Microsoft

Secured-core Servers

有効化ガイド

FUJITSU Server PRIMERGY

第 1.0 版

2022 年 3 月

FUJITSU

目次

1. 概要

本書は、Secured-core server AQ を取得している製品において、secured-core 機能を有効化する手順を記載しています。

2. 対象製品

本書は以下の要件を満たした製品を対象としています。

2.1. ソフトウェア要件

- Windows Server 2022 Datacenter または Windows Server 2022 Standard

2.2. ハードウェア要件

- Secured-core server AQ を取得している製品
- 最新版の BIOS
- 対象 OS にて使用可能な TPM2.0

Secured-core server AQ を取得している製品を確認するには以下を参照して下さい。

https://www.windowsservercatalog.com/

BIOS は以下から最新版を適用できます。

https://jp.fujitsu.com/platform/server/primergy/bios/

使用可能な TPM2.0 については以下を参照してください。

https://jp.fujitsu.com/platform/server/primergy/system/

3. UEFI 設定

BIOS セットアップユーティリティから、下表のように設定します。

表 3-1 BIOS セットアップユーティリティの設定項目と設定値

設定項目の箇所	設定項目	設定値
Security > Secure Boot Configuration	Current Secure Boot State	Enabled
Configuration > Security Configuration	TPM Support	Enabled
Configuration > CPU Configuration	Intel Virtualization Technology	Enabled
Configuration > CPU Configuration	Intel (R) VT-d	Enabled
Configuration > CPU Configuration	Intel TXT Support	Enabled

設定可能な項目、設定画面の表記、既定値は機種や BIOS 版数等により異なる場合があります。

BIOS 設定に関する詳細は、以下から該当機種のマニュアルを参照してください。

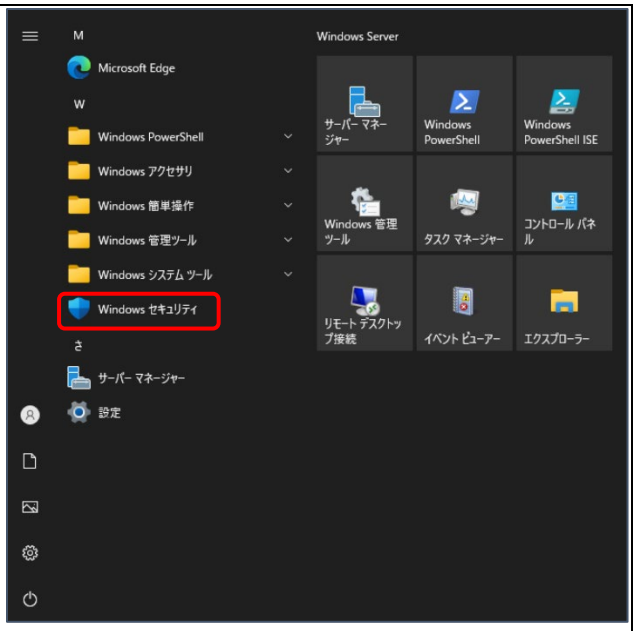
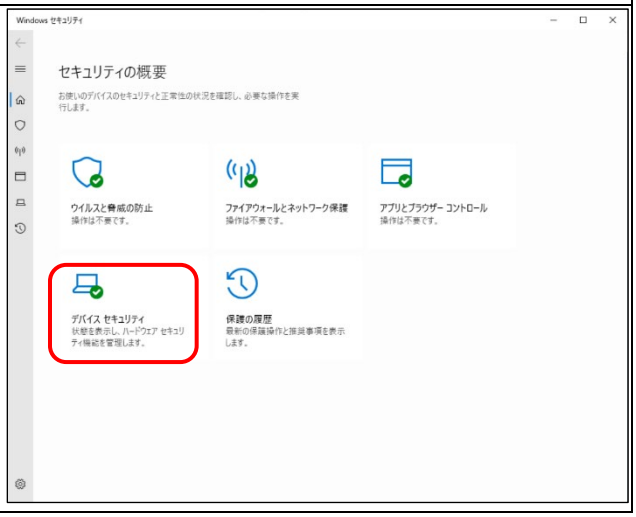
https://www.fujitsu.com/jp/products/computing/servers/primergy/manual/

4. OS 設定

OS で Secured-core 機能を設定するためには 2 通りの手順があります。

仮想化ベースのセキュリティ、ハイパーバイザーによるコードの整合性の強制、システムガードを有効にするために以下 2 つのうち 1 つの手順に従ってください。

4.1. Windows セキュリティアプリでの設定 (デスクトップエクスペリエンスのみ)

1	スタートメニューから「 Windows セキュリティ」アプリを起動します。	
2	「デバイスセキュリティ」を選択します。	

3	「コア分離の詳細」をクリックします。	
4	「メモリ整合性」と「ファームウェアの保護」を“オン”にして、再起動します。	

4.2.レジストリキーでの設定

または、下記のレジストリキー設定をすることで 4.1 と同じ結果を得ることもできます。

- reg add "HKLM¥SYSTEM¥CurrentControlSet¥Control¥DeviceGuard¥Scenarios¥HypervisorEnforcedCodeIntegrity" /v "Enabled" /t REG_DWORD /d 1 /f
- reg add "HKLM¥SYSTEM¥CurrentControlSet¥Control¥DeviceGuard¥Scenarios¥HypervisorEnforcedCodeIntegrity" /v "WasEnabledBy" /t REG_DWORD /d 0 /f
- reg add "HKLM¥SYSTEM¥CurrentControlSet¥Control¥DeviceGuard¥Scenarios¥SystemGuard" /v "Enabled" /t REG_DWORD /d 1 /f

5. Secured-core 状態の確認

すべての Secured-Core 機能が正しく設定され、有効化されていることを確認するためには次の手順に従って下さい。

5.1.TPM 2.0

PowerShell で Get-Tpm を実行して、下図と同じ表記になっていることを確認してください。

図 5-1　Get-Tpm の実行結果

5.2.セキュアブート、カーネル DMA 保護、仮想化ベースのセキュリティ、ハイパーバイザーによるコードの整合性の強制、システムガード

MSinfo32 を起動して、該当項目が下表の設定値になっている、もしくは下表の設定値を含んでいるか確認してください。

表 5-1 Msinfo32 で確認する項目とその設定値

項目	設定値
セキュアブートの状態	有効
カーネル DMA 保護	有効
仮想化ベースのセキュリティ	実行中
仮想化ベースのセキュリティの実行中サービス	ハイパーバイザーによるコードの整合性の強制、セキュア起動

図 5-2 Secured-core 機能有効時の Msinfo32 の表記