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。

アラート グループへの登録

アラート グループは、ASA でサポートされる Smart Call Home アラートの定義済みサブセットです。Smart Call Home アラートにはさまざまなタイプがあり、タイプに応じてさまざまなアラート グループにグループ化されます。各アラート グループは、特定の CLI の出力を報告します。サポートされる Smart Call Home アラート グループは次のとおりです。

- syslog
- diagnostic
- 環境
- インベントリ
- 設定
- 脅威
- snapshot
- telemetry
- テスト

アラート グループの属性

アラート グループには次の属性があります。

- イベントはまず 1 個のアラート グループに登録します。
- 1 個のグループを、複数のイベントに関連付けることができます。
- 個々のアラート グループに登録できます。
- 個々のアラート グループをイネーブルまたはディセーブルにできます。デフォルト設定では、すべてのアラート グループに対してイネーブルです。
- 診断および環境アラート グループは定期的なメッセージのサブスクリプションをサポートします。
- syslog アラート グループは、メッセージ ID ベースのサブスクリプションをサポートします。
- 環境アラート グループの CPU とメモリの使用率のしきい値を設定できます。特定のパラメータが定義済みしきい値を超えると、メッセージが送信されます。しきい値のほとんどは、プラットフォームによって決まっており、変更できません。
- 指定する CLI 出力を送信するようスナップショット アラート グループを設定します。

アラート グループによって Cisco に送信されるメッセージ

メッセージは、定期的に、および ASA がリロードされるたびにシスコに送信されます。これらのメッセージは、アラート グループによって分類されます。

インベントリ アラートは、次のコマンドによる出力で構成されます。

- **show version**：ASA ソフトウェア バージョン、ハードウェア構成、ライセンス キー、および関連するデバイスの稼働時間を表示します。
- **show inventory—**ネットワーキング デバイスにインストールされている各 Cisco 製品のインベントリ情報を取得および表示します。各製品は UDI と呼ばれる一意のデバイス情報で識別されます。UDI は、製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）の 3 つの異なるデータ要素の組み合わせです。
- **show failover state**：フェールオーバー ペアの両方のユニットのフェールオーバー状態を表示します。表示される情報は、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。
- **show environment**：シャーシ、ドライバ、ファン、および電源のハードウェア動作ステータスや、温度ステータス、電圧、CPU 使用率などの、ASA システム コンポーネントのシステム環境情報を表示します。

コンフィギュレーション アラートは、次のコマンドによる出力で構成されます。

- **show context**：割り当てられているインターフェイスと設定ファイルの URL、設定済みコンテキストの数を表示します。または、システム実行スペースで Anonymous Reporting を有効にしている場合には、すべてのコンテキストのリストを表示します。
- **show call-home registered-module status**：登録されたモジュールのステータスを表示します。システム コンフィギュレーション モードを使用している場合、コマンドによって、コンテキストごとではなく、デバイス全体に基づくシステムモジュールのステータスが表示されます。
- **show running-config**：ASA で現在実行されている設定を表示します。
- **show startup-config**：スタートアップ コンフィギュレーションを表示します。
- **show access-list | include elements**：アクセス リストのヒット カウンタおよびタイム スタンプ値を表示します。

診断アラートは、次のコマンドによる出力で構成されます。

- **show failover**：ユニットのフェールオーバー ステータスに関する情報を表示します。
- **show interface**：インターフェイス統計情報を表示します。
- **show cluster info**：クラスタ情報を表示します。
- **show cluster history**：クラスタの履歴を表示します。
- **show crashinfo**（切り捨て）：予期しないソフトウェアのリロード後に、デバイスは、変更されたクラッシュ情報ファイルをファイルのトレースバック セクションだけを含めて送信します。したがって、ファンクション コール、レジスタ値、およびスタック ダンプだけがシスコに報告されます。
- **show tech-support no-config**：テクニカル サポート アナリストによる診断に使用される情報を表示します。

環境アラートは、次のコマンドによる出力で構成されます。

- **show environment**：シャーシ、ドライバ、ファン、および電源のハードウェア動作ステータスや、温度ステータス、電圧、CPU 使用率などの、ASA システム コンポーネントのシステム環境情報を表示します。
- **show cpu usage**：CPU 使用率情報を表示します。
- **show memory detail**：空きおよび割り当て済みのシステム メモリの詳細情報を表示します。

脅威アラートは、次のコマンドによる出力で構成されます。

- **show threat-detection rate**：脅威検出統計情報を表示します。
- **show threat-detection shun**：現在排除されているホストを表示します。
- **show shun**：排除情報を表示します。

- **show dynamic-filter reports top**：ボットネット トラフィック フィルタによって分類された上位 10 のマルウェア サイト、ポート、および感染ホストのレポートを生成します。

スナップショット アラートは、次のコマンドによる出力で構成されます。

- **show conn count**：アクティブな接続の数を表示します。
- **show asp drop**：高速セキュリティ パスでドロップされたパケットまたは接続を表示します。

テレメトリ アラートは、次のコマンドによる出力で構成されます。

- **show perfmon detail**：ASA パフォーマンスの詳細を表示します。
- **show traffic**：インターフェイスの送受信アクティビティを表示します。
- **show conn count**：アクティブな接続の数を表示します。
- **show vpn-sessiondb summary**：VPN セッションのサマリー情報を表示します。
- **show vpn load-balancing**：VPN ロードバランシングの仮想クラスタ コンフィギュレーションの実行時統計情報を表示します。
- **show local-host | include interface**：ローカル ホストのネットワーク状態を表示します。
- **show memory**：物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。
- **show context**：割り当てられているインターフェイスと設定ファイルの URL、設定済みコンテキストの数を表示します。または、システム実行スペースで Anonymous Reporting を有効にしている場合には、すべてのコンテキストのリストを表示します。
- **show access-list | include elements**：アクセス リストのヒット カウンタおよびタイム スタンプ値を表示します。
- **show interface**：インターフェイス統計情報を表示します。
- **show threat-detection statistics protocol**：IP プロトコルの統計情報を表示します。
- **show phone-proxy media-sessions count**：電話プロキシによって保存されている、対応するメディア セッションの数を表示します。
- **show phone-proxy secure-phones count**：データベースに保存されているセキュア モード対応の電話機の数を表示します。
- **show route**：ルーティング テーブルを表示します。
- **show xlate count**：NAT セッション（xlates）の数を表示します。

メッセージ重大度しきい値

特定のアラート グループに宛先プロファイルを登録すると、メッセージの重大度に基づいてアラート グループ メッセージを送信するしきい値を設定できます。宛先プロファイルに指定したしきい値より低い値のメッセージは、宛先に送信されません。

次の表にメッセージの重大度と syslog の重大度のマッピングを示します。

表 *1 :* メッセージの重大度と *syslog* レベルのマッピング

レベル	メメッセージ重大度レベル	Syslog 重大度レベル	説明
9	Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
8	Disaster	該当なし	ネットワークに重大な影響が及びます。
7	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	0	緊急事態。システムが使用不可能な状態。
6	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	1	アラート。クリティカルな状態。ただちに注意が必要。
5	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	2	Critical 重大な状態。
4	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	3	エラー。軽微な状態。
3	警告	4	警告状態。
2	通知	5	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	標準	6	Information。通常のイベント。通常の状態に戻ることを意味します。

レベル	メメッセージ重大度レベル	Syslog 重大度レベル	説明
0	Debugging	7	デバッグ メッセージ（デフォルト設定）。

サブスクリプション プロファイル

サブスクリプションプロファイルを使用すると宛先受信者と関心のあるグループを関連付けることができます。プロファイルにあるサブスクライブされたグループに登録されているイベントがトリガーされると、イベントに関連付けられたメッセージが設定された受信者に送信されます。サブスクリプション プロファイルには次の属性があります。

- 複数のプロファイルを作成および設定できます。
- 1 個のプロファイルに複数の電子メールまたは HTTPS の受信者を設定できます。
- 1 個のプロファイルで、指定した重大度に複数のグループを登録できます。
- 1 個のプロファイルで、3 種類のメッセージ フォーマット（ショート テキスト、ロング テキスト、XML）をサポートします。
- 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できます。デフォルトでは、プロファイルはディセーブルです。
- 最大メッセージ サイズを指定できます。デフォルトは 3 MB です。

デフォルト プロファイル「Cisco TAC」が提供されました。デフォルト プロファイルには、事前定義されたモニタ対象グループ（診断、環境、インベントリ、コンフィギュレーション、テレメトリ）のセットと、事前定義された宛先電子メールおよび HTTPS URL があります。デフォルト プロファイルは、Smart Call Home を初めて設定するときに自動的に作成されます。宛先電子メールは callhome@cisco.com で、宛先 URL は https://tools.cisco.com/its/service/oddce/services/DDCEService です。

（注） デフォルト プロファイルの宛先電子メールと宛先 URL は変更できません。

コンフィギュレーション、インベントリ、テレメトリ、またはスナップショット アラート グループに宛先プロファイルを登録すると、アラート グループ メッセージを非同期に、または定期的に指定の時間に受信するよう選択できます。

次の表に、デフォルトのアラート グループと重大度のサブスクリプションおよび期間（該当する場合）のマッピングを示します。

表 *2:* アラート グループと重大度のサブスクリプションのマッピング

アラート グループ	重大度	Period
設定（Configuration）	Informational	Monthly

アラート グループ	重大度	Period
診断	Informational 以上	該当なし
環境	Notification 以上	該当なし
インベントリ	Informational	Monthly
Snapshot	Informational	該当なし
Syslog	同等の syslog	該当なし
Telemetry	Informational	Daily
Test	N/A	なし
Threat	通知	N/A

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。

コンフィギュレーション モードに入ると、次のガイドラインに従って Anonymous Reporting および Smart Call Home サービスをイネーブルにすることを要求するプロンプトが出ます。

- このプロンプトで、[Y]es、[N]o、または [A]sk later を選択できます。[[A]sk later] を選択した場合、7 日後または ASA をリロードしたときに再度通知されます。[[A]sk later] を連続で選択すると、さらに ASA で 7 日ごとに 2 回プロンプトが表示されたのち、[[N]o] という答えだと見なされて再度表示されることはなくなります。

- プロンプトが表示されない場合は、Anonymous Reporting の設定 （11 ページ）またはSmart Call Home の設定 （11 ページ）の手順を実行して、Anonymous Reporting または Smart Call Home をイネーブルにすることができます。

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 Anonymous Reporting 機能をイネーブルにし、新しい匿名のプロファイルを作成します。

call-home reporting anonymous

例：

```
ciscoasa(config)# call-home reporting anonymous
```

このコマンドを入力すると、トラスト ポイントが作成され、シスコの Web サーバーの識別情報を検証するために使用する証明書がインストールされます。

ステップ 2 （オプション）このサーバーへの接続があり、システムがメッセージを送信できることを確認します。

call-home test reporting anonymous

例：

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

成功またはエラー メッセージは、テスト結果を返します。

Smart Call Home の設定

ASA で Smart Call Home サービスを設定するには、次のタスクを実行します。

手順

ステップ 1 Smart Call Home サービスをイネーブルにします。Smart Call Home のイネーブル化 （12 ページ）を参照してください。

ステップ 2 Smart Call Home メッセージがサブスクライバに配信される際に通過するメール サーバーを設定します。メール サーバーの設定 （17 ページ）を参照してください。

ステップ 3 Smart Call Home メッセージの連絡先情報を設定します。顧客連絡先情報の設定 （16 ページ）を参照してください。

ステップ 4 処理できるイベントの最大レートなどのアラート処理パラメータを定義します。アラート グループ サブスクリプションの設定 （14 ページ）を参照してください。

ステップ 5 アラート サブスクリプション プロファイルを設定します。宛先プロファイルの設定 （20 ページ）を参照してください。

個々のアラート サブスクリプション プロファイルによって、次の内容が特定されます。

- シスコの Smart Call Home サーバーや電子メール受信者のリストなど、Smart Call Home メッセージの送信先となるサブスクライバ。
- コンフィギュレーション情報またはインベントリ情報など、受信するアラートの情報カテゴリ。

Smart Call Home のイネーブル化

Smart Call Home をイネーブルにして、Call Home プロファイルをアクティブにするには、次の手順を実行します。

手順

ステップ 1 Smart Call Home サービスをイネーブルにします。

service call-home

例：

```
ciscoasa(config)# service call-home
```

ステップ 2 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call home
```

認証局のトラスト ポイントの宣言および認証

HTTPS 経由で Web サーバーにメッセージを送信するように Smart Call Home が設定されている場合、Web サーバーの証明書または証明書を発行した認証局（CA）の証明書を信頼するように ASA を設定する必要があります。Cisco Smart Call Home 実稼働サーバー証明書は、Verisign によって発行されます。Cisco Smart Call Home Staging サーバーの証明書は Digital Signature Trust Company によって発行されます。

（注） VPN 検証に使用されないために、no client-types および no validation-usage 用のトラスト ポイントを設定する必要があります。

Cisco サーバー セキュリティの証明書を宣言および認証し、Smart Call Home サービス用に Cisco HTTPS サーバーとの通信を確立するには、次の手順を実行します。

手順

ステップ 1 （マルチ コンテキスト モードのみ）管理コンテキストで証明書をインストールします。

changeto context *admincontext*

例：

```
ciscoasa(config)# changeto context contextA
```

ステップ 2 トラスト ポイントを設定し、証明書登録の準備を整えます。

crypto ca trustpoint *trustpoint-name*

例：

```
ciscoasa(config)# crypto ca trustpoint cisco
```

（注）
転送方法として HTTP を使用する場合は、セキュリティ証明書をトラストポイント経由でインストールする必要があります。HTTPS には、これが必須です。次の URL で、インストールする指定の証明書を探します。

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

ステップ 3 証明書登録に、手動でのカットアンドペースト方式を指定します。

enroll terminal

例：

```
ciscoasa(ca-trustpoint)# enroll terminal
```

ステップ 4 指定した CA を認証します。CA の名前は、**crypto ca trustpoint** コマンドで指定したトラストポイント名と一致している必要があります。プロンプトで、セキュリティ証明書のテキストを貼り付けます。

crypto ca authenticate trustpoint

例：

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

ステップ 5 セキュリティ証明書のテキストの終わりを指定し、入力されたセキュリティ証明書の受け入れを確認します。

quit

例：

```
ciscoasa(ca-trustpoint)# quit
%Do you accept this certificate [yes/no]:
yes
```

環境およびスナップショット アラート グループの設定

環境およびスナップショット アラート グループを設定するには、次の手順を実行します。

手順

アラート グループ コンフィギュレーション モードを開始します。

alert-group-config {**environment** | **snapshot**}

例：

```
ciscoasa(config)# alert-group-config environment
```

アラート グループ サブスクリプションの設定

宛先プロファイルをアラート グループに登録するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 指定した Smart Call Home アラート グループをイネーブルにします。

alert-group {**all** |**configuration** |**diagnostic** |**environment** |**inventory** |**syslog**}

例：

```
ciscoasa(cfg-call-home)# alert-group syslog
```

すべてのアラート グループをイネーブルにするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。

ステップ 3 指定された宛先プロファイルに対するプロファイル コンフィギュレーション モードを開始します。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

ステップ 4 使用可能なすべてのアラート グループに登録します。

subscribe-to-alert-group all

例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

ステップ 5 この宛先プロファイルをコンフィギュレーション アラート グループに登録します。

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
 Wednesday 23:30
```

periodic キーワードを指定すると、定期的に通知するようにコンフィギュレーション アラート グループが設定されます。デフォルトの間隔は daily です。

daily キーワードでは、送信する時刻を 24 時間制の *hh:mm* 形式（例：14:30）で指定します。

weekly キーワードでは、曜日と時刻を *day hh:mm* 形式で指定します。曜日は英語で記述します（例：Monday）。

monthly キーワードでは、1 ～ 31 の日付と時刻を *date hh:mm* 形式で指定します。

顧客連絡先情報の設定

顧客連絡先情報を設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 顧客電話番号を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

phone-number *phone-number-string*

例：

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

ステップ 3 顧客の住所（自由形式の文字列、最長 255 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

street-address *street-address*

例：

```
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
```

ステップ 4 顧客名（最長 128 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

contact-name *contact-name*

例：

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

ステップ 5 シスコ カスタマー ID（最長 64 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

customer-id *customer-id-string*

例：

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

ステップ 6 顧客サイト ID（最長 64 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

site-id *site-id-string*

例：

```
ciscoasa(cfg-call-home)# site-id site1234
```

ステップ 7 顧客連絡先 ID（最長 128 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

contract-id *contract-id-string*

例：

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

例

次に、連絡先情報を設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

メール サーバーの設定

メッセージの転送には、最もセキュアなHTTPSを使用することをお勧めします。ただし、Smart Call Home宛ての電子メールを設定し、電子メール メッセージ転送を使用するようメール サーバーを設定できます。

電子メール サーバーを設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 SMTP メール サーバーを指定します。

mail-server*ip-address* **name priority** [**1-100**] [**all**]

例：

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

最大 5 つのメール サーバーを指定できます。その場合は、コマンドを 5 回実行します。Smart Call Home メッセージの電子メール転送を使用するには、最低 1 つのメール サーバーを設定する必要があります。

番号が小さいほどメール サーバーの優先順位が高くなります。

ip-address 引数には、IPv4 と IPv6 のどちらのメール サーバー アドレスも指定できます。

例

次に、プライマリ メール サーバー（smtp.example.com）および IP アドレス 10.10.1.1 にあるセカンダリ メール サーバーを設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

トラフィック レートの制限の設定

トラフィック レートの制限を設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 Smart Call Home が 1 分間に送信できるメッセージの数を指定します。デフォルト値は、1 分間に 10 のメッセージです。

rate-limit *msg-count*

例：

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Smart Call Home 通信の送信

特定の Smart Call Home 通信を送信するには、次の手順を実行します。

手順

次のいずれかのオプションを選択します。

- オプション 1：プロファイル コンフィギュレーションを使用して、テスト メッセージを送信します。

  call-home test [*test-message*] **profile** *profile-name*

  例：

  ```
  ciscoasa# call-home test [testing123] profile CiscoTAC-1
  ```

- オプション 2：アラート グループ メッセージを 1 つの宛先プロファイルに送信します（指定されている場合）。プロファイルが指定されていない場合は、インベントリ、コンフィギュレーション、スナップショット、またはテレメトリ アラート グループの通知を受け取るように設定されたすべてのプロファイルにメッセージが送信されます。

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  例：

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- オプション 3：コマンド出力を電子メールアドレスに送信します。指定する CLI コマンドは、どのようなコマンドでもかまいません。これには、すべての登録済みモジュールのコマンドも含まれます。

  call-home send*cli command* [**email** *email*]

例：

```
ciscoasa# call-home send cli destination email username@example.com
```

電子メールアドレスを指定した場合、コマンド出力はそのアドレスに送信されます。電子メール アドレスを指定していない場合、出力は Cisco TAC に送信されます。電子メールは、件名行にサービス番号を付けて（指定した場合）ログテキスト形式で送信されます。

電子メール アドレスを指定しない場合、または Cisco TAC 電子メール アドレスを指定した場合に限り、サービス番号が必要になります。

宛先プロファイルの設定

電子メールまたは HTTP の宛先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 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 指定された宛先プロファイルに対するプロファイル コンフィギュレーション モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

最大10個のアクティブプロファイルを作成できます。デフォルトプロファイルは、Cisco TAC に報告するように設定されています。Call Home情報を別の場所（たとえば、自社のサーバー）に送信するには、別のプロファイルを設定します。

ステップ 3 宛先、メッセージのサイズ、メッセージの形式、および Smart Call Home メッセージ受信者への転送方法を設定します。デフォルトのメッセージ形式は XML です。デフォルトでイネーブルになっている転送方法は、電子メールです。

destination address { **email** *address* | **http** *url*[**reference-identity** *ref-id-name*]} |**message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

例：

```
ciscoasa(cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService reference-identity
 ExampleService
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

reference-identity オプションは、受信したサーバー証明書に対する RFC 6125 参照 ID チェックを有効にします。このチェックは、HTTP アドレスが設定されている宛先にのみ適用されます。ID チェックは設定済みの参照 ID オブジェクトに基づいて行われます。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。

電子メールアドレスは、Smart Call Home のメッセージを受け取る電子メールアドレスです（最長 100 文字）。デフォルトの最大 URL サイズは 5 MB です。

モバイル デバイスでメッセージを送信し、読み取るにはショート テキスト形式を使用し、コンピュータでメッセージを送信し、読み取るにはロング テキスト形式を使用します。

メッセージの受信者が Smart Call Home バックエンド サーバーの場合、バックエンド サーバーは XML 形式のメッセージのみ受け入れられるため **preferred-msg-format** の値が XML であることを確認します。

電子メールの転送方式をメールに戻すには、このコマンドを使用します。

宛先プロファイルのコピー

既存の宛先プロファイルをコピーして新しい宛先プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 コピーするプロファイルを指定します。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

ステップ 3 既存のプロファイルの内容を新しいプロファイルにコピーします。

copy profile *src-profile-name dest-profile-name*

例：

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

既存のプロファイル（*src-profile-name*) と新しいプロファイル (*dest-profile-name*）は最大 23 文字です。

例

次に、既存のプロファイルをコピーする例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

宛先プロファイルの名前の変更

既存のプロファイルの名前を変更するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 名前を変更するプロファイルを指定します。

profile *profilename*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

ステップ 3 既存のプロファイルの名前を変更します。

rename profile *src-profile-name dest-profile-name*

例：

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

既存のプロファイル（*src-profile-name*) と新しいプロファイル (*dest-profile-name*）は最大 23 文字です。

例

次に、既存のプロファイルの名前を変更する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

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。

- **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。

Smart Call Home の例

次の例は、Smart Call Home サービスを設定する方法を示しています。

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
 Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly
Monday 23:30
```

Anonymous Reporting および Smart Call Home の履歴

表 *3 : 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。 次のコマンドを導入または変更しました。 **active (call home)**、**call-home**、**call-home send alert-group**、**call-home test**、**contact-email-addr**、**customer-id (call home)**、**destination (call home)**、**profile**、**rename profile**、**service call-home**、**show call-home**、**show call-home detail**、**show smart-call-home alert-group**、**show call-home profile**、**show call-home statistics**、**show call-home mail-server status**、**show running-config call-home**、**show call-home registered-module status all**、**site-id**、**street-address**、**subscribe-to-alert-group all**、**alert-group-config**、**subscribe-to-alert-group configuration**、**subscribe-to-alert-group diagnostic**、**subscribe-to-alert-group environment**、**subscribe-to-alert-group inventory periodic**、**subscribe-to-alert-group snapshot periodic**、**subscribe-to-alert-group syslog**、**subscribe-to-alert-group telemetry periodic**。
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。 **call-home reporting anonymous**、**call-home test reporting anonymous** コマンドが導入されました。
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。

機能名	プラットフォーム リリース	説明
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。 次のコマンドが追加または変更されました。**[no] crypto ca reference-identity**、**call home profile destination address http**。

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。