SASE 最新アップデート

～導入事例に学ぶ成功ポイントと最新機能ご紹介～

シスコシステムズ合同会社
セキュリティ事業　サイバーセキュリティ製品担当　福留 康修

2025/5/21

アジェンダ

1. SASE の市場トレンドと期待
2. Cisco Secure Access 概要
3. 最新顧客事例と成功のポイント
4. 進化し続ける要件と SASE 最新機能

SASE の市場トレンドと期待

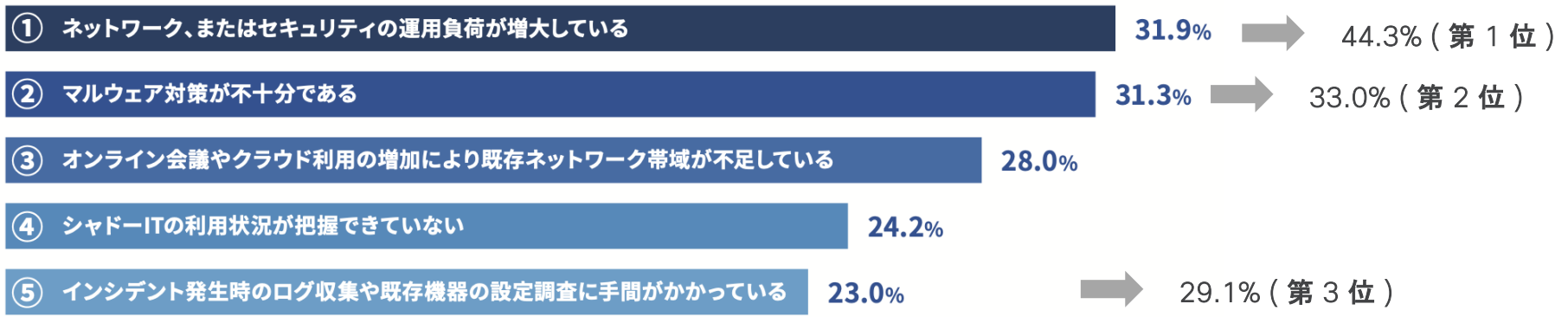
世界のネットワーク セキュリティ市場規模
212 億 4000 万米ドルと推定（2023 年）
729 億 6000 万米ドルに成長すると予測（2032 年まで）
14.6% の CAGR

ソース：ネットワークセキュリティ市場規模、シェアおよび業界分析、展開別、タイプ別、企業タイプ別、業界別、および地域別予測、2024 ～ 2032 年
Fortune Business Insights (2025.1)

ネットワーク セキュリティ市場の成長要因
ネットワーク ポイントでのサイバー脅威の増加により、ネットワーク セキュリティ ソリューションの需要が増加

サイバー攻撃はより高度かつ複雑になり、エンドポイント、ゲートウェイ、クラウド環境などのさまざまなネットワーク ポイントをターゲットにしています。高度な持続的脅威 (APT)、ランサムウェア、ゼロデイ エクスプロイトには高度な検出および防止メカニズムが必要であり、堅牢なネットワーク セキュリティ ソリューションの必要性が高まっています。デジタルトランスフォーメーション、IoT、クラウドコンピューティングによるデータ生成とネットワークトラフィックの急激な増加により、攻撃対象領域が拡大しました。転送中のデータが増えると傍受や悪用の可能性が高まるため、データの整合性と機密性を確保するための包括的なネットワーク セキュリティ対策が必要になります。

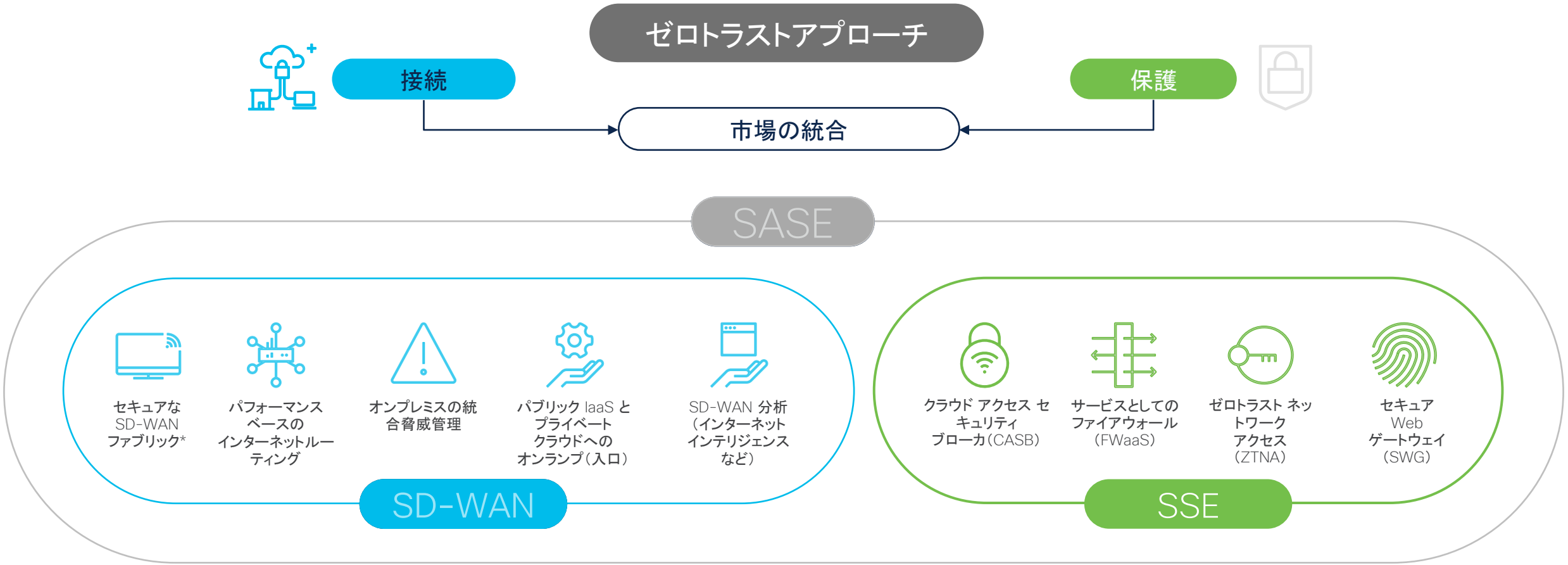
回答の多かった、ネットワークおよびセキュリティ課題のトップ 5（2023 年 → 2024 年）



ソース：国内企業における SASE 実態調査結果（2023/2024 年度版）-- SCSK 調査

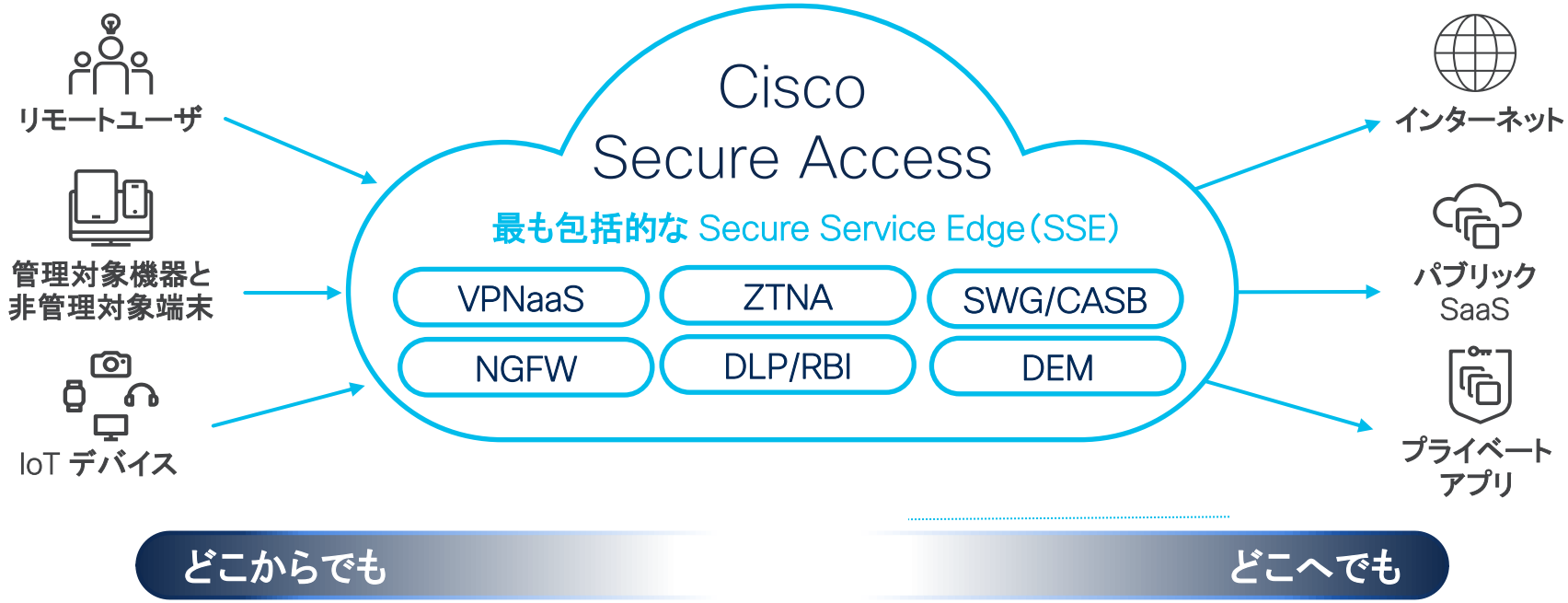
ゼロトラスト アプローチにおいて重要となる SASE

超分散型の世界におけるセキュリティ戦略の基盤



Cisco Secure Access 概要

ゼロトラストに基づく統合クラウドセキュリティで防御を近代化する最新型 SSE

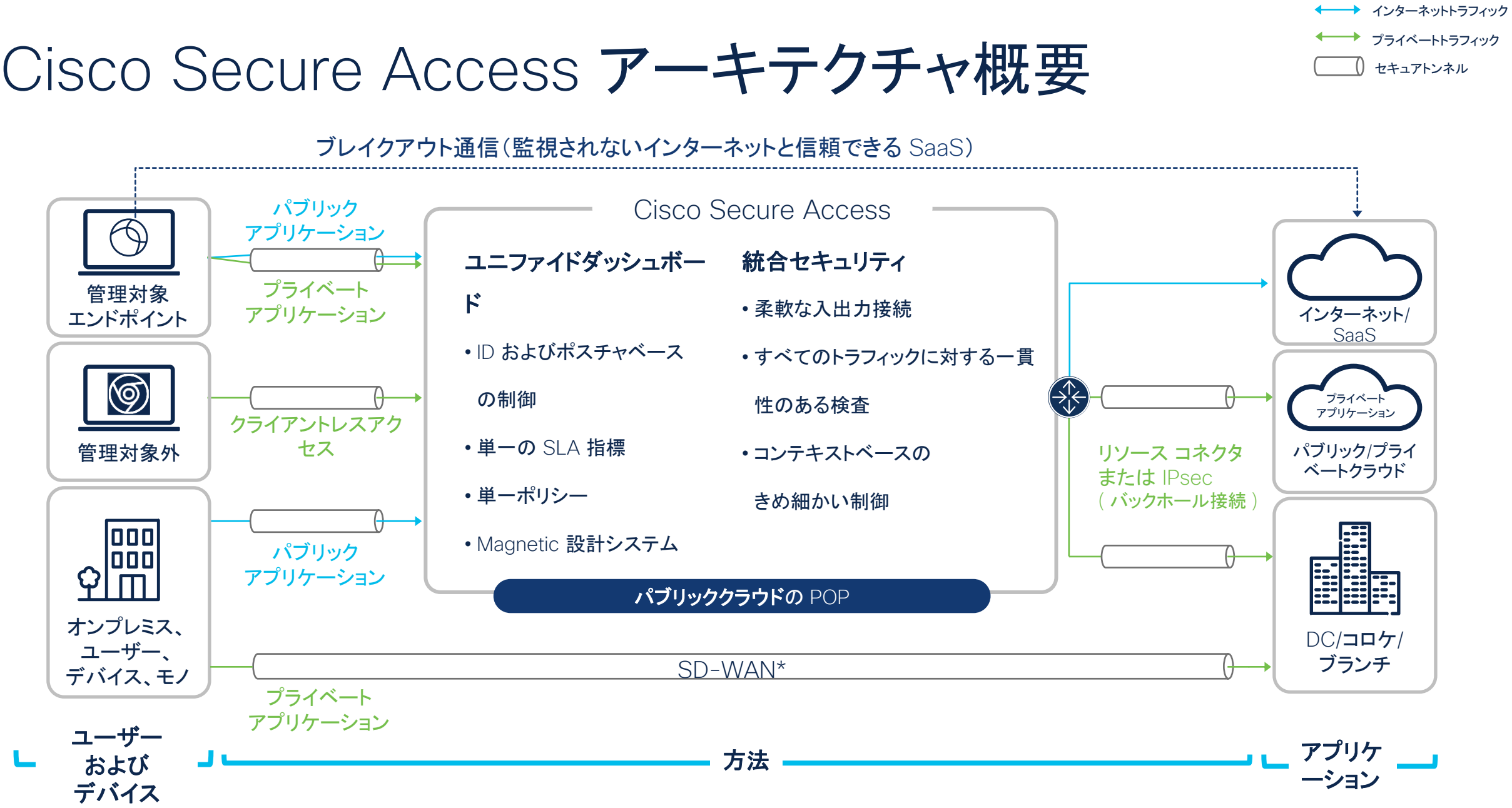


ユーザーにとってより快適に
スムーズなユーザー
エクスペリエンスで仕事を支援

IT をより使いやすく
コストを削減し効率を向上

すべての人にとってより安全に
リスクを緩和しビジネスのレジリエンスを強化

Cisco Secure Access アーキテクチャ概要



＊ 必須ではないが、ほとんどのユースケースで必要とされている

Cisco Secure Access
最新顧客事例

Cisco Secure Access 販売実績

（2023/10/27 サービス開始）

- 海外数百社
- 国内数十社
- 10 万ユーザ以上複数社（国内・海外）

ユーザ事例

海外製造業

サイバーセキュリティの強化とグローバル ワークフォースのパフォーマンス向上

工業用接着剤、シーラント、特殊化学品のグローバル リーダーであり、従業員数は 7,000 人を超え、140 か国以上で販売している H.B.Fuller は、リモートフレンドリーな職場として認められていますが、それには課題がないわけではありません。多くのグローバル企業と同様、この企業もコロナ禍、パンデミックの初期にテレワークへの移行を急ぎ、デジタル資産を保護しつつ、グローバル戦力にシームレスなアクセス確保するという課題に直面しました。

課題

- グローバルレベルのセキュリティのスケーリング：パンデミックによるテレワークの急増など VPN インフラストラクチャは限界
- 強固なサイバーセキュリティ管理：脅威に対する防御の強化と安全性の確保（最小権限のリソースアクセス）
- シームレスな統合：H.B.Fuller のセキュリティエコシステムへの新規買収の迅速な組み込み
- ユーザーエクスペリエンスの向上

ソリューション

- Security Service Edge(SSE) の採用でインターネットの使用とアプリケーションアクセス全体で、速度とパフォーマンスが大幅に向上
- 従来の VPN アクセスと比較して、ネットワーク全体またはセグメントへのきめ細かなアクセス制御を実現
- IT 管理が簡素化され、プラットフォームの管理が大幅に改善
- モバイルデバイス対応

結果

- 従業員からの好意的なフィードバック
- サードパーティのアカウントに対するきめ細かなアクセス制御を単一のシステムで提供
- 外出先で見積りでき生産性が向上。お客様満足度も向上。

業界:
工業用接着剤

場所:
ミネソタ州セントポール

組織:
7,000 人以上の従業員、
世界 120 拠点

ソリューション:
Cisco Secure Access

Why Cisco?

「これまでの道のりにより、運用アプローチが再構築され、セキュリティ態勢が強化されました。」
–H.B.Fuller グローバルバイスプレジデント兼最高情報責任者

ユーザ事例

海外製造業

Swire Coca-Cola 社がCisco Secure アクセスを使用して分散型従業員の保護を簡素化

Swire Coca-Cola は、56 のオフィスと複数のデータセンタに分散したワーカーを抱える大規模な組織で、ネットワーク管理と保護において重大な課題に直面していました。8,000 人の従業員を抱え、年間収益が 30 億ドルを超える同社は、リソースへのアクセスをシームレスに保護し、ユーザーがどこでも作業を行うために必要なツールを入手できるよう、堅牢、スケーラブルかつ使いやすいソリューションを必要としていました。

業界:
製造業

場所:
ユタ州ドレイパー

組織:
8,000 人の従業員、56 拠点

ソリューション:
Cisco Secure Access

課題

- 分散したワーカー: 多数のオフィスや複数のデータに分散しているワーカーとローミング ユーザーが世界中のさまざまな DC にあるデータへアクセスする必要性。
- 複雑なネットワーク管理: 複数のベンダー製品を含む既存のネットワークインフラ (RAVPN を含む) は管理が困難かつ分散されて展開され、持続不可能な状態。
- スキルセットの不一致: エンドユーザのリテラシーが既存のソリューションの複雑さにマッチしておらず、宛先に応じた VPN 利用の必要性およびセキュリティタスクの頻度についても不満。
- セキュリティ上の懸念: 海外出張の際に、データおよびユーザの脅威からの保護は重大な懸念事項。

ソリューション

- SSE により安全なアクセスを提供、データセキュリティを提供し、Meraki とシームレスに統合。
- ネットワーク全体を、ワイヤレス、からコアに至るまで Meraki スタックに統一し一貫性のある管理しやすいネットワーク環境を実現。
- ユーザーのエクスペリエンスをトラックおよび改善することで、ヘルプデスクへの問い合わせを減らし、問題をより迅速に解決。

結果

- 管理の簡素化: シンプルで管理しやすいネットワーク環境が提供され、複雑さやスキルの不一致の問題を軽減。
- ユーザーエクスペリエンス向上: VPN 等アクセス問題の障害対応について心配不要に。アプリケーションやリソースへのアクセスとしてバックグラウンドで実行される高度な保護機能を実現
- 自動化と標準化: 自動化を通じてソフトウェアインストールと設定を大幅に改善。生産性を大幅に向上。

Why Cisco?

「Cisco Secure Access への移行を決めた最大の理由は、エンドユーザのワーク フローを簡素化し、IT 部門にとってより簡単にソリューションを実現できるからです。」
–アレン・アンダーソン、IT インフラストラクチャー担当ディレクター

ユーザ事例

海外 IT・通信

シスコ IT による Cisco Secure Access の導入

すべての大企業と同じように、シスコ IT は、ワークフォースが広範囲に分散するという動向を受け入れ、そうした環境で積極的にセキュリティを確保する必要がありました。これが、セキュア アクセス サービスエッジ（SASE）への移行における重要な推進要因となりました。シスコ IT は長年にわたってこのような取り組みを進めてきましたが、その流れを加速させる必要がありました。シスコ IT は、セキュリティ戦略を強化して運用を合理化し、チームが働く場所に関係なくシームレスなユーザー体験を提供するために、シスコ独自の Secure Access の展開を開始しました。

課題

- 多様性に富んだ環境: 300 以上の大中小様々な拠点、2 万台以上のビデオデバイス、約 100 万の IP 接続されたモノ、6 万台以上のモバイルデバイス。
- 事業の成長に応じた企業買収と環境への統合: 2023 年だけでも新たに 9 社を買収してシスコの組織に統合。
- 自社開発した SASE における運用とリソースにおける負担: 自社開発システムにより、SASE の機能の大部分は正常に提供されたが、ソリューションの統合と運用に多大な時間とリソースを投入する必要性。

ソリューション

- 幅広い接続オプション、単一のエージェントによる接続と可視化、合理化されたユーザー体験を提供する Secure Access を採用
- 決定した要因
  - 優れたスムーズなユーザー体験
  - セキュリティ ポリシーの一貫性向上
  - IT リソースのより効果的な使用
  - 新しい機能やイノベーションの迅速な展開
  - ビジョンの完全性

得られた教訓

- 関係するチームを凌駕するエグゼクティブの確固たるコミットメントが必要
- IT、ネットワーキング、セキュリティ チームの根本的な変化： セキュリティと効率を実現するための共有
- 求めているすべての機能をすぐに利用できなかった複雑・多様な環境に対して新機能適用を迅速化
- トラブルシューティングの可視性
- 進捗状況とエンド ユーザによる選択制のバランスにより業務影響懸念を払拭

業界:
IT・通信業

場所:
カリフォルニア州サンホセ

組織:
86,000 の従業員、300 拠点

ソリューション:
Cisco Secure Access

Why Cisco?

「ビジネスを新しい地域に拡大したり、VPN、ブランチ、インターネットエッジのために別のコロケーション施設に移動したりすることの複雑さを想像してみてください。Cisco Secure Access は、クラウドエッジの拡張を大幅に簡素化し、セットアップに必要な時間を数ヵ月から数時間に短縮してくれます」
–ネットワーク設計・導入および運用担当責任者 Jon Woolwine

Secure Access お客様事例（国内）

Secure Private Access (SPA)

お客様プロフィール
- 情報・通信業
- 従業員 2,000名以上
- Umbrella のお客様

顧客ニーズ
- VPN のセキュリティ強化
- 既存環境への影響およびエンドユーザへの負担を最小限に（利便性の維持）
- 短期間での展開

シスコを選んだ理由
- Umbrella を通じたセキュリティ強化の実績
- 少ないエンドユーザへの負担
- 導入が容易
- ソリューションの将来性

Secure Internet Access (SIA)

お客様プロフィール
- 小売業
- 従業員 10,000名以上
- Secure Web Appliance (旧名 WSA) のお客様

顧客ニーズ
- 既存アプライアンスのサポート終了に伴う更新
- 移行に伴う業務影響の最小化
- インターネットアクセス高速化

シスコを選んだ理由
- 迅速なトライアル提供
- 既存コンテンツフィルタの活用
- 必要機能および展開実現性確認時におけるサポート体制

Secure Private Access (SPA)

お客様プロフィール
- サービス業
- 従業員 60,000名以上
- 他社 VPN ソリューションのお客様

顧客ニーズ
- アプライアンスのサポート終了に伴う更新
- 運用工数削減
- ZTNA へのシームレスな移行

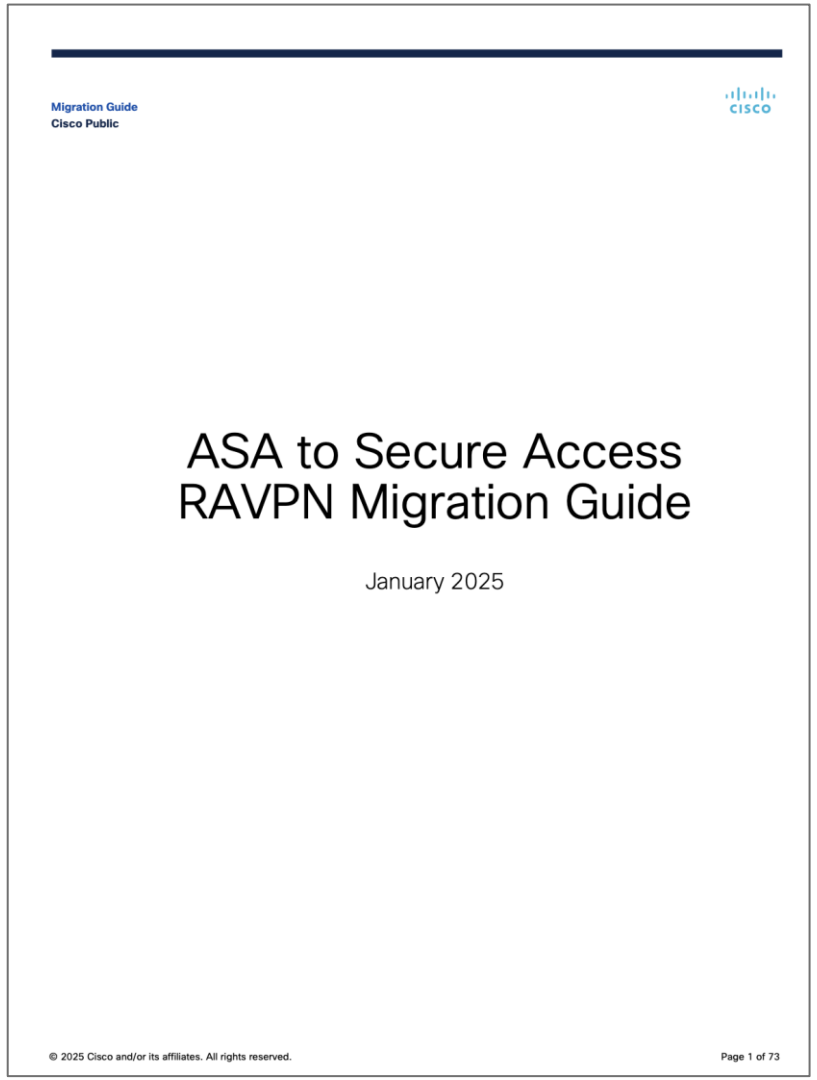
シスコを選んだ理由
- 5 社机上検討比較の結果
- レガシー VPN 同等機能を実証
- 価格妥当性
- 既存環境適合性検証におけるサポート体制

事例に見る成功のポイント

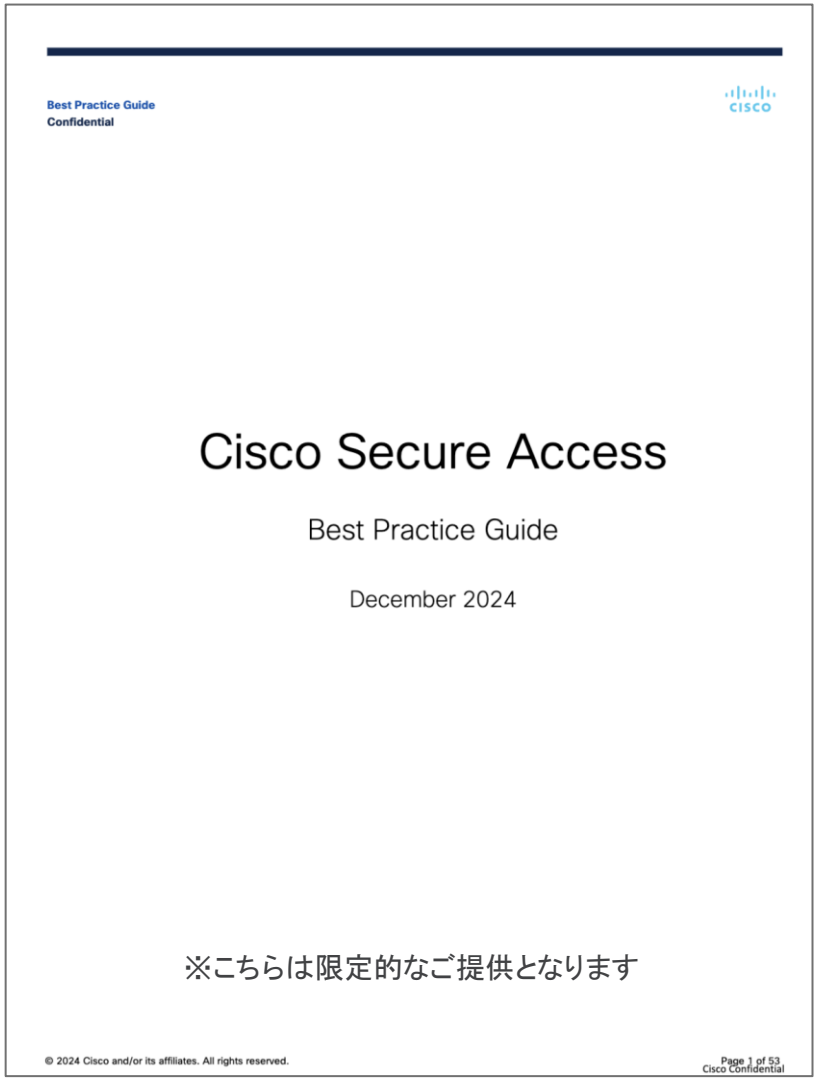
1. 事前評価
   ① 環境構築段階におけるベンダーサポート
   ② 必要機能（ユースケース）および移行に関する検証の実施
   ③ 製品ロードマップの確認および（適宜）展開計画への反映
2. 本番環境
   ① 評価環境を本番環境へ移行
   ② パイロットユーザを通じ、追加で必要な設定等の対応
   ③ エンド ユーザ理解の醸成
   - 展開（移行）時期や切り戻しに関する選択肢の提供、SASE/SSE 化にともなうメリットの提示など
   ④ ベンダーの有償支援を活用した本番設計
   ⑤ アフターサポート体制および問い合わせフローの明文化

（ご参考）各種ガイド

- ASA to Secure Access RAVPN 移行ガイド

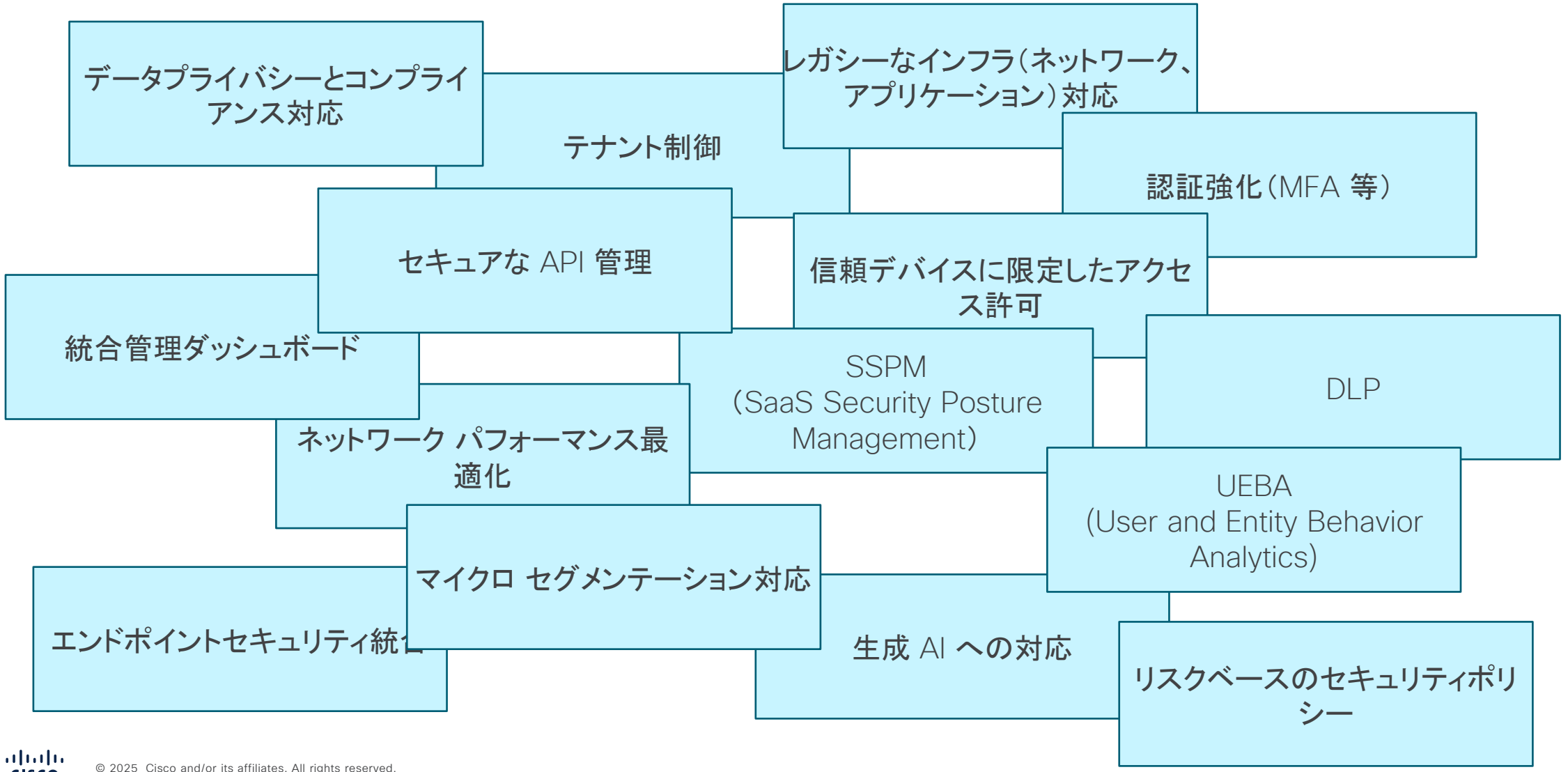


- Cisco Secure Access Best Practice Guide



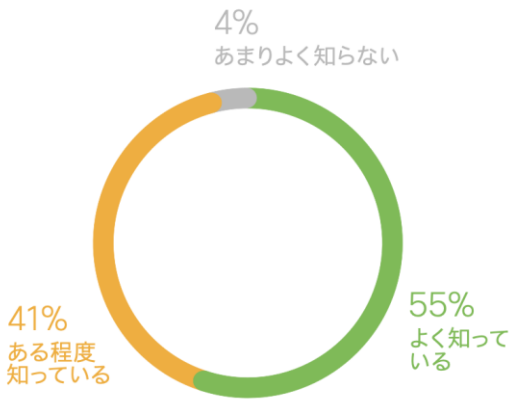
進化し続ける要件と SASE 最新機能

進化しつつある SASE への期待

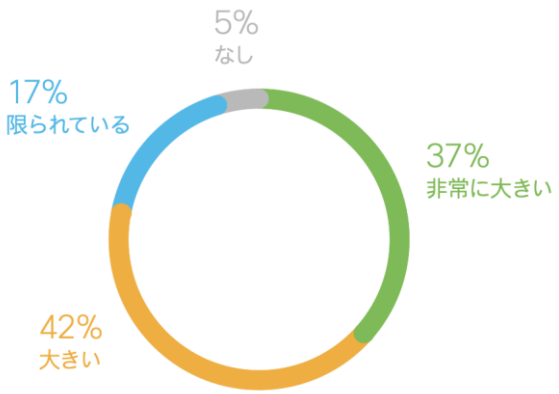


生成系 AI 関連のデータへの懸念

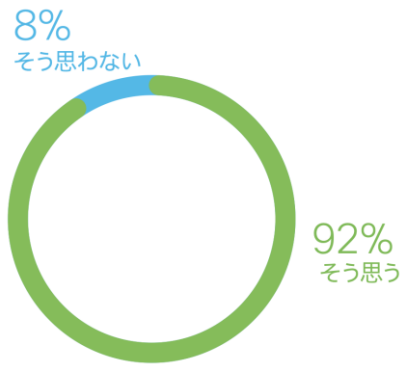
① 生成系 AI (GenAI) についての知識



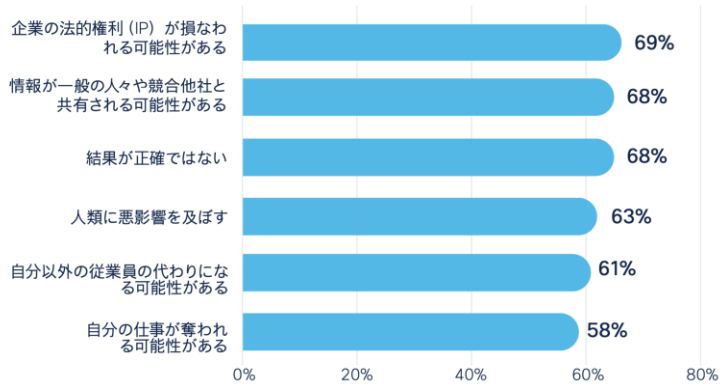
② AI の使用に関して組織が取ることのできる対策



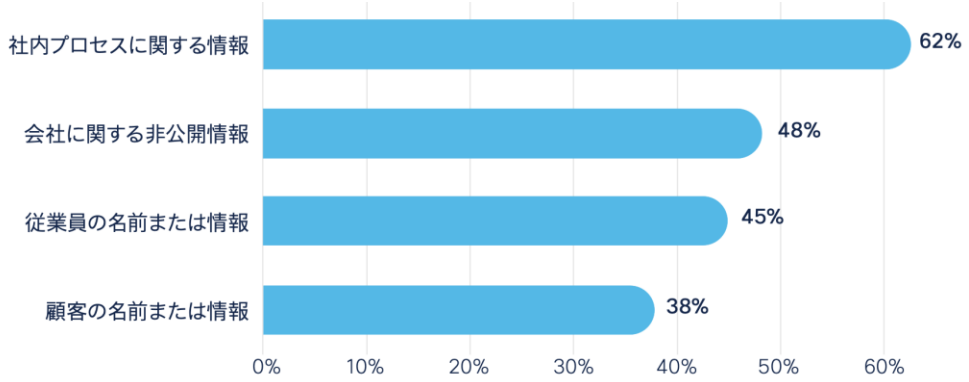
③ 生成系 AI は根本的に異なるものであり、データとリスクを管理するための新しい手法が必要



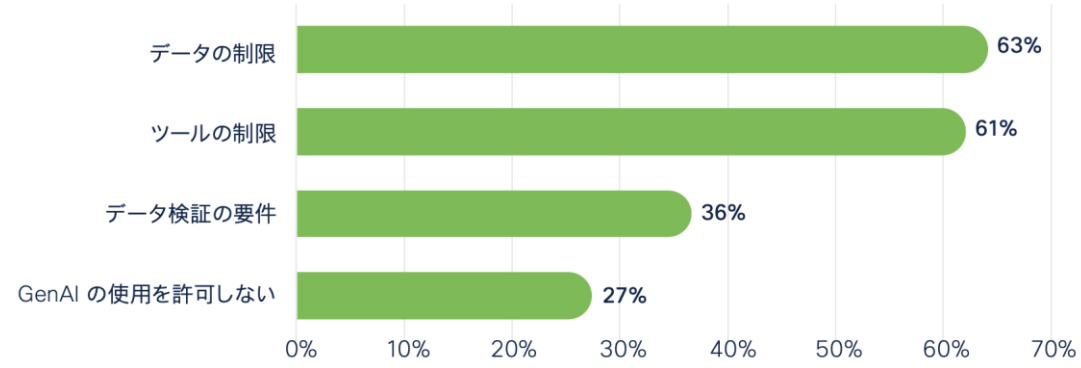
④ 生成系 AI に関するユーザーの懸念



⑤ 生成系 AI アプリケーションに入力された情報の種類



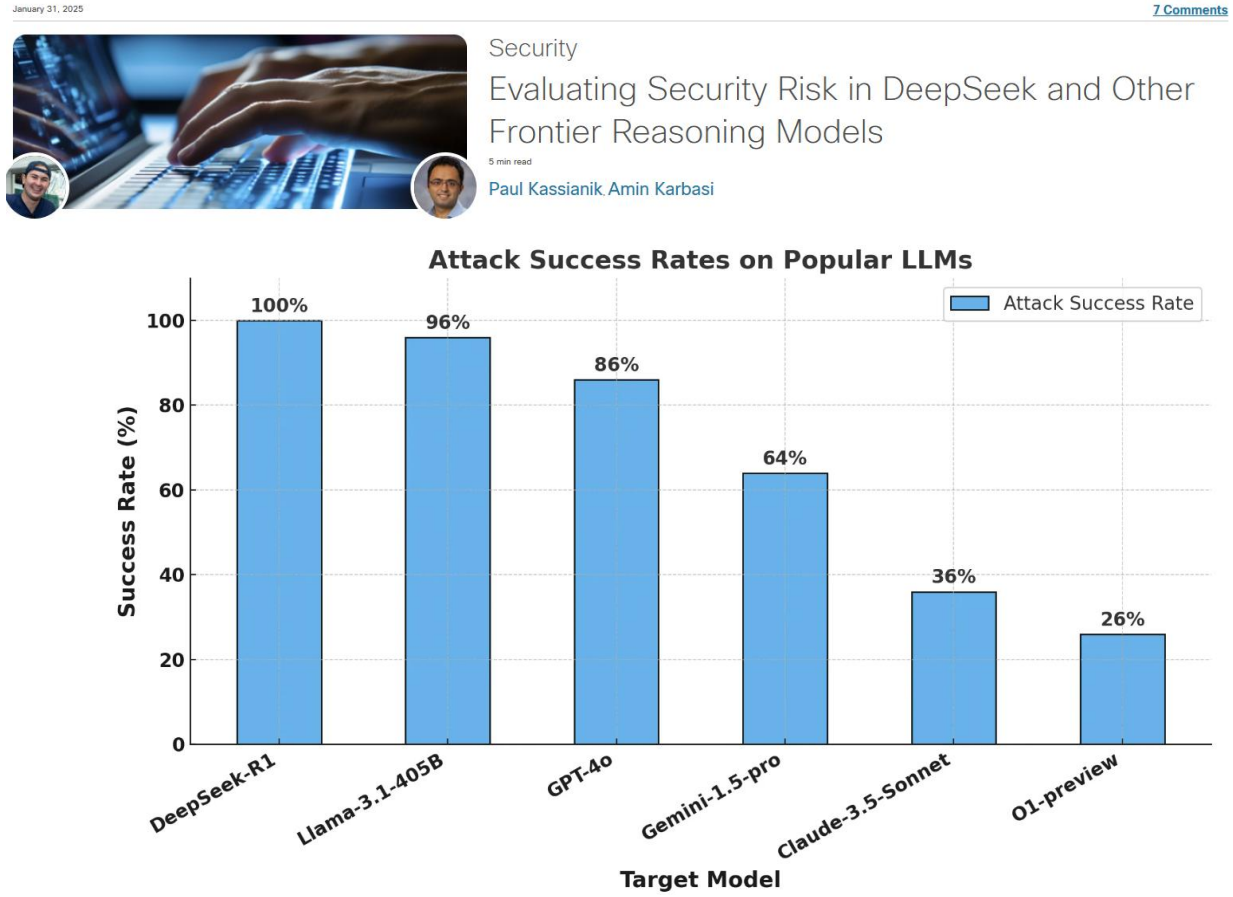
⑥ 生成系 AI の管理



ソース: シスコ 2024 データ プライバシー ベンチマーク調査

（ご参考）シスコが Deep Seek R1の脆弱性を評価

- 中国の AI 企業である DeepSeek がリリースした生成 AI サービス R1 が Apple 全米ダウンロードトップになり NVIDIA 株が急落し話題に
- Cisco の研究チームは、100% の攻撃成功率で DeepSeek R1 をジェイルブレイクすることに成功
- 均一にサンプリングされた 50 個のプロンプトに対して自動ジェイルブレイク アルゴリズムを実行
- モデル ガードレールで敵対的攻撃の大部分をブロックする o1 などの他の最先端モデルとは対照的な結果に
- パフォーマンスだけに焦点を当てるのではなく、安全性とセキュリティに関する重大なトレードオフを理解する必要がある



DeepSeek、素直すぎて研究機関による安全テストに全部不合格
https://www.gizmodo.jp/2025/02/deepseek-gets-an-f-in-safety-from-researchers.html

https://blogs.cisco.com/security/evaluating-security-risk-in-deepseek-and-other-frontier-reasoning-models

（ご参考）
DeepSeek に関する情報提供

生成AIサービスについては、その利用が世界的に普及している中、新たにDeepSeek社[注1]による生成AIサービスが開発され、サービス提供が開始されています。同社の生成AIサービスについては、日本国内でサービス提供体制が構築されている他のサービスとは異なり、留意すべき点がありますが、同社が公表するプライバシーポリシーは中国語と英語表記のもののみとなっています。このため、同社が公表するプライバシーポリシーの記載内容に関して、以下のとおり、情報提供を行います。

①当該サービスの利用に伴いDeepSeek社が取得した個人情報を含むデータは、中華人民共和国に所在するサーバに保存されること
②当該データについては、中華人民共和国の法令が適用されること

（参考）
上記②に関して、当該データに対しては、例えば以下のような法令が適用されることとなります。

- 中華人民共和国個人情報保護法
- サイバーセキュリティ法
- データセキュリティ法
- 中華人民共和国国家情報法　　等

ソース：令和7年2月3日　個人情報保護委員会事務局
https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/

AI Access: サードパーティ生成 AI むけアプリケーション セキュリティ

発見

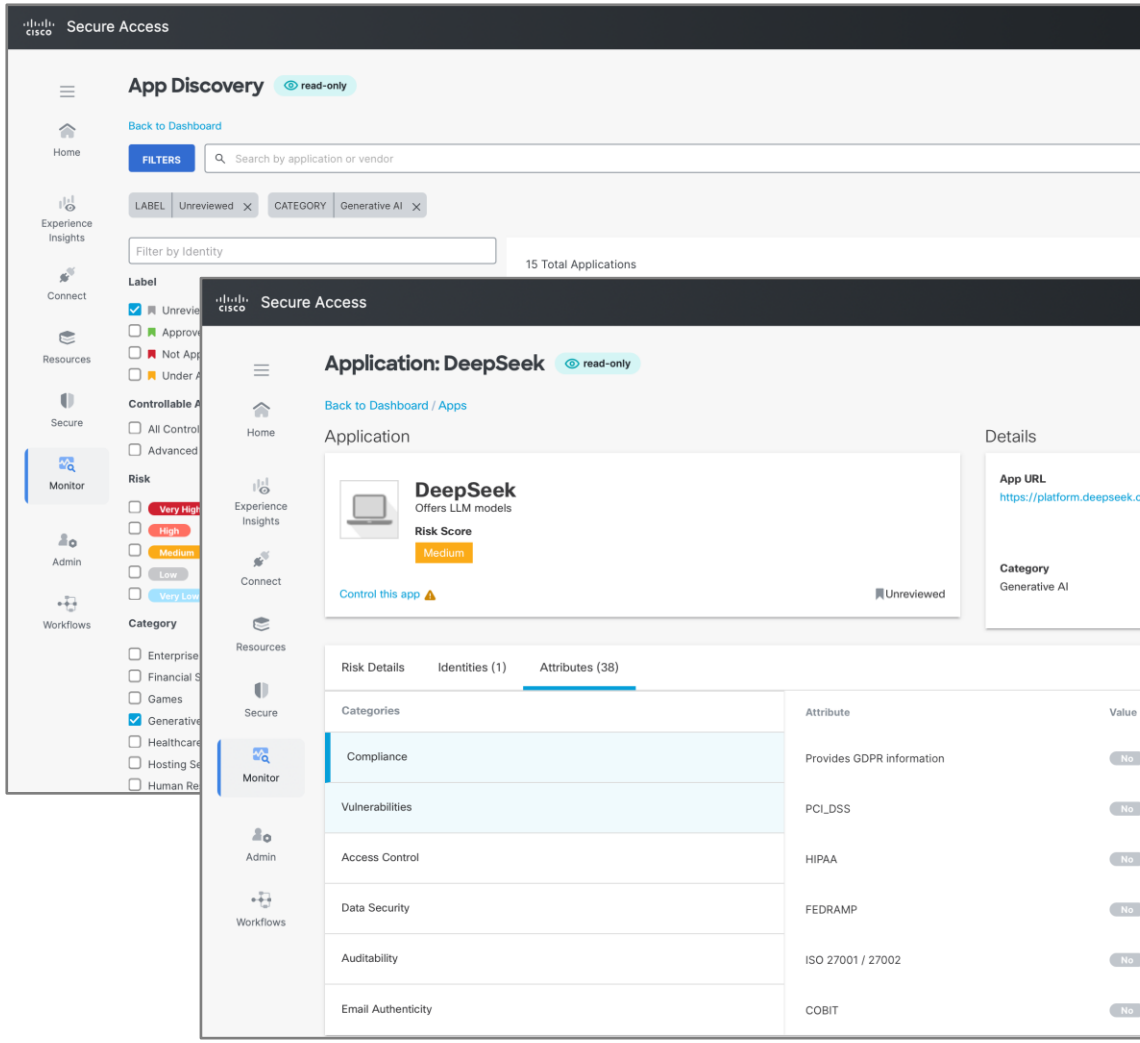
組織全体でシャドー AI アプリの利用を発見

検出

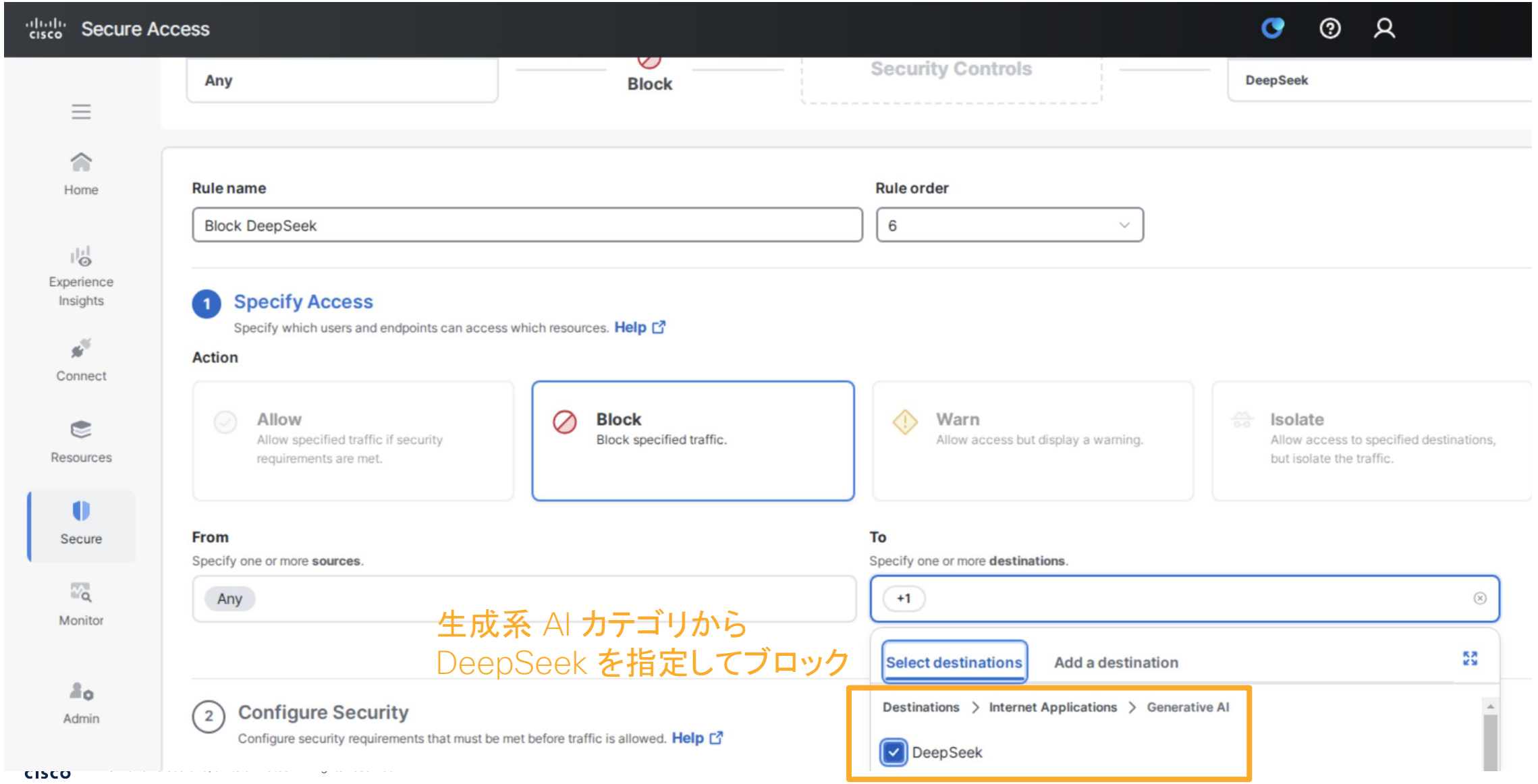
サードパーティ製アプリのリスクを評価し、デバイス、場所、ネットワークなどのコンテキストを取得

保護

クラス最高の ML モデルを使用したアクセス制御により、機密データの漏洩や脅威の伝播からプロンプトと回答を保護

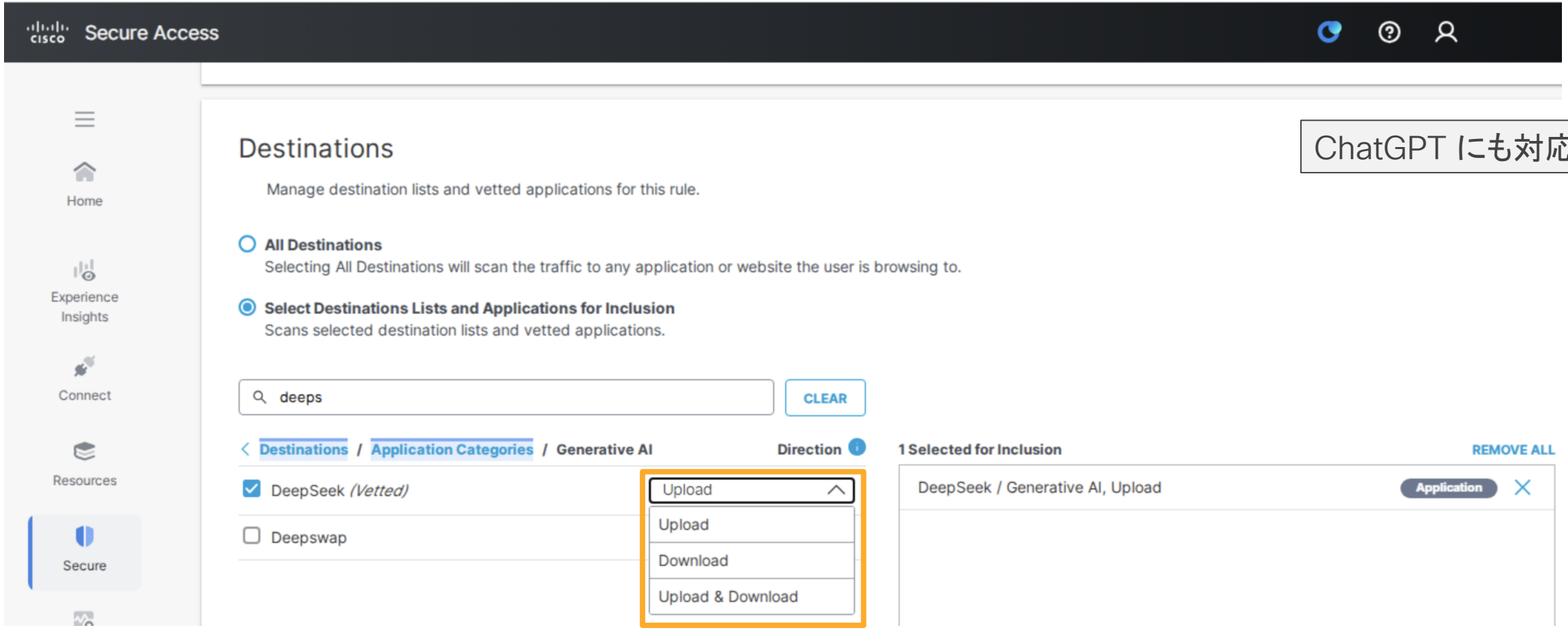


AI Access による DeepSeek 利用制御



生成系 AI カテゴリから
DeepSeek を指定してブロック

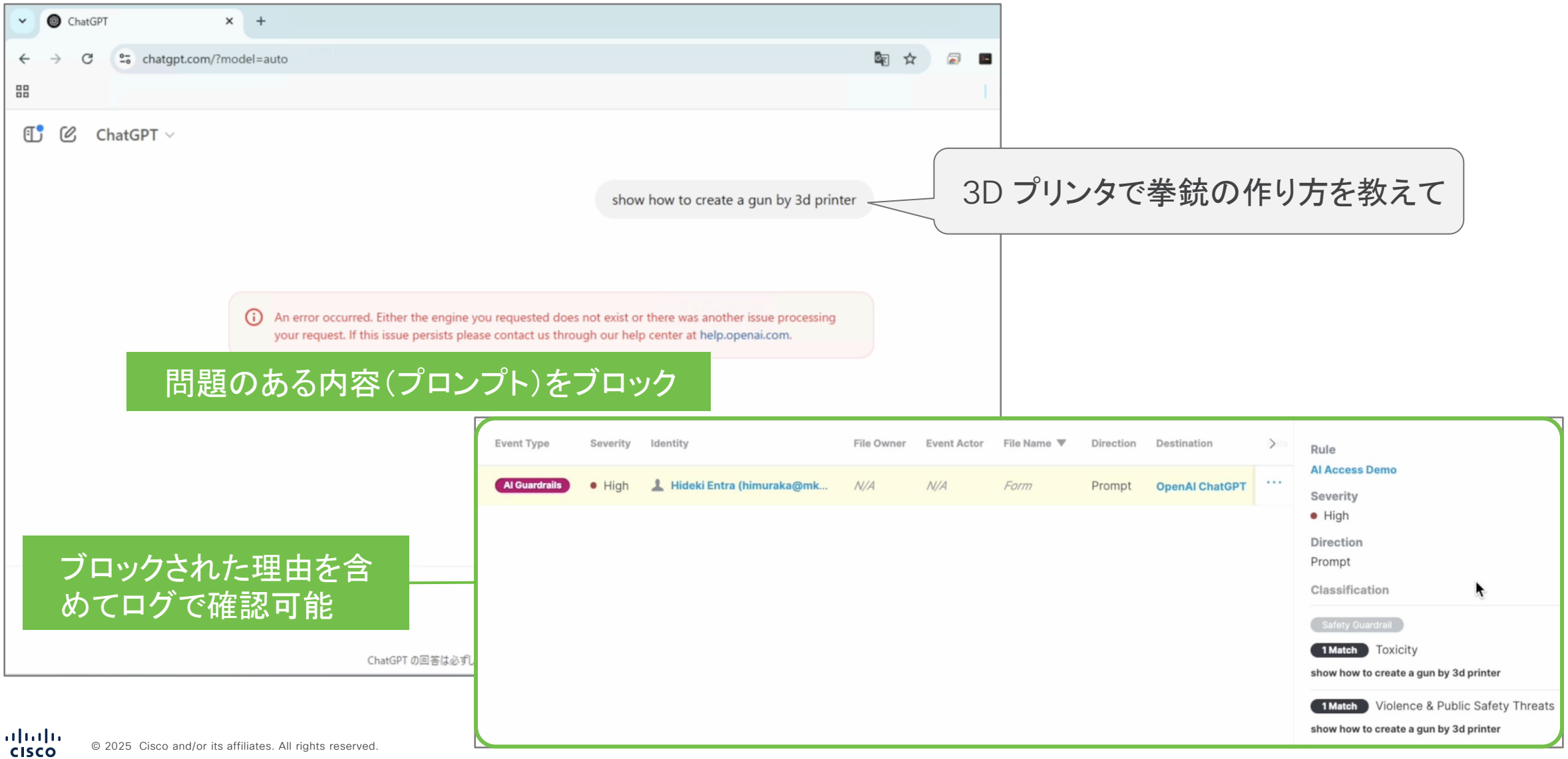
AI Access による DeepSeek の詳細な制御



ChatGPT にも対応

AI プロンプト、応答、または双方向の監視や制御に対応

AI Access による許可された AI の安全な利用



AI Access の差別化要素

- **インテリジェンスにもとづく保護**
- コンテキストを考慮した検出
  - 非構造化テキスト内のパターンレス PII/PHI/PCI 識別
  - 高度なデータ保護のための意図分析
  - 誤検知の低減

- **セキュリティ ガードレール**
- **脅威の防止**
  - プロンプトインジェクション、データポイズニング、独自の AI モデルを使用した OWASP/MITRE Atlas スタイルの AI 攻撃などの高度な攻撃の防止
  - 悪意のあるコードの検出

- **アドバンスド セキュリティ ガードレール**
- **コンテンツの安全性**
  - 意図に基づく毒性検出
  - 文脈に基づく安全性分析
  - 高度な有害コンテンツ防止

- **単一のユニファイド・ポリシー・フレームワーク**
  - インラインとアウトオブバンドのすべてのセキュリティポリシーに対応する単一のコントロールプレーン

- **真のゼロ・フリクション・プロテクション**
  - Secure Access にネイティブに組み込まれており、追加のインフラは不要

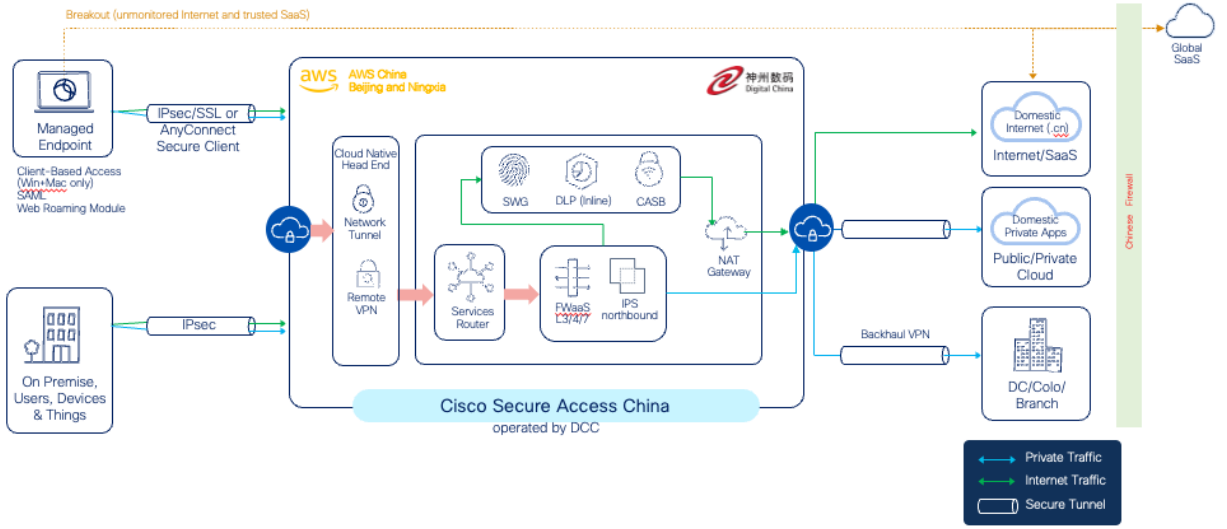
1500以上の AI アプリをカバー

トップ 15 の AI アプリ保護

高度なコンプライアンスと利用状況レポート

中国 DC

- シスコのアプローチは「コンプライアンスファースト」
- 2025 年 5 月からご利用可能
- AWS 中国でホストされているインスタンス
  - リージョン – 北京
  - マルチテナントとエラスティック パフォーマンス
  - 高可用性とクラウドのレジリエンシ
- 使いなれた Secure Client（エージェント）
- ブランチ接続用の標準 IPsec（中国国内）
- 中国国内で提供される管理者ダッシュボード
  - デプロイメント時のセキュリティと遵守リスクを軽減
  - グローバルの Secure Access と同様のダッシュボードと同様見た目
  - 英語 – 中国語に対応したブロックページ
- 中国における複合 TAC サポート
  - DCC ー ティア 1 サポート
  - シスコ ー ティア 2 およびティア 3
  - 現地ビジネスアワーにおける現地語サポート



サポートされるユースケース

- Branch to Internet
- Branch to Branch (In-Country)
- RAVPN User to Internet
- RAVPN User to Branch/Private App
- RAVPN User to RAVPN User
- SWG Roaming User to Internet

まとめ

1. ハイブリッド検討の重要性
2. 目指すべき成功、および成功にむけた SASE 導入・検討のポイント
3. 大手企業の様々な要望に応えられる SASE は、Catalyst SD-WAN + Secure Access
4. Secure Access は大規模実績が増えつつあり、公開事例も今後増えるみこみ
5. SASE/SSE は成功するための取り組み・枠組みが重要
6. Secure Access は多くのお客様が抱えるビジネス課題を解決しながら幅広い環境に適合できる包括型 SSE として、今後更なる機能拡充を予定


CISCO