7.3 Security Measures

7.3.1 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.

7.3.2 Security Measures for Communications, etc.

In Interactive Processing Mode (netNACCS), WebNACCS Processing Mode, and Interactive Processing Mode (netAPI), a de facto standard TLS shall be adopted in HTTP encryption as a measure against tapping, alteration, and spoofing, etc. of Transmission/Receipt Messages. On terminals using Interactive Processing Mode (netNACCS), WebNACCS Processing Mode, and Interactive Processing Mode (netAPI), 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 the communication encryption, etc. adopted for Interactive Processing Mode (netNACCS), WebNACCS Processing Mode, and Interactive Processing Mode (netAPI).

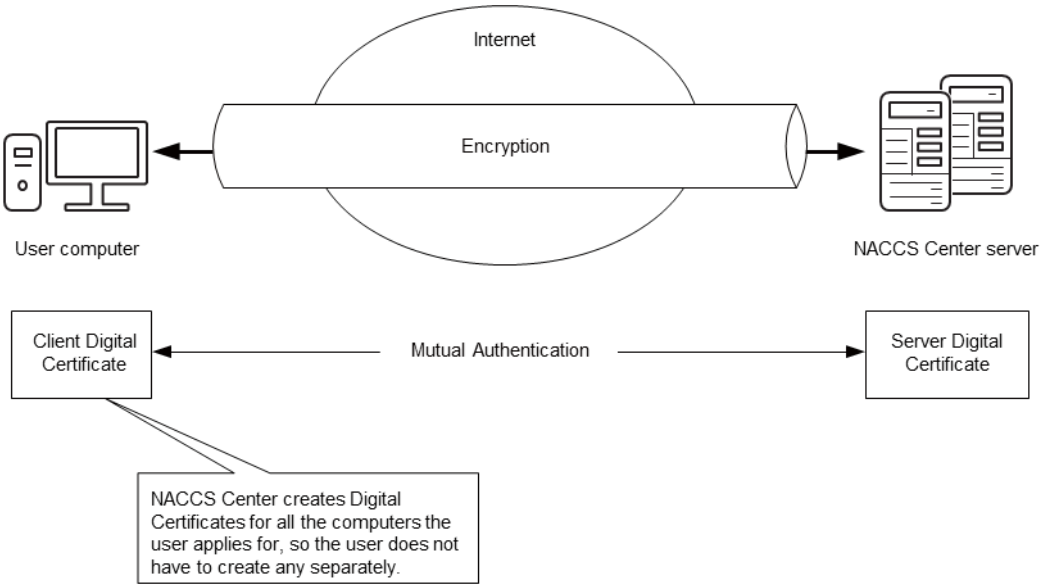

Figure 7.3.1 Outline of the Communication Encryption, etc. Used

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

Furthermore, in Interactive Processing Mode (netNACCS), WebNACCS Processing Mode, and Interactive Processing Mode (netAPI), 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 NACCS Packaged Software (Interactive Processing Mode), access eligibility shall be checked using the User Codes, Identifying Numbers, and passwords.

7.3.3 Security Measures Implemented by Users

When accessing NACCS Center server, users shall comply with the security measures specified by NACCS Center and report to NACCS Center on details of security measures they have actually implemented. The content of security measures that users must comply with are shown below.

Table 7.3.1 Content of Security Measures That Users Must Comply with

Content	Connection Mode			Details	Remarks
	Router connection	Gateway connection (including netAPI)	netNACCS WebNACCS		
(1) Management of IDs and passwords	O	O	O	• The system administrator shall manage IDs and passwords used for NACCS.	The relevant office's system administrator shall also manage the IDs and passwords appropriately if they are to be used somewhere other than an office where using NACCS is covered by the system use agreement (e.g., for working from home or a satellite office due to a disaster or similar unavoidable reason).
(2) Anti-virus measures	O	O	O	• All computers connecting to NACCS Center server shall have commercially available anti-virus software installed therein, and such anti-virus software shall be kept up to date. If any of the computers get infected by a virus, the matter shall be reported to NACCS Center promptly.	Commercially available anti-virus software shall also include anti-virus software built into the OS (e.g., Microsoft Defender).
(3) Reporting of user system configuration	O	O		• The following documents pertinent to user system that connects to NACCS Center server shall be submitted to NACCS Center:	

				[1] System configuration diagram [2] Configuration list of devices used	
(4) Submission of security measures of the company	O	O	O	• Appropriate security measures (including agent authentication, access control, encryption, and vulnerability measures such as applying security patches) shall be taken for the users' own NACCS-related system (servers, network devices, client terminals, etc.).	Submission of security measures of the company is required when deemed necessary by NACCS Center.
(5) Log management		O		In order to identify who has connected to the NACCS Center server from gateway computers, etc., users shall construct a system to manage the history (log) of data transmission/ reception, and ensure it can be submitted to NACCS Center as required.	Submission of the log is required when deemed necessary by NACCS Center. See (*) for how to implement log management.

(*) Log management (for gateway connections)

Log management for gateway connections shall be implemented as follows:

(1) Items to be logged and retained

Of the messages transmitted and received by NACCS Center server, the following items shall be logged and retained:

Table 7.3.2 Items to Be Logged and Retained by Users Using Gateway Connections

Transmission/reception / Item	Upon transmission	Upon reception
User Code	○	○
Identifying Numbers	○	-
Procedure Code	○	○
Date and time	○	○

○: Required –: Not required

(2) Period of log retention

Logs shall be retained for a period of one year.

(3) Location and method of log retention

Although users can decide on the location and method of log retention by themselves, they must be able to promptly disclose retained logs to NACCS Center whenever they are requested to do so.

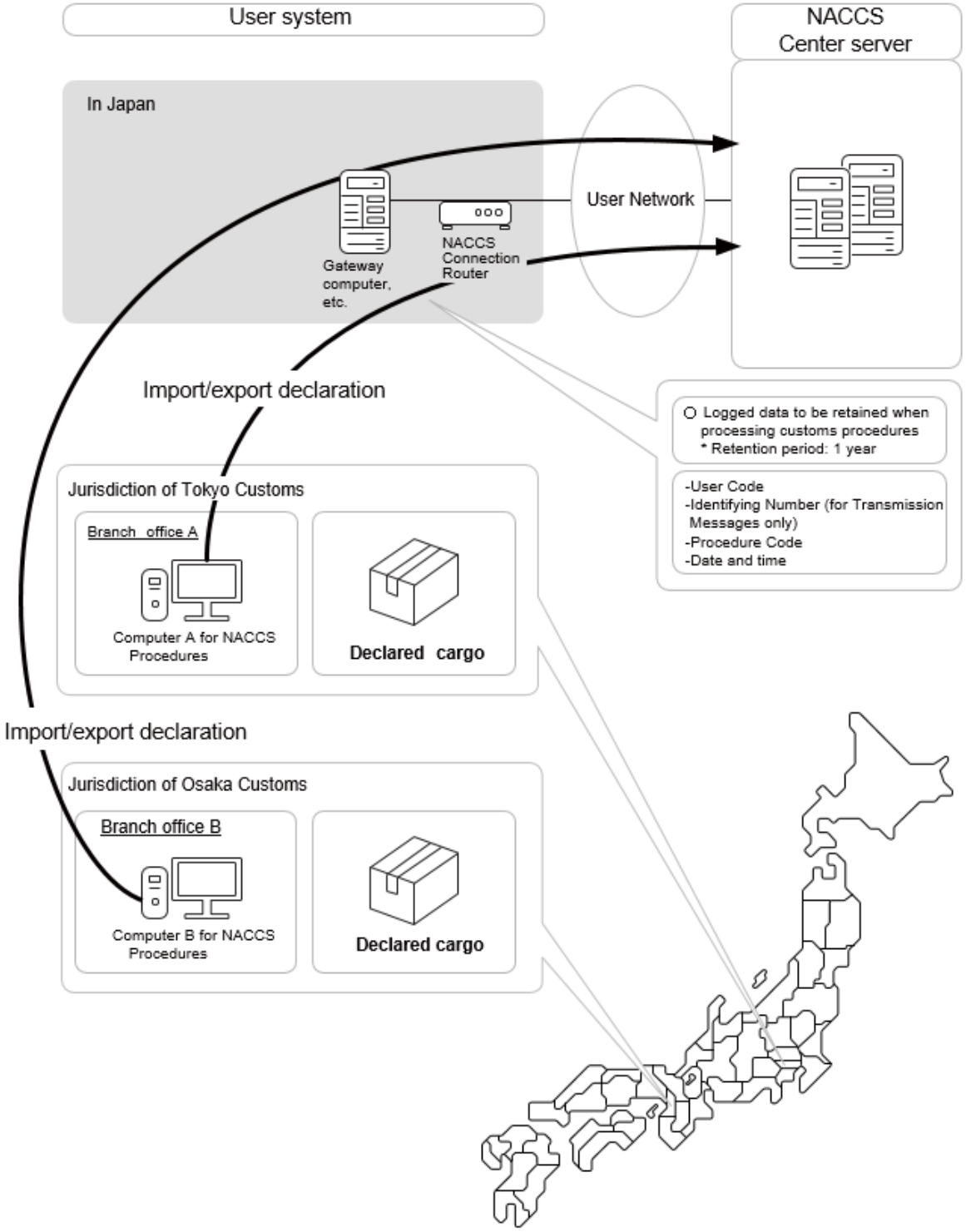

Figure 7.3.2 Logs for Import/Export Declaration Procedures, etc. Processed on computers Connected to Gateway Computers

7.3.4 Security Standards for Connections to External Networks

(1) Restrictions on the Use of NACCS Connection Router

(A) Use of LAN port

In the case of connections via a router or gateway, the LAN port of the NACCS Connection Router on user system side shall be set exclusively for access to the NACCS server, and therefore the LAN port cannot be used for other purposes. (The WAN port also cannot be used.)

(B) Use of console port

The console port is used by NACCS Center to set the NACCS Connection Router, and users must not connect any device to it.

(2) Restrictions on Connection to External Networks without Using NACCS Connection Router

(A) Case of connection to external networks using LAN connection (network-to-network connection)

Prior to connecting to any external network, the user is required to undergo security screening conducted by NACCS Center.

Examples of cases where connection to external networks (other companies' networks, Internet, etc.) is allowed are as follows.

Example 1: Case where a mechanism provided in the user network (proxy server being installed, etc.) does not allow access to user computers from external networks.

Example 2: Case where functions of the router (not the one provided by NACCS Center) used to connect to external networks include a NAT equivalent function (IP address conversion) that hides the User Internal Network from the outside.

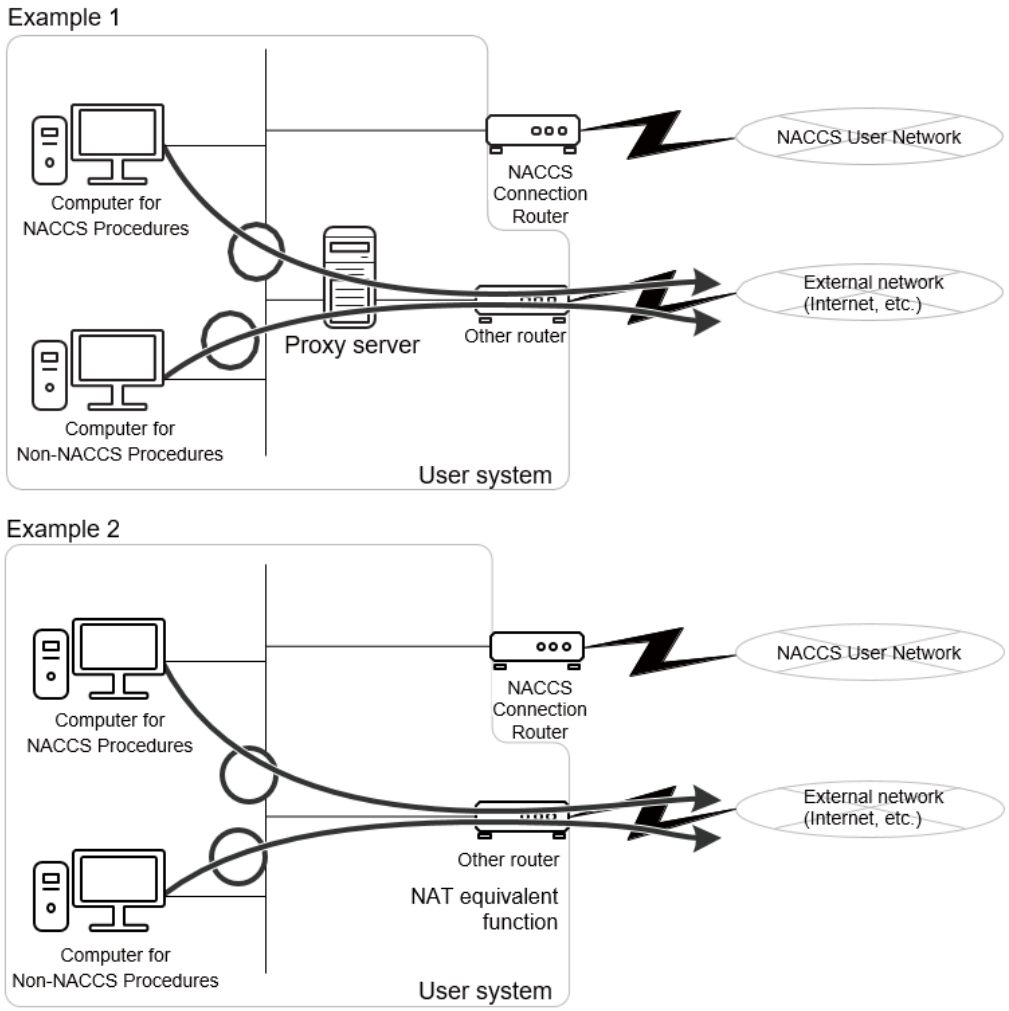

Figure 7.3.3 Examples (1 and 2) of Cases Where Connection to External Networks is Allowed

(B) Case of remote connection to external networks

Prior to connecting to any external network, the user is required to undergo security screening conducted by NACCS Center.

An example of a case where connection to external networks (other companies' networks, Internet, etc.) is allowed is as follows.

Case where a mechanism provided in the user network (VPN device being installed, etc.) does not allow third parties to access User Internal Network computers, external network computers, or networks between them. (Measures equivalent to those for User Internal Network computers are also taken for remote-connection external network computers.)

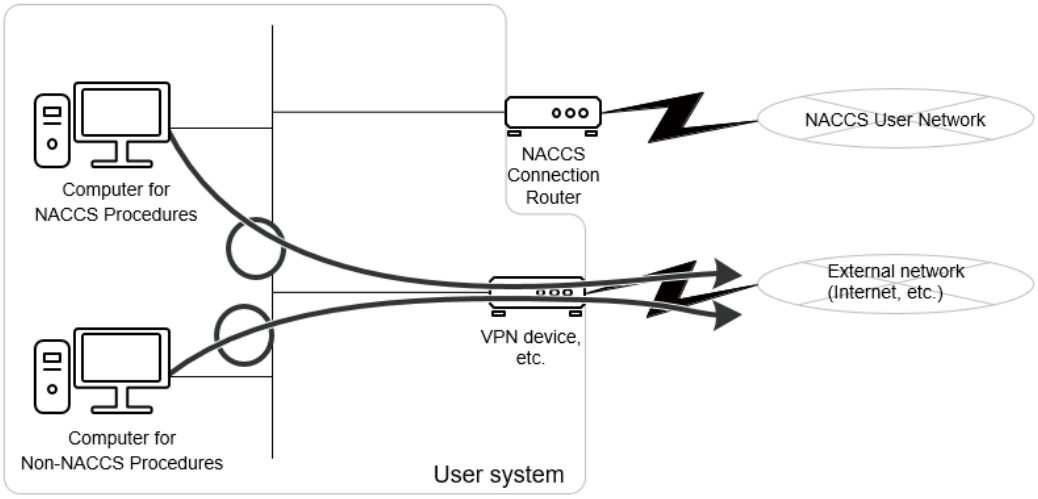

Figure 7.3.4 Example of Case Where Connection between External Networks and NACCS Processing Computer is Allowed

Table 7.3.3 Restrictions on Connection to External Networks without Using NACCS Connection Router

	LAN connection	Remote connection
Computer for NACCS procedures	Subject to security screening conducted by NACCS Center	
Computer for Non-NACCS procedures		