CHAPTER 1

AnyConnect Secure Mobility Client の概要

Cisco AnyConnect Secure Mobility Client は、Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）への、安全な IPsec（IKEv2）または SSL VPN 接続をリモート ユーザに提供する次世代型 VPN クライアントです。AnyConnect は、今日の増殖を続けるマネージドおよびアンマネージド モバイル デバイス全体でのセキュア モビリティにより、インテリジェントでシームレスな常時接続をエンド ユーザに体験させてくれます。

ASA またはエンタープライズ ソフトウェア導入システムから導入可能

AnyConnect は、ASA から、またはエンタープライズ ソフトウェア導入システムを使用してリモート ユーザに導入できます。ASA から導入する場合、リモート ユーザはクライアントレス SSL VPN 接続を許可するよう設定された ASA のブラウザで IP アドレスまたは DNS 名を入力することで、ASA に最初の SSL 接続を行います。ブラウザ ウィンドウにログイン画面が表示され、ユーザがログインおよび認証に成功すると、コンピュータのオペレーティング システムに対応したクライアントがダウンロードされます。ダウンロードした後、クライアントは自動的にインストールと設定を行い、ASA への IPsec（IKEv2）または SSL 接続を確立します。

カスタマイズ可能および変換可能

AnyConnect をカスタマイズして、リモート ユーザに、自社企業のイメージを表示できます。デフォルトの GUI コンポーネントを置き換えて AnyConnect のブランドを変更し、より広範囲にブランド変更するために作成したトランスフォームを導入したり、AnyConnect API を使用する自分のクライアント GUI を導入したりできます。AnyConnect またはインストーラ プログラムの表示メッセージは、リモート ユーザが希望する言語に翻訳することもできます。

簡単な設定

ASDM を使用して、AnyConnect 機能を簡単にクライアント プロファイルに設定できます。この XML ファイルは、接続確立に関する基本情報、および Start Before Logon（SBL）などの拡張機能を提供します。一部の機能については、ASA の設定を行うことも必要です。ASA は AnyConnect のインストールおよびアップデート中にプロファイルを導入します。

その他のサポート対象モジュール

Cisco AnyConnect Secure Mobility Client バージョン 3.1 は、以下のモジュールを AnyConnect クライアント パッケージに統合します。

- AnyConnect ネットワーク アクセス マネージャ：（以前の Cisco Secure Services Client）このモジュールは、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、有線およびワイヤレス ネットワークの両方へのアクセスに対するデバイス認証を実行します。
- AnyConnect ポスチャ アセスメント：AnyConnect Secure Mobility Client に、ASA へのリモート アクセス接続を確立する前に、ホストにインストールされているオペレーティング システム、およびアンチウイルス、アンチスパイウェア、ファイアウォールの各ソフトウェアを識別する機能を提供します。プリログイン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。ホスト スキャン アプリケーションは、ポスチャ モジュールに同梱される、この情報を収集するアプリケーションです。
- AnyConnect テレメトリ：アンチウイルス ソフトウェアで検出された悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティ アプライアンス（WSA）の Web フィルタリング インフラストラクチャに送信します。WSA では、このデータを使用して、URL のフィルタリング ルールを改善します。
- AnyConnect Web セキュリティ：HTTP トラフィックを、コンテンツ分析、マルウェアの検出、およびアクセプタブル ユース ポリシーの管理を実行する ScanSafe Web Security スキャン プロキシ サーバにルーティングします。
- AnyConnect Diagnostic and Reporting Tool（DART）：トラブルシューティング情報を簡単に Cisco TAC に送信できるように、システム ログのスナップショットおよびその他の診断情報をキャプチャし、.zip ファイルをデスクトップに作成します。
- AnyConnect Start Before Logon（SBL）：Windows のログイン ダイアログボックスが表示される前に AnyConnect を開始することにより、ユーザを Windows へのログイン前に VPN 接続を介して企業インフラへ強制的に接続させます。
- AnyConnect カスタマー エクスペリエンスのフィードバック：ソフトウェアの品質やユーザ エクスペリエンスがさらに改善されるよう、ユーザ エクスペリエンス、クラッシュ インシデントの基本などを探るためのクライアント情報をシスコに提供する機能です。

この章は、次の項で構成されています。

AnyConnect ライセンス オプション

概要

AnyConnect Secure Mobility Client は、VPN セッションおよび Web セキュリティをサポートするためにライセンス アクティベーションを必要とします。必要なライセンスは、使用する AnyConnect VPN Client および Secure Mobility の機能、およびサポートするセッションの数によって異なります。導入には次の AnyConnect ライセンスが 1 つまたは複数必要になる場合があります。

ライセンス	説明	適用先
AnyConnect Essentials	SSL および IPSec VPN 接続用の基本的な AnyConnect 機能をサポートします。このライセンスは、同時にサポートされるリモート アクセス セッションの最大数を指定します。	Cisco ASA 8.0(x) 以降
AnyConnect Premium	AnyConnect Essentials の基本的な機能すべてに加えて、ブラウザ ベースの VPN アクセスなどの Premium AnyConnect クライアント機能、Cisco Secure Desktop、およびホスト スキャン/ポスチャ モジュール機能をサポートします。このライセンスは、同時にサポートされるリモート アクセス セッションの最大数を指定します。このライセンス タイプは共有することもできます。	Cisco ASA 8.0(x) 以降
AnyConnect Mobile	セキュリティ アプライアンスへの AnyConnect モバイル アクセスをサポートします。AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのいずれかの追加として使用できます。追加するには、これらのいずれかが必要です。	Cisco ASA 8.0(x) 以降
AnyConnect Flex	Flex ライセンスは、すべてのライセンスされた機能に対してビジネスの継続性をサポートします。	Cisco ASA 8.0(x) 以降
Advanced Endpoint Assessment	高度なエンドポイント アセスメント機能（自動修復など）を有効にします。アクティブな AnyConnect Premium ライセンスが必要です。	Cisco ASA
Cisco Secure Mobility for AnyConnect	Cisco IronPort Web セキュリティ アプライアンス（WSA）によって提供される Web セキュリティ機能をサポートします。ライセンス名は、ASA 上でアクティブな AnyConnect ライセンス（Essentials または Premium）によって異なります。Cisco IronPort Web セキュリティ アプライアンスのライセンスも必要です。	Cisco WSA 7.0 以降
Cisco Secure Mobility for Cisco Cloud Web Security	AnyConnect Web セキュリティ モジュールのセキュリティ機能をサポートし、ローミング ユーザを Cisco Cloud Web Security（ScanSafe）によって保護します。Cisco Cloud Web Security Web Filtering ライセンスおよび Cisco Cloud Web Security Malware Scanning ライセンスのいずれか一方または両方に加えて、このライセンスが必要です。	

AnyConnect Essentials ライセンスおよび Premium ライセンス

- AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのいずれかを Cisco ASA 8.0(x) 以降でアクティブにできますが、両方のライセンスを同時にアクティブにすることはできません。一部の機能では、機能表に示すように、それ以降の ASA のバージョンが必要です。使用する AnyConnect Secure Mobility 機能に基づきアクティブにするライセンスを選択します。
- AnyConnect 接続に加えて、ASA でアクティブにされた AnyConnect Essentials は、シスコのレガシー VPN クライアントを使用して確立されたセッションをサポートし、企業アプリケーションへフル トンネリング アクセスを行います。クライアントレス VPN アクセスと Cisco Secure Desktop は AnyConnect Essentials ライセンスでは使用できません。
- AnyConnect Premium ライセンスでアクティブにされた ASA は、AnyConnect Essentials ライセンスで許可されたすべてのアクセスと次の AnyConnect Premium 機能をサポートします。
  - クライアントレス VPN アクセス：リモート ユーザはブラウザを使用して VPN セッションを確立でき、特定のアプリケーションはブラウザを使用して、そのセッションにアクセスできます。

  - Cisco Secure Desktop：ブラウザベースのセッションと AnyConnect セッションの両方向けです。
  - ログイン後の VPN 常時接続：ユーザがコンピュータにログインすると、自動的に VPN セッションを常時接続で確立します。詳細については、VPN 常時接続を参照してください。この機能には、接続失敗ポリシーとキャプティブ ポータル ホットスポットの検出と修復も含まれています。

    （注）　常時接続は、WSA で Cisco Secure Mobility for AnyConnect ライセンス、ASA で AnyConnect Essentials ライセンスをアクティブにして有効にすることもできます。

  - エンドポイント アセスメント：選択したアンチウイルス ソフトウェアのバージョン、アンチスパイウェアのバージョン、関連する更新定義、ファイアウォール ソフトウェアのバージョン、および企業財産の検証チェックがポリシーを遵守しているかどうかを確認し、VPN にアクセスできるようにセッションに資格を与えます。

    エンドポイント修復には、以下で説明するように AnyConnect Premium ライセンスの他に Advanced Endpoint Assessment ライセンスが必要です。
  - 検疫：Dynamic Access Policies を使用した非準拠 AnyConnect ユーザの検疫。ユーザにカスタム メッセージを通知できます。

- 次には AnyConnect Essentials ライセンスまたは Premium ライセンスのいずれも必要ありません。
  - ネットワーク アクセス マネージャ モジュール。シスコ ワイヤレス アクセス ポイント、ワイヤレス LAN コントローラ、スイッチ、RADIUS サーバで使用する場合は、無償でライセンスが与えられています。関連するシスコの装置では、現在の SmartNet 契約が必要です。
  - DART モジュールおよびカスタマー フィードバック機能。

AnyConnect Mobile ライセンス

ASA での AnyConnect Mobile ライセンスのアクティブ化はモバイル アクセスに対応していますが、AnyConnect 機能には対応していません。AnyConnect Essentials ライセンスまたは AnyConnect Premium ライセンスのいずれかで、オプションとして使用できます。

AnyConnect 3.1 は現在、モバイル デバイスには対応していません。旧バージョンの AnyConnect で動作している Android または Apple iOS デバイスから接続したい場合は、ASA でこのライセンスをアクティブにする必要があります。

AnyConnect Flex ライセンス

AnyConnect Flex ライセンスは、ライセンスを取得した機能に対してのみビジネスの継続性をサポートします。ビジネス継続性は、ライセンスされたリモート アクセス VPN セッション数を増やし、大流行など異常事態時の一時的な使用の急増に備えます。各 Flex ライセンスは、ASA 専用であり、60 日間サポートします。この日数は、連続した日数および連続していない日数の両方で構成できます。

Advanced Endpoint Assessment ライセンス

Advanced Endpoint Assessment ライセンスは、AnyConnect Premium ライセンスとともにアクティブにする必要があります。このライセンスで、エンドポイント修復を開始できます。

エンドポイント修復は、ASA で Dynamic Access Policies（DAPs）による接続ができなくなった場合に開始します。エンドポイント修復は、エンドポイントのアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール保護のソフトウェアで別のアプリケーションが修復を開始することを許可している場合に、そのソフトウェアのさまざまな側面を修復しようとします。エンドポイント修復が正常に行われると、DAP は以降の接続を許可します。

Cisco Secure Mobility for AnyConnect ライセンス

WSA でアクティブにされた Cisco Secure Mobility for AnyConnect ライセンスは、次のようなブラウザベースの SSL セッションおよび AnyConnect VPN セッションのサービスを提供します。

- マルウェア防御
- アクセプタブル ユース ポリシーの適用
- Web でのデータ漏洩の防止
- すべての HTTP および HTTPS 要求を許可または拒否することによる、安全でないとわかった Web サイトからのエンドポイントの保護
- すべての VPN セッションのインターネット使用状況レポートへの管理者アクセスの提供

Cisco Secure Mobility for AnyConnect ライセンスは、次のようにアクティブにする必要があります。

- Cisco Secure Mobility for AnyConnect Premium ライセンスを WSA でアクティブにするには、ASA で AnyConnect Premium ライセンスまたは AnyConnect Essentials ライセンスのいずれかをアクティブにする必要があります。
- Cisco Secure Mobility for AnyConnect Essentials ライセンスを WSA でアクティブにするには、ASA で AnyConnect Essentials ライセンスをアクティブにする必要があります。WSA でアクティブにされた Cisco Secure Mobility for AnyConnect Essentials ライセンスは、ASA でアクティブにされた AnyConnect Premium ライセンスとともに使用することはできません。

  （注） Premium 機能であるログイン後の VPN 常時接続は、AnyConnect ライセンスを WSA、また AnyConnect Essentials ライセンスを ASA でアクティブにして有効にできます。

- WSA でアクティブにされた Cisco Secure Mobility for AnyConnect ライセンスは、ASA でアクティブにされた AnyConnect ライセンスでサポートされている VPN セッション数と一致するか、それを超える必要があります。

AnyConnect、Premium または Essentials のこの Cisco Secure Mobility ライセンスは、アクティブにされた Cisco IronPort Web セキュリティ アプライアンスのライセンスとは別に追加されます。

詳細については、『*Cisco IronPort Web Security Appliances Introduction*』を参照してください。

AnyConnect ライセンスの組み合わせ

セッション ライセンス	ライセンス オプション	基本アクセス	モバイル アクセス	クライアントレス アクセス	ログイン後の VPN 常時接続	マルウェア防御、アクセプタブル ユース ポリシーの適用、および Web でのデータ漏洩の防止	エンドポイント アセスメント	エンドポイント修復
AnyConnect Essentials	(ベース ライセンス)	✓						
+	AnyConnect Mobile	✓	✓					
+	Cisco Secure Mobility for AnyConnect Essentials	✓	✓		✓	✓		
+	AnyConnect Flex[1]	✓	✓		✓	✓		
AnyConnect Premium SSL VPN Edition	(ベース ライセンス)	✓		✓	✓		✓	
+	AnyConnect Mobile	✓	✓	✓	✓		✓	
+	Cisco Secure Mobility for AnyConnect Premium	✓	✓	✓	✓	✓	✓	
+	Advanced Endpoint Assessment	✓	✓	✓	✓	✓	✓	✓
+	AnyConnect Flex[1]	✓	✓	✓	✓	✓	✓	✓

1. Flex ライセンスは、マルウェア防御、アクセプタブル ユース ポリシーの適用、Web でのデータ漏洩の防止、およびエンドポイント修復の各機能がライセンスされている場合に限り、これらの機能に対するビジネス継続性をサポートします。

Standalone オプションと WebLaunch オプション

ユーザは AnyConnect を次のモードで使用できます。

- Standalone モード：ユーザは、Web ブラウザを使用せずに AnyConnect 接続を確立できます。ユーザの PC に AnyConnect を永続的にインストールした場合、Standalone モードで実行できます。Standalone モードでは、ユーザは AnyConnect をその他のアプリケーションと同じように開き、ユーザ名とパスワード クレデンシャルを AnyConnect GUI のフィールドに入力します。システムの設定によっては、グループを選択する必要もあります。接続が確立すると、ASA は、ユーザの PC 上の AnyConnect のバージョンを調べ、必要に応じて、クライアントは最新バージョンをダウンロードします。

- WebLaunch モード：ユーザは、HTTPS プロトコルを使用して、ブラウザの [Address] または [Location] フィールドに ASA の URL を入力します。次に、ユーザ名とパスワードの情報を [Logon] 画面で入力し、グループを選択して、[Submit] をクリックします。バナーが指定されている場合はその情報が表示され、[Continue] をクリックしてバナーを確認します。

  ポータル ウィンドウが表示されます。AnyConnect を開始するには、メイン ペインで [Start AnyConnect] をクリックします。一連の文書ウィンドウが表示されます。[Connection Established] ダイアログボックスが表示されると、接続が機能し、ユーザがオンライン アクティビティを処理できるようになります。

ASA を設定して AnyConnect パッケージを導入する場合、AnyConnect を企業ソフトウェア展開システムに導入する場合でも、AnyConnect のどのバージョンがセッションを確立できるかという点について、ASA がシングル ポイント適用になるようにします。AnyConnect パッケージを ASA にロードする場合、ASA でロードされたバージョンと同じ新しいバージョンが接続できるポリシーを適用します。AnyConnect は ASA に接続すると自動的にアップグレードされます。または、クライアントがクライアント ダウンローダをバイパスし、ASA でクライアント パッケージ ファイルが必要なくなるようなローカル ポリシー ファイルを導入できます。ただし、Weblaunch や自動アップデートなど他の機能は無効になっています。

コンフィギュレーションおよび導入の概要

ユーザはブラウザで ASA に VPN 接続を行う場合、AnyConnect Profile エディタを使用して、プロファイル ファイルの AnyConnect 機能を設定します。次に、ASA を設定して AnyConnect クライアントとともにこのファイルを自動的にダウンロードします。プロファイル ファイルによって、ユーザ インターフェイスの表示が決まり、ホスト コンピュータの名前とアドレスが定義されます。さまざまなプロファイルを作成し、ASA で設定されたグループ ポリシーに割り当てることで、これらの機能へのアクセスを区別できます。該当するグループ ポリシーへの割り当てに続いて、ASA は、接続設定時にユーザに割り当てられたプロファイルを自動的にプッシュします。

プロファイルによって、接続設定に関する基本情報が提供されますが、ユーザはそれを管理または変更できません。プロファイルは、アクセスできるようにするセキュア ゲートウェイ（ASA）ホストを識別できるようにする XML ファイルです。さらに、ユーザについての追加の接続属性および制約がプロファイルで伝搬されます。一部の機能については、プロファイルの一部の設定をユーザが制御できる設定として指定できます。AnyConnect グラフィカル ユーザ インターフェイスは、これらの設定のコントロールをエンド ユーザに表示します。

ユーザが 1 つのプロファイル ファイルを持っている場合、このプロファイルにはユーザで必要なすべてのホスト、また必要に応じてその他の設定が入っています。特定のユーザに複数のプロファイルを割り当てたい場合があります。たとえば、複数の場所で作業するユーザは、複数のプロファイルが必要な場合があります。ただし、Start Before Login など、一部のプロファイル設定は、グローバル レベルで接続を制御します。特定のホストに固有の設定など、その他の設定は、選択されたホストにより異なります。

または、後でアクセスできるよう、エンタープライズ ソフトウェア導入システムを使用して、プロファイル ファイルおよびクライアントをアプリケーションとしてコンピュータにインストールできます。

AnyConnect Secure Mobility 機能設定ガイドライン

AnyConnect Secure Mobility は、VPN エンドポイントのセキュリティを最適化するために設定できる機能セットです。AnyConnect Secure Mobility Client オプションをすべて設定するには、次の項を参照してください。

ステップ 1　AnyConnect をサポートするための WSA 設定ガイドとして、『Cisco AnyConnect Secure Mobility Solution Guide』の 17 ページにある「Configuring WSA Support of the AnyConnect Secure Mobility Solution」の項に移動します。

ステップ 2　AnyConnect プロファイル エディタを使用して次の機能を設定します。

- 「Trusted Network Detection」（P.3-21）
- 「VPN 常時接続」（P.3-23）
- 「VPN 常時接続用の [Disconnect] ボタン」（P.3-28）
- 「VPN 常時接続に関する接続障害ポリシー」（P.3-29）
- 「キャプティブ ポータル ホットスポットの検出と修復」（P.3-32）
- 「SCEP による認証登録の設定」（P.3-45）

API

AnyConnect との VPN 接続を別のアプリケーションから自動的に行う場合は、次のような Application Programming Interface（API）を使用します。

- プリファレンス
- tunnel-group メソッドの設定

API パッケージには、AnyConnect の C++ インターフェイスに対応するマニュアル、ソース ファイル、およびライブラリ ファイルが含まれています。Windows、Linux、および Mac OS X で AnyConnect を構築する際に、ライブラリおよびプログラム例を使用できます。API パッケージには Windows プラットフォーム用のプロジェクト ファイル（Makefile）が付属しています。その他のプラットフォームに対しては、プラットフォーム固有のスクリプトにサンプル コードのコンパイル方法が示されています。アプリケーション（GUI、CLI、または組み込みアプリケーション）と、これらのファイルやバイナリをリンクできます。

この API は、クライアントの VPN 機能のみサポートします。これは、ネットワーク アクセス マネージャ、Web セキュリティ、テレメトリなど、オプションの AnyConnect モジュールをサポートしません。

AnyConnect アクセシビリティ

AnyConnect には、マウスを使用せずにウィンドウ上のボタンにアクセスできる機能が用意されています。

次のナビゲーション ショートカットは、視力に問題があるか目の見えない担当者がアプリケーションを使用する際に役立ちます。

キーストローク	アクション
Alt	フォーカスをブラウザのメニュー バーに移動します。
Enter	フォーカスされたアイテムを選択します。
Alt+ 矢印キー	ブラウザ メニュー間を移動します。
Alt+ アンダースコア	メニューに移動します。

キーストローク	アクション
Space	チェックボックスのオンとオフなど、コントロールを切り替えます。
Tab	タブ順の次のアイテムまたは次のコントロール グループにフォーカスを移動します。
Shift+Tab	タブ順の前のアイテムまたはグループにフォーカスを移動します。
矢印キー	グループ内のコントロール間を移動します。
Home	複数画面にわたる情報がある場合、ウィンドウの一番上に移動します。 ユーザが入力したテキストの行頭に移動します。
End	ユーザが入力したテキストの行末に移動します。 複数画面にわたる情報がある場合、ウィンドウの一番下に移動します。
Page Up	1 画面分上にスクロールします。
Page Down	1 画面分下にスクロールします。