



Cisco TrustSec インターフェイスと SGT のマッピング

Cisco TrustSec インターフェイスと SGT のマッピング機能は、レイヤ 3 入力インターフェイス上のすべてのトラフィックを、セキュリティグループタグ (SGT) にバインドします。このマッピングを実装すると、Cisco TrustSec では、SGT を使用してさまざまな論理レイヤ 3 入力インターフェイスからトラフィックを分離できるようになります。

- [Cisco TrustSec インターフェイスと SGT のマッピングに関する情報 \(1 ページ\)](#)
- [Cisco TrustSec インターフェイスと SGT のマッピングの設定方法 \(2 ページ\)](#)
- [Cisco TrustSec インターフェイスと SGT のマッピングの設定例 \(4 ページ\)](#)
- [Cisco TrustSec インターフェイスと SGT のマッピングに関する追加情報 \(5 ページ\)](#)
- [Cisco TrustSec インターフェイスと SGT のマッピングの機能情報 \(6 ページ\)](#)

Cisco TrustSec インターフェイスと SGT のマッピングに関する情報

インターフェイスと SGT のマッピング

インターフェイスとセキュリティグループタグ (SGT) 間のマッピングを使用して、基盤となる物理インターフェイスに関わらず、SGT を次の論理レイヤ 3 入力インターフェイスいずれかのトラフィックにマッピングします。

- レイヤ 3 (ルーテッド) イーサネット インターフェイス
- レイヤ 3 (ルーテッド) イーサネット 802.1Q サブインターフェイス
- トンネル インターフェイス

設定された SGT タグは、レイヤ 3 入力インターフェイスのすべてのトラフィックに割り当てられ、インライン タギングとポリシーの適用に使用できます。

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（IP アドレスからセキュリティ グループ タグへ）バインディング ソース間の競合を解決します。現在の優先順位の適用順序は、最小から最大まで、次のとおりです。

1. CLI : **cts role-based sgt-map sgt** コマンドを使用して設定されたバインド。
2. L3IF : 一貫した L3IF-SGT（レイヤ 3 インターフェイスから SGT へ）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ド。
3. SXP : SXP（SGT Exchange Protocol）ピアから学習されたバインド。
4. 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 間のバインド。

Cisco TrustSec インターフェイスと SGT のマッピングの設定方法

レイヤ 3 インターフェイスと SGT のマッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type slot/port**
4. **cts role-based sgt-map sgt sgt-number**
5. **end**

手順の詳細

	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 slot/port 例 : Device(config)# interface gigabitEthernet 0/0	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。

	コマンドまたはアクション	目的
ステップ 4	cts role-based sgt-map sgt sgt-number 例 : Device(config-if)# cts role-based sgt-map 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。 <ul style="list-style-type: none"> • <i>sgt-number</i> : セキュリティグループタグ (SGT) 番号を指定します。有効値は 2 ~ 65519 です。
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。

レイヤ 3 インターフェイスと SGT のマッピングの確認

手順の概要

1. **enable**
2. **show cts role-based sgt-map all**

手順の詳細

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)。

例 :

```
Device> enable
```

ステップ 2 show cts role-based sgt-map all

レイヤ 3 インターフェイスの入力トラフィックに対するセキュリティグループタグ (SGT) マッピングを表示します。

例 :

次は、**show cts role-based sgt-map all** コマンドからの出力例です。Cisco TrustSec インターフェイスと SGT のマッピング機能が実装されると、入力インターフェイスのトラフィックは、レイヤ 3 インターフェイス (L3IF) によって適切にタグ付けされます。この出力では、IP アドレスからセキュリティグループタグ (IP-SGT) バインディング ソースの優先方式を表示します (IP-SGT バインディング ソースの優先度について、詳細は「バインディング送信元プライオリティ」の項を参照)。

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

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

```
192.0.2.1          4      INTERNAL
192.0.2.5/24      3      L3IF
192.0.2.10/8     3      L3IF
192.0.2.20       5      CLI
198.51.100.1     4      INTERNAL
```

```
IP-SGT Active Bindings Summary
```

```
=====
Total number of CLI      bindings = 1
Total number of L3IF    bindings = 2
Total number of INTERNAL bindings = 2
Total number of active  bindings = 5
```

Cisco TrustSec インターフェイスと SGT のマッピングの設定例

例：レイヤ3 インターフェイスと SGT のマッピングの設定

次の例は、レイヤ3 入力インターフェイスへのセキュリティグループタグ (SGT) のマッピング設定を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# cts role-based sgt-map sgt 77
Device(config-if)# end
```

Cisco TrustSec インターフェイスと SGT のマッピングに関する追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	<ul style="list-style-type: none"> 『Cisco IOS Security Command Reference Commands A to C』 『Cisco IOS Security Command Reference Commands D to L』 『Cisco IOS Security Command Reference Commands M to R』 『Cisco IOS Security Command Reference Commands S to Z』
Cisco TrustSec と SXP の設定	『Cisco TrustSec スイッチ コンフィギュレーション ガイド』

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	http://www.cisco.com/cisco/web/support/index.html

Cisco TrustSec インターフェイスと SGT のマッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: Cisco TrustSec インターフェイスと SGT のマッピングの機能情報

機能名	リリース	機能情報
Cisco TrustSec インターフェイスと SGT のマッピング		<p>Cisco TrustSec インターフェイスと SGT のマッピング機能は、レイヤ3入力インターフェイス上のすべてのトラフィックを、セキュリティグループタグ (SGT) にバインドします。このマッピングを実装すると、Cisco TrustSec では、SGT を使用してさまざまな論理レイヤ3入力インターフェイスからトラフィックを分離できるようになります。</p> <p>次のコマンドが導入または変更されました。 cts role-based sgt-map sgt</p>

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。