テクニカル ホワイト ペーパー:
第14世代Dell EMC PowerEdgeサーバのサイバー レジリエント セキュリティ

Dell EMC サーバのソリューション

2018 年 1 月

Dell EMC テクニカル ホワイト ペーパー

リビジョン

日付	説明
2018 年 1 月	初期リリース

目次

1 はじめに

経済雑誌エコノミストの最近の記事によると「世界で最も重要なリソースはもはや石油ではない。データである」とのことです。[1]あらゆる規模の組織がこの主張に同意するでしょう。データは多くの組織にとって最も重要な資産になりました。データの保護とこれをサポートする基盤 IT インフラストラクチャは、CIO、CISO、IT マネージャ、データセンター マネージャらにとって主要な心配の種です。高度なマルウェアがさらに複雑化し、その量が増大していることによって、IT インフラストラクチャの保護も複雑化しています。2016 年だけで 3 億 5700 万の新しいマルウェア亜種が検出されました。わずか 2 年間で 8200 万の増加です。[2]

ただし、今日のサイバーセキュリティの関心事のほとんどは、OS およびアプリケーションを悪意のある攻撃から保護することです。基盤となるサーバ インフラストラクチャ（ハードウェア、ファームウェアを含む）のセキュリティには、時折わずかな注意が振り向けられる程度です。サーバ インフラストラクチャがデータセンター セキュリティの鍵です。ファームウェアをターゲットとするサイバー攻撃は長く続き、目に付きにくいからです。2017 年、McAfee Labs は「高度な攻撃者は自分たちが悪用できるハードウェアおよびファームウェアの脆弱性を探し続ける[3]」と予言しています。しかし、非営利 IT 監査組織である ISACA によると、セキュリティに優先的に取り組んでいる企業の 50%以上が依然としてマルウェアに感染しています。また、17%がそのインシデントによって重大な影響を被ったと明かしました。[4]

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の重要度が増すと、サーバのセキュリティが企業のセキュリティ全体の基礎になります。サーバは、ハードウェア レベルとファームウェア レベルの両方でセキュリティを重視する必要があります。そのために、サーバ内で次の操作を確認するために使用できる不変のルート オブ トラストを利用します。これは、サーバのライフサイクル全体（導入、メンテナンス、廃棄）にわたる信頼チェーンを確立します。

第 14 世代の PowerEdge サーバはこの信頼チェーンを提供し、包括的な管理ツールと組み合わせて、ハードウェアとファームウェアに堅牢なセキュリティ レイヤーを提供します。その結果として得られるものは、組み込みのサーバ ファームウェア、システムに保管されるデータ、オペレーティング システム、周辺機器、および内部での管理操作など、サーバのあらゆる側面にわたる**サイバー レジリエント アーキテクチャ**です。組織は、貴重なサーバ インフラストラクチャおよびその中のデータを保護し、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リカバリするプロセスを構築できます。このペーパーでは、第 14 世代 Dell EMC PowerEdge サーバのライフサイクル全体にわたって提供されるセキュリティ機能を詳細に説明します。

---

[1] https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource（2017 年 5 月）
[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf（インターネット セキュリティ脅威レポート、ボリューム 22、2017 年 4 月）
[3] https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf（2016 年 11 月）
[4] https://www.isaca.org/About-ISACA/Press-room/News-Releases/2016/Pages/ISACA-Firmware-Security-Research-Highlights-Shortcomings-Vulnerabilities.aspx（2016 年 10 月）

2 安全なサーバ インフラストラクチャへの道

Dell EMC PowerEdge サーバは、シリコン ベースのデータ セキュリティを使用した革新性など堅牢なセキュリティを数世代にわたって提供しています。第 14 世代では、シリコン ベースのセキュリティを拡張し、サーバのブートプロセス中に暗号化形式のルート オブ トラストで BIOS およびファームウェアを認証します。Dell EMC 製品チームは、現代の IT 環境で直面するセキュリティ脅威に対応して、第 14 世代 PowerEdge サーバの設計中に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、および物理ハードウェアを含む、ライフサイクルのあらゆる側面でのサーバの保護。
- **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**: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。

Dell EMC PowerEdge サーバは、このペーパーを通じて詳しく説明するように、暗号化およびセキュリティに関して主要な業界標準に準拠し、新たな脆弱性を継続的に追跡し、管理します。

Dell EMC は、開発、調達、製造、輸送、およびサポートの各側面の重要な要素として *セキュリティ開発ライフサイクル* プロセスを導入しました。その結果、第 14 世代サーバでは *サイバー レジリエント アーキテクチャ*を実現しました。

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 アーキテクチャを提供するには、開発の各段階でセキュリティ意識向上と規律が必要です。このプロセスは SDL(セキュリティ開発ライフサイクル)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、以下に箇条書きし、図 1 に示すように、サーバのライフサイクル全体にわたってセキュリティ ニーズのビューを網羅します。

- セキュリティを優先して機能を考案、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、および阻止するようにサーバ ファームウェアを設計する
  - 設計プロセスは脅威モデリングと侵入テストの対象
  - ファームウェア開発の各段階で安全なコーディング方法を適用
- 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 プロセスを補い、ファームウェアを既知のセキュリティ ベスト プラクティスに確実に準拠する
- 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

- 重要な CVE（共通脆弱性識別子）に対する迅速な対応（保証されている場合には推奨される改善対策を含む）

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

第 14 世代 Dell EMC PowerEdge サーバは、機能強化したサイバー レジリエント アーキテクチャを採用し、サイバー攻撃からの保護、検出、復旧のためにサーバ設計を強化しています。このアーキテクチャの特徴の一部を次に示します。

- 攻撃からの効果的な保護
  - シリコン ベースのルート オブ トラスト
  - 署名されたファームウェアの更新
  - システム ロックダウン
- 攻撃の信頼できる検出
  - 構成とファームウェアのドリフト検出
  - 永続的なイベント ログ
  - セキュリティ アラート
- ほとんどビジネスを中断することなく高速リカバリ
  - 自動 BIOS リカバリ
  - 迅速な OS 復旧
  - ファームウェア ロールバック

2.3 今日の脅威

今日の変化するランドス ケープには多くの脅威ベクトルが存在しています。表 1 には、重大バックエンド脅威を管理する Dell EMC のアプローチがまとめられています。

表 1. 一般的な脅威ベクトルに対する Dell EMC の対処方法

サーバ プラットフォーム レイヤー		
セキュリティ レイヤー	**脅威ベクトル**	**Dell EMC のソリューション**
物理サーバ	サーバの改ざん	物理的防止策
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 ベースのルート オブ トラスト、Intel Boot Guard、AMD の安全なルート オブ トラスト 暗号化形式を用いて署名され検証されたファームウェア
	ソフトウェア	必要に応じてパッチ適用
認証信頼機能	サーバ ID のスプーフィング	TPM、TXT、信頼チェーン
サーバー管理	不正な構成と更新、不正なオープン ポート攻撃	iDRAC9

サーバ環境レイヤー		
セキュリティ レイヤー	**脅威ベクトル**	**Dell EMC のソリューション**
データ	データ侵害	SED（自己暗号化ドライブ）–FIPS または Opal/TCG ISE のみ（迅速かつセキュアな消去）ドライブ 安全な鍵管理 セキュアなユーザー認証
サプライ チェーンの整合性	偽のコンポーネント マルウェアの脅威	すべてのグローバル サーバ製造サイトが ISO9001 認定 SDL（安全な開発ライフサイクル）プロセスの一部としてセキュリティ対策を実装
サプライ チェーンのセキュリティ	製造サイトの物理的セキュリティ 輸送中の盗難や改ざん	TAPA（Transported Asset Protection Association：輸送中資産保護協会）の施設セキュリティ要件 C-TPAT（Customs-Trade Partnership Against Terrorism：テロ行為防止のための税関産業界提携）

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、サイバー セキュリティ攻撃対策に使用できます。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、保護テクノロジーを含むいくつかのカテゴリーで構成されます。基盤となる重要な理念は、インフラストラクチャ資産には、包括的かつ安全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堅牢な保護が用意されている必要があるということです。これには、BIOS、ファームウェアなどの重要なコンポーネントの不正な変更からの保護が含まれます。このプラットフォームは、NIST SP 800-193（Draft Platform Firmware Resiliency Guidelines：プラットフォーム ファームウェア復元性ガイドラインの草案）の現行の推奨事項を満たしています。

PowerEdge サーバの**サイバー レジリエント アーキテクチャ**は、以下の機能を含む高度なプラットフォーム保護を提供します。

- 暗号化形式を用いて検証された信頼性の高いブート
- ユーザー アクセスのセキュリティ
- 署名されたファームウェアの更新
- 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 チェーンの整合性とセキュリティ

3.1 暗号化形式を用いて検証された信頼性の高いブート

サーバ セキュリティの最も重要な側面の 1 つは、ブート プロセスが安全であることを検証できるようにすることです。このプロセスは、OS のブートやファームウェアの更新などの後続のすべての操作に、信頼できる基盤をもたらします。PowerEdge サーバは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います。これは、機密データを格納する iDRAC の暗号化された安全なメモリである iDRAC 認証情報ヴォールトなどの機能を実現するためのものです。ブート プロセスは、NIST SP 800-147B（BIOS Protection Guidelines for Servers：サーバの BIOS を保護するためのガイドライン）および NIST SP 800-155（BIOS Integrity Measurement Guideline：BIOS 整合性測定ガイドライン）の推奨事項を満たすようにシリコン ベースのルート オブ トラストを使用して検証されます。

3.1.1 シリコン ベースのルート オブ トラスト

現在、第 14 世代 PowerEdge サーバ（Intel ベースと AMD ベースの両方）は、不変のシリコン ベースのルート オブ トラストを使用して、BIOS および iDRAC ファームウェアの整合性を暗号化形式を用いて証明しています。このルート オブ トラストは、マルウェアによる改ざんに対する保護を提供する、1 回限りプログラム可能な、読み取り専用公開キーに基づいています。BIOS のブート プロセスは、Intel Boot Guard テクノロジーまたは AMD のルート オブ トラスト テクノロジーを利用しています。これらのテクノロジーは、ブート イメージの暗号ハッシュのデジタル署名が工場で Dell EMC によってシリコンに格納された署名と一致するかどうかを検証します。検証に失敗すると、サーバがシャットダウンし、ライフサイクル コントローラー ログでユーザに通知されます。その後ユーザは BIOS のリカバリ プロセスを開始できます。Boot Guard による検証に成功すると、残りの BIOS モジュールは信頼チェーンの手順を使用して検証され、その後 OS またはハイパーバイザーに制御が引き渡されます。

さらに詳しく信頼チェーンを見てみましょう。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 の主要なモジュールは、IBB（Initial Boot Block）、SEC（セキュリティ）、PEI（Pre-EFI Initialization）、MRC（Memory Reference Code）、DXE（Driver Execution Environment）、および BDS（Boot

Device Selection）です。Intel Boot Guard が IBB（Initial Boot Block）を認証すると、次に IBB が SEC+PEI を認証し、その後制御をこのモジュールに渡します。次に SEC+PEI は 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。この時点で制御が UEFI セキュア ブートに渡されます（次のセクションで説明します）。

同様に、AMD のルート オブ トラスト テクノロジーである AMD EPYC に基づく Dell EMC PowerEdge サーバでは、サーバは信頼できるファームウェア イメージからのみブートすることが保証されています。また、AMD Secure Run テクノロジーは、メイン メモリを暗号化してプライベートに保ち、悪意のある侵入者がハードウェアにアクセスできないように設計されています。この機能を使用するためにアプリケーションを変更する必要はありません。また、セキュリティ プロセッサーが暗号化キーをプロセッサーの外部に公開することは決してありません。

IDRAC ブート プロセスは、iDRAC ファームウェア イメージを検証する独自のシリコン ベースのルート オブ トラストを使用します。IDRAC のルート オブ トラストは、Dell EMC ファームウェア更新パッケージ（DUP）の署名を認証するための重要な信頼基盤も提供します。

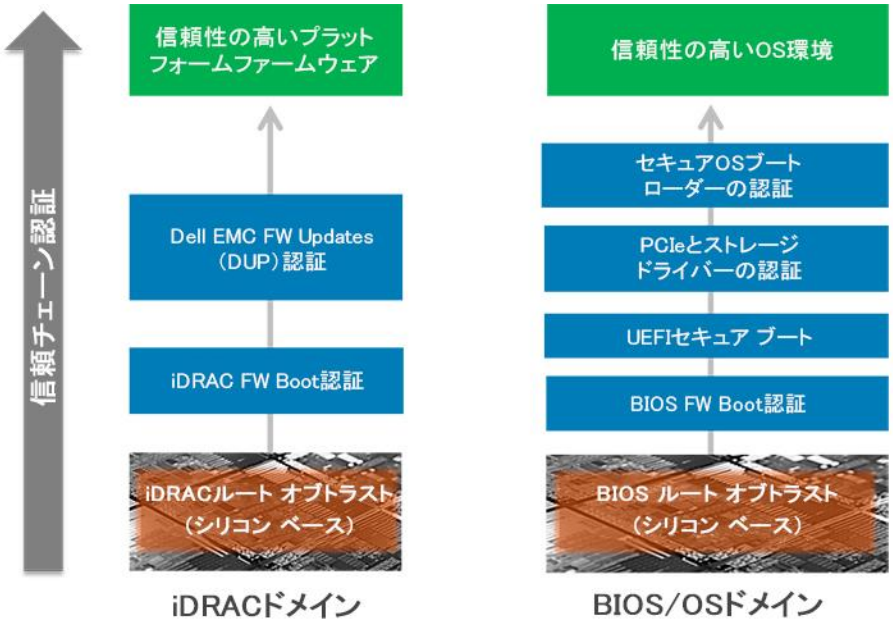


図 2　第 14 世代 PowerEdge サーバのシリコン ベースのルート オブ トラスト ドメイン

3.1.2 UEFI セキュア ブートのサポート

PowerEdge サーバでは業界標準の UEFI セキュア ブートもサポートしています。これは OS の実行前にロードされる UEFI ドライバと他のコードの暗号署名を確認するものです。セキュア ブートは、ブート前環境のセキュリティの業界標準を表します。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、この仕様を共同作成して相互運用性を高めています。

UEFI セキュア ブートを有効にすると、署名のない（つまり信頼できない）UEFI デバイス ドライバのロードが阻止され、エラー メッセージが表示され、そのデバイスは動作しません。署名のないデバイス ドライバをロードするには、セキュア ブートを無効にする必要があります。

また、第 14 世代 PowerEdge サーバでは、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できるというユニークな柔軟性が与えられます。これは主に、独自の OS ブート ローダーを署名したい Linux 環境の管理者用の機能です。カスタム証明書は、お客様固有の OS ブート ローダーを認証するために推奨の iDRAC API 経由でアップロードできます。

3.1.3 TPM サポート

PowerEdge サーバは、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 中国（NationZ）

TPM は、公開キーの暗号形式機能の実行、ハッシュ関数の計算、キーの生成、管理、安全保管、および証明に使用できます。Intel の TXT（Trusted Execution Technology）機能および Windows Server 2016 での Microsoft のプラットフォーム保証機能もサポートされます。TPM は、Windows Server 2012/2016 で BitLocker™のハード ディスク ドライブの暗号化機能を有効にするために使用できます。

TPM はリモート証明 HyTrust CloudControl ソリューションと互換性があります。証明およびリモート証明ソリューションでは、TPM を使用してサーバのハードウェア、ハイパーバイザー、BIOS、および OS のブート時に測定を行い、暗号化形式を用いた安全な方法で、TPM に格納されている基準の測定値と比較できます。それらが一致しない場合、サーバが侵害されている可能性があり、システム管理者はローカルまたはリモートでサーバを無効にするまたは切断できます。

TPM は BIOS オプションで有効化されます。これはプラグ イン モジュール ソリューションとして提供されます。プレーナーにプラグ イン モジュール用のコネクタがあります。

3.1.4 セキュリティ認可

Dell EMC は、NIST FIPS 140-2 やコモン クライテリア EAL-4 などの標準の認定を受けています。これらは米国国防総省やその他の法令上の要件を遵守するために重要です。PowerEdge サーバは次の認定を受けています。

- サーバ プラットフォーム：コモン クライテリア EAL4 + RHEL 認定
- iDRAC および CMC FIPS 140-2 レベル 1 認定
- TPM 1.2 および 2.0 に関する FIPS 140-2 およびコモン クライテリア認定
- SED ストレージ ドライブに関する FIPS 140-2 認定

3.2 ユーザー アクセスのセキュリティ

適切な認証と許可を得ることは、最新のアクセス制御ポリシーの主要な要件です。PowerEdge サーバの主なアクセス インターフェイスは、API、CLI または組み込み iDRAC の GUI です。サーバ管理を自動化するために優先される API および CLI を以下に示します。

- Redfish を伴う iDRAC Restful API

- iDRAC WS-MAN API
- RACADM CLI
- SSH/CLI

これらそれぞれが、ユーザー名とパスワードによるセキュリティなどの堅牢な資格情報を提供し、必要な場合には HTTPS などの暗号化された接続経由で送信されます。SSH は、一致する暗号化キーのセットを使用してユーザーを認証します（そのため、安全性で劣るパスワード入力操作の必要はありません）。IPMI などの従来のプロトコルはサポートされますが、ここ数年で検出されたさまざまなセキュリティ上の問題を考慮すると、新たに導入することはお勧めしません。現在 IPMI を使用している場合、Redfish を伴う iDRAC Restful API を評価し、これに移行することをお勧めします。

TLS/SSL 証明書は、iDRAC にアップロードして Web ブラウザ セッションを認証できます。3 つのオプション:

- **Dell EMC 自己署名 TLS/SSL 証明書** : 証明書は自動生成され、iDRAC によって自己署名されます。
  - 利点 : 個別の認証機関を管理する必要はありません（X.509/IETF PKIX 規格を参照してください）。
- **カスタム署名 TLS/SSL 証明書** : 証明書は自動生成され、iDRAC にすでにアップロードされている秘密キーで署名されます。
  - 利点 : すべて iDRAC に対して必要な信頼済み CA は 1 つのみです。社内 CA がすでに管理ステーションで信頼されている可能性があります。
- **CA 署名 TLS/SSL 証明書** : CSR（証明書署名リクエスト）が生成されて社内 CA に送信されるかまたは署名のために VeriSign や Thawt、Go Daddy などのサード パーティ CA によって生成されます。
  - 長所 : 商用の認証機関を使用することができます（X.509/IETF PKIX 規格を参照してください）。すべて iDRAC に対して必要な信頼済み CA は 1 つのみです。商用の CA 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高いです。

iDRAC9 は、PowerEdge サーバへの安全なアクセスをすでに提供しているお客様の既存に認証および認可スキーマを利用して、**Active Directory** および **LDAP** との統合が可能です。また、**RBAC（ロールに基づいたアクセス制御）**もサポートし、サーバ操作をする人のロールと一致する適切なアクセス レベル（管理者、オペレーター、読み取り専用）を付与します。このように RBAC を使用し、単純に最高レベル（つまり管理者）をすべてのユーザーに付与しないことを強くお勧めします。

2 要素認証（2FA）は、ユーザー名とパスワードに基づく 1 要素認証方式の脆弱性が増しているため、現在使用が増加しています。iDRAC9 ではリモート GUI アクセスのためのスマート カードの使用が許可されています。2 要素とは、スマート カードが物理的に存在していることとスマート カードの PIN です。

iDRAC9 には、**IP ブロックやフィルタリング**など不正アクセスから保護する追加の方法も用意されています。IP ブロックは、ログイン失敗回数の超過が特定の IP アドレスで発生したときにこれを動的に判定し、このアドレスの iDRAC9 へのログインを事前に選択された時間ブロック（防止）します。IP フィルタリングを行うと、iDRAC にアクセスするクライアントの IP アドレスの範囲を制限できます。これは、受信したログインの IP アドレスを指定した範囲と比較し、送信元 IP アドレスがその範囲内の管理ステーションからのログインのみ iDRAC へのアクセスを許可します。その他のすべてのログイン リクエストは拒否されます。

3.2.1 工場出荷時のデフォルト パスワード

デフォルトでは、すべての第 14 世代 PowerEdge サーバには、一意の工場で生成された iDRAC パスワードが付属していて、追加のセキュリティを実現しています。このパスワードは工場で生成され、シャーシ前面のプル アウト情報タグに記載されています。サーバ資産ラベルの横です。このデフォルトのオプションを選択したユーザーは、このパスワードをメモし、iDRAC への初めてのログインにこのパスワードを使用する必要があります。セキュリティを確保するために、Dell EMC はデフォルト パスワードを変更することを強くお勧めします。

3.2.2 システム ロックダウン

iDRAC9 には、サーバのハードウェアおよびファームウェアの構成を「ロック」する新機能が用意されています。このモードは、GUI、RACADM などの CLI を使用して、またはサーバ構成プロファイルの一部として有効化できます。管理権限を持つユーザーは、下位の権限を持つユーザーがサーバを変更できないようにするシステム ロックダウン モードを設定できます。この機能は、IT 管理者によって有効化/無効化できます。システム ロックダウンが無効のときに行われた変更はすべてライフサイクル コントローラー ログで追跡されます。ロックダウン モードを有効にすることによって、Dell EMC のツールおよびエージェントを使用するときにデータセンターの構成が変更されるのを防ぐことができ、また、Dell EMC の更新パッケージを使用するときに組み込みファームウェアへの悪意のある攻撃から保護できます。

3.2.3 ドメイン分離

第 14 世代 PowerEdge サーバには、**ドメイン分離**によるセキュリティが追加されました。これはマルチ テナント ホスティング環境にとって重要な機能です。サーバのハードウェア構成を保護するために、ホスティング プロバイダーはテナントによる再構成を一切できないようにする必要があります。ドメイン分離は、帯域外の iDRAC または ME（管理エンジン）や IE（イノベーション エンジン）などの Intel チップセットの機能にホスト OS の管理アプリケーションが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更新

PowerEdge サーバは、サーバ プラットフォーム上で動作しているファームウェアが正規品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の更新にデジタル署名を使用してきました。当社は、当社のすべてのファームウェア パッケージを 2048 ビットの RSA 暗号化が含まれている SHA-256 ハッシュでデジタル署名しています。これは重要なすべてのサーバ コンポーネントの署名用です。対象のコンポーネントは、iDRAC のファームウェア、BIOS、PERC、I/O アダプター、LOM、PSU、ストレージ デバイス、CPLD、バックプレーン コントローラーなどです。iDRAC は、シリコン ベースのルート オブ トラストを使用して、ファームウェアの更新をスキャンし、その署名を想定される署名と比較します。検証に失敗したファームウェア パッケージの更新は中止され、エラー メッセージが LCL（ライフサイクル ログ）にログされ、IT 管理者を警告します。

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 パーティの更新ツールを使用して悪意のあるファームウェアが NIC やストレージ ドライブなどにロードされないようにしています（また、署名された Dell EMC の更新パッケージの使用をバイパスしないようにしています）。

PowerEdge サーバに付属のサード パーティ製 PCIe およびストレージ デバイスの多くは、ハードウェアのルート オブ トラストを使用して、それぞれのファームウェアの更新を検証しています。

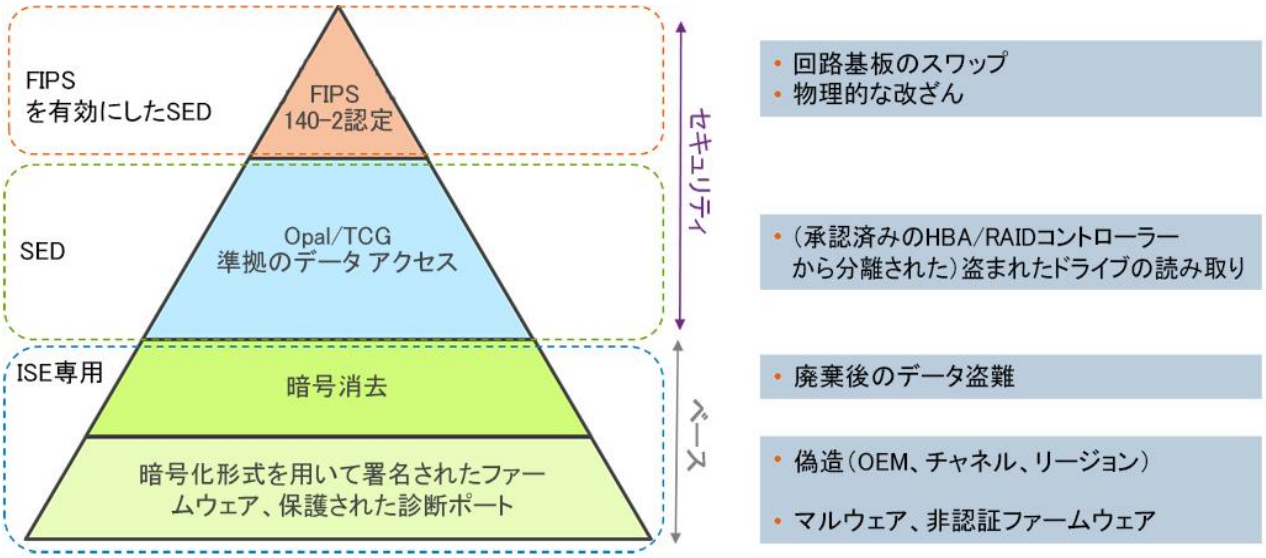
任意のデバイスのファームウェアが悪意のある改ざんをされた疑いがある場合、IT 管理者は、プラットフォーム ファームウェア イメージの多くを iDRAC に格納されている以前の信頼できるバージョンにロールバックできます。当社は、サーバに 2 つのバージョンのデバイス ファームウェアを保持しています。既存の本番バージョン("N")と以前の信頼できるバージョン("N-1")です。

3.4 暗号化されたデータ ストレージ

第 14 世代 PowerEdge サーバは、データを保護するためにいくつかのストレージ ドライブ オプションを用意しています。以下に示すように、最初のオプションは迅速かつ安全にユーザー データを消去する新しいテクノロジーである ISE(Instant Secure Erase)です。第 14 世代サーバは、デフォルトで ISE 対応のドライブを用意しています。ISE については、システム消去機能の説明の一部としてこのペーパーで詳細に後述します。

次の高度なセキュリティ オプションは、SED(自己暗号化ドライブ)です。これは、ストレージ ドライブをサーバおよび使用中の RAID カードにバインドするロック保護を提供します。これは「smash and grab」と呼ばれるドライブ盗難とその後の機密ユーザー データの損失に対する保護を提供します。窃盗犯は、このドライブを使用するために必要なロック キー パスフレーズを知らないため、暗号化されたドライブ データへのアクセスを阻止されます、

最も高度な保護は、NIST FIPS 140-2 認定の SED によって提供されます。この規格に準拠するドライブは、複数のテスト ラボによって認定され、改ざん耐性ステッカーがドライブに貼られています。Dell EMC の SED ドライブは、デフォルトで FIPS 140-2 認定を受けています。



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 ユーザー資格情報と自己署名 SSL 証明書の秘密キーなどのさまざまな機密性の高いデータを保護する安全なストレージ メモリを提供します。シリコン ベースのセキュリティの別の例とし

て、このメモリは、製造時に iDRAC チップそれぞれにプログラムされた一意で不変のルート キーで暗号化されています。これは、攻撃者がデータにアクセスしようとしてチップのハンダを除去するという物理的な攻撃に対する保護を提供します。

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、あらゆる包括的なセキュリティ ソリューションの不可欠な要素です。USB などの入力ポートへのアクセスを制限することを希望するお客様もいます。通常、本番環境になった後にはサーバ シャーシを開ける必要はありません。どのような場合でも、お客様は少なくともそのような行為を追跡し、ログすることを希望します。全体的な目標は、あらゆる物理的な侵入を抑制し、制限することです。

3.5.1 シャーシ侵入アラート

PowerEdge サーバは、ハードウェア侵入検知およびログを提供します。この検知は AC 電源が使用できない場合でも動作します。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 USB ポートの無効化

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できます。前面の USB ポートのみを無効化することもできます。たとえば、本番用の USB ポートを無効にして、デバッグ目的でクラッシュ カートへのアクセスを許可するために一時的に有効化できます。

3.5.3 iDRAC Direct

iDRAC Direct は、サーバ本体でのデバッグおよびサーバの前面（冷気の通路）からの管理のために iDRAC サービス プロセッサーに組み込まれた特別な USB ポートです。これを使用すると、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、他方の端（Type A）をノートパソコンに接続できます。標準的な Web ブラウザを iDRAC GUI にアクセスし、サーバの詳細なデバッグと管理を実行できます。IDRAC Enterprise のライセンスがインストールされている場合、ユーザーは iDRAC の仮想コンソールの機能を使用して OS デスクトップにもアクセスできます。

ログインには通常の iDRAC 認定資格が使用されるため、iDRAC Direct は、安全なクラッシュ カートとして動作し、詳細なハードウェア管理とサービスの診断の利点が追加されます。これは、遠隔地にあるサーバへの物理的なアクセスを安全に行うための魅力的なオプションです（この場合には、ホストの USB ポートと VGA 出力を無効にできます）。

3.5.4 iDRAC Connection View とジオロケーション

第 14 世代の新機能に Connection View があります。これは、サーバ I/O に接続された外部スイッチおよびポートを報告する iDRAC の機能です。これは、ネットワーキング デバイス（通常、より新しくより高速なカード）を選択する機能で、接続されているスイッチの LLDP（Link Layer Discovery Protocol）を有効にする必要があります。

Connection View のメリットの一部を以下に示します。

- サーバ I/O モジュール（LOM、NDC、およびアドイン PCIe カード）が正しいスイッチおよびポートに接続されているかどうかを遠くから迅速にチェックできる
- 配線のエラーを修正するために、コストがかかる遠方からの技術者派遣を回避できる
- サーバ ルームの暑い通路でケーブルをたどる作業が不要になる
- GUI から実行できる、RACADM コマンドによってすべての第 14 世代の接続についての情報を提供できる

明白な時間とコストの節約の他にも Connection View にはメリットがあります。それは、物理サーバまたは仮想マシンのジオロケーションがリアルタイムでわかることです。iDRAC Connection View を使用すると、管理者は、サーバを特定し、そのサーバが接続されているスイッチおよびポートを正確に確認できます。この機能によって、会社のセキュリティ ガイドラインまたはベスト プラクティスに準拠していないネットワークおよびデバイスにサーバが接続されないようにできます。

Connection View は、接続されているスイッチの ID を報告することによって間接的にサーバの場所を検証します。スイッチ ID を使用するとジオロケーションがわかり、サーバが非公認サイトにある違法サーバでないことを確認でき、物理的セキュリティのレイヤーが追加されます。この機能によって、アプリケーションまたは VM が国境を「超えて」おらず、承認された安全な環境で動作していることも検証されます。

3.6 サプライ チェーンの整合性とセキュリティ

サプライ チェーンの整合性は以下の 2 つの重要な課題が重視されます。

(i) ハードウェアの整合性の維持：お客様に製品を出荷する前に製品の改ざんまたは偽造コンポーネントの挿入がないことを確認する

(ii) ソフトウェアの整合性の維持：製品をお客様に出荷する前にマルウェアがファームウェアまたはデバイス ドライバに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ぐ

Dell EMC は、サプライ チェーンのセキュリティを、物理資産、在庫、情報、知的財産、および人を保護する、防止および検出の制御手段の実践と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を講じると、悪意によるまたは不注意によるマルウェアや偽造コンポーネントのサプライ チェーンへの侵入機会が減ることによって、サプライ チェーンの保証と整合性をもたらす役にも立ちます。

3.6.1 ハードウェアとソフトウェアの整合性

Dell EMC は、品質管理プロセスを確実に整備し、偽造コンポーネントが当社のサプライ チェーンに侵入する機会を最小限に抑えることに重点を置いています。Dell EMC が整備している管理は、サプライヤーの選択、調達、生産プロセス、ガバナンス、監査、テストにまで及びます。サプライヤーを選択すると、新製品導入プロセスによって、すべての構築ステージで使用されるすべての材料が承認済みベンダー リストから調達され、適切に部品表と照合されます。生産中に材料の検査を行うことによって、マーキングミスされている、正常な性能パラメーターから逸脱している、または正しくない電子 ID が含まれているコンポーネントを特定できます。

部品は、可能な場合には、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）から直接調達されます。新製品導入プロセス中に行う材料検査によって、サプライ チェーンに入り込んでいたかもしれない偽造コンポーネントまたは破損しているコンポーネントを特定する複数の機会がもたらされます。

また、Dell EMC は、すべてのグローバル製造サイトで ISO 9001 認定を保持しています。これらのプロセスおよび制御を厳守していることによって、偽造コンポーネントが Dell EMC 製品に組み込まれる、またはマルウェアがファームウェアやデバイス ドライバに挿入されるリスクを最小化できます。これらの対策は、SDL（ソフトウェア開発ライフサイクル）プロセスの一部として実装されます。

3.6.2 物理セキュリティ

Dell EMC には、製造施設および物流ネットワークのセキュリティを確立し、維持する、長年にわたって実践されてきた重要な慣習がいくつかあります。たとえば、Dell EMC 製品を製造している特定の工場に、TAPA（Transported Asset Protection Association：輸送中資産保護協会）の施設セキュリティ要件を満たすことを要求しています。この要件には、重要エリアでの有線監視カメラの使用、アクセス制御、入口と出口の常時警備が含まれます。業界をリードするロジスティクス プログラムの一環として、輸送中の盗難や改ざんから製品を守るための保護対策も整備しています。このプログラムでは、スタッフが常駐しているコマンド センターを用意していて、世界中の入庫と出庫を監視し、ある出荷先から別の出荷先に遅延なく出荷できるようにしています。

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アティブにも積極的に関与しています。このようなイニシアティブの 1 つが C-TPAT（Customs-Trade Partnership Against Terrorism：テロ行為防止のための税関産業界提携）です。これは、9/11 後に米国政府によって導入され、国境の強化やサプライ チェーンのセキュリティ対策を通じてテロの可能性を低減する役に立っています。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、セキュリティ プラクティスの整合性の確保と、セキュリティ ガイドラインのサプライ チェーン内のビジネス パートナーへの伝達を参加メンバーに求めています。Dell EMC は、2002 年以来積極的に参加しており、最上位のメンバーシップ ステータスを保持しています。

4 検出

サーバ システム内の構成、稼働状態ステータス、および変更イベントに対する完全な可視性を提供する検出能力を持つことが重要です。この可視性によって、ブートおよび OS ランタイム プロセス中の BIOS、ファームウェア、およびオプション ROM への悪意のあるまたはその他の変更も検出する必要があります。プロアクティブなポーリングは、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と組み合わせる必要があります。ログは、サーバへのアクセスと変更に関する詳細な情報を提供する必要があります。最も重要な点として、サーバは、すべてのコンポーネントにこれらの機能を拡張する必要があります。

4.1 IDRAC を通じた包括的なモニタリング

iDRAC は、サーバの管理対象リソースと通信する OS エージェントに依存するのではなく、各デバイスに直接サイドバンド パスを使用します。Dell EMC は、MCTP、NC-SI、NVMe-MI などの業界標準のプロトコルを活用して、PERC RAID コントローラ、Ethernet NIC、ファイバ チャネル HBA、SAS HBA、NVMe ドライブなどの周辺デバイスと通信します。このアーキテクチャは、PowerEdge サーバでエージェントレスのデバイス管理を実施する、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結果、生まれたものです。構成とファームウェア アップデート操作は、Dell EMC とパートナーがサポートする、強力な UEFI と HII の機能を活用します。

この機能により、iDRAC はシステムを監視して、構成イベント、侵入イベント（このペーパーで前述したシャーシ侵入検知など）、および稼働状態の変更を検出できます。構成イベントは変更を行ったユーザーの ID に直接結び付けられ、変更が GUI ユーザー、API ユーザー、またはコンソール ユーザーのいずれのユーザーによって行われたかがわかります。

4.1.1 ライフサイクル ログ

ライフサイクル ログは、一定期間にサーバで発生したイベントのコレクションです。ライフサイクル ログはイベントを説明するものです。これにはタイムスタンプ、重大度、ユーザーID またはソース、推奨されるアクション、およびその他の技術情報が含まれ、トラッキングや警告の目的に非常に役立ちます。

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

- 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 の構成変更
- 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の更新履歴
- 交換したパーツについての情報
- 障害が発生したパーツについての情報
- イベント ID とエラー メッセージ ID
- ホストの電源関連のイベント
- POST エラー
- ユーザー ログイン イベント
- センサーの状態変更イベント

4.1.2 アラート

iDRAC は、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を提供します。イベントが生成されると、選択したアラート タイプのメカニズムを使用して構成された宛先に転送されます。アラートを有効または無効にするには、iDRAC の Web インターフェイス、RACADM、または iDRAC 設定ユーティリティを使用します。

iDRAC は、次に示すさまざまなタイプのアラートをサポートしています。

- 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 のイベント
- WS のイベント

アラートは、重大度（重要、警告、情報）で分類することもできます。

アラートには次のフィルターを適用できます。

- 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して異なるアクション（再起動、電源の入れ直し、電源オフ、または何もしない）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、あらゆる変更に対して「ゼロ トレランス」ポリシーを採用することで、組織は悪用の可能性を低減できます。Dell EMC OpenManage Essentials コンソールを使用すると、お客様は、独自のサーバ構成のベースラインを定義して、本番サーバのそのベースラインからのドリフトを監視できます。ベースラインは、セキュリティやパフォーマンスなどのさまざまな生産条件に合うようにさまざまな基準に基づいて構築できます。OpenManage Essentials はベースラインからの逸脱を報告できます。また、オプションで簡単なワークフローを使用してドリフトを修復し、iDRAC バンド外での変更を段階的に実行できます。この変更は、次のメンテナンス ウィンドウでサーバの再起動中に実行され、本番環境のコンプライアンスを再度準拠するようにできます。この段階的なプロセスによって、お客様は、非メンテナンス時間中にサーバのダウンタイムなしで構成の変更を本番環境に展開できます。このことによって、保守性とセキュリティを犠牲にせずにサーバの可用性を向上できます。

5 リカバリ

サーバー ソリューションでは、次のようなさまざまなイベントに対する応答として既知の一貫性のある状態へのリカバリをサポートする必要があります。

- 新しく発見された脆弱性
- 悪意のある攻撃やデータの改ざん
- メモリ障害または不適切な更新手順によるファームウェアの破損
- サーバ コンポーネントの交換
- サーバの廃棄や転用

これから、新たな脆弱性や破損の問題への対応方法、および必要に応じてサーバを元の状態にリカバリする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応答

CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子）は、ソフトウェアおよびハードウェア製品を危険にさらす新たに発見された攻撃経路です。リスクを迅速に評価し、適切なアクションを取るためには、ほとんどの企業にとって CVE へのタイムリーな対応が重要です。

以下を含む多くのアイテムで発見される新しい脆弱性に対応して CVE が拡散される可能性があります。

- OpenSSL などのオープン ソース コード
- Web ブラウザなどのインターネット アクセス用ソフトウェア
- 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 システムとハイパーバイザー

Dell EMC は PowerEdge サーバの新しい CVE に迅速に対応することに積極的に取り組み、以下を含むタイムリーな情報をお客様に提供します。

- どの製品が影響を受けるか
- 使用可能な修正ステップ
- CVE に対処するために更新を利用可能な時期（必要な場合）

5.2 BIOS Recovery と OS Recovery

Dell EMC の第 14 世代 PowerEdge サーバには 2 種類のリカバリがあります。BIOS Recovery と Rapid OS（Operating System）Recovery 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、特別なストレージ領域はランタイム ソフトウェア（BIOS、OS、デバイス ファームウェアなど）からは認識されません。これらのストレージ領域には初期イメージが含まれていて、被害を受けたプライマリ ソフトウェアの代わりに使用できます。

Rapid OS Recovery を使用すると、破損した OS イメージ（または悪意のある改ざんを受けた疑いがある OS イメージ）を迅速にリカバリできます。リカバリ メディアは、内部 SD カード、SATA ポート、M.2 ドライブ、または内部 USB から取得できます。選択したデバイスをブート リストおよび OS に公開してリカバリ イメージをインストールできます。その後無効にし、ブート リストと OS から認識できないようにできます。認識できない状態では、BIOS は、OS からデバイスにアクセスできないようにデバイスを無効にします。OS イメージが破損した場合、再起動できるようにリカバリ場所を有効化できます。これらの設定は、BIOS または iDRAC インターフェースからアクセスできます。

極端な場合、つまり（悪意のある攻撃、または更新プロセス中の電源喪失、またはその他の予期できないイベントによって）BIOS が破損した場合、BIOS を元の状態にリカバリする方法を提供することが重要です。バックアップ BIOS イメージは、必要に応じて BIOS イメージをリカバリするために使用できるように、iDRAC に保存されます。iDRAC は、エンド ツー エンドのリカバリ プロセスを調整します。

- *BIOS の自動リカバリ*は BIOS 自体によって開始されます。
- *オン デマンド BIOS リカバリ*は、RACADM CLI コマンドを使用してユーザーが開始できます。

5.3 ファームウェア ロールバック

ファームウェアを更新された状態に維持し、確実に最新機能が導入され、セキュリティ更新が実行されるようにすることをお勧めします。ただし、更新後に問題が発生した場合、更新をロールバックしたり、前のバージョンをインストールしたりする必要が生じる場合があります。前のバージョンにロールバックする場合、その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」から以前のバージョン「N-1」へのファームウェア ロールバックは、現在、以下のファームウェア イメージに対してサポートされています。

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

以下の方法のいずれかを使用して、ファームウェアを前にインストールしたバージョン（「N-1」）に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 と CMC
- Lifecycle Controller GUI
- Lifecycle Controller：リモート サービス

Lifecycle Controller がサポートする iDRAC のファームウェアまたは任意のデバイスをロールバックできます。前回のアップグレードに別のインターフェースが使用された場合でも可能です。たとえば、ファームウェアが Lifecycle Controller GUI を使用してアップグレードされた場合、iDRAC Web インターフェイスを使用してそのファームウェアをロールバックできます。1 回のシステム再起動で複数のデバイスのファームウェア ロールバックを実行できます。

1 つの iDRAC と Lifecycle Controller ファームウェアがある第 14 世代 PowerEdge サーバでは、iDRAC ファームウェアをロールバックすると、Lifecycle Controller 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構成のリストア

保守イベントの改善は IT 運用の重要部分です。リカバリ時間目標およびリカバリ ポイント目標を満たすことができるかどうかは、ソリューションのセキュリティに直接影響を与えます。サーバ構成とファームウェアをリストアできれば、サーバ運用のセキュリティ ポリシーが自動的に満たされていることになります。

PowerEdge サーバは、次の状況でサーバ構成を迅速にリストアする機能を提供します。

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

5.4.1 パーツの交換

iDRAC は、NIC カード、RAID コントローラー、および PSU(電源ユニット)のファームウェア イメージと構成設定を自動的に保存します。これらのパーツのフィールド交換イベントでは、iDRAC は自動的に新しいカードを検出し、ファームウェアと構成を交換後のカードにリストアします。この機能を使用すると重要な時間を節約でき、一貫性のある構成およびセキュリティ ポリシーが確保されます。更新は、サポート パーツ交換後のシステム再起動時に自動的に行われます。

5.4.2 Easy Restore(マザーボードの交換用)

マザーボードの交換は時間がかかり、生産性に影響しがちです。iDRAC は、PowerEdge サーバの構成とファームウェアをバックアップおよびリストアする機能を提供し、障害が発生したマザーボードを交換する際に必要な労力を最小限に抑えることができます。

PowerEdge サーバのバックアップおよびリストアの方法は 2 つあります。

1. PowerEdge サーバは、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 データをフラッシュ メモリに自動的にバックアップします。

   サーバのマザーボードを交換した後、Easy Restore によってこのデータの自動リストアが求められます。

2. より包括的なバックアップの場合、ユーザーは、BIOS、RAID、NIC、iDRAC、Lifecycle Controller、NDC(ネットワーク付属カード)などさまざまなコンポーネント上にインストールされたファームウェア イメージお

よびこれらのコンポーネントの構成設定を含むシステム構成をバックアップできます。バックアップ操作には、ハード ディスクの構成データ、マザーボードおよび交換パーツも含まれます。バックアップを行うと、vFlash SD カードまたはネットワーク共有（CIFS、NFS、HTTP または HTTPS）に保存できる 1 つのファイルが作成されます。

このプロファイルのバックアップは、ユーザーがいつでもリストアできます。Dell EMC は、ある時点でリストアする必要が生じるかもしれないと思われるすべてのシステム プロファイルのバックアップ操作を実行することをお勧めします。

5.5 システム消去

システムのライフサイクルの終わりには、システムを廃棄または転用する必要があります。システム消去の目標は、機密情報は誤ってリークしないように機密データと設定を消去することです。これは、Lifecycle Controller のユーティリティで、ログ、構成データ、ストレージ データ、キャッシュ、および組み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。

システム消去の機能を使用して、次のデバイス、構成設定、および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
- LC（Lifecycle Controller）のデータ
- BIOS
- 組み込まれた診断プログラムと OS ドライバ パック
- iSM
- SupportAssist Collection のレポート

また、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（クリア PERC NVCache）
- vFlash SD カード（初期化カード）

次のコンポーネントに関するデータは、次のようにシステム消去によって暗号化されて廃棄されます。

- SED（自己暗号化ドライブ）
- ISE 専用ドライブ（Instant Secure Erase ドライブ）
- NVM デバイス（Apache Pass、NVDIMMs）：2018 年後半に提供予定

また、非 ISE SATA ハード ディスク ドライブはデータ上書きによって消去できます。

ISE（Instant Secure Erase）は第 14 世代ドライブで使用される内部暗号化キーを破壊するため、ユーザー データがリカバリ不能になることに注意してください。ISE は、NIST Special Publication 800-88「Guidelines for Media Sanitization」で示されている、ストレージ ドライブ上のデータ消去方法として広く認められています。

システム消去を含む新しい ISE 機能のメリットは次のとおりです。

- **速度**：DoD 5220.22-M などのデータの上書き手法と比べてはるかに高速（何時間もから数秒に短縮）

- **効率性**:ISE はドライブのすべてのデータ(予約済みブロックを含む)を完全に読み取り不可能にする
- **TCO の向上**:ストレージ デバイスを物理的に破壊するのではなく再使用が可能

システム消去は、Lifecycle GUI、WS-Man API、または RACADM CLI からアクセスできます。

5.6 すべての電源の入れ直し

すべての電源の入れ直しでは、サーバとそのすべてのコンポーネントが再起動します。サーバおよびすべてのコンポーネントから主電源および予備電源が失われます。揮発性メモリ内のデータもすべて消去されます。

*物理的な*すべての電源の入れ直しを行うには、AC 電源ケーブルを抜き、30 秒間待機してからケーブルを再度差し込む必要があります。これはリモート システムで動作している場合の課題です。第 14 世代サーバの新しい機能を使用すると、iSM、IDRAC GUI、BIOS、またはスクリプトからすべての電源の入れ直しを有効に実行できます。すべての電源の入れ直しは次の電源の入れ直しで有効になります。

すべての電源の入れ直し機能を使用すると、誰かがデータセンターに実際に行く必要がなくなるため、トラブルシューティングの時間を低減できます。たとえば、メモリに常駐しているマルウェアを排除できます。

6 サマリー

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 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。ハードウェアを対象としたサイバー攻撃からの保護、その検出、およびリカバリを行うには、サーバのハードウェア設計にセキュリティを構築する必要があります。後から追加するものではありません。

Dell EMC は、過去 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を保護し PowerEdge サーバの機密ユーザー データを保護することをリードしてきました。新しい第 14 世代 PowerEdge 製品ラインは、シリコン ベースのルート オブ トラストを使用する強化されたサイバー レジリエント アーキテクチャが特長です。これによって、以下の機能を含むサーバ セキュリティがさらに強化されています。

- **暗号化形式を用いて検証された信頼性の高いブート**:エンド ツー エンドのサーバ安全性およびデータセンター全体のセキュリティの基盤です。これには、シリコン ベースのルート オブ トラスト、デジタル署名されたファームウェア、BIOS の自動リカバリなどの機能が含まれます。
- **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安全なストレージ領域です。
- **システム ロックダウン**:PowerEdge 固有の機能で、悪意の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安全に保護し、システムを変更しようとしたことをユーザーに警告します。
- **システム消去**:これを使用すると、ストレージ ドライブやその他の組み込み型の非揮発性メモリから安全かつ迅速にデータを消去することによって、第 14 世代 PowerEdge サーバをユーザーが簡単に廃棄および転用できます。

結論として、業界をリードするセキュリティを備えた第 14 世代 PowerEdge サーバは、モダン データセンターの信頼性の高い基盤を形成し、お客様はそこから IT 運用およびワークロードを安全に実行できます。

A 付録:参考資料

セキュリティのホワイト ペーパーおよび販促資料

- (開発から直接)SYSTEM ERASE ON POWEREDGE SERVERS(POWEREDGE サーバのシステム消去)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242

  SECURING 14TH GENERATION DELL EMC POWEREDGE SERVERS WITH SYSTEM ERASE(システム消去による第 14 世代 DELL EMC POWEREDGE サーバの保護)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- (開発から直接)SECURITY IN SERVER DESIGN(サーバ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)CYBER-RESILIENCY STARTS AT THE CHIPSET AND BIOS(チップセットと BIOS で始まるサイバー レジリエンシー)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- FACTORY GENERATED DEFAULT IDRAC9 PASSWORD(IDRAC9 の工場出荷時デフォルト パスワード)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368

  DELL EMC IDRAC RESPONSE TO CVE-2017-1000251 “BLUEBORNE”(CVE-2017-1000251 “BLUEBORNE”への DELL EMC IDRAC のレスポンス)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605

  (ビデオ)SECURE BOOT CONFIGURATION AND CERTIFICATE MANAGEMENT USING RACADM (RACADM を使用した安全なブート構成と証明書管理)
  https://youtu.be/mrIIN4X380c
- (ビデオ)SECURE BOOT CONFIGURATION AND CERTIFICATE MANAGEMENT USING WSMAN (WSMAN を使用した安全なブート構成と証明書管理)
  https://youtu.be/0D1Zq1CtRwg

  SECURE BOOT MANAGEMENT ON DELL EMC POWEREDGE SERVERS(DELL EMC POWEREDGE サーバの安全なブート管理)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- Signing UEFI images for Secure Boot feature in the 14th generation and later Dell EMC PowerEdge servers(第 14 世代以降の Dell EMC PowerEdge サーバの Secure Boot 機能の UEFI イメージの署名)
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255

- RAPID OPERATING SYSTEM RECOVERY
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- Managing iDRAC9 Event Alerts on 14th generation (14G) Dell EMC PowerEdge Servers（第 14 世代 Dell EMC PowerEdge サーバの iDRAC9 イベント アラートの管理）
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266

PowerEdge ホワイト ペーパー

- iDRAC Overview（iDRAC の概要）
  http://www.DellTechCenter.com/iDRAC

- OpenManage Console Overview（OpenManage コンソールの概要）
  http://www.DellTechCenter.com/OME

- OpenManage Mobile Overview（OpenManage Mobile の概要）
  http://www.DellTechCenter.com/OMM

- Lifecycle Controller Part Replacement（Lifecycle Controller のパーツ交換）
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457

- Motherboard Replacement（マザーボードの交換）
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832

- Managing Server Configuration by using Dell EMC OpenManage Essentials (OME)
  （Dell EMC OpenManage Essentials（OME）を使用したサーバ構成の管理）
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444397