TrustSec 動作データへの外部アクセス

Cisco TrustSec は、信頼できるネットワーク デバイスのドメインを確立することによってセキュア ネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。

Cisco TrustSec は、グループベースのアクセス制御を使用したセキュリティも提供します。Cisco TrustSec ドメイン内のアクセスポリシーは、トポロジとは無関係であり、ネットワークアドレスではなく送信元デバイスおよび宛先デバイスのロールに基づいています。個々のパケットには、送信元のセキュリティ グループ番号のタグが付けられます。

Cisco TrustSec は、設定データと動作データの 2 種類のデータを生成します。設定データは設定プログラミングモデルから取得され、動作データは動作データモデルから取得されます。

TrustSec の運用データには、YANG を使用して構造化されたデータを処理できる外部アプリケーションからアクセスできます。Netconf および Restconf プロトコルを使用して、外部デバイスは Cisco デバイスから動作情報を抽出できます。これにより、外部インターフェイスを介したプログラマビリティが提供されます。

Cisco TrustSec 動作データへの外部アクセスの前提条件

- Cisco TrustSec、ネットワークデバイス間での SXP を使用したセキュリティタグの伝達、およびポリシーの適用について理解している必要があります。
- Cisco IOS XE Everest 16.5.1 以降、Cisco TrustSec は、IP Services または IP Base のライセンスでのみ暗号 k9 イメージをサポートします。

- Cisco デバイスで NETCONF または RESTCONF プロトコルを有効にする必要があります。NETCONF プロトコルを有効にするには、コンフィギュレーション モードで **netconf-yang** コマンドを使用します。

（注） LANbase ライセンスは SXP のみをサポートします。SGACL および IP-SGT 動作データはサポートされていません。

Cisco TrustSec 動作データへの外部アクセスの制限

- SGACL ポリシーと IP-SGT および SXP 接続に限定された動作データには、外部からのみアクセスできます。
- 次の TrustSec 動作データのリストは、Cisco IOS XE Everest 16.5.1 ではサポートされていません。
  - Cisco TrustSec PAC データ、環境データ、およびリンクレベルの動作データ。
  - IPV6 ベースの SGACL ポリシー、IP-SGT マッピング、および SXP 接続動作データ。
  - VFR ベースの IP-SGT マッピングおよび SXP 接続動作データ。

Cisco TrustSec 動作データに関する情報

YTOOL などのアプリケーションを使用すると、Cisco デバイスに直接ログインして専用のコマンドで情報を取得することなく、外部インターフェイスから Cisco TrustSec の動作データに柔軟にアクセスできます。

外部デバイスからは、次のタイプの動作データにアクセスできます。

- 特定のデバイスのアクティブな SXP 接続。

  次に、デバイスの SXP 接続を表示する出力例を示します。

```
Device# show cts sxp connections brief
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set

---------------------------------------------------------------------------------------
---------------
Peer_IP          Source_IP        Conn Status
    Duration
```

```
---------------------------------------------------------------------------
---------------
10.10.1.1         11.11.1.1         Off
    0:00:36:24 (dd:hr:mm:sec)
10.10.1.2         11.11.1.2         Off
    0:00:36:24 (dd:hr:mm:sec)
10.10.1.3         11.11.1.3         Off
    0:00:36:23 (dd:hr:mm:sec)
10.10.1.4         11.11.1.4         Off
    0:00:36:22 (dd:hr:mm:sec)
10.10.1.5         11.11.1.5         Off
    0:00:36:22 (dd:hr:mm:sec)
10.10.1.6         11.11.1.6         Off
    0:00:36:21 (dd:hr:mm:sec)
10.10.1.7         11.11.1.7         Off
    0:00:36:21 (dd:hr:mm:sec)
10.10.1.8         11.11.1.8         Off
    0:00:36:20 (dd:hr:mm:sec)
10.10.1.9         11.11.1.9         Off
    0:00:36:15 (dd:hr:mm:sec)
10.10.1.10        11.11.1.10        Off(Speaker)::Off(Listener)
    0:00:33:40 (dd:hr:mm:sec)::0:00:33:40 (
dd:hr:mm:sec)
```

- IP-SGT マッピング情報。

  すべての送信元 IP が、対応する SGT にマッピングされ、IP-SGT バインディングが作成されます。このマッピング情報は、ロールベースマネージャ（RBM）データベースに保存されます。

  次に、IP-SGT マッピング情報を表示する出力例を示します。

```
Device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.10.10.10             10      CLI
20.20.20.20             20      CLI
30.30.30.30             30      CLI
32.1.1.32               40      CLI
45.1.1.45               100     CLI
69.1.1.1                103     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 6
Total number of active   bindings = 6

asr1k-cts-2006#
```

- すべてのデータパスに現在適用されているポリシーの名前。

  SGACL ポリシーは、2 つの TrustSec 対応エンドポイント間で SGT タグ付きパケットが転送されるときに適用されます。ポリシーは、スタティックまたはダイナミックのいずれかです。デバイスで CLI コマンドの **cts role-based permissons** を使用して設定されるポリシーは、スタティックポリシーです。ダイナミックポリシーは Cisco ISE（Identiy Services Engine）で設定されます。ダイナミックポリシーは、スタティックポリシーに優先します。スタティックポリシーは、ダイナミックポリシーがない場合にのみ適用されます。

  次に、SGT タグ付きトラフィックのポリシーを表示する出力例を示します。

```
Device# show cts role-based permissions
IPv4 Role-based permissions default:

        Permit IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 10:SGT_10:

        Collab1-10
IPv4 Role-based permissions from group 10:SGT_10 to group 20:SGT_20:

        SGACL_2-30
IPv4 Role-based permissions from group 11:SGT_11 to group 20:SGT_20:

        SGACL_2-30

        SGACL_3-10

        SGACL_4-90
IPv4 Role-based permissions from group 12:SGT_12 to group 20:SGT_20:

        SGACL_3-10
IPv4 Role-based permissions from group 13:SGT_13 to group 20:SGT_20:

        SGACL_4-90
IPv4 Role-based permissions from group 14:SGT_14 to group 20:SGT_20:
        SGACL_5-20
IPv4 Role-based permissions from group 15:SGT_15 to group 20:SGT_20:
        SGACL_6-30
IPv4 Role-based permissions from group 16:SGT_16 to group 20:SGT_20:
        SGACL_101-90
IPv4 Role-based permissions from group 17:SGT_17 to group 20:SGT_20:
        SGACL_2-30
IPv4 Role-based permissions from group 18:SGT_18 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 19:SGT_19 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 10:SGT_10 to group 30:SGT_30:
        SGACL_6-30
IPv4 Role-based permissions from group 10:SGT_10 to group 40:SGT_40:
        SGACL_2-30
IPv4 Role-based permissions from group 10:SGT_10 to group 100:SGT_100:
        SGACL_4-90
IPv4 Role-based permissions from group 102:SGT_102 to group 100:SGT_100:
        Permit IP-00
IPv4 Role-based permissions from group 102:SGT_102 to group 103:SGT_103:
        SGACL_2-30
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

asr1k-cts-2006#
```

- 各ポリシーの内容。これには、ポリシー内のACE（アクセス制御エントリ）と、ポリシーのライフタイムおよび更新時間が含まれます。

  ポリシーには、最大 256 の ACE を組み合わせて含めることができます。ライフタイムと更新時間の情報は、ダイナミックポリシーにのみ適用されます。スタティックポリシーのライフタイムと更新時間の値は 0 になります。

  次に、SGT タグ付きトラフィックのポリシーを表示する出力例を示します（出力の一部のみが表示されます）。

```
Device# show cts policy sgt
CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0x41408001
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:42 IST Mon Feb 20 2017
Policy expires in 0:00:03:04 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:04 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 65535-52:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-52:ANY-0, Destination SGT: 65535-52:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 4
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:43 IST Mon Feb 20 2017
Policy expires in 0:00:03:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:05 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 10-2770:SGT_10
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 10-2770:SGT_10-0, Destination SGT: 10-2770:SGT_10-0
  rbacl_type = 80
  rbacl_index = 1
  name   = Collab1-10
  IP protocol version = IPV4
  refcnt = 2
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:43 IST Mon Feb 20 2017
Policy expires in 0:00:03:04 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:04 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 20-44:SGT_20
SGT Policy Flag: 0x41400001
RBACL Source List:
```

```
Source SGT: 10-2770:SGT_10-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 1
name   = SGACL_2-30
IP protocol version = IPV4
refcnt = 8
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip

Source SGT: 12-17:SGT_12-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 2
name   = SGACL_3-10
IP protocol version = IPV4
refcnt = 5
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip

Source SGT: 13-14:SGT_13-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 3
name   = SGACL_4-90
IP protocol version = IPV4
refcnt = 5
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  deny tcp

Source SGT: 14-14:SGT_14-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 4
name   = SGACL_5-20
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip

Source SGT: 15-1410:SGT_15-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 5
name   = SGACL_6-30
IP protocol version = IPV4
refcnt = 4
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit icmp log
  permit udp log
  permit tcp log

Source SGT: 16-14:SGT_16-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 6
name   = SGACL_101-90
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
```

```
stale  = FALSE
RBACL ACEs:
  permit ip
```

外部デバイス YTOOL の設定方法

YTOOL を設定する前に、Cisco デバイスで NETCONF または RESTCONF プロトコルが有効になっていることを確認します。YTOOL が Cisco デバイスと通信するには、これらのプロトコルのいずれかが必要です。

（注） NETCONF プロトコルを有効にするには、コンフィギュレーション モードで **netconf-yang** コマンドを使用します。NETCONF を有効にしたら、CLI で **show onep session all** を実行して、NETCONF を使用するために必要な 3 つのプロセスが実行されているかどうかを確認します。NETCONF は、これらの 3 つのプロセスが実行された後にのみ使用できます。

また、デバイスとの通信に使用する IP アドレスを特定します。

（注） YTOOL は「yang-explorer」とも呼ばれます。このアプリケーションは、次の場所からダウンロードできます。

Yang Explorer：

YTOOL を Cisco デバイスに接続するには、Cisco デバイスを YTOOL に追加します。YTOOL にシスコデバイスを追加する手順は、次のとおりです。

1. YTOOL を開きます。
2. **[管理（Admin）]** を選択します。
3. **[Ytool ユーティリティ（Ytool Utilities）]** ページで、**[プロファイルの管理（Manage Profiles）]**（**[デバイスプロファイルの管理（Manage Device Profiles）]** の下）を選択します。
4. **[デバイスプロファイル名（Device Profile Name）]** ドロップダウンから **[新規デバイス（New Device）]** を選択します。
5. [デバイスプロファイルの管理（Manage Device Profile）] ページで、デバイスのすべての詳細情報（テストデバイスの IP アドレス、テストデバイスの SSH ポート番号、NETCONF ユーザー名、NETCONF パスワードなど）を入力します。

図 *1*: デバイス プロファイルの管理

6. デバイスへの接続を確認するには、**[ビルド（Build）]** > **[デバイス設定（Device Settings）]** の順に選択します。**[プロファイル（Profile）]** からデバイスを選択し、**[Hello]** をクリックします。**[コンソール（Console）]** に応答が表示された場合は、YTOOL がデバイスと通信できることを意味します。

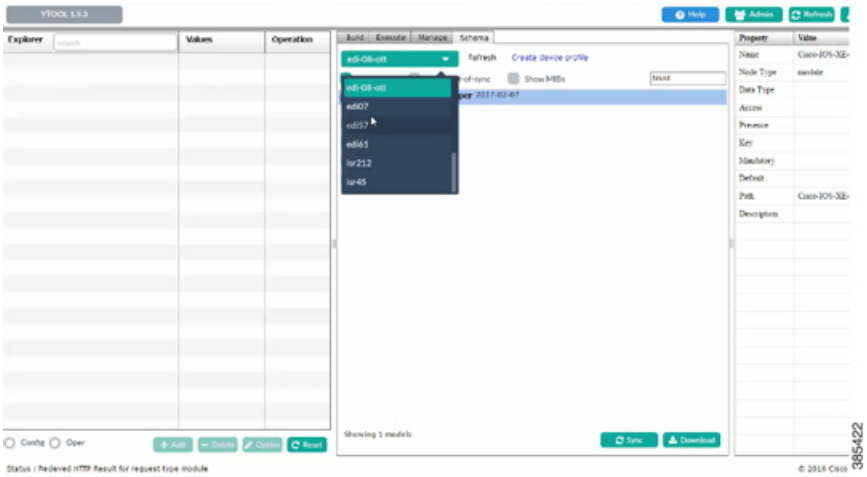
（注） Cisco デバイスと通信するために、YANG を使用して構造化されたデータを処理できる他の外部アプリケーションを選択できます。このセクションは、Cisco デバイスにアクセスするために YTOOL を選択した場合にのみ関係します。

動作データへのアクセス

開始する前に、動作データを抽出する Cisco デバイスが YTOOL で設定されていることを確認します。詳細については、「外部デバイス YTOOL の設定方法」を参照してください。

1. Cisco デバイスから Cisco TrustSec 動作情報スキーマをダウンロードします。
   1. **[スキーマ（Schema）]** を選択します。
   2. デバイスを選択します。デバイス内のスキーマのリストが表示されます。

図 *2:* デバイスの選択

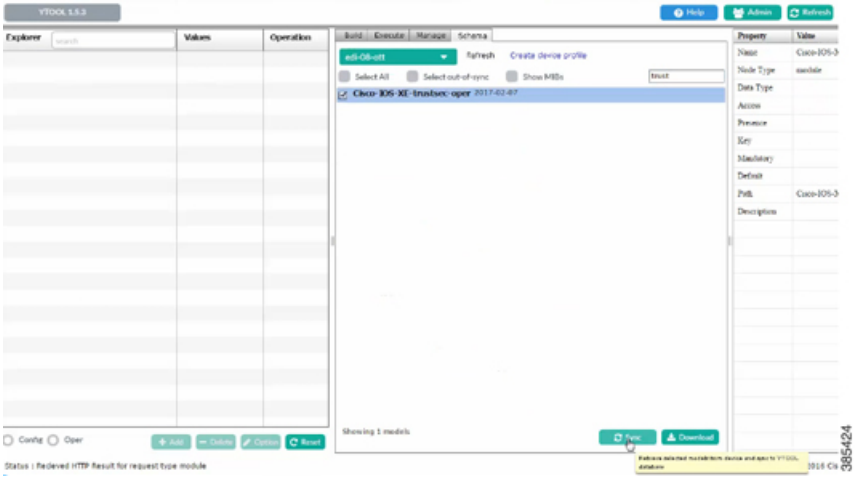


3. Cisco TrustSec 動作情報スキーマを選択します。検索ボックスを使用して、このスキーマを検索してください。

（注） 動作情報スキーマの名前は「**oper**」で終わります。

4. [同期（Sync）] をクリックします。スキーマが YTOOL にダウンロードされます。

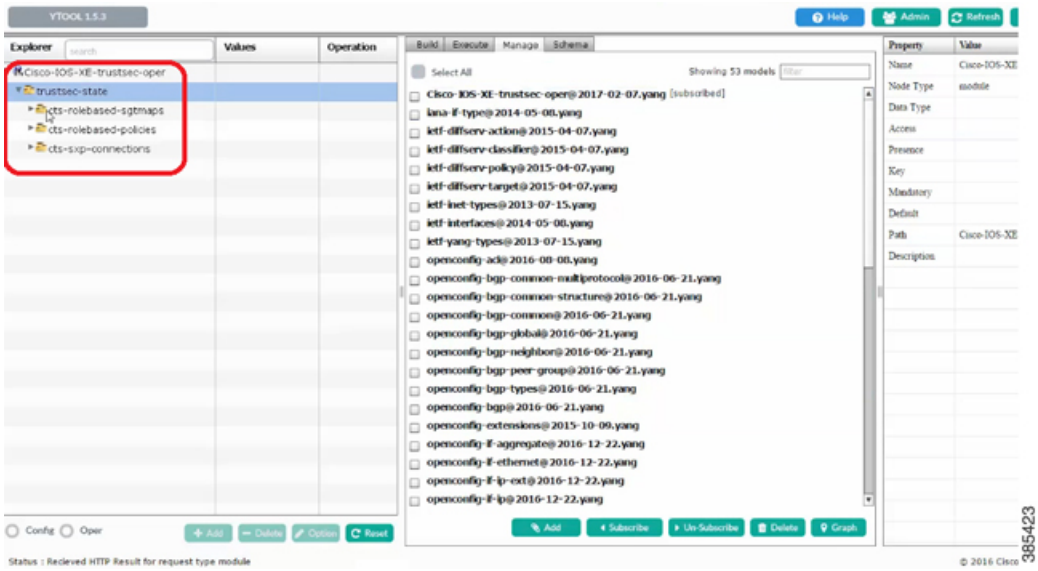
図 *3:* スキーマのダウンロード



2. YTOOL でダウンロードした動作情報スキーマに登録します。
   1. **[管理（Manage）]** を選択します。
   2. スキーマのリストから、動作情報スキーマを選択します。
   3. [Subscribe] をクリックします。

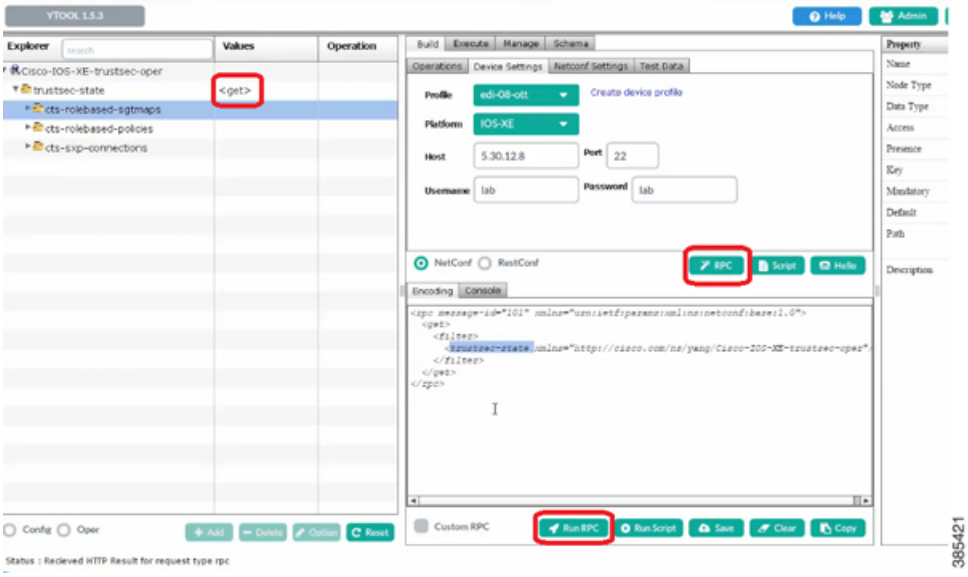
（注） 登録すると、スキーマが [エクスプローラ（Explorer）] の欄に表示されます。

図 *4:* スキーマの登録



3. スキーマを使用して、選択した動作データを取得します。
   1. 動作情報スキーマの関連情報レベルに対して、**[値（Values）]** の欄の **[取得（get）]** を選択します。
   2. **[RPC]** をクリックします。XML 生成の RPC メッセージが生成されます。
   3. **[RPC の実行（Run RPC）]** をクリックします。動作データは、RPC 生成の XML 形式で Cisco デバイスから取得されます。

図 *5 :* 動作データの取得



（注） 運用データへのアクセスに使用されるコマンドについては、「Cisco TrustSec 動作データに関する情報 （2 ページ）」の項を参照してください。

（注） Cisco デバイスと通信するために、YANG を使用して構造化されたデータを処理できる他の外部アプリケーションを選択できます。このセクションは、Cisco デバイスにアクセスするために YTOOL を選択した場合にのみ関係します。

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。