

Check the client PCs before network connection. If a security problem is found, it is immediately remedied, so a safe business environment can be maintained.

**HITACHI**  
Inspire the Next

## Introduction to Quarantine System



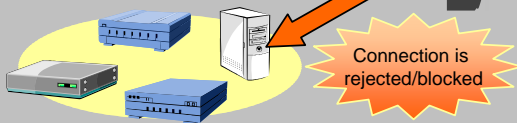
Client PCs with insufficient security are highly likely to be infected with viruses or leak confidential information. It is possible not to allow poorly protected client PCs to connect to a network, but sometimes such measures can cause problems for employees' business operations.

**Quickly detects client PCs that are violating the security policy!**  
**Automatically isolates the machine, treats the problem, helps the machine and restore a connection to the network.**

### Implementation of client PC Quarantine System

Distress in client PC security management

Connection from a PC with insufficient security



For PCs used for business purposes,  
- Unable to use PC, work stops  
- Blocking is not good enough

To keep business activities operating, a system is required that remedies the PC and allows quick re-connection to the business network

Countermeasures for security threats that change daily

Is mandatory software installed?

Is the virus definition file updated?

Are latest OS patches applied?

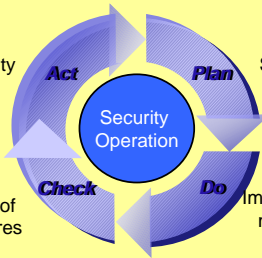


Remedy PCs and establish network connection based on the security policy!

PDCA cycle of security measures

Revise security policy

Monitor status of security measures



Set up security policy

Implement preventive measures against security threats

JP1's Quarantine System designs the security policy according to asset management information, allowing the system to quickly respond to new security threats.

Since client PCs with insufficient security countermeasures can be remedied automatically, corporate network security level can be maintained without hindering business operations.



Ensure the security level of client PCs  
Stop improper use of client PCs  
Prevent information leaks  
Remedy and recover client PCs with security problems

#### Client PC remedy flow

Authenticate/Inspect

- Authenticate PC
- Inspect security (patches, unauthorized software)

Isolate

- Block/restrict connection to business network
- Connect to quarantine network

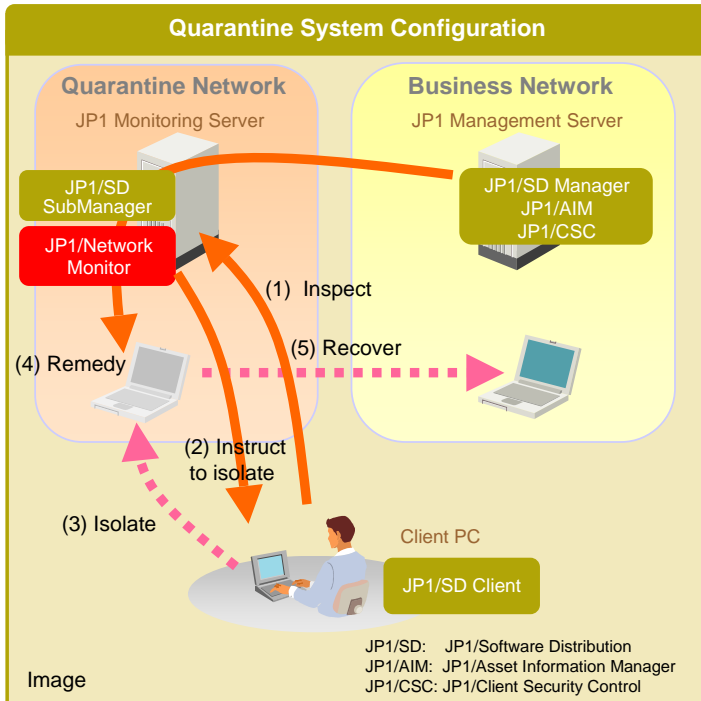
Remedy

- Update security patch
- Update virus definition file
- Install mandatory software

Recover

- Connect to business network

## The Quarantine System can be established using the following configuration:



- It is not necessary to introduce new network equipment or change the network configuration. (Connection is controlled by software.)
- Client PCs do not require supplicant software.
- It is not necessary to request that the client PC user perform authentication operation (ID/password input).
- The entire network can be monitored with one machine by connecting the JP1 Monitoring Server to the tag port of the network switch.
- Client PCs can be used both in fixed-address and DHCP environments.
- JP1 Monitoring Server must be Windows XP or Windows Server 2003.

### Required Products

Product Name
JP1/Client Security Control - Manager
JP1/Asset Information Manager
JP1/Software Distribution Manager
JP1/Client Security Control - Agent
JP1/Network Monitor
JP1/Network Monitor - Manager
JP1/Software Distribution Client

### Inquiries about these products

Feel free to contact us regarding these products:

### Information service

Further information about JP1 can be found online at:

<http://www.hitachi.co.jp/jp1-e>

JP1 is an acronym for Job Management Partner 1.

The company and product names in this document are trademarks or registered trademarks of their respective companies.