TITLE

SYSTEM, COMMUNICATION SYSTEM FOR GENERATING ADDRESSES AUTOMATICALLY, AND ADDRESS CONVERSION SYSTEM

BACKGROUND OF THE APPLICATION

Field of the Application

[0001] The present invention relates to a communication apparatus, a method for controlling communication between different types of devices, and a method for eliminating specificity of operational management.

Description of the Related Art

[0002] Until the middle 1980s, a computer was constituted by a combination of a universal machine and an input terminal. Using the central universal machine to process all processing is referred to as an application in a closed space.

[0003] However, LAN and WAN were introduced to connect a company's internal network environment. Using the Internet to connect the company's internal/external network environments has had an impact on computer systems since around 1995. Currently, a service called the cloud is employed. With continuing advances being made in this type of service, connections with the company's external resources or the network connections of business and globalization in numerous foreign currency denominations have further become general connections. Nowadays, it is becoming important to use a secure network to transmit data when working with numerous foreign currency denominations.

[0004] Although the cloud services use the Internet and matching, the Internet is

management information to the device 107 via a management information transmission 404. The device 107 receiving the management information executes a determination command of a communication status to the OS of the device 107 to obtain the latest information about how the communication status of device 107 is constituted, and compares the received management information with the communication status of the device 107 itself to recognize an increase or decrease in other devices 107. When a device 107 is removed from the management information, the device 107 cannot communicate with the device 107 which is the target. The operation center 101 is notified of an exclusion report of the subject device in an exclusion processing completion report 410.

When a device is added, a device adding processing is performed. (Refer to FIG. 6).

The console performs a forced exclusion processing of the device 107 by a forced cut 412. Other devices 107 in the group of the device 107 which has been forcibly excluded are notified that the device 107 has been forcibly excluded. The device 107 receiving the notification cannot immediately perform any communication with the device 107 which has been forcibly excluded and notifies the operations center 101 of the exclusion report of the subject device in the exclusion processing completion report 410.

[0021] FIG. 5 illustrates that the operations center 101 reports an urgent error to the administrator when an emergency state is confirmed in the most recent log.

[0022] In a log processing of the operations center 101, the operations center 101 regularly confirms the logs stored in a database of the operations center 101. When a new log is added after the last confirmation, the operations center 101 reads the new log. When it is determined that the content of the new log is urgent by urgency determination processing 503, the urgent content is edited by notification content editing processing 504. Notification destination ensuring processing 505 is used to ensure notification of the

encryption connection completion report 611 and an encryption connection completion report 612. The operations center 101 receives the encryption connection completion report by receipt of the encryption connection completion report 613, and records a device adding completion record into the management information of the operations center 101 by a device adding processing completion record 614.

[0025] The purpose of FIG. 7 is to illustrate that the operations center 101 is instructed by the console 103 to publish a certificate of terminal software 108 and to encrypt the published certificate when the terminal software 108 is newly installed. The encrypted certificate and the connection completion used as the new terminal software 108 are transmitted to administrators who add a PC, etc.

[0026] A client certificate issue instruction 701 and a client certificate issue processing 702 indicate that when the new terminal software is installed in a PC and a multifunction portable terminal including tablets, smartphones, etc., the console 103 instructs the operations center 101 or the certificate authority 102 to perform client certificate issue processing 702 to create a version of the certificate. The certificate authority 102 assigns unique serial numbers to number the certificates and creates signatures for public key certificates, etc., as the certificates of the terminal software 108. Set information connection 703 is used to connect and use the certificates issued by the client certificate issue processing 702, the information of the operations center and the extended setting information as terminal software connection information. The terminal software connection information is encrypted by encryption 704. The terminal software connection information is transmitted to the administrator of the terminal software 108 by transmission 705 using an email of the terminal software connection information, etc., or the encrypted terminal software connection information is written into the external memory medium and is transmitted by mail or another means. The administrator

of the terminal software 108 receives the terminal software connection information in the mail or by other means by reception 706 of the terminal software connection information, such as mailing, etc. The administrator of the terminal software 108 installs the terminal software in a PC or a multifunction portable terminal including tablets, smartphones, etc., by terminal software installation processing 707. Next, the administrator of the terminal software 108 inputs the encrypted terminal software connection information to a PC, or a multifunction portable terminal including tablets, smartphones, etc. for decryption to set the terminal software 108 by connection information decryption 708. ID creation 710 is used to create a unique ID of a PC, or a multifunction portable terminal including tablets, smartphones, etc., set by the terminal software. The terminal software connection information is used to connect to the operations center 101 by terminal software control center authentication 711. The authentication is requested, and the authentication confirmation is performed by authentication OK 712. When the authentication is confirmed, the terminal software is used as registration information by terminal software registration 713. Individual information, etc., of a PC, or a multifunction portable terminal including tablets, smartphones, etc., is registered into a database of the operations center 101, and terminal software 108 is notified that registration is completed. When the authentication fails by the authentication OK 712, the authentication which has failed is output to the error log, and the communication conforming to the terminal software is cut.

[0027] FIG. 8 illustrates cases where the terminal software 108 cuts the connection with the real network via the device 107, the device 107 performs operations according to a new situation notified by the operations center 101 when the console 103 adds or deletes a device 107, the device 107 is changed because of inappropriate factors, or the device 107 periodically issues a request to the operations center 101 and the operations

center 101 replies to the requests.

[0028] An authentication request 801 of FIG. 8 is used to request authentication connection from the terminal software 108 to the operations center 101. When authentication can be performed, the operations center 101 checks whether there is a device 107 connected to the terminal software 108 by a connection destination device confirmation 803. When no device 107 is connected to the terminal software 108, a destination without connection is transmitted to the terminal software 108 to cut the connection. When multiple devices 107 are connected to the terminal software 108, an optimal device 107 having a minimum number of connections at present is determined by an optimal device search 804. The connection information of the terminal software 108, such as global IP addresses and so on, is transmitted to the device 107 by a connection permission instruction 806. The firewall settings can be changed to accept communication with the terminal software 108 by connection preparation processing 807. In the stage at which the setting is completed, the device 107 reports to the operations center 101 and terminal software 108 that the connection preparation is completed by sending a connection preparation completion report 808. The operations center 101 indicates the connection methods, such as a general address for the device 107, to the terminal software 108 by notification of a connection destination device 809. The terminal software 108 determines a communication protocol in accordance with the received connection method, and transmits the ID, password, certificate, etc., to the device 107 by the transmission of connection authorization information 810. The device 107 confirms the received ID, password, certificate, etc., and transmits the confirmation to the terminal software 108 when the received ID, password, certificate, etc., can be confirmed. The terminal software 108 performs encryption communication with the device 107 by encryption data communication 812 and encryption data

What is claimed is

1. A system for generating addresses automatically, which is a system for assigning a unique address automatically to an existing network where the IP addresses have already been set to each PC, server, etc.,

automatically investigating and analyzing the IP addresses and port numbers or identifiers which are in use according to the IP addresses assigned to the existing network;

filtering out IP addresses and port numbers or identifiers which are not in use;

using one of the IP addresses which are in use and one of the port numbers or identifiers which are not in use to generate a new real IP address; and

assigning the new real IP address to the PC, server, etc.

2. A communication system, which is a system for assigning a unique address automatically to an existing network where the IP addresses have already been set to each PC, server, etc.,

automatically investigating and analyzing the IP addresses and port numbers or identifiers which are in use according to the IP addresses assigned to the existing network;

filtering out IP addresses and port numbers or identifiers which are not in use;

using one of the IP addresses which are in use and one of the port numbers or identifiers which are not in use to generate a new real IP address;

virtually assigning the real IP address to the device itself and the PC or the server connected to the device;

hiding the device and IP address in the network; and

using the real IP address for communication so that the IP address cannot be accessed by external systems.

3. An address conversion system, which is a system for assigning a unique address automatically to an existing network where the IP addresses have already

been set to each PC, server, etc.,

automatically investigating and analyzing the IP addresses and port numbers or identifiers which are in use according to the IP addresses assigned to the existing network;

filtering out IP addresses and port numbers or identifiers which are not in use;

using one of the IP addresses which are in use and one of the port numbers or identifiers which are not in use to generate a new real IP address;

virtually assigning the real IP address to the device itself and the PC or the server connected to the device; and

using IP conversion addresses of three real IP addresses to communicate with the PC or the server which is the destination when communicating with a PC or a server connected to an opposing device,