CDATA

ホワイトペーパー

エンタープライズセキュリティベストプラクティスガイド

AI のデータ接続のための セキュアな
MCP アーキテクチャの構築

2026年3月

本ガイドの内容

- MCP のセキュリティリスクの理解と、マネージドプラットフォームが重要である理由
- エンタープライズ向け MCP 導入におけるセキュリティアーキテクチャの基本
- ID ファーストのアクセス制御と、データソース側で適用されるロールベースアクセス制御
- ガバナンス、監査証跡、コンプライアンスのベストプラクティス
- セキュリティレビューでよく寄せられる質問への回答

対象読者：IT 責任者、セキュリティチーム、データアーキテクト

エグゼクティブサマリー

企業が AI エージェントや AI アシスタントを導入してビジネスプロセスを自動化するなかで、3つの重要な課題、いわゆる「3つの C」が浮かび上がっています。社内のデータソースへの Connectivity（接続）、そのデータが何を意味するかという Context（文脈や状況の理解）、そして AI が何にアクセスし何を実行できるかという Control（管理）です。

CData Connect AI は、これら3つの要件すべてに対応し、エンタープライズグレードのセキュリティを最初から組み込んだ、初のマネージド型 Model Context Protocol（MCP）プラットフォームです。本ガイドは、IT 責任者とセキュリティチームに向けて、スケーラブルでセキュアな MCP アーキテクチャを構築するための実践的なベストプラクティスを提供します。

Connect AI のセキュリティ基盤

CData は、第三者機関による SOC 2 Type II および ISO/IEC 27001:2022 のコンプライアンス監査を完了しています。Connect AI は、PKCE（Proof Key for Code Exchange）を用いた OAuth 2.1、SSO（シングルサインオン）連携、保管時の AES-256 暗号化、転送時の TLS 1.3 など、包括的なセキュリティを提供します。データは保存もコピーもされず、すべてのクエリはソースシステムに対してリアルタイムで実行されるため、データ主権とコンプライアンスが維持されます。

MCP のセキュリティリスクの理解

Model Context Protocol（MCP）は、AI エージェントが企業システムとリアルタイムに対話することを可能にします。これは大きな価値を生み出す一方、最近の業界調査では、本番導入前に企業が対処すべきセキュリティ上の懸念がいくつか指摘されています。

AI のデータ接続でセキュリティが重要な理由

MCP は、従来のデータ連携手法だけでは十分にカバーできない、新しいセキュリティ上の論点をもたらします。

- AI エージェントは非決定論的な挙動をするため、従来の認証ワークフローが複雑化する
- プロンプトインジェクションにより、エージェントが機密データを意図せず開示してしまうリスクがある
- 複数のシステムにまたがるトークンや認証情報の管理には、慎重なオーケストレーションが必要となる
- MCP プロトコル自体には、サーバーレベルでのオプションの基本的なセキュリティ機能しか備わっていない。AI ユーザー全体にまたがるセキュリティ制御を実現するには、MCP の実装方法が重要となる

管理下にない MCP 導入のリスク

MCP のインフラを自社で構築したり、コミュニティ提供のサーバーを利用したりする企業は、深刻なセキュリティ上の課題に直面します。

サプライチェーンリスク

MCP サーバーをローカルにインストールすることは、多くの場合、素性が検証されていないソースから任意のコードを実行するに等しい行為です。現在の MCP サーバー配布は非公式のレジストリに大きく依存しており、インストール手順も「pipe curl to bash」（curl で取得したスクリプトをそのまま bash に流し込む）のようなアンチパターンに陥っています。バージョン固定も、署名も、パッケージのロックもありません。

レジストリと信頼性の問題

公開されている MCP サーバーのレジストリは、オープンソースエコシステムでよく知られたリスクを抱えています。

- タイポスクワッティング（typo + squatting）：人気パッケージに似た名前で公開される悪意あるパッケージ
- なりすまし：知名度の高いプロジェクトの関係者だと偽る開発者
- ラグプル（Rug pull）：普及した後で悪意あるコードに更新されるパッケージ
- アカウント乗っ取り：侵害された開発者アカウントから配信される悪意あるアップデート

現状のレジストリには、信頼を判断するための十分な手がかりがありません。「Official」や「Verified」といったラベルが付いていても、開発者の身元が確認されているとは限らず、そのサーバーが代表すると称する製品との結びつきが信頼に足るものだと保証されているわけでもありません。

リモートサーバーの脆弱性

リモート MCP サーバーはローカルでは実行されないものの、リモートコード実行、認証情報の窃取、クライアントから利用できる他のツール経由での不正アクセスといったリスクは依然として存在します。ベンダー側のリスクも無視できません。リモートサーバーは、機密性の高い認証データや顧客情報を保存・処理する可能性があるからです。

クライアント側のリスク

MCP クライアントは、セキュリティへの配慮の度合いに大きな差があります。多くは、人間の承認を経ずにツールを自動実行できる仕組みを許容しており、ツールからの応答を暗黙的に信頼してしまうため、サーバーが侵害された際の影響範囲が広がります。さらに、ツール名の衝突、スラッシュコマンドの乗っ取り、信頼できないコンテンツに仕込まれた間接的なプロンプトインジェクションといったリスクも存在します。

Connect AI によるリスクへの対処

リスク領域	管理下にない MCP	Connect AI のソリューション
プロンプトインジェクション	権限の肥大化、デフォルトで読み書きが可能なスコープ	カスタム MCP ツールで権限のないプロンプト操作を制御し、特定のエージェントが実行可能なアクションを制限
サプライチェーン	公開コードリポジトリにある検証されていないコード	SOC 2 Type II 監査と第三者によるペネトレーションテストが施された、マネージドかつ監査済みのプラットフォーム
認証	個々のサーバーレベルで独自に実装された認証	MCP サーバーと AI ユーザー全体での、PKCE 付き OAuth 2.1 と SSO 連携の一元化
アクセス制御	システムごとの権限の再構築	RBAC パススルーによる、既存のソースシステム側の制御の引き継ぎ
データセキュリティ	複数システムにまたがるデータコピー	インプレースアクセス。ソースシステムからのデータ複製なし
監査ログ	一貫性のない、もしくは不足したログ	ユーザー、クエリ、タイムスタンプ、エラーまでを網羅した包括的な監査証跡
認証情報の管理	分散したトークンやシークレット	暗号化された認証情報の一元的なストレージ
ガバナンス	標準化された制御の欠如	CRUD スコープ設定、ワークスペース、派生ビュー、カスタム MCP ツール、ツールキットによる統制

CDATA

業界からの推奨：マネージド MCP プラットフォームの活用

セキュリティ研究者は、監査ログ、モニタリング、ガードレール、ガバナンス機能を備えたマネージドプラットフォームを通じて、MCP サーバーの利用を一元化することを推奨しています。これにより、分散して管理下にないサーバー群ではなく、セキュリティ統制の一元的な拠点を構築できます。

セキュリティアーキテクチャの基本

Connect AI のセキュリティアーキテクチャは、3つの基本原則の上に成り立っています。ID ファーストアクセス、インプレースのデータ接続、包括的な監査ログです。

インプレースデータアクセス

データを抽出して複製する従来の統合パターンとは異なり、Connect AI はソースシステムからデータをコピーすることなく、インプレース（その場でアクセスする方式）でデータにアクセスします。CData はデータを永続ストレージやキャッシュに保存することはなく、クエリ実行時に一時的に転送するだけです。これにより、以下のようなセキュリティ上のメリットが得られます。

- ソースシステムのアクセス制御が、変わらずそのまま効力を持つ
- 保護・管理・同期の対象となるデータコピーが発生しない
- データ主権の要件に本質的に適合する
- ソース側のガバナンス制御が、AI からのアクセスにも自動的に適用される

オンプレミスにデータを持つ企業向けには、Connect Gateway が同等のセキュリティ特性をファイアウォールの内側まで拡張します。ゲートウェイは社内インフラ内で軽量なエージェントとして動作し、Connect AI へ送信専用のセキュアな接続を確立します。オンプレミスのシステムが直接インターネットから到達可能になることはなく、ゲートウェイ経由で接続されたオンプレミスのシステムにも、クラウドソースと同じ監査証跡、RBAC パススルー、権限制御が適用されます。

ID ファーストのセキュリティモデル

Connect AI は、ソースシステムの RBAC をそのまま引き継ぐパススルー認証モデルを採用しています。ユーザーや AI エージェントがデータを要求すると、プラットフォームは以下を実行します。

- 設定された ID プロバイダーを使用してリクエストを認証する
- 認証情報をソースシステムに渡す
- ユーザー個人の権限、またはロールから継承された権限に従ってクエリを実行する
- 認証された ID のもとで、監査のためにアクションを記録する

このアプローチにより、ユーザーや AI エージェントは、自身がアクセス権を持つデータだけを参照することになります。IT 部門が権限体系をシステムごとに作り直す必要はありません。

プラットフォームの認証・準拠状況

認証・準拠状況	説明
SOC 2 Type II	セキュリティ管理策の運用上の有効性を時間軸で検証する独立監査。Connect AI を含む CData の全製品を対象とする。
ISO/IEC 27001:2022	情報セキュリティマネジメントシステム（ISMS）に関する国際標準。機密データ管理に対する体系的なアプローチを示す。
GDPR 準拠	プラットフォーム設計により、データ最小化、インプレースアクセス、包括的な監査機能を通じて GDPR の要件をサポートする。

セキュリティテスト

CData は、独立した第三者のペネトレーションテスターを起用し、Connect AI のセキュリティ評価を定期的に実施しています。加えて、外部監査の合間も、社内のセキュリティチームが継続的にペネトレーションテストおよび脆弱性評価を行っています。第三者による評価のサマリーは、NDA のもとで請求に応じて提供可能です。

認証のベストプラクティス

適切な認証設定は、セキュアな MCP 導入の土台となります。Connect AI は、既存の ID 基盤に組み込めるよう、複数の認証方式をサポートしています。

シングルサインオン（SSO）連携

Connect AI は、業界標準のプロバイダーを通じたシングルサインオンをサポートしています。SSO を有効化すると、ユーザーは Connect AI のログイン認証情報ではなく、自社で選択したプロバイダーを経由して認証されます。

対応する SSO プロバイダー：

- SAML 2.0 および OpenID Connect
- Microsoft Entra ID（旧 Azure AD）
- Google Workspace
- Active Directory Federation Services（ADFS）および AD/LDAP
- Ping Federate および Okta Workforce Identity Cloud

推奨：本番環境では SSO の有効化を

エンタープライズ環境では、SSO の有効化を推奨します。認証の一元化、既存のセキュリティポリシーの適用、ユーザープロビジョニングの簡素化、ID 基盤全体での一貫した監査証跡の維持が実現できます。お客様のアカウントで SSO を有効化するには、CData のアカウントチームまでお問い合わせください。

PKCE 付き OAuth 2.1

Connect AI は、認可フローを保護するために PKCE（Proof Key for Code Exchange）付きの OAuth 2.1 を採用しています。この新しい認可規格により、MCP 接続のセキュリティが以下のように強化されます。

- 認可コードの横取り攻撃を防止する
- パブリッククライアントでクライアントシークレットを保持する必要がなくなる
- 認証情報を露出させずにトークンを安全にリフレッシュできる

ユーザークレデンシャルモード

対応するデータソースについて、Connect AI は ユーザークレデンシャル（User Credentials）モードを提供しています。これは、共有のコネクション用認証情報ではなく、各ユーザー自身の認証情報での認証を要求するモードです。

対応データソース：Salesforce、Snowflake、SharePoint、Workday、Sage Intacct、RedShift、Paylocity。これら以外のソースで ユーザークレデンシャルモードを有効化する場合は、アカウントマネージャーまでお問い合わせください。

有効化した場合、何人のユーザーが認証しても ユーザークレデンシャルモードは1つのコネクションスロットとして扱われるため、セキュアでありながらコスト効率にも優れます。

SCIM 2.0 サポート：ID ライフサイクル管理の自動化

Connect AI は SCIM 2.0 によるプロビジョニングをサポートしており、Okta、Microsoft Entra ID、Ping Identity などの ID プロバイダーから、ユーザー、グループ、権限を直接同期できます。これにより、以下のメリットが得られます。

- ユーザーのライフサイクル管理が自動化され、手作業によるプロビジョニング／デプロビジョニングが不要になる
- 認証情報の残存リスクが解消される。ID プロバイダー側でユーザーが削除された瞬間に、Connect AI 側のアクセス権も失効する
- SOC 2 や ISO 27001 で必須とされる自動化されたアクセス制御の要件に適合する。セキュリティチームの承認を得るうえでの典型的なボトルネックを解消する

アクセス制御の設定

Connect AI は、最小権限の原則に基づき、ユーザーや AI エージェントが必要なデータにだけアクセスできるよう、多層のアクセス制御を提供しています。

ID パススルー

ID パススルー方式は、ロールベースアクセス制御（RBAC）をソース側に適用します。新しいシステムで権限を作り直すのではなく、Connect AI はソースシステム側の既存のアクセス制御をそのまま引き継ぎます。

RBAC パススルーのメリット：

- 権限体系をシステムごとに重複して持つ必要がない
- ソースシステム側の権限変更が、AI からのアクセスにも自動的に反映される
- 管理上の手間や設定の食い違い（configuration drift）が減る
- 権限管理の単一の情報源（single source of truth）が確保され、コンプライアンス監査が簡素化される

CRUD 操作のスコープ設定

ソースシステムの権限制御に加え、Connect AI では管理者が AI エージェントの実行可能な操作をさらに制限できます。Create（作成）、Read（読み取り）、Update（更新）、Delete（削除）の各操作について、ユーザーごと、またはコネクションごとに個別の制御が可能です。

操作	ユースケース	推奨設定
Create	新規レコードの作成、データ入力の自動化	自動化ワークフロー向けに選択的に有効化
Read	データ取得、レポート、分析	ほとんどのユースケースでデフォルトで有効化
Update	レコードの修正、ステータス更新	信頼できる特定のワークフローに限定
Delete	レコードの削除、データクリーンアップ	明示的に必要な場合を除き、無効化

ユーザー権限の設定

Connect AI は、各ユーザーが利用できるデータ種別をきめ細かく制御できる管理レイヤーを備えています。

- コネクションレベルのアクセス制御：各ユーザーがアクセスできるデータソースを制御
- スキーマレベルの制限：コネクション内の特定のスキーマだけにアクセスを限定
- 操作のスコープ設定：Create／Read／Update／Delete の権限を独立して制御
- ロールベースの割り当て：類似のアクセス要件を持つユーザーをグループ化

セキュアなアクセスのためのデータ整理

Connect AI には、アクセス対象のデータを整理・キュレーションする機能があり、セキュリティの枠組みを維持しつつ、AI エージェントに必要なデータだけを公開できます。

ワークスペース

ワークスペース（Workspaces）は、接続済みのデータソースからデータカタログを作成し、関連するデータ項目をまとめてバンドルする仕組みです。これにより、データサイロを減らしつつ、チーム横断での統制の取れたアクセスを促進できます。

セキュリティ上のメリット：

- テーブル、ビュー、派生ビューを論理的なコレクションにまとめられる
- 変換を加えずにデータを公開でき、元のカラム名やプロパティを維持できる
- 一意のエイリアスでアイテムを参照でき、識別が容易
- ワークスペース内のテーブルに対しては、必要に応じて CRUD のすべての操作を有効化できる

ベストプラクティス：目的特化型のワークスペースを作成する

事前定義された、複数ソースにまたがるデータコレクションを、特定のユースケースに合わせたカスタムツールと組み合わせて用意します。このアプローチは、用途を絞ったデータセットと汎用ツールセットを組み合わせることで、特化型エージェントの性能とセキュリティの両方を高めます。たとえば、営業レポートに必要な Salesforce のオブジェクトと Snowflake のテーブルだけを含む「Sales Analytics」ワークスペースを作成する、といった使い方が可能です。

派生ビュー

派生ビューは、アクセス時にデータを動的に取得する保存済みクエリです。
機密情報を事前にフィルタリングすることで、AIエージェントが参照できるデータを制御する強力な仕組みを提供します。

セキュリティ用途：

- 機密性の高いカラムやレコードを除外するためにデータを事前にフィルタリング
- 特定のユースケース向けに、一貫性のあるキュレーション済みデータサブセットを作成
- 公開するデータを絞り込むことで、攻撃対象領域を縮小
- データマスキングや集計の要件を適用する

権限の継承について：保存された派生ビューは、アカウント内のすべてのユーザーが派生ビュー一覧で確認できます。ただし、派生ビューを実行するユーザーは、その派生ビューが参照する各データソースに対する適切な権限を持っている必要があります。権限が不足している場合はエラーとなるため、派生ビューを介してソースシステムのアクセス制御を迂回することはできません。

カスタムツールとツールキット

Connect AI は、エージェントが何を参照し何を実行できるかを精密に制御できる、3階層のツールアーキテクチャを提供します。各層はガバナンス構造の中で異なる役割を担います。

- ユニバーサルツール（Universal Tools）：350以上の接続済みシステム全体で一貫して動作する、コンパクトでスキーマを認識するインターフェースを提供します。システムごとに固有の操作を何百も公開する代わりに、エージェントには正規化されたツールセットが提供されます。これにより、トークン消費を削減し、探索的なクエリの際の不必要なデータ露出を抑えられます。
- カスタムツール（Custom Tools）：特定のワークフロー向けに、用途特化型の操作を組織が独自に定義できます。各ツールは、データアクセスの上限を明示した、最適化済みのクエリを実行します。エージェントは生のスキーマを推論するのではなく、確定済みの操作を呼び出すだけで済みます。これにより、意図しないデータ露出が排除され、トークン使用量が削減され、複数ステップにわたるエージェント型ワークフローでも決定論的な実行が実現されます。

- ソースツール（Source Tools）：システムごとに厳格に定義された操作を公開し、承認済みのアクションに直接マッピングします。本番ワークフローに必要な、予測可能な実行、トランザクションの安全性、監査可能性を徹底します。

ツールキット（Toolkits）は、キュレーションされた MCP ツールのセットを、ガバナンス統制下の単一の MCP エンドポイントとして束ねます。特定のチームやユースケース向けに用途特化型に作られ、組織はどのコネクション、ツール、ロジックを公開するかを正確に定義し、AI ツールが直接接続する単一の MCP サーバー URL を発行できます。各ツールキットは専用の MCP サーバーとしてデプロイ可能で、エージェントが意図したスコープ内でのみ動作することを担保します。

クエリフェデレーションのセキュリティ

Connect AI は、複数のソースのデータを直接、オンデマンドで組み合わせるフェデレーテッドクエリを可能にします。フェデレーテッドクエリ使用時には、次の制御が働きます。

- フェデレーテッドクエリ内の各ソースシステムについて、それぞれ権限がチェックされる
- 結合されるすべてのデータソースへのアクセス権がユーザーに必要となる
- クエリで使用された各ソースシステムへのアクセスが監査ログに記録される

監査証跡とガバナンス

包括的な監査証跡は、コンプライアンス、セキュリティモニタリング、そして AI エージェントが自社データとどのようにやり取りしているかを把握するために不可欠です。Connect AI は、AI からのすべてのデータクエリについて、完全な可視性とログを提供します。

記録される内容

ログ要素	説明
ユーザーID	リクエストを行ったユーザーまたはエージェントの認証済み ID
セッションのアクティビティ	セッションの開始／終了時刻と、関連するアクション
ツールの呼び出し	どの MCP ツールが、どのパラメータで呼び出されたか
クエリの実行	アクセス先のソースシステムを含むクエリの完全なトレース
タイムスタンプ	すべての操作の正確な時刻
エラー報告	失敗したアクセス試行や、権限不足によるアクセス拒否

コンプライアンスモニタリング

監査証跡の機能は、主要なコンプライアンス要件をサポートします。

- SOC 2：アクセス制御とセキュリティモニタリングの証跡。「誰が、いつ、どのデータにアクセスしたか」を提示できる
- ISO 27001：情報セキュリティ事象のロギング。セキュリティ調査のための記録を維持できる
- GDPR：データアクセスの透明性。個人データの処理活動を文書化できる

Microsoft Agent 365 との連携

Microsoft Copilot Studio を利用している企業向けに、Connect AI は Microsoft Agent 365 と連携し、ガバナンス機能を拡張します。

- AI エージェント全体にわたるポリシー管理の一元化
- Connect AI と Copilot のアクティビティを統合した監査証跡
- Agent 365 のトレーシングで MCP ツールの呼び出しを可視化
- 接続されたすべてのシステムにわたる、一貫したガバナンスフレームワーク

インシデント対応とアクセス停止

認証情報の漏洩、AI エージェントの異常な挙動、不正アクセスの試みなど、セキュリティインシデントが発生した際には、対応のスピードと、対応できる手段の豊富さが重要になります。Connect AI は、迅速な封じ込めのために、複数のレベルでアクセスを停止できる仕組みを提供しています。

即時停止のオプション

Connect AI は、複数階層できめ細かいキルスイッチ（緊急停止スイッチ）を備えており、セキュリティチームは精度の高い封じ込めを実施できます。

レベル	アクション	ユースケース
ユーザー	個別ユーザーのアクセスを取り消し	アカウント侵害、退職者
コネクション	特定のデータソースを無効化	1つのシステムでの不審なアクティビティ
ワークスペース	ワークスペースへのアクセスを一時停止	チームやユースケース単位での隔離
アカウント全体	緊急時のアカウントロックダウン	重大な侵害や深刻なインシデント

ユーザーアクセスの取り消し：個別ユーザーの権限は、Connect AI の管理コンソールから取り消すことができます。ユーザーのアクセスが取り消されると、次の処理が即時に行われます。

- 割り当てられていたすべてのコネクションとワークスペースへのアクセスを失う
- CRUD 操作の権限が直ちに無効化される
- 以降のクエリは認可エラーを返す

コネクションレベルの無効化：管理者は、個別のデータソースコネクションを無効化できます。

ワークスペースの隔離：ワークスペースは一時停止が可能で、そのワークスペースに割り当てられたすべてのユーザーから、束ねられているデータソースへのアクセスを即座にブロックできます。

SSO とセッション管理

SSO 連携を利用している企業の場合、アクセス停止は ID プロバイダー経由で実行されます。ID プロバイダー（Entra ID、Okta など）でユーザーのアクセスを取り消すと、新規の認証はブロックされます。

推奨事項：セキュリティポリシー上、セッションの即時終了が必要な場合は、ID プロバイダーでのアクセス取り消しと、Connect AI 上でのユーザー削除を並行して実施し、新規セッションと既存セッションの両方がブロックされるようにしてください。

インシデント時の監査ログへのアクセス

セキュリティインシデント発生時には、関連ログへの迅速なアクセスが調査と対応の鍵となります。Connect AI の監査証跡には次の情報が記録されています。

- ユーザーID と認証イベント
- セッションの開始／終了時刻
- 実行されたすべてのツール呼び出しとクエリ
- アクセスされたデータソースと実行された操作
- 失敗したアクセス試行と権限不足によるアクセス拒否
- すべてのアクションに対する正確なタイムスタンプ

インシデント対応チェックリスト

Connect AI が関係するセキュリティインシデントに対応する際の手順です。

- 範囲の特定：インシデントが単一のユーザー、コネクション、もしくはより広範なアクセスに影響しているかを判断する
- 即時の封じ込め：適切なレベルのキルスイッチを使い、進行中の不正アクセスを停止する
- 証拠の保全：ログ保持に影響する変更を加える前に、関連する監査ログをエクスポートする
- 調査：影響を受けた期間の監査証跡をレビューし、インシデントの範囲を把握する
- 是正：根本原因に対処する（認証情報のローテーション、権限の更新、脆弱性のパッチ適用など）
- 復旧：対処が完了したことを確認したうえで、段階的にアクセスを再開する

セキュリティレビュー FAQ

セキュリティレビュアーからよく寄せられる質問と、その回答例です。

データはどこに保存されますか？

Connect AI はデータにインプレースでアクセスし、顧客データを保存、コピー、キャッシュすることは一切ありません。すべてのクエリはソースシステムに対してリアルタイムで実行されます。データが元の場所から離れることがないため、データ主権の要件は本質的に満たされます。

認証はどのように扱われますか？

Connect AI は主要な ID プロバイダーおよびプロトコル（SAML 2.0、OpenID Connect、Microsoft Entra ID、Okta など）との SSO 連携をサポートし、セキュアな認可フローのために PKCE 付き OAuth 2.1 を採用しています。データソースへのアクセスについては、ユーザークレデンシャルモードを採用することで個人単位の説明責任を担保します。

どのようなコンプライアンス認証を取得していますか？

CData は、第三者機関による SOC 2 Type II および ISO/IEC 27001:2022 のコンプライアンス監査を完了しています。監査報告書を含むセキュリティドキュメント一式は、リクエストに応じて提供可能です。

ペネトレーションテストは実施していますか？

はい。CData は独立した第三者のペネトレーションテスターを起用し、Connect AI のセキュリティ評価を定期的に実施しています。これに加え、外部監査の合間も、社内のセキュリティテストを継続的に実施しています。第三者評価のサマリーは NDA のもとで提供可能です。

不正アクセスをどのように防いでいますか？

Connect AI は RBAC パススルーを採用し、ソースシステム側の既存の権限をそのまま引き継ぎます。さらに、CRUD 操作のスコープ設定、コネクションレベルのアクセス制御、機密データを事前フィルタリングする派生ビューといった追加レイヤーがあります。ユーザーは、ソースシステム側で認可された範囲のデータのみ参照できます。

どのような暗号化を使用していますか？

保管時には AES-256 で暗号化し、転送時には TLS 1.3 を使用しています。なお、米国連邦政府の準拠要件で最低基準とされるのは AES-128 です。すべての認証情報は暗号化されて保存され、ログや応答に露出することは決してありません。

監査ログはどのように維持されていますか？

すべてのデータインタラクションについて、ユーザーID、セッションアクティビティ、ツール呼び出し、クエリ実行の詳細、タイムスタンプ、エラー報告がログに記録されます。これらのログは、SOC 2、ISO 27001、GDPR の各コンプライアンス要件を支えるものです。

プロンプトインジェクションのリスクへはどう対策していますか？

Connect AI には複数の保護策が組み込まれています。RBAC パススルーにより、仮にエージェントが操作されたとしても、そのユーザーがアクセス権を持っていないデータには到達できません。CRUD スコープ設定は破壊的操作を制限し、派生ビューはエージェントのコンテキストに渡される前に機密データをフィルタリングします。

セルフホスト型の MCP サーバーではなく、マネージドプラットフォームを使うのはなぜですか？

セルフホスト型の MCP サーバーは、サプライチェーンリスク（検証されていないコード）を抱え、標準化されたセキュリティ管理を欠き、認証と監査ログを独自に実装する必要があり、分散管理の負担も発生します。Connect AI は、セキュリティ、ガバナンス、コンプライアンスをマネージドサービスとして一元的に提供します。

導入チェックリスト

Connect AI の導入時に、セキュリティのベストプラクティスに沿った実装を実現するためのチェックリストです。

導入前

- 接続予定のデータソースと、それぞれの機密度を文書化する
- ユーザーグループと、それぞれに必要なアクセスレベルを特定する
- ソースシステム側の既存の RBAC 設定をレビューする
- SSO プロバイダーと認証要件を決定する
- 監査ログの保持期間とレビューポリシーを定める

認証の設定

- ID プロバイダーとの SSO 連携を有効化する
- 対応するデータソースについて ユーザークレデンシャルモードを設定する
- OAuth／PKCE フローが正しく動作することを検証する
- 代表的なユーザーアカウントで RBAC パススルーをテストする
- ID プロバイダーとの SCIM 2.0 プロビジョニングを設定し、ユーザーライフサイクル管理を自動化する

アクセス制御の設定

- データソースごとにユーザー権限を設定する
- CRUD 操作のスコープ設定を適用する（書き込みが必要でなければ、デフォルトでは読み取り専用にする）
- ユースケース／チームごとにワークスペースを作成する
- 機密データを事前フィルタリングする派生ビューを定義する

ガバナンスとモニタリング

- 監査ログの設定と保持期間を構成する
- 定期的な監査ログレビューのプロセスを確立する
- 異常なアクセスパターンに対するアラートを設定する
- セキュリティ事象に対するインシデント対応手順を文書化する

継続的な運用

- アクセスレビューと権限監査を定期的にスケジュールする
- ユーザーのオンボーディング／オフボーディングを継続的にモニタリングする
- データ要件の変化に応じて派生ビューをレビューおよび更新する
- Connect AI のセキュリティアップデートとベストプラクティスを最新の状態に保つ

総括

CData Connect AI は、本番環境での AI 導入を支えるデータ接続向けに必要となる、エンタープライズグレードのセキュリティ基盤を提供します。同プラットフォームに組み込まれたセキュリティ機能、すなわち SSO 連携、RBAC パススルー、SCIM プロビジョニング、CRUD スコープ設定、カスタムツールとツールキット、ワークスペース、派生ビュー、包括的な監査証跡を活用することで、IT 責任者は、データアクセスとコンプライアンス要件を統制下に置きながら、確信を持って AI エージェントを導入できます。

主なポイント

- マネージドプラットフォームにより、検証されていない MCP サーバーに起因するサプライチェーンリスクを排除できる
- インプレースアクセスによりデータが移動せず、ソースシステムの制御が変わらずそのまま効力を持つ
- RBAC パススルーによる ID ファーストのセキュリティ。権限体系を作り直す必要がない
- 多層のアクセス制御。ソース側の権限と Connect AI の CRUD スコープ設定を組み合わせられる
- ワークスペースと派生ビューによるデータキュレーション。必要なものだけを公開できる
- 包括的な監査証跡により、コンプライアンスとセキュリティモニタリングのための完全な可視性を確保
- Connect Gateway を通じて、オンプレミスのデータ接続も同じガバナンスレイヤーで統制可能

セキュリティキットのリクエスト

CData は、エンタープライズ向け評価のために、SOC 2 Type II レポート、ISO/IEC 27001:2022 認証ドキュメント、詳細なアーキテクチャ図を含む包括的なセキュリティキットを提供しています。セキュリティドキュメント一式のリクエストは、CData の営業担当までお問い合わせいただくか、jp.cdata.com/security をご覧ください。

jp.cdata.com

データアクセスとデータ連携のリーディングプロバイダー

CData Software は、データアクセスおよびデータ連携ソリューションのリーディングプロバイダーです。標準ベースのコネクターにより、データアクセスを効率化し、オンプレミスおよびクラウドのデータベース、SaaS、API、NoSQL、ビッグデータとの連携の煩雑さからお客様を解放します。