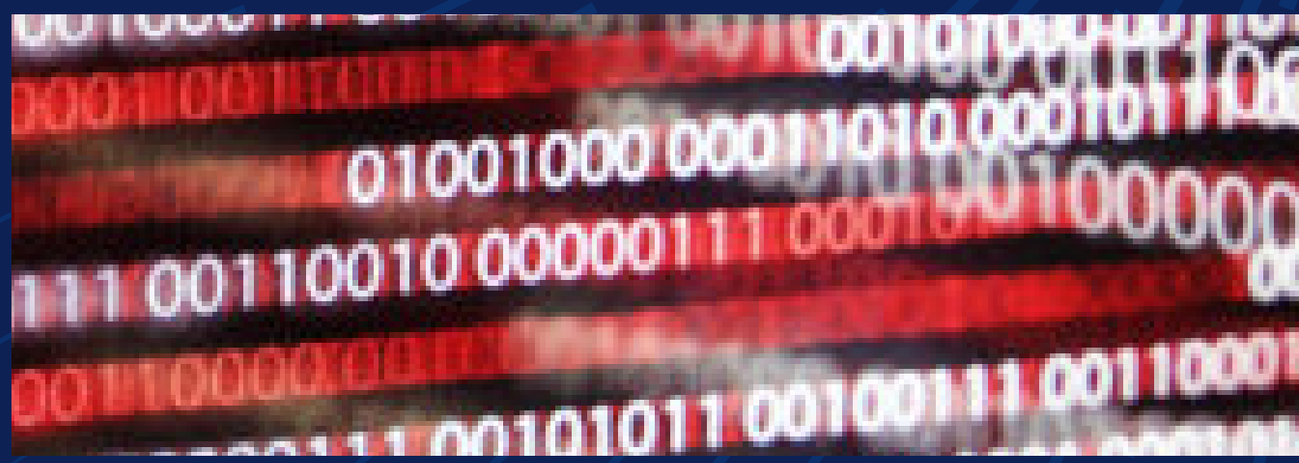
サイバーセキュリティの真偽検証：

AIセキュリティの誤解を解く



AIは産業に変革をもたらしていますが、AIの保護に関しては多くの組織が迷信に惑わされており、実際よりも複雑に捉えられています。実際のところ、AIシステムを保護するために、ゼロから始める必要はありません。既存のサイバーセキュリティ原則をAI固有の課題に適用するだけで、大きな効果があります。

AIを支えるアーキテクチャを理解しているデル・テクノロジーズは、お客様が現在お使いのソリューションを、この新しいフレームワークに合わせて適応させることができます。AIセキュリティのよくある誤解を整理し、真実を明らかにして、システムを効果的に保護しましょう。

誤解1：「AIシステムは複雑すぎてセキュリティを確保できない」

真実：AIが、プロンプト インジェクション、データ操作、機密情報漏えいなど、数々の新しいサイバーセキュリティ リスクを生み出していることは事実です。加えて、エージェンティックAIシステムは、結果操作や権限昇格に悪用される形で攻撃対象領域を広げる可能性があります。

これらの脆弱性を認識し、AIシステムを従来の脅威とAI固有の脅威から保護するためのセキュリティ対策を講じることが極めて重要になるとはいえ、リスク管理は可能であり、AIモデルは保護できます。AIシステムは入力として膨大なデータを必要とし、出力として大量のデータを生成する点に留意することが重要です。この点を最優先事項とし、以下の事項とともに取り組むことが、データ保護の主要なセキュリティ戦略になります。

- ID管理、ロールベース アクセス、継続的検証などのゼロトラスト原則。
- 脆弱性を特定するための定期的な侵入テストと脆弱性管理。
- データの入出力を検証するためのログと監査

誤解2：「既存のツールではAIを保護できない」

真実：AIセキュリティとは、最初からやり直すことではありません。すでにお使いのツールをさらにスマートに活用することです。既存のサイバーセキュリティ ツールのほとんどは、AIシステムを効果的に保護するために適応させることが可能です。AIは独自の特性を備えていますが、本質的にはビジネス推進手段に加わるワークロードの1つに過ぎません。ID管理、ネットワークのセグメンテーションと監視、エンドポイント保護、データ保護などの基本的なサイバーセキュリティ プラクティスは、AI環境を保護するために引き続き不可欠です。重要なのは、これらのプラクティスをAI課題（トレーニング データの保護、アルゴリズムの保護、敵対的入力などのリスク軽減）に対応させることです。

強力な防御は、システム パッチ適用、アクセス制御、脆弱性管理などの適切なサイバー ハイジーンから始まります。ポイントは、上述のプラクティスをAI固有のリスクに対処するようカスタマイズすることです。AIに焦点を当てた戦略を現在のセキュリティ アプローチに統合し、適切なツールを使用することで、AIセキュリティは管理しやすく効果的なものになります。

ただし、ここで注目すべきは、サイバー攻撃に対抗する上で極めて重要な役割を果たしうるのがアップデートされたハードウェアであるということです。例えば、最新のAI PCは、主要な攻撃ベクトルであるエンドポイントに対して強力な防衛線を張ることができます。古いパソコンは、Windows 10のサポート終了に伴いセキュリティ リスクにさらされます。さらにWindows 11では、暗号化、セキュア ブート、ファームウェア攻撃からの保護を支援するセキュリティ チップ Trusted Platform Module (TPM)バージョン2.0が必要です。古いパソコンの多くは、TPMを一切搭載していないか、古いバージョンのみをサポートしています。Dellの安全なビジネス向けAI PCには、こうした機能が最初から組み込まれています。

サーバーやストレージなどのAIインフラストラクチャも同様です。Dell AI Factoryには、AIセキュリティ向けに最適化されたハードウェアが含まれており、安全なサプライ チェーンから、データの不変性、分離、暗号化まで、さまざまなセキュリティ機能が組み込まれています。

誤解3：「AIセキュリティはデータ保護のみを目的としている」

真実：AIセキュリティとは、基本的なデータ保護だけでなく、モデル、API、出力、システム、デバイスを含むAIエコシステム全体を保護するものです。AIが重要なアプリケーションに統合されるにつれて、誤用や悪用に伴うリスクも高まります。堅牢なセキュリティ対策がなければ、AIモデルは改ざんされて有害な出力や誤解を招く出力を生成し、APIは悪用されて機密性の高いシステムに不正にアクセスし、出力から意図せず個人情報や機密情報が漏えいする可能性があります。

包括的なAIセキュリティには、多層的なアプローチが必要です。これには、入力データを操作してAIシステムを欺こうとする攻撃からモデルを保護すること、強力な認証方法でAPIを保護して不正使用を防止すること、**出力を継続的に監視して**攻撃や誤動作を示す可能性のある異常なパターンや不審なパターンを発見することが含まれます。効果的なAIセキュリティでは、悪意のある使用や意図しない結果が生じるリスクを軽減します。そうすることで、AIシステムの整合性と信頼性を確保すると同時に、ユーザーやステークホルダーとの信頼関係を築けるからです。

誤解4：「AIに人間による監視は必要ない」

真実：AIシステムを人間の価値観に沿って倫理的かつ予測可能な状態で動作させるためには、ガバナンスと人間の監視が不可欠です。高度なAIシステム、特に自律型の意思決定機能を備えるエージェンティックAIでは、堅牢な安全対策を必要とする固有の課題が生じます。適切に監視しなければ、こうしたシステムは意図した目標から逸脱したり、リスクを引き起こす可能性のある意図しない動作をしたりする可能性があります。

この課題に対処するには、明確な境界を設定すること、多層的な制御メカニズムを実装すること、重要な意思決定プロセスに継続的に人間が関与することが不可欠です。定期的な監査、AI運用の透明性、徹底的なテストにより、説明責任と信頼性をさらに強化し、誤用を防止し、AIテクノロジーの責任ある導入を促進できます。

AIセキュリティを強化するためのベスト プラクティス

AI固有のセキュリティ ギャップを埋めるには、プロアクティブで戦略的なアプローチを採用する必要があります。
AIシステムを保護するための10のベスト プラクティスをご紹介します。

セキュリティ アーキテクチャの多層化：
セグメンテーション、ファイアウォール、強力な認証を使用し、すべてのレイヤーでインフラストラクチャ、ソフトウェア、データを保護します。

AI出力の監視と検証：
異常検出、ログ、アラートを使用して、AI出力の異常なパターンや有害な動作を監視します。

サプライ チェーンの保護：
強力なサプライヤー管理プログラムを実装します。ベンダーとサードパーティー製コンポーネントを監査し、整合性を検証し、署名済みコードを利用することで、AI開発ライフサイクルの脆弱性を防止します。

レジリエンスの計画：
定期的なデータのバック アップとディザスター リカバリー計画のテストにより、ダウンタイムを最小限に抑え、侵害発生時の迅速なリカバリーを可能にします。

トレーニング データとモデルの保護：
データの整合性を監視し、堅牢な検証ツールを用いることで、有害なデータ、敵対的入力、その他の脅威から保護します。

堅牢な暗号化の実装：
強力なアルゴリズムを使用して静止中および転送中の機密データを暗号化し、暗号化キーを安全に管理して定期的にローテーションします。

アクセス制御の強化：
最小権限原則の適用、ロールベース アクセス制御(RBAC)の実装、認証情報の定期的なローテーション、権限の監査により、不正アクセスを防止します。

定期的なセキュリティ監査と侵入テストの実施：
システムの脆弱性をこまめに評価し、侵入テストを使用して、悪用される前にリスクを明らかにします。

APIの保護：
強力な認証プロトコル（OAuth 2.0など）を使用し、HTTPS暗号化を適用し、APIを定期的にアップデートして、潜在的な脆弱性を解消します。

AIセキュリティのベスト プラクティスに関するスタッフ トレーニング：
セキュリティ侵害を防ぐための安全な開発、脅威の認識、強力なセキュリティ プラクティスの維持について、チームを定期的にトレーニングします。

DELL Technologies

Dellの価値提案：実用的なAIセキュリティ ソリューション

AIセキュリティは複雑に思えるかもしれませんが、見た目ほど難しくありません。実際のところ、AIの保護は既存のワークロードのセキュリティ保護とそれほど変わりません。重要なのは、アーキテクチャを理解し、適切な戦略を適用することです。この点こそ、デル・テクノロジーズが得意とする分野なのです。

AIセキュリティの難解なイメージを取り除くため、お客様が持っているソリューションを活用し、AIに重点を置いたアーキテクチャにシームレスに統合します。インフラストラクチャを刷新せずとも、プロンプト インジェクション、APIの悪用、敵対的攻撃などの課題に対処します。

Dellには、AIセキュリティに関する誤解を整理し、それが実際に達成可能であると示せるだけの専門性があります。AIの導入を始めたばかりのお客様でも、防御を強化したいお客様でも、自信を持って効果的に投資を守り、システムを保護し、レジリエンスに優れたデジタルの未来を構築できるようにお手伝いいたします。一緒にAIセキュリティをシンプルにしましょう。

有効なDellの製品とソリューション

注目のDellソリューション	説明
Dell AI 工場	Dell AI Factoryは、安全なサプライ チェーンを通じてAIワークロードを保護し、開発から導入まで信頼できるインフラストラクチャを確保します。データの不変性、分離、暗号化などの機能により、機密性の高いモデルとデータセットを保護し、サイバー脅威を防御し、動的なデータ主導型の環境で拡張性と効率性に優れたシームレスなAI運用を可能にします。
サイバー レジリエンス	PowerProtectの高度な機能（不変性や分離など）がAIワークロードを守り、データの整合性を確保しながらサイバー脅威から保護します。エンドツーエンドの暗号化と異常検出を提供すると同時に、迅速なリカバリーを通じてダウンタイムを最小限に抑えます。
Dell Trusted Workspace (Endpoint Security)	組み込み機能とオプションのアドオン機能の組み合わせ。ビジネス向けAI PCとその上で実行されるAIワークロードを保護するように設計されています。安全なサプライ チェーン プラクティスに基づいて構築された組み込み機能には、SafeBIOSとTPMを使用したSafeIDが含まれます。オプションのアドオンには、Secured Component Verification、ControlVaultを使用したSafeID、パートナー ソフトウェアのCrowdStrikeとAbsoluteなどがあり、ワークスペースのセキュリティを最大限に高められます。
AIセキュリティ アドバイザリー サービス	包括的なAIセキュリティ戦略の策定と実装を支援する、サービス一式。アドバイザリー サービス、AI vCISO、データ セキュリティ計画が含まれます。
Managed Security Operations for AI	スタック全体を詳細に可視化し、脅威を迅速に検出して対応します。機能には、Managed Detection and Response、Managed AI Guard、Penetration Testing for AI、Incident Response and Recovery Servicesが含まれます。
セキュリティ ソフトウェア統合	アクセス管理、アプリケーション、ネットワーク、クラウドなどを保護するセキュリティ ツールを設計、インストール、構成します。

dell.com/cybersecuritymonth
で今日のサイバーセキュリティの重要な課題に対処する方法をご紹介しています