CHAPTER 1

AnyConnect Secure Mobility Client の概要

Cisco AnyConnect Secure Mobility Client は、バージョン ASA 8.0(2) 以降および Adaptive Security Device Manager（ASDM）ソフトウェア バージョン 6.1(3) 以降を実行している Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）へのセキュアな 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。ダウロード後、クライアントはインストールと設定を行い、ASA への 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。

この章は、次の項で構成されています。

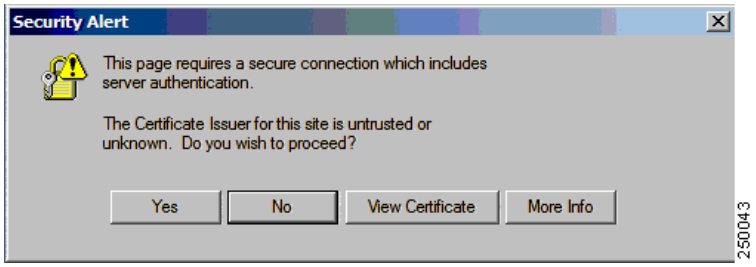
リモート ユーザ インターフェイス

リモート ユーザには AnyConnect ユーザ インターフェイス（図 1-1）が表示されます。Connection タブのドロップダウン リストに、リモート システムに接続するためのプロファイルが表示されます。オプションで、表示するバナー メッセージを [Connection] タブで設定できます。インターフェイスの下部のステータス行に、接続のステータスが表示されます。

図 1-1　[Connection] タブ

証明書を設定していない場合は、図 1-2 のようなダイアログボックスが表示されます。

図 1-2　[Security Alert] ダイアログボックス



（注） このダイアログボックスが表示されるのは、正しい証明書が導入されていない場合だけです。[Yes] をクリックすると、証明書の要件を回避できます。

[Security Alert] ダイアログボックスは、指定された ASA への最初に接続しようとした場合のみ表示されます。接続の確立に成功すると、サーバ証明書の「サムプリント」がプリファレンス ファイルに保存されるため、同じ ASA への以降の接続では、ユーザにプロンプトは表示されません。

ユーザが、別の ASA に接続してから戻ると、[Security Alert] ダイアログボックスが再表示されます。

クライアントが、ローカル ポリシー ファイルを導入して証明書サムプリントをキャッシュに入れるかどうか制御できます。このファイルは、より多くのクライアント セキュリティ パラメータを指定する XML ファイルです。ローカル ポリシーでは、デフォルトでサムプリントはキャッシュに入れられません。無効な証明書で ASA に接続するたびに、[Security Alert] ダイアログボックスが表示されます。ローカル ポリシーの詳細については、第 4 章「FIPS およびその他のセキュリティのローカル ポリシーでのイネーブル化」を参照してください。

表 1-1 に、[Security Alert] ダイアログボックスが表示される条件と結果を示します。セキュリティ アラートの詳細については、第 2 章「AnyConnect を導入するためのセキュリティ アプライアンスの設定」の「ブラウザの警告ウィンドウに対応するセキュリティ証明書の追加」（P.2-4）を参照してください。

表 1-1　証明書、セキュリティ アラート、および接続のステータス

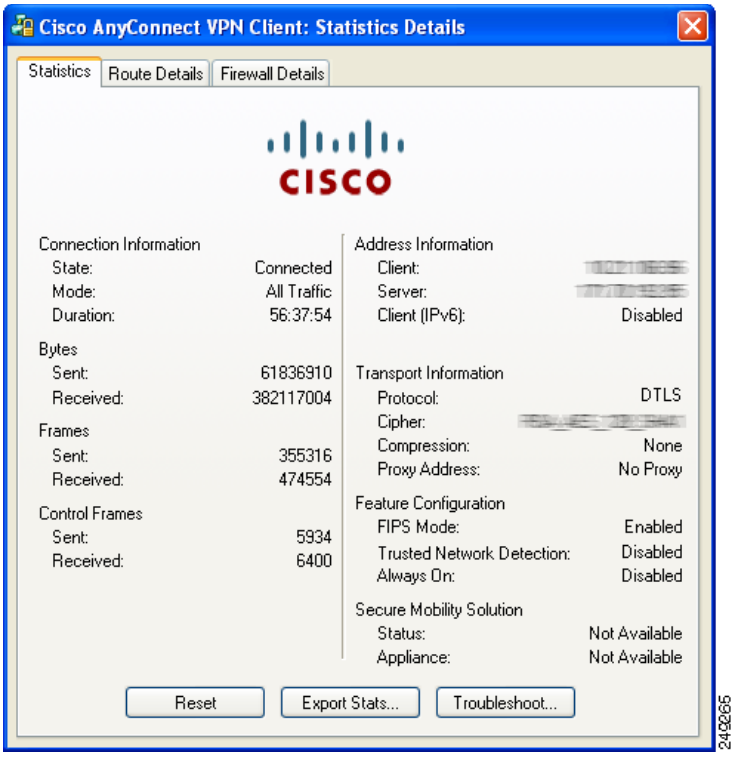
証明書のステータス	セキュリティ アラートが表示されるか	AnyConnect 接続のステータス
AnyConnect から ASA に送信されたサーバ証明書が、独立して検証可能で、かつ証明書に重大なエラーがない。	No	Success
AnyConnect から ASA に送信されたサーバ証明書が、独立して検証可能でなく、かつ証明書に重大なエラーがある。	No	Failure
AnyConnectから ASA に送信されたサーバ証明書が、独立して検証可能でなく、かつ証明書に重大なエラーがない。	Yes	AnyConnect で証明書を確認できないため、セキュリティに問題があると考えられます。AnyConnect はユーザに接続を続けるかどうか尋ねます。

図 1-3 に、現在の接続情報が表示されている [Statistics] タブを示します。

図 1-3　[Statistics] タブ

[Details] をクリックすると、[Statistics Details] ウィンドウが表示されます（図 1-4）。

図 1-4　[Statistics] タブ > [Statistics Details]

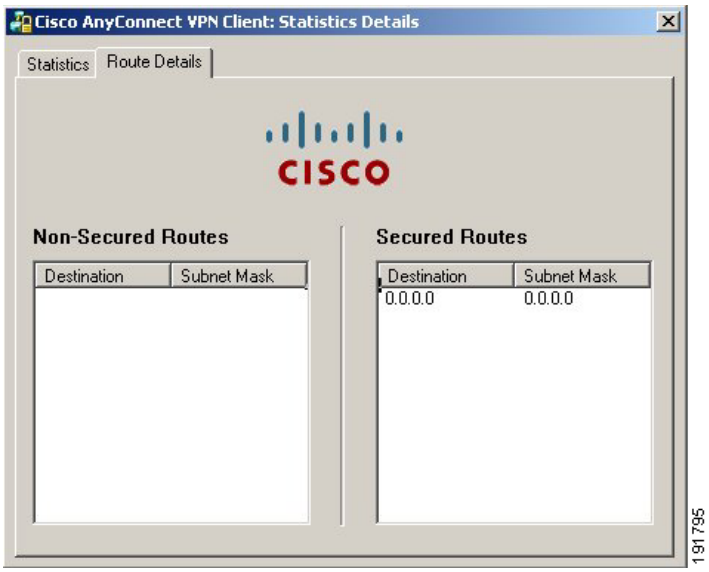


このウィンドウに表示されるオプションは、クライアント PC にロードされているパッケージによって異なります。オプションを使用できない場合は、ダイアログボックスでそのオプション ボタンがアクティブにならず、オプション名の横に [Not Installed] というインジケータが表示されます。オプションは次のとおりです。

- [Reset] をクリックすると、接続情報がゼロにリセットされます。AnyConnect による新しいデータの収集がすぐに開始されます。
- [Export Stats...] をクリックすると、接続の統計情報がテキスト ファイルに保存され、あとから分析とデバッグを行えます。
- [Troubleshoot...] をクリックすると、DART（Diagnostic AnyConnect Reporting Tool）ウィザードが起動されます。指定したログ ファイルと診断情報を結び付けることで、AnyConnect 接続の分析とデバッグに使用できます。DART パッケージの詳細については、「DART を使用したトラブルシューティング情報の収集」（P.8-5）を参照してください。

[Route Details] タブ（図 1-5）には、この接続のセキュアなルートとセキュアでないルートが表示されます。

図 1-5　ユーザ インターフェイス、[Statistics] タブ > [Route Details]



（注）　宛先が 0.0.0.0 でサブネット マスクが 0.0.0.0 の Secured Routes エントリは、すべてのトラフィックがトンネルで処理されることを意味します。

[Export] ボタンおよび [View Log] ボタンを使用した接続のモニタリングの詳細については、「詳細な統計情報の表示」（P.8-2）を参照してください。

[About] タブ（図 1-6）には、AnyConnect のバージョン情報、著作権情報、および文書情報が表示されます。

図 1-6　[About] タブ

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 : 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。接続が確立されると、ASA はユーザの PC にある AnyConnect のバージョンをチェックし、必要な場合、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。

Standalone モードと WebLaunch モードのどちらで接続する場合でも、AnyConnect を接続するには、ASA に AnyConnect パッケージがインストールされている必要があります。そうすることで、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 AnyConnect を導入した場合でも、どのバージョンの AnyConnect がセッションを確立できるかを、ASA で一元的に実施できるようになります。AnyConnect パッケージを ASA にロードすると、ロードされたものと同じ最新バージョンだけが接続可能というポリシーが実施されます。AnyConnect は ASA に接続すると自動的にアップグレードされます。

AnyConnect ライセンス オプション

一度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には、AnyConnect Essentials ライセンスまたは AnyConnect Premium SSL VPN Edition ライセンスが必要です。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 1-2 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 1-2　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 1-2 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、ログイン後の VPN 常時接続を参照してください。この機能には VPN 常時接続に関する接続障害ポリシーおよびキャプティブ ポータルの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、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs, Release 2.5*』を参照してください。

ファイルおよびコンポーネント

インストールおよび設定の手順は、ASA で実行する必要がある手順と、リモート コンピュータで実行する必要がある手順の 2 つで構成されています。AnyConnect ソフトウェアは、ASA リリース 8.0（1）以降に組み込まれています。AnyConnect ソフトウェアを永続的にリモート PC 上に常駐させることも、接続の間だけ常駐させることもできます。

AnyConnect は、セキュリティ アプライアンスにロードして、リモート ユーザが ASA にログインしたときに自動的に導入することも、PC 上のアプリケーションとして、ネットワーク管理者が標準のソフトウェア導入メカニズムを使用してインストールすることもできます。

AnyConnect ファイルと API パッケージは次の場所で入手できます。
http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect

Start Before Logon コンポーネントのインストール（Windows のみ）

AnyConnect の WebLaunch に ASA を設定した場合、クライアントによってコンポーネントが自動的に正しい順序で指定されます。それ以外の場合は、Start Before Logon コンポーネントを、コア クライアントのインストール*後に*インストールする必要があります。クライアントおよび MSI ファイルを使用した Start Before Logon コンポーネントを導入する前の場合（Altiris、Active Directory または SMS など独自のソフトウェア導入手段を持つ大企業の場合など）、コンポーネントを正しい順序で指定する必要があります。

ローカル コンピュータにインストールされた AnyConnect プロファイル ファイル

AnyConnect によって、次の AnyConnect プロファイル ファイルがローカル コンピュータにダウンロードされます。

表 1-3　エンドポイントのプロファイル ファイル

ファイル	説明
anyfilename.xml	AnyConnect プロファイル。このファイルは、特定のユーザ タイプに対して設定される機能および属性値を指定します。
AnyConnectProfile.tmpl	AnyConnect ソフトウェアによって提供されたクライアント プロファイルの例
AnyConnectProfile.xsd	XML スキーマ フォーマットを定義します。AnyConnect はこのファイルを使用して、プロファイルを確認します。

AnyConnect によってこの 3 つのファイルが、次に示す同じディレクトリにダウンロードされます。

表 1-4　エンドポイントのプロファイル ファイルへのパス

OS	ディレクトリ パス
Windows 7 および Vista	C:¥ProgramData¥Cisco¥Cisco AnyConnect VPN Client¥Profile¥
Windows XP	C:¥Documents and Settings¥All Users¥Application Data¥Cisco¥Cisco AnyConnect VPN Client¥Profile¥
Windows Mobile	C:¥Program Files¥Cisco AnyConnect VPN Client
Mac OS X および Linux	/opt/cisco/vpn/profile/

ローカル コンピュータにインストールされたユーザ プリファレンス

また一部のプロファイル設定は、ユーザ コンピュータ上のユーザ プリファレンス ファイルまたはグローバル プリファレンス ファイルにローカルに保存されます。ユーザ ファイルには、クライアント GUI の [Preferences] タブにユーザ制御可能設定をクライアントで表示するうえで必要となる情報、およびユーザ、グループ、ホストなど、直近の接続に関する情報が保存されます。

グローバル ファイルには、ユーザ制御可能設定に関する情報が保存されます。これにより、ログイン前でも（ユーザがいなくても）それらの設定を適用することができます。たとえば、クライアントでは Start Before Logon や起動時自動接続が有効になっているかどうかをログイン前に認識する必要があります。

表 1-5 は、クライアント コンピュータでのプリファレンス ファイルのファイル名およびインストール パスを示しています。

表 1-5　ユーザ プリファレンス ファイルおよびインストール パス

オペレーティング システム	タイプ	ファイルおよびパス
Windows Vista Windows 7	ユーザ	C:¥Users¥*username*¥AppData¥Local¥Cisco¥ Cisco AnyConnect VPN Client¥preferences.xml
	グローバル	C:¥ProgramData¥Cisco¥Cisco AnyConnect VPN Client¥ preferences_global.xml
Windows XP	ユーザ	C:¥Documents and Settings¥**username**¥Local Settings¥ApplicationData¥ Cisco¥Cisco AnyConnect VPN Client¥preferences.xml
	グローバル	C:¥Documents and Settings¥AllUsers¥Application Data¥Cisco¥ Cisco AnyConnect VPN Client¥preferences_global.xml
Mac OS X	ユーザ	/Users/username/.anyconnect
	グローバル	/opt/cisco/vpn/.anyconnect_global
Linux	ユーザ	/home/username/.anyconnect
	グローバル	/opt/cisco/vpn/.anyconnect_global

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。

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。Windows Mobile デバイスでは、この代替方法だけがサポートされています。

AnyConnect Secure Mobility 機能設定時の注意事項

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.2-20）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）
- 「ログイン後の VPN 常時接続」（P.3-19）
- 「VPN 常時接続用の [Disconnect] ボタン」（P.3-25）
- 「VPN 常時接続に関する接続障害ポリシー」（P.3-26）
- 「キャプティブ ポータル ホットスポットの検出と修復」（P.3-29）
- 「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 での AnyConnect の構築に使用できるライブラリとサンプル プログラムもあります。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。

Host Scan 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には、Host Scan を設定して、SSL セッションを確立する条件と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、および関連する定義ファイルの更新をダウンロードおよびチェックします。Host Scan は、Cisco Secure Desktop（CSD）に含まれています。

（注）　Host Scan 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。

CSD は AnyConnect と協調して動作しますが、別の製品であり、本書では扱いません。CSD の詳細と CSD のインストールについては、『*Release Notes for Cisco Secure Desktop*』および『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。