



(11) **EP 1 834 677 A1**

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 158(3) EPC

(43) Date of publication:
19.09.2007 Bulletin 2007/38

(51) Int Cl.:
A63F 9/00 (2006.01) G06F 13/00 (2006.01)

(21) Application number: **05814455.1**

(86) International application number:
PCT/JP2005/022777

(22) Date of filing: **12.12.2005**

(87) International publication number:
WO 2006/064764 (22.06.2006 Gazette 2006/25)

(84) Designated Contracting States:
DE ES FR GB IT

(30) Priority: **16.12.2004 JP 2004364123**
16.12.2004 JP 2004364124

(71) Applicant: **SEGA CORPORATION**
Tokyo 144-8531 (JP)

(72) Inventors:
• **Furuhashi, Shinichi**
c/o Sega Corporation
Tokyo 1448531 (JP)

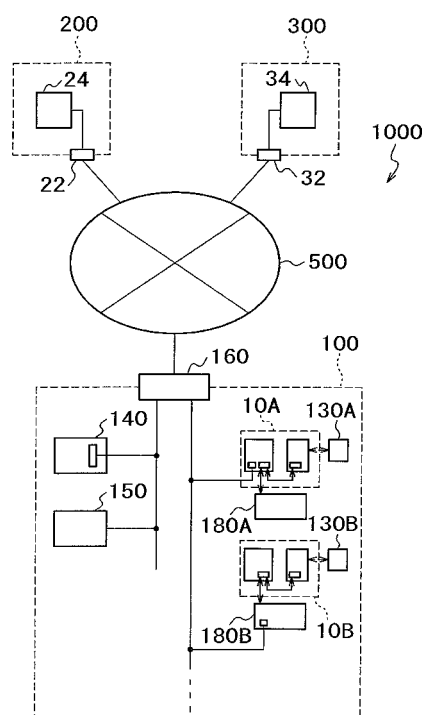
• **Yoshida, Jiro**
c/o Sega Corporation
Tokyo 1448531 (JP)
• **Okunoki, Yutaka**
c/o Sega Corporation
Tokyo 1448531 (JP)

(74) Representative: **Betten & Resch**
Patentanwälte,
Theatinerstrasse 8
80333 München (DE)

(54) **GAME MACHINE MANAGEMENT DEVICE HAVING PENALTY FUNCTION, GAME DEVICE, OPERATION PROGRAM THEREOF, AND PENALTY SETTING SERVER**

(57) The present invention provides a game machine authentication management device 10 and a game device for transmitting an authentication request and ID data to an authentication server 24 through first communication means 110, waiting for a response including the authentication result data in a reception-enabled state, acquiring authentication level data capable of indicating any one of the events of authentication OK, authentication NG and timeout, transmitting electronic money terminal setting data and an electronic money operation instruction according to the authentication level data to an electronic money terminal 134 through second communication means or third communication means, and suspending the electronic money terminal setting data and the electronic money operation instruction in at least one of the cases. The electronic money terminal setting data may be stored in a penalty setting server 140 or the like.

FIG.1



Description

Technical Field

[0001] The present invention relates to a game machine management device, game device, operation program thereof and server to set the game machine management device.

The present invention relates, more particularly, to a device for managing with authentication a game machine used for commercial purposes in running a game and billing and settlement, a game device which carries out such authentication, operation program thereof and a server to control the settings of such a device.

Background Art

[0002] Conventionally, a game system such as an electronic game or video game which allows many remotely located game participants to participate in a game using a communication network is known (e.g., see Japanese Patent Laid-Open No. 08-000829 (hereinafter, referred to as "Patent Document 1")). This game system allows a player to enjoy a game, for example, at an amusement facility after conducting appropriate logging in. Such a game machine (game device) is sometimes connected to an in-store network at the amusement facility such as a so-called game center. This network is also connected to, for example, an appropriate outside server. In order to prevent unauthorized alteration of an electronic circuit board of a game machine, unauthorized transfer from its original setting location or unauthorized tampering of communication data (hereinafter, generically referred to as "unauthorized use or the like"), authentication is carried out by a server thereof at the start of the game machine or the game machine is periodically authenticated.

[0003] Such an amusement facility uses game machines which allow players to play games. Examples of such a game machine include a video game machine whereby a player plays a video game and a prize game machine aimed at prize winning or the like. Furthermore, at the amusement facility, game machines such as a medal dispensing machine to provide players medals which can be used for the game machines and which are obtained by paying some money are used. The entity who manages the amusement facility is generally called an "operator."

[0004] Furthermore, media such as an IC card and an electronic money function incorporated in a cellular phone are recently known as a means for carrying out billing and settlement processing of various charges. Electronic money (Bitwallet, Inc., Edy (registered trademark), etc.) using a non-contact electromagnetic communication is known as a typical example. This technique is disclosed, for example, in Japanese Patent Laid-Open No. 2000-251005 (hereinafter, referred to as "Patent Document 2").

[0005] When the function of electronic money is added to each of the above described game machines, authentication can be carried out using a dedicated additional unit. Here, electronic money is related to sales and payment of a game machine. For the operator, it is desirable that electronic money always operates normally unless unauthorized use is attempted. On the other hand, when an investigation is made into causes why authentication of an actual game machine is not concluded successfully, most of the causes are not related to unauthorized use, but they can simply be the poor condition of the network in the store or the poor condition of the network connecting the store and the authentication server due to lack of maintenance work or the like. That is, when authentication fails or a timeout occurs (a response as to whether or not authentication fails is not obtained within a predetermined time), stopping the use of the game machine or prohibiting the game using electronic money across the board will cause the game using the game machine or the game using electronic money to be prohibited, placing an excessive burden on the business even if the user does not attempt unauthorized use. A similar situation may also occur if no maintenance staff is available due to holidays, etc. when authentication fails, and when authentication fails or a timeout occurs, stopping the use of the game machine or prohibiting the game using electronic money immediately thereafter should also be avoided.

[0006] Furthermore, when authentication fails, since there is a possibility that the operator's business may be affected, taking measures such as stopping the use of the actual game machine or prohibiting the game using electronic money (these are generically called "penalties") should be performed based on a precise time. Moreover, though authentication should be repeatedly performed with appropriate frequency, it is desirable to operate a clock to determine authentication timing or the like so as to appropriately prevent behaviors like avoidance of authentication or reducing the frequency with which authentication is performed.

Patent Document 1: Japanese Patent Laid-Open No. 8-829

Patent Document 2: Japanese Patent Laid-Open No. 2000-251005

Disclosure of the Invention

[0007] It is an object of the present invention to provide a game machine authentication management device, a game

device, operation program thereof and penalty setting server capable of appropriately managing a game machine such as a conventional video game machine, prize game machine or medal dispensing machine used in a game center and appropriately using the game machine except in cases with actual unauthorized use or the like.

[0008] Here, the present invention provides a remote authentication management system capable of limiting functions of a device located in a remote place through a network without being limited to the above described game machine.

[0009] More specifically, the present invention provides a remote authentication management system, including an authentication server (24) provided with a function of authenticating an apparatus (180) to be authenticated, a penalty setting server (140) which stores integrated penalty setting data, the integrated penalty setting data storing at least one of a first setting table and a second setting table including set values which define an authentication level of the apparatus (180), the first setting table being different from the second table in at least one of the set values that define the authentication level, an authentication management device (10) which stores unit penalty setting data including a set value which is different from the integrated penalty setting data, a first network (LAN) which connects the penalty setting server (140) and the apparatus (10) and a second network (WAN) which connects the first network (LAN) and the authentication server (24), wherein the authentication server (24) permits operation of the apparatus (180) when the apparatus (10) can invoke the authentication server (24) at predetermined timing, the apparatus (10) accesses the penalty setting server (140) when the apparatus (10) cannot invoke the authentication server (24) at predetermined timing or cannot invoke within a predetermined time, the apparatus (10) refers to the first setting table or the second setting table of the integrated penalty setting table when the access succeeds, and the apparatus (10) refers to the unit penalty setting table when the access fails.

[0010] Here, the remote authentication management system of the present invention preferably includes a mode in which the integrated penalty setting table can be set or referred to by a maintenance computer (28) connected through the network or a different communication path, a mode in which the unit penalty setting table can be set or referred to from the maintenance computer (28) connected through the network or a different communication path. Furthermore, a mode in which the maintenance computer (28) is the authentication server (24) is more preferable. Furthermore, a mode in which an authentication scheduling server which stores authentication schedule data which determines the predetermined timing is further connected to the network or a mode in which the authentication scheduling server is the penalty setting server (140) is preferable. A mode in which an authentication pause scheduling server which stores authentication pause schedule data is further connected to the network is more preferable. Here, the authentication pause scheduling server may also be the penalty setting server or the authentication scheduling server.

[0011] Furthermore, the present invention provides an apparatus to be authenticated, provided with authentication management means. More specifically, the present invention provides an apparatus to be authenticated, including first communication means configured to be connectable to a computer network and communicable with an authentication server, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, payment means configured to be communicable with at least one of payment apparatuses and function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and change a payment function for at least one of the payment apparatuses based on payment setting data which defines a payment setting, wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means, waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time and changes the payment function for at least one of the payment apparatuses based on payment setting data according to the authentication level data at any of the cases.

[0012] Furthermore, the present invention provides an authentication management device which is different from the apparatus to be authenticated. More specifically, the present invention provides an authentication management device, including first communication means configured to be connectable to a computer network and communicable with an authentication server, second communication means configured to be communicable with the apparatus to be authenticated, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, payment means configured to be communicable with at least one of payment apparatuses through the second communication means or third communication means and function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data

stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit payment means setting data which defines operable functions of the payment means or a payment means operation instruction according to the payment means setting data to the payment means through the second communication means or the third communication means, wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means, waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time and transmits the payment means setting data according to the authentication level data or the payment means operation instruction to the payment means through the second communication means or the third communication means at any one of the cases or suspends the transmission of the payment means setting data or the payment means operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

[0013] Furthermore, when authentication fails, the present invention provides a penalty setting server to be used for an apparatus which stops or prohibits the use of an apparatus to be authenticated. More specifically, the present invention provides a penalty setting server to be used for an authentication management device or an apparatus to be authenticated, configured to be communicable with the function setting means through the first communication means of the apparatus to be authenticated or the authentication management device through the computer network, including storage means for storing the integrated penalty setting table and outside communication means communicable with an outside network connected to any one of the computer network and another computer network logically separated from the computer network, wherein the integrated penalty setting table is configured to be rewritable from a maintenance computer in the outside network through the outside communication means.

[0014] Furthermore, the present invention provides a method of operating a remote authentication management system. More specifically, the present invention provides a method of operating a remote authentication management system, including an authentication server provided with a function of authenticating an apparatus to be authenticated, a penalty setting server which stores integrated penalty setting data, the integrated penalty setting data storing at least one of a first setting table and a second setting table including set values which define authentication levels of the apparatus and the first setting table being different from the second table in at least one of the set values which define the authentication levels, an authentication management device which stores unit penalty setting data including a set value which is different from the integrated penalty setting data, a first network (LAN) which connects the penalty setting server and the apparatus and a second network (WAN) which connects the first network (LAN) and the authentication server, the method including a step of permitting the operation of the apparatus by the authentication server when the device can invoke the authentication server at predetermined timing, a step by the device of accessing the penalty setting server when the apparatus cannot invoke the authentication server at predetermined timing or cannot invoke the authentication server within a predetermined time, a step by the device of referring to the first setting table or the second setting table of the integrated penalty setting table when the access succeeds and a step by the device of referring to the unit penalty setting table when the access fails.

[0015] Furthermore, the present invention provides a method of managing authentication of an apparatus to be authenticated. More specifically, the present invention provides a method of operating an authentication management device, including first communication means configured to be connectable to a computer network and communicable with an authentication server, second communication means configured to be communicable with an apparatus to be authenticated, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, payment means configured to be communicable with at least one of payment apparatuses through the second communication means or third communication means and function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit payment means setting data which defines operable functions of the payment means or a payment means operation instruction according to the payment means setting data to the payment means through the second communication means or the third communication means, the method including a step by the function setting means of transmitting the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means, a step by the function setting means of waiting for a response including the authentication

result data from the authentication server in a reception-enabled state within a predetermined standby time, a step by the function setting means of acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time and a step by the function setting means of transmitting the payment means setting data according to the authentication level data or the payment means operation instruction to the payment means through the second communication means or the third communication means at any one of the cases or suspending the transmission of the payment means setting data or the payment means operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

[0016] Furthermore, the present invention provides a method of operating a penalty setting server. More specifically, the present invention provides a method of operating a penalty setting server configured to be communicable with the function setting means through the first communication means of the apparatus to be authenticated or the authentication management device through the computer network, including a step of storing the integrated penalty setting table in the storage means of the penalty setting server, a step by outside communication means of the penalty setting server of making communicable with an outside network connected to any one of the computer network and another computer network logically separated from the computer network and a step of configuring the integrated penalty setting table to be rewritable from a maintenance computer which is in the outside network through the outside communication means.

[0017] Furthermore, the present invention provides a program to manage authentication of an apparatus to be authenticated. More specifically, the present invention provides a computer program for causing a computer to operate as an authentication management apparatus, the computer including first communication means configured to be connectable to a computer network and communicable with an authentication server, second communication means configured to be communicable with an apparatus to be authenticated, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, payment means configured to be communicable with at least one of payment apparatuses through the second communication means or third communication means and calculation means for operating as function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and configured to be able to transmit payment means setting data which defines operable functions of the payment means or a payment means operation instruction according to the payment means setting data to the payment means through the second communication means or third communication means, the computer program causing the computer to execute a step by the calculation means of transmitting the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means, a step by the calculation means of waiting for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, a step by the calculation means of acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time, and a step by the calculation means of transmitting the payment means setting data according to the authentication level data or the payment means operation instruction to the payment means through the second communication means or the third communication means at any one of the cases or suspending the transmission of the payment means setting data or the payment means operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

[0018] Furthermore, the present invention provides a computer program which causes calculation means of a penalty setting server configured to be communicable with the function setting means through the first communication means of the apparatus to be authenticated or the authentication management device through the computer network to execute a step of storing the integrated penalty setting table in the storage means of the penalty setting server, a step of making the outside communication means of the penalty setting server communicable with any one of the computer network and an outside network connected to another computer network logically separated from the computer network and a step of configuring the integrated penalty setting table to be rewritable from a maintenance computer which is in the outside network through the outside communication means.

[0019] Furthermore, the present invention also provides a recording medium which stores any one of the above described programs. Examples of such a recording medium may include a rewritable nonvolatile memory such as a

flash memory, EEPROM (Electrically Erasable Programmable Read Only Memory) and hard disk drive, read-only non-volatile memory such as a mask ROM or rewritable or read-only optical disk such as CD and DVD.

[0020] Here, the above described "payment apparatus" or "payment means" may include an apparatus for carrying out payment through cash, a prepaid card, electronic money or the like. Examples thereof may include an electronic money reader/writer apparatus. Furthermore, the above described "apparatus to be authenticated" may include an apparatus which has the function of providing a service and selling articles such as a game machine, karaoke apparatus, jukebox and vending machine. Moreover, the above described "authentication management device" is not limited to a "game machine authentication management device" and may include an apparatus for appropriately managing the above described "apparatus to be authenticated" and "payment apparatus" or the like.

[0021] Moreover, the present invention provides a game machine authentication management device, including first communication means configured to be connectable to a computer network and communicable with an authentication server, second communication means configured to be communicable with a game machine, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means, and function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means, wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means, waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time, transmits the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases or suspends the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

[0022] Here, in the present invention, the electronic money terminal setting data in general is data to determine operation of an electronic money terminal and the electronic money terminal operation instruction is a command to cause the electronic money terminal to perform a specific operation (e.g., billing of a predetermined amount of money on electronic money or the like). When the electronic money terminal setting data is stored in the apparatus authentication management device, the apparatus authentication management device transmits an electronic money terminal operation instruction according to the electronic money terminal setting data and the electronic money terminal operates accordingly. Furthermore, when the electronic money terminal is provided with some storage means, the apparatus authentication management device transmits the electronic money terminal setting data itself and the electronic money terminal performs an operation according to the electronic money terminal setting data. Furthermore, in the present invention, timing for transmitting electronic money terminal setting data and an electronic money terminal operation instruction in general is not particularly limited. For example, the game machine authentication management device of the present invention may store the authentication level data in either the storage means or the electronic money terminal setting data and an electronic money terminal operation instruction according to the authentication level data may be transmitted only after a signal reporting that an attempt to perform payment using electronic money is being made has been received from the electronic money terminal through the second communication means or third communication means. Furthermore, the game machine authentication management device of the present invention may acquire the authentication level data, immediately transmit the electronic money terminal setting data and the electronic money terminal may store the data and change its operation.

[0023] Furthermore, according to the present invention, electronic money terminal setting data or an electronic money terminal operation instruction according to the authentication level data in general is transmitted to the electronic money terminal through the second communication means or third communication means or the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication

means or the third communication means is suspended according to the authentication level data in at least one of the cases. The specific configuration of data or an instruction in the electronic money terminal setting data or an electronic money terminal operation instruction is determined by the mounting specification of the electronic money terminal. Therefore, when, for example, the electronic money terminal has a plurality of operating modes and when the operating mode of the electronic money terminal is switched according to the authentication level data or the like, the electronic money terminal setting data or an electronic money terminal operation instruction is transmitted to the electronic money terminal through the second communication means or the third communication means. Furthermore, when the electronic money terminal requires an explicit operation instruction for the operation, the transmission of electronic money terminal setting data or an electronic money terminal operation instruction is suspended, and the operation of the electronic money terminal is thereby restricted.

[0024] Furthermore, as another mode of the present invention, the first communication means may not be provided for the game machine authentication management device but the first communication means may be provided for the game machine. In such a case, when the game machine authentication management device of the present invention communicates with the computer network, the game machine authentication management device carries out communications through the second communication means and the first communication means which communicate with the game machine.

[0025] Furthermore, as a further mode, the present invention may also be implemented as a game device. That is, the present invention provides a game device, including first communication means configured to be connectable to a computer network and communicable with an authentication server, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and change a payment function for at least one of the electronic money medium and the apparatus with a built-in electronic money function based on the payment setting data which defines a payment setting, wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means, waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time and changes the payment function for at least one of the electronic money medium and the apparatus with a built-in electronic money function based on payment setting data according to the authentication level data in at least one of the cases.

[0026] Here, the payment setting data refers to data which defines the setting of a payment with electronic money and is similar to the electronic money terminal setting data which has already been explained.

[0027] Furthermore, as a still further mode of the present invention, the authentication scheduling server provided with the instruction transmission means for transmitting an authentication request generating instruction for causing the function setting means to generate an authentication request to the function setting means through the first communication means according to authentication schedule data or a program is provided with second storage means, and it is possible to transmit the authentication request when the function setting means of the game machine authentication management device receives the authentication request generating instruction from the instruction transmission means. This mode may also be realized in a mode in which the present invention is implemented as a game device. The mode in which the authentication scheduling server causes the instruction transmission means to operate may be such that the game machine authentication management device which is a client is always set in a waiting state and data is transmitted from the server as PUSH type data or another mode may be such that the game machine authentication management device sends some request first and the authentication scheduling server passively causes the instruction transmission means to operate according to the request.

[0028] Moreover, the game machine authentication management device or the game device of the present invention can set functions of the game machine or send a game machine operation instruction. That is, according to the present invention, the function setting means is configured to be able to transmit game machine setting data which defines the operable function of the game machine or a game machine operation instruction according to the game machine setting data to the game machine through the second communication means and it is preferable, at least at any one of the above described events, to transmit the game machine setting data or the game machine operation instruction to the

game machine through the second communication means according to the authentication level data or suspend the transmission of the game machine setting data or the game machine operation instruction to the game machine through the second communication means. The game machine setting data defines operable functions of the game machine, but the game machine may also include storage means for storing this game machine setting data and the game machine may change its functions with reference to the game machine setting data. Furthermore, the game machine operation instruction is a command to cause the game machine to perform a specific operation (e.g., starting a game or the like). The game machine authentication management device stores game machine setting data in some storage means and when an explicit operation instruction is required from the game machine authentication management device to the game machine or by the game machine for the operation, the transmission of the game machine setting data or the game machine operation instruction is suspended and the operation of the game machine is thereby restricted. In order to realize this, the game device of the present invention incorporates the second communication means and the game machine section of the game device uses means similar to that of the game machine and realizes a function similar to that of the game machine.

[0029] Furthermore, the game machine authentication management device or the game device of the present invention preferably uses a penalty setting server configured to be communicable with the function setting means. This penalty setting server stores an integrated penalty setting table in the storage means. The function setting means refers to the integrated penalty setting table stored in the penalty setting server through the first communication means. The integrated penalty setting table stores the set value of the electronic money terminal setting data (the set value of payment setting data), the set value of the game machine setting data and the set value of the display setting data in association with their respective authentication levels so that the function setting means can transmit or suspend the transmission of the electronic money terminal setting data (payment setting data) and the electronic money terminal operation instruction, transmit or suspend the transmission of the game machine setting data and the game machine operation instruction or control the display means.

[0030] In the game machine authentication management device or the game device of the present invention, the authentication scheduling server preferably stores authentication pause schedule data which defines at least one of the time at which authentication by the authentication server should be performed or the time at which authentication should be paused, the function setting means refers to the authentication pause schedule data stored in the authentication scheduling server according to at least one of the authentication schedule data and the program stored in the second storage means, determines whether or not it is the time at which authentication by the authentication server should be performed and transmits an authentication request and ID data to the authentication server through the first communication means. This authentication pause schedule data is also preferably stored in the penalty setting server.

[0031] In the game machine authentication management device or the game device of the present invention, the authentication scheduling server preferably stores at least one of penalty disabling schedule data which defines the times at which the penalty setting should be enabled and disabled, the function setting means refers to the penalty disabling schedule data stored in the authentication scheduling server before or after transmitting an authentication request and ID data to the authentication server and does not transmit at least one of electronic money terminal setting data (payment setting data), electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display setting data corresponding to any one of authentication level data that the authentication result data indicating that authentication failed has been received from the server during a predetermined standby time and that authentication result data has not been received during the predetermined standby time at least until the time at which the penalty setting should be enabled next time or stops the suspension of the transmission of the electronic money terminal setting data (payment setting data), electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display setting data corresponding to the authentication level data that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time until the time. This penalty disabling schedule data is also preferably stored in the penalty setting server.

[0032] The game machine authentication management device or the game device according to the present invention preferably further includes third storage means for storing a unit penalty setting table which stores set values corresponding to the authentication levels about at least one of the setting of operable functions of the electronic money terminal (or setting of payment with electronic money), the setting of operable functions of the game machine and setting of display contents, wherein the function setting means refers to the unit penalty setting table, transmits, at least at any one of the events, electronic money terminal setting data (payment setting data), electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display setting data or suspends the transmission of the electronic money terminal setting data (payment setting data), electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display setting data.

[0033] In the game machine authentication management device or the game device of the present invention, any one of the integrated penalty setting table and the unit penalty setting table preferably includes a first setting table and a second setting table, the function setting means refers to the first setting table for a predetermined penalty suspension

period after receiving an authentication result or after acquiring authentication level data, refers to the second setting table after the lapse of the penalty suspension period and the first setting table and the second setting table are configured to be different from each other in the set value for at least one of values of the authentication levels.

[0034] The present invention also realizes a method of causing the above described game machine authentication management device or the game device to operate and also a computer program to cause the computer to operate as the above described game machine authentication management device.

[0035] Furthermore, the present invention also provides a penalty setting server to be used for a game machine authentication management device configured to be able to communicate with the function setting means through the first communication means of the above described game machine authentication management device or the game device through a computer network, including storage means for storing an integrated penalty setting table and outside communication means communicable with an outside network connected to any one of a computer network and another computer network logically separated from the computer network, wherein the integrated penalty setting table is configured to be rewritable from a maintenance computer which is in the outside network through the outside communication means.

[0036] The game machine authentication management device or the game device according to the present invention transmits electronic money terminal setting data corresponding to authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during a predetermined standby time, that authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that authentication result data has not been received during the predetermined standby time to the electronic money terminal or changes the payment function for at least one of an electronic money medium and a device with a built-in electronic money function based on the payment setting data according to the authentication level data. Therefore, when managed the game machine using authentication, it is possible to transmit electronic money terminal setting data according to the authentication level and change the payment function of electronic money, appropriately manage payment with electronic money and appropriately use payment with electronic money except in cases with actual unauthorized use or the like.

[0037] When using the authentication scheduling server which stores authentication schedule data or a program in the game machine authentication management device or the game device of the present invention, it is possible to use a common scheduling server for a plurality of game machines and manage an authentication schedule in a centralized manner and easily manage many game machines appropriately.

[0038] Furthermore, the game machine authentication management device or the game device of the present invention can transmit the game machine setting data to the game machine according to the level of authentication, appropriately manage the game machine and moreover appropriately use the game machine except in cases with actual unauthorized use or the like.

[0039] Moreover, when the function setting means of the game machine authentication management device or the game device refers to the integrated penalty setting table of the penalty setting server, it is possible to use a common penalty setting server for a plurality of game machines, manage the display settings of the game machine, the electronic money terminal and the game machine authentication management device in a centralized manner and more easily manage many game machines appropriately.

[0040] Furthermore, the present invention provides a game machine authentication management device, including first communication means configured to be connectable to a computer network and communicable with an authentication server, second communication means configured to be communicable with a game machine, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, an electronic money terminal including a reader/writer section configured to be communicable with any one of an electronic money medium and an apparatus with a built-in electronic money function, configured to be communicable through the second communication means or third communication means, function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means, manual clock setting means capable of receiving a manual time setting and stopping the reception of the manual time setting based on a signal from the function setting means, a clock which can be set to an arbitrary time by the manual clock setting means and the function setting means and time storage means for storing a time at which authentication succeeded last time, wherein the function setting means determines a schedule according to at least one of the authentication schedule data and the program of the second storage means using the time of the clock, transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule,

waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, stores, when authentication result data indicating that authentication succeeded is received from the authentication server during a predetermined standby time, any one of the time data of the clock and authentication time data included in the authentication result data in the time storage means and transmits, when the authentication result data indicating that authentication succeeded is not received during a predetermined standby time, a signal of stopping the reception of the manual time setting to the manual clock setting means, acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time and transmits the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or third communication means at least at any one of the events or suspends the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or third communication means according to the authentication level data at least at any one of the events.

[0041] Here, in the present invention, the electronic money terminal setting data in general is data to determine operation of an electronic money terminal and the electronic money terminal operation instruction is a command to cause the electronic money terminal to perform a specific operation (e.g., billing of a predetermined amount of money on electronic money or the like). When the electronic money terminal setting data is stored in the apparatus authentication management device, the apparatus authentication management device transmits an electronic money terminal operation instruction according to the electronic money terminal setting data and the electronic money terminal operates accordingly. Furthermore, when the electronic money terminal is provided with some storage means, the apparatus authentication management device transmits the electronic money terminal setting data itself and the electronic money terminal performs an operation according to the electronic money terminal setting data. Furthermore, in the present invention, timing for transmitting electronic money terminal setting data and an electronic money terminal operation instruction in general is not particularly limited. For example, the game machine authentication management device of the present invention may store the authentication level data either the storage means or the electronic money terminal setting data and an electronic money terminal operation instruction according to the authentication level data may be transmitted only after a signal reporting that an attempt to perform payment using electronic money is being made has been received from the electronic money terminal through the second communication means or third communication means. Furthermore, the game machine authentication management device of the present invention may acquire the authentication level data, immediately transmit the electronic money terminal setting data and the electronic money terminal may store the data and change its operation.

[0042] Furthermore, according to the present invention, electronic money terminal setting data or an electronic money terminal operation instruction according to the authentication level data in general is transmitted to the electronic money terminal through the second communication means or third communication means or the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means is suspended according to the authentication level data in at least one of the cases. The specific configuration of the data or an instruction in the electronic money terminal setting data or an electronic money terminal operation instruction is determined by the mounting specification of the electronic money terminal. Therefore, when, for example, the electronic money terminal has a plurality of operating modes and when the operating mode of the electronic money terminal is switched according to the authentication level data or the like, the electronic money terminal setting data or an electronic money terminal operation instruction is transmitted to the electronic money terminal through the second communication means or the third communication means. Furthermore, when the electronic money terminal requires an explicit operation instruction for the operation, the transmission of electronic money terminal setting data or an electronic money terminal operation instruction is suspended, and the operation of the electronic money terminal is thereby restricted.

[0043] Furthermore, as another mode of the present invention, the first communication means may not be provided for the game machine authentication management device but the first communication means may be provided for the game machine. In such a case, when the game machine authentication management device of the present invention communicates with the computer network, the game machine authentication management device carries out communications through the second communication means and the first communication means which communicate with the game machine.

[0044] Furthermore, in the game machine authentication management device of the present invention, the above described manual clock setting means, the above described clock and the above time storage means are provided not for the game machine authentication management device but for the game machine, and the above described function setting means can transmit an instruction for causing the manual clock setting means of the game machine to stop the reception of the manual time setting through the second communication means.

[0045] Moreover, as another mode, the present invention may also be implemented as a game device. That is, the present invention provides a game device, including first communication means configured to be connectable to a computer network and communicable with an authentication server, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, a reader/writer section configured to be communicable with at least one of an electronic money medium or an apparatus with a built-in electronic money function, and function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and change a payment function for at least one of the electronic money medium and the apparatus with a built-in electronic money function based on the payment setting data which defines a payment setting, manual clock setting means capable of receiving a manual time setting and stopping the reception of the manual time setting based on a signal from the function setting means, a clock which can be set to an arbitrary time by the manual clock setting means and the function setting means and time storage means for storing a time at which authentication succeeded last time, wherein the function setting means determines a schedule according to at least one of the authentication schedule data and the program of the second storage means using the time indicated by the clock, transmits the authentication request and the ID data to the authentication server through the first communication means according to the schedule, waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, stores, when authentication result data indicating that authentication succeeded is received from the authentication server during the predetermined standby time, any one of the time data of the clock and the authentication time data included in the authentication result data in the time storage means, transmits, when authentication result data indicating that authentication succeeded is not received from the authentication server during the predetermined standby time, a signal for causing the manual clock setting means to stop the reception of the manual time setting, acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time and changes the payment function for at least one of the electronic money medium and the apparatus with a built-in electronic money function based on payment setting data according to the authentication level data at least at any one of the above described events.

[0046] Here, the payment setting data refers to data which defines the setting of a payment with electronic money and is similar to the electronic money terminal setting data which has already been explained.

[0047] Furthermore, the game machine authentication management device or the game device of the present invention can set functions of the game machine. That is, according to the present invention, the function setting means is preferably configured to be able to transmit a game machine operation instruction according to the game machine setting data or the game machine setting data which defines the operable functions of the game machine to the game machine through the second communication means, transmit, at least at any one of the above described events, the game machine setting data or the game machine operation instruction to the game machine according to the authentication level data through the second communication means or suspend the transmission of the game machine setting data or the game machine operation instruction to the game machine through the second communication means. The game machine setting data defines operable functions of the game machine, but the game machine may be provided with storage means for storing this game machine setting data and the game machine itself may also change its functions with reference to the game machine setting data. Furthermore, the game machine operation instruction is a command to cause the game machine to perform a specific operation (e.g., starting a game or the like). The game machine authentication management device stores game machine setting data in some storage means and when an explicit operation instruction is required from the game machine authentication management device to the game machine or by the game machine for the operation, the transmission of the game machine setting data or the game machine operation instruction is suspended and the operation of the game machine is thereby restricted. In order to realize this, the game device of the present invention incorporates the second communication means and the game machine section of the game device uses means similar to that of the game machine and realizes a function similar to that of the game machine.

[0048] Furthermore, the game machine authentication management device or the game device of the present invention preferably further includes display means whose display contents can be changed and display control means for controlling the display means and the function setting means generates display setting data which defines display contents according to the authentication level data, transmits the display setting data to the display control means and the display control means controls the display means so that the display means displays display contents according to the display setting data at least at any one of the above described events or controls the display means so that the display means stops the display according to the display setting data.

[0049] The game machine authentication management device or the game device of the present invention preferably

further uses a penalty setting server configured to be communicable with the function setting means. This penalty setting server stores an integrated penalty setting table in the storage means. The function setting means refers to the integrated penalty setting table stored in the penalty setting server through the first communication means. The integrated penalty setting table stores the set value of the electronic money terminal setting data (set value of payment setting data), the set value of the game machine setting data and the set value of the display setting data in association with their respective authentication levels so that the function setting means can transmit the electronic money terminal setting data (payment setting data) and the electronic money terminal setting instruction, transmit the game machine setting data and the game machine setting instruction or transmit the display setting data or suspend the transmissions thereof.

[0050] The penalty setting server used together with the game machine authentication management device or the game device of the present invention preferably stores the authentication pause schedule data which defines at least one of the time at which authentication by the authentication server should be executed and the time at which authentication should be paused, the function setting means refers to the authentication pause schedule data stored in the penalty setting server according to at least one of the authentication schedule data and the program stored in the second storage means, determines whether or not it is the time at which authentication by the authentication server should be executed and transmits an authentication request and ID data to the authentication server through the first communication means.

[0051] The game machine authentication management device or the game device according to the present invention preferably further includes third storage means for storing a unit penalty setting table which stores set values corresponding to the authentication levels about at least one of the setting of operable functions of the electronic money terminal, the setting of operable functions of the game machine and the setting of display contents, wherein the function setting means refers to the unit penalty setting table, transmits, at least at any one of the above described events, electronic money terminal setting data (payment setting data), electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display setting data or suspends the transmission of the electronic money terminal setting data (payment setting data), electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display setting data.

[0052] In the game machine authentication management device or the game device of the present invention, the function setting means preferably transmits, after the time of the clock has passed a predetermined suspension period from the time at which authentication succeeded last time and which is stored in the time storage means, electronic money terminal setting data (payment setting data) or an electronic money terminal operation instruction according to the authentication level data which indicates any one of the events that the authentication result data indicating that authentication failed has been received from the server during a predetermined standby time and that the authentication result data has not been received during the predetermined standby time or suspends the transmission of the electronic money terminal setting data (payment setting data) or the electronic money terminal operation instruction according to the authentication level data indicating an event that the authentication result data indicating that authentication succeeded has been received from the server during a predetermined standby time. This function setting means more preferably uses different predetermined suspension periods in the case where the authentication level data indicates the event that the authentication result data indicating that authentication failed has been received from the server during a predetermined standby time and in the case where the authentication level data indicates the event that the authentication result data has not been received during the predetermined standby time.

[0053] In the game machine authentication management device or the game device of the present invention, the integrated penalty setting table preferably includes a first setting table and a second setting table, the function setting means refers to the first setting table when the authentication level data indicates an event that the authentication result data indicating that authentication failed has been received from the server during a predetermined standby time and refers to the second setting table when the authentication level data indicates an event that the authentication result data has not been received during the predetermined standby time and the first setting table and the second setting table are configured to have different set values for at least one of values of the authentication levels.

[0054] In the game machine authentication management device or the game device of the present invention, the unit penalty setting table includes a first setting table and a second setting table, the function setting means refers to the first setting table when the authentication level data indicates an event that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and refers to the second setting table when the authentication level data indicates an event that the authentication result data has not been received during the predetermined standby time, and the first setting table and the second setting table are configured to have different set values for at least one of values of the authentication levels.

[0055] The present invention also implements a method of operating the above described game machine authentication management device or the game device and a computer program for causing a computer to operate as the above described game machine authentication management device.

[0056] Furthermore, the present invention provides a penalty setting server to be used for the above described game machine authentication management device or game device configured to be communicable with the function setting

means through the first communication means of the game machine authentication management device or the game device, including storage means for storing an integrated penalty setting table and outside communication means communicable with an outside network connected to any one of a computer network and another computer network logically separated from the computer network, wherein the integrated penalty setting table is configured to be rewritable from a maintenance computer in the outside network through the outside communication means.

[0057] The game machine authentication management device or the game device of the present invention stores, when authentication succeeds, the time thereof and causes, when authentication fails, the manual clock setting means 122 to stop the reception of the manual time setting. Furthermore, the game machine authentication management device or the game device of the present invention transmits electronic money terminal setting data according to the authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during a predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time to the electronic money terminal or changes the payment function for at least one of an electronic money medium and an apparatus with a built-in electronic money function based on payment setting data according to the authentication level data. Therefore, it is possible to prevent unauthorized use through the manual setting function of the clock, transmit, when managing a game machine using authentication, the electronic money terminal setting data according to the level of authentication, change the payment function of electronic money, appropriately manage payment with electronic money and also appropriately use payment with electronic money except in cases with actual unauthorized use or the like.

[0058] When using the authentication scheduling server which stores authentication schedule data or a program, it is possible, for example, to use a common scheduling server for a plurality of game machines, manage the authentication schedule in a centralized manner and manage many game machines more easily and appropriately.

[0059] Furthermore, it is possible to transmit the game machine setting data according to the level of authentication, appropriately manage the game machine and appropriately use the game machine except in cases with actual unauthorized use.

[0060] Furthermore, when the function setting means of the game machine authentication management device or the game device of the present invention refers to the integrated penalty setting table of the penalty setting server, it is possible to manage the settings of the game machine and the electronic money terminal, the display of the game machine authentication management device in a centralized manner using a common penalty setting server for a plurality of game machines and thereby manage many game machines more easily and appropriately.

Brief Description of the Drawings

[0061]

Figure 1 is a system configuration diagram showing the overall configuration of a game machine authentication system including a game machine authentication management device and a penalty setting server according to an embodiment of the present invention;

Figure 2 is a block diagram showing the configuration of a dedicated unit (game machine authentication management device) according to the embodiment of the present invention;

Figure 3 is a block diagram showing the configuration of a game machine according to the embodiment of the present invention;

Figure 4 is a block diagram showing the configuration of a dedicated unit (game machine authentication management device) according to another embodiment of the present invention;

Figure 5 is a block diagram showing the configuration of a game machine according to the other embodiment of the present invention;

Figure 6 is a block diagram showing the configuration of a penalty setting server used in the embodiment of the present invention;

Figure 7 is a system configuration diagram showing the overall configuration of a game machine authentication system according to a further embodiment of the present invention;

Figure 8 is a flow chart showing processing of a game machine authentication management device 10 according to an embodiment of the present invention; and

Figure 9 is a flow chart showing processing of a game machine authentication management device 10 according to another embodiment of the present invention.

Best Mode for Carrying Out the Invention

[0062] Hereinafter, embodiments of the present invention will be explained with reference to the attached drawings.

[0063] Figure 1 is a system configuration diagram showing the overall configuration of a game machine authentication system including a game machine authentication management device and a penalty setting server according to an embodiment of the present invention, Figure 2 is a block diagram showing the configuration of the game machine authentication management device and electronic money terminal of the present invention and Figure 3 is a block diagram showing an example of the configuration of a game machine managed by the game machine authentication management device of the present invention.

[0064] The game machine authentication system 1000 shown in Figure 1 is constructed of a plurality of computers or apparatuses using a computer network 500 connecting a plurality of sites. The "computer network" in the present invention refers to an arbitrary network in which computers can communicate data with each other according to an appropriate protocol, includes the computer network 500 (e.g., the Internet) connecting between a plurality of sites and further includes networks such as an intranet within each site. The computer network 500 which connects between a plurality of sites is also called "WAN (Wide Area Network)" and a network within a site is also called "LAN (Local Area Network)."

[0065] The game machine authentication system 1000 shown in Figure 1 is provided with an authentication server 24 at a data center site 200. This authentication server 24 is typically managed, not by an operator who manages each amusement facility store, but by a game system provider who provides the operator with a game machine 180 and undertakes system management of the game machine 180 from the operator. However, the present invention is not limited to such a commercial mode. The authentication server 24 is connected to the WAN 500 via an appropriate router 22. Here, the authentication server is an arbitrary server computer which is connected to a computer network thereof and has the function of performing authentication. This authentication is performed to authenticate whether or not ID data for authentication is authentic and thereby authenticate whether or not a game machine authentication management apparatus 10 (hereinafter, referred to as a "dedicated unit") is authentic and whether or not the game machine 180 in which the dedicated unit 10 is mounted is installed in an appropriate place. Though not limited particularly, when a network open to the public such as the Internet is used as the computer network 500, it is possible to include appropriate encryption processing or the like and prevent skimming, tampering or the like of the ID data.

[0066] In the game machine authentication system 1000 shown in Figure 1, an amusement facility store site 100 is provided with a game machine 180A and a game machine 180B. The amusement facility store site 100 has a LAN and the LAN is connected to the outside WAN 500 via an appropriate router 160. The game machines 180A, 180B are not only game machines per se such as a video game machine for playing a video game or a prize game machine aimed at prize winning, whereby the player can play the game, but also a medal dispensing machine to provide medals or the like which can be used for the game machine by paying the corresponding amount of money. As shown by the figure with two game machines 180A, 180B within the amusement facility store site 100, the game machine authentication system 1000 can be provided with a plurality of game machines 180. Only one amusement facility store site 100 is described in the figure, but the game machine authentication system 1000 may also include other amusement facility store sites and a plurality of game machines 180 may also be included in the plurality of store sites.

[0067] The amusement facility store site 100 in Figure 1 is provided with the dedicated unit 10 accompanying the game machines 180A, 180B and also includes a store server 140 and a management operator computer 150. The operator computer 150 is used for the purpose of management not related to authentication by the operator who manages the amusement facility store. For example, the operator computer 150 is connected to the LAN of the amusement facility store and used to generate a message to the player displayed on a display device 118 (Figure 2) of the dedicated unit 10 directly which is directly connected to the LAN and perform various kinds of management of the game machines connected to the LAN through the dedicated unit 10.

[0068] An electronic money issuer also participates in the game machine authentication system 1000. The "electronic money issuer" refers to a company or the like which issues electronic money. The electronic money issuer receives payment with normal currency from a holder of electronic money and provides a usable electronic money medium 130 to the holder according to the amount of payment. When the holder uses electronic money to pay for some goods or service, the electronic money issuer executes payment with currency according to the amount of payment for the person who received the payment with electronic money. In the embodiment of the present invention, the electronic money issuer may be, for example, an entity which provides an infrastructure of electronic money or a credit card issuing company or a prepaid card issuing company. This electronic money issuer is connected to the computer network 500 at an electronic money issuer site 300. The electronic money issuer site 300 is typically provided with an electronic money server 34 which records the amount of money given/received for each electronic money medium 130 and for each electronic money terminal and receives information from each electronic money terminal through the computer network 500. There are various modes in which the electronic money terminal 34 sums the amount of electronic money given/received and, for example, in stored value-type electronic money, the electronic money terminal 34 performs summation from each electronic money terminal 34 once a day. The electronic money terminal 34 is provided with the function of identifying each electronic money medium 130 and keeping a log of the amount of electronic money given/received using the electronic money terminal.

[0069] Figure 2 is a block diagram showing the configuration of the dedicated unit 10 (game machine authentication

management device) according to the embodiment of the present invention. The dedicated unit 10 is provided with several storage means. Here, the storage means is one that can record data into a volatile or non-volatile arbitrary data recording medium unless otherwise specified and, for example, a volatile memory such as a register in a CPU, DRAM, or rewritable nonvolatile memory such as flash memory, EEPROM (Electrically Erasable Programmable Read Only Memory), hard disk drive or read-only nonvolatile memory such as a mask ROM can be used. A rewritable or read-only optical disk such as a CD, DVD can also be used instead of or together with these memories. Furthermore, the logical format thereof is also arbitrary and refers to logically identifiable arbitrary storage means such as a binary format, ASCII text file, part of a relational database file, file managed by some operating system, combination of records of a list format file.

[0070] The dedicated unit 10 is provided with first storage means 102. The first storage means 102 is typically realized by an EEPROM or the like and stores ID data for authentication. The ID data for authentication includes ID data for identifying, for example, a dedicated unit and an electronic circuit board of an electronic money terminal as values indicating the game machine authentication management device. Furthermore, the ID data can include data which identifies the place where the game machine 180 is located (for example, global IP address which is given to a place of installation), and it is also possible to extract the place where the game machine 180 is located from, for example, a frame of communication data and make it as part of the ID data instead of the contents of communication data itself. As another mode of the data which identifies the place where this game machine 180 is located, private IP addresses assigned appropriately for different amusement facility stores so as not to overlap with each other may also be included in the ID data. In this case, even when a global IP address of the amusement facility store is automatically assigned from a higher ISP (Internet Service Provider) through DHCP (Dynamic Host Configuration Protocol), it is possible to identify the amusement facility store and identify the place where the game machine 180 is located. Moreover, the ID data can include data which identifies the game machine 180 or the like. The ID data may be a combination of a plurality of these data. It is possible to identify the place where the game machine 180 in which this dedicated unit 10 is mounted is operating from the relationship between individual ID data of the dedicated unit 10 and a value indicating the place of installation.

[0071] The dedicated unit 10 is provided with second storage means 104. The second storage means 104 is also typically realized by an EEPROM or the like and stores a schedule according to which authentication should be requested. The "schedule according to which authentication should be requested" refers to arbitrary data which can specify the timing for requesting authentication. Examples of this timing include specification of timing with an appropriate repetition period such as once a day, specification of timing using an appropriate time such as a specific time of the day, specification of timing further combining the day of the week on which to perform authentication and specification of timing associated with an appropriate event (e.g., start-up of the game machine authentication management device), though not using any specific time or period. The data of the schedule according to which authentication should be requested can be stored in the second storage means 104 in an appropriate format and the authentication schedule may also be directly specified in the program.

[0072] The dedicated unit 10 can also be further provided with third storage means 106. This third storage means 106 stores a unit penalty setting table which stores set values corresponding to an authentication level about at least one of a setting of operable functions of an electronic money terminal 134, a setting of operable functions of the game machine 180 and a setting of display contents of the display device 118. The third storage means 106 is also typically realized by an EEPROM or the like.

[0073] The dedicated unit 10 may be further provided with time storage means 108 in addition to the above described storage means. This time storage means 108 is used to store a time at which authentication succeeded last time.

[0074] The dedicated unit 10 can be further provided with an RTC (Real Time Clock) 124 which functions as a clock which can reset the time. This RTC 124 is provided with an appropriate backup battery (not shown) and can continue to time even when power to the dedicated unit 10 is stopped or the like. Furthermore, the RTC 124 is connected with manual clock setting means 122 which can accept the manual time setting of the RTC 124 and can also stop the manual time setting based on a signal from function setting means 114. When the time of the RTC 124 is manually changed, the time can be adjusted by operating the manual clock setting means 122 with input using appropriate input means (not shown).

[0075] The dedicated unit 10 is further provided with first communication means 110. The first communication means 110 is an appropriate network interface and is typically an Ethernet (registered trademark) interface or the like which operates with an appropriate bus. The first communication means 110 is connected with the LAN within the amusement facility store site 100. This first communication means 110 is connectable to the WAN 500 (Figure 1) through the router 160 and communicable with the authentication server 24.

[0076] The dedicated unit 10 is further provided with second communication means 112. The second communication means 112 is arbitrary communication means capable of carrying out a local data communication with the game machine 180 and is appropriate communication means using an interface such as RS-232C, USB (Universal Serial Bus), IEEE1394 or the like.

[0077] The dedicated unit 10 is further provided with the electronic money terminal 134. Here, "electronic money" generally refers to payment means which can realize payment by exchanging electronic data instead of currency. That is, electronic money typically refers to stored value-type electronic money using the IC card 130 which becomes the electronic money medium or a medium incorporated in the apparatus, but in addition to this, electronic money can be used as payment means such as a so-called prepaid card, credit card and debit card for which eventual payment with currency is assured, capable of carrying out payment by reading electronic data. Since a medium such as the IC card 130 or an apparatus with a built-in electronic money function (e.g., cellular phone terminal) or the like is used, such an electronic money terminal 134 is provided with a reader/writer 136 configured to be communicable with such a medium or apparatus to enable payment with electronic money. This electronic money terminal 134 is provided with communication means 138 which can communicate with the second communication means 112 of the dedicated unit 10 or third communication means (not shown). The second communication means is used when the electronic money terminal can communicate with the game machine management device using the second communication means, while the third communication means is used when the electronic money terminal cannot communicate with the game machine management device using the second communication means. This third communication means is an arbitrary communication means and can carry out a communication through a normal serial communication or the like using, for example, an RS-232C terminal. The IC card 130 is carried by a player in the amusement facility store to pay for their own game and incorporates an IC memory 132 storing balance data and data to identify the IC card 130.

[0078] The electronic money terminal 134 is a terminal which makes a payment using the IC card 130 instead of payment using currency and is a terminal which should be used only by a registered terminal in a registered place of installation. The dedicated unit 10 of the present invention uses authentication to assure authenticity and correctness of the place of installation required for this electronic money terminal 134.

[0079] The dedicated unit 10 of the present invention has the function setting means 114. When the game machine authentication management device is a processor base system, this function setting means 114 is the function means realized by a calculation apparatus such as a CPU and a main memory 120 such as a RAM is used and a specific procedure of the information processing is specified by the program stored in the appropriate non-volatile storage device (e.g., second storage means 104).

[0080] This function setting means 114 can generate an authentication request to the authentication server 24 and transmit the authentication request and the ID data stored in the first storage means 102 to the authentication server 24 (Figure 1) through the first communication means and receive the authentication result data showing the success or failure of the authentication from the authentication server 24 through the first communication means 110. Furthermore, the function setting means 114 can transmit the electronic money terminal setting data which defines the operable functions of the electronic money terminal 134 to the game machine 180 through the second communication means 112 or the third communication means. In the example shown in Figure 2, the second communication means 112 carries out this transmission. The electronic money terminal setting data is a data signal in an arbitrary format and is the data which can determine whether or not the functions such as the medium reading function and payment function of the electronic money terminal 134 are operable. When the electronic money terminal has some storage means, these electronic money terminal setting data are stored in the electronic money terminal and the electronic money terminal can determine its functions. Furthermore, when the function and operation as the electronic money terminal are determined according to an external instruction (electronic money terminal operation instruction), the function setting means 114 can also transmit an electronic money terminal operation instruction to the electronic money terminal 134 through the second communication means or the third communication means. Examples of the operable functions of the electronic money terminal 134 include a payment function using electronic money, a summation function using electronic money when this electronic money terminal has a mechanism of summation processing and a unit price setting function which sets the unit price of payment using electronic money or the like.

[0081] A more specific operation of this function setting means 114 is to determine a schedule determined by at least one of the authentication schedule data of the second storage means 104 and program using the time indicated by the RTC 124 first. This determines whether or not to send an authentication request. According to the schedule, the authentication request and ID data are transmitted to the authentication server 24 (Figure 1) through the first communication means 110. The function setting means 114 then waits for a response including the authentication result data from the authentication server 24 within a predetermined standby time in a reception-enabled state. This standby time is a time determined in consideration of a time of communication on the network during a time related to the authentication of the authentication server 24 such as 10 seconds and 1 minute. The authentication result data is data which is communicated according to an appropriate protocol and includes data indicating whether authentication succeeded or failed and the format thereof is optional.

[0082] Since this authentication may result in a case of receiving authentication result data of authentication succeeded from the authentication server 24 during a predetermined standby time (hereinafter referred to as "authentication OK"), a case of receiving authentication result data of authentication failed from the authentication server 24 during a predetermined standby time (hereinafter referred to as "authentication NG") or a case of not receiving authentication result

data during a predetermined standby time (hereinafter referred to as "timeout"), the function setting means 114 obtains data (authentication level data) indicating the level of authentication according to these cases. This data can be data, for example, combining appropriate flags.

[0083] Here, in the case of receiving the authentication result data of authentication succeeded from the authentication server during this standby time (case of authentication OK), the function setting means 114 stores any one of the time data of the clock and the authentication time data included in the authentication result data in the time storage means 108. On the other hand, in the case of not receiving the authentication result data of authentication succeeded from the authentication server during a predetermined standby time (case of authentication NG or timeout), the function setting means 114 transmits a signal to the manual clock setting means 122 to stop the reception of the manual time setting. When authentication fails, this prevents the time from being manually reset.

[0084] In at least one of these cases, the function setting means 114 transmits electronic money terminal setting data according to the authentication level data to the electronic money terminal 134 through the second communication means 112 or the third communication means. Alternatively, the electronic money terminal 134 of a different specification can also be used. That is, it is possible to adopt such a specification that the electronic money terminal 134 transmits a signal reporting that a game player is attempting to use electronic money by holding up the IC card 130 of electronic money to make a payment with electronic money and the electronic money terminal 134 also transmits the balance data recorded in the memory 132 of the IC card 130 of the electronic money. In the case of such a specification, the function setting means 114 can judge the signal and balance data from the electronic money terminal 134 and the function setting means 114 can transmit an electronic money terminal operation instruction for extracting data of a predetermined amount of money from the IC card 130 whereby the player is attempting to make a payment at that moment through the second communication means or the third communication means.

[0085] For example, the function setting means 114 can transmit electronic money terminal setting data only in the case of authentication NG or timeout and not transmit electronic money terminal setting data in the case of authentication OK. To which authentication level data the electronic money terminal setting data should be transmitted also depends on the setting as to how the electronic money terminal 134 uses the electronic money terminal setting data for the setting of the operation functions. For example, if the electronic money terminal 134 is designed such that when the electronic money terminal setting data is not received, all functions of the electronic money terminal 134 are operable and restricting the functions of the electronic money terminal 134 requires explicit restrictions with the electronic money terminal setting data, it is possible to prevent the electronic money terminal setting data from being transmitted in the case of authentication OK and allow the electronic money terminal setting data to be transmitted in the case of authentication NG or timeout.

[0086] Furthermore, as another example, in such a case where an electronic money terminal operation instruction is necessary for the electronic money terminal 134 to operate, the function setting means 114 can transmit an electronic money terminal operation instruction for causing the electronic money terminal to make a payment in response to a request from the electronic money terminal only in the case of authentication OK and not transmit such an instruction in the cases of authentication NG and timeout. To which authentication level data an electronic money terminal operation instruction should be transmitted is determined depending on the actual operation of penalties.

[0087] ID data for authentication is registered beforehand in appropriate storage means of the authentication server 24 (Figure 1). With the ID data registered beforehand, the authentication server 24 can determine whether or not authentication should be concluded for the ID data transmitted together with the authentication request from the dedicated unit 10.

[0088] It is when the authentication server 24 receives the authentication result of authentication succeeded from the ID data during a standby time that the authentication result becomes authentication OK. Such an authentication result is obtained when, for example, the game machine 180 managed by the dedicated unit 10 is authentic and the game machine 180 is installed in a place where it is supposed to be installed.

[0089] It is when the authentication server 24 receives an authentication result of authentication failed from the ID data during the standby time that the authentication result becomes authentication NG. Examples of cases where such events actually occur include a case where the dedicated unit is counterfeited, a case where the dedicated unit is used in an unapproved place though it is a regular dedicated unit or a case where communication data is tampered. Besides, there is also a case where a simple operational mistake results in authentication NG. This operational mistake occurs when, for example, the dedicated unit not registered in the authentication server 24 is used or when the business location in which the game machine 180 is installed is a place not registered in the authentication server 24.

[0090] The authentication result times out when the authentication result data is not received within the standby time. Examples of such cases include a case where some communication trouble has occurred, typically a case disconnection of the network cable, malfunction of LAN in a store (e.g., malfunction of the network hub, breakage of a cable or the like) or trouble of the router 60 which connects the LAN with the WAN 500, interruption of the WAN 500 due to maintenance work or the like, authentication server 24 going down (not operating normally) or the like.

[0091] A timeout is often the cause for authentication not becoming ON in a communication at a store of an actual amusement facility and authentication does not often result in NG. When authentication NG results, there is a doubt

about an operational mistake by the operator or unauthorized use by the operator. On the other hand, a timeout is often caused by trouble in the LAN, WAN or the like at the amusement facility managed by the operator. Therefore, handling the case of authentication NG and the case of a timeout across the board on the grounds that they are not cases of authentication OK may place an excessive business burden on the operator. Therefore, the present invention can change at least one of electronic money terminal setting data, electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display data so that different penalties are applied when the authentication result shows authentication NG and when the authentication result shows a timeout.

[0092] At this time, when the function setting means 114 has the third storage means 106, it refers to the unit penalty setting table of the third storage means 106 and can transmit at least one of electronic money terminal setting data, electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display data in at least one of cases of authentication OK, authentication NG and timeout. Depending on the electronic money terminal and the specification of the game machine, it is also possible to suspend transmission of at least one of electronic money terminal setting data, electronic money terminal operation instruction, game machine setting data, game machine operation instruction and display data. When the dedicated unit 10 itself has a unit penalty setting table, even when authentication cannot be performed appropriately due to, for example, network trouble, it is possible to appropriately operate the electronic money terminal 134, game machine 180 and display device in such a case with reference to the unit penalty setting table. Therefore, when authentication fails or a timeout occurs, the dedicated unit 10 can refer to the unit penalty setting table as a default (preset value). The unit penalty setting table stores the set value of the electronic money terminal setting data, set value of the game machine setting data and set value of the display setting data in association with the authentication levels such as authentication OK, authentication NG and timeout respectively so that the function setting means 114 can transmit electronic money terminal setting data, transmit game machine setting data and transmit display setting data. The unit penalty setting table may be adapted so that these set values are common to a plurality of dedicated units 10A, 10B or the unit penalty setting table may also be adapted so that the individual dedicated units 10A, 10B have different set values. At least one of the electronic money terminal setting data, game machine setting data and display data in the unit penalty setting table can be described such that the authentication level differs between authentication NG and a timeout so that different penalties are applied when the authentication result is authentication NG and when the authentication result is a timeout.

[0093] The game machine authentication management device according to another embodiment of the present invention may also be configured to be able to communicate with an authentication scheduling server through the first communication means 110 such as Ethernet (registered trademark). In this case, instead of the unit 10, the authentication scheduling server has second storage means 104 for storing authentication schedule data or a program to define a schedule according to which the game machine authentication management device should request the authentication server 24 to perform authentication and also has instruction transmission means for transmitting an authentication request generating instruction for causing the function setting means 114 to generate an authentication request to the function setting means 114 through the first communication means 110 according to the authentication schedule data or the program. When the authentication scheduling server is a processor base system, this instruction transmission means is function means realized by executing a program using a calculation apparatus and a main storage unit. The authentication scheduling server can be realized through, for example, a server computer identical to the penalty setting server 140 in Figure 1.

[0094] In this embodiment, the function setting means 114 receives an authentication request generating instruction from the instruction transmission means in the authentication scheduling server and thereby transmits an authentication request and ID data to the authentication server 24 through the first communication means 110. The processing thereafter is the same as that in the case of the above described embodiment.

[0095] Here, when the authentication result data indicating that authentication succeeded is received from the authentication server during this standby time (case of authentication OK), the function setting means 114 stores any one of the time data of the clock and the authentication time data included in the authentication result data in time storage means 108. On the other hand, when the authentication result data indicating that authentication succeeded is not received from the authentication server during the predetermined standby time (case of authentication NG or a timeout), the function setting means 114 transmits a signal for causing the manual clock setting means 122 to stop the reception of the manual time setting. When authentication fails, this prevents the time from being manually reset.

[0096] According to the embodiment of the present invention, the function setting means 114 can transmit the game machine setting data which defines operable functions of the game machine 180 to the game machine 180 through the second communication means 112. The operable functions of the game machine 180 are, for example, operations of the game machine as a whole and are a cash payment function and cash summation function or the like when, for example, there is a mechanism for cash payment in game machine 180 (mechanism of credit management or the like using cash coin). Other examples of such operable functions are a service point payment function and a service point summation function when the game machine 180 is provided with a mechanism for payment with service points acquired in a game played (mechanism of point reading or the like of a point card) and functions of limiting purchase of game

items (gadgets) through a network or limiting a network match or limiting access to a network database of the game server when the game machine 180 is provided with a mechanism for the network game using a game server (function of communication with the game server or the like). This game machine setting data is transmitted to the game machine 180 according to the authentication level data in at least one of cases of authentication OK, authentication NG and timeout.

[0097] The game machine authentication management device of the present invention is provided with the display means whose display contents can be changed and the display control means for controlling display means. Figure 2 shows this display device 118 and display control means 116. The display device 118 is, for example, a display device such as a VFD (fluorescence display tube) display device and a liquid crystal display device, and can be used, for example, to report to the player that payment with electronic money is possible in addition to the applications of the present invention. The display control means 116 is, for example, an appropriate controller chip or the like. According to the present invention, this display device 118 provides different expressions in cases of authentication OK, authentication NG and timeout. For example, in the case of authentication NG or a timeout, the display device 118 displays, in addition to normal display, information indicating authentication NG and timeout using predetermined symbols or marks in such a way that only employees at the amusement facility can understand them. Therefore, the function setting means 114 generates display setting data which defines display contents according to the authentication level data, transmits the display setting data to the display control means 116 and the display control means 116 controls the display means 116 so that the display device 118 displays the display contents according to the display setting data in at least one of cases of authentication OK, authentication NG and timeout.

[0098] This display setting data according to the embodiment of the present invention can include display contents warning that the reception of the manual time setting is stopped, display contents warning that a penalty will be set immediately after the time is changed and display contents reporting that cancellation of a penalty setting requires authentication to be concluded successfully.

[0099] The game machine authentication management device 10 or the game machine 180 is further provided with an input device (not shown) and after displaying any one of the above described display contents, when the display contents function setting means 114 accepts the input of the manual time setting from this input device, it can immediately transmit the electronic money terminal setting data according to the authentication level data in cases of either authentication NG or timeout to the electronic money terminal through the second communication means 112 or the third communication means.

[0100] Figure 3 shows the configuration of the game machine 180 according to an embodiment of the present invention. The game machine 180 here is a game machine with which the player can play a game. The game machine 180 is provided with a communication interface 184 which can communicate with the second communication means 112 (or the third communication means (not shown)) of the dedicated unit (game machine authentication management device) 10, a control device 182 which controls the operation of the game machine, an input controller 186 for input operation of the game machine, a coin management section 188 which manages insertion or ejection of medal or cash coins lent out in the store, a speaker section 190 which plays sound effects or the like for the game and a speaker control section 190a, a display section 192 to display the game to the player and a display control section 192a, a storage section 194 which stores a program and various kinds of data to make a game progress, an RTC 196 and manual clock setting means 196a and a time storage section 198 which stores the time at which authentication succeeded last time. Some game machines 180 store game machine setting data in some storage device and set the function and operation of the game machine 180 itself, while others change the function and operation of the device for a game machine operation instruction from outside.

[0101] Figure 4 shows the configuration of a dedicated unit 10' used in another embodiment of the present invention. Furthermore, Figure 5 shows the configuration of a game machine 180' used in this embodiment. In this embodiment, unlike the configuration shown in Figure 2, first communication means 110' is not provided for the dedicated unit 10', but provided for the game machine 180'. In this case, network data through the first communication means 110' is communicated with the dedicated unit 10' through a communication interface 184 and a second communication means 112 and the dedicated unit 10' can perform operation similar to that of the dedicated unit 10.

[0102] Using Figure 6, the configuration of a penalty setting server 140 used in the embodiment of the present invention will be explained. The penalty setting server 140 of the embodiment of the present invention is a server computer provided with nonvolatile storage means 142 such as a hard disk drive, calculation means 146 such as a CPU which operates in cooperation with a main storage unit 144 such as a RAM and communication means 148 such as an Ethernet. (registered trademark) interface. The communication means 148 is connected with a LAN at an amusement facility store and the storage means 142 can communicate with the function setting means 114 of the dedicated unit 10. This penalty setting server 140 stores an integrated penalty setting table in the storage means 142. The function setting means 114 of the dedicated unit (game machine authentication management device) 10 refers to the integrated penalty setting table stored in the penalty setting server 140 through the first communication means 110. As in the case of the unit penalty setting table, the integrated penalty setting table also stores the set value of electronic money terminal setting data, the set value of game machine setting data, the set value of display setting data in association with authentication OK, authen-

tication NG and timeout respectively so that the function setting means 114 can transmit the electronic money terminal setting data, transmit the game machine setting data and transmit the display setting data. As in the case of the unit penalty setting table, the integrated penalty setting table may also be designed so that these set values are common to a plurality of dedicated units 10A, 10B or may also be designed to differ between the individual dedicated units 10A, 10B.

[0103] Furthermore, in the present invention, the game machine 180 can be connected with the computer network through the first communication means 110 or the second communication means 112, the authentication result data includes data indicating whether authentication through the authentication server 24 has succeeded or failed, the authentication result data can include authentication time data from the authentication server 24 and address data of the game server on an outside network to which the game machine 180 is connected. In this way, it is possible to store the time of authentication in the case of authentication OK, for example, in the storage means 108 in Figure 2 and use it for subsequent processing. Furthermore, when authentication OK results especially after authentication NG or a timeout, the game machine 180 can be connected to the game server so that the game can be fully enjoyed.

[0104] A further embodiment of the present invention will be explained using Figure 7. In this embodiment, communication means 148 of a penalty setting server 140 can operate as outside communication means capable of communicating with any one of outside networks which are a computer network 500 such as the Internet and another computer network 600. Examples of the other computer network 600 may include a network which is not open to the public such as a channel connected via a VPN (Virtual Private Network) in the Internet and an ISDN channel separated from the Internet or the like. A LAN in an amusement facility store site 100 can be provided with, for example, a router 162 which has a VPN function or an ISDN terminal adapter (not shown) which has a router function for connections with outside networks. To simply make a distinction, the figure shows that different routers 160 and 162 are used for the computer networks 500 and 600, but it is also possible to change the setting of an identical router or the like and switch between the settings.

[0105] An integrated penalty setting table is made rewritable from a maintenance computer 28 which is on an outside network such as a data center site 200 through communication means 148. The maintenance computer 28 is connected to the outside network through an appropriate router 26. After some trouble, this maintenance computer 28 is used to remotely rewrite the integrated penalty setting table which is in the penalty setting server 140. When the integrated penalty setting table is rewritten, each dedicated unit 10 can change the operation settings of the electronic money terminal 134 and game machine 180 or the like, for example, in the case of authentication NG or a timeout. When the cause of the timeout is, for example, a malfunction of the network 500 and even if the communication of the first communication means 110 is interrupted, this allows the communication to be recovered from the trouble remotely using the maintenance computer.

[0106] Figure 8 is a flow chart showing the processing of the game machine authentication management device 10 according to an embodiment of the present invention. In this embodiment, the game machine authentication management device 10 has second storage means and stores authentication schedule data or a program therein. The functions of the game machine are also set by the game machine authentication management device 10. Furthermore, an integrated penalty setting table is stored in the storage means 142 of the penalty setting server 140 and a unit penalty setting table is stored in the third storage means 106 of the game machine authentication management device 10.

[0107] The function setting means 114 of the game machine authentication management device 10 transmits an authentication request and ID data to the authentication server 24 through the first communication means 110 according to the schedule of at least one of the authentication schedule data of the second storage means 104 and the program (step S102). Then, the function setting means 114 waits for a response including authentication result data from the authentication server 24 within a predetermined standby time in a reception-enabled state (step S104).

[0108] When the function setting means 114 receives the authentication result data from the authentication server 24 during the standby time (step S106) and moreover authentication is concluded successfully (step S108), the authentication level is set to authentication OK (step S110). Furthermore, when the authentication result data received shows an authentication failure, the authentication level is set to authentication NG (step S112). In response to this, when the function setting means 114 has not received the authentication result data from the authentication server 24 during a standby time, the authentication level is set to a timeout (step S114).

[0109] After acquiring the authentication level data in this way, the function setting means 114 tries to invoke the integrated penalty setting table from the storage means 142 of the penalty setting server 140. When it is possible to invoke the desired integrated penalty setting table (step S116), the function setting means 114 refers to the integrated penalty setting table (step S118). On the other hand, when it is not possible to invoke the desired integrated penalty setting table, the function setting means 114 refers to the unit penalty setting table (step S120). These tables store what kind of electronic money terminal setting data and game machine setting data should be transmitted in at least one of cases of authentication OK, authentication NG and timeout.

[0110] The function setting means 114 refers to the table, transmits the electronic money terminal setting data according to the authentication level data to the electronic money terminal 134 through the second communication means 112 or the third communication means (step S122) and further transmits the game machine setting data according to the

authentication level data to the game machine 180 through the second communication means 112 (step S124). These steps of transmitting electronic money terminal setting data and game machine setting data according to the authentication level data in the case of authentication OK are substantially skipped, for example, in a configuration in which the electronic money terminal setting data and game machine setting data are not transmitted when authentication is OK.

[0111] Figure 9 is a flow chart showing the processing of the game machine authentication management device 10 according to an embodiment of the present invention. The function setting means 114 of the game machine authentication management device 10 transmits an authentication request and ID data to the authentication server 24 through the first communication means 110 according to the schedule of at least one of the authentication schedule data of the second storage means 104 and the program (step S102). The function setting means 114 waits for a response including the authentication result data from the authentication server 24 within a predetermined standby time in a reception-enabled state (step S104).

[0112] When the function setting means 114 receives the authentication result data from the authentication server 24 during the standby time (step S106) and moreover when authentication has succeeded (step S108), the authentication level is assumed to be authentication OK (step S110). Furthermore, when the authentication result data received shows that authentication failed, the authentication level is assumed to be authentication NG (step S112). On the other hand, when the function setting means 114 has not received the authentication result data from the authentication server 24 during the standby time, the authentication level is assumed to be a timeout (step S114).

[0113] In the case of authentication OK, the function setting means 114 transmits a signal which allows the manual clock setting means 122 to receive the manual time setting (S130), stores the time data obtained from the RTC 124 or RTC 196 or the time data included in the authentication result data in the time storage means 108 (S132). Furthermore, in the case of authentication NG or a timeout, the function setting means 114 transmits a signal to cause the manual clock setting means 122 to stop the reception of the manual time setting (S134) and further decides whether or not a predetermined time has passed from the time stored in the time storage means 108 at which authentication succeeded last time using the time data obtained from the RTC 124 or RTC 196 or the time data included in the authentication result data (S136). As a result of this decision, when the predetermined time has not passed from the time at which authentication succeeded last time, the system inserts an appropriate wait time in the processing, that is, temporarily stops the processing (S138) and then transmits an authentication request and ID data again. Moreover, as a result of this decision, when a predetermined time has passed from the time at which authentication succeeded last time or in the case of authentication OK, the system transmits electronic money terminal setting data according to the authentication level data to the electronic money terminal (S140). Step S140 of transmitting electronic money terminal setting data according to the authentication level data in the case of authentication OK is substantially skipped, for example, in a configuration in which electronic money terminal setting data and game machine setting data are not transmitted in the case of authentication OK. Though not shown, it is also possible to carry out a step similar to step S140 instead of step S112 and provide a penalty different from authentication NG in the case of a timeout.

[0114] Next, the format of setting data used for the setting of operable functions of the electronic money terminal used in the embodiment of the present invention, setting of operable functions of the game machine and setting of display contents will be explained. These setting data can be expressed as a flag string storing set values of the respective settings in the bit string of the communication data. For example, as enumerated in Table 1 and Table 2, it is possible to express the setting data as 1-Flag1, 1-Flag2 ... FlagZ using the grouped flags and extract such setting data from the communication data. The setting data here is used for the setting of the operable functions of the electronic money terminal, setting of the operable functions of the game machine and setting of display contents, and by transmitting the setting data common to all these settings and distinguishing flags used for the respective settings of the electronic money terminal, the game machine and the dedicated unit, the setting data can be used as data to set the respective operable functions or the like.

[0115] Table 1 shows grouped flags used in the embodiment of the present invention and the setting targets of the flags. The flags in Table 1 are grouped into groups identified by numbers 1, 2, 3 as 1-Flag1, 1-Flag2, First letters of the respective flags indicate group numbers. As for the groups used here, for example, group 1 indicates a payment, group 2 indicates closing processing of a payment (summation processing) and group 3 indicates a setting change. Furthermore, as described in association with each flag, the setting target of 1-Flag1 is an electronic money terminal and that of 1-Flag2 is processing of service points of the game machine. That is, Table 1 shows that 1-Flag1 is a flag which sets payment processing at the electronic money terminal and 1-Flag2 is a flag which sets the payment processing of service points of the game machine. Hereinafter, each flag is expressed as ON when asserted (enabled state) and OFF when not asserted (negated; disabled state) and suppose an asserted (ON) flag prohibits the function set by the flag.

5
10
15
20
25
30
35
40
45
50
55

[Table 1]

Flag name	Group	Setting target
1-Flag 1	1 (payment)	Electronic money terminal
1-Flag 2		Game machine (service point)
1-Flag 3		Game machine (cash coin)
2-Flag 1	2 (payment closing processing)	Electronic money terminal
2-Flag 2		Game machine (service point)
2-Flag 3		Game machine (cash coin)
3-Flag 1	3 (setting change)	Electronic money terminal (unit price setting change), game machine (unit price setting change of service point)
:	:	:

[0116] In addition to the above described flags, Table 1 describes that 1-Flag3 is a flag which sets a payment of the game machine using cash coins, that 2-Flag1 is a flag which sets payment closing processing at the electronic money terminal, that 2-Flag2 is a flag which sets payment closing processing of service points at the game machine, that 2-Flag3 is a flag which sets payment closing processing with cash coins at the game machine, that 3-Flag1 is a flag which sets both a unit price setting change at the electronic money terminal and a unit price setting change of service points at the game machine. In addition to the flags specified here, it is also possible to use flags pursuant to these flags.

[0117] Table 2 shows the settings of special flags which are not grouped using descriptions similar to those in Table 1. FlagZ is a flag which sets a warning display in the display device 118 of the dedicated unit 10, displays a warning when it is ON and displays no warning when it is OFF. In this way, flags which are not especially grouped can also be included in the setting data.

[Table 2]

Flag name	Group	Target
Flag z	-	Warning display on display device in dedicated unit

[0118] Table 3 shows the settings (penalty settings) of the respective flags specified by part of the integrated penalty setting table and the unit penalty setting table. The combination of the values of the respective flags shown in this Table 3 is selected, for example, at the time of authentication NG and timeout, and at the time of authentication OK, the values of the setting table are referred to and the operations of the respective apparatuses are switched. The expression "flag" is used in the explanation, but the operation may also be such an operation that simply changes the operation of the apparatus with reference to the values of the setting table without necessarily having inner flags. In the case of Table 3, penalties which prohibit these operations are executed according to the operations of the target apparatuses of Flag1 of group 1, Flag2, FlagZ of group 1 defined in Table 1 and Table 2.

[Table 3]

Flag	Value
Flag 1 of group 1	ON
Flag 2 of group 1	ON
Flag z	ON
Other than above	OFF

[0119] Table 4 shows the settings (penalty settings) of the respective flags specified by part of the integrated penalty setting table and the unit penalty setting table. The combination of the values of the flags shown in this Table 4 is selected, for example, at the time of authentication NG and at the time of a timeout, and all flags are set to "OFF" at the time of authentication OK. Here, in these penalty setting tables, it is possible to specify whether all flags in each group should be set to "ON" or "OFF" at the same time. For example, 1-Flag1, 1-Flag2 and 1-Flag3 which are all flags of group 1 can be set to "ON." Furthermore, in these penalty setting tables, it is possible to specify whether a plurality of flags having the same index at the end across groups (e.g., 1-Flag1 and 2-Flag2) should be set to "ON" or "OFF" at the same time. The combination of the values of flags shown in Table 4 shows such penalty settings that setting all flags of group 1 to "ON" stops service points at the electronic money terminal and the game machine and a cash payment at the game machine, that setting flags Flag1 and Flag2 of each group to "ON" stops the payment closing processing at the electronic money terminal and a payment with service points and the payment closing processing at the game machine and that setting FlagZ to "ON" displays a warning on the display device 118 of the dedicated unit 10. In this way, with the integrated penalty setting table and the unit penalty setting table, it is possible not only to describe settings that all flags are individually set to "ON" or "OFF" but also make flexible settings using groups.

[Table 4]

Flag	Value
All flags of group 1	ON
Flag 1 and Flag 2 of all groups	ON
Flag z	ON

(continued)

Flag	Value
Other than above	OFF

[0120] In the present invention, the penalty setting server 140 can store authentication pause schedule data which defines at least one of the time at which authentication by the authentication server 24 should be executed or the time at which authentication by the authentication server 24 should be paused in the storage means 142. At this time, the function setting means 114 of the dedicated unit (game machine authentication management device) 10 can, instead of directly sending an authentication request to the authentication server 24, refer to authentication pause schedule data stored in the penalty setting server 140 according to the schedule of at least one of the authentication schedule data or a program stored in the dedicated unit 10 or the second storage means 104 in the authentication scheduling server. Furthermore, even in this case, the operation can be such that the dedicated unit 10 directly sends an authentication request to the authentication server 24, accesses, in the case of NG or a timeout, the penalty setting server 140, refers to authentication pause schedule data and suspends the execution of the penalty in the case of an authentication pause period. When it is the time at which authentication by the authentication server 24 is possible, the function setting means 114 transmits an authentication request and ID data to the authentication server 24 through the first communication means 110. In an embodiment in which an authentication scheduling server is used, the authentication scheduling server can also have this authentication pause schedule data.

[0121] Table 5 is an example of the authentication pause schedule data stored in the penalty setting server 140 and the authentication scheduling server. Here, the time to start and the time to stop a period during which authentication should be paused are defined about two settings. Using such authentication pause schedule data, it is possible to prevent authentication from being carried out for the period specified here. That is, before sending an authentication request to the authentication server 24 according to the program and the authentication schedule data in the second storage means in the dedicated unit 10 and the scheduling server, the function setting means 114 of the dedicated unit refers to such authentication pause schedule data of the penalty setting server, and can thereby determine whether it is the time at which authentication should be carried out by the authentication server or the time at which authentication should not be carried out. Here, the schedule according to which authentication should be paused is specified, but the authentication pause schedule data may also be such data that specifies the schedule according to which authentication should be carried out.

[Table 5]

Setting No.	Time to start authentication pause	Pause time
Setting 1	9:00, October 12, 2004	8 hours
Setting 2	15:00, October 19, 2004	8 hours

[0122] In the embodiment of the present invention, the penalty setting server 140 can store the penalty disabling schedule data that defines the time at which the penalty setting by the penalty authentication server 24 should be enabled or the time at which it should be disabled in the storage means 142.

[0123] At this time, the function setting means 114 of the dedicated unit (game machine authentication management device) 10 refers to the penalty disabling schedule data before or after transmitting an authentication request and ID data to the authentication server 24. The function setting means 114 then does not transmit at least one of electronic money terminal setting data, game machine setting data and display setting data until the time at which the penalty setting should be enabled. In the embodiment in which the authentication scheduling server is used, the authentication scheduling server can also have this authentication pause schedule data.

[0124] Table 6 is an example of the penalty disabling schedule data stored in the penalty setting server 140 and the authentication scheduling server. Here, the time to start the period during which the penalty setting should be disabled and the time during which the penalty setting should be disabled are defined about two settings. Using such penalty disabling schedule data, it is possible to suspend the penalty setting even if authentication is carried out for the period specified here. Here, the schedule according to which the penalty setting should be disabled is specified, but it is also possible to use data to specify a schedule according to which the penalty setting should be enabled.

[Table 6]

Setting No.	Time to start disabling of penalty setting	Disabling time
Setting 1	9:00, October 12, 2004	8 hours
Setting 2	15:00, October 19, 2004	8 hours

[0125] Table 7 is an example of the integrated penalty setting table and the unit penalty setting table. These penalty setting tables specify values as to how flags should be set according to conditions under which a penalty occurs. Since the conditions under which a penalty occurs are decided based on the authentication level data, such a penalty setting table defines values of various setting data to be transmitted from the function setting means 114 to the authentication level data.

[Table 7]

Penalty condition	Flag	Value
Authentication NG	All flags of group 1	ON
	Flag 1 and Flag 2 of all groups	ON
	Flag z	ON
	Other than above	OFF
Timeout	All flags of group 2	ON
	Flag 1 and Flag 2 of all groups	ON
	Flag z	ON
	Other than above	OFF

[0126] In Table 7, in the case of authentication NG, all flags of group 1 are set to ON, and therefore a relatively heavy penalty is set such that payment by the electronic money terminal and payment with cash and service points by the game machine are stopped, but in case of a timeout, 1-Flag3 of the flags of group 1 is set to OFF, and therefore a relatively light penalty is set such that payment with cash coins by the game machine is permitted.

[0127] The integrated penalty setting table used in the present invention can include a first setting table and a second setting table. At this time, the function setting means 114 can refer to the first setting table in a predetermined penalty suspension period after receiving an authentication result or obtaining the authentication level data and refer to the second setting table after the penalty suspension period elapses. This first setting table and second setting table are configured such that their set values differ from each other for at least one of values of the authentication levels. Therefore, it is possible to cause the electronic money terminal 134, game machine 180 and display device or the like to operate by imposing light function restrictions for the penalty suspension period and impose greater function restrictions when the penalty suspension period is past. When the dedicated unit 10 has the third storage means 106, a multi-stage penalty setting using such a penalty suspension period can also be performed when the unit penalty setting table has a first setting table and a second setting table.

[0128] Table 8 is an example of the integrated penalty setting table and the unit penalty setting table having such a first setting table and a second setting table. A relatively light penalty is set immediately after authentication NG and a relatively heavy penalty is set when a predetermined time (here, 24 hours) has elapsed after authentication NG without ever resulting in authentication OK. Here, a setting related to authentication NG is used, but similar processing can also be used, for example, in the case of a timeout.

[Table 8]

Penalty condition	Setting time	Flag	Value
Immediately after authentication NG	-	All flags of group 2	ON
		Flag 1 and Flag 2 of all groups	ON
		Flag z	ON
		Other than above	OFF

(continued)

Penalty condition	Setting time	Flag	Value
Lapse of set time after authentication NG	24 hours	All flags of group 1	ON
		Flag 1 and flag 2 of all groups	ON
		Flag z	ON
		Other than above	OFF

[0129] Table 9 and Table 10 show examples of flags when using a network game using a game server and examples of the integrated penalty setting table and the unit penalty setting table for setting penalties. Using such flags and penalty setting tables, it is also possible to set penalties for the operation functions of the game machine of the network game using the game server.

[Table 9]

Management flag	Contents
Flag 1	Payment with electronic money
Flag 2	Payment with service points
Flag 3	Payment with cash coin
:	:
Flag n	Purchase of electronic item through network in network game
Flag (n+1)	Network match in network game
Flag (n+2)	Network database access in network game
:	:
Flag z	Warning display on screen of dedicated unit

[Table 10]

Penalty set value	
Flag 1,2,n,...(n+1), (n+2)...	ON
Flag z:	ON
Flag other than above:	OFF

[0130] The embodiments of the present invention have been described so far, but the present invention is not limited to the above described embodiments and various modifications, changes and combinations are possible based on the technical thought of the present invention.

[0131] For example, the embodiments have explained so far the case where the present invention is implemented as the game machine authentication management device, but the present invention can also be implemented as a game device. In this case, the game device is provided with a game machine section corresponding to the game machine 180 and a game machine authentication management section corresponding to the dedicated unit (game machine authentication management device) 10. In this case, the game machine authentication management section can be further provided with an electronic money terminal section. This electronic money terminal section may be similar to the electronic money terminal 134 of the game machine authentication management device. Furthermore, in this case, ID data and data which becomes part thereof and which specifies the game machine (value indicating a game machine or the value indicating a game program) may be stored in some storage section. For example, the data may be stored as part of the game program. The data may also be stored in other places. For example, when the data is specified as a MAC address of a communication interface, the data can be stored in the communication interface. Furthermore, the data may also be stored in an ID of the CPU used for a game or boot ROM. Of course, the location of this storage information is not limited and it can be stored in a memory on the game housing side instead of inside the board of the electronic circuit. This allows the game device to be implemented as a game device having components such as a game machine au-

thentication management section, an electronic money terminal section and a game machine section in addition to the manual clock setting means, clock and time storage means. The operations of the game machine authentication management section, electronic money terminal section and game machine section may be similar to the operations of the game machine authentication management device, electronic money terminal and game machine explained in the above described embodiments. Furthermore, in this case, the electronic money terminal section uses not electronic money terminal setting data but payment setting data which defines the setting of a payment with electronic money. Furthermore, the processing in the operation method of the above described dedicated unit 10 can be likewise realized by a game device provided with a game machine authentication management section, game machine section and electronic money terminal section. In addition, each table such as the penalty setting table and each flag can also be realized by a game device provided with a game machine authentication management section, game machine section and electronic money terminal section.

Claims

1. A remote authentication management system comprising:

an authentication server (24) provided with a function of authenticating an apparatus (180) to be authenticated; a penalty setting server (140) which stores integrated penalty setting data, the integrated penalty setting data storing at least one of a first setting table and a second setting table including set values which define an authentication level of the apparatus (180), the first setting table being different from the second table in at least one of the set values that define the authentication level;

an authentication management device (10) which stores unit penalty setting data including a set value which is different from the integrated penalty setting data;

a first network (LAN) which connects the penalty setting server (140) and the apparatus (10); and

a second network (WAN) which connects the first network (LAN) and the authentication server (24),

wherein the authentication server (24) permits operation of the apparatus (180) when the apparatus (10) can invoke the authentication server (24) at predetermined timing, the apparatus (10) accesses the penalty setting server (140) when the apparatus (10) cannot invoke the authentication server (24) at predetermined timing or cannot invoke within a predetermined time, the apparatus (10) refers to the first setting table or the second setting table of the integrated penalty setting table when the access succeeds, and the apparatus (10) refers to the unit penalty setting table when the access fails.

2. The authentication management system according to claim 1, wherein the integrated penalty setting table can be set or referred to by a maintenance computer (28) connected through the network or a different communication path.

3. The authentication management system according to claim 1, wherein the unit penalty setting table can be set or referred to from the maintenance computer (28) connected through the network or a different communication path.

4. The authentication management system according to claim 2 or 3, wherein the maintenance computer (28) is the authentication server (24).

5. The authentication management system according to claim 1, wherein an authentication scheduling server which stores authentication schedule data which determines the predetermined timing is further connected to the network.

6. The authentication management system according to claim 5, wherein the authentication scheduling server is the penalty setting server (140).

7. The authentication management system according to claim 5, wherein an authentication pause scheduling server which stores authentication pause schedule data is further connected to the network.

8. The authentication management system according to claim 7, wherein the authentication pause scheduling server is the penalty setting server or the authentication scheduling server.

9. An apparatus to be authenticated, comprising:

first communication means configured to be connectable to a computer network and communicable with an authentication server;

first storage means for storing ID data for authentication;
 second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server;
 payment means configured to be communicable with at least one of payment apparatuses through the third communication means; and
 function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and change a payment function for at least one of the payment apparatuses based on payment setting data which defines a payment setting,
 wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means; waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time; acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and changes the payment function for at least one of the payment apparatuses based on payment setting data according to the authentication level data with any one of the events.

10. An authentication management device, comprising

first communication means configured to be connectable to a computer network and communicable with an authentication server;
 second communication means configured to be communicable with the apparatus to be authenticated;
 first storage means for storing ID data for authentication;
 second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server;
 payment means configured to be communicable with at least one of payment apparatuses through the second communication means or third communication means; and
 function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit payment means setting data which defines operable functions of the payment means or a payment means operation instruction according to the payment means setting data to the payment means through the second communication means or the third communication means,
 wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means; waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time and transmits the payment means setting data according to the authentication level data or the payment means operation instruction to the payment means through the second communication means or the third communication means at any one of the cases or suspends the transmission of the payment means setting data or the payment means operation instruction through the second communication means or the third communication means according to the authentication level data with any one of the events.

11. A penalty setting server to be used for an authentication management device or an apparatus to be authenticated, configured to be communicable with the function setting means through the first communication means of the apparatus to be authenticated according to claim 9 or the authentication management device according to claim 10 through the computer network, comprising:

storage means for storing the integrated penalty setting table; and
 outside communication means communicable with an outside network connected to any one of the computer
 network and another computer network logically separated from the computer network,
 wherein the integrated penalty setting table is configured to be rewritable from a maintenance computer in the
 outside network through the outside communication means.

12. A method of operating a remote authentication management system, comprising an authentication server (24)
 provided with a function of authenticating an apparatus to be authenticated (180), a penalty setting server (140)
 which stores integrated penalty setting data, the integrated penalty setting data storing at least one of a first setting
 table and a second setting table including set values which define authentication levels of the apparatus (180) and
 the first setting table being different from the second table in at least one of the set values which define the authen-
 tication levels, an authentication management device (10) which stores unit penalty setting data including a set
 value which is different from the integrated penalty setting data, a first network (LAN) which connects the penalty
 setting server and the apparatus and a second network (WAN) which connects the first network (LAN) and the
 authentication server (24), the method comprising the steps of:

permitting the operation of the apparatus (180) by the authentication server (24) when the device (10) can
 invoke the authentication server (24) at predetermined timing;
 at the device (10), accessing the penalty setting server (140) when the apparatus cannot invoke the authentication
 server (24) at predetermined timing or cannot invoke the authentication server (24) within a predetermined time;
 at the device (10), referring to the first setting table or the second setting table of the integrated penalty setting
 table when the access succeeds; and
 at the device (10), referring to the unit penalty setting table when the access fails.

13. A method of operating an authentication management device, comprising first communication means configured to
 be connectable to a computer network and communicable with an authentication server, second communication
 means configured to be communicable with an apparatus to be authenticated, first storage means for storing ID
 data for authentication, second storage means for storing authentication schedule data or a program to determine
 a schedule according to which authentication should be requested from the authentication server, payment means
 configured to be communicable with at least one of payment apparatuses through the second communication means
 or third communication means and function setting means configured to be able to generate an authentication
 request to the authentication server, transmit the authentication request and the ID data stored in the first storage
 means to the authentication server through the first communication means, receive the authentication result data
 indicating a success or failure of authentication from the authentication server through the first communication means
 and transmit payment means setting data which defines operable functions of the payment means or a payment
 means operation instruction according to the payment means setting data to the payment means through the second
 communication means or the third communication means, the method comprising the steps of:

with the function setting means, transmitting the authentication request and the ID data to the authentication
 server through the first communication means according to a schedule based on at least one of the authentication
 schedule data and the program of the second storage means;
 at the function setting means, waiting for a response including the authentication result data from the authen-
 tication server in a reception-enabled state within a predetermined standby time;
 at the function setting means, acquiring authentication level data which can indicate any one of the events that
 the authentication result data indicating that authentication succeeded has been received from the authentication
 server during the predetermined standby time, that the authentication result data indicating that authentication
 failed has been received from the server during the predetermined standby time and that the authentication
 result data has not been received during the predetermined standby time; and
 with the function setting means, transmitting the payment means setting data according to the authentication
 level data or the payment means operation instruction to the payment means through the second communication
 means or the third communication means at any one of the cases or suspending the transmission of the payment
 means setting data or the payment means operation instruction through the second communication means or
 the third communication means according to the authentication level data at any one of the cases.

14. A method of operating a penalty setting server configured to be communicable with the function setting means
 through the first communication means of the apparatus to be authenticated according to claim 9 or the authentication
 management device according to claim 10 through the computer network, comprising the steps of:

storing the integrated penalty setting table in the storage means the penalty setting server;
 with outside communication means of the penalty setting server making communicable with an outside network
 connected to any one of the computer network and another computer network logically separated from the
 computer network; and
 5 configuring the integrated penalty setting table to be rewritable from a maintenance computer which is in the
 outside network through the outside communication means.

- 15 15. A computer program for causing a computer to operate as an authentication management apparatus, the computer
 comprising first communication means configured to be connectable to a computer network and communicable with
 10 an authentication server, second communication means configured to be communicable with an apparatus to be
 authenticated, first storage means for storing ID data for authentication, second storage means for storing authen-
 tication schedule data or a program to determine a schedule according to which authentication should be requested
 from the authentication server, payment means configured to be communicable with at least one of payment appa-
 15 ratuses through the second communication means or third communication means and calculation means for oper-
 ating as function setting means configured to be able to generate an authentication request to the authentication
 server, transmit the authentication request and the ID data stored in the first storage means to the authentication
 server through the first communication means, receive the authentication result data indicating a success or failure
 of authentication from the authentication server through the first communication means and configured to be able
 20 to transmit payment means setting data which defines operable functions of the payment means or a payment
 means operation instruction according to the payment means setting data to the payment means through the second
 communication means or third communication means, causing the computer to execute:

a step by the calculation means of transmitting the authentication request and the ID data to the authentication
 server through the first communication means according to a schedule based on at least one of the authentication
 25 schedule data and the program of the second storage means;
 a step by the calculation means of waiting for a response including the authentication result data from the
 authentication server in a reception-enabled state within a predetermined standby time;
 a step by the calculation means of acquiring authentication level data which can indicate any one of the events
 30 that the authentication result data indicating that authentication succeeded has been received from the authen-
 tication server during the predetermined standby time, that the authentication result data indicating that authen-
 tication failed has been received from the server during the predetermined standby time and that the authenti-
 cation result data has not been received during the predetermined standby time; and
 a step by the calculation means of transmitting the payment means setting data according to the authentication
 level data or the payment means operation instruction to the payment means through the second communication
 35 means or the third communication means at any one of the cases or suspending the transmission of the payment
 means setting data or the payment means operation instruction through the second communication means or
 the third communication means according to the authentication level data at any one of the cases.

- 40 16. A computer program which causes calculation means of a penalty setting server configured to be communicable
 with the function setting means through the first communication means of the apparatus to be authenticated according
 to claim 9 or the authentication management device according to claim 10 through the computer network to execute:

a step of storing the integrated penalty setting table in the storage means of the penalty setting server;
 a step of making the outside communication means of the penalty setting server communicable with any one
 45 of the computer network and an outside network connected to another computer network logically separated
 from the computer network; and
 a step of configuring the integrated penalty setting table to be rewritable from a maintenance computer which
 is in the outside network through the outside communication means.

- 50 17. A recording medium which stores the program according to claim 15 or 16.

18. A game machine authentication management device, comprising:

first communication means configured to be connectable to a computer network and communicable with an
 55 authentication server;
 second communication means configured to be communicable with a game machine;
 first storage means for storing ID data for authentication;
 second storage means for storing authentication schedule data or a program to determine a schedule according

to which authentication should be requested from the authentication server;
 an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means; and
 5 function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means,
 10 wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means, waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time, acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time, and transmits the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases or suspends the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

19. A game machine authentication management device comprising:

second communication means configured to be communicable with a game machine provided with first communication means connectable to a computer network including an authentication server ;
 30 first storage means for storing ID data for authentication;
 second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server;
 an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means; and
 35 function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and the second communication means and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means,
 40 wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means and the second communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means; waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time; acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and transmits the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases or suspends the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data with any one of the events.

20. A game machine authentication management device comprising:

first communication means configured to be connectable to a computer network and communicable with an authentication server and an authentication server scheduling server;

second communication means configured to be communicable with a game machine;

first storage means for storing ID data for authentication;

an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means; and

function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means,

wherein the authentication scheduling server comprises second storage means for storing an authentication schedule data or a program which determines a schedule according to which the game machine authentication management device should request authentication from the authentication server and instruction transmission means for transmitting an authentication request generating instruction for causing the function setting means to generate the authentication request to the function setting means through the first communication means according to the authentication schedule data or the program,

upon receiving the authentication request generating instruction from the instruction transmission means, the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means; waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time; acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and transmits the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases or suspends the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data with any one of the events.

21. The game machine authentication management device according to any one of claims 18 to 20, wherein the function setting means is configured to be able to transmit game machine setting data which defines operable functions of the game machine or a game machine operation instruction according to the game machine setting data to the game machine through the second communication means and transmits the game machine setting data or the game machine operation instruction through the second communication means at least at any one of the events according to the authentication level data or suspends the transmission of the game machine setting data or the game machine operation instruction to the game machine through the second communication means.

22. The game machine authentication management device according to any one of claims 18 to 20, further comprising display means whose display contents can be changed and display control means for controlling the display means, wherein the function setting means generates display setting data which defines the display contents according to the authentication level data, transmits the display setting data to the display control means, and the display control means controls the display means so that the display means displays display contents according to the display setting data at least at any one of the events or controls the display means so that the display means stops the display according to the display setting data.

23. The game machine authentication management device according to any one of claims 18 to 20, wherein a penalty setting server configured to be communicable with the function setting means stores an integrated penalty setting table which stores set values of the electronic money terminal setting data corresponding to the authentication levels, the function setting means refers to the integrated penalty setting table stored in the penalty setting server through

the first communication means about the setting of operable functions of the electronic money terminal, transmits the electronic money terminal setting data or the electronic money terminal operation instruction at least at any one of the cases or suspends the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction at least with any one of the events.

- 5
24. The game machine authentication management device according to claim 21, wherein a penalty setting server configured to be communicable with the function setting means stores an integrated penalty setting table which stores set values of the game machine setting data corresponding to the authentication levels,
10 the function setting means refers to the integrated penalty setting table stored in the penalty setting server through the first communication means about the setting of operable functions of the game machine, transmits the game machine setting data or the game machine operation instruction at least at any one of the cases or suspends the transmission of the game machine setting data or the game machine operation instruction at least with any one of the events.
- 15 25. The game machine authentication management device according to claim 22, wherein a penalty setting server configured to be communicable with the function setting means stores an integrated penalty setting table which stores set values of the display setting data corresponding to the authentication levels,
the function setting means refers to the integrated penalty setting table stored in the penalty setting server through the first communication means and controls the display means.
20
26. The game machine authentication management device according to claim 20, wherein the authentication scheduling server stores authentication pause schedule data which defines at least one of a time at which authentication by the authentication server should be executed and a time at which authentication by the authentication server should be paused, and
25 the function setting means refers to the authentication pause schedule data stored in the authentication scheduling server according to a schedule based on at least one of the authentication schedule data stored in the second storage means and a program, determines whether or not it is the time at which authentication should be executed by the authentication server and transmits the authentication request and the ID data to the authentication server through the first communication means.
30
27. The game machine authentication management device according to any one of claims 23 to 25, wherein the penalty setting server stores authentication pause schedule data which defines at least one of a time at which authentication by the authentication server should be executed and a time at which authentication by the authentication server should be paused, and
35 the function setting means refers to the authentication pause schedule data stored in the penalty setting server according to a schedule based on at least one of the authentication schedule data stored in the second storage means and a program, determines whether or not it is the time at which authentication should be executed by the authentication server and transmits the authentication request and the ID data to the authentication server through the first communication means.
40
28. The game machine authentication management device according to claim 20, wherein the authentication scheduling server stores penalty disabling schedule data which defines at least one of a time at which the penalty setting should be enabled or a time at which the penalty setting should be disabled, and
45 the function setting means refers to the penalty disabling schedule data stored in the authentication scheduling server before or after transmitting the authentication request and the ID data to the authentication server and does not transmit at least one of the electronic money terminal setting data, the electronic money terminal operation instruction, the game machine setting data, the game machine operation instruction and the display setting data corresponding to any one of authentication level data that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that authentication result data
50 has not been received during the predetermined standby time at least until the time at which the penalty setting should be enabled next time or stops the suspension of the transmission of the electronic money terminal setting data, the electronic money terminal operation instruction, the game machine setting data, the game machine operation instruction and the display setting data corresponding to the authentication level data that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time until the time.
55
29. The game machine authentication management device according to any one of claims 23 to 25, wherein the penalty setting server stores penalty disabling schedule data which defines at least one of a time at which the penalty setting

should be enabled or a time at which the penalty setting should be disabled, and the function setting means refers to the penalty disabling schedule data stored in the penalty setting server before or after transmitting the authentication request and the ID data to the authentication server and does not transmit at least one of the electronic money terminal setting data, the electronic money terminal operation instruction, the game machine setting data, the game machine operation instruction and the display setting data corresponding to any one of authentication level data that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that authentication result data has not been received during the predetermined standby time at least until the time at which the penalty setting should be enabled next time or stops the suspension of the transmission of the electronic money terminal setting data, the electronic money terminal operation instruction, the game machine setting data, the game machine operation instruction and the display setting data corresponding to the authentication level data that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time until the time.

30. The game machine authentication management device according to any one of claims 18 to 22, further comprising third storage means for storing a unit penalty setting table which stores set values corresponding to the authentication levels about at least one of the setting of operable functions of the electronic money terminal, the setting of operable functions of the game machine and the setting of the display contents, wherein the function setting means refers to the unit penalty setting table, transmits, at least at any one of the events, the electronic money terminal setting data, the electronic money terminal operation instruction, the game machine setting data, the game machine operation instruction and the display setting data or suspends the transmission of the electronic money terminal setting data, the electronic money terminal operation instruction, the game machine setting data, the game machine operation instruction and the display setting data.

31. The game machine authentication management device according to any one of claims 23 to 25, wherein the integrated penalty setting table comprises a first setting table and a second setting table, the function setting means refers to the first setting table for a predetermined penalty suspension period after receiving the authentication result or after acquiring the authentication level data and refers to the second setting table after the lapse of the penalty suspension period, and the first setting table is configured to be different from the second setting table in the set value for at least one of values of the authentication levels.

32. The game machine authentication management device according to claim 30, wherein the integrated penalty setting table comprises a first setting table and a second setting table, the function setting means refers to the first setting table for a predetermined penalty suspension period after receiving the authentication result or after acquiring the authentication level data and refers to the second setting table after the lapse of the penalty suspension period, and the first setting table and the second setting table are configured to be different from each other in the set value for at least one of values of the authentication levels.

33. The game machine authentication management device according to any one of claims 18 to 20, wherein the ID data includes a value indicating the game machine authentication management device and the ID data further includes at least one of a value indicating the place of installation and a value indicating the game machine.

34. The game machine authentication management device according to any one of claims 18 to 20, wherein the game machine is connectable to the computer network through the first communication means, the authentication result data includes data indicating whether authentication by the authentication server succeeded or failed, and the authentication result data includes authentication time data from the authentication server and address data of a game server on the outside network to which the game machine is connected.

35. A game device comprising:

first communication means configured to be connectable to a computer network and communicable with an authentication server;
first storage means for storing ID data for authentication;
second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server;

a reader/writer section configured to be communicable with at least one of an electronic money medium or an apparatus with a built-in electronic money function;
 function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server
 5 through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and change a payment function for at least one of the electronic money medium and the apparatus with a built-in electronic money function based on the payment setting data which defines a payment setting,

10 wherein the function setting means transmits the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data of the second storage means and program; waits for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time; acquires authentication level data which can indicate any one of the events that the authentication result data indicating that authentication
 15 succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and changes the payment function for at least one of the electronic money medium and the apparatus with a built-in electronic money function based on payment setting data according to the authentication level data at least
 20 at any one of the events.

36. A method of operating a game machine authentication management device, comprising first communication means configured to be connectable to a computer network and communicable with an authentication server, second communication means configured to be communicable with a game machine, first storage means for storing ID data
 25 for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means and function setting means configured
 30 to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means, and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the
 35 electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means, the method comprising the steps of:

with the function setting means, transmitting the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication
 40 schedule data and the program of the second storage means;
 at the function setting means, waiting for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time;
 at the function setting means, acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication
 45 server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and
 with the function setting means, transmitting the electronic money terminal setting data or the electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through
 50 the second communication means or the third communication means at any one of the cases or suspending the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the events.

37. A method of operating a game machine authentication management device, comprising second communication means configured to be communicable with a game machine provided with first communication means connectable
 55 to a computer network including an authentication server, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to

which authentication should be requested from the authentication server, an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means and function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and the second communication means, and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means, the method comprising the steps of:

with the function setting means, transmitting the authentication request and the ID data to the authentication server through the first communication means and the second communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means; a step by the function setting means of waiting for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time; a step by the function setting means of acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and a step by the function setting means of transmitting the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases or suspending the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

38. A method of operating a game machine authentication management device, comprising first communication means configured to be connectable to a computer network and communicable with an authentication server and an authentication server scheduling server, second communication means configured to be communicable with a game machine, first storage means for storing ID data for authentication, an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means and function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means, and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means, the device configured to be communicable with the authentication scheduling server, wherein the authentication scheduling server comprises second storage means for storing an authentication schedule data or a program which determines a schedule according to which the game machine authentication management device should request authentication from the authentication server and instruction transmission means for transmitting an authentication request generating instruction for causing the function setting means to generate the authentication request to the function setting means through the first communication means according to the authentication schedule data or the program, the method comprising the steps of:

with the function setting means, receiving the authentication request generating instruction from the instruction transmission means; with step of the function setting means, transmitting the authentication request and the ID data to the authentication server through the first communication means; at the function setting means, waiting for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time; at the function setting means, acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication

server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and
 with the function setting means, transmitting the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases or suspending the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

39. A method of operating a game device comprising first communication means configured to be connectable to a computer network and communicable with an authentication server, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, a reader/writer section configured to be communicable with at least one of an electronic money medium or an apparatus with a built-in electronic money function, function setting means configured to be able to generate an authentication request to the authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and change a payment function for at least one of the electronic money medium and the apparatus with a built-in electronic money function based on the payment setting data which defines a payment setting, the method comprising the steps of:

with the function setting means, transmitting the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data of the second storage means and program;
 at the function setting means, waiting for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time;
 at the function setting means, acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and
 with step of the function setting means, changing the payment function for at least one of the electronic money medium and the apparatus with a built-in electronic money function based on payment setting data according to the authentication level data at least at any one of the events.

40. A computer program for causing a computer to operate as a game machine authentication management device, comprising first communication means configured to be connectable to a computer network and communicable with an authentication server, second communication means configured to be communicable with a game machine, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means and calculation means for operating as function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means, the computer program causing the computer to execute:

a step by the calculation means of transmitting the authentication request and the ID data to the authentication server through the first communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means;
 a step by the calculation means of waiting for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time;

a step by the calculation means of acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and

a step by the calculation means of transmitting the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases or suspending the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

- 41.** A computer program for causing a computer to operate as a game machine authentication management device, comprising second communication means configured to be communicable with a game machine provided with first communication means connectable to a computer network including an authentication server, first storage means for storing ID data for authentication, second storage means for storing authentication schedule data or a program to determine a schedule according to which authentication should be requested from the authentication server, an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means and calculation means operating as function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means and the second communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and the second communication means and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means, the computer program causing the computer to execute:

a step by the calculation means of transmitting the authentication request and the ID data to the authentication server through the first communication means and the second communication means according to a schedule based on at least one of the authentication schedule data and the program of the second storage means;

a step by the calculation means of waiting for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time;

a step by the calculation means of acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and

a step by the calculation means of transmitting the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases or suspending the transmission of the electronic money terminal setting data or the electronic money terminal operation instruction through the second communication means or the third communication means according to the authentication level data at any one of the cases.

- 42.** A computer program for causing a computer to operate as a game machine authentication management device, comprising first communication means configured to be connectable to a computer network and communicable with an authentication server and an authentication server scheduling server, second communication means configured to be communicable with a game machine, first storage means for storing ID data for authentication, an electronic money terminal provided with a reader/writer section configured to be communicable with at least one of an electronic money medium and an apparatus with a built-in electronic money function and configured to be made communicable through the second communication means or third communication means and calculation means operating as function setting means configured to be able to generate an authentication request to an authentication server, transmit the authentication request and the ID data stored in the first storage means to the authentication server through the first communication means, receive the authentication result data indicating a success or failure of authentication from the authentication server through the first communication means and transmit electronic money terminal setting data which defines operable functions of the electronic money terminal or an electronic money

terminal operation instruction according to the electronic money terminal setting data to the electronic money terminal through the second communication means or the third communication means, the computer program causing the computer to execute:

5 a step by the calculation means of receiving the authentication request generating instruction from the instruction transmission means;
a step by the calculation means of transmitting the authentication request and the ID data to the authentication server through the first communication means;
a step by the calculation means of waiting for a response including the authentication result data from the authentication server in a reception-enabled state within a predetermined standby time;
10 a step by the calculation means of acquiring authentication level data which can indicate any one of the events that the authentication result data indicating that authentication succeeded has been received from the authentication server during the predetermined standby time, that the authentication result data indicating that authentication failed has been received from the server during the predetermined standby time and that the authentication result data has not been received during the predetermined standby time; and
15 a step by the calculation means of transmitting the electronic money terminal setting data or electronic money terminal operation instruction according to the authentication level data to the electronic money terminal through the second communication means or the third communication means at any one of the cases.

20 **43.** A penalty setting server to be used for a game authentication management device, configured to be communicable with the function setting means through the first communication means of the game authentication management device according to any one of claims 18 to 20 or the game device according to claim 35 through the computer network, comprising:

25 storage means for storing the integrated penalty setting table; and
outside communication means communicable with an outside network connected to any one of the computer network and another computer network logically separated from the computer network,
wherein the integrated penalty setting table is configured to be rewritable from a maintenance computer in the outside network through the outside communication means.
30

35

40

45

50

55

FIG.1

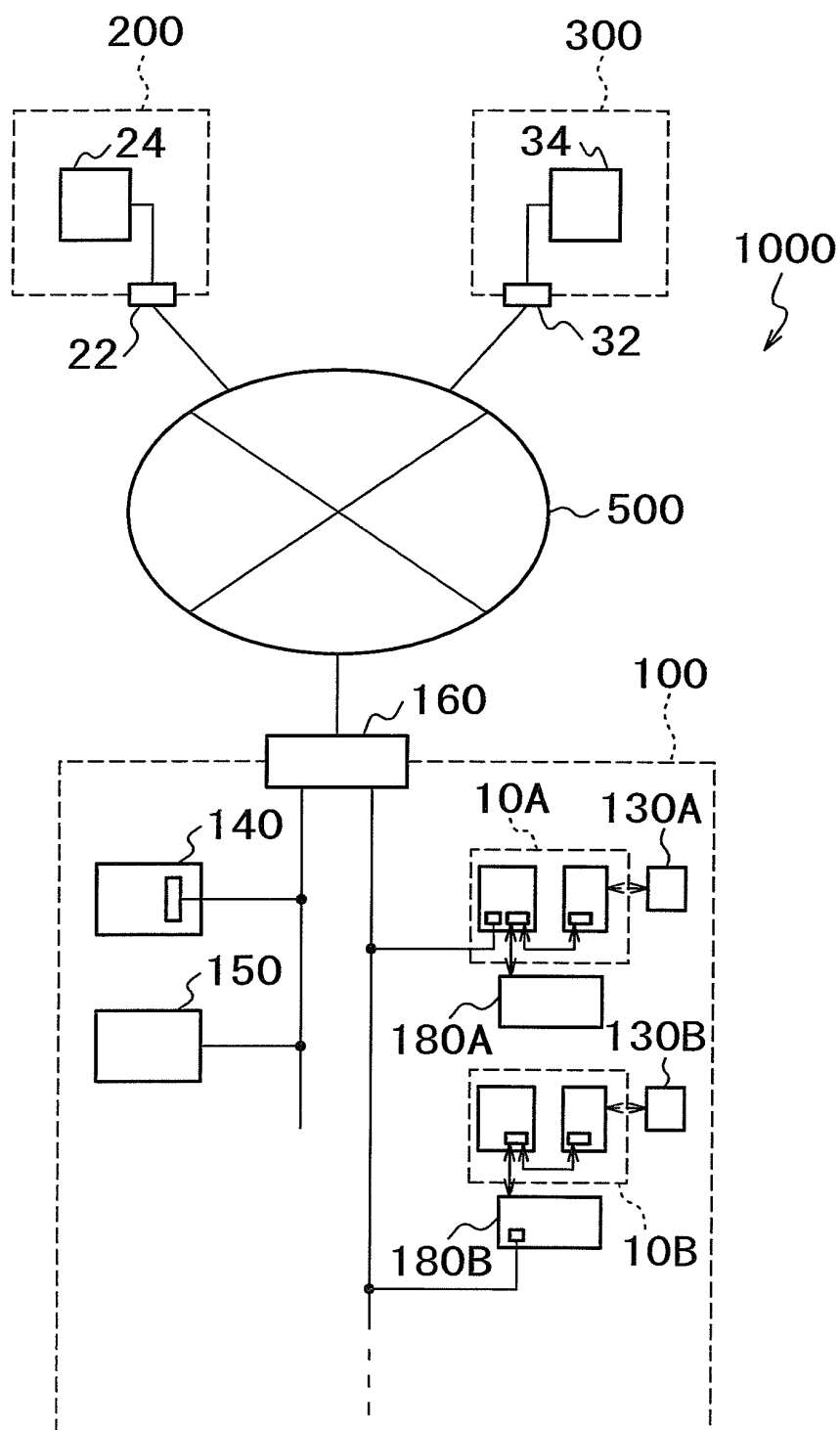


FIG.2

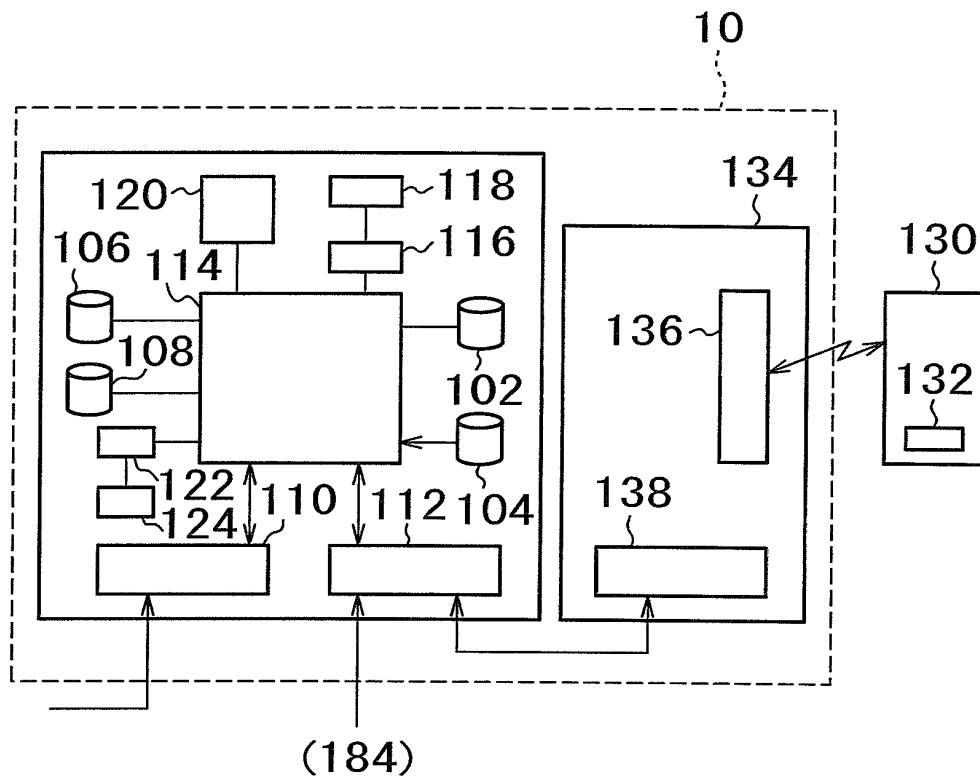


FIG.3

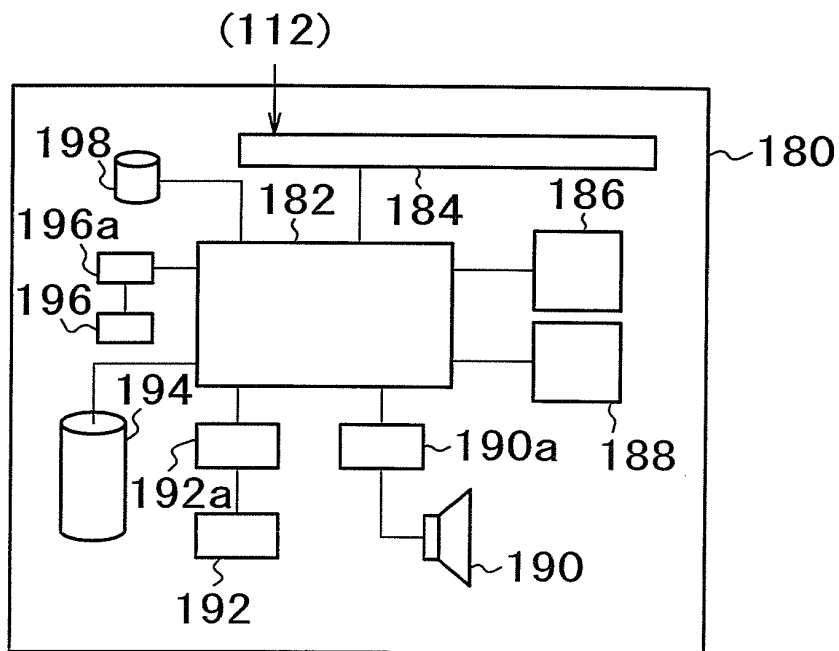


FIG.4

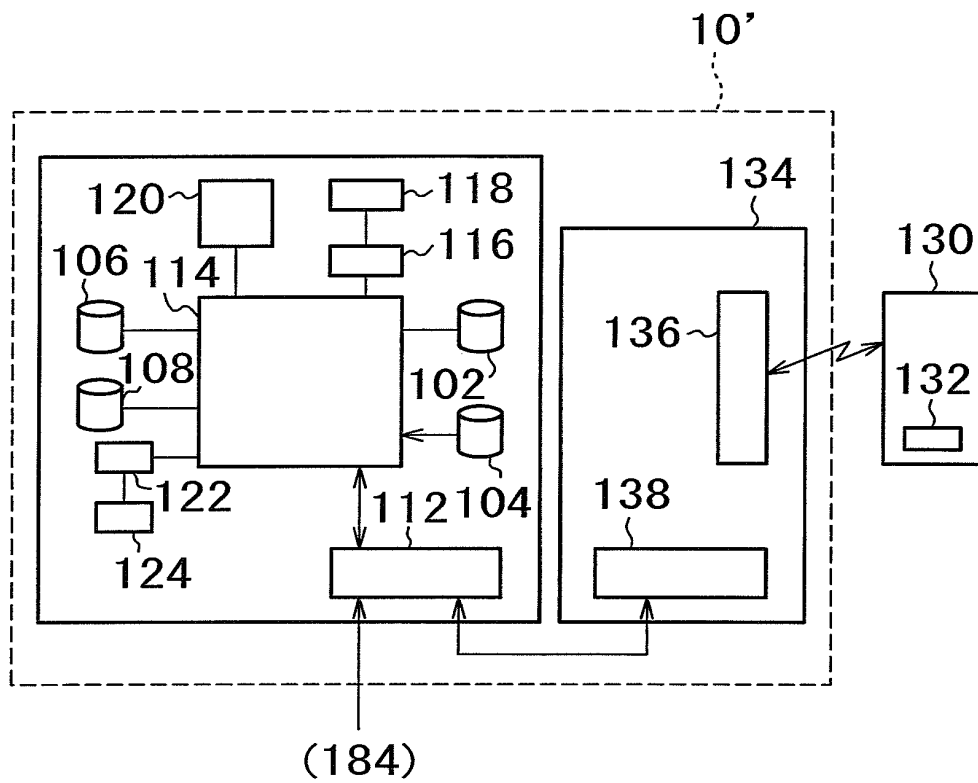


FIG.5

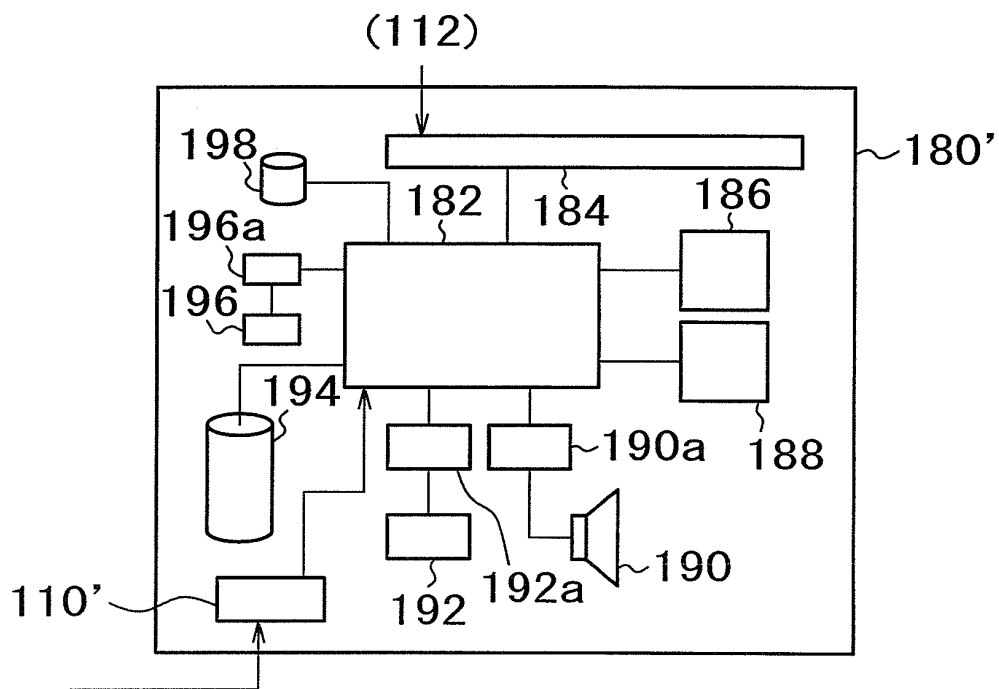


FIG.6

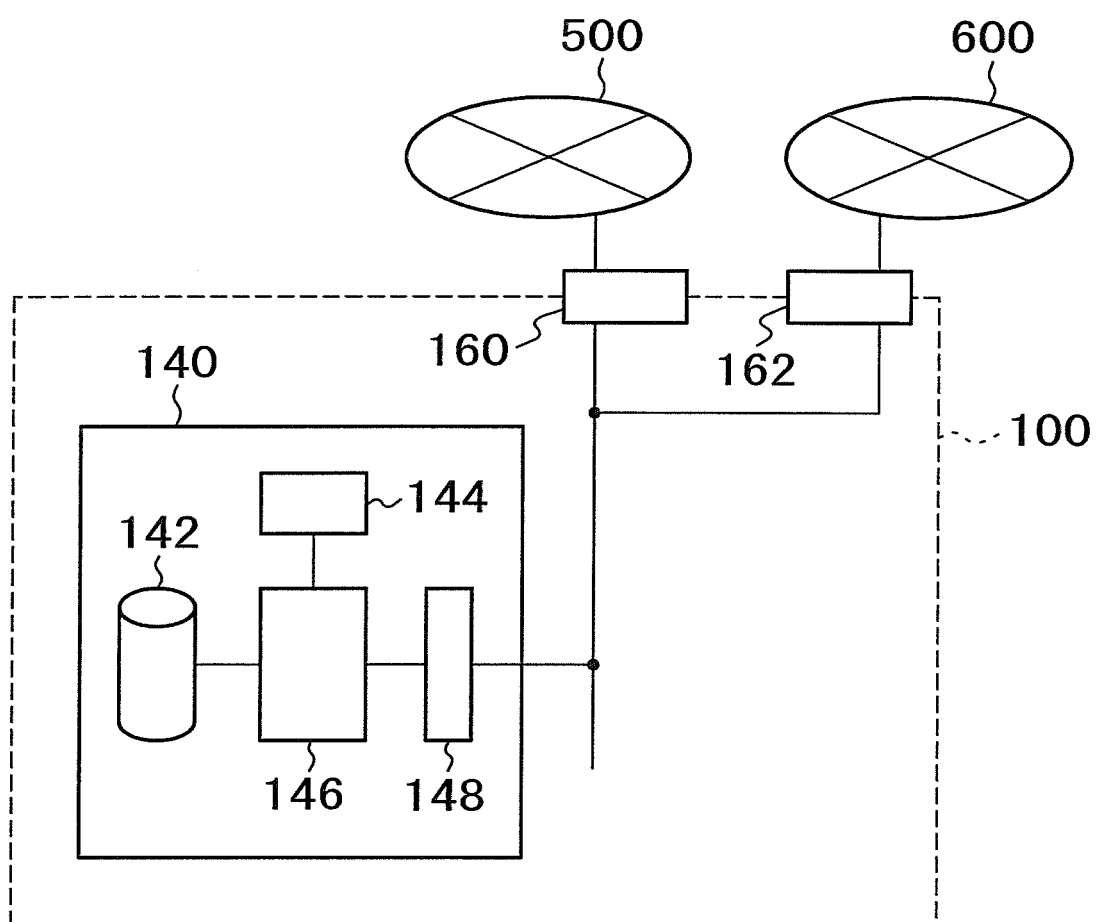


FIG.7

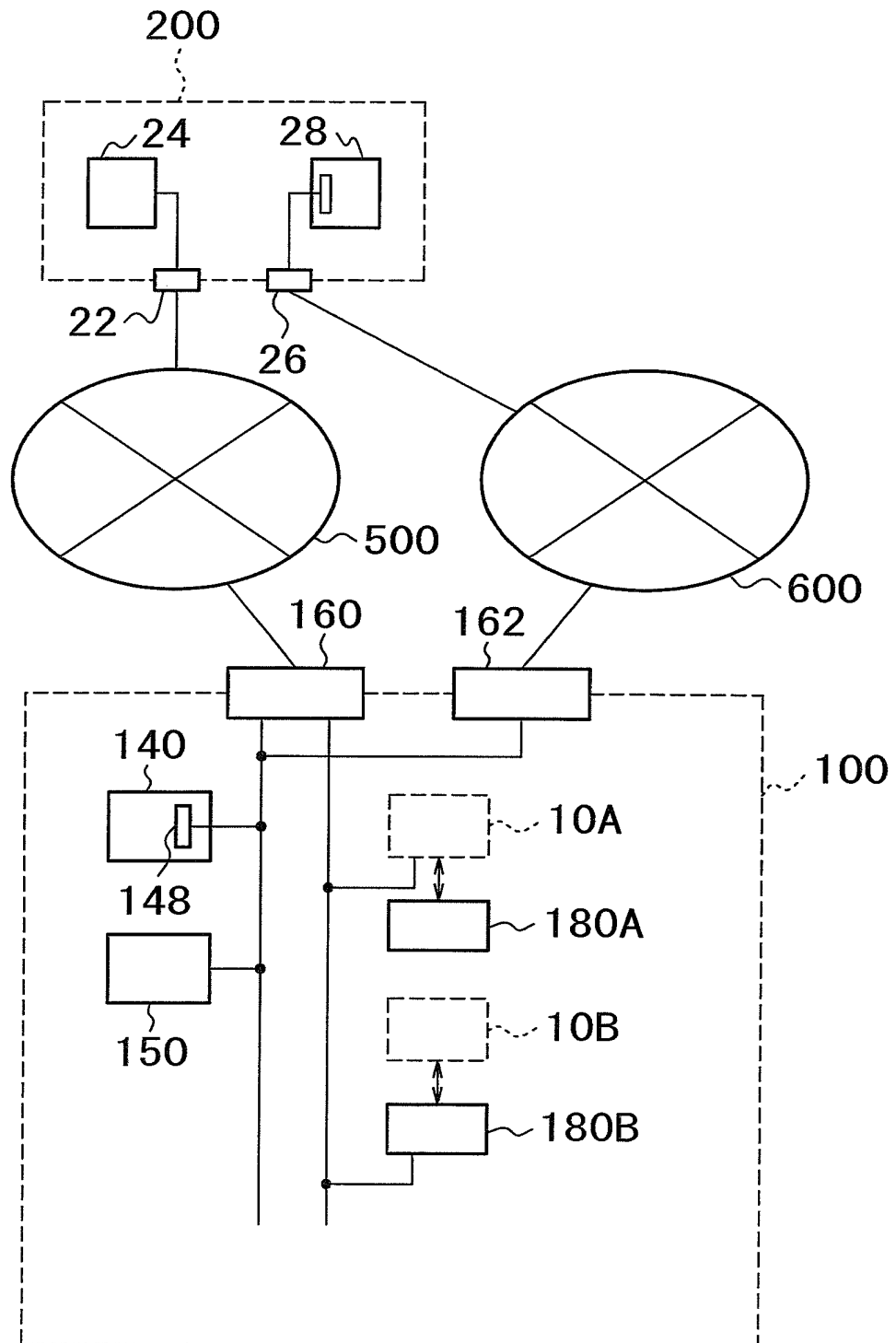


FIG.8

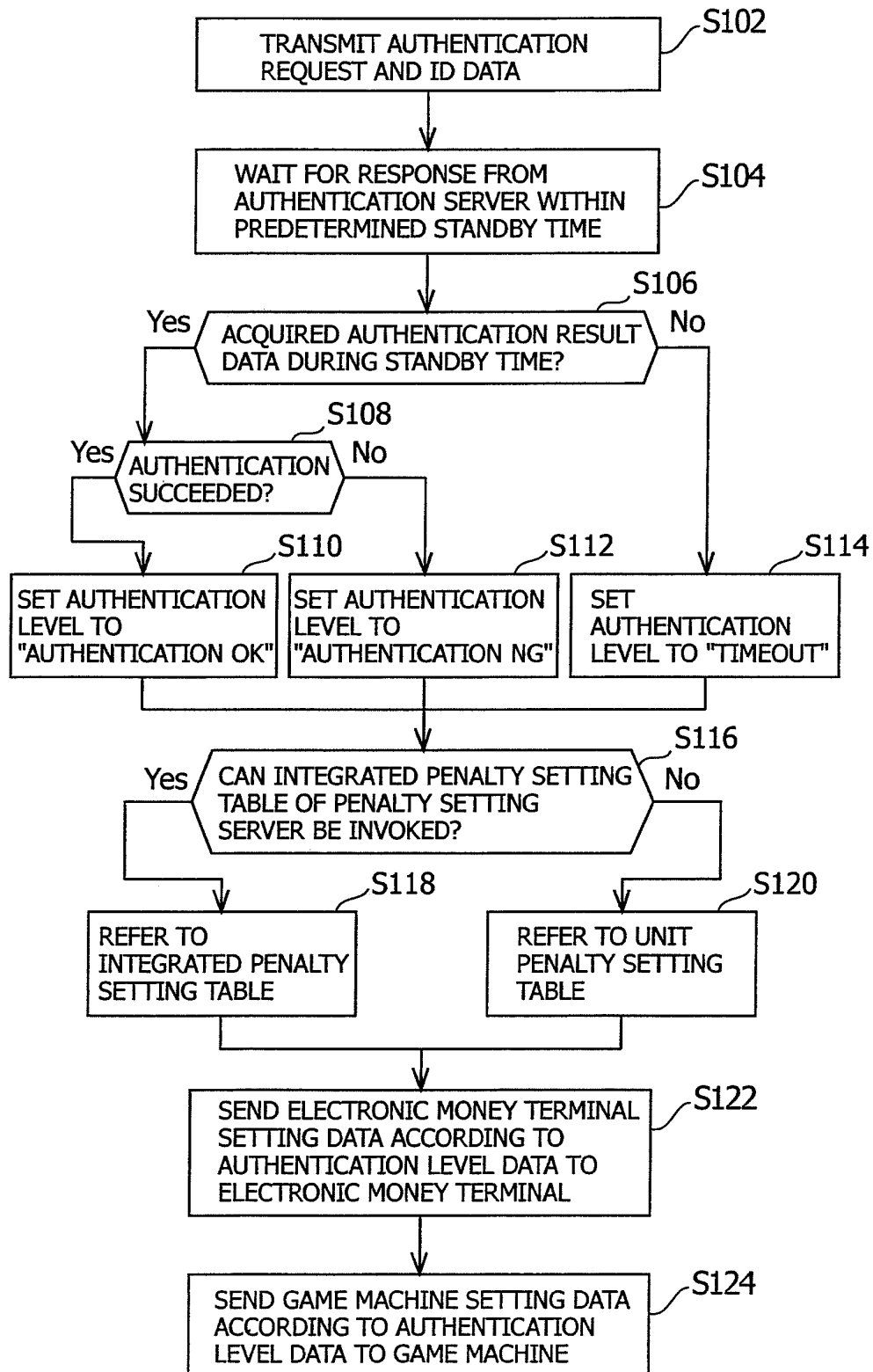
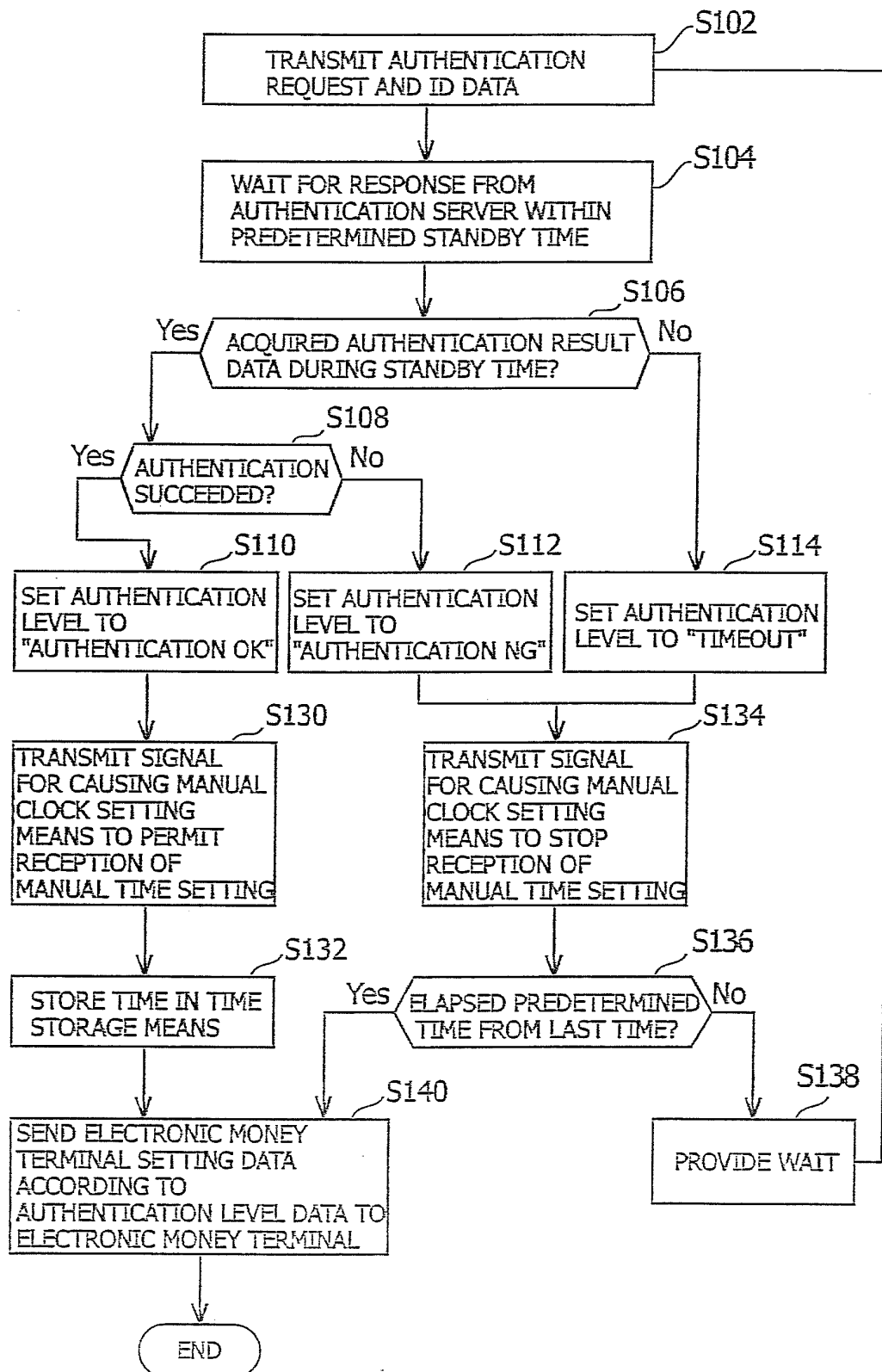


FIG.9



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/022777

A. CLASSIFICATION OF SUBJECT MATTER

A63F9/00(2006.01), **G06F13/00**(2006.01), **G06Q50/00**(2006.01)

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)

A63F9/00, **G06F13/00**, **G06Q50/00**

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

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006

Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

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

JSTPlus (JOIS) [(ROKARU NINSHO + OFURAIN NINSHO)*SHOGAIJI*NINSHO SABA]

(in Japanese)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-143250 A (Fujitsu Ltd.), 16 May, 2003 (16.05.03), Par. Nos. [0030] to [0035]; Fig. 1 & US 2003/0088679 A1	1-43
Y	JP 2004-255194 A (WMS Gaming Inc.), 16 September, 2004 (16.09.04), Par. No. [0056]; Fig. 2 & EP 1463008 A2 & US 2004/0229684 A1	1-43
A	JP 2004-318582 A (Nippon Telegraph and Telephone East Corp.), 11 November, 2004 (11.11.04), Par. Nos. [0026], [0034] (Family: none)	1-43

☐ Further documents are listed in the continuation of Box C.☐ 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 application or patent 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

"I" 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

07 March, 2006 (07.03.06)

Date of mailing of the international search report

14 March, 2006 (14.03.06)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- JP 8000829 A [0002] [0006]
- JP 2000251005 A [0004] [0006]