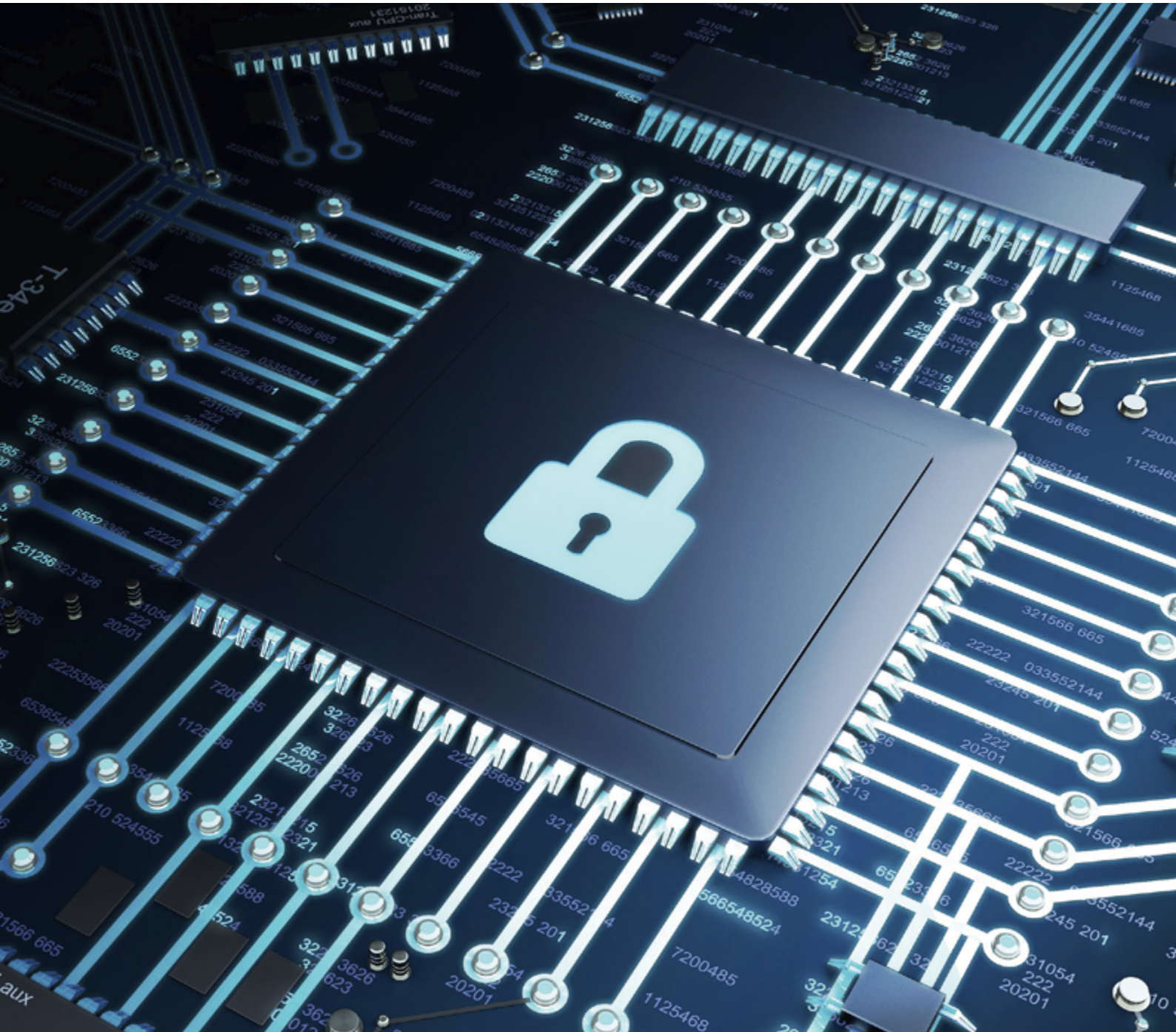
DELL Technologies

Microsoft

ホワイトペーパー

エンドツーエンドでデータ セキュリティを強化：Microsoft SQL Server、Dell™ PowerEdge™ サーバー、Windows Server 2022



さまざまな業界でリモートワークへの移行が広がるなか、企業はニューノーマルへ適応しつつ、セキュリティの優先順位をより一層高めています。2021 年の調査では多くのビジネス リーダーが「リモートワークは当分の間続くだろう」と回答しました。[1] 従業員の働く場所や地域がかつてないほど多様化し、また攻撃を受けやすいエンドポイントも増加しているため、企業の IT 管理者はこれまで以上に包括的なセキュリティ強化策をとる必要があります。

88% の IT リーダーが「リモートワークは何らかの形で継続すると予想し、コンテンツ リポジトリの複数利用は短期的に問題が残りそうだ」と回答しています。[1]

企業全体でデータ セキュリティを強化するには「ホール スタック（全階層）」アプローチ、すなわちハードウェアからデータベース アプリケーション、オペレーティング システムまでの包括的な対策が有効です。Dell™ PowerEdge™ サーバーと Windows Server 2022 上に最新版の Microsoft SQL Server を導入してインフラをモダナイズし、データを統合することで、企業は、働く場所の多様化に左右されない、データをエンドツーエンドで保護できる強力な基盤を構築できます。

企業が直面している現在のセキュリティ課題

リモートワークの増加によって、企業のサイバー攻撃に対する脆弱性はさらに深刻化しています。

- **コンテンツのスプロール化。** 多くの従業員が四六時中、企業のデータやアプリケーションにアクセス、使用する状態が何年も続けば、コンテンツのスプロール化が生じるのは当然のことです。データはさまざまな場所、複数のリポジトリに保存され、しかも増え続けています。IDC は、今後 5 年間でデータが年平均成長率（CAGR）24%のペースで増加すると予測しています。[2]また、調査では半数以上 (52%) の IT リーダーが「社内にファイルを保存するリポジトリが 10 個以上存在する」と回答しています。[1] 家に物が多ければ雑然として紛失の可能性が高まるのと同様に、複数のサーバーやデータベースにコンテンツが保存・複製されれば、データがリスクにさらされる可能性が高まります。

41%の IT リーダーが「コンテンツのスプロール化に対す最大の懸念事項は、データ侵害や漏えいリスクの増大である」と回答しています。[1]

- **BYOD (Bring Your Own Device) とシャドー IT。** コンテンツのスプロール化で高まったセキュリティ リスクは、BYOD ポリシー (私物のスマートフォンやタブレットの業務利用を企業が許可すること) でさらに深刻化します。私物のデバイスは最新のセキュリティ パッチによるアップデートが定期的に実施されていなかったり、安全ではない Wi-Fi ネットワークで使用されたりする危険性があります。またクラウドベース アプリの自称セキュリティ機能へ依存する「シャドー IT」は、組織の内部統制や可視化の欠如につながり、ハッカーにとって新たな攻撃ベクトルとなる可能性があります。
- **セキュリティ パッチごとのスケジュール調整が困難。** 多くの企業が SQL Server をデータ プラットフォームとして使用していますが、時間の経過とともにデータベース ソフトウェアのバージョンが更新され、データの管理やセキュリティ パッチの適用が複雑になります。また、パッチの適用でシステムが遅くなったり、サーバー停止が必要となったりすることから、IT チームはバージョンごとに最適なパッチ適用の時間帯を決める必要があり、結果的にアップデートが遅くなりがちです。
- **従業員ごとに適切なアクセス権限の設定が必要。** IT 管理者は、従業員の入退社に合わせて常に権限設定を管理しなければなりません。権限を適切かつタイムリーに設定・更新しなければ、組織内の誰かが誤ってあるいは故意に会社や顧客のデータをランサムウェアやハッカーにさらす可能性があります。

セキュアな基盤でデータ管理をモダナイズする

Dell PowerEdge サーバーと Windows Server 2022上でSQL Serverを稼働させると、こうした課題を克服できます。最新のインフラストラクチャによってビジネス クリティカルなワークロードのセキュリティを、ハードウェア、オペレーティング システム (OS) 、ソフトウェアのすべてのレベルで保護します。

> 65%の CIO や IT リーダーが「機密情報を含むファイルや文書が従業員の私物デバイスに保存されていると考えています。[1]

Dell PowerEdge サーバー

Dell PowerEdge サーバーは、セキュリティ対策が組み込まれたインフラストラクチャを実現することで、企業が内在的リスクを防御しながら、現代のあらゆるワークロードや目的に対応できるようサポートします。PowerEdge サーバーは、データベース アプリケーション、ハイパフォーマンス コンピューティング(HPC)、仮想化環境、エッジ コンピューティングなどデプロイの迅速化とパフォーマンスの向上を目的に設計されています。また、Dell™ OpenManage™ ツールを使うことで、IT 管理者は大規模クラスタの簡単かつ効果的な管理が可能になります。

PowerEdge サーバーは改ざん不可能なシリコンベースのルート オブ トラスト (信頼の基点) に基づいて構築されており、ブート検証などエンドツーエンドのセキュリティ機能、具体的には UEFI のセキュア ブートのカスタマイズ、高信頼性の BIOS、ファームウェアのチェーン オブ トラスト、検証された OS ブートローダーなどが搭載されています。ファームウェアには NIST (米国立標準技術研究所) のガイドラインに準拠した保護対策(署名付きファームウェア アップデートなど)を講じており、自動更新によるシンプルな証明書管理も実現しています。

PowerEdge サーバーでは、Secure Enterprise Key Manager (SEKM) を使用して保存データを保護し、CPU のコンフィデンシャル コンピューティング テクノロジーによって使用中のデータを保護します。サプライ チェーンのセキュリティ対策として、偽造コンポーネント、マルウェア、ファームウェアの改ざんなどの脅威を軽減するため、デル・テクノロジーズでは偽造防止、製造過程の管理、コード署名、シャーシ侵入検知の各ツールや改ざんを検出可能なパッケージなどを組み合わせて包括的なアプローチを導入しています。さらに、Secured Component Verification (SCV) でサーバー コンポーネントの完全性を検証することによってサプライ チェーン保証を強化しています。

デル・テクノロジーズは Microsoft の主要パートナーの1社として40年近く Microsoft と緊密に連携しながら、セキュリティ組み込みのハードウェアやソフトウェア ソリューションの開発で業界をリードしてきました。この協業により、Windows Server や SQL Server といった Microsoft のソフトウェアは Dell PowerEdge サーバー上で最適に稼働します。

Windows Server 2022

Windows Server 2022 は Windows ベースの Secured-core Server を特長とし、ハードウェア、ファームウェア、OS の機能を利用して現在および将来の脅威を防御します。Secured-core Server は、DRTM (Dynamic Root of Trust for Measurement) によるプロセッサ サポート テクノロジーを使用してファームウェアを分離するので、いかなる侵害でもファームウェアのコードに影響が及ぶ可能性は低くなります。さらに、仮想化ベースのセキュリティ (VBS) によってカーネルなどOSの重要な部分をシステムの他の部分から分離してアプリケーションとデータを保護し、サーバーが重要なワークロードの実行に専念できるようにします。

この Secured-core 機能は、攻撃者がシステムの脆弱性を利用するのに使う経路の多くをプロアクティブに防御したり、破壊したりする際に効果を発揮します。他にも Microsoft の複数のセキュリティ技術、たとえばVBSのハイパーバイザーで保護されたコード整合性、Trusted Platform Module (TPM) 2.0、BitLockerドライブ暗号化、UEFIセキュア ブートなどが Secured-core Server に標準採用、またはサポートされています。

ホワイトペーパーをご覧ください「Windows Server 2022 と次世代 Dell EMC™ PowerEdge™ サーバーの機能を組み合わせることで、高度なセキュリティ保護を実現」

データベース アプリケーション レベルでデータを保護する

SQL Server はセキュリティを考慮して実装されています。しかし前述のとおり、多くの企業は複数バージョンの SQL Server を運用しており、IT 部門はよりシンプルで統合されたデータベース戦略を模索しています。

また、SQL Server 2012 の延長サポートは 2022 年 7 月に終了しているため、最新バージョンの SQL Server にデータベースを統合することがこれまで以上に緊急の課題となっています。旧バージョンの SQL Server データベースは今後も稼働はしますが、問題が発生した場合、Microsoft のサポートによる修正プログラムは利用できません。また、パッチやセキュリティ アップデートも提供されないため、システムは悪意のある攻撃に対して脆弱な状態のままとなる可能性があります。

多くの企業にとってデータベース統合の最も容易で現実的な方法は、最新バージョンの SQL Server にアップグレードし、旧バージョンを互換モードで運用することです。データベース管理者はレガシー SQL Server のデータベースをバックアップし、その後 SQL Server 2019/2022 に互換モードでロードし起動させるだけで済みます。完全なリグレッションテスト (回帰テスト) が必要ない場合は、これが迅速かつ簡単にアップグレードする方法といえるでしょう。SQL Server 2019 (互換性レベル150) であれば SQL Server 2008 R2 (互換性レベル100) までのバージョンをサポートできます。

セキュリティのベスト プラクティス

データ保護の強化に向けて、IT チームは SQL Server のセキュリティのベスト プラクティスに沿っているか確認する必要があるかもしれません (ベスト プラクティスの内容や実施方法について詳しくは、Microsoft のブログ記事「SQL Server の保護」をお読みください) 。このセキュリティのベスト プラクティスはデータセンター インフラストラクチャのすべてのレベル (ハードウェア、OS を含む) を対象としています。以下にその一部をご紹介します。

- **物理的なセキュリティを強化する。** 物理的なセキュリティにより、物理サーバーとハードウェアコンポーネントへのアクセスが厳重に制限されます。これは部屋を施錠することでサーバーおよびネットワーク機器へのアクセスを制限することを意味します。バックアップ用のメディアはオフサイトの安全な場所に保管しアクセスを制限します。また、敷地の境界、建物の境界、建物内部、データセンター フロアの各所で立ち入りを制限したり、カード キーまたは許可証を求めたりすることで、重層的に対策することをお勧めします。
- **OS を常に最新の状態にしておく。** OS のサービスパックやアップグレードには重要なセキュリティ強化策が含まれています。OS のアップデートおよびアップグレードは、データベース アプリケーションでテストした後に適用してください。
- **ファイアウォールを使用する。** セキュリティ対策に重点的に取り組めるチョークポイントを設けることにより、ファイアフォールは OS レベルでのセキュリティを高めます。
- **攻撃対象範囲を減らす。** 使用していない機能やコンポーネントを停止したり無効にしたりすることで、侵入に対して脆弱な領域を減らします。必要なサービスに「最小の権限」を設定し、サービスやユーザーに適切なレベルの権限だけを与えた状態で実行することで、SQL Server の攻撃対象範囲を減らすことができます。
- **「セキュリティ保護可能なリソース」にロールベース アクセス 制御 (RBAC) を実装する。**[3] セキュリティ保護可能なリソースとは、サーバー、データベース、およびデータベースに含まれるオブジェクトのようなコンポーネントを指します。セキュリティ保護可能なリソースは、SQL Server データベース エンジンのアクセス許可によってアクセスが制限されたリソースです。
- **すべてのレベルでデータを暗号化する。** アプリケーションやストレージのデータを暗号化します。
- **証明書を作成し、使用する。** 証明書とは、2つのサーバー間で安全な通信を可能にするためのソフトウェア キーです。SQL Server は証明書によってオブジェクトと接続のセキュリティを強化しています。
- **SQL Server で使用する OS ファイルへのアクセスを制限する。**
- **組織全体で強固なパスワードを使用する。** これはシンプルながら、軽視されがちなセキュリティ対策です。
- **監査を実施する。** バックアップ後に問題なく復旧し、適切にアクセスが実行されていることを確認します。
- **Microsoft Defender for SQL を使用する。** Microsoft Defender for SQL はデータベースの脆弱性をスキャンします。データベースに対するアクセスや悪用が疑われる、異常な動きや有害な可能性がある動きを検出します。これには、データベース上の不審なアクティビティ、潜在的な脆弱性、SQ L インジェクション攻撃、異常なデータベース アクセスや異常なクエリ パターンが含まれます。

最後に、最新バージョンの SQL Server にはすべてデータ保護を強化する新たなセキュリティ機能が搭載されています。SQL Server 2022 で発表された新たな台帳機能 (Ledger) は、時間が経つにつれ更新されるデータについて変更不可能な追跡記録を作成でき、データの完全性を保護するのに役立ちます。この機能は悪意をもったアクターによる改ざんからデータを保護するのに加えて、内部監査や外部監査などのシーンでも役に立ちます。

SQL Server Ledger

- 改ざん不可能な台帳でデータを保護し、悪意をもった攻撃者による不正改ざんを防止
- 中央集権型システムのデジタル トラスト確立にブロックチェーン技術を採用
- データの完全性が損なわれていないことを他者に証明

ハードウェアからデータベースまでの統合的な保護強化

デジタル企業のデータ量が増加するにつれ、IT の役割もますます大きくなるでしょう。データが増えればそれだけサイバー攻撃はより巧妙かつ頻繁になるため、IT チームはインフラストラクチャを保護するためのデータ セキュリティ戦略をすべてのレベルで採用する必要があります。SQL Server と Windows Server を最新バージョンにアップグレードし、それらを Dell PowerEdge サーバー上で稼働させることで、機密性の高い企業データや顧客データの保護が可能になります。

インフラストラクチャにセキュリティ ファーストなアプローチを導入しましょう。Dell と Microsoft の各ソリューションがお客様をどのようにサポートできるか、詳細はこちらにてご確認ください。
https://www.dell.com/ja-jp/dt/solutions/microsoft-data-platform/index.htm#accordion0%26tab0%3D0&accordion0&tab0=0

参考資料：「Windows Server 2022 と次世代 Dell EMC™ PowerEdge™ サーバーの機能を組み合わせることで、高度なセキュリティ保護を実現」

1 Egnyte、"2021 Data Governance Trends: Predictions, pitfalls and technologies for the future of digital work"、2021年
www.egnyte.com/sites/default/files/2021-09/2021DataGovernanceTrendsReport.pdf
2 IDC、"Data Creation and Replication Will Grow at a Faster Rate than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts."、2021年3月、www.idc.com/getdoc.jsp?containerId=prUS47560321
3 セキュリティ保護可能なリソースについて詳しくはhttps://learn.microsoft.com/ja-jp/sql/relational-databases/security/securables?view=sql-server-ver16をご覧ください。

DELL Technologies

Microsoft

Modernize with Windows Server 2022.
The cloud-ready operating system that boosts on-premises investments with hybrid capabilities.