7.5 netNACCS Processing Mode, WebNACCS Processing Mode, and ebMS Processing Mode

The following methods are used.

7.5.1 Security Measures by NACCS Center

As security measures by NACCS Center, firewall and unauthorized access detection devices, etc. shall be installed and the best measures that can be assumed at present shall be taken in setting and operating them.

7.5.2 Security Measures for Communications, etc.

In netNACCS Processing Mode, WebNACCS Processing Mode, and ebMS Processing Mode, a de facto standard TLS shall be adopted in HTTP encryption as a measure against tapping, alteration, and spoofing, etc. of messages transmitted/received.
On terminals using netNACCS or WebNACCS, client digital certificates provided by NACCS Center shall be deployed.

[For reference] TLS

TLS stands for Transport Layer Security. It is an encrypted communications protocol standardized based on SSL and is used to ensure safe communication on the Internet.

[For reference] SSL

SSL stands for Secure Socket Layer. It is an encrypted communications protocol developed by Netscape Communications Corporation of the United States and is used to ensure safe communication on the Internet. Since the data exchanged between Web servers and Web browsers can be encrypted, it is suited for the communication of data such as private information of which the leakage can cause problems and is widely recognized as a de facto standard for Web browsers. SSL consists of multiple encryption related components.

The following figure shows the outline of communication encryption, etc. adopted for netNACCS processing mode and WebNACCS processing mode.

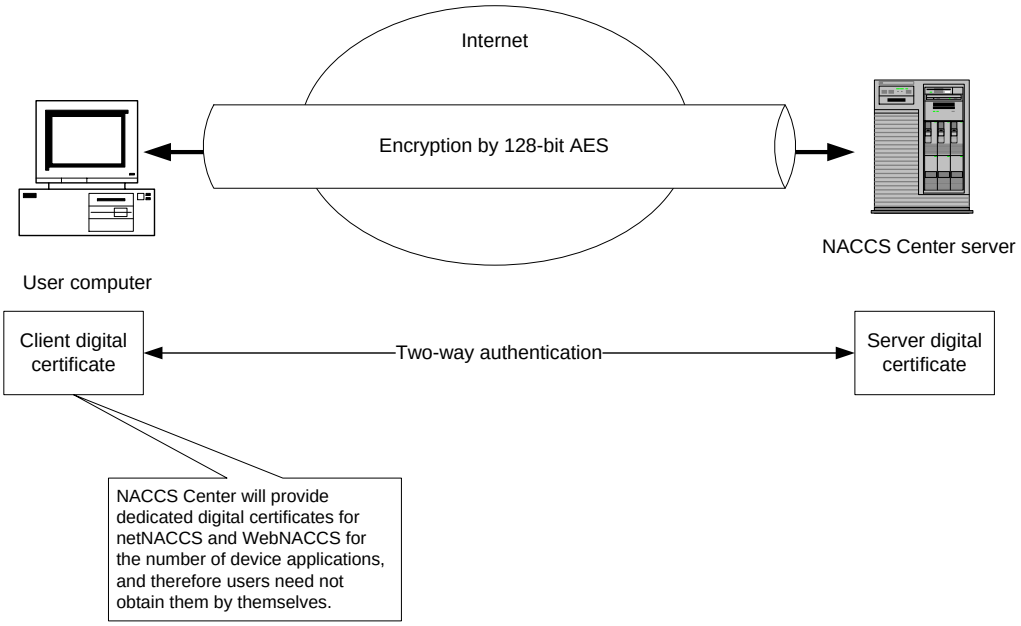

Figure 7.5.1 Outline of Communication Encryption, etc. Adopted for netNACCS Processing Mode and WebNACCS Processing Mode

Encryption methods shall be reviewed as required in consideration of the security situation in the future.

Furthermore, in netNACCS processing mode, WebNACCS processing mode, and ebMS processing mode, whether the users are eligible to process procedures or not shall be checked using the user codes, identifying numbers, and user passwords issued/managed by NACCS Center.

In the retrieval of reports, like interactive processing mode (packaged software), access eligibility shall be checked using the user codes, identifying numbers, and passwords.

7.5.3 netNACCS Processing Mode Connection Example

(1) When connecting directly to the Internet with a dial-up router or modem

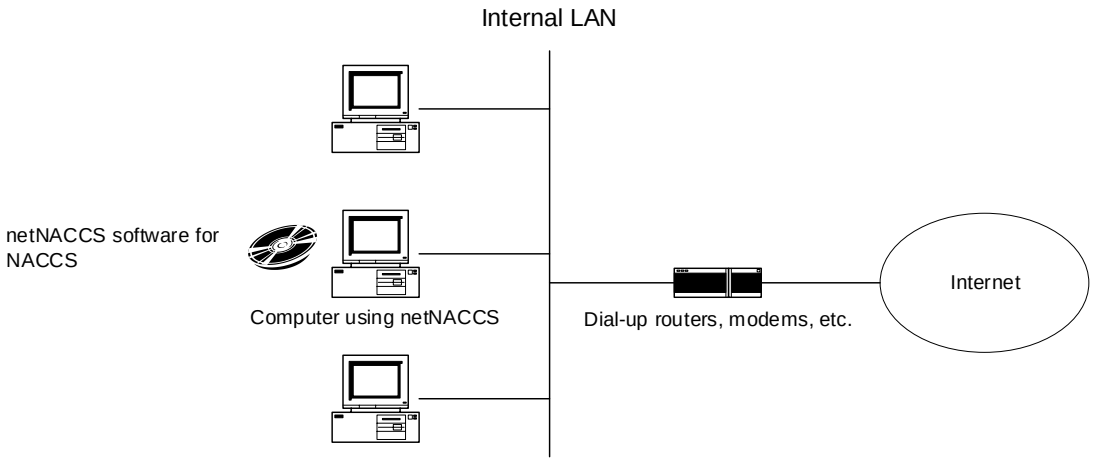

Figure 7.5.2 Example of connecting directly to the Internet with a dial-up router or modem

(2) When connecting to the Internet via an internal firewall

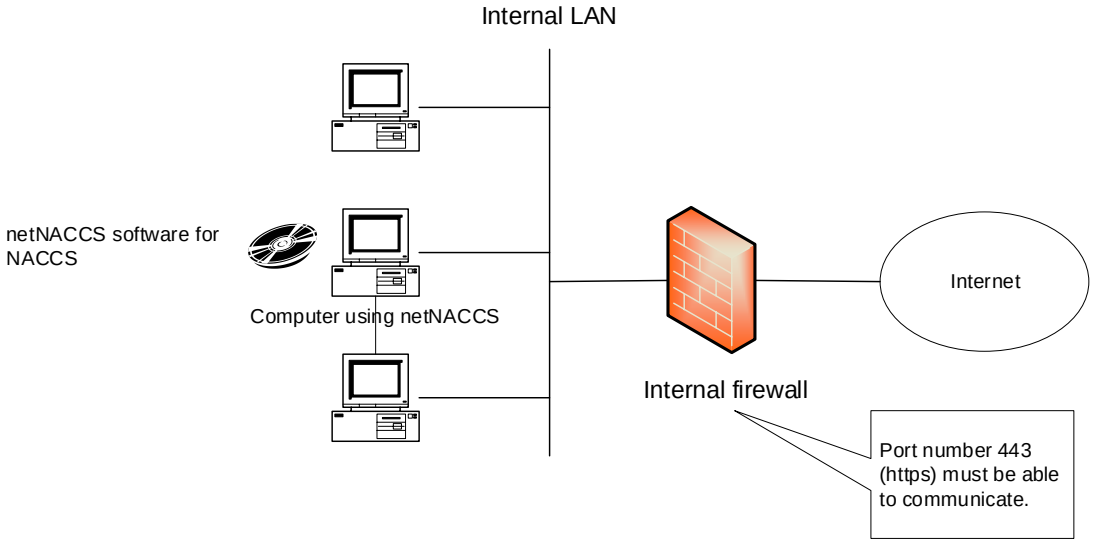

Figure 7.5.3 Example of connecting to the Internet via an internal firewall

(3) When netNACCS software and NACCS packaged software are used together

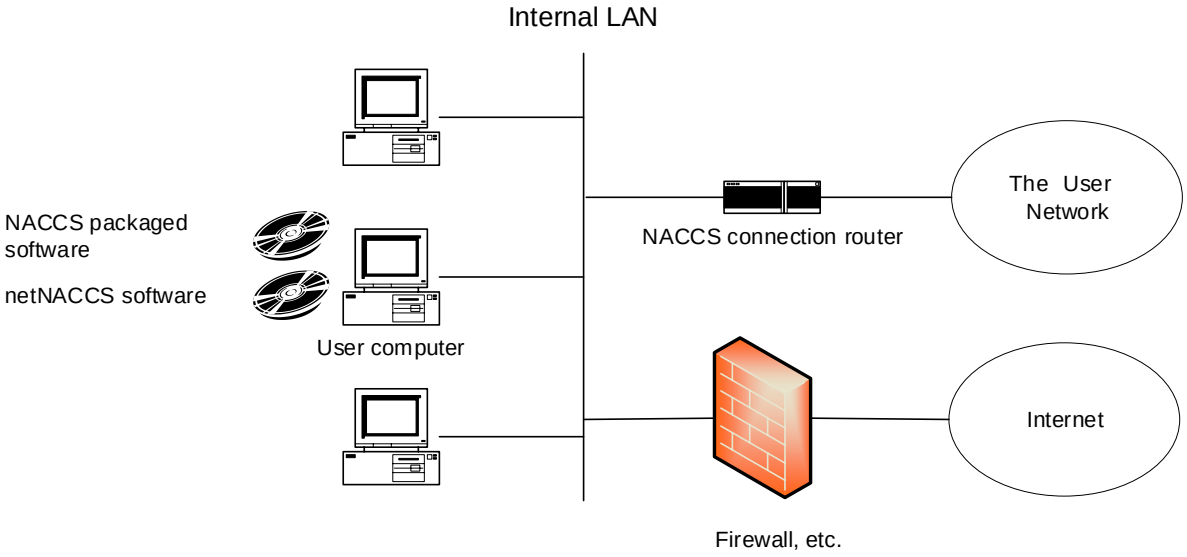

Figure 7.5.4 Example of when netNACCS software and NACCS package software are used together

(Note 1) It is possible to install netNACCS software and NACCS packaged software (a packaged software for connecting to NACCS using the user Network) on one computer, but it is not possible to start and use both softwares at the same time.

(Note 2) When using netNACCS with the NACCS package software together, refer to “7.4.2 Security standards for connections to external networks”.

7.5.4 WebNACCS Processing Mode Connection Example

(1) When connecting directly to the Internet with dial-up router or modem

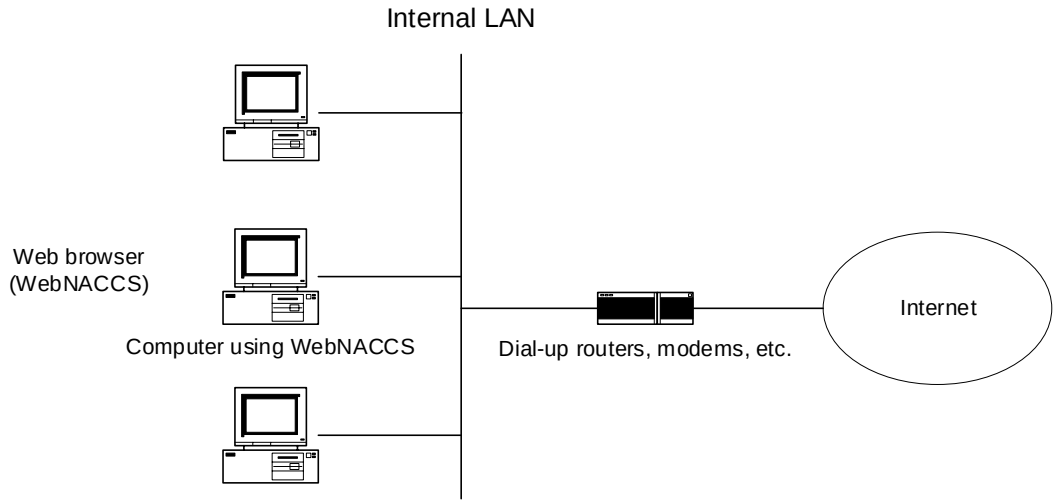

Figure 7.5.5 Example of connecting directly to the Internet with a dial-up router or modem

(2) When connecting to the Internet via an internal firewall

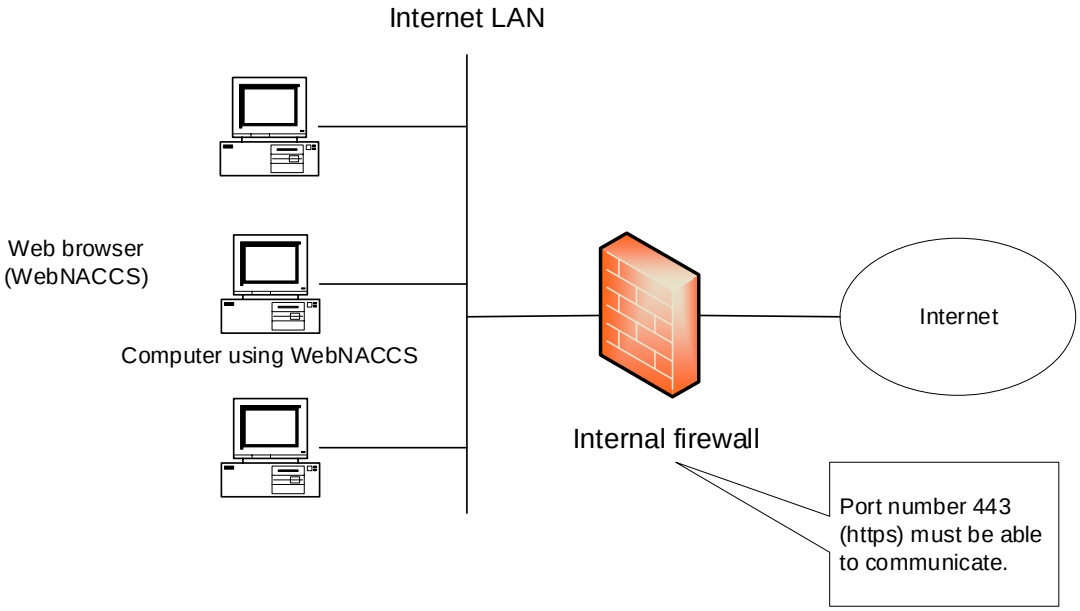

Figure 7.5.6 Example of connecting to the Internet via an internal firewall

(3) When WebNACCS processing mode and netNACCS software are used together

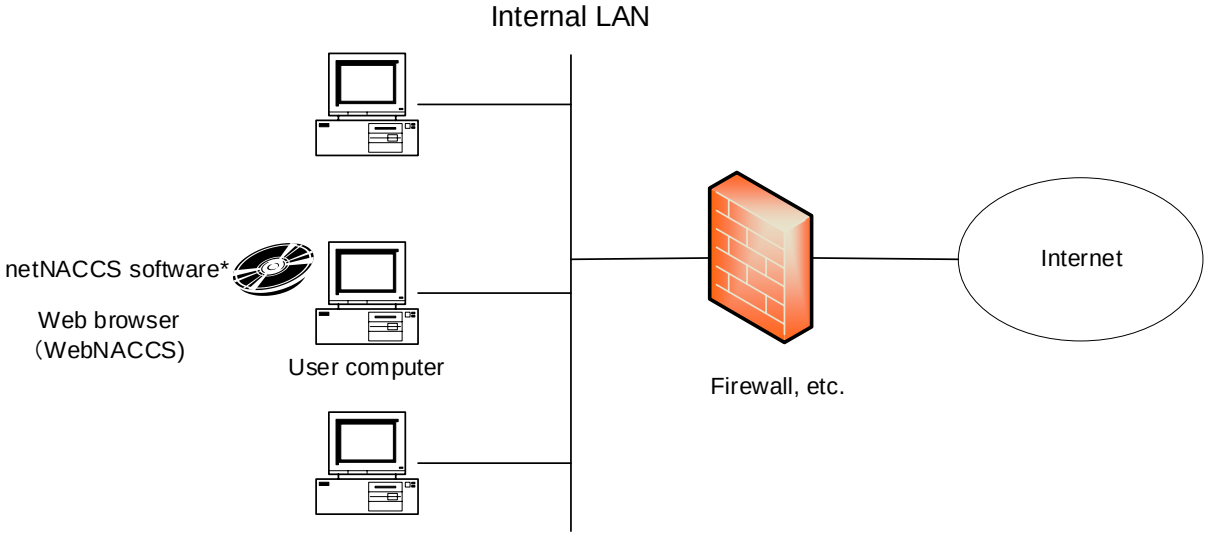

Figure 7.5.7 Example of when WebNACCS processing mode and netNACCS software are used together

(Note 1) When using netNACCS with the NACCS package software together, refer to “7.4.2 Security standards for connections to external networks”.

7.5.5 Notes for Using netNACCS Processing Mode, WebNACCS Processing Mode, and ebMS Processing Mode

(1) Responses in netNACCS Processing Mode and WebNACCS Processing Mode

Response in netNACCS processing mode and WebNACCS processing mode depends on the speed of the Internet lines used. In netNACCS processing mode and WebNACCS processing mode, the response is considered to be lower when compared to the case of using NACCS packaged software (to connect to NACCS via the user network) as there are many required processes, including the time required for encryption and authentication and the time required for converting messages transmitted/received in netNACCS processing mode and WebNACCS processing mode into NACCS messages to be processed by the NACCS Center server, etc.

(2) netNACCS Processing Mode and WebNACCS Processing Mode During Internet Congestion

At present, the user network provided by NACCS Center guarantees connection to the NACCS Center server even when a congestion occurs in the network. Since the Internet lines provided by users are used in netNACCS processing mode and WebNACCS processing mode, however, a reliable connection to the NACCS Center server cannot be guaranteed.

(3) Loss of Messages

As netNACCS processing mode and WebNACCS processing mode use the Internet connection, if communication failures occur when users are receiving processing result messages (screen messages) transmitted in response to processing requests from users, messages may be lost.

(4) Digital Signature for ebMS Processing Mode

Digital signature functions perform issuance and validation of electronic signatures by XML signatures using digital certificates based on X.509. XML signatures shall include ebXML Messaging envelopes and payloads. As for certificates for electronic signatures, those provided by NACCS Center shall be used.

(5) Server Certificates Used in ebMS Processing Mode

In ebMS processing mode, server certificates provided by NACCS Center shall be deployed in the user server.

(6) Other Important Notes

Since the Internet connection is used in netNACCS processing mode and WebNACCS processing mode, completely preventing unauthorized access and DoS attacks, etc. against netNACCS processing mode and WebNACCS processing mode is difficult. NACCS Center takes the best security measures in netNACCS processing mode and WebNACCS processing mode at all times. However, when concentrated DoS attacks are made or serious new security holes are discovered, etc., netNACCS processing mode and WebNACCS processing mode may have to be stopped while measures are taken.

(Note) DoS attack

DoS attack stands for "Denial of Service" attack. For example, when a number of telephone calls are simultaneously made to the same telephone number through telephone lines, the lines may be flooded. Similarly, on the Internet, when millions of computers simultaneously access a certain Web server, the Web server suffers serious damage and goes down. DoS (Denial of Service) attack is a method used to cause certain servers to go down by intentionally creating such situations.

7.5.6 Security Measures by Users

The content of security measures that users shall abide by in using netNACCS processing mode and WebNACCS processing mode is as follows.

Table 7-5-1 Content of Security Measures That Users Must Abide By

Content	Details	Remarks
[1] Placement of system administrator	Administrator shall be placed at each office where netNACCS processing mode and WebNACCS processing mode is used in the user system and reported to NACCS Center (Unless a service contract is already concluded with NACCS Center and administrators are reported)	
[2] Management of IDs and passwords	The system administrator as given in [1] above shall manage IDs and passwords used in netNACCS processing mode and WebNACCS processing mode	Even when IDs and passwords are used outside the office where NACCS is supposed to be used in accordance with an applied system use contract, such as when using IDs and passwords at home or a satellite office due to a natural disaster or other uncontrollable circumstances, the system administrator at the office will still manage the IDs and passwords in an appropriate manner
[3] Anti-virus measures	All computers (refer to computers) using netNACCS processing mode and WebNACCS processing mode shall have commercially available anti-virus software installed therein, and such anti-virus software shall be kept up to date	Commercially available anti-virus software includes anti-virus software built into an OS (such as Microsoft Defender)
[4] Security measures of the company	Appropriate security measures (including measures against vulnerability, such as user authentication, access control, encryption and security patch) shall be taken for users' own system	The NACCS Center may request the submission of users' own security measures if it deems it necessary