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ー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 サーバー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。
- サーバーの統計情報は、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 サーバーはサポートされていません。
- Cisco IOS XE Amsterdam 17.1.1 では、サーバーごとに 1 つの IPv4 アドレスのみがサポートされています。
- RADIUS 自動テスト機能は、VRF 環境ではサポートされていません。

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 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。

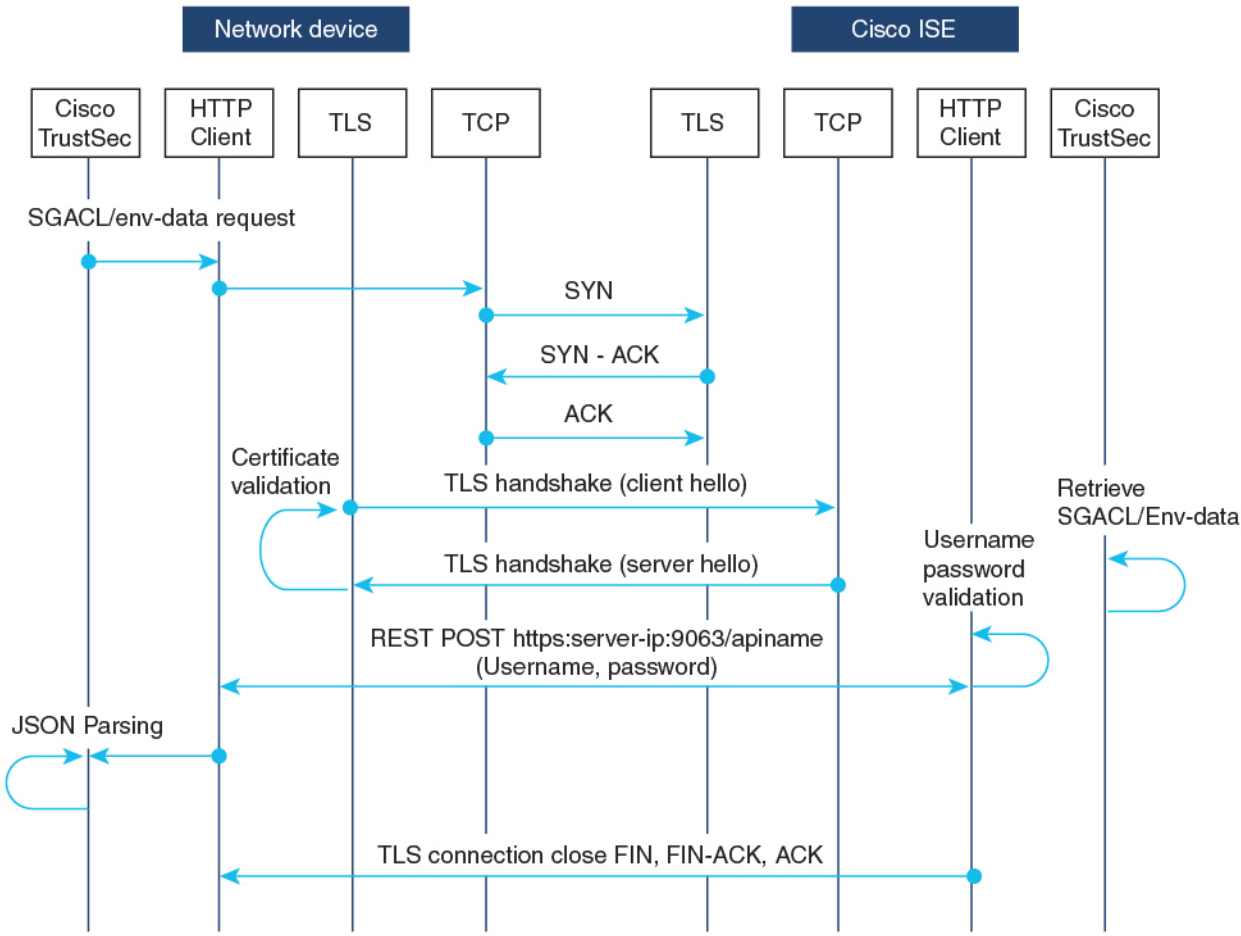
- デバイスのセキュリティグループタグ（SGT）：デバイス名に基づいて Cisco ISE から取得されます。
- サーバーリスト：Cisco ISE で指定された Cisco TrustSec サーバーのリストを表示します。
- SG-Name テーブル：SGT とデバイス名の間のマッピングを表示します。SGT は数字で表示され、デバイス名はテキスト形式で表示されます。
- リフレッシュ時間：環境データがリフレッシュされる時間を示します。

（注） Cisco TrustSec 環境のデータ更新の一環として、最後に受信したサーバーが削除され、新しく受信したサーバーがサーバーリストに追加されます。更新後、サーバーリストの統計がゼロから再開され、サーバーのステータスが [Inactive] に設定されます。また、IP アドレスの状態が [Reachable] に設定されます。次に、デバイスは、後続のポリシー要求と応答に基づいてサーバーの統計とステータスを更新します。

ネットワークデバイスとサーバー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ー間の 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ー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 サーバー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、サーバーからの 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、サーバー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。
- ユーザー名とパスワード：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ー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、サーバー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、サーバーを信頼するために、デバイスにサーバー証明書署名または 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。サーバー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。サーバー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。

ポリシーサーバーの選択基準

複数の HTTP ポリシーサーバーが Cisco TrustSec デバイスに設定されています。サーバーが選択されると、デバイスはこのサーバーを使用して、サーバー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。

サーバーの選択には 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。サーバーが設定された順序（パブリックサーバーリスト）またはダウンロードされた順序（プライベートサーバーリスト）で選択されます。サーバーが選択されると、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ーが選択されます。

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

- ランダムなサーバー選択：デバイスで複数の HTTP ポリシーサーバーが設定されている場合、常に最初に設定されたサーバーが選択されると、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ーを選択します。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 CTS 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。

  サーバーが選択されると、サーバー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ーに送信されます。サーバーがデッドになると、ランダムなサーバー選択ロジックが次のアライブサーバーを選択します。新しいサーバーを選択する場合、アクティブサーバーの数にデッドサーバーは追加されません。サーバー番号は 0 から始まります。

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

サーバー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。

サーバーは、プライベートサーバーリスト（サーバーリストダウンロードの一部として受信）、パブリックサーバーリスト（設定済みサーバー）の順に選択されます。これらのサーバーリス

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。

サーバーの有効性チェック

サーバー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。サーバーがサーバー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ーステータスは、すべてのサーバータイプで有効です。

要求が Cisco ISE に送信され、サーバーに到達できない場合、または応答が失われた場合、サーバーはデッド状態に移行します。サーバー選択ロジックは、次のサーバーと IP アドレスを選択して、Cisco ISE 要求の次のセットを送信します。現在のサーバーに複数の IP アドレスがある場合でも、ロジックはリスト内の次のサーバーを選択します。基本的に、ロジックはサーバーを切り替えますが、同じサーバー内の IP アドレスは切り替えません。

サーバーは、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。
- TLS ハンドシェイクが失敗した。
- 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）。

サーバーに静的 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、サーバー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ー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ー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、すべてのサーバーをアライブと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、サーバー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

ユーザー名とパスワードの設定

デバイスで設定する前に、Cisco ISE でユーザー名とパスワードを 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 ポリシーサーバーを設定し、ポリシーサーバー 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`	ポリシーサーバー 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*}	ユーザー名とパスワードを設定します。

	コマンドまたはアクション	目的
	例： `Device(config)# cts policy-server username admin password 6 password1`	（注） デバイスで設定する前に、Cisco ISE でこのユーザー名とパスワードを 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。

	コマンドまたはアクション	目的
		（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 ポリシーサーバーを設定し、ポリシーサーバー 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`	ポリシーサーバーのドメイン名のアドレスを設定します。
ステップ 5	**address ipv4** *ip-address* 例： `Device(config-policy-server)# address ipv4 10.1.1.1`	ポリシーサーバーの IP アドレスを設定します。
ステップ 6	**tls server-trustpoint** *name* 例：	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。

	コマンドまたはアクション	目的
	`Device(config-policy-server)# tls server-trustpoint tls1`	
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）サーバー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： `Device(config-policy-server)# port 9063`	（任意）ポリシーサーバーのポート番号を設定します。 （注） ERS サーバーのポート番号は 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`	ポリシーサーバー 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。

REST での SGACL と環境データのダウンロード

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ーのデバイス 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。
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ー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
```

REST での SGACL と環境データのダウンロード

```
  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ー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、すべてのサーバー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ーのリストを表示します。これらのサーバーは、プライベートサーバー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: Http_Server_1
Server Status: DEAD
    IPv4 Address: 10.78.105.148
    IPv6 Address: Not Supported
    Domain-name: http_server_1.ise.com
    Port: 9063


Server Name: Http_Server_2
Server Status: ALIVE
    IPv4 Address: 10.78.105.149
    IPv6 Address: Not Supported
    Domain-name: http_server_2.ise.com
```

```
Status = ALIVE
```

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：ユーザー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)# 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 ポリシーサーバーによる HTTP SGACL の適用	ポリシーサーバーの 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 [英語] からアクセスします。

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。