


# Secured-core Servers

## 有効化ガイド

FUJITSU Server PRIMERGY

第 1.1 版

2023 年 4 月

 FUJITSU

# 目次

---

1	概要 .....	3
2	対象製品 .....	3
2.1	ソフトウェア要件 .....	3
2.2	ハードウェア要件 .....	3
3	UEFI 設定 .....	4
4	OS 設定 .....	4
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) .....	4
4.2	レジストリキーでの設定 .....	6
5	Secured-core 状態の確認 .....	6
5.1	TPM 2.0 .....	6
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 .....	7
5.3	Windows Admin Center を使用した確認 .....	7

# 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

以下いずれかの OS を対象とします。

- Windows Server 2022 Datacenter
- Windows Server 2022 Standard
- Windows Server 2022 Essentials

### 2.2 ハードウェア要件

以下すべての要件を満たしたハードウェアを対象とします。

- 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 TPM 2.0

Secured-core server AQ を取得している製品を確認するには、以下を参照してください。

<https://www.windowsservercatalog.com/>

BIOS は、以下から最新版を適用してください。

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

使用可能な TPM 2.0 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、以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 URL から該当機種のマニュアルを参照してください。

<https://support.ts.fujitsu.com/IndexDownload.asp?lng=jp>

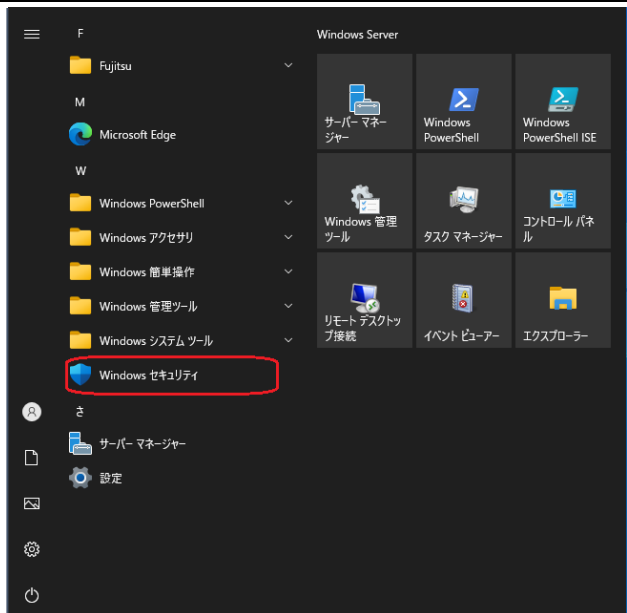
※BIOS 設定に関するマニュアル選択例：

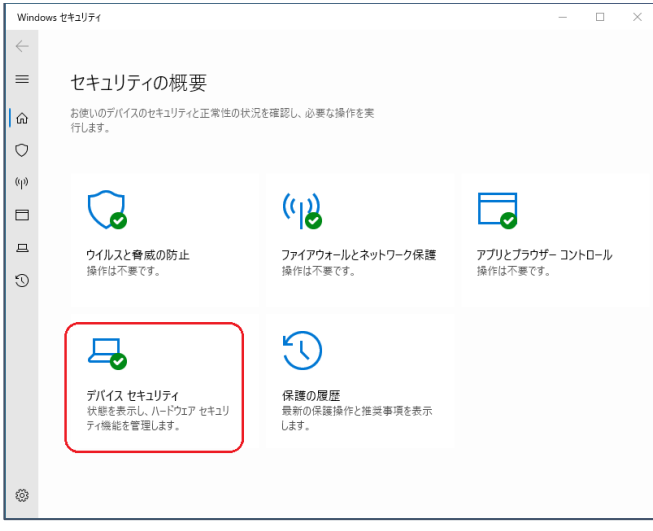


カテゴリから探す > PRIMERGY 該当機種を選択 > OS 一覧から選択 > ドキュメントのタブを選択 > Systemboard

## 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、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)

Windows セキュリティアプリでの設定	
1	<div>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。</div> <div></div>

2	[デバイスセキュリティ]を選択します。	 <p>Windows セキュリティ</p> <p>セキュリティの概要</p> <p>お使いのデバイスのセキュリティと正常性の状況を確認し、必要な操作を実行します。</p> <p>ウイルスと脅威の防止 操作は不要です。</p> <p>ファイアウォールとネットワーク保護 操作は不要です。</p> <p>アプリとブラウザー コントロール 操作は不要です。</p> <p><b>デバイス セキュリティ</b> 状態を表示し、ハードウェア セキュリティ機能を管理します。</p> <p>保護の履歴 最新の保護操作と推奨事項を表示します。</p>
3	[コア分離の詳細]をクリックします。	 <p>Windows セキュリティ</p> <p>デバイス セキュリティ</p> <p>お使いのデバイスに組み込まれているセキュリティです。</p> <p><b>コア分離</b> 仮想化ベースのセキュリティにより、お使いのデバイスの中核部分が保護されます。 <b>コア分離の詳細</b></p> <p><b>セキュリティ プロセッサ</b> トラステッド プラットフォーム モジュール (TPM) と呼ばれるセキュリティ プロセッサにより、お使いのデバイスに追加の暗号化が提供されています。 <a href="#">セキュリティ プロセッサの詳細</a></p> <p>標準ハードウェアセキュリティはサポートされていません。 <a href="#">詳細情報</a></p> <p>Windows コミュニティのビデオ <a href="#">デバイス セキュリティの詳細</a></p>
4	[メモリ整合性]と[ファームウェアの保護]を“オン”にして、OS を再起動します。	 <p>Windows セキュリティ</p> <p><b>コア分離</b></p> <p>お使いのデバイスで使用可能な、仮想化ベースのセキュリティを使用するセキュリティ機能です。</p> <p><b>メモリ整合性</b> 攻撃によって悪意のあるコードが高セキュリティ プロセッサに挿入されるのを防ぎます。 <b>オン</b> <a href="#">詳細情報</a></p> <p><b>メモリ アクセス保護</b> 悪意のある外部デバイスによる攻撃からデバイスのメモリを保護します。 <a href="#">詳細情報</a></p> <p><b>ファームウェアの保護</b> Microsoft Defender System Guard は、危害を受けたファームウェアからデバイスを保護します。 <b>オン</b> <a href="#">詳細情報</a></p> <p>プライバシーの設定を変更する Windows 10 デバイスのプライバシー設定を表示および変更します。 <a href="#">プライバシーの設定</a> <a href="#">プライバシー デッシュボード</a> <a href="#">プライバシーに関する声明</a></p>

## 4.2 レジストリキーでの設定

または、下記レジストリキーを設定することで、4.1と同じ結果を得ることができます。

```
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

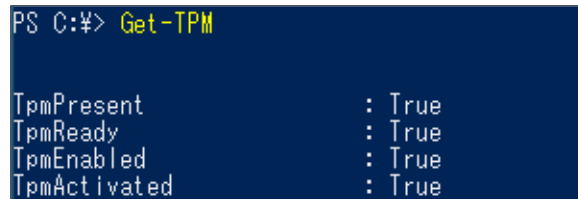
---

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、次の手順に従ってください。

### 5.1 TPM 2.0

PowerShell で Get-TPM を実行して、以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



```
PS C:\> Get-TPM

TpmPresent      : True
TpmReady        : True
TpmEnabled      : True
TpmActivated    : True
```

## 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、該当項目が以下表の設定値になっている、もしくは以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 表記

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必須セキュリティ プロパティ	
仮想化ベースのセキュリティの利用可能なセキュリティ プロパティ	仮想化の基本サポート、セキュアブート、DMA 保護、セキュリティで保護されたメモリ上書き、
仮想化ベースのセキュリティの構成済みサービス	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
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

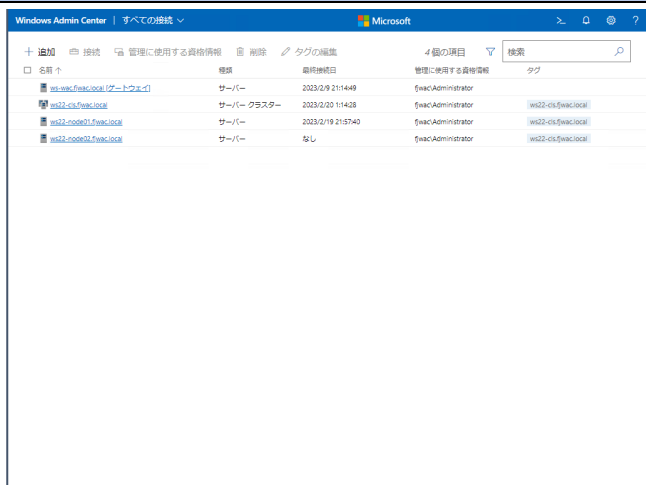
## 5.3 Windows Admin Center を使用した確認

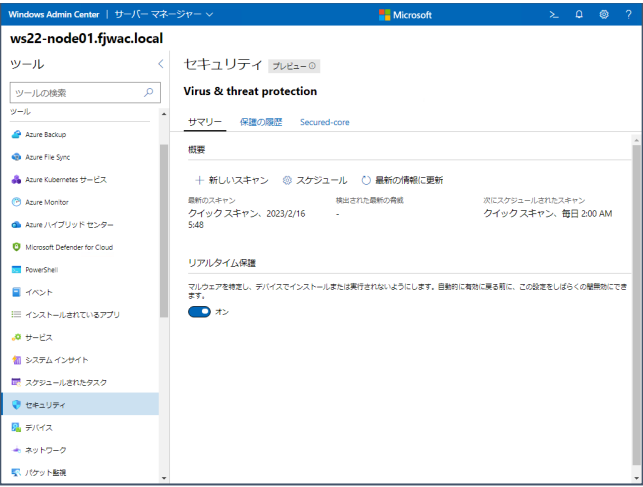
Windows Admin Center を使用して Secured-Core Server が有効化されているかを確認します。Windows Admin Center についての詳細は、以下 URL を参照してください。

<https://www.microsoft.com/ja-jp/windows-server/windows-admin-center>

### Windows Admin Center を使用した確認

- Windows Admin Center を実行すると[すべての接続]画面が表示されます。  
対象のサーバーを選択し[接続]をクリックします。



<p>2</p>	<p>左ペインから[セキュリティ]を選択します。</p> <p>[サマリー]タブは、以下の操作/設定が可能です。</p> <ul style="list-style-type: none"> <li>● 新しいスキャン (クイック/フル)</li> <li>● スケジュール</li> <li>● 最新の情報に更新(画面の更新)</li> <li>● リアルタイム保護</li> </ul>	
<p>3</p>	<p>[Secured-core]タブは、Secured-core server の確認とセキュリティ機能の有効化を設定します。</p> <p>以下セキュリティ機能の状態を確認します。すべての状態が[オン]と表示されることで Secured-core server が有効化されたと確認できます。</p> <ul style="list-style-type: none"> <li>● ハイパーバイザー強制のコード整合性(HVCI)</li> <li>● DMA 保護の起動</li> <li>● System Guard</li> <li>● セキュアブート</li> <li>● 仮想化ベースのセキュリティ(VBS)</li> <li>● トラストッドプラットフォームモジュール 2.0 (TPM2.0)</li> </ul> <p>[サポートされていません]と表示された場合は、物理ハードや BIOS 設定などが対応していない状況を示します。</p> <p>[未構成]と表示された場合は、BIOS や OS で設定されていない状況です。</p> <p>※"ハイパーバイザー強制のコード整合性(HVCI)"/"System Guard"/"仮想化ベースのセキュリティ(VBS)"に関しては、チェックして[有効にする]をクリックすることで、Windows Admin Center から有効化することができます。</p>	