by setting a new validity period for the certificate whose validity period has expired. The certificate update unit 64 issues, for example, a certificate in which the validity period of the certificate issued to the communication control device 30 (31) is extended on the basis of an update request from the communication control device 30 (31) and transmits the issued certificate to the communication control device 30 (31). Information indicating the issued certificate is received by the communication control device 30 (31) and stored in the certificate information storage unit ~~405~~ 55 of the IC card 40 of the communication control device 30 (31), so that the validity period of the certificate of the communication control device 30 (31) is extended.

The certificate management unit 65 manages certificates that have already been issued. For example, the certificate management unit 65 performs a process of invalidating the certificate issued to the communication control device 30 (31) when validity in mutual authentication has not been mutually proved due to falsification, theft, or the like of the IC card 40 attached to the communication control device 30 (31). The certificate management unit 65 may be configured to respond regarding whether or not certificates issued to the communication control device 30 (31) and other communication devices have been issued by the certificate management unit 65 on the basis of an inquiry from the

prevent infection with malware or the like.

In the communication system 1 described above, the server device 20 is connected to the server-side communication control device 31 and no authentication process is performed inside the server device 20. Therefore, it is not necessary to hold a certificate or the like inside the server device 20 and it becomes clear that the server device 20 connected to the server-side communication control device 31 is under the management of the communication control management device 5. However, when the server device 20 already has a functional unit corresponding to the server-side communication control device 31, the server-side communication control device 31 is not necessarily required to be physically connected between the server device 20 and the network NW. In this case, an authentication process is performed in communication with the client-side communication control device 30 by a functional unit corresponding to the server-side communication control device 31 originally provided in the server device 20.

In the communication system 1, the control unit ~~401~~ 51 of the IC card 40 causes at least one of a mutual authentication process and an encryption/decryption process to be performed. Thus, the device cost of the communication control device 30 (31) can be reduced.

An example in which the IC card 40 attached to the communication control device 30 (31) performs at least one

transmission source of the information indicating the problem, to switch to the normal communication mode (step S106). The instruction to switch to the normal communication mode from the communication control management device 5 is acquired by the second communication device 111B of the communication control device 101, which is the source of the information indicating the problem (step S107). Accordingly, the controller 120 of the second communication device 111B switches the operation mode to the normal communication mode in response to the instruction to switch to the normal communication mode from the communication control management device 5 (step S108).

In addition, upon receipt of the information indicating the problem from the first communication device 111A, the control unit 61 of the communication control management device 5 instructs the first communication device 111A of the communication control device 101, which is the transmission source of the information indicating the problem, to be in the non-communication state (step S109). The instruction to switch to the non-communication state from the communication control management device 5 is acquired by the first communication device ~~111B~~111A, which is the source of the information indicating the problem (step S110). Accordingly, the controller 120 of the first communication device 111A switches the operation mode to the non-communication state in response to the instruction to switch to the non-communication state from the

device and the entire communication system so as to execute self-diagnosis with a minimum load. Therefore, the controller of the communication control device determines that the self-diagnosis is not to be executed (to be postponed) when the actual communication amount is larger.

If the self-diagnosis is to be executed (step S311, YES), the controller 320 executes the self-diagnosis (step S312), and transmits information indicating an execution result of the self-diagnosis to the communication control management device 5. In this case, the information indicating the execution result of the self-diagnosis is transmitted from the communication control device 301 and acquired by the communication control management device 5 (step S313).

If the self-diagnosis is not to be executed (step S311, NO), the controller 320 transmits a notification indicating that the self-diagnosis is not executed to the communication control management device 5 (step S314). In this case, a notification indicating that the self-diagnosis is not executed is acquired by the communication control management device 5 as a response to the request to execute the self-diagnosis (step S315).

Upon receipt of a result in reply to the request to execute the self-diagnosis, the control unit 61 of the communication control management device 5 stores the result of the self-diagnosis in the storage unit 66 (step S316). For example, if the self-diagnosis is executed in the

the communication amount in the communication control device. The controller~~ unit~~ 320~~1~~ may select a time (transmission time) when the communication control device 301 can transmit the log information from a time zone in which the communication amount is less than a predetermined threshold value based on the analysis information of the communication amount in the communication control device.

Upon selection of the candidate for the transmission time of the log information, the controller 32~~1~~0 transmits the selected candidate for the transmission time of the log information to the communication control management device 5 (step S424). Thus, the communication control management device 5 acquires the candidate for the transmission time of the log information selected by the communication control device 301.

The control unit 61 of the communication control management device 5 stores the information indicating the candidate for the transmission time of the log information received by the NW communication unit 60 in the storage unit 66, in association with the identification information indicating the communication control device 301 which is the transmission source (step S425). As a result, the information indicating the candidates for the transmission time of the log information from each communication control device 301 in the communication system is accumulated in the storage unit 66.

The control unit 61 of the communication control

CLAIMS

1. A communication system comprising:

a first communication control device connected between a first device and a network communication network; and

a second communication control device connected between a second device and the network communication network,

the first communication control device including:

a first communication system connected between the first device and the network communication network; and

a second communication system connected between the first device and the network communication network separately from the first communication system,

the first communication system and the second communication system each including:

a first authentication unit;

a first controller configured to request the first authentication unit to perform at least one of a mutual authentication process with the second communication control device using a secret key and a client certificate issued by a private authentication authority or an encryption and decryption process for ~~execute communication in a first communication mode for transmitting, to the second communication control device, information obtained by~~ encrypting information transmitted from the first device to the second device using a common key determined by the

first device and the second device, and ~~for transmitting, to the first device, information obtained by~~ decrypting information transmitted from the second device to the first device, and to execute communication in a first communication mode for transmitting and receiving plain text data with the first device, ~~using a common key determined by a mutual authentication process with the second communication control device using a secret key and a client certificate issued by a private authentication authority,~~

wherein the first controllers of the first communication system and the second communication system execute switching such that one of the communication systems executes communication in the first communication mode, and when a problem is detected in the communication system executing communication in the first communication mode, the other communication system executes communication in the first communication mode, and

the second communication control device including:

a second authentication unit;

a second controller configured to request the second authentication unit to perform at least one of a mutual authentication process with the first communication control device using a secret key and a server certificate issued by the private authentication authority or an encryption and decryption process for ~~transmit, to the first communication control device, information obtained by~~

encrypting information transmitted from the second device to the first device using a common key determined by the first device and the second device, and ~~to transmit, to the second device, information obtained by~~ decrypting information transmitted from the first device to the second device, and to transmit and receive plain text data with the second device~~using a common key determined by a mutual authentication process with the first communication control device using a secret key and a server certificate issued by the private authentication authority~~.

2. The communication system according to claim 1, wherein:

the first communication system and the second communication system are arranged in parallel between the first device and the network communication network; and

when a problem is detected in the communication system executing communication in the first communication mode, the first controllers of the first communication system and the second communication system set the communication system in which the problem is detected to a non-communication state and switch the other communication system to the first communication mode.

3. The communication system according to claim 1, wherein:

the first communication system and the second

communication system are arranged in series between the first device and the network communication network; and

when a problem is detected in the communication system executing communication in the first communication mode, the first controllers of the first communication system and the second communication system set the communication system in which the problem is detected to a second communication mode that allows data to pass through and switch the other communication system to the first communication mode.

4. The communication system according to any one of claims 1 to 3, wherein:

the first communication system and the second communication system each include a communication unit that communicates with a device management server, and

the first controllers of the first communication system and the second communication system transmit, to the device management server, information indicating a problem detected during execution of communication in the first communication mode, and switch the communication system to execute communication in the first communication mode in accordance with an instruction from the device management server.

5. A communication control device comprising:

a first communication system connected between a first

device and a network communication network; and

a second communication system connected between the first device and the network communication network separately from the first communication system,

the first communication system and the second communication system each including:

an authentication unit;

a controller configured to request the authentication unit to perform at least one of a mutual authentication process with ~~execute communication in a first communication mode for transmitting, to~~ a second communication control device connected between the network communication network and a second device using a secret key and a client certificate issued by a private authentication authority or an encryption and decryption process for~~, information obtained by~~ encrypting information transmitted from the first device to ~~a~~ the second device using a common key determined by the first device and the second device, and ~~for transmitting, to the first device, information obtained by~~ decrypting information transmitted from the second device to the first device, and to execute communication in a first communication mode for transmitting and receiving plain text data with the first device~~using a secret key issued by a private authentication authority and a common key determined by a mutual authentication process with the second communication control device connected between the network communication network and the second device using a~~

~~client certificate~~,

wherein the controllers of the first communication system and the second communication system execute switching such that one of the communication systems performs communication in the first communication mode, and when a problem is detected in the communication system executing communication in the first communication mode, the other communication system performs communication in the first communication mode.

6. The communication control device according to claim 5, wherein:

the first communication system and the second communication system are arranged in parallel between the first device and the network communication network; and

when a problem is detected in the communication system executing communication in the first communication mode, the controllers of the first communication system and the second communication system set the communication system in which the problem is detected to a non-communication state and switch the other communication system to the first communication mode.

7. The communication control device according to claim 5, wherein:

the first communication system and the second communication system are arranged in series between the

first device and the network communication network; and

when a problem is detected in the communication system executing communication in the first communication mode, the controllers of the first communication system and the second communication system set the communication system in which the problem is detected to a second communication mode that allows data to pass through, and switch the other communication system to the first communication mode.

8. The communication control device according to any one of claims 5 to 7, wherein:

the first communication system and the second communication system each include a communication unit that communicates with a device management server; and

the controllers of the first communication system and the second communication system transmit, to the device management server, information indicating a problem detected during execution of communication in the first communication mode, and switch the communication system to execute communication in the first communication mode in accordance with an instruction from the device management server.