信頼できるプラットフォーム(Trusted Platform)

信頼できるプラットフォーム(Trusted Platform)

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できるトラステッドプラットフォーム BIOS 設定の一覧を示します。

名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
Multikey Total Memory Encryption (MK-TME)	MK-TME を使用すると、独自のキーを持つ 1 つの暗号化ドメインを複数持つことができます。異なるメモリページを異なるキーで暗号化できます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	
[拡張ソフトウェア保護機能（SGX）（Software Guard Extensions (SGX)）]	拡張ソフトウェア保護機能（SGX）を有効にすることができます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	
Total Memory Encryption(TME)	システムの物理メモリ全体を暗号化する機能を提供します。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	Platform Default	

名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
[所有者 EPOCH 入力タイプを選択（Select Owner EPOCH Input Type）]	作成され、ロックされたメモリ領域に使用されるセキュリティ キーのシードを変更できます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	SGX 所有者 EPOCH がアクティブ化されました。新しいランダム所有者 EPOCH に変更します。**手動でユーザー定義の所有者 EPOCH** を作成します。	
SGX自動MP登録エージェント	レジストレーション エージェント サービスがプラットフォーム キーを保存できるようにします。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	
[SGX Epoch 0]	0 で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	
[SGX Epoch 1]	1 で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	
SGX初期設定へのリセット	その後の起動時にシステムがSGXの工場出荷時リセットを実行できるようにします。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	

名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
[SGX PubKey Hash *n*] *n* の範囲は 0 ～ 3 です。	ソフトウェア ガード拡張（SGX）の値を設定できます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**SGX PUBKEY HASH0**、SGX PUBKEY HASH1、SGX PUBKEY HASH2、SGX PUBKEY HASH3 • SGX PUBKEY HASH0 — 7 ～ 0 の間 • SGX PUBKEY HASH1 : 15 ～ 8 の間 • SGX PUBKEY HASH2 : 23 ～ 16 の間 • SGX PUBKEY HASH3 : 31 ～ 24 の間	
SGX書き込みが有効	SGX 書き込み機能を有効にすることができます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	

信頼できるプラットフォーム(Trusted Platform)

名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
[SGX パッケージ情報インバンド アクセス（SGX Package Information In-Band Access）]	SGX パッケージ情報インバンドアクセスを有効にすることができます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	有効、**無効**	
SGX QoS	SGX QoS を有効にすることができます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	
SHA-1 PCRバンク	プラットフォーム構成レジスタ（PCR）は、TPM内のメモリ位置です。複数のPCRをまとめてPCRバンクと呼びます。セキュア ハッシュ アルゴリズム1またはSHA-1 PCRバンクでは、TPMセキュリティを有効または無効にすることができます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	セキュリティ デバイス サポートが無効になっている場合、TPM操作全体が失敗します。
SHA256 PCRバンク	プラットフォーム構成レジスタ（PCR）は、TPM内のメモリ位置です。複数のPCRをまとめてPCRバンクと呼びます。セキュア ハッシュ アルゴリズム256ビットまたはSHA-256 PCRバンクでは、TPMセキュリティを有効または無効にすることができます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	セキュリティ デバイス サポートが無効になっている場合、TPM操作全体が失敗します。

名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
[信頼されたプラットフォームモジュールの状態（Trusted Platform Module State）]	サーバーの認証に使用するアーティファクトを安全に保存するコンポーネントであるトラステッド プラットフォーム モジュール（TPM）の有効と無効を切り替えます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	セキュリティ デバイス サポートが無効になっている場合、TPM 操作全体が失敗します。
TPM保留中の操作	トラステッド プラットフォーム モジュール（TPM）Pending Operation オプションを使用すると、保留中の操作のステータスを制御できます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**なし**、TpmClear	セキュリティ デバイス サポートが無効になっている場合、TPM 操作全体が失敗します。
[TPM の最小限の物理的存在（TPM Minimal Physical Presence）]	TPM の最小限の物理的存在を有効または無効にするかどうか。セキュリティを損なうことなく TPM を管理するために、OS と BIOS 間の通信を有効または無効にします。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	有効、**無効**	セキュリティ デバイス サポートが無効になっている場合、TPM 操作全体が失敗します。

名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
[Intel Trusted Execution Technology のサポート（Intel Trusted Execution Technology Support）]	ビジネス サーバー上で使用され、保管される情報の保護機能を強化する、Intel Trusted Execution Technology（TXT）の有効と無効を切り替えます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	TXT を無効にしない限り、TPM を無効にすることはできません。
セキュリティデバイスのサポート	TPM機能全体を制御します。	4.2(3)	C240M6、C220M6、C225M6、C245M6、B200M6、X210CM6	**有効**、無効	
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）]	このトークンを有効にすると、Windows 2022 カーネル DMA 保護機能が有効になります。OSはこれを、悪意のあるデバイスからのDMA攻撃を防ぐためにIOMMU を有効にする必要があるというヒントとして扱います。	4.2(2)、4.2(3)	C220 M6 および C240 M6、B200 M6、X210C M6	有効、**無効**	

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。