The bridge to possible

Cisco Secure Connect

The bridge to possible

概要

業界をリードするシンプルさを備えた Cisco Secure Connect は、**SASE への移行計画を簡素化**する統合ターンキーソリューションです。より高いネットワークの復元力と安全なハイブリッドワーク環境の構築を支援し、シームレスで統合された体験を実現するこのソリューションは、SASE への近道となります。また、Secure Connect では、オンプレミスからクラウドまで一貫した運用モデルを拡張することで、シームレスで安全な接続性を提供し、単一のダッシュボードでの運用管理を容易にし、可視性と制御を向上できます。1 つの強力なプラットフォームに統合された Secure Connect は、ネットワークとセキュリティを調和させ、体験の統一、SASE に関する複雑さの低減、お客様に安心感をもたらすネットワークの構築を実現します。

Q : SASE とは何ですか。

A : SASE (セキュア アクセス サービス エッジ) は、あらゆる組織のハイブリッドワーク戦略を実現する上で重要な役割を果たします。SASE によって、クラウド型のネットワークおよびセキュリティ機能とともに、キャンパスやブランチのユーザー、リモートワーカー、請負業者(B2B) が接続可能な環境を実現することで、勤務場所に関係なく安全でシームレスなユーザー体験を提供できます。ただし、SASE の展開は複雑になる可能性があるため、ブランチの既存 SD-WAN アプライアンスや膨大な数のユーザーエンドポイントを安全なクラウドベースファブリックに接続させるには、計画、統合、設定が必要となります。

SASE の主な基盤は、ルーティングを含む SD-WAN と、セキュリティサービスエッジ (SSE) であり、SSE は、ゼロトラスト ネットワーク アクセス (ZTNA)、クラウド アクセス セキュリティ ブローカ (CASB)、サービスとしてのファイアウォール (FWaaS)、セキュア Web ゲートウェイ (SWG)、サービスとしてのリモートアクセスで構成されます。

Q : ゼロトラスト ネットワーク アクセス (ZTNA) とは何ですか。

A:ゼロトラスト ネットワーク アクセス (ZTNA) とは、ユーザーとデバイスを信頼できるものと判断するモデルであり、その検証のために各アクセス試行の認証と継続的なモニタリングを行い、カスタム セキュリティ ポリシーを適用し、すべてのアプリケーションを保護します。Secure Connect では、ユーザーが企業アプリケーションへのアクセスを許可する前に、アイデンティティ、ポスチャ、コンテキストに基づいて検証します。ユーザーがアクセスできるのは、業務上必要な特定のアプリケーションのみです。

Q : Secure Connect とは何ですか。

A : Secure Connect は、統合されたターンキー SASE ソリューションであり、これを導入することで、複数のパブリッククラウドやプライベートクラウドなど、さまざまな稼働先のアプリケーションやリソースへのアクセスが大幅に簡素化され、これらのリソースに、いつでもどこからでも安全にアクセスできるようになります。このソリューションの展開、利用、管理は、統合クラウドダッシュボードから簡単に行えるため、組織内で運用する際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。

Secure Connect を導入すると、ブランチやリモートなどの勤務場所に関わらずプライベートデータセンター、パブリッククラウド、SaaS といったあらゆる稼働先のアプリケーションに安全に接続できる環境を 1 つのサブスクリプションで実現できます。また、クライアントベースおよびクライアントレス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、ゼロトラスト ネットワーク アクセス (ZTNA) による包括的なセキュリティ機能が統合されています。

Secure Connect では、次の主要機能によって、包括的な SASE ソリューションを実現します。

- Complete パッケージの一部としての ZTNA とエンドポイントのポスチャ検証によるリモートワーカー接続
- SASE の SD-WAN および SSE コンポーネントの両方を管理、設定、トラブルシューティング、可視化を実現する統合 SASE ダッシュボード
- 安全なブランチ接続を実現する Meraki SD-WAN をシンプルかつシームレスにサポート ***
- 市場で最も包括的で強力、しかもシンプルな統合 SASE ソリューションである Cisco Umbrella®(将来的には Cisco® Secure Access) によるクラス最高水準のクラウドベースのセキュリティ機能を提供

Q : Secure Connect と市場に見られる同様のソリューションにはどのような違いがありますか。

A : Secure Connect は、市場に見られる同様の選択肢よりも明らかな利点をもたらします。主な差別化要因は次のとおりです。

- インターネットアクセス、プライベートアクセス、安全な SD-WAN 接続を実現する統合ターンキーソリューションであり、ブランチワーカーとリモートワーカーの両方に対応しています。統合ダッシュボードで管理し、単一のサブスクリプションで利用できます。
- セキュリティとネットワークを統合し、さまざまな技術で一貫した体験を実現する、最新化かつ将来性のあるアーキテクチャによって豊富なセキュリティ、相互接続性、可視性を備えています。
- 実績ある Cisco® コンポーネントを基に構築されており、Umbrella SIG によるクラウドセキュリティを備えています。
- Meraki SD-WAN と緊密な連携を提供し、わずか数クリックでファブリックをクラウドに拡張することで統合された SASE 体験を実現します。また、高い信頼性と次世代ポリシーエンジンによって組織全体で管理を一元化できるほか、セキュリティポリシー適用を分散化しエンドユーザー体験を最適化します。
- Secure Connect では、お客様の利用用途に応じて、柔軟に利用可能なユースケースパッケージを用意しています。
  - **Foundation パッケージ** : 次の機能で構成されます。ブランチおよびローミングユーザーに安全なインターネットアクセスを提供する Umbrella SIG 機能、ブランチユーザーがプライベート アプリケーションにアクセスを提供する Secure Connect ファブリック インターコネクト、セキュリティおよびネットワークポリシーの可視化と制御をシームレスに提供する統合ダッシュボード、お客様の SASE ニーズを支援するシームレスな統合サポート。またこの Foundation パッケージには、ホストされたリモートアクセスの無料トライアル (本番ではない環境向け) 10 ライセンスも付属しています。これによって、プライベート アプリケーションへのアクセスをリモートユーザーに提供できます。このパッケージは、オフィス環境でのみ働くユーザー向けに設計されています。
  - **Complete パッケージ** : 次の機能で構成されます。本番環境レベルでご利用いただける、クライアントベースのリモートアクセス機能、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。このパッケージは、オフィスだけでなくリモートでも働くハイブリッドユーザー向けに設計されています。

Q : Secure Connect によって、お客様が抱えているどのような課題や問題点を解決できますか。

A : Secure Connect は、次のような問題を解決したいお客様に適しています。

- SASE のネットワークおよびセキュリティ機能を 1 つのソリューションに統合することで、運用の簡素化、効率化、エンドユーザー体験の向上を図りたい。
- 従業員が自宅でもオフィスでも働くハイブリッドワークモデルを活用したい。
- ブランチユーザーのセキュリティ確保を最適化するため、ネットワーク変革を実施したい。

- リモートユーザーと企業（サイト）ユーザー全体を対象に監査とリスクを最小化に取り組む、スリムな IT 部門を支援したい。
- ネットワーク主導の SASE に基づく決定により、ネットワークとセキュリティの単一チームの効率を高めたい。
- ユーザーにリモートアクセスを提供するために必要な資本と、運用の展開時間を最小化したい。
- SD-WAN とクラウド全体を横断するポリシーと、セキュリティをエンドツーエンドで管理し可視化することで、ネットワークのセキュリティ態勢と復元力を向上させたい。

Q：競合する SASE aaS（サービスとしての SASE）ソリューションを考えた場合、Secure Connect にはどのような差別化要因がありますか。

A：シスコの主な差別化要因は、ターンキー統合 SASE ソリューションの提供です。これによって SD-WAN 運用とセキュリティポリシー適用を一元化することで、ネットワークおよびセキュリティ管理を 1 つのプラットフォームに統合し合理化できます。この市場で SD-WAN と SSE ソリューションを両方提供している他社は、SASE の成果を迅速に実現する統合プラットフォームの提供に苦労しています。この統合プラットフォームは新しいコンポーネントが拡張されると自動的に SASE の価値を追加する SASE ファブリックと、ストリームラインされたインターフェースを作成することで SASE の成果を迅速に実現します。

その他の主な差別化要因：

- ブランチユーザーにもリモートワーカーにも、インターネットアクセス、プライベートアクセス、安全な SD-WAN 接続を提供可能な統合ソリューションであり、統合ダッシュボードから管理し、単一のサブスクリプションで利用できます。
- セキュリティとネットワークを統合することで、異なるテクノロジー間で一貫した体験に加え、豊富なセキュリティ、相互接続性、可視性を備えた最新かつ将来性のあるアーキテクチャを提供します。
- Fortune 100 社全企業を保護する実績を有する、業界をリードするシスコのコンポーネントと、世界中のユーザーを接続し保護したグローバル経験に基づき構築されています。

Q：Cisco Umbrella SIG/Meraki/SD-WAN コネクタをすでに導入している場合、新しい Secure Connect Foundation パッケージによってどのような利点がありますか。

A：Umbrella SIG 契約を拡張し、価値提案の強化により Secure Connect Foundation への拡張を検討しているお客様は、営業担当者に連絡して移行オプションについてご相談ください。

技術

Q：Secure Connect のデータセンターはどの地域にありますか。またどの地域でどのようなサービスを利用できるか教えてください。

A：利用可能なデータセンターとサービスを利用できる地域の最新情報については、https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco___Secure_Connect_Pre-configuration_Checklist/Data_Centers をご覧ください。

Q：Secure Connect が対応するサイト数とユーザー数はどれくらいですか。

Secure Connect は、最大 5,000 サイトと 50,000 ユーザーに対応しています。

Q：Secure Connect と Cisco Umbrella Meraki SD-WAN コネクタにはどのような違いがありますか。

Cisco Umbrella Meraki SD-WAN コネクタは、ブランチサイトからインターネットに安全にアクセスするための機能であり、これによって、Meraki SD-WAN ファブリックを Umbrella クラウドまで拡張できます。このコネクタは、Meraki SD-WAN と Umbrella SIG の導入後に有効になります。展開済みの各コネクタには 250 Mbps という制限があり、展開可能なコネクタ数にも制限が設けられています。これら 2 つのソリューション（Meraki SD-WAN と Umbrella SIG）は、Secure Connect 内ではなく 2 つの別々のダッシュボードで管理します。

Secure Connect は、統合 SASE 体験の提供に重点が置かれており、セキュリティとネットワークを Meraki ダッシュボードで一元的に管理します。このソリューションを導入すると、安全で高パフォーマンスのインターネットアクセスのほか、リモートアクセス、ZTNA、相互接続 (ユーザー、サイト、アプリケーション間)、統合技術への対応といった新規ユースケースも実現可能です。

お客様は、Secure Connect Complete を利用して、導入対象の SASE ユースケースを選択することも、Secure Connect Foundation を利用して、セキュア インターネット アクセスのユースケースを選択することもできます。いずれの場合も、統合 SASE 体験が得られます。

Q : Cisco Umbrella SIG/Meraki/SD-WAN コネクタをすでに導入している場合、新しい Secure Connect Foundation パッケージによってどのような利点がありますか。

A : Meraki MX と Umbrella SIG を統合して利用しているほとんどのお客様は、新しい Foundation ライセンスに無料でアップグレードできます。エンタープライズ アグリーメント (EA) に含めず、かつ、アドオン (予約 IP、RBI、または複数組織) なしで SIG を購入したお客様は、このアップグレードを利用できます。アドオンを購入済み、あるいは EA を契約済みのお客様は、将来的にアップグレードが可能です。ソリューションのアップグレードに関心をお持ちの場合は、シスコの営業担当者にお問い合わせください。

Q : リモートユーザーが接続を行うには、どのようなユーザー デバイス エンドポイント (ラップトップ、携帯電話など) が必要ですか。

A : エンドポイントソフトウェアは、Microsoft Windows 7、8、10、11、MacOS 10.8 以降、Linux で利用でき、Apple iOS、Android、Google Chrome OS 向けのモバイル版も用意されています。

Q : Meraki を利用した Cisco SD-WAN を導入済みですが、どうすれば Secure Connect を追加できますか。

A : Meraki を利用した Cisco SD-WAN は、Secure Connect 内にすぐに展開でき、その方法もシンプルです。このソリューションのサブスクリプションを利用すると、実際にわずか数クリックで、既存の SD-WAN を Secure Connect ファブリックに接続できます。

Secure Connect では、地域に応じて各種接続タイプを利用できます。サイトを Secure Connect に接続する方法の詳細については、https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco__Secure_Connect_Now-_Sites をご覧ください。

データセンターに応じて、Secure Connect 機能の一部またはすべてを利用できます。データセンターごとに利用可能な機能の詳細については、https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco___Secure_Connect_Pre-configuration_Checklist/Data_Centers をご覧ください。

Q : Secure Connect は、スプリットトンネリングまたはトラフィックステアリングに対応していますか。

A : はい。Meraki SD-WAN のネットワークとリモートワーカーの両方にトラフィックステアリングを利用できます。リモートアクセスを行う場合、Secure Connect のトラフィックステアリングは、適応型セキュリティアプライアンス (ASA) を使用したリモートアクセスの場合とまったく同じように動作します。トンネルモードでは、全トラフィックのトンネリングの他、トンネルの内部または外部へのステアリングが可能です。

Q : Secure Connect と Cisco SecureX の統合および連携は可能ですか。可能な場合、どのようなことができますか。

A : Secure Connect は Cisco SecureX と統合してセキュリティの監視と制御に使用できます。プロキシイベントや DNS イベントの記録、検索に対応し、悪意のあるファイルの分析や悪意のあるドメインのブロックなどのイベントに関するインサイトや、無害な宛先への送信が許可されるトラフィックに関するインサイトをユーザーに提供します。

Cisco SecureX から Secure Connect に安全にログインする方法も利用できます。SecureX ログインの設定方法については、https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco___Secure_Connect_Onboarding/Cisco__Secure_Connect_-_Secure_X_Integration をご覧ください。

The bridge to possible

ゼロトラスト ネットワーク アクセス（ZTNA）

Q : Secure Connect には、どのようなゼロトラスト ネットワーク アクセス（ZTNA）機能が用意されていますか。

ZTNA のユースケースとして、リモートワーカーや B2B 請負業者による管理対象外デバイスからプライベート アプリケーションへの安全な接続が挙げられます。シスコが証明書とドメイン名を提供し、管理者が簡単に設定できるクライアントレス ZTNA によって、エンドユーザーは、ブラウザだけでアプリケーションに安全にアクセスできます。

また IT 管理者は、ユーザーのデバイスにインストールされたクライアント（Cisco Secure Client、旧称 Cisco AnyConnect®）でも、上記と同じ成果を得られ、ユーザーとアプリケーション間のきめ細やかなアクセス制御やポスチャチェックも行えます。

Q : クライアントレス ZTNA は、どのようなプロトコルをサポートしていますか。

A : 現在、クライアントレス ZTNA ソリューションは、HTTP と HTTPS をサポートしています。

Q : クライアントレス ZTNA には、利用している MFA を実装できますか。

A : Secure Connect の ZTNA 機能は、お客様が SAML 認証の一部として使用しているすべての MFA ソリューションに対応しているため、お客様がすでに利用している MFA の実装にも対応しています。

Q : Secure Connect はどのようなポスチャ機能をサポートしていますか。

A : シスコが提供している、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では、各エンドポイントのマシンの証明書、OS（オペレーティングシステム）、ファイアウォール、ディスク暗号化、マルウェア対策が確認されます。ポスチャポリシーの判定は「ブロック」か「許可」のどちらかになります。「検疫」は対応していません。

クライアントレス ZTNA ソリューションでは、IT 管理者は OS の種類とバージョン、ブラウザの種類とバージョン、地理位置情報に基づいて、ポスチャプロファイルを作成できます。

Q : 自前の Cisco ISE インフラストラクチャを介してポスチャを実行することはできますか。できる場合は、どのように実行できますか。

A : Cisco ISE を介したポスチャチェックはサポートされていません。

Cisco Catalyst SD-WAN 統合

Q : Cisco Catalyst® SD-WAN（Viptela®）統合は、どのようなユースケースを カバーしていますか。

A : Cisco Catalyst SD-WAN をご利用中であれば、Secure Connect でターンキー SASE ソリューションとして提供する主要なユースケースを活用できます。次のようなユースケースが含まれます。

- ブランチや企業のサイトからパブリックおよびプライベート アプリケーションへのアクセスを保護する。
- リモートワーカーがプライベートおよびパブリック アプリケーションに安全に接続できるようにする。たとえば
  - ゼロトラストでの検証結果に基づいてクライアントに接続を許可し、プライベート アプリケーションへのアクセスにアイデンティティベースのポリシーを適用する。
  - ブラウザベースのクライアントレス接続を可能にする。

統合の最初の段階では、Cisco Catalyst SD-WAN デバイスと Secure Connect 間の接続に焦点を当てます。これにより、SIG と Cisco Catalyst SD-WAN の間に導入済みの自動化を引き続き活用し、プライベートアクセスの機能と、セットアップを容易にする動的ルーティングを追加できます。

Q : Cisco Umbrella SIG と Viptela 間で行うこれまでの統合とは、どのような点が異なりますか。

A : Umbrella SIG および Catalyst SD-WAN 間で行う統合と、Secure Connect には、次のような違いがあります。

ユースケースに関しては、Cisco Umbrella SIG では、ブランチユーザーに安全なインターネットアクセスを提供すると同時に、リモートユーザー向けのローミング（SWG）を行えますが、Secure Connect でも、そうしたユースケースに対応可能です。さらに、クライアントベースのリモートアクセスによって、プライベート アプリケーションへの ID ベースのアクセスと、Secure Connect を介したすべてのポートとプロトコルへの安全なインターネットアクセスが可能になるほか、HTTP/HTTPS アプリケーションへのクライアントレスアクセスも実現できます。

Secure Connect と Cisco Catalyst SD-WAN を連携させると、統合管理とポリシー管理によって Viptela サービスハブの背後にあるプライベート アプリケーションやリソースを統合できます。これにより、相互接続機能を実現し、リモートアクセスユーザーが Secure Connect と統合されている Cisco Catalyst SD-WAN リソースに安全にアクセスすることも可能です。

Q : Cisco Catalyst SD-WAN（Viptela）は、どのダッシュボードで管理しますか。

A : Secure Connect は Meraki ダッシュボードで管理し、特定のタスクについては Cisco Umbrella ダッシュボードとの相互起動を行います。Meraki と Umbrella のダッシュボードは緊密に連携しており、シングルサインオンと RBAC をこれら 2 つの間で同期することで、シームレスなユーザー体験を得られます。Cisco SD-WAN の設定（トンネル設定、BGP 設定など）は、引き続き Cisco vManage で行います。

Q : Cisco Catalyst SD-WAN 統合は、Secure Connect Foundation パッケージと Complete パッケージのどちらでも利用できますか。

A : はい。可能です。例えば、Cisco Meraki と Catalyst SD-WAN が混在している場合や、セキュアなインターネットアクセスとセキュアなプライベートアクセスの両方が必要な場合など。

ユースケースが安全なインターネットアクセスのための Cisco Catalyst SD-WAN のみの場合、SIG の統合を活用した方が、より良い体験提供できる可能性があります。

サポート

Q:Secure Connect では、どのようなトラブルシューティング サポート モデルを採用していますか。

A : Secure Connect では、24 時間 365 日のトラブルシューティング サポートを受けることができます。サポートでは、ソリューションのすべての部分、つまり、ネットワークとセキュリティの両方について、連絡窓口が 1 つに統一されており、Secure Connect に問題がある場合の問い合わせ先としてこれを利用できます。問い合わせは、直通の電話番号でも、ダッシュボードからでも行えます。詳細については、https://documentation.meraki.com/CiscoPlusSecureConnect/Cisco___Secure_Connect_Troubleshooting_Guides/How_to_Contact_Cisco___Secure_Connect_Support をご確認ください。

Q : Secure Connect は、どのようなオンボーディングサービスに対応していますか。

A : シスコは、新製品である Secure Connect を安心してご利用いただけるよう努めており、2023 年度は、規模に関係なく、すべてのお客様に無料のオンボーディングサポートを提供します。ただし、2024 年度からは、現在利用可能な無料のオンボーディングサポートに代えて、強化したプレミアムサポート SKU を展開します。新しい SKU は 2024 年度第 1 四半期に導入する予定です。

料金とパッケージ

Q : Secure Connect では、どのようなパッケージオプションを利用できますか。

A : Secure Connect には、組織のニーズに適した保護レベルと適用範囲を簡単に選択できるよう、Secure Connect Foundation と Secure Connect Complete の 2 つのパッケージが用意されています。

Secure Connect Foundation パッケージ

Secure Connect Foundation パッケージは次の機能で構成されます。ブランチおよびローミングユーザーに安全なインターネットアクセスを提供する Umbrella SIG の各種機能、ブランチユーザーがプライベートアプリケーションにアクセスできるようにする Secure Connect ファブリック インターコネクト、運用管理の合理化と可視化やセキュリティおよびネットワークポリシーの管理を行える統合ダッシュボード、SASE のニーズをシームレスに満たすための統合サポート。このパッケージには、ホストされたサービスとしてのリモートアクセスを 10 ユーザーが利用可能な無料トライアル（本番ではない環境向け）ライセンスも付属しております。これはリモートユーザーにプライベート アプリケーション アクセスを提供します。

The bridge to possible

表 1.　Secure Connect Foundation パッケージ

機能	Cisco+ Secure Connect Foundation パッケージ	
	Essentials	Advantage
セキュリティ		
セキュア Web ゲートウェイ	✓	✓
URL フィルタリング	✓	✓
セキュアマルウェア分析	✓	✓
サンドボックス機能	500	無制限
クラウド アクセス セキュリティ ブローカ	✓	✓
クラウドマルウェア検出	2 つまで	無制限
DNS レイヤセキュリティ	✓	✓
L3 クラウド型ファイアウォール	✓	✓
L4 クラウド型ファイアウォール	✓	✓
L7 クラウド型ファイアウォール		✓
IPS ファイアウォール		✓
統合型 SASE		
統合されたセキュリティポリシー	✓	✓
ホワイトグローブ オンボーディング サポート (2024 年度で終了)	✓	✓
24 時間 365 日の統合サポート	✓	✓

機能	Cisco+ Secure Connect Foundation パッケージ	
	Essentials	Advantage
統合ダッシュボード	✓	✓
ターンキー方式の体験	✓	✓
ファブリック インターコネクト (CNHE : クラウド ネイティブ ヘッド エンド)	✓	✓
リモートアクセス		
クライアントベースアクセス	10 ユーザーが無料で利用可能 *	10 ユーザーが無料で利用可能 *
ブラウザベースのクライアントレスアクセス		
詳細設定が可能な、アプリケーションベースのユーザーアクセスポリシー	*	*
SAML 認証	*	*
組み込み 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	*	*

*** 6 ヵ月のトライアル（本番でない環境向け）**

The bridge to possible

Secure Connect Complete パッケージ

Secure Connect Complete パッケージは次の機能で構成されます。本番環境レベルのサポート、クライアントベースのリモートアクセス機能、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。

表 2. Secure Connect Complete パッケージ

機能	Cisco+ Secure Connect Complete パッケージ	
	Essentials	Advantage
セキュリティ		
セキュア Web ゲートウェイ	✓	✓
URL フィルタリング	✓	✓
セキュアマルウェア分析	✓	✓
サンドボックス機能	500	無制限
クラウド アクセス セキュリティ ブローカ	✓	✓
クラウドマルウェア検出	2 つまで	無制限
DNS レイヤセキュリティ	✓	✓
L3 クラウド型ファイアウォール	✓	✓
L4 クラウド型ファイアウォール	✓	✓
L7 クラウド型ファイアウォール		✓
IPS ファイアウォール		✓

機能	Cisco+ Secure Connect Complete パッケージ	
	Essentials	Advantage
統合型 SASE		
統合されたセキュリティポリシー	✓	✓
ホワイトグローブ オンボーディング サポート (2024 年度で終了)	✓	✓
24 時間 365 日の統合サポート	✓	✓
統合ダッシュボード	✓	✓
ターンキー方式の体験	✓	✓
ファブリック インターコネクト (CNHE : クラウド ネイティブ ヘッド エンド)	✓	✓
リモートアクセス		
クライアントベースアクセス	✓	✓
ブラウザベースのクライアントレスアクセス	10 アプリまで	300 アプリまで
詳細設定が可能な、アプリケーションベースのユーザーアクセスポリシー	✓	✓
SAML 認証	✓	✓
組み込み 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	✓	✓

Q : Secure Connect は現在、どの地域で利用できますか。

A : このソリューションは、パッケージ内容に応じて、次の特定地域で利用できます。

Foundation パッケージは、中国、キューバ、イラン、北朝鮮、ロシア、スーダン、シリアを**除く**すべての国で提供されています。

Complete パッケージは現在、次の各国で利用できます。オーストリア、ベルギー、ブルガリア、クロアチア、チェコ共和国、キプロス、デンマーク、エストニア、フィンランド、フランス、ドイツ、ギリシャ、ハンガリー、アイルランド、イタリア、ラトビア、リトアニア、ルクセンブルク、マルタ、オランダ、ノルウェー、ポーランド、ポルトガル、ルーマニア、スロバキア、スロベニア、スペイン、スウェーデン、スイス、英国、米国。

Q:Secure Connect の購入方法を教えてください。

A : Secure Connect サブスクリプションの購入については、シスコの営業担当者またはシスコパートナーにお問い合わせください。

Q:Secure Connect の価格体系を教えてください。

A : Secure Connect は Essentials と Advantage という 2 つのパッケージからなるサブスクリプションベースでライセンス提供されます。

Secure Connect Foundation パッケージ : ブランチ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に重点を置いています。

- Essentials : 安全なネットワーク接続
- Advantage : データ保護と高度なセキュリティ

Secure Connect Complete パッケージ : ハイブリッドユーザー向けの安全なインターネットアクセス、ZTNA、サービスとしてのリモートアクセスに重点を置いています。

- Essentials : 安全なネットワーク接続
- Advantage : データ保護と高度なセキュリティ

サブスクリプションを利用できる標準期間は 12 ヵ月、36 ヵ月、または 60 ヵ月です。Secure Connect のライセンスは、シート単位です。シートとは、サービスにアクセスできるインターネット接続ユーザーを指します。ユーザー数は、保護対象のデバイスまたはエンドポイントの数とは関係ありません。価格設定については、シスコの営業担当者またはシスコパートナーにお問い合わせください。

Q : リモートブラウザ分離（RBI）機能は Secure Connect に搭載されていますか。RBI を追加するにはどうすればよいですか。

A : リモートブラウザ分離 (RBI) は現在、Secure Connect では利用できず、RBI を個別に購入して Secure Connect で使用することもできません。また、サブスクリプションの変更によって、次に示す現在の Cisco Umbrella パッケージを Secure Connect に置き換えることはできません。Cisco Umbrella RBI、エンタープライズ アグリーメント(EA) で購入した Cisco Umbrella、または Cisco Umbrella Premium サポート、または今後 36 ヵ月以上有効な既存の Cisco Umbrella サブスクリプション。

Q : Secure Connect では、予約済み IP を利用できますか。どうすれば予約済み IP を追加できるでしょうか。

A : 予約済み IP は、Secure Connect Complete および Foundation のアドオンとして提供されます。

Q : IP はいくつ注文できますか。

A : IP の最小要件は 2 つです。1 つがプライマリ用、1 つがフェールオーバー用に使用されます。

Q:データセンターのペアが重要なのはなぜですか。

A : IPsec トンネルを提供するデータセンターのペアは、一方のデータセンターが利用できない場合のバックアップやフェールオーバーサイトとして機能します。ペアが設定されていないデータセンターも利用できますが、お客様が手作業でフェールオーバーを管理する必要があります。

Q : どのデータセンターが予約済み IP に対応していますか。

A : 利用可能なデータセンターの一覧については、https://docs.umbrella.com/umbrella-user-guide/docs/cisco-umbrella-data-centers をご覧ください。

Q : 予約済み IP はエニーキャストをサポートしていますか。

A : 現在、予約済み IP はエニーキャストをサポートしていないため、予約済み IP を確実に使用するには、IPsec トンネルを使用してネットワークを Cisco Umbrella に接続する必要があります。ローミングコンピュータの場合、クライアント VPN を使用して、予約済み IP でプロビジョニングされた Cisco Umbrella データセンターへの IPsec トンネルが確立されているネットワークに Web トラフィックを転送する必要があります。

Q : Secure Connect Foundation パッケージから Secure Connect Complete パッケージにアップグレードまたは移行することはできますか。

A : Secure Connect Foundation Essentials をご利用中の場合、Complete の Essentials または Advantage パッケージにアップグレードできます。Secure Connect Foundation Advantage をご利用中の場合、Complete Advantage パッケージにのみ移行できます。

C67-3064206-03 01/24