

Dell Trusted Infrastructure

モダンで安全性と対障害性に優れる
インテリジェントなテクノロジー基盤で
組織のイノベーションを促進

物理システムに、ソフトウェア定義システム、AI、マルチクラウド環境、エッジ デバイス、アズ ア サービス。現代のインフラストラクチャは、サイバーセキュリティとサイバー レジリエンスに関する私たちの認識を一変させつつあります。

私たち Dell は、IT のセキュリティとレジリエンスの中核に次の 3 つの柱を据える必要があると考えています。

- 攻撃対象領域の縮小
- サイバー脅威の検出と対処
- サイバー攻撃からの復旧

これらに加えてゼロトラスト原則を活用することで、サイバー セキュリティとサイバー レジリエンスの体制を強化できます。

現代のインフラストラクチャ

世界は今や、データ主導の時代です。ビジネスのあらゆる場面で IT が活躍し、あらゆる場所でデータが生まれ、利用されています。一元化されたモノリシックなデータセンターは過去の話です。今日の「インフラストラクチャ」という言葉には、物理的に分散しているか、アズ ア サービスとして提供される、データストレージ、ハイパーコンバージドシステム、サーバー、ネットワーキング、データ保護が含まれます。私たち Dell は、IT インフラストラクチャはその用途を問わず、お客様やパートナーの信頼を得るものでなければならないと考えています。

信頼を得るインフラストラクチャとは、どこにあってもセキュリティが脅かされることなく、最大限の柔軟性とビジネス俊敏性をもって稼働するインフラストラクチャです。モダンで耐障害性と柔軟性に優れ、ゼロトラストなど、最も重要なデジタル資産を保護し維持するために企業が採用する、各種セキュリティ方式をサポートします。



モダン

モダン インフラストラクチャはイノベーションを追求します。高度な分散型、またはアズ ア サービスの形で提供され、モダンな組織運営を可能にするエッジ デバイスやマルチクラウド環境を含みます。



耐障害性

耐障害性を高めるには、安全なライフサイクルでソリューションを開発する必要があります。安全なサプライチェーンは、コンポーネント、システム、完全統合型のソリューションに至るまで、環境内のあらゆるデバイスの信頼性を確保します。



インテリジェント

インテリジェントなインフラストラクチャには、AI、機械学習、自動化などの高度な機能が組み込まれており、一貫したガバナンスと適用によってセキュリティ体制を拡張できます。



Dell Trusted Infrastructure

Dell Trusted Infrastructure は、安全性と耐障害性をハードウェアとソフトウェアの両面で追求した IT ソリューションおよびサービス群です。信頼性、制御性、拡張性の向上を目的として設計および構築されています。



Protect
データとシステム



**強調
強化**



**セキュリティの複雑さを
克服**



DELLTechnologies

データとシステムの保護

組織の重要なシステム、アプリケーション、データが、エッジやオンプレミスにある場合でも、複数のクラウドプロバイダーにまたがっている場合でも、これらすべてに対するサイバー脅威には 1 つのプロバイダーで対処できます。Dell Trusted Infrastructure は、ストレージ、サーバー、ハイパーコンバージド、ネットワーキング、データ保護といったエンタープライズ向けソリューションの全ラインにセキュリティ機能を組み込むことで、ゼロトラスト原則の実装を支援します。

システムへの安全なアクセスを確保するため、脅威を検出して無効化します。堅牢なデバイスとプロセスで構成される Dell のソリューションは、データやアプリケーションが存在するあらゆる場所でイントリンシック（内在的）なセキュリティ上の優位性を確保します。

エッジからコア、クラウドに至るすべてを保護するため、革新的なソリューションとベストプラクティスを用いてリスクに対処します。インテリジェントなソフトウェア、AI、機械学習を活用して、データ、ネットワーク、システムを守ります。

確信を持って IT インフラストラクチャを運用できるよう、静止時、稼働時、移動時のデータの安全性を確保します。広範囲をカバーするセキュリティを実装して重要なデータ、アプリケーション、運用の整合性と可用性を確保します。

サイバー レジリエンスの強化

サイバー攻撃の影響を軽減し、迅速かつ確実に業務を再開できるようにするには、復旧の計画、準備、演習が必要です。自動化されたワークフローとソフトウェアデファインド ソリューションを提供する Dell Trusted Infrastructure は、環境の分散化に合わせて重要なシステム、アプリケーション、データを保護できます。

データ、システム、運用のサイバー攻撃耐性を高めます。適切な IRR 計画があれば、インシデントが発生しても適切な支援を受けて復旧できます。

運用の継続性とデータの可視性を維持するために MDR 機能を使用し、サイバー インシデント発生時にはインシデント対応と復旧にビジネス プロセスを合わせられるようにします。

コンプライアンスを確立してゼロトラスト原則に従うため、最新のテクノロジーを適用して、高度に分散したテレワークやマルチクラウドの環境内におけるアクセス、認証、承認を強化します。



セキュリティの複雑さの解消

セキュリティ運用をモダナイズすると、複雑化が進んでも、自信を持ってゼロトラストアーキテクチャの構築や拡張を行うことができます。Dell Trusted Infrastructure は、自動化、オーケストレーション、インテリジェントなイノベーションを通してハードウェア、ファームウェアベース、ソフトウェアのセキュリティ機能を補完します。

インフラストラクチャを合理化するため、セキュリティ関連のアプリケーションとベンダーの数を減らします。デル・テクノロジーズはエンタープライズ規模のソリューションプロバイダーとして、お客様の環境におけるセキュリティ機能の統合をエンドツーエンドのソリューションで支援します。お客様にとっては、自社の課題を熟知するパートナー1社と信頼関係を構築し、安心して任せられるというメリットがあります。

自社のセキュリティ担当を増やしたかのように、専門的なリソースとサービスを利用できます。Dell のセキュリティエキスパートと協力してサイバーセキュリティサービスやアズアサービスを利用することで、人的リソースを拡大し、コストを運用コストに転換できます。

既存のセキュリティシステムを強化してセキュリティ戦略をすばやく拡大できます。人の手作業の代わりに自動化とインテリジェンスを活用できます。



IT インフラストラクチャ全体にわたって信頼できる最新のセキュリティをプロバイダー 1 社が提供

Dell Storage 保護された安全なデータをいつでも利用できるという安心感をいただけます。	安全なストレージ ソリューションを確保すると同時に、脅威を包括的に検出し対応することは可能でしょうか？はい。当社のソリューションは、脅威インテリジェンスを集約し、アップストリーム セキュリティ プラットフォームにカスケードすることで、セキュリティの複雑さを解消します。
Dell サーバー セキュリティ制御、機能、ソリューションが進化するサイバーレジリエント アーキテクチャで、現代の脅威ランドスケープに対処します。	組み込み型セキュリティを用い、製品ライフサイクルの全段階においてサイバーレジリエンスを強化します。シリコン ルート オブ トラストをアンカーとして、署名されたファームウェア、ドリフト検出、BIOS リカバリー、システム管理統合、サプライチェーン保証を制御します。
Dell Networking ハードウェアとソフトウェア内の複数の防御レイヤーで、エッジとネットワークのセキュリティを強化します。	今日のダイナミックなビジネス環境において信頼と制御を維持するには、包括的で適応性のあるセキュリティ戦略が鍵となります。高度なアーキテクチャ、厳格なセキュリティ認可、堅牢なアクセス プロトコル、シームレスな統合を組み合わせるというアプローチで、ネットワークのパフォーマンスを最大化しながらセキュリティを確保します。
Dell ハイパーコンバージド インフラストラクチャ サプライチェーンから、ハードウェア インフラストラクチャ、ソフトウェア開発、ライフサイクル管理ソフトウェアに至るまで、スタックのあらゆるレイヤーでアプリケーションを強化し、変更します。	ハイパーコンバージド インフラストラクチャ ソリューションは、どれも同じではありません。Dell のソリューションは、フル スタック統合の包括的なライフサイクル管理を備える俊敏なインフラストラクチャで、運用効率を高めてリスクを軽減します。これが、Dell が 20 四半期連続で HCI のリーディングカンパニー ¹ となっている理由です。チームは最新の脅威への対応に追われることなく、ビジネスに集中できます。
Dell Data Protection インフラストラクチャと IT のニーズに最適なソリューションで、コア、エッジ、マルチクラウド環境全体のデータを保護します。	業界で実績のあるインテリジェントな最新のデータ保護機能が、大規模な運用の簡素化と自動化を実現します。統合された一連の製品、サービス、管理ツールをフル活用できるため、重要なデータの分離、疑わしいアクティビティの特定のほか、自動データリカバリーの時間を短縮できます。Dell Data Protection があれば、通常業務を迅速に再開できます。
Dell APEX AIOps サイバーセキュリティ評価と迅速な修復を通して、インフラストラクチャを安全に保ちます。	インフラストラクチャの正常性、容量、パフォーマンスを管理するアプリケーションの中から、セキュリティ通知に適切に対応できます。モニタリングと予測分析により、人と機械のインテリジェンスが融合。IT インフラストラクチャをビジネス ニーズに適応させるためのインサイトが得られます。
Dell Professional Services 自動化および最適化された統合的な体験を通じて、セキュリティの運用を簡単に行えます。	組織がより包括的なアプローチでサイバーセキュリティに対応できる方法について説明します。強固な環境を作るには、サイバーレジリエンスを実現する IT ソリューションが必要です。データとシステムを保護し、サイバーレジリエンスを強化し、セキュリティの複雑さを克服しましょう。デル・テクノロジーズが提供する最新のエンドツーエンド ソリューションなら、セキュリティ課題の対処に必要な信頼性、制御性、拡張性を確保できます。

¹ IDC Worldwide Quarterly Converged Systems Tracker, 2022 年第 1 四半期

モダンで耐障害性に優れるインテリジェントなインフラストラクチャ ソリューションとサービス

どれが欠けても、セキュリティリスクが生じます。



デル・テクノロジーズは、この現代において安全なテクノロジーはこれまでになく重要になっていると考えています。

企業は、グローバル IT 環境のデータセンターを構成するサーバー 1 台、チップ 1 個に至るまで、あらゆる要素が安全に保護されている状況を確認しながら、ビジネスに集中しなければなりません。Dell の設計すべてにセキュリティが組み込まれているのは、そのためです。

当社は数十年にわたり、[安全なサプライチェーン](#)から[安全な開発ライフサイクル](#)まで、あらゆるものを再定義してきました。お客様が自社環境で Dell の製品やサービスを安心して利用できるよう、設計、調達、製造、出荷、管理の方法に細心の注意を払っています。

Dell Trusted Infrastructure

サイバー脅威が消えることはありません。けれども、セキュリティを確保しながらITトランスフォーメーションの取り組みを進めることはできます。

[詳細はこちら](#)

