Strategy₿

ホワイトペーパー

AIセキュリティ

データの完全性と倫理的なAI実装を実現するための
実践的な手順の研究

目次

はじめに

ビジネスインテリジェンス（BI）において人工知能（AI）を効果的に導入できるかどうかは、その基盤となるデータの完全性（インテグリティ）に大きく左右されます。AIシステムがビジネスの意思決定を促進する用途として用いられる場合、正確性はメリットではなく、必須条件です。システムが真に有用であるには信頼できるものでなければなりません。

こうした中で、Strategyは信頼できる基盤として注目を集めており、ビジネスユーザーに向けて正確かつセキュアなデータを提供しています。さらに、Strategy AIを導入すればその取り組みはより一層強化され、BIの精度とAIの革新的な機能を融合したプラットフォームを実現できます。

当社のAIソリューションは、自然言語で表現されたビジネス上の質問を正確に解釈し、論理的な推論を行った上で、関連する結果を自動的に生成するように設計されています。このようにBIの構造化された分析とAIの柔軟性を組み合わせることで、Strategy AIはデータの完全性と柔軟なユーザー体験という2つのニーズを満たすことができます。

Strategy AIは、当社の実績あるプラットフォームを進化させたものであり、高度なAIと機械学習機能をシームレスに統合しています。AIによるデータ探索、ダッシュボード設計の自動化、特殊ツール（SQL生成や機械学習によって強化されたデータ分析用ビジュアリゼーションなど）の使用といったプロセスを効率化します。こうした機能を活用することで、Strategyエコシステムの慣れ親しんだ環境の中でより深いデータインサイトを得ることができます。

Strategy AIの信頼性は、Strategyセマンティックレイヤーの細部まで行き届いた設計とその包括的なセキュリティフレームワークに基づいています。当社のAIアシスタントである「Auto」は、Strategyが提供するデータを活用しており、すべての分析は当社の実績ある分析エンジンによって行われます。これによってデータ処理や表現の一貫性・正確性・安全性を確保することができ、企業は安心して意思決定ができるようになります。

Strategy AI環境の分離

エンタープライズ向けAIソリューションの強みは、データを処理して洞察を提供するだけにとどまりません。外部の脅威に対してレジリエンシーの高いアーキテクチャーも大きな強みとなります。Strategy Cloud Environment（MCE）は、環境の分離、セキュアなアクセス、外部またはマルチテナントサービス内における安全なリクエストの実行を最優先に考えたアーキテクチャーによって支えられています。

分離のための設計：

MCEは、「環境の分離」をセキュリティ上の重要な指針として捉えた上で戦略的に設計されたソリューションです。各顧客のデータが安全に分離された環境で運用されることで、データが混在してしまうリスクを排除し、データ保護を強化します。システムが外部サービスと接続したり、リクエストを送信したりする必要がある場合、これらのワークフローは厳格なセキュリティ対策と通信プロトコルに沿って実行されます。例えば、データの送受信は暗号化され、リクエストは各顧客のインスタンス内にて独立してステートレスに処理されるようになっています。

MCE上のStrategy AI：

Strategy Cloudの提供内容には、Strategy AIモジュールが組み込まれており、これによって機能が強化されています。このAIモジュールをMCEフレームワークに基づいて運用することで、Strategy AIはMCEに固有の強固なセキュリティ基準の恩恵を常に受けることができ、それに準拠した運用が可能になります。

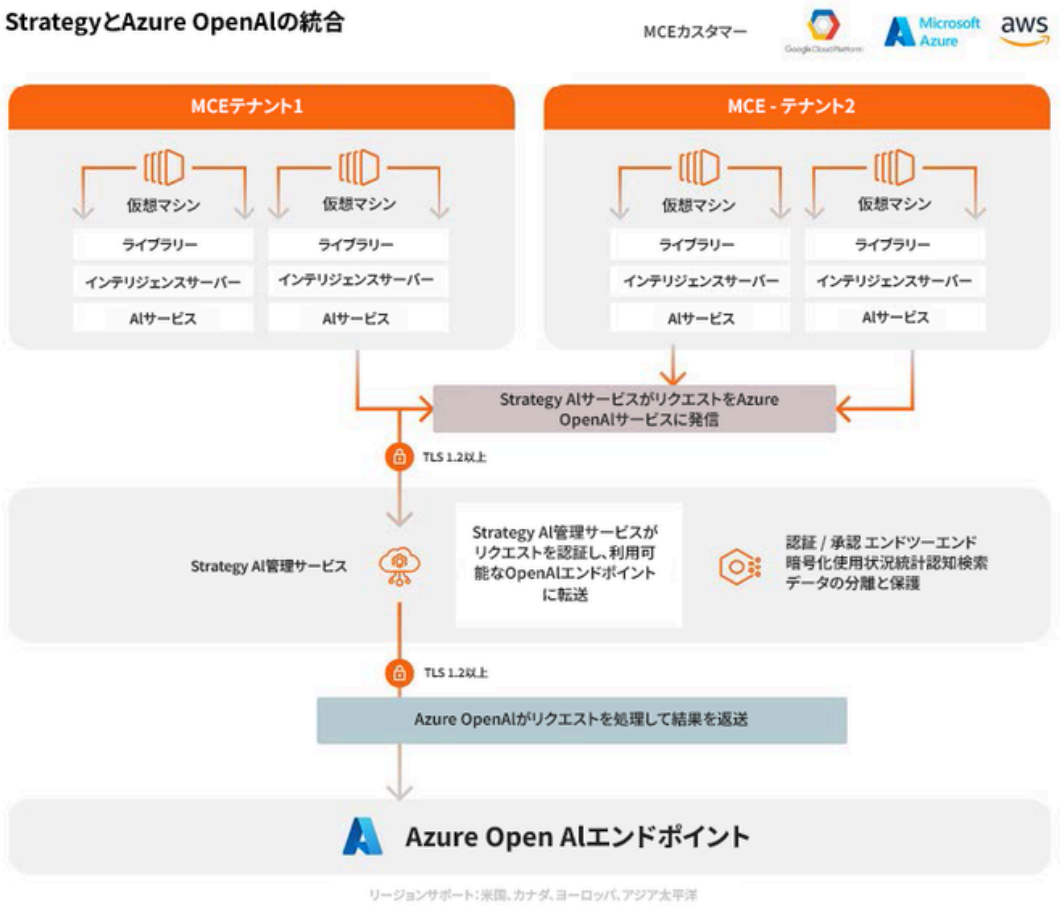
MCEの分離の特長：

- **カスタム設定：**Strategyは、リソースを仮想プライベートクラウド（VPC）に展開し、IPアドレス範囲、ルートテーブル、ネットワークゲートウェイ、関連するセキュリティ設定をチューニングできます。これにより、各顧客の環境は個別のニーズに応じながらもセキュリティ基準を遵守することがきます。

- **堅牢なファイアウォールの実装：**各顧客のテナントは、ハイパーバイザーレベルのファイアウォールやセキュリティグループにより厳重に保護されます。高度なクラウドおよび仮想化ソフトウェアを活用することで、これらのファイアウォールは、MCEインスタンスをさらに分離し、完全に独立したクライアント処理スペースを確立します。このような分離を行うことで不正アクセスを防ぎ社外秘の情報を確実に保護できるようになります。

このように、Strategy AIは単なる高度なデータ処理ツールではなく、クラウド環境に深く統合された製品であり、そのシステム設計でのあらゆる側面において、ユーザーのセキュリティが最優先に考慮されています。MCEの厳密な環境セキュリティ特性は、顧客データの完全性を守るという当社の揺るぎないコミットメントを改めて示しているのです。

StrategyとAzure OpenAIの統合



Strategy AIによるデータのプライバシーと完全性の確保

Strategy AI

Strategy AIは、組織内のさまざまなスキルレベル、さまざまな職務のユーザーに対応する数々のAI機能を提供します。ビジネスユーザーやアナリストは、Autoアンサーというチャットボット体験を活用して、ダッシュボードをより深く掘り下げて、洞察や詳細なデータ分析結果を得ることができます。これには、機械学習機能を活用した要因分析、予測、トレンドを生成する高度なQ&AやAIのビジュアライゼーションが含まれます。また、特定のユースケースやペルソナに特化したボットを使用することもできます。このボットは、「ナレッジアセット」や「カスタム命令フィールド」を活用して豊富なビジネスコンテキストを提供するためのカスタマイズも可能です。Strategy AIで利用できるその他の機能には、 ユーザーがダッシュボードをより効率的に設計できるようにするための「Autoダッシュボード」のほか、 管理者やアーキテクトがSQLを生成してデータモデリングを高速化できる「Auto SQL」があります。

自社環境でAIを活用するすべての顧客は、顧客ごとに環境が独立したテナントとして設計されたアーキテクチャーを活用します。このテナントはStrategy AI管理サービスに接続し、そこではリクエストがLLM（大規模言語モデル）によって処理されます。

Strategyでは、ナレッジアセット機能を使用し、ファイルを介して文脈情報を追加することで、利用者がボットを微調整（ファインチューニング）できるようにしています。「ナレッジマネージャー」は、Excelファイル経由で更新されたすべての情報を処理し、Strategy AIのナレッジを拡張するものです。その後、組み込みモデルがこの情報を処理し、「ナレッジストア」に保存される定義に変換します。ナレッジストアは、認知処理技術を使用してエンコードされたドメイン知識を保存する安全な格納庫としての役割を担うものです。このエンコーディングは、データの整合性を保持するだけでなく、コグニティブ検索処理を行うためのアクセシビリティも強化します。

生成AIモジュールと相互通信する際、ナレッジストアはコンテキストに関連する情報を提供する重要な役割を果たします。これにより、生成AIは正確かつ的確なStrategyクエリを作成できます。このナレッジストアは迅速かつ高速なナレッジ検索を可能にする高度なエンコーディングアルゴリズムを備えています。

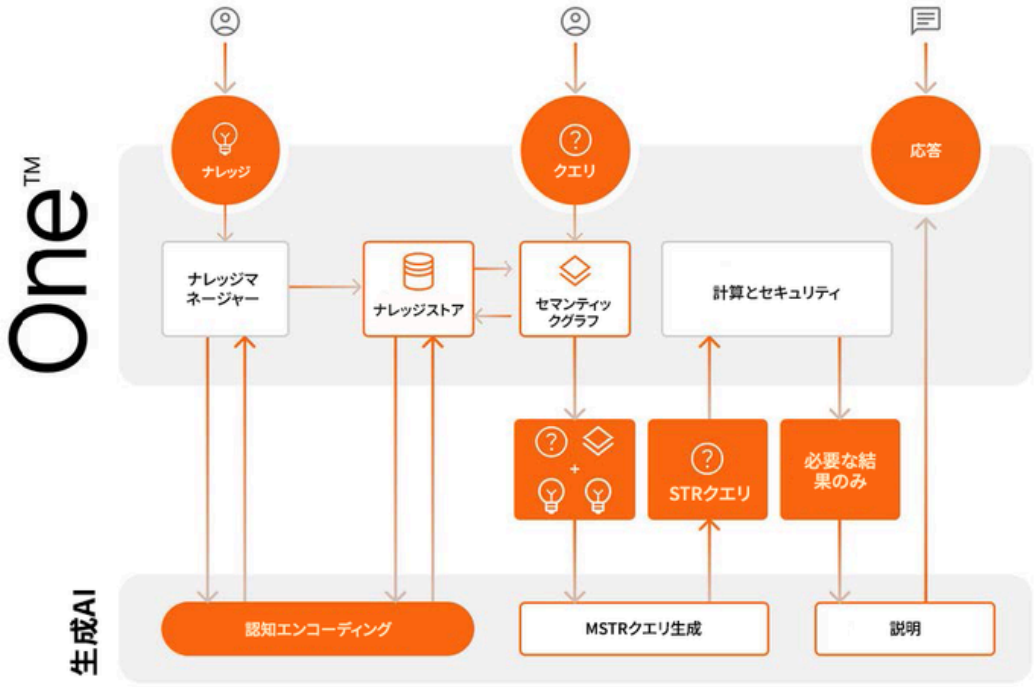
ナレッジストアには、セキュリティおよびデータガバナンスを強化する設計が施されています。そのため、不正なアクセスや改ざんからデータを確実に保護します。このように、高水準のデータセキュリティを保持することで、ナレッジストアは信頼性の高い分析結果を生成するための堅牢な基盤を実現しています。

なお、ナレッジアセットをアップロードしてデータを拡張できるのは特権を持つユーザーのみです。データはアクセス制御、特権、暗号化により保護されています。

StrategyとAzure OpenAI LLMの間で転送される情報は、データセットのスキーマと最小限のサンプルデータのみです。そのため、LLMはユーザーの質問を処理するために必要なコンテキストを得ることができます。ナレッジアセット機能とコグニティブ検索を統合すれば、さらに追加のコンテキスト情報をLLMに提供でき、より精度の高い応答が可能になります。リクエストはLLMを介して実行計画に変換され、その後、Strategyのセマンティックグラフおよび分析エンジンを通じて計算が行われます。これにより、返される情報がガバナンスに準拠した安全かつ信頼できるものであると保証されるため、LLMソリューションで生じがちなハルシネーションを防ぐことができます。計算が完了すると、計算結果はLLMに戻されて解釈され、最終的にユーザーに自然言語として表示されます。

Strategy AIはMicrosoft Azure OpenAIを使用しており、すべての通信はTLS 1.2以上に準拠したセキュアなチャネルを介して厳密に行われます。データは転送中常に暗号化が保証され、不正アクセスや漏えいを防ぐことができます。

このようにAI機能は、Strategyプラットフォームでユーザーに指定されたアクセス制御、アクセス制御リスト（ACL）およびデータセキュリティ対策の範囲内にて厳格に動作します。



データ保持

Autoアンサー機能は、アクティブなユーザーセッション後に会話履歴を保持しません。

Strategy Autoボットでは、ユーザーがチャット履歴を保持して、そのデータのスナップショットを保存できる機能を提供します。これらのチャット履歴およびスナップショット情報へのアクセスは、ユーザーごとに管理され、ユーザー間で情報が共有されることはありません。さらに、この情報はテナント専用のストレージスペースに保管され、AES-256ビット暗号化によって完全に暗号化されます。

Strategy Platform Analyticsは、ユーザーとAutoとのやり取りに関するテレメトリーデータを収集し、管理者を支援します。これには、ユーザーの質問や、質問の解釈（要求された場合）、質問に対して生成されたSQLクエリ、結果を取得して表示するために作成されたStrategyテンプレートのキャプチャが含まれます。このデータへのアクセスは、Auto AdoptionおよびAuto Question Analysisダッシュボードに加え、それに依存するスキーマオブジェクトへのアクセスを制限することによって管理されています。Platform Analyticsは、各カスタマーのテナントで提供されます。

履歴データ保持

Strategy AIは、データのセキュリティとプライバシーを確保しながらユーザーのニーズを満たすよう設計された堅牢なデータ保持機能を提供します。各ユーザーは、最大30件の履歴の質問と回答データを保持できます。この機能により、ユーザーは過去のやり取りにアクセスして内容を確認し、過去の質問から学びながら一貫した体験を得られるようになります。

履歴データの手動削除

Strategy AIでは、ユーザーが自分のデータを管理できるように、過去の会話から質問や応答を手動で削除できます。ユーザーは不要なエントリを削除できるので、自分の好みに合わせてポイントを絞ったクリーンな履歴データを維持できます。

スナップショット

ユーザーは履歴データに加えて、特定の質問と応答のスナップショットを作成して保存できます。このスナップショットは通常の履歴とは独立して保管され、重要なデータポイントやインサイトを保存するのに使用できます。各ユーザーは、最大50件のスナップショットを保持でき、データの管理・取得を柔軟に行うことができます。

データの保管場所

テキストコンテンツ ストレージ：質問と応答のテキストコンテンツは、Strategyメタデータ データベースに安全に保管されます。このデータベースは、高可用性を考慮して設計されており、効率良くデータ取得できるように最適化されています。

ビジュアリゼーション データストレージ：各応答を可視化するために使用されるデータポイントは、Strategyストレージサービスに保管されます。ユーザーは、ビジュアリゼーションデータを保存する前に、適切なデータ処理とセキュリティを確保するためにStrategyストレージサービスを設定する必要があります。

テキストコンテンツ ストレージとビジュアリゼーション データストレージは、各顧客のテナント内にあります。

ユーザーデータプライバシー

ユーザー固有の質問、応答、スナップショットは非公開情報であり、各ユーザーのみがアクセスできます。この厳密なアクセス制御は、当社のユーザープライバシーおよびデータセキュリティに対するコミットメントの一環であり、機密情報の保護を保証します。

こうしたデータ保持ポリシーは、透明性が高く安全かつユーザーを第一に考えた体験を提供するために当社が行っている取り組みの1つです。これがあることで、Strategy AIは効率的かつ効果的に利用することができるのです。

Strategy Cloud環境におけるAIコンポーネントの規制遵守

Strategy AIは、Microsoft Azure OpenAIと統合されたCCPA、GDPR、SOC 2、ISO 27001などの重要な国際データ保護規制に関する認証を取得しています。MCE上のStrategy AIコンポーネントの設計と運用手順は、これらの規制基準に基づいて調整されています。当社の厳格な規制遵守のアプローチは、規制当局が定めた基準を満たすだけでなく、さらにそれを上回ろうとする当社のコミットメントを示しています。

Strategyは規制遵守に対して系統的かつ徹底的な姿勢を貫いており、業界標準に適合するために専任の内部コンプライアンスチームを設置しています。このチームは、特に一般データ保護規則（GDPR）の厳格な要件を満たすことを目的とした強固なデータ保護およびプライバシープロトコルを設計しました。Strategyは、Strategy Cloudが運用されるすべての地域において、規制に対して完全に準拠していることを保証しています。

MCEは、AWS、Azure、Google Cloudで利用でき、以下のリスク管理および情報セキュリティフレームワークに適合しています。なお、準拠しているかどうかは定期的に検証され、必要に応じて内部および第三者の専門家による厳密な評価を通じて認証されます。

- 一般データ保護規則（GDPR）
- AICPA SSAE-18、システムおよび組織コントロール – SOC 2 Type 2レポート
- ISO/IEC 27001:2013（ISO 27001:2013） – 認証番号：ISMS-MI-13123
- EU-米国およびスイス-米国間のデータプライバシーフレームワーク
- 1996年医療保険の相互運用性と説明責任に関する法律（HIPAA）セルフアセスメント

EU AI法を遵守するStrategy AI

EU AI法は、ヨーロッパにおけるAI技術の安全かつ倫理的な使用を確保することを目的とした法律です。Strategy AIはこの法律を遵守することを目指しています。Strategy AIは、汎用AI（GPAI）大規模言語モデルであるAzure OpenAIを組み込み、顧客にAI機能を提供しています。基本レベルの機能をベースとしているため、AIシステムとしてリスクは限定的です。Strategy AIの機能（Autoアンサー、Autoボット、Autoダッシュボードなど）はすべて、常にチャットベースでユーザーにサービスを提供するものであり、意思決定が自動的に行われるものではありません。さらに、リスクの低いAIシステムを提供するStrategy AIは、意図的に透明性を確保しており、当社ではStrategy AI製品に関して次のような品質管理の取り組みを導入しています。

- 強固な安全対策
- 意思決定の透明性
- AIとの対話に関する明確なユーザー情報
- AIシステムの定期的な評価と改善

最後に、Strategy AIおよびそのすべてのインテリジェント機能は、Strategy独自の信頼性の高い計算エンジンのみに依存しています。Strategy AIでは、ユーザーの入力やチャット履歴、またその他の通信が、LLMやGPAI、その他のサードパーティAIモデルの学習に使われることはありません。

Strategy内でのAI使用の監視、ログ記録、監査

Strategyでは、自社プラットフォーム内のAI利用の監視・ログ記録・監査を極めて重要視しており、透明性と説明責任を確保しています。導入されている監視システムを用いて、顧客は自らAIの利用状況を包括的に確認することができます。使いやすいダッシュボードを活かして、顧客は自社が行った質問をトラッキングして、どのユーザーがどんな質問をしたのかについて洞察を得られます。このような透明性により、企業は自社のAI活用を効果的に最適化できます。

ログ記録メカニズム

Strategyは、ユーザーデータプライバシーおよびセキュリティを保護するために、慎重に設計されたログ記録メカニズムを導入しています。Strategyプラットフォーム内では、特定の情報がログに記録され、それ以外の情報は意図的に除外されます。これによりユーザーデータを保護し、データコンプライアンス法に準拠します。

具体的には、Strategyのログシステムは、運用目的として必要不可欠なデータを記録しています。例えば、ユーザーが行った質問に使用したトークン数を記録しており、それによって消費量と使用状況をトラッキングすることができます。なお、このログに記録されたデータはAIモデルの学習を含め、ユーザープライバシーを侵害する可能性がある他の目的には使用されません。

このように、プライバシーに配慮した方針は、現代のデータ保護基準および規制と整合するものであり、ユーザーは自身の機微情報のセキュリティについて心配することなく、StrategyのAIツールを安心して取り扱うことができます。

監査証跡

監査証跡は、Strategyプラットフォーム内で説明責任とトレーサビリティを保証する上で極めて重要です。Strategyは、Platform Analyticsに堅牢なシステムを実装しており、顧客が効率的に監査証跡を記録できるようにしています。このシステムの重要な要素の1つは、一意の質問IDを保持することです。これによって、個々のユーザーに関連付けられた実際の利用状況を追跡できます。ここで重要なのは、Strategyでは生成された結果を記録せず、代わりに質問IDに焦点を当てている点です。これによって、どのユーザーがクエリを行ったか、あるいは特定のAI機能を使用したかを正確に判定できます。このアプローチによって、説明責任とデータプライバシーのバランスを保ちつつ、ユーザーの行動を確実に追跡・監視できるようになります。

アクセス制御リストおよびデータセキュリティ対策の遵守

Strategyは、サービスの革新と拡大を進める中で、ユーザーデータの安全とセキュリティを常に最優先事項として捉えています。優れたAutoの機能をはじめ、Strategy AI機能の導入は、実績あるStrategyプラットフォームの包括的なセキュリティモデルとシームレスに統合するよう慎重に設計されています。これによって、データアクセスにおける一貫性を確保するとともに、厳格なセキュリティプロトコルを忠実に遵守していることが保証されます。

- **一貫性のあるアクセス制御リスト（ACL）および権限：**当社のAIアシスタントであるAutoは、アクセスが許可されたデータセットからの応答だけを受信するように設計されています。Autoに提示されたすべてのクエリは、セマンティックレイヤーの基盤となるオブジェクトに設定されたACL（アクセス制御リスト）と照合されます。これは、ユーザーがAI機能を取り扱う際も、アクセス制御のインテグリティが損なわれないことを意味します。

- **セキュリティフィルターを介した粒度の高いデータアクセス：**基本的なACL設定に加えて、当社のプラットフォームはセキュリティフィルターを使用してきめ細かなデータアクセス制御を提供します。こうしたフィルターはユーザーがクエリを実行できるデータ範囲を絞り込む追加の制御レイヤーとして機能します。これにより、管理者はデータアクセスに対して正確な境界線を定義することができ、ユーザーは許可されたセグメントのデータとのみやり取りができます。

- **AI機能用の設定可能な特権：**すべての企業には各社特有のニーズとセキュリティ上の懸念があるはずです。そのため、当社のAI機能には設定可能な権限を組み込んでいます。これにより、企業のリーダーは、Autoやより高度なMLを活用したアナリティクスやビジュアリゼーションなど、高度なAI機能を活用できるユーザーを指定できます。イノベーションとセキュリティプロトコルのバランスを取るための柔軟性を確保できます。

データの完全性確保と悪用の防止

Strategyのコアとなる信念は、データのセキュリティを完全に保証すること、また不正利用を防止することです。デジタル環境が拡大する現在において、データ保護の重要性がより高まっています。そうした中で当社はプラットフォームを守るために以下のような対策を行っています。

- **堅牢な暗号化プロトコル：**当社のプラットフォームは、転送中のデータや保存されたデータのセキュリティを保証します。Microsoft Azure OpenAIなどの外部サービスとの通信には、TLS 1.2以上の業界標準の暗号化技術を使用し、データが転送中に盗聴されないように保護しています。また、保管されたデータを保護するためにAES-256などの高度な暗号化規格を活用して保存中のデータの暗号化を実施し、頻繁に転送されない時でも機密情報を不正アクセスから確実に保護しています。

- **Microsoft Azure OpenAIを用いた設定：**Microsoft Azure OpenAIとの統合における設定により、OpenAIに送信されるデータは保持されず、モデルの学習に使用されないことが保証されています。この技術的な設定により、外部とのやり取りにおいてもユーザーデータが安全に保護されていることが確実となります。

- **ユーザーインタラクションのプライバシー：**Strategyは、質問の頻度と種類を監視するために使用状況のデータは記録しますが、ユーザーとの会話の詳細にアクセスすることはありません。これはまさにユーザー中心のデータプライバシーに対する当社のコミットメントを反映しています。こうした緻密な設定により、 ユーザーとAIのやり取りの本質的な内容については非公開のまま保つことができます。

これらのプロトコルに従い、当社は高度なソリューションの提供を優先的に考えながらデータ保護とユーザーの信頼を常に重視しています。またこうした実践が、機能面での卓越性と厳格なデータセキュリティを重視する当社の姿勢を明確に表しています。

結論

Strategyのデータのセキュリティと完全性への取り組みは、Strategy AIにおいても明確に示されています。データの信頼性がAIの精度に直接影響を与える分野において、当社はプラットフォームを慎重に設計し、厳格なデータ基準を満たすだけでなく、さらにそれを超えることを目指しています。

当社のBIの精度とAIの適応性を組み合わせることで、セキュリティを犠牲にすることなく、ユーザーは最先端の分析のメリットを享受できます。Strategy Cloud環境では、当社独自の環境分離によりデータプライバシーは一貫して優先され、データ侵害のリスクが低減されます。国際的なデータ保護規制への遵守は、当社のプラットフォーム設計に不可欠であり、グローバル基準に対する当社の献身的な姿勢を示しています。

アクセス制御リストと厳格なデータセキュリティ対策を遵守することで、ユーザーは常に事前に定義されたデータアクセス範囲内でのみ操作を行うことが保証されます。さらに、Microsoft Azure OpenAIとの連携は、業界のベストプラクティスに基づいており、データが直接的な使用範囲を越えて保持されたり、意図から外れて使用されたりすることはありません。

以上のように、Strategy AIは、高度な分析機能と厳格なデータ保護基準を統合します。データセキュリティとデータの保護を徹底しながら、信頼できるAIインサイトを提供すること。これが当社の目指すべき明確な方向性であり最優先事項です。Strategy AIに関する詳細は、当社のWebサイトをご覧ください。

Strategy Incorporated, 1850 Towers Crescent Plaza, Tysons Corner, VA 22182.
 MSTR-TR-202502-025

strategysoftware.com

Strategy₿