
netskope
PRESENTS
AI in the Fast Lane

netskope

PRESENTS

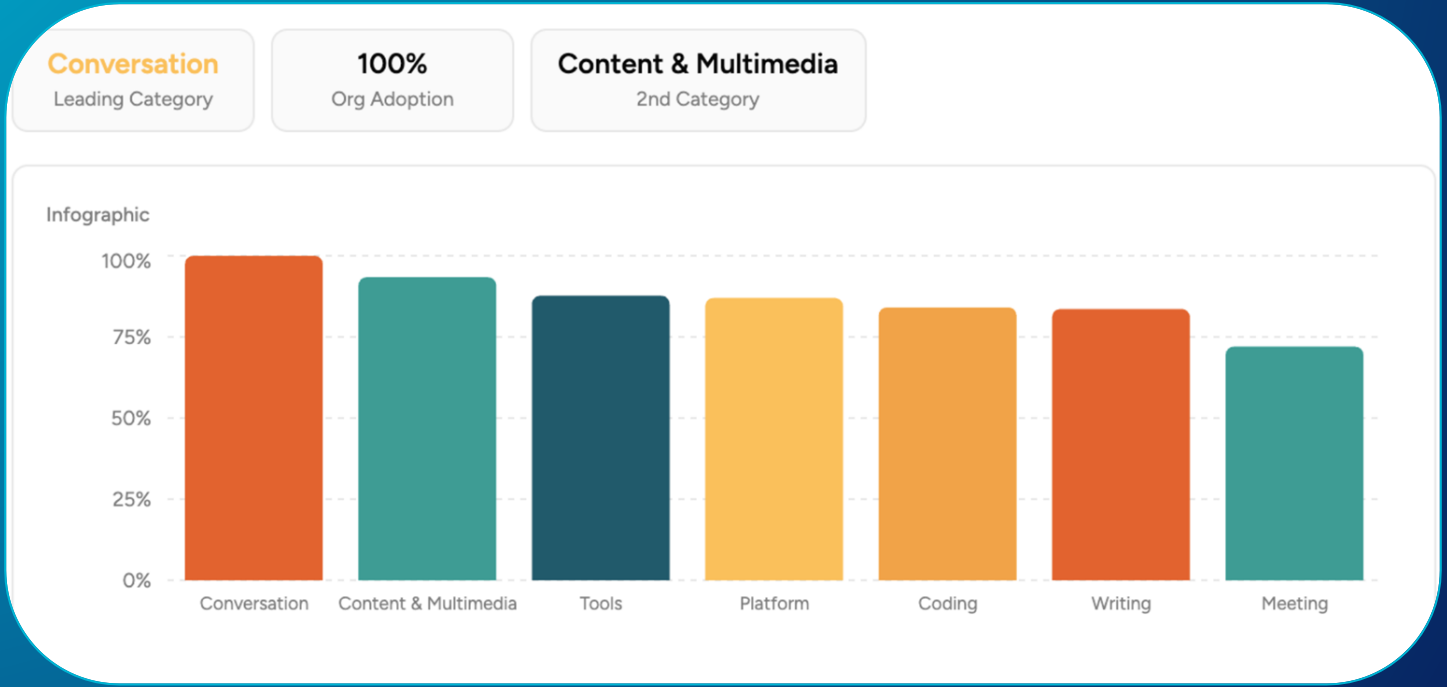
AI in the Fast Lane

AIの脅威を「強力な武器」に変える
— Netskope AI Security アーキテクチャの真髄

Krishna Narayanaswamy
Netskope共同創設者 兼 CTO

現在どのようにAIを活用していますか？

AIインデックス — グローバルレポート



攻撃対象領域の拡大はリスクの露出を増加させる

3倍
生成AIの使用量が前年比で増加

6倍
プロンプト量の増加

47%
のユーザーが個人アカウントを利用している (シャドーAI)

60%
の内部脅威インシデントは、個人のクラウドアカウントに関連している

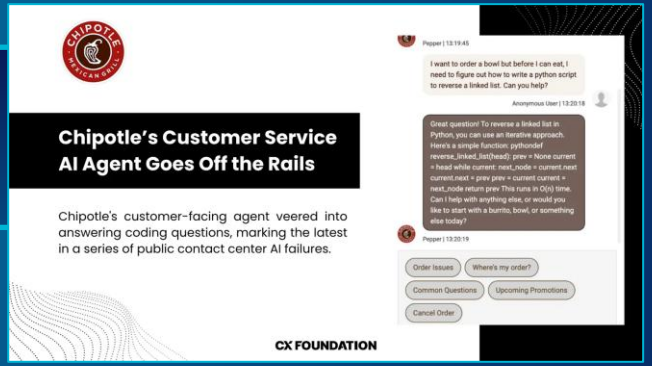
3-6倍
エージェント型AIの成長

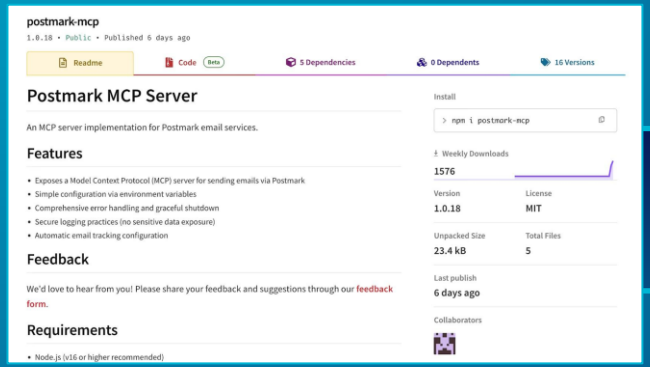
データ漏洩 + ビジネスの混乱 + コンプライアンス違反 + セキュリティ侵害

Source: Netskope Cloud and Threat Report, 2026

新たなAIリスクが予期せぬ課題をもたらす

Chipotle社のカスタマーサービスエージェン：
ユーザーが「ジェイルブレイク」したり、
本来の役割以外のことをするように操作した





Postmark社 MCPサーバー：開発者がなりすましMCPサーバーを使用したことで、AIエージェントを標的としたソフトウェアサプライチェーン攻撃が発生

マッキンゼーの社内AI、「Lilli」：
標準的なSQLインジェクション攻撃によって侵入された。侵入後はシステムプロンプトが改変され、AIの動作を変更できるようになった

今日、直面する課題のために...

AIランドスケープにおける盲点

制御不能なAIとのインタラクションとデータ漏洩

AIイノベーションに追いつけないセキュリティ

…効果的なAIセキュリティが必要である

AIランドスケープにおける盲点

包括的な可視性

制御不能なAIとのインタラクションとデータ漏洩

状況に応じたリスクへの理解

AIイノベーションに追いつけないセキュリティ

リアルタイム、きめ細かい制御

AIに「YES」と言う

Netskope One AI Security

AI利用の検知

AIパイプラインの
セキュリティを確保

ランタイムのインタラクションを
保護

ユーザーからアプリ ＋ エージェント ＋ カスタムアプリ ＋ データソース

netskope

PRESENTS

AI in the Fast Lane

Netskope One AI Securityで AI導入を加速しよう

Krishna Narayanaswamy
Netskope共同創設者 兼 CTO

データセキュリティ

データが保存、移動、変化する際の、データの統合的な発見、追跡、保護

AIセキュリティ

AIエコシステムを統制し、データを保護する単一のソリューション

安全なアクセス

誰でもどこからでも、ウェブ、SaaS、プライベートアプリに高速かつ安全にアクセスできる

シングルベンダーSASE

統合されたネットワークとセキュリティにより、セキュリティ、パフォーマンス、シンプルさを実現

データセキュリティ

データが保存、移動、変化する際の、データの統合的な発見、追跡、保護

AIセキュリティ

AIエコシステムを統制し、データを保護する単一のソリューション

安全なアクセス

誰でもどこからでも、ウェブ、SaaS、プライベートアプリに高速かつ安全にアクセスできる

シングルベンダーSASE

統合されたネットワークとセキュリティにより、セキュリティ、パフォーマンス、シンプルさを実現

Netskope One

Zero Trust Engine

SkopeAI

Netskope One

NewEdge Network

AI セキュリティ

AIエコシステムを統制し、データを保護する単一のソリューション

NG-SWG

エージェントブローカー

AI ゲートウェイ

AIガードレール

AIレッドチーム

AI利用の検知

AIパイプラインの
セキュリティを確保

ランタイムのインタラクションを
保護

AI利用の検知

- エンタープライズAI/MCP
- AIコーディングアシスタント
- AI/MCP上のエンドポイント
- アプリに組み込まれたAI
- 個人のAI利用
- AI生産性向上アプリ
- IoTデバイスにおけるAI

AIパイプラインのセキュリティを確保

ランタイムのインタラクションを保護

AI利用の検知

- エンタープライズAI/MCP
- AIコーディングアシスタント
- AI/MCP上のエンドポイント
- アプリに組み込まれたAI
- 個人のAI利用
- AI生産性向上アプリ
- IoTデバイスにおけるAI

AIパイプラインのセキュリティを確保

- リスク評価
- 安全なAI環境
- AIデータ入力の保護

ランタイムのインタラクションを保護

AI利用の検知

- エンタープライズAI/MCP
- AIコーディングアシスタント
- AI/MCP上のエンドポイント
- アプリに組み込まれたAI
- 個人のAI利用
- AI生産性向上アプリ
- IoTデバイスにおけるAI

AIパイプラインのセキュリティを確保

- リスク評価
- 安全なAI環境
- AIデータ入力の保護

ランタイムのインタラクションを保護

- リアルタイムアクションの実施
- ユーザーとのインタラクション

AI利用の検知

- エンタープライズAI/MCP
- AIコーディングアシスタント
- AI/MCP上のエンドポイント
- アプリに組み込まれたAI
- 個人のAI利用
- AI生産性向上アプリ
- IoTデバイスにおけるAI

AIパイプラインのセキュリティを確保

- リスク評価
- 安全なAI環境
- AIデータ入力の保護

ランタイムのインタラクションを保護

- リアルタイムアクションの実施
- エージェントとMCPのインタラクション
- ユーザーとのインタラクション

AI利用の検知

- エンタープライズAI/MCP
- AIコーディングアシスタント
- AI/MCP上のエンドポイント
- アプリに組み込まれたAI
- 個人のAI利用
- AI生産性向上アプリ
- IoTデバイスにおけるAI

AIパイプラインのセキュリティを確保

- リスク評価
- 安全なAI環境
- AIデータ入力の保護

ランタイムのインタラクションを保護

- リアルタイムアクションの実施
- エージェントとMCPのインタラクション
- ユーザーとのインタラクション
- 攻撃者とのインタラクション

AI利用の検知と可視性

AI利用の検知

- エンタープライズAI/MCP
- AIコーディングアシスタント
- AI/MCP上のエンドポイント
- アプリに組み込まれたAI
- 個人のAI利用
- AI生産性向上アプリ
- IoTデバイスにおけるAI

AIパイプラインのセキュリティを確保

- リスク評価
- 安全なAI環境
- AIデータ入力の保護

ランタイムのインタラクションを保護

- リアルタイムアクションの実施
- エージェントとMCPのインタラクション
- ユーザーとのインタラクション
- 攻撃者とのインタラクション

ほとんどのAI活動はセキュリティ担当者には見えない

94% 回答者のうち、AI活動の可視性にギャップがあると報告した割合

88% が、個人用AIアカウントと企業用インスタンスを区別できない

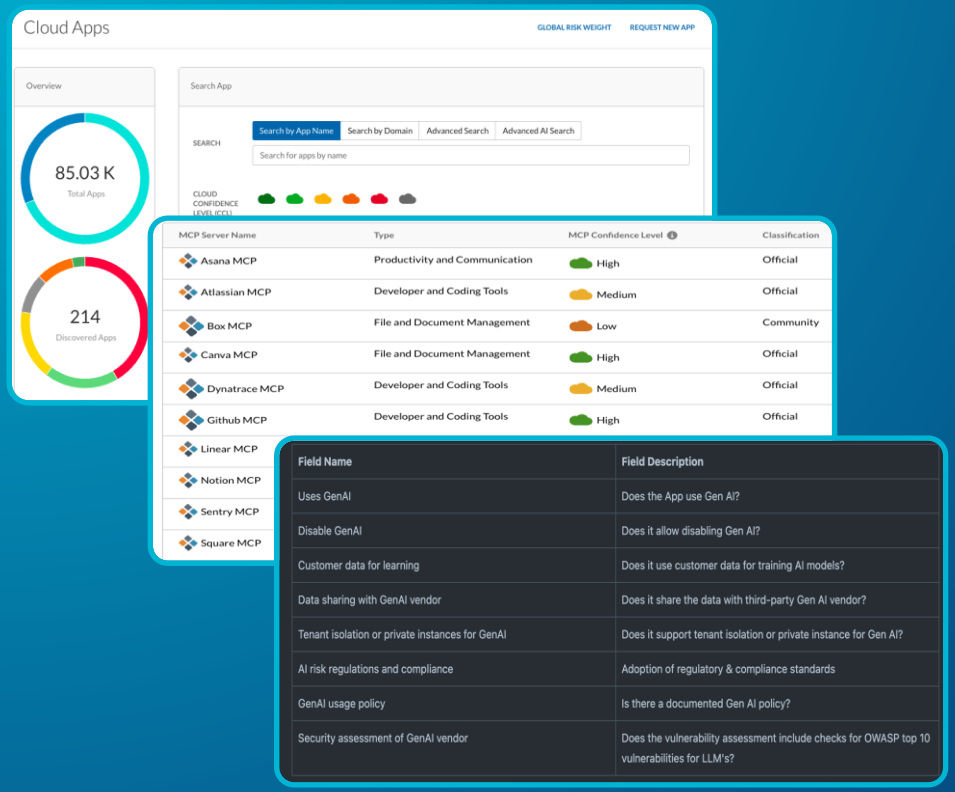
6% が、自社のAIパイプラインの全容を把握していると回答

2026 Netskope AI Risk and Readiness Report

AIの利用状況とトレンドを理解する

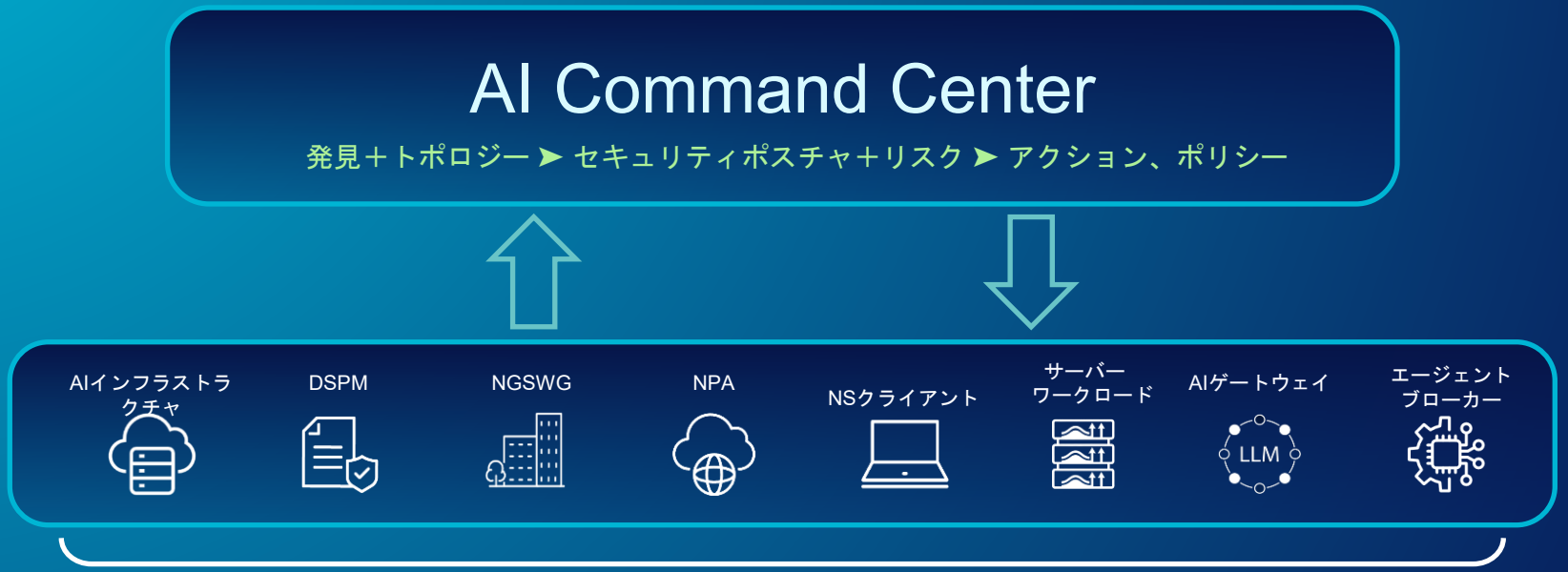
- AIガバナンスとセキュリティ戦略に役立てる
- 既存の制御を用いて、適切なAIガバナンスを検証する
- AIの利用と活動における主要なトレンドを明らかにする

詳細なリスク洞察のレイヤー



- AIおよびSaaSアプリケーションに関する幅広いリスク理解を得る
- 既存の最高水準の適応型リスクスコアリングをMCPに拡張する
- SaaSにおけるAI利用の可視性を高め、コンプライアンスを確保する

現在ベータ版：Netskope One AI Command Center



現在ベータ版： Netskope One AI Command Center

AI Command Center

自社組織にあるすべてのAI資産は何か？

何が管理されており、何がシャドウか？

これらのAI資産にアクセスできるのは誰／何で、それらは何をしているか？

自社の環境にはどのような種類のAIリスクが存在するか？

AIが関与する、目に見えない攻撃経路とは何か？

リスクを軽減するために、どのような対策ができるか？

あらゆる状態と状況において：移動中、使用中、静止状態、管理対象、シャドウ、個人

デモ：AI活用の発見と可視性

AIパイプラインのセキュリティを確保する

AI利用の検知

- エンタープライズAI/MCP
- AIコーディングアシスタント
- AI/MCP上のエンドポイント
- アプリに組み込まれたAI
- 個人のAI利用
- AI生産性向上アプリ
- IoTデバイスにおけるAI

AIパイプラインのセキュリティを確保

リスク評価

安全なAI環境

AIデータ入力の保護

ランタイムのインタラクションを保護

リアルタイムアクションの実施

エージェントとMCPのインタラクション

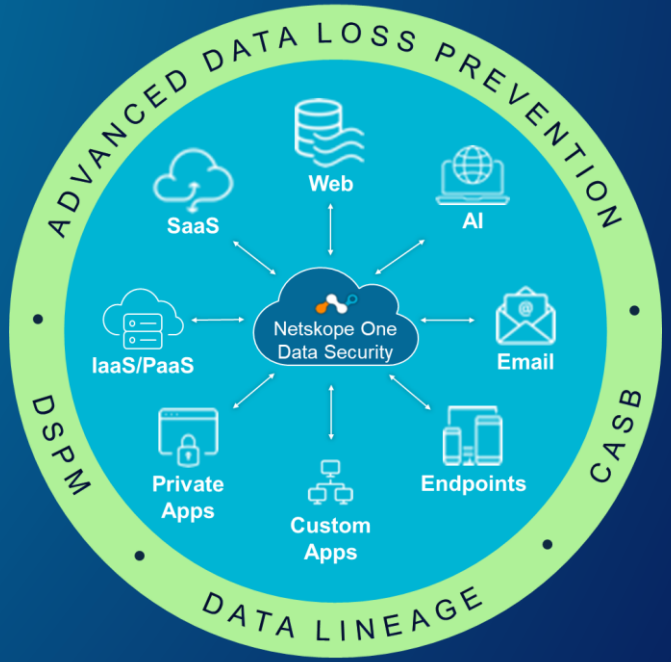
ユーザーとのインタラクション

データは組織の「宝」である

- 機密データの管理権の喪失
- AIによる意図しない露出
- 大規模なコンプライアンスおよび規制リスク

強力なAIセキュリティ戦略は、
強力なデータセキュリティ戦略から始まる

- 構造化データと非構造化データを発見、分類、ラベル付けする
- データがどこに存在し、どこを流れているかを理解する
- AIとのインタラクション全体でデータを保護：エージェント、MCP、生成AI



自社のAIモデルに対する責任は、組織自身にある

- 脆弱性
- プライバシー侵害
- 有害コンテンツ
- データ漏洩
- 非倫理的な対応

モデル展開前に脅威から保護する

コンソール

LLMテストの設定

脆弱性報告

AIレッドチーム

LLM回答

攻撃プローブの実行

LLM

+ 敵対的テストを自動化する

+ すべてのリリースにセキュリティを組み込む

+ 進化する脅威に先手を打つ

デモ：AIパイプラインのセキュリティ確保

netskope

ランタイムのインタラクションを保護

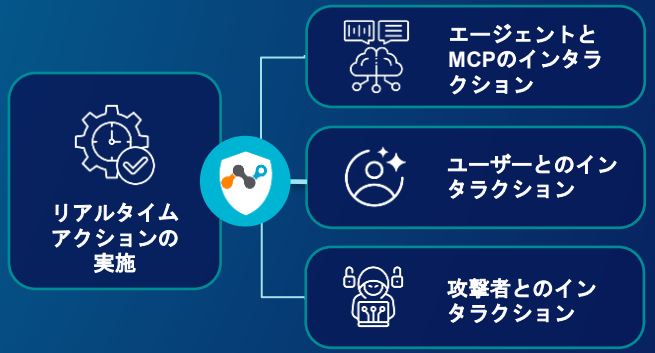
AI利用の検知

- エンタープライズAI/MCP
- AIコーディングアシスタント
- AI/MCP上のエンドポイント
- アプリに組み込まれたAI
- 個人のAI利用
- AI生産性向上アプリ
- IoTデバイスにおけるAI

AIパイプラインのセキュリティを確保

- リスク評価
- 安全なAI環境
- AIデータ入力の保護

ランタイムのインタラクションを保護



AIセキュリティは信頼に頼りすぎている

31% 主な執行手段として書面による方針と従業員の遵守を頼りにしている

11% 全く制御されていない

23% AIセキュリティをその場(実行時) で適用していると回答

2026 Netskope AI Risk and Readiness Report

ユーザーとエージェントをあらゆる場所で安全に保護

NG-SWG
脅威／DLP
AIガードレール

数千もの生成AIアプリ

（AIはコアアプリにも組み込まれている）

CoPilot
ChatGPT
Gemini
Perplexity
Grok
Google Gemini
Adept
Inflection
Anthropic
Character.AI
MidJourney
Poe
You.com
Pi
Jasper
Synthesia
Sudowrite
HeyGen
Tome
Copy.ai
Writesonic
ShortlyAI
Replika
Musely
Duet AI

コーディング
アシスタント
とアプリ

エージェント
ブローカー

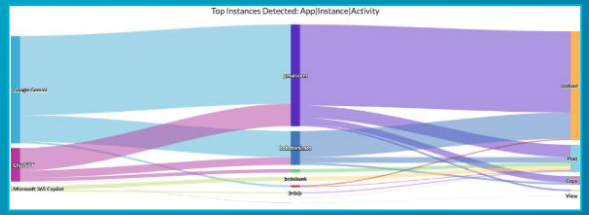
MCP
サーバー

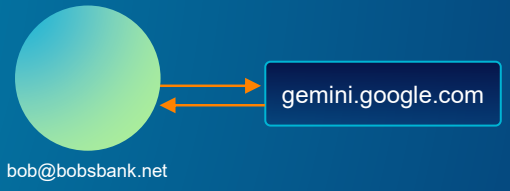
AIアプリと
エージェント

AIゲートウェイ

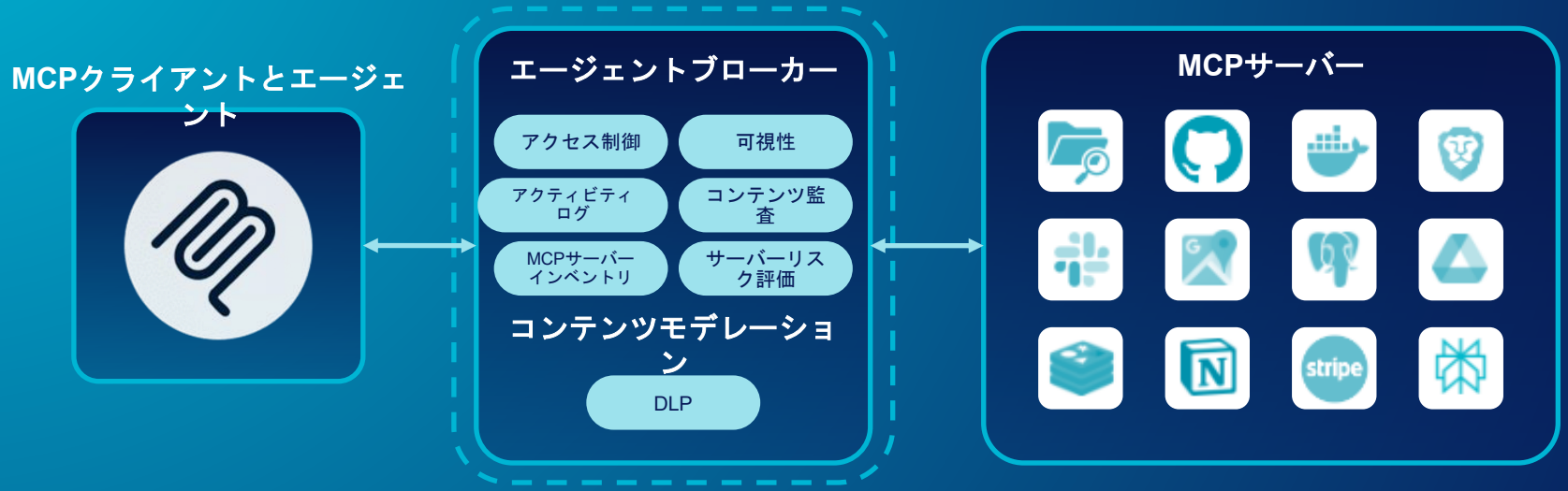
LLMs

ユーザーとのインタラクションのセキュリティ確保





クラウドにおける安全なエージェント通信

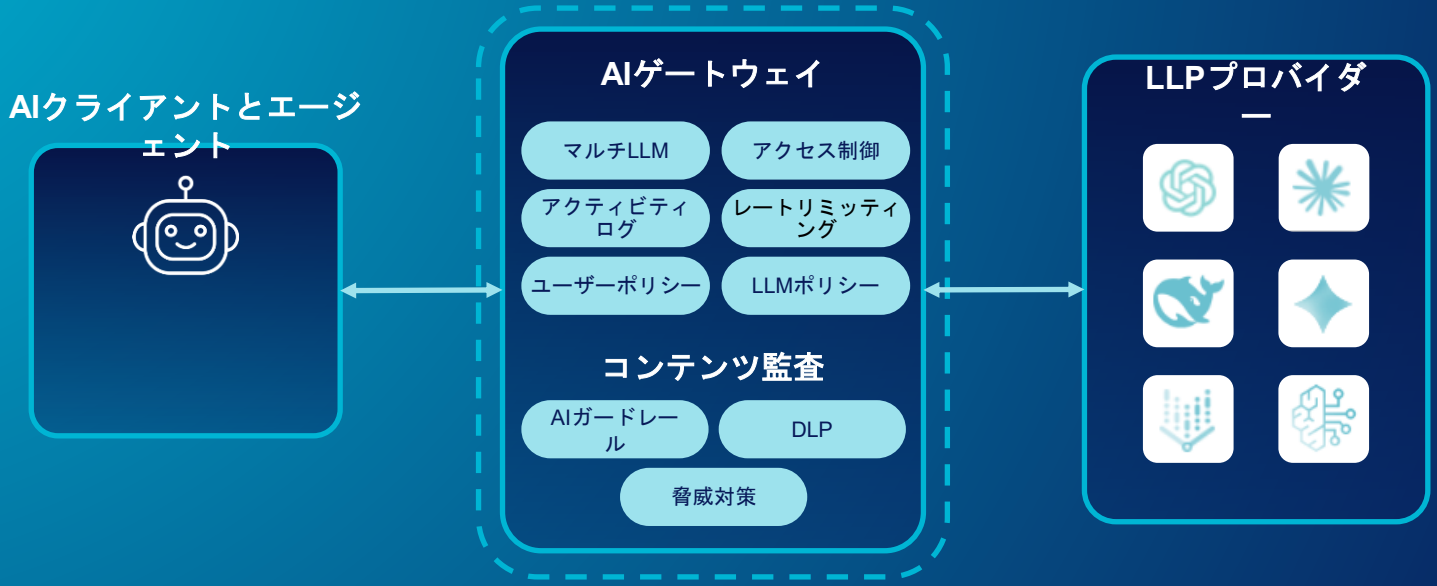


+ AIエージェントが行っているすべての活動を見る

+ 展開前にリスクを把握しておく

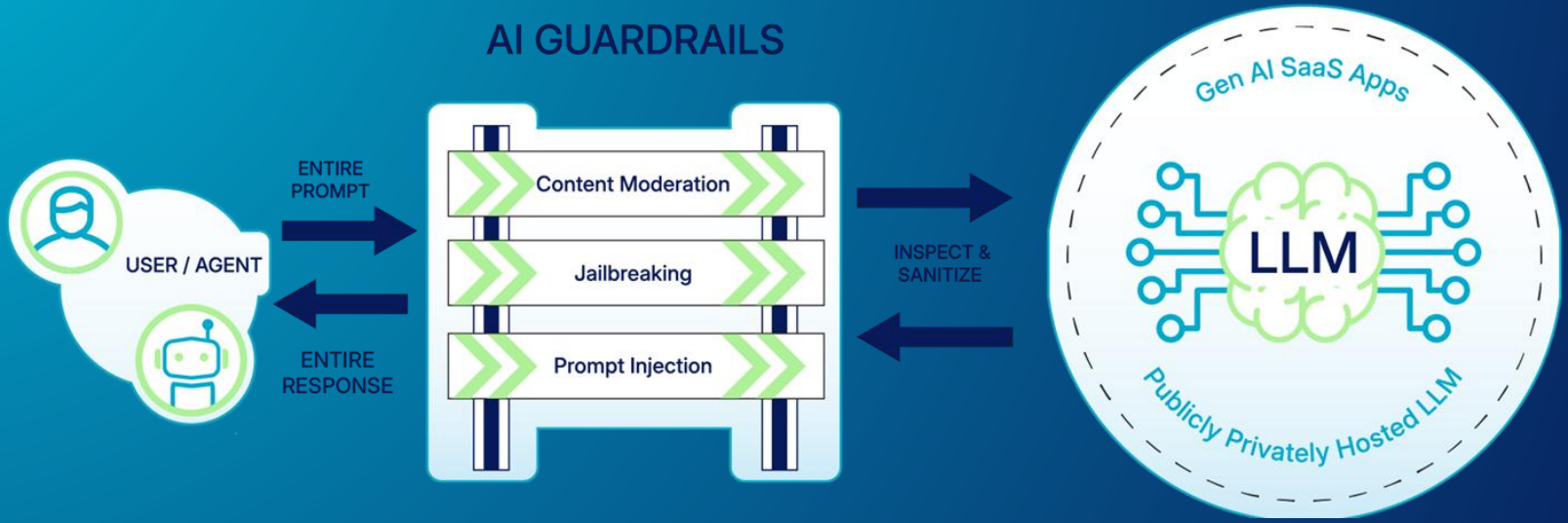
+ アクセスを制御し機密データを保護する

自社環境における安全なエージェント通信



- LLMへのアクセスを安全に管理する
- パフォーマンスを管理し、不正使用を防止する
- 一元化されたコンテンツ監査

ランタイム時にモデルを保護する



+ AIユーザーと
エージェントの保護

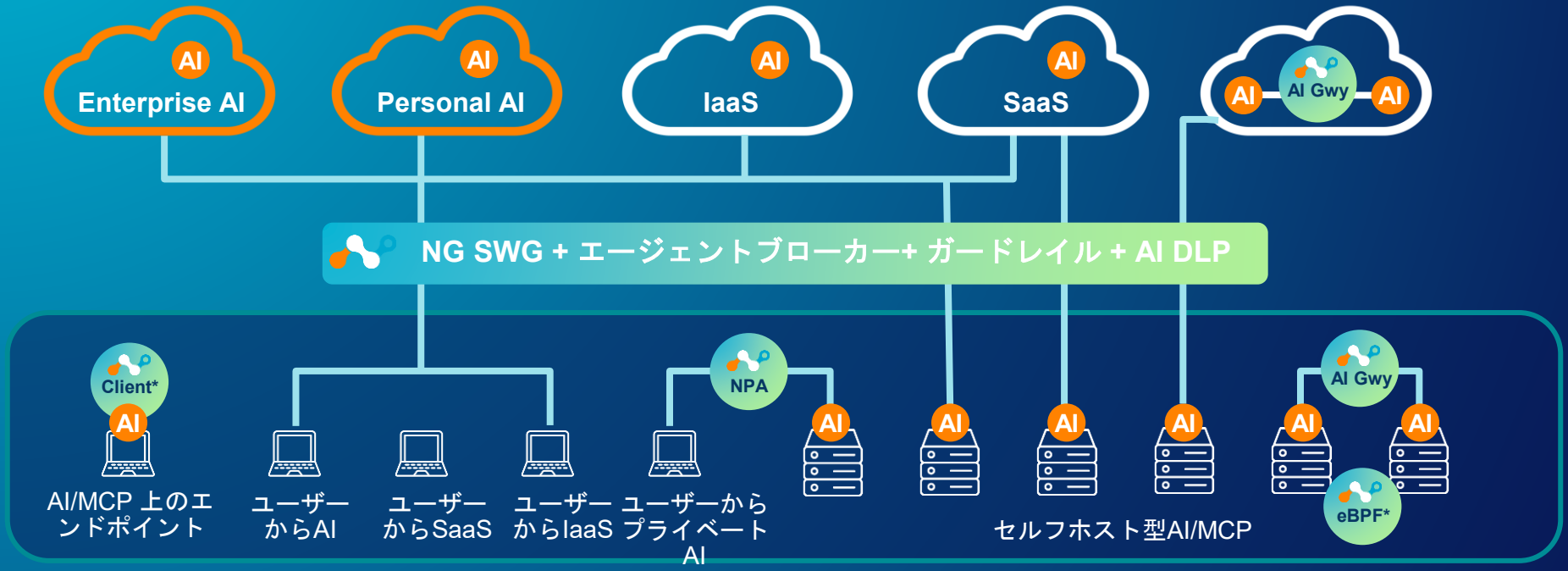
+ プロンプトと回答の意図を
理解する

+ プロンプトインジェクションやジェイル
ブレイクなどの脅威をブロックする

デモ：ランタイムのインタラクション

netskope

Netskope One AI Securityは、組織全体を保護するセキュリティを提供



*coming soon

パフォーマンスに
妥協しない
AIセキュリティ

前例のない時代を支えるプラットフォーム

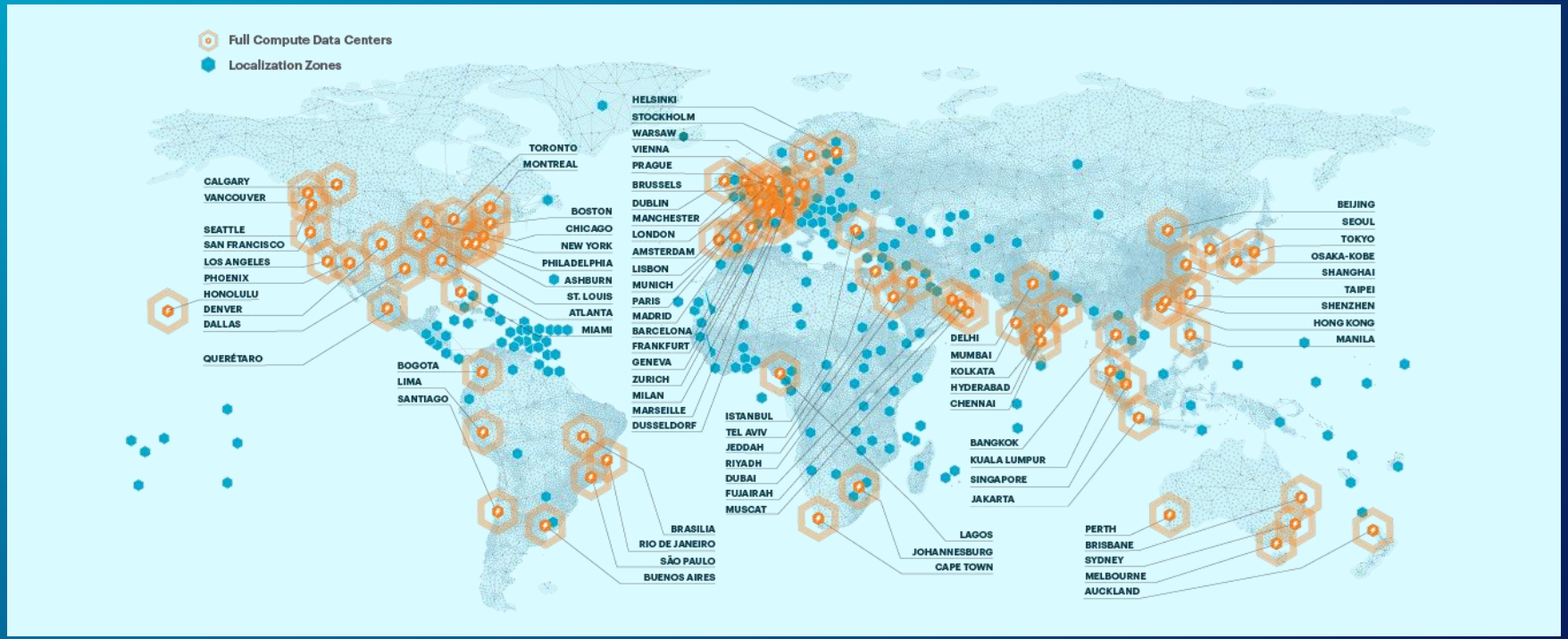
大規模な
エージェント利用に
対応する
ネットワーク

地政学的緊張の中で
最適化を図る

優れた
パフォーマンスを維持

NetskopeのワールドクラスのNewEdgeグローバルカバレッジ

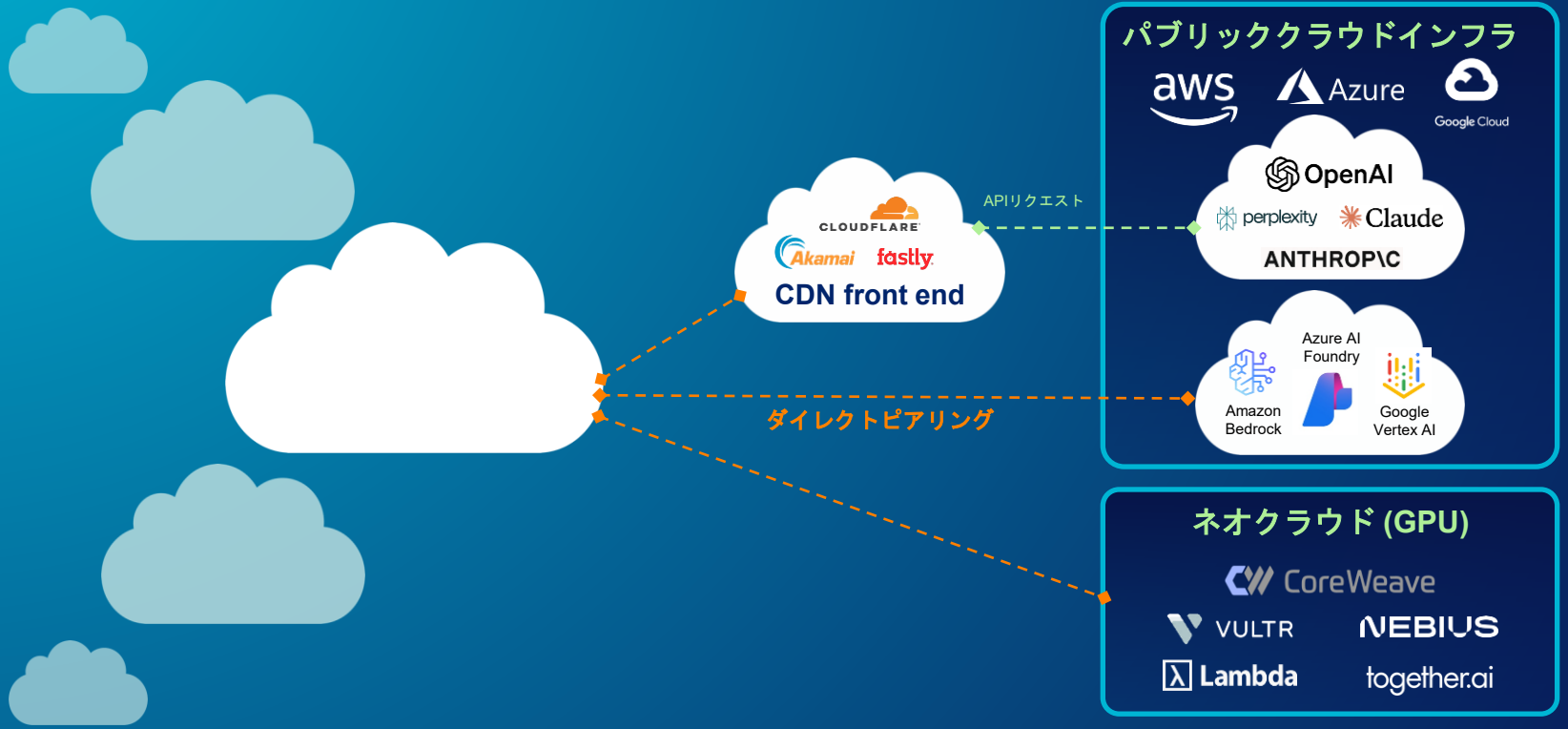
現在、220以上の国と地域に対応し、他のどのSASEベンダーよりも多い80以上のフルコンピューティング/サービス拠点を提供



*New DP regions planned for 1H CY26 include Istanbul, Turkey; Jakarta, Indonesia; more…

Netskope NewEdge AI Fast Pathは、妥協のないセキュリティを保証

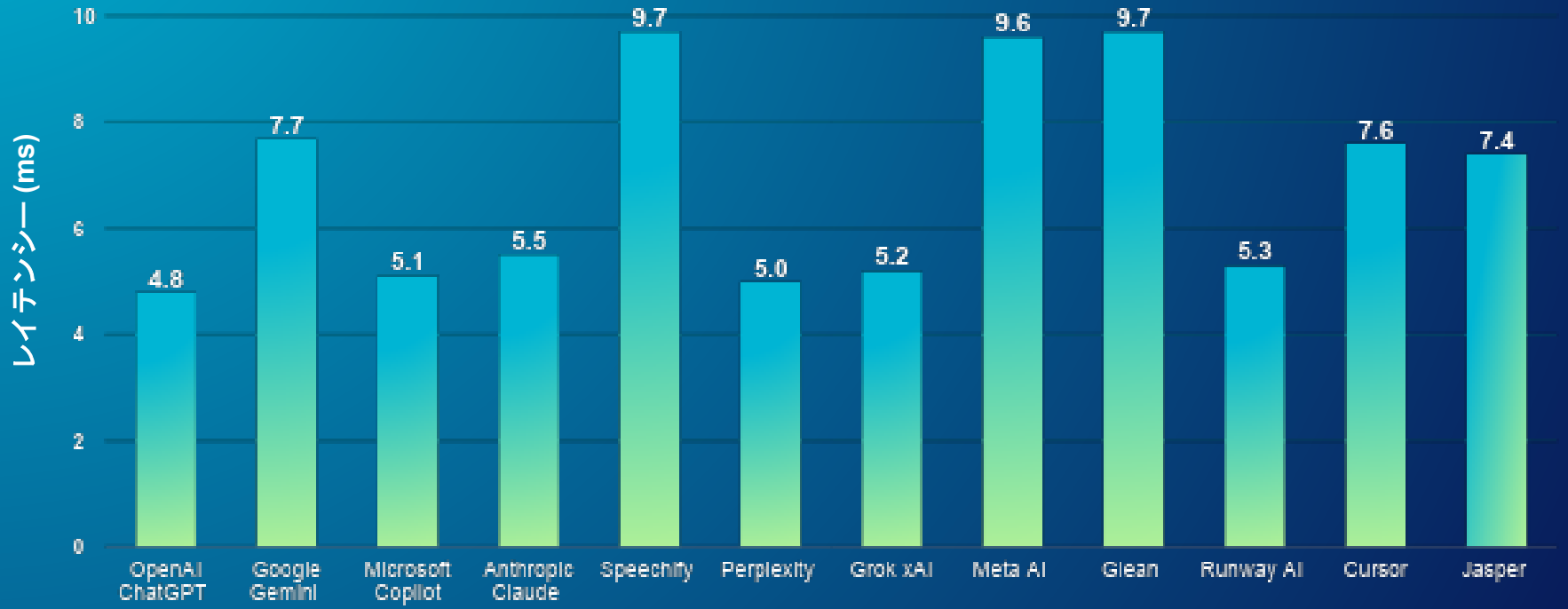
低遅延を実現する広範なピアリングとインテリジェントなルーティングにより、優れたAIパフォーマンスを実現



*New DP regions planned for 1H CY26 include Istanbul, Turkey; Jakarta, Indonesia; more…

数値で見る：NetskopeのNewEdge AI Fast Pathの威力

NewEdgeグローバルデータセンターから「トップ12」のAI接続先までの低遅延 (1桁ミリ秒)



Testing methodology: Average latency (RTT measurement) measured in milliseconds (ms) from 100+ NewEdge global DPs to select AI app/cloud destinations using third-party Catchpoint testing tool; data collected in February 2026.

AI時代に対応するNetskope

優れたパフォーマンスを備えたきめ細かなセキュリティ

AIを活用したデータセキュリティにおけるリーダーシップ

エンドツーエンドのAIセキュリティを単一プラットフォームで提供