Cisco Secure Connect

あらゆる場所でホストされているアプリケーションとリソースに安全にアクセス

2023 年 6 月

目次

製品の概要

新しいハイブリッドワークの時代に伴って新しいアプローチが必要な中、あらゆる組織のハイブリッドワーク戦略において重要な成功の鍵を握っているのが、SASE（セキュア アクセス サービスエッジ）です。SASE は、クラウド内のネットワーキングおよびセキュリティ機能を、キャンパス、ブランチ、リモートワーカー、および請負業者（B2B）接続と組み合わせて、オフィス、家、コーヒーショップなど、ユーザーが作業する場所を問わず、安全でシームレスなユーザー体験を提供します。ただし、SASE の展開は複雑になる場合があります。既存のブランチ SD-WAN アプライアンスと無数のユーザーエンドポイントをクラウドベースのファブリックに接続するには、計画、統合、および設定が必要です。

Cisco Secure Connect はターンキー型の統合 SASE です。企業がいくつものパブリッククラウドやプライベートクラウドであらゆる場所でホストされているアプリケーションとリソースに、いつでも、どこからでも安全にアクセスできる環境を非常にシンプルな方法で実現できます。統合されたクラウドダッシュボードを通じて簡単に導入、使用、管理できるので、企業の運用の複雑さが大幅に軽減され、俊敏性、速度、拡張性が向上します。

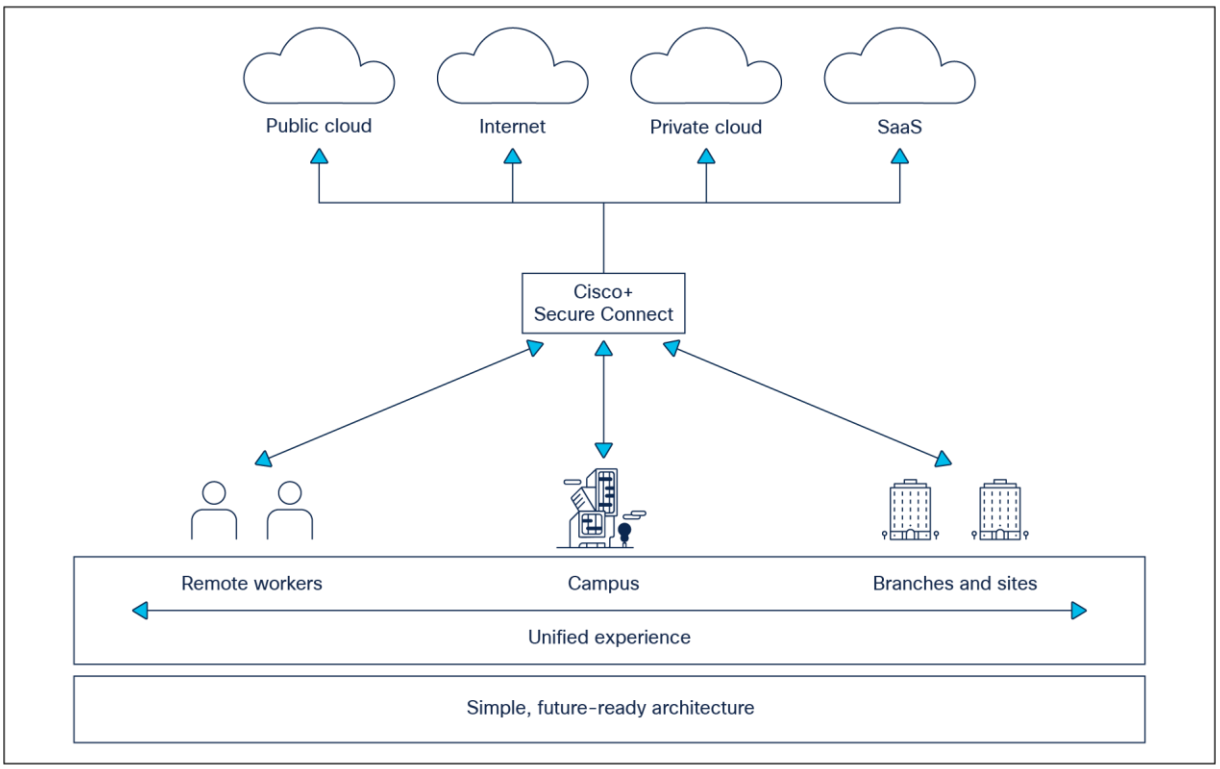

図 1.
Cisco Secure Connect ユースケース

Cisco Secure Connect は、1 つのサブスクリプションで、あらゆる場所（ブランチまたはリモート）のユーザーをあらゆるアプリケーション（プライベートデータセンター、パブリッククラウド、または SaaS）に安全に接続します。このソリューションは、クライアントベースおよびクライアントレスでのリモートワーカーアクセス、Cisco Meraki™ SD-WAN のネイティブ接続、Zero-Trust Network Access（ZTNA）による包括的なクラウドベースのセ

キュリティ機能、強化されたトラフィック収集、Cisco Meraki SD-WAN ポリシーのインポートを統合しており、近い将来には統合ポリシーによるポスチャ強化も予定されています。

Cisco Secure Connect は、パッケージ形態で提供されており、お客様が組織のニーズに適したレベルの保護とカバレッジを簡単に選択でき、思い通りの SASE を行うことができます。Cisco Secure Connect は、2 つのパッケージ形態で提供されているため、お客様が組織のニーズに適したレベルの保護とカバレッジを簡単に選択できます。

Cisco Secure Connect Foundation

Cisco Secure Foundation パッケージには、ブランチユーザーとローミングユーザーにセキュアなインターネットアクセス接続を提供する Cisco Umbrella® SIG 機能、ブランチユーザーにプライベート アプリケーション アクセスを提供する Cisco Secure Connect ファブリック インターコネクト、セキュリティとネットワークポリシーに関する合理化された運用管理の可視性と制御を提供する統合ダッシュボード、および SASE のニーズをシームレスにサポートする統合サポートが含まれています。また、Foundation パッケージには、リモートユーザーにプライベート アプリケーション アクセスを提供するホスト型のサービスとしてのリモートアクセスの無料トライアル（非プロダクション）ライセンスが 10 個付帯します。***

Cisco Secure Connect Complete

Cisco Secure Complete パッケージには、実稼働レベルのサポート、クライアントベースのサービスとしてのリモートアクセス機能、およびユーザーにゼロトラスト セキュリティ モデルを提供するクライアントレス ZTNA 機能が含まれています。

表 1. コア製品パッケージ

パッケージ	説明	特長
Cisco Secure Connect Foundation Essentials	ブランチユーザーおよびローミングユーザー向けの安全なインターネットアクセス接続	• リモートアクセス：クライアントベースのアクセスで 10 ユーザの無料トライアル • セキュリティ：セキュア Web ゲートウェイ（Web トラフィックのプロキシと検査、URL フィルタリング、Cisco Secure Malware Analytics - 最大 500 サンプル/日）、クラウド アクセス セキュリティ ブローカ（クラウドアプリケーションの検出、リスクスコアリング、ブロック、2 アプリケーションのクラウドマルウェア検出）、Layer-3/Layer-4 クラウドファイアウォール、DNS レイヤセキュリティ • 接続性：プライベートアクセス、ネットワーク アクセス コントロール、ダイレクト SaaS および IaaS ピアリング、Cisco Meraki Secure SD-WAN 統合、サイト、ユーザー、アプリケーションの相互接続 • 管理ダッシュボード：Cisco Meraki による接続およびセキュリティのシンプルな管理と一元的な可視化 • サポート：電子メールと電話による 24 時間 365 日の統合 SASE サポートへのアクセス、セルフヘルプ用のドキュメントポータルへのアクセス
Cisco Secure Connect Foundation Advantage	データ保護、高度なポリシー	Cisco Secure Connect Foundation Essentials に含まれるすべての機能に加えて、次の機能を備えています。 • セキュリティ：Layer-7 クラウド提供型ファイアウォール + IPS、インライン データ損失防止、クラウドマルウェア検出（サポートされているすべてのアプリケーション用）、Cisco Secure Malware Analytics（サンドボックスへの無制限送信無制限）

パッケージ	説明	特長
Cisco Secure Connect Complete Essentials	ハイブリッドユーザー向けの安全なインターネット、サービスとしてのリモートアクセス、および ZTNA	• リモートアクセス/ZTNA：クライアントベースのアクセス、クライアントレスのブラウザベースアクセス（最大 10 アプリケーション）、ユーザーおよびアプリケーションベースのきめ細かいアクセスポリシー、SAML 認証、組み込みアイデンティティプロバイダー（IdP）、ポスチャおよびコンテキストに応じたアクセス制御、レポート • セキュリティ：セキュア Web ゲートウェイ（Web トラフィックのプロキシと検査、URL フィルタリング、Cisco Secure Malware Analytics - 最大 500 サンプル/日）、クラウド アクセス セキュリティ ブローカ（クラウドアプリケーションの検出、リスクスコアリング、ブロック、2 アプリケーションのクラウドマルウェア検出）、Layer-3/Layer-4 クラウドファイアウォール、DNS レイヤセキュリティ • 接続性：プライベートアクセス、ネットワーク アクセス コントロール、ダイレクト SaaS および IaaS ピアリング、Cisco Meraki Secure SD-WAN 統合、サイト、ユーザー、アプリケーションの相互接続 • 管理ダッシュボード：Cisco Meraki による接続およびセキュリティのシンプルな管理と一元的な可視化 • サポート：電子メールと電話による 24 時間 365 日の統合 SASE サポートへのアクセスと、セルフヘルプ用のドキュメントポータルへのアクセス
Cisco Secure Connect Complete Advantage	データ保護、高度なポリシー	Cisco Secure Connect Essentials に含まれるすべての機能に加えて、次の機能を備えています。 • リモートアクセス/ZTNA：クライアントレスのブラウザベースアクセス（最大 300 アプリケーション） • セキュリティ：Layer-7 クラウド提供型ファイアウォール + IPS、インライン データ損失防止、クラウドマルウェア検出（サポートされているすべてのアプリケーション用）、Cisco Secure Malware Analytics（サンドボックスへの無制限送信無制限）

機能と利点

表 2. 新機能と利点

機能	利点
Meraki SD-WAN ネイティブ統合	インターネット、SaaS、プライベートアプリケーションへのアクセスを可能にする Meraki SD-WAN のネイティブ統合により、ブランチサイトを Cisco Secure Connect に簡単に接続できます。ブランチサイトで Meraki SD-WAN アプライアンスの AutoVPN 機能を活用して SASE ファブリックに接続すると、レジリエンシが向上し、インテリジェントなパス選択が実現します。これにより、組織は、接続されているすべてのサイトに一貫したアクセスとセキュリティ制御を実装することもできます。
Meraki SD-WAN クラウドトラフィック取得の強化	Cisco Secure Connect は、Meraki SD-WAN 統合のための動的にスケーラブルな高帯域幅ヘッドエンドソリューションを導入します。Meraki の AutoVPN ソリューションを活用することで、この拡張されたクラウドトラフィック取得ソリューションは、接続する Meraki SD-WAN サイトごとに帯域幅を動的に拡張します。サイトあたりの現在の帯域幅スケールは、単方向と双方向の両方で約 500 Mbps です。このソリューションでは、Meraki SD-WAN と Cisco Secure Connect の統合について、よりシンプルなユーザー体験も提供します。
クライアントレスのゼロトラスト ネットワーク アクセス（ZTNA）。	Cisco Secure Connect は、エンドポイントデバイスにエージェントやクライアントをインストールすることなく、プライベートアプリケーションの最小権限アクセス制御を可能にします。管理者は、請負業者や従業員に対して、横移動を行うことなく、アクセスが必要なリソースのみにアクセス権限を簡単に割り当てることができます。管理者は、エンドポイントの OS のタイプとバージョン、ブラウザのタイプとバージョン、およびアクセス制御で使用される地理位置情報のポスチャプロファイルを設定できます。

機能	利点
クライアントベースの安全なリモートワーク	Cisco Secure Connect を使用すると、リモートユーザーは Cisco AnyConnect® クライアントを使用して、Cisco Secure Connect ファブリックを介してどこからでもプライベート アプリケーションにアクセスできます。お客様の IdP で SAML 認証を行うことで、ID ベースのアクセス制御が可能です。エンドポイントのポスチャも評価されます。これにより、プライベートリソースに対するきめ細かいアクセス制御が可能になります。
セキュアなインターネットアクセス	セキュアなインターネットアクセスは、ユーザーの居場所や VPN の使用状況に関わらず、安全なインターネットアクセスを実現するものです。Cisco Secure Connect は、ユーザーが接続先に接続する前に、インターネットへのセキュアなオンランプとして機能し、エッジとクラウドのハイブリッド保護により、防御と検査の第一線を提供します。ユーザーの居場所や接続先に関わらず、トラフィックはまずファブリックを通過できます。トラフィックがクラウドプラットフォームに到達すると、トラフィックのセキュリティのニーズに基づいて各種の検査とポリシー適用が行われます。 Cisco Secure Connect には、セキュア Web ゲートウェイ、クラウド提供型ファイアウォール、DNS レイヤセキュリティ、クラウド アクセス セキュリティ ブローカ、およびデータ損失防止が含まれています。この堅牢なセキュリティソリューションは Cisco® Talos® インテリジェンスからリアルタイムのプロアクティブな脅威の最新情報を取得してユーザーの安全を確保するとともに、脅威の情報入手という面倒なプロセスから IT チームを解放します。
ユーザー認証	Cisco Secure Connect では、エンドユーザー認証のために独自の SAML プロバイダーを利用するか、バンドルされているクラウド アイデンティティ プラットフォームを使用して、ユーザーを簡単に設定し、サービスを迅速に開始することができます。クラウドアイデンティティ機能は、SAML IdP が設定されていないお客様、またはサービスにアクセスするためのユーザー認証に既存の SAML IdP を使用したくないお客様が利用できます。クラウドアイデンティティ機能は、Cisco Secure Connect ダッシュボードからいくつかの簡単な手順で設定できます。また、既存の Meraki クラウド認証設定をワンクリックでサービスに適用することもできます。
Meraki ポリシーのインポート	Cisco Secure Connect は、現在リモートワーカーを Meraki MX ヘッドエンドへのリモートアクセス接続を介して会社のリソースにアクセスさせている人のために特別に設計されたポリシーのインポート機能をネイティブに導入しました。これらのお客様が Secure Connect リモートアクセスサービスに移行する場合、この機能により、クライアント VPN トラフィックに影響する MX ファイアウォールポリシーを、ガイド付きウィザードを使用して Secure Connect のクラウドファイアウォールにインポートできます。これにより、管理者がポリシーを作成および合理化するために必要な時間を短縮できます。さらに、移行前に重複を検出します。
統合管理	Cisco Secure Connect の管理は、サービスの設定、モニター、およびトラブルシューティングを行う単一のダッシュボードで処理されます。ガイド付きフローと動的チェックリストにより、設定が簡素化されます。ユーザーとサイトのモニタリングは、セキュリティと接続のインジケータを統合する単一のペインで行われます。
ネットワークインターコネクト	ネットワークインターコネクトは、Cisco Secure Connect に接続された送信元と接続先の間のインテリジェントなルーティングを提供します。インターコネクトに接続されたどのノードも、すでに接続されているどのノードにもシームレスにアクセスできるようになり、Cisco Secure Connect からエッジとクラウド全体で統一された方法でアクセスポリシーが適用されます。これにより、ネットワークの複雑さが大幅に軽減され、最小限のセットアップとメンテナンスで可用性の高いネットワークファブリックが提供されます。

カスタマー サポート

Cisco Secure Connect では現在、+1.617.206.4332 にお電話いただくか、製品ダッシュボードからサポートケースを開いていただくことで、24 時間 365 日のカスタマーサポートを提供しています。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明箇所	日付
Foundation と Complete の詳細を含むようにパッケージセクションを更新	4 ～ 5 ページ	2023 年 6 月 21 日
ユースケースの図を含む、製品概要を調整	3 ページ目	2023 年 3 月 29 日
その他の機能と利点を追加	5、6 ページ	2023 年 3 月 29 日
新しいカスタマーサポート時間/対応可否を反映するようにサービスを変更	6 ページ	2022 年 10 月 20 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

0731-2023-000-X