「便利だから使う」を「安心して使い倒す」へ
― AI時代のBox活用とデータ中心セキュリティの極意

Mick Etoh, Ph.D.

CXO Advisor, Netskope, Inc.
7/16/2026

なぜ、Box × Netskope なのか

Box ＝ 中身を守る
誰が・どのファイルを・どこまで見てよいか（権限とガバナンス）

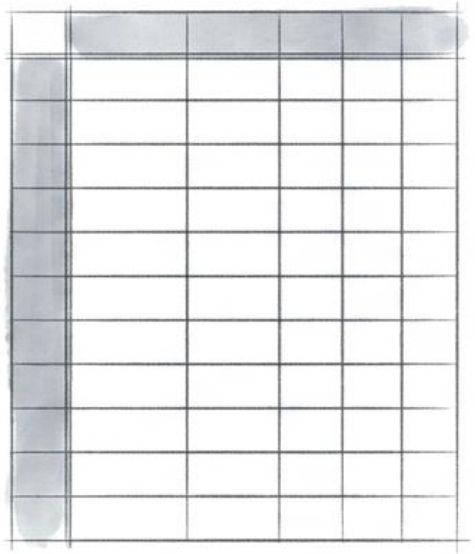
Netskope ＝ 通信と挙動を見る
TLSの中身まで復号し、何が・どこへ・どう動いたかを可視化・制御（インライン＋UEBA）

AI時代 ＝ 出入りするのは人だけではない
AIエージェントが自律的にデータへアクセスする。だから両方が要る

企業データの90%は、未開拓の「非構造化データ」である

有効活用されるべき
価値ある情報源は、
ここにある。

10% 構造化データ（データベース）



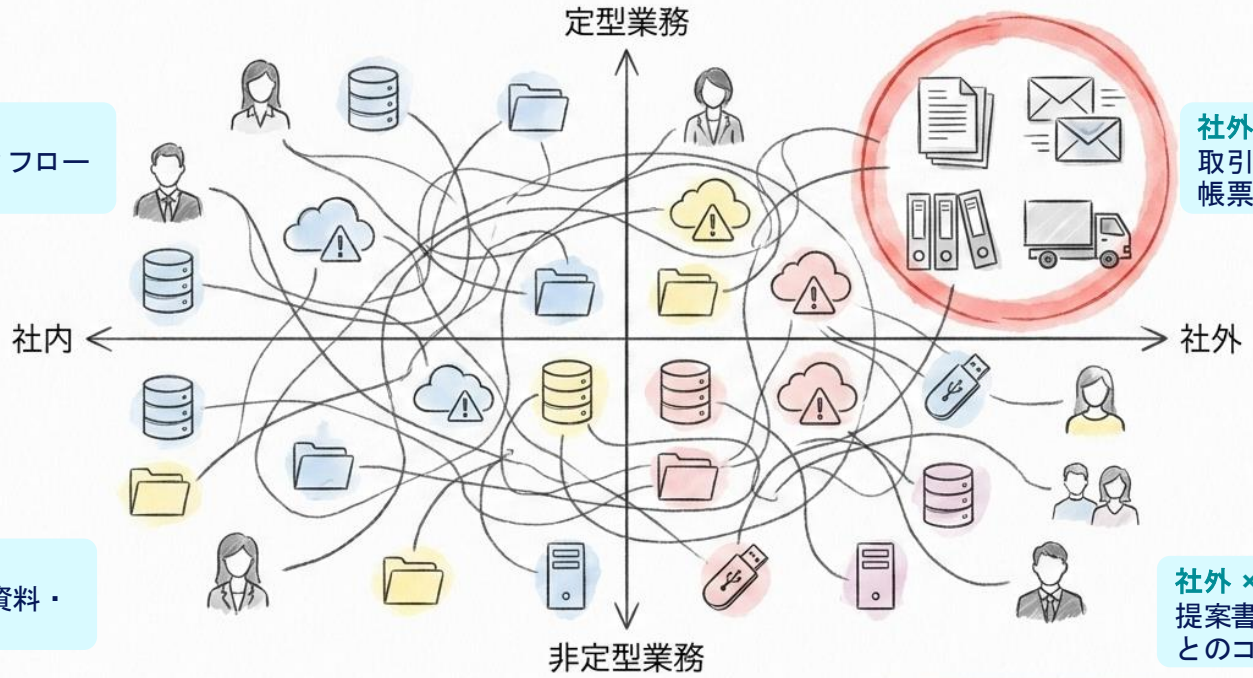
90% 非構造化データ（ドキュメント、画像、音声など）

90%はIDCのアナリスト推計（2023）

DX推進がもたらした弊害：「サイロ化」という新たな迷宮

社内 × 定型
基幹システム・ワークフロー・定例レポート

社外 × 定型
取引先との受発注・請求書・帳票（メール添付常態化）



社内 × 非定型
企画書・議事録・設計資料・チャットでの共有

社外 × 非定型
提案書・契約ドラフト・外部とのコラボレーション

各アプリケーション（Microsoft 365, Salesforce, Slackなど）が独自の保管庫を持つことで、ファイルが分散し、システム間の「見えない壁」が生まれている。

YouTube動画（PIVOT公式チャンネルでのBox Japan佐藤社長のプレゼンより描画

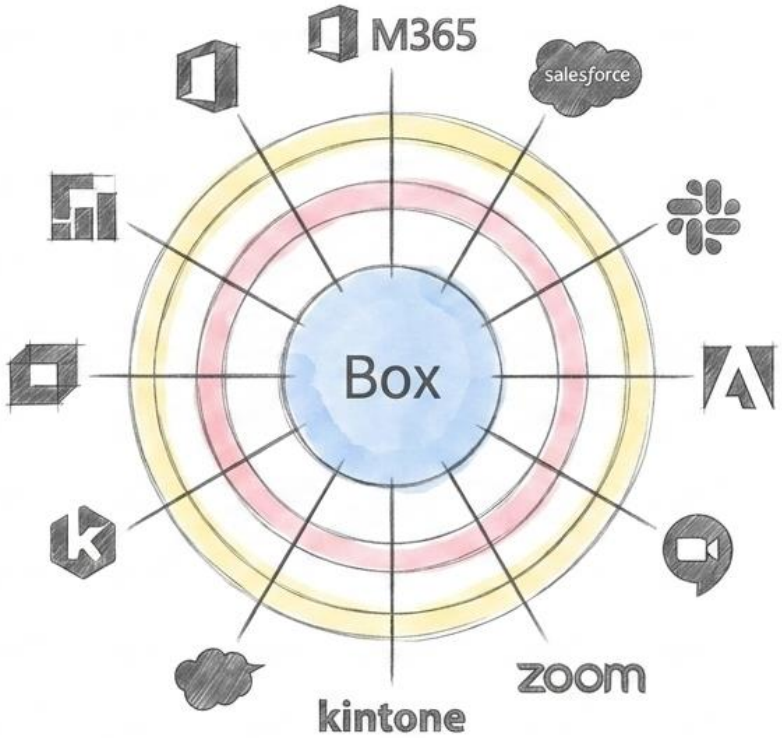
生成AI最大の壁：「アクセス制御」なきAI連携は情報漏洩に直結する

ファイルとLLM（大規模言語モデル）の相性は抜群。しかし、権限設定が曖昧なサイロ化されたデータをAIに読み込ませることは、機密文書の社内漏洩リスクを伴う。

AIを安全に機能させるには、コンテンツの「一元管理」と「厳密なアクセス権限の適用」が不可欠である。

業務プロセスを変えず、コンテンツのみを中央集権化する

1,500以上の
連携ソリューション
（コネクター）。



アプリケーションと
コンテンツの置き場を
分離するアーキテクチャ。

M365やSalesforce、
複合機（FAX自動格納）
など、使い慣れたツール
から意識することなく
Boxへデータを一元化。

基盤の確立：「コンテンツの城」としてのBox

正本の一元管理

企業の最も重要な機密情報（財務資料、顧客情報、設計書）を、一つの強固な環境に集約。

7段階の細粒度な権限設定

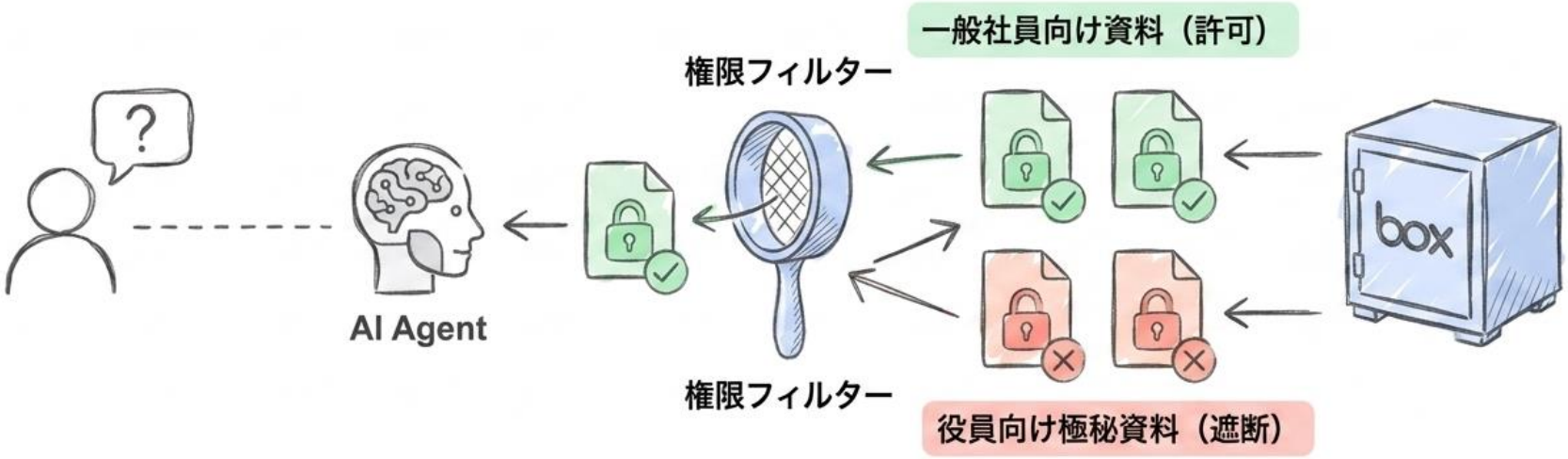
閲覧のみ、ダウンロード禁止、編集可など、役割に応じた厳密なアクセス制御をファイル単位で適用。

コンテキストベースの防御

ファイル内の文脈を自動検知し、機密分類ラベルを自動付与。

誰がどのデータに触れてよいかを完璧にコントロールする、強固な「入口の防御」。

AIへの権限継承：Security-Trimmed Search



権限の完全な引き継ぎ

ユーザーが持つアクセス権限をAIエージェントの検索クエリにそのまま反映。

MCP連携のブリッジ

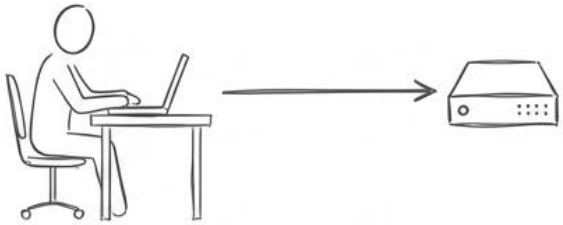
AIが既存のセキュリティポリシーを尊重するための標準化されたプロトコル。

安全な回答生成

一般社員の検索に極秘ドキュメントが混入するリスクを根本から排除。

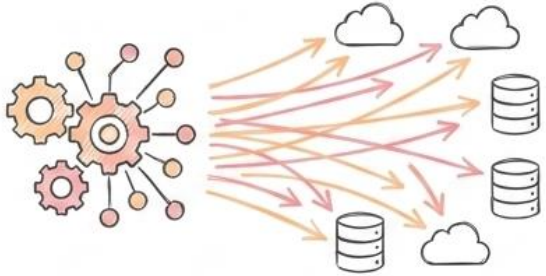
従来型セキュリティの限界：「非ヒューマントラフィック」

人間のトラフィック（Human）



- ブラウザ操作が中心
- 可視化しやすく、行動が予測可能
- 単一のサービスを利用する

AIのトラフィック（Non-Human / MCP）

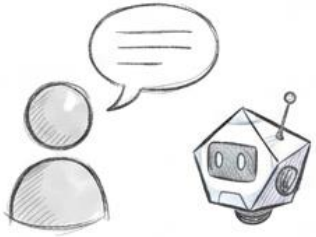


- APIやMCPによる自律的な通信
- 暗号化されたトンネルを通り、高速かつ大量のデータを取得
- 複数の外部ツールやLLMを横断して自律的につなぎ合わせる

結論：TLSで暗号化されたAIの通信は、従来のネットワーク監視では単なるブラックボックスとなり、実態が全く把握できない。

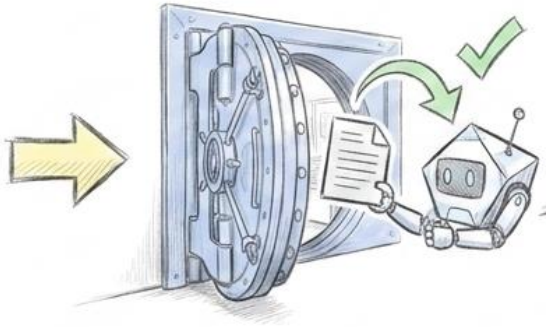
リスクシナリオ 1：過剰権限エージェントによる情報流出

指示



「過去の契約書のM&A条項を要約して」とAIに指示（善意の行動）

合法的取得



エージェントは正当な権限を利用し、Boxから機密文書を読み出す。

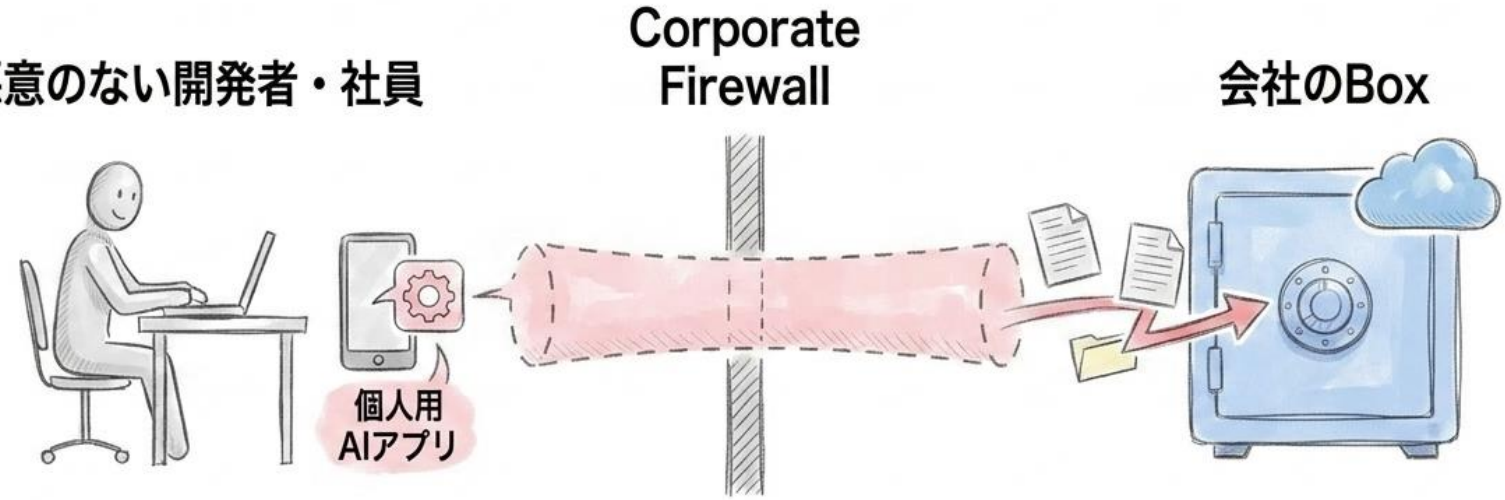
意図せぬ外部送信

要約を生成するため、エージェントが機密データを会社の管理外にあるパブリックAIへ自律的に送信してしまう。

目的達成のための自律的な行動が、結果として情報漏洩に直結する。

調査項目実態データ（Teleport社調査、2026年）セキュリティへの影響
インシデント発生率過剰権限のAIを持つ企業は76%、最小権限を適用している企業は17%

リスクシナリオ 2：シャドーMCPの侵入



個人AIの無断接続

社員が悪意なく、個人のAIクライアントに公開MCPコネクタを設定し、会社のBoxへ直接接続する。

シャドーMCPの誕生

会社の承認を受けていないAI環境へ、社内データが直接流れ込む経路が完成してしまう。

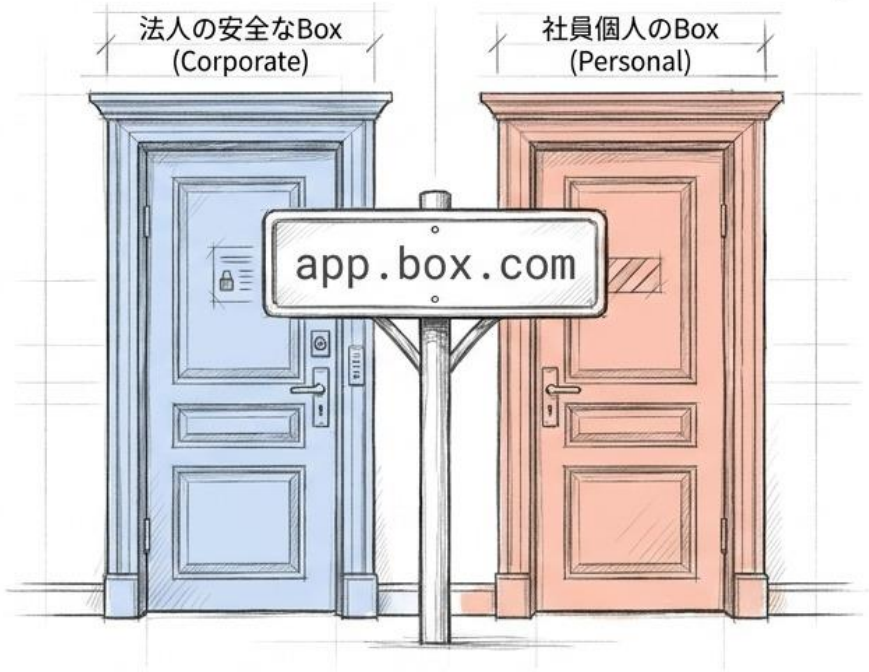
制御不能なデータフロー

入力データが外部でどのように学習され、どこに保存されるか、企業側で一切追跡・統制できなくなる。

同じURLの裏に潜む「2つの顔」：境界防御の限界

従来のファイアウォールや一般的なプロキシは、「どのURL（例: app.box.com）にアクセスしているか」というWebサイトの単位でしか通信を判別できません。

従来型プロキシの視界: URLという「表札」しか見えない

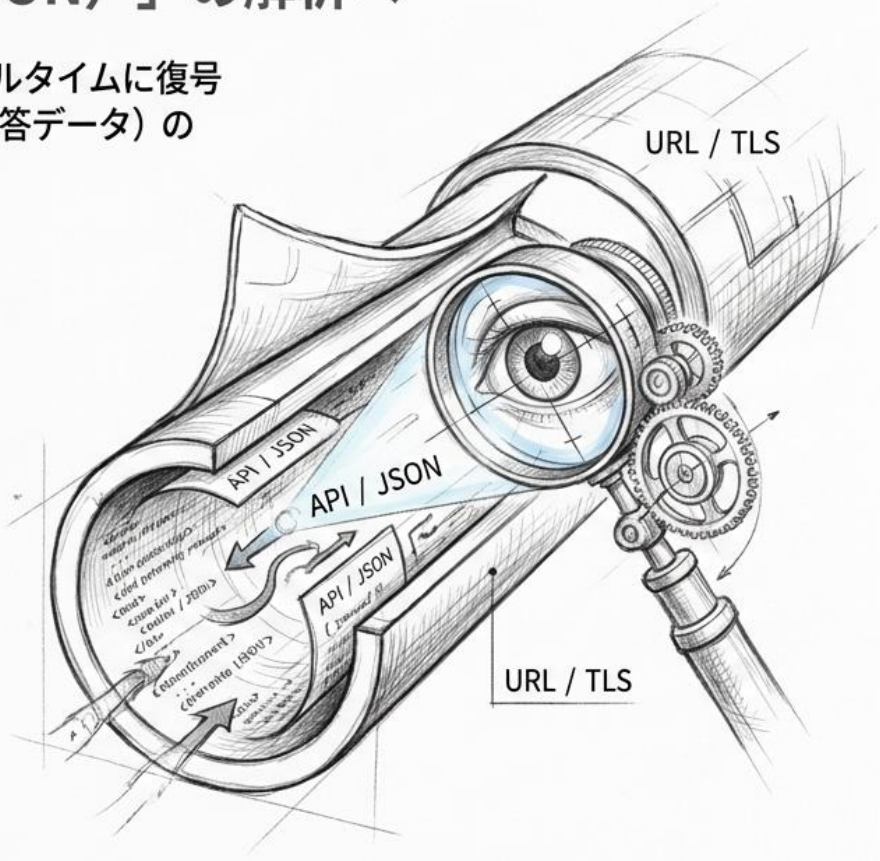


同じサービスを使っている限り、従来技術ではこの2つを区別することは不可能

URLベースから「通信の中身（API/JSON）」の解析へ

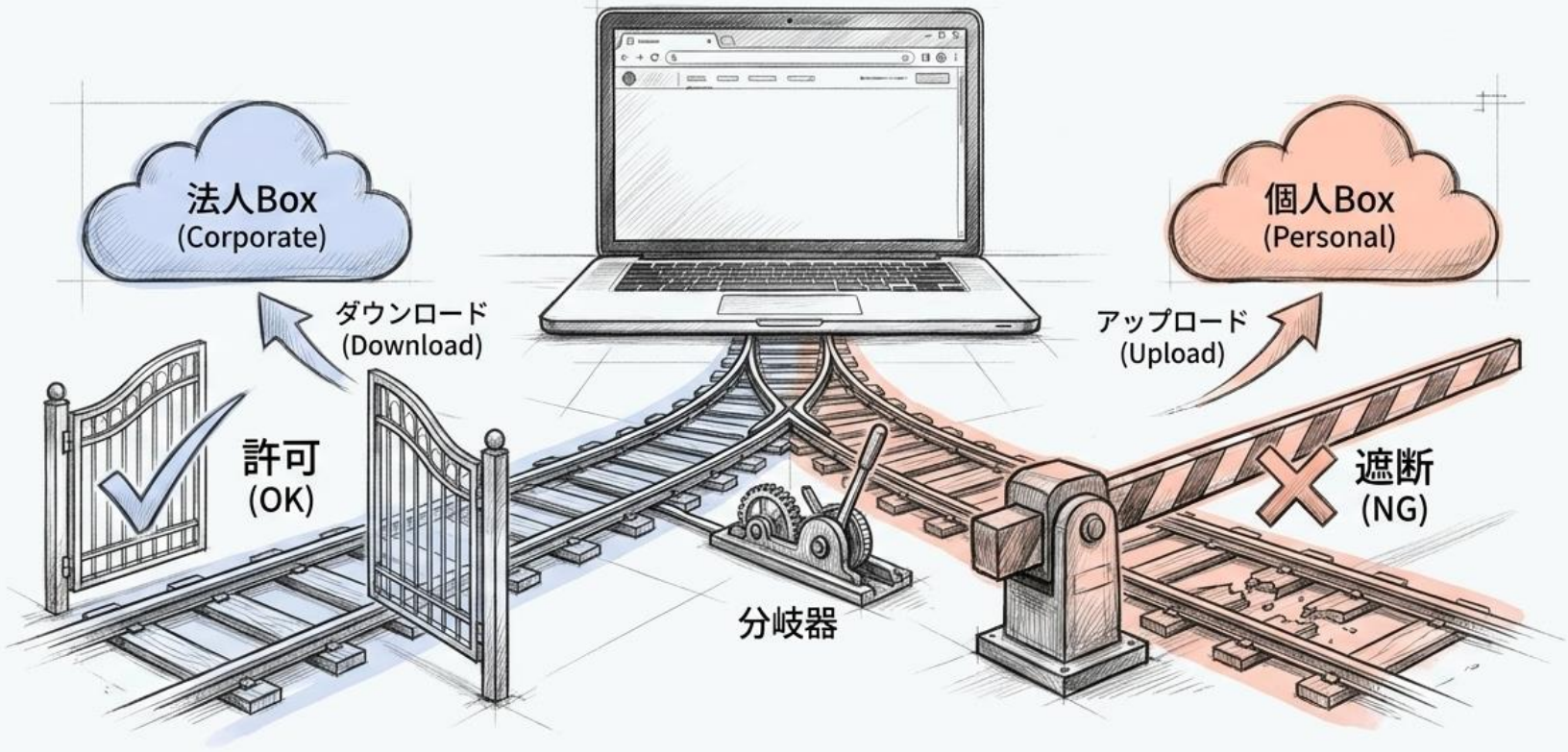
Netskopeは通信経路（インライン）でTLS暗号化通信をリアルタイムに復号し、URLの先にあるAPIコール（命令）やJSONレスポンス（応答データ）の深部まで潜り込んで検査します。

比較次元	従来型の境界防御 (FW/一般的なプロキシ)	Netskope (Instance Awareness)
可視化の単位	Webサイト・URL単位 (例: app.box.com)	**動作・API・JSON ペイロードの深部**
識別の解像度	「Boxを使っている」 ことしか分からない	**「法人用Boxか、 個人のBoxか」を 瞬時に判別**
アクセス制御	サイト全体の「許可」 または「遮断」 (ALL or NOTHING)	**アクティビティ単位** (例: ダウンロードは許可、 アップロードは遮断)
AI対応	暗号化された通信の 塊にしか見えない	**MCP/APIの非ヒト トラフィックを リアルタイム復号・検証**



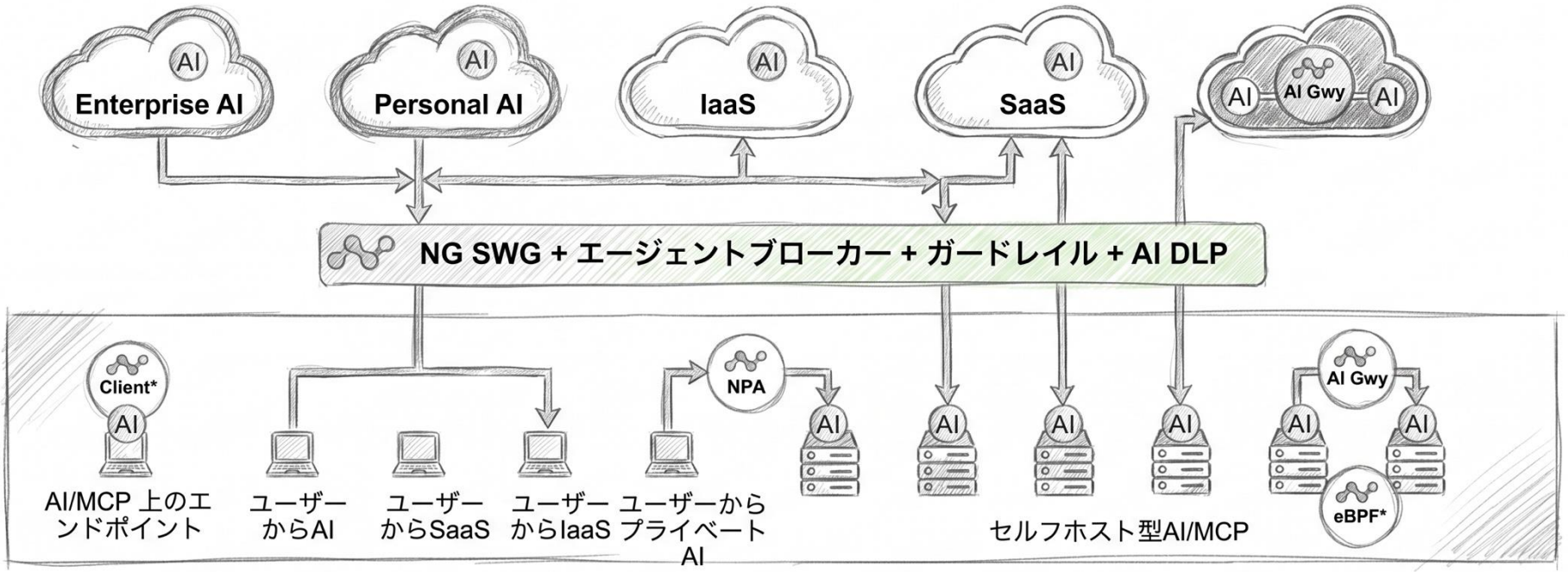
防御シナリオ 1：業務を止めないピンポイントの「防壁」

同一ブラウザ、同一アプリ上であっても、宛先インスタンスの違いを相関検知し、狙い撃ちで遮断します。



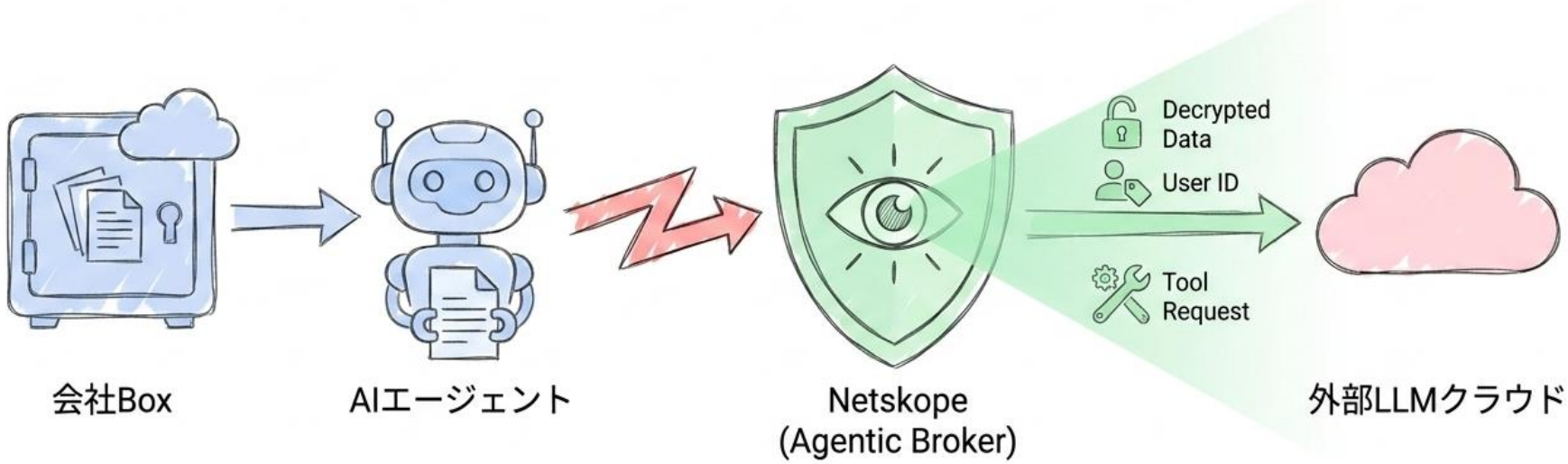
業務の利便性を損なわずに、個人アカウント側へのデータアップロード操作だけを自律的に制御。

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

欠けていたピース：実行時の経路を守るNetskope



Agentic Brokerによる可視化

NetskopeはAIと外部環境の経路に配置され、暗号化されたMCPトラフィックをリアルタイムで復号・インライン検査する。

非ヒューマントラフィックの解読

「どのAIクライアントが」「どのMCPサーバーへ」「何のデータを送ろうとしているか」を完全に可視化。

意味のあるログへの変換

理解不能な通信の塊を、検索・監査可能な業務トラフィックへと変える。

シャドーAIの可視化

CASB GenAI

社員の生成AI利用状況を可視化。シャドーAIの発見と、法人／個人インスタンスの識別・制御

Agentic Broker

MCPサーバー利用状況の可視化。野良MCPサーバー・未承認AIクライアントを検知しブロック

AI Command Center

組織内のAI資産（アプリ・エージェント・MCP）を自動的に発見し、リスクを相関分析

エンドポイントとサーバー（eBPF）の両面でAIトラフィックを捕捉

AISecOpsエージェントが検知から対応までを自律実行し、管理者の負担を軽減

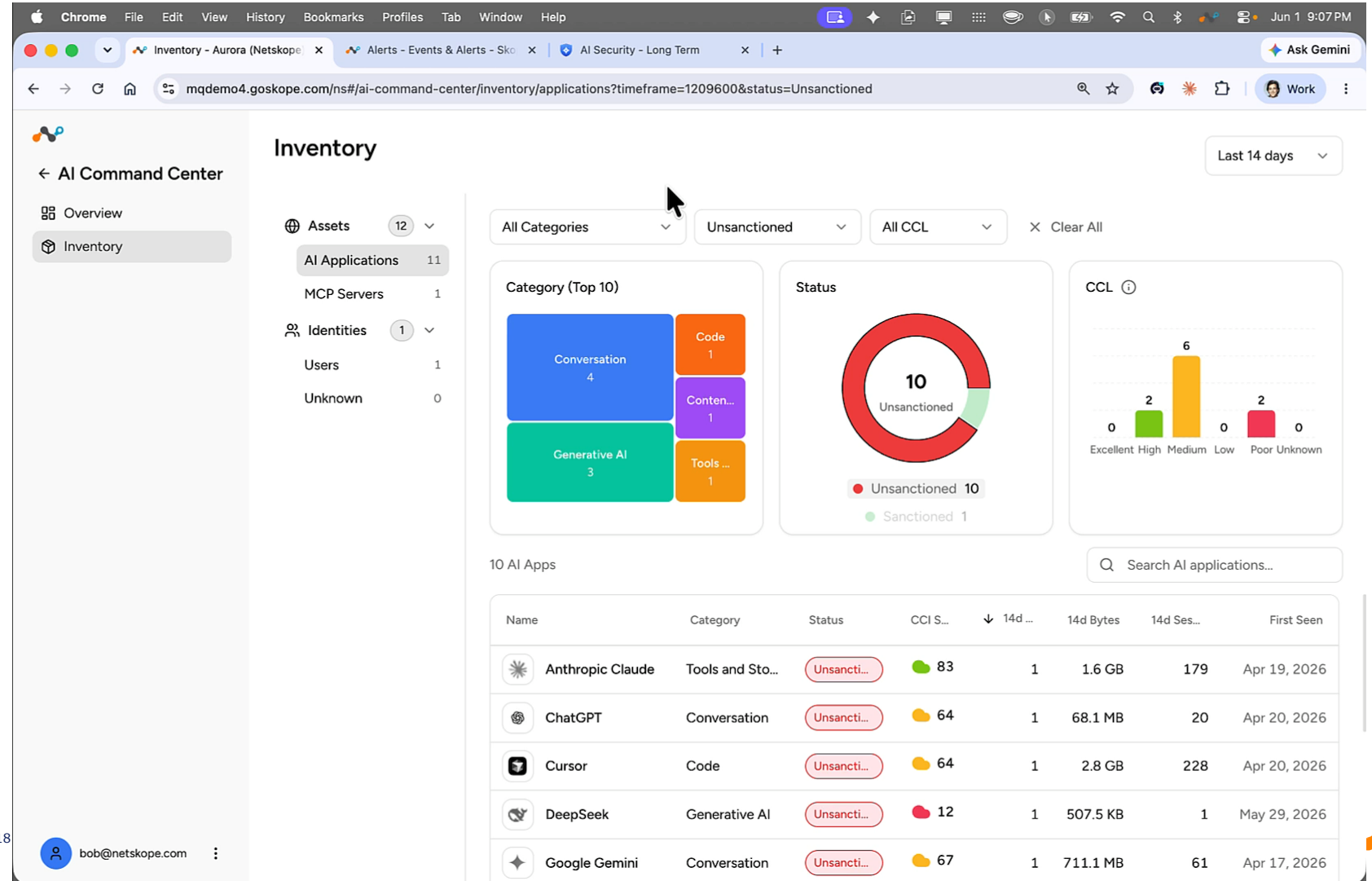
94%

AI活動の可視性にギャップ

91%

エージェントを行動前に止められない

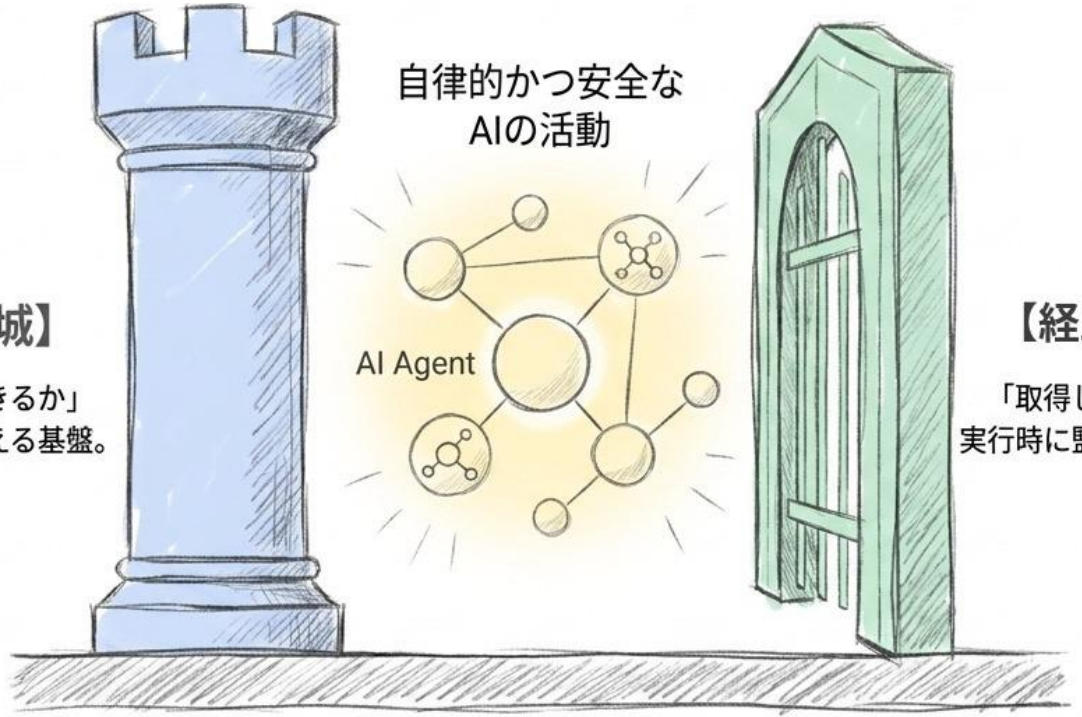
https://www.netskope.com/press-releases/netskope-unveils-ai-command-center-delivering-comprehensive-ai-discovery-and-correlated-risk-intelligence-with-fully-coordinated-agentic-response
https://www.netskope.com/resources/reports-guides/ai-risk-and-readiness-report


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Jun 1 9:07 PM
Inventory - Aurora (Netskope
Alerts - Events & Alerts - Sko
AI Security - Long Term
Ask Gemini
mqdemo4.goskope.com/ns#/ai-command-center/inventory/applications?timeframe=1209600&status=Unsanctioned
Work
AI Command Center
Overview
Inventory
Inventory
Last 14 days
Assets 12
AI Applications 11
MCP Servers 1
Identities 1
Users 1
Unknown 0
All Categories
Unsanctioned
All CCL
Clear All
Category (Top 10)
Conversation 4
Code 1
Conten... 1
Generative AI 3
Tools ... 1
Status
10
Unsanctioned
Unsanctioned 10
Sanctioned 1
CCL
0 2 6 0 2 0
Excellent High Medium Low Poor Unknown
10 AI Apps
Search AI applications...
Name Category Status CCI S... 14d ... 14d Bytes 14d Ses... First Seen
Anthropic Claude Tools and Sto... Unsancti... 83 1 1.6 GB 179 Apr 19, 2026
ChatGPT Conversation Unsancti... 64 1 68.1 MB 20 Apr 20, 2026
Cursor Code Unsancti... 64 1 2.8 GB 228 Apr 20, 2026
DeepSeek Generative AI Unsancti... 12 1 507.5 KB 1 May 29, 2026
Google Gemini Conversation Unsancti... 67 1 711.1 MB 61 Apr 17, 2026
bob@netskope.com

二層の守り：ゼロトラスト・AIアーキテクチャ

Box
【コンテンツの城】

「誰が情報にアクセスできるか」
AIに正しい権限と知識を与える基盤。



Netskope
【経路安全の執行者】

「取得した情報がどこへ流れるか」
実行時に監視・制御し、盲点を可視化。

統合の価値：Boxが入口を守り、Netskopeが出口を守る。この二層構造により、
AIエージェントの自律性を殺すことなく、データを完全に保護するゼロトラスト環境が完成する。

AI利用の必須要件：3つの統制 ＋ アクセス制御

Netskope ― 通信と挙動の統制

1 可視化

・シャドーAI・野良MCPの発見
・法人／個人インスタンスの識別
・組織内AI資産の把握（AI Command Center）

2 検証

・接続元アプリと宛先MCPサーバーの検証
・送信内容のDLP検査
・API／JSONの中身まで解析

3 実行時強制制御

・危険な操作をその場で遮断
・ガードレールとコーチング
・最小権限を実行時にも維持

＋

土台：データのアクセス制御 ― Box

誰が・どのデータに触れてよいか：7段階の権限設定、Security-Trimmed Search、機密分類ラベル

3つの統制（Netskope）と土台のアクセス制御（Box）。4つ揃って初めて、AIを安心して使い倒せる

まとめ：なぜ Box × Netskope か

Boxが権限を守り、Netskopeが通信と挙動を見る
「誰が見てよいか」と「実際に何がどう動いたか」の二層で守る

軸は「シャドーAIの可視化」
見えるから、禁止せずに使える。管理者の負担はAIが減らす

「便利だから使う」を「安心して使い倒す」へ
Boxの利便性を保ったまま、AI活用を全社に広げる