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。ダウンロード後、クライアントは自動的にインストールおよび設定され、ASA への IPsec（IKEv2）接続または SSL 接続が確立されます。

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。

追加されたサポート対象モジュール

Cisco AnyConnect Secure Mobility Client バージョン 3.0 は、以下の新しいモジュールを AnyConnect クライアント パッケージに統合します。

- ネットワーク アクセス マネージャ：（以前は Cisco Secure Services Client と呼ばれていました）レイヤ 2 のデバイス管理、および有線と無線の両方のネットワーク アクセスの認証を提供します。
- ポスチャ評価：このモジュールにより、AnyConnect Secure Mobility Client は、ASA へのリモート アクセス接続を作成するよりも前にホストにインストールされた、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できま

す。このプリログイン評価に基づいて、どのホストに対して、セキュリティ アプライアンスへのリモート アクセス接続の作成を許可す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。

- テレメトリ：アンチウイルス ソフトウェアによって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 は、このデータを使用して、より優れた URL のフィルタリング ルールを提供します。
- Web セキュリティ：HTTP トラフィックおよび HTTPS 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。
- 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。
- Start Before Logon（SBL）：Windows ダイアログボックスが表示される前に AnyConnect を起動します。Windows ログイン ダイアログボックスが表示される前に AnyConnect を起動することによって、ユーザは Windows にログインする前に VPN 接続を介して企業インフラストラクチャに強制的に接続されます。

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

AnyConnect Secure Mobility Client では、VPN セッションをサポートするために、ライセンスのアクティブ化が必要です。シスコでは、AnyConnect クライアントと Secure Mobility 機能、およびサポートするセッションの数に応じて、以下の 3 段階のライセンス オプションを提供しています。

- AnyConnect Essentials：AnyConnect Secure Mobility Client をサポートします。このライセンスは、Premium としてラベル付けされている機能を除く、すべての AnyConnect クライアント機能をサポートします。また、従来のクライアント（Cisco VPN Client）を使用して確立されたセッションもサポートします。このライセンスは適応型セキュリティ アプライアンスでアクティブ化します。
- Premium：すべての AnyConnect Essentials 機能、ブラウザベースの VPN アクセス、Premium AnyConnect クライアント機能、およびブラウザベースと AnyConnect セッションの両方の Cisco Secure Desktop をサポートします。このライセンスは適応型セキュリティ アプライアンスでアクティブ化します。
- AnyConnect Secure Mobility：Web セキュリティ機能をサポートします。このライセンスは、Cisco Web セキュリティ アプライアンスでアクティブ化します。ライセンス名は、ライセンス適応型セキュリティ アプライアンスに応じて異なります。
- Cisco IronPort Web セキュリティ アプライアンス ライセンス。

ASA 上でアクティブ化され、AnyConnect Premium ライセンスでアクティブ化された適応型セキュリティ アプライアンスは、AnyConnect Essentials ライセンスおよび以下の AnyConnect Secure Mobility Client Premium 機能によってサポートされるのと同じアクセス テクノロジーをサポートします。

- VPN 常時接続および関連オプション機能：接続障害終了ポリシー、キャプティブ ポータルの修復、ローカル印刷、およびテザー デバイスのサポート。
- Cisco Secure Desktop。
- 最適ゲートウェイの選択。
- グループ ポリシーごとのファイアウォール ルール。
- VPN セッションが隔離状態になった場合のユーザ メッセージ。

AnyConnect Essentials および AnyConnect Premium の両方のライセンスには、サポートされる VPN セッションの合計数を指定する段階オプションがあります。

Cisco Secure Mobility for AnyConnect Premium ライセンスまたは Cisco Secure Mobility for AnyConnect Essentials ライセンスでアクティブ化された Cisco IronPort Web セキュリティ アプライアンスによって、適応型セキュリティ アプライアンスを使用するブラウザベースの SSL セッションおよび AnyConnect VPN セッションの以下のサービスが提供されます。

- アクセプタブル ユース ポリシーを強制し、すべての HTTP と HTTPS の要求を許可または拒否することによって、安全でないと見なされる Web サイトからエンドポイントを保護します。
- 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を提供します。

これらのサービスでは、Cisco IronPort Web セキュリティ アプライアンス ライセンスが必要です。Cisco Secure Mobility for AnyConnect Premium ライセンスをアクティブ化するには、適応型セキュリティ アプライアンスでの 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化する必要があります。Cisco Secure Mobility for AnyConnect Essentials ライセンスのアクティブ化でも、適応型セキュリティ アプライアンスでの AnyConnect Essentials ライセンスをアクティブ化する必要があります。適応型セキュリティ アプライアンスでアクティブ化した Premium ライセンスと組み合わせて、Web セキュリティ アプライアンスでアクティブ化した Essentials ライセンスは使用できません。Web セキュリティ アプライアンスでアクティブ化した AnyConnect ライセンスは、適応型セキュリティ アプライアンスでアクティブ化した AnyConnect ライセンスによってサポートされる VPN セッションの数に一致するか、または超えている必要があります。

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、グループを選択しなければならない場合もあります。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 [アドレス（Address）] または [場所（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 [ログイン（Logon）] 画面で入力し、グループを選択して、[送信（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、[続行（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 [AnyConnect の起動（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。[接続を確立しました（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 パッケージを展開するときは、企業のソフトウェア展開システムを使用して AnyConnect を展開する場合でも、ASA が、AnyConnect のバージョンがセッションを確立できる、唯一の適用ポイントであることを確認します。ASA に AnyConnect パッケージをロードするとき、ASA にロードされるバージョンと同じバージョンのみ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 ASA のクライアント パッケージ ファイルの要件を排除して、クライアント ダウンローダを無視するかどうかを指定するローカル ポリシー ファイルを展開できます。ただし、WebLaunch や自動アップデートのようなその他の機能が無効になります。

AnyConnect ライセンス オプション

以下のセクションでは、ライセンス オプションを AnyConnect コンポーネントに関連付けます。

ネットワーク アクセス マネージャ

AnyConnect ネットワーク アクセス マネージャは、無償でシスコの無線アクセス ポイント、ワイヤレス LAN コントローラ、スイッチ、および RADIUS サーバで使用できるようにライセンスされています。AnyConnect Essentials ライセンスまたは Premium ライセンスは必要ありません。関連するシスコの装置では、現在の SmartNet 契約が必要です。

Web セキュリティ

Web セキュリティには、サポート対象となるエンドポイントの数を指定する Web セキュリティ ライセンスが必要です。

VPN ライセンス

SSL および IKEv2 アクセスの AnyConnect サポートには、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する、以下のいずれかのライセンスが必要です。

- AnyConnect Essentials ライセンス
- AnyConnect Premium SSL VPN Edition ライセンス

いずれのライセンスも AnyConnect 基本機能をサポートしています。

表 1-1 は Essentials ライセンスおよび Premium ライセンスと組み合わせることができるライセンスを示しています。

表 1-1　VPN の高度な AnyConnect ライセンス オプション

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	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	クライアントレス アクセス	エンドポイント アセスメント	エンドポイント修復	ビジネス継続性
AnyConnect Essentials	(ベース ライセンス)	✓						
	Cisco Secure Mobility for AnyConnect Essentials	✓	✓	✓				
AnyConnect Premium SSL VPN Edition	(ベース ライセンス)	✓	✓		✓	✓		
	Cisco Secure Mobility for AnyConnect Premium	✓	✓	✓	✓	✓		
	Advanced Endpoint Assessment	✓	✓		✓	✓	✓	
	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。

AnyConnect Essentials、*AnyConnect Premium SSL VPN Edition*、*Advanced Endpoint Assessment*、および *Flex* の各ライセンスは、8.0(x) 以降を実行しているシスコ適応型セキュリティ アプライアンス（ASA）でアクティブ化している必要がありますが、それ以降のバージョンの ASA が必要な機能もあります。

Cisco Secure Mobility ライセンスは、7.0 以降を実行する Cisco IronPort Web Security Appliance（WSA）でアクティブ化する必要があります。

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、この表の機能には対応していません。AnyConnect Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition 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 Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition ライセンスのいずれかで使用できる機能のリストについては、基本機能テーブルを参照してください。

表 1-1 に示すオプション ライセンスでイネーブルにされている機能は次のとおりです。

- *ログイン後の VPN 常時接続*は、ユーザがコンピュータにログインすると、自動的に VPN セッションを確立します。詳細については、常時接続 VPN を参照してください。この機能には常時接続 VPN に関する接続障害ポリシーおよびキャプティブ 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。

- *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*は、Cisco IronPort Web Security Appliance（WSA）で提供される機能です。詳細については、『*Cisco IronPort Web Security Appliances Introduction*』を参照してください。
- *クライアントレス アクセス*では、ブラウザを使用して VPN セッションを確立し、特定のアプリケーションでブラウザを使用して、このセッションにアクセスできます。
- *エンドポイント アセスメント*は、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。
- *エンドポイントの修復*は、エンドポイントの障害を解決し、アンチウイルス、アンチスパイウェア、ファイアウォール ソフトウェアおよび定義ファイルの各要件に関する企業の要件を満たそうとします。
- *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 日間のサポートを提供します。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。

『*Cisco Secure Remote Access: VPN Licensing Overview*』では、AnyConnect ライセンス オプションおよび SKU の例が簡単に説明されています。

AnyConnect の機能、ライセンス、リリース要件、および各機能に対応しているエンドポイント OS の詳しいリストについては、『*Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 3.0*』を参照してください。

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。一部の機能では、プロファイルの特定の設定をユーザ設定可能として指定できます。AnyConnect GUI 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。

通常、ユーザごとに 1 つのプロファイル ファイルを使用します。このプロファイルには、ユーザが必要とするすべてのホスト、および必要に応じて追加の設定が含まれます。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 機能の設定ガイドライン

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 Secure Mobility ソリューションの WSA をサポートするための ASA の設定」（P.2-49）に移動します。

ステップ 2　『*Cisco AnyConnect Secure Mobility Solution Guide*』を AnyConnect をサポートするための WSA を設定する注意事項として使用します。

ステップ 3　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.3-17）
- 「常時接続 VPN」（P.3-19）
- 「常時接続 VPN 用の [接続解除（Disconnect）] ボタン」（P.3-26）
- 「常時接続 VPN に関する接続障害ポリシー」（P.3-27）
- 「キャプティブ ポータル ホットスポットの検出と修復」（P.3-30）
- 「SCEP による認証登録の設定」（P.3-34）

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 上で AnyConnect を構築するために、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。

API は、クライアントの VPN 機能のみをサポートします。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。

ホスト スキャンのインストール

ホストが VPN 接続を確立することによって発生するイントラネット感染の可能性を減らすために、ホスト スキャンを設定して、アンチウイルス、アンチスパイウェア、ファイアウォール ソフトウェア（および VPN セッションを確立する条件として、関連する定義ファイルの更新）をダウンロードおよ

び確認できます。以前は、ホスト スキャンは Cisco Secure Desktop（CSD）のコンポーネントとしてのみ使用できました。AnyConnect Secure Mobility Client の今回のリリースでは、ホスト スキャンは、CSD とは別にインストールおよびアップデートできる別個のモジュールになりました。

（注）　ホスト スキャンおよび一部のサードパーティ ファイアウォールは、グループ ポリシーにより任意に導入されたファイアウォール機能と干渉する可能性があります。

ホスト スキャンのインストールおよび管理の詳細については、第 5 章「ホスト スキャンの設定」を参照してください。