Cisco AnyConnect セキュア モビリティ クライアント

2020 年 12 月

目次

使いやすさと、高い安全性。それが Cisco AnyConnect® セキュア モビリティ クライアントが世界中で人気を集めている理由です。またお客様は、AnyConnect が新しいリリースのたびに、さまざまなデスクトップデバイスやモバイルデバイスに対応する、より強力なリモートアクセスを取り入れていることを理解しています。

製品の概要

モバイルワーカーはさまざまな場所に移動するので、AnyConnect クライアントデバイスは、常時利用可能なインテリジェント VPN を通じて、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ます。遅延の影響を受けやすいトラフィックのための Voice over IP（VoIP）トラフィック、TCP ベースのアプリケーションアクセス、または Datagram Transport Layer Security（DTLS）プロトコルなどがそれに含まれます。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。選択されたアプリケーション VPN アクセスは、Release 4.x のアプリごとの VPN 機能を使用して、Apple iOS、Google Android（5.0 以降）および Samsung KNOX で実行できます。

AnyConnect 4.x は、堅牢な統合エンドポイント コンプライアンスをサポートしています。また、エンドポイントのセキュリティポスチャに基づいて、Cisco Adaptive Security アプライアンスで終端する VPN アクセスを制限することによって、企業ネットワークの整合性を保護します。有線環境とワイヤレス環境にまたがるエンドポイントポスチャの評価と修復によって、各種アンチウィルス、パーソナルファイアウォール、アンチスパイウェア製品の状態を検証します。コンプライアンス違反のエンドポイント エンフォースメントには、アクセスを許可する前に修正したり、追加のシステムチェックを実装するためのオプションがあります。

AnyConnect セキュア モビリティ ソリューションには、リモートアクセスに加えて、Web セキュリティ、マルウェア脅威防御、フィッシング保護、およびコマンドとコントロールのコールバックブロッキング機能が内蔵され、包括的でセキュアなエンタープライズ モビリティ ソリューションを実現します。Web セキュリティでは、構内ベースの Cisco Secure Web Appliance またはクラウドベースの Cisco クラウド Web セキュリティを選択して、企業リソースおよびクラウド保護サービスへの従業員のアクセスの信頼性とセキュリティを高めます。VPN がオフの場合の保護を提供する、Cisco Umbrella ローミングは、マルウェア、フィッシング、およびコマンドとコントロールのコールバックからデバイスをどこでも保護する、クラウド提供のセキュリティサービスです。

Windows、macOS、Linux、Samsung モバイルデバイスで Network Visibility Module を使用すると、管理者はエンドポイント アプリケーションの使用状況をモニターして、潜在的な動作の異常を発見し、より多くの情報に基づいてネットワーク設計を決定できます。使用状況データは、Cisco Secure Network Analytics などの NetFlow 分析ツールと共有できます。

AnyConnect では Cisco Secure Endpoint イネーブラにより、Cisco Secure Endpoint の導入もサポートされます。この機能は、VPN 対応エンドポイントや、AnyConnect サービスが（802.1X ネットワークアクセス、ポスチャなどに）使用されているあらゆる場所に、エンドポイント脅威保護を大幅に拡張します。そして、エンタープライズ接続ホストからの攻撃の可能性をさらに低下させます。Secure Endpoint は、AnyConnect とは別にライセンスが提供されます。

AnyConnect モビリティクライアントは、業界をリードする VPN 機能に加えて IEEE 802.1X 機能に対応しており、有線ネットワークからワイヤレスネットワークへのスムーズな移行に必要なユーザーとデバイスのアイデンティティ、ならびにネットワークアクセス プロトコルを管理する、単一の認証フレームワークを提供します。

このソリューションは、VPN 機能のサポートとともに、有線ネットワークにおけるデータの機密性と整合性の確保および発信元の認証用に IEEE 802.1AE（MACsec）をサポートし、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します。

図 1 に、Microsoft Windows の VPN 設定を示します。

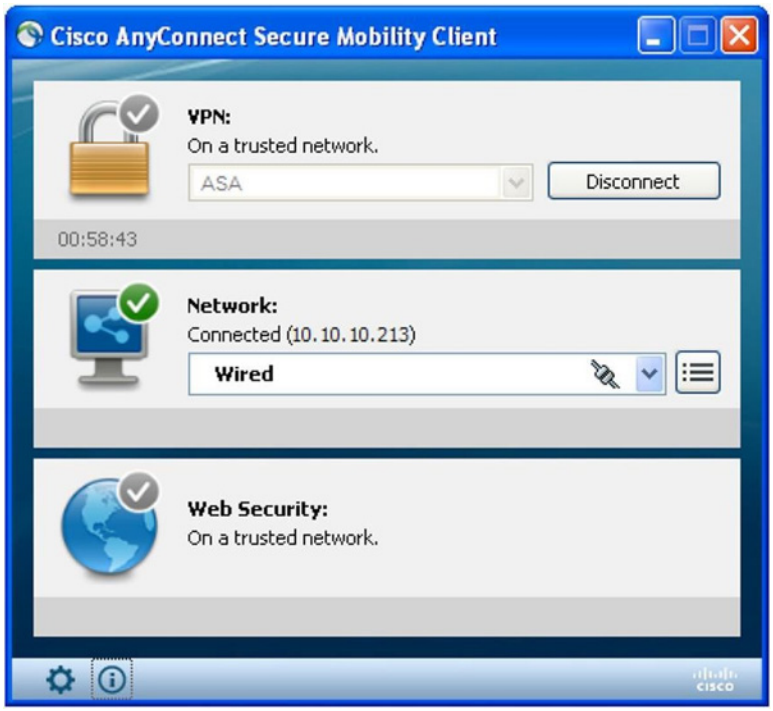

図 1.
Microsoft Windows でのアイコンと VPN 設定例

図 2 に、Apple OS X の VPN 設定を示します。

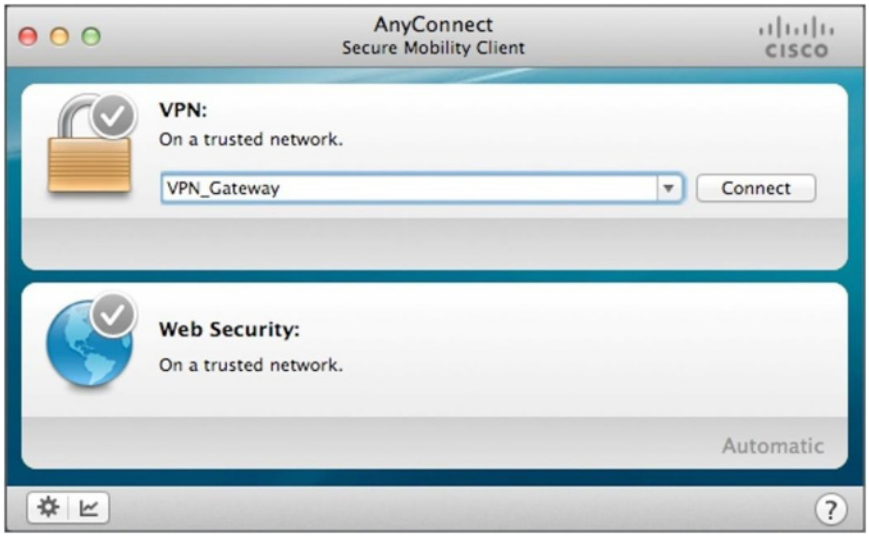

図 2.
Apple OS X でのアイコンと VPN 設定例

クライアントモジュール

AnyConnect クライアントは、軽量でモジュール化されたセキュリティクライアントで、個別のビジネスニーズに基づいてカスタマイズできます。VPN、802.1X、コンプライアンスチェック、ネットワークの可視性、Cisco Umbrella ローミング、クラウド Web セキュリティとの統合などの機能と、Secure Endpoint をインストールまたはアンインストールする機能は、個別に導入できるモジュールまたはサービスとして利用可能で、組織は接続ニーズに最適な機能を選択できます。このため、俊敏性と運用効率が維持され、組織は AnyConnect の柔軟性と利点を最大限に活用できます。

図 3 に、有線環境とワイヤレス環境にまたがる AnyConnect 統合エンドポイント コンプライアンスを示します。

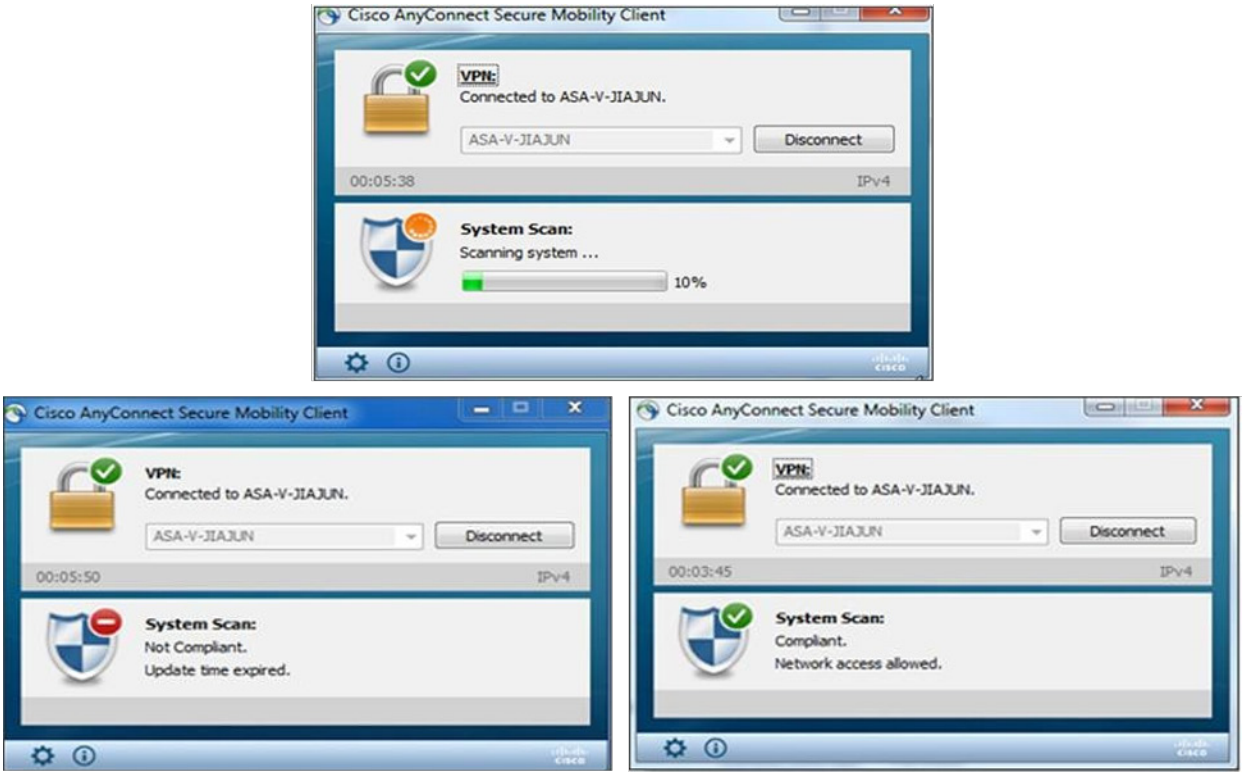

図 3.
エンドポイント コンプライアンス チェック

機能とメリット

表 1 に、Cisco AnyConnect セキュア モビリティ クライアントの機能と利点を示します。

表 1. 機能とメリット

機能	利点と詳細
リモートアクセス VPN	
幅広いオペレーティングシステムのサポート	• Windows 10、8.1、8、7 • Mac OS X 10.8 以降 • Linux Intel（x64）

機能	利点と詳細
	モバイルプラットフォームの情報については、AnyConnect Mobile のデータシートを参照してください。
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 AnyConnect 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）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	• AES-256 および 3DES-168 を含む強力な暗号化をサポート（セキュリティ ゲートウェイ デバイスで強力な暗号化ライセンスが有効になっている必要があります）。 • 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。AnyConnect Apex ライセンスが必要
多様な導入および接続オプション	**展開オプション：** • Microsoft Installer などによる事前導入 • ActiveX（Windows のみ）および Java によるセキュリティゲートウェイの自動導入（初期インストールには管理権限が必要） **接続モード：** • システムアイコンごとのスタンドアロン • ステルスエージェント • テンポラルエージェント • ブラウザからの接続（Web 起動） • ポータルからのクライアントレス接続 • CLI からの接続 • API からの接続
多様な認証オプション	• RADIUS • NT LAN Manager（NTLM）のパスワード期限切れ機能（MSCHAPv2）をサポートする RADIUS • RADIUS ワンタイムパスワード（OTP）のサポート（State 属性および Reply-Message 属性） • RSA SecurID（SoftID の統合を含む）

機能	利点と詳細
	• Active Directory または Kerberos • 組み込みの認証局（CA） • デジタル証明書またはスマートカード（マシン証明書のサポートを含む）、自動選択またはユーザーによる選択が可能 • パスワード期限切れ機能とエージング機能をサポートする Lightweight Directory Access Protocol（LDAP） • 汎用 LDAP サポート • 証明書とユーザー名/パスワードを組み合わせた多因子認証（二重認証）
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 • プッシュされた更新の保留が可能 • 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 • 証明書の表示と管理をローカルで実行可能
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およびオールトンネリング ネットワーク アクセス ポリシー • アクセス コントロール ポリシー • Apple iOS、Google Android、および Samsung Knox 用の Per-App VPN ポリシー（Release 4.0 の新機能：OS 9.3 以降の Cisco ASA 5500-X と AnyConnect 4.0 のライセンスが必要） **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）
堅牢な統合エンドポイント コンプライアンス **（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。 • 機能はオペレーティングシステムによって異なります。詳細については、ホストスキャンサポートのチャートを参照してください。
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 クライアントと共に使用（印刷用、係留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 のアクセス コントロール 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

機能	利点と詳細
ローカリゼーション	**英語に加えて、以下の言語に翻訳** • チェコ語（cs-cz） • ドイツ語（de-de） • スペイン語（es-es） • フランス語（fr-fr） • 日本語（ja-jp） • 韓国語（ko-kr） • ポーランド語（pl-pl） • 簡体字中国語（zh-cn） • 中国語（台湾）（zh-tw） • オランダ語（nl-nl） • ハンガリー語（hu-hu） • イタリア語（it-it） • ポルトガル語（ブラジル）（pt-br） • ロシア語（ru-ru）
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 • 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
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	
Web セキュリティとの統合 （クラウド Web セキュリティのライセンスが必要）	• Software as a Service（SaaS）Web セキュリティの世界最大のプロバイダーであるクラウド Web セキュリティを使用して、マルウェアを企業ネットワークから遠ざけ、従業員による Web 利用を管理および保護 • クラウドにホスティングされている設定と動的ロードのサポート • 構内ベースのサービスに加えて、クラウドベースのサービスのサポートによる柔軟性と幅広い選択肢の提供 • Web セキュリティアプライアンスと統合 • 信頼ネットワーク検出のサポート • ユーザーのロケーションに関係なく、すべてのトランザクションにセキュリティポリシーを適用 • ネットワーク接続を許可、またはアクセス不能な場合は拒否するポリシーを備えた、常時接続可能できわめてセキュアなネットワーク接続が必要 • ホットスポットとキャプティブポータルを検出
Cisco Umbrella Roaming （Cisco Umbrella Roaming ライセンスが必要）	• 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

機能	利点と詳細
ネットワーク可視性モジュール（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
Advanced Malware Protection（AMP）for Endpoints イネーブラ（AMP for Endpoints は別ライセンス）	• Secure Endpoint の配信と有効化によって、AnyConnect のエンドポイントに対する脅威防御サービスの実施をシンプル化 • 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
幅広いオペレーティングシステムのサポート	• Windows 10、8.1、8、7 • Mac OS X 10.8 以降 • モバイルプラットフォームの情報については、AnyConnect Mobile のデータシートを参照してください。
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

機能	利点と詳細
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） • CCKM（Cisco CB21AG ワイヤレス NIC が必要）
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 • Rivest Cipher 4（RC4）ストリーム暗号を使用する Temporal Key Integrity Protocol（TKIP）
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 • PMK-ID キャッシュ（Proactive Key Caching または Opportunistic Key Caching）、Windows XP のみ
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
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

機能	利点と詳細
	• 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
リモートデスクトップのサポート	• Remote Desktop Protocol（RDP）を使用する場合、ローカルネットワークに対するリモートユーザーの資格情報を認証

プラットフォームの互換性

AnyConnect は、Cisco ASA ソフトウェアリリース 8.0(4) 以降を実行するすべての Cisco ASA 5500-X シリーズ次世代ファイアウォールおよび 5500 シリーズ エンタープライズ ファイアウォール エディション モデル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。

一部の機能には、上記以降の Cisco ASA ソフトウェアリリースまたは ASA 5500-X モデルが必要です。

シスコは、特定の機能に限定されたセキュリティゲートウェイとして機能する、Cisco IOS® Release 15.1(2)T 以降への AnyConnect VPN アクセスをサポートします。詳細については、Cisco IOS SSL VPN でサポートされていない機能 [英語] をご覧ください。

その他の Cisco IOS 機能のサポート情報については、https://www.cisco.com/go/fn を参照してください。

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

AnyConnect 4.x 以降には、AnyConnect Plus または Apex ライセンスが必要です。

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/dam/en/us/products/security/anyconnect-og.pdf 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 AnyConnect セキュア モビリティ クライアントのホームページ：https://www.cisco.com/jp/go/anyconnect
- Cisco AnyConnect 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 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/jp/go/asa
- Cisco クラウド Web セキュリティ：https://www.cisco.com/jp/go/cws
- Cisco Secure Endpoint：https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoint/index.html
- Cisco AnyConnect セキュア モビリティ クライアント - 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

0524-2022-000-X