[DESCRIPTION]

[TITLE OF INVENTION]

COMMUNICATION CONTROL SYSTEM

[Technical Field]

[0001]

Embodiments of the present invention relate to a communication control system and a communication control device.

[Background Art]

[0002]

In social infrastructure systems such as monitoring cameras, the control of equipment and data to be handled may need to be protected from an attack of malware or the like. However, it is difficult to frequently replace equipment constituting a social infrastructure system. Thus, there is a problem in that security measures may become insufficient.

[Citation List]

[Patent Literature]

[0003]

[Patent Literature 1]

Japanese Unexamined Patent Application, First Publication No. 2009-117887

[Summary of Invention]

[Technical Problem]

[0004]

The problem to be solved by the present invention is to provide a communication control system and a communication control device capable of

[CLAIMS]

[Claim 1]

A communication control system comprising:

a first communication control device connected to a client device and a network communication grid; and

a second communication control device connected to a server device and the network communication grid,

wherein the first communication control device comprises:

a first authentication unit; and

a first control unit that is configured to request the first authentication unit to perform at least one of a mutual authentication process and an encryption/decryption process, the mutual authentication process performing mutual authentication in communication with the second communication control device using a secret key and a client certificate issued by a private authentication authority, the encryption/decryption process encrypting information, that is transmitted to the server device by the client device, using a common key determined for communication between the first communication control device and the second communication control device, and the encryption/decryption process decrypting information, that is transmitted to the client device by the server device, using the common key, and

wherein the second communication control device comprises:

a second authentication unit; and

a second control unit that is configured to request the second authentication unit to perform at least one of a mutual authentication process and an encryption/decryption process, the mutual authentication process performing mutual authentication in communication with the first communication control device, using a secret key and a server certificate issued by the private authentication authority, the encryption/decryption process encrypting information, that is transmitted to the client device by the server device, using the common key, and the encryption/decryption process decrypting information, that is transmitted to the server device by the client device, using the common key.

[Claim 2]

The communication control system according to claim 1, wherein the first authentication unit is attached to the first communication control device so that the first authentication unit is able to be attached to or detached from the first communication control device.

[Claim 3]

The communication control system according to claim 1 or 2, further comprising the private authentication authority,

wherein the private authentication authority transmits the secret key and the client certificate to be stored in the first authentication unit to the first communication control device and transmits the secret key and the server certificate to be stored in the second authentication unit to the second communication control device.

[Claim 4]

The communication control system according to any one of claims 1 to 3, wherein the first control unit requests the first authentication unit to perform the mutual authentication in communication with a communication device transmitting information to the client device, determines whether or not to permit communication with the client device for the communication device on the basis of a result of the mutual authentication, and transmits a determination result to the private authentication authority.

[Claim 5]

The communication control system according to any one of claims 1 to 4, wherein the first control unit requests the first authentication unit to perform a firmware verification process of performing verification of whether or not details of information about firmware of the client device transmitted to the client device are correct using a key issued by the private authentication authority.

[Claim 6]

The communication control system according to any one of claims 1 to 5, wherein the first authentication unit determines whether or not to permit communication with the client device for a communication device transmitting information to the client device on the basis of a transmission destination list indicating information about communication equipment for which communication with the client device is permitted.

[Claim 7]

The communication control system according to claim 3,

wherein the private authentication authority further comprises a certificate update unit configured to update the client certificate on the basis of a validity period of the client certificate, and

wherein the private authentication authority transmits the client certificate updated by the certificate update unit to the first communication control device.

[Claim 8]

The communication control system according to claim 3 or 7, wherein the private authentication authority further comprises a management unit configured to invalidate the client certificate when validity has not been mutually proved in the mutual authentication process of the first communication control device.

[Claim 9]

The communication control system according to any one of claims 1 to 8, wherein the first communication control device determines whether or not a connection with the client device is being maintained at a predetermined timing.