Cisco AnyConnect セキュア モビリティ クライアントのデータ シート

製品の概要

使いやすさと 強固なセキュリティ—— 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より強力なリモートアクセス テクノロジーを取り入れ、広範な PC やモバイル デバイスに対応していることを理解しています。モバイル ワーカーはさまざまな場所に移動するので、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。その中には、遅延の影響を受けやすいトラフィック、Voice over IP（VoIP）トラフィック、または TCP ベースのアプリケーション アクセス用の Datagram Transport Layer Security（DTLS）プロトコルが含まれる場合があります。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 Per-App VPN 機能を使用して、Google Android（Lollipop）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。

Cisco AnyConnect セキュア モビリティ ソリューションは、組み込みの Web セキュリティおよびマルウェア脅威防御機能を備えています。構内ベースの Cisco Web セキュリティ アプライアンス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、企業リソースへの従業員のアクセスの信頼性とセキュリティを高めることができます。Web セキュリティ、マルウェア脅威防御、リモート アクセスを統合して、包括的でセキュアなエンタープライズ モビリティ ソリューションにします。一貫性のあるコンテキスト認識型セキュリティ ポリシーを採用しているため、生産性の高い保護された作業環境が維持されます。

Release 4.1 とその Cisco Advanced Malware Protection（AMP）Enabler によって、AnyConnect は Cisco Advanced Malware Protection for Endpoints の導入を支援できるようになりました。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。Cisco AMP for Endpoints は、AnyConnect とは別にライセンスされます。

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とデバイスのアイデンティティ、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 のサンプル VPN 設定を示します。

図 1. アイコンと Microsoft Windows のサンプル VPN 設定

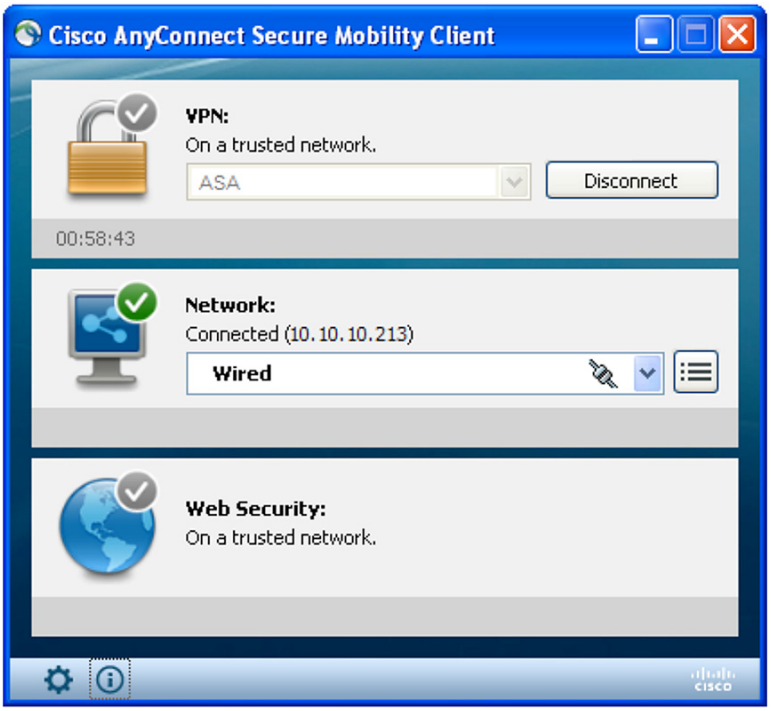
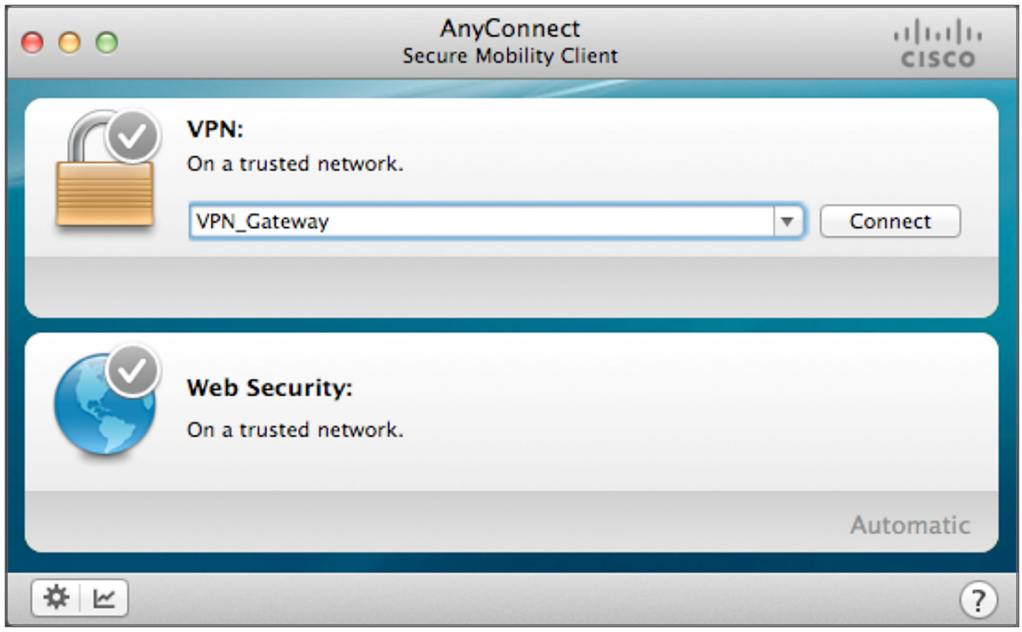


図 2 に、Apple OS X のサンプル VPN 設定を示します。

図 2. アイコンと Apple OS X のサンプル VPN 設定

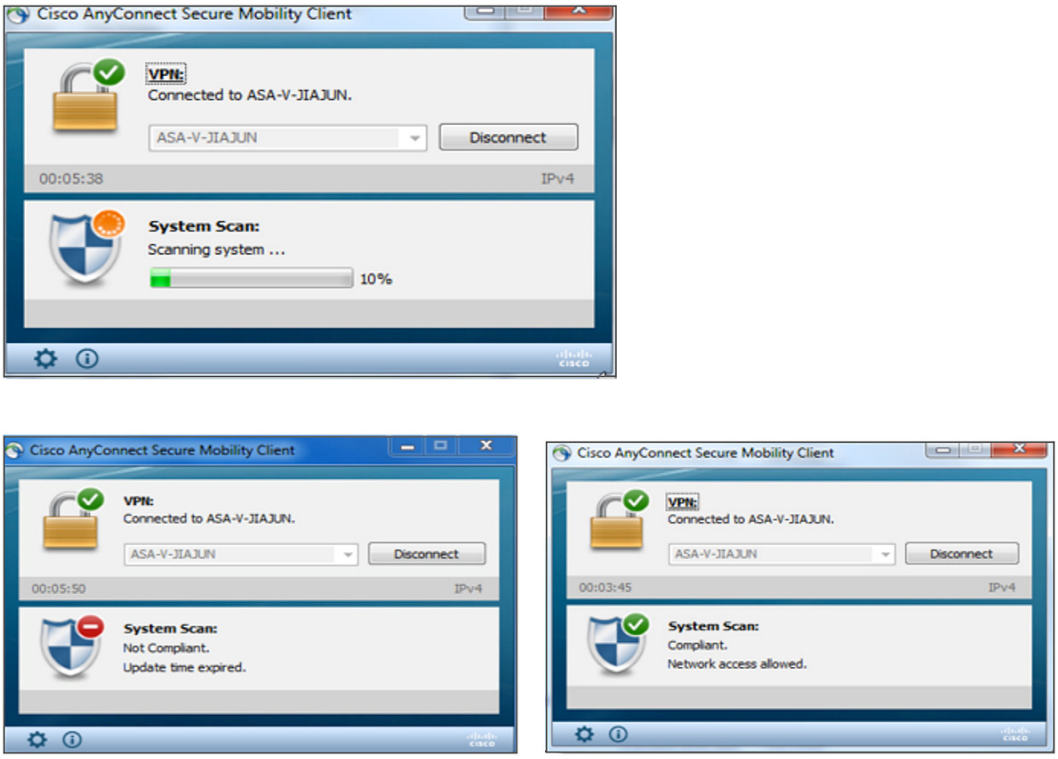


クライアント モジュール

AnyConnect クライアントは、軽量で高度に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 ニーズに基づいて容易に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、Cisco クラウド Web セキュリティとの統合などの機能と、AMP for Endpoints 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



機能と利点

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. 機能と利点

機能	利点と詳細
リモート アクセス仮想プライベート ネットワーク	
幅広いオペレーティング システムのサポート	• Windows 8 および 8.1 • Windows 7 32 ビット（x86）および 64 ビット（x64） • Mac OS X 10.8 以降 • Linux Intel（x64）
ソフトウェアの提供方法	• Cisco.com のソフトウェア センターで入手可能 • 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

機能	利点と詳細
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、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（Internet Key Exchange バージョン 2）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
最適なゲートウェイの選択	• 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、エンドユーザがオフィスにいる間は VPN 接続を自動的に切断し、ユーザ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	導入関連オプション • 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 • 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） • 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 エクスペリエンス	• LAN と同様の安定したユーザ 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 AnyConnect の更新の保留が可能 • 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、ユーザ警告を発行 • 証明書の表示と管理をローカルで実行可能

機能	利点と詳細
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 ● アクセス制御ポリシー ● Google Android（Lollipop）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 ● スタティック（静的） ● 内部プール ● Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル） ● 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）**	● **AnyConnect 4.0 の新機能**：有線環境とワイヤレス環境のエンドポイント ポスチャの評価と修復（Cisco Identity Services Engine NAC エージェントと置き換え）。Cisco Identity Services Engine 1.3 以降と Cisco Identity Services Engine Apex ライセンスが必要です。 ● Cisco Hostscan は、ネットワーク アクセスを許可する前に、エンドポイント システムにウィルス対策ソフトウェア、パーソナル ファイアウォール ソフトウェア、Windows サービス パックが存在することの検出を試みます。 ● 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です。 ● Cisco Hostscan 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。ウォーターマークのチェック機能には、システム レジストリ値、ファイルの存在の照合、必須の CRC32 チェックサム、IP アドレス範囲の照合、および照合認証局によって、または照合認証局に対して発行された証明書が含まれます。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された保護機能 ● 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 7、8、8.1、および Mac OS X 10.8 以降で利用可能
ローカリゼーション	英語に加えて、以下の言語に翻訳 ● 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
AnyConnect 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 ● デバイスでのログ表示 ● 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）

機能	利点と詳細
セキュア モビリティ	
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 セキュリティの最大の世界的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 ● 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 アプライアンスとの統合 ● 信頼ネットワーク検出 ● ユーザ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 ● ホットスポットおよびキャプティブ ポータルの検出
Advanced Malware Protection（AMP）for Endpoints Enabler （AMP for Endpoints は別ライセンス）	● Cisco AMP for Endpoints 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、さらに確実にリモート エンドポイントで攻撃を迅速に軽減
幅広いオペレーティング システムのサポート	● Windows 8 および 8.1 ● Windows 7 32 ビット（x86）および 64 ビット（x64） ● Mac OS 10.8 以降
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 802.11a/b/g/n）
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 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（MSCHAP） ◦ 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 • 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）
セッションの再開	• 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に対して 30 以上のルールをサポート
EAP キャッシュ（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とデバイスを検証
Enterprise Connection Enforcement（ECE）	• ユーザ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 • 手間のかかるブラックリストを排除
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 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 ユーザの資格情報を認証
サポートされているオペレーティング システム	• Windows 8 および 8.1 • Windows 7（32 ビットおよび 64 ビット）

プラットフォームの互換性

AnyConnect モビリティ クライアントは、Cisco ASA Software Release 8.0(4) 以降が動作しているすべての Cisco ASA 5500-X シリーズ Adaptive Security アプライアンス 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。

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、http://www.cisco.com/go/fn [英語] 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、http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html [英語] を参照してください。

ライセンス オプション

- 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 http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf [英語] から確認できます。
- その他の Cisco ASA 5500-X のライセンス ドキュメントについては、http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html [英語] 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：http://www.cisco.com/jp/go/anyconnect
- Cisco AnyConnect ドキュメント：http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html [英語]
- Cisco ASA 5500-X シリーズ Adaptive Security アプライアンス：http://www.cisco.com/jp/go/asa/
- Cisco クラウド Web セキュリティ

  http://www.cisco.com/jp/go/cws
- Cisco Advanced Malware Protection for Endpoints

  http://www.cisco.com/web/jp/product/hs/security/fireamp-endpoints/index.html
- Cisco AnyConnect ライセンス契約書およびプライバシー ポリシー：http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/eula-seula-privacy/AnyConnect_Supplemental_End_User_License_Agreement.htm [英語]

お問い合せ先

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
http://www.cisco.com/jp

C78-733184-02JA 15.11