



データの脆弱性を縮小する

前面USBポート無効化の所要時間を85%短縮

Vendor K BMCと比較したiDRAC9
の実績



二酸化炭素排出の緩和に役立つ

25種類のカスタマイズ可能な電力消費レポート

OMEでの数（Vendor Kのエンタープライズ管理コンソールでは0レポート）



ファームウェアの自動的な

アップデートのスケジュールをわずか41秒で設定

APEX AIOps Infrastructure Observability（旧称CloudIQ）
での実績

Dellのサーバー管理ツールはセキュリティ、サステナビリティ、管理効率の向上に役立つ

Vendor Kの同等のサーバー管理ツールとの比較

データセンターが拡大を続けると、管理者の責務もそれに比例します。インフラストラクチャが初めから堅牢な管理と監視のツールを備え、自動化も可能ならば、過負荷になりがちな管理者もデータセンターのセキュリティ維持と管理を簡単にできるようになります。当社は、Dellとその競合他社（ここではVendor Kと呼びます）のそれぞれが提供する管理ポートフォリオの機能および能力を比較しました。

表1：当社がテストした管理ツール。

	Dell	Vendor K
組み込み型またはリモートサーバー管理	Dell Technologies Integrated Dell Remote Access Controller 9 (iDRAC9)	Vendor K Baseboard Management Controller (BMC)
1対多デバイスおよびコンソール管理	Dell Technologies OpenManage™ Enterprise (OME) APEX AIOps Infrastructure Observability（旧称 CloudIQ）	Vendor Kのエンタープライズ管理コンソール

iDRAC9、OME、APEX AIOps Infrastructure Observability（旧称 CloudIQ）から成る強力な管理ツールファミリーは、Vendor K提供の同様のツールと比較してセキュリティを強化し、サステナビリティの取り組みを支援し、日常的な管理タスクを容易にすることが判明しました。

データセンターのセキュリティを強化

機密性の高い顧客データを保管する組織にとっては、サイバー攻撃の脅威が常に存在することから、データが攻撃者の手に渡るのを防ぐ強力なエンドツーエンドのセキュリティ機能が求められます。実際に、最大で「組織の83%が2022年に複数のデータ侵害を経験した」¹という統計もあり、消費者の信頼を高めるために顧客データに関して予防措置を取ることの重要性が強調されています。

組織とそのデータをコストのかかるサイバー攻撃から保護するために、Dellの管理ツールの強力なセキュリティ機能がiDRAC9を介してサーバーに組み込まれ、さらに包括的なコンソールとクラウド管理ソフトウェアにも組み込まれています。ここでは、システムを保護するためにDellのツールで使用されている主なセキュリティ機能について、Vendor K提供の対応する製品と比較しながら詳しく見ていきます。

内蔵セキュリティ機能

どのDell PowerEdgeサーバーにもiDRAC9を介して組み込まれているセキュリティ機能が、攻撃者によるデータへのアクセスを阻止します。なかでも重要な機能は次の3つです。

- **動的システム ロックダウン**：意図しない、または悪意のある活動によってシステムBIOS、iDRAC、ファームウェアの設定が変更されるのをシステム ロックダウンによって防止します。動的とは、これらの機能を設定した後に、必要に応じて有効化できることを指します。（注：この機能はiDRAC9 EnterpriseおよびDatacenterのライセンスで使用可能です。）
- **多要素認証(MFA)**：管理者にログイン認証情報に加えてパスコードの入力を求めるという方法でセキュリティを補強します。
- **動的USBポートの有効化と無効化**：USBポートの有効化と無効化を通して、管理者はUSBポートを介したサーバーへのアクセスを制御できます。動的とは、サーバーやOSの再起動は不要でUSBポートを有効または無効にできることを指します。管理者からアクセスが許可されない限り、誰もUSBメモリーやキーボードを接続してシステム、OS、BIOSの構成設定を変更することはできません。

表2に示すように、Vendor Kは動的システム ロックダウンもMFAも未提供で、同社の動的USB機能はシステム ダウンタイムを要する（組織にとってはコストが高くつく可能性がある）ため、Dellのソリューションと比較して有用性が低く、コストが高くなります。

表2：サーバー管理ツールの内蔵セキュリティ機能の比較。出典：Principled Technologies

	iDRAC9	Vendor K BMC
動的なSystem Lockdown	✓	✗
MFA	✓	✗
ダイナミックUSB	✓	✓*

*システム ダウンタイムが必要

Dell Technologies Integrated Dell Remote Access Controller 9について

Dell PowerEdge™サーバーにはiDRAC9とDell Lifecycle Controllerが含まれており、これらが提供するシステム管理機能でシステムアラートとリモート管理が可能です。Dellによれば、iDRAC9の主なメリットは次のとおりです。

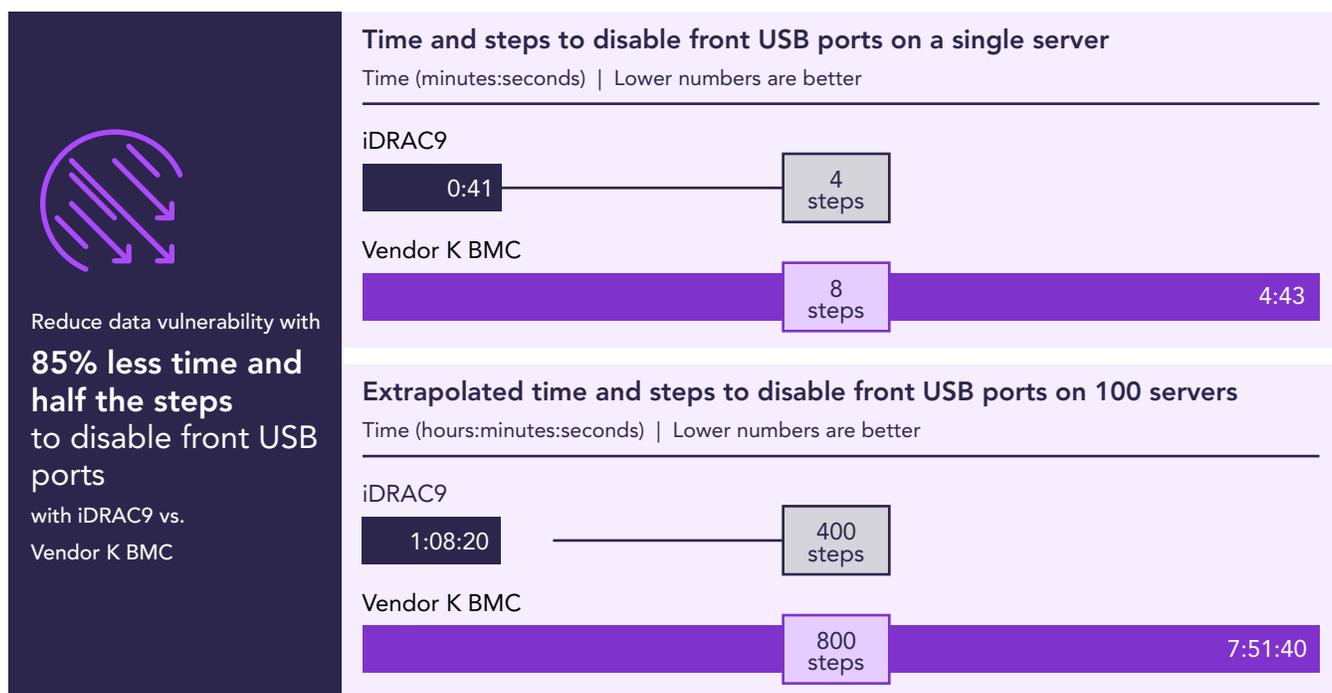
- 拡張性のある自動化。標準ベースのAPI（たとえばRedfish）と堅牢なスクリプティング ツール（たとえばRedHat Ansible、Python、PowerShell、Terraform）を使用して数千台のサーバーを管理できます。
- 組み込みのサポートによってサーバーの正常性とステータスを見ることができ、数千のパラメーターが監視される
- 強力なセキュリティ機能とオプション²

iDRAC9の機能の詳細については、<https://www.dell.com/en-us/lp/dt/open-manage-idrac>にアクセスしてください。

図1は、当社の実地テストでiDRAC9とVendor K BMCを使用してUSBポートを動的に無効にした結果の比較です。

iDRAC9を使用すると、管理者は1台のサーバーの前面USBポートをわずか41秒、4ステップで無効にできることが判明しています。対照的に、Vendor K BMCでは同じプロセスにサーバーあたり4分43秒、8ステップを要します。つまり、サーバー1台につき**Dellのソリューションでは前面USBポートの無効化に要する時間を85%短縮し、ステップ数を半分に減らすことができます**。³ これらのステップをデータセンターで実施することを考えると、節約できる時間はさらに大きくなり、サーバー100台が導入済みの場合に、iDRAC9ではVendor K BMCと比べて管理者の時間を6時間43分節約できます。

iDRAC9ではVendor K BMCよりも簡単かつ迅速にこれらの機能にアクセスできるだけでなく、iDRAC9なら管理者はサーバーを本番稼働状態にしたまま（ダウンタイムなしで）これらの機能を有効または無効にできます。Vendor K方式ではダウンタイムを要するため、かなりのコストが発生し、システム セットアップ構成の変更が毎回必要になります。



1 1台のサーバーの前面USBポート無効化に要する時間と、100台のサーバーの前面USBポート無効化に要する推定時間。時間とステップ数が少ないほうが優れています。出典：Principled Technologies

セキュリティ維持のための認証情報管理がOMEでは容易

OMEでは、管理者がiDRAC9のパスワードローテーションを単純明快な方法で管理できます。静的な既知の管理者アカウントの代わりに、OMEではiDRACの管理がサービス アカウントを介して行われます。これに必要なパスワードローテーションポリシーをお客様が選択することも（そのパスワードが公開されることは決してありません）、管理者が外部でサードパーティーを使用して管理することもできます。Vendor Kのエンタープライズ管理コンソールには内部パスワードローテーション機能がないため、この機能が**必要な場合はサードパーティーに依存せざるを得ません**。当社は、iDRAC9で管理されるサーバーが、完全な管理者特権を持つOMEアカウントと統合されており、認証情報管理が容易であることを確認しました。

注：このレポートのグラフはそれぞれ尺度が異なります。比較する際は、各グラフのデータ範囲に注意してください。

サステナビリティ目標を達成

米国エネルギー省によれば、「データセンターは米国の総電力消費量の約2%を占めていますが、データセンターの冷却はデータセンター全体のエネルギー使用量の最大40%を占める可能性があります」⁴。データの急増が続くなかで、これらの数値は増加する一方であるため、データセンターのコストを削減するとともに二酸化炭素排出の緩和に向けたサステナビリティ目標を達成するためには、温度と電源の管理が不可欠になっています。組織の電力使用量を削減できるように、OMEには電力消費の監視と管理のさまざまな機能が採用されています。表3は、この後で詳しく説明するこれらの機能の主なメリットをまとめたものです。

3 OMEとVendor Kのエンタープライズ管理コンソールのサステナビリティに関する主な機能の概要。出典：Principled Technologies

特長	Dellの管理ツールの主なメリット	Vendor Kの管理ツールのデメリット
 二酸化炭素排出量計算とキャパシティプランニングのツール	サステナビリティの目標の達成に役立つために、カスタマイズ可能な値を使用して 温室効果ガス排出量を 推定できる	Vendor Kのエンタープライズ管理コンソールには 同等の機能がない
 電力上限ポリシー	OME Power Managerプラグインには単体またはグループのデバイスの 電力上限を管理する 機能があり、有効化すると電力上限を強制できる	Vendor Kのエンタープライズ管理コンソールには 同等の機能がない
 電力管理および温度管理の自動化	電力と温度をトリガーとするポリシー のオプション（サーバーが電力消費または温度のしきい値を超えたときにトリガーするオプションを備える）	Vendor Kのエンタープライズ管理コンソールには 同等の機能がない
 電力消費ダッシュボード	Power ManagerデータにOME Power Managerプラグイン ダッシュボードからすばやくアクセス でき、 メトリック数は2.75倍（11種類）	Vendor Kのエンタープライズ管理コンソールではダッシュボードの メトリックは4種類のみ
 電力消費レポート	OME Power Managerプラグインでは 25種類のデフォルトと追加のカスタマイズ可能なレポート を利用可能	Vendor Kのエンタープライズ管理コンソールには 電源管理レポートはない
 電源管理メトリック	メトリック数は最大3倍 であり、電力消費管理に関する細分化されたインサイトが 21種類のメトリック で得られる	Vendor Kのエンタープライズ管理コンソールにある電源管理関連の メトリックは7種類のみ

電力管理および温度管理の自動化

OME Power Managerでは電力管理および温度管理が自動化されていますが、これには静的な電力と温度をトリガーとするポリシー オプションの両方が使用されているため、管理者が電力消費または温度のしきい値を設定することによって冷却コストを削減し、節電戦略を支え、熱関連の事象に対応することができます。対照的に、**Vendor Kには自動化された電力管理および温度管理機能はありません**。温度に基づく上限の設定ができないため、エネルギー使用量が想定を超える可能性があり、サステナビリティを念頭に置いた計画立案が難しくなります。電力消費の最適化は、サステナビリティの目標達成への重要な戦略です。OME Power Managerプラグインで**電源管理関連の25種類のデフォルトまたはカスタマイズ可能なレポート**（17種類はPower Managerデバイスで、8種類はPower Managerグループで）が利用可能になるため、管理者がキャパシティプランニングを最適化するとともに効率を最大化するように電力を管理できます。**Vendor Kのエンタープライズ管理コンソールには、同様の電源管理レポートはありません**（図2を参照）。



Optimize capacity planning and address sustainability goals with **25 power management reports** in OME vs. Vendor K's enterprise management console

Power consumption reports

Number of reports | Higher numbers are better

OME

25

Vendor K's enterprise management console

No power consumption reports in Vendor K appliance

2 OMEとVendor Kのエンタープライズ管理コンソールにある電源管理レポートの数の比較。レポートが多いほうが優れています。出典：Principled Technologies

電源管理をさらに最適化するために、OME Power Managerプラグインで管理者が見ることができる**メトリックの数はVendor Kのエンタープライズ管理コンソールの最大3倍となっています**（図3を参照）。OMEのメトリックは21種類（これには個々のコンポーネント、エアフロー、コンポーネント使用率別の電力使用量も含まれます）あるのに対し、Vendor Kのエンタープライズ管理コンソールにあるメトリックは7種類のみです。



Optimize power management with **3x the power management metrics** in OME vs. Vendor K's enterprise management console

Power management metrics

Number of metrics | Higher numbers are better

OME

21

Vendor K's enterprise management console

7

3 OMEとVendor Kのエンタープライズ管理コンソールにある電源管理メトリックの数の比較。メトリックが多いほうが優れています。出典：Principled Technologies

二酸化炭素排出量とカーボン フットプリントの分析

サステナビリティに関する主要機能の1つとして、**OMEには二酸化炭素排出量計算とキャパシティ プランニングのツールがあります**。このツールは、組織の温室効果ガス排出量を推計するのに役立ち、電力コストと、消費されるエネルギーの単位あたりの二酸化炭素排出量のデフォルト値が得られます。この機能はカスタマイズも可能であり、組織が所在する地域の電力コストと二酸化炭素排出量の値を入力できるので、組織のデータセンターの消費モデルに固有のデータが得られます。**Vendor Kのエンタープライズ管理コンソールには同等の機能がないため、組織がサステナビリティを念頭に置いて計画を立てることが難しくなります。**

管理の負荷を軽減する堅牢な監視と管理の機能

インフラストラクチャが拡大すると、データセンター管理者の責務もそれに比例します。特定のタスクを自動化し、日常的な管理を改善できるようなサーバー管理ツールを選択すれば、管理者の作業効率が向上し、将来に向けた計画立案のための時間を増やすことができます。Dellのサーバー管理ポートフォリオには、管理者のタスクをシンプルにする機能が多数あることが判明しています。表4は、Dellの管理ポートフォリオとVendor Kの管理ツールにある、使いやすさに関する主な機能を比較して要約したものです。

4 Dellの管理ツールとVendor Kの管理ツールにある、使いやすさに関する主な機能を比較した概要。出典：Principled Technologies

特長	Dellの管理ツールの主なメリット	Vendor Kの管理ツールのデメリット
 リモートBIOS機能の数の多さ	リモート管理を容易にする リモートBIOS機能がiDRAC9には51個ある	Vendor K BMCのリモートBIOS機能は 1個のみ
 BIOS構成の変更が容易	BIOS構成の変更に要する 時間が87%少なく、ステップ数は半分	Vendor Kでは変更をシステムユーティリティ内から行うために 手動の管理者介入が必要
 サーバー構成全体のインポートとエクスポート	完全に構成されたサーバーの構成設定のエクスポートとインポートができるので 複数の同一サーバーの構成に要する時間を短縮 できる	Vendor Kでは 個々のサーバーのBMCのバックアップとリストアのみ が可能
 スケジュールされたアップデートの自動化	iDRAC9ではリポジトリからの 自動アップデートをメンテナンス時間内にスケジュール することができ、管理者による追加の介入は不要	Vendor K BMCには スケジュールされた自動アップデートの機能はない
 包括的なストレージ ステータス概要	iDRAC9ではストレージのステータスが視覚的に表現されるため、 アラート状態のドライブを迅速に特定 できる	Vendor K BMCには同様のビューは ない
 テレメトリ ストリーミング	iDRAC9のテレメトリ対象のメトリック カテゴリ数は2倍（計8カテゴリ）	Vendor K BMCでのテレメトリの対象は 4カテゴリのみ
 接続ビュー	iDRAC9の接続ビューには サーバーのネットワークポートとiDRAC専用ポート接続へのスイッチポートの物理的マッピングの詳細が表示 される	Vendor K BMCにはアップストリームスイッチへの 物理的接続情報はない
 拡張性	OMEでは デバイス最大8,000台を管理 できる ⁵	Vendor Kでは最大で デバイス1,000台のみを管理 できる
 アラートベースのアクション	OMEにはアラートからの入力に基づいてアクションをトリガーする アラートベースのアクション数が2倍（12個） ある	Vendor Kの アラートベースのアクションは4個のみ
 プラグイン アーキテクチャ	OMEではコンソールに追加される プラグインを使用して機能を拡張 できるため、機能を追加しても管理者が追加のアプリケーションを管理する必要はない	Vendor Kのエンタープライズ管理コンソールには 拡張性のためのプラグインベースのアーキテクチャはない

特長	Dellの管理ツールの主なメリット	Vendor Kの管理ツールのデメリット
 サードパーティー製デバイス監視	OMEでは サードパーティー製デバイスとサーバーの監視がサポートされる	Vendor Kのエンタープライズ管理コンソールではサードパーティー製デバイスとサーバーの監視は サポートされない
 レポート作成	OMEでは 42種類の内蔵レポート がありカスタマイズも可能であるため、管理者は目的に応じて最も重要なデータを細分化して選択できる	Vendor Kのエンタープライズ管理コンソールには ネイティブのレポート作成機能はない

リモート管理

iDRAC9なら、管理者は変更のたびにデータセンターに入る必要はありません。iDRAC9には51個のリモートBIOS機能があり、管理者はデータセンターの外部から自由に多数の変更を行うことができるので（Vendor K BMCでは1個だけ）、管理者はBIOS構成の大幅に細分化された制御をどこからでも実行できます（図4を参照）。

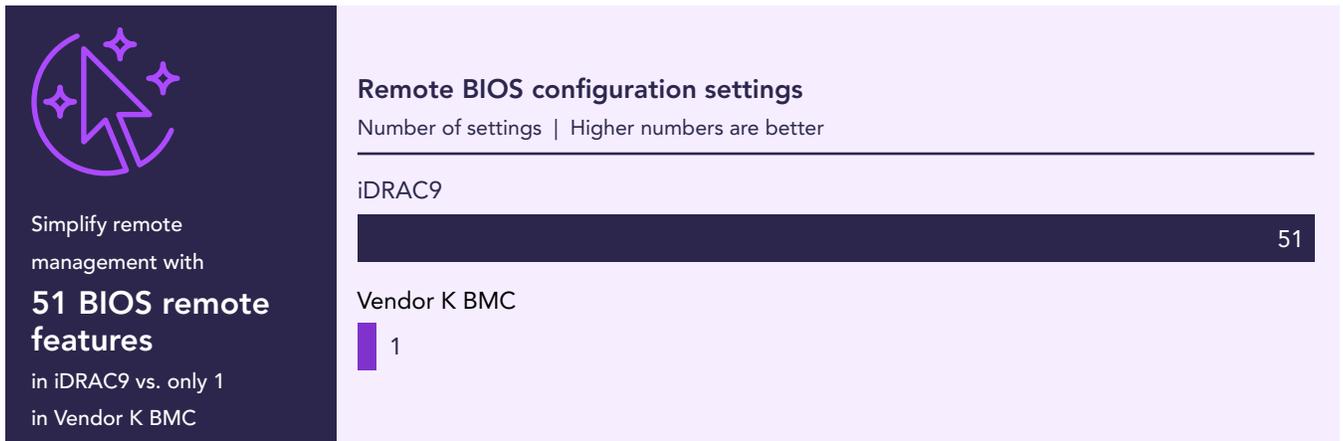


図4：各管理ツールのBIOSリモート機能数の比較。機能がより多いほうが優れています。出典：Principled Technologies

構成に変更を加える

iDRAC9では、管理者はBIOS構成の設定を変更してから、後のリブートのためにアップデートをステージングできるので、管理者の追加の立ち会いは不要ですが、Vendor K BMCでは変更をシステムユーティリティー内から行うこと、変更中に管理者が手動介入する必要があります。図5に示すように、スケジュールに従ったリブートのためにBIOS構成の変更をステージングするときに、iDRAC9ではVendor K BMCと比較して所要時間が87%短く、ステップ数は半分になります。このような節約を大規模な導入環境に当てはめると、管理者が節約できる時間はさらに大きくなります。たとえば、サーバー100台の導入環境では、管理者がBIOS構成項目の変更に必要な時間を6時間以上節約できます。

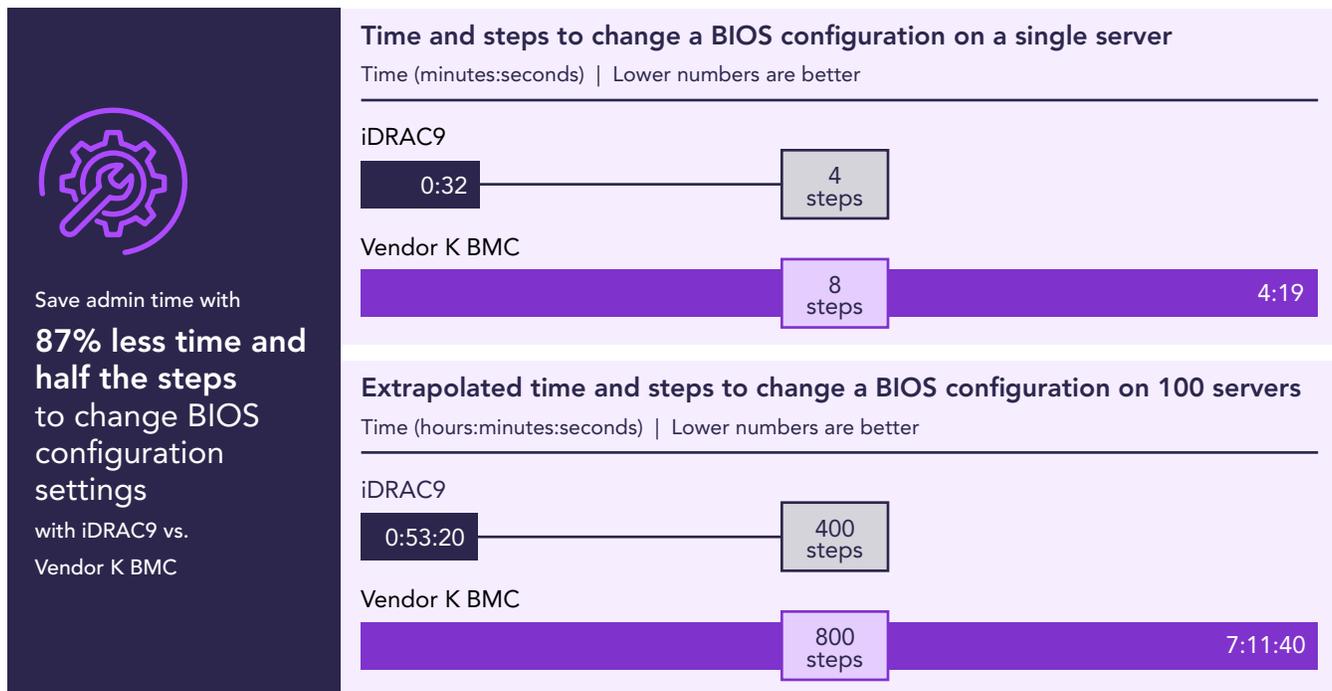


図5：サーバー1台のBIOS構成設定を変更して後のリブートのためにステージングするのに要する時間と、サーバー100台の場合の推定時間。時間とステップ数が少ないほうが優れています。出典：Principled Technologies

アラートベースのアクションのセットアップ

管理者は、自分の席にいないときでも環境の正常性を監視できれば、時間を有効に活用できます。図6に示すように、OMEでは12種類のポリシー駆動型オプションを使用してアラートベースのアクションを実行できるため、環境の状態が特定のしきい値に達するたびに問題軽減措置が自動的に開始されます。対照的に、Vendor Kのエンタープライズ管理コンソールでは、管理者が構成できるアラートベースのイベントは4種類だけです。

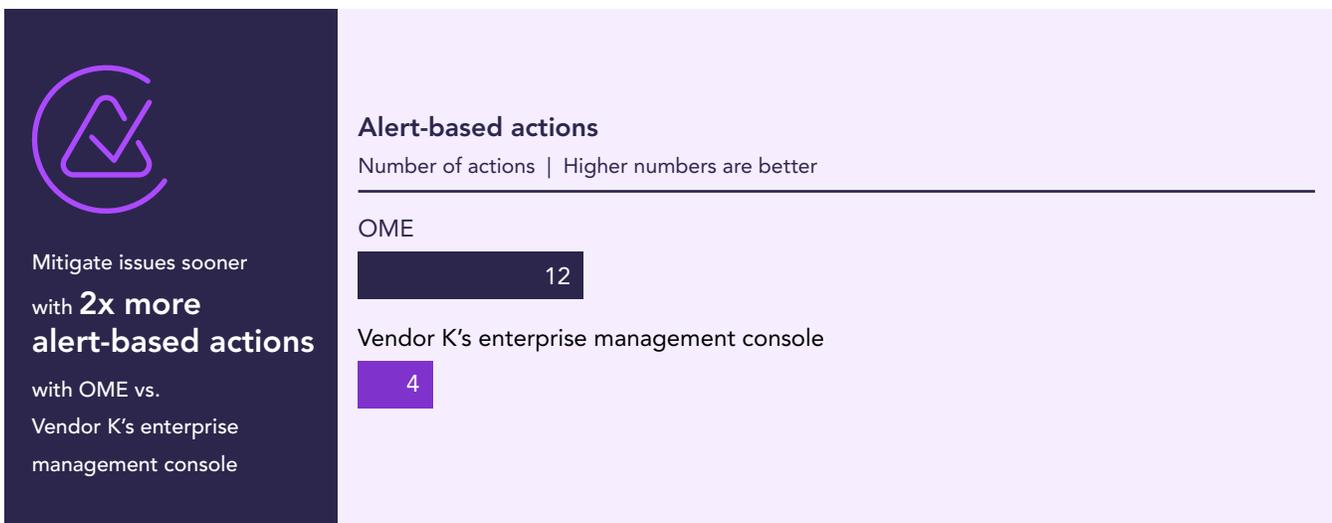


図6：各管理ツールのアラートベースのアクション数の比較。アクション数が多いほうが優れています。出典：Principled Technologies

Dell Technologies OpenManage Enterpriseについて

OMEは、データセンターのための1対多システム管理コンソールです。このコンソールはモダンなHTML5グラフィカル ユーザー インターフェイスを備えており、仮想アプライアンスとしてVMware ESXi™、Microsoft Hyper-V、カーネルベース仮想マシン(KVM)の環境向けに導入できます。OMEではIPv4およびIPv6のネットワーク上での最大8,000台のデバイス（Dell製ラックサーバー、Dell製タワーサーバー、Dell製ブレード、シャーシなど）の検出およびインベントリ登録を行うことができます。⁶ 最近のPT調査で、OMEとOpenManage Enterprise Modular (OME-M)を使用するDell環境ではVLANの変更に必要な時間を短縮でき、スケジュールされたファームウェア アップデート中の介入を回避できることが判明しています。⁷

OMEの詳細情報を<https://www.dell.com/en-us/lp/dt/open-manage-enterprise>でご覧ください。

APEX AIOps Infrastructure Observability（旧称CloudIQ）によるクラウドベースの管理

組み込みツールとエンタープライズ管理コンソールの他にも、Dellのサーバー管理ポートフォリオにはさまざまなツールがあります。APEX AIOps Infrastructure Observability（旧称CloudIQ）も、管理者のための使いやすい自動化ツールであり、インフラストラクチャの正常性とセキュリティの維持をクラウドから行うことができます。

APEX AIOps Infrastructure Observability（旧称CloudIQ）で利用可能な追加のセキュリティ機能

APEX AIOps Infrastructure Observability（旧称CloudIQ）はさまざまなセキュリティ機能を備えており、攻撃に対する組織の防御をさらに強化できます。表5は、その主なセキュリティ機能をまとめたものです。

5 APEX AIOps Infrastructure Observability（旧称CloudIQ）の主なセキュリティ機能の概要。出典：Principled Technologies

特長	APEX AIOps Infrastructure Observability（旧称CloudIQ）がどのように環境のセキュリティを維持するか
 サイバーセキュリティ リスク レベル アラート	サイバーセキュリティに関するインサイトが 特定のセキュリティ リスク レベル アラート とともに自動的に提供されるため、管理者はデータのセキュリティを保つためにさらに速く反応して問題にすばやく対処できます。
 ポリシーベースのセキュリティ構成	ポリシーベースのセキュリティ構成設定が可能であり、簡単に適用できるテンプレートが用意されているため 管理者はセキュリティのベスト プラクティス設定を確実に実施でき、PowerEdge環境が保護されます。
 サイバーセキュリティ アドバイザー	関連性の高いセキュリティ アドバイザーが報告されるため 、具体的な脆弱性の詳細と修復のための推奨事項が得られ、セキュリティ ギャップを埋めるための迅速なアクションが可能になります。

APEX AIOps Infrastructure Observability (旧称CloudIQ) について

APEX AIOps Infrastructure Observability (旧称CloudIQ) はクラウドベースのAIOpsツールであり、「プロアクティブなモニタリング、機械学習、予測分析」をDellの多数の製品とサービス（サーバー、ストレージ、データ保護アプライアンス、ハイパーコンバージド インフラストラクチャなど）に対して行うことができます。⁸ 2022年のPrincipled Technologiesの調査で、CloudIQではネットワーク帯域幅にほとんど影響を与えずにテレメトリ、正常性ステータス、アラート、インベントリを単一のコンソールから監視できることが判明しています。⁹

APEX AIOps Infrastructure Observability (旧称CloudIQ) の詳細を<https://www.dell.com/en-us/dt/apex/aiops.htm>をご覧ください。

APEX AIOps Infrastructure Observability (旧称CloudIQ) のサステナビリティと効率性に関する追加機能

APEX AIOps Infrastructure Observability (旧称CloudIQ) にはサステナビリティと効率性を補強する機能もあり、iDRAC9およびOMEと統合されているため、管理者がPowerEdge環境の正常性を監視するのが容易になります。表6は、その主な機能をまとめたものです。

6 APEX AIOps Infrastructure Observability (旧称CloudIQ) のサステナビリティと使いやすさに関する管理機能の概要。出典：Principled Technologies

特長	APEX AIOps Infrastructure Observability (旧称CloudIQ) の主なメリット
 カーボン フットプリント分析	【モニタリング】セクションにあるこのツールでは、環境全体の二酸化炭素排出量の状況を概要レベルで見ることができ、 予測も可能
 パフォーマンス ビュー	パフォーマンス ビューと異常および使用率のチャートで、 管理者が問題の最初の兆候を知ることができる
 カスタム コンプライアンス レポート	選択されたデバイスについてユーザーが カスタム コンプライアンス レポートを作成できる
 カスタマイズ可能なパフォーマンスとインベントリのレポート	サーバー パフォーマンスとインベントリ データについての カスタム レポート作成オプション があり、管理者は注目しているパフォーマンスとデバイスのメトリックをより詳細に制御できる
 電源に関するアクションのジョブのスケジュール設定	電源に関するアクション（たとえば監視対象の複数のDell PowerEdgeサーバーの電力上限設定）を わずか35秒、6ステップ で実行できる
 ファームウェア アップデートのスケジュール設定	複数の監視対象サーバーのPowerEdgeファームウェア アップデートのスケジュールを わずか41秒、9ステップ で設定できる

結論

セキュリティ、サステナビリティ、管理および監視の機能を比較した結果、Dellのサーバー管理ツールのポートフォリオの管理と監視の機能はVendor Kのポートフォリオよりも堅牢であることが判明しました。セキュリティ面では、iDRAC9のほうが機能が多く、これに含まれる動的システム ロックダウンや多要素認証はVendor Kではまったく提供されていません。さらに、iDRAC9ではデータの脆弱性を縮小するためのUSBポートの無効化に要する時間が大幅に短縮されます。

カーボン フットプリント分析と堅牢な電源管理ツールを備えるOMEを使用すると、Vendor Kのエンタープライズ管理コンソールを使用するときと比べて、組織のサステナビリティ目標達成に向けた計画立案がしやすくなることが判明しました。さらに、Dellのサーバー管理ポートフォリオのほうが自動化とリモート管理のオプションが多いため、特定の定型的な監視とメンテナンスのタスクに要する管理者の時間と労力が削減されることが判明しました。このように優れたセキュリティ、サステナビリティ、管理および監視の機能を備えるDellのサーバー管理ポートフォリオは、効率的でセキュリティが万全なデータセンターを求めている組織にとって魅力的な選択肢です。

1. Harvard Business Review『The Devastating Business Impacts of a Cyber Breach』（2024年4月10日にアクセス）
<https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>
2. Dell『Integrated Dell Remote Access Controller (iDRAC)』（2024年5月17日にアクセス）
<https://www.dell.com/en-us/lp/dt/open-manage-idrac>
3. 注：Vendor KのUSBポート無効化はカスタマイズ可能ですが、それには管理者が無効化対象のポートを個別に（まとめてではなく）選択する必要があります。
4. DOE『DOE Announces \$40 Million for More Efficient Cooling for Data Centers』（2024年5月20日にアクセス）
<https://www.energy.gov/articles/doe-announces-40-million-more-efficient-cooling-data-centers>
5. Dell『OpenManage Enterpriseサポート マトリックス』（2024年5月21日にアクセス）
<https://www.dell.com/support/kbdoc/en-us/article/lkbprint?ArticleNumber=000217909&AccessLevel=10&Lang=en>
6. Dell『OpenManage Enterprise』（2024年5月17日にアクセス）
<https://www.dell.com/en-us/work/learn/openmanage-enterprise>
7. Principled Technologies『A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators』（2024年5月17日にアクセス）
<https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>
8. Dell『APEX AI Ops : デジタル ビジネスにおけるITの複雑さを軽減』（2024年6月11日にアクセス）
<https://www.dell.com/en-us/dt/apex/aiops.htm>
9. Principled Technologies『Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests』（2024年4月9日にアクセス）
<https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>

このレポートの背景情報をご覧ください ▶

▶ オリジナルの英語版レポートはこちらをご覧ください



Facts matter.®

Principled Technologiesは、Principled Technologies, Inc.の登録商標です。他のすべての製品名は各社の商標です。詳細情報については、このレポートの背景情報を参照してください。

このプロジェクトは、デル・テクノロジーズの委託を受けて作成されています。