双方向 SXP サポートの有効化

双方向 SXP サポート機能は、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）バインドのサポートを追加することで、SXP バージョン 4 を使用した Cisco TrustSec の機能を強化します。このバインドは、単一の接続でスピーカーとリスナーどちらの方向へも伝播できます。

双方向 SXP サポートの前提条件

- Cisco TrustSec がデバイス上に設定されていること。詳細については、『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章を参照してください。
- Cisco TrustSec の機能を既存のデバイスで使用するには、次のセキュリティライセンスのいずれかを購入していること。
  - IP Base ライセンス
  - LAN Base ライセンス

（注） LAN Base ライセンスは、Cisco IOS XE Everest 16.5.1 から使用できます。

  - IP サービスライセンス
- すべてのネットワークデバイスに接続が存在すること。

- 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。

双方向 SXP サポートの制約事項

- 接続のそれぞれの端のピアは、**both** キーワードを使用して双方向接続として設定する必要があります。一方の端を **both** キーワードを使用した双方向接続として設定し、他方の端をスピーカーまたはリスナーとして設定（単方向接続）するのは、誤った設定です。

双方向 SXP サポートに関する情報

双方向 SXP サポートの概要

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。データを生成するピアはスピーカーで、対応するピアはリスナーになります。

双方向セキュリティ グループ タグ（SGT）交換プロトコル（SXP）の設定をサポートすることで、ピアはスピーカーとリスナーのどちらとしても動作し、単一の接続を使用する双方向の SXP バインドを伝播できるようになります。

双方向 SXP の設定は、IP アドレスのペア 1 組と管理されます。いずれかの端で、SXP 接続を開始するのはリスナーのみであり、スピーカーは着信接続を受け入れます。

図 *1:* 双方向 *SXP* 接続

さらに、SXP バージョン 4（SXPv4）は、引き続きループ検出メカニズムをサポートしています（ネットワークの古いバインディングを防ぐため）。

双方向 SXP サポートを有効化する方法

双方向 SXP サポートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts sxp enable**

4. **cts sxp default password**
5. **cts sxp default source-ip**
6. **cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*]
7. **cts sxp speaker hold-time** *minimum-period*
8. **cts sxp listener hold-time** *minimum-period maximum-period*
9. **exit**

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	**cts sxp enable** 例： `Device(config)# cts sxp enable`	Cisco TrustSec セキュリティ グループ タグ（SGT）交換プロトコル バージョン4（SXPv4）をネットワーク デバイスで有効にします。
ステップ 4	**cts sxp default password** 例： `Device(config)# cts sxp default password Cisco123`	（オプション）Cisco TrustSec SGT SXP のデフォルト パスワードを指定します。
ステップ 5	**cts sxp default source-ip** 例： `Device(config)# cts sxp default source-ip 10.20.2.2`	（オプション）Cisco TrustSec SGT SXP 送信元 IPv4 アドレスを設定します。
ステップ 6	**cts sxp connection peer** *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} **both** [**vrf** *vrf-name*] 例： `Device(config)# cts sxp connection peer 10.20.2.2 password default mode local both`	双方向 SXP 設定用の Cisco TrustSec SXP ピア アドレス接続を設定します。**both** キーワードは、双方向 SXP 設定を設定します。 **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。接続アドレスが指定されていない場合、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。

	コマンドまたはアクション	目的
		password キーワードには、Cisco TrustSec 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 Cisco TrustSec SXP パスワードを使用します。 • **none**：パスワードは使用されません。 **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。 • **peer**：指定したモードはピアデバイスを参照します。 • **both**：デバイスが双方向 SXP 接続のスピーカーとリスナー両方であることを指定します。 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 7	**cts sxp speaker hold-time** *minimum-period* 例： `Device(config)# cts sxp speaker hold-time 950`	（オプション）Cisco TrustSec SGT SXPv4 用のスピーカー ネットワーク デバイスのグローバル ホールド時間（秒単位）を設定します。有効な範囲は 1 ～ 65534 です。デフォルトは 120 です。
ステップ 8	**cts sxp listener hold-time** *minimum-period maximum-period* 例： `Device(config)# cts sxp listener hold-time 750 1500`	（オプション）Cisco TrustSec SGT SXPv4 用のリスナー ネットワーク デバイスのグローバル ホールド時間（秒単位）を設定します。有効な範囲は 1 ～ 65534 です。デフォルトは 90 ～180 です。 （注） *maximum-period* 値は、*minimum-period* 値よりも大きいか等しくする必要があります。
ステップ 9	**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。

双方向 SXP サポート設定の確認

手順の概要

1. **enable**
2. **show cts sxp** {**connections** | **sgt-map**} [**brief** | **vrf** *vrf-name*]

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 sxp {connections | sgt-map} [brief | vrf vrf-name]

Cisco TrustSec 交換プロトコル（SXP）のステータスと接続を表示します。

例：

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
------------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)


Device# show cts sxp connection brief

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
------------------------------------------------------
```

```
Peer_IP Source_IP Conn Status Duration
-----------------------------------------------
2.0.0.2 1.0.0.2 On(Speaker)::On(Listener) 0:00:37:17 (dd:hr:mm:sec)::0:00:37:19 (dd:hr:mm:sec)
```

次のテーブルに、接続ステータス出力のさまざまなシナリオを示します。

表 *1*: 接続ステータスの出力シナリオ

Node1	Node2	接続ステータスについての Node1 CLI 出力	接続ステータスについての Node2 CLI 出力
両方	両方	オン（スピーカー） オン（リスナー）	オン（スピーカー） オン（リスナー）
スピーカー	リスナー	オン	点灯
リスナー	スピーカー	オン	点灯

双方向 SXP サポートの設定例

例：双方向 SXP サポートの設定

次の例は、双方向 CTS-SXP を有効化し、Device_A 上の SXP ピア接続が Device_B に接続するよう設定する方法を示します。

```
Device_A> enable
Device_A# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local both
Device_A(config)# exit
```

次の例は、Device_B 上の双方向 CTS-SXP ピア接続が Device_A に接続するように設定する方法を示します。

```
Device_B> enable
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Password123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local both
Device_B(config)# exit
```

双方向 SXP サポートに関する追加情報

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	• 『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 の設定	『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/support

双方向 SXP サポートの機能情報

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 トレイ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 *2:* 双方向 *SXP* サポートの機能情報

機能名	リリース	機能情報
双方向 SXP サポート		双方向 SXP サポート機能は、セキュリティ グループ タグ（SGT）交換プロトコル（SXP）バインドのサポートを追加することで、SXP バージョン 4 を使用した Cisco TrustSec の機能を強化します。このバインドは、単一の接続でスピーカーとリスナーどちらの方向へも伝播できます。 • Cisco Catalyst 3750-X シリーズ スイッチ • Cisco Catalyst 3560-X シリーズ スイッチ • Cisco Catalyst 4500E Supervisor Engine 7-E • Cisco Catalyst 4500E Supervisor Engine 7L-E • Cisco Catalyst 4500-X シリーズ スイッチ • Cisco Catalyst 4500E Supervisor Engine 8-E • Cisco Catalyst 3850 シリーズ スイッチ • Cisco Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**cts sxp connection peer**

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。