Boxの“使いやすさ“を殺さずに守る
- AI時代のコラボレーションを支えるデータ保護とは

2026年6月4日

Netskope Japan株式会社
シニアソリューションエンジニア
二正寺敏彦

2026 © Netskope Public. All rights reserved.

Netskope について

The Leading Secure Access Service Edge

イノベーションの文化

275件以上の特許
従業員3,500人の約50%が開発者
100人以上のデータサイエンティスト

マーケットリーダー

8年連続 Gartner MQ リーダー
CASBで創業しSASE/SSEのリーダー企業として業界をリード

ハイパフォーマンス プライベートクラウド

グローバルインフラNewEdge
77以上の地域でシームレスでローカライズされた優れたパフォーマンスを提供

AI/ML/生成AI

安全な生成AIの利用制御によりDXを促進
AIセキュリティソリューションの拡充
AIを様々な機能への活用

大規模なクラウドトラフィックを インラインで処理

インラインプロキシは、世界数億人のユーザーのトラフィックを復号化し検査

ゼロトラストエンジンの コンプライアンス

データプライバシー規制へのコンプライアンスを確保しながら、重要なデータとのあらゆるやり取りにゼロトラストの原則を適用

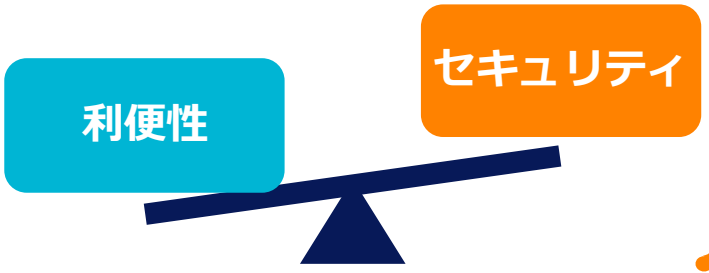
導入社数 4,500以上 | フォーチュン100の 30社以上

金融サービス	ヘルスケア	通信キャリア	小売
トップ 5 のうち 3社	トップ 5 のうち 4社	トップ 4 のうち 3社	トップ 4 のうち 3社

2026 © Netskope Public. All rights reserved.

Box利用における管理者のジレンマ

- **Boxは圧倒的な利便性を提供**
  - 社内外のコラボレーションを加速
- **一方、管理者が直面する現実**
  - 利便性とセキュリティのバランス
    - 制限を緩くすると、利便性は高まるが、情報漏洩リスクも高くなる
    - 制限を厳しくすると、情報漏洩リスクは低くなるが、利便性も損なわれる
  - 個人Boxへの持ち出しリスク
  - 共有設定・アクセスログの確認が属人的なチェックに依存し、運用負荷が増大
  - 生成AI・AIエージェントの利用拡大により、データの流出経路と保護対象がさらに複雑化
- **従来の常識: 利便性とセキュリティはトレードオフ**
  - **本当にトレードオフなのか？**
    → 本セッションで両立の道筋を提示



2026 © Netskope Public. All rights reserved.

本セッションの内容

NetskopeによるBoxを利用する上での、ユーザー利便性を落とさず、
セキュリティを保ちながら管理者の運用負荷を軽減する3つの切り口

1. 利便性を犠牲にしない透過的なデータ保護
2. AI/MLを活用したスマートな運用
3. AIエージェント時代に向けた安全なAI連携

2026 © Netskope Public. All rights reserved.

第1部
利便性を犠牲にしない透過的なデータ保護

2026 © Netskope Public. All rights reserved.

Netskopeのアーキテクチャ概要

インライン + API で包括的な保護を実現

クラウド型プロキシとして、端末とWeb/SaaS通信の間に
介在することで、リアルタイムでの通信の可視化・制御
（CASB※1、DLP※2、Webフィルタリング、脅威防御）が可能

SaaSとのAPI連携によりセキュリティポスチャの管理
や保存データに対する可視化・制御（CASB※1、DLP※2、
脅威防御）が可能

※1. Cloud Access Security Broker: クラウド利用の可視化・制御機能
※2. Data Loss Prevention: データ漏洩防止機能

2026 © Netskope Public. All rights reserved.

ユースケース①：Box以外へのデータアップロード禁止

【シナリオ】

- データのサイロ化や情報漏洩や防ぐためにBox以外へのアップロードをリアルタイムにブロック
- シャドーITへのアップロードをブロック
- 他社からのファイル共有やコミュニケーションのため、閲覧やダウンロード、Web会議などは許可

【従来型プロキシの課題】

- URL単位でのアクセス許可 or ブロックしかできず、アップロードのみ禁止するといった制御ができない
- リモートユーザーに対する制御が難しい

【Netskopeによる解決】

- アプリケーション/テナント毎の柔軟なアクティビティ制御（アップロードのみ許可 or ブロックなど）により、ユーザーの利便性を落とさず、情報漏洩のリスクを排除することが可能
- 働く場所を問わず柔軟なポリシー制御が可能

2026 © Netskope Public. All rights reserved.

ユースケース②: Boxラベルがないコンテンツの保護

【シナリオ】

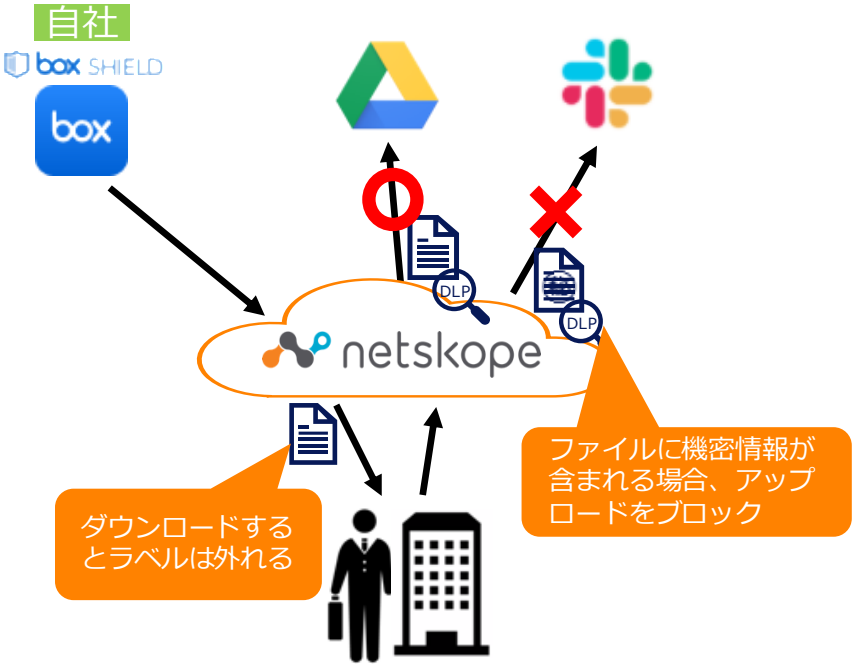
- 業務内容やプロジェクトによっては他クラウドサービスにファイルをアップロードする必要がある
- Boxからダウンロードされるとラベルは外れるため、アップロードが必要な場合は機密情報が含まれていないかの確認が必要

【従来型プロキシの課題】

- DLP機能がないため検知不可
- または簡易的なDLPのみのため、誤検知や過検知が多く運用が回っていない

【Netskopeによる解決】

- 日本語検知含めた高度なDLPを用いて機密情報を検知し、アップロードのブロックが可能
- 柔軟なユーザーアラートによる業務を止めない利便性とセキュリティを両立



2026 © Netskope Public. All rights reserved.

柔軟なユーザーアラート

ブロックや検知された理由をポップアップでユーザーに通知することで、ユーザーに納得感を与える
業務を止めない柔軟な制御（コーチング）も可能

例 1：マイナンバーやクレジットカード番号、銀行口座などの個人情報を検知した場合はブロック

例 2：住所やEメールアドレスを検知した場合にはアクションを続行するか確認（コーチング）

2026 © Netskope Public. All rights reserved.

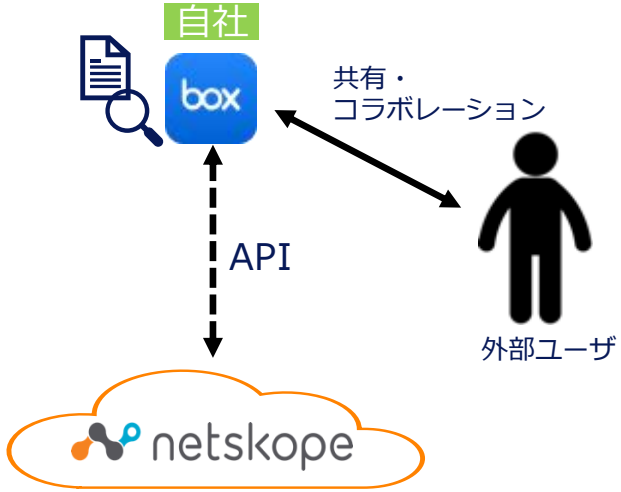
ユースケース③: 保存済みデータや外部ユーザの管理

【シナリオ】

- Boxに保存されているデータに関して機密情報がないか、また機密情報の場合は社内・社外に公開されていないかの確認がしたい
- 共有・コラボレーションした外部ユーザーのアップロード/ダウンロードの監視。アップロードしたファイルのDLPやマルウェアスキャン
- Netskope DLPエンジンのスキャンによりBoxラベルの自動付与・付け替えをしたい

【Netskopeによる解決】

- BoxとのAPI連携により日本語検知含めた高度なDLPを用いて機密情報を検知し分類
- 公開リンクの削除やアクセス権の変更、Boxラベル付与などの制御
- マルウェアを検知した場合や削除や隔離



2026 © Netskope Public. All rights reserved.

第2部
AI/MLを活用したスマートな運用

2026 © Netskope Public. All rights reserved.

Netskopeにおける主な AI/ML の利用用途

DLP	CASB	UEBA	Threat Detection	SWG	IoT Security	SD-WAN	AIOps
機密文書や画像、ソースコードなど分類	新しいアプリの分類、CCIリスクの計算	異常な行動を検出: 悪意のある内部者、侵害されたアカウント、ブルートフォース、データの流出	シグネチャ、ヒューリスティック、サンドボックス	Webコンテンツのフィルタリング/分類	IoTデバイスの分類と識別、動的デバイスグループ化、異常検出	WAN アクセス異常検出	ワークフロー自動化、アプリの健全性監視、クラウドの自動スケーリング、適応型インシデントの優先順位付け

自然言語処理 (NLP)、コンピューター ビジョン、教師あり/教師なし ML、統計モデリング

2026 © Netskope Public. All rights reserved.

Netskope DLP (データ漏洩防止)：AI/MLの活用

ML画像分類


パスポート

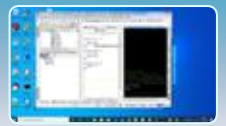

運転免許証


社会保障カード


クレジットカード/
デビットカード


ペイチェック


保険カード


スクリーンショット


ホワイトボード

ML文書分類

- 銀行取引明細書
- コンサルティング契約
- M&Aドキュメント
- NDA
- オファーレター
- パートナー契約
- 特許
- 委任状
- 履歴書
- ソースコード
- 株式契約
- 税務書類

Train Your Own Classifier（TYOC）

お客様のデータを学習させ、独自の機械学習モデルをトレーニングして利用することも可能

2026 © Netskope Public. All rights reserved.

MLを利用したユーザーの振る舞い検知

大量アップロードポリシー(100ファイルのアップロード)

- Standard UEBA – 簡単で調節可能なルール、微調整が必要

鈴木さん	Boxに99ファイルアップロード → **OK**
佐藤さん	Boxに100ファイルアップロード → リスクあり(**SUSPICIOUS**)

- Advanced UEBA – 機械学習、相関分析、スコアリング

鈴木さん	・通常、Boxに1日1ファイルしかアップロードしませんが、今日は、99ファイルアップロードしました。これは**リスクあり(**SUSPICIOUS**)** ・さらに、それが個人アカウントであり、いくつかの**DLP**違反も含まれていました。加えて、**管理対象の場所から普段よりも多く**ダウンロードを行いました。 ・これらを考慮し、**LOW CONFIDENCE**と判断し、**アクセスを制限**します。

2026 © Netskope Public. All rights reserved.

DLP AISecOps エージェント

DLPインシデントの発生件数、複雑さ、対応時間を大幅に削減

重複排除	誤検出	クラスタ	自動化されたワークフロー	エージェントによるトリアージ	エージェント調査	エージェントの行動
ユーザーに基づいて類似のインシデントを重複排除	過去の行動に基づいて誤検出を提案	関連するインシデントをインテリジェントにクラスタリングしてケースに分類	Netskopeのベストプラクティスワークフローは自動的に実行され、推奨事項が表示	エージェントの推奨事項と調査結果に基づく自然言語によるトリアージ	アナリストは、結論が出ない行動や重大な脅威についてさらに調査可能	自然言語で修復措置をリクエストすれば、エージェントがそれを実行

2026 © Netskope Public. All rights reserved.

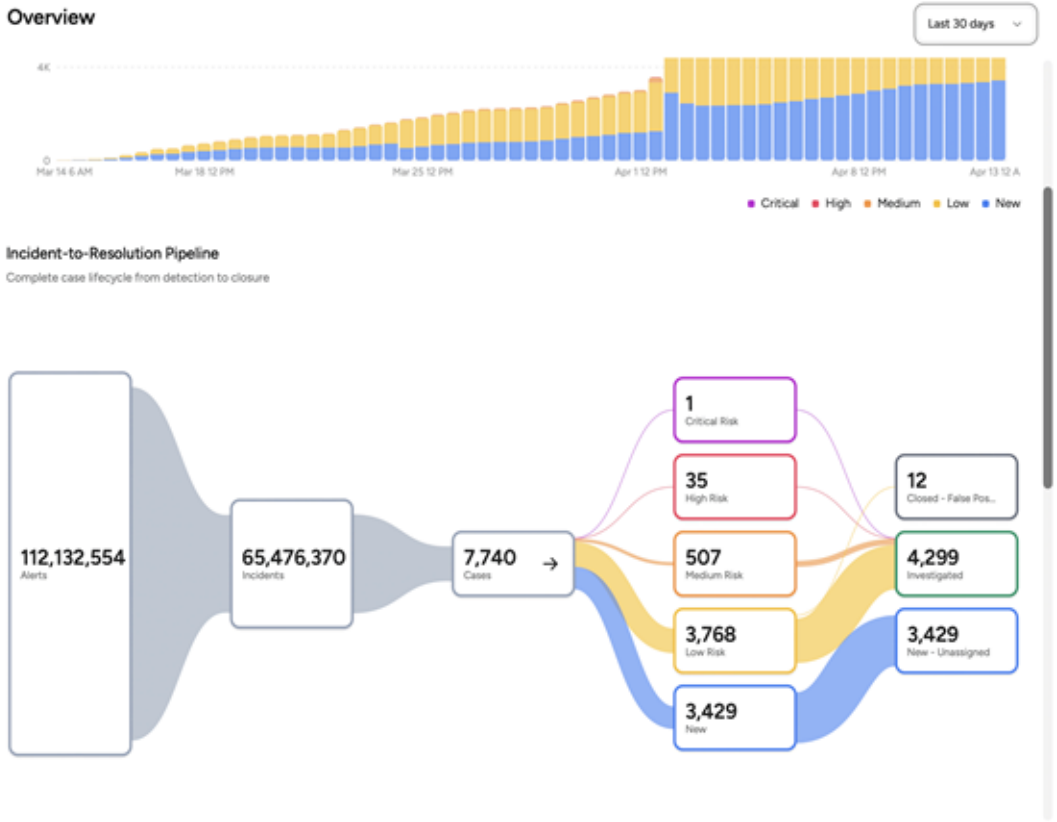
DLP AISecOps エージェント

Netskope DLP AISecOps Agentは、上級セキュリティアナリストの機能を模倣し、エンドツーエンドの保護ワークフローを実行・加速

アラート疲労：数千件のアラートを、高精度な事例に絞り込みます。

インテリジェント・トリアージ：リスクに基づいた優先順位付けにより、リスクの高い案件に重点を置くことで、投資対効果を向上

戦力増強効果：人員増なしで拡張可能なオペレーション



2026 © Netskope Public. All rights reserved.

第3部
AIエージェント時代に向けた安全なAI連携

2026 © Netskope Public. All rights reserved.

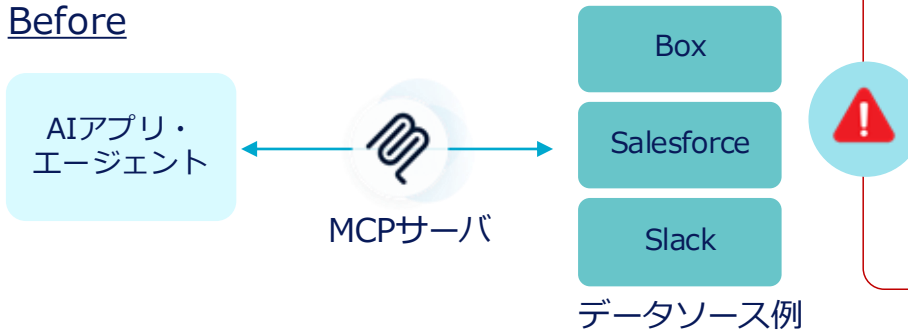
AIエージェントがBoxを使う時代

- **AIエージェントとは**
  - 人間の指示を受けて自律的にタスクを計画・実行するAI。検索、要約、文書作成、データ操作などを一連の業務フローとして遂行する
- **Box内のデータをナレッジベースとしてAIが活用するシナリオ**
  - 社内規程・契約書・議事録・顧客資料などをAIが横断的に参照し、問い合わせ対応、提案書作成、リサーチ業務を自動化
- **新たなリスク：AIがアクセス権限を超えてデータを取得・流出する可能性**
  - AIエージェントが利用者の権限範囲を超えて機密情報を参照・出力するリスク、外部AIサービスへのデータ送信による情報漏洩、ハルシネーションによる誤情報拡散など、従来のアクセス制御では捉えきれない脅威が発生

2026 © Netskope Public. All rights reserved.

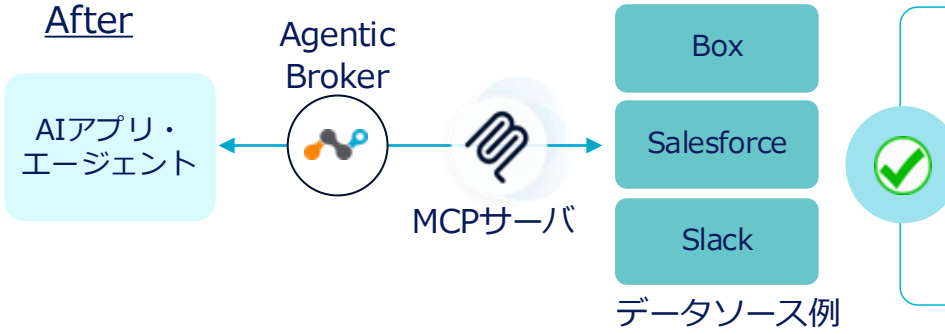
AIエージェントへの対応

Netskope Agentic BrokerによるセキュアなMCP利用



課題

- Model Context Protocol（MCP）サーバーは、アプリ、エージェント、LLM間のシームレスな双方向データ共有
- データ漏洩や不正アクセスのリスク
- 可視性、制御、保護の欠如



Netskope Agentic Brokerによる解決

- MCP使用における可視性、制御、保護
- リアルタイムポリシー適用、DLP、およびガードレール
- 危険な活動やデータ漏洩を防止

2026 © Netskope Public. All rights reserved.

まとめ

2026 © Netskope Public. All rights reserved.

Boxを「守る」から「活かす」へ

- **Netskopeが提供するBox活用の3つのアプローチ**
  - **ユーザーの利便性を奪わない透過的な保護**
    - 業務を止めず、共有・編集・閲覧はそのままに、機密データのみを文脈で識別して制御
  - **AI/ML活用による運用負担の軽減**
    - 機密データの自動分類と異常検知でポリシーを継続的に最適化
    - トリアージによるインシデントの優先度把握と対応時間の削減
  - **AIエージェント対応**
    - MCPサーバ通信を可視化し、生成AI・AIエージェントによるBoxデータ参照をDLP含めて制御

- **Netskopeが提供する価値の全体像**
  - 「守る」と「活かす」を両立し、Boxを中心としたコラボレーションとAI活用を加速
  - SSE/SASEを単一プラットフォームで実現し、Box以外のSaaS・Webも一貫したポリシーで保護

2026 © Netskope Public. All rights reserved.

Thank You

2026 © Netskope Public. All rights reserved.