## 7.4 Security Measures for Users

When accessing the NACCS Center server, users shall comply with the security measures specified by NACCS Center and report to NACCS Center on details of safety measures they have actually implemented.

When security measures implemented are deemed to be inadequate or inappropriate, NACCS Center shall direct the users to take remedial measures.

### 7.4.1 Security Measures Implemented by Users

Table 7-4-1 Content of Security Measures That Users Must Comply with

| Content | Connection mode | | | Details | Remarks |
|---|---|---|---|---|---|
| | Peer-to-peer connection | Router connection | Gateway connection | | |
| (1) Placement of system administrator | ○ | ○ | ○ | • A system administrator shall be placed at each office where NACCS is used and at each location where a gateway computer is installed and reported to NACCS Center | |
| (2) Management of IDs and passwords | ○ | ○ | ○ | • The system administrator as given in (1) above shall manage IDs and passwords used for NACCS | 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 connecting to the NACCS Center server 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) Reporting of user system configuration | ○ | ○ | ○ | • The following documents pertinent to the user system that connects to the NACCS Center server shall be submitted to NACCS Center: | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | [1] System configuration diagram<br>[2] Configuration list of devices used | |
| (5) 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 |
| (6) Log management | | | ○ | In order to identify users that connect to the NACCS Center server from gateway computers, etc., administrator shall construct a system to manage the history (log) of data transmission/reception | See (*) for how to implement log management<br>The NACCS Center may request the submission of history log if it deems it necessary |

(*) 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 the NACCS Center server, the following items shall be logged and retained:

Table 7-4-2 Items to Be Logged and Retained by Users Using Gateway Connections

| **Transmission/ reception**<br>**Item** | **Upon transmission** | **Upon reception** |
|---|---|---|
| User code | ○ | ○ |
| Identifying number | ○ | – |
| 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.

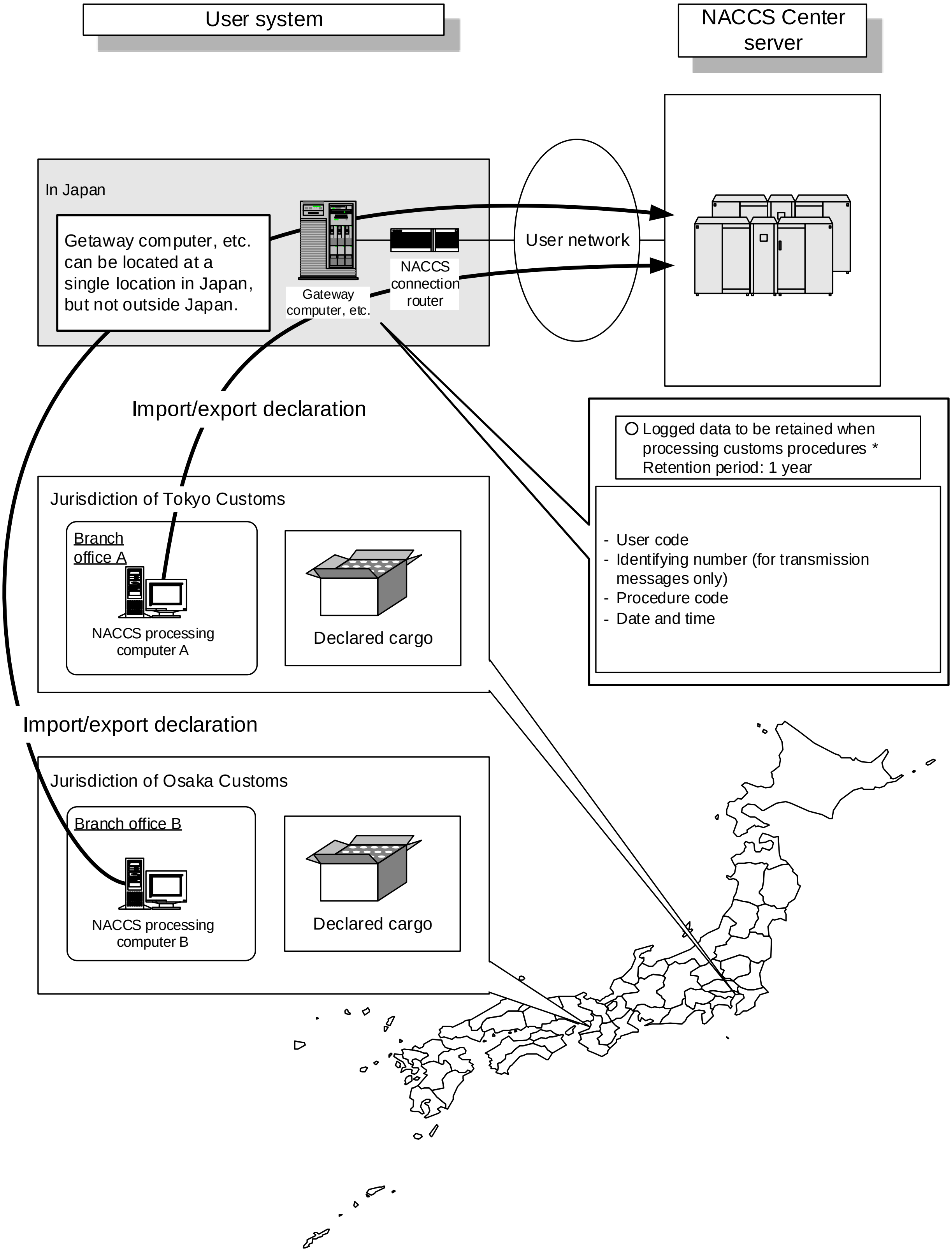
User system
NACCS Center server
In Japan
Getaway computer, etc. can be located at a single location in Japan, but not outside Japan.
Gateway computer, etc.
NACCS connection router
User network
Import/export declaration
○ Logged data to be retained when processing customs procedures * Retention period: 1 year
- User code
- Identifying number (for transmission messages only)
- Procedure code
- Date and time
Jurisdiction of Tokyo Customs
Branch office A
NACCS processing computer A
Declared cargo
Import/export declaration
Jurisdiction of Osaka Customs
Branch office B
NACCS processing computer B
Declared cargo

Figure 7-4-1 Logs for Import/Export Declaration Procedures, etc. Processed on computers Connected to Gateway Computers

Figure 7-4-2 [Deleted]

## 7.4.2 Security Standards for Connections to External Networks

(1) Restrictions on the Use of NACCS Connection Router

[1] Use of LAN port

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

[2] 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

[1] 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 internal network from the outside.

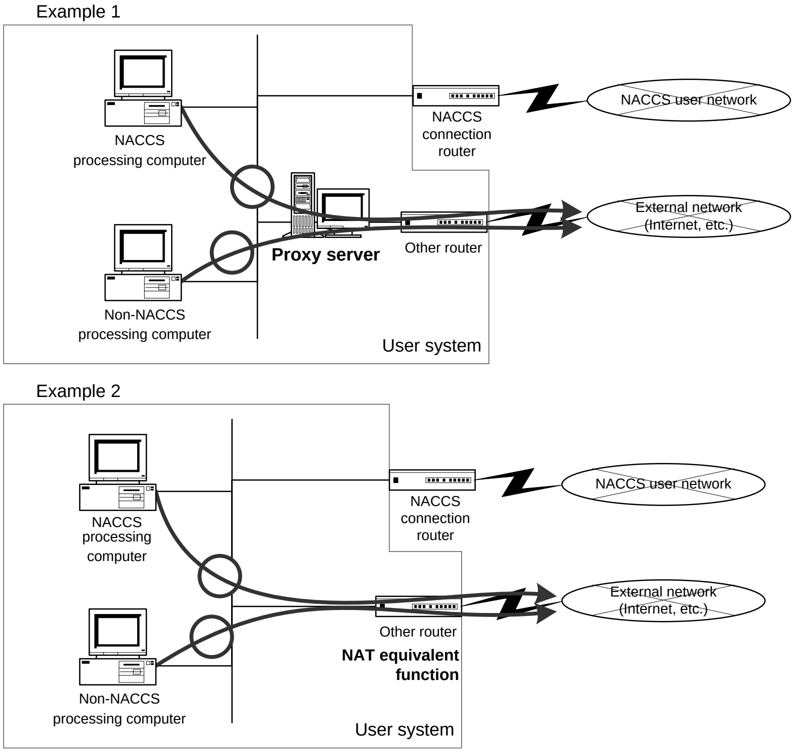

Figure 7-4-3 Examples (1 and 2) of Cases Where Connection to External Networks is Allowed

[2] 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.

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

Case where a mechanism provided does not allow a third party to access to a computer in an internal network and a computer in an external network and the network between the computers by users installing VPN devices, etc. (The same security measures must be taken for computers on the external network that are connected remotely as measures for computers on the internal network.)

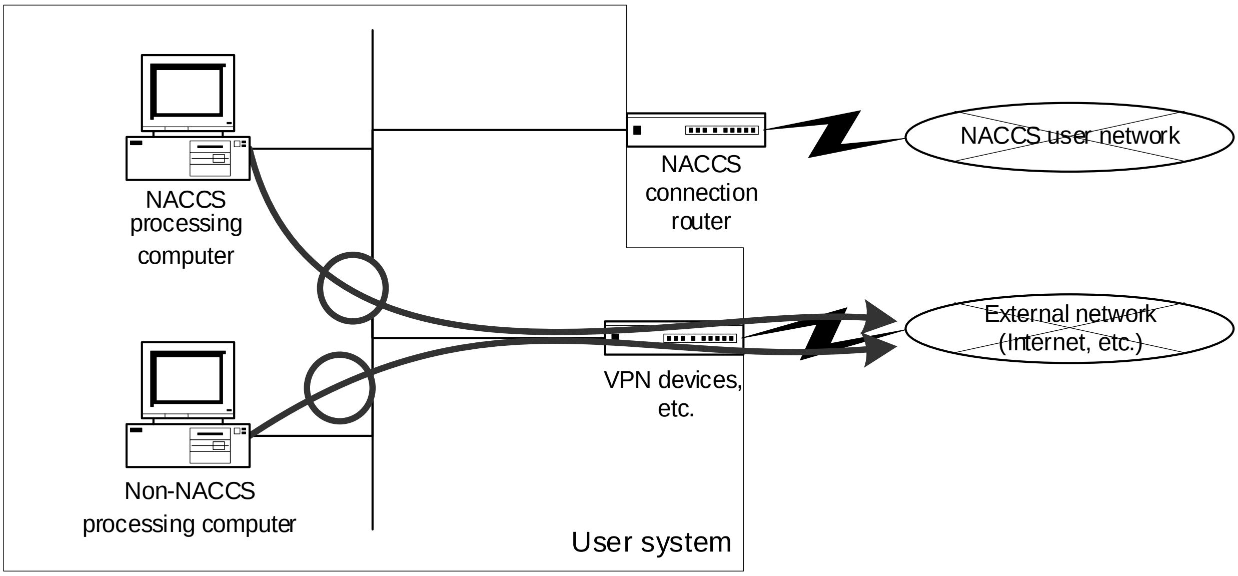
NACCS processing computer
Non-NACCS processing computer
NACCS connection router
VPN devices, etc.
User system
~~NACCS user network~~
~~External network (Internet, etc.)~~

Figure 7-4-4 Example of Case Where Connection between External Networks and NACCS Processing Computer is Allowed.

Figure 7-4-5 [Deleted]

Table 7-4-3 Restrictions on Connection to External Networks without Using NACCS Connection Router

| | LAN connection | Remote connection |
|---|---|---|
| NACCS processing computer | Subject to security screening conducted by NACCS Center | |
| Non-NACCS processing computer | | |