DELL Technologies

ゼロトラスト
サイバーセキュリティ強化への道

テクノロジーとセキュリティに精通した経験豊富なパートナー
とともに、ゼロトラストの取り組みを進めましょう。

高度なサイバーセキュリティ対策に先んじている組織では実践的なロードマップを構築しています。どのように攻撃の対象となる領域を狭め、サイバー脅威を検出して対処するのか、またサイバー攻撃を受けた場合の復旧など、明確な対策を策定し、すべてをゼロトラストに対応させています。

Dellはますます巧妙化するサイバー脅威に対処するため、自社のソリューションに組み込まれたセキュリティ機能を活用し、パートナーと協力して、お客様がビジネス目標に沿ったゼロトラストを達成できるよう支援しています。

ゼロトラストとは

ネットワークを城だと想像してみてください。跳ね橋が下ろされ、いったん入城すれば、その中を自由に歩き回ることができてしまいます。今こそ、境界線で囲む防御セキュリティ モデルから、より安全性の高い最新のゼロトラスト フレームワークにアップデートを行うときです。

ゼロトラストとは、製品として購入するものではなく、セキュリティに対する構造的なアプローチです。いかなる人も物も決して信頼せず、リソースへのアクセス権を付与する前にビジネス上の正当な用途であることを常に検証します。
つまり、許可されたネットワークに接続している場合でも、以前に検証済みである場合でも、ユーザーやデバイスをデフォルトでは信頼しないということです。

決して信頼せず、常に検証

セキュアなITエコシステムの基本です。

米国国立標準技術研究所(NIST)が定義されているゼロトラスト フレームワークは、米国国防総省(DoD)で採用され、アーキテクチャに組み込まれています。

相互に関連する7つの柱から成り、すべてのセキュリティ領域においてデル・テクノロジーズの指針となります。7つの柱を組み合わせることで多面的かつ統合的なアーキテクチャを構成することができます。この包括的なセキュリティ アプローチで組織のデータとインフラストラクチャを保護します。

ゼロトラストの採用は、多岐にわたるセキュリティ機能を統合し、多くのセキュリティプロバイダーから提供される多様なオプションから適切な選択肢を選ぶという複雑な作業を伴うため、その実現は非常に難易度の高いものになります。

NIST

U.S. Department of Defense

DELL Technologies

ゼロトラストの採用を実現する

お客様の取り組みがどの段階にあっても、Dellのソリューションでサポートします。

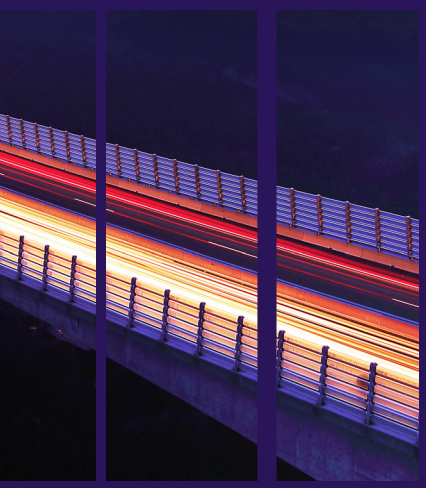
デル・テクノロジーズは、組織に選択肢と柔軟性をもたらします。高度なサイバーセキュリティ対策を目指すお客様のために、ゼロトラストの各種機能を備えたセキュリティ ソリューションを取り揃えています。悪意のあるサイバー活動に対する強化、検出、防御、復旧の能力を高めることができます。

ゼロトラストの原則を推進

さまざまな選択肢と柔軟性で高度なサイバーセキュリティ対策を実現します。

デル・テクノロジーズはセキュリティ ソリューションとゼロトラスト機能を取り揃えています。悪意のあるサイバー活動に対する強化、検出、防御、復旧の能力を高めることができます。どのようにして：

- 組み込み型の保護で自動化、脅威インテリジェンス、認証、可視性などを強化
- ゼロトラストを支えるサービスを活用することで、ロードマップを作成し、主要なテクノロジーを統合し、プロアクティブに管理
- プロフェッショナル サービス、マネージド サービス、セキュリティ アドバイザリー サービス
- 幅広いパートナー エコシステム



ゼロトラストの採用を飛躍的に簡略化

すべてを備えた完全統合型のアーキテクチャを導入できます。

ゼロトラストは、セキュリティに対する構造的なアプローチであり、単一の製品ではありません。複数のソリューション間の調整を慎重に計画する必要があります。Dellは、ゼロトラストにおけるこの統合の負担を取り除きます。どのようにして：

- Dellは、他に類を見ない完全統合型のゼロトラスト アーキテクチャを構築しています。米国国防総省により設計、テスト、検証が行われたアーキテクチャです。

DELL Technologies

ゼロトラストの原則を推進

お客様固有のセキュリティ エコシステムを基盤にしてゼロトラストを達成します。

Dellは、ゼロトラスト戦略を活用した高度なサイバーセキュリティ対策の推進を支援します。攻撃対象領域の縮小、サイバー脅威の検出強化、攻撃後の復旧時間の短縮を可能します。

ゼロトラストの柱それぞれに、重要な領域に沿ったテクノロジー、プロセス、人材が描写されています。重要な領域とは、組織を保護するためにセキュリティ ポリシーとビジネス ポリシーが必要となる場所です。Dellのセキュリティ サービスは、次のような点で役立ちます。

- セキュリティ レベルの評価、ゼロトラストの評価、リスク アセスメント
- 戦略とロードマップの策定
- 重要となるゼロトラスト機能のマネージド サービス

DELL Technologies

ゼロトラストの基盤

当社が提供する高度な組み込み型セキュリティ ソリューションで、ゼロトラストの採用を優位に進めることができます。

Dellのデータ保護

Cyber Recoveryヴォールト | PowerProtect Data Manager | CyberSense Transparent Snapshot | CloudIQ | システムロックダウン | 逸脱の検出 | セキュアなエンタープライズ キー管理 | TLS 1.3 | IPv6 | 多要素認証 | シングル サインオン | ロール ベースのアクセス | CloudIQ

Dell PowerEdgeサーバー

ソフトウェア部品表 | セキュア コンポーネント検証 | シリコン ルート オブ トラスト | システムロックダウン | 逸脱の検出 | セキュアなエンタープライズ キー管理 | TLS 1.3 | IPv6 | 多要素認証 | シングル サインオン | ロール ベースのアクセス | Cloud IQ

Dellストレージ プラットフォーム

データ分離 | データ不変性 | 脅威検出 | アクセス制御認証 | データ暗号化 | STIG強化 | HWルート オブ トラスト | セキュア ブート | デジタル署名されたファームウェア | ロール ベースのアクセス | セキュアなスナップショット

Dell HCI/CI

ハードウェア ルート オブ トラスト | セキュア ブート チェーン オブ トラスト | デジタル署名されたアップデート | キー管理 | 安全なログ記録 | 分散仮想スイッチ | VMの分離 | 認証と承認 | エコシステムのコネクター | 継続的に検証されている状態 | ソフトウェア コードの整合性 | 電子的互換性マトリックス

Dellビジネス向けPC

BIOS/ファームウェアのセキュリティ | ハードウェア セキュリティ | サプライ チェーン保証 | 脅威管理ソフトウェア（EDR、XDR、VDR） | ネットワークとクラウドのデータ保護ソフトウェア

Dellのエッジ ソリューション

HW/SW/VMの構成証明 | セキュアなオンボーディング | チェーン オブ トラスト | セキュアなOS/アプリケーションのデリバリー | データ権利の管理

Dellのネットワーク スイッチ

SmartFabric | CloudIQ | SD-WAN | VLANセグメンテーション | Enterprise SONiC | アクセス制御リスト | RADIUS | TACACS+ | 暗号技術 | スイッチ強化 | マイクロセグメンテーション | 仮想ルーティングと転送

時間を短縮するアプローチ

Project Fort Zeroで迅速かつ徹底的、包括的にゼロトラストを組織全体に採り入れます。

Project Fort Zeroなら、検証済みのメソッドでゼロトラストによる高度なセキュリティ対策を短時間で達成できます。導入時間を短縮、業務の中断を減らしてコストを抑えることができます。

当社の専門技術と業界内のネットワークを基に、デル・テクノロジーズは米国国防総省よりゼロトラストの採用時間の短縮に関する支援要請を受けました。民間部門や公共部門の組織によるシンプルなゼロトラスト アーキテクチャの採用とグローバルな拡張を可能にするため、Dellはエコシステムを構築し、30社を超える大手テクノロジー企業やセキュリティ企業の統合を主導しています。当社は世界中の民間企業と公共機関の双方に対応するゼロトラスト アーキテクチャの開発とグローバルな拡張に率先して取り組んでいるのです。これは、米国国防総省がゼロトラスト達成に向けて掲げる目標に対して、Dellが取り組んでいる証しです。

オンプレミス

データ セキュリティとコンプライアンスの重要性が高い組織のデータセンター。

リモートまたは地域的

顧客データを安全かつリアルタイムに分析することで競争優位性を得られる小売店などのロケーション。

取り外しが可能なエッジ

一時的な実装が運用を継続する上で必要となる場所、航空機や車両などの断続的な接続が発生する場所。

DELL Technologies

当社は、お客様の迅速なゼロトラスト採用を支援するため、米国国防総省が定めた高度なゼロトラスト達成のためのアクティビティ152種をすべて導入する予定です。

実行を可能にする要素

方針 | 組織 | 研修 | 資料 | リーダーシップと教育 | スタッフ | 設備 | ポリシー

ゼロトラストの目標レベル

ユーザーの信頼性

- ユーザー インベントリー
- アプリケーション ベースの許可
- ルール ベースの動的アクセス パート1
- 組織における MFA/IDP
- システムの実装と特権ユーザーの権限縮小 パート1
- 組織のIDライフサイクル管理
- デフォルト ポリシーでのユーザーの拒否
- 単一認証
- システムの実装と特権ユーザーの権限縮小 パート2
- エンタープライズのIDライフサイクル管理パート1
- UEBAツールの実装
- 定期的な認証
- エンタープライズの公開鍵基盤/IDPパート1

デバイスの信頼性

- デバイスのヘルプ ツールのギャップ分析
- 次世代型AVツールのC2Cとの統合
- NPE/公開鍵基盤の被管理デバイス
- デフォルト ポリシーでのデバイスの拒否
- UEDMまたは同等のツールの実装
- エンタープライズのデバイス管理パート1
- EDRツールの実装とC2Cとの統合
- 資産、脆弱性、パッチを管理するツールの実装
- エンタープライズのIDP パート1
- C2C/コンプライアンス ベースのネットワーク認証の実装パート1
- アプリケーション制御とFIMのツールの実装
- 管理された制限付きBYODとIoTのサポート
- エンタープライズのデバイス管理パート2
- XDRツールの実装とC2Cとの統合 パート1

アプリケーションとワークロード

- アプリケーション/コードの識別
- リソースの承認パート1
- DevSecOpsソフトウェア ファクトリーの構築パート1
- 承認されたバイナリ/コード
- 脆弱性管理プログラム パート1
- SDCリソースの承認パート1
- リソースの承認パート2
- DevSecOpsソフトウェア ファクトリーの構築パート2
- アプリケーションのセキュリティとコード修復の自動化パート1
- 脆弱性管理プログラム パート2
- 継続的な検証
- SDCリソースの承認パート2

データの信頼性

- データ分析
- DLP適用ポイントのロギングと分析
- DRM適用ポイントのロギングと分析
- データ タグ付け基準の定義
- データのタグ付けと分類のためのツールの実装
- ファイル アクティビティのモニタリング パート1
- DRMツールと保護ツールの実装パート1
- 適用ポイントの実装
- 相互運用性基準
- SDSポリシーの開発
- 手動でのデータ タグ付けパート1
- ファイル アクティビティのモニタリング パート2
- DRMツールと保護ツールの実装パート2
- データのタグと分析によるDLP適用パート1
- DAASアクセスのSDSポリシーとの統合パート1
- データのタグと分析によるDRM適用パート1
- SDSソリューションおよびポリシーのエンタープライズIDPとの統合パート1

ネットワークと環境

- きめ細かい制御アクセスのルールとポリシーの定義パート1
- SDN APIの定義
- きめ細かい制御アクセスのルールとポリシーの定義パート2
- SDNのプログラム可能なインフラストラクチャの実装
- データセンターのマクロ セグメンテーション
- マイクロ セグメンテーションの実装
- 制御管理プレーンとデータ プレーンへのフローの区分化
- B/C/P/Sのマクロ セグメンテーション
- アプリケーションとデバイスのマイクロ セグメンテーション
- 転送中のデータの保護

自動化とオーケストレーション

- ポリシーのインベントリーと開発
- タスク自動化分析
- 対応自動化分析
- ツールのコンプライアンス分析
- 組織のアクセス プロファイル
- SOARツールの実装
- 標準化されたAPI呼び出しとスキーマ パート1
- ワークフローのエンリッチ化パート1
- エンタープライズのセキュリティ プロファイル パート1
- エンタープライズの統合とワークフロー プロビジョニング パート1
- データのタグ付けと分類のためのMLツールの実装
- 標準化されたAPI呼び出しとスキーマ パート2
- ワークフローのエンリッチ化パート2

可視性と分析

- スケールに関する考慮事項
- ログ解析
- 資産IDとアラートの相関関係
- 脅威アラート パート1
- 分析ツールの実装
- サイバー脅威インテリジェンス プログラム パート1
- ログの分析
- 脅威アラート パート2
- ユーザー/デバイスのベースライン
- ユーザーのベースライン行動の確立
- ベースラインとプロファイリング パート1
- サイバー脅威インテリジェンス プログラム パート2

目標のアクティビティの総数： 91

出典：米国国防総省のゼロトラスト戦略、2022年11月7日公開

DELL Technologies

高度なゼロトラスト

ユーザーの信頼性

- ルール ベースの動的アクセス パート2
- エンタープライズの役割と許可パート1
- 代替の柔軟なMFAパート1
- リアルタイムの承認とJIT/JEA分析パート1
- エンタープライズのIDライフサイクル管理パート2
- ユーザー アクティビティのモニタリング パート1
- 継続的認証パート1
- 継続的認証パート2
- エンタープライズの公開鍵基盤/IDPパート3
- エンタープライズの役割と許可パート2
- 代替の柔軟なMFAパート2
- リアルタイムの承認とJIT/JEA分析パート2
- エンタープライズのIDライフサイクル管理パート3
- ユーザー アクティビティのモニタリング パート2
- エンタープライズの公開鍵基盤/IDPパート2

デバイスの信頼性

- エンタープライズのIDP パート2
- C2C/コンプライアンス ベースのネットワーク認証の実装パート2
- エンティティ アクティビティのモニタリング パート1
- デバイス セキュリティ スラックのC2Cとの完全な統合
- エンタープライズの公開鍵基盤パート1
- 管理された完全なBYODとIoTのサポート パート1
- XDRツールの実装とC2Cとの統合パート2
- エンティティ アクティビティのモニタリング パート2
- エンタープライズの公開鍵基盤パート2
- 管理された完全なBYODとIoTのサポート パート2

アプリケーションとワークロード

- リソースの承認を行うための属性のエンリッチ化パート1
- リソースの承認を行うための属性のエンリッチ化パート2
- 継続的な運用許可(ATO)パート1
- アプリケーションのセキュリティとコード修復の自動化パート2
- REST APIのマイクロセグメント
- 継続的な運用許可(ATO)パート2

データの信頼性

- 手動でのデータ タグ付けパート2
- データベース アクティビティのモニタリング
- データのタグ付けとサポートの自動化パート1
- データのタグと分析によるDRM適用パート2
- データのタグと分析によるDLP適用パート2
- DAASアクセスのSDSポリシーとの統合パート2
- SDSソリューションおよびポリシーのエンタープライズIDPとの統合 パート2
- SOSツールの統合および/またはDRMツールとの統合パート1
- データのタグ付けとサポートの自動化パート2
- データ アクティビティの包括的なモニタリング
- データのタグと分析によるDRM適用パート3
- データのタグと分析によるDLP適用パート3
- DAASアクセスのSDSポリシーとの統合パート3
- SDSツールの統合および/またはDRMツールとの統合パート2

ネットワークと環境

- ネットワーク資産の検出と最適化
- リアルタイムのアクセス決定
- プロセスのマイクロ セグメンテーション

自動化とオーケストレーション

- エンタープライズのセキュリティ プロファイル パート2
- エンタープライズの統合とワークフロー プロビジョニング パート2
- AI自動化ツールの実装
- ワークフローのエンリッチ化パート3
- 分析に基づくAI駆動型のA&O変更の決定
- プレイブックの実装
- ワークフローの自動化

可視性と分析

- 脅威アラート パート3
- ベースラインとプロファイリング パート2
- UEBAのベースラインのサポート パート1
- UEBAのベースラインのサポート パート2
- AI対応のネットワーク アクセス
- AI対応の動的アクセス制御

高度なアクティビティの総数： 61

デル・テクノロジーズは、ゼロトラストの成熟度を迅速に達成するための複雑なプロセスをシンプルにできます。

出典：米国国防総省のゼロトラスト戦略、2022年11月7日公開

DELL Technologies

すべての組織のニーズに対応

ゼロトラストの成熟度を高めましょう。

ゼロトラストは、定義済みのフレームワークであり、セキュリティに対するアプローチの指針となる原則を集めたものです。さまざまな機能を使用することで実装できます。お客様がゼロトラストに全力で取り組んでいる場合でも、ターゲットを絞った改善に重点を置いている場合でも、Dellはゼロトラストの原則に沿って、経験豊富なセキュリティ パートナーとして、セキュリティ向上の取り組みを支援します。

化学	情報技術	通信	救急サービス
食品/農業	防衛	医療/公衆衛生	製造
金融	原子炉	商業	行政機関
エネルギー	輸送	上下水道	ダム

DELL Technologies

DELL Technologies

テクノロジーとセキュリティの経験豊富なパートナーとして、ゼロトラストに向けた組織の取り組みを支援します。

ゼロトラストを実装して、長期的にサイバーセキュリティを強化しましょう。

Dellが提供するセキュリティ サービス

セキュリティの成熟度と全体的なリスクに関する専門家による評価。

ゼロトラスト ロードマップの作成。

セキュリティ アクティビティの継続的な管理。

DELL Technologies

Dell.com/SecuritySolutions

コールバックのお申し込みはこちらから

セキュリティ アドバイザーとのチャットはこちらから

お電話は1-800-433-2393まで