Dell PowerEdge サーバーの サイバーレジリエントセキュリティ

2023年10月

H19738.1

ホワイトペーパー

概要

このホワイトペーパーはDell PowerEdge の サイバーレジリエント アーキテクチャに焦点を当て、お客様のインフラストラクチャーにゼロトラスト方針を導入するためのサーバー ライフサイクルについてご説明します。Dell PowerEdge のセキュリティ制御能力は、ゼロトラスト体制を実施しながらセキュリティ レジリエンシーを確保できる、包括的なセキュリティ ソリューションをご提供します。

DELL Technologies

Copyright

目次

エグゼクティブ サマリー

概要

セキュリティに対するデル・テクノロジーズのアプローチは内在的、つまりセキュリティを後付けの機能とするのではなく、Dell セキュア開発ライフサイクル全体を通じて、製品開発のあらゆるステップに組み込んでいます。変化し続ける脅威の状況に対応し、お客様がゼロトラスト方針の導入を加速できるよう、当社は Dell PowerEdge のセキュリティ制御、機能、およびソリューションを継続的に進化させるよう努めています。

インフラストラクチャーのセキュリティ確保は1度限りの投資ではなく、マインドセットと全体的なアプローチにより実現します。本ホワイトペーパーでは、セキュリティに関するこの道程の視点を用いて、サーバーのライフサイクル全体における PowerEdge の優位性について説明します。PowerEdge のサイバーレジリエントアーキテクチャによるセキュリティ機能が、サーバーの導入から保守、廃棄に至るライフサイクルの各段階でどのように連携して、レジリエンシーとゼロトラスト アプローチの両方を実現しているかをご紹介します。これらの機能の多くが、Dell Remote Access Controller (iDRAC9) で実現されています。

当社は継続的に、シリコンベースのルート オブ トラスト（信頼の基点）を基軸としてセキュリティを強化し続けています。PowerEdge サイバーレジリエントセキュリティの前回のホワイトペーパーの発行以降も多くの新機能が追加されており、それはユーザー アクセスの制御からデータの暗号化、サプライチェーン保証に至るまで多岐に渡ります。すべての機能は、インテリジェンスと自動化を広範に活用することでお客様が脅威曲線の先を行くことを支援し、拡大し続けるユースケースの要求に応じた拡張も可能です。長年にわたって強化されてきた Dell サイバー レジリエント アーキテクチャは、ゼロトラスト環境の重要な要素基盤となります。

改定歴

日付	Part number/ 改定	内容
2022年11月	H19738	初版発行
2023年10月	H19738.1	第16世代のPowerEdgeサーバーを反映して更新

フィードバックをお寄せください

デル・テクノロジーズおよび本書の作成者は、本書に関するお客様のフィードバックを歓迎します。デル・テクノロジーズの担当チームまで 電子メール にてご連絡ください。

著者: Deepak Rangaraj, Kim Kinahan

寄稿者: Marshal Savage

注: このトピックに関する他の文書については Dell Technologies Info Hub for PowerEdge を参照ください。

イントロダクション

デジタル インフラストラクチャーの複雑性

現代のIT環境は、オンプレミス、マルチクラウド、エッジ、Telco など様々なユースケースでサーバーが導入され、ここ数年で劇的に変化しました。設定と管理のためにファームウェアを必要とするコンポーネントの数は増え続け、サーバー プラットフォームがより複雑になっています。私たちはかつてないスピードと量でデータを生成しており、そのデータは多くの場合、地理的に分散した多数の場所で生成・保存されています。こうして複雑さが増す中、攻撃対象の拡大を緩和するためにも、セキュリティ制御を効果的に管理する必要があります。

脅威の高度化と複雑化

デル・テクノロジーズの Digital Transformation Index によると、デジタルトランスフォーメーションの主要な障壁はデータプライバシーとサイバーセキュリティへの懸念です[1]。サイバー攻撃の複雑さ、巧妙さ、頻度は増加の一途を辿り、攻撃による被害は、より甚大なものとなっています。さらに問題を複雑にしているのは、今日の脅威アクターが AI や参入コストの低下といった技術的な進歩を活用する点です。悪意の行為者は、悪用できる脆弱性を常に探しています。高度な AI システムの支援を得た彼らは、前例のない規模で悪質な活動を行い、人間の能力を超えた革新的で有害な方法でシステムを操ります。サイバー犯罪に関連する世界の被害額は、2025年までに10兆5,000億ドルに達すると予測されています。[2]

法規制の状況と社内の義務

世界的な脅威の増大に伴い、世界各国の政府はサイバー脅威に対応するための規制ガイダンスを策定しています。その結果、民間の機関も、高度な持続的脅威を軽減するためにより強力なポリシーや義務付けを策定しています。また、政府と協力するために必要なセキュリティ要件の義務化も進んでおり、これらの要件はサプライヤー、ベンダー、そして政府と提携するあらゆる組織に影響を与えています。こうした規制はさらに、医療、運輸、金融などの重要インフラ部門に及んでいます。そして政府の規制以外でも多くのお客様がインフラを強化したいと考え、独自の社内規定やセキュリティ ポリシーを策定しています。

現代社会のためのゼロトラスト戦略

インフラの複雑化とそれに対する脅威の増大は、ハードウェアだけでなくファームウェアや、サプライチェーンそのものをセキュアにするという、重要な必要性も促進しています。ゼロトラスト戦略を適用する際はよく、経営管理、コントロールプレーン、アプリケーションとデータに焦点が当たりますが、より下のレイヤー、つまりインフラのハードウェアやファームウェア、サプライチェーン、インフラ構築の設計やプロセスのセキュリティもきわめて重要です。これらすべての側面でのゼロトラスト原則の適用が、より包括的なサイバーレジリエンスの実現には必要です。

デル・テクノロジーズは、業界をリードするサーバー、ストレージ、HCI、データ保護アプライアンスにセキュリティを組み込んでおり、データの保存・管理・使用場所を問わずデータ保護を支援します。PowerEdge をベースとする製品の安全性を確保する基盤として、PowerEdge サーバーには、サイバー脅威を予測し、それに耐え、回復できるサイバーレジリエンシーが備わっています。

---

[1] Dell Technologies 2020 Digital Transformation Index

[2] www.cybersecurityventures.com /cybercrime-damage-costs-10-trillion-by-2025/

同時に、PowerEdge サーバーのセキュリティ制御とツールの設計プロセスには、ゼロトラストの原則が組み込まれています。お客様がゼロトラストの導入に着手するにあたり、これらの機能がどう使われるかを予測し、アプローチを適応させています。当社は、お客様がゼロトラスト導入への道程のどこにいても、当社とはより簡単に連携できると考えます。

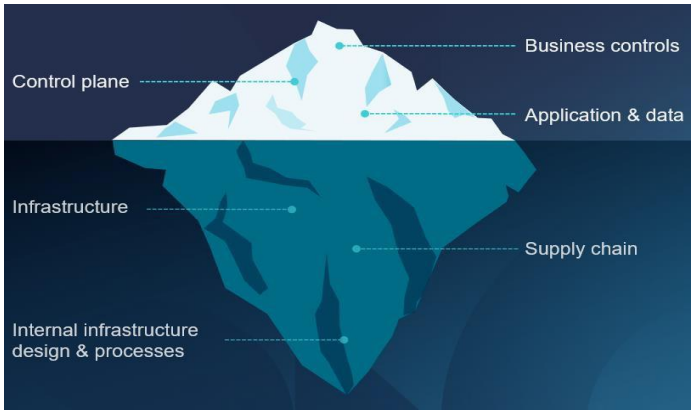


図1. インフラのセキュリティとゼロトラスト

Dell のインフラ セキュリティのアプローチは当社製品に不可欠で、お客様のゼロトラスト導入を加速します。

- ゼロトラストの原則に基づいた製品設計と製造
- ゼロトラストの機能と特長の提供
- 共通の一貫した動作の提供

ゼロトラストの基本原則

ゼロトラスト アーキテクチャの原則は、ネットワークは常に脆弱である前提で、重要なデータやリソースへのアクセスの保護を目的とする一連の原則に基づき構築されます。信頼して検証するフレームワークとは違い、ゼロトラスト アプローチでは暗黙の信頼が排除されます。すべてのユーザー、デバイス、アプリケーションは、ID、デバイスの状態、場所、行動などの要因に基づく継続的な認証と、明示的な承認が必要とされます。

アイデンティティは、ゼロトラストで重要な役割を果たします。その識別は、人だけでなく、アプリケーション、通信経路、ネットワークデバイス、データ自体も関係します。IT資産が識別され、認証され、明示的に承認されると、最小特権の原則が適用されます。このアプローチは、特定のタスクを実行するために必要な最小レベルのアクセス権を承認されたエンティティにのみ与えることを確実にします。データ中心のセキュリティモデルは、アクセスを常に制限すると同時に、異常な活動や悪意ある行動を探します。ゼロトラストアプローチは、信頼性の認証にとって重要な交点で、検証の粒度をより細かくし、最小特権をワークロードの効率に影響を与えることなく最適化します。ここでの目標は、攻撃の抑止と侵入時点での攻撃の拒否です。ただし万が一侵害が発生した場合は、それを即座に検知して修復する能力を強化しておくことで、被害額を最小限に抑制できます。

ゼロトラストの理念を採用し、ゼロトラストの原則を使用することで、システム管理者はユーザー、プロセス、デバイスがどのようにデータと連携するかを制御できます。これらの原則は、侵害されたユーザー情報の悪用、

リモートエクスプロイト、インサイダーの脅威を防ぎ、悪意あるサプライチェーン活動の影響の軽減さえ可能です。

ゼロトラストの7つの柱

米国国立標準技術研究所 (NIST)[3] が定義したゼロトラスト モデルは、相互に関連する7つの柱を定め、それらを連携させてインフラストラクチャーとデータのセキュリティに包括的かつ総合的なアプローチを提供します。各柱は、ゼロトラスト セキュリティ対策を実施するための特定の機能または重点分野を表します。7つの柱を組み合わせることで、多面的、重層的、統合的なセキュリティの枠組みが提供されるのです。

Dell のゼロトラスト アプローチは、インフラとその上のアプリケーションを管理するための幅広いセキュリティ制御と自動化機能を統合します。NIST が概説する7つの柱に沿った Dell の能力を、次の表で示します。

表1. 7つの柱に沿った Dell のゼロトラスト アプローチ

ゼロトラストの柱	NIST の説明[3]	PowerEdge の特長
ユーザー	ユーザーの識別、認証、アクセス制御: • 認証され承認されたユーザーのみデータやリソーにアクセスできる • 最小特権の原則が適用、ユーザーには特定のタスクの実行に必要な最小レベルのアクセスのみ許可する	• IDおよびアクセス管理 • 多要素認証 - RSA Secure ID • シングルサインオン (SSO) をサポートするActive DirectoryまたはLDAPの統合 • ロールベースのアクセス制御と監査
デバイス	デバイスの正常性、コンプライアンス、デバイス ポスチャー評価の監視と適用: • 監視 - 異常や疑わしい読み取り/書き込みアクティビティを探す • 正常性 - ファームウェアの最新バージョンを確認する • すべてのデバイスを識別、インベントリ、承認、認証、更新できる	• シリコン ルートオブトラストとそれを補うインテル Boot Guard またはAMD Platform Secure Boot (AMD PSB) • Secured Component Verification (SCV) によるセュアなサプライチェーン • シャーシ ロックと侵入検知 • USB ポートの動的な有効化・無効化 • Trusted Platform Module (TPM) • SPDM (DMTFのセキュリティ プロトコル データモデル) によるデバイス認証
データ	エンタープライズクラスのインフラストラクチャー、アプリケーション、標準化、強固なエンドツーエンドの暗号化、データタギングの使用によりデータの透明性と可視性を確保する	保存データの保護: • ローカルおよびセキュア エンタープライズ キーマネジメント (LKMおよびSEKM) によるドライブ暗号化 ※直接接続式NVMeにも対応 • ベースボード管理コントローラ (BMC) によるローカル鍵管理 (iLKM) 使用中のデータの保護:

[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust architecture

ゼロトラストの柱	NISTの説明[3]	PowerEdge の特長
		• コンフィデンシャル コンピューティング - インテル SGX、インテル MKTME、AMD SME (Secure Memory Encryption)、AMD (SEV Secure Encrypted Virtualization)、AMD 永続メモリー暗号化
アプリケーションとワークロード	アプリケーションとワークロードをセキュアにしてコンテナとVMを保護する	• セキュア開発ライフサイクル • 暗号で署名されたBIOSとファームウェアのアップデート • セキュアなエンド ツー エンド ブートと UEFI (Unified Extensible Firmware Interface) ブート機能 • ドリフト検出 • CVEに対する迅速な対応と緩和策
ネットワークと環境	ネットワークを暗号化、監視、分析する きめ細かなアクセスとポリシー制限を使用して、ネットワークと環境(オンプレミスとオフプレミス)を論理的および物理的にセグメント化、分離、制御する	• 専用のBMC (iDRAC) ネットワークモジュール • SSH/TLS通信オプション • TLS 1.3 のサポート • DPU/SmartNIC
可視性と分析	インフラ (ユーザー、デバイス、データ、ネットワーク、アプリケーション) 全体のアクティビティと動作を監視して、パターンと異常を特定。アナリティクスを使用して、セキュリティの脅威を検出して対応する	• 永続的なイベントのログ記録と監査 • リアルタイムおよび起動時のファームウェアスキャン • セキュリティの警告 • CloudIQ
自動化およびオーケストレーション	手動のセキュリティ プロセスやその他の該当するプロセスを自動化し、企業全体でポリシー・ベースのアクションを迅速かつ大規模に実行する	• OpenManage Enterprise のドリフト検出機能 • ファームウェアのロールバック • BIOSとOSの自動回復 • 一元的なアップデート • SSL証明書の自動更新

デル・テクノロジーズの優位性

セキュリティは当社の DNA に刻まれており、当社製品は、設計上セキュアな製品であり、デフォルトでセキュアな状態であることをコミットします。PowerEdge サーバーは Dell 社内でゼロトラスト原則に基づき製造され、お客様がゼロトラストの IT 環境と運用を設定できる機能を備えています。また当社の製品は、ポートフォリオ全体で共通の一貫した動作と制御を提供するよう努めています。

iDRAC9 搭載の PowerEdge サーバーは、不変のシリコンベースのプラットフォーム ルートオブトラスト (RoT) を備えており、それはサーバーの導入からメンテナンス、廃棄に至るまでのライフサイクル全体で、検証された信頼の連鎖を確立するために活用されます。このRoTと、セキュリティ管理および包括的な管理ツールとを組み合わせて、PowerEdge のハードウェアとファームウェア全体に強固なセキュリティのレイヤーを提供します。

PowerEdge のこうした機能は、サイバー攻撃からの保護、検出、リカバリのためのレジリエンスを確保するだけでなく、最小権限のゼロトラスト アプローチのためのロックダウン態勢も維持します。最小特権により、ユーザーとデバイスにはタスクの実行に必要なものへのアクセスのみが許可されます。我々の目標はゼロトラストをお客様のために実現し、その導入スピードを加速させることです。

サーバーのライフサイクル全体にわたるセキュリティの道程

インフラ全体にセキュリティを導入するには、基盤となるシステム、ネットワーク、リソースを保護するための一連の継続的な取り組みと対策が必要です。成熟したセキュリティ モデルへの移行は一過性の投資ではなく、一夜にして達成できるものではありません。これは、厳格なセキュリティポリシーの導入への継続的な「旅」でありアプローチなのです。ゼロトラストの実装が時間の経過とともに成熟するにつれ、強化された可視性と広範なコントロールによって脅威の状況に対応できるようになります。当社はこの道程を5つの段階で整理しました。

- **第1段階: サーバーの選定** - お客様はセキュリティが製品の最優先事項であり、設計のあらゆる側面に組み込まれているという保証を求めています。
- **第2段階: サプライチェーン セキュリティの確保** - お客様は、悪意ある犯罪者が元のコンポーネントを偽造品、インプラント、マルウェアに置き換えるという現実的なリスクに直面しています。
- **第3段階: 大規模サーバー環境の効率的な導入と設定** - サーバーをどのように導入するかは、パフォーマンス、安定性、セキュリティに直接影響します。サーバーが正しくセットアップされ、必要なコンポーネントがすべて配置されていることを確認するには、適切な計画と構成が欠かせません。
- **第4段階: セキュリティ管理と監視** - 攻撃は人が検知するより速く発生するため、プロアクティブな環境監視と迅速な対応が必須です。スキルやトレーニング不足も問題を悪化させることがあります。
- **第5段階: サーバーの廃棄と再利用に関するセキュリティ** - データセキュリティは、サーバーを再利用または廃棄する際の重要な考慮事項です。ITのベスト プラクティスでは、機密情報が誤って共有されたり危険にさらされたりしないよう、サーバーのすべてのデータを削除することを推奨します。

第1段階 - サーバーの選定

課題

お客様は、自社のサーバーが全体として安全であり、自社環境に脆弱性を持ち込まないことを確信したいため、ハードウェア、ソフトウェア、ファームウェアを含むサプライチェーン全体と製品設計のあらゆる側面に関し、サーバーベンダーからの保証を求めます。このレベルの保証は、ブラックボックスなインフラのみを提供する可能性のあるクラウドサービスプロバイダーと比較すると、オンプレミスのインフラの差別化要素とも言えます。クラウドベースのシステムを支えるコンポーネントのセキュリティに、お客様が不確かさを感じる可能性があるからです。

PowerEdge のセキュリティ ソリューション

デル・テクノロジーズとのゼロトラストへの第一歩は、PowerEdge サーバーを受け取る前に始まります。本質的なセキュリティ対策は、ハードウェア製品の設計とソフトウェア、ファームウェアのコード開発に組み込まれています。こうした慣行には、製品開発時にセキュリティ機能を確実に実装し、開発サイクル全体を通じてそれを継続する

プロセスとポリシーが含まれます。つまり、「ビルトイン」されたセキュリティです。これを効果的に実践するため、当社のエンジニアにはコードを扱う前に必須のセキュリティ トレーニングの受講が義務付けられています。また各開発チームにセキュリティ チャンピオンを配置し、組織内のセキュリティカルチャーを推進しています。

Dell セキュア開発ライフサイクル

サイバーレジリエント アーキテクチャの実現には、開発の各段階でセキュリティに対する意識と規律が必要です。セキュリティをサーバー設計プロセス全体の不可欠な一部とするために、当社はセキュア開発ライフサイクル (SDL) モデルを活用しています。これには以下の重要な側面が含まれます。

- セキュリティを最優先事項として考案、設計、試作、実装、本番稼動、配備、保守が行われる機能
- 開発ライフサイクルの全フェーズで悪意あるコードの侵入を妨害・阻止・対抗すべく設計したファームウェア:
  - 設計プロセス内で、脅威モデリングと侵入テストを網羅
  - ファームウェア開発の各段階で、セキュアなコーディングの実践を適用
- 重要なテクノロジーについては、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を遵守していることを確認するために、内部 SDL プロセスを補完する外部監査を実施
- 最新のセキュリティ評価ツールを使用した、新たな潜在的脆弱性の継続的なテストと評価
- 重大な共通脆弱性識別子 (CVE) への迅速な対応 (必要な場合は推奨される修復手段を含む)

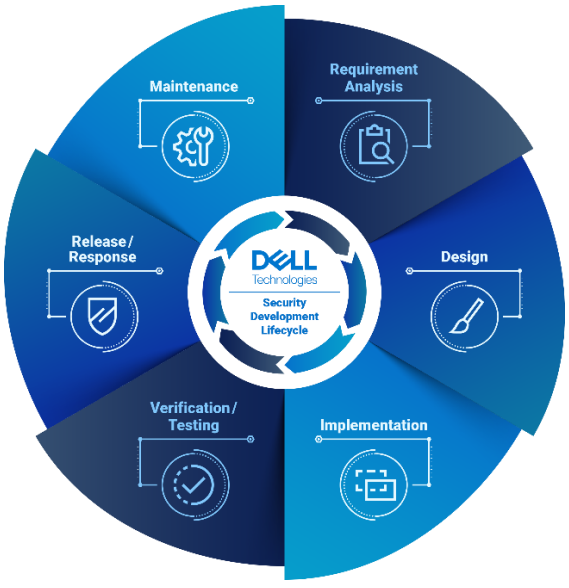


図 2. Dell セキュア開発ライフサイクル

コンプライアンス面の優位性

デル・テクノロジーズは、次の表に示すように、米国連邦政府およびその他の世界の主要な政府要件、および NIST などの業界標準に準拠するために必要な認定を取得しています。

表2. 認証の内容

認証	説明
Common Criteria	PowerEdge サーバーの特定の構成には、コモンクライテリア認定のコンポーネントが含まれています。(例：iDRAC や TPM)
FIPS 140	PowerEdge サーバーの特定の構成には、FIPS 140認定の暗号化モジュール (TPM、IDRAC9、Chassis Management Controller (CMC)、自己暗号化ドライブ (SED)、SSDなど) が含まれます。
IPv6	• PowerEdgeサーバーは、Red Hat Enterprise Linux 8.4 や Windows 2019 または Windows 2022 Server の該当バージョン実行時は、 USGv6r1 および IPv6 Ready ロゴに完全に準拠しており、IPv6 オンリーの機能で認定されています。 • Dell PowerEdge iDRAC9 (v5.1x以降に搭載) は、USGv6r1 および IPv6 Ready ロゴに準拠し、IPv6オンリーの機能で認定されています。

新たな脆弱性への迅速な対応

CVE とは、ソフトウェアや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ベクトルのことです。CVE へのタイムリーな対応は、ほとんどの企業にとって、そのエクスポージャーを迅速に評価し、適切な措置を講じるために重要です。

デル・テクノロジーズは PowerEdge サーバーの新しい CVE に迅速に対応し、次のようなタイムリーな情報を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
- 修復の手順
- 必要に応じて、CVE に対処するための更新プログラムの提供状況

バグ バウンティ プログラム

デル・テクノロジーズは、潜在的な脆弱性や脅威に対する可視性を広げるセキュリティ リサーチ コミュニティの価値を認識しており、この共通の目標を共有するコミュニティ メンバーと協力する機会を歓迎します。

Dell のバグ報奨プログラムは、Dell ブランド製品または現在サポートされている製品で特定されたセキュリティの脆弱性に適用されます。

サーバーのあらゆるレイヤーで脅威のベクトルをカバーするソリューション

日々変化する今日の状況には、多くの脅威ベクトルがあります。以下の表は、各サーバーレイヤーでの重大な脅威を管理するための Dell のアプローチをまとめたものです。

表3. 一般的なサーバー プラットフォーム レイヤーの脅威ベクトルに対する Dell のソリューション

サーバー 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 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または盗難	• Secured Component Verification (SCV) • シャーシ侵入検知機能 • Secure Enterprise Key Management • インテル TME • SPDM
ファームウェアとソフトウェア	• ファームウェアの改ざん • マルウェアの挿入	• シリコンベースのルートオブトラスト • 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機能 • 暗号で署名され、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適用
証明信託の機能	サーバーIDの偽装	• TPM • インテル TXT • 信頼の連鎖 • 802.1x 機能 • SPDM
サーバー管理	• 不正な設定とアップデート • 不正なオープンポート攻撃	• iDRAC9 リモート構成証明

表4. 一般的なサーバー 環境レイヤーの脅威ベクトルに対する Dell のソリューション

サーバー 環境レイヤー		
セキュリティレイヤー	**脅威ベクトル**	**Dell のソリューション**
データ	データ漏洩	• 自己暗号化ドライブ (SED) - FIPS または Opal/TCG • Secure Enterprise Key Management、ISE (Instant Secure Erase) 限定のドライブ • セキュアなユーザー認証
サプライチェーンの整合性	• 偽造コンポーネント • マルウェアの脅威	• ISO9001 認証をグローバル製造拠点で取得 • Secured Component Verification • 所有証明 • Software Bill of Materials (SBOM) • セキュア開発ライフサイクルの一環として実装されるセキュリティ対策
サプライチェーンセキュリティ	• 製造現場の物理的セキュリティ • 輸送中の盗難と製品改ざん	• 輸送資産保護協会（TAPA）の施設セキュリティ要件 • テロ対策税関・貿易パートナーシップ (C-TPAT) • Secured Component Verification (SCV)

第2段階 - サプライチェーン セキュリティ

課題

最新のサーバー プラットフォームは、コンフィギュレーションと管理のためにファームウェアを必要とする何百ものコンポーネントを備え、より複雑になってきています。その結果、サーバーのサプライチェーンもますます複雑になり、何百ものサードパーティベンダーがコンポーネントを供給したり、オープンソースソフトウェアを使用したりしています。この複雑なサプライチェーンは、適切に管理されていない場合、脅威アクターが利用可能な攻撃対象領域の増加の一因となります。サプライチェーンの整合性が保証されていない場合、お客様は脆弱性や脅威が自社の環境に侵入するリスクに直面します。サプライチェーンの整合性には、主に以下の2つの側面があります。

- **ハードウェアの整合性の維持** - 製品がお客様に納品される前に製品の改ざんや偽造コンポーネント、悪意のあるインプラントの挿入がないことを保証
- **ソフトウェアの整合性の維持** - 製品がお客様に納品される前にファームウェアやデバイス ドライバーにマルウェアが挿入されていないことを保証し、既知の脆弱性を持つコードが環境に導入されることを抑止

PowerEdge のセキュリティ ソリューション

エンド ツー エンドのサプライチェーン保証

デル・テクノロジーズは、多面的なアプローチを採用してサプライ チェーンを保護し、脅威が増大する環境においてお客様が信頼できるソリューションを提供しています。当社のサプライチェーンセキュリティは、物的資産、在庫、情報、知的財産、および人を保護する、予防および検出管理で構成されます。こうしたセキュリティ

対策は、悪意や過失によって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混入する機会を減らすことで、サプライチェーンを保証し、完全性を確保します。

Dell のサプライチェーン管理は、監査とテストを通じて、サプライヤーの選定、調達、生産プロセス、ガバナンスにまで及びます。サプライヤーが選択されると、新製品の導入プロセスでは、すべての製造段階で使用されるあらゆる部材が、承認されたベンダーリストから調達され、必要に応じて部品表と一致することが検証されます。生産中の部材検査は、不当なマーキングや、通常の性能パラメータから逸脱したコンポーネントや不正な電子識別子を含むコンポーネントの特定に役立ちます。

パーツ類は、可能な場合は ODM (相手先ブランド設計メーカー) または OCM (相手先ブランド構成部品メーカー) から直接調達されます。当社が新製品の導入プロセス内で実施する材料検査は、サプライチェーンに侵入した可能性のある偽造品や、破損した部品を特定するための、複数の機会を提供します。

デル・テクノロジーズはさらに、世界中のすべての製造拠点で ISO 9001 認証を維持しています。これらのプロセスと管理を厳守することで、Dell 製品に偽造コンポーネントが埋め込まれたり、ファームウェアやデバイスドライバーにマルウェアが挿入されたりするリスクを最小限に抑えます。デル・テクノロジーズは長年、製造施設と物流ネットワークのセキュリティ確立・維持のための多くの重要な慣行を、SDLの一環として実施しています。

Dell 製品の設計、製造、カスタマイズ、および注文の履行に使用される施設は、TAPA (Transported Asset Protection Association)、ASIS (American Society for Industrial Security)、ISO (国際標準化機構)、Business Alliance for Secure Commerce (BASC) が定義する、国際的に認められた物理セキュリティ基準に準拠していることを証明することが義務付けられています。

また、業界をリードする物流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保護するための防御と対策も講じられています。このプログラムでは、常時スタッフを配置したコマンドセンターが、世界中の厳選された入荷および出荷される貨物を監視し、貨物が目的地から別の目的地に中断なく届くことを確実にします。

デル・テクノロジーズはサプライヤーと施設の監査も行います。これには、デジタル閉回路テレビカメラの使用やアクセス制御システム、侵入検知、警備サービスのプロトコルなど様々な要素が含まれます。輸送と物流プロセスでの貨物の保護も行っており、不正開封防止梱包、貨物の施錠とセキュリティシール、主要な貨物レーンの脅威インテリジェンスの監視などが該当します。一部の貨物には IoT 追跡装置も配備し、リアルタイムのテレメトリーデータ監視を可能にして、輸送中に観察されたセキュリティ違反イベントをエスカレーションします。

また、当社は米国 C-TPAT (Customs-Trade Partnership Against Terrorism) のTier 3認証、カナダの PIP (Partners in Protection)、シンガポールの Secure Trade Partnership、その他数か国の AEO (Authorized economic Operator) など、安全な貿易・通商プログラムの認定を複数維持しています。いずれも、世界税関機構の加盟国により国際的に認知されたプログラムであり、民間での「クラス最高」のサプライチェーンセキュリティ基準を実証します。こうしたプログラムはサプライヤーの説明責任、セキュリティ管理

方針、密輸対策、人身売買規制、改ざん防止に重点を置き、国境を越えた貿易の安全を目的としています。

サプライチェーンの整合性は、製品が安全に配送され、お客様が受領した際に意図された通りに動作することを確実にします。サプライチェーン整合性における重要な機能は、ハードウェアとソフトウェアのベースライン仕様の開発です。この仕様書は安全に保存され、後に不正な変更がされていないことを確認するための基準として使用されます。

Secured Component Verification (SCV)

デル・テクノロジーズの Secured Component Verification (SCV) for PowerEdge は、お客様が受け取ったサーバーが、工場出荷時の構成と一致することを検証するサプライチェーン保証サービスです。Dell の工場は、特定のサーバーに固有のコンポーネント ID を含む証明書を生成します。この証明書は iDRAC 内の暗号化された安全な保管庫に保存されます。サーバーを受け取ると、お客様はホスト上で SCV アプリケーションを実行して、一意のコンポーネント ID を含む手元のシステムのインベントリを生成し、iDRAC に保存されている SCV 証明書のゴールデンファクトリー インベントリと照合できます。

SCV アプリケーションは、Dell 工場でインストールされたコンポーネントと納品されたものの不一致を特定するレポートを生成します。また、証明書と信頼の連鎖、および iDRAC の SCV 秘密鍵の所有証明も検証します。現状は直送のお客様が対象となり、VAR や部品交換のシナリオは含まれていません。

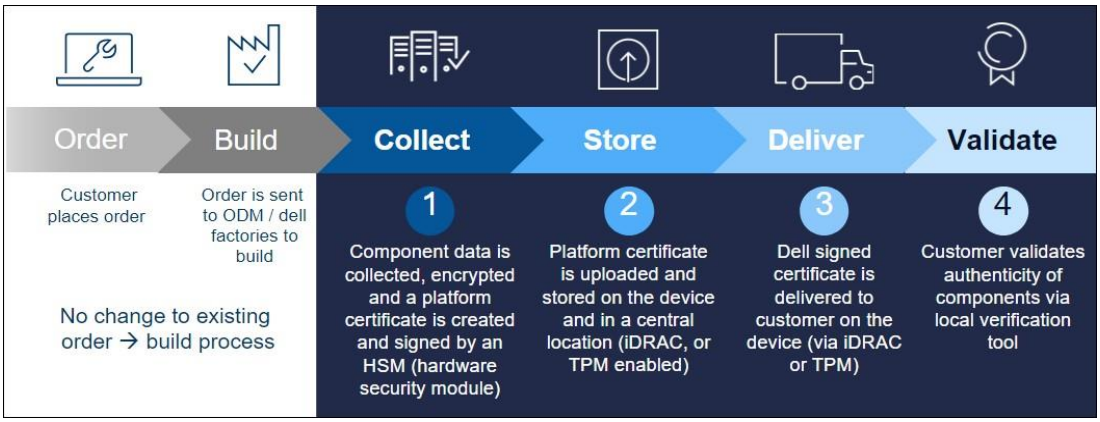


図3. Dell Secured Component Verification (SCV)

Software Bill of Materials

Dell のソフトウェア サプライチェーン セキュリティ管理と、NIST 準拠の一環、さらに大統領令14028に呼応する形で、当社は Software Bill of Materials (ソフトウェア部品表) をポートフォリオ全体のいくつか製品で提供しています。Dell の SBOM データは SPDX 規格 (Software Package Data Exchange) に準拠し、JSON形式で提供されます。SBOM データは、ソフトウェアサプライチェーンの透明性を提供し、お客様側の脆弱性スキャンや資産追跡ツールで使用できます。

SBOM はプラットフォーム上のソフトウェア コンポーネント、バージョン、ライセンスとオープンソース ソフトのより明快な理解を可能にし、既知の脆弱性の迅速な検知と、セキュリティの確保につなげます。

第3段階 - 大規模サーバー環境の効率的な導入と設定

課題

サイバー レジリエントなサーバーの設定と導入は、サーバーのライフサイクルにおける重要なステップです。このプロセスでミスや見落としがあると、サーバーのパフォーマンス低下やダウンタイム、さらにはセキュリティ侵害につながる可能性があります。サーバーの運用全般を通じてシステムとデータの整合性を確保するためには、適切な一連の管理とゲートが設置されていなければなりません。この設定と導入は、数百または数千のサーバーに対して実行しながら、一貫性を確保し、手作業によるミスを最小限に抑える必要があります。

PowerEdge のセキュリティ ソリューション

システムの整合性

システムの整合性の確保は、サーバーを保護し、ゼロトラスト運用のためのロックダウン体制を確立する基礎になります。この整合性は、サーバーのハードウェアとコンポーネントが本物であり、信頼できる承認済みの供給元からのものであるという保証から始まります。次に、ファームウェアとソフトウェアが悪意ある者に改ざんされていないことの確認が必要です。PowerEdge でシステムの整合性を担保するこのプロセスの起点は、シリコンベースのプラットフォーム ルートオブトラスト (RoT) です。この RoT が、サーバー プラットフォームの他のセキュリティ管理を固定し、サーバー上のハード ウェアとソフトウェア コンポーネントを暗号検証する信頼のチェーンを確立します。

暗号で検証されたトラステッド ブートのアンカーとしての*RoT*

サーバー セキュリティの最も重要な側面の1つは、ブート プロセスの安全性が確認可能であることです。このプロセスは、OS の起動やファームウェアの更新など、後続のすべての操作に信頼できるアンカーを提供します。

すべての PowerEdge サーバーには、工場出荷時にシリコンベースの不変のルートオブトラスト (ROT) が焼き付けられています。この RoT は、暗号検証や完全性の証明に使用できる、1回限りプログラム可能な読み取り専用の公開鍵を持っています。

BIOS ブート プロセスでは、ロードされる BIOS コードを暗号で検証する インテル Boot Guard もしくは AMD PSB が使われます。検証に失敗するとサーバーはシャットダウンし、Lifecycle Controller ログに通知されます。その後 IT管理者は BIOS リカバリーを開始できます。Boot Guard が 正常に検証されると、信頼のチェーンの手順によって残りの BIOS のモジュールが検証され、最終的に OSかハイパーバイザーへ制御が委譲されます。

Boot Guard の検証メカニズムに加え、iDRAC9 4.10.10.10 以降ではホストの起動時に BIOS イメージを検証する RoT メカニズムも提供されます。ホストは、BIOS イメージが正常に検証された後にのみ起動できます。iDRAC9 は、リアルタイム、オンデマンド、事前スケジュールで BIOS イメージを検証する仕組みも提供します。

暗号的に検証されたトラステッド ブート

PowerEdge サーバーは数世代に渡り、機密データを保存するための iDRAC 内の暗号化セキュア メモリーである iDRAC Credential Vault などの機能に、シリコンベースのセキュリティを使用してきました。ブートプロセスは、NIST SP 800-147B (BIOS Protection Guidelines for Servers）と NIST SP 800-155 (BIOS Integrity Measurement Guidelines) の推奨事項を満たすよう、シリコンベースの RoT で検証されてます。

コンポーネント認証のためのセキュリティ プロトコル データ モデル

デル・テクノロジーズが主要メンバーでもある DMTF (Distributed Management Task Force) は、Security Protocol Data Model (SPDM) を定めています。その SPDM は、サーバー コンポーネントの情報を収集するためのサーバー内の通信方法を一貫性がありオープンな基準で定義しています。iDRAC は SPDM の実装により、PERC12 や特定の NICコンポーネントを可視化できています。iDRAC は、PERC12 と NIC デバイスの ID、ファームウェア、および設定を暗号で検証してその信頼性と整合性を検証します。

TPM のサポート

PowerEdge サーバーは、2つのバージョンのTPMをサポートしています。

- TPM 2.0 FIPS + コモンクライテリア + TCG認証 (Nuvoton)
- TPM 2.0 中国 (NationZ)

TPM の使用により、公開キー暗号化関数の実行、暗号化ハッシュ関数の計算、キーの生成・管理・安全な格納・認証の実行が可能になります。インテルの Trusted Execution Technology (TXT) と Microsoft Windows Server 2016 の Platform Assurance もサポートされています。また、TPM は Windows Server 2012、2016、2022 の BitLocker ハード ドライブ暗号化機能も有効化します。

認証およびリモート認証ソリューションは、サーバーのハードウェア、ハイパーバイザー、BIOS、OS の起動時に TPM を使った測定を行い、それを暗号的に安全な方法で「ゴールデン」または「ベース」の測定値と比較します。これらの測定値は通常 TPM の外部、リモートの認証サーバー ソリューション内に格納されます。TPM に格納されている TPM PCR 測定値は、起動のたびに再計算されます。これが一致しない場合はサーバー システム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ーを無効にして切断できます。

サーバーは TPM ありでもなしでも注文できますが、昨今、多くの OS やその他のセキュリティ規定で TPM が標準になりつつあります。TPM は BIOS の選択で有効になります。プラグイン モジュールのソリューションであり、システムプラナー上にこのモジュール用のコネクタがあります。

ファームウェアの*UEFI* セキュアブート

PowerEdge は、OS 実行前にロードされる UEFI ドライバーやその他コードの暗号署名を照合する業界標準、UEFI セキュアブートもサポートしています。これはプリブート環境での業界全体のセキュリティ基準です。システム ベンダー、拡張カード ベンダー、OS のプロバイダーは相互運用性の促進の為にこの仕様に協力しています。

UEFI セキュア ブートを有効にすると、署名されていない (つまり信頼されていない) UEFI デバイス ドライバーが読み込まれるのを防ぎ、エラー メッセージを表示し、デバイスを機能させません。署名されていないデバイス ドライバーをロードするには、セキュアブートの無効化が必要です。

第14、15、16 世代の PowerEdge は、カスタマイズされたブート ローダー証明書を使うという、独自の柔軟性も提供しています。この証明書は主に、Linux 環境の管理者が Microsoft の UEFI 認証局 (CA) により提供されるデフォルトの署名証明書に依存せず、独自の OS ブート ローダーに署名するための機能です。カスタム証明書は任意の iDRAC API を使ってアップロードでき、お客様はそれを用いて特定の OS ブート

ローダーを認証できます。PowerEdge のこの UEFI カスタマイズ機能は、NSA により、サーバーの Grub 2 の脆弱性を緩和する手法として引用されています[4]。PowerEdge は Microsoft、VMware、および UEFI CA が提供する、すべての業界標準証明書の削除を含む、セキュアブートの完全なカスタマイズをサポートしています。

インテル Boot Guard および AMD PSB

インテル Boot Guard と AMD PSBは、Dell OEM により承認されていないファームウェアがシステム上で実行されることを防ぎ、ファームウェアの整合性を強力に保証する、ホスト プロセッサー機能です。こうした機能を追加の多層防御手段として有効にすることで、フラッシュメモリーの交換や再プログラミング、Time-of-Check-Time-of-Use (TOCTOU) 競合といった、特定のクラスの物理攻撃リスクを軽減できます。システム内の RoT 機能をすべて組み合わせることで、トラステッドコンピューティングベース (TCB) の侵害を困難なものにします。

iDRAC/BMC

iDRAC (integrated Dell Remote Access Controller) は、Dell PowerEdge サーバーに内蔵されているベースボード管理コントローラ (BMC) です。iDRAC は、多くの一般的な管理機能に対して安全なリモートサーバーアクセスを提供します。管理者はエージェントを使用せず、帯域外の任意の場所から Dell サーバーを導入、管理、監視、更新、トラブルシューティングおよび修復できます。

iDRAC は業界トップクラスのセキュリティ機能を提供しており、よく知られている NIST 標準、コモンクライテリア、FIPS 140-2 に準拠し認定されています。エンドユーザーは iDRAC9 を介してセキュリティ機能を設定し、システムのセキュリティ体制を最大限に高めることができます。

iDRAC Credential Vault

iDRAC サービスプロセッサーは、iDRAC ユーザー認証情報や自己署名 SSL 証明書の秘密鍵などの機密データを保護する、セキュアなストレージ 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であるこのメモリーは、製造時に各 iDRAC チップにプログラムされる一意の不変のルートキーで暗号化されています。このメモリーは、攻撃者がデータにアクセスするためにチップを破壊する物理的な攻撃から保護されます。

SELinux フレームワーク

SELinux は iDRAC のコア カーネル レベルで動作するため、ユーザー入力や設定は必要ありません。攻撃が検出されると SELinux はセキュリティメッセージをログに記録します。このログメッセージは、攻撃者がいつ、どのようにシステムに侵入しようとしたかを示します。そのログは SupportAssist を通じて登録済みのお客様に提供されます。今後の iDRAC リリースでは、このログが Lifecycle Controller ログでも利用可能になる予定です。

工場出荷時に生成されるデフォルト パスワード

第14、15、16世代の PowerEdge はすべて、セキュリティ強化のために一意の iDRAC パスワードを工場で生成して出荷されるのがデフォルトです。このパスワードは、シャーシ前面の資産ラベル横にある引き出し式のサービスタグに記載されます。このデフォルトオプションを選択した場合、iDRAC への初回ログイン時はこのパスワードを使います。セキュリティ上の理由から、当社はデフォルトのパスワードの変更を強くお勧めしています。

[4] CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF (defense.gov)

ハードウェアのセキュリティ

ハードウェア セキュリティは、包括的なセキュリティ ソリューションに欠かせない要素です。一部のお客様は、USB などのサーバー外付けポートへのアクセスを制限したいと考えています。一般的に、本番稼動開始後にサーバー シャーシを開ける必要はありません。少なくとも、お客様は常にそのような行為を追跡し、ログに残すことを望んでいます。この分野における目標は、総じて、サーバーへの物理的な侵入の阻止と制限です。

シャーシ侵入検知およびアラート

PowerEdge サーバーは、ハードウェア侵入検知とロギング機能を備えており、AC電源の入っていない時でも検出が機能します。製品の輸送中でも誰かがシャーシを開いたり改ざんしたりすると、シャーシのセンサーが検知します。輸送中に開かれたサーバーは、電源投入後に iDRAC ライフサイクルログにエントリーを生成します。

USBポートの動的な管理

セキュリティをより強化するため、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オプションもあります。例えば、本番使用時は USB ポートを無効にしておき、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にする、といった運用も可能です。

iDRAC Direct

iDRAC Direct は iDRAC サービスプロセッサーに配線された特別な USB ポートです。サーバー設置場所で前面 (コールドアイル) からデバッグと管理を可能にします。標準的な Micro-AB USB ケーブルをこのポートに、もう一方 (Type A) を PCに接続すれば、標準的なブラウザで iDRAC GUI にアクセスし、広範なデバッグと管理もできます。iDRAC Enterprise ライセンス適用時は仮想コンソールからOSデスクトップにアクセスできます。

iDRAC Direct はログインに iDRAC 認証情報を使うため、安全なクラッシュカートとして機能します。広範なハードウェア管理とサービス診断ができるという利点もあります。この手法は遠隔地のサーバーの物理的アクセスのセキュリティ確保の魅力的なオプションです。(この場合、ホスト USB ポートと VGA 出力は無効にできます。)

iDRAC Connection View と位置情報

Connection View を利用すると、サーバーの I/O に接続されている外部スイッチとそのポートを、iDRAC がレポートできるようになります。この機能は一部のネットワークデバイスで使えます。接続元のスイッチでは LLDP (Link Layer Discovery Protocol) が有効になっている必要があります。

Connection View の使用には以下の利点があります。

- サーバーの I/O モジュール (LOM、NDC、アドインPCIeカード) が正しいスイッチとポートに接続されているかどうかをリモートで迅速に確認できます。
- 配線ミスを修正するために、コストのかかるリモートからの技術者の派遣が不要になります。
- サーバー ルームのホットアイルで対象のケーブルを探す手間が省けます。
- GUI にアクセスするか、RACADM コマンドを使用して、すべての接続情報を取得できます。

Connection View には時間とコストの節約に加え、物理サーバーや VM のリアルタイム位置情報の取得というメリットもあります。管理者は iDRAC Connection View を利用してサーバーをピンポイントで特定し、サーバーがどのスイッチとポートに接続されているかを確認できます。この情報は、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が接続されることを防ぐのに役立ちます。

Connection View は、サーバーが接続されているスイッチ ID を報告することで、間接的にサーバーの場所を検証します。スイッチ ID は地理的な位置を特定し、サーバーが許可されていないサイトの不正なサーバーではないことを保証するのに役立ち、物理的なセキュリティに追加のレイヤーを提供します。また、この情報はアプリケーションや VM が国境を「越えて」おらず、承認された安全な環境で実行されていることの検証にもなります。

保存データの保護

保存データの保護により、ストレージに存在する機密データは、暗号化と外部キー管理によって不正アクセスから保護されます。

デル・テクノロジーズは以下を提供します。

- ソフトウェアベースの暗号化 (仮想デバイスなど)
- エンタープライズキー管理 (例：SED デバイスや鍵管理)
- ハードウェア ドライブの暗号化 (SED デバイスなど)

社内のポリシーによるものであれ社外のコンプライアンスによるものであれ、データの保護は、あらゆる規模の企業にとって、引き続き最優先事項です。

データを保護するために、PowerEdge の第14、15、16 世代では、以下のように複数のストレージ ドライブオプションを提供しています。

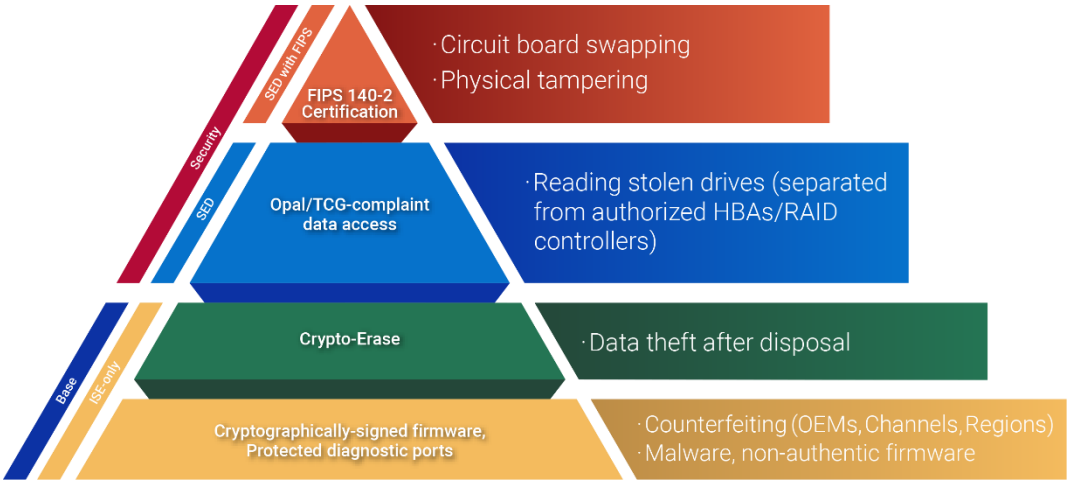


図1. ストレージデバイスの選択肢

まずは、ユーザーデータを瞬時かつ安全に消去する新技術、Instant Secure Erase (ISE) をサポートするドライブから選択肢は始まります。第14、15、16 世代の PowerEdge サーバーでは、標準で ISE 対応ドライブが選べます。この文書では ISE の詳細は、System Erase 機能の一部として後述します。

第3段階 - 大規模サーバー環境の効率的な導入と設定

次にセキュリティの高い選択肢は自己暗号化ドライブ (SED) です。ストレージドライブのロック保護をサーバーや RAID カードにバインドして提供します。この方法は、いわゆる「スマッシュ&グラブ」によるドライブの盗難とそれに伴う機密性の高いユーザーデータの損失を防御します。窃盗犯がドライブを使おうとしても必要なロックキーの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は阻止されます。以下で説明する Secure Enterprise Key Manager (SEKM) を利用すれば、サーバー自体の盗難に対する保護もできます。

NIST FIPS 140-2 認定の SED は最高レベルの保護を提供します。この規格に準拠したドライブはテスト機関からも認定され、改ざん防止ラベルも貼られています。Dell SED はすべて FIPS 140-2 認証済みです。

Secure Enterprise Key Manager

OpenManage Secure Enterprise Key Manager (SEKM) は、企業全体で保存データを管理する一元的な鍵管理ソリューションです。外部の鍵管理サーバー (KMS) の利用により、サーバー内のストレージ デバイスのロックとその解除に使う鍵をiDRAC が管理できます。iDRAC は、特別なライセンスでアクティブ化された組み込みコードを使い、KMS に各ストレージコントローラの鍵の作成を要求します。iDRAC はホストの起動のたびにこの鍵を取得してストレージコントローラに提供し、コントローラが SED のロックを解除をできるようにします。

ローカル鍵管理 (LKM) と比べた場合の、SEKM の利点は次のとおりです。

- 鍵はサーバーには保存されず外部に保存され、接続されたPowerEdge サーバーノード (iDRACを活用) から取得されるため「サーバーの盗難」に対する防御が可能
- 高可用性を備えた暗号化デバイスの、一元化・中央化されたスケーラブルな鍵管理
- 業界標準 KMIP (Key Management Interoperability Protocol) のサポートにより、他の KMIP 互換デバイスの利用も可能
- ドライブまたはサーバー全体が危険にさらされた場合でも、保存データを保護
- ドライブ数に応じて拡張可能なオンドライブの暗号化パフォーマンス

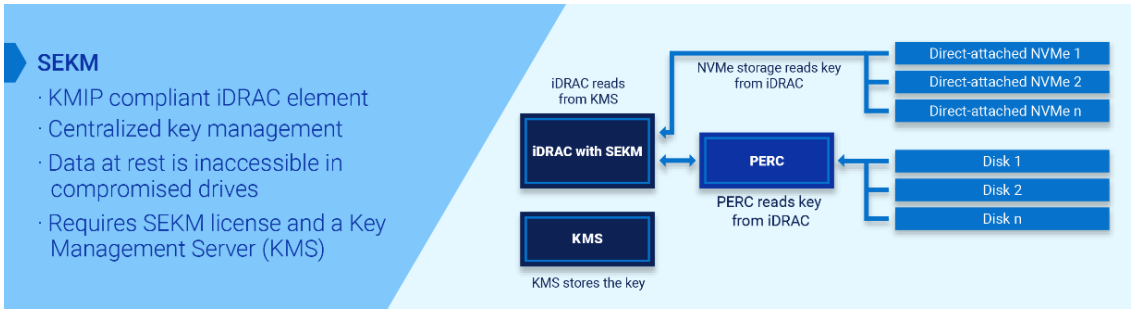


図2. Secure Enterprise Key Manager (SEKM)

ローカル鍵管理

Dell PowerEdge サーバーでは、ローカル鍵管理 (LKM) により、PERCコントローラに接続された SED ドライブを保護できます。

ドライブが盗難された場合にユーザーデータを確実に保護するには、SED は別の鍵でロックされ、その鍵が提供されない限りユーザー データは復号化されないようにする必要があります。この鍵は

鍵暗号化鍵 (KEK) と呼ばれます。KEKは、外部サーバーではなく PERC 上に保存されます。

SED が接続されている PERC コントローラに keyId/パスフレーズを設定します。次に、PERC コントローラは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。ドライブに通電すると、ロックされた SED として起動し、PERC が KEK にロック解除の許可を与えた場合にのみ、ユーザーデータを暗号化または復号化します。ロックされたドライブを盗んでも攻撃者は KEK を提供できず、ユーザーデータは保護されます。次の図は、LKM ソリューションを示しています。

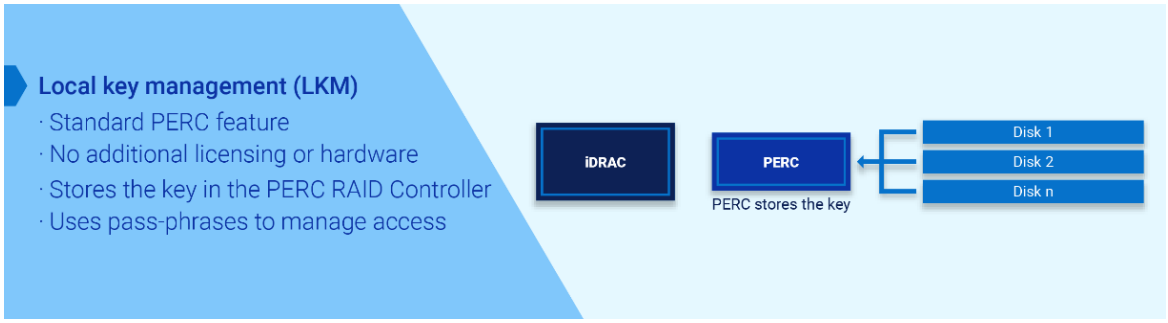


図3. ローカル鍵管理 (LKM)

iLKM

PERC RAID コントローラが使われない直接接続式の NVMe では、iDRAC をキーマネージャとして使用できます。OpenManage iLKM と呼ばれるこのソリューションは iDRAC ベースで、ローカルでの鍵交換が可能です。iDRAC はキーマネージャーとして機能し、ストレージデバイスの保護に使える認証キーを生成します。iDRAC ベースの iLKM から、iDRAC ベースの SEKM への移行、すなわち、外部鍵管理へのアップグレードも可能です。次の図は、iLKM ソリューションを示しています。

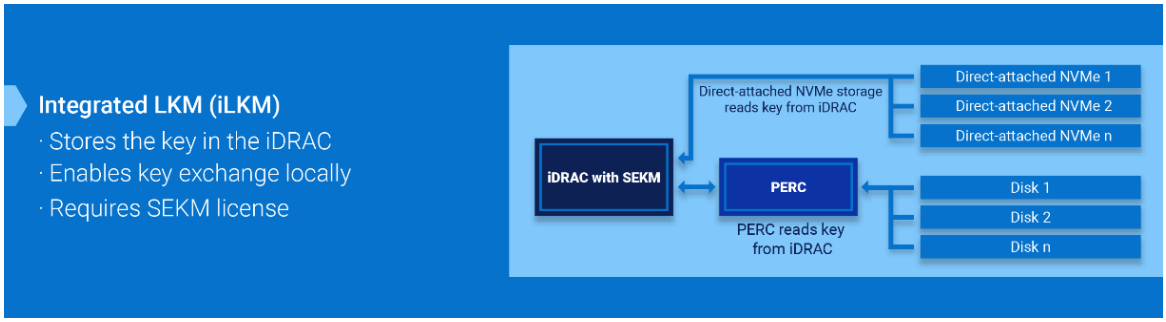


図4. Integrated Local Key Management (iLKM)

転送中のデータの保護

転送中のデータの保護は、データがネットワークやシステム間を移動する際に不正な開示や傍受されるリスクから確実に保護します。機密データは転送中に傍受・盗難・変更されるリスクがあり、データ侵害、知的財産の損失、その他のセキュリティリスクにつながります。

データがシステム間やネットワーク間で絶えず移動する分散型およびクラウド環境では、暗号化とアクセス制御によるデータ保護が、ゼロトラスト環境における転送中のデータの保護の重要な要素となります。

TLS 1.3

iDRAC web サーバーは、TLS/SSL 証明書を使用してリモートクライアントとの安全な通信を確立し、維持します。Web ブラウザや RACADM や WS-Man などのコマンドラインユーティリティは、この TLS/SSL 証明書を使用してサーバー認証を行い、暗号化された接続を確立します。

TLS/SSL 証明書を使用してネットワーク接続を保護するには、いくつかのオプションがあります。iDRAC の webサーバーには、デフォルトで自己署名 TLS/SSL 証明書があります。自己署名証明書は、カスタム証明書、カスタム署名証明書、またはよく知られた認証局 (CA) により署名された証明書に置き換えることができます。どの方法を選択しても、iDRAC が設定され TLS/SSL 証明書が管理ステーションにインストールされている場合、TLS/SSL 対応クライアントは証明書の警告なしで安全に iDRAC へアクセスできます。

SSH

iDRAC では、SSH デーモンの暗号化設定をユーザーが制御できるため、環境に最適な設定を決定できます。ユーザーに与えられるコントロール権限は、設定の緩和ではなく、この機能で各オプションに設定された値を変更して、より狭く厳格な暗号化ポリシーを実現することです。つまり、オプションから値を削除できるのみで、デフォルトの値セットで定義され許可されている値以外の値を追加することはできません。

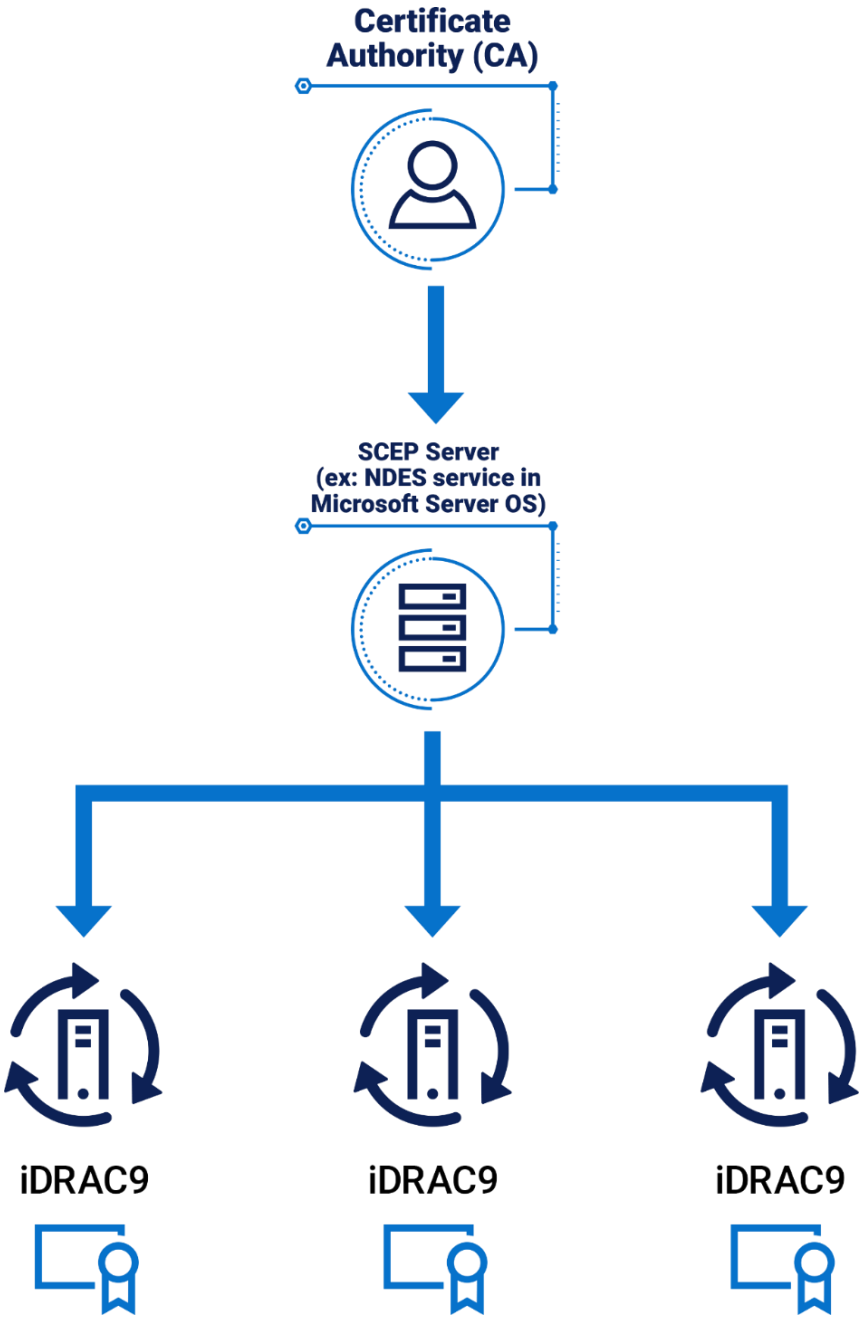
暗号化ポリシーは、次のオプションを使用して構成されます。

- 暗号 - Ciphers
- ホスト鍵アルゴリズム - HostKeyAlgorithms
- 鍵交換アルゴリズム - KeyExchangeAlgorithms
- メッセージ認証符号 (MAC) - MACs

通常、これらの各オプションの値は様々な環境に対応するセキュリティのベスト プラクティスを反映して、慎重に設定されます。そのため、これらのオプションの iDRAC デフォルト設定は、SSH パッケージのオープン ソース コミュニティによって割り当てられたオプションと同じです。これらの設定は RACADM コマンドラインインタフェースを使用して構成できます。『iDRAC RACADM CLI ユーザーズガイド』を参照してください。

自動証明書登録

iDRAC9 v4.0 以降では、SCEP (Simple Certificate Enrollment Protocol) をサポートするクライアントが追加されています。利用には iDRAC 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の証明書を管理するために使用される標準プロトコルです。iDRAC は、Microsoft ServerNDES サービスなどの SCEP 互換サーバーと統合して、SSL/TLS 証明書を自動的に維持できるようになりました。この機能は、期限切れ間近の Web サーバー証明書を登録し、更新するために使用できます。サーバー構成プロファイルを使用して iDRAC GUI で証明書を1対1で設定することも、RACADM などのツールを使用してスクリプトを提供することも、どちらも可能です。



iDRAC 暗号スイートの選択

暗号スイートの選択 は、Web ブラウザが iDRAC との通信に使用できる暗号を制限するために使用できます。接続のセキュリティを決定することもできます。これらの設定は、iDRAC Webインターフェース、RACADM、および Redfish を使用して構成できます。この機能は、iDRAC7、iDRAC8（2.60.60.60 以降）、現在の iDRAC9（3.30.30.30 以降）の複数の iDRAC リリースで利用可能です。

Commercial National Security Algorithm (CNSA) のサポート

TLS1.3 ビット および 256ビット暗号化で iDRAC9 がサポートする暗号は次の図のとおりです。使用可能な暗号には、CNSA 承認セットの暗号が含まれます。

```
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 2048 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA       DHE 2048 bits
```

iDRAC 接続を保護するためのヒント

最も安全なネットワーク接続は iDRAC の専用 NIC です。物理的に本番ネットワークから分離されたネットワークに接続できるからです。この方法では、iDRAC 管理トラフィックは本番ネットワークから物理的に分離されます。iDRAC の専用 NIC が使用できない場合は、VLAN を有効にして共有 LOM モードで iDRAC を実行可能ですが、iDRAC の管理トラフィックは、本番ネットワークと同じ接続で送信されます。もし共有 LOM モードで VLAN が使えない場合は、強力なパスワードや各種セキュリティ対策で iDRAC へのアクセスを保護することが必須です。詳細については『 iDRAC Security Configuration Guide 』を参照してください。

IEEE.802.1x

PowerEdge では、ポートベース認証を提供するネットワークプロトコルの標準規格、IEEE 802.1x が有効化されています。LAN か WLAN へアクセスを求めるデバイスは、承認される前に認証・検証される必要があります。

ドメインの分離

PowerEdge サーバーの第 14、15、16 世代は、マルチテナントのホスティング環境で重要な機能となるドメイン分離の活用で、さらなるセキュリティ強化が可能です。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保護のため、テナントによる再構成をブロックしたい場合があります。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 やインテルのマネジメント エンジン、イノベーション エンジンといった、チップセットの機能にアクセスできないようにする設定オプションです。

使用中のデータの保護

メモリー内で使用されているアプリケーション データを保護することは、ますます重要になっています。使用中のデータは、それが機械学習データセットであろうと、マルチテナント環境のようにメモリー内に秘密を保持することに関連していようと、メモリーの内容またはアクセスバスに侵入可能性のある脅威ベクトルに、脆弱になる可能性が

あります。使用中のデータの保護は、昨今増えている、メモリー上の大規模データセット上で動作する計算の保護に欠かせません。さらに、データ上で実行されるコードは信頼でき改ざんされていない必要があります。使用中のデータに対して、信頼できるコード実行環境と信頼できないコード実行環境を分離する機能が必要です。

コンフィデンシャル コンピューティング向けの CPU テクノロジーの開発により、セキュアなエンクレーブがハードウェア層でアプリケーションデータを保護できるようになり、より包括的なデータ保護戦略が可能です。第15世代以降の PowerEdge はインテル SGX/TME および AMD SEV/SME などの CPU テクノロジーを備えています。

AMD のコンフィデンシャル コンピューティング機能

AMDは、第1世代 AMD EPYC プロセッサーで Secure Encrypted Virtualization (SEV) を導入しました。この機能はシステム メモリ全体と個々の仮想マシン (VM) のメモリーを暗号化し、VM メモリーをハイパー バイザーから分離します。AMD は EPYC プロセッサーの世代ごとにSEV を強化しており、現在はプロセッサーのみが認識する最大509 の暗号化キーの1つで VM を暗号化して、プライバシーと整合性を保護する機能を備えています。この鍵は、メモリーコントローラ内の 128 ビット AES 暗号化エンジンを利用したメモリーの暗号化に使われます。ハイパーバイザーは、AMD セキュアプロセッサーの助けを借りてメモリーコントローラ内の鍵を管理します。以下に、AMD Infinity Guard テクノロジー ソリューション スイートに含まれる、様々なユースケースと導入パターン、脅威モデルに対応した主要な AMD SEV テクノロジーを挙げます。

- AMD の SME テクノロジーは、システム メモリーを暗号化するために単一のキーを使用することを指します。
- AMD SEV は、VM ごとに 1 つのキーを使用して、ゲストとハイパーバイザーを互いに分離します。
- AMD SEV-ES は、VM の実行停止時にすべてのCPUレジスタの内容を暗号化して、CPU レジスタからハイパーバイザーへの情報漏えいを防止します。
- AMD SEV-SNP は強力なメモリ整合性保護を追加し、データ リプレイ攻撃やメモリ リマッピング攻撃などのハイパーバイザー ベースの攻撃を防止します。

インテルのコンフィデンシャル コンピューティング機能

第3世代のインテル Xeon プラットフォームからいくつかの重要なセキュリティ イノベーションが導入されています。TME (Total Memory Encryption) は CPU からアクセスされるメモリーの確実な暗号化に使えます。すべてのメモリーを暗号化することで、既存のソフトウェア アプリケーションは変更なくシステム メモリーの保護を強化します。

インテル TME は、お客様の資格情報、暗号化キー、外部メモリー バスに関するその他の知的財産や個人情報など、インテル CPU からアクセスされるすべてのメモリーの確実な暗号化に役立ちます。インテルは、液体窒素を吹き付けて DIMM を取り外し読み取ったり、専用の攻撃用ハードウェアを設置したりするようなハード ウェア攻撃に対するメモリー保護の強化のために、この機能を開発しました。NISTのストレージ暗号化規格、AES XTSを利用し、ソフトウェアに触れることなく、プロセッサー内の強化された乱数発生器を使用して暗号化キーが生成されます。既存のソフトウェアを変更せずに実行しながら、メモリーをより適切に保護できます。

IDアクセス管理

アイデンティティとアクセス管理 (IAM) は、デジタルID を管理し、不正アクセスを制限するために要求者の情報やリソースへのアクセスを適切なレベルと適切なタイミングで制御することにより、認証と承認を提供する 一連のセキュリティ管理です。IAM フレームワークには、単純なパスワードに比べて次のような利点があります。

- **セキュリティの強化** - シングル サインオン (SSO) サービス、多要素認証 (MFA)、特権アクセス管理などの様々なツールを含み、セキュリティを強化するとともに脆弱なパスワードによるリスクを回避します。強力な認証、アクセス制御、監視、ユーザー教育を実施することで、フィッシングやソーシャル・エンジニアリング攻撃から組織を保護する上で重要な役割を果たします。これにより、組織が攻撃対象領域を減らし、脅威に対して効果的に対応できるよう支援します。
- **パスワード漏洩の削減** - MFAと追加のセキュリティレイヤーを使用して、フィッシング、ソーシャルエンジニアリング、ブルートフォース攻撃による認証情報の盗難を阻止します。
- **きめ細かなアクセス制御** - ロールベースのアクセス制御 (RBAC) と属性ベースのアクセス制御 (ABAC) によってユーザーのアクセス権限をきめ細かく制御し、必要なリソースとデータにのみにアクセス可能にします。
- **一元管理** - ユーザーアカウントとアクセスポリシーを管理することで、組織への参加、組織内での移動、または組織からの脱退に伴うユーザーの管理を容易にします。
- **監査とログ記録** - ユーザーの行動を監視し、不審なアクセス試行を特定して修正します。
- **拡張性** - ユーザー数とリソースの増加に対応します。
- **法規制の遵守** - 法的な影響を回避するため、規制要件を遵守します。
- **ユーザー エクスペリエンス** - SSO サービスとパスワード管理を提供し、ユーザーが 1つの認証情報を使用して複数のアプリケーションやサービスにアクセスできるようにします。
- **適応型認証** - リスク要因を評価することで、追加のセキュリティ対策を適用します。
- **緊急アクセスと復旧** - セキュリティ制御を維持しながら、重大な状況に対する一時的な緊急アクセスを許可します。
- **統合** - 様々なシステム、アプリケーション、クラウドサービスと統合し、ITエコシステム全体でシームレスなアクセス管理を実現します。

IAM はすべての企業にとって、技術的要件から規制上の要件にまで及ぶITの広範な課題として、セキュリティとレジリエンスを強化するための戦略的なビジネス上の必須事項です。ゼロトラスト アーキテクチャ (ZTA) は、あらゆるレベルのインフラを保護するための標準的な選択肢として登場し、ZTA の基盤となる部分です。ゼロトラストの非公式なマントラは「決して信用せず、常に検証せよ」であり、検証できなければ信頼はできません。IAMは、その検証を提供します。

強力なサイバーセキュリティのフレームワークとゼロトラストの原則の採用と実施の基礎となるのが ID です。これは、人だけでなく、アプリケーション、通信経路、ネットワーク デバイスおよびデータ自体の識別を指します。組織が強力な ID 認証付与およびアクセス管理 (ICAM) を実践していない場合、根本的なセキュリティの実践が危険にさらされます。効果的な ID およびアクセス ソリューションには、ユーザーのログイン詳細の取得と保存、ユーザー アクセス資格情報の割り当てと取り消しを容易にし、ユーザーのロールとそのレベル、アクセス権限を網羅した、一元的なエンタープライズ データベースの監視に必要なツールと制御が含まれていなければなりません。少なくとも、アクセスは、組織が定義した必要な機能を容易にするためにのみ許可されなければなりません。たとえば、ユーザーは、データ、アプリケーション、サービスへのアクセスと権限を、自分の職務で定義されたことを実行する為にのみ、持たなければなりません。各ロールが確実に維持され、そのロールであっても、データ活用に関する組織の目標に反する行動がとられていないことを確認するための、プラクティスとツールの導入が必須です。

MFA - スマートカード (CAC/PIV)

スマートカード用 MFA (CAC/PIV) は、共通アクセス・カード (CAC) および個人識別検証 (PIV) カードを含む汎用的な証明書認証です。証明書認証は、クライアント ID 証明書を使用してユーザー認証をします。これは主に、連邦業界と連携する政府または組織で使用されます。

MFA - RSASecurID

システム上でユーザーを認証するもう一つの手段が RSA SecurID です。iDRAC9 では2つめの二要素認証として、Datacenter ライセンスとファームウェア 4.40.00.00 以降で、RSA SecurID がサポートされています。

認証のためのディレクトリの統合

ユーザーとドメイン管理の一元化のため、iDRAC は LDAP (Lightweight Directory Access Protocol) や Active Directory などの特権管理ツールへの統合も可能です。ディレクトリ サービスにより、ユーザー インベントリの管理やユーザー アカウントのアクセス制御ならびに設定の割り当てを、一元的な場所でより簡単に行えます。

iDRAC では、LDAP を使用してユーザーとグループを認証できます。LDAP ディレクトリサービスの設定には、config コマンドで cfgLdap グループと cfgLdapRoleGroup グループのオブジェクトを使用します。また、iDRAC.LDAP および iDRAC.LDAPRole グループのオブジェクトは、set コマンド 12 でも使用できます。

Active Directory への統合は、iDRAC で LDAP over SSL (LDAPS) を設定して Active Directory ドメインコントローラと通信します。有効な証明書がドメインコントローラーにインストールされ、ポート 636から DC への SSL接続の確認後、iDRAC/OME のディレクトリサービス統合テストを行いドメインコントローラーと通信します。

SSO (シングルサインオン)

iDRAC は SSO をサポートしており、ユーザーの再チャレンジや再認証なしで、検証済みの認証情報や識別情報を複数ドメイン間で共有できます。SSO により、認証された OS 管理者は、別の iDRAC 管理者認証情報でのログインなしに直接 iDRAC Webインターフェースにアクセスできます。以下のプロトコルが利用できます。

- **OpenID connect** はオープン規格で分散型の認証プロトコルであり、通常は M2M (Machine-to-Machine) 的な RestAPI に利用されます。

- オープン基準の **Security Assertion Markup Language (SAML)** は通常、UI の SSO に使われます。

ロールベースのアクセス制御

ロールベースのアクセス制御 (RBAC) は、アクセス制御の最も一般的な形態です。権限はロールでグループ化され、通常はグループに割り当てます。ユーザーとグループへの権限付与は、Active Directory で管理されます。

特定の権限 (iDRAC を使用してシステムを管理し、システム セキュリティを維持するためのロール・役割ベースの権限) を持つユーザーアカウントを設定できます。デフォルトでは iDRAC はローカル管理者アカウントで設定されています。デフォルトの iDRAC ユーザー名とパスワードはシステムタグに付属しています。管理者は他のユーザーが iDRAC にアクセスできるようにユーザーアカウントを設定できます。詳細はマニュアルを参照してください。

ローカルユーザーの設定も、Microsoft Active Directory や LDAP などのディレクトリサービスを使ったユーザーアカウントの設定もできます。ディレクトリサービスの利用で、承認されたユーザー アカウントを一元管理できます。

iDRAC では、関連する一連の権限を持つユーザーへのロールベースのアクセスがサポートされています。役割には、管理者、オペレータ、読み取り専用、または「なし」があります。ロールは利用可能な最大権限を定義します。

時間ベースのアクセス制御

時間ベースのアクセス制御は、セキュリティを強化し、厳重に管理・監視された環境で、機密データ、設備、システムへのアクセスを管理できる、価値あるツールです。例えば、技術者がサーバーの USB ポートに物理的にアクセスする必要がある場合、iDRAC 管理者はそのアクセスを特定の時間で有効・無効化できます。

スコープベースのアクセス制御

スコープベースのアクセス制御は、ユーザーベースやロールベースのアクセス制御よりもきめ細かい制御を提供します。エンティティがリソースへのアクセスを試みると、管理者は、複数パターンのアクセス許可に基づくポリシーを評価して適用できます。たとえば、リソースの場所や IP アドレスの範囲などに基づいてアクセスを制限できます。

大規模導入を効率化する機能とオートメーション

iDRACによるゼロタッチ自動化 - サーバー構成プロファイル

ゼロタッチ プロビジョニングは、iDRAC Enterprise または Datacenter ライセンスで利用できます。ゼロタッチ プロビジョニングはすべてのハードウェア構成、証明書のインストール、リポジトリ ファームウェアの更新、OS 導入を自動化します。IT 管理者はセキュリティ設定を事前に構成し、均一なサーバーイメージを確保できます。ゼロタッチ プロビジョニングは、iDRAC サーバー構成プロファイル機能と OpenManage Enterprise で利用できます。

CloudIQ

CloudIQ は、企業全体のサーバーの健全性とサイバーセキュリティを監視し、そのパフォーマンスを予測することで、ビジネスに影響が及ぶ前に、プロアクティブに問題に対処できるようにします。

CloudIQ は、BIOS、iDRAC、NIC、PERC、ドライブ、サポートされている周辺機器など、PowerEdge サーバーからファームウェアの詳細を収集するためのシンプルで直感的なソリューションを提供します。最近のOpenManage Enterprise (OME) と CloudIQ には、更新が必要な BIOS とファームウェアを識別する機能があります。

CloudIQ は、現在インストールされているバージョンを報告し、利用可能な Dell の最新リリースと比較し、アップデートをスケジュールできます。この情報は、エージェント不要の iDRAC により各サーバーから 収集されて OME に統合された後 CloudIQ に転送されて処理されます。この強力な機能には、OME とCloudIQ の両方に統合されたユーザー権限も含まれるため、これらのコマンドは許可されたユーザーのみが実行できます。

また、CloudIQ は複数の OME インスタンスを1つのサーバーフリート管理ビューに統合できます。

第4段階 - セキュリティ管理と監視

課題

見えないものを守ることはできません。攻撃は、人間が検知して対応できるよりも速く、迅速に発生します。ダイナミックで複雑な脅威環境の中で、重要な資産をリアルタイムで保護することは困難です。また、スキルとリソースの不足が問題をさらに悪化させています。IT 管理者がその環境において継続的な課題に直面する中、さらなる自動化、より少ないタスク手順、より直感的な操作を通じて、インフラストラクチャーをより簡単に管理することが、管理者の生産性向上の鍵となります。

不利な結果に左右されることなく、ビジネスは常にレジリエンスを維持することが重要です。以下のように、検知、対応、回復に機敏であり続けなければなりません。

- オブザーバビリティと透明性により、効果的なセキュリティイベントの認識とタイムリーな修復を実現。
- スキルやリソースの不足が問題を増大：インフラ (ユーザー、デバイス、データ、ネットワーク、アプリケーション) 全体の活動を監視しパターンと異常を特定。セキュリティ脅威の検出と対応にアナリティクスを活用。
- 自動化が重要。
- イベント、アクティビティ、挙動を分析してコンテキストを導き出し、AI/MLを適用してリアルタイムにアクセス決定を行う際の検出時間・応答時間を改善するモデルを実現。簡素化はレジリエントなインフラの基礎。

PowerEdge のセキュリティ ソリューション

Dell の管理ポートフォリオは、管理者のタスクを簡素化します。自動化とインテリジェンスの活用でセキュリティと健全性監視を向上し、自信を持ってセキュリティを拡張できます。監視とロギングはゼロトラストの重要な要素です。

可視性、ロギング、アラート

サーバー システムの構成、健全性ステータス、および変更イベントを完全に可視化する検出機能を持つことが重要です。この可視性は、ブートおよび OS のランタイムプロセスにおける BIOS、ファームウェア、およびオプション ROM に対しての、悪意ある変更やその他の変更も検出しなければなりません。プロアクティブなポーリングは、システム内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、サーバーへのアクセスと変更に関する完全な情報を提供しなければなりません。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ことです。

Dell OpenManage Enterprise (OME) では、ポリシーを一度アラートに設定すると、その後のアラートに自動的に適用されます。また OME は、一度に多数のサーバーにテンプレートを適用できます。OME ソリューションは、管理者がポリシーを作成後、アラートに基づくアクションを自動化することで、最終的に時間と労力を節約します。

テレメトリー

iDRAC9 v4.00.00.00ファームウェア と Datacenter ライセンス以降、IT管理者は高度なサーバーハードウェア稼働テレメトリーを既存の分析ソリューションに統合できます。テレメトリーは、ストリーミングまたはプッシュされる粒度の細かい時系列データとして提供されます。iDRAC9 の高度なエージェントフリーアーキテクチャは、サーバーと周辺機器の稼働に関する 180 を超えるデータ メトリクスを提供します。メトリクスは正確にタイムスタンプされて内部的にバッファリングされるため、最小限のネットワーク負荷で非常に効率的なデータストリームの収集と処理が可能です。この包括的なテレメトリーを分析ツールに入力して、障害イベントの予測、サーバー運用の最適化、サイバーレジリエンスの強化ができます。iDRAC9 テレメトリストリーミングは 1台または複数の PowerEdge サーバーから、ライブシステムデータを収集し、集中型コレクターにストリーミングします。

iDRAC Lifecycle ログ

Lifecycle ログは時間の経過とともにサーバーで発生するイベントのコレクションです。イベントの説明、タイムスタンプ、重大度、ユーザー ID またはソース、推奨アクションが表示されます。この技術情報はセキュリティ追跡やその他のハードウェア警告に役立ちます。

Lifecycle Controller Log (LCL) には、以下のような様々な種類の情報が記録されます。

- システムハードウェアコンポーネントの設定変更
- iDRAC、BIOS、NIC、RAID の設定変更
- すべてのリモート操作のログ
- デバイス、バージョン、日付に基づくファームウェア更新履歴
- 交換されたパーツに関する情報、故障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の 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

アラート

iDRAC では、Lifecycle ログイベント発生時に実行される様々なイベントアラートとアクションを設定できます。イベントが生成されると、選択済みのアラート タイプのメカニズムを使用し、設定済みの宛先に転送されます。アラートの有効・無効化は、iDRAC webインターフェース、RACADM、iDRAC 設定ユーティリティで可能です。iDRAC は、以下のような様々な種類のアラートをサポートしています。

- Eメール または IPMI アラート
- SNMP トラップ
- オペレーティングシステムおよびリモートシステム ログ
- Redfish イベント

アラートは、重大度 (重大、警告、または情報) により分類されます。アラートには次のフィルターを適用できます。

- **システムの正常性** - 温度、電圧、デバイス エラーなど
- **ストレージの正常性** - コントローラのエラー、物理ディスクまたは仮想ディスクのエラーなど
- **設定の変更** - RAID 設定の変更、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** - アップグレードやダウングレードなど

IT 管理者はアラートに対し様々なアクション (再起動、電源再投入、電源オフ、アクションなし) を設定できます。

リモート*Syslog*のための*TLS*

iDRAC リモート Syslog を利用すると、RAC ログとシステム イベント ログ (SEL) を外部の Syslog サーバーにリモートから書き込めるため、サーバーファーム全体の全てのログを中央ログで確認できます。リモート Syslog プロトコルはユーザー認証を必要としません。ログをリモート Syslog サーバーに入力するには、iDRAC とリモート Syslog サーバーとの間に適切なネットワーク接続があり、同じネットワーク上で実行されている必要があります。iDRAC の webサーバーには、デフォルトで自己署名 TLS/SSL 証明書があります。自己署名証明書は、カスタム証明書、カスタム署名証明書、またはよく知られた認証局 (CA) により署名された証明書に置き換えることができます。Redfish スクリプトは、証明書の自動アップロードを実行できます。2 つのサーバー間でリンクが確立されると、TLS 暗号化と SSL 復号化による安全なデータ転送が可能になります。

SELinuxフレームワーク

SELinux は iDRAC のコアカーネルレベルで動作し、ユーザー入力や設定は不要です。SELinux は、攻撃が検出されるとセキュリティメッセージを記録します。このログメッセージは、攻撃者がいつ、どのようにシステムに侵入しようとしたかを示します。ログは、この新機能に登録されたお客様に SupportAssist 経由で提供されます。このログは、iDRAC の今後のリリースでLifecycle Controller ログでも利用可能になります。

リアルタイムでの検知 – BIOSライブスキャン

BIOS ライブ スキャンは、ホストの電源がオンの状態で、プライマリ ROM の BIOS イメージの整合性と信頼性を検証します。POST プロセスではありません。iDRAC9 の 4.10.10.10 (AMD サーバー) および 4.40.20.00 (インテル サーバー) を対象に、Datacenter ライセンスのみで利用できます。実行には、管理者権限もしくは「デバッグコマンドの実行」の可能なデバッグ権限を持つオペレーター権限が必須です。BIOS イメージスキャンはオンデマンドで、もしくは iDRAC UI、RACADM、Redfish インターフェースでスケジュールして実行できます。AMD「Rome」とインテル「Ice Lake」搭載の第15世代 PowerEdge かそれ以降で使用できます。

ブート時とランタイムのBIOSスキャン

ブート プロセスが安全であることの確認はサーバー セキュリティの重要な側面です。このプロセスは、OS の起動やファームウェアの更新など、後続のすべての操作に信頼できるアンカーを提供します。PowerEdgeサーバーでは、機密データを保存するためのiDRACの暗号化されたセキュア メモリであるiDRAC Credential Vault などの機能に、数世代にわたりシリコンベースのセキュリティが使用されてきました。ブートプロセスは、シリコンベースのRoT を使用して検証され、以下の推奨事項を満たしています。

- NIST SP 800-147B：サーバーの BIOS 保護ガイドライン
- NIST SP 800-155：BIOS 整合性測定ガイドライン

iDRAC9 搭載の Dell PowerEdge サーバーでは、まず iDRAC が信頼のチェーン認証で起動し、次に BIOS の整合性を検証します。iDRAC はハードウェアベースのルートオブトラスト (信頼の基点) の役割を担います。AMD サーバーでは、iDRAC は SPI と AMD フュージョンコントローラーハブ (FCH) を介してプライマリ BIOS ROMにアクセスし、RoT プロセスを実行します。インテル サーバーでは、iDRAC は SPI とインテル プラットフォームコントローラハブ (PCH) を介してプライマリ BIOS ROM にアクセスし、RoT プロセスを実行します。

iDRAC9 は BIOS プライマリ ROM に直接アクセスし、セキュリティブロックとホストイニシャルブートブロックの両方で、プロセッサーの RoT オペレーションを実行します。

シリコンベースのルートオブトラスト

PowerEdge サーバーは、不変のシリコンベースの RoT を使ってBIOS と iDRAC9 ファームウェアの整合性を暗号で証明します。このRoTは、1回限りプログラム可能な読み取り専用の公開鍵に基づいており、マルウェアによる改ざんから保護します。BIOS ブートプロセスはインテル Boot Guard テクノロジーまたは AMD Platform Secure Boot テクノロジーを利用します。この機能が、ブートイメージの暗号化ハッシュのデジタル署名と、デル・テクノロジーズが工場でシリコンに保存した署名とが一致することを検証します。検証に失敗すると、サーバーはシャットダウンされ、Lifecycle Controller ログにユーザー通知が記録されます。BIOS 復旧プロセスはユーザー自身で行えます。Boot Guard が正常に検証されると、信頼の連鎖 (Chain of Trust) に基づいて他の BIOS モジュールも検証されます。その後 OS またはハイパーバイザーに制御が与えられます。iDRAC9 4.10.10.10 以降では、Boot Guard に加えてホストのブート時に BIOS イメージを検証する RoT メカニズムも提供されています。ホストは、BIOS イメージが正常に検証された後にのみ起動できます。iDRAC9 は、ランタイムで、オンデマンドで、またはスケジューリングによる任意の間隔で、BIOSイメージを検証するメカニズムも提供しています。信頼のチェーンのために、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 の主要モジュールに含まれるのは、次の通りです。

- テクニカルサポートとリソース ID 483
- イニシャル ブート ブロック (IBB)
- セキュリティ (SEC)
- EFI 初期化前 (PEI)

第4段階 - セキュリティ管理と監視

- メモリー参照コード (MRC) o ドライバー実行環境 (DXE)
- ブート デバイスの選択 (BDS)

インテル Boot Guard が IBB モジュールを認証すると、IBB モジュールは SEC と PEI モジュールを検証したのち制御を渡します。次に SEC と PEI モジュールが PEI と MRC モジュールを検証し、さらに DXE と BDS モジュールを検証します。その後 UEFI セキュアブートに制御が引き継がれます。AMD EPYC 搭載の PowerEdge も同様で、AMD Secure Root of Trust テクノロジーにより、サーバーは信頼できるファーム ウェア イメージからのみ起動します。AMD Secure Run テクノロジーはメインメモリーを暗号化し、ハードウェアへアクセスする悪意ある侵入者からメモリーを保護します。この機能のためにアプリケーションを変更する必要はなく、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もありません。iDRACは、ハードウェアベースのセキュリティ技術の役割を担い、SPI を介してプライマリ BIOS ROM にアクセスします。iDRACは、AMD フュージョン・コントローラー・ハブ (FCH) とともに RoT プロセスを実行します。

以下の条件下では、iDRAC9 は BIOS を回復します。

- BIOS の整合性チェックに失敗する
- BIOSセルフチェックに失敗する

注：BIOSセットアップを回復するには、RACADMコマンドを使用します。

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独立したシリコンベースの RoT を利用します。iDRAC RoT は、Dell Update Package (DUP) のファームウェア署名認証のための重要なトラストアンカーも提供します。

システムロックダウン

iDRAC9 には、サーバーのハードウェアとファームウェアの設定を「ロックダウン」する機能があります。(Enterprise または Datacenter ライセンスが必須。) このモードは、GUI、RACADM CLI またはサーバー構成プロファイルで有効にできます。管理者権限を持つユーザーはシステムロックダウンを使い、より低い権限のユーザーがサーバーを変更できないように設定できます。この機能は、IT 管理者が有効にも無効にもできます。システムロックダウン無効時に行われた変更は、Lifecycle Controller ログで追跡されます。ロックダウンモードを有効にすると、Dell のツールとエージェントを使用する際のデータセンターの設定のずれを防ぎ、Dell Update Packages (DUP) 利用時の組み込みファームウェアを、悪意ある攻撃から保護できます。ロックダウンはシステムの再起動を必要とせず、動的に有効化できます。iDRAC9 v4.40 からは、DUP を使用時にアップデートのみを制御する従来のシステムロックダウンに加え、一部のNICもロックダウンする機能拡張が行われています。

注: 新機能として追加された NIC のロックダウンは、ファームウェア更新をブロックするロックダウンのみが含まれます。

x-UEFI Configuration のロックダウンはできません。サポートされているインターフェースから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設定すると、iDRAC が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 の検出プロセス内で検出されたサードパーティ製デバイスにより異なります。

ドリフトの検知

標準化された設定を強制し、いかなる変更に対しても「ゼロトレランス」ポリシーを採用することで、企業は悪用

の可能性を減らすことができます。Dell OpenManage Enterprise (OME) コンソール では、独自のサーバー設定ベースラインを定義し、そのベースラインからの本番サーバー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多様な運用環境の適用に合わせて、様々な基準に基づいて構築できます。

OMEは、ベースラインからのドリフトを報告し、必要に応じて簡単なワークフローでドリフトを修正して、帯域外のiDRAC 上で変更をステージングすることができます。サーバーは再起動して本番環境が再び準拠状態になり、この変更は次のメンテナンス期間で反映されます。この段階的プロセスにより、メンテナンス時間外のサーバーの停止なしに本番環境で設定の修正を行えるため、保守性とセキュリティを維持しながら、可用性を高められます。

シャーシ侵入検知

PowerEdge サーバーはハードウェア侵入検知とロギング機能を備えており、AC 電源が供給されていない状態でも検出が機能します。シャーシのセンサーは、輸送中でも、誰かがシャーシを開いたり改ざんしたりすればそれを検知します。転送中に開かれたサーバーは、電源供給後にiDRACライフサイクルログにエントリを生成します。

自動および手動のリカバリー

BIOS および OS リカバリー

第14、15、16世代の PowerEdge サーバーには BIOS リカバリーと Rapid OS リカバリーという2 種類の復旧手法があり、破損した BIOS または OS イメージからの迅速な復旧が可能です。どちらも、利用される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) から隠されています。このストレージ領域には、破損したプライマリーソフトウェアの代替として使用できる元のイメージが含まれています。

Rapid OS リカバリーにより、破損した OS イメージ (または悪意ある改ざんが疑われる OS イメージ) からの迅速な回復が可能になります。リカバリーメディアには、内蔵SDカード、SATAポート、M.2ドライブ、内蔵USBを使ってアクセスできます。選択したデバイスをブートリストと OS に公開してリカバリー イメージをインストールできます。その後は使用不可にして、ブートリストと OS で非表示にします。非表示状態では、BIOS がデバイスを無効化して OS からアクセスできない状態にします。OS イメージが破損している場合は、ブートプロセス用にリカバリー ロケーションを有効化できます。この設定は、BIOS または iDRAC インターフェースから可能です。

極端なケースでは、悪意ある攻撃、アップデートプロセス中の電源喪失、またはその他の不測の事態によって BIOS が破損した場合、BIOS を元の状態に回復する方法も重要です。バックアップ BIOS イメージは iDRAC に保存されており、必要に応じて BIOS イメージの回復に使えます。復旧プロセス全体は、iDRAC がエンドツーエンドで調整します。

- BIOS 自体が自動 BIOS リカバリを開始
- RACADM CLI コマンドを使用するユーザーは、オンデマンドで BIOS リカバリを開始可能

ファームウェア ロールバック

最新の機能とセキュリティアップデートをご利用いただくためにファームウェアのアップデートをお勧めします。ただし、アップデート後に問題が発生した場合は、アップデートをロールバックするか、以前のバージョンをインストールする必要があります。以前のバージョンにロールバックする場合、その署名も検証されます。

次のファームウェアイメージにおいて、既存の最新バージョン「N」から前のバージョン「N-1」へのロールバックがサポートされています。

- BIOS
- iDRAC with Lifecycle Controller
- Network Interface Card (NIC)
- PowerEdge RAID Controller (PERC)
- Power Supply Unit (PSU)
- Backplane

次のいずれかの方法で、ファームウェアを以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 インターフェース
- CMC web インターフェース
- RACADM CLI for iDRAC and CMC
- Lifecycle Controller UI
- Lifecycle Controller リモートサービス

iDRAC または Lifecycle Controller がサポートするデバイスのファームウェアは、前回は別のインターフェースを使ってアップグレードを実行した場合でもロールバックできます。例えば、Lifecycle Controller UI を使用してアップグレードされたファームウェアを iDRAC webインターフェースを使用して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。

iDRAC と Lifecycle Controller で共通の単一ファームウェアを持つ PowerEdge 第14、15、16 世代では、iDRAC ファームウェアをロールバックすると Lifecycle Controller のファームウェアもロールバックされます。

ファームウェア ロールバックの保護

もし特定のファームウェアに既知の脆弱性があり、サーバーが攻撃にさらされる可能性がある場合、BIOS 自体が旧バージョンへのダウングレードを防ぎます。該当するファームウェアはそのリリースノートに、アップデート実行時にロールバックはできない旨が記載されています。

Full Power Cycle

Full Power Cycle 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から主電力と補助電源の電力が排出され、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 Full Power Cycleでは、AC電源ケーブルを外し、30秒間待ってからケーブルを戻す必要があります。この方法は、リモートのシステムで作業する場合に問題となります。PowerEdge サーバー第14、15、16世代の機能により、iDRAC サービスモジュール (iSM) 、iDRAC GUI、BIOS、またはスクリプトから効率的にこの機能を実行できます。Full Power Cycle は、次の電源サイクルで有効になります。

Full Power Cycle 機能により、メンテナンス要員がデータセンターに物理的に出向く必要がなくなるため、トラブルシューティングにかかる時間が短縮されます。たとえば、メモリに常駐しているマルウェアを除去できます。

アップデート

デル・テクノロジーズは、サーバーのファームウェアと BIOS を最新の状態に保ち、迅速にアップデートするための豊富なツールを提供しています。ファームウェアを最新の状態に保つことは、本番サーバーのセキュリティを維持し、効率的に運用するために不可欠なタスクです。アップデートのトラックと実装は管理者の負担になる場合があるため、iDRAC9 には自動アップデート機能と、それを必要に応じてスケジューリングする機能が含まれます。

多くの企業では、OS、アプリケーション、およびファームウェアのアップデートを処理するために、毎月のメンテナンス期間をスケジュールしています。OpenManage Enterprise を使用すると、システム管理者はファームウェアのアップデートを、次回のシステム再起動時またはスケジュールされた導入時に、段階的に行うことができます。この方法により、アップデートを実行するために誰も物理的に立ち会う必要はなくなります。

PowerEdge は、Dellセキュリティアドバイザリーに基づき、セキュリティ脆弱性に対するパッチを提供しています。アドバイザリーでは、セキュリティ脆弱性に関連するリスクを最小化するための情報、ガイダンス、および緩和策がタイムリーに提供されます。

ハードウェア保守後のサーバー設定の復元

サービスイベントの修復は、IT運用の重要な部分です。復旧時間の目標と復旧ポイントの目標を達成できるかどうかは、ソリューションのセキュリティに直接影響します。サーバー構成とファームウェアの復元は、そのサーバーの運用セキュリティ ポリシーも自動的に満たします。

PowerEdgeサーバーには、次の状況でサーバー構成を迅速に復元する機能があります。

- 個々のパーツ交換
- マザーボードの交換 (サーバープロファイルの完全バックアップと復元)
- マザーボードの交換 (Easy Restore)

パーツ交換

iDRACは、NIC、RAIDコントローラ、および電源ユニット (PSU) 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。現場でこれらのパーツを交換する場合、iDRAC が自動的に新しいカードを検出し、交換したカードにファームウェアと設定を復元します。この機能は貴重な時間を節約し、設定の一貫性とセキュリティポリシーを確実化します。アップデートは、対象のパーツを交換した後のシステム再起動時に、自動的に行われます。

Easy Restore (マザーボードの交換時用)

Easy Restoreは、重要な構成情報を保持する統合ストレージ コンポーネントです。Easy Restore (簡易復元) 機能を使用すると、システムボードの交換後にシステムのサービスタグ、すべてのライセンス、UEFI 設定、システム設定 (BIOS、iDRAC、NIC)、OEM ID (パーソナリティモジュール) を復元できます。すべてのデータは

自動的にバックアップフラッシュデバイスにバックアップされます。BIOS が新しいシステム ボードとサービス タグをバックアップ フラッシュ デバイスで検出すると、バックアップ情報を復元するよう BIOS がユーザーを促します。このソリューションはハードウェアの設定に加え、実際のファームウェアバージョンをバックアップおよび復元します。Easy Restoreではサイズ制限により、ファームウェア ドライバーのコピーはされません。

CloudIQ

インフラ システムの設定ミスは、組織をサイバー侵入の危険にさらす可能性があり、データセキュリティの主要な脅威となります。CloudIQ のサイバーセキュリティ機能は、Dell PowerStore、PowerMax、PowerEdge のセキュリティ設定をプロアクティブに監視し、セキュリティリスクをユーザーに通知します。各システムにはリスクレベルが割り当てられ、システムは問題の数と深刻度に応じて4つのカテゴリ (標準、低、中、高) に分類されます。

CloudIQ Cybersecurity のポリシー テンプレートを使用すると、ユーザーはセキュリティ構成評価テストを迅速に設定し、数度のクリックだけで多数のシステムに割り当てることができます。一度割り当てられると、テスト計画は該当する各システムに対する評価を行い、好ましくない構成設定は数分でシステム管理者に通知されます。

セキュリティリスクが検出されると、問題への迅速な対処を支援するための修復手順が提供されます。CloudIQ は Dell セキュリティ アドバイザリ (DSA) を評価し、アドバイザリが特定のソフトウェアとファームウェア バージョンを持つ特定の Dell システムに適用される場合、ユーザーにインテリジェントに通知します。この通知で、ユーザーはセキュリティアドバイザリが自社のシステムに該当するかどうかを調べる必要がなくなり、すぐに修復に専念できます。

Managed detection and responseサービス

デル・テクノロジーズの Managed Detection and Response サービスは、IT部門の負担を軽減しながら、企業のセキュリティ体制を迅速かつ大幅に改善する、クラウドベースのサービスです。この、フルマネージドのエンド ツーエンドの24時間365日サービスは、IT環境全体の脅威を監視、検出、調査、および対応します。

50以上のエンドポイントを持つ企業向けに設計されたこのユニークなサービスは、2つの主要機能を活用します。

- 実際の脅威インテリジェンスとその調査、高度な脅威の検出と対応経験を含む、20年以上の SecOps の専門知識に基づき開発された、Secureworks Taegis XDR セキュリティ分析ソフトウェアの能力
- 世界中の組織がビジネスをより適切に保護できるよう長年にわたって支援してきた経験から得た、デル・テクノロジーズのセキュリティ アナリストの専門知識

Dell Technologies Managed Detection and Response はセキュリティの専門家に24時間アクセスできます。エンドポイントからクラウドまで、エンドツーエンドの可視性と保護を提供し、日々管理・更新される 52,000 の固有の脅威指標を含む Taegis XDR データベースに基づき、高度な脅威の検知と対応の全側面を含みます。Taegis XDR は既存のセキュリティソリューションからデータを取り込むため、従来のセキュリティ投資も活用します。

デル・テクノロジーズのセキュリティ アナリストは、初期セットアップ、監視、検出、修復、対応のすべてを、予測できる単格で支援します。Dell のセキュリティ アナリストは、お客様のITチームと緊密に連携して環境を理解します。セキュリティ体制の改善に関するアドバイスを提供し、Taegis XDR ソフトウェアエージェントのセットアップとエンドポイントへの配備を支援します。その後、Taegis XDR アプリケーションを使用して、24時間365日無休

でアラートを監視およびレビューします。アラートが調査に値する場合、アナリストが適切な対応を決定し実行します。脅威が悪意によるものであったり、対応が必要な場合はお客様に通知され、必要に応じてステップ バイ ステップの手順を提供します。デル・テクノロジーズはこのサービスの一環として、トラブルシューティング、問題解決、ソフトウェアの導入、パッチおよび資産の評価、IT環境の構成など、四半期ごとに最大40時間の Remote Remediation Assistance も提供します。

セキュリティ インシデントが発生した場合は、デル・テクノロジーズはお客様のビジネスを復旧させるためのプロセスを開始し、年間最大40時間のリモート インシデント対応支援を提供します。

第5段階 – サーバーの廃棄と再利用に関するセキュリティ

課題

データセキュリティは、サーバーの再利用や廃棄など、ライフサイクル全体を通じて重要な考慮事項です。サーバーの多くは、ワークロードからワークロードへの移行や、組織から別の組織への所有者の変更に伴い、再利用されます。すべてのサーバーは、耐用年数の終わりに達すると廃棄されます。このような移行が発生した場合、IT のベスト プラクティスでは、機密情報が不注意で共有されることがないようにすべてのデータをサーバーから削除することが推奨されています。

PowerEdge のセキュリティ ソリューション

ベストプラクティスだけでなく多くの場合、政府のプライバシー権に関する規制により、ITリソースの移行時にはデータの完全な削除が必要です。データ消去は、Dell セキュア開発ライフサイクル (SDL) に含まれる重要な機能です。この SDL とセキュアなサーバー管理ツールにより、PowerEdge サーバーはサーバーの構想、設計、製造から運用、廃棄までのライフサイクルのあらゆる段階で、確実にセキュアであり続けます。

ライフサイクルの最終段階 (利用停止/廃棄時) や、ワークロードや所有者の変更によりサーバーを再利用する場合、第14世代の PowerEdge サーバーから搭載された機能を使って、データ消去を簡素化できます。

第14、15、16世代 PowerEdge サーバー搭載のiDRAC9 が持つ System Eraseは、ストレージデバイスやキャッシュやログなどの、サーバー内の不揮発性記憶装置のデータ消去プロセスを簡素化します。管理者の多用なニーズに対応すべく、System Erase は以下の方法で実行できます。

- Lifecycle Controller UI
- WS-Man API
- RACADM CLI

管理者は上記いずれかの方法で PowerEdge サーバーを選択的に元の状態 (工場出荷時の設定) にリセットし、サーバー内の不揮発性記憶装置やストレージデバイスからデータを削除できます。
System Eraseは、HDD、SED、ISE、不揮発性メモリー ドライブ (NVM) などのサーバー ストレージを検出できます。ISE、SED、NVMe デバイスに保存されているデータは暗号化消去を使用してアクセス不能にすることができ、非ISE SATA HDD などのデバイスは、データを上書して消去できます。

セキュア消去

Lifecycle Controllerを通じてシステムの再利用や廃止ができます。現在 PowerEdge で出荷されるドライブはすべて安全に消去できます。暗号化対応ドライブを搭載しない旧機種では「標準ディスク (データの上書き)」が使えます。データが回復不能になるプロセスでは警告メッセージが生成されます。サーバーの廃棄または再利用の操作後、電源が切れます。操作の成功は、iDRAC ライフサイクルログで確認できます。

システムはライフサイクルの終了後、廃棄または再利用されます。いずれのシナリオでも、System Erase はサーバーから機密データと設定情報を削除します。セキュア消去は、機密情報が意図せず漏洩しないよう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の不揮発性記憶データを消去します。これはログ、設定データ、ストレージデータ、キャッシュを消去する、Lifecycle Controller (F10) 内のユーティリティです。

System Erase 機能は、以下のデバイス、構成設定、アプリケーションを消去できます。

- iDRAC をデフォルト設定にリセットし、すべてのデータと設定を消去
- Lifecycle Controller (F10) のデータをクリア
- BIOS と NVRAM をデフォルト設定にリセット
- 組み込み診断ツールとOSドライバーパックをクリア
- iDRAC Service Module (iSM) をクリア
- SupportAssist コレクション レポートをクリア

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をクリア)
- vFlash SD Card (カードを初期化)

注: vFlashは第15世代以降のPowerEdgeサーバーでは使用できません。

System Erase は、以下のコンポーネントのデータを暗号的に破棄します。

- 自己暗号化ドライブ (SED) およびISE ドライブ
- NVM (不揮発性メモリー) デバイス - インテル Optane パーシステントメモリーやNVDIMMなど

セキュア消去 – 物理ディスク

ドライブを工場出荷時の設定にリセットします。SSD上の全データは完全に削除され、復元できません。ドライブのサニタイズではマッピングテーブルが削除され、データが書き込まれたすべてのブロックが消去されます。すべてのSSDがサニタイズ機能をサポートしているわけではありません。

上書き消去

上書き消去は、データをゼロと1で上書きするソフトウェアベースの方法です。データの上書きは、非ISE SATA ハードドライブを消去することができます。

暗号消去

ISEは、第14、15、16世代の PowerEdge サーバーのドライブで使われる内部暗号化キーを破壊し、ユーザーデータを復元不可能にします。自己暗号化ドライブの場合は暗号化キーを消去します。データはドライブに残りますが、キーがないとアクセスできません。NIST Special Publication 800-88 Guidelines for Media Sanitization に記載の通り、ISEはストレージドライブのデータ消去方法として認められています。

System Erase が活用する ISE の新機能の利点は以下です。

- **スピード** - ISE は、DoD 5220.22-M のようなデータ上書き技術より高速です。（数時間に対して、数秒）
- **効果** - ISE は、予約済みブロックを含むドライブ上のすべてのデータを読み取り不能にします。
- **TCOの改善** - ストレージデバイスは、物理的に破壊する代わりに再利用できます。

System Erase 機能は以下の手法で実行できます。

- Lifecycle Controller インターフェース (F10)
- RACADM CLI
- Redfish

データ サニタイゼーションおよびデータ廃棄サービス

データは増え続け、戦略的優位性を高めます。一方で国家安全保障問題やデータ プライバシーの規制がエスカレートしています。企業がテクノロジーの変化に対応するにあたり、データ セキュリティとコンプライアンスの課題は高まっています。

製品ライフサイクルの終了は、データセキュリティの重要な側面です。企業向けのデータ サニタイゼーションは、データを安全に上書きして復元不可能にするソフトウェアベースの方法です。様々なオプションがあります。

- **Data Sanitization for Enterprise Onsite** - 資産のリフレッシュや再展開をお考えのお客様向けのサービスです。オンサイトでサニタイズを実行し、資産を環境に残しつつデータを保護します。
- **Data Sanitization for Enterprise Offsite with Asset Resale and Recycle** - 資産を環境から取り出して安全な場所でサニタイズしたうえで再販・再利用の為の評価を行うサービスです。資産に価値のある場合はお客様は補償を受け、ない場合は地域の規制に沿ってリサイクルされます。
- **Data Destruction for Enterprise** - 物理的なシュレッダー処理でデータをアクセス不能にします。対象はすべてのDellインフラストラクチャーと、サードパーティー製アセットです。システムを動作させる必要はありません。

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最優先事項であり、基盤となるサーバーインフラストラクチャーのセキュリティはきわめて重要です。サイバー攻撃は、システムやビジネスのダウンタイムの長期化、収益と顧客の損失、法的損害、企業の評判の低下につながる可能性があります。ハード ウェアを標的としたサイバー攻撃に対する防御、検出、回復の能力を持つためには、セキュリティは後から追加するのではなく、サーバー ハードウェアの設計に組み込む必要があります。

デル・テクノロジーズは過去2世代にわたり、シリコンベースのセキュリティを使用してPowerEdgeサーバーのファームウェアを保護し、機密性の高いユーザーデータを保護してきたリーダーです。第14、15、16世代の PowerEdge サーバー製品ラインには、シリコンベースのルートオブトラスト (信頼の基点) の利用で強化されたサイバーレジリエント アーキテクチャが搭載されており、以下のような機能により、サーバーセキュリティがさらに強化されています。

- 暗号的に検証されたトラステッド ブートは、サーバーとデータセンター全体のエンドツーエンドのセキュリティを支えます。これには、シリコンベースのルートオブトラスト、デジタル署名付きファームウェア、自動 BIOS リカバリーなどの機能が含まれます。
- セキュアブートは、オペレーティングシステムの実行前に読み込まれた UEFI ドライバーやその他のコードの暗号化署名をチェックします。
- iDRAC Credential Vault は、認証情報、証明書、その他の機密データを安全に保管するためのスペースで、各サーバーに固有のシリコンベースの鍵で暗号化されています。
- PowerEdgeサーバー固有の機能であるダイナミック システム ロックダウンは、システムの設定とファームウェアを悪意のある変更や意図しない変更から保護し、システム変更の試みをユーザーに警告します。
- Enterprise Key Management は、企業全体の保存データを管理するための一元的な鍵管理ソリューションです。
- System Erase は、ストレージ ドライブやサーバー内の不揮発性メモリーからデータを安全かつ迅速に消去することで、第14世代、第15世代、第16世代のPowerEdgeサーバーを簡単に廃棄または再利用可能にします。
- Secure Component Verification は、お客様が製品を手にする前に製品が改ざんされたり偽造コンポーネントが混入していないことを確認可能にするサプライチェーン保証の提供手法です。

第14、15、16世代の PowerEdge サーバーは、業界をリードするセキュリティを備えており、お客様が IT 運用とワークロードを安全に実行し、ゼロトラストモデル導入を加速できる、信頼のできるIT トランスフォーメーションの基盤を形成します。デル・テクノロジーズは、お客様が画期的なサーバー導入を実現できるようにあらゆる手段を講じています。当社の最新のセキュリティ アプローチは、お客様がコアコンピタンスに集中し、イノベー ションを導入して人類の進歩を促進できるよう、企業の IT 環境の安全性とレジリエンシーを確実なものにします。

参考資料

デル・テクノロジーズの各種ドキュメント

以下の Dell Technologies のドキュメントには、当ホワイトペーパーに関連する各種情報が記載されています。これらのドキュメントへのアクセスは、ログイン認証情報によって異なりますので、アクセスできない場合はデル・テクノロジーの担当者までお問い合わせください。

- *iDRAC9 Security Configuration Guide*
- *Dell EMC Secured Component Verification Reference Guide for Servers*
- *Understanding Confidential Computing with Trusted Execution Environments and Trusted Computing Base models*
- *iDRAC9 システムロックダウン：意図しないサーバーの設定変更を防止*
- *Next Generation Dell PowerEdge Servers: Transition to Modern UEFI*
- *Dell EMC PowerEdge UEFI Secure Boot Customization: Reduce Attack Surface with Complete Control of Certificates*
- *Dell Technologies のサプライチェーンセキュリティ: Secured Component Verification for PowerEdge*
- *Dell PowerEdge: iDRAC Automatic Certificate Enrollment*
- *Improved iDRAC9 Security using TLS 1.3 over HTTPS on Dell PowerEdge Servers*
- *A Partnership of Trust: Dell Supply Chain Security*
- *PowerEdge Advantages in your Zero Trust Journey – Video*
- *AMD on PE - Extending Data Protection to Data in Use - Video*
- *AMD on PE – Extended Boot Protection - Video*
- *Zero Trust Architecture - Video*
- *Cyber Resilient Architecture - Video*
- *Secured Component Verification - Video*
- *SEKM – Video*
- *IPv6* – Direct from Development
- *iDRAC9 Virtual Power Cycle: Remotely power cycle Dell EMC PowerEdge Servers* -Direct from Development
- *Transform Datacenter Analytics with iDRAC9 Telemetry Streaming*
- *Configure iDRAC to use Active Directory Authentication (dell.com)*
- *Securing 14th Generation Dell EMC PowerEdge Servers with System Erase*
- *Direct from Development - セキュリティ最重視のサーバ設計*
- *Direct from Development - Cyber-Resiliency Starts At The Chipset And Bios*
- *Factory Generated Default Password for iDRAC9 for Dell EMC 14th Generation (14G) PowerEdge Servers*

- Dell EMC iDRAC Response to Common Vulnerabilities and Exposures (CVE) CVE-2017- 1000251 “BlueBorne”
- *(Video) Secure Boot Configuration And Certificatemanagement Using RACADM- Video*
- *Secure Boot Management on Dell EMC PowerEdge Servers*
- *Signing UEFI images for Secure Boot feature in the 14th and 15th generation and later Dell EMC PowerEdge servers*
- *Rapid Operating System Recovery*
- *Managing iDRAC9 Event Alerts on 14th generation (14G) Dell EMC PowerEdge Servers*
- *UEFI Secure Boot Customization*
- *iDRAC Overview*
- *OpenManage Console Overview*
- *OpenManage Mobile Overview*
- *Motherboard Replacement*