UCS サーバの BIOS トークン

リリースでのサーバ BIOS トークン 4.2(2c)

Cisco UCS Manager は、4.2(2c) リリースで次のサーバーをサポートします。

- C220 M6
- C240 M6

M4 および M5 サーバでサポートされる Cisco UCS C シリーズおよび B シリーズ BIOS トークンについては、Cisco UCS サーバ BIOS トークン、リリース 4.1 を参照してください。

4.2(2c) の C220 M6 と C240 M6 の BIOS トークン

次の表に、4.2(2c) リリース用の新規 BIOS トークンを示します。

名前	デフォルト値	M6 サーバでサポートされている値	プラットフォーム	新規/変更
[TPM の最小限の物理的存在（TPM Minimal Physical Presence）]	無効	[ディセーブル（Disabled）]、[イネーブル（Enabled）]	C220 M6 および C240 M6	New
[DMA 制御オプトインフラグ（DMA Control Opt-In Flag）]	無効	[ディセーブル（Disabled）]、[イネーブル（Enabled）]	C220 M6 および C240 M6	新たな統合

リリースでのサーバ BIOS トークン 4.2(1m)

Cisco UCS Manager は、4.2(1m) で次のサーバーを引き続きサポートします。

- C220 M6
- C240 M6
- C225 M6
- C245 M6
- B200 M6

M4 および M5 サーバでサポートされる Cisco UCS C シリーズおよび B シリーズ BIOS トークンについては、Cisco UCS サーバ BIOS トークン、リリース 4.1 を参照してください。

4.2(1m) の新規および変更された BIOS トークン

名前	デフォルト値	M6 サーバでサポートされている値	プラットフォーム	依存関係	新規/変更
Execute Disable Bit	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C220 M6、C240 M6、C225 M6、C245 M6、B200 M6		新たな統合

リリースでのサーバ BIOS トークン 4.2(1l)

Cisco UCS Manager では、4.2(1l) で次のサーバーのサポートが導入されています。

- C225 M6

Cisco UCS Manager は、4.2(1l) で次のサーバーを引き続きサポートします。

- C220 M6
- C240 M6
- C245 M6
- B200 M6

M4 および M5 サーバでサポートされる Cisco UCS C シリーズおよび B シリーズ BIOS トークンについては、Cisco UCS サーバ BIOS トークン、リリース 4.1 を参照してください。

C225 M6 の BIOS トークン（4.2(1l) 内）

名前	デフォルト値	M6 サーバでサポートされている値	プラットフォーム	依存関係
MLOM Link Speed	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C225 M6	
MLOM OptionROM	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C225 M6	
[PCIe スロット（PCIe Slot）：*n* リンク速度（Link Speed）]	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C225 M6	*n* は、1 から 3 までの整数を指します。
PCIe Slot *n* OptionROM	イネーブル	Enabled、Disabled	C225 M6	*n* は、1 から 3 までの整数を指します。
MRAID Link Speed	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C225 M6	
MRAID OptionROM	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C225 M6	
[フロント NVMe（Front NVME）] *n* [リンク速度（Link Speed）]	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C225 M6	*n* は、1 から 10 までの整数を指します。
[フロント NVMe（Front NVME）] *n* [OptionROM]	イネーブル	Enabled、Disabled	C225 M6	*n* は、1 から 10 までの整数を指します。
PCIeスロットMSTORリンク速度	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C225 M6	
PCIeスロットMSTOR RAID OptionROM	イネーブル	Enabled、Disabled	C225 M6	
コア パフォーマンス ブースト	自動	無効、自動	C225 M6	

名前	デフォルト値	M6 サーバでサポートされている値	プラットフォーム	依存関係
グローバル C 状態制御	自動（Auto）	無効、有効、自動	C225 M6	
L1 ストリーミング HW プリフェッチャ	自動（Auto）	無効、有効、自動	C225 M6	
L2 ストリーミング HW プリフェッチャ	自動（Auto）	無効、有効、自動	C225 M6	
ソケットごとのNUMA ノード	自動（Auto）	NPS0、NPS1、NPS2、NPS4、自動	C225 M6	
メモリインターリーブサイズ	自動（Auto）	256 Bytes、512 Bytes、1 KB、2 KB、4KB、自動	C225 M6	
Chipselect インターリーブ	自動	無効、自動	C225 M6	
バンク グループ スワップ	自動	有効、無効、自動	C225 M6	
Determinism スライダ	自動	パワー、パフォーマンス、自動	C225 M6	
[IOMMU]	自動（Auto）	無効、有効、自動	C225 M6	
[SMT モード（SMT Mode）]	有効	無効、有効、自動	C225 M6	
SVMモード	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C225 M6	
効率モードが有効	自動（Auto）	自動、有効	C225 M6	
SNPメモリカバレッジ	自動（Auto）	自動、有効、無効、カスタム	C225 M6	
カバーされるSNPメモリサイズ(MB)	0	0 ～ 1048576	C225 M6	
CPPC	自動	自動、有効、無効	C225 M6	
SEV-SNPサポート	ディセーブル	Enabled、Disabled	C225 M6	
[SMEE]	自動	自動、有効、無効	C225 M6	

名前	デフォルト値	M6 サーバでサポートされている値	プラットフォーム	依存関係
CPUダウンコア制御7xx3	自動（Auto）	自動、ワン（1+0）、ツー（2+0）、スリー（3+0）、フォー（4+0）、ファイブ（5+0）、シックス（6+0）、セブン（7+0）	C225 M6	
ダウンコア制御7xx2	自動（Auto）	自動、TWO (1 + 1)、FOUR (2 + 2)、SIX (3 + 3)	C225 M6	
固定されたSOC P-State	自動（Auto）	P0、P1、P2、P3、自動	C225 M6	
APBDIS	自動（Auto）	0、1、自動	C225 M6	
CCD制御	自動（Auto）	自動、2 CCD、3 CCD、4 CCD、6 CCD	C225 M6	
Cisco xGMIの最大速度	無効	[ディセーブル（Disabled）]、[イネーブル（Enabled）]	C225 M6	
NUMAドメインとしてのACPI SRAT L3キャッシュ	自動（Auto）	無効、有効、自動	C225 M6	
ストリーミングストア制御	自動（Auto）	無効、有効、自動	C225 M6	
DF C-State	自動（Auto）	無効、有効、自動	C225 M6	
バーストリフレッシュおよび遅延リフレッシュ	ディセーブル	Enabled、Disabled	C225 M6	
[SR-IOV のサポート（SR-IOV Support）]	イネーブル	Enabled、Disabled	C225 M6	
PCIe ARIサポート	自動	自動、有効、無効	C225 M6	
TSME	自動	自動、有効、無効	C225 M6	
[BIOS Techlogレベル（BIOS Techlog Level）]	最小ハードウェア	Maximum、Normal、Minimum	C225 M6	
[OptionROM起動最適化（OptionROM Launch Optimization）]	イネーブル	Enabled、Disabled	C225 M6	

名前	デフォルト値	M6 サーバでサポートされている値	プラットフォーム	依存関係
4 GB 以上の復号化	イネーブル	Enabled、Disabled	C225 M6	
[SMEE]	イネーブル	Enabled、Disabled	C225 M6	
[SMT モード（SMT Mode）]	消灯	Auto, Off	C225 M6	
[SR-IOV のサポート（SR-IOV Support）]	イネーブル	Enabled、Disabled	C225 M6	
SVMモード	イネーブル	Enabled、Disabled	C225 M6	
端末タイプ	VT 100	PC-ANSI、VT100、VT100-PLUS、VT-UTF8	C225 M6	
SHA-1 PCRバンク	イネーブル	Enabled、Disabled	C225 M6	
SHA256 PCRバンク	イネーブル	Enabled、Disabled	C245 M6	
[FRB 2 タイマー（FRB 2 Timer）]	イネーブル	Enabled、Disabled	C225 M6	
[OS ウォッチドッグタイマー（OS Boot Watchdog Timer）]	イネーブル	Enabled、Disabled	C225 M6	
OS Boot Watchdog Timer Policy	Power Off	Power Off、Reset	C225 M6	
OS Boot Watchdog Timer Timeout	10 分	5 minutes、10 minutes、15 minutes、20 minutes	C225 M6	
Flow Control	なし	None、RTS-CTS	C225 M6	
[ボー レート（Baud rate）]	115.2k	9.6k、19.2k、38.4k、57.6k、115.2k	C225 M6	
端末タイプ	VT100	PC-ANSI、VT100、VT100-PLUS、VT-UTF8	C225 M6	コンソールリダイレクションが COM 0 である場合にのみ適用されます。

名前	デフォルト値	M6 サーバでサポートされている値	プラットフォーム	依存関係
[コンソールのリダイレクト（Console Redirection）]	ディセーブル	無効、COM0、COM1 または serial-port-b	C225 M6	

リリースでのサーバ BIOS トークン 4.2(1i)

Cisco UCS Manager では、4.2(1i) で次のサーバーのサポートが導入されています。

- C245 M6

Cisco UCS Manager は、4.2(1i) で次のサーバーを引き続きサポートします。

- C220 M6
- C240 M6
- B200 M6

M4 および M5 サーバでサポートされる Cisco UCS C シリーズおよび B シリーズ BIOS トークンについては、Cisco UCS サーバ BIOS トークン、リリース 4.1 を参照してください。

C245 M6 の BIOS トークン（4.2(1i) 内）

名前	デフォルト値	M6サーバでサポートされている値	プラットフォーム	依存関係
MLOM Link Speed	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C245 M6	
MLOM OptionROM	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C245 M6	
[PCIe スロット（PCIe Slot）：*n* リンク速度（Link Speed）]	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C245 M6	*n* は、1 から 8 までの整数を指します。
PCIe Slot *n* OptionROM	イネーブル	Enabled、Disabled	C245 M6	*n* は、1 から 8 までの整数を指します。
[MRAID]*n* [リンク速度（Link Speed）]	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C245 M6	*n* は整数 1 または 2 を表します。

名前	デフォルト値	M6サーバでサポートされている値	プラットフォーム	依存関係
MRAID*n* OptionROM	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C245 M6	*n* は整数 1 または 2 を表します。
[フロント NVMe（Front NVME）] *n* [リンク速度（Link Speed）]	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C245 M6	*n* は、1 から 4 までの整数を指します。
[フロント NVMe（Front NVME）] *n* [OptionROM]	イネーブル	Enabled、Disabled	C245 M6	*n* は、1 から 4 までの整数を指します。
[背面 NVMe（Rear NVME）] *n* [リンク速度（Link Speed）]	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C245 M6	*n* は、1 から 4 までの整数を指します。
[背面 NVMe（Rear NVME）] *n* [OptionROM]	イネーブル	Enabled、Disabled	C245 M6	*n* は、1 から 4 までの整数を指します。
PCIeスロットMSTORリンク速度	自動（Auto）	無効、自動、GEN1、GEN2、GEN3、GEN4	C245 M6	
PCIeスロットMSTOR RAID OptionROM	イネーブル	Enabled、Disabled	C245 M6	
[FRB 2 タイマー（FRB 2 Timer）]	イネーブル	Enabled、Disabled	C245 M6	
OS Boot Watchdog Timer Policy	Power Off	Power Off、Reset	C245 M6	
Flow Control	なし	None、RTS-CTS	C245 M6	
[ボー レート（Baud rate）]	115.2k	9.6k、19.2k、38.4k、57.6k、115.2k	C245 M6	

名前	デフォルト値	M6サーバでサポートされている値	プラットフォーム	依存関係
端末タイプ	VT100	PC-ANSI、VT100、VT100-PLUS、VT-UTF8	C245 M6	コンソールリダイレクションが COM 0 である場合にのみ適用されます。
[コンソールのリダイレクト（Console Redirection）]	ディセーブル	COM 0、COM 1、ディセーブル	C245 M6	コンソールリダイレクションが COM 0 である場合にのみ適用されます。
[信頼されたプラットフォームモジュールの状態（Trusted Platform Module State）]	イネーブル	Enabled、Disabled	C245 M6	
SHA-1 PCRバンク	イネーブル	Enabled、Disabled	C245 M6	
SHA256 PCRバンク	イネーブル	Enabled、Disabled	C245 M6	
ポストパッケージ修復	ハードPPR	無効、ハード PPR	C245 M6	
4G以上の復号(Above 4G Decoding)	イネーブル	Enabled、Disabled	C245 M6	
CDN Control	イネーブル	Enabled、Disabled	C245 M6	
[OptionROM起動最適化（OptionROM Launch Optimization）]	イネーブル	Enabled、Disabled	C245 M6	
[BIOS Techlogレベル（BIOS Techlog Level）]	最小ハードウェア	Maximum、Normal、Minimum	C245 M6	
[電源オンパスワード（Power ON Password）]	ディセーブル	Enabled、Disabled	C245 M6	
IPV6 PXE サポート（IPV6 PXE Support）	ディセーブル	Enabled、Disabled	C245 M6	
BME DMA 緩和	ディセーブル	Enabled、Disabled	C245 M6	

名前	デフォルト値	M6サーバでサポートされている値	プラットフォーム	依存関係
ネットワークスタック	イネーブル	Enabled、Disabled	C245 M6	
IPv4 PXEサポート	イネーブル	Enabled、Disabled	C245 M6	
IPv4 HTTPサポート	イネーブル	Enabled、Disabled	C245 M6	
IPv6 HTTPサポート	イネーブル	Enabled、Disabled	C245 M6	
コアパフォーマンス ブースト	自動	無効、自動	C245 M6	
グローバル C 状態制御	自動（Auto）	無効、有効、自動	C245 M6	
L1 ストリーミング HW プリフェッチャ	自動（Auto）	無効、有効、自動	C245 M6	
L2 ストリーミング HW プリフェッチャ	自動（Auto）	無効、有効、自動	C245 M6	
ソケットごとのNUMA ノード	自動（Auto）	NPS0、NPS1、NPS2、NPS4、自動	C245 M6	
メモリインターリーブサイズ	自動（Auto）	256 Bytes、512 Bytes、1 KB、2 KB、4KB、自動	C245 M6	
Chipselect インターリーブ	自動	無効、自動	C245 M6	
バンク グループ スワップ	自動	有効、無効、自動	C245 M6	
Determinism スライダ	自動	パワー、パフォーマンス、自動	C245 M6	
[IOMMU]	自動（Auto）	無効、有効、自動	C245 M6	
[SMT モード（SMT Mode）]	有効	無効、有効、自動	C245 M6	
SVMモード	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C245 M6	
効率モードが有効	自動（Auto）	自動、有効	C245 M6	
SNPメモリカバレッジ	自動（Auto）	自動、有効、無効、カスタム	C245 M6	

名前	デフォルト値	M6サーバでサポートされている値	プラットフォーム	依存関係
カバーされるSNPメモリサイズ(MB)	0	0 ～ 1048576	C245 M6	
CPPC	自動	自動、有効、無効	C245 M6	
SEV-SNPサポート	ディセーブル	Enabled、Disabled	C245 M6	
[SMEE]	自動	自動、有効、無効	C245 M6	
CPUダウンコア制御7xx3	自動（Auto）	自動、ワン（1+0）、ツー（2+0）、スリー（3+0）、フォー（4+0）、ファイブ（5+0）、シックス（6+0）、セブン（7+0）	C245 M6	
固定されたSOC P-State	自動（Auto）	P0、P1、P2、P3、自動	C245 M6	
APBDIS	自動（Auto）	0、1、自動	C245 M6	
CCD制御	自動（Auto）	自動、2 CCD、3 CCD、4 CCD、6 CCD	C245 M6	
Cisco xGMIの最大速度	無効	[ディセーブル（Disabled）]、[イネーブル（Enabled）]	C245 M6	
NUMAドメインとしてのACPI SRAT L3キャッシュ	自動（Auto）	無効、有効、自動	C245 M6	
ストリーミングストア制御	自動（Auto）	無効、有効、自動	C245 M6	
DF C-State	自動（Auto）	無効、有効、自動	C245 M6	
ポストパッケージ修復	ハードPPR	無効、ハード PPR	C245 M6	
バーストリフレッシュおよび遅延リフレッシュ	ディセーブル	Enabled、Disabled	C245 M6	
[SR-IOV のサポート（SR-IOV Support）]	イネーブル	Enabled、Disabled	C245 M6	
PCIe ARIサポート	自動	自動、有効、無効	C245 M6	
TSME	自動	自動、有効、無効	C245 M6	

名前	デフォルト値	M6サーバでサポートされている値	プラットフォーム	依存関係
[BIOS Techlogレベル（BIOS Techlog Level）]	最小ハードウェア	Maximum、Normal、Minimum	C245 M6	
[OptionROM起動最適化（OptionROM Launch Optimization）]	イネーブル	Enabled、Disabled	C245 M6	
4 GB 以上の復号化	イネーブル	Enabled、Disabled	C245 M6	
[SMEE]	イネーブル	Enabled、Disabled	C245 M6	
[SMT モード（SMT Mode）]	消灯	Auto, Off	C245 M6	
[SR-IOV のサポート（SR-IOV Support）]	イネーブル	Enabled、Disabled	C245 M6	
SVMモード	イネーブル	Enabled、Disabled	C245 M6	
端末タイプ	VT 100	PC-ANSI、VT100、VT100-PLUS、VT-UTF8	C245 M6	
[OS ウォッチドッグ タイマー（OS Boot Watchdog Timer）]	イネーブル	Enabled、Disabled	C245 M6	
OS Boot Watchdog Timer Timeout	10 分	5 minutes、10 minutes、15 minutes、20 minutes	C245 M6	

リリースでのサーバ BIOS トークン 4.2(1f)

Cisco UCS Manager は、4.2(1f) リリースで次のサーバーをサポートします。

- C220 M6
- C240 M6
- B200 M6

次の表に、4.2(1f) リリース用の新規および更新された BIOS トークンを示します。

表 *1* : 新規および更新された *BIOS* トークン *4.2(1f)*

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	新規/変更
強力なCPUパフォーマンス	無効	無効、自動	C220 M6、C240 M6、および B200 M6	新たな統合
UPIリンク有効化	自動（Auto）	自動、1、2	C220 M6、C240 M6、および B200 M6	新たな統合
仮想Numa	ディセーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
LLCデッドライン	有効	自動、有効、無効	C220 M6、C240 M6、および B200 M6	新たな統合
C1自動降格	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
C1自動降格解除	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
XPTリモートプリフェッチ	自動	自動、有効、無効	C220 M6、C240 M6、および B200 M6	新たな統合
[UPI電源管理（UPI Power Management）]	無効	[ディセーブル（Disabled）]、[イネーブル（Enabled）]	C220 M6、C240 M6、および B200 M6	新たな統合
SHA-1 PCRバンク	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C220 M6、C240 M6、および B200 M6	新たな統合
SHA256-PCR-Bank	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C220 M6、C240 M6、および B200 M6	新たな統合
[FRB 2 タイマー（FRB 2 Timer）]	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
OS Boot Watchdog Timer Policy	Power Off	Power Off、Reset	C220 M6、C240 M6、および B200 M6	新たな統合

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	新規/変更
[OS ウォッチドッグ タイマー（OS Boot Watchdog Timer）]	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
Flow Control	なし	None、RTS-CTS	C220 M6、C240 M6、および B200 M6	新たな統合
Legacy USB Support	イネーブル	有効、無効、自動	C220 M6、C240 M6、および B200 M6	新たな統合
[ボー レート（Baud rate）]	115.2k	9.6k、19.2k、38.4k、57.6k、115.2k	C220 M6、C240 M6、および B200 M6	新たな統合
端末タイプ	VT100	PC-ANSI、VT100、VT100-PLUS、VT-UTF8	C220 M6、C240 M6、および B200 M6	新たな統合
[コンソールのリダイレクト（Console Redirection）]	ディセーブル	無効、COM0、COM1 または serial-port-b	C220 M6、C240 M6、および B200 M6	新たな統合
トラステッド プラットフォームモジュールサポート	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
[TPM 保留中の操作（TPM Pending operation）]	なし	なし、TpmClear	C220 M6、C240 M6、および B200 M6	新たな統合
Intel VT for directed IO	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
Intel VTD coherency support	ディセーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	新規/変更
Intel Trusted Execution Technology サポート（Intel Trusted Execution Technology Support）	ディセーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
インテル バーチャライゼーション テクノロジー	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
MLOM OptionROM	イネーブル	[無効（Disabled）]、[有効（Enabled）]	C220 M6、C240 M6、および B200 M6	新たな統合
OS Boot Watchdog Timer Timeout	10 分	5 minutes、10 minutes、15 minutes、20 minutes	C220 M6、C240 M6、および B200 M6	新たな統合
[メモリ RAS 構成の選択（Select Memory RAS Configuration）]	ADDDC のスペアリング	Maximum performance、Mirror-mode-1lm、ADDDC Sparing、Partial-mirror-mode-1lm	C220 M6、C240 M6、および B200 M6	新たな統合
[ターボ モード（Turbo Mode）]	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
EIST PSD関数（EIST PSD Function）	HW all	HWすべて、SWすべて	C220 M6、C240 M6、および B200 M6	新たな統合
非コア周波数スケーリング	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合
SpeedStep(Pstates)	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	新たな統合

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	新規/変更
[CPU PA を 46 ビットに制限（LIMIT CPU PA to 46 Bits）]	イネーブル	Enabled、Disabled	C220 M6、C240 M6、および B200 M6	変更済み
[仮想 NUMA（Virtual NUMA）]	無効	有効、無効、自動	C220 M6、C240 M6、および B200 M6	変更済み
LLCデッドライン	有効	有効、無効、自動	C220 M6、C240 M6、および B200 M6	変更済み
XPTリモートプリフェッチ	自動	有効、無効、自動	C220 M6、C240 M6、および B200 M6	変更済み
スロット9の状態	無効	Disabled、Enabled、UEFI Only、Legacy Only	C220 M6、C240 M6、および B200 M6	変更済み

リリースでのサーバ BIOS トークン 4.2(1d)

Cisco UCS Manager では、4.2(1d) で次のサーバーのサポートが導入されています。

- C220 M6：4.2(1d) の C220 M6 と C240 M6 の BIOS トークン （17 ページ）
- C240 M6：4.2(1d) の C220 M6 と C240 M6 の BIOS トークン （17 ページ）
- B200 M6：B200 M6 の BIOS トークン（4.2(1d) 内） （22 ページ）

Cisco UCS Manager は、4.2(1d) で次のサーバーを引き続きサポートします。

- B200 M5
- B480 M5
- C220 M5
- C240 M5
- C240 SD M5
- C480 M5
- S3260 M5
- C125 M5

- C480 M5 ML
- C220 M4
- C240 M4
- C460 M4
- S3260 M4

M4 および M5 サーバでサポートされる Cisco UCS C シリーズおよび B シリーズ BIOS トークンについては、Cisco UCS サーバ BIOS トークン、リリース 4.1 を参照してください。また、更新された M5 サーバーのサポートについては、以下の 4.2(1d) の M5 サーバーの新規および変更された BIOS トークン （27 ページ） を参照してください。

4.2(1d) の C220 M6 と C240 M6 の BIOS トークン

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
Core Multi Processing	すべて（All）	すべて、1 ～ 48	C220 M6 および C240 M6	
CR QoS	モード 0 : PMem QoS 機能を無効にする	レシピ 1、レシピ 2、レシピ 3、無効、モード 0 - PMem QoS 機能を無効にする、モード 1 - M2M QoS Enable ;CHA QoS 無効、モード 2 - M2M QoS Enable;CHA QoS 有効	C220 M6 および C240 M6	
IIO eDPCサポート	OnFatal エラーと致命的でないエラー	致命的なエラー、無効、OnFatal および致命的でないエラーについて	C220 M6 および C240 M6	
Multikey Total Memory Encryption (MK-TME)	ディセーブル	Enabled、Disabled	C220 M6 および C240 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
SWガード拡張(SGX)	ディセーブル	Enabled、Disabled	C220 M6 および C240 M6	
Total Memory Encryption(TME)	ディセーブル	Enabled、Disabled	C220 M6 および C240 M6	
Owner EPOCH入力タイプを選択	手動ユーザー定義の所有者EPOCH	SGX 所有者 EPOCH がアクティブ化されました。新しいランダム所有者 EPOCH に変更します。手動でユーザー定義の所有者 EPOCH を作成します。	C220 M6 および C240 M6	
UPIプリフェッチ	自動	自動、有効、無効	C220 M6 および C240 M6	
部分的なキャッシュ行の節約	イネーブル	Enabled、Disabled	C220 M6 および C240 M6	
[PPR タイプ構成の選択（Select PPR Type Configuration）]	ハードPPR	ハード PPR、ソフト PPR、無効	C220 M6 および C240 M6	
SGX自動MP登録エージェント	ディセーブル	Enabled、Disabled	C220 M6 および C240 M6	
SProcessor Epoch*n*	0	*n*	C220 M6 および C240 M6	
[SGX 初期設定へのリセット（SGX Factory Reset）]	ディセーブル	Enabled、Disabled	C220 M6 および C240 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
[SGX PUBKEY HASH*n*]	0	SGX PUBKEY HASH0-Between 7-0、SGX PUBKEY HASH1-Between 15-8、SGX PUBKEY HASH2-Between 23-16、SGX PUBKEY HASH3-Between 31-24	C220 M6 および C240 M6	
SGX書き込みが有効	イネーブル	Enabled、Disabled	C220 M6 および C240 M6	
SGXパッケージ情報インバンドアクセス	ディセーブル	Enabled、Disabled	C220 M6 および C240 M6	
SGX QoS	イネーブル	Enabled、Disabled	C220 M6 および C240 M6	
強力なメモリテスト	自動	自動、無効、有効	C220 M6 および C240 M6	
Intel Dynamic Speed Select	ディセーブル	Enabled、Disabled	C220 M6 および C240 M6	
[インテル Speed Select（Intel Speed Select）]	基本	ベース、構成 1、構成 2、構成 3、構成 4	C220 M6 および C240 M6	
UPI Link Frequency Select	自動	9.6GT/s、10.4GT/s、11.2GT/s、自動、リンクごとの設定を使用	C220 M6 および C240 M6	
[UMA クラスタリング（UMA Clustering）]	Hemisphere(2-clusters)	Hemisphere(2-clusters), Disable(All-2-All)	C220 M6 および C240 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
MLOM Link Speed	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C220 M6 および C240 M6	
[PCIe スロット MSTOR-RAID リンク速度（PCIe Slot MSTOR-RAID Link Speed）]	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C220 M6 および C240 M6	
MRAID Link Speed	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C220 M6	
[MRAID]*n* [リンク速度（Link Speed）]	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C240 M6	*n* は、1 から 2 までの整数を指します。
[MRAID*n* OptionROM]	イネーブル	Enabled、Disabled	C240 M6	*n* は、1 から 2 までの整数を指します。
[フロント Nvme（Front NVME） *n* OptionROM]	イネーブル	[無効（Disabled）]、[有効（Enabled）]	1 から 10 までの *n* の場合、C220 M6 および C240 M6 をサポートします。 *n* 範囲 11 および 24 は、C240 M6 をサポートします	
[フロント NVMe（Front NVME）] *n* [リンク速度（Link Speed）]	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	1 から 10 までの *n* の場合、C220 M6 および C240 M6 をサポートします。 *n* 範囲 11 および 10 は、C240 M6 をサポートします	*n* は、1 から 12 までの整数を指します。

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
[PCIe スロット（PCIe Slot）：*n* リンク速度（Link Speed）]	自動（Auto）	自動、無効、GEN1、GEN2、GEN3、GEN4	C240 M6	*n* は、4 から 8 までの整数を指します。
PCIe Slot *n* OptionROM	イネーブル	Enabled、Disabled	C240 M6	*n* は、4 から 8 までの整数を指します。
[背面 NVMe（Rear NVME）] *n* [リンク速度（Link Speed）]	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C240 M6	*n* は、1 から 4 までの整数を指します。
リア NVME n オプション ROM	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C240 M6	*n* は、1 から 4 までの整数を指します。
eADRサポート	無効	自動、有効、無効	C220 M6 および C240 M6	
揮発性メモリモード	2LM	2LM、1LM	C220 M6 および C240 M6	
メモリ帯域幅ブースト	イネーブル	Enabled、Disabled	C220 M6 および C240 M6	
CR FastGo設定	自動	自動、デフォルト、オプション 1、オプション 2、オプション 3、オプション 4、オプション 5、最適化を有効にする、最適化を無効にする	C220 M6 および C240 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
メモリのリフレッシュレート	2x更新	1x リフレッシュ、2x リフレッシュ	C220 M6 および C240 M6	
[コンソールのリダイレクト（Console Redirection）]	ディセーブル	無効、COM0、COM1 または serial-port-b	C220 M6 および C240 M6	

B200 M6 の BIOS トークン（4.2(1d) 内）

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
Core Multi Processing	すべて（All）	すべて、1 ～ 48	B200 M6	
CR QoS	モード 0 : PMem QoS 機能を無効にする	レシピ 1、レシピ 2、レシピ 3、無効、モード 0 - PMem QoS 機能を無効にする、モード 1 - M2M QoS Enable ;CHA QoS 無効、モード 2 - M2M QoS Enable;CHA QoS 有効	B200 M6	
IIO eDPCサポート	OnFatal エラーと致命的でないエラー	致命的なエラー、無効、OnFatal および致命的でないエラーについて	B200 M6	
Multikey Total Memory Encryption (MK-TME)	ディセーブル	Enabled、Disabled	B200 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
SWガード拡張(SGX)	ディセーブル	Enabled、Disabled	B200 M6	
Total Memory Encryption(TME)	ディセーブル	Enabled、Disabled	B200 M6	
Owner EPOCH入力タイプを選択	手動ユーザー定義の所有者EPOCH	SGX 所有者 EPOCH がアクティブ化されました。新しいランダム所有者 EPOCH に変更します。手動でユーザー定義の所有者 EPOCH を作成します。	B200 M6	
UPIプリフェッチ	自動	自動、有効、無効	B200 M6	
部分的なキャッシュ行の節約	イネーブル	Enabled、Disabled	B200 M6	
[PPR タイプ構成の選択（Select PPR Type Configuration）]	ハードPPR	ハード PPR、ソフト PPR、無効	B200 M6	
SGX自動MP登録エージェント	ディセーブル	Enabled、Disabled	B200 M6	
SProcessor Epoch*n*	0	*n*	B200 M6	
[SGX 初期設定へのリセット（SGX Factory Reset）]	ディセーブル	Enabled、Disabled	B200 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
[SGX PUBKEY HASH*n*]	0	SGX PUBKEY HASH0-Between 7-0、SGX PUBKEY HASH1-Between 15-8、SGX PUBKEY HASH2-Between 23-16、SGX PUBKEY HASH3-Between 31-24	B200 M6	
SGX書き込みが有効	イネーブル	Enabled、Disabled	B200 M6	
SGXパッケージ情報インバンドアクセス	ディセーブル	Enabled、Disabled	B200 M6	
SGX QoS	イネーブル	Enabled、Disabled	B200 M6	
強力なメモリテスト	自動	自動、無効、有効	B200 M6	
Intel Dynamic Speed Select	ディセーブル	Enabled、Disabled	B200 M6	
[インテル Speed Select（Intel Speed Select）]	基本	ベース、構成 1、構成 2、構成 3、構成 4	B200 M6	
UPI Link Frequency Select	自動	9.6GT/s、10.4GT/s、11.2GT/s、自動、リンクごとの設定を使用	B200 M6	
[UMA クラスタリング（UMA Clustering）]	Hemisphere(2-clusters)	Hemisphere(2-clusters), Disable(All-2-All)	B200 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
eADRサポート	無効	自動、有効、無効	B200 M6	
揮発性メモリモード	2LM	2LM、1LM	B200 M6	
メモリ帯域幅ブースト	イネーブル	Enabled、Disabled	B200 M6	
CR FastGo設定	自動	自動、デフォルト、オプション 1、オプション 2、オプション 3、オプション 4、オプション 5、最適化を有効にする、最適化を無効にする	B200 M6	
メモリのリフレッシュレート	2x更新	1x リフレッシュ、2x リフレッシュ	B200 M6	
[コンソールのリダイレクト（Console Redirection）]	ディセーブル	無効、COM0、COM1 または serial-port-b	B200 M6	
端末タイプ	VT100	PC-ANSI、VT100、VT100-PLUS、VT-UTF8	B200 M6	
[TPM サポート（TPM Support）]	イネーブル	Enabled、Disabled	B200 M6	
[TPM 保留中の操作（TPM Pending operation）]	なし	なし、TpmClear	B200 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
SHA-1 PCRバンク	イネーブル	Enabled、Disabled	B200 M6	
SHA256 PCR バンク	イネーブル	Enabled、Disabled	B200 M6	
Flow Control	なし	None、RTS-CTS	B200 M6	
[ボー レート（Baud rate）]	115.2k	9.6k、19.2k、38.4k、57.6k、115.2k	B200 M6	
[OS ウォッチドッグ タイマー（OS Boot Watchdog Timer）]	イネーブル	Enabled、Disabled	B200 M6	
OS Boot Watchdog Timer Timeout	10 分	5 minutes、10 minutes、15 minutes、20 minutes	B200 M6	
OS Boot Watchdog Timer Policy	Power Off	Power Off、Reset	B200 M6	
Intel VT for directed IO	イネーブル	Enabled、Disabled	B200 M6	
Intel VTD coherency support	ディセーブル	Enabled、Disabled	B200 M6	
Intel Trusted Execution Technology サポート（Intel Trusted Execution Technology Support）	ディセーブル	Enabled、Disabled	B200 M6	

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係
インテル バーチャライゼーション テクノロジー	イネーブル	Enabled、Disabled	B200 M6	
Legacy USB Support	イネーブル	有効、無効、自動	B200 M6	

4.2(1d) の M5 サーバーの新規および変更された BIOS トークン

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係	新規/変更
MRAID Link Speed	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C220 M5 と C240 M5		変更済み
[RAID]*n* [リンク速度（Link Speed）]	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C480 M5		変更済み
[PCIe スロット MRAID（PCIe Slot MRAID）*n* OptionROM]	イネーブル	Enabled、Disabled	C220 M5 と C240 M5		変更済み
[フロント NVMe（Front NVME）] *n* [リンク速度（Link Speed）]	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C220 M5 と C240 M5		変更済み

名前	デフォルト値	サーバーでサポートされている値	プラットフォーム	依存関係	新規/変更
[PCIe スロット（PCIe Slot）：*n* リンク速度（Link Speed）]	自動（Auto）	自動、無効、GEN1、GEN2、GEN3、GEN4	C220 M5、C240 M5、C480 M5、および C125 M5		変更済み
[背面 NVMe（Rear NVME）] *n* [リンク速度（Link Speed）]	自動	自動、無効、有効、GEN1、GEN2、GEN3、GEN4	C240 M5		変更済み
[メモリ RAS 構成の選択（Select Memory RAS Configuration）]	ADDDC のスペアリング	Maximum performance、Mirror mode 1lm、ADDDC Sparing、Patrol mirror mode 1lm	C240 M5		変更済み
[ターボモード（Turbo Mode）]	イネーブル	Enabled、Disabled	C240 M5		変更済み
EIST PSD関数（EIST PSD Function）	HW all	HWすべて、SWすべて	C240 M5		変更済み
非コア周波数スケーリング	イネーブル	Enabled、Disabled	C240 M5		変更済み
SpeedStep(Pstates)	イネーブル	Enabled、Disabled	C240 M5		変更済み

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。