THE POSSIBILITIES ARE INFINITE FUJITSU

Cautions When Using BitLocker™Drive Encryption on PRIMERGY

July 2008

Fujitsu Limited

Table of Contents

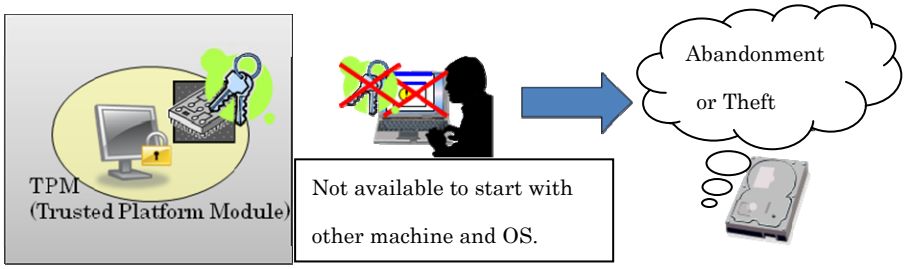
Windows Server and BitLocker are trademarkds or registered trademarks of Microsoft Corporation in the United States and other countries.

Preface

BitLocker™ Drive Encryption (BitLocker) is a new security feature in the Windows Server 2008 operating system. Fujitsu offers the PRIMERGY servers that are equipped with a TPM (Trusted Platform Module)*1 security chip to support the BitLocker feature in Windows Server 2008.*2 BitLocker encrypts the system volume and the data volume.*3 A BitLocker-encrypted system requires special considerations when you expand the system or during planned maintenance. This document provides information you need to use BitLocker and how to resolve the encountered issues.

*1: Trusted Platform Module security chip

A baseboard on the PRIMERGY server is equipped with a TCG (Trusted Computing Group)-compliant TPM security chip. The specifications of the TPM are defined by the TCG. BitLocker interacts with the TPM to provide enhanced protection for your hardware.

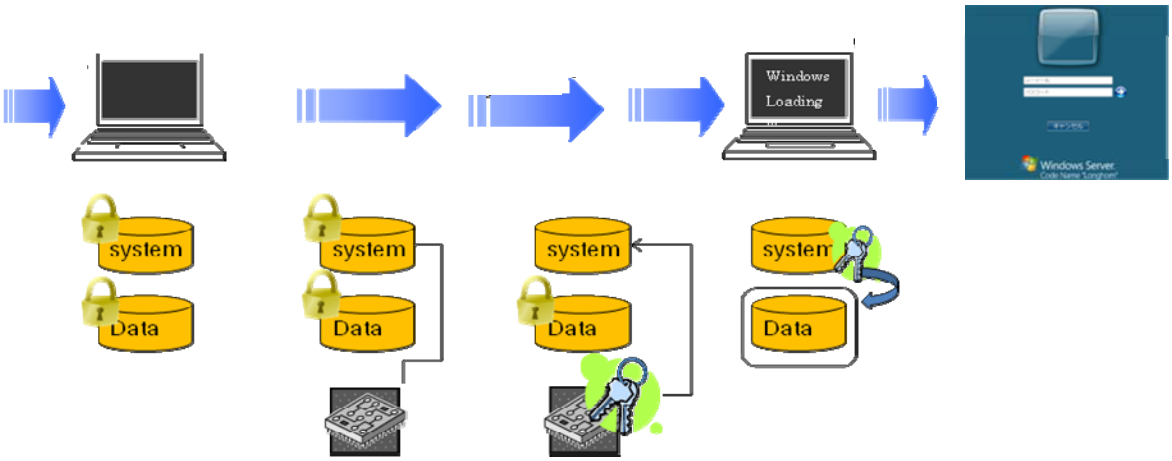


*2: For more information about Fujitsu hardware that has a compatible TPM security chip

>>http://www.fujitsu.com/global/services/computing/server/ia/global/services/computing/server/ia/driver/w2k8

*3: BitLocker encryption

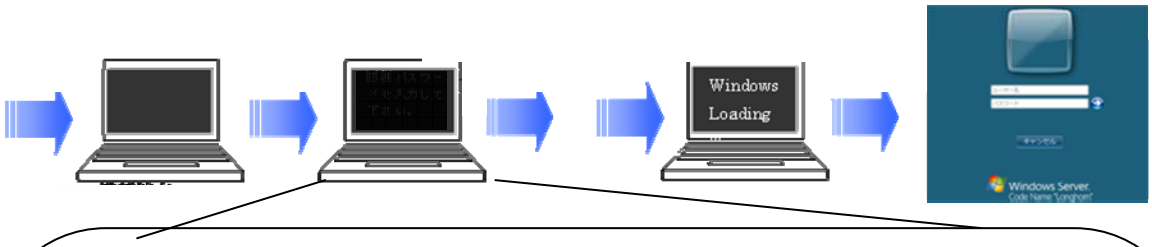
BitLocker encrypts volumes. At system startup, BitLocker compares the current boot environment with that of the last time to verify the integrity of the system configuration. Only if those environments match, the system volume will be decoded and your OS will boot by using the stored key in the TPM.



1 Recovery mode

At system startup, a BitLocker-enabled system interacts with the TPM to verify the integrity of the system. When you startup the system after hardware maintenance work or system expansion, any changes made will be detected and the system will enter recovery mode. In that case, you are required to type your recovery password to startup the system.

■ Detect changes in the hardware configuration, and enter recovery mode

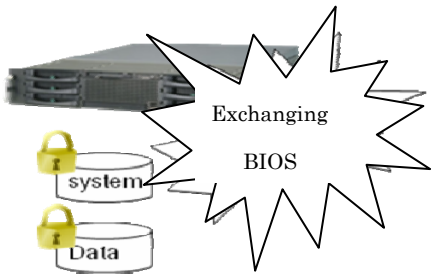


[Recovery mode]

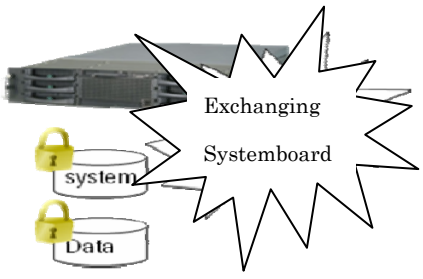
At system startup, you are prompted to type your recovery password.

* Examples of hardware configuration changes that will result in recovery mode

Example 1. Updating system BIOS



Example 2. Replacing a baseboard



2 Changes in hardware configurations

The table below shows examples of system configuration changes. Based on the table, you can clarify what kind of configuration changes will make your system enter recovery mode. [**Yes**] in the table indicates that the system will enter recovery mode after the change. Fujitsu highly recommends that you turn off BitLocker prior to hardware maintenance work and re-enable BitLocker after the completion of maintenance work. (Disabling BitLocker can prevent your system from entering recovery mode). The procedure for turning off BitLocker will be described later in this document.

Table 1. Examples of hardware configuration changes

	Baseboard	CPU	Memory	RAID *6	SAS HBA	SCSI	NIC	Fibre channel	Backup device	FDD	ODD
Upgrading BIOS version/ extension BIOS version	Yes	N/A	N/A	N/A	Yes	Yes	N/A	Yes	N/A	N/A	N/A
Updating Firmware version	-	N/A	N/A	Yes *7	-	-	N/A	-	N/A	N/A	N/A
Changing BIOS settings/ extension BIOS settings	Yes *1	N/A	N/A	-	-	-	N/A	-	N/A	N/A	N/A
Changing Firmware settings	Yes	N/A	N/A	-	-	-	N/A	N/A	N/A	N/A	N/A
Replacement (Without changing the BIOS version/ Firmware version)	Yes	- *2	- *2	-	-	-	-	-	-	-	-
New addition	-	-	-	Yes	Yes	Yes	Yes *4	Yes	-	-	-
Expansion	N/A	-	-	Yes *4	Yes	Yes	Yes *4	Yes	N/A	N/A	N/A
Removing HW	N/A	- *3	- *3	Yes	Yes	Yes	Yes *4	Yes	-	-	Yes *5
Changing a driver	-	N/A	N/A	-	-	-	-	-	N/A	N/A	N/A

[**Yes**]: Your system will enter recovery mode, [**-**]: Not affected, [**N/A**]: Not applicable

* The results above were verified by using the PCR 0,1,2,3,4,5,8,9,10,11.

<Note>

*1: When changes are made to (1) Boot order, (2) Expansion ROM scan on a PCI slot or (3) BIOS password/ System password, the system will enter recovery mode.

*2: Your system will not enter recovery mode with changes in stepping versions or vendors.

*3: A degenerate operation will not make your computer enter recovery mode.

*4: Your computer might not be affected instead of entering recovery mode.

*5: Changes in the BIOS settings (boot order) will make your computer enter recovery mode.

- If the priority of ODD is higher than that of HDD, the computer will enter recovery mode.
- Your computer might not be affected instead of entering recovery mode.

*6: Changes in a RAID configuration (when adding an array configuration) might make your computer enter recovery mode.

If you create a logical drive under a card that originally has array configurations, your computer will not be affected. However, if you create a logical drive under an additionally installed card, your computer might enter recovery mode.

*7: When you change the Firmware version, your computer will or will not be affected, depending on the combination of Firmware versions.

Acronyms in text (Acronym expansion)

The following acronyms are used in the above table.

・SAS HBA (Serial Attached SCSI, Host Bus Adapter)
A device for connecting computers with other network or storage devices that uses a point-point serial protocol.

・Fibre Channel
An interface protocol for connecting computers with other peripherals.

・NIC (Network Interface Card)

・FDD (Floppy Disk Device)

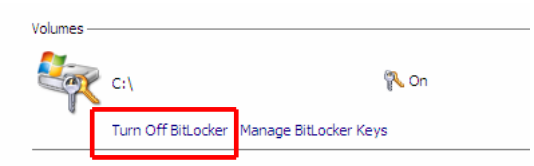
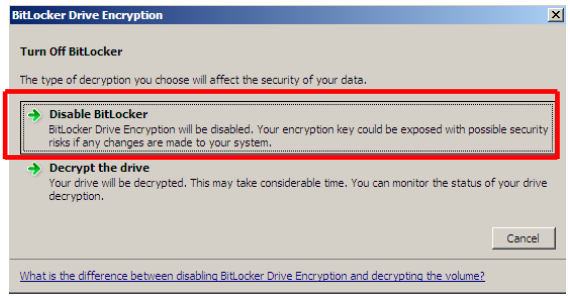
・ODD (Optical Disk Device)

・PCR (Platform Configuration Register)
Space that stores hash values in a TPM

3 Prior to hardware maintenance work

This chapter provides the procedures to turn off BitLocker before beginning hardware maintenance work or system expansion. If you are unable to boot your OS, you cannot turn off BitLocker in advance. In that case, you will be prompted to type your recovery password after the completion of maintenance work or system expansion.
<Caution> If you lose the recovery password, you will be required to re-install the system.

3.1 To turn off BitLocker Drive Encryption

1	Click [**Start**] > [**Control Panel**]> [**Security**] > [**BitLocker Drive Encryption**], and the BitLocker Drive Encryption page will appear.	
2	Click the [**Turn Off BitLocker Drive Encryption**] menu on the system volume (labeled C).	
3	In the BitLocker Drive Encryption dialog box, click [**Disable BitLocker Drive Encryption**].	

<Note>

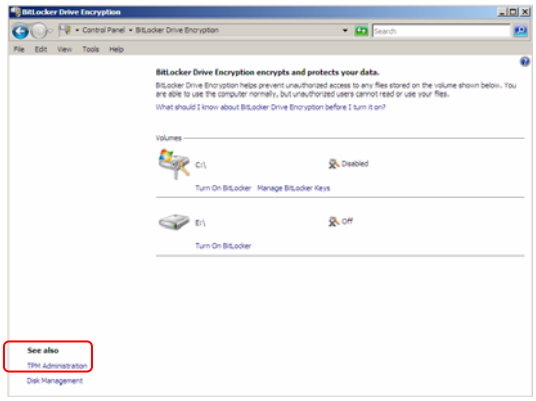
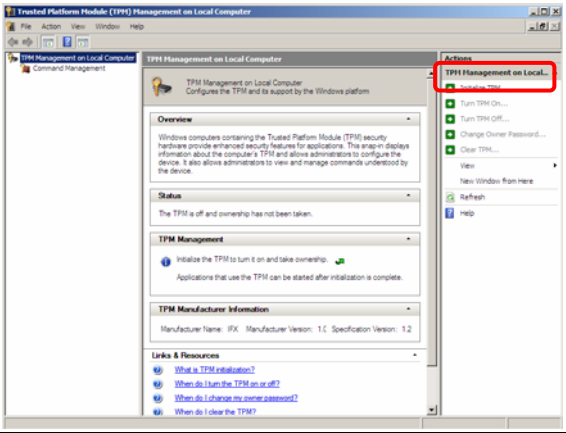
・Your system will enter recovery mode only if [**BitLocker is enabled**] on the system volume. Turning off BiLocker for the data volume is not required.

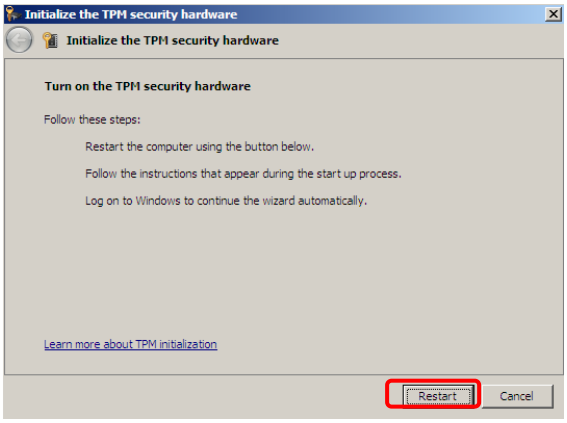
You can only choose [**Decrypt the volume**] for the data volume.
If you decrypt the volume, re-encryption of the volume or obtaining a recovery password again will be required.

4 Recovery procedures after maintenance work

This chapter describes how to recover the BitLocker Drive Encryption after conducting hardware maintenance work. Special procedures are required only if you need to replace a baseboard on your computer, because replacing the baseboard will clear password information of the TPM. You are required to newly set ownership of the TPM after you replaced the baseboard.

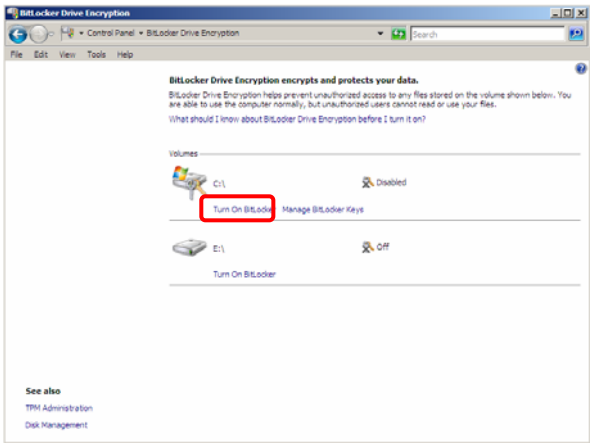
4.1 Replacing a baseboard

1	Start your computer. As BitLocker is turned off, the system will startup instead of entering recovery mode.	
2	Click [**Start**] > [**Control Panel**] > [**Security**] > [**BitLocker Drive Encryption**], and the [**BitLocker Drive Encryption**] page will appear.	
3	Click [**TPM Administration**, located in the lower left of the screen. The [**Trusted Platform Module (TPM) Management on Local Computer**] page will appear.	
4	In the right pane, click [**Initialize TPM**.	

5	In the [**Initialize the TPM security hardware**] dialog box, click [**Shutdown**] to shut down your system.	
6	After shutting down your computer, turn on the computer again to continue the procedures.	
7	After your computer restarts, on the BIOS screen, you will be asked whether to continue the TPM initialization process. Select [**Execute**].	
8	After logging on to Windows, the [**Initialize the TPM security hardware**] dialog box will be displayed again.	
9	Select [**Automatically create the password**], and save the TPM owner password.	
	<Note> ・BitLocker Drive Encryption automatically performs the initialization process. When you first enable BitLocker Drive Encryption, the TPM owner password will be automatically created and stored on the same location as your recovery password. ・Only the TPM owner password will be updated, and your recovery password will not be updated.	
10	Click [**Start**] > [**Control Panel**] > [**Security**] > [**BitLocker Drive Encryption**], and the [**BitLocker Drive Encryption**] page will appear.	
11	Click [**Turn On BitLocker**] on the system volume (C) to re-enable the drive encryption.	

12	The [**BitLocker Drive Encryption Platform Check**] dialog box will be displayed, and then click [**Continue with BitLocker Drive Encryption**].	

4.2 Others (Adding PCI slots, changing the BIOS boot order)

1	Click [**Start**] > [**Control Panel**] > [**Security**] > [**BitLocker Drive Encryption**], and the [**BitLocker Drive Encryption**] page will appear.	
2	Click [**Turn On BitLocker**] on the system volume (C) to re-enable the drive encryption.	
3	The [**BitLocker Drive Encryption Platform Check**] dialog box will be displayed, and then click [**Continue with BitLocker Drive Encryption**].	

5 [Appendix 1] How to deploy BitLocker on PRIMERGY

1 Make sure that your computer is equipped with a compatible TPM.
>>http://www.fujitsu.com/global/services/computing/server/ia/global/services/computing/server/ia/driver/w2k8

2 Turn on your computer and set BIOS.
   1 Turn on the server.
   2 During POST, you will see the [**<F2> BIOS Setup/ <F12> Boot Menu**] message on the screen, and then press the F2 key while the message is being displayed.
   3 The [**TPM (Security Chip) Settings**] submenu will be displayed under the [**Security**] menu.
   4 Select the [**Enabled**] option under [**Security Chip**], and then [**Change TPM State**] will be displayed.
   5 Select the [**Enable & Activate**] setting under [**Change TPM State**].
   6 The [**Exit**] menu will appear.
   7 Move your mouse cursor to [**Save Changes & Exit**] and press the [**Enter**] key.
   8 You will see the [**Save configuration changes and exit now?**] message, and then point your mouse cursor to [**Yes**] and press the [**Enter**] key.
   9 After re-booting, the BIOS setup utility will automatically start.
   10 From the [**Physical Presence operations**] menu, select [**Execute**].

3 Prepare partitions required for BitLocker.
   1 Boot your computer from the installation disk.
   Select [**Repair your computer**] on the OS installation page.

   If you use an array model, install a device driver for an array controller as needed.
   For more information, refer to the [Installation procedures] document for Windows Server 2008 (available only in Japanese).
   >> http://www.fujitsu.com/global/services/computing/server/ia/driver/w2k8

   3 Click [**Next**] on the [**System Recovery Options**] menu. (Do not select [**OS**].)
   4 Click [**Command Prompt**].
   5 Type the following series of commands.
      1 diskpart
      2 select disk 0
      3 Clean

4 create partition primary size = 1500
5 assign letter = S
6 Active
7 create partition primary size = 20000
8 assign letter = C
9 Exit
10 format C: /y /q /fs:NTFS
11 format S: /y /q /fs:NTFS
12 Exit

The procedures above lets you create new two partitions:

Two partitions required for BitLocker	
Primary partition	S drive (NTFS), 1.5GB, set as the active partition A boot loader will be located on this partition.
Secondary Partition	C drive (NTFS), 20GB

* You may be required to create an additional partition or change the size, depending on your server usage or disk capacity.

6 Click the close window icon in the upper right of your screen to close the window. (Do not shut down or restart your computer.)

7 Select [**Install now**] to continue the installation process.

8 Install the Windows operating system on the larger partition (C drive, 20GB).

4 Afer the completion of OS installation, activate BitLocker.

1 Start Server Manager.

[**All Programs**] > [**Administrative Tools**] > [**Server Manager**] to startup Server Manager.

2 Activate the BitLocker function.

Click [**Features**] in the left pane of Server Manager, and then click [**BitLocker Drive Encryption**] > [**Install BitLocker**] under **Add Features**.

3 Restart your system.

Your computer will restart and will become BitLocker-compartible.

5 Turn on BitLocker to encrypt your disks.

1 Double-click [**Control Panel**] > [**Security**] > [**BitLocker Drive Encryption**], and the **BitLocker Drive Encryption** page will appear.

2 When you are about to encrypt the system volume, click [**Turn On BitLocker**] on the system volume.

3 Save your recovery password on the [**Save the Recovery Password**] page (Using several options is highly advised to preserve the recovery password), and then click [**Next**].

4 When you are about to encrypt the data volume, click [**Turn On BitLocker**] on the data volume.

5 Save your recovery password on the [**Save the Recovery Password**] page (Using several options is highly advised to preserve the recovery password), and then click [**Next**].

<Note>

・When BitLocker is first enabled, initializing the encryption process will be performed. The initialization process might take some time to complete, depending on your disk capacity or frequency of use (It might take approximately 10 minutes to encrypt a 10GB of empty partition).

・You can encrypt several drives concurrently.

・If you terminate the process of turning on/off BitLocker, BitLocker will remain disabled.

6 [Appendix 2] How to clear the TPM

The procedures below describe how to clear and reset the TPM to factory defaults. Clearing the TPM should not be performed during the BitLocker encryption feature is enabled.

1 Turn on your server.

2 During POST, you will see the [**<F2> BIOS Setup/ <F12> Boot Menu**] message on the screen, and then press the F2 key while the message is being displayed.

3 The [**TPM (Security Chip) Settings**] submenu will be displayed under the [**Security**] menu.
If the **Current TPM Status** indicates anything other than [**Enabled & Activated**], you cannot clear and reset the TPM. Try again after you activate the TPM.

4 Select [**Clear**] setting under [**Change TPM State**].

5 The [**Exit**] menu will be displayed.

6 Move your mouse cursor to [**Save Changes & Exit**] and press the [**Enter**] key.

7 You will see the [**Save configuration changes and exit now?**] message, and then point your mouse cursor to [**Yes**] and press the [**Enter**] key.

8 After re-booting, the BIOS setup utility will automatically start.

9 From the [**Physical Presence operations**] menu, select [**Execute**].
The TPM will be cleared and your computer will restart.

7 [Appendix 3] Prior to hardware maintenance work (For a system installing the Server Core installation)

7.1 To turn off BitLocker Drive Encryption

1 At an administrator command prompt, execute the following command and verify the status.

cscript manage-bde.wsf –status

Verify that you will see the following page being displayed.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C:[]
[OS Volume]
Size: xx.xxGB
Conversion Status:
Percentage Encrypted: 100%
Encryption Method: AES 128 with Diffuser
Protection Status: Protection On
Lock Status: Unlocked
Key Protectors:
External Key
Numerical Password
TPM

When the **Protection Status** is [**Protection On**], it indicates that BitLocker is enabled.

2 Perform the following command to turn off BitLocker.

cscript manage-bde.wsf –protectors –disable C:

8 [Appendix 4] Recovery procedures after maintenance work (For a system installing the Server Core installation)

8.1 Replacing a baseboard

1 At an administrator command prompt, execute the following command to enable the TPM.

cscript manage-bde.wsf –tpm -TurnOn

You will see the following page being displayed. Follow the instructions on your screen.

This computer requires you to follow these steps to turn on the TPM:

1. Restart the computer.

(Type “shutdown /?” for command line instructions.)

2. Follow the instructions at the prompt in the boot screen

---

2 Execute the following command, and shut down the system.

shutdown /s /t 0

3 After your computer restarts, on the BIOS screen, you will be asked whether to continue the TPM initialization process. Select [**Execute**].

4 After logging on the Windows, at an administrator command prompt, excute the following command to set your TPM password and set ownership of the TPM.

cscript manage-bde.wsf –tpm –TakeOwnerShip XXXXX

For [**XXXX**], type your password that has more than 8 digits.

A system that installs the Server Core feature doesn’t have the optional function to automatically create the TPM owner password. You will be prompted to type your password.

5 Execute the following command to enable BitLocker (*When you replace components other than a baseboard, you are only required to perform this process).

cscript manage-bde.wsf –protectors –enable C:

For technical information on the Fujitsu PRIMERGY servers, see the followings:

・PRIMERGY industry-standard server
http://www.fujitsu.com/global/services/computing/server/ia/

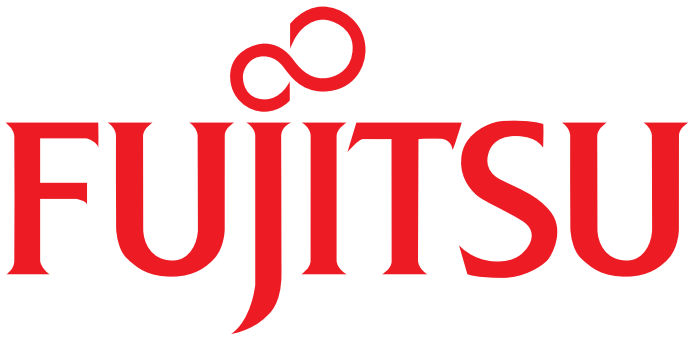
・Comparison of PRIMERGY machine types
http://www.fujitsu.com/global/services/computing/server/ia/towerserver/

Contact Fujitsu

・Support and contact for PRIMERGY

http://www.fujitsu.com/global/contact/computing/PRMRGY_index.html

This document was created based on information as of the published date. To obtain the latest information about the PRIMERGY products, please visit our website. Fujitsu assumes no responsibility for any damge or trouble caused by the use of this documents.



THE POSSIBILITIES ARE INFINITE