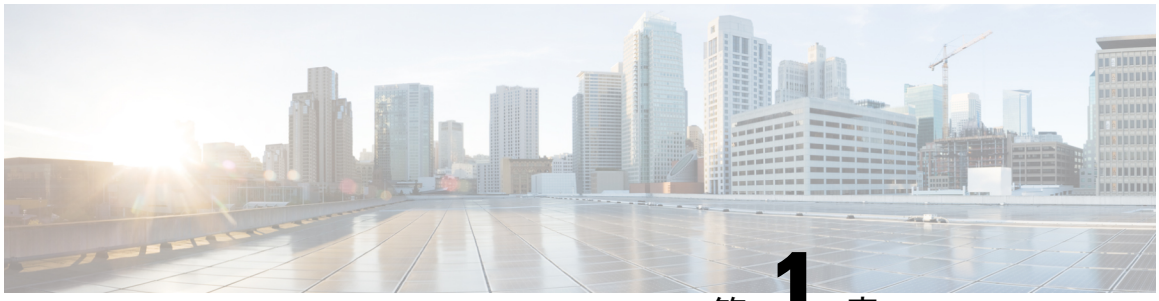
Cisco IOS XE Amsterdam 17.3.x（Catalyst 9300 スイッチ）Cisco TrustSec コンフィギュレーション ガイド

初版：2020 年 7 月 31 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

Cisco TrustSec の概要

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 の制約事項

- 無効なデバイス ID が指定された場合、Protected Access Credential（PAC）のプロビジョニングが失敗し、ハング状態のままになります。PAC をクリアし、正しいデバイス ID とパスワードを設定した後でも、PAC は失敗します。

  回避策として、Cisco Identity Services Engine（ISE）で、PAC が機能するように、[Administration] > [System] > [Settings] > [Protocols] > [Radius] メニューの [Suppress Anomalous Clients] オプションをオフにします。

- FIPS モードで Cisco TrustSec はサポートされていません。

Cisco TrustSec のアーキテクチャに関する情報

Cisco TrustSec のセキュリティ アーキテクチャは、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、ネットワークに入るようにセキュリティ グループ（SG）がパケットを分類するために認証中に取得したデバイスおよびユーザー クレデンシャルを使用します。このパケット分類は、Cisco TrustSec ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータパス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。このタグはセキュリティ グループ タグ（SGT）と呼ばれ、エンドポイント デバイスはこの SGT に基づいてトラフィックをフィルタリングできるので、ネットワークへのアクセス コントロール ポリシーの適用が可能になります。

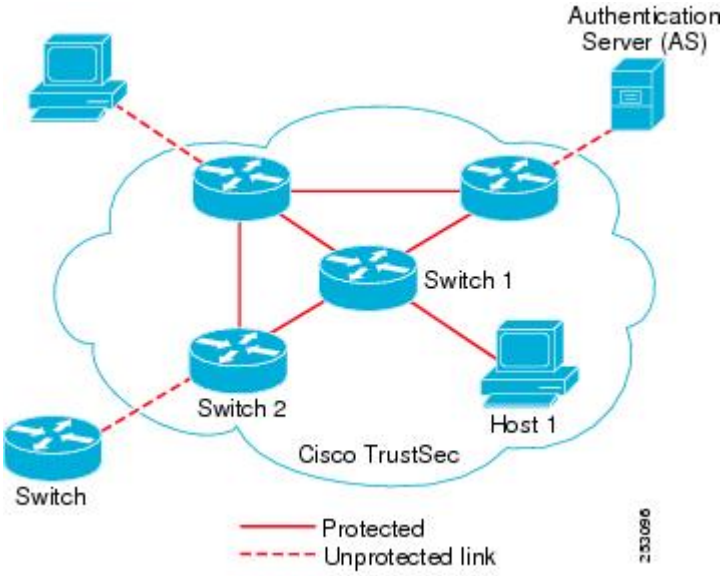
（注） Cisco TrustSec IEEE 802.1X リンクは、Cisco IOS XE Denali、Cisco IOS XE Everest、および Cisco IOS XE Fuji リリースでサポートされているプラットフォームではサポートされていないため、オーセンティケータのみがサポートされます。サプリカントはサポートされていません。

Cisco TrustSec のアーキテクチャは、3 種類の主要コンポーネントで構成されています。

- 認証されたネットワーキング インフラストラクチャ：Cisco TrustSec ドメインを開始するために最初のデバイス（シードデバイス）が認証サーバーで認証した後に、ドメインに追加された新しい各デバイスはドメイン内のピア デバイスにより認証されます。ピアは、ドメインの認証サーバーに対する媒介として動作します。それぞれの新たに認証されたデバイスは認証サーバーによって分類され、アイデンティティ、ロールおよびセキュリティ ポスチャに基づいてセキュリティ グループ番号が割り当てられます。
- セキュリティ グループ ベースのアクセス コントロール：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、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（セキュリティ グループ番号で指定）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。
- セキュアな通信：暗号化対応ハードウェアでは、暗号化、メッセージ整合性検査、データパス リプレイ保護メカニズムの組み合わせを使用してドメイン内のデバイス間の各リンクの通信を保護できます。

次の図に、Cisco TrustSec ドメインの例を示します。この例では、Cisco TrustSec ドメイン内に、ネットワーク接続されたデバイスが数台とエンドポイント装置が 1 台あります。エンドポイント装置 1 台とネットワーク接続デバイス 1 台がドメインの外部にあるのは、これらが Cisco TrustSec 対応デバイスでないか、またはアクセスを拒否されたためです。認証サーバーは、Cisco TrustSec ドメインの外部にあると見なされます。これは、Cisco Identities Service Engine（Cisco ISE）、または Cisco Secure Access Control System（Cisco ACS）です。

図 *1 : Cisco TrustSec* ネットワーク ドメインの例



Cisco TrustSec 認証プロセスの各参加者は、次のいずれかの役割を果たします。

- サプリカント：Cisco TrustSec ドメインへの参加を試行している、Cisco TrustSec ドメイン内のピアに接続されている認証されないデバイス。
- 認証サーバー：サプリカントのアイデンティティを確認し、Cisco TrustSec ドメイン内のサービスへのサプリカントのアクセスを決定するポリシーを発行します。
- オーセンティケータ：すでに Cisco TrustSec ドメインの一部であり、認証サーバーに代わって新しいピアサプリカントを認証できる認証済みデバイス。

サプリカントとオーセンティケータの間のリンクの初回の確立時には、通常は次の一連のイベントが発生します。

1. 認証（802.1X）：サプリカントは認証サーバーによって認証され、オーセンティケータが仲介として機能します。相互認証は、2 つのピア（サプリカントとオーセンティケータ）間で実行されます。
2. 認可：サプリカントのアイデンティティ情報に基づいて、認証サーバーは、リンクされた各ピアにセキュリティグループの割り当てや ACL などの認可ポリシーを提供します。認証サーバーは各ピアのアイデンティティを相互に提供し、各ピアはリンクに適切なポリシーを適用します。
3. セキュリティアソシエーションプロトコル（SAP）ネゴシエーション：リンクの両側で暗号化がサポートされている場合、サプリカントとオーセンティケータはセキュリティアソシエーション（SA）を確立するために必要なパラメータをネゴシエートします。

（注） SAP は 100G インターフェイスではサポートされていません。100G インターフェイスでは、MACsec Key Agreement Protocol（MKA）と Extended Packet Numbering（XPN）を使用することを推奨します。

3 つのステップがすべて完了すると、オーセンティケータはリンクの状態を無許可（ブロッキング）状態から許可状態に変更し、サプリカントは Cisco TrustSec ドメインのメンバになります。

Cisco TrustSec では、入力タギングと出力フィルタリングを使用して、スケーラブルな方法でアクセス コントロール ポリシーを適用します。ドメインに入るパケットは、送信元デバイスに割り当てられたセキュリティグループ番号を含むセキュリティグループタグ（SGT）でタグ付けされます。このパケット分類は、Cisco TrustSec ドメイン内のデータ パスに沿ってセキュリティ、およびその他のポリシーの基準を適用するために維持されます。データ パスの最後の Cisco TrustSec デバイス（エンドポイントまたはネットワークの出力ポイント）は、Cisco TrustSec 送信元デバイスのセキュリティ グループおよび最終の Cisco TrustSec デバイスのセキュリティ グループに基づいてアクセス コントロール ポリシーを適用します。ネットワーク アドレスに基づいた以前のアクセス コントロール リストとは異なり、Cisco TrustSec アクセス コントロール ポリシーは、セキュリティ グループ アクセス コントロール リスト（SGACL）と呼ばれるロール ベース アクセス コントロール リスト（RBACL）形式です。

（注） 入力とは、宛先へのパス上のパケットが最初の Cisco TrustSec 対応デバイスに入るパケットを指します。出力とは、パス上の最後の Cisco TrustSec 対応デバイスを出るパケットを指します。

セキュリティ グループ ベースのアクセス コントロール

このセクションでは、セキュリティグループベースのアクセスコントロールリスト（SGACL）について説明します。

セキュリティ グループおよび SGT

セキュリティ グループは、アクセス コントロール ポリシーを共有するユーザー、エンドポイント デバイス、およびリソースのグループです。セキュリティ グループは Cisco ISE または Cisco Secure ACS の管理者が定義します。新しいユーザーおよびデバイスが Cisco TrustSec ドメインに追加されると、認証サーバーは、適切なセキュリティ グループにこれらの新しいエンティティを割り当てます。Cisco TrustSec は各セキュリティグループに一意の 16 ビットのセキュリティグループ番号を割り当てます。番号の範囲は Cisco TrustSec ドメイン内でグローバルです。デバイス内のセキュリティグループの数は認証済みのネットワークエンティティの数に制限されます。セキュリティ グループ番号を手動で設定する必要はありません。

デバイスが認証されると、Cisco TrustSec はそのデバイスから発信されるすべてのパケットに、デバイスのセキュリティ グループ番号が含まれているセキュリティ グループ タグ（SGT）をタグ付けします。タグ付けされたパケットはネットワークを通じて Cisco TrustSec ヘッダーで SGT を運びます。SGT は全社内の送信元の許可を特定する単一ラベルです。

SGT には、送信元のセキュリティ グループが含まれているため、タグは送信元 SGT と呼ばれることもあります。宛先デバイスもまたセキュリティグループ（宛先 SG）に割り当てられるため、便宜上、このセキュリティグループを接続先グループタグ（DGT）と呼ぶこともあります。ただし、実際の Cisco TrustSec パケットタグには、宛先デバイスのセキュリティグループ番号は含まれていません。

セキュリティグループ ACL のサポート

セキュリティ グループ アクセス コントロール リスト（SGACL）はポリシーの適用です。これによって管理者は、セキュリティグループの割り当てと宛先リソースに基づいてユーザーが実行する操作を制御できます。Cisco TrustSec ドメイン内のポリシーの適用は、軸の 1 つが送信元セキュリティ グループ番号、もう 1 つの軸が宛先セキュリティグループ番号である、アクセス許可マトリックスで表示されます。マトリックス内の各セルには、SGACL の番号付きリストが含まれます。ここでは、送信元セキュリティグループに属し宛先セキュリティグループに属する宛先 IP を持つ、IP から送信されるパケットに適用される必要があるアクセス権限を指定します。

SGACL は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティグループタグ値に基づいたステートレスのアクセス制御メカニズムを提供し、フィルタリングします。SGACL ポリシーをプロビジョニングするには、次の 3 つの方法があります。

- スタティック ポリシー プロビジョニング：**cts role-based permission** コマンドを使用して、ユーザーが SGACL ポリシーを定義します。
- ダイナミック ポリシー プロビジョニング：SGACL ポリシーの設定は、Cisco Secure ACS または Cisco Identity Services Engine の主にポリシー管理機能によって実行する必要があります。
- 認可変更（CoA）：更新されたポリシーは、SGACL ポリシーが ISE で変更され、CoA が Cisco TrustSec デバイスにプッシュされるとダウンロードされます。

  デバイスデータプレーンは、ポリシープロバイダー（ISE）から CoA パケットを受信し、CoA パケットにポリシーを適用します。その後、パケットはデバイス コントロールプレーンに転送され、着信 CoA パケットに対して次のレベルのポリシーが適用されます。ハードウェアとソフトウェアのポリシーカウンタのヒット情報を表示するには、特権 EXEC モードで **show cts role-based counters** コマンドを実行します。

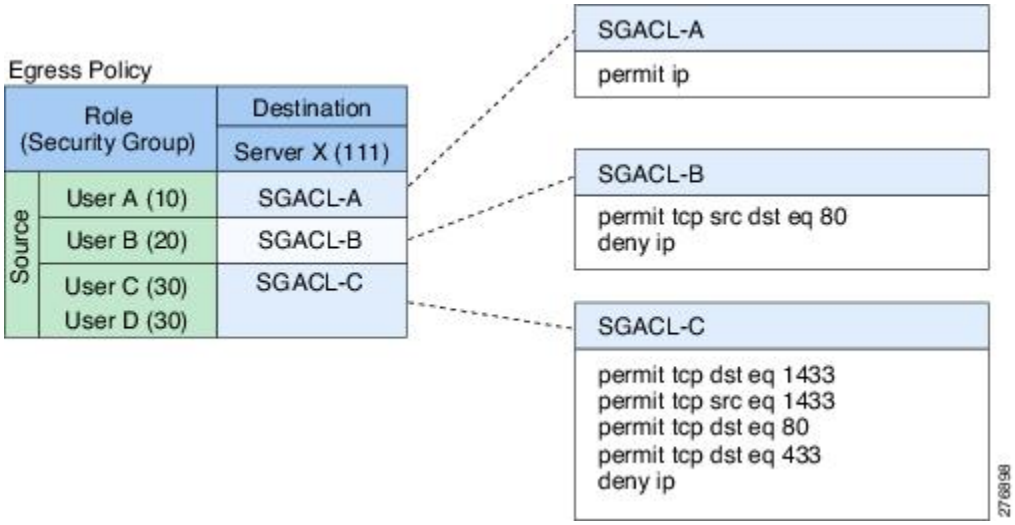
SGACL ポリシー

セキュリティ グループ アクセス コントロール リスト（SGACL）を使用して、ユーザーと宛先リソースのセキュリティ グループの割り当てに基づいて、ユーザーが実行できる操作を制御できます。Cisco TrustSec ドメイン内のポリシーの適用は、軸の 1 つが送信元セキュリティグ

ループ番号、もう1つの軸が宛先セキュリティグループ番号である、許可マトリックスで表示されます。マトリクスの本体の各セルには送信元セキュリティ グループから宛先セキュリティ グループ宛てに送信されるパケットに適用される必要がある許可を指定する SGACL の順序リストを含めることができます。

次の図に、3 つの定義済みのユーザーロールと 1 つの定義済み宛先リソースを含むシンプルなドメインの Cisco TrustSec 許可マトリックスの例を示します。ユーザーの役割に基づいて宛先サーバーへのアクセスを 3 つの SGACL ポリシーで制御します。

図 *2: SGACL* ポリシー マトリクスの例



ネットワーク内のユーザーとデバイスをセキュリティグループに割り当て、セキュリティグループ間でアクセス制御を適用することにより、Cisco TrustSec はネットワーク内でロールベースのトポロジに依存しないアクセス制御を実現します。SGACL は従来の ACL とは異なり、IP アドレスではなくデバイス アイデンティティに基づいてアクセス コントロール ポリシーを定義するため、ネットワーク デバイスはネットワーク全体を移動し、IP アドレスを変更することができます。ロールと許可が同じであれば、ネットワークトポロジが変更されてもセキュリティポリシーには影響しません。ユーザーがデバイスに追加されたら、適切なセキュリティグループにユーザーを割り当てるだけで、ユーザーはただちにそのグループの許可を受信します。

（注） SGACL ポリシーは、デバイスからエンドホストデバイスに生成されるトラフィックではなく、2 つのホストデバイス間で生成されるトラフィックに適用されます。

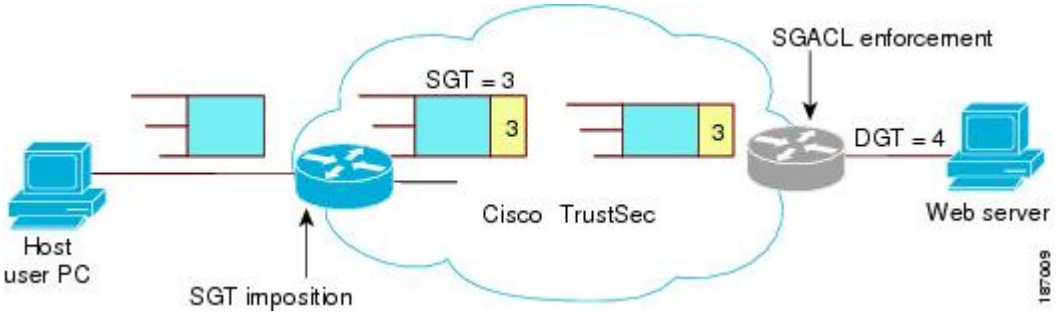
ロール ベースの許可を使用すると ACL のサイズが大幅に節約され、メンテナンス作業も簡単になります。Cisco TrustSec によって、設定されているアクセス コントロール エントリ（ACE）の数は、指定されている許可の数によって決定されるため、ACE の数は従来の IP ネットワークでよりもずっと小さくなります。Cisco TrustSec での SGACL の使用は、従来の ACL と比較して TCAM リソースをより効率的に使用します。では、最大 1,408 の SGACL ポリシーがサポートされます。

入力タギングおよび出力の強制

Cisco TrustSecアクセス コントロールは、入力タギングと出力の適用を使用して実装されます。Cisco TrustSec ドメインの入力点では、送信元からのトラフィックは、送信元エンティティのセキュリティグループ番号を含む SGT でタグ付けされます。SGT は、ドメイン全体にわたってトラフィックと合わせて伝播されます。Cisco TrustSec ドメインの出力ポイントで、出力デバイスは送信元SGTおよび宛先エンティティのセキュリティ グループ番号（宛先SG、またはDGT）を使用して、SGACL ポリシー マトリクスから適用するアクセス ポリシーを決定します。

Cisco TrustSec ドメインでは、次の図のように SGT の割り当てと SGACL の適用が実行されます。

図 *3 : Cisco TrustSec* ドメインの *SGT* と *SGACL*



1. ホスト PC は Web サーバーにパケットを送信します。PC と Web サーバーは Cisco TrustSec ドメインのメンバではありませんが、パケットのデータパスには Cisco TrustSec ドメインが含まれています。
2. Cisco TrustSec の入力デバイスは、ホスト PC の認証サーバーにより割り当てられたセキュリティグループ番号である、セキュリティグループ番号 3 の SGT を追加するようにパケットを変更します。
3. Cisco TrustSec の出力デバイスは、Web サーバーの認証サーバーによって割り当てられたセキュリティグループ番号である、送信元グループ 3 と接続先グループ 4 に適用する SGACL ポリシーを適用します。
4. SGACL がパケットを転送するように許可している場合は、Cisco TrustSec 出力スイッチは SGT を削除するようにパケットを変更し、Web サーバーにパケットを転送します。

送信元セキュリティ グループの判断

Cisco TrustSec ドメインの入口のネットワークデバイスは、Cisco TrustSec ドメインにパケットを転送する際に、パケットに SGT をタグ付けできるように、Cisco TrustSec ドメインに入るパケットの SGT を判断する必要があります。出力のネットワーク デバイスは、SGACL を適用するために、パケットの SGT を判断する必要があります。

ネットワーク デバイスは、次のいずれかの方法でパケットの SGT を判断できます。

- ポリシー取得時に送信元の SGT を取得する：Cisco TrustSec 認証フェーズ後、ネットワーク デバイスは、ピア デバイスが信頼できるかどうかを示すポリシー情報を、認証サーバーから取得します。ピア デバイスが信頼できない場合、認証サーバーはそのピア デバイスから着信するすべてのパケットに適用する SGT も提供します。
- パケットの送信元 SGT を取得する：パケットが信頼できるピア デバイスから送信される場合、パケットは、SGT を伝送します。これは、そのパケットにとって、そのネットワーク デバイスが Cisco TrustSec ドメイン内の最初のネットワーク デバイスではない場合に適用されます。
- 送信元アイデンティティに基づいて送信元 SGT を検索する：アイデンティティ ポート マッピング（IPM）を使用すると、接続されているピア アイデンティティのリンクを手動で設定できます。ネットワーク デバイスは、SGT および信頼状態を含むポリシー情報を認証サーバーに要求します。
- 送信元 IP アドレスに基づいて送信元 SGT を検索する：場合によっては、送信元 IP アドレスに基づいてパケットの SGT を判断するようにパケットを手動で設定できます。SGT Exchange Protocol（SXP）も、IP-address-to-SGT マッピング テーブルに値を格納できます。

宛先セキュリティグループの判断

Cisco TrustSec ドメインの出力のネットワーク デバイスは、SGACL を適用する宛先グループ（DGT）を決定します。ネットワーク デバイスは、パケットの送信元セキュリティ グループを決定するために使用されるのと同じ方法（パケットのタグからのグループ番号の取得を除く）を使用して宛先セキュリティグループを決定します。宛先セキュリティグループ番号はパケットのタグに含まれません。

場合によっては、入口のデバイスまたは出口以外のその他のデバイスが、使用できる宛先グループの情報を持っていることもあります。このような場合、SGACL は出力デバイスではなくこれらのデバイスに適用されます。

ルーテッドおよびスイッチド トラフィックでの SGACL の強制

SGACL の強制は IP トラフィックだけに適用されますが、強制はルーティングまたはスイッチングされるトラフィックに適用できます。

ルーテッドトラフィックの場合、SGACL の適用は、宛先ホストに接続されたルーテッドポートを持つ出力スイッチ（通常はディストリビューション スイッチまたはアクセススイッチ）によって実行されます。SGACL の適用をグローバルに有効にすると、SVI インターフェイスを除くすべてのレイヤ 3 インターフェイスで適用が自動的に有効になります。

スイッチングされるトラフィックの場合は、SGACL の強制はルーティング機能のない単一スイッチング ドメイン内のトラフィック フローで実行されます。2 台の直接接続されたサーバー間のサーバー間トラフィックのデータセンター アクセス スイッチ上で実行された SGACL の強制が、その例です。この例では、通常、サーバー間のトラフィックはスイッチングされます。SGACL の強制は、VLAN 内でスイッチングされるパケットまたは VLAN に関連付けられ

た SVI に転送されるパケットに適用できます。ただし実行は VLAN ごとに明示的にイネーブルにする必要があります。

SGACL ロギングと ACE 統計情報

SGACL でロギングが有効になっている場合、デバイスは次の情報を記録します。

- 送信元セキュリティグループタグ（SGT）および宛先 SGT
- SGACL ポリシー名
- パケットプロトコルタイプ
- パケットで実行されるアクション

ログオプションは個々の ACE に適用され、ACE に一致するパケットがログに記録されます。log キーワードで記録された最初のパケットは、syslog メッセージを生成します。後続のログメッセージは 5 分間隔で生成および報告されます。ロギング対応 ACE が別のパケット（ログメッセージを生成したパケットと同一の特性を持つ）と一致する場合、一致したパケットの数が増加（カウンタ）し、レポートされます。

ロギングを有効にするには、SGACL 構成の ACE 定義の前に **log** キーワードを使用します。たとえば、**permit ip log** のようになります。

次に、送信元と宛先の SGT、ACE の一致（許可または拒否アクション）、およびプロトコル、つまり TCP、UDP、IGMP、および ICMP 情報を表示するサンプルログを示します。

```
*Jun 2 08:58:06.489: %C4K_IOSINTF-6-SGACLHIT: list deny_udp_src_port_log-30 Denied
udp 24.0.0.23(100) -> 28.0.0.91(100), SGT8 DGT 12
```

show cts role-based counters コマンドを使用して表示できる既存の「セルごとの」SGACL 統計情報に加えて、**show ip access-list** *sgacl_name* コマンドを使用して ACE 統計情報も表示できます。これについて追加設定は必要ありません。

次に、show ip access-list コマンドを使用して ACE カウントを表示する例を示します。

```
Device# show ip access-control deny_udp_src_port_log-30

Role-based IP access list deny_udp_src_port_log-30 (downloaded)
10 deny udp src eq 100 log (283 matches)
20 permit ip log (50 matches)
```

（注） 着信トラフィックがセルに一致するが、セルの SGACL に一致しない場合、トラフィックは許可され、セルの HW-許可のカウンタが増加します。

次に、セルの SGACL の動作例を示します。

SGACL ポリシーは「deny icmp echo」で 5 ー 18 に設定され、TCP ヘッダーで 5 ー 18 の着信トラフィックがあります。セルが 5 ー 18 に一致するが、トラフィックが icmp と一致しない場合、トラフィックは許可され、セル 5 ー 18 の HW-許可カウンタが増加します。

```
Device# show cts role-based permissions from 5 to 18

IPv4 Role-based permissions from group 5:sgt_5_Contractors to group
18:sgt_18_data_user2:sgacl_5_18-01
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

Device# show ip access-lists sgacl_5_18-01
Role-based IP access list sgacl_5_18-01 (downloaded)
10 deny icmp echo log (1 match)

Device# show cts role-based counters from 5 to 18
Role-based IPv4 counters
From   To   SW-Denied   HW-Denied   SW-Permitt   HW-Permitt   SW-Monitor   HW-Monitor
  5    18       0           0            0        1673202          0            0
```

VRF 対応 SGACL ロギング

SGACL システムログには VRF 情報が含まれます。現在ログに記録されているフィールドに加えて、ロギング情報には VRF 名が含まれます。更新されたロギング情報は次のようになります。

```
*Nov 15 02:18:52.187: %RBM-6-SGACLHIT_V6: ingress_interface='GigabitEthernet1/0/15'
sgacl_name='IPV6_TCP_DENY' action='Deny' protocol='tcp' src-vrf='CTS-VRF' src-ip='25::2'
 src-port='20'
dest-vrf='CTS-VRF' dest-ip='49::2' dest-port='30' sgt='200' dgt='500'
logging_interval_hits='1'
```

SGACL モニター モード

Cisco TrustSec の事前導入段階で、管理者は、モニターモードを使用して、ポリシーが意図したとおりに機能することを確認するために、セキュリティポリシーを適用しない状態でテストします。セキュリティポリシーが意図したとおり機能しない場合には、モニターモードが、その問題を識別するための便利なメカニズムと、SGACL の適用を有効にする前にポリシーを修正する機会を提供します。これにより、管理者は、ポリシーを適用する前にポリシーアクションの結果をより可視的に確認でき、対象のポリシーがセキュリティ要件を満たしている（ユーザーが認証されなければリソースへのアクセスは拒否される）ことを確認できます。

モニタリング機能は、SGT-DGT ペア レベルで提供されます。SGACL モニター モード機能を有効にすると、拒否アクションがライン カード上の ACL 許可として実装されます。これにより、SGACL カウンタおよびロギングでは、接続が SGACL ポリシーによりどう処理されてい

るかを表示できます。すべてのモニター対象トラフィックが許可されるため、SGACLモニターモードでは、SGACL によるサービスの中断はありません。

許可とポリシーの取得

デバイス認証が終了すると、サプリカントとオーセンティケータの両方が認証サーバーからセキュリティ ポリシーを取得します。2 つのピアは、リンク認可を実行し、Cisco TrustSec デバイス ID に基づいてリンク セキュリティ ポリシーを相互に適用します。リンクの認証方式は、802.1X または手動認証に設定できます。リンクのセキュリティが 802.1X である場合、各ピアは認証サーバーから受信したデバイスIDを使用します。リンクのセキュリティが手動の場合、ピア デバイス ID を割り当てる必要があります。

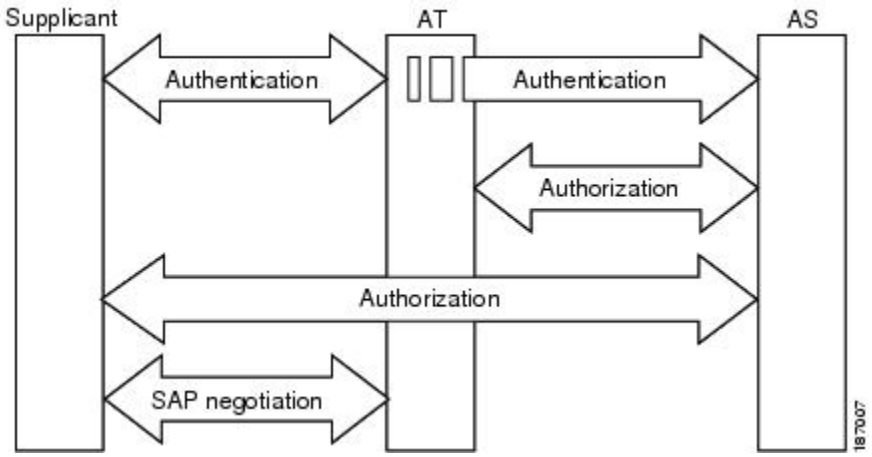
認証サーバーは次の属性を返します。

- Cisco TrustSec の信頼状態：パケットに SGT を付けるにあたり、ピア デバイスが信用できるかどうかを示します。
- ピア SGT：ピアが属しているセキュリティ グループを示します。ピアが信頼できない場合は、ピアから受信したすべてのパケットにこの SGT がタグ付けされます。SGACL がピアの SGT に関連付けられているかどうかデバイスが認識できない場合、デバイスは認証サーバーに追加要求を送信して SGACL をダウンロードする場合もあります。
- 許可期限：ポリシーの期限が切れるまでの秒数を示します。Cisco TrustSec デバイスはポリシーと許可を期限が切れる前にリフレッシュする必要があります。デバイスはデータの有効期限が切れていなければ認証およびポリシーデータをキャッシュし、リブート後に再利用できます。

（注） Cisco TrustSec デバイスは、認証サーバーからピアの適切なポリシーを取得できない場合に備えて、最小限のデフォルト アクセス ポリシーをサポートする必要があります。

次の図に、NDAC および SAP ネゴシエーションプロセスを示します。

図 *4 : NDAC* および *SAP* ネゴシエーション



環境データのダウンロード

Cisco TrustSec 環境データは、Cisco TrustSec ノードとしてのデバイスの機能を支援するひとまとまりの情報またはポリシーです。デバイスは、Cisco TrustSec ドメインに最初に加入する際に、認証サーバーから環境データを取得しますが、一部のデータをデバイスに手動で設定することもできます。たとえば、Cisco TrustSec のシード デバイスには認証サーバーの情報を設定する必要がありますが、この情報は、デバイスが認証サーバーから取得するサーバー リストを使用して、後から追加することができます。

デバイスは、期限前に Cisco TrustSec 環境データをリフレッシュする必要があります。また、このデータの有効期限が切れていなければ、環境データをキャッシュし、リブート後に再利用することもできます。

デバイスは RADIUS を使用して、認証サーバーから次の環境データを取得します。

- サーバーリスト：クライアントがその後の RADIUS 要求に使用できるサーバーのリスト（認証および許可の両方）PAC のリフレッシュは、これらのサーバーを介して行われます。
- デバイス SG：そのデバイス自体が属しているセキュリティグループ
- 有効期間：Cisco TrustSec デバイスが環境データをリフレッシュする頻度を左右する期間

RADIUS リレー機能

802.1X 認証プロセスで Cisco TrustSec オーセンティケータのロールを引き受けるデバイスは、認証サーバーへの IP 接続を通じて、UDP/IP での RADIUS メッセージの交換により、デバイスが認証サーバーからポリシーと許可を取得できるようにします。サプリカントデバイスは認証サーバーとの IP 接続がなくてもかまいません。サプリカントに認証サーバーとの IP 接続がな

い場合、Cisco TrustSec はオーセンティケータをサプリカントの RADIUS リレーとして機能させることができます。

サプリカントは、RADIUS サーバーの IP アドレスと UDP ポートを持つオーセンティケータに特別な EAPOL メッセージを送信し、RADIUS 要求を完了します。オーセンティケータは、受信した EAPOL メッセージから RADIUS 要求を抽出し、これを UDP/IP を通じて認証サーバーに送信します。認証サーバーから RADIUS 応答が返ると、オーセンティケータはメッセージを EAPOL フレームにカプセル化して、サプリカントに転送します。

リンク セキュリティ

リンクの両側で 802.1AE Media Access Control Security（MACsec）をサポートしている場合、セキュリティ アソシエーション プロトコル（SAP）ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティ パラメータの交換、およびキーの管理が実行されます。これら 3 つの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョン、暗号ライセンス、およびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois/Counter Mode（GCM）：認証および暗号化ありを指定します
- GCM 認証（GMAC）：認証あり、暗号化なしを指定します
- カプセル化なし：カプセル化なし（クリア テキスト）を指定します
- ヌル：カプセル化あり、認証なし、暗号化なしを指定します

カプセル化なしを除くすべてのモードで、Cisco TrustSec 対応のハードウェアが必要です。

リンクセキュリティ用の SAP-PMK 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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet 1/1/4`	インターフェイスを設定し、インターフェイス 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	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	トランキング VLAN レイヤ 2 インターフェイスを指定します。
ステップ 5	**cts manual** 例： `Device(config-if)# cts manual`	Cisco TrustSec 手動コンフィギュレーション モードを開始します。
ステップ 6	**no propagate sgt** 例： `Device(config-if-cts-manual)# no propagate sgt`	ピアが SGT を処理できない場合、このコマンドの **no** 形式を使用します。 **no propagate sgt** コマンドを使用すると、インターフェイスからピアに SGT が送信されなくなります。
ステップ 7	**sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]] 例： `Device(config-if-cts-manual)# sap pmk 00000000000000000000000000000000000000000000000000000000000000001234567890 mode-list gcm-encrypt gmac`	SAP の Pairwise Master Key（PMK）と動作モードを設定します。Cisco TrustSec の手動モードでは、SAP はデフォルトでディセーブルになっています。 • *key*：文字数が偶数個で最大 32 文字の 16 進値。 SAP 動作の mode オプションの詳細は次のとおりです。 • **gcm-encrypt**：認証および暗号化 （注） ソフトウェア ライセンスが MACsec 暗号化をサポートする場合、MACsec の認証と暗号化にこのモードを選択します。 • **gmac**：認証、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化、認証または暗号化なし

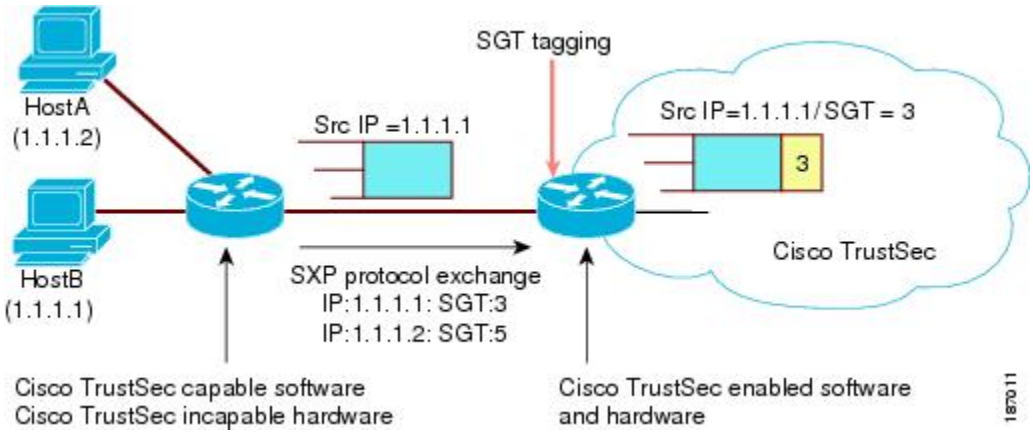
	コマンドまたはアクション	目的
		（注） インターフェイスでデータリンク暗号化を使用できない場合は、デフォルトおよび唯一使用可能な SAP 動作モードは **no-encap** コマンドです。SGT はサポートされません。
ステップ 8	**end** 例： `Device(config-if-cts-manual)# end`	Cisco TrustSec 手動コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SXP によるレガシー アクセス ネットワークへの SGT の伝播

パケットへの SGT のタグ付けには、ハードウェアによるサポートが必要です。Cisco TrustSec 認証に参加する機能があっても、パケットに SGT をタグ付けするハードウェア機能がないデバイスがネットワークにある場合があります。SGT 交換プロトコル（SXP）を使用して、これらのデバイスは、Cisco TrustSec 対応のハードウェアを搭載している Cisco TrustSec ピア デバイスに IP アドレスと SGT のマッピングを渡すことができます。

通常、SXP は Cisco TrustSec ドメイン エッジの入力アクセス レイヤ デバイスと Cisco TrustSec ドメイン内のディストリビューション レイヤ デバイス間で動作します。アクセス レイヤ デバイスは入力パケットの適切な SGT を判断するために、外部送信元デバイスの Cisco TrustSec 認証を実行します。アクセスレイヤデバイスはIPデバイストラッキングおよび（任意で）DHCP スヌーピングを使用して送信元デバイスの IP アドレスを学習し、その後 SXP を使用して送信元デバイスの IP アドレスおよび SGT を、ディストリビューション デバイスに渡します。Cisco TrustSec 対応のハードウェアを備えたディストリビューション デバイスはこの IP と SGT のマッピング情報を使用してパケットに適切にタグを付け、SGACL ポリシーを適用します。

図 *5 : SXP* プロトコルによる *SGT* 情報の伝播



Cisco TrustSec ハードウェア サポート対象外のピアと Cisco TrustSec ハードウェア サポート対象のピア間の SXP 接続は、手動で設定する必要があります。SXP 接続を設定する場合は、次の作業を実行する必要があります。

- SXP データの整合性と認証が必要になる場合は、ピア デバイスの両方に同じ SXP パスワードを設定する必要があります。SXP パスワードは各ピア接続に対して明示的に指定することも、デバイスに対してグローバルに設定することもできます。SXP パスワードは必須ではありませんが、使用することを推奨します。
- 各ピアを SXP 接続に SXP スピーカーまたは SXP リスナーとして設定する必要があります。スピーカー デバイスはリスナー デバイスに IP-to-SGT 情報を渡します。
- 送信元 IP アドレスを指定して各ピアの関係付けに使用したり、特定の送信元 IP アドレスを設定していないピア接続に対してデフォルトの送信元 IP アドレスを設定したりすることができます。送信元 IP アドレスを指定しない場合、デバイスはピアへの接続のインターフェイスの IP アドレスを使用します。

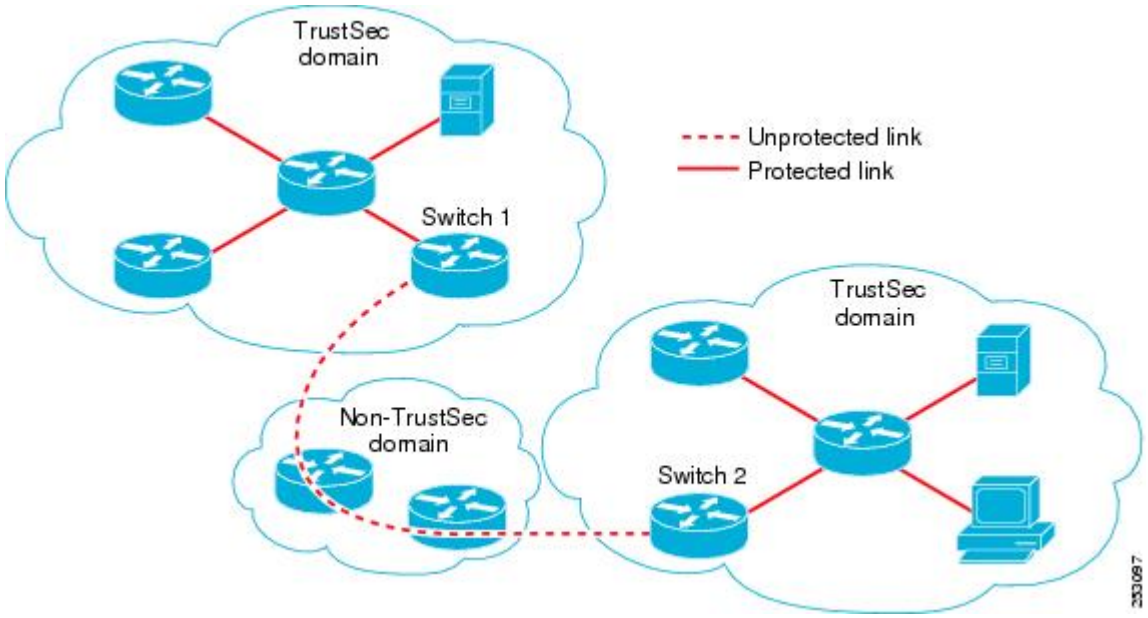
SXP は複数のホップを許可します。つまり、Cisco TrustSec ハードウェア サポート対象外デバイスのピアが Cisco TrustSec ハードウェア サポートの対象外でもある場合、2 番目のピアはハードウェア対応ピアに到達するまで IP と SGT のマッピング情報の伝播を継続して、3 番目のピアへの SXP 接続を設定できます。デバイスは 1 つの SXP 接続では SXP リスナーとして、別の SXP 接続では SXP スピーカーとして設定できます。

Cisco TrustSec デバイスは TCP キープアライブ メカニズムを使用して、SXP ピアとの接続を維持します。ピア接続を確立または回復するために、デバイスは設定可能な再試行期間を使用して接続が成功するか、接続が設定から削除されるまで接続の確立を繰り返し試行します。

非 TrustSec 領域のスパニングのためのレイヤ 3 SGT トランスポート

パケットが非 TrustSec を宛先として Cisco TrustSec ドメインを離れると、出力 Cisco TrustSec デバイスは外部ネットワークにパケットを転送する前に Cisco TrustSec ヘッダーおよび SGT を削除します。ただし、次の図に示すように、パケットが別の Cisco TrustSec ドメインへのパス上にある非 TrustSec ドメインを通過するだけの場合、Cisco TrustSec レイヤ 3 SGT トランスポート機能を使用して SGT を維持できます。この機能では、出力 Cisco TrustSec デバイスは、SGT のコピーを含む ESP ヘッダーを使用してパケットをカプセル化します。カプセル化されたパケットが次の Cisco TrustSec ドメインに到達すると、入力 Cisco TrustSec デバイスは ESP カプセル化を解除して、SGT のパケットを伝播します。

図 *6 :* 非 *TrustSec* ドメインのスパニング



Cisco TrustSec レイヤ 3 SGT トランスポートをサポートするために、Cisco TrustSec 入力または出力レイヤ 3 ゲートウェイとして機能するすべてのデバイスは、リモート Cisco TrustSec ドメインの適格なサブネットと、それらの領域内の除外されたサブネットを一覧表示するトラフィック ポリシー データベースを維持する必要があります。Cisco Secure ACS から自動的にダウンロードできない場合、デバイスごとにこのデータベースを手動で設定できます。

デバイスは 1 つのポートからレイヤ 3 SGT トランスポートデータを送信し、別のポートでレイヤ 3 SGT トランスポートデータを受信できますが、入力および出力ポートの両方が Cisco TrustSec 対応のハードウェアであることが必要です。

（注） Cisco TrustSec はレイヤ 3 SGT トランスポートのカプセル化パケットを暗号化しません。非 TrustSec ドメインを通過するパケットを保護するために、IPsec などの他の保護方式を設定できます。

VRF-Aware SXP

仮想ルーティングおよびフォワーディング（VRF）の SXP の実装は、特定の VRF と SXP 接続をバインドします。Cisco TrustSec を有効にする前に、ネットワーク トポロジがレイヤ 2 またはレイヤ 3 の VPN に対して正しく設定されており、すべての VRF が設定されていることを前提としています。

SXP VRF サポートは、次のようにまとめることができます。

- 1 つの VRF には 1 つの SXP 接続のみをバインドできます。
- 別の VRF が重複する SXP ピアまたは送信元 IP アドレス持つ可能性があります。
- 1 つの VRF で学習（追加または削除）された IP-SGT マッピングは、同じ VRF ドメインでのみ更新できます。SXP 接続は異なる VRF にバインドされたマッピングを更新できません。SXP 接続が VRF で終了しない場合は、その VRF の IP-SGT マッピングは SXP によって更新されません。
- VRF ごとに複数のアドレス ファミリがサポートされています。そのため、VRF ドメインの 1 つの SXP 接続が IPV4 および IPV6 両方の IP-SGT マッピングを転送できます。
- SXP には VRF あたりの接続数および IP-SGT マッピング数の制限はありません。

レイヤ 2 VRF-Aware SXP および VRF の割り当て

VRF からレイヤ 2 VLAN への割り当ては、**cts role-based l2-vrf vrf-name vlan-list** グローバル コンフィギュレーション コマンドで指定されます。VLAN は VLAN 上に IP アドレスが設定されたスイッチ仮想インターフェイス（SVI）がない限り、レイヤ 2 VLAN と見なされます。VLAN の SVI に IP アドレスが設定されると、VLAN はレイヤ 3 VLAN になります。

cts role-based l2-vrf コマンドで設定された VRF 割り当ては、VLAN がレイヤ 2 VLAN として維持されている間はアクティブです。VRF の割り当てがアクティブな間に、学習した IP-SGT バインディングも VRF と IP プロトコルバージョンに関連付けられた転送情報ベース（FIB）テーブルに追加されます。VLAN の SVI がアクティブになると、VRF から VLAN への割り当てが非アクティブになり、VLAN で学習されたすべてのバインドが SVI の VRF に関連付けられた FIB テーブルに移動されます。

VRF から VLAN への割り当ては、割り当てが非アクティブになっても保持されます。SVI が削除された、または SVI の IP アドレスの設定が解除された場合に再アクティブ化されます。再アクティブ化された場合、IP-SGT バインドは、SVI の FIB に関連付けられた FIB テーブル

から、**cts role-based l2-vrf** コマンドによって割り当てられた VRF に関連付けられた FIB テーブルに戻されます。

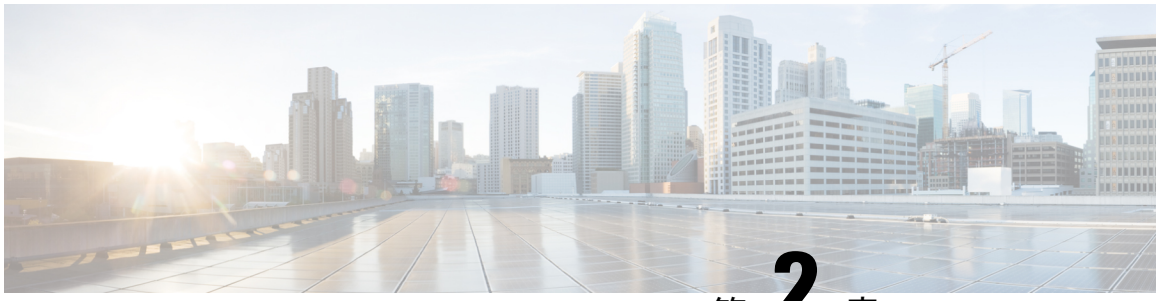
Cisco TrustSec の機能履歴の概要

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 Fuji 16.9.2	Cisco TrustSec Overview	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。

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。



第 2 章

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。
- 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。
- サーバーごとに 1 つの完全修飾ドメイン名（FQDN）のみがサポートされます。
- 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 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。Cisco IOS XE Amsterdam 17.2.1 以降のリリースでは、サーバーごとに 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。特定のサーバーの429応答コードを受信すると、デバイスはサーバーをデッドとしてマークし、リスト内の次のサーバー（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。

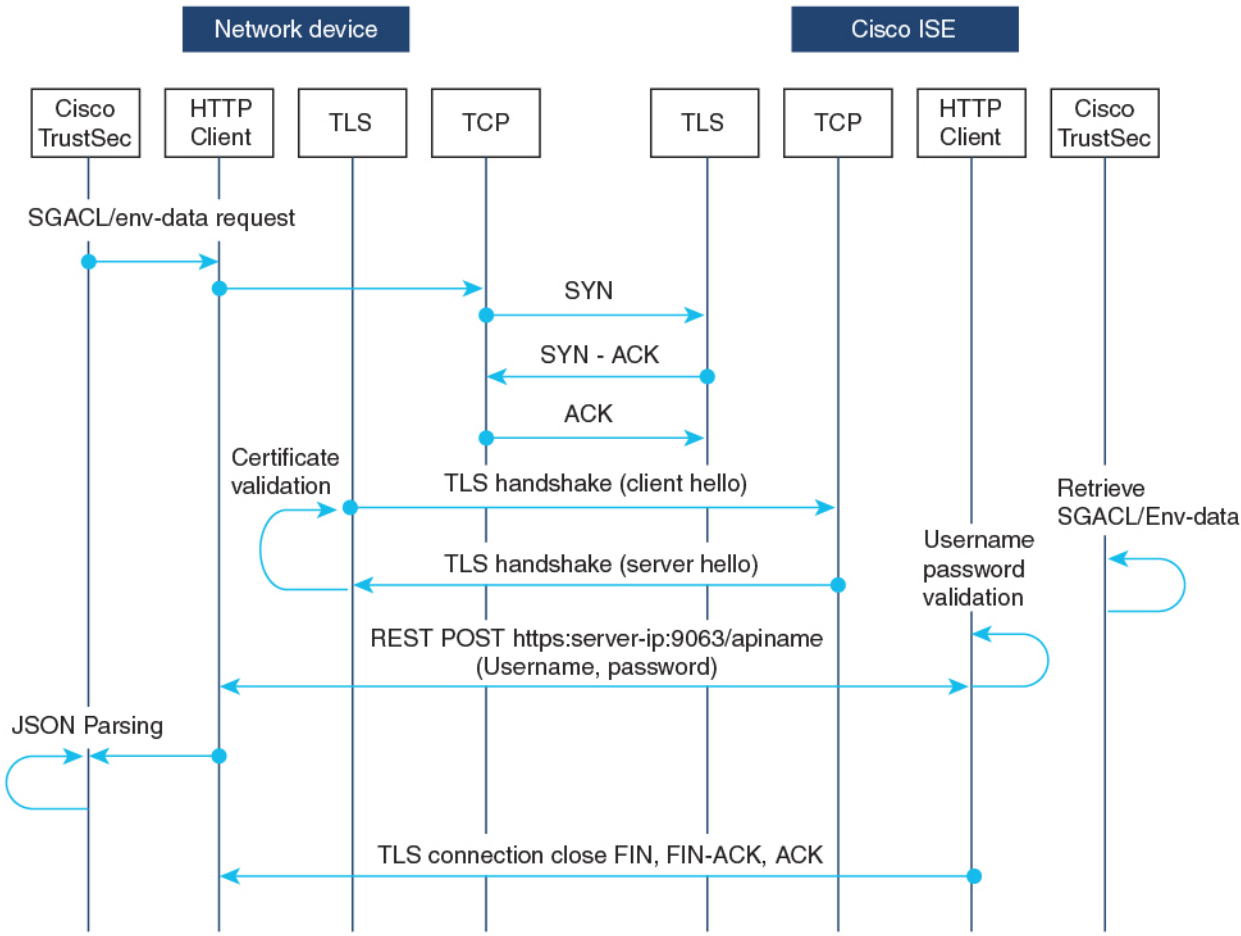
- デバイスのセキュリティグループタグ（SGT）：デバイス名に基づいて Cisco ISE から取得されます。
- サーバーリスト：Cisco ISE で指定された Cisco TrustSec サーバーのリストを表示します。
- SG-Name テーブル：SGT とデバイス名の間のマッピングを表示します。SGT は数字で表示され、デバイス名はテキスト形式で表示されます。
- リフレッシュ時間：環境データがリフレッシュされる時間を示します。

（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 7: 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 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。

サーバーと IP アドレスの選択プロセス

サーバー選択の順序は、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）の順です。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。

Cisco IOS XE 17.2.1 以降のリリースでは、サーバーごとに複数の 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、サーバーと 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）リストからサーバーが選択されます。
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ーを使用して Cisco ISE からプライベートサーバー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. サーバーと IP アドレスを選択すると、デバイスはサーバーと IP アドレスの組み合わせを使用して Cisco ISE に接続します。このサーバーは、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ー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ーに切り替えます。サーバー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. サーバーと 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ー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ーへの接続を試みます。サーバー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. サーバーの変更は、サーバー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ーリストとパブリックサーバーリストの両方のすべてのサーバーが停止している場合、デバイスはサーバーと 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. 特定のサーバーと 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、同じサーバーと次の 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ーを選択します。

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。
- 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*} 例： `Device(config)# cts policy-server username admin password 6 password1`	ユーザー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。 （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**| **ipv6** *policy-server-address*
	例：
	`Device(config-policy-server)# address ipv4 10.1.1.1`
	`Device(config-policy-server)# address ipv6 2001.DB8::1`
		ポリシーサーバーの 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：	（任意）ポリシーサーバー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。

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

	コマンドまたはアクション	目的
		（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
  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      : 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)# 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
```

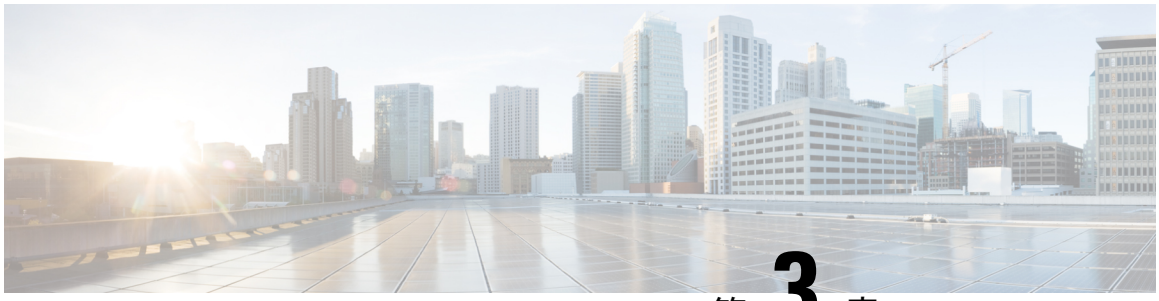
REST での SGACL と環境データのダウンロードの機能履歴

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。



第 3 章

セキュリティグループACLポリシーの設定

セキュリティ グループ アクセス コントロール リスト（SGACL）を使用して、ユーザーと宛先リソースのセキュリティ グループの割り当てに基づいて、ユーザーが実行できる操作を制御できます。Cisco TrustSec ドメイン内のポリシーの適用は、軸の 1 つが送信元セキュリティ グループ番号、もう 1 つの軸が宛先セキュリティグループ番号である、許可マトリックスで表示されます。マトリクスの本体の各セルには送信元セキュリティ グループから宛先セキュリティ グループ宛てに送信されるパケットに適用される必要がある許可を指定する SGACL の順序リストを含めることができます。

SGACL ポリシーの設定の制約事項

- ハードウェアの制限により、Cisco TrustSec SGACL はハードウェアのパント（CPUバウンド）トラフィックに適用できません。ソフトウェアでの SGACL の適用は、SVI、レイヤ 2 とレイヤ 3 の Location Identifier Separation Protocol（LISP）、およびループバック インターフェイスの CPU バウンドトラフィックではバイパスされます。
- SGACL ポリシーを設定する際に、IP バージョンを **IPv4** または **IPv6** から **非依存**（IPv4 と IPv6 の両方に適用）に変更した場合（逆も同様）、IPv4 と IPv6 に対応する SGACL ポリシーは管理 VRF インターフェイスを介して完全にダウンロードされません。
- SGACL ポリシーを設定する際に、既存の IP バージョンを他のバージョン（**IPv4** または **IPv6** または **非依存**）に変更した場合（逆も同様）、RADIUS を使用して Cisco Identity Services Engine（ISE）からの認可変更（CoA）を実行しないでください。代わりに、SSH を使用して **cts refresh policy** コマンドを実行し、手動でポリシーをリフレッシュします。
- デフォルトのアクションを **deny all** とした SGT 許可リストモデルを使用する場合、デバイスのリロード後に Cisco TrustSec ポリシーが ISE サーバーから部分的にダウンロードされることがあります。

これを回避するには、デバイスで静的ポリシーを定義します。**deny all** オプションが適用されている場合でも、静的ポリシーはトラフィックを許可します。これにより、デバイスはISEサーバーからポリシーをダウンロードし、定義された静的ポリシーを上書きできます。デバイス SGT では、グローバル コンフィギュレーション モードで次のコマンドを設定します。

- **cts role-based permissions from** <*sgt_num*> **to unknown**
- **cts role-based permissions from unknown to** <*sgt_num*>

SGACL ポリシーに関する情報

このセクションでは、SGACL ポリシーの設定について説明します。

SGACL ロギング

標準 IP アクセスリストによって許可または拒否されたパケットに関するログメッセージが、デバイスによって表示されます。つまり、SGACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、syslog メッセージを管理する **logging console** コマンドで管理されます。Cisco IOS XE Amsterdam 17.3.1 以前のリリースでは、SGACL ロギングは、CPU 集約型のメカニズムで行われていました。Cisco IOS XE Amsterdam 17.3.1 以降のリリースでは、SGACL ロギングは、はるかに高いロギングレートを可能にするNetFlowハードウェアを使用するように拡張されました。

（注） ハードウェアでのSGACLロギングは、ロールベースアクセスコントロールリスト（RBACL）でのみサポートされています。

SGACL をトリガーする最初のパケットはフローを作成し、非アクティブフローとアクティブフローのNetFlowタイムアウトはそれぞれ30秒および1分でロギングされます。後続のパケットは、5分間隔で収集された後、ロギングされます。ログメッセージにはアクセスリスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレスまたは宛先 IP アドレス、パケットが入力されたインターフェイス、および直前の5分間に許可または拒否された送信元からのパケット数が示されます。

（注）
- ハードウェアでの SGACL ロギングは NetFlow を使用して行われるため、NetFlow ベースの機能がインターフェイスに適用されると、そのインターフェイスのロギングは古いメカニズムにフォールバックします。NetFlow ベースの機能が削除されると、そのインターフェイスの NetFlow ハードウェアを介したロギングが再開されます。残りのインターフェイスは、NetFlow ハードウェアを介してロギングを継続します。
- 一度にデバイスに接続できる NetFlow モニターは 15 台だけです。SGACL ロギングには、IPv4 および IPv6 ロギング用にそれぞれ 1 つの NetFlow モニターが必要です。ロギング用の NetFlow モニターが使用できない場合、SGACL ロギングは古いメカニズムによって行われます。必要な数の NetFlow モニターが使用可能になったら、**cts role-based permissions** コマンドを実行して、NetFlow ハードウェアを介してロギングを再度トリガーします。
- ログ ACE に送信元ポート番号、宛先ポート番号、使用中のプロトコル以外のフィールドがある場合、ロギングは古いメカニズムによって行われます。

SGACL ポリシーの設定方法

このセクションでは、さまざまな SGACL ポリシー設定について説明します。

SGACL ポリシーの設定プロセス

Cisco TrustSec のセキュリティグループ ACL（SGACL）ポリシーを設定してイネーブルにするには、次の手順を実行します。

1. SGACL ポリシーの設定は、Cisco Secure Access Control Server（ACS）または Cisco Identity Services Engine（ISE）の主にポリシー管理機能によって実行する必要があります。

   SGACL ポリシーの設定のダウンロードに Cisco Secure ACS または Cisco ISE 上の AAA を使用しない場合は、SGACL のマッピングとポリシーを手動で設定できます。

（注） Cisco Secure ACS または Cisco ISE からダイナミックにダウンロードされた SGACL ポリシーは、競合のローカル定義されたポリシーよりも優先されます。

2. ルーテッドポートの出力トラフィックに対する SGACL ポリシーの適用を有効にするには、「SGACL ポリシーの適用のグローバルな有効化」セクションに記載されているように、SGACL ポリシー適用を有効にします。
3. VLAN 内のスイッチングされたトラフィック、または VLAN に関連付けられた SVI に転送されるトラフィックに対して SGACL ポリシーの適用を有効にするには、「VLAN に対する SGACL ポリシーの適用の有効化」セクションの説明に従って、特定の VLAN に対して SGACL ポリシーの適用を有効にします。

SGACL ポリシーの適用のグローバルな有効化

Cisco TrustSec をイネーブルにしたルーテッド インターフェイスで SGACL ポリシーの強制をグローバルにイネーブルにする必要があります。

ルーテッドインターフェイスの SGACL ポリシーの強制をイネーブルにするには、次の作業を行います。

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 role-based enforcement** 例： `Device(config)# cts role-based enforcement`	ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。
ステップ 4	**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。

インターフェイスあたりの SGACL ポリシーの適用の有効化

まず、Cisco TrustSec を有効にしたルーテッドインターフェイスで SGACL ポリシーの適用をグローバルに有効にする必要があります。この機能はポート チャネル インターフェイスではサポートされません。

レイヤ 3 インターフェイスでの SGACL ポリシーの適用を有効化するには、次の作業を行います。

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）。

	コマンドまたはアクション	目的
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	**interface** *type slot/port* 例： `Device(config)# interface gigabitethernet 6/2`	インターフェイスを設定し、インターフェイス 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	**cts role-based enforcement** 例： `Device(config-if)# cts role-based enforcement`	ルーテッド インターフェイスで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス 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。
ステップ 6	**show cts interface** 例： `Device# show cts interface`	（任意）インターフェイスごとの Cisco TrustSec ステートおよび統計情報を表示します。

VLAN に対する SGACL ポリシーの強制のイネーブル化

VLAN 内のスイッチングされたトラフィック、または VLAN に関連付けられた SVI に転送されるトラフィックに対してアクセス コントロールを適用するには、特定の VLAN に対して SGACL ポリシーの強制をイネーブルにする必要があります。

VLAN または VLAN リスト内で、SGACL ポリシーの強制をイネーブルにするには、次の作業を行います。

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。

	コマンドまたはアクション	目的
ステップ 3	**cts role-based enforcement vlan-list** *vlan-list* 例： `Device(config)# cts role-based enforcement vlan-list 31-35,41`	VLAN または VLAN リストで Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。
ステップ 4	**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。

SGACL モニター モードの設定

SGACL モニターモードを設定する前に、次の点を確認してください。

- Cisco TrustSec が有効になっている。
- カウンタが有効になっている。

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 role-based monitor all** 例： `Device(config)# cts role-based monitor all`	グローバルモニターモードを有効にします。
ステップ 4	**cts role-based monitor permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**] 例： `Device(config)# cts role-based permissions from 2 to 3 ipv4`	IPv4/IPv6 ロール ベース アクセス コントロール リスト（RBACL）（セキュリティグループタグ（SGT）：接続先グループタグ（DGT）ペア）のモニターモードを有効にします。
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。

	コマンドまたはアクション	目的
ステップ 6	**show cts role-based permissions from** {*sgt_num*} **to** {*dgt_num*} [**ipv4** | **ipv6**] [**details**] 例： `Device# show cts role-based permissions from 2 to 3 ipv4 details`	（任意）SGACL ポリシーとペアごとのモニターモード機能に関する詳細を表示します。<SGT-DGT> ペアでセルごとのモニターモードが有効になっている場合、コマンド出力にはモニター対象が表示されます。
ステップ 7	**show cts role-based counters** [**ipv4** | **ipv6**] 例： `Device# show cts role-based counters ipv4`	（任意）IPv4 および IPv6 イベントのすべての SGACL 適用の統計情報を表示します。

SGACL ポリシーの手動設定

SGT と DGT の範囲にバインドされたロールベース アクセス コントロール リストは、出力トラフィックに適用される Cisco TrustSec ポリシーである SGACL を形成します。SGACL ポリシーの設定は、Cisco ISE または Cisco Secure ACS のポリシー管理機能を使用して行うのが最適です。SGACL ポリシーを手動で（つまりローカルに）設定するには、ロールベース ACL を設定し、ロールベース ACL を SGT の範囲にバインドします。

（注） Cisco ISE または Cisco ACS からダイナミックにダウンロードされた SGACL ポリシーは、競合の手動設定されたポリシーよりも優先されます。

IPv4 SGACL ポリシーの設定と適用

（注） SGACL およびロールベース アクセス コントロール リスト（RBACL）を設定する場合、名前付きアクセスコントロールリスト（ACL）はアルファベットで始まる必要があります。

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。

	コマンドまたはアクション	目的
ステップ 3	**ip access-list role-based** *rbacl-name* 例： `Device(config)# ip access-list role-based allow_webtraff`	ロールベースの ACL を作成して、ロールベース ACL 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	{[*sequence-number*] | **default** | **permit** | **deny** | **remark**} 例： `Device(config-rb-acl)# 10 permit tcp dst eq 80 dst eq 20`	RBACL のアクセス コントロール エントリ（ACE）を指定します。 拡張名前付きアクセス リスト コンフィギュレーション モードで使用可能なコマンドおよびオプションの大部分を、送信元および宛先フィールドを省略して使用できます。 Enter キーを押して ACE を完了し、次の手順を開始します。 次の ACE コマンドまたはキーワードはサポートされていません。 • **reflect** • **evaluate** • **time-range**
ステップ 5	**exit** 例： `Device(config-rb-acl)# exit`	ロールベース ACL 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 6	**cts role-based permissions {default** | **[from** {*sgt_num* | **unknown**} **to** {*dgt_num* | **unknown** }] {*rbacls* | **ipv4** *rbacls*} 例： `Device(config)# cts role-based permissions from 55 to 66 allow_webtraff`	SGT と DGT を RBACL にバインドします。この設定は、Cisco ISE または Cisco Secure ACS で設定された許可マトリックスにデータを入力することに似ています。 • デフォルト：デフォルトの権限リスト • *sgt_num*：0 ～ 65,519。送信元グループタグ。 • *dgt_num*：0 ～ 65,519。接続先グループタグ。 • unknown：SGACL がセキュリティグループ（送信元または宛先）を特

	コマンドまたはアクション	目的
		定できないパケットに適用されます。 • ipv4：次の RBACL が IPv4 であることを示します。 • *rbacls*：RBACL の名前
ステップ 7	**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。
ステップ 8	**show cts role-based permissions** 例： `Device# show cts role-based permissions`	（任意）RBACL 設定に対する権限を表示します。
ステップ 9	**show ip access-lists** {*rbacls* | **ipv4** *rbacls*} 例： `Device# show ip access-lists allow_webtraff`	（任意）すべての RBACL または指定された RBACL の ACE を表示します。

IPv6 SGACL ポリシーの設定

IPv6 SGACL ポリシーを手動で設定するには、次の作業を行います。

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	**ipv6 access-list role-based** *sgacl-name* 例： `Device(config)# ipv6 access-list role-based sgaclname`	名前付き IPv6 SGACL を作成して、IPv6 ロールベース ACL 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	{**permit** | **deny** } *protocol* [**dest-option** | **dest-option-type** {*doh-number* | *doh-type*}] [**dscp** *cp-value*] [**flow-label** *fl-value*]	RBACL のアクセス コントロール エントリ（ACE）を指定します。

	コマンドまたはアクション	目的
	[**mobility** | **mobility-type** {*mh-number* | *mh-type*}] [**routing** | **routing-type** *routing-number*] [**fragments**] [**log** | **log-input**] [**sequence** *seqno*] 例： `Device(config-ipv6rb-acl)# permit 33 dest-option dscp af11`	拡張名前付きアクセス リスト コンフィギュレーション モードで使用可能なコマンドおよびオプションの大部分を、送信元および宛先フィールドを省略して使用できます。 次の ACE コマンドまたはキーワードはサポートされていません。 • **reflect** • **evaluate** • **time-range**
ステップ 5	**end** 例： `Device(config-ipv6rb-acl)# end`	IPv6 ロールベース ACL 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。

手動で SGACL ポリシーを適用する方法

手動で SGACL ポリシーを適用するには、次の作業を行います。

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 role-based permissions default** [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3 ...*]]] 例： `Device(config)# cts role-based permissions default MYDEFAULTSGACL`	デフォルト SGACL を指定します。デフォルト ポリシーは明示的なポリシーが送信元と宛先セキュリティグループの間にない場合に適用されます。
ステップ 4	**cts role-based permissions from** {*source-sgt* | **unknown**} **to** {*dest-sgt* | **unknown**} [**ipv4** | **ipv6**] *sgacl-name1* [*sgacl-name2* [*sgacl-name3 ...*]]]	送信元セキュリティ グループ（SGT）と宛先セキュリティグループ（DGT）に適用する SGACL を指定します。source-sgt と dest-sgt の値範囲は 1 ～

	コマンドまたはアクション	目的
	例： `Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5`	65533 です。デフォルトでは、SGACL は IPv4 であると見なされます。 • **from**：送信元 SGT を指定します。 • **to**：宛先セキュリティグループを指定します。 • **unknown**：SGACL がセキュリティグループ（送信元または宛先）を特定できないパケットに適用されます。 （注） ACS から動的にダウンロードされた SGACL ポリシーは、競合の手動ポリシーよりも優先されます。
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。

SGACL ポリシーの表示

Cisco TrustSec デバイス クレデンシャルと AAA の設定後、認証サーバーからダウンロードされたか、または手動で設定された Cisco TrustSec SGACL ポリシーを検証できます。Cisco TrustSec は、インターフェイスに対する認証および許可、SXP、または IP アドレスおよび SGT の手動マッピングによって新しい SGT を学習すると、SGACL ポリシーをダウンロードします。

キーワードを使用して、許可マトリクスの全部または一部を表示できます。

- **from** キーワードを省略すると、許可マトリックスのカラムが表示されます。
- **to** キーワードを省略すると、許可マトリックスの行が表示されます。
- **from** および **to** キーワードを省略すると、許可マトリックス全体が表示されます。
- **from** および **to** キーワードが指定されている場合、許可マトリックスから 1 つのセルが表示され、**details** キーワードを使用できます。**details** が入力された場合、1 つのセルの SGACL の ACE が表示されます。

SGACL ポリシーの許可マトリクスの内容を表示するには、次の作業を行います。

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	**show cts role-based permissions default** [**ipv4** | **ipv6** | **details**] 例： `Device# show cts role-based permissions default MYDEFAULTSGACL`	デフォルトポリシーの SGACL のリストを表示します。
ステップ 3	**show cts role-based permissions from** {*source-sgt* | **unknown**} **to** {*dest-sgt* | **unknown**}] [**ipv4** | **ipv6** | **details**] 例： `Device# show cts role-based permissions from 3`	送信元セキュリティ グループ（SGT）と宛先セキュリティグループ（DGT）に適用する SGACL を指定します。source-sgt と dest-sgt の値範囲は 1 ～ 65533 です。デフォルトでは、SGACL は IPv4 であると見なされます。 • **from**：送信元 SGT を指定します。 • **to**：宛先セキュリティグループを指定します。 • **unknown**：SGACL がセキュリティグループ（送信元または宛先）を特定できないパケットに適用されます。 （注） ACS から動的にダウンロードされた SGACL ポリシーは、競合の手動ポリシーよりも優先されます。
ステップ 4	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。

ダウンロードされた SGACL ポリシーのリフレッシュ

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	**cts refresh policy** {**peer** [*peer-id*] | **sgt** [*sgt_number* | **default** | **unknown**]} 例： `Device# cts refresh policy peer my_cisco_ise`	認証サーバーからの SGACL ポリシーの即時リフレッシュを実行します。 • *peer-id* が指定される場合、指定されたピア接続に関連するポリシーだけがリフレッシュされます。すべてのピア ポリシーを更新するには、ID を指定しないで Enter を押します。 • SGT 番号が指定されている場合、その SGT に関連するポリシーだけがリフレッシュされます。すべてのセキュリティ グループ タグ ポリシーをリフレッシュするには、SGT 番号を指定せずに Enter を押します。デフォルトポリシーをリフレッシュするには、default を選択します。不明なポリシーをリフレッシュするには、unknown を選択します。
ステップ 3	**exit** 例： `Device# exit`	特権 EXEC モードを終了します。

SGACL ポリシーの設定例

次のセクションでは、さまざまな SGACK ポリシーの設定例を示します。

例：SGACL ポリシーの適用のグローバルな有効化

次に、 SGACL ポリシーの適用をグローバルに有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement
```

例：インターフェイスあたりの SGACL ポリシーの適用の有効化

次に、インターフェイスごとに SGACL ポリシーの適用を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

例：VLAN に対する SGACL ポリシーの適用の有効化

次に、VLAN 上で SGACL ポリシーの適用を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement vlan-list 31-35,41
Device(config)# exit
```

例：SGACL モニターモードの設定

次に、SGACL モニターモードを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
Details:
Role-based IP access list denytcpudpicmp-10 (downloaded)
        10 deny tcp
        20 deny udp
        30 deny icmp
Role-based IP access list Permit IP-00 (downloaded)
        10 permit ip

Device# show cts role-based counters ipv4

Role-based IPv4 counters
From     To     SW-Denied  HW-Denied  SW-Permitt  HW_Permitt  SW-Monitor  HW-Monitor
```

```
*          *     0          0          8          18962      0          0
2          3     0          0          0          0          0          341057
```

例：SGACL ポリシーの手動設定

次に、SGACL ポリシーを手動で設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access role allow_webtraff
Device(config-rb-acl)# 10 permit tcp dst eq 80
Device(config-rb-acl)# 20 permit tcp dst eq 443
Device(config-rb-acl)# 30 permit icmp
Device(config-rb-acl)# 40 deny ip
Device(config-rb-acl)# exit
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff

Device# show ip access allow_webtraff

Role-based IP access list allow_webtraff
    10 permit tcp dst eq www
    20 permit tcp dst eq 443
    30 permit icmp
    40 deny ip

Device# show cts role-based permissions from 2 to 5

Role-based permissions from group 2 to group 5:
srb2
srb5
```

例：SGACL の手動適用

次に、SGACL ポリシーを手動で適用する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based permissions default MYDEFAULTSGACL
Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
Device(config)# exit
```

例：SGACL ポリシーの表示

次に、セキュリティ グループ 3 から送信されたトラフィックの SGACL ポリシーの許可マトリクスの内容を表示する例を示します。

```
Device> enable
Device# show cts role-based permissions from 3

Role-based permissions from group 3 to group 5:
        SRB3
        SRB5
```

```
Role-based permissions from group 3 to group 7:
        SRB4
```

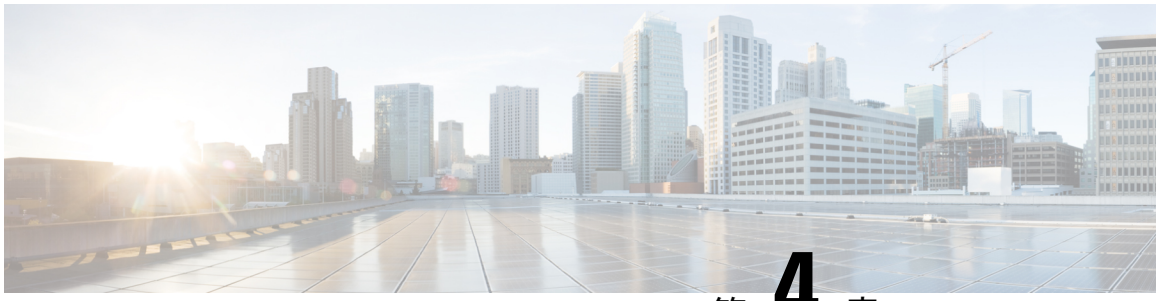
セキュリティグループ ACL ポリシーの機能履歴

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 Fuji 16.9.2	セキュリティグループ ACL ポリシー	SGACL を使用して、ユーザーと宛先リソースのセキュリティグループの割り当てに基づいて、ユーザーが実行できる操作を制御できます。
Cisco IOS XE Amsterdam 17.3.1	拡張 SGACL ロギング	拡張 ACL ロギングにより、NetFlow ハードウェアを使用してはるかに高いレートでロギングを実行できます。

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。



第 4 章

Cisco TrustSec SGACL のハイ アベイラビリティ

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）は、Cisco StackWise 技術をサポートしているスイッチでのハイアベイラビリティ機能をサポートしています。この技術によってステートフルな冗長性が提供され、スイッチスタックはアクセス制御エントリを強制し、処理できます。

Cisco TrustSec SGACL のハイアベイラビリティの前提条件

このマニュアルでは、次のことを前提としています。

- Cisco TrustSec およびセキュリティ グループ アクセス コントロール リスト（SGACL）構成を理解している。
- デバイスは、スタックとして機能するように設定されている。
- スタック内のすべてのデバイスが同一バージョンの Cisco IOS XE ソフトウェアを実行している。

Cisco TrustSec SGACL のハイアベイラビリティの制約事項

- アクティブスイッチとスタンバイスイッチの両方で同時に障害が発生した場合、SGACL のステートフルスイッチオーバーは発生しません。

Cisco TrustSec SGACL のハイアベイラビリティに関する情報

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）は、Cisco StackWise 技術をサポートしているスイッチでのハイアベイラビリティ機能をサポートしています。この技術によってステートフルな冗長性が提供され、スイッチスタックはアクセス制御エントリを強制し、処理できます。

この機能を有効にする Cisco TrustSec 固有の設定はありません。これは、Cisco IOS XE Denali 16.2.1 以降のリリースでサポートされます。

高可用性の概要

スイッチスタックでは、スタックマネージャが最も高い優先順位を持つスイッチをアクティブスイッチとして割り当て、次に高い優先順位を持つスイッチをスタンバイスイッチとして割り当てます。自動または CL I ベースのステートフルスイッチオーバー中は、スタンバイスイッチがアクティブスイッチになり、次に優先順位の高いスイッチなどがスタンバイスイッチになります。

運用データは、初期のシステムブートアップ、運用データの変更（認可変更（CoA）とも呼ばれる）、または運用データのリフレッシュ時に、アクティブスイッチからスタンバイスイッチに同期されます。

ステートフルスイッチオーバー中に、新たにアクティブになったスイッチは、運用データを要求してダウンロードします。環境データ（ENV-data）とロールベース アクセス コントロール リスト（RBACL）は、リフレッシュ時間が完了するまで更新されません。

次の運用データがアクティブスイッチにダウンロードされます。

- 環境データ（ENV-data）：リフレッシュ時または初期化時に RBACL 情報を取得するための優先サーバーリストで構成される可変長フィールド。
- Protected Access Credential（PAC）：セキュアトンネリング（EAP-FAST）のトンネルを介した拡張可能な認証プロトコル Flexible Authentication（FlexAuth; フレキシブル認証）を保護するために、スイッチとオーセンティケータ間で相互に一意に共有される共有秘密。
- ロールベースのポリシー（RBACL または SGACL）：スイッチ上のすべてのセキュリティグループタグ（SGT）マッピングのポリシー定義で構成される可変長ロールベースのポリシーリスト。

（注） デバイス ID とパスワードの詳細で構成される Cisco TrustSec クレデンシャルは、アクティブスイッチでコマンドとして実行されます。

Cisco TrustSec SGACL のハイアベイラビリティの確認

Cisco TrustSec SGACL ハイアベイラビリティ設定を確認するには、アクティブスイッチとスタンバイスイッチの両方で **show cts role-based permissions** コマンドを実行します。コマンドの出力は、両方のスイッチで同じである必要があります。

次に、アクティブスイッチでの **show cts role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

次に、スタンバイスイッチでの show cts role-based permissions コマンドの出力例を示します。

```
Device-stby# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

ステートフルスイッチオーバー後、アクティブスイッチで次のコマンドを実行して機能を確認します。

次に、**show cts pacs** コマンドの出力例を示します。

```
Device# show cts pacs

AID: A3B6D4D8353F102346786CF220FF151C
PAC-Info:
    PAC-type = Cisco Trustsec
    AID: A3B6D4D8353F102346786CF220FF151C
    I-ID: CTS_ED_21
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 17:22:32 IST Mon Mar 14 2016
PAC-Opaque:
000200B80003000100040010A3B6D4D8353F102346786CF220FF151C0006009C00030100E044B2650D8351FD06
F23623C470511E0000001356DEA96C00093A80538898D40F633C368B053200D4C9D2422A7FEB4837EA9DBB89D1
E51DA4E7B184E66D3D5F2839C11E5FB386936BB85250C61CA0116FDD9A184C6E96593EEAF5C39BE08140AFBB19
4EE701A0056600CFF5B12C02DD7ECEAA3CCC8170263669C483BD208052A46C31E39199830F794676842ADEECBB
A30FC4A5A0DEDA93
Refresh timer is set for 01:00:05
```

次に、**show cts environment-data** コマンドの出力例を示します。

```
Device# show cts environment-data

CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0:Unknown
Server List Info:
Installed list: CTSServerList1-000D, 1 server(s):
  *Server: 10.78.105.47, port 1812, A-ID A3B6D4D8353F102346786CF220FF151C
  Status = ALIVE
  auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0001-45 :
  0-00:Unknown
  2-ba:SGT_2
  3-00:SGT_3
  4-00:SGT_4
  5-00:SGT_5
  6-00:SGT_6
  7-00:SGT_7
  8-00:SGT_8
  9-00:SGT_9
  10-16:SGT_10
!
!
!
Environment Data Lifetime = 3600 secs
Last update time = 14:32:53 IST Mon Mar 14 2016
Env-data expires in 0:00:10:04 (dd:hr:mm:sec)
Env-data refreshes in 0:00:10:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

次に、ステートフル スイッチオーバー後の **show cts role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-01
        Deny IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 15:SGT_15:
        SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group 15:SGT_15:
        multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

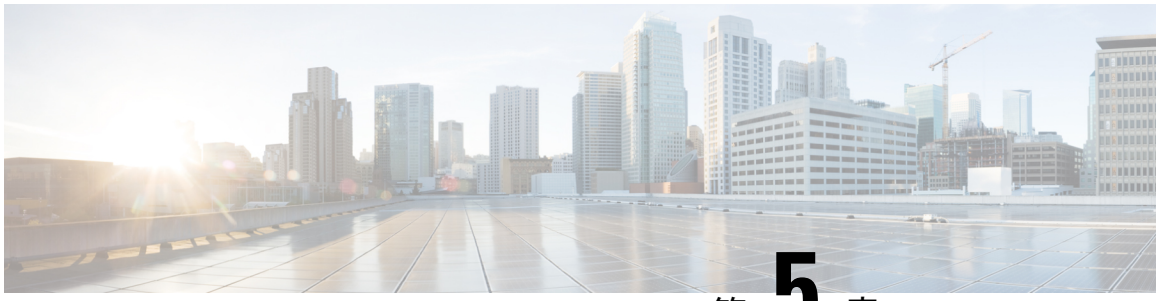
SGACL ハイアベイラビリティの機能履歴

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 Fuji 16.9.2	SGACL ハイ アベイラビリティ	Cisco TrustSec SGACL は、Cisco StackWise 技術をサポートしているスイッチでのハイアベイラビリティ機能をサポートしています。この技術によってステートフルな冗長性が提供され、スイッチスタックはアクセス制御エントリを強制し、処理できます。

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。



第 5 章

SGT 交換プロトコルの設定

SGT 交換プロトコル（SXP）を使用すると、Cisco TrustSec のハードウェアサポートがないネットワークデバイスにセキュリティグループタグ（SGT）を伝播できます。このモジュールでは、ネットワークのスイッチに Cisco TrustSec SXP を設定する方法について説明します。

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。

セキュリティグループタグ（SGT）交換プロトコル（SXP）は、CTS をサポートする複数のプロトコルの 1 つであり、本書では Cisco TrustSec-SXP と呼びます。Cisco TrustSec-SXP は、パケットのタグ付け機能がないネットワークデバイス全体に IP と SGT のバインドの情報を伝播する、制御プロトコルです。Cisco TrustSec-SXP は、IP と SGT のバインドをネットワーク上の認証ポイントからアップストリームデバイスへ渡します。このプロセスにより、スイッチ、ルータ、ファイアウォールのセキュリティ サービスは、アクセス デバイスから学習したアイデンティティ情報を伝えることができます。

SGT 交換プロトコルの前提条件

SXP を導入する前に、Cisco TrustSec-SGT Over Exchange Protocol （SXP）ネットワークを確立する必要があります。このネットワークには次の前提条件があります。

- Cisco TrustSec の機能を既存のルータで使用するには、Cisco TrustSec のセキュリティ ライセンスを購入していること。ルータを発注済みで Cisco TrustSec の機能が必要な場合は、発送前に、このライセンスが使用するルータにプリインストールされていること。

- Cisco TrustSec ソフトウェアをすべてのネットワークデバイス上で実行すること。
- すべてのネットワークデバイス間が接続されていること。
- 認証には Cisco Identity Services Engine 1.0 が必要です。認証には Secure Access Control Server（ACS）Express Appliance サーバーも使用できますが、Cisco TrustSec ではすべての ACS 機能がサポートされていません。ACS 5.1 が Cisco TrustSec-SXP ライセンスで動作していること。
- 異なるルータで異なる値に **retry open timer** コマンドを設定します。

SGT 交換プロトコルの制約事項

- Cisco TrustSec 交換プロトコルは論理インターフェイスでサポートされておらず、物理インターフェイスだけでサポートされています。
- Cisco IOS XE Everest 16.6.4 以降のリリースでは、ダイナミックホスト制御プロトコル（DHCP）スヌーピングが有効になっている場合、DHCP パケットに対する Cisco TrustSec の適用は、適用ポリシーによってバイパスされます。

SGT 交換プロトコルに関する情報

このセクションでは、SGT 交換プロトコルについて説明します。

SGT 交換プロトコルの概要

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。

セキュリティグループタグ（SGT）交換プロトコル（SXP）は、Cisco TrustSec をサポートする複数のプロトコルの 1 つです。SXP は、パケットのタグ付け機能がないネットワークデバイス全体に IP と SGT のバインドの情報を伝播する、制御プロトコルです。Cisco TrustSec は、出力インターフェイスでパケットをフィルタリングします。エンドポイント認証時に、Cisco TrustSec ドメイン（エンドポイントの IP アドレス）にアクセスするホストはダイナミックホスト制御プロトコル（DHCP）スヌーピングおよびIPデバイストラッキングによってアクセスデバイスで SGT に関連付けられます。アクセスデバイスは、Cisco TrustSec ハードウェア対応出力のデバイスに、SXP経由でそのアソシエーションまたはバインドを送信します。これらのデバイスは、送信元の IP と SGT のバインドのテーブルを維持します。パケットは、セキュリティ グループ アクセス コントロール リスト（SGACL）を適用することにより、Cisco TrustSec ハードウェア対応デバイスによって出力インターフェイスでフィルタリングされます。SXP は、IP と SGT のバインドをネットワーク上の認証ポイントからアップストリームデバイスへ渡しま

す。このプロセスにより、スイッチ、ルータ、ファイアウォールのセキュリティ サービスは、アクセス デバイスから学習したアイデンティティ情報を伝えることができます。

SGT は、次のエンドポイント アドミッション コントロール（EAC）アクセス方式のいずれかを使用して割り当てることができます。

- 802.1X ポートベースの認証
- MAC 認証バイパス（MAB）
- Web 認証

SXP は、トランスポートプロトコルとして TCP を使用し、接続を開始するために TCP ポート 64999 を使用します。SXP は、認証と完全性チェックに Message Digest 5（MD5）を使用します。これには、定義された 2 つのロールとして、スピーカー（イニシエータ）とリスナー（レシーバ）があります。

セキュリティ グループ タギング

セキュリティグループタグは、一意のロールに割り当てられる一意の 16 ビットタグです。送信元ユーザー、デバイス、またはエンティティの権限を表し、Cisco TrustSec ドメインの入力でタグ付けされます。SXP は、認証時に取得したデバイスおよびユーザーのクレデンシャルを使用して、ネットワークに進入するパケットをセキュリティグループ（SG）で分類します。このパケット分類は、Cisco TrustSec ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータパス全体を通じて識別され、セキュリティおよびその他のポリシー基準が適用されます。セキュリティグループタグ（SGT）によってエンドポイントデバイスはトラフィックをフィルタリングできるので、ネットワークへのアクセス コントロール ポリシーの適用が可能になります。静的ポート ID は、ポートに接続された特定のエンドポイントの SGT 値をルックアップするために使用されます。

SGT の割り当て

パケットのセキュリティグループタグ（SGT）は、パケットが Cisco TrustSec リンクでタグ付けされたとき、または単一のエンドポイントがポートで認証されたときに、ポートレベルで割り当てることができます。着信パケットの SGT は、次の方法で決定されます。

- SGT でタグ付けされたパケットが信頼ポートに着信すると、パケットのタグはパケットの SGT と見なされます。
- パケットが SGT でタグ付けされているが、信頼できないポートに着信した場合、パケットの SGT は無視され、ピア SGT がポートに設定されます。
- パケットに SGT がない場合、ピア SGT はポートに設定されます。

SGT を割り当てる次の方法がサポートされています。

- IPM（dot1x、MAB、Web 認証）

- VLAN と VLAN と SGT のマッピングは、認証方式がすでに IP アドレスを割り当てられた認証済みエントリに SGT を提供する際に確立されます。デバイスプロセスは、エンドポイントセッションをモニターし、IP と SGT のバインドの変更または削除を検出します。
- SXP（SGT 交換プロトコル）リスナー

SGT 交換プロトコルの設定方法

このセクションでは、SGT 交換プロトコルを設定する方法について説明します。

デバイス SGT の手動設定

通常の Cisco TrustSec 動作では、認証サーバーがデバイスから発信されるパケット用に、そのデバイスに SGT を割り当てます。認証サーバーにアクセスできない場合は、使用する SGT を手動で設定できますが、認証サーバーから割り当てられた SGT のほうが、手動で割り当てた SGT よりも優先されます。

デバイスの SGT を手動で設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# configure terminal`	グローバル設定モードを開始します。
ステップ 2	**cts sgt** *tag* **例：** `Device(config)# cts sgt tag`	デバイスから送信されるパケットの SGT を設定します。tag 引数は 10 進表記です。指定できる範囲は 1 ～ 65533 です。
ステップ 3	**exit** **例：** `Device(config)# exit`	設定モードを終了します。

SXP ピア接続の設定

両方のデバイスで SXP ピア接続を設定する必要があります。一方のデバイスはスピーカーで、他方のデバイスはリスナーになります。パスワード保護を使用している場合は、必ず両エンドに同じパスワードを使用してください。

（注） デフォルトの SXP 送信元 IP アドレスが設定されておらず、かつ接続の SXP 送信元アドレスが指定されていない場合、Cisco TrustSec ソフトウェアは既存のローカル IP アドレスから SXP 送信元 IP アドレスを抽出します。SXP 送信元アドレスは、デバイスから開始される各 TCP 接続ごとに異なる場合があります。

SXP ピア接続を設定するには、次の作業を行います。

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 sxp connection peer** *peer-ipv4-addr*[**source** *src-ipv4-addr*] **password** {**default | none**} **mode** {**local | peer**} {**speaker | listener**} { **vrf** *vrf-name*} 例： `Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener`	SXP アドレス接続を設定します。 オプションの **source** キーワードには発信元デバイスの IPv4 アドレスを指定します。アドレスが指定されていない場合、接続は、デフォルトの送信元アドレス（設定されている場合）、またはポートのアドレスを使用します。 **password** キーワードには、SXP で接続に使用するパスワードを指定します。次のオプションがあります。 • **default**：**cts sxp default password** コマンドを使用して設定したデフォルトの SXP パスワードを使用します。 • **none**：パスワードを使用しないでください。 mode キーワードでは、リモート ピア デバイスのロールを指定します。 • **local**：指定したモードはローカルデバイスを参照します。

	コマンドまたはアクション	目的
		• **peer**：指定したモードはピアデバイスを参照します。 • **speaker**：デフォルトこのデバイスが接続の際にスピーカーになります。 • **listener**：このデバイスが接続の際にリスナーになります。 オプションの **vrf** キーワードでは、ピアに対する VRF を指定します。デフォルトはデフォルト VRF です。
ステップ 4	**exit** 例： `Device(config)# exit`	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。
ステップ 5	**show cts sxp connections** 例： `Device# show cts sxp connections`	（任意）SXP 接続情報を表示します。

デフォルトの SXP パスワードの設定

デフォルトでは、SXP は接続のセットアップ時にパスワードを使用しません。

デフォルト SXP パスワードを設定するには、次の作業を行います。

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 sxp default password** [**0** | **6** | **7**] *password* 例： `Device(config)# cts sxp default password 0 hello`	SXP のデフォルト パスワードを設定します。クリアテキストパスワード（**0** を使用するかオプションなし）または暗号化パスワード（**6** または **7** オプションを

	コマンドまたはアクション	目的
		使用）を入力できます。パスワードの最大長は 32 文字です。
ステップ 4	**exit** 例： `Device(config)# exit`	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。

デフォルトの SXP 送信元 IP アドレスの設定

SXP は送信元 IP アドレスが指定されないと、新規の TCP 接続すべてにデフォルトの送信元 IP アドレスを使用します。デフォルト SXP 送信元 IP アドレスを設定しても、既存の TCP 接続には影響しません。

デフォルト SXP 送信元 IP アドレスを設定するには、次の作業を行います。

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 sxp default source-ip** *src-ip-addr* 例： `Device(config)# cts sxp default source-ip 10.0.1.2`	SXP のデフォルトの送信元 IP アドレスを設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	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。

SXP の復帰期間の変更

ピアが SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、SXP 復帰期間タイマーが開始されます。SXP 復帰期間タイマーがアクティブな間、Cisco TrustSec ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。デフォルト値は 120 秒

（2 分）です。SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

SXP の復帰期間を変更するには、次の作業を行います。

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 sxp reconciliation period** *seconds* 例： `Device(config)# cts sxp reconciliation period 360`	SXP復帰タイマーを変更します。デフォルト値は 120 秒（2 分）です。範囲は 0 ～ 64000 です。
ステップ 4	**exit** 例： `Device(config)# exit`	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。

SXP リトライ期間の変更

SXP リトライ期間によって、Cisco TrustSec ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、Cisco TrustSec ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。デフォルト値は 120 秒です。SXP 再試行期間を 0 秒に設定するとタイマーは無効になり、接続は再試行されません。

SXP のリトライ期間を変更するには、次の作業を行います。

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：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**cts sxp retry period** *seconds* 例： `Device(config)# cts sxp retry period 360`	SXP リトライ タイマーを変更します。デフォルト値は 120 秒（2 分）です。範囲は 0 ～ 64000 です。
ステップ 4	**exit** 例： `Device(config)# exit`	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。

SXP で学習された IP アドレスと SGT マッピングの変更をキャプチャするための syslog の作成方法

グローバル コンフィギュレーション モードで **cts sxp log binding-changes** コマンドを設定すると、IP アドレスと SGT バインドの変更（追加、削除、変更）が発生するたびに SXP の syslog（sev 5 syslog）が生成されます。これらの変更は SXP 接続で学習されて伝播されます。デフォルトは、**no cts sxp log binding-changes** です。

バインディングの変更のロギングをイネーブルにするには、次の作業を実行します。

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 sxp log binding-changes** 例： `Device(config)# cts sxp log binding-changes`	IP と SGT のバインドの変更のロギングを有効にします。
ステップ 4	**exit** 例： `Device(config)# exit`	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。

SGT 交換プロトコルの設定例

このセクションでは、SGT 交換プロトコルの設定例を示します。

例：Cisco TrustSec SXP および SXP ピア接続の有効化

以下に、SXP を有効にし、デバイス A（スピーカー）とデバイス B（リスナー）間に SXP ピア接続を設定する方法の例を示します。

```
Device# configure terminal
Device(config)# cts sxp enable
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.10.1.1
Device(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

以下に、デバイス B（リスナー）とデバイス A（スピーカー）間に SXP ピア接続を設定する方法の例を示します。

```
Device# configure terminal
Device(config)# cts sxp enable
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.20.2.2
Device(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

例：デフォルトの SXP パスワードと送信元 IP アドレスの設定

次に、デフォルトのSXPパスワードとの送信元IPアドレスを設定する例を示します。

```
Device# configure terminal
Device(config)# cts sxp default password Cisco123
Device(config)# cts sxp default source-ip 10.20.2.2
Device(config)# end
```

SGT 交換プロトコルの接続の確認

SXP 接続を表示するには、次の作業を行います。

コマンド	目的
show cts sxp connections	SXP ステータスと接続に関する詳細情報を表示します。
show cts sxp connections [brief]	SXP ステータスと接続に関する要約情報を表示します。

次に、**show cts sxp connections** コマンドの出力例を示します。

```
Device# show cts sxp connections

SXP                      : Enabled
Default Password         : Set
Default Source IP        : 10.10.1.1
Connection retry open period: 10 secs
Reconcile period         : 120 secs
Retry open timer is not running
------------------------------------------------
Peer IP                  : 10.20.2.2
Source IP                : 10.10.1.1
Conn status              : On
Conn Version             : 2
Connection mode          : SXP Listener
Connection inst#         : 1
TCP conn fd              : 1
TCP conn password        : default SXP password
Duration since last state change: 0:00:21:25 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

次に、**show cts sxp connections brief** コマンドの出力例を示します。

```
Device# show cts sxp connections brief

SXP                      : Enabled
Default Password         : Set
Default Source IP        : Not Set
Connection retry open period: 120 secs
Reconcile period         : 120 secs
Retry open timer is not running
-----------------------------------------------------------------------------
Peer_IP          Source_IP          Conn Status    Duration
-----------------------------------------------------------------------------
10.1.3.1         10.1.3.2           On             6:00:09:13 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

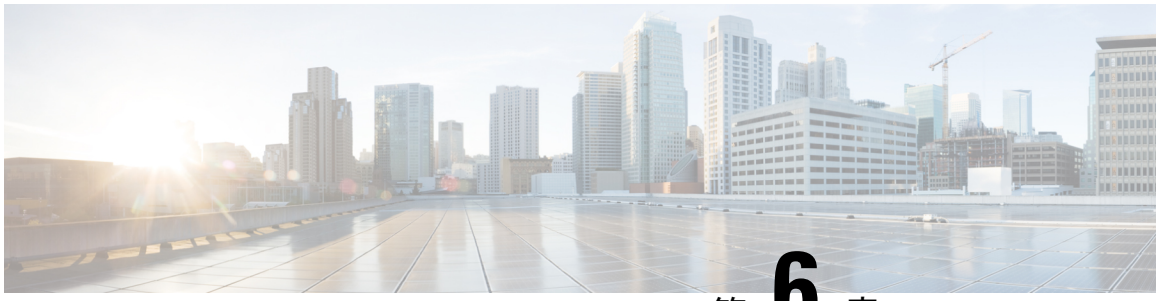
SGT 交換プロトコルの機能履歴

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 Fuji 16.9.2	SGT 交換プロトコル	SXP は、Cisco TrustSec のハードウェアサポートがないネットワークデバイスに SGT を伝播します。

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。



第 6 章

セキュリティグループタグのマッピングの設定

サブネットとセキュリティ グループ タグ（SGT）のマッピングは、指定したサブネット内のすべてのホスト アドレスに SGT をバインドします。このマッピングが実行されると、Cisco TrustSec により、指定のサブネットに属する送信元 IP アドレスを持つ任意の着信パケットに SGT が課せられます。

SGT のマッピングの制約事項

サブネットと SGT のマッピングの制約事項

- /31 プレフィックスの IPv4 サブ ネットワークを拡張できません。
- サブネットホストアドレスは、**network-map** *bindings* bindings パラメータが、指定したサブネットのサブネットホストの合計数よりも小さいか、bindings が 0 の場合、セキュリティグループタグ（SGT）にバインドできません。
- セキュリティ交換プロトコル（SXP）スピーカーおよびリスナーが SXPv3 以降のバージョンを実行している場合のみ、IPv6 拡張および伝播が実行されます。

デフォルトルートの SGT マッピングの制約事項

- デフォルトルートの設定は、サブネット **/0** でのみ受け入れられます。サブネット /0 なしで host-ip のみを入力すると、次のメッセージが表示されます。

```
Device(config)#cts role-based sgt-map 0.0.0.0 sgt 1000
Default route configuration is not supported for host ip
```

SGT のマッピングに関する情報

このセクションでは、SGT マッピングに関する情報を提供します。

サブネットと SGT のマッピングの概要

サブネットと SGT のマッピングは、指定したサブネット内のすべてのホストアドレスに SGT をバインドします。Cisco TrustSec は着信パケットの送信元 IP アドレスが指定したサブネットに属する場合そのパケットに SGT を適用します。サブネットおよび SGT は、**cts role-based sgt-map** *net_address/prefix* **sgt** *sgt_number* グローバル コンフィギュレーション コマンドを使用して CLI で指定されます。単一のホストは、このコマンドでマップされる可能性があります。

IPv4 ネットワークでは、セキュリティ交換プロトコル（SXP）v3 以降のバージョンは SXPv3 ピアからサブネットの *net_address/prefix* ストリングを受信し、解析できます。SXP の以前のバージョンでは、SXP リスナー ピアにエクスポートする前に、サブネットのプレフィックスをホスト バインドのセットに変換します。

たとえば、IPv4 サブネット 192.0.2.0/24 は次のように拡張されます（ホストアドレスの 3 ビットのみ）。

- ホストアドレス 198.0.2.1 から 198.0.2.7：タグ付けされて SXP ピアに伝播します。
- ネットワークおよびブロードキャストアドレス 198.0.2.0 および 198.0.2.8：タグ付けされず、伝播しません。

SXPv3 がエクスポートできるサブネットバインドの数を制限するには、**cts sxp mapping network-map** グローバル コンフィギュレーション コマンドを使用します。

サブネット バインディングはスタティックで、アクティブ ホストの学習はありません。これらは SGT インポジションおよび SGACL の適用にローカルで使用できます。サブネットと SGT のマッピングによってタグ付けされたパケットは、レイヤ 2 またはレイヤ 3 Cisco TrustSec リンクに伝播できます。

IPv6 ネットワークの場合、SXPv3 は SXPv2 または SXPv1 ピアにサブネット バインディングをエクスポートできません。

VLAN と SGT のマッピングの概要

VLAN と SGT のマッピング機能は、指定した VLAN からのパケットに SGT をバインドします。これは、次のような点で、レガシーネットワークからの Cisco TrustSec 対応ネットワークへの移行を簡素化します。

- レガシーのスイッチ、ワイヤレスコントローラ、アクセスポイント、VPN などの、Cisco TrustSec 対応ではないが VLAN 対応のデバイスをサポートします。

- データセンターのサーバー セグメンテーションなどの、VLAN および VLAN ACL がネットワークを分割するトポロジに対する下位互換性を提供します。

VLAN と SGT のバインドは、**cts role-based sgt-map vlan-list** グローバル コンフィギュレーション コマンドで設定します。

Cisco TrustSec 対応スイッチ上で、スイッチ仮想インターフェイス（SVI）であるゲートウェイが VLAN に割り当てられており、そのスイッチで IP デバイストラッキングが有効になっている場合、Cisco TrustSec は、SVI サブネットにマッピングされている VLAN 上のすべてのアクティブなホストに対して IP と SGT のバインドを作成できます。

アクティブ VLAN のホストの IP-SGT バインディングは SXP リスナーにエクスポートされます。マッピングされた各 VLAN のバインドは VRF に関連付けられた IP-to-SGT テーブルに挿入されます。VLAN は SVI または **cts role-based l2-vrf** コマンドでマッピングされます。

VLAN と SGT のバインドの優先順位は最も低く、SXP または CLI ホスト コンフィギュレーションなどのその他のソースからのバインドを受け取った場合は、無視されます。バインドの優先順位は、「バインド送信元の優先順位」セクションに記載されています。

レイヤ 3 論理インターフェイスと SGT のマッピング（L3IF-SGT マッピング）の概要

L3IF-SGTマッピングは、基盤となる物理インターフェイスに関係なく、次のレイヤ3インターフェイスのいずれかのトラフィックに SGT を直接マッピングできます。

- ルーテッド ポート
- SVI（VLAN インターフェイス）
- レイヤ 2 ポートのレイヤ 3 サブインターフェイス
- トンネル インターフェイス

（SGT アソシエーションが Cisco ISE または Cisco ACS アクセスサーバーから動的に取得される）特定の SGT 番号またはセキュリティグループ名を指定するには、**cts role-based sgt-map interface** グローバル コンフィギュレーション コマンドを使用します。

アイデンティティ ポート マッピング（ctsインターフェイス手動サブモードコンフィギュレーション）および L3IF-SGT が異なる IP と SGT のバインドを必要とする場合、IPM が優先されます。IP と SGT のバインドのその他の競合は、「バインド送信元の優先順位」セクションにリストされている優先順位に従って解決されます。

バインディング送信元プライオリティ

Cisco TrustSec は完全優先方式で IP-SGT バインドソース間の競合を解決します。たとえば、SGT は **policy** { **dynamic identity** *peer-name* | **static sgt** *tag*} Cisco Trustsec 手動インターフェイス モード コマンド（アイデンティティ ポート マッピング）を使用してインターフェイスに適用

されます。現在の優先順位の適用順序は、最も小さい（1）から最高（7）まで、次のとおりです。

1. VLAN：VLAN-SGT マッピングが設定された VLAN 上のスヌーピングされた ARP パケットから学習されたバインディング。
2. CLI：cts role-based sgt-map グローバル コンフィギュレーション コマンドの IP-SGT 形式を使用して設定されたアドレス バインディング。
3. レイヤ 3 インターフェイス：（L3IF）一貫した L3IF-SGT マッピングやアイデンティティ ポート マッピングを使用する 1 つ以上のインターフェイスを通るパスを持つ FIB 転送エントリが原因で追加されたバインディング。
4. SXP：SXP ピアから学習されたバインディング。
5. IP_ARP：タグ付けされた ARP パケットが CTS 対応リンクで受信されたときに学習されたバインディング。
6. LOCAL：EPM とデバイス トラッキングによって学習された認証済みホストのバインディング。このタイプのバインディングには、L2 [I]PM が設定されたポートの ARP スヌーピングによって学習された個々のホストも含まれます。
7. INTERNAL：ローカルで設定された IP アドレスとデバイス独自の SGT 間のバインディング。

デフォルトルートの SGT

デフォルトルートのセキュリティグループタグ（SGT）は、デフォルトルートに SGT 番号を割り当てます。

デフォルトルートは、指定されたルートと一致しないルートであるため、ラストリゾートの宛先へのルートです。デフォルトルートは、ルーティングテーブルに明示的にリストされていないネットワークが宛先になっているパケットの転送に使用されます。

SGT のマッピングの設定方法

このセクションでは、SGT マッピングを設定する例を示します。

デバイス SGT の手動設定

通常の Cisco TrustSec 動作では、認証サーバーがデバイスから発信されるパケット用に、そのデバイスに SGT を割り当てます。認証サーバーにアクセスできない場合は、使用する SGT を手動で設定できますが、認証サーバーから割り当てられた SGT のほうが、手動で割り当てた SGT よりも優先されます。

デバイスの SGT を手動で設定するには、次の作業を行います。

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 sgt** *tag* 例： `Device(config)# cts sgt 1234`	Cisco TrustSec の SXP をイネーブルにします。
ステップ 4	**exit** 例： `Device(config)# exit`	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。

サブネットと SGT のマッピングの設定

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	**cts sxp mapping network-map** *bindings* 例： `Device(config)# cts sxp mapping network-map 10000`	• サブネットと SGT のマッピングのホスト数の制限を設定します。bindings 引数は、SGT にバインドされ、SXP リスナーにエクスポートできるサブネット IP ホストの最大数を指定します。 • *bindings*：（0 ～ 65,535）デフォルトは 0（実行される拡張なし）です。

	コマンドまたはアクション	目的
ステップ 4	**cts role-based sgt-map** *ipv4_address/prefix* **sgt** *number* 例： `Device(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234`	（IPv4）CIDR 表記でサブネットを指定します。 • サブネットと SGT のマッピング設定を取り消すには、このコマンドの *no* 形式を使用します。ステップ 2 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。sgt number キーワードは、指定したサブネットの各ホスト アドレスにバインドするセキュリティ グループ タグを指定します。 • *ipv4_address*：ドット付き 10 進表記で IPv4 ネットワークアドレスを指定します。 • *prefix*：（0 ～ 30）ネットワークアドレス内のビット数を指定します。 • **sgt** *number*：（0 ～ 65,535）セキュリティグループタグ（SGT）番号を指定します。
ステップ 5	**cts role-based sgt-map** *ipv6_address::prefix* **sgt** *number* 例： `Device(config)# cts role-based sgt-map 2020::/64 sgt 1234`	（IPv6）コロン 16 進表記でサブネットを指定します。サブネットと SGT のマッピング設定を取り消すには、このコマンドの *no* 形式を使用します。 ステップ 2 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。sgt number キーワードは、指定したサブネットの各ホスト アドレスにバインドするセキュリティ グループ タグを指定します。 • *ipv6_address*：コロン 16 進表記で IPv6 ネットワークアドレスを指定します。 • *prefix*：（0 ～ 128）ネットワークアドレス内のビット数を指定します。

	コマンドまたはアクション	目的
		• **sgt** *number*：（0 ～ 65,535）セキュリティグループタグ（SGT）番号を指定します。
ステップ 6	**exit** 例： `Device(config)# exit`	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。

VLAN と SGT のマッピングの設定

Cisco TrustSec デバイスで VLAN-SGT マッピングを設定するタスクフロー。

- 着信 VLAN の同じ VLAN_ID でデバイス上に VLAN を作成します。
- エンドポイントのクライアントに対して、デフォルトゲートウェイになるようにデバイスの VLAN に SVI を作成します。
- VLAN トラフィックに SGT を適用するようにデバイスを設定します。
- デバイスの IP デバイストラッキングを有効にします。
- VLAN にデバイストラッキングポリシーをアタッチします。

（注） マルチスイッチネットワークでは、SISF ベースのデバイストラッキングにより、機能を実行しているスイッチ間でバインドテーブルエントリを分散できます。これは、ホストがアクセスポートに表示されるスイッチでバインドエントリが作成され、トランクポートを介して表示されるホストに対してエントリが作成されないことを前提としています。マルチスイッチセットアップでこれを行うには、『*Security Configuration Guide*』の「*Configuring SISF-Based Device Tracking*」の章にある「*Configuring a Multi-Switch Network to Stop Creating Binding Entries from a Trunk Port*」の手順に従って、別のポリシーを設定し、トランクポートにアタッチすることを推奨します。

- VLAN と SGT のマッピングがデバイスで発生することを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device# enable`	• 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	**vlan** *vlan_id* 例： `Device(config)# vlan 100`	TrustSec 対応ゲートウェイデバイスに VLAN 100 を作成し、VLAN 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	[**no**] **shutdown** 例： `Device(config-vlan)# no shutdown`	VLAN 100 をプロビジョニングします。
ステップ 5	**exit** 例： `Device(config-vlan)# exit`	VLAN 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 6	**interface** *type slot/port* 例： `Device(config)# interface vlan 100`	インターフェイス タイプを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *slot/port* 例： `Device(config-if)# ip address 10.1.1.2 255.0.0.0`	VLAN 100 のスイッチ仮想インターフェイス（SVI）を設定します。
ステップ 8	[**no**] **shutdown** 例： `Device(config-if)# no shutdown`	SVI をイネーブルにします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス 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 10	**cts role-based sgt-map vlan-list** *vlan_id* **sgt** *sgt_number* 例： `Device(config)# cts role-based sgt-map vlan-list 100 sgt 10`	指定した SGT を指定した VLAN を割り当てます。

	コマンドまたはアクション	目的
ステップ 11	**device-tracking policy** *policy-name* 例： `Device(config)# device-tracking policy policy1`	ポリシーを指定し、デバイストラッキング ポリシー コンフィギュレーション モードを開始します。
ステップ 12	**tracking enable** 例： `Device(config-device-tracking)# tracking enable`	ポリシー属性のデフォルトのデバイス トラッキング設定を上書きします。
ステップ 13	**exit** 例： `Device(config-device-tracking)# exit`	デバイストラッキング ポリシー コンフィギュレーション モードを終了します。続いて、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 14	**vlan configuration** *vlan_id* 例： `Device(config)# vlan configuration 100`	デバイス トラッキング ポリシーをアタッチする VLAN を指定し、その VLAN のコンフィギュレーション モードを開始します。
ステップ 15	**device-tracking attach-policy** *policy-name* 例： `Device(config-vlan-config)# device-tracking attach-policy policy1`	指定された VLAN にデバイス トラッキング ポリシーをアタッチします。
ステップ 16	**end** 例： `Device(config-vlan-config)# end`	VLAN 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。
ステップ 17	**show cts role-based sgt-map** {*ipv4_netaddr* | *ipv4_netaddr/prefix* | *ipv6_netaddr* | *ipv6_netaddr/prefix* |**all** [**ipv4** |**ipv6**] |**host** { *ipv4__addr* |*ipv6_addr* } |**summary** [**ipv4** |**ipv6**] 例： `Device# show cts role-based sgt-map all`	（任意）VLAN と SGT のマッピングを表示します。
ステップ 18	**show device-tracking policy** *policy-name* 例： `Device# show device-tracking policy policy1`	（任意）現在のポリシー属性を表示します。

L3IF と SGT のマッピングの設定

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	**cts role-based sgt-map interface** *type slot/port* [**security-group** *name* | **sgt** *number*] 例： `Device(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77`	SGT は指定されたインターフェイスへの入力トラフィックに適用されます。 • **interface** *type slot/port*：使用可能なインターフェイスのリストを表示します。 • **security-group** *name*：SGT ペアリングに対するセキュリティグループ名は Cisco ISE または Cisco ACS で設定されています。 • **sgt** *number*：（0 ～ 65,535）。セキュリティグループタグ（SGT）番号を指定します。
ステップ 4	**exit** 例： `Device(config)# exit`	設定モードを終了します。
ステップ 5	**show cts role-based sgt-map all** 例： `Device# cts role-based sgt-map all`	入力トラフィックに指定された SGT がタグ付けされたことを確認します。

ハードウェアキーストアのエミュレート

ハードウェアキーストアが存在しないか使用できない場合は、キーストアのソフトウェアエミュレーションを使用するようにスイッチを設定できます。ソフトウェアキーストアの使用を設定するには、次の作業を行います。

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 keystore emulate** 例： `Device(config)# cts keystore emulate`	ハードウェアキーストアの代わりにキーストアのソフトウェアエミュレーションを使用するようにスイッチを設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	設定モードを終了します。
ステップ 5	**show keystore** 例： `Device# show keystore`	キーストアのステータスと内容を表示します。保存された秘密は表示されません。

デフォルトルートの SGT の設定

始める前に

ip route 0.0.0.0 コマンドを使用して、デバイスにデフォルトルートがすでに作成されていることを確認します。そうでない場合、デフォルトルート（デフォルトルートの SGT に付属）は不明な宛先を取得するため、ラストリゾートの宛先は CPU を指します。

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。

	コマンドまたはアクション	目的

ステップ 3	**cts role-based sgt-map 0.0.0.0/0 sgt** *number*
	例：
	`Device(config)# cts role-based sgt-map 0.0.0.0/0 sgt 3`
		デフォルトルートの SGT 番号を指定します。有効値は 0 ～ 65,519 です。
		（注）
		• **host_address/subnet** は、IPv4 アドレス（0.0.0.0/0）または IPv6 アドレス（0:0::/0）のどちらかです。
		• デフォルトルートの設定は、サブネット **/0** でのみ受け入れられます・サブネット /0 なしで host-ip のみを入力すると、次のメッセージが表示されます。
		`Device(config)#cts role-based sgt-map 0.0.0.0 sgt 1000`
		`Default route configuration is not supported for host ip`

ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

SGT のマッピングの確認

次のセクションでは、SGT マッピングを確認する方法を示します。

サブネットと SGT のマッピングの設定確認

サブネットと SGT のマッピングの設定情報を表示するには、次の show コマンドのいずれかを使用します。

コマンド	目的
show cts sxp connections	SXP スピーカーとリスナーの接続と、動作ステータスを表示します。
show cts sxp sgt-map	SXP リスナーにエクスポートした IP と SGT のバインディングを表示します。

コマンド	目的
show running-config	サブネットと SGT のコンフィギュレーション コマンドが実行コンフィギュレーション ファイル内にあることを確認します。

VLAN と SGT のマッピングの確認

VLAN と SGT の設定情報を表示するには、次の show コマンドを使用します。

表 *1:*

コマンド	目的
show device-tracking policy	デバイストラッキング ポリシーの現在のポリシー属性を表示します。
show cts role-based sgt-map	IP アドレスと SGT のバインドを表示します。

L3IF と SGT のマッピングの確認

L3IF と SGT の設定情報を表示するには、次の show コマンドを使用します。

コマンド	目的
show cts role-based sgt-map all	すべての IP アドレスと SGT のバインドを表示します。

デフォルトルートの SGT の設定確認

デフォルトルートの SGT の設定確認

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

IP Address              SGT     Source
============================================
0.0.0.0/0               3       CLI
11.0.0.0/8              11      CLI
11.0.0.10               1110    CLI
11.1.1.1                1111    CLI
21.0.0.2                212     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 5
Total number of active   bindings = 5
```

SGT のマッピングの設定例

このセクションでは、SGT のマッピングの設定例を示します。

例：デバイス SGT の手動設定

```
Device# configure terminal
Device(config)# cts sgt 1234
Device(config)# exit
```

例：サブネットと SGT のマッピングの設定

次の例は、SXPv3 を実行しているデバイス（Device 1 と Device 2）間の IPv4 サブネットと SGT のマッピングを設定する方法を示します。

1. デバイス間の SXP スピーカー/リスナー ピアリングを設定します。

```
Device1# configure terminal
Device1(config)# cts sxp enable
Device1(config)# cts sxp default source-ip 1.1.1.1
Device1(config)# cts sxp default password 1syzygy1
Device1(config)# cts sxp connection peer 2.2.2.2 password default mode local speaker
```

2. Device 1 の SXP リスナーとして Device 2 を設定します。

```
Device2(config)# cts sxp enable
Device2(config)# cts sxp default source-ip 2.2.2.2
Device2(config)# cts sxp default password 1syzygy1
Device2(config)# cts sxp connection peer 1.1.1.1 password default mode local listener
```

3. Device 2 で、SXP 接続が動作していることを確認してください。

```
Device2# show cts sxp connections brief | include 1.1.1.1
          1.1.1.1                 2.2.2.2          On                 3:22:23:18
 (dd:hr:mm:sec)
```

4. サブネットワークが Device 1 に拡張されるように設定します。

```
Device1(config)# cts sxp mapping network-map 10000
Device1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Device1(config)# cts role-based sgt-map 11.11.11.0/29 sgt 11111
Device1(config)# cts role-based sgt-map 192.168.1.0/28 sgt 65000
```

5. Device 2 で、Device1 からのサブネットと SGT の拡張を確認します。ここには、10.10.10.0/30 サブネットワーク用の拡張が 2 個、11.11.11.0/29 サブネットワーク用の拡張が 6 個、192.168.1.0/28 サブネットワーク用の拡張が 14 個存在する必要があります。

```
Device2# show cts sxp sgt-map brief | include 101|11111|65000
            IPv4,SGT: <10.10.10.1 , 101>
            IPv4,SGT: <10.10.10.2 , 101>
            IPv4,SGT: <11.11.11.1 , 11111>
            IPv4,SGT: <11.11.11.2 , 11111>
            IPv4,SGT: <11.11.11.3 , 11111>
```

```
IPv4,SGT: <11.11.11.4 , 11111>
IPv4,SGT: <11.11.11.5 , 11111>
IPv4,SGT: <11.11.11.6 , 11111>
IPv4,SGT: <192.168.1.1 , 65000>
IPv4,SGT: <192.168.1.2 , 65000>
IPv4,SGT: <192.168.1.3 , 65000>
IPv4,SGT: <192.168.1.4 , 65000>
IPv4,SGT: <192.168.1.5 , 65000>
IPv4,SGT: <192.168.1.6 , 65000>
IPv4,SGT: <192.168.1.7 , 65000>
IPv4,SGT: <192.168.1.8 , 65000>
IPv4,SGT: <192.168.1.9 , 65000>
IPv4,SGT: <192.168.1.10 , 65000>
IPv4,SGT: <192.168.1.11 , 65000>
IPv4,SGT: <192.168.1.12 , 65000>
IPv4,SGT: <192.168.1.13 , 65000>
IPv4,SGT: <192.168.1.14 , 65000>
```

6. Device 1 の拡張数を確認します。

```
Device1# show cts sxp sgt-map
            IP-SGT Mappings expanded:22
            There are no IP-SGT Mappings
```

7. Device 1 と Device 2 の設定を保存し、グローバル コンフィギュレーション モードを終了します。

```
Device1(config)# copy running-config startup-config
Device1(config)# exit
Device2(config)# copy running-config startup-config
Device2(config)# exit
```

例：アクセスリンクを介した1つのホストに対するVLANとSGTのマッピングの設定

次の例では、単一のホストは、アクセスデバイス上の VLAN 100 に接続します。TrustSec デバイスのスイッチ仮想インターフェイスは VLAN 100 のエンドポイントのデフォルトゲートウェイになります（IP アドレス 10.1.1.1）。TrustSec デバイスは VLAN 100 からのパケットにセキュリティグループタグ（SGT）10 を適用します。

1. アクセスデバイス上に VLAN 100 を作成します。

```
access_device# configure terminal
access_device(config)# vlan 100
access_device(config-vlan)# no shutdown
access_device(config-vlan)# exit
access_device(config)#
```

2. アクセスリンクとして TrustSec デバイスのインターフェイスを設定します。エンドポイントのアクセス ポートの設定は、この例では省略されます。

```
access_device(config)# interface gigabitEthernet 6/3
access_device(config-if)# switchport
access_device(config-if)# switchport mode access
access_device(config-if)# switchport access vlan 100
```

3. TrustSec デバイスに VLAN 100 を作成します。

```
TS_device(config)# vlan 100
TS_device(config-vlan)# no shutdown
TS_device(config-vlan)# end
TS_device#
```

4. 着信 VLAN 100 のゲートウェイとして SVI を作成します。

```
TS_device(config)# interface vlan 100
TS_device(config-if)# ip address 10.1.1.2 255.0.0.0
TS_device(config-if)# no shutdown
TS_device(config-if)# end
TS_device(config)#
```

5. VLAN 100 のホストにセキュリティ グループ タグ（SGT）10 を割り当てます。

```
TS_device(config)# cts role-based sgt-map vlan 100 sgt 10
```

6. TrustSec デバイスの IP デバイストラッキングを有効にします。それが動作していることを確認します。

```
TS_device(config)# ip device tracking
TS_device# show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 100
--------------------------------------------------------------------
  IP Address     MAC Address   Vlan   Interface          STATE
--------------------------------------------------------------------
Total number interfaces enabled: 1
Vlan100
```

7. （任意）エンドポイントからデフォルトゲートウェイを ping します（この例では、ホスト IP アドレス 10.1.1.1）。SGT 10 が VLAN 100 のホストにマッピングされていることを確認します。

```
TS_device# show cts role-based sgt-map all

Active IP-SGT Bindings Information

IP Address          SGT          Source
============================================

10.1.1.1            10            VLAN

IP-SGT Active Bindings Summary
============================================
Total number of VLAN bindings = 1
Total number of CLI bindings = 0
Total number of active bindings = 1
```

例：入力ポートでの L3IF と SGT のマッピングの設定

次の例では、デバイスラインカードのレイヤ3インターフェイスで、すべての入力トラフィックにSGT3がタグ付けされるように設定します。接続されたサブネットのプレフィックスがすでにわかっています。

1. インターフェイスを設定します。

```
Device# configure terminal
Device(config)# interface gigabitEthernet 6/3 sgt 3
Device(config)# exit
```

2. インターフェイスに着信するトラフィックが適切にタグ付けされることを確認します。

```
Device# show cts role-based sgt-map all
IP Address          SGT             Source
========================================
15.1.1.15           4               INTERNAL
17.1.1.0/24         3               L3IF
21.1.1.2            4               INTERNAL
31.1.1.0/24         3               L3IF
31.1.1.2            4               INTERNAL
43.1.1.0/24         3               L3IF
49.1.1.0/24         3               L3IF
50.1.1.0/24         3               L3IF
50.1.1.2            4               INTERNAL
51.1.1.1            4               INTERNAL
52.1.1.0/24         3               L3IF
81.1.1.1            5               CLI
102.1.1.1           4               INTERNAL
105.1.1.1           3               L3IF
111.1.1.1           4               INTERNAL
IP-SGT Active Bindings Summary
========================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 7
Total number of INTERNAL bindings = 7
Total number of active   bindings = 15
```

例：ハードウェアキーストアのエミュレート

次に、ソフトウェアキーストアの使用を設定および確認する例を示します。

```
Device# configure terminal
Device(config)# cts keystore emulate
Device(config)# exit
Device#show keystore
No hardware keystore present, using software emulation.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):
Index    Type     Name
-----    ----     ----
0         S       CTS-password
1         P       ECF05BB8DFAD854E8376DEA4EF6171CF
```

例：デバイスルートの SGT の設定

```
Device# configure terminal
Device(config)# cts role-based sgt-map 0.0.0.0/0 sgt 3
Device(config)# exit
```

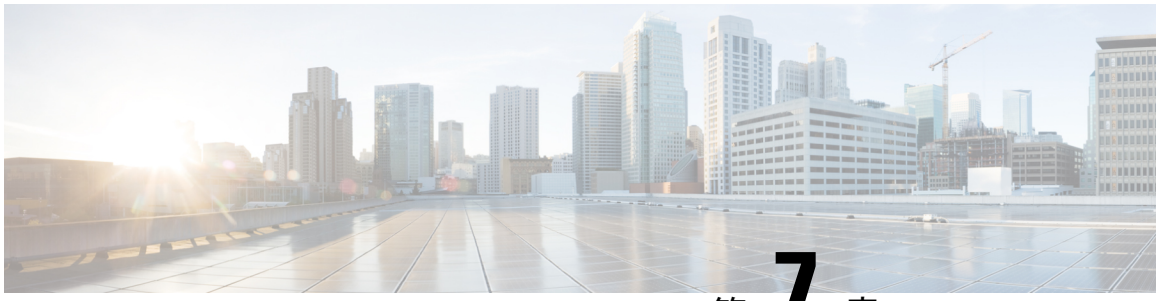
セキュリティグループタグのマッピングの機能履歴

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 Fuji 16.9.2	セキュリティグループタグのマッピング	サブネットと SGT のマッピングは、指定したサブネット内のすべてのホストアドレスに SGT をバインドします。このマッピングが実行されると、Cisco TrustSec により、指定のサブネットに属する送信元 IP アドレスを持つ任意の着信パケットに SGT が課せられます。
Cisco IOS XE Gibraltar 16.11.1	デフォルトルート SGT の分類	デフォルトルート SGT は、指定されたルートと一致しないルートに SGT タグ番号を割り当てます。

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。



第 7 章

Cisco TrustSec VRF 対応 SGT

Cisco TrustSec VRF 対応 SGT 機能は、特定の Virtual Route Forwarding（VRF）インスタンスとセキュリティグループタグ（SGT）の交換プロトコル（SXP）接続をバインドします。

VRF-Aware SXP

仮想ルーティングおよびフォワーディング（VRF）の SXP の実装は、特定の VRF と SXP 接続をバインドします。Cisco TrustSec を有効にする前に、ネットワーク トポロジがレイヤ 2 またはレイヤ 3 の VPN に対して正しく設定されており、すべての VRF が設定されていることを前提としています。

SXP VRF サポートは、次のようにまとめることができます。

- 1 つの VRF には 1 つの SXP 接続のみをバインドできます。
- 別の VRF が重複する SXP ピアまたは送信元 IP アドレス持つ可能性があります。
- 1 つの VRF で学習（追加または削除）された IP-SGT マッピングは、同じ VRF ドメインでのみ更新できます。SXP 接続は異なる VRF にバインドされたマッピングを更新できません。SXP 接続が VRF で終了しない場合は、その VRF の IP-SGT マッピングは SXP によって更新されません。
- VRF ごとに複数のアドレス ファミリがサポートされています。そのため、VRF ドメインの 1 つの SXP 接続が IPV4 および IPV6 両方の IP-SGT マッピングを転送できます。
- SXP には VRF あたりの接続数および IP-SGT マッピング数の制限はありません。

Cisco TrustSec VRF 対応 SGT の設定方法

このセクションでは、Cisco TrustSec VRF 対応 SGT の設定方法について説明します。

VRF とレイヤ 2 VLAN の割り当ての設定

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	**interface** *type number* 例： `Device(config)# interface vlan 101`	インターフェイスを設定し、インターフェイス 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	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding vrf-intf`	VRF インスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。 （注） 管理インターフェイスで VRF を設定しないでください。
ステップ 5	**exit** 例： `Device(config-if)# end`	インターフェイス 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 6	**cts role-based l2-vrf vrf1 vlan-list 20** 例： `Device(config)# cts role-based l2-vrf vrf1 vlan-list 20`	レイヤ 2 VLAN の VRF インスタンスを選択します。

	コマンドまたはアクション	目的
ステップ 7	**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。

VRF と SGT のマッピングの設定

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	**cts role-based sgt-map vrf vrf-name** {**ip4_netaddress** | *ipv6_netaddress* | **host** {*ip4_address* | *ip6_address*}} **sgt** *sgt_number* 例： `Device(config)# cts role-based sgt-map vrf red 10.0.0.3 sgt 23`	指定された VRF のパケットに SGT を適用します。 IP-SGT バインドは、指定された VRF と、IP アドレスのタイプによって示される IP プロトコルのバージョンに関連付けられた IP-SGT のテーブルに入力されます。
ステップ 4	**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 VRF 対応 SGT の設定例

このセクションでは、Cisco TrustSec VRF 対応 SGT の設定例を示します。

例：VRF とレイヤ 2 VLAN の割り当ての設定

```
Device> enable
Device# configure terminal
```

```
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf-intf
Device(config-if)# exit
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
Device(config)# end
```

例：VRF と SGT のマッピングの設定

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vrf red 23.1.1.2 sgt 23
Device(config)# end
```

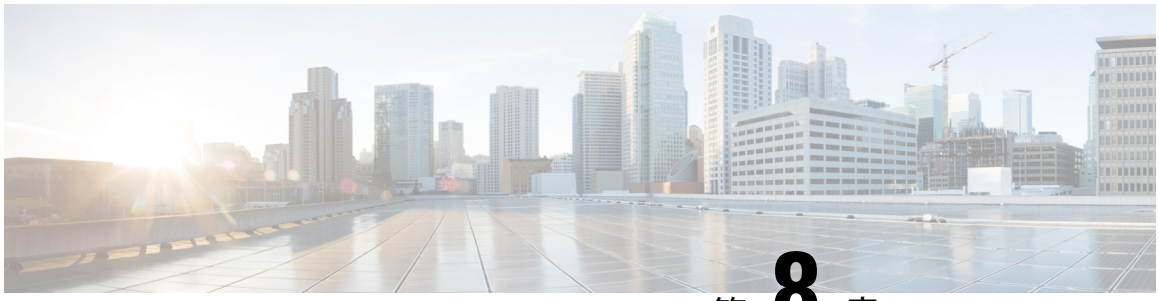
Cisco TrustSec VRF 対応 SGT の機能履歴

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 Fuji 16.9.2	Cisco TrustSec VRF 対応 SGT	Cisco TrustSec VRF 対応 SGT 機能は、SGT SXP 接続を特定の VRF インスタンスにバインドします。

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。



第 8 章

IP プレフィックスと SGT ベースの SXP フィルタリング

セキュリティグループタグ（SGT）交換プロトコル（SXP）は、Cisco TrustSec をサポートする複数のプロトコルの 1 つです。SXP は、パケットのタグ付け機能がないネットワークデバイス全体に IP と SGT のバインドの情報を伝播する、制御プロトコルです。SXP は、IP と SGT のバインドをネットワーク上の認証ポイントからアップストリームデバイスへ渡します。このプロセスにより、スイッチ、ルータ、ファイアウォールのセキュリティサービスは、アクセスデバイスから学習したユーザーアイデンティティ情報を伝えることができます。

IP プレフィックスと SGT ベースの SXP フィルタリング機能を使用すると、IP と SGT のバインドをエクスポートまたはインポートするときにフィルタリングできます。このフィルタリングは、IP プレフィックス、SGT、またはその両方の組み合わせに基づいて実行できます。

IP プレフィックスとセキュリティグループタグ（SGT）ベースのセキュリティ交換プロトコル（SXP）フィルタリングの制約事項

- アクティブデバイスとスタンバイデバイス間のセキュリティ交換プロトコル（SXP）データベースでの、IP セキュリティグループタグ（SGT）バインドのステートフルな同期のハイアベイラビリティのサポートはありません。

- 既存の接続に適用されたフィルタは、エクスポートまたはインポートされた後続のバインドでのみ有効になります。フィルタは、フィルタを適用する前にエクスポートまたはインポートされたバインドには適用されません。
- Virtual Route Forwarding（VRF）固有のフィルタリングはサポートされておらず、ピア IP に指定されたフィルタはデバイス上のすべての VRF に適用されます。
- フィルタルールの SGT 値は、単一の SGT 番号のリストになります。SGT の範囲はサポートされていません。

IP プレフィックスと SGT ベースの SXP フィルタリングに関する情報

概要

IP プレフィックスと SGT ベースの SXP フィルタリング機能を使用すると、IP と SGT のバインドをエクスポートまたはインポートするときにフィルタリングできます。このフィルタリングは、IP プレフィックス、SGT、またはその両方の組み合わせに基づいて実行できます。

セキュリティグループタグ（SGT）交換プロトコル（SXP）は、Cisco TrustSec をサポートする複数のプロトコルの 1 つです。SXP は、パケットのタグ付け機能がないネットワークデバイス全体に IP と SGT のバインドの情報を伝播する、制御プロトコルです。SXP は、IP と SGT のバインドをネットワーク上の認証ポイントからアップストリームデバイスへ渡します。このプロセスにより、スイッチ、ルータ、ファイアウォールのセキュリティサービスは、アクセスデバイスから学習したユーザーアイデンティティ情報を伝えることができます。

IP-to-SGT フィルタリングにより、システムは対象のバインドだけを選択的にインポートまたはエクスポートできます。SXP 接続では、バインドのエクスポートまたはインポート中に発生するフィルタリングに基づいて、スピーカーまたはリスナーのどちらかとして機能するデバイスにフィルタを設定できます。

双方向 SXP 接続の場合、スピーカーまたはリスナーのフィルタが設定されているかどうかに基づいて、どちらかの方向にフィルタが適用されます。ピアがスピーカーとリスナーの両方のフィルタグループの一部である場合、フィルタリングは両方向に適用されます。

フィルタは、ピアツーピアベースまたはグローバルに適用できます（すべての SXP 接続に適用可能）。どちらの場合も、フィルタはスピーカーまたはリスナーに適用できます。

フィルタ ルール

デバイスに適用する必要があるフィルタは、一連のフィルタルールを使用して作成されます。各フィルタルールは、特定の SGT 値や IP プレフィックス値を持つバインドに対して実行するアクションを指定します。各バインドは、フィルタルールで指定された値と照合されます。一致が見つかった場合は、フィルタルールで指定された対応するアクションが適用されます。選択したバインドに適用できるアクションは、許可アクションまたは拒否アクションです。IP-SGT

バインドのエクスポートまたはインポート中に、スピーカーまたはリスナーでフィルタが有効になっている場合、バインドはフィルタルールに基づいてフィルタリングされます。

フィルタリストでバインドにルールが指定されていない場合は、フィルタリストに設定されているキャッチオールルールが実行されます。キャッチオールルールがない場合、対応するバインドは暗黙的に拒否されます。

SXP フィルタリングのタイプ

IP-SGT バインドは、次のいずれかの方法でフィルタリングされます。

- SGT ベースのフィルタリング：SGT 値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。
- IP プレフィックスベースのフィルタリング：IP プレフィックス値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。
- SGT および IP プレフィックスベースのフィルタリング：SGT 値と IP プレフィックス値に基づいて SXP 接続の IP-SGT バインドをフィルタリングします。

フィルタルールは、各 IP-SGT バインドに適用されます。

IP プレフィックスと SGT ベースの SXP フィルタリングの設定方法

このセクションでは、IP-prefix と SGT-cased の SXP フィルタリングの設定方法について説明します。

SXP フィルタリストの設定

このステップでは、ルールセットを保持するフィルタリストを作成します。これらのルールは、許可されたバインドを検証し、拒否されたバインドをブロックすることによって、IP-SGT バインドをフィルタリングします。各ルールは、SGT、IP プレフィックス、または SGT と IP プレフィックスの両方の組み合わせに基づいて設定できます。

フィルタリストに特定の IP-SGT バインドと一致するルールがない場合、デフォルトまたはキャッチオールルールが定義されていない限り、バインドは暗黙的に拒否されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**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）。

	コマンドまたはアクション	目的
ステップ 2	**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 sxp filter-list** *filter-name*	Cisco TrustSec フィルタリストを設定し、フィルタリス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	*sequence-number* **permit ipv4** *ip-address/prefix* **deny sgt** *sgt-value*	フィルタリストのルールを設定します。
ステップ 5	**exit**	フィルタリスト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 6	**cts sxp filter-list** *filter-name*	Cisco TrustSec フィルタリストを設定し、フィルタリス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 7	[*sequence-number*] **deny sgt** *sgt-value* **permit ipv6** *ipv6-address/prefix*	フィルタリストのルールを設定します。
ステップ 8	**exit**	フィルタリスト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 9	**cts sxp filter-list** *filter-name*	Cisco TrustSec フィルタリストを設定し、フィルタリス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 10	[*sequence-number*] **permit ipv6** *ipv6-address/prefix* **permit** *sgt-value* **permit**	フィルタリストのルールを設定します。
ステップ 11	**end**	フィルタリスト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。

SXP フィルタグループの設定

このステップでは、ピアセットを1つのグループにまとめ、そのグループにフィルタリストを適用します。フィルタグループは、スピーカーグループまたはリスナーグループとして定義できます。すべてのスピーカーまたはすべてのリスナーに同じフィルタリストを適用するには、グローバルスピーカーのフィルタグループまたはグローバルリスナーのフィルタグループを作成します。

（注） フィルタグループにアタッチできるフィルタリストは 1 つだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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 sxp filter-group listener** *listener-name*	SXP フィルタグループのリスナーを設定し、フィルタグループ 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	**filter** *filter-list-name*	フィルタリストのルールを設定します。
ステップ 5	**peer** *ipv4-address*	ピアの IP アドレスを設定します。
ステップ 6	**exit**	フィルタグループ 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 7	**cts sxp filter-group speaker** *speaker-name*	複数の VLAN アクセス ポートで音声 VLAN を設定します。
ステップ 8	**filter** *filter-list-name*	フィルタリスト名を設定します。
ステップ 9	**peer** *ipv4-address*	ピアの IP アドレスを設定します。
ステップ 10	**end**	フィルタグループ 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。

グローバルリスナーまたはグローバルスピーカーのフィルタグループの設定

グローバルリスナーとグローバルスピーカーのフィルタグループを設定すると、リスナーモードまたはスピーカーモードのすべての SXP 接続のボックス全体にフィルタが適用されます。

フィルタグループにフィルタリストを追加すると、ボックスに現在設定されているフィルタリストのセットがヘルプストリングとして表示されます。

（注） **peer** コマンドは、グローバルリスナーとグローバルスピーカーのフィルタグループでは使用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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 sxp filter-group listener global** *filter-list-name*	グローバルリスナーのフィルタグループを設定します。
ステップ 4	**cts sxp filter-group speaker global** *filter-list-name*	グローバルスピーカーのフィルタグループを設定します。
ステップ 5	**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。

SXP フィルタリングの有効化

SXP フィルタリストとフィルタグループを設定した後は、フィルタリングを有効に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**	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**	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。

	コマンドまたはアクション	目的
ステップ 3	**cts sxp filter enable**	インターフェイスにソース テンプレートを設定します。
ステップ 4	**exit**	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。
ステップ 5	**show cts sxp filter-list** *filter_name*	デバイスに設定されているフィルタリストを、各フィルタリストのフィルタルールとともに表示します。

デフォルトルールまたはキャッチオールルールの設定

デフォルトまたはキャッチオールルールは、フィルタリスト内のどのルールとも一致しない IP-SGT バインドに適用されます。デフォルトルールが指定されていない場合、これらの IP-SGT バインドは拒否されます。

対応するフィルタリストのフィルタリスト コンフィギュレーション モードで、デフォルトまたはキャッチオールルールを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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 sxp filter-list** *filter-name*	Cisco TrustSec フィルタリストを設定し、フィルタリスト 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	**permit ipv4** *ip-address/prefix*	条件が一致した場合にアクセスを許可します。
ステップ 5	**deny ipv6** *ipv6-address/prefix*	条件に一致する場合、アクセスを拒否します。
ステップ 6	**permit sgt all**	すべての SGT に対応するバインドを許可します。

	コマンドまたはアクション	目的
ステップ 7	**end**	フィルタリスト 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。

IP プレフィックスと SGT ベースの SXP フィルタリングの設定例

このセクションでは、IP プレフィックスと SGT ベースの SXP フィルタリングの設定例を示します。

例：SXP フィルタリストの設定

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-list filter1
Device(config-filter-list)# permit ipv4 10.1.1.0/24 deny sgt 3 4
Device(config-filter-list)# exit
Device(config)# cts sxp filter-list filter2
Device(config-filter-list)# permit sgt all
Device(config-filter-list)# exit
Device(config)# cts sxp filter-list filter3
Device(config-filter-list)# deny ipv6 2001:db8::1/64 permit sgt 67
Device(config-filter-list)# end
```

例：SXP フィルタグループの設定

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-group listener group1
Device(config-filter-group)# filter filter1
Device(config-filter-group)# peer 172.16.0.1 192.168.0.1
Device(config-filter-group)# exit
Device(config)# cts sxp filter-group listener global group2
Device(config)# end
```

例：SXP フィルタリングの有効化

```
Device> enable
Device# configure terminal
Device(config)# cts sxp filter-enable
Device(config)# end
```

例：デフォルトルールまたはキャッチオールルールの設定

次に、すべての IPv4 および IPv6 アドレスに対応するバインドを許可するデフォルトのプレフィックスルールを作成する例を示します。

```
Device(config)# cts sxp filter-list filter1
Device(config-filter-list)# permit ipv4 10.0.0.0/0
Device(config-filter-list)# deny ipv6 2001:db8::1/0
```

次に、すべての SGT に対応するバインドを許可するデフォルトの SGT ルールを作成する例を示します。

```
Device(config)# cts sxp filter-list filter_1
Device(config-filter-list)# permit sgt all
```

IP プレフィックスと SGT ベースの SXP フィルタリングの確認

設定を確認するには、次のコマンドを使用します。

debug cts sxp filter events コマンドは、フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録するために使用されます。このコマンドは、フィルタリングプロセスの一致アクションに関連するイベントをキャプチャするためにも使用されます。

```
Device# debug cts sxp filter events
```

次に、SXP スピーカーのフィルタグループを表示する **show cts sxp filter-group speaker** コマンドの出力例を示します。

```
Device# show cts sxp filter-group speaker group1
   Filter-group: group1
   Filter-name: filter1
   Peer-list: 172.16.0.1 192.168.0.1
```

次に、SXP スピーカーのリスナーグループを表示する **show cts sxp filter-group listener** コマンドの出力例を示します。

```
Device# show cts sxp filter-group listener

Global Listener Filter: Not configured
   Filter-group: group1
   Filter-name: filter1
   Peer-list: 172.16.0.1 192.168.0.1
   Filter-group: group2
   Filter-name: filter1
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

次に、SXP スピーカーのフィルタグループに関する詳細情報を表示する **show cts sxp filter-group speaker detailed** コマンドの出力例を示します。

```
Device# show cts sxp filter-group speaker group1 detailed

   Filter-group: group1
   Filter-name: filter1
   Filter-rules:
      10 deny sgt 30
      20 deny prefix 10.1.0.0/16
      30 permit sgt 60-100
   Peer-list: 172.16.0.1 192.168.0.1
```

次に、設定されたすべてのフィルタグループに関する情報を表示する **show cts sxp filter-group** コマンドの出力例を示します。

```
Device# show cts sxp filter-group

Global Listener Filter: Not configured

Global Speaker Filter: Not configured

Listener Group:
   Filter-group: group1
   Filter-name: filter1
   Peer-list: 172.16.0.1 192.168.0.1
   Filter-group: group2
   Filter-name: filter1
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1

Speaker Group:
   Filter-group: group3
   Filter-name: filter1
   Peer-list: 172.16.0.1 192.168.0.13
   Filter-group: group2
   Filter-name: filter1
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

次に、設定されたすべての SXP フィルタグループに関する詳細情報を表示する **show sxp filter-group detailed** コマンドの出力例を示します。

```
Device# show cts sxp filter-group detailed

Global Listener Filter: Configured
   Filter-name: global1
   Filter-rules:
      10 deny 192.168.0.13/32
      20 deny sgt 100-200

Global Speaker Filter: Configured
   Filter-name: global2
   Filter-rules:
      10 deny 192.168.0.13/32
      20 deny sgt 100-200

Listener Group:
   Filter-group: group1
   Filter-name: filter1
   Filter-rules:
```

```
      10 deny sgt 30
      20 deny prefix 172.16.0.0/16
      30 permit sgt 60-100
   Peer-list: 172.16.0.1, 192.168.0.13

   Filter-group: group2
   Filter-name: filter1
   Filter-rules:
      10 deny sgt 30
      20 deny prefix 172.16.0.0/16
      30 permit sgt 60-100
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1

Speaker Group
   Filter-group: group3
   Filter-name: filter1
   Filter-rules:
      10 deny sgt 30
      20 deny prefix 172.16.0.0/16
      30 permit sgt 60-100
   Peer-list: 10.10.10.1, 172.16.0.1, 192.168.0.13

   Filter-group: group2
   Filter-name: filter1
   Filter-rules:
      10 deny sgt 30
      20 deny prefix 172.16.0.0/16
      30 permit sgt 60-100
   Peer-list: 192.0.2.1, 198.51.100.1, 203.0.113.1
```

SXP フィルタリングの syslog メッセージ

SXPフィルタリングのsyslogメッセージは、フィルタリングに関連するさまざまなイベントを示すために生成されます。

フィルタルールの syslog メッセージ

単一のフィルタに設定できるルールの最大数は 128 です。単一のフィルタに設定されているフィルタルールの数が制限の 20% 増加するたびに、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in
filter [filter-name].
```

単一のフィルタに設定されているルールの数が、フィルタリストに許可されているルールの最大数の 95% に達すると、次のメッセージが生成されます。

```
CTS SXP filter rules exceed [ ] threshold. Reached count of [count] out of [max] in
filter [filter-name].
```

次のメッセージは、単一のフィルタで設定されたルールの数が許可されたルールの最大数に達し、それ以上ルールを追加できない場合に生成されます。

```
Reached maximum filter rules. Could not add new rule in filter [filter-name]
```

フィルタリストの syslog メッセージ

設定できるフィルタリストの最大数は256です。設定されているフィルタリストの数がこの制限の 20% 増加するたびに、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max] in
filter [filter-name].
```

設定されているフィルタリストの数が、許可されたフィルタリストの最大数の 95% に達すると、次のメッセージが生成されます。

```
CTS SXP filter rules exceed %[ ] threshold. Reached count of [count] out of [max]
```

次のメッセージは、設定されているフィルタリストの数が許可されたフィルタリストの最大数に達し、それ以上フィルタリストを追加できない場合に生成されます。

```
Reached maximum filter count. Could not add new filter
```

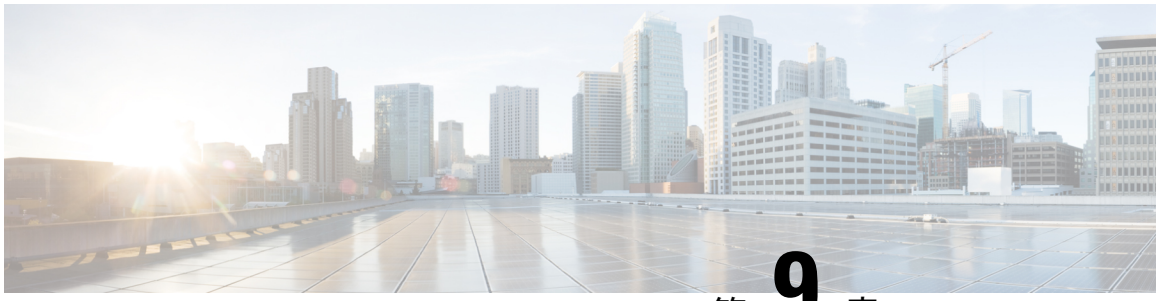
IP プレフィックスと SGT ベースの SXP フィルタリングの機能履歴

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 Fuji 16.9.2	IP プレフィックスと SGT ベースの SXP フィルタリング	IP プレフィックスと SGT ベースの SXP フィルタリング機能は、高い IP-SGT バインドの拡張性の問題を解決するためのフィルタリングメカニズムを提供します。

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。



第 9 章

Cisco TrustSec フィールドの Flexible NetFlow エクスポート

Cisco TrustSec フィールドの Flexible NetFlow エクスポート

Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、Flexible Netflow（FNF）フローレコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニター、トラブルシューティング、および特定を支援します。

このモジュールでは、Cisco TrustSec と FNF のインタラクションについてと、NetFlow バージョン 9 フロー レコードの Cisco TrustSec フィールドを設定しエクスポートする方法を説明します。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの制約事項

- FNF レコードでエクスポートされるセキュリティグループタグ（SGT）値は、次のシナリオでは 0 になります。
  - 対応するパケットは、信頼されたインターフェイスから、0 の SGT 値とともに受信します。
  - 対応するパケットは SGT なしで受信します。
  - IP-SGT ルックアップ中に SGT が検出されません。（パケットが SGT なしで受信されるため、SGT は同じパケット内に見つかりません）。
  - フローレコードに SGT と接続先グループタグ（DGT）のフィールド（またはこの 2 つのどちらかのフィールドだけ）が含まれる場合、両方の値を適用できないとしても、SGT と DGT に値 0 を設定したフローが作成されます。フロー レコードには、SGT および DGT フィールドと一緒に、送信元および宛先 IP アドレスが含まれる必要があります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートに関する情報

Flexible NetFlow の Cisco TrustSec フィールド

FNF フローレコード内の Cisco TrustSec フィールド、送信元 SGT および宛先 DGT は、管理者によるフローとアイデンティティ情報の関連付けに役立ちます。ネットワークエンジニアは、これにより、顧客がネットワークリソースおよびアプリケーションリソースをどのように利用しているかついて詳しく理解できます。この情報を使用して、潜在的なセキュリティやポリシーの違反を検出して解決するために、アクセスおよびアプリケーションリソースを効率的に計画して割り当てることができます。

Cisco TrustSec フィールドは入力/出力 FNF、ユニキャスト/マルチキャスト トラフィックでサポートされています。

次のテーブルに、Cisco TrustSec 用の NetFlow バージョン 9 の企業固有フィールドタイプを示します。これは、Cisco TrustSec の送信元/宛先 SGT の FNF テンプレートで使用されます。

フローフィールドタイプ	説明
CTS_SRC_GROUP_TAG	Cisco TrustSec 送信元 SGT
CTS_DST_GROUP_TAG	Cisco TrustSec 宛先 SGT

FNF フローレコードで既存の一致するフィールドに加えて、Cisco TrustSec フィールドが設定されます。次の設定を使用して、Cisco TrustSec フローオブジェクトをキーフィールドまたは非キーフィールドとして FNF フローレコードに追加し、パケット用の送信元と宛先の SGT を設定します。

match flow cts {source | destination} group-tag コマンドは、キーフィールドとして Cisco TrustSec フィールドを指定するため、対応するフローレコード以下で設定されます。キーフィールドはフローを差別化するものです。各フローには、一連の一意の値が設定されています。フローレコードをフローモニターで使用するには、1 つ以上のキーフィールドが必要になります。送信元 SGT、宛先 SGT、またはその両方に同時に **match** コマンドを設定できます。

フローレコードは、フローモニター下で設定され、フローモニターはインターフェイスに適用されます。FNF データをエクスポートするには、フロー エクスポータを設定し、フロー モニター以下に追加する必要があります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定方法

次のセクションでは、Cisco TrustSec フィールドの FNF エクスポートを構成するさまざまなタスクについて説明します。

フロー レコードのキー フィールドとしての Cisco TrustSec フィールドの設定

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	**flow record** *record-name* 例： `Device(config)# flow record cts-record-ipv4`	FNF フローレコードを作成するか、または既存の FNF フローレコードを変更して、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。 • このコマンドでは、既存のフローレコードを変更することもできます。
ステップ 4	**match ipv4 protocol** 例： `Device(config-flow-record)# match ipv4 protocol`	（任意）フローレコードのキーフィールドとして IPv4 プロトコルを設定します。
ステップ 5	**match ipv4 source address** 例： `Device(config-flow-record)# match ipv4 source address`	（任意）IPv4 送信元アドレスをフローレコードのキーフィールドとして設定します。
ステップ 6	**match ipv4 destination address** 例： `Device(config-flow-record)# match ipv4 destination address`	（任意）IPv4 宛先アドレスをフローレコードのキーフィールドとして設定します。
ステップ 7	**match transport source-port** 例： `Device(config-flow-record)# match transport source-port`	（オプション）フロー レコードのキーフィールドとして、トランスポート送信元ポートを設定します。

	コマンドまたはアクション	目的
ステップ 8	**match transport destination-port** 例： `Device(config-flow-record)# match transport destination-port`	（オプション）フロー レコードのキー フィールドとして、トランスポート宛先ポートを設定します。
ステップ 9	**match flow direction** 例： `Device(config-flow-record)# match flow direction`	（オプション）フローがモニターされる方向をキーフィールドとして設定します。

ステップ 10	**match flow cts** {**source** | **destination**} **group-tag**
	例：
	`Device(config-flow-record)# match flow cts source group-tag`
	`Device(config-flow-record)# match flow cts destination group-tag`
		FNF フローレコード内のレコードのキーフィールドとして、Cisco TrustSec の送信元グループタグまたは接続先グループタグを設定します。
		• 入力：
		• 着信パケットでは、ヘッダーがある場合、SGT にはヘッダーと同じ値が反映されます。値がない場合は、0 が示されます。
		• DGT 値は入力ポートの SGACL 設定に依存しません。
		• 出力：
		• **propagate-sgt** コマンドまたは Cisco TrustSec のどちらかが出力インターフェイス上で無効化されていると、SGT は 0 になります。
		• 発信パケットで、SGT または DGT に対応する SGACL 設定が存在すれば、DGT は 0 以外の数値になります。
		• SGACL が出力ポートまたは VLAN で無効化されているか、またはグローバル SGACL の適用を無効化されている場合、DGT は 0 になります。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Device(config-flow-record)# end`	Flexible NetFlow フロー レコード コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

NetFlow での SGT 名のエクスポートの設定

フローエクスポータごとに、1 つの宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフロー エクスポータを設定してフロー モニターに割り当てる必要があります。

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	**flow exporter** *exporter-name* 例： `Device(config)# flow exporter EXPORTER-1`	フロー エクスポータを作成するか、または既存のフロー エクスポータを変更して、Flexible NetFlow フロー エクスポータ 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	**destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*] 例： `Device(config-flow-exporter)# destination 172.16.10.2`	エクスポータの宛先システムの IP アドレスまたはホスト名を指定します。
ステップ 5	**option cts-sgt-table** [**timeout** *seconds*] 例： `Device(config-flow-exporter)# option cts-sgt-table timeout 1200`	エクスポータの SGT ID-to-name テーブルオプションを選択します。 • このオプションにより、FNF は SGT をセキュリティグループ名にマッピングする Cisco TrustSec 環境データ テーブルをエクスポートできます。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-flow-exporter)# end`	Flexible NetFlow フロー エクスポータ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

Cisco TrustSec フィールドの Flexible NetFlow エクスポートの設定例

次のセクションでは、Cisco TrustSec フィールドの FNF エクスポートの設定に関する例を示します。

例：フロー レコードのキー フィールドとしての Cisco TrustSec フィールドの設定

次の例は、Cisco TrustSec フロー オブジェクトを、IPv4 Flexible NetFlow フロー レコードのキー フィールドとして設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow record cts-record-ipv4
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match flow direction
Device(config-flow-record)# match flow cts source group-tag
Device(config-flow-record)# match flow cts destination group-tag
Device(config-flow-record)# end
```

例：NetFlow での SGT 名のエクスポートの設定

次に、NetFlow で SGT 名のエクスポートを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# flow exporter EXPORTER-1
Device(config-flow-exporter)# destination 172.16.10.2
Device(config-flow-exporter)# option cts-sgt-table timeout 1200
Device(config-flow-exporter)# end
```

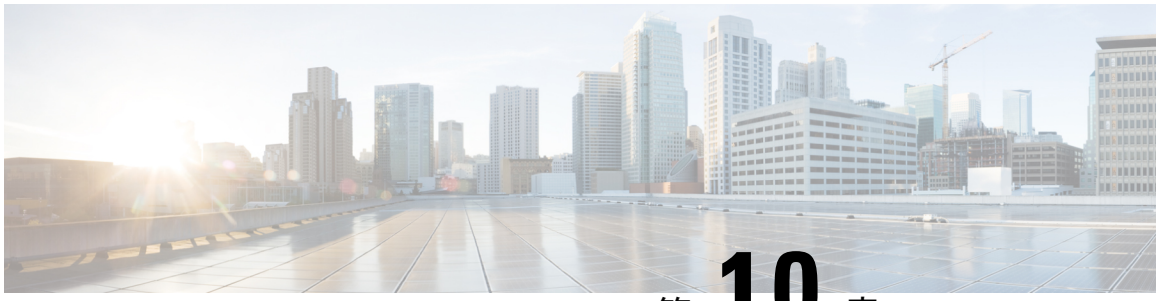
Cisco TrustSec フィールドの Flexible NetFlow エクスポートの機能履歴

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 Fuji 16.9.2	Cisco TrustSec フィールドの Flexible NetFlow エクスポート	Cisco TrustSec フィールドの Flexible NetFlow エクスポートでは、FNF フローレコード内の Cisco TrustSec フィールドをサポートし、Cisco TrustSec 導入の標準から外れた動作のモニター、トラブルシューティング、および特定を支援します。

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。



第 10 章

SGT インライン タギングの設定

SGT インラインタギングの制約事項

- Cisco TrustSec の手動設定と 802.1x 設定は共存できません。

SGT インラインタギングに関する情報

Cisco TrustSec ドメイン内の各セキュリティ グループは、セキュリティグループタグ（SGT）と呼ばれる一意の 16 ビットタグが割り当てられます。SGT はネットワーク全体で送信元の権限を示す単一ラベルです。これは、ネットワーク ホップ間で順番に伝搬され、任意の中間デバイス（スイッチ、ルータ）はこれによってアイデンティティ タグに基づいたポリシーを適用できます。

Cisco TrustSec 対応デバイスには、MAC（L2）レイヤ内に組み込まれた SGT を持つパケットを送受信できる、ハードウェア機能が組み込まれています。この機能は、レイヤ 2 （L2）-SGT インポジションと呼ばれます。この機能により、デバイスのイーサネットインターフェイスで L2-SGT インポジションを有効にできるため、そのデバイスはネクスト ホップ イーサネット ネイバーに伝送されるパケット内に SGT を挿入できるようになります。SGT-over-Ethernet は、クリアテキスト（非暗号化）イーサネットパケットに組み込まれた SGT のホップバイホップの伝達方式です。インラインアイデンティティ伝達はスケーラブルで、ほぼラインレートのパフォーマンスを提供し、コントロールプレーンのオーバーヘッドを防ぎます。

Cisco TrustSec SGT Exchange Protocol V4（SXPv4）機能は、Cisco TrustSec メタデータベースの L2-SGT をサポートします。パケットが Cisco TrustSec 対応インターフェイスに入力されると、IP-SGT マッピングデータベース（SXP によって構築されたダイナミックエントリや設定コマ

ンドによって構築されたスタティックエントリがある）が分析され、パケットの送信元 IP アドレスに対応する SGT が学習されます。この SGT はパケットに挿入され、Cisco TrustSec ヘッダー内でネットワーク全体に運ばれます。

このタグは、送信元のグループを表しているので、送信元グループ タグ（SGT）としても参照されます。ネットワークの出力エッジでは、パケットの宛先に割り当てられたグループが既知になります。この時点で、アクセス制御を適用できます。Cisco TrustSec を使用すると、セキュリティ グループ アクセス コントロール リスト（SGACL）と呼ばれるアクセス コントロール ポリシーがセキュリティグループ間で定義されます。任意のパケットから見れば、SGACL は単純にセキュリティグループから送信され、別のセキュリティグループに送信されています。

信頼されるインターフェイスからのパケット内で受信した SGT タグはネットワークに伝播され、アイデンティティ ファイアウォールの分類にも使用されます。IPSec サポートが追加される場合は、受信した SGT タグは SGT タギング用の IPSec と共有されます。

Cisco TrustSec クラウドの入口のネットワーク デバイスは、Cisco TrustSec クラウドにパケットを転送する際に、パケットに SGT をタグ付けできるように、Cisco TrustSec クラウドに入るパケットの SGT を判断する必要があります。パケットの SGT は次の方法で判断できます。

- Cisco TrustSec ヘッダーの SGT フィールド：パケットを信頼されたピアデバイスから受信している場合は、Cisco TrustSec ヘッダーは正しい SGT フィールドを運んでいることを前提としています。この状況は、そのパケットにとって、そのネットワークが Cisco TrustSec クラウド内の最初のネットワークデバイスではない場合に適用されます。
- 送信元 IP アドレスに基づいた SGT ルックアップ：この場合、送信元 IP アドレスに基づいてパケットの SGT を決定するポリシーを、管理者が手動で設定できます。IP アドレスから SGT へのテーブルも、SXP プロトコルによって入力できます。

ユニキャスト送信元 IPv6 アドレスを持つ IPv6 マルチキャストトラフィックに対する L2 インラインタギングがサポートされています。

NAT 対応デバイスでの SGT インラインタギング

次のシナリオでは、入力ポートと出力ポートの両方でネットワークアドレス変換（NAT）が有効化されているプライマリデバイスから、セカンダリデバイスに流れるパケットの SGT の決定方法について説明します。

（注） フローに使用されるすべてのポートには **CTS manual** があり、両方のデバイスで信頼され、設定されている必要があります。

- 両方のデバイス間でインラインタギングが有効化されており、SGT タグが CLI で変更されていない場合：

  この場合、プライマリデバイスでは Cisco TrustSec がパケットの送信元 IP に対応する SGT タグに適用されます。同じ SGT タグが NAT IP にタグ付けされます。セカンダリデバイスでは、パケットの送信元 IP に対応する SGT タグにも Cisco TrustSec が適用されます。

SGT インライン タギングの設定

たとえば、送信元 IP 192.0.2.5 および SGT タグ 133 を持つパケットがプライマリデバイスで受信されます。Cisco TrustSec は、プライマリデバイスの SGT タグ 133 に適用されます。NAT 変換後、パケットの IP は 198.51.100.10 に変更され、SGT タグ 133 にタグ付けされます。セカンダリデバイスでは、パケットは IP アドレス 198.51.100.10 および SGT タグ 133 で受信されます。Cisco TrustSec は、セカンダリデバイスで SGT タグ133を使用して適用されます。

- 両方のデバイス間でインラインタギングが有効になっており、SGTタグがCLIで変更されている場合：

  この場合、プライマリデバイスでは Cisco TrustSec がパケットの送信元 IP に対応する SGT タグに適用されます。SGT タグは CLI によって変更されますが、パケットの送信元 IP に対応する SGT タグは、パケットの NAT IP にタグ付けされます。セカンダリデバイスでは、パケットの送信元 IP に対応する SGT タグにも Cisco TrustSec が適用されます。

  たとえば、送信元 IP 192.0.2.5 および SGT タグ 133 を持つパケットがプライマリデバイスで受信されます。Cisco TrustSec は、プライマリデバイスの SGT タグ 133 に適用されます。SGT タグは CLI で 200 に変更されます。NAT 変換後、パケットの IP は 198.51.100.10 に変更されます。ただし、SGT タグ 133 にタグ付けされます。セカンダリデバイスでは、パケットは IP アドレス 198.51.100.10 および SGT タグ 133 で受信されます。Cisco TrustSec は、セカンダリデバイスで SGT タグ133 に適用されます。

- インラインタギングが無効化されており（SGT がセカンダリデバイスの SXP プロトコルを介して入力されている）、SGT タグが CLI で変更されている場合：

  この場合、プライマリデバイスでは Cisco TrustSec がパケットの送信元 IP に対応する SGT タグに適用されます。NAT 後の IP への SGT は CLI を介して定義され、プライマリデバイスで学習されます。プライマリデバイスとセカンダリデバイス間に Cisco TrustSec の直接リンクが存在せず、IP と SGT のバインディングがセカンダリデバイスの SXP を通じて学習される場合、セカンダリデバイスでは、NAT IP に対応する SGT タグに Cisco TrustSec が適用されます。

  たとえば、送信元 IP 192.0.2.5 および SGT タグ 133 を持つパケットがプライマリデバイスで受信されます。NAT 変換後、送信元 IP は 198.51.100.10 に変更され、SGT は CLI を介して 200 として定義されます。Cisco TrustSec は、プライマリデバイスの SGT タグ 133 に適用されます。セカンダリデバイスでは、IP から SGT へのバインディングが SXP 経由で受信され、セカンダリデバイスの SGT タグ 200 に Cisco TrustSec が適用されます。

SGT インライン タギングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

SGT インライン タギングの設定

	コマンドまたはアクション	目的
	`Device> enable`	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	**interface** {**gigabitethernet port** | **vlan number**} 例： `Device(config)# interface gigabitethernet 1/0/1`	Cisco TrustSec SGT 認証と転送が有効化されるようにインターフェイスを設定し、インターフェイス 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	**cts manual** 例： `Device(config-if)# cts manual`	インターフェイスで Cisco TrustSec SGT 認証と転送を有効化し、Cisco TrustSec 手動インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**propagate sgt** 例： `Device(config-if-cts-manual)# propagate sgt`	インターフェイスでの Cisco TrustSec SGT 伝達を有効化します。 （注） このコマンドは、ピア デバイスで SGT over Ethernet パケットを受信できない状況（つまり、ピア デバイスが Cisco Ethertype CMD 0x8909 フレーム形式をサポートしない場合）で使用します。
ステップ 6	**policy static sgt** *tag* [**trusted**] 例： `Device(config-if-cts-manual)# policy static sgt 77 trusted`	インターフェイスでスタティック SGT 入力 ポリシーを設定し、インターフェイスで受信する SGT の信頼性を定義します。

	コマンドまたはアクション	目的
		（注） **trusted** キーワードは、そのインターフェイスが Cisco TrustSec に信頼されていることを示します。このインターフェイス上のイーサネットパケット内で受信した SGT 値は信頼され、デバイスによって任意の SG 認識型ポリシーの適用または出力タギングに使用されます。
ステップ 7	**end** 例： `Device(config-if-cts-manual)# end`	Cisco TrustSec 手動インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

例：SGT 静的インラインタギングの設定

この例では、デバイスのインターフェイスで L2-SGT タギングまたはインポジションを有効にして、インターフェイスが Cisco TrustSec に信頼されるかどうかを定義する方法を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# cts manual
Device(config-if-cts-manual)# propagate sgt
Device(config-if-cts-manual)# policy static sgt 77 trusted
```

SGT インラインタギングの機能の履歴

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 Fuji 16.9.2	SGTインライン タギング	Cisco TrustSec ドメイン内の各セキュリティグループは、SGT と呼ばれる一意の 16 ビットタグが割り当てられます。SGT はネットワーク全体で送信元の権限を示す単一ラベルです。

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。

第 11 章

エンドポイントアドミッションコントロールの設定

このモジュールでは、TrustSec ネットワークでの認証および許可のためのエンドポイント アドミッション コントロール（EAC）のアクセス方式について説明します。

エンドポイント アドミッション コントロールの概要

TrustSec ネットワークでは、パケットはネットワークへの入力ではなく出力でフィルタリングされます。TrustSec エンドポイント認証では、TrustSec ドメイン（エンドポイントの IP アドレス）にアクセスするホストは DHCP スヌーピングおよび IP デバイス トラッキングによってアクセス デバイスでセキュリティ グループ タグ（SGT）に関連付けられます。アクセスデバイスは、継続的に更新される送信元 IP と SGT のバインディングテーブルを維持する TrustSec ハードウェア対応出力のデバイスに、SXP 経由でそのアソシエーション（バインド）を送信します。パケットは、セキュリティグループ ACLS（SGACL）を適用することにより、TrustSec ハードウェア対応デバイスによって出力でフィルタリングされます。

認証および許可のためのエンドポイント アドミッション コントロール（EAC）アクセス方式には、次のものがあります。

- 802.1X ポートベースの認証
- MAC 認証バイパス（MAB）

- Web 認証（WebAuth）

すべてのポートベース認証は、authentication コマンドでイネーブルにできます。各アクセス方式はポート単位で個別に設定する必要があります。複数の認証モードが設定され、アクティブ方式が失敗すると柔軟な認証シーケンスおよびフェールオーバー機能により管理者は、フェールオーバーおよびフォールバック シーケンスを指定することができます。802.1X ホスト モードは、802.1X ポートごとに接続できるエンドポイントのホスト数を決定します。

例：Example: 802.1X 認証の設定

次に、ギガビット イーサネット ポートでの基本的な 802.1x の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# dot1x system-auth-control
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# dot1x pae authenticator
```

例：MAC 認証バイパスの設定

MAC 認証バイパス（MAB）は 802.1X 対応ではないホストまたはクライアントが 802.1X をイネーブルにしたネットワークに参加できるようにします。MAB をイネーブルにする前に、802.1X 認証をイネーブルにする必要はありません。

次の例では、基本的な MAB 設定の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# mab
```

MAB 認証の設定の詳細については、アクセスデバイスのコンフィギュレーション ガイドを参照してください。

例：Web 認証プロキシの設定

Web 認証プロキシ（WebAuth）は、ユーザーが Web ブラウザを使用して、アクセス デバイスの Cisco IOS Web サーバー経由で Cisco Secure ACS にログイン クレデンシャルを送信できるようにするものです。WebAuth は独立してイネーブルにできます。これは、802.1X または MAB の設定は必要ではありません。

次の例では、ギガビット イーサネット ポートでの基本的な WebAuth 設定の例を示します。

```
Device(config)# ip http server
Device(config)# ip access-list extended POLICY
Device(config-ext-nacl)# permit udp any any eq bootps
Device(config-ext-nacl)# permit udp any any eq domain
Device(config)# ip admission name HTTP proxy http
Device(config)# fallback profile FALLBACK_PROFILE
Device(config-fallback-profile)# ip access-group POLICY in
Device(config-fallback-profile)# ip admission HTTP
Device(config)# interface GigabitEthernet2/1
Device(config-if)# authentication port-control auto
Device(config-if)# authentication fallback FALLBACK_PROFILE6500(config-if)#ip access-group
POLICY in
```

例：Flexible Authentication（FlexAuth; フレキシブル認証）シーケンスおよびフェールオーバー コンフィギュレーション

Flexible Authentication（FlexAuth; フレキシブル認証）シーケンス（FAS）を使用すると、802.1X、MAB、および WebAuth 認証方式用にアクセスポートを設定でき、1 つ以上の認証方式が使用できない場合にフォールバックシーケンスを指定できます。デフォルトのフェールオーバーシーケンスは次のとおりです。

- 802.1X ポートベースの認証
- MAC 認証バイパス
- Web 認証

レイヤ 2 認証はレイヤ 3 の認証前に常に実行されます。つまり、802.1X と MAB は WebAuth の前に発生する必要があります。

次の例では、MAB、dot1X および WebAuth の順で認証シーケンスを指定します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 2/1
Device(config-if)# authentication order mab dot1x webauth
Device(config-if)# ^Z
```

FAS の詳細については、『Flexible Authentication Order, Priority, and Failed Authentication』を参照してください。

802.1X ホスト モード

ポート単位で 4 種類の分類モードを設定できます。

- Single Host：1 個の MAC アドレスを持つインターフェイス ベースのセッション

- Multi Host：ポートごとに複数の MAC アドレスを持つインターフェイス ベースのセッション
- Multi Domain：MAC + ドメイン（VLAN）セッション
- Multi Auth：ポートごとに複数の MAC アドレスを持つ MAC ベースのセッション

認証前オープン アクセス

認証前オープンアクセス機能は、ポートの認証の実行前に、クライアントとデバイスがネットワーク アクセスを取得できるようにするものです。このプロセスが主に、PXE がタイムアウトする前にデバイスがネットワークにアクセスし、サプリカントが含まれる可能性のあるブート可能イメージをダウンロードする必要がある PXE のブートのシナリオで必要です。

例：DHCP スヌーピングおよび SGT の割り当て

認証プロセス後は、デバイス認証が発生します（たとえば、ダイナミック VLAN 割り当て、ACL プログラミングなど）。TrustSec ネットワークの場合、セキュリティ グループ タグ（SGT）は Cisco ACS のユーザー コンフィギュレーションごとに割り当てられます。SGT はそのエンドポイントから DHCP スヌーピングおよび IP デバイス トラッキング インフラストラクチャを使用して送信されたトラフィックにバインドされます。

次の例では、アクセスデバイスで DHCP スヌーピングおよび IP デバイストラッキング を有効にします。

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip dhcp snooping
Device(config)# ip dhcp snooping vlan 10
Device(config)# no ip dhcp snooping information option
Device(config)# ip device tracking
```

エンドポイントアドミッションコントロールの機能履歴

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 Fuji 16.9.2	エンドポイントアドミッション コントロール	Cisco TrustSec ネットワークでは、パケットはネットワークへの入力ではなく出力でフィルタリングされます。Cisco TrustSec エンドポイント認証では、Cisco TrustSec ドメイン（エンドポイントの IP アドレス）にアクセスするホストは DHCP スヌーピングおよび IP デバイストラッキングによってアクセスデバイスで SGT に関連付けられます。

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。