



セキュリティを強化する
**セキュリティ機能の数が
3.5倍**

iDRAC9での2要素認証と
外部キー管理を含む



エネルギー効率を最適化する
**電力消費レポートの
数が6倍**

Dell OMEのレポート数は20、
Supermicro SSMのレポート数は3



**管理時間を1時間50分
短縮して運用効率を
向上**

サーバー100台あたり

Dell iDRAC9で自動アップデートを
使用する場合と、自動アップデートが
ないSupermicro IPMIとの比較

セキュリティ、サステナビリティ、効率性を 高める堅牢な Dell のサーバー管理 ツール

Supermicro 管理ポートフォリオとの比較

データセンター用の新しいサーバーに投資する際は、ハードウェアを選定するだけでなく、運用管理ソリューションの選定も必要になります。効率性の高い機能豊富なツールを使用し、エネルギー効率の向上を図りながらインフラストラクチャの導入、監視、保守、保護ができれば、管理者の日々の管理業務は容易になり、組織を前進させるイノベーションに多くの時間を費やせます。堅牢な管理ツールを備えるベンダーからソリューションを購入することで、将来的に時間とコストを節約することができます。

Dell™ と Supermicro® のサーバー管理ポートフォリオを評価するため、このテストでは Dell の3つのツールと Supermicro の2つのツールを比較しました。

表 1：当社がテストした管理ツール。*Dell CloudIQ はクラウドベースの監視と分析のツールです。Supermicro から同等のツールは提供されていません。

出典：Principled Technologies

	Dell	Supermicro
組み込み型またはリモートサーバー管理	iDRAC9 (Integrated Dell Remote Access Controller)	Supermicro Intelligent Management (IPMI)
1対多デバイス管理コンソール	Dell OpenManage™ Enterprise (OME) Dell CloudIQ*	Supermicro Server Manager (SSM)

サステナビリティ、セキュリティ、日常的な管理体験の観点から、より多くの機能を備えたツールセットを一貫して提供しているのは Dell であり、幅広いオプションと能力で管理者を支援していることがわかりました。

サーバー管理の自動化と簡素化を可能にする豊富な機能

IT チームが求めているのは、日常業務の所要時間を短縮し、セキュリティや効率性の最新基準に対応する、機能豊富な最新の管理ツールです。今回評価した Dell の管理ツールには、Supermicro 管理ポートフォリオにはない多数の機能が含まれています。

サステナビリティ

エネルギー コストの上昇と環境規制の増加に伴い、多くの組織がサステナビリティに重点を置くようになりました。データセンターは本質的に大量の電力を必要としますが、温度や電力消費を慎重に管理することで消費電力を削減できます。Dell OpenManage Enterprise には、電力消費の綿密な監視と管理を可能にするさまざまな機能が組み込まれているため、サステナビリティの目標到達を支援できる可能性があります。表 2 と表 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。

表 2: Dell OpenManage Enterprise と SSM のサステナビリティの相違点。出典: Principled Technologies

特長	Dell の管理ツール		Supermicro の管理ツール	
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		✓		×
カーボン フットプリント分析		✓		×
温度をトリガーとする電源管理ポリシー		✓		×
静的電源管理ポリシー		✓		✓

表 3: Dell OME と Supermicro SSM および IPMI の比較の概要。出典: Principled Technologies

特長	Dell の管理ツールの主なメリット	Supermicro 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達成に役立てるために、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	同等の機能がない ため、サステナビリティ目標を達成するための計画が困難
 カーボン フットプリント分析	OpenManage Enterprise Power Manager を使用することで 可能 。サステナビリティの目標達成に役立つ二酸化炭素排出量に関するデータが提供される	同等の機能がない 。サステナビリティの目標達成を監視する際に役立つカーボンフットプリントの追跡方法がない
 電源管理と温度管理の自動化	静的および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）	静的ポリシー タイプは 1 つで 、トリガーオプションが関連付けられていない
 電力消費レポート	レポートの数が 6 倍以上 。E メール配信のスケジュール設定およびカスタマイズオプションを備える 20 種類の組み込み レポート	組み込みレポート 2 種類 (SSM)、エクスポート不可のレポート 1 種類 (Supermicro IPMI)
 電源管理指標	最大 15 倍の指標 から、電力消費管理に関する細かいインサイトを得られる	1 種類のみ 。電力消費に関するインサイトや管理が少ない

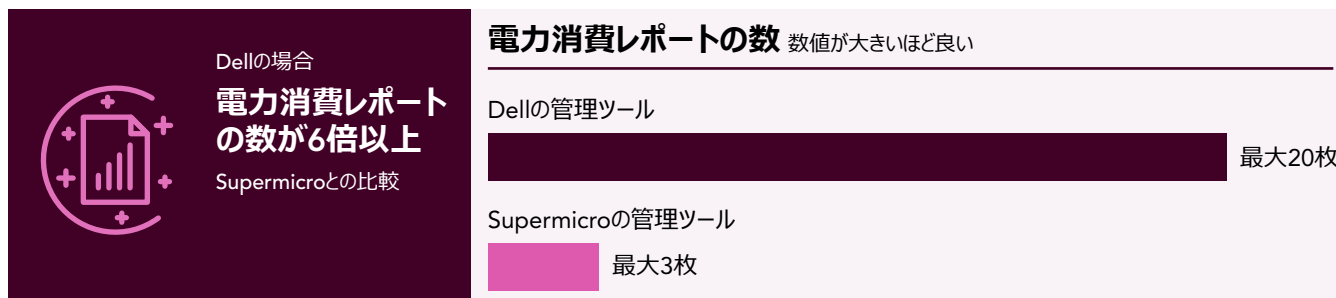


図1: Dell OMEとSupermicro SSMで使用可能な電力消費レポートの数。出典: Principled Technologies

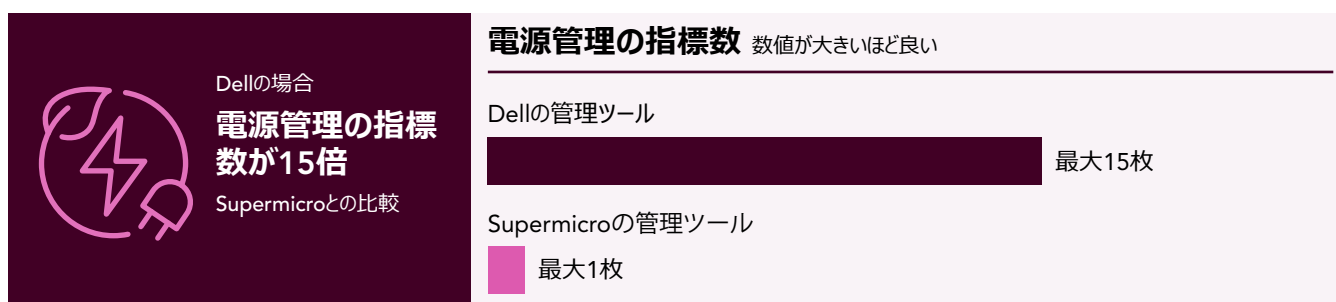


図2: Dell OMEとSupermicro SSMで使用可能な電源管理指標の数。出典: Principled Technologies

電源管理と温度管理の自動化

OpenManage Enterprise Power Managerでは電源管理と温度管理を自動化でき、電力と温度の両方をトリガーとする静的ポリシー オプションを備えているため、管理者は電力消費または温度のしきい値を設定して冷却コスト削減に役立てることができます。一方、SSM にはポリシーが 1 つしかありません。これは電力消費に対する静的な制限であり、サーバーがこの制限を超えても自動的にトリガーされるわけではないため、エネルギー コストが高くなる可能性があります。

最適化を視野に入れてデータセンターの電力消費管理を考えている組織は、**20 種類の電力消費レポートが組み込まれた** OpenManage Enterprise Power Manager からメリットを得ることができます。これらのレポートは、効率性を最大限に高めるためのキャパシティ プランニングや電源管理に役立ちます。SSM のレポート オプションには多くの制限があります。管理者はサービス レポートを備えるホストを 1 台しか実行できません。また、電力消費の傾向をモニタリング画面で確認することしかできません。Supermicro IPMI では、コンポーネントレベルの電力グラフを BMC に表示できますが、グラフのデータはエクスポートできないため分析には使用できず、画像として保存することしかできません。

OpenManage Enterprise Power Manager プラグインを使用すると、コンポーネント別の電力使用量、エアフロー、コンポーネント使用率など、**最大 15 種類の指標を表示できます**。一方、SSM で確認できるのは総電力使用量のみです。

二酸化炭素排出量とカーボン フットプリントの分析

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含まれています。各種機能の中でも、特にこれらの機能は温室効果ガスの排出量推定に役立ちます。このツールは、エネルギー消費量単位に対する電力コストと二酸化炭素排出量のデフォルト値を示しますが、地域の電力コストとデータセンターの消費モデルに合わせて値をカスタマイズできます。SSM は同等の機能を提供していないため、組織がサステナビリティ目標に向けて計画を立て、進捗を監視することは困難です。

セキュリティ

サイバー犯罪は急増しており、データの損傷や破壊、金銭の盗難、生産性の低下、知的財産の盗難、個人情報や財務情報の盗難、横領、詐欺、攻撃後の通常業務の混乱、フォレンジック調査、ハッキングされたデータとシステムの復元や削除、評判への危害など、大きな脅威を企業に与えています。¹ このような状況においては、セキュリティを考慮してサーバー購入の意思決定を行うことが不可欠です。Dell OpenManage Enterpriseにはデータの安全性を保つための機能が複数組み込まれています。このような機能はSupermicroツールには含まれていません（表4および5を参照）。

表4： Dell管理ツールとSupermicro管理ツールのセキュリティの相違点。出典：Principled Technologies

特長	Dellの管理ツール		Supermicroの管理ツール	
多要素認証		✓		x
外部キー管理		✓		x
スコープベースのアクセス制御		✓		x
ポリシーベースのセキュリティ構成		✓		x
サイバーセキュリティ アドバイザリー		✓		x
ロールベースアクセス制御		✓		✓
動的USBポート無効化		✓		✓

表5： DellとSupermicroの管理ツールのセキュリティ機能比較の概要。出典：Principled Technologies

特長	Dell の管理ツールの主なメリット	Supermicro の管理ツールのデメリット
 多要素認証 (MFA)	E メールと RSA SecurID のいずれかを使用する iDRAC の 2 要素認証により、権限のないユーザーが機密データにアクセスするのを防止	同等の機能がないため、セキュリティ ギャップが生じ、権限のないユーザーに機密データへのアクセスを許可してしまう可能性がある
 外部キー管理	iDRAC の Secure Enterprise Key Manager により、さらなるセキュリティ層が追加され、サーバー上の静止データをドライブの暗号化と一元管理を通じて保護できる	同等の機能がないため、さらに別のセキュリティ ギャップが生じる
 アクセスコントロール	OME には、ロールベースのアクセス制御 (RBAC) とスコープベースのアクセス制御 (SBAC) の両方があるため、デバイス マネージャーがアクセスできるデバイス グループを制限できる	RBAC のみ。アクセス制限に関する管理能力が限定される
 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 (CloudIQ 経由) により、管理者に不一致を警告	同等の機能がないため、侵害に対するアクションや修復が遅れる可能性がある
 サイバーセキュリティ アドバイザリー	セキュリティ アドバイザリー レポート (Dell CloudIQ セキュリティ経由)。脆弱性の詳細や適用可能な修復策がわかり、迅速に措置を講じることができる	同等の機能がないため、セキュリティ ギャップが生じ、攻撃者に悪用される可能性がある

多要素認証

多要素認証 (MFA) は、権限のないユーザーや攻撃者による機密データへのアクセスを防止するのに役立ちます。Dell iDRAC では、E メールまたは RSA SecurID (多くの業界で使用されている外部多要素認証テクノロジーのセット) を使用した 2 要素認証が可能です。² この機能は Supermicro IPMI にも SSM にも存在しないため、セキュリティギャップが生じます。

キー管理

外部キー管理システム (KMS) を使用すると、サーバーのストレージのロックとロック解除に使用するキーをサードパーティ製の独立したサーバーで管理できるため、セキュリティがさらに強化されます。iDRAC には、すべての新しい Dell PowerEdge サーバーに対応する Local Key Manager (LKM) が含まれています。一部のライセンスでは Secure Enterprise Key Manager (SEKM) も提供されるため、フル ディスク暗号化と外部キー管理によるさらなるセキュリティ強化が可能です。SEKM は業界標準の OASIS KMIP プロトコルをサポートしているため、この標準を使用している任意の外部 KMS プロバイダーを選択して利用できます。Supermicro には、このセキュリティ機能または同等の機能はありません。

アクセスコントロール

アクセス可能なシステム領域と実行可能なタスクをユーザーのロールによって決定する、ロールベースのアクセス制御 (RBAC) は、多くのサーバー セキュリティ戦略にとって不可欠な要素です。OpenManage Enterprise の RBAC では、管理者、デバイス マネージャー、閲覧者という 3 つの組み込みロールでユーザー権限を定義します。³ また、デバイス マネージャーがアクセス可能なデバイス グループを管理者が制限できる、スコープベースのアクセス制御 (SBAC) も提供されています。⁴ 管理者は、デバイスのサブセットに対するアクセス権をユーザーに付与できます。Supermicro は RBAC を提供していますが、SBAC は提供していません。

認証情報の管理

iDRAC のパスワード ローテーションは、セキュリティポリシーに従って OpenManage Enterprise へのアクセスをローテーションさせる (デフォルトは月ごと)、外部パスワード ハンドラと連携する、パスワードを管理するため CyberArk をサポートする、など、複数の目的を果たします。^{5,6}

OpenManage Enterprise を使うと、管理者は静的な既知の管理者アカウントの代わりに OME が管理するサービス アカウントを使用して、iDRAC パスワード ローテーションを管理できます。SSM にはこの機能はありません。

ポリシーベースのセキュリティ構成

Dell の CloudIQ for PowerEdge AIOps ソリューションは、ポリシーベースのサイバーセキュリティ機能を備えています。導入済みの PowerEdge サーバーの構成を、Dell のベスト プラクティスを基準とするセキュリティ関連の構成ポリシーと比較するという機能で、CloudIQ は不一致を検出すると、管理者にその旨を通知し、修復手順を提示します。⁷ SSM には同等の機能がないため、侵害の検出が遅れる可能性があります。

サイバーセキュリティ アドバイザリー

セキュリティ アドバイザリーとは、セキュリティ問題を一般に通知することです。Dell によると、CloudIQ の Dell Security Advisories ページには、該当するセキュリティ アドバイザリーの完全なリストと、それらの影響、影響を受けるシステムの数、公開日が記載されています。⁸ Dell CloudIQ には、脆弱性の詳細と修復の提案を含むセキュリティ アドバイザリー レポート作成機能があります。SSM には同等の機能がなく、システムに脆弱性が生まれる可能性があります。

Dell CloudIQ について

Dell CloudIQ はクラウドベースの AIOps ツールです。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、Dell のさまざまな製品やサービスに「プロアクティブなモニタリング、機械学習、予測分析」の機能を提供します。⁹ 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ることなくテレメトリー、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。¹⁰

CloudIQ の詳細については、<https://www.dell.com/en-us/dt/solutions/cloudiq.htm> を参照してください。

動的 USB ポート無効化

USB ポート経由でのサーバー アクセスは、USB ポートの無効化と有効化で制御できます。これにより、サーバーの悪用を防止したり、禁止されているアプリケーションやウイルスがインストールされるリスクを回避したりできます。

Dell iDRAC には動的 USB ポートを無効化する独立した機能があり、ダウンタイムを必要としません。Supermicro は動的な前面 USB（および背面 USB）を無効化する機能が BIOS 内にありますが、有効化するには Supermicro DataCenter Management Suite per Node License Key が必要です。この機能をトリガーするためシステム ロックダウン コマンドを実装し、BMC または Supermicro IPMI コンソールから実行することもできますが、システム ロックダウン モードからは独立していません。¹¹

図 3 に示すように、Dell iDRAC を使用してポートを無効化するプロセスは**わずか 41 秒、4 ステップで完了したの**に対し、Supermicro IPMI は**4 倍以上の 2 分 50 秒を要し、6 ステップが必要になりました**。100 台のシステムを考えると、3 時間 35 分もの時間を節約できることになります。つまり、Supermicro IPMI を使用するとおよそ半日を費やす作業になるところ、Dell iDRAC を使用すれば 1 時間強しかかかりません。

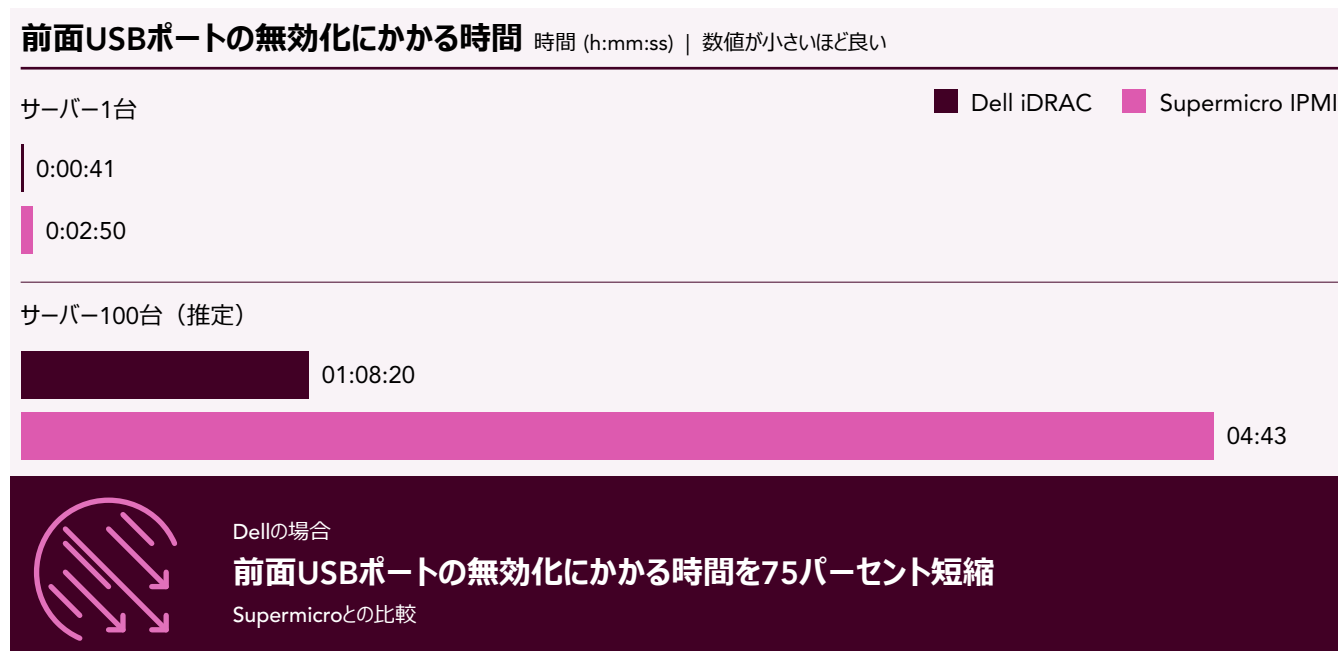


図 3：1 台のサーバーの前面 USB ポート無効化に要する時間と、100 台のサーバーの前面 USB ポート無効化に要する推定時間。数値が低いほど良い。出典：Principled Technologies

Dell OpenManage Enterprise について

OpenManage Enterprise は、データセンター用の 1 対多のシステム管理コンソールです。最新の HTML5 グラフィカル ユーザー インターフェイスを備え、仮想アプライアンスとして VMware ESXi™ 環境、Microsoft Hyper-V 環境、カーネルベースの仮想マシン (KVM) 環境に導入できます。OpenManage Enterprise では、Dell 製ラックサーバー、Dell 製タワーサーバー、Dell 製ブレードやシャーシなど、IPv4 および IPv6 ネットワーク上のデバイスを 8,000 台まで検出でき、インベントリ登録できます。¹² 最近の PT 調査で、OpenManage Enterprise と OpenManage Enterprise Modular (OME-M) を使用する Dell 環境では VLAN の変更に要する時間を短縮できるほか、スケジュールされたファームウェア アップデートに人が介入しなくてよいことが判明しています。¹³

OpenManage Enterprise の詳細については、<https://www.dell.com/en-us/lp/dt/open-manage-enterprise> を参照してください。

モニタリング、分析、使いやすさ

モニタリング、分析、日常的なタスク実行（アップデートのスケジュール設定など）といった管理者業務をどのようにサポートするかについては、各社の管理ツールによって大きな違いがあります。このセクションでは、それらの違いを Dell と Supermicro の管理ツールの調査結果から考察します。サステナビリティとセキュリティ機能の調査から、Dell の管理ツール スイートには、Supermicro のツールにはない、管理者業務を楽にする多数の機能が備わっていることがわかりました。表 6 は、ツールに要求される管理上のメリットを比較したものです。

表 6：Dell と Supermicro の管理ツールの比較の概要。出典：Principled Technologies

特長	Dell の管理ツールの主なメリット	Supermicro の管理ツールのデメリット
 テレメトリー ストリーミング	リモート Syslog サーバーで 使用可能な iDRAC9 テレメトリー ストリーミング 。障害の予測とパフォーマンスの最適化に役立つ。Grafana や Splunk などの分析ツールにサーバー 指標をストリーミング可能	自動テレメトリー ストリーミングなし
 モバイル監視および管理	OME および iDRAC9 と連携する機能豊富な iOS および Android 向けの OpenManage Mobile アプリ	SSM と 連携しない Supermicro IPMIView アプリ
 サードパーティ製デバイスやサーバーの監視	OME は サードパーティ製デバイスやサーバーの監視をサポート （主要競合他社のものを含む）	サポートしているサードパーティ製デバイスは、Supermicro のエージェントや BMC を使用しているデバイス、IPMI に対応する同社の旧バージョンの機器、Redfish 対応デバイスのみ
 資産の監視	OME および CloudIQ 経由で利用可能。OME では、ライセンスを受けた管理対象サーバー上のデータを CloudIQ に送信し、複数のデータセンターにわたるモニタリングが可能	クラウドベースのポータルがないため、複数のデータセンターのモニタリング データを集約できない
 アラートベースのアクション	OME のポリシー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はない
 サーバーへの導入が容易（システム構成のインポート / エクスポート機能）	iDRAC9 を使用してサーバーのすべての構成項目を インポートまたはエクスポートできる 。インポートには 48 秒と 5 ステップ、エクスポートには 1 分 9 秒、7 ステップしかかからない	インポートまたはエクスポートできるのは Baseboard Management Controller (BMC) 構成のみ で、サーバーごとに大量の手動構成が必要
 BIOS 構成設定の変更にかかる時間を短縮	すべての BIOS 設定を iDRAC から直接速やかに変更 でき、メンテナンス ウィンドウに向けてアップデートのステー징や再起動ができるため、管理時間を大幅に削減できる	一部の BIOS 変更は BMC から実行可能 。それ以外の場合はサーバーの再起動が必要。手動の手順が多く、管理に時間がかかる
 仮想アプライアンスとしての実行	OME で 可能 。OS のアップデートが不要になる	同等の機能はなく 、管理対象 OS 内で実行する必要があるため、パッチ適用やアップデート用のコンポーネントが 1 つ増える
 接続ビュー	iDRAC で 使用可能 。LLDP を使用するトラブルシューティング ツールとして、ケーブル接続やスイッチ ポート不良などのネットワーク問題を診断できる	接続ビューなし 。アップストリーム スイッチ ポートに関する物理的接続の情報なし
 ファームウェアとドライバーのアップデートをスケジュールする機能	OME と iDRAC で 使用可能	BIOS や BMC ファームウェアのアップデートはスケジュールできるが、 ドライバーのアップデートはスケジュールできない

BIOS 構成項目の変更

Dell の場合、すべての BIOS 構成設定を iDRAC から直接変更でき、次の再起動に備えて変更をステージングできます。Supermicro の場合、BMC から設定できるのは一部の BIOS 設定のみです。設定項目が限定されているのに加え、Supermicro サーバーで BIOS 構成を変更する場合は、1 つの構成項目ごとに管理者がサーバーを再起動し、ブート画面から BIOS 構成メニューにアクセスしなければなりません。

図 4 は、Dell iDRAC と Supermicro IPMI を使用して、単一サーバーで BIOS 構成設定を変更したときの所要時間を示しています。**Supermicro ツールを使用する手動プロセスの所要時間は、iDRAC で自動プロセスを設定する場合よりも 2 分 6 秒長く(4.9 倍) になります。**同一構成のサーバー 100 台で所要時間を推定すると、iDRAC では 3.5 時間もの時間を節約できます(サーバーが同一構成でない場合、これほどの時間は節約できない可能性があります)。



図4：1台のサーバーと100台の同一構成サーバーでBIOS構成変更を実行したときの所要時間（推定）。数値が低いほど良い。出典：Principled Technologies

iDRAC9 について

Dell PowerEdge™ サーバーには Integrated Dell Remote Access Controller 9 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。

- API とスクリプティング ツールを使用して数千台のサーバーを管理できる
- 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 ¹⁴

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。

ファームウェアとドライバーのアップデートの自動化

iDRAC

Supermicro IPMIとは異なり、Dell iDRACではファームウェアの自動アップデートをスケジュールできます。スケジュールに基づく自動アップデートの構成は1回限りの作業であるため、アップデートサイクルのたびに時間を節約できます。図5は、Dell iDRACとSupermicro IPMIを使用して、100台のサーバーにファームウェアの自動アップデートを初めてスケジュールする際の推定所要時間を示しています。Supermicro ツールを使用する手動プロセスの所要時間は、iDRACで自動プロセスを設定する場合よりも**13分長**くなります。

管理者が毎月第1土曜日の夜にその月のスケジュールを設定すると仮定すると、iDRACを使用する管理者はサーバーあたり58秒の時間投資を一度だけ行うことになります。サーバーが100台ある場合は1時間36分40秒が必要ですが、この作業は1回限りです。一方、Supermicro IPMIを使用する管理者は、メンテナンスウィンドウごとに、100台のサーバーに対して1時間50分の時間投資を行うことになります。1回限りのiDRACのセットアップ時間と、毎回必要なSupermicro IPMIの最初のセットアップ時間を比較すると、Dell管理ツールでは約13分20秒の時間を節約できます。(図5を参照)。

ただし、Dellの場合、2回目以降は管理者がタスクを実行する必要がないため、**毎回110分の時間を節約できることになります。**(図6を参照)。100台のサーバーが同一構成でない場合でも、同様に時間を節約できます。ここに示されている時間は、あくまでファームウェアをBMCにアップロードする時間です。Supermicroファームウェアのダウンロードや抽出にかかる時間は反映されていないことに留意してください。

OME

Dell OMEは、**すべてのコンポーネントのファームウェアアップデート**と、Windowsドライバーアップデートをサポートしています。SSMはBIOSおよびBMCファームウェアのアップデートをサポートしていますが、**ドライバーのアップデートや他のコンポーネントのアップデートはサポートしていません。**

自動ファームウェア アップデートを初めてスケジュール設定する際の推定所要時間 (100台のサーバー)

時間 (h:mm:ss) | 数値が小さいほど良い

Dell iDRACの自動スケジュール設定プロセス

01:36:40

Supermicro IPMIの手動プロセス

01:50:00



ファームウェアの自動アップデートを100台のサーバーに対して初めてスケジュールするときに、最大13分の時間を節約できる

図5: 100台のサーバーでファームウェアを最初にアップデートするのに要する推定時間。数値が低いほど良い。出典: Principled Technologies

自動ファームウェア アップデートを2回目以降にスケジュール設定する際の各回の推定所要時間 (100台のサーバー)

時間 (h:mm:ss) | 数値が小さいほど良い

Dell iDRACの自動スケジュール設定プロセス

追加の作業時間は発生しない

Supermicro IPMIの手動プロセス

01:50:00



プロセスの自動化により管理時間を短縮。初回設定後はアップデート時間が不要

図6: 100台のサーバーでファームウェアを各回アップデートするのに要する推定時間。数値が低いほど良い。出典: Principled Technologies

結論

サーバーを購入するベンダーを選定する際は、ハードウェア プラットフォームだけでなく様々な要素を考慮することが重要です。意思決定者は、システムやデータのセキュリティ、エネルギー効率、管理の容易性といった長期的な懸念事項についても検討する必要があります。これらの懸念事項を考えれば、ベンダーが提供するシステム管理ツールはハードウェアと同様に重要です。

今回のサーバー管理ツール調査では、Dell iDRAC9 と Supermicro IPMI を比較して組み込みサーバー管理機能を評価し、Dell の OpenManage Enterprise と CloudIQ を Supermicro Server Manage と比較して、一対多デバイスおよびコンソール管理および監視機能を評価しました。その結果、Dell の管理ツールは、Supermicro サーバーよりも包括的なセキュリティ、サステナビリティ、管理および監視機能を備えていることがわかりました。また、Dell のツールは多くのタスクを自動化してサーバー管理を容易にし、管理者の時間を大幅に節約しているのに対し、Supermicro ツールでは管理者が同じタスクを繰り返し手動で実行する必要があります。

サーバーを購入する際には、データの保護、より持続可能な環境のサポート、システム メンテナンスの簡素化という点から、ベンダーが提案する管理製品について検討することが不可欠です。当社のテストと調査によると、PowerEdge サーバー向けの Dell 管理ポートフォリオは、Supermicro が提供する同等の管理製品よりも、これらの目標を達成するための機能をより多く提供していることがわかりました。

1. Steve Morgan 「Cybercrime To Cost The World \$10.5 Trillion Annually By 2025」 (2024 年 2 月 15 日にアクセス) <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>
2. Dell 「Using iDRAC9 RSA SecurID 2FA」 (2024 年 2 月 15 日にアクセス) <https://dl.dell.com/Manuals/Common/dellemc-idrac9-rsa-securid-2fa.pdf>
3. Dell 「Dell EMC OpenManage Enterprise SupportAssist バージョン 1.1 ユーザーズ ガイド」 (2024 年 2 月 15 日にアクセス) [https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?](https://www.dell.com/support/manuals/en-us/openmanage-enterprise-supportassist/omesapuserguide11/role-and-scope-based-access-control-in-openmanage-enterprise?context=server)
4. Dell 「Dell EMC OpenManage Enterprise SupportAssist バージョン 1.1 ユーザーズ ガイド」
5. Dell 「OpenManage Enterprise 4.0:iDRAC のパスワード管理とローテーション」 (2024 年 2 月 15 日にアクセス) <https://www.dell.com/support/kbdoc/en-us/000219279/openmanage-enterprise-4-0-idrac-password-management-and-rotation>
6. Dell 「OpenManage Portfolio Software Licensing Guide」 (2024 年 4 月 3 日にアクセス) <https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/openmanage-portfolio-software-licensing-guide.pdf>
7. Mark Maclean および Kyle Shannon 「Dell CloudIQ Cybersecurity For PowerEdge: The Benefits Of Automation」 (2024 年 2 月 15 日にアクセス) <https://infohub.delltechnologies.com/en-US/p/dell-cloudiq-cybersecurity-for-poweredge-the-benefits-of-automation/>
8. Dell 「Security Advisories」 (2024 年 2 月 15 日にアクセス) <https://infohub.delltechnologies.com/en-US/l/cloudiq-a-detailed-review/security-advisories/>
9. Dell 「Dell CloudIQ - AIOps for Intelligent IT Infrastructure Insights」 (2024 年 2 月 15 日にアクセス) <https://www.dell.com/en-us/dt/solutions/cloudiq.htm>
10. Principled Technologies 「Dell CloudIQ provides a single console for proactive monitoring and had negligible impact on network bandwidth in our tests」 (2024 年 1 月 17 日にアクセス) <https://www.principledtechnologies.com/dell/CloudIQ-network-0422.pdf>
11. Supermicro 「X13DEM User's Manual」 (2024 年 2 月 16 日にアクセス) <https://www.supermicro.com/manuals/motherboard/X13/MNL-2407.pdf>
12. Dell 「OpenManage Enterprise」 (2023 年 12 月 20 日にアクセス) <https://www.dell.com/en-us/work/learn/openmanage-enterprise>
13. Principled Technologies 「A Dell PowerEdge MX environment using OpenManage Enterprise and OpenManage Enterprise Modular can make life easier for administrators」 (2024 年 1 月 17 日にアクセス) <https://www.principledtechnologies.com/Dell/PowerEdge-MX-OME-OME-M-0124.pdf>
14. Dell 「Integrated Dell Remote Access Controller (iDRAC)」 (2024 年 1 月 16 日にアクセス) <https://www.dell.com/en-us/lp/dt/open-manage-idrac>

このレポートの背景情報を読む ▶



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。