CHAPTER 5

ホスト スキャンの設定

AnyConnect ポスチャ モジュールにより、AnyConnect Secure Mobility クライアントは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 モジュールのコンポーネントに含まれる、こうした情報を収集するアプリケーションです。

適応型セキュリティ アプライアンス（ASA）では、オペレーティング システム、IP アドレス、レジストリ エントリ、ローカル証明書、ファイル名など、エンドポイント属性を評価するプリログイン ポリシーを作成できます。プリログイン ポリシーの評価結果に基づいて、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ホストを制御できます。

AnyConnect 3.0 より、ホスト スキャン パッケージは AnyConnect Secure Mobility クライアントおよび Cisco Secure Desktop（CSD）の共有コンポーネントになっています。それ以前は、ホスト スキャン パッケージは CSD をインストールすることによってのみ利用可能になるコンポーネントの 1 つでした。

ホスト スキャン パッケージを CSD から分離したのは、CSD の一部として提供されていたときよりも、ユーザが頻繁にホスト スキャン サポート表を更新できるようにするためです。ホスト スキャン サポート表には、ダイナミック アクセス ポリシー（DAP）を割り当てるために使用されるアンチウイルス、スパイウェア、およびファイアウォールのアプリケーションの製品名とバージョン情報が記載されます。シスコでは、ホスト スキャン パッケージにホスト スキャン アプリケーション、ホスト スキャン サポート表、および他のコンポーネントを含めて提供しています。

スタンドアロン ホスト スキャン パッケージおよびポスチャ モジュールに同梱されるホスト スキャン パッケージでは、同じ機能が提供されます。シスコでは、ホスト スキャン サポート表を簡単に更新できるように、別個のホスト スキャン パッケージを提供しています。

ホスト スキャン パッケージは、現在、AnyConnect ポスチャ モジュールとともに、CSD とともに、またはスタンドアロン パッケージとして、これら 3 つの方法のいずれかで提供されます。AnyConnect ポスチャ モジュールには 2 つのタイプがあります。1 つ目のバージョンは、AnyConnect のインストールと一緒に ASA によってプッシュされます。もう 1 つのバージョンは、事前展開モジュールとして設定されます。事前展開モジュールは、ASA への初期接続を確立する前に、エンドポイントにインストールできます。

エンドポイン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することに加え、ホスト スキャン パッケージによって、プリログイン評価の実行、キーストローク ロガーの識別、およびエンドポイントで実行されるホスト エミュレーションと仮想マシンの検出を行うコンポーネントが提供されます。キーストローク ロガーの検出およびホスト エミュレーションと仮想マシンの検出は、CSD の機能でもありましたが、今ではホスト スキャン パッケージに組み込まれています。

しかし、ホスト スキャン パッケージは、CSD に代わるものではありません。Secure Vault が必要なお客様は、ホスト スキャン パッケージの他に CSD をインストールして、有効にする必要があります。Secure Vault 機能の詳細については、CSD 設定ガイド http://www.cisco.com/en/US/products/ps6742/products_installation_and_configuration_guides_list.html を参照してください。

AnyConnect クライアントは、Secure Desktop 内から起動することはできません。最初に ASA へのクライアントレス SSL VPN 接続を確立し、ポータル ページから AnyConnect を起動することで、ユーザは AnyConnect に接続できます。

ASA の Adaptive Security Device Manager（ASDM）またはコマンドライン インターフェイスを使用して、ホスト スキャンのインストール、アンインストール、イネーブル、およびディセーブルを行えます。ASDM の Secure Desktop Manager ツールを使用して、プリログイン ポリシーを設定できます。

ポスチャ評価および AnyConnect テレメトリ モジュールを使用するには、ホスト スキャンがホストにインストールされている必要があります。

この章は、次の内容で構成されています。

ホスト スキャン ワークフロー

以下のワークフローで説明するように、ホスト スキャンは ASA と連携して、企業ネットワークを保護します。

1. リモート デバイスでは、クライアントレス SSL VPN またはセキュリティ アプライアンスとの AnyConnect Client セッション確立が試行されます。
2. ASA はホスト スキャンをクライアントにダウンロードして、ASA とクライアントが同じバージョンのホスト スキャンを使用するようにします。
3. プリログイン評価は、リモート コンピュータについて以下のチェックを行います。
   - オペレーティング システム
   - CSD 管理者が指定するファイルの有無。
   - CSD 管理者が指定するレジストリ キーの有無。このチェックは、コンピュータが Microsoft Windows を実行している場合だけに適用されます。
   - CSD 管理者が指定するデジタル証明書の有無。このチェックについても、コンピュータが Microsoft Windows を実行している場合だけに適用されます。

- CSD 管理者が指定する IP アドレスの範囲。

4. クライアントでプリログイン評価が実行されているときに並行して、ホスト スキャンはエンドポイント アセスメントを実行し、アンチウイルス、ファイアウォール、およびアンチスパイウェアのバージョン情報を収集します。また、ダイナミック アクセス ポリシーで指定したレジストリ キー、ファイル、およびプロセスのスキャンも行います。
5. プリログイン評価の結果に応じて、次のイベントのいずれかが発生します。
   - プリログイン評価が実行され、[ログインが拒否されました（Login Denied）] エンドノードで終了するシーケンスを経由する場合は、リモート コンピュータに「ログインが拒否されました（Login Denied）」メッセージが表示されます。この場合、ASA とリモート デバイス間の対話は停止します。
   - プリログイン評価は、プリログイン ポリシー名をデバイスに割り当て、そのプリログイン ポリシー名を ASA に報告します。
6. ホスト スキャンは、プリログイン評価後にリモート コンピュータが割り当てられたプリログイン ポリシーの設定に基づいて、リモート コンピュータのキーストローク ロガーおよびホスト エミュレーションをチェックします。
7. 保証対象であり、Advanced Endpoint Assessment のライセンスがある場合、アンチウイルス、ファイアウォール、またはアンチスパイウェアの修復が実行されます。
8. ユーザがログインします。
9. ASA は、通常、3. で収集された認証データとともに、4. で収集されたエンドポイント属性の設定基準（これには、プリログイン ポリシーやホスト スキャンの結果と同様の値が含まれる場合があります）を使用して、ダイナミック アクセス ポリシーをセッションに適用します。
10. ユーザ セッションが終了した後、ホスト スキャンが終了し、キャッシュ クリーナがクリーンアップ機能を実行します。

AnyConnect ポスチャ モジュールで使用可能な機能

プリログイン評価

プリログイン評価は、ユーザが ASA に接続した後、かつログインする前に、実行されます。この評価では、ファイル、デジタル証明書、OS、IP アドレス、および Microsoft Windows レジストリ キーについてリモート デバイスをチェックできます。

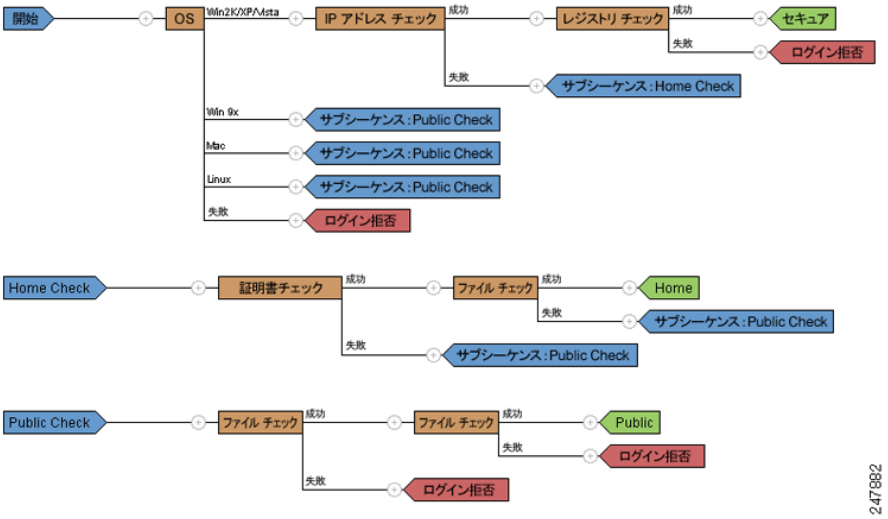
管理者とホスト スキャンのインターフェイスとなる Secure Desktop Manager では、プリログイン評価モジュールを簡単に設定できるグラフィカル シーケンス エディタが提供されます。

プリログイン評価モジュールを設定するときに、ホスト スキャン管理者は「*シーケンス*」と呼ばれるノードのブランチを作成します。各シーケンスは [スタート（Start）] ノードで始まり、続いてエンドポイント チェックが実行されます。チェックの結果により、別のエンドポイント チェックを実行するかどうか、またはエンドノードでシーケンスを終了するかどうかを判定します。

エンドノードでは、「ログインが拒否されました（Login Denied）」メッセージを表示するかどうか、プリログイン ポリシーをデバイスに割り当てるかどうか、または「サブシーケンス」と呼ばれるセカンダリ チェックのセットを実行するかどうかを判定します。「*サブシーケンス*」は、シーケンスの連続で、通常、詳細なエンドポイント チェックとエンドノードで構成されます。この機能は、以下の処理を行う場合に便利です。

- 特定のケースで、チェックのシーケンスを再利用する。
- サブシーケンス名を使用して文書化するといった全体的な目的を持つ条件セットを作成する。
- グラフィカル シーケンス エディタが占める水平方向の領域を制限する。

図 5-1　　完全なプリログイン評価の例

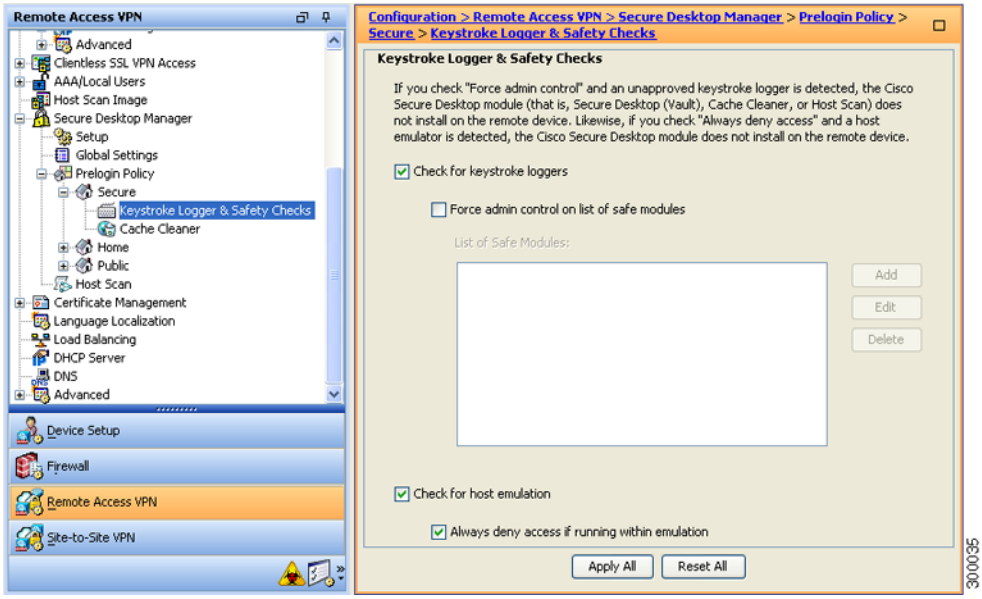


プリログイン ポリシー

グラフィカル シーケンス エディタで設定されたプリログイン評価（図 5-1）のチェックの結果によって、プリログイン評価が特定のプリログイン ポリシーに割り当てられるか、または拒否されるリモート アクセス接続となるかが判明します。

ポリシーを作成するたびに、Secure Desktop Manager によりポリシーにちなんだ名前が追加されます。ポリシーのメニューごとに、ポリシーに対して一意な設定を割り当てることができます。これらの設定によって、キーストローク ロガー検出、ホスト エミュレーション検出、またはキャッシュ クリーナが、ポリシーに割り当てられたプリログイン条件に一致するリモート デバイスにインストールされるかどうかが決定します。管理者は通常、これらのモジュールを企業以外のコンピュータに割り当て、セッション終了後の企業データやファイルへのアクセスを防止します。

図 5-2　プリログイン ポリシー



キーストローク ロガー検出

ユーザが入力したキー入力を記録するプロセスまたはモジュールのスキャンを選択したプリログイン ポリシーを設定して、疑わしいキー入力ロギング アプリケーションが存在する場合は、VPN アクセスを拒否できます。

デフォルトでは、キーストローク ロガー検出はすべてのプリログイン ポリシーでディセーブルになっています。Secure Desktop Manager を使用して、キーストローク ロガー検出をイネーブルまたはディセーブルにできます。安全なキーストローク ロガーを指定するか、またはリモート コンピュータ上のキャッシュ クリーナまたはホスト スキャンを実行するための条件としてスキャンで識別されたキーストローク ロガーをリモート ユーザに対話的に承認させることができます。

イネーブルにすると、キーストローク ロガー検出はキャッシュ クリーナまたはホスト スキャンとともにリモート コンピュータにダウンロードされます。ダウンロードが完了したキーストローク ロガー検出は、OS が Windows で、かつユーザが管理者権限を持っている場合に限り実行されます。

関連モジュールは、スキャンに問題がない場合、または、管理者がユーザに管理作業を割り当て、スキャンで識別されたアプリケーションをユーザが承認する場合に限り実行されます。

（注）　キーストローク ロガー検出は、エンドユーザが管理者権限でログインしている限り、ユーザ モードとカーネル モードの両方のロガーに適用されます。

キーストローク ロガー検出は、32 ビット版 Microsoft Windows OS 環境に限り実行できます。「キーストローク ロガー検出およびホスト エミュレーション検出の対応オペレーティング システム」（P.5-6）を参照してください。

キーストローク ロガー検出では、潜在的に悪意のあるキーストローク ロガーのすべてを検出できない場合があります。ハードウェアのキー入力ロギング デバイスは検出されません。

ホスト エミュレーション検出

プリログイン ポリシーのもう 1 つの機能であるホスト エミュレーション検出では、リモートの Microsoft Windows オペレーティング システムがバーチャライゼーション ソフトウェア上で実行されているかどうかを判断します。Secure Desktop Manager を使用して、この機能をイネーブルまたはディセーブルにできます。また、ホスト エミュレータが存在する場合にアクセスを拒否したり、ユーザに検出を報告し、続行するか終了するかの判断をユーザに委ねることができます。

デフォルトでは、ホスト エミュレーション検出はすべてのプリログイン ポリシーでディセーブルになっています。この機能をイネーブルにすると、Secure Desktop、Cache Cleaner、またはホスト スキャンと共にリモート コンピュータにダウンロードされます。ダウンロードが完了すると、まずホスト エミュレーション検出が実行され、キーストローク ロガー検出の実行が設定されている場合は同時に実行されます。続いて、次のいずれかの条件に当てはまる場合は、関連モジュールが実行されます。

- ホストがエミュレータ（または、バーチャライゼーション ソフトウェア）上で実行されていない。
- アクセスを常に拒否するように設定しておらず、ユーザが検出されたホスト エミュレータを承認する。

「キーストローク ロガー検出およびホスト エミュレーション検出の対応オペレーティング システム」（P.5-6）を参照してください。

キーストローク ロガー検出およびホスト エミュレーション検出の対応オペレーティング システム

キーストローク ロガー検出およびホスト エミュレーション検出は、以下のオペレーティング システムで実行します。

- x86（32 ビット）の Windows Vista SP1 および SP2

  SP1 および SP2 を使用しない Windows Vista を実行するコンピュータの場合、KB935855 をインストールする必要があります。
- x86（32 ビット）の Windows XP SP2 および SP3

（注）　Secure Desktop、キーストローク ロガー検出、およびホスト エミュレーション検出は Windows 7 ではサポートされません。

Cache Cleaner

Secure Desktop の代替機能となる Cache Cleaner は機能面で制限がありますが、多くのオペレーティング システムをサポートする柔軟性を備えています。Cache Cleaner では、クライアントレス SSL VPN または AnyConnect Client セッション終了時に、ブラウザ キャッシュから情報を削除しようとします。この情報には、入力されたパスワード、オートコンプリート テキスト、ブラウザでキャッシュされたファイル、セッション時に行われたブラウザ設定の変更、およびクッキーが含まれます。

Cache Cleaner は、Microsoft Windows、Apple Mac OS、Linux 上で実行されます。システム要件の詳細については、『Cisco Secure Desktop Release Notes』を参照してください。

これは、通常、キャッシュ クリーナが展開され、エンドポイントがクライアントレス SSL VPN 接続を作成しようとするとき、または Web 起動を使用する AnyConnect を起動しようとするときのイベントのシーケンスになります。

ステップ 1　ユーザがブラウザに URL を入力すると、エンドポイントは ASA に接続します。

ステップ 2　ホスト スキャンはプリログイン評価を実行します。

ステップ 3　エンドポイントがプリログイン評価を通過することが前提ですが、AnyConnect の認証が開始されます。ユーザはパスワードを入力するか、認証用の証明書を使用できます。

ステップ 4　[現在のセッションのキャッシュに加えてすべてのキャッシュのクリーニングを行う（IE のみ）(Clean the whole cache in addition to the current session cache (IE only))] をイネーブルにしないで Internet Explorer を実行しているユーザ、または Safari や Firefoxfor を実行しているユーザの場合、ユーザ認証の後、約 1 分間、キャッシュ クリーナによってブラウザのキャッシュのスナップショットが取られます。

ステップ 5　ユーザが操作すると、ブラウザは情報をキャッシュします。

ステップ 6　ユーザが VPN セッションをログアウトすると、以下が実行されます。

- [現在のセッションのキャッシュに加えてすべてのキャッシュのクリーニングを行う（IE のみ）(Clean the whole cache in addition to the current session cache (IE only))] をイネーブルにして Internet Explorer を実行しているユーザの場合、キャッシュ クリーナはブラウザのすべてのキャッシュを削除しようとします。
- [現在のセッションのキャッシュに加えてすべてのキャッシュのクリーニングを行う（IE のみ）(Clean the whole cache in addition to the current session cache (IE only))] をイネーブルにしないで Internet Explorer を実行しているユーザ、または Safari や Firefoxfor を実行しているユーザの場合、キャッシュ クリーナはブラウザのすべてのキャッシュの削除を試行してから、そのキャッシュに対して取ったスナップショットを復元します。

  機密情報をコンピュータに復元しないようにするため、セッションが終了した後、ブラウザを閉じてから、ブラウザのキャッシュを手動で消去することを推奨します。

（注）　[現在のセッションのキャッシュに加えてすべてのキャッシュのクリーニングを行う（IE のみ）(Clean the whole cache in addition to the current session cache (IE only))] オプションをイネーブルにしてキャッシュ クリーナを設定することを推奨します。

ホスト スキャン

ホスト スキャンは、ユーザが ASA に接続した後、かつログインする前に、リモート デバイス上にインストールされるパッケージです。ホスト スキャンは、CSD 管理者が設定する基本ホスト スキャン モジュール、エンドポイント アセスメントモジュール、Advanced Endpoint Assessment モジュールの任意の組み合わせで構成されます。ホスト スキャンは、Microsoft Windows、Apple Mac OS X、および Linux 上で実行されます。詳細な要件については、「システム要件」（P.5-11）を参照してください。

ホスト スキャン パッケージは、CSD とバンドルされて、スタンドアロン モジュールとして、また AnyConnect 3.0 クライアントのポスチャ モジュールの一部として提供されます。

基本ホスト スキャン機能

ホスト スキャンは、CSD またはホスト スキャン /CSD が ASA でイネーブルにされている場合に、Cisco クライアントレス SSL VPN または AnyConnect クライアント セッションを確立するリモート デバイスのオペレーティング システムおよびサービス パックを自動的に識別します。

Secure Desktop Manager を使用して、特定のプロセス、ファイル、レジストリ キー、デジタル証明書、および IP アドレスについて、エンドポイントを検査するようにホスト スキャンを設定することもできます。Secure Desktop Manager は、ASA 上で Adaptive Security Device Manager（ASDM）と統合されます。

ホスト スキャンは、ユーザがコンピュータにログオンする前に、これらすべての検査を実行します。

ホスト スキャンは、オペレーティング システムとサービス パックの情報とともに、収集するように設定されたプロセス、ファイル、レジストリ キー、デジタル証明書、および IP アドレスをエンドポイントから収集した後、その情報を ASA に送信します。ASA では、その情報は、企業所有のコンピュータ、個人用コンピュータ、パブリック コンピュータを区別するために使用されます。また、この情報はプリログイン評価にも使用されます。詳細については、「プリログイン評価」（P.5-3）を参照してください。

また、ホスト スキャンは、設定した DAP エンドポイント条件と照合して評価するために、以下の追加の値を自動的に返します。

- Microsoft Windows、Mac OS、Linux のビルド
- Microsoft Windows が実行されている接続ホスト上でアクティブなリスニング ポート
- 接続ホスト上にインストールされている CSD コンポーネント
- Microsoft サポート技術情報（KB）番号

DAP および Lua 表現の詳細については、「Dynamic Access Policies との統合」（P.5-10）および『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』の第 7 章「Using Match Criteria to Configure Dynamic Access Policies」を参照してください。

エンドポイント アセスメント

エンドポイント アセスメントは、ホスト スキャンの拡張機能であり、アンチウイルスとアンチスパイウェアのアプリケーション、関連する定義の更新、およびファイアウォールの大規模な収集について、リモート コンピュータを検査します。ASA によって特定のダイナミック アクセス ポリシー（DAP）がセッションに割り当てられる前に、この機能を使用して要件を満たすようにエンドポイント条件を組み合わせることができます。DAP の詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』の第 7 章「Using Match Criteria to Configure Dynamic Access Policies」を参照してください。

Advanced Endpoint Assessment：アンチウイルス、アンチスパイウェア、およびファイアウォールの修復

ASA にインストールされた **Advanced Endpoint Assessment** ライセンスを購入すると、以下のホスト スキャンの高度な機能を使用できます。

修復

Windows、Mac OS X、および Linux のデスクトップでは、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、Advanced Endpoint Assessment は、それらのソフトウェアに関するさまざまな修復を開始しようとします。

アンチウイルス：Advanced Endpoint Assessment は、アンチウイルス ソフトウェアの以下のコンポーネントを修復しようとします。

- ファイル システム保護の強制：アンチウイルス ソフトウェアがディセーブルの場合に、Advanced Endpoint Assessment はこのコンポーネントをイネーブルにできます。
- ウイルス定義更新の強制：Advanced Endpoint Assessment の設定で定義された日数の間、アンチウイルス定義が更新されなかった場合に、Advanced Endpoint Assessment は、ウイルス定義の更新を開始しようとします。

アンチスパイウェア：Advanced Endpoint Assessment の設定で定義された日数の間、アンチスパイウェア定義が更新されなかった場合に、Advanced Endpoint Assessment は、アンチスパイウェア定義の更新を開始しようとします。

パーソナル ファイアウォール：ファイアウォール設定およびルールが Advanced Endpoint Assessment の設定で定義された要件を満たしていない場合、Advanced Endpoint Assessment モジュールは、それらを再設定しようとします。

- ファイアウォールは、イネーブルまたはディセーブルにできます。
- アプリケーションを実行しないように、または実行するようにできます。
- ポートをブロックする、または開くこともできます。

（注） この機能は、すべてのパーソナル ファイアウォールでサポートされているわけではありません。

エンドユーザがアンチウイルスまたはパーソナル ファイアウォールをディセーブルにした場合、正常に VPN 接続を確立した後、Advanced Endpoint Assessment の機能は約 60 秒以内にそのアプリケーションを再びイネーブルにしようとします。

ホスト スキャン サポート表

ホスト スキャン サポート表に、プリログイン ポリシーで使用するアンチウイルス、アンチスパイウェア、およびファイアウォールのアプリケーションの製品名およびバージョン情報が記載されます。ホスト スキャンおよびホスト スキャン サポート表は、ホスト スキャン パッケージに同梱されます。

AnyConnect Secure Mobility Client のこのリリースでは、ホスト スキャン パッケージは、Cisco Secure Desktop（CSD）とは別にアップロードできます。これは、CSD をインストールしなくてもホスト スキャンの機能を展開できること、また、最新のホスト スキャン パッケージに更新することで、ホスト スキャン サポート表を更新できることを意味します。

ホスト スキャン サポート表は、cisco.com（http://www.cisco.com/en/US/products/ps10884/products_device_support_tables_list.html）からダウンロードできます。

これらのサポート表は、Microsoft Excel、Microsoft Excel Viewer、または OpenOffice を使用して表示できます。Firefox、Chrome、Safari などのブラウザでは、ダウンロードの最適な操作性が提供されます。

ホスト スキャン用のアンチウイルス アプリケーションの設定

アンチウイルス アプリケーションが、ポスチャ モジュールやホスト スキャン パッケージを含む一部のアプリケーションの動作を誤って悪意のあるものと判断する場合があります。ポスチャ モジュールまたはホスト スキャン パッケージをインストールする前に、以下のホスト スキャン アプリケーションをアンチウイルス ソフトウェアの「ホワイトリスト」に設定するか、セキュリティ例外を設けます。

- cscan.exe
- ciscod.exe
- cstub.exe

Dynamic Access Policies との統合

ASA では、ホスト スキャンの機能が Dynamic Access Policies（DAP）に統合されます。設定に応じて、ASA では、DAP 割り当ての条件として、オプションの AAA 属性値と組み合わせたエンドポイント属性値が 1 つ以上使用されます。DAP のエンドポイント属性でサポートされるホスト スキャンの機能には、OS 検出、プリログイン ポリシー、基本ホスト スキャン結果、およびエンドポイント アセスメントがあります。

（注） ホスト スキャンの機能をイネーブルにするには、AnyConnect Premium ライセンスを ASA にインストールする必要があります。

管理者は、セッションに DAP を割り当てるために必要な条件を構成する属性を、単独で、または組み合わせて指定できます。DAP により、エンドポイント AAA 属性値に適したレベルでネットワーク アクセスが提供されます。設定したエンドポイント条件がすべて満たされたときに、ASA によって DAP が適用されます。

ポスチャ モジュールとスタンドアロン ホスト スキャン パッケージの相違点

AnyConnect ポスチャ モジュールは、ASA を使用してエンドポイントに展開できます。または、エンドポイントが ASA への初期接続を行う前に、事前展開キットを使用してエンドポイントにインストールできます。

ポスチャ モジュールには、ホスト スキャン パッケージ、プリログイン評価、キーストローク ロガー検出、ホスト エミュレーション検出、キャッシュ クリーナ、およびホスト スキャン アプリケーションが必要とするいくつかのその他のモジュールが含まれます。ポスチャ モジュールを展開することにより、エンドポイントのユーザが管理者ではなくても、ホスト スキャンは特権動作を実行できます。また、その他の AnyConnect モジュールをホスト スキャンを使用して開始することもできます。

スタンドアロン ホスト スキャン パッケージは、ホスト スキャン エンジン、プリログイン評価モジュール、キーストローク ロガー検出、およびホスト エミュレーション検出を提供します。

AnyConnect ポスチャ モジュールの依存関係およびシステム要件

AnyConnect ポスチャ モジュールには、ホスト スキャン パッケージやその他のコンポーネントが含まれています。

依存関係

AnyConnect Secure Mobility Client をポスチャ モジュールとともに使用するには、最低でも次のような ASA コンポーネントが必要です。

- ASA 8.4
- ASDM 6.4

これらの AnyConnect 機能は、ポスチャ モジュールをインストールする必要があります。

- ホスト スキャン
- SCEP 認証
- AnyConnect テレメトリ モジュール

ホスト スキャン、CSD、および AnyConnect Secure Mobility Client の相互運用性

注意　ホスト スキャンを AnyConnect Secure Mobility Client バージョン 3.0.x で展開する場合、AnyConnect Secure Mobility Client は、同じバージョン番号、または自分よりも新しいバージョン番号のホスト スキャンが必要です。

Cisco Secure Desktop（CSD）バージョン 3.5 以前を ASA でイネーブルにしていて、展開している AnyConnect Secure Mobility Client 3.0.x のバージョンに一致するまたはそれ以降のホスト スキャン パッケージにアップグレードしない場合、プリログイン評価は失敗し、ユーザは VPN セッションを確立できません。ASA は、ASA でイネーブルにされているホスト スキャン パッケージに一致するように、エンドポイントのホスト スキャン パッケージを自動的にダウングレードするため、AnyConnect 3.0.x ポスチャ モジュールがエンドポイントに事前展開されていても、この問題は発生します。

AnyConnect 2.5.3005 以前の場合は、Host Scan と互換性がありません。

システム要件

ポスチャ モジュールは、以下のプラットフォームにインストールできます。

- Windows XP（x86 版、および x64 環境で動作する x86 版）
- Windows Vista（x86 版、および x64 環境で動作する x86 版）
- Windows 7（x86 版、および x64 環境で動作する x86 版）
- Mac OS X 10.5、10.6（32 ビット版、および 64 ビット環境で動作する 32 ビット版）
- Linux（32 ビット版、および 64 ビット環境で動作する 32 ビット版）

（注）　ホスト スキャンは、32 ビット アプリケーションで、コア 32 ビット ライブラリを 64 ビット版 Linux オペレーティング システムにインストールする必要があります。ホスト スキャンは、インストールされた時点で、これらの 32 ビット ライブラリを提供しません。まだプロビジョニングしていない場合、お客様は自分で 32 ビット ライブラリをエンドポイントにインストールする必要があります。

ライセンシング

ポスチャ モジュールには、以下の AnyConnect のライセンシング要件があります。

- AnyConnect Premium ライセンスは、基本ホスト スキャン、エンドポイント アセスメント、および Advanced Endpoint Assessment を含むホスト スキャンによって提供されるすべての機能に対して必要です。
- Advanced Endpoint Assessment ライセンスは、以下の機能が必要とする追加のライセンスです。

- 修復
- モバイル デバイス管理

Advanced Endpoint Assessment をサポートするためのアクティベーション キーの入力

Advanced Endpoint Assessment には、エンドポイント アセスメントのすべての機能が含まれており、バージョン要件を満たすために非準拠のコンピュータのアップデートを試行するように設定できます。次の手順に従い、Advanced Endpoint Assessment をサポートするために、シスコからキーを取得したら、ASDM を使用してキーのアクティベーションを行います。

ステップ 1　[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [アクティベーション キー（Activation Key）] を選択します。

ステップ 2　[新規アクティベーション キー（New Activation Key）] フィールドにキーを入力します。

ステップ 3　[アクティベーション キーの更新（Update Activation Key）] をクリックします。

ステップ 4　[ファイル（File）] > [実行コンフィギュレーションをフラッシュに保存する（Save Running Configuration to Flash）] を選択します。

Advanced Endpoint Assessment のエントリが表示され、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [ホスト スキャン（Host Scan）] ペインの [ホスト スキャン拡張（Host Scan Extensions）] の領域内の [設定（Configure）] ボタンが有効になります。[ホスト スキャン（Host Scan）] ペインは、CSD がイネーブルになっている場合に限りアクセスできます。

ホスト スキャン パッケージ

ASA へのホスト スキャン パッケージは次のいずれかの方法でロードできます。

- **hostscan-*version*-k9.pkg** は、スタンドアロン パッケージとしてアップロードできます。
- **anyconnect-win-*version*-k9.pkg** は、AnyeConnct Secure Mobility パッケージをアップロードすることにより、アップロードできます。
- **csd_version-k9.pkg** は、Cisco Secure Desktop パッケージをアップロードすることによってアップロードできます。

表 5-1　ASA にロードするホスト スキャン パッケージ

ファイル	説明
hostscan-*version*-k9.pkg	このファイルには、ホスト スキャン イメージ、ホスト スキャン サポート表、プリログイン評価モジュール、キャッシュ クリーナ、キーストローク ロガー検出、およびホスト エミュレーション検出が含まれます。
anyconnect-win-*version*-k9.pkg	このパッケージには、hostscan-*version*-k9.pkg ファイルに含まれるすべての Cisco AnyConnect Secure Mobility Client の機能が含まれます。

表 5-1　ASA にロードするホスト スキャン パッケージ

ファイル	説明
csd_*version*-k9.pkg	このファイルには、ホスト スキャン ソフトウェア、ホスト スキャン サポート表、Secure Desktop（Vault）、キャッシュ クリーナ、キーストローク ロガー検出、ホスト エミュレーション検出など、すべての Cisco Secure Desktop 機能が含まれます。

ASA 上に複数ロードされた場合にイネーブルになるホスト スキャン イメージ

ホスト スキャン イメージは、ホスト スキャン パッケージに同梱されます。このイメージは、スタンドアロン ホスト スキャン パッケージ、完全な AnyConnect Secure Mobility Client パッケージ、および Cisco Secure Desktop からエンドポイントに展開できます。ASA にインストールしたライセンスの内容によっては、ASA にこれらのすべてのパッケージをロードできます。この場合、ASA は、ホスト スキャン イメージとして最初に指定したイメージをイネーブルにします。1 つも指定しなかった場合、ASA は Cisco Secure Desktop からホスト スキャンの機能をイネーブルにします。「ホスト スキャンのインストールまたはアップグレード」（P.5-16）を参照してください。

ホスト スキャン パッケージをアンインストールすると、ASA はそのホスト スキャン イメージをイネーブルにできなくなります。

以下のシナリオは、複数ロードされた場合に、ASA が配布するホスト スキャン パッケージについて説明します。

- ASA にスタンドアロン ホスト スキャン パッケージをインストールし、それをホスト スキャン イメージとして指定して、CSD/hostscan をイネーブルにしている場合、ASA はスタンドアロン ホスト スキャン パッケージを配布します。
- ASA にスタンドアロン ホスト スキャン パッケージをインストールして、それをホスト スキャン イメージとして指定し、また ASA に CSD イメージをインストールして、CSD/hostscan をイネーブルにしている場合、ASA はスタンドアロン ホスト スキャン イメージを配布します。
- ASA にホスト スキャン イメージをインストールしたが、それをイネーブルにはせず、また ASA に CSD イメージをインストールして、CSD/hostscan をイネーブルにしている場合、ホスト スキャン イメージがアンインストールされていないため、ASA はスタンドアロン ホスト スキャン イメージを配布します。
- ASA に AnyConnect Secure Mobility Client パッケージをインストールし､それをホスト スキャン イメージとして指定した場合、ASA はそのパッケージからホスト スキャン イメージを配布します。
- ASA に AnyConnect Secure Mobility Client パッケージ ファイルをインストールしたが、それをホスト スキャン イメージとして指定しない場合、ASA はその AnyConnect パッケージに関連付けられたホスト スキャン パッケージを配布しません。ASA は、インストールされたホスト スキャン パッケージまたは CSD パッケージを配布し、提供される CSD はイネーブルにされます。

AnyConnect ポスチャ モジュールおよびホスト スキャンの展開

ポスチャ モジュールおよびホスト スキャンには、2 つの異なる展開シナリオがあります。

Pre-Deployment. 事前展開方式を使用する場合、エンドポイントが ASA への接続を確立しようとする前に、AnyConnect クライアントおよびポスチャ モジュールをインストールします。事前展開のポスチャ モジュール パッケージには、ポスチャ属性や「AnyConnect ポスチャ モジュールで使用可能な機能」（P.5-3）で説明されている機能を提供するアプリケーションを収集するために使用するすべてのコンポーネント、ライブラリ、およびサポート表が含まれています。ASA にインストールされている AnyConnect クライアントおよびポスチャ モジュールの同じバージョンをエンドポイントに事前展開する場合、エンドポイントが ASA に接続するときに、追加のポスチャ モジュールが ASA からプッシュされることはありません。

Web-Deployment. Web 展開方式を使用する場合、エンドポイントが ASA に接続するときに、ASA は AnyConnect クライアントおよびポスチャ モジュールをエンドポイントにプッシュします。可能な限り短時間かつ効率的にダウンロードを実行するために、ASA は必須のポスチャ モジュール ファイルのみをダウンロードします。

エンドポイントが再び接続するときに、必須のポスチャ モジュール ファイルが、エンドポイント アセスメントを実行するために必要な他のライブラリまたはファイルを判別し、それらのファイルを ASA から取得します。たとえば、ポスチャ モジュールは、Norton アンチウイルスのあるバージョンがエンドポイントで実行されているために、すべての Norton アンチウイルス ソフトウェアのホスト スキャン サポート表を取得する場合があります。ポスチャ モジュールは必要とする追加ファイルを取得した後、エンドポイント アセスメントを実行し、ASA に属性を転送します。エンドポイントの属性がダイナミック アクセス ポリシー（DAP）ルールを満たしていると、ASA はエンドポイントに接続を許可します。DAP を満たした結果に従って、ポスチャ モジュールの残りの部分をエンドポイントにプッシュするかどうかについて、ASA を設定できます。

ポスチャ モジュール全体をエンドポイントに Web 展開しない場合、1 つのポスチャ ファイルのみをエンドポイントにダウンロードする、またエンドポイント アセスメントを実行するために必要なホスト スキャン ライブラリのみを要求する制限付き Web 展開を実行できます。このシナリオでは、非常に短い時間で ASA からエンドポイントにダウンロードできますが、Advanced Endpoint Assessment を実行する機能やアンチウイルス、アンチスパイウェア、またはファイアウォールの修復タスクを実行する機能は使用できなくなります。

AnyConnect ポスチャ モジュールの事前展開

ポスチャ モジュールを事前展開する場合、AnyConnect クライアントが ASA への初期接続を行う前に、そのポスチャ モジュールをエンドポイントにインストールします。

ポスチャ モジュールをインストールする前に、AnyConnect Secure Mobility Client をエンドポイントにインストールする必要があります。Web 展開方式および事前展開方式を使用して、AnyConnect Secure Mobility Client およびポスチャ モジュールをインストールする手順については、第 2 章「AnyConnect Secure Mobility Client の展開」を参照してください。

表 5-2 では、ポスチャ モジュールの事前展開キットがリストされています。

表 5-2　ポスチャ モジュールの Pre-Deployment キット

ファイル	説明
Windows	anyconnect-posture-win-*version*-pre-deploy-k9.msi
Linux	anyconnect-linux-*version*-posture-k9.tar.gz
Mac OS X	anyconnect-macosx-posture-i386-*version*-i386-k9.dmg

ASA でのホスト スキャンのインストールおよびイネーブル化

以下のタスクでは、ASA 上でのホスト スキャンのインストールとイネーブル化について説明します。

- 最新のホスト スキャン エンジン更新のダウンロード
- ホスト スキャンのインストールまたはアップグレード
- ASA でのホスト スキャンのイネーブル化またはディセーブル化
- ホスト スキャンのアンインストール
- AnyConnect ポスチャ モジュールのグループ ポリシーへの割り当て

最新のホスト スキャン エンジン更新のダウンロード

最新の Cisco ホスト スキャン エンジンの更新をダウンロードするには、Cisco.com に登録されたユーザである必要があります。

ステップ 1　次のリンクをクリックして、Cisco VPN Client ツールのソフトウェア ダウンロード エリアに移動します。

http://www.cisco.com/cisco/software/release.html?mdfid=282414594&flowid=4470&softwareid=282364364&release=Engine%20Updates&relind=AVAILABLE&rellifecycle=&reltype=latest

ステップ 2　製品ディレクトリ ツリーの [最新リリース（Latest Releases）] を展開します。

ステップ 3　[エンジンの更新（Engine Updates）] をクリックします。

ステップ 4　右側の列で、**hostscan_3.0.xxxx-k9.pkg** の最新バージョンを探し、[今すぐダウンロード（Download Now）] をクリックします。

ステップ 5　cisco.com クレデンシャルを入力し、[ログイン（Login）] をクリックします。

ステップ 6　[ダウンロードに進む（Proceed with Download）] をクリックします。

ステップ 7　エンド ユーザ ライセンス契約書を読み、[同意（Agree）] をクリックします。

ステップ 8　ダウンロード マネージャ オプションを選択し、[ダウンロード（download）] リンクをクリックして、ダウンロードを続行します。

ホスト スキャンのインストールまたはアップグレード

以下の手順を使用して、ASA での新規ホスト スキャン イメージのアップロードまたはアップグレード、およびイネーブル化を実行します。このイメージを使用して、AnyConnect のホスト スキャンの機能をイネーブルにするか、または Cisco Secure Desktop（CSD）の既存の展開のホスト スキャン サポート表をアップグレードします。

スタンドアロン ホスト スキャン パッケージまたは AnyConnect Secure Mobility Client バージョン 3.0 以降のパッケージをフィールドに指定できます。

以前に、CSD イメージを ASA にアップロードしたことがある場合、指定するホストスキャン イメージは、その CSD パッケージに同梱されていた既存のホスト スキャン ファイルをアップグレードまたはダウングレードします。

ホスト スキャンをインストールまたはアップグレードした後に、セキュリティ アプライアンスを再起動する必要はありませんが、Adaptive Security Device Manager（ASDM）の Secure Desktop Manager ツールにアクセスするには、ASDM を終了して再起動する必要があります。

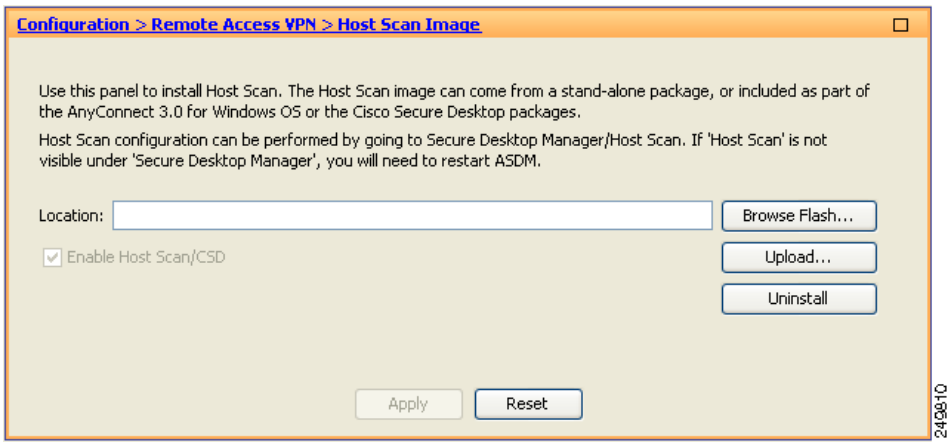
（注）　ホスト スキャンには、AnyConnect Secure Mobility Client Premium ライセンスが必要です。

ステップ 1　「最新のホスト スキャン エンジン更新のダウンロード」（P.5-15）を使用して、最新バージョンのホスト スキャン パッケージをダウンロードします。

（注）　ソフトウェアをダウンロードするには、Cisco.com のアカウントを使用してログインする必要があります。

ステップ 2　ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。ASDM は [ホスト スキャン イメージ（Host Scan Image）] パネル（図 5-3）を開きます。

図 5-3　ホスト スキャン イメージ パネル



ステップ 3　[アップロード（Upload）] をクリックして、ホスト スキャン パッケージのコピーをコンピュータから ASA のドライブに転送する準備を行います。

ステップ 4　[イメージのアップロード（Upload Image）] ダイアログボックスで [ローカル ファイルの参照（Browse Local Files）] をクリックし、ローカル コンピュータのホスト スキャン パッケージを検索します。

ステップ 5　手順 1 でダウンロードした **hostscan_*version*.pkg** ファイルまたは **anyconnect-win-*version*-k9.pkg** ファイルを選択し、[選択（Select）] をクリックします。選択したファイルへのパスは、[ローカル ファイルのパス（Local File Path）] フィールドに表示され、[フラッシュ ファイルのシステム パス（Flash File System Path）] フィールドには、ホスト スキャン パッケージの宛先パスが反映されます。ASA に複数のフラッシュ ドライブがある場合、[フラッシュ ファイルのシステム パス（Flash File System Path）] を編集して別のフラッシュ ドライブを指定できます。

ステップ 6　[ファイルのアップロード（Upload File）] をクリックします。ASDM によって、ファイルのコピーがフラッシュ カードに転送されます。[情報（Information）] ダイアログボックスには、次のメッセージが表示されます。

```
File has been uploaded to flash successfully.
```

ステップ 7　[OK] をクリックします。

ステップ 8　[アップロードしたイメージの使用（Use Uploaded Image）] ダイアログで [OK] をクリックして、現在のイメージとしてアップロードしたホスト スキャン パッケージ ファイルを使用します。

ステップ 9　[ホスト スキャン/CSD の有効化（Enable Host Scan/CSD）] がまだオフになっている場合、オンにします。

ステップ 10　[適用（Apply）] をクリックします。

（注）　ASA 上で AnyConnect Essentials がイネーブルになっている場合、ホスト スキャンおよび CSD は AnyConnect Essentials では機能しないというメッセージが表示されます。AnyConnect Essentials を**ディセーブル**にするか、**保持**するかを選択します。

ステップ 11　[保存（Save）] をクリックします。

ASA でのホスト スキャンのイネーブル化またはディセーブル化

ASDM を使用してホスト スキャン イメージを最初にアップロードまたはアップグレードするときに、その手順の一環としてイメージをイネーブルにします。「ASA でのホスト スキャンのインストールおよびイネーブル化」（P.5-15）を参照してください。

それ以外の場合、ASDM を使用してホストスキャン イメージをイネーブルまたはディセーブルにするには、以下の手順に従います。

ステップ 1　ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。ASDM は [ホスト スキャン イメージ（Host Scan Image）] パネル（図 5-3）を開きます。

ステップ 2　[ホスト スキャン/CSD の有効化（Enable Host Scan/CSD）] をオンにして、ホスト スキャンをイネーブルにする、または [ホスト スキャン/CSD の有効化（Enable Host Scan/CSD）] をオフにしてホスト スキャンをディセーブルにします。

ステップ 3　[適用（Apply）] をクリックします。

ステップ 4　[保存（Save）] をクリックします。

ASA 上での CSD の有効化または無効化

Cisco Secure Desktop（CSD）をイネーブルにすると、CSD 設定ファイルおよび data.xml がフラッシュ デバイスから実行コンフィギュレーションにロードされます。CSD をディセーブルにしても、CSD 設定は変更されません。

次の手順に従い、ASDM を使用して CSD をイネーブルまたはディセーブルにします。

ステップ 1　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [設定（Setup）] を選択します。

ASDM によって、[設定（Setup）] ペインが開きます（図 5-3）。

（注）　[Secure Desktop イメージ（Secure Desktop Image）] フィールドに現在インストールされているイメージ（およびバージョン）が表示されます。[Secure Desktop の有効化（Enable Secure Desktop）] チェックボックスは、CSD がイネーブルになっているかどうかを示します。

ステップ 2　[Secure Desktop の有効化（Enable Secure Desktop）] をオンにして CSD をイネーブルにするか、[Secure Desktop の有効化（Enable Secure Desktop）] をオフにして CSD をディセーブルにします。

ステップ 3　[ASDM] を閉じます。次のメッセージがウィンドウに表示されます。

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

ステップ 4　[保存（Save）] をクリックします。ASDM は設定を保存して閉じます。

ホスト スキャンおよび CSD のアップグレードとダウングレード

ASA は、イネーブルにされたホスト スキャン パッケージがスタンドアロン ホスト スキャン パッケージ、AnyConnect Secure Mobility Client に含まれるパッケージ、または Cisco Secure Desktop に含まれるパッケージであるかにかかわらず、そのパッケージをエンドポイントに自動的に配布します。エンドポイントに古いバージョンのホスト スキャン パッケージがインストールされている場合、エンドポイントのそのパッケージはアップグレードされます。エンドポイントに新しいバージョンのホスト スキャン パッケージがある場合、エンドポイントのそのパッケージはダウングレードされます。

ASA でイネーブルにされたホスト スキャン イメージの判別

ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。

[ホスト スキャン イメージ（Host Scan Image）] ロケーション フィールドにホスト スキャン イメージが指定されていて、[ホスト スキャン/CSD の有効化（Enable HostScan/CSD）] ボックスがオンの場合、そのイメージのバージョンが ASA によって使用されるホスト スキャンのバージョンになります。

[ホスト スキャン イメージ（Host Scan Image）] フィールドが空で、[ホスト スキャン/CSD の有効化（Enable HostScan/CSD）] ボックスがオンの場合、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] を選択します。[Secure Desktop イメージのロケーション（Secure Desktop Image Location）] フィールドの CSD のバージョンが、ASA によって使用されるホスト スキャンのバージョンになります。

ホスト スキャンのアンインストール

ホスト スキャン パッケージのアンインストール

ホスト スキャン パッケージをアンインストールすると、ASDM インターフェイス上のビューから削除されます。これにより、ホスト スキャンまたは CSD がイネーブルの場合でも ASA によってホスト スキャン パッケージは展開されません。ホスト スキャンをアンインストールしても、ホスト スキャン パッケージはフラッシュ ドライブから削除されません。

以下の手順を使用して、セキュリティ アプライアンスでホスト スキャンをアンインストールします。

ステップ 1　ASDM を開いて [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ホスト スキャン イメージ（Host Scan Image）] を選択します。

ステップ 2　[ホスト スキャン イメージ（Host Scan Image）] ペインで、[アンインストール（Uninstall）] をクリックします。ASDM はテキストを [ロケーション（Location）] テキスト ボックスから削除します。

ステップ 3　[保存（Save）] をクリックします。

ASA からの CSD のアンインストール

Cisco Secure Desktop（CSD）をアンインストールすると、**フラッシュ カード上のデスクトップ ディレクトリから CSD 設定ファイルおよび data.xml が削除されます**。このファイルを保存する場合は、CSD をアンインストールする前に、別の名前を使用してファイルをコピーするか、ワークステーションにダウンロードします。

以下の手順を使用して、セキュリティ アプライアンスで CSD をアンインストールします。

ステップ 1　ASDM を開き、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [設定（Setup）] を選択します。

ASDM によって、[設定（Setup）] ペインが開きます（図 5-3）。

ステップ 2　[アンインストール（Uninstall）] をクリックします。

次のメッセージが確認ウィンドウに表示されます。

```
Do you want to delete disk0:/csd_<n>.<n>.*.pkg and all CSD data files?
```

ステップ 3　[はい（Yes）] をクリックします。

ASDM によって、[ロケーション（Location）] テキスト ボックスからテキストが削除され、[設定（Setup）] の下にある [Secure Desktop Manager] メニュー オプションが削除されます。

ステップ 4　[ASDM] を閉じます。次のメッセージがウィンドウに表示されます。

```
The configuration has been modified. Do you want to save the running configuration to
flash memory?
```

ステップ 5　[保存（Save）] をクリックします。ASDM は設定を保存して閉じます。

AnyConnect ポスチャ モジュールのグループ ポリシーへの割り当て

ステップ 1　ASDM を開き、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] を選択します。

ステップ 2　[グループ ポリシー（Group Policies）] パネルで、[追加（Add）] をクリックし、新規グループ ポリシーを作成するか、ホスト スキャン パッケージを割り当てるグループ ポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3　[内部グループ ポリシーの編集（Edit Internal Group Policy）] パネルで、パネルの左側にある [詳細（Advanced）] ナビゲーション ツリーを拡張し、[AnyConnect クライアント（AnyConnect Client）] を選択します。

ステップ 4　[ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] の [継承（Inherit）] チェックボックスをオフにします。

ステップ 5　[ダウンロードするオプションのクライアント モジュール（Optional Client Modules to Download）] ドロップダウン メニューで、[AnyConnect Posture モジュール（AnyConnect Posture Module）] をオンにし、[OK] をクリックします。

ステップ 6　[OK] をクリックします。

ホスト スキャン ロギング

ホスト スキャンは、Windows プラットフォームの場合イベント ビューアに、また Windows プラットフォーム以外の場合 syslog にログを記録します。イベント ビューアでは、すべてのログは、独自の「Cisco AnyConnect Secure Mobility Client Posture」フォルダに保存されます。

すべてのポスチャ モジュール コンポーネントのロギング レベルの設定

デフォルトでは、ポスチャ モジュールのコンポーネントは、「Error」重大度レベルのイベントをログに記録します。以下の手順を使用して、ポスチャ モジュールのすべてのコンポーネントのロギング重大度レベルを変更します。

ポスチャ モジュールは、ユーザのホーム フォルダに cscan.log ファイルをインストールします。cscan.log ファイルには、最後の VPN セッションからのエントリだけが表示されます。ユーザが ASA に接続するたびに、ホスト スキャンでは新しいロギング データでこのファイルのエントリを上書きします。

ポスチャのロギング レベルを表示または変更するには、次の手順に従います。

ステップ 1　ASDM インターフェイスから、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [Secure Desktop Manager] > [グローバル設定（Global Settings）] を選択します。[グローバル設定（Global Settings）] パネルが開きます。

ステップ 2　パネル内の [ロギング レベルの定義（Logging Level Definitions）] を参考に、[ロギング レベル（Logging Level）] を設定します。

ステップ 3　実行コンフィギュレーションに加えられた変更を保存するには、[すべて適用（Apply All）] をクリックします。

（注）　特定の接続プロファイルに対してホスト スキャンがディセーブルになっている場合、その接続プロファイルを使用しているユーザにはホスト スキャンのロギングは実行されません。

ポスチャ モジュールのログ ファイルと場所

ポスチャ モジュール コンポーネントは、ご使用のオペレーティング システム、特権レベル、および起動メカニズム（Web 起動または AnyConnect）に基づいて、以下の 3 つのログに出力します。

- cstub.log：AnyConnect Web 起動が使用されると、ロギングをキャプチャします。
- libcsd.log：ホスト スキャン API を使用する AnyConnect スレッドによって作成されます。ログ レベル設定に応じて、このログにデバッグのエントリが入力される場合があります。
- cscan.log：スキャニング実行可能ファイル（cscan.exe）によって作成され、ポスチャおよびホスト スキャンのメイン ログになります。ログ レベル設定に応じて、このログにデバッグのエントリが入力される場合があります。

ポスチャ モジュールは、これらのログ ファイルをユーザのホーム フォルダに配置します。場所は、オペレーティング システムおよび VPN 方式によって異なります。

Cisco Technical Assistant Center（TAC）では、必要が生じた場合に、これらのログ ファイルを使用して問題のデバッグを行います。お客様がこれらのファイルを確認する必要はありません。Cisco TAC では、これらのログ ファイルを必要とする場合に、DART バンドルを使用してそれらのファイルを提供するようにお客様に依頼することがあります。DART ユーティリティは、すべての AnyConnect 設定およびログ ファイルを収集し、TAC に送信することになる圧縮ファイルにそれらのログ ファイルを保存します。DART 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.12-4）を参照してください。

Lua 表現での BIOS シリアル番号の使用

ホスト スキャンは、ホストの BIOS シリアル番号を取得できます。ダイナミック アクセス ポリシー（DAP）を使用し、その BIOS シリアル番号に基づいて ASA への VPN 接続を許可または拒否できます。

Lua 表現での BIOS の表現

これは、ASDM の [ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] 画面の [詳細（Advanced）] フィールドで使用できる Lua 論理式です。

endpoint.device.id=***BIOSSerialNumber***

ここで、***BIOSSerialNumber*** は、ASA への接続を試行するハードウェア デバイスの BIOS シリアル番号を表します。この文字列は可変長文字列で、通常、OS 固有の文字列です。

DAP エンドポイント属性としての BIOS の指定

ステップ 1　ASDM にログオンします。

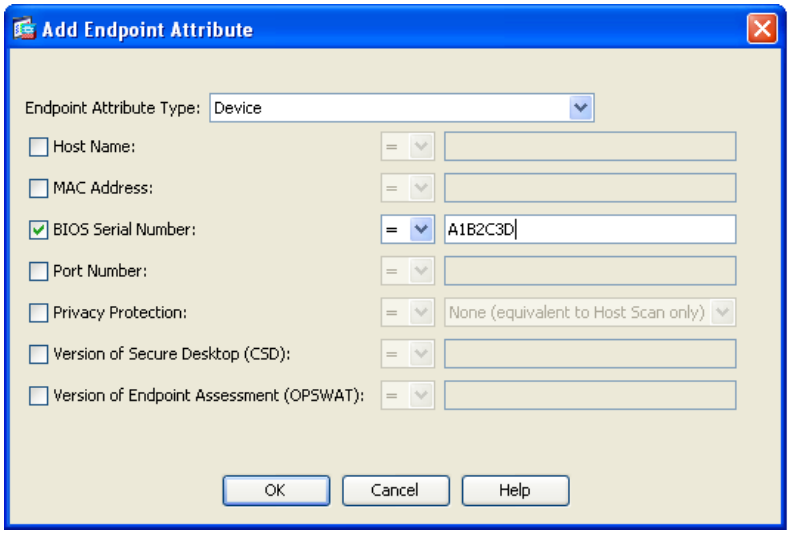
ステップ 2　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] を選択するか、[クライアントレス SSL VPN アクセス（Clientless SSL VPN Access）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] を選択します。

ステップ 3　[ダイナミック アクセス ポリシーの設定（Configure Dynamic Access Policies）] パネルで、[追加（Add）] または [編集（Edit）] をクリックして、BIOS を DAP エンドポイント属性として設定します。

ステップ 4　エンドポイント ID 表の右にある [追加（Add）] をクリックします。

ステップ 5　[エンドポイント属性タイプ（Endpoint Attribute Type）] フィールドで、[デバイス（Device）] を選択します。

ステップ 6　[BIOS シリアル番号（BIOS Serial Number）] チェックボックスをオンにし、[=]（等しい）または [!=]（等しくない）を選択して、[BIOS シリアル番号（BIOS Serial Number）] フィールドに BIOS 番号を入力します。



ステップ 7　[OK] をクリックし、[エンドポイント属性（Endpoint Attribute）] ダイアログボックスでの変更を保存します。

ステップ 8　[OK] をクリックして、[ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] への変更を保存します。

ステップ 9　[適用（Apply）] をクリックして、ダイナミック アクセス ポリシーへの変更を保存します。

ステップ 10　[保存（Save）] をクリックします。

BIOS シリアル番号の取得方法

以下のリソースは、さまざまなエンドポイントで BIOS シリアル番号を取得する方法を説明しています。

- Windows：http://support.microsoft.com/kb/558124
- Mac OS X：http://support.apple.com/kb/ht1529
- Linux：次のコマンドを使用します。

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

その他の重要な資料

ホスト スキャンがエンドポイント コンピュータからポスチャ クレデンシャルを収集した後は、情報を活用するために、ユーザはプリログイン ポリシーの設定、ダイナミック アクセス ポリシーの設定、Lua の式の使用などのサブジェクトを理解する必要があります。

これらの内容については、次のマニュアルで詳しく説明します。

- 『Cisco Secure Desktop Configuration Guides』
- 『Cisco Adaptive Security Device Manager Configuration Guides』

- ホスト スキャンによってサポートされるアンチウイルス、アンチスパイウェア、およびファイアウォールのアプリケーションのリスト