Intersight 管理モードの Cisco USC サーバー BIOS トークン

初版：2022 年 6 月 8 日

最終更新：2023 年 3 月 3 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

通信、サービス、偏向のない言語、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービスリクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

Cisco バグ検索ツール

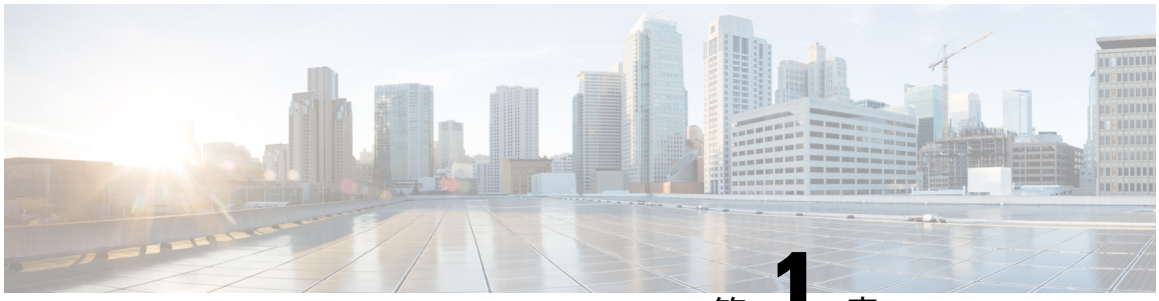
Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアの問題に関する詳細な情報を提供します。

偏向のない言語

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザーインターフェ

通信、サービス、偏向のない言語、およびその他の情報

イスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



第 1 章

Intersight 管理モード サーバー BIOS トークンの導入

Intersight 管理モード サーバー BIOS トークンの導入

Intersight 管理モードでは、Cisco UCS ドメイン内のサーバー上の BIOS 設定をグローバルに変更する方法が2通り用意されています。サーバーまたはサーバーの集合のニーズに合う特定の BIOS 設定グループを含む BIOS ポリシーを 1 つ以上作成するか、特定のサーバー プラットフォームに対するデフォルトの BIOS 設定を使用できます。

BIOS ポリシーおよびサーバー プラットフォームのデフォルトの BIOS 設定のどちらででも、IMM によって管理されるサーバーの BIOS 設定を微調整できます。

データセンターのニーズに応じて、一部のサービス プロファイルについては BIOS ポリシーを構成し、同じ Cisco UCS ドメイン内の他のサービス プロファイルについては BIOS のデフォルトを使用したり、そのいずれかのみを使用したりできます。また、IMM を使用して、サーバーの実際の BIOS 設定を表示し、それらが現在のニーズを満たしているかどうかを確認できます。

Cisco Intersight 管理モードは、次の M5 および M6 サーバーをサポートします。

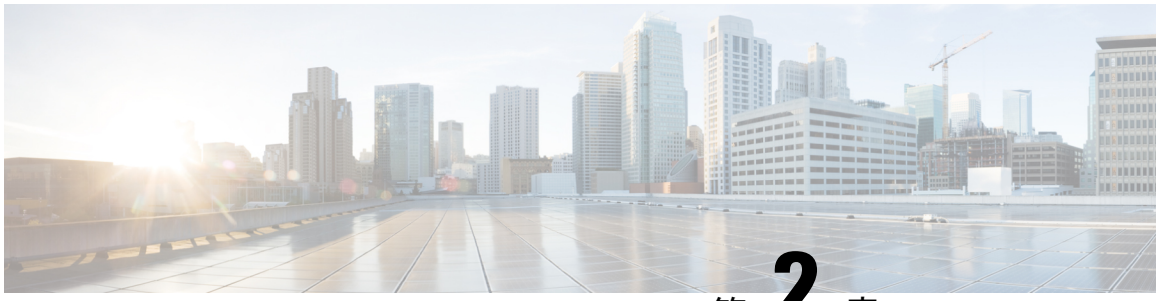
- Cisco UCS C220 M6
- Cisco UCS C225 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C240 SD M5
- Cisco UCS C480 M5

Intersight 管理モード サーバー BIOS トークンの導入

- Cisco UCS B200 M6
- Cisco UCS B200 M5
- Cisco UCS B480 M5
- Cisco UCS X210C M6
- Cisco UCS S3260 M5

（注） 表の **[バージョン（Version）]** 列は、トークンがサポートされている最初の Cisco UCS Manager バージョンと、その連続したバージョンのサポートを示しています。

（注） 値の説明が長いトークンの場合、**[値（Values）]** 列は空白で表示されます。この場合、列を下にスクロールして値を表示できます。



第 2 章

ブート オプションの BIOS 設定

ブート オプションの BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるブート オプションの BIOS 設定を示しています。

（注） すべてのトークンには、「プラットフォームのデフォルト」オプションも含まれています。プラットフォームのデフォルトは、太字の設定によって識別されます。BIOS は、サーバ タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。

ブート オプションの BIOS 設定

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
[試行数（Number of Retries）]	ブートの試行数。	4.1(1)	B200 M5、B480 M5、C480 M5	無制限**13**, 5 • **Infinite** システムは、構成されたすべてのブートオプションを試行し、システムがブートするか、手動で中断されるまで繰り返します。 • **5**、**13** システムは、構成されたすべてのブートオプションを試行し、システムがブートするか中断されるまで、選択した回数を繰り返します。すべての試行が失敗した場合、システムは続行するように求めます。値 13 は Cisco UCS B200 M5 のデフォルト値で、5 は Cisco UCS B480 M5 のデフォルト値です。	ブート オプション再試行が 有効の場合にのみ適用されます。
[クール ダウン時間（Cool Down Time（秒）]	次のブートを試行するまで待機する時間（秒単位）。次のいずれかになります。	4.1(1)	B200 M5、B480 M5、C480 M5	15 秒、45 秒、**90 秒** • **15**、**45**、**90** 次のブートを試行するまで、システムは選択された秒数間待機します。	ブート オプション再試行が 有効の場合にのみ適用されます。

ブート オプションの BIOS 設定

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
Boot Option Retry	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうかを設定します。	4.1(1)	B200 M5、B480 M5、C480 M5	**無効**、有効 • [Disabled]：ユーザー入力を待機してから非 EFI ベースのブート オプションを再試行します。 • [Enabled]：ユーザー入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。	
IPV4 HTTP のサポート	HTTP の IPv4 サポートを有効または無効にします。	4.2(1)	C245 M6	無効、**有効** • **無効**：IPv4 HTTP サポートは使用できません。 • **有効**：IPv4 PXE サポートを使用できます。	Network Stack トークンの値を有効にする必要があります。
IPV6 HTTP のサポート	HTTP の IPv6 サポートを有効または無効にします。	4.2(1)	C245 M6	無効、**有効** • **無効**：IPv46 HTTP サポートは使用できません。 • **有効**：IPv6 PXE サポートを使用できます。	Network Stack トークンの値を有効にする必要があります。

ブート オプションの BIOS 設定

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
[IPV6 PXE サポート（IPV6 PXE Support）]	PXE の IPv6 サポートを有効または無効にします。	4.2(1)	C245 M6	無効、**有効** • **無効**：IPv46 PXE サポートは使用できません。 • **有効**：IPv6 PXE サポートを使用できます。	Network Stack トークンの値を有効にする必要があります。
ネットワーク スタック	このオプションを使用すると、システムの完全なネットワーク スタイルを有効または無効にすることができます。	4.1(1)、4.2(1)	C245 M6、B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5	無効、**有効** • **無効**：ネットワーク スタックのサポートは使用できません。 • **有効**：ネットワーク スタックのサポートを使用できます。	無効にすると、 IPV6 PXE、IPV4HTTP、および IPV6HTTP サポートに設定された値はシステムに影響しません。

ブート オプションの BIOS 設定

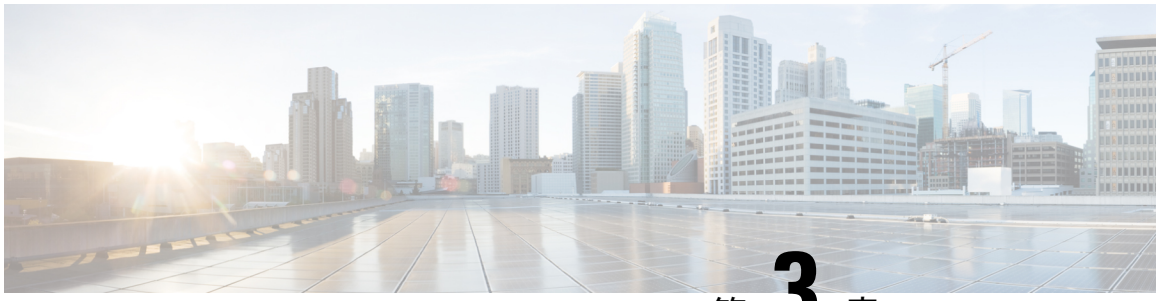
名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
[電源オンパスワード（Power ON Password）]	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。	4.1(1)、4.2(1)	C220 M5、C240 M5、C480 M5、C125 M5、C245 M6	**無効**、有効 • **無効**：電源オンパスワードは無効になります。 • **有効**：電源オンパスワードは有効になります。	
P-SATAモード	このオプションでは、P-SATA モードを選択できます。	4.1(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5	無効、**LSI SW RAID** • 無効：P-SATA モードは無効です。 • LSI SW RAID：SATA コントローラと sSATA コントローラを LSI SW RAID の RAID モードに設定します。	

ブート オプションの BIOS 設定

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
SATA Mode	このオプションでは、SATA モードを選択できます。	4.1(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5	AHCI、**LSISW RAID**、無効 AHCI は S3260 のデフォルト値であり、LSISW RAID は他のすべてのサーバーのデフォルト値です。 • 無効：SATA モードは無効です。 • LSI SW RAID：SATA コントローラと sSATA コントローラを LSI SW RAID の RAID モードに設定します。 • AHCI	

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
[VMD 有効化（VMD Enablement）]	PCIe バスに接続されている NVMe SSD をスワップできるかどうかを指定します。この設定により、これらのドライブの LED ステータス ライトも標準化されます。LED ステータス ライトは、特定の障害インジケータ パターンを表示するようにオプションでプログラムできます。	4.1(1)	C220 M5、C240 M5、B200 M5、B480 M5	**無効**、有効 • 無効：PCIe バスに接続されている NVMe SSD のホット スワップを禁止します。 • 有効：PCIe バスに接続されている NVMe SSD のホット スワップを許可します。	

ブート オプションの BIOS 設定



第 3 章

Intelダイレクト IO(Intel Directed IO)

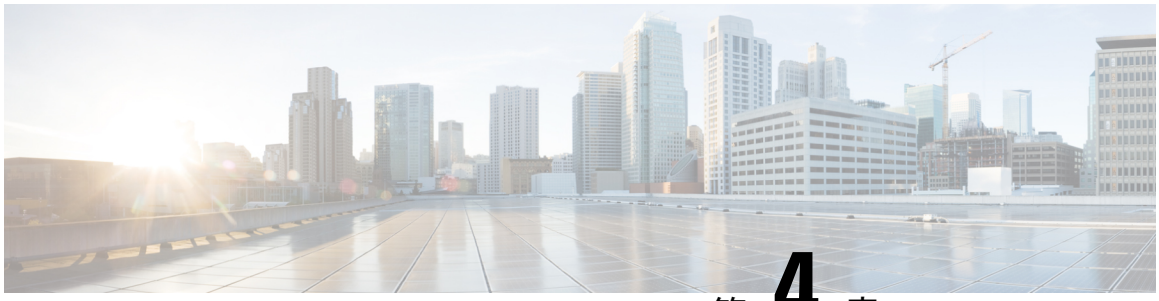
Intelダイレクト IO(Intel Directed IO)

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができる Intel Directed I/O の BIOS 設定を示しています。

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 VT for directed IO]	Intel Virtualization Technology for Directed I/O （VT-d） をプロセッサで使用するかどうか設定します。	4.1(1)、5.0(1)、5.0(2)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5、B200 M6、X210C M6	**有効**、無効 • [Disabled]：プロセッサで仮想化テクノロジーを使用しません。 • [Enabled]：プロセッサで仮想化テクノロジーを使用します。	
[Intel(R) VT-d Coherency サポート （Intel(R) VT-d Coherency Support）]	プロセッサで Intel VT-d Coherency をサポートするかどうか設定します。	4.1(1)、5.0(1)、5.0(2)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5、B200 M6、X210C M6	有効、**無効** • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [Enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。	

Intelダイレクト IO(Intel Directed IO)

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(R) VT-d Interrupt Remapping]	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか設定します。	4.1(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5	**有効**、無効 • [Disabled]：プロセッサでリマッピングをサポートしません。 • [Enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。	
Intel(R) VT-d PassThrough DMAサポート(Intel(R) VT-d PassThrough DMA Support)	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか設定します。	4.1(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5	有効、**無効** • **無効**：プロセッサでパススルー DMA をサポートしません。 • [Enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。	
Intel VTD ATSサポート	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか設定します。	4.1(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5	無効、**有効** • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。	



第 4 章

LOMとPCIeスロット

LOMとPCIeスロット

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して構成できる LOM および PCIe BIOS 設定を示しています。

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
[ACS 制御 GPU *n*（ACS Control GPU n）]（*n* は 1 ～ 14 の範囲）	アクセスコントロールサービス（ACS）を使用すると、プロセッサは、GPU の複数のデバイス間のピアツーピア通信を有効または無効にすることができます。。	4.0(4)、4.1(1)	C480 M5	有効、**無効** • **無効**：GPU の複数のデバイス間のピアツーピア通信を無効にします。 • **有効**：GPU の複数のデバイス間のピアツーピア通信を有効にします。	

LOMとPCIeスロット

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
[LOM の CDN サポート（CDN Support for LOM）]	イーサネットネットワーキング識別子の命名規則を、Consistent Device Naming（CDN）と従来の命名規則のどちらに準拠させるかを指定します。	4.0(4)、4.1(1)	C480 M5	有効、**無効**、LOM のみ • **無効**：OSイーサネットネットワーキング ID は、ETH0 や ETH1 など、デフォルトの規則で名前が付けられます。 • **有効**：OSイーサネットネットワーク識別子に、LOM ポート 0 や LOM ポート 1 のように、物理的な LAN on Motherboard（LOM）のポート番号付けに基づく Consistent Device Naming（CDN）規則で名前を付けます。	
外部SSCの有効化	このオプションでは、外部クロック ジェネレータのクロック拡散スペクトルを有効または無効にすることができます。	4.1(2)	B480M5、B200M5、S3X60M5	有効、**無効**、0P3_Percent、0P5_Percent、ハードウェア、オフ ブレードおよび Cisco UCS S3260 M5 ストレージ サーバでは無効	
[IIO eDPC サポート（IIO eDPC Support）]	このオプションを使用すると、修正不可能なエラーの後にダウンストリームリンクを無効にすることができるため、制御された堅牢な方法で回復することが可能になります。	4.2(1)、5.0(1)、5.0(2)	C220 M6 および C240 M6、B200 M6、X210C M6	無効、致命的なエラーで、**致命的なエラーおよび致命的でないエラーで**	

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
[LOM ポート *n* OptionROM（LOM Port n OptionROM）]。*n* の範囲は 0 ～ 3 です。	オプション ROM が LOM ポート *n* で使用できるかどうか	4.0(4)、4.1(1)、	C220 M6 および C240 M6C220 M5、C240 M5、C480 M5	無効、**有効**、Legacy のみ、UEFI のみ • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。。 • **UEFI のみ**：拡張スロットをUEFIでのみ使用できます。 • **Legacy Only**：拡張スロットをレガシーでのみ使用できます。	

LOMとPCIeスロット

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
[すべてのオンボード LOM ポート（All Onboard LOM Ports）]	すべてのオンボード LOM ポートがイネーブルであるか、ディセーブルであるか。	4.0(2)、4.0(4)、4.1(1)、	C220 M5、C240 M5、C480 M5	無効、**有効** • **無効**：LOM Port 0 OptionROM と LOM Port 1 OptionROM は [無効] に設定されています。 • **有効**：LOM Port 0 OptionROM と LOM Port 1 OptionROM は [有効] に設定されています。。	[無効] として設定している場合、LOM Port 0 OptionROM と LOM Port 1 OptionROM は [無効] に設定されています。[有効] として設定している場合、LOM Port 0 OptionROM と LOM Port 1 OptionROM は [無効] に設定されています。

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
[すべての PCIe スロット オプション ROM（All PCIe Slots OptionROM）]	すべての PCIe OptionROM ポートが有効であるか、無効であるか。	4.0(2)、4.0(4)、4.1(1)、	C220 M5、C240 M5、C480 M5、	無効、**有効**、Legacy のみ、UEFI のみ • **無効**：LOM Port 0 OptionROM と LOM Port 1 OptionROM は [無効] に設定されています。 • **有効**：LOM Port 0 OptionROM と LOM Port 1 OptionROM は [有効] に設定されています。。 • **UEFI のみ**：拡張スロットをUEFIでのみ使用できます。 • **Legacy のみ**：拡張スロットをレガシーでのみ使用できます。	
[PCI ROM CLP]	すべての PCI ROM CLP ポートが有効であるか、無効であるか。	4.0(2)、4.0(4)、4.1(1)、	C220 M5、C240 M5、C480 M5、	[ディセーブル（Disabled）]、[イネーブル（Enabled）] • **無効**：オプションは無効です。 • **有効**：オプションは有効です。。	
PCIe ARIサポート	すべての ARI サポート ポートが有効であるか、無効であるか。	4.2(1)	C225 M6 および C245 M6	無効、有効、**自動** • **無効**：このオプションは無効です。 • **有効**：このオプションは有効です。 • **自動**：PCIe ARI サポートは自動モードです。。	

LOMとPCIeスロット

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
PCIe FPGA SSC	すべての PCIe PLL SSC ポートが有効であるか、無効であるか。	4.1(2)	すべての M5 サーバー	無効、**有効**、Legacy のみ、UEFI のみ • **無効**：LOM Port 0 OptionROM と LOM Port 1 OptionROM は [無効] に設定されています。 • **有効**：LOM Port 0 OptionROM と LOM Port 1 OptionROM は [有効] に設定されています。。	

LOMとPCIeスロット

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
[MRAID *n* リンク速度（MRAID n Link Speed）]。n の範囲は 1 ～ 2 です。	このオプションでは、MRAID の最高速度を制限することができます。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、C225 M6、C245 M6	**自動**、無効、有効、GEN 1、GEN 2、GEN 3、GEN 4、GEN 5 • [Disabled]：最大速度は制限されません。 • **有効**：最大速度は、制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5 GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。 • **GEN 5**：最大 32 GT/s までの速度が許可されます。	
[MRAID *n* OptionROM]。n の範囲は 1 ～ 2 です。	MRAID ポートでオプション ROM を使用可能にするかどうか設定。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、C225 M6、C245 M6	無効、**有効** • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。。	

LOMとPCIeスロット

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
PCIeスロット MSTORリンク速度	このオプションを使用するとMSTOR アダプタの最大速度を制限できます。	4.2(1)	C225 M6 および C245 M6	**自動**、無効、GEN 1、GEN 2、GEN 3、GEN 4 • [Disabled]：最大速度は制限されません。 • **自動**：最高速度は自動的に設定されます。 • **GEN 1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5 GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。	
PCIeスロット MSTOR RAID OptionROM	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。	4.2(1)	C225 M6 および C245 M6	無効、**有効**、Legacy のみ、UEFI のみ • Disabled：オプション ROM は使用できません。 • [Enabled]—オプション ROM は使用できます。	

LOMとPCIeスロット

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
[NVME *n* リンク速度（NVME n Link Speed）]。*n* の範囲は 0 ～ 6 です。	このオプションでは、PCIe スロットに取り付けられたNVMEカードの最高速度を制限することができます。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、S3260 M5、C225 M6、C245 M6	無効、**自動**、GEN1、GEN2、GEN3、GEN4 • **無効**：最大速度は制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN 1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5 GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。	
[NVME *n* OptionROM]。*n* の範囲は 0 ～ 6 です。	このオプションでは、SSD:NVMe スロットnに接続された PCIe アダプタのオプション ROM の実行を制御することができます。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、S3260 M5、C225 M6、C245 M6	Enabled、Disabled • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	

LOMとPCIeスロット

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
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）]。*n* の範囲は 1 ～ 12 です。	スロット n で指定された PCIe スロットのリンク速度。	4.0(1)、4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、C480 M5、C125 M5、C225 M6、C245 M6	無効、**自動**、GEN1、GEN2、GEN3、GEN4、GEN5 GEN5 は、速度 1 ～ 6 でのみサポートされます。 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN 1**：最大 2 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。 • **GEN 5**：最大 32 GT/s までの速度が許可されます。	

LOMとPCIeスロット

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
[スロット*n*の状態（Slot n State）]。*n* は 1 ～ 14 の範囲。	PCIe スロット n に取り付けられているアダプタカードの状態。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C480 M5 ML、C220 M6、C240 M6、B200 M6	無効、**有効**、Legacy のみ、UEFI のみ • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。 • **UEFIのみ**：拡張スロットをUEFIでのみ使用できます。 • **Legacy のみ**：拡張スロットをレガシーでのみ使用できます。	C220 M6、C240 M6、B200 M6は、スロット9の状態のみをサポートします。
PCIe スロット: FLOM リンク速度（PCIe Slot:FLOM Link Speed）	PCIe Slot:FLOM のリンク速度を構成するには。	4.0(1)、4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、S3260 M5、C225 M6、C245 M6	無効、**自動**、GEN1、GEN2、GEN3 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN 1**：最大 2 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。	

LOMとPCIeスロット

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
[前面 NVME *n* リンク速度（Front NVME n Link Speed）]。*n* の範囲は 1 ～ 12 です。	このオプションでは、フロント PCIe スロットに取り付けられた NVME カードの最高速度を制限することができます。	4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、C225 M6、C245 M6	無効、**自動**、GEN1、GEN2、GEN3、GEN4、GEN5 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。 • **GEN 5**：最大 32 GT/s までの速度が許可されます。	
[前面 NVME *n* OptionROM（Front NVME n OptionROM）]。*n* の範囲は 1 ～ 24 です。	このオプションでは、SSD:NVMe スロットnに接続された PCIe アダプタのオプション ROM の実行を制御することができます。	4.2(1)	C225 M6, C245 M6	**有効**、無効 • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	

LOMとPCIeスロット

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
[前面 1 および 2 リンク速度（Front 1 and 2 Link Speed]	このオプションでは、スロット 1 および 2 に接続された前面 PCIe アダプタのリンク速度の実行を制御することができます。	4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、S3260 M5、C225 M6、C245 M6	無効、**自動**、GEN1、GEN2、GEN3、GEN4 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。	

LOMとPCIeスロット

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
PCIe Slot:HBA Link Speed	このオプションでは、HBA カードの最高速度を制限することができます。	4.2(1)	C225 M6, C245 M6	無効、**自動**、GEN1、GEN2、GEN3、GEN4 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。	
[PCIe スロット：HBA オプション ROM（PCIe Slot:HBA OptionROM）]	このオプションを使用すると、HBA カードのオプション ROM 実行を構成できます。	4.2(1)	C225 M6, C245 M6	無効、**有効**、Legacy のみ、UEFI のみ • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。 • **UEFI のみ**：拡張スロットをUEFIでのみ使用できます。 • **Legacy のみ**：拡張スロットをレガシーでのみ使用できます。	

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
[GPU *n* OptionROM]。*n* の範囲は 1 ～ 8 です。	GPU スロット n でオプション ROM を有効にするかどうか設定します。	4.0(4)、4.1(1)	C480 M5 ML	**有効**、無効 • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	
[PCIe LOM:1 および 2 リンク（PCIe LOM:1 and 2 Link）]	このオプションを使用すると、PCIe スロット 1 および 2 に装着されているアダプタカードの最大速度を制限できます。	4.0(1)、4.0(2)、4.0(4)、4.1(1)	すべての M5 サーバー	Enabled、Disabled • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	
スロットメザニンの状態	このオプションを使用すると、PCIe スロットの Mezz 状態を構成できます。	4.0(1)、4.0(2)、4.1(1)	S3260 M5	無効、**有効**、Legacy のみ、UEFI のみ • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。 • **UEFI のみ**：拡張スロットをUEFIでのみ使用できます。 • **Legacy のみ**：拡張スロットをレガシーでのみ使用できます。	

LOMとPCIeスロット

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
PCIe スロット: MLOM リンク速度（PCIe Slot:FLOM Link Speed）	このオプションを使用するとMLOM アダプタの最大速度を制限できます。	4.0(1)、4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5、C480 M5、C125 M5	**自動**、無効、GEN 1、GEN 2、GEN 3、GEN 4、GEN 5 • [Disabled]：最大速度は制限されません。 • **自動**：最高速度は自動的に設定されます。 • **GEN1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5 GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。 • **GEN 5**：最大 32 GT/s までの速度が許可されます。	

LOMとPCIeスロット

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
PCIe Slot:MLOM OptionROM	オプション ROM が MLOM ポートで使用できるかどうか。	4.0(1)、4.0(2)、4.0(4)、4.1(1)、5.0(1)、5.0(2)	C220 M5、C240 M5、C480 M5、C125 M5、B200 M6、X210C M6	無効、**有効**、Legacy のみ、UEFI のみ • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。 • **UEFI のみ**：拡張スロットをUEFIでのみ使用できます。 • **Legacy のみ**：拡張スロットをレガシーでのみ使用できます。	

LOMとPCIeスロット

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
[MRAID リンク速度（MRAID Link Speed）]	このオプションでは、MRAID の最高速度を制限することができます。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、C225 M6、C245 M6	**自動**、無効、GEN 1、GEN 2、GEN 3、GEN 4、GEN 5 • [Disabled]：最大速度は制限されません。 • **自動**：最高速度は自動的に設定されます。 • **GEN1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5 GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。 • **GEN 5**：最大 32 GT/s までの速度が許可されます。	
[PCIe Slot:MRAID OptionROM]	オプション ROM が MLOM ポートで使用できるかどうか。	4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5、C480 M5、C125 M5	無効、有効、Legacy のみ、UEFI のみ • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。	

LOMとPCIeスロット

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
[PCIe スロット *n* OptionROM（PCIe Slot n OptionROM）]。n の範囲は 1 ～ 24 です。	オプション ROM がポートで使用できるかどうか。	4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5、C480 M5、C125 M5	無効、**有効**、Legacy のみ、UEFI のみ • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。	
RAID Link Speed	このオプションを使用すると RAID の最大速度を制限できます。	4.0(1)、4.0(4)、4.1(1)、	C480 M5	無効、**自動**、GEN1、GEN2、GEN3 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN 1**：最大 2 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。	
[PCIe スロット RAID オプション ROM（PCIe Slot MLOM OptionROM）]	オプション ROM が RAID スロットで使用できるかどうか。	4.0(1)、4.0(4)、4.1(1)、	C480 M5	**有効**、無効 • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	

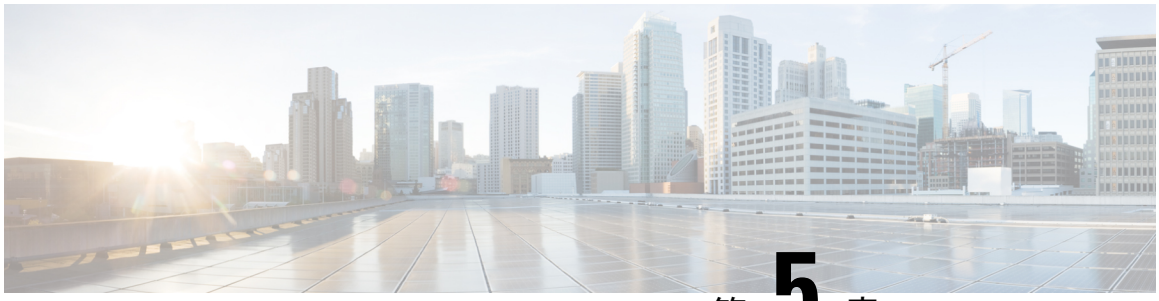
LOMとPCIeスロット

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
[背面 NVME *n* リンク速度（Rear NVME n Link Speed）]。n の範囲は 1 ～ 4 です。	このオプションを使用すると背面 NVME の最大速度を制限できます。	4.0(4)、4.0(1)、4.2(1)	C240 M5、C240 M6、C245 M6	**自動**、無効、GEN 1、GEN 2、GEN 3、GEN 4、GEN 5 • [Disabled]：最大速度は制限されません。 • **自動**：最高速度は自動的に設定されます。 • **GEN1**：最大 2.5 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5 GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。 • **GEN 4**：最大 16 GT/s までの速度が許可されます。 • **GEN 5**：最大 32 GT/s までの速度が許可されます。	
[背面 NVME *n* OptionROM（Rear NVME n OptionROM）]。n の範囲は 1 ～ 8 です。	オプション ROM が背面 NVME で使用できるかどうか。	4.0(4)、4.0(1)、4.2(1)	C240 M5、C240 M6、C245 M6	**有効**、無効 • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	

LOMとPCIeスロット

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
[PCIe Slot:Riser リンク速度 *n*（PCIe Slot:Riser Link Speed n）]。nは1および2です。	このオプションを使用するとライザーの最大速度を制限できます。	4.0(4)、4.0(1)、4.2(1)	C220 M5、C240 M5、C480 M5、C125 M5	無効、**自動**、GEN1、GEN2、GEN3 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN 1**：最大 2 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。	
[PCIe Slot:Riser *n* スロット *x* リンク速度（PCIe Slot:Riser n Slot x Link Speed）]。*n* は1と2、*x* は1～6です。	このオプションを使用すると*x*スロットのライザーの最大速度を制限できます。	4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5、C480 M5、C125 M5	無効、**自動**、GEN1、GEN2、GEN3 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN 1**：最大 2 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大 5GT/s までの速度が許可されます。 • **GEN 3**：最大 8 GT/s までの速度が許可されます。	

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
PCIeスロット：SASオプションROM（PCIe Slot:SAS OptionROM）	オプションROMがSASスロットで使用できるかどうか。	4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5、C480 M5、C125 M5	無効、**有効**、Legacyのみ、UEFIのみ • **無効**：拡張スロットを使用できません。 • **有効**：拡張スロットを使用できます。 • **UEFIのみ**：拡張スロットをUEFIでのみ使用できます。 • **Legacyのみ**：拡張スロットをレガシーでのみ使用できます。	
[PCIe Slot:FrontSSD *n* リンク速度（PCIe Slot:FrontSSD nLink Speed）]。*n*は1および2です。	このオプションを使用すると前面SSDの最大速度を制限できます。	4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5、C480 M5、C125 M5	無効、**自動**、GEN1、GEN2、GEN3 • **無効**：最大スピードは制限されていません。 • **自動**：最高速度は自動的に設定されます。 • **GEN 1**：最大2 GT/s（ギガトランスファー/秒）までの速度が許可されます。 • **GEN 2**：最大5GT/sまでの速度が許可されます。 • **GEN 3**：最大8 GT/sまでの速度が許可されます。	



第 5 章

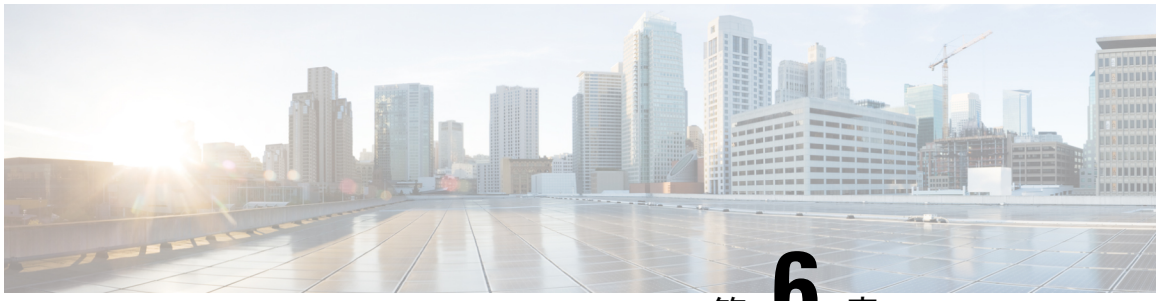
メイン

メイン

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるメイン BIOS 設定を示しています。

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
PCIeスロットCDN制御	PCIe スロットの Consistent Device Naming（CDN）制御により、PCIe スロットに一貫した方法で名前を付けることができます。これにより PCIe スロットの名前は、より統一され、識別しやすくなり、構成に変更が加えられても永続的に保持されます。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5、C225 M6、C245 M6	有効、**無効** • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	デフォルトでは、CDN制御は UCSM Manager で無効になっています。（Standalone モードではデフォルトで有効になっています。）

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[POST エラーの一時停止（POST Error Pause）]	POST 中にサーバーで重大なエラーが発生した場合について説明します。	4.0(1)、4.0(2)、4.0(4)、4.1(1)	すべての M5 サーバー	有効、**無効** • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	
[TPM サポート（TPM Support）]	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)	すべての M5、M6、および X210C M6 サーバー。	**有効**、無効 • **無効**：オプションは制限されていません。 • **有効**：オプションは制限されています。	



第 6 章

メモリ

メモリ

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して設定できるメモリの 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
強力なメモリテスト	システムの起動中に拡張メモリ テストを有効にします。メモリ量に応じて起動時間は長くなります。	4.0 (1)、4.0(2)、4.0(4)、4.1(1)、4.2(1)、5.0(1)、5.0(2)	C220 M5、C240 M5、B200 M6、C240 M6、C225 M6、C245 M6、X210C M6	無効、有効、**自動** • **無効**：オプションは無効です。 • **有効**：オプションは有効です。 • **自動**：オプションは自動モードです。	この設定は、デフォルト状態の自動のままにしておくことをお勧めします。

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
[BME DMA 緩和（BME DMA Mitigation）]	不正な外部 DMA からの脅威を緩和するため、PCI BME ビットを無効にできます。	4.0(1)、4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、B200 M6、S3260 M5、C240 M6、C225 M6、C245 M6、X210C M6	有効、**無効** • 無効：オプションは制限されていません。 • 有効：オプションは制限されています。	
バーストリフレッシュおよび遅延リフレッシュ	メモリがアクティブで、指定されたウィンドウ内でリフレッシュを実行するときに、メモリ コントローラがリフレッシュ サイクルを延期できるようにします。遅延リフレッシュ サイクルは、複数のリフレッシュ サイクルのバーストで実行される場合があります。	4.0(1)、4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、B200 M6、S3260 M5、C240 M6、C225 M6、C245 M6、X210C M6	有効、**無効** • 無効：オプションは制限されていません。 • 有効：オプションは制限されています。	
[CPU SMEE]	プロセッサで、メモリの暗号化サポートを実現するセキュアメモリ暗号化有効（SMEE）機能を使用するかどうかを指定します。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C125 M6、C225 M6、C245 M6	無効、**有効**、自動 • 無効：オプションは無効です。 • 有効：オプションは有効です。 • **自動**：オプションは自動モードです。	

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
[IOMMU]	出入力メモリ管理ユニット（IOMMU）により、AMDプロセッサが物理アドレスへ仮想アドレスをマッピングすることが可能です。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C125 M6、C225 M6、C245 M6	無効、有効、**自動** • 無効：オプションは無効です。 • 有効：オプションは有効です。 • 自動：オプションは自動モードです。	
[バンク グループ スワップ（Bank Group Swap）]	物理アドレスをアプリケーションに割り当てる方法を決定します。	4.0(1)、4.0(4)、4.1(1)4.2(10	C125 M5、C225 M6、C245 M6	無効、有効、**自動** • 無効：オプションは無効です。 • 有効：オプションは有効です。 • 自動：オプションは自動モードです。	
チップセットインターリーブ	ノード 0 に選択した DRAM チップ経由でメモリ ブロックがインターリーブされるかどうか設定します。	4.2(1)	C225 M6, C245 M6	無効、有効、**自動** • 無効：オプションは無効です。 • 有効：オプションは有効です。 • 自動：オプションは自動モードです。	

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
SNPメモリカバレッジ	このオプションは、Secured Nested Paging（SNP）メモリとリバースマップテーブル（RMP）の動作モードを選択します。RMPは、システムの物理アドレスとゲストの物理アドレス間の1対1のマッピングを保証するために使用されます。	4.2(1)	C225 M6, C245 M6	無効、有効、**自動** • 無効：オプションは無効です。 • 有効：オプションは有効です。 • 自動：オプションは自動モードです。	
[カバーされる SNP メモリ サイズ（MiB）（SNP Memory Size to Cover in MiB）]	SNP メモリ サイズを設定できます。	4.2(1)	C225 M6, C245 M6	無効、有効、**自動** • 無効：オプションは無効です。 • 有効：オプションは有効です。 • 自動：オプションは自動モードです。	

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
ソケットごとのNUMAノード	4GB を超える MMIO が有効か無効か。	4.2(1)	C225 M6, C245 M6	**自動**、NPS0、NPS1、NPS2、NPS4 • NPS0：ソケットごとの NUMA ノード数を 0 にします。 • NPS1：ソケットごとの NUMA ノード数を 1 にします。 • NPS2：ソケットごとの NUMA ノード数を 2 にします。 • NPS4：ソケットごとの NUMA ノード数を 4 にします。 • 自動：チャネル数を自動に設定します。	
AMD メモリインターリーブ	インターリーブされるメモリ ブロックを決定します。また、インターリーブの開始アドレス（ビット 8、9、10、11）も指定します。	4.0(2)、4.0(4)、4.1(1)	C125 M5	**自動**、チャネル、Die、なし、ソケット	
AMD メモリインターリーブ サイズ	インターリーブされるメモリ ブロックのサイズを決定します。また、インターリーブの開始アドレス（ビット 8、9、10、11）も指定します。	4.0(2)、4.0(4)、4.1(1)	C125 M5	1 KB、2 KB、256 Bytes、512 Bytes、**自動**	

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
SEV-SNPサポート	セキュア ネスティッド ページング機能を有効にできます。	4.2(1)	C225 M6, C245 M6	**無効**、有効 • 無効：オプションは無効です。 • 有効：オプションは有効です。	
CR QoS	同時DCPMM BW飽和スレッドの存在下でのDRAMおよびシステム全体のBWドロップを防止し、同種のDDRTのみの使用への影響を最小限に抑えます。マルチテナントの使用例、VMなどに適していますが、メモリモードも向上します。「ワーストケース」の低下をターゲットにします。	4.1(2)、4.2(1)、5.0(1)、5.0(2)	C220 M5、C240 M5、C220 M6、C240 M6 サーバー、B200 M6、および X210C M6	**無効**、レシピ 1、レシピ 2、レシピ 3、モード 0、モード 1、モード 2 • 無効：この機能が無効になります。 • レシピ 1：6 モジュール、最適化されたソケットあたり 4 モジュール • レシピ 2：最適化されたソケットあたり 2 モジュール • レシピ 3：最適化されたソケットあたり 1 モジュール • モード 0：PMem QoS 機能を無効にする • モード 1：M2M QoS Enable;CHA QoS Disable • モード 2：M2M QoS Enable;CHA QoS Enable	

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
CR FastGo設定	CR FastGo Config は、FastGO が無効になっている場合の DDRT 非一時書き込み帯域幅を改善します。FastGO を有効にすると、アンコアへの NT 書き込みのフローが高速になります。FastGO を無効にすると、CPU アンコアの NT 書き込みキューが減少し、DCPMM で連続して改善され、帯域幅が向上します。	4.1(2)、4.2(1)、5.0(1)、5.0(2)	C220 M5、C240 M5、C220 M6、C240 M6	**自動**、オプション 1 ～ 5、最適化を有効にする、最適化を無効にする	
[DCPMM ファームウェアのダウングレード（DCPMM Firmware Downgrade）]	DCPMM ファームウェアのダウングレードを構成するには	4.0(1)、4.0(2)、4.0(4)、4.1(1)、4.2(1)	すべての M5 サーバー	**無効**、有効 • 無効：オプションは無効です。 • 有効：オプションは有効です。	
[DRAM リフレッシュレート（DRAM Refresh Rate）]	内部メモリ用のリフレッシュ間隔レートを構成するには	4.0(1)、4.0(2)、4.0(4)、4.1(1)、4.2(1)	C125 M5	自動、1x、**2x**、3x、4x	
DRAM SWのサーマルスロットリング	DRAM SW サーマルスロットリングを構成するには	4.0(1)、4.0(2)、4.0(4)、4.1(1)	C125 M5	[ディセーブル（Disabled）]、[イネーブル（Enabled）] • 無効：オプションは無効です。 • 有効：オプションは有効です。	

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
eADRサポート	拡張非同期DRAMリフレッシュ (eADR) により、データを含むCPUキャッシュラインが適切なタイミング、必要な順序でフラッシュされます。電源障害から保護されたドメインにも含まれます。	4.2(1)、5.0(1)、5.0(2)	B200 M6、X210C M6	**無効**、有効、自動 • 無効：オプションは無効です。 • 有効：オプションは有効です。 • 自動：オプションは自動モードです。	
[低電圧DDRモード（Low Voltage DDR Mode）]	低電圧と高周波数のどちらのメモリ動作をシステムで優先するかを設定します。。	4.0(1)、4.0(2)、4.0(4)、4.1(1)	すべてのM5サーバー	**自動**、省電力モード、パフォーマンスモード • 自動：CPUが低電圧メモリ動作または高周波メモリ動作のどちらを優先するかを決定します。 • [Power Saving Mode]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • パフォーマンスモード：高周波数の動作が低電圧の動作よりも優先されます。 • 自動：オプションは自動モードです。	

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
メモリ帯域幅ブースト	メモリ帯域幅を増やすことができます。	4.2(1)、5.0(1)、5.0(2)	C220 M6 および C240 M6、B200 M6、X210C M6	[ディセーブル（Disabled）]、[イネーブル（Enabled）] • 無効：オプションは無効です。 • 有効：オプションは有効です。	
メモリのリフレッシュレート	メモリ コントローラのリフレッシュ レートを制御し、メモリ構成とワークロードに応じて、メモリのパフォーマンスと電力に影響を及ぼせるようにします。	4.0(2)、4.0(4)、4.1(1)、4.2(1)、5.0(1)、5.0(2)	C220 M5、C240 M5、B200 M6、S3260 M5、C240 M6、C225 M6、C245 M6、X210C M6	1x リフレッシュ、**2x リフレッシュ**	
メモリサイズの制限 (GiB)	部分的なメモリのミラー モードの容量を、合計メモリ容量の 50% に制限します。メモリサイズは、0 GB ~ 65535 GB の範囲で 1 GB ずつ増加します。	4.0(2)、4.0(4)、4.1(1)、4.2(1)	C220 M5、C240 M5、B200 M6、S3260 M5、C240 M6、C225 M6、C245 M6、X210C M6	**0**：65535（ステップ サイズが 1）	

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
メモリのサーマル スロットリング モード	メモリの温度が制限内にあることを保証する保護メカニズムを提供します。温度が最高しきい値を超えると、メモリ アクセス レートが下げられ、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、過熱による DIMM の損傷を防ぎます。	4.0(1)、4.0(2)、4.0(4)、4.1(1)	すべての M5 サーバー	**PECI を使用した CLTT**、無効 • 無効：オプションは無効です。 • PECI を使用した CLTT：プラットフォーム環境制御インターフェイス（PECI）を使用してクローズドループ サーマル スロットリング（CLTT）を有効にします。	このトークンは、C125 M5 サーバーではサポートされていません。
[ミラーリング モード（Mirroring Mode）]	メモリのミラーリングは、メモリに 2 つの同じデータ イメージを保存することにより、システムの信頼性を向上させます。	4.0(1)、4.0(2)、4.0(4)、4.1(1)	すべての M5 サーバー	**ソケット間**、ソケット内 • ソケット間：メモリは、CPU ソケット間にまたがる 2 つの Integrated Memory Controller（IMC）間でミラーリングされます。 • ソケット内：1 つの IMC が同じソケット内の別の IMC とミラーリングされます。	

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
NUMA最適化	BIOS で NUMA をサポートするかどうか設定します。	4.0(1)、4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5、B200 M6、S3260 M5、X210C M6	**有効**、無効 • [Disabled]：BIOS で NUMA をサポートしません。 • [Enabled]：NUMA に対応したオペレーティングシステムに必要な ACPI テーブルを BIOS に含めます。このオプションを有効にする場合は、一部のプラットフォームでシステムのソケット間メモリ インターリーブを無効にする必要があります。	
NVMパフォーマンス設定	NVMパフォーマンス設定により、DDR チャネル上の DDR と DDRT トランザクション間の効率的なメジャー モード調停が可能になり、チャネル BW と DRAM の遅延が最適化されます。	4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5、B200 M6、S3260 M5、X210C M6	**BW 最適化**、レイテンシー最適化、バランシング プロファイル • BW 最適化：DDR および DDRT BW 用に最適化されています。これがデフォルトのオプションです。 • 遅延最適化：DDRT BW が存在する場合 DDR 遅延が改善します。 • バランシング プロファイル：メモリ モード用に最適化されています。	

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
オペレーションモード	このオプションを使用すると、操作モードを構成できます。	4.2(1)、4.2(2)	C225 M5、C245 M5	**テスト専用**、テストと修復	

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
パニックと高水準点	メモリ コントローラの遅延リフレッシュ機能を制御します。	4.2(1)	C240 M6、C225 M6、C245 M6		Rowhammerスタイルの攻撃を軽減するために、この設定はデフォルト状態（**[低（Low）]**）のままにすることを推奨します。

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
				高、**低** • [高（High）]：メモリコントローラは、最大 8 つのリフレッシュコマンドを延期できます。メモリコントローラはリフレッシュ間隔内で延期されたすべてのリフレッシュを実行します。9 番目のリフレッシュコマンドについては、リフレッシュの優先順位をパニックにします。メモリコントローラは、延期されたすべてのリフレッシュコマンドが実行されるまで、通常のメモリ トランザクションを一時停止します。 • 低：メモリコントローラは、リフレッシュコマンドを延期することはできません。 （注） Rowhammer スタイルの攻撃を軽減するために、この設定はデフォルト状態（[低（Low）]	

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
				）のままにすることを推奨します。	
部分的なキャッシュ行の節約	パーシャル キャッシュ ライン スペアリング (PCLS) は、メモリ コントローラーのエラー防止メカニズムです。PCLS は、メモリ アクセス中に置換できるように、ビットの欠陥のあるニブルの場所を、対応するデータ コンテンツとともにスペア ディレクトリに静的にエンコードします。	4.2(1)、5.0(1)、5.0(2)	B200 M6、C240 M6、C220 M6、C225 M6、C245 M6、X210C M6	無効、**有効** • 無効：オプションは無効です。 • 有効：オプションは有効です。	

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
メモリパーシャルミラーモード	メモリ パーシャル ミラー モードを使用すると、GB単位またはメモリ容量の割合によって部分的にミラーリングすることができます。ここで選択したオプションに応じて、使用可能なフィールドで、部分的なミラーの割合または部分的なミラー容量を GB 単位で定義できます。メモリ容量の最大 50% を部分的にミラーリングできます。	4.1(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5		

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
				無効、パーセンテージ、GB 単位の値 • 無効：オプションは無効です。 • 容量：部分メモリモードでミラーリングされるメモリの量は、合計メモリの割合として定義されます。 • 値 (GB): 部分的なメモリ モードでミラーリングされるメモリの合計は GB で定義されます。 （注） 部分的なメモリ ミラーモードは標準のミラーリング モードに対して相互に排他的です。 部分的な	

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
				ミラー 1 ~ 4 は、関連オプションで GB または割合で設定されている容量制限を超えない限り、任意の数または設定で使用できます。	

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
パーシャルミラー率	使用可能なメモリの総量を、合計メモリの割合として制限します。これは、0.000.01 %から 50.00 % まで、0.01 % 単位で増加させられます。	4.1(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5	**0.00**：50.00（0.01 のステップ サイズ）	
[パーシャルミラー *n* GB 単位のサイズ（Partial Mirror n Size in GB）]。*n* の範囲は 1 ～ 4 です。	パーシャル ミラー *n* のメモリの量を GB 単位で制限します。これは、0 GB ~ 65535 GB の範囲で 1 GBずつ増加します。	4.1(1)	B200 M5、B480 M5、C220 M5、C240 M5、C480 M5、S3260 M5、C125 M5	**0**：65535（ステップ サイズが 1）	
PCIe RASサポート	PCIe RAS ポートが有効か、無効かどうか。	4.0 (1)、4.0(2)、4.0(4)、4.1(1)、4.1(3)	すべての M5 サーバー	無効、**有効**、自動 • 無効：このオプションは無効です。 • 有効：このオプションは有効です。 • 自動：PCIe RAS サポートは自動モードです。	

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
ポストパッケージ修復	Post Package Repair (PPR) は、スペア セルに置き換えて、障害のあるメモリ セルを修復する機能を提供します。	4.2(1)	B200 M6、C240 M6、C220 M6、C225 M6、C245 M6、X210C M6	無効、**ハード PPR** • 無効：このオプションは無効です。 • ハード PPR：これにより、破損したストレージセルが永続的に再マッピングされることになります。	

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
メモリRAS設定	サーバに対するメモリの RAS（信頼性、可用性、有用性）の設定方法です。	4.0 (1)、4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)、5.0(1)、5.0(2)	C220 M5、C240 M5、C240 M6、C220 M6		

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
				最大パフォーマンス、ミラーリング、ロックステップ、ミラーモード 1LM、パーシャル ミラー モード 1LM、スペアリング、**ADDDC スペアリング** • 最大パフォーマンス：システム パフォーマンスを最適化し、すべての高度な RAS 機能を無効にします。 • [Mirroring]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。このモードは UCS M4 以前のブレードサーバーに使用します。 • [Lockstep]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップモードをイネーブルにすることで、メモリアクセス遅延の最小化およびパフォーマンスの向上を図ることがで	

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
				きます。B440 サーバーでは [lockstep] がデフォルトで有効になっています。 • ミラー モード 1LM：ミラーモード 1LM は、ミラーリングされるシステム内の 1LM メモリ全体を設定し、結果的にメモリ容量を半減させます。このモードは UCS M5 および M6 ブレード サーバーに使用します。 • [部分的なミラーモード 1LM (Partial Mirror Mode 1LM)]：部分的なミラーモード 1LM は、ミラーリングされるシステム内の 1LM メモリの一部全体を設定し、結果的にメモリ容量を半減させます。このモードは UCS M5 および M6 ブレード サーバーに使用します。	

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
				• スペアリング：システムの信頼性は、他のDIMMが故障した場合に使用できるように、メモリを予備に保持することによって最適化されます。このモードは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。 • ADDDC スペアリング：システムの信頼性は、他のDIMMが故障した場合に使用できるように、メモリを予備に保持することによって最適化されます。このモードは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。	

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
PPRタイプ	Post Package Repair (PPR) は、スペア セルに置き換えて、障害のあるメモリ セルを修復する機能を提供します。	4.1(1)、4.2(1)	C220 M5、C240 M5、B200 M5、S3260 M5、B200 M6、C240 M6、C220 M6、C225 M6、C245 M6	無効、**ハード PPR** • 無効：オプションは無効です。 • ハード PPR：これにより、破損したストレージセルが永続的に再マッピングされることになります。	
Secure Encrypted Virtualization	VM のコードとデータが分離された、暗号化仮想マシン（VM）の実行を有効にします。	4.2(1)	C125 M5、C225 M6、C245 M6	253 ASID、509 ASID、自動 • 253 ASID • 509 ASID • 自動 （注） Rowhammer スタイルの攻撃を軽減するために、この設定は [自動（Auto）] のデフォルト状態のままにすることを推奨します。	

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
[SMEE]	プロセッサで、メモリの暗号化サポートを実現するセキュアメモリ暗号化有効（SMEE）機能を使用するかどうかを指定します。	4.0(4)、4.1(1)、4.1(3)、4.2(1)	C125 M5、C225 M6、C245 M6	無効、**有効** • 無効：このオプションは無効です。 • 有効：このオプションは有効です。	

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
2LMのSnoopyモード		4.0 (1)、4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべてのM5 サーバー	**無効**、有効 • 無効：このオプションは無効です。 • 有効：このオプションは有効です。	

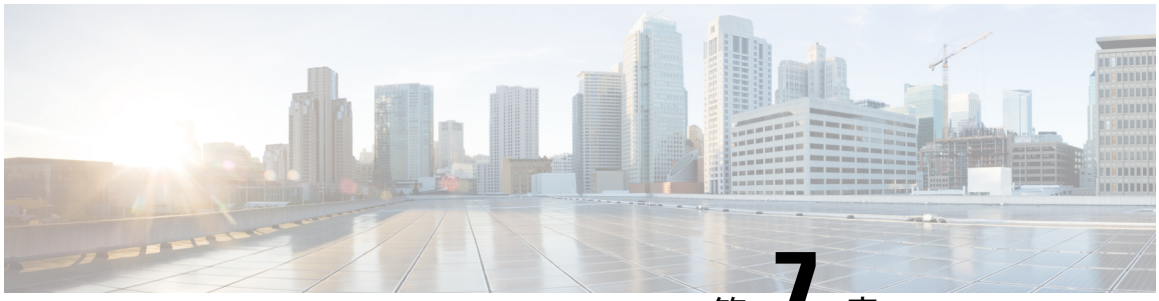
名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
	すべてのDRAMアクセスでディレクトリを維持しながら、DCPMM アクセスのスヌーピング モードを有効にします。スヌープは、ソケット間のキャッシュの一貫性を維持します。ディレクトリは、リモート ノード情報をローカル（メモリ内）に保持することでスヌープを削減します。ディレクトリのルックアップと更新により、メモリ トラフィックが追加されます。 ディレクトリは、DRAM には適していますが、DCPMM には必ずしも適していません。非 NUMA ワークロードの場合、この機能を有効にすると、DCPMM に対するディレクトリの更新が排除されるため、DDRT の帯域幅が制限されたワークロードに役立ちます。ディレクトリは、ファー メモリ アクセスに対して無効になっており、代わりにリモート ソケットをスヌーピングして所有権を確認します。ディレクト				

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
	リは DRAM (メモリの近く)にのみ使用されます。				

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
ADのSnoopyモード		4.0 (1)、4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべてのM5 サーバー	**無効**、有効 • 無効：このオプションは無効です。 • 有効：このオプションは有効です。	

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
	すべてのDRAMアクセスでディレクトリを維持しながら、DCPMMアクセスのスヌーピングモードを有効にします。スヌープは、ソケット間のキャッシュの一貫性を維持します。ディレクトリは、リモートノード情報をローカル（メモリ内）に保持することでスヌープを削減します。ディレクトリのルックアップと更新により、メモリトラフィックが追加されます。 ディレクトリは、DRAMには適していますが、DCPMMには必ずしも適していません。非NUMAワークロードの場合、この機能を有効にすると、DCPMMに対するディレクトリの更新が排除されるため、DDRTの帯域幅が制限されたワークロードに役立ちます。ディレクトリはADへのアクセスに対して無効になり、代わりにリモートソケットをスヌーピングして所有権を確認します。ディレクトリはDRAMアク				

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
	セスにのみ使用されます。				
透過的セキュアメモリ暗号化	システム メモリに格納されているすべてのデータの透過的なハードウェア メモリ暗号化を提供します。	4.1(3)	C125 M5 サーバー	無効、有効、**自動** • 無効：このオプションは無効です。 • 自動：このオプションは自動モードに設定されています。	
[UMA ベースのクラスタリング（UMA Based Clustering）]	名前が示すように、UMA ベースのクラスタリングは、プロセッサが Uniform Memory Access（UMA）ノードとして構成されている場合、つまり SNC が無効になっている場合に推奨されるクラスタリング モードです。	4.2(1)	C220 M6、C240 M6、B200 M6、X210 M6	Disable-All-2All, **Hemisphere-2-clusters**	
揮発性メモリモード	メモリ モードの構成を許可します。	4.0(2)、4.0(4)、4.1(1)、4.2(1)、5.0(1)、5.0(2)	C220 M6、C240 M6、B200 M6、X210C M6	1LM、**2LM** • 1LM：1 層メモリ（1LM）を構成します。 • 2LM：2 層メモリ（1LM）を構成します。	



第 7 章

PCI

PCI

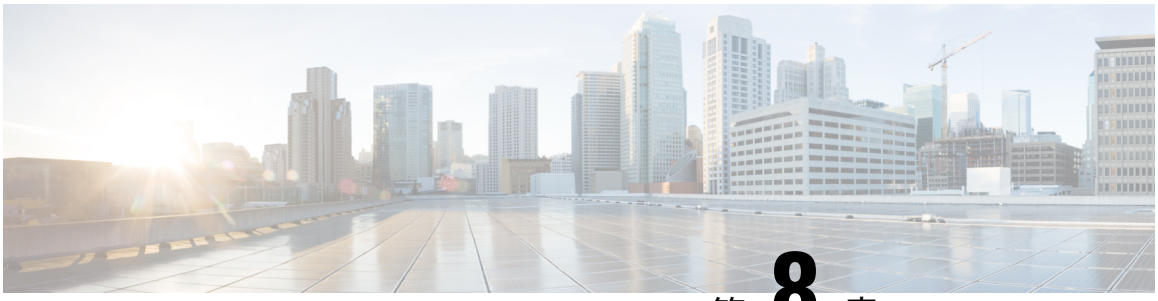
次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができる PCI BIOS 設定を示しています。

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
[ASPM のサポート（ASPM Support）]	BIOS での ASPM（アクティブ電源状態管理）サポートのレベルを設定できます。	4.0(1)、4.0(2)、4.0(4)、4.1(1)	すべての M5 サーバー	無効、**自動**、ForceL0 • **ForceL0**：すべてのリンクを強制的に L0 スタンバイ（L0s）状態にします。	

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
4GiB超のメモリマップ式IO	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリマップド I/O を有効または無効にします。レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。	4.0 (1)、4.0(2)、4.0(4)、4.1(1)、4.1(3)	すべての M5 サーバー	**無効**、有効 • **無効**：このオプションは無効です。 • **有効**：このオプションは有効です。	
[SR-IOV のサポート（SR-IOV Support）]	サーバ上で SR-IOV（Single Root I/O Virtualization）を有効または無効にします。	4.2 (1)	C225M6、C245M6 C125M5、C220M4、C240M4、C3X60M4	無効、**有効** • **無効**：このオプションは無効です。 • **有効**：このオプションは有効です。	

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
[VGA の優先順位（VGA Priority）]	システムに複数の VGA デバイスがある場合、VGA グラフィックス デバイスの優先順位を設定できるようにします。	4.0(2)、4.0(4)、4.1(1)	C220 M5、C240 M5	オフボード、**オンボード**、オンボード VGA が無効 • [Onboard]：オンボード VGA デバイスが優先されます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • **オフボード**：PCIE グラフィックス アダプタが優先されます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • **オンボード VGA が無効**：PCIE グラフィックス アダプタが優先され、オンボード VGA デバイスは無効になります。 （注） オンボード VGA がディセーブルの場合、vKVM は機能しません。	

PCI



第 8 章

電源およびパフォーマンス

電源およびパフォーマンス

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して構成できる BIOS 設定の電源とパフォーマンスを示しています。

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
C1自動降格	有効にすると、CPU は非コア自動降格情報に基づいてC1 状態に自動的に降格します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	無効、**有効** • 無効：このオプションは無効です。 • 有効：このオプションは有効です。	
C1自動降格解除	プロセッサがC1 降格状態から自動的に解除できるようにするかどうかを選択します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	無効、**有効** • 無効：このオプションは無効です。 • 有効：このオプションは有効です。	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[コア パフォーマンス ブースト（Core Performance Boost）]	AMDプロセッサがアイドル状態（ほとんど使用されていない状態）のときにコアの周波数を上げるかどうかを指定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	無効、**自動** • 無効：このオプションは無効です。 • 自動：パフォーマンスをブーストする方法をCPUで自動的に決定します。	
[グローバル C ステート制御（Global C State Control）]	AMDプロセッサがIOベースの C ステート ジェネレーションおよびDF Cステートを制御するかどうかです。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効 • 自動：このオプションは自動モードに設定されています。 • 無効：このオプションは無効です。 • 有効：このオプションは有効です。	
[L*n* ストリーム HW プリフェッチャー（Ln Stream HW Prefetcher）]。n の値は 1 および 2 です。	プロセッサで、AMDハードウェアプリフェッチ機構が必要に応じてデータおよび命令ストリームをメモリから取得し、L1 または L2 キャッシュに入れることを許可するかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効 • 自動：このオプションは自動モードに設定されています。 • 無効：このオプションは無効です。 • 有効：このオプションは有効です。	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[デタミニズムスライダ（Determinism Slider）]	AMDプロセッサにより動作方法を決定できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、パフォーマンス、電源 • 自動：CPU はデフォルトの決定論的な電源設定を自動で使用します。 • パフォーマンス：プロセッサは、最適なパフォーマンスかつ一貫した方法で動作します。 • 電源：プロセッサは、ダイごとに許容される最大のパフォーマンスで動作します。	
効率モードが有効	効率に基づいて消費電力を設定できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、有効 • 有効：このオプションは有効です。 • 自動：CPU はデフォルト設定を自動で使用します。	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
CPPC	コラボレーティブプロセッサ パフォーマンス制御を設定できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効 • 有効：このオプションは有効です。 • 無効：このオプションは無効です。 • 自動：CPU はデフォルト設定を自動で使用します。	
[cTDP コントロール（cTDP Control）]	熱設計出力（TDP）のカスタマイズされた値を設定できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	自動、手動 • 自動：プロセッサの定格 TDP 値を使用します。 • 手動：TDP 値をカスタマイズできます。	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
強力なCPUパフォーマンス	サーバー設定を自動的に調整することにより、CPU パフォーマンスを向上させます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)、5.0(1)、5.0(2)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	無効、**自動** • 無効：このオプションは無効です。 • 自動：サーバー設定を調整して、プロセッサのパフォーマンスを向上させることができます。 （**注**） この機能を有効にすると、消費電力が増加する可能性があります。	

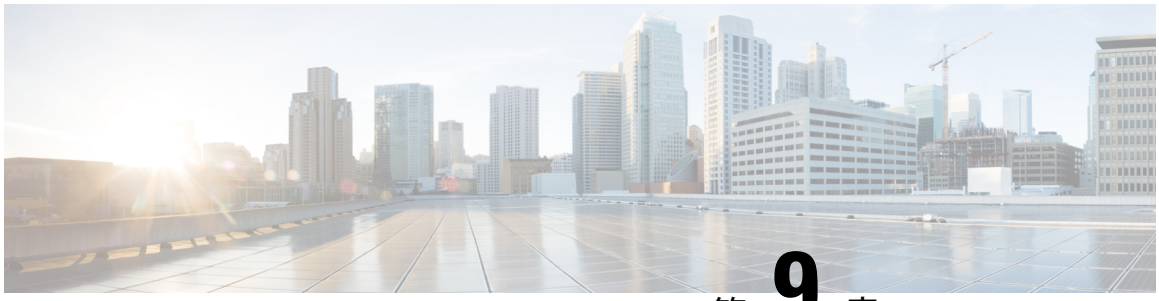
名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
					この機能を使用するには、サーバーが次の要件を満たしている必要があります。 • サーバーが、Intel Apache Pass DCPMM を使用していないこと。 • Cisco UCS C220 M6 サーバーの DCPMM モジュールサ

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
					イズは64 GB未満であり、Cisco UCS C240 M6サーバーでは256 GB未満であること。

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
					• サーバーにCPUカードが搭載されていないこと。
LLCデッドライン	CPU の非包括的キャッシュ スキームでは、中間レベル キャッシュ（MLC）から削除された内容が最終レベル キャッシュ（LLC）に書き込まれます。行を MLC から削除する際、コアはそれらにデッドとしてフラグを立てることがあります（再度読み取られる可能性が小さい場合）。LLC には、デッド ラインを削除し、LLC に書き込まないオプションがあります。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	無効、有効、**自動** • **無効**：デッドラインは常に削除されます。LLC に書き込まれることはありません。 • **有効**：使用可能な空きスペースがある場合、デッドラインを LLC に書き込むことを LLC に許可します。これがデフォルトのオプションです。 • 自動：CPU が LLC のデッドラインの割り当てを決定します。	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
UPIリンク有効化	プロセッサが必要とする数のウルトラ パスインターコネクト（UPI）リンクを有効にします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)、5.0(1)、5.0(2)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	**自動**、1、2、3	
UPI電源管理	UPI 電力管理は、サーバーの電力を節約するために使用できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	無効、**有効** • **無効**：このオプションは無効です。 • **有効**：このオプションは有効です。	
[仮想 NUMA（Virtual NUMA）]	仮想 NUMA（仮想非均一メモリ アクセス）は、VMware 仮想マシン（VM）のメモリ アクセス最適化方法であり、メモリ帯域幅のボトルネックを防ぐのに役立ちます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)、5.0(1)、5.0(2)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	**無効**、有効 • **無効**：このオプションは無効です。 • **有効**：このオプションは有効です。	
XPTリモートプリフェッチ	この機能は、LLC 要求を複製し、最近の LLC 履歴に基づいてリモート マシンの適切なメモリ コントローラに送信して、待ち時間を減らします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)、5.0(1)、5.0(2)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	**無効**、有効 • **無効**：このオプションは無効です。 • **有効**：このオプションは有効です。 • **自動**：CPU が機能を決定します。	

電源およびパフォーマンス



第 9 章

プロセッサ

プロセッサ

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるプロセッサの BIOS 設定を示しています。

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
[隣接キャッシュ行のプリフェッチ（Adjacent Cache Line Prefetcher）]	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効 • **無効**：このオプションは無効です。 • **有効**：このオプションは有効です。	この値を指定するには、[CPU Performance] を [Custom] に設定する必要があります。[Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンスプロファイルの設定が優先されます。

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
[高度（Altitude）]	物理サーバがインストールされている地点のおよその海抜（m 単位）。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、300、900、1500、3000 • [Auto]：物理的な高度を CPU によって判別します。 • *.n* M（*n* が 300、900、1500、3000 の場合）：サーバーは海抜約 *n* メートルです。	
[自律コア C 状態（Autonomous Core C state）]	HALT 命令を MWAIT 命令に変換する CPU 自律 C-state を有効にします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[CPU 自律 C 状態（CPU Autonomous C State）]	これにより、CPU 自律状態が有効または無効になります。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	

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
[ブート パフォーマンス モード（Boot Performance Mode）]	オペレーティング システムのハンドオフ前に設定される BIOS パフォーマンス状態を選択できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
バーストリフレッシュおよび遅延リフレッシュ	メモリがアクティブで、指定されたウィンドウ内でリフレッシュを実行するときに、メモリ コントローラがリフレッシュ サイクルを延期できるようにします。遅延リフレッシュ サイクルは、複数のリフレッシュ サイクルのバーストで実行される場合があります。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	Rowhammer スタイルの攻撃を軽減するために、この設定は**無効**のデフォルト状態のままにすることを推奨します。

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
APBDIS	SMU の APBDIS（アルゴリズム パフォーマンス ブースト（APB）無効化）値を選択できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、0、1 • **自動**：SMU の自動 ApbDis を設定します。これがデフォルトのオプションです。 • **0**：SMU への ApbDis をクリアします。 • **1**：SMU への ApbDis をセットします。	

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
ダウンコア制御	1 つ以上のコアの動作を停止する機能を提供します。シリコン回路でサポートされています。OS の制限、またはシステムの電力削減要件により、コア数を減らすことが望ましい場合があります。この項目により、実行中のコアの数を制御できます。この設定では、プロセッサで使用可能なコアの数を減らすことしかできません。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6		このトークンは、7xx2 および 7xx3 モデルのプロセッサを搭載したサーバーにのみ適用されます。

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
				自動、2（2+0）、2（1+1）、3（3+0）、6（3+3）、4（2+2）、4（2+0） • **自動**：有効化する必要のあるコアの数を CPU で判断します。これがデフォルトのオプションです。 • **2（2+0）/（1+1）**：片方の CPU コンプレックスで 2 つのコアを有効にします。 • **3（3+0）**：1 つの CPU コンプレックスで 3 つのコアを有効にします。 • **4（4+0）/（2+2）**：	

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
				1 つの CPU コンプレックスで 4 つのコアを有効にします。 • **6（3+3）**：1 つの CPU コンプレックスで 6 つのコアを有効にします。	
ストリーミングストア制御	ストリーミング ストア機能を有効にします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効	

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
固定された SOC P-State	このオプションは、APBDIS（アルゴリズム パフォーマンス ブースト（APB）無効化） が設定されている場合のターゲット P ステートを定義します。**P-x**は、取り付けられているプロセッサの有効な P ステートを指定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、P0、P1、P2、P3 • **自動**：プロセッサに適した有効な P 状態を設定します。これがデフォルトのオプションです。 • **P0 ～ P3**：最高の SOC P 状態から最低の SOC P 状態。	
DF C-State	システムで長時間のアイドル状態が予想される場合、この制御により、システムは、システムをさらに低電力状態に設定できる DF C ステートに移行できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効	
CCD制御	システムで有効にしたい電荷結合デバイス CCD の数を指定できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効	

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
[CPU ダウンコア制御（CPU Downcore control）]	1 つ以上のコアの動作を停止する機能を提供します。シリコン回路でサポートされています。OS の制限、またはシステムの電力削減要件により、コア数を減らすことが望ましい場合があります。この項目により、実行中のコアの数を制御できます。この設定では、プロセッサで使用可能なコアの数を減らすことしかできません。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効	

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
[CPU SMT モード（CPU SMT Mode）]	同時マルチスレッド化（SMT）は、複数の命令ストリーム（スレッド）を同じ物理プロセッサー上で同時に実行できるようにするプロセッサテクノロジーであり、全体的なスループットを向上させます。	4.2(1)	C225 M6, C245 M6	無効、**有効**	
NUMAドメインとしてのACPI SRAT L3キャッシュ	各CCXがそのオン ドメインにあると宣言されている物理ドメインの上に仮想ドメインのレイヤーを作成します。	4.2(1)	C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効	
[チャネルインターリーブ（Channel Interleaving）]	CPUがメモリブロックを分割して、インターリーブされたチャネル間にデータの連続部分を分散し、同時読み取り動作を有効にするかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべてのM5サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、片道から四方	

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
Cisco xGMIの最大速度	このオプションは、18 Gbps XGMI リンク速度を有効にします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[クローズドループ サーマル スロットリング（Closed Loop Thermal Throttling）]	クローズドループ サーマル スロットリングを構成するには	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[プロセッサ CMCI（Processor CMCI）]	CMCI の生成を有効にします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[TDP 構成（Config TDP）]	TDP を構成するには。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
設定可能な TDPレベル	熱設計出力（TDP）のカスタマイズされた値を設定できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**通常**、レベル 1、レベル 2	

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
Core Multi Processing	パッケージ内の CPU ごとの論理プロセッサ コアの状態を設定します。値として [すべて（All）] を選択すると、Intel ハイパースレッディング テクノロジーも有効になります。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)、5.0(1)、5.0(2)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	**すべて**、1 ～ 64 • [All]：すべての論理プロセッサ コアの多重処理を有効にします。 • 1 ～64：サーバーで実行可能な CPU あたりの論理プロセッサ コアの数を指定します。マルチ プロセッシングを無効にして、サーバーで動作する CPU ごとの論理プロセッサ コアを 1 つのみにするには、[1] を選択します。	オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

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
[エネルギーパフォーマンス（Energy Performance）]	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを決定できるようにします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**パフォーマンス**、バランスの取れたパフォーマンス、バランスの取れたエネルギー、エネルギー効率	**電源テクノロジー** を**カスタム**に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[周波数フロアオーバーライド（Frequency Floor Override）]	アイドル状態のときに CPU を最大非ターボ周波数未満にすることができるかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[CPUパフォーマンス プロファイル（CPU Performance）]	サーバー設定を自動的に調整することによる CPU パフォーマンス。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[電源テクノロジー（Power Technology）]	Enhanced Intel Speedstep Technology、Intel ターボブースト テクノロジー、およびプロセッサ パワー ステート C6 の CPU 電源管理設定を構成できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、エネルギー効率、カスタム、パフォーマンス	

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
[スクラブを要求（Demand Scrub）]	CPU または I/O から読み取り要求があった時に発生したシングル ビット メモリ エラーを、システムで修正するかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[ダイレクト キャッシュ アクセスのサポート（Direct Cache Access Support）]	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュ ミスを減らすのに役立ちます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、無効、有効	
[DRAM クロック スロットリング（DRAM Clock Throttling）]	メモリ帯域幅と消費電力に関してシステム設定を調整できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、バランス、パフォーマンス、エネルギー効率	

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
[エネルギー効率ターボ（Energy Efficient Turbo）]	エネルギー効率の高いターボが有効になっている場合、CPU の最適なターボ周波数は、CPU 使用率に基づいてダイナミックになります。パワー/パフォーマンスのバイアス設定も、エネルギー効率の高いターボに影響します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[エネルギーパフォーマンスチューニング（Energy Performance Tuning）]	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	

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
[拡張 Intel Speedstep テクノロジー（Enhanced Intel Speedstep\（R\) Technology）]	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
プロセッサ EPPの有効化	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを決定できるようにします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[EPP プロファイル（EPP Profile）]	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを決定できるようにします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	

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
Execute Disable Bit	サーバーのメモリ領域を分類し、アプリケーションコードを実行可能な場所を指定します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効化します。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[ローカル X2 Apic（Local X2 Apic）]	Application Policy Infrastructure Controller（APIC）アーキテクチャ タイプを設定できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効、X2APIC、XAPIC	

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
[ハードウェアプリフェッチ（Hardware Prefetcher）]	プロセッサで、インテルハードウェアプリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[CPU ハードウェア パワー管理（CPU Hardware Power Management）]	プロセッサの Hardware Power Management（HWPM）を有効にします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、HWPM ネイティブモード、HWPM OOB モード	
[IMC インターリーブ（IMC Interleaving）]	この BIOS オプションは、Integrated Memory Controller（IMC）間のインターリーブを制御します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、1 方向インターリーブ、2 方向インターリーブ	

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 Dynamic Speed Select	Intel ダイナミック速度選択モードでは、ユーザーは自動モードで異なる速度とコアを使用して CPU を動作させることができます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、5.0(1)、5.0(2)	すべての M5 サーバー、B200 M6、X210C M6	**無効**、有効	
[インテル ハイパースレッディング テクノロジー（Intel HyperThreading Tech）]	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか設定します。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)	すべての M5 サーバー	**無効**、有効	

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
[インテル ターボ ブースト テクノロジー（Intel Turbo Boost Tech）]	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか設定します。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、	すべての M5 サーバー	**無効**、有効	
Intel(R) VT	Intel Virtualization Technology for Directed I/O（VT-R）をプロセッサで使用するかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)	すべての M5 サーバー	**無効**、有効	
[DCU IP プリフェッチ（DCU IP Prefetcher）]	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)	すべての M5 サーバー	**無効**、有効	

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
[KTI プリフェッチ（XPT Prefetch）]	KTI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。	4.0(2)、4.0(4)、4.1(1)、4.1(3)	すべての M5 サーバー	**無効**、有効	
LLC プリフェッチ（LLC Prefetch）	プロセッサが LLC プリフェッチ メカニズムを使用してデータを LLC にフェッチするかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー	**無効**、有効	
Intelメモリインターリーブ	メモリの更新中に別のメモリにアクセスできるように、CPU が物理メモリをインターリーブするかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)	すべての M5 サーバー	**無効**、有効	
[パッケージ C State リミット（Package C State Limit）]	アイドル時にサーバ コンポーネントが使用できる電力量を設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	**パッケージ C の状態制限**を変更する場合は、**電源テクノロジー**が**カスタム**に設定されていることを確認します。

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
[パトロールスクラブ（Patrol Scrub）]	フルメモリスキャンの間隔を設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6		間隔が短いほど、スクラブにより多くのメモリ帯域幅が使用されます。

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
				無効、有効 • 有効：システムは定期的にメモリを読み書きして ECC エラーを探します。エラーが見つかると、システムは修復を試みます。このオプションにより、単一ビットエラーは複数ビット エラーになる前に修正される場合がありますが、パトロールスクラブの実行時にパフォーマンスが低下する場合もあります。 • 無効：CPU がメモリ アド	

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
				レスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。	
[パトロール スクラブ間隔（Patrol Scrub Interval）]	システムに、5 ～ 23 時間間隔でサーバーのメモリ（未使用部分も含む）における単一ビット メモリ エラーを検出させて修復させるかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	プラットフォームのデフォルト	
[プロセッサ C1E（Processor C1E）]	C1 に入ってプロセッサが最低周波数に遷移できるようにします。この設定は、サーバをリブートするまで有効になりません。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	

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
[プロセッサ C3 レポート（Processor C3 Report）]	プロセッサからオペレーティング システムに C3 レポートを送信するかどうか。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効、ACPI C2、ACPI C3	
[プロセッサ C6 レポート（Processor C3 Report）]	プロセッサからオペレーティング システムに C6 レポートを送信するかどうか。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[CPU C State]	AMD プロセッサが IO ベースの C ステートジェネレーションおよび DF C ステートを制御するかどうかです。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	C225 M5、C245 M5、C225 M6、C245 M6	**自動**、無効、有効	
[P-State の調整（P-STATE Coordination)]	BIOS がオペレーティングシステムに P-state サポートモデルを伝達する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様では、次の 3 つのモデルが定義されています。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**SW All**、HW All、SW Any	**電源テクノロジー** を**カスタム**に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

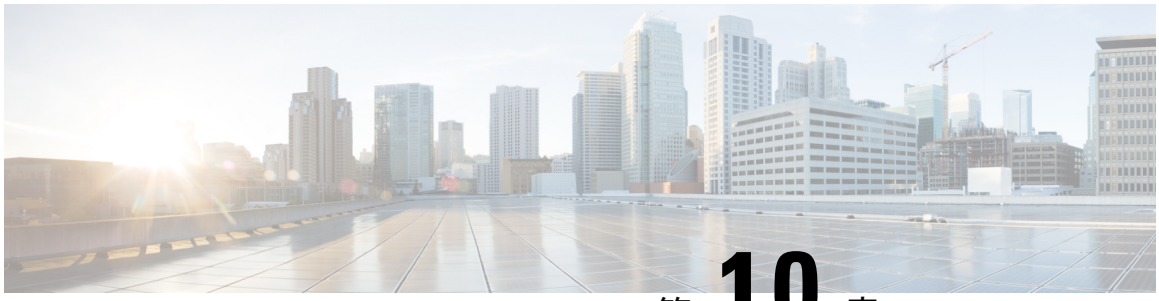
名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
[電力パフォーマンス調整（Power Performance Tuning）]	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	BIOS、**OS**、PECI	
UPI Link Frequency Select	拡張 APIC サポートをイネーブルまたはディセーブルにできます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)、5.0(1)、5.0(2)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	**自動**、9.6GT/S、10.4GT/S、11.2GT/S、12.8GT/s、14.4GT/s、16.0GT/s	
[ランク インターリーブ（Rank Interleaving）]	1 つのランクを更新中に別のランクにアクセスできるよう、CPU がメモリの物理ランクをインターリーブするかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**自動**、1 方向、2 方向、4 方向、8 方向	

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
[SMT モード（SMT Mode）]	プロセッサで AMD 同時マルチスレッディング（Simultaneous MultiThreading）テクノロジーを使用するかどうかを指定します。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[サブ NUMA クラスタリング（Sub Numa Clustering）]	CPU がサブ NUMA クラスタリングをサポートするかどうか設定します。そのクラスタリングでは、タグ ディレクトリとメモリ チャネルは常に同じ領域になります。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効、SNC2、SNC4	

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
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）]	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
[SVM モード（SMT Mode）]	プロセッサが AMD セキュア仮想マシン テクノロジを使用するかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
非コア周波数スケーリング	プロセッサの非コア部分の周波数のスケーリングを設定できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)、5.0(1)、5.0(2)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6、B200 M6、X210C M6	無効、**有効**	
[ワークロード設定（Workload Configuration）]	この機能を使用すると、ワークロードを最適化できます。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	平衡化、**I/O 重視**、NUMA、UMA	

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
[XPT プリフェッチ（XPT Prefetch）]	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリコントローラのプリフェッチャに発行するかどうか設定します。	4.0(2)、4.0(4)、4.1(1)、4.1(3)、4.2(1)	すべての M5 サーバー、C220 M6、C240 M6、C225 M6、C245 M6	**無効**、有効	
X2APICオプトアウト フラグ	OS が x2APIC で動作していないときに、OS が拡張 xAPIC（x2APIC）モードを有効にしないようにします。	4.2(3)	C220M6、C240M6、B200M6、X210C M6	**無効**、有効	

プロセッサ



第 10 章

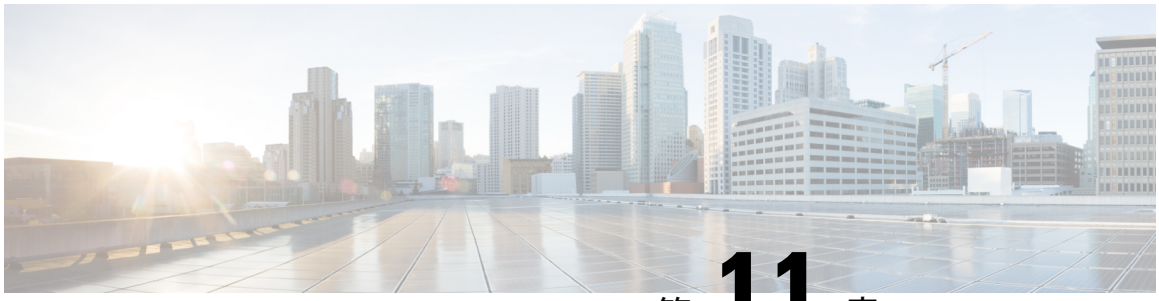
QPI

QPI

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができる QPI の BIOS 設定を示しています。

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
[QPI リンクの周波数選択（QPI Link Frequency Select）]	Intel QuickPath Interconnect（QPI）のリンク周波数で、MT/s（毎秒 100 万転送）単位で選択します。	4.0(4)、4.1(1)、4.1(3)、4.2(1)	C220 M5、C240 M5、B200 M5、C240 M6、C220 M6、C225 M6、C245 M6	自動、6.4 GT/s、7.2 GT/s、8.0 GT/s、9.6 GT/s	

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
[QPI スヌープモード（QPI Snoop Mode）]	いずれかのスヌープ モードで QPI を構成できます。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6	ホーム スヌープ、Cluster On Die、OSB 付きホームディレクトリ スヌープ、早期スヌープ、**自動** • [ホーム スヌープ（Home Snoop）]：スヌープは、常に、メモリ コントローラのホーム エージェント（集中型リング停止）によって起動されます。このモードは、早期スヌープよりローカル遅延が多くなりますが、未処理トランザクションが増えた場合に予備のリソースを使用できます。 • **Cluster On Die**：このモードは、コアが 10 以上のプロセッサでのみ使用できます。高度に NUMA 最適化されたワークロードに最適なモードです。 • [早期スヌープ（Early Snoop）]：分散キャッシュ リング停止で、別のキャッシング エージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータ セットを共有しているためにキャッシュ間転送からメリットが得られるワークロードや NUMA 最適化されていないワークロードに最適です。	



第 11 章

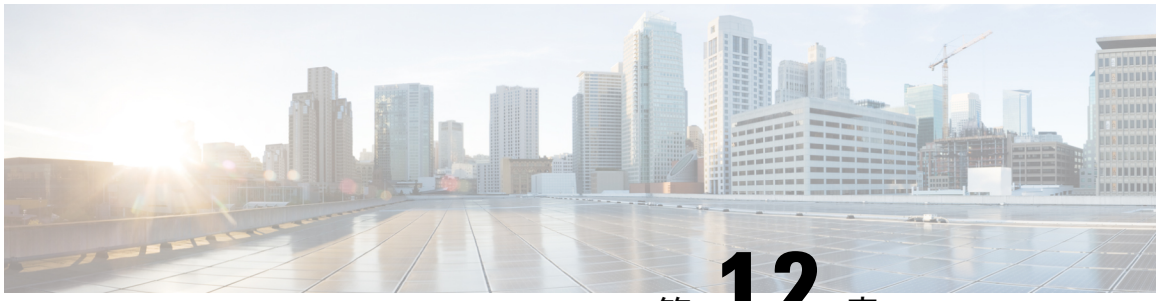
シリアルポート

シリアルポート

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シリアル ポートの 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
[シリアル A 有効化（Serial A Enable）]	シリアル ポート A を有効または無効にします。	4.2(1)	C225 M6、C245 M6、B200 M6、X210C M6	有効、無効	

シリアルポート



第 12 章

サーバ管理

サーバ管理

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サーバー管理 BIOS 設定の一覧を示します。

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[PERR 上の NMI アサート（Assert NMI on PERR）]	プロセッサバスパリティエラー（PERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうかを設定します。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6	**有効**、無効	
[SERR 上の NMI アサート（Assert NMI on SERR）]	システム エラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうかを設定します。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6	**有効**、無効	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[ボーレート（Baud Rate）]	シリアルポートの伝送速度として使用されるボーレート。[コンソールリダイレクション（Console Redirection）] を無効にした場合、このオプションを使用できません。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	9.6k、19.2k、38.4k、57.6k、**115.2k**	この設定は、リモートターミナルアプリケーション上の設定と一致している必要があります。
[コンシステントデバイスネーミング（Consistent Device Naming]）	一貫したデバイスの命名によって、一貫した方法でイーサネットインターフェイスに名前を付けることができます。これによりイーサネットインターフェイスの名前は、より統一され、識別しやすくなり、アダプタや他の設定に変更が加えられても永続的に保持されます。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6	有効、**無効**	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[適応型メモリトレーニング（Adaptive Memory Training）]	このトークンが有効になっているときに、BIOSはCPU/メモリ設定情報と共にメモリ トレーニング結果(最適化されたタイミング/電圧値) を保存し、それらをその後のリブートに再使用して、ブート時間を短縮します。保存済みメモリのトレーニング結果は、最後の保存操作後の24時間以内に、リブートが発生した場合にのみ使用されます。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6、X210C M6	**有効**、無効	
[BIOS Techlog レベル（BIOS Techlog Level）]	このオプションは、BIOS tech ログファイルのメッセージのタイプを示します。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6	最大、**最大**、標準 • 最小：重要なメッセージがログファイルに表示されます。これはデフォルトのオプションです。 • 最小：警告およびロード メッセージがログファイルに表示されます。 • 標準：標準に加え、情報関連のメッセージがログファイルに表示されます。	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[オプションROM起動最適化（OptionROM Launch Optimization）]	オプション ROM の起動は PCI スロット レベルで管理されます。デフォルトで有効になっています。多数のネットワークコントローラおよびオプション ROM をもつストレージHBAから成る設定では、すべてのオプションROMは、PCIスロットのオプション ROM コントロールがすべてに対して有効になっている場合に起動できます。ただし、ブート プロセスでは、コントローラのサブセットのみを使用できます。このトークンが有効になっているときに、ブートポリシーに存在するこれらのコントローラでのみ、オプションROMが起動されます。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6	**有効**、無効	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
コンソール リダイレクション（Console Redirection）	POST および BIOS のブート中に、シリアルポートをコンソール リダイレクションで使用できるようにします。BIOS のブートが完了し、オペレーティング システムがサーバーを担当すると、コンソール リダイレクションの関連性はなくなり、無効になります。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**無効**、COM0、COM1、serial-port-b プラットフォーム デフォルト • COM 0 は POST 中にコンソール リダイレクション用のシリアル ポートを有効にします。このオプションは M6 ブレード サーバーおよびラックマウント サーバーに対してのみ有効です。 • COM1 または serial-port-b はコンソール リダイレクション用にシリアル ポート B を有効にし、サーバー管理タスク実行を許可します。このオプションは、ラックマウント サーバーでのみ有効です。	このオプションを有効にする場合は、POST 中に表示される Quiet Boot のロゴ画面を無効にします。

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[フロー制御（Flow Control）]	フロー制御にハンドシェイクプロトコルを使用するかどうかを設定します。送信要求/クリアツーセンド（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレームコリジョンを減らすことができます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**なし**、RTC-CTS	この設定は、リモートターミナルアプリケーション上の設定と一致している必要があります。
[FRB-2 タイマー（FRB-2 Timer）]	POST 中にシステムがハングアップした場合に、システムを回復するために FRB2 タイマーを使用するかどうかを指定します。	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	
レガシーOSリダイレクト（Legacy OS Redirection）	シリアルポートでのレガシーなオペレーティングシステム（DOS など）からのリダイレクションをイネーブルにするかどうか設定します。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6	**有効**、無効	

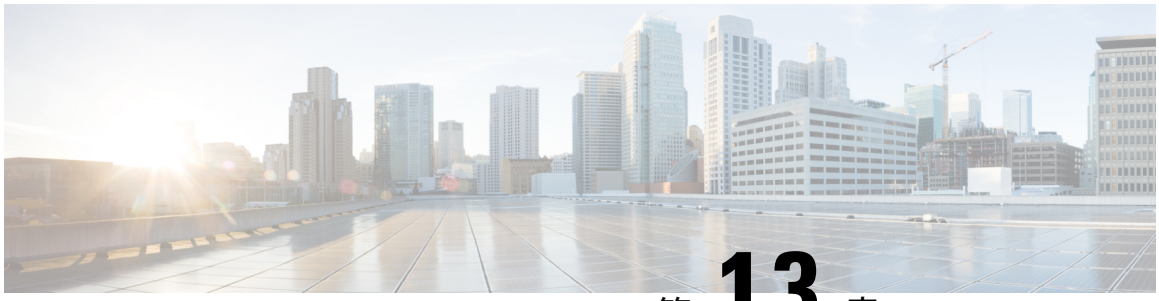
名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[OS ウォッチドッグ タイマー（OS Boot Watchdog Timer）]	BIOSが、定義済みのタイムアウト値を持つウォッチドッグタイマーをプログラムするかどうか設定します。タイマーが切れる前にオペレーティングシステムのブートが完了しないと、CIMC はシステムをリセットし、エラーがログに記録されます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**有効**、無効	
[OS Boot Watchdog Timer Policy	ウォッチドッグタイマーが切れた場合にシステムで実行されるアクション。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**電源オフ**、リセット	
[OS ブートウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout]）	BIOS でウォッチドッグタイマーの設定に使用されるタイムアウト値。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	5 分、**10 分**、15 分、20 分	
[アウトオブバンド管理ポート（Out-of-Band Mgmt Port）]	Windows の Special Administration Control（SAC）で使用。このオプションを使用すると、Windows 緊急管理サービスに使用できる COM ポート 0 を設定できます。このセットアップオプションに基づいてACPI SPCR テーブルが報告されます。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6	**有効**、無効	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[Putty キーパッド（Putty KeyPad）]	PuTTY ファンクションキーおよびテンキーの最上段のキーのアクションを変更できます。	4.2(1)	C240 M6、C220 M6、C225 M6、C245 M6		

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
				VT100、**Linux**、XTERMR6、SCO、ESCN、VT400 • [VT100]：ファンクション キーによって ESC OP ～ ESC O[を生成します。 • Linux：Linux 仮想コンソールに類似しています。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は ESC [[A ～ ESC [[E を生成します。 • [VT400]：ファンクション キーはデフォルト モードと同様に動作します。テンキーの最上段のキーによって ESC OP ～ ESC OS を生成します。 • [ESCN]：デフォルト モードです。ファンクション キーはデジタル端末の一般的な動作と一致します。	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
				ファンクションキーによってESC [11~ やESC [12~ などのシーケンスを生成します。 • SCO：ファンクションキー F1 ～ F12 は、ESC [M ～ ESC [X. を生成します。ファンクションキーとシフトキーは、ESC [Y ～ ESC [j を生成します。コントロールキーとファンクション キーは、ESC [k ～ ESC [v を生成します。シフト、コントロール、およびファンクションキーは、ESC [w ～ ESC [{ を生成します。	

名前	説明	サポートされている属性			
		バージョン	プラットフォーム	値	依存関係
[BIOS POST後のリダイレクション（Redirection After BIOS POST]）	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか設定します。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**常に有効**、ブートローダー • 常に有効：OS のブートおよび実行時に BIOS レガシー コンソール リダイレクションがアクティブになります。 • [Bootloader]：OS ブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションがディセーブルになります。	
[ターミナル タイプ（Terminal Type)]	コンソール リダイレクションに使用される文字フォーマットのタイプ。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	PC-ANSI、**VT100**、VT100-PLUS、VT-UTF8	この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。



第 13 章

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	

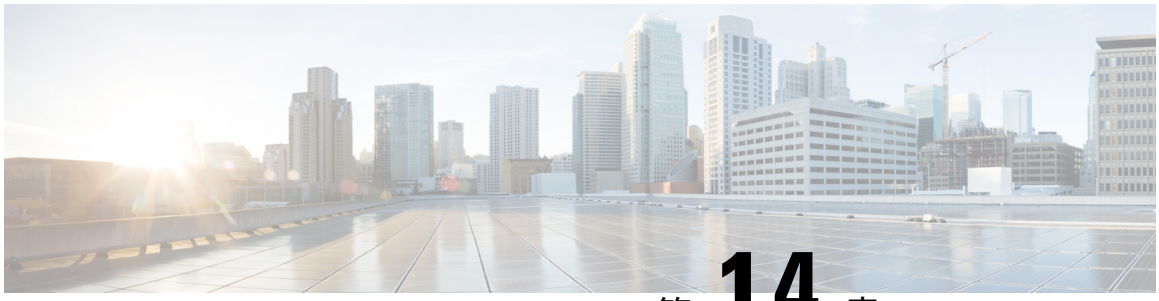
名前	説明	サポートされる属性			
		バージョン	プラットフォーム	値	依存関係
[SGX PubKey Hash *n*] *n* の範囲は 0 ～ 3 です。	ソフトウェア ガード拡張（SGX）の値を設定できます。	4.2(1)、5.0(1)、5.0(2)	C240 M6、C220 M6、C225 M6、C245 M6、B200 M6、X210C M6	**SGX PUBKEY HASH0**、SGX PUBKEY HASH1、SGX PUBKEY HASH2、SGX PUBKEY HASH3 • SGX PUBKEY HASH0 — 7 ～ 0 の間 • SGX PUBKEY HASH1 : 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	

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。

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
[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**	



第 14 章

USB

USB

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 USB 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
[すべての USB デバイス（All USB Devices）]	すべての物理および仮想 USB デバイスを有効にするか無効にするか。	4.2(1)	C220 M6、C240 M6、B200 M6、X210C M6	**有効**、無効	
[レガシー USB のサポート（Legacy USB Support）]	システムでレガシー USB デバイスをサポートするかどうか設定します。	4.2(1)、5.0(1)、5.0(2)	C220 M6、C240 M6、B200 M6、X210C M6	**自動**、有効、無効	
[デバイスをブート不可にする（Make Device Non Bootable）]	サーバが USB デバイスからブートできるかどうか設定します。	4.2(1)	C220 M5、C240 M5、C480 M5	**有効**、無効	
[xHCI モード（xHCI Mode）]	xHCI モードを有効または無効にします。	4.2(1)	C220 M5、C240 M5、C480 M5	**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
[ポート 60/40 エミュレーション（Port 60/64 Emulation）]	完全なUSBキーボードレガシー サポートのために60h/64hエミュレーションをシステムでサポートするかどうか設定します。	4.2(1)	C220 M5、C240 M5、C480 M5	有効、**無効**	サーバーでUSB非対応オペレーティングシステムを使用する場合は、このオプションを有効にする必要があります。
[USBポートフロント（USB Port Front）]	フロントパネルのUSBデバイスを有効または無効にします。	4.2(1)	C220 M5、C240 M5、C480 M5	**有効**、無効	
[USB ポート内部（USB Port Internal）]	内部USBデバイスを有効または無効にします。	4.2(1)	C220 M5、C240 M5、C480 M5	**有効**、無効	
[USB ポート KVM（USB Port KVM）]	USB ポート KVM デバイスを有効または無効にします。	4.2(1)	C220 M5、C240 M5、C480 M5	**有効**、無効	
[USB ポート リア（USB Port Rear）]	USB ポート背面デバイスを有効または無効にします。	4.2(1)	C220 M5、C240 M5、C480 M5	**有効**、無効	
[USB ポート SD カード（USB Port SD Card）]	SDカードドライブを有効または無効にします。	4.2(1)	C220 M5、C240 M5、C480 M5	**有効**、無効	
[USB ポート VMedia（USB Port VMedia）]	仮想メディア デバイスを有効または無効にします。	4.2(1)	C220 M5、C240 M5、C480 M5	**有効**、無効	
[XHCI レガシーサポート（XHCI Legacy Support）]	xHCIモードを有効または無効にします。	4.2(1)	C220 M5、C240 M5、C480 M5	**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。