会社92は所定の申込用紙を利用者12に発送する(S1302)。利用者12は申込用紙に引落しを希望する銀行の口座番号や信販会社のクレジットカード番号などを記入した後、決済機関90に返送する。決済機関90は利用者12から返送された申込用紙を受取る(S1302)。この申込用紙に記入された事項に基づいて、データ処理部301は利用者情報910をデータベース922に登録する(S1303)。具体的には、利用者12の会員番号、携帯電話番号、携帯電話会社、銀行の口座番号、信販会社のクレジットカード番号などを登録する。続いて、データ処理部921は会員番号を携帯電話会社10に通知する(S1304)。

携帯電話会社10のサーバ30においては、データ処理部301が決済機関90から送信された会員番号を受信し(S23)、これを利用者12に通知する(S24)。利用者12の携帯電話機13においては、送受信部135が携帯電

話会社10から送信された会員番号を受信し(S12)、利用者12がその申込を承認した場合はその旨を携帯電話会社10に通知する(S13)。携帯電話会社10のサーバ30においては、データ処理部301が携帯電話機13から送信された申込承認の通知を受信し(S25)、これを決済機関90に通知する(S26)。

決済機関90のサーバ92においては、データ処理部921が携帯電話会社10から送信された申込承認の通知を受信し(S1305)、仮想口座110を開設し(S1306)、本サービスの開始を携帯電話会社10に通知する(S1307)。携帯電話会社10のサーバ30においては、データ処理部301が決済機関90から送信されたサービス開始の通知を受信し(S27)、個人情報11の利用状況を「未登録」から「利用可」に更新する(S28)。続いて、データ処理部301は本サービスの開始を利用者12に通知する(S29)。利用者12の携帯電話機13においては、送受信部135が携帯電話会社10から送信されたサービス開始の通知を受信し(S14)、利用状況を「利用不可」から「利用可」に更新する(S15)。

2-2. 仮想口座への資金移動

図49は、図42に示した資金移動に用いられる利用者12の携帯電話機13、携帯電話会社10のサーバ30、決済機関90のサーバ92、金融機関170のサーバ172のハードウェア構成を示すブロック図である。図49に示すように、金融機関170に設置されるサーバ172は、データ処理部174と、データベース176とを備える。データ処理部174はデータベース176のデータを処理するとともに、携帯電話会社10に設置されているサーバ30のデータ処理部301に接続される。データベース176には、利用者の住所や氏名などの利用者情報177と、金融機関170に開設されている実在口座に関する実在口座情報178と、実在口座における入出金などの実在口座履歴179とが登録される。

図50～図52は、図42に示したように金融機関170から決済機関90の仮想口座110に資金を移動する場合における携帯電話機13、携帯電話会社10のサーバ30および決済機関90のサーバ92の動作を示すフローチャートである。

ここでは、パスワードの入力（S 1 0 1）前に、携帯電話機 1 3 が利用状況を確認し、利用不可の場合はその旨を表示装置 1 3 7 に表示する（S 1 0 0）。利用可の場合は利用者 1 2 に対してパスワードの入力を促す（S 1 0 1）。また、パスワードの検証（S 1 0 2）後、前払金額の入力（S 1 0 4）前に、図 2 1 と
5 同様に未通知データを確認して利用可能残高を表示する（S 7 1 4）。

続いて、携帯電話機 1 3 の送受信部 1 3 5 はステップ S 1 0 4 で入力された前払金額などを携帯電話会社 1 0 に送信するが（S 1 0 6）、ここではステップ S 1 0 1 で入力されたパスワードも携帯電話会社 1 0 に送信する。

携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が受信した携
10 帯電話番号に基づいて個人情報 1 1 を検索した後（S 2 0 2）、受信したキーコードおよびパスワードを検証する（S 2 0 3）。キーコードまたはパスワードが一致しない場合、個人情報 1 1 の利用状況を「利用可」から「利用不可」に変更し（S 2 5 0）、認証の異常を利用者 1 2 に通知する（S 2 5 1）。

利用者 1 2 の携帯電話機 1 3 においては、送受信部 1 3 5 が携帯電話会社 1 0
15 から認証異常の通知を受信し（S 1 5 0）、これに応じてデータ処理部 1 3 1 は携帯電話機 1 3 の利用状況を「利用可」から「認証異常」に変更し（S 1 5 1）、本サービスの利用停止を表示装置 1 3 7 に表示する（S 1 5 2）。

一方、ステップ S 2 0 3 でキーコードおよびパスワードの両方が一致した場合、データ処理部 3 0 1 は個人情報 1 1 の利用状況を確認し（S 2 0 4）、利用状況
20 が「利用可」の場合は未通知データがあるか否かを判定する（S 2 5 3）。未通知データがある場合、データ処理部 3 0 1 はステップ S 2 0 1 で受信した前払金額とともに未通知データを決済機関 9 0 に送信する（S 2 5 4）。一方、未通知データがない場合、データ処理部 3 0 1 は前払金額のみを決済機関 9 0 に送信する（S 2 5 5）。このように携帯電話会社 1 0 から決済機関 9 0 に前払金額を送
25 信する際には、利用者 1 2 の携帯電話番号も送信する。

決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が携帯電話会社 1 0 から送信された携帯電話番号や前払金額などを受信し（S 1 3 0 0）、その受信した情報およびデータベース 9 2 2 に登録されている利用者情報 9 1 0 に基づいて利用者 1 2 が口座を開設している金融機関 1 7 0 に対する請求データを作成

する（S 1 3 0 1）。決済機関90はその請求データに従って金融機関170に前払金額の引落しを依頼する（S 1 3 0 2）。

金融機関170は、決済機関90からの引落し依頼に応じて利用者12の口座160から前払金額を引落す（S 1 4 0 0）。続いて、データ処理部174は引落しが可能か否か、すなわち前払金額が口座残高以内か否かを判定する（S 1 4 0 1）。引落しが不可能な場合、データ処理部174は決済機関90にその旨を通知する（S 1 4 0 2）。決済機関90のサーバ92においては、データ処理部921が金融機関170から引落し不可の通知を受信し（S 1 3 0 3）、これを利用者12の携帯電話番号とともに携帯電話会社10に通知する（S 1 3 0 4）。
10 携帯電話会社10のサーバ30においては、データ処理部301が決済機関90から引落し不可の通知を受信し（S 2 5 6）、これを利用者12の携帯電話機13に通知する（S 2 3 2）。

一方、ステップS 1 4 0 1において引落しが可能な場合、サーバ172のデータ処理部174は振替データを決済機関90に送信し（S 1 4 0 3）、利用者12の口座160から決済機関90の口座に前払金額を振替える支払処理を実行する（S 1 4 0 4）。
15

決済機関90のサーバ92においては、データ処理部921が金融機関170から送信された振替データを受信し（S 1 3 0 5）、続いて前払金額の入金をデータベース922に記録することにより入出金履歴912を更新する（S 1 3 0 6）。未通知データが送信されて来ている場合は、ここで決済金額をデータベース922に記録することにより決済履歴914を更新する（S 1 3 0 7）。続いて、データ処理部921は仮想口座110の残高に前払金額を加算することにより仮想口座残高を更新する（S 1 3 0 8）。未通知データがあった場合はこれを「無」に変更する。続いて、データ処理部921は仮想口座110の残高を携帯電話番号とともに携帯電話会社10に送信する（S 1 3 0 9）。
20
25

携帯電話会社10のサーバ30においては、データ処理部301が決済機関90から送信された仮想口座残高を受信し（S 2 5 7）、その仮想口座残高を送信データ102としてメモリ303に記憶する（S 2 5 8）。続いて、データ処理部301は未通知データを「無」に変更する（S 2 5 9）。続いて、データ処理

部 3 0 1 は、メモリ 3 0 3 に記憶された送信データ 1 0 2 を利用者 1 2 の携帯電話機 1 3 に送信する (S 2 6 0)。続いて、上記送信が正常に終了したか否かを判定し (S 2 6 1)、正常に終了した場合は送信データ 1 0 2 をクリアし (S 2 6 2)、利用者 1 2 が電波圏外にいたり携帯電話機 1 3 の電源を切っていた場合など、送信データを携帯電話機 1 3 に送信できず、送信が正常に終了しなかった場合は再送信処理を行なう (S 2 6 3)。具体的には、所定期間経過後に送信データ 1 0 2 を再び携帯電話機 1 3 に送信する。

2-3. 仮想店舗での決済

図 5 3 は、図 4 3 に示した仮想店舗 2 4 での決済に用いられるパーソナルコンピュータ 4 0、携帯電話機 1 3、携帯電話会社 1 0 のサーバ 3 0、決済機関 9 0 のサーバ 9 2 および仮想店舗 2 4 のサーバ 5 0 のハードウェア構成を示すブロック図である。図 5 3 に示すように、決済機関 9 0 に設置されたサーバ 9 2 のデータ処理部 9 2 1 はインターネット 6 0 に接続される。

図 5 4 ~ 図 5 6 は、図 4 3 に示したように仮想店舗 2 4 で決済する場合におけるパーソナルコンピュータ 4 0、携帯電話機 1 3、携帯電話会社 1 0 のサーバ 3 0、決済機関 9 0 のサーバ 9 2、および仮想店舗 2 4 のサーバ 5 0 の動作を示すフローチャートである。

ここでは、利用者 1 2 のパーソナルコンピュータ 4 0 または携帯電話機 1 3 は注文内容とともに会員番号 (顧客番号) を仮想店舗 2 4 に送信する (S 3 0 1)。仮想店舗 2 4 のサーバはこれらを受信し (S 6 0 1)、電子請求書を作成して会員番号とともに請求内容をインターネット 6 0 を介して決済機関 9 0 に送信する (S 6 0 2)。

決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が仮想店舗 2 4 から送信された電子請求書を受信し (S 1 3 1 0)、その受信した会員番号に基づいてデータベース 9 2 2 を検索して利用者情報 9 1 0 の中から利用者 1 2 の携帯電話番号および携帯電話会社を特定する (S 1 3 1 1)。続いて、データ処理部 9 2 1 は受信した電子請求書を該当の携帯電話会社 1 0 に携帯電話番号とともに送信する (S 1 3 1 2)。

携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が決済機関 9

0から送信された電子請求書を携帯電話番号とともに受信する（S501）。データ処理部301は個人情報11中の利用状況を確認し（S503）、利用状況が「利用不可」の場合はその旨を携帯電話番号とともに決済機関90に通知する（S504）。

5 決済機関90のサーバ92においては、携帯電話会社10から携帯電話番号とともに通知されたサービス利用不可の通知を受信し（S1313）、これをインターネット60を介して仮想店舗24に通知する（S1314）。

また、利用者12は、携帯電話会社10から送信され、携帯電話機13で受信した電子請求書を開封し（S418）、携帯電話機13のデータ処理部131は
10 受信した電子請求書の請求内容および利用可能な仮想口座残高を表示装置137に表示する（S154）。

また、電子請求書の請求金額が利用可能残高を超えている場合、データ処理部131は表示装置137を通じて利用者12に対して仮想口座110への追加振替を行なうか否かを問合せ（S155）。追加振替を行なう場合、データ処理
15 部131は資金振替の処理を実行する（S156）。

また、決済を承認するか否かの判定（S402）は、利用可能残高の検証（S408）後に行なう。携帯電話会社10のサーバ30においては、データ処理部301が受信した決済の取消または拒否を携帯電話番号とともに決済機関90に送信する（S507）。決済機関90のサーバ92においては、データ処理部9
20 21が携帯電話会社10から送信された決済の取消または拒否を受信し（S1315）、これをインターネット60を介して仮想店舗24に送信する（S1316）。決済の取消または拒否は上記実施の形態と同様に仮想店舗24を介して利用者12に返信される（S605, S606, S304）。利用者12のパーソナルコンピュータ40または携帯電話機13においては、データ処理部401または131がその受信した決済の取消または拒否（受注取消）を表示装置406
25 または137に表示する（S308）。

また、利用者12の携帯電話機13においては、パスワードの入力（S411）後に、データ処理部131がその入力されたパスワードの検証を行なう（S157）。パスワードが誤っている場合はデータ処理部131はその旨を表示装

置 1 3 7 に表示し (S 1 5 8)、パスワードが正しい場合は送受信部 1 3 5 は決済の承認を携帯電話会社 1 0 に通知する (S 4 1 2)。

また、携帯電話会社 1 0 のサーバ 3 0 においては、キーコードまたはパスワードが不一致の場合、データ処理部 3 0 1 は個人情報 1 1 の利用状況を「利用可」
5 から「認証異常」に変更し (S 5 2 2)、その旨を利用者 1 2 に通知し (S 5 2 3)、さらに決済機関 9 0 にも携帯電話番号とともに通知する (S 5 2 4)。利用者 1 2 の携帯電話機 1 3 においては、送受信部 1 3 5 が携帯電話会社 1 0 から送信された認証異常の通知を受信し (S 1 5 9)、データ処理部 1 3 1 は利用状況を「利用可」から「認証異常」に変更し、さらに本サービスの利用停止を表示
10 装置 1 3 7 に表示する (S 1 6 1)。一方、決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が携帯電話会社 1 0 から送信された認証異常の通知を受信し (S 1 3 1 7)、認証異常を理由に決済が不可能である旨をインターネット 6 0 を介して仮想店舗 2 4 に通知する (S 1 3 1 8)。仮想店舗 2 4 のサーバ 5 0 においては、モデム 5 0 4 が決済機関 9 0 から送信された決済不可の通知を受
15 信し (S 6 1 3)、これに応じて受注の取消をインターネット 6 0 を介して利用者 1 2 のパーソナルコンピュータ 4 0 または携帯電話機 1 3 に送信する (S 6 1 4)。利用者 1 2 のパーソナルコンピュータ 4 0 または携帯電話機 1 3 においては、モデム 4 0 4 または送受信部 1 3 5 が仮想店舗 2 4 から送信された受注の取消を受信し (S 3 0 9)、データ処理部 4 0 1 または 1 3 1 がその旨を表示装置
20 4 0 6 または 1 3 7 に表示する (S 3 1 0)。

ステップ S 5 1 1、S 5 1 2 においてキーコードおよびパスワードがともに一致した場合、データ処理部 3 0 1 は未通知が「有」か否かを判定し (S 5 2 5)、未通知データがある場合は決済データおよび未通知データを携帯電話番号とともに決済機関 9 0 に送信する (S 5 2 6)。未通知データがない場合はデータ処理
25 部 3 0 1 は決済データを携帯電話番号とともに決済機関 9 0 に送信する (S 5 2 7)。決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が携帯電話会社 1 0 から送信された決済データ (および未通知データがある場合は未通知データ) を受信し (S 1 3 1 9)、その受信した決済データ (および未通知データがある場合は未通知データ) に基づいて入出金履歴 9 1 2 を更新し (S 1 3 2 0)、

決済履歴 914 を更新し (S1321)、さらに仮想口座 110 の残高を更新する (S1322)。ここで、データ処理部 921 は仮想口座 110 の未通知を「無」にする。

5 続いて、データ処理部 921 は更新した仮想口座 110 の残高を携帯電話番号とともに携帯電話会社 10 に送信し (S1323)、決済の完了をインターネット 60 を介して仮想店舗 24 に通知し (S1324)、さらに仮想店舗 24 への支払処理を行なう (S1325)。決済完了の通知は仮想店舗 24 を介して利用者 12 にも通知される (S612, S307)。利用者 12 のパーソナルコンピュータ 40 または携帯電話機 13 においては、データ処理部 401 または 131
10 がその受信した決済の完了を表示装置 406 または 137 に表示する (S311)。

一方、携帯電話会社 10 のサーバ 30 においては、データ処理部 301 が決済機関 90 から送信された仮想口座残高を受信し (S528)、その残高を送信データ 102 としてメモリ 303 に記憶する (S529)。続いて、データ処理部
15 301 は個人情報 11 の未通知を「無」にし (S530)、メモリ 303 に記憶された送信データ (仮想口座残高) 102 を利用者 12 の携帯電話機 13 に送信する (S531)。

続いて、データ処理部 301 は上記データの送信が正常に終了したか否かを判定し (S532)、正常に終了した場合はメモリ 303 に記憶された送信データ
20 102 をクリアし (S533)、正常に終了しなかった場合は再び送信処理を行なう (S534)。

利用者 12 の携帯電話機 13 においては、送受信部 135 が携帯電話会社 10 から送信された送信データ 102 を受信し (S162)、データ処理部 131 がその受信した送信データ 102 に基づいて仮想口座残高を更新する (S163)。
25 続いて、データ処理部 131 は未通知データをクリアし (S164)、仮想口座残高とともに決済の完了を表示装置 137 に表示する (S165)。

2-4. 実在店舗での決済

図 57 は、図 44 に示した実在店舗での決済に用いられる携帯電話機 13、P
OS 端末 27、携帯電話会社 10 のサーバ 30 および決済機関 90 のサーバ 92

のハードウェア構成を示すブロック図である。ここでは図 20 と異なり、決済機関 90 のサーバ 92 が実在店舗 26 の POS 端末 27 および携帯電話会社 10 のサーバ 30 に接続される。

5 図 58～図 60 は、図 57 に示した携帯電話機 13、POS 端末 27、携帯電話会社 10 のサーバ 30 および決済機関 90 のサーバ 92 の動作を示すフローチャートである。

ここでは、携帯電話会社 10 のサーバ 30 において、ステップ S525 の判定の結果、未通知データがある場合、データ処理部 301 はその未通知データを携帯電話番号とともに決済機関 90 に送信する (S535)。決済機関 90 のサーバ 92 においては、未通知データがある場合、データ処理部 921 は入出金履歴 912 を更新する (S1330)。続いて、データ処理部 921 は決済履歴 914 を更新し、該当する決済の状態を「通知済」とする (S1331)。続いて、データ処理部 921 は未通知データがある場合に仮想口座 110 の残高を更新し、未通知を「無」にする (S1332)。

15 また、ここでは図 22 と異なり、利用者 12 の携帯電話機 13 において、残高の検証 (S718) 後に、データ処理部 131 は未通知データに決済内容を記憶し (S722)、その後、携帯電話番号、キーコード、パスワードといった携帯電話機 13 の端末情報を POS 端末 27 に送信する (S720)。ステップ S802～S804、S721 は図 22 と同じである。ステップ S721 で POS 端末 27 から決済完了の通知を受信した後、データ処理部 131 は決済モードをオフにし (S723)、決済の終了を表示装置 137 に表示する (S731)。

20 また、POS 端末 27 のデータ処理部 271 はステップ S802 で受信した携帯電話番号、キーコードおよびパスワードとともに、ステップ S803 で記録した決済内容を決済機関 90 に送信する (S805)。決済機関 90 のサーバ 92 においては、データ処理部 921 が POS 端末 27 から携帯電話番号などとともに送信された決済内容を受信し (S1333)、その受信した携帯電話番号に基づいてデータベース 922 に記憶された利用者情報 910 を検索する (S1334)。この検索結果に従って、データ処理部 921 は該当の携帯電話会社 10 に認証を依頼するためにステップ S1333 で受信した携帯電話番号、キーコード

およびパスワードを携帯電話会社 10 に送信する (S 1 3 3 5)。

携帯電話会社 10 のサーバ 30 においては、図 5 5 と同様にデータ処理部 30
1 が認証を行なう (S 5 1 1, S 5 1 2)。ただしここでは、キーコードまたは
5 パスワードが不一致の場合、データ処理部 30 1 は個人情報 1 の利用状況を「利
用不可」に変更し (S 5 2 2)、本サービスの利用停止を利用者 1 2 に通知する
(S 5 2 3)。利用者 1 2 の携帯電話機 1 3 においては、データ処理部 1 3 1 は
利用状況を「利用不可」に変更する (S 1 6 0)。

一方、キーコードおよびパスワードが一致した場合、データ処理部 30 1 は個人
10 情報 1 1 の未通知を「有」に変更し (S 9 2 5)、認証の成功を決済機関 9 0
に通知し、さらに後述する未通知データの要求処理を行なう (S 9 2 7)。

決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が携帯電話会社 1
0 から送信された認証成功の通知を受信し (S 1 3 3 0)、入出金履歴 9 1 2、
15 決済履歴 9 1 4 および仮想口座 1 1 0 の残高をそれぞれ更新する (S 1 3 2 0 ~
S 1 3 2 2)。ここでは、決済履歴 9 1 4 を更新したときその状態を「未通知」
とする。続いて、データ処理部 9 2 1 は仮想口座 1 1 0 の未通知を「有」に変更
する (S 1 3 3 1)。

また、データ処理部 9 2 1 が携帯電話会社 10 から認証異常の通知を受信した
場合も (S 1 3 1 7)、データ処理部 9 2 1 は実在店舗 2 6 に対する決済金額の
20 支払処理を行なう (S 1 3 3 2)。このような認証異常が起こる原因として利用
者 1 2 の不正が考えられるが、この場合も決済機関 9 0 は実在店舗 2 6 に対して
支払を保証することになる。決済機関 9 0 は不正使用による損害を負担すること
になるが、上記のように認証異常を検出した時点で本サービスの利用を停止して
いるので損害を最小限に抑えることができる。

2-5. 未通知データの要求

25 図 6 1 は、携帯電話会社 10 が利用者 1 2 に対して未通知データを要求する場
合における携帯電話機 1 3、携帯電話会社 10 のサーバ 30 および決済機関 9 0
のサーバ 9 2 の動作を示すフローチャートである。なお、未通知データは図 2 4
に示した第 1 の実施の形態と同様に携帯電話機 1 3 の RAM 1 3 2 に記憶されて
いる。また、未通知データの要求の際には図 4 7 に示したハードウェア構成が用

いられる。

携帯電話会社 10 のサーバ 30 においては、データ処理部 301 が予め定められた時間間隔おきに利用者 12 の携帯電話機 13 に対して未通知データの送信を要求する (S 540)。利用者 12 の携帯電話機 13 においては、送受信部 135 が携帯電話会社 10 から送信された未通知データの送信要求を受信し (S 170)、これに応じてデータ処理部 131 が RAM 132 に記憶されている未通知データを携帯電話番号、キーコードおよびパスワードとともに携帯電話会社 10 に送信する (S 706)。以下、図 58 および図 59 と同様に携帯電話会社 10 のサーバ 30 は認証などを行ない、決済機関 90 のサーバ 92 は決済履歴 914 の更新などを行なう。

2-6. 請求代行

図 62 は、図 46 に示した請求代行に用いられるパーソナルコンピュータ 40、携帯電話機 13、携帯電話会社 10 のサーバ 30、仮想店舗 24 のサーバ 50、決済機関 90 のサーバ 92、金融機関 170 のサーバ 94 のハードウェア構成を示すブロック図である。図 62 に示すように、金融機関のサーバ 94 は、データ処理部 941 と、データベース 942 とを備える。データ処理部 941 は、インターネット 60 と、決済機関 90 に設置されているサーバ 92 のデータ処理部 921 とに接続される。データベース 942 には、利用者情報 943、加盟店情報 944 および利用者履歴 945 が蓄積される。利用者情報 943 は、利用者の住所、氏名、電話番号などの他、銀行の場合は口座番号、信販会社の場合はクレジットカード番号および引落銀行口座などである。加盟店情報 944 は、デビットカードやクレジットカードによる決済を受付ける加盟店の住所、名称などである。利用者履歴 945 は、デビットカードやクレジットカードによる決済金額、決済日、利用加盟店の名称などである。

図 63 および図 64 は、図 62 に示したパーソナルコンピュータ 40、携帯電話機 13、携帯電話会社 10 のサーバ 30、決済機関 90 のサーバ 92、金融機関のサーバ 94 および仮想店舗 24 のサーバ 50 の動作を示すフローチャートである。

図 63 および図 64 に示した請求代行の処理は、図 54～図 56 に示した仮想

店舗での決済の処理に類似している。ただし、請求代行の際には利用者12の携帯電話機13において、ステップS418で電子請求書を開封した後直ちに、決済の承認を行なう（S402）。また、ステップS157でパスワードが一致した場合に、デビットカードによる決済かクレジットカードによる決済かという決済方法の選択を利用者12に対して促す（S171）。続いて、携帯電話機13の送受信部135は、決済の承認を携帯電話会社10に通知する（S412）。このとき、携帯電話番号、キーコード、パスワード、決済内容の他、決済方法も合わせて携帯電話会社10に送信する。

また、携帯電話会社10のサーバ30においては、ステップS511、S512でキーコードおよびパスワードが一致した場合に、データ処理部301はステップS510で受信した決済の承認を携帯電話番号とともに決済機関90に送信する。決済機関90のサーバ92においては、データ処理部921がこの決済の承認をインターネット60を介して仮想店舗24に通知し（S1335）、仮想店舗24のサーバ50においてはモデム504がこの通知を受信する（S615）。

続いて、データ処理部921は金融機関に決済内容を通知する（S1336）。金融機関のサーバ94においては、データ処理部941が決済機関90から送信された決済内容を受信し（S1500）、所定の決済処理を行なう（S1501）。続いて、データ処理部941は決済の可否を仮想店舗24に通知する（S1502）。仮想店舗24のサーバ50においては、モデム504が金融機関から送信された決済可否の通知を受信し（S616）、決済が可能か否かを判定し（S617）、決済が不可能な場合は受注の取消を利用者12のパーソナルコンピュータ40または携帯電話機13に送信する（S618）。利用者12のパーソナルコンピュータ40または携帯電話機13においては、モデム404または送受信部135が仮想店舗24から送信された受注取消を受信し（S315）、その旨を表示装置406または137に表示する（S316）。

上記第3の実施の形態は仮想口座110を決済機関90に設けている点で上記第1および第2の実施の形態と大きく相違するが、その他の点でも相違している。これらの相違点は上記第1および第2の実施の形態でも採用することは可能であ

る。

[第4の実施の形態]

上記第3の実施の形態では携帯電話会社10に設けた個人情報11に基づいて利用者12の認証を行なっているが、以下に述べる第4の実施の形態では決済機
5 関90に設けた利用者情報910に基づいて利用者12の認証を行なう。この第
4の実施の形態のためのハードウェア構成は、図47、図49、図53、図57
および図62に示したものと同一であるから、その説明は繰返さない。以下、第
4の実施の形態を上記第3の実施の形態との相違点を中心に説明する。

1. 前払い方法

10 まず、仮想口座に入金する前払い方法について説明する。図65は、この発明
の第4の実施の形態に従う前払い方法を示す概略図である。ここでは、携帯電話
機13のRAM132内に、後述するワンタイムID、小口口座残高および小口
決済履歴を記憶するための領域が確保されている。また、決済機関90の利用者
15 情報910には、利用者12を認証するためのキーコードおよびパスワードが含
まれている。利用者情報910にはまた、携帯電話機13のメールアドレス、利
用状況および会員区分が含まれている。会員区分には個人利用者の「一般」と
「加盟店」とがある。仮想口座110には、小口口座残高およびワンタイムID
が含まれている。図66および図67は、図65に示した場合における、携帯電
20 話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャ
ートである。

まず、利用者12は携帯電話機13を用い、メニュー画面で「前払い」を選択
する(S98)。具体的には、図47、図49、図53、図57および図62に
示した携帯電話機13において、利用者12の操作に応じて入力装置136が
「前払い」の選択信号をデータ処理部131に与える。以降、ステップS99～
25 S103は図50に示したものと同一であるから、その説明は繰返さない。

パスワードの検証(S102)後、利用者12は携帯電話機13を用い、予め
付与されている顧客番号を入力する(S175)。具体的には、利用者12の操
作に応じて入力装置136が入力された顧客番号をデータ処理部131に与える。
ここでは利用者12が顧客番号を入力しているが、最初に入力された顧客番号を

RAM 132 に記憶しておき、2 回目以降はこの記憶された顧客番号を送信するようにしてもよい。また、上記実施の形態のように携帯電話機 13 の電話番号を顧客番号として用いてもよい。

5 続いて、携帯電話機 13 の送受信部 135 がステップ S 175 で入力された顧客番号、ROM 133 に予め登録されているキーコード、およびステップ S 101 で入力されたパスワードを携帯電話会社 10 に送信する (S 176)。

携帯電話会社 10 のサーバ 30 においては、データ処理部 301 が携帯電話機 13 から送信された顧客番号、キーコードおよびパスワードを受信し、これらをそのままインターネット 60 を介して決済機関 90 に送信する。すなわち、携帯電話会社 10 は携帯電話機 13 から送信された顧客番号、キーコードおよびパスワードを決済機関 90 に転送する (S 265)。

15 決済機関 90 のサーバ 92 においては、携帯電話機 13 から携帯電話会社 10 を介して送信された顧客番号、キーコードおよびパスワードをデータ処理部 921 が受信する (S 200)。以降、決済機関 90 のサーバ 92 は、図 50 および図 51 に示したステップ S 203 ~ S 205, S 250, S 251 と同じ処理を携帯電話会社 10 のサーバ 30 に代わって実行する。但しここでは、決済機関 90 のサーバ 92 は認証異常通知を携帯電話会社 10 に送信し、携帯電話会社 10 のサーバ 30 はこれを携帯電話機 13 に転送する (S 266)。また、決済機関 90 のサーバ 92 は利用不可通知を携帯電話会社 10 に送信し、携帯電話会社 10 のサーバ 30 はこれを携帯電話機 13 に転送する (S 267)。携帯電話機 13 のステップ S 150 ~ S 152, S 110, S 111 は図 51 に示したものと
20 同じであるから、その説明は繰返さない。

利用状況の確認 (S 204) の結果、利用状況が「利用可」の場合、決済機関 90 は利用者 12 に対して前払金額の入力を要求する。具体的には、決済機関 90 のサーバ 92 において、データ処理部 921 が前払金額の要求を携帯電話機 13 に送信する (S 1340)。携帯電話会社 10 のサーバ 30 においては、データ処理部 301 が決済機関 90 からインターネット 60 を介して送信された前払金額の要求を利用者 12 の携帯電話機 13 に転送する (S 268)。

利用者 12 の携帯電話機 13 においては、送受信部 135 が決済機関 90 から

携帯電話会社 10 を介して送信された前払金額の要求を受信する (S 1 7 7)。

利用者 1 2 はこの要求に応じて携帯電話機 1 3 の入力装置 1 3 6 を操作し、所望の前払金額を入力するとともに前払金額の支払方法を選択する (S 1 7 8)。
この支払方法としては、上記と同様に銀行口座からの引落とし、デビット決済、クレジット決済の他、振込み、電子マネーによる決済などがある。携帯電話機 1 3 の送受信部 1 3 5 は、この入力された前払金額および選択された支払方法を決済機関 9 0 に送信する。携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が携帯電話機 1 3 から送信された前払金額および支払方法を決済機関 9 0 に転送する (S 2 6 9)。

10 決済機関 9 0 のサーバ 9 2 においては、携帯電話機 1 3 から携帯電話会社 1 0 を介して送信された前払金額および支払方法をデータ処理部 9 2 1 が受信する (S 1 3 4 1)。

続いて、データ処理部 9 2 1 は選択された支払方法で所望の前払金額の決済処理を実行する (S 1 3 4 2)。

15 続いて、データ処理部 9 2 1 は決済が可能か否かを判定する (S 1 3 4 3)。決済が不可能な場合、決済機関 9 0 は利用者 1 2 に前払不可を通知する。具体的には、決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が前払不可の通知を携帯電話機 1 3 に送信する (S 1 3 4 4)。携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が決済機関 9 0 からインターネット 6 0 を介して送信された前払不可の通知を携帯電話機 1 3 に転送する (S 2 7 0)。

20 利用者 1 2 の携帯電話機 1 3 においては、送受信部 1 3 5 が決済機関 9 0 から携帯電話会社 1 0 を介して送信された前払不可の通知を受信し (S 1 7 9)、前払不可を表示装置 1 3 7 に表示する (S 1 8 0)。

一方、ステップ S 1 3 4 3 で決済が可能な場合、決済機関 9 0 は利用者 1 2 に
25 仮想口座の新しい残高とともに前払完了を通知する。具体的には、データ処理部 9 2 1 が仮想口座の残高とともに前払完了の通知を携帯電話機 1 3 に送信する (S 1 3 4 5)。携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が決済機関 9 0 からインターネット 6 0 を介して送信された仮想口座の残高および前払完了の通知を利用者 1 2 の携帯電話機 1 3 に転送する (S 2 7 1)。

利用者 1 2 の携帯電話機 1 3 においては、送受信部 1 3 5 が決済機関 9 0 から携帯電話会社 1 0 を介して送信された仮想口座の残高および前払完了の通知を受信し (S 1 8 1)、データ処理部 1 3 1 が仮想口座の残高とともに前払完了を表示装置 1 3 7 に表示する (S 1 8 2)。

- 5 前払完了の通知 (S 1 3 4 5) 後、データ処理部 9 2 1 は前払金額に基づいて入出金履歴 9 1 2 を更新し (S 1 3 0 6)、さらに仮想口座 1 1 0 の残高を更新する (S 1 3 0 8)。

上述したステップ S 2 6 5 ~ S 2 7 1 に係る通信は同一セッション内で行なわれる。したがって、入出金履歴や仮想口座残高を更新する前に通信が遮断された場合は入出金履歴や仮想口座残高は更新されない。

2. 仮想店舗での決済

次に、仮想店舗での決済について説明する。以下に仮想口座から仮想店舗に請求金額を送金する 2 つの方法を挙げる。

2-1. 第 1 の送金方法

- 15 図 6 8 は、この発明の第 4 の実施の形態に従う第 1 の送金方法を示す概念図である。ここでは、決済機関 9 0 のサーバ 9 2 に設けられたデータベース 9 2 2 に、加盟店請求履歴 9 1 8 および加盟店入金履歴 9 2 0 が記録される。図 6 9 および図 7 0 は、図 6 8 に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

上記第 3 の実施の形態と同様に、利用者 1 2 のパーソナルコンピュータ 4 0 または携帯電話機 1 3 は注文内容とともに顧客番号を仮想店舗 2 4 に送信する (S 3 0 1)。仮想店舗 2 4 のサーバ 5 0 はこれらを受信し (S 6 0 1)、顧客番号とともに請求内容を決済機関 9 0 に送信する (S 6 0 2)。

- 25 決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が仮想店舗 2 4 から送信された請求内容を受信する (S 1 3 1 0)。

続いて、決済機関 9 0 のサーバ 9 2 は、図 5 4 に示したステップ S 5 0 2, S 5 0 3, S 5 0 5 と同じ処理を携帯電話会社 1 0 のサーバ 3 0 に代わって実行する。但しここでは、携帯電話番号の代わりに顧客番号に基づいて決済機関 9 0 の

サーバ 9 2 がデータベース 9 2 2 中の利用者情報 9 1 0 を検索する (S 5 0 2)。

利用状況の確認 (S 5 0 3) の結果、利用状況が「利用可」の場合、決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が顧客番号に基づいてデータベース 9 2 2 を検索し、利用者情報 9 1 0 の中から携帯電話機 1 3 の電子メールアドレスを読み出し、その電子メールアドレスに従って電子請求書を電子メールで
5 携帯電話機 1 3 に送信する (S 5 0 5)。この電子請求書には、請求番号、請求金額、送金先 (加盟店番号) などが記録されている。

続いて、データ処理部 9 2 1 は加盟店請求履歴 9 1 8 を更新し、仮想店舗 2 4 から送信された電子請求書に基づいて、請求番号、請求日、請求金額などを記録
10 する (S 1 3 4 0)。

携帯電話会社 1 0 のサーバ 3 0 においては、データ処理部 3 0 1 が決済機関 9 0 からインターネット 6 0 を介して送信された電子メールを利用者 1 2 の携帯電話機 1 3 に転送する (S 2 7 2)。

携帯電話機 1 3 においては、送受信部 1 3 5 が決済機関 9 0 から携帯電話会社 1 0 を介して送信された電子メールを受信し (S 4 0 1)、データ処理部 1 3 1 が利用者 1 2 の操作に応じて電子メールを開封し、電子請求書を表示装置 1 3 7 に表示する (S 4 1 8)。
15

続いて、利用者 1 2 が電子請求書を確認し、そこに記録されている請求金額を仮想店舗 2 4 に送金する場合は「送金」を選択する。このとき、利用者 1 2 は入力装置 1 3 6 を操作して顧客番号およびパスワードも入力する。これにより携帯電話機 1 3 は電子メールに埋込まれている送金 URL (Uniform Resource Locator) に従って決済機関 9 0 のサーバ 9 2 に接続され、送受信部 1 3 5 がキーコード、顧客番号およびパスワードとともに送金選択信号を決済機関 9 0 に送信する (S 4 3 0)。携帯電話会社 1 0 のサーバ 3 0 は、携帯電話機 1 3 から送信
20 された送金選択信号をインターネット 6 0 を介して決済機関 9 0 に転送する (S 2 7 3)。

決済機関 9 0 のサーバ 9 2 においては、データ処理部 9 2 1 が携帯電話機 1 3 から携帯電話会社 1 0 を介して送信されたキーコード、顧客番号、パスワードおよび送金選択信号を受信し (S 1 3 4 1)、その受信した顧客番号に基づいてデ

データベース 922 中の利用者情報 910 を検索する (S1342)。以降、決済機関 90 のサーバ 92 は図 55 に示したステップ S511, S512, S522 ~ S524 と同じ処理を携帯電話会社 10 のサーバ 30 に代わって実行する。

データ処理部 921 がキーコードおよびパスワードを検証し (S511, S512)、両方共一致した場合は仮想口座 110 の新しい残高とともに送金完了の通知を携帯電話会社 10 を介して利用者 12 の携帯電話機 13 に送信する (S1343)。携帯電話会社 10 のサーバ 30 は、決済機関 90 からインターネット 60 を介して送信された送金完了の通知を利用者 12 の携帯電話機 13 に転送する (S275)。携帯電話機 13 においては、送受信部 135 が決済機関 90 から携帯電話会社 10 を介して送信された送金完了通知を受信し (S431)、さらにデータ処理部 131 が送金後の仮想口座残高とともに送金完了を表示装置 137 に表示する (S432)。

送金完了の通知 (S1343) 後、決済機関 90 のサーバ 92 は図 56 に示したステップ S1320 ~ S1322 と同じ処理を実行する。

仮想口座残高の更新 (S1322) 後、データ処理部 921 はデータベース 922 中の加盟店請求履歴 918 を更新し、入金日を記録する (S1344)。

続いて、データ処理部 921 はデータベース 922 中の加盟店入金履歴 920 を更新し、請求番号、入金日、入金額、送金顧客番号などを記録する (S1345)。

続いて、データ処理部 921 は入金通知をインターネット 60 を介して仮想店舗 24 に送信する (S1346)。仮想店舗 24 のサーバ 50 においては、モデム 504 が決済機関 90 から送信された入金通知を受信する (S619)。

ここでは、ステップ S272 ~ S275 に係る通信は同一セッション内で行なわれる。

25 2-2. 第 2 の送金方法

図 71 は、この発明の第 4 の実施の形態に従う第 2 の送金方法を示す概念図である。図 72 および図 73 は、図 71 に示した場合における、パーソナルコンピュータ、携帯電話機、携帯電話会社のサーバ、決済機関のサーバ、および仮想店舗のサーバの動作を示すフローチャートである。

注文を受けた仮想店舗 24 は、上記第 1 の送金方法のように支払内容を決済機関 90 を介して利用者 12 に通知するのではなく、ここでは支払内容を利用者 12 に直接通知する。具体的には、仮想店舗 24 のサーバ 50 においては、注文の受信 (S 601) 後、データ処理部 501 は仮想店舗 24 の加盟店番号と請求金額などの請求内容をインターネット 60 を介して利用者 12 の携帯電話機 13 またはパーソナルコンピュータ 40 に送信する (S 620)。利用者 12 の携帯電話機 13 またはパーソナルコンピュータ 40 においては、送受信部 135 またはモデム 404 がこれらを受信する (S 312)。

利用者 12 は通知された請求内容を見て携帯電話機 13 を操作し、メニュー画面から「送金」を選択する (S 97)。図 66 に示したステップ S 99 ~ 103, S 175, S 176, S 265, S 200 と同様に、利用者 12 はパスワードおよび顧客番号を入力し、携帯電話機 13 はこれらをキーコードとともに決済機関 90 に送信し、決済機関 12 はこれらを受信する。

続いて、図 69 に示したステップ S 502, S 503, S 1314, S 603, S 604, S 302, S 303, S 511, S 512, S 522 ~ S 524, S 274, S 159, S 613 と同様に、決済機関 90 は認証を行ない、ステップ S 511, S 512 でキーコードおよびパスワードの両方が一致した場合、具体的な送金内容を入力するよう利用者 12 に要求する。利用者 12 はこの要求に応じて具体的な送金内容を入力して決済機関 90 に送信する。

具体的には、決済機関 90 のサーバ 92 においては、データ処理部 921 が送金内容の要求を利用者 12 の携帯電話機 13 に送信する (S 1347)。携帯電話会社 10 のサーバ 30 においては、データ処理部 301 が決済機関 90 からインターネット 60 を介して送信された送金内容の要求を携帯電話機 13 に転送する (S 276)。

利用者 12 の携帯電話機 13 においては、送受信部 135 が決済機関 90 から携帯電話会社 10 を介して送信された送金内容の要求を受信する (S 433)。

続いて、入力装置 136 は利用者 12 の操作に応じて入力された送金内容をデータ処理部 131 に与え、送受信部 135 はその入力された送金内容を決済機関 90 に送信する (S 434)。送金内容としては、送金先の加盟店番号、送金金

額などがある。携帯電話会社10のサーバ30においては、データ処理部301が携帯電話機13から送信された送金内容を決済機関90に転送する（S277）。決済機関90のサーバ92においては、データ処理部921が携帯電話機13から携帯電話会社10を介して送信された送金内容を受信する（S1348）。以降は、図70に示したステップS1343, S275, S431, S432, S1320~S1322; S1345, S1346, S619と同じであるから、その説明は繰返さない。ただしここでは、図68に示した請求履歴918はないので請求履歴の更新（S1344）は行なわれない。

3. 実在店舗での決済

次に、実在店舗での決済について説明する。ここでは、仮想口座からの振替えが可能な小口座をさらに設け、その小口座の使用を可能にするワンタイムID（識別子）を発行する。

3-1. ワンタイムIDの発行（小口座への振替え）

図74および図75は、この発明の第4の実施の形態に従ってワンタイムIDの発行方法を示す概念図である。図74は小口決済履歴がない場合を示し、図75は小口決済履歴がある場合を示す。ここでは、決済機関90のサーバ92に設けられたデータベース922に、小口座の入出金履歴915が記録される。図76および図77は、図74および図75に示した場合における、携帯電話機、携帯電話会社のサーバ、および決済機関のサーバの動作を示すフローチャートである。

実在店舗で決済をするために仮想口座から小口座に所望の金額を振替えようとする場合、利用者12は携帯電話機13を操作し、メニュー画面で「ワンタイムID」を選択する（S96）。具体的には、携帯電話機13において、入力装置136が利用者12の操作に応じて「ワンタイムID」の選択信号をデータ処理部131に与える。以降、ステップS99~S103, S175は図66に示したものと同じであるから、その説明は繰返さない。

顧客番号の入力（S175）後、携帯電話機13においては、送受信部135が顧客番号、キーコード、パスワードおよび小口座情報を決済機関90に送信する（S185）。小口座情報には、RAM132に記録されている小口座

残高および小口決済履歴が含まれる。但し、初めてワнтаイムIDを要求する場合、小口決済履歴はまだ存在していない。以降、ステップS 265～S 267, S 200, S 202～S 205, S 250, S 251, S 150～S 152, S 110, S 111は図66に示したものと同じであるから、その説明は繰返さない。

利用者12の認証(S 203)の結果、キーコードおよびパスワードが共に一致し、かつ利用状況の確認(S 204)の結果、利用状況が「利用可」の場合、決済機関90は利用者12に対して仮想口座から小口座への振替金額を要求する。具体的には、決済機関90のサーバ92において、データ処理部921が小口座への希望振替金額の要求を利用者12の携帯電話機13に送信する(S 1350)。このとき、振替可能な限度額(通常は仮想口座の残高)も併せて送信する。携帯電話会社10のサーバ30においては、データ処理部301が決済機関90からインターネット60を介して送信された振替金額の要求を携帯電話機13に転送する(S 278)。

利用者12の携帯電話機13においては、送受信部135が決済機関90から携帯電話会社10を介して送信された振替金額の要求を受信する(S 186)。

この要求に応じ、利用者12は携帯電話機13の入力装置136を操作して所望の振替金額を指定する(S 187)。入力装置136は利用者12により指定された振替金額をデータ処理部131に与える。

データ処理部131はステップS 187で指定された決済金額をステップS 186で受信した限度額と比較し、指定された決済金額が限度額以内か否かを判定する(S 188)。指定された振替金額が限度額を超えている場合、データ処理部131は振替不可を表示装置137に表示する(S 189)。一方、指定された振替金額が限度額以内の場合、送受信部135はその指定された振替金額を決済機関90に送信する(S 190)。携帯電話会社10のサーバ30においては、データ処理部301が利用者12の携帯電話機13から送信された振替金額をインターネット60を介して決済機関90に転送する(S 279)。

決済機関90のサーバ92においては、データ処理部921が利用者12の携帯電話機13から携帯電話会社10を介して送信された振替金額を受信し(S 1

351)、さらにランダムにワンタイムIDを生成する(S1352)。

続いて、データ処理部921はステップS1351で受信した振替金額に基づいて、仮想口座の入出金履歴912を更新し(S1320)、仮想口座の決済履歴914を更新し(S1321)、仮想口座110の残高を更新し(S1322)、さらに小口口座の入出金履歴915を更新する(S1345)。

たとえば図74に示すように利用者12が振替金額を1000円に指定した場合、仮想口座の入出金履歴912には1000円が小口口座に出金された旨が記録される。また、仮想口座110の残高は1000円減額され、小口口座の残高は1000円増額される。さらに、小口口座の入出力履歴915には1000円が入金された旨が記録される。この場合、小口決済履歴は携帯電話機13から送信されて来ないので、仮想口座の決済履歴914は更新されない。

次に、図75に示すように携帯電話機13の小口決済履歴に300円を使用した旨が記録されている(つまり携帯電話機13の小口口座残高が700円になっている)場合において利用者12が振替金額を1500円に指定したときは、この振替金額(1500円)と現在の小口口座残高(700円)との差額(800円)が計算され、仮想口座の入出力履歴912には800円が出金された旨が記録される。また、携帯電話機13の小口決済履歴に基づいて仮想口座の決済履歴914には300円が決済に使用された旨が記録される。また、上記差額に基づいて仮想口座110の残高は800円減額され、200円になる。小口口座から300円が決済に使用されたが、新たに800円が小口口座に振替えられるので、小口口座の残高は上記振替金額に等しい1500円になる。また、小口口座の入出金履歴915には携帯電話機13の小口決済履歴に基づいて300円が出金された旨が記録され、さらに上記差額に基づいて800円が入金された旨が記録される。

最後に、データ処理部921はステップS1352で生成したワンタイムIDや小口口座残高などの振替内容を利用者12の携帯電話機13に送信する(S1353)。携帯電話会社10のサーバ30においては、データ処理部301が決済機関90からインターネット60を介して送信された振替内容を携帯電話機13に転送する(S280)。

利用者12の携帯電話機13においては、送受信部135が決済機関90から携帯電話会社10を介して送信された振替内容を受信する(S119)。

続いて、データ処理部131はRAM132に記録されている小口決済履歴をクリアする(S192)。続いて、データ処理部131は、RAM132に記録
5 されている小口口座残高を書替え(S193)、さらにRAM132に記録されているワнтаイムIDを書替える(S194)。

たとえば図74に示した場合、決済機関90で生成された「98765」のワ
ンタイムIDが携帯電話機13のRAM132に記録される。また、利用者12
が指定した振替金額に従って小口口座残高が「0円」から「1000円」に更新
10 される。また、図75に示した場合、決済機関90で生成された「34567」
の新しいワнтаイムIDが携帯電話機13のRAM132に記録される。また、
決済機関90で計算された「1500円」の新しい小口口座残高が携帯電話機1
3のRAM132に記録される。

最後に、データ処理部131は小口口座残高とともに小口口座への入金完了を
15 表示装置137に表示する(S195)。

3-2. ワンタイムIDの使用(小口口座からの支払い)

図78は、この発明の第4の実施の形態に従い、ワンタイムIDを使用して実
在店舗で決済する方法を示す概念図である。図79は、図78に示した場合にお
ける、携帯電話機、实在店舗のPOS端末、および決済機関のサーバの動作を示
すフローチャートである。
20

小口口座に所望の金額を振替えてワンタイムIDを獲得した後、实在店舗26
で決済を行なう場合、利用者12は携帯電話機13を操作し、メニュー画面で
「支払い」を選択する(S95)。具体的には、携帯電話機13において、入力
装置136が利用者12の操作に応じて「支払い」の選択信号をデータ処理部1
25 31に与える。以降、ステップS99~S103は図66に示したものと同じで
あるから、その説明は繰返さない。

パスワードの検証(S102)後、データ処理部131はRAM132に記録
されているワンタイムIDが有効か否かを判定する(S735)。ワンタイムID
には有効日が付与されており、小口口座の残高はその有効日までしか实在店舗

での決済に使用することができない。ワンタイムIDは実在店舗での決済に1回使用すれば無効になるようにしてもよい。

ワンタイムIDが無効な場合、データ処理部131はその旨を表示装置137に表示する(S736)。一方、ワンタイムIDが有効な場合、データ処理部131は小口口座からの支払いが可能である旨を表示装置137に表示する(S737)。以降、ステップS716~S719, S801は図5-9に示したものと
5 同じであるから、その説明は繰返さない。

残高検証(S718)の結果、POS端末27から送信された決済金額が小口口座の残高以内の場合、携帯電話機13のインターフェイス部139はPOS端末27にRAM132に記録されているワンタイムIDを送信する(S738)。
10

続いて、データ処理部131はRAM132に記録されている小口決済履歴を更新する(S739)。具体的には、データ処理部131は、POS端末27から送信された決済金額、決済日、実在店舗26の加盟店番号などを記憶する。

続いて、データ処理部131はRAM132に記録されている小口口座の残高を更新する(S740)。具体的には、データ処理部131は、小口口座の残高から決済金額を減算して新しい残高を記録する。この時点で、携帯電話機13の小口口座の残高は決済機関90の小口口座の残高とずれる。
15

最後に、データ処理部131は小口口座の新しい残高とともに決済の完了を表示装置137に表示する(S741)。

実在店舗26のPOS端末27においては、インターフェイス部276が携帯電話機13から送信されたワンタイムIDを受信する(S810)。
20

続いて、データ処理部271はその決済金額に基づいて売上計上処理を実行する(S811)。

続いて、インターフェイス部276は、加盟店番号とともにワンタイムID、決済日、決済金額、顧客番号などの決済内容を決済機関90に送信する(S805)。
25

決済機関90のサーバ92においては、データ処理部921がPOS端末27から送信された決済内容を受信し(S1333)、その受信した決済内容に基づいて加盟店の入金履歴920を更新する(S1355)。

続いて、データ処理部 9 2 1 はその支払を承認した旨の通知を実在店舗 2 6 に送信する (S 1 3 2 4)。実在店舗 2 6 の P O S 端末 2 7 は、決済機関 9 0 から送信された支払承認の通知を受信する (S 8 0 6)。

最後に、データ処理部 9 2 1 はたとえば月末に 1 ヶ月間の総支払金額を計算し、
5 実在店舗 2 6 に対する支払処理を実行する (S 1 3 2 5)。

上述した第 4 の実施の形態では、携帯電話会社 1 0 のサーバ 3 0 が携帯電話機 1 3 から送信されたキーコードをそのまま決済機関 9 0 のサーバ 9 2 に転送しているが、携帯電話機 1 3 から送信されたキーコードをこれと 1 対 1 に対応する別のキーコードに変換して決済機関 9 0 のサーバ 9 2 に送信するようにしてもよい。

10 また、小口口座への振替えの際にワンタイム I D をダウンロードするようにしているが、利用者 1 2 が携帯電話機 1 3 で決済機関 9 0 が提供するサービスサイトにアクセスする度に自動的に新しいワンタイム I D をダウンロードするようにしてもよい。この場合、ワンタイム I D の更新頻度が増すため、セキュリティがさらに高くなる。

15 また、ワンタイム I D を 1 次元または 2 次元バーコードのイメージとし、実在店舗での決済の際には携帯電話機 1 3 に表示されたバーコードを P O S 端末 2 7 のリーダで光学的に読取るようにしてもよい。この場合、携帯電話機 1 3 から情報を読取るための専用機器を P O S 端末 2 7 に取付ける必要はなく、既存のバーコードリーダを用いればよい。また、小口口座の残高をワンタイム I D のバーコードに付加してもよい。
20

この発明の第 4 の実施の形態によれば、決済機関 9 0 が携帯電話機 1 3 から出力されるキーコードを取得し、利用者 1 2 の認証を行なっているため、認証を携帯電話会社 1 0 に依存することはない。そのため、決済会社 9 0 だけで本サービスを提供することができる。

25 また、仮想口座とは別に小口口座を設け、実在店舗で決済する際には予め仮想口座から小口口座に振替えを行なっておき、小口口座から代金を支払うようにしているため、上記第 1 ~ 第 2 の実施の形態のように仮想口座の残高が真の残高からずれることはない。また、決済機関が小口口座からの出金を可能にするためのワンタイム I D を発行し、ワンタイム I D が有効でかつ決済金額が小口口座の残

高以内の場合だけ携帯電話機 1 3 から P O S 端末 2 7 にワンタイム I D が出力され、 P O S 端末 2 7 はこのワンタイム I D に基づいて決済を完了するようにしているため、セキュリティが高くなる。

5 上記各コンピュータには所定のプログラムがインストールされている。この各プログラムは、フローチャートで示した各列に並ぶ一連のステップを対応のコンピュータに実行させるためのものである。各プログラムは C D - R O M のようなコンピュータ読取可能な媒体に記録して配布可能である。

10 今回開示された実施の形態はすべての点で例示であって制限的なものではないと解釈されるものである。本発明の範囲は上述した実施の形態ではなく特許請求の範囲によって定められ、特許請求の範囲と均等の意味およびその範囲内でのすべての変更が含まれることを意図するものである。

産業上の利用可能性

この発明は、携帯電話機を用いた決済サービスに適用可能である。

請求の範囲

1. 売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であつて、前記利用者の金銭を蓄積するための第1の口座を有するコンピュータにおいて、
- 5 前記携帯電話機から送信された所望の金額を受信するステップと、
前記受信した所望の金額を前記利用者の第1の口座に入金してその口座の残高を更新するステップと、
前記更新した第1の口座の残高を前記携帯電話機に送信するステップと、
- 10 決済金額を受信するステップと、
前記受信した決済金額を前記第1の口座の残高から減じるステップと、
前記受信した決済金額を前記売り主に支払うステップとを含む、方法。
2. 前記受信した所望の金額を前記利用者に対して課金するステップをさらに含む、請求項1に記載の方法。
- 15 3. 前記携帯電話機から送信された識別情報を受信するステップと、
前記受信した識別情報に基づいて前記利用者の認証を行なうステップとをさらに含む、請求項1に記載の方法。
4. 前記識別情報は前記利用者に固有の利用者固有情報を含む、請求項3に記載の方法。
- 20 5. 前記利用者固有情報は前記携帯電話機の電話番号を含む、請求項4に記載の方法。
6. 前記利用者固有情報はパスワードをさらに含む、請求項5に記載の方法。
7. 前記利用者固有情報は前記利用者に予め付与された利用者識別子を含む、請求項4に記載の方法。
- 25 8. 前記利用者固有情報はパスワードをさらに含む、請求項7に記載の方法。
9. 前記識別情報は前記携帯電話機に固有の電話機固有情報をさらに含む、請求項4に記載の方法。
10. 前記電話機固有情報は前記携帯電話機の製造番号を含む、請求項9に記載の方法。

- 1 1. 前記電話機固有情報は前記携帯電話機のサブスクライバ識別子を含む、請求項 9 に記載の方法。
- 1 2. 前記サブスクライバ識別子は携帯電話局を介して送信される、請求項 1 1 に記載の方法。
- 5 1 3. 前記コンピュータは第 2 の口座をさらに有し、
前記携帯電話機から送信された振替金額を受信するステップと、
前記受信した振替金額を前記第 1 の口座から前記第 2 の口座に振替えるステップと、
前記第 2 の口座の残高を使用可能にするためのワンタイム識別子を生成して前記携帯電話機に送信するステップとをさらに含む、請求項 1 に記載の方法。
- 10 1 4. 前記コンピュータは携帯電話会社に設けられる、請求項 1 に記載の方法。
1 5. 前記コンピュータは決済機関に設けられる、請求項 1 に記載の方法。
1 6. 前記コンピュータは金融機関に設けられる、請求項 1 に記載の方法。
1 7. 売り主と携帯電話機の利用者たる買い主との間の決済を仲介する方法であって、前記利用者の金銭を蓄積するための口座を有する金融機関のコンピュータにおいて、
携帯電話局のコンピュータから決済金額を受信するステップと、
前記受信した決済金額を前記口座の残高から減じるステップと、
前記受信した決済金額を前記売り主に支払うステップとを含む、方法。
- 15 1 8. 前記携帯電話機から送信された金額を前記携帯電話局のコンピュータを介して受信するステップと、
前記受信した金額を前記利用者の口座に振替えてその口座の残高を更新するステップと、
前記更新した口座の残高を前記携帯電話局のコンピュータを介して前記携帯電話機に送信するステップとをさらに含む、請求項 1 7 に記載の方法。
- 20 1 9. 売り主と携帯電話機の利用者たる買い主との間の決済に用いられ、前記利用者の金銭を蓄積するための第 1 の口座を有するコンピュータにアクセス可能な携帯電話機であって、
前記利用者の操作に応じて前記第 1 の口座に入金されるべき所望の金額を入力

する入力手段と、

前記入力された金額を前記コンピュータに送信し、前記コンピュータから送信された前記第 1 の口座の残高を受信する送受信手段と、

前記受信した第 1 の口座の残高を記憶する手段とを備える、携帯電話機。

- 5 20. 前記送受信手段はさらに前記利用者の認証に必要な識別情報を前記コンピュータに送信する、請求項 19 に記載の携帯電話機。
21. 前記識別情報は前記利用者に固有の利用者固有情報を含む、請求項 20 に記載の携帯電話機。
- 10 22. 前記利用者固有情報を記憶する手段をさらに備える、請求項 21 に記載の携帯電話機。
23. 前記利用者固有情報は前記携帯電話機の電話番号を含む、請求項 21 に記載の携帯電話機。
24. 前記利用者固有情報はパスワードをさらに含む、請求項 23 に記載の携帯電話機。
- 15 25. 前記利用者固有情報は前記利用者に予め付与された利用者識別子を含む、請求項 21 に記載の携帯電話機。
26. 前記利用者固有情報はパスワードをさらに含む、請求項 25 に記載の携帯電話機。
- 20 27. 前記識別情報は前記携帯電話機に固有の電話機固有情報をさらに含む、請求項 21 に記載の携帯電話機。
28. 前記電話機固有情報を記憶する手段をさらに備える、請求項 27 に記載の携帯電話機。
29. 前記電話機固有情報は携帯電話機の製造番号を含む、請求項 28 に記載の携帯電話機。
- 25 30. 前記電話機固有情報は前記携帯電話機のサブスクライバ識別子を含む、請求項 28 に記載の携帯電話機。
31. 前記送受信手段はさらに決済金額を受信し、
前記送受信手段により受信された決済金額を記憶する手段をさらに備え、
前記送受信手段はさらに前記記憶された決済金額を讀出して前記コンピュータ

に送信する、請求項 1 9 に記載の携帯電話機。

3 2. 前記記憶された第 1 の口座の残高から前記記憶された決済金額を減算する手段をさらに備える、請求項 3 1 に記載の携帯電話機。

3 3. 前記コンピュータは第 2 の口座をさらに有し、

5 前記入力手段は前記利用者の操作に応じて前記第 1 の口座から前記第 2 の口座に振替えられるべき振替金額を入力し、

前記送受信手段はさらに前記入力された振替金額を前記コンピュータに送信し、
前記送受信手段はさらに前記第 2 の口座の残高を使用可能にするためのワンタイム識別子を受信し、

10 前記ワンタイム識別子が有効か否かを判定する手段と、

前記ワンタイム識別子の判定の結果、前記ワンタイム識別子が有効な場合、前記送受信手段により受信された決済金額が前記第 2 の口座の残高以内か否かを判定する手段と、

15 前記決済金額の判定の結果、前記決済金額が前記第 2 の口座の残高以内の場合、前記受信したワンタイム識別子を出力する手段と、

前記決済金額を前記第 2 の口座から減じる手段とをさらに備える、請求項 3 1 に記載の携帯電話機。

FIG. 1

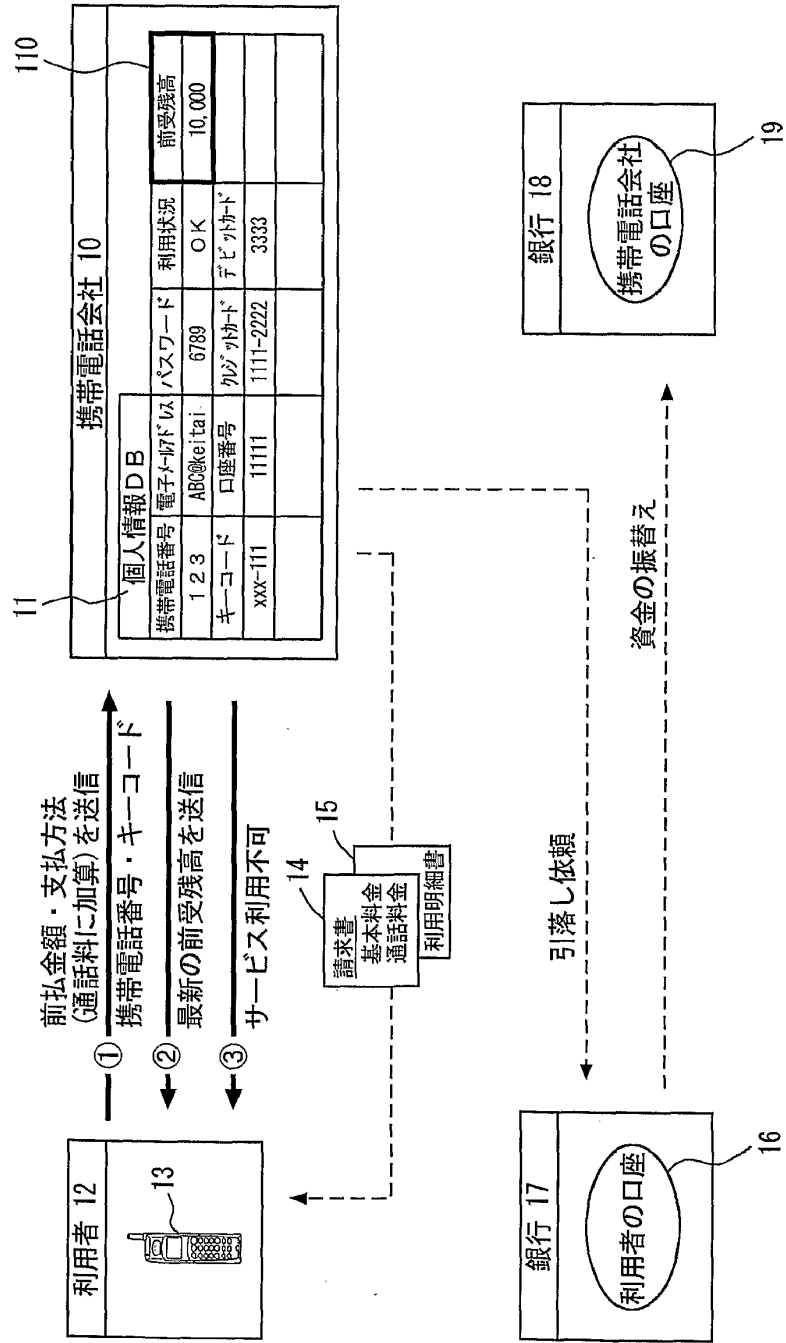


FIG. 2

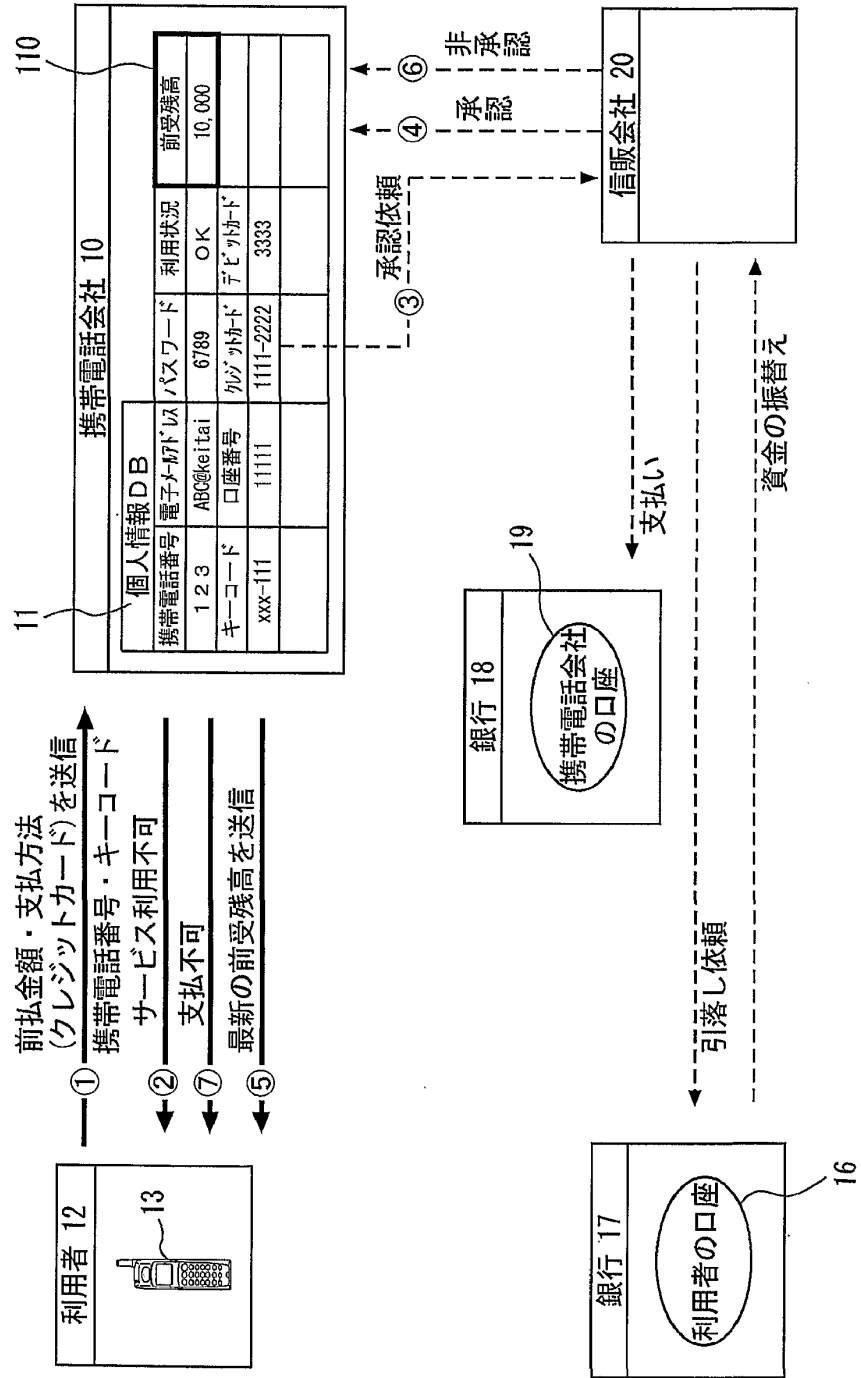


FIG. 3

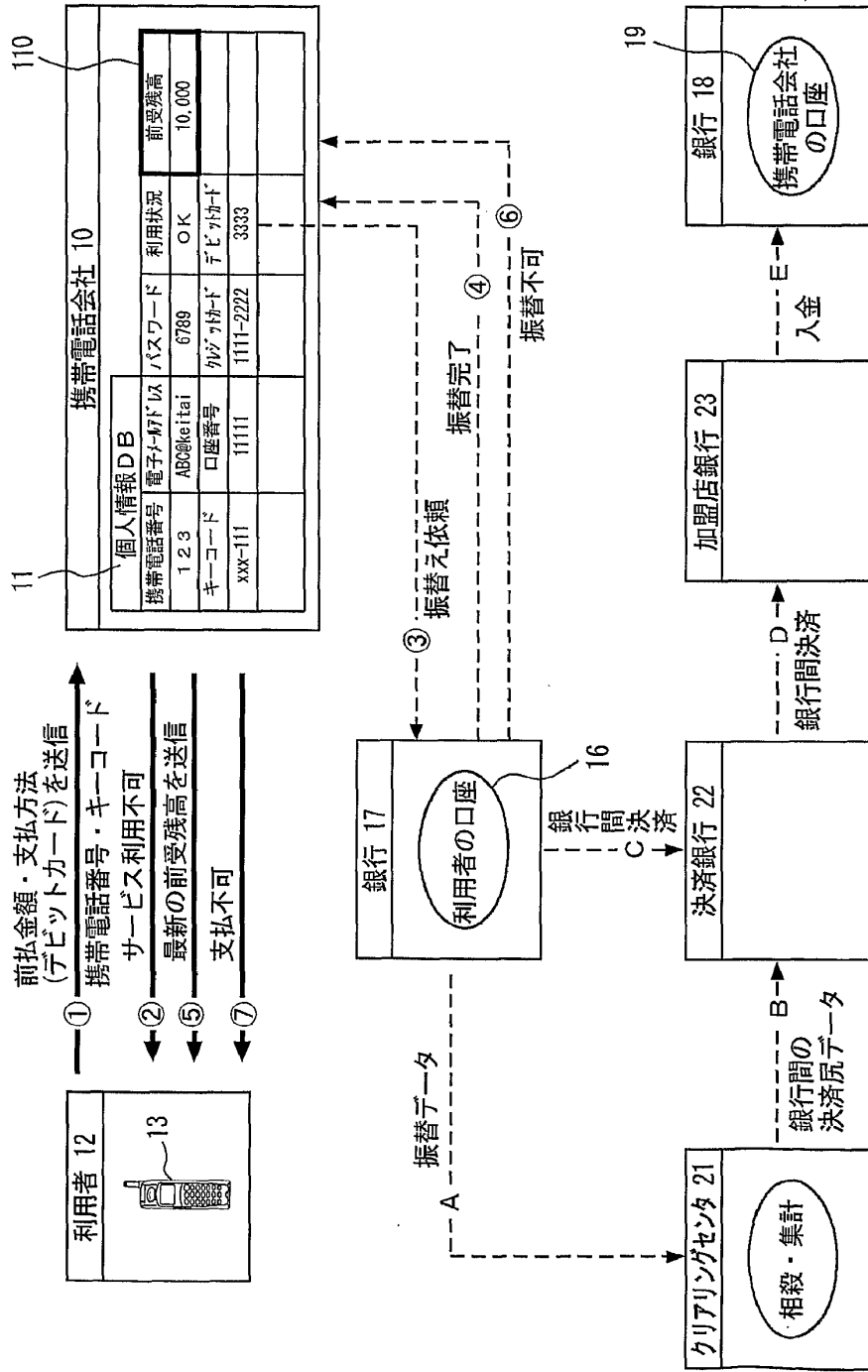


FIG. 4

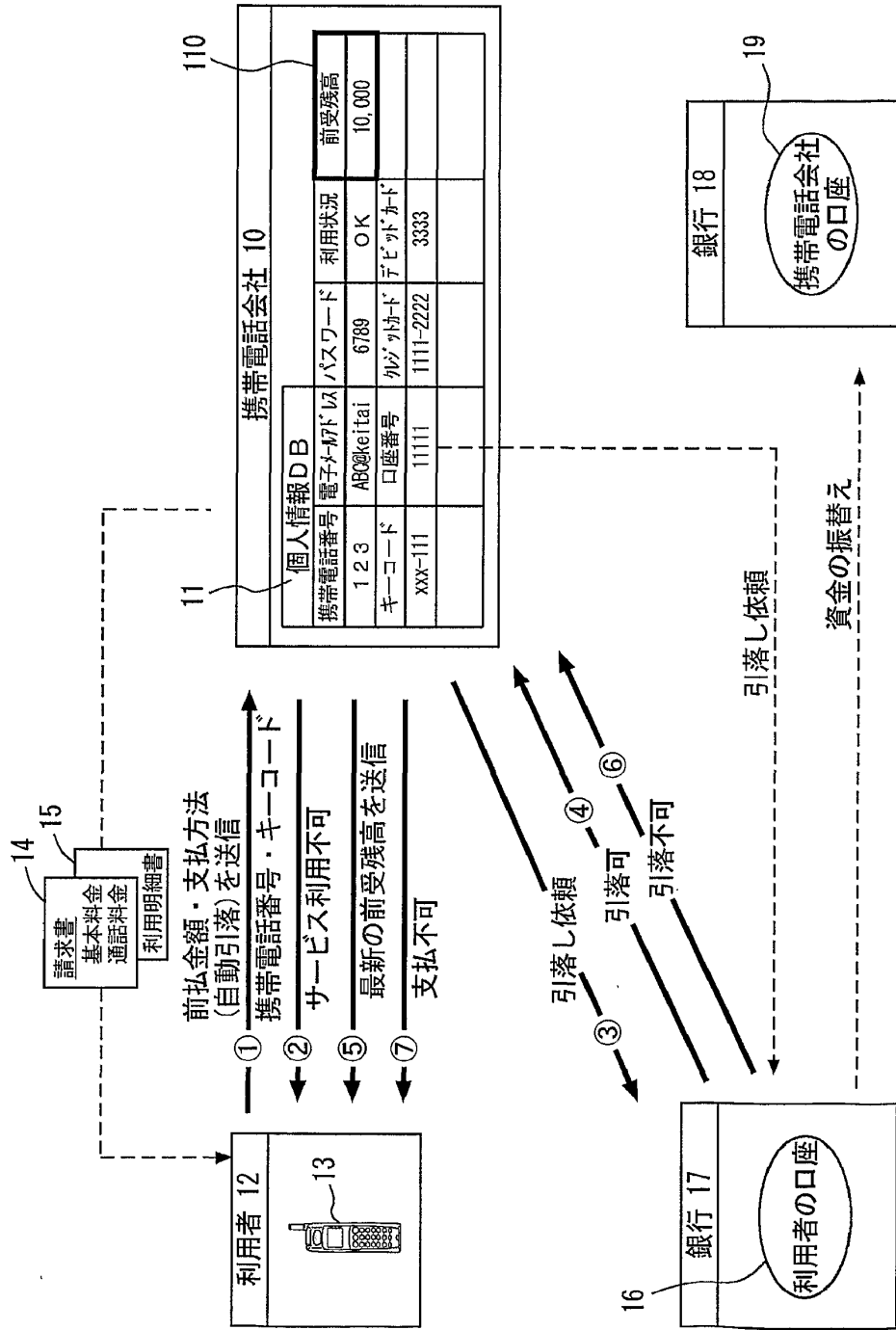


FIG. 5

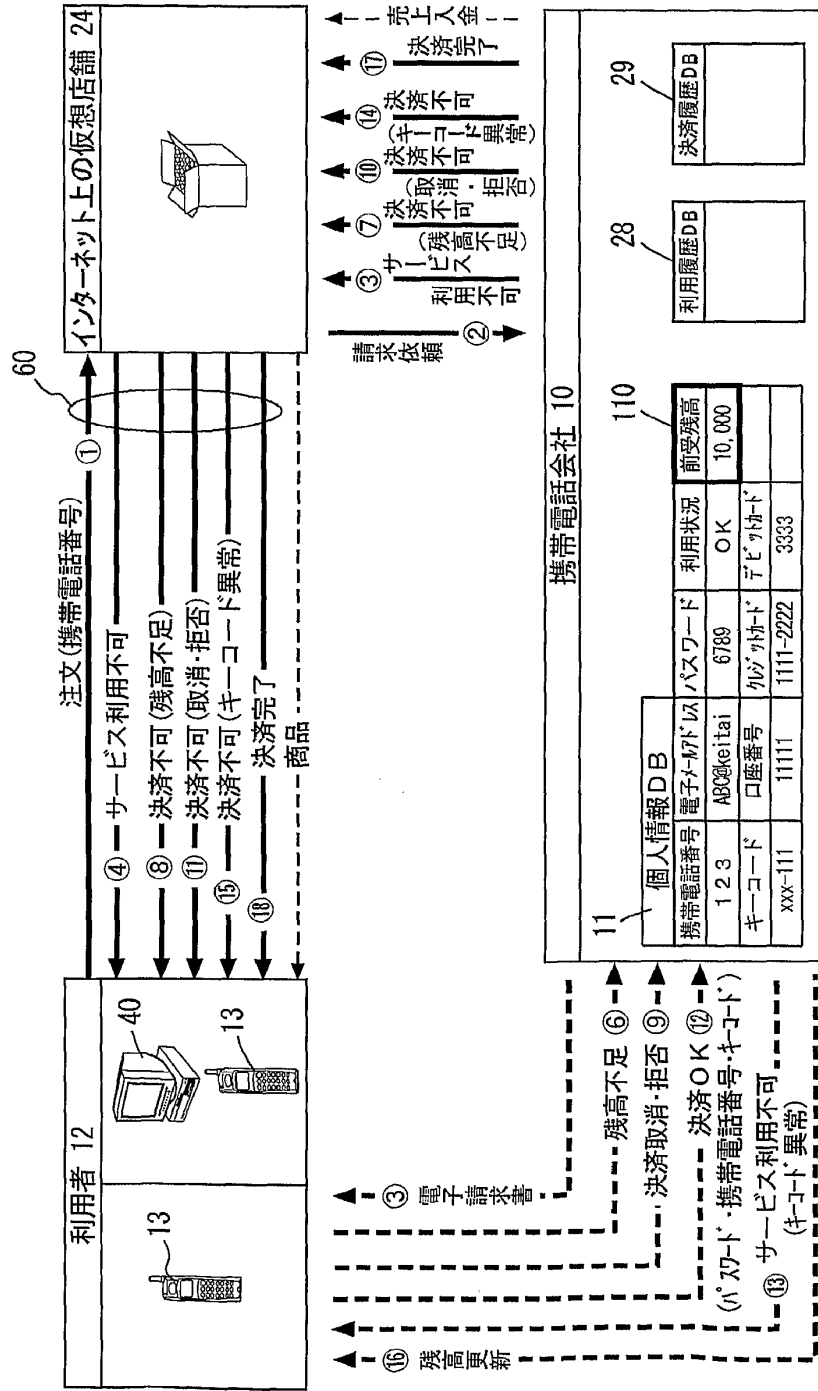


FIG. 6

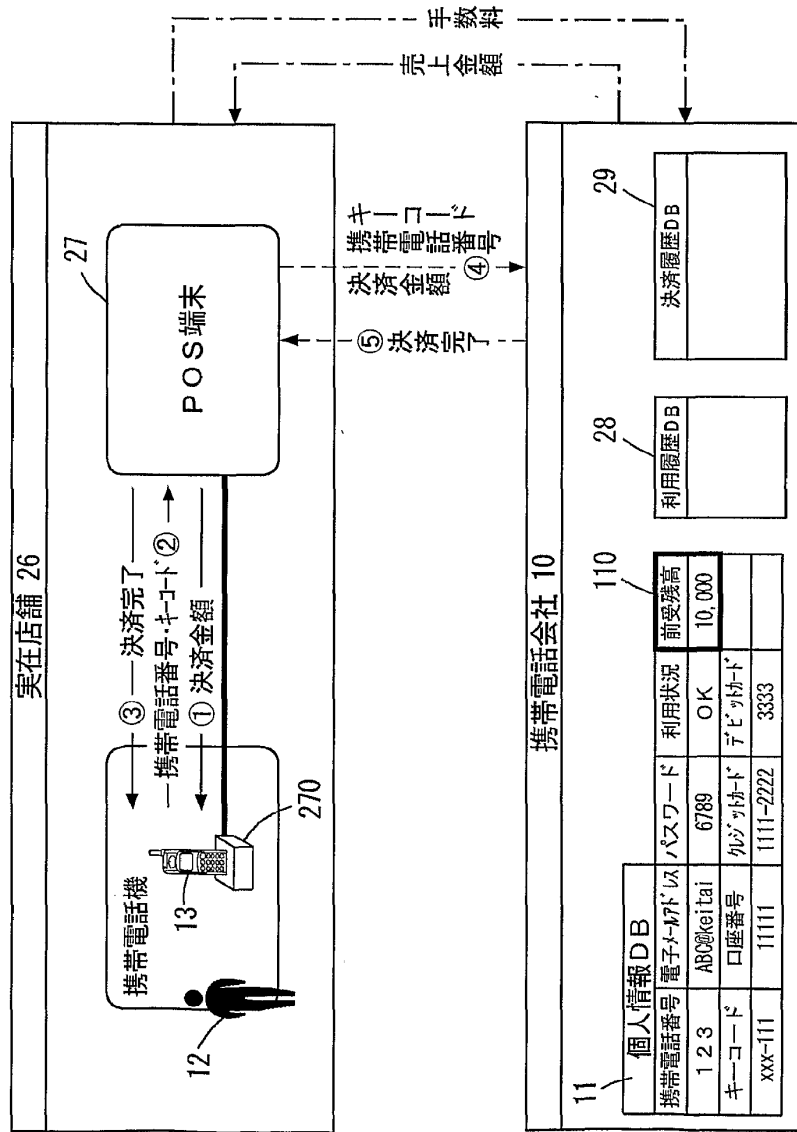


FIG. 7

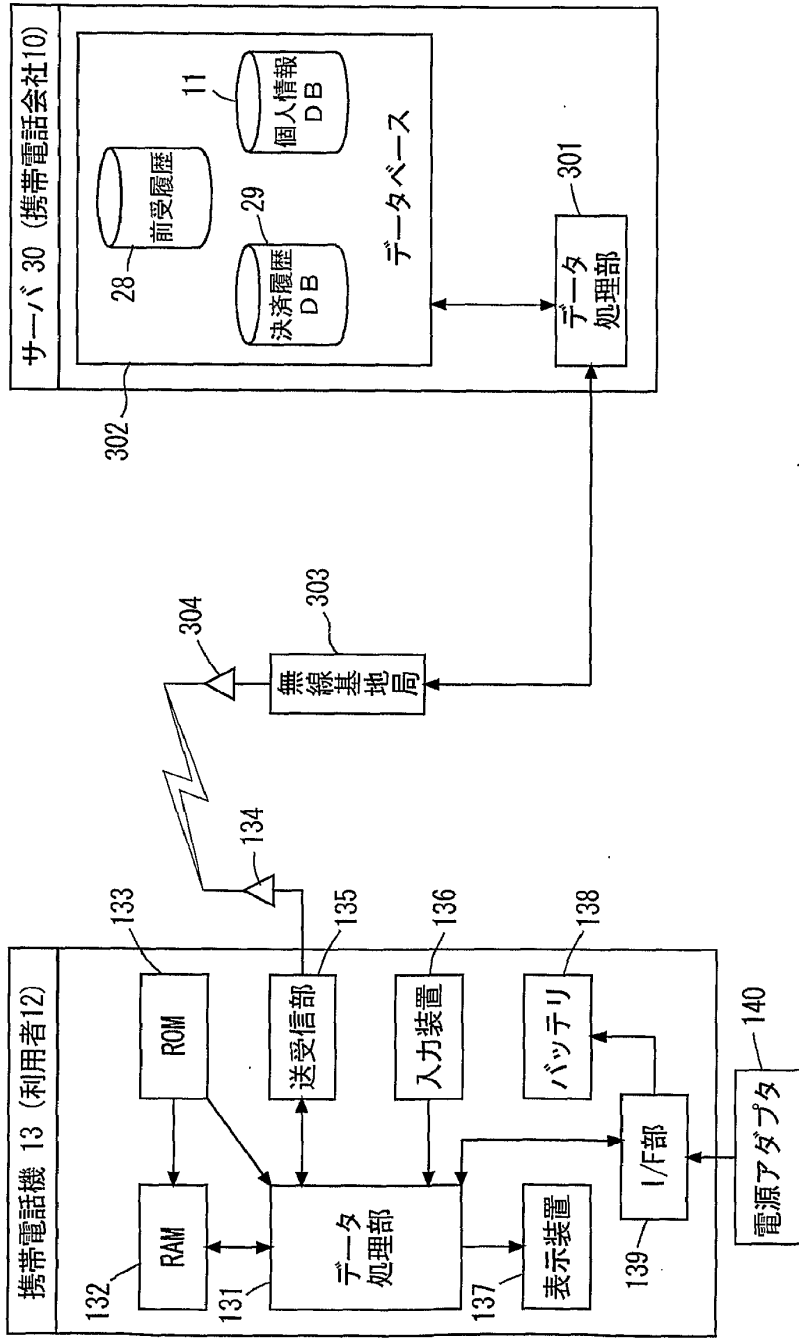


FIG. 8

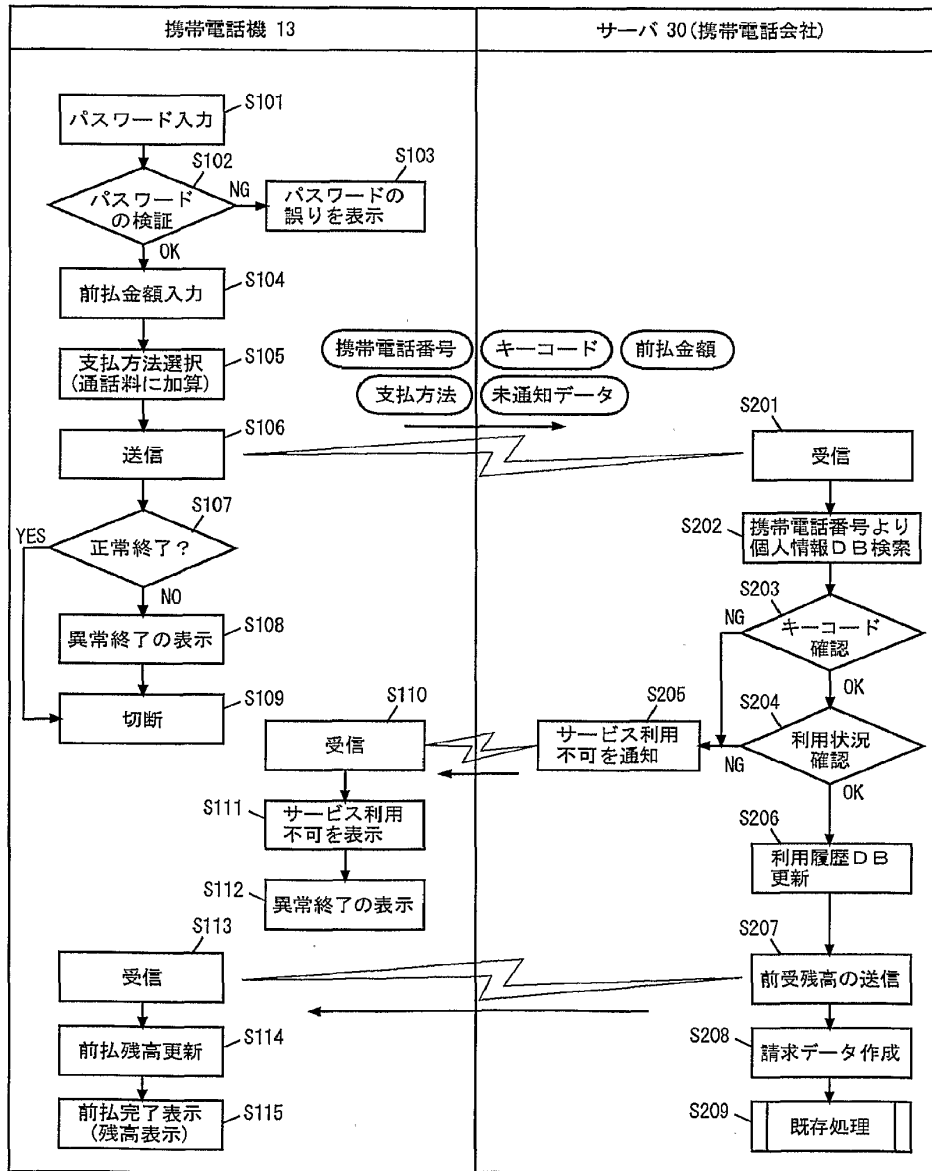


FIG. 9

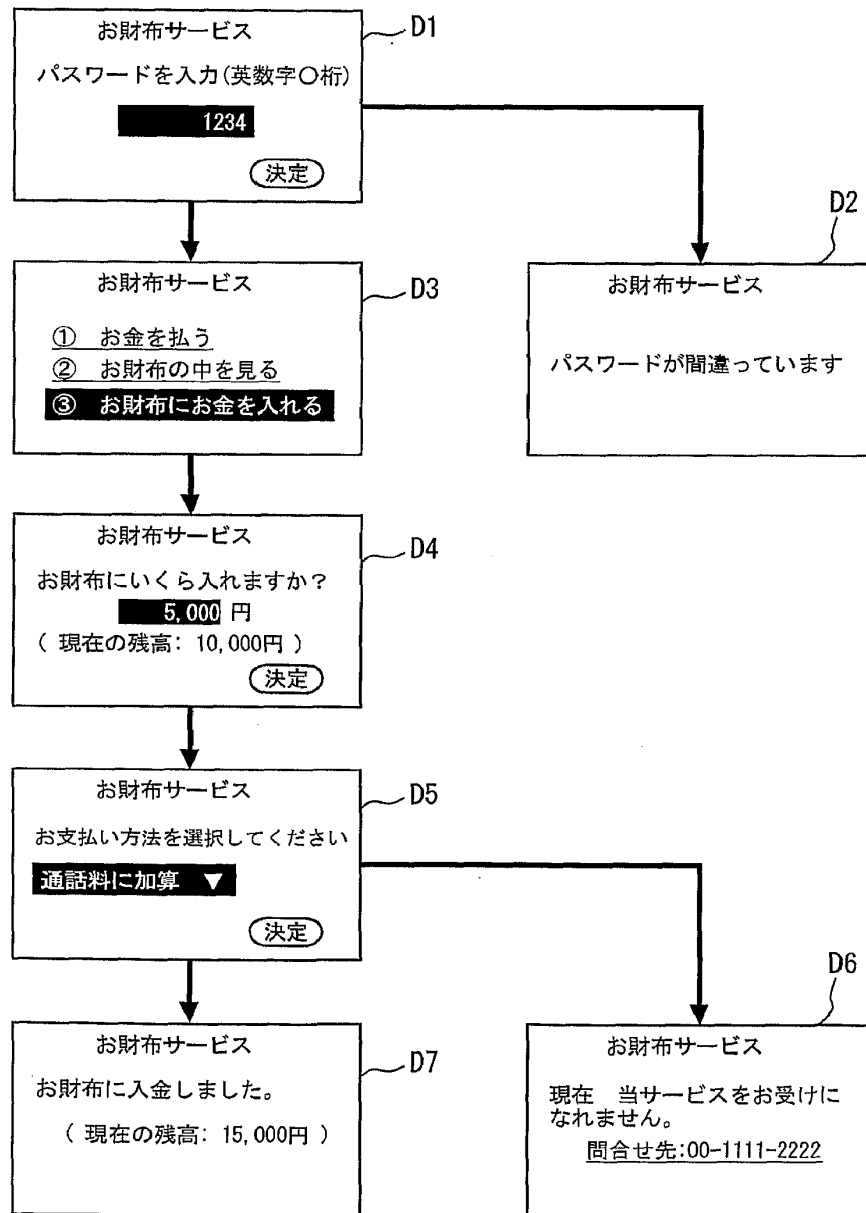


FIG. 10

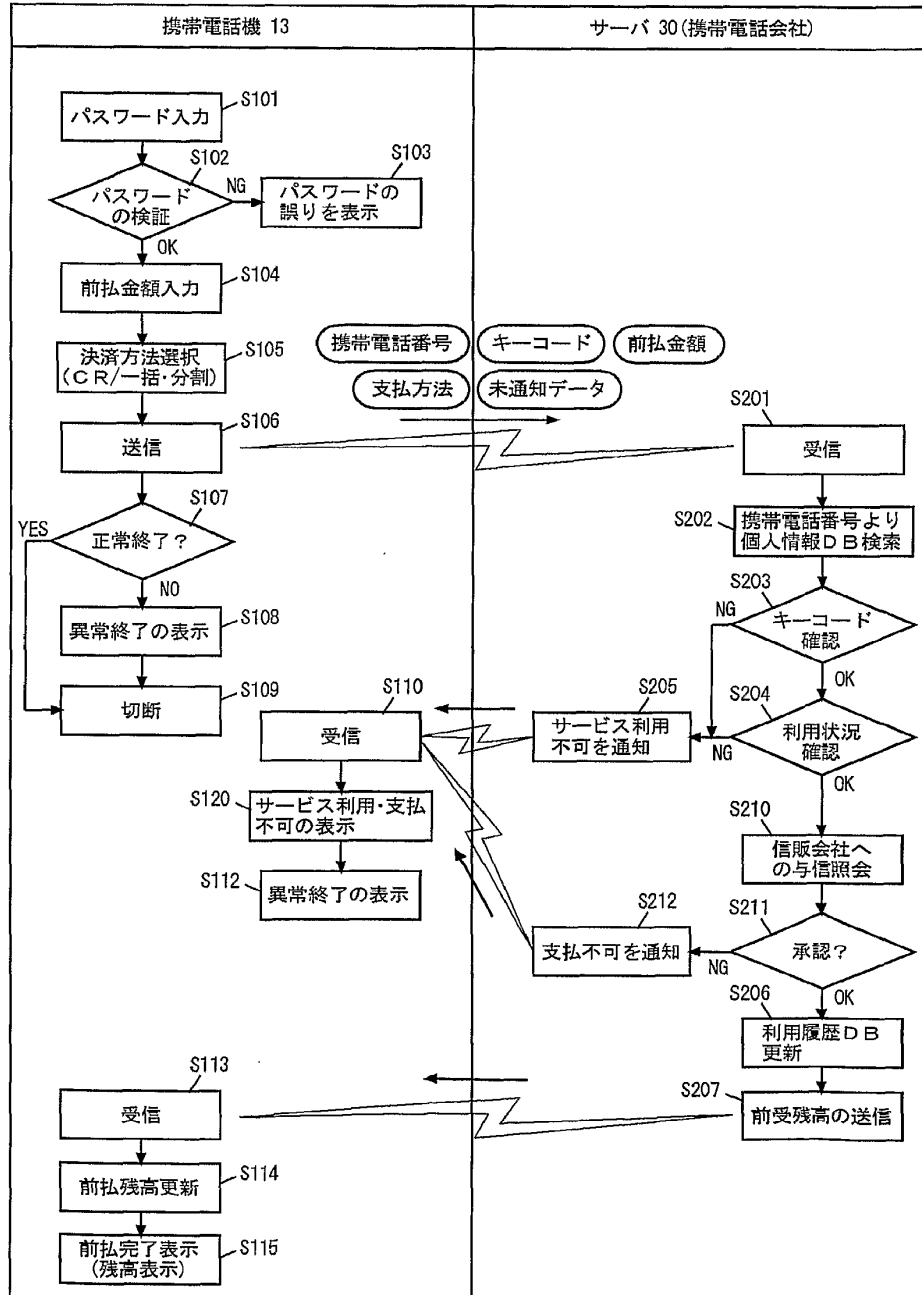


FIG. 11

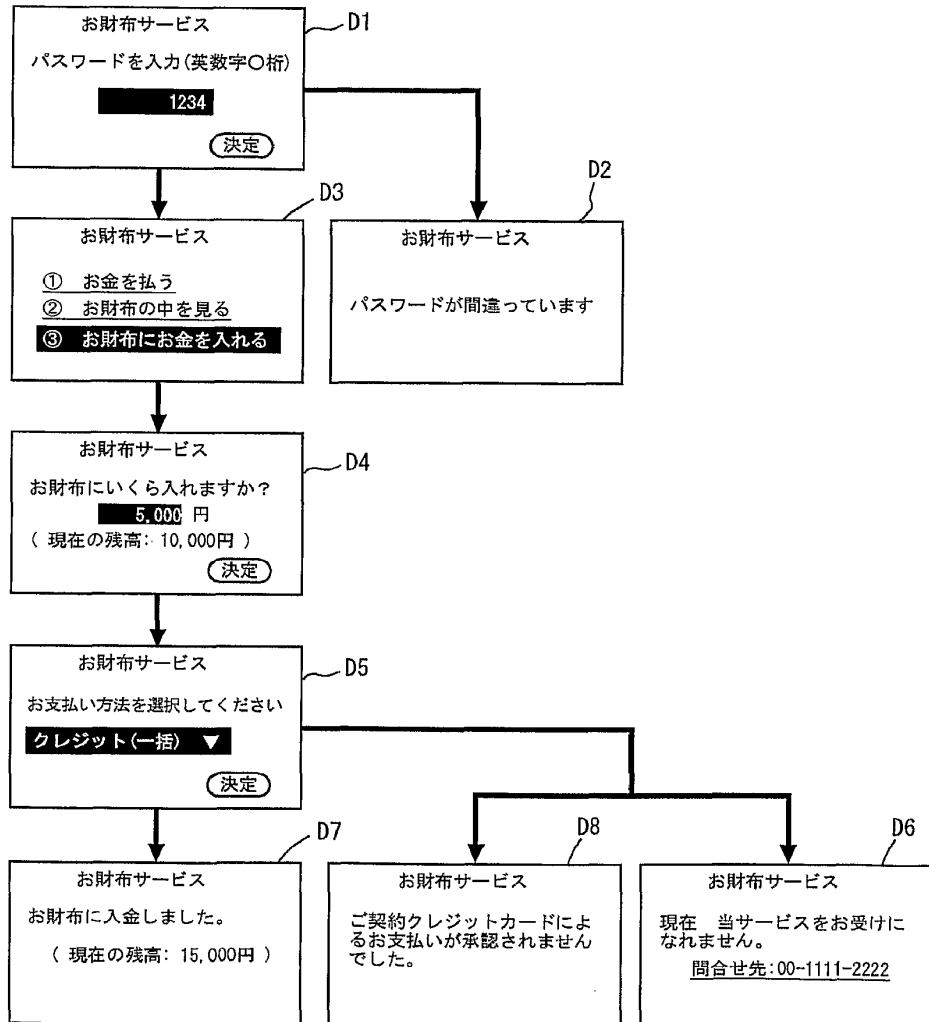


FIG. 12

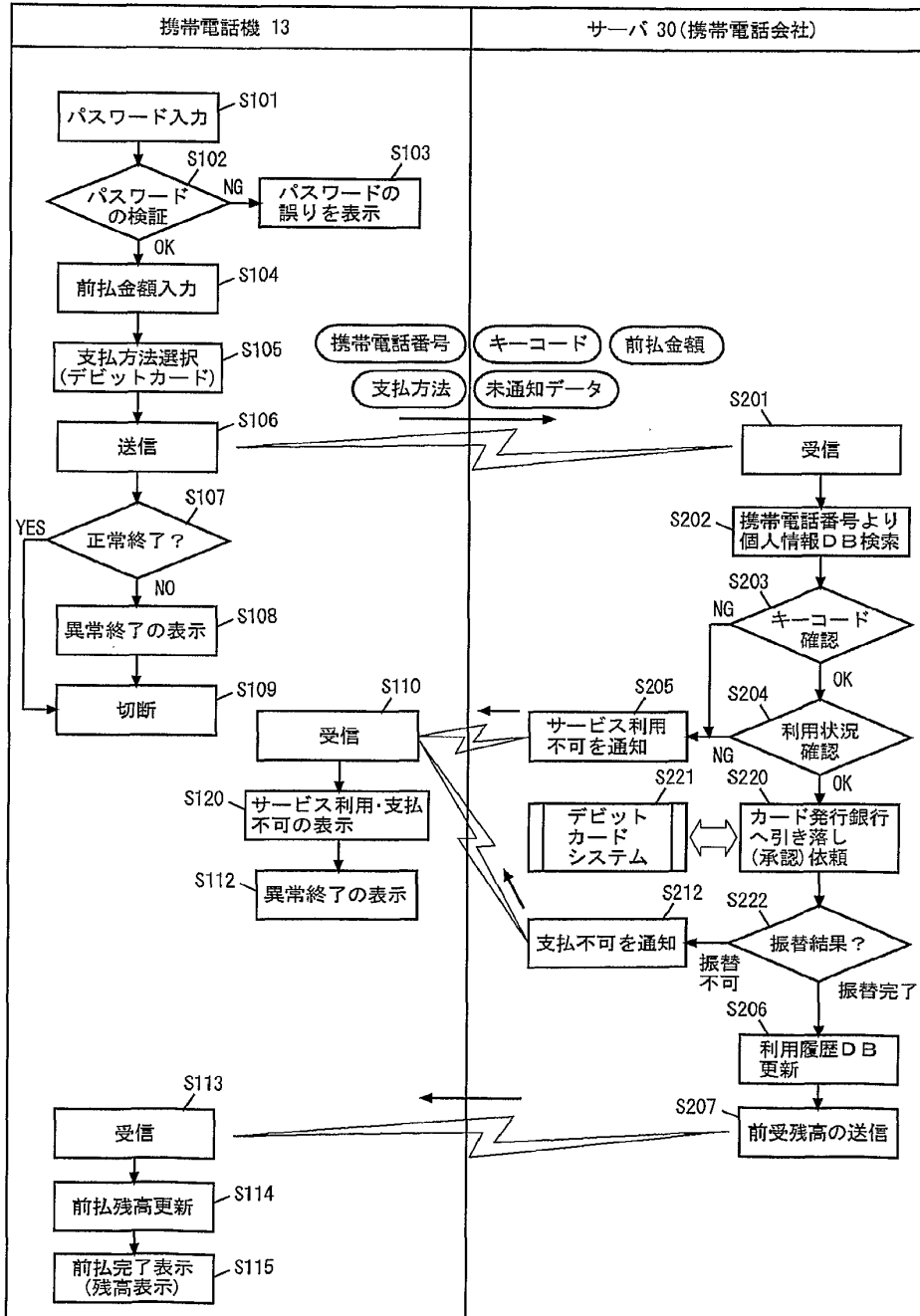


FIG. 13

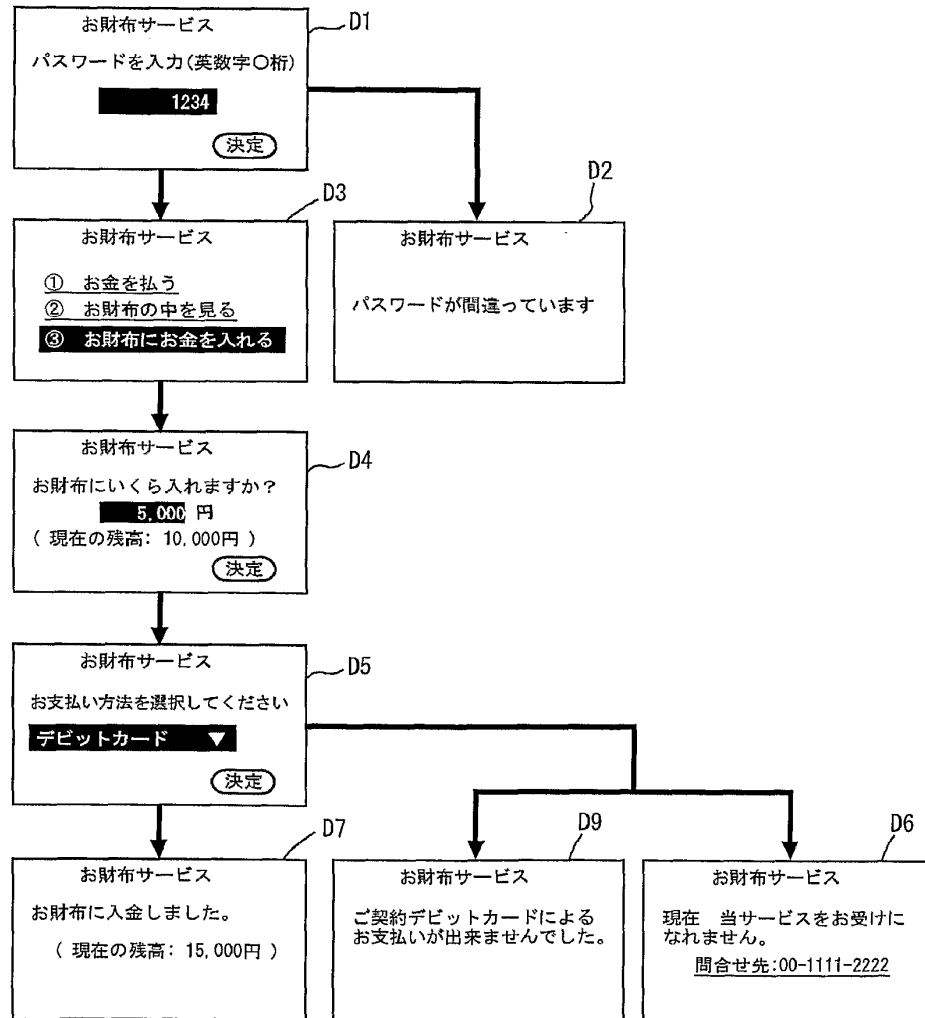


FIG. 14

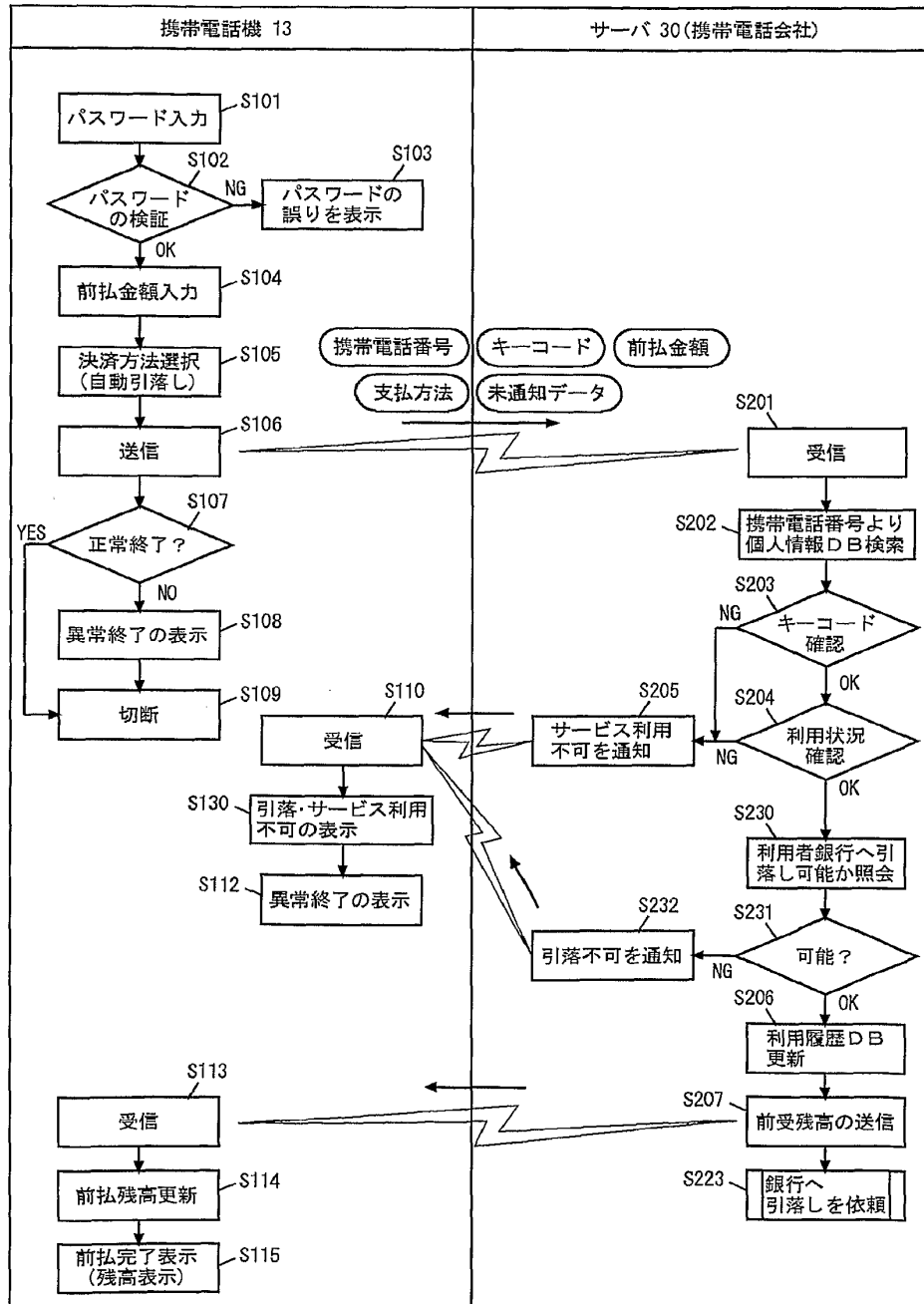


FIG. 15

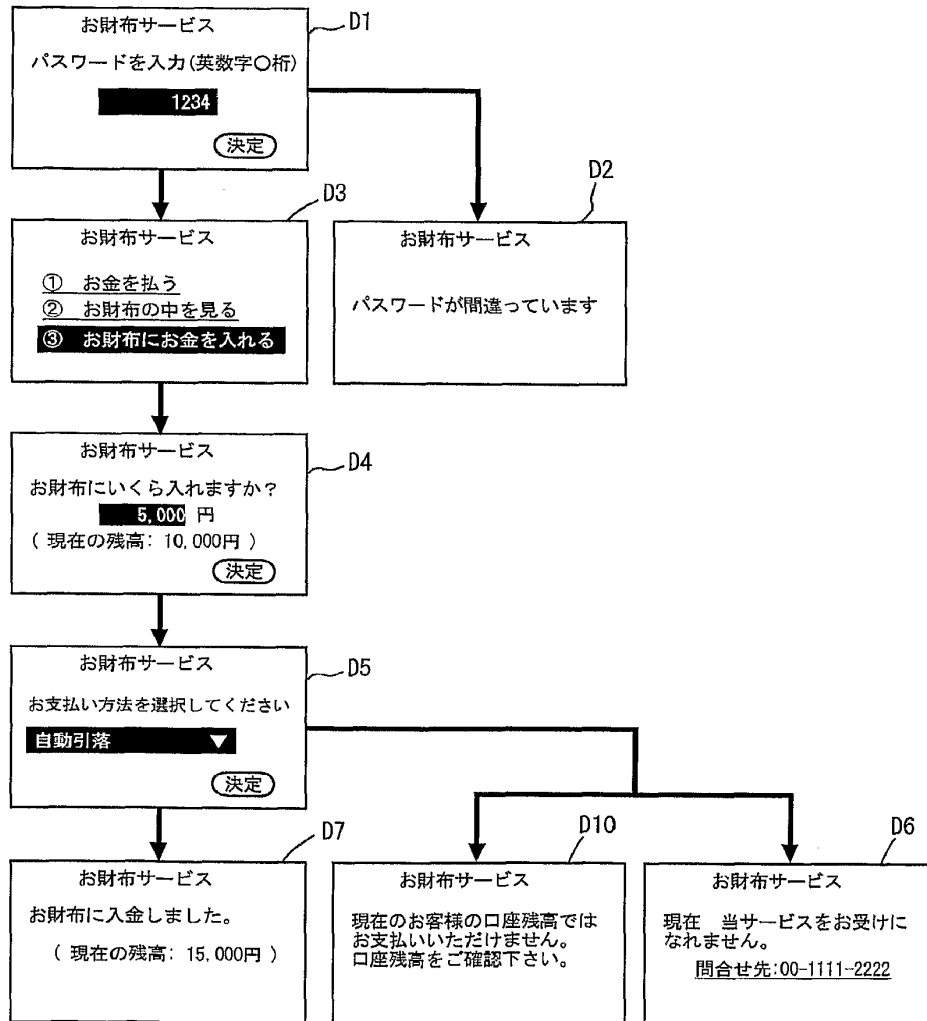


FIG. 16

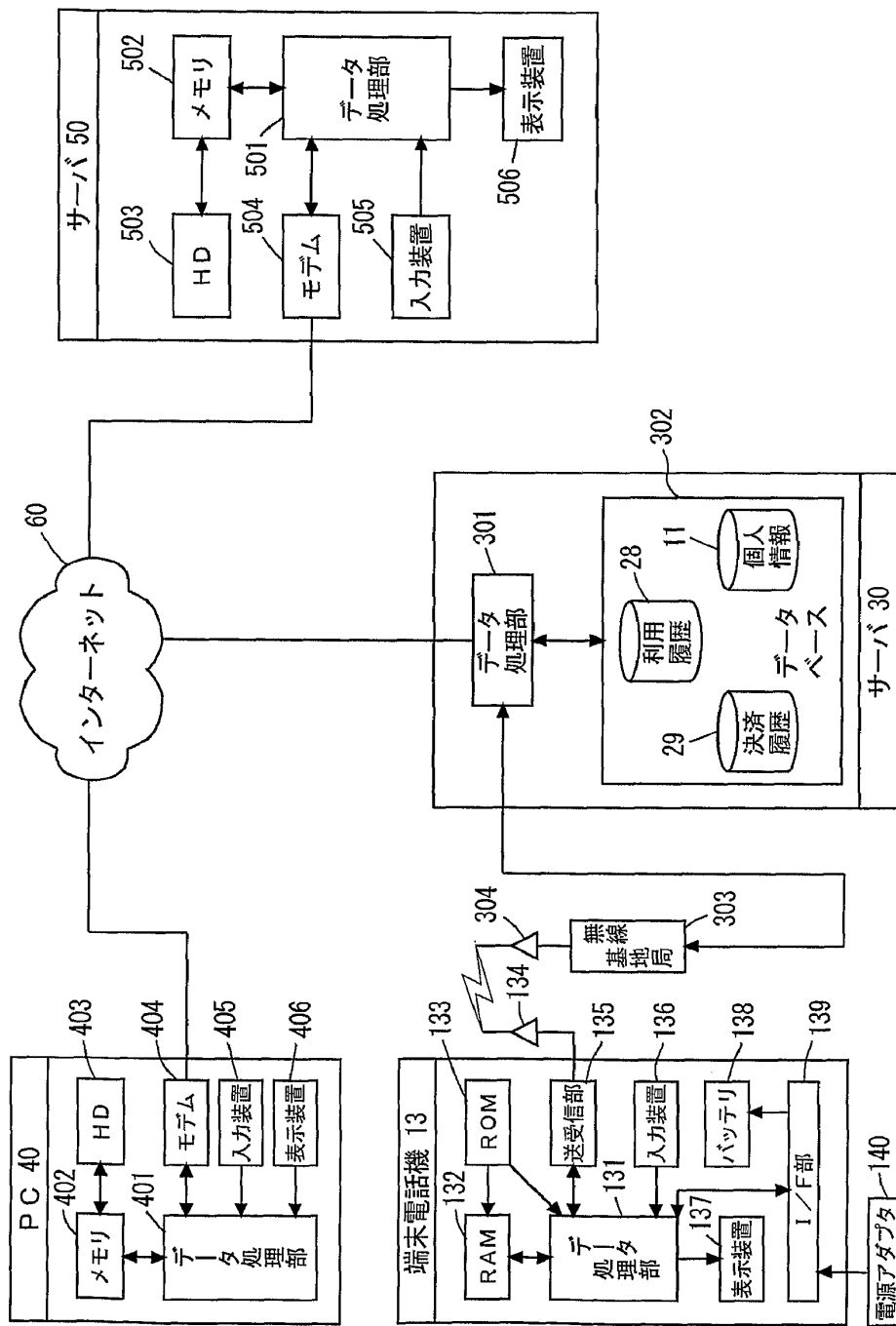


FIG. 17

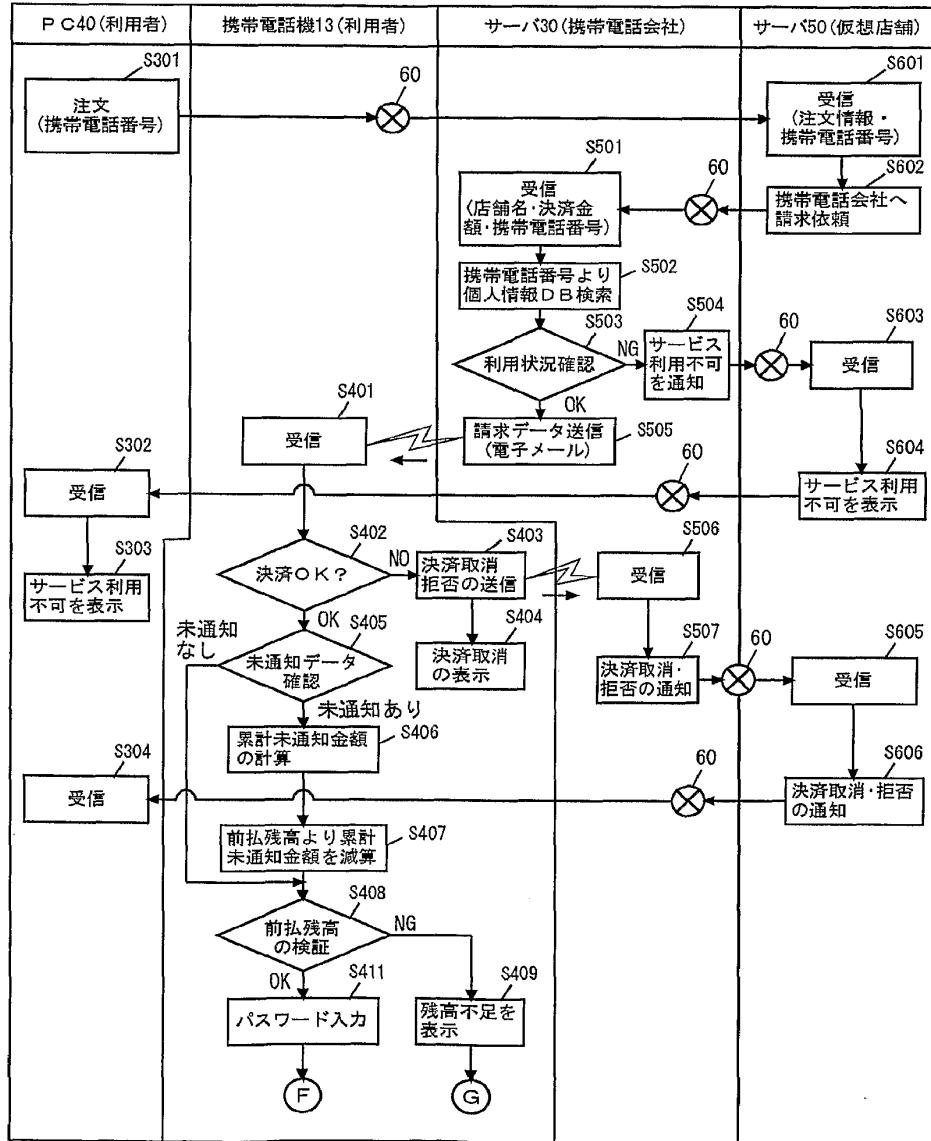


FIG. 18

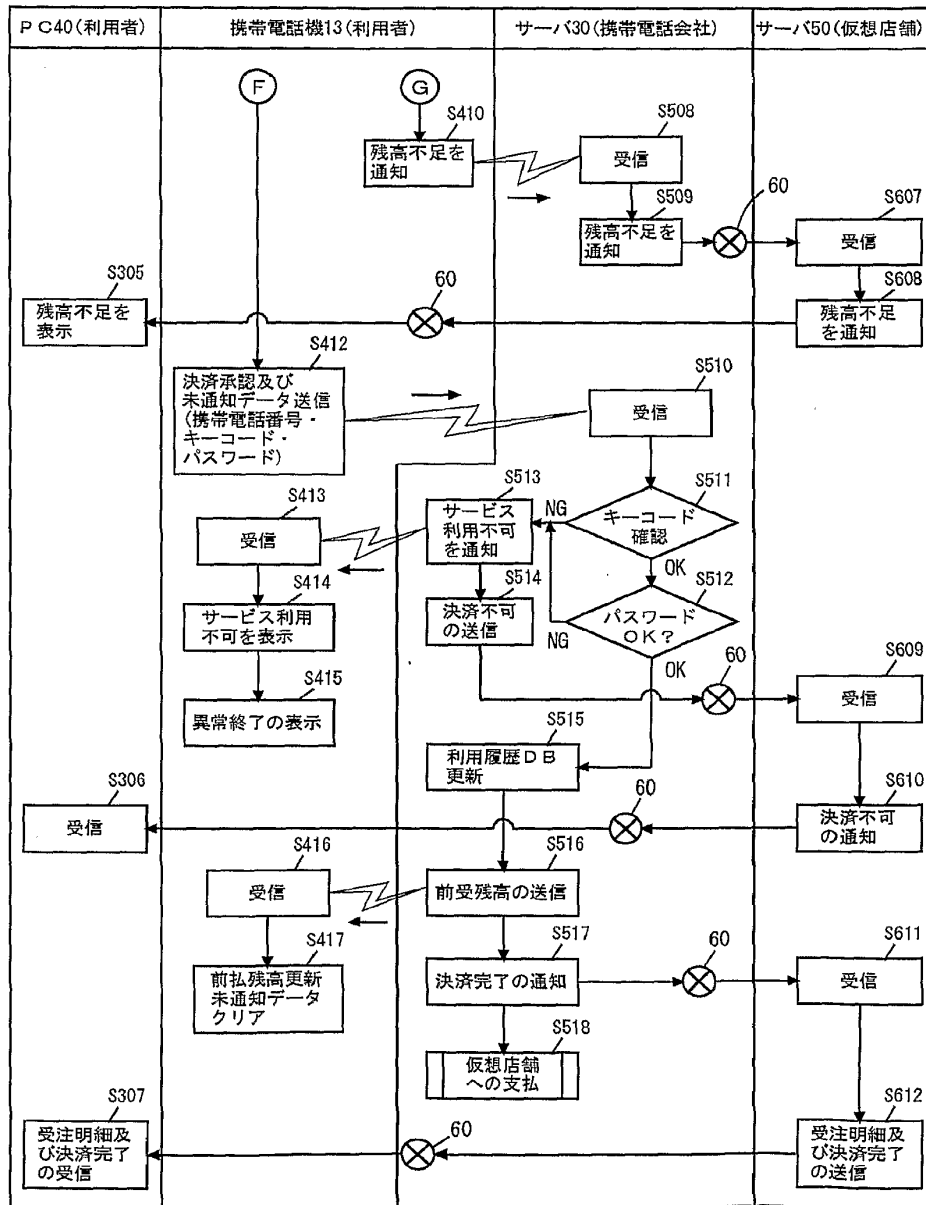


FIG. 19

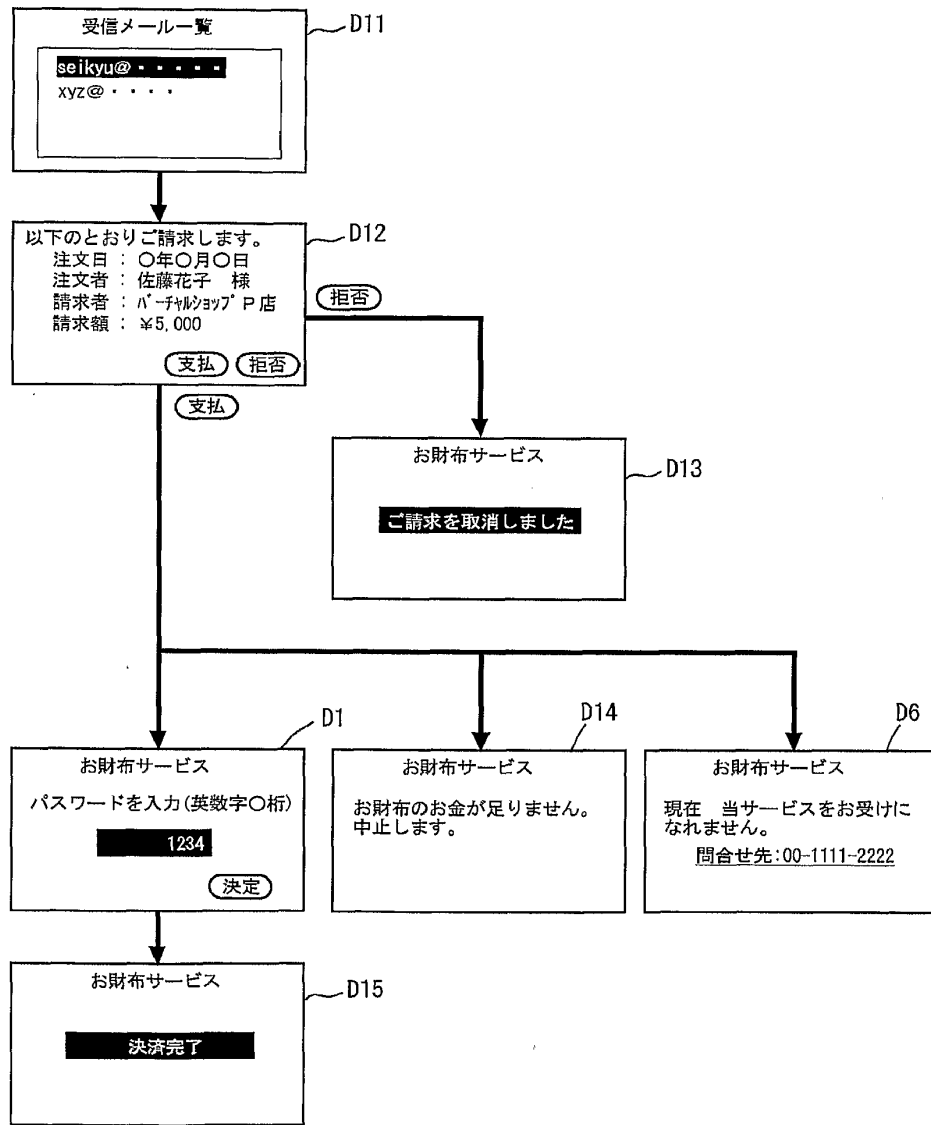


FIG. 20

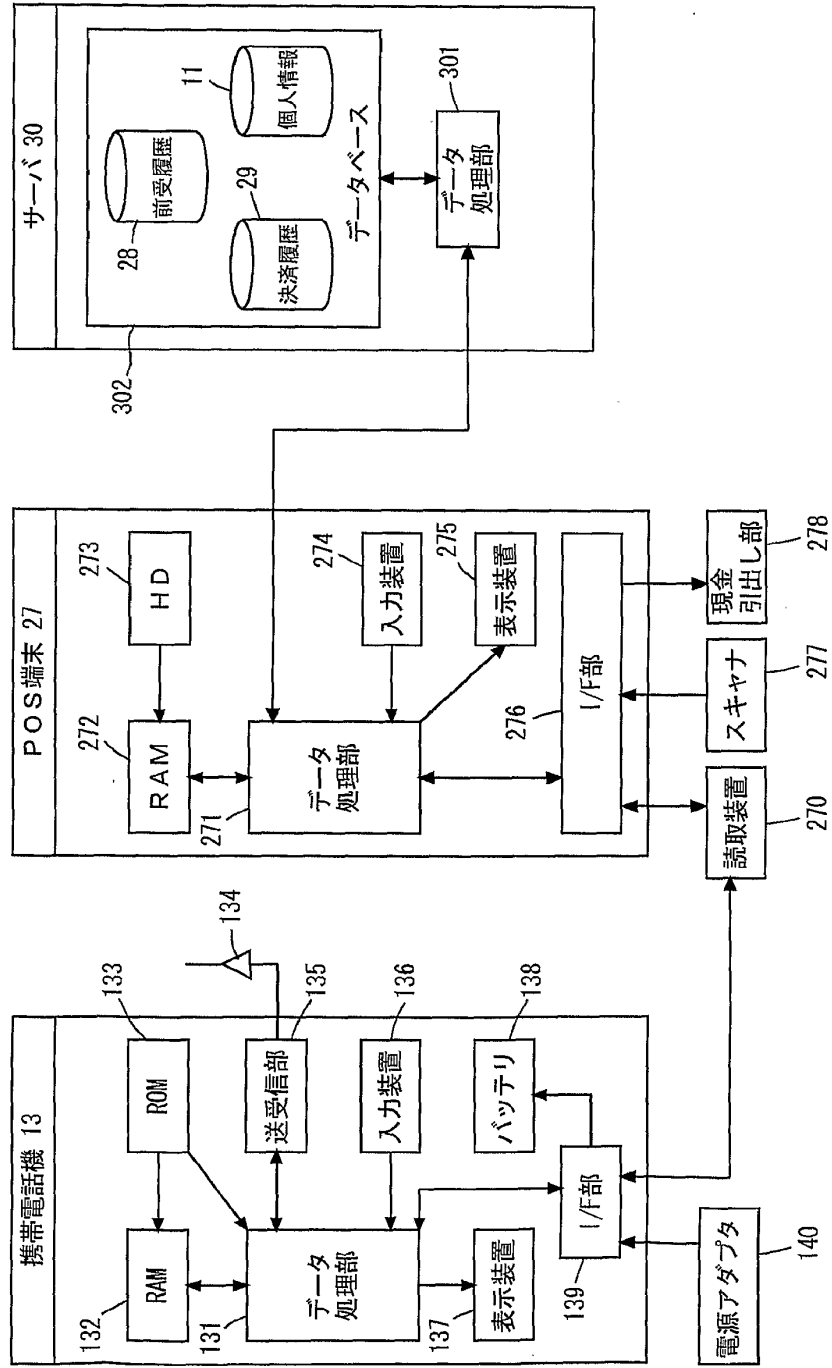


FIG. 21

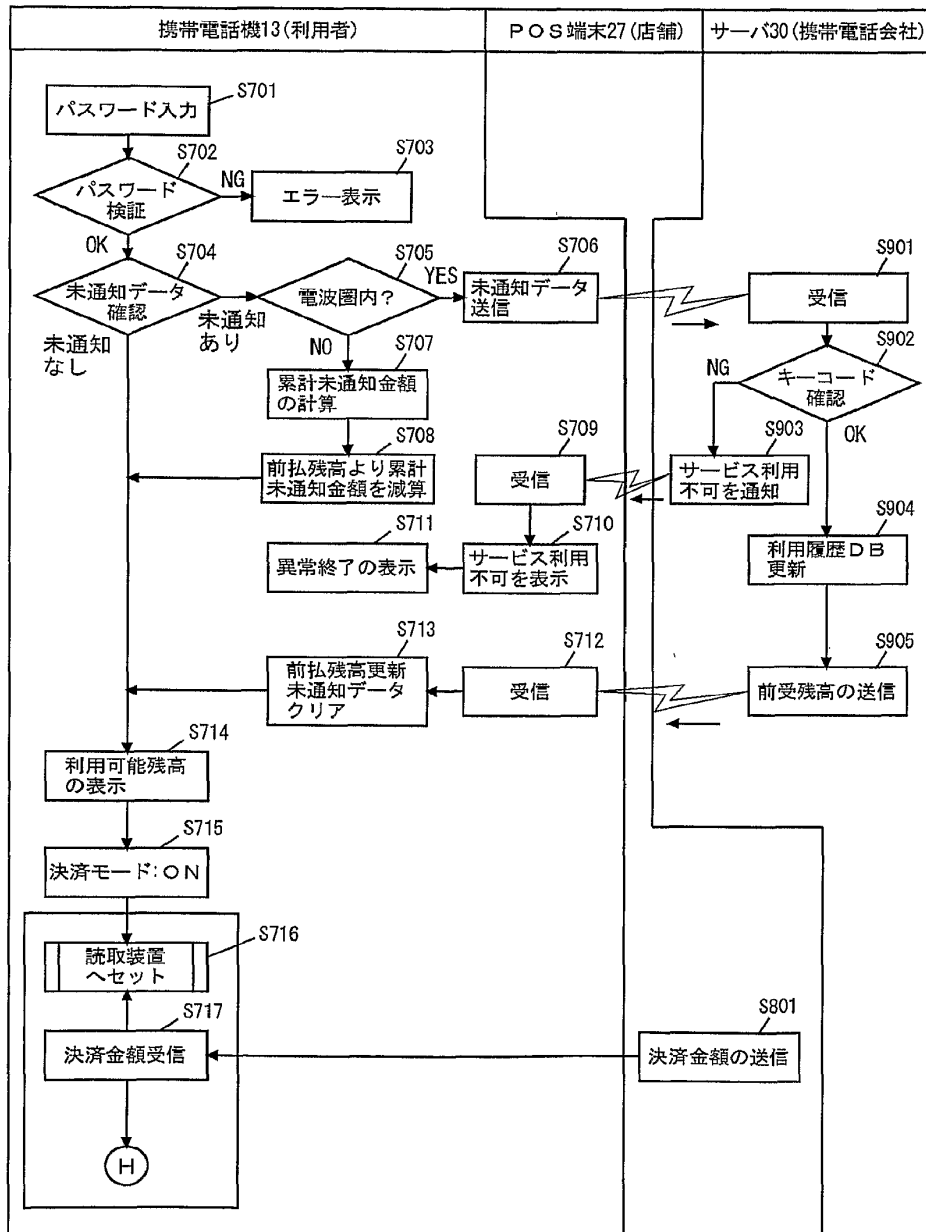


FIG. 22

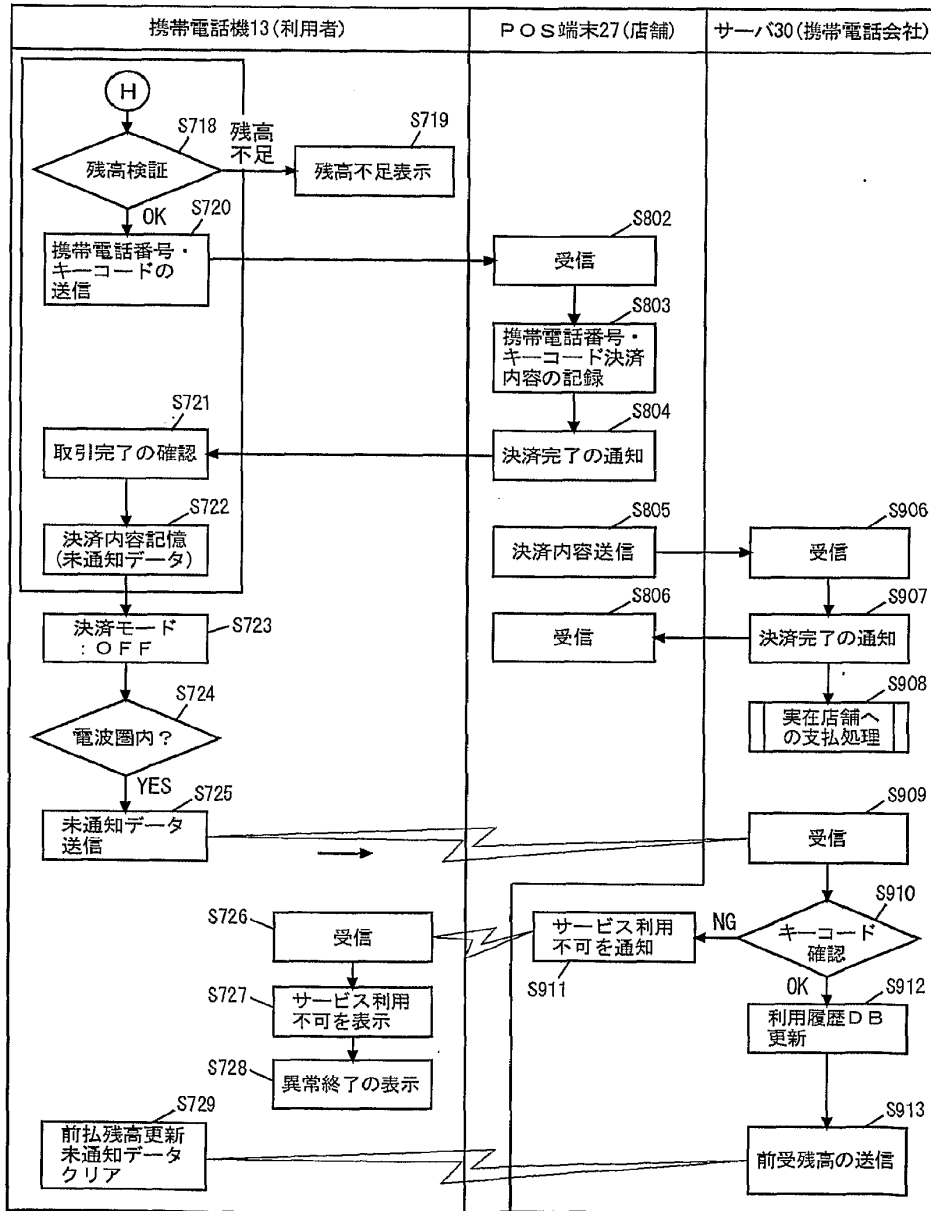


FIG. 23

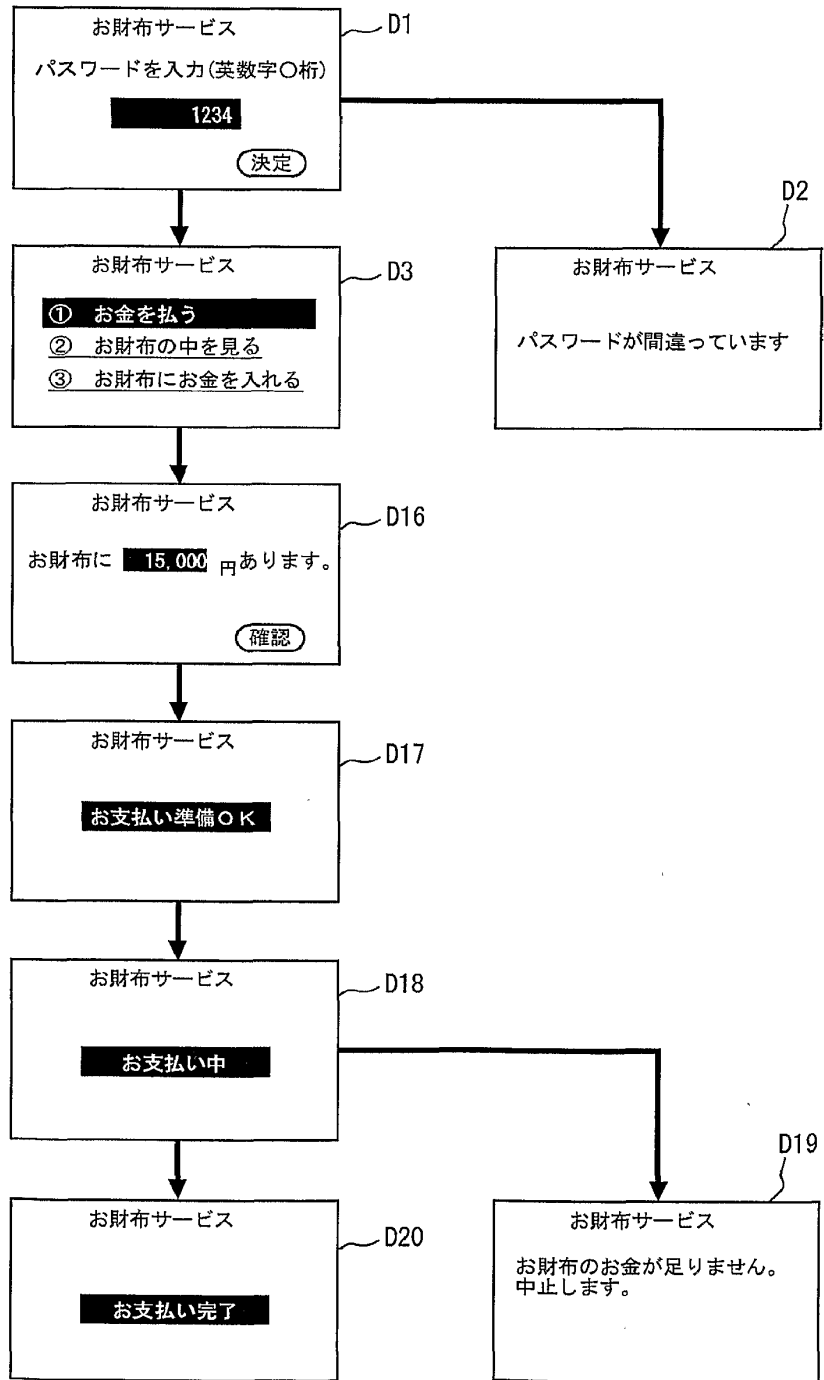


FIG. 24

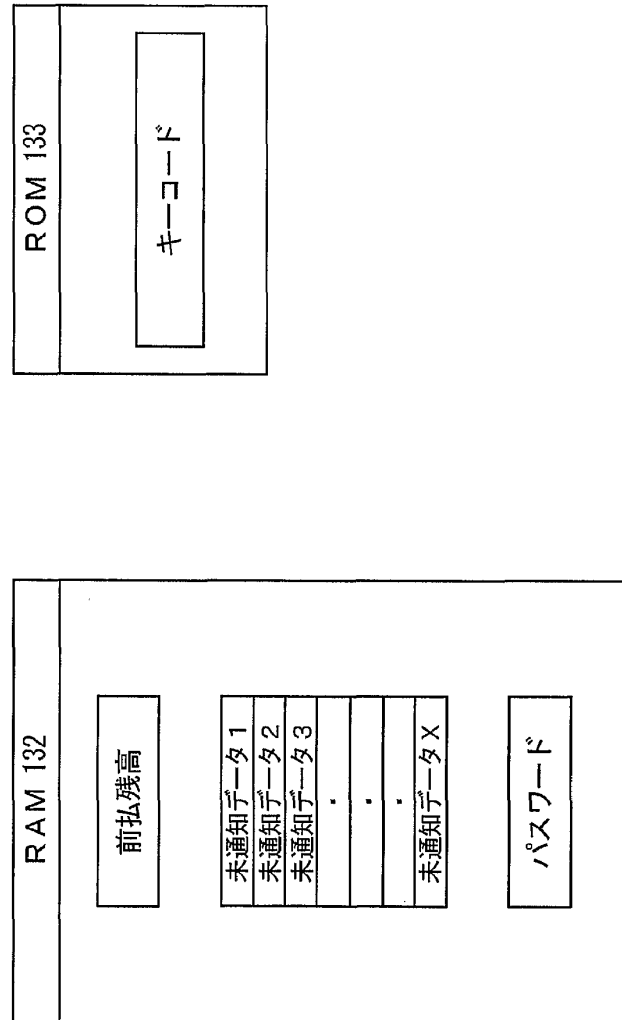


FIG. 25

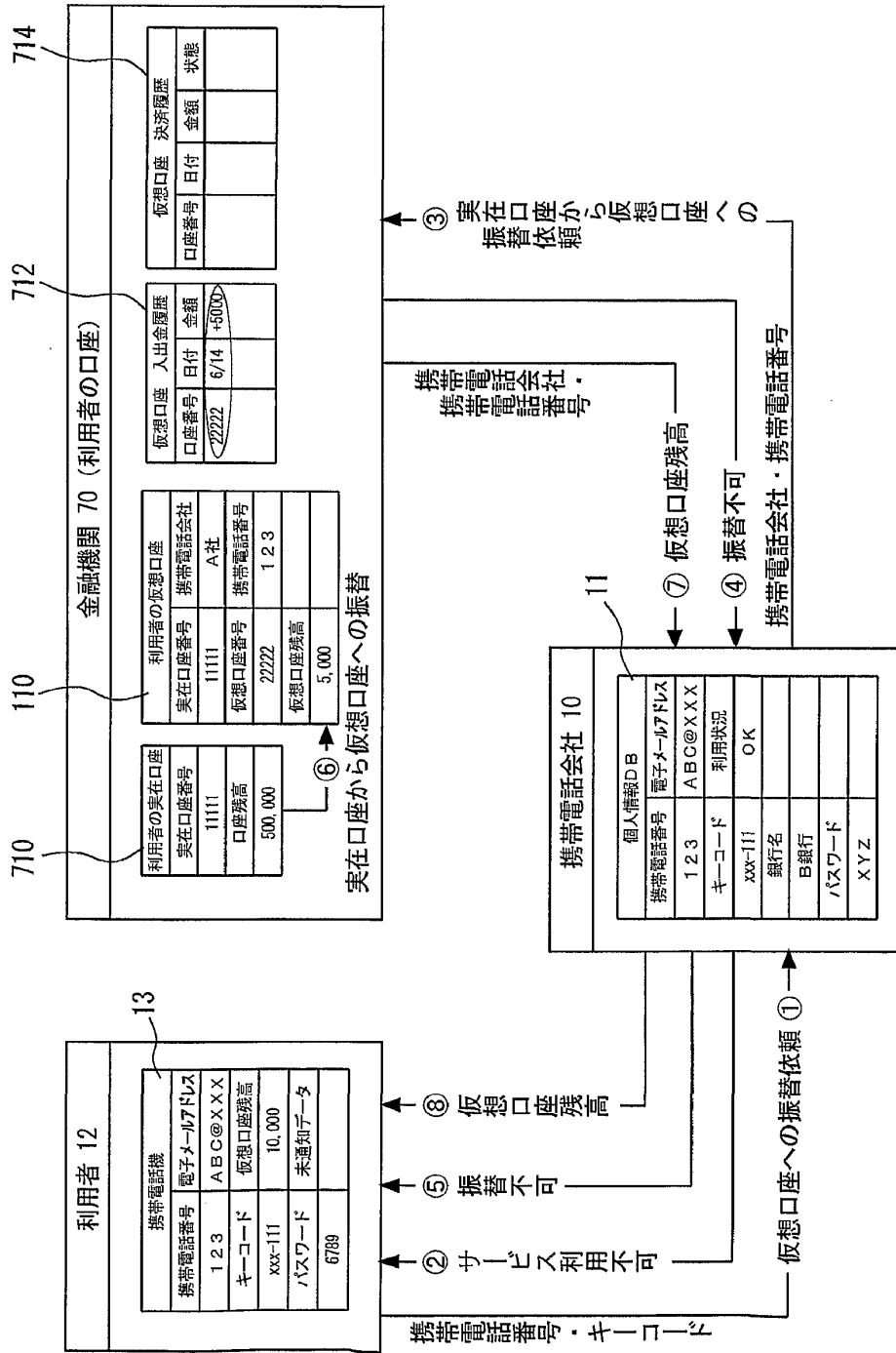


FIG. 26

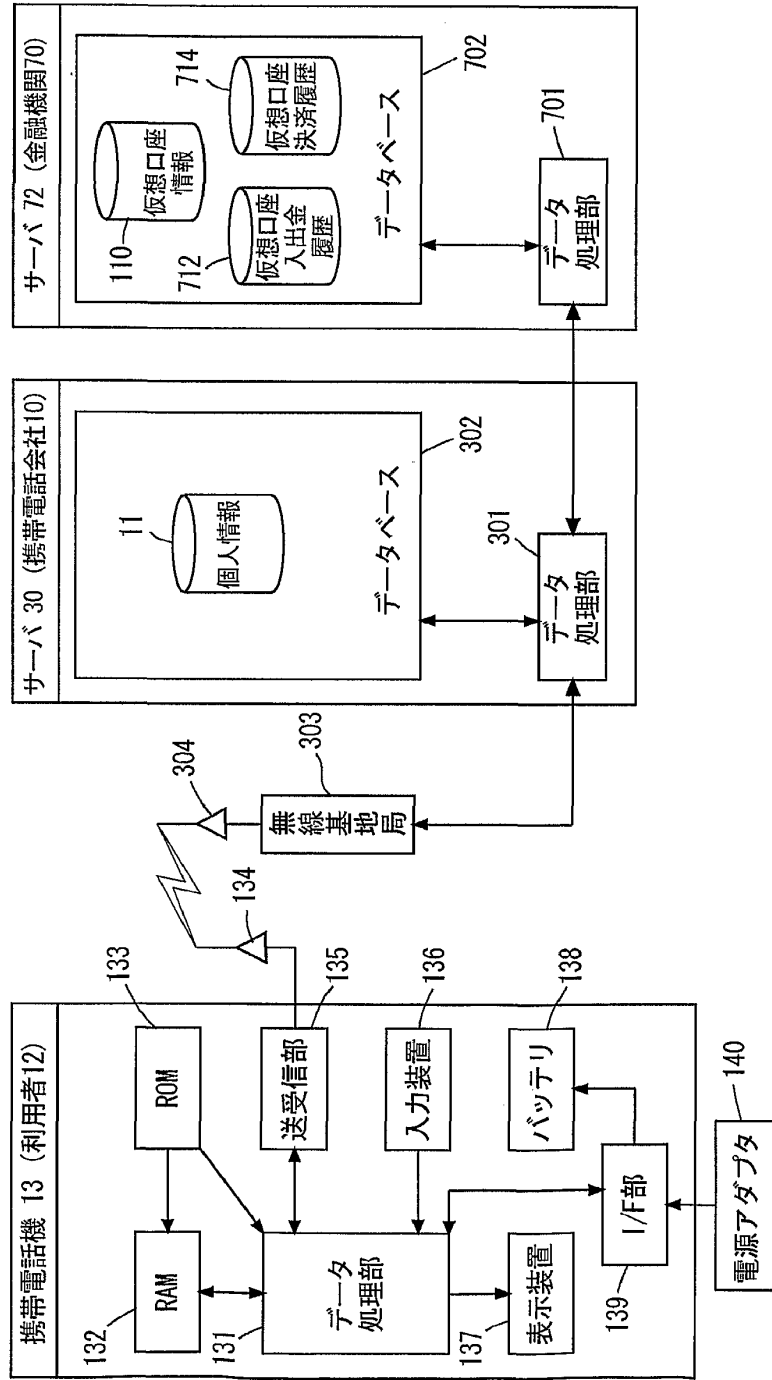


FIG. 27

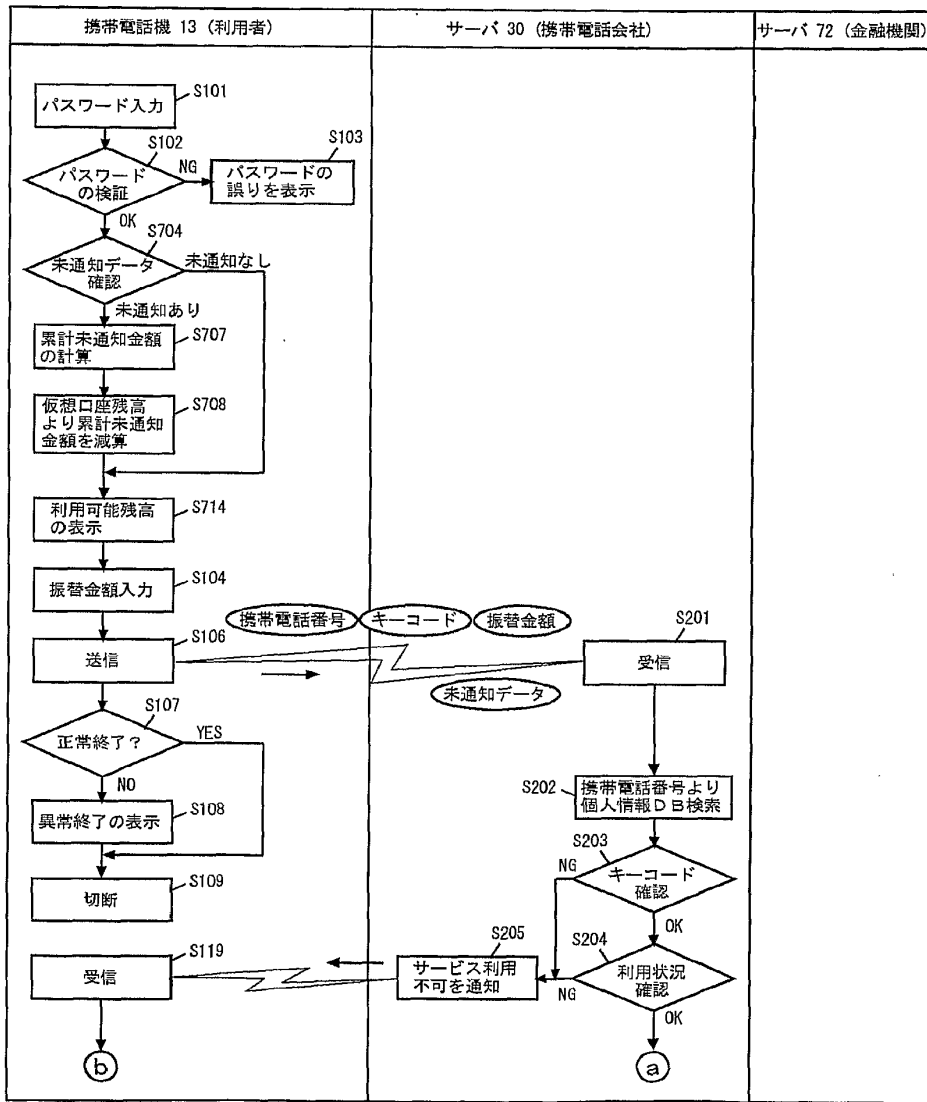


FIG. 28

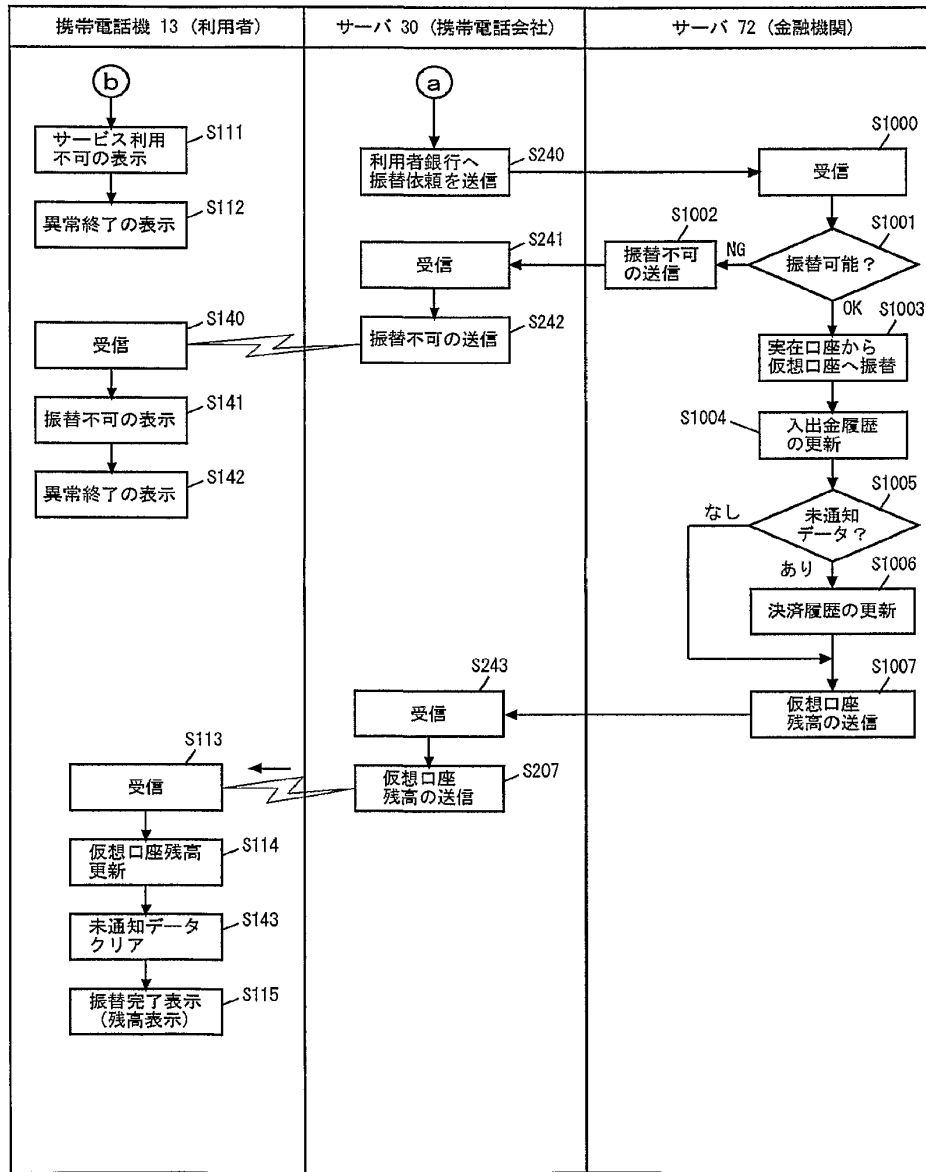


FIG. 29

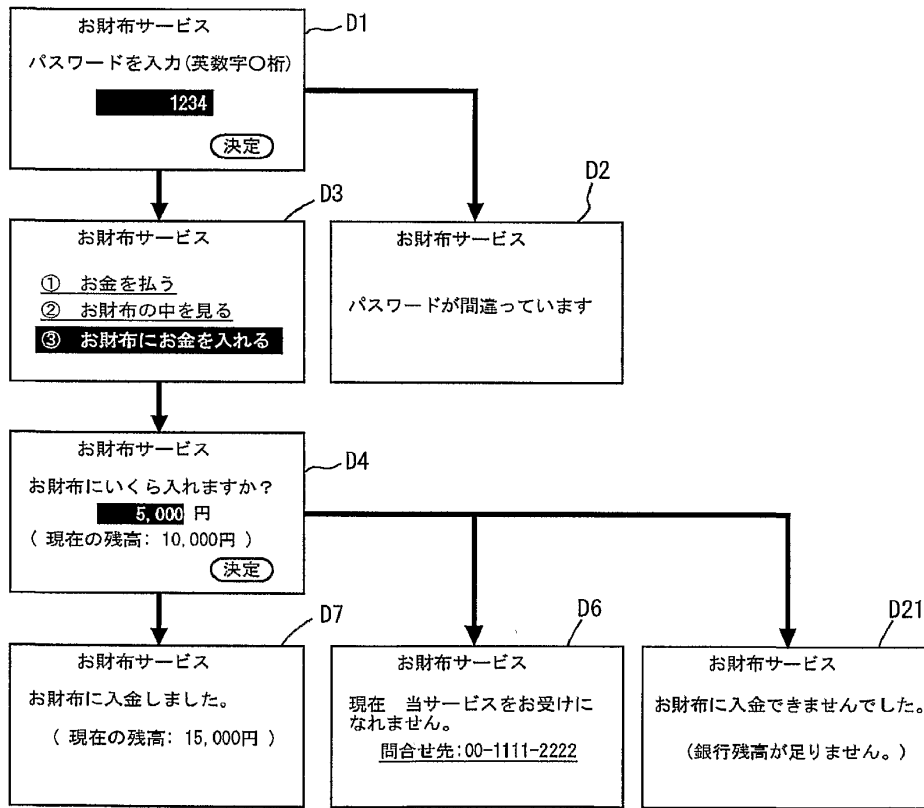


FIG. 30

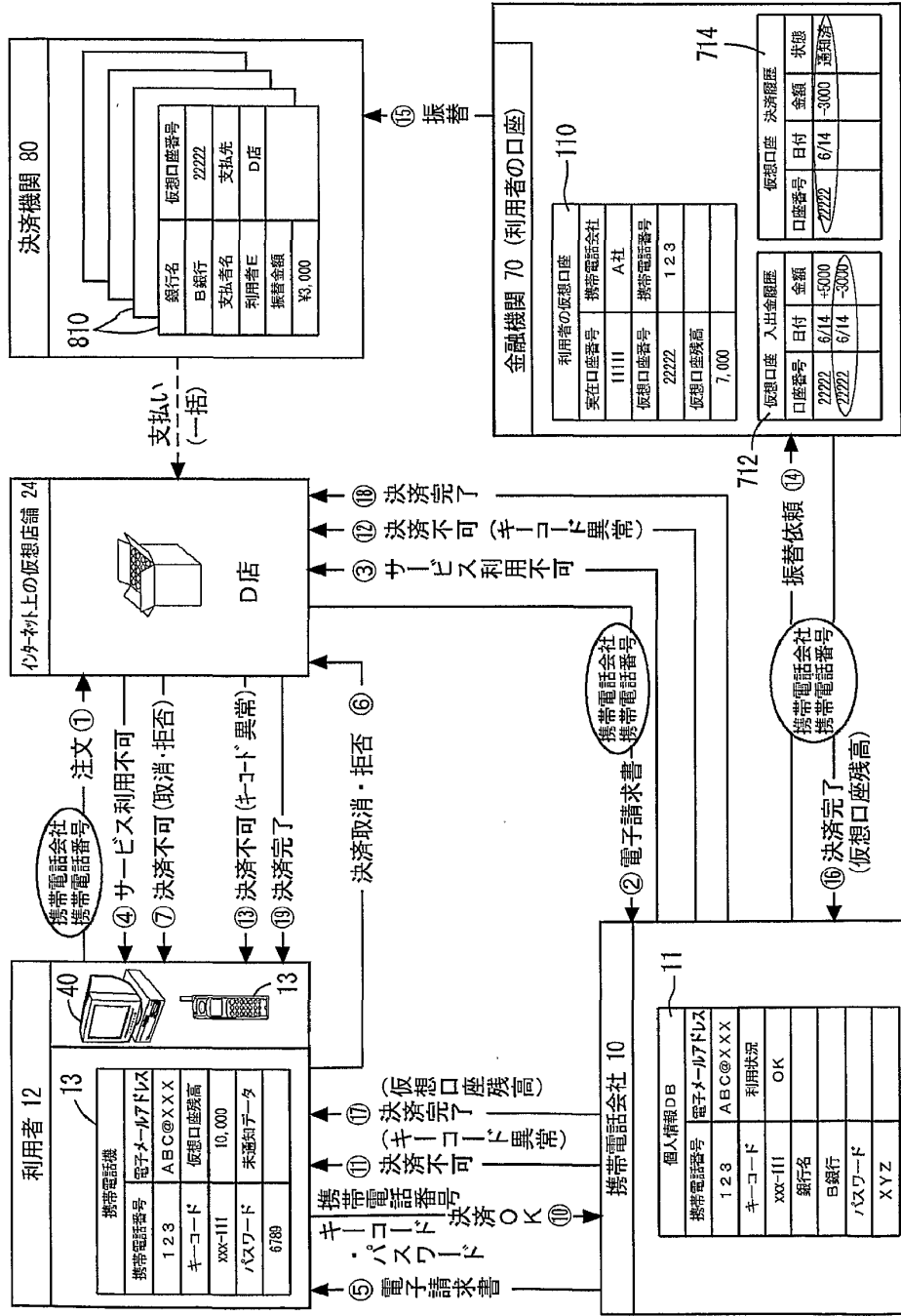


FIG. 31

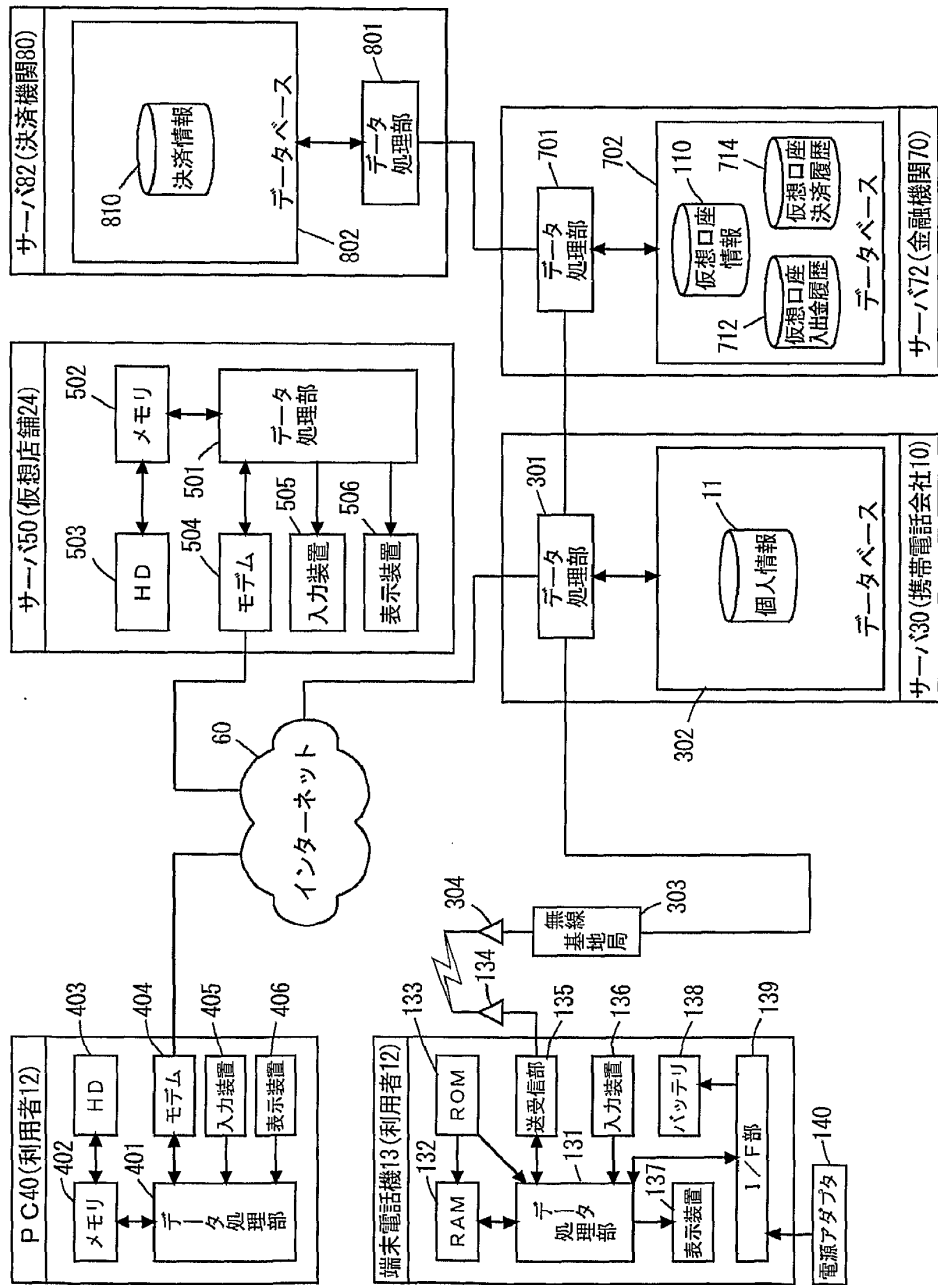


FIG. 32

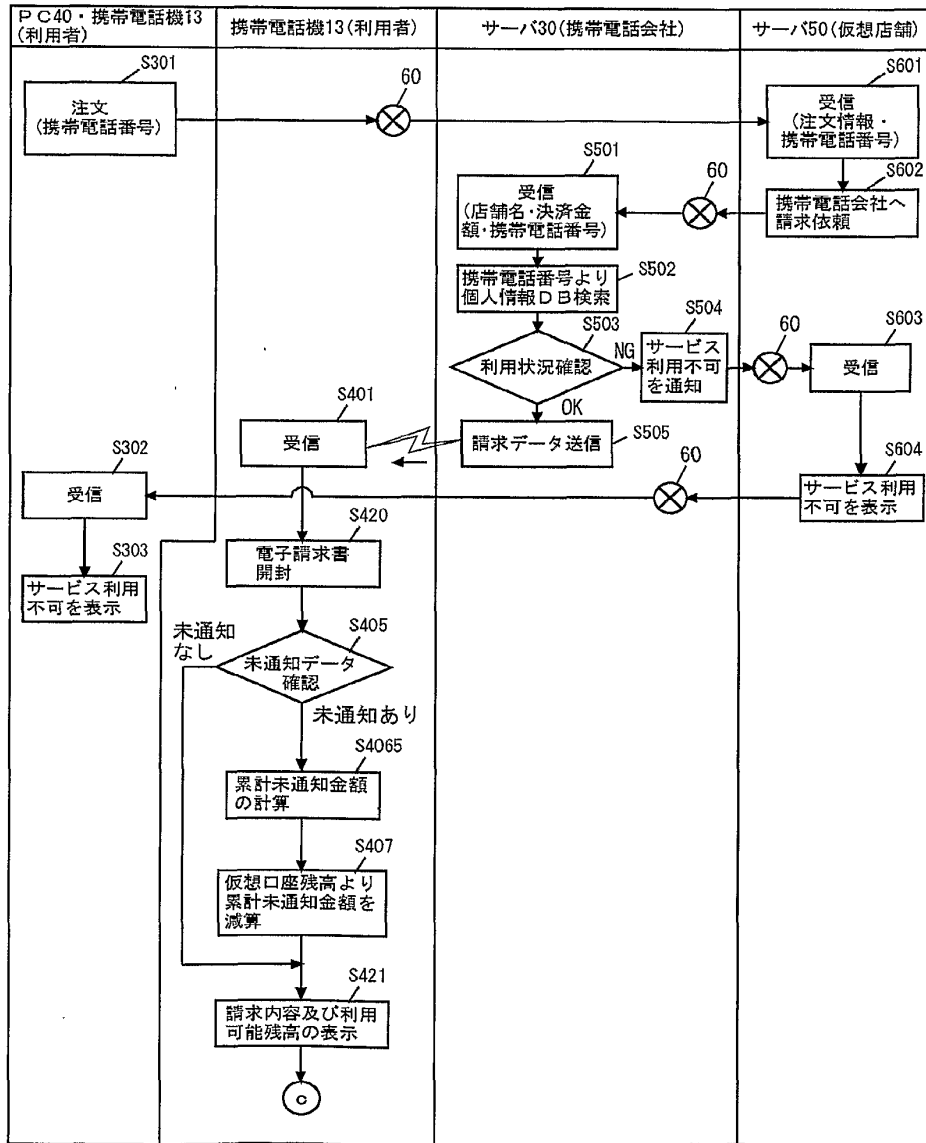


FIG. 33

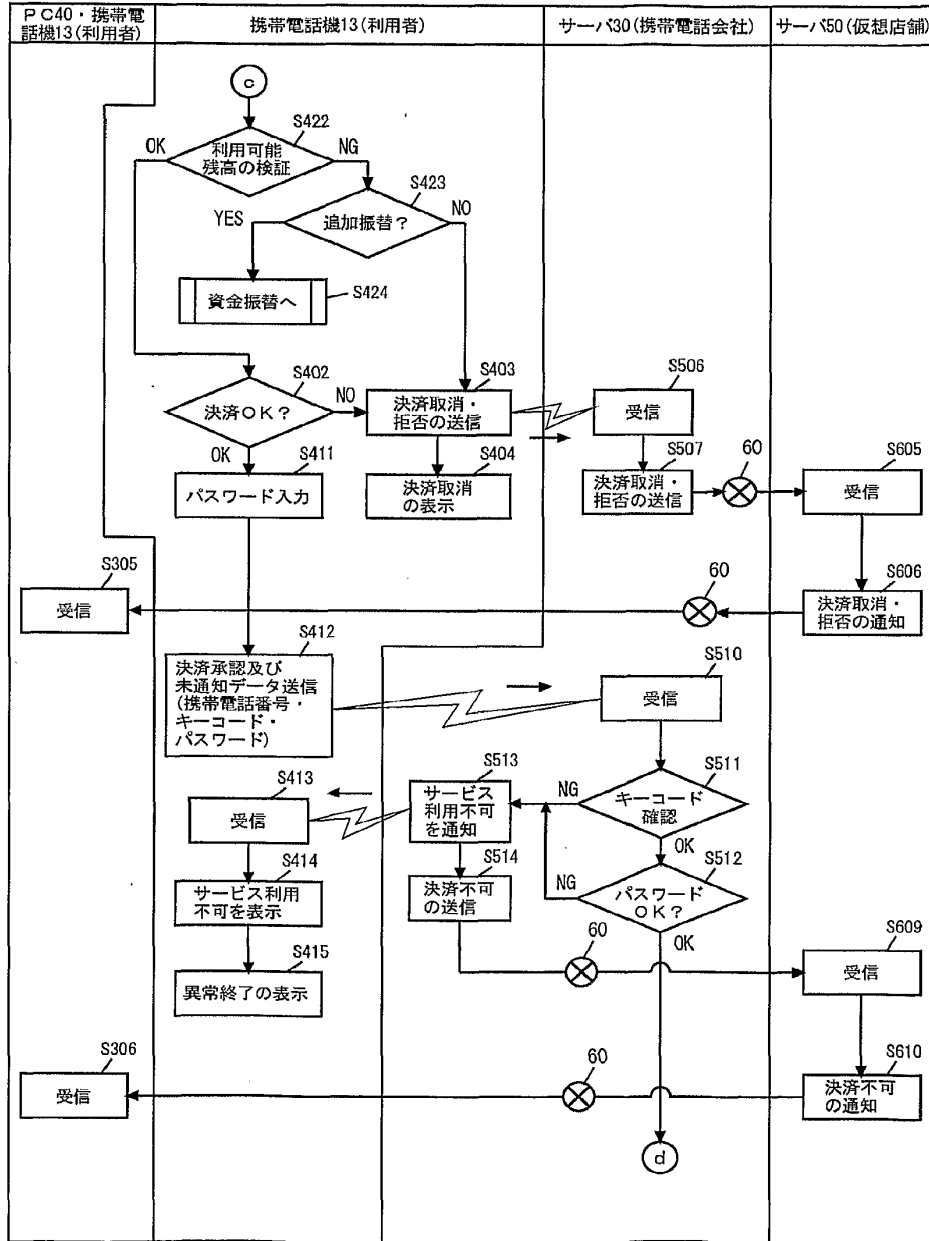


FIG. 34

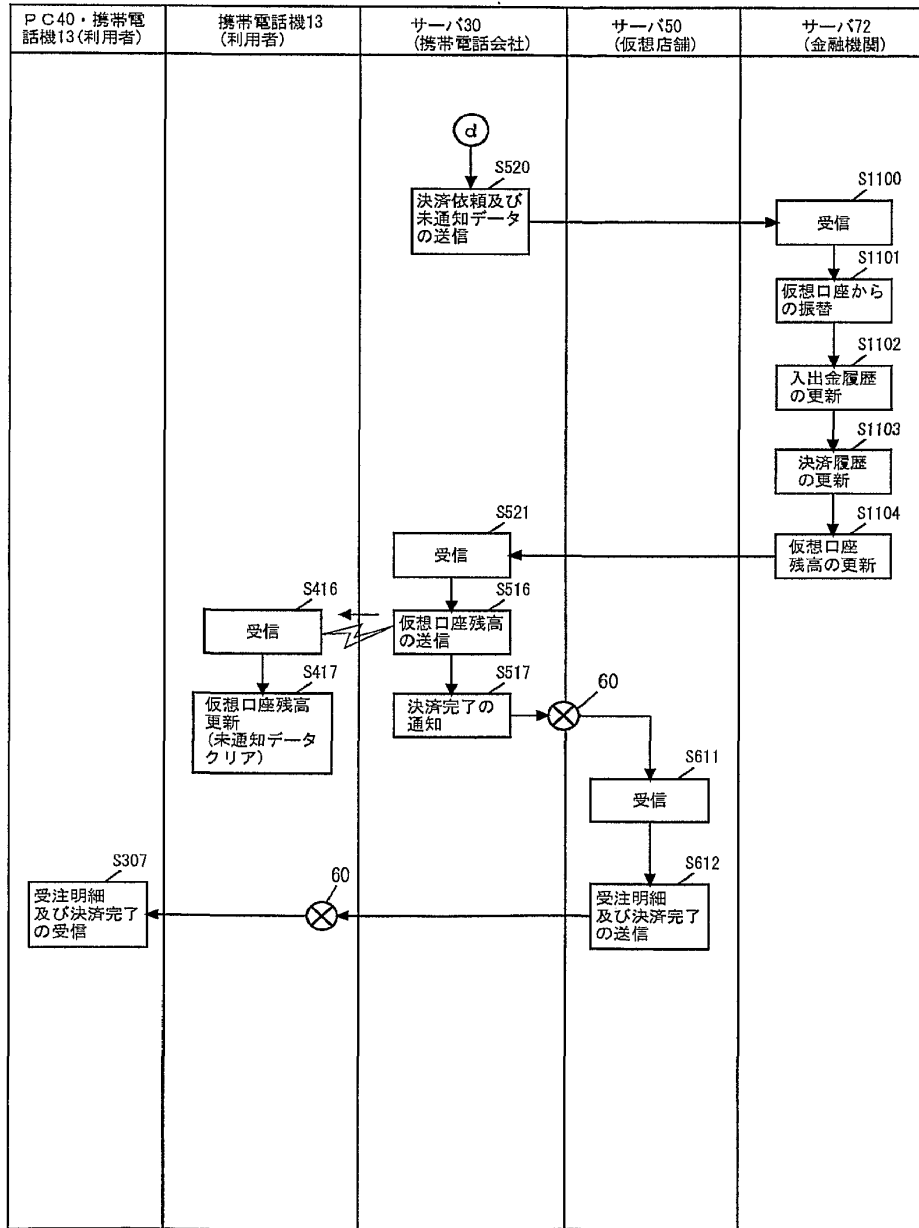


FIG. 35

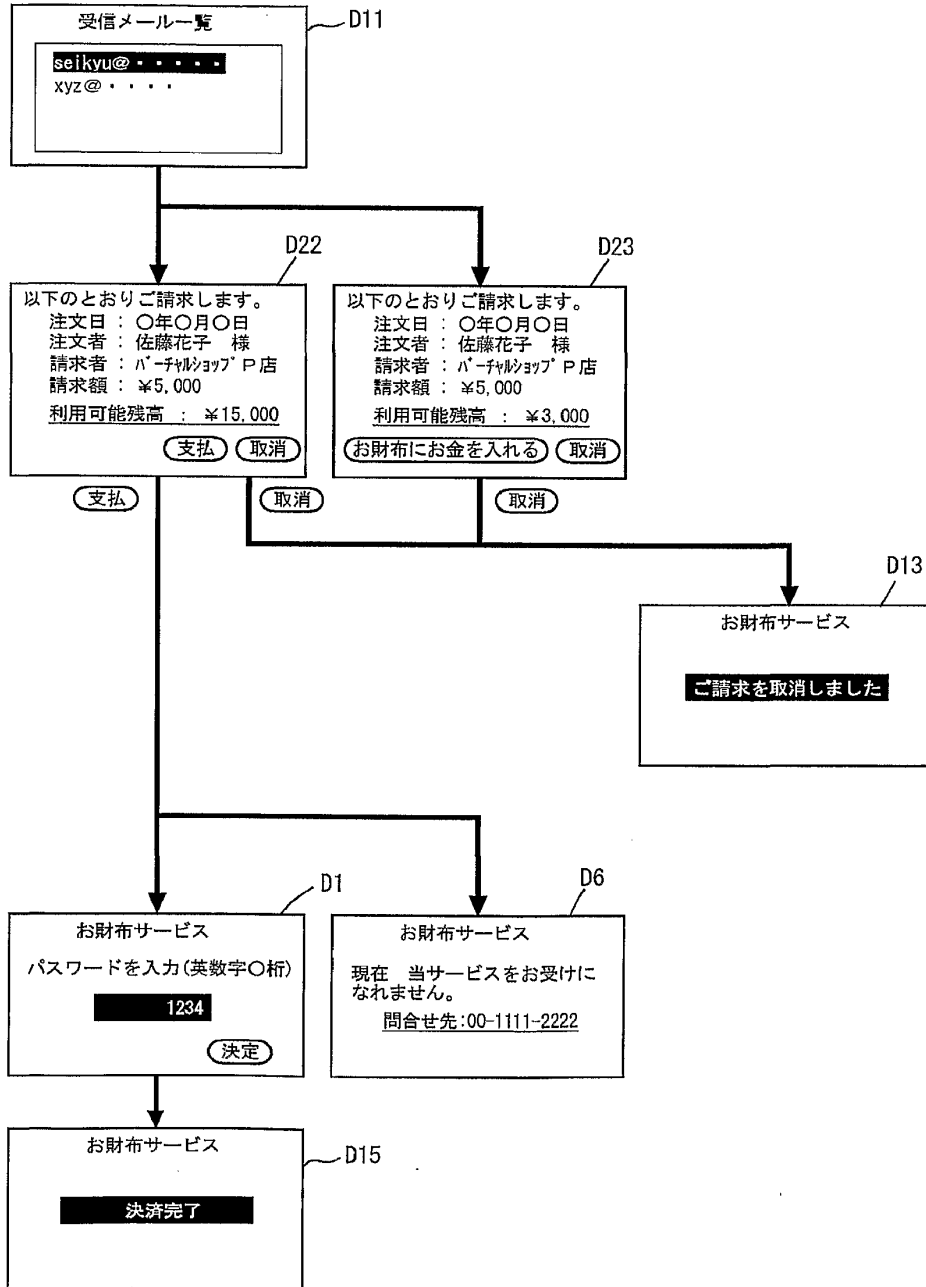


FIG. 36

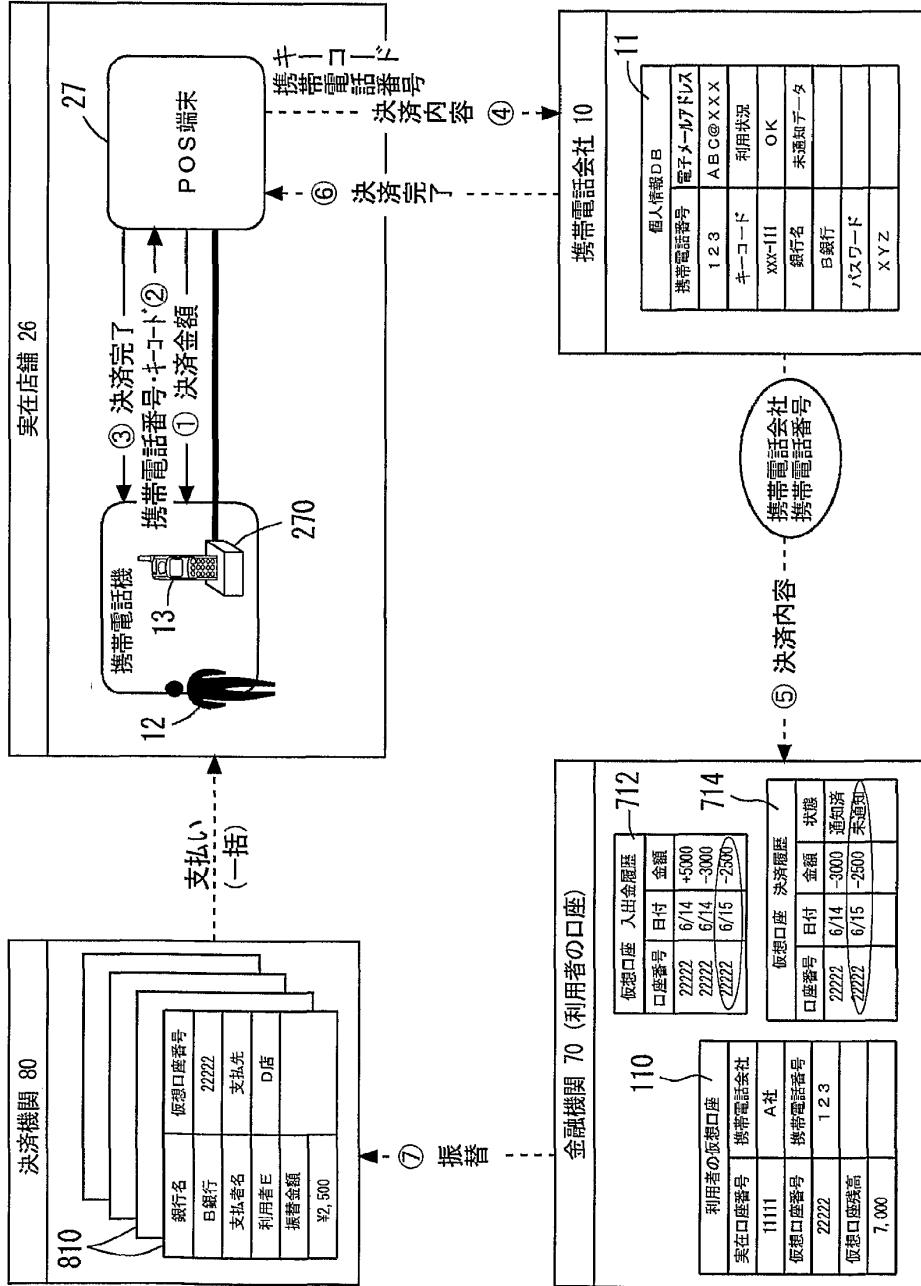


FIG. 37

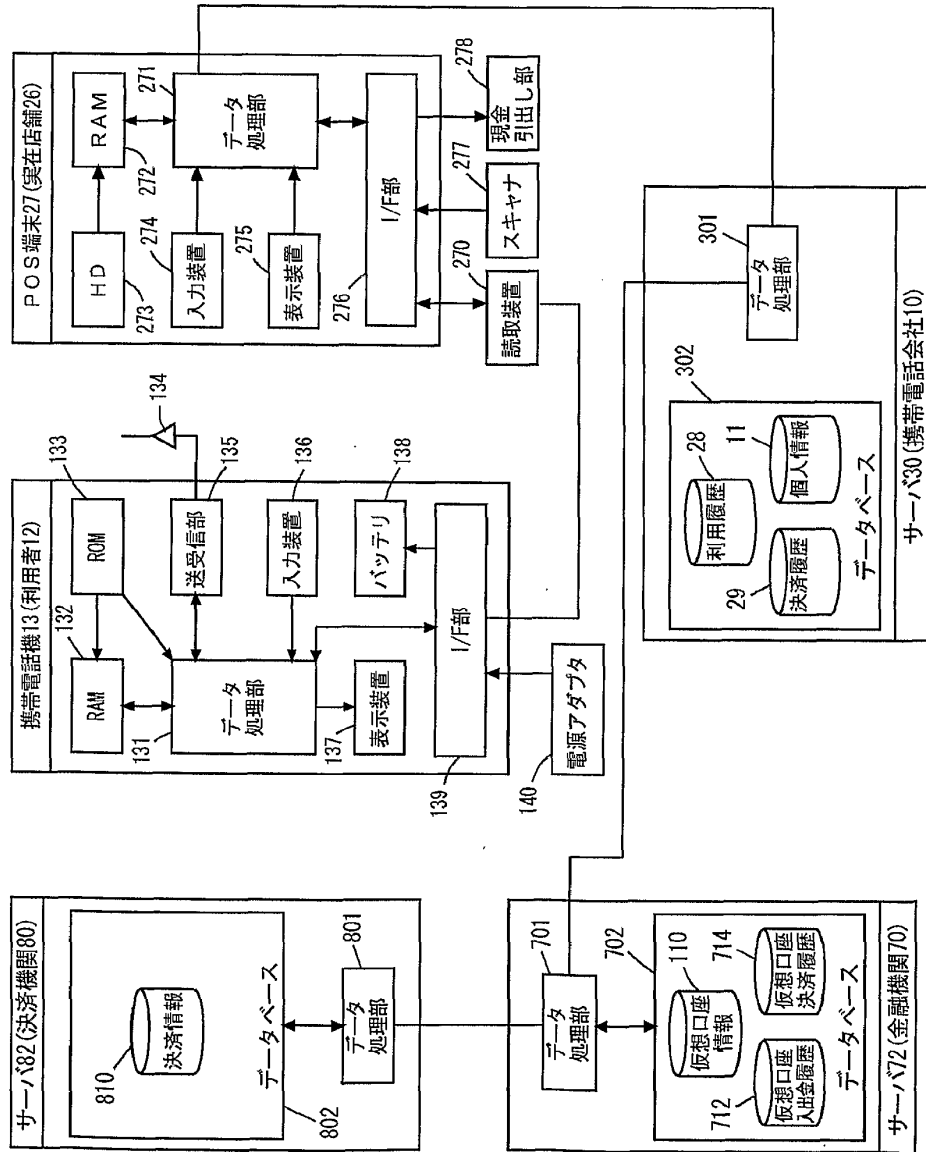


FIG. 38

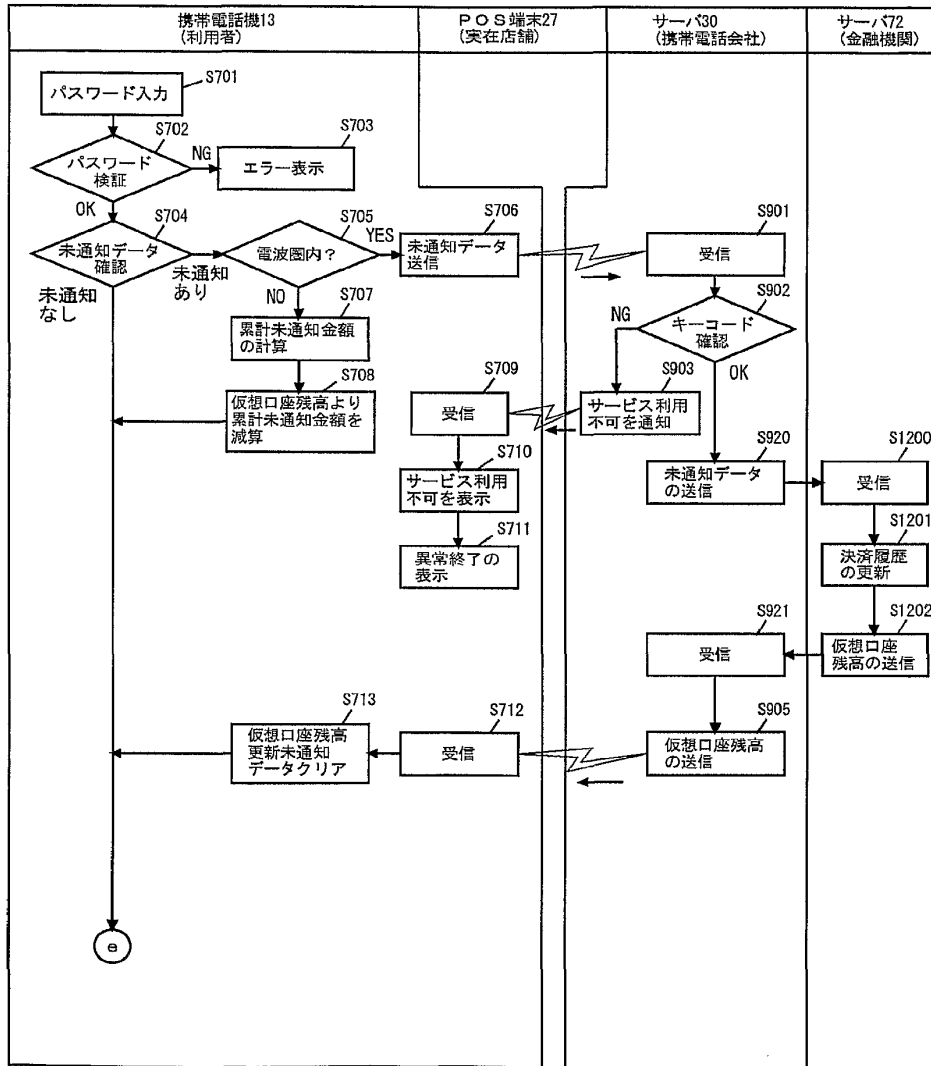


FIG. 39

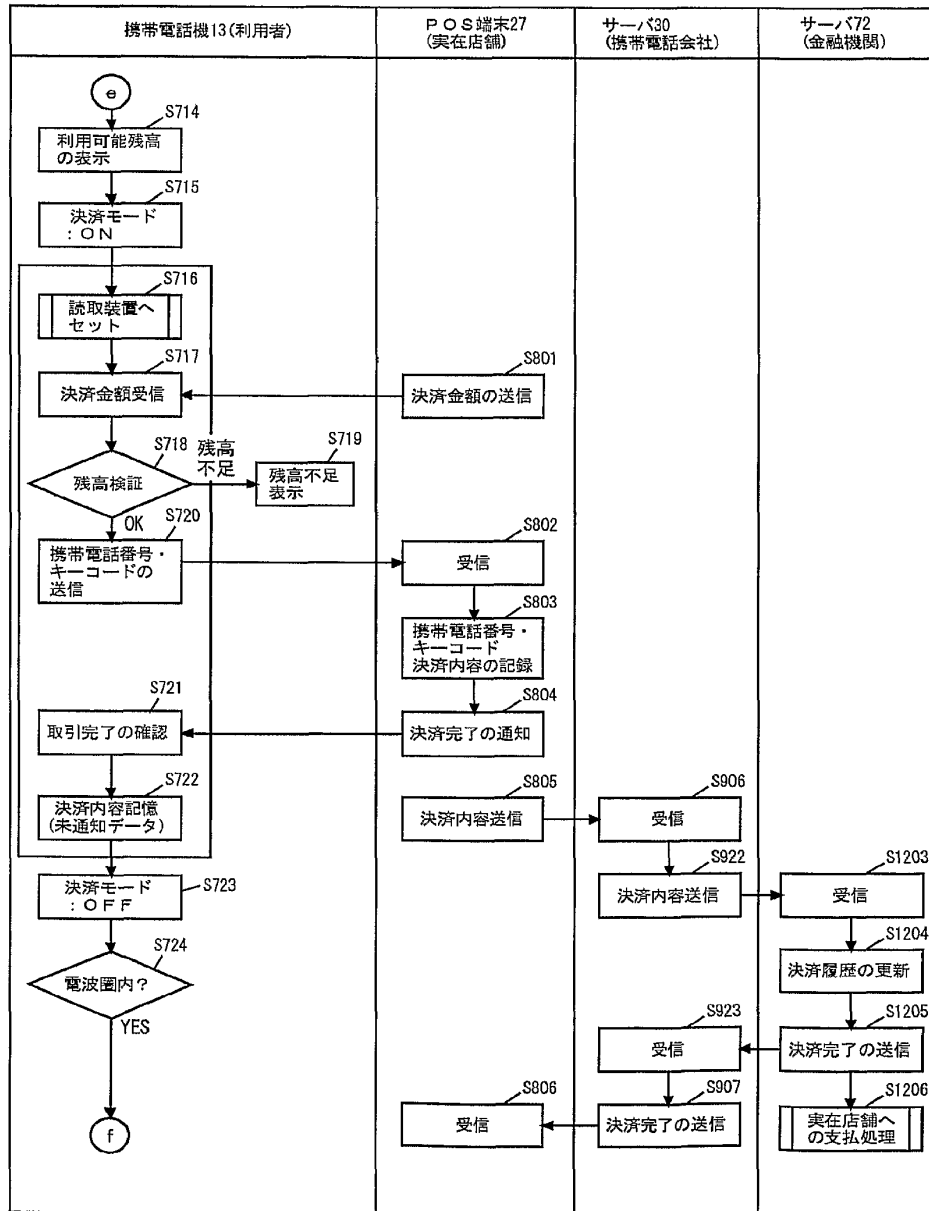


FIG. 40

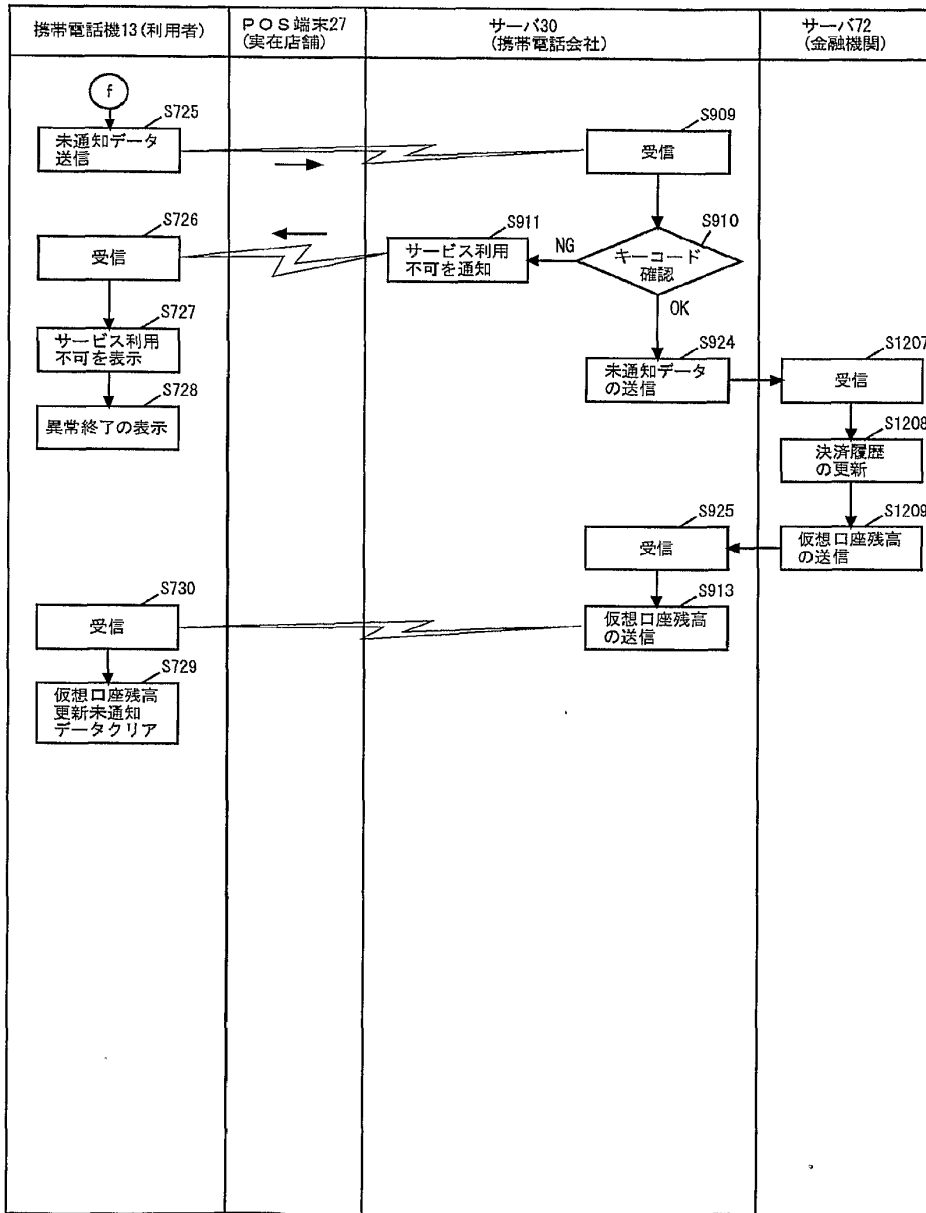


FIG. 41

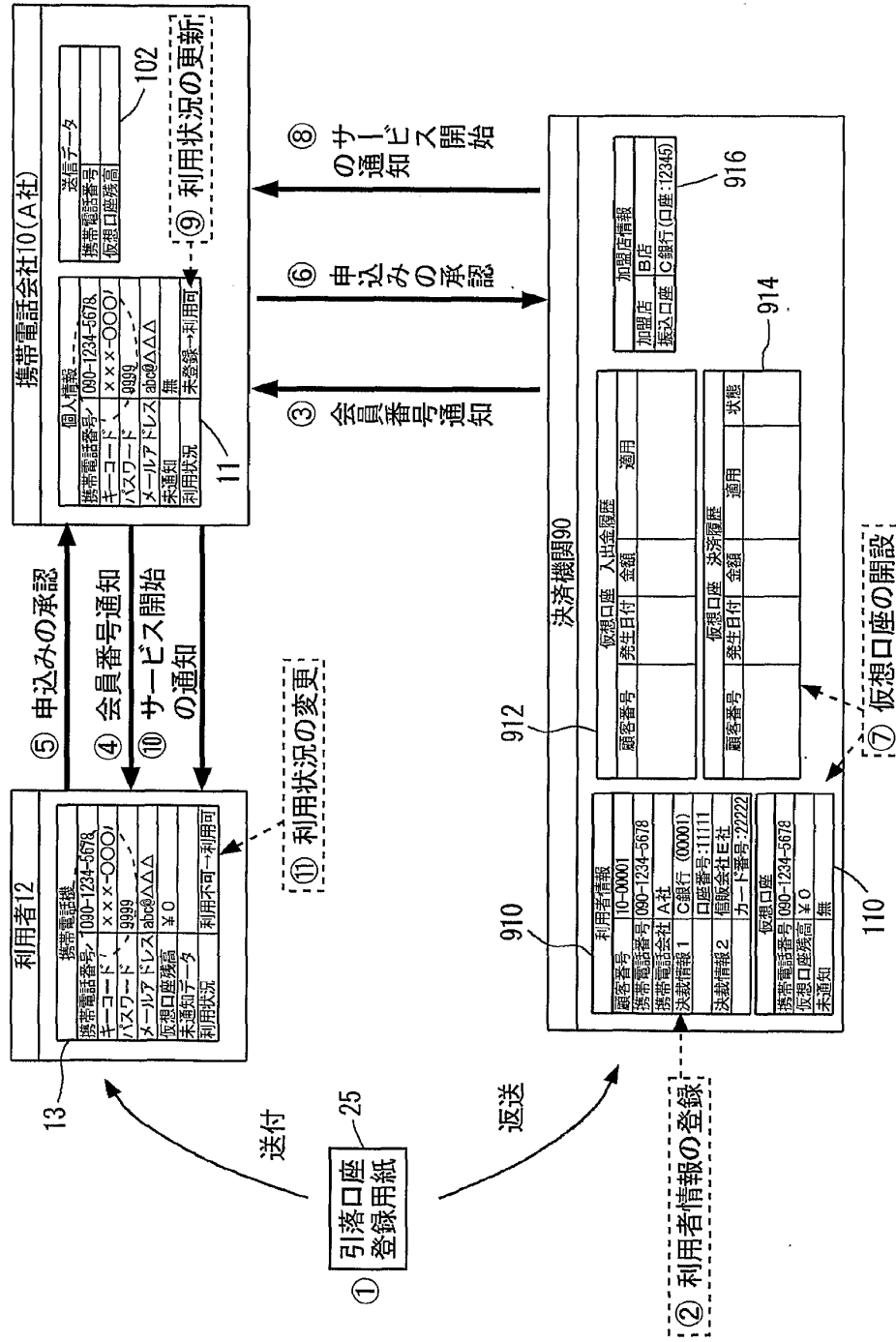


FIG. 42

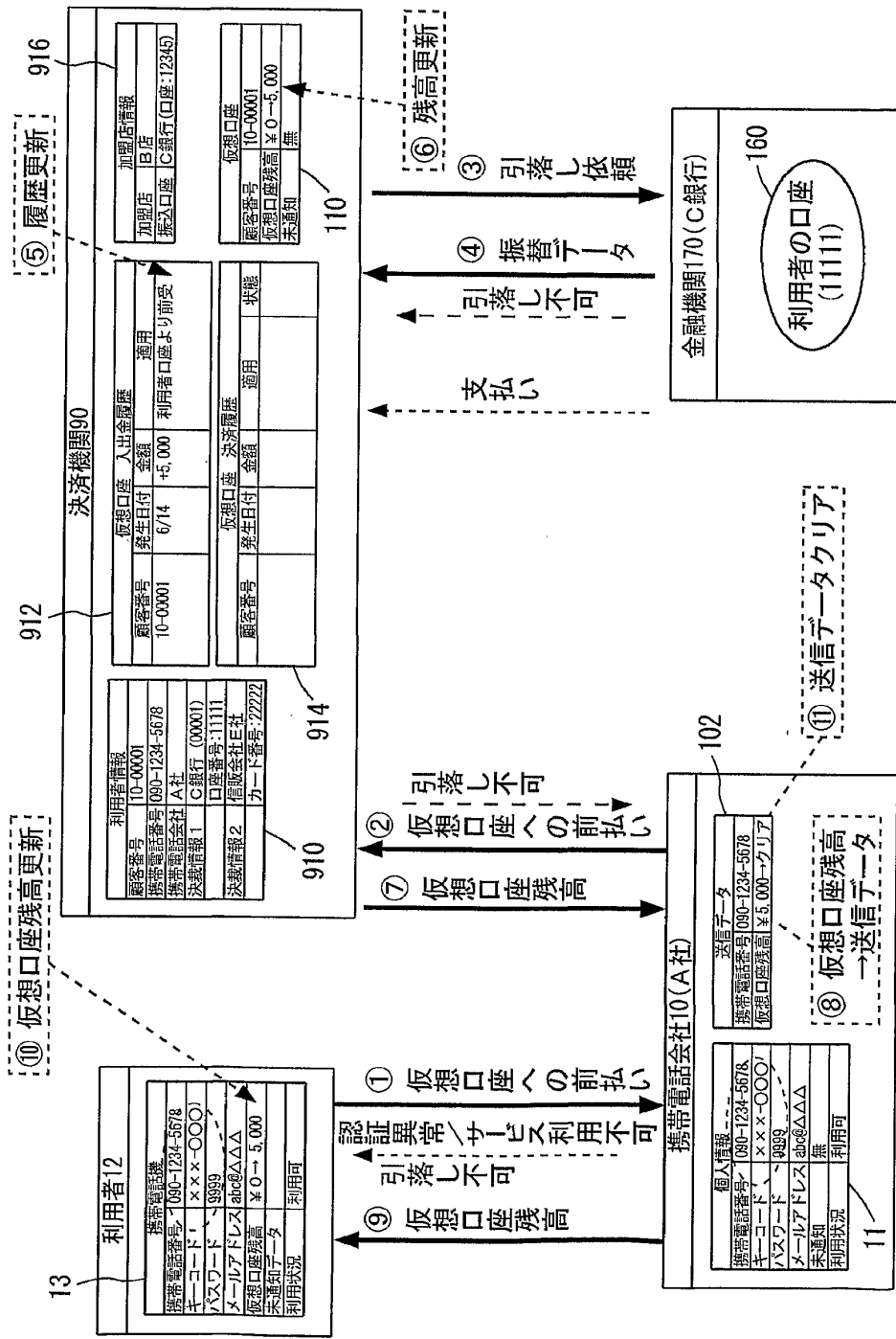


FIG. 43

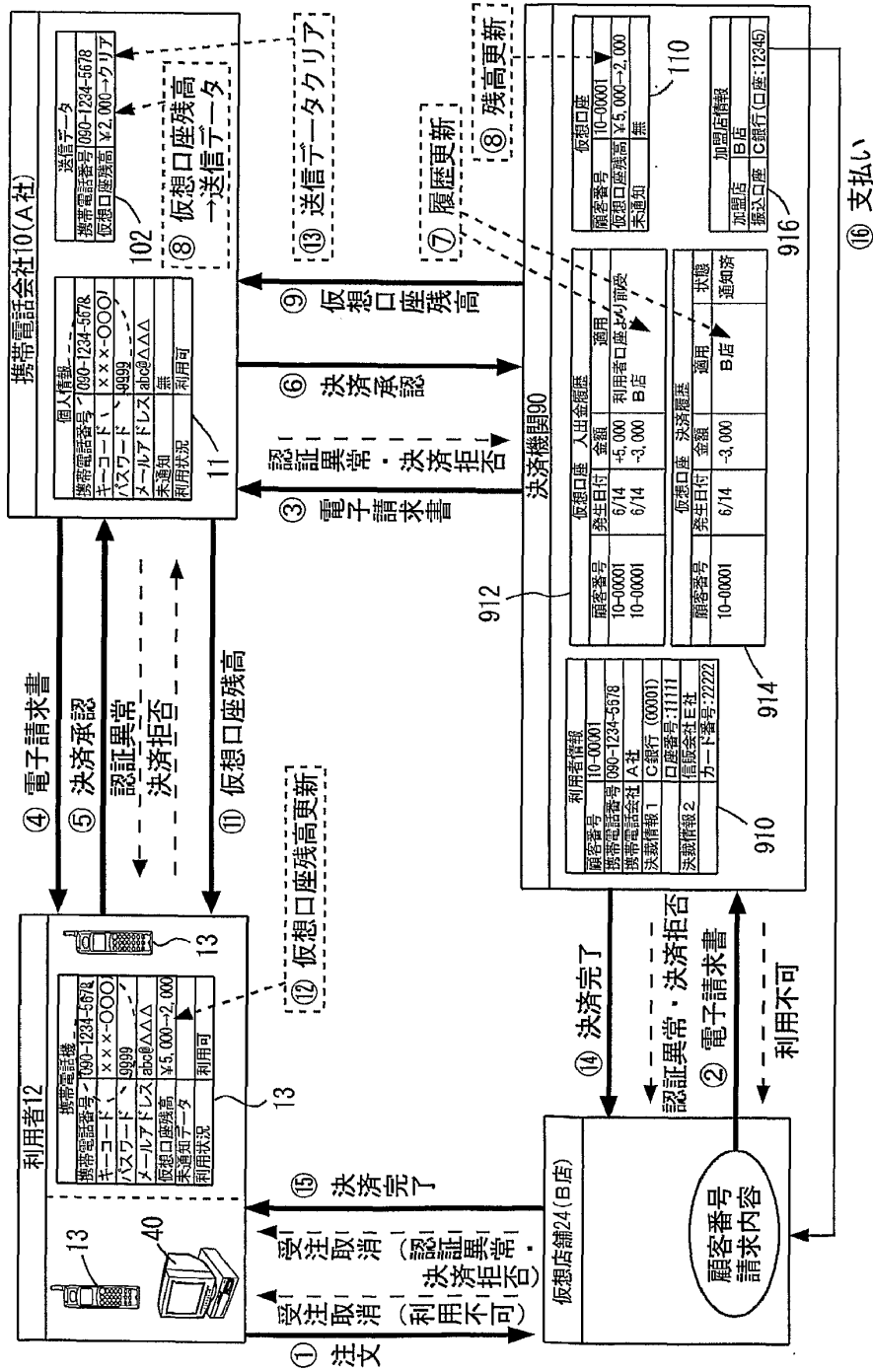


FIG. 44

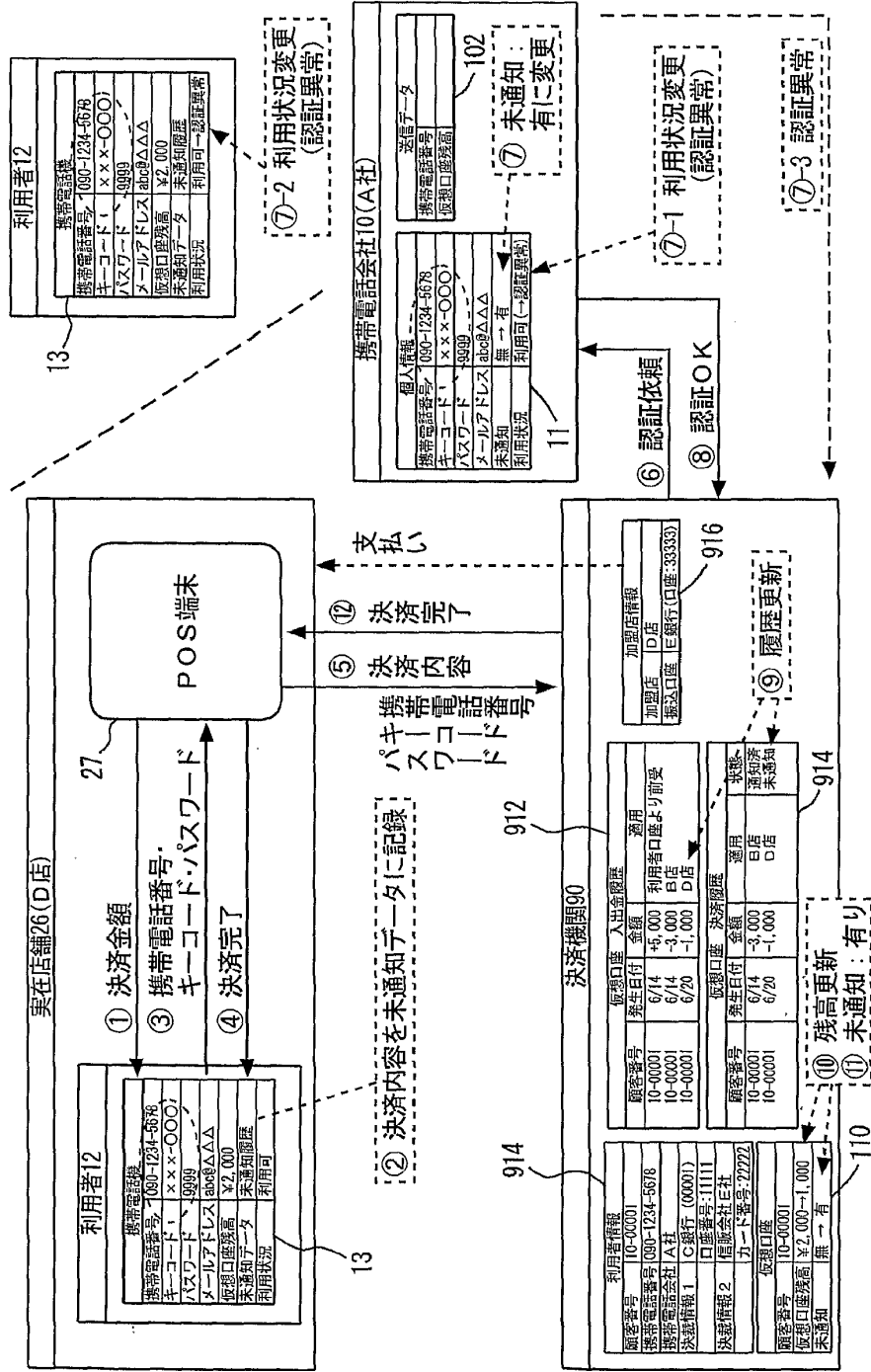


FIG. 45

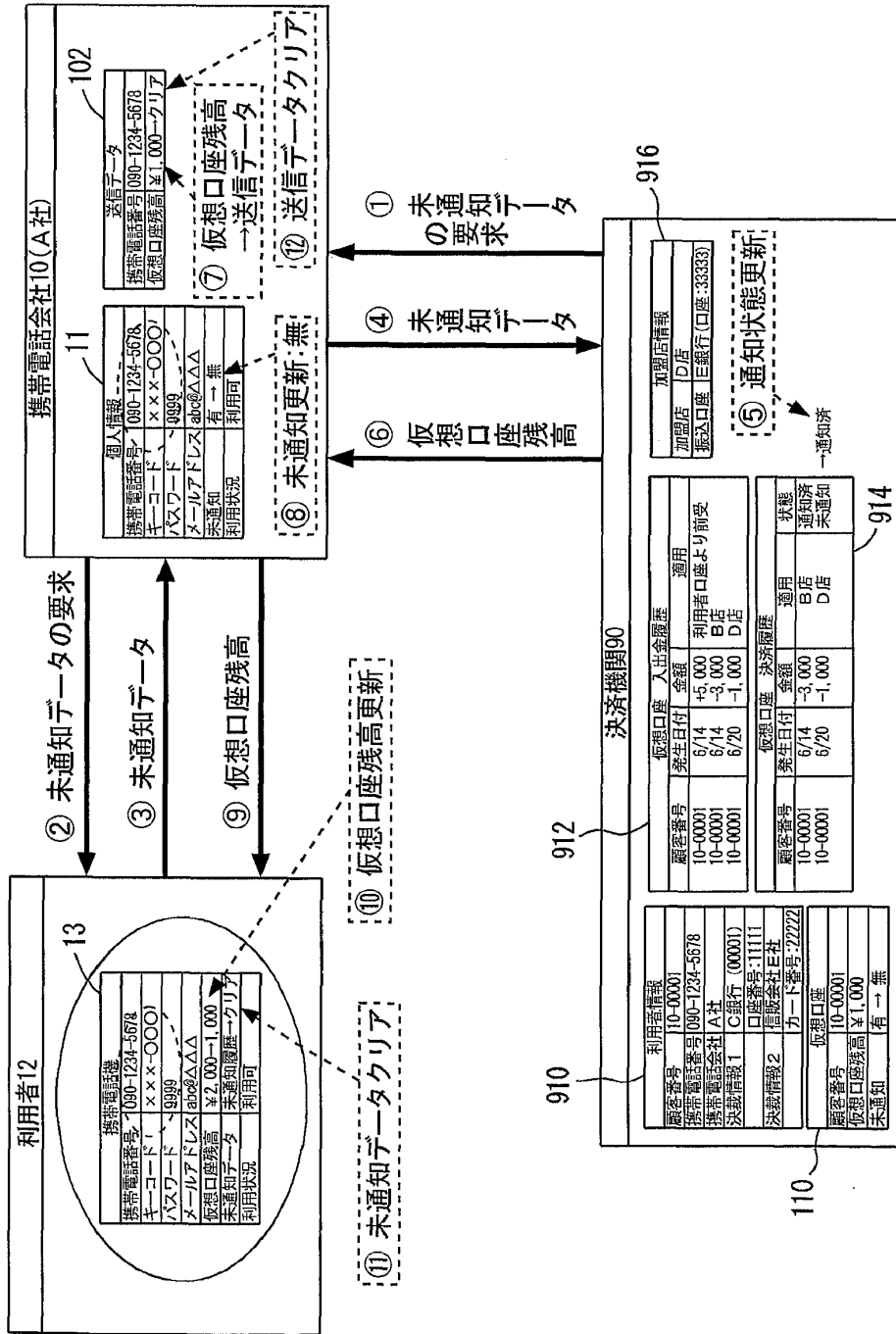


FIG. 46

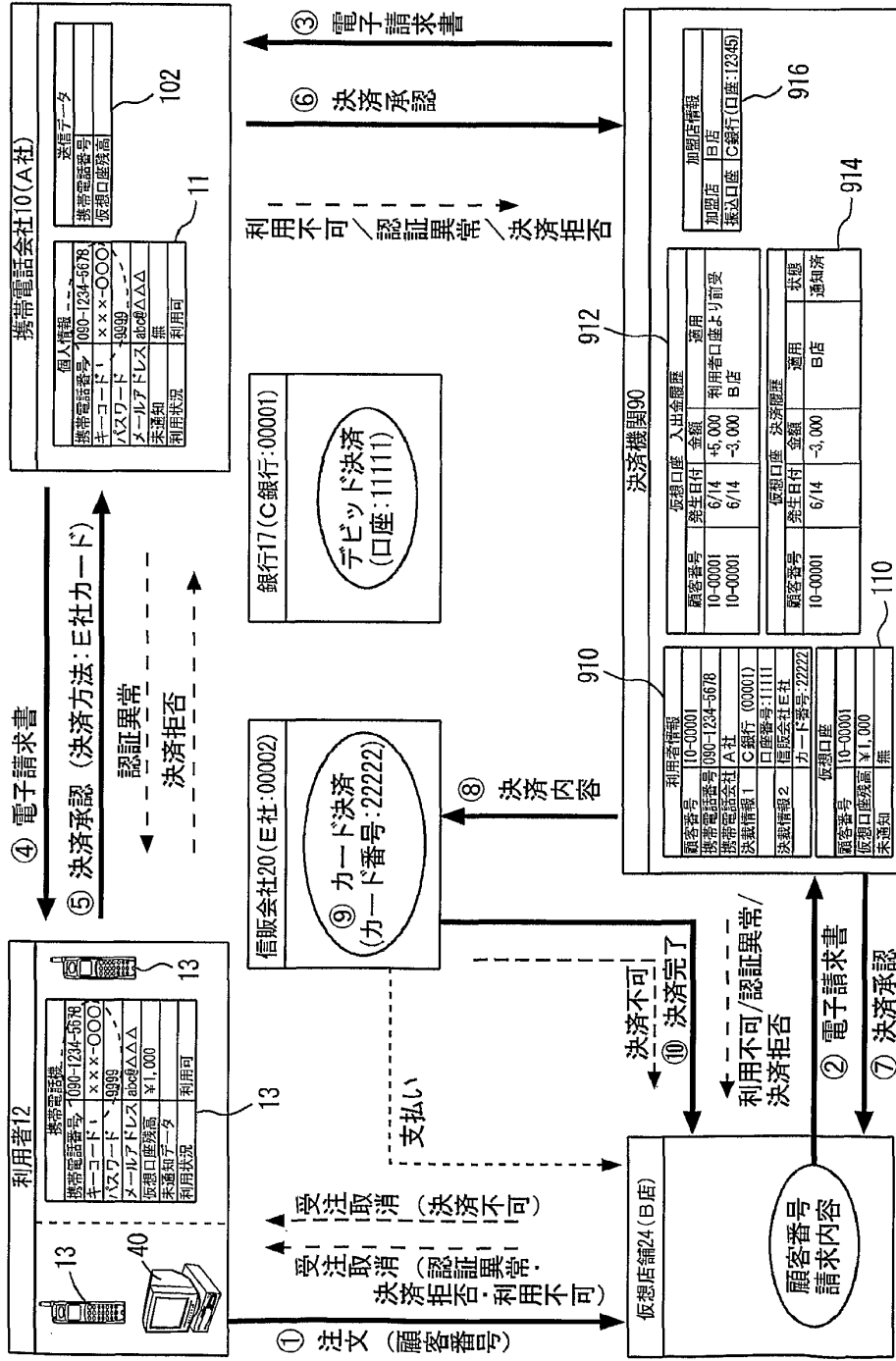


FIG. 47

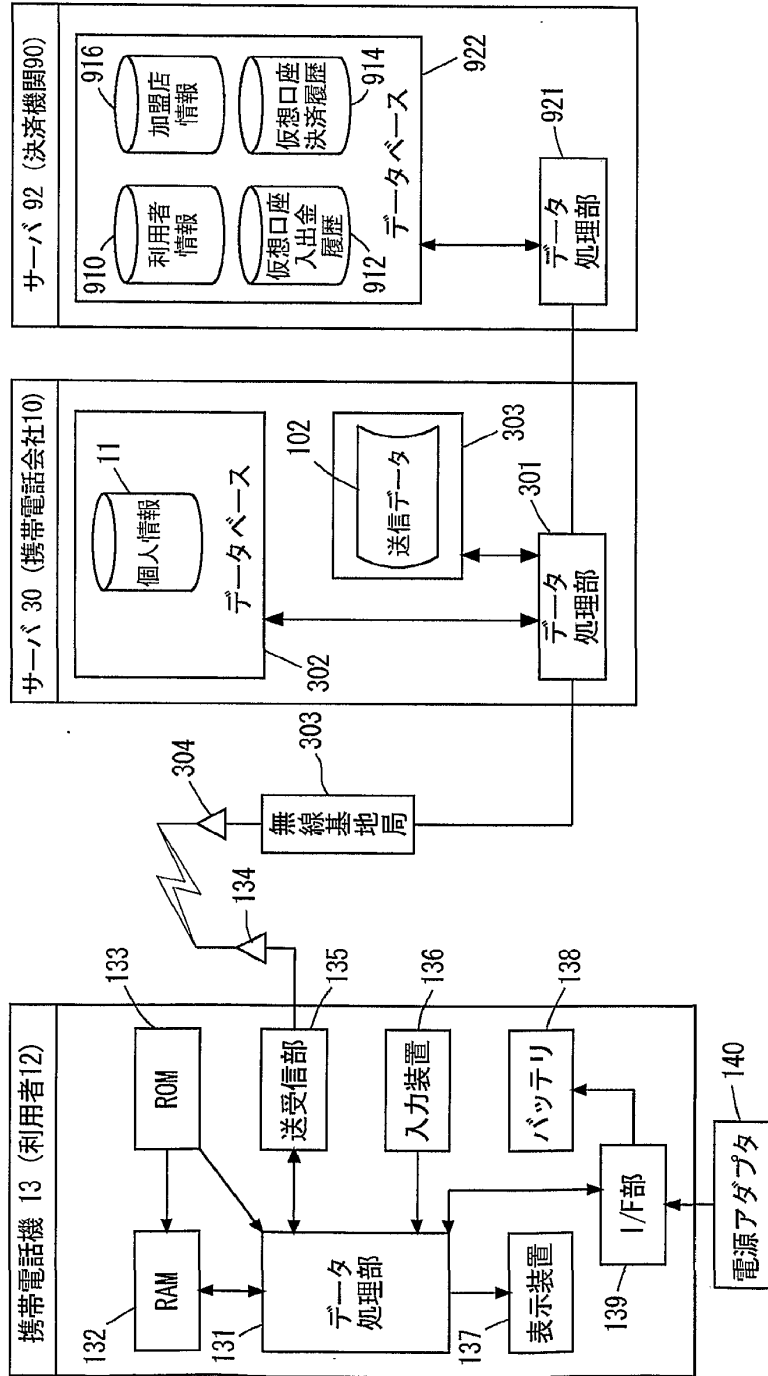


FIG. 48

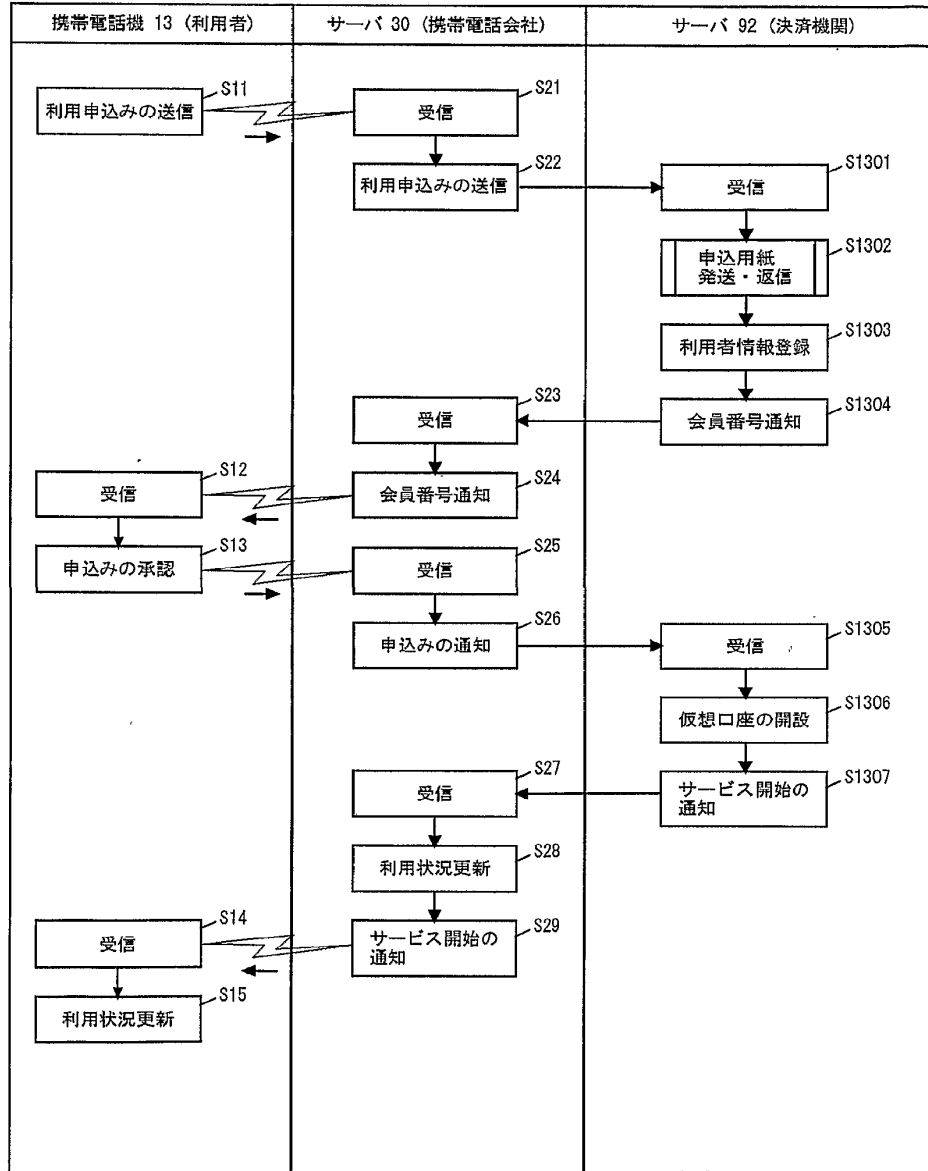


FIG. 49

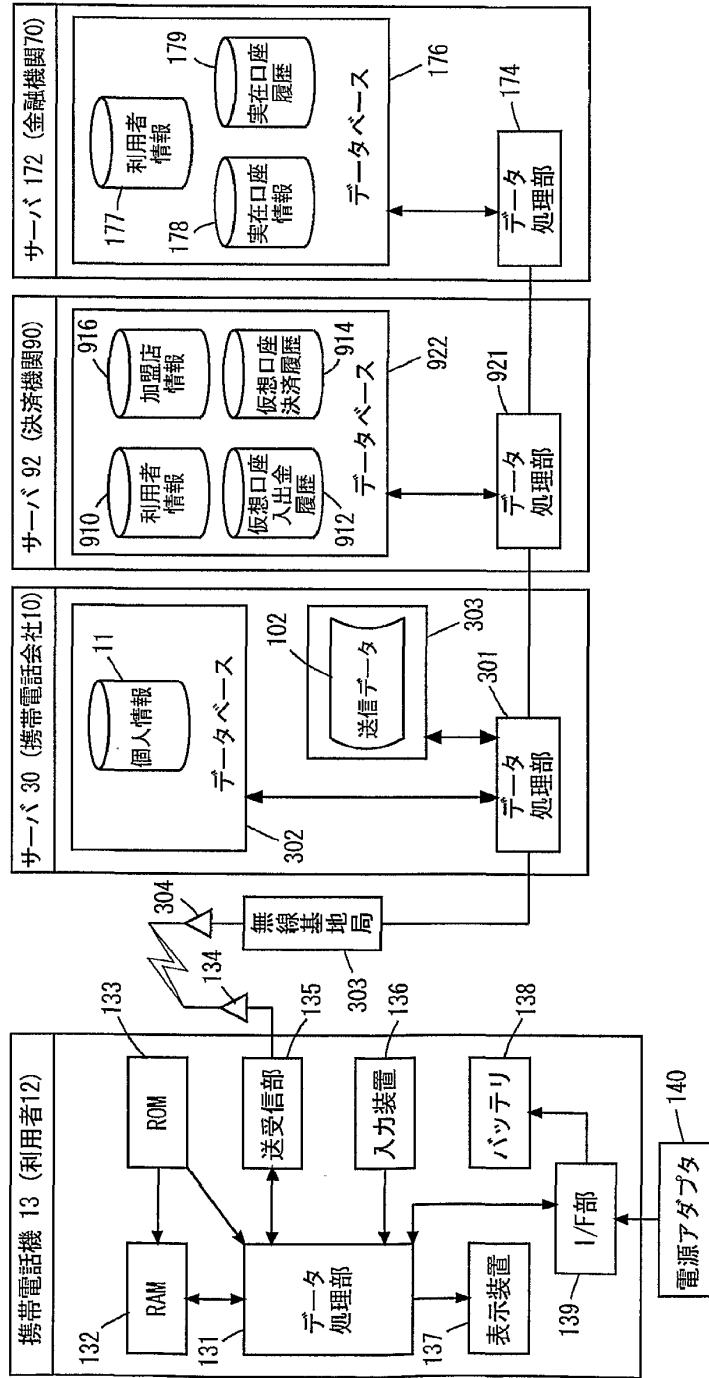


FIG. 50

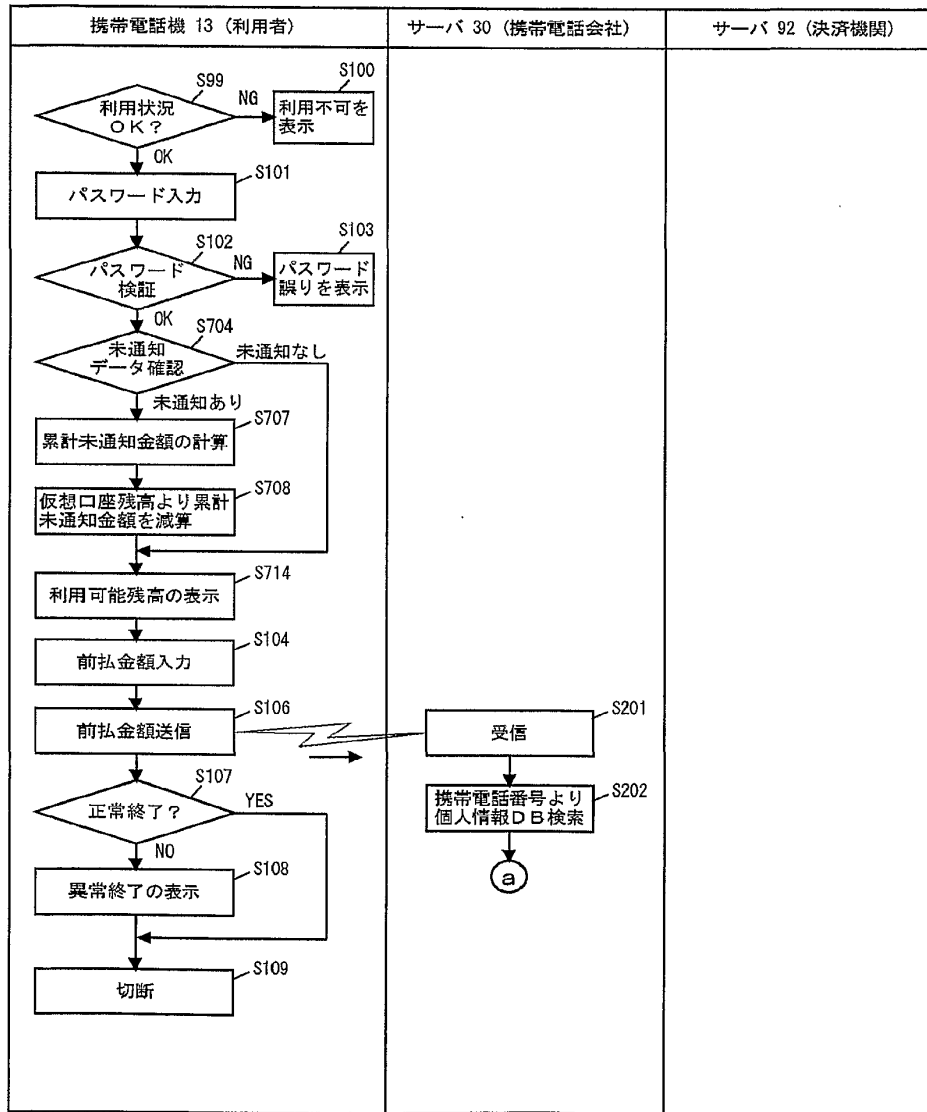


FIG. 51

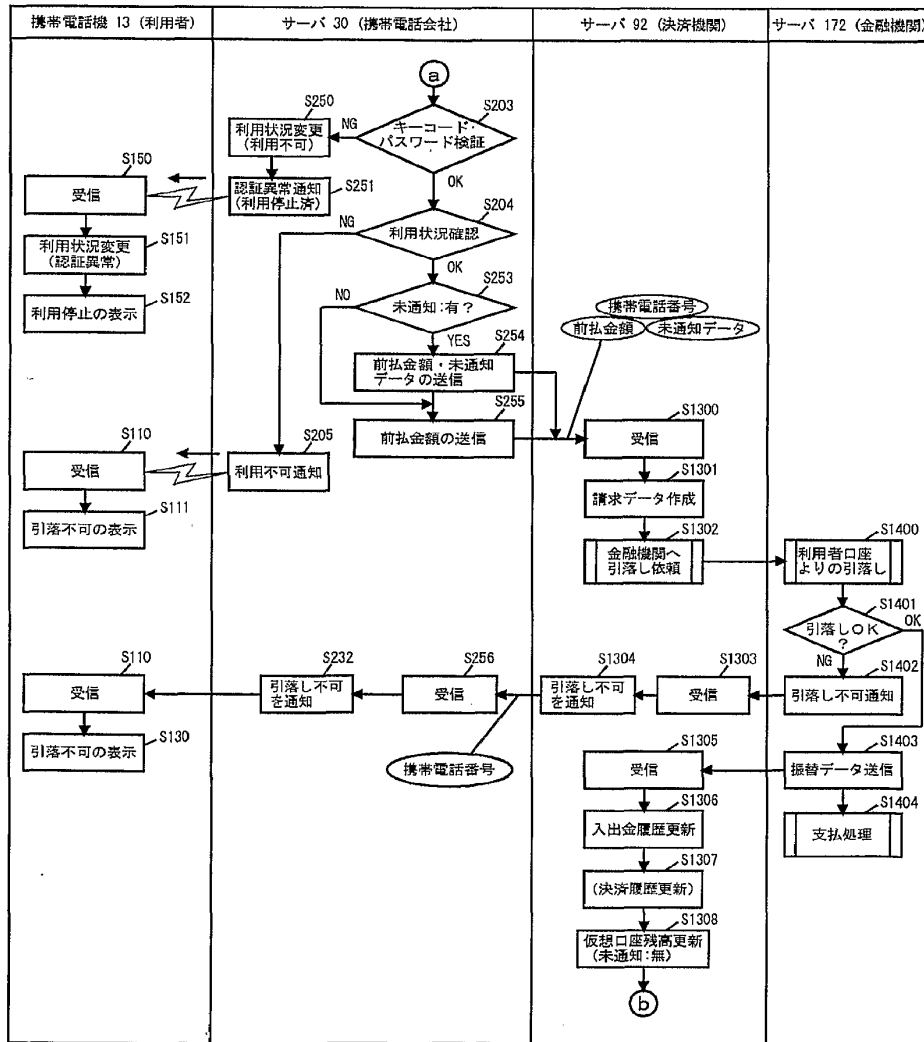


FIG. 52

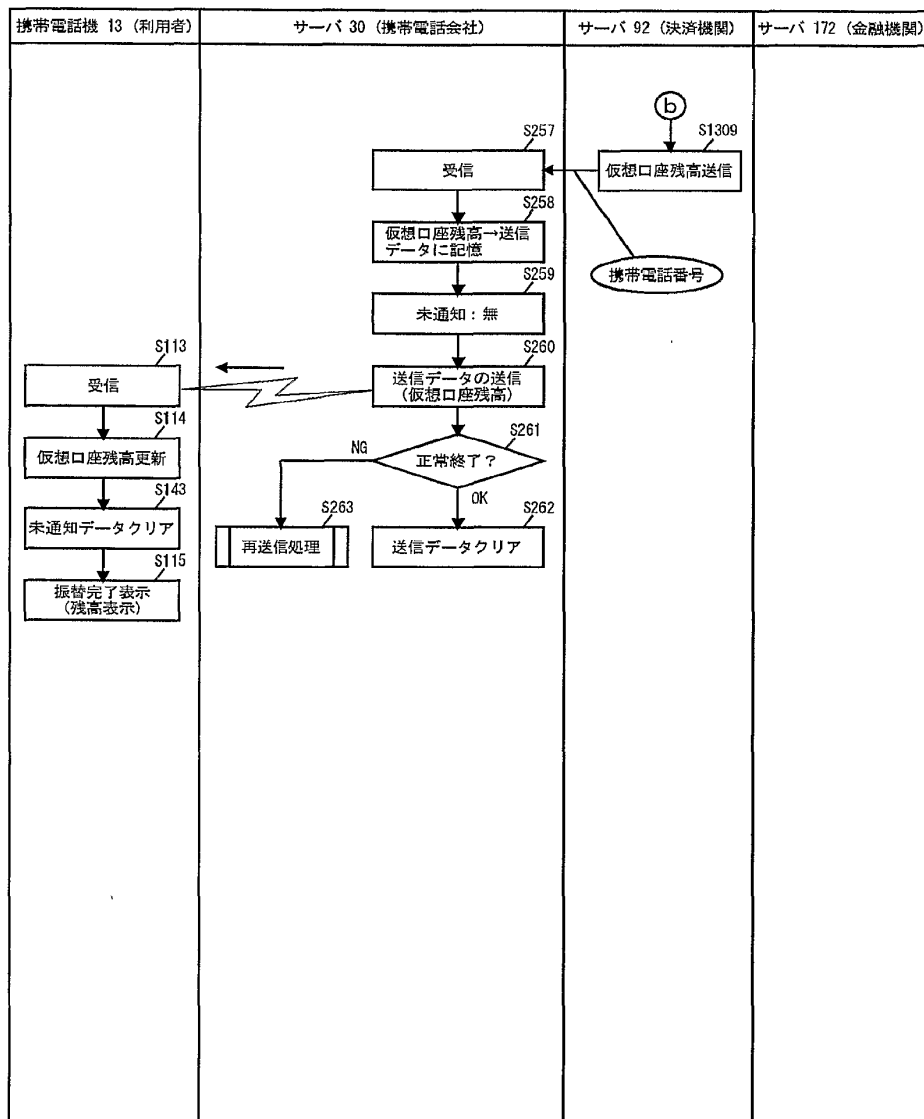


FIG. 53

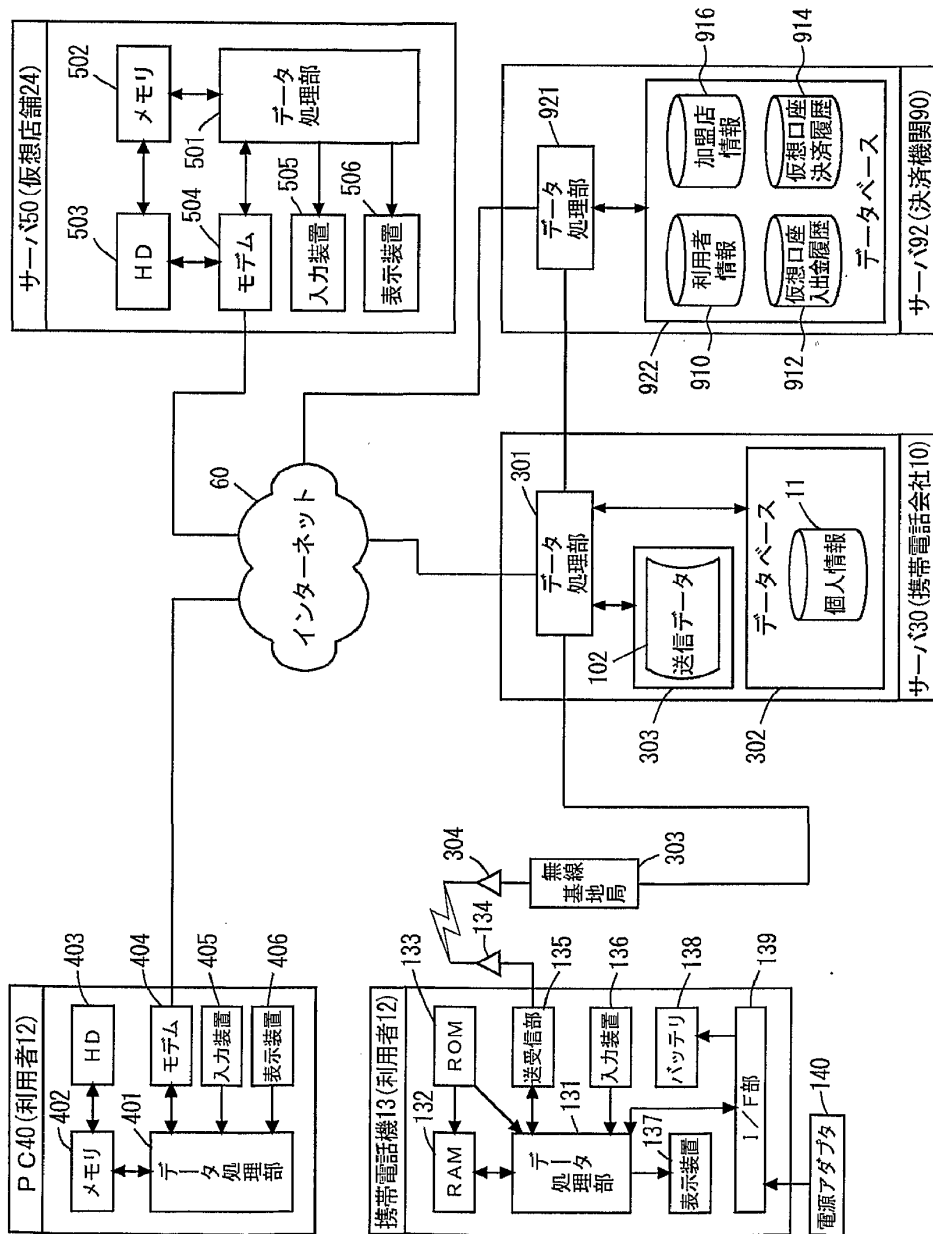


FIG. 54

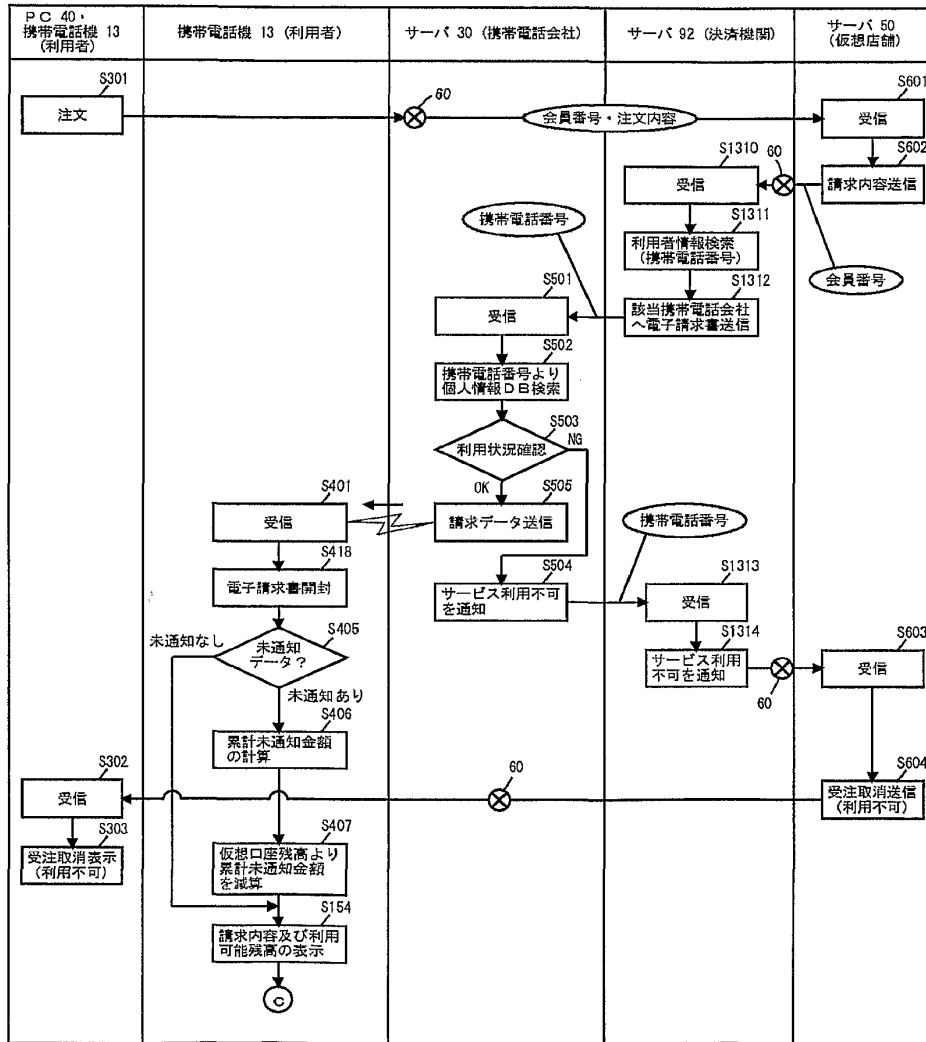


FIG. 55

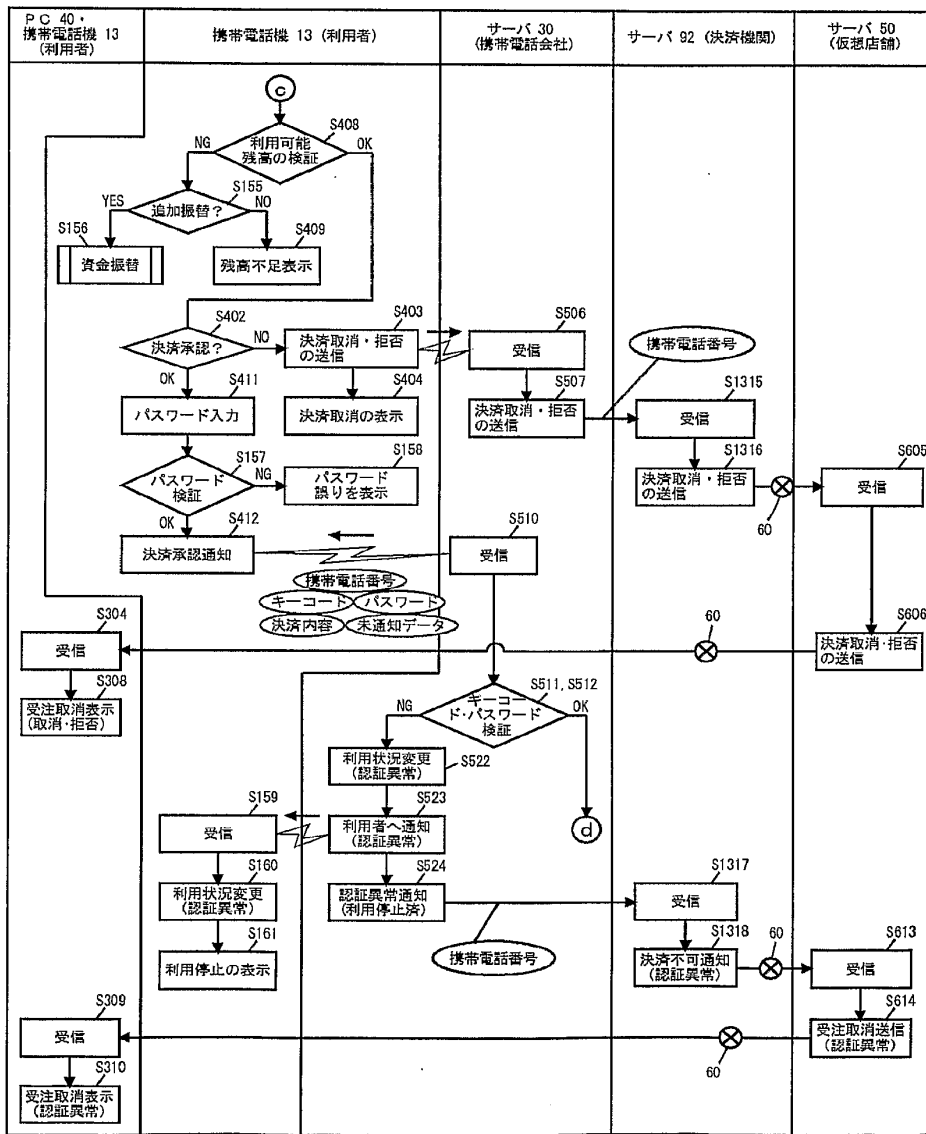


FIG. 56

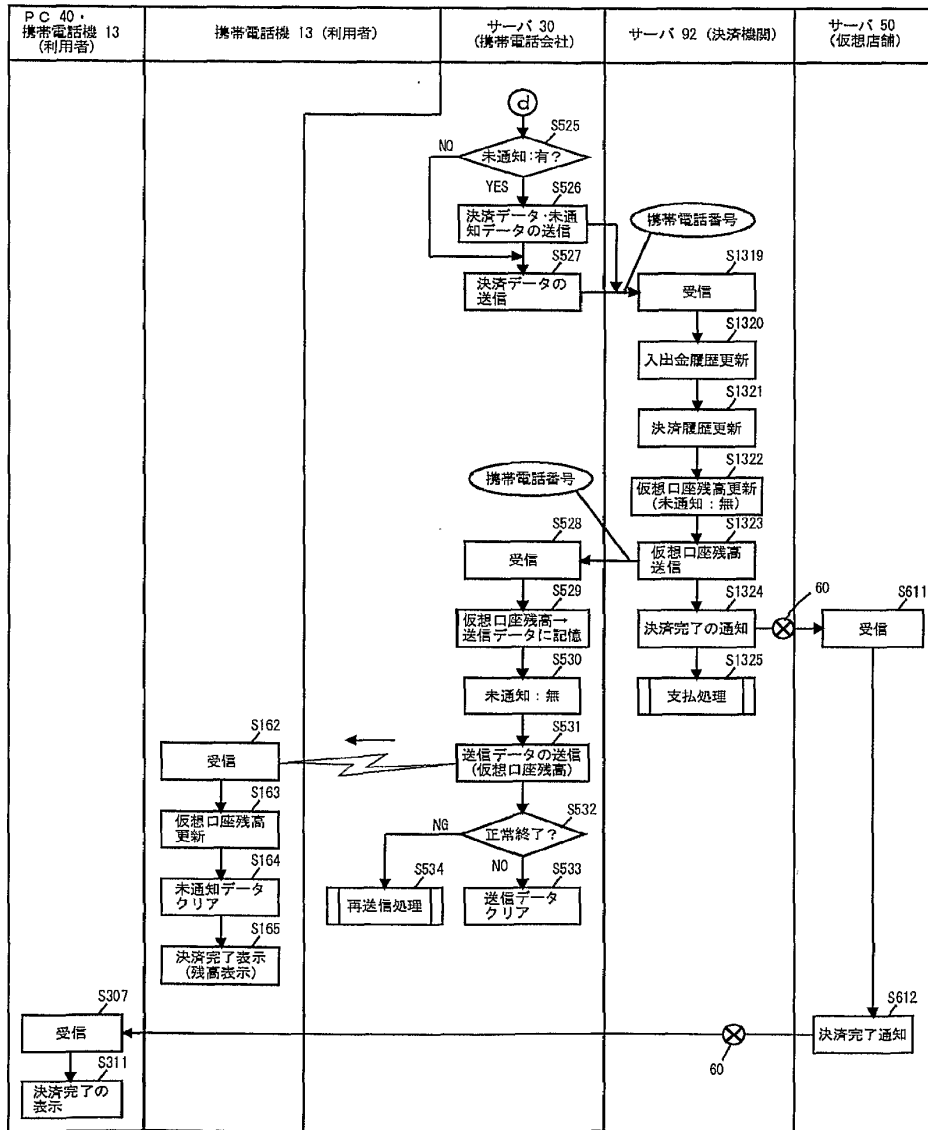


FIG. 57

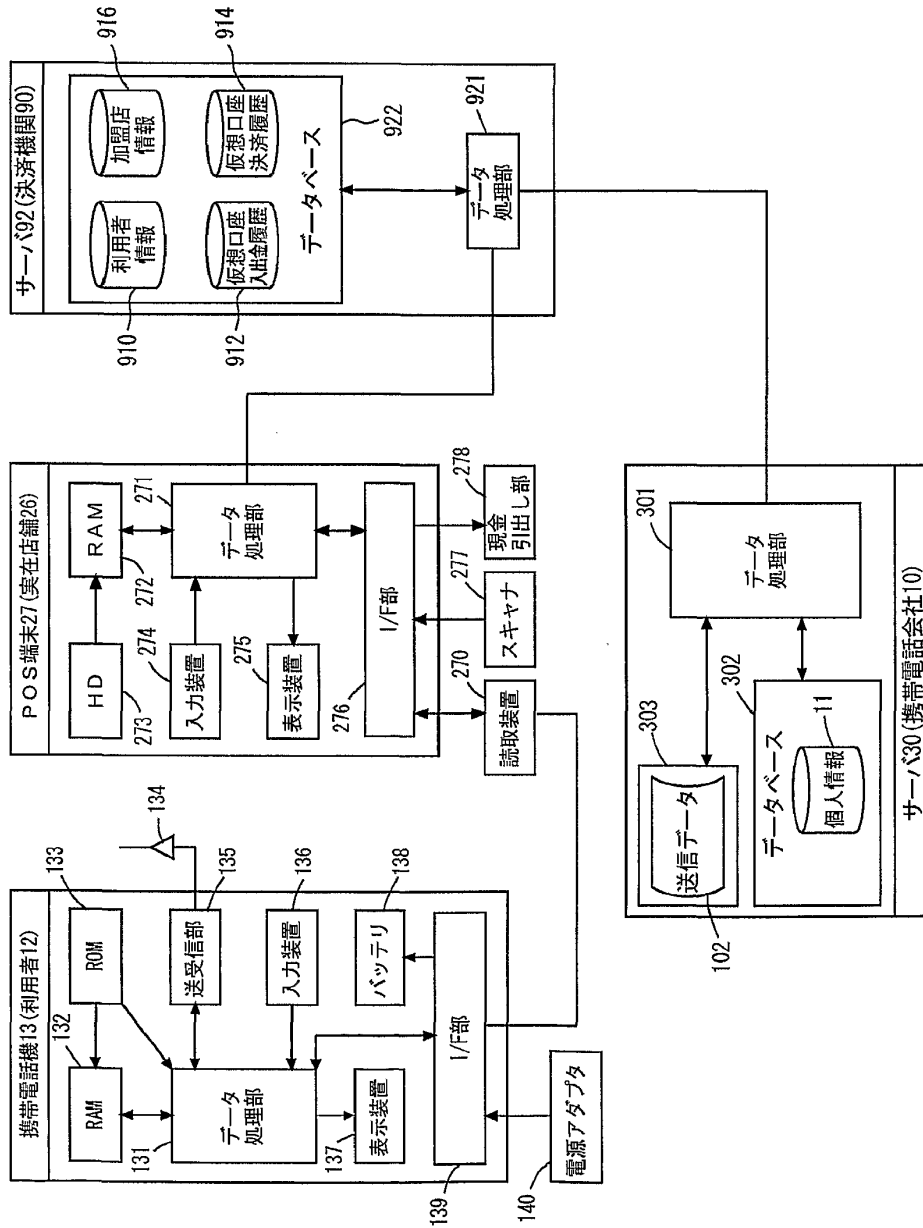


FIG. 58

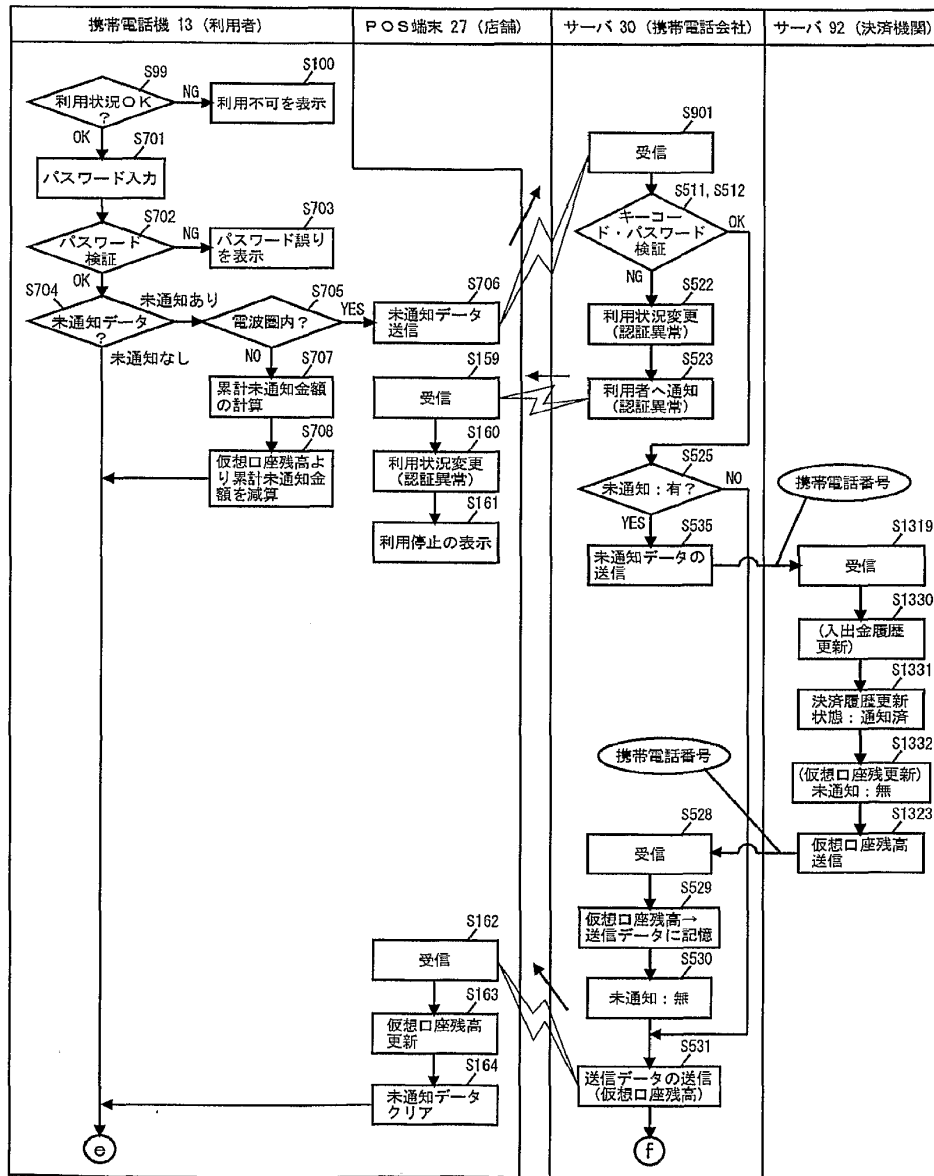


FIG. 59

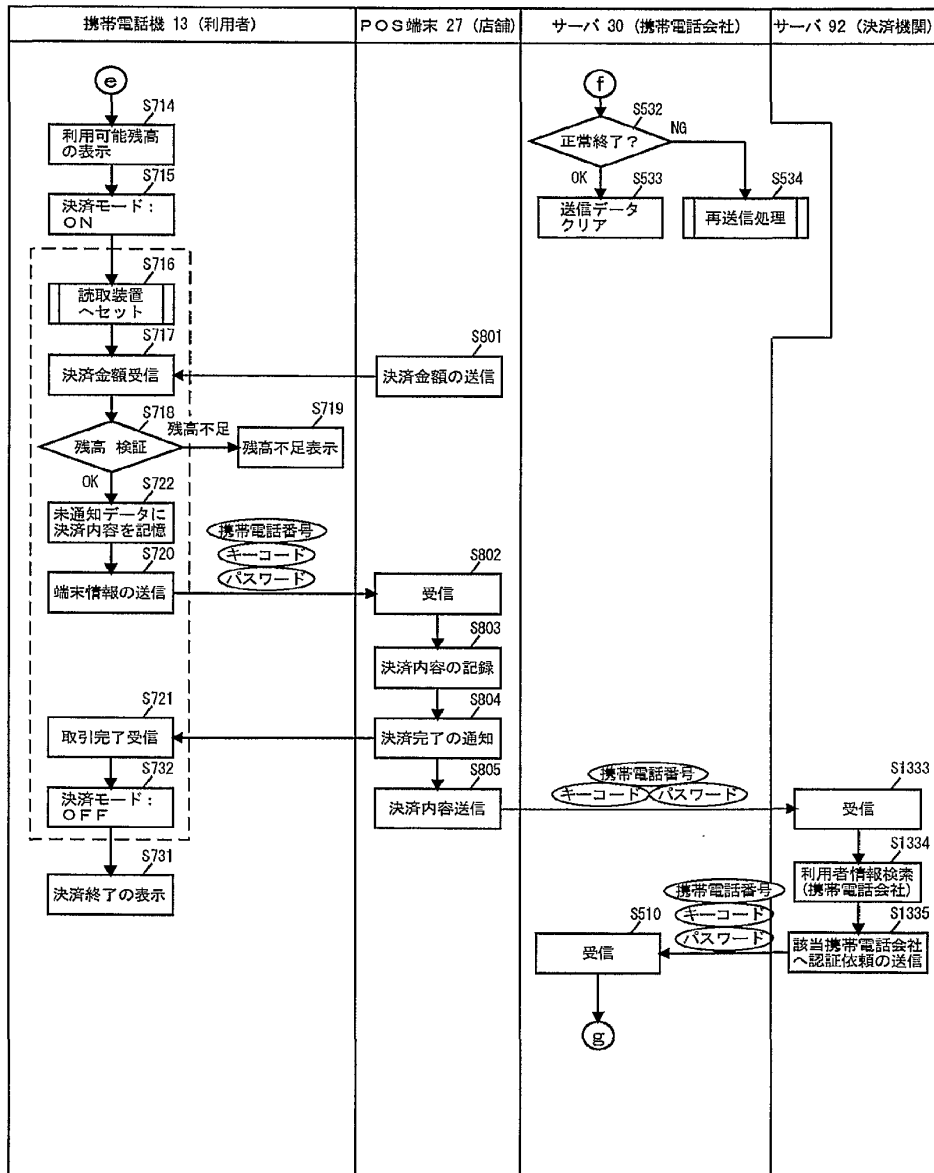


FIG. 60

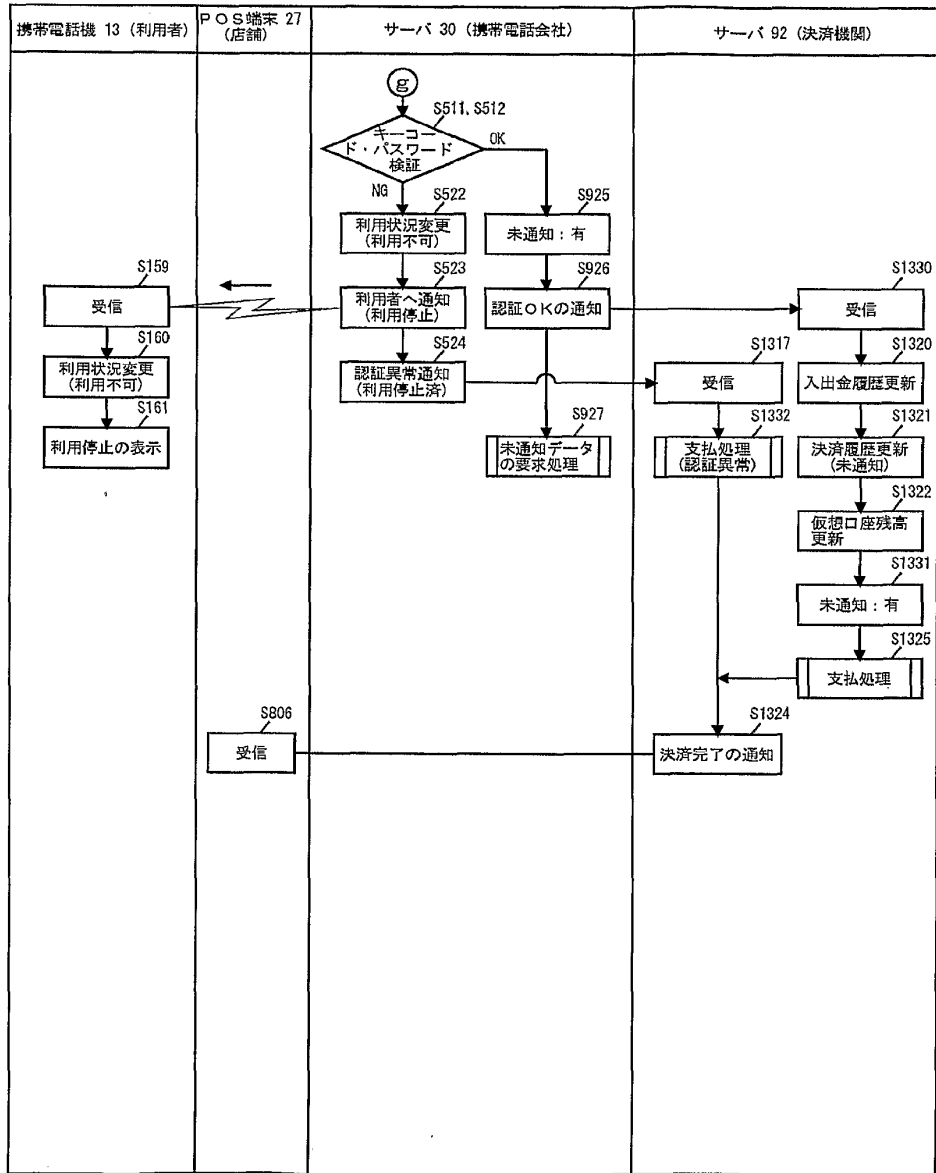


FIG. 61

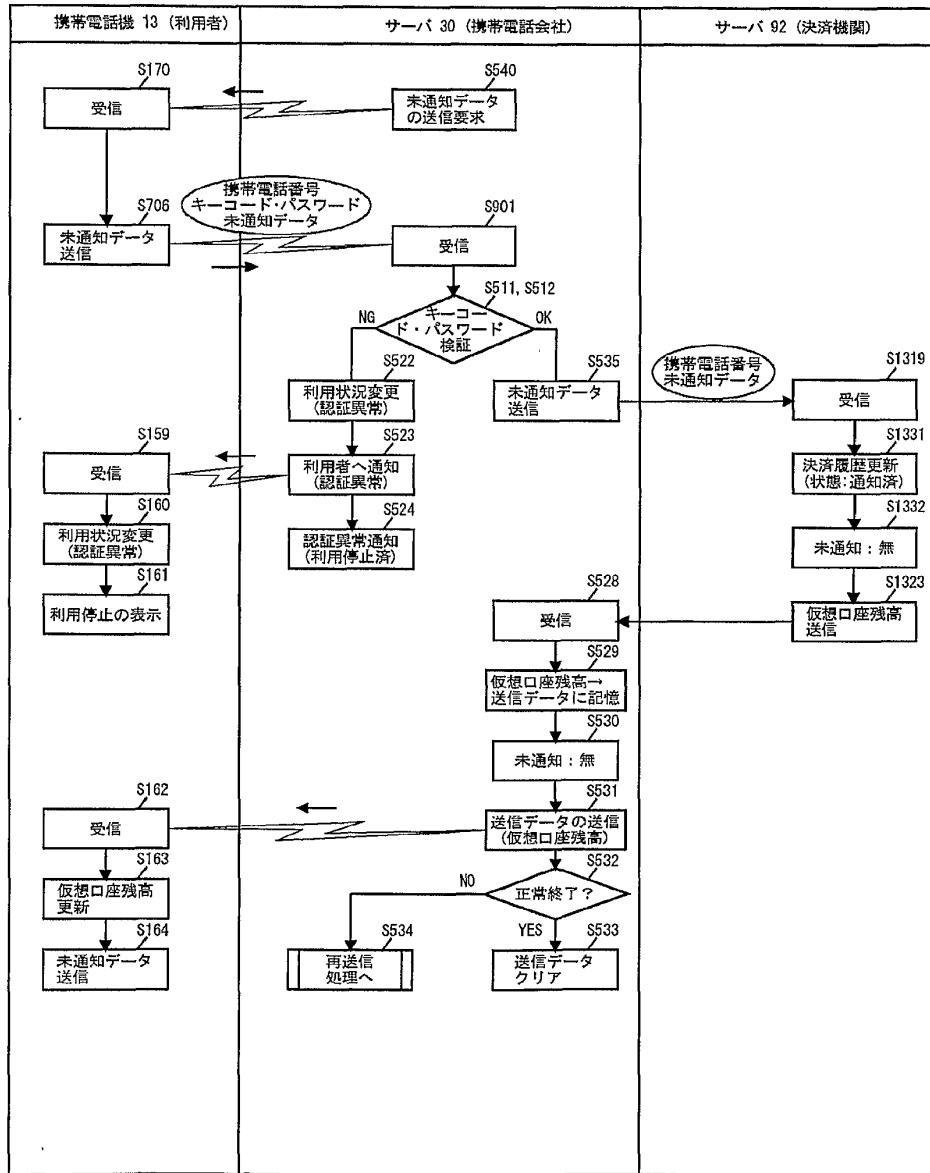


FIG. 62

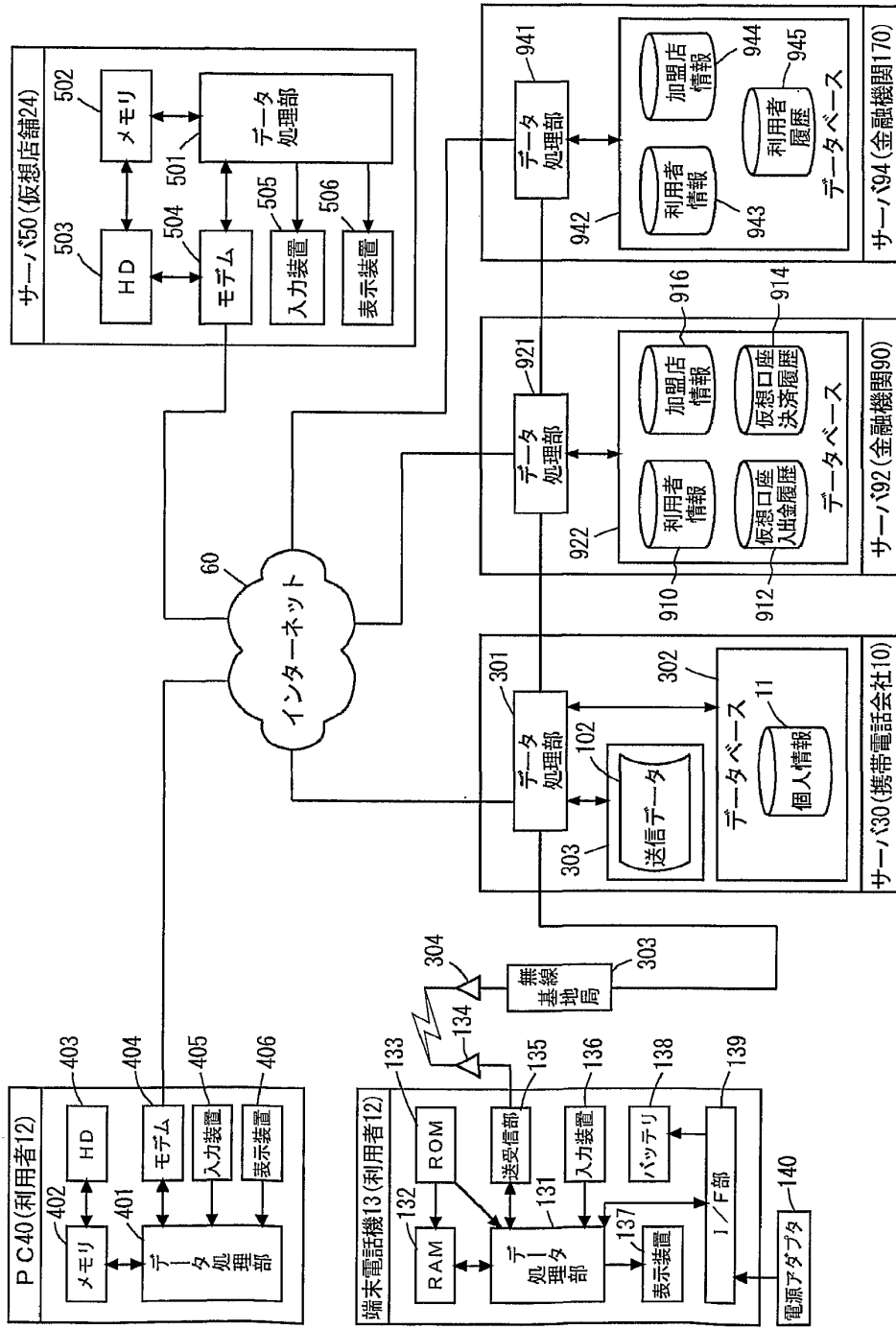


FIG. 63

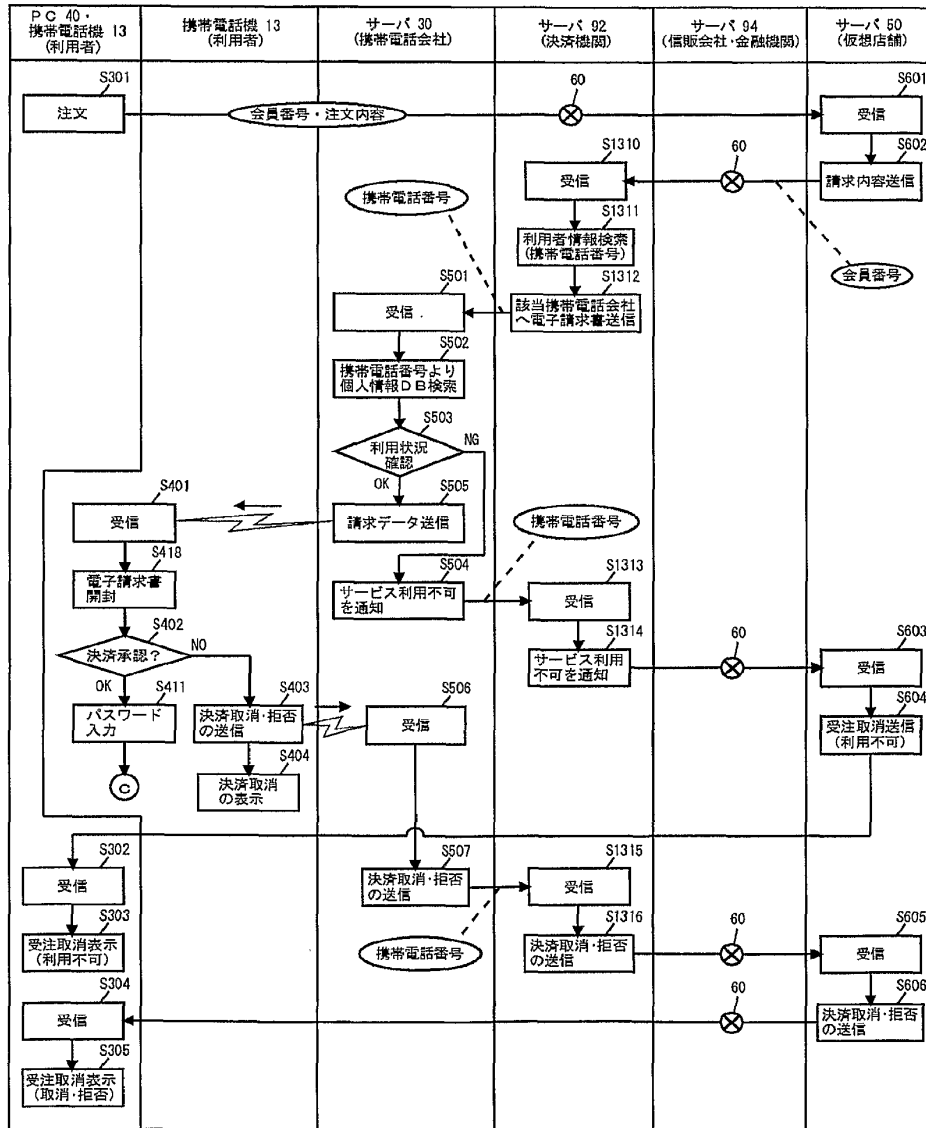


FIG. 64

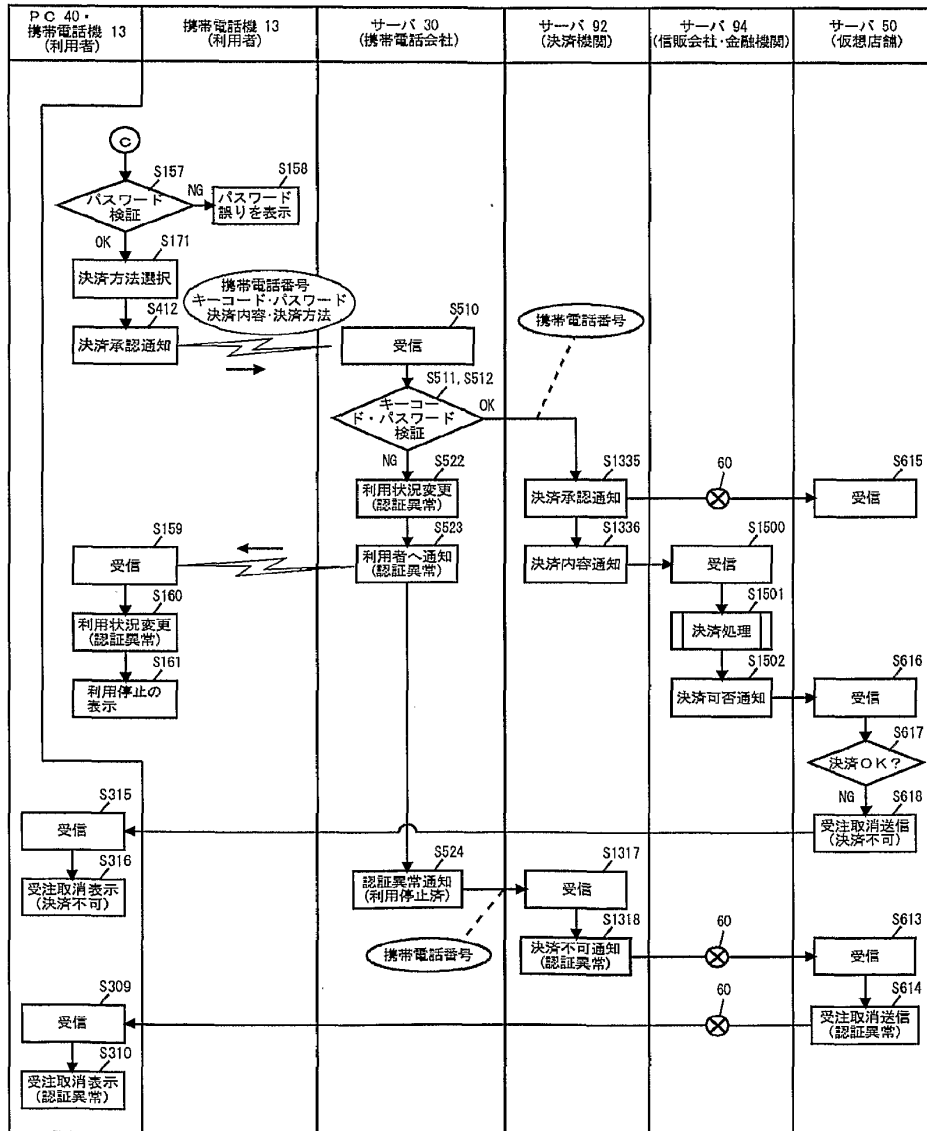


FIG. 65

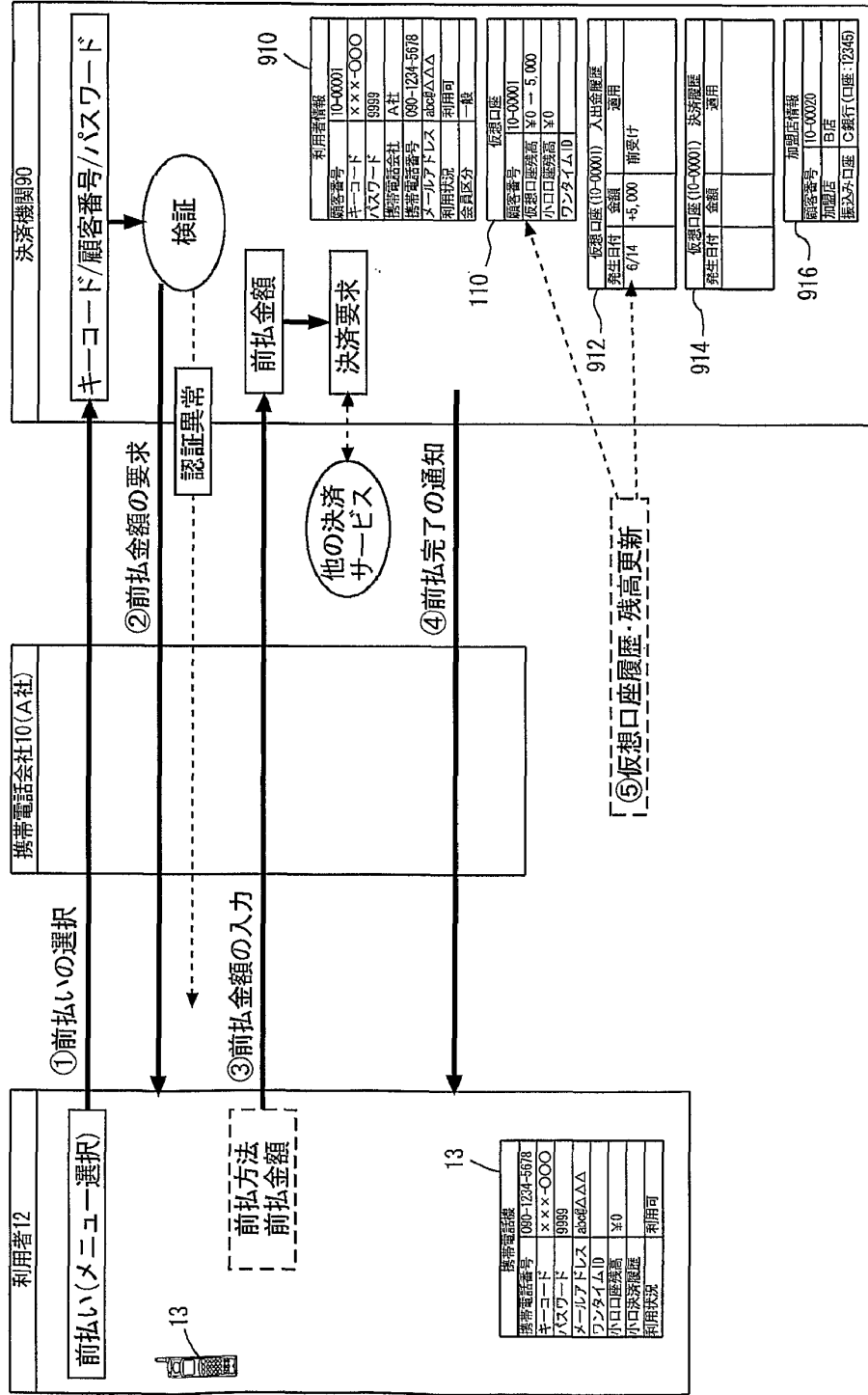


FIG. 66

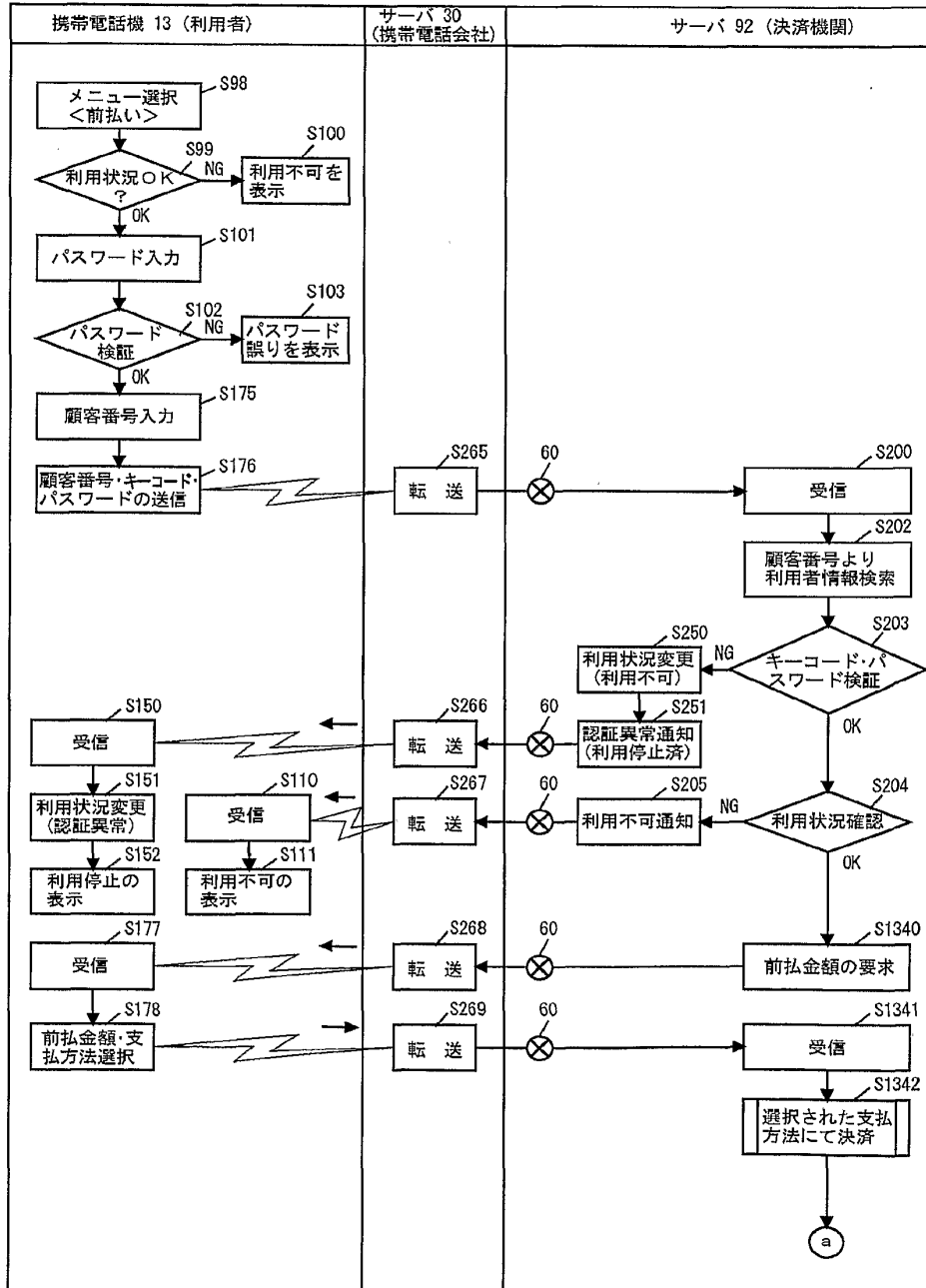


FIG. 67

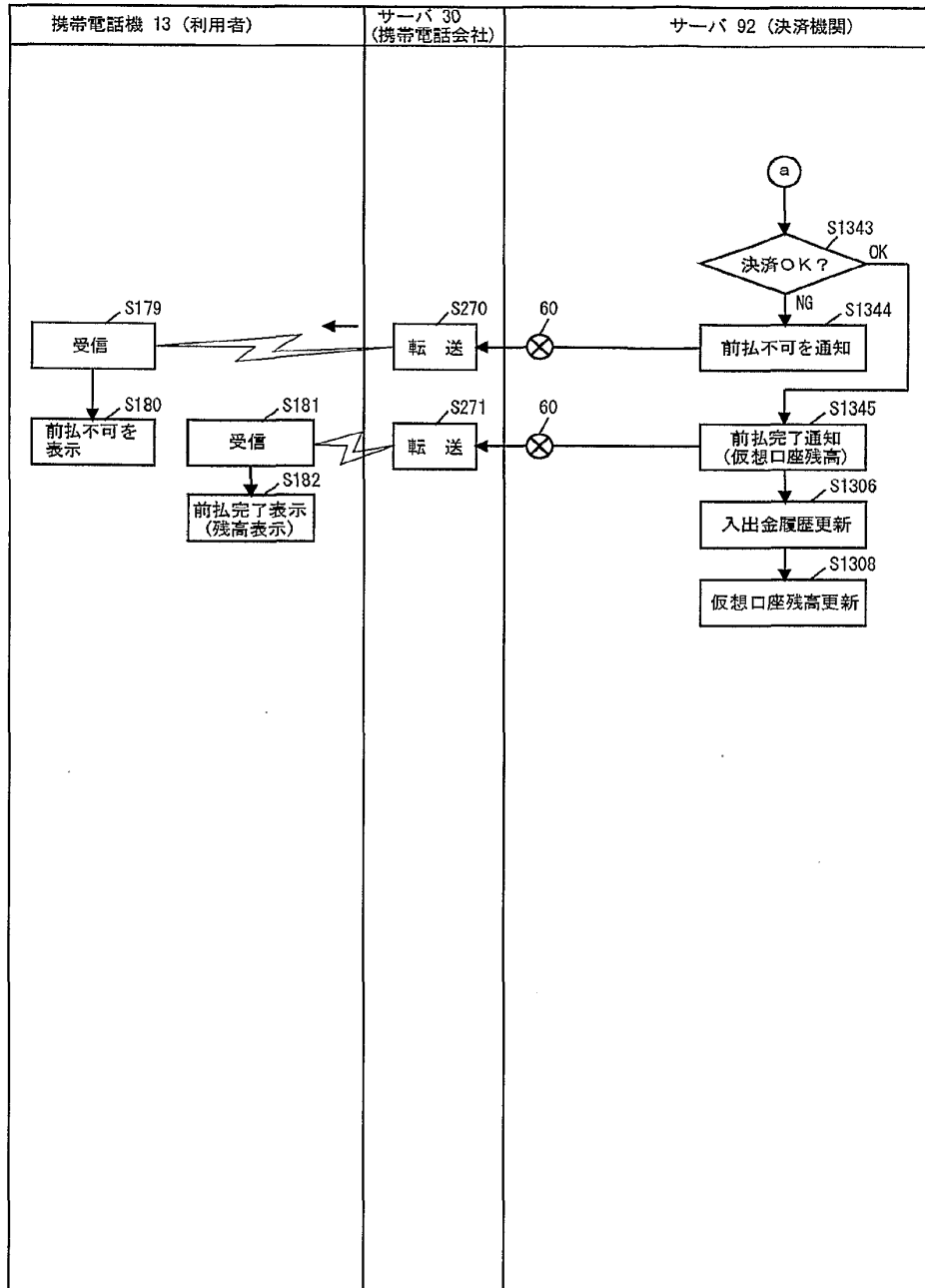


FIG. 68

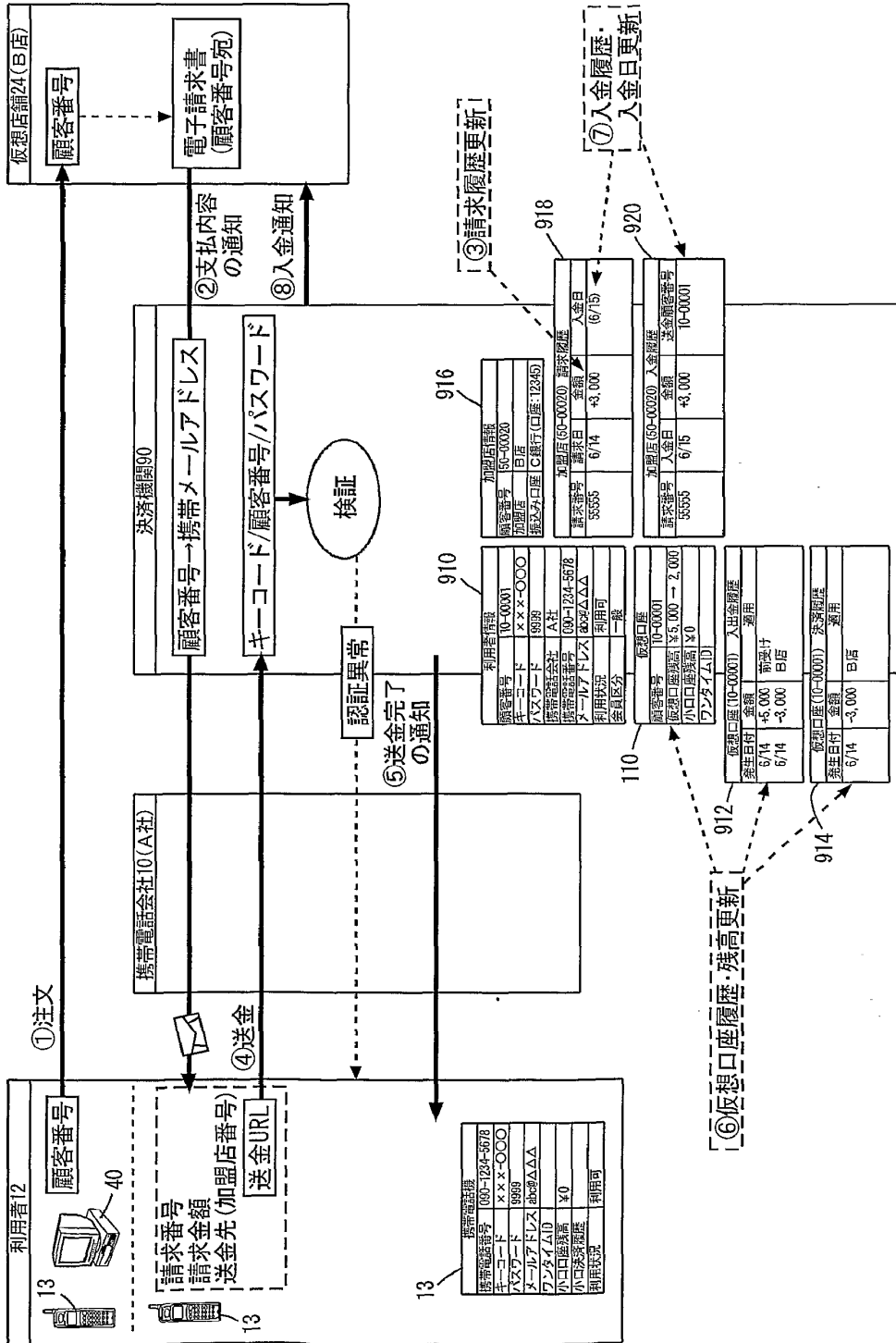


FIG. 69

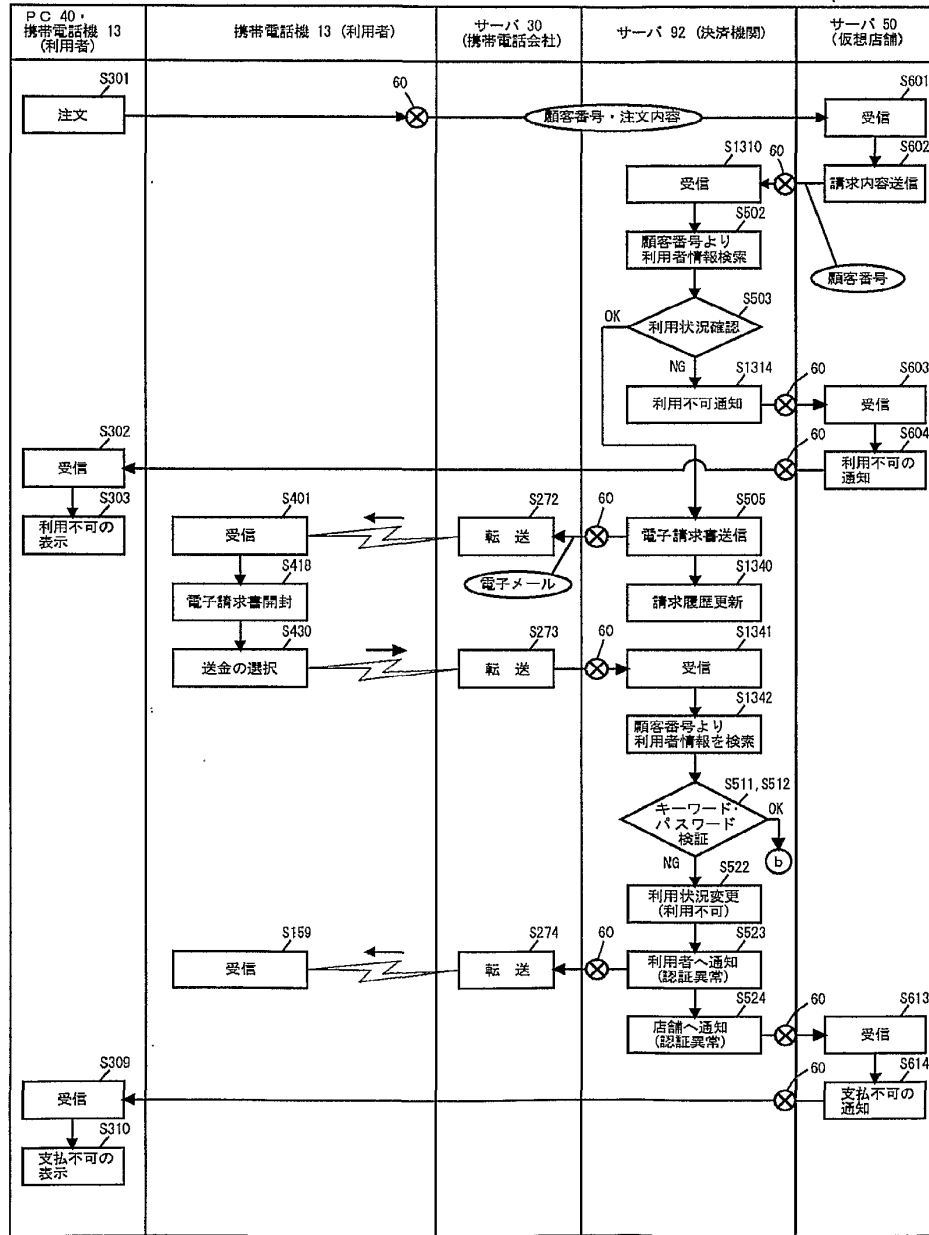


FIG. 70

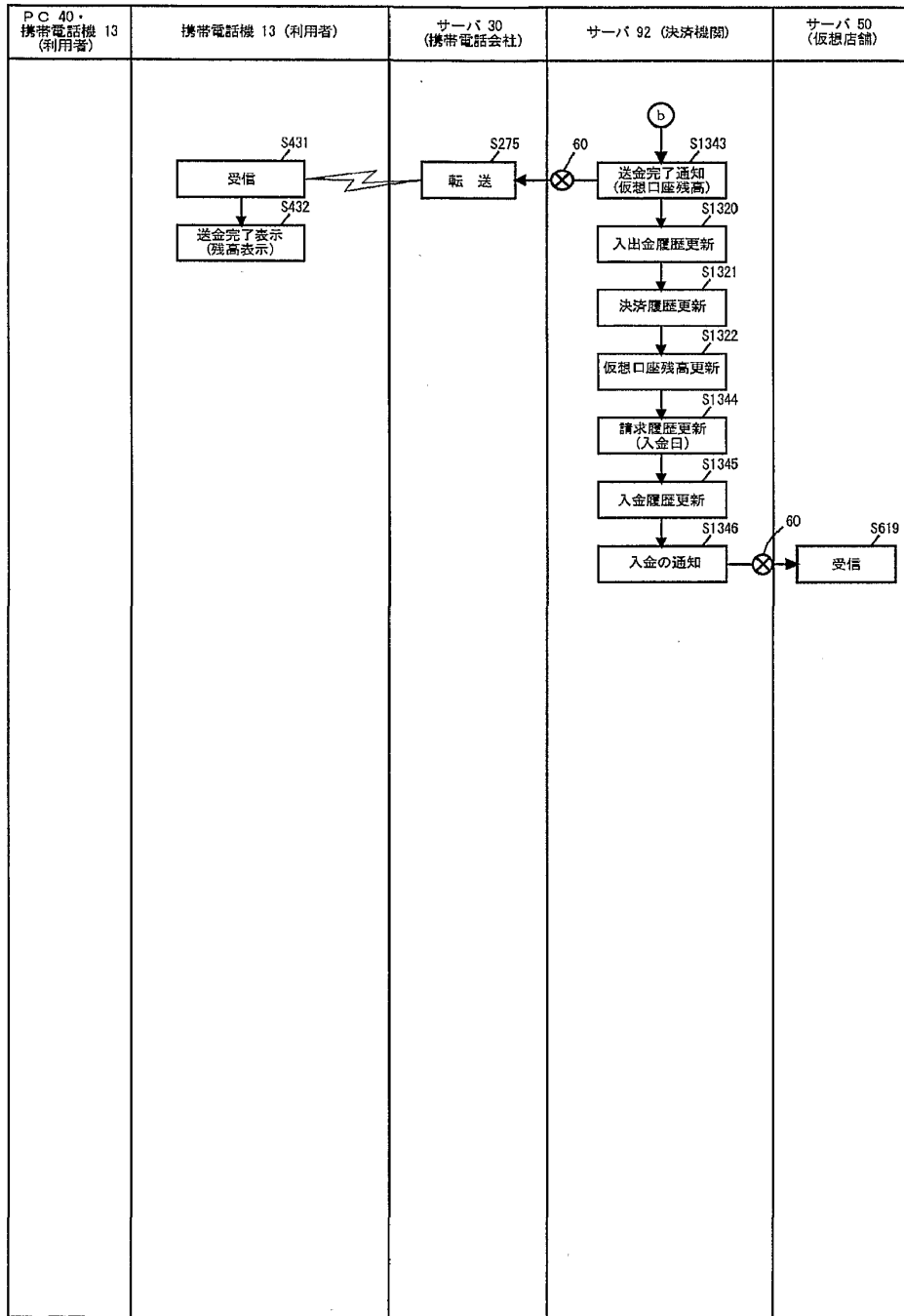


FIG. 71

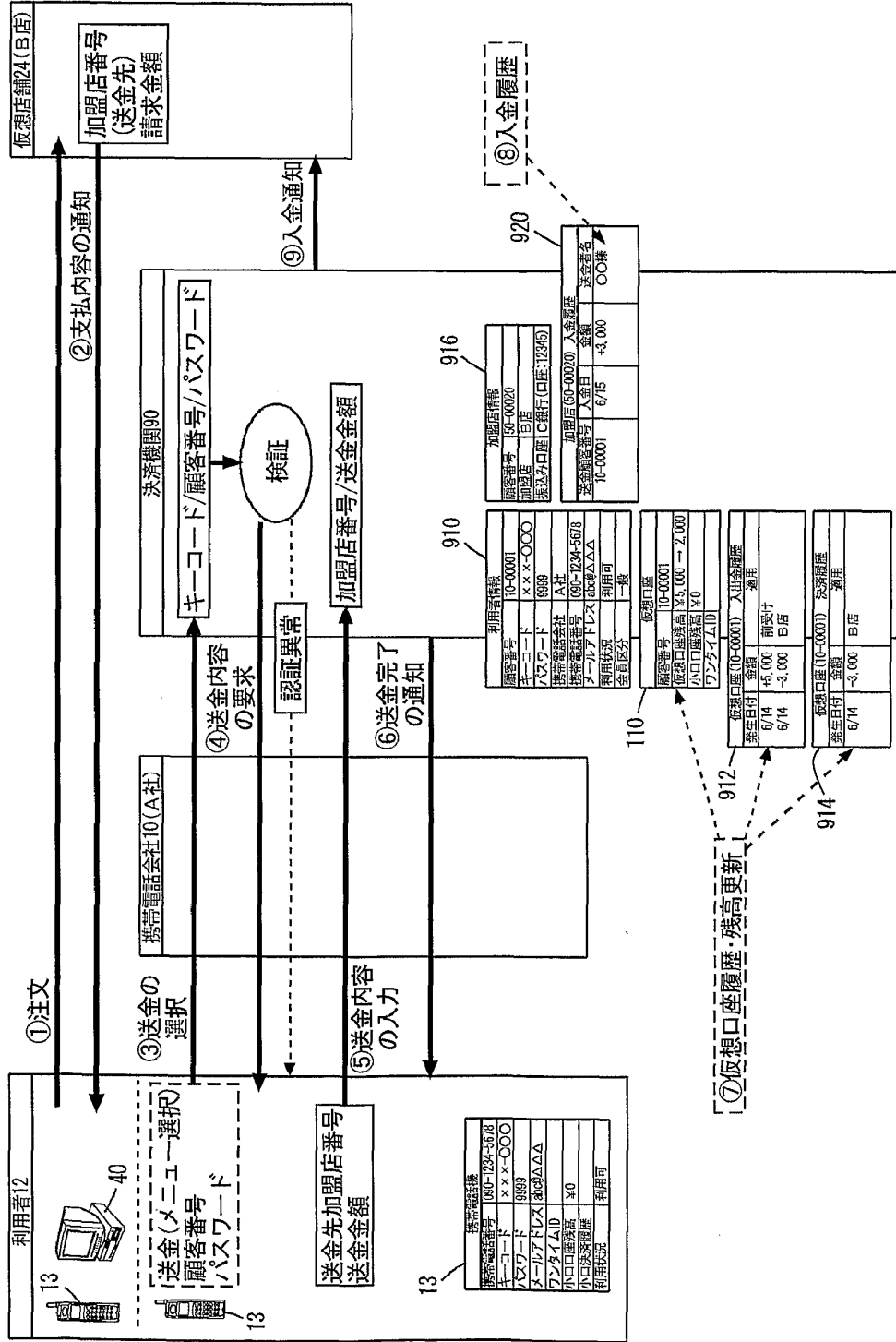


FIG. 72

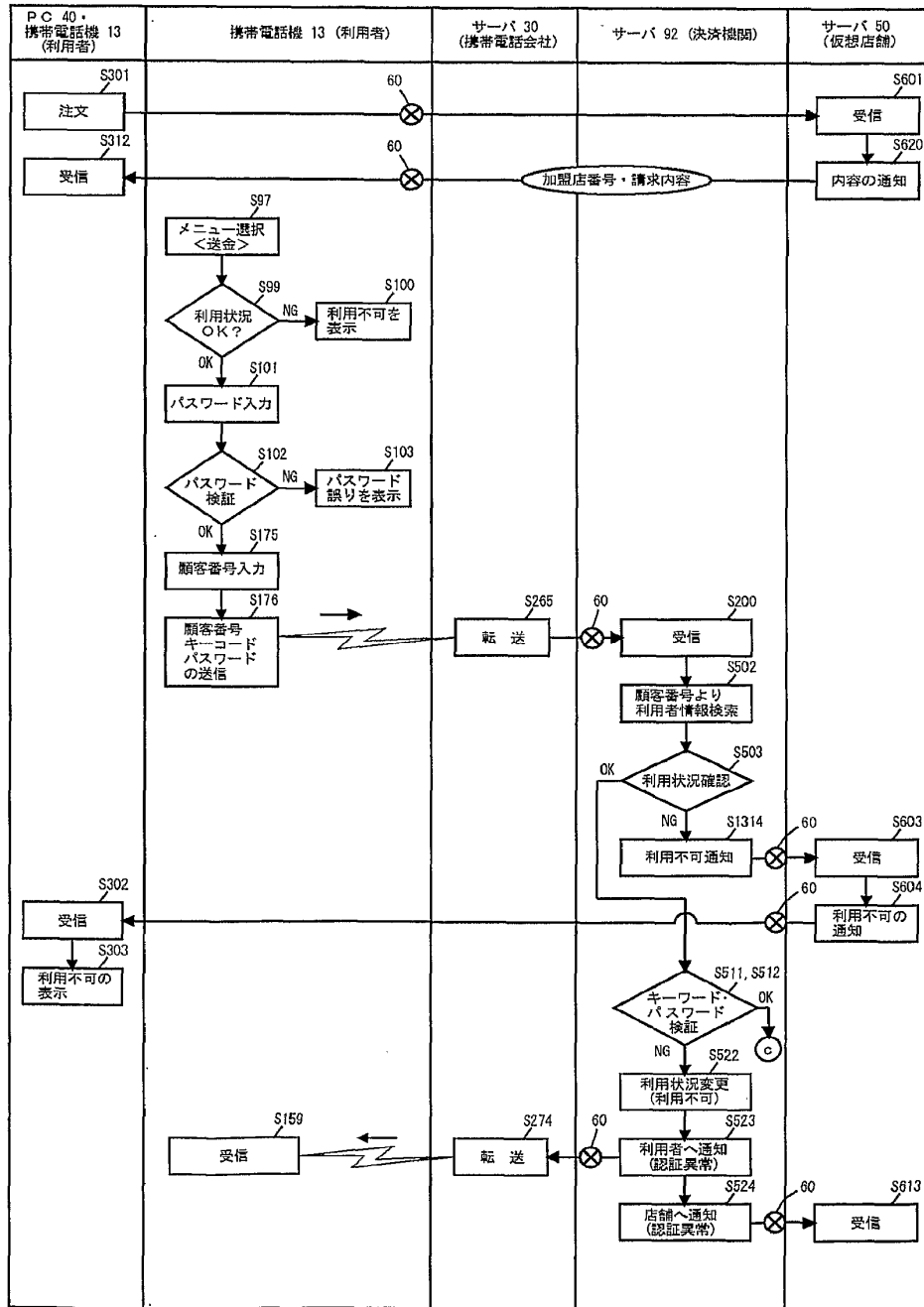


FIG. 73

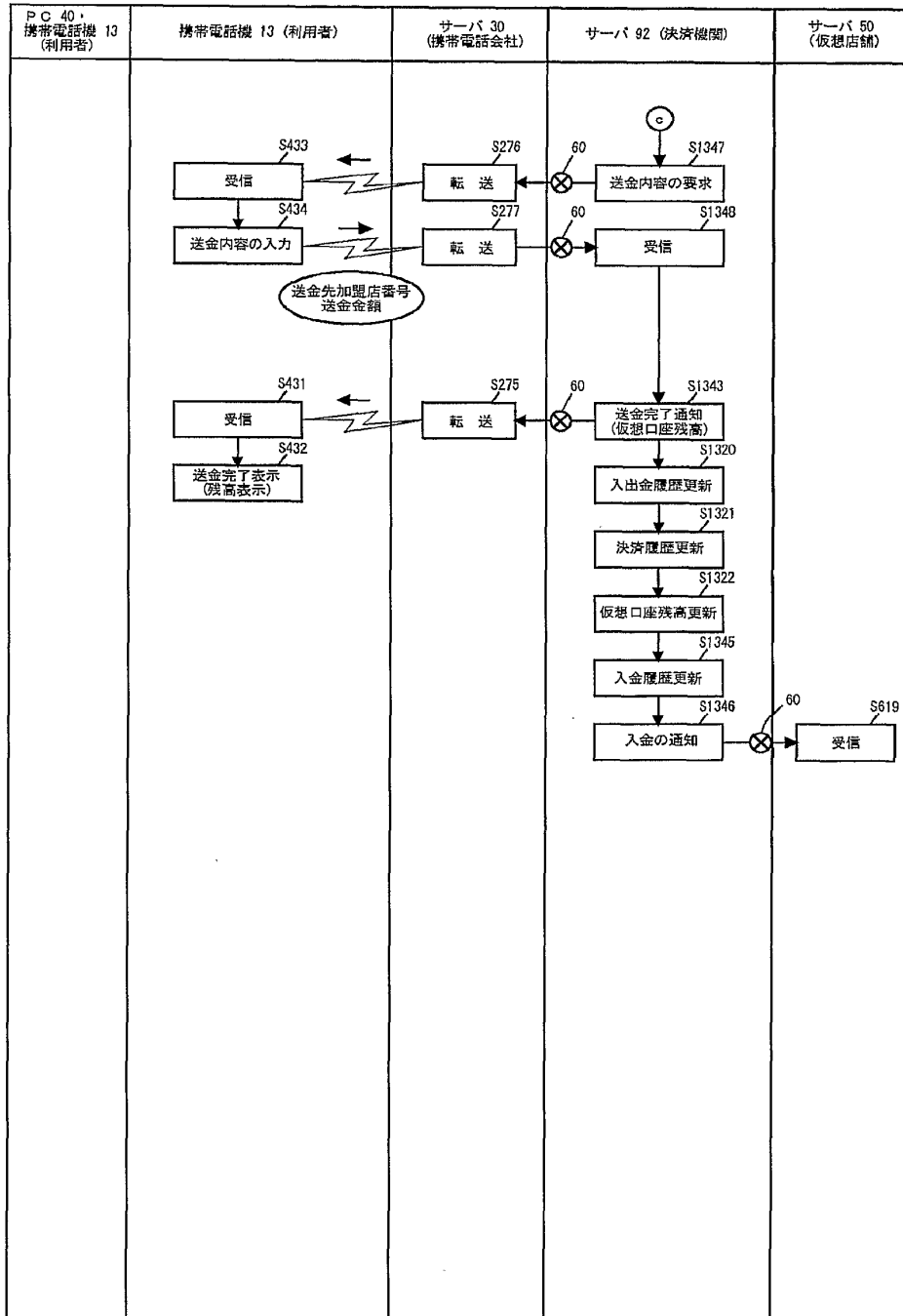


FIG. 74

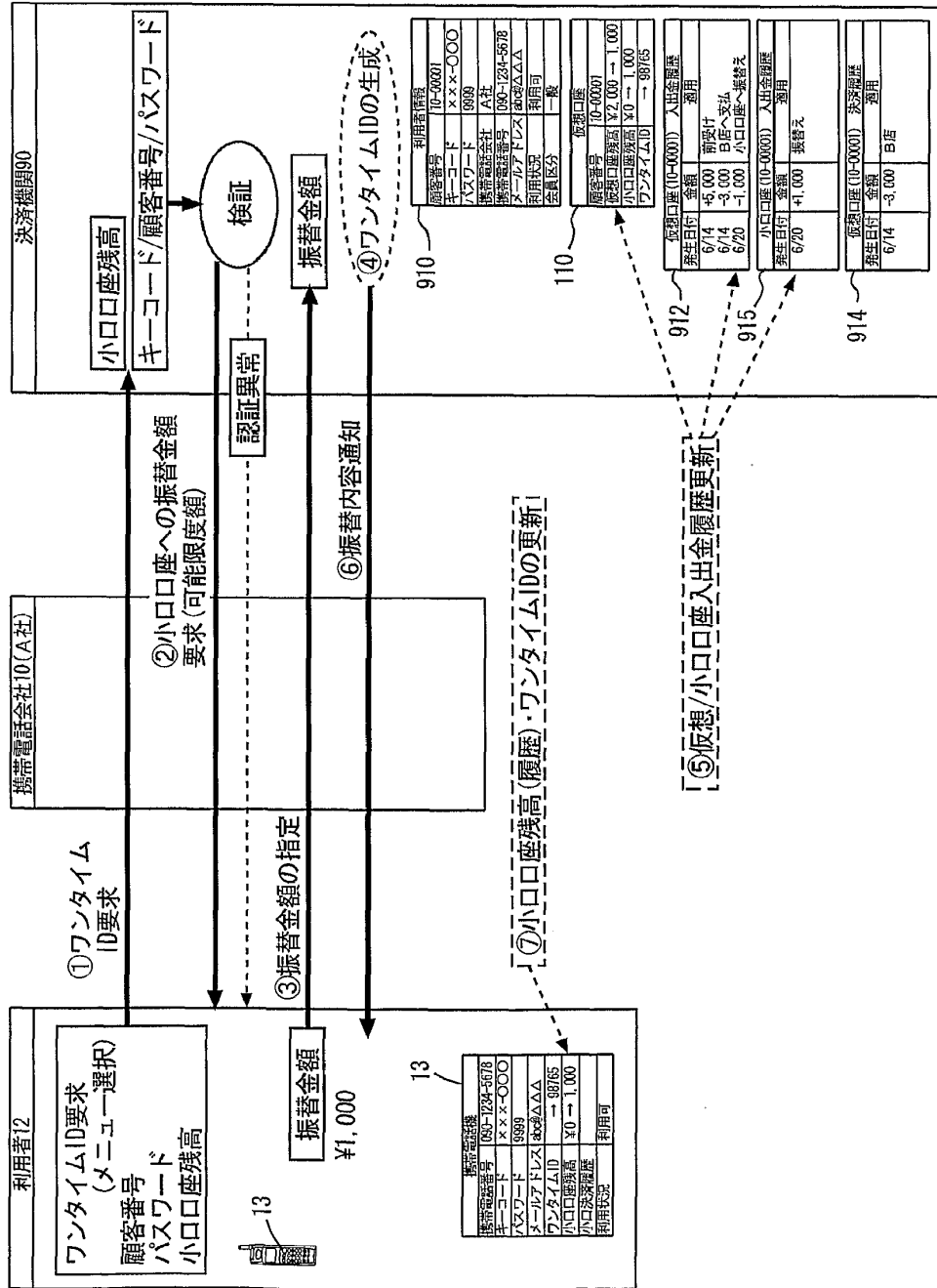


FIG. 75

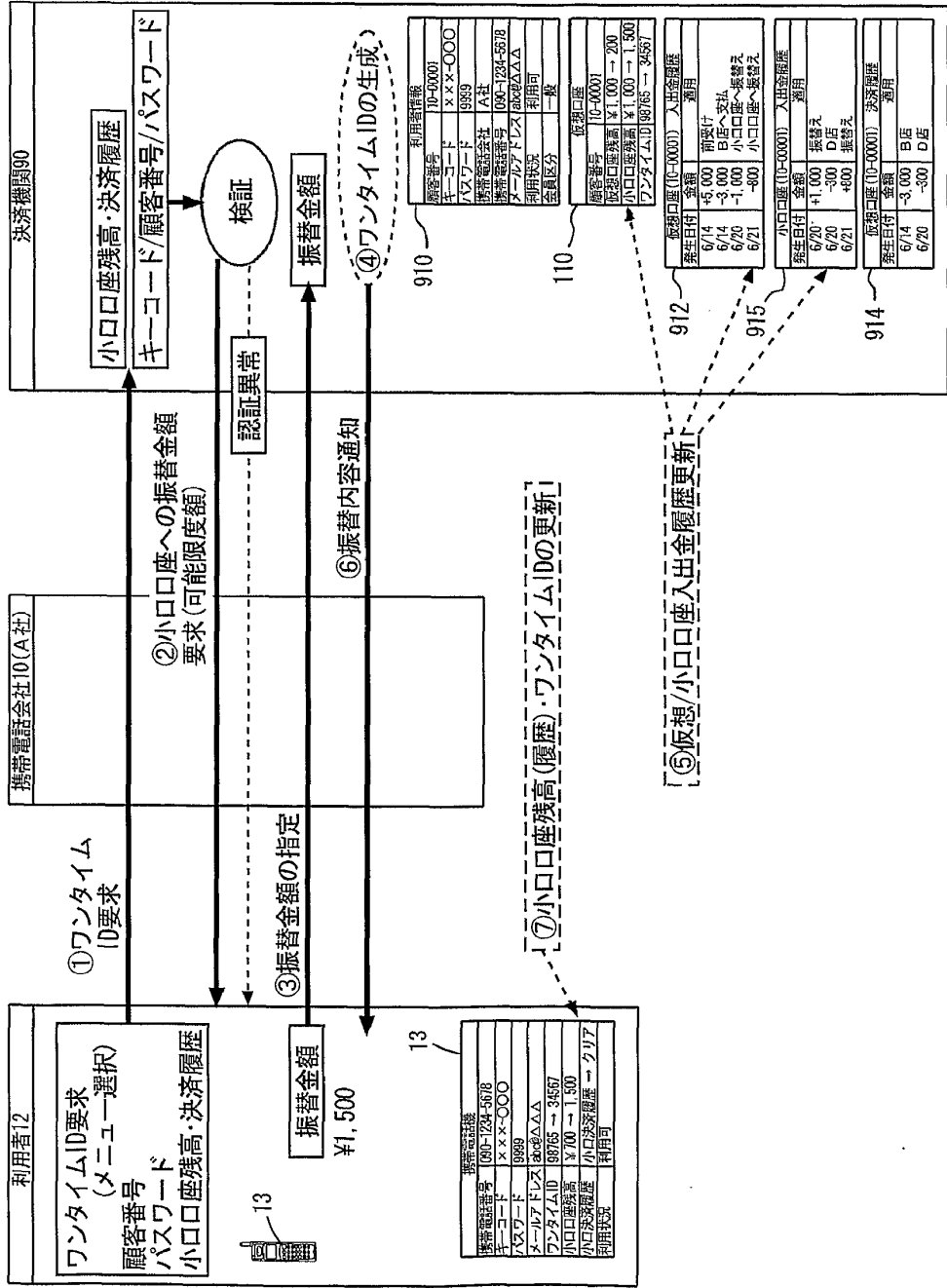


FIG. 76

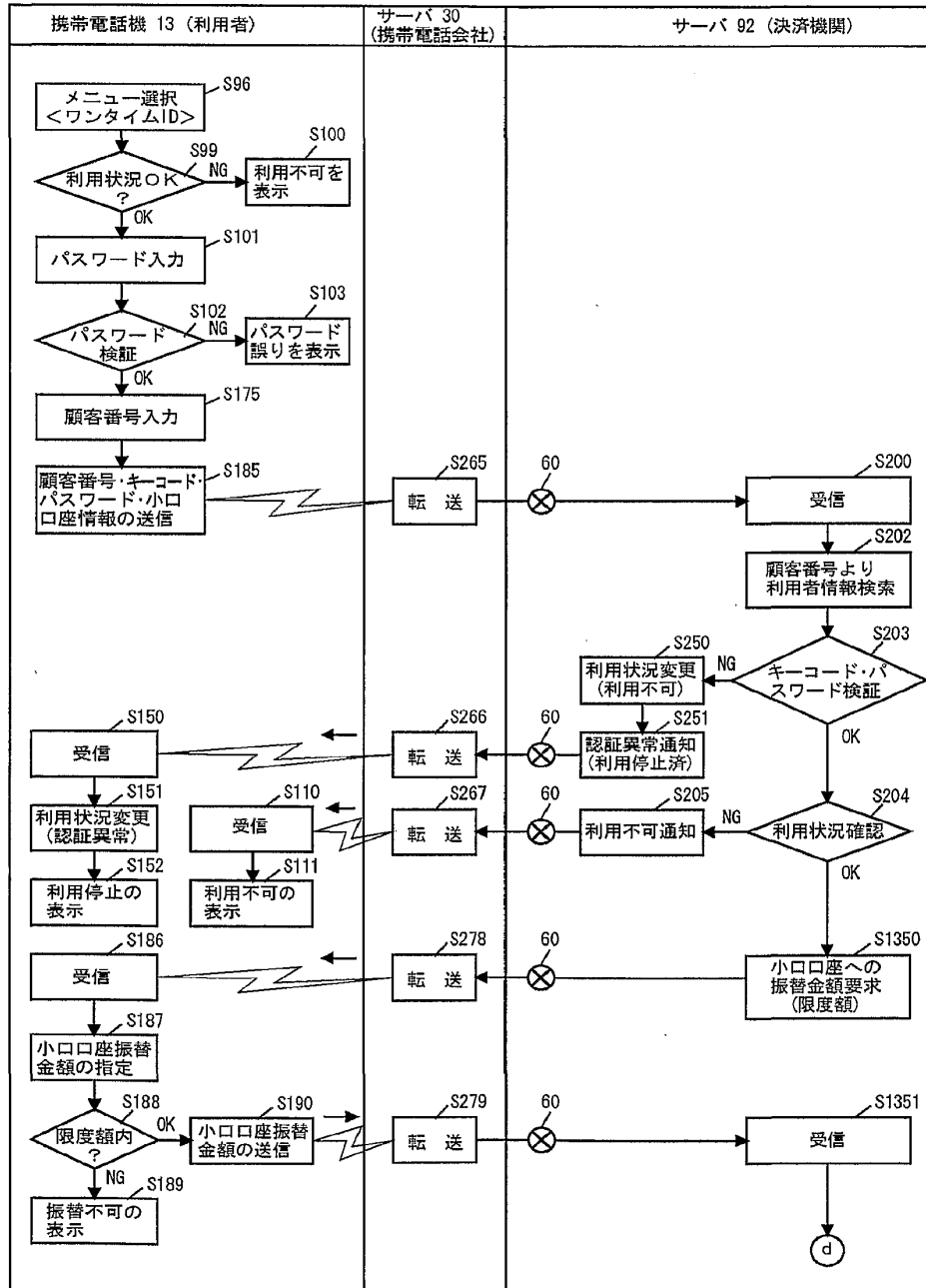


FIG. 77

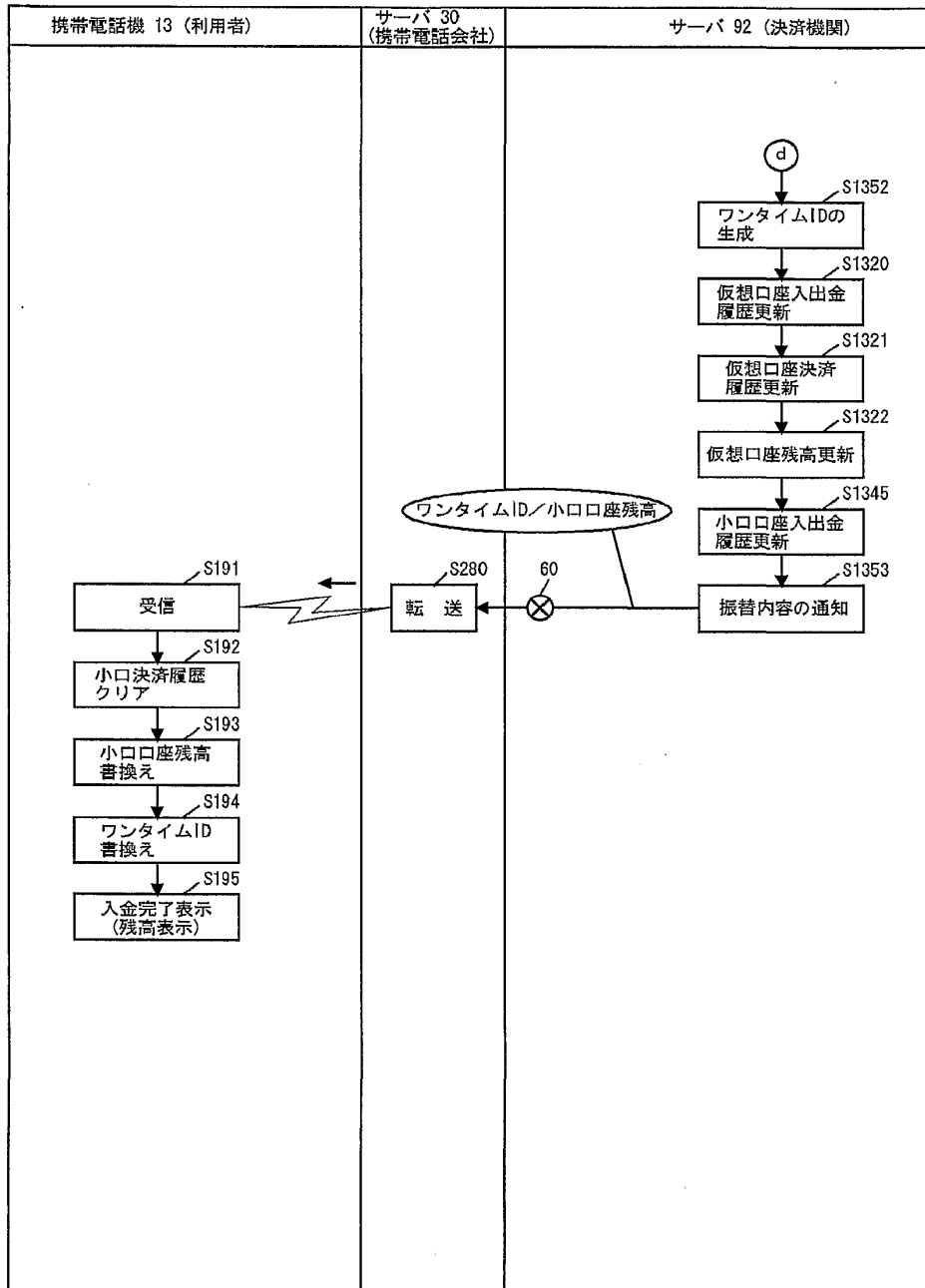


FIG. 78

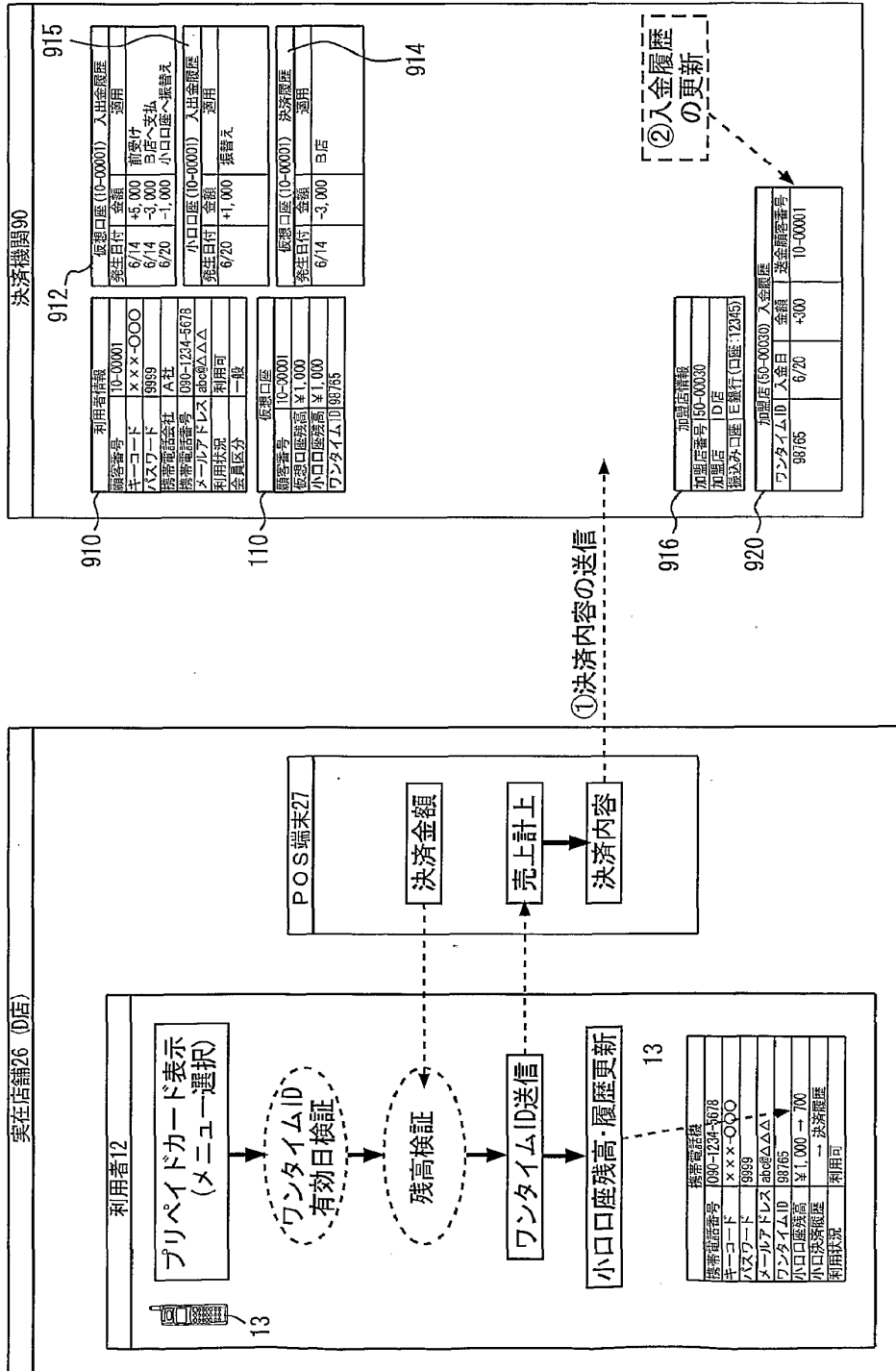
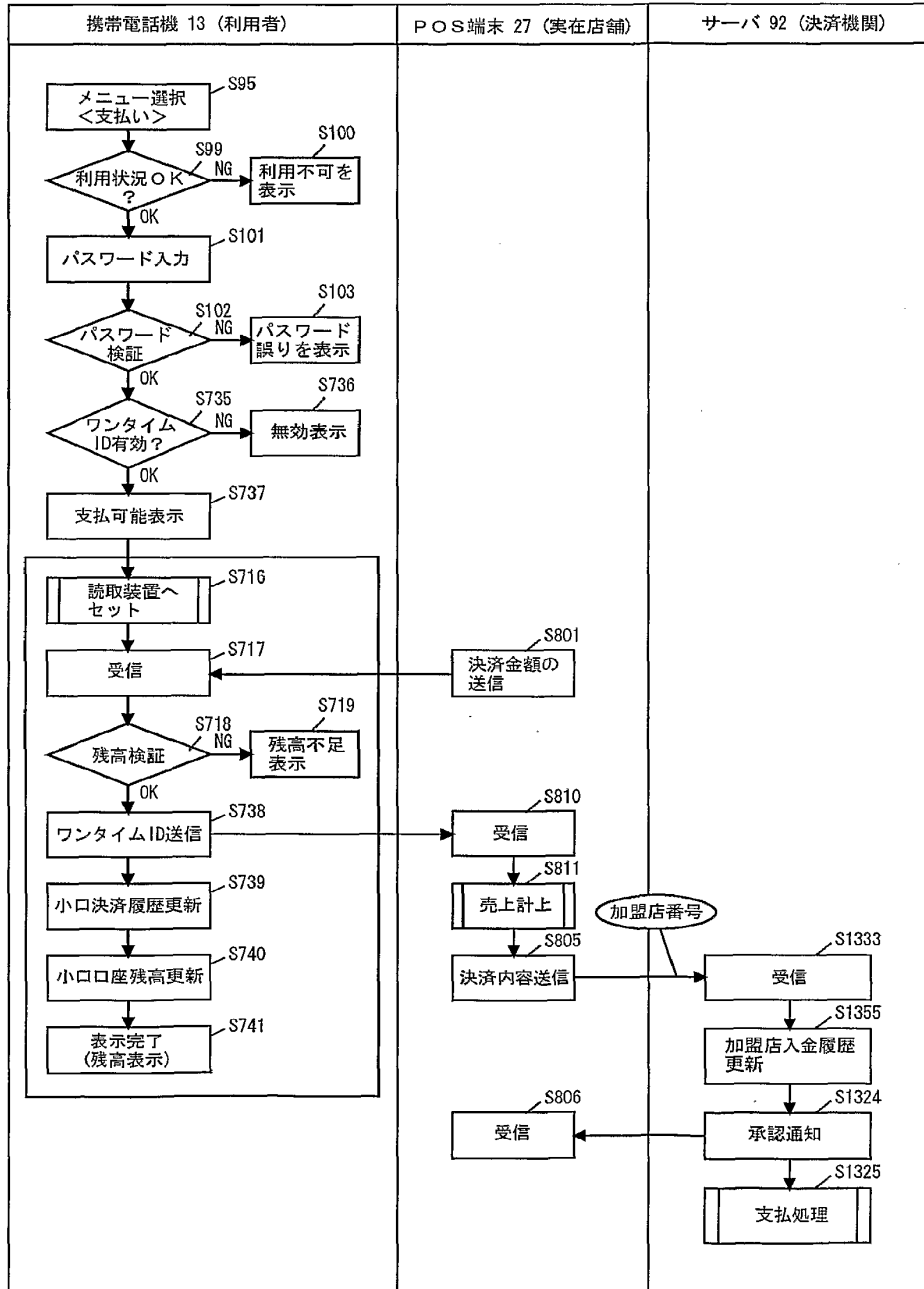


FIG. 79



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05039

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl ⁷ G06F17/60, G06F19/00		
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.Cl ⁷ G06F17/60, G06F19/00		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001		
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	WO 96/25828 A1 (Nokia Mobile Phones, Ltd.), 22 August, 1996 (22.08.96), page 16, lines 18 to 26; page 18, lines 22 to 25 & AU 46247/96 A & AU 696876 B & CN 1174648 A & EP 809916 A1 & FI 950685 A & FI 99071 B & JP 11-501424 A & US 5887266 A	1-33
Y	WO 92/11598 A1 (Motorola, Inc.), 09 July, 1992 (09.07.92), Figs. 5(A) to 5(E) & AT 188562 E & CA 2096730 A & DE 69131897 T & EP 564469 A1 & EP 940760 A1 & ES 2141092 T & GR 3032864 T & KR 97-07003 B1 & JP 6-501329 A & JP 3010069 B2 & US 5221838 A	1-33
Y	JP 6-121075 A (Nippon Telegr. & Teleph. Corp. <NTT>), 28 April, 1994 (28.04.94), Par. Nos. [0026] to [0027] (Family: none)	1-33
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "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) "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	"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 "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 "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 "&" document member of the same patent family	
Date of the actual completion of the international search 11 September, 2001 (11.09.01)	Date of mailing of the international search report 18 September, 2001 (18.09.01)	
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer	
Facsimile No.	Telephone No.	

Form PCT/ISA/210 (second sheet) (July 1992)


INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05039

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2-061786 A (NEC Corporation), 01 March, 1990 (01.03.90), Fig. 1 (Family: none)	1-33
Y	EP 416916 A2 (Fujitsu Ltd.), 13 March, 1991 (13.03.91), Column 23, line 54 to Column 24, line 6 & DE 69033207 T & ES 2136057 T & JP 3-092966 A & JP 3184196 B2 & KR 9607940 A	1-33
Y	WO 99/24892 A1 (Citicorp Development Center, Inc.), 20 May, 1999 (20.05.99), page 11, lines 5 to 29; page 14, lines 18 to 24 & AU 92346/98 A & EP 917120 A2 & JP 11-232348 A & SG 78323 A	1-33
Y	WO 98/026381 A1 (Nixu OY), 18 June, 1998 (18.06.98), Figs. 6, 7; page 16, lines 1 to 6 & AU 52246/98 A & AU 729844 B & CN 1245574 A & DE 69603971 T & EP 848361 A1 & JP 2001-507487 A & NO 992776 & US 6029151 A	1-33
Y	JP 2000-113085 A (Sony Corporation), 21 April, 2000 (21.04.00), Fig. 1 (4, 5, 8) (Family: none)	1-33
A	DUKACH, Semyon, "SNPP: A Simple Network Payment Protocol", In: <i>Proceedings of the Eighth Annual Computer Security Applications Conference</i> , 30 November, 1992 (30.11.92), pages 173 to 179	1-33

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int.Cl. ⁷ G06F17/60, G06F19/00		
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.Cl. ⁷ G06F17/60, G06F19/00		
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 1922-1996年 日本国公開実用新案公報 1971-2001年 日本国登録実用新案公報 1994-2001年 日本国実用新案登録公報 1996-2001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	WO 96/25828 A1 (NOKIA MOBILE PHONES LTD) 22. 8 月. 1996 (22.08.96) 16 ページ, 18-26 行; 18 ページ, 22-25 行 & AU 46247/96 A & AU 696876 B & CN 1174648 A & EP 809916 A1 & FI 950685 A & FI 99071 B & JP 11-501424 A & US 5887266 A	1-33
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> 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	11.09.01	国際調査報告の発送日 18.09.01
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) 阿波 進 
		5 L 9168
		電話番号 03-3581-1101 内線 3561

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
Y	WO 92/11598 A1 (MOTOROLA INC) 9. 7 月. 1992 (09.07.92) 図 5A-5E & AT 188562 E & CA 2096730 A & DE 69131897 T & EP 564469 A1 & EP 940760 A1 & ES 2141092 T & GR 3032864 T & KR 97-07003 B1 & JP 6-501329 A & JP 3010069 B2 & US 5221838 A	1-33
Y	JP 6-121075 A (日本電信電話株式会社) 28. 4 月. 1994 (28.04.94) 段落[0026]-[0027] (ファミリーなし)	1-33
Y	JP 2-061786 A (日本電気株式会社) 1. 3 月. 1990 (01.03.90) 図 1 (ファミリーなし)	1-33
Y	EP 416916 A2 (FUJITSU LTD) 13. 3 月. 1991 (13.03.91) コラム 23, 54 行 — コラム 24, 6 行 & DE 69033207 T & ES 2136057 T & JP 3-092966 A & JP 3184196 B2 & KR 9607940 A	1-33
Y	WO 99/24892 A1 (CITICORP DEVELOPMENT CENTER INC) 20. 5 月. 1999 (20.05.99) 11 ページ, 5-29 行, 14 ページ, 18-24 行 & AU 92346/98 A & EP 917120 A2 & JP 11-232348 A & SG 78323 A	1-33

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
Y	WO 98/026381 A1 (NIXU OY) 18. 6 月. 1998 (18.06.98) 図 6, 7; 16 ページ, 1-6 行 & AU 52246/98 A & AU 729844 B & CN 1245574 A & DE 69603971 T & EP 848361 A1 & JP 2001-507487 A & NO992776 & US 6029151 A	1-33
Y	JP 2000-113085 A (ソニー株式会社) 21. 4 月. 2000 (21.04.00) 図 1 (4, 5, 8 を見よ) (ファミリーなし)	1-33
A	DUKACH, Semyon, SNPP: A Simple Network Payment Protocol, in <i>Proceedings of the Eighth Annual Computer Security Applications Conference</i> , 30 November 1992 (30.11.92), pp 173-179.	1-33

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
12 September 2002 (12.09.2002)

PCT

(10) International Publication Number
WO 02/071354 A2

- (51) International Patent Classification⁷: G07F 19/00
- (21) International Application Number: PCT/CA02/00272
- (22) International Filing Date: 4 March 2002 (04.03.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/272,300 2 March 2001 (02.03.2001) US
- (71) Applicant (for all designated States except US): **SOFT TRACKS ENTERPRISES LTD.** [CA/CA]; Suite 1258, 13351 Commerce Parkway, Richmond, British Columbia V6V 2X7 (CA).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **SWAIN, Alan, L.** [CA/CA]; 9740 Snowdon Avenue, Richmond, British Columbia V7A 2M1 (CA). **WOO, Kevin, K., M.** [CA/CA]; 10368 - 167th Street, Surrey, British Columbia V4N 1Z2 (CA).
- (74) Agent: **FASKEN MARTINEAU DUMOULIN LLP**; Toronto Dominion Bank Tower, Box 20, Suite 4200, Toronto Dominion Centre, Toronto, Ontario M5K 1N6 (CA).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



WO 02/071354 A2

(54) Title: SYSTEM AND METHOD FOR FACILITATING AN M-COMMERCE TRANSACTION

(57) Abstract: A method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, the method comprising the steps of receiving at an application server first information indicative of the transaction device authentication; receiving at the application server second information for verification of the user; and using both the first and second information to authorise top-up payment of the prepaid service.

SYSTEM AND METHOD FOR FACILITATING AN M-COMMERCE
TRANSACTION

BACKGROUND OF THE INVENTION

5

Payments in commercial transactions have evolved over time, from cash transactions, to credit card transactions to present day payment via electronic devices. Each step in the evolution has spawned its own industry and infrastructure, and successive levels in the evolution have built on the existing infrastructure. Collectively these
10 infrastructures and processes are referred to as the payment industry.

While wireless and Internet technologies are fuelling change within the current payment industry, there is a need for new innovative payment solutions, which leverage the hard earned trust of existing financial institutions. It is the eventual goal
15 to effect a transformation of the payment industry by enabling secure and trusted payments, in any form of tender, via any electronic device.

In general, mobile e-commerce (m-commerce) is defined as online purchasing of goods and services, including subscription based services, such as news, music and
20 financial services, using a mobile phone service. A major challenge inhibiting widespread adoption of m-commerce solutions today is that purchasers often do not trust a mobile device as a secure way of making online payments.

A first step in overcoming this challenge is to involve the wireless carrier as the
25 merchant in selling its own prepaid subscription service in real time. Mobile carriers currently provide three prepay top up solutions. In the first solution, customers purchase a card such as a magnetic stripe card or similar encoding mechanism to indicate that the customer has paid a predetermined prepaid value for the card. These so-called "prepaid vouchers" are purchased at retail outlets. The code on the prepaid
30 voucher is read by the purchaser and communicated either directly on the phone with a carrier customer service representative, or through the carrier's IVR (Interactive Voice Response) system. The code represents a monetary value, which may be added

to the balance of the customer's prepaid account maintained by the carrier. A second solution is payment via credit card, wherein credit card information is either communicated to a carrier's customer service representative via voice or through a PC based web interface. A third solution involves customers prepaying for airtime through automated telemachines (ATM's). This solution is similar to prepaid vouchers in that a code printed on the ATM receipt is communicated to the carrier's customer service representative or entered through the carrier's IVR system.

As may be seen, none of the above solutions allow immediate, secure, authenticated and non-repudiable prepay top up of the customers pre paid value via the customer's wireless telephone or similar device. Because of this, current pre-paid solutions are not as successful as anticipated.

It is thus an objective of the present invention to mitigate some of the above disadvantages.

SUMMARY OF THE INVENTION

One objective of the present invention is to enable authenticated credit transactions and real time payment for top-up of prepaid cellular phones, which uses existing interfaces at both the cell phone carrier network and at the financial institution effecting the top up payment.

In accordance with this invention there is provided a method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, the method comprising the steps of receiving at an application server first information indicative of the transaction device authentication; receiving at the application server second information for verification of the user; and using both the first and second information to authorize top-up payment of the prepaid service

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the preferred embodiments of the invention will become
 5 more apparent in the following detailed description in which reference is made to the
 appended drawings wherein:

Figure 1 is schematic diagram of a payment system according to the present
 invention;

Figure 2 is a schematic diagram of a payment system according to one
 10 embodiment of the invention;

Figure 3 is a schematic diagram of a payment system according to another
 embodiment of the invention;

Figures 4, 5, 6 and 7 show ladder diagrams for use-case scenarios of the
 system of figure 3.

15

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description like numerals refer to like structures in the drawings. For
 convenience, the definitions, acronyms, and abbreviations used in the description are
 20 listed in table 1

Table I

Acronym/ Abbreviation	Expansion
TGS	Transaction Gateway Server
AS	Application Server
RTP	Real Time Payment
MWS	Merchant Wallet Server
VTs	Virtual Terminal Server
IVR	Interactive Voice Response
MT	Mobile Terminal
CDPD	Cellular Digital Packet Data

Acronym/ Abbreviation	Expansion
ASCII	American Standard Code for Information Interchange

Referring now to Figure 1, there is shown a block diagram of the main components in a system 100 for facilitating prepaid-type transactions according to an embodiment of the present invention. This system includes an application server (AS) 120 for processing transaction requests from at least one wireless device 122, such as a cellular telephone, the application server 120 is also capable of forwarding transactions to an acquiring financial institution 124a or an issuing financial institution depending on whether the transaction is, respectively, a credit card transaction or a real time payment (RTP) transaction. A real time payment transaction refers to a payment mechanism where funds from the purchaser's bank account are debited in near real time. The system 100 also includes a merchant wallet server (MWS) 126, which acts as a proxy between a Virtual Terminal Server (VTS) and one or more electronic wallets (e-Wallets) 130 containing user credit card numbers, bank ATM card numbers or bank account numbers, stored value account numbers, billing addresses and shipping addresses stored in a carrier subscriber database 132. The MWS is able to extract information from the e-wallets 130 and present them in a form that can be used by the VTS. In effect, the MWS acts as a front end to the VTS, enabling the support of m-commerce.

Credit card and RTP transactions may also be sent through a transaction gateway server (TGS) 134 to the acquiring bank's 124a interface.

The system 100 may also include carrier's IVR server 136, which transmits payment information to the AS. Payment information captured by a carrier's IVR system is sent to the AS in the same manner as that of a WAP enabled phone. Information entered by the IVR system is combined with information stored at the carrier's subscriber database. Credit card and RTP transactions are then routed to a TGS. The

TGS is an optional intermediary in communication with the various financial institutions.

5 The prepaid transactions of the present invention are facilitated by payment applications (PA) running on the AS. The AS is a multi-application server, which allows for a variety of different payment methods and tender types. The payment applications have support for tender types such as credit card, cash, cheque, and e-Wallets. The e-Wallets themselves may contain references to credit cards, bank
10 accounts, and stored value accounts. In addition, the payment application has an Enterprise Reporting feature allowing reports on usage per subscriber. An important feature of the AS is the ability to route the prepay transactions to the appropriate processing interface based on the payment type. In the case of WAP enabled digital phones, the owner of the prepaid mobile device communicates with the AS via the
15 payment application residing on the AS. Information entered by the user, along with information kept within the carrier's prepaid database / e-Wallet is aggregated in the AS. The AS handles payment types as described below.

The payment types supported by the system 100 are generally credit card transactions
20 and RTP transactions. With each of these payment types, there are different levels of device 122 and user authentication, different interface requirements, and differences in response mechanisms. The transaction types implemented will require mutual resolution and agreement between the parties.

Non-Face-To-Face Transactions Using Credit Cards

25 In a credit card transaction, only the credit card number of the prepaid user is stored in a subscriber e-Wallet 130. This is what is currently used to effect Internet based payment. There is no authentication for the card or account, no authentication of the owner of the card or account and no authentication of the owner's intent to complete the transaction as is evidenced in a card present credit card transaction when the card
30 is swiped and the owner signs the receipt or as is evidenced in an on-line debit transaction when the card is swiped and the owner of a debit card enters a secret PIN

associated with the debit card. Rather, this type of transaction is typically called a Mail Order Telephone Order (MOTO) transaction. This does not fulfill general requirements of a go-to-market strategy for m-Commerce as these types of transactions can be easily repudiated and hence are highly subject to fraud. This invention enables m-commerce transactions that can generally not be repudiated. This invention meets the general requirements for non-repudiation of ensuring that the transaction process itself requires something that only the consumer has in possession and that the consumer intended to complete the transaction by requiring consumer to securely disclose to the system, something that only the consumer knows. The challenge of m-Commerce to achieve this is made even more difficult as often, the consumer and the merchant are not face-to-face as is the case with a an on-line credit card or an on-line debit card transaction.

Credit Card with Subscriber Device Authentication

Subscriber handset identities (SID) are commonly used within cellular networks to authenticate user phones. In this case, a credit card number is associated with the phone's secure identity to satisfy the concept of a virtual card. Currently, to effect a card present transaction, the card must be physically swiped and the data (called track2 data) on the magstripe of the card must be captured. If a trust relationship is set up between the carrier and the financial institution, the combination of the phone's secure identity and credit card number represents an equivalent risk to a card present transaction. This may be referred to as a "virtual card present transaction".

Credit Card with Subscriber Device & Password Authentication

Building on the virtual credit card transaction, a password can be associated with the subscriber's e-Wallet. The password is used to authenticate the owner of the e-Wallet (i.e. the subscriber), allowing access to the associated virtual credit card contained in the e-Wallet. User authentication lowers the risk of fraud involved in using a virtual credit card. By agreement between the owner of the e-Wallet and the e-Wallet service provider, the use of a password to authenticate the subscriber can be considered as a replacement for a signed receipt for purposes of non-repudiation.

RTP through EFT

The AS can route RTP transactions via the TGS to an Electronic Funds Transfer (EFT) interface of banks. This mechanism transfers money from the subscriber's bank account to the merchant's bank account overnight. The attractiveness of EFT is the ability to handle transactions for all banks through one interface. The EFT backend deals with the transfer of funds between the individual banks. A limitation of the EFT interface is that payment transfers are typically delayed up to 24 hours, and are not immediate. Responses are typically batched into one file and extracted from the EFT interface, when the file is available. Therefore, prepay top up transactions may take up to 24 hours before receiving a response from the bank, hence failing to meet a real time acknowledgement requirement.

This delay is addressed in one of several ways. A first option is that the financial institution processes and acknowledges an EFT transaction in real time in a scenario where the merchant (i.e. carrier) account and subscriber account is within its own domain. A second option is that a notification is sent to the subscriber some time in advance when the number of minutes still remaining in the subscriber's prepay account is below a certain level so that the 24-hour delay is inconsequential.

RTP through Real Time Payment Gateway

The AS can route RTP transactions via the TGS to evolving bank interfaces. The goal of these interfaces is to process funds transfer transactions in real time. Transactions belonging to the bank, hosting the interface, may be processed in real time. These interfaces, often based on XML standards such as OFX, provide a real time confirmation for a given transaction, unlike an EFT interface. Real time responses allow a subscriber to issue a payment transaction online and wait for the acknowledgement. Within this scenario the financial institution can only process and acknowledge transactions in real time when the subscriber holds an account at that bank.

Debit Transactions

With Debit transactions networks such as the Interac[™] network the underlying principles of authentication can be satisfied with today's cellular security and

authentication technologies, hence making debit transactions acceptable, most especially in the closed environment of prepay.

As described earlier, the MWS acts as a proxy between the VTS and e-Wallets that
5 hold subscriber credentials. The MWS combines information from e-Wallets and
information entered from either the carrier's IVR system or the WAP based prepay
application. The information is used to construct a credit or RTP transaction. Once a
successful response message is received, the MWS is responsible for notifying both
the user of the mobile device, and the carrier's prepay subscriber database. The
10 response can be sent to the WAP based prepay application or the carrier's IVR
system. In the case that the subscriber database held at the carrier receives a
successful response, the appropriate amount is added to the user's prepaid account.

Another feature of the MWS is the ability for a merchant to be authenticated as part of
15 the transaction. Merchant credentials can be securely stored within the MWS and can
be included in the transaction details, if the bank requires. This is a major step
towards having the ability to authenticate both the subscriber and the merchant in a
financial transaction. Optionally, if a PKI-enabled MWS is used, merchant
credentials can be encrypted and digitally signed before sending the authentication to
20 the bank. There are three e-Wallet configurations that the MWS supports.

Bank Hosted Wallet Server 140

The bank may choose to hold all of the subscriber's credentials within their own e-
Wallet. The carrier's subscriber database is used as an authentication mechanism to
enable payment through the bank e-Wallet. One authentication scheme involves the
25 use of a token, which is stored at the subscriber database held at the carrier, and that
token is used to extract subscriber credentials within the bank e-Wallet. This token
can take the form of a PKI public key or certificate. If the prepay user has multiple e-
Wallets with different banks, the carrier's subscriber database facilitates an
authentication mechanism for each of the e-Wallets.

Carrier Hosted Wallet Server 130

The MWS can operate in an environment where a carrier hosts an e-Wallet. User information, along with credit card numbers and bank account numbers is held within the carrier's e-Wallet. This information is sent to the MWS, when a prepay top up transaction is being constructed. There is also a method for the MWS to update the user prepay account information at the carrier's subscriber database. In this scenario, the carrier subscriber database is proxied by the e-Wallet server. Therefore, once a response from a top up transaction is received, the MWS passes the details of the response to the e-Wallet server. The e-Wallet server, in turn, updates the users prepay account information held within the subscriber database.

Carrier and Bank Jointly Hosts the Wallet Server

The bank may choose to hold some of the e-Wallet credentials such as bank account information. They may also choose to hold only those credentials pertaining to the particular bank. This is an example of a multiple e-Wallet implementation. The MWS is capable of supporting connections to multiple e-Wallet servers whether they are hosted at the carrier or the bank.

While the overall system components, and payment types handle by the system have been describe above, the security mechanism implemented by the system 100 is now described.

Device Authentication

A device can be authenticated before any interactions with a financial institution. Carriers use subscriber identity authentication mechanisms and other security measures to safeguard the security and identity of a cellular phone. This technology, especially in the digital space has proven effective in authentication of mobile phones. The MWS solution builds on the carrier's authentication mechanisms. A devices authenticated identity is associated with a credit card number creating the notion of a virtual credit card. In actuality, the carrier's authentication procedure will enable the first step in granting access to a subscriber's e-Wallet that contains a subscriber's virtual credit cards. A password is used to authenticate the owner of the e-Wallet and

forms the second step in granting access to transact with the virtual credit cards in the e-Wallet.

User Authentication

To enable a prepay transaction, the carrier may choose to authenticate the user before
5 accepting the transaction. There may be one or more passwords depending on the payment method. Typically, an e-Wallet password will be required to initiate a top up transaction. A second password may be needed to affect an RTP transaction. This is similar to an online bill payment scenario, where typically a username and password is required. The subscriber handset identity (SID) is used in place of the username.
10 By agreement between the owner of the e-Wallet and the e-Wallet service provider, the use of a password to authenticate the subscriber can be considered as a replacement for a signed receipt for purposes of non-repudiation. PKI technologies will be implemented as these technologies mature within cellular devices.

Communication between Infrastructure Components

15 Standard Secure Sockets Layer (SSL) communications protocols are implemented on wide-area communications.

Referring to figure 2, there is shown another embodiment of the system 200 of the
20 present invention. The system 200 comprises four interfaces into the AS, namely a carrier IVR system, carrier WAP gateway, carrier subscriber database via the e-Wallet, and the financial institution's acquiring interface via the TGS. It is noted that the carrier subscriber database is represented as an entity that accepts transaction responses and exception codes.

25 This implementation builds on the existing carrier infrastructure and requires only changes to the carrier's IVR system interface so that the IVR system communicates with the AS. All other four interfaces stay intact.

Prepay top up transactions can originate from either the carrier's IVR system or a
30 WAP enabled phone. The IVR system communicates via an IP based connection into the AS business logic. XML based communications protocols may be used.

Whereas, the WAP enabled phone will access a prepay application hosted at the AS. Although, both mechanisms use different input strategies, the backend processing does not change.

5 The e-Wallet function has been split up into two components. The first component is an implementation of a simple e-Wallet for storage of subscriber payment information. The second component is the subscriber database that is currently in use at the carriers. When a top up transaction is created, user credentials are retrieved from the e-Wallet. This information is combined with the information entered by the
10 user to affect the transaction. Once a transaction response has been received, an account update request is sent from the MWS to the subscriber database via the e-Wallet server. Both types of payment types are supported: credit card, and RTP.

Referring to figure 3, there is shown a further embodiment of an implementation of
15 the system 100. In this scenario, the subscriber prepay database function has been separated from the client e-Wallet server. Once a transaction response has been received, an account update request is sent from the MWS directly to the subscriber database. Transaction details may be sent to the e-Wallet server to provide the subscriber with a transaction history.

20

Referring to figure 4, there is shown a ladder diagram describing a first use case for the embodiment of figure 3. This use-case describes a subscriber initiated prepay via WAP Phone scenario.

25 This scenario is a two-step transaction. The subscriber is involved in two phone sessions, where the second session is used as a further subscriber authentication step. The first session involves the subscriber affecting a prepay application. The prepay application may be accessible from either the WAP browser's default menu or by typing the URL of the application. The second session involves pushing an alert back
30 to the subscriber. The second step removes the possibility that the original prepay transaction was not initiated by the intended subscriber. The subscriber ID of the

mobile device held within the e-Wallet defines the destination device of the push alert.

Each of the steps in the ladder diagram of figure 4 may be described as follows:

1. The subscriber enters the URL of WAP prepay application.
- 5 2. The carrier network validates ESN and MIN of subscriber phone.
3. Secure session is initiated with WAP gateway and prepay application host – the subscriber ID (SID) of the phone is passed to the application in the request header.
- 10 4. The subscriber is prompted by the prepay application for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.
- 15 5. Prepay application builds an XML based message and sends the message to the MWS. The request will minimally contain the SID for device authentication and optionally a password for subscriber authentication.
6. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
- 20 7. Based on the SID, the subscriber's credentials are extracted from the e-Wallet. Optionally, if a password has been specified, the SID and password pair is authenticated against the SID and password held in the e-Wallet.
- 25 8. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
9. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay

transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the SID extracted from the e-Wallet is sent to enable the WAP push mechanism in the next step.

- 5
- 10
- 15
- 20
- 25
10. The web server generates a WAP push message out to the subscriber device. The destination device can be determined by the SID. The push message can take the form of a real WAP push message through the WAP browser, or an indirect WAP push through the SMS messaging mechanism of the phone. In either case, the push message will contain a URL for triggering the prepay transaction. To complete the authentication loop, the URL will consist partly of the transaction ID of the temporary prepay transaction held at the MWS.
 11. The subscriber authorizes the prepay transaction by selecting the URL and confirming the transaction.
 12. The prepay web server sends a second XML based request to the MWS, which is an authorization request (confirmation) of the original prepay transaction.
 13. The MWS sends the payment request to the VTS using an XML based protocol.
 14. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.
 15. The TGS processes the transaction through the financial payment gateway.
 16. The TGS receives a transaction response from the financial payment gateway.
 17. The transaction response is routed back from the TGS to the VTS.
 18. The transaction result is passed from the VTS to the MWS.

- 5 19. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the subscriber device. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.
- 10 20. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.
21. To update the subscriber's device, the prepay result is sent from the MWS to the payment application.
- 15 22. The payment application generates a WAP push on the subscriber's device notifying the subscriber the prepay transaction has been processed.

20 Referring to figure 5, there is shown a ladder diagram describing a second use case for the embodiment of figure 3. This use case describes a System Initiated Prepay Via WAP Phone scenario.

25 This scenario is a one-step transaction. Unlike the subscriber initiated prepay, described with reference to figure 4, we are certain that the push alert will arrive at the intended subscriber device. A process continuously monitors the prepay database. If a subscriber's prepay amount falls below a certain threshold, a push alert is generated from the system. The subscriber acts on this push alert to affect a prepay transaction.

Each of the steps in the ladder diagram of figure 5 may be described as follows:

- 30 1. A database trigger is setup within the prepaid database. Once a subscriber's prepay amount falls below a certain threshold, an event is

generated and a request is made to the MWS to initiate a prepay transaction. The request will also contain a reference to the subscriber record within the e-Wallet.

- 5 2. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
- 10 3. The subscriber's credentials are extracted from the e-Wallet. Since the system is initiating a prepay request, the password held at the e-Wallet does not need to be validated.
4. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
- 15 5. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the SID extracted from the e-Wallet is sent to enable the WAP push mechanism in the next step.
- 20 6. The web server generates a WAP push message out to the subscriber device. The destination device can be determined by the SID. The push message can take the form of a real WAP push message through the WAP browser, or an indirect WAP push through the SMS messaging mechanism of the phone. In either case, the push message will contain a URL for triggering the prepay transaction. To complete the authentication loop, the URL will consist partly of the transaction ID of the temporary prepay transaction held at the MWS.
- 25 7. The subscriber authorizes the prepay transaction by selecting the URL and confirming the transaction. The subscriber is also prompted for
- 30

additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.

- 5 8. The prepay web server sends an XML based request to the MWS, which is an authorization (confirmation) of the prepay transaction.
9. The MWS sends the payment request to the VTS using an XML based protocol.
- 10 10. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.
11. The TGS processes the transaction through the financial payment gateway.
12. The TGS receives a transaction response from the financial payment gateway.
- 15 13. The transaction response is routed back from the TGS to the VTS.
14. The transaction result is passed from the VTS to the MWS.
- 20 15. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the subscriber device. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.
- 25 16. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.
17. To update the subscriber's device, the prepay result is sent from the MWS to the payment application.

18. The payment application generates a WAP push on the subscriber's device notifying the subscriber the prepay transaction has been processed.

5 Referring to figure 6, there is shown a ladder diagram describing a third use case for the embodiment of figure 3. This use case describes a Subscriber Initiated Prepay Via IVR System scenario.

This scenario is a two-step transaction. The subscriber is involved in two IVR
10 sessions, where the second session is used as a further subscriber authentication step. The first session involves the subscriber affecting a prepay application. The second session involves pushing an alert back to the subscriber. The push alert takes the form of a phone call to the subscriber device. The second step removes the possibility that the original prepay transaction was not initiated by the intended subscriber. The
15 phone number (Mobile Identity Number, MIN) held within the e-Wallet defines the destination device of the push alert.

Each of the steps in the ladder diagram of figure 6 may be described as follows:

- 20 1. The subscriber dials the IVR system through the subscriber's device. The prepay application is selected from the list of options.
2. The carriers network validations ESN and MIN of subscriber phone.
3. The subscriber is prompted by the IVR system for additional field information to complete the transaction. Fields may include prepay
25 amount, credit card or real-time payment (RTP) information.
4. The IVR system builds the appropriate XML based message and sends the message to the MWS. The request will minimally contain the MIN
30 for device authentication and optionally a DTMF password for subscriber authentication. The assumption is that caller ID is activated for the subscriber's device; therefore, the IVR system receives and passes through the MIN of the phone.

5. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
- 5 6. Based on the MIN, the subscriber's credentials are extracted from the e-Wallet. Optionally, if a password has been specified, the SID and password pair is authenticated against the SID and password held in the e-Wallet.
7. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
- 10 8. An XML based response message is sent back to the IVR system. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the MIN extracted from the e-Wallet is sent to enable the IVR callback in the next.
- 15 9. An IVR callback to the subscriber phone is performed using the MIN sent from the MWS. The IVR system outlines the transaction details to the subscriber. To complete the authentication loop, the IVR system will temporarily hold the transaction ID of the temporary prepay transaction held at the MWS.
- 20 10. The subscriber authorizes the prepay transaction through the IVR system.
- 25 11. The IVR system sends a second XML based request to the MWS, which is an authorization (confirmation) request of the original prepay transaction.
12. The MWS sends the payment request to the VTS using an XML based protocol.

13. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.
14. The TGS processes the transaction through the financial payment gateway.
15. The TGS receives a transaction response from the financial payment gateway.
16. The transaction response is routed back from the TGS to the VTS.
17. The transaction result is passed from the VTS to the MWS.
18. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the IVR system. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.
19. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.
20. To update the subscriber device, the prepay result is sent from the MWS to the IVR system.
21. The IVR system calls the subscriber's device notifying the subscriber the prepay transaction has been processed.

25

Referring to figure 7, there is shown a ladder diagram describing a third use case for the embodiment of figure 3. This use case describes a System Initiated Prepay Via IVR System scenario.

This scenario is a one-step transaction. Unlike the subscriber initiated prepay, we are certain that the IVR callback mechanism will arrive at the intended subscriber device. A process continuously monitors the prepay database. If a subscriber's prepay amount falls below a certain threshold, an IVR phone call is generated from the system. The subscriber confirms through the IVR system to affect a prepay transaction.

Each of the steps in the ladder diagram of figure 7 may be described as follows:

1. A database trigger is setup within the prepaid database. Once a subscriber's prepay amount falls below a certain threshold, an event is generated and a request is made to the MWS to initiate a prepay transaction. The request will also contain a reference to the subscriber record within the e-Wallet.
2. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
3. The subscriber's credentials are extracted from the e-Wallet. Since the system is initiating a prepay request, the password held at the e-Wallet does not need to be validated.
4. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
5. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the MIN extracted from the e-Wallet is sent to enable the IVR callback mechanism in the next step.

6. The IVR system outlines the transaction details to the subscriber. To complete the authentication loop, the IVR system will temporarily hold the transaction ID of the temporary prepay transaction held at the MWS.
- 5 7. The subscriber authorizes the prepay transaction through the IVR system. The subscriber is also prompted for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.
- 10 8. The prepay web server sends an XML based request to the MWS, which is an authorization (confirmation) of the prepay transaction.
9. The MWS sends the payment request to the VTS using an XML based protocol.
- 15 10. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.
11. The TGS processes the transaction through the financial payment gateway.
12. The TGS receives a transaction response from the financial payment gateway.
- 20 13. The transaction response is routed back from the TGS to the VTS.
14. The transaction result is passed from the VTS to the MWS.
- 25 15. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the IVR system. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.
16. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may

optionally be viewable from the online customer care website as a prepay transaction history.

17. To update the subscriber device, the prepay result is sent from the MWS to the IVR system.
- 5 18. The IVR system calls the subscriber's device notifying the subscriber the prepay transaction has been processed.

Accordingly it may be seen that the system of the present invention provides a secure real-time top-up service that can be implemented in existing payment infrastructures.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, said method comprising the steps of:

- (a) receiving at an application server first information indicative of the transaction device authentication;
- (b) receiving at said application server second information for verification of said user; and
- (c) using both said first and second information to authorize top-up payment of said prepaid service from said financial institution.

2. A method as defined in claim 1, said prepaid service being a prepaid cellular phone.

3. A method as defined in claim 2, said first information being a hardware identification of said cellular telephone.

4. A method as defined in claim 2, said second information being a personal identification number (PIN) of said user.

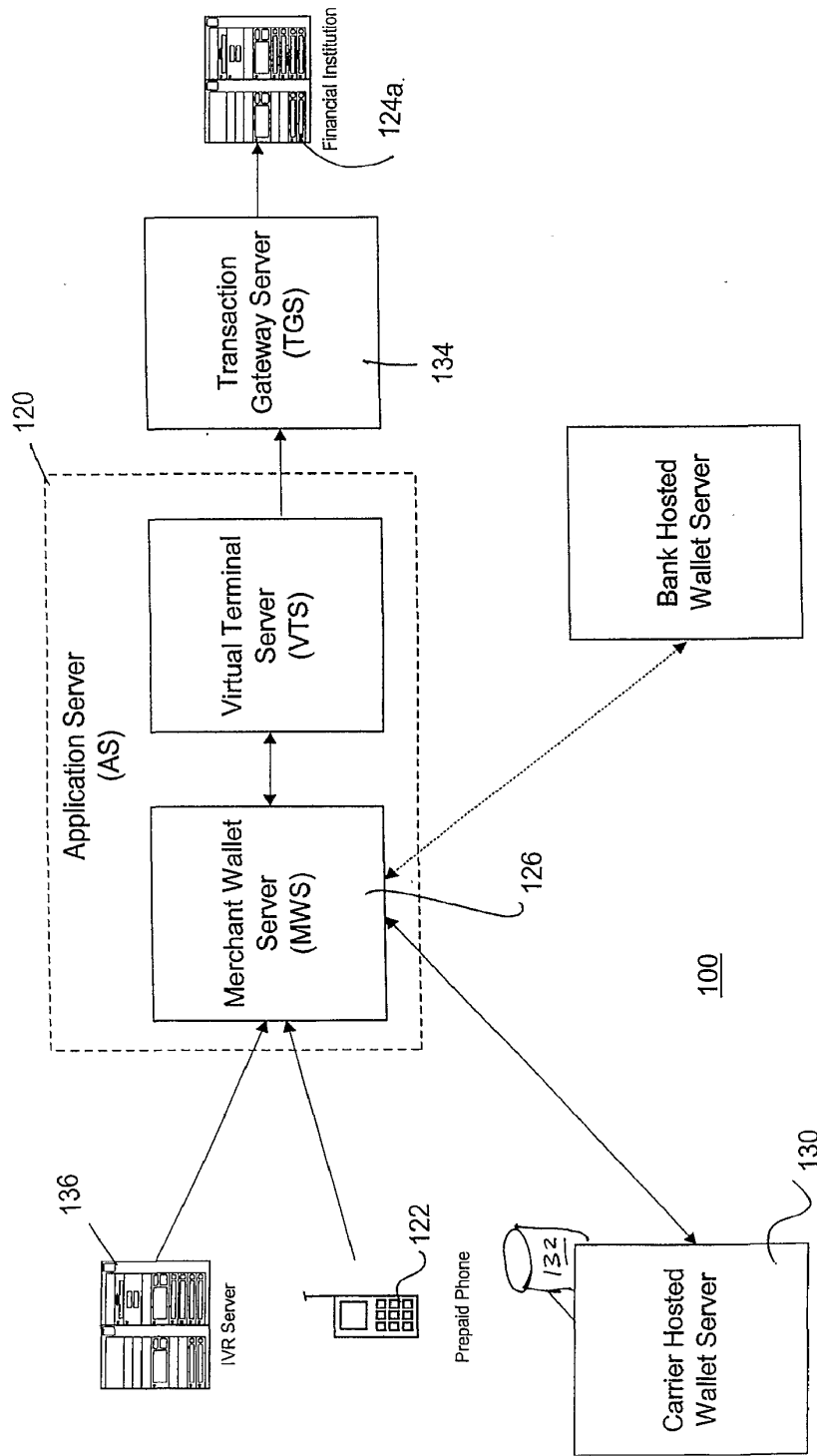


Figure 1

SUBSTITUTE SHEET (RULE 26)

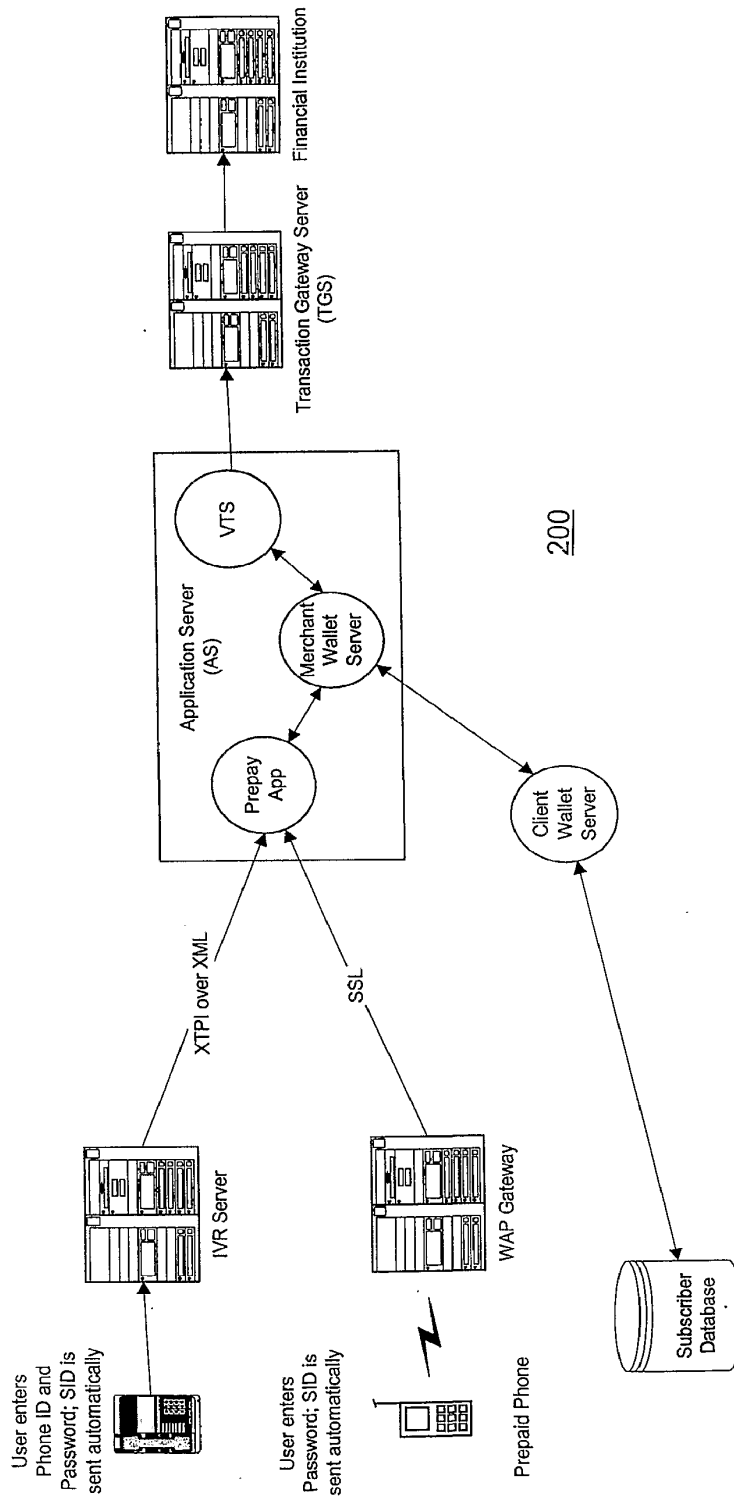


Figure 2

SUBSTITUTE SHEET (RULE 26)

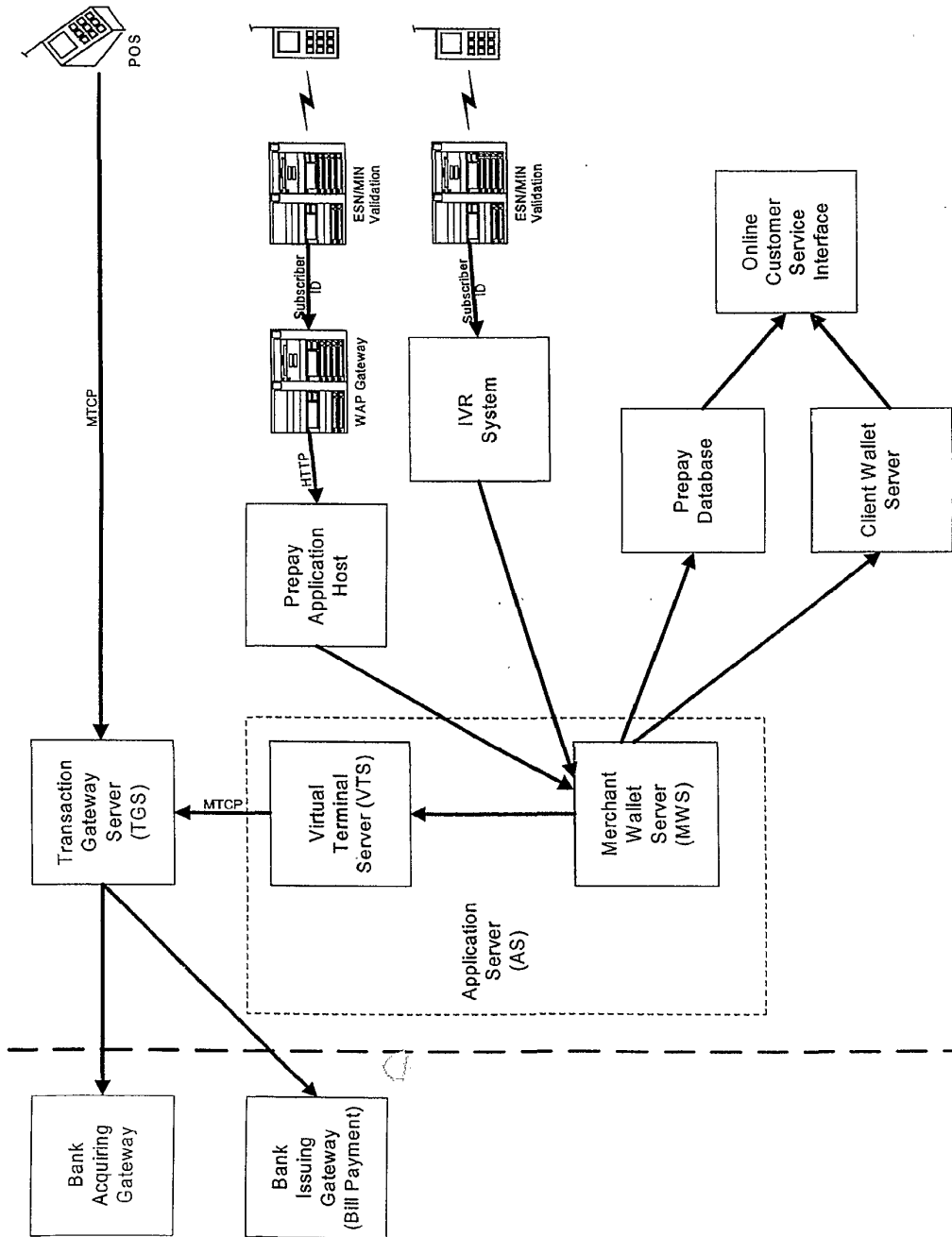


Figure 3

SUBSTITUTE SHEET (RULE 26)

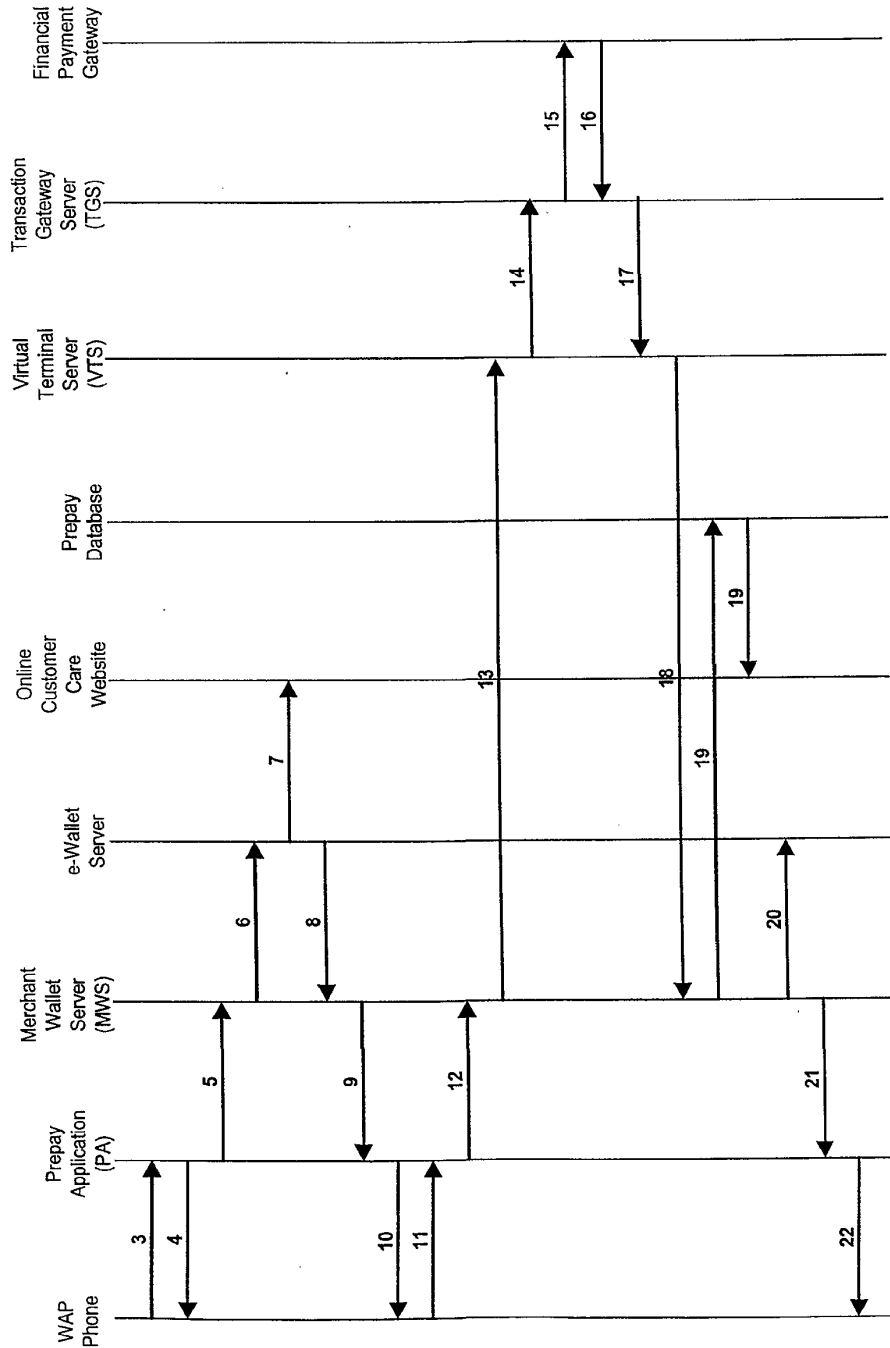


Figure 4

SUBSTITUTE SHEET (RULE 26)

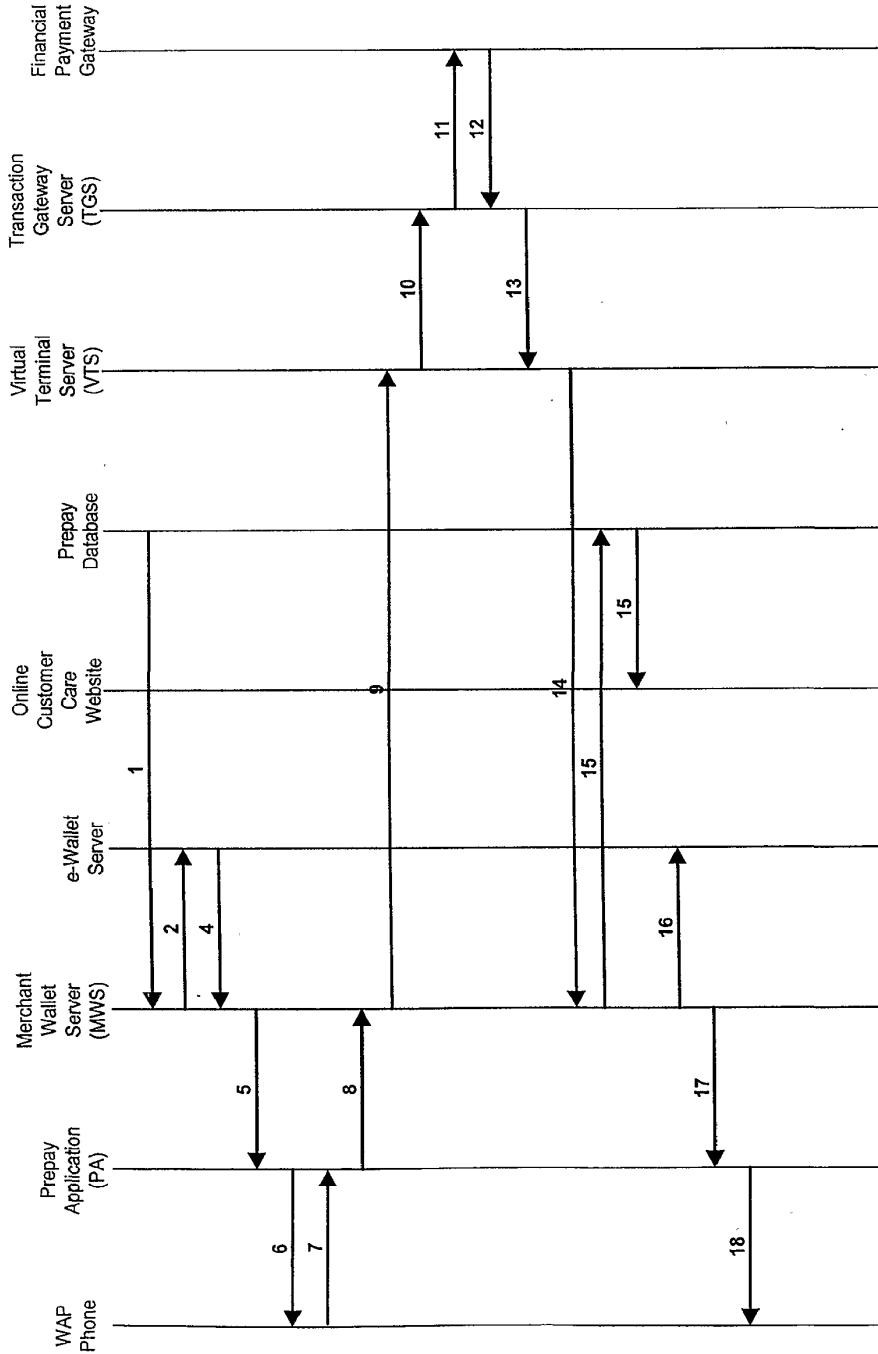


Figure 5

SUBSTITUTE SHEET (RULE 26)

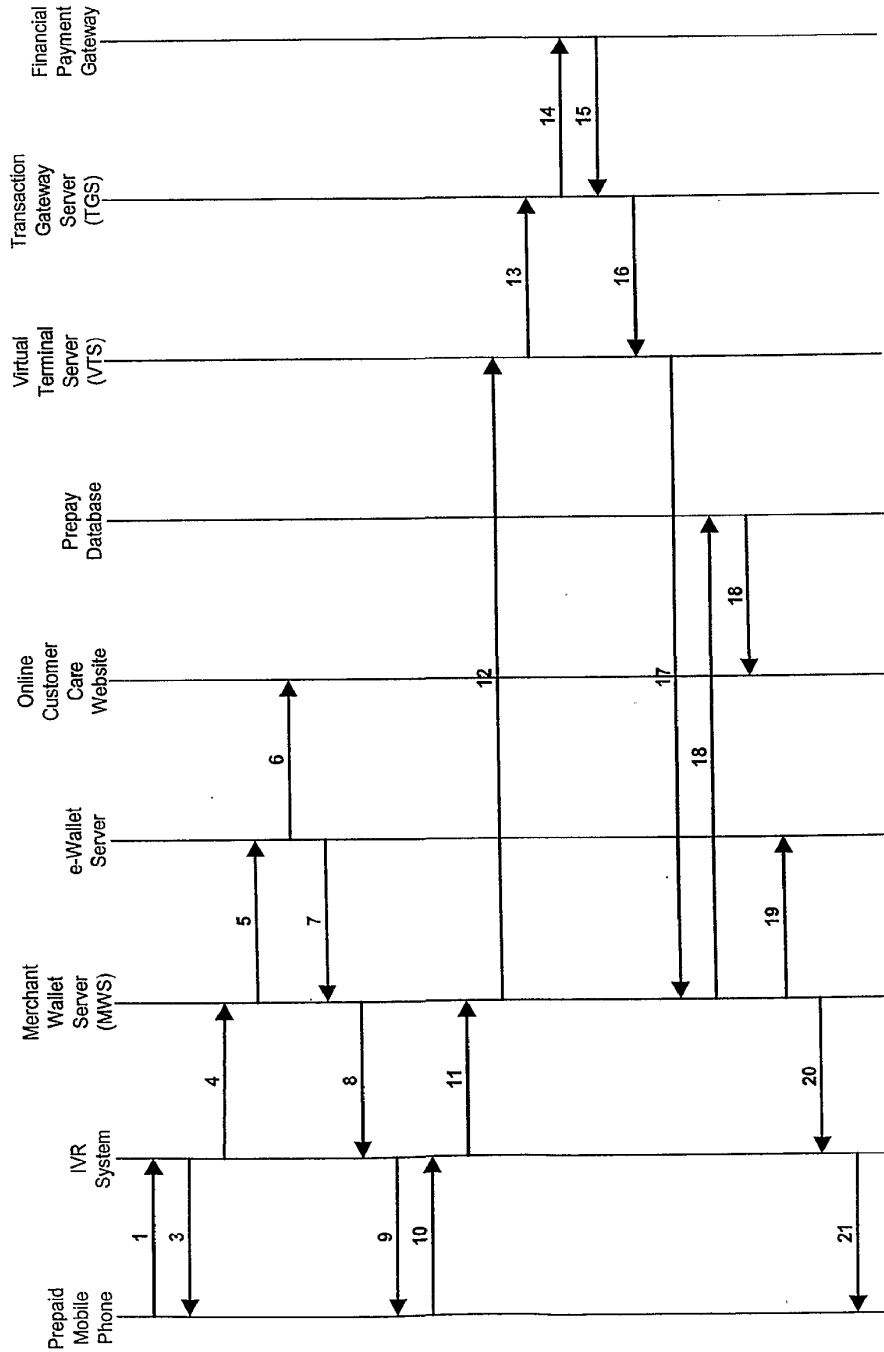


Figure 6

SUBSTITUTE SHEET (RULE 26)