However, with the above-described systems, communication security at the time of service delivery is not sufficiently secured, and thus, it is creating a breeding ground for illegal use.

[0006]

The present invention is made in order to solve the above-described problem, and an object thereof is to provide a server system, and the like, that are capable of improving security at the time of delivering various kinds of services and that are capable of preventing illegal use.

Means for Solving the Problem

[0007]

(1) In order to solve the above-described problem, the server system~~, and the like,~~ of the present invention ha~~ve~~s:

a receiver that receives, via a network, data from a communication terminal device that communicates with and is connected to the server system;

a controller that controls a database in which table data is recorded in association with identification information for identifying a user, the table data being predetermined for each user of the communication terminal device and having entry target characters entered at the communication terminal device and figures pre-allocated to the respective entry target characters that are associated with each other;

a data specifying processer that specifies, when a given request designated by a user from the communication terminal device is received by the receiver, table data that corresponds to the user;

an extracting processer that extracts the figures that correspond to entry target characters to be specified by the user based on the specified table data;

a distributer that generates data for entry that is associated with each of the extracted figures and that includes marker information to be used when relevant figures are displayed at a relevant communication terminal device, and that distributes the generated data for entry to the communication terminal device;

an acquiring processer that acquires, when the figures are displayed at the communication terminal device based on the distributed data for entry, the marker information that corresponds to the figures entered by the user from the communication terminal device;

a determining processer that determines the relevant figures based on the acquired marker information; and

a processer that specifies the entry target characters to be specified based on the determined figures and that executes a given process based on the specified entry target characters.

[0008]

Based on this configuration, the server system, ~~and the like,~~ of the present invention makes use of figures when the user enters the entry target characters. Thus, the server system, and the like is capable of specifying account information (account number and remittance amount), authentication information (login information) or other information to be specified by the user, without directly entering such information to be specified by an input device such as a keyboard.

[0009]

Accordingly, the server system, ~~and the like,~~ of the present invention ~~are~~ is capable of preventing: the leakage of security-related information (for example, a password) caused by a user's carelessness, for example, by entering, all at once, at a phishing site, all of the information described in a number table, or the like, which is issued to the user in advance; and the transfer of information to a third party who performs an illegal login.

[0010]

In addition, the server system, ~~and the like~~, of the present invention makes use of the marker information, such as the display positions of the figures, instead of the entry target characters or the figures specifying the entry target characters, for the data communication between the communication terminal devices and the server systems. Thus, the server system, and the like, of the present invention is capable of preventing the information to be specified by a user from being stolen or tampered with by a third party, between the communication terminal device and the server system.

[0011]

Accordingly, the server system, and the like, of the present invention is capable of preventing illegal logins and man-in-the-middle attacks made by a third party to the services delivered to the users.

[0012]

Consequently, the server system of the present invention is capable of preventing the leakage of the security-related information, illegal uses and man-in-the-middle attacks, and of improving the security at the time of delivering various services including Internet banking service, or the like.

[0013]

(2) In order to solve the above-described problem, the communication terminal device, ~~and the like,~~ of the present invention is a communication terminal device that is connected to a

server system that executes various processes, via a network, and that deliver various services to a user while they transmit/receive data to/from such server systems, and the communication terminal device, and the like, of the present invention have a configuration in which the following units are provided:

an acquiring processer that acquires part of table data , along with control information for controlling, at least, display positions for displaying figures on a display, from the server system, the table data being table data predetermined for each user, the table data including entry target characters that are entered by the user and figures that are pre-allocated to the respective entry target characters, the entry target characters and the figures in the table data being associated with each other;

an receiver that receives an input operation of the user in accordance with an image displayed based on the acquired table data;

a specifying processer that specifies the display positions corresponding to the figures designated by the user in response to the input operation; and

a transmitter that transmits information that indicates the display positions corresponding to the specified figures to the server system.

[0014]

Based on this configuration, the communication terminal device of the present invention makes use of figures when the user enters the entry target characters. Thus, the communication terminal device of the present invention is capable of specifying account information (account number and remittance amount), authentication information (login information) or other information to be specified by the user, without directly entering such information to be specified by an input device such as a keyboard.

[0015]

Accordingly, the communication terminal device ~~server system, and the like, of~~ the present invention ~~are~~ is capable of preventing: the leakage of security-related information (for example, a password) caused by a user's carelessness, for example, by entering, all at once, at a phishing site, all of the information described in random number table, or the like, which is issued to a user in advance; and the transfer of information to a third party who performs an illegal login.

[0016]

In addition, the communication terminal device server system, and the like, of the present invention makes use of the marker information, such as the display positions of the figures, instead of the entry target characters or the figures specifying the entry target characters, for the data communication between the communication terminal device and the server system. Thus, the server system, and the like, of the present invention are capable of preventing the information to be specified

by a user from being stolen or tampered with by a third party, between the communication terminal device and the server system.

[0017]

Accordingly, the communication terminal device ~~server system~~ of the present invention is capable of preventing illegal logins and man-in-the-middle attacks made by a third party to the services delivered to the users.

[0018]

Consequently, the communication terminal device ~~server system~~ of the present invention is capable of preventing the leakage of the security-related information, illegal uses and man-in-the-middle attacks, and of improving the security at the time of delivering various services including the Internet banking service, or the like.

[0019]

(3) In order to solve the above-described problem, a recording medium of the present invention is a recording medium having figures that are visible and that are for specifying, at a server system that delivers various services, entry target characters entered by a user when the user accesses the server system by making use of a communication terminal device, the recording medium comprising:

a table that has a plurality of rows and a plurality of columns, a plurality of different entry target characters and a plurality of figures that differ for each entry target character being arranged in a row or column, and

each figure having a shape that is unconverted by a character code used at the time of user operational input based on an input device to be used by the user for entering predetermined information.

[0020]

Based on this configuration, the recording medium of the present invention is formed with a random number table in which figures such as, for example, symbols, designs, pictures or images (for example, still images including photographs, moving images or hand-written characters), from which the entry target characters cannot be deduced directly (i.e. shapes that cannot be converted by means of character codes used at the time of user operational input based on an input device used by the user for entering predetermined information) are associated with entry target characters. Thus, when entering the entry target characters, such entry target characters can be specified without using such entry target characters.

[0021]

Accordingly, the storage medium of the present invention is capable of preventing: the leakage of security-related information (for example, a password) caused by a user's carelessness, for example, by entering, all at once, at a phishing site, all of the information

This is a man-in-the middle attack type where information sent from the user's terminal device to the server of the banking organization is tampered with on the network, and money is caused to be received at a beneficiary different from the original beneficiary by changing the beneficiary, the amount of money, etc. For example, when an instruction to make a remittance to the server of (receiving banking organization B is provided to the server of (paying) banking organization A from the terminal device, based on the user's instruction, such remittance instruction is analyzed and is tampered with into an instruction to be transmitted to the server of (illegal remittance beneficiary) banking organization C, and a process to make an illegal remittance to such illegal remittance beneficiary is executed. Furthermore, a remittance result from the illegal remittance beneficiary is disguised into a remittance result from the server of (receiving) banking organization B and is notified as a remittance completion of the server of (paying) banking organization A.

[0039]

(4) Type 4 ([4] in Fig. 2)

This is a phishing fraud type ([4] in Fig. 2) where a URL of a website (i.e. a phishing website) that differs from the original website delivering services is sent to the user's terminal device by way of an email, etc., and the user is led to the phishing website, and various kinds of information, such as a password, a random graphic table or the like, are swindled by deceiving the user into entering such information in such phishing website. In this case, the malicious third party illegally logs into the server of (paying) banking organization A as a legitimate user, using the illegally-obtained password, etc., and provides a remittance instruction, and an illegal remittance process is executed in which an illegal remittance is made to an account, etc. of the malicious third party, and more specifically, to a server of (illegal remittance beneficiary) banking organization C.

[0040]

Accordingly, in order to secure safety in the Internet banking service, it is necessary to take measures against all types of the various attacks and fraud described above so as to prevent the same.

[0041]

On the other hand, conventional approaches for avoiding the various attacks described above include:

(A) an approach where a client certificate is used;

(B) an approach where a cryptographic token that generates a one-time password is used; and;

(C) an approach where authentication is performed by means of unique information (a subscriber number, serial number, or the like) inside the user's terminal device, or biological information such as fingerprints, veins, or the like.

[0042]

However, in addition to the fact that it is easy for a client certificate to be taken over and it is therefore not an effective means of preventing attacks, it cannot be used for international commercial transactions since the types of such certificates differ from country to country. Moreover, in the case of making use of a cryptographic token, since it is expensive to manufacture a machine dedicated to cryptographic tokens, it is not widely used. Furthermore, the unique information of the user's terminal device is likely to be extracted by malware, and thus, in many cases, the effectiveness thereof cannot be ensured as a method for preventing attacks. Also, the case where biological information is used has not become popular due to the high cost of introducing devices, the decrease in user-friendliness such that the information cannot be easily entered, or difficulties in obtaining accurate biological information.

[0043]

On the other hand, in addition to the above-described approaches (A) to (C), there is also an approach where a random number table (a table in which numbers are randomly arranged in a matrix), which is made available for user entry, is separately issued for each user by a banking organization, and identification is verified by performing an entry using such random number table ~~RMT~~.

[0044]

However, in such case, the content of the information sent from the user to the banking organization is expressed in a character code, such as ASCII code, which can be specified in other general terminal devices. Accordingly, a malicious third party can easily specify the character string expressed by the transmitted/received information, and it is difficult to prevent man-in-the middle attacks that perform tampering with and disguising of the information during communication.

[0045]

In addition, in the case of using such random number table ~~RMT~~, it is quite common for the user to be led to a phishing site and to inadvertently enter all of the information of the random number table in such phishing site. When all information of random number table ~~RMT~~ is entered, the user is spoofed based on such random number table ~~RMT~~ and illegal remittances are carried out.

[0046]

Moreover, when the user's terminal device, etc. is infected with malware, such as a key logger, all information entered by the user in accordance with random number table ~~RMT~~ may be stolen by a third party.

[0047]

Hence, network system 1 of the present embodiment adopts a configuration in which:

(1) random graphic table RMT is used, which is issued at a banking organization in advance for each user and in which entry target characters, such as numerical characters and alphabetical characters, and figures, from which the above entry target characters cannot be deduced directly, such as symbols, photographs, graphics or pictures, are associated with each other as illustrated in Fig. 3;

(2) random graphic table data, in which random graphic tables RMTs of the respective users are compiled into data, and user IDs for identifying such users are managed by associating them with each other;

(3) when a user uses the Internet banking service, data (hereinafter referred to as "data for entry") is distributed, such data is for displaying to an appropriate user a plurality of figures, including figures corresponding to the entry target characters, based on the random graphic table data corresponding to the respective users and such data is for making the entry target characters to be entered by the figures;

(4) when a plurality of figures is provided (displayed) to the user based on the data for entry, positional information that indicates display positions for specifying the figures selected by the user and information for specifying such display positions (hereinafter referred to as "marker information") are specified; and

(5) the figures are determined based on the specified marker information and finally the entry target characters are specified.

[0048]

In particular, the present embodiment has a configuration in which the entry target characters, which are to be specified, are communicated as the marker information by making use of the above-described random graphic table RMT, and while the entry target characters cannot be specified by a third party during communication, the entry target characters, which are to be specified for the respective users, can be specified at banking organization servers 30.

[0049]

Specifically, communication terminal device 10 is a communication terminal device, such as a personal computer (PC), a smartphone, or the like, used by a user, and it is adapted to connect to network 20, either directly or via base station BS, and to execute data communication with banking organization servers 30.

[0050]

the column display for displaying row B, such that the figure at row B and column 2 is displayed at the far right and the figure at row B and column 5 is displayed at the display position in the next row. Then, data for entry generation and distribution part 353 generates the data for entry that includes the positional information that indicates the determined display positions of the figures.

[0123]

It should be noted that data for entry generation and distribution part 353 determines the display positions for displaying the respective figures in a line and in a random manner on communication terminal device 10, based on the column display for displaying row E.

[0124]

In addition, as for the indication data for indicating the figures to be selected by the user, the indication data includes, for example, character string (text) data, such as "please select the figures corresponding to the characters you would like to enter from row B of random graphic table ~~RMT~~."

[0125]

When specification process part 354 receives the positional information (i.e. the marker information corresponding to the figures entered based on the data for entry and random graphic table RMT), which is acquired when the figures are entered by the user, based on the data for entry, at communication terminal device 10, specification process part 354 specifies the entry target characters corresponding to the figures selected by the user based on: the received positional information; the relevant random graphic table data; and information used for the generation of the data for entry by figure extraction part 352, such information being information indicating the rows of random graphic table RMT when the figures are extracted (hereinafter referred to as the "extracted information").

[0126]

For example, for the random graphic table data corresponding to random graphic table RMT shown in Fig. 3, when the image data of the respective figures arranged in row B in the random graphic table data corresponding to random graphic table RMT shown in Fig. 3 is read and when the figure at row B and column 2 is arranged at the far right and the positional information (the marker information) that indicates the position thereof is received, specification process part 354 specifies entry target character "2" corresponding to position "row B and column 2" as the entry target character.

[0127]

It should be noted that specification process part 354 specifies a plurality of entry target characters, for example, in accordance with the order in which the entry target characters are entered. More specifically, when specification process part 354 is to specify double-digit

For example, data for entry generation and distribution part 353 generates, as illustrated in Fig. 12, the data for entry that includes:

data for displaying, at communication terminal device 10,

(1) the name of the money-receiving banking organization,

(2) the money-receipt amount,

(3) the name of the money-receiving branch office,

(4) a pull-down box for selecting an account type (savings, checking, or the like), and

(5) a text box for entering a predetermined number of digits from the top (for example, the first five digits) of the money-receiving account number;

(6) image data corresponding to a character string, such as "please select the figure relevant to (the second digit from the bottom) from row B," and figures in row B in order to select entry target characters (for example, the last two digits of the account number) to be entered by means of figures; and

(7) image data corresponding to a character string, such as "please select the figure corresponding to the last digit from row E," and figures in row E.

[0147]

It should be noted that each text box may be replaced by a pull-down box.

[0148]

Subsequently, at communication terminal device 10, network communication part 110 receives the data for entry distributed from banking organization server 30 (Step Sa111). Then, application execution unit 170 causes an entry screen (hereinafter also referred to as the "screen for entering account information"), such as that illustrated in Fig. ~~13~~12(B), to be displayed based on the received data for entry (Step Sa112).

[0149]

Subsequently, application execution unit 170, in coordination with Operational unit 150 and in accordance with the screen for entering account information, acquires the entered remittance amount, the name of the beneficiary bank, the name of the branch office, the account type, and part of the account number. Application execution unit 170 also acquires the entered account information, including the positional information of the figures for specifying the other part (i.e. the entry target characters) of the account number, which was entered by referring to the relevant random graphic table RMT (Step Sa113).

[0150]

In particular, when application execution unit 170 of the present embodiment detects the positions of the figures corresponding to the numbers of the last two digits of the account number, it specifies the positional information that indicates the detected positions of the figures, as the information for specifying the entry target characters by means of the figures.

[0151]

For example, when the last two digits of the account number, which are to become the entry target characters, are "2~~1~~7" and when the figure at row B and column 2 and the figure at row E and column 1 in random graphic table RMT are selected by Operational unit 150 (i.e. when the display positions of the relevant figures are touched), application execution unit 170 specifies, as the positional information of the figure of the upper digit, the positional information of the image data that indicates the ~~eighth~~ seventh position from the left facing the plane of Fig. 12 and, as the positional information of the figure of the lower digit, the positional information of the image data that indicates fifth position from the left facing the plane of Fig12.

[0152]

Subsequently, application execution unit 170 displays, on the display 140, the entered account information including the positional information as the marker information (Step Sa114). Then, application execution unit 170 transmits such entered account information to banking organization server 30 and stands by for the receipt of information indicating the remittance result (Step Sa115).

[0153]

It should be noted that application execution unit 170 displays on display 140, in coordination with Display control unit 130 and for example as shown in Fig. 14~~3~~ , the information (the banking service specific information) acquired in Step Sa113, which includes the positional information as the marker information. However, application execution unit 170 may display, in coordination with banking organization server 30, the banking service specific information on display 140 after the acquisition thereof when the account is confirmed at the relevant banking organization server 30.

[0154]

Subsequently, at banking organization server 30, communication control part 310 receives the entered account information transmitted by communication terminal device 10 (Step Sa321). Then, specification process part 354 specifies the entry target characters corresponding to the figures selected by the user, based on the positional information included in the received entered account information, the data for entry distributed to the relevant user, and the random graphic table data of such user (Step Sa322).

[0155]

More particularly, in the present embodiment, specification process part 354 determines the beneficiary account number, which is made up of seven digits, by combining the characters for the last two digits, which are specified by the positional information, with the first five digits of the account number, which are entered by the user in the entry screen.

11. The server system according to any one of claims 1 to 9, wherein

the entry target character includes English characters A to Z.

12. The server system according to any one of claims 1 to 11, wherein

the processer executes a process of a bank clearance, as the given process, based on account information specified by the specified entry target character, the account information including at least one of a user's account number, remittance amount, a banking organization account number and an account number of a branch office.

13. A communication system, comprising:

a server system according to any one of claims 1 to 12; and

a plurality of communication terminal devices that communicates with and is connected to the server system via a network.

14. A computer program executed by computer functioning as a serve, the program causing the computer to function as:

a receiver that receives, via a network, data from a communication terminal device that communicates with and is connected to the server system;

a controller that controls a database in which table data is recorded in association with identification information for identifying a user, the table data being predetermined for each user of the communication terminal device and having entry target characters entered at the communication terminal device and figures pre-allocated to the respective entry target characters that are associated with each other;

a data specifying processer that specifies, when a given request designated by a user from the communication terminal device is received ~~by the receiver~~, table data that corresponds to the user;

an extracting processer that extracts the figures that correspond to entry target characters to be specified by the user based on the specified table data;

a distributer that generates data for entry that is associated with each of the extracted figures and that includes marker information to be used when relevant figures are displayed at a relevant communication terminal device, and that distributes the generated data for entry to the communication terminal device;

an acquiring processer that acquires, when the figures are displayed at the communication terminal device based on the distributed data for entry, the marker information that corresponds to the figures entered by the user from the communication terminal device;