ネットワークとセキュリティの分離はもう限界

運用のシンプル化と AI時代に備えるセキュリティ対策の最前線

シスコシステムズ合同会社
セキュリティ事業
アカウントエグゼクティブ
藤田　佑未子

シスコシステムズ合同会社
スケールビジネス部　広域法人エンジニアリング部
ソリューションズエンジニア
Vlad Ivanovic（ヴラッド　イヴァノヴィチ）

Nov 4, 2026

Agenda

- 国内の不正アクセス動向と国が求める対策
- ゼロトラストを実現する Ciscoの解決策
- Secure Access ＋ Meraki による運用のシンプル化
  - Meraki SD-WAN / AutoVPN と VPNaaS＋ZTNA の無理のない段階移行
  - Cisco Duo 連携による User Trust Level 動的アクセス制御
- 可視性の向上（DEM）によるトラブル対応の迅速化
  - Experience Insights による通信遅延・障害原因の即時特定
- AI対応まで見据えたセキュリティポリシーの集中管理
  - シャドーAI対策・データ持ち出し防止（DLP）と包括的SSE
- デモンストレーション
- まとめ
- Q&A

© 2026 Cisco and/or its affiliates. All rights reserved.

国内の不正アクセス動向と国が求める対策

情報漏洩インシデントの「5大攻撃パターン」

① 境界VPN・露出管理機能の悪用	VPN機器の脆弱性突破に加え、インターネットに露出した社内管理画面・CMSの脆弱性を直接攻撃
② 委託先SaaSの連鎖侵害	自社が堅牢でも、利用中の問い合わせSaaSや保守会社が侵害され、複数顧客のDBが横串で窃取
③ Web API認可不備・A2B攻撃	アプリを解析してバックエンドAPIを特定し、認可制御の不備を突いて大量の会員データを自動スクレイピング
④ 仮想化基盤標的ランサムウェア	個別端末ではなく仮想化基盤（ハイパーバイザー）とオンラインバックアップを同時に暗号化し事業停止
⑤ 人的・運用ミス（全体の25%）	サイバー攻撃を伴わない設定ミス（何年間も気づかれず放置）、非表示シート残存、外部生成AIへの誤入力

© 2026 Cisco and/or its affiliates. All rights reserved.

背景：攻撃側の「産業化」とAIによる効率化



分業化したRaaSエコシステム

開発者・侵入担当・交渉担当が分業し、技術のない犯罪者も参入可能に。Qilinは幹部拘束後もリークサイトへの掲載が続き、1人の逮捕では止まらない



生成AIによる攻撃の量産

偵察・フィッシング文面・脆弱性調査・マルウェア開発にAIが使われ、攻撃の速度と規模が拡大。侵入後の操作をAIエージェントが担ったとみられる事案も報告



窃取データの換金ルート

本人確認画像・口座情報・認証情報は闇市場で売買され、二次被害（なりすまし・フィッシング）の原資になる。暗号化せず窃取だけで恐喝する手口も増加

© 2026 Cisco and/or its affiliates. All rights reserved.

不正アクセスによる漏えい等の事案を踏まえた対応について



総務省
MIC Ministry of Internal Affairs and Communications

○ よく見られるページ　○ ご意見・ご提案　○ ENGLISH(TOP)

総務省の紹介 ｜ 報道・広報 ｜ 政策 ｜ 組織案内 ｜ 所管法令

総務省トップ > お知らせ > 不正アクセスによる情報漏えい等の事案を踏まえた対応について（注意喚起）

お知らせ

令和8年10月9日

不正アクセスによる情報漏えい等の事案を踏まえた対応について（注意喚起）

大量の個人情報を取り扱う事業者等の情報システムが不正アクセスにより侵入され、個人情報を含むデータが窃取される事案が相次いで確認されています。

このような状況を踏まえ、内閣官房国家サイバー統括室から、事業者等に対し、迅速な脆弱性対応や、多要素認証等の認証機能の強化、漏えいした情報の悪用を防止する対策等について、委託先も含めた一層の対策の徹底を速やかに検討するよう、注意喚起が行われています。

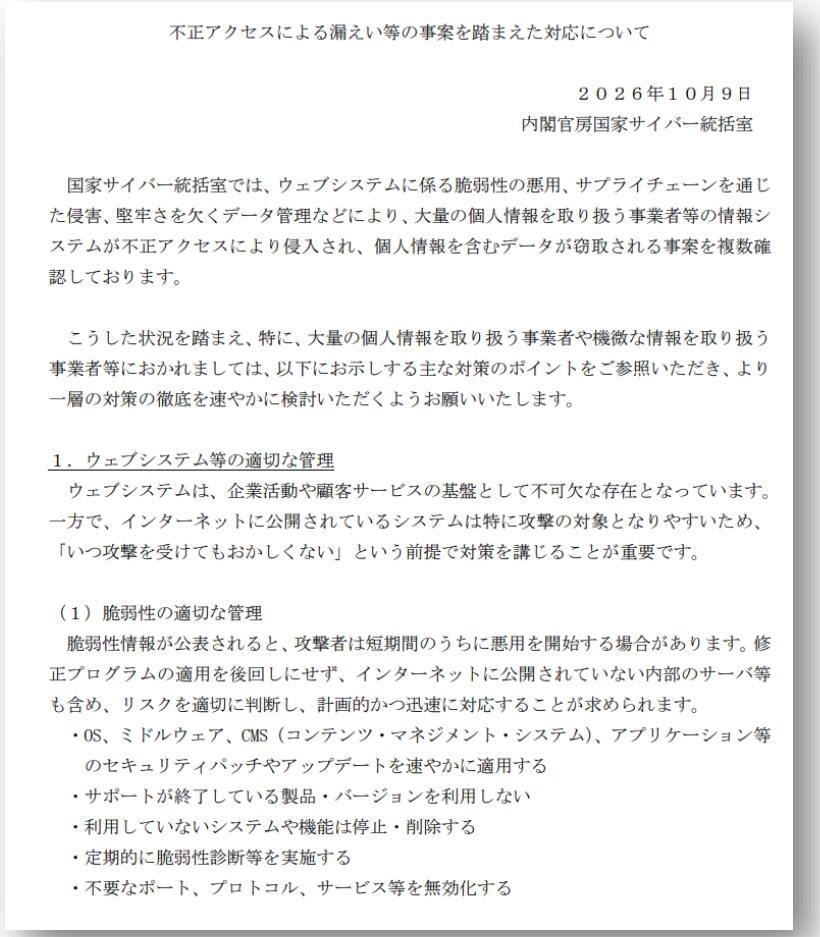
総務省においても、所管事業者及び関係団体に対し、同内容の注意喚起を行いました。事業者の皆様におかれましては、経営層のリーダーシップの下、サイバーセキュリティ対策の一層の強化に取り組んでいただくようお願いいたします。特に、大量の個人情報を保有する事業者や機微な情報を取り扱う事業者等におかれましては、十分に御注意ください。

○不正アクセスによる漏えい等の事案を踏まえた対応について（国家サイバー統括室）
https://www.cyber.go.jp/pdf/press/taiou.pdf

参考情報として、個人情報保護委員会及びJPCERT/CCによる注意喚起についても、以下のとおりお知らせします。

○大規模な漏えい等事案を踏まえた対応について（注意喚起）［個人情報保護委員会］
https://www.ppc.go.jp/news/press/2026/261007_houdou/

○直近で相次いでいる国内組織における不正アクセスに関する注意喚起［JPCERT/CC］
https://www.jpcert.or.jp/at/2026/at260030.html



不正アクセスによる漏えい等の事案を踏まえた対応について

２０２６年１０月９日
内閣官房国家サイバー統括室

国家サイバー統括室では、ウェブシステムに係る脆弱性の悪用、サプライチェーンを通じた侵害、堅牢さを欠くデータ管理などにより、大量の個人情報を取り扱う事業者等の情報システムが不正アクセスにより侵入され、個人情報を含むデータが窃取される事案を複数確認しております。

こうした状況を踏まえ、特に、大量の個人情報を取り扱う事業者や機微な情報を取り扱う事業者等におかれましては、以下にお示しする主な対策のポイントをご参照いただき、より一層の対策の徹底を速やかに検討いただくようお願いいたします。

１．ウェブシステム等の適切な管理

ウェブシステムは、企業活動や顧客サービスの基盤として不可欠な存在となっています。一方で、インターネットに公開されているシステムは特に攻撃の対象となりやすいため、「いつ攻撃を受けてもおかしくない」という前提で対策を講じることが重要です。

（１）脆弱性の適切な管理

脆弱性情報が公表されると、攻撃者は短期間のうちに悪用を開始する場合があります。修正プログラムの適用を後回しにせず、インターネットに公開されていない内部のサーバ等も含め、リスクを適切に判断し、計画的かつ迅速に対応することが求められます。

・OS、ミドルウェア、CMS（コンテンツ・マネジメント・システム）、アプリケーション等のセキュリティパッチやアップデートを速やかに適用する
・サポートが終了している製品・バージョンを利用しない
・利用していないシステムや機能は停止・削除する
・定期的に脆弱性診断等を実施する
・不要なポート、プロトコル、サービス等を無効化する

https://www.cyber.go.jp/pdf/press/taiou.pdf

© 2026 Cisco and/or its affiliates. All rights reserved.

国が求める対策ポイント

1. ウェブシステム等の適切な管理

1) 脆弱性の適切な管理
インターネットに公開されていない
内部のサーバ等も含める

2) アカウント管理・認証
・MFAを導入する
・アクセス権を必要最小限にする
・不要なアカウントを速やかに
無効化する

3) レジリエンスの向上
ログを適切に取得・保管する
不正な通信やアクセスを監視する
外部からの異常な認証試行を把握する

2. サプライチェーンを通じた侵害への対策

1) 委託先企業等のセキュリティ対策状況の
把握

2) 委託契約におけるセキュリティ要件の
明確化

3) 情報共有範囲の適正化

4) サプライチェーン全体のリスクマネジメント

3. データの適切な管理

1) 保有する情報資産の適切な管理

2) 保有情報の最小化

3) 適切なアカウント管理・アクセス制御
・業務上必要な者のみにアクセスを許可する
・閲覧権限と更新権限を適切に分離する
・管理者権限の付与を必要最小限とする
・定期的にアカウントや権限設定を確認する

4) データ保護の徹底

5) ログ取得・監視・分析の強化

© 2026 Cisco and/or its affiliates. All rights reserved.

Ciscoの解決策

優先すべき対策とCiscoソリューションの対応（全体像）

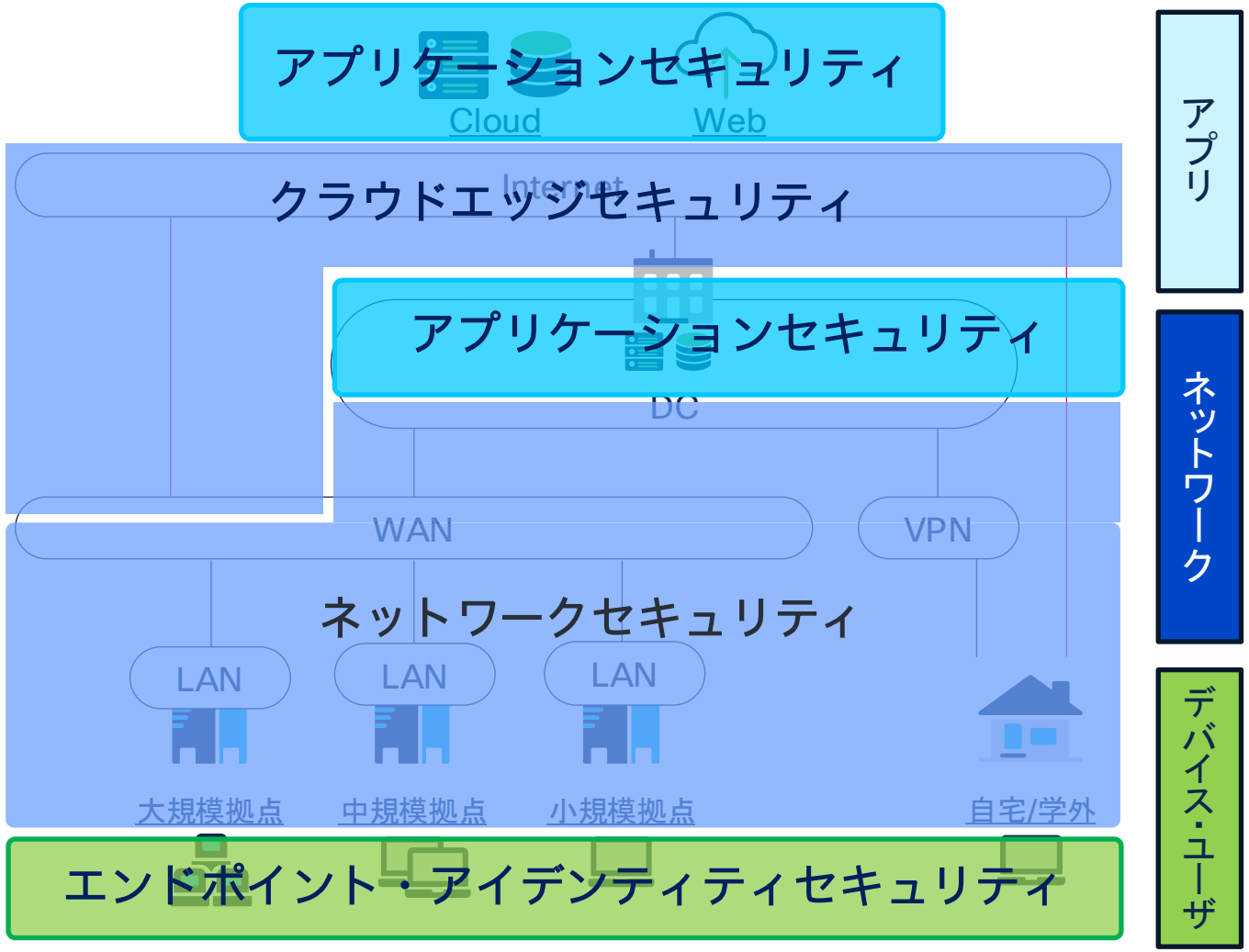
今後優先すべき対策	Ciscoの主なソリューション・サービス
1 境界・管理画面・APIのゼロトラスト化	・Secure Access（ZTNA）でVPN公開を廃止し、社内管理画面・業務システムを完全不可視化（Dark化） ・Live Protectによるパッチ適用前の実行時防御 ・Cisco IQでサポート切れ・脆弱性該当機器を自動可視化
2 委託先・アイデンティティと特権の管理	・Duo（全アカウントMFA・SSO・証明書レス端末ポスチャ） ・Cisco Identity Intelligence（休眠・過剰権限・放置トークンの自動検知） ・Secure Access（委託先アクセスを特定サーバーに限定し横展開を物理遮断）
3 正規アクセス異常検知とDLP	・Secure Access クラウドDLP（大量個人データの外部持ち出しをインライン遮断） ・Duo Passport（Cookie窃取対策）／Duo ITDR（異常時の即時セッション切断） ・Splunk Enterprise Security・Cisco XDR（異常アクセス相関分析）
4 持たない・分ける・戻せる（内部防衛・特権防御）	・Duo AD Defense（Kerberos/NTLMインラインMFAでAD特権昇格・横展開を阻止） ・Hypershield／Hybrid Mesh Firewall（セグメント分割） ・Multicloud Defense（クラウド保護、バックアップ連携）
5 ログ収集・管理・分析	・Splunk Enterprise Security・Cisco XDR（異常アクセス相関分析）

※製品名・機能は2026年10月時点の公開情報に基づく考察。国内での提供状況・ライセンス要件は個別に要確認

© 2026 Cisco and/or its affiliates. All rights reserved.

一般的なネットワーク構成における それぞれの役割範囲

既存のネットワーク環境をまるごとSASEに移行することが難しい場合が多く、SD-WANとの共存/連携を柔軟に設計、導入できることが重要。SASE化と同時にリモートアクセスの認証の強化は必要不可欠



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Secure AccessとMerakiによるネットワークセキュリティ対応

ネットワーク管理においてよくある課題

マルチベンダー環境による管理の煩雑化

ダッシュボードの乱立:
ベンダーごとに管理画面が分かれているため、ネットワーク全体の状況を把握するために複数のツールを使い分ける必要があり、管理が非常に煩雑

切り分けの複雑化:
トラブル発生時に、どのベンダーのどの製品に起因する問題なのかを特定するための切り分け作業に時間がかかり、迅速な復旧を妨げている

ネットワークの不可視化とトラブルシューティングの長期化

LAN/WANの可視化不足:
物理的な接続状況やトポロジーが可視化されておらず、LANからWANに至るまでの通信経路の状況を即座に把握できない

原因特定までの時間ロス:
「通信が遅い」といったユーザーからの不満に対し、過去のログ分析や詳細なデータ確認に多大な時間を要し、迅速な原因特定と解決が困難

ポリシー不整合によるセキュリティリスクの増大

セキュリティルールの不整合:
キャンパス、ブランチ、クラウドなど異なるドメインで個別にポリシーを構築しているため、ルールに不整合が生じやすく、設定ミスによるセキュリティホールが発生するリスク

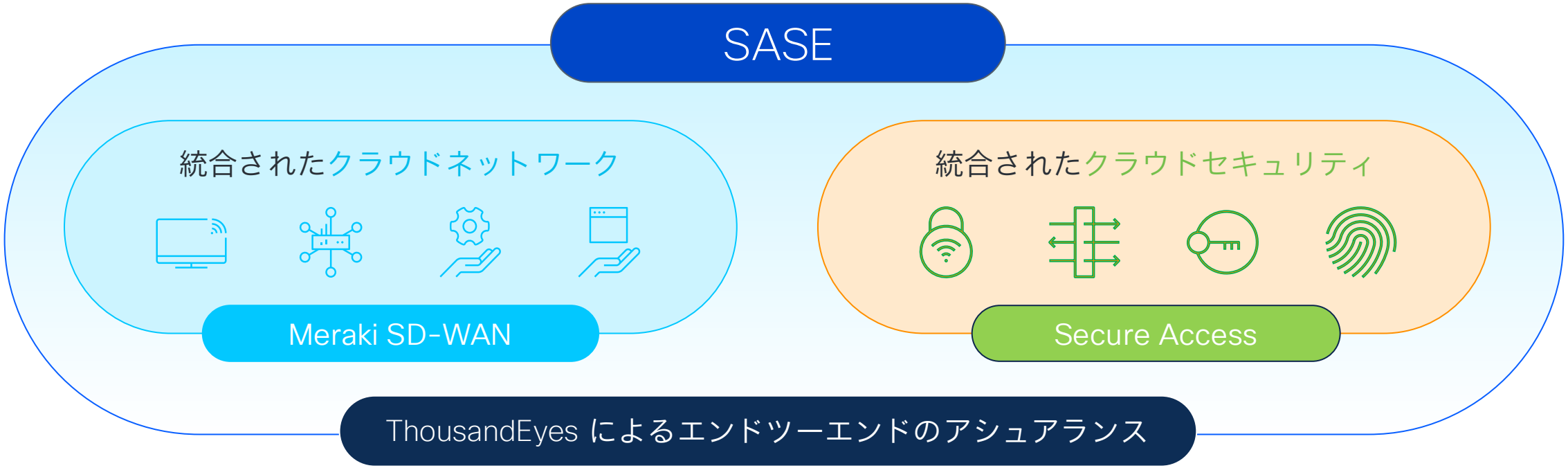
一貫性の欠如:
ネットワーク全体で統一されたセキュリティポリシーを維持できないことが、サイバー攻撃に対する防御力の低下

© 2026 Cisco and/or its affiliates. All rights reserved.

運用のシンプル化

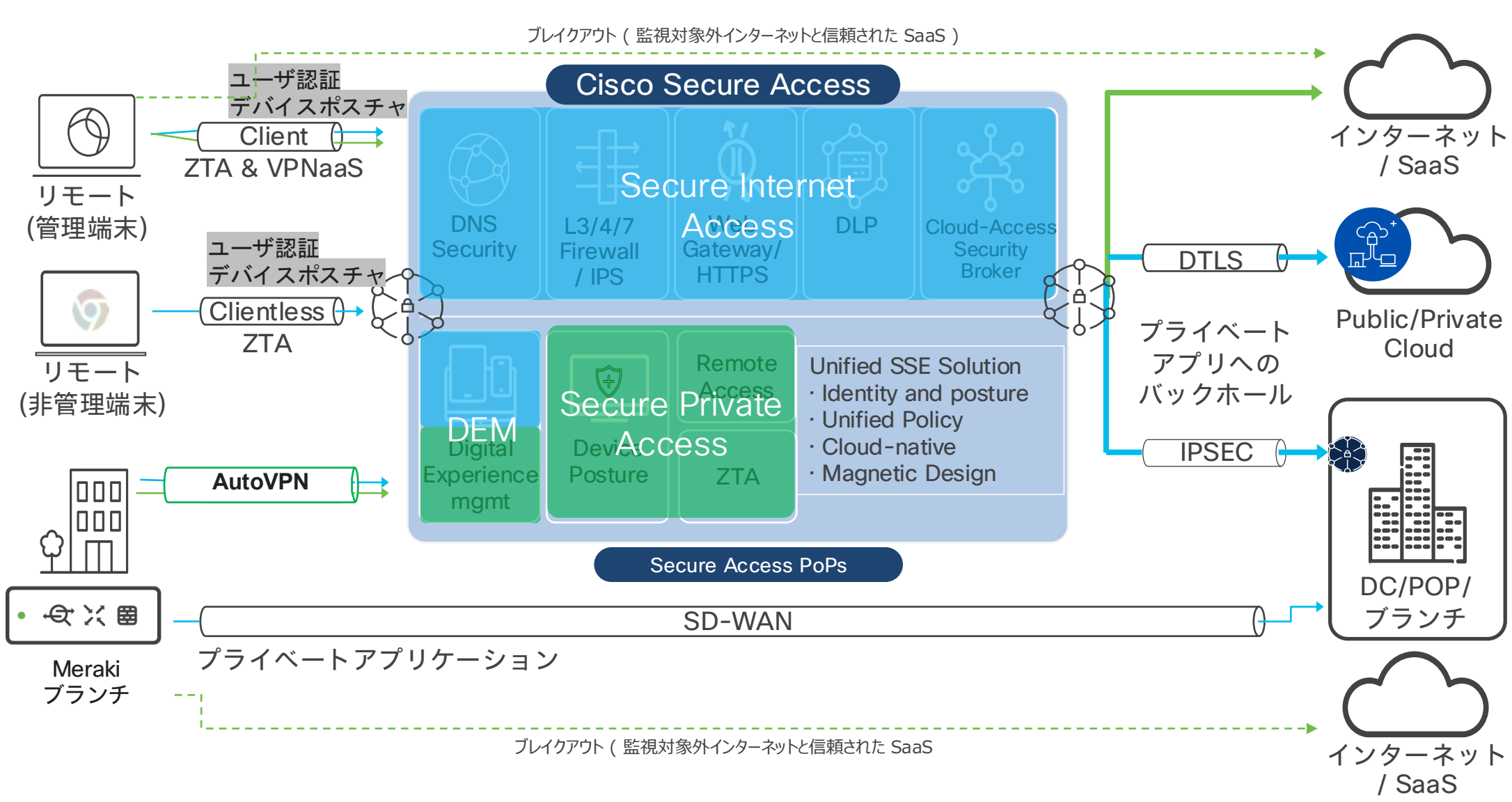
SASE：Secure Access と Meraki SD-WAN の統合

- ネットワーク（SD-WAN）とセキュリティの機能を統合して提供



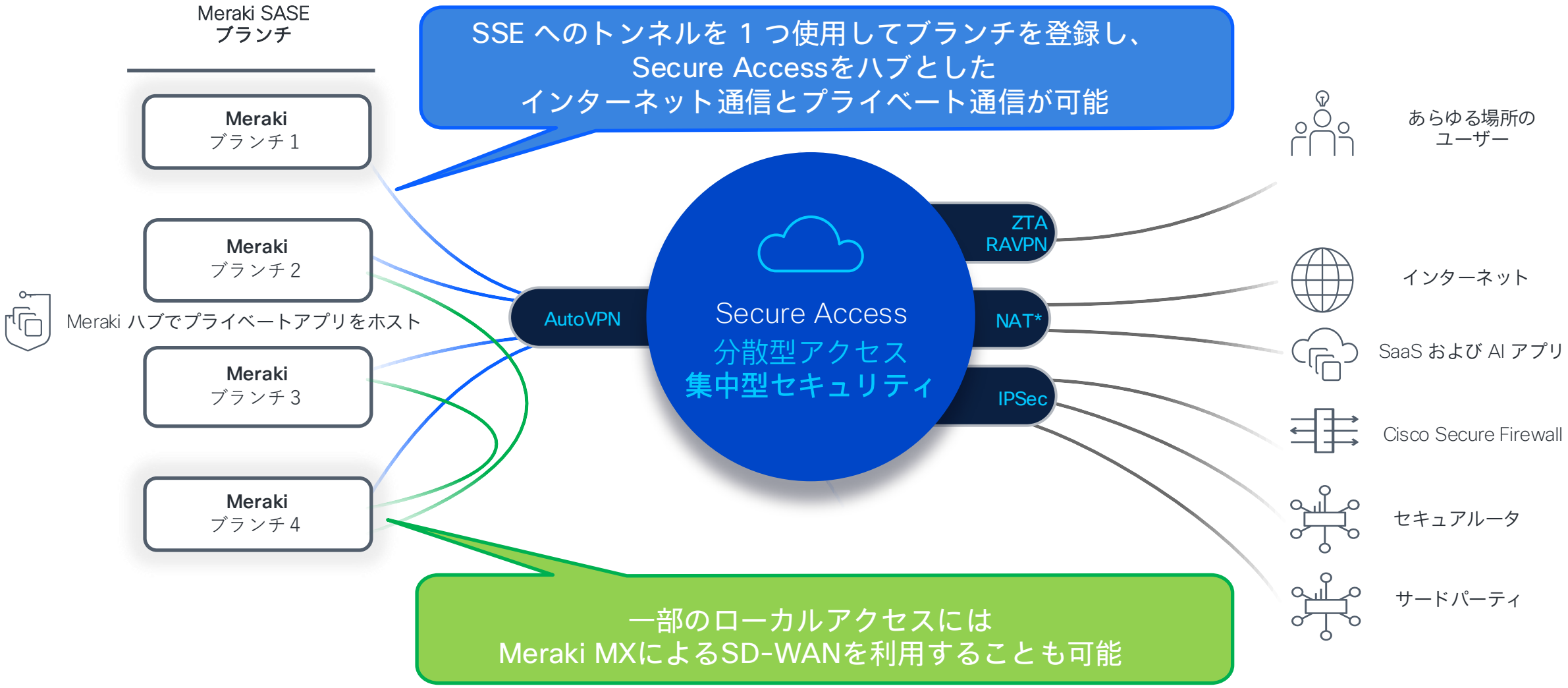
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Access 全体像



© 2025 Cisco and/or its affiliates. All rights reserved.

Meraki AutoVPN を Secure Access に拡張

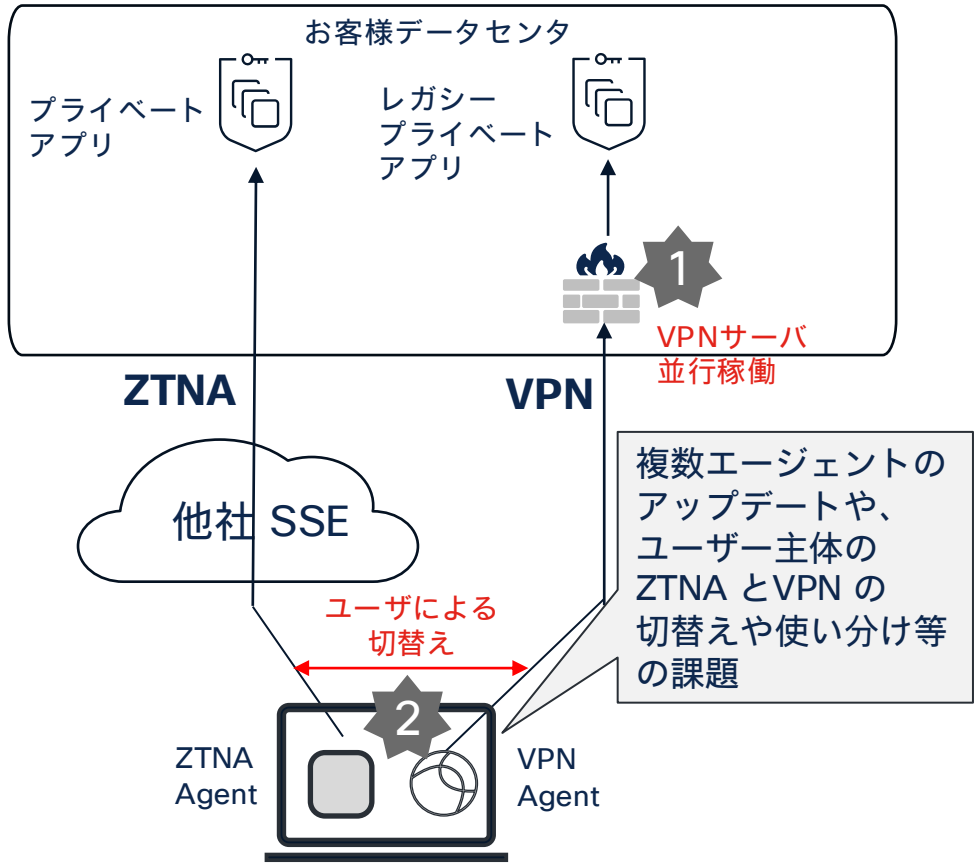


© 2026 Cisco and/or its affiliates. All rights reserved.

VPNaaSとZTNAの併用により無理なくSASEへ移行可能

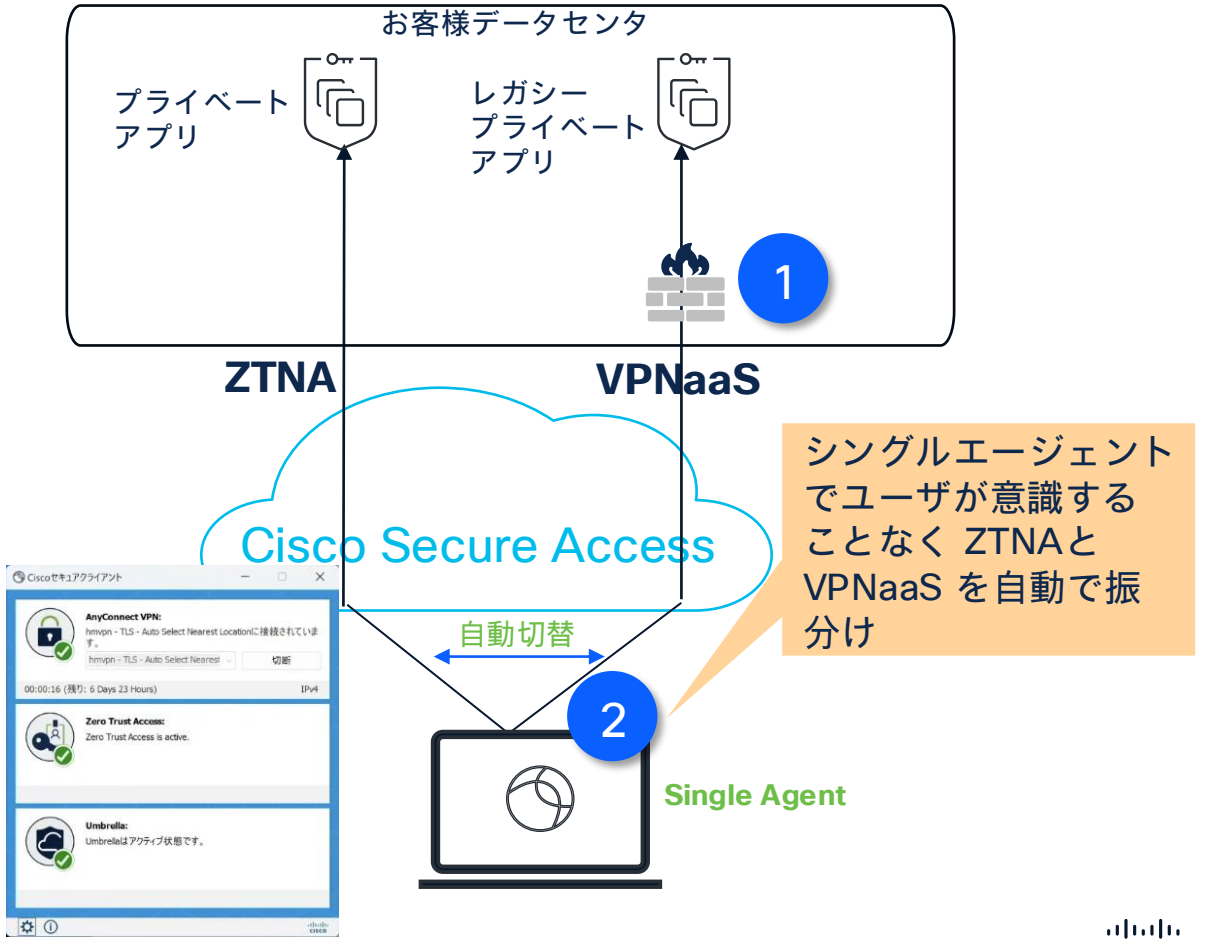
他社

レガシーアプリの ZTNA 非対応により、ZTNA と VPN の平行稼働となり、VPN の運用負担およびコストの増加



Cisco Secure Access

ZTNA と VPNaaS を利用可能なため既存 VPN を廃止することで並行稼働で発生していた運用負担とコストをなくすことが可能に



© 2025 Cisco and/or its affiliates. All rights reserved.

ユニファイドエージェントによる移行のシンプル化

一気にZTNAへ移行しようとすると
利用アプリの把握やZTNA非対応アプリなどにより失敗する例が多い

ZTNA

＋解決できる課題

- 最重要なアプリから**無理なくZTNA化可能**

クラウド型VPN
(VPN as a Service)

解決できること

- VPN機器管理不要
- クラウド型VPN Head-endが処理を行うため、**サイジング不要**
- デバイスポスチャ機能でアクセス時のセキュリティ強化

オンプレ
VPN

よくある課題

- ネットワーク集中による負荷増大
- ネットワーク機器管理の手間
- 脆弱性対策、セキュリティ維持運用



© 2025 Cisco and/or its affiliates. All rights reserved.

MFAもCisco Duoと統合して提供



Cisco Duo

- MFA
- デバイス認証
- User Trust Level

SecureAccess

- ZTNA
- VPN
- SaaS
- Direct

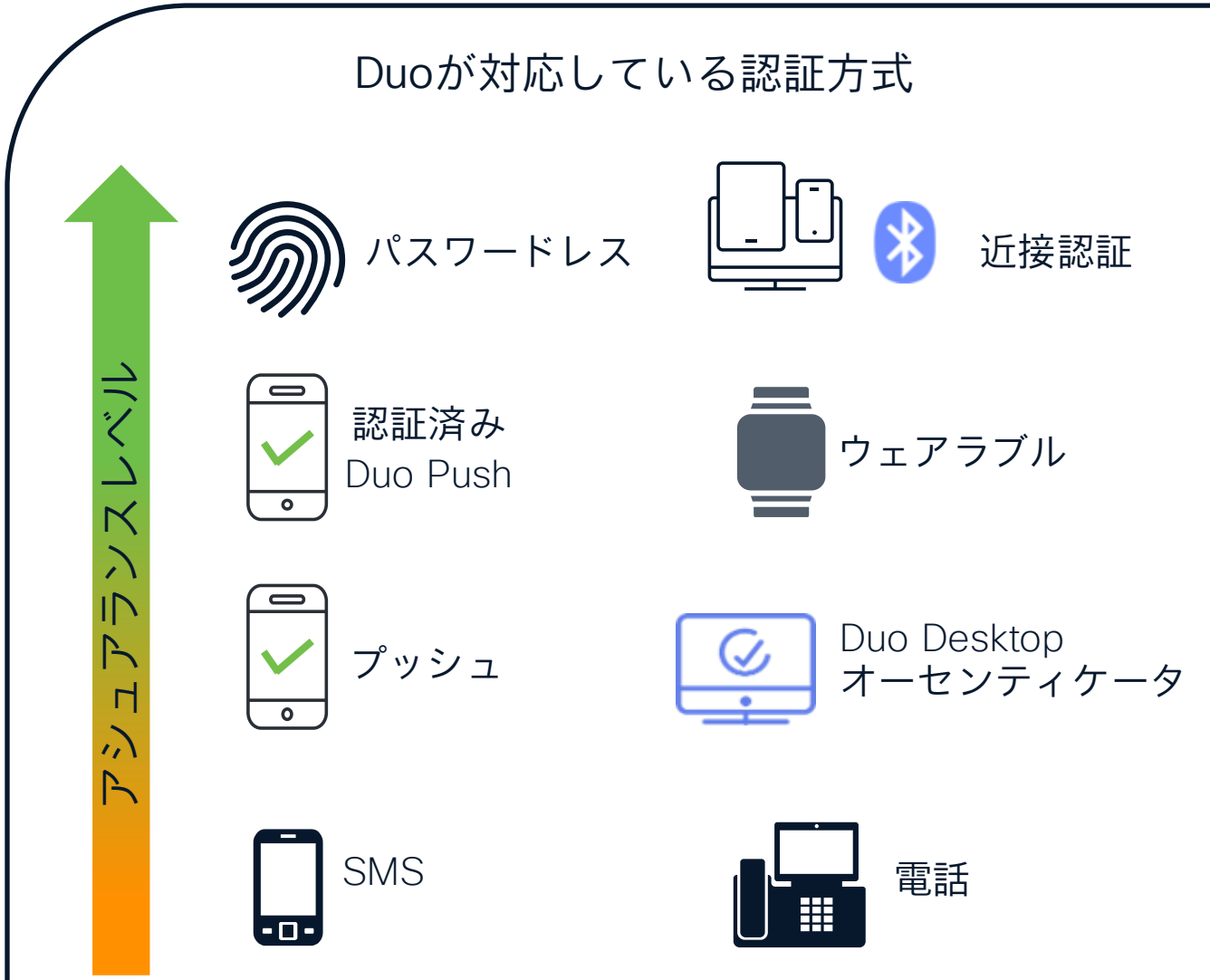
- Private apps
- Traditional apps
- SaaS apps
- Internet apps

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Duoによるフィッシングに強いMFA

詳しくは18日のWebinarで
ご紹介します

- 業界をリードする多様な認証手段
- ユーザーまたはアプリケーショングループごとに柔軟な認証ポリシーが設定可能
- フィッシングに強いMFA とパスワードレスを簡単に導入
- ニーズに応じて、複数の要素やオフラインの認証手段を展開



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Duo連携：User Trust Levelに基づく動的アクセス制御

ユーザの信頼度(User Trust Level)をDuoが検知し、Secure Accessがリスク度に応じたアクセス制御・遮断を自動適用

通常時：高信頼ユーザーのアクセス

ユーザー・端末
- 正規の社内PC
- FIDO2 MFA認証
- 端末ポスチャ健全

➔

Cisco Duo / CII
信頼度スコア判定
【Trusted】🟢
(リスクなし・高信頼)

➔ (即時共有)

Secure Access
動的ポリシー適用
【ALLOW (許可)】
ZTNA経由で接続

➔

業務リソース
- **社内Private App**
- 基幹DB / サーバー
- 業務SaaS (M365等)

✅ 【アクセス許可】

脅威検知時：User Trust低下による動的遮断

異常・侵害発生
- MFA連続拒否/疲労
- 海外/不審なIP
- EDR無効/感染兆候
- AD特権昇格試行

➔

Duo / CII 検知
信頼度を即時格下げ
【Untrusted】🔴
または
【Questionable】⚠
(信頼不可・危険)

➔ (シグナル通知)

Secure Access
動的ポリシー発動
【BLOCK (遮断)】
確立済セッションも切断・防御

✕

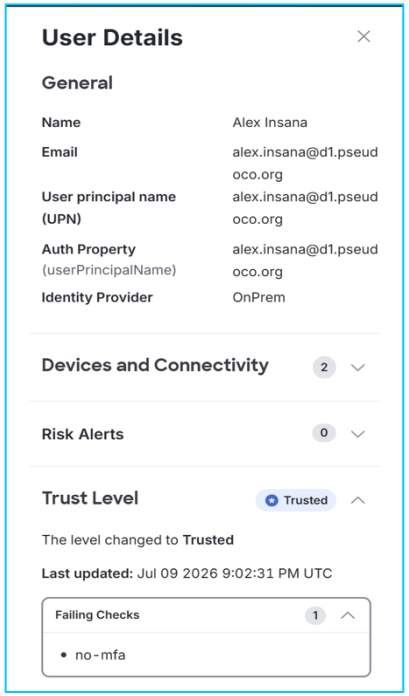
業務リソース
- **社内Private App**
- 機密DB / サーバー
- 業務SaaS (M365等)

⛔ 【アクセス遮断】
※内部横展開を阻止

User Trust Level と制御ポリシー

Duo/CII 信頼度 ➔ Secure Access 制御

- 🟢 **Trusted** ： 全アクセス許可 (通常利用)
- 🟢 **Favorable** ： 許可 (7日ごとに再認証)
- 🟡 **Neutral** ： 許可 (3日ごとに再認証)
- 🟠 **Questionable** ： 制限/追加認証 (24h毎)
- 🔴 **Untrusted** ： ⛔ 即時ブロック (遮断)
- ⚪ **Unknown** ： 追加認証要求 (24h毎)



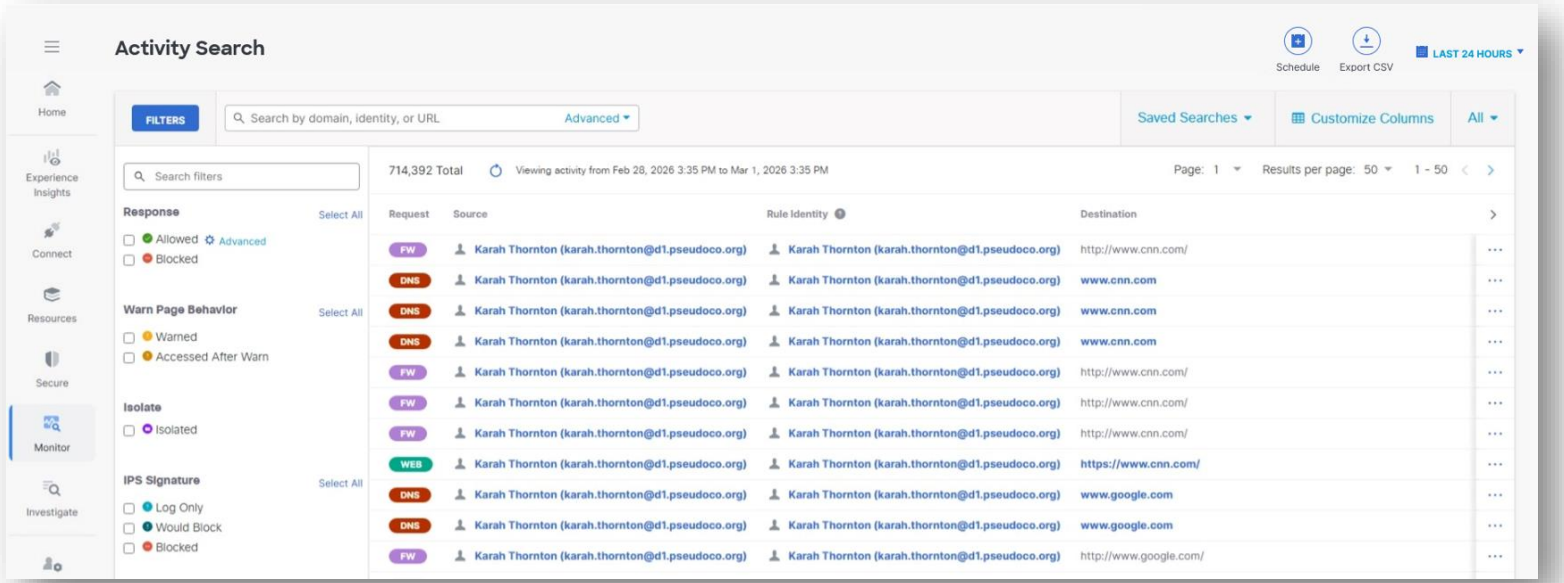
© 2025 Cisco and/or its affiliates. All rights reserved.

可視性の向上による
トラブル対応の迅速化

Secure Accessが処理した通信を一覧で確認可能

誰がどこにアクセスしようとしたのか、どのルールに基づいてどのようなアクションが行われたのかなど、様々な情報を一元的に確認可能

➢ Secure Accessログ画面



- 定期スケジューリング可能なレポート一覧
- Remote Access Log
- Activity Search
- Network Connectivity Log
- Total Requests
- Activity Volume
- Top Destinations
- Top Categories
- Data Loss Prevention
- Cloud Malware
- Events

➢ SIEMなどログの長期保管、分析連携可能

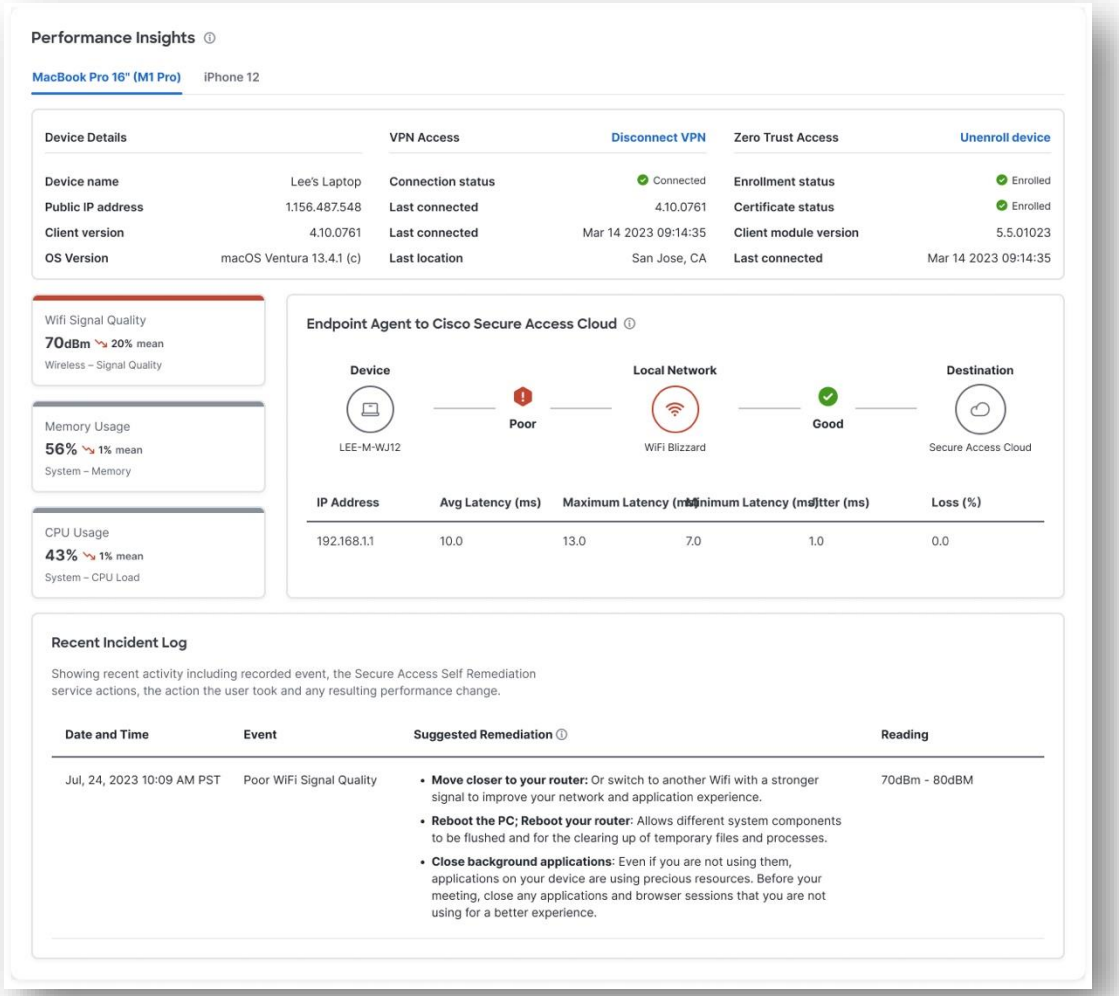


- CSVファイルまたはAmazon S3 にエクスポート可能
- Splunkをはじめ各種SIEMやTAPに連携可能

© 2026 Cisco and/or its affiliates. All rights reserved.

パフォーマンス監視も「シングル コンソール」

エクスペリエンス インサイト機能でネットワーク障害の調査工数を大幅削減



管理コンソールで通信の健全性を確認可能

- 端末環境の健全性、アプリケーション疎通、ネットワークの健全性を Cisco Secure Access が監視
- 通信障害による利用者からの問い合わせに対して、管理者が早期に原因を特定可能
- ネットワークオペレーションの負担を大幅に軽減

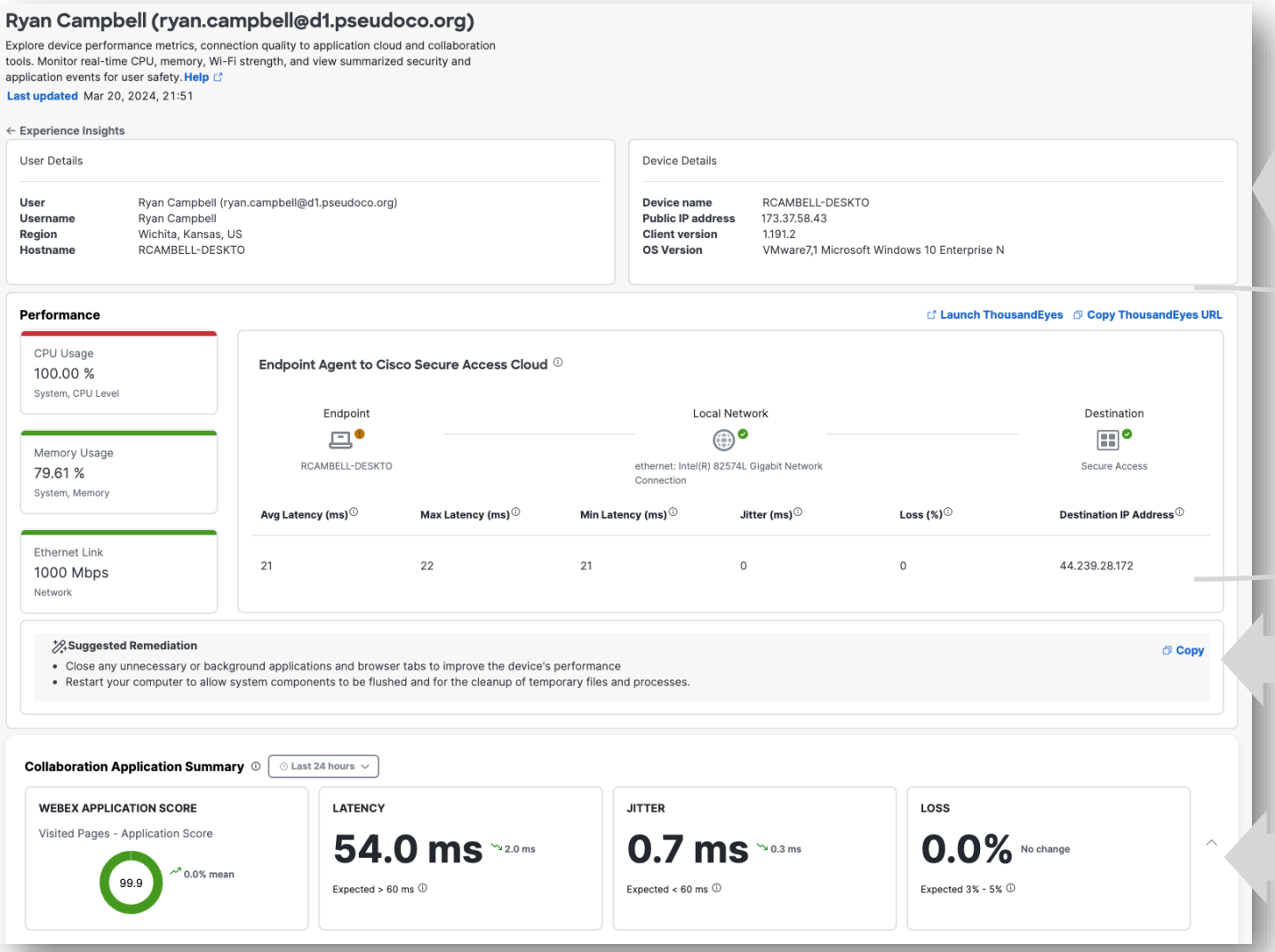
モニタリング可能な項目の例

- エンドポイントのパフォーマンス - CPU、メモリ、WiFi
- ネットワーク・パフォーマンス – Endpoint から Secure Access まで
- トップ 20 の SaaS アプリケーション パフォーマンス
- ユーザー固有のイベント

SASE で複雑化する日常的な問題を解決

© 2026 Cisco and/or its affiliates. All rights reserved.

ワークフォースの生産性をプロアクティブに監視



接続しているユーザの詳細

アプリへの接続性に影響する Local 無線 LAN、CPU、メモリのエラーを特定

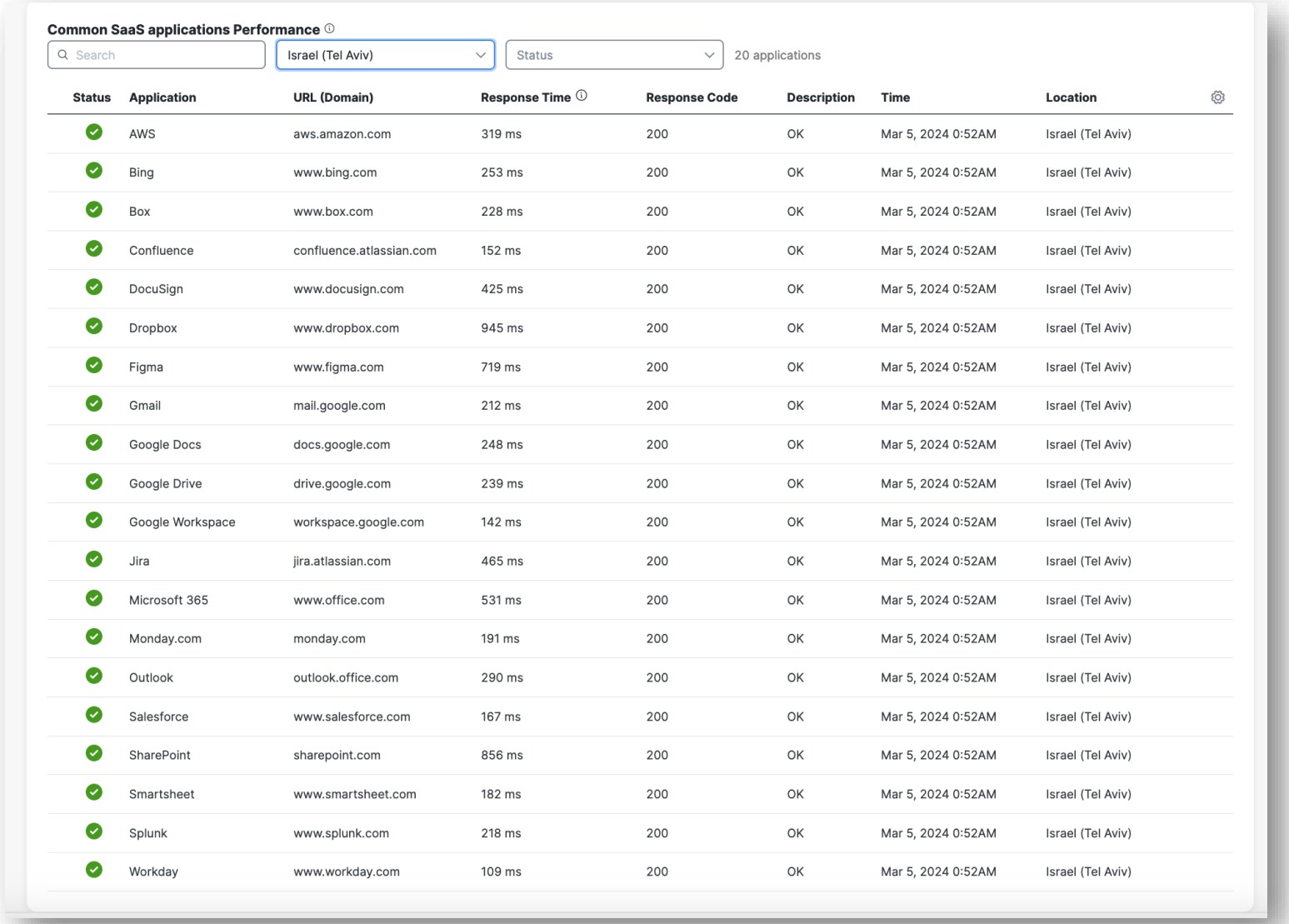
端末から Secure Access への接続品質

解決までの平均時間を短縮するための改善策のヒント

UcaaS モニタリング

© 2026 Cisco and/or its affiliates. All rights reserved.

アプリとネットワークのパフォーマンスの相関



Common SaaS applications Performance

Search | Israel (Tel Aviv) | Status | 20 applications

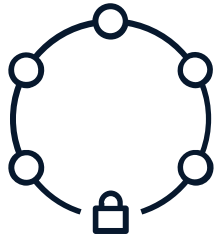
Status	Application	URL (Domain)	Response Time	Response Code	Description	Time	Location
✓	AWS	aws.amazon.com	319 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Bing	www.bing.com	253 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Box	www.box.com	228 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Confluence	confluence.atlassian.com	152 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	DocuSign	www.docusign.com	425 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Dropbox	www.dropbox.com	945 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Figma	www.figma.com	719 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Gmail	mail.google.com	212 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Google Docs	docs.google.com	248 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Google Drive	drive.google.com	239 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Google Workspace	workspace.google.com	142 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Jira	jira.atlassian.com	465 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Microsoft 365	www.office.com	531 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Monday.com	monday.com	191 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Outlook	outlook.office.com	290 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Salesforce	www.salesforce.com	167 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	SharePoint	sharepoint.com	856 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Smartsheet	www.smartsheet.com	182 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Splunk	www.splunk.com	218 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)
✓	Workday	www.workday.com	109 ms	200	OK	Mar 5, 2024 0:52AM	Israel (Tel Aviv)

- すべての Secure Access DC から上位 20 の SaaS アプリとそれらのパフォーマンスへ、ダッシュボードから簡単にアクセス
- 地域のパフォーマンス問題を迅速に診断
- ThousandEyes Enterprise Agents を使用して測定 (構成不可)

© 2026 Cisco and/or its affiliates. All rights reserved.

AI対応まで見据えた
セキュリティポリシーの集中管理

Cisco Secure Acces機能一覧
シングルベンダーで、必要な全てのSSE機能を提供



豊富な機能かつ柔軟な接続性をもつ
インターネットアクセス、プライベートアクセスを提供

- ゼロ トラスト ネットワーク アクセス (ZTNA)
- クラウド型 VPNサービス (VPNaaS)
- デバイスポスチャ
- モバイルZTNA
- 統合エージェント
- DNS レイヤ セキュリティ
- セキュア ウェブ ゲートウェイ(SWG)
- HTTPS復号
- クラウド提供型 ファイアウォール (L3-4, L7)
- クラウド提供型IPS
- クラウド セキュリティ アクセス ブローカ (CASB)
- SaaS テナント制御
- 情報漏えい防止 (DLP)
- ウェブ分離 (RBI)
- Talos脅威 インテリジェンス
- マルウェア対策 (Sandbox)
- クラウド マルウェア検知
- フルアクセスログ
- エクスペリエンス・ インサイト(DEM)
- AIアシスタント

© 2026 Cisco and/or its affiliates. All rights reserved.

Security for AI : AIアプリケーションの可視化と制御

発見

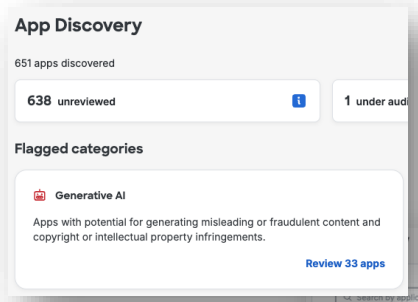
- 組織全体でのシャドー IT/AI アプリケーション の使用を発見

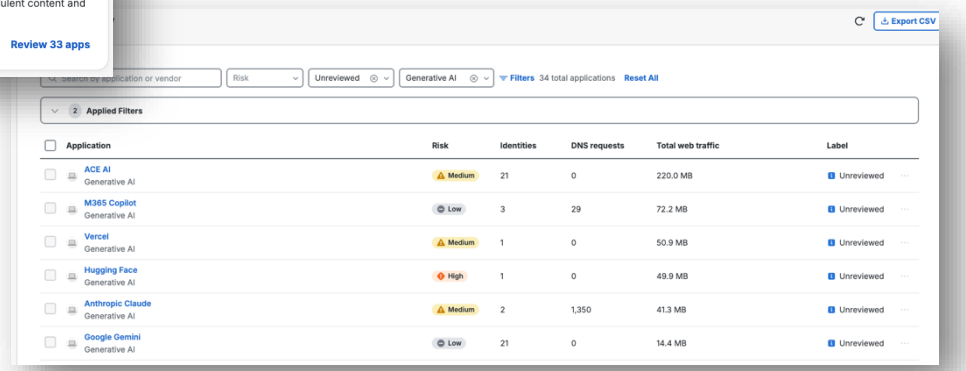
検出

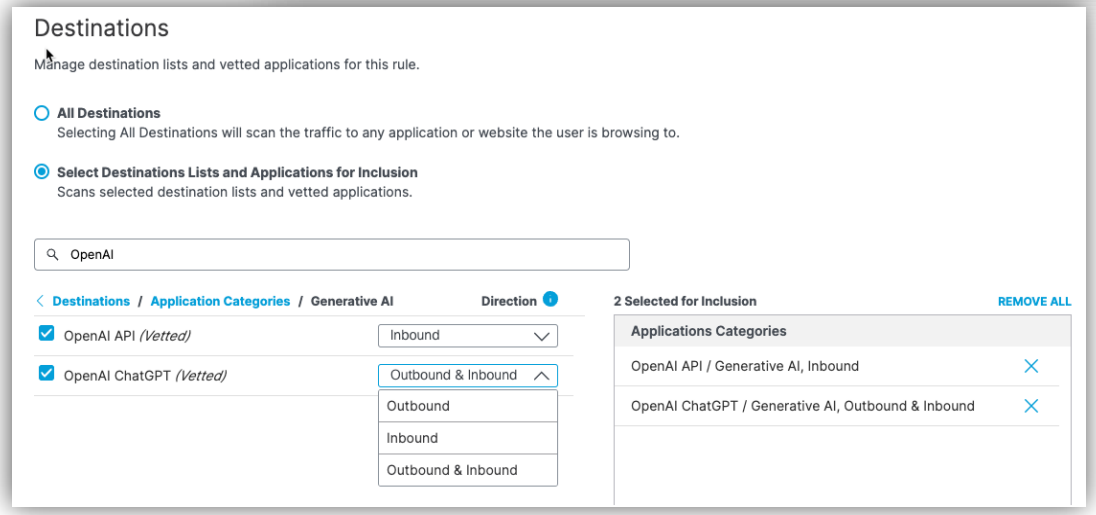
- サードパーティ製アプリのリスクを評価し、デバイス、場所、ネットワークなどに関するコンテキストを取得
- AIモデルとアプリを継続的に検証

保護

- ガードレールで機密データを保護
- プロンプト・インジェクションやDoSなどの脅威からの防御
- アプリやデータへのアクセスポリシーの設定
- 規制、フレームワーク、標準への準拠

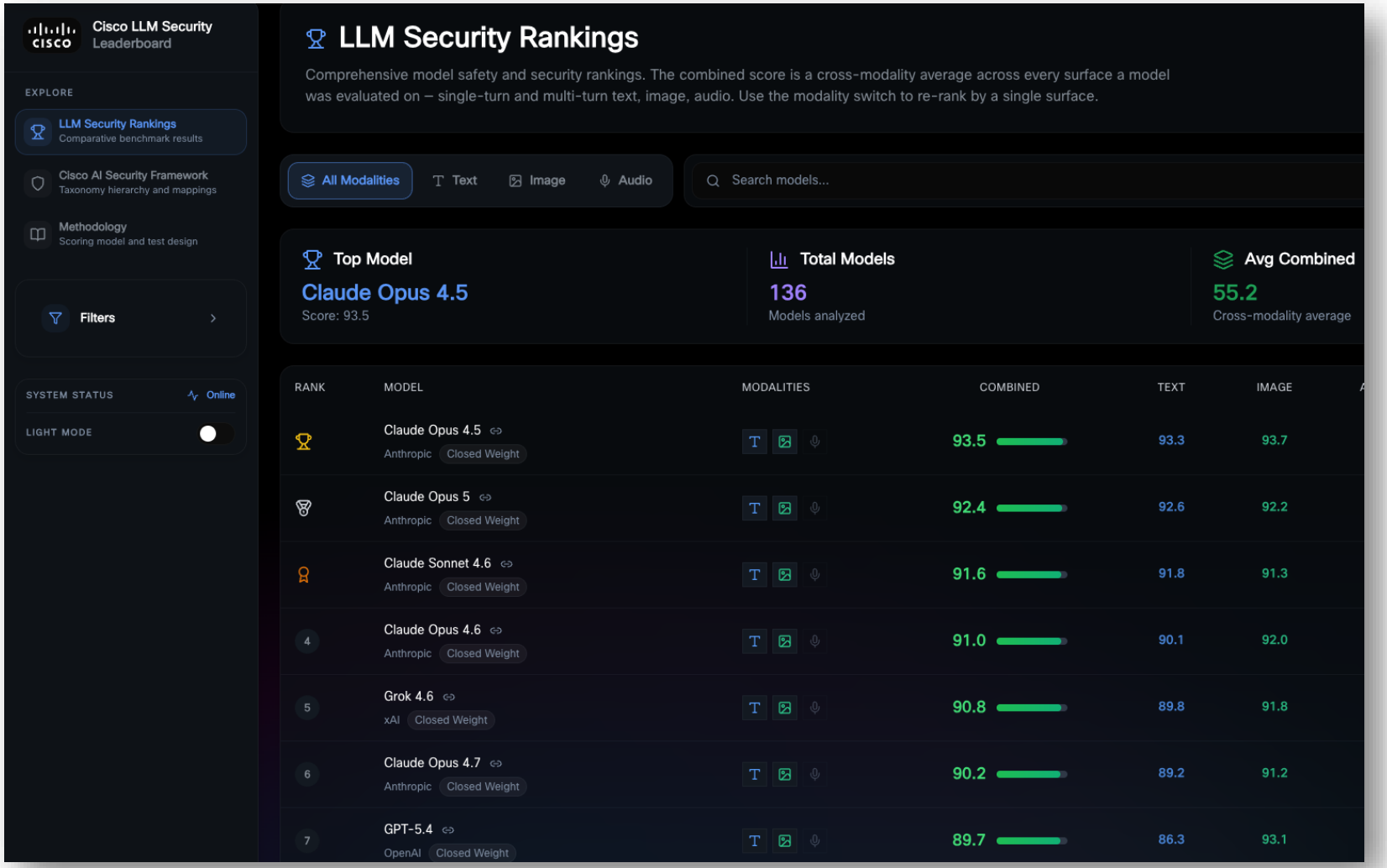






© 2026 Cisco and/or its affiliates. All rights reserved.

LLM Security Rankings



https://leaderboard.aidefense.cisco.com/rankings

© 2026 Cisco and/or its affiliates. All rights reserved.

デモンストレーション

© 2026 Cisco and/or its affiliates. All rights reserved.

まとめ

ネットワークとセキュリティを統合し、AI時代に備える4つの要点

～ 不正アクセス対策・SASE段階移行・Duo動的制御・DEM可視化からAI保護まで、シスコが届ける包括価値 ～

侵入前提の「ゼロトラスト防衛」への転換

- **境界防御の限界**
  侵入経路の9割はアクセス境界（VPN機器・露出管理画面・委託先）。脆弱性ゼロは不可能なため「侵入前提」の対策が急務。
- **国の要請に完全準拠**
  国家サイバー統括室の要請に沿い、耐フィッシングMFA、ZTNA化、ユーザーごとのアクセス制御を実現。

Secure Access ＋ Meraki による無理のないSASE化

- **Meraki AutoVPN による拠点接続の自動化**
  Merakiから数クリックでSecure Accessへのトンネルを展開。拠点側ルータの設定やAPIキー管理を自動化し、クラウドハブ接続を即座に確立。
- **VPNaaS ＋ ZTNA の自動振分け（Single Agent）**
  Cisco Secure Client単体でZTNAとVPNaaSを自動制御。クラウドVPNでレガシーアプリも並行収容しつつ、重要アプリから段階的にZTNA化が可能。

エンドツーエンド可視化とログ統合管理

- **Experience Insights（ThousandEyes統合）**
  端末環境（CPU/メモリ/Wi-Fi）、Secure Accessへの接続品質、上位20の主要SaaSの疎通状態をシングルコンソールで一元可視化。「通信が遅い」原因を即座に特定。
- **フルアクセスログとSIEM連携**
  誰が・どこへ・どのルールで通信したかを網羅的に記録。定期レポートの自動生成に加え、Splunk等のSIEMやクラウドストレージ（S3等）へログを連携・長期保管。

Duo動的アクセス制御と次世代「AIセキュリティ」

- **Duo × User Trust Level 動的制御**
  耐フィッシングMFAに加え、CIIが判定したユーザー信頼度スコアを連携。リスク上昇時にSecure Access側で通信遮断（BLOCK）や再認証を自動適用。
- **Security for AI（AI Access）**
  組織内のシャドーAI利用の発見・リスク評価から、機密データのプロンプト入力持ち出し遮断（DLP）、不審なAI通信防御まで包括的に保護。

© 2026 Cisco and/or its affiliates. All rights reserved.

Thank you

