

PCs with low security levels are automatically removed to protect the system from information leakage and virus threats

HITACHI
Inspire the Next

Client Security Control with Network Monitor



Is your company exposed to viruses and confidential information being exported because unauthorized private PCs are connected to your network? Do you spend valuable time and effort dealing with such problems?

JP1 Client Security Strengthened Solutions protects systems from information leakage and virus threats by automatically removing unauthorized private PCs and comprehensively monitoring security conditions.



We can protect your system from security threats by rapidly detecting clients who have inadequate security solutions, and then implementing preventative measures according to security policies.

Client Security Solutions



Client security solutions using JP1

JP1/Client Security Control

Administrators can uniformly manage asset information for all clients, and monitor client security solutions. When a client who has inadequate security solutions is detected, preventative measures against security threats can be implemented according to security policies.

JP1/Network Monitor

By constantly monitoring corporate networks, the connection of unauthorized PCs is immediately detected, and such PCs are automatically removed from the network. The system administrator can also remove authorized PCs that have inadequate solutions against viruses or other problems.

JP1/Client Security Control can be linked to JP1/Network Monitor to provide faster and stronger preventative measures against security threats.

Reducing the security management burden allows administrators to concentrate on setting and improving security policies



Ensure the security level of client PCs
Stop invalid use of client PCs
Prevent information leaks
Eliminate vulnerable client PCs

Key Functions

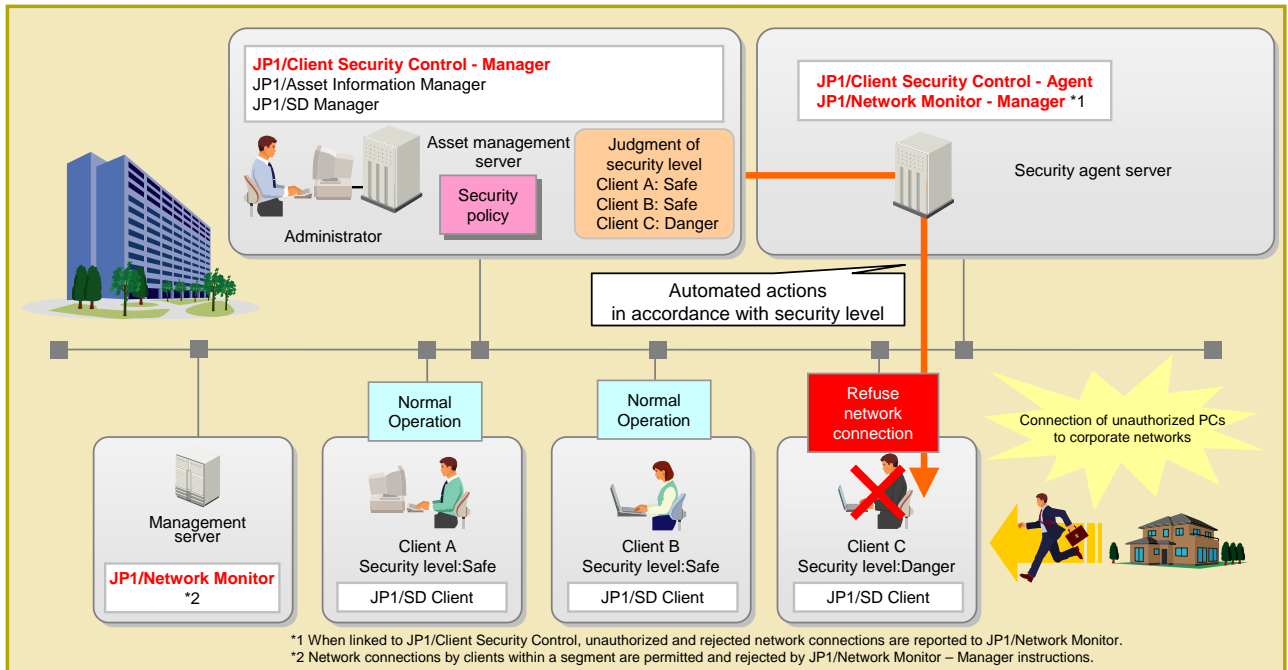
JP1/Client Security Control

- Monitor status of security measures
- Manage security policy
- Implement preventative measures against security threats (execute automated actions)
- Automated actions:
 - Notify the administrator by email
 - Send a warning message to the user
 - Permit / refuse network connection

JP1/Network Monitor

- Detect an unauthorized PC
- Bar an unauthorized PC
- Flexibly compatible with IP address systems and network configurations

Strong security solutions are possible by linking JP1/Client Security Control to JP1/Network Monitor.
The security level of the entire system is maintained.



*1 When linked to JP1/Client Security Control, unauthorized and rejected network connections are reported to JP1/Network Monitor.
 *2 Network connections by clients within a segment are permitted and rejected by JP1/Network Monitor – Manager instructions.

Monitor status of security measures

Security solution conditions can be comprehensively monitored through automatic collection of client inventory information. Specifically, installation conditions of Windows updates, anti-virus products, and other software can be monitored.

Manage security policy

The security policy that is derived from the judgment policies for judging client security levels and security policies based on the action policies for implementing actions can be managed. When a client updates software or anti-virus product information, the client security level is automatically judged according to the security policy.

Implement preventive measures against security threats (automatic action)

If a client that has insufficient security solutions is detected, action appropriate for that security level is automatically implemented according to the action policy. When linked to JP1/Network Monitor, clients with low security levels can be automatically removed from the network.

Benefits of JP1/Network Monitor

- Since corporate networks can be self-monitored and unauthorized PC connections are rapidly detected and removed, the dispersal of viruses can be prevented even if an unauthorized connection with a contaminated PC occurs. The export of data via an unauthorized connection can also be prevented.
- Even in environments that use wireless LAN, HUB, and switches, unauthorized connections can be pinpointed and removed.
- Networks can be used without interruption to authorized PCs or servers when unauthorized PCs are being removed.
- Monitoring and removal can be performed regardless of the address system (such as for fixed IP addresses, DHCP, or their combined use).

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/Software Distribution Client

* Includes the license of JP1/Network Monitor - Manager

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.