




Dell EMC PowerEdge UEFIカスタム セキュア ブート

データセンターサーバーにおけるセキュリティ対策は従来、オペレーティング システム、アプリケーション、およびネットワークのレベルに焦点が当てられていました。ハードウェア インフラストラクチャのセキュリティに関する懸念が高まり続ける中で、ITセキュリティ管理者にとって複雑さが増えています。サーバーとセキュリティを担当するITチームの基本的なニーズは、信頼できるコンピューティング基盤を確立し、その信頼をオペレーティング システムとアプリケーションにまで広げることにあります。通常は最も安全で機密性の高いアプリケーションとデータセットのためとされる、カスタマイズされたインフラストラクチャ セキュリティが急速に目立つようになってきました。サーバー ハードウェアへの脅威の進化を受けて、この信頼された基盤を強化するために、UEFIカスタム セキュア ブートなど、より包括的なアプローチが必要になります。

その先駆けとなるのが、Dell EMCのサイバー レジリエント アーキテクチャです。これは、Integrated Dell Remote Access Controller (iDRAC) のBIOSとファームウェアがロードされる前に検証を行う機能を備えています。その他の重要なコンポーネントのファームウェアも同様に、保存された暗号化証明書を使用して検証され、サーバー上で信頼できるファームウェアが実行されていることが保証されます。

Dell EMCサイバー レジリエント アーキテクチャ

 <h4>効果的な 保護</h4> <ul style="list-style-type: none"> 信頼の根幹となるシリコンベース ハードウェア 署名されたファームウェアのアップデート システムのロックダウン セキュアなデフォルト パスワード 	 <h4>信頼性の高い検知</h4> <ul style="list-style-type: none"> 構成およびファームウェアのドリフト検出 ユーザー アクティビティを含む永続的なイベント ロギング セキュアなアラート 	 <h4>Rapid Recovery</h4> <ul style="list-style-type: none"> 自動 BIOS リカバリー 迅速な OS 復旧 システム 消去
--	--	---

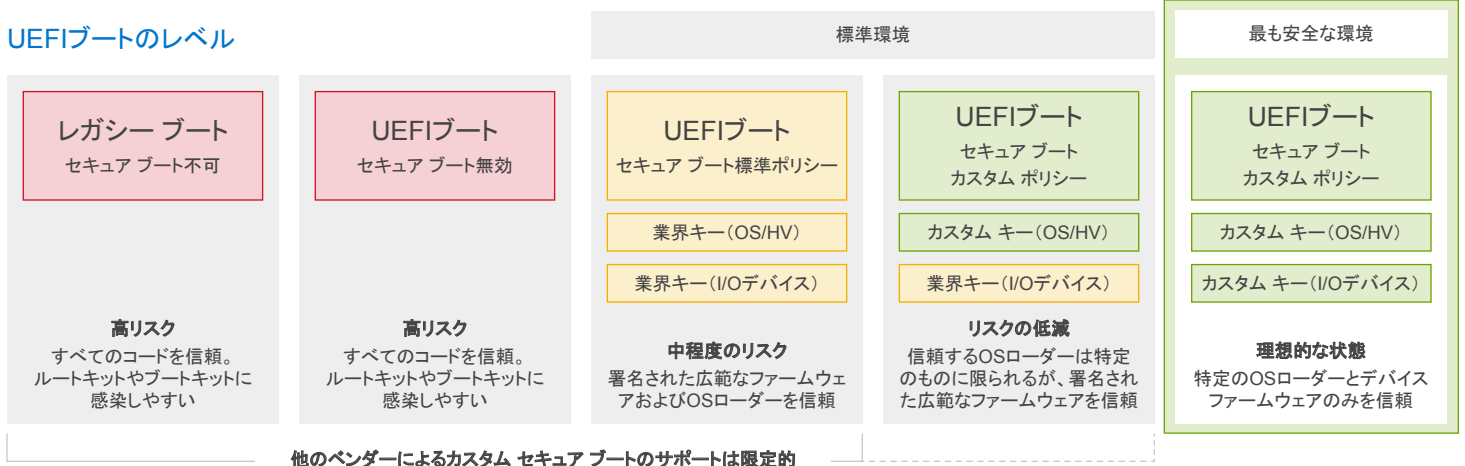
レガシーBIOS構成とスタートアップ制御に代わり最新の機能を備えたUEFIセキュア ブートは、ハイパーバイザーまたはオペレーティング システムが起動する前にサーバーのベースライン機能を初期化します。PowerEdgeサーバーはUEFIセキュア ブートを使用して、UEFIドライバーおよびオペレーティング システム ブートローダーの暗号生成された証明書を確認します。これらの「キー」によって、サーバーは次の検証を行います。

- PCIeカードからロードされたUEFIドライバー
- 大容量ストレージ デバイスからロードされたUEFIドライバーおよび実行ファイル
- オペレーティング システムのブートローダー (通常はLinuxまたはMicrosoft Windows)

この検証プロセスは、オペレーティング システムを起動する前に、サーバーが許可されていないコードを起動することがないようにするために重要なはたらきをします。ブートローダー、カーネル、およびその他のユーザー空間コードのシグネチャを確認することで、UEFIのファームウェア検証はシステムで未署名のソフトウェアの実行を禁止するように設計されています。

Dell EMC PowerEdge UEFIカスタム セキュア ブートには、Microsoft以外の機関によって生成および署名されたカスタム証明書をサポートする独自の機能もあります。Microsoftは、UEFIでサポートされるデバイスとオペレーティング システムのデフォルト認証局です。多くの標準的なLinuxディストリビューションは、Microsoftの証明書を実装しています。非標準のLinux環境 (独自仕様のカーネルまたはドライバーの変更など) が使用されている状況では、カスタム生成された証明書、ユーザーによる暗号化署名、ブートローダーの自己検証、ハードウェアとソフトウェアチェーンの信頼の輪を維持することが必要です。

UEFIブートのレベル



妥協のないサーバー セキュリティの強化

起動プロセスは、あらゆるデバイスのセキュリティの基盤です。さまざまなファームウェアを使用することで、デバイスのコンポーネントと周辺機器の起動方法やオペレーティング システムのロードを制御します。コードが早い段階でロードされるほど多くの特権が付与され、最初に認証がなされないと、より多くの損害を与える可能性があります。起動プロセスが侵害されると、攻撃者はセキュリティ制御を無効にして、システムのさまざまな部分へ不正アクセスができる状態となります。さらに、悪意のある UEFI ブートローダーを使用して起動時にサーバーの制御を取得し、コンピューターの再構成、データの暗号化を行い、大きな損害を与えるランサムウェアを作成することも可能です。

リスクの低減

最新のコントロールと構成オプションを使用することで、ファームウェアやブートローダーの攻撃からサーバーを保護するための最高の備えができます。Dell EMC PowerEdge UEFI カスタム セキュア ブートは、旧来の BIOS ベースの起動方法を捨て、サーバー インフラストラクチャのセキュリティを向上させます。最近の米国家安全保障局 (NSA) による勧告には、サーバー ハードウェア セキュリティの強化に関するトピックが記載されています。特に、複数のオペレーティング システムをサポートする柔軟性ととも、非常に高いレベルのセキュリティを提供する手段として PowerEdge UEFI カスタム セキュア ブートの使用が提唱されています。関連する NSA のサイバーセキュリティ テクニカル レポート¹には、「カスタム モードはシステム所有者が信頼できるハードウェアとソフトウェア ソリューションの選択を狭めることや広げることが可能 ...」と記され、Dell の組込型 UEFI 構成ユーティリティー¹を使用してこれを行う方法が説明されています。このきめ細かな制御により、誤設定、改ざん、およびマルウェアの脅威を軽減または排除することができます。システム管理者は新しいブートの脅威に迅速に対応ができ、ベンダーによる証明書の署名ミスの影響を受けることはありません。

カスタム証明書を使用した UEFI セキュア ブートの特長

特長	説明	メリット
セキュア ブート	<ul style="list-style-type: none">主要コンポーネントとファームウェアの検証	<ul style="list-style-type: none">最新のファームウェア検証を採用し、レガシー BIOS の制限とセキュリティの脅威を解消
自己署名証明書	<ul style="list-style-type: none">サーバーの運用全般にわたり、セキュアなファームウェア、ブートローダー、およびオペレーティング システムの起動を維持	<ul style="list-style-type: none">高度に安全な導入環境におけるカスタマイズされた OS 構築のサポートカスタムビルド ハードウェアと関連ファームウェアの実装時のデフォルト署名権限からの独立性
セキュリティ ガイドラインへの準拠	<ul style="list-style-type: none">サーバー起動プロセス、ファームウェア検証、およびカスタム証明書管理のためのセキュリティ標準に適合	<ul style="list-style-type: none">サーバーのハードウェアおよびファームウェアのセキュリティ標準を確立機密性の高い環境における将来のサーバー セキュリティガイドライン準拠に備えたサーバー運用
iDRAC および TPM との統合	<ul style="list-style-type: none">PowerEdge サーバーに統合済みの既存ハードウェアおよびファームウェアのセキュリティ機能を活用	<ul style="list-style-type: none">統合型セキュリティ機能の価値を最大限に高め、包括的なハードウェア ルートの信頼を確立

¹ ほとんどのシステム設定と同様に、管理者はシステム セットアップ以外の他のツールを使用して、セキュア ブートの標準ポリシーを有効にすることができます。デルの導入ツールキット™ (DTK)、ライフサイクル コントローラー™、OpenManage™ ツール、RACADM コンソール、および WS-MAN コンソールでもセキュア ブートの標準ポリシーを有効にできます。

PowerEdge サーバーをもっと詳しく知る



Dell EMC OpenManage Enterprise に関する
[詳細情報](#)



Dell Technologies のシステム管理ソリューションの
[詳細はこちら](#)



リソース ライブラリーを検索する



Twitter で PowerEdge Servers をフォローする



セールスまたはサポート
について Dell Technologies のエキスパートに問い合わせる