MasterScope SystemManager G
Function Introduction
# Major functions of MasterScope SystemManager G (standard functions)

<table>
<thead>
<tr>
<th>Category</th>
<th>Function</th>
<th>Functional outline</th>
</tr>
</thead>
</table>
| Monitoring functions | **Service and process monitoring** | • Windows service alive monitoring/process alive monitoring  
• Threshold monitoring of process ID changes and the number of startup processes. |
| | **Performance monitoring** | • Resource information (CPU/memory usage, disk usage, etc.) is collected from each server and threshold monitoring of upper and lower limitation is performed. Performance monitoring per process is available as well.  
• Threshold monitoring and notification to the operator by three judgment methods: sequential, N times continuous, N times average.  
• Resource information can be accumulated and displayed as a graph or printed out. Support for analyzing operating status and problems. |
| | **Log monitoring** | • Message monitoring by extracting necessary logs from syslogs, event log, and any text log files output by applications.  
• Suppress identical messages on the Agent side to avoid message overload. |
| | **File and directory capacity monitoring** | • Monitor existence, capacity, and updates of files and directories.  
• Prevent disk space exhaustion and enable early detection of essential system file deletion or update. |
| | **Service port monitoring** | • Monitor open/close status of user-specified TCP/UDP ports |
| Management functions | **Topology management** | Monitoring target servers can be grouped by location or customer-specified role. |
| | **Message management** | Messages can be accumulated and managemed per server or system. Messages can be marked according to the presence of comments or response status, allowing information to be shard between operators. |
| | **Notification control** | • Notification by email or alarm lamp triggered by message issuance, change in monitoring process or service status, or excess of resource threshold values.  
• Commands can be executed on the Manager triggered by message issuance. |
| | **Configuration management** | Centralized view of monitoring target server configuration information (such as devices, systems, software, networks, and disks) |
| | **User management** | Limitation of investigation range authorities for each user prevents operational errors and improves security by assigning appropriate authorities. |
| | **Audit logs management** | Support for internal control by managing the operational details and result history of operations performed on the console and automatically executed. |
| | **Schedule control** | Schedule monitoring to start/stop for each server. |
| | **Command execution** | Predefined recovery commands can be executed triggered by events. |
| Build functions | **Agent auto-build** | Ansible scenarios (roles) is provided to perform operations from Agent installation to monitoring configuration. Remote execution and error-free auto-building of Agents. |
## Major functions of MasterScope SystemManager G (optional functions)

<table>
<thead>
<tr>
<th>Category</th>
<th>Function</th>
<th>Functional outline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitoring functions</strong></td>
<td><strong>Application monitoring</strong></td>
<td>Monitoring of performance with graphical view of application operating status. Accumulation of operating status data as statistics for system problem analysis and improvement.</td>
</tr>
<tr>
<td></td>
<td><strong>IT service response monitoring</strong></td>
<td>Monitoring of end-to-end operating status and response for HTTP, Mail, DNS, TCP, and FCP based on settings that accord with the user’s purpose.</td>
</tr>
<tr>
<td></td>
<td><strong>Hypervisor monitoring</strong></td>
<td>Monitoring of virtual server resources and events for the hypervisor (VMware ESXi).</td>
</tr>
<tr>
<td></td>
<td><strong>Cloud monitoring</strong></td>
<td>Instances on the cloud can be monitored via an API provided by public cloud (CloudWatch) without installing an Agent.</td>
</tr>
<tr>
<td></td>
<td><strong>Customizable performance monitoring</strong></td>
<td>User-specified commands and program output results can be extracted by column and used as monitor counters. It can be displayed as a graph or output as a unified form.</td>
</tr>
<tr>
<td><strong>Management functions</strong></td>
<td><strong>Message management (Monitoring from a business perspective)</strong></td>
<td>Events reported from monitoring targets can be classified on the Business View from the perspective of the customer’s business.</td>
</tr>
<tr>
<td></td>
<td><strong>Knowledge management</strong></td>
<td>Users are informed of actions to take for failure recovery.</td>
</tr>
<tr>
<td></td>
<td><strong>Message correlation analysis</strong></td>
<td>Correlation analysis function of multiple event information, automated action, and notification. Conditions can be specified such as the satisfaction of condition 1 &amp; condition 2, and the occurrence of an event for the specified number of times within the specified time frame.</td>
</tr>
<tr>
<td></td>
<td><strong>Hierarchical Manager</strong></td>
<td>Messages across the entire system are monitored centrally by linking multiple Managers hierarchically and having lower-level Managers report collected messages to higher level Managers.</td>
</tr>
<tr>
<td></td>
<td><strong>System performance analysis</strong></td>
<td>Regression analysis on collected performance data shows the tendency and predicts the future values. Correlation analysis on collected performance data detects abnormal behavior and suggests the cause.</td>
</tr>
<tr>
<td></td>
<td><strong>Web Console</strong></td>
<td>Web-based monitoring dashboard to view overall system status at a glance.</td>
</tr>
<tr>
<td><strong>Control functions</strong></td>
<td><strong>Operation control</strong></td>
<td>Commands can be executed for monitoring target servers at user-specified timing.</td>
</tr>
<tr>
<td></td>
<td><strong>Workflow control</strong></td>
<td>Flows such as failure recovery and daily operations can be predefined as scenarios and automatically executed.</td>
</tr>
<tr>
<td><strong>Linkage functions</strong></td>
<td><strong>Application linkage</strong></td>
<td>Logs collected by MasterScope SystemManager G can be output as text files.</td>
</tr>
<tr>
<td></td>
<td><strong>Service desk linkage</strong></td>
<td>Incidents can be registered to incident management software automatically or manually.</td>
</tr>
</tbody>
</table>
Function Detail
Service and Process Monitoring

Monitoring processes and services allows admin to receive alerts when an anomaly is detected.

- System down
- Visually keep track of service/process status
- Improve usability of system information by grouping
Service and Process Monitoring Setup

- **Service monitoring setup**
  - Check the services you want to monitor

- **Process monitoring setup**
  - Select the running process you want to monitor from the list
  - Specify the maximum/minimum number of monitored processes
Performance Monitoring

Monitor OS information (like CPU utilization, memory, and disk space) by simply setting thresholds to warning and anomaly notifications.

Available threshold setting can be selected from the following patterns:
- **Sequential**: an event occurs when a collected value exceeds threshold
- **Continuous**: an event occurs when a collected value exceeds threshold consecutively for the specified number of times
- **Average**: an event occurs when the average collected values of the specified number of times exceeds threshold.

Example:
If available MEM become less than 50Mbytes, notify admins of an anomaly.

Performance data accumulation enables Tendency/Resource analysis

Performance data accumulation could be utilized for operations status/failure analysis

Performance data accumulation can be enabled simply by checking settings boxes
SystemManager G provides a multi-graph view to visualize the data gathered from the hosts and quickly creates a graph to compare the past data and the current data.

For example, you can create a graph to display CPU performance data on all hosts.
Reporting (Print view)

Report the performance data collected on SystemManager G to a PDF file.

- Graph of performance data
- Reporting the performance data in predefined intervals (weekly/monthly/yearly)
- Maximum, minimum and average of each counter
- History of each counter

Administrator
Log Monitoring (event log/syslog/application log)

Monitor all text-based log/syslog/event log, and notifies admin on specified information with the keyword filtering.

*Some text-based log files are rotated in some unintentional situations (its size exceeds some values, date change, etc.). MasterScope SystemManager G is capable of monitoring this type of text-based log.
Filtering

Message filtering extracts important messages and suppresses duplicate messages for efficient analysis.

**Functions**

<table>
<thead>
<tr>
<th>Functions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter for extraction</td>
<td>Notify if a message includes the specified keywords.</td>
</tr>
<tr>
<td>Filter for deletion</td>
<td>Do not notify if a message include the specified keywords.</td>
</tr>
<tr>
<td>Suppression of duplicate messages</td>
<td>Do not notify if identical messages are generated during the specified time frame.</td>
</tr>
</tbody>
</table>
File and Directory Monitoring

File/directory monitoring prevents disk depletion by monitoring file size and enables early detection of deletion/modification of important files.

- Monitors target agents’ files and directories for their existence, used space and modification
- Changes the color of icon if utilization of file exceeds specified value, or file is deleted
- Message or alert is notified if its status changes (including file modification)

<Example: monitoring log files/folders>

- If used space of disk c exceeds 80%, send warning message. (performance monitoring)
- If used space of folder exceeds 2Mbytes, send warning message.
- If size of specified file exceeds 1Mbytes, send warning message.

Manage and monitor status change of files by each group.

- Change color while size of file exceed specified value.
- Notify admins if status changes (including file modification).
Monitor TCP/UDP port (ftp, telnet, http, etc.) on the agent. Show message on message view if the status of monitored port is changed.

Remote agent can monitor the port on a remote host

Service Port Monitor Setting

Display name: NTP
Port number: 12345
Protocol: TCP
Detail:
- Normal port status: Open
- Interval: 10 Sec
- Connect timeout: 1 Sec
- Retry count: 0
- Monitoring address: localhost
- Report only when the service port status is OPEN

OK
Cancel
Topology Management (from the view point of managing server)

Topology view allows you not only to monitor server physically, but also to manage servers with information about location and role.

- NEC
  - Manage servers in NEC

- NEC DataCenter
  - Manage servers on datacenter in NEC

- Rack01
  - Manage servers on rack01

Trouble on a server in rack01

☆ Check the red colored icons to see the install location of the failed server.
Message Management (1/2)

Message management function allows you to monitor messages generated by log monitoring, process monitoring, and so on.

Box color changes according to the priority of the generated messages

This view shows messages generated by monitoring function
Message Management (2/2)

Messages can be displayed per server or for all monitored servers in one console.

This view shows generated messages from all monitored servers. When Network Manager has been installed in, messages from monitoring network devices are also displayed in this view.

This view shows generated messages per monitored server.
Easy Process of Identifying Failure

1. Confirmation of server status
   - System Configuration / Status
   - Report by email and flasher

2. Check message index.
   Detailed message by double-click.

3. Refer to message details
   - Messages from all servers
Share Recovery Status

Registering troubleshooting steps to messages enables team members to share the current working status, ensuring a smooth handover.
Notification Control

Automatically send e-mail and execute recovery command in case of failure.

This is alert from MasterScope.
-----------------------------------------
Date       : 2016/06/06
Time       : 10:22:32
-----------------------------------------
Node        : DB Server01
Severity    : Critical
Application : Oracle
Object      : OracleMonitor
-----------------------------------------
Message ID  : 00410102
Message     : Failed to connect to database
-----------------------------------------

Receive current machine status by e-mail

Execute pre-defined command according to failure events
Configuration Management

Centrally manage and view the monitored servers via console

Even if communication with agent is not available, configuration view is available.

<table>
<thead>
<tr>
<th>Item</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device information</td>
<td>Device name and its vendor information (i.e. HDD)</td>
</tr>
<tr>
<td>System information</td>
<td>OS version, host name, CPU information, etc.</td>
</tr>
<tr>
<td>Software information</td>
<td>Installed software with its version.</td>
</tr>
<tr>
<td>Network information</td>
<td>IP, MAC address, network identifier, etc.</td>
</tr>
<tr>
<td>Disk information</td>
<td>Drive name, available space, etc.</td>
</tr>
</tbody>
</table>

Note: acquirable information is dependent on platforms
User Management

Assigns operating permission to each user to prevent operation mistakes and enhance security

- Operator can see only his own servers
- Admin can see overall system information

Set permission and add users to group.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>Refer to the information of the system.</td>
</tr>
<tr>
<td>Operation</td>
<td>Perform operations such as confirming messages and starting/stopping processes/Windows services.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Define configuration with the configuration mode.</td>
</tr>
<tr>
<td>License</td>
<td>Register and manage licenses.</td>
</tr>
<tr>
<td>User Management</td>
<td>Create users/groups and assign permissions to them.</td>
</tr>
</tbody>
</table>
Audit Logs Management

For operations on SystemManager G, when, who, and what are recorded and admin is notified as configured.

- Operations on MasterScope SystemManager G (including monitored nodes, manager’s GUI, automatic operations) are recordable as audit logs for future tracing.
- These logs can be displayed by categories and notification settings can be specified for categories.

**Tree view for audit logs mgmt**

<table>
<thead>
<tr>
<th>Category</th>
<th>Log details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Record logs generated by applications</td>
</tr>
<tr>
<td>Security</td>
<td>Record audit logs from user management</td>
</tr>
<tr>
<td>System</td>
<td>Record audit logs from SystemManager G</td>
</tr>
<tr>
<td>Audit logs</td>
<td>Record audit logs from this function itself</td>
</tr>
</tbody>
</table>

Who operated

What is operated (apply, create, add, modify, delete, refer, execute, notify)
Schedule Control

SystemManager G can start and stop monitoring according to pre-defined schedule.

It allows you to set monitoring schedule per server.
SystemManager G can execute commands i.e. recovery job and log collect job on monitoring server by manual or automatic.

In case of manual recovery, administrator judges command execution.

1. Notification
2-1 Execute recovery command
2-2 Execute log collection command

Manager

System Admin

Monitored Server

Recovery Type Setting

Description: Reboot Web Service
Type: Auto Execute

Recovery List:

Description: Reboot Web Service
Type: Auto Execute

Action List:

Description: Reboot service
Target Host: SYSMGRS-PDC-MGR
Command: C:/web service reboot.bat

NEC Provides “Role” of Ansible which automates the procedure to install and setup an agent, reducing setup time, human error, and SI costs.

Before

- Need to install an agent on each server. Currently engineers are manually setting parameters via install wizard (GUI).

Manual installation of agents on many servers may
- require so much time and workload
- cause human errors such as mistyping parameters

After

Agent installation is completed just by running playbook from Ansible server.

Automated installation -> Low cost
Automated setting -> No human errors
Application Monitoring

Monitor application performance by simply setting thresholds for warning and anomaly.

Available threshold setting can be selected from the following patterns:
- **Sequential**: an event occurs when a collected value exceeds threshold
- **Continuous**: an event occurs when a collected value exceeds threshold consecutively for the specified number of times
- **Average**: an event occurs when the average collected values of the specified number of times exceeds threshold.

If buffer cache hits of Oracle become less than threshold, please notify.

Performance data accumulation enables Tendency/Resource analysis.

Performance data accumulation could be utilized in operations status/failure analysis.

Performance data accumulation can be enabled simply by checking settings boxes.

Monitor performance with two level threshold settings.

Threshold monitoring

Threshold exceeding!

Notify
Support Application Lists

The following table provides support platform information.

<table>
<thead>
<tr>
<th>Middleware</th>
<th>Support version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Base</strong></td>
<td></td>
</tr>
<tr>
<td>Oracle Database</td>
<td>• Oracle 11gR2, 12cR1, 12cR2</td>
</tr>
<tr>
<td>SQL Server</td>
<td>• SQL Server 2008 SP4, 2008R2 SP3, 2012 SP3, 2014 SP1/SP2, 2016(SP1), 2017</td>
</tr>
<tr>
<td><strong>Web/AP Server</strong></td>
<td></td>
</tr>
<tr>
<td>IIS</td>
<td>• IIS 7.0, 7.5, 8.0, 8.5, 10.0</td>
</tr>
<tr>
<td>WebLogic Server</td>
<td>• WebLogic Server 11gR1, 12cR1, 12cR2</td>
</tr>
<tr>
<td>WebSphere</td>
<td>• WebSphere Application Server 7.0, 8.0, 8.5</td>
</tr>
<tr>
<td>Application Server</td>
<td></td>
</tr>
<tr>
<td>Apache HTTP Server</td>
<td>• Apache 2.2, 2.4</td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td>• Tomcat 6.0, 7.0, 8.0, 8.5</td>
</tr>
<tr>
<td><strong>Others</strong></td>
<td></td>
</tr>
<tr>
<td>SAP</td>
<td>• SAP ERP 6.0</td>
</tr>
<tr>
<td></td>
<td>• SAP NetWeaver 7.0, 7.3</td>
</tr>
<tr>
<td>Java application</td>
<td>• Running applications on Java 6, 7, 8, 9</td>
</tr>
</tbody>
</table>
Application Monitoring Template

Addition/change of monitoring items can be implemented easily.

Extensive monitoring items
Monitoring items are available as template

Easy settings of monitoring items
Detailed settings are in dialogue form and can be set easily

Customization
Monitoring items can be added/modified easily

High Operability
Operation is possible right after implementation

3 Steps to start monitoring after installation.
Easy customize of monitoring items by GUI.

1. Import template files
2. Select an application instance name and check whether to store history log or not.
3. Start monitoring based on the template

- It looks too difficult to set monitoring items to all target servers.
- Only experts know what monitoring items are necessary to our system

Option
Oracle Monitoring etc.
Accesses Web System periodically using Probe (simulate users) and monitors availability and end-to-end performance.

Note: Scenario is a record of executed operation in the browser. It is used to access IT server for monitoring.
Hypervisor Monitor option enables integrated monitoring of Hypervisor and VMs.

SystemManager G Agent monitors application log, process, service and performance on VMs.

Administrator can see running status on VM and Hypervisor in one single console.

Resource Monitoring monitors CPU and Memory Usage.

Event Log Monitoring monitors Alert logs of hypervisor.

Hypervisor monitoring is performed by Hypervisor Monitor.
Cloud Monitoring option enables integrated monitoring of on-premise and Amazon Web Services.

Cloud Monitoring monitors performance data and events in AWS through Amazon CloudWatch API.

- Operation and performance monitoring
- Resource status event monitoring
Customizable Performance Monitoring

The numerical data results of arbitrary command and program are stored in database as performance data. The data is used for threshold monitoring, performance chart, and report.

Use Case

Users want to integrate new system and existing system, but existing system collects performance data using user defined program. ⇒ Utilize the existing program and realize integrated monitoring

There are programs to output data of user access and users want to show the data on chart and report. ⇒ Customizable performance monitoring realizes this request by monitoring data of user access

Display custom monitoring items

3. Configure the monitoring settings in the same way as with regular performance monitoring.

- Collect performance data at every defined interval
- Threshold is also displayed

SystemManager G View
1. Send monitoring definition files
SystemManager G Manager
2. Send the definition to agent
SystemManager G Agent

Option
Customizable
Performance Monitoring
Not only are online messages displayed, Business View also allows you to categorize messages and change message levels for easy management.

In this example, messages of development, operation, and security system are managed.
Knowledge Management (Share Operation Know-How)

Knowledge function enables to share daily operation as know-how, standardize the skill and speedy action, and reduce operational cost.

Knowledge can be displayed only by clicking the [Help] tab.

Linked application or file can be activated from the button on message detail.
Correlation monitoring of multiple events enables to detect failures which cannot be discovered by monitoring single event.

Monitoring only normal messages cannot detect abnormal status.

SystemManager G sends alert messages if correlated filter rule is not satisfied. For example, the backup starts normally but it is not responding for more than 30 minutes.

Correlation Message Logs

- 2017/12/25 02:30:00 Normal Backup Start
- 2017/12/25 03:30:00 Critical Backup Error
Hierarchical architecture redistributes workload to available resources and enables system administrator to monitor all systems in one console.

Master of Manager (MoM)

MoM receives only important messages by filtering

SysMgrG(MG)

SysMgrG(View)

Regional Manager(RM)

SysMgrG(View)

Monitoring System A

SysMgrG(MG)

SysMgrG(AG)

Monitored Servers

System A

SysMgrG(View)

Regional Manager(RM)

SysMgrG(View)

Monitoring System B

SysMgrG(MG)

SysMgrG(AG)

Monitored Servers

System B

MoM receives a failure message from RM and orders RM to execute recovery commands on the failed server.
Graphs indicate the time of occurrence and severity of failures. Map view shows specific component primarily causing “abnormal behavior” and its impact.

- Extract and visualize specific component primarily causing the “abnormal behavior” by automatic analysis.
- The impact of abnormal behavior can also be observed at a glance.

Visualize “abnormal behaviors”
Shows the time of occurrence and the severity of the abnormal behavior using an intuitive graph.

Visualize by map views
The red point indicates the component primarily causing the “abnormal behavior” and its severity. The blue points indicate all the components affected by the root cause.
Silent Failure Detection

For failures without error messages, various system components need to be checked by specialists with specific skills and experience.

- Silent failure occurs often in complex large-scale IT systems and it is difficult to resolve the failure.
- Silent failure may generate performance degradation caused by undetectable bottlenecks.

Response is so slow...

Silent failure occurred

Users

What is the problem?

Is this the cause?

Too much info to search...

This looks suspicious...

I can't find any error messages

System Admin

AP Admin

DB Specialist

NW Specialist

Web

AP

DB

HW Admin

Silent failure occurs often in complex large-scale IT systems and it is difficult to resolve the failure.

Silent Failure:

Period while Silent failure is undetected

Analyze failure and localize root cause

Trouble Shooting

No error messages

User escalation

It takes too long time to detect root cause

MasterScope SystemManager G Invariant Analyzer Option can resolve it
Difference between SystemManager G and other performance monitoring tools

Complex configurations are not required. You just need to input performance data. It is unnecessary to set up thresholds since it focuses only on invariant relationships among performance data.

**Traditional Monitoring tool**

Analyzing numerous data points is not simple and easy.

Frequent review of the thresholds is required due to business condition changes.

Workload is **heavy**

**SystemManager G**

Just input performance data. Easy analysis without specialized expertise.

No need to adjust the configuration from time to time due to business conditions.

Workload is **light**
Web browser console allows you to monitor systems from terminals without View installed.

*MasterScope SystemManager G8 Web Console is required.

Option
Web Console

Server Status

Message Monitoring
*BussinessView Option is required.

Monitoring Template

Performance Report

Web Console

Infrastructure Management

System Administrator

System Manager

Configuration/Reference

HTTP or HTTPS

Application Management

Application Administrator

Configuration/Reference

Configuration/Reference

Message Monitoring

Failure Monitoring

Monitoring Operator

Configuration/Reference

Configuration/Reference

Configuration/Reference

Configuration/Reference

Configuration/Reference
Monitoring Dashboard (Web Console)

You can create and customize your dashboard with widgets to get a quick view of the system status as soon as you login.

Widgets can be freely added and adjustable on a personal dashboard for each user.

Option
Web Console

Move from severity counter to server status screen. Search result with the severity is shown.

Move from severity counter to message screen. Search result with the severity is shown.

BusinessView Option is required.
Performance reports are displayed using tabs. Host availability, ranking, and capacity management by regression lines are newly added features.

Drawing a regression line based on performance data during the specified time period enables you to estimate resource scarcity in the future.
You can execute frequently used commands from integrated console. Visual command control helps reduce human error and simplify the operation.

Useful for executing routine commands such as deleting log files, starting and restarting services, etc.

No need to develop remote execution setup.

Integrated console shows execution status

Visualized list of defined commands help reduce operation mistakes.

You can keep track with all the operations.
Workflow Control

Execute various commands by operation workflow registered in advance. Automatic operation realizes safe and efficient management.

Reduce human error and workload by automating alert settings for daily reboot, planned system down for maintenance, etc.

Easy setup for operation workflow using GUI.

Operations can be scheduled.

Automates process

Forgetting to stop alert triggers it at reboot

Stop server alert (automatic)

Automated process

Restart server monitoring (automatic)

Forgetting to restart monitoring risks system stability. Operational error.

Restart server monitoring (manual)

Automates complicated manual operation by scenario control

Stop server alert (manual)

Reboot

Daily Reboot

With SysMgrG

Operational error.

Process

Problem

Daily Reboot
SystemManager G can link another monitoring tool by outputting collected messages to an external file.

SystemManager G can format and output message as text.

Monitoring tool processes the text file generated by SystemManager G.

User application

Monitoring tool
Collaborating HP Service Manager and SystemManager G makes the acquisition of the server status and tracking work progress very easy.

- HPE Service Manager
- MasterScope SystemManager G

Automatically register events to HP Service Manager
Register incidents

Service Desk Linkage (Integration with HPE Service Manager)

- Query
- Users
- Monitoring
- Error
- Disk Failure

Option
ServiceManagerLinker

GUI setting to map error events to ticket on Service Manager
Thank You

Realize simple and integrated system operation

For more product information, visit >> http://www.nec.com/masterscope/

For more information, please contact your local NEC representative or contact us at global@soft.jp.nec.com