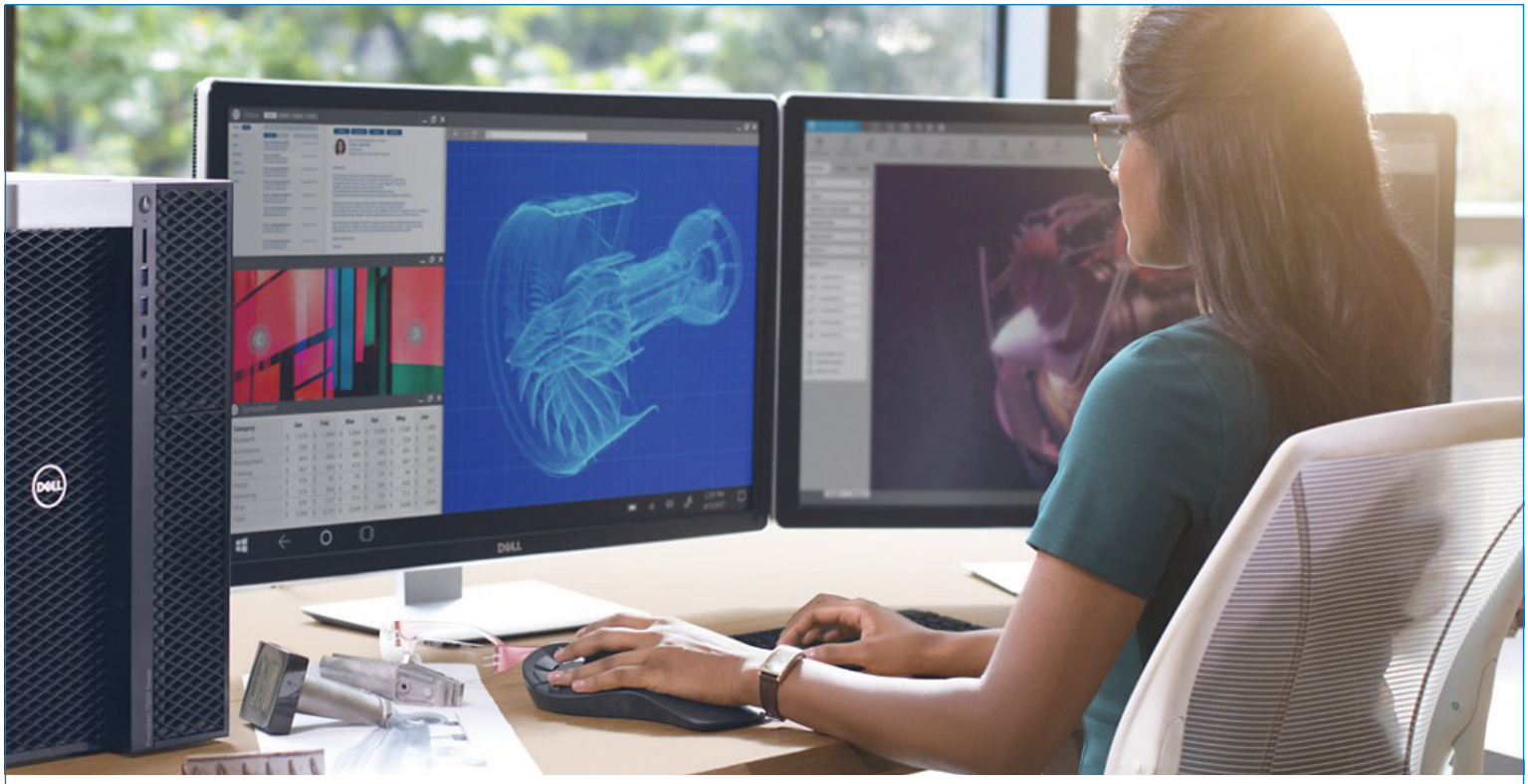
SupportAssist for Business PCs：セキュリティ概要

SupportAssistのセキュリティに関する5つの主な疑問とその回答

SupportAssistを使用すると、すべてのPCにわたってハードウェアとソフトウェアの問題を特定して、デル・テクノロジーズからのサポートを自動化できます。SupportAssistは、システムのパフォーマンスと安定化の問題に対処し、セキュリティの脅威を軽減して、ハードウェア障害の監視と検出を行い、Dellテクニカル サポートとのエンゲージメント プロセスを自動化します。

また、SupportAssistは、パソコンからテレメトリー データをプロアクティブに収集し、お客様のサービスプランに基づいてPC使用率と修復に関するインサイトを提供します。



目次

I：はじめに

ノートパソコンで障害が発生すると、混乱を招き、満足が低下する可能性があります。このような問題は、従業員の生産性に深刻な影響を与える可能性があり、最悪のタイミングで発生することもしばしばあります。このため、企業のCIO（最高情報責任者）は、自社のコンピューター デバイスの品質とアップタイムについてますます懸念を抱くようになっています。

多くのCIOは、データサイエンスから得たインサイトを使用して数十億ものデータ ポイントを処理し、IT管理者の効率性を高める最新かつ最先端のテクノロジーに注目しています。これは、エンドユーザー システムから企業のIT部門やハードウェア/ソフトウェア ベンダーにシステム状態情報を送信して、問題が発生したらすぐに解決することで、あるいは問題を発生させないようにすることで成し遂げられます。SupportAssist接続テクノロジーを備えたDell ProSupport Plusは、TechDirectポータルからすべてのPCを一元的に表示することで、障害が発生しているハード ドライブについてアラートを発します。

このテクノロジーはアップタイムと効率性を確保する上で必須となります。これに関し、収集される情報とその処理方法についてCIOから疑問が提起されることもあります。

その中でも重要とされる疑問は次のとおりです。

- SupportAssistが収集するデータの種類とは？
- 会社のIT部門やコンピューター ベンダーにデータを送り返す際、このデータをどのように保護するのか？
- データが届いたら、プライバシーと安全性を保つようにデータは保管されるのか？

このホワイトペーパーでは、データサイエンス対応テクノロジーを評価する手段として、これらの疑問や関連する他の疑問を評価します。問題が大きくなる前に問題を予測して修正できる総合的なサポート サービスとして、SupportAssistがProSupport Suite for PCsをどのように差別化しているかについての概要を説明します。また、Dell Technologies Servicesがプロセス、データ転送、データストレージにおいて機密データをどのように保護しているかについても詳しく説明します。

II：SupportAssistについて

SupportAssistは、組織がすべてのPCに対して自動化されたテクニカル サポートを受けられるようにするスマート接続テクノロジー[1]です。エンド ユーザー デバイスを監視し、ハードウェアとソフトウェアの両方の問題をプロアクティブに検出して、システムの使用状況に関するインサイトを提供します。

問題が検出されると、SupportAssistはテクニカル サポートへのサポート リクエストを自動的にオープンします。問題のタイプに応じて、アラートからテクニカル サポート リクエストまたは自動パーツ ディスパッチを開始できます。SupportAssistは、テクニカル サポートが問題のトラブルシューティングと解決のために使用するハードウェア データとソフトウェア データの両方を収集します。

Dell ProSupport Suite for PCsは、最も包括的なサポート機能を単一のソリューションで提供します。サービスをスタックする必要はありません[2]。
詳細はこちら。

主要機能

- デバイス全体のプロアクティブかつ予測的な検出により、問題をより迅速に解決
- 正常性スコア、アプリケーション エクスペリエンス スコア、セキュリティ スコアを1つの画面で迅速に分析
- カスタマイズされたルールで、修復ワークフローを定義
- Dell BIOS、ドライバー、ファームウェア、アプリケーションのカスタム アップデート カタログの作成と導入を自動化
- TechDirectで表示とダッシュボードを柔軟にカスタマイズ

利用できる機能は、パソコンについてご購入いただいたサポート プランに応じて異なります。

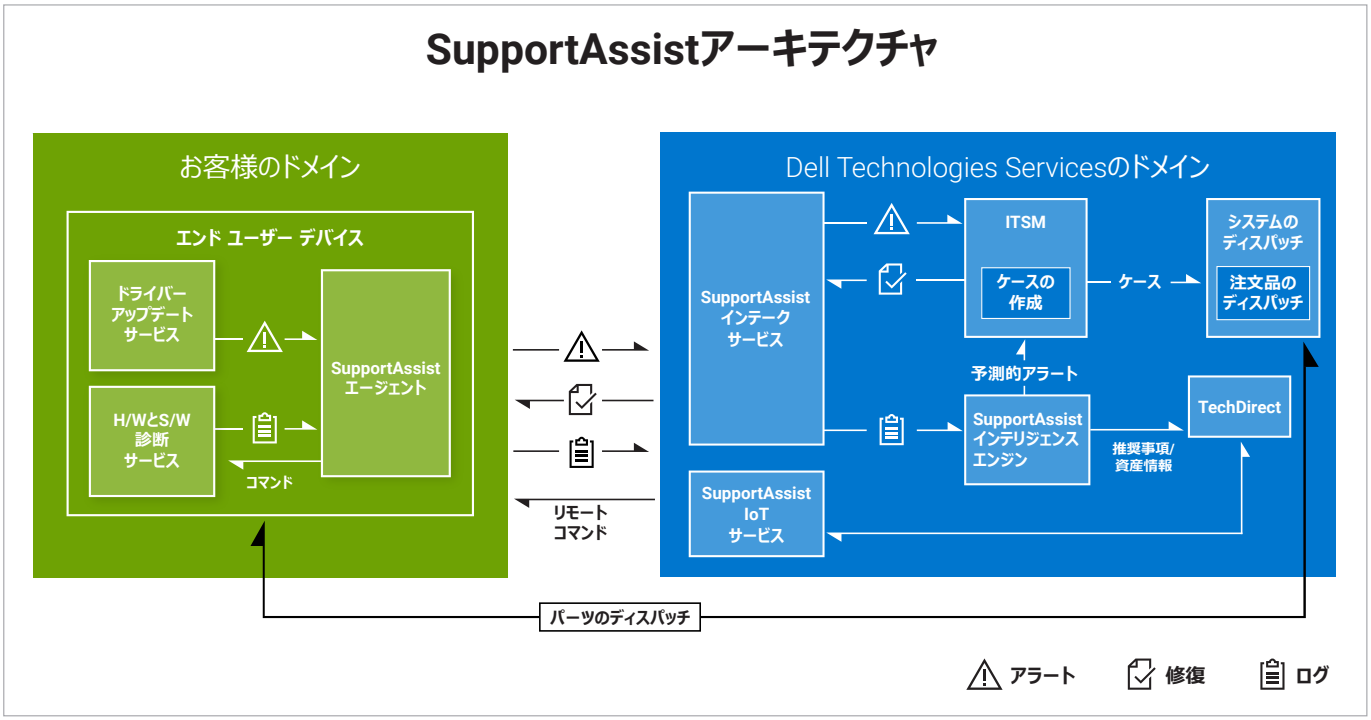
- ProSupport Plusをご利用のエンド ユーザーには、予測型の問題検出や障害防止など、SupportAssist機能のすべてが提供されます。

機能の一覧については、管理者ガイドを参照してください。

III. SupportAssistアーキテクチャ

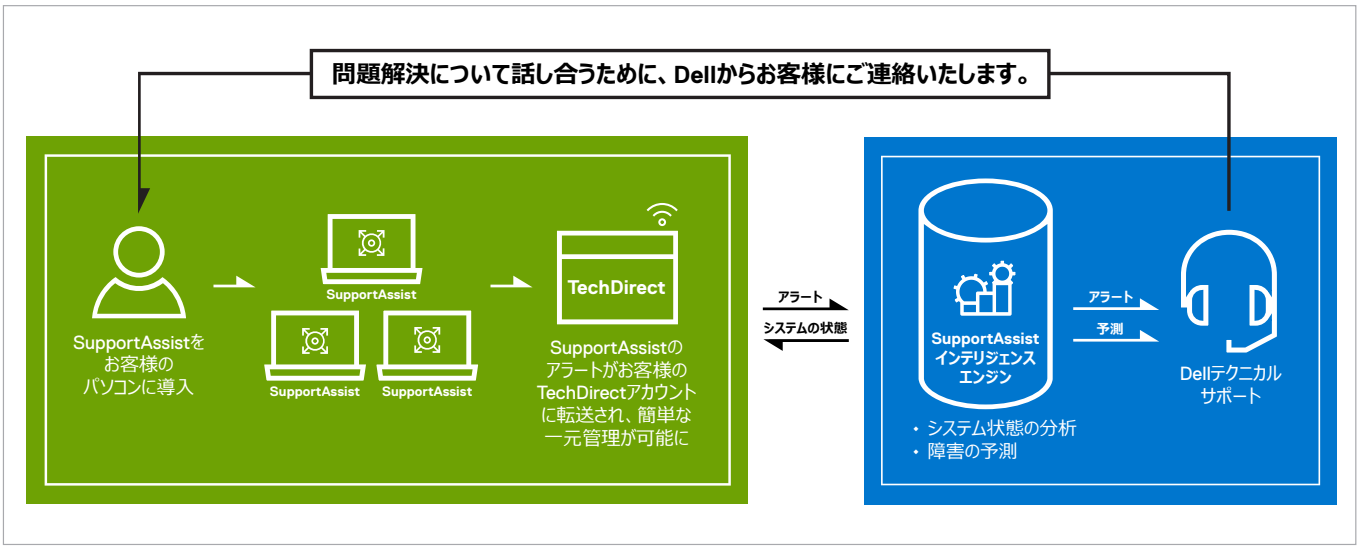
SupportAssistは、システムを継続的に監視し、設定したスケジュールでデバイスのヘルス チェックを実行する一連のサービスで構成されています。この情報は、データを分析して推奨事項を提示するために、デル・テクノロジーズのサーバーに送信されます。

SupportAssistの導入と修復に関するネットワーク、エンドポイント、ポート、ファイアウォール、ゲートウェイの要件の一覧については、導入ガイドを参照してください。修復スクリプトは、Dellが開発、テスト、署名した後、実行前に確認されています。



TechDirectを使用したSupportAssistの一元管理

SupportAssistアラートは組織のTechDirectアカウントに転送され、便利な一元管理を可能にします。ProSupportまたはProSupport Plusサービス プランをご利用の組織は、Dell Technologies Servicesへのアラートの自動転送を選択することもできます。

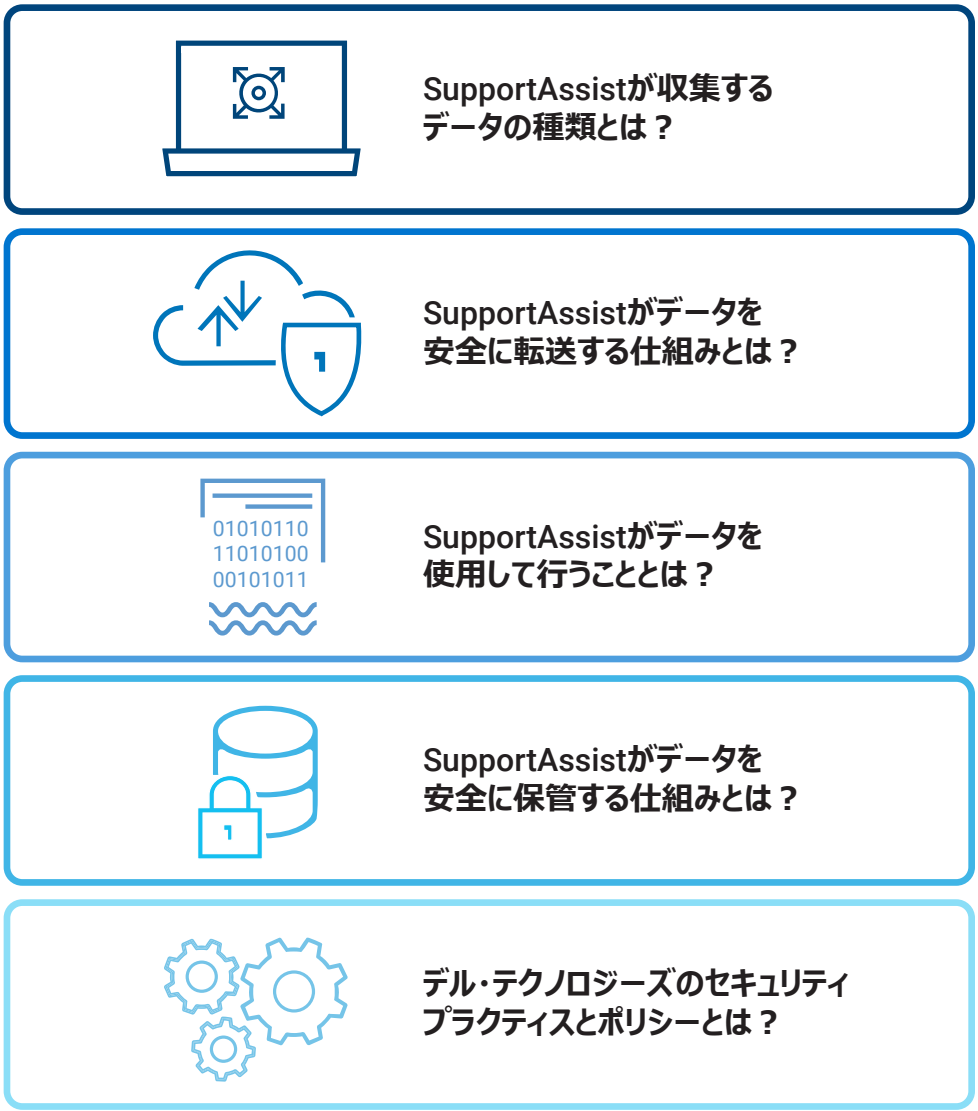


TechDirectを使用したSupportAssistの一元管理（続き）：

SupportAssistのインサイトは非常に有用な分析コンポーネントであり、TechDirectコンソール内で表示可能なシステム使用率データを収集します。このデータには、CPUの利用率、ドライブの空き容量、最大バッテリー容量、バッテリー持続時間など、多くの有用なインサイトがあります。TechDirectでは、すべてのシステムのほか、特定のデバイス グループのシステムや個々のシステムについて、このような情報を表示できます。お客様は、パフォーマンスの問題を特定し、より適切なビジネス上の意思決定（ハードウェアをアップグレードするかどうか、または交換するかどうかなど）を行うことができます。

IV. SupportAssistのセキュリティ

組織には、SupportAssist for Business PCsでどのようなデータが収集されて、どのように処理されるのか疑問を持たれているCIOやCSOがいらっしゃるかと思います。このセクションでは、SupportAssistがお客様の問題の解決に必要なデータのみをどのように収集し、最適なセキュリティを念頭に置きながらデータをどのように処理するのかなど、次のような疑問についてお答えいたします。



SupportAssistが収集するデータの種類とは？

SupportAssistは、問題のトラブルシューティングに必要なデータを自動的に収集し、テクニカル サポートに安全に送信します。このデータによって私たちは、適応性の高いインテリジェントで迅速なサポート エクスペリエンスを提供できるようになります。

サービス タグは、作業中の特定のエンドユーザー デバイスを識別するために必要であり、デバイスから収集される、企業に関する唯一の情報です。SupportAssistがパーツをプロアクティブに出荷する必要があると判断した場合、当社では、デル・テクノロジーズのサーバーに安全に保存されている既存の連絡先情報を使用します。

日常のシステム モニタリングの一環として収集され24時間ごとに送信されるシステム情報は次のとおりです。

- **スキーマ バージョン：**日常的なシステム モニタリングに使用するスキーマのバージョン
- **エージェント バージョン：**システムに導入されているSupportAssistのバージョン
- **サービス タグ：**システムの一意の識別子
- **システム モデル：**システムのモデル名
- **登録情報：**SupportAssistの登録ステータス
- **OSバージョン：**デバイスで実行されているオペレーティング システムのバージョン
- **SPバージョン：**オペレーティング システムのサービス パック
- **UTC日付：**日常的なシステム モニタリング情報がDell Technologies Servicesに送信された日付と時刻
- **BIOSバージョン：**システムにインストールされているBIOSのバージョン
- **ステータス：**アラートのステータス（重大度に応じて異なる。例：警告）
- **説明：**システム障害に関する情報（例：CPUの利用率が高い）
- **ハード ドライブの空き容量：**システムのハード ドライブで使用可能な空き容量
- **メモリー使用量：**システム メモリーの使用量
- **CPU使用率：**CPUの使用量
- **ローカル日付：**システムの日付と時刻
- **前回起動日：**システムが最後に再起動された日付と時刻
- **Windows Update実行日：**システムでWindowsが最後に更新された日付と時刻
- **BSOD数/24時間：**過去24時間に発生したブルー スクリーン エラーの回数
- **アラート情報：**アラートの一意の識別子

アクティブなシステムから収集されるシステム モニタリング データの詳細については、こちらのDell.comページをご覧ください。

すべての情報は、セキュリティで保護されたチャネルを介して送信されます。

SupportAssistがデータを安全に転送する仕組みとは？

SupportAssistからDell Technologies Servicesに送信されるデータは、256ビット暗号化によって暗号化され、トランスポート層セキュリティ(TLS)プロトコルを使用して安全に転送されます。

暗号化キーは、パッケージをインストールする際の各マシンでの実行時に生成されます。暗号化キーとソルトは、インストールされた情報を暗号化するために使用されます。静止データの暗号化には、業界標準のアルゴリズムが使用されます。

暗号法におけるソルトとは、データ、パスワード、またはパスフレーズを「ハッシュ化」する一方向関数に入力されるランダム データのことです。ソルトの主な機能は、辞書攻撃やハッシュ化された同等の攻撃（事前に計算されたレインボー テーブル攻撃）から防御することです。

すべての暗号化キーは、安全な乱数発生器を使用して生成されます。転送中のデータは、TLS over Hypertext Transfer Protocol Secure (HTTPS)を使用して保護されます。すべての暗号化アルゴリズムは業界標準であり、静止データは暗号化されます。

ユーザーから提供されるフィードバック、診断テレメトリー イベント、復旧プロセスで使用されるシステム情報を調べるためのDell.comまたはMicrosoft Azure IoT Hub上のAPIに対するクエリーを送信するオフボックス通信には、HTTPSが使用されます。pub-subアプローチにはセキュアMQTTが使用されます。

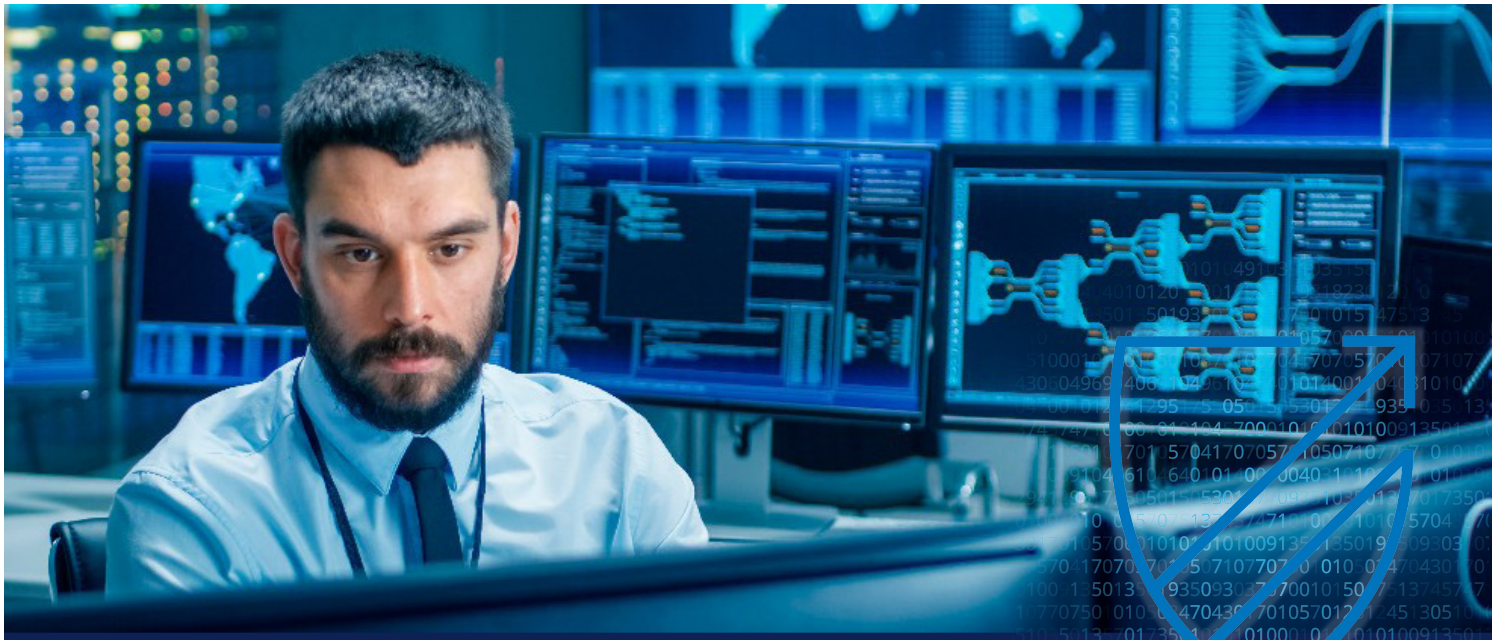
標準HTTPSは、エンドユーザー デバイスにコンテンツを送信またはダウンロードする際に、クライアントとバックエンド インフラストラクチャ間の通信を保護するために使用されます。HTTPSまたはセキュアMQTTは、テレメトリー データの転送、Dell.comまたはMicrosoft Azure IoT Hub上のバックエンドAPIとの通信、Dell.comから取得したコンテンツのダウンロードを保護するために使用されます。

すべてのネットワーク コンポーネントはファイアウォールによって保護され、ネットワーク セキュリティ チームによって管理されています。ネットワーク トラフィックは厳重に制御されています。すべての受信トラフィックは、特定のポートを介して転送され、適切な宛先ネットワーク アドレスのみに送信されます。SupportAssistは、Dell Technologies Servicesインフラストラクチャへの接続を必要とするさまざまなイベントに対応するためにネットワーク帯域幅を使用します。使用される帯域幅は、SupportAssistが監視するターゲット システムの数に応じて異なる場合があります。表1は、SupportAssistが1台のパソコンのモニタリングに使用する平均的なネットワーク帯域幅を示しています。

表1.平均データ消費量

イベント	イベントの頻度	パソコンあたりのデータ消費量
SupportAssistの登録	導入後1回	15 KB
PC情報または最小限のテレメトリー データの送信	6～24時間に1回	4 KB
定期スキャン実行時のPC情報のアップロード	TechDirectでのSupportAssistの設定に従って、毎週または毎月	120 KB
定期的なPCモニタリング情報の送信	導入後30～45日ごと	135 KB
アラートおよびシステム状態情報の送信	アラートが検出されたとき、または障害が確認されたとき	145 KB
サポート リクエストの作成	サポート リクエストを作成するだけの根拠がアラートにある場合	160～350 KB
SupportAssistのバージョン アップグレードの確認	週1回	16 KB
SupportAssistの最新バージョンへのアップグレード	最新バージョンが利用可能な場合	318 MB
パソコンのアップデートに関するDellの推奨事項の確認	週2回	1～2 MB*
スマートPCのアップデートに関する推奨事項の確認	週2回	65 KB
PCインサイトの送信（正常性とアプリケーション エクスペリエンスに関する情報）	1時間に1回	2320 KB

メモ：データは、SupportAssist for Business PCsリリースv3.5.0に基づいて提供されたものです。
*データはアップデートに応じて異なります。



物理的および論理的なセキュリティ対策を講じてデータを安全に保管

SupportAssistがデータを使用して行うこととは？

SupportAssistは、収集されたデータを使用して、プロアクティブかつ予測型の自動化されたサポートをお客様に提供します。システムに問題がある場合、SupportAssistは、テクニカル サポート エージェントがトラブルシューティングを実施できるようにアラートを生成します。

また、SupportAssistは、現場の数千万台のDell製システムから収集したデータをベースとした人工知能ソフトウェアを使用して、コンポーネントに障害が発生する可能性があるタイミングを予測するために収集したデータを使用します。この予測的アラートを使用すると、パーツが故障する前にディスパッチできるため、システムのアップタイムとデータ保護が最適化されます。

SupportAssistはこのデータを使用して、ユーザー システムのウイルスやマルウェアの検出と除去、オペレーティング システムのパフォーマンスの最適化、BIOS、ドライバー、ファームウェアのアップデートに関する推奨事項の提供を行います。

システム アプリの使用状況では、インサイト コンポーネントを使用して、システムの使用状況に関するインサイトを把握できます。

物理的なセキュリティ

Dell Technologies Servicesは、高いレベルの可用性とセキュリティを確保するように設計された米国のデータセンターで、アプリケーション、システム、ネットワーク、セキュリティ コンポーネントを含むSupportAssistデータを管理しています。SupportAssistのデータは、さまざまな方法で保護されています。

インフラストラクチャが配置されているデータセンターへのアクセスは、許可されたスタッフに限定されます。アクセスはスマート カードで制御されます。

論理的なセキュリティ

SupportAssistによって生成されたデータは、Dellのプライバシーポリシーに則って保管されます。

Dell Technologies Servicesインフラストラクチャ（サーバー、ロード バランサー、ネットワーク共有など）への論理的アクセスは、内部ツールを通じて制限が課されます。このツールはDell Digital (IT)ガイドラインに従って監査および評価されます。

- **監査：**監視対象デバイスのログは保持され、Dell Technologies Servicesインフラストラクチャやアプリケーションを使用した場合にのみアクセスできます。これらのログには、オペレーティング システムまたはSupportAssist Webサーバー コンソールへのログイン試行またはアクセス試行がすべて記録されます。

IT部門が管理するビルドは、セキュリティのベスト プラクティスに基づいて、Center for Internet Security (CIS)が推奨する制御を使用して強化されています。

SupportAssistエコシステムでは、データセンター内におけるローカルでの高可用性と、別のデータセンターの同一インフラストラクチャの両方が採用されています。唯一の例外は、ビッグデータ クラスターやプライベートクラウドなど、本質的に可用性の高いテクノロジーです。

データ分析については、Dell Technologies Servicesは、プライベートクラウド、ハイブリッドクラウド、パブリッククラウドなど、当社が全面的に制御して管理するクラウド環境を活用します。リレーショナル データベース、シンプルなストレージ サービス、データ ウェアハウスはすべて暗号化され、最小限の権限を使用します。リレーショナル データベースは公開されていません。データ ウェアハウスはHTTPSを使用して保護されます。

デル・テクノロジーズのセキュリティ プラクティスとポリシーとは？

開発

当社の社内セキュア開発ライフサイクル基準(SDL)は、デル・テクノロジーズ製品組織の基礎的な参考資料としての役割を果たし、製品とアプリケーションの安全な開発に不可欠なベンチマークを提供します。Dellは、ISO/IEC 27034と、NIST Secure Software Development Framework (SSDF)に基づく基準をベースにした、定義済みのSDLコントロール カタログを提供しています。これらのツールは、Dellチームがお客様のためにセキュアな製品を構築し、Dellが開発/サポートするソフトウェアとハードウェアにセキュリティ上の脆弱性が入り込むのを防ぐ上で役立ちます。これらのコントロールは、新しい機能の開発中にエンジニアリング チームによって導入されることが義務付けられています。また、これらのコントロールには、分析アクティビティだけでなく、主要なリスク領域に焦点を当てた規範的でプロアクティブな対策も含まれます。

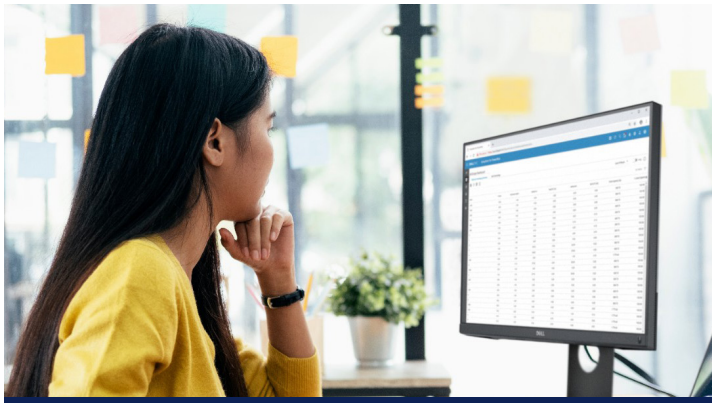
脅威モデリング、静的コード分析、スキャン、セキュリティ テストなどの分析アクティビティは、開発ライフサイクル全体を通じてセキュリティの欠陥を特定して軽減することを目的とした不可欠なコンポーネントです。さらに、SDLには、Open Web Application Security Project (OWASP) Top 10やSANS Top 25などの業界基準で概説されている問題など、開発チームが特定のセキュリティ問題にプロアクティブに対処できるようにするための規範的なコントロールが含まれています。

SupportAssist for Business PCsはこの堅牢なSDLフレームワークと連携し、Dell SDL成熟度モデルを採用して、業界基準に準拠したセキュリティ コントロールを実装します。DevSecOpsプログラムは、継続的インテグレーションと継続的導入(CI/CD)環境でSDLコントロールを自動化してセキュリティ ポリシーを適用することで、Dellの最新のソフトウェア開発と導入プロセスを保護します。これらのCI/CDツールは、ビルド、テスト、導入プロセスを自動化し、開発ワークフローの一部としてコードの変更が継続的に統合されテストされるようにします。

SDLのエンジニアは、SDLセキュリティ評価を実施して、ソフトウェアのセキュリティ上の問題や脆弱性を特定し、これらのセキュリティ上の問題や脆弱性を修正するための推奨事項を開発チームに提供します。これを保証することで、セキュリティ プラクティスの成熟度と、ソフトウェアとハードウェアのセキュリティ体制が可視化されます。

この評価では次のことが行われます。

- 侵入テストによる脆弱性診断。
- Secureworksのような定評のあるベンダーが実施するサードパーティーのセキュリティ テスト。
- 認証、承認、ID管理ソリューションの評価。
- 業界をリードするソフトウェア構成分析ツールを使用した、すべてのサード パーティー製ライブラリーとコンポーネントの徹底的なスキャン。
- 特定のセキュリティ強化に関するDellセキュリティ アドバイザリーの通達。
- 電子データを保護するためのプライバシーとセキュリティの取り組みに沿った、当社のグローバル セキュリティ組織との連携による厳格なデータ分類。
- アプリケーションへのセキュリティ監査とガバナンス手順の適用。



安全性の高いプロセスと実績のある業界プラクティスにより、SupportAssistのセキュリティを確保。

セキュリティ検証テスト

サード パーティーによるセキュリティ評価が、SupportAssistアプリケーションとそれを支えるインフラストラクチャに対して定期的に実施されます。

アプリケーション評価の対象には、データ転送とAPIセキュリティ、静的および動的なソース コード分析、Open Web Application Security Project (OWASP)のクロスチェック、サード パーティー製ライブラリーなどが挙げられます。

インフラストラクチャ評価の対象には、内外のネットワーク デバイス、サーバー、サービス プロバイダーなどが挙げられます。

変更管理

デル・テクノロジーズの変更管理プロセスは、社内の変更管理委員会によって指示されているように、ITIL Foundationのベスト プラクティスに従っています。すべての変更は、変更リクエスト チケットを通じて管理されます。変更を開始するために当社のシステムにアクセスするユーザーは、SDLに精通しているだけでなく、ITILトレーニングを受ける必要があります。バックエンド インフラストラクチャに適用されるすべての更新とアップグレードは、適切に追跡とトレーサビリティを行うためにバージョン管理されます。チームは、自動化されたビルド プロセスを採用して、新しいビルドの適用や、導入されたビルドまたはホット フィックスの取り消しを行います。

Dell.com/supportにプロモートされたすべてのリリースには、既知の制限事項とともに、導入された変更に関する情報が記載されています。

すべての新機能と変更は、当社の製品管理チームによって調整され、記録計画と変更管理プロセスを使用して優先順位が付けられます。

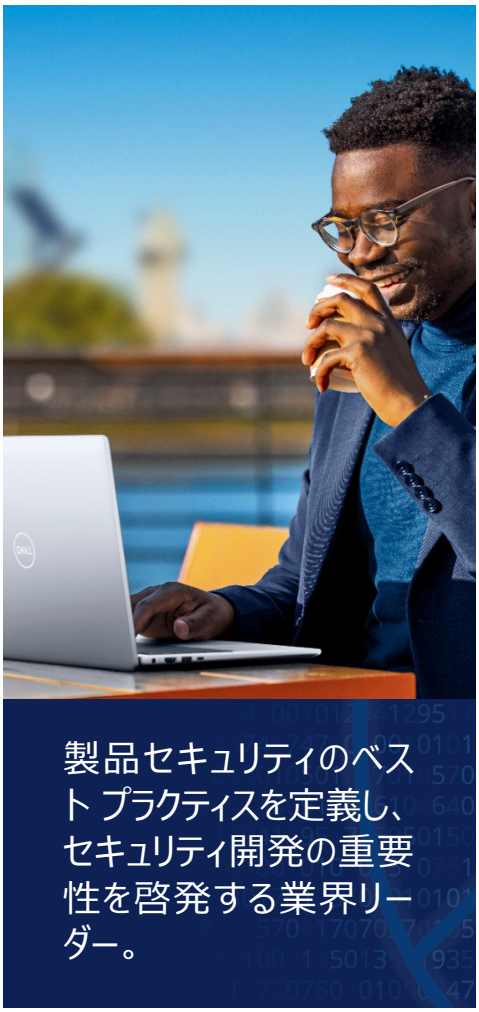
認証

SupportAssistでは、Dell Technologies Servicesインフラストラクチャ、アプリケーションのランダム対称キー、JWTを使用した認証にはDellのマイアカウントを使用し、ボックス内認証にはOSログイン グループを使用します。

データベース管理チームや運用サポート チームなど、SupportAssistコンポーネントへのアクセス権を持つグループには、個別の職務とアクセス権が割り当てられます。また、稼働環境のアップデートはすべて、チェックやバランシングが組み込まれた定義済みの変更管理プロセスを通じて行われます。

セキュリティ意識の高いコミュニティ

職務に固有のセキュリティ ベスト プラクティスや関連リソースの使用方法について新入社員や既存社員を教育するために、当社では、ロール ベースのセキュリティ トレーニング カリキュラムを提供しています。デル・テクノロジーズは、コミュニティー全体でセキュリティ意識の高い文化を築くよう努めています。また、当社の開発者コミュニティーは、ソフトウェア開発プラクティスにおけるセキュリティのシフト レフトを促進することを目的としたDell Security Championプログラムに参加しています。



インシデント レポート

デル・テクノロジーズでは、疑わしいアクティビティー、サイバーセキュリティの問題、または脅威を発見した場合は、security@dell.com宛にEメールを送信して、Computer Security Incident Response Team (CSIRT)に速やかに報告することを全社員に義務付けています。

脆弱性への対策

デル・テクノロジーズでは、製品、アプリケーション、クラウド サービスにおけるセキュリティ上の脆弱性に関連するリスクを最小限に抑えるよう努めています。適切なタイミングで脆弱性に対処できるように、デル・テクノロジーズ脆弱性対応基準(VRT)に記載されているガイドラインを遵守しています。Dellは、Forum of Incident Response and Response Teams (FIRST)やSoftware Assurance Forum for Excellence in Code (SAFECode)など、さまざまなコミュニティーの取り組みに積極的に参加しています。当社のプロセスや手順は、FIRST PSIRT Services Framework、ならびにISO/IEC 29147:2018やISO/IEC 30111:2019などの他の基準に沿っています。

デル・テクノロジーズは、製品、アプリケーション、クラウド サービスの脆弱性に対して、ビジネス上合理的な最短の時間で対処するよう努めています。正確なタイムラインは、脆弱性に対する取り組みの複雑さや修復への影響など、特定の脆弱性とその影響に応じて異なる場合があります。当社のProduct Security Incident Response Team (PSIRT)は、当社に報告されたすべての製品の脆弱性に対する対応と情報の開示を担当しています。デル・テクノロジーズ製品の脆弱性の開示情報はすべて、「Dellセキュリティ アドバイザリー、通知、リソース」ページからオンラインで入手できます。Dellの脆弱性対応プラクティスの詳細については、Dellの脆弱性対応ポリシーを参照してください。

業界内での提携

デル・テクノロジーズは複数の業界団体に参加し、他の大手ベンダーとの連携を通じて製品セキュリティのベスト プラクティスの定義、発展、共有や、セキュリティ開発の重要性の啓発に努めています。業界間連携の実例としては次のものが挙げられます。

- デル・テクノロジーズはSoftware Assurance Forum for Excellence in Code (SAFECode)の共同設立者であり、現在は取締役会議長を務めています。その他の取締役会メンバーには、Microsoft、Adobe、SAP、インテル、Siemens、CA、Symantecの代表者が名を連ねています。SAFECodeメンバーは、ソフトウェア アシュアランスのプラクティスとトレーニングを共有し、公開しています。

業界内での提携（続き）

- デル・テクノロジーズは、Forum of Incident Response and Security Teams (FIRST)の活動的なメンバーになっています。FIRSTは、インシデントと脆弱性への対応における主要な組織であり、グローバル リーダーとして認められています。
- 当社は、The Open Group Trusted Technology Forum (OTTF)に積極的に参加しています。OTTFは、グローバルなサプライ チェーン インテグリティ プログラムとフレームワークの開発を主導しています。
- Dellの従業員は、IEEE Center for Secure Designの創設メンバーです。IEEE Center for Secure Designは、IEEEサイバーセキュリティ イニシアティブの下、ソフトウェア アーキテクトによる一般的なセキュリティ設計の欠陥の把握と防止を支援する目的で立ち上げられました。

業界のセキュリティ基準

- Dellの従業員は、セキュリティ基準の策定と業界別のセキュリティ プラクティスの定義に注力している規格団体と業界コンソーシアムに積極的に関与しています。このような団体には以下が挙げられます。
- Cloud Security Alliance (CSA)
- Forum of Incident Response and Security Teams (FIRST)
- The Open Group
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

デル・テクノロジーズはISO 9001認証を取得しています。当社は、すべての開発および製造センターに対して、四半期ごとの定期監査とコンプライアンス レビューを実施しています。

V. まとめ

SupportAssist接続テクノロジーは、インテリジェントな自動化と修復機能を提供して、組織のDell製デスクトップやノートパソコンすべてのアップタイムを最大化できるようにします。Dell Technologies Servicesは、セキュアなプロセス、データ転送、データストレージに重点を置くことで、この最先端テクノロジーに最適なセキュリティを提供できています。

質問および詳細については、Dell.com/SupportAssistをご覧ください

[1] サポート対象システムと要件については、管理者ガイドを参照し、［supported PCs］を選択してください。プロアクティブな予測型機能を利用できるかどうかは、アクティブなサービス プランとデル・テクノロジーズのビジネス ルールに応じて異なります。ProSupport Suite for PCsの機能については、管理者ガイドを参照し、［Connect and manage capabilities and Dell service plans］を選択してください。

[2] Dellの分析（2023年12月）に基づきます。