Anonymous Reporting および Smart Call Home

この章では、Anonymous Reporting および Smart Call Home サービスを設定する方法について説明します。

Anonymous Reporting について

Anonymous Reporting をイネーブルにして ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーと正常性に関する最小限の情報をデバイスからシスコに安全に送信できます。この機能をイネーブルにした場合、お客様のアイデンティティは匿名のままとなり、識別情報は送信されません。

Anonymous Reporting をイネーブルにすると、トラスト ポイントが作成され、証明書がインストールされます。CA 証明書は、ASA でメッセージを安全に送信できるように、Smart Call Home Web サーバー上のサーバー証明書を検証して、HTTPS セッションを形成するために必要です。ソフトウェアに事前定義済みの証明書が、シスコによってインポートされます。Anonymous Reporting をイネーブルにする場合は、ハードコードされたトラスト ポイント名の _SmartCallHome_ServerCA で証明書が ASA にインストールされます。Anonymous Reporting をイネーブルにすると、このトラスト ポイントが作成され、適切な証明書がインストールされて、このアクションに関するメッセージが表示されます。これで、証明書が設定の中に存在するようになります。

Anonymous Reporting をイネーブルにしたときに、適切な証明書がすでに設定に存在する場合、トラスト ポイントは作成されず、証明書はインストールされません。

（注） Anonymous Reporting をイネーブルにすると、指定されたデータをシスコまたはシスコの代わりに運用するベンダー（米国以外の国を含む）に転送することに同意することになります。シスコでは、すべてのお客様のプライバシーを保護しています。シスコの個人情報の取り扱いに関する詳細については、次の URL にあるシスコのプライバシー声明を参照してください。
http://www.cisco.com/web/siteassets/legal/privacy.html

ASA はバックグラウンドで Smart Call Home 匿名レポートを設定するときに、Call Home サーバー証明書を発行する CA の証明書を含むトラストポイントを自動生成します。ASA は、サーバー証明書の発行階層が変更された場合に証明書の検証をサポートするようになりました。カスタマーが証明書階層を変更する必要はありません。また、手動介入なしに ASA が証明書階層を更新できるよう、トラストプールの証明書を自動的にインポートすることもできます。

ASA 9.14（2.14）をアップグレードすると、トラストポイントの設定が CallHome_ServerCA から CallHome_ServerCA2 に自動的に変更されます。

DNS 要件

ASA が Cisco Smart Call Home サーバーに到達してシスコにメッセージを送信できるように DNS サーバーを正しく設定する必要があります。ASA をプライベート ネットワークに配置し、パブリック ネットワークにはアクセスできないようにすることが可能なため、シスコでは DNS 設定を検証し、必要な場合には次の手順を実行して、ユーザーの代わりにこれを設定します。

1. 設定されているすべての DNS サーバーに対して DNS ルックアップを実行します。
2. 最もセキュリティレベルの高いインターフェイスで DHCPINFORM メッセージを送信して、DHCP サーバーから DNS サーバーを取得します。
3. ルックアップにシスコの DNS サーバーを使用します。
4. tools.cisco.com に対してランダムに静的 IP アドレスを使用します。

これらの作業は、現在の設定を変更せずに実行されます。（たとえば、DHCP から学習された DNS サーバーは設定には追加されません）。

設定されている DNS サーバーがなく、ASA が Cisco Smart Call Home サーバーに到達できない場合は、各 Smart Call Home メッセージに対して、重大度「warning」の syslog メッセージが生成されます。これは、DNS を適切に設定するようお願いするためです。

syslog メッセージについては、syslog メッセージガイドを参照してください。

Smart Call Home の概要

完全に設定が終わると、Smart Call Home は設置場所での問題を検出し、多くの場合はそのような問題があることにユーザーが気付く前に、シスコにレポートを返すか、別のユーザー定義のチャネル（ユーザー宛の電子メールまたはユーザーに直接など）を使用してレポートを返します。シスコでは、これらの問題の重大度に応じて次のサービスを提供することにより、システ

ムコンフィギュレーションの問題、製品ライフサイクル終了通知の発表、セキュリティ勧告問題などに対応します。

- 継続的モニタリング、リアルタイムの予防的なアラート、および詳細な診断により、問題を迅速に識別する。
- サービス要求が開かれ、すべての診断データが添付された Smart Call Home 通知を使用して、潜在的な問題をユーザーに認識させる。
- Cisco TAC の専門家に自動的に直接アクセスすることにより、重大な問題を迅速に解決する。
- トラブルシューティングに必要な時間を短縮することにより、スタッフリソースを効率よく使用する。
- Cisco TAC へのサービス リクエストを自動的に生成し（サービス契約がある場合）、適切なサポート チームに提出する。問題解決の時間を短縮する、詳細な診断情報を提供します。

Smart Call Home ポータルを使用すると必要な情報に迅速にアクセスできるため、以下の事項が実現されます。

- すべての Smart Call Home メッセージ、診断、および推奨事項を一箇所で確認する。
- サービス リクエスト ステータスを確認する。
- すべての Smart Call Home 対応デバイスに関する最新のインベントリ情報およびコンフィギュレーション情報を表示する。

Anonymous Reporting および Smart Call Home のガイドライン

この項では、Anonymous Reporting と Smart Call Home を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

Anonymous Reporting のガイドライン

- DNS が設定されていること。
- Anonymous Reporting のメッセージを最初の試行で送信できなかった場合、ASA はメッセージをドロップする前にさらに 2 回試行します。
- Anonymous Reporting は、既存の設定を変更せずに、他の Smart Call Home 設定と共存させることができます。たとえば、Anonymous Reporting をイネーブルにする前に Smart Call Home がディセーブルになっている場合、Anonymous Reporting をイネーブルにした後でも、ディセーブルのままです。

- Anonymous Reporting をイネーブルにしている場合、トラスト ポイントを削除することはできません。また、Anonymous Reporting をディセーブルにした場合、トラスト ポイントはそのまま残ります。Anonymous Reporting がディセーブルの場合は、トラスト ポイントを削除できますが、Anonymous Reporting をディセーブルにしてもトラスト ポイントは削除されません。
- マルチ コンテキスト モード設定を使用している場合は、**dns**、**interface**、**trustpoint** コマンドは管理コンテキストにあり、**call-home** コマンドはシステム コンテキストにあります。
- CA サーバーの自己署名証明書が変更された場合に、Smart Call Home がアクティブな状態を維持できるように、定期的な trustpool バンドルの更新を自動化できます。このトラストプール自動更新機能は、マルチ コンテキストの導入ではサポートされません。

Smart Call Home のガイドライン

- マルチ コンテキスト モードでは、subscribe-to-alert-group snapshot periodic コマンドは、システム コンフィギュレーションから情報を取得するコマンドと、ユーザ コンテキストから情報を取得するコマンドの 2 つのコマンドに分割されます。
- Smart Call Home のバックエンド サーバーは、XML 書式のメッセージのみ受け取ることができます。
- Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタ イベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次のイベントに対してのみ送信されます。
  - ユニットがクラスタに参加したとき
  - ユニットがクラスタから脱退したとき
  - クラスタユニットがクラスタ制御ユニットになったとき
  - クラスタのセカンダリ ユニットが故障したとき

  送信される各メッセージには次の情報が含まれています。
  - アクティブ クラスタのメンバ数
  - クラスタ制御ユニットでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力

Anonymous Reporting および Smart Call Home の設定

Anonymous Reporting は Smart Call Home サービスの一部であり、これを使用すると、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに匿名で送信できます。一方、Smart Call Home サービスは、システム ヘルスのサポートをカスタマイズする機能です。Cisco TAC

がお客様のデバイスをモニタして、問題があるときにケースを開くことができるようになります。多くの場合は、お客様がその問題に気付く前に発見できます。

両方のサービスをシステム上で同時に設定できますが、Smart Call Home サービスを設定すれば、Anonymous Reporting と同じ機能に加えて、カスタマイズされたサービスも使用できるようになります。

Anonymous Reporting の設定

Anonymous Reporting を設定するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Smart Call Home] の順に選択します。

ステップ 2 [Enable Anonymous Reporting] チェックボックスをオンにします。

ステップ 3 [Test Connection] をクリックして、システムでメッセージを送信できることを確認します。

ASDM は成功メッセージまたはエラー メッセージを返して、テスト結果を通知します。

ステップ 4 [Apply] をクリックして設定を保存し、Anonymous Reporting をイネーブルにします。

Smart Call Home の設定

Smart Call Home サービス、システム セットアップ、およびアラート サブスクリプション プロファイルを設定するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Smart Call Home]** の順に選択します。

ステップ 2 [Enable Registered Smart Call Home] チェックボックスをオンにして、Smart Call Home をイネーブルにし、ASA を Cisco TAC に登録します。

ステップ 3 [Advanced System Setup] をダブルクリックします。この領域は、3 個のペインで構成されています。各ペインは、タイトル行をダブルクリックすると展開または縮小できます。

a) [Mail Servers] ペインで、Smart Call Home メッセージを電子メールのサブスクライバに配信する際に通過するメール サーバーを設定できます。

b) ASA の [Contact Information] ペインで、Smart Call Home メッセージに表示される担当者の個人情報を入力できます。このペインには、次の情報が含まれます。

- 連絡先担当者の名前。
- 連絡先の電話番号。

- 連絡先担当者の住所。
- 連絡先の電子メール アドレス。
- Smart Call Home 電子メールの「from」電子メール アドレス。
- Smart Call Home 電子メールの「reply-to」電子メール アドレス。
- カスタマー ID。
- サイト ID。
- 連絡先 ID。

c) [Alert Control] ペインで、アラートの制御パラメータを調整できます。このペインには、[Alert Group Status] ペインが含まれ、ここには次のアラート グループのステータス（イネーブルまたはディセーブル）がリストされます。

- 診断アラート グループ。
- コンフィギュレーション アラート グループ。
- 環境アラート グループ。
- インベントリ アラート グループ。
- スナップショット アラート グループ。
- syslog アラート グループ。
- テレメトリ アラート グループ。
- 脅威アラート グループ。
- 1 分間に処理される Smart Call Home メッセージの最大数。
- Smart Call Home 電子メールの「from」電子メール アドレス。

ステップ 4 [Alert Subscription Profiles] をダブルクリックします。指定した各サブスクリプション プロファイルによって、サブスクライバおよび対象とするアラート グループが特定されます。

a) [Add] または [Edit] をクリックして、**サブスクリプション プロファイル エディタ**を表示します。ここでは、新規サブスクリプションプロファイルを作成したり、既存のサブスクリプション プロファイルを編集したりできます。
b) [Delete] をクリックして、選択したプロファイルを削除します。
c) [Active] チェックボックスをオンにして、選択されたサブスクリプション プロファイルの Smart Call Home メッセージをサブスクライバに送信します。

ステップ 5 [Add] または [Edit] をクリックして、[Add Alert Subscription Profile] ダイアログボックスまたは [Edit Alert Subscription Profile] ダイアログ ボックスを表示します。

a) [Name] フィールドは読み取り専用であり、編集できません。
b) [Enable this subscription profile] チェックボックスをオンにして、この特定のプロファイルをイネーブルまたはディセーブルにします。

c) [Alert Delivery Method] 領域で、[HTTP] または [Email] オプション ボタンのいずれかをクリックします。

d) [Subscribers] フィールドに電子メール アドレスまたは Web アドレスを入力します。

e) [Reference Identity] に、syslog サーバーから受信した証明書に対する RFC 6125 参照 ID チェックをイネーブルにする参照 ID オブジェクトを名前で指定します。

参照 ID オブジェクトについて詳しくは、参照 ID の設定を参照してください。

ステップ 6 [Alert Dispatch] 領域では、管理者が、サブスクライバに送信する Smart Call Home 情報の種類と送信の条件を指定できます。時間ベースとイベントベースの 2 種類のアラートがあり、アラートのトリガー方法に応じて選択します。コンフィギュレーション、インベントリ、スナップショット、およびテレメトリの各アラート グループは時間ベースです。診断、環境、Syslog、および脅威の各アラート グループはイベントベースです。

ステップ 7 [Message Parameters] 領域では、優先されるメッセージ形式や最大メッセージ サイズなど、サブスクライバに送信されるメッセージを制御するパラメータを調整できます。

ステップ 8 時間ベースのアラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Add Configuration Alert Dispatch Condition] または [Edit Configuration Alert Dispatch Condition] ダイアログボックスを表示します。

a) [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。

b) [Basic] または [Detailed] オプション ボタンをクリックして、サブスクライバに必要な情報のレベルを指定します。

c) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 9 イベントベースの診断、環境、および脅威アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Diagnostic Alert Dispatch Condition] または [Edit Diagnostic Alert Dispatch Condition] ダイアログボックスを表示します。

ステップ 10 [Event Severity] ドロップダウン リストで、サブスクライバへのアラートのディスパッチをトリガーするイベントの重大度を指定し、[OK] をクリックします。

ステップ 11 時間ベースのインベントリ アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Inventory Alert Dispatch Condition] または [Edit Inventory Alert Dispatch Condition] ダイアログボックスを表示します。

ステップ 12 [Alert Dispatch Frequency] ドロップダウン リストで、サブスクライバにアラートをディスパッチする頻度を指定し、[OK] をクリックします。

ステップ 13 時間ベースのスナップショット アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Snapshot Alert Dispatch Condition] または [Edit Snapshot Alert Dispatch Condition] ダイアログボックスを表示します。

a) [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。
- 間隔サブスクリプションの場合、サブスクライバに情報を送信する頻度を分単位で指定します。この要件は、スナップショット アラート グループにのみ適用されます。

b) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 14 イベントベースの syslog アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Syslog Alert Dispatch Condition] または [Edit Syslog Alert Dispatch Condition] ダイアログボックスを表示します。

a) [Specify the event severity which triggers the dispatch of alert to subscribers] チェックボックスをオンにして、ドロップダウン リストからイベントの重大度を選択します。

b) [Specify the message IDs of syslogs which trigger the dispatch of alert to subscribers] チェックボックスをオンにします。

c) 画面の指示に従って、サブスクライバへのアラートのディスパッチをトリガーする syslog メッセージ ID を指定します。

d) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 15 イベントベースのテレメトリ アラートの場合、[Alert Dispatch] 領域で [Add] または [Edit] をクリックして、[Create Telemetry Alert Dispatch Condition] または [Edit Telemetry Alert Dispatch Condition] ダイアログボックスを表示します。

a) [Alert Dispatch Frequency] 領域で、サブスクライバに情報を送信する頻度を指定します。

- 毎月のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎週のサブスクリプションのための情報として、送信日、時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。
- 毎日のサブスクリプションには、情報を送信する時刻を指定します。この指定がない場合は、ASA が適切な値を選択します。

- 時間単位のサブスクリプションには、情報を送信する時間（分単位）を指定します。この指定がない場合は、ASA が適切な値を選択します。時間単位のサブスクリプションが適切なのは、スナップショットおよびテレメトリ アラート グループのみです。

b) [OK] をクリックしてコンフィギュレーションを保存します。

ステップ 16 [Test] をクリックして、設定したアラートが正しく動作しているかどうかを判別します。

trustpool 証明書の自動インポートの設定

スマートライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA は、サーバー証明書の発行階層が変更された場合に証明書の検証をサポートするようになりました。カスタマーが証明書階層の変更を調整する必要はありません。CA サーバーの自己署名証明書が変更された場合に、Smart Call Home がアクティブな状態を維持できるように、定期的な trustpool バンドルの更新を自動化できます。この機能はマルチ コンテキスト展開ではサポートされません。

trustpool の証明書バンドルを自動的にインポートするには、ASA がバンドルのダウンロードとインポートに使用する URL を指定する必要があります。次のコマンドを入力すると、デフォルトの Cisco URL とデフォルトの時間（22 時間）を使用して、毎日一定の間隔でインポートが実行されます。

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

また、次のコマンドを使用して、カスタム URL による自動インポートをイネーブルにできます。

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

オフピーク時またはその他の都合のよい時間帯に柔軟にダウンロードを設定できるようにするには、次のコマンドを入力して、カスタム時間によるインポートをイネーブルにします。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

カスタム URL とカスタム時間の両方による自動インポートを設定するには、次のコマンドを使用する必要があります。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

Anonymous Reporting および Smart Call Home のモニタリング

Anonymous Reporting および Smart Call Home サービスのモニタリングについては、次のコマンドを参照してください。**[Tools] > [Command Line Interface]**を使用してこのコマンドを入力できます。

- **show call-home detail**

このコマンドは、現在の Smart Call Home の詳細設定を表示します。

- **show call-home mail-server status**

  このコマンドは、現在のメール サーバーのステータスを表示します。

- **show call-home profile** {profile name | **all**}

  このコマンドは、Smart Call Home プロファイルのコンフィギュレーションを表示します。

- **show call-home registered-module status** [**all**]

  このコマンドは、登録されているモジュールのステータスを表示します。

- **show call-home statistics**

  このコマンドは、Call Home の詳細ステータスを表示します。

- **show call-home**

  このコマンドは、現在の Smart Call Home のコンフィギュレーションを表示します。

- **show running-config call-home**

  このコマンドは、現在の Smart Call Home の実行コンフィギュレーションを表示します。

- **show smart-call-home alert-group**

  このコマンドは、Smart Call Home アラート グループの現在のステータスを表示します。

- **show running-config all**

  このコマンドは、Anonymous Reporting ユーザー プロファイルに関する詳細を表示します。

Anonymous Reporting および Smart Call Home の履歴

表 *1 : Anonymous Reporting* および *Smart Call Home* の履歴

機能名	プラットフォーム リリース	説明
Smart Call Home	8.2(2)	Smart Call Home サービスは、ASA に関するプロアクティブ診断およびリアルタイム アラートを提供し、ネットワークの可用性と運用効率を向上させます。 次の画面が導入されました。 [Configuration] > [Device Management] > [Smart Call Home]。

機能名	プラットフォーム リリース	説明
Anonymous Reporting	9.0(1)	Anonymous Reporting をイネーブルにして、ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。 次の画面が変更されました。[Configuration] > [Device Monitoring] > [Smart Call Home]。
Smart Call Home	9.1(2)	テレメトリ アラート グループ レポートのための **show local-host** コマンドは、**show local-host | include interface** コマンドに変更になりました。
Smart Call Home	9.1(3)	Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタイベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次の 3 種類のイベントに対してのみ送信されます。 • ユニットがクラスタに参加したとき • ユニットがクラスタから脱退したとき • クラスタユニットがクラスタ制御ユニットになったとき 送信される各メッセージには次の情報が含まれています。 • アクティブ クラスタのメンバ数 • クラスタ制御ユニットでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力
セキュアな Smart Call Home サーバー接続のリファレンス ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバー ID の検証ルールをサポートするようになりました。ID 検証は、Smart Call Home サーバーへの TLS 接続の PKI 確認中に実行されます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のページが変更されました。[Configuration] > [Device Management] > [Smart Call Home]。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。