159159

G00002

DESCRIPTION

ELECTRONIC-COMMERCE ASSISTING METHOD

Technical Field

The present invention relates to an electronic-commerce assisting method capable of smoothly and securely conducting electronic commerce on a communication network such as the Internet, and to an electronic-commerce assisting server for realizing the electronic-commerce assisting method. More particularly, the present invention relates to an electronic-commerce assisting method, in which a person desiring to purchase a product can pay using a credit card without letting the credit card number become known to another person, and the cybershop can prevent losses due to "posing", wherein a credit card number is illegally obtained, thus reducing the risk of charge back, and to an electronic-commerce assisting server for realizing the electronic-commerce assisting method.

Furthermore, the present invention relates to an electronic-commerce assisting method, in which costs required for countermeasures against leakage of card information in a cybershop and an NSP (Network Service Provider) having a membership server in which card information of members is stored can be reduced, and to an

electronic-commerce assisting server for realizing the electronic-commerce assisting method.

Background Art

Electronic commerce, that is, buying and selling of products and services (hereinafter simply called as "products") in cybershops or cybermalls, which is one use of cyberspace constructed on a communication network such as the Internet, has become active.

Current electronic-commerce transactions are dominated by credit sales wherein payment is settled after a predetermined period of time has elapsed from when the product was purchased. When purchasing a product in a cybershop or a cybermall, a person desiring to purchase a product completes a product purchase procedure by inputting credit card information using a browser displayed on a display device provided in a communication terminal such as a personal computer (hereinafter referred to as a "PC").

The inputting of credit card information in electronic commerce is usually performed in such a manner that the person desiring to purchase a product inputs data of only the credit card number or both the credit card number and the card expiration date using the browser, and then transmits the data to the cybershop.

The cybershop transmits the received data of the credit

card number, or the credit card number and the card expiration date to the credit card company via a dedicated line, etc. Based on the data, the credit card company confirms the validity of the credit card and the credit limit, and transmits the results to the cybershop. Based on the received confirmation results, the cybershop determines whether or not the product should be transferred. As a result, in electronic commerce, credit risk to the cybershop can be avoided.

Since the electronic commerce is conducted in cyberspace, and, unlike an actual shop, the person desiring to purchase a product and the shop are not face to face, forgery cannot be detected by actually confirming the credit card, and the signature written on the credit card cannot be verified. For this reason, it is very difficult for the cybershop to determine whether or not the credit card user in electronic commerce is a true user, and there is no effective means for preventing an illegal product purchase by someone illegally obtaining a credit card number of another person and posing as the card user (hereinafter referred to as "posing").

In this manner, there is no means for preventing fraud including illegally obtaining a credit card number by "posing". However, on the other hand, since the determining right for selling the product is on the shop side, the risk

of charge back (refund) for making up money lost by a true credit card owner and a credit card company due to the payment settlement for illegally purchased products is imposed on the shop.

The charge-back risk on the cybershop in electronic commerce is higher than that in actual transactions. In particular, in online shopping in which products such as marketable commodities are handled, a very high charge-back risk is imposed on the shop.

The cybershop constructs and manages a membership information database in which the credit card numbers of the members are stored in such a manner as to be associated with membership IDs and passwords. A strict security system needs to be organized so that credit card numbers of members cannot be illegally disclosed to a malicious hacker (cracker), and the cost of maintaining and controlling the security system is high enough not to be ignored.

On the other hand, the true credit card owner has a risk in that, if the credit card number of the owner is illegally obtained and abused, the owner becomes involved in trouble caused through no fault of his/her own and unnecessary dispute.

The presence of such a risk becomes a large factor for preventing the widespread use of electronic commerce. Therefore, in order that the credit card number is not

illegally obtained by another person on the Internet, for example, a technology for encrypting and transmitting credit card numbers (for example, SSL (Secure Socket Layer)) has been put into practical use. However, since the transmission data usually passes through a large number of unspecified nodes on the Internet until the data reaches its destination, simply by encrypting the data, it cannot be said that sufficient countermeasures against the risk of theft and falsification of data have been taken.

With respect to this, an NSP in which the following electronic-commerce assisting system is adopted has appeared. In this system, the membership IDs and the passwords of the registered members of the NSP are stored in the membership database in such a manner as to be associated with the credit card numbers.

When a member purchases a product in a cybershop which is affiliated with the corresponding NSP, the purchase procedure is completed by merely inputting the membership ID and the password. Based on the input membership ID and password, the NSP, instead of the cybershop, searches the membership database in order to specify the credit card number, requests the credit card company which handles the credit card to confirm the credit, and charges the credit card company on the basis of the credit card number. Since this system obviates the need for the cybershop to record

and hold the credit card numbers of the members, the cybershop is released from the risk of the card numbers being disclosed due to access by a cracker.

However, in this system, in order that the membership IDs and passwords are associated with the credit card numbers, it is necessary to transmit the data of the credit card number to the corresponding NSP over the Internet when the card number is registered at the first time, when the credit card is changed, or when the card number is changed. Therefore, at that time, there is a risk of the credit card number being stolen and used on the Internet. In place of this data transmission, notification of the credit card number using a telephone or a facsimile is possible. However, this is not practical because the procedure is complex and time-consuming, and security problems are likely to occur because the data is updated through human intervention.

According to this system, although the leakage of credit card numbers from the cybershop can be prevented, a strict security system needs to be provided in the membership information database at the NSP so that credit card numbers of members cannot be illegally obtained by a malicious hacker (cracker), and the cost of maintaining and controlling the security system is so high that it cannot be ignored.

On the other hand, for the point of view of the credit card owner, even though the above-described system makes it possible to avoid the risk that the card number is disclosed on the network in individual electronic-commerce transactions, when the card number is registered in a plurality of NSPs, the credit card number of the owner exists in a distributed manner in a plurality of membership databases on the network in a manner similar to the conventional case in which the card owner may worry that there is an increased chance of the card number being stolen and used. In the case where the membership ID also serves as the electronic mail address, if only the password is disclosed, it is possible for a recipient receiving electronic mail from that member to take "posing". Consequently, a security problem occurs, and also a situation occurs in which the recipient becomes unnecessarily suspected and is given trouble.

In addition to the above-described system, the following Internet settlement system has been proposed. In this system, when a person desiring to purchase a product connects to the Internet via a predetermined NSP and purchases a product from a cybershop, the transaction is concluded after an authentication assisting server queries the NSP on the basis of the IP address of the person desiring to purchase a product in order to identify that

person (U.S. Patent No. 5,899,980 is a related invention). In this system, since a payment settlement using a credit card is not used, as long as this system is used, the credit card number data will not be disclosed and will not be stored anywhere on the Internet. However, since in this system, electronic commerce using credit cards is not presupposed from the beginning, the leakage of credit card numbers does not become a problem, and does not solve problems arising from electronic commerce on the presumption of the use of credit cards on a communication network.

An object of the present invention is to provide an electronic-commerce assisting method capable of smoothly and securely conducting electronic commerce on a communication network, and an electronic-commerce assisting server for realizing the electronic-commerce assisting method.

Another object of the present invention is to provide an electronic-commerce assisting method in which a person desiring to purchase a product can pay using a credit card without letting the credit card number become known to another person, and an electronic-commerce assisting server for realizing the electronic-commerce assisting method.

Another object of the present invention is to provide an electronic-commerce assisting method capable of reducing the risk of charge back in a cybershop in credit sales in electronic commerce, and an electronic-commerce assisting

server for realizing the electronic-commerce assisting method.

Another object of the present invention is to provide an electronic-commerce assisting method capable of reducing costs required for countermeasures against leakage of card information in a cybershop and an NSP having a membership server in which card information of members is stored, and an electronic-commerce assisting server for realizing the electronic-commerce assisting method.

Disclosure of the Invention

The aforementioned object can be achieved by an electronic-commerce assisting server for assisting a user in the purchase of products or services, the electronic-commerce assisting server comprising: a management section for managing credit card numbers and unique numbers differing from the credit card numbers stored in a credit card in such a manner that these are associated with each other for each user; a transmission section for transmitting an instruction for a settlement to the user when a request of the settlement associated with the purchase is received; and a settlement section for performing a settlement by converting the unique number received in such a manner as to correspond to the instruction into a credit card number inside the management section.

In the electronic-commerce assisting server of the present invention, the management section further manages personal attribute information in such a manner as to be associated therewith, the instruction for a settlement containing an instruction for requesting an input of the personal attribute information, and the settlement section performs personal identification authentication using the personal attribute information received in such a manner as to correspond to the input, and performs a settlement.

In the electronic-commerce assisting server of the present invention, the personal information contains one or more of the telephone number information, the name information, the birthday information, and the security code of the user.

The aforementioned object can be achieved by a settlement method performed on a computer used by a user when products or services are purchased, the settlement method comprising: a step of receiving an instruction for a settlement associated with the purchase; a step of operating a credit card in accordance with the instruction and transmitting a unique number differing from a credit card number stored in the credit card to an electronic-commerce assisting server; and a step of receiving the result in which a settlement is performed using the credit card number associated with the unique number in the electronic-commerce

assisting server.

The aforementioned object can be achieved by an electronic-commerce assisting method for assisting a user in the purchase of products or services, the electronic-commerce assisting method comprising the steps of: managing credit card numbers and unique numbers differing from the credit card numbers stored in a credit card in such a manner that these are associated with each other for each user; transmitting an instruction for a settlement to the user when a request of the settlement associated with the purchase is received; and performing a settlement by converting the unique number received in such a manner as to correspond to the instruction into a credit card number inside the management section.

The electronic-commerce assisting method of the present invention further comprises the step of: managing personal attribute information in such a manner as to be associated therewith, the instruction for the settlement containing an instruction for requesting an input of the personal attribute information; and performing personal identification authentication using the personal attribute information received in such a manner as to correspond to the input, and performing a settlement.

In the electronic-commerce assisting method of the present invention, the personal information contains one or

more of the telephone number information, the name information, the birthday information, and the security code of the user.

The aforementioned object can be achieved by an electronic-commerce assisting program for assisting a user in the purchase of products or services, the electronic-commerce assisting program comprising the steps of: managing credit card numbers and unique numbers differing from the credit card numbers stored in a credit card in such a manner that these are associated with each other for each user; transmitting an instruction for a settlement associated with the purchase to the user when a request of the settlement associated with the purchase is received; and performing a settlement by converting the unique number received in such a manner as to correspond to the instruction into a credit card number inside the management section.

The electronic-commerce assisting program of the present invention further comprises the steps of: managing personal attribute information in such a manner as to be associated therewith, the instruction for the settlement containing an instruction for requesting an input of the personal attribute information; and performing personal identification authentication using the personal attribute information received in such a manner as to correspond to the input, and performing a settlement.

In the electronic-commerce assisting program of the present invention, the personal information contains one or more of the telephone number information, the name information, the birthday information, and the security code of the user.

Brief Description of the Drawings

Fig. 1 shows the network configuration in an electronic-commerce assisting server 1 according to an embodiment of the present invention.

Fig. 2 shows the overall configuration of a communication terminal 2 in the electronic-commerce assisting server 1 according to the embodiment of the present invention.

Fig. 3 shows the overall configuration of an IC card 10 used in the electronic-commerce assisting server 1 according to the embodiment of the present invention.

Fig. 4 shows an example of data within a customer database in the electronic-commerce assisting server 1 according to the embodiment of the present invention.

Fig. 5 chronologically shows the procedure of electronic commerce in the communication terminal 2 of a person desiring to purchase a product and an electronic-commerce server 46 in a cybershop in the electronic-commerce assisting server 1 according to the embodiment of the

present invention.

Fig. 6 shows an example of a screen displayed on a browser of the communication terminal 2 of a person desiring to purchase a product in each operation procedure of the electronic-commerce assisting server 1 according to the embodiment of the present invention.

Best Mode for Carrying Out the Invention

Referring to Figs. 1 through 6, a description will be given of an electronic-commerce assisting method and an electronic-commerce assisting server for realizing the electronic-commerce assisting method according to an embodiment of the present invention. The overall configuration of the electronic-commerce assisting server according to this embodiment will be described first with reference to Fig. 1.

Fig. 1 shows the network configuration in the embodiment of the present invention. As shown in Fig. 1, in an electronic-commerce assisting server 1 according to this embodiment, cybershops 40 and 42 (two shops are shown as an example in Fig. 1) which are connected to a communication network and which are opened in cyberspace, and a communication terminal (one communication terminal is shown as an example in Fig. 1) 2 of a person desiring to purchase a product, who accesses the cybershops 40 and 42, etc., in

order to purchase a product, exist.

A communication network 32 is a network of either a domestic or an international value-added communication network (VAN), or in which these are combined. As a combined example of a domestic and an international value-added communication network, there is the so-called Internet. Furthermore, for example, a communication network containing a digital public telephone line, such as a packet communication network and ISDN, which is used to transfer data in a cellular phone, etc., as a component of the network, is also included. Furthermore, a communication network in which a digital television broadcast network (including both wireless and wired communication such as a cable television), a public telephone line, etc., are linked, is also included. In the manner described above, the communication network 32 of this embodiment has a wide concept including one of these various forms of communication broadcast networks and a combined unit thereof.

For example, when the communication network 32 is the Internet, the communication terminal 2 of the person desiring to purchase a product is a work station or a PC having an electronic-mail transmission/receiving function and a browser function, and the communication terminal 2 is connected to the communication network 32 through an ISP (Internet service provider (one form of NSP)) 30 via a

communication line 6 such as a dedicated line or a public line. The browser has a function for accessing a predetermined URL (Uniform Resource Locator) on the Internet and for displaying a home page. The communication terminal 2 of the person desiring to purchase a product is able to obtain product information by accessing the cybershops 40 and 42 on the Internet via the browser and to transmit the intent of purchasing a product.

The cybershops 40 and 42 has an electronic-commerce server 46 for processing various requests relating to the purchase of products from the communication terminal 2 of the person desiring to purchase a product, so that product information can be provided to the communication terminal 2 of the person desiring to purchase a product on the Internet, and data for carrying on with a product purchase procedure is transmitted to or received from the communication terminal 2 of the person desiring to purchase a product.

Furthermore, for example, when the communication network 32 is a network including a packet communication network, the communication terminal 2 of the person desiring to purchase a product is a cellular phone having an electronic-mail transmission/receiving function and a browser function, so that data can be transmitted to or received from the cybershops 40 and 42 via the packet communication network.

With remarkable advances in information technology (IT) in recent years, a use of a communication network using PCs has become easy. Furthermore, electronic commerce using the communication terminal 2 including at least one of a cellular phone, a personal handyphone system (PHS (registered trademark)), and a portable information terminal has come to be conducted frequently and extensively, and services in which cellular phones are used as connection terminals for the Internet have already started. For example, in i-mode (registered trademark of NTT DoCoMo, Inc.) provided by NTT DoCoMo, Inc., a cellular phone having a browser function is connected to the Internet via an i-mode server in order to access the cybershops 40 and 42, making it possible to purchase a product.

In the electronic-commerce assisting system according to this embodiment, furthermore, an electronic-commerce assisting server 44 is connected to the communication network 32. The electronic-commerce assisting server 44 responds to an authentication assisting request output from the cybershops 40 and 42 via the communication network 32. Based on the IP address of the communication terminal 2 of the person desiring to purchase a product, sent from the cybershops 40 and 42 together with the authentication assisting request, the electronic-commerce assisting server 44 allows the browser of the communication terminal 2 to

display a screen for requesting the output of credit card information. It is possible for the electronic-commerce assisting server 44 to specify the card number of the credit card on the basis of the received credit card information.

For this purpose, the electronic-commerce assisting server 44 includes a management section for managing credit card numbers and unique numbers differing from the credit card numbers stored in a credit card in such a manner that these are associated with each other for each user; a transmission section for transmitting an instruction for a settlement to the user when a request of the settlement associated with the purchase is received; and a settlement section for performing a settlement by converting the unique number received in such a manner as to correspond to the instruction into a credit card number inside the management section.

Based on the specified credit card number, the management section of the electronic-commerce assisting server 44 accesses an authentication database (not shown) disposed within a credit card company, searches for credit OK/NG data of that credit card stored in the authentication database, generates the credit OK/NG data of the credit card of that card number, and transmits the data to the cybershops 40 and 42 from the transmission section.

Here, between the cybershops 40 and 42 and the

electronic-commerce assisting server 44, in addition to the connection by the communication network 32, a dedicated-line connection, an OBN (Open Business Network) connection, or an Internet VPN connection may be selected. OBN is an IP (Internet Protocol) service dedicated to businesses, disconnected from the Internet. OBN has a low cost, and a high-level security comparable to that of a dedicated line and high-speed communication using a wide band can be obtained in almost the entire area of Japan. The Internet VPN is a service in which the Internet can be used like a dedicated network. Although it is easy to make an overseas connection, there are cases in which the security is lower and the band is narrower compared to the above-described dedicated line and OBN.

Next, referring to Fig. 2, the overall configuration of the communication terminal 2 according to this embodiment will be described. The communication terminal 2 is connected to an ISP 30 via the communication line 6. A reading/writing device 4 for reading/writing various types of data from and into a storage device of the IC card 10 having a credit card function is connected to the communication terminal 2.

The communication terminal 2 has a display device 24 for displaying a browser screen and a printing device 26 for printing the screen. Also, the communication terminal 2 has

a control section 20 for centrally controlling all the devices and for performing various computation processes, and a storage device 22 for storing various types of data. The control section 20 stores various types of data of the IC card 10, input from the reading/writing device 4, into the storage device 22, reads predetermined data from the storage device 22, and performs a computation thereon.

Fig. 3 shows the overall configuration of the IC card 10 according to the embodiment. The IC card 10 has a credit card function. The IC card 10 has a storage device 12 formed of a semiconductor memory such as a flash EEPROM, a communication control section 16 and an antenna 18 for performing communication with the outside in a non-contact manner in order to transmit/receive data, and a control section 14 for centrally controlling them.

When the IC card 10 is held above the reading/writing device 4, transmission/reception of data using electromagnetic waves is performed between the antenna 18 of the IC card 10 and the antenna (not shown) within the reading/writing device 4. The electromagnetic-wave data has been encrypted by triple DES in which, for example, an encryption process based on a data encryption standard which is made public by U.S. National Bureau of Standards is performed in triple.

The storage device 12 within the IC card 10 has stored

therein unique number data for the electronic-commerce assisting server 44 to specify the credit card number of the card. The unique number data is written into the storage device 12 when the IC card 10 is issued from a credit card issuing company. The unique number is, for example, a code sequence, in which alphanumeric characters of about 16 to 24 digits coexist, which is formed of codes which have a one-to-one correspondence to the credit card number, but differ from that number.

At least the unique number data is sent as the credit card information to the electronic-commerce assisting server 44. Of course, the card expiration date, other personal identification information, and so on may be added as the credit card information. When a network other than a communication network of CAFIS, such as OBN, is to be used, personal attribute information other than the credit card number can be transmitted. In that case, as in the customer database shown in Fig. 4, the electronic-commerce assisting server 44 manages credit card numbers and unique numbers differing from the credit card numbers in such a manner as to be associated with each other, and also manages the personal attribute information in such a manner as to be associated therewith. The personal attribute information is attribute information associated with the owner of the credit card, for example, birthday information (4-digit

information of the year of birth, 8- or 6-digit information of the date of birth), telephone number information (including the whole or a part), a security code, and name information (including one or more combinations of surname in katakana, first name in katakana, surname written in English, and first name written in English). The phrase "manages in such a manner as to be associated with each other" may be such that, as shown in Fig. 4, the above may be managed by one database, and a plurality of databases may be used by using certain key information (for example, customer numbers (not shown), unique numbers, and credit card numbers) as in an RDB (Relational Database).

In this case, personal attribute information is not stored in the storage device 12 of the IC card. When the electronic-commerce server 46 instructs an operation of the credit card (the screen 56 of Fig. 6), a screen (e.g., a pop-up window) for instructing an input of personal attribute information is displayed together with the screen 56 of Fig. 6 so as to request the user to input the personal attribute information. In this case, the personal attribute information to be input may be one or more of the above. Furthermore, the number of pieces of personal attribute information to be input may be determined on the basis of the amount of the purchase. For example, for more than 2000 yen, one piece of personal attribute (security code) may be

input, and for more than 4000 yen, two pieces of personal attribute (security code and birthday information) may be input.

When the personal attribute information input by the user is received, the electronic-commerce assisting server 44 determines whether or not the input personal attribute information matches the information managed by the customer database illustrated in Fig. 4, and the electronic-commerce assisting server 44 may not allow the settlement when the whole or a part of the information (e.g., birthday information) does not match. When they match, the electronic-commerce assisting server 44 performs a settlement process. As a result of the above, even if a malicious third party obtains the credit card itself, since the malicious third party does not know the personal attribute information, a settlement process is not performed, and thus a more secure transaction environment can be provided to the user.

While referring to Figs. 1 through 4, the operation procedure in the electronic-commerce assisting server 1 having the above configuration will now be described further with reference to Figs. 5 and 6. A description will now be given by using an example in which a person desiring to purchase a product operates the communication terminal 2 so as to connects to the cybershop 40 which provides a home

page for electronic commerce on the communication network 32 (assumed to be the Internet). Fig. 5 chronologically shows the procedure of electronic commerce in the communication terminal 2 of a person desiring to purchase a product and the electronic-commerce server 46 and the electronic-commerce assisting server 44 in the cybershop 40 in the electronic-commerce assisting server 1 according to this embodiment. Fig. 6 shows examples of the screen displayed on the browser of the communication terminal 2 of the person desiring to purchase a product in each operation procedure.

Initially, the person desiring to purchase a product allows a Web browser to be displayed on the display device 24 of the communication terminal 2, and inputs a predetermined URL for the cybershop, so that a top page 50 of the cybershop shown in Fig. 6 is displayed via the communication network 32. Next, the person desiring to purchase a product positions the pointer of the mouse in, for example, a "product purchase site" button shown in the top page 50 and clicks the mouse button, so that a product purchase screen display request is sent (step S1).

The electronic-commerce server 46 receiving the product purchase screen display request displays a product purchase screen 52 shown in Fig. 6 on the browser of the communication terminal 2 (step S2). When the person desiring to purchase a product inputs the retrieval keyword

of a desired product from the product purchase screen 52 on the communication terminal 2, the electronic-commerce server 46 searches the product database (not shown) on the basis of the retrieval keyword input by the person desiring to purchase a product, and displays the searching result on the product purchase screen 52.

When the person desiring to purchase a product has found the desired product on the product purchase screen 52 displayed on the browser of the communication terminal 2, the person positions the pointer of the mouse in "purchase" and clicks the mouse button, so that a product purchase request is sent to the electronic-commerce server 46 (step S3).

The electronic-commerce server 46 of the cybershop receiving the product purchase request transmits the data of a payment method selection screen 54, shown in Fig. 6, for selecting a payment method, so that the data is displayed on the browser of the communication terminal 2 (step S4). Here, if the person desiring to purchase a product selects a payment settlement using a credit card, a credit-card settlement selection request is sent to the electronic-commerce server 46 (step S5).

When the credit-card settlement selection request is received, the electronic-commerce server 46 sends out a credit confirmation request together with the IP address of

the communication terminal 2 of the person desiring to purchase a product to the electronic-commerce assisting server 44 (step S6).

Based on the IP address of the communication terminal 2 of the person desiring to purchase a product, associated with the authentication assisting request, the electronic-commerce assisting server 44 transmits the data of an input prompting screen 56 of "Please hold up the card to the reading/writing device", shown in Fig. 6, to the communication terminal 2, whereby the data is displayed on the browser of the communication terminal 2 (step S7).

When the person desiring to purchase a product holds up the IC card 10 to the reading/writing device 4, at least the unique number data within the credit card information stored in the storage device 12 of the IC card 10 is received, as electromagnetic data encrypted by triple DES, by the reading/writing device 4. The encrypted unique number data received by the reading/writing device 4 is temporarily decrypted, then, an encryption process by SSL is performed thereon, and the resulting data is transmitted from the communication terminal 2 to the electronic-commerce assisting server 44 (step S8).

After the electronic-commerce assisting server 44 decrypts the received unique number data, the electronic-commerce assisting server 44 specifies the card number of

the credit card from the unique number data. The electronic-commerce assisting server 44 has a correspondence table of unique numbers and credit card numbers stored, for example, in a storage device (not shown), and based on the correspondence table, the electronic-commerce assisting server 44 specifies the card number of the credit card from the unique number data.

Based on the specified credit card number, the electronic-commerce assisting server 44 accesses an authentication database disposed inside the credit card company, searches for the credit OK/NG data of the credit card, stored in the authentication database, and generates credit OK/NG data of the credit card of that card number. Next, the electronic-commerce assisting server 44 transmits to the cybershop 40 the generated credit OK/NG data to which unique number data corresponding to the credit card number is attached (step S9).

Based on the received credit OK/NG data, the electronic-commerce server 46 of the cybershop 40 determines whether or not the credit of the card is allowed to conclude an electronic-commerce transaction (step S10).

When it is determined in step S10 that the credit cannot be allowed, a transaction unconclusion screen 60, shown in Fig. 6 is displayed on the browser of the communication terminal 2 so as to ask the person desiring to

purchase a product as to whether this processing should be terminated so as to cause the product transaction to be unconcluded, or the price should be paid by another method (step S11 indicated by the broken line in Fig. 5).

When it is determined that the credit can be allowed, a transaction conclusion screen 58, shown in Fig. 6, is displayed on the browser of the communication terminal 2 (step S12). Nearly in synchronization with the display of the transaction conclusion screen 58, the electronic-commerce server 46 of the cybershop 40 creates a sales file, and transmits to the electronic-commerce assisting server 44 the sales file to which the unique number data is attached (step S13).

In the electronic-commerce assisting server 44, the unique number data of the received sales file is converted into the credit card number, the settlement result is transmitted to the user, and when a predetermined deadline is reached for the credit sales volume by the card, the settlement section of the electronic-commerce assisting server 44 issues a bill for the person who has purchased the products (step S14).

As has been described in the foregoing, in this embodiment, since the unique number data instead of the credit card number is disclosed on the communication network 32, the credit card number of the person desiring to

purchase a product is not disclosed on the communication network 32, including the cybershops 40 and 42, and the ISP 30, or the credit card number is not stored in any node. Furthermore, also in the electromagnetic data communication between the IC card 10 and the reading/writing device 4, the unique number data leaks, and the credit card number is not transmitted or received.

As a result, the credit card owner can avoid the risk of the card number being disclosed on the communication network 32 and being stolen and used in individual electronic-commerce transactions. Furthermore, even if membership registration is made in a plurality of ISPs 30 and cybershops 40 and 42, the credit card number of the owner is not stored in a plurality of membership information databases connected to the communication network 32. Therefore, it is possible to greatly reduce the risk of the card number being stolen and used.

According to this embodiment, in electronic commerce, among those other than the true owner of the credit card, it is only the electronic-commerce assisting server 44 that can handle the credit card number. Furthermore, it is only the authentication database (not shown) of the credit card company, which can be accessed by only the electronic-commerce assisting server 44, where the credit card number is stored. That is, if the assisting system according to

this embodiment is used, an electronic-commerce system, in which the possibility of the credit card number being illegally obtained by a third party is considerably reduced, can be realized.

According to this embodiment, it is not necessary for individual cybershops 40 and individual ISPs 30 to construct and manage a membership information database in which credit card numbers of members are stored in such a manner as to be associated with member IDs and passwords. As a result, it is possible to greatly reduce the cost of maintaining and managing the security system for preventing illegal leakage of credit card numbers by a cracker.

In the manner described above, according to this embodiment, it is possible to realize an IC card by which electronic commerce on a communication network can be conducted smoothly and securely, and an electronic-commerce assisting method and system using the IC card. This makes it possible to make a payment which feels secure when using a credit card without letting the credit card number become known to another person in the electronic commerce.

According to this embodiment, it is possible to reduce the risk of charge back in cybershop, which occurs by an illegal electronic-commerce transaction as a result of "posing" in which the credit card number is illegally obtained. Furthermore, it is possible to reduce costs

required for countermeasures against leakage of card information in a cybershop and an NSP having a membership server in which card information of members is stored.

The present invention is not limited to the above-described embodiments, and various modifications are possible.

For example, although in the above-described embodiments, the electronic-commerce assisting server 44 requests unique number data from the communication terminal 2, this may be executed instead by the electronic-commerce server 46 of the cybershop 40.

However, the above-described embodiments in which the electronic-commerce assisting server 44 directly obtains unique number data have a higher security. In particular, when other credit card information, such as the card expiration date, the personal authentication data, and so on, is to be requested, preferably, the method of this embodiment in which the electronic-commerce assisting server 44 directly receives the transmission data from the communication terminal 2 is adopted.

The electronic-commerce assisting server 44 of the above-described embodiments specifies the card number of the credit card from the received unique number data on the basis of the correspondence table of unique numbers and credit card numbers, but the present invention is not

limited to this example. Of course, for example, the following method may be used in which a unique number is derived from the credit card number by using a predetermined algorithm and is stored in the IC card, and the credit card number is specified from the unique number data by a procedure reverse to the above.

An IC card in which unique number data is stored is issued from a specific credit card company. When the need to present, input, or transmit the credit card number occurs when a credit card is used in a shop which is not affiliated therewith, of course, the credit card number may be displayed on the surface of the IC card.

In the above-described embodiments, although a description is given by using a non-contact IC card as an example, the present invention is not limited to this example, and of course can be applied to a contact-type IC card. In this case, transmission/reception of data is performed by bringing the data reading/writing terminals of an IC card into contact with the data input/output terminals of a dedicated reading/writing device.

As described above, according to the present invention, it is possible to smoothly and securely conduct electronic commerce on a communication network.

According to the present invention, payment using a credit card can be conducted without letting the credit card

number become known to another person in electronic commerce.

In addition, according to the present invention, it is possible to reduce the risk of charge back in a cybershop in credit sales in electronic commerce.

Furthermore, costs required for countermeasures against leakage of card information in a cybershop and an NSP having a membership server in which card information of members is stored can be reduced

CLAIMS

1. An electronic-commerce assisting server for assisting a user in the purchase of products or services, said electronic-commerce assisting server comprising:

a management section for managing credit card numbers and unique numbers differing from said credit card numbers stored in a credit card in such a manner that these are associated with each other for each said user;

a transmission section for transmitting an instruction for a settlement to said user when a request of a settlement associated with the purchase is received; and

a settlement section for performing a settlement by converting said unique number received in such a manner as to correspond to the instruction into a credit card number inside said management section.

2. An electronic-commerce assisting server according to Claim 1, wherein said management section further manages personal attribute information in such a manner as to be associated therewith, said instruction for a settlement containing an instruction for requesting an input of said personal attribute information, and

said settlement section performs personal identification authentication using the personal attribute

information received in such a manner as to correspond to said input, and performs a settlement.

3. An electronic-commerce assisting server according to Claim 2, wherein said personal information contains one or more of the telephone number information, the name information, the birthday information, and the security code of said user.

4. A settlement method performed on a computer used by a user when products or services are purchased, said settlement method comprising:

a step of receiving an instruction for a settlement associated with the purchase;

a step of operating a credit card in accordance with the instruction and transmitting a unique number differing from a credit card number stored in said credit card to an electronic-commerce assisting server; and

a step of receiving the result in which a settlement is performed using said credit card number associated with said unique number in said electronic-commerce assisting server.

5. An electronic-commerce assisting method for assisting a user in the purchase of products or services, said electronic-commerce assisting method comprising the

steps of:

managing credit card numbers and unique numbers differing from said credit card numbers stored in a credit card in such a manner that these are associated with each other for each said user;

transmitting an instruction for a settlement to said user when a request of the settlement associated with the purchase is received; and

performing a settlement by converting said unique number received in such a manner as to correspond to the instruction into a credit card number inside said management section.

6. An electronic-commerce assisting method according to Claim 5, further comprising the steps of:

managing personal attribute information in such a manner as to be associated therewith, the instruction for said settlement containing an instruction for requesting an input of said personal attribute information; and

performing personal identification authentication using the personal attribute information received in such a manner as to correspond to said input, and performing a settlement.

7. An electronic-commerce assisting method according to Claim 6, wherein said personal information contains one

or more of the telephone number information, the name information, the birthday information, and the security code of said user.

8. An electronic-commerce assisting program for assisting a user in the purchase of products or services, said electronic-commerce assisting program comprising the steps of:

managing credit card numbers and unique numbers differing from said credit card numbers stored in a credit card in such a manner that these are associated with each other for each said user;

transmitting an instruction for a settlement associated with the purchase to said user when a request of the settlement associated with the purchase is received; and

performing a settlement by converting said unique number received in such a manner as to correspond to the instruction into a credit card number inside said management section.

9. An electronic-commerce assisting program according to Claim 8, further comprising the steps of:

managing personal attribute information in such a manner as to be associated therewith, the instruction for said settlement containing an instruction for requesting an

input of said personal attribute information; and

performing personal identification authentication using the personal attribute information received in such a manner as to correspond to said input, and performing a settlement.

10. An electronic-commerce assisting program according to Claim 9, wherein said personal information contains one or more of the telephone number information, the name information, the birthday information, and the security code of said user.