REST での SGACL と環境データのダウンロード

このモジュールでは、REST API での SGACL および環境データのダウンロードについて説明します。

REST での SGACL と環境データのダウンロードの前提条件

- Cisco Identity Services Engine（ISE）のバージョンは 2.7 以降である必要があります。
- Cisco TrustSec 対応デバイスは、Cisco IOS XE Amsterdam 17.1.1 以降のリリースを使用する必要があります。
- Cisco ISE のネットワークデバイス設定を更新して、ネットワークデバイスの IP アドレス（NAS-IP）からの REST API コールを許可する設定を含める必要があります。Cisco ISE 設定で指定されたデバイス ID とパスワードは、Cisco ISE への REST API コールを行うネットワークデバイスによってユーザ名とパスワードとして含まれます。

REST での SGACL と環境データのダウンロードの制約事項

- Cisco TrustSec の認可変更（CoA）は、プロトコルとして RADIUS を使用します。
- ERS サーバポートとしてサポートされるのはポート 9063 だけです。
- Cisco IOS XE Amsterdam 17.1.1 では、サードパーティ認証局（CA）証明書はサポートされていません。自己署名証明書のみがサポートされています。
- サーバの統計情報は、環境データのリフレッシュ後は保持されません。
- Cisco IOS XE Amsterdam 17.1.1 では、IPv6 サーバはサポートされていません。Cisco IOS XE 17.2.1 では、IPv6 サーバがサポートされています。
- Cisco IOS XE Amsterdam 17.1.1 では、サーバごとに 1 つの IPv4 アドレスのみがサポートされています。
- サーバごとに 1 つの完全修飾ドメイン名（FQDN）のみがサポートされます。

REST での SGACL と環境データのダウンロードに関する情報

REST での SGACL と環境データのダウンロードの概要

Cisco IOS XE Amsterdam 17.1.1 以降のリリースでは、Cisco TrustSec は、Cisco Identity Services Engine（ISE）からのポリシーのプロビジョニングと環境データのダウンロードに REST ベースのトランスポートプロトコルを使用します。REST ベースのプロトコルは安全性に優れ、以前のリリースで使用されていた RADIUS プロトコルよりも、信頼性の高い高速なセキュリティグループ アクセス コントロール リスト（SGACL）ポリシーおよび環境データのプロビジョニングを提供します。

Cisco TrustSec データの REST API ベースおよび RADIUS ベースのダウンロードの両方がサポートされています。ただし、1 つのデバイスでアクティブにできるプロトコルは 1 つだけです。Cisco IOS XE Amsterdam 17.1.1 では、REST ベースのプロトコルがデフォルトです。ただし、**cts authorization list** コマンドを設定することで、プロトコルを RADIUS に変更できます。

（注） Cisco TrustSec の認可変更（CoA）は、引き続きプロトコルとして RADIUS を使用します。

Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）と環境データは、ポリシーのインストール後にアクティブデバイスからスタンバイデバイスに同期されます。ただし、REST API 接続またはセッションはスイッチオーバー中に同期されません。

Cisco IOS XE Amsterdam 17.1.1 では、サーバごとに 1 つの IPv4 アドレスのみがサポートされています。Cisco IOS XE Amsterdam 17.2.1 以降のリリースでは、サーバごとに 8 つの IPv4 アドレスと 8 つの IPv6 アドレスがサポートされています。

Cisco IOS XE Amsterdam 17.2.1 では、Cisco TrustSec デバイスは Cisco ISE からの 429 応答コードを受け入れます。この応答コードは、過負荷になると Cisco ISE によって送信されます。特定のサーバの 429 応答コードを受信すると、デバイスはサーバをデッドとしてマークし、リスト内の次のサーバ（プライベートまたはパブリック）に切り替えます。次の再試行は 60 秒後に行われます。

Cisco TrustSec 環境データ

環境データは、Cisco TrustSec 機能を補足する運用データで構成されます。デバイスから Cisco ISE への環境データ要求は、次のデータで構成されます。

- デバイス名：デバイスの名前を指定します。
- デバイス機能：追加データを指定します。

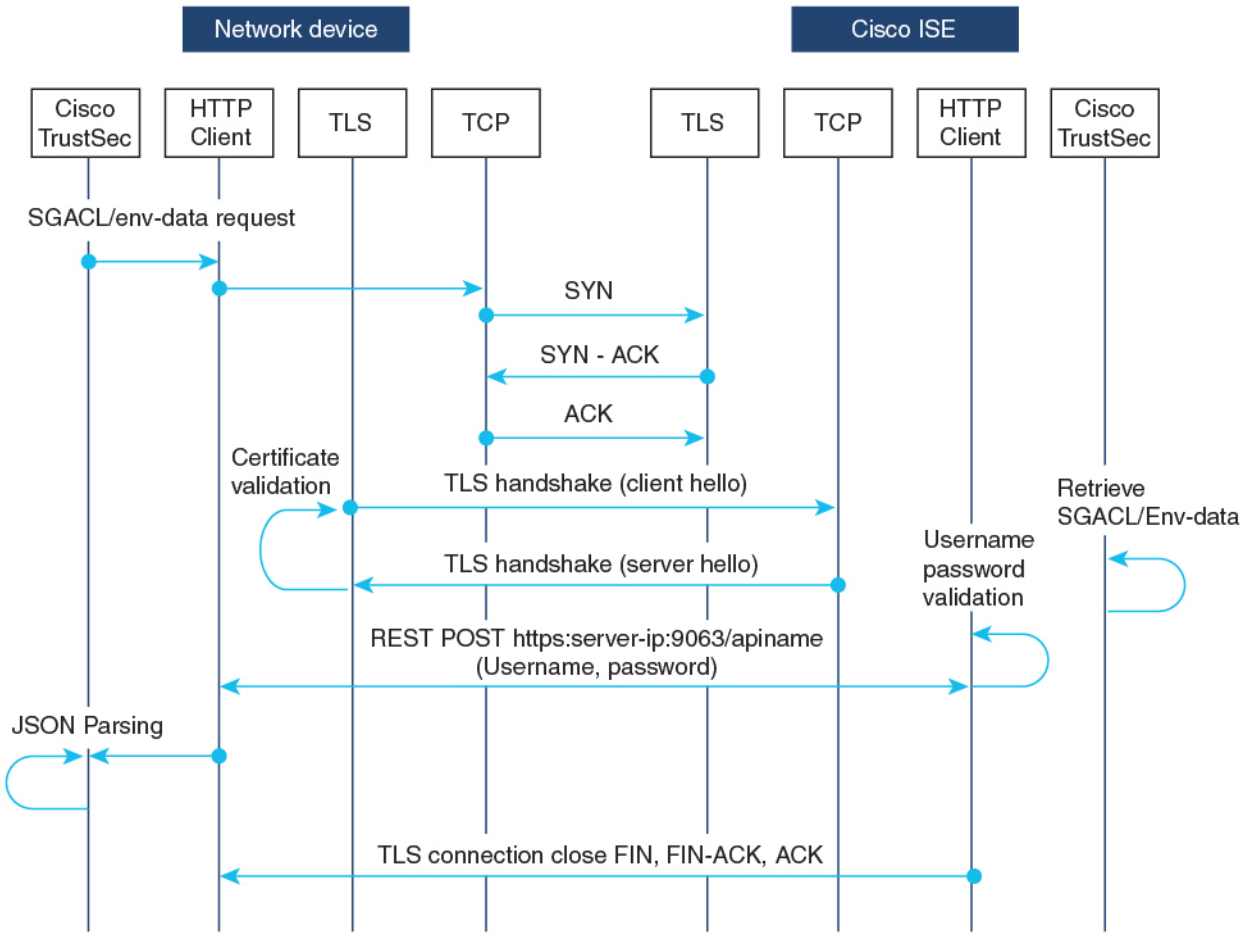
Cisco ISE からデバイスへの環境データ応答は、次のデータで構成されます。

- デバイスのセキュリティグループタグ（SGT）：デバイス名に基づいて Cisco ISE から取得されます。
- サーバリスト：Cisco ISE で指定された Cisco TrustSec サーバのリストを表示します。
- SG-Name テーブル：SGT とデバイス名の間のマッピングを表示します。SGT は数字で表示され、デバイス名はテキスト形式で表示されます。
- リフレッシュ時間：環境データがリフレッシュされる時間を示します。

ネットワークデバイスとサーバ間のメッセージフロー

次の図は、ネットワークデバイスとサーバ間の REST コールの接続管理を示しています。

図 *1:* ネットワークデバイスとサーバ間のメッセージフロー



- Cisco ISE REST API サービスは、ポート 9063 で Transport Layer Security（TLS）1.2 サーバを実行するセキュアソケットで実行され、SGACL および環境データのネットワークデバイス要求を処理します。
- デバイスによる TLS 接続の確立には「Make or Break」のアプローチが使用され、デバイスと Cisco ISE の間に永続的な TLS 接続はありません。TLS 接続が確立された後、その接続を使用して、デバイスから特定のリソースの Uniform Resource Locator（URL）に複数の REST API コールを送信できます。すべての REST 要求が処理されると、サーバからの TCP-FIN メッセージによって接続が切断されます。新しい REST API コールを送信するには、サーバとの新しい接続を確立する必要があります。
- デバイスから Cisco ISE への REST API コールは、TCP 接続の確立で開始されます。デバイスからの入力接続を許可するには、デバイスの IP アドレスを使用して Cisco ISE を設定する必要があります。Cisco ISE で設定されていない送信元 IP アドレスからの TCP 接続要求はドロップされ、監査ログが作成されます。
- ユーザ名とパスワード：すべての RESTAPI コールに、リソースの Uniform Resource Identifier（URI）へのアクセスを要求する際のユーザ名とパスワード認証を含める必要があります。

この認証により、サーバは発信者にリソースへのアクセス権を付与するか、要求を拒否するかを決定できます。

- Cisco ISE との TLS 接続を正常に確立するには、サーバを信頼するために、デバイスにサーバ証明書署名または PEM をトラストポイントとして（**crypto pki trustpoint** コマンドを使用して）インストールする必要があります。サーバ証明書のフィンガープリントまたは署名のみをエクスポートし、トラストポイントのデバイスにインストールする必要があります。サーバ証明書の秘密キーのインポートは必要ありません。
- TLS 接続の確立後、デバイス上の HTTP クライアントは、指定されたリソースで Cisco ISE への REST コールを開始します。

ポリシーサーバの選択基準

複数の HTTP ポリシーサーバが Cisco TrustSec デバイスに設定されています。サーバが選択されると、デバイスはこのサーバを使用して、サーバがデッドとしてマークされるまで Cisco ISE とやり取りします。

サーバの選択には 2 つのタイプがあります。

- 順序どおりの選択：これはデフォルトの動作です。サーバが設定された順序（パブリックサーバリスト）またはダウンロードされた順序（プライベートサーバリスト）で選択されます。サーバが選択されると、そのデバイスがデッドとしてマークされるまで使用され、その後にリストの次のサーバが選択されます。

  環境データが正常にダウンロードされ、サーバリストが使用可能になると、これらのサーバがプライベートサーバリストに追加されます。

- ランダムなサーバ選択：デバイスで複数の HTTP ポリシーサーバが設定されている場合、常に最初に設定されたサーバが選択されると、1 つの Cisco ISE インスタンスが過負荷になる可能性があります。この状況を回避するには、各デバイスでランダムにサーバを選択します。ランダムな番号がデバイスによって生成され、この番号に基づいてサーバが選択されます。デバイスごとにランダムな番号を生成するには、デバイスの一意のボード ID と Cisco TrustSec プロセス ID を使用して乱数ジェネレータを初期化します。

  サーバが選択されると、サーバがデッドとしてマークされるまで、以降のすべての要求がこのサーバに送信されます。サーバがデッドになると、ランダムなサーバ選択ロジックが次のアライブサーバを選択します。新しいサーバを選択する場合、アクティブサーバの数にデッドサーバは追加されません。サーバ番号は 0 から始まります。

  選択されたサーバ = (生成された乱数) % (アクティブサーバの総数) 。

サーバ選択ロジックをランダム方式に変更するには、**cts policy-server order random** コマンドを使用します。

サーバと IP アドレスの選択プロセス

サーバ選択の順序は、プライベートサーバリスト（サーバリストダウンロードの一部として受信）、パブリックサーバリスト（設定済みサーバ）の順です。これらのサーバリスト内での順序は、**cts policy-server order random** コマンドが有効かどうかに基づいて、ランダムな選択または順序どおり選択のどちらかになります。

Cisco IOS XE 17.2.1 以降のリリースでは、サーバごとに複数の IP（IPv4 と IPv6 の両方）アドレスがサポートされています。IP 選択の順序は、IPv4 アドレス、IPv6 アドレス、FQDN の順です。

このセクションでは、サーバと IP アドレスの選択の仕組みについて説明します。

1. デバイスを初めてブートアップすると、パブリック（設定済み）リストからサーバが選択されます。
2. **cts environment-data enable** コマンドが設定されている場合、デバイスはパブリックサーバを使用して Cisco ISE からプライベートサーバリストをダウンロードします。
3. プライベートリストを正常に受信すると、後続のすべての要求はプライベートリストを使用します。
4. サーバと IP アドレスを選択すると、デバイスはサーバと IP アドレスの組み合わせを使用して Cisco ISE に接続します。このサーバは、応答の取得に失敗するまで Cisco ISE とやり取りします。
5. プライベートリスト内の現在アクティブなサーバから応答を受信しなかった場合、デバイスはリスト内の次のサーバに切り替えます。サーバが初めて選択された場合、IP 選択ロジックは最初の到達可能な IP または IPv6 アドレスを検索します。
6. サーバと IP アドレスを選択すると、デバイスはダウンするまで使用されます。
7. プライベートリスト内のどのサーバにも到達できない場合、デバイスはパブリックリスト内のサーバへの接続を試みます。サーバスイッチングロジックと IP 選択は、プライベートリストとパブリックリストで同じです。
8. サーバの変更は、サーバリストがリフレッシュされたときにのみ行われます。
9. プライベートサーバリストとパブリックサーバリストの両方のすべてのサーバが停止している場合、デバイスはサーバと IP アドレスの選択ロジックをプライベートリストの先頭から再起動します。
10. 特定のサーバと IP アドレスの組み合わせに障害が発生すると、デバイスは 60 秒間待機してから新しい組み合わせを試行します。

サーバの有効性チェック

サーバが動作しているかどうかは、環境データまたは SGACL 要求を Cisco ISE に送信した後に判別されます。サーバがサーバリストの一部として設定またはダウンロードされた後は、有

効性検出のフェーズはありません。デフォルトのサーバステータスは、すべてのサーバタイプで有効です。

要求が Cisco ISE に送信され、サーバに到達できない場合、または応答が失われた場合、サーバはデッド状態に移行します。サーバ選択ロジックは、同じサーバと次の IP アドレス（複数のアドレスが設定されている場合）を選択して、Cisco ISE 要求の次のセットを送信します。デバイスが Cisco ISE から過負荷応答（HTTP 429）を受信した場合、ロジックはリスト内の次のサーバを選択します。

サーバは、次のいずれかの理由でデッドとしてマークされる可能性があります。

- 設定された IP アドレスに到達できない。
- ポート番号が正しくない。
- IP アドレスを持つ Cisco ISE インスタンスがダウンしている。
- Cisco ISE へのインターフェイスがダウンしている。
- Transport Layer Security（TLS）ハンドシェイクに失敗した。
- HTTP レスポンスのタイムアウト。
- ドメイン名が正しく設定されていない（ドメイン名が使用されている場合）。

サーバに静的 IP アドレスとドメイン名の両方が設定されている場合は、静的 IP アドレスが優先されます。静的 IP アドレスへの応答がない場合、デバイスはドメイン名で試行します。静的 IP アドレスとドメイン名の両方を含む応答を受信しない場合、サーバはデッドとしてマークされます。

プライベートリストのすべてのサーバがデッドとしてマークされると、デバイスはパブリックリストを使用します。残りのすべてのサーバもデッドとしてマークされると、回復メカニズムが開始されます。デバイスは、次の Cisco TrustSec 要求（ポリシーのリフレッシュ、環境データのダウンロードまたはリフレッシュなど）を待機し、すべてのサーバをアライブとしてマークしてダウンロードを再試行します。新しい Cisco TrustSec 要求のトリガーがない場合、サーバはデッド状態のままになります。

REST での SGACL と環境データのダウンロードを設定する方法

ユーザ名とパスワードの設定

デバイスで設定する前に、Cisco ISE でユーザ名とパスワードを REST API アクセス用のログイン情報として設定します。詳細については、「Cisco TrustSec Policies Configuration」の章の「Cisco TrustSec HTTP Servers」セクションを参照してください。

（注） **cts authorization-list** コマンドを使用して RADIUS ベースの設定を試行したときに HTTP ベースの構成がすでに有効になっている、コンソールに次のエラーメッセージが表示されます。

```
Error: 'cts policy-server or cts environment-data' related configs are enabled.
Disable http-based configs, to enable 'cts authorization'
```

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts policy-server name** *server-name* 例： `Device(config)# cts policy-server name ISE-server`	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバ コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-policy-server)# exit`	ポリシーサーバ コンフィギュレーション モードを終了して、グローバル コンフィギュレーションモードに戻ります。
ステップ 5	**cts policy-server username** *username* **password** {**0** | **6** |**7** | *password*} {*password*} 例： `Device(config)# cts policy-server username admin password 6 password1`	ユーザ名とパスワードを設定します。 （注） デバイスで設定する前に、Cisco ISE でこのユーザ名とパスワードを REST API アクセス用のログイン情報として作成する必要があります。
ステップ 6	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

証明書登録の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint mytp`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**crypto pki authenticate** *name* 例： `Device(config)# crypto pki authenticate mytp`	認証局（CA）証明書を取得して、認証します。証明書フィンガープリントをチェックするよう求められた場合、証明書フィンガープリントをチェックします。 （注） CA 証明書がコンフィギュレーションにすでにロードされている場合、このコマンドはオプションです。
ステップ 6	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco TrustSec ポリシーのダウンロード

cts role-based enforcement は、Cisco TrustSec ポリシーをダウンロードするようにすでに設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts policy-server name** *server-name* 例： `Device(config)# cts policy-server name ISE-server`	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバコンフィギュレーション モードを開始します。
ステップ 4	**address domain-name** *name* 例： `Device(config-policy-server)# address domain-name domain1`	ポリシーサーバのドメイン名のアドレスを設定します。

ステップ 5	**address** {**ipv4**| **ipv6** *policy-server-address*
	例：
	`Device(config-policy-server)# address ipv4 10.1.1.1`
	`Device(config-policy-server)# address ipv6 2001.DB8::1`
		ポリシーサーバの IPv4 または IPv6 アドレスを設定します。
		• Cisco IOS XE Amsterdam 17.1.1 では、IPv4 アドレスのみがサポートされています。

ステップ 6	**tls server-trustpoint** *name* 例： `Device(config-policy-server)# tls server-trustpoint tls1`	トランスポート層セキュリティのトラストポイントを設定します。
ステップ 7	**timeout** *seconds* 例： `Device(config-policy-server)# timeout 15`	（任意）応答のタイムアウトを秒単位で設定します。 • デフォルトは 5 秒です。
ステップ 8	**retransmit** *number-of-retries* 例： `Device(config-policy-server)# retransmit 4`	（任意）サーバからの最大リトライ回数を設定します。 • デフォルトは 4 です。
ステップ 9	**port** *port-number* 例：	（任意）ポリシーサーバのポート番号を設定します。

	コマンドまたはアクション	目的
	`Device(config-policy-server)# port 9063`	（注） ERS サーバのポート番号は 9063 である必要があります。このポート番号は変更できません。
ステップ 10	**content-type json** 例： `Device(config-policy-server)# content-type json`	（任意）Cisco ISE から SGACL および環境データを送信するコンテンツタイプを設定します。 （注） デフォルトでは、このコマンドが設定されていない場合でも、JSON がコンテンツタイプとして使用されます。
ステップ 11	**end** 例： `Device(config-policy-server)# end`	ポリシーサーバコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

環境データのダウンロード

HTTP 接続に使用する送信元インターフェイスは、 **ip http client source-interface** コマンドで指定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts policy-server device-id** *device-ID* 例： `Device(config)# cts policy-server device-id server1`	環境データ要求を Cisco ISE に送信するようにポリシーサーバのデバイス ID を設定します。 • このデバイス ID は、Cisco ISE でネットワーク アクセス デバイス（NAD）を追加するために使用したものである必要があります。

REST での SGACL と環境データのダウンロード

	コマンドまたはアクション	目的
ステップ 4	**cts environment-data enable** 例： `Device(config)# cts environment-data enable`	Cisco ISE からの環境データのダウンロードを有効にします。 （注） **cts environment-data enable** コマンドと **cts authorization list** コマンドは相互に排他的な関係にあります。これらのコマンドを一緒に設定することはできません。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

REST での SGACL と環境データのダウンロード

次のコマンドを任意の順序で使用します。

- **show cts policy-server details name**

  指定されたポリシーサーバに関する情報を表示します。

```
Device# show cts policy-server details name ise_server_1

Server Name   : ise_server_1
Server Status : Active
  IPv4 Address     : 10.64.69.84
  IPv6 Address     : 2001:DB::2
  Trustpoint       : ISE84
  Port-num         : 9063
  Retransmit count : 3
  Timeout          : 15
  App Content type : JSON
```

- **show cts policy-server statistics active**

  アクティブなポリシーサーバに関する静的情報を表示します。

  activeにせずにコマンドを使用すると、すべてのサーバの統計情報が表示されます。

```
Device# show cts policy-server statistics active

Server Name  : ise_server_1
Server State : ALIVE
  Number of Request sent        : 7
  Number of Request sent fail   : 0
  Number of Response received   : 4
  Number of Response recv fail  : 3
    HTTP 200 OK                 : 4
    HTTP 400 BadReq             : 0
    HTTP 401 UnAuthorized Req   : 0
    HTTP 403 Req Forbidden      : 0
```

```
    HTTP 404 NotFound           : 0
    HTTP 408 ReqTimeout         : 0
    HTTP 415 UnSupported Media  : 0
    HTTP 500 ServerErr          : 0
    HTTP 501 Req NoSupport      : 0
    HTTP 503 Service Unavailable: 0
    TCP or TLS handshake error  : 3
    HTTP Other Error            : 0
```

- **show cts server-list**

  環境データの一部としてダウンロードされるサーバのリストを表示します。これらのサーバは、プライベートサーバリストの一部になります。

  （注） 次の出力には、HTTP ベースのダウンロード情報が表示されています。

```
Device# show cts server-list

HTTP Server-list:
  Server Name      : cts_private_server_0
  Server State     : ALIVE
  IPv4 Address     : 10.64.69.151
  IPv6 Address     : 2001:DB8:8086:6502::
  IPv6 Address     : 2001:db8::2
  IPv6 Address     : 2001:db8::402:99
  IPv6 Address     : 2001:DB8:4::802:16
  Domain-name      : ise-267.cisco.com
  Trustpoint       : cts_trustpoint_0

  Server Name      : cts_private_server_1
  Server State     : ALIVE
  IPv4 Address     : 10.10.10.3
  IPv4 Address     : 10.10.10.2
  IPv6 Address     : 2001:DB8::20
  IPv6 Address     : 2001:DB8::21
  Domain-name      : www.ise.cisco.com
  Trustpoint       : cts_trustpoint_1
```

REST 設定での SGACL と環境データのデバッグ

設定をデバッグするには、次の **debug** コマンドを使用します。

- **debug cts policy-server http**

  HTTP クライアントのデバッグを有効にします。

- **debug cts policy-server json**

  JSON クライアントのデバッグを有効にします。

REST での SGACL と環境データのダウンロードの設定例

例：ユーザ名とパスワードの設定

```
Device> enable
Device# configure terminal
Device(config)# cts policy-server name ISE-server
Device(config-policy-server)# exit
Device(config)# cts policy-server username admin 6 password1
Device(config)# end
```

例：Cisco TrustSec ポリシーのダウンロード

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement
Device(config)# cts policy-server name ISE-server
Device(config-policy-server)# address domain-name domain1
Device(config-policy-server)# address ipv4 10.1.1.1
Device(config-policy-server)# address ipv6 2001:DB8::1
Device(config-policy-server)# tls server-trustpoint tls1
Device(config-policy-server)# timeout 15
Device(config-policy-server)# retransmit 4
Device(config-policy-server)# port 2010
Device(config-policy-server)# end
```

例：環境データのダウンロード

```
Device> enable
Device# configure terminal
Device(config)# cts policy-server name ISE-server
Device(config-policy-server)# exit
Device(config)# cts policy-server device-id server1
Device(config)# cts env-data enable
Device(config)# end
```

REST での SGACL と環境データのダウンロードの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.1.1	REST での SGACL と環境データのダウンロード	Cisco TrustSec は、Cisco ISE からの SGACL ポリシーのプロビジョニングとデータのダウンロードに REST ベースのトランスポートプロトコルを使用します。
Cisco IOS XE Amsterdam 17.2.1	IPv6 ポリシーサーバによる HTTP SGACL の適用	ポリシーサーバの IPv6 アドレスがサポートされています。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。