



レイヤ 2 SGT インポジションと転送

- [レイヤ 2 SGT インポジションと転送の機能履歴, on page 1](#)
- [レイヤ 2 SGT インポジションと転送, on page 1](#)
- [レイヤ 2 SGT インポジションと転送を設定するためのガイドライン, on page 2](#)
- [SGT 処理の設定方法: L2 SGT インポジションと転送, on page 2](#)

レイヤ 2 SGT インポジションと転送の機能履歴

次の表に、このモジュールで説明する機能のリリース情報とプラットフォームサポート情報を示します。

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	機能名と説明	サポートされるプラットフォーム
Cisco IOS XE 17.18.1	レイヤ 2 SGT インポジションと転送: レイヤ 2 SGT インポジションと転送を使用すると、スイッチ上のインターフェイスを Cisco TrustSec 用に手動で設定することが可能になり、スイッチが SGT をネットワークパケットに挿入できるようになります。	Cisco C9610 シリーズ スマートスイッチ

レイヤ 2 SGT インポジションと転送

レイヤ 2 SGT インポジションと転送機能を使用すると、スイッチ上のインターフェイスを Cisco TrustSec 用に手動で設定することが可能になり、スイッチが SGT をネットワークパケットに挿入できるようになります。SGT は Cisco TrustSec ヘッダーでネットワーク全体に伝送されるため、

インフラストラクチャ全体での一貫したセキュリティ グループ ポリシーの適用が可能になります。

レイヤ 2 SGT インポジションと転送を設定するためのガイドライン

L2 SGT インポジションと転送の機能を導入する前に、次の前提条件で Cisco TrustSec ネットワークを確立する必要があります。

- 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。
- Cisco Secure Access Control System (ACS) 5.1 が、Cisco Trustsec -SXP ライセンスで動作していること
- ディレクトリ、DHCP、DNS、認証局、および NTP サーバーがネットワーク内で機能すること。
- ルータごとに、それぞれ異なる `retry open timer` コマンドの値を設定してください。

SGT 処理の設定方法: L2 SGT インポジションと転送

以下のセクションでは、SGT 処理: L2 SGT インポジションと転送に関する設定情報を提供します。

インターフェイスでのレイヤ 2 SGT のインポジションと転送の有効化

次のタスクを実行して、Cisco TrustSec のデバイス上のインターフェイスを手動で有効化します。これによりデバイスは、ネットワーク全体で伝達するパケットに SGT を追加し、静的認証ポリシーを導入できます。

Procedure

Step 1 enable

Example:

```
Device# enable
```

特権 EXEC モードを有効にします。

プロンプトが表示されたらパスワードを入力します。

Step 2 configure terminal

Example:

```
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。

Step 3 **interface {GigabitEthernet port | Vlan number}**

Example:

```
Device(config)# interface gigabitethernet 0
```

CTS SGT の認証と転送が有効なインターフェイスを開始します。

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

CTS SGT 認証と転送のインターフェイスを有効化し、CTS 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。

Step 5 **policy static sgt tag [trusted]**

Example:

```
Device(config-if-cts-manual)# policy static sgt 100 trusted
```

SGT の信頼性を定義するタグ付きパケットを使用して、CTS セキュリティ グループのスタティック認証ポリシーを設定します。

Step 6 **end**

Example:

```
Device(config-if-cts-manual)# end
```

CTS 手動インターフェイス構成モードを終了し、特権 EXEC モードを開始します。

Step 7 **show cts interface [GigabitEthernet port | Vlan number | brief | summary]**

Example:

```
Device# show cts interface brief
```

インターフェイスの CTS 設定の統計情報を表示します。

インターフェイスでの CTS SGT 伝達の無効化

ピアデバイスがSGTを受信できない場合、次の手順を実行して、インスタンス内のインターフェイスで CTS SGT 伝達を無効化します。

Procedure

Step 1 **enable**

Example:

```
Device# enable
```

特権 EXEC モードを有効にします。

プロンプトが表示されたらパスワードを入力します。

Step 2 **configure terminal**

Example:

```
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。

Step 3 **interface {GigabitEthernet port | Vlan number}**

Example:

```
Device(config)# interface gigabitethernet 0
```

CTS SGT の認証と転送が有効なインターフェイスを開始します。

Step 4 **cts manual**

Example:

```
Device(config-if)# cts manual
```

CTS SGT の承認と転送用のインターフェイスを有効化します。

CTS 手動インターフェイス コンフィギュレーションモードは、CTS パラメーターを設定できる場合に開始されます。

Step 5 **no propagate sgt**

Example:

```
Device(config-if-cts-manual)# no propagate sgt
```

ピア デバイスが SGT を受信できない状況では、インターフェイスの CTS SGT 伝達を無効化します。

Note

CTS SGT 伝達はデフォルトで有効化されています。ピアデバイスで CTS SGT 伝達を再度オンにする必要がある場合、**propagate sgt** コマンドを使用できます。

no propagate sgt コマンドが入力されると、SGT タグは L2 ヘッダーに追加されなくなります。

Step 6 **end**

Example:

```
Device(config-if-cts-manual)# end
```

CTS 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。

Step 7 **show cts interface [GigabitEthernet port | Vlan number | brief | summary]**

Example:

```
Device# show cts interface brief
```

インターフェイスで CTS SGT 伝達が無効化されていることを確認するため、CTS 設定の統計情報を表示します。

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。