CHAPTER 7

WSA に対する AnyConnect テレメトリの設定

AnyConnect Secure Mobility Client 用の AnyConnect テレメトリ モジュールでは、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。この Web フィルタリング インフラストラクチャでは、Web セキュリティ スキャニング アルゴリズムの強化、URL カテゴリと Web レピュテーション データベースの精度の向上、最終的な URL フィルタリング ルールの改良のために、このデータを使用します。

AnyConnect テレメトリ モジュールは、次の機能を実行します。

- エンドポイントでコンテンツの到着を監視します。
- 可能であれば、エンドポイントで受信する任意のコンテンツの発信元を識別および記録します。
- 悪意のあるコンテンツの検出およびその発信元を、シスコの Threat Operations Center にレポートします。
- 24 時間ごとに ASA を調べて、更新されたホスト スキャン イメージを確認します。更新されたホスト スキャン イメージが提供されている場合は、イメージをエンドポイントにダウンロードします。

ここでは、次の項目について説明します。

- システム要件
- AnyConnect テレメトリ モジュールのインストール
- AnyConnect テレメトリ モジュールの相互運用性
- テレメトリ アクティビティ履歴リポジトリ
- テレメトリのレポート
- テレメトリ クライアント プロファイルの設定
- 設定プロファイルの階層

システム要件

AnyConnect テレメトリ モジュール（以降、「テレメトリ モジュール」）は、以下のプラットフォームで実行されている、このリリースの AnyConnect Secure Mobility Client で使用可能です。

- Windows 7（x86（32 ビット）および x64（64 ビット））
- SP2 を適用した Windows Vista（x86（32 ビット）および x64（64 ビット））
- Windows XP SP3（x86（32 ビット）および x64（64 ビット））

テレメトリ モジュールでは、Internet Explorer 7、Internet Explorer 8 など、**wininit.dll** を使用するブラウザについてのみ、URL 発信元のトレースを実行できます。Firefox、Chrome など **wininit.dll** を使用しないブラウザを使用してファイルをダウンロードした場合、ファイルのダウンロードに使用されたブラウザは識別できますが、ファイルのダウンロード元の URL は識別できません。

テレメトリ モジュールを使用するには、AnyConnect ポスチャ モジュールでサポートしているアンチウイルス アプリケーションをエンドポイントにインストールする必要があります。

（注）　AnyConnect ポスチャ モジュールは、CSD に付属しているイメージと同じホスト スキャン イメージを含みます。ホスト スキャンでサポートされるアンチウイルス、アンチスパイウェア、ファイアウォール アプリケーションのリストは、AnyConnect と CSD で同一です。

ASA と ASDM に関する要件

AnyConnect Secure Mobility Client をテレメトリ 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 が 6.3.1

AnyConnect Secure Mobility Client モジュールに関する要件

テレメトリ モジュールは AnyConnect Secure Mobility Client のアドオンであり、以下のモジュールを以下の順序でエンドポイントにインストールする必要があります。

1. AnyConnect VPN モジュール
2. AnyConnect ポスチャ モジュール
3. AnyConnect テレメトリ モジュール

Cisco IronPort Web セキュリティ アプライアンスの相互運用性に関する要件

テレメトリ機能は、Cisco IronPort Web セキュリティ アプライアンス（WSA）と組み合わせて AnyConnect セキュア モビリティ ソリューションを使用している場合のみイネーブルにできます。WSA を使用するには、WSA セキュア モビリティ ソリューション ライセンスが必要です。必要な WSA の最小バージョンは 7.1 です。

AnyConnect テレメトリ機能を使用するには、セキュア モビリティ ソリューションを適切に設定しておく必要があります。まだ設定していない場合は、「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）を参照し、説明に従って、WSA と適切に連携するように ASA を設定してください。

Cisco IronPort Web セキュリティ アプライアンス上での SenderBase のイネーブル化

テレメトリ モジュールでは、Threat Operations Center に転送したり、他の脅威情報と集約したりできるように、ウイルス攻撃のインシデント情報およびアクティビティ情報を WSA に送信します。これを行うには、WSA で、標準モードの SenderBase ネットワーク参加がイネーブルになっている必要があります。

以下は、SenderBase セキュリティ サービスをイネーブルにする手順の概略です。SenderBase セキュリティ サービスの詳細な説明については、WSA のマニュアルを参照してください。

1. Web ブラウザを使用して、WSA 管理者 GUI にログインします。
2. [セキュリティ サービス（Security Services）] > [SenderBase] を選択します。
3. SenderBase ネットワーク参加がディセーブルの場合は、[有効（Enable）] をクリックしてから [グローバル設定の編集（Edit Global Settings）] をクリックして、参加レベルを設定します。標準（フル）参加をお勧めします。

（注）　制限付き参加レベルと標準参加レベルの違いの詳細については、『*IronPort AsyncOS for Web User Guide*』を参照してください。

4. 変更を送信し、保存します。

AnyConnect テレメトリ モジュールのインストール

テレメトリ モジュールをインストールする前に、エンドポイントに AnyConnect Secure Mobility Client および AnyConnect 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。Web 展開方式および事前展開方式を使用してテレメトリ 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。テレメトリ モジュールを展開する基本手順のみを知りたい場合は、AnyConnect テレメトリ モジュールの高速展開を参照してください。

テレメトリ モジュールをインストールすると、開始されるすべての新規プロセスについて、アクションの記録が即座に開始されます。ただし、テレメトリ モジュールでは、モジュールをインストールする前からコンピュータ上で実行されていたプロセスのアクションは記録できません。

テレメトリ モジュールのインストール後、ユーザがログアウトしてログインし直すまでは、ファイルのコピーや名前変更など、Windows エクスプローラ（explorer.exe）のプロセスはテレメトリ モジュールによって追跡されません。さらに、テレメトリ モジュールでは、ユーザがコンピュータをリブートしないうちは、ユーザ ログインの前に開始された他のプロセスのアクションを記録できません。

（注）　要件ではありませんが、テレメトリ モジュールのインストール後にエンドポイントをリブートすることを、強くお勧めします。

AnyConnect テレメトリ モジュールの高速展開

AnyConnect とともにテレメトリ モジュールを展開する場合に実行する必要のある手順の概略を以下に示します。この手順は、グループ ポリシーおよび AnyConnect VPN ユーザ用の接続プロファイルをすでに設定してあることを前提としています。AnyConnect テレメトリ モジュールを展開するには、次の手順を実行します。

ステップ 1　Cisco.com から AnyConnect Windows パッケージをダウンロードします。このファイルは、次の命名規則に従っています。anyconnect-win-<*version*>-k9.pkg

ステップ 2　AnyConnect Windows パッケージを ASA にアップロードします。

a. ASDM を起動し、[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）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します。

b. [追加（Add）] をクリックします。

c. AnyConnect Windows パッケージを ASDM に**アップロード**します。プロンプトが表示されたら、AnyConnect パッケージを現在の新しいイメージとして使用するために、[OK] をクリックします。

d. [OK] をクリックします。[適用（Apply）] をクリックします。

e. **ASDM** を再起動します。

ステップ 3　AnyConnect パッケージをホスト スキャン パッケージに指定し、ホスト スキャンをイネーブルにします。

a. ASDM で、[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。

b. [フラッシュの参照（Browse Flash）] をクリックし、前のステップでホスト スキャン イメージとしてアップロードした anyconnect-win-<*version*>-k9.pkg を選択します。

c. [ホスト スキャン /CSD の有効化（Enable Host Scan/CSD）] をオンにします。

d. [適用（Apply）] をクリックします。

e. **ASDM** を再起動します。

（注）　このステップを実行すると、クライアントレス SSL VPN アクセスのホスト スキャンもイネーブルになります。

ステップ 4　テレメトリをオプション モジュールとして展開するように、グループ ポリシーを設定します。

a. ASDM で、[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、編集するグループ ポリシーを選択して [編集（Edit）] をクリックします。

b. [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] の順に選択します。

c. [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）] オプションの [継承（Inherit）] チェックボックスをオフにします。ドロップダウン ボックスから、[AnyConnect テレメトリ（AnyConnect Telemetry）] および [AnyConnect ポスチャ（AnyConnect Posture）] を選択します。

d. [OK] をクリックします。[適用（Apply）] をクリックします。[保存（Save）] をクリックします。

ステップ 5　ここで設定したグループ ポリシーを指定する接続プロファイルを設定します。

a. ASDM で、[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）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択し、テレメトリ用に設定する接続プロファイルを選択します。[編集（Edit）] をクリックします。[Basic] 設定パネルが自動的に開きます。

b. [デフォルト グループ ポリシー（Default Group Policy）] エリアで、前のステップでテレメトリの展開用に設定したグループ ポリシーを選択します。

c. [OK] をクリックします。[適用（Apply）] をクリックします。[保存（Save）] をクリックします。

ステップ 6　テレメトリ クライアント プロファイルを作成し、テレメトリをイネーブルにします。

a. ASDM で、[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）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します。

b. [追加（Add）] をクリックしてテレメトリ プロファイルを作成します。プロファイルに名前を付け、[プロファイルの使用（Profile Usage）] フィールドで [テレメトリ（Telemetry）] を選択します。

c. [グループ ポリシー（Group Policy）] フィールドで、テレメトリの展開用に作成したグループ ポリシーをオプション モジュールとして選択します。[OK] をクリックします。

d. [プロファイル名（Profile Names）] リストから、ここで作成したテレメトリ クライアント プロファイルを選択し、[Edit] をクリックします。

e. [テレメトリ サービス（Telemetry Policy）] パネルの [サービスの有効化（Enable Service）] をクリックし、テレメトリ クライアント プロファイルに対するすべてのデフォルト値を受け入れます。

f. [OK] をクリックします。[適用（Apply）] をクリックします。[保存（Save）] をクリックします。

ステップ 7　セキュア モビリティ ソリューションをイネーブルにします。

a. ASDM で、[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）] > [セキュア モビリティ ソリューション（Secure Mobility Solution）] を選択します。

b. [サービスの設定（Service Setup）] エリアで、[モバイル ユーザ セキュリティ サービスの有効化（Enable Mobile User Security Service）] をオンにします。

c. [適用（Apply）] をクリックします。[保存（Save）] をクリックします。

AnyConnect テレメトリ モジュールの相互運用性

この項では、テレメトリ モジュールと他の AnyConnect Secure Mobility Client コンポーネントの対話について説明します。

- AnyConnect VPN モジュール
- AnyConnect ポスチャ モジュール
- サードパーティ製アンチウイルス ソフトウェア

AnyConnect VPN モジュール

AnyConnect VPN モジュールでは、以下の方法でテレメトリ モジュールと対話します。

- AnyConnect の VPN サービス プロセスは、サービスの開始時に、他のすべてのプラグイン モジュールとともに、テレメトリ モジュールのロードと初期化を行います。
- AnyConnect VPN モジュールでは、状態が変化したときに、セッション状態情報および AnyConnect Secure Mobility（ACSM）状態情報を提供します。
- AnyConnect VPN モジュールでは、WSA からテレメトリ設定を取得するための、WSA からのセキュア モビリティ サービス ステータス応答の XML を用意します。

これ以外に、テレメトリ モジュールと VPN モジュールとの対話はほとんどなく、VPN モジュールがテレメトリ モジュールをシャットダウンするか、VPN プロセスが終了するまで、独立してを実行されます。

AnyConnect ポスチャ モジュール

AnyConect ポスチャ モジュール（以降「ポスチャ モジュール」）は、ホスト スキャン イメージを含みます。ホスト スキャン イメージは、ホスト スキャン互換のアンチウイルス ソフトウェアからのウイルス検出情報をテレメトリ モジュールに渡します。ホスト スキャンでは、テレメトリ レポートで必要な場合、システム ポスチャ情報を AnyConnect テレメトリ モジュールに渡すこともできます。

テレメトリ モジュールでは、24 時間ごとに ASA を調べて更新されたホスト スキャン イメージを確認します。更新されたホスト スキャン イメージが ASA にインストールされている場合、テレメトリ モジュールはイメージを取得して、更新をエンドポイントに自動的にインストールします。

サードパーティ製アンチウイルス ソフトウェア

AnyConnect テレメトリ モジュールを使用するには、ウイルスおよびマルウェアを検出する、ホスト スキャン準拠のアンチウイルス アプリケーションが必要です。ホスト スキャンでは、アンチウイルス アプリケーションの脅威ログを定期的に確認し、ウイルス検出インシデントをテレメトリ モジュールに転送します。

アンチウイルス アプリケーションの脅威ログは、常にイネーブルにされている必要があります。そうでない場合、ホスト スキャンでは、テレメトリ レポートをトリガーできません。

テレメトリ アクティビティ履歴リポジトリ

テレメトリ アクティビティ履歴リポジトリは、テレメトリ モジュールでアクティビティ ファイルを保存する、エンドポイント上のディレクトリです。アクティビティ履歴リポジトリは次の場所にあります。

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Telemetry\data\

テレメトリ モジュールでは、システム操作、ユーザ操作、API 関数呼び出しを代行受信します。テレメトリ モジュールでは、これらの情報を使用して、エンドポイントに着信するコンテンツの発信元を識別できます。テレメトリ モジュールでは、Internet Explorer（iexplorer.exe）による URL からのファイルのダウンロード、Windows エクスプローラ（explorer.exe）によるリムーバブル デバイスからのファイルのコピーなど、アプリケーション アクティビティに、この情報を集約します。

テレメトリ モジュールは、このアクティビティを収集し、activity.dat ファイルに記録します。activity.dat ファイルが、アクティビティ履歴ファイルです。

activity.dat ファイルのサイズがほぼ 1 MB になると、テレメトリ モジュールは、保存時点のタイムスタンプを名前とする新しいファイル、たとえば、20110114111312430.dat として、現在の activity.dat ファイルを保存します。テレメトリ モジュールは、次に、引き続き最新のアクティビティ履歴を保存する、新しい activity.dat ファイルを作成します。

アクティビティ履歴リポジトリが一定のサイズに達すると、テレメトリ モジュールは、一番古いアクティビティ履歴ファイルを削除します。アクティビティ履歴リポジトリのサイズは、テレメトリ プロファイルに設定されている [Maximum History Log] 変数によって管理されます。一定期間が経過したアクティビティ履歴ファイルは、テレメトリ モジュールによって、アクティビティ履歴リポジトリから削除されます。アクティビティ履歴ファイルの存続期間は、テレメトリ プロファイルに設定されている [Maximum History (Days)] 変数によって定義されます。これらの変数の設定手順については、「テレメトリ クライアント プロファイルの設定」（P.7-10）を参照してください。

（注）　テレメトリ モジュールでは、winnit.dll、Kerel32.dll などの Windows 関数からアクティビティ情報を受信します。これらの関数を使用していないブラウザまたは電子メール アプリケーションの場合、テレメトリ モジュールでは、いずれのアクティビティ データも受信しません。したがって、テレメトリ モジュールでは、Firefox、Chrome などのブラウザからアクティビティ履歴を受信しません。

（注）　アクティビティ履歴リポジトリに保存されている URL は、機密情報であると見なされます。テレメトリ モジュールは、これらの URL を暗号化して不正アクセスを防止します。詳細については、「URL の暗号化」（P.7-9）を参照してください。

テレメトリのレポート

テレメトリ レポートは、ローカル アンチウイルス ソフトウェアによって識別されたウイルスに関する情報およびエンドポイントをウイルスから保護するためにアンチウイルス ソフトウェアが実行したアクションに関する情報を含みます。テレメトリ モジュールは、レポートを暗号化して WSA に送信します。WSA は、このレポートを Cisco Threat Operations Center（TOC）に転送します。TOC では、このレポートを他のレポートと組み合わせて、新しい URL フィルタとマルウェア フィルタ エンジンの更新を生成し、すべての WSA に配布します。

各テレメトリ レポートは、インシデント セクション 1 つと、それに続く 1 つ以上のアクティビティ セクションを持ちます。インシデント セクションは、マルウェア、ローカル アンチウイルス アプリケーション、マルウェアから防御するために実行されたアクション、エンドポイントのシステム情報に関する情報を含みます。アクティビティ セクションは、インシデントにつながったアクティビティおよびウイルスの発信元の候補に関する情報を含みます。

エンドポイントがバーチャル プライベート ネットワークを介して ASA に接続されている場合、テレメトリ モジュールでは、ASA を介して、WSA に即座にレポートを送信します。WSA へのレポートの送信を終えたテレメトリ モジュールは、ローカル コピーを削除します。

エンドポイントが VPN を介して ASA に接続されていない場合、テレメトリ モジュールでは、エンドポイント上の次の場所にレポートを保存します。

%ALLUSERSPROFILE%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Telemetry\reports\

テレメトリ レポート ファイル名には、レポートの作成時刻の年月日、時間、分、秒を反映する、**YYYYMMDDHHSSmmm.trt** という命名規則が使用されます。

（注）　テレメトリ レポートに保存されている URL は、機密情報であると見なされます。テレメトリ モジュールは、これらの URL を暗号化して不正アクセスを防止します。詳細については、「URL の暗号化」（P.7-9）を参照してください。

テレメトリ モジュールによる個人情報の移動の可能性

テレメトリ インシデント レポートは、マルウェアの名前に加え、ローカル システム上でマルウェアが検出された場所も含みます。この場所であるディレクトリ パスは、多くの場合、マルウェアをダウンロードしたユーザのユーザ ID を含みます。たとえば、Jonathan Doe が「malware.txt」をダウンロードした場合、テレメトリ レポートに含まれるディレクトリ名は、「C:\Documents and Settings**jdoe**\Local Settings\Temp\Cookies**jdoe**@malware[1].txt」のようになります。

（注）　シスコのエンド ユーザ ライセンス契約書に同意してテレメトリ モジュールをインストールすると、シスコによる個人情報および非個人情報の収集、使用、処理、保管に同意することになります。この個人情報と非個人情報は、ユーザによるシスコ製品との対話方法をシスコが知るためや、ネットワーク処理の技術サポートの提供とシスコの製品とサービスの改良を目的として、シスコに転送されます。これには、米国や欧州経済領域外のその他の国に対するこれらの情報の転送を含みます。シスコは、選ばれた第三者と、匿名化して集約された形式で、この情報を共有することがあります。この個人情報および非個人情報を使用して、個人の特定や問い合わせを行うことはありません。これらの個人情報および非個人情報の使用には、シスコのプライバシー ポリシー（http://www.cisco.com/web/siteassets/legal/privacy.html）が適用されます。個人情報および非個人情報の収集、使用、処理、保管に関するこの同意は、テレメトリ モジュールをオフにするか、テレメトリ モジュールをアンインストールすることにより、随時撤回できます。

テレメトリのワークフロー

以下の手順は、テレメトリ モジュールによる情報の収集方法と WSA へのレポート方法の一例を示します。

1. ユーザが Web サイト **http://www.unabashedevil.com** を開き、圧縮ファイル **myriad_evils.zip** をダウンロードします。テレメトリ モジュールは、両方のアクティビティを記録し、activity.dat に保存します。
2. 少し経ってから、ユーザが圧縮ファイルから内容の **evil_virus.exe** を解凍します。テレメトリ モジュールは、このアクティビティを記録し、activity.dat に保存します。
3. ホスト スキャン準拠のアンチウイルス アプリケーションが **evil_virus.exe** に含まれているウイルスを識別し、ファイルを削除します。アンチウイルス アプリケーションのアクティビティを契機として、テレメトリ モジュールは、このインシデントに関するレポートを作成します。
4. テレメトリ モジュールは、この時点で activity.dat ファイル内の情報をさかのぼりながら処理して、ウイルスの発信元を判別します。テレメトリ モジュールでは、アンチウイルス アプリケーション インシデントから、**evil_virus.exe** がウイルスであったこと、およびアンチウイルス アプリケーションによって削除されたことを確認します。テレメトリ モジュールは、activity.dat ファイルから、**evil_virus.exe** が **myriad_evils.zip** から解凍されたことおよびこの圧縮ファイルは **http://www.unabashedevil.com** からダウンロードされたことを確認します。

   このすべての情報が、1 つのレポートに結合されます。
5. テレメトリ モジュールは、テレメトリ レポートを WSA に転送します。
   - エンドポイントがバーチャル プライベート ネットワークを介して ASA に接続されている場合、テレメトリ モジュールでは、レポートを即座に WSA に送信し、レポートのローカル コピーを削除します。
   - エンドポイントが VPN を介して ASA に接続されていない場合、テレメトリ モジュールは、レポート リポジトリにレポートを保存し、次回チャンスのあるときに WSA に送信します。
6. SenderBase ネットワークへの参加がイネーブルの場合、WSA では、Threat Operations Center にレポートを転送します。そこで、他の情報源からのデータと合わせて、この情報が分析されます。WSA は、テレメトリ データなど複数情報源からの情報を組み込んだ、URL カテゴリおよび Web レピュテーション データベースに対するシグニチャ更新を受信します。この新規シグニチャ更新および WSA に設定されているさまざまなポリシーに応じて、ユーザによる **http://www.unabashedevil.com** へのアクセスがブロックされ、**myriad_evils.zip** のダウンロードが禁止されます。

URL の暗号化

アクティビティ履歴リポジトリおよびテレメトリ レポート リポジトリに保存されている URL は、機密情報であると見なされます。テレメトリ モジュールは、これらの URL を暗号化して不正アクセスを防止します。

テレメトリ モジュールでは、URL を「内部」または「外部」のいずれかとして扱います。内部 URL の例としては、会社のイントラネット ホーム ページがあります。外部 URL の例としては、インターネット上でアクセスできる任意の URL があります。

SenderBase ネットワークへの参加から除外するように WSA 上に設定されているすべてのドメインおよび IP アドレスは、テレメトリ モジュールでは、内部 URL として定義されます。いずれのドメインおよび IP アドレスも Senderbase ネットワークへの参加から除外しない場合、テレメトリ モジュールでは、すべての URL を外部として扱います。

内部と外部の両方の URL が暗号化された形式でテレメトリ レポートに組み込まれ、WSA に送信されます。

テレメトリ レポートおよびアクティビティ履歴リポジトリに指定されるすべての内部 URL は、内部 URL 用の対称 AES キーを使用して暗号化されます。テレメトリ レポートおよびアクティビティ履歴リポジトリに指定されるすべての外部 URL は、外部 URL 用の対称 AES キーを使用して暗号化されます。これらの対称 AES キーは、各 VPN セッションの開始時またはテレメトリ サービスの開始時に、ランダムに生成されます。

内部 URL の暗号化に使用された AES キーは、自社の公開キーで暗号化されて、AES 暗号化された内部 URL とともに、テレメトリ レポートに含めて送信されます。テレメトリ プロファイル内の公開キーは、[カスタム証明書（Custom Certificates）] エリアで指定できます。自社で用意した、PEM 形式の任意の X.509 公開キー証明書を公開キーとして使用できます。

外部 URL の暗号化に使用された AES キーは、シスコの公開キーおよび自社の公開キーによって暗号化されます。両方の暗号化バージョンの AES キーが、AES 暗号化された外部 URL とともに、テレメトリ レポートに含めて送信されます。シスコの公開キーは、シスコの公開証明書の 1 つであり、テレメトリ モジュールと一緒に配布されます。ASDM または ASA を使用してシスコの公開キーを変更することはできません。

したがって、内部 URL は、会社の秘密キーを使用して復号化できます。外部 URL は、シスコの秘密キーまたは自社の秘密キーを使用して復号化できます。これにより、シスコの秘密キーを持ち、他の会社の秘密キーを持たない Cisco Threat Operations Center では、外部 URL を調査できる一方で、内部 URL は復号化できません。

最後に、WSA の SenderBase 参加レベルによって、暗号化およびレポートされる URL の量が決まります。

- [標準（Standard）]。URL 全体がシスコの公開キーで暗号化されてレポートされます。
- [制限付き（Limited）]。URL の URI 部分が各社の秘密キーで暗号化されて、結果の URL 全体がシスコの公開キーで暗号化されます。

  たとえば、URL https://www.internetdocs.example.com/Doc?docid=a1b2c3d4e5f6g7h8=en に関するテレメトリ レポートの場合は、**Doc?docid=a1b2c3d4e5f6g7h8=en** の部分が各社の秘密キーで暗号化されます。使用する秘密キーに応じて、結果の URL は、次のような文字列になります。

  https://www.internetdocs.example.com/93a68d78c787d8f6sa7d09s1455623

この文字列がシスコの公開キーで暗号化されてレポートされます。この結果、シスコの Threat Operations Center では、URL に含まれているドメイン名のみを復号化できます。

テレメトリ レポートの暗号化

新規テレメトリ レポートを WSA に送信する準備のできたテレメトリ モジュールでは、エンドポイント、ASA、WSA 間に設定されている共有秘密に基づいてレポートを暗号化します。テレメトリ モジュールでは、次に、HTTP POST 要求を WSA に送信することにより、暗号化されたレポートを送信します。WSA では、データを集約し、SenderBase ネットワークへの参加を使用して Threat Operations Center に送信します。この POST 要求が正常に完了した場合、テレメトリ モジュールでは、ローカル レポート リポジトリからレポートを削除します。

テレメトリ クライアント プロファイルの設定

ステップ 1　ASDM を開き、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [設定（Configuration）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）] を選択します。

ステップ 2　[追加（Add）] をクリックしてクライアント プロファイルを作成します。

ステップ 3　クライアント プロファイルの**名前**を指定します。

ステップ 4　[プロファイルの使用（Profile Usage）] フィールドをクリックし、[テレメトリ（Telemetry）] を選択します。

ステップ 5　デフォルトのプロファイルの場所を使用するか、[参照（Browse）] をクリックして代わりのファイルの場所を指定します。

ステップ 6　（任意）[グループ ポリシー（Group Policy）] を選択してクライアント プロファイルを添付するか、クライアント プロファイルを <Unassigned> のままにします。

ステップ 7　[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ページで、作成したばかりのテレメトリ プロファイルを選択し、[編集（Edit）] をクリックします。これで、テレメトリ プロファイル エディタ画面で、テレメトリ プロファイルを編集できるようになりました。

ステップ 8　テレメトリをイネーブルにするために、[サービスの有効化（Enable Service）] チェックボックスをオンにします。

ステップ 9　[最大履歴ログ（MB）（Maximum History Log (MB)）] フィールドで、アクティビティ履歴リポジトリの最大サイズを指定します。

- 値の範囲：2 ～ 1,000 MB。
- デフォルト値：100 MB。

ステップ 10　[最大履歴（日数）（Maximum History (Days)）] フィールドで、アクティビティ履歴を保持する最大日数を指定します。

- 値の範囲：1 ～ 1,000（日間）。
- デフォルト値：180 日間。

ステップ 11　[アンチウイルス確認間隔（秒）（Antivirus Check Interval (secs)）] フィールドで、テレメトリ モジュールが新しいアンチウイルス脅威ログ情報を確認するようにポスチャ モジュールに促す間隔を指定します。

- 値の範囲：5 ～ 300 秒。
- デフォルト値：60 秒

ステップ 12　[再送信試行回数（Retry Send Attempts）] フィールドで、最初の試行が失敗した場合に、テレメトリ モジュールで WSA へのテレメトリ レポートの送信を試行する回数を指定します。

- 値の範囲：0 ～ 10

- デフォルト値：2

ステップ 13　[管理者定義除外（Administrator Defined Exceptions）] フィールドで、そのアプリケーションの動作についての情報をテレメトリ レポートから除外する、アプリケーションの実行ファイルを指定します。実行ファイルは、2 通りの方法で追加できます。

- [管理者定義除外（Administrator Defined Exceptions）] テキスト ボックスに、テレメトリ レポートから除外するファイルの名前またはファイルのフル パスを入力し、[追加（Add）] をクリックします。次に、例を示します。

  trusted.exe

  C:\Program Files\trusted.exe

  ファイル名だけを指定した場合は、ファイルのあるディレクトリにかかわらず、そのファイルの動作は追跡され**ません**。フル ディレクトリ パスおよびファイル名を追加した場合は、指定したディレクトリにある場合に、そのファイルの動作は追跡され**ません**。

- [参照（Browse）] ボタンをクリックし、テレメトリ レポートから除外するローカル ファイルを選択します。追加するファイルを参照して選択すると、テレメトリ プロファイル エディタにより、ファイルのフル パスが入力されます。テレメトリ モジュールでは、このテレメトリ プロファイルを使用するすべてのエンドポイント上で、このパスの終端にある、このファイルを探します。このパスおよびファイル名は、管理者だけでなくこのテレメトリ プロファイルのすべてのユーザにとって正しい必要があります。

  いずれの場合も、ファイルは、[管理者定義除外（Administrator Defined Exceptions）] リスト ボックスにリストされます。

ステップ 14　[ファイルからのカスタム証明書の選択（Custom Certificate Select from file）] フィールドで、[参照（Browse）] をクリックして、XML 形式で証明書を含むプロファイルを生成するために、プライバシー エンハンスト メール（**.pem**）タイプの証明書を見つけます。

ステップ 15　[OK] をクリックします。

ステップ 16　[適用（Apply）] をクリックします。

設定プロファイルの階層

テレメトリ動作を制御するクライアント プロファイル リソースは 3 種類あります。これらのファイルは、優先順序に従って作用します。

表 7-1　テレメトリ クライアント プロファイル ファイル

ファイル名	ロケーション	説明および優先順位
actsettings.xml	エンドポイントの %ALLUSERSPROFILE%\Application Data にインストールされます。\Cisco\Cisco AnyConnect Secure Mobility Client \Telemetry	テレメトリ用の基本設定を含むファイル。
telemetry_profile.tsp このファイル名前は、ASA 管理者によって指定されます。	ASA 上に保存されます。このファイルの場所は、次の画面で指定します。 [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）] > [AnyConnect クライアント プロファイル（AnyConnect Client Profile）]	テレメトリ クライアント プロファイル ファイル。作成されて、ASA 上に保存されます。 このメッセージに定義されている要素は、いずれも、actsettings.xml ファイル内の要素を上書きします。
WSA によって送信されるテレメトリ プロファイル メッセージ	該当なし これは、ファイルではありません。	WSA 上に XML ファイルはありませんが、ステータス クエリー要求に応答するとき、WSA では、XML 形式のメッセージを送信します。 このメッセージに定義されている要素は、いずれも、*telemetry_profile*.tsp ファイル内の要素を上書きします。