サーバー モデル別 BIOS パラメータ

C220 M7 および C240 M7 サーバー

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the server.

Table 1: BIOS Parameters in I/O Tab

Name	Description
Reboot Host Immediately check box	If the Reboot Host Immediately check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.

サーバー モデル別 BIOS パラメータ

Name	Description
MLOM OptionROM drop-down list **set PcieSlotMLOMOptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the MLOM slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the MLOM slot.
MLOM Link Speed drop-down list **set PcieSlotMLOMLinkSpeed**	This option allows you to restrict the maximum speed of an adapter card installed in PCIe MLOM slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.
PCIe Slot*n* OptionROM drop-down list **set PcieSlot*n*OptionROM**	Whether the server can use the Option ROMs present in the PCIe card slot designated by *n*. This can be one of the following: • **Disabled**—Option ROM for slot *n* is not available. • **Enabled**—Option ROM for slot *n* is available.

Name	Description
PCIe Slot*n* Link Speed drop-down list **set PcieSlot*n*LinkSpeed**	System IO Controller *n* (SIOCn) add-on slot (designated by *n*) link speed. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**— The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
MRAID OptionROM drop-down list **set PcieSlotMRAIDOptionROM**	This options allows you to control the Option ROM execution of the MRAID PCIe adapter connected. This can be one of the following: • **Disabled**—Does not execute Option ROM of the MRAID PCIe adapter. • **Enabled**—Executes Option ROM of the MRAID PCIe adapter.
MRAID Link Speed drop-down list **set PcieSlotMRAIDLinkSpeed**	This option allows you to restrict the maximum speed of an MRAID adapter card installed. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.

サーバー モデル別 BIOS パラメータ

Name	Description
Front NVME-*n* OptionROM drop-down list **set PcieSlotFrontNvme*n*OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Front NVME-*n* Link Speed drop-down list **set PcieSlotFrontNvme*n*LinkSpeed**	Link speed for NVMe front slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.
PCIe Slot MSTOR RAID OptionROM drop-down list **set PcieSlotMSTORRAIDOptionROM**	Whether the server can use the Option ROMs present in the PCIe MSTOR RAID. This can be one of the following: • **Disabled**—Option ROM is not available. • **Enabled**—Option ROM is available.
Intel VTD Coherency Support drop-down list **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.

Name	Description
Intel VT for Directed IO drop-down list **set IntelVTD**	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
VMD Enable drop-down list **set VMDenable**	Intel Volume Management Device (VMD) is for PCIe NVMe SSDs that provides hardware logic to manage and aggregate NVMe SSDs. This can be one the following: • **Enabled**— Enables benefits like robust surprise hot-plug, status LED management. • **Disabled**— Disables the feature. Default value: **Disabled**. Refer Intel® Virtual RAID on CPU User Guide to configure VMD. **Note** VROC is not supported with Cisco UCS C-Series M7 servers.
PCIe RAS Support drop-down list **set PCIeRASSupport**	Whether PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Disabled**—PCIe RAS is not available on the slot. • **Enabled**—PCIe RAS is available on port.
USB Port Rear drop-down list **set UsbPortRear**	Whether the rear panel USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

サーバー モデル別 BIOS パラメータ

Name	Description
VGA Priority drop-down list **set VgaPriority**	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **OnBoard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **OffBoard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **OnBoardDisabled**—Priority is given to the PCIe Graphics adapter, and the onboard VGA device is disabled. The vKVM does not function when the onboard VGA is disabled.
IPV6 PXE Support drop-down list **set IPV6PXE**	Enables or disables IPv6 support for PXE. This can be one of the following • **disabled**—IPv6 PXE support is not available. • **enabled**—IPv6 PXE support is always available.
PCIe PLL SSC drop-down list **set PciePllSsc**	Enable this feature to reduce EMI interference by down spreading clock 0.5%. Disable this feature to centralize the clock without spreading. This can be one of the following: • **auto**—EMI interference is auto adjusted. **Disabled**—EMI interference is auto adjusted. • **ZeroPointFive**—EMI interference is reduced by down spreading the clock 0.5%.
Network Stack drop-down list **set NetworkStack**	This option allows you to monitor IPv6 and IPv4. This can be one of the following • **disabled**—Network Stack support is not available. **Note** When disabled, the value set for **IPV4 PXE Support** does not impact the system. • **enabled**—Network Stack support is always available.

Name	Description
IPV4 PXE Support drop-down list **set IPV4PXE**	Enables or disables IPv4 support for PXE. This can be one of the following • **disabled**—IPv4 PXE support is not available. • **enabled**—IPv4 PXE support is always available.
External SSC enable drop-down list **set EnableClockSpreadSpec**	This option allows you to reduce the EMI of your motherboard by modulating the signals it generates so that the spikes are reduced to flatter curves. This can be one of the following: • **Disabled**—Clock Spread Spectrum support is not available. • **Enabled**—Clock Spread Spectrum support is always available.
IPV4 HTTP Support drop-down list **set IPV4HTTP**	Enables or disables IPv4 support for HTTP. This can be one of the following: • **disabled**—IPv4 HTTP support is not available. • **enabled**—IPv4 HTTP support is always available.
IIO eDPC Support drop-down list **set EdpEn**	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal Error—eDPC is enabled only for fatal errors. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
IPV6 HTTP Support drop-down list **set IPV6HTTP**	Enables or disables IPv6 support for HTTP. This can be one of the following: • **disabled**—IPv6 HTTP support is not available. • **enabled**—IPv6 HTTP support is always available.

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *2 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	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。次のいずれかになります。 • [電源オフ（Power Off）]：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [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）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト **set BaudRate**	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。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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。
[フロー制御（Flow Control）] ドロップダウン リスト **set FlowCtrl**	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 セント（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。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） 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。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **set ConsoleRedir**	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。OS起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • **[COM 1]**：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **set TerminalType**	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。次のいずれかになります。 • [PC-ANSI]：PC-ANSI端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト **set PcieSlotsCdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。

名前	説明
[CDN コントロール（CDN Control）] ドロップダウン リスト **set cdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[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。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：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。 • [最大（Maximum）]：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。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *3*：*[*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウン リスト **set TPMControl**	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかになります。 • [Disabled]：サーバーはTPMを使用しません。 • [有効（Enabled）]：サーバはTPMを使用します。 （注） 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ください。
セキュリティ デバイス サポート（Security Device Support）] ドロップダウン リスト **set TpmSupport**	セキュリティ デバイスのサポートを有効にするには、TPM サポートを有効にする必要があります。次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：TPM が有効な場合、機能が有効になります。
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウン リスト **set SHA256PCRBank**	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA256 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA256 PCR バンクは BIOS で使用できます。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウン リスト **set SHA1PCRBank**	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA-1 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA-1 PCR バンクは BIOS で使用できます。

名前	説明
[TPM の最小限の物理的存在（TPM Minimal Physical Presence）] ドロップダウン リスト	このトークンを使用すると、TPM に推奨される Microsoft のデフォルト設定を適用できます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM 保留中の操作（TPM Pending Operation）] ドロップダウン リスト **set TPMPendingOperation**	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。次のいずれかになります。 • [None]：アクションなし。 • TpmClear：保留中の操作をクリアします。
[電源オン パスワード（Power On Password）] ドロップダウン リスト **set PowerOnPassword**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Intel Trusted Execution Technology サポート（Intel Trusted Execution Technology Support）] ドロップダウン リスト **set TXTSupport**	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[マルチキー トータル メモリ暗号化（Multikey Total Memory Encryption、MK-TME） ドロップダウン リスト **set EnableMktme**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[トータル メモリ暗号化（Total Memory Encryption、TME）] ドロップダウン リスト **set EnableTme**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 工場出荷時リセット（SGX Factory Reset）] ドロップダウン リスト **set SgxFactoryReset**	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。これにより、すべての登録データが削除されます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SWガード拡張（SW Guard Extensions、SGX）] ドロップダウン リスト **set EnableSgx**	ソフトウェア ガード拡張（SGX）機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[SGX QoS] ドロップダウン リスト **set SgxQoS**	SGX QoS を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX パッケージ情報インバンド アクセス（SGX Pkg info In-Band Access）] ドロップダウン リスト **set SgxPackageInfoInBandAccess**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 書き込み有効（SGX Write Enable）] ドロップダウン リスト **set SgxLeWr**	SGX 書き込み機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[所有者 EPOCH入力タイプ選択（Select Owner EPOCH input type）] ドロップダウン リスト **set EpochUpdate**	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。次のいずれかになります。 • **SGX 所有者 EPOCH 有効化（SGX Owner EPOCH activated）]**：現在の入力タイプを変更しません。 • **[新しいランダム所有者 EPOCH に変更（Change to New Random Owner EPOCHs）]**：EPOCH をシステムが生成したランダムな数値に変更します。 • **[手動ユーザー定義所有者 EPOCH（Manual User Defined Owner EPOCHs）]**：EPOCH シードをユーザーが入力した 16 進値に変更します。

名前	説明
[SProcessor Epoch*n*] フィールド **set SgxEpoch0**	*n* で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。
[SGX 自動 MP レジストレーション エージェント（SGX Auto MP Registration Agent）] ドロップダウン リスト **set SgxAutoRegistrationAgent**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX PUBKEY HASH*n*] フィールド **set SgxLePubKeyHash*n***	ソフトウェア ガード拡張（SGX）の値を設定できます。この値の設定範囲は、以下のとおりです。 • 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
[CPU PA を 46 ビットに制限（LIMIT CPU PA to 46 Bits）] ドロップダウン リスト **set CpuPaLimit**	Intel ® VT-d でこのオプションを有効にして、2019 OS でブートできるようにします。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）] ドロップダウン リスト	DMA 制御オプトイン フラグ：このトークンを有効にすると、オペレーティング システムは入出力メモリ管理ユニット（IOMMU）を有効にして、悪意のあるデバイスからの DMA 攻撃を防ぐことができます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *4: [*メモリ（***Memory***）*]* タブの ***BIOS*** パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：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。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

名前	説明
[NUMA] ドロップダウン リスト **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分的なキャッシュ行の節約（Partial Cache Line Sparing）] ドロップダウンリスト **set PartialCacheLineSparing**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト **set SelectPprType**	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト **set BmeDmaMitigation**	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） 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。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト **set PartialMirrorModeConfig**	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**: 部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**: 部分的なメモリ ミラーが無効になります。

名前	説明
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)] ドロップダウン リスト **set DCPMMFirmwareDowngrade**	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分ミラー *n* サイズ（GB）（Partial Mirror n Size in GB）] フィールド **set PartialMirrorValue1**	最初の部分メモリ ミラーのサイズ（GB）。 n = 1、2、または 3 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド **set PartialMirrorPercent**	4GB を超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド **set MemorySizeLimit**	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト **set NvmdimmPerformConfig**	ワークロードの動作に応じて、NVM ベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[CR QoS] ドロップダウンリスト **set CRQoS**	CR QoS 調整を選択できます。 次のいずれかになります。 • **[モード 1（Mode 1）]**： • **[モード 2（Mode 2）]**： • **[モード 0（Mode 0）]**：**[CR QoS]** 機能は無効です。

名前	説明
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト **set SnoopyModeForAD**	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRT メモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト **set CrfastgoConfig**	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **[最適化の有効化（Enable Optimization）]** • **[最適化の無効化（Disable Optimization）]** • **Auto**
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト **set MemoryRefreshRate**	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト **set SnoopyModeFor2LM**	NUMA に最適化されていないワークロードから far メモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト **set MemoryThermalThrottling**	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **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を使用してクローズドループ サーマル スロットリングを有効にします。
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト **set PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[UMA] ドロップダウンリスト **set UmaBasedClustering**	UMA 設定を設定できます。次のいずれかになります。 • Disable(All2All) • Hemisphere(2-clusters)

名前	説明
[拡張メモリ テスト（Enhanced Memory Test）] ドロップダウンリスト **set AdvancedMemTest**	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[eADR サポート（eADR Support）] ドロップダウンリスト **set EadrSupport**	拡張非同期 DRAM リフレッシュ（eADR）のサポートにより、CPU キャッシュに格納されているデータを永続メモリに移動するためのキャッシュ フラッシュ コマンドの待機期間を回避できます。これによりパフォーマンスが向上します。次のいずれかになります。 • **Disabled** • **有効化** • **Auto**
[揮発性メモリ モード（Volatile Memory Mode）] ドロップダウンリスト **set VolMemoryMode**	揮発性メモリ モードの設定は、BIOS が Intel® Optane™ PMem をサポートしている場合に表示されます。次のいずれかになります。 • **[1LM]**：このオプションは、Intel® Optane™ PMem を App-Direct モードで設定するために使用できます。 • **[2LM]**：このオプションにより、2LM は DDR4 メモリをキャッシュとして動作させることができます。

名前	説明
[アダプティブ リフレッシュ管理レベル（Adaptive Refresh Management Level）] ドロップダウン リスト **set AdaptiveRefreshMgmtLevel**	リフレッシュ管理設定は読み取り専用です。現用系 RFM により、コントローラは RFM レベルと呼ばれる追加の RFM しきい値設定を柔軟に選択できます。RFM レベルにより、コントローラが発行した RFM コマンドと、これらのコマンドの DRAM 内管理との調整が可能になります。 次のいずれかになります。 • **デフォルト (Default)** • **[レベル A（Level A）]** • **[レベル B（Level B）]** • **[レベル C（Level C）]**
[メモリ帯域幅ブースト（Memory Bandwidth Boost）] ドロップダウンリスト **set MemoryBandwidthBoost**	Intel® メモリ帯域幅ブーストは、Intel® Optane™ パーシステント メモリの機能であり、サーマル ヘッドルームが利用可能な場合に、ダイナミック レンジの電力と帯域幅を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[エラー チェック スクラブ（Error Check Scrub）] ドロップダウン リスト **set ErrorCheckScrub**	結果収集の有無にかかわらず、メモリ チェックを有効にすることができます。次のいずれかになります。 • **Disabled** • **[結果収集なしで有効化（Enabled without Result Collection）]** • **[結果収集ありで有効化（Enabled with Result Collection）]**

名前	説明
[ランク マージン ツール（Rank Margin Tool）] ドロップダウン リスト **set EnableRMT**	ランク マージン ツールが使用されているかどうか、およびマージン テスト（メモリ シーケンスと電圧信号をテストするもの）が実行されているかどうかを示します。次のいずれかになります。 • **Disabled** • **有効化**

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *5 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **set AdjacentCacheLinePrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。

名前	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **set HardwarePrefetch**	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。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト **set DcuStreamerPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。

名前	説明
[仮想 Numa（Virtual Numa）] ドロップダウン リスト **set VirtualNuma**	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。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト **set CPUPerformance**	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。

名前	説明
[LLC デッドライン（LLC Dead Line）] ドロップダウンリスト **set LLCALLoc**	CPU の非包括的キャッシュ スキームでは、MLC から削除された内容が 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（dead）]** 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。 この機能が無効の場合、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。 この機能が有効の場合、使用可能な空きスペースがある場合にデッドラインを LLC に書き込むことを LLC に許可します。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。 • **[自動（Auto）]**：CPU が LLC のデッドラインの割り当てを決定します。
[XPT リモート プリフェッチ（XPT Remote Prefetch） ドロップダウンリスト **set XPTRemotePrefetch**	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。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。 • **[自動（Auto）]**：CPU が機能を決定します。
[UPI リンク有効化（UPI Link Enablement）] ドロップダウンリスト **set UPILinkEnablement**	プロセッサが必要とする最小数の UPI リンクを有効にします。 次のいずれかになります。 • **1** • **2** • **Auto**

名前	説明
[強化 CPU パフォーマンス（Enhanced CPU Performance）] ドロップダウンリスト **set EnhancedCPUPerformance**	（注） この機能を有効にすると、**[電源特性の有効化（Enable Power Characterization）]** および **[パワーキャッピング（Power Capping）]** を有効にすることはできません。 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。 （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。 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、Barlow Pass DIMM を使用していないこと • Cisco UCS C220 M6 サーバーの DIMM モジュール サイズは 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 • サーバーに GPU カードが搭載されていないこと。 次のいずれかになります。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[自動（Auto）]**：Cisco IMC がサーバー設定を調整して、パフォーマンスを向上させることができます。
[C1 自動降格（C1 Auto Demotion）] ドロップダウンリスト **set C1AutoDemotion**	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。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

名前	説明
[UPI 電力管理（UPI Power Manangement）] ドロップダウンリスト **set UPIPowerManagement**	UPI 電力管理は、サーバーの電力を節約するために使用されます。 次のいずれかになります。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[自動（Auto）]**：機能は有効です。
[C1 自動降格解除（C1 Auto UnDemotion）] ドロップダウンリスト **set C1AutoUnDemotion**	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。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *6 : [プロセッサ（Processor）] タブの BIOS パラメータ*

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[拡張 APIC（Extended APIC）] ドロップダウンリスト **set LocalX2Apic**	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。次のいずれかになります。 • 有効：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト **set IntelVT**	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

名前	説明
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト **set ProcessorC1E**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト **set ExecuteDisable**	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • **[HW ALL]**：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • **[SW ALL]**：OS Power Manager によって、依存関係にある論理プロセッサ間の P-state を調整します。すべての論理プロセッサで遷移を開始します。

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト **set IntelTurboBoostTech**	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。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。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト **set UFSDisable**	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の **[非コア周波数スケーリング (Uncore Frequency Scaling)]** の固定の上限値と下限値が記されています。
[ブート パフォーマンス モード（Boot Performance Mode）] ドロップダウン リスト **set BootPerformanceMode**	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。次のいずれかになります。 • [Max Performance]：プロセッサの P-state 率は最大です • **[最大効率（Max Efficient）]**：プロセッサの P-state の比率が最小です。 • **[Intel NM による設定（Set by Intel NM）]**：値は自動的に設定されます。

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト **set ConfigTDPLevel**	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[SpeedStep（Pstates）] ドロップダウンリスト **set EnhancedIntelSpeedStep**	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。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 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。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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
[Processor CMCI] ドロップダウン リスト **set ProcessorCMCI**	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）] : CMCI が無効になります。 • [有効（有効）] : CMCI が有効になります。これはデフォルト値です。
[HyperThreading [All]] ドロップダウン リスト **set IntelHyperThread**	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。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。次のいずれかになります。 • [Disabled] : プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）] : プロセッサでの複数スレッドの並列実行を許可します。
[Workload Configuration] ドロップダウン リスト **set WorkLdConfig**	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **[バランス（Balanced）]** • **[I/O 重視（IO Sensitive）]**

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウン リスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • **[1] ～ [48]**：サーバーで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 （注） 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ください。
[UPI リンク周波数選択 (UPI Link Frequency Select)] ドロップダウン リスト **set QpiLinkSpeed**	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (Auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

名前	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト **set KTIPrefetch**	UPI 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。これは次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：プロセッサでキャッシュ データをプリロードしません。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャで最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。 • **[自動（Auto）]**：CPU が UPI プリフェッチ モードを決定します。
[Sub NUMA Clustering] ドロップダウンリスト **set SNC**	CPUがサブNUMAクラスタリングをサポートするかどうか。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あります。次のいずれかになります。 • [disabled][Disabled]：サブNUMAクラスタリングは発生しません。 • [enabled][Enabled]：サブ NUMAクラスタリングが発生します。
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト **set PwrPerfTuning**	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。 • **[BIOS]**：エネルギー効率の調整のためにBIOS を選択します。 • **[OS]**：エネルギーパフォーマンスの調整にOSを選択します。 • **[PECI]**：エネルギー パフォーマンス チューニング用のプラットフォーム環境制御インターフェースを選択します。

名前	説明
[XPT Prefetch] ドロップダウン リスト **set XPTPrefetch**	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。次のいずれかになります。 • [disabled][Disabled]：CPU はXPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPU はXPT プリフェッチ オプションを有効にします。

名前	説明
[パッケージのCステート（Package C State）] ドロップダウン リスト **set PackageCstateLimit**	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意の Cステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度を CPUが決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバーコンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。この場合、必要な電力はC1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、またはC3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C6 保持（C6 Retention）]：CPUのアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。

名前	説明
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウン リスト **set CpuEngPerfBias**	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ーで重要かどうかを判断できます。次のいずれかになります。 • —サーバではすべてのサーバ コンポーネントにフルパワーを常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • —サーバはすべてのサーバ コンポーネントに、パフォーマンスとパワーのバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバーコンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト **set CpuHWPM**	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPM がディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPM ネイティブモードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPM アウトオブボックスモードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）

名前	説明
[LLC Prefetch] ドロップダウン リスト **set LLCPrefetch**	プロセッサがLLCプリフェッチ メカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [enabled][Enabled]：LLC Prefetcherで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウン リスト **set AutoCCState**	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト **set EnergyEfficientTurbo**	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。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト **set PatrolScrub**	システムにサーバーのメモリ（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ことが可能です。次のいずれかになります。 • [Disabled]：CPU がメモリ アド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。 • [有効（Enabled）]：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。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト **set EPPProfile**	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ーで重要かどうかを判断できます。次のいずれかになります。 • Performance • Balanced Performance • Balanced Power • 電源

名前	説明
[Intel ダイナミック速度選択（Intel Dynamic Speed Select）] ドロップダウンリスト **set IntelDynamicSpeedSelect**	**[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** 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。次のいずれかになります。 • **[無効（Disabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が無効になっています。 • **[有効（Enabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が有効になっています。
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト **set IntelSpeedSelect**	**[Intel の速度選択（Intel Speed Select）]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本**): ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 3** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **[構成 4（Config 4）]** : ユーザーは **[構成 3（Config 3）]** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。

C220 M6 および C240 M6 サーバー

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the server.

サーバー モデル別 BIOS パラメータ

Table 7: BIOS Parameters in I/O Tab

Name	Description
Reboot Host Immediately check box	If the Reboot Host Immediately check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
MLOM OptionROM drop-down list **set PcieSlotMLOMOptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the MLOM slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the MLOM slot.
MLOM Link Speed drop-down list **set PcieSlotMLOMLinkSpeed**	This option allows you to restrict the maximum speed of an adapter card installed in PCIe MLOM slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.
PCIe Slot*n* OptionROM drop-down list **set PcieSlot*n*OptionROM**	Whether the server can use the Option ROMs present in the PCIe card slot designated by *n*. This can be one of the following: • **Disabled**—Option ROM for slot *n* is not available. • **Enabled**—Option ROM for slot *n* is available.

Name	Description
PCIe Slot*n* Link Speed drop-down list **set PcieSlot*n*LinkSpeed**	System IO Controller *n* (SIOCn) add-on slot (designated by *n*) link speed. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**— The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
Front NVME-*n* OptionROM drop-down list **set PcieSlotFrontNvme*n*OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Front NVME-*n* Link Speed drop-down list **set PcieSlotFrontNvme*n*LinkSpeed**	Link speed for NVMe front slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.

Name	Description
Rear NVME-*n* OptionROM drop-down list **set PcieSlotRearNvme*n*OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the rear SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Rear NVME-*n* Link Speed drop-down list **set PcieSlotRearNvme*n*LinkSpeed**	Link speed for NVMe rear slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.
Legacy USB Support drop-down list **set UsbLegacySupport**	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled**—USB devices are only available to EFI applications. • **Enabled**—Legacy USB support is always available. • **Auto**—Feature is is automatically assigned.
PCIe Slot MSTOR RAID OptionROM drop-down list **set PcieSlotMSTORRAIDOptionROM**	Whether the server can use the Option ROMs present in the PCIe MSTOR RAID. This can be one of the following: • **Disabled**—Option ROM is not available. • **Enabled**—Option ROM is available.

Name	Description
Intel VTD Coherency Support drop-down list **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT for Directed IO drop-down list **set IntelVTD**	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
VMD Enable drop-down list **set VMDenable**	Intel Volume Management Device (VMD) is for PCIe NVMe SSDs that provides hardware logic to manage and aggregate NVMe SSDs. This can be one the following: • **Enabled**— Enables benefits like robust surprise hot-plug, status LED management. • **Disabled**— Disables benefits like robust surprise hot-plug, status LED management. Default value: **Disabled**. Refer Intel® Virtual RAID on CPU User Guide and Intel® Virtual RAID on CPU (Intel® VROC) to configure VMD.

サーバー モデル別 BIOS パラメータ

Name	Description
	Details of VMD supported and unsupported ports for Cisco UCS C480 M5 servers: Cisco UCS C480 NVMe SKU (32 drive NVME System) • DMI connected ports 7, 8, and 23 do not support VMD. • All other twenty nine ports support VMD. Cisco UCS C480 Non-NVMe SKU • DMI connected ports 1, 2, and 18 do not support VMD. • Ports 7, 8, 9, 10, 15, 16, 17, 23, 24 support VMD.
Intel VTD ATS support drop-down list **set ATS**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.
LOM Port *n* OptionROM drop-down list **set LomOpromControlPort0**	Whether Option ROM is available on the LOM port slot *n*. This can be one of the following: • **Disabled**—Option ROM is not available on LOM port 1. • **Enabled**—Option ROM is available on LOM port 1.
PCIe RAS Support drop-down list **set PCIeRASSupport**	Whether PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Disabled**—PCIe RAS is not available on the slot. • **Enabled**—PCIe RAS is available on port.
All Onboard LOM Ports drop-down list **set AllLomPortControl**	Whether Option ROM is available on all LOM ports. This can be one of the following: • **Disabled**—Option ROM is disabled on all the ports. • **Enabled**—Option ROM is enabled on all the ports.

Name	Description
USB Port Rear drop-down list **set UsbPortRear**	Whether the rear panel USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
VGA Priority drop-down list **set VgaPriority**	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **OnBoard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **OffBoard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **OnBoardDisabled**—Priority is given to the PCIe Graphics adapter, and the onboard VGA device is disabled. The vKVM does not function when the onboard VGA is disabled.
IPV6 PXE Support drop-down list **set IPV6PXE**	Enables or disables IPv6 support for PXE. This can be one of the following • **disabled**—IPv6 PXE support is not available. • **enabled**—IPv6 PXE support is always available.
USB Port Internal drop-down list **set UsbPortInt**	Whether the internal USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.

サーバー モデル別 BIOS パラメータ

Name	Description
PCIe PLL SSC drop-down list **set PciePllSsc**	Enable this feature to reduce EMI interference by down spreading clock 0.5%. Disable this feature to centralize the clock without spreading. This can be one of the following: • **auto**—EMI interference is auto adjusted. **Disabled**—EMI interference is auto adjusted. • **ZeroPointFive**—EMI interference is reduced by down spreading the clock 0.5%.
Network Stack drop-down list **set NetworkStack**	This option allows you to monitor IPv6 and IPv4. This can be one of the following • **disabled**—Network Stack support is not available. **Note** When disabled, the value set for **IPV4 PXE Support** does not impact the system. • **enabled**—Network Stack support is always available.
IPV4 PXE Support drop-down list **set IPV4PXE**	Enables or disables IPv4 support for PXE. This can be one of the following • **disabled**—IPv4 PXE support is not available. • **enabled**—IPv4 PXE support is always available.
External SSC enable drop-down list **set EnableClockSpreadSpec**	This option allows you to reduce the EMI of your motherboard by modulating the signals it generates so that the spikes are reduced to flatter curves. This can be one of the following: • **Disabled**—Clock Spread Spectrum support is not available. • **Enabled**—Clock Spread Spectrum support is always available.
IPV4 HTTP Support drop-down list **set IPV4HTTP**	Enables or disables IPv4 support for HTTP. This can be one of the following: • **disabled**—IPv4 HTTP support is not available. • **enabled**—IPv4 HTTP support is always available.

Name	Description
IIO eDPC Support drop-down list **set EdpEn**	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal Error—eDPC is enabled only for fatal errors. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
IPV6 HTTP Support drop-down list **set IPV6HTTP**	Enables or disables IPv6 support for HTTP. This can be one of the following: • **disabled**—IPv6 HTTP support is not available. • **enabled**—IPv6 HTTP support is always available.

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *8 : [*サーバ管理（***Server Management***）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	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。次のいずれかになります。 • [電源オフ（Power Off）]：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [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）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト **set BaudRate**	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。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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。
[フロー制御（Flow Control）] ドロップダウン リスト **set FlowCtrl**	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 セント（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。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） 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。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **set ConsoleRedir**	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。OS起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • **[COM 1]**：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **set TerminalType**	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。次のいずれかになります。 • [PC-ANSI]：PC-ANSI端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト **set PcieSlotsCdnEnable**	（注） このオプションは、スロット 2 または 5 に Mellanox カードを搭載した Cisco UCS C240 M6 サーバーでのみ使用できます。 イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[CDN コントロール（CDN Control）] ドロップダウン リスト **set cdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[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。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：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。 • [最大（Maximum）]：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。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *9*：*[セキュリティ管理（Security Management）] タブの BIOS パラメータ*

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウンリスト **set SHA1PCRBank**	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA-1 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA-1 PCR バンクは BIOS で使用できます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウンリスト **set TPMControl**	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかになります。 • [Disabled]：サーバーはTPMを使用しません。 • [有効（Enabled）]：サーバはTPMを使用します。 （注） 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ください。
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）] ドロップダウンリスト	DMA 制御オプトイン フラグ：このトークンを有効にすると、オペレーティング システムは入出力メモリ管理ユニット（IOMMU）を有効にして、悪意のあるデバイスからの DMA 攻撃を防ぐことができます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM 保留中の操作（TPM Pending Operation）] ドロップダウンリスト **set TPMPendingOperation**	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。次のいずれかになります。 • [None]：アクションなし。 • TpmClear：保留中の操作をクリアします。

名前	説明
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウンリスト **set SHA256PCRBank**	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA256 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA256 PCR バンクは BIOS で使用できます。
[電源オン パスワード（Power On Password）] ドロップダウン リスト **set PowerOnPassword**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM の最小限の物理的存在（TPM Minimal Physical Presence）] ドロップダウンリスト	このトークンを使用すると、TPM に推奨される Microsoft のデフォルト設定を適用できます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Intel Trusted Execution Technology サポート（Intel Trusted Execution Technology Support）] ドロップダウン リスト **set TXTSupport**	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[マルチキー トータル メモリ暗号化（Multikey Total Memory Encryption、MK-TME） ドロップダウンリスト **set EnableMktme**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[トータル メモリ暗号化（Total Memory Encryption、TME）] ドロップダウンリスト **set EnableTme**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 工場出荷時リセット（SGX Factory Reset）] ドロップダウンリスト **set SgxFactoryReset**	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。これにより、すべての登録データが削除されます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SWガード拡張（SW Guard Extensions、SGX）] ドロップダウンリスト **set EnableSgx**	ソフトウェア ガード拡張（SGX）機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[SGX QoS] ドロップダウンリスト **set SgxQoS**	SGX QoS を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX パッケージ情報インバンド アクセス（SGX Pkg info In-Band Access）] ドロップダウンリスト **set SgxPackageInfoInBandAccess**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 書き込み有効（SGX Write Enable）] ドロップダウンリスト **set SgxLeWr**	SGX 書き込み機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[所有者 EPOCH入力タイプ選択（Select Owner EPOCH input type）] ドロップダウンリスト **set EpochUpdate**	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。次のいずれかになります。 • **SGX 所有者 EPOCH 有効化（SGX Owner EPOCH activated）]**：現在の入力タイプを変更しません。 • **[新しいランダム所有者 EPOCH に変更（Change to New Random Owner EPOCHs）]**：EPOCH をシステムが生成したランダムな数値に変更します。 • **[手動ユーザー定義所有者 EPOCH（Manual User Defined Owner EPOCHs）]**：EPOCH シードをユーザーが入力した 16 進値に変更します。

名前	説明
[SProcessor Epoch*n*] フィールド **set SgxEpoch0**	*n* で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。
[SGX 自動 MP レジストレーション エージェント（SGX Auto MP Registration Agent）] ドロップダウンリスト **set SgxAutoRegistrationAgent**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX PUBKEY HASH*n*] フィールド **set SgxLePubKeyHash*n***	ソフトウェア ガード拡張（SGX）の値を設定できます。この値の設定範囲は、以下のとおりです。 • 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
[CPU PA を 46 ビットに制限（LIMIT CPU PA to 46 Bits）] ドロップダウンリスト **set CpuPaLimit**	Intel ® VT-d でこのオプションを有効にして、2019 OS でブートできるようにします。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

サーバー モデル別 BIOS パラメータ

表 *10 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：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。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

名前	説明
[NUMA] ドロップダウン リスト **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[パーシャル キャッシュ ライン スペアリング（Partial Cache Line Sparing）] ドロップダウン リスト **set PartialCacheLineSparing**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト **set SelectPprType**	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト **set BmeDmaMitigation**	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） 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。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト **set PartialMirrorModeConfig**	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**: 部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**: 部分的なメモリ ミラーが無効になります。

名前	説明
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)] ドロップダウン リスト **set DCPMMFirmwareDowngrade**	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分ミラー *n* サイズ（GB）（Partial Mirror n Size in GB）] フィールド **set PartialMirrorValue1**	最初の部分 *nth* メモリ ミラーのサイズ（GB）。 n = 1、2、または 3 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド **set PartialMirrorPercent**	4GB を超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド **set MemorySizeLimit**	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト **set NvmdimmPerformConfig**	ワークロードの動作に応じて、NVM ベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[CR QoS] ドロップダウンリスト **set CRQoS**	CR QoS 調整を選択できます。 次のいずれかになります。 • **[モード 1（Mode 1）]**： • **[モード 2（Mode 2）]**： • **[モード 0（Mode 0）]**：**[CR QoS]** 機能は無効です。

名前	説明
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト **set SnoopyModeForAD**	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRT メモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト **set CrfastgoConfig**	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **[最適化の有効化（Enable Optimization）]** • **[最適化の無効化（Disable Optimization）]** • **Auto**
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト **set MemoryRefreshRate**	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト **set SnoopyModeFor2LM**	NUMA に最適化されていないワークロードから far メモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト **set MemoryThermalThrottling**	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **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を使用してクローズドループ サーマル スロットリングを有効にします。
[パニックと高水準点（Panic and High Watermark）] ドロップダウン リスト **set PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[UMA] ドロップダウン リスト **set UmaBasedClustering**	UMA 設定を設定できます。次のいずれかになります。 • Disable(All2All) • Hemisphere(2-clusters)

名前	説明
[高度なメモリ テスト（Advanced Memory Test）] ドロップダウン リスト **set AdvancedMemTest**	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[eADR サポート（eADR Support）] ドロップダウン リスト **set EadrSupport**	拡張非同期 DRAM リフレッシュ（eADR）のサポートにより、CPU キャッシュに格納されているデータを永続メモリに移動するためのキャッシュ フラッシュ コマンドの待機期間を回避できます。これによりパフォーマンスが向上します。次のいずれかになります。 • **Disabled** • **有効化** • **Auto**
[揮発性メモリ モード（Volatile Memory Mode）] ドロップダウン リスト **set VolMemoryMode**	揮発性メモリ モードの設定は、BIOS が Intel® Optane™ PMem をサポートしている場合に表示されます。次のいずれかになります。 • **[1LM]**：このオプションは、Intel® Optane™ PMem を App-Direct モードで設定するために使用できます。 • **[2LM]**：このオプションにより、2LM は DDR4 メモリをキャッシュとして動作させることができます。

名前	説明
[メモリ帯域幅ブースト（Memory Bandwidth Boost）] ドロップダウン リスト **set MemoryBandwidthBoost**	Intel® メモリ帯域幅ブーストは、Intel® Optane™ パーシステント メモリの機能であり、サーマル ヘッドルームが利用可能な場合に、ダイナミック レンジの電力と帯域幅を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *11 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **set AdjacentCacheLinePrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。

名前	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **set HardwarePrefetch**	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。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト **set DcuStreamerPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。

名前	説明
[仮想 Numa（Virtual Numa）] ドロップダウン リスト **set VirtualNuma**	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。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト **set CPUPerformance**	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。

名前	説明
[LLC デッド ライン（LLC Dead Line）] ドロップダウン リスト **set LLCALLoc**	CPU の非包括的キャッシュ スキームでは、MLC から削除された内容が 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（dead）]** 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。 この機能が無効の場合、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。 この機能が有効の場合、使用可能な空きスペースがある場合にデッドラインを LLC に書き込むことを LLC に許可します。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。 • **[自動（Auto）]** — CPU が LLC のデッド ラインの割り当てを決定します。
[XPT リモート プリフェッチ（XPT Remote Prefetch） ドロップダウン リスト **set XPTRemotePrefetch**	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。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。 • **[自動（Auto）]** — CPU が機能を決定します。
[UPI リンク有効化（UPI Link Enablement）] ドロップダウン リスト **set UPILinkEnablement**	プロセッサが必要とする最小数の UPI リンクを有効にします。 次のいずれかになります。 • **1** • **2** • **Auto**

名前	説明
[強化 CPU パフォーマンス（Enhanced CPU Performance）] ドロップダウン リスト **set EnhancedCPUPerformance**	（注） この機能を有効にすると、**[電源特性の有効化（Enable Power Characterization）]**および**[パワーキャッピング（Power Capping）]**を有効にすることはできません。 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。 （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。 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、Barlow Pass DIMM を使用していないこと • Cisco UCS C220 M6 サーバーの DIMM モジュール サイズは 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 • サーバーにGPUカードが搭載されていないこと。 次のいずれかになります。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[自動（Auto）]** — Cisco IMC がサーバー設定を調整して、パフォーマンスを向上させることができます。
[C1 自動降格（C1 Auto Demotion）] ドロップダウン リスト **set C1AutoDemotion**	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。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

名前	説明
[UPI 電力管理（UPI Power Manangement）] ドロップダウン リスト **set UPIPowerManagement**	UPI 電力管理は、サーバーの電力を節約するために使用されます。 次のいずれかになります。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[自動（Auto）]** — 機能は有効です。
[C1 自動降格解除（C1 Auto UnDemotion）] ドロップダウン リスト **set C1AutoUnDemotion**	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。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[有効（Enabled）]** — 機能は有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *12 : [プロセッサ（Processor）] タブの BIOS パラメータ*

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[拡張 APIC（Extended APIC）] ドロップダウンリスト **set LocalX2Apic**	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。次のいずれかになります。 • 有効：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト **set IntelVT**	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

名前	説明
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト **set ProcessorC1E**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト **set ExecuteDisable**	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • **[HW ALL]**：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • **[SW ALL]**：OS Power Manager によって、依存関係にある論理プロセッサ間の P-state を調整します。すべての論理プロセッサで遷移を開始します。

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト **set IntelTurboBoostTech**	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。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。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト **set UFSDisable**	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の **[非コア周波数スケーリング (Uncore Frequency Scaling)]** の固定の上限値と下限値が記されています。
[ブート パフォーマンス モード（Boot Performance Mode）] ドロップダウン リスト **set BootPerformanceMode**	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。次のいずれかになります。 • [Max Performance]：プロセッサの P-state 率は最大です • **[最大効率（Max Efficient）]**：プロセッサの P-state の比率が最小です。 • **[Intel NM による設定（Set by Intel NM）]**：値は自動的に設定されます。

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト **set ConfigTDPLevel**	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[SpeedStep（Pstates）]ドロップダウンリスト **set EnhancedIntelSpeedStep**	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。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 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。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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
[Processor CMCI] ドロップダウン リスト **set ProcessorCMCI**	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。
[HyperThreading [All]] ドロップダウン リスト **set IntelHyperThread**	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。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。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。
[Workload Configuration] ドロップダウン リスト **set WorkLdConfig**	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **[バランス（Balanced）]** • **[I/O 重視（IO Sensitive）]**

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウン リスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • **[1] ～ [48]**：サーバーで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 （注） 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ください。
[UPI リンク周波数選択 (UPI Link Frequency Select)] ドロップダウン リスト **set QpiLinkSpeed**	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (Auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

名前	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト **set KTIPrefetch**	UPI 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。これは次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：プロセッサでキャッシュ データをプリロードしません。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャで最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。 • **[自動（Auto）]**：CPU が UPI プリフェッチ モードを決定します。
[Sub NUMA Clustering] ドロップダウンリスト **set SNC**	CPUがサブNUMA クラスタリングをサポートするかどうか。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あります。次のいずれかになります。 • [disabled][Disabled]：サブ NUMAクラスタリングは発生しません。 • [enabled][Enabled]：サブ NUMAクラスタリングが発生します。
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト **set PwrPerfTuning**	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。 • **[BIOS]**：エネルギー効率の調整のためにBIOS を選択します。 • **[OS]**：エネルギーパフォーマンスの調整にOSを選択します。 • **[PECI]**：エネルギー パフォーマンス チューニング用のプラットフォーム環境制御インターフェースを選択します。

名前	説明
[XPT Prefetch] ドロップダウン リスト **set XPTPrefetch**	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。次のいずれかになります。 • [disabled][Disabled]：CPU はXPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPU はXPT プリフェッチ オプションを有効にします。

名前	説明
[パッケージのCステート（Package C State）] ドロップダウン リスト **set PackageCstateLimit**	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意の Cステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度を CPUが決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバーコンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。この場合、必要な電力はC1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、またはC3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C6 保持（C6 Retention）]：CPUのアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。

名前	説明
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウン リスト **set CpuEngPerfBias**	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ーで重要かどうかを判断できます。次のいずれかになります。 • ―サーバではすべてのサーバ コンポーネントにフルパワーを常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • ―サーバはすべてのサーバ コンポーネントに、パフォーマンスとパワーのバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバーコンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト **set CpuHWPM**	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPM がディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPM ネイティブモードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPM アウトオブボックスモードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）

名前	説明
[LLC Prefetch] ドロップダウン リスト **set LLCPrefetch**	プロセッサがLLCプリフェッチメカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [enabled][Enabled]：LLC Prefetcherで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウン リスト **set AutoCCState**	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト **set EnergyEfficientTurbo**	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。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト **set PatrolScrub**	システムにサーバーのメモリ（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ことが可能です。次のいずれかになります。 • [Disabled]：CPU がメモリ アド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。 • [有効（Enabled）]：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。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト **set EPPProfile**	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ーで重要かどうかを判断できます。次のいずれかになります。 • Performance • Balanced Performance • Balanced Power • 電源

名前	説明
[Intel ダイナミック速度選択（Intel Dynamic Speed Select）] ドロップダウンリスト **set IntelDynamicSpeedSelect**	**[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** 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。次のいずれかになります。 • **[無効（Disabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が無効になっています。 • **[有効（Enabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が有効になっています。
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト **set IntelSpeedSelect**	**[Intel の速度選択（Intel Speed Select）]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本)**: ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 3** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **[構成 4（Config 4）]** : ユーザーは **[構成 3（Config 3）]** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。

C225 M6 および C245 M6 サーバー

[I/O] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *13 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[MLOM OptionROM] ドロップダウン リスト **set PcieSlotMLOMOptionROM**	このオプションでは、MLOM スロットに接続された 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。次のいずれかになります。 • [無効（Disabled）] : MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）] : MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[MLOM リンク速度（MLOM Link Speed）] ドロップダウン リスト **set PcieSlotMLOMLinkSpeed**	このオプションを使用すると、PCIe MLOM スロット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。次のいずれかになります。 • [無効（Disabled）] : 最大スピードは制限されていません。 • [自動（Auto）] : システムは許可される最大速度を選択します。 • [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。 • [GEN2] : 最大 5 GT/s までの速度が許可されます。 • [GEN3] : 最大 8 GT/s までの速度が許可されます。 • **[GEN3]** : 最大 16GT/s までの速度が許可されます。

名前	説明
[PCIe Slot*n* OptionROM] ドロップダウン リスト **set PcieSlot*n*OptionROM**	サーバーが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト **set PcieSlot*n*LinkSpeed**	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
MRAID OptionROM **set PcieSlotMRAID*n*OptionROM**	サーバーが *n* で指定された PCIe カード スロット内の RAID オプションの ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。

名前	説明
[MRAID リンク速度（MRAID Link Speed）] ドロップダウン リスト **set PcieSlotMRAID*n*LinkSpeed**	RAID IO コントローラ *n*（SIOCn）アドオン スロット（*n*によって指定）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[前面 NVME-*n* OptionROM（Front NVME-n OptionROM）] ドロップダウン リスト **set PcieSlotFrontNvme*n*OptionROM**	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。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します

名前	説明
[前面 NVME *n*リンク速度（Front NVME n Link Speed）] [ドロップダウン リスト（drop-down list）] **set PcieSlotFrontNvme*n*LinkSpeed**	スロット *n* で指定された NVMe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[背面 NVME-*n* OptionROM（Rear NVME-n OptionROM）] ドロップダウンリスト **set PcieSlotRearNvme*n*OptionROM**	（注） このオプションは、Cisco UCS C245 M6 サーバーにのみ適用されます。 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。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します

名前	説明
Rear NVME *n* Link Speed [ドロップダウンリスト（drop-down list）] **set PcieSlotRearNvme*n*LinkSpeed**	（注） このオプションは、Cisco UCS C245 M6 サーバーにのみ適用されます。 スロット *n* で指定された NVMe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト **set PcieSlotMSTORRAIDOptionROM**	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • 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。

名前	説明
[PCIe Slot MSTOR リンク速度（PCIe Slot MSTOR Link Speed）] ドロップダウンリスト **set PcieSlotMSTORRAIDLinkSpeed**	スロット *n* で指定された PCIe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト **set IPV6PXE**	PXE の IPv6 サポートを有効または無効にします。次のいずれかになります • **[無効 (disabled)]** : PV6 PXE のサポートは利用できません。 • **[enabled (有効)]**:IPV6 PXE のサポートを常に利用できます。
[IPV4 PXE サポート (IPV4 PXE Support)] ドロップダウン リスト **set IPV4PXE**	PXE の IPv4 サポートを有効または無効にします。次のいずれかになります • **[無効 (disabled)]**: IPV4 PXE のサポートは利用できません。 • **[enabled (有効)]**: IPV4 PXE のサポートを常に利用できます。

名前	説明
[PCIe ARI サポート (PCIe ARI Support)] ドロップダウン リスト **set PcieARISupport**	Windows での PCI 代替ルーティング ID 解釈（ARI）サポートが有効になっているかどうか。次のいずれかになります。 • **[自動（auto）]**：ARI サポートは、システムによって自動制御されるように設定されます。 • **[無効（disabled）]**：ARI サポートは使用できません。 • **[有効（enabled）]**：ARI サポートを常に使用できます。
[SR-IOVサポート（SR-IOV Support）] ドロップダウン リスト **set SrIov**	SR-IOV 機能により、PCIe デバイスは複数の個別の物理 PCIe デバイスのように見えます。次のいずれかになります。 • **[無効（Disabled）]**：SR-IOV 機能は無効です。 • **[有効（Enabled）]**：SR-IOV 機能は有効です。
[IPv6 HTTP サポート（IPv6 HTTP Support）] ドロップダウン リスト **set IPV6HTTP**	HTTP の IPv6 サポートを有効または無効にします。次のいずれかになります。 • **[無効（disabled）]**：IPv6 HTTP サポートは使用できません。 • **[有効（enabled）]**：IPv6 HTTP サポートを常に使用できます。
[IPV4 HTTP サポート（IPV4 HTTP Support）] ドロップダウン リスト **set IPV4HTTP**	HTTP の IPv4 サポートを有効または無効にします。次のいずれかになります。 • **[無効（disabled）]**：IPv4 HTTP サポートは使用できません。 • **[有効（enabled）]**：IPv4 HTTP サポートを常に使用できます。

名前	説明
[Network Stack (ネットワーク スタック)] ドロップダウン リスト **set NetworkStack**	このオプションでは、IPv6 と IPv4 をモニタできます。次のいずれかになります • **[無効 (disabled)]**: ネットワーク スタックのサポートは使用できません。 （注） 無効にすると、 **IPV4 PXE サポート**に設定された値はシステムに影響しません。 • **[enabled (有効)]**: ネットワーク スタックのサポートを常に利用できます。

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *14 : [*サーバ管理（***Server Management***）*]* タブの ***BIOS*** パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	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。次のいずれかになります。 • [電源オフ（Power Off）] : OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset] : OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

名前	説明
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [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）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト **set BaudRate**	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。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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。
[フロー制御（Flow Control）] ドロップダウン リスト **set FlowCtrl**	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 セント（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。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） 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。

サーバー モデル別 BIOS パラメータ

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **set ConsoleRedir**	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。OS起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：POST 中に COM 1 でコンソール リダイレクションを有効にします。 • **[COM 1]**：POST 中に COM 1 でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **set TerminalType**	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。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト **set PcieSlotsCdnEnable**	（注） このオプションは、スロット 2 または 5 に Mellanox カードを搭載した Cisco UCS C245 M6 サーバーでのみ使用できます。 イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[CDN コントロール（CDN Control）] ドロップダウン リスト **set cdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）] **set CiscoOpromLaunchOptimization**	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）] **set CiscoDebugLevel**	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。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：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。 • [最大（Maximum）]：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。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *15 : [*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウンリスト **set TPMControl**	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかになります。 • [Disabled]：サーバーはTPMを使用しません。 • [有効（Enabled）]：サーバはTPMを使用します。 （注） 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ください。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウンリスト **set SHA1PCRBank**	SHA-1 PCRバンクを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：サーバーはこの機能を使用しません。 • **[有効（Enabled）]**：サーバーはこの機能を使用します。
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウンリスト **set SHA256PCRBank**	SHA256 PCR バンクを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：サーバーはこの機能を使用しません。 • **[有効（Enabled）]**：サーバーはこの機能を使用します。

名前	説明
[電源オン パスワード（Power On Password）] ドロップダウン リスト **set PowerOnPassword**	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。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *16 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しいBIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[ソケットごとのNUMAノード（NUMA Nodes per Socket）] ドロップダウンリスト **set CbsDfCmnDramNps**	ソケットごとにメモリNUMAドメインを構成できます。次のいずれかになります。 • **[自動（Auto）]**：チャネル数を自動に設定します。 • **[NPS0]**：システムごとのNUMAノード数を1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、SoCの左半分と右半分に1つずつにします。 • **[NPS4]**：ソケットごとのNUMAノード数を4にし、クワドラントごとに1つにします。
[4 G以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB以上のMMIOを有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは64ビットPCIデバイスのI/Oを4 GB以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで64ビットPCIデバイスのI/Oを4 GB以上のアドレス空間にマッピングします。 （注） 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。

名前	説明
[Chipselect Interleaving] ドロップダウンリスト **set CbsCmnMemMapBankInterleaveDdr4**	ノード 0 に選択する 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。次のいずれかになります。 • **[無効（Disabled）]**：チップの選択は、メモリ コントローラ内でインターリーブされません。 • **[自動（Auto）]**：CPU でチップ セレクトのインタリーブの方法を自動的に決定します。
[メモリ インターリービング サイズ（Memory Interleaving Size）] ドロップダウンリスト **set CbsDfCmnMemIntlvSize**	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。次のいずれかになります。 • **Auto** • **256 バイト** • **512 バイト** • **1 KB** • **2 KB** • **4 KB**
[IOMMU] ドロップダウンリスト **set CbsCmnGnbNbIOMMU**	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。次のいずれかになります。 • **[自動（Auto）]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[無効（Disabled）]**：IOMMU は使用されません。 • **[有効（Enabled）]**：IOMMU によりアドレスマッピングを行います。

名前	説明
BankGroupSwap **set CbsCmnMemCtrlBankGroupSwapDdr4**	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。次のいずれかになります。 • **[自動（Auto）]**：アプリケーションへの物理アドレスの割り当て方法を CPU で自動的に決定します。 • **[無効（Disabled）]**：バンク グループ スワップは使用されません。 • **[有効（Enabled）]**：バンク グループ スワップによりアプリケーションのパフォーマンスを向上させます。
[TSME] ドロップダウンリスト **set TSME**	透過的セキュア メモリ暗号化（TSME）を有効にすることができます。次のいずれかになります。 • **[自動（Auto）]**：機能の使用は自動に設定されます。 • **[無効（Disabled）]**：プロセッサで TSME 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで TSME 機能を使用します。
[SMEE] ドロップダウンリスト **set CbsCmnCpuSmee**	プロセッサで、メモリの暗号化サポートを実現する Secure Memory Encryption Enable（SMEE）機能を使用するかどうかを指定します。次のいずれかになります。 • **[自動（Auto）]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[無効（Disabled）]**：プロセッサで SMEE 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで SMEE 機能を使用します。

名前	説明
[SNP メモリ カバレッジ（SNP Memory Coverage）] ドロップダウンリスト **set CbsDbgCpuSnpMemCover**	SNP メモリ カバレッジを設定できます。次のいずれかになります。 • **[自動（Auto）]**：システムがメモリ カバレッジを決定します。 • **[無効（Disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（Enabled）]**：この機能は有効です。 • **[カスタム（Custom）]**：カスタム サイズは、**[カバーする SNP メモリ サイズ（SNP Memory Size to Cover）]** で定義できます。
[SEV-SNP サポート（SEV-SNP Support）] ドロップダウン リスト **set CbsSevSnpSupport**	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。次のいずれかになります。 • **[無効（Disabled）]**：プロセッサで SEV-SNP 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで SEV-SNP 機能を使用します。
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト **set BmeDmaMitigation**	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[カバーされる SNP メモリ サイズ（MB）（SNP Memory Size to Cover in MB）] フィールド **set CbsDbgCpuSnpMemSizeCover**	SNP メモリ サイズを設定できます。
バーストおよび遅延された更新（Burst and Postponed Refresh）] フィールド **set BurstAndPostponedRefresh**	• **[無効（disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（enabled）]**：プロセッサはこの機能を使用します。

名前	説明
[パッケージ修復のポスト（Post Package Repair）] フィールド **set PostPackageRepair**	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、ハード PPRをサポートしています。次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 • [Disabled]：サポートはディセーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *17 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[Core Performance Boost] ドロップダウンリスト **set CbsCmnCpuCpb**	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。次のいずれかになります。 • **[auto]**：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。 • **[disabled]**：CPU により自動的にブーストパフォーマンスが決定されます。

名前	説明
[Global C-state Control] ドロップダウンリスト **set CbsCmnCpuGlobalCstateCtrl**	AMD プロセッサが IO ベースの C ステートおよびDF Cステートを制御するかどうかに関係なく、これは次のうちいずれかになります。 • **[auto]**：CPU で IO ベースの C ステートの生成方法を自動的に決定します。 • **[disabled]**：グローバル C ステートの制御が無効になります。 • **[enabled]**：グローバル C ステートの制御が有効になります。
[L1 Stream HW Prefetcher] ドロップダウンリスト **set CbsCmnCpuL1StreamHwPrefetcher**	プロセッサで、AMD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、L1 キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [auto][Auto]：CPU は、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェアプリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェア プリフェッチャを使用します。
[L2 Stream HW Prefetcher] ドロップダウンリスト **set CbsCmnCpuL2StreamHwPrefetcher**	プロセッサで、AMDハードウェアプリフェッチャが必要に応じてメモリからデータおよび命令ストリームを取得し、L2 キャッシュに入れることを許可するかどうかを指定します。次のいずれかになります。 • [auto][Auto]：CPU は、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェアプリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェア プリフェッチャを使用します。

名前	説明
[Determinism Slider] ドロップダウンリスト **set CbsCmnDeterminismSlider**	AMDプロセッサにより動作方法を決定できます。次のいずれかになります。 • **[auto]**：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。 • **[performance]**：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。 • **[power]**：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。
[CPPC] ドロップダウンリスト **set CbsCmnGnbSMUCPPC**	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。 次のいずれかになります。 • **自動**：CPU はデフォルトの CPPC 設定を自動で使用します。 • **無効**：機能は無効です。 • **有効**：コラボレーティブ プロセッサ パフォーマンスが有効になっています。
[効率モードの有効（Efficiency Mode Enable）] ドロップダウン リスト **set CbsCmnEfficiencyModeEn**	効率に基づいて消費電力を設定できます。 次のいずれかになります。 • **自動**：CPU はデフォルトの設定を自動で使用します。 • **有効**：効率モードは有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *18 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[SVM Mode] ドロップダウンリスト **set SvmMode**	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。次のいずれかを選択できます。 • **[disabled]**：プロセッサで SVM テクノロジーを使用しません。 • **[enabled]**：プロセッサで SVM テクノロジーを使用します。
[SMT Mode] ドロップダウンリスト **set CbsCpuSmtCtrl**	プロセッサで AMD 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。次のいずれかになります。 • **[auto]**：プロセッサは、マルチスレッドの並列実行を許可します。 • **[**無効（**disabled**）**]**：プロセッサで SMT モードを使用しません。 • **[**有効（**enabled**）**]**：プロセッサで SMT モードを使用します。

名前	説明
[ダウンコア制御 7xx2（Downcore control 7xx2）] ドロップダウンリスト **set CbsCmnCpuGenDowncoreCtrl**	（注） このトークンは、7xx2 モデルのプロセッサを搭載した Tehama サーバーにのみ適用されます。 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。次のいずれかになります。 • **[auto]**：有効化する必要のあるコアの数を CPU で判断します。 • TWO（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。 • FOUR（2+2）：1 つの CPU コンプレックスで 4 つのコアを有効にします。 • SIX（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。

名前	説明
[CPU ダウンコア制御 7xx3（CPU Downcore control 7xx3） ドロップダウンリスト **set CbsCpuCoreCtrl**	（注） このトークンは、7xx3モデルのプロセッサを搭載した Tehama サーバーにのみ適用されます。 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。次のいずれかになります。 • **[auto]**：有効化する必要のあるコアの数をCPU で判断します。 • One（1+0）：1 つの CPU コンプレックスで 1 つのコアを有効にします。 • [TWO（2+0）]：片方の CPU コンプレックスのみで 2 つのコアを有効にします。 • [THREE（3+0）]：片方のCPUコンプレックスのみで 3 つのコアを有効にします。 • [FOUR（4+0）]：片方の CPU コンプレックスのみで 4 つのコアを有効にします。 • Five（5+0）：1 つの CPU コンプレックスで 5 つのコアを有効にします。 • SIX（6+0）：1 つの CPU コンプレックスで 6 つのコアを有効にします。 • SEVEN（7+0）：1 つの CPU コンプレックスで 7 つのコアを有効にします。

名前	説明
[固定 SOC P ステート（Fixed SOC P-State）] ドロップダウンリスト **set CbsCmnFixedSocPstate**	このオプションは、APBDIS が設定されている場合のターゲット PState を定義します。**P*x***：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。次のいずれかになります。 • P0 • P1 • P2 • P3 • 自動（Auto）
[APBDIS] ドロップダウンリスト **set CbsCmnApbdis**	SMU の APB 無効化の値を選択できます。次のいずれかになります。 • **0**：SMU への ApbDis をクリアします。 • **[1]**：SMU への ApbDis を設定します。 • **[自動（auto）]**：CPU が値を判断します。
[CCD 制御（CCD Control）] ドロップダウンリスト **set CbsCpuCcdCtrlSsp**	システムで有効にしたい CCD の数を指定できます。次のいずれかになります。 • **[自動（Auto）]**：プロセッサによって提供される最大数の CCD が有効になります。 • 2 CCD • 3 CCD • 4 CCD • 6 CCD
[Cisco xGMI 最大速度（Cisco xGMI Max Speed）] ドロップダウンリスト **set CiscoXgmiMaxSpeed**	このオプションは、18 Gbps XGMI リンク速度を有効にします。次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。

名前	説明
[NUMAドメインとしての ACPI SRAT L3 キャッシュ（ACPI SRAT L3 Cache As NUMA Domain）] ドロップダウンリスト **set CbsDfCmnAcpiSratL3Numa**	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。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：ドメイン構成に NPS 設定を使用します。 • **[有効（Enabled）]**：各 CCX を独自のドメインにあると宣言します。
[ストリーミング ストア制御（Streaming Stores Control）] ドロップダウンリスト **set CbsCmnCpuStreamingStoresCtrl**	ストリーミング ストア機能を有効にします。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。
[DF C ステート（DF C-States）] ドロップダウンリスト **set CbsCmnGnbSMUDfCstates**	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。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：長時間のアイドル状態は予想されないため、省電力は実現されません。 • **[有効（Enabled）]**：このオプションはアクティブです。システムがアイドル状態のときに電力を節約します。

C125 サーバの場合

[Server Management] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *19 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	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。次のいずれかになります。 • [電源オフ（Power Off）] : OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset] : OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [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）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[ボー レート（Baud Rate）] ドロップダウン リスト **set BaudRate**	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。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **set ConsoleRedir**	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。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • [シリアル ポート A（Serial Port A）]：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • [シリアル ポート B（Serial Port B）]：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [無効（Disabled）]：POST 中にコンソール リダイレクションは発生しません。

名前	説明
[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。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：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。 • [最大（Maximum）]：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。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザは次のトークンを下記の説明のとおりに設定する必要があります。 [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） ブート順序のポリシーにはリストされていないオンボードストレージコントローラでは、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にのみ適用されます。
[フロー制御（Flow Control）] ドロップダウン リスト **set FlowCtrl**	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 セント（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。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） 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。

名前	説明
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **set TerminalType**	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。次のいずれかになります。 • [PC-ANSI]：PC-ANSI端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。
[CDN コントロール（CDN Control）] ドロップダウン リスト **set cdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。

[セキュリティ（Security）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *20 : [*セキュリティ（*Security*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	**[**ホストを即座にリブート（**Reboot Host Immediately**）**]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい **BIOS** 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[信頼されたプラットフォームモジュールのサポート（Trusted Platform Module Support）] ドロップダウン リスト **set TPMAdminCtrl**	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） 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ください。
[電源オン パスワード（Power On Password）] ドロップダウン リスト **set PowerOnPassword**	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。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • [Enabled]：サポートはイネーブルになっています。

[Memory] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *21 : [*メモリ（***Memory***）*]* タブの ***BIOS*** パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） 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。

名前	説明
[Memory Interleaving]ドロップダウン リスト	物理メモリの更新中に別のメモリにアクセスできるよう、AMD CPU がメモリをインターリーブするかどうかを指定します。このオプションは、ファブリック レベルでメモリのインターリーブを制御します。チャネル、ダイ、ソケットの要件はメモリによって異なるため、選択したオプションがメモリでサポートされない場合これらは無視されます。次のいずれかを選択できます。 • **[auto]**：CPUがメモリのインターリーブの方法を決定します。 • **[channel]**：各チャネルに単一の連続したアドレス空間を配置するのではなく、複数のチャネル全体に物理アドレス空間をインターリーブします。 • **[die]**：各ダイに単一の連続したアドレス空間を配置するのではなく、複数のダイ全体に物理アドレス空間をインターリーブします。 • **[none]**：同一の物理メモリから連続したメモリ ブロックにアクセスします。 • **[socket]**：各ソケットに単一の連続したアドレス空間を配置するのではなく、複数のソケット全体に物理アドレス空間をインターリーブします。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Memory Interleaving] ドロップダウン リスト	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。次のいずれかになります。 • 1 KB • 2 KB • 256 バイト • 512 バイト • **自動**: CPU、メモリ ブロックのサイズを決定します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[Chipselect Interleaving] ドロップダウンリスト	ノード 0 に選択する 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。次のいずれかになります。 • **[auto]**：CPU でチップ セレクトのインタリーブの方法を自動的に決定します。 • **[disabled]**：チップの選択は、メモリ コントローラ内でインターリーブされません。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Bank Group Swap] ドロップダウンリスト	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。次のいずれかになります。 • **[auto]**：アプリケーションへの物理アドレスの割り当て方法を CPU で自動的に決定します。 • **[disabled]**：バンク グループ スワップは使用されません。 • **[enabled]**：バンク グループ スワップによりアプリケーションのパフォーマンスを向上させます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[IOMMU] ドロップダウンリスト	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。次のいずれかになります。 • **[auto]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[disabled]**：IOMMU は使用されません。 • **[enabled]**：IOMMU によりアドレス マッピングを行います。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SMEE] ドロップダウンリスト	プロセッサで、メモリの暗号化サポートを実現する Secure Memory Encryption Enable（SMEE）機能を使用するかどうかを指定します。次のいずれかになります。 • **[disabled]**：プロセッサで SMEE 機能を使用しません。 • **[enabled]**：プロセッサで SMEE 機能を使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[TSME] ドロップダウンリスト	プロセッサで、メモリの暗号化サポートを実現する透過的セキュアメモリ暗号化（TSME）機能を使用するかどうかを指定します。次のいずれかになります。 • **[無効（disabled）]**：プロセッサは TSME 機能を使用しません。 • **[有効（enabled）]**：プロセッサは TSME 機能を使用します。 • **[自動（auto）]**：BIOS は、サーバー 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。
[SEV] ドロップダウンリスト	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。次のいずれかになります。 • **[253_ASIDs]**：値は 253 の最小アドレス空間識別子（ASID）に設定されます。 • **[509_ASIDs]**：値は 509 の最小アドレス空間識別子（ASID）に設定されます。 • **[自動（auto）]**：BIOS は、サーバー 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。

名前	説明
[DRAM SW サーマル スロットリング（DRAM SW Thermal Throttling）] ドロップダウンリスト	ソフトウェアが温度制限内で機能することを保証する保護メカニズムを提供します。温度が最大しきい値を超えると、パフォーマンスを低下させ、最小しきい値まで冷却します。次のいずれかになります。 • **[無効（disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（enabled）]**：プロセッサはこの機能を使用します。 • **[自動（auto）]**：BIOS は、サーバー 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。
[バーストおよび遅延リフレッシュ（Burst and Postponed Refresh）] ドロップダウンリスト	• **[無効（disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（enabled）]**：プロセッサはこの機能を使用します。 • **[自動（auto）]**：BIOS は、サーバー 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。

[I/O] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *22 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。

名前	説明
[PCIe スロット *n* Oprom（Pcie Slot n Oprom）] ドロップダウン リスト **set PcieSlotnOptionROM**	サーバーが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト **set PcieSlotnLinkSpeed**	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト **set IPV6PXE**	PXE の IPv6 サポートを有効または無効にします。次のいずれかになります • [無効（disabled）][無効（Disabled）]：IPV6 PXEのサポートは利用できません。 • [enabled][Enabled]：IPV6 PXEのサポートを常に利用できます。
[IPV4 PXE サポート (IPV4 PXE Support)]ドロップダウン リスト **set IPV4PXE**	PXE の IPv4 サポートを有効または無効にします。次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：IPV4 PXEのサポートは利用できません。 • [enabled][Enabled]：IPV4 PXEのサポートを常に利用できます。
[SR-IOV サポート（SR-IOV Support）] ドロップダウン リスト **set SrIov**	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（Enabled）]：SR-IOV はイネーブルになります。

名前	説明
[前面 NVME *n* OptionROM（Front NVME n OptionROM）] ドロップダウンリスト **set PcieSlot *n*OptionROM**	このオプションでは、SSD:NVMe*n*スロットに接続された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。次のいずれかになります。 • **[無効（disabled）]**：SSD:NVMe *n* スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • **[有効（enabled）]**：SSD:NVMe *n* スロットに接続されている PCIe アダプタのオプションの ROM を実行します。
[前面 NVME *n* リンク速度（Front NVME n Link Speed）] ドロップダウンリスト **set PcieSlotFrontNvme1LinkSpeed**	NVMe 前面スロット *n* のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト **set PcieSlotMSTORRAIDOptionROM**	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • 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。
[PCIe ARI サポート (PCIe ARI Support)] ドロップダウン リスト **set PcieARISupport**	リリース 4.1(2a) 以降、Cisco IMC は PCIe 代替ルーティング ID (ARI) 解釈機能をサポートしています。PCIe 仕様では、8 個以上の機能を有効にするPCIeヘッダーのデバイス番号フィールドを再解釈する ARI の実装を通じて、より多くの仮想機能をサポートしています。次のいずれかになります。 • **無効**：PCIe ARI サポートは使用できません。 • **有効**：PCIe ARIサポートを使用できます。 • **自動**：PCIe ARI サポートは自動モードです。

名前	説明
[IPv6 HTTP サポート（IPv6 HTTP Support）] ドロップダウンリスト **set IPV6HTTP**	HTTP の IPv6 サポートを有効または無効にします。次のいずれかになります。 • **[無効（disabled）]**：IPv6 HTTP サポートは使用できません。 • **[有効（enabled）]**：IPv6 HTTP サポートを常に使用できます。
[IPV4 HTTP サポート（IPV4 HTTP Support）] ドロップダウンリスト **set IPV4HTTP**	HTTP の IPv4 サポートを有効または無効にします。次のいずれかになります。 • **[無効（disabled）]**：IPv4 HTTP サポートは使用できません。 • **[有効（enabled）]**：IPv4 HTTP サポートを常に使用できます。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *23 : [*電源/パフォーマンス（*Power/Performance*）*] タブの BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[Core Performance Boost] ドロップダウンリスト	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。次のいずれかになります。 • **[auto]**：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。 • **[disabled]**：CPUにより自動的にブースト パフォーマンスが決定されます。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Global C-state Control] ドロップダウンリスト	AMD プロセッサが IO ベースの C ステートおよび DF C ステートを制御するかどうかに関係なく、これは次のうちいずれかになります。 • **[auto]**：CPU で IO ベースの C ステートの生成方法を自動的に決定します。 • **[disabled]**：グローバル C ステートの制御が無効になります。 • **[enabled]**：グローバル C ステートの制御が有効になります。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[L1 Stream HW Prefetcher] ドロップダウンリスト	プロセッサで、AMD 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、L1 キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [auto][Auto]：CPUは、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェアプリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェア プリフェッチャを使用します。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[L2 Stream HW Prefetcher] ドロップダウンリスト	プロセッサで、AMD ハードウェア プリフェッチャが必要に応じてメモリからデータおよび命令ストリームを取得し、L2 キャッシュに入れることを許可するかどうかを指定します。次のいずれかになります。 • [auto][Auto]：CPU は、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェアプリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェア プリフェッチャを使用します。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[Determinism Slider] ドロップダウンリスト	AMDプロセッサにより動作方法を決定できます。次のいずれかになります。 • **[auto]**：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。 • **[performance]**：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。 • **[power]**：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。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

[Processor] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *24 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[SMT Mode] ドロップダウンリスト	プロセッサで AMD 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。次のいずれかになります。 • **[auto]**：プロセッサは、マルチスレッドの並列実行を許可します。 • **[off]**：プロセッサでマルチスレッディングを禁止します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[SVM Mode] ドロップダウンリスト	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。次のいずれかを選択できます。 • **[disabled]**：プロセッサで SVM テクノロジーを使用しません。 • **[enabled]**：プロセッサで SVM テクノロジーを使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Downcore control] ドロップダウンリスト	AMDプロセッサ コアを無効にしているため、有効にするコアの数を選択できます。次のいずれかになります。 • [FOUR（2+2）]：各 CPU コンプレックスで 2 つのコアを有効にします。 • [FOUR（4+0）]：片方の CPU コンプレックスのみで 4 つのコアを有効にします。 • [SIX（3+3）]：各 CPU コンプレックスで 3 つのコアを有効にします。 • [THREE（3+0）]：片方の CPU コンプレックスのみで 3 つのコアを有効にします。 • [TWO（1+1）]：各 CPU コンプレックスで 1 つのコアを有効にします。 • [TWO（2+0）]：片方の CPU コンプレックスのみで 2 つのコアを有効にします。 • **[auto]**：有効化する必要のあるコアの数を CPU で判断します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

C220 M5、C240 M5、C240 SD M5、および C480 M5 サーバ

I/O タブ

（注） このタブに記載されている BIOS のパラメータは、サーバによって異なります。

表 *25 : [I/O]* タブの *BIOS* のパラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	オンにすると、ホスト サーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。
[レガシー USB サポート（Legacy USB Support）] ドロップダウン リスト **set UsbLegacySupport**	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。次のいずれかになります。 • [Disabled]：USB デバイスは、EFI アプリケーションでのみ使用できます。 • [Enabled]：レガシー USB のサポートは常に使用できます。
[ダイレクト IO への Intel VT（Intel VT for directed IO）] ドロップダウン リスト **set IntelVTD**	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [Enabled]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
[Intel VTD coherency サポート（Intel VTD coherency support）] ドロップダウン リスト **set CoherencySupport**	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [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 VTD ATS サポート（Intel VTD ATS support）] ドロップダウン リスト **set ATS**	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [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。

名前	説明
[VMD Enable (VMD の有効化)] ドロップダウン リスト	Intel Volume Management Device (VMD) は、NVMe SSD を管理および集約するためのハードウェア ロジックを提供する PCIe NVMe SSD 向けです。 これは次のいずれかになります。 • **有効**: 堅牢で安定したホットプラグ、ステータス LED 管理などの利点を有効にします。 • **無効**: 堅牢で安定したホットプラグ、ステータス LED 管理などの利点を無効にします。 デフォルト値：**無効**。 VMD を設定するには、『CPU ユーザー ガイドの Intel® 仮想 RAID』と『CPU の Intel® 仮想 RAID』を参照してください。
	Cisco UCS C480 M5 サーバでサポートされている VMD およびサポートされていないポートの詳細は次のとおりです。 Cisco UCS C480 NVMe SKU (32 ドライブ NVME システム) • DMI 接続ポート7、8、および 23 は、VMD をサポートしていません。 • その他の 29 個のポートはすべて、VMD をサポートしています。 Cisco UCS C480 非 NVMe SKU • DMI 接続ポート 1、2、および 18 は、VMD をサポートしていません。 • ポート7、8、9、10、15、16、17、23、24 は、VMD をサポートします。
[すべてのオンボード LOM Oprom（All Onboard LOM Oprom）] ドロップダウン リスト **set AllLomPortControl**	オプション ROM がすべての LOM ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：すべてのポートでオプション ROM を無効にします。 • [有効（Enabled）]：すべてのポートでオプション ROM を有効にします。

名前	説明
[オンボードLOMポート0 Oprom（Onboard LOM Port0 Oprom）] ドロップダウン リスト **set LomOpromControlPort0**	オプション ROM が LOM ポート 0 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：LOM ポート 0 でオプション ROM を 使用できません。 • [有効（Enabled）]：LOM ポート 0 でオプション ROM を使用できます。
[オンボードLOMポート1 Oprom（Onboard LOM Port1 Oprom）] ドロップダウン リスト **set LomOpromControlPort1**	オプション ROM が LOM ポート 1 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：LOM ポート 1 でオプション ROM を 使用できません。 • [有効（Enabled）]：LOM ポート 1 でオプション ROM を使用できます。
[PCIe スロット *n* Oprom（Pcie Slot n Oprom）] ドロップダウン リスト **set PcieSlotnOptionROM**	サーバが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプション ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[MLOM Oprom] ドロップダウン リスト **set PcieSlotMLOMOptionROM**	このオプションでは、MLOM スロットに接続された 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。次のいずれかになります。 • [無効（Disabled）]：MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[HBA Oprom] ドロップダウン リスト **set PcieSlotHBAOptionROM**	このオプションでは、HBA スロットに接続された 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。次のいずれかになります。 • [無効（Disabled）]：HBA スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：HBA スロットに接続されている PCIe アダプタのオプション ROM を実行します。

名前	説明
[フロント NVME1 Oprom（Front NVME1 Oprom）] ドロップダウン リスト **set PcieSlotN1OptionROM**	このオプションでは、SSD:NVMe1 スロットに接続された 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。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[フロント NVME2 Oprom（Front NVME2 Oprom）] ドロップダウン リスト **set PcieSlotN2OptionROM**	このオプションでは、SSD:NVMe2 スロットに接続された 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。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[HBA リンク速度（HBA Link Speed）] ドロップダウン リスト **set PcieSlotHBALinkSpeed**	このオプションを使用すると、PCIe HBA スロット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。次のいずれかになります。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（Auto）]：システムは許容最大速度を選択します。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。
[MLOM リンク速度（MLOM Link Speed）] ドロップダウン リスト **set PcieSlotMLOMLinkSpeed**	このオプションを使用すると、PCIe MLOM スロット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。次のいずれかになります。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（Auto）]：システムは許容最大速度を選択します。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。

名前	説明
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト **set PcieSlotnLinkSpeed**	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[フロントNVME1リンク速度（Front NVME1 Link Speed）] ドロップダウン リスト **set PcieSlotFrontNvme1LinkSpeed**	NVMeフロントスロット1のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[フロントNVME2リンク速度（Front NVME2 Link Speed）] ドロップダウン リスト **set PcieSlotFrontNvme2LinkSpeed**	NVMeフロントスロット2のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。

名前	説明
[リア NVME1 リンク速度（Rear NVME1 Link Speed）] ドロップダウン リスト **set PcieSlotRearNvme1LinkSpeed**	NVMe 背面のスロット 1 のリンク速度。次のいずれかになります。 • [無効（Disabled）] : スロットは無効であり、カードは列挙されません。 • [自動（Auto）] : デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1] : リンク速度は第 1 世代まで到達可能です。 • [GEN2] : リンク速度は第 2 世代まで到達可能です。 • [GEN3] : リンク速度は第 3 世代まで到達可能です。
[リア NVME2 リンク速度（Rear NVME2 Link Speed）] ドロップダウン リスト **set PcieSlotRearNvme2LinkSpeed**	NVMe 背面のスロット 2 のリンク速度。次のいずれかになります。 • [無効（Disabled）] : スロットは無効であり、カードは列挙されません。 • [自動（Auto）] : デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1] : リンク速度は第 1 世代まで到達可能です。 • [GEN2] : リンク速度は第 2 世代まで到達可能です。 • [GEN3] : リンク速度は第 3 世代まで到達可能です。
[VGA 優先順位（VGA Priority）] ドロップダウン リスト **set VgaPriority**	システムに複数の VGA デバイスがある場合は、VGA グラフィックス デバイスの優先順位を設定できます。次のいずれかになります。 • [オンボード（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（OffBoard）] : 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。 • [オンボードを無効（OnBoardDisabled）] : 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。オンボード VGA が無効の場合、vKVM は機能しません。

名前	説明
[P-SATA OptionROM] ドロップダウン リスト **set pSATA**	PCH SATA オプション ROM モードを選択できます。次のいずれかになります。 • [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。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[M2.SATA OptionROM] ドロップダウン リスト **set SataModeSelect**	Serial Advanced Technology Attachment（SATA）ソリッド ステート ドライブ（SSD）の動作モード。次のいずれかになります。 • [AHCI]： SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [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。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[リア USB ポート（USB Port Rear）] ドロップダウン リスト **set UsbPortRear**	背面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：背面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：背面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[フロント USB ポート（USB Port Front）] ドロップダウン リスト **set UsbPortFront**	前面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：前面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：前面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。

名前	説明
[内部 USB ポート（USB Port Internal）] ドロップダウン リスト **set UsbPortInt**	内部 USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）] : 内部の USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）] : 内部の USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[KVM USB ポート（USB Port KVM）] ドロップダウン リスト **set UsbPortKVM**	vKVM ポートが有効になっているか、無効になっているか。次のいずれかになります • **[無効（Disabled）]**—vKVM キーボードとマウス デバイスを無効にします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • **[有効 (Enabled)]**—vKVM キーボードとマウス デバイスを有効にします。
[SD カード USB ポート（USB Port SD Card）] ドロップダウン リスト **set UsbPortSdCard**	SD カードが有効か無効か。次のいずれかになります。 • [無効（Disabled）] : SD カードのポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）] : SD カードのポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト **set IPV6PXE**	PXE の IPv6 サポートを有効または無効にします。次のいずれかになります • **[無効 (disabled)]** : PV6 PXE のサポートは利用できません。 • **[enabled (有効)]**:IPV6 PXE のサポートを常に利用できます。
PCIe PLL SSC ドロップダウン リスト **set PciePllSsc**	この機能を有効にすると、クロックを 0.5% 下方に拡散することにより、EMI 干渉が軽減されます。この機能を無効にすると、拡散せずにクロックを集中管理できます。 これは次のいずれかになります。 • **[自動 (auto)]**—EMI 干渉は自動調整されます。 **[無効 (Disabled)]**—EMI 干渉は自動調整されます。 • **[ZeroPointFive]**—クロックを 0.5% 下方に拡散することにより、EMI 干渉を軽減します。

名前	説明
[IPV4 PXE サポート (IPV4 PXE Support)] ドロップダウン リスト **set IPV4PXE**	PXE の IPv4 サポートを有効または無効にします。次のいずれかになります • **[無効 (disabled)]**: IPV4 PXE のサポートは利用できません。 • **[enabled (有効)]**: IPV4 PXE のサポートを常に利用できます。
[Network Stack (ネットワーク スタック)] ドロップダウン リスト **set NetworkStack**	このオプションでは、IPv6 と IPv4 をモニタできます。次のいずれかになります • **[無効 (disabled)]**: ネットワーク スタックのサポートは使用できません。 （注） 無効にすると、 **IPV4 PXE サポート**に設定された値はシステムに影響しません。 • **[enabled (有効)]**: ネットワーク スタックのサポートを常に利用できます。
[外部データベース（External Database）] ドロップダウン リスト **set EnableClockSpreadSpec**	このオプションを使用すると、マザーボードからの EMI を、マザーボードが発生する信号に変調をかけ、スパイクがより平坦な曲線になるようにして、軽減します。 次のいずれかになります。 • **[無効 (Disabled)]**—クロック拡散スペクトルのサポートは使用できません。 • **[Enabled (有効)]**—クロック拡散スペクトルのサポートは常に使用できます。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト **set PcieSlotMSTORRAIDOptionROM**	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • 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。

[Server Management] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *26 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	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。次のいずれかになります。 • [電源オフ（Power Off）]：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [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）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。
[ボー レート（Baud Rate）] ドロップダウン リスト **set BaudRate**	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。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **set ConsoleRedir**	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。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • [シリアル ポート A（Serial Port A）]：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • [シリアル ポート B（Serial Port B）]：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [無効（Disabled）]：POST 中にコンソール リダイレクションは発生しません。

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[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。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：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。 • [最大（Maximum）]：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。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよびGPUコントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]
[CDN コントロール（CDN Control）] ドロップダウン リスト **set cdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。

サーバー モデル別 BIOS パラメータ

名前	説明
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。
[フロー制御（Flow Control）] ドロップダウン リスト **set FlowCtrl**	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。次のいずれかになります。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） 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。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **set TerminalType**	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。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト **set PcieSlotsCdnEnable**	（注） このオプションは、スロット 2 または 5 に Qlogic カードを搭載した Cisco UCS C240 M5 サーバーでのみ使用できます。 イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [Enabled]：VIC カードの CDN サポートが有効になります。

[セキュリティ（Security）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *27 : [*セキュリティ（***Security***）*]* タブの ***BIOS*** パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	**[**ホストを即座にリブート（**Reboot Host Immediately**）**]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい **BIOS** 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[トラステッド プラットフォーム モジュール状態（**Trusted Platform Module State**）**]** ドロップダウンリスト **set TPMAdminCtrl**	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） 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ください。
SHA-1 PCRバンク	SHA-1 PCR バンクを有効または無効にします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
SHA256 PCRバンク	SHA256 PCR バンクを有効または無効にします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[Reboot Host Immediately] チェックボックス	**[ホストを即座にリブート（Reboot Host Immediately）]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい **BIOS** 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[Intel Trusted Execution Technology のサポート（Intel Trusted Execution Technology Support）]	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[電源オン パスワード（Power On Password）] ドロップダウンリスト **set PowerOnPassword**	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。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • [Enabled]：サポートはイネーブルになっています。

[Processor] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *28 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト **set IntelVT**	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。
[拡張 APIC（Extended APIC）] ドロップダウンリスト **set LocalX2Apic**	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。次のいずれかになります。 • [有効（Enabled）]：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト **set ProcessorC1E**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

名前	説明
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[XD ビット（Execute Disable Bit）] ドロップダウンリスト **set ExecuteDisable**	アプリケーション コードを実行できる場所を指定するために、サーバーのメモリ領域を分類します。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。次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [有効（Enabled）]：プロセッサでメモリ領域を分類します。 （注） 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ください。

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト **set IntelTurboBoostTech**	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。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。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • HW ALL：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • SW ALL：OS Power Manager によって、依存関係にある論理プロセッサ間の P-state を調整します。すべての論理プロセッサで遷移を開始します。

名前	説明
[SpeedStep（Pstates）] ドロップダウンリスト **set EnhancedIntelSpeedStep**	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。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 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。 （注） [CPUPowerManagement] を [カスタム（Custom）] 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。
[HyperThreading [All]] ドロップダウンリスト **set IntelHyperThread**	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。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。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウンリスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • **[1] ～ [27]**：サーバーで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 （注） 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ください。
[Processor CMCI] ドロップダウン リスト **set ProcessorCMCI**	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。

名前	説明
[Enhanced Intel SpeedStep Tech] ドロップダウン リスト **set EnhancedIntelSpeedStep**	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。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 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。 （注） [CPUPowerManagement] は、[カスタム（Custom）] に設定する必要があります。設定しな場合、サーバはこのパラメータの設定を無視します。
[Workload Configuration] ドロップダウン リスト **set WorkLdConfig**	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **NUMA** • **UMA**

名前	説明
[Sub NUMA Clustering] ドロップダウンリスト	CPUがサブNUMAクラスタリングをサポートするかどうか。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あります。次のいずれかになります。 • [disabled][Disabled]：サブNUMAクラスタリングは発生しません。 • [enabled][Enabled]：サブNUMAクラスタリングが発生します。 • [自動（Auto）][自動（auto）]：BIOSかサブNUMAのクラスタ リングされるかが決まります。
エネルギー/パフォーマンスのバイアス構成	エネルギーまたはパフォーマンスのバイアス構成を表示します。 次のいずれかになります。 • Balanced Performance • Performance • Balanced Power • 電源
[XPT Prefetch] ドロップダウン リスト	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。次のいずれかになります。 • [disabled][Disabled]：CPU はXPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPU はXPTプリフェッチ オプションを有効にします。

名前	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト	UPI 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。これは次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：プロセッサでキャッシュ データをプリロードしません。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャで最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウンリスト **set CpuEngPerfBias**	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ーで重要かどうかを判断できます。次のいずれかになります。 • [パフォーマンス（Performance）]：サーバーでは、すべてのサーバーコンポーネントに全電力を常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [バランス パフォーマンス（Balanced Performance）]：サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバーコンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。

名前	説明
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト **set PwrPerfTuning**	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。 • [bios][BIOS]： エネルギー効率を調整する場合は [BIOS] を選択します。 • [os][OS]： エネルギー効率を調整する場合は [OS] を選択します。
[LLC Prefetch] ドロップダウン リスト	プロセッサが LLC プリフェッチ メカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [enabled][Enabled]：LLC Prefetcherで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

名前	説明
[パッケージのCステート（Package C State）] ドロップダウン リスト **set package-c-state-limit-config package-c-state-limit**	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意の Cステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度を CPUが決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバーコンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。この場合、必要な電力はC1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、またはC3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C6 保持（C6 Retention）]：CPUのアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。

名前	説明
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト **set CpuHWPM**	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPM がディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPM ネイティブモードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPM アウトオブボックスモードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト **set IntelSpeedSelect**	**[Intel Speed Select (Intel の速度選択)]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本**): ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 1** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **設定 2** ユーザーは **設定 1** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト **set UFSDisable**	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の **[非コア周波数スケーリング (Uncore Frequency Scaling)]**の固定の上限値と下限値が記されています。

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト **set ConfigTDPLevel**	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[UPI リンク速度（UPIH Link Speed）] ドロップダウンリスト **set QpiLinkSpeed**	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (Auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

名前	説明
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト **set EnergyEfficientTurbo**	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。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。
プロセッサEPPの有効化	プロセッサ EPP の有効化で選択した値を表示します。 • **[無効（Dissabled）]**：プロセッサ EPP の有効化が無効です。 • **[有効（Enabled）]**：プロセッサ EPP の有効化が有効です。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウンリスト **set AutoCCState**	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト **set PatrolScrub**	システムにサーバーのメモリ（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ことが可能です。次のいずれかになります。 • [Disabled]：CPU がメモリ アド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。 • [有効（Enabled）]：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。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト **set EPPProfile**	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ーで重要かどうかを判断できます。次のいずれかになります。 • Performance • Balanced Performance • Balanced Power • 電源

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *29 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）] : システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）] : 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。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

名前	説明
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） 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。
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)]ドロップダウン リスト **set DCPMMFirmwareDowngrade**	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト **set PartialMirrorModeConfig**	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**: 部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**: 部分的なメモリ ミラーが無効になります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド **set PartialMirrorPercent**	4GBを超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。

名前	説明
[部分ミラー 1 サイズ (GB) (Partial Mirror1 Size in GB)] フィールド **set PartialMirrorValue1**	最初の部分メモリ ミラーのサイズ (GB)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 2 サイズ (GB) (Partial Mirror2 Size in GB)] フィールド **set PartialMirrorValue2**	2 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 3 サイズ (GB) (Partial Mirror3 Size in GB)] フィールド **set PartialMirrorValue3**	3 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 4 サイズ (GB) (Partial Mirror4 Size in GB)] フィールド **set PartialMirrorValue4**	4 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド **set MemorySizeLimit**	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。

名前	説明
[NUMA] ドロップダウン リスト **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト **set BmeDmaMitigation**	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト **set SelectPprType**	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[CR QoS] ドロップダウンリスト **CRQoS**	CR QoS 調整を選択できます。 次のいずれかになります。 • **[レシピ 1 (Recipe 1)]**: QoS ノブ向けで、アクティブなディレクトリでの2-2-2 メモリ設定に推奨されます。 • **[レシピ 2 (Recipe 2)]**: QoS ノブ向けで、アクティブなディレクトリでの他のメモリ設定に推奨されます。 • **[レシピ 3 (Recipe 3)]**: QoS ノブ向けで、チャネルごとに1つの DIMM を設定することを推奨します。 • **[無効 (Disabled)]**:**CR QoS**機能は無効になります。
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト **SnoopyModeForAD**	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRT メモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト **CrfastgoConfig**	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **デフォルト (Default)** • **オプション 1 (Option 1)** • **オプション 2 (Option 2)** • **オプション 3 (Option 3)** • **オプション 4 (Option 4)** • **オプション 5 (Option 5)** • **自動 (Auto)**

名前	説明
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト **NvmdimmPerformConfig**	ワークロードの動作に応じて、NVMベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト **SnoopyModeFor2LM**	NUMA に最適化されていないワークロードから far メモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト **MemoryThermalThrottling**	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **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を使用してクローズドループ サーマル スロットリングを有効にします。

名前	説明
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト **MemoryRefreshRate**	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト **PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[高度なメモリ テスト（Advanced Memory Test）] ドロップダウンリスト **AdvancedMemTest**	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[拡張メモリ テスト（Enhanced Memory Test）] ドロップダウンリスト	次のいずれかになります。 • **[自動（Auto）]**：サポートは自動に設定されています。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *30 : [*電源/パフォーマンス（*Power/Performance*）*] タブの BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[ハードウェアプリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **set HardwarePrefetch**	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。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **set AdjacentCacheLinePrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。

サーバー モデル別 BIOS パラメータ

名前	説明
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト **set DcuStreamerPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含むL1キャッシュをプリロードします。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト **set CPUPerformance**	上記のオプションに対しCPUパフォーマンス プロファイルを設定します。次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバのBIOSセットアップから設定できます。さらに、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ：ライン プリフェッチ（Adjacent Cache-Line Prefetch）] オプションも設定できます。

C460 M4 サーバ

C460 M4 サーバの [メイン（Main）] タブ

主要な BIOS パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[TPM Support] **set TPMAdminCtrl**	TPM（トラステッドプラットフォーム モジュール）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） 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。
[Power ON Password Support] ドロップダウン	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。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • **[有効（Enabled）]**：サポートは有効になります。

[Actions] 領域

名前	説明
[**Save**] ボタン	BIOS パラメータの設定を保存して、ダイアログボックスを閉じます。 **[Reboot Host Immediately]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[Reset] ボタン	3 つすべてのタブ上の BIOS パラメータの値が、このダイアログボックスを最初に開いた際に有効だった設定にリセットされます。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。

C460 M4 サーバの [詳細設定（Advanced）] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

[Processor Configuration] のパラメータ

名前	説明
[Intel Hyper-Threading Technology] ドロップダウン リスト **set IntelHyperThread**	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。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。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。 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。
[有効化されたコア数（Number of Enabled Cores）] ドロップダウン リスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1] ～ [***n***]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 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てください。

名前	説明
[Execute Disable] ドロップダウン リスト **set ExecuteDisable**	アプリケーション コードを実行できる場所を指定するために、サーバーのメモリ領域を分類します。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。次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [有効（Enabled）]：プロセッサでメモリ領域を分類します。 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。
[Intel VT] **set IntelVT**	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティングシステムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバーの電源を再投入する必要があります。
[Intel VT-d] **set IntelVTD**	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [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。

名前	説明
[Intel(R) 割り込み再マッピング（Intel(R) Interrupt Remapping）] ドロップダウン リスト **set InterruptRemap**	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。次のいずれかになります。 • [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) パススルー DMA（Intel(R) Passthrough DMA）] ドロップダウン リスト **set PassThroughDMA**	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。次のいずれかになります。 • [Disabled]：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 VT-d Coherency Support] **set CoherencySupport**	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [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 VT-d ATS Support] **set ATS**	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [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。

名前	説明
[CPU Performance] **set CPUPerformance**	サーバーのCPUパフォーマンスプロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • ハードウェア プリフェッチャ • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [HighThroughput]**[High_Throughput]**：DCU IP Prefetcher のみがイネーブルです。残りのオプションはディセーブルになります。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **set HardwarePrefetch**	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。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。

名前	説明
[隣接キャッシュラインプリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **set AdjacentCacheLinePrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [有効（Enabled）]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCUストリーマープリフェッチ（DCU Streamer Prefetch）] ロップダウン リスト **set DcuStreamerPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IPプリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含むL1キャッシュをプリロードします。
[ダイレクトキャッシュアクセスサポート（Direct Cache Access Support）] ドロップダウン リスト **set DirectCacheAccess**	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。次のいずれかになります。 • [Disabled]：データはI/Oデバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データはI/Oデバイスから直接プロセッサ キャッシュに入れられます。

サーバー モデル別 BIOS パラメータ

名前	説明
[Power Technology] **set CPUPowerManagement**	次のオプションのCPU電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Custom]：前述のBIOSパラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Disabled]：サーバーで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • [Energy Efficient][Energy_Efficient]：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。
[Enhanced Intel Speedstep Technology] ドロップダウン リスト **set EnhancedIntelSpeedStep**	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。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 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。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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
[Intel Turbo Boost Technology] **set IntelTurboBoostTech**	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。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。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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。
[Processor C3 Report] **set ProcessorC3Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C3 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS は C3 レポートの送信を行いません。 • [Enabled]：BIOS から C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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
[Processor C6 Report] **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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。
[プロセッサの電源状態C1拡張（Processor Power State C1 Enhanced）] ドロップダウン リスト **set ProcessorC1EReport**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。

名前	説明
[P-STATE調整（P-STATE Coordination）] ドロップダウン リスト **set PsdCoordType**	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。 • [HW_ALL]：プロセッサ ハードウェアによって、依存関係にある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）によって、依存関係にある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）によって、依存関係にある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始できます。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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。
[SINGLE_PCTL] ドロップダウン リスト **get SinglePCTLEn**	プロセッサの電源管理を向上させるために単一 PCTL サポートを促進します。次のいずれかになります。 • **[いいえ（No）]** • ○
[TDPの設定（Config TDP）] ドロップダウン リスト **get ConfigTDP**	システムの熱設計電力（TDP）を設定できます。TDP は、過熱イベントを引き起こすことなくアプリケーションを実行できる最大電力量です。次のいずれかになります。 • [無効（Disabled）]：TDP の設定を無効にします。これはデフォルト値です。 • [有効（Enabled）]：TDP の設定を有効にします。

名前	説明
[エネルギーパフォーマンスの調整（Energy Performance Tuning）] ドロップダウン リスト **set PwrPerfTuning**	エネルギー効率のバイアス調整のために BIOS またはオペレーティング システムを選択できます。次のいずれかになります。 • [OS]：エネルギーパフォーマンスの調整にOSを選択します。 • [BIOS]：エネルギー効率の調整のために BIOS を選択します。
[エネルギーパフォーマンス（Energy Performance）] ドロップダウン リスト **set CpuEngPerfBias**	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ーで重要かどうかを判断できます。次のいずれかになります。 • **Balanced_Energy** • **Balanced_Performance** • **Energy_Efficient** • **Performance**

名前	説明
[パッケージのCステートの制限（Package C State Limit）] ドロップダウン リスト **set PackageCStateLimit**	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [C0 state][C0_state]：サーバーはすべてのサーバー コンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • **[C1_state]**：CPU のアイドル時に、システムは電力消費を少し減らします。このオプションでは、必要な電力が C0 よりも少なく、サーバーはすばやくハイ パフォーマンス モードに戻ることができます。 • **[C3_state]**：CPU のアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • **[C6_state]**：CPU のアイドル時に、システムは C3 オプションの場合よりもさらに電力消費を減らします。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • **[C7_state]**：CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。このオプションでは、節約される電力量が最大になりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • **[No_Limit]**：サーバは、使用可能な任意の C ステートに入ることがあります。
[Extended APIC] **set LocalX2Apic**	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。次のいずれかになります。 • [XAPIC]：APIC サポートを有効にします。 • [X2APIC]：APIC を有効にして、Intel VT-d と Interrupt Remapping も有効にします。

名前	説明
[Workload Configuration] **set WorkLdConfig**	ワークロードの特性を最適化するようにパラメータを設定できます。次のいずれかになります。 • [Balanced]：最適化のためにバランスのとれたオプションを選択します。 • [I/O Sensitive]：最適化のために I/O を考慮したオプションを選択します。 （注） ワークロード構成は [Balanced] に設定することをお勧めします。
[IIO エラーの有効化（IIO Error Enable）] ドロップダウン リスト **get IohErrorEn**	IIO 関連のエラーを生成できます。次のいずれかになります。 • 〇 • **[いいえ（No）]**

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性および機密性（RAS）の設定方法。次のいずれかになります。 • **[Maximum_Performance]**：システムのパフォーマンスが最適化されます。 • [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。 • [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きます。このオプションを使用した場合、[Mirroring] よりもシステム パフォーマンスが向上し、[Maximum Performance] よりも信頼性が向上しますが、[Mirroring] よりも信頼性が低く、[Maximum Performance] よりもシステム パフォーマンスは低下します。

名前	説明
[DRAMクロックスロットリング（DRAM Clock Throttling）] ドロップダウン リスト **set DRAMClockThrottling**	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。次のいずれかになります。 • [Balanced]：DRAM クロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [Performance]：DRAM クロック スロットリングを無効化し、追加の電力を使用してメモリ帯域幅を増やします。 • [Energy Efficient]：DRAMのクロック スロットリングを上げてエネルギー効率を向上させます。
[低電圧DDRモード（Low Voltage DDR Mode）] ドロップダウン リスト **set LvDDRMode**	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。次のいずれかになります。 • [Power Saving Mode][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。 • [Performance Mode][Performance_Mode]：高周波数の動作が低電圧の動作よりも優先されます。
[クローズドループ サーマル スロッティング（Closed Loop Therm Throt）] ドロップダウン リスト **set closedLoopThermThrotl**	閉ループ サーマル スロットリングのサポートを可能にします。これにより信頼性が向上し、CPU がアイドル状態の間は自動電圧制御により CPU の電力消費が低減します。次のいずれかになります。 • [無効（Disabled）]：閉ループ サーマル スロットリングを無効にします。 • [有効（Enabled）]：閉ループ サーマル スロットリングを有効にします。これがデフォルト値です。

名前	説明
[チャネルインターリーブ（Channel Interleaving）] ドロップダウン リスト **set ChannelInterLeave**	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。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1Way][1_Way]：一部のチャネル インターリーブが使用されます。 • [2Way][2_Way] • [3Way][3_Way] • [4Way][4_Way]：最大のチャネル インターリーブが使用されます。
[Rank Interleaving] **set RankInterLeave**	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。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1Way][1_Way]：一部のランク インターリーブが使用されます。 • [2Way][2_Way] • [4Way][4_Way] • [8Way][8_Way]：最大量のランク インターリーブが使用されます。

名前	説明
[Patrol Scrub] **set PatrolScrub**	システムがサーバー上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [Disabled]：CPU がメモリ アド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。 • [有効（Enabled）]：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。
[デマンドスクラブ（Demand Scrub）] ドロップダウン リスト **set DemandScrub**	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。次のいずれかになります。 • [無効（Disabled）]：シングル ビット メモリ エラーは修正されません。 • [Enabled]：シングル ビット メモリ エラーがメモリ内部で修正され、修正されたデータが読み取り要求に応じて設定されます。
[高度（Altitude）] ドロップダウン リスト **set Altitude**	物理サーバーがインストールされている地点のおよその海抜（m 単位）。次のいずれかになります。 • [Auto]：物理的な高度を CPU によって判別します。 • [300M][300_M]：サーバーは海抜約 300 m の位置にあります。 • [900M][900_M]：サーバーは海抜約 900 m の位置にあります。 • [1500M][1500_M]：サーバーは海抜約 1500 m の位置にあります。 • **[3000_M]**：サーバーは、海抜約 3000 m です。

名前	説明
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト **PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリ コントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。

[QPI Configuration] のパラメータ

名前	説明
[QPI Link Frequency Select] **set QPILinkFrequency**	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（GT/s）単位）。次のいずれかになります。 • [Auto]：QPI リンク周波数はCPUによって決定されます。 • **6.4_GT/s** • 7.2_GT/s] • **8.0_GT/s**
[QPI Snoop Mode] **set QpiSnoopMode**	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [無効（Disabled）]：QPI スヌープ モードを無効にします。 • [クラスタ オン ダイ（Cluster on Die）]：クラスタ オン ダイが有効になります。有効化したLLCはそれぞれに独立したキャッシング エージェントで2つのパートに分割されます。これにより、一部のワークロードのパフォーマンスが向上します。このモードは、10個以上のコアを搭載した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。 • [自動（Auto）]：CPU は自動的に早期スヌープ モードとして認識します。これはデフォルト値です。

[USB Configuration] のパラメータ

名前	説明
[レガシーUSBサポート（Legacy USB Support）] ドロップダウン リスト **set LegacyUSBSupport**	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。次のいずれかになります。 • [無効（Disabled）]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [有効（Enabled）]：レガシーUSBのサポートは常に使用できます。 • [Auto]：USBデバイスが接続されていない場合、レガシーUSBのサポートがディセーブルになります。
[Port 60/64 Emulation] **set UsbEmul6064**	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。次のいずれかになります。 • [無効（Disabled）]：60h/64エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64エミュレーションはサポートされます。 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、このオプションを選択する必要があります。
[すべてのUSBデバイス（All USB Devices）] ドロップダウン リスト **set AllUsbDevices**	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。次のいずれかになります。 • [Disabled]：すべてのUSBデバイスが無効です。 • [Enabled]：すべてのUSBデバイスが有効になります。
[USB Port: Rear] **set UsbPortRear**	背面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：背面パネルのUSBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティングシステムによって検出されません。 • [有効（Enabled）]：背面パネルのUSBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティングシステムによって検出されます。

名前	説明
[USB Port: Internal] **set UsbPortInt**	内部USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：内部USBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティングシステムによって検出されません。 • [有効（Enabled）]：内部USBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。
[USB Port: KVM] **set UsbPortKVM**	vKVM ポートが有効か無効か。次のいずれかになります。 • **無効**：vKVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスはvKVM ウィンドウで機能しなくなります。 • **有効**：vKVM キーボードとマウス デバイスを有効にします。
[USB Port: vMedia] **set UsbPortVMedia**	仮想メディア デバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：vMediaデバイスをディセーブルにします。 • [Enabled]：vMedia デバイスを有効にします。
[xHCI Mode] **set PchUsb30Mode**	xHCIコントローラのレガシーサポートを有効または無効にします。次のいずれかになります。 • [Disabled]：xHCI コントローラのレガシー サポートを無効にします。 • [Enabled]：xHCIコントローラのレガシーサポートを有効にします。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] **set MemoryMappedIOAbove4GB**	4GB を超える MMIO をイネーブルまたはディセーブルにするかどうか。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） 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。
[SR-IOV サポート（SR-IOV Support）] ドロップダウン リスト **set SrIov**	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（Enabled）]：SR-IOV はイネーブルになります。

[Serial Configuration] のパラメータ

名前	説明
[Out-of-Band Mgmt Port] **set comSpcrEnable**	Windows 緊急管理サービスで使用可能な COM ポート 0 を設定することができます。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。次のいずれかになります。 • [Disabled]：Windows オペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [有効（Enabled）]：Windows 緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。

名前	説明
[コンソールリダイレクション（Console redirection）] ドロップダウン リスト **set ConsoleRedir**	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。次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。 • [COM 0]：POST中に COM ポート 0 でコンソール リダイレクションを有効にします。 • [COM 1]：POST中に COM ポート 1 でコンソール リダイレクションを有効にします。
[Terminal type] **set TerminalType**	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。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100+]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） 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。
[Bits per second] **set BaudRate**	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。[Console Redirection] を無効にする場合は、このオプションを使用できません。次のいずれかになります。 • [9600]：9,600 ボー レートが使用されます。 • [19200]：19,200 ボー レートが使用されます。 • [38400]：38,400 ボー レートが使用されます。 • [57600]：57,600 ボー レートが使用されます。 • [115200]：115,200 ボー レートが使用されます。 （注） 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。

名前	説明
[フロー制御（Flow Control）] ドロップダウン リスト **set FlowCtrl**	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。次のいずれかになります。 • [None]：フロー制御は使用されません。 • **Hardware_RTS/CTS**：フロー制御に RTS/CTS が使用されます。 （注） 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。
[Putty KeyPad] **set PuttyFunctionKeyPad**	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。次のいずれかになります。 • [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 仮想コンソールを模倣します。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。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 によって ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 によって **ESC [M** ～ **ESC [X** を生成します。ファンクション キーと Shift キーによって **ESC [Y** ～ **ESC [j** を生成します。Ctrl キーとファンクション キーによって **ESC [k** ～ **ESC [v** を生成します。Shift、Ctrl およびファンクション キーによって **ESC [w** ～ **ESC [{** 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。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。 • [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。

名前	説明
[Redirection After BIOS POST] **set RedirectionAfterPOST**	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。次のいずれかになります。 • **[Always_Enable]**：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。

[LOM and PCIe Slots Configuration] のパラメータ

名前	説明
[VICに対するCDNサポート（CDN Support for VIC）] ドロップダウン リスト **set CdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。
[PCI ROM CLP] **set PciRomClp**	PCI ROM Command Line Protocol（CLP）は、カード上の iSCSI や PxE などのさまざまなオプション ROM の実行を制御します。デフォルト設定は、ディセーブルです。 • [Enabled]：ポートごとに個別に、iSCSI や PxE などのさまざまなオプション ROM の実行を設定できるようにします。 • [Disabled]：デフォルト オプションです。異なるオプション ROM は選択できません。デフォルト オプション ROM は PCI 列挙中に実行されます。

名前	説明
[PCH SATA Mode] **set SataModeSelect**	このオプションでは、PCH SATA モードを選択できます。次のいずれかになります。 • [AHCI]：SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [Disabled]：SATA コントローラと sSATA コントローラを無効にします。 • [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。
[All Onboard LOM Ports] **set AllLomPortControl**	すべての LOM ポートを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべての LOM ポートが無効です。 • [Enabled]：すべての LOM ポートが有効になります。
[LOM Port *n* OptionROM] **set LomOpromControlPort*n***	***n*** で指定された LOM ポートでオプション ROM を使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI_Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy_Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。
[All PCIe Slots OptionROM] **set PcieOptionROMs**	PCIe カードのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI_Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy_Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。

名前	説明
[PCIe Slot:*n* OptionROM **set PcieSlot*n*OptionROM**	PCIe カードのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI_Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy_Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:MLOM OptionROM] **set PcieSlotMLOMOptionROM**	このオプションでは、MLOM スロットに接続された 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。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:HBA OptionROM] **set PcieSlotHBAOptionROM**	このオプションでは、HBA スロットに接続された 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。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。

名前	説明
[PCIe Slot:N1 OptionROM] **set PcieSlotN1OptionROM**	このオプションでは、SSD:NVMe1スロットに接続された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。次のいずれかになります。 • [Enabled]：レガシーおよびUEFIオプションROMの両方を実行します。 • **[無効（Disabled）]**：レガシーおよびUEFIの両方のオプションROMは実行されません。 • **[UEFIのみ（UEFI Only）]**：UEFIオプションROMのみを実行します。 • [Legacy Only]：レガシー オプションROMのみを実行します。
[PCIe Slot:N2 OptionROM] **set PcieSlotN2OptionROM**	このオプションでは、SSD:NVMe2スロットに接続された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。次のいずれかになります。 • [Enabled]：レガシーおよびUEFIオプションROMの両方を実行します。 • **[無効（Disabled）]**：レガシーおよびUEFIの両方のオプションROMは実行されません。 • **[UEFIのみ（UEFI Only）]**：UEFIオプションROMのみを実行します。 • [Legacy Only]：レガシー オプションROMのみを実行します。
[PCIe Slot:N2 OptionROM] **set PcieSlotN2OptionROM**	このオプションでは、SSD:NVMe2スロットに接続された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。次のいずれかになります。 • [Enabled]：レガシーおよびUEFIオプションROMの両方を実行します。 • **[無効（Disabled）]**：レガシーおよびUEFIの両方のオプションROMは実行されません。 • **[UEFIのみ（UEFI Only）]**：UEFIオプションROMのみを実行します。 • [Legacy Only]：レガシー オプションROMのみを実行します。

サーバー モデル別 BIOS パラメータ

名前	説明
[PCIe Slot:HBA Link Speed] **PCIe SlotHBALinkSpeed**	このオプションを使用すると、PCIe HBA スロット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。次のいずれかになります。 • [自動（Auto）]：システムは許可される最大速度を選択します。 • [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。 • [GEN2]：最大 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。 • [Disabled]：最大速度は制限されません。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C460 M4 サーバの [サーバ管理（Server Management）] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

サーバ管理 BIOS パラメータ

名前	説明
[FRB-2 Timer] **set FRB-2**	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 Cisco IMC で FRB2 タイマーを使用するかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバーのブートにかかる時間をウォッチドッグ タイマーでトラッキングします。サーバーが **set OSBootWatchdogTimerTimeout** コマンドにより、Cisco IMC はエラーをログに記録し、**set OSBootWatchdogTimerPolicy** コマンドで指定されたアクションを実行します。

名前	説明
[OSウォッチドッグタイマータイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	OSが指定された時間内にブートしない場合、OSウォッチドッグ タイマーの期限が切れ、システムはタイマー ポリシーに基づいてアクションを実行します。次のいずれかになります。 • **[5_Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • **[10_Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • **[15_Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • **[20_Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[OSウォッチドッグタイマーポリシー（OS Watchdog Timer Policy）] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	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。次のいずれかになります。 • **Do_Nothing**：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、アクションは実行されません。 • **Power_Down**：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバーの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C220 M4 および C240 M4 サーバ

C220M4 および C240M4 サーバのメイン タブ

主要な BIOS パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。

名前	説明
[TPM Support] **set TPMAdminCtrl**	TPM（トラステッドプラットフォームモジュール）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） 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。
[Power ON Password Support] ドロップダウン	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。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • **[有効（Enabled）]**：サポートは有効になります。

[Actions] 領域

名前	説明
[**Save**] ボタン	BIOS パラメータの設定を保存して、ダイアログボックスを閉じます。 **[Reboot Host Immediately]** チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[Reset] ボタン	3 つすべてのタブ上の BIOS パラメータの値が、このダイアログボックスを最初に開いた際に有効だった設定にリセットされます。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。

C220M4 および C240M4 サーバの [詳細（Advanced）] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

[Processor Configuration] のパラメータ

名前	説明
[Intel Hyper-Threading Technology] ドロップダウン リスト **set IntelHyperThread**	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。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。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）]：プロセッサでの複数スレッドの並列実行を許可します。 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
[有効化されたコア数（Number of Enabled Cores）] ドロップダウン リスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1] ～ [***n***]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 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てください。
[Execute Disable] ドロップダウン リスト **set ExecuteDisable**	アプリケーション コードを実行できる場所を指定するために、サーバーのメモリ領域を分類します。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。次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [有効（Enabled）]：プロセッサでメモリ領域を分類します。 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
[Intel VT] **set IntelVT**	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティングシステムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバーの電源を再投入する必要があります。
[Intel VT-d] **set IntelVTD**	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [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 VTD割り込み再マッピング（Intel VTD interrupt Remapping）] ドロップダウンリスト **set InterruptRemap**	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。次のいずれかになります。 • [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 VT-d PassThrough DMA] ドロップダウン リスト **set PassThroughDMA**	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。次のいずれかになります。 • [Disabled]：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。

名前	説明
[Intel VT-d Coherency Support] **set CoherencySupport**	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [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 VT-d ATS Support] **set ATS**	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [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。
[CPU Performance] **set CPUPerformance**	サーバーの CPU パフォーマンス プロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • ハードウェア プリフェッチャ • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [HighThroughput]**[High_Throughput]**：DCU IP Prefetcher のみがイネーブルです。残りのオプションはディセーブルになります。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。

名前	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **set HardwarePrefetch**	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。次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
[隣接キャッシュラインプリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **set AdjacentCacheLinePrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [有効（Enabled）]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCUストリーマープリフェッチ（DCU Streamer Prefetch）] ロップダウン リスト **set DcuStreamerPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IPプリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	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。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP プリフェッチャで最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。

サーバー モデル別 BIOS パラメータ

名前	説明
[ダイレクトキャッシュアクセスサポート（Direct Cache Access Support）] ドロップダウン リスト **set DirectCacheAccess**	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。次のいずれかになります。 • [Disabled]：データはI/Oデバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データはI/Oデバイスから直接プロセッサ キャッシュに入れられます。
[Power Technology] **set CPUPowerManagement**	次のオプションのCPU電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Custom]：前述のBIOSパラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Disabled]：サーバーで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • [Energy Efficient][Energy_Efficient]：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。

名前	説明
[Enhanced Intel Speedstep Technology] ドロップダウン リスト **set EnhancedIntelSpeedStep**	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。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 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。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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。
[Intel Turbo Boost Technology] **set IntelTurboBoostTech**	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。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。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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
[Processor C3 Report] **set ProcessorC3Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C3 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS は C3 レポートの送信を行いません。 • [Enabled]：BIOS から C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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。
[Processor C6 Report] **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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。
[プロセッサの電源状態C1拡張（Processor Power State C1 Enhanced）] ドロップダウン リスト **set ProcessorC1EReport**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。

名前	説明
[P-STATE調整（P-STATE Coordination）] ドロップダウン リスト **set PsdCoordType**	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。 • [HW_ALL]：プロセッサ ハードウェアによって、依存関係にある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）によって、依存関係にある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）によって、依存関係にある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始できます。 （注） [Power Technology][CPUPowerManagement] を [Custom] 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。
[Boot Performance Mode] ドロップダウン リスト **set BootPerformanceMode**	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。次のいずれかになります。 • [最大パフォーマンス（Max Performance）]：プロセッサの P-state の比率が最大です。 • [Max Efficient]：プロセッサの P-state 率は最小です
[エネルギーパフォーマンスの調整（Energy Performance Tuning）] ドロップダウン リスト **set PwrPerfTuning**	エネルギー効率のバイアス調整のために BIOS またはオペレーティング システムを選択できます。次のいずれかになります。 • [OS]：エネルギーパフォーマンスの調整にOSを選択します。 • [BIOS]：エネルギー効率の調整のために BIOS を選択します。

名前	説明
[エネルギーパフォーマンス（Energy Performance）] ドロップダウン リスト **set CpuEngPerfBias**	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ーで重要かどうかを判断できます。次のいずれかになります。 • **Balanced_Energy** • **Balanced_Performance** • **Energy_Efficient** • **Performance**
[パッケージのCステートの制限（Package C State Limit）] ドロップダウン リスト **set PackageCStateLimit**	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 • [C0 state][C0_state]：サーバーはすべてのサーバー コンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • **[C1_state]**：CPU のアイドル時に、システムは電力消費を少し減らします。このオプションでは、必要な電力が C0 よりも少なく、サーバーはすばやくハイ パフォーマンス モードに戻ることができます。 • **[C3_state]**：CPU のアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • **[C6_state]**：CPU のアイドル時に、システムは C3 オプションの場合よりもさらに電力消費を減らします。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバーがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • **[C7_state]**：CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。このオプションでは、節約される電力量が最大になりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • **[No_Limit]**：サーバは、使用可能な任意の C ステートに入ることがあります。

名前	説明
[Extended APIC] **set LocalX2Apic**	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。次のいずれかになります。 • [XAPIC]：APIC サポートを有効にします。 • [X2APIC]：APIC を有効にして、Intel VT-d と Interrupt Remapping も有効にします。
[Workload Configuration] **set WorkLdConfig**	ワークロードの特性を最適化するようにパラメータを設定できます。次のいずれかになります。 • [Balanced]：最適化のためにバランスのとれたオプションを選択します。 • [I/O Sensitive]：最適化のために I/O を考慮したオプションを選択します。 （注） ワークロード構成は [Balanced] に設定することをお勧めします。
[CPU HWPM] ドロップダウンリスト **set HWPMEnable**	CPU のパフォーマンスやエネルギー効率を引き上げるためのハードウェア電源管理（HWPM）インターフェイスを有効にします。次のいずれかになります。 • [無効（Disabled）]：P-state は前世代のプロセッサと同じ方法で制御されます。 • [ネイティブモード（Native Mode）]：HWPM はソフトウェアインターフェイスを介してオペレーティング システムと連動します。 • [OOBモード（OOB Mode）]：CPU は、オペレーティング システムのエネルギー効率に基づいて周波数を自律的に制御します。
[CPU自律C-state] ドロップダウン リスト **set AutonumousCstateEnable**	HALT 命令を MWAIT 命令に変換する CPU 自律 C-state を有効にします。次のいずれかになります。 • [無効（Disabled）]：CPU 自律 C-state が無効になります。これはデフォルト値です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。

名前	説明
[プロセッサCMCI（Processor CMCI）] ドロップダウン リスト **set CmciEnable**	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性および機密性（RAS）の設定方法。次のいずれかになります。 • **[Maximum_Performance]**：システムのパフォーマンスが最適化されます。 • [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。 • [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きます。このオプションを使用した場合、[Mirroring] よりもシステム パフォーマンスが向上し、[Maximum Performance] よりも信頼性が向上しますが、[Mirroring] よりも信頼性が低く、[Maximum Performance] よりもシステム パフォーマンスは低下します。

名前	説明
[NUMA] ドロップダウン リスト **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [有効（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。
[チャネルインターリーブ（Channel Interleaving）] ドロップダウン リスト **set ChannelInterLeave**	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。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1Way][1_Way]：一部のチャネル インターリーブが使用されます。 • [2Way][2_Way] • [3Way][3_Way] • [4Way][4_Way]：最大のチャネル インターリーブが使用されます。
[Rank Interleaving] **set RankInterLeave**	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。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1Way][1_Way]：一部のランク インターリーブが使用されます。 • [2Way][2_Way] • [4Way][4_Way] • [8Way][8_Way]：最大量のランク インターリーブが使用されます。

名前	説明
[Patrol Scrub] **set PatrolScrub**	システムがサーバー上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [Disabled]：CPUがメモリ アド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。 • [有効（Enabled）]：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。
[デマンドスクラブ（Demand Scrub）] ドロップダウン リスト **set DemandScrub**	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。次のいずれかになります。 • [無効（Disabled）]：シングル ビット メモリ エラーは修正されません。 • [Enabled]：シングル ビット メモリ エラーがメモリ内部で修正され、修正されたデータが読み取り要求に応じて設定されます。
[高度（Altitude）] ドロップダウン リスト **set Altitude**	物理サーバーがインストールされている地点のおよその海抜（m 単位）。次のいずれかになります。 • [Auto]：物理的な高度をCPUによって判別します。 • [300M][300_M]：サーバーは海抜約 300 m の位置にあります。 • [900M][900_M]：サーバーは海抜約 900 m の位置にあります。 • [1500M][1500_M]：サーバーは海抜約 1500 m の位置にあります。 • **[3000_M]**：サーバーは、海抜約 3000 m です。

名前	説明
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト **PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリ コントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。

[QPI Configuration] のパラメータ

名前	説明
[QPI Link Frequency Select] **set QPILinkFrequency**	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（GT/s）単位）。次のいずれかになります。 • [Auto]：QPI リンク周波数は CPU によって決定されます。 • **6.4_GT/s** • 7.2_GT/s] • **8.0_GT/s**

名前	説明
[QPI Snoop Mode] **set QpiSnoopMode**	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [Auto]：CPU は自動的に早期スヌープ モードとして認識します。 • [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。 • [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もローカル遅延が高くなりますが、多数の未処理トランザクションに追加のリソースを提供します。 • [Home Directory Snoop]：ホーム ディレクトリはオプションで使用できる機能で、プロセッサ内の HA ロジックと iMC ロジックの両方に実装されています。ディレクトリの目的は、スケーラブルなプラットフォーム、および 2S と 4S の設定内のリモートソケット、およびノード コントローラへスヌープをフィルタリングすることです。 • [Home Directory Snoop with OSB]：Opportunistic Snoop Broadcast（OSB）ディレクトリ モードでは、HA は、ディレクトリ情報が収集されてチェックされる前であっても、非常に負荷の軽い状況下で推測的ホーム スヌープ ブロードキャストを選択できます。 • [クラスタ オン ダイ（Cluster on Die）]：クラスタ オン ダイが有効になります。有効化した LLC はそれぞれに独立したキャッシング エージェントで 2 つのパートに分割されます。これにより、一部のワークロードのパフォーマンスが向上します。このモードは、10 個以上のコアを搭載した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。

[USB Configuration] のパラメータ

名前	説明
[レガシーUSBサポート（Legacy USB Support）] ドロップダウン リスト **set LegacyUSBSupport**	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。次のいずれかになります。 • [無効（Disabled）]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [有効（Enabled）]：レガシーUSBのサポートは常に使用できます。 • [Auto]：USBデバイスが接続されていない場合、レガシーUSBのサポートがディセーブルになります。
[Port 60/64 Emulation] **set UsbEmul6064**	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。次のいずれかになります。 • [無効（Disabled）]：60h/64エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64エミュレーションはサポートされます。 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、このオプションを選択する必要があります。
[xHCI Mode] **set PchUsb30Mode**	xHCIコントローラのレガシーサポートを有効または無効にします。次のいずれかになります。 • [Disabled]：xHCIコントローラのレガシーサポートを無効にします。 • [Enabled]：xHCIコントローラのレガシーサポートを有効にします。
[xHCI Legacy Support] ドロップダウン リスト **set UsbXhciSupport**	システム上でのレガシーxHCIコントローラのサポートを有効/無効にします。次のいずれかになります。 • [無効（Disabled）]：xHCIレガシーサポートを無効にします。 • [有効（Enabled）]：xHCIレガシーサポートを有効にします。これはデフォルト値です。

名前	説明
[すべてのUSBデバイス（All USB Devices）] ドロップダウン リスト **set AllUsbDevices**	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。次のいずれかになります。 • [Disabled]：すべての USB デバイスが無効です。 • [Enabled]：すべての USB デバイスが有効になります。
[USB Port: Rear] **set UsbPortRear**	背面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：背面パネルのUSBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：背面パネルのUSBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[USB ポート：前面（USB Port:Front）] **set UsbPortFront**	前面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：前面パネルのUSBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：前面パネルのUSBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[USB Port: Internal] **set UsbPortInt**	内部USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：内部USBポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティングシステムによって検出されません。 • [有効（Enabled）]：内部USBポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。

名前	説明
[USB Port: KVM] **set UsbPortKVM**	vKVM ポートが有効か無効か。次のいずれかになります。 • **無効**：vKVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスは vKVM ウィンドウで機能しなくなります。 • **有効**：vKVM キーボードとマウス デバイスを有効にします。
[USB Port: vMedia] **set UsbPortVMedia**	仮想メディア デバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：vMediaデバイスをディセーブルにします。 • [Enabled]：vMedia デバイスを有効にします。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] **set MemoryMappedIOAbove4GB**	4GB を超える MMIO をイネーブルまたはディセーブルにするかどうか。次のいずれかになります。 • [Disabled]：サーバーでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効（Enabled）]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） 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。
[Sriov] **set SrIov**	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（Enabled）]：SR-IOV はイネーブルになります。

名前	説明
[ASPM サポート（ASPM Support）] ドロップダウン リスト **set ASPMSupport**	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。次のいずれかになります。 • [Disabled]：BIOS での ASPM サポートが無効です。 • [Force L0]：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。 • [自動（Auto）]：電力状態を CPU によって判別します。
[NVMe SSD ホットプラグのサポート（NVMe SSD Hot-Plug Support）] ドロップダウン リスト **set PCIeSSDHotPlugSupport**	サーバの電源を切ることなく、NVMe SSD を交換できます。次のいずれかになります。 • [無効（Disabled）]：NVMe SSD ホットプラグ サポートが無効です。これはデフォルト値です。 • [有効（Enabled）]：NVMe SSD ホットプラグ サポートが有効です。
[VGA 優先順位（VGA Priority）] ドロップダウン リスト **set VgaPriority**	システムに複数の VGA デバイスがある場合は、VGA グラフィックス デバイスの優先順位を設定できます。次のいずれかになります。 • [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。 • [Offboard]：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 無効（Onboard VGA Disabled）]：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。

[Serial Configuration] のパラメータ

名前	説明
[Out-of-Band Mgmt Port] **set comSpcrEnable**	Windows 緊急管理サービスで使用可能な COM ポート 0 を設定することができます。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。次のいずれかになります。 • [Disabled]：Windows オペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [有効（Enabled）]：Windows 緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。
[コンソールリダイレクション（Console redirection）] ドロップダウン リスト **set ConsoleRedir**	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。次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。 • [COM 0]：POST中に COM ポート 0 でコンソール リダイレクションを有効にします。 • [COM 1]：POST中に COM ポート 1 でコンソール リダイレクションを有効にします。
[Terminal type] **set TerminalType**	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。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100+]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） 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。

名前	説明
[Bits per second] **set BaudRate**	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。[Console Redirection] を無効にする場合は、このオプションを使用できません。次のいずれかになります。 • [9600]：9,600 ボー レートが使用されます。 • [19200]：19,200 ボー レートが使用されます。 • [38400]：38,400 ボー レートが使用されます。 • [57600]：57,600 ボー レートが使用されます。 • [115200]：115,200 ボー レートが使用されます。 （注） 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。
[フロー制御（Flow Control）] ドロップダウン リスト **set FlowCtrl**	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。次のいずれかになります。 • [None]：フロー制御は使用されません。 • **Hardware_RTS/CTS**：フロー制御に RTS/CTS が使用されます。 （注） 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。

名前	説明
[Putty KeyPad] **set PuttyFunctionKeyPad**	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。次のいずれかになります。 • [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 仮想コンソールを模倣します。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。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 によって ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 によって **ESC [M** ～ **ESC [X** を生成します。ファンクション キーと Shift キーによって **ESC [Y** ～ **ESC [j** を生成します。Ctrl キーとファンクション キーによって **ESC [k** ～ **ESC [v** を生成します。Shift、Ctrl およびファンクション キーによって **ESC [w** ～ **ESC [{** 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。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。 • [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。
[Redirection After BIOS POST] **set RedirectionAfterPOST**	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。次のいずれかになります。 • **[Always_Enable]**：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。

[LOM and PCIe Slots Configuration] のパラメータ

名前	説明
[VICに対するCDNサポート（CDN Support for VIC）] ドロップダウン リスト **set CdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。
[PCI ROM CLP] **set PciRomClp**	PCI ROM Command Line Protocol（CLP）は、カード上の iSCSI や PxE などのさまざまなオプション ROM の実行を制御します。デフォルト設定は、ディセーブルです。 • [Enabled]：ポートごとに個別に、iSCSI や PxE などのさまざまなオプション ROM の実行を設定できるようにします。 • [Disabled]：デフォルト オプションです。異なるオプション ROM は選択できません。デフォルト オプション ROM は PCI 列挙中に実行されます。
[PCH SATA Mode] **set SataModeSelect**	このオプションでは、PCH SATA モードを選択できます。次のいずれかになります。 • [AHCI]：SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [Disabled]：SATA コントローラと sSATA コントローラを無効にします。 • [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。
[All Onboard LOM Ports] **set AllLomPortControl**	すべての LOM ポートを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべての LOM ポートが無効です。 • [Enabled]：すべての LOM ポートが有効になります。

名前	説明
[LOM Port *n* OptionROM] **set LomOpromControlPort*n***	***n*** で指定された LOM ポートでオプション ROM を使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI_Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy_Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。
[All PCIe Slots OptionROM] **set PcieOptionROMs**	PCIe カードのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI_Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy_Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:*n* OptionROM **set PcieSlot*n*OptionROM**	PCIe カードのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット ***n*** のオプション ROM は使用できません。 • [Enabled]：スロット ***n*** のオプション ROM は使用可能です。 • **[UEFI_Only]**：スロット ***n*** のオプション ROM は UEFI にのみ使用できます。 • **[Legacy_Only]**：スロット ***n*** のオプション ROM はレガシーにのみ使用できます。

名前	説明
[PCIe Slot:MLOM OptionROM] **set PcieSlotMLOMOptionROM**	このオプションでは、MLOM スロットに接続された 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。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:HBA OptionROM] **set PcieSlotHBAOptionROM**	このオプションでは、HBA スロットに接続された 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。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:N1 OptionROM] **set PcieSlotN1OptionROM**	このオプションでは、SSD:NVMe1 スロットに接続された 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。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。

名前	説明
[PCIe Slot:N2 OptionROM] **set PcieSlotN2OptionROM**	このオプションでは、SSD:NVMe2 スロットに接続された 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。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[PCIe Slot:HBA Link Speed] **PCIe SlotHBALinkSpeed**	このオプションを使用すると、PCIe HBA スロット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。次のいずれかになります。 • [自動（Auto）]：システムは許可される最大速度を選択します。 • [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。 • [GEN2]：最大 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。 • [Disabled]：最大速度は制限されません。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。

名前	説明
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C220M4 および C240M4 サーバの [サーバ管理（Server Management）] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[Save Changes] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

サーバ管理 BIOS パラメータ

名前	説明
[FRB-2 Timer] **set FRB-2**	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 Cisco IMC で FRB2 タイマーを使用するかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバーのブートにかかる時間をウォッチドッグタイマーでトラッキングします。サーバーが **set OSBootWatchdogTimerTimeout** コマンドにより、Cisco IMC はエラーをログに記録し、**set OSBootWatchdogTimerPolicy** コマンドで指定されたアクションを実行します。
[OSウォッチドッグタイマータイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	OSが指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • **[5_Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • **[10_Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • **[15_Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • **[20_Minutes]**：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。

名前	説明
[OSウォッチドッグタイマーポリシー（OS Watchdog Timer Policy）] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	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。次のいずれかになります。 • **Do_Nothing**：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、アクションは実行されません。 • **Power_Down**：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバーの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

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。