

Dell EMC PowerEdge R440

BIOS および UEFI リファレンス ガイド

メモ、注意、警告

 **メモ:** 製品を使いやすくするための重要な情報を説明しています。

 **注意:** ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。

 **警告:** 物的損害、けが、または死亡の原因となる可能性があることを示しています。

章 1: プレオペレーティング システム管理アプリケーション	4
プレオペレーティング システム アプリケーションを管理するためのオプション.....	4
システム セットアップ.....	4
セットアップユーティリティの表示.....	4
セットアップユーティリティ詳細.....	5
システム BIOS.....	5
iDRAC 設定ユーティリティー.....	26
デバイス設定.....	26
Dell Lifecycle Controller.....	27
組み込み型システム管理.....	27
ブートマネージャー.....	27
ブートマネージャの表示.....	27
ブートマネージャーのメインメニュー.....	27
ワンショット UEFI 起動メニュー.....	28
システムユーティリティ.....	28
PXE 起動.....	28

プレオペレーティング システム管理アプリケーション

システムのファームウェアを使用して、オペレーティング システムを起動せずにシステムの基本的な設定や機能を管理することができます。

トピック：

- [プレオペレーティング システム アプリケーションを管理するためのオプション](#)
- [システム セットアップ](#)
- [Dell Lifecycle Controller](#)
- [ブートマネージャー](#)
- [PXE 起動](#)

プレオペレーティング システム アプリケーションを管理するためのオプション

お使いのシステムには、プレオペレーティング システム アプリケーションを管理するための次のオプションがあります。

- システム セットアップ
- Dell Lifecycle Controller
- ブートマネージャー
- PXE (Preboot Execution Environment)

システム セットアップ

システム セットアップ画面を使用して、お使いのシステムの BIOS 設定、iDRAC 設定、デバイス設定を構成できます。

メモ: デフォルトでは、選択したフィールドのヘルプ テキストはグラフィカル ブラウザー内に表示されます。テキスト ブラウザー内でヘルプ テキストを表示するには、F1 を押してください。

次のいずれかで、セットアップユーティリティにアクセスできます

- 標準グラフィカルブラウザ — このブラウザはデフォルトで有効になっています。
- テキストブラウザ — コンソールリダイレクトの使用によって有効になります。

セットアップユーティリティの表示

System Setup (セットアップユーティリティ) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティング システムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

セットアップユーティリティ詳細

System Setup Main Menu (セットアップユーティリティメインメニュー) 画面の詳細は次のとおりです。

オプション	説明
システム BIOS	BIOS を設定できます。
iDRAC 設定	iDRAC を設定できます。 iDRAC 設定ユーティリティは、UEFI (Unified Extensible Firmware Interface) を使用することで iDRAC パラメーターをセットアップして設定するためのインタフェースです。iDRAC 設定ユーティリティを使用することで、さまざまな iDRAC パラメーターを有効または無効にすることができます。このユーティリティの詳細については、 www.dell.com/poweredge manuals で『Integrated Dell Remote Access Controller ユーザーズガイド』を参照してください。
デバイス設定	デバイスを設定できます。
サービス タグ設定	サービス タグを設定できます。

システム BIOS

システム BIOS 画面を使って、起動順序、システムパスワード、セットアップパスワードなどの特定の機能を編集し、SATA および PCIe NVMe RAID モードを設定し、USB ポートの有効/無効を切り替えることが可能です。

システム BIOS の表示

System BIOS (システム BIOS) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。

システム BIOS 設定の詳細

このタスクについて

System BIOS Settings (システム BIOS 設定) 画面の詳細は次の通りです。

オプション	説明
システム情報	システム モデル名、BIOS バージョン、サービス タグといったシステムに関する情報を指定します。
メモリー設定	取り付けられているメモリーに関連する情報とオプションを指定します。
プロセッサ設定	速度、キャッシュ サイズなど、プロセッサに関連する情報とオプションを指定します。
SATA 設定	内蔵 SATA コントローラとポートの有効/無効を切り替えるオプションを指定します。
NVMe 設定	NVMe 設定を変更するためのオプションを指定します。システムが RAID アレイ内に設定するには、NVMe ドライブが含まれている場合、する必要があります設定の両方にこのフィールドおよび 内蔵 SATA フィールドで、 SATA 設定 メニューを RAID モードにします。することがありますも必要に変更するには、 起動モード を設定するには、 UEFI を押します。それ以外の場合は、必要に設定します。このフィールドを RAID 非対応 モードにします。

オプション	説明
起動設定	起動モード (BIOS または UEFI) を指定するオプションが表示されます。UEFI と BIOS の起動設定を変更することができます。
ネットワーク設定	UEFI ネットワーク設定および起動プロトコルを管理するオプションを指定します。 レガシーネットワークの設定は、管理下から デバイス設定 メニューがあります。
内蔵デバイス	内蔵デバイス コントローラ とポートの管理を行うオプションを提供し、関連する機能とオプションを指定します。
シリアル通信	シリアル ポートおよびそれに関連する機能とオプションを管理するオプションを指定します。
システムプロファイル設定	プロセッサの電源管理設定、メモリー周波数を変更するオプションを指定します。
システムセキュリティ	システムパスワード、セットアップパスワード、TPM (Trusted Platform Module) セキュリティ、UEFI セキュア ブートなどのシステム セキュリティ設定を行うオプションを指定します。システムの電源ボタンを押します。
冗長 OS 制御	冗長 OS 制御用の冗長 OS 情報を設定します。
その他の設定	システムの日時を変更するオプションを指定します。

システム情報

システム情報画面を使用して、サービス タグ、システム モデル名、BIOS バージョンなどのシステムのプロパティを表示できます。

システム情報の表示

System Information (システム情報) 画面を表示するには、次の手順を実行します。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、**システム BIOS** をクリックします。
4. **System BIOS** (システム BIOS) 画面で、**System Information** (システム情報) をクリックします。

システム情報の詳細

このタスクについて

System Information (システム情報画面) の詳細は、次の通りです。

オプション	説明
システムモデル名	システム モデル名を指定します。
システム BIOS バージョン	システムにインストールされている BIOS バージョンを指定します。
システム管理エンジンバージョン	管理エンジンファームウェアの現在のバージョンを指定します。
System Service Tag (システムサービスタグ)	システムのサービス タグを指定します。

オプション	説明
システム製造元	システム メーカーの名前を指定します。
システム製造元の 連絡先情報	システム メーカーの連絡先情報を指定します。
システム CPLD バ ージョン	システム コンプレックス プログラマブル ロジック デバイス (CPLD) ファームウェアの現在のバージョンを 指定します。
UEFI 準拠バージョ ン	システム ファームウェアの UEFI 準拠レベルを指定します。

メモリー設定

メモリー設定画面を使用して、メモリーの設定をすべて表示し、システムのメモリーのテストやノードのインターリーピングなど、特定のメモリー機能を有効または無効にできます。

メモリー設定の表示

Memory Settings (メモリー設定) 画面を表示するには、次の手順を実行します。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。
4. System BIOS (システム BIOS) 画面で、Memory Settings (メモリー設定) をクリックします。

メモリー設定の詳細


このタスクについて

メモリー設定画面の詳細は、次のとおりです。

オプション	説明
システムメモリー のサイズ	システム内のメモリー サイズを指定します。
システムメモリー のタイプ	システムに取り付けられているメモリーのタイプを指定します。
システムメモリー スピード	システムメモリーのスピードを指定します。
システムメモリー 電圧	システムメモリーの電圧を指定します。
ビデオメモリー	ビデオメモリーの容量を指定します。
システムメモリー テスト	システム起動時にシステムメモリーテストを実行するかどうかを指定します。オプションは 有効 および 無効 です。このオプションは、デフォルトで 無効 に設定されています。
DRAM リフレッシュ の延期	CPU メモリー コントローラーを有効にしてリフレッシュコマンドの実行を延期することにより、一部のワークロードのパフォーマンスを向上させることができます。延期時間を最小限に抑えることで、メモリーコントローラーは一定間隔でリフレッシュコマンドを実行することが保証されます。インテルベースのサーバーの場合、この設定は、8 Gb 密度 DRAM を使用する DIMM で構成されたシステムにのみ影響します。

オプション 説明

メモリー動作モード メモリーの動作モードを指定します。使用可能なオプションは、**最適化モード**、**シングル ランク スペア モード**、**マルチ ランク スペア モード**、および**ミラー モード**です。デフォルトでは、このオプションは**最適化モード**に設定されています。

 **メモ:** メモリー動作モードオプションには、システムメモリー構成に応じて異なるデフォルトおよび使用可能オプションがあります。

メモリー動作モードの現在の状態 メモリーの動作モードの現在の状態を示します。

ノードインターリーブ 不均一メモリーアーキテクチャ (NUMA) をサポートするかどうかを指定します。このフィールドが**有効**になっている場合は、対称的なメモリー構成がインストールされている場合にメモリーのインターリーブがサポートされます。このフィールドが**無効**に設定されている場合、システムは NUMA (非対称) メモリー構成をサポートします。このオプションは、デフォルトで**無効**に設定されています。

ADDDC 設定 **ADDDC 設定機能**を有効または無効にします。Adaptive Double DRAM Device Correction (ADDDC) が有効になっている場合、DRAM が失敗すると動的に訂正されます。**有効**に設定すると、特定のワークロードではシステムパフォーマンスに影響が出る可能性があります。この機能は x4 DIMM にのみ適用されます。このオプションは、デフォルトで**有効**に設定されています。

16Gb DIMM のネイティブな tRFC タイミング 16 Gb 密度 DIMM を、プログラムされた行更新サイクル時間 (tRFC) で動作させることができます。この機能を有効にすると、一部の構成でシステムパフォーマンスが向上する場合があります。ただし、この機能を有効にすると、16 Gb 3DS/TSV DIMM の構成には影響しません。このオプションは、デフォルトで**有効**に設定されています。

便宜的セルフリフレッシュ 便宜的セルフリフレッシュ機能を有効または無効にします。このオプションは、デフォルトで**無効**に設定されており、システムに DCPMM が含まれている場合はサポートされません。

修正可能なエラーのログ 修正可能なメモリーしきい値エラーのログを有効または無効にします。このオプションは、デフォルトで**有効**に設定されています。

プロセッサ設定

Processor Setting 画面を使用して、プロセッサ設定を表示し、仮想化テクノロジー、ハードウェアプリフェッチャ、論理プロセッサアイドルリングなどの特定の機能を実行できます。


プロセッサ設定の表示

Processor Settings 画面を表示するには、次の手順を実行します。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

 **メモ:** F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。



3. システムセットアップメインメニュー画面で、**システム BIOS** をクリックします。
4. **System BIOS** 画面で **Processor Settings** をクリックします。

プロセッサ設定の詳細

このタスクについて

Processor Setting (プロセッサ設定) 画面の詳細は、次のとおりです。

オプション	説明
論理プロセッサ	論理プロセッサの有効/無効を切り替えて論理プロセッサの数を表示します。このオプションが 有効 に設定されている場合、BIOSにはすべての論理プロセッサが表示されます。このオプションが 無効 に設定されている場合、BIOSにはコアにつき1つの論理プロセッサのみが表示されます。このオプションは、デフォルトで 有効 に設定されています。
CPU インターコネクト スピード	システム内のプロセッサ間の通信リンクの頻度を制御することができます。  メモ: 標準のと基本的なピンのプロセッサ下部リンク周波数をサポートします。 使用できるオプションは、 最大データレート 、 10.4 GT/s 、および 9.6 GT/s です。このオプションはデフォルトで 最大データレート に設定されています。 最大データ転送速度は、プロセッサがサポートする最大周波数での BIOS による通信リンクの実行を示します。サポートするさまざまな周波数の中から特定の周波数を選択することも可能です。 最適なパフォーマンスを得るには、 最大データレート を選択する必要があります。通信リンクの頻度で任意の削減の非パフォーマンスにローカルのメモリアクセスは、およびキャッシュの一貫性のトラフィックに影響します。加えて、特定のプロセッサからローカル以外の I/O デバイスへのアクセスが遅くなる可能性があります。 ただし、パフォーマンスよりも省電力を優先する場合は、プロセッサの通信リンクの周波数を下げることがあります。これを行う場合、メモリーおよびローカライズする必要があります。I/O 近くの NUMA ノードを、システムパフォーマンスに影響を最小限するためにアクセスします。
仮想化テクノロジー	プロセッサの仮想化テクノロジーを有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。
隣接キャッシュラインのプリフェッチ	シーケンシャルメモリアクセスの頻繁な使用率を必要とするアプリケーション用にシステムを最適化します。このオプションは、デフォルトで 有効 に設定されています。ランダムなメモリアクセスの使用率が高いアプリケーションを使用する場合は、このオプションを 無効 にできます。
ハードウェアプリフェッチャ	ハードウェアプリフェッチャを有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。
ソフトウェアプリフェッチャ	ソフトウェアプリフェッチャの有効/無効を切り替えます。このオプションは、デフォルトで 有効 に設定されています。
DCU ストリーマプリフェッチャ	データキャッシュユニット (DCU) ストリーマプリフェッチャの有効/無効を切り替えます。このオプションは、デフォルトで 有効 に設定されています。
DCU IP プリフェッチャ	データキャッシュユニット (DCU) IP プリフェッチャの有効/無効を切り替えます。このオプションは、デフォルトで 有効 に設定されています。
サブ NUMA クラスタ	サブ NUMA クラスタリング (SNC) は、アドレス範囲に基づいて LLC をばらばらのクラスタに分散する機能で、各クラスタをシステム内のメモリーコントローラーのサブセットにバインドします。これにより、平均レイテンシーを LLC まで改善します。仮想 NUMA クラスタを有効または無効にします。このオプションは、デフォルトで 無効 に設定されています。
UPI プリフェッチ	DDR バス上でメモリーの読み取りを早期に開始できます。Ultra Path Interconnect (UPI) Rx バスは、Integrated Memory Controller (iMC) への予測的なメモリー読み取りを直接行います。このオプションは、デフォルトで 有効 に設定されています。
LLC プリフェッチ	すべてのスレッドでの LLC プリフェッチを有効または無効にします。このオプションは、デフォルトで 無効 に設定されています。
デッドライン LLC 配分	デッドライン LLC 配分を有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。このオプションを有効にしてデッドラインを LLC に格納することや、このオプションを無効にしてデッドラインを LLC に格納しないことができます。
ディレクトリー AtoS	ディレクトリー AtoS を有効または無効にします。AtoS 最適化を有効にすると、リモートの読み取り遅延が低減し、書き込みによる中断なしに読み取りアクセスを繰り返すことができます。このオプションは、デフォルトで 無効 に設定されています。
論理プロセッサのアイドルング	有効にするを改善するには、エネルギー効率を実現するシステム押します。オペレーティングシステムのコアパーキングアルゴリズムを使用して、システムの論理プロセッサの一部を保留し、対応するプロセッサコアを順に低電力アイドル状態に遷移できます。このオプションは、オペレーティングシステムがサポートする場合のみ有効にすることができます。このオプションは、デフォルトで 無効 に設定されています。
設定可能 TDP	TDP レベルを設定できます。使用可能なオプションは Nominal 、 Level 1 、 Level 2 です。このオプションは、デフォルトで Nominal (公称) に設定されています。

オプション	説明
	 メモ: このオプションは、プロセッサの特定の最小在庫管理単位 (SKUs) でのみ利用可能です。
x2APIC モード	x2APIC モードを有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。 従来の xAPIC アーキテクチャと比較すると、xAPIC ではプロセッサのアドレス可能な範囲が拡張され、割り込みデリバリーのパフォーマンスが向上します。x2APIC モードを有効または無効にするには、仮想化テクノロジーを有効にする必要があります。仮想化テクノロジーが無効にされている場合、x2APIC モードは強制的に無効になります。
プロセッサあたりのコア数	プロセッサごとの有効なコアの数を制御します。このオプションは、デフォルトで All (すべて) に設定されています。
プロセッサ コア スピード	プロセッサの最大コア周波数を指定します。
プロセッサのバス速度	プロセッサのバス速度が表示されます。
プロセッサ n	 メモ: プロセッサの数に応じて、最大 2 個のプロセッサがリストされている場合があります。 システムに取り付けられている各プロセッサについて、次の設定が表示されます。

オプション	説明
ファミリー - モデル - ステッピング	インテルによって定義されているとおりにプロセッサのファミリー、モデル、およびステッピングを指定します。
ブランド	ブランド名を指定します。
レベル 2 キャッシュ	L2 キャッシュの合計を指定します。
レベル 3 キャッシュ	L3 キャッシュの合計を指定します。
コア数	プロセッサごとのコア数を指定します。
最大メモリー容量	プロセッサあたりの最大メモリー容量を指定します。
マイクロコード	マイクロコードを指定します。

SATA 設定

SATA 設定画面を使用して、SATA デバイスの設定を表示し、システムで SATA および PCIe NVMe RAID モードを有効にすることができます。


SATA 設定の表示

SATA Settings (SATA 設定) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

 **メモ:** F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。
4. System BIOS (システム BIOS) 画面で、SATA Settings (SATA 設定) をクリックします。

SATA 設定の詳細

このタスクについて

SATA Settings (SATA 設定) 画面の詳細は、次の通りです。

オプション	説明
内蔵 SATA	内蔵 SATA オプションを AHCI Mode 、または RAID Mode のいずれかに設定できます。このオプションは、デフォルトで AHCI Mode (AHCI モード) に設定されています。
セキュリティフリーズロック	POST 中に セキュリティフリーズロック コマンドを内蔵 SATA ドライブに送信できます。このオプションは、AHCI mode にのみ適用されます。このオプションは、デフォルトで 有効 に設定されています。
書き込みキャッシュ	POST 中に内蔵 SATA ドライブの コマンドを有効または無効にします。このオプションは、デフォルトで 無効 に設定されています。
ポート n	選択したデバイスのドライブ タイプを設定できます。 AHCI モード または RAID モード の場合、BIOS サポートは常に有効です。
オプション	説明
モデル	選択されたデバイスのドライブモデルを指定します。
ドライブタイプ	SATA ポートに接続されているドライブのタイプを指定します。
容量	ドライブの合計容量を指定します。光学ドライブなどのリムーバブルメディアデバイスに対しては未定義です。

NVMe 設定

NVMe 設定では、NVMe ドライブを **RAID** モードまたは **RAID 非対応** モードに設定できます。

メモ: これらのドライブを RAID ドライブとして構成するには、**SATA 設定** メニューの NVMe ドライブ オプションと内蔵 SATA オプションを **RAID** モードに設定する必要があります。それ以外の場合は、このフィールドを **RAID 非対応** モードに設定します。

NVMe 設定の表示

NVMe Settings 画面を表示するには、次の手順を実行します。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。
4. System BIOS 画面で、NVMe Settings をクリックします。

NVMe 設定の詳細

このタスクについて

NVMe 設定画面の詳細は、次のとおりです。

オプション	説明
NVMe モード	NVMe モードを設定することができます。このオプションは、デフォルトで RAID なし に設定されています。

起動設定

起動設定画面を使用して、起動モードを **BIOS** または **UEFI** のいずれかに設定することができます。起動順序を指定することも可能です。

- **UEFI** : Unified Extensible Firmware Interface(uefi) は、オペレーティングシステムとプラットフォームファームウェア間に新しいインターフェイス。このインターフェイスは、プラットフォーム関連の情報を含んだデータテーブル群と、オペレーティングシステムとそのローダーが使用できるブートおよびランタイム サービス コールから構成されています。起動モードが **UEFI** に設定されている場合は、次のメリットが得られます。
 - 2TB を超えるドライブパーティションをサポートします。
 - 強化されたセキュリティ (例えば、UEFI セキュア ブート) します。
 - 高速起動時間。
- **メモ**: NVMe ドライブから起動するには、UEFI 起動モードのみを使用する必要があります。
- **BIOS**: では、**BIOS 起動モード** は、レガシー起動モードがあります。後方互換性がサポートされています。

起動設定の表示

Boot Settings (起動設定) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

- **メモ**: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。



3. システム セットアップ メイン メニュー画面で、システム **BIOS** をクリックします。
4. **System BIOS** (システム BIOS) 画面で、**Boot Settings** (起動設定) をクリックします。

起動設定の詳細

このタスクについて

Boot Settings (起動設定) 画面の詳細は、次のとおりです。

オプション	説明
起動モード	<p>システムの起動モードを設定できます。</p> <p>注意: オペレーティングシステム インストール時の起動モードが異なる場合、起動モードを切り替えるとシステムが起動しなくなることがあります。</p> <p>オペレーティングシステムが UEFI をサポートしている場合は、このオプションを UEFI に設定できます。このフィールドを BIOS に設定すると、UEFI 非対応のオペレーティングシステムとの互換性が有効になります。このオプションはデフォルトで UEFI に設定されています。</p> <ul style="list-style-type: none"> ○ メモ: このフィールドを UEFI に設定すると、BIOS Boot Settings (BIOS 起動設定) メニューが無効になります。
ブート シーケンス再試行	<p>ブート シーケンス再試行機能を有効または無効にします。このフィールドが Enabled (有効) に設定されていて、システムが起動に失敗した場合、システムは 30 秒後にブート シーケンスを再試行します。このオプションは、デフォルトで 有効 に設定されています。</p>


Hard-Disk フェールオーバー	ドライブ障害発生時に起動するドライブを指定します。では、デバイスが選択されているハードディスクドライブシーケンスで、 起動オプションを設定 します。このオプションを Disabled (無効) に設定すると、リストの最初のドライブだけが起動を試行されます。このオプションを Enabled (有効) に設定すると、すべてのドライブが、 Hard-Disk Drive Sequence (ハードディスクドライブのシーケンス) で選択された順序で起動を試行されます。このオプションは、 UEFI 起動モード では使用できません。このオプションは、デフォルトで 無効 に設定されています。
汎用 USB 起動	USB 起動オプションを有効または無効にします。このオプションは、デフォルトで 無効 に設定されています。
ハードディスクドライブのプレースホルダー	ハードディスクドライブのプレースホルダーオプションを有効または無効にします。このオプションは、デフォルトで 無効 に設定されています。
BIOS Boot Settings	BIOS 起動オプションを有効または無効にします。  メモ: このオプションは、起動モードが BIOS の場合にのみ有効になります。
UEFI 起動設定	UEFI 起動オプションを有効または無効にします。 起動オプションを含めるには IPv4 PXE および IPv6 PXE を押します。このオプションは、デフォルトで IPv4 に設定されています。  メモ: このオプションは、起動モードが UEFI の場合にのみ有効になります。
UEFI ブート シーケンス	起動デバイスの順序を変更できます。
Boot Options Enable/Disable	起動デバイスの有効/無効を選択できます。


システム起動モードの選択

セットアップユーティリティでは、以下のオペレーティングシステムのいずれかのインストール用起動モードを指定することができます。

- BIOS 起動モードは、BIOS レベルの標準的な起動インターフェースです。
- UEFI 起動モード (デフォルト) は、拡張 64 ビット起動インターフェースです。

UEFI モードで起動するようシステムを設定すると、システム BIOS の設定が置換されます。

1. **System Setup Main Menu (セットアップユーティリティのメインメニュー)** で、**Boot Settings (起動設定)** をクリックし、**Boot Mode (起動モード)** を選択します。
2. UEFI 起動モードを選択し、このモードでシステム起動されるようにします。
 **注意:** オペレーティングシステムインストール時の起動モードが異なる場合、起動モードを切り替えるとシステムが起動しなくなることがあります。
3. 指定した起動モードでシステムを起動した後、そのモードからオペレーティングシステムのインストールに進みます。

 **メモ:** UEFI 起動モードからインストールするオペレーティングシステムは UEFI 対応である必要があります。DOS および 32 ビットのオペレーティングシステムは UEFI 非対応で、BIOS 起動モードからのみインストールできます。

 **メモ:** サポートされているオペレーティングシステムの最新情報については、www.dell.com/ossupport を参照してください。

起動順序の変更

このタスクについて

USB キーまたは光学ドライブから起動する場合は、起動順序を変更する必要がある場合があります。**Boot Mode (起動モード)** で **BIOS** を選択した場合は、以下の手順が異なる可能性があります。

手順

1. **System Setup Main Menu (セットアップユーティリティのメインメニュー)** 画面で、**System BIOS (システム BIOS) > Boot Settings (起動設定) > UEFI/BIOS Boot Settings (UEFI/BIOS 起動設定) > UEFI/BIOS ブート シーケンス** の順にクリックします。

2. 終了時に設定を保存するには、**Exit** (終了) をクリックして、**Yes** (はい) をクリックします。

ネットワーク設定

ネットワーク設定画面を使用して、UEFI PXE、iSCSI、および HTTP の起動設定を変更できます。ネットワーク設定オプションは UEFI モードでのみ使用できます。

メモ: BIOS モードでは、BIOS はネットワーク設定を制御しません。BIOS 起動モードの場合は、ネットワークコントローラーのオプションの起動 ROM でネットワーク設定を処理します。

ネットワーク設定の表示

Network Settings (ネットワーク設定) 画面を表示するには、次の手順を実行します。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システムセットアップメインメニュー画面で、システム BIOS をクリックします。
4. **System BIOS** (システム BIOS) 画面で、**Network Settings** (ネットワーク設定) をクリックします。

ネットワーク設定画面の詳細

Network Settings (ネットワーク設定) 画面の詳細は、次のとおりです。

このタスクについて

オプション	説明				
UEFI PXE 設定	<table><thead><tr><th>オプション</th><th>説明</th></tr></thead><tbody><tr><td>PXE デバイス n (n は 1~4)</td><td>デバイスを有効または無効にします。有効にすると、デバイスの UEFI PXE 起動オプションが作成されます。</td></tr></tbody></table>	オプション	説明	PXE デバイス n (n は 1~4)	デバイスを有効または無効にします。有効にすると、デバイスの UEFI PXE 起動オプションが作成されます。
オプション	説明				
PXE デバイス n (n は 1~4)	デバイスを有効または無効にします。有効にすると、デバイスの UEFI PXE 起動オプションが作成されます。				
UEFI HTTP 設定	<table><thead><tr><th>オプション</th><th>説明</th></tr></thead><tbody><tr><td>HTTP デバイス (n は 1~4)</td><td>デバイスを有効または無効にします。有効にすると、デバイスの UEFI HTTP 起動オプションが作成されます。</td></tr></tbody></table>	オプション	説明	HTTP デバイス (n は 1~4)	デバイスを有効または無効にします。有効にすると、デバイスの UEFI HTTP 起動オプションが作成されます。
オプション	説明				
HTTP デバイス (n は 1~4)	デバイスを有効または無効にします。有効にすると、デバイスの UEFI HTTP 起動オプションが作成されます。				
UEFI iSCSI 設定	iSCSI デバイスの設定を制御できます。				

表 1. UEFI iSCSI 設定画面の詳細

オプション	説明
iSCSI のイニシエーター名	iSCSI イニシエーターの名前を IQN 形式で指定します。
iSCSI デバイス 1	iSCSI デバイスを有効または無効にします。無効の場合は、iSCSI デバイスに UEFI 起動オプションが自動的に作成されます。このオプションは、デフォルトで設定されています。
iSCSI デバイス 1 の設定	iSCSI デバイスの設定を制御できます。

オプション	説明
TLS 認証の構成	このデバイスの起動 TLS 認証モードを表示または変更します。 None は、HTTP サーバーとクライアントが、この起動に対して相互に認証しないことを意味します。 1つの方法 として、HTTP サーバーはクライアントによって認証されますが、クライアントはサーバーによって認証されません。デフォルトでは、このオプションはなしに設定されています。

内蔵デバイス

Integrated Devices (内蔵デバイス) 画面を使用して、ビデオコントローラ、内蔵 RAID コントローラ、および USB ポートを含むすべての内蔵デバイスの設定を表示し設定することができます。

内蔵デバイスの表示

Integrated Devices (内蔵デバイス) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。
4. **System BIOS** (システム BIOS) 画面で、**Integrated Devices** (内蔵デバイス) をクリックします。

内蔵デバイスの詳細

このタスクについて

Integrated Devices (内蔵デバイス) 画面の詳細は、次のとおりです。

オプション	説明
ユーザー アクセス可能 USB ポート	ユーザーアクセス可能 USB ポートを設定します。 Only Back Ports On (背面ポートのみオン) を選択すると、前面の USB ポートが無効になります。 All Ports Off (すべてのポートをオフ) を選択すると、前面と背面のすべての USB ポートが無効になります。 USB キーボードとマウスは、選択に応じて起動プロセス中も特定の USB ポートで機能します。オペレーティングシステムドライバがロードされた後、フィールドの設定に応じて USB ポートは有効/無効が切り替わります。
内蔵 USB ポート	内蔵 USB ポートを有効または無効にします。このオプションはオンまたはオフに設定されています。デフォルトでは、このオプションはオンに設定されています。 メモ: PCIe ライザー上の内蔵 SD カード ポートは内蔵 USB ポートによって制御されます。
iDRAC ダイレクト USB ポート	iDRAC ダイレクト USB ポートは iDRAC によってのみ管理され、ホストの可視性はありません。このオプションはオンまたはオフに設定されています。ときに設定をオフにするには、iDRAC はこの管理対象ポートに取り付けられた USB デバイスを検出しません。デフォルトでは、このオプションはオンに設定されています。
内蔵 RAID コントローラ	内蔵 RAID コントローラを有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。
内蔵 NIC1 および NIC2	メモ: Embedded NIC1 および NIC2 オプションは、 内蔵ネットワークカード 1 がないシステムでのみ使用できます。 Embedded NIC1 および NIC2 オプションの有効/無効を切り替えます。 Disabled (無効) に設定されている場合、NIC は、組み込み管理コントローラにより共有ネットワークアクセス用に引き続き使用可能となって

オプション	説明
	<p>いる可能性があります。Embedded NIC1 と NIC2 オプションはネットワークドーターカード (NDC) がないシステムでのみご利用いただけます。Embedded NIC1 および NIC2 オプションは、内蔵ネットワークカード 1 オプションと同時に指定することはできません。システムの NIC 管理ユーティリティを使用して、Embedded NIC1 および NIC2 オプションを設定します。</p>
I/OAT DMA エンジン	<p>I/O 加速テクノロジー (I/OAT) オプションの有効/無効を切り替えます。I/OAT は、ネットワークトラフィックを高速化しながら CPU の利用率を低減するように設計された DMA 機能のセットです。ハードウェアおよびソフトウェアがこの機能をサポートしている場合にのみ有効にします。このオプションは、デフォルトで 無効 に設定されています。</p>
I/O Snoop HoldOff Response	<p>PCI I/O が CPU からのスヌープリクエストを保留できるサイクル数を選択し、LLC への独自の書き込みを完了する時間を確保します。この設定では、スループットを向上させ、レイテンシーが重要な作業負荷でのパフォーマンスが向上できます。</p>
内蔵ビデオコントローラー	<p>内蔵ビデオコントローラーをプライマリディスプレイとして使用するが 有効 に設定すると、アドイングラフィックスカードが取り付けられている場合でも、内蔵ビデオコントローラーがプライマリディスプレイとして使用されます。 無効 に設定すると、アドイングラフィックスカードがプライマリディスプレイとして使用されます。BIOS は POST 中に出力をプライマリビデオと内蔵ビデオで追加の両方に表示され、プレブート環境。オペレーティングシステムが起動する前に内蔵ビデオが無効になります。このオプションは、デフォルトで 有効 に設定されています。</p>
	<p>メモ: 次の場合は、複数のシステムにインストールされてグラフィックスカードで、PCI 列挙中に検出された最初のカードがプライマリビデオとして選択されて追加されます。に、スロット内のどちらをプライマリビデオカードがを制御するには、カードを調整し直す必要があります。</p>
内蔵ビデオコントローラーの現在の状態	<p>組み込みビデオコントローラーの現在の状態を表示します。 Current State of Embedded Video Controller (組み込みビデオコントローラーの現在の状態) オプションは、読み取り専用フィールドです。内蔵ビデオコントローラーがシステム内で唯一の表示機能である (つまり、増設グラフィックスカードが取り付けられていない) 場合、 Embedded Video Controller (内蔵ビデオコントローラ) 設定が Disabled (無効) となっても、内蔵ビデオコントローラーが自動的にプライマリディスプレイとして使用されます。</p>
SR-IOV グローバルの有効化	<p>シングルルート I/O 仮想化 (SR-IOV) デバイスの BIOS 設定の有効/無効を切り替えます。このオプションは、デフォルトで 無効 に設定されています</p>
内蔵 SD カードポート	<p>内蔵デュアル SD モジュール (IDSDM) の内蔵 SD カードポートの有効/無効を切り替えます。デフォルトでは、このオプションは オン に設定されています。</p>
内蔵 SD カードの冗長性	<p>内蔵デュアル SD モジュール (IDSDM) の冗長性モードを設定します。「ミラーモード」に設定すると、データは両方の SD カードに書き込まれます。どちらかのカードに不具合が発生し、不具合の発生したカードを交換すると、システム起動中にアクティブなカードのデータがオフラインカードにコピーされます。</p> <p>「冗長性」を 無効 に設定すると、プライマリ SD カードのみが OS にこのオプションは、デフォルトで 無効 に設定されています。</p>
内蔵 SD プライマリカード	<p>デフォルトでは、SD カード 1 がプライマリ SD カードとして選択されます。SD カード 1 が存在しない場合、SD カード 2 がプライマリ SD カードとしてコントローラーから選択されます。</p>
OS ウォッチドッグタイマー	<p>システムが応答を停止した場合、このウォッチドッグタイマーはオペレーティングシステムのリカバリーに便利です。このオプションが Enabled (有効) に設定されている場合、オペレーティングシステムはタイマーを初期化します。このオプションが Disabled (無効) に設定されている場合、タイマーはシステムに何ら影響しません。</p>
空のスロットの表示	<p>BIOS と OS にアクセスできるすべての空のスロットの root ポートを有効または無効にします。このオプションは、デフォルトで 無効 に設定されています。</p>
4 GB を超える I/O のメモリマップ化	<p>大容量メモリを必要とする PCIe デバイスのサポートの有効/無効を切り替えます。このオプションは、64 ビットのオペレーティングシステムに対してのみ有効にします。このオプションは、デフォルトで 有効 に設定されています。</p>
I/O ベースメモリマップ化	<p>12 TB に設定すると、MMIO ベースは 12 TB にマップされます。この 44 ビットの PCIe アドレス指定が必要に OS をインストールするためのオプションを有効にします。 512 GB に設定すると、システムによって MMIO ベースが 512 GB にマップされ、メモリの最大サポートを 512 GB 未満に低減します。4 GPU DGMA の不具合に対してだけ有効にします。このオプションは、デフォルトで 56 TB に設定されています。</p>
スロット無効化	<p>お使いのシステムで利用可能な PCIe スロットの有効/無効を切り替えます。Slot Disablement (スロット無効) 機能により、指定のスロットに取り付けられている PCIe カードの構成が管理されます。スロット無効の使用は、取り付けられている周辺機器 (拡張) カードによってオペレーティングシステムの起動が妨げられているか、またはシステム起動の遅延が生じて場合のみでなければなりません。スロットが無効になる</p>

オプション

説明

と、Option ROM と UEFI ドライバの両方が無効になります。制御が可能なのは、システムに存在するスロットに限られます。

表 2. スロット無効化

オプション	説明
スロット 1	有効または無効にするか、起動ドライバーは、PCIe スロット 1 にのみ無効になります。このオプションは、デフォルトで 有効 に設定されています。
スロット 2	有効または無効にするか、起動ドライバーは、PCIe スロット 2 にのみ無効になります。このオプションは、デフォルトで 有効 に設定されています。
スロット 3	有効または無効にするか、起動ドライバーは、PCIe スロット 3 にのみ無効になります。このオプションは、デフォルトで 有効 に設定されています。

スロット分岐

Platform Default Bifurcation、**Auto Discovery of Bifurcation**、**Manual Bifurcation Control** を許可します。デフォルトは、**Platform Default Bifurcation** に設定されています。スロット分岐フィールドは、**Manual Bifurcation Control** に設定された場合に利用でき、**Platform Default Bifurcation** または **Auto Discovery of Bifurcation** に設定されている場合には無効になります。

表 3. スロット分岐

オプション	説明
自動検出分岐設定	プラットフォームのデフォルト分岐、自動分岐、手動分岐
スロット 2 分岐	x16 分岐、x4 分岐、x8 分岐、x4x4x8 分岐、x8x4x4 分岐のいずれか

シリアル通信

Serial Communication (シリアル通信) 画面を使用して、シリアル通信ポートのプロパティを表示します。

シリアル通信の表示

Serial Communication (シリアル通信) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メインメニュー画面で、**システム BIOS** をクリックします。
4. **System BIOS** (システム BIOS) 画面で **Serial Communication** (シリアル通信) をクリックします。

シリアル通信の詳細

このタスクについて

シリアル通信画面の詳細は、次のとおりです。

オプション	説明
シリアル通信	BIOS でシリアル通信デバイス (シリアル デバイス 1 およびシリアル デバイス 2) を選択することができます。BIOS コンソールリダイレクトを有効にして、ポートアドレスを指定できます。このオプションは、デフォルトで Auto (自動) に設定されています。
シリアルポートアドレス	シリアル デバイスのポート アドレスを設定することができます。このフィールドは、シリアル ポート アドレスを COM1 または COM2 (COM1=0x3F8、COM2=0x2F8) に設定します。デフォルトでは、このオプションは、シリアル デバイス 1= COM2 、またはシリアル デバイス 2= COM1 に設定されます。 メモ: シリアルオーバー LAN (SOL) 機能にはシリアルデバイス 2 のみ使用できます。SOL でコンソールのリダイレクトを使用するには、コンソールのリダイレクトとシリアルデバイスに同じポートアドレスを設定します。 メモ: システムを起動するたびに、BIOS は iDRAC で保存された設定でシリアル MUX を同期します。シリアル MUX 設定は、iDRAC で個別に変更できます。したがって、BIOS セットアップユーティリティから BIOS のデフォルト設定をロードしても、シリアル MUX の設定がシリアルデバイス 1 のデフォルト設定に戻らない場合があります。
外付けシリアルコネクタ	このオプションを使用して、外付けシリアルコネクタを Serial Device 1 、 Serial Device 2 、または Remote Access Device に関連付けることができます。このオプションは、デフォルトで Serial Device 1 に設定されています。 メモ: Serial Over LAN (SOL) には Serial Device 2 のみ使用できます。SOL でコンソールのリダイレクトを使用するには、コンソールのリダイレクトとシリアルデバイスに同じポートアドレスを設定します。 メモ: システムを起動するたびに、BIOS は iDRAC で保存された設定でシリアル MUX を同期します。シリアル MUX 設定は、iDRAC で個別に変更できます。したがって、BIOS セットアップユーティリティから BIOS のデフォルト設定をロードしても、この設定がシリアルデバイス 1 のデフォルト設定に戻らない場合があります。
フェイルセーフポーレート	コンソールのリダイレクトに使用されているフェイルセーフポーレートが表示されます。BIOS は自動的にポーレートの決定を試みます。このフェイルセーフポーレートは、その試みが失敗した場合にのみ使用されます。また、値は変更しないでください。デフォルトでは、このオプションは 115200 に設定されています。
リモートターミナルタイプ	リモートコンソールターミナルのタイプを設定することができます。このオプションは、デフォルトで VT100/VT220 に設定されています。
起動後のリダイレクト	オペレーティングシステムのロード時に BIOS コンソールのリダイレクトの有効または無効を切り替えることができます。このオプションは、デフォルトで 有効 に設定されています。

システムプロファイル設定

System Profile Settings (システムプロファイル設定) 画面を使用して、電源管理などの特定のシステムパフォーマンス設定を有効にできます。

システムプロファイル設定の表示

System Profile Settings (システムプロファイル設定) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティング システムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。
4. **System BIOS** (システム BIOS) 画面で、**System Profile Settings** (システムプロファイル設定) をクリックします。

システム プロファイル設定の詳細

このタスクについて

System Profile Settings 画面の詳細は、次のとおりです。

オプション	説明
システムプロファイル	システムプロファイルを設定します。System Profile (システムプロファイル) オプションを Custom (カスタム) 以外のモードに設定すると、BIOS が残りのオプションを自動的に設定します。モードが カスタム に設定した場合は、オプションの残りの部分のみを変更することができます。このオプションをに設定し、 ワット (DAPC) ごとのデフォルトで、DAPC は Dell Active Power Controller です。この他のオプションとして ワットあたりのパフォーマンス (OS) 、 パフォーマンス 、および ワークステーションのパフォーマンス があります。 メモ: システムプロファイル設定画面のすべてのパラメーターは、システムプロファイルオプションが Custom に設定されている場合のみ使用可能です。
CPU 電源管理	CPU 電源管理を設定します。デフォルトでは、このオプションはシステム DBPM (DAPC) に設定されています。DBPM は Demand-Based Power Management (デマンドベースの電源管理) の略です。その他のオプションとして、 OS DBPM と 最大限のパフォーマンス があります。
メモリー周波数	システムメモリーの速度を設定します。 最大限のパフォーマンス 、 Maximum Reliability 、または特定の速度を選択することができます。デフォルトでは、このオプションは 最大限のパフォーマンス に設定されています。
ターボブースト	プロセッサがターボブーストモードで動作するかどうかを設定できます。このオプションは、デフォルトで 有効 に設定されています。
C1E	アイドル時にプロセッサが最小パフォーマンス状態に切り替わるかどうかを設定できます。このオプションは、デフォルトで 有効 に設定されています。
Cステート	プロセッサが利用可能なすべての電源状態で動作するかどうかを設定できます。このオプションは、デフォルトで 有効 に設定されています。
書き込みデータCRC	書き込みデータCRCを有効または無効にします。このオプションは、デフォルトで 無効 に設定されています。
メモリー巡回スクラップ	メモリー巡回スクラップの周波数を設定することができます。デフォルトでは、このオプションは Standard (標準) に設定されています。
メモリーリフレッシュレート	メモリーリフレッシュレートを 1x または 2x に設定します。このオプションは、デフォルトで 1x に設定されています。
アンコアの周波数	Processor Uncore Frequency オプションを選択できます。 Dynamic mode によって、プロセッサがランタイム中のコアおよびアンコア全体の電源リソースを最適化できます。電力を節約、またはパフォーマンスを最適化するためのアンコア周波数の最適化は、 エネルギー効率のポリシー の設定の影響を受けます。
エネルギー効率のポリシー	Energy Efficient Policy オプションを選択することが可能になります。 CPU はプロセッサの内部動作を操作するための設定を使用して、より高いパフォーマンスを求めるか、それともより良い省電力を求めるかを判断します。デフォルトでは、このオプションは Balanced Performance に設定されています。
プロセッサ1のターボブースト対応コアの数	メモ: システムに取り付けられているプロセッサが2台ある場合は、 Number of Turbo Boost Enabled Cores for Processor 2 のエントリが表示されます。 プロセッサ1のターボブースト対応コア数を制御します。コアの最大数がデフォルトで有効にします。
Monitor/Mwait	プロセッサ内の Monitor/Mwait 命令を有効にします。デフォルトでは、このオプションは Custom を除くすべてのシステムで、 Enabled に設定されています。

オプション	説明
	<p>① メモ: このオプションは、Custom モードの C States オプションが Disabled に設定されている場合に限り、無効化できます。</p> <p>① メモ: Custom モードで C States が Enabled に設定されている場合に、Monitor/Mwait 設定を変更しても、システムの電力またはパフォーマンスは影響を受けません。</p>
CPU バス相互リンクの電源管理	CPU バス相互リンク電源管理を有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。
PCI ASPM L1 リンクの電源管理	PCI ASPM L1 リンクの電源管理を有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。

システムセキュリティ

System Security (システムセキュリティ) 画面を使用して、システムパスワードとセットアップパスワードの設定や、電源ボタンの無効化などの特定の機能を実行できます。

システムセキュリティの表示

System Security (システムセキュリティ) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

① **メモ:** F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。
4. **System BIOS** (システム BIOS) 画面で **System Security** (システムセキュリティ) をクリックします。

システムセキュリティ設定の詳細

このタスクについて

システムセキュリティ設定画面の詳細は次の通りです。

オプション	説明
CPU AES-NI	Advanced Encryption Standard Instruction Set (AES-NI) を使用して暗号化および復号を行うことによって、アプリケーションのスピードを向上させます。このオプションは、デフォルトで 有効 に設定されています。
System Password	システムパスワードを設定することができます。このオプションは、デフォルトで Enabled に設定されており、システムにパスワードジャンパが取り付けられていない場合は、読み取り専用になります。
Setup Password	システム セットアップパスワードを設定することができます。システムにパスワードジャンパーが取り付けられていない場合、このオプションは読み取り専用です。
Password Status	システムパスワードをロックすることができます。デフォルトでは、このオプションは ロック解除 に設定されています。
TPM Security	<p>① メモ: TPM メニューは、TPM モジュールがインストールされている場合のみ使用可能です。</p> <p>TPM の報告モードを制御することができます。デフォルトでは、TPM Security オプションは オフ に設定されています。[TPM Status] フィールド、[TPM Activation] フィールド、および [Intel TXT] フィールドは、TPM Status フィールドが On with Pre-boot Measurements または On without Pre-boot Measurements のいずれかに設定されている場合に限り、変更できます。</p>

表 4. TPM 1.2 セキュリティ情報

オプション	説明
TPM 情報	TPM の動作状態を変更することができます。このオプションは、デフォルトで 変更なし に設定されています。
TPM ファームウェア	TPM のファームウェアバージョンを示します。
TPM Status	TPM ステータスを指定します。
TPM Command	トラステッドプラットフォームモジュール (TPM) を制御します。 なし に設定すると、どのコマンドも TPM に送信されません。 アクティブにする に設定すると、TPM は有効かつアクティブになります。 無効にする に設定すると、TPM は無効かつ非アクティブになります。 クリアする に設定すると、TPM のすべてのプロパティがクリアされます。デフォルトでは、このオプションは None に設定されています。

表 5. TPM 2.0 セキュリティ情報

オプション	説明
TPM 情報	TPM の動作状態を変更することができます。このオプションは、デフォルトで 変更なし に設定されています。
TPM ファームウェア	TPM のファームウェアバージョンを示します。
TPM Hierarchy (TPM 階層)	ストレージと承認階層を有効または無効にするか、クリアします。 Enabled (有効) に設定すると、ストレージと承認階層を使用できます。 Disabled (無効) に設定すると、ストレージと承認階層を使用できません。 Clear (クリアする) に設定すると、ストレージと承認階層の値がすべてクリアされ、 Enabled (有効) にリセットされます。

TPM 情報

TPM の動作状態を変更することができます。このオプションは、デフォルトで**変更なし**に設定されています。

TPM Status

TPM ステータスを指定します。

TPM Command

トラステッドプラットフォームモジュール (TPM) を制御します。**なし**に設定すると、どのコマンドも TPM に送信されません。**アクティブにする**に設定すると、TPM は有効かつアクティブになります。**無効にする**に設定すると、TPM は無効かつ非アクティブになります。**クリアする**に設定すると、TPM のすべてのプロパティがクリアされます。デフォルトでは、このオプションは **None** に設定されています。

△ 注意: TPM をクリアすると、TPM 内のすべてのキーが失われます。TPM キーが失われると、オペレーティングシステムの起動に影響するおそれがあります。

TPM セキュリティがオフに設定されている場合、このフィールドは読み取り専用になります。このアクションの結果を有効にするには、再起動が必要になります。

TPM の詳細設定

[TPM Security] が [ON] に設定されている場合のみ、この設定は有効になります。

Intel(R) TXT

Intel® Trusted Execution Technology (TXT) オプションを設定することができます。**Intel TXT** オプションを有効にするには、仮想化テクノロジーと TPM セキュリティを起動前測定ありで有効にする必要があります。このオプションは、デフォルトで**オフ**に設定されています。

Power Button

システムの前面にある電源ボタンを設定することができます。このオプションは、デフォルトで**有効**に設定されています。

オプション	説明								
AC Power Recovery	AC 電源が回復した後のシステムの動作を設定します。このオプションは、デフォルトで 前回 に設定されています。								
AC Power Recovery Delay	システムの AC 電源が回復した後、システムが電源をオンにするのにかかる時間を設定することができます。デフォルトでは、このオプションは Immediate に設定されています。								
ユーザー定義の遅延 (60 ~ 600 秒)	AC 電源リカバリー遅延 に ユーザー定義 オプションが選択されている場合、 ユーザー定義の遅延 オプションを設定することができます。								
UEFI Variable Access	UEFI 変数を安全に維持するためのさまざまな手段を提供します。 Standard (デフォルト) に設定されている場合、UEFI 変数は UEFI 仕様によってオペレーティング システムでアクセス可能です。 制御 に設定されている場合、選択した UEFI 変数は環境内で保護され、新しい UEFI 起動エントリが現在の起動順序の最後に実行されます。								
インバンド管理機能インターフェイス	ときに設定を 無効 にすると、この設定は、管理エンジンの (ME)、HECI デバイスは、およびシステムのオペレーティング システムから IPMI デバイスを非表示にします。これにより、ME の電源上限が設定を変更するには、オペレーティング システム、および防止します。すべてのインバンド管理ツールへのアクセスをブロックすべての管理を介して管理帯域外になります。このオプションは、デフォルトで 有効 に設定されています。 メモ: BIOS アップデートの HECI デバイスで動作可能と DUP アップデート IPMI インターフェイスを操作可能にする必要があります。この設定をする必要がセットに なっている エラーのアップデートを避けてください。								
Secure Boot	セキュア ブートを有効にします。ここでは BIOS はセキュア ブートポリシーの証明書を使用して各プリブートイメージを認証します。セキュア ブートはデフォルトで 無効 になっています。セキュア ブートはデフォルトで 無効 に設定されています。								
Secure Boot Policy	セキュア ブート ポリシーが 標準 に設定されている場合、BIOS はシステムの製造元のキーと証明書を使用して起動前イメージを認証します。セキュア ブート ポリシーが カスタム に設定されている場合、BIOS はユーザー定義のキーおよび証明書を使用します。セキュア ブート ポリシーはデフォルトで 標準 に設定されています。								
Secure Boot Mode	BIOS によるセキュア ブート ポリシー オブジェクト (PK、KEK、db、dbx) の使用方法を設定することができます。 現在のモードが 展開モード に設定されている場合、設定可能なオプションは ユーザーモード と 展開モード です。現在のモードが ユーザーモード に設定されている場合、設定可能なオプションは ユーザーモード 、 監査モード 、 展開モード です。								
	<table border="1"> <thead> <tr> <th>オプション</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>User Mode</td> <td>ユーザーモードでは、PK、取り付け、および BIOS を使ったプログラムのポリシー オブジェクトをアップデートしようとする署名の検証を実行している必要があります。 BIOS では、未認証のプログラムによるモード間の遷移が許可されます。</td> </tr> <tr> <td>Audit Mode</td> <td>監査モードでは、PK は存在しません。BIOS は、ポリシー オブジェクトのプログラムによるアップデートおよびモード間の遷移を認証しません。 監査モードは、ポリシー オブジェクトのワーキングセットをプログラムによって決定する際に役立ちます。 BIOS はプリブートイメージに対して署名検証を実行します。BIOS は起動前イメージで署名確認を実行して、その結果をイメージ実行情報テーブルに記録しますが、確認の可否にかかわらずそのイメージを承認します。</td> </tr> <tr> <td>展開モード</td> <td>展開モードは最も安全なモードです。展開されたモードでは、PK にインストールすると、BIOS プログラムのポリシー オブジェクトをアップデートしようとする署名の検証を実行している必要があります。 展開されたモードは、プログラムによるモードの移行を制限します。</td> </tr> </tbody> </table>	オプション	説明	User Mode	ユーザーモード では、PK、取り付け、および BIOS を使ったプログラムのポリシー オブジェクトをアップデートしようとする署名の検証を実行している必要があります。 BIOS では、未認証のプログラムによるモード間の遷移が許可されます。	Audit Mode	監査モード では、PK は存在しません。BIOS は、ポリシー オブジェクトのプログラムによるアップデートおよびモード間の遷移を認証しません。 監査モード は、ポリシー オブジェクトのワーキングセットをプログラムによって決定する際に役立ちます。 BIOS はプリブートイメージに対して署名検証を実行します。BIOS は起動前イメージで署名確認を実行して、その結果をイメージ実行情報テーブルに記録しますが、確認の可否にかかわらずそのイメージを承認します。	展開モード	展開モード は最も安全なモードです。 展開されたモード では、PK にインストールすると、BIOS プログラムのポリシー オブジェクトをアップデートしようとする署名の検証を実行している必要があります。 展開されたモード は、プログラムによるモードの移行を制限します。
オプション	説明								
User Mode	ユーザーモード では、PK、取り付け、および BIOS を使ったプログラムのポリシー オブジェクトをアップデートしようとする署名の検証を実行している必要があります。 BIOS では、未認証のプログラムによるモード間の遷移が許可されます。								
Audit Mode	監査モード では、PK は存在しません。BIOS は、ポリシー オブジェクトのプログラムによるアップデートおよびモード間の遷移を認証しません。 監査モード は、ポリシー オブジェクトのワーキングセットをプログラムによって決定する際に役立ちます。 BIOS はプリブートイメージに対して署名検証を実行します。BIOS は起動前イメージで署名確認を実行して、その結果をイメージ実行情報テーブルに記録しますが、確認の可否にかかわらずそのイメージを承認します。								
展開モード	展開モード は最も安全なモードです。 展開されたモード では、PK にインストールすると、BIOS プログラムのポリシー オブジェクトをアップデートしようとする署名の検証を実行している必要があります。 展開されたモード は、プログラムによるモードの移行を制限します。								
Secure Boot Policy Summary	イメージを認証するためにセキュア ブートが使用する証明書とハッシュのリストを指定します。								

オプション 説明

セキュア ブート カスタム ポリシーの設定
セキュア ブート カスタム ポリシーを設定します。このオプションを有効にするには、セキュア ブート ポリシーをカスタムに設定します。

システムパスワードおよびセットアップパスワードの作成

前提条件

パスワードジャンプが有効になっていることを確認します。パスワードジャンプによって、システムパスワードとセットアップパスワードの機能の有効/無効を切り替えることができます。詳細については、「システム ボードのジャンプ設定」の項を参照してください。

メモ: パスワードジャンプの設定を無効にすると、既存のシステムパスワードとセットアップパスワードは削除され、システムの起動にシステムパスワードを入力する必要がなくなります。

手順

1. システム セットアップを起動するには、システムの電源投入または再起動の直後に F2 を押します。
2. **System Setup Main Menu** (セットアップユーティリティメインメニュー) 画面で、**System BIOS (システム BIOS) > System Security (システムセキュリティ)** の順にクリックします。
3. **System Security (システムセキュリティ)** 画面で、**Password Status (パスワードステータス)** が **Unlocked (ロック解除)** に設定されていることを確認します。
4. システムパスワードフィールドに、システムパスワードを入力して、Enter または Tab を押します。
以下のガイドラインに従ってシステムパスワードを設定します。
 - パスワードの文字数は 32 文字までです。
 - 0 から 9 までの数字を含めることができます。

システムパスワードの再入力を求めるメッセージが表示されます。

5. システムパスワードをもう一度入力し、**OK** をクリックします。
6. **Setup Password (セットアップパスワード)** フィールドに、セットアップパスワードを入力して、Enter または Tab を押します。
セットアップパスワードの再入力を求めるメッセージが表示されます。
7. セットアップパスワードをもう一度入力し、**OK** をクリックします。
8. Esc を押してシステム BIOS 画面に戻ります。もう一度 Esc を押します。
変更の保存を求めるプロンプトが表示されます。

メモ: システムが再起動するまでパスワード保護機能は有効になりません。

システムを保護するためのシステムパスワードの使い方

このタスクについて

セットアップパスワードが割り当てられている場合、システムはセットアップパスワードをシステムパスワードの代用として受け入れます。

手順

1. システムの電源を入れるかまたは再起動します。
2. システムパスワードを入力し、Enter を押します。

次の手順

パスワードステータスがロックに設定されている場合は、再起動時に画面の指示に従ってシステムパスワードを入力し、Enter を押します。

メモ: 間違ったシステムパスワードが入力されると、メッセージが表示され、パスワードの再入力が求められます。パスワードの入力は 3 回試行できます。3 回目の入力エラーになると、システムは機能を停止して電源を切る必要があるというエラー

メッセージがシステムによって表示されます。システムをシャットダウンして再起動しても、正しいパスワードを入力するまで、このエラーメッセージが表示されます。

システムおよびセットアップパスワードの削除または変更

前提条件

- ① **メモ: Password Status** (パスワードステータス) が **Locked** (ロック) に設定されている場合、既存のシステムパスワードまたはセットアップパスワードを削除または変更することはできません。

手順

1. セットアップユーティリティを起動するには、システムの電源投入または再起動の直後に F2 を押します。
2. **System Setup Main Menu** (セットアップユーティリティメインメニュー) 画面で、**System BIOS** (システム BIOS) > **System Security** (システムセキュリティ) の順にクリックします。
3. **System Security** (システムセキュリティ) 画面で **Password Status** (パスワードステータス) が **Unlocked** (ロック解除) に設定されていることを確認します。
4. システムパスワードフィールドで、既存のシステムパスワードを変更または削除して、Enter または Tab を押します。
5. **Setup Password** (セットアップパスワード) フィールドで、既存のシステムパスワードを変更または削除して、Enter または Tab を押します。
 - ① **メモ:** システムパスワードまたはセットアップパスワードを変更する場合は、新しいパスワードの再入力を求めるメッセージが表示されます。システムパスワードまたはセットアップパスワードを削除する場合は、削除の確認を求めるメッセージが表示されます。
6. Esc を押してシステム BIOS 画面に戻ります。もう一度 Esc を押すと、変更の保存を求めるプロンプトが表示されます。
7. セットアップパスワードを選択し、既存のセットアップパスワードを変更または削除して、Enter または Tab を押します。
 - ① **メモ:** システムパスワードまたはセットアップパスワードを変更する場合は、新しいパスワードの再入力を求めるメッセージが表示されます。システムパスワードまたはセットアップパスワードを削除する場合は、削除の確認を求めるメッセージが表示されます。

セットアップパスワード使用中の操作

セットアップパスワードが**有効**に設定されている場合は、システム セットアップ オプションを変更する前に正しいセットアップパスワードを入力します。

誤ったパスワードを3回入力した場合は、システムに次のメッセージが表示されます。

```
Number of unsuccessful password attempts: <3> Maximum number of password attempts exceeded.  
System Halted!
```

システムを再起動しても、正しいパスワードを入力するまではこのエラーメッセージが表示されます。次のオプションがサポートされています。

- システムパスワードが**有効**に設定されておらず、**パスワードステータス** オプションでロックされていない場合は、システムパスワードを設定できます。詳細については、「[システムセキュリティ設定の詳細](#)」の項を参照してください。
- 既存のシステムパスワードは、無効にすることも変更することもできません。

- ① **メモ:** 不正な変更からシステムパスワードを保護するため、パスワードステータスオプションをセットアップパスワードオプションと併用することができます。

冗長 OS 制御

Redundant OS Control 画面では、冗長 OS 情報を設定することができます。これにより、システムで物理リカバリディスクをセットアップすることができます。

冗長 OS 制御の表示

Redundant OS Control 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。
4. System BIOS 画面で、Redundant OS Control をクリックします。

Redundant OS Control 画面の詳細

Redundant OS Control 画面の詳細は、次のとおりです。

このタスクについて

オプション	説明
冗長 OS の場所	次のデバイスからバックアップ ディスクを選択できます。 <ul style="list-style-type: none">● なし● IDSDM● AHCI での SATA ポート● BOSS PCIe Cards (Internal M.2 Drives)● 内蔵 USB <p>メモ: RAID 構成と NVMe カードは含まれません。これらの構成で個々のドライブを区別する機能が BIOS にはないためです。</p>
冗長 OS の状態	<p>メモ: このオプションは、Redundant OS Location が None に設定されている場合は、無効になります。</p> <p>Visible に設定すると、バックアップ ディスクがブート リストと OS で認識されます。Hidden に設定すると、バックアップ ディスクは無効になり、ブート リストと OS で認識されません。このオプションは、デフォルトで Visible に設定されています。</p> <p>メモ: BIOS がハードウェアのデバイスを無効にするため、OS からデバイスにアクセスできません。</p>
冗長 OS 起動	<p>メモ: このオプションは、Redundant OS Location が None に設定されている場合、または Redundant OS State が Hidden に設定されている場合は、無効になります。</p> <p>Enabled に設定すると、BIOS は Redundant OS Location に指定されているデバイスを起動します。Disabled に設定すると、BIOS は現在のブート リストの設定を保持します。このオプションは、デフォルトで無効に設定されています。</p>

その他の設定

Miscellaneous Settings (その他の設定) 画面を使用して、Asset Tag の更新やシステムの日付と時刻の変更などの特定の機能を実行できます。

その他の設定の表示

Miscellaneous Settings (その他の設定) 画面を表示するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたらすぐに F2 を押します。

F2 = System Setup

メモ: F2 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

3. システム セットアップ メイン メニュー画面で、システム BIOS をクリックします。
4. **System BIOS** (システム BIOS) 画面で、**Miscellaneous Settings** (その他の設定) をクリックします。

Miscellaneous Settings の詳細

このタスクについて

Miscellaneous Settings 画面の詳細は、次のとおりです。

オプション	説明
システム時刻	システムの時刻を設定することができます。
システム日付	システムの日付を設定することができます。
Asset Tag	Asset Tag を指定して、セキュリティと追跡のために変更することができます。
キーボード NumLock	NumLock が有効または無効のどちらの状態でもシステムが起動するかを設定できます。デフォルトでは、このオプションは オン に設定されています。 メモ: このフィールドは 84 キーのキーボードには適用されません。
エラー時 F1/F2 プロンプト	エラー時の F1/F2 プロンプトを有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。F1/F2 プロンプトは、キーボードエラーも含まれます。
レガシービデオオプション ROM のロード	システム BIOS でビデオコントローラーからレガシービデオ (INT 10H) オプション ROM をロードするかを決定できます。オペレーティングシステムで 有効 を選択すると、UEFI ビデオ出力標準をサポートしません。このフィールドは UEFI 起動モードでのみ有効です。 UEFI Secure Boot モードが Enabled の場合は、このオプションを有効に設定できません。このオプションは、デフォルトで 無効 に設定されています。
Dell Wyse P25/P45 BIOS Access	Dell Wyse P25 / P45 BIOS Access を有効または無効にします。このオプションは、デフォルトで 有効 に設定されています。
電源サイクルリクエスト	電源サイクルリクエストを有効または無効にします。デフォルトでは、このオプションは なし に設定されています。

iDRAC 設定ユーティリティ

iDRAC 設定ユーティリティは、UEFI を使用して iDRAC パラメーターをセットアップおよび設定するためのインターフェイスです。iDRAC 設定ユーティリティを使用することで、さまざまな iDRAC パラメーターを有効または無効にすることができます。

メモ: 一部の iDRAC 設定ユーティリティ機能へのアクセスには、iDRAC Enterprise ライセンスのアップグレードが必要です。

iDRAC 使用の詳細については、www.dell.com/poweredgemanuals で『Dell Integrated Dell Remote Access Controller ユーザーズガイド』を参照してください。

デバイス設定

Device Settings では、以下のデバイスパラメータを設定することができます。

- コントローラ構成のユーティリティ
- 組み込み NIC Port1-X の構成
- SlotX の NIC、Port1-X の構成
- BOSS カードの構成

Dell Lifecycle Controller

Dell Lifecycle Controller (LC) は、システムの導入、構成、更新、保守、診断などの高度な組み込み型システム管理機能を提供します。LC は、iDRAC 帯域外ソリューションおよび Dell 製システム内蔵 Unified Extensible Firmware Interface (UEFI) アプリケーションの一部として提供されます。

組み込み型システム管理

Dell Lifecycle Controller により、システムのライフサイクル全体にわたって高度な組み込みシステム管理が提供されます。Dell Lifecycle Controller はブートシーケンス中に開始でき、オペレーティングシステムに依存せずに動作することができます。

メモ: 一部のプラットフォーム構成では、Dell Lifecycle Controller の提供する機能の一部がサポートされない場合があります。

Dell Lifecycle Controller のセットアップ、ハードウェアとファームウェアの設定、およびオペレーティングシステムの導入の詳細については、www.dell.com/poweredgemanuals で Dell Lifecycle Controller のマニュアルを参照してください。

ブートマネージャー

Boot Manager (起動マネージャ) 画面では、起動オプションと診断ユーティリティを選択できます。

ブートマネージャの表示

このタスクについて

Boot Manager (ブートマネージャ) を起動するには、次の手順を実行してください。

手順

1. システムの電源を入れるか、または再起動します。
2. 次のメッセージが表示されたら F11 を押します。

F11 = Boot Manager

F11 を押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、システムを再起動してもう一度やり直してください。

ブートマネージャのメインメニュー

メニュー項目	説明
Continue Normal Boot (通常の起動を続行)	システムは起動順序の先頭にあるデバイスから順に起動を試みます。起動が失敗すると、システムは起動順序内の次のデバイスから起動を試みます。起動が成功するか、起動オプションがなくなるまで処理は続行されます。
One Shot Boot Menu (ワンショット起動メニュー)	起動メニューにアクセスし、ワнтаイム起動デバイスを選択して、このデバイスから起動できます。
Launch System Setup (セットアップユーティリティの起動)	セットアップユーティリティにアクセスできます。
Launch Lifecycle Controller (Lifecycle Controller の起動)	起動マネージャを終了し、Dell Lifecycle Controller プログラムを起動します。
システムユーティリティ	システム診断などのシステムユーティリティメニューを起動できます。

ワンショット UEFI 起動メニュー

ワンショット UEFI 起動メニューでは、起動元となる起動デバイスを選択できます。

システムユーティリティ

System Utilities (システムユーティリティ) には、起動可能な次のユーティリティが含まれています。

- 診断プログラムの起動
- BIOS アップデートファイルエクスプローラ
- システムの再起動

PXE 起動

Preboot Execution Environment (PXE) オプションを使用してネットワーク接続されたシステムをリモートに起動および設定することができます。

PXE boot オプションにアクセスするには、BIOS セットアップから標準のブート シーケンスを使用するかわりに、システムを起動してから POST 中に F12 を押します。それによってメニューが表示されたり、ネットワーク デバイスを管理できたりすることはありません。