Cisco Secure Access

クラウドベースのアジャイルなセキュリティでハイブリッドワーク環境を保護

2024 年 12 月

目次

ハイブリッドワークとセキュリティサービスエッジ

現在のハイブリッドワーク環境に伴ってセキュリティへのアプローチの見直しが求められる中、あらゆる組織のハイブリッドワーク戦略において成功の鍵を握っているのが SSE（セキュリティサービスエッジ）です。SSE はクラウド内の複数のセキュリティ機能を組み合わせ、パブリック SaaS アプリケーション（アプリケーション）、データセンターやプライベートクラウドのプライベートアプリケーション、インターネット全体などのさまざまなリソースに場所を問わずにアクセスして作業するユーザーを保護します。エンドユーザーは、オフィス、自宅、外出先など、どこで仕事をしても、安全で透過的なユーザー体験が確保されます。最大限の効果を引き出すため、SSE ソリューションは優れたユーザー体験を提供し、IT の複雑さを軽減し、セキュリティの有効性を高める必要があります。

Cisco Secure Access 製品の概要

Cisco Secure Access はゼロトラストに基づくクラウドベースのセキュリティ SSE ソリューションであり、デバイスや接続先を問わずシームレスで透過的かつ安全なアクセスを提供します。すべてのコア SSE コンポーネント（ZTNA、セキュア Web ゲートウェイ（SWG）、クラウド アクセス セキュリティ ブローカ（CASB）、FWaaS）に加えて、VPN-as-a-Service（VPNaaS）、マルチモード DLP、AI Assistant、AI 使用時の保護、DEM インサイト、予約済み IP、 RBI、DNS Security などの拡張機能を 1 つのライセンスと管理プラットフォームで利用できます。組織は、プロトコルやポート、カスタマイズのレベルに関係なく、必要なすべてのリソースとアプリケーションにシームレスにアクセスできるようにユーザーを保護することが可能になります。図 1 を参照してください。

Cisco Secure Access は、他のシスコやサードパーティベンダーの製品との相互運用を容易にする共通の管理制御、データ構造、およびポリシー管理の機能を備えています。たとえば Secure Access には、AD、Azure AD、Okta、Ping などのさまざまな SAML ID プロバイダー（IDP）が統合されています。また、SD-WAN、XDR、ThousandEyes（ThousandEyes に基づく Experience Insights は Secure Access に含まれています）に加え、Menlo Remote Browser Isolation、Google Chrome Enterprise Browser、AppOmni for SSPM などのサードパーティテクノロジーも統合されています。

Secure Access は、セキュリティを強化してリスクを減らし、IT 運用を簡素化して複雑さを軽減し、ユーザーにスムーズなアクセスを提供して生産性を高めます。

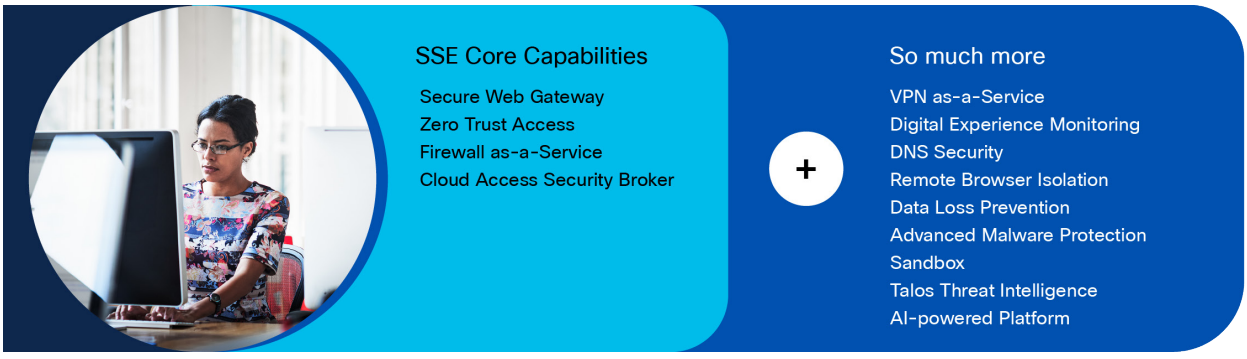

図 1.
Cisco Secure Access の機能

ユーザーにとっての改良点

Secure Access は、ユーザー体験を大幅に向上させることで、ユーザーの生産性を高めるだけでなく、ユーザーが故意にセキュリティの手順を怠ってリスクを高めてしまう状況を減らします。単一の統合クライアントによってユーザーの接続方法が簡素化されるため、ユーザーが認証を行い、目的のアプリケーションに直接接続できるようになります。

プライベート アプリケーションにアクセスする場合、ユーザーは ZTNA または VPNaaS を介して自動的かつ透過的に接続でき、追加の手順や面倒な検証タスクの繰り返しは必要ありません。さまざまなサインオンプロセスで複数のクライアントを起動する必要がないため、ユーザーの手間が最小限に抑えられます。すべてのアプリケーションに一元的にアクセスできることで、ユーザーの接続が大幅に簡素化され、ユーザーやデバイスのポスチャ検証などのセキュリティが確保され、生産性が向上します。

IT をより簡単に

現在の IT チームは、大量のセキュリティツール、複数の管理コンソールとポリシーエンジン、そして多様なユーザーやデバイスタイプに向けたさまざまなソフトウェアエージェントに手を焼いています。こうした課題は、各セキュリティポイントの製品から発生する個別のレポート、アラート、およびインシデントによってさらに増大していきます。

Cisco Secure Access は、単一のクラウド管理コンソール、統合クライアント、一元化されたポリシー作成プロセス、および集約されたレポート作成機能によって、運用を簡素化および自動化します。ユーザーはデバイスが管理対象であるかどうかに関係なくどこからでもアプリケーションにアクセスできるため、IT チームは異なる複数の製品ではなく 1 つのツールを管理するだけで場所を問わずユーザーをきめ細かく制御できます。IT チームは脅威を迅速に検出してブロックし、調査を効率よく実施して、修復タスクを最小限に抑えることで手動の集約作業を減らしながら、エンドユーザー アクティビティの可視性を高めることができます。

すべてのユーザーにより安全な環境を

Cisco Secure Access の多層防御アーキテクチャアプローチは、高度なサイバー脅威を防ぐため、その業界をリードするセキュリティの有効性が高い評価を得ています。エンドユーザーは、感染したファイル、悪質な Web サイト、フィッシングやランサムウェアといったスキームから保護されます。IT チームやセキュリティチームは、攻撃対象領域を減らし、最小権限の制御を実施できるほか、ポスチャ検証を有効にして、分散環境でのセキュリティギャップをなくすことができます。許可されていないアプリケーションの使用を可視化し、ブロックします。内部リソースをクローキングしてハッカーから隠すことで、セキュリティを一層強化します。

Cisco Talos の脅威インテリジェンスはその比類のないテレメトリ、広範なリサーチ、高度な AI によってこの機能を支え、脅威を特定して阻止し、修復を迅速化しています。リスクを軽減することで、組織は事業継続性を維持し、侵害によるレピュテーションや財務への影響を回避します。

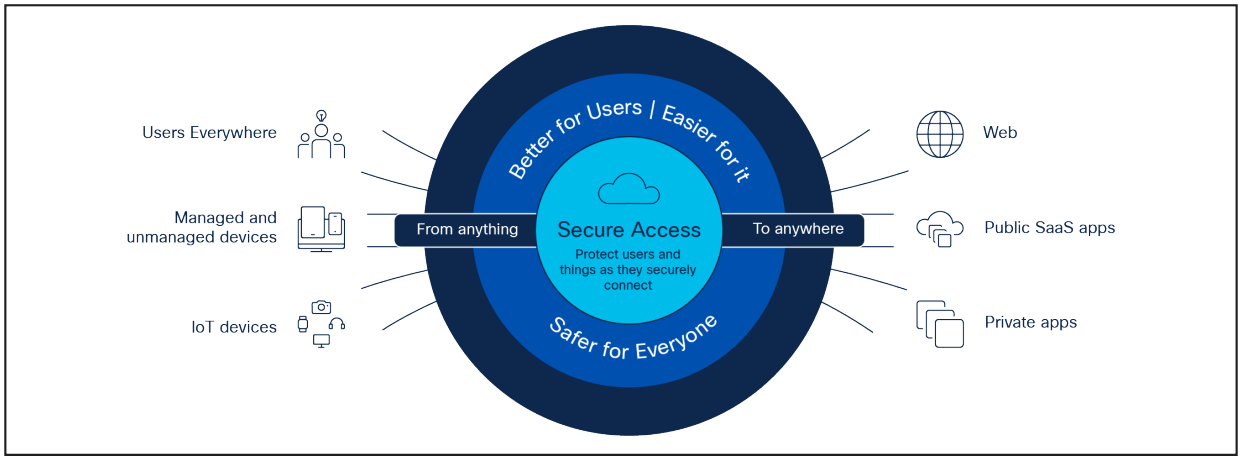

図 2.
デバイスや接続先を問わないセキュアな接続

機能とメリット

機能	利点
ゼロトラスト ネットワーク アクセス（ZTNA）	オンプレミスのデータセンターまたはクラウド/IaaS 環境にあるプライベート アプリケーションに対して、アプリケーション固有のきめ細かくセキュアなアクセスを提供します。 そのアイデンティティ認識型プロキシ設計では、最小権限の原則とコンテキストに基づくインサイトを活用してデフォルトでアクセスをきめ細かなレベルで拒否し、ポリシーによって明示的に許可されている場合はアプリケーションへのアクセスを許可します。 • Cisco Secure Client（Cisco Secure Access 用の単一の統合クライアント）を介したクライアントベースのアクセス。 • クライアントレスアクセス（ブラウザ経由）は、ブラウザベースの SSH および RDP プロトコルのサポートにより、Web アプリケーション（http/https）およびプライベート アプリケーションへのトラフィックを保護します。これにより、クライアントレス ZTNA を介して保護できるアプリケーションが大幅に増えます。 • デバイスポスチャのチェック後、セッションごとにセキュアなアクセスが確立されます。 • セキュアな暗号化トンネルによってユーザーを認証するため、ユーザーはアクセス権限を持つアプリケーションのみを表示できます（攻撃者のラテラルムーブメントを防ぎます）。 • アプリケーションプロキシは、アプリケーションをインターネットに公開することなく透過的でセキュアなリモートアクセスを提供し、アプリケーションを使用するクライアントからネットワークの詳細を隠します。デバイスが侵害された場合でも、悪意のある IP 偵察を阻止します。 • デバイス固有のアクセス コントロール ポリシーを実装し、侵害されている可能性のあるデバイスはそのサービスに接続できないようにします。 • 管理者には、適切なユーザーに適切なアクセス権を厳密に割り当てるための広範なポリシー「レバー」があります。例としては、請負業者と従業員に異なる権限を割り当てる、さまざまなエンドポイントとブラウザを評価するポスチャプロファイルを作成する、特定のアプリケーションに追加のユーザー認証を適用する、などがあります。

機能	利点
VPN-as-a-Service（VPNaaS）	ZTNA によってすべてのプライベート アプリケーションの安全が確保されるわけではありません。VPNaaS オプションを使用すると、Secure Access は ZTNA でサポートされていないアプリケーションを含む（一部だけではない）すべてのプライベート アプリケーションに対して、クラウドベースのセキュアなアクセスを提供します。VPNaaS はさらに、Web 以外のインターネットトラフィックのアクセスも保護できます。 • ユーザーの使いやすさ（常に VPN 接続、ログオン前に開始）。 • IT の簡素化（ローカル IP プール、複数の VPN プロファイル）。 • SAML、RADIUS、証明書などの複数の認証方式を使用したアイデンティティベースのアクセス制御。 • エンドポイントポスチャ評価により、アクセス制御のきめ細かさが向上します。 • ヘッドエンドまたはトンネルタイプを選択する必要がなく、接続が簡素化されます。 • Identity Services Engine（ISE）との統合により、SGT および RADIUS の認可変更（COA）を活用します。 • 機能の例：スプリットトンネリングとトンネルのすべてのサポート、ピアツーピア通信、信頼ネットワーク検出、BYO 証明書、スプリット DNS、ダイナミックスプリット DNS。
セキュアウェブゲートウェイ（フルプロキシ）	すべての Web トラフィック（http/https）をログに記録して検査し、透過性、制御、および保護を強化します。IPsec トンネル、PAC ファイル、プロキシチェーンを使用してトラフィックを転送し、完全な可視性、URL およびアプリケーションレベルの制御、高度な脅威からの保護を実現します。 • ポリシーやコンプライアンス規制に違反する接続先をブロックするための、カテゴリまたは特定の URL によるコンテンツフィルタリング。 • ダウンロードしたファイルをスキャンして、マルウェアやその他の脅威を検出します。 • 不明なファイルのサンドボックス分析を行います（Cisco Secure Malware Analytics の専用セクションを参照）。 • ファイルタイプごとのブロッキング（例：.exe ファイルのダウンロードのブロック）。 • TLS の全体または一部を復号することで、隠蔽された攻撃や感染から保護します。 • 一部のアプリで特定のユーザーアクティビティをブロックするためのきめ細かなアプリ制御（例：Dropbox へのファイルアップロード、Gmail へのファイル添付、Facebook での投稿/共有）。 • 完全な URL アドレス、ネットワーク アイデンティティ、許可またはブロックされたアクション、外部 IP アドレスが含まれた詳細なレポート。 • カスタマイズ可能な制御とトラフィックパスオプションを備えたインターネットベースの SaaS アプリのマルチモード保護。
クラウド アクセス セキュリティ ブローカ（CASB）	• 生成 AI を含む、使用中の選択したクラウドアプリケーションを検出、レポート、ブロックします。クラウドの利用を管理し、攻撃的、非生産的、高リスク、または不適切なクラウドアプリケーションの使用をブロックしてリスクを軽減します。ユーザーまたはグループのアクティビティを検出、記録、および制御するマルチモード機能を備えています。 • OAuth ベースの承認から Microsoft 365 や Google のテナントまで、リスクの高いプラグインや拡張機能の承認の検出、ブロック、および取り消しを行います。 • ベンダーカテゴリ、アプリケーション名、検出された各アプリケーションのアクティビティ量に関するレポート。 • Web レピュテーションスコア、財務状態、関連するコンプライアンス認定といったアプリの詳細やリスク情報。 • グループ/個人がアクセスできる SaaS アプリケーションのインスタンスを制御するためのテナント制限。 • 720 以上の生成 AI アプリケーションの使用状況または使用試行を検出して制御します。使用をブロックするか、これらのアプリケーションの使用方法を制御するポリシーを作成して適用します。

機能	利点
データ漏洩防止（DLP）	マルチモードのデータ損失防止（DLP）。データをインラインで分析し、組織外部へ流出する機密データを可視化および制御します。クラウドに保存されているデータのアウトオブバンド分析を行うための API ベースの機能。より効率的な管理と規制順守のための統合されたポリシーとレポート機能。 • 77 ヵ国にわたる 1,200 以上の組み込みグローバル識別子：個人識別情報（PII）、個人医療情報（PHI）、コンプライアンス（GDPR、HIPAA、PCI）、クラウド サービス プロバイダーのセッション トークン（AWS、GCP、Azure）、API トークン、キー、およびシークレット。 • 12 の LLM を活用する人工知能と機械学習は、特許申請、機密保持契約、パートナーシップおよびコンサルティング契約などの文書、および IRS フォームやストックドキュメントなどの財務記録を保護するのに役立ちます。このタイプの文書の分類では、複雑なデータ分類をゼロから作成するのではなく、事前に定義された事前トレーニング済みの文書タイプから選択できるため、データ損失防止ポリシーの管理が容易になります。 • オンプレミスの DLP ソリューションとの統合により、イベント管理と修復ワークフローを一元化します。 • 危険なコンテンツを検出してブロックすることで、IP の損失や汚染を防ぎ、AI サービスをより安全に使用できるようにします。ChatGPT の応答をスキャンして、法廷で使用する法的文書など、生成されたコンテンツの管理をサポートします。 • ChatGPT については、不当な漏洩を防ぐためにソースコードのアップロードをブロックします。ダウンロードをブロックすることで、ユーザーが ChatGPT でソースコードを生成し、ダウンロードしてコードリポジトリにコミットするのを防ぎます。 • しきい値と近接性を備えたカスタマイズ可能な組み込みのコンテンツ分類機能により、誤検出を調整および低減。 • カスタムフレーズ（プロジェクト名など）を追加できるユーザー定義のディクショナリ。 • 機密データの使用状況の検出と報告、および不正使用の特定に役立つドリルダウンレポート。 • API 機能は、Microsoft 365（SharePoint および OneDrive）、Google Drive、Webex、Box、Dropbox、Slack、および ServiceNow をサポートします。
クラウドマルウェアの検出	クラウドベースのファイル ストレージ アプリケーションからマルウェアを検出して削除します。悪意のあるファイルをエンドポイントに到達する前に検出して修復することにより、セキュリティ保護を強化します。 • セキュリティ管理者の有効性と効率を高めます。 • アクティブ化すると、クラウドベースのサービス内にあるすべてのファイルがハッシュ化され、マルウェアのスキャンを行うために自動的に送信されます。マルウェアを含むファイルにはフラグが付けられるため、セキュリティ管理者は検疫や削除などの修復処理を実行できます。 • Box、Dropbox、Webex、Microsoft 365、および Google Drive、AWS S3、Azure をサポートします。
人工知能アシスタント	生成 AI 機能は、セキュリティ管理者が時間を節約し、業務効率を向上させ、複雑さを軽減するのに役立ちます。 ポリシーアシスタントは、英語の会話フレーズを特定のセキュリティポリシーに自動的に変換します。 • 複数のユーザーがいる管理者グループは、より一貫性のある効果的なポリシーセットを作成できます。 • 大規模なポリシーセットが必要な場合は、コスト削減とリソース節約を拡大できます。 ドキュメントアシスタントは、文書の検索と理解を簡素化し、Secure Access の質問に対する回答をすばやく簡単に得られるようにします。 • 自然言語による質問を解釈し、Secure Access の文書から回答を提供します。 • 複数の文書やページを検索して包括的な応答を行う複雑なクエリを処理します。

機能	利点
エクスペリエンスに関するインサイト：デジタル エクスペリエンス モニタリング（DEM）	ユーザーがリソースにアクセスする際に、エンドポイント、アプリケーション、およびネットワーク接続の正常性とパフォーマンスをモニターします。ユーザーのエンドツーエンドのエクスペリエンスの詳細を自動的にキャプチャすることで、ユーザーの生産性を最適化し、障害対応を簡素化し、インシデントの解決時間を短縮します。 主なインサイトの例： • エンドポイントのパフォーマンス：CPU 使用状況、メモリ使用率、および Wi-Fi 信号強度。 • ネットワークのパフォーマンス：遅延、ジッター、パケット損失、推奨される修復などのメトリックを含む、エンドポイントから Secure Access までのセグメントの可視化。 • Outlook、Slack、Workday、SharePoint など、一般的に使用されている（上位 20）SaaS アプリケーションのパフォーマンスステータス。 • ユーザー固有のセキュリティイベント。 • 履歴データやデジタル体験スコアを含む、Webex、Zoom、Microsoft Teams などのコラボレーション アプリケーションのパフォーマンス。 • 組織全体のグローバルなエンドポイント トポロジ マップ。 • ThousandEyes エンドポイントライセンスを購入すると、エンドツーエンドの模擬テスト（任意のエンドポイントからパブリックとプライベートの両方のアプリケーションまで）をすべて Secure Access 統合ダッシュボード内で管理できます。
サービスとしてのファイアウォール（FWaaS） **これを次のように書き換えます。** **侵入防御システム（IPS）**	すべてのポートとプロトコルにおいて、インターネット上またはお客様のプライベート インフラストラクチャ上で、ユーザーと接続先/アプリケーション間のトラフィックを完全に可視化し、包括的なセキュリティ制御を可能にします。ローミング中の、または分散拠点のキャンパスネットワークからインターネットやプライベート アプリケーションにアクセスするリモートユーザーが含まれます。 • インターネット、プライベートネットワーク、プライベート アプリケーションにアクセスするユーザー/グループ、ネットワーク、またはデバイスを保護するための L3/4 アクセス制御ルール。 • Snort 3.0 をサポートするカスタマイズ可能な IPS プロファイル。インターネットとプライベートアクセスの両方について、ルールに一致するトラフィックパターンに対してルールごとに IPS 検査を行います。 • 特定されるアプリケーションの継続的な増加に基づく、レイヤ 7 アプリケーション、アプリケーションプロトコル、およびポート/プロトコルの可視性と制御。 • 検査の前に、インターネットまたはプライベートアクセスのトラフィックを復号します。 • ユーザーとプライベート アプリケーション間のトラフィックに対する双方向のファイル検査とファイルタイプの制御。 • スケーラブルなクラウド コンピューティング リソースにより、アプライアンスのキャパシティに関する問題を解消します。
Cisco Secure Malware Analytics	高度なサンドボックス分析と脅威インテリジェンスを組み合わせて 1 つの統合ソリューションを提供し、マルウェアから組織を保護します。Cisco Secure Malware Analytics コンソールへのフルアクセスを提供して、Glovebox での悪意のあるファイルの実行を可能にし、ファイル実行アクションを追跡し、ファイルによって生成されたネットワークアクティビティをキャプチャします。 Investigate API と組み合わせると、セキュリティアナリストはさらに踏み込んで悪意のあるドメイン、IP、ファイルのアクションにマッピングされた ASN を検出し、攻撃者のインフラストラクチャ、戦術、およびテクニックの最も包括的なビューを取得できます。 • 隠蔽された攻撃方法を検出し、悪意のあるファイルについて報告する機能。 • セキュリティデータを強化するために XDR と一般的に使用される SIEM を統合する API。 • ファイルの性質が変更された場合（当初は良好だったが、後に悪意があると見なされた場合など）のレトロスペクティブな通知。
リモートブラウザ分離（RBI）	RBI は、ユーザーによるブラウジングアクティビティの実行をリモートのクラウドベースの仮想化ブラウザに移行することによって、ブラウザベースの脅威を阻止します。Web サイト コードは個別に実行され、その Web の安全なバージョンのみがユーザーに配信されます。エンドユーザーに対しては完全に透過的です。まだ署名が作成されていないマルウェアについて心配する必要はありません。 • ユーザーデバイスとブラウザベースの脅威との間にある Web トラフィックの隔離。

機能	利点
	• ゼロデイ脅威からの保護。 • さまざまなリスクプロファイルの詳細な制御。 • 既存のブラウザ設定を変更せずに迅速に展開。 • オンデマンドの拡張性で追加のユーザーを簡単に保護。 • 既知の危険なインターネットサイトにアクセスする必要がある従業員を保護します。ブロッキングによって生産性が低下することはなく、ユーザーの安全性が維持されます。
DNS レイヤセキュリティ	DNS レイヤでフィルタ処理を行い、ネットワークやエンドポイントへの接続が確立される前に、ポートまたはプロトコル上で悪意のある不適切な接続先への要求をブロックします。 • すべてのネットワークデバイス、オフィスの場所、およびローミングユーザーやモバイルデバイスのインターネットアクセスを保護します。 • セキュリティ脅威や Web コンテンツの種類、および実行されたアクションごとに DNS アクティビティに関する詳細なレポートを提供します。 • シスコの DNS トンネリングで使用している人工知能アルゴリズムは、データ漏洩をリアルタイムで検出して阻止します。 • 数千におよぶ場所やユーザーに対して迅速に運用を開始し、即時に保護できます。 • Cisco Secure Client、仮想アプライアンス、およびサードパーティの統合を活用することで、レポートと適用されたポリシーをユーザーレベルまで可視化します。
Talos 脅威インテリジェンス **および** **Investigate API**	世界最大の民間の脅威インテリジェンスチームの 1 つである Cisco Talos は、その脅威データと分析の巨大なデータベースに対する AI、統計、および機械学習モデルを継続的に実行し、サイバー脅威に関するインサイトを提供してインシデント対応率を向上させます。 API を介して利用できる Investigate は Talos のデータを活用しており、セキュリティチームがこの脅威インテリジェンスにプログラムでアクセスして分析し、インシデントの調査と対応を迅速化するのに役立ちます。その例を次に示します。 • 脅威のコンテキスト（ドメインと IP の分析、脅威スコア、ドメインの分類、履歴データ）に関するインサイトを取得します。 • 攻撃を特定のドメイン、IP、ASN、およびマルウェアに関連付けることで、攻撃者のインフラストラクチャをマッピングします。 • 新たな脅威を特定し、今後の攻撃のステージを予測します。 • カスタムクエリを作成し、より詳細なコンテキストを取得して、意思決定と修復を迅速化します。
単一の管理およびレポートコンソール	インターネット、パブリック SaaS アプリケーション、およびプライベート アプリケーションへのアクセス全体における、インテントベースのルールを使用した統合されたセキュリティポリシーの作成と管理。広範なロギングや、企業 SOC へのログのエクスポート機能を提供します。 • あらゆるユーザーのあらゆるアプリに対するポリシーを一元的に定義。セキュリティポリシーの構築プロセスを簡素化し、組織全体でポリシー定義の一貫性を促進します。 • 統合されたソース（ユーザー、デバイス）と統合されたリソース（アプリケーション、接続先）により、アタッチポイントやアクセスするアプリケーションに関係なく、セキュリティポリシーがユーザーに対応するようになります。 • 進行中のポリシー管理アクティビティを削減します。 • 集約されたレポート作成機能により、可視化と検出までの時間が改善されます。 • SOC/セキュリティアナリストの調査プロセス全体を簡素化します。
リソースコネクタ	リソースコネクタは、オンプレミスのデータセンターとクラウドのどちらにあるかに関係なく、プライベート アプリケーションへのセキュアな接続を設定するための管理タスクを簡素化します。AWS、Azure、および VMWare をサポートします。 • デバイスおよびファイアウォールルールの変更に関するネットワークチームへの依存を軽減します。 • ダイナミックルーティングの設定やサブネットの重複といったルーティングの複雑さを解消します。 • 合併などのシナリオでは、重複する IP でネットワークが異なる状況が多く見られます。トンネルを使用すると複雑になるため、アプリケーションコネクタによってこの複雑な状況を解消します。 • プライベートアプリの場所（IP アドレス）を非表示にし、セキュリティアクセス内のゼロトラストポリシーを介した接続のみを許可することで、プライベートアプリを保護します。

機能	利点
	• リソースとネットワークを分離することで、ラテラルムーブメントを防止します。
デバイス サポート Cisco Secure Client は Secure Access に含まれており、追加料金はかかりません。	• インターネットトラフィック、ZTA 経由のプライベートトラフィック、VPNaaS 経由のプライベートトラフィック用の Windows および MacOS 上の Secure Client。 • インターネットトラフィックおよび VPNaaS 経由のプライベートトラフィック用の Linux、iOS、Android 上の Secure Client。 • プライベートトラフィック用のクライアントレス ZTNA オプション、ブラウザベース（クライアントなし）。 • Cisco Security for Chromebook Client は、DNS および SWG 保護を適用します。Chromebook OS 全体を対象とする DNS レイヤセキュリティ。Chrome ブラウザの SWG 保護。 • Apple および Samsung の次世代モバイルデバイスのサポート（モバイルデバイスの ZTNA サポートについては、以下のセクションを参照）。
モバイルデバイスの ZTNA サポート	シスコは Apple と Samsung の両社とのコラボレーションにより、パフォーマンスとセキュリティの利点を備えた独自の合理化された ZTNA プロセスを作成しました。シスコはその他の Android モバイルデバイスからの ZTNA もサポートしています。 • Secure Access は、登録、設定、障害対応、およびトラフィックステアリングを効率化します。 • QUIC および MASQUE プロトコルを使用してトランジットを高速化し、VPP アクセラレーションを使用してスループットを向上させます。 • デスクトップと同じモバイル ZTA 登録エクスペリエンス。 • 管理者は、コネクテッドデバイスの詳細を表示できます。 • 障害対応においては、ユーザーはクライアントから使用可能なログをエクスポートし、ヘルプデスクと対話するときにそれを使用できます。 • iOS デバイスで完全なクライアントを導入および管理する必要がなく、展開が簡素化されます。 • iOS オペレーティングシステム内に組み込まれている機能を利用して単一レイヤの暗号化を備えた Apple の iCloud プライベートリレーを活用し、高速でセキュアなアクセスを実現します。
Catalyst SD-WAN との統合：インターネット/SaaS アプリケーションにアクセスするブランチユーザー	Catalyst SD-WAN と Secure Access の統合と自動化により、ブランチユーザーから Web および SaaS アプリケーションへのステアリングを Cisco Secure Access で保護することが可能になります。 • Secure Access のマルチレイヤ セキュリティ ソリューションによる脅威からの保護の強化。 • ブランチの SD-WAN ロケーションと Secure Access 間のトンネルを自動化し、IT の展開を簡素化します。 • ユーザーがローミング場所とオンプレミスの場所の間を移動するときのエクスペリエンスの一貫性が向上します。 • Secure Access の一元化されたポリシー管理、容易な拡張/縮小性、およびキャパシティの制約からの解放により、IT/セキュリティ運用を簡素化します。 • SD-WAN から送信された VPN/VRF（オプションで SGT）データを使用して、Secure Access で異なるタグ/ラベルに異なるポリシーを適用できるようにし、よりきめ細かなセキュリティ保護を実現します。ブランチ全体およびクラウドでのセキュリティポリシー適用の一貫性が向上します。
Identity Services Engine（ISE）との統合	ISE と Secure Access の統合により、アイデンティティベースのきめ細かな情報を提供し、ユーザーが何を、いつ、どのように行っているかを詳細に可視化します。インターネットおよび SaaS アプリケーション トラフィックのポリシー制御と適用を強化して、ネットワークの攻撃対象領域を縮小し、脅威のラテラルムーブメントの可能性を制限します。 • 適切なユーザーまたはデバイスに対して、適切なポリシーを適切なタイミングでより正確に適用できます。 • ISE を使用した認証要求の RADIUS をサポートします。 • セキュリティグループタグ（SGT）を使用してユーザーとモノを細かくセグメント化します。これはマイクロセグメンテーションとも呼ばれます。 • Secure Access と ISE のシームレスな統合エクスペリエンスは、SGT の標準的かつ一貫した表現を提供するコアプラットフォームである Security Cloud Control のコンテキストサービスを介して実現されます。

パッケージオプション

Cisco Secure Access には、Secure Access Essentials と Secure Access Advantage の 2 つの主要な階層があります。どちらの階層も、セキュア インターネット アクセス（SIA）とセキュア プライベート アクセス（SPA）の 2 つのユースケースで使用できます。これらは単一のサブスクリプションの一部として購入され、単一の統合されたダッシュボードとサービスとして提供されます。お客様は、階層でユースケースを一方のみ購入するか両方購入するかを選択できます。

Essentials と Advantage の 2 つの階層の機能の比較については、この文書を参照してください。

Cisco Secure Access：ソフトウェア サポート サービス

Cisco Secure Access には、Software Support-Enhanced 用の個別の SKU と、Software Support Premium へのアップグレードオプションが必要です。

Cisco Software Support Enhanced

- テクニカルサポート（Cisco Cloud Security Support への 24 時間 365 日のアクセス：電話/オンライン）。
- ソフトウェアアップデート。
- ソフトウェアの専門知識を持つ主要な連絡窓口。
- 技術的なオンボーディングと導入支援。

Cisco Software Support Premium（オプションのアップグレード）

Enhanced レベルの機能に加えて、以下が含まれます。

- Enhanced サポートよりも優先的にケースを処理。
- セキュリティソフトウェアの導入と継続的な管理・最適化を成功させるために、インシデント管理、プロアクティブなコンサルティングや提案を行う専門家をアサイン。
- サポートケース分析。

セキュリティソフトウェアに関するシスコのサポートサービスの詳細については、こちらをクリックしてご確認ください。

詳細情報

詳細については、Cisco Secure Access をご覧ください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-4843018-00 12/24