# ちょっと待った！脱VPNの先にある“漏洩ゼロ”の現実解

# Netskope（ネットスコープ）
## クラウドとAI時代のセキュリティネットワークをリード

| 設立 | 本社 | プラットフォーム |
| --- | --- | --- |
| 2012年 | 米国カリフォルニア州<br>サンタクララ | Netskope One<br>SASE / SSE |

どこからでも、あらゆるデバイス・クラウド・
データ・AIをリアルタイムに保護し、高速化

**自社所有のグローバル・プライベートバックボーン**

**80+**
リージョン

**120+**
データセンター

**データ中心の防御**

統合されたデータ保護と
ゼロトラストを通信経路上で実行

**AIセキュリティ内蔵**

生成AIやシャドーAIの利用を
可視化し、安全に活用を促進

企業文化
**イノベーション**
取得済みと申請中の特許を合わせて275 件
研究開発に人材の **50%** を集中

国内パートナー

SoftBank

netskope

2026 © Netskope Confidential. All rights reserved.

# CASB/DLPの原点から SSE/SASEリーダーへの軌跡

2025 Gartner Magic Quadrant for
SSE ( Security Service Edge )


2025 Gartner Magic Quadrant for
SASE Platforms


2012年
ある予言が・・

**創業期:**
**CASB・DLPのイノベーター**

CASB

DLP
Threat
Protection

User Coaching
Sandboxing
API-Based CASB

**拡大期:**
**包括的なSSE**
**プラットフォームの構築**

CSPM
Next-Gen SWG
Encryption

**統合期:**
**SASEへの進化と**
**Converged Platform**

Cloud Exchange
Adv. Analytics
ZTNA NPA
NewEdge

RBI
FWaaS
SSPM
DEM

Borderless SD-WAN
IoT Security

AI

**リーダーの確立:**
**2025 Gartner MQ**
**両分野でリーダー！**

VALIDATED
LEADERSHIP

netskope

2025 © Netskope All rights reserved.

# Netskope の夜明け

## 2012年に予言された課題:
## クラウドによるデータ漏洩と爆発

- 従来のファイアウォールは「0か1か」（許可／拒否）のみ。
- データの詳細「context（文脈）」が見えない致命的な盲点が存在。


CEO : Sanjay Beri

CTO : Krishna Narayanaswamy

## 予言者たちの直感
## ホワイトボードから生まれた、新しいアーキテクチャ

元Juniperの二人が共に描いたネットワークとクラウド
AIサービスを可視化するアーキテクチャ。

シマンテック元CEOや元MS会長ら超大物たちが、
クラウドとAIの未来を予言するその直感に唸り投資を即決。

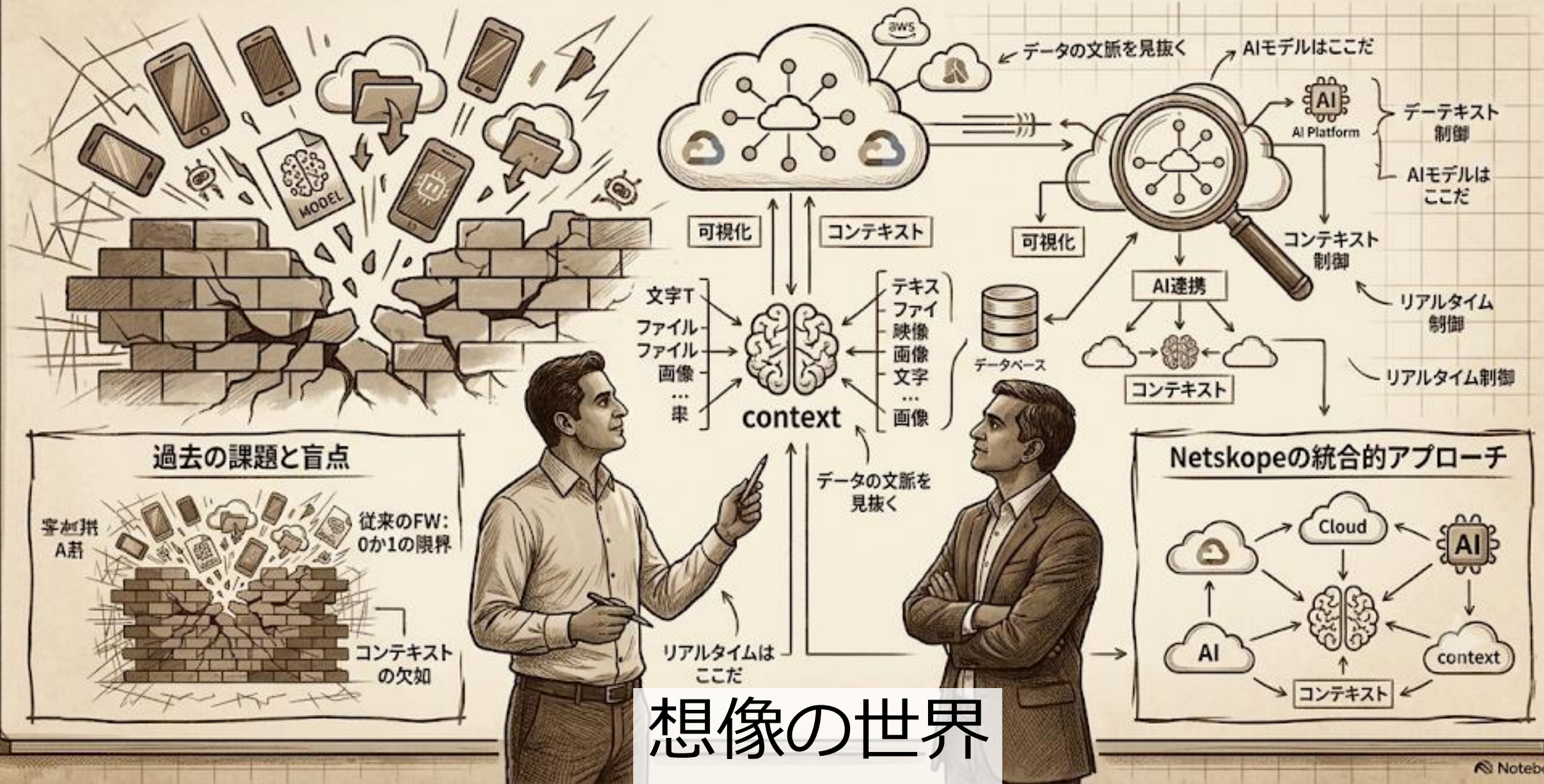
そして、2012年10月創業

**社名の由来**
「Network（ネットワーク）」+
「Scope（覗き見・可視化）」
= Netskope

netskope

2026 © Netskope Confidential. All rights reserved.

# 予言されたアーキテクチャの青写真：クラウドとAI時代の新しいセキュリティ




NotebookLM

# 6月4日　ネットスコープ
# 「Netskope One AI Security」を発表


# AI 可視化

# 無償体験


2026 © Netskope Public. All rights reserved.

# 迫り来る脅威
# DXの影に潜む、AIモンスターの正体

## 制御不能な「シャドーAI」という怪物

AIモンスターとは、高度に便利でありながら人間が
制御しきれない「生成AIのリスク」のメタファー

### シャドーIT/AIの脅威

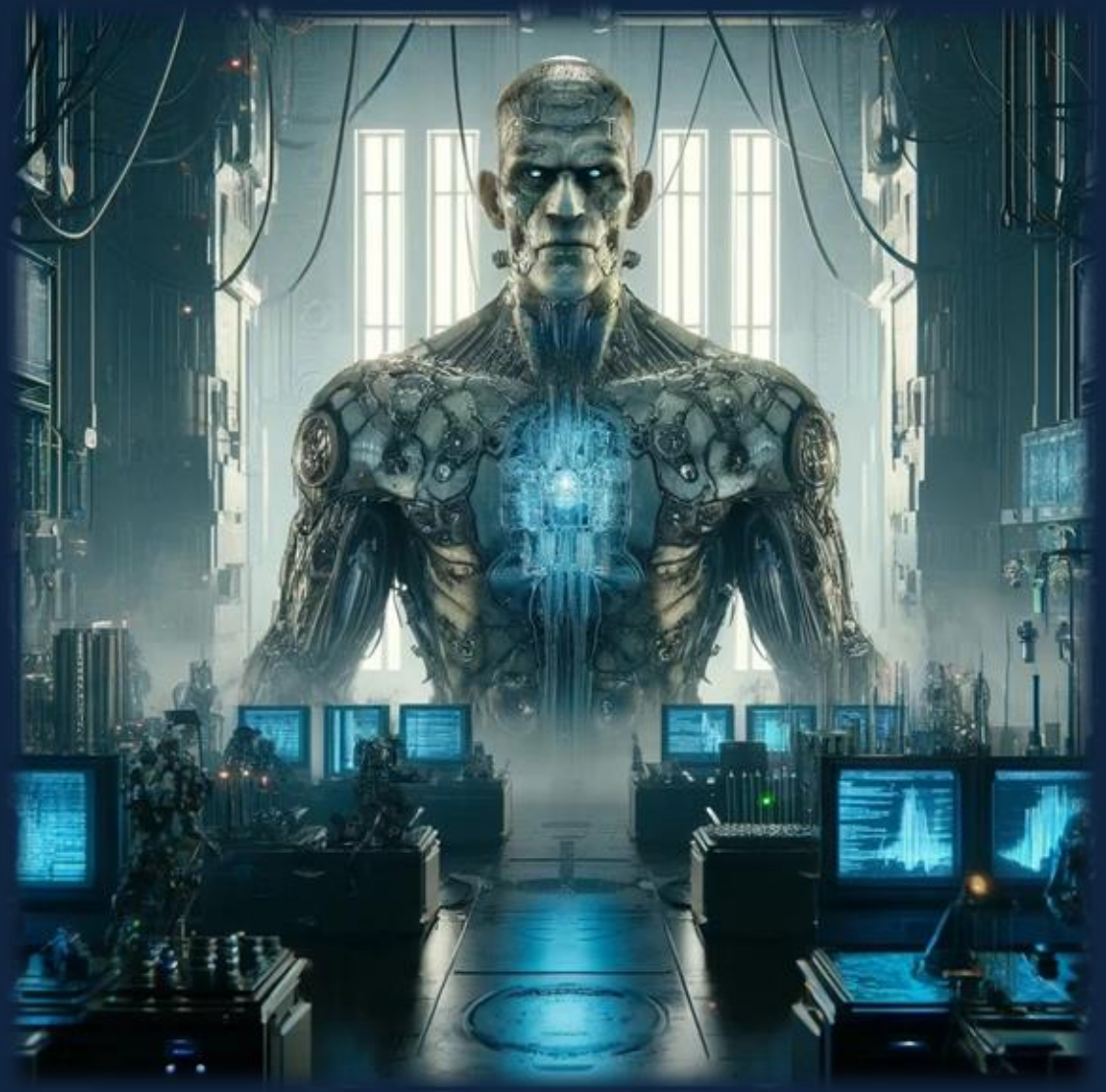
従業員によるブラウザからの個人的利用を
完全にブロックすることは非常に困難

### 機密データの流出

プロンプトに入力された特許情報やソースコード、
顧客データを無意識にAIの学習へ提供してしまう。

### API/脆弱性への攻撃

AIモンスター自身がネットワークの穴を見つけ、
自動で高速な侵入を仕掛ける時代。



# 救世主の誕生

## ネットスコープの夜明け – 見えないクラウドとの戦い

**2012**
**サンジェイ・ベリの予言**
多くのデータはクラウドに移行され、従来のあらゆる区切り(境界線)は消滅

**2014**
**CASB担当「セク」誕生**
クラウドへの全データを完全可視化

**2018**
**超高速網 NewEdge 完成**



**2021-2026**
**One Team への進化**
SD-WANとDEMが合流
最強SASE体制へ

### SSE/セキュリティ【セク】

**クラウドからオンプレまで**
シャドーITの通信や
エンドポイントからクラウドへの
全データを監視・可視化

### SD-WAN 【ネット】

**セキュア通信＆ZTNAの職人**
ゼロトラストなプライベートアクセス
通信経路をコントロールし
安全・高速にネットワークを制御

### DEM/I&O【アイオ】

**DX監視と可視化の達人**
『重い』というクレームのもと
端末、Wi-Fi、回線、クラウドの
遅延箇所を一発で仕分ける

# 最強の防衛軍基地：超高速網「NewEdge」


Netskope
Unified Client

通信暗号化

ユーザー
からの
情報漏洩


外部からの脅威

クラウドサービス利用の可視化と制御

認可クラウドサービス
(M365/Googleなど)

外部連携先
クラウドサービス

シャドーIT・AI

URLフィルタ

Web

DLP

SaaS/Web/メール

ZTNAによるセキュアリモートアクセス

データセンタにある
オンプレミス機器

IaaS上のオンプレミス
アプリケーション

# 超高速網「NewEdge」の全貌

世界
８０リージョン

全POPから
全機能提供

プライベート
クラウド

高い処理能力
と低遅延

シングル
ファブリック


- 日本に4か所のDC（東京x２、大阪x2）
- 高い可用性：99.999%
- 低遅延：往復時間 10ミリ秒以下

netskope

2026 © Netskope Confidential. All rights reserved.

# Netskope SASE


USBメモリ/プリンタ/
ネットワークドライブ制御

エンドポイント DLP

低遅延のPOP へ自動接続

ブレイクアウト

Netskope Unified Client

通信暗号化

DEM ( Digital Experience Management )

Netskope Intelligent SSE
Zero Trust Engine

| | |
|---|---|
| SWG | URLカテゴリによるアクセス制御 |
| CASB | クラウドアクセスの可視化と制御 |
| Dedicated Egress IP | テナントへの固定IPアドレス付与 |
| SSL/TLS 復号化 | SSL/TLSトラフィックの復号化と暗号化 |
| 脅威防御 | マルウェアチェック/IPS/DNS Security |
| RBI | リモートブラウザ分離 |
| DLP | コンテンツによる制御 |
| Cloud FW | アウトバウンドのトラフィック制御 |
| UEBA | ユーザの振る舞いによるアクセス制御 |
| Advanced Analytics | レポートの生成 |
| ZTNA | ゼロトラストに基づいたリモートアクセス |
| SD-WAN | SD-WAN機能 |

すべての操作 OK

ダウンロード のみOK

ブロック

URL, カテゴリ フィルタ

個人情報を 含むファイルは アップロード ブロック

ZTNA

クラウドサービス利用の可視化と制御

認可クラウドサービス (M365/Googleなど)

外部連携先 クラウドサービス

シャドーIT・AI

URLフィルタ

Web

DLP

SaaS/Web/メール

ZTNAによるセキュアリモートアクセス

データセンタにある オンプレミス機器

IaaS上のオンプレミス アプリケーション

# データセキュリティの重要性

## 業界別 データセキュリティ 重要ポイント例

| 業界 | 守るべき最重要データ | 最優先ソリューション・対策 |
|---|---|---|
| **製造** | • 設計データ<br>• 技術ノウハウ<br>• 設備制御データ | ZTNA によるリモート保守・外部ベンダーのゼロトラスト接続と、CASB / DLPによる技術ノウハウのクラウド持ち出し・シャドーIT制御 |
| **金融・保険** | • 口座・決済情報<br>• 個人信用情報 | 高精度な DLPによるコンプライアンスに準拠した個人情報漏洩防止と、SSPM / CASBによるクラウド環境の誤設定検知・アクセス統制 |
| **医療** | • 電子カルテ<br>• 診療・検査データ | ZTNA による院外からのカルテ・医療情報への安全なアクセスと、Next-Gen SWG / Threat Protectionによるランサムウェア感染経路（Web/クラウド）の遮断 |
| **EC・小売り** | • クレジットカード情報<br>• 会員データ | Real-time DLPによるカード・会員情報の未許可ストレージへのアップロード遮断と、Next-Gen SWGによるWeb脅威・悪意ある通信の防衛 |
| **IT・SaaS** | • 顧客預かりデータ<br>• ソースコード | DLPによるソースコードやAPIキーの外部流出防止と、SSPM / CASBによるマルチクラウド・SaaSのセキュリティ設定管理 |
| **公共・教育** | • 住民情報<br>• マイナンバー<br>• 成績データ | Next-Gen SWGによるWebフィルタリング・脅威対策と、DLP / CASBによる住民・学籍データのクラウド経由の不正持ち出し防止 |

# Netskope オリジナルストーリー


- Episode 1：【セク】AIモンスターと戦うCASBの守護神
- Episode 2：【ネット】ランサムウェア脅威から脱VPN
- Episode 3：【アイオ】クレームからDX向上へ導く女神

# Episode 1
# SaaS到来と「JSON」に潜むAIモンスターの罠

## 見えないテキスト「JSON」の恐怖

SaaSやAIの通信は、従来のファイアウォール（L4ポート制御）からは単なる「Webアクセス」に見える
しかしその中身は、複雑な JSONフォーマット

- **AIモンスターの巧妙な侵入**

一見普通のHTTPS通信の中に
「プロンプトへの機密流出コード」

- **ファイアウォール防衛線の崩壊**

「通す」か「止める」の二択では、
業務を止めずにモンスターを防げない。

## ヒーロー「セク」の登場

**DLPとコンテキストCASB**

セクは、その透視力でJSONを解読し、
文脈（コンテキスト）を見抜く力を持つ

# 見えないトラフィックを「可視化」

## 特徴: リクエスト・コンテキストの高い認識力

- **コンテキストとは「背景、状況、場面、文脈」という意味。**
  - **「リクエスト」**がどのような状況で発生したかを理解
  - 何が信用できるか**「リスク」**を分析そして判断

許可
ブロック
コーチ
再認証

アクセス
理由の確認

ユーザ | デバイス | ロケーション | アプリ | インスタンス | アクティビティ | データ

何を信用するか？

**コンテキストを理解したうえでリスクに応じて正しいアクションが取れる**

どのアクションを
取るべきか？

# Netskopeの強み ＝ データの流れを完全に可視化・制御

## 特許技術による他社には侵害できないテクノロジー

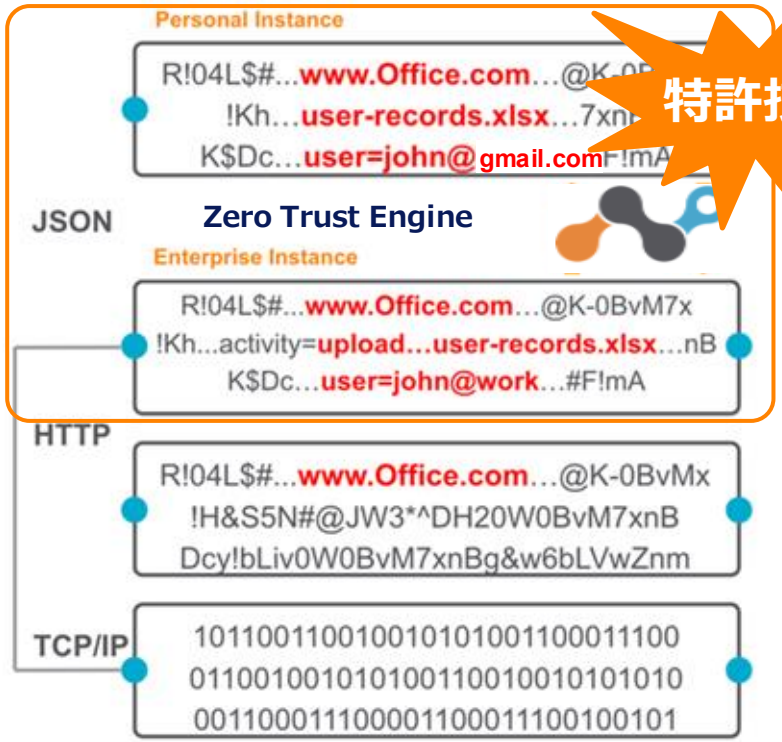
### 従来型 SASE では…


他社SSE/SASEでは
見えない部分

- 企業と個人のインスタンス識別なし
- アクティビティ識別なし

同じ通信でも

### Netskopeは！



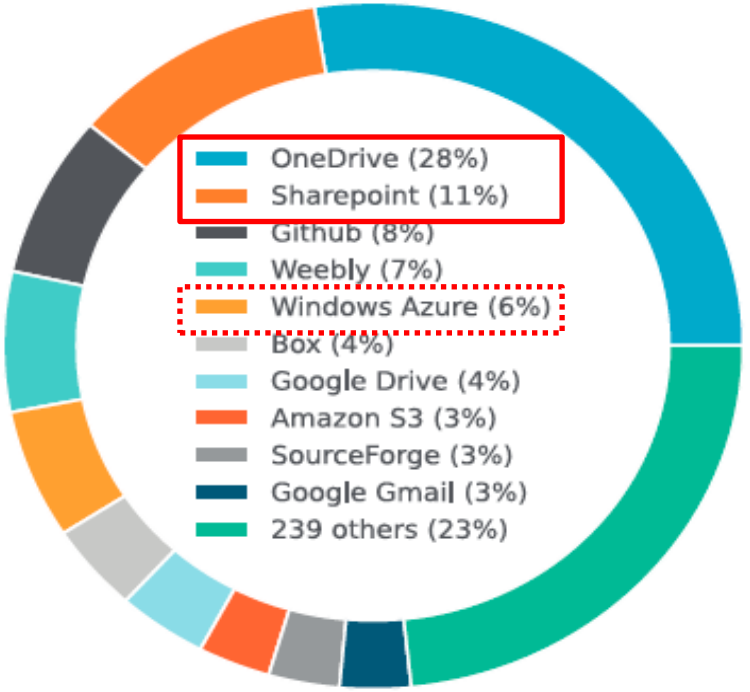

- 企業と個人のインスタンス識別
- アクティビティ識別
(作成、削除、アップ/ダウンロード、表示、編集、投稿など)

2024 © Netskope Confidential. All rights reserved.

# 【M365】バイパス不要の「フル検査」

従来型SWG

M365/O365通信は
SSLインスペクション
無しでバイパスを推奨


マルウェアのソースとなっている
クラウドサービスの
**約1/3は M365/O365**

netskope

積極的にM365/O365通信の
SSLインスペクションを推奨


netskope

# 機密漏洩の検知・コーチング・ブロック

プロンプト・インジェクションや、シャドーAIへの無意識のデータ投入を瞬時に見抜く。

## Step 1: 検知 (Detect)


## Step 2: コーチング (Coach)

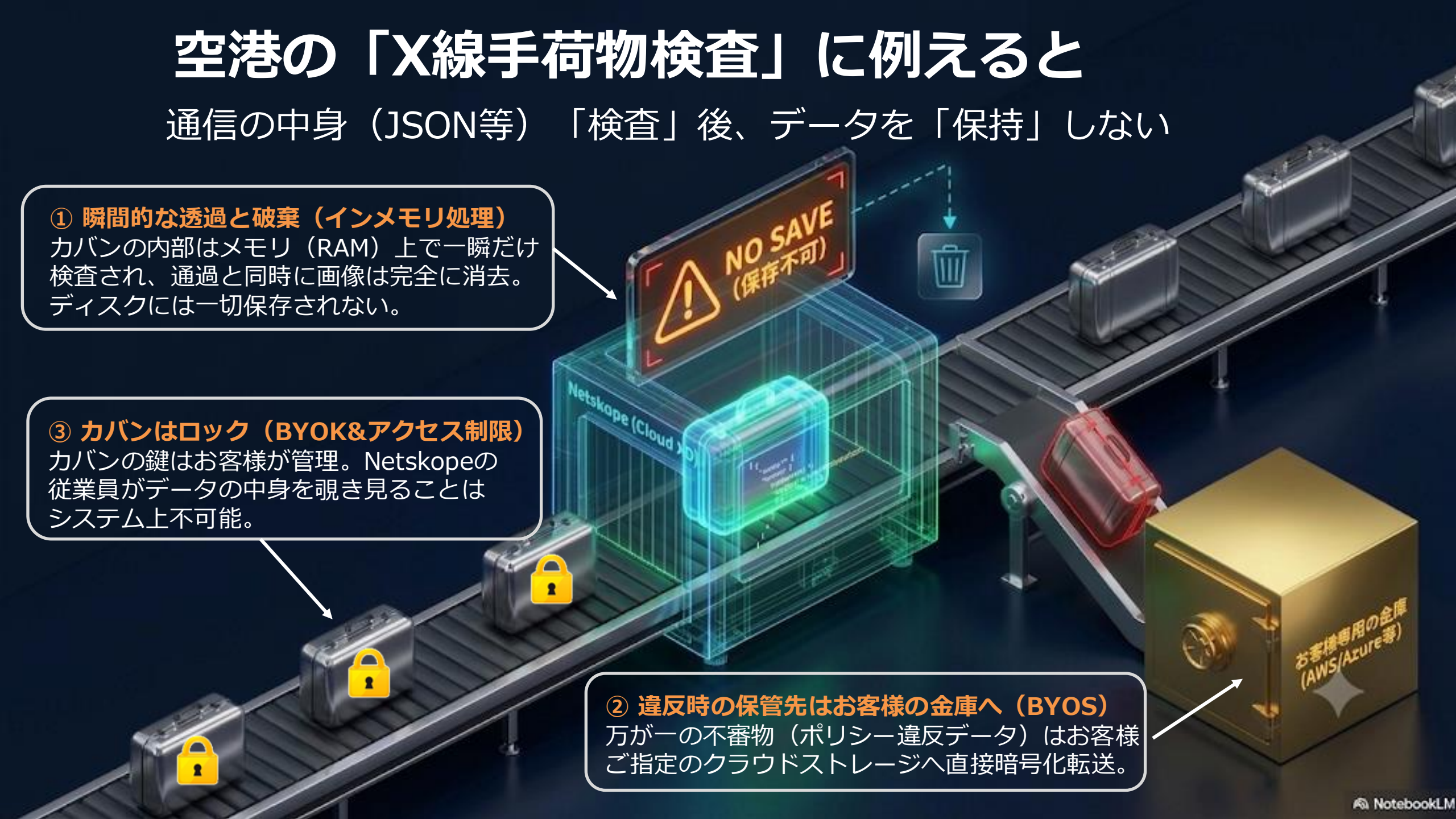

## Step 3: ブロック (Block)

# 空港の「X線手荷物検査」に例えると

通信の中身（JSON等）「検査」後、データを「保持」しない

**① 瞬間的な透過と破棄（インメモリ処理）**
カバンの内部はメモリ（RAM）上で一瞬だけ検査され、通過と同時に画像は完全に消去。ディスクには一切保存されない。

**③ カバンはロック（BYOK&アクセス制限）**
カバンの鍵はお客様が管理。Netskopeの従業員がデータの中身を覗き見ることはシステム上不可能。




**② 違反時の保管先はお客様の金庫へ（BYOS）**
万が一の不審物（ポリシー違反データ）はお客様ご指定のクラウドストレージへ直接暗号化転送。

NotebookLM

# Episode 2
# SASE 到来！AIモンスターが脆弱性を襲撃する

## ボスからの緊急司令

脆弱な*VPN*を突いたランサムウェア
が多発しているらしい！
今すぐ『脱*VPN*』を完了せよ！

VPN装置に存在する 脆弱性 を常に探索

## ヒーロー「ネット」の登場

脱VPNとSD-WAN：
侵入口を塞ぐゼロトラスト接続

- **VPNは「モンスター門番」を欺く**

一度侵入されたら、社内ネットワーク全体を
横展開（ラテラルムーブ）されてしまう。

- **ネットの解決策：脱VPN（ZTNA）**

ネットワークにIPアドレスを公開せず、
検証された認可ユーザーだけを
AIとクラウドに直結。

# 【課題】レガシーネットワークは「経営の足かせ」へ

## 【セキュリティの危機】
## VPNは「攻撃者の入り口」に

**脆弱性の深刻化**：ランサムウェア被害が急増。
VPNの存続は許容できないビジネスリスクに。


## 【ビジネスの危機】
## 海外 MPLS（閉域網）の重い足かせ

**競争力の低下**：高コストで柔軟性が低い「私道」の維持は、クラウド時代の競争力を削ぐ。


**【結論】 単なる「技術的負債」ではなく「経営レベルの阻害要因」**

# 【動向】加速する「ZTNA化」と「脱VPNの踊り場」

## 【市場トレンド】 Internet-First と ZTNA の同時推進

## 【ユーザーの実態】「脱VPNの踊り場」を生む **技術的制約**


VPN完全廃止を目指すも
「ZTNAとVPN」
とのハイブリッド構成
を余儀なくされるケースが多数

### サーバー発のPush型通信

運用管理ツールのパッチ配布や、複合機オンプレミスのIP電話（VoIP)の制御が通らない

### レガシー・非HTTP通信

動的ポートを使う Active FTPや、ネットワーク診断用のICMP/UDP等、ZTNAがサポートしない古いプロトコルの残存。

# SASE クライアント / ゲートウェイ

単にアクセスを「止める/通す」だけでなく
中身を見て、安全な使い方だけを許可し、通信を遅くさせない

## Unified SASE Client


Windows, macOS, Linux,
iOS, Android, ChromeOS

## 50Mbps/LTE

小規模

**NSG-101**

- 4 x 1G
- Wi-Fi 5

## 500Mbps

小規模

**NSG-500**

- 4 x 1G
- Wi-Fi 6

## 1Gbps

小～中規模

**NSG-1500**

- 2 x 1G
- 4 x 2.5G
- 2 x 10G
- Wi-Fi 6

## 2Gbps

中～大規模

**NSG-2000**

- 2 x 1G
- 4 x 2.5G
- 2 x 10G

## 5Gbps/LTE

中～大規模

**NSG-2108CW**

- 1 x 1G
- 4 x 2.5G
- 2 x 10G
- Wi-Fi6

## 10Gbps

大規模/DC

**NSG-3000**

- 6 x 1G
- 6 x 10G

## 1/3/5Gbps

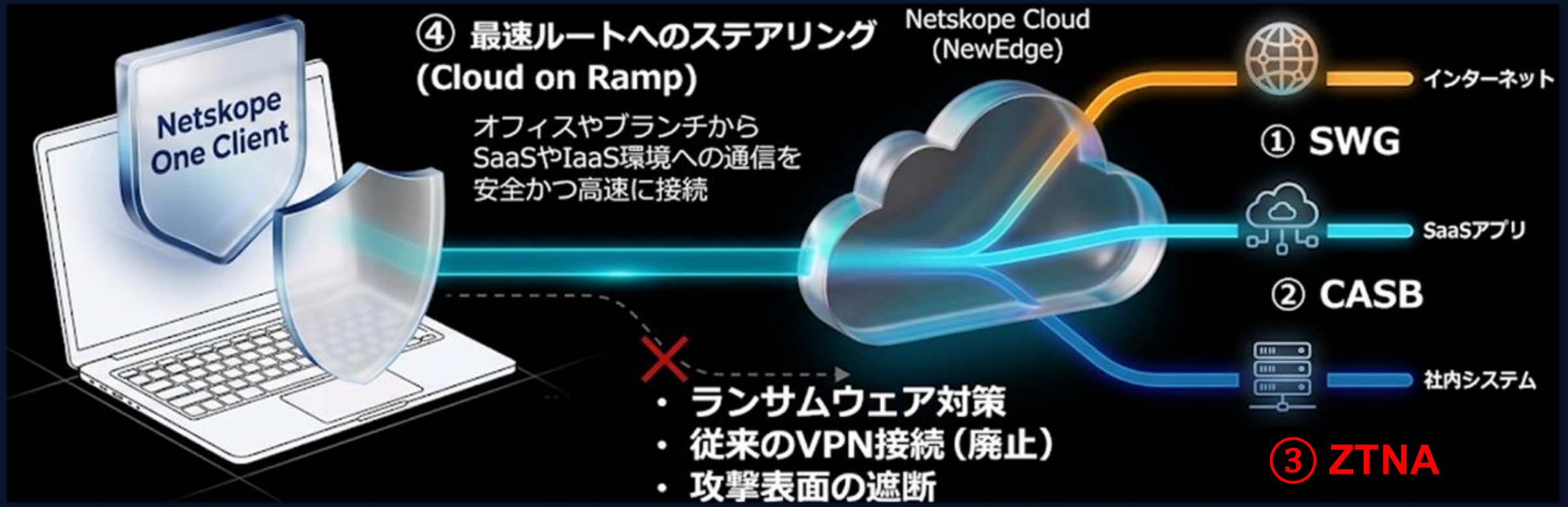
大規模/DC

**Software**
AWS/Azure/
GCP/VM

- 2/4/8 Core

AWS/Azure
GCP/VM対応

# ３人の力の結集！　Netskope Unified Client




**⑤ 脱VPNのための L3アクセス**
**（Endpoint SD-WAN ）**
ZTNAへの移行にリスクとなるサーバー発
通信やレガシープロトコルを完全サポート

# 脱VPN：NewEdge Cloud Gateway


**Netskope**

SWG・CASB
CFW

Web & SaaS

大阪

Netskope **NewEdge**

東京

従業員

Unified
SASE Client

自社インフラ

Public Cloud

Publisher

アプリ

自社データセンター

**SASE Gateway**

- サーバーからクライアントへの通信
  - 運用管理ツール
  - 複合機運用
  - オンプレ型 VoIP/Web会議
  - リモートアシスタンス）
  - 古いクラサバ型アプリ

netskope


Publisher
aws
AWS
Unified SASE Clients
Netskope NewEdge
Multi-Cloud
Publisher
Tokyo
Osaka
Unified SASE Clients
Multi-Cloud
Publisher
Web & SaaS
必殺！
NewEdge Cloud Gateway

# Episode 3
# クレーム からDX向上へ導く女神の出現

## ボスからの緊急司令

ユーザーから「遅い」「つながらない」
のクレームが連発している
ただちに原因究明せよ！

## スーパーヒロイン「アイオ」あらわる

IT部門が最も頻繁に直面する現場からの抗議

モンスター退治後の平和な世界に
「ネットが遅い！」「アプリがノロい！」の声が・・

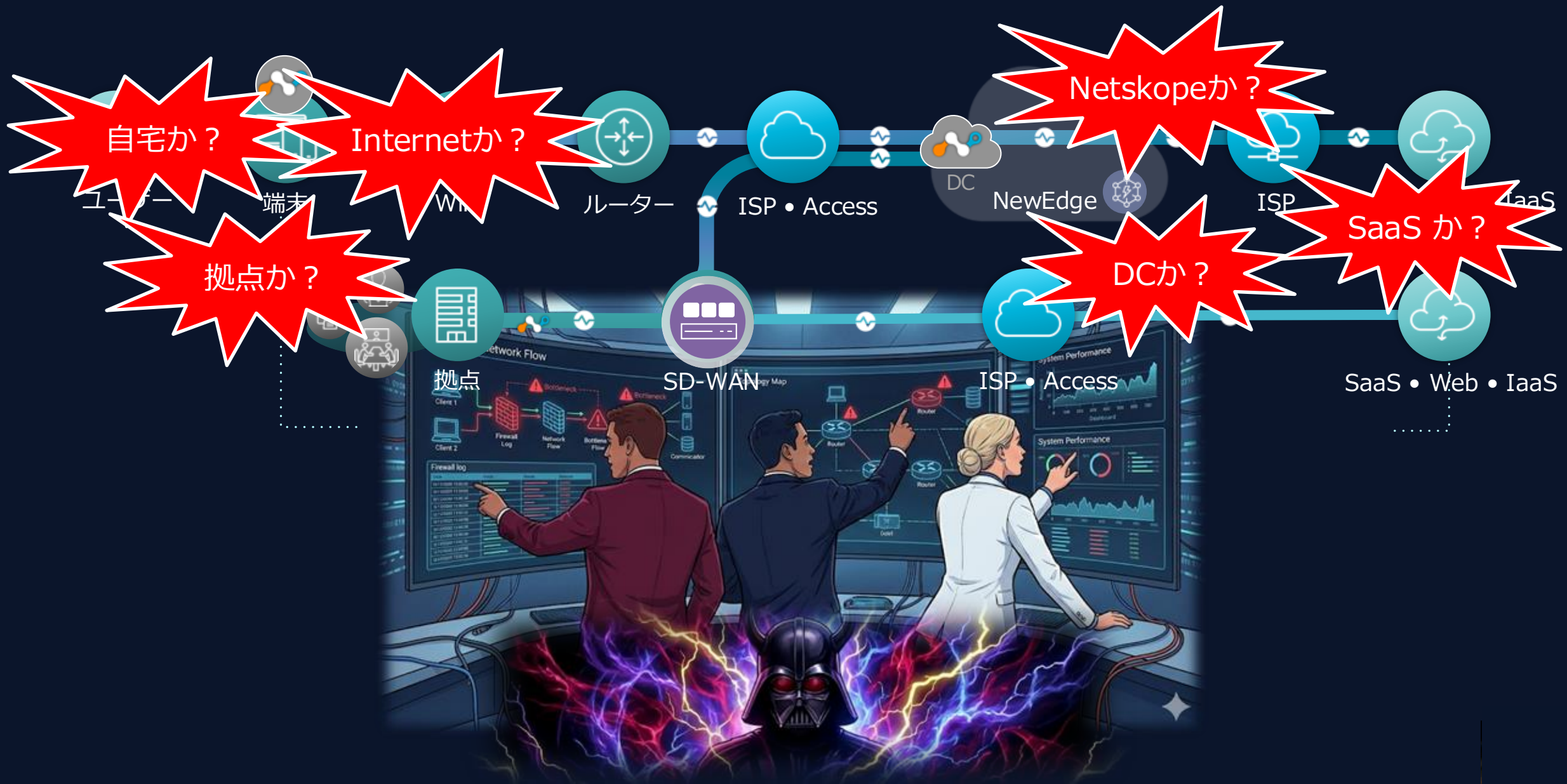
### アイオの全方位可視化（DEM）

PC端末、自宅のWi-Fi回線、ISPプロバイダ
どこで遅延が発生しているかを即時に診断

### 責任追及から「解決」へ

「Netskopeが遅い」という誤解を解き、
プロアクティブな運用の健全化を実現

# どこに潜むかわからない ボトルネック



# 障害解決の「50%以上」が原因探しに


**以上の時間の浪費**

障害解決にかかる時間の半分以上が、単なる「原因究明」に費やされている

**の平均MTTR（修復時間）**

原因特定が遅れることで、従業員の業務が停止するビジネスダウンタイムが平均4.9時間にも及んでいる

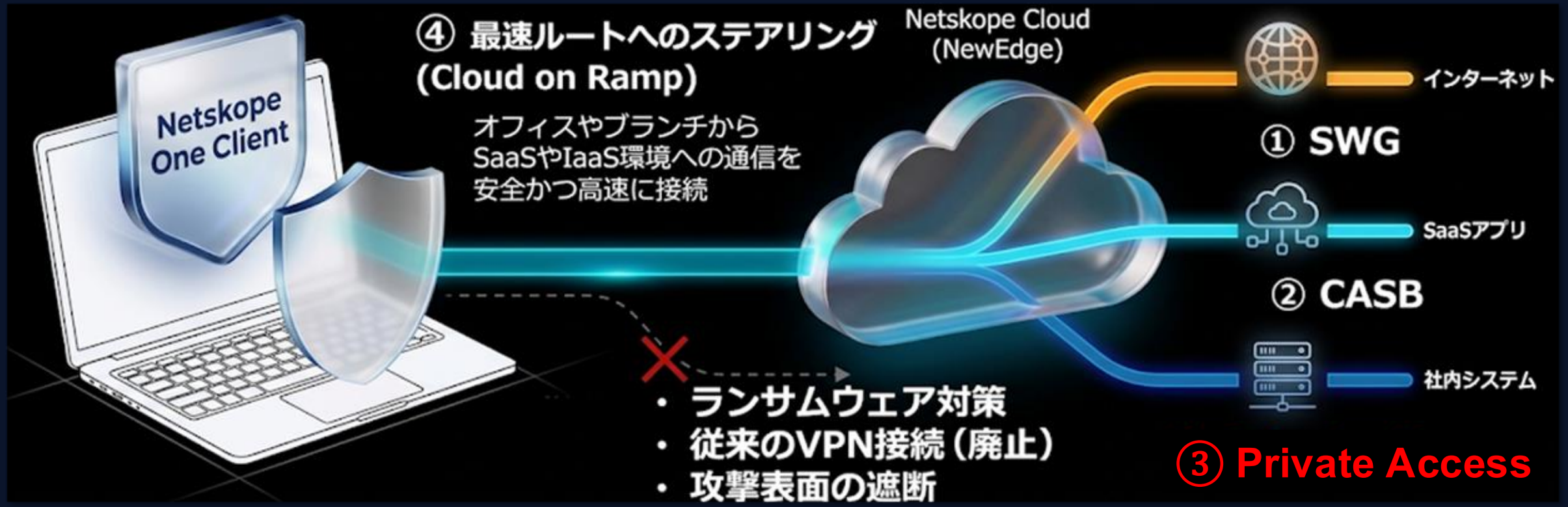
**の企業が導入を計画**

2026年までに、60%の企業のIT部門が監視ツールの乱立を統合し、制御を取り戻すためにDEMの導入を計画

無駄な時間の浪費

# Digital Experience Management
# （デジタル体験管理）発動

# ３人の力の結集！　Netskope Unified Client




**⑤ 脱VPNのための L3アクセス（Endpoint SD-WAN ）**

ZTNAへの移行にリスクとなるサーバー発通信やレガシープロトコルを完全サポート

**⑥ ユーザーからアプリまでの可視化（DEM）**

デバイスからアプリまで全ての「道筋」を可視化
通信の不調や遅延をリアルタイムで監視

(Mon) 2026-03-23 00:00 – (Mon) 2026-03-30 00:00 | Auto (1 hour)

Applications Overview | Application Details | Path Performance

Steered | Bypassed | AVG | Application = vietnam-gov-vn | Site | Country | Other Filters


Digital Experience Management

User Overview
Tenant Overview
Network Steering
Client Steering
NPA
Email Outbound
Bandwidth Consumption
Alerts

ADVANCED DIAGNOSTICS
Sites
Applications

SETTINGS
Monitoring Sources
Topologies
Monitoring Policies

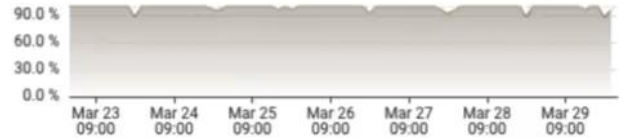
Settings
Help
Account


## Overview

**Availability**
99.0 %

**Tests**
2.0 k

**Availability**




## Performance Metrics Summary


## Sites

Site | Continent | Country | Region | City

☑ Sites to Pops ☑ POPs ☑ POPs to Apps ☑ End-to-End

| | | | | Site to POPs | | | POPs | POPs to Apps | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Site | POP | Availability | DNS AVG | Connection AVG | TLS AVG | Transit AVG | Connection AVG | TLS AVG | Server AVG | Redirects |
| kk-tokyo-office-site | JP-NRT2 | 99.0 % | 218 ms | 8.1 ms | 13 ms | 450 ms | 118 ms | 118 ms | 168 ms | 0 |

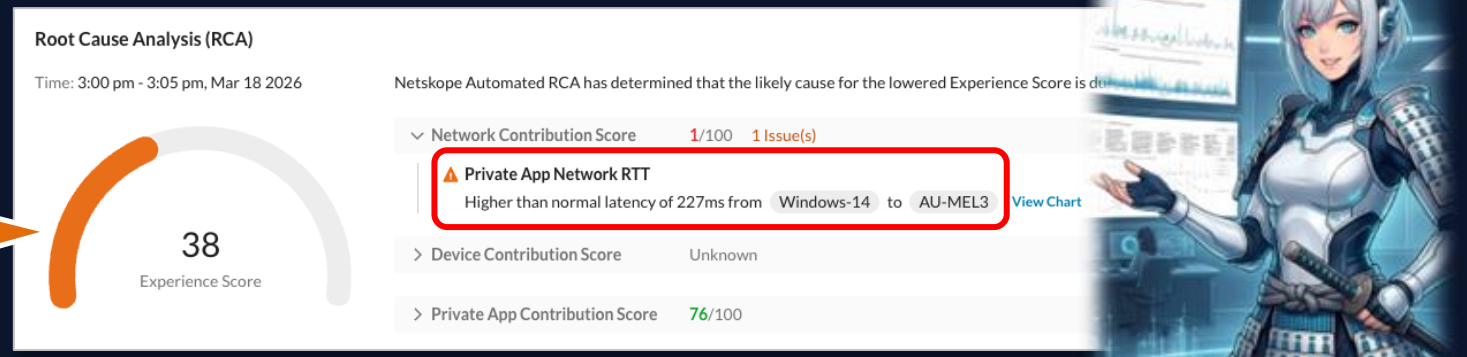
## Servers

Application | URL ☑ Sites to POPs ☑ POPs ☑ POPs to Apps ☑ End-to-End

| | | | Site to POPs | | | POPs | POPs to Apps | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Target IP | Target Country | Availability | DNS AVG | Connection AVG | TLS AVG | Transit AVG | Connection AVG | TLS AVG | Server AVG | Redirec |
| 14.225.10.58 | Viet Nam | 98.4 % | 228 ms | 8.1 ms | 14 ms | 467 ms | 122 ms | 118 ms | 171 ms | |

# AI によるピンポイント検知＆解析

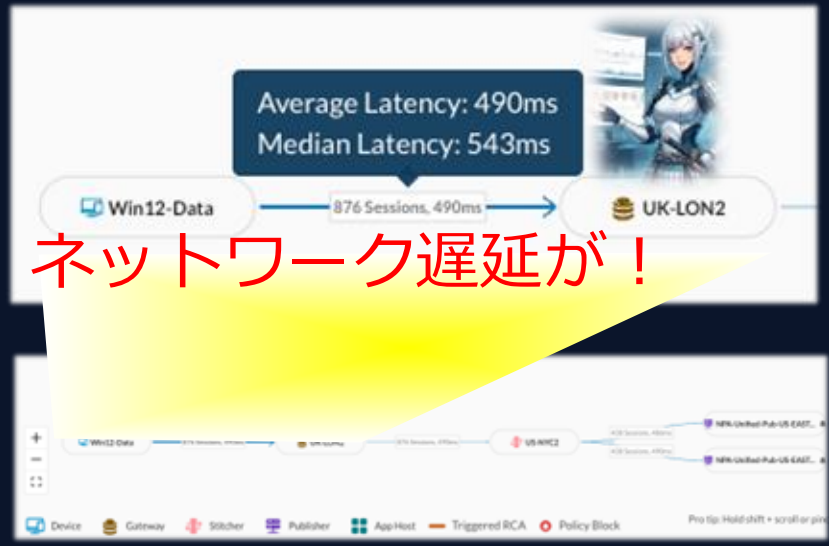
DXスコア
根本原因解析



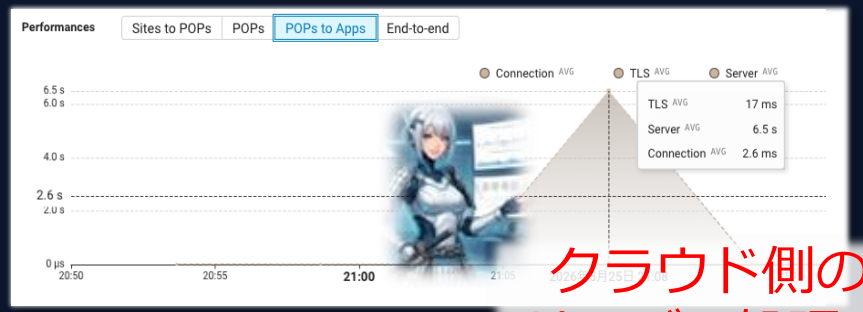



## Wi-Fi接続


## ISPネットワーク




## SaaS サーバー処理


クラウド側の
サーバー処理で
6.5秒の遅延が

# チャット型データ分析（β版）

Digital Experience Management / Insights

Insights　P95 Metrics　Widgets　Ask Data Intelligence Agent

## Netskope One Data Intelligence Agent

Managing digital experiences in your organization through intelligent conversations

Try one of these suggestions to get started

- Which applications are slow?
- Which applications have the highest error rates?
- Which applications are consuming the most resources?
- Which applications have both transaction and probe data available?

Can you list up applications and users with low experience score within 24 hours ?

この３日間で、DX値が60以下だったアプリケーションとユーザーをリストアップして原因解析をしてください

Netskope Data Intelligence Agent can make mistakes. Please double-check responses.

### データ分析

過去24時間で、15のユーザーとアプリケーションの組み合わせにおいて、ユーザーエクスペリエンススコアが低い（70未満）ことが判明し、6つのアプリケーションで4人のユーザーに影響が出ました。

**主な調査結果：**

- 10.100.12.4 にアクセスした 2 人のユーザー (jocelyn.reyes@netskope.com と jdavis@netskope.com) は、デバイスのパフォーマンスは完璧であるにもかかわらず、ネットワーク スコアが 0 であることのみが原因で、エクスペリエンス スコアが 3 と 39 という極めて低い値を示しています。
- rdeen@netskope.com は、Salesforce.com、JIRA、Dropbox、および Microsoft Office 365 Suite 全体で一貫してパフォーマンスが低く (スコア 41～59)、デバイス スコアが 73.21 であることから、デバイス側に中程度の問題があることが示されています。
- tbrown@netskope.com は、デバイススコアが 0 であるにもかかわらず、JIRA、Dropbox、Microsoft Office 365 Suite、Salesforce.com のネットワークスコアが 100 と完璧なパターンを示しており、デバイスレベルの問題を示唆している。
- Salesforce.comは最もパフォーマンスのばらつきが大きく、3人のユーザー間でエクスペリエンススコアが41から59まで変動し、1つのインスタンスではアプリケーションスコアが22という極めて低い値を示しました。
- 低評価のユーザー体験スコアはすべて早朝（午前5時～6時）に記録されており、オフピーク時のインフラまたは接続の問題の可能性を示唆している。

**ビジネスインサイト：**

データからは、2つの異なる根本原因が明らかになりました。1つは、IPベースのアプリケーション10.100.12.4へのアクセスに影響を与えるネットワーク接続障害（ネットワークスコア0）であり、もう1つは、rdeen@netskope.comとtbrown@netskope.comに影響を与えるデバイスのパフォーマンス低下です。問題が営業時間前（午前5時～6時）に集中していることから、潜在的なメンテナンス期間、バックアップ操作、またはオフピーク時のインフラストラクチャ容量の低下が考えられます。ネットワーク接続の問題については、ルーティング、VPNトンネル、またはファイアウォール構成を直ちに調査する必要があります。一方、デバイス側の問題は、リソースの制約、クライアントソフトウェアの旧バージョン、またはエンドポイントのトラブルシューティングを必要とするローカルシステムの問題を示している可能性があります。

**推奨される次のステップ：**

- 10.100.12.4 にアクセスするユーザーのネットワーク接続を調査し、ネットワークスコアが 0 になる原因となっているルーティングまたはトンネルの障害を特定します。
- tbrown@netskope.com (デバイススコア 0) と rdeen@netskope.com (デバイススコア 73.21) のデバイス健全性指標を調べて、CPU、メモリ、またはクライアントソフトウェアの問題を特定します。
- 午前5時から6時の時間帯にインフラ容量とメンテナンススケジュールを確認し、オフピーク時の運用がユーザーエクスペリエンスに影響を与えているかどうかを判断します。

| アプリケーション名 | ユーザーID | 経験値 | デバイススコア | アプリスコア |
|---|---|---|---|---|
| 10.100.12.4 | jocelyn.reyes@netskope.com | 3 | 100 | ヌル |
| 10.100.12.4 | jdavis@netskope.com | 39 | 100 | ヌル |
| Salesforce.com | rdeen@netskope.com | 41 | 73.21 | 22 |
| アトラシアン - JIRA | jdavis@netskope.com | 52 | 100 | ヌル |
| アトラシアン - JIRA | rdeen@netskope.com | 52 | 73.21 | ヌル |

Powered by Google NotebookLM

# 【状況報告】パフォーマンス低下の根本要因とNext Steps

過去3日間のスコア低下（エクスペリエンススコア60未満・全75件）は、深刻な「ネットワーク品質低下」が牽引。
社内アプリとSaaS（Salesforce）で異なる障害傾向を確認し、3方向からの原因究明に着手。

## 1. 低下要因の内訳


⚠ 最主要因: ネットワークスコア「0」を記録する致命的な深刻ケースが、全体の数値を大きく押し下げている。

## 2. 主要な問題発生ターゲットの比較

### 社内アプリ (10.100.12.4)
[ プライベート/内部アプリ ]

- 影響度: 【最高】（最悪スコア 2, 24, 39 を記録 / ネットワークスコア0が原因）
- 頻度・特徴: 局所的・ターゲット型（特定の場所や環境に依存）
- 最悪記録: 6月9日 5:05 AM に特定ユーザーがスコア「2」を記録
- 推定要因: 内部インフラ、または Private Access ルーティングの異常

### Salesforce.com
[ SaaS ]

- 影響度: 中 ～ 高 （11件のインスタンス、複数ユーザーに広範囲に影響）
- 頻度・特徴: 広範なユーザーの間で頻発
- 最悪記録: システム全体に及ぶ多数のアラート
- 推定要因: システム全体にわたるSaaS側の劣化、または宛先への経路問題

## 3. 根本原因の推測と次のステップ

⚠ 警告箇所: 「ユーザー端末 ～ Netskope POP」および「Netskope POP ～ 各アプリ」間の通信経路

### ① ネットワーク経路の調査

対象: ネットワークスコア「0」のユーザー
アクション: Tunnel RTT（往復遅延時間）や Traceroute の統計、POPからアプリへのレイテンシ確認。
目的: ボトルネック箇所（クライアント側 / ISPバックボーン / 宛先インフラ）の特定。

### ② Salesforceのトレンド分析

アクション: 過去1週間のパフォーマンス推移を確認。
目的: 最近の劣化が「一時的なもの」か「継続的な問題」かの見極め。

### ③ デバイスの健全性確認

対象: 複合的要因（Mised issues）を抱えるユーザー
アクション: 端末のメトリクス（CPUやメモリの利用状況など）を確認。
目的: クライアント側のリソース不足による影響の可能性を排除。

NotebookLM

# WE ARE ONE TEAM

## 三人が力を合わせて
## これからのAI時代に人類を守る！

Netskope One Platformこそが、AIモンスターに支配されないセキュアで快適な
DX世界を実現する、現代企業のための「唯一無二のヒーロー」です。


アンケートよろしくお願いいたします

# 是非、みなさんの声をお聞かせください

ありがとうございました