



Hewlett Packard
Enterprise

HPE ProLiant m510 および m710x サーバーカートリッジ用 UEFI 設定 クイックリファレンスガイド

摘要

このガイドでは、UEFI (Unified Extensible Firmware Interface) ベースのすべての HPE ProLiant m510 および m710x サーバーカートリッジのシステム ROM に組み込まれている、UEFI で使用可能なシステムユーティリティの構成オプションを一覧にして記載します。このガイドは、サーバーおよびストレージシステムのインストール、管理、トラブルシューティングの担当者を対象とし、コンピューター機器の保守の資格があり、高電圧製品の危険性について理解していることを前提としています。

部品番号: 868916-191
2016 年 7 月
第 1 版

© Copyright 2016 Hewlett Packard Enterprise Development LP

本書の内容は、将来予告なしに変更されることがあります。Hewlett Packard Enterprise 製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、脱落に対して、責任を負いかねますのでご了承ください。

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、その保有、使用、または複製には、Hewlett Packard Enterprise から使用許諾を得る必要があります。FAR 12.211 および 12.212 に従って、商業用コンピューターソフトウェア、コンピューターソフトウェアドキュメンテーション、および商業用製品の技術データ (Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items) は、ベンダー標準の商業用使用許諾のもとで、米国政府に使用許諾が付与されます。

商標

Linux® は、Linus Torvalds 氏の米国における登録商標です。

Intel®、インテル、Itanium®、Pentium®、Intel Inside®、および Intel Inside ロゴは、インテルコーポレーションまたはその子会社のアメリカ合衆国およびその他の国における商標または登録商標です。

Microsoft® および Windows® は、米国および/またはその他の国における Microsoft Corporation の登録商標または商標です。



® は UEFI Forum, Inc. の登録商標です。

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に掲載されている製品情報には、日本国内で販売されていないものも含まれている場合があります。

UEFI システムユーティリティのオプションと設定

次の表に、UEFI システムユーティリティで使用可能な各オプションをアルファベット順に記載します。また、システムユーティリティのメイン画面からオプションへのメニューパス、オプションの使用方法についての簡潔な説明、および使用可能な設定（該当する場合）についても記載します。

- ① **重要:** UEFI システム構成オプションは、ご使用のシステムにインストールされているプラットフォームおよび独自のコンポーネントによって異なります。したがって、ここに記載されているオプションの中には、ご使用のシステムでは表示されないものがある可能性があります。各オプションについて詳しくは、『HPE ProLiant m510 および m710x サーバーカートリッジ用 UEFI システムユーティリティユーザーガイド』を参照してください。

オプション	システムユーティリティのメニューパス	使用方法	設定
iSCSI ブート試行を追加	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Network Options]→[iSCSI Boot Configuration]→[Add an iSCSI Boot Attempt]	iSCSI ブートターゲットを構成します。	N/A
ブートオプションの追加	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Boot Options]→[Advanced UEFI Boot Maintenance]→[Add Boot Option]	UEFI ブート順序リストに x64 UEFI アプリケーションを追加します。	N/A
内蔵 UEFI シェルをブート順序に追加	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Embedded UEFI Shell]→[Add Embedded UEFI Shell to Boot Order]	次の再起動時に、内蔵 UEFI シェルを UEFI ブート順序リストのエントリーとして追加します。	<ul style="list-style-type: none"> 有効 無効
隣接セクターのプリフェッチャー	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Performance Options]→[Advanced Performance Tuning Options]→[Adjacent Sector Prefetcher]	隣接セクターのプリフェッチ機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
管理者情報	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Asset Information]→[Administrator Information]	サーバー管理者の連絡先情報を指定します。	N/A
ASR ステータス	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Availability]→[ASR Status]	自動サーバー復旧 (ASR) を有効または無効にします。ASR は、サーバーがロックアップした場合にサーバーを自動的に再起動します。	<ul style="list-style-type: none"> 有効 無効
ASR タイムアウト	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Availability]→[ASR Timeout]	ASR ステータスが有効になっている場合は、オペレーティングシステムのクラッシュ時またはサーバーのロックアップ時にサーバーを再起動するまでの待ち時間を設定します。	<ul style="list-style-type: none"> 5 分 10 分 15 分 20 分 30 分
自動電源オン	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Availability]→[Automatic Power-On]	AC 電源がシステムに接続されたときにサーバーの電源を自動的に	<ul style="list-style-type: none"> 常に電源をオン 常に電源をオフ

オプション	システムユーティリティのメニューパス	使用方法	設定
		オンにする方法を構成します。	<ul style="list-style-type: none"> 最後の電源状態を復元
ブート順序ポリシー	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Boot Options]→[Boot Order Policy]	UEFI ブート順序リストに従ってデバイスのブートを試みたときにブート可能なデバイスが見つからない場合に、システムの動作を制御します。	<ul style="list-style-type: none"> ブート順序を無限に再試行 ブート順序を 1 回試行 ブート試行の失敗後リセット
チャンネルインターリーブ	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Advanced Power Options]→[Channel Interleaving]	電力プロファイル [Custom] に設定している場合、高レベルのメモリインターリーブを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
協調電力制御	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Advanced Power Options]→[Collaborative Power Control]	電力プロファイルが [Custom] に設定されている場合、プロセッサクロッキングコントロール (PCC) インターフェイスをサポートしているオペレーティングシステムに対する協調電力制御を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
一貫性のあるデバイスの名前付け	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Advanced Options]→[Advanced System ROM Options]→[Consistent Device Naming]	デバイスの名前付けのレベルを指定します。これにより、システム内の NIC ポートの位置に基づく NIC ポートの名前付けを制御します。	<ul style="list-style-type: none"> LOM のみの一貫性のあるデバイスの名前付け 無効
カスタム POST メッセージ	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Asset Information]→[Custom POST Message]	サーバーの POST 処理中に ProLiant POST 画面に表示するカスタムメッセージを指定します。	N/A
日付と時刻	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Date and Time]	システムによって表示される日時を指定します。	N/A
DCU IP プリフェッチャー	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Performance Options]→[Advanced Performance Tuning Options]→[DCU IP Prefetcher]	DCU IP のプリフェッチ機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
DCU ストリームプリフェッチャー	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Performance Options]→[Advanced Performance Tuning Options]→[DCU Stream Prefetcher]	DCU ストリームのプリフェッチ機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
デフォルトの UEFI デバイス優先順位	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Default Options]→[Default UEFI Device Priority]	デフォルトのシステム設定が復元されるときに使用される UEFI デバイスの優先順位を変更します。	N/A

オプション	システムユーティリティのメニューパス	使用方法	設定
すべてのキーを削除 (PK、KEK、DB、DBX)	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Delete all keys (PK, KEK, DB, DBX)]	プラットフォームキーを含む、システム内のすべてのキーを削除します。	N/A
ブートオプションの削除	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Boot Options]→[Advanced UEFI Boot Maintenance]→[Delete Boot Option]	UEFI ブート順序リストから x64 UEFI アプリケーションを削除します。	N/A
iSCSI ブート試行を削除	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Network Options]→[iSCSI Boot Configuration]→[Delete iSCSI Boot Attempts]	1つ以上の iSCSI ブートターゲットを削除します。	N/A
KEK エントリーを削除	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Platform Key (PK) Options]→[Delete KEK Entry]	キー交換キーを削除します。	N/A
プラットフォームキー (PK) を削除	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Platform Key (PK) Options]→[Delete Platform Key (PK)]	プラットフォームキーの証明書を削除します。	N/A
署名を削除 (許可済み DB)	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Allowed Signatures Database (DB) Options]→[Delete Signature]	許可済み署名データベースから署名を削除します。	N/A
署名を削除 (禁止された DB)	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Forbidden Signatures Database (DBX) Options]→[Delete Signature]	禁止された署名データベースから署名を削除します。	N/A
動的消費電力上限機能	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[Boot Time Optimizations]→[Dynamic Power Capping Functionality]	ブートプロセス中にシステム ROM がいつ電力較正を実行するかを構成します。	<ul style="list-style-type: none"> 自動 有効 無効
ダイナミックパワーセービングモードレスポンス	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Advanced Power Options]→[Dynamic Power Savings Mode Response]	電力プロファイルが [Custom] に設定されている場合、プロセッサのワークロードに合わせてプロセッサのパフォーマンスと電源の状態をシステム ROM で制御できます。	<ul style="list-style-type: none"> 高速 低速
内蔵 SATA 構成	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[SATA Controller Options]→[Embedded SATA Configuration]	内蔵チップセット SATA (Serial Advanced Technology Attachmen) コント	<ul style="list-style-type: none"> SATA AHCI サポートを有効

オプション	システムユーティリティのメニューパス	使用方法	設定
		ローラーサポートを有効にします。	
Embedded UEFI Shell (有効化/無効化)	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Embedded UEFI Shell]→[Embedded UEFI Shell]	内蔵 UEFI シェルを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
Embedded UEFI Shell (起動)	[Embedded Applications]→[Embedded UEFI Shell]	内蔵 UEFI シェルを起動します。	N/A
内蔵ビデオ接続	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Advanced Options]→[Embedded Video Connection]	内蔵ビデオコントローラに外部ビデオ接続を構成します。	<ul style="list-style-type: none"> 自動 常に無効 常に有効
EMS コンソール	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[BIOS Serial Console and EMS]→[EMS Console]	Windows Server 緊急管理サービス (EMS) コンソールにリダイレクトするシリアルポート設定を構成します。	<ul style="list-style-type: none"> 無効 COM1 COM2
エネルギーパフォーマンスバイアス	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Advanced Power Options]→[Energy/Performance Bias]	電力プロファイルを [Custom] に設定している場合、複数のプロセッササブシステムを構成して、プロセッサのパフォーマンスと電力使用を最適化します。	<ul style="list-style-type: none"> 最大パフォーマンス パフォーマンスの最適化 電力の最適化 省電力モード
KEK エントリーを登録	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Key Exchange Key (KEK) Options]→[Enroll KEK Entry]	キー交換キーの証明書を登録します。	N/A
PK を登録	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Platform Key (PK) Options]→[Enroll PK]	プラットフォームキーの証明書を登録します。	N/A
署名を登録 (許可済み DB)	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Allowed Signatures Database (DB) Options]→[Enroll Signature]	許可済み署名データベースに署名を登録します。	N/A
署名を登録 (禁止された DB)	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Forbidden Signatures Database (DBX) Options]→[Enroll Signature]	禁止された署名データベースに署名を登録します。	N/A
システムを終了して再起動	システムユーティリティのメイン画面	システムユーティリティを終了して、ブートプロセスを再開します。	N/A
拡張メモリテスト	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System	メモリの初期化プロセス時にシステムが拡張メモリテストを実行す	<ul style="list-style-type: none"> 有効 無効

オプション	システムユーティリティのメニューパス	使用方法	設定
	Options] → [Boot Time Optimizations] → [Extended Memory Test]	るかどうかを有効または無効にします。	
HW プリフェッチャー	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [Performance Options] → [Advanced Performance Tuning Options] → [HW Prefetcher]	インテルプロセッサを搭載するサーバーでのプロセッサプリフェッチ機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
インテル NIC DMA チャンネル (IOAT)	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [Performance Options] → [Advanced Performance Tuning Options] → [Intel NIC DMA Channels (IOAT)]	インテル NIC 上での DMA アクセラレーションを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
インテル (R) ハイパースレッディングオプション	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [System Options] → [Processor Options] → [Intel (R) Hyperthreading Options]	インテルハイパースレッディングテクノロジーをサポートするプロセッサ上の論理プロセッサコアを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
Intel (R) TXT Support	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [Server Security] → [Intel (R) TXT Support]	インテルプロセッサを搭載するサーバーでの Intel TXT (Trusted Execution Technology) のサポートを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
Intel (R) VT-d	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [System Options] → [Virtualization Options] → [Intel (R) VT-d]	Virtual Machine Manager (VMM) でダイレクト I/O (VT-d) 対応のインテル仮想化テクノロジーを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
I/O 非ポストプリフェッチ	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [Performance Options] → [Advanced Performance Tuning Options] → [I/O Non-posted Prefetching]	I/O 非ポストプリフェッチ機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
IPv6 DHCP ユニーク識別子	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [Network Options] → [Network Boot Options] → [IPv6 DHCP Unique Identifier]	IPv6 DHCP ユニーク識別子 (DUID) の設定方法を制御します。	<ul style="list-style-type: none"> 自動 DUID-LLT
iSCSI 試行	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [Network Options] → [iSCSI Boot Configuration] → [iSCSI Attempts]	iSCSI ブート試行の詳細を表示します。	N/A
最大メモリバス周波数	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [Power Management] → [Advanced Power Options] → [Maximum Memory Bus Frequency]	電力プロファイルが [Custom] に設定されている場合、取り付けられているプロセッサ/DIMM の構成でサポートされているよりも低い最高速度でメモリが動作するように構成できます。	<ul style="list-style-type: none"> 自動 1333M Hz 1066M Hz 800M Hz
最大 PCI Express 速度	[System Configuration] → [BIOS/Platform Configuration (RBSU)] → [Power Management] → [Advanced Power Options] → [Maximum PCI Express Speed]	電力プロファイルが [Custom] に設定されている場合、PCI Express デバイスがサーバーで稼働できる	<ul style="list-style-type: none"> 最大サポート PCIe Generation 1.0

オプション	システムユーティリティのメニューパス	使用方法	設定
		最大 PCI Express 速度を下げます。	
メモリの高速トレーニング	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[Boot Time Optimizations]→[Memory Fast Training]	サーバーの再起動時のメモリートレーニングを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
I/O のメモリ近接関係レポート	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Performance Options]→[Advanced Performance Tuning Options]→[Memory Proximity Reporting for I/O]	I/O デバイスと、オペレーティングシステムのシステムメモリとの間の近接関係をシステム ROM がレポートするかどうかを設定します。	<ul style="list-style-type: none"> 有効 無効
最小プロセッサアイドル電力コア C ステート	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Minimum Processor Idle Power Core C-State]	電源プロファイルが [Custom] に設定されている場合、オペレーティングシステムが使用する、プロセッサの最小アイドル電力 (C ステート) を設定します。	<ul style="list-style-type: none"> C6 ステート C3 ステート C1E ステート C ステートなし
最小プロセッサアイドル電力パッケージ C ステート	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Minimum Processor Idle Power Package C-State]	電力プロファイルを [Custom] に設定している場合、最小のプロセッサアイドル電力ステート (C ステート) を設定します。	<ul style="list-style-type: none"> パッケージ C6 (リテンション) ステート パッケージ C6 (リテンションなし) ステート パッケージステートなし C ステートなし
Network Boot Options (特定の NIC 用)	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Network Options]→[Network Boot Options]	取り付けられた NIC のネットワークブートを有効または無効にします。	<ul style="list-style-type: none"> ネットワークブート 無効
ネットワークブートリトライサポート	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Network Options]→[Network Boot Options]→[Network Boot Retry Support]	ネットワークブートリトライ機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
シェルの自動開始スクリプトのネットワーク上の位置	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Embedded UEFI Shell]→[Network Location for Shell Script-Auto Start]	UEFI シェル起動スクリプトのネットワークの URL の場所を設定します。	N/A
NMI デバッグボタン	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Advanced Options]→[Advanced System ROM Options]→[NMI Debug Button]	システムでソフトウェアのロックアップが発生したときのデバッグ機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
No-Execute メモリ保護	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[Server Security]→[No-Execute Protection]	悪意のあるコードやウイルスに対する保護を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
ワнтаイムブートメニュー	システムユーティリティのメイン画面	ワнтаイムブートのオーバーライドに対する UEFI ブートオプションを選択します。	構成に応じて異なる

オプション	システムユーティリティのメニューパス	使用方法	設定
ワンタイムブートメニュー（F11プロンプト）	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[One-Time Boot Menu (F11 Prompt)]	現在のブート時に、F11 キーを押してワンタイムブートメニューに直接ブートできるかどうかを制御します。	<ul style="list-style-type: none"> 有効 無効
PCIバスパディングオプション	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Advanced Options]→[Advanced System ROM Options]→[PCI Bus Padding Options]	デフォルトのPCIバスパディングを有効または無効にします。これは、各拡張スロットに追加のPCIバス番号を付与する機能です。	<ul style="list-style-type: none"> 有効 無効
PCI デバイスの有効/無効	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[PCI Device Enabled/Disable]	内蔵PCIデバイスとアドインPCIデバイスを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
PCIe スロットネットワークブート	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Network Options]→[Network Boot Options]→[PCIe Slot Network Boot]	PCIe スロット内のNIC カードのUEFI PXE ブートを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
POST F1 プロンプト	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Availability]→[POST F1 Prompt]	サーバーのPOST 画面でのF1 キーの表示方法を構成します。	<ul style="list-style-type: none"> 20 秒の遅延 2 秒の遅延 無効
電源ボタンモード	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Availability]→[Power Button Mode]	電源ボタンを一瞬押す機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
電源投入遅延	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Availability]→[Power-On Delay]	指定した時間にサーバーの電源をオンにすることを遅らせるかどうかを設定します。	<ul style="list-style-type: none"> 遅延なし ランダムに遅延 15 秒遅延 30 秒遅延 45 秒遅延 60 秒遅延
電源プロファイル	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Power Profile]	電力とパフォーマンスの特性に基づいて電力プロファイルを選択します。	<ul style="list-style-type: none"> 電力およびパフォーマンスの最適化 最小消費電力 最大パフォーマンス カスタム
パワーレギュレーター	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Power Regulator]	電力プロファイルを[Custom] に設定している場合、パワーレギュレーターモードを設定します。	<ul style="list-style-type: none"> ダイナミックパワーセービングモード スタティックローパワーモード スタティックハイパフォーマンスモード OSコントロールモード
プリブートネットワーク設定	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Network Options]→[Pre-boot Network Settings]	起動前のネットワークインターフェイスおよび関連設定を構成します。	<p>起動前のネットワークインターフェイス</p> <ul style="list-style-type: none"> 自動 内蔵 NIC

オプション	システムユーティリティのメニューパス	使用方法	設定
			DHCPv4 <ul style="list-style-type: none"> 有効 無効 URL からのブート
プロセッサ AES-NI 有効	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Processor AES-NI Support]	プロセッサ内の Advanced Encryption Standard Instruction Set を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
プロセッサコア無効	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[Processor Options]→[Processor Core Disable]	各プロセッサソケットで有効にするコアの数を指定します。	N/A
プロセッサ x2APIC サポート	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[Processor Options]→[Processor x2APIC Support]	x2APIC サポートを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
製品 ID	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Advanced Options]→[Advanced System ROM Options]→[Product ID]	システムボードを交換した後の製品 ID 番号を指定します。	N/A
QPI バンド幅の最適化 (RTID)	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Performance Options]→[Advanced Performance Tuning Options]→[QPI Bandwidth Optimization (RTID)]	最適なパフォーマンスを得るために 2 つのプロセッサ間の QPI リンクを構成します。	<ul style="list-style-type: none"> パフォーマンスの最適化 I/O の最適化 (代替 RTID)
システムを再起動する	システムユーティリティのメイン画面	システムを再起動します。	N/A
冗長化電源装置モード	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Power Management]→[Advanced Power Options]→[Redundant Power Supply Mode]	電力プロファイルを [Custom] に設定している場合、システムが冗長電源装置の構成をどのように取り扱うかを設定します。	<ul style="list-style-type: none"> バランスモード 高効率モード (自動) 高効率モード (奇数サプライがスタンバイ) 高効率モード (偶数サプライがスタンバイ)
すべてのキーをプラットフォームのデフォルトにリセット	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Advanced Secure Boot Options]→[Reset all keys to platform defaults]	すべてのキーをプラットフォームのデフォルトにリセットします。	N/A
工場デフォルト設定の復元	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Default Options]→[Restore Default Manufacturing Settings]	すべての BIOS 構成設定を工場デフォルト値にリセットして、不揮発性のすべての UEFI 変数を削除します。	<ul style="list-style-type: none"> いいえ、復元の操作を中止します。 はい、デフォルト設定を復元します。
システムデフォルト設定の復元	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Default Options]→[Restore Default System Settings]	すべての BIOS 構成設定をデフォルト値にリセットし、直ちに、か	<ul style="list-style-type: none"> いいえ、復元の操作を中止します。 はい、デフォルト設定を復元します。

オプション	システムユーティリティのメニューパス	使用方法	設定
		つ自動的にサーバーを再起動します。	
SATA セキュア消去	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[SATA Controller Options]→[SATA Secure Erase]	SATA セキュア消去機能を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
セキュアブート強制	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Secure Boot Settings]→[Secure Boot Enforcement]	セキュアブートを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
シリアル番号	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Advanced Options]→[Advanced System ROM Options]→[Serial Number]	システムボードのシリアル番号を表示します。	N/A
サービスコンタクト情報	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Asset Information]→[Administrator Information]	サーバー管理者のサービス連絡先情報を指定します。	N/A
管理者パスワードの設定	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Set Admin Password]	管理者パスワードを設定します。	N/A
電源投入時パスワードの設定	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Set Power On Password]	ブートプロセス中にサーバーにアクセスするためのパスワードを設定します。	N/A
サーバー情報	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Asset Information]→[Server Information]	サーバー管理者に関する参照情報を指定します。	N/A
言語の選択	システムユーティリティのメイン画面	システムで使用される言語を選択します。	N/A
シェル自動起動スクリプトロケーション	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Embedded UEFI Shell]→[Shell Auto-Start Script Location]	内蔵 UEFI シェル起動スクリプトの場所を指定します。	<ul style="list-style-type: none"> 自動 接続メディアのファイルシステム ネットワークの場所
システム情報	システムユーティリティのメイン画面	システム情報を表示します。	N/A
TPM 2.0 Operation	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Trusted Platform Module options]→[TPM 2.0 Operation]	Trusted Platform Module (TPM) を搭載したサーバーで、TPM 2.0 の操作状態を設定します。	<ul style="list-style-type: none"> 操作なし 有効 無効
TPM 2.0 Visibility	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Trusted Platform Module options]→[TPM 2.0 Visibility]	TPM を搭載したサーバーで、TPM がオペレーティングシステムから隠されているかどうかを設定します。	<ul style="list-style-type: none"> 表示 非表示
TPM Binding	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Trusted Platform Module options]→[TPM Binding]	TPM を搭載したサーバーで、TPM バインドキー（一意の RSA キー）を使用してデー	<ul style="list-style-type: none"> 有効 無効

オプション	システムユーティリティのメニューパス	使用方法	設定
		タを暗号化するかどうかを設定します。	
TPM UEFI Option ROM Measurement	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Security]→[Trusted Platform Module options]→[TPM UEFI Option ROM Measurement]	TPM を搭載したサーバーで、UEFI PCI 操作 ROM の測定を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
UEFI ブート順序	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Boot Options]→[UEFI Boot Order]	UEFI ブート順序リスト内のエントリーのブート順序を変更します。	構成に応じて異なる
UEFI 最適化ブート	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Boot Options]→[UEFI Optimized Boot]	システム BIOS をネイティブの UEFI グラフィックドライバを使用して起動するかどうかを制御します。	<ul style="list-style-type: none"> 有効 無効
UEFI PXE ブートポリシー	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Network Options]→[Network Boot Options]→[UEFI PXE Boot Policy]	UEFI ブート順序リスト内のネットワークブートターゲットの順序を設定します。	<ul style="list-style-type: none"> IPv4 次に IPv6 IPv4 IPv6 IPv6 次に IPv4 自動
UEFI シェルスク립ト自動起動	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Embedded UEFI Shell]→[UEFI Shell Script Auto-Start]	シェル起動中の内蔵 UEFI シェル起動スク립トの自動実行を有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
ユーザーデフォルトオプション	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Default Options]→[User Default Options]	構成をカスタムデフォルト構成として保存または消去します。	<ul style="list-style-type: none"> ユーザーデフォルトの保存 ユーザーデフォルトの消去
ビデオオプション	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Advanced Options]→[Video Options]	ビデオの表示を構成します。	<ul style="list-style-type: none"> アドインビデオ有効、内蔵ビデオ無効 アドインビデオと内蔵ビデオの両方が有効
View System Health	[System Health]→[View System Health]	システム内のすべてのデバイスのヘルステータスを表示します。	N/A
仮想化テクノロジー	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[Virtualization Options]→[Virtualization Technology]	Virtual Machine Manager (VMM) でインテル仮想化テクノロジーを有効または無効にします。	<ul style="list-style-type: none"> 有効 無効
Virtual Serial Port	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[System Options]→[Serial Port Options]→[Virtual Serial Port]	仮想シリアルポートで使用する論理 COM ポートと関連デフォルト	<ul style="list-style-type: none"> COM 1: IRQ4: I/O: 3F8h-3FFh COM 2: IRQ3: I/O: 2F8h-2FFh

オプション	システムユーティリティのメニューパス	使用方法	設定
		トリソースを割り当てます。	<ul style="list-style-type: none"> 無効
VLAN の構成	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Network Options]→[VLAN Configuration]	有効なすべてのネットワークインターフェイスにグローバルな VLAN 構成を設定します。	VLAN 制御 <ul style="list-style-type: none"> 有効 (VLAN ID および優先順位の設定) 無効
ウェイクオン LAN	[System Configuration]→[BIOS/Platform Configuration (RBSU)]→[Server Availability]→[Wake-On LAN]	WOL 対応 NIC を使用してリモートでシステムに電源を投入できるかどうかを設定します。	<ul style="list-style-type: none"> 有効 無効