セキュア コネクト ゲートウェイ

このテクノロジーは、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化サポート体験を提供するサービスです。

最大で

60%

Forresterによるアンケートで、リスクの低減のために接続テクノロジーを活用していると答えた**IT**リーダーの割合[1]

また、一部のDell EMCハードウェアでは直接接続バージョンとして実装されており、さらにOpenManage Enterprise for PowerEdgeサーバー内のサービス プラグインとしても実装されています。Dell Technologies Servicesではお客様のセキュリティ目標とコンプライアンス要件を満たす製品をお届けするために、市場、規制、お客様のインサイトに基づくセキュリティ機能の実装に取り組んでいます。

目次

1：はじめに

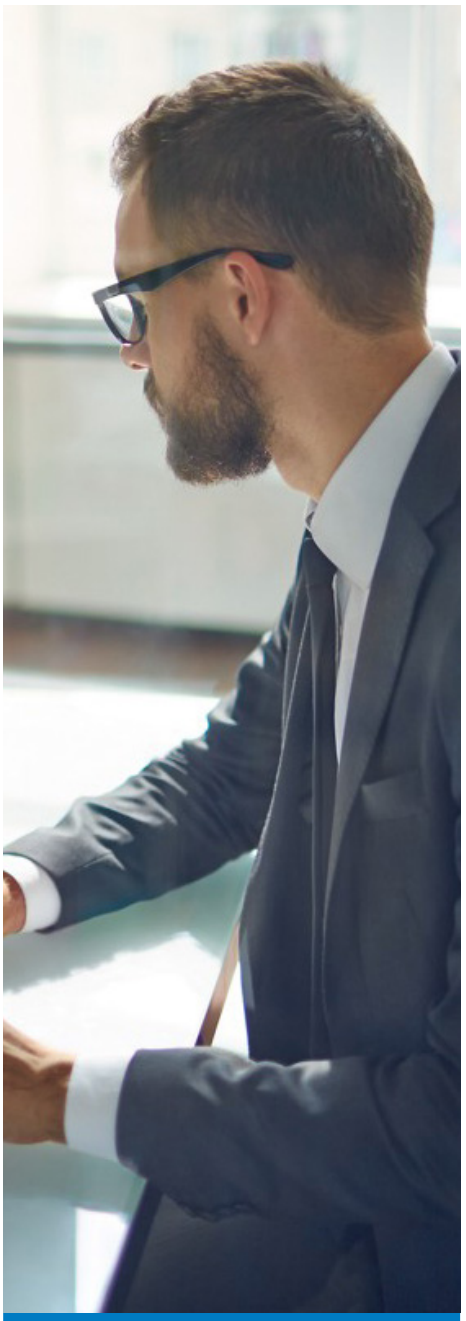
今日のデジタル化が極度に進んだ社会において、成功を収めているイノベーション リーダーは、ITサポートをITサービス プロバイダーにアウトソーシングしています。Dell Technologies ServicesがForrester Consultingに委託した調査によると[1]、ITリーダーの59%は、適切なITサービス プロバイダーと提携することで、ITスタッフの時間を日常業務からイノベーションや戦略的イニシアティブにシフトできると述べています。

大手ITサービス プロバイダーであるDell Technologies Servicesは、自社のITサポート サービスおよびテクノロジーからセキュリティ脅威が拡散されることがないように努めています。当社は、一日も欠かすことなく、Dell EMC製品を自社環境に導入したお客様に対するリスクを最小限に抑えるために、あらゆる対策を講じています。本書では、セキュア コネクト ゲートウェイの設計、導入、および運用にセキュリティを組み込んで、安全性の高い自動化ITサポート体験を複雑なデータ センター インフラストラクチャで実現する方法について説明します。

25年以上にわたるITサポート テクノロジーの先駆者としての経験を結集させたセキュア コネクト ゲートウェイ セキュリティ アーキテクチャは、脅威の侵入を食い止めて、データの整合性を保護するように設計されています。デルのテクノロジーには、お客様のデバイスの問題を継続的に監視して迅速な解決を促すと同時に、以下のような特徴があります。

- デルで利用するのはアクティブ システムから収集されたテレメトリー データとイベント データだけです。
- システム状態データは暗号化され、トランスポート層セキュリティ（TLS）プロトコルを使用したHTTPS経由のインターネットで送信されます。
- デルの認定テクニカル サポート エンジニアが、接続されているシステムに多要素認証を使用してリモートでアクセスして問題解決にあたります。
- デルでは、業界をリードするセキュリティ プラクティスに従い、テレメトリーおよびイベント データを当社ロケーション内で処理、保管、および使用します。

さらに、セキュア コネクト ゲートウェイ アーキテクチャおよびプロセス全体に統合するセキュリティ対策を、Secureworksをはじめとする一流クラスのベンダー数社と連携しながら吟味することで、信頼性の高い、プライバシーが保護された安心できる体験をお客様に提供します。



サイバー攻撃やデータの不正および窃取は、CEOにとって上位10個の問題に数えられます[2]

2：セキュア コネクト ゲートウェイについて

デル・テクノロジーズがお届けするセキュアな接続テクノロジーを使用することで、問題防止から当て推量を排除し、最も重要なプロジェクトに費やす時間を増やすことができます。仮想アプライアンスおよびアプリケーションの各エディションは、お客様の環境とDell Technologies Servicesとの間にセキュアな双方向接続を確立し、データ センター全体でDell EMCデバイス（データ ストレージ、サーバー、ネットワーキング、CI/HCI、データ保護など）を1か所で監視するのに最適なプラットフォームです。

このテクノロジーは導入方法に柔軟性があり、一部のDell EMC製品の直接接続バージョンとして導入することも、OpenManage Enterprise for PowerEdgeサーバー内のサービス プラグインを使用して導入することもできます。特定のDell EMCハードウェアおよびソフトウェアでサポートされている接続オプションについては、Dell.com/Supportでご確認ください。

セキュア コネクト ゲートウェイにとってデータは生命線です。デルは、お客様の環境のシステム状態データを利用し、現場チームとテクニカル サポート チームだけでなく、コンポーネント メーカーから長年にわたって得られたインシデントおよびエンジニアリングデータとの関連付けを行います。

セキュア コネクト ゲートウェイとOpenManage Enterprise向けサービス プラグインのレポート対象項目および収集対象のシステム状態情報については、こちらをご覧ください。

デル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、パターンを発見して適用することにより、初動で的確な問題を正確に検出して対処することができます。コストのかかる問題に発展する前に、ハードウェアとソフトウェアの問題を特定してケースを作成し、デルとの問い合わせを開始して問題の解決に取り掛かります。セキュア コネクト ゲートウェイを経由して接続が確立されると、サーバーのハード ドライブおよびバックプレーンの障害を予測します。問題のタイプによっては、アラート発生と同時にパーツの自動発送を開始することもできます。

さらに、このテクノロジーでは、安全性の高い双方向通信を確立し、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トラブルシューティングして解決することができます。

接続のセキュリティ

サードパーティー セキュリティ評価が、セキュア コネクト ゲートウェイ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、データ転送および**API**セキュリティ、静的および動的なソース コード分析、共通脆弱性識別子（**CVE**）と**Open Web Application Security Project**（**OWASP**）のクロスチェック、サードパーティー ライブラリーおよび製品が含まれます。

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、およびサービス プロバイダーが含まれます。

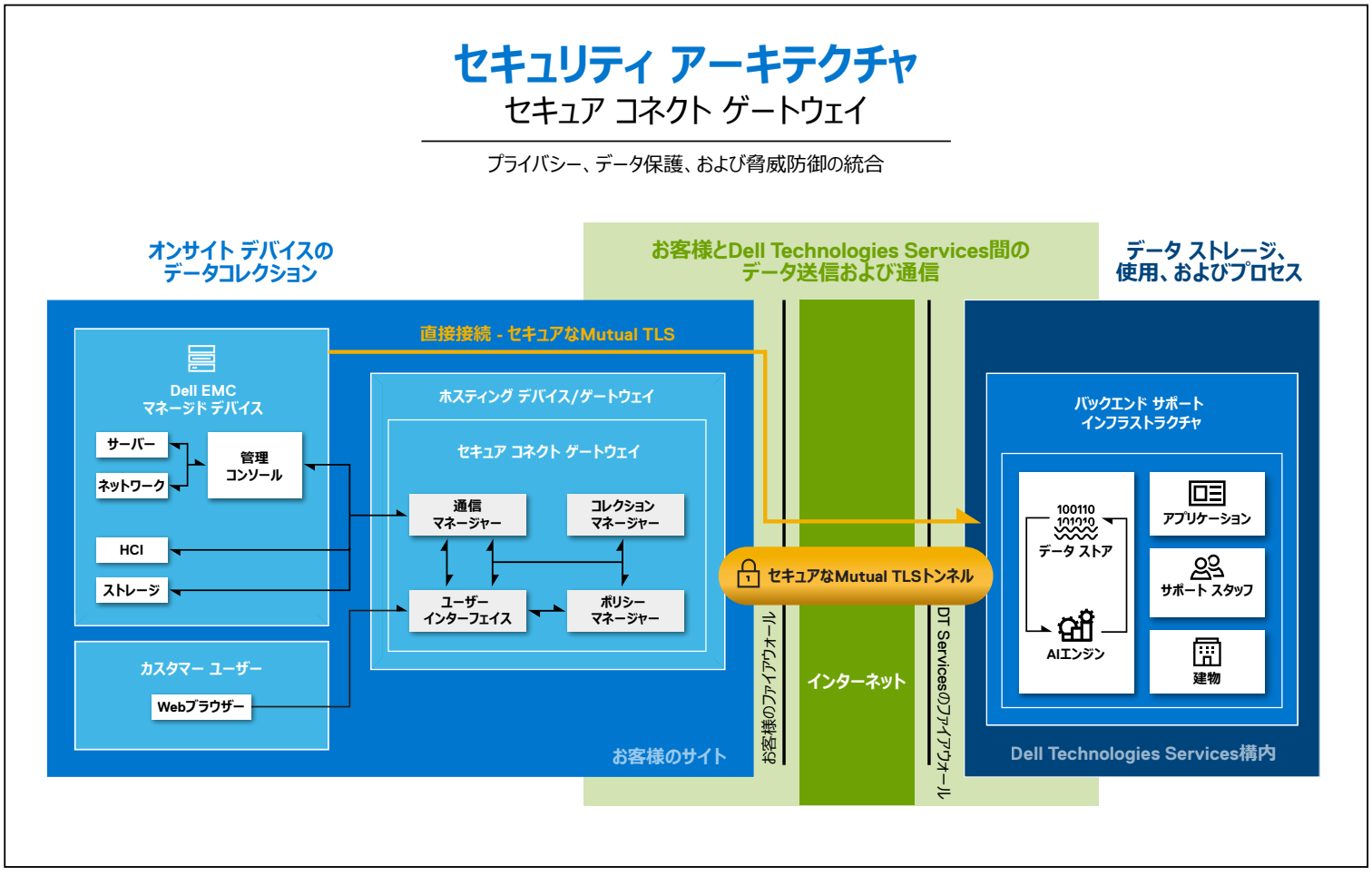
3：セキュリティ アーキテクチャの概要

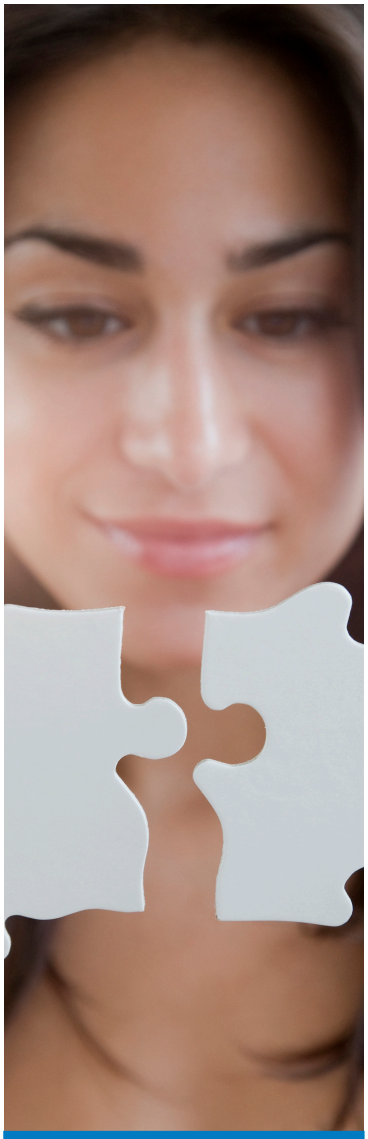
Dell Technologies Servicesは、予防的かつ予測型の自動化接続テクノロジーによってセキュリティ脅威のリスクを最小限に抑えることに取り組んでいます。デルのセキュリティ アーキテクチャは、厳格な業界規格に従って構築されており、測定可能および再現可能なセキュリティ プラクティスに則って製品の開発および導入を着実に進めていくことができます。詳細については、セクション4を参照してください。

以下の図Aは、セキュア コネクト ゲートウェイ セキュリティ アーキテクチャの概要を示しています。以降のセクションでは、問題の診断と修正に必要なDell EMCマネージド デバイスからどのようにシステム データを収集して問題を解決し、また、以下のセキュリティおよびプライバシーを最大限に高めながらデータを処理するのか詳しく掘り下げます。

- オンサイト デバイスのデータコレクション
- データの転送と通信
- Dell Technologies Servicesのデータ ストレージ、使用、およびプロセス

図A：





お客様は、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の監査機能を通じて、オンサイト データ コレクションのためのセキュリティ レイヤーを強化することができます。

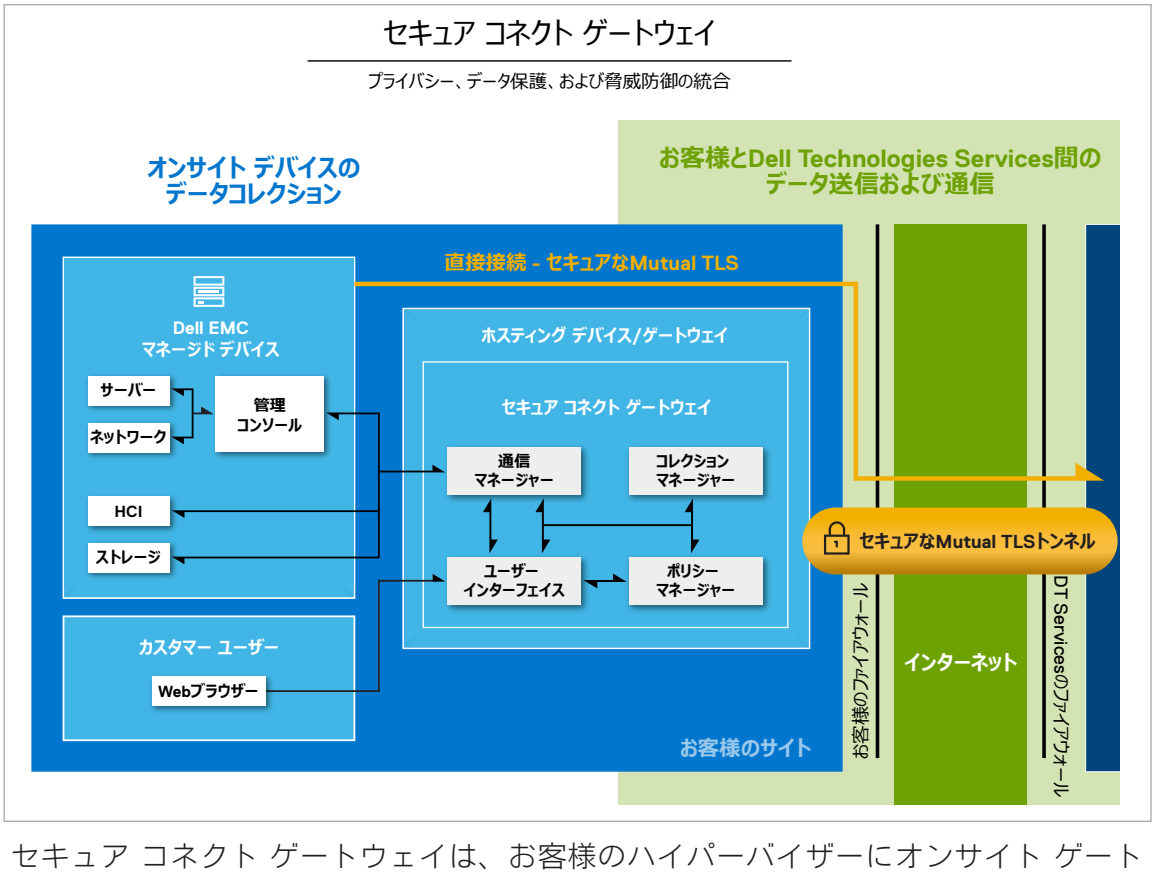
4：セキュア コネクト ゲートウェイの詳細なセキュリティ アプローチ

4-1：セキュアなオンサイト データコレクション

ファイアウォールのアクセス ポイント数の最小化

セキュア コネクト ゲートウェイは、Dell EMCデバイスとの通信を集約し、お客様のファイアウォール内でIPベースのリモート サービス アクティビティの唯一の出入口として機能します。図Bをご覧ください。リモートITサポート テクノロジーのファイアウォール アクセス ポイント数を最小限に抑えることで、企業のファイアウォール経由によるセキュリティ リスクを緩和します。

図B（図Aの抜粋 – セキュリティ アーキテクチャ）：



セキュア コネクト ゲートウェイは、お客様のハイパーバイザーにオンサイト ゲートウェイとして仮想的に導入されます。各ゲートウェイ サーバーはプロキシとして機能し、管理対象デバイス間で情報をやり取りします。セキュア コネクト ゲートウェイでは、ローカル ネットワークに一時的な障害が発生した場合に、コネクト ホーム イベントをキューに入れることもできます。これらのゲートウェイ サーバーは、基盤となるオペレーティング システムをベースとする独自のWebユーザー インターフェイスを備えています。

直接接続バージョンは、複数のDell EMCハードウェア製品を異種混在環境に導入しようとしているお客様に適しています。このソリューションは、お客様のファイアウォールを経由する唯一のセキュアな通信ポイントとして機能します。このバージョンは製品の運用環境に統合されるため、別途サーバーを用意して、インバウンド リモート サポートおよびコール ホーム機能を提供する必要はありません。

ファイアウォールのアクセス ポイント数の最小化（続き）

OpenManage Enterpriseシステムの管理コンソールを使用しているPowerEdgeデータ センターのお客様にとって代替の実装オプションとなるのが、組み込みサービス プラグインです。OpenManage Enterprise仮想アプライアンス内のこの接続プラグインは、お客様が用意したハイパーバイザー上で実行されます。これはマネージド サーバーおよびシャーシ デバイスのサービス自動化レイヤーとして機能し、Dell Technologies Servicesバックエンドへのセキュアな直接接続を1つ提供します。

セキュアな通信ブローカーとして機能

セキュア コネクト ゲートウェイは、管理対象デバイス、ポリシーマネージャー、およびDell Technologies Servicesのバックエンド サポート インフラストラクチャ間の通信ブローカーとして機能します。導入されているゲートウェイ サーバーは、HTTPSハンドラーとして機能します。セキュア コネクト ゲートウェイでは、デバイス検出、イベント管理、テレメトリー データコレクション、テレメトリー データ管理などのさまざまな通信方法が使用されます。メッセージのタイプには以下のものがあります。

- デバイス状態のハートビート ポーリング
- データ ファイルの転送（コネクト ホーム）
- ライセンス使用データの転送
- ユーザー認証要求
- デバイス管理の同期

すべてのメッセージは、複数のプロトコルを使用して安全性を確保されます。次のセクションでは、エンドツーエンドのトランスポート層セキュリティ（TLS）トンネリングおよび業界標準の暗号化方式とHTTPSプロトコルの併用など、セキュア コネクト ゲートウェイのデータ通信および転送への追加セキュリティの組み込みについて詳しく見ていきます。

承認要件およびアクセス許可のお客様による管理

お客様のデータ センターでデバイスをセキュア コネクト ゲートウェイで監視している場合、お客様は、ポリシーマネージャーを使用して、リモート アクセス接続、診断スクリプトの実行、その他の関連アクティビティの承認要件を制御することができます。お客様は、リモート接続して問題を診断および修正するスタッフおよびテクニカル サポート エンジニアに対してアクセス許可を設定できます。

承認およびアクセス許可を管理するためのセキュリティは、以下のポリシーマネージャーの機能によって保証されます。

- セキュア コネクト ゲートウェイが、アクセス許可の変更がないかポリシーマネージャーを定期的にポーリングし、アクセス許可をローカルの場所にキャッシュします。ポリシーマネージャー側では以下の処理が行われます。
  - 最終ポーリング サイクルが完了すると、設定の更新情報がルール セットのキャッシュに自動的に反映されます。
  - 特定の取り決められたポートのHTTPSリスナーとしてメッセージを受信するように設定されています。
- セキュア コネクト ゲートウェイは、リモート アクセス要求または他のアクションを受信すると、ポリシーマネージャーのキャッシュから受け取ったポリシーを実行します。
  - アクセス許可は、デバイスのタイプに基づいて、またはデバイスの1つのタイプの特定のモデルに基づいて、ポリシーに階層的に割り当てることができます。
  - お客様は、ポリシーマネージャーのWebユーザーインターフェイスを通じ、要求されたアクションを承認または拒否することができます。また、承認とアクションに対してさらに制限を課すフィルターを作成することもできます。

ログ記録と監査証跡

お客様は、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の監査機能を使用することで、オンサイト データコレクションのセキュリティ レイヤーを強化することができます。ポリシーマネージャーは、すべてのリモート サービス イベントおよび接続、診断スクリプトの実行、およびサポート ファイルの転送操作を記録します。次にこの情報を、ポリシーマネージャーのデータベース内に単純なテキストの監査ログ ファイルとして保存します。ポリシーマネージャーはポリシーマネージャーに対するアクセス、ポリシーの変更、およびアクセス アクティビティの承認または却下すべてを追跡します。

セキュア コネクト ゲートウェイ

サポートされているTLS 1.2暗号スイート：

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

以下の理由から、お客様はこの情報のすべてをいつでも利用することができます。

- 監査情報はポリシーマネージャーのWebユーザー インターフェイスに表示されますが、これを編集することはできません。
- 監査ログは、その環境内のsyslogサーバーにストリーミングされるように設定することもできます。

デバイス制御のセキュリティ オプション

承認およびアクセス許可の管理にポリシーマネージャーを使用しないお客様のために、セキュア コネクト ゲートウェイにはデバイス制御オプションによる関連セキュリティ機能が用意されています。

お客様が使用できる機能は次のとおりです。

- デバイスのタイプ、管理者グループ、組織ユニットまたはビジネス ユニット、デバイスの物理的な場所、または採用する他の基準に基づいてカスタム グループを作成する
- これらのデバイス グループ別に具体的な権限とアクセス権を定義する

テクニカル サポート エンジニアが実行したリモート アクティビティなど、すべてのデバイス管理操作がログに記録されます。これらの操作は、テクニカル サポート エージェントによるバックエンドでの承認を必要とします。

このようにしてお客様は、セキュア コネクト ゲートウェイを通じて管理されるデバイスを完全に制御し、透明性を維持することができます。

二要素認証とデジタル証明書管理

認証は、安全性の高いオンサイト データコレクションの重要な要素です。セキュア コネクト ゲートウェイは、お客様のゲートウェイ サーバーに導入する際の身元証明にデジタル証明書を使用します。この証明書では、ゲートウェイ サーバーのIDが、バックエンドとの通信を暗号化して認証するために使用されるキー ペアにバインドされています。Dell Technologies Servicesの認証局（CA）は、セキュア コネクト ゲートウェイの主要インフラストラクチャの中央リポジトリーです。

デジタル証明書管理を使用して、デルのプライベート認証局を通じたデジタル証明書の登録を自動化します。その結果、以下が実現します。

- それぞれの証明書要求の生成と認証をプログラムで記述できます。
- 証明書の発行とインストールはゲートウェイ サーバー上でしか行われません。証明書をコピーして別のマシンで使用することはできません。

セキュア コネクト ゲートウェイは、デルのバックエンド サポート インフラストラクチャに導入されたデジタル証明書を使用して接続と認証を行います。テクニカル サポート エージェントは、二要素認証を使用して、お客様の環境内のセキュア コネクト ゲートウェイに接続します。

4-2：セキュアなデータ転送および通信

安全性の高い通信トンネル

お客様とDell Technologies Serviceのバックエンド サポート インフラストラクチャ間の通信はすべて、セキュア コネクト ゲートウェイによってお客様のサイトからアウトバウンドで開始されます。インターネット経由による業界標準のトランスポート層セキュリティ（TLS）256ビット暗号化とDell Technologies Servicesが署名したデジタル証明書認証を使用して、安全性の高いエンドツーエンドの通信トンネルが作成されます。このデジタル証明書認証については、前述のセキュアなオンサイト データコレクションに関するセクションで詳しく説明しています。

結果として、セキュア コネクト ゲートウェイ接続は以下の特性を持つようになります。

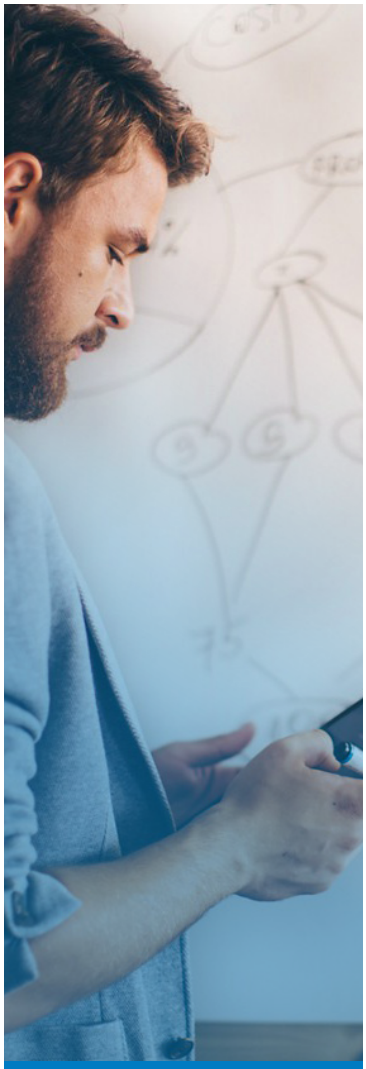
- **信頼性の高いデータ転送：**送信される各メッセージには、メッセージ認証コードを使用したメッセージ整合性チェックが含まれており、転送中のデータの損失や改ざんの未検出を防止できます。
- **TLSによるプライベートでセキュアなセッション：**業界標準のアルゴリズムを使用した対称暗号化により、接続ごとに固有のキーが生成されます。ネゴシエーション中に発生した通信の改ざんは必ず検知されます。
- **認証済みの通信相手：**この接続は安全性が高いため、公開キー暗号化を使用して通信相手を識別し認証します。この手法により、スプーフィング攻撃および中間者（MITM）攻撃を防止します。

セキュアなTLSトンネルを使用した通信

ゲートウェイ サーバーは、TLSトンネル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 アクセスの各機能のためにセキュアな環境を確保します。このセクションおよび図Cでは、デルのテクノロジーによる自動化された予防的かつ予測型の体験を実現するための中核をなす通信プロセスおよびプロトコルについて詳しく見ていきます。

ハートビート ポーリング

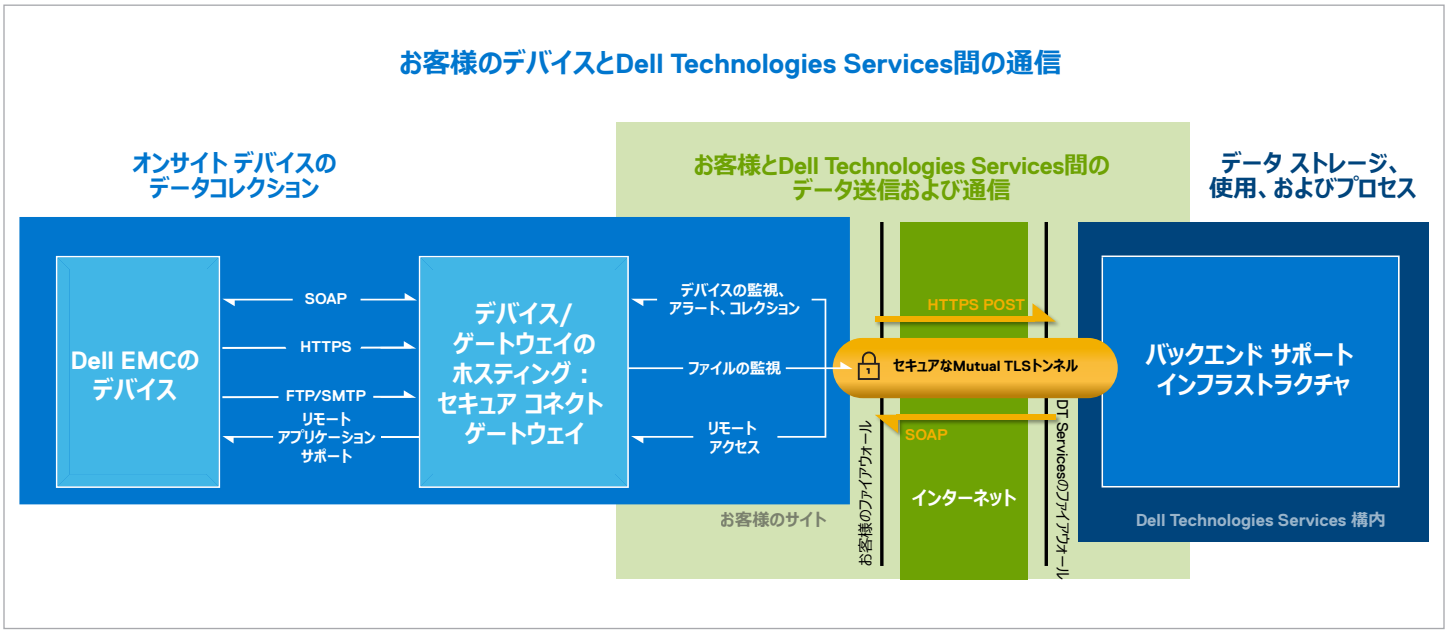
セキュア コネクト ゲートウェイ体験のメリットを手にするには、お客様のシステム同士を接続する必要があります。ハートビート ポーリングは、デバイスの接続ステータスをチェックし、収集したテレメトリー データをバックエンドに定期的に送信します。このデータを使用すると、セキュア コネクト ゲートウェイが導入されているゲートウェイ サーバーも識別できます。



業界をリードする認証により、スプーフィング攻撃と中間者攻撃から接続の安全を守ります

セキュアなTLSトンネルを使用した通信（続き）

図C：セキュリティ アーキテクチャ



リモート通知またはコネクト ホーム機能

セキュア コネクト ゲートウェイは、バックエンドにイベント ファイルを送信するデバイスにとって安全性の高い経路として機能します。これには、エラー、アラート、警告状態、健全性レポート、設定データ、スクリプト実行ステータスなどがあります。

- アラートが発生するとイベント ファイルが生成され、セキュア コネクト ゲートウェイに送信されます。
- HTTPSリスナー サービスを介してセキュア コネクト ゲートウェイがこのファイルを受信します。
- セキュア コネクト ゲートウェイについてFTPリスナーやSMTPリスナーを使用しているレガシー製品の場合、ファイルは暗号化されて転送されます。
- セキュア コネクト ゲートウェイはファイルを圧縮してTLSトンネル経由でバックエンドに送信します。次に、リスナー ディレクトリーからこのファイルを削除します。
- その後、ファイルは分析のためにバックエンドで解凍されます。
- セキュア コネクト ゲートウェイでは、暗号化された通信トンネル経由でバックエンドにファイルを送信することもできます。さらに、フェールオーバー チャネル（FTPS）またはお客様がご利用のEメール サーバーを使用するように設定することもできます。

アクティブなシステムのさまざまなコンポーネントからシステム監視データを収集することで、Dell Technologies Servicesは、順応性の高いインテリジェントで迅速なサポート体験を提供します。デバイスから収集される企業に関する情報は、現在稼働している特定のシステムの識別に必要なシステムIDだけです。パーツを前倒しで発送する必要があるとデルが判断した場合、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が使用されます。

アクティブなシステムから収集されたシステム監視データの完全なリスト（通常の24時間サイクル外に収集されたデータを含む）は、セキュア コネクト ゲートウェイ向けのレポート対象項目ドキュメントと、OpenManage Enterprise向けサービス プラグインで確認できます。

リモート アクセス

また、デルのテクニカル サポート チームは、お客様のサイトのデバイスにリモートでアクセスして、問題のトラブルシューティングを行ったり、デバイス固有のアクションを実行したりします。非同期メッセージングにより、リモート アクセス セッションが、お客様のサイトのセキュア コネクト ゲートウェイから開始されるようにします。次に、セキュアなリモート アクセス セッションが次のように確立されます。

- Dell Technologies Servicesのバックエンドでのセッション認証後、テクニカル サポート エージェントが、サービス リクエスト番号（該当する場合）とその他のデバイスIDまたはユーザーIDなどを含め、デバイスへのアクセスを要求します。
- このリモート アクセス要求は、セキュア コネクト ゲートウェイがデバイスのハートビート メッセージをこのバックエンドに送信して取得するまで、バックエンドのキューに入れられた状態になります。
- この要求に対し、バックエンド サーバーは、要求情報、バックエンド サーバーのアドレス、およびセキュア コネクト ゲートウェイに接続するための固有のセッションIDなどを送り返します。
- セキュア コネクト ゲートウェイはそのローカル リポジトリーを使用して、デバイスのローカルIPアドレスを特定します。次に、ポリシーマネージャーのキャッシュに保存されているポリシーをチェックして、接続を許可するかどうか吟味します。
- セキュア コネクト ゲートウェイは、許可されている場合、バックエンド サーバーとの個別の永続的なTLS接続を確立します。TLS接続は、常にセキュア コネクト ゲートウェイによって開始され、バックエンド サーバーは、ゲートウェイ サーバーとのインバウンド接続を開始できません。これにより、外部からの攻撃に対する脆弱性が生じないようになっています。

通信はセキュア コネクト ゲートウェイとバックエンド サーバー間のトンネルを通過し、一定期間非アクティブ状態になると停止するかタイムアウトになります。

ネットワーク セキュリティ

すべてのネットワーク監視コンポーネントは、ファイアウォールの背後に配置されており、ネットワーク セキュリティ チームによって管理されます。ネットワーク トラフィックは厳重に制御されます。すべての着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 アドレスに限定して送信されます。

4-3：セキュアなデータ ストレージ、使用、およびプロセス

ストレージと使用のセキュリティ

物理的セキュリティ

Dell Technologies Servicesは、アプリケーション、システム、ネットワーク、およびセキュリティ コンポーネントを含むほとんどのセキュア コネクト ゲートウェイ データを、高い可用性とセキュリティを保持できる能力がある米国を拠点とするデータ センターでホスティングしています。データは、物理的なセキュリティはもちろんのこと、さまざまな対策により保護されています。このような機能には以下が含まれますが、これらに限定されません。

- オンプレミスのセキュリティ対策
- カメラ
- 疑似エントランス
- 車両封鎖ゲート
- 特殊な駐車場設計
- 防弾ガラスと防弾壁
- 標的となっていない建物の使用

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、許可を受け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。

論理的セキュリティ

セキュア コネクト ゲートウェイによって生成されたデータは、デルのプライバシー 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ITガイドラインに従って監査および評価されます。

論理的セキュリティ（続き）

- **サーバーおよびデータベースのセキュリティ：**サーバーおよびオペレーティング システム コンポーネントは、セキュリティ審査を受けた標準イメージに配置されています。アプリケーションで使用されるセキュリティ更新プログラムに対しては、Microsoftおよびその他のソフトウェア ベンダーによって公開されているものを含め、定期的にレビューが行われます。重要なセキュリティ アップデートが発行されると、まず非運用イメージ上でテストを行い、通常はライブ サーバーに適時に適用されてリスクを防ぎます。
- **監査：**監視対象デバイスのログが保持されます。Dell Technologies Servicesによって認可されたインフラストラクチャとアプリケーション以外はログにアクセスできません。このログには、オペレーティング システムやセキュア コネクト ゲートウェイ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、Center for Internet Security（CIS）Controlsの推奨セキュリティ ベスト プラクティスを採用することで強化されています。業界標準のセキュリティ ガイドラインも、すべてのサーバーおよびネットワーク機器に実装されています。

また、セキュア コネクト ゲートウェイ エコシステムは、そのデータ センター内と別のデータ センターの同一のインフラストラクチャ内でローカル性と高可用性を両立します。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Dell Technologies Servicesが使用するのは、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、自在に制御および管理可能なクラウド環境です。

認証

セキュア コネクト ゲートウェイでは、Dell Technologies Servicesによる認証にデルのマイアカウントを使用し、Box内認証に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、セキュア コネクト ゲートウェイ コンポーネントに対する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ています。運用環境に対するすべての更新には、チェックとバランスを図る定義済みの変更管理プロセスが適用されます。

デルでは、製品およびアプリケーションに再現性と安全性の高い開発プロセスを採用しています。

プロセスのセキュリティ

セキュリティ意識の高いコミュニティ

当社は、職務内容別のセキュリティ ベスト プラクティスと関連リソースの使用方法について、新規および既存の社員を教育することを目的とした、マルチレベルのロール ベース 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を意識した文化を醸成することに努めています。また、当社の開発者コミュニティーは、ソフトウェア開発の実践においてシフトレフトのセキュリティを促進することを目的としたDellセキュリティ チャンピオン プログラムの一部です。

開発

デルの**セキュリティ開発ライフサイクル基準（SDL）**は、Dell Technologiesの製品組織にとって、製品およびアプリケーションのセキュリティ開発作業を市場の期待と業界慣行と照らし合わせながら評価するための共通基

準です。製品チームが新機能を開発する際に導入しなければならないセキュリティ制御が定義されています。SDLには、分析作業と、主要なリスク分野に関する規定の予防的制御の両方が含まれています。脅威のモデリング、静的コード分析、スキャン、セキュリティ テストなどの分析作業は、開発ライフサイクル全体にわたってセキュリティ上の欠陥を発見して対処することを目的としています。規定の制御は、Open Web Application Security Project（OWASP）の上位10位またはSANSの上位25位に入るものも含め、開発チームが特定の一般的なセキュリティ問題を防ぐための防御的なコードを記述できるようにすることを目的としています。セキュア コネクト ゲートウェイでは、

開発（続き）

業界標準に合わせたセキュリティ統制を実装するために、Dell SDL成熟度フレームワークが採用されています。

セキュア コネクト ゲートウェイのコードは、アジャイル開発手法を使用して開発されています。コードは、業界標準の自動化ソフトウェアを使用して継続的に統合されます。コードのバージョンは、セキュリティ グループ権限を使用してチェックインおよび管理されます。

すべてのソフトウェア リリースには、セキュリティ ポリシーに従ってセキュリティ評価が行われます。このセキュリティ評価には以下が含まれます。

- 侵入テストによる脆弱性診断
- Secureworksなどの複数のクラス最高のベンダーを使用したサードパーティー セキュリティ テスト
- 認証、承認、およびID管理ソリューションの評価
- サード パーティー製のライブラリーとコンポーネントはすべて、業界をリードするソフトウェア構成分析ソリューションを使用してスキャンされます。また、特定のセキュリティ改善事項については、Dellセキュリティ アドバイザリーが通知されます。
- デルのグローバル セキュリティ組織によるデータ分類。このプロセスでは、プライバシーとセキュリティを1つにまとめることで電子データが確実に保護されます。

また、アプリケーションには、セキュリティ監査とガバナンスも適用されます。

変更管理

Dell Technologiesの変更管理プロセスは、デルの企業変更管理委員会によって決定されたITIL Foundationのベスト プラクティスを踏襲しています。すべての変更は、変更要求チケットによって管理されます。デルのシステムにアクセスして変更を開始するユーザーは、ITILのト

レーニングを受けるだけでなく、SDLについて習熟することが必要です。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アップデートおよびアップグレードはバージョン管理されるため、適切な追跡とトレーサビリティが実現します。チームは、自動化ビルド プロセスを使用して新しいビルドを適用したり、導入されたビルドまたはホット フィックスを取り消したりできます。

お客様の構内でインストールされたアプリケーションは、お客様の裁量でアップグレードすることができます。Dell.com/supportに移行されたすべてのリリースには、既知の制限事項によって導入された変更に関する情報が含まれています。

すべての新しい機能および変更は、デルの製品管理チームによって整備され、変更管理委員会の審査と承認を受けたPOR（Plan of Record）変更プロセスを使用して優先順位が付けられます。

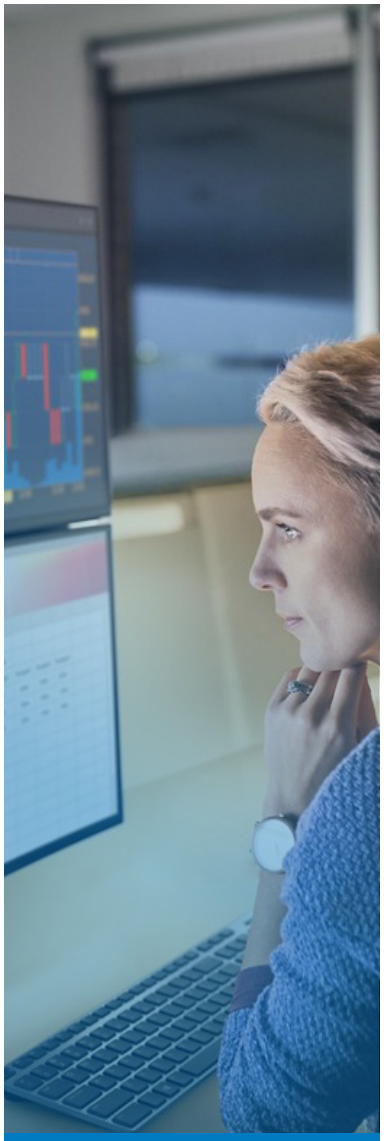
サプライ チェーンのリスク管理

Dell Technologiesは、計画-資源および調達-製造-配送-返品ライフサイクルの各段階で業界をリードするベスト プラクティスに従っています。デルは、グローバル市場において信頼できるICTサプライヤーであり続けるため、国際的なSCRM規格およびベスト プラクティスの推進を含め、サプライ チェーンの安全を保証するための包括的なアプローチを採用しています。

デルのサプライ チェーン保証慣行については、こちらをご覧ください。

インシデント レポート

デル・テクノロジーズの社員は、疑わしいアクティビティに気付いた場合や、サイバーセキュリティの問題や脅威があると考えられる場合に、直ちにPCセキュリティ インシデント対応チーム（CSIRT）にインシデントを報告する必要があります。これには、セキュリティ プ



製品セキュリティのベストプラクティスに関する業界コラボレーション

ロセスの弱点やギャップが含まれ、環境に影響を及ぼしたり、システムやデータの侵害につながったりする可能性があります。CSIRTは次に、インシデントの全面的な調査を開始し、インシデントの報告者は、CSIRTが調査を実行するために必要なすべてのアーティファクトと詳細を提供します。CSIRTチームは、CSIRTインシデント対応計画を使用します。この計画には、Dell社内のお客様に対するものではないサイバーセキュリティ インシデントに対応して解決するための正式なプロセスが詳しく説明されています。これらのインシデントは、Dellの資産、PCネットワーク、データ処理機器、およびDellとその該当する子会社、スタッフ、サービス プロバイダー、パートナー、またはお客様の情報に潜在的な脅威をもたらす可能性があります。

脆弱性への対策

デル・テクノロジーズは、脆弱性による脅威に対処するためのタイムリーな情報、ガイダンス、および緩和策をお客様に提供することにより、当社製品のセキュリティ脆弱性に関連したリスクを最小限に抑える支援に取り組んでいます。Dellの製品セキュリティ インシデント対応チーム（PSIRT）は、当社に報告されたすべての製品の脆弱性への対策および情報開示を責務としています。デル・テクノロジーズ製品の脆弱性に関するすべての開示情報は、オンラインで入手できます。

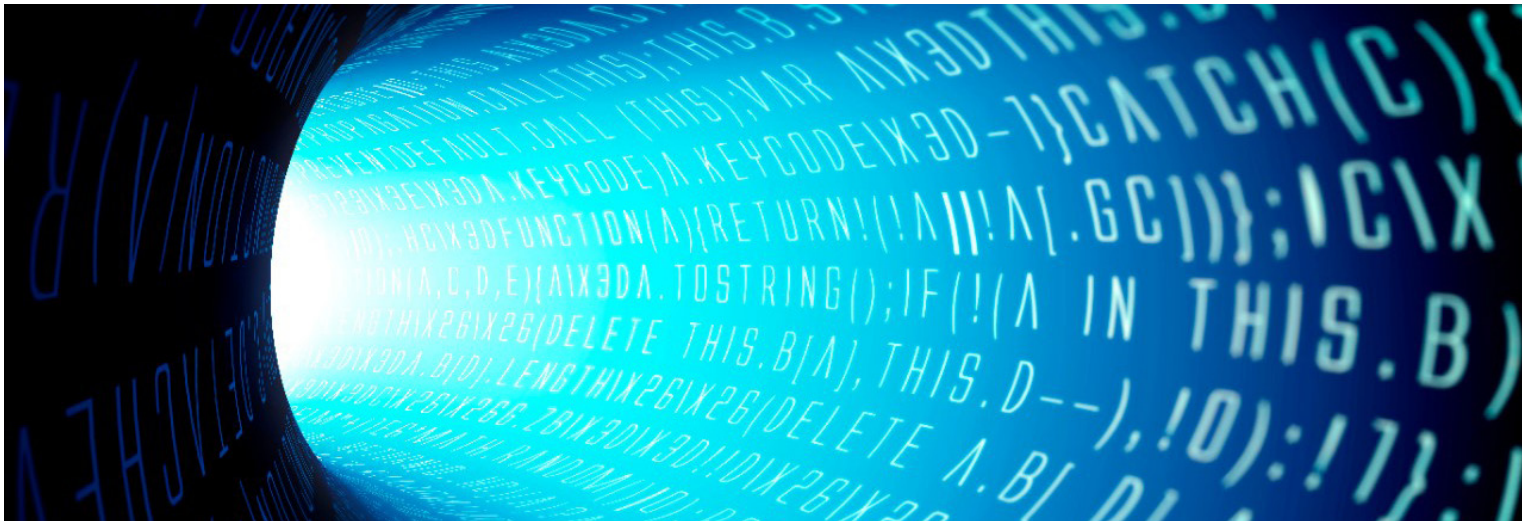
デルの脆弱性対策ポリシーを
ご覧ください

業界内での提携

Dell Technologies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、および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以下のものがあります。

- デルは、現在、子会社であるEMCと共同創設したSoftware Assurance Forum for Excellence in Code（SAFECode）取締役会の委員長を務めています。他の取締役会メンバーには、Microsoft、Adobe、SAP、Intel、Siemens、CA、およびSymantecの代表者が含まれています。SAFECodeのメンバーは、ソフトウェアの信頼性保証に関する慣行を共有して公開し、研修も行っています。
- Dell Technologiesは、Forum for Incident Response and Security Teams（FIRST）の常勤委員です。FIRSTは、権威ある機関であり、インシデントおよび脆弱性対応において世界をリードしています。
- デルは、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 サプライ チェーンのインテグリティ プログラムおよびフレームワークの策定を主導しています。
- デルは、遡ること2008年にBuilding Security In Maturity Model（BSIMM）プロジェクトで初めて評価対象となった9社のうちの1つであり、以来、このプロジェクトへの参加を続けています。Dell Technologiesの代表はBSIMM顧問委員会のメンバーです。

エンタープライズ セキュリティの質問に対する答えを見つけるのに役立つリソースとソリューションについては、セキュリティおよびトラスト センターにアクセスしてください。



- 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

デルの従業員は、セキュリティ規格の策定と業界別のセキュリティ慣行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）
- Distributed Management Task Force（DMTF）
- Forum for Incident Response and Security Teams（FIRST）
- 情報技術規格国際委員会（INCITS）
- 国際標準化機構（ISO）
- Internet Engineering Task Force（IETF）
- The Open Group
- 構造化情報標準促進協会（OASIS）
- Software Assurance Forum for Excellence in Code（SAFECode）
- Storage Networking Industry Association（SNIA）

ISO 9001認証

Dell TechnologiesはISO 9001認証を取得しています。デルは、すべての開発および製造センターに対して定期的な四半期ごとの監査とコンプライアンス審査を実施しています。

5：まとめ

デルの接続テクノロジーは、重要なデータ センター インフラストラクチャのアップタイムを最大化する主体的かつ予測型の自動化アラートにより、快適なITサポート体験を提供します。お客様は、Dell Technologies Servicesとパートナーシップを結ぶことにより、プライバシーが保証された環境で安全にテレメトリー データを収集、通信、転送、利用、および保管することができます。

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

1 出典：『The Role Of IT Services Providers Expands To Strategic Collaboration』Forrester Consultingがデル・テクノロジーズに委託されて実施した調査、2021年4月

2 出典：世界経済フォーラム グローバル リスク レポート2021。http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf