Dellインフラストラクチャ システムの接続

目次

目次（続き）

概要

1：セキュア コネクト ゲートウェイ テクノロジー プラットフォームとは何ですか？

セキュア コネクト ゲートウェイ5.xテクノロジーは、Dell Technologies Servicesが提供する次世代の接続ソフトウェアです。

Dellのインフラストラクチャ ポートフォリオ全体（サーバー、ネットワーキング、データストレージ、データ保護、コンバージド、ハイパーコンバージド(CI/HCI)の各ソリューション）**に適用できる単一の接続ソリューション**です。これはレガシー ソフトウェアのSupportAssist EnterpriseおよびSecure Remote Servicesに替わるものです。これらのレガシー ソリューションの機能は、このテクノロジーに統合されています。

お客様によるインストールとアップグレードが可能な柔軟な導入オプションが用意されています。ゲートウェイ オプション（仮想アプライアンス、スタンドアロン アプリケーション、またはコンテナ エディションとして提供）、直接接続オプション、プラグイン オプションが用意されているため、環境に適したものを選択できます。

当社のテクノロジーは、**リモートITサポートおよびモニタリング ソフトウェアとも呼ばれ**、以下を可能にします。

- 極めて重要な問題に関するインサイト
- デル・テクノロジーズとお客様の環境をリモートで結ぶ安全な双方向通信で、問題をより迅速に解決
- 高度な監査および制御機能を備えたポリシーマネージャー ソフトウェア、クラス最高レベルのMQTTプロトコル、および新しい開発プロセスによって、継続的にセキュリティを注視
- Dell Enterprise環境全体でより多くのテレメトリー データとアクションを処理するゲートウェイによる、パフォーマンスと拡張性の向上
- オンプレミス接続管理ダッシュボード向けの強化されたWeb UIエクスペリエンス

購入したDellインフラストラクチャ製品にサポート サービス契約（たとえば、ProSupport Infrastructure Suiteの任意のサービス レベル）がバンドルされていると、この接続ソフトウェアを無償で設定できます。ライセンスは必要ありません。

当社のソフトウェアでこれらのシステムをモニタリングすると、よりスマートなAI、自動サポート、リアルタイム分析の独自の統合が提供されます。

2：ゲートウェイ オプションを使用する以外にも接続する方法はありますか？

はい。Secure Connect Gatewayテクノロジーは、一部のDell製ハードウェアとプラグインの直接接続バージョンとしても実装されています。

一部のDell製品では、デル・テクノロジーズのバックエンドに直接接続できます。この方法は、別途ソフトウェアをセットアップすることを希望されないお客様に適しています。製品マニュアルを参照してください。*詳細については、Q12とQ28をお読みください。*

OpenManageをご利用のPowerEdgeデータセンターのお客様は、OpenManage Enterpriseのサービス プラグインに接続して、アラート、自動ディスパッチ、収集の各機能を使用できるようになりました。

テクノロジーの詳細：Dell.comにアクセスすると、当社のエキスパートの意見を聞いたり、技術リソースを入手したりできます

インフォグラフィックと重要なリンク：データセンターへの接続を始める

3：レガシー ソフトウェア（SupportAssist EnterpriseとSecure Remote Services）は廃止されていますか？

Secure Remote Services v3.xのVirtual EditionとDocker Editionは、2024年1月31日に完全に廃止されました。サポート対象のDell Storage、ネットワーキング、CI/HCIシステムのインテリジェントな自動サポートは廃止されました。

- メモ：**直接接続を利用するDell PowerStoreおよびUnity製品**を使用しているお客様の場合、そのテクノロジーは2024年12月31日をもって廃止されました。サービスの中断を回避するために、サポート終了日前に動作環境のアップデートが利用可能になります。

SupportAssist Enterprise 4.xおよび2.xは、2022年7月31日をもって廃止されました。Dellのサーバー、ストレージ、ネットワーキング、CI/HCIシステムのインテリジェントな自動サポートは廃止されました。

4：このソフトウェアは、ユーザーによるインストールとアップグレードが可能ですか？

はい。接続テクノロジーは、デル・テクノロジーズのサポートなしでダウンロードしてインストールできます。

ゲートウェイおよびプラグイン ソフトウェアのリソースについては、Dellサポート サイトにアクセスしてください。

- **ヒント：**インタラクティブなテクニカル デモ（英語のみ）で、ゲートウェイ エディションとポリシーマネージャー ソフトウェアをインストール、登録、使用する方法を確認できます。

5：ライセンスは必要ですか？

ソフトウェア ライセンスは必要ありません。ただし、ソフトウェアをダウンロードして登録するには、Dell.comサポートで認証を受ける必要があります。

テクノロジーの特長と価値

6：接続ソフトウェアを使用すると、Dellのサポート体験からどのような価値が得られますか？

企業が当社の接続ツールを使用する主な理由は、環境内のダウンタイムを短縮し、重大な問題をモニタリングする負担を軽減し、小さな問題がコストのかかる大きな問題になる前に特定して修正することです。

接続をセットアップすると、ProSupport Infrastructure Suiteのあらゆるサービス レベルなど、**サポート サービスを備えたDellインフラストラクチャ製品のサポート エクスペリエンスが向上します。**ゲートウェイとして実装される当社のSecure Connect Gatewayテクノロジー（直接接続またはプラグイン オプション）は、環境内のこれらのシステムを監視し、プロアクティブで予防的な、場合によっては予測型のサポートを提供します。

データは当社の接続テクノロジーの生命線です。**当社はお客様の環境からのシステム状態データを活用します。**そのデータと、フィールドおよびテクニカル サポート チーム、コンポーネント メーカーから得た**長年にわたるインシデント データおよびエンジニアリング データを関連付けます。**当社の接続テクノロジーは、**機械学習などの高度なAIモデル**を使用して、テレメトリーとイベントデータにパターンを見つけて適用し、適切な問題を正確に検出して対応できます。

当社のテクノロジーは、ハードウェアとソフトウェアの問題を特定し、**ケースを作成し、コストのかかる問題になる前に問題の解決を開始できるよう当社から連絡を開始します。**問題の種類に応じて、アラートに基づく**自動パーツ ディスパッチが開始される**こともあります。これにより、ハードウェア部品の受け取りが迅速化されます。

もう1つの優れた機能は、ほとんどのストレージ、データ保護、コンバージドおよびハイパーコンバージド(CI/HCI)製品に含まれる**リモート サポートです。**このシナリオでは、当社側でケースがオープンされた場合にリモート サポートを通じてトラブルシューティングを行うことができれば、このテクノロジーにより、認定テクニカル サポート エージェントが管理対象デバイスにリモートでアクセスして問題を診断、解決するための安全な双方向通信が可能になります。

また、Dellサポートが関与した場合、Dellにテレメトリーを送信することで、お使いの**システムの履歴データが解決までの時間を短縮するのに役立ちます。**たとえば、アラートがDellに返送されると、サポート技術者は（お客様が設定したポリシーに基づいて）デバイスに接続し、実行する必要があるアクションを確認して、アクション プランをお客様に提供できます。実際に故障する前にパーツを交換し、最終的にダウンタイムのリスクを最小限に抑えることも可能です。

リモート サポート機能のもう1つのメリットは、**リモート アップグレードです。**これは、安全な接続をどのように活用しているかを示す良い例です。多くの製品では、お客様が都合の良いときに適用できるように、製品のアップグレード コードまたはセキュリティ パッチがお客様に直接送信される場合があります。または、リモート変更管理チームが、オンサイトにいなくても、最初から最後までアップグレードをスケジュールして実行できます。

当社のエキスパートの話を聞く：

- ポッドキャストを聴く（英語のみ）： Maximizing datacenter uptime with intelligent support
- ポッドキャストを聴く（英語のみ）：Maximize PowerEdge uptime with proactive, predictive support

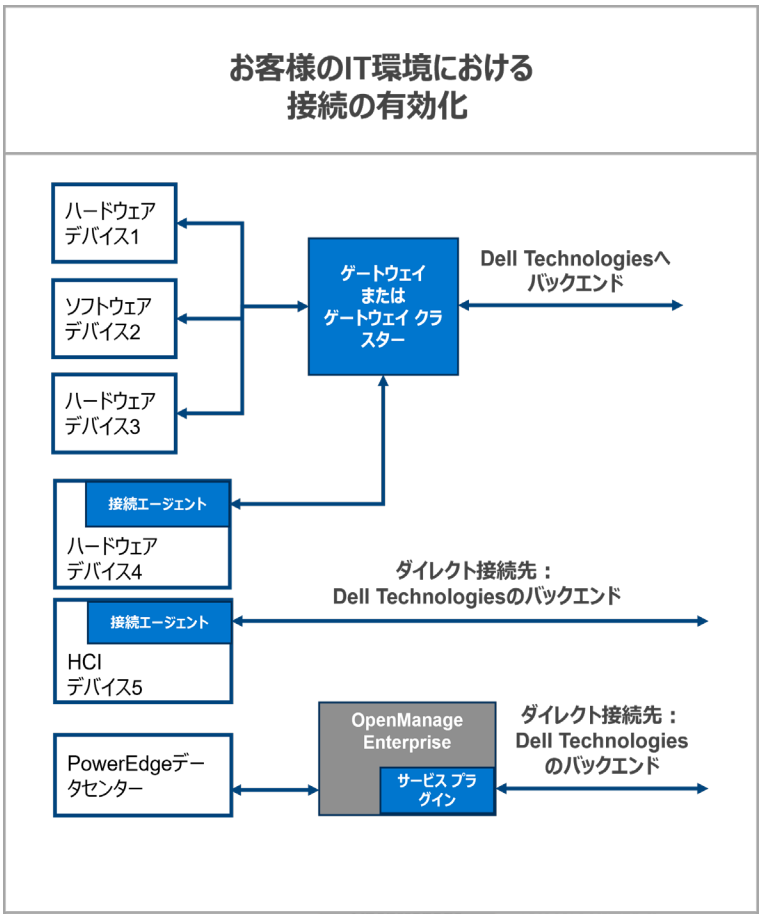
短いビデオを見る（英語のみ）：

- Connectivity features and benefits
- Security architecture and features

テクノロジーの導入オプション

7：環境に接続ソフトウェアを導入および構成するには、どのような方法がありますか？

柔軟なインストール オプション（ゲートウェイ オプション、直接接続オプション、プラグイン オプション）の中からお客様の環境に適したものを選択できます。すべてお客様によるインストールとアップグレードが可能です。



Secure Connect **Gatewayオプション**を使用すると、Dell製システムをゲートウェイに接続して、Dell Technologies Servicesと通信することができます。これにより、ファイアウォール/ネットワーキングのセットアップがシンプルになり、ゲートウェイがインターネット経由でアウトバウンドに接続する唯一のものになります。

Dellのゲートウェイ オプションでは、VMware、Microsoft Hyper-V、Linux KVM環境向けの**仮想エディション**をご用意しています。また、Docker、Podman、Kubernetes、OpenShift環境向けの**コンテナ エディション**もあります。小規模サーバーのお客様向けには、Windows/Linuxバージョンの**アプリケーション エディション**をご用意しています。*Q8-11を参照してください。*

システムの高可用性とフェールオーバーを求めているお客様は、複数のゲートウェイを設定するか、1つのゲートウェイが使用不可能になった場合に備えて冗長性をもたらすクラスターを設定できます。

（当社の接続テクノロジーとDell製品の操作環境の統合によって可能になる）**直接接続オプション**は、追加のソフトウェア設定を望まない小規模のお客様や従来とは異なるお客様に適しています。*詳細はQ12とQ28をご覧ください。*

最後に、コンピューティング中心のお客様向けには、PowerEdgeサーバー フリート用の**OpenManage Enterpriseのサービス プラグイン**があり、単一の安全な直接接続が可能です。*詳細はQ13とQ23-25をご覧ください。*

インフォグラフィックと重要なリンク：データセンターへの接続を始める

7（続き）：環境に接続ソフトウェアを導入および構成するには、どのような方法がありますか？

次の表を使用して、お使いの環境に適したオプションを特定してください。Secure Connect Gatewayの製品サポート マトリックスを確認するか、dell.com/supportのハードウェア製品サポート ページにアクセスしてください。アプリケーション バージョンが適しているのは、仮想化環境を持たず、サポートされているDellのハードウェアとソフトウェアを使用している小規模のお客様です。

接続し、1つの場所ですべてのデバイスをモニタリング

	統合ソリューション	サポートされているハードウェアとソフトウェア
統合ソリューション	**Secure Connect Gateway 5.x – 仮想アプライアンス エディション** *VMware、Microsoft HyperV、Linux KVM環境向けコンテナ パッケージ：Docker、Podman、Kubernetes、OpenShift*	Dell製品ポートフォリオ全体：データストレージ、サーバー、ネットワーク、CI/HCI、データ保護
	Secure Connect Gateway 5.x – アプリケーション エディション *サーバー上でのWindows Enterpriseの管理* *サーバー上でのLinuxの管理*	PowerEdge、iDRAC、PowerSwitch、Webscale、PeerStorage、EqualLogic、Compellent、Fluid File System（FluidFS）、PowerVault
	OpenManage Enterprise Servicesプラグイン *OpenManage Enterprise環境の場合*	PowerEdgeサーバー
選択したDellハードウェア向けのダイレクト接続	• Dell製品操作環境への接続の統合。Dell製品サポート ドキュメントを参照して、特定の製品モデルとバージョンを確認してください。 • 複数Dellハードウェア製品の異種混在導入に最適。 • デル・テクノロジーズに直接接続、またはSecure Connect Gatewayサーバーを介して接続。	

インフォグラフィックと重要なリンク： データセンターへの接続を始める

8：使用環境に推奨されるゲートウェイ ソフトウェアと最小要件は何ですか？

ゲートウェイ ソフトウェア	
セキュア コネクト ゲートウェイ - 仮想エディション 以下のバージョンがあります。 • VMware、Microsoft HyperV、Linux KVM環境 • コンテナ パッケージ：Docker、Podman、Kubernetes、OpenShift Dell.com/Supportからドキュメントとすべてのリソースをダウンロード。	セキュア コネクト ゲートウェイ - アプリケーション エディション 以下のバージョンがあります。 • Windows管理サーバー（WindowsとLinuxデバイスの両方をモニタリング） • Linux管理サーバー（Linuxデバイスをモニタリング） Dell.com/Supportからドキュメントとすべてのリソースをダウンロード。
インストール、登録、使用に関する技術的なヒントについては、インタラクティブなテクニカル デモをご覧ください。	
セキュア コネクト ゲートウェイ ソフトウェアをインストールして使用するための最小要件を必ず確認してください	

お客様が接続するための4つのステップ

1. **サイトの準備とアカウントの確認**
   ネットワーク管理者と技術要件および計画をプレビューします。ステップ2の前に、Dell.com/Supportでエンタープライズ ビジネス アカウントを設定します。
2. **ダウンロード**
   Dell.com/Supportのセキュア コネクト ゲートウェイ製品サポート ページで、アカウント認証情報を使用してサインインします。
   環境の適切なエディションを取得し、認証アクセス キーを作成します。
3. **インストールとプロビジョニング**
   仮想アプライアンスまたはコンテナ テンプレートを導入するか、アプリケーション ソフトウェアをインストールします。初期登録手順を完了します。
4. **デバイスの接続**
   Dell製品とゲートウェイ サーバー間の通信を構成し、有効にします

使用を開始する際の新規ユーザー向けヒント：

- 新規ユーザーは、ステップ2の前にDell.com/Supportでエンタープライズ ビジネス アカウントを設定します。Secure Connect Gatewayのダウンロード ページからサインインしてこの手順を完了するように求められます。
- 完了したら、Dell.com/Supportのセキュア コネクト ゲートウェイ製品サポート ページでアカウントの認証情報を使用してサインインします。
- ソフトウェアをインストールするサイトの場所を入力してください。これは、より優れたサポート エクスペリエンスの提供に役立ちます。
- ご使用の環境に適したエディションを入手できます。この手順では、認証アクセス キーを作成する必要があります。

メモ：*初めて接続する場合は、サイトの準備に最も時間がかかります。ネットワーク ポリシーとセキュリティ ポリシーの複雑さに応じて、数日から数か月になる可能性があります。セキュリティ チームとネットワーキング チームが、実装前に製品レビューを依頼する場合があります。*セキュリティ ペーパーを入手してください。

テクノロジーの詳細：Dell.comにアクセスすると、当社のエキスパートの意見を聞いたり、技術リソースを入手したりできます。

お問合せ先サポートが必要な場合は、Secure Connect Gatewayフォーラムで当社のエキスパートにお尋ねください

9：セキュア コネクト ゲートウェイ デバイスをデル・テクノロジーズに登録する必要がありますか？

はい。Secure Connect Gatewayを使用してクラス最高レベルのセキュリティを利用するには、デル・テクノロジーズに登録する必要があります。

> **ヒント：**エンタープライズ ビジネス アカウントの設定方法をご確認ください。Dell.com/Supportで自分の名前の横に黒いチェックマークが表示されていれば正しく認証されています。

エンタープライズ ビジネス アカウントを使用してダウンロード ページにログインし、アクセス キーとPINを生成してから、それらを使用してセキュア コネクト ゲートウェイをアクティブ化します。

ビジネス アカウントをお持ちでないお客様は、組織と製品に関する追加情報を求められます。お客様は、認証プロセスを実行した後に続行できます。

10：リモート サポート機能を備えているゲートウェイ テクノロジーはどれですか？また、Secure Connect Gatewayによって管理されているリモート アクセス機能を持つ製品を教えてください。

リモート サポート機能は、Secure Connect Gatewayの仮想エディションとコンテナ エディションでのみ使用でき、アプリケーション エディションでは使用できません。

データストレージ、データ保護、コンバージドおよびハイパーコンバージド(CI/HCI)製品には、リモート アクセス機能があります。PowerEdgeおよびPowerSwitch製品は、オンプレミス ゲートウェイ管理ユーザー インターフェイスの［デバイスの概要］でリモート サポートを有効にすることもできます。

認定テクニカル サポート エージェントは、必要な2要素認証を使用して管理対象デバイスにリモートでアクセスし、問題のトラブルシューティングと解決を行います。すべてのリモート セッションが監査され、Secure Connect Gatewayのオンプレミス ゲートウェイ管理コンソールの［監査］セクションから詳細にアクセスできます。

お客様は、追加の制御と高度な監査機能を利用するために、すべてのリモート アクセス セッションを柔軟にブロックまたは許可することができる、ポリシー管理サーバーを設定できます。

11：ポリシーマネージャー ソフトウェアとは何ですか？また、ゲートウェイ オプションでどのように使用されますか？

セキュア コネクト ゲートウェイのポリシーマネージャーは、高度な監査機能とリモート コントロール機能のためにインストールできる独立した補完的な外部ソフトウェアです。

ポリシーマネージャーを使用すると、これらのリモート アクセス機能の1つ以上をサポートする製品に対して、リモート サポート、ファイル転送、リモート アクションのポリシーを設定できます。

メモ：*ポリシーマネージャーは、ゲートウェイの仮想エディションおよびコンテナ エディションでのみ使用できます。アプリケーション エディションでは使用できません。*

> **ヒント：**インタラクティブ デモでポリシー管理モジュールをプレビューします。仮想アプライアンス エディションの技術的なハウツー ビデオをご覧ください。

12：直接接続が有効な製品はどれですか？ゲートウェイとの直接接続も使用できますか？

一部の例では、接続テクノロジーがDell製品の操作環境に統合されており、サービスのバックエンドへの直接接続が可能です。これが、「直接接続」の意味するところです。

Dellハードウェアおよびソフトウェア製品のセットアップ中に、接続サービスを有効にするように求められます。

ただし、直接接続対応のDell製品はいつでも、ゲートウェイ経由の接続に切り替えることができます。お客様の会社のセキュリティおよびネットワーキング ポリシーが、構成に関する意思決定に影響します。

直接接続に対応したDellインフラストラクチャ製品 *サポート対象製品の最新リストをDell.com/Supportで常にご確認ください*
AppSync | APEX AIOps Infrastructure Observabilityコレクター | CMS – VxBlockソフトウェア
データ バックアップ / Avamar | Data Domain | Data Domain管理コンソール | エッジ オーケストレーター
Elastic Cloud Storage | Metroノード アプライアンス | ObjectScale
PowerFlexファミリー – アプライアンス、ラック、ソフトウェア
PowerProtect - Data Manager、Data Managerアプライアンス、スケール アウト アプライアンス
PowerScale | PowerStore | PowerVault | S5000シリーズ | SRM | Streaming Data | Unity | VxRail
直接接続機能を備えた特定の製品モデルとバージョンを確認するには、製品サポート ドキュメントを参照してください。

メモ：*SupportAssist、SupportAssist Enterprise、Secure Remote Services ソフトウェアの機能は、次世代型接続ソフトウェア プラットフォームに統合されています。製品のユーザー インターフェイスに表示されるこれらのソフトウェア リファレンスは、時間の経過とともに適宜更新されます。*

サーバーの直接接続オプションのアップデートについては、*Q28をお読みください*。メモ：ゲートウェイを介して接続することはできません。

13：OpenManage Enterpriseのサービス プラグインとは何ですか？

Secure Connect Gatewayテクノロジーは、プラグインとしても実装されています。OpenManageをご利用のPowerEdgeデータセンターのお客様は、OpenManage Enterpriseのサービス プラグインに接続して、アラート、自動ディスパッチ、収集の各機能を使用できるようになりました。*Q27*も参照してください。

リソース：

- プラグインの詳細と技術リソースの入手
- サポート対象製品については、OpenManage Enterprise Services製品サポート ページの製品サポート マトリックス ドキュメントを参照してください。

当社のエキスパートの話を聞く：

- **短いビデオを見る**（英語のみ）：Services plugin for OpenManage Enterprise
- **ポッドキャストを聴く**（英語のみ）：Maximize PowerEdge uptime with proactive, predictive support
- **読む**：セキュリティ関連のペーパー

14：接続ソフトウェアの導入時にサポートを受けるにはどうすればよいですか？

多くのお客様は、接続テクノロジーをデル・テクノロジーズのサポートなしでダウンロードしてインストールできます。すべてのリソースについては、当社のWebページをご覧ください。

ヒント：インタラクティブなテクニカル デモを起動して詳細を確認できます

- *ゲートウェイ エディションとポリシーマネージャーのインストール、登録、使用方法を確認する*

サポートが必要な場合は、ProDeploy Infrastructure Suiteでセキュア コネクト ゲートウェイの有効化や設定などのさまざまなサービスをご利用いただけます。

ProSupport Plusの対象となるお客様には、インストールと登録に関する質問に対応できるTechnical Customer Success Managerが割り当てられます。

それ以外の場合は、必要に応じてデル・テクノロジーズ サポートにサポートを依頼してください。

15：問題が発生した場合、サポートに連絡するにはどうすればよいですか？

Dell.comオンラインサポートまたはSecure Connect Gatewayで問題が発生した場合は、こちらから管理サポート ページにアクセスしてサポートをリクエストしてください。問題に最も近いカテゴリーを選択し、指示に従って詳細を入力します。テクニカル サポートの問題に関して緊急のサポートが必要な場合は、こちらまでお問い合わせください。該当する場合は、Technical Customer Success Managerにお問い合わせください。

セキュリティ

16：ユーザーの環境でのこのソフトウェアと、Dellへの接続について詳しく教えてください。これらはどのように保護されていますか？

お客様の環境とDellの間の接続は、相互TLSトンネルと証明書チェーンを介して保護されます。このタイプの構成では、システムはお客様の環境内のDellソフトウェアに接続され、これらの接続は内部ポート/ネットワーキングの変更のみに留まる必要があります。このソフトウェアは、インターネット経由でアウトバウンドに接続し、Dellに戻る唯一のものです。これは、イベントおよびテレメトリー データについて、接続されたすべてのシステムの集約ポイントとして機能します。その情報は、送信される唯一のシステム状態情報となります。

システムからのすべてのテレメトリーは、HTTPS TTLS 1.3を使用して転送されます。また、セキュアなトンネルを使用してシステムにアクセスし、トラブルシューティングを行うリモート サポート機能も提供しており、問題解決の迅速化とダウンタイムの回避に役立ちます。

詳細については、セキュリティ関連のペーパーを参照してください。

17：リモート サポートはどのように実施されますか？リモート サポート セッションを通じてDellからシステムにアクセスできるのは誰ですか？

Dellのテクニカル サポート エンジニアは、ポータルを使用してリモート サポート セッションを作成し、トラブルシューティングやアップグレード アクティビティーのためにシステムにアクセスします。エンジニアは多要素認証を使用してこのポータルにアクセスします。これらのDellチーム メンバーは厳格なトレーニングを受ける必要があり、アクセスには管理者のサインオフが必要です。当社のリモート サポート エージェントは、エンタープライズ接続システム向けに広く受け入れられているソリューションであるMQTTプロトコルを使用しています。

18：セキュリティに重点を置いて、このシステム状態データ イベントとテレメトリー情報は監査されていますか？ポリシーマネージャーの役割は何ですか？

すべてのトランザクションは監査されており、ソフトウェアではユーザー インターフェイスでこの情報を表示できます。すべてのリモート サポート セッション、イベント、テレメトリー転送を表示できます。

より厳格なセキュリティ ポリシーを使用しているお客様、またはこの情報の長期保存を要求するサードパーティーの監査人と連携しているお客様には、ポリシーマネージャー ソフトウェアの設定をお勧めします。当社のポリシーマネージャーは、Secure Connect Gatewayと連携して、高度な監査機能とリモート サポート制御機能を提供します。*Q11も参照してください。*

19：接続テクノロジーのセキュリティ アーキテクチャに関する詳細情報はどこで入手できますか？

セキュア コネクト ゲートウェイがデータ保護と脅威防御を組み合わせて1つのセキュアな自動サポート体験を提供する仕組みについては、セキュリティ関連のペーパーをダウンロードしてご確認ください。

このホワイト ペーパーの内容は次のとおりです。

- **セキュアなオンサイト データ コレクション：**セキュアな通信ブローカーとしてのセキュア コネクト ゲートウェイの機能原理、セキュア コネクト ゲートウェイを使用した認証要件の管理方法、セキュア コネクト ゲートウェイにおける二要素認証プロトコルの活用方法について説明します。
- **セキュアなデータ転送および通信：**暗号化と双方向認証を使用して、ハートビート ポーリング、リモート通知およびリモート アクセス機能に使用するセキュアなTLSトンネルをセキュア コネクト ゲートウェイで作成する方法について説明します。
- **セキュアなデータ ストレージ、使用、およびプロセス：**物理的なセキュリティ、サプライ チェーンのリスク管理、セキュリティ開発プロセスなど、データを保護するために日常的に導入可能な一連の対策について説明します。

当社のエキスパートの話を聞く：

- **ポッドキャストを聴く**（英語のみ）**：**Maximizing datacenter uptime with intelligent support
- **読む：**セキュリティ関連のペーパー

短いビデオを見る（英語のみ）**：**

- Security architecture and features
- Security configuration for large and small scale environments
- Security features for financial sector

またはウェビナーを見る（英語のみ）**：**このSpiceworks Communityイベントで当社のエキスパートが以下について語ります。

- セキュア コネクト ゲートウェイでプライバシー、データ保護、脅威防御を統合する方法
- 小規模環境、大規模環境、非従来型環境にわたって接続を柔軟に導入する方法
- 接続されたシステムに関する問題の防止と軽減に自動サポートが役立つ理由

構成シナリオ

20：会社のニーズに合わせて接続テクノロジーを導入および構成する際に考慮すべき事項は何ですか？

最初に考慮すべき項目は、接続用に構成する**コンピューティング、ストレージ、データ保護、コンバージド/ハイパーコンバージド(CI/HCI)**といった製品の種類と、次のような**現在の環境**です

- データセンター間はネットワークで接続されているか？
- コンピューティングまたはストレージ（データ保護、CI/HCI製品など）を個別に管理しているか、一緒に管理しているか？

また、企業の**セキュリティおよびネットワーキング ポリシー**も考慮する必要があります。さらに、**チームがすべての製品をまとめて管理するか、地理的な場所や製品タイプ別にセグメント化するか**を考えます。

基本的に、接続方法、チームの連携方法、ネットワークの複雑さを最小限に抑える方法を考えなければなりません。これにより、さまざまな導入オプションに基づいて、最も効果的なアーキテクチャを設計できます。

以下の内容について説明している接続構成に関する考慮事項の概要を読んで、共有してください。

1. セキュリティを重視する大規模な企業では、どのような構成が推奨されますか？
2. 中規模から小規模の組織向けの構成および導入オプションにはどのようなものがありますか？
3. コンピューティング中心の環境を持つ大規模から中規模の企業の場合はどうすればよいですか？使用するツールはどのように決めればよいですか？
4. 1～50台のPowerEdgeサーバーがあり、仮想化環境がない場合はどうすればよいですか？ゲートウェイ オプションにはどのようなものがありますか？
5. 直接接続を利用できるDell製品がある場合はどうすればよいですか？　一般的なユース ケースはどのようなものですか？
6. 自社にとって最適な構成はどれですか？

サポート サービス

21：接続は、Dellインフラストラクチャ製品のサポート サービス契約の価値にどの程度関連していますか？

簡単に言うと、お客様の環境に接続ソフトウェアを導入し、監視対象のDell製デバイスをこのソフトウェアによって接続することで、Dell製システムに関する有効なサポート契約からより多くの価値を得ることができます。これはフリー ソフトウェアであり、ライセンスは必要ありません。当社は、90以上のDellインフラストラクチャ製品（ハードウェアおよびソフトウェア）をサポートしています。よりスマートなAI、自動化されたサポート、リアルタイム分析の当社独自の統合からメリットを得ることができます。

ProSupport Infrastructure Suiteサービスをご利用のお客様は、あらゆるレベルで大きな価値を享受できます。

- 詳細を見る：Dellインフラストラクチャ システムに対するProSupportおよびProSupport Plusの対象
    - 詳細を見る：Lifecycle Extension with ProSupport or ProSupport Plus
- メモ：Basic Hardware Support（翌営業日対応）契約のあるDell製システムでは、接続ソフトウェアによって監視されている場合、プロアクティブな自動問題検出、ケース作成、通知機能も利用できます。問題が検出された場合、ベーシック サポートのお客様は、ケース番号が記載されたメールを受け取り、問題のトラブルシューティングと解決のためにDellサポートに連絡するよう促されます。

この他にも、インフラストラクチャ向けの専門サポート サービスをご覧ください

22：モニタリング対象システムでProSupport Infrastructure Suiteなどのサポート サービス契約の有効期限が切れた場合、自動サポート機能はどうなりますか？

ProSupport Infrastructure Suiteのいずれかのレベルのサービス契約の有効期限が切れると、ケースの自動作成機能が無効になります。ただし、ゲートウェイ、直接接続、またはプラグインとして導入されたSecure Connect Gatewayテクノロジーは、システム状態データの自動収集を引き続き実行します。システム（サービス タグ）の契約をアップグレードまたは延長すると、そのシステムで自動的にケースの自動作成が再度有効になります。

PowerEdgeの接続

23：この接続ソフトウェアをサーバーに導入して構成する最適な方法は何ですか？使用するツールはどのように決定しますか？

一言で言えば、OpenManage Enterpriseソリューションを介したサービス プラグインは、コンピューティング中心の環境を持つお客様に適しています。また、ゲートウェイ ソリューションは、さまざまなDellインフラストラクチャ製品を管理する場合に最適な方法です。

どちらのソリューションにも、サポート契約を結んでいるPowerEdgeサーバー向けのアラート機能、ケースの自動作成機能、自動ディスパッチ機能、テレメトリー収集機能があります。

何を選択するかは、ユーザーの環境の種類、それらの環境間のネットワーク、モニタリング対象のデバイス タイプ、および設定によって異なります。

OpenManage Enterpriseを設定している場合、または設定を検討している場合は、サービス プラグインが最適です。OpenManage Enterpriseは、単一のコンソールから簡単に数千台のPowerEdgeサーバーのライフサイクルを管理できる、Dellのインフラストラクチャ ソリューションです。

- 初めて使用する場合は、環境にOpen Manage Enterpriseをインストールし、サーバー製品をオンボードしてから、サービス プラグインをインストールするだけで、ファイアウォールが正しく構成され、アラートとテレメトリーのDellへの送信が開始されます。

PowerEdgeと一緒に実行しているPowerStore、PowerMax、PowerScale、Data Domain、VxRailなどのDellインフラストラクチャ製品を組み合わせて使用しているお客様には、セキュア コネクト ゲートウェイ ソリューションを設定して、単一のUIからこれらのシステムを管理することをお勧めします。

当社のエキスパートの話を聞く：

- **ポッドキャストを聴く**（英語のみ）**：**Maximize PowerEdge uptime with proactive, predictive support
  - OpenManage Enterpriseソリューションを介したPowerEdgeシステムの接続に関連する内容と、ゲートウェイ ソリューションを介した接続との比較
  - PowerEdgeデバイス自体に接続する方法
  - 接続されているサーバーの数を時間の経過とともに簡単に拡張する方法
  - その他の構成シナリオ：プラグイン オプションとゲートウェイ オプションの両方を実行する

サーバーの直接接続オプションのアップデート

- 製品および地域固有の詳細、接続に関する考慮事項に関するガイダンスなど、あらゆる詳細については、*Q28をお読みください。*

24：サービスの接続機能は、OpenManage Enterpriseによるデータセンター管理ライフサイクル モニタリング機能をどのように補完しますか？

OpenManage Enterpriseは、操作性に優れた、1対多のシステム管理コンソールです。1つのコンソールで、PowerEdgeサーバーとシャーシの包括的なライフサイクル管理をコスト効率よく促進します。OpenManage Enterpriseの接続プラグインがデータセンターのOpenManage Enterpriseエクスペリエンスをどのように補完するかについては、次の図を参照してください。これは現在、**OpenManage Enterpriseのサービス プラグインを**介して利用できます。詳細とリソースについては、こちらをご覧ください。

25：OpenManage Enterpriseのサービス プラグインでサポートされているシステムにはどのようなものがありますか？

PowerEdgeサーバーとシャーシ、iDRACとChassis Management Controller (CMC)に加え、Linuxサーバーがサポートされています。

特定のサポート対象製品を確認するには、Dell.com/Supportサイトにアクセスし、OpenManage Enterpriseサービス製品サポート ページのサポート マトリックス ドキュメントを参照してください。

26：サービス用の接続ソフトウェアを使用すると、OpenManage Enterpriseと同様に、PowerEdgeサーバーのデータセンター ライフサイクル管理タスクを実行できますか？

いいえ。当社のサービス向け接続ソフトウェアは、データセンター内のスタンドアロンPowerEdgeデバイスのBIOSおよびファームウェア アップデートの転送やオーケストレーションを行いません。通常、スタンドアロン サーバー環境を持つコンピューティング中心のお客様は、OpenManage Enterpriseをインストールして、これらのタイプのライフサイクル管理機能を使用します。

メモ：OpenManage Enterpriseのサービス プラグインを有効にすると、アクティブなサポート契約のあるPowerEdgeサーバーのアラート、自動ケース作成、自動ディスパッチ、テレメトリー収集機能がアクティブになります。ただし、サービス プラグインでは、管理対象システムのアップグレード コードの配信およびリモート サポート アクセス機能は有効になりません。

27：OpenManage Enterprise環境でサービス プラグインとAIOpsプラグインを使用する必要があるのはいつですか？AIOpsプラグインを使用して、自動化されたプロアクティブなサポート ケースを作成できますか？

OpenManage Enterpriseは、単一のコンソールから簡単に数千台のPowerEdgeサーバーのライフサイクルを管理できる、Dellのインフラストラクチャ ソリューションです。次の表は、AIOpsプラグインと比較したサービス プラグインの使用方法と機能について説明しています。

ServicesプラグインとAIOpsプラグイン*の両方*を有効にして、OpenManage Enterpriseコンソールからそれぞれの機能を最大限に活用することをお勧めします。

機能とユース ケースの概要		
プラグイン	OpenManage Enterprise **サービス プラグイン**	OpenManage Enterprise **AIOpsプラグイン**
どんな場合に使用するか	**自動化されたプロアクティブ サポート機能**が必要な場合に有効にする	**クラウドベースのダッシュボードのDell AIOps機能**が必要な場合に有効にする
プラグイン機能	アラート、自動ケース作成、部品の自動配送、テレメトリー収集機能を提供する	容量不足、パフォーマンス異常、サイバーセキュリティリスク、サステナビリティに関する正常性監視と予測インサイトを可能にする
機能の対象	ProSupportおよびProSupport Plus契約を含む、有効なサポート契約のある資産。*Q21*を参照してください。	ProSupportおよびProSupport Plus契約のある資産
セキュアな接続のセットアップの説明	メモ：お客様の環境では、2つではなく1つの接続を有効にします。 Secure Connect Gatewayテクノロジーに基づいて、お客様の環境内のOpenManageアプライアンスとDellのバックエンド間の1つの安全な相互TLS接続です。	
重要なポイント	サービス プラグインのみを有効にする場合、AIOpsプラグイン機能は利用できません。 AIOpsプラグインのみを有効にすると、Servicesプラグイン機能は利用できません。 **ベスト プラクティスとしての推奨事項：両方のプラグインを有効化します。**	

28：一部のPowerEdgeシステムに表示されるDell Connectivity Clientとは何ですか？Secure Connect Gatewayテクノロジーと互換性がありますか？

iDRAC搭載のPowerEdgeサーバーの特定のモデルには、Dell Connectivity Clientと呼ばれるIntegrated Dell Remote Access Controller (iDRAC)プラグインが含まれています。製品および地域固有の詳細については、FAQを参照してください。このクライアントは、iDRACからDellバックエンド サービスへの直接接続を可能にし、OpenTelemetryフレームワークを使用してストリーミング テレメトリーを提供します。

- **メモ**：このPowerEdge製品構成はDellによって事前に有効化されているため、お客様はセールス プロセス中にDell Connectivity Clientの使用を明示的にオプトイン/オプトアウトする必要があります。

現時点では、Dell Connectivity Clientは、Secure Connect Gatewayの仮想エディション、コンテナ エディション、アプリケーション エディション、またはOpenManage Enterpriseのサービス プラグインに接続することはできません。

Q28の回答は次のページに続きます…

28の続き：一部のPowerEdgeシステムに表示されるDell Connectivity Clientとは何ですか？Secure Connect Gatewayテクノロジーと互換性がありますか？

お使いの環境でPowerEdgeシステムのSecure Connect Gatewayまたはサービス プラグインをすでに使用している場合は、次の手順を実行します。

- これらの既存の構成を引き続き使用できます。Dell Connectivity Clientを介してこれらのPowerEdgeシステムを再びDellに接続する*必要はありません*。ただし、これらのPowerEdgeシステムのDell Connectivity Clientを無効にするには、*操作を実行する必要があります*。Dell Connectivity Client構成を無効にする方法については、こちらのガイドをお読みください。

ゲートウェイ接続などのセキュリティ ポリシーに準拠するために、単一の安全な接続が必要な場合は、次のことをお勧めします。

- Secure Connect Gateway用の仮想エディション、コンテナ エディション、アプリケーション エディション、またはOpenManage Enterprise用のサービス プラグインの適切なバージョンをダウンロードしてインストールします。
- さらに、これらのPowerEdgeシステムのDell Connectivity Clientを無効にするアクションを実行する必要があります。その後、これらのシステムをゲートウェイに接続するか、OpenManage Enterpriseを介してモニタリングします。テクニカル ガイドに従ってください。これらのテクノロジー導入オプションの詳細をご覧ください。

その他の一般的なハイライト

29：Secure Connect Gatewayのアラート ポリシーに関する情報はどこで入手できますか？ハードウェア障害の予測型のサポート ケースはいつ開かれますか？

Secure Connect Gatewayアラート ポリシーには、デル・テクノロジーズ テクニカル サポートでケースを開くアラートに関する情報が記載されています。Secure Connect Gatewayを使用しているお客様は、ProSupport Plusサービス契約のあるシステム上のサーバー ハードウェア（ハード ディスク、バックプレーン、エキスパンダー）の自動予測ケース作成のみを受け取ります。予測アラートは、デル・テクノロジーズに送信されるスケジュール設定されたコレクションに基づいています。

30：ゲートウェイの認証情報管理機能についてどのようなことを知っておく必要がありますか？

Secure Connect Gatewayでは、複数の認証情報アカウントとプロファイルを柔軟に追加できます。認証情報アカウントを使用すると、管理者は製品タイプごとに認証を追加できます。さらに、プロファイルを使用すると、機能や地域によって異なる複数の管理者が特定のアカウントを管理できます。認証情報が必要な製品には、PowerEdgeサーバー、iDRAC、Compellent、ネットワーキング、PS Series、MD Series、Webscaleシステムが含まれます。

また、認証情報ヴォールトの統合も提供しています。これは、セキュリティを侵害したり手作業を増やしたりすることなく、システムを追加し、正しい認証情報を維持できるため、多くのデバイスを使用するお客様にとって優れた機能です。当社は、現在サポート対象のCyberArk Conjur APIおよびCyberArk Credential Provider製品を使用して、市場をリードするCyberArkと統合されています。Microsoft Azure Key VaultとHashiCorp認証情報ヴォールトもサポートしています。ベンダーは今後さらに追加される予定です。最新のリストについては、サポート ドキュメントを確認してください。

ヒント：これらの機能については、インタラクティブ デモの*Device Management*モジュールで確認してください

31：メンテナンス モードの主要機能にはどのようなものがありますか？

「イベント ストーム」は、ハードウェア アラートが連続して発行され、事前定義されたカウント制限を超えたときに発生します。このシナリオでは、Secure Connect Gatewayは、イベント ストームをトリガーした特定のデバイスのアラートの処理を停止します。その他のすべてのデバイスは、サポート ケースが作成される可能性のある検証済みのアラートについて、引き続きSecure Connect Gatewayによって監視されます。

さらに、ユーザーはシステム内から1つ以上のデバイスのメンテナンスを手動で有効にするオプションを使用できるようになりました。これは定期メンテナンスに使用し、Secure Connect Gatewayでこれらのデバイスを監視しない場合に導入できます。定期メンテナンス アクティビティーが完了したら、メンテナンス モードを手動で無効にして、Secure Connect Gatewayにモニタリングを再開するように信号を送信できます。

32：ゲートウェイ オプションでは、Eメール通知の設定を行うことができますか？

はい。Eメール通知の設定は、セキュア コネクト ゲートウェイ ユーザー インターフェイスの［設定］タブ内で調整できます。詳細については、ユーザー ガイドを確認してください。

33：オンプレミス ゲートウェイ管理ダッシュボードではどの言語がサポートされていますか？

Secure Connect Gatewayソフトウェアのインターフェイスは、英語、ドイツ語、ポルトガル語（ブラジル）、フランス語、スペイン語、簡体中国語、日本語で使用できます。ただし、サービス リクエスト インシデントの発生時に送信される自動Eメール通知には、28の言語のいずれかを選択できます。メモ：一部のEメール通知は、OSの制限によりローカル言語に翻訳されません。

34：REST APIはどのように使い始めたらよいですか？

ゲートウェイ オプションを利用することで、お客様はREST APIを活用して独自のカスタム スクリプト作成を実行し、サポートすることが可能です。ドキュメント セクションからREST APIのユーザー ガイドをダウンロードしてください。

35：この接続ソフトウェアはDell AIOpsポータルでどのように使用されますか？

Dell AIOps（旧称APEX AIOps Infrastructure ObservabilityおよびCloudIQ）は、Dellインフラストラクチャを最適化するように設計された、クラウドベースでAI主導の可観測性および管理ソリューションです。

リアルタイム インサイトを提供してインフラストラクチャのパフォーマンスを最大限に高め、サイバーセキュリティの強化とサステナビリティの向上を推進して、プロアクティブな計画をサポートします。直感的なプラットフォームと生成AIアシスタントが特長のDell AIOpsは、リスクの最小化、効率の向上、IT運用のシンプル化に役立ちます。

- 主な属性：正常性ステータスとサイバーセキュリティのリスク アセスメントと修復のための推奨事項、パフォーマンスと容量の追跡、異常の検出と予測、故障予測、エネルギーと排出量の追跡と予測、仮想化リソースのモニタリング。

当社の接続ソフトウェアは、お客様の環境からのシステムおよびイベント データの転送にのみ使用されます。テレメトリーはDellバックエンドに安全に送信され、Dell AIOpsのAIアルゴリズムによって分析されます。

36：TechDirectポータルでサポート契約が有効な接続済みのDellインフラストラクチャ製品を表示して管理できますか？

いいえ。TechDirectでは、接続されているDellインフラストラクチャ製品の表示や管理はできません。当社の接続ソフトウェアはTechDirectと統合されていないため、接続されているDell製システムのアラート データと自動サポート ケースはサポートされておらず、ポータルのダッシュボードにも表示されません。

ただし、ゲートウェイ、直接接続、プラグイン オプションを介して接続されているDell製システムの自動サポート ケースの詳細には、オンライン サポート サイトとMyService360分析ダッシュボードでアクセスでき、そこで管理することが可能です。