データシート

Cisco Public

CISCO SECURE

Cisco Secure Client

旧称 Cisco AnyConnect

2022 年 7 月

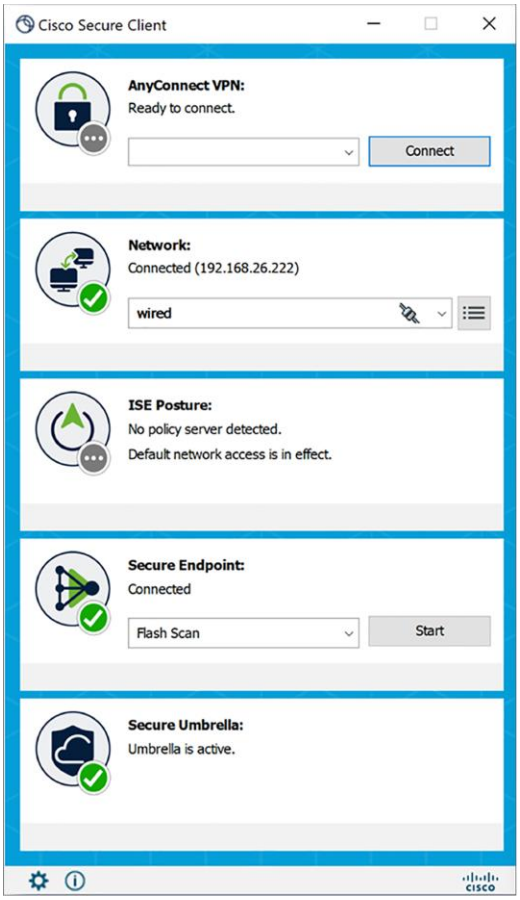
Contents

概要

Cisco Secure Client（旧称 Cisco AnyConnect セキュア モビリティ クライアント）は、Windows 10 および 11 で使用できます。ユーザーインターフェイスは現在の AnyConnect ユーザーが慣れ親しんだものとなり、一部のブランディングとアイコンが更新されます。

macOS および Linux を実行しているお客様は、Cisco Secure Client で OS が完全にサポートされるまで、AnyConnect 4.x を引き続きご利用いただけます。

Cisco Secure Client と AnyConnect



Cisco Secure Client は、最も広く展開されているセキュリティクライアントの最新バージョンです。Secure Client は、リモートアクセスサービスと一連のモジュラー セキュリティ サービスを提供する Cisco AnyConnect をベースに構築されています。

重要情報

AnyConnect は、現在、Cisco Secure Client と呼ばれています。さらに、Cisco Secure Endpoint は Secure Client の新しいオプションモジュールであり、統合された高度な Endpoint Detection and Response（EDR）および Extended Detection and Response（XDR）機能をお客様に提供します。

新規のユーザーは従来通りの方法で Secure Client をインストールでき、新しいクラウド管理機能の導入を検討しているお客様は、パッケージ化されたインストーラーを Cisco Secure Endpoint ポータルからダウンロードしてインストールできます。

Device Insights を使用した SecureX によるクラウド管理は、Secure Client の新しいオプション機能です。この新機能により、Secure Client の展開、構成、および監視が簡単になります。お客様はクラウド管理を導入する必要がなく、現在のメカニズム、つまり Cisco Secure Firewall、ISE、ソフトウェア管理ツール（一例が SCCM）を使用して、または MSI を使用して直接的に、展開を継続できます。

クラウド管理用の新しい SecureX の画面とツールを以下に示します。

- Secure Client 用のネットワークインストーラのカスタマイズと生成
- Secure Client 用のカスタム VPN プロファイルの作成とダウンロード
- Device Insights との統合による、Secure Client がインストールされているエンドポイントのインベントリの監視および管理

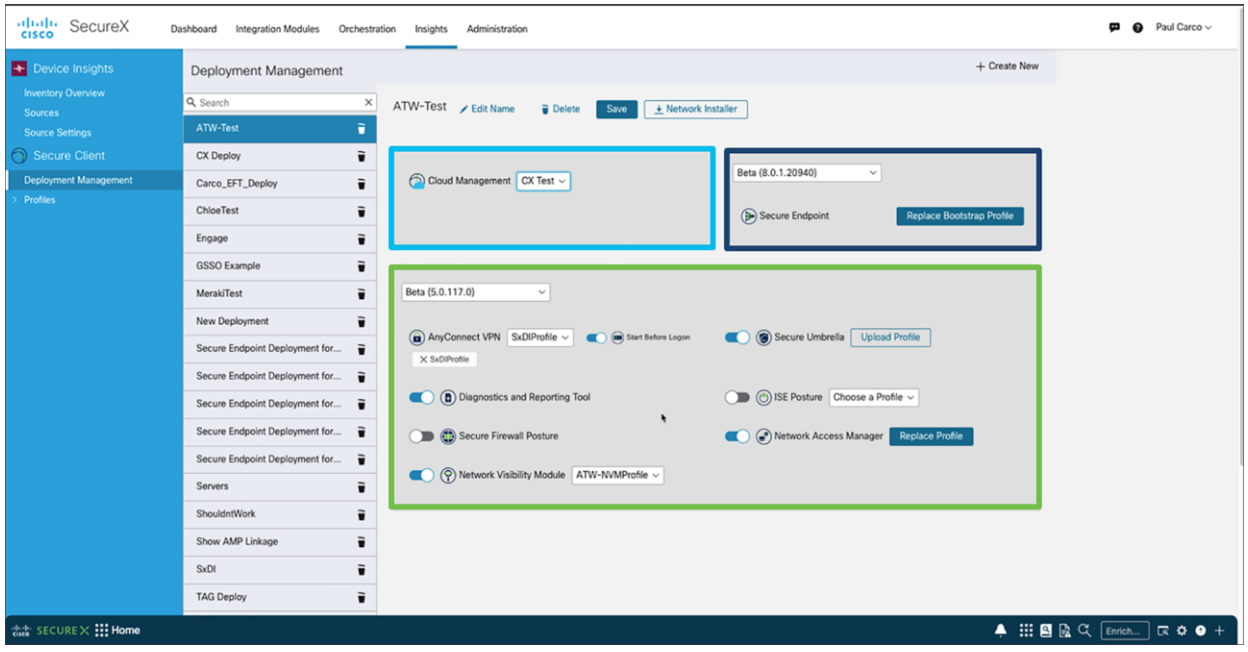


図 1.
クラウド管理

Cisco Secure Endpoint モジュール

Secure Client モジュール

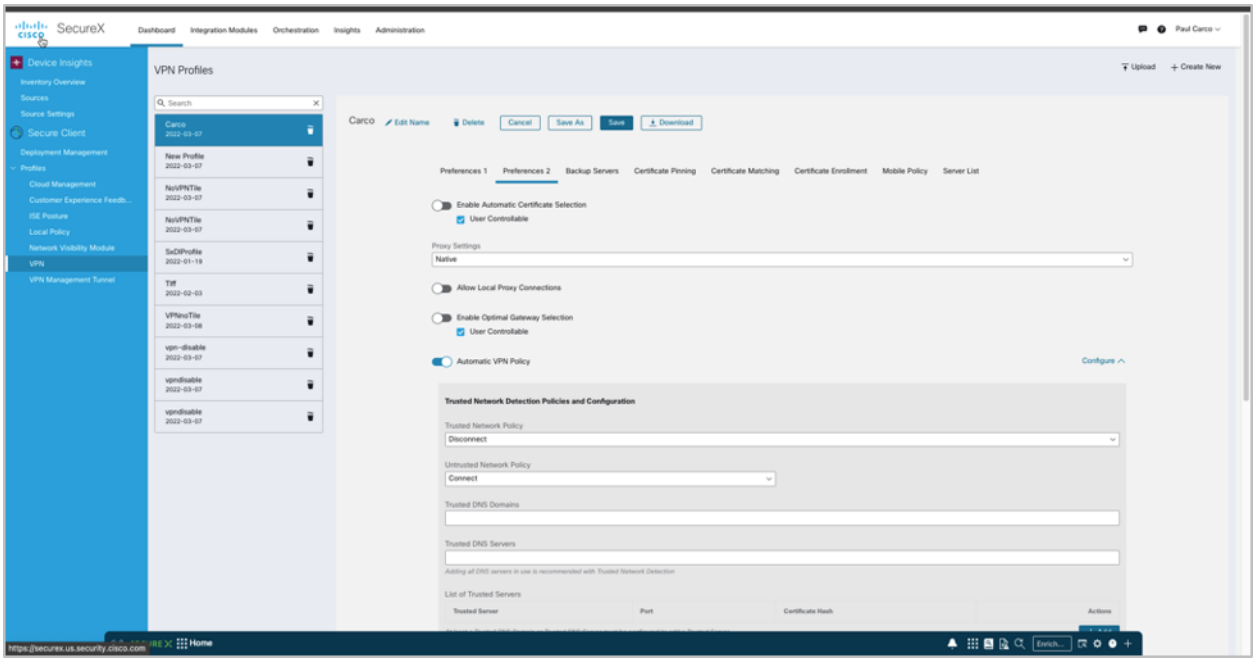


図 2.
VPN プロファイル

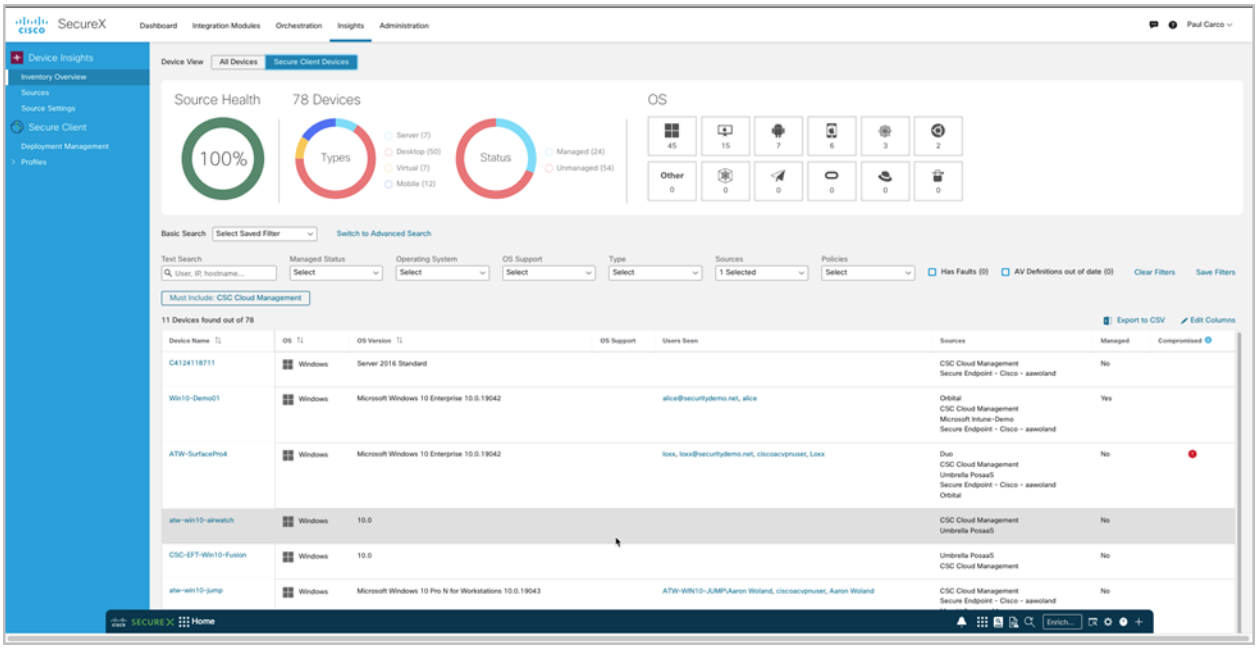


図 3.
Device Insights

モジュールと機能

AnyConnect VPN/ZTNA ユーザーおよび管理トンネル

Cisco Secure Client には、自動的に VPN セッションを接続、再接続、または切断するための多数のオプションが用意されています。これらのオプションは、ユーザーが VPN に接続するための便利な方法をもたらし、ネットワークセキュリティの要件をサポートします。常に有効なインテリジェント VPN は、AnyConnect クライアントデバイスが最適なネットワーク アクセス ポイントを自動的に選択し、そのトンネリングプロトコルを最も効率的な方法に適応させることに役立ちます。これには、遅延の影響を受けやすいトラフィック用の Datagram Transport Layer Security（DTLS）プロトコルや、ゼロトラスト ネットワーク アクセスに入るためのパスが含まれます。トンネリングサポートは、IP Security Internet Key Exchange バージョン 2（IPsec IKEv2）にも利用できます。一部のアプリケーションの VPN アクセスは、Apple iOS および Google Android に適用される場合があります。

管理 VPN トンネルは、エンドユーザーによって VPN 接続が確立されるときだけでなく、クライアントシステムの電源が入るたびに社内ネットワークへの接続を提供します。その結果、オフィス外のエンドポイント（特に、ユーザーが VPN 経由でオフィスネットワークに頻繁に接続しないデバイス）でパッチ管理を行うことができます。この機能には、社内ネットワークの接続を必要とするエンドポイント OS ログインスクリプトに対するメリットもあります。この機能のエンド ユーザー インターフェイスはありません。

Cisco Secure Endpoint

Windows 用 Cisco Secure Client で使用できる Cisco Secure Endpoint は、Cisco Secure Client 内のモジュールとして機能し、Cisco Secure Client ユーザーインターフェイスを介してアクセスできます。Cisco Secure Endpoint Cloud は、SecureX Cloud Management と同様に、Cisco Secure Client を Cisco Secure Endpoint とともに展開することもできます。この統合を利用することで、お客様は管理下にあるクライアントの数を減らすことができます。

クラウド管理モジュール

Cisco Secure Client 用の SecureX Cloud Management デプロイメントを使用すると、管理者は Cisco Secure Client のクラウド管理型デプロイメントを作成できます。デプロイメント構成により、軽量のブートストラッパをダウンロードするオプションが生成されます。このブートストラッパには、関連付けられたプロファイルを使用して、デプロイメントによって指定された Cisco Secure Client モジュールのクラウドに接続するため、エンドポイントが必要とする情報が含まれます。フルインストーラーも利用できます。いずれの場合も、管理者は、好みのソフトウェア方法を使用して、インストーラーをエンドポイントに配布できます。

ネットワーク可視性モジュール

Network Visibility Module は、価値の高いエンドポイントテレメトリを継続的に提供します。それにより、組織はネットワーク上のエンドポイントとユーザーの動作を確認できます。ユーザー、アプリケーション、デバイス、場所、接続先などの貴重なコンテキストとともに、オンプレミスとオフプレミス両方のエンドポイントからフローを収集します。このデータをキャッシュし、信頼できるネットワーク（オンプレミスまたは VPN 経由の企業ネットワーク）上にある Network Visibility Module コネクタに送信します。Network Visibility Module コレクタは、Internet Protocol Flow Information Export（IPFIX）データとオプションのフィルターを受信するサーバーであり、それらは Cisco Secure Network Analytics エンドポイントライセンス、Syslog、またはサードパーティのコレクタにエクスポートされます。Network Visibility Module コレクタは、nvzFlow プロトコル仕様に準拠する受信メッセージを処理します。

NVM がフロー情報を送信するのは、信頼できるネットワーク上に限られます。デフォルトでは、データは収集されません。データが収集されるのは、プロファイルでそのように設定されている場合のみです。エンドポイントが接続されている間は、データが継続して収集されます。非信頼ネットワーク上で収集が行われた場合、データはキャッシュされ、エンドポイントが信頼ネットワーク上に接続された際に送信されます。UI なし

Cisco Umbrella ローミング セキュリティ モジュール

Cisco Umbrella ローミング セキュリティ サービスを利用するには、Professional、Insights、Platform、または MSP パッケージのサブスクリプションが必要です。Cisco Umbrella ローミングセキュリティはアクティブな VPN がないときに DNS レイヤセキュリティを提供し、インテリジェントプロキシを追加します。さらに、Cisco Umbrella サブスクリプションでは、コンテンツフィルタリング、複数のポリシー、強力なレポート、機能ディレクトリの統合などが提供されます。サブスクリプションに関係なく、同じ Cisco Umbrella ローミング セキュリティ モジュールが使用されます。

ISE ポスチャモジュール

ISE ポスチャは、Cisco Secure Client 製品に追加のセキュリティコンポーネントとしてインストールできるモジュールです。エンドポイント ポスチャ アセスメントは、すべての必須要件を満たさず、非準拠と見なされたエンドポイントに対して実施します。その他のエンドポイントの許可ステータスは、ポスチャ不明または準拠（必須要件に合致）です。クライアントは、ヘッドエンドからポスチャ要件ポリシーを受信し、ポスチャデータを収集し、結果をポリシーと比較し、評価結果をヘッドエンドに返します。エンドポイントが準拠しているかどうかは ISE が判断しますが、それは Cisco Secure Endpoint によるポリシーの評価に依存しています。

Network Access Manager

Network Access Managerは、セキュアなアクセスに必要なユーザおよびデバイス アイデンティティならびにネットワーク アクセス プロトコルを管理します。管理者定義のポリシーに違反する接続をエンドユーザーが確立しないように、インテリジェントに動作します。最適なレイヤ 2 アクセスネットワークを検出して選択し、有線ネットワークとワイヤレスネットワークの両方へのアクセスに対してデバイス認証を実行します。

ポスチャ（Cisco Secure Firewall 用）

Cisco Secure Firewall ポスチャはサーバ側評価を実行します。Cisco Secure Firewall がエンドポイント属性（オペレーティングシステム、IP アドレス、レジストリエントリ、ローカル証明書、ファイル名など）のリストのみを要求し、これらが Cisco Secure Firewall によって返されます。ポリシーの評価結果に基づいて、どのホストがセキュリティアプライアンスへのリモートアクセス接続を確立できるかを制御できます。

機能	利点と詳細
リモートアクセス VPN/ZTNA	
幅広いオペレーティングシステムのサポート	Windows 11（64 ビット）、現在 Microsoft がサポートしているバージョンの Windows 10 x86（32 ビット）と x64（64 ビット）、および Windows 8 ARM64 ベース用に Microsoft がサポートしているバージョンの Windows 11 ARM64 ベースの PC 用に Microsoft がサポートしているバージョンの Windows 10 **注：Cisco Secure Client 5.0 は Windows 10/11 のみです。**AnyConnect は、上記のすべてをサポートします。 macOS 12、11.2、10.15、および 10.14（すべて 64 ビット）

機能	利点と詳細
	Red Hat Ubuntu SUSE（SLES） モバイル OS のサポートについては、モバイルデータシートを参照してください。

機能	利点と詳細
ソフトウェアアクセス	Cisco.com の Software Center からダウンロード可能 AnyConnect 用のテクニカルサポートおよびソフトウェア使用許可は、期間ベースのすべての Plus および Apex ライセンスに含まれており、Plus の永続ライセンスとは別に購入可能 契約番号は Cisco.com ID にリンクされている必要があります。詳細は「Secure Client 発注ガイド」を参照してください
最適化されたネットワークアクセス：VPN プロトコルが選択する SSL（TLS と DTLS）、IPsec IKEv2	AnyConnect で VPN プロトコルを選択できるため、管理者はビジネスニーズに最適なプロトコルを使用可能 SSL（TLS 1.2 と DTLS 1.2）および次世代 IPsec IKEv2 などのトンネリングサポート DTLS を使用して、VoIP トラフィックや TCP ベースのアプリケーションアクセスなど、遅延の影響を受けやすいトラフィックの接続を最適化 TLS 1.2（HTTP over TLS / SSL）を使用して、ロックダウンされた環境（Web プロキシサーバーを使用する環境などを含む）からのネットワーク接続の可用性を確保 セキュリティポリシーで IPsec を使用する必要がある場合に、IPsec IKEv2 を使用して、遅延の影響を受けやすいトラフィックの接続を最適化
最適ゲートウェイ選択	最適なネットワークアクセス ポイントが特定され接続が確立されるため、エンドユーザーによる最寄りのロケーションの特定が不要
モビリティ機能	モバイルユーザーに適した設計 IP アドレスが変更されたとき、接続が失われたとき、またはデバイスが休止状態やスタンバイ状態になったときにも、VPN 接続が維持されるように設定可能 信頼ネットワーク検出機能により、エンドユーザーがオフィスにいる間は VPN 接続を自動的に切断し、ユーザーが遠隔地にいる場合には接続することが可能
暗号化	TLS/DTLS 1.2 の強力な暗号をサポート NSA Suite B アルゴリズム、IKEv2 を使用した ESPv3、4096 ビットの RSA キー、Diffie-Hellman グループ 24 および強化された SHA2（SHA-256 および SHA-384）などの次世代暗号化。IPsec IKEv2 接続にのみ適用。Premier（旧 AnyConnect Apex）が必要です
多様な展開オプション	**展開オプション：** 事前展開：新規インストールとアップグレードは、エンドユーザーによって、または社内のソフトウェア管理システム（SMS）を使用して実行されます。 Web 展開： Cisco Secure Client パッケージは、ヘッドエンド（Secure Firewall ASA、Secure Firewall Threat Defense、または ISE サーバー）にロードされます。ユーザーがファイアウォールまたは ISE に接続すると、Cisco Secure Client がクライアントに展開されます。 SecureX クラウド管理展開：Cisco Secure Client 5.0 は、カスタマイズ可能なデプロイメントを使用してクラウドから展開できます。

機能	利点と詳細
多様な認証オプション	**プロトコル：** 組み込みまたはネイティブブラウザ（SSO）を使用した SAML 2.0 RADIUS LDAP 証明書。 TACACS+ HTTP Form SDI Kerberos **ヘッドエンド方式** AAA AAA と証明書 証明書のみ SAML 複数の証明書と AAA
一貫したユーザーエクスペリエンス	LAN と同様の安定したユーザーエクスペリエンスを必要とするリモートアクセスユーザーを、完全トンネルクライアントモードでサポート 複数の配信方式で、AnyConnect の幅広い互換性を実現 管理者によって設定されている場合、ユーザーはクライアントソフトウェアの更新を延期することが可能 カスタマーエクスペリエンスのフィードバックオプション
ポリシーの制御および管理の一元化	ポリシーを事前に設定またはローカルで設定し、VPN セキュリティゲートウェイから自動更新することが可能 AnyConnect 用の API によって、Web ページまたはアプリケーションからの導入が容易 信頼できない証明書に対して確認を行い、ユーザー警告を発行 Cisco Secure Client は SecureX プラットフォームを使用した展開と管理をサポート
高度な IP ネットワーク接続	IPv4 および IPv6 ネットワークとのパブリック接続 内部の IPv4 および IPv6 ネットワークリソースにアクセス可能 管理者が制御するスプリットトンネリング（ネットワークと動的（ドメイン）およびフル トンネル ネットワーク アクセス ポリシー ダイナミック アクセス ポリシーまたはアイデンティティ サービス エンジンを使用したアクセス コントロール ポリシー Apple iOS および Google Android 用のアプリごとの VPN ポリシー **IP アドレス割り当てメカニズム：** 静的 内部プール Dynamic Host Configuration Protocol（DHCP） RADIUS/Lightweight Directory Access Protocol（LDAP）

機能	利点と詳細
堅牢な統合エンドポイント コンプライアンス **（Premier 旧 Apex ライセンスが必要）**	有線環境とワイヤレス環境でエンドポイントポスチャの評価と修復をサポート（Cisco Identity Services Engine NAC エージェントと置き換え）。Identity Services Engine（ISE）1.3 以降と Identity Services Engine Apex ライセンスが必要 ISE ポスチャ（ISE と連動）およびホストスキャン（VPN のみ）は、ネットワークアクセスを許可する前に、マルウェア対策ソフトウェアの存在、Windows サービスパック/パッチ適用状態、およびエンドポイントシステム上のその他のソフトウェアサービスの範囲を検出しようとします。 管理者は実行中のプロセスの情報に基づいて、独自のポスチャチェックも定義可能 ISE ポスチャとホストスキャンは、リモートシステムにウォーターマークが存在することも検出します。ウォーターマークを使用して企業が所有する資産を識別できるため、これによって異なるアクセスを提供できます。ウォーターマークチェック機能には、システムレジストリ値、必要な CRC32 チェックサムに一致するファイルの存在、およびその他のさまざまな機能が含まれます。コンプライアンス違反のアプリケーション向けに追加機能がサポートされます。
クライアント ファイアウォール ポリシー	スプリットトンネリング設定用に追加の保護を提供 ローカルアクセスの例外を許可するために AnyConnect および Cisco Secure クライアントと共に使用（印刷用、テザリングされたデバイスのサポートなど） ポートベースのルール（IPv4 の場合）、ネットワークおよび IP アクセス制御リスト（ACL）（IPv6 の場合）をサポート Windows および Mac OS X プラットフォームで使用可能
ローカリゼーション	**英語に加えて、以下の言語に翻訳** cs-CZ チェコ語（チェコ共和国） de-DE ドイツ語（ドイツ） es-ES スペイン語（スペイン） fr-CA フランス語（カナダ） fr-FR フランス語（フランス） hu-HU ハンガリー語（ハンガリー） it_IT イタリア語（イタリア） ja-JP 日本語（日本） ko-KR 韓国語（韓国） nl-NL オランダ語（オランダ） pl-PL ポーランド語（ポーランド） pt-BR ポルトガル語（ブラジル） ru-RU ロシア語（ロシア） zh-CN 中国語（中国） zh-HANS 中国語（簡体字） zh-HANT 中国語（繁体字） zh-TW 中国語（台湾）

機能	利点と詳細
簡単なクライアント管理	管理者はヘッドエンド セキュリティ アプライアンスからソフトウェアおよびポリシーの更新を自動的に配信できるため、クライアントソフトウェアの更新に伴う管理作業が不要です。Cisco Secure Client 5.0 には、管理者が SecureX Cloud からクライアントを展開および管理する機能もあります。 管理者はエンドユーザーが利用可能な設定機能を指定可能 ドメインログインスクリプトを利用できない場合に、管理者は接続および切断時のエンドポイントスクリプトをトリガーすることが可能 管理者は、エンドユーザーに表示されるメッセージを完全にカスタマイズまたはローカライズ可能
プロファイル エディタ	AnyConnect ポリシーを Cisco Adaptive Security Device Manager（ASDM）から直接カスタマイズ可能 スタンドアロン プロファイル エディタ SecureX Cisco Secure Client プロファイルページ
診断	デバイスごとの統計情報およびロギング情報が利用可能 ログはデバイスで表示可能 シスコや管理者に分析用として電子メールでログを簡単に送信可能
米国連邦情報処理標準（FIPS）	FIPS 140-2 Level 2 に準拠（プラットフォーム、機能、バージョンに関する制限が適用されます）
セキュアなモビリティとネットワークの可視性	
Cisco Umbrella Roaming（Cisco Umbrella Roaming ライセンスが必要）	Umbrella ローミング セキュリティ モジュールには、Professional、Insights、Platform、MSP のいずれかのパッケージでの Umbrella ローミング セキュリティ サービスのサブスクリプションが必要です。Umbrella ローミングセキュリティはアクティブな VPN がないときに DNS レイヤセキュリティを提供し、Cisco Umbrella サブスクリプションはインテリジェントプロキシを追加します。さらに、Cisco Umbrella サブスクリプションはコンテンツ フィルタリング、複数ポリシー、強力なレポート、Active Directory の統合などの機能を提供します。サブスクリプションに関係なく、同じ Umbrella ローミング セキュリティ モジュールが使用されます。 • VPN がオフの場合にローミングデバイスのセキュリティを適用 • ローミングデバイスでマルウェア、フィッシング、および C2 コールバックを自動的にブロック • どこにいてもデバイスを保護する最もシンプルな方法 VPN がオフの場合、またはスプリットトンネルを使用している場合（トンネル外部の通信に適用）、エンドポイント リダイレクションを使用して DNS ベースのセキュリティを適用します。
Network Visibility module（Premier 旧 Apex ライセンスが必要）	豊富なユーザー、エンドポイント、アプリケーション、ロケーション、および接続先コンテキストを使用したエンドポイントフローのキャプチャ オンプレミスとオフプレミスの柔軟な収集設定 アプリケーションの使用状況を監視することで、潜在的な動作異常を発見 より多くの情報に基づいたネットワーク設計の決定が可能 Cisco Network Analytics などの NetFlow 分析ツールと使用状況データを共有可能

機能	利点と詳細
Cisco Secure Endpoint（旧 Advanced Malware Protection（AMP）for Endpoints） **（Cisco Secure Endpoint には別のライセンスが付与されます）**	Cisco Secure Client は、AnyConnect VPN/ZTNA と Cisco Secure Endpoint の両方の機能を統合 エンドポイント脅威防御サービスをリモートエンドポイントに拡張して、エンドポイントの脅威防御範囲を増大 よりプロアクティブな保護機能を提供して、リモートエンドポイントで攻撃をさらに確実かつ迅速に軽減 macOS エンドポイントは、スタンドアロンの Secure Endpoint クライアントを引き続き使用できる
Network Access Manager および 802.1X	
メディアサポート	• イーサネット（IEEE 802.3） • Wi-Fi（IEEE 802.11）
ネットワーク認証	• IEEE 802.1X-2001、802.1X-2004、および 802.1X-2010 • 単一の 802.1X 認証フレームワークを導入して、有線ネットワークとワイヤレスネットワークの両方にアクセスすることが可能 • きわめてセキュアなアクセスに必要な、ユーザーとデバイスのアイデンティティおよびネットワーク アクセス プロトコルを管理 • シスコの有線およびワイヤレス統合ネットワークに接続する場合のユーザーエクスペリエンスを最適化
拡張認証プロトコル（EAP）方式	• EAP-Transport Layer Security（TLS） • EAP-Protected Extensible Authentication Protocol（PEAP）（内部で以下の方式を利用） • EAP-TLS • EAP-MSCHAPv2 • EAP-Generic Token Card（GTC） • EAP-Flexible Authentication via Secure Tunneling（FAST）（内部で以下の方式を利用） • EAP-TLS • EAP-MSCHAPv2 • EAP-GTC • EAP-Tunneled TLS（TTLS）（内部で以下の方式を利用） • Password Authentication Protocol（PAP） • Challenge Handshake Authentication Protocol（CHAP） • Microsoft CHAP（MS-CHAP） • MSCHAPv2 • EAP-MD5 • EAP-MSCHAPv2 • Lightweight EAP（LEAP）、Wi-Fi のみ • EAP-Message Digest 5（MD5）、管理設定済み、イーサネットのみ • EAP-MSCHAPv2、管理設定済み、イーサネットのみ • EAP-GTC、管理設定済み、イーサネットのみ
ワイヤレス暗号化方式（対応する 802.11 NIC のサポートが必要）	• オープン（Open） • Wired Equivalent Privacy（WEP） • 動的 WEP • Wi-Fi Protected Access（WPA）Enterprise • WPA2 Enterprise • WPA Personal（WPA-PSK） • WPA2 Personal（WPA2-PSK）

機能	利点と詳細
ワイヤレス暗号化プロトコル	Advanced Encryption Standard（AES）アルゴリズムを使用する CBC-MAC（Cipher Block Chaining Message Authentication Code Protocol）プロトコルによるカウンタモード
セッション再開	EAP-TLS、EAP-FAST、EAP-PEAP、および EAP-TTLS を使用する RFC2716（EAP-TLS）によるセッション再開 EAP-FAST によるステートレスなセッション再開
イーサネット暗号化	メディアアクセス制御：IEEE 802.1AE（MACsec） キー管理：MACsec Key Agreement（MKA） 有線イーサネットネットワークのセキュリティ インフラストラクチャを定義し、データの機密性と整合性を確保して発信元の認証を実行 ネットワークの信頼済みコンポーネント間の通信を保護
一度に 1 つの接続 **（ネットワーク アクセス マネージャを使用する Windows のみ）**	ネットワークに対して 1 つの接続のみを許可し、その他をすべて切断 アダプタ間のブリッジングなし イーサネット接続を自動的に優先
複雑なサーバー検証	「次で終わる」ルールと「完全一致」ルールをサポート 名前に共通点のないサーバーに対して 30 以上のルールをサポート
EAP-Chaining（EAP-FASTv2）	企業および企業以外の資産に基づいてアクセスを区別 単一の EAP トランザクションでユーザーとデバイスを検証
Enterprise Connection Enforcement（ECE）	ユーザーによる適切な企業ネットワークのみへのアクセスを保証 ユーザーのサードパーティ アクセス ポイントへの接続によるオフィス内でのネットサーフィンを防止 ユーザーによるゲスト ネットワークへのアクセスの確立を防止 手間のかかるブロックリストを排除
次世代暗号化（スイート B）	最新の暗号化標準をサポート： 楕円曲線 Diffie-Hellman 鍵交換 楕円曲線デジタル署名アルゴリズム（ECDSA）証明書
クレデンシャルタイプ	• インタラクティブなユーザーパスワードまたは Windows パスワード • RSA SecurID トークン • ワンタイムパスワード（OTP）トークン • スマートカード（Axalto、Gemplus、SafeNet iKey、Alladin） • X.509 証明書 • 楕円曲線デジタル署名アルゴリズム（ECDSA）証明書

プラットフォームの互換性

Secure Client は、さまざまな Cisco Secure Firewall、Meraki デバイス、Cisco Secure Connect Choice、および Cisco Secure Connect Flex と互換性があります。最新のアプライアンス ソフトウェア リリースを導入することをお勧めします。

互換性に関するその他の情報については、https://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html を参照してください。

ライセンスオプション

Secure Client Advantage、Premium、または VPN のみのライセンスが必要です。AnyConnect Plus、Apex、または VPN のみの有効なライセンスをお持ちのお客様は、Cisco Secure Client を利用できます。

ライセンスオプションと購入案内については、発注ガイド
https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/secure-client-og.html から確認できます。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

詳細情報

- Cisco Secure Client のホームページ：https://www.cisco.com/go/secureclient
- Cisco Secure Client（旧称 AnyConnect）のドキュメント：https://www.cisco.com/c/ja_jp/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html
- モバイルプラットフォーム向け Cisco Secure Client（旧称 AnyConnect）のデータシート：https://www.cisco.com/c/ja_jp/products/collateral/security/anyconnect-secure-mobility-client/data_sheet_c78-527494.html
- Cisco ASA 5500-X シリーズ Adaptive Security アプライアンス：https://www.cisco.com/c/ja_jp/products/security/asa-firepower-services/index.html
- Cisco Secure Endpoint：https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoints/index.html
- Cisco Secure Client（旧称 AnyConnect）- ライセンス契約書およびプライバシーポリシー：https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html

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

0314-2022-000-X