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 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 communication control device 30 (31). The certificate management unit 65 may be configured to periodically check whether the issued certificate is being used in the valid communication control device 30 (31).

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 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 of a mutual authentication process and an encryption/decryption process in the communication system 1 has been described. However, in the communication system 1, the configuration for performing the mutual authentication

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 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 communication control management device 5 (step S111).

Here, the operation modes of the first and second communication devices are switched so as not to interrupt communication as the communication control device 101. For

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 communication control device 30, the control unit 61 stores information indicating the execution result of the self-diagnosis in the storage unit 66 in association with the identification information of the communication control device 301 together with the execution date and time. If

to the fourth embodiment.

First, as in the first operation example described above, the controller 320 in the communication control device 301 analyzes information indicating the communication amount accumulated as log information in the data memory 324, and stores the analysis information of the communication amount as an analysis result in the data memory 324 (step S421).

The controller 320 of the communication control device 301 selects a candidate for the transmission time at which the communication control device 301 transmits the log information based on the analysis information of the communication amount stored in the data memory 324 (step S422). The number of candidates for the transmission time may be one, two or more, or instead indicated as a time zone.

For example, the controller 320 selects, as a candidate for the transmission time, a time when the communication control device 301 can transmit the log information in a time zone in which the communication amount is smallest, based on the analysis information of the communication amount in the communication control device. The controller 320 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 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 320 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 management device 5 creates a schedule (log collection schedule) of the time at which each communication control device 31 of the entire system transmits the log information, based on the candidates for the transmission time of the log information of each communication control device 301 stored in the storage unit 66 (step S426). For

CLAIMS

1. A communication system comprising:

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

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

a device management server configured to collect log information indicating contents of processing executed by the first communication control device,

the first communication control device including:

a communication interface configured to communicate with a device connected via the first device and the network communication network;

a first controller configured to transmit, to the second communication control device, information obtained by encrypting information transmitted from the first device to the second device, and to transmit, to the first device, information obtained by decrypting information transmitted from the second device to 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; and

a memory configured to store analysis information of a communication amount of data communication carried out via

the communication interface,

wherein the first controller transmits log information to the device management server at an execution time set based on the analysis information of the communication amount stored in the memory, wherein the first controller transmits log information to the device management server at a transmission time of log information set based on the analysis information of the communication amount stored in the memory, and wherein the first controller checks a congestion degree in a network between the first controller and the device management server at a transmission time of log information set based on the analysis information of the communication amount stored in the memory, and transmits the log information to the device management server if the congestion degree is within a permissible range, and

the second communication control device including:

a second controller configured to transmit, to the first communication control device, information obtained by encrypting information transmitted from the second device to the first device, and to transmit, to the second device, information obtained by decrypting information transmitted from the first device to the second device, using a common key determined by a mutual authentication process 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 controller transmits, to the device management server, the analysis information of the communication amount stored in the memory, and transmits log information to the device management server at a transmission time of log information instructed from the device management server.

3. The communication system according to claim 1, wherein the first controller transmits, to the device management server, a candidate for a transmission time of log information selected based on the analysis information of the communication amount stored in the memory, and transmits log information to the device management server at a transmission time of log information instructed from the device management server.

4. A communication control device which is a first communication control device connected between a first device and a network communication network, the communication control device comprising:

a communication interface configured to communicate with a device connected via the first device and the network communication network;

a controller configured to transmit, to a second communication control device connected between a second device and a network communication network, information

obtained by encrypting information transmitted from the first device to the second device, and to transmit, to the first device, information obtained by decrypting information transmitted from the second device to 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; and

a memory configured to store analysis information of a communication amount of data communication carried out via the communication interface,

wherein the controller transmits log information to a device management server at an execution time set based on the analysis information of the communication amount stored in the memory, wherein the controller transmits log information to the device management server at a transmission time of log information set based on the analysis information of the communication amount stored in the memory, and wherein the controller checks a congestion degree in a network between the first controller and the device management server at a transmission time of log information set based on the analysis information of the communication amount stored in the memory, and transmits the log information to the device management server if the congestion degree is within a permissible range.

5. The communication control device according to

claim 4, wherein the controller transmits, to the device management server, the analysis information of the communication amount stored in the memory, and transmits log information to the device management server at a transmission time of log information instructed from the device management server.

6. The communication control device according to claim 4, wherein the controller transmits, to the device management server, a candidate for a transmission time of log information selected based on the analysis information of the communication amount stored in the memory, and transmits log information to the device management server at the transmission time of log information instructed from the device management server.