SupportAssist for Business PCs：セキュリティの概要

SupportAssist のセキュリティに関する 5 つの主要な質問とその回答をご紹介しています。

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 3

II. SupportAssist について 4

a. 主要機能 4

III. SupportAssist アーキテクチャ 5

a. TechDirect を使用した SupportAssist の一元管理 5

IV. SupportAssist セキュリティ 6

a. SupportAssist が収集するデータの種類とは？ 7

b. 修復スクリプトはどのように保護されているか？ 8

c. SupportAssist がデータを安全に保管および転送する仕組みとは？ 8

d. SupportAssist がデータを使用して行うこととは？ 9

e. 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？ 11

V. まとめ 14

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かねません。また、最悪のタイミングで発生することも少なくありません。このため、企業の CIO（最高情報責任者）は、自社のすべてのパソコンの品質とアップタイムにますます関心を向けています。

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。エンドユーザー システムのシステム状態情報は、問題の迅速な解決や防止のために、企業の IT 部門やハードウェア ベンダー、ソフトウェア ベンダーに送信されます。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稼働時間と効率性を確保するうえで必須です。これに関し、SupportAssist で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ています。

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？
- Dell は GDPR および他の規格にどうやって準拠しているのか？

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。ProSupport Suite for PCs の一部である SupportAssist が、問題を発生前に予測して解決できる包括的なサポート サービスをどのように提供するのかについて、簡単に概要を説明しています。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、自動化されたテクニカル サポートを組織のすべてのパソコンで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 はサポート ケースを自動作成し、サービス プランに基づきテクニカル サポートを提供します。問題のタイプに応じて、アラートによりテクニカル サポート リクエストまたは自動部品ディスパッチが開始されます。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、単一のソリューションで最も包括的なサポート機能を提供します。複数のサービスを契約する必要はありません。[2]
詳細はこちら。

主な機能

- 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、アプリケーション エクスペリエンス、セキュリティ スコアを単一の画面で迅速に分析
- Dell 製スクリプト ライブラリーで全 PC のタスクを自動化し問題を修復
- Dell BIOS、ドライバー、ファームウェア、アプリケーション用のカスタム アップデート カタログの作成と導入を自動化
- TechDirect でビューや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。

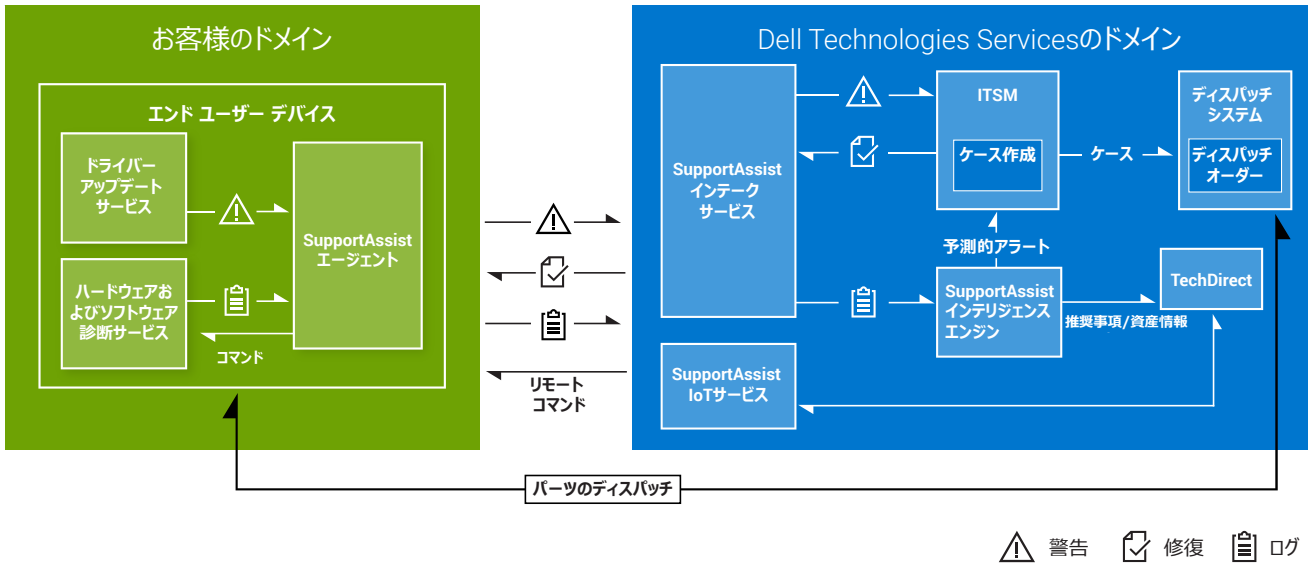
機能の一覧については、管理者ガイドを参照してください。

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。

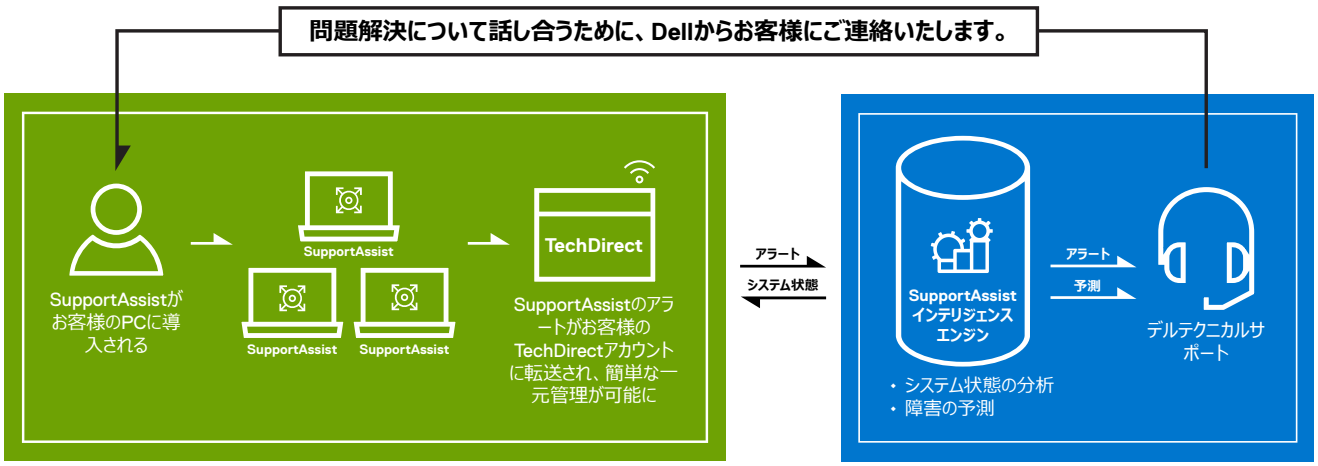
SupportAssist の導入と修復に関するネットワーク、エンドポイント、ポート、ファイアウォール、ゲートウェイの要件の一覧については、導入ガイドを参照してください。修復スクリプトは Dell が開発したものです。実行前に、テスト、署名、確認が行われています。

SupportAssistアーキテクチャ



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。

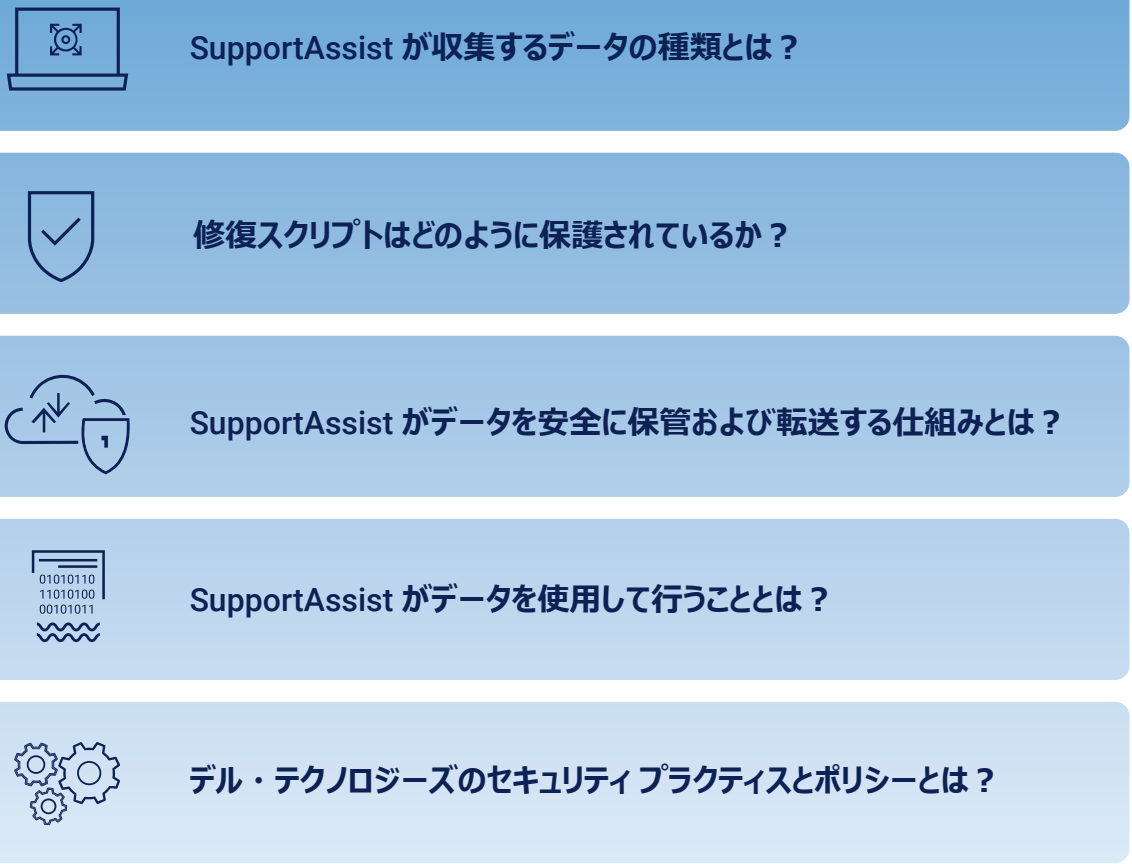


TechDirect を使用した SupportAssist の一元管理（続き）：

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 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 セキュリティ

CIO や CSO が確認したいのは、SupportAssist が収集するデータの種類や管理方法でしょう。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、最適化された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、以下の質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。このデータにより、当社はお客様にあわせたインテリジェントなサポートを迅速に行うことができます。

デバイスから収集される情報のうち、お客様に関するものは、作業対象のエンドユーザー デバイスの特定に必要なサービス タグのみです。部品のプロアクティブな配送が必要であると SupportAssist が判断した場合は、デル・テクノロジーズのサーバーに（暗号化、保存ポリシーなどを用いて）安全に保存されている既存の連絡先情報が使用されます。

日常のシステム監視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：**日常的なシステム監視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た 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：**日常的なシステム監視情報が 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：**使用されているシステム メモリー量
- **CPU の利用率：**使用されている CPU 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 更新日：**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監視データの詳細については、Dell.com のこちらの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。

修復スクリプトはどのように保護されているか？

Dell が作成した修復スクリプトは、修復プラットフォームにアップロードされる前に、Dell の証明書で署名され、広範なテストや検証を経て、意図したとおりに機能すること（予期せぬ結果をもたらさないこと）が確認されています。これは、実行前のスクリプトの信頼性確認における基礎部分です。例えば、エンドポイントでスクリプトが変更または置換された場合、証明書署名の検証は失敗し、SupportAssist によってスクリプトの実行がブロックされます。これにより、不正なコードや潜在的に有害なコードの実行を防ぐことができます。スクリプトは Dell 以外のユーザーには変更できないことから、整合性が確保されています。広範な導入を行う前に、特定のパソコン グループでスクリプトをテストすることを推奨します。

カスタム ワークフロー スクリプトでは、異なるプロセスが実行されます。お客様が独自のスクリプトをアップロードするとき、修復システムは未署名のスクリプトと、お客様の証明書で署名されたスクリプトの両方を受け入れます。これらのスクリプトの整合性は、パソコンに転送するときや保管されているときも維持されます。より広範な導入を行う前に、特定のパソコン グループでカスタム スクリプトをテストすることを推奨します。

TechDirect の［接続と管理］ではサイトやグループを作成できます。お客様は、Dell が作成したスクリプトやカスタム スクリプトをテストマシン上で検証することができます。修復コンソールのすべての情報は、TechDirect のテナント境界内で保護され、テナント管理者によって割り当てられた適切な役割を持つユーザーのみがアクセスできます。詳細な分析のために、結果を CSV ファイルにエクスポートすることも可能です。

SupportAssist がデータを安全に保管および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。

パッケージのインストール実行時には、マシンごとに暗号化キーが生成されます。この暗号化キーとソルトを使用し、インストールした情報が暗号化されます。静止データは、業界標準のアルゴリズムにより暗号化されます。

ソルトは、暗号化技術における無作為なデータであり、データ、パスワード、パスフレーズを「ハッシュ化」する一方向性関数の入力として使用されます。ソルトの主な機能は、辞書攻撃、およびそのハッシュ化版であるレインボー テーブル攻撃を防ぐことです。

暗号化キーはすべて、セキュアな乱数発生器により生成されます。転送中のデータは、TLS over Hypertext Transfer Protocol Secure (HTTPS) で保護されます。暗号化アルゴリズムはすべて業界標準のものであり、静止データを暗号化します。

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。

コンテンツをエンドユーザーのデバイスに転送またはダウンロードする場合、標準 HTTPS により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が保護されます。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。平均データ消費量の詳細については、接続済みパソコンから収集されるデータについてのドキュメントを参照してください。

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。

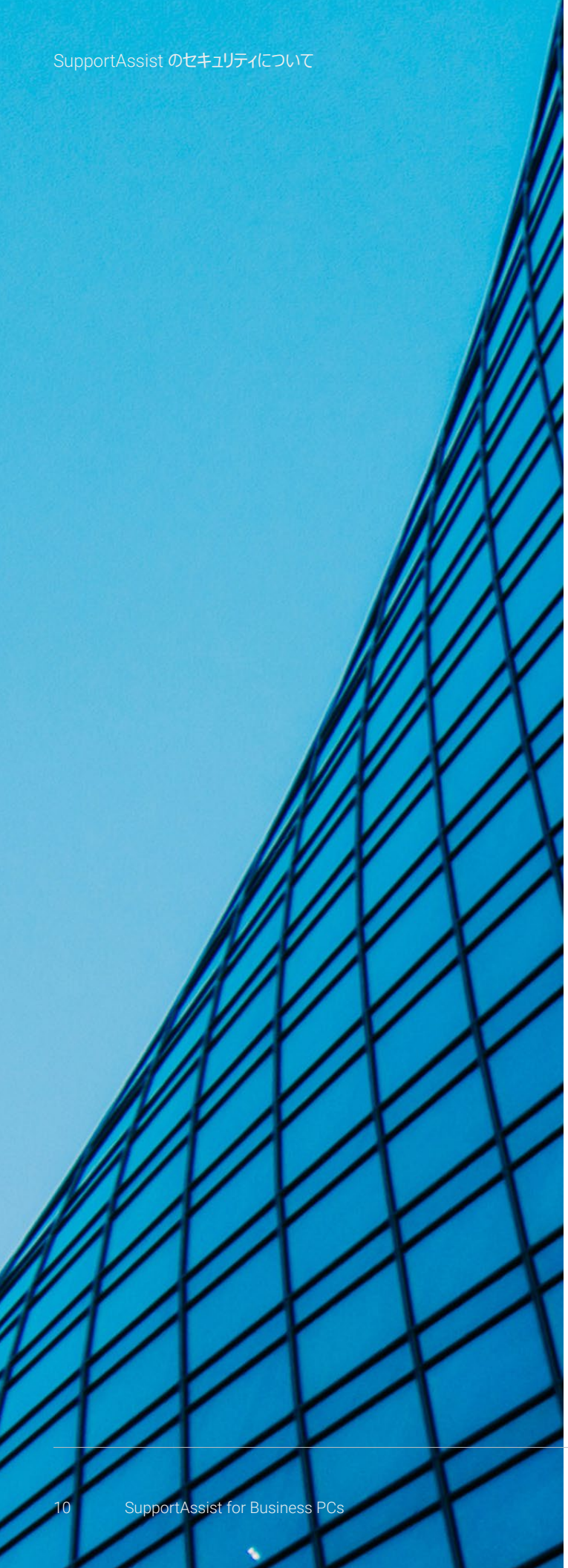
システム アプリの使用状況では、インサイト コンポーネントを使用して、システムの使用状況に関するインサイトを把握できます。

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。

保管されるデータは、物理的および論理的なセキュリティ対策によって安全に維持されます。



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 の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。

GDPR（一般データ保護規則）

Dell は、GDPR に基づく義務の履行に必要なプロセスと手順を確保するため、対策を講じてきました。Dell は、世界中のプライバシー法の動向を追跡し、関連するプライバシー法のもとで適用される義務を確実に遵守します。Dell が処理者として行動する場合、相互に合意した形式、または標準的なデータ処理契約書に従って行動します。詳細については、次のリンクを参照してください。

- Dell's GDPR Information Security Corporate Statement and Controls Summary
- Dell's Commitment to GDPR Compliance
- Dell's Compliance FAQs for Dell Technologies Customers

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 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が定めたとおり、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 に掲出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、Dell 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、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 プログラムの一環です。

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、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、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、各種コミュニティー活動に積極的に参加しています。Dell 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。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開示情報はすべて、「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。

製品セキュリティのベスト
プラクティスを定義し、
セキュリティ開発の重要性を
啓発する業界リーダー。

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です。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。
- Dell 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。
- デルの従業員は、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 イニシアチブの下、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理解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規格

- 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。Dell は、すべての開発センターと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、ユーザーズ ガイド（個人向けの SupportAssist for Home PCs の場合）または管理者ガイド（すべてのパソコンを管理する SupportAssist for Business PCs の場合）の「Supported PCs」をクリックしてください。プロアクティブで予測的な機能を利用できるかどうかは、有効なサービス プランとデル・テクノロジーズのビジネス規則によって異なります。ProSupport Suite for PCs の機能については、管理者ガイドの「接続および管理の機能と Dell サービス プラン」をクリックしてください。Dell Care Suite、Premium Support Suite、Alienware Care Suite for Pcs の機能については、ユーザーズ ガイドの「SupportAssist 機能と Dell サービス プラン」をクリックしてください。

[2] Dell の分析（2023 年 12 月）に基づきます。

© 2025 Dell Inc. All rights reserved.（不許複製・禁無断転載）本書内の商標および商標名は、それらの商標または商標名を主張する団体、もしくはその製品を表すために使用される場合があります。サービス内容は公開時の情報に基づいており、予告なく変更されることがあります。Dell およびその関連会社は、誤植や入力ミスによる、または写真に関する誤りや遺漏について、一切の責任を負いません。Dell の販売およびサービス契約条件が適用され、請求に応じて提供されます。デルのサービスが、お客様の法的権利を侵害することはありません。2025 年 3 月 | KI