Microsoft

Express５８００シリーズ

Secured-core Servers

有効化ガイド

2022 年 4 月

目次

1 概要

本ガイドは、Secured-core Server 追加要件を取得済みのサーバー製品において、その機能を有効化する手順を記載しています。

2 対象製品

本ガイドの対象サーバー製品については、以下を参照してください。
https://www.support.nec.co.jp/View.aspx?id=3140108402

3 UEFI 設定

システムユーティリティ*から、以下の"**Microsoft(R) Secured-core Support**"オプションを「**Enabled**」に設定します。

System Utilities ＞ System Configuration > BIOS/Platform Configuration (RBSU) > Server Security
Microsoft(R) Secured-core Support = **[Enabled]** (default: Disabled)

*システムユーティリティについては、当該サーバー製品のユーザーズガイドを参照してください。
ユーザーズガイドは、以下からダウンロードできます。

https://www.support.nec.co.jp/
(「NEC サポートポータル内検索」より、当該サーバー製品の「モデル名」で検索)

4 OS 設定

4.1 仮想化ベースのセキュリティ(VBS)、ハイパーバイザーで保護されているコード整合性 (HVCI)、システムガードの有効化手順

Windows Server 2022 で Secured-core Server の機能を利用するためには、仮想化ベースのセキュリティ(VBS)、ハイパーバイザーで保護されているコード整合性 (HVCI)、システムガードの有効化が必要です。

4.1.1 レジストリキーによる設定手順

コマンドプロンプトを管理者として実行し、以下のコマンドでレジストリキーを設定してください。
レジストリキー設定完了後、OS を再起動することで設定が反映されます。

```
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 動作状況の確認

全ての Secured-core 機能が正しく有効化され、機能していることは以下の手順で確認できます。

5.1 TPM 2.0

5.1.1 イベントログの確認

システムイベントログに以下のイベント(イベント ID、ソース、Error code)が**記録されていないこと**を確認してください。

ID：**124**
ソース：**Kernel-Boot**
レベル：エラー

仮想化ベースのセキュリティ有効化ポリシー チェックがフェーズ 7 で失敗しました。
状態: Unknown NTSTATUS Error code: **0xc028014b**

システムイベントログに上記のイベントが記録されている場合は、TPM の NV 領域が不足しているため、TPM をクリアする必要があります。TPM クリアの手順は Microsoft 社の以下のページの手順に従って実施してください。
https://docs.microsoft.com/archive/blogs/askcorejp/tpmclear

5.1.2 TPM 動作の確認

PowerShell を起動し、"Get-Tpm"コマンドを実行し以下の通りになっていることを確認してください。

```
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(VBS)、ハイパーバイザーで保護されているコード整合性 (HVCI)、システムガード

コマンドプロンプトを起動し、"msinfo32"コマンドを実行し以下の項目の設定値を確認します。

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のサービス	"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"

"msinfo32"コマンドでの該当箇所表示例

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
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