DELL Technologies

ホワイトペーパー

テクニカル ホワイト ペーパー：Dell EMC PowerEdgeサーバーのサイバーレジリエント セキュリティ

2020年12月

改訂

日付	説明
2018年1月	イニシャルリリース
2020年11月	改訂版

目次

目次

概要

デル・テクノロジーズは、内在的アプローチでセキュリティに取り組んでいます。セキュリティを後付けの機能とするのではなく、デルのセキュアな開発ライフサイクル全体を通してあらゆるステップにセキュリティを組み込んでいます。当社は増大し続ける脅威に対処するために、PowerEdgeのセキュリティ管理策、機能、およびソリューションを継続的に進化させ、シリコンベースのRoot of Trust（信頼の基点）を使用してセキュリティを強化し続けています。 このホワイト ペーパーでは、PowerEdgeサイバーレジリエント プラットフォームに内蔵され、Dell Remote Access Controller（iDRAC9）によって有効化されるさまざまなセキュリティ機能について詳しく説明します。以前のPowerEdgeセキュリティ ホワイト ペーパー以降、アクセス制御からデータ暗号化、サプライ チェーン保証まで、多くの新機能が加わっています。機能の例としては、BIOSライブ スキャン、UEFIセキュア ブートのカスタマイズ、RSA SecurID MFA、Secure Enterprise Key Management（SEKM）、Secured Component Verification（SCV）、System Erase、証明書の自動登録および更新、Cipher SelectおよびCNSAのサポートなどがあります。 すべての機能がインテリジェンスと自動化を幅広く活用しており、脅威曲線の先を行き、拡大し続ける使用モデルに合わせて拡張することを可能にしています。

1.はじめに

脅威状況が進化するにつれて、ITおよびセキュリティ担当者がデータとリソースに対するリスクの管理に悪戦苦闘しています。データは多くのデバイスにわたって、またオンプレミスやクラウドで使用されているため、データ侵害の影響は大きくなる一方です。従来、セキュリティ機能は、OSやアプリケーション、ファイアウォール、IPSおよびIDSシステムに配置されてきました。これらすべてが対処すべき重要な領域であることには変わりありません。しかし、この1年または2年の間にハードウェアに発生した脅威を考えると、ファームウェア、BIOS、BMC、およびその他のハードウェア保護（サプライ チェーン保証など）のようなハードウェアベースのインフラストラクチャを保護することが不可欠になっています。

Dell Technologies 2020 Digital Transformation Indexでは、データ プライバシーおよびサイバーセキュリティの懸案事項がデジタル トランスフォーメーションの最大の障壁であることが分かりました。[1] 企業の63%が、脆弱性を悪用したデータ侵害を経験しています[2]。サイバー犯罪に関連する世界的な損害額は、2021年に6兆ドルに達します[3]。

ソフトウェアデファインド データセンター アーキテクチャにおいてサーバーの重要性が高まり、サーバーのセキュリティが企業全体のセキュリティの基盤となっています。サーバー内での後続の操作を検証できる不変のRoot of Trustを活用することで、ハードウェアとファームウェアの両方のレベルでサーバーのセキュリティを強化する必要があります。これによって、導入からメンテナンス、廃棄に至るまでのサーバー ライフサイクル全体にわたって信頼チェーンが確立されます。

iDRAC9を搭載した第14世代および第15世代Dell EMC PowerEdgeサーバーは、この信頼の連鎖を実現し、セキュリティ制御と包括的な管理ツールを組み合わせることで、ハードウェアとファームウェアにわたって強固なセキュリティ レイヤーを提供します。その結果、組み込みのサーバー ファームウェア、システムに格納されているデータ、オペレーティング システム、周辺機器、その内部での管理操作など、サーバーのあらゆる面にわたってサイバーレジリエント アーキテクチャが拡張されます。貴重なサーバー インフラストラクチャと内部のデータを保護し、異常、侵害、または不正な操作を検出し、意図しない、または悪意のあるイベントからのリカバリーを行うためのプロセスを構築することが可能です。

[1] Dell Technologies 2020 Digital Transformation Index

[2] BIOSレベルの制御で、現在のセキュリティ上の脅威に対応します。デルの委託によるForrester Consulting Thought Leadership Paper、2019年

[3] Ransomware Attacks Predicted to Occur... The National Law Review、2020年

2.セキュアなサーバー インフラストラクチャへの道程

Dell EMC PowerEdgeサーバーは、シリコンベースのデータ セキュリティを使用した技術革新などの堅牢なセキュリティ機能を複数世代にわたって備えています。Dell EMC 14G PowerEdgeサーバーはシリコンベースのセキュリティを拡張し、サーバー起動プロセス中に、暗号化されたRoot of Trustを使用してBIOSとファームウェアを認証しています。Dell EMC製品チームは第14世代および第15世代のPowerEdgeサーバーの設計において、モダンIT環境において直面しているセキュリティ上の脅威に対応するためのいくつかの重要な要件を検討しました。

- **保護:** BIOS、ファームウェア、データ、物理ハードウェアなど、ライフサイクルのあらゆる局面においてサーバーを保護。
- **検出:** 悪意のあるサイバー攻撃や許可されていない変更の検出。IT管理者の積極的関与。
- **リカバリー:** BIOS、ファームウェア、およびOSを既知の良好な状態にリカバリ。サーバを安全に廃棄または転用。

本書で詳しく説明するように、Dell EMC PowerEdgeサーバーは暗号化とセキュリティに関する主要な業界標準に準拠し、新しい脆弱性の追跡と管理を行っています。

Dell EMCは、開発、調達、製造、出荷、およびサポートといったセキュリティ開発ライフサイクル プロセスのあらゆる面に、セキュリティを重要な要素として実装し、サイバーレジリエント アーキテクチャを実現しています。

2.1 セキュリティ開発ライフサイクル

サイバーレジリエント アーキテクチャを実現するためには、開発の各段階においてセキュリティの意識と規律が必要です。このプロセスはセキュリティ開発ライフサイクル（SDL）モデルと呼ばれています。このプロセスでは、セキュリティは後で考えることではなく、サーバー設計プロセス全体の必須要素です。この設計プロセスは、以下の箇条書きと図1に示すように、サーバー ライフサイクル全体にわたるセキュリティ ニーズを網羅します。

- セキュリティを重要優先事項として、機能を考案、設計、試作、実装、生産、導入、メンテナンスする
- 製品開発ライフサイクルのすべてのフェーズ中に悪意のあるコードの挿入を妨害、抵抗、阻止するようにサーバ ファームウェアを設計する
  - » 設計プロセスで脅威のモデリングと侵入テストを考慮に入れる
  - » ファームウェア開発の各段階で安全なコーディング手法を適用する
- 重要なテクノロジーについては、外部監査によって内部のSDLプロセスを補完し、ファームウェアが既知のセキュリティのベスト プラクティスに準拠するようにする
- 最新のセキュリティ評価ツールを使用して新たな潜在的な脆弱性を継続的にテストおよび評価する
- 正当な事由がある場合、推奨される修復手段を含め、重要な共通脆弱性識別子（CVE）に迅速に対処する

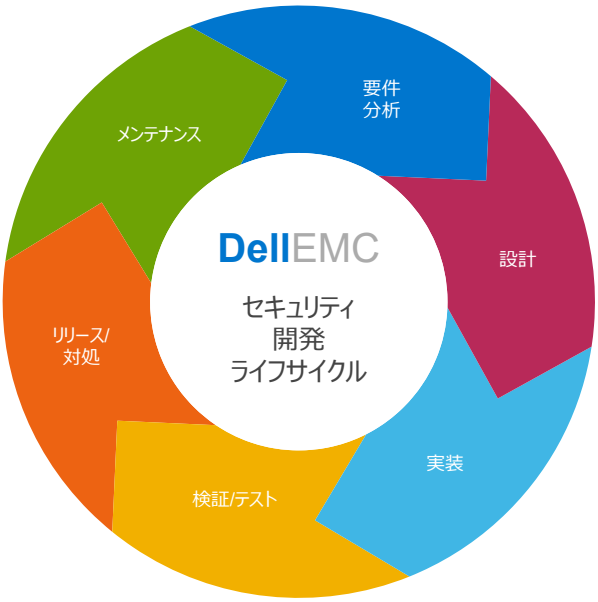


図1：Dell EMCのセキュリティ開発ライフサイクル

2.2 サイバーレジリエント アーキテクチャ

Dell EMC第14世代および第15世代PowerEdgeサーバーは、サイバー攻撃からの保護、検出、およびリカバリーのための強化されたサーバー設計を提供する、高度なサイバーレジリエント アーキテクチャを備えています。このアーキテクチャの主な特徴は、次のとおりです。

- **攻撃からの効果的な保護**
  - » シリコンベースのRoot of Trust
  - » セキュア ブート
  - » 署名されたファームウェアのアップデート
  - » 動的なSystem Lockdown
  - » ハード ドライブの暗号化とエンタープライズ キー管理
- **信頼性の高い攻撃検出**
  - » 構成およびファームウェアのドリフト検出
  - » 永続的なイベント ロギング
  - » 監査ログと警告
  - » シャーシ イントルージョン検出
- **ビジネスの中断を（ほぼ）ゼロに抑えた迅速なリカバリーを実現**
  - » BIOSの自動リカバリー
  - » 迅速なOS復旧
  - » ファームウェアのロールバック
  - » 迅速なSystem Erase

2.3 今日の脅威

変化の激しい今日の環境には、多くの脅威ベクターが存在しています。表1は、重要なバックエンドの脅威を管理するためのDell EMCのアプローチをまとめたものです。

テーブル1: Dell EMCが共通の脅威ベクターに対処する方法

サーバー プラットフォームのレイヤー		
セキュリティ レイヤー	**脅威ベクター**	**Dell EMCのソリューション**
物理サーバー	サーバー/コンポーネントの改ざん	Secured Component Verification（SCV）、シャーシ侵入検知
ファームウェアとソフトウェア	ファームウェアの破損、マルウェア インジェクション	シリコンベースのRoot of Trust、インテルBoot Guard、AMD Secure Root of Trust、UEFIセキュア ブートのカスタマイズ 暗号化形式で署名および検証されたファームウェア
	ソフトウェア	CVEレポート（必要に応じてパッチを適用）
アテステーションによる信頼機能	サーバーIDのなりすまし	TPM、TXT、信頼チェーン
サーバー管理	不正な構成とアップデート、不正なオープンポート攻撃	iDRAC9、リモート アテステーション

サーバー環境のレイヤー		
セキュリティ レイヤー	**脅威ベクター**	**Dell EMCのソリューション**
データ	データ漏洩	SED（自動暗号化ドライブ） - FIPSまたはOpal/TCG Secure Enterprise Key Management ISE（Instant Secure Erase）専用ドライブ セキュアなユーザー認証
サプライ チェーンの完全性	偽造コンポーネント マルウェアの脅威	すべてのグローバル サーバー製造拠点でISO9001認定を取得、Secured Component Verification、保持の証明 セキュリティ開発ライフサイクル（SDL）プロセスの一環として実装されたセキュリティ対策
サプライ チェーンのセキュリティ	製造拠点での物理的セキュリティ 輸送中の盗難および改ざん	Transported Asset Protection Association（TAPA）施設のセキュリティ要件 Customs-Trade Partnership Against Terrorism（C-TPAT）、SCV

3.保護

「保護」機能はNISTサイバーセキュリティ フレームワークの主要なコンポーネントであり、サイバーセキュリティ攻撃に対する防御を行います。この機能は、アクセス制御、データ セキュリティ、メンテナンス、および保護テクノロジーなどの複数のカテゴリーで構成されています。根底にあるのは、インフラストラクチャ資産は包括的でセキュアなインストールおよびコンピューティング環境の一部としてリソースおよびデータへの不正アクセスに対する強固な保護を提供しなければならない、という重要な理念です。これには、BIOSやファームウェアなどの重要なコンポーネントが不正に変更されないように保護することも含まれます。このプラットフォームは、NIST SP 800-193の現在の推奨事項を満たしています。

PowerEdgeサーバーのサイバーレジリエント アーキテクチャは、次のような高度なプラットフォーム保護機能を備えています。

- 暗号化形式で検証されたTrusted Boot
- ユーザー アクセスに関するセキュリティ
- 署名されたファームウェアのアップデート
- 暗号化されたデータ ストレージ
- 物理的セキュリティ
- サプライ チェーンの完全性とセキュリティ

3.1 暗号化形式で検証されたTrusted Boot

サーバー セキュリティの最も重要な側面の一つとして、ブート プロセスがセキュアであることを確認できることが挙げられます。このプロセスでは、OSの起動やファームウェアのアップデートなど、後続のすべての操作に対してトラスト アンカーが提供されます。PowerEdgeサーバーは複数世代にわたってシリコンベースのセキュリティを使用しており、iDRAC認証情報ヴォールトなどの機能を提供しています。これは機密データを格納するためのiDRACで暗号化された安全なメモリーです。起動プロセスはシリコンベースのRoot of Trustを使用して検証され、NIST SP 800-147B（「サーバーのBIOS保護ガイドライン」）およびNIST SP 800-155（「BIOS完全性測定ガイドライン」）に記載されている推奨事項に対応しています。

3.1.1 シリコンベースのRoot of Trust

第14世代および第15世代のPowerEdgeサーバー（インテルまたはAMDベース）は、不変のシリコンベースのRoot of Trustを使用して、BIOSおよびiDRACファームウェアの完全性を暗号化して証明するようになりました。このRoot of Trustは、マルウェアによる改ざんから保護する、1回限りのプログラム可能な読み取り専用の公開キーに基づいています。BIOS起動プロセスではインテルのBoot Guardテクノロジーまたは AMDのRoot of Trustテクノロジーを活用し、ブート イメージの暗号化ハッシュのデジタル署名がDell EMCが工場でシリコンに保存した署名と一致していることを確認します。Lifecycle Controllerログでサーバーのシャットダウンとユーザー通知の結果を確認できない場合は、ユーザーがBIOSリカバリー プロセスを開始できます。Boot Guardでの検証が正常に完了した場合、残りのBIOSモジュールが信頼チェーンの手順を使用して検証された後、制御権がOSまたはハイパーバイザーに渡されます。

iDRAC9 4.10.10.10以上には、Boot Guardの検証メカニズムに加えて、ホスト起動時にBIOSイメージを検証するためのRoot of Trustメカニズムもあります。ホストを起動できるのは、BIOSイメージの検証が正常に完了した後のみです。また、iDRAC9には、実行時、オンデマンド、またはユーザーが指定した間隔で、BIOSイメージを検証するメカニズムもあります。

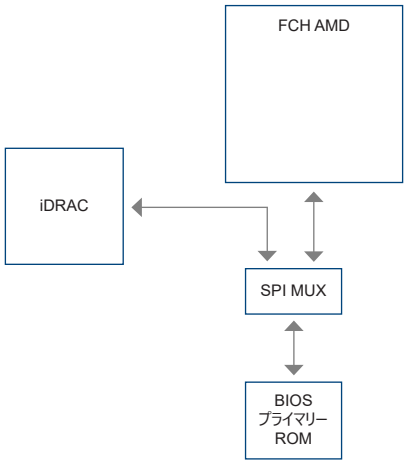
信頼チェーンについて、さらに詳しく見ていきましょう。各BIOSモジュールには、チェーン内の次のモジュールのハッシュが含まれています。BIOSの主要モジュールは、IBB（初期起動ブロック）、SEC（セキュリティ）、PEI（EFI前初期化）、MRC（メモリー参照コード）、DXE（ドライブ実行環境）、BDS（起動デバイス選択）です。インテルBoot GuardがIBB（初期起動ブロック）を認証すると、IBBはSEC+PEIを検証してから制御権を渡します。その後SEC+PEIがPEI+MRCを検証し、さらにPEI+MRCがDXE+BDSモジュールを検証します。この時点で、制御権はUEFIセキュア ブートに渡されます。これについては次のセクションで説明します。

同様に、AMD EPYCベースのDell EMC PowerEdgeサーバーでは、AMD Secure Root of Trustテクノロジーにより、信頼できるファームウェア イメージからのみサーバーが起動されます。さらに、AMD Secure Runテクノロジーは、ハードウェアにアクセスできる悪意ある侵入者から守るために、メイン メモリーを暗号化するよう設計されています。この機能を使用するためのアプリケーションの変更は必要ありません。また、セキュリティ プロセッサーによって、プロセッサー外部に暗号化キーが公開されることはありません。

iDRACはハードウェアベースのセキュリティ テクノロジーの役割も担っています。AMDのFusion Controller Hub（FCH）に加えてSPIを通じてプライマリーBIOS ROMにアクセスし、RoTプロセスを実行します。

iDRAC9は次の条件下でBIOSをリカバリーします。

1. BIOS完全性チェックに失敗した。
2. BIOSセルフ チェックに失敗した。
3. RACADMコマンド **racadm recover BIOS.Setup.1-1** を使用した。



iDRAC起動プロセスでは、固有の独立したシリコンベースのRoot of Trustを使用して、iDRACファームウェア イメージを検証します。iDRACのRoot of Trustにより、Dell EMCファームウェア アップデート パッケージ（DUP）の署名を認証するための重要なトラスト アンカーも提供されます。

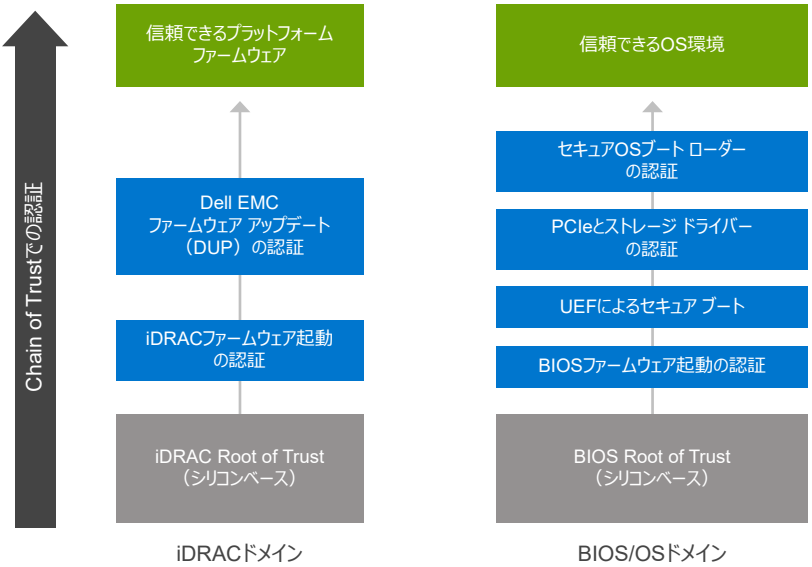


図2：PowerEdgeサーバーにおける、シリコンベースのRoot of Trustドメイン

3.1.2 BIOSライブ スキャン

BIOSライブ スキャンでは、ホストの電源がオンになっているが、POSTプロセスが開始されていない場合に、プライマリーROMのBIOSイメージの完全性と真正性が検証されます。これはAMDのみの機能であり、DatacenterライセンスがiDRAC9 4.10.10.10以上でのみ使用できます。この操作を実行するには、「Debugコマンド実行」権限を持つAdministrator権限またはオペレーター権限が必要です。iDRAC UI、RACADM、Redfishインターフェイスを通じて、スキャンをスケジュール設定できます。

3.1.3 UEFIセキュア ブートのカスタマイズ

PowerEdgeサーバーは、業界標準であるUEFI（Unified Extensible Firmware Interface）セキュア ブートもサポートしています。これにより、OSの実行前にロードされたUEFIドライバーおよびその他のコードの暗号署名がチェックされます。セキュア ブートは、起動前の環境における業界全体のセキュリティ標準を表しています。コンピューター システム ベンダー、拡張カード ベンダー、およびオペレーティング システム プロバイダーは、この仕様に基づいて協力し、相互運用性を促進しています。

UEFIセキュア ブートを有効にすると、署名されていない（つまり、信頼できない）UEFIデバイス ドライバーがロードされるのを防ぎ、エラー メッセージを表示し、デバイスが機能すること許可しません。未署名のデバイス ドライバーをロードするには、セキュア ブートを無効にする必要があります。

さらに、第14世代および第15世代のPowerEdgeサーバーには、Microsoftによって署名されていないカスタマイズされたブート ローダー証明書を使用するという独自の柔軟性があります。これは主に、自身のOSブート ローダーに署名したいと考えているLinux環境の管理者向けの機能です。お客様固有のOSブート ローダーを認証するには、推奨されているiDRAC APIを通じてカスタム証明書をアップロードできます。PowerEdgeでのこのUEFIのカスタマイズ方法は、サーバーのGrub2の脆弱性に対する緩和策として、NSAでも引用されています。

3.1.4 TPMのサポート

PowerEdgeサーバーは、次の3つのバージョンのTPMをサポートしています。

- TPM 1.2 FIPS + コモン クライテリア + TCG認定（Nuvoton）
- TPM 2.0 FIPS + コモン クライテリア + TCG認定（Nuvoton）
- TPM 2.0 China（NationZ）

TPMを使用して、公開キーの暗号化機能、コンピューティング ハッシュ機能、キーの生成、管理、および安全な保存、およびアテステーションを行うことができます。インテルのTXT（Trusted Execution Technology）機能と、Windows Server 2016でのMicrosoftプラットフォーム保証機能もサポートされています。TPMによって、Windows Server 2012/2016のBitLocker™ハード ドライブ暗号化機能を有効にすることもできます。

アテステーションおよびリモート アテステーション ソリューションでは、TPMを使用して、サーバーのハードウェア、ハイパーバイザー、BIOS、およびOSの起動時に測定を行い、TPMに保存されているベースの測定値に対して、暗号化された安全な方法で比較することができます。一致しない場合は、サーバーIDが漏洩している可能性があります。システム管理者はローカルまたはリモートでサーバーを無効にして切断できます。

サーバーの注文はTPMありでもTPMなしでも可能ですが、多くのOSやその他のセキュリティ条項ではTPMありが標準になっています。TPMの有効化はBIOSオプションを通じて行います。TPMはプラグイン モジュール ソリューションであり、このプラグイン モジュール用のコネクターがプレーナーにあります。

3.1.5 セキュリティ認定

Dell EMCは、NIST FIPS 140-2、コモン クライテリアEAL4などの標準に対する認定を受けています。これらは、米国国防総省およびその他の政府機関の要件に準拠するために重要です。PowerEdgeサーバーは、次の認定を受けています。

- サーバー プラットフォーム：RHELとともにコモン クライテリアEAL4+認定、パートナーのCC認定のサポートにも使用
- iDRACおよびCMC FIPS 140-2レベル1認定
- OpenManage Enterprise – ModularはEAL2+認定
- TPM 1.2および2.0について、FIPS 140-2およびコモン クライテリア認定

3.2 ユーザー アクセスに関するセキュリティ

適切な認証および認可を確実に行うことは、モダン アクセス制御ポリシーの重要な要件です。PowerEdgeサーバーの主なアクセス インターフェイスには、API、CLI、または組み込みのiDRACのGUIを使用します。サーバー管理の自動化のために推奨されているAPIおよびCLIは、次のとおりです。

- iDRAC Restful API with Redfish
- RACADM CLI
- SELinux

ユーザー名とパスワードのような認証情報が必要に応じてHTTPSなどの暗号化された接続を介して転送されるなど、それぞれに堅牢なセキュリティ機能があります。SSHでは、暗号化キーの一致セットを使用してユーザーを認証します（そのため、安全性の低いパスワードを入力する必要はありません）。IPMIなどの旧式のプロトコルもサポートされていますが、近年さまざまなセキュリティ問題が発覚したため、新たな導入は推奨されていません。現在、IPMIを使用している場合は、iDRAC Restful API with Redfishの評価を行って移行することをお勧めします。

TLS/SSL証明書をiDRACにアップロードし、Webブラウザー セッションを認証できます。3つのオプションがあります。

- **Dell EMCの自己署名TLS/SSL証明書 –** 証明書が自動生成され、iDRACによって自己署名されます。
  - » メリット：別の認証局を持つ必要がありません（x.509/IETF PKIX stdを参照）。
- **カスタム署名されたTLS/SSL証明書 –** 証明書が自動生成され、iDRACにすでにアップロードされている秘密キーを使用して署名されます。
  - » メリット：すべてのiDRACが単一の信頼できる認証局を使用します。社内の認証局が管理ステーションですでに信頼されている可能性があります。
- **認証局によって署名されたTLS/SSL証明書 –** 証明書署名リクエスト（CSR）が生成され、社内の認証局、またはサード パーティー認証局（VeriSign、Thawte、Go Daddyなど）によって署名されます。
  - » 長所：商用認証局を使用できます（x.509/IETF PKIX標準を参照）。すべてのiDRACが単一の信頼できる認証局を使用します。商用認証局を使用する場合、管理ステーションですでに信頼されている可能性が非常に高くなります。

iDRAC9は、PowerEdgeサーバーへのセキュアなアクセスをすでに提供しているお客様の既存の認証および承認スキーマを活用して、**Active Directory**および**LDAP**との統合を可能にします。また、**ロールベースのアクセス制御（RBAC）**によって、適切なレベルのアクセス権（管理者、オペレーター、または読み取り専用の）を付与することもできます。これはサーバー運用における個人のロールと一致している必要があります。このようにRBACを使用し、すべてのユーザーに最高レベル（管理者）を付与しないすることを強くお勧めします。

また、iDRAC9は**、IPブロッキングやフィルタリング**など、不正アクセスから保護するための追加の方法も提供します。IPブロッキングでは、特定のIPアドレスからのログイン失敗が規定回数を超えたかどうかが動的に判断され、事前に指定された期間、そのアドレスがiDRAC9にログインできないようにブロック（拒否）されます。IPフィルタリングでは、iDRACにアクセスするクライアントのIPアドレス範囲が制限されます。入ってきたログインのIPアドレスを指定された範囲にと比較し、ソースIPアドレスが範囲内にある管理ステーションからのみiDRACへのアクセスを許可します。その他のログイン リクエストはすべて拒否されます。

多要素認証（MFA）は、ユーザー名とパスワードに基づく単一要素認証スキームの脆弱性の増加に伴い、今日広く使用されています。iDRAC9ではリモートGUIアクセスにスマート カードを使用でき、RSAトークンもサポートしています。どちらの場合も、デバイスまたはカードが物理的に存在し、PINが関連付けられていることが多要素の前提となります。

3.2.1 RSA SecurID MFA

RSA SecurIDは、システム上でユーザーを認証するもう一つの手段として使用できます。iDRAC9は、もう一つの2要素認証方法として、Datacenterライセンスとファームウェア4.40.00.00を使用するRSA SecurIDのサポートを開始します。

3.2.2 簡素化された2FA

別の認証方法として、簡易な2FAがあります。iDRACへのログイン時に、ランダムに生成されたトークンをユーザーのEメールに送信します。

3.2.3 SELinuxフレームワーク

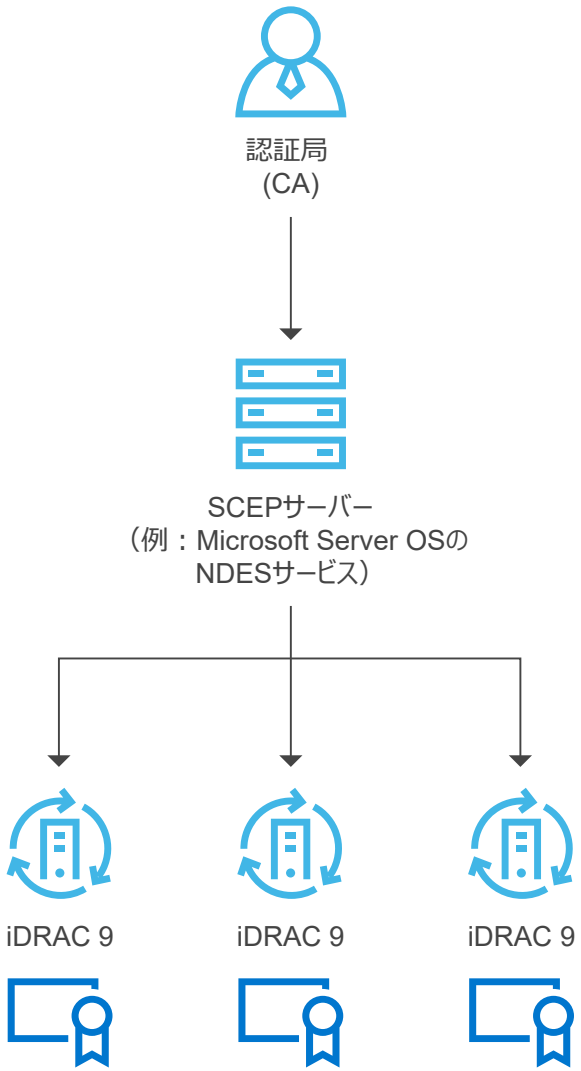
SELinuxはiDRACのコア カーネル レベルで作動し、ユーザーからの入力や設定は必要ありません。SELinuxは、攻撃が検知された時点でセキュリティ メッセージをログに記録します。これらのログ メッセージから、攻撃者がシステムに侵入しようとしたタイミングと方法が分かります。現在、この新機能の利用を登録しているお客様はSupportAssistを通じてこれらのログを利用できます。今後のiDRACのリリースでは、これらのログはLifecycle Controllerのログに記録されます。

3.2.4 必要最小限の権限

iDRAC内で実行されているすべての内部プロセスは、必要最小限の権限で実行されます。これはUnixのセキュリティの中核的な考え方です。この保護によって、攻撃を受ける可能性があるシステムのプロセスが、そのプロセスの範囲外のファイルやハードウェアにアクセスできなくなります。例えば、仮想KVMサポートを提供するプロセスは、ファン速度を変更できないようになっている必要があります。この2つのプロセスを個別の機能として実行することで、攻撃がプロセスを通じて広まらないように阻止することで、システムを保護できます。

3.2.5 証明書の自動登録および更新

iDRAC9 v4.0では、Simple Certificate Enrollment Protocol（SCEP）をサポートするクライアントを追加しました。これを使用するにはDatacenterライセンスが必要です。SCEPは、自動登録プロセスを使用して、多数のネットワーク デバイスに対して証明書を管理するために使用されるプロトコル標準です。iDRACをMicrosoft ServerNDESサービスのようなSCEP対応サーバーと統合し、SSL/TLS証明書を自動的に管理できるようになりました。この機能を使用して、期限切れの近いWebサーバー証明書を登録および更新することができます。iDRACのGUIを使用して1対1で行うことが可能で、サーバー構成プロファイルを使用して設定するか、RACADMなどのツールでスクリプトを作成します。



3.2.6 工場出荷時に生成されるデフォルト パスワード

すべての第14世代PowerEdgeサーバーは、デフォルトで工場出荷時に生成された一意のiDRACパスワードを使用して、セキュリティを強化しています。このパスワードは工場で生成され、シャーシの前面、サーバー資産ラベルの隣にある、取り外せる情報タグに記載されています。このデフォルト オプションを選択したユーザーは、汎用のデフォルト パスワードを使用するのではなく、このパスワードをメモしておき、iDRACに初めてログインするときに使用する必要があります。セキュリティのため、デフォルトのパスワードを変更することを強くお勧めします。

3.2.7 動的なSystem Lockdown

iDRAC9には、1台または複数のサーバーのハードウェアおよびファームウェア構成を「ロックダウン」する新機能が加わっています。この機能を使用するには、EnterpriseライセンスまたはDatacenterライセンスが必要です。このモードを有効にするには、GUI、RACADMなどのCLIを使用するか、サーバー構成プロファイルの一部として設定します。Administrator権限を持つユーザーは、System Lockdownモードを設定できます。これにより、権限の低いユーザーはサーバーに変更を加えることができなくなります。IT管理者はこの機能を有効/無効にすることができます。System Lockdownが無効になっているときに行われた変更は、Lifecycle Controllerのログに記録されます。ロックダウン モードを有効にすると、Dell EMCツールとエージェントを使用しているときにデータセンターの構成のドリフトを防止でき、Dell EMC Update Packagesの使用中に組み込みファームウェアへの悪意ある攻撃から保護できます。ロックダウン モードは動的に有効化でき、システムの再起動は不要です。iDRAC9 v 4.40では、Dell Update Package（DUP）を使用したアップデートのみを制御する現在のSystem Lockdownに加えて機能強化を行っています。この機能は一部のNICに拡張されています。（注：NIC向けに機能強化されたロックダウンに含まれるのは、ファームウェアのアップデートを防止するためのファームウェア ロックダウンのみです）。構成（x-UEFI）のロックダウンはサポートされていません。お客様がサポートされているインターフェイスの属性を有効化または設定してシステムをロックダウン モードにすると、iDRACはシステム構成に応じて追加のアクションを実行します。これらのアクションは、iDRAC検出プロセスの一部として検出されたサード パーティー製デバイスによって異なります。

3.2.8 ドメイン分離

第14世代および第15世代PowerEdgeサーバーは、マルチテナント ホスティング環境にとって重要な機能である**ドメイン分離**により、セキュリティを強化しています。ホスティング プロバイダーは、サーバーのハードウェア構成を保護するために、テナントによる再構成をブロックすることがあります。ドメイン分離は、ホストOSの管理アプリケーションが帯域外のiDRACまたはインテル チップセット機能（管理エンジン（ME）やイノベーション エンジン（IE）など）にアクセスできないようにする構成オプションです。

3.3 署名されたファームウェアのアップデート

PowerEdgeサーバーは、サーバー プラットフォーム上で作動しているファームウェアが正規のもののみであることを保証するために、数世代にわたってファームウェア アップデートにデジタル署名を使用してきました。iDRAC、BIOS、PERC、I/Oアダプター、LOM、PSU、ストレージ ドライブ、CPLD、およびバックプレーン コントローラーのファームウェアを含むすべての主要なサーバー コンポーネントの署名に対し、2,048ビットのRSA暗号化を使用したSHA-256ハッシュを使用して、すべてのファームウェア パッケージにデジタル署名を行っています。iDRACはファームウェア アップデートをスキャンし、シリコンベースのRoot of Trustを使用してその署名と期待される内容を比較します。検証に失敗したファームウェア パッケージはすべて中止され、ライフサイクル ログ（LCL）にエラー メッセージが記録され、IT管理者にアラートが送信されます。

強化されたファームウェア認証は、署名を検証する多くのサード パーティ デバイスに組み込まれていて、これらのデバイスは独自のルート オブ トラスト メカニズムを使用して検証を行っています。これにより、侵害されたサード パーティー製アップデート ツールを使用して、悪意あるファームウェアをNICやストレージ ドライブなどにロードすること（また、署名済みのDell EMC Update Packagesの使用を回避すること）ができなくなります。PowerEdgeサーバーに同梱されているサード パーティー製PCIeおよびストレージ デバイスの多くは、ハードウェアのRoot of Trustを使用してそれぞれのファームウェア アップデートを検証しています。

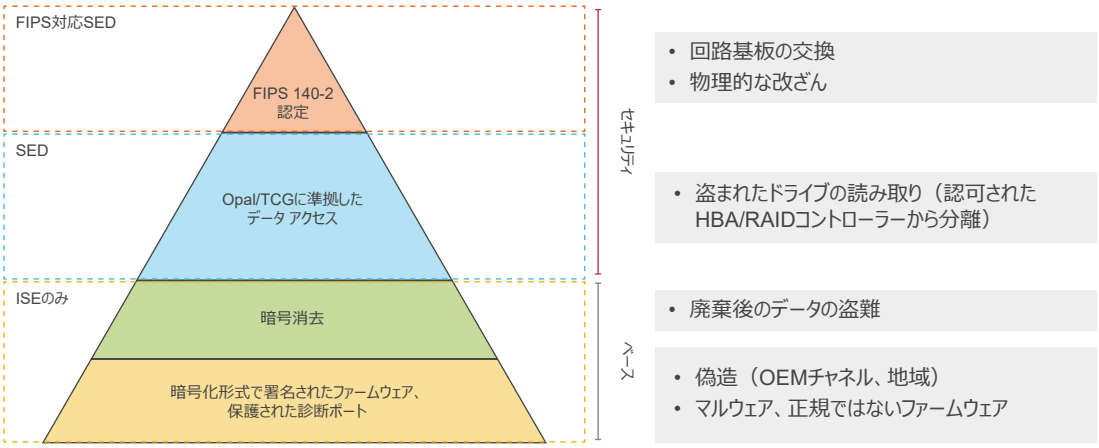
デバイスのファームウェアに悪意ある改ざんの疑いがある場合、IT管理者はプラットフォームのファームウェア イメージの多くを、iDRACに保存されている以前の信頼できるバージョンにロールバックできます。サーバーには2つのバージョンのデバイス ファームウェアがあります。既存の本稼働バージョン（「N」）と、以前の信頼できるバージョン（「N-1」）です。

3.4 暗号化されたデータ ストレージ

第14世代および第15世代PowerEdgeサーバーでは、データを保護するための複数のストレージ ドライブ オプションを用意しています。次の図に示すように、まずユーザー データを瞬時に安全に消去する新しいテクノロジー、Instant Secure Erase（ISE）をサポートするドライブがあります。第14世代および第15世代サーバーは、ISE対応ドライブをデフォルトとして提供しています。ISEについては、本書のSystem Erase機能に関する項目で詳しく説明します。

その上のセキュリティ オプションは、自動暗号化ドライブ（SED）です。ストレージ ドライブをサーバーと使用中のRAIDカードにバインドするロッキング保護機能を備えています。これによって、ドライブを壊すタイプの盗難と、その後の機密ユーザー データの喪失から保護できます。盗んだ者がドライブを使用しようとしても、必要なロッキング キーのパスフレーズが分からないため、暗号化されたドライブ データにはアクセスできません。Secured Enterprise Key Manager（SEKM）を使用すれば、サーバー全体を盗難から保護できます。これについては、この後で説明します。

一番上の保護機能は、NIST FIPS 140-2認定SEDによって提供されています。この規格に準拠したドライブは試験所で認定されており、改ざん防止ステッカーがドライブに貼付されています。Dell EMC SEDドライブは、デフォルトでFIPS 140-2認定を取得しています。



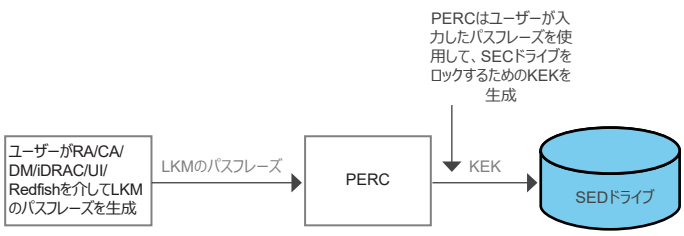
3.4.1 iDRAC認証情報ヴォールト

iDRACサービス プロセッサーは、iDRACユーザー資格情報や自己署名SSL証明書の秘密キーなどのさまざまな機密データを保護する安全なストレージ メモリーを提供します。シリコンベースのセキュリティのもう一つの例として、このメモリーは製造時に各iDRACチップにプログラムされている一意の不変のルート キーを使用して暗号化されています。これにより、攻撃者がデータにアクセスしようとしてチップを除去する物理的な攻撃から保護されます。

3.4.2 ローカル キー管理（LKM）

現在のPowerEdgeサーバーは、ローカル キー管理を使用してPERCコントローラーに接続されているSEDドライブを保護する機能を備えています。

ドライブが盗難に遭ったときにユーザー データを保護するためには、SEDを別のキーでロックする必要があります。キーが入力されないかぎり、ユーザー データを復号化することはできません。このキーを、キー暗号化キー（KEK）と呼びます。これを行うには、SEDが接続されているPERCコントローラーのkeyId/passphraseを設定します。PERCコントローラーがパスフレーズを使用してKEKを生成し、それを使用してSEDをロックします。ドライブの電源がオンになると、ロックされたSEDとして認識され、ロック解除するためのKEKを入力した場合のみ、ユーザー データの暗号化/復号化が行われます。ドライブをロック解除するためのKEKは、PERCによって提供されます。盗まれたドライブは「ロックされた状態」として認識され、攻撃者がKEKを入力できなければ、ユーザー データは保護されます。パスフレーズとKEKがPERCでローカル保存されるため、ローカルという言葉が使われています。次の図は、LKMソリューションを示しています。

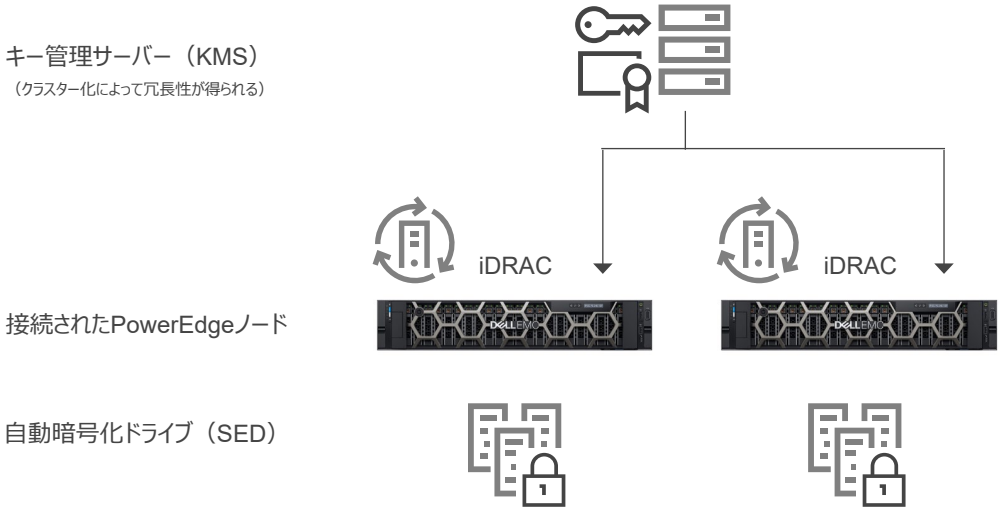


3.4.3 Secure Enterprise Key Manager（SEKM）

OpenManage SEKMは、組織全体の静止データを管理するための一元的なキー管理ソリューションを提供します。お客様は外部のキー管理サーバー（KMS）を使用して、Dell EMC PowerEdgeサーバー上のストレージ デバイスのロック/ロック解除を行うためにiDRACで使用できるキーを管理できます。iDRACは特殊ライセンスでアクティブ化された組み込みコードを使用して、各ストレージ コントローラーのキーを作成するようにKMSに要求します。iDRACはホストの起動ごとにキーを取得してストレージ コントローラーに提供し、ストレージ コントローラーが自動暗号化ドライブ（SED）をロック解除できるようにします。

ローカル キー管理（LKM）ではなくSEKMを使用するメリットは次のとおりです。

- キーがサーバーに保存されず、外部に保存されており、（iDRACを介して）接続されたPowerEdgeサーバー ノードによって取得されるため、「サーバーの盗難」から保護できる
- 高可用性を備えた暗号化デバイスで、一元的で拡張性のあるキー管理が可能
- 業界標準のKMIPプロトコルをサポートしているため、他のKMIP互換デバイスを使用できる
- ドライブまたはサーバー全体が侵害されているときに、静止データを保護できる
- ドライブ数に合わせてオンドライブ暗号化パフォーマンスを工場できる



3.5 ハードウェア セキュリティ

ハードウェア セキュリティは、包括的なセキュリティ ソリューションに不可欠な要素です。お客様によっては、USBなどの入力ポートへのアクセスを制限したいと考えることがあります。一般的に、本番環境に導入したサーバー シャーシを開く必要はありません。状況にかかわらず、少なくともこのような活動を追跡してログに記録することが望まれています。総合的な目標は、物理的な侵入を阻止し、制限することです。

3.5.1 シャーシ侵入アラート

PowerEdgeサーバーにはハードウェア侵入検出機能とログがあり、AC電源を使用できない場合でも検出が可能です。シャーシのセンサーは、誰かがシャーシを開くかまたはいじると検知します。輸送中でも同様です。輸送中にサーバが開けられると、電源が供給された後にiDRACライフサイクル ログに記録されます。

3.5.2 動的なUSBポート管理

セキュリティを強化するために、USBポートを完全に無効にすることができます。また、前面のUSBポートのみを無効にすることも可能です。例えば、本番に使用できないようUSBポートを無効にした後、デバッグ用のクラッシュ カートへのアクセス権を付与するためにそのポートを一時的に有効にすることができます。

3.5.3 iDRAC Direct

iDRAC Directは、サーバーの前面（冷気通路）からサーバーのデバッグおよび管理を行うために、iDRACサービス プロセッサーに組み込まれている特別なUSBポートです。ユーザーは標準のMicro-AB USBケーブルをこのポートに接続し、もう一方の端子（Type A）をノートパソコンに接続できます。その後、標準のWebブラウザーでiDRACのGUIにアクセスし、サーバーのさまざまなデバッグおよび管理を行うことができます。iDRAC Enterpriseライセンスがインストールされている場合、iDRACの仮想コンソール機能を使用してOSデスクトップにアクセスすることもできます。

ログインには通常のiDRAC認証情報が使用されるため、iDRAC Directはさまざまなハードウェア管理およびサービス診断というメリットが加わった安全なクラッシュ カートとして機能します。これは、リモート サイトでサーバーへの物理的アクセスを確保するための魅力的なオプションです（この場合、ホストのUSBポートとVGA出力を無効にすることができます）。

3.5.4 iDRACコネクション ビューと地理位置情報

コネクション ビューでは、iDRACでサーバーI/Oに接続されている外部スイッチおよびポートをレポートする機能が提供されます。この機能は一部のネットワーキング デバイスに搭載されています。この機能を使用するには、接続されているスイッチでLLDP（Link Layer Discovery Protocol）が有効になっている必要があります。

コネクション ビューのメリットには、次のようなものがあります。

- サーバーI/Oモジュール（LOM、NDC、およびアドインPCIeカード）が適切なスイッチおよびポートに接続されているかどうかをリモートですばやく確認できる
- 技術者が配線エラーを修復するために費用のかかるリモートディスパッチを行うことを避けられる
- サーバー ルームの暖気通路でのケーブルの追跡が不要
- GUIを使用して実行することも、RACADMコマンドを使用してすべての第14世代接続についての情報を提供することも可能

時間とコストの明らかな節約にとどまらず、物理サーバーまたは仮想マシンのリアルタイムの地理位置情報が提供されるというメリットも加わります。iDRACコネクション ビューを使用すると、管理者はサーバーを特定し、そのサーバーが接続されているスイッチおよびポートを正確に把握できます。この機能は、企業のセキュリティ ガイドラインやベスト プラクティスに準拠していないネットワークやデバイスにサーバーを接続しないようにするために役立ちます。

コネクション ビューで接続されているスイッチIDがレポートされることで、サーバーの場所が間接的に検証されます。スイッチIDによって地理位置情報を特定し、そのサーバーが無認可サイトの不正なサーバーではないことを確認できるため、物理的セキュリティ レイヤーが追加されることになります。また、アプリケーションまたはVMが国境を「越境」していないこと、また承認された安全な環境で実行されていることを確認することもできます。

3.6 サプライ チェーンの完全性とセキュリティ

サプライ チェーンの完全性については、主な課題が2つあります。

1. ハードウェアの完全性の確保：製品がお客様に向けて出荷される前に、製品の改ざんや偽造コンポーネントの挿入が行われていないことを確認すること
2. ソフトウェアの完全性の確保：製品がお客様に向けて出荷される前に、ファームウェアまたはデバイス ドライバーにマルウェアが挿入されていないことを確認するとともに、コーディングの脆弱性を防止すること

Dell EMCでは、サプライ チェーンのセキュリティとは、物理資産、在庫、情報、知的財産、および人材を保護する、予防および検出の管理策の実践および適用であると定義しています。これらのセキュリティ対策は、悪意または怠慢からマルウェアや偽造コンポーネントがサプライ チェーンに投入される機会を減らすことによって、サプライ チェーンの保証と完全性を実現するためにも役立ちます。

3.6.1 ハードウェアおよびソフトウェアの完全性

Dell EMCは、偽造コンポーネントがサプライ チェーンに入り込む機会を最小限に抑えるために、品質管理プロセスが適切に実装されていることの確認に注力しています。監査とテストによって、サプライヤーの選定、調達、生産プロセス、およびガバナンスに対応する管理策を講じています。サプライヤーの選定後、新製品導入プロセスを通じて、構築段階で使用されているすべての材料が承認されたベンダー リストから調達され、部品表と一致することを適宜確認します。生産中に材料の検査を行うことによって、マーキングミスがあったり、正常な性能パラメーターから逸脱していたり、または正しくない電子IDが含まれていたりするコンポーネントを特定できます。

可能な場合は、ODM（相手先ブランド設計製造業者）またはOCM（部品の本来の製造業者）からパーツが直接調達されます。新製品導入プロセスでの材料検査により、サプライ チェーンに入り込んだ可能性のある偽造コンポーネントまたは破損コンポーネントを特定する機会が複数回得られます。

さらに、Dell EMCはすべてのグローバル製造拠点でISO 9001認定を取得しています。これらのプロセスと管理策を厳格に遵守することで、Dell EMC製品の中に偽造コンポーネントが組み込まれるリスク、またファームウェアまたはデバイス ドライバーにマルウェアが挿入されるリスクを最小限に抑えることができます。これらの対策は、ソフトウェア開発ライフサイクル（SDL）プロセスの一部として実装されています。

3.6.2 物理的セキュリティ

Dell EMCには、製造設備および物流網のセキュリティを確立し維持するにあたり、長年にわたって実践してきた重要事項がいくつかあります。例えば、Dell EMC製品を製造する特定の工場には、Transported Asset Protection Association（TAPA）施設の特定のセキュリティ要件を満たすことを求めています。重要エリアでの有線監視カメラの使用、入出管理、入退の継続的な警備などです。また、業界をリードする物流プログラムの一部として、輸送中の盗難や改ざんから製品を保護するための保護策も講じています。このプログラムでは、継続的にスタッフが配置された指令センターを使用して、世界中で特定の貨物の出入をモニタリングし、混乱なく貨物が輸送されるようにします。

また、Dell EMCはいくつかの自発的なサプライ チェーン セキュリティ プログラムおよびイニシティチブに積極的に取り組んでいます。このようなイニシアティブの一つとして、アメリカ同時多発テロ事件の後に米国政府によって発表されたテロ防止のための税関産業界提携プログラム（C-TPAT）があります。国境とサプライ チェーンでのセキュリティ対策を強化することでテロの可能性を低減させます。このイニシアティブの一環として、米国税関・国境警備局は参加メンバーに対し、セキュリティ慣行の完全性を確保し、サプライ チェーン内のビジネス パートナーにセキュリティ ガイドラインを伝えることを求めています。Dell EMCは2002年以降、積極的な参加者として最高クラスのメンバーシップ ステータスを維持しています。

3.6.3 Dell Technologies Secured Component Verification（SCV）for PowerEdge

Dell Technologies Secured Component Verification（SCV）for PowerEdgeは、サプライ チェーン保証ソリューションです。Dell EMCのお客様は、受け取ったPowerEdgeサーバーが工場で製造されたものと一致していることを自ら確認できます。暗号化された安全な方法でコンポーネントを検証するために、工場での製造プロセス中に特定のサーバーの一意のコンポーネントIDを含む証明書が生成されます。この証明書はデル・テクノロジーズの工場で署名され、iDRACに保存されており、その後お客様がこれをSCVアプリケーションで使用します。お客様はSCVアプリケーションを使用して一意のコンポーネントIDを含む現在のシステム インベントリーを収集し、SCV証明書のインベントリーと照らし合わせて検証します。

SCVアプリケーションによって生成されたレポートで、どのコンポーネントが工場でインストールされたもの一致しているか、またどのコンポーネントが一致しないかを確認できます。また、証明書と信頼チェーン、iDRACのSCV秘密キーの保持の証明を検証します。現在の実装では直接配送のお客様をサポートしていり、VARまたはパーツ交換のシナリオは含まれていません。

4.検出

サーバー システム内の構成、稼働状態ステータス、変更イベントに対する完全な可視性を提供する検出機能を持つことは重要です。この可視性によって、起動およびOS実行時プロセスにおいて、BIOS、ファームウェア、およびオプションROMに対する悪意ある変更等を検出することも必要です。プロアクティブなポーリングと、システム内のすべてのイベントに対してアラートを送信する機能を組み合わせる必要があります。ログは、サーバーへのアクセスおよび変更に関する完全な情報を提供するものである必要があります。最も重要なのは、サーバーがこれらの機能をすべてのコンポーネントに拡張する必要がある点です。

4.1 iDRACによる包括的なモニタリング

iDRACはサーバー内の管理リソースと通信するためにOSエージェントに依存するのではなく、各デバイスへの直接側波帯パスを採用しています。Dell EMCは、PERC RAIDコントローラー、Ethernet NIC、ファイバー チャネルHBA、SAS HBA、NVMeドライブなどの周辺機器と通信するために、MCTP、NC-SI、NVMe-MIなどの業界標準プロトコルを活用してきました。このアーキテクチャは、PowerEdgeサーバーにおいてエージェント フリーのデバイス管理を実現するための、業界をリードするベンダーとの長年にわたるパートナーシップの賜物です。また、構成およびファームウェア アップデート操作では、Dell EMCとパートナー各社がサポートする強力なUEFIおよびHII機能も活用できます。

この機能により、iDRACでは、システムの構成イベント、侵入イベント（本書で前述したシャーシ侵入検出など）、および稼働状態の変化をモニタリングできます。構成イベントは、（GUIユーザー、APIユーザー、またはコンソール ユーザーを問わず）変更を開始したユーザーのIDに直接結び付けられています。

4.1.1 ライフサイクル ログ

ライフサイクル ログは、一定期間にわたってサーバーで発生したイベントを収集したものです。ライフサイクル ログには、イベントの詳細とともに、タイムスタンプ、重要度、ユーザーIDまたはソース、推奨されるアクション、追跡またはアラートのために有用なその他の技術情報が記録されています。

次に、ライフサイクル ログ（LCL）に記録されるさまざまなタイプの情報を示します。

- システム ハードウェア コンポーネントの構成変更
- iDRAC、BIOS、NIC、およびRAID構成の変更
- すべてのリモート操作のログ
- デバイス、バージョン、および日付に基づくファームウェア アップデート履歴
- 交換パーツに関する情報
- 障害が発生したパーツに関する情報
- イベントおよびエラー メッセージID
- ホストの電源関連イベント
- POSTエラー
- ユーザー ログイン イベント
- センサー状態変化イベント

4.1.2 アラート

iDRACに、さまざまなイベントのアラートや特定のライフサイクル ログ イベントが発生したときに実行されるアクションを構成する機能があります。イベントが生成されると、選択されたアラート タイプのメカニズムを使用して、設定された宛先に転送されます。iDRAC Webインターフェイス、RACADM、またはiDRAC設定ユーティリティーを通じて、アラートを有効または無効にすることができます。

iDRACでは、次のようなさまざまなタイプのアラートがサポートされています。

- メールまたはIPMIアラート
- SNMPトラップ
- OSとリモート システム ログ
- Redfishイベント

アラートを重要度（重大、警告、または情報）で分類することもできます。

アラートに適用できるフィルターは次のとおりです。

- システムの稼働状態（温度、電圧、デバイスのエラーなど）
- ストレージの稼働状態（コントローラーのエラー、物理ディスクまたは仮想ディスクのエラーなど）
- 構成の変更（RAID構成の変更、PCIeカードの取り外しなど）
- 監査ログ（パスワード認証の失敗など）
- ファームウェア/ドライバー（アップグレードまたはダウングレードなど）

最後に、IT管理者はアラートに対するさまざまなアクション（再起動、電源サイクル、電源オフ、またはアクションなし）を設定できます。

4.2 ドリフト検出

標準化された構成を適用し、変更に対する「ゼロ トレランス」ポリシーを採用することによって、悪用の可能性を減らすことができます。Dell EMC OpenManage Enterpriseコンソールを使用すると、お客様独自のサーバー構成ベースラインを定義し、そのベースラインを基準として本番サーバーのドリフトをモニタリングできます。ベースラインは、セキュリティやパフォーマンスなど、さまざまな本番稼働の実施状況に適合するように、さまざまな基準に基づいて構築できます。OpenManage Enterpriseでは、ベースラインからの逸脱をレポートできます。また、シンプルなワークフローでドリフトを修復して、iDRAC帯域外の変更をステージングすることもできます。次のメンテナンス期間のサーバーの再起動時に変更が実行されるので、本番環境でのコンプライアンスを再度確認することができます。この段階的なプロセスによって、メンテナンス時間帯以外にダウンタイムを発生させることなく、本番環境に構成変更を導入できます。保守性やセキュリティを損なうことなく、サーバーの可用性が向上します。

5.リカバリー

サーバー ソリューションは、次のようなさまざまなイベントに対する対処として、既知の整合性のとれた状態へのリカバリーを支援するものである必要があります。

- 新たに検出された脆弱性
- 悪意ある攻撃やデータの改ざん
- メモリー障害または不適切なアップデート手順によるファームウェアの破損
- サーバー コンポーネントの交換
- サーバーの廃棄または転用

次に、新たな脆弱性および破損の問題への対処方法、また必要に応じてサーバーを元の状態に戻す方法について詳しく説明します。

5.1 新たな脆弱性に対する迅速な対処

共通脆弱性識別子（CVE）は、ソフトウェアおよびハードウェア製品を侵害するものとして新たに検出された攻撃ベクターです。ほとんどの企業にとって、CVEへのタイムリーな対処応は、迅速にエクスポージャーを評価し、適切な措置を取るために不可欠です。

CVEは、次のような多くの項目で特定された新たな脆弱性に対して発行されます。

- OpenSSLなどのオープン ソース コード
- Webブラウザーおよびその他のインターネット アクセス ソフトウェア
- ベンダー製品のハードウェアおよびファームウェア
- オペレーティングシステムおよびハイパーバイザ

Dell EMCは、PowerEdgeサーバーにおいて新しいCVEに迅速に対処し、お客様に次の情報をタイムリーに提供するために積極的に取り組んでいます。

- 影響を受ける製品
- 取り得る修復手順
- 必要に応じて、CVEに対処するためのアップデートが提供されます。

5.2 BIOSおよびOSのリカバリー

Dell EMCの第14世代および第15世代PowerEdgeサーバーには、次の2種類のリカバリーがあります。BIOSリカバリ-と迅速なオペレーティング システム（OS）リカバリーです。これらの機能を使用すると、破損したBIOSイメージまたはOSイメージから迅速にリカバリできます。どちらの場合も、特殊なストレージ領域がランタイム ソフトウェア（BIOS、OS、デバイス ファームウェアなど）に認識されません。これらのストレージ領域には、元のイメージが含まれており、侵害されたプライマリ ソフトウェアの代わりとして使用できます。

OSの迅速なリカバリーによって、破損したOSイメージ（または悪意ある改ざんの疑いがあるOSイメージ）から迅速にリカバリーできます。リカバリー メディアとして、内蔵SDカード、SATAポート、M.2ドライブ、または内蔵USBを使用できます。リカバリー イメージのインストールのために、選択したデバイスをブート リストおよびOSに対して開示することができます。その後、無効にすると、ブート リストおよびOSに対して非開示になります。非開示の状態では、BIOSによってデバイスが無効にされ、OSからアクセスできなくなります。OSイメージが破損した場合は、起動のためにリカバリー場所を有効にすることができます。これらの設定には、BIOSまたはiDRACインターフェイスを通じてアクセスできます。

極端なケースでは、BIOSが破損している場合（悪意ある攻撃、アップデート プロセス中の電源喪失、または不測の事態の発生など）、BIOSを元の状態に戻す方法を確保することが重要です。バックアップBIOSイメージはiDRACに保存されており、BIOSイメージをリカバリーするために必要に応じて使用できます。iDRACが、エンドツーエンドのリカバリー プロセス全体をオーケストレーションします。

- BIOSの自動リカバリーは、BIOSそのものによって開始されます。
- BIOSのオンデマンド リカバリーは、ユーザーがRACADM CLIコマンドを使用して開始できます。

5.3 ファームウェアのロールバック

ファームウェアを最新の状態に保ち、最新の機能およびセキュリティ アップデートを確実に使用できるようにすることをお勧めします。ただし、アップデート後に問題が発生した場合は、アップデートのロールバックや、前のバージョンのインストールが必要になることがあります。前のバージョンにロールバックすると、署名に対する検証も実行されます。

既存の本番バージョン「N」から前のバージョン「N-1」へのファームウェアのロールバックは現在、次のファームウェア イメージでサポートされています。

- BIOS
- iDRAC with Lifecycle Controller
- ネットワークインターフェイスカード（NIC）
- PowerEdge RAIDコントローラ（PERC）
- 電源ユニット（PSU）
- バックプレーン

次のいずれかの方法で、以前にインストールしたバージョン（「N-1」）にファームウェアをロールバックできます。

- iDRAC Webインターフェイス
- CMC Webインターフェイス
- RACADM CLI - iDRACおよびCMC
- Lifecycle ControllerのGUI
- Lifecycle Controller - リモート サービス

以前に別のインターフェイスを使用してアップグレードを実行した場合も、iDRACまたはLifecycle Controllerでサポートされている任意のデバイスのファームウェアをロールバックできます。例えば、Lifecycle ControllerのGUIでファームウェアをアップグレードした場合、iDRAC Webインターフェイスでファームウェアをロールバックすることが可能です。1回のシステム再起動で、複数のデバイスに対してファームウェアロールバックを実行できます。

1台のiDRACおよびLifecycle Controllerのファームウェアを搭載した第14世代および第15世代PowerEdgeサーバーでは、iDRACファームウェアをロールバックすることで、Lifecycle Controllerのファームウェアもロールバックされます。

5.4 ハードウェア修理後のサーバー構成のリストア

修復サービス イベントは、IT運用の重要な部分です。目標リカバリー時間と目標リカバリー ポイントを達成する能力は、ソリューションのセキュリティに直接的な影響を及ぼします。サーバー構成とファームウェアをリストアすることで、サーバー運用のセキュリティ ポリシーが自動的に遵守されます。

PowerEdgeサーバーには、次のような状況で、サーバー構成を迅速にリストアする機能があります。

- 個々のパーツの交換
- マザーボードの交換（サーバー プロファイルのフル バックアップおよびリストア）
- マザーボードの交換（Easy Restore）

5.4.1 パーツ交換

iDRACにより、NICカード、RAIDコントローラー、および電源供給ユニット（PSU）のファームウェア イメージおよび構成設定が自動的に保存されます。これらのパーツをフィールド交換した場合、iDRACによって新しいカードが自動的に検出され、ファームウェアおよび構成が交換済みのカードにリストアされます。この機能により、貴重な時間を節約し、構成およびセキュリティ ポリシーの一貫性を確保することができます。サポート対象パーツを交換した後、システムの再起動時にアップデートが自動的に実行されます。

5.4.2 Easy Restore（マザーボード交換時）

マザーボードの交換には時間がかかるため、生産性に影響する可能性があります。iDRACは、PowerEdgeサーバーの構成とファームウェアのバックアップとリストアを行い、障害が発生したマザーボードの交換に必要な労力を最小限に抑える機能を提供します。

PowerEdgeサーバーのバックアップおよびリストアには、次の2つの方法があります。

1. PowerEdgeサーバーによって、システム構成設定（BIOS、iDRAC、NIC）、サービス タグ、UEFI診断アプリケーション、およびその他のライセンス データがフラッシュ メモリーに自動的にバックアップされます。

   サーバーのマザーボードを交換した後、Easy Restoreにより、このデータを自動的にリストアするように求められます。

2. より包括的なバックアップのためには、BIOS、RAID、NIC、iDRAC、Lifecycle Controller、ネットワーク ドーターカード（NDC）などのさまざまなコンポーネントにインストールされているファームウェア イメージと、それらのコンポーネントの構成設定などを含めて、システム構成をバックアップできます。バックアップ オペレーションには、ハード ディスク構成データ、マザーボード、および交換パーツも含まれます。バックアップで作成される単一ファイルは、vFlash SDカードまたはネットワーク共有（CIFS、NFS、HTTP、またはHTTPS）に保存可能です。

   このプロファイル バックアップは、ユーザーがいつでもリストアできます。リストアが必要と思われるすべてのシステム プロファイルについて、ある時点でバックアップ オペレーションを実行することをお勧めします。

5.5 System Erase

ライフサイクルが終了したシステムは、廃棄するか、再利用する必要があります。System Eraseの目的は、機密情報が誤って漏洩することがないように、サーバーのストレージ デバイスと、キャッシュやログなどのサーバー不揮発性ストアから機密データおよび設定を消去することです。これは、Lifecycle Controllerに含まれるユーティリティーであり、ログ、構成データ、ストレージ データ、キャッシュ、あらゆる埋め込み型アプリケーションを消去するように設計されています。

System Erase機能を使用して、次のデバイス、構成設定、アプリケーションを消去できます。

- iDRACはデフォルトにリセットされる
- Lifecycle Controller（LC）のデータ
- BIOS
- 埋め込み型の診断およびOSドライバー パック
- iSM
- SupportAssistコレクション レポート

さらに、次のコンポーネントも消去できます。

- ハードウェア キャッシュ（PERC NVCacheのクリアー）
- vFlash SDカード（初期化カード）（注：vFlashは第15世代以降のサーバーでは使用できません）

次のコンポーネントのデータは、この後で説明するようにSystem Eraseによって暗号化形式で破棄されます。

- SED（自動暗号化ドライブ）
- ISE専用ドライブ（Instant Secure Eraseドライブ）
- NVMデバイス（Apache Pass、NVDIMM）

さらに、データ上書きを使用して、ISE以外のSATAハード ドライブを消去することもできます。

Instant Secure Erase（ISE）では、第14世代および第15世代ドライブで使用されている内部暗号化キーが破壊されるため、ユーザー データをリカバリーすることはできません。ISEは、NIST Special Publication 800-88「媒体のサニタイズに関するガイドライン」に記載されているストレージ ドライブでのデータ消去方法として認められています。

System Eraseを備えた新しいISE機能には、次のメリットがあります。

- **スピード：**DoD 5220.22-Mのようなデータ上書き手法と比べてもはるかに高速（数時間ではなく数秒）
- **有効性：**ISEではドライブ上のすべてのデータ（予約済みブロックを含む）が完全に読み取り不能に
- **TCOの向上：**ストレージ デバイスを物理的に破壊（分解など）せず、再利用することが可能

System Eraseを実行するには、次の方法があります。

- Lifecycle Controller GUI（F10）
- RACADM CLI
- Redfish

5.6 iDRAC9 Cipher Select

Cipher Suite Selectionを使用して、WebブラウザーがiDRACと通信する際に使用できる暗号化方式を制限することが可能です。また、接続の安全度も決定できます。これらの設定は、iDRAC Webインターフェイス、RACADM、およびRedfishを通じて構成できます。この機能はiDRACの複数のリリース（iDRAC7、iDRAC8（2.60.60.60以上）、および現在のiDRAC9（3.30.30.30以上））で使用できます。

5.7 CNSAのサポート

TLS 1.2 256ビット暗号化を使用するiDRAC9でサポートされている暗号化方式は、下のスクリーンショット画像のとおりです。使用可能な暗号化方式には、CNSA承認済みセットの暗号化方式が含まれています。

5.8 フル パワー サイクル

フル パワー サイクルでは、サーバーとそのすべてのコンポーネントが再起動されます。サーバーとすべてのコンポーネントのメイン電源と補助電源が使用されます。揮発性メモリー内のすべてのデータも消去されます。

物理的なフル パワー サイクルを発生させるには、AC電源ケーブルを取り外し、30秒間待機してからケーブルを戻す必要があります。これは、リモート システムを使用している場合に課題となります。第14世代および第15世代サーバーの新機能を使用すると、iSM、iDRACのGUI、BIOS、またはスクリプトから、効果的なフル パワー サイクルを実行できます。次の電源サイクルでフル パワー サイクルが有効になります。

フル パワー サイクル機能により、データ センターにスタッフが物理的に存在する必要がなくなり、トラブルシューティングのための時間を短縮できます。例えば、メモリー常駐型のマルウェアを排除することが可能です。

6.まとめ

データ センターのセキュリティはビジネスの成功にとって不可欠です。また、基盤となるサーバー インフラストラクチャのセキュリティは重大事です。サイバー攻撃は、拡張システムおよびビジネスのダウンタイム、利益とお客様の損失、法的損害や企業の評判低下を招く可能性があります。ハードウェアを標的としたサイバー攻撃からの保護、検出、回復を行うには、事後に追加するのではなく、サーバー ハードウェアの設計にセキュリティを組み込む必要があります。

Dell EMCは、2世代にわたってシリコンベースのセキュリティを活用することで、ファームウェアの保護、そしてPowerEdgeサーバーの機密ユーザー データの保護をリードしてきました。第14世代および第15世代PowerEdge製品ラインは、強化されたサイバーレジリエント アーキテクチャを採用しており、シリコンベースのRoot of Trustを使用して、次のようなサーバー セキュリティ機能をさらに強化しています。

- **暗号化形式で検証されたTrusted Boot**：エンドツーエンドのサーバー セキュリティと、データ センター全体のセキュリティを強化します。これには、シリコンベースのRoot of Trust、デジタル署名されたファームウェア、およびBIOSの自動リカバリーなどの機能が含まれます。
- **セキュア ブート**：OSの実行前にロードされたUEFIドライバーおよびその他のコードの暗号署名をチェックします。
- **iDRAC認証情報ヴォールト：**認証情報、証明書、および各サーバーに一意のシリコンベースのキーで暗号化されている他の機密データのための安全なストレージ領域です。
- **動的なSystem Lockdown**：悪意ある、または意図しない変更からシステム構成およびファームウェアを保護し、試みられたシステムの変更についてのアラートをユーザーに送信する、PowerEdge固有の機能です。
- **Enterprise Key Management**：組織全体の静止データを管理するための一元的なキー管理ソリューションを提供します。
- **System Erase**：ストレージ ドライブやその他の組み込みの不揮発性メモリーからデータが安全かつ迅速に消去されることで、第14世代および第15世代PowerEdgeサーバーを簡単に廃棄または転用できます。
- **サプライ チェーンのセキュリティ**：製品がお客様に向けて出荷される前に、製品の改ざんや偽造コンポーネントがないことを確認することで、サプライ チェーンの保証を提供します。

このように第14世代および第15世代PowerEdgeサーバーは業界をリードするセキュリティ機能を備えており、ITトランスフォーメーションのための信頼できる基盤を構築し、お客様がITオペレーションおよびワークロードを安全に実行できるようにします。

A. 付録：詳細情報

セキュリティ ホワイト ペーパーおよび資料

- （開発から直接）PowerEdgeサーバーでのSystem Erase
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242
- 第14世代Dell EMC PowerEdgeサーバーとSystem Erase
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- （開発から直接）サーバー設計におけるセキュリティ
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243
- （開発から直接）サイバーレジリエンシーはチップセットとBIOSから
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- 工場出荷時に生成されるデフォルトのiDRAC9パスワード
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368
- Dell EMC iDRACでのCVE-2017-1000251「BLUEBORNE」への対応
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605
- （ビデオ）RACADMを使用したセキュア ブート構成および証明書管理
  https://youtu.be/mrIIN4X380c
- Dell EMC PowerEdgeサーバーでのセキュア ブート管理
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- 第14世代および第15世代以降のDell EMC PowerEdgeサーバーでセキュア ブート機能を使用するためのUEFIイメージへの署名
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255
- オペレーティング システムの迅速なリカバリー
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- 第14世代（14G）Dell EMC PowerEdgeサーバーでのiDRAC9イベント アラートの管理
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266
- UEFIセキュア ブートのカスタマイズ
  https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

PowerEdgeホワイト ペーパー

- iDRACの概要
  http://www.DellTechCenter.com/iDRAC
- OpenManageコンソールの概要
  http://www.DellTechCenter.com/OME
- OpenManage Mobileの概要
  http://www.DellTechCenter.com/OMM
- Lifecycle Controllerのパーツ交換
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- マザーボードの交換
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- iDRAC証明書の自動登録
  https://www.dellemc.com/resources/en-us/asset/white-papers/products/software/direct-from-development-idrac-automatic-certificate-enrollment.pdf
- SELinuxを使用したiDRAC9のサーバー セキュリティ機能の強化
  https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_en-us.pdf
- iDRAC9 Cipher Select - Dell EMC PowerEdgeサーバーでのセキュリティ強化
  https://downloads.dell.com/manuals/all-products/esuprt_software_int/esuprt_software_ent_systems_mgmt/idrac9-lifecycle-controller-v33-series_white-papers11_en-us.pdf

PowerEdgeサーバーをもっと詳しく知る

PowerEdgeサーバーの詳細はこちら

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

DELL Technologies