Cisco TrustSec スイッチ コンフィギュレーション ガイド

Cisco Catalyst スイッチについて

更新：2012 年 10 月

Text Part Number: OL-22192-02-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco TrustSec スイッチ コンフィギュレーション ガイド

CONTENTS

はじめに

マニュアルの構成

このマニュアルは、次の章および付録から構成されています。

章または付録のタイトル	説明
第 1 章「Cisco TrustSec の概要」	Cisco TrustSec ネットワークを作成するプロセスと要素について説明します。
第 2 章「Cisco TrustSec ソリューションの設定」	Cisco TrustSec ネットワークを実装するために必要な設定作業の概要について説明します。
第 3 章「アイデンティティ、接続および SGT の設定」	NDAC および TrustSec シード デバイスの設定手順について説明します。
第 4 章「SGT 交換プロトコル over TCP（SXP）およびレイヤ 3 トランスポートの設定」	SGT over TCP プロトコル（SXP）設定手順について説明します。
第 5 章「SGACL ポリシーの設定」	スイッチの CLI からのセキュリティ グループ ACL の設定の手順を説明します。
第 6 章「エンドポイント アドミッション コントロールの設定」	TrustSec コンテキストでの 802.1X、MAB、WebAuth の設定手順について説明します。
第 7 章「Cisco TrustSec コマンドの概要」	Cisco TrustSec CLI コマンドのリストと簡単な説明を示します。
付録 A「Catalyst 3750、3560、および 2960 シリーズ スイッチのリリース ノート」	Catalyst 3750 および Catalyst 3560 シリーズ スイッチの TrustSec 実装に関する制約、制限、または考慮事項について説明します。
付録 B「Catalyst 4500 シリーズ スイッチのノート」	Catalyst 4500 シリーズ スイッチの TrustSec 実装に関する制約、制限、または考慮事項について説明します。
付録 C「Catalyst 6500 シリーズ スイッチのノート」	Catalyst 6500 シリーズ スイッチの TrustSec 実装に関する制約、制限、または考慮事項について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
*イタリック体*フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*イタリック体*フォントで示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	いずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイントアドバイス *時間を節約する方法*です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 **「*警告*」の意味です。人身事故を予防するための注意事項が記述されています。**

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

Cisco TrustSec の概要

この章は、次の内容で構成されています。

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 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。

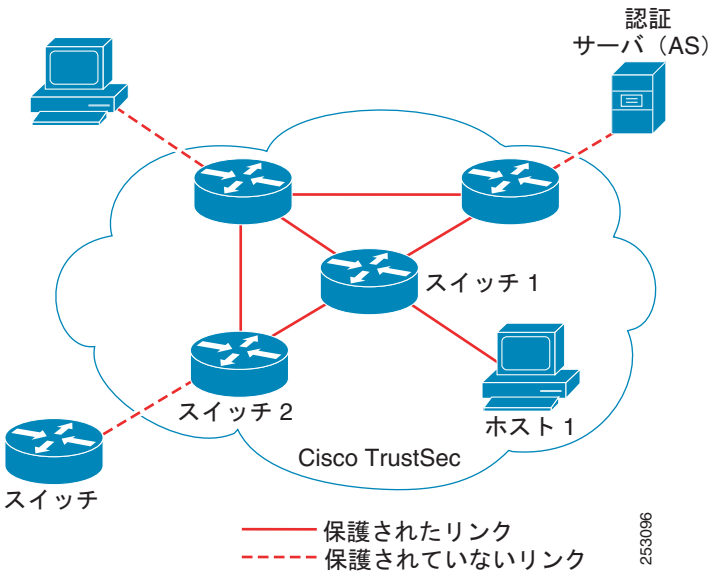
Cisco TrustSec のアーキテクチャは、3 種類の主要コンポーネントで構成されています。

- 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。

図 1-1 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 1-1　Cisco TrustSec ネットワーク ドメインの例



Cisco TrustSec 認証プロセスの各関係者は次のいずれかのロールで動作します。

- 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：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、認証サーバの代わりに新しいピアサプリカントを認証できる認証デバイス。

オーセンティケータとサプリカント間のリンクが最初に起動すると、通常次の一連のイベントが発生します。

1. 認証（802.1X）：オーセンティケータが媒介として機能し、サプリカントが認証サーバにより認証されます。相互認証は 2 ピア間で実行されます（サプリカントとオーセンティケータ）。
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、認証サーバはリンクされた各ピアにセキュリティ グループ割り当ておよび ACL などの、認可ポリシーを提供します。認証サーバが各ピアのアイデンティティを相手側に提供し、その後各ピアは、リンクの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：リンクの両側が暗号化をサポートしている場合、サプリカントおよび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。

この 3 段階の手順がすべて完了すると、オーセンティケータは不正（ブロッキング）ステートから許可ステートにリンク状態を変更し、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、割り当てられた送信元デバイスのセキュリティ 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ことです。出力とは、パケットがパス上の最後の Cisco TrustSec 対応デバイスを出ることです。

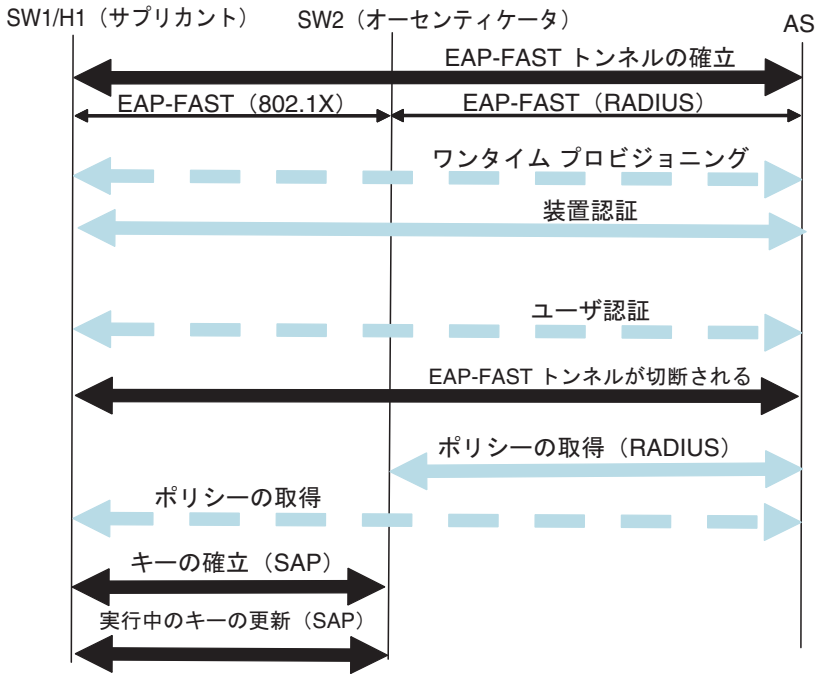
認証

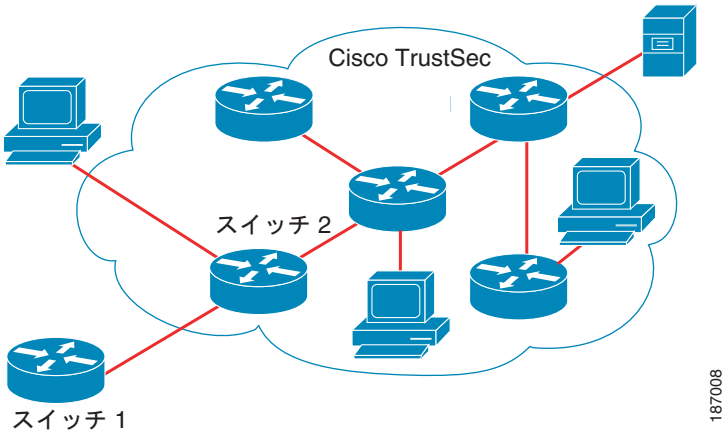
ここでは、次の内容について説明します。

Cisco TrustSec と認証

ネットワーク デバイス アドミッション コントロール（NDAC）を使用して、Cisco TrustSec は、デバイスがネットワークに参加できるようにする前にデバイスを認証します。NDAC は、拡張認証プロトコル（EAP）方式としての Extensible Authentication Protocol Flexible Authentication via Secure Tunnel（EAP-FAST）とともに、802.1X 認証を使用して、認証を実行します。EAP-FAST カンバセーションによって、チェーンを使用した EAP-FAST トンネル内で他の EAP 方式の交換が可能になります。この方法では、管理者は Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAPv2）のような従来型のユーザ認証方式を使用しながら、EAP-FAST トンネルが提供するセキュリティも利用できます。EAP-FAST 交換中に、認証サーバは認証サーバとの将来のセキュアな通信に使用される共有キーおよび暗号化されたトークンが含まれる一意の保護されたアクセス クレデンシャル（PAC）を作成し、サプリカントに配信します。図 1-2 に、EAP-FAST トンネルおよび Cisco TrustSec で使用する内部方式を示します。

図 1-2　Cisco TrustSec の認証





ここでは、次の内容について説明します。

- 「EAP-FAST への Cisco TrustSec の機能拡張」（P.1-5）
- 「802.1X ロールの選択」（P.1-5）
- 「Cisco TrustSec 認証の概要」（P.1-5）

EAP-FAST への Cisco TrustSec の機能拡張

Cisco TrustSec に EAP-FAST を実装することにより、次の機能拡張が実現しました。

- オーセンティケータの認証：オーセンティケータと認証サーバの間の共有キーを得るために PAC を使用するようにオーセンティケータに求めることにより、オーセンティケータのアイデンティティをセキュアに判断します。また、この機能により、オーセンティケータが使用できる可能なすべての IP アドレスに関して認証サーバに RADIUS 共有キーを設定する手間が省けます。
- ピアのアイデンティティを各デバイスに通知：認証交換の完了までに、認証サーバはサプリカントとオーセンティケータの両方を識別します。認証サーバは、保護された EAP-FAST 終端で追加の type-length-value（TLV）パラメータを使用して、オーセンティケータのアイデンティティと、そのオーセンティケータが Cisco TrustSec に対応しているかどうかをサプリカントに伝えます。認証サーバはさらに、Access- Accept メッセージの RADIUS 属性を使用して、サプリカントのアイデンティティおよびそのサプリカントが Cisco TrustSec に対応しているかどうかをオーセンティケータに伝えます。各デバイスは、ピアのアイデンティティを認識しているため、認証サーバに追加の RADIUS Access-Requests を送信し、リンクに適用されるポリシーを取得できます。

802.1X ロールの選択

802.1X では、オーセンティケータに認証サーバとの IP 接続が必要です。オーセンティケータは RADIUS over UDP/IP を使用してサプリカントとオーセンティケータの認証交換をリレーする必要があるためです。PC などのエンドポイント装置はネットワークへの接続時にサプリカントとして機能することになります。ただし、2 つのネットワーク デバイス間の Cisco TrustSec 接続の場合、各ネットワーク デバイスの 802.1X ロールが他方のネットワーク デバイスに即座に認識されない場合もあります。

隣接する 2 つのスイッチにオーセンティケータとサプリカントのロールを手動で設定する代わりに、Cisco TrustSec は自動的にロール選択アルゴリズムを実行して、いずれのスイッチがオーセンティケータとして機能し、いずれがサプリカントとして機能するかを決定します。ロール選択アルゴリズムは、RADIUS サーバに IP で到達可能なスイッチにオーセンティケータ ロールを割り当てます。どちらのスイッチもオーセンティケータとサプリカントの両方のステート マシンを起動します。あるスイッチが、ピアに RADIUS サーバへのアクセス権があることを検出すると、そのデバイスは自身のオーセンティケータ ステート マシンを終了し、サプリカントのロールを引き受けます。両方のスイッチが RADIUS サーバにアクセスできる場合、RADIUS サーバから最初に応答を受信したスイッチがオーセンティケータになり、もう 1 つのスイッチがサプリカントになります。

Cisco TrustSec 認証の概要

Cisco TrustSec 認証プロセスが完了するまでに、認証サーバは次の処理を行います。

- サプリカントとオーセンティケータのアイデンティティの検証
- サプリカントがエンドポイント装置の場合はユーザの認証

Cisco TrustSec 認証プロセスの完了時には、オーセンティケータおよびサプリカントの両方が次の情報を取得しています。

- ピアのデバイス ID
- ピアの Cisco TrustSec 機能についての情報
- SAP に使用されるキー

デバイスのアイデンティティ

Cisco TrustSec はデバイスの ID として IP アドレスも MAC アドレスも使用しません。その代わり、各 Cisco TrustSec 対応スイッチに、Cisco TrustSec ドメインで一意に識別できる名前（デバイス ID）を割り当てる必要があります。このデバイス ID は次の操作に使用されます。

- 認証ポリシーの検索
- 認証時におけるデータベース内のパスワードの検索

デバイスの証明書

Cisco TrustSec はパスワードベースのクレデンシャルをサポートしています。Cisco TrustSec はパスワードでサプリカントを認証し、相互認証を提供するために MSCHAPv2 を使用します。

認証サーバはこれらのクレデンシャルを EAP-FAST フェーズ 0（プロビジョニング）の交換（サプリカントで PAC がプロビジョニングされる）中にサプリカントの相互認証に使用します。Cisco TrustSec は PAC の期限が切れるまで、EAP-FAST フェーズ 0 の交換は再実行しません。その後のリンク起動時には、EAP-FAST フェーズ 1 とフェーズ 2 の交換だけを実行します。EAP-FAST フェーズ 1 交換では、認証サーバとサプリカントの相互認証に PAC を使用します。Cisco TrustSec がデバイスのクレデンシャルを使用するのは、PAC プロビジョニング（または再プロビジョニング）段階だけです。

サプリカントが最初に Cisco TrustSec ドメインに加入する際に、認証サーバはサプリカントを認証し、PAC を使用してサプリカントに共有キー、および暗号化されたトークンをプッシュします。認証サーバとサプリカントは、その後の EAP-FAST フェーズ 0 交換の相互認証にこのキーとトークンを使用します。

ユーザの証明書

Cisco TrustSec には、エンドポイント装置の特定タイプのユーザ クレデンシャルは必要ありません。認証サーバでサポートされるユーザ認証方式を任意に選択して、対応するクレデンシャルを使用できます。たとえば、Cisco Secure Access Control System（ACS）バージョン 5.1 は MSCHAPv2、汎用トークン カード（GTC）、または RSA ワンタイム パスワード（OTP）をサポートします。

セキュリティ グループ ベースのアクセス コントロール

ここでは、次の内容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、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 は各スコープが Cisco TrustSec ドメイン内でグローバルに一意の 16 ビットのセキュリティ グループ番号を各セキュリティ グループに割り当てます。スイッチセキュリティ 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。

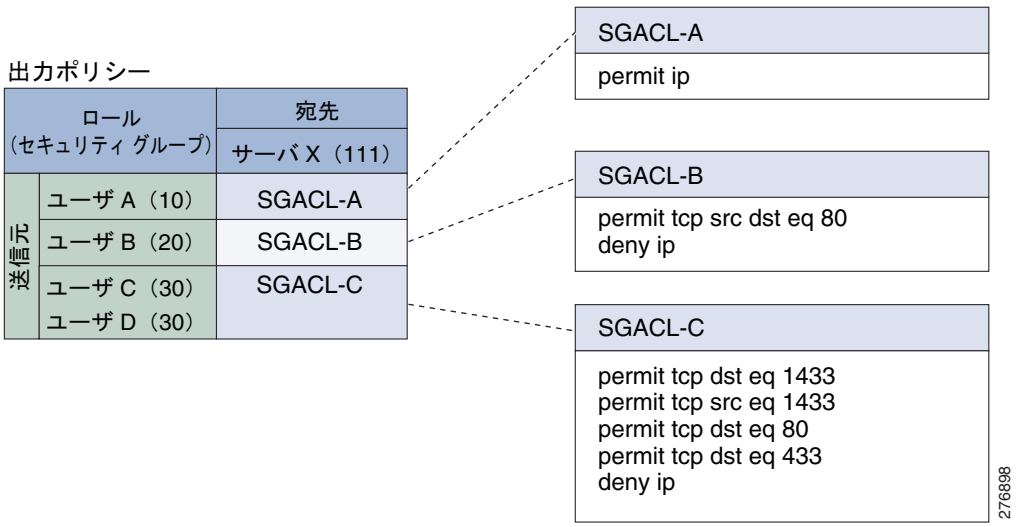
SGT には、送信元のセキュリティ グループが含まれているため、タグは送信元 SGT と呼ばれることもあります。宛先デバイスは、簡素化のために宛先グループ タグ（DGT）と呼ばれることがあるセキュリティ グループ（宛先 SG）にも割り当てられます。ただし、実際の Cisco TrustSec パケット タグには宛先デバイスのセキュリティ グループ番号は含まれていません。

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強制は、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。

図 1-3 に、3 つの定義済みのユーザ 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 許可マトリクスの例を示します。ユーザの役割に基づいて宛先サーバへのアクセスを 3 つの SGACL ポリシーで制御します。

図 1-3　　SGACL ポリシー マトリクスの例



ネットワーク内のユーザおよび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 コントロールを適用することで、Cisco TrustSec はネットワーク内のロール ベースのトポロジに依存しないアクセス コントロールを実現します。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。ユーザがスイッチに追加されたら、適切なセキュリティ グループにユーザを割り当てるだけで、ユーザはただちにそのグループの許可を受信します。

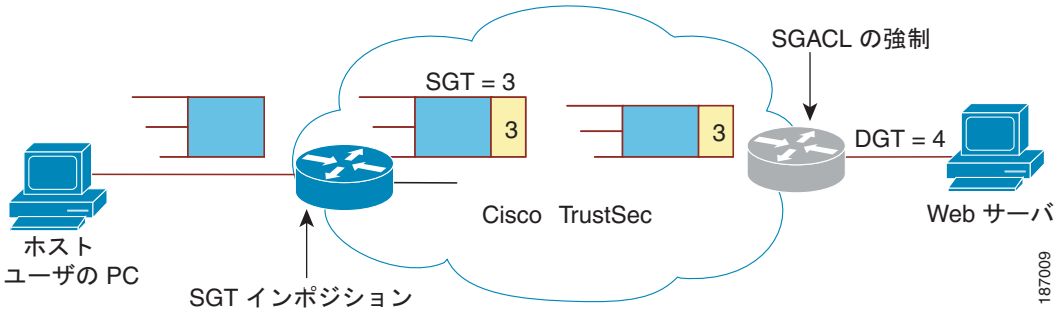
ロール ベースの許可を使用すると ACL のサイズが大幅に節約され、メンテナンス作業も簡単になります。Cisco TrustSec によって、設定されているアクセス コントロール エントリ（ACE）の数は、指定されている許可の数によって決定されるため、ACE の数は従来の IP ネットワークでよりもずっと小さくなります。Cisco TrustSec での SGACL の使用は、従来の ACL と比較して TCAM リソースをより効率的に使用します。

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および出力の強制を使用して実装されます。Cisco TrustSec ドメインへの入力点で、送信元からのトラフィックに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 がタグ付けされます。SGT はドメイン全体でトラフィックで伝播されます。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、図 1-4 のように SGT の割り当てと SGACL の強制が実行されます。

図 1-4　Cisco TrustSec ドメインの SGT と SGACL



ステップ 1　ホスト PC が Web サーバにパケットを送信します。PC と Web サーバは Cisco TrustSec ドメインのメンバではないが、パケットのデータ パスに Cisco TrustSec ドメインが含まれています。

ステップ 2　Cisco TrustSec の入力スイッチは、ホスト PC の認証サーバ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。

ステップ 3　Cisco TrustSec 出力スイッチは、Web サーバの認証サーバ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 と宛先グループ 4 に適用する SGACL ポリシーを適用します。

ステップ 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 ドメインの入力ネットワーク デバイスは、Cisco TrustSec ドメインに転送するときに、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 交換プロトコル（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。

ルーティングされたトラフィックについては、SGACL の強制は出力スイッチ、通常分散スイッチや、ルーテッド ポートが宛先ホストに接続するアクセス スイッチによって実行されます。SGACL の実行をグローバルにイネーブルにすると、強制は SVI インターフェイスを除く各レイヤ 3 インターフェイスで自動的にイネーブルになります。

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間のサーバ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。

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。

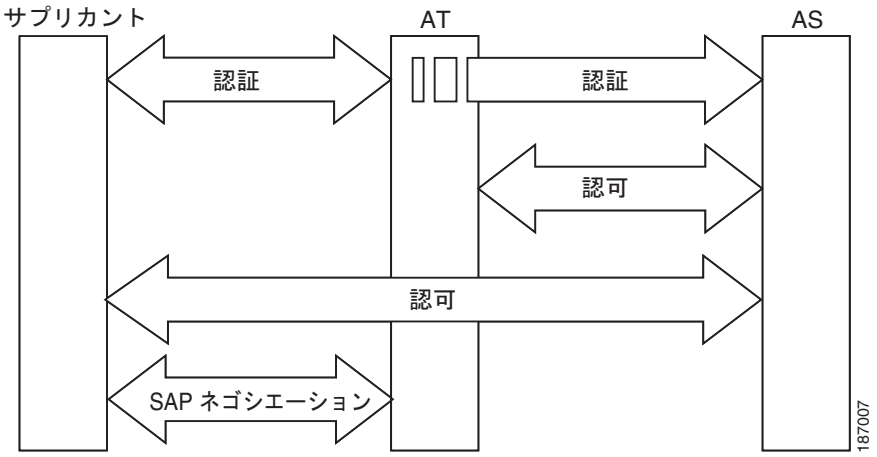
認証サーバは次の属性を返します。

- 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。Cisco IOS Release 12.2(33)SXI では、ポリシー データおよび環境データだけがキャッシュされます。

ヒント　Cisco TrustSec デバイスは、認証サーバ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。

図 1-5 に、NDAC および SAP ネゴシエーション プロセスを示します。

図 1-5　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から取得するサーバ 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、認証サーバから次の環境データを取得します。

- サーバ 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のリスト（認証および許可の両方）
- 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スイッチは、認証サーバへの IP 接続を通じて、UDP/IP での RADIUS メッセージの交換により、スイッチが認証サーバ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に送信します。認証サーバから 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、Security Association（SA; セキュリティ アソシエーション）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。

Cisco IOS Release 12.2(50)SY 以降のリリースの Cisco Catalyst 6500 シリーズ スイッチについては、Cisco TrustSec は、IEEE 802.1AE 標準に準拠した AES-128 GCM および GMAC を使用します。

Cisco TrustSec ネットワークでの Cisco TrustSec 非対応デバイスおよびネットワークの使用

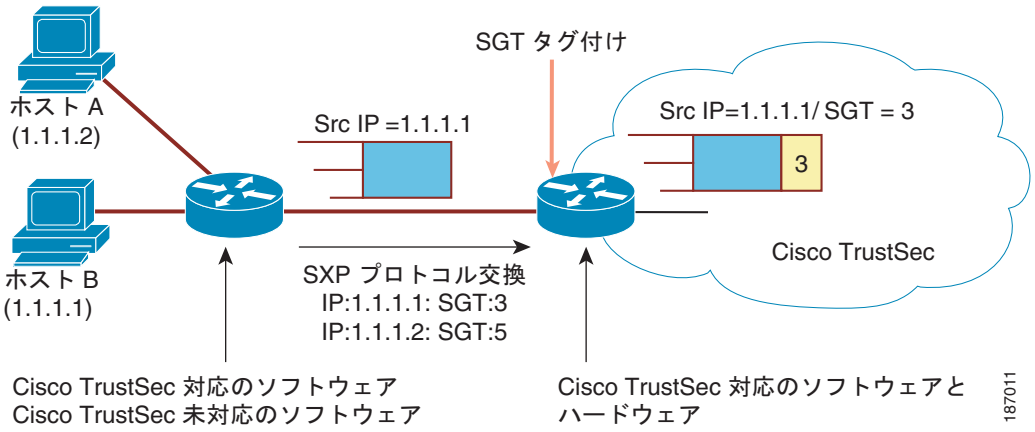
ここでは、次の内容について説明します。

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 スイッチに渡します。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 スイッチはこの 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 ポリシーを強制します（図 1-6 を参照）。

図 1-6　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。

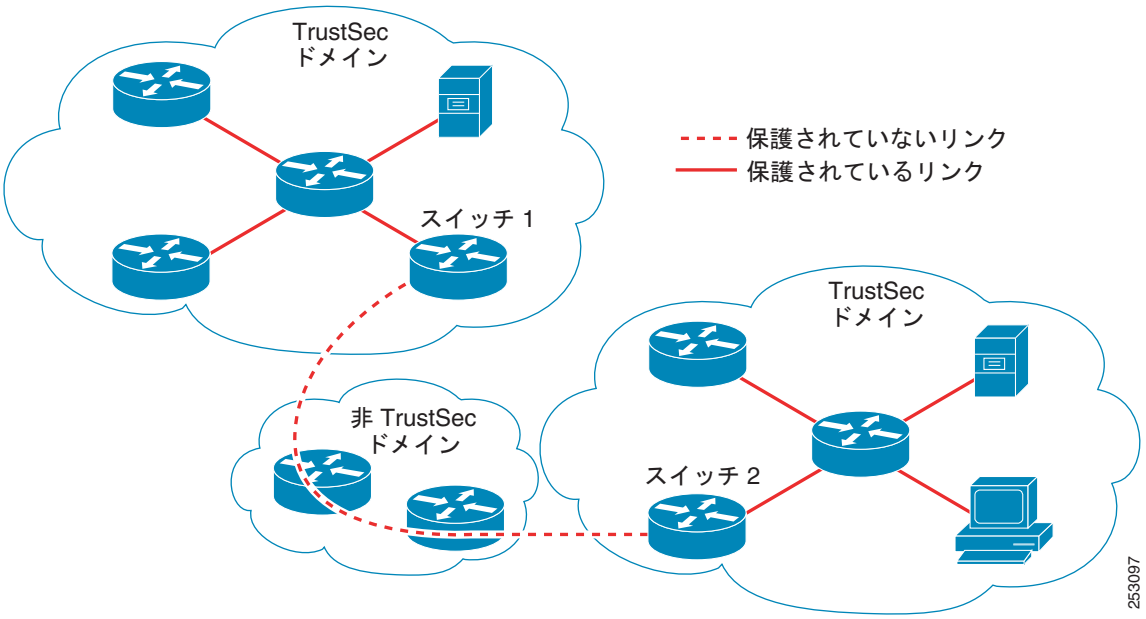
SXP は複数のホップを許可します。つまり、Cisco TrustSec ハードウェア サポート対象外デバイスのピアが Cisco TrustSec ハードウェア サポートの対象外でもある場合、2 番目のピアはハードウェア対応ピアに到達するまで IP と SGT のマッピング情報の伝播を継続して、3 番目のピアへの SXP 接続を設定できます。デバイスは 1 つの SXP 接続では SXP リスナーとして、別の SXP 接続では SXP スピーカーとして設定できます。

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、図 1-7 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 1-7　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。

Cisco TrustSec 非対応スイッチング モジュールの Cisco TrustSec リフレクタ

Cisco TrustSec ドメインの Catalyst 6500 シリーズ スイッチ には、次のいずれかのタイプのスイッチング モジュールが含まれている場合があります。

- Cisco TrustSec 対応：ハードウェアは SGT の挿入および伝播をサポートします。
- Cisco TrustSec-Aware：ハードウェアは SGT の挿入および伝播をサポートしませんが、ハードウェアはパケットの送信元および宛先 SGT を特定するために検索を実行できます。
- Cisco TrustSec 非対応：ハードウェアは SGT の挿入および伝播をサポートせず、ハードウェア検索で SGT を特定することもできません。

スイッチに Cisco TrustSec 対応のスーパーバイザ エンジンが含まれる場合は、同じスイッチ内のレガシー Cisco TrustSec 非対応スイッチング モジュールに対応するために、Cisco TrustSec リフレクタ機能を使用できます。Cisco IOS Release 12.2(50)SY 以降のリリースでは、Cisco TrustSec リフレクタは SPAN を使用して Cisco TrustSec 非対応スイッチング モジュールからのトラフィックを、SGT の割り当ておよび挿入のためにスーパーバイザ エンジンにリフレクトします。

2 つの相互に排他的なモード（入力および出力）は、Cisco TrustSec リフレクタでサポートされます。デフォルトはいずれのリフレクタもイネーブルでないピュア モードです。Cisco TrustSec 入力のリフレクタは、ディストリビューション スイッチに対向しているアクセス スイッチで設定され、Cisco TrustSec 出力のリフレクタはディストリビューション スイッチで設定されます。

サポート対象 TrustSec リフレクタのハードウェア

Cisco TrustSec リフレクタ機能の詳細およびサポートされるハードウェアの一覧については、次の URL にある『*Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection*』のマニュアルを参照してください。

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-658388.html

入力のリフレクタ

Cisco TrustSec 入力のリフレクタは、Cisco TrustSec 非対応スイッチング モジュールが Cisco TrustSec ドメインのエッジにあり、Cisco TrustSec 対応のスーパーバイザ エンジンのアップリンク ポートが Cisco TrustSec 対応ディストリビューション スイッチに接続している、アクセス スイッチで実装されます。

Cisco TrustSec 入力のリフレクタの設定を受け入れるには、次の条件を満たす必要があります。

- スーパーバイザ エンジンが Cisco TrustSec 対応でなければなりません。
- Cisco TrustSec 非対応 DFC は、すべて電源がオフにする必要があります。
- Cisco TrustSec 出力のリフレクタはスイッチ上に設定しないでください。
- Cisco TrustSec 入力リフレクタをディセーブルにする前に、Cisco TrustSec 非対応スイッチング モジュールの電力を切る必要があります。

出力のリフレクタ

Cisco TrustSec 出力のリフレクタは Cisco TrustSec 非対応スイッチング モジュールがアクセス スイッチに対向するレイヤ 3 のアップリンクを使用して、ディストリビューション スイッチに実装されます。Cisco TrustSec 出力のリフレクタはレイヤ 3 のアップリンクだけでサポートされ、レイヤ 2 インターフェイス、SVI、サブインターフェイス、またはトンネルではサポートされないので、NAT トラフィックではサポートされません。

Cisco TrustSec 出力のリフレクタの設定を受け入れるには、次の条件を満たす必要があります。

- スーパーバイザ エンジンまたは DFC のスイッチング モジュールが Cisco TrustSec 対応である必要があります。
- Cisco TrustSec は、スーパーバイザ エンジンのアップリンク ポートまたは Cisco TrustSec 対応 DFC スイッチング モジュールの非ルーテッド インターフェイスでイネーブルにしないでください。
- Cisco TrustSec 出力リフレクタをディセーブルにする前に、Cisco TrustSec 非対応スイッチング モジュールの電力を切る必要があります。
- Cisco TrustSec 入力のリフレクタはスイッチ上に設定しないでください。

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 をイネーブルにする前に、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 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ディングが 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 バインディングは、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。

CHAPTER 2

Cisco TrustSec ソリューションの設定

この章では、次の事項について説明します。

設定の概要

このマニュアルは、Cisco Catalyst スイッチの基本的な Cisco TrustSec 設定手順を説明し、TrustSec コマンド リファレンスが含まれます。

ネットワーク全体の導入設定については、Cisco TrustSec 設定のハウツー マニュアルのセクションを参照してください。

ネットワーク全体の導入には、Cisco Identity Services Engine（Cisco ISE）、Cisco Secure Access Control System（Cisco ACS）、Cisco IP Phone、シスコのルータ、シスコのネットワーク機器などの、複数のデバイスの設定、相互運用性と管理が含まれています。

Cisco TrustSec Solution を説明するホワイト ペーパーとプレゼンテーションは次の URL にあります。
http://www.cisco.com/en/US/netsol/ns1051/index.html

Cisco TrustSec 設定のハウツー マニュアル

一連の「ハウツー」コンフィギュレーション マニュアルは、複雑なシナリオで実績のあるネットワーク アーキテクチャを実現するための導入ガイドラインとベスト プラクティスについて説明します。Cisco TrustSec の「ハウツー」マニュアルは、すべて次の URL にあります。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

『TrustSec 2.1 Configuration How-to Guide』には次のトピックが含まれます。

- 概要
- 計画と導入前チェック リスト
- ISE の基本設定：ISE のブートストラップ
- ID ストアの追加と認証の作成
- グローバル スイッチの設定
- Wireless LAN Controller の基本設定
- 段階的な導入の概要

- モニタ モード
- モニタ モードからの移行
- ロー インパクト モード
- クローズド モード
- ISE プロファイリング サービス
- ISE の基本設定 : 無差別 VMware
- 中央 Web 認証
- 複数の Active Directory ドメインに対するユーザ認証および認可
- ISE の導入タイプおよびガイドライン
- アクセスを区別する証明書の使用
- オンボーディングおよびプロビジョニング
- セキュリティ グループ アクセスを使用したサーバ間セグメンテーション
- AnyConnect NAM と Cisco ISE を使用した EAP の連結の導入
- 失敗した認証および認可

サポート対象ハードウェアおよびソフトウェア

TrustSec リリースごとの TrustSec のサポート対象ハードウェアとソフトウェアの一覧については、次を参照してください。
次の URL の『*Release Notes for Cisco TrustSec General Availability Releases*』
http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

ご使用のデバイスのリリース ノート、コンフィギュレーション ガイド、コマンド リファレンスも参照してください。

Cisco TrustSec の前提条件

次に、Catalyst スイッチで TrustSec ネットワークを構築するための前提条件を示します。

- すべてのネットワーク デバイスの TrustSec ソフトウェア
- すべてのネットワーク デバイス間の接続
- TrustSec ライセンスで動作する Cisco Secure ACS 5.1 または Cisco ISE のネットワークの可用性
- ネットワーク上で機能するディレクトリ、DHCP、DNS、認証局および NTP サーバ

Cisco TrustSec の注意事項および制限事項

Catalyst スイッチの Cisco TrustSec に関する次のガイドラインおよび制限があります。

- Cisco TrustSec の AAA は RADIUS を使用し、Cisco Secure Access Control System（ACS）バージョン 5.1 以降のみでサポートされています。
- NDAC 認証を実行するには Cisco TrustSec で 802.1X 機能をグローバルにイネーブルにする必要があります。802.1X をグローバルにディセーブルにすると、NDAC はディセーブルにあります。
- Cisco TrustSec は物理インターフェイスだけでサポートされ、論理インターフェイスでサポートされません。
- Cisco TrustSec はこのガイドで参照されているリリースでは IPv6 をサポートしていません。
- スイッチにデフォルトのパスワードが実装されている場合、そのスイッチでの接続は、デフォルトパスワードを使用するようにパスワードを設定する必要があります。デフォルトのパスワードが設定されていない場合、そのスイッチでの接続はパスワード設定を使用しないように設定してください。パスワード オプションの設定は導入ネットワーク全体で一貫している必要があります。
- 異なるスイッチ上の異なる値には **retry open timer** コマンドを設定します。

デフォルト設定

表 2-1 に Cisco TrustSec パラメータのデフォルトの設定値を示します。

表 2-1　Cisco TrustSec パラメータのデフォルト値

パラメータ	デフォルト
Cisco TrustSec	ディセーブル。
SXP	ディセーブル。
SXP デフォルト パスワード	なし。
SXP の復帰期間	120 秒（2 分）
SXP リトライ期間	60 秒（1 分）
Cisco TrustSec のキャッシング	ディセーブル。

その他のマニュアル

リリース固有のドキュメント

リリース固有のドキュメントのタイトル	TrustSec トピック
『Release Notes for Cisco TrustSec General Availability Releases』	• オープンおよび解決済みの注意事項 • 現在のハードウェアおよびソフトウェアのサポート

プラットフォーム固有のマニュアル

プラットフォーム固有のマニュアルのタイトル	TrustSec トピック
Catalyst 3000 シリーズ スイッチ	
『Release Notes for Catalyst 3560 and 3750 Switches』	オープンおよび解決済みの注意事項。サポートされる機能
『Catalyst 3560 Software Configuration Guides』	802.1x 設定手順
『Catalyst 3750-E and 3560-E Switch Software Configuration Guide』	
『Cisco Catalyst 3560-X Series Switches Software Configuration Guides』	
『Catalyst 3750 Metro Series Switches Software Configuration Guides』	
『Cisco Catalyst 3750-X Series Switches Software Configuration Guides』	
Catalyst 4500 シリーズ スイッチ	
『Cisco Catalyst 4500 Series Switches Release Notes』	オープンおよび解決済みの注意事項。サポートされる機能
『Catalyst 4500 Series Switches Software Configuration Guides』	802.1x 設定手順
Catalyst 6500 シリーズ スイッチ	
『Cisco Catalyst 6500 Series Switches Release Notes』	オープンおよび解決済みの注意事項。サポートされる機能
『Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide』	802.1x 設定手順
『Catalyst 6500 Release 12.2SY Software Configuration Guide』	
『Catalyst 6500 Release 15.0SY Software Configuration Guide』	
Nexus 7000 シリーズ スイッチ	
『Cisco Nexus 7000 Series Switches Release Notes』	オープンおよび解決済みの注意事項
『Cisco Nexus 7000 Series Switches Configuration Guides』	• Cisco Nexus 7000 シリーズ スイッチ、リリース 4.1 以降の TrustSec 機能の設定 • 802.1X 設定手順
Cisco Secure Access Control System および Cisco Identity Services Engine	
『Cisco Secure Access Control System Release Notes』	オープンおよび解決済みの注意事項
『Cisco Secure Access Control System End-User Guides』	Cisco ACS 5.1 以降の TrustSec の設定
Cisco Identity Services Engine	TrustSec の設定。ISE のマニュアルでは、TrustSec は SGA、またはセキュリティ グループ アクセスと呼ばれます。

Cisco IOS ソフトウェア マニュアル セット

Cisco IOS マニュアルのタイトル	TrustSec トピック
『Cisco IOS Security Configuration Guide: Securing User Services, Release 12.2SX』	802.1x、SXP、L2 SGT インポジションの設定手順
『Securing User Services Configuration Guide Library, Cisco IOS Release 15.2S』	

CHAPTER 3

アイデンティティ、接続および SGT の設定

ここでは、次の内容について説明します。

Cisco TrustSec シード デバイスのクレデンシャル、AAA 設定

認証サーバに直接接続されているか、または接続は間接でも TrustSec ドメインを開始する最初のデバイスである Cisco TrustSec 対応デバイスは、シード デバイスと呼ばれます。他の Cisco TrustSec ネットワーク デバイスは非シード デバイスです。

Cisco TrustSec ドメインを開始できるように、シード スイッチで NDAC および AAA をイネーブルにするには、次の手順を実行します。

リリース	機能の履歴
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが、Catalyst 3750(E)、3560(E)、および 3750(X) シリーズ スイッチに追加されました（**vrf** または IPv6 サポートなし）。

	コマンド	目的
ステップ 1	`Router# cts credentials id device-id password password`	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのスイッチが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。*device-id* 引数は、最大 32 文字で大文字と小文字を区別します。
ステップ 2	`Router# 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	`Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	`Router(config)# aaa authentication dot1x default group radius`	RADIUS として 802.1X ポート ベース認証方式を指定します。
ステップ 5	`Router(config)# aaa authorization network mlist group radius`	ネットワーク関連のすべてのサービス要求に対して RADIUS 認証を使用するようにスイッチを設定します。 • *mlist* : Cisco TrustSec AAA サーバ グループ。
ステップ 6	`Router(config)# cts authorization list mlist`	Cisco TrustSec の AAA サーバ グループを指定します。非シード デバイスはオーセンティケータからサーバ リストを取得します。
ステップ 7	`Router(config)# aaa accounting dot1x default start-stop group radius`	RADIUS を使用して 802.1X アカウンティングをイネーブルにします。
ステップ 8	`Router(config)# radius-server host ip-addr auth-port 1812 acct-port 1813 pac key secret`	RADIUS 認証サーバのホスト アドレス、サービス ポートおよび暗号キーを指定します。 • *ip-addr* : 認証サーバの IP アドレス。 • *secret* : 認証サーバによって共有される暗号キー。
ステップ 9	`Router(config)# radius-server vsa send authentication`	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）を認識して使用するようにスイッチを設定します。
ステップ 10	`Router(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 11	`Router(config)# exit`	コンフィギュレーション モードを終了します。

（注）　Cisco Secure ACS でスイッチの Cisco TrustSec クレデンシャルを設定する必要があります（『*Configuration Guide for the Cisco Secure ACS*』を参照）。

次に、Cisco TrustSec シード デバイスの AAA を設定する例を示します。

```
Router# cts credentials id Switch1 password Cisco123
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network MLIST group radius
Router(config)# cts authorization list MLIST
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(config)# exit
```

Cisco TrustSec 非シード デバイスのクレデンシャル、AAA 設定

リリース	機能の履歴
12.2(33) SXI3	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
15.0(1)SE	この機能が、Catalyst 3750(E)、3560(E)、および 3750(X) シリーズ スイッチに追加されました。

Cisco TrustSec ドメインに参加できるように、非シード スイッチで NDAC および AAA をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router# cts credentials id device-id password password`	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのスイッチが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。*device-id* 引数は、最大 32 文字で大文字と小文字を区別します。
ステップ 2	`Router# 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	`Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	`Router(config)# aaa authentication dot1x default group radius`	RADIUS として 802.1X ポート ベース認証方式を指定します。
ステップ 5	`Router(config)# aaa authorization network mlist group radius`	ネットワーク関連のすべてのサービス要求に対して RADIUS 認証を使用するようにスイッチを設定します。 • *mlist*：Cisco TrustSec の AAA サーバ グループを指定します。
ステップ 6	`Router(config)# aaa accounting dot1x default start-stop group radius`	RADIUS を使用して 802.1X アカウンティングをイネーブルにします。
ステップ 7	`Router(config)# radius-server vsa send authentication`	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）を認識して使用するようにスイッチを設定します。
ステップ 8	`Router(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 9	`Router(config)# exit`	コンフィギュレーション モードを終了します。

（注）　Cisco Secure ACS でスイッチの Cisco TrustSec クレデンシャルを設定する必要があります（『*Configuration Guide for the Cisco Secure ACS*』を参照）。

次に、非シード デバイスに Cisco TrustSec の AAA を設定する例を示します。

```
Router# cts credentials id Switch2 password Cisco123
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network MLIST group radius
```

```
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(config)# exit
```

アップリンク ポートでの 802.1X モードの Cisco TrustSec 認証のイネーブル化

リリース	機能の履歴
12.2(33) SXI3	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
15.0(1)SE	この機能が、Catalyst 3750(X) シリーズ スイッチに追加されました。

別の Cisco TrustSec デバイスに接続する各インターフェイスで Cisco TrustSec 認証をイネーブルにする必要があります。別の Cisco TrustSec デバイスにアップリンク インターフェイス上で 802.1X を使用して Cisco TrustSec 認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# interface` *type slot/port*	アップリンク インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-if)# cts dot1x`	アップリンク インターフェイスを NDAC 認証を実行するように設定します。
ステップ 4	`Router(config-if-cts-dot1x)# [no] sap mode-list` *mode1* [*mode2* [*mode3* [*mode4*]]]	（任意）インターフェイスに SAP 動作モードを設定します。インターフェイスは相互に受け入れ可能なモード用のピアとネゴシエートします。優先順位で許容されるモードをリストします。*mode* の選択肢は次のとおりです。 • **gcm**：認証および暗号化 • **gmac**：認証あり、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化あり、認証なし、暗号化なし **（注）** インターフェイスで SGT 挿入またはデータ 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** です。
ステップ 5	`Router(config-if-cts-dot1x)# [no] timer reauthentication` *seconds*	（任意）認証サーバが期間を指定しなかった場合、再認証期間を使用するように設定します。再認証期間が指定されていない場合、デフォルトの期間は 86400 秒です。

	コマンド	目的
ステップ 6	`Router(config-if-cts-dot1x)# [no] propagate sgt`	（任意）このコマンドの **no** 形式は、ピアが SGT を処理できない場合に使用されます。**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	`Router(config-if-cts-dot1x)# exit`	Cisco TrustSec 802.1X インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	`Router(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 9	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。
ステップ 10	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

この例では、優先 SAP モードとして GCM を使用しているインターフェイス上で、802.1X モードで Cisco TrustSec 認証をイネーブルにする方法を示します。認証サーバは、再認証タイマーを提供していません。

```
Router# configure terminal
Router(config)# interface gi2/1
Router(config-if)# cts dot1x
Router(config-if-cts-dot1x)# sap mode-list gcm null no-encap
Router(config-if-cts-dot1x)# timer reauthentication 43200
Router(config-if-cts-dot1x)# exit
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

アップリンク ポートでの手動モードによる Cisco TrustSec 認証の設定

リリース	機能の履歴
IOS 12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
IOS 15.0(1) SE	この機能が、Catalyst 3750(X) シリーズ スイッチに追加されました。

スイッチが認証サーバにアクセスできない場合、または 802.1X 認証が必要でない場合には、インターフェイスで Cisco TrustSec を手動で設定できます。接続の両側のインターフェイスに手動で設定する必要があります。

別の Cisco TrustSec デバイスにアップリンク インターフェイス上で手動で Cisco TrustSec を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# interface` *type slot/port*	アップリンク インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	`Router(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 4	`Router(config-if-cts-manual)# [no] sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]]`	（任意）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* オプションは次のとおりです。 • **gcm**：認証および暗号化 • **gmac**：認証あり、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化あり、認証または暗号化なし **（注）** インターフェイスで SGT 挿入または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** です。
ステップ 5	`Router(config-if-cts-manual)# [no] policy dynamic identity peer-name`	（任意）ピアのアイデンティティに基づいた認可サーバからの認可ポリシーの動的ダウンロードを許可するようにアイデンティティ ポート マッピング（IPM）を設定します。この作業の次に記載されている追加の使用上の注意を参照してください。 • *peer-name*：ピア デバイスの Cisco TrustSec デバイス ID。ピア名では、大文字と小文字が区別されます。 **（注）** Cisco TrustSec クレデンシャルが設定されていることを確認します（「Cisco TrustSec シード デバイスのクレデンシャル、AAA 設定」（P.3-1）を参照）。
	`Router(config-if-cts-manual)# [no] policy static sgt tag [trusted]`	（任意）スタティック許可ポリシーを設定します。この作業の次に記載されている追加の使用上の注意を参照してください。 • *tag*：10 進表記の SGT。指定できる範囲は 1 ～ 65533 です。 • **trusted**：この SGT を使用するインターフェイスの入力トラフィックのタグを上書きしてはいけないことを示します。
ステップ 6	`Router(config-if-cts-manual)# [no] propagate sgt`	（任意）このコマンドの **no** 形式は、ピアが SGT を処理できない場合に使用されます。**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	`Router(config-if-cts-manual)# exit`	Cisco TrustSec 手動インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	`Router(config-if)# shutdown`	インターフェイスをディセーブルにします。

	コマンド	目的
ステップ 9	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。
ステップ 10	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

アイデンティティ ポート マッピング（IPM）は、そのポートに着信するすべてのトラフィックに対して、単一の SGT が適用されるように、物理ポートを設定します。この SGT は、新しいバインディングが取得されるまで、そのポートから発信されるすべての IP トラフィックに適用されます。IPM は次のように設定されます。

- CTS 手動インターフェイス コンフィギュレーション モードで **policy static sgt** *tag* コマンドを使用
- CTS 手動インターフェイス コンフィギュレーション モードで **policy dynamic identity** *peer-name* コマンドを使用。Cisco ACS または Cisco ISE 設定では、*peer-name* は non-trusted に指定されています。

IPM は、次のポートでサポートされます。

- ルーテッド ポート
- アクセス モードのスイッチ ポート
- トランク モードのスイッチ ポート

インターフェイスの Cisco TrustSec を手動で設定する場合は、次のような使用上の注意事項、および制約事項を考慮してください。

- SAP パラメータが定義されていない場合、Cisco TrustSec カプセル化または暗号化は行われません。
- 選択した SAP モードで SGT を挿入可能にし、すべての着信パケットが SGT を伝送していない場合、タギング ポリシーは次のとおりです。
  - **policy static** コマンドが設定されている場合、パケットには **policy static** コマンドで設定した SGT がタグ付けされます。
  - **policy dynamic** コマンドが設定されている場合、パケットはタグ付けされません。
- 選択した SAP モードで SGT を挿入可能にし、着信パケットが SGT を伝送している場合、タギング ポリシーは次のとおりです。
  - **policy static** コマンドが **trusted** キーワードを指定せずに設定されている場合、SGT は **policy static** コマンドで設定した SGT に置き換えられます。
  - **policy static** コマンドが **trusted** キーワードを使用して設定されている場合、SGT は変更されません。
  - **policy dynamic** コマンドが設定されていて、認証サーバからダウンロードされた認可ポリシーがパケットの送信元が信頼できないことを示している場合、SGT はダウンロードしたポリシーで指定されている SGT に置き換えられます。
  - **policy dynamic** コマンドが設定されていて、ダウンロードされた認可ポリシーがパケットの送信元が信頼できることを示している場合、SGT は変更されません。

次に、インターフェイスに Cisco TrustSec 認証を手動モードで設定する例を示します。

```
Router# configure terminal
Router(config)# interface gi2/1
Router(config-if)# cts manual
Router(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Router(config-if-cts-manual)# exit
```

```
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

インターフェイスの SAP キーの再生成

暗号キーを手動で更新する機能は、多くの場合、ネットワーク アドミニストレーションのセキュリティ要件の一部です。SAP キー リフレッシュは通常、ネットワーク イベントおよび設定不可能な内部タイマーの組み合わせによりトリガーされ、自動的に行われます。

機能	履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
15.0(1)SE	この機能が、Catalyst 3750(E)、3560(E)、および 3750(X) シリーズ スイッチに追加されました。

	コマンド	目的
ステップ 1	`Router# cts rekey interface int slot/port`	MACsec リンクで SAP キーの再ネゴシエーションを強制します。

Cisco TrustSec インターフェイス設定の確認

TrustSec-relate MLS インターフェイスの設定を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show cts interface [interface type slot/port | brief | summary]`	TrustSec-related インターフェイス コンフィギュレーションを表示します。

次に、TrustSec-related インターフェイス コンフィギュレーションを表示する例を示します。

```
Router# show cts interface interface gi3/3

Global Dot1x feature is Enabled
Interface GigabitEthernet3/3:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "sanjose"
        Peer's advertised capabilities: ""
        802.1X role:         Supplicant
        Reauth period applied to link:  Not applicable to Supplicant role
    Authorization Status:    SUCCEEDED
        Peer SGT:            11
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
```

```
        Replay protection mode: OUT-OF-ORDER

        Selected cipher:

    Cache Info:
        Expiration            : 23:32:40 PDT Jun 22 2009
        Cache applied to link : NONE
        Expiration            : 23:32:40 PDT Jun 22 2009

    Statistics:
        authc success:              1
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              1
        authz fail:                 0
        port auth fail:             0

Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 55
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

デバイス SGT の手動設定

リリース	機能の履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。

通常の Cisco TrustSec 動作では、認証サーバ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。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(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	`Router(config)# exit`	コンフィギュレーション モードを終了します。

次に、デバイス SGT を手動で設定する例を示します。

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

IP-Address-to-SGT マッピングの手動設定

リリース	機能の履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
15.0(0)SY	SXPv3 が Catalyst 6500 スイッチに追加されました。 次のキーワードが、Catalyst 6500 シリーズ スイッチの **cts role-based sgt-map** コマンドに追加されました。 • *ipv4-address/prefix* • *ipv6-address/prefix* • **interface**

この項では、SGT と送信元 IP アドレスのマッピングについて説明します。

- 「サブネットと SGT のマッピング」（P.3-10）
- 「VLAN と SGT のマッピング」（P.3-15）
- 「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）」（P.3-19）

cts インターフェイス手動モードでのアイデンティティ ポート マッピングについては、次の項を参照してください。

- 「アップリンク ポートでの手動モードによる Cisco TrustSec 認証の設定」（P.3-5）

サブネットと SGT 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。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、SXPv3 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。以前の SXP バージョンは SXP リスナー ピアへエクスポートする前にサブネット プレフィックスをホストのバインディングのセットに変換します。

たとえば、IPv4 サブネット 198.1.1.0 /29 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 198.1.1.1 ～ 198.1.1.7：タグ付けされ SXP ピアに伝播されます。
- ネットワーク、およびブロードキャスト アドレス 198.1.1.0 および 198.1.1.8：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 バインディング数は制限するには、**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 の強制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 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。

サブネットと SGT のマッピングの機能履歴

機能名	リリース	機能情報
サブネットと SGT のマッピング	15.0 (1) SY	このコマンドのサポートが Catalyst 6500 シリーズ スイッチの SXPv3 で導入されました。関連する CLI は以前のリリースで表示されています。

デフォルト設定値

この機能には、デフォルト設定はありません。

サブネットと SGT のマッピングの設定

ここでは、次の内容について説明します。

- 「サブネットと SGT マッピング設定の確認」（P.3-13）
- 「サブネットと SGT のマッピングの設定」（P.3-11）

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* 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、SGT にバインドできません。
- 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。

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** switch# config t switch(config)#	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 2	[**no**] **cts sxp mapping network-map** *bindings* **Example:** switch(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）
ステップ 3	[**no**] **cts role-based sgt-map** *ipv4_address/prefix* **sgt** *number* **Example:** switch(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 4	[**no**] **cts role-based sgt-map** *ipv6_address::prefix* **sgt** *number* **Example:** switch(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。

	コマンド	目的
ステップ 5	**exit** **Example:** switch(config)# exit switch#	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。
ステップ 6	**show running-config** | include *search_string* **Example:** switch# show running-config | include sgt 1234 switch# show running-config | include network-map	実行コンフィギュレーションに **cts role-based sgt-map** および **cts sxp mapping network-map** コマンドがあることを確認します。
ステップ 7	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

サブネットと SGT マッピング設定の確認

サブネットと SGT のマッピング設定情報を表示するには、次のいずれかの作業を行います。

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。
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。

これらのコマンド出力に含まれるフィールドの詳細については、第 7 章「Cisco TrustSec コマンドの概要」を参照してください。

サブネットと SGT のマッピングの設定例

次に、SXPv3 を実行している 2 台の Catalyst 6500 シリーズ スイッチ（Switch1 と Switch2）間で IPv4 のサブネットと SGT のマッピングを設定する例を示します。

ステップ 1　Switch1（1.1.1.1）とスイッチ 2（2.2.2.2）間の SXP スピーカー / リスナー ピアリングを設定します。

```
Switch1# config t
Switch1(config)# cts sxp enable
```

```
Switch1(config)# cts sxp default source-ip 1.1.1.1
Switch1(config)# cts sxp default password 1syzygy1
Switch1(config)# cts sxp connection peer 2.2.2.2 password default mode local speaker
```

ステップ 2　Switch1 の SXP リスナーとしてスイッチ 2 を設定します。

```
Switch2(config)# cts sxp enable
Switch2(config)# cts sxp default source-ip 2.2.2.2
Switch2(config)# cts sxp default password 1syzygy1
Switch2(config)# cts sxp connection peer 1.1.1.1 password default mode local listener
```

ステップ 3　Switch2 で、SXP 接続が動作していることを確認してください。

```
Switch2# 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)
```

ステップ 4　サブネットワークを Switch1 に拡張されるように設定します。

```
Switch1(config)# cts sxp mapping network-map 10000
Switch1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Switch1(config)# cts role-based sgt-map 11.11.11.0/29 sgt 11111
Switch1(config)# cts role-based sgt-map 192.168.1.0/28 sgt 65000
```

ステップ 5　Switch2 で、Switch1 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。

```
Switch2# 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>
```

ステップ 6　Switch1 拡張数を確認します。

```
Switch1# show cts sxp sgt-map

    IP-SGT Mappings expanded:22
    There are no IP-SGT Mappings
```

ステップ 7　設定をスイッチ 1 およびスイッチ 2 に保存し、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。

```
Switch1(config)# copy running-config startup-config
Switch1(config)# exit
Switch2(config)# copy running-config startup-config
```

```
Switch2(config)# exit
```

VLAN と SGT のマッピング

VLAN と SGT のマッピング機能にでは、指定された 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 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、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 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 のバインディングは **cts role-based sgt-map vlan-list** グローバル コンフィギュレーション コマンドで設定されます。

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 トラッキングがイネーブルになっている場合、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 のバインディングを作成できます。

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 のバインディングは 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** cts グローバル コンフィギュレーション コマンドでマッピングされます。

VLAN と SGT のバインディング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ディングが受信された場合は、無視されます。バインディング優先順位は「バインディング送信元プライオリティ」（P.3-21）に記載しています。

VLAN と SGT のマッピングの機能履歴

表 3-1　VLAN と SGT のマッピングの機能履歴

機能名	リリース	機能情報
VLAN と SGT のマッピング	15.0 (1) SY	このコマンドのサポートが Catalyst 6500 シリーズ スイッチの SXPv3 で導入されました。関連する CLI は以前のリリースで表示されています。

デフォルト設定値

デフォルト設定はありません。

VLAN と SGT のマッピングの設定

ここでは、次の内容について説明します。

- 「VLAN-SGT マッピングを設定するためのタスク フロー」（P.3-16）

VLAN-SGT マッピングを設定するためのタスク フロー

- 着信 VLAN で同じ VLAN_ID で TrustSec スイッチ上に 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、デフォルトのゲートウェイになるように TrustSec スイッチの 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 TrustSec スイッチを設定します。
- TrustSec スイッチで IP デバイス トラッキングをイネーブルにします。
- VLAN と SGT のマッピングが TrustSec スイッチで発生することを確認します。

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	Example:
	`TS_switchswitch# config t`
	`TS_switchswitch(config)#`
		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 2	**vlan** ***vlan_id***
	
	Example:
	`TS_switch(config)# vlan 100`
	`TS_switch(config-vlan)#`
		TrustSec 対応ゲートウェイ スイッチに VLAN 100 を作成し、VLAN コンフィギュレーション サブモードを開始します。

ステップ 3	[**no**] **shutdown** **Example:** `TS_switch(config-vlan)#` **no shutdown**	VLAN 100 をプロビジョニングします。

ステップ 4	**exit**
	
	Example:
	`TS_switch(config-vlan)# exit`
	`TS_switch(config)#`
		VLAN 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 モードを開始します。

ステップ 5	**interface** type *slot/port*
	
	Example:
	`TS_switch(config)# interface vlan 100`
	`TS_switch(config-if)#`
		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 6	**ip address** *slot/port* **Example:** `TS_switch(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 7	[**no**] **shutdown** **Example:** `TS_switch(config-if)#` **no shutdown**	SVI をイネーブルにします。

ステップ 8	**exit**
	
	Example:
	`TS_switch(config-if)# exit`
	`TS_switch(config)#`
		VLAN インターフェイス コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 9	**cts role-based sgt-map vlan-list** *vlan_id* **sgt** *sgt_number* **Example:** TS_switch(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。
ステップ 10	**ip device tracking probe** [**count** *count* | **delay** *seconds* | **interval** *length*]	IP デバイス トラッキングをイネーブルにします。アクティブ ホストが検出されると、スイッチは IP デバイス トラッキング テーブルに次のエントリを追加します。 • ホストの IP アドレス • ホストの MAC アドレス • ホストの VLAN • スイッチがホストを検出したインターフェイス • ホスト ステート（アクティブまたは非アクティブ）
	Example: TS-switch(config)# **ip device tracking**	IP デバイス トラッキング テーブルに追加されたホストは、定期的な ARP プローブによって監視されます。応答が得られなかったホストがテーブルから削除されます。
ステップ 11	**exit** **Example:** TS_switch(config)# exit TS_switch#	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。
ステップ 12	**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**] **Example:** TS_switch# 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 13	**show ip device tracking {all|interface|ip|mac}** **Example:** TS_switch# show ip device tracking all	（任意）IP デバイス トラッキングの動作ステータスを確認します。
ステップ 14	**copy running-config startup-config** **Example:** TS_switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

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。

コマンド	目的
show ip device tracking	VLAN のアクティブ ホストの IP アドレスを識別する IP デバイスのトラッキングのステータスを表示します。
show cts role-based sgt-map	IP アドレスと SGT のバインディングを表示します。

これらのコマンドの出力フィールドの詳細については、第 7 章「Cisco TrustSec コマンドの概要」または『Cisco IOS 15.0SY Security and VPN Command Reference』を参照してください。

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例

次の例では、単一のホストは、アクセス スイッチ上の VLAN 100 に接続します。アクセス スイッチから Catalyst 6500 シリーズ TrustSec ソフトウェア対応スイッチにアクセス モードのリンクがあります。TrustSec スイッチ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 スイッチは 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。

ステップ 1　アクセス スイッチ上に VLAN 100 を作成します。

```
access_switch# config t
access_switch(config)# vlan 100
access_switch(config-vlan)# no shutdown
access_switch(config-vlan)# exit
access_switch(config)#
```

ステップ 2　アクセス リンクとして TrustSec スイッチ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_switch(config)# interface gigabitEthernet 6/3
access_switch(config-if)# switchport
access_switch(config-if)# switchport mode access
access_switch(config-if)# switchport access vlan 100
```

ステップ 3　TrustSec スイッチに VLAN 100 を作成します。

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

ステップ 4　着信 VLAN 100 のゲートウェイとして SVI を作成します。

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

ステップ 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_switch(config)# cts role-based sgt-map vlan 100 sgt 10
```

ステップ 6　TrustSec スイッチで IP デバイス トラッキングをイネーブルにします。それが動作していることを確認します。

```
TS_switch(config)# ip device tracking
TS_switch# 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
```

ステップ 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_switch# 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
```

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）

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トラフィックに直接 SGT を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 のバインディングを必要とする場合、IPM が優先されます。IP と SGT のバインディングのその他の競合は、「バインディング送信元プライオリティ」（P.3-21）にリストされている優先順位に従って解決されます。

L3IF-SGT マッピングの機能履歴

機能名	リリース	機能情報
L3IF と SGT のマッピング	15.0 (1) SY	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

デフォルト設定

デフォルト設定はありません。

L3IF と SGT のマッピングの設定

手順の詳細

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# cts role-based sgt-map interface` type *slot/port* [**security-group** *name* | **sgt** *number*] `Router(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 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show 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。

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 のバインディングを表示します。

入力ポートでの L3IF と SGT のマッピングの設定例

次の例では、Catalyst 6500 シリーズ スイッチ 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 SGT 3 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。

ステップ 1　インターフェイスを設定します。

```
Switch# config t
Switch(config)# interface gigabitEthernet 6/3 sgt 3
Switch(config)# exit
```

ステップ 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。

```
Router# 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
```

バインディング送信元プライオリティ

TrustSec は完全優先方式で IP-SGT バインディング 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*} CTS 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。

追加認証サーバ関連のパラメータの設定

スイッチと Cisco TrustSec サーバ間の相互対話を設定するには、次の作業を 1 つまたは複数行います。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# [no] cts server deadtime seconds`	（任意）いったん停止中としてマークされたグループ内のサーバを、どのくらいの期間、サービス用に選択してはいけないかを指定します。デフォルトは 20 秒です。指定できる範囲は 1 ～ 864000 です。
ステップ 3	`Router(config)# [no] cts server load-balance method least-outstanding [batch-size transactions] [ignore-preferred-server]`	（任意）Cisco TrustSec プライベート サーバ グループに RADIUS ロード バランシングをイネーブルにし、最も未処理のトランザクションが少ないサーバを選択します。デフォルトでは、ロード バランシングは適用されません。 デフォルトの *transactions* は 25 です。 **ignore-preferred-server** キーワードは、セッション全体を通じて同じサーバを使用しないようにスイッチに指示します。
ステップ 4	`Router(config)# [no] cts server test {server-IP-address | all} {deadtime seconds | enable | idle-time seconds}`	（任意）指定されたサーバまたはダイナミック サーバ リスト内のすべてのサーバに対してサーバ存続性テストを設定します。デフォルトでは、テストはすべてのサーバに対してイネーブルになっています。デフォルトの **idle-time** は 60 秒で、範囲は 1 ～ 14400 です。
ステップ 5	`Router(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 6	`Router# show cts server-list`	Cisco TrustSec サーバのリストのステータスおよび設定の詳細を表示します。

次に、サーバ設定を設定して Cisco TrustSec サーバ リストを表示する例を示します。

```
Router# configure terminal
Router(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Router(config)# cts server test all deadtime 20
Router(config)# cts server test all enable
Router(config)# cts server test 10.15.20.102 idle-time 120
Router(config)# exit

Router# show cts server-list
CTS Server Radius Load Balance = ENABLED
  Method     = least-outstanding
  Batch size = 50
  Ignore preferred server
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
```

```
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
                Status = ALIVE
                auto-test = TRUE, idle-time = 120 mins, deadtime = 20 secs
Installed list: SL1-1E6E6AE57D4E2A9B320D1844C68BA291, 3 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: SL2-1E6E6AE57D4E2A9B320D1844C68BA293, 3 server(s):
 *Server: 10.0.0.1, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
                Status = DEAD
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

認証サーバでの新規または交換パスワードの自動設定

リリース	機能の履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
15.0(1) SE	この機能が、Catalyst 3750(X) シリーズ スイッチに追加されました。

スイッチと認証サーバ間のパスワードを手動で設定する方法の代替方法として、スイッチからパスワード ネゴシエーションを開始できます。パスワード ネゴシエーションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# cts change-password server` *ip-address port* {**key** *secret* | **a-id** *a-id*}	スイッチと認証サーバ間のパスワード ネゴシエーションを開始します。 • *ip-address*：認証サーバの IP アドレス。 • *port*：認証サーバの UDP ポート。 • **key** *secret*：認証サーバの RADIUS 共有秘密。 • **a-id** *a-id*：認証サーバに関連付けられた A-ID。

CHAPTER 4

SGT 交換プロトコル over TCP（SXP）およびレイヤ 3 トランスポートの設定

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 SGT を伝播できます。ここでは、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。

ここでは、次の内容について説明します。

Cisco TrustSec SXP の設定

Cisco TrustSec SXP を設定するには、次の手順を実行します。

ステップ 1 Cisco TrustSec 機能をイネーブルにします（「アイデンティティ、接続および SGT の設定」の章を参照）。

ステップ 2 Cisco TrustSec SXP をイネーブルにします（「Cisco TrustSec SXP のイネーブル化」（P.4-2）を参照）。

ステップ 3 SXP ピア接続を設定します（「SXP ピア接続の設定」（P.4-2）を参照）。

Cisco TrustSec SXP のイネーブル化

ピアの接続を設定する前に、Cisco TrustSec SXP をイネーブルにする必要があります。Cisco TrustSec SXP をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# [no] cts sxp enable`	Cisco TrustSec の SXP をイネーブルにします。
ステップ 3	`Router(config)# exit`	コンフィギュレーション 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いない場合に、接続の SXP 送信元アドレスを設定しないと、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、スイッチから開始される各 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。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# cts sxp connection peer` *peer-ipv4-addr* `[source` *src-ipv4-addr*`] password {default | none} mode {local | peer} {speaker | listener} [vrf` *vrf-name*`]`	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**：指定モードはローカル デバイスを示します。 • **peer**：指定モードはピア デバイスを示します。 • **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 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show cts sxp connections`	（任意）SXP 接続情報を表示します。

次に、SXP をイネーブルにし、SwitchA（スピーカー）で SwitchB（リスナー）への SXP ピア接続を設定する例を示します。

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

次に、SwitchB（リスナー）で SwitchA（スピーカー）への SXP ピア接続を設定する例を示します。

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

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。スイッチのデフォルト SXP パスワードを設定できます。Cisco IOS Release 12.2(50)SY 以降では、SXP のデフォルト パスワードに暗号化されたパスワードを指定できます。

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。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`Router(config)# cts sxp default password [0 | 6 | 7] password`	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** またはオプションなしを使用）または暗号化パスワード（**6** または **7** オプションを使用）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 3	`Router(config)# exit#`	コンフィギュレーション モードを終了します。

次に、デフォルト SXP パスワードを設定する例を示します。

```
Router# configure terminal
Router(config)# cts sxp default password Cisco123
```

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。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`Router(config)# cts sxp default source-ip src-ip-addr`	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 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。

次に、SXP のデフォルトの送信元 IP アドレスを設定する例を示します。

```
Router# configure terminal
Router(config)# cts sxp default source-ip 10.20.2.2
```

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。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`Router(config)# cts sxp reconciliation period` *seconds*	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 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。

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。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`Router(config)# cts sxp retry period` *seconds*	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 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。

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

cts sxp log binding-changes グローバル コンフィギュレーション コマンドを実行すると、IP アドレスと SGT バインディングの変更（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。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`Router(config)# cts sxp log binding-changes`	IP と SGT のバインディングの変更のロギングをオンにします。

SXP 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
ステップ 1	Router# **show cts sxp connections** [**brief**]	SXP のステータスと接続を表示します。

次に、SXP 接続を表示する例を示します。

```
Router# 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
```

Cisco TrustSec ドメイン間のレイヤ 3 SGT トランスポートの設定

機能	履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。

Cisco TrustSec 対応のデバイスが存在しないネットワーク ドメインのエッジに Cisco TrustSec ゲートウェイ デバイスのレイヤ 3 SGT トランスポートを設定できます。

レイヤ 3 SGT トランスポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# [no] cts policy layer3 {ipv4 | ipv6} traffic acl-name`	（任意）認証サーバがトラフィック ポリシーをダウンロードするために使用できない場合に適用されるフォール バックのトラフィック ポリシーを指定します。 • *acl-name*：デバイスにすでに設定されている従来のインターフェイス ACL の名前。 この作業の次に記載されている追加の使用上の注意を参照してください。
ステップ 3	`Router(config)# [no] cts policy layer3 {ipv4 | ipv6} exception acl-name`	（任意）認証サーバが例外ポリシーをダウンロードするために使用できない場合に適用されるフォールバックの例外ポリシーを指定します。 この作業の次に記載されている追加の使用上の注意を参照してください。
ステップ 4	`Router(config)# interface type slot/port`	インターフェイスを指定し、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 5	`Router(config-if)# [no] cts layer3 {ipv4 | ipv6} trustsec forwarding`	（Cisco TrustSec 対応の物理ポートで設定）このインターフェイス上の出力トラフィックが、トラフィック ポリシーおよび例外ポリシーの決定に従って Cisco TrustSec レイヤ 3 SGT トランスポートのカプセル化を使用することを指定します。
	`Router(config-if)# [no] cts layer3 {ipv4 | ipv6} policy`	（ルーテッド ポートまたは SVI で設定）このインターフェイス上の出力トラフィックが、トラフィック ポリシーおよび例外ポリシーの決定に従って Cisco TrustSec レイヤ 3 SGT トランスポートのカプセル化を使用することを指定します。
ステップ 6	`Router(config-if)# end` `Router(config)# end`	インターフェイス コンフィギュレーション モードおよびグローバル コンフィギュレーション モードを終了します。
ステップ 7	`Router# show cts policy layer3 {ipv4 | ipv6}`	（任意）インターフェイスのレイヤ 3 SGT トランスポート設定を表示します。

Cisco TrustSec レイヤ 3 SGT トランスポートを設定する場合は、次の使用上のガイドラインおよび制約事項を考慮してください。

- Cisco TrustSec レイヤ 3 SGT トランスポート機能はハードウェア暗号化をサポートするポートだけで設定できます。
- Cisco TrustSec レイヤ 3 SGT トランスポートのトラフィック ポリシーおよび例外ポリシーには次の制限があります。
  - ポリシーは、IP 拡張または IP 名前付き拡張 ACL として設定する必要があります。
  - ポリシーには **deny** エントリを含めることはできません。

  - 同じ ACE がトラフィック ポリシーおよび例外ポリシーの両方に存在する場合は、例外ポリシーが優先されます。Cisco TrustSec レイヤ 3 カプセル化は、その ACE に一致するパケットで実行されます。

- トラフィック ポリシーおよび例外ポリシーは認証サーバからダウンロード（ご使用の Cisco IOS Release でサポートされている場合）するか、またはデバイスに手動で設定できます。ポリシーは次のルールに基づいて適用されます。
  - トラフィック ポリシーまたは例外ポリシーが認証サーバからダウンロードされる場合、手動で設定されたトラフィック ポリシーまたは例外ポリシーよりも優先されます。
  - 認証サーバが使用できず、トラフィック ポリシー、および例外ポリシーの両方を手動で設定すると、手動で設定されたポリシーが使用されます。
  - 認証サーバが使用できず、トラフィック ポリシーを例外ポリシーなしで設定すると、例外ポリシーは適用されません。Cisco TrustSec レイヤ 3 カプセル化がトラフィック ポリシーに基づいてインターフェイスに適用されます。
  - 認証サーバが使用できず、トラフィック ポリシーが手動で設定されていない場合は、Cisco TrustSec レイヤ 3 カプセル化がインターフェイスで実行されません。

次に、リモート Cisco TrustSec ドメインにレイヤ 3 SGT トランスポートを設定する例を示します。

```
Router# configure terminal
Router(config)# ip access-list extended traffic-list
Router(config-ext-nacl)# permit ip any 10.1.1.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended exception-list
Router(config-ext-nacl)# permit ip any 10.2.2.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# cts policy layer3 ipv4 traffic traffic-sgt
Router(config)# cts policy layer3 ipv4 exception exception-list
Router(config)# interface gi2/1
Router(config-if)# cts layer3 trustsec ipv4 forwarding
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

Cisco TrustSec 非対応スイッチング モジュールでの Cisco TrustSec リフレクタの設定

機能	履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。

（注）　Cisco TrustSec スーパーバイザの入力リフレクタおよび Cisco TrustSec 出力リフレクタは相互に排他的です。両方の機能をイネーブルにしないでください。

出力リフレクタは ERSPAN を設定する場合は無効にします。

Cisco TrustSec スーパーバイザの入力リフレクタ機能を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`Router(config)# [no] platform cts ingress`	Cisco TrustSec スーパーバイザの入力のリフレクタをアクティブにします。
ステップ 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show platform cts`	Cisco TrustSec リフレクタ モード（Ingress、Egress、Pure、または No CTS）を表示します。

次に、Cisco TrustSec 入力リフレクタを設定する例を示します。

```
Router# configure terminal
Router(config)# platform cts ingress
Router(config)# exit
Router# show platform cts
 CTS Ingress mode enabled
```

（注）　Cisco TrustSec 入力リフレクタをディセーブルにする前に、Cisco TrustSec 非対応スイッチング モジュールの電力を切る必要があります。

Cisco TrustSec 出力リフレクタ機能を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`Router(config)# [no] platform cts egress`	Cisco TrustSec 出力リフレクタをアクティブにします。
ステップ 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show platform cts`	Cisco TrustSec リフレクタ モード（Ingress、Egress、Pure、または No CTS）を表示します。

次に、Cisco TrustSec 出力リフレクタを設定する例を示します。

```
Router# configure terminal
Router(config)# platform cts egress
Router(config)# exit
Router# show platform cts
 CTS Egress mode enabled
```

（注）　Cisco TrustSec 出力リフレクタをディセーブルにする前に、Cisco TrustSec 非対応スイッチング モジュールの電力を切る必要があります。

Cisco TrustSec のキャッシングの設定

ここでは、次の内容について説明します。

Cisco TrustSec のキャッシングのイネーブル化

短時間停止から迅速にリカバリするために、Cisco TrustSec 接続の認証、許可、およびポリシー情報のキャッシングをイネーブルにできます。キャッシングすることで、Cisco TrustSec ドメインを完全に再認証しなくても、Cisco TrustSec デバイスが期限の切れていないセキュリティ情報を使用して停止後にリンクを復元できるようになります。Cisco TrustSec デバイスは DRAM にセキュリティ情報をキャッシュします。不揮発性（NV）ストレージもイネーブルにしている場合は、DRAM のキャッシュ情報も NV のメモリに保存されます。リブート中に NV のメモリの内容が DRAM に入力されます。

（注）　長時間の停止中に、Cisco TrustSec キャッシュ情報が期限切れになる可能性が高くなります。

Cisco TrustSec キャッシングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	`Router(config)# [no] cts cache enable`	DRAM への認証、許可、および環境データ情報のキャッシュをイネーブルにします。デフォルトでは無効になっています。 このコマンドの **no** 形式は DRAM および不揮発性ストレージからすべてのキャッシュ情報をクリアします。
ステップ 3	`Router(config)# [no] cts cache nv-storage {bootdisk: | bootflash: | disk0:} [directory dir-name]`	DRAM キャッシングをイネーブルにすると、DRAM のキャッシュ更新が不揮発性ストレージに書き込まれるようになります。また、デバイスの起動時に DRAM キャッシュが不揮発性ストレージから初期入力されるようになります。
ステップ 4	`Router(config)# exit`	コンフィギュレーション モードを終了します。

次に、不揮発性ストレージなどの、Cisco TrustSec キャッシングを設定する例を示します。

```
Router# configure terminal
Router(config)# cts cache enable
Router(config)# cts cache nv-storage bootdisk:
Router(config)# exit
```

Cisco TrustSec キャッシュのクリア

Cisco TrustSec 接続用のキャッシュをクリアするには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **clear cts cache** [**authorization-policies** [**peer**] | **environment-data** | **filename** *filename* | **interface-controller** [*type slot/port*]]	Cisco TrustSec 接続情報のキャッシュをクリアします。

次に、Cisco TrustSec キャッシュをクリアする例を示します。

```
Router# clear cts cache
```

CHAPTER 5

SGACL ポリシーの設定

SGACL ポリシーの設定

ここでは、次の内容について説明します。

SGACL ポリシーの設定プロセス

Cisco TrustSec の 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。

ステップ 1 SGACL ポリシーの設定は、主に Cisco Secure ACS または Cisco Identity Services Engine のポリシー管理機能を使用して行う必要があります（『*Configuration Guide for the Cisco Secure ACS*』または『*Cisco Identity Services Engine User Guide*』を参照）。

Cisco Secure ACS または Cisco ISE での SGACL ポリシー設定のダウンロードに AAA を使用していない場合、またはローカル ポリシーが短期間必要な場合は、SGACL のマッピングとポリシーを手動で設定することもできます（「SGACL ポリシーの手動設定」（P.5-3）および「SGACL ポリシーの手動設定」（P.5-3）を参照）。

（注） ACS から動的にダウンロードされた SGACL ポリシーは、競合のローカル定義されたポリシーよりも優先されます。

ステップ 2 ルーテッド ポートの出力トラフィックに対する SGACL ポリシーの強制をイネーブルにするには、「SGACL ポリシーの強制のイネーブル化」（P.5-2）に記載されているように、SGACL ポリシー強制をイネーブルにします。

ステップ 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 ポリシーの強制をイネーブルにするには、「VLAN に対する SGACL ポリシーの強制のイネーブル化」（P.5-2）の説明に従って、特定の VLAN に対して SGACL ポリシーの強制をイネーブルにします。

SGACL ポリシーの強制のイネーブル化

機能	履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。

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。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(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。

次に、Cisco TrustSec をイネーブルにしたルーテッド インターフェイスの SGACL ポリシーの強制をグローバルにイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# cts role-based enforcement
Router(config)# exit
```

VLAN に対する SGACL ポリシーの強制のイネーブル化

機能	履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。

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。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# cts role-based enforcement vlan-list` *vlan-list*	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。

次に、VLAN リスト内で、SGACL ポリシーの強制をイネーブルにする例を示します。

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

SGACL ポリシーの手動設定

機能	履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。

SGACL ポリシーの設定は、主に Cisco Secure ACS または Cisco ISE のポリシー管理機能を使用して行う必要がありますが、Cisco ACS または Cisco ISE が使用できないか、またはローカル ポリシーが短期間必要な場合は、スイッチで手動で SGACL ポリシーを設定できます。

（注）　ポリシーで使用する前に SGACL を作成する必要があります。

（注）　ACS から動的にダウンロードされた SGACL ポリシーは、競合のローカル定義されたポリシーよりも優先されます。

IPv4 ポリシーの設定

IPv4 SGACL ポリシーを手動で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# ip access-list role-based` *sgacl-name*	名前付き SGACL 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。

	コマンド	目的
ステップ 3	Router(config-rb-acl)# [*sequence-number* | **no**] {**permit** | **deny**} *protocol* [**option** *option-name*] {[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]} [**log**] [**fragments**]	SGACL 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。 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
	Router(config-rb-acl)# [*sequence-number* | **no**] [**permit** | **deny**] **icmp** [*icmp-type* [*icmp-code*] | *icmp-message*] {[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]} [**log**] [**fragments**]	
	Router(config-rb-acl)# [*sequence-number* | **no**] {**permit** | **deny**} **tcp** [**src** *operator* {*src-port*}+] [**dst** *operator* {*dst-port*}+] {[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]} [**log**] [**fragments**] [**established** | {{**match-any** | **match-all**} {{+ | -}*flag-name*}+]	
	Router(config-rb-acl)# [*sequence-number* | **no**] {**permit** | **deny**} **udp** [**src** *operator* {*src-port*}+] [**dst** *operator* {*dst-port*}+] {[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]} [**log**] [**fragments**]	
	Router(config-rb-acl)# [*sequence-number* | **no**] {**permit** | **deny**} **igmp** [*igmp-type*] {[**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*]} [**log**] [**fragments**]	
ステップ 4	Router(config-rb-acl)# **exit**	ACL コンフィギュレーション モードを終了します。

次に、IPv4 SGACL ポリシーを設定および確認する例を示します。

```
Router(config)# ip access-list role-based RBAC2
Router(config-rb-acl)# permit tcp src eq 10 dst eq 20
Router(config-rb-acl)# permit udp src range 3100 4200
Router(config-rb-acl)# end
Router# show ip access-lists RBAC2

Role-based IP access list RBAC2
    10 permit tcp src eq 10 dst eq ftp-data
    20 permit udp src range 3100 4200
```

IPv6 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。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# ipv6 access-list role-based sgacl-name`	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 3	`Router(config-ipv6rb-acl)# [no] {permit | deny} protocol [dest-option | dest-option-type {doh-number | doh-type}] [dscp cp-value] [flow-label fl-value] [mobility | mobility-type {mh-number | mh-type}] [routing | routing-type routing-number] [fragments] [log | log-input] [sequence seqno]`	IPv6 SGACL 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。 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 4	`Router(config-ipv6rb-acl)# exit`	IPv6 ACL コンフィギュレーション モードを終了します。

手動で SGACL ポリシーを適用する方法

機能	履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。

手動で SGACL ポリシーを適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# 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 2	`Router(config)# cts role-based permissions default [ipv4 | ipv6] sgacl-name1 [sgacl-name2 [sgacl-name3 ...]]]`	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 3	`Router(config)# 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 ～ 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。

次に、手動でデフォルトおよびカスタム SGACL ポリシーを適用する例を示します。

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

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。

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。

	コマンド	目的
ステップ 1	`Router# show cts role-based permissions default [ipv4 | ipv6 | details]`	デフォルト ポリシーの SGACL のリストを表示します。
	`Router# show cts role-based permissions [from {source-sgt | unknown}] [to {dest-sg | unknown}] [ipv4 | ipv6] [details]`	認証サーバからダウンロードされた、またはスイッチに手動で設定された SGACL を含め、許可マトリクスの内容を表示します。

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。

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。

```
Router# 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
```

ダウンロードされた SGACL ポリシーのリフレッシュ

認証サーバによりスイッチにダウンロードされた SGACL ポリシーをリフレッシュするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# cts refresh policy {peer [peer-id] | sgt [sgt_number| default|unknown]}`	認証サーバからの 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。

CHAPTER 6

エンドポイント アドミッション コントロールの設定

この章は、次の内容で構成されています。

エンドポイント アドミッション コントロールに関する情報

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、TrustSec ハードウェア対応デバイスでセキュリティ グループ ACL（SGACL）を適用することで、出力でフィルタリングされます。

認証および認可のエンドポイント 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。

表 6-1 に、TrustSec をサポートする Cisco Catalyst スイッチのコンフィギュレーション ガイドをリストします。この章の TrustSec に固有でないトピックはコンフィギュレーション ガイドでさらに詳しく説明します。

表 6-1　Cisco スイッチのコンフィギュレーション ガイド

コンフィギュレーション ガイド	URL
『Catalyst 3560 Software Configuration Guide, Release 12.2(52)SE』	http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_52_se/configuration/guide/3560scg.html
『Catalyst 3750 Switch Software Configuration Guide, 12.2(52)SE』	http://www9.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_52_se/configuration/guide/3750scg.html
『Catalyst 4500 Series Switch Software Configuration Guide, 12.2(53)SG』	http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/53SG/configuration/config.html
『Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide』	http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html
『Cisco IOS Security Configuration Guide: Securing User Services』	http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-0sy/secuser-15-0sy-library.html

基本的な EAC の設定シーケンス

1. 認証されたエンドポイント ホストに SGT をプロビジョニングするために、Cisco Secure ACS を設定します。
2. アクセス スイッチで SXP をイネーブルにします。SGT 交換プロトコル over TCP（SXP）およびレイヤ 3 トランスポートの設定の章を参照してください。
3. アクセス スイッチで 802.1X、MAB、または WebAuth 認証方式の任意の組み合わせをイネーブルにします。
4. アクセス スイッチで DHCP および IP デバイス トラッキングをイネーブルにします。

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。

```
Router(config)# dot1x system-auth-control
Router(config)# interface GigabitEthernet2/1
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
```

802.1x 認証の設定の詳細については、表 6-1 にリストされている、アクセス スイッチのコンフィギュレーション ガイドを参照してください。

802.1X 設定の確認

802.1X 認証設定を確認するには、**show authentication interface** コマンドを使用します。

```
Router# show authentication interface gigabitEthernet 2/1
*May  7 11:22:06: %SYS-5-CONFIG_I: Configured from console by console

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000904BBECD8

Available methods list:
  Handle  Priority  Name
    3        0      dot1x
Runnable methods list:
  Handle  Priority  Name
    3        1      dot1x
```

ポートが正常に認証されたことを確認するには、次のようにします。

```
Router# show dot1x interface gigabitEthernet 2/1 details

Dot1x Info for GigabitEthernet2/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 000c.293a.048e
Session ID                = AC1AD01F0000000904BBECD8
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
Port Status               = AUTHORIZED
```

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、Catalyst スイッチでの基本的な MAB 設定の例を示します。

```
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config-if)# mab
```

MAB 認証の設定の詳細については、表 6-1 にリストされている、アクセス スイッチのコンフィギュレーション ガイドを参照してください。

MAB 設定の確認

MAC 認証バイパスの設定を確認するには、**show authentication interface** コマンドを使用します。

```
switch# show authentication interface gigabitEthernet 2/1

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000A04CD41AC

Available methods list:
  Handle  Priority  Name
    2        1      mab
Runnable methods list:
  Handle  Priority  Name
    2        0      mab
```

ポートが認証に成功したことを確認するには、**show mab interface** コマンドを使用します。

```
switch# show mab interface gigabitEthernet 2/1 details
MAB details for GigabitEthernet2/1
-------------------------------------
Mac-Auth-Bypass           = Enabled

MAB Client List
---------------
Client MAC                = 000c.293a.048e
Session ID                = AC1AD01F0000000A04CD41AC
MAB SM state              = ACQUIRING
Auth Status               = UNAUTHORIZED
```

Web 認証プロキシの設定

Web 認証プロキシ（WebAuth）は、ユーザが 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。

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

Web ベース認証の設定の詳細については、表 6-1 にリストされている、アクセス スイッチのコンフィギュレーション ガイドを参照してください。

ip http server コマンドの詳細については、次の URL で『*Cisco IOS Network Management Command Reference*』のエントリを参照してください。

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_08.html#wp1022387

Web 認証プロキシ設定の確認

Web 認証プロキシの設定を確認するには、Web ブラウザを使用してインターフェイスの IP アドレスにアクセスします。正しく設定されていれば、それらのアクセス デバイスは身元証明要求を生成し、有効なログイン情報を受け入れます。

CLI で Web 認証プロキシの設定を確認するには、**show authentication interface** コマンドを使用します。

```
switch# show authentication interface gigabitEthernet 2/1

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000904BBECD8

Available methods list:
  Handle  Priority  Name
    1        2      webauth
Runnable methods list:
  Handle  Priority  Name
    1        0      webauth
```

柔軟な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

認証方式の 1 つ以上が利用可能でない場合、Flexible Authentication Sequence（FAS）では、フォールバック シーケンスを指定して、アクセス ポートが 802.1X、MAB、および WebAuth 認証方式で設定されるようにできます。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 および 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。

```
switch(config)# interface gigabitEthernet 2/1
switch(config-if)# authentication order mab dot1x webauth
switch(config-if)^Z
```

認証方式シーケンスの設定の詳細については、表 6-1 にリストされている、アクセス スイッチのコンフィギュレーション ガイドを参照してください。

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

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html

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

802.1x ホスト モードの設定の詳細については、表 6-1 にリストされている、アクセス スイッチのコンフィギュレーション ガイドを参照してください。

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。

認証前オープン アクセスの設定の詳細については、表 6-1 にリストされている、アクセス スイッチのコンフィギュレーション ガイドを参照してください。

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 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 スイッチで DHCP スヌーピングおよび IP デバイス トラッキングをイネーブルにします。

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 10
switch(config)# no ip dhcp snooping information option
switch(config)# ip device tracking
```

DHCP スヌーピングおよび IP デバイス トラッキングの設定に関する詳細については、表 6-1 にリストされている、アクセス スイッチのコンフィギュレーション ガイドを参照してください。

SGT とエンドポイント ホストのバインディングの確認

ホストが DHCP スヌーピングおよび IP デバイス トラッキングで表示されることを確認するには、**show ip dhcp snooping binding** および **show ip device tracking** コマンドを使用します。

```
switch# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:0C:29:3A:04:8E   10.252.10.10     84814       dhcp-snooping   10    GigabitEthernet2/1
Total number of bindings: 1


switch# show ip device tracking all
IP Device Tracking = Enabled
```

```
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------------
  IP Address     MAC Address       Interface           STATE
-----------------------------------------------------------------
10.252.10.10    000c.293a.048e GigabitEthernet2/1     ACTIVE
```

正しい SGT がエンドポイントの IP アドレスにバインドされていることを確認するには、**show cts role-based sgt-map** コマンドを使用します。

```
switch# show cts role-based sgt-map all
Active IP-SGT Bindings Information
IP Address   SGT Source
============================================
1.1.1.1       7 INTERNAL
10.252.10.1   7 INTERNAL
10.252.10.10  3 LOCAL
10.252.100.1  7 INTERNAL
172.26.208.31 7 INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of INTERNAL bindings = 4
Total number of active   bindings = 5
```

CHAPTER 7

Cisco TrustSec コマンドの概要

Cisco TrustSec 特権 EXEC コマンド	
cts change-password	AAA サーバのパスワード変更を開始します
cts credentials	キーストアに CTS デバイス ID およびパスワードを挿入します。
cts refresh	環境、ピアと RBACL ポリシーをリフレッシュします。
cts rekey	CTS SAP キーを再生成します
Cisco TrustSec グローバル コンフィギュレーション コマンド	
cts authorization list	CTS のグローバルな認証の設定を設定します。
cts cache	DRAM および NVRAM への TrustSec 許可および環境データ情報のキャッシュをイネーブルにします。
cts manual	CTS のキーストアの動作を定義します
cts policy layer3	CTS レイヤ 3 トランスポート ゲートウェイ インターフェイスのトラフィック ポリシーおよび例外ポリシーを指定します。
cts role-based	SGT への IP アドレス、L3 インターフェイス、VRF のマッピング。CTS のキャッシュおよび SGACL 強制をイネーブルにします。
cts server	RADIUS サーバのリストの設定を設定します。
cts sgt	ローカル デバイスのセキュリティ グループ タグを設定します。
cts sxp	TCP での SGT 交換を設定します。
CTS Flexible Netflow コマンド	
match flow cts	

CTS インターフェイス コンフィギュレーション コマンド

cts dot1x	CTS dot1x 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（config-if-cts-dot1x）。
cts layer3	トラフィック ポリシーおよび例外ポリシーをイネーブルにし、CTS のレイヤ 3 トランスポート ゲートウェイ インターフェイスに適用します。
cts manual	（config-if）CTS パラメータのフィードのローカル コンフィギュレーションを指定します
platform cts	TrustSec 出力または入力のリフレクタをイネーブルにします。

CTS dot1x サブモード コマンド

default（cts dot1x インターフェイス コンフィギュレーション サブモード）	CTS dot1x コマンドのデフォルトを復元します。
propagate（cts dot1x サブモード）	dot1x モードの SGT 伝搬をイネーブルまたはディセーブルにします。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
timer（cts do1x インターフェイス サブモード）	CTS のタイマーを設定します。

CTS 手動インターフェイス コンフィギュレーション サブモード コマンド

default（cts 手動インターフェイス コンフィギュレーション サブモード）	CTS 手動モードのデフォルト コンフィギュレーション復元します。
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS ポリシーを設定します
propagate（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS SGT 伝搬を設定します
sap（cts 手動インターフェイス サブモード）	手動モードの CTS SAP を設定します。

Cisco TrustSec クリア コマンド

clear cts cache	TrustSec キャッシュ ファイルをタイプごとまたはファイル名ごとにクリアするか、すべてのキャッシュ ファイルをクリアします。
clear cts counter	単一 TrustSec インターフェイスまたはすべてのインターフェイスのカウンタをクリアします
clear cts credentials	すべての PAC を含むすべての CTS クレデンシャルをクリアします。
clear cts environment-data	キャッシュからの TrustSec 環境データをクリアします。
clear cts macsec	指定されたインターフェイスの MACsec カウンタをクリアします。
clear cts pac	キーストアから 1 つまたはすべての PAC をクリアします。
clear cts role-based counters	SGT および DGT のロールベース アクセス コントロール強制の統計情報を表示します。

clear cts server	指定された認証サーバを削除します。
Cisco TrustSec Show コマンド	
show cts authorization entries	認可エントリを表示します。
show cts credentials	CTS 認証に使用するクレデンシャルを表示します。
show cts environment-data	CTS 環境データを表示します。
show cts interface	インターフェイスごとの CTS ステートおよび統計情報を表示します。
show cts macsec	インターフェイス単位の暗号 ASIC のパケット カウンタを表示します。
show cts pacs	キーストアの PAC の A-ID および PAC 情報を表示します。
show cts policy peer	TrustSec ピアのピア認可ポリシーを表示します。
show cts policy layer3	CTS レイヤ 3 トランスポートで使用されるトラフィック ポリシーおよび例外ポリシーを表示します。
show cts provisioning	未処理の CTS のプロビジョニング ジョブが表示されます
show cts role-based sgt-map	IP アドレスとセキュリティ グループ タグのマッピングを表示します。
show cts role-based counters	SGT および DGT のロールベース アクセス コントロール強制の統計情報を表示します。
show cts role-based sgt-map	IP と SGT のバインディング、許可リスト、および Netflow 統計情報を表示します。
show cts server-list	AAA サーバとロード バランシング設定のリストを表示します。
show cts sxp	CTS SXP プロトコル情報を表示します。
show platform cts reflector	インターフェイスごとの CTS のリフレクタのステータスを表示します。
エンドポイント アドミッション コントロール（EAC）を設定するコマンド	
aaa accounting	
aaa authorization	
aaa authentication	
order	
priority	
event	
periodic	
timer	
host-mode	
authorization	
accounting	
radius-server host	
authentication port-control	

debug コマンド	
debug authentication event	
debug authentication feature	
debug cts aaa	
debug cts authentication events	
debug cts authorization	
debug cts authorization events	
debug cts authorization rbacl	
debug cts authorization snmp	
debug cts cache	
debug cts coa events	
debug cts dp errors	
debug cts dp info	
debug cts dp packets	
debug cts environment-data	
debug cts environment-data events	
debug cts error	
debug cts fips	
debug cts ha	
debug cts ha core	
debug cts ha infra	
debug cts ifc	
debug cts ifc cache	
debug cts ifc events	
debug cts ifc snmp	
debug cts layer3-trustsec	
debug cts provisioning	
debug cts provisioning event	
debug cts provisioning pak	
debug cts relay event	
debug cts relay pak	
debug cts sap events	
debug cts sap packets	
debug cts sap pakdump	
debug cts server-list	
debug cts states	
debug cts sxp	
debug cts sxp conn	
debug cts sxp error	
debug cts sxp internal	

debug cts sxp mdb	
debug cts sxp message	
debug dot.1x	
debug epm	
debug event	
debug mab	
debug radius	
debug rbm api	
debug rbm cli	
debug rbm bindings	
debug rbm dp errors	
debug rbm dp events	
debug rbm dp packets	
debug rbm platform	
debug rbm policy	

cts authorization list

TrustSec シード デバイスで使用する AAA サーバのリストを指定するには、TrustSec シード デバイスで、グローバル コンフィギュレーション モードで **cts authorization** コマンドを使用します。認証中にリストの使用を停止するには、このコマンドの **no** 形式を使用します。

cts authorization list *server_list*

no cts authorization list *server_list*

構文の説明

server_list	Cisco TrustSec の AAA サーバ グループを指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、シード デバイスだけです。非シード デバイスは、TrustSec 環境データのコンポーネントとして TrustSec オーセンティケータのピアからの TrustSec AAA サーバ リストを取得します。

例

次の例は、TrustSec シード デバイスの AAA コンフィギュレーションを表示します。

```
Router# cts credentials id Switch1 password Cisco123
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network MLIST group radius
Router(config)# cts authorization list MLIST
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key
AbCe1234
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(config)# exit
```

関連コマンド

コマンド	説明
show cts server-list	RADIUS サーバ設定を表示します。

cts cache

DRAM および NVRAM への TrustSec 認可および環境データ情報のキャッシングをイネーブルにするには、**cts cache** 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。キャッシングをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **cts cache** {
　enable |
　nv-storage {**bootflash:** [*dir*] | **disk0:** [*dir*] | **disk1:** [*dir*] | **sup-bootflash:** [*image*]}

}

構文の説明

enable	CTS のキャッシュ サポートをイネーブルにします
nv-storage	DRAM キャッシュ更新が不揮発性ストレージに書き込まれるようにし、ネットワーク デバイスの起動時に nv ストレージから DRAM キャッシュが初期入力されるようにします。
bootflash: *dir*	nv ストレージの位置としてブートフラッシュ ディレクトリを指定します。
disk0: *dir*	nv ストレージの位置としてディスク 0 ディレクトリを指定します。
disk1: *dir*	nv ストレージの位置としてディスク 1 ディレクトリを指定します。
sup-bootflash: *image*	nv ストレージの位置としてスーパーバイザ ブートフラッシュのディレクトリを指定します。

デフォルト

デフォルトはキャッシュはディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2(50) SY	PMK キャッシュのサポートは、Catalyst 6500 シリーズ スイッチに追加されます。

使用上のガイドライン

cts cache コマンドは認証、許可、および環境データ情報の DRAM へのキャッシュをイネーブルにします。キャッシングは、認証および認可によって取得された情報のメンテナンスおよび再使用のためです。キーストアはデバイス自身のクレデンシャル（パスワード、証明書、PAC）のセキュアなストレージを、ソフトウェアまたは専用のハードウェア コンポーネントで提供します。専用のハードウェア キーストアがない場合、ソフトウェア エミュレーション キーストアは DRAM および NVRAM を使用して作成されます。

Cisco TrustSec では、各デバイスが信頼できる AAA サーバ（Cisco Secure ACS 5.1 以降）を使用して各自のネイバーを認証および認可してから、TrustSec ネットワークへのアクセスが承認されるように要求することで、ネットワーク デバイスのセキュア クラウドを作成します。認証および認可が完了すると、情報はしばらくの間有効です。キャッシングがイネーブルになっている場合、その情報は再利用できるため、ネットワーク デバイスは ACS に接続しなくてもリンクを起動できるため、リブート時に

CTS クラウドが素早く形成でき、ネットワークのアベイラビリティが向上して、ACS の負荷が低減します。キャッシングは揮発性メモリ（情報はリブート時に消える）または不揮発性メモリ（情報はリブート後も存続）に保存できます。

例

次に、キャッシュ サポートをイネーブルにする例を示します。

```
Router# config t
Router(config)# cts cache nv-storage disk0:
Router(config)# cts cache enable
```

関連コマンド

コマンド	説明
clear cts cache	キーストアの内容をクリアします。
show cts keystore	キーストアの内容を表示します。
cts rekey	
cts credentials	

cts change-password

ローカル デバイスと認証サーバの間でパスワードを変更するには、**cts change-password** 特権 EXEC コマンドを使用します。

cts change-password server *ipv4_address udp_port* {**a-id** *hex_string* | **key** *radius_key* } [**source** interface_list]

構文の説明

server	認証サーバを指定します。
ipv4_address	認証サーバの IP アドレス。
udp_port	認証サーバの UDP ポート。
a-id *hex_string*	ACS サーバの識別ストリングを指定します
key	プロビジョニングに使用する RADIUS キーを指定します
source	要求パケットの送信元アドレスのインターフェイスを指定します
interface_list	表示されたリストあたりのインターフェイス タイプおよび ID パラメータを指定します。

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンドの種類

次のコマンド構文を使用します

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

cts change-password コマンドにより、管理者は認証サーバを再設定しなくても、ローカル デバイスと Cisco Secure ACS 認証サーバ間で使用されるパスワードを変更することができます。

（注） **cts change-password** は、Cisco Secure ACS の 5.1 以降のバージョンでサポートされています。

デュアル スーパーバイザ シャーシの Catalyst 6500 では、2 つめのスーパーバイザのラインカードを挿入するときに、ハードウェア ベースのキーストアを手動で同期する必要があります。パスワード変更プロセスにより、アクティブおよびスタンバイ スーパーバイザに、同じデバイス パスワードが設定される場合があります。

cts credentials

ネットワーク デバイスの TrustSec ID およびパスワードを指定するには、特権 EXEC モードで **cts credentials** コマンドを使用します。クレデンシャルを削除するには、**clear cts credentials** コマンドを使用します。

cts credentials id *cts_id* **password** *cts_pwd*

構文の説明

credentials id *cts_id*	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用する Cisco TrustSec デバイス ID を指定します。*cts-id* 変数は、最大 32 文字で大文字と小文字を区別します。
password *cts_pwd*	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用するパスワードを指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）認証で使用する場合、**cts credentials** コマンドは、EAP-FAST を使用して別の Cisco TrustSec デバイスと認証を行う際に、このスイッチが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。CTS のクレデンシャル情報は startup-config ではなくキーストアに保存されているため、CTS のクレデンシャルの状態取得は不揮発性生成（NVGEN）プロセスでは実行されません。デバイスは、Cisco Secure Access Control Server（ACS）から CTS アイデンティティを割り当てられるか、ACS から要求されたときに新しいパスワードを自動生成するようにできます。これらのクレデンシャルは、キーストアで保存され、running-config を保存する必要性がなくなります。CTS デバイス ID を表示するには、**show cts credentials** コマンドを使用します。保存されたパスワードは表示されません。

デバイス ID またはパスワードを変更するには、コマンドを再入力します。キーストアをクリアするには、**clear cts credentials** コマンドを使用します。

（注） CTS デバイス ID が変更された場合、Protected Access Credential（PAC）は古いデバイス ID に関連付けられており、新しいアイデンティティに対しては有効でないため、すべての PAC はキーストアから消去されます。

例

次に、CTS デバイス ID を himalaya、パスワードを cisco に設定する例を示します。

```
Router# cts credentials id himalaya password cisco
```

```
CTS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

次に、CTS バイス ID を atlas、パスワードを cisco123 に変更する例を示します。

```
Router# cts credentials id atlas pacssword cisco123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y

TS device ID and password have been inserted in the local keystore. Please make sure that
the same ID and password are configured in the server database.
```

次に、CTS デバイス ID およびパスワード ステートを表示する例を示します。

```
Router# show cts credentials
CTS password is defined in keystore, device-id = atlas
```

関連コマンド

コマンド	説明
clear cts credentials	Cisco TrustSec デバイス ID とパスワードをクリアします。
show cts credentials	現在の Cisco TrustSec デバイス ID およびパスワードの状態を表示します。
show cts keystore	ハードウェアおよびソフトウェアのキーストアの内容を表示します。

cts dot1x

CTS dot1x インターフェイス コンフィギュレーション モード（config-if-cts-dot1x）を開始してインターフェイスの TrustSec 再認証タイマーを設定するには、**cts dot1x** コマンドを使用します。インターフェイス タイマーをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **cts dot1x**

構文の説明　このコマンドには、引数またはキーワードはありません。

デフォルト　インターフェイスの CTS dot1x コンフィギュレーションはデフォルトではディセーブルです。

コマンド モード　インターフェイス コンフィギュレーション（config-if）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン　TrustSec dot1x 再認証タイマーを設定する前に、インターフェイス コンフィギュレーション モードからインターフェイスからの dot1x をグローバルに設定します。CTS dot1x の設定は、TrustSec EAC プロセスではなく TrustSec NDAC を制御します。

例　次の例では、Catalyst 6500 シリーズ スイッチは最初に dot1x インターフェイス コンフィギュレーション モードをイネーブルにせずに CTS コンフィギュレーション モードを開始します。

```
Router(config-if)# cts dot1x
Warning: Global dot1x is not configured, CTS will not run until dot1x is enabled
. (Gi3/1)

Router(config-if-cts-dot1x)# ?
CTS dot1x configuration commands:
  default  Set a command to its defaults
  exit     Exit from CTS dot1x sub mode
  no       Negate a command or set its defaults
  timer    CTS timer configuration
```

関連コマンド

コマンド	説明
default timer reauthentication（cts インターフェイス）	CTS dot1x 再認証タイマーをデフォルト値にリセットします。
timer reauthentication（cts インターフェイス）	CTS dot1x 再認証タイマーを設定します。
show cts interface	CTS インターフェイスのステータスおよび設定を表示します。
show dotx interface	IEEE 802.1x の設定と統計情報を表示します。

default timer reauthentication（cts インターフェイス）

CTS dot1x 認証タイマーをデフォルト値にリセットするには、CTS インターフェイス コンフィギュレーション モードで **default timer reauthentication** コマンドを使用します。

default timer reauthentication

構文の説明

timer reauthentication	CTS 認証タイマーをデフォルト値に設定します。

デフォルト

3600 秒

コマンド モード

CTS インターフェイス コンフィギュレーション（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

CTS 再認証タイマーのデフォルト値はグローバルな dot1x 再認証のデフォルト（3600 秒）です。このタイマーが満了すると、デバイスは、CTS のネットワークに再認証します（NDAC）。

例

次に、グローバル デフォルト値に CTS 再認証タイマーをリセットする例を示します。

```
Router # configure terminal
Router(config)# interface gigabitEthernet 3/1
Router(config-if)# cts dot1x
Router(config-if-cts-dot1x)# default timer reauthentication
```

関連コマンド

コマンド	説明
cts dot1x	CTS dot1x 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（config-if-cts-dot1x）。
timer reauthentication（cts インターフェイス）	CTS 再認証タイマーを設定します。
show cts interface	CTS インターフェイスのステータスおよび設定を表示します。
show dotx interface	IEEE 802.1x の設定と統計情報を表示します。

timer reauthentication（cts インターフェイス）

再認証タイマーを設定するには、CTS インターフェイス コンフィギュレーション モードで **timer reauthentication** コマンドを使用します。タイマーをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **timer reauthentication** *seconds*

構文の説明

reauthentication *seconds*	再認証タイマーを設定します。

デフォルト

なし

コマンド モード

CTS インターフェイス コンフィギュレーション（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、TrustSec 再認証タイマーを設定します。このタイマーが満了すると、デバイスは、CTS のネットワークに再認証します（NDAC）。

例

次に、再認証タイマーを 44 秒に設定する例を示します。

```
Router(config-if-cts-dot1x)# timer reauthentication 44
```

関連コマンド

コマンド	説明
cts dot1x	CTS dot1x 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（config-if-cts-dot1x）。
default timer reauthentication（cts インターフェイス）	CTS dot1x 再認証タイマーをデフォルト値にリセットします。
show cts interface	CTS インターフェイスのステータスおよび設定を表示します。
show dotx interface	IEEE 802.1x の設定と統計情報を表示します。

cts layer3

CTS レイヤ 3 トランスポート ゲートウェイ インターフェイスをイネーブルに設定し、例外ポリシーとトラフィック ポリシーを適用するには、**cts layer 3** インターフェイス コンフィギュレーション コマンドを使用します。

cts layer3 {**ipv4** | **ipv6**} {**policy** | **trustsec forwarding**}

構文の説明

ipv4 | **ipv6**	IPv4 または IPv6 のいずれかを指定します
policy	ゲートウェイ インターフェイスにトラフィック ポリシーおよび例外ポリシーを適用します。
trustsec forwarding	ゲートウェイ インターフェイスの CTS レイヤ 3 トランスポートをイネーブルにします。

デフォルト

デフォルトでは CTS レイヤ 3 トランスポートは有効になっていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

いずれのトラフィック コマンドおよび例外コマンドを CTS レイヤ 3 ゲートウェイに適用するかを指定するには、**cts policy layer3** 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。CTS レイヤ 3 ゲートウェイ インターフェイスをイネーブルにして、トラフィック ポリシーおよび例外ポリシーを適用するには、**cts layer3** インターフェイス コンフィギュレーション コマンドを使用します。トラフィック ポリシーおよび例外ポリシーの詳細については、cts policy layer3 を参照してください。

例

次に、CTS レイヤ 3 トランスポート ゲートウェイ インターフェイスをイネーブルにする例を示します。

```
Router# config t
Router(config)# interface gigabitEthernet 6/1
Router(config-if)# cts layer3 ipv4 trustsec forwarding
Router(config-if)# cts layer3 ipv4 trustsec
Router(config-if)# cts layer3 ipv4 policy
```

関連コマンド

コマンド	説明
cts policy layer3	CTS レイヤ 3 トランスポートのトラフィック ポリシーおよび例外ポリシーを指定します。
show cts policy layer3	CTS レイヤ 3 トランスポート コンフィギュレーションで使用されるトラフィック ポリシーおよび例外ポリシーの名前を表示します。

cts manual

TrustSec 手動インターフェイス コンフィギュレーション サブモードを開始するには、**cts manual** インターフェイス コンフィギュレーション コマンドを使用します。

cts manual

構文の説明

このコマンドの構文はありません

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

リンクにポリシーおよびセキュリティ アソシエーション プロトコル（SAP）を設定する TrustSec 手動インターフェイス コンフィギュレーション サブモードを開始するには、**cts manual** インターフェイス コンフィギュレーション コマンドを使用します。**sap** または **policy** サブ コマンドが設定されていない場合、TrustSec にインターフェイスが設定されていないように見えます。

CTS 手動モードが設定された場合、802.1X 認証はリンクで実行されません。ポリシーを定義し、リンクに適用するには、**policy** サブコマンドを使用します。デフォルトは no policy です。MACsec リンク間暗号化を設定するには、SAP ネゴシエーション パラメータを定義する必要があります。デフォルトは no SAP です。同じ SAP PMK をリンクの両端で設定する必要があります（つまり、共有秘密）。

例

次に、CTS 手動モードを開始する例を示します。

```
router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# interface giga 2/1
router(config-if)# cts manual
router(config-if-cts-manual)# ?
CTS manual configuration commands:
  default    Set a command to its defaults
  exit       Exit from CTS manual sub mode
  no         Negate a command or set its defaults
  policy     CTS policy for manual mode
  propagate  CTS SGT Propagation configuration for manual mode
  sap        CTS SAP configuration for manual mode
```

関連コマンド

コマンド	説明
policy（cts 手動インターフェイス コンフィギュレーション サブモード)	
sap（cts 手動インターフェイス サブモード)	
show cts interface	

cts policy layer3

Cisco Secure ACS が使用できない場合、システムで CTS レイヤ 3 トランスポート用にトラフィック ポリシーと例外ポリシーを指定するには、**cts policy layer3** 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。

[**no**] **cts policy layer3 ipv4** {[**exception** *access_list*] | [**traffic** *access_list*]}

[**no**] **cts policy layer3 ipv6** {[**exception** *access_list*] | [**traffic** *access_list*]}

構文の説明

ipv4 exception *access_list*	（任意）IPv4 L3 のトラフィック ポリシーに例外を定義する定義済みの ACL を指定します。
ipv4 traffic *access_list*	IPv4 TrustSec をイネーブルにしたサブネットおよびゲートウェイをリストした定義済みの ACL を指定します。
ipv6 exception *access_list*	（任意）IPv6 L3 のトラフィック ポリシーに例外を定義する定義済みの ACL を指定します。
ipv6 traffic *access_list*	IPv6 TrustSec をイネーブルにしたサブネットおよびゲートウェイをリストした定義済みの ACL を指定します

デフォルト

デフォルトは no policy です。

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

CTS レイヤ 3 トランスポート機能は、TrustSec をイネーブルにしたネットワーク セグメントからのレイヤ 2 SGT タグ付きトラフィックが、アプリケーションにより非 TrustSec ネットワーク セグメントを経由して転送され、指定した CTS レイヤ 3 ゲートウェイでレイヤ 3 カプセル化が解除されるようにできます。トラフィック ポリシーは、すべての TrustSec をイネーブルにしたサブネットおよびこれに対応するゲートウェイ アドレスをリストしたアクセス リストです。例外ポリシーは、CTS レイヤ 3 トランスポートのカプセル化を適用しないトラフィックをリストするアクセス リストです。たとえば、ポリシーの取得に使用される RADIUS パケットは、クリアで送信する必要があります。

トラフィック ポリシーおよび例外ポリシーは、**cts policy layer3 {ipv4 | ipv6} traffic** *access_list* and the **cts policy layer3 {ipv4 | ipv6} exception** *access_list* グローバル コンフィギュレーション コマンドで指定します。CTS L3 ゲートウェイ インターフェイスにトラフィック ポリシーおよび例外ポリシーを適用するには、**cts layer3 {ipv4 | ipv6} policy** インターフェイス コンフィギュレーション コマンドを使用します。CTS L3 ゲートウェイ インターフェイスをイネーブルにするには、**cts layer3 {ipv4 | ipv6} trustsec forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

次のような使用上のガイドラインおよび制限を考慮して Cisco TrustSec レイヤ 3 SGT トランスポートを設定します。

- Cisco TrustSec レイヤ 3 SGT トランスポート機能はハードウェア暗号化をサポートするポートだけで設定できます。
- Cisco TrustSec レイヤ 3 SGT トランスポートのトラフィック ポリシーおよび例外ポリシーには次の制限があります。
  - ポリシーは、IP 拡張または IP 名前付き拡張 ACL として設定する必要があります。
  - ポリシーには **deny** エントリを含めることはできません。
  - 同じ ACE がトラフィック ポリシーおよび例外ポリシーの両方に存在する場合は、例外ポリシーが優先されます。Cisco TrustSec レイヤ 3 カプセル化は、その ACE に一致するパケットで実行されます。
- トラフィック ポリシーおよび例外ポリシーは認証サーバからダウンロード（ご使用の Cisco IOS Release でサポートされている場合）するか、または **ip access-list global** コンフィギュレーション コマンドを使用して、デバイスに手動で設定できます。ポリシーは次のルールに基づいて適用されます。
  - トラフィック ポリシーまたは例外ポリシーが認証サーバからダウンロードされる場合、手動で設定されたトラフィック ポリシーまたは例外ポリシーよりも優先されます。
  - 認証サーバが使用できず、トラフィック ポリシー、および例外ポリシーの両方を手動で設定すると、手動で設定されたポリシーが使用されます。
  - 認証サーバが使用できず、トラフィック ポリシーを例外ポリシーなしで設定すると、例外ポリシーは適用されません。Cisco TrustSec レイヤ 3 カプセル化がトラフィック ポリシーに基づいてインターフェイスに適用されます。
  - 認証サーバが使用できず、トラフィック ポリシーが手動で設定されていない場合は、Cisco TrustSec レイヤ 3 カプセル化がインターフェイスで実行されません。

例

次に、リモート Cisco TrustSec ドメインにレイヤ 3 SGT トランスポートを設定する例を示します。

```
Router# configure terminal
Router(config)# ip access-list extended traffic-list
Router(config-ext-nacl)# permit ip any 10.1.1.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended exception-list
Router(config-ext-nacl)# permit ip any 10.2.2.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# cts policy layer3 ipv4 traffic traffic-sgt
Router(config)# cts policy layer3 ipv4 exception exception-list
Router(config)# interface gi2/1
Router(config-if)# cts layer3 trustsec ipv4 forwarding
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

関連コマンド

コマンド	説明
cts layer3	トラフィック ポリシーおよび例外ポリシーをイネーブルにし、CTS のレイヤ 3 トランスポート ゲートウェイ インターフェイスに適用します。
show cts policy layer3	CTS レイヤ 3 トランスポートで使用されるトラフィック ポリシーおよび例外ポリシーを表示します。

cts refresh

すべてまたは特定の CTS ピアの TrustSec ピア認可ポリシーをリフレッシュするか、認証サーバによりスイッチにダウンロードされた SGACL ポリシーをリフレッシュするには、特権 EXEC モードで **cts refresh** コマンドを使用します。

cts refresh environment-data

cts refresh policy {**peer** [*peer_id*] | **sgt** [*sgt_number* | **default** | **unknown**] }

構文の説明

environment-data	環境データをリフレッシュします。
peer *Peer-ID*	（任意）*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 *sgt_number*	認証サーバからの SGACL ポリシーの即時リフレッシュを実行します。 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。
default	デフォルトの SGACL ポリシーをリフレッシュします。
unknown	未知の SGACL ポリシーをリフレッシュします。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドは、Catalyst 6500 シリーズ スイッチで **cts policy refresh** として追加されました。
12.2(50) SY	このコマンドは、Catalyst 6500 シリーズ スイッチで **cts refresh policy** に変更されました。**sgt**、**default**、および **unknown** キーワードが追加されました。

使用上のガイドライン

すべての TrustSec ピアのピア認可ポリシーをリフレッシュするには、ピア ID を指定しないで **cts policy refresh** を入力します。

ピア認可ポリシーは EAP-FAST NDAC 認証の成功の最後に Cisco ACS から最初にダウンロードされます。Cisco ACS はピア認可ポリシーを更新するように設定されていますが、**cts policy refresh** コマンドにより、Cisco ACS タイマーが期限切れになる前にポリシーの即時更新を強制できます。このコマンドは、セキュリティ グループ タグ（SGT）を適用でき、セキュリティ グループ アクセス コントロール リスト（SGACL）を強制できる TrustSec デバイスだけに関連します。

例

次に、すべてのピアの TrustSec ピア認可ポリシーをリフレッシュする例を示します。

```
Router# cts policy refresh
Policy refresh in progress
```

次に、すべてのピアの TrustSec ピア認可ポリシーを表示する例を示します。

```
VSS-1# show cts policy peer
CTS Peer Policy
===============
device-id of the peer that this local device is connected to
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE
```

関連コマンド

コマンド	説明
cts refresh	
clear cts policy	CTS ポリシーをすべてクリアするか、ピア ID または SGT により単独でクリアします。
show cts policy peer	すべてまたは特定の TrustSec ピアのピア認可ポリシーが表示されます。

cts rekey

セキュリティ アソシエーション プロトコル（SAP）で使用する Pairwise Master Key を再生成するには、**cts rekey** 特権 EXEC コマンドを使用します。

構文の説明

interface type *slot*/*port*	SAP キーを再生成する CTS インターフェイスを指定します。

デフォルト

デフォルト値はありません。

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	このコマンドが、Catalyst 4500 シリーズ スイッチに追加されました。
IOS 15.0(1) SE	このコマンドが、Catalyst 3000 シリーズ スイッチに追加されました。

使用上のガイドライン

SAP の Pairwise Master Key（PMK）リフレッシュは通常、ネットワーク イベントおよび Dot1X 認証に関連する設定不可能な内部タイマーの組み合わせによりトリガーされ、自動的に行われます。暗号キーを手動で更新する機能は、多くの場合、ネットワーク アドミニストレーションのセキュリティ要件の一部です。手動で PMK のリフレッシュを強制するには、**cts rekey** コマンドを使用します。

TrustSec は、Dot1X 認証でスイッチ間のリンク間暗号化を作成する必要のない手動コンフィギュレーション モードをサポートします。この場合、PMK は、**sap pmk** CTS 手動インターフェイス コンフィギュレーション コマンドを使用してリンクの両端のデバイスで手動で設定されます。

例

次の例では、指定したインターフェイスの PMK を再生成します。

```
switch# cts rekey interface gigabitEthernet 2/1
switch#
```

関連コマンド

コマンド	説明
sap（cts 手動インターフェイス サブモード）	
show cts	

cts role-based

SGT のインポジション、TrustSec NetFlow パラメータと SGACL 強制を手動で設定するには、**cts role-based** 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。コンフィギュレーションを削除するには、コマンドの **no** 形式を使用します。

[**no**] **cts role-based enforcement** [**vlan-list** {*vlan-ids* | **all**}]

[**no**] **cts role-based** {**ip** | **ipv6**} **flow monitor fnf-ubm dropped**

[**no**] **cts role-based ipv6-copy**

[**no**] **cts role-based l2-vrf** *instance_name* **vlan-list** *vlan-ids* [**all**]

[**no**] **cts role-based permissions default** {*access-list* | **ipv4** | **ipv6**} *access-list access-list . . .*

[**no**] **cts role-based permissions from** {*sgt* | **unknown to** {*sgt* | **unknown**}} {*access-list* | **ipv4** | **ipv6**} *access-list , access-list, . . .*

[**no**] **cts role-based sgt-caching vlan-list** {*vlan_ids* | **all**}

[**no**] **cts role-based sgt-caching with-enforcement**

[**no**] **cts role-based sgt-map** {i*pv4_netaddress* | *ipv6_netaddress*} | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map** {i*pv4_netaddress/prefix* | *ipv6_netaddress/prefix*} | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map host** {i*pv4_hostaddress* | *ipv6_hostaddress* | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map vrf** *instance_name* {*ip4_netaddress* | *ipv6_netaddress* | **host** {*ip4_address* | *ip6_address*}}] **sgt** *sgt_number*

[**no**] **cts role-based sgt-map interface** interface_type *slot*/*port* {**security-group** | **sgt**} *sgt_number*

[**no**] **cts role-based sgt-map vlan-list** [*vlan_ids*| **all**] *slot*/*port* **sgt** *sgt_number*

構文の説明

l2-vrf *instance_name*	（任意）レイヤ 2 VRF インスタンス名を指定します。
enforcement	すべてのレイヤ 3 CTS インターフェイスのローカル デバイスの SGACL 強制をイネーブルにします。
interface interface_type	指定 SGT はこの論理または物理レイヤ 3 インターフェイスからのトラフィックにマッピングされます。
vlan-list *vlan-ids*	VLAN ID を指定します。各 VLAN ID はカンマで区切られ、ID の範囲はハイフンで指定されます。
all	（任意）すべての VLAN ID を指定します。
with-enforcement	SGACL 強制がイネーブルの SGT キャッシングをイネーブルにします。
sgt-map *ipv4_netaddress* | *ipv6_netaddress*	（任意）SGT に関連付けるネットワークを指定します。IPv4 アドレスをドット付き 10 進数表記で、IPv6 をコロン 16 進数表記で入力します。
sgt-map *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix*	（任意）SGT が、指定したサブネット アドレス（IPv4 または IPv6）のすべてのホストにマッピングされるように指定します。IPv4 はドット付き 10 進数 CIDR 表記で、IPv6 はコロン 16 進数表記で指定されます。*（0 ～ 128）*

sgt-map host *ipv4_hostaddress* | *ipv6_hostaddress*	指定したホスト IP アドレスと指定した SGT をバインドします。IPv4 アドレスをドット付き 10 進数表記で、IPv6 をコロン 16 進数表記で入力します。
sgt *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。
vrf *instance_name*	以前デバイスで作成した VRF インスタンスを指定します。

デフォルト　なし

コマンド モード　グローバル コンフィギュレーション（config）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが、Catalyst 3750(E)、3560(E)、および 3750(X) シリーズ スイッチに追加されました（**vrf** または IPv6 サポートなし）。
12.2(50) SY	次のキーワードは、Catalyst 6500 シリーズ スイッチに追加されました。 • [no] cts role-based enforcement • [no] cts role-based ip flow monitor user-defined-monitor dropped • [no] cts role-based ipv6 flow monitor user-defined-monitor dropped • [no] cts role-based ipv6 copy • [no] cts role-based permissions
15.0(0) SY	次のキーワードは、Catalyst 6500 シリーズ スイッチに追加されました。 • [no] cts role-based sgt-map interface • [no] cts role-based sgt-map vlan-list

使用上のガイドライン　自動的に SGT を送信元 IP アドレスにマッピングするための、Cisco Identity Services Engine、Cisco Secure ACS、ダイナミック ARP インスペクション、DHCP スヌーピング、ホスト トラッキングがスイッチで使用できない場合、**cts role-based sgt-map** コマンドを使用して SGT を次の内容にマッピングできます。

- 単一ホストの IPv4 または IPv6 アドレス
- IPv4 または IPv6 ネットワークまたはサブネットワーク上のすべてのホスト
- VRF
- 単一または複数の VLAN
- レイヤ 3 物理または論理インターフェイス

単一のホスト アドレスと SGT のバインディング

cts role-based sgt-map host コマンドは、IP 送信元アドレスが指定ホスト アドレスが一致した場合に、この着信パケットに指定 SGT をバインドします。この IP-SGT バインディングは優先順位が最も低く、他の送信元から動的に検出されたその他のバインディング（SXP またはローカルで認証済みホストなど）が存在する場合は無視されます。バインディングは、SGT インポジションおよび SGACL 強制用にスイッチ上でローカルに使用されます。このバインディングが指定したホスト IP アドレスに認識される唯一のバインディングである場合、これが SXP ピアにエクスポートされます。

ネットワークまたはサブネットワーク アドレスと SGT のバインディング

cts role-based sgt-map *ipv4_netaddress* | *ipv6_netaddress* および **cts role-based sgt-map** *ipv4_subnetaddress/prefix* | *ipv6_subnetaddress/prefix* コマンドは、指定したネットワーク アドレス範囲内のパケットに、指定した SGT をバインドします。

SXP は指定されたネットワークまたはサブネットワーク内のすべての可能な個別 IP-SGT バインディングの包括的な拡張をエクスポートします。IPv6 バインディングとサブネット バインディングは SXP バージョン 2 以降の SXP リスナー ピアだけにエクスポートされます。

VRF と SGT のバインディング

vrf キーワードは、以前に **vrf definition** グローバル コンフィギュレーション コマンドで定義された仮想ルーティングおよびフォワーディング テーブルを指定します。VRF コンテキストの設定はこのマニュアルの範囲外です。**cts role-based sgt-map vrf** 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た IP-SGT バインディングは、指定された VRF と、入力された 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。

VLAN と SGT のマッピング

cts role-based sgt-map vlan-list コマンドは、SGT を指定された VLAN または VLAN のセットにバインドします。キーワード **all** は、スイッチでサポートされている VLAN の全範囲と同じで、不揮発性生成（NVGEN）プロセスで保持されません。指定 SGT は指定した VLAN のいずれかで受信した着信パケットにバインドされます。

レイヤ 3 インターフェイス マッピング（L3IF）

cts role-based sgt-map interface コマンドは、指定したレイヤ 3 論理インターフェイスをセキュリティ グループの名前または SGT にバインドします。セキュリティ グループの名前に SGT をマッピングするセキュリティ グループ情報テーブルは、TrustSec 環境データと一緒に認証サーバからダウンロードされます。**cts role-based sgt-map interface security-group** コマンドは、セキュリティ グループの名前のテーブルが使用できない場合は拒否されます。

セキュリティ グループのテーブルが初めてダウンロードされるか更新されるたびに、すべての L3IF マッピングは再処理されます。指定されたインターフェイスを経由する出力パスを持つすべてのネットワーク プレフィックスに対して、IP-SGT バインディングが追加、更新、または削除されます。

バインディング送信元プライオリティ

TrustSec は完全優先方式で、マスター バインディング データベースの IP-SGT バインディング ソース間の競合を解決します。たとえば、SGT も **policy** {**dynamic identity** *peer-name* | **static sgt** *tag*} cts interface コマンドでインターフェイスに適用される場合があります（アイデンティティ ポート マッピング）。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. 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。

L2 VRF の割り当て

[**no**] **cts role-based l2-vrf vrf-name vlan-list** {**vlan-list** | **all**} グローバル コンフィギュレーション コマンドでは、**vlan-list** 引数には単一の VLAN ID、カンマで区切った VLAN ID のリスト、またはハイフンで区切った VLAN ID の範囲を指定できます。

キーワード **all** は、ネットワーク デバイスによってサポートされている VLAN の全範囲と同等です。キーワード **all** は、不揮発性生成（NVGEN）プロセスで保持されません。

cts role-based l2-vrf コマンドが同じ VRF に複数回実行する場合、入力される連続した各コマンドは、指定された VRF に指定された VLAN ID を追加します。

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ディングが 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 バインディングは、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。

ロールベースの強制

システムの CTS をイネーブルにしたレイヤ 3 インターフェイスの SGACL 強制をグローバルにイネーブルまたはディセーブルにするには、[**no**] **cts role-based enforcement** コマンドを使用します。

（注）　CTS の CLI コマンドの説明に表示されるロールベース アクセス コントロールおよびロールベース ACL は、Cisco TrustSec マニュアルのセキュリティ グループ アクセス コントロール リスト（SGACL）に相当します。

VLAN 強制

SVI インターフェイス上でのレイヤ 2 スイッチド パケットと L3 スイッチド パケットに対する SGACL 強制をイネーブルまたはディセーブルにするには、[**no**] **cts role-based enforcement vlan-list** {*vlan-ids* | **all**} コマンドを使用します。

vlan-ids 引数には単一の VLAN ID、VLAN ID リスト、または VLAN ID 範囲を指定できます。複数のエントリはハイフン「-」またはカンマ「,」で区切ります。

キーワード **all** は、プラットフォームによってサポートされている VLAN の全範囲と同等です（たとえば、Catalyst 6500 VLAN 範囲は 1 ～ 4094 です）。複数のコマンドを発行すると、付加的な効果があります。SGACL が指定されたすべてのリストのすべての VLAN に適用されます。キーワード **all** は、不揮発性生成（NVGEN）プロセスで保持されません。

（注） デフォルトでは、SGACL 強制は VLAN でイネーブルではありません。VLAN の SGACL 強制をイネーブルにするためには、**cts role-based enforcement vlan-list** コマンドを発行する必要があります。

（注） ロールベース アクセス コントロール（RBAC）が強制されている VLAN で SVI がアクティブである場合、RBAC はその VLAN 内のレイヤ 2 およびレイヤ 3 の両方のスイッチド パケットに対して強制されます。レイヤ 3 スイッチングは SVI を使用しない VLAN 内では使用できないため、SVI を使用しない場合、RBAC はレイヤ 2 スイッチド パケットのみに対して強制されます。

Flexible NetFlow

標準の 5 タプル フロー オブジェクトを使用してフロー レコードに SGT および DGT フロー オブジェクトが設定されている場合、Flexible NetFlow は、SGACL 強制によってドロップされたパケットに対応できます

flow record および **flow exporter** 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フロー レコードおよびフロー エクスポータを設定してから、それらを **flow monitor** コマンドを使用してフロー モニタに追加します。**show flow** show コマンドを使用して設定を確認します。

SGACL のドロップされたパケットだけを収集するには、**[no] cts role-based {ip | ipv6} flow monitor dropped** 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。

Flexible NetFlow の概要および設定の詳細については、次のマニュアルを参照してください。

『Getting Started with Configuring Cisco IOS Flexible NetFlow』

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html

『Cisco IOS Flexible Netflow Configuration Guide, Release 15.0SY』

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-0sy/fnf-15-0sy-book.html

例

次の例では、Catalyst 4500 シリーズ スイッチが、ホスト IP アドレス 10.1.2.1 を SGT 3 に、10.1.2.2 を SGT 4 にバインドしてから、**show** コマンドで確認します。これらのバインディングは、SXP によって SGACL 強制のスイッチに転送されます。

```
cat4k# (config)# cts role-based sgt-map host 10.1.2.1 sgt 3
cat4k(config)#cts role-based sgt-map host 10.1.2.2 sgt 4

cat4k# show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address    SGT  Source
============================================
10.1.2.1       3   CLI
10.1.2.2       4   CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of active   bindings = 2
```

次の例では、Catalyst 6500 シリーズで、VLAN 57、および 89 ～ 101 を VRF l2ipv4 に割り当てます。VRF は **vrf** グローバル コンフィギュレーション コマンドで作成済みです。

```
Cat6k(config)# cts role-based l2-vrf l2ipv4 vlan-list 57, 89-101
```

関連コマンド

コマンド	説明
cts sxp	ネットワーク デバイスに SXP を設定します。
cts sgt	ローカル デバイスのセキュリティ グループ タグを設定します。
show cts role-based sgt-map	ロールベース アクセス コントロール情報を表示します

cts server

RADIUS サーバ グループのロード バランシングを設定するには、グローバル コンフィギュレーション モードで **cts server** コマンドを使用します。ロード バランシングをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **cts server deadtime** *timer_secs*

[**no**] **cts server key-wrap enable**

[**no**] **cts server load-balance method least-outstanding** [**batch-size** *transactions*] [**ignore-preferred-server**]

[**no**] **cts server test** {*ip4_address* | **all**} {**deadtime** *seconds* | **enable** | **idle-time** *minutes*}

構文の説明

deadtime *timer_secs*	いったん停止中としてマークされたグループ内のサーバを、どのくらいの期間、サービス用に選択してはいけないかを指定します。デフォルトは 20 秒です。指定できる範囲は 1 ～ 864000 です。
load-balance method least-outstanding	Cisco TrustSec プライベート サーバ グループに RADIUS ロード バランシングをイネーブルにし、最も未処理のトランザクションが少ないサーバを選択します。デフォルトでは、ロード バランシングは適用されません。
batch-size *transactions*	（任意）バッチごとに割り当てられるトランザクションの数。デフォルトの *transactions* は 25 です。 **（注）** バッチ サイズがスループットと CPU の負荷に影響する場合があります。デフォルト バッチ サイズの 25 の使用を推奨します。これは、CPU の負荷に悪影響を及ぼさない、高スループットに最適化されているためです。
ignore-preferred-server	（任意）セッション全体を通じて同じサーバを使用しないようにスイッチに指示します。
test {*ip4_address* | **all** {**deadtime** *seconds* | **enable** | **idle-time** *minutes* } }	指定された RADIUS サーバまたはダイナミック サーバ リスト内のすべてのサーバに対してサーバ存続性テストを設定します。デフォルトでは、テストはすべてのサーバに対してイネーブルになっています。デフォルトの **deadtime** は 20 秒です。指定できる範囲は 1 ～ 864000 秒です。デフォルトの **idle-time** は 60 秒で、範囲は 1 ～ 14400 秒です。
key-wrap enable	TrustSec の RADIUS サーバ通信に対して、AES キーラップの暗号化をイネーブルにします。

デフォルト

Deadtime	20 秒
Batch-size	25 トランザクション
test idle-time	60 秒

コマンド モード　グローバル コンフィギュレーション（config）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2(50) SY	**key-wrap** キーワードは、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン　スイッチを FIPS モードで稼働させる場合は、**key-wrap** キーワードを使用します。

RADIUS サーバ ロード バランシングの情報は次の URL で入手できます。

http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sbrdldbl.html

例　次に、サーバ設定を設定して Cisco TrustSec サーバ リストを表示する例を示します。

```
Router# configure terminal
Router(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Router(config)# cts server test all deadtime 20
Router(config)# cts server test all enable
Router(config)# cts server test 10.15.20.102 idle-time 120
Router(config)# exit

Router# show cts server-list
CTS Server Radius Load Balance = ENABLED
  Method     = least-outstanding
  Batch size = 50
  Ignore preferred server
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
                Status = ALIVE
                auto-test = TRUE, idle-time = 120 mins, deadtime = 20 secs
Installed list: SL1-1E6E6AE57D4E2A9B320D1844C68BA291, 3 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: SL2-1E6E6AE57D4E2A9B320D1844C68BA293, 3 server(s):
 *Server: 10.0.0.1, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
                Status = DEAD
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

関連コマンド

コマンド	説明
show cts server-list	AAA サーバとロード バランシング設定のリストを表示します。

cts sgt

手動でネットワーク デバイスにセキュリティ グループ タグ（SGT）番号を割り当てるには、グローバル コンフィギュレーション モードで **cts sgt** コマンドを使用します。タグを削除するには、コマンドの **no** 形式を使用します。

[**no**] **cts sgt** *tag-number*

構文の説明

tag-number	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。

デフォルト

SGT 番号が割り当てられません。

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが Catalyst 3750(E) および 3560(E) シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが、Catalyst 3750(X) シリーズ スイッチに追加されました。

使用上のガイドライン

通常の Cisco TrustSec 動作では、認証サーバ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。

例

次に、ネットワーク デバイスの SGT を手動で設定する例を示します。

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

関連コマンド

コマンド	説明
show cts environment-data	CTS 環境データを表示します。

cts sxp

ネットワーク デバイスに SXP を設定するには、**cts sxp** 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。このコマンドは、SXP をイネーブルにし、SXP パスワード、ピアのスピーカーとリスナー関係および復帰期間を決定します。また、バインディング変更のログのオン/オフを切り替えます。SXP コンフィギュレーションをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **cts sxp connection peer** *ip4_address* **password** {**default | none**} **mode** {**local | peer**} [**speaker | listener**] [**vrf** *vrf_name*]

[**no**] **cts sxp connection peer** *ip4_address* **source** *ip4_address* **password** {**default | none**} **mode** {**local | peer**} [**speaker | listener**] [**vrf** *vrf_name*]

[**no**] **cts sxp default password** {**0** *unencrypted_pwd* **| 6** *encrypted_key* **| 7** *encrypted_key* **|** *cleartext_pwd* }

[**no**] **cts sxp default source-ip** *ip4_address*

[**no**] **cts sxp enable**

[**no**] **cts sxp log binding-changes**

[**no**] **cts sxp mapping network-map** *bindings*

[**no**] **cts sxp reconciliation period** *seconds*

[**no**] **cts sxp retry period** *seconds*

構文の説明

connection peer *ip4_address*	ピア SXP アドレスを指定します。
password {default | none}	次のオプションを使用して、SXP がピア接続で使用するパスワードを指定します。 • **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ません。 パスワードの最大長は 32 文字です。
mode {local | peer}	リモート ピア デバイスのロールを指定します。 • **local**：指定モードはローカル デバイスを示します。 • **peer**：指定モードはピア デバイスを示します。
network-map *bindings*	0 ～ 65535。IP-SGT タギングおよびエクスポートのサブネットを拡張する場合は許可される、SGT にバインディングできるサブネット ホスト アドレスの最大数。拡張なしにするには 0 を入力します。
speaker | listener	**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。
vrf *vrf_name*	（任意）ピアの VRF を指定します。デフォルトはデフォルト VRF です。

default password **0** *unencrypted_pwd* | **6** *encrypted_key* | **7** *encrypted_key* | *cleartext_pwd*	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** またはオプションなしを使用）または暗号化パスワード（**6** または **7** オプションを使用）を入力できます。パスワードの最大長は 32 文字です。
source-ip *ip4_address*	（任意）送信元デバイスの 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。
enable	Cisco TrustSec で SGT 交換プロトコル over TCP（SXP）イネーブルにします。
log binding-changes	IP と SGT のバインディングの変更のロギングをオンにします。デフォルトはオフです。
reconciliation period *seconds*	SXP 復帰タイマーを変更します。範囲は 0 ～ 64000 です。デフォルトは 120 秒（2 分）です。
retry period *seconds*	SXP リトライ タイマーを変更します。範囲は 0 ～ 64000 です。デフォルト値は 120 秒（2 分）です。

デフォルト

sxp	デフォルトでディセーブル
log binging-changes	off
password	none
reconciliation period	120 秒
retry period	60 秒
source-ip	デフォルトの送信元 IP アドレス（設定されている場合）またはポート アドレス
VRF	デフォルトの VRF 名

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドは、Catalyst 3750(E) および 3560(E) シリーズ スイッチに追加されました（**log binding-changes** キーワードなし）。
12.2 (53) SE2	このコマンドは、Catalyst 3750(X) シリーズ スイッチに追加されました（**log binding-changes** キーワードなし）。
12.2 (50) SY	**mapping** キーワードが追加されました。

使用上のガイドライン

ピアへの SXP 接続が **cts sxp connection peer** コマンドを使用して設定された場合、接続モードだけを変更できます。**vrf** キーワードは任意です。VRF 名が指定されていない、または VRF 名が「default」という名前で指定されている場合、接続はデフォルト ルーティングまたはフォワーディング ドメインで設定されます。

SXP 接続パスワードのデフォルト設定は **none** です。SXP 接続は IP アドレスごとに設定されるため、複数のピアを持つデバイスは、できるだけ多くの SXP 接続を持つことができます。**cts sxp default password** コマンドは、デバイスに設定されているすべての SXP 接続に任意で使用するデフォルト SXP パスワードを設定します。SXP パスワードは、**0 | 7 | 6** *encrypted_key* 暗号化タイプ オプションを使用してクリア テキストまたは暗号化したものを使用します。デフォルトはタイプ 0（クリア テキスト）です。暗号化タイプが 6 または 7 である場合、暗号化の password 引数は、有効なタイプ 6 またはタイプ 7 の暗号テキストである必要があります。SXP パスワードを削除するには、**no cts sxp default password** コマンドを使用します。

cts sxp default source-ip コマンドは、送信元 IP アドレスが指定されていない場合に、SXP が新規の TCP 接続すべてに使用するデフォルトの送信元 IP アドレスを設定します。既存の TCP 接続は、このコマンドが入力されても影響を受けません。SXP 接続は 3 台のタイマーによって制御されます。

- 再試行タイマー
- 削除のホールドダウン タイマー
- 復帰タイマー

再試行タイマー

再試行タイマーは、少なくとも 1 つの SXP 接続が稼働していない場合にトリガーされます。このタイマーの期限が切れると新しい SXP 接続が試行されます。このタイマー値を設定するには、**cts sxp retry period** コマンドを使用します。デフォルト値は 120 秒です。指定できる範囲は 0 ～ 64000 秒です。ゼロの値は、再試行が発生しなくなります。

削除のホールドダウン タイマー

削除のホールドダウン タイマー値は設定できず、120 秒に設定されています。このタイマーは、SXP リスナー接続がダウンするとトリガーされます。ダウンした接続から学習した IP-SGT マッピングは、このタイマーが期限切れになると削除されます。削除のホールドダウン タイマーが期限切れになる前にダウンした接続が復元された場合、復帰タイマーが開始されます。

復帰タイマー

ピアが SXP 接続を終了すると、内部の削除のホールドダウン タイマーが開始されます。削除のホールドダウン 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。このタイマーを設定するには、**cts sxp reconciliation period** コマンドを使用します。

例

次に、SXP をイネーブルにし、SwitchA（スピーカー）で SwitchB（リスナー）への SXP ピア接続を設定する例を示します。

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

次に、SwitchB（リスナー）で SwitchA（スピーカー）への SXP ピア接続を設定する例を示します。

```
SwitchB# configure terminal
```

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

関連コマンド

コマンド	説明
show cts sxp	すべての SXP 設定のステータスを表示します。

clear cts cache

TrustSec 認可をクリアし、**clear cts counter** 特権 EXEC コマンドを使用します。

clear cts cache authorization-policies [**peer** | **sgt**]

clear cts cache environment-data

clear cts cache filename *file*

clear cts cache interface-controller [**type** *slot*/*port*]

構文の説明

authorization-policies [peer | sgt]	すべてのキャッシュされた SGT およびピア認可ポリシーをクリアします。
environment-data	環境データ キャッシュ ファイルをクリアします。
filename *file*	クリアするキャッシュ ファイルのファイル名を指定します。
interface-controller type *slot*/*port*	クリアするインターフェイス コントローラ キャッシュを指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2(50) SY	**interface-controller** キーワードは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次に、キャッシュから環境データを削除する例を示します。

```
Router# clear cts cache environment-data
Router#
```

（注） ピアの認可および SGT ポリシーのクリアは、SGACL を強制できる TrustSec デバイスだけに関連します。

関連コマンド

コマンド	説明
cts cache	DRAM および NVRAM への TrustSec 許可および環境データ情報のキャッシュをイネーブルにします

clear cts counter

指定したインターフェイスの TrustSec 統計情報をクリアするには、**clear cts counter** 特権 EXEC コマンドを使用します。

clear cts counter [**type** *slot*/*port*]

構文の説明

type *slot*/*port*	（任意）クリアするインターフェイスのインターフェイスタイプ、スロット、およびポートを指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

clear cts counter コマンドは、選択したインターフェイスに固有の CTS カウンタをクリアします。インターフェイスが指定されていない場合、すべての TrustSec インターフェイスのすべての TrustSec カウンタがクリアされます。

例

次に、GigabitEthernet インターフェイス 3/1 の CTS 統計情報をクリアしてから、**show cts interface** コマンドを使用して確認する例を示します（**show** コマンド出力のフラグメントを表示）。

```
Router# clear cts counter gigabitEthernet3/1
Router# show cts interface  gigabitEthernet3/1
Global Dot1x feature is Disabled
Interface GigabitEthernet3/1:
<snip>

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
<snip>
```

関連コマンド

コマンド	説明
show cts interface	CTS インターフェイスのステータスおよび設定を表示します。

clear cts credentials

TrustSec デバイス ID およびパスワードを削除するには、特権 EXEC モードで **clear cts credentials** コマンドを使用します。

clear cts credentials

構文の説明　このコマンドには、引数またはキーワードはありません。

デフォルト　なし

コマンド モード　特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

```
Router# clear cts credentials
Router# clear cts environment-data
Router# show cts environment-data
CTS Environment Data
====================
Current state = START
Last status = Cleared
Environment data is empty
State Machine is running
Retry_timer (60 secs) is running
```

関連コマンド

コマンド	説明
cts credentials	TrustSec ID およびパスワードを指定します。

clear cts environment-data

キャッシュから TrustSec 環境データを消去するには、特権 EXEC モードで **clear cts environment-data** コマンドを使用します。

clear cts environment-data

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、キャッシュから環境データをクリアする例を示します。

```
Router# clear cts environment-data
```

関連コマンド

コマンド	説明
show cts environment-data	CTS 環境データを表示します。

clear cts macsec

指定されたインターフェイスの MACsec カウンタをクリアするには、**clear cts macsec counters** コマンドを使用します。

clear cts macsec counters interface type *slot*/*port*

構文の説明

interface type *slot*/*port*	インターフェイスを指定します。

コマンド モード

特権 EXEC

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次の例では、Catalyst 6500 シリーズ スイッチの gigabitEthernet インターフェイス カウンタをクリアします。

```
Router# clear cts macsec counters interface gigabitEthernet 6/2
```

関連コマンド

コマンド	説明
show cts macsec	
show cts interface	

clear cts pac

キーストアから TrustSec Protected Access Credential（PAC）情報をクリアするには、特権 EXEC モードで **clear cts pac** コマンドを使用します。

clear cts pac {**A-ID** *hexstring* | **all**}

構文の説明

A-ID *hexstring*	キーストアから削除する PAC のオーセンティケータ ID（A-ID）を指定します。
all	デバイスのすべての PAC を削除するように指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次のコマンドは、キーストアのすべての PAC をクリアします。

```
Router# clear cts pac all
```

関連コマンド

コマンド	説明
show cts pacs	キーストアの PAC の A-ID および PAC 情報を表示します。
show cts keystore	キーストアの内容を表示します。

clear cts policy

TrustSec ピアのピア認可ポリシーを削除するには、特権 EXEC モードで **clear cts policy** コマンドを使用します。

clear cts policy {**peer** [*peer_id*] | **sgt** [*sgt*]}

構文の説明

peer *peer_id*	TrustSec ピア デバイスのピア ID を指定します。
sgt *sgt*	TrustSec ピア デバイスのセキュリティ グループ タグ（SGT）を、16 進数で指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド デフォルト

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

すべての TrustSec ピアのピア認可ポリシーをクリアするには、ピア ID を指定しないで **clear cts policy peer** コマンドを使用します。TrustSec ピアのセキュリティ グループ タグをクリアするには、**clear cts policy sgt** コマンドを使用します。確認するには、**show cts policy peer** コマンドを使用します。

例

次の例では、ピア ID が atlas2 の TrustSec ピアのピア認可ポリシーをクリアします。

```
Router# clear cts policy peer atlas2
Delete all peer policies? [confirm] y
Router#
```

関連コマンド

コマンド	説明
cts refresh	ピア認可ポリシーを強制的にリフレッシュします。
show cts policy peer	TrustSec ピアのピア認可ポリシーを表示します。

clear cts role-based counters

セキュリティ グループ ACL 統計カウンタをリセットするには、EXEC モードまたは特権 EXEC モードで **clear cts role-basedcounters** コマンドを使用します。

clear cts role-based counters default [**ipv4** | **ipv6**]

clear cts role-based counters from {*sgt_num* | **unknown**} [**ipv4** | **ipv6** | **to** {*sgt_num* | **unknown**} [**ipv4** | **ipv6**]]

clear cts role-based counters to {*sgt_num* | **unknown**} [**ipv4** | **ipv6** | **]**

clear cts role-based counters [**ipv4** | **ipv6**]

構文の説明

default	デフォルト ポリシー カウンタ
from	送信元セキュリティ グループを指定します
ipv4	IP バージョン 4 ネットワークでセキュリティ グループを指定します
ipv6	IP バージョン 6 ネットワークでセキュリティ グループを指定します
to	宛先セキュリティ グループを指定します
sgt_num	（0 ～ 65533）セキュリティ グループ タグ番号を指定します
unknown	すべての送信元グループを指定します

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

指定したスコープのセキュリティ グループ ACL（SGACL）強制カウンタをクリアするには、**clear cts role-based counters** コマンドを使用します。**show cts role-based counters** は、最後に clear コマンドが発行されてから蓄積された統計情報を、例 7-1 に示されているような表形式で表示します。

例 7-1　show role-based カウンタからの表形式の SGACL 出力

```
router# show cts role-based counters
Role-based counters
From    To      SW-Denied       HW-Denied       SW-Permitted    HW_Permitted
2       5       129               89762               421      7564328
3       5        37              123456              1325     12345678
3       7         0               65432               325      2345678
```

from キーワードで送信元 SGT を、**to** キーワードで宛先 SGT を指定します。**from** および句、**to** キーワードの両方が省略された場合は、許可マトリクス全体のカウンタがクリアされます。

default キーワードは、デフォルトのユニキャストのポリシー統計情報をクリアします。

ipv4 および **ipv6** のいずれも指定しない場合、コマンドは IPv4 カウンタだけをクリアします。

例

次の例では、IPv4 トラフィックの SGACL 強制の統計情報をコンパイルしているすべてのロールベース カウンタをクリアします。

```
router# clear cts role-based counters ipv4
```

関連コマンド

clear cts server

CTS の AAA サーバ リストからサーバを削除するには、**clear cts server** コマンドを使用します。

clear cts server *ip_address*

構文の説明

ip_address	サーバ リストから削除する AAA サーバの IPv4 アドレス。

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、**cts authorization list** グローバル コンフィギュレーション コマンドで設定された CTS AAA サーバのリスト、または CTS のオーセンティケータのピアによりプロビジョニングされた AAA サーバ リストから、サーバを削除します。

例

次の例は、CTS の AAA サーバ リストから AAA サーバ 10.10.10.1 を削除します。

```
router# clear cts server 1.1.1.1
```

関連コマンド

コマンド	説明
show cts server-list	
cts server	

default（cts dot1x インターフェイス コンフィギュレーション サブモード）

任意の **cts dot1x** コンフィギュレーションをデフォルト値に復元するには、CTS dot1x インターフェイス コンフィギュレーション サブモードで **default** コマンドを使用します。

default propagate sgt

default sap

default timer reauthentication

構文の説明

propagate sgt	propagate sgt をイネーブルにしたデフォルトに復元します。
sap	デフォルトの **sap modelist gcm-encrypt null** に復元します。
timer	dot1x 再認証時間が 86,400 秒のデフォルトに復元します。

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

CTS dot1x インターフェイス コンフィギュレーション サブモード（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、SGT 伝搬を再イネーブル化する例を示します。

```
router# config t
router(config)# interface gigabit 6/1
router(config-if)# cts dot1x
router(config-if-cts-dot1x)# default propagate sgt
```

関連コマンド

コマンド	説明
propagate（cts dot1x サブモード）	dot1x モードの SGT 伝搬をイネーブルまたはディセーブルにします。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
timer（cts do1x インターフェイス サブモード）	CTS のタイマーを設定します。

default（cts 手動インターフェイス コンフィギュレーション サブモード）

任意の **cts manual** コンフィギュレーションをデフォルト値に復元するには、CTS 手動インターフェイス コンフィギュレーション サブモードで **default** コマンドを使用します。

default policy dynamic identity

default policy static sgt

default propagate sgt

default sap

構文の説明

dynamic identity	ピア ポリシーを AAA サーバからダウンロードするデフォルトに復元します。
policy static sgt	デフォルトの no policy に復元します。つまり、SGT は入力トラフィックに適用されません。
policy propagate sgt	SGT の伝播のモードを On に指定します。
sap	デフォルト SAP 値を指定します。（GCM-Encrypt、null）

コマンド モード

CTS 手動インターフェイス コンフィギュレーション サブモード（config-if-cts-manual）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

CTS の手動インターフェイス コンフィギュレーション サブモード パラメータをデフォルト値に戻すには、**default** サブコマンドを使用します。

例

次に、Catalyst 6500 シリーズ スイッチの CTS イネーブルにされたインターフェイスのデフォルトのダイナミック ポリシーと、SGT 伝播ポリシーを復元する例を示します。

```
router# config t
router(config)# interface gigbitEthernet 6/1
router(config-if)# cts manual
router(config-if-cts-manual)# default policy dynamic identity
router(config-if-cts-manual)# default propagate sgt
```

関連コマンド

コマンド	説明
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS ポリシーを設定します
sap（cts 手動インターフェイス サブモード）	手動モードの CTS SAP を設定します。

match flow cts

Flexible NetFlow フロー レコードに、Cisco TrustSec フロー オブジェクトを追加するには、**match flow cts** レコード コンフィギュレーション コマンドを使用します。

[**no**] **match flow cts destination group-tag**

[**no**] **match flow cts source group-tag**

構文の説明

destination group-tag	Cisco TrustSec セキュリティ グループ タグ（SGT）の宛先フィールドを照合します
source group-tag	Cisco TrustSec セキュリティ グループ タグ（SGT）の送信元フィールドを照合します

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

Flexible NetFlow レコード コンフィギュレーション（config-flow-record）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

標準の 5 タプル フロー オブジェクトを使用してフロー レコードに SGT および DGT フロー オブジェクトが設定されている場合、Flexible NetFlow は、SGACL 強制によってドロップされたパケットに対応できます

flow record および **flow exporter** 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フロー レコードおよびフロー エクスポータを設定してから、それらを **flow monitor** コマンドを使用してフロー モニタに追加します。**show flow** show コマンドを使用して設定を確認します。

SGACL のドロップされたパケットだけを収集するには、[**no**] **cts role-based** {**ip** | **ipv6**} **flow monitor dropped** 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。

Flexible NetFlow の概要および設定の詳細については、次のマニュアルを参照してください。

『Getting Started with Configuring Cisco IOS Flexible NetFlow』

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html

『Catalyst 6500 Release 12.2SY Software Configuration Guide』

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/netflow_hw_support.html

例

次に、IPv4 フロー レコード（5 タプル、方向、SGT、SGT）を設定する例を示します。

```
router(config)# flow record cts-record-ipv4
router(config-flow-record)# match ipv4 protocol
```

```
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match transport source-port
router(config-flow-record)# match transport destination-port
router(config-flow-record)# match flow direction
router(config-flow-record)# match flow cts source group-tag
router(config-flow-record)# match flow cts destination group-tag
router(config-flow-record)# collect counter packets
```

関連コマンド

コマンド	説明
show flow monitor	Flexible NetFlow フロー モニタのステータスおよび統計情報を表示します
cts role-based	Flexible NetFlow では、このコマンドには、すべてのレイヤ 3 インターフェイスにフロー モニタを接続して、SGACL によってドロップされるトラフィックの統計情報を収集するように設定するオプションがあります。

platform cts

TrustSec 出力または入力のリフレクタをイネーブルにするには、**platform cts** 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。リフレクタをディセーブルにするには、コマンドの **no** 形式を入力します。

[**no**] **platform cts** {**egress** | **ingress**}

構文の説明

egress	イネーブルまたはディセーブルにされる出力 TrustSec リフレクタを指定します。
ingress	イネーブルまたはディセーブルにされる入力 TrustSec リフレクタを指定します。

デフォルト

デフォルトは、no ingress または egress reflector です。

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次の例では、Catalyst 6500 スイッチで CTS 入力リフレクタをイネーブル化します。

```
switch(config)# platform cts egress
```

次の例では、Catalyst 6500 スイッチで CTS 入力リフレクタをディセーブル化します。

```
switch(config)# no platform cts egress
```

関連コマンド

コマンド	説明
show platform cts reflector	Cisco TrustSec リフレクタ モードのステータスを表示します。

policy（cts 手動インターフェイス コンフィギュレーション サブモード）

手動で設定された TrustSec リンクにポリシーを適用するには、**policy** インターフェイス手動サブモード コマンドを使用します。ポリシーを削除するには、コマンドの **no** 形式を使用します。

[**no**] **policy dynamic identity** *peer_deviceID*

[**no**] **policy static sgt** *sgt_number* [**trusted**]

構文の説明

dynamic	認証サーバからポリシーを取得します。
identity *peer_deviceID*	認証サーバのポリシー データベースの、ピアに適用されるポリシーに関連付けられたピア デバイス名またはシンボリック名。
static	リンクの着信トラフィックに SGT ポリシーを指定します。
sgt *sgt_number*	ピアからの着信トラフィックに適用するセキュリティ グループ タグ番号。
trusted	コマンドで SGT が指定されたインターフェイスの入力トラフィックでは、SGT を上書きしてはいけないことを示します。デフォルトは untrusted です。

デフォルト

デフォルトは no policy です。

コマンド モード

CTS インターフェイスの手動サブモード（config-if-cts-manual）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

TrustSec リンクを手動で設定する場合はポリシーを適用するには、**policy** コマンドを使用します。デフォルトは **no policy** で、すべてのトラフィックを SGT を適用しないで通過させます。**sap** CTS 手動モード サブコマンドはまた、TrustSec リンクをアップするように設定する必要があります。

選択した SAP モードで SGT を挿入可能にし、すべての着信パケットが SGT を伝送していない場合、タギング ポリシーは次のとおりです。

- **policy static** コマンドが設定されている場合、パケットには **policy static** コマンドで設定した SGT がタグ付けされます。
- **policy dynamic** コマンドが設定されている場合、パケットはタグ付けされません。

選択した SAP モードで SGT を挿入可能にし、着信パケットが SGT を伝送している場合、タギング ポリシーは次のとおりです。

- **policy static** コマンドが **trusted** キーワードを指定せずに設定されている場合、SGT は **policy static** コマンドで設定した SGT に置き換えられます。

- **policy static** コマンドが **trusted** キーワードを使用して設定されている場合、SGT は変更されません。
- **policy dynamic** コマンドが設定されていて、認証サーバからダウンロードされた認可ポリシーがパケットの送信元が信頼できないことを示している場合、SGT はダウンロードしたポリシーで指定されている SGT に置き換えられます。

  認可ポリシーは、ピアの SGT、ピアの SGT 割り当ての信頼状態、関連するピア SGT の RBACL、およびインターフェイス ACL を指定できます。
- **policy dynamic** コマンドが設定されていて、ダウンロードされた認可ポリシーがパケットの送信元が信頼できることを示している場合、SGT は変更されません。

静的に設定された SGT については RBACL は適用されませんが、従来のインターフェイス ACL は、必要に応じてトラフィック フィルタリング用に個別に設定できます。

例

次の例では、タグ付け済みのトラフィックを除き、ピアからの着信トラフィックに SGT 3 を適用します（Cisco Secure ACS サーバと通信していないインターフェイス）。

```
Router# configure terminal
Router(config)# interface gi2/1
Router(config-if)# cts manual
Router(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Router(config-if-cts-manual)# policy static sgt 3 trusted
Router(config-if-cts-manual)# exit
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit

Router# show cts interface GigabitEthernet 2/1
Global Dot1x feature is Enabled
Interface GigabitEthernet2/1:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    SUCCEEDED
        Peer SGT:            3
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
        Version:             1
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:           Enabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
```

```
sap success:                1
sap fail:                   0
authz success:              5
authz fail:                 0
port auth fail:             0
Ingress:
    control frame bypassed: 0
    sap frame bypassed:     0
    esp packets:            0
    unknown sa:             0
    invalid sa:             0
    inverse binding failed: 0
    auth failed:            0
    replay error:           0
Egress:
    control frame bypassed: 0
    esp packets:            0
    sgt filtered:           0
    sap frame bypassed:     0
    unknown sa dropped:     0
    unknown sa bypassed:    0
```

関連コマンド

コマンド	説明
show cts interface	インターフェイスごとの TrustSec 設定の統計情報を表示します。
default（cts 手動インターフェイス コンフィギュレーション サブモード）	CTS 手動モードのデフォルト コンフィギュレーション復元します。
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS ポリシーを設定します。
sap（cts 手動インターフェイス サブモード）	手動モードの CTS SAP を設定します。

propagate（cts dot1x サブモード）

Cisco TrustSec インターフェイスで SGT 伝播をイネーブルまたはディセーブルにするには、CTS dot1x インターフェイス コンフィギュレーション サブモードで propagate sgt コマンドを使用します。

[**no**] **propagate sgt**

構文の説明

sgt	CTS SGT 伝搬を指定します。

デフォルト

SGT 伝播は、CTS dot1x および CTS 手動インターフェイス コンフィギュレーション サブモードでデフォルトでイネーブルになっています。

コマンド モード

CTS Dot1x インターフェイス コンフィギュレーション サブモード（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

SGT の伝播（SGT タグ カプセル化）は、CTS dot1x および CTS 手動インターフェイス コンフィギュレーション サブモードの両方でデフォルトでイネーブルになっています。TrustSec 対応ポートはレイヤ 2 MACsec および SGT カプセル化をサポートできます。SGT のタグとデータの送信のためにピアと最もセキュアなモードをネゴシエートします。MACsec はスイッチおよびサーバが使用する 802.1AE 規格ベースのリンク間プロトコルです。ピアは MACsec をサポートできますが、SGT カプセル化はサポートできません。このような場合、**no propagate sgt** CTS Dot1x インターフェイス コンフィギュレーション コマンドを使用して、このレイヤ 2 SGT 伝播をディセーブルにしておくことをお勧めします。

SGT の伝播を再度イネーブルにするには **propagate sgt** コマンドを入力します。SGT の伝播の状態を確認するには、**show cts interface** コマンドを使用します。ディセーブル ステートだけが不揮発生成（NVGEN）に保存されます。

例

次の例は、TrustSec 対応インターフェイスで SGT 伝播をディセーブル化します。

```
router(config) interface gigabit 6/1
router(config-if) cts dot1x
router(config-if-cts-dot1x)# no propagate sgt

router# show cts interface gigabit 6/1
Global Dot1x feature is Enabled
Interface GigabitEthernet6/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               INIT

<snip> . . .

SAP Status:              UNKNOWN
```

```
Configured pairwise ciphers:
    gcm-encrypt
    null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:

    Propagate SGT:           Disabled
<snip> . . .
```

関連コマンド

コマンド	説明
show cts interface	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。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
timer（cts do1x インターフェイス サブモード）	CTS のタイマーを設定します。

propagate（cts 手動インターフェイス コンフィギュレーション サブモード）

セキュリティ グループ タグをインターフェイス上で伝播するインターフェイスの機能をイネーブルまたはディセーブルにするには、**cts propagate** cts インターフェイス手動設定サブモード コマンドを使用します。

[**no**] **propagate sgt**

構文の説明

sgt	セキュリティ グループ タグを指定します

デフォルト

デフォルトは、SGT を伝播することです。

コマンド モード

CTS 手動インターフェイス コンフィギュレーション サブモード（config-if-cts-manual）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

セキュリティ グループ タグの伝播は、CTS dot1x および CTS 手動モードの両方でデフォルトでイネーブルです。SGT 処理をディセーブルにするには、**no propagate sgt** コマンドを入力します。再度イネーブルにするには、**propagate sgt** を入力します。不揮発生成（NVGEN）プロセスを呼び出す CLI コマンドを発行した場合、**no propagate sgt** ステートだけが保存されます（たとえば、**copy system running-config**）。

TrustSec 対応インターフェイスは MACsec（レイヤ 2 802.1AE のセキュリティ）および SGT タギングをサポートできます。TrustSec 対応インターフェイスがピアと最もセキュアなモードをネゴシエートしようとします。ピアは、MACsec 対応ですが、SGT を処理できないことがあります。手動 CTS インターフェイス コンフィギュレーションでは、MACsec 機能のみを設定している場合、CTS 対応インターフェイスで SGT 伝播をディセーブルにします。

例

次に、手動で設定した TrustSec 対応インターフェイスで SGT タギングをディセーブル化する例を示します。

```
router(config-if)# cts manual
router(config-if-cts-manual)# sap pmk FFFE
router(config-if-cts-manual)# no propagate sgt
router(config-if-cts-manual)# exit
router(config-if)# exit
router(config)# exit
router# show running-config
. . .
interface GigabitEthernet6/2
 ip address 172.16.4.12 255.255.255.0
cts manual
```

```
  no propagate sgt
  sap pmk 00000000000000000000000000000000000000000000000000000000000000000000FFFE
. . .
```

関連コマンド

コマンド	説明
show cts interface	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。
show running-config	現在のシステム設定を表示します。

sap（cts dot1x インターフェイス サブモード）

2 個のインターフェイス間のリンク暗号化をネゴシエーションするために、セキュリティ アソシエーション プロトコル（SAP）の認証および暗号化モード選択するには、**sap mode-list** コマンドを使用します。modelist を削除してデフォルトに戻すには、このコマンドの **no** 形式を使用します。

[**no**] **sap mode-list** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**] . . .}

構文の説明

mode-list	アドバタイズされた SAP 認証および暗号化モードをリストします（最高から最低に優先順位付け）
gcm-encrypt	GMAC 認証、GCM 暗号化を指定します
gmac	GMAC 認証だけを指定し、暗号化を指定しません
no-encap	カプセル化を指定しません
null	カプセル化あり、認証なし、暗号化なしを指定します

デフォルト

デフォルトの暗号化は、**sap modelist gcm-encrypt null** です。ピア インターフェイスが dot1x、802.1AE MACsec、または 802.REV レイヤ 2 リンク暗号化をサポートしない場合、デフォルトの暗号化は **null** です

コマンド モード

CTS dot1x インターフェイス サブモード（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	このコマンドが、Catalyst 4500 シリーズ スイッチに追加されました。
IOS 15.0(1) SE	このコマンドが、Catalyst 3000 シリーズ スイッチに追加されました。

使用上のガイドライン

Dot1x 認証中に使用する認証および暗号化方式を指定するには、**sap mode-list** コマンドを使用します。

セキュリティ アソシエーション プロトコル（SAP）は 802.11i IEEE プロトコルのドラフト バージョンに基づいた暗号キーの取得および交換プロトコルです。SAP は MACsec をサポートするインターフェイス間の 802.1AE リンク間暗号化（MACsec）を確立および管理するために使用します。

Dot1x 認証後に SAP 交換が開始される前に、両側（サプリカントとオーセンティケータ）で Cisco Secure Access Control Server（Cisco Secure ACS）から Pairwise Master Key（PMK）とピアのポートの MAC アドレスを受信しています。802.1X 認証が不可能である場合、CTS 手動コンフィギュレーション モードで、SAP および PMK を 2 個のインターフェイス間で手動で設定できます。

デバイスが CTS-Aware ソフトウェアを実行していて、ハードウェアが CTS 非対応である場合は、**sap modelist no-encap** コマンドを使用してカプセル化を拒否します。

期間が Cisco Secure ACS から使用できない場合は、**timer reauthentication** コマンドを使用して CTS リンクに適用する再認証期間を設定します。デフォルトの再認証期間は 86,400 秒です。

（注）　TrustSec NDAC および SAP はスイッチ間リンクでスイッチングだけでサポートされているため、dot1x はマルチホスト モードで設定する必要があります。オーセンティケータ PAE は **dot1x system-auth-control** がグローバルにイネーブルになっている場合のみ開始されます。

例

次に、SAP が CTS カプセル化の使用を GCM 暗号化と、または第 2 の選択肢として null-cipher とネゴシエートするが、ピアがハードウェアで CTS カプセル化をサポートしない場合は CTS カプセル化を受け入れることができない例を示します。

```
Router(config-if-cts-dot1x)# sap modelist gcm-encrypt  null  no-encap
```

関連コマンド

コマンド	説明
propagate（cts dot1x サブモード）	dot1x モードの SGT 伝搬をイネーブルまたはディセーブルにします。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
timer（cts do1x インターフェイス サブモード）	CTS のタイマーを設定します。

sap（cts 手動インターフェイス サブモード）

2 個のインターフェイス間で MACsec のリンク暗号化のネゴシエーションを行うために、Pairwise Master Key（PMK）と Security Association Protocol（SAP）の認証および暗号化モードを手動で指定するには、**sap mode-list** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

[**no**] **sap pmk** *hex_value* [**modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**] . . .]

構文の説明

pmk *hex_value*	16 進数データの PMK（先頭の 0x は付けません。偶数の 16 進数文字を入力し、最後の文字に 0 をプレフィックスします）
modelist	アドバタイズド モードのリスト（最高から最低に優先順位付け）
gcm-encrypt	GCM 認証、GCM 暗号化を指定します
gmac	GCM 認証を指定し、暗号化を指定しません
no-encap	カプセル化を指定しません
null	カプセル化あり、認証なし、暗号化なしを指定します

デフォルト

デフォルトの暗号化は、**sap modelist gcm-encrypt null** です。ピア インターフェイスが dot1x、802.1AE MACsec、または 802.REV レイヤ 2 リンク暗号化をサポートしない場合、デフォルトの暗号化は **null** です

コマンド モード

CTS 手動インターフェイス コンフィギュレーション サブモード（config-if-cts-manual）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

セキュリティ アソシエーション プロトコル（SAP）は 802.11i IEEE プロトコルのドラフト バージョンに基づいた暗号キーの取得および交換プロトコルです。TrustSec 設定では、キーは 2 個のインターフェイス間での MACsec のリンク間暗号化に使用されます。

802.1X 認証が不可能である場合、SAP、および Pairwise Master Key（PMK）を **sap pmk** コマンドで 2 個のインターフェイス間に手動で設定できます。802.1X 認証を使用する場合、両方（サプリカントおよびオーセンティケータ）が Cisco Secure Access Control Server からピアのポートの PMK および MAC アドレスを受信します。

例

次に、ギガビット イーサネット インターフェイスの SAP 設定の例を示します。

```
router(config)# interface gigabitEthernet 2/1
router(config-if)# cts manual
router(config-if-cts-manual)# sap pmk FFFEE mode-list gcm-encrypt
```

関連コマンド

コマンド	説明
default（cts 手動インターフェイス コンフィギュレーション サブモード）	CTS 手動モードのデフォルト コンフィギュレーション復元します。
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS ポリシーを設定します
propagate（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS SGT 伝搬を設定します
show cts interface	インターフェイスごとの TrustSec 設定の統計情報を表示します。

show cts

Cisco TrustSec に関連するステートおよび統計情報を表示するには、**show cts** 特権 EXEC コマンドを使用します。

show cts [

authorization entries |

credentials |

environment-data

interface {type *slot*/*port* **| vlan** *vlan_number* **|**

keystore |

macsec counters interface type *slot*/*port* [**delta**] |

pacs |

policy layer3 [**ipv4** | **ipv6**] |

policy peer *peer_id* |

provisioning |

role-based counters . . . |

role-based flow . . . |

role-based permissions . . . |

role-based sgt-map . . . |

server-list |

sxp connections . . . |

sxp sgt-map . . . |

構文の説明

authorization	認可エントリを表示します。
credentials	CTS 認証に使用するクレデンシャルを表示します。
environment-data	CTS 環境データを表示します。
interface	CTS インターフェイスのステータスと設定を表示します。
keystore	キーストアの情報を表示します。
macsec	MACSec カウンタ情報を表示します。
pacs	キーストアの PAC の A-ID および PAC 情報を表示します。
policy	CTS ポリシーを表示します。
provisioning	未処理の CTS のプロビジョニング ジョブを表示します。
role-based	ロールベース アクセス コントロール情報（SGACL 情報）を表示します。
server-list	CTS のサーバ リストを表示します。
sxp	CTS SXP プロトコル情報を表示します。

デフォルト

なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2(50) SY	次のキーワードは、Catalyst 6500 シリーズ スイッチに追加されました。

例　次に、キーワードを使用しないで入力した **show cts** の例を示します。

```
Router# show cts
Global Dot1x feature: Enabled
CTS device identity: "dcas1"
CTS caching support: disabled

Number of CTS interfaces in DOT1X mode:  19,    MANUAL mode: 5
Number of CTS interfaces in LAYER3 TrustSec mode: 0

Number of CTS interfaces in corresponding IFC state
  INIT            state:  19
  AUTHENTICATING  state:  0
  AUTHORIZING     state:  0
  SAP_NEGOTIATING state:  0
  OPEN            state:  5
  HELD            state:  0
  DISCONNECTING   state:  0
  INVALID         state:  0

CTS events statistics:
  authentication success: 14
  authentication reject : 19
  authentication failure: 0
  authentication logoff : 1
  authentication no resp: 0
  authorization success : 19
  authorization failure : 3
  sap success           : 12
  sap failure           : 0
  port auth failure     : 0
```

関連コマンド

コマンド	説明
cts credentials	TrustSec ID およびパスワードを指定します。

show cts authorization entries

TrustSec NDAC 認証エントリを表示するには、EXEC モードまたは特権 EXEC モードで **show cts authorization entries** コマンドを使用します。

show cts authorization entries

構文の説明　このコマンドには、引数またはキーワードはありません。

デフォルト　なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例　次の例では、Catalyst 6500 スイッチからの **show** コマンドの出力です。

```
router# show cts authorization entries
Authorization Entries Info
 Peer-name                = annapurna
Peer-SGT                 = 7-1F05D8C1
Entry State              = COMPLETE
Entry last refresh       = 01:19:37 UTC Sat Dec 8 2007
Session queuesize        = 1
  Interface:       Gi2/3
  status:          SUCCEEDED
Peer policy last refresh = 01:19:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:19:37 UTC Sat Dec 8 2007
Peer policy refresh time = 2000
Policy expires in     0:00:28:26 (dd:hr:mm:sec)
Policy refreshes in  0:00:28:26 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied           = NONE
Entry status                 = SUCCEEDED

Peer-name = Unknown-0000
Peer-SGT = 0-AD23BDF78
Entry State = COMPLETE
Entry last refresh       = 01:30:37 UTC Sat Dec 8 2007
session queuesize = 0
Peer policy last refresh = 01:30:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:30:37 UTC Sat Dec 8 2007
Peer policy refresh time = 0
SGT policy refresh time = 2000
Policy expires in    0:00:29:27 (dd:hr:mm:sec)
Policy refreshes in 0:00:29:27 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied      = NONE
```

```
Entry status                 = SUCCEEDED

Peer-name = Unknown-FFFF
Peer-SGT = FFFF-ABC876234
Entry State = COMPLETE
Entry last refresh       = 01:30:37 UTC Sat Dec 8 2007
session queuesize = 0
Peer policy last refresh = 00:20:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:30:37 UTC Sat Dec 8 2007
Peer policy refresh time = 0
SGT policy refresh time = 2000
Policy expires in    0:00:29:27 (dd:hr:mm:sec)
Policy refreshes in 0:00:29:27 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied       = NONE
Entry status                  = SUCCEEDED
```

関連コマンド

コマンド	説明
cts credentials	TrustSec ID およびパスワードを指定します。

show cts credentials

TrustSec デバイス ID を表示するには、EXEC モードまたは特権 EXEC モードで **show cts credentials** コマンドを使用します。

show cts credentials

構文の説明

このコマンドには、コマンドまたはキーワードはありません。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

```
Router# show cts credentials
CTS password is defined in keystore, device-id = r4
```

関連コマンド

コマンド	説明
cts credentials	TrustSec ID およびパスワードを指定します。

show cts environment-data

TrustSec 環境データを表示するには、EXEC モードまたは特権 EXEC モードで **show cts environment-data** コマンドを使用します。

show cts environment-data

構文の説明

このコマンドには、コマンドまたはキーワードはありません。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次の例は、Cisco Catalyst 6500 シリーズ スイッチの環境データを表示します。

```
Router# show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 11-ea7f3097b64bc9f8
Server List Info:
Preferred list, 0 server(s):
Installed list: SL1-15A25AC3633E7F074FF7E0B45861DF15, 1 server(s):
 *Server: 43.1.1.3, port 1812, A-ID 05181D8147015544BC20F0119BE8717E
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
  Multicast Group Addresses:
Multicast Group SGT Table:
  Name = mcg_table_2-4ff532e525a3efe4
  Multicast SGT:
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 2000 secs
Last update time = 21:43:28 UTC Mon Aug 27 2007
Data loaded from cache = FALSE
Refresh timer is running
State Machine is running
```

関連コマンド

コマンド	説明
clear cts environment-data	キャッシュからの TrustSec 環境データをクリアします。

show cts interface

TrustSec 設定の統計情報を表示するには、EXEC モードまたは特権 EXEC モードで **show cts interface** コマンドを使用します。

show cts interface [**type** *slot*/*port*] | [**brief**] | [**summary**]

構文の説明

type *slot*/*port*	（任意）インターフェイス タイプ、スロット番号、およびポート番号を指定します。このインターフェイスの冗長ステータス出力が返されます。
brief	（任意）すべての CTS インターフェイスの短縮ステータスを表示します。
summary	（任意）インターフェイスごとに、すべての CTS インターフェイスのサマリーを、4 個または 5 個のキー ステータス フィールドを持つ表形式で表示します。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

すべての CTS インターフェイスの冗長ステータスを表示するには、キーワードなしで **show cts interface** コマンドを使用します。

例

次に、キーワードを使用せずに出力を表示する例を示します（すべての CTS インターフェイスの冗長ステータス）。

```
Router# show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet4/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "r1"
        Peer is:             CTS capable
        802.1X role:         Authenticator
        Reauth period configured:       0 (locally not configured)
        Reauth period per policy:       3000 (server configured)
        Reauth period applied to link:  3000 (server configured)
    Authorization Status:    SUCCEEDED
        Peer SGT:            0
        Peer SGT assignment: Untrusted
    SAP Status:              NOT APPLICABLE
```

```
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: OUT-OF-ORDER
        SPI range:              (256, 1023)
        Pairwise Master Session Key:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

        Selected cipher:
        Current receive SPI:    0
        Current transmit SPI:   0
        Current Transient Session Key:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

        Current Offset:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

    Statistics:
        authc success:              1
        authc reject:               18
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              1
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0

Dot1x Info for GigabitEthernet4/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Enabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3000 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

次に、**brief** キーワードを使用した出力例を表示します。

```
Router# show cts interface brief
Global Dot1x feature is Enabled
Interface GigabitEthernet4/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "r1"
        Peer is:             CTS capable
        802.1X role:         Authenticator
        Reauth period configured:       0 (locally not configured)
        Reauth period per policy:       3000 (server configured)
        Reauth period applied to link:  3000 (server configured)
    Authorization Status:    SUCCEEDED
        Peer SGT:            0
        Peer SGT assignment: Untrusted
    SAP Status:              NOT APPLICABLE

Dot1x Info for GigabitEthernet4/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Enabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3000 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

次に、**summary** キーワードを使用した出力例を表示します。

```
Router# show cts interface summary
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache  Dot1x
------------------------------------------------------------------------
Gi4/1      DOT1X   OPEN      Authent    r1         invalid    enabled
```

関連コマンド

コマンド	説明
cts sxp	ネットワーク デバイスに SXP を設定します。

show cts macsec

CTS リンク間暗号化に関連するインターフェイスごとに暗号 ASIC のパケット カウンタを表示するには、**show cts macsec** コマンドを使用します。

show cts macsec counters interface interface_type *slot*/*port* [**delta**]

構文の説明

interface interface_type *slot*/*port*	CTS MACsec インターフェイスを指定します。
delta	最後にクリアされた時点以降のカウンタ値を表示します。

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、インターフェイス単位の暗号 ASIC のパケット カウンタを表示します。セキュリティ アソシエーション（SA）がインストールされている場合（NDAC または **sap** cts インターフェイス do1x または手動サブコマンドを介して）、アクティブな SA カウンタが表示されます。一度に 1 つの SA しかアクティブになりません。SA のサポートされる値は 1 と 2. です。delta キーワードにより、**clear cts macsec counters interface** コマンドが発行された時点以降のカウンタ値がリストされます。

例

次の例では、Catalyst 6500 シリーズ スイッチ上で手動で設定された CTS アップリンク インターフェイスの MACsec カウンタを表示します。

```
router# show cts macsec counters interface gigabitEthernet 6/2
CTS Security Statistic Counters:
                    rxL2UntaggedPkts = 0
                       rxL2NotagPkts = 0
                      rxL2SCMissPkts = 0
                        rxL2CTRLPkts = 0
                        rxL3CTRLPkts = 0
                    rxL3UnknownSAPkts = 0
                       rxL2BadTagPkts = 0
                    txL2UntaggedPkts = 0
                        txL2CtrlPkts = 0
                        txL3CtrlPkts = 0
                       txL3UnknownSA = 0
GENERIC Counters:
                      CRCAlignErrors = 0
                      UndersizedPkts = 0
                       OversizedPkts = 0
                        FragmentPkts = 0
                             Jabbers = 0
                          Collisions = 0
                            InErrors = 0
                           OutErrors = 0
                        ifInDiscards = 0
```

```
                ifInUnknownProtos = 0
                    ifOutDiscards = 0
dot1dDelayExceededDiscards = 0
                          txCRC = 0
                     linkChange = 0
```

関連コマンド

コマンド	説明
show cts interface	
sap（cts dot1x インターフェイス サブモード)	
sap（cts 手動インターフェイス サブモード)	

show cts pacs

Protected Access Credential（PAC）を表示するには、EXEC モードまたは特権 EXEC モードで **show cts pacs** コマンドを使用します。

show cts pacs

構文の説明

このコマンドには、コマンドまたはキーワードはありません。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

NDAC オーセンティケータを識別し、NDAC の完了を確認するには、このコマンドを使用します。

例

次に、atlas という名前のデバイスによって acs1 のオーセンティケータ ID（A-ID–Info）を使用して Cisco ACS から受け取った Protected Access Credential（PAC）を表示する例を示します。

```
Router# show cts pacs
  AID: 1100E046659D4275B644BF946EFA49CD
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: 1100E046659D4275B644BF946EFA49CD
    I-ID: atlas
    A-ID-Info: acs1
    Credential Lifetime: 13:59:27 PDT Jun 5 2010
  PAC-Opaque: 000200B000030001000400101100E046659D4275B644BF946EFA49CD0006009400
0301008285A14CB259CA096487096D68D5F34D000000014C09A6AA00093A808ACA80B39EB656AF0B
CA91F3564DF540447A11F9ECDFA4AEC3A193769B80066832495B8C40F6B5B46B685A68411B7DF049
A32F2B03F89ECF948AC4BB85CF855CA186BEF8E2A8C69A7C0BE1BDF6EC27D826896A31821A7BA523
C8BD90072CB8A8D0334F004D4B627D33001B0519D41738F7EDDF3A
  Refresh timer is set for 00:01:24
```

関連コマンド

コマンド	説明
clear cts pac	キーストアから 1 つまたはすべての PAC をクリアします。
cts sxp	ネットワーク デバイスに SXP を設定します。

show cts policy layer3

CTS レイヤ 3 トランスポート コンフィギュレーションに使用されるトラフィック ポリシーおよび例外ポリシーの名前を表示するには、EXEC モードまたは特権 EXEC モードで **show cts policy layer3** コマンドを使用します。

show cts policy layer3 {**ipv4** | **ipv6**}

構文の説明

ipv4	IPv4 ポリシーを指定します。
ipv6	IPv6 ポリシーを指定します

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

トラフィックまたは例外ポリシーは、ローカルで設定されるか、Cisco Secure ACS から取得されます。CTS レイヤ 3 トランスポート機能の詳細については、「cts policy layer3」を参照してください。

例

次に、**show cts policy3** のコマンドの出力を表示します。

```
router# show cts policy layer3 ipv4
No CTS L3 IPV4 policy received from ACS
Local CTS L3 IPv4 exception policy name  : cts-exceptions-local
Local CTS L3 IPv4 traffic policy name     : cts-traffic-local
Current CTS L3 IPv4 exception policy name: cts-exceptions-local
Current CTS L3 IPv4 traffic policy name   : cts-traffic-local
```

関連コマンド

コマンド	説明
cts policy layer3	CTS レイヤ 3 トランスポートのトラフィック ポリシーおよび例外ポリシーを指定します。
cts layer3	トラフィック ポリシーおよび例外ポリシーをイネーブルにし、CTS のレイヤ 3 トランスポート ゲートウェイ インターフェイスに適用します。

show cts policy peer

TrustSec ピアのピア認可ポリシーのデータを表示するには、EXEC モードまたは特権 EXEC モードで **show cts policy peer** コマンドを使用します。

show cts policy peer

構文の説明　このコマンドには、コマンドまたはキーワードはありません。

デフォルト　なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例　次に、すべてのピアの TrustSec ピア認可ポリシーを表示する例を示します。

```
VSS-1# show cts policy peer
CTS Peer Policy
===============
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE
```

出力フィールド	説明
Peer name	ローカル デバイスが接続されたピアの CTS デバイス ID。
Peer SGT	ピアのセキュリティ グループ タグ。
Trusted Peer	TRUE：ローカル デバイスはこのピアから送信される SGT タグが付けられたパケットを信頼します。 FALSE：デバイスはこのピアから送信される SGT タグが付けられたパケットを信頼しません。
Peer Policy Lifetime	リフレッシュされるまでの、ポリシーが有効な時間の長さ。
Peer Last update time	このポリシーが最後にリフレッシュされた時刻
Policy expires in (dd:hr:mm:sec)	このピア ポリシーはこの時間が経過すると期限切れになります

出力フィールド	説明
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)	このピア ポリシーはこの時間が経過するとリフレッシュされます
Cache data applied = NONE	このポリシーはキャッシュから入力されませんでした。つまり、ACS から取得されました

関連コマンド

コマンド	説明
cts refresh	ピア認可ポリシーを強制的にリフレッシュします。
clear cts policy	TrustSec ピアのピア認可ポリシーをクリアします。

show cts provisioning

待機中の RADIUS サーバ CTS プロビジョニング ジョブを表示するには、EXEC モードまたは特権 EXEC モードで **show cts provisioning** コマンドを使用します。

show cts provisioning

構文の説明　このコマンドには、コマンドまたはキーワードはありません。

デフォルト　なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

使用上のガイドライン　Protected Access Credential Provisioning（PAC-provisioning）ジョブ用のキューを表示するには、このコマンドを使用します。PAC が期限切れになるか、またはデバイスが再設定されたときに再プロビジョニングが発生します。

例　次の出力では、CTS のプロビジョニング ドライバが PAC プロビジョニングを再試行している AAA サーバのリストを表示します。

```
router# show cts provisioning
A-ID: 0b2d160f3e4dcf4394262a7f99ea8f63
   Server 41.16.19.201, using existing PAC
      Req-ID EB210008: callback func 418A8990, context 290F14D0
A-ID: Unknown
   Server 41.16.19.203, using shared secret
      Req-ID 49520002: callback func 40540CF0, context AE000007
```

関連コマンド

コマンド	説明
show cts pacs	キーストアの PAC の A-ID および PAC 情報を表示します。
radius-server host	デバイス認証用に RADIUS サーバを指定します。

show cts role-based counters

セキュリティ グループ ACL 強制の統計情報を表示するには、**show cts role-based** カウンタの show コマンドを使用します。カウンタをクリアするには、**clear cts role-based counters** コマンドを使用します。

show cts role-based counters

show cts role-based counters default [**ipv4** | **ipv6**]

show cts role-based counters from {*sgt_num* | **unknown**} [**ipv4** | **ipv6** | **to** {*sgt_num* | **unknown**} [**ipv4** | **ipv6**]]

show cts role-based counters to {*sgt_num* | **unknown**} [**ipv4** | **ipv6** | **]**

show cts role-based counters [**ipv4** | **ipv6**]

構文の説明

default	デフォルト ポリシー カウンタ
from	送信元セキュリティ グループを指定します
ipv4	IP バージョン 4 ネットワークでセキュリティ グループを指定します
ipv6	IP バージョン 6 ネットワークでセキュリティ グループを指定します
to	宛先セキュリティ グループを指定します
sgt_num	（0 ～ 65533）セキュリティ グループ タグ番号を指定します
unknown	すべての送信元グループを指定します

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

セキュリティ グループ ACL（SGACL）強制の統計情報を表示するには、**show cts role-based counters** コマンドを使用します。すべてまたは任意の範囲の統計情報をリセットするには、**clear cts role-based counters** を使用します。

from キーワードで送信元 SGT を、**to** キーワードで宛先 SGT を指定します。**from** および **to** の両方のキーワードを省略すると、すべての統計情報が表示されます。

default キーワードは、デフォルトのユニキャストのポリシー統計情報を表示します。

ipv4 および **ipv6** のいずれも指定しない場合、このコマンドは IPv4 カウンタだけを表示します。

例

次の例は、IPv4 および IPv6 イベントのすべての強制の統計情報を表示します。

```
router# show cts role-based counters
Role-based counters
From    To      SW-Denied       HW-Denied       SW-Permitted    HW_Permitted
2       5       129                 89762               421      7564328
```

```
3        5          37                123456               1325      12345678
3        7           0                 65432                325       2345678
```

関連コマンド

コマンド	説明
clear cts role-based counters	セキュリティ グループ ACL 統計情報カウンタをリセットします。
cts role-based	手動で送信元 IP アドレスをホストまたは VRF 上のセキュリティ グループ タグ（SGT）にマッピングし、SGACL 強制をイネーブルにします。

show cts role-based sgt-map

SXP 送信元 IP と SGT のバインディング テーブル（IP-SGT バインディング）を表示するには、EXEC モードまたは特権 EXEC モードで **show cts role-based sgt-map** コマンドを使用します。

show cts role-based sgt-map {*ipv4_dec* | *ipv4_cidr* | *ipv6_hex* | *ipv6_cidr* | **all** [**ipv4** | **ipv6**] | **host** {*ipv4_decimal* | *ipv6_dec*} | **summary** [**ipv4** | **ipv6**] |

vrf *instance_name* {*ipv4_dec* | *ipv4_cidr* | *ipv6_dec* | *ipv6_cidr* | **all** {**ipv4** | **ipv6**} | **host** {*ipv4_decimal* | *ipv6_dec*} |**summary** {**ipv4** | **ipv6**} }

構文の説明

ipv4_dec	ドット付き 10 進数表記で IPv4 アドレスを指定します。 例（208.77.188.166）
ipv4_cidr	Classless Inter-Domain Routing（CIDR）で IPv4 アドレス範囲を指定します。たとえば、35.0.0.0/8 では、/8 は最上位 8 ビットがネットワークを識別し、最下位 24 ビットがホストを識別することを表します。
ipv6_hex	コロンで区切られた 16 進数の IP Version 6 アドレスを指定します。 たとえば、2001:db8:85a3::8a2e:370:7334 です。
ipv6_cidr	16 進数の CIDR 表記で IPv6 アドレスの範囲を指定します。
host *ipv4_decimal* | *ipv6_hex*	特定の IPv4 または IPv6 ホストのマッピングを指定します。IPv4 にはドット付き 10 進数、IPv6 にはコロン 16 進数を使用します。
all	表示されるすべてのマッピングを指定します。
summary ipv4 | **ipv6**	IPv4 または IPv6 マッピングの概要。キーワードを指定しない場合、IPv4 と IPv6 の両方を表示します。
vrf *instance_name*	マッピング用の VPN ルーティング / 転送インスタンスを指定します。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが Catalyst 4000 シリーズ スイッチに追加されました（**vrf** キーワードなし）。
12.2 (53) SE2	このコマンドは、Catalyst 3750(E) および 3560(E) シリーズ スイッチに追加されました（**vrf** キーワードなし）。
12.2 (53) SE2	このコマンドが Catalyst 3750(X) シリーズ スイッチに追加されました（**vrf** キーワードなし）。

使用上のガイドライン

SXP が適切なセキュリティ グループ タグ（SGT）に送信元 IP アドレスを正しくバインドしていることを確認するには、このコマンドを使用します。VRF のレポートは、特権 EXEC モードからだけ使用できます。

例

次の例は、IP アドレスおよび SGT の送信元名のバインディングを表示します。

```
Router# show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address    SGT Source
============================================
1.1.1.1       7   INTERNAL
10.252.10.1   7   INTERNAL
10.252.10.10  3   LOCAL
10.252.100.1  7   INTERNAL
172.26.208.31 7   INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of INTERNAL bindings = 4
Total number of active   bindings = 5
```

関連コマンド

コマンド	説明
cts role-based	手動でセキュリティ グループ タグ（SGT）に送信元 IP アドレスをマッピングします。
cts sxp	ネットワーク デバイスに SXP を設定します。
show cts sxp	CTS SXP プロトコル情報を表示します

show cts server-list

TrustSec シードおよび非シード デバイスで利用可能な RADIUS サーバのリストを表示するには、EXEC モードまたは特権 EXEC モードで **show cts server-list** コマンドを使用します。

show cts server-list

構文の説明

このコマンドには、コマンドまたはキーワードはありません。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次の例は、TrustSec RADIUS サーバ リストを表示します。

```
Router> show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: ACSServerList1-0001, 1 server(s):
 *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

関連コマンド

コマンド	説明
cts server	CTS のサーバ リストの設定を表示します。

show cts sxp

SXP 接続または SourceIP-to-SGT マッピング情報を表示するには、EXEC モードまたは特権 EXEC モードで **show cts sxp** コマンドを使用します。

show cts sxp {**connections** | **sgt-map**} [**brief** | **vrf** *instance_name*]

構文の説明

connections	CTS SXP 接続情報を表示します。
sgt-map	SXP 経由で受信した IP-SGT マッピングを表示します。
brief	（任意）SXP 情報の省略形を表示します。
vrf *instance_name*	（任意）指定された VRF インスタンス名の SXP 情報を表示します。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました
12.2 (53) SE2	このコマンドが Catalyst 3750(E) および 3560(E) シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが、Catalyst 3750(X) シリーズ スイッチに追加されました。

使用上のガイドライン

ネットワーク デバイスの SXP 設定のステータスを表示するには、**cts sxp connections** のコマンドを使用します。現在の SourceIP-to-SGT のマッピング データベースを表示するには、**cts sxp sgt-map** コマンドを使用します。

例

次の例では、Catalyst 6500 シリーズ スイッチのデフォルト SXP の設定を表示します。

```
Router# show cts sxp connections
 SXP              : Disabled
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
There are no SXP Connections.
```

次に、**brief** キーワードを使用して Catalyst 6500 スイッチの SXP 接続を表示する例を示します。

```
Router# show cts sxp connection brief
 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
```

```
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running

------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
------------------------------------------------------------------------------
2.2.2.1          2.2.2.2          On                0:00:02:14 (dd:hr:mm:sec)
3.3.3.1          3.3.3.2          On                0:00:02:14 (dd:hr:mm:sec)

Total num of SXP Connections = 2
```

次の例では、Catalyst 6500 シリーズ スイッチの SXP 接続を表示します。

```
Router# show cts sxp connections
 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 2.2.2.1
Source IP        : 2.2.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)

----------------------------------------------
Peer IP          : 3.3.3.1
Source IP        : 3.3.3.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)


Total num of SXP Connections = 2
```

次の例は、SXP スピーカーへの接続が切断された SXP リスナーからの出力を表示します。SourceIP-to-SGT のマッピングは 120 秒（削除のホールドダウン タイマーのデフォルト値）の間保持されます。

```
Router# show cts sxp connections
 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 2.2.2.1
Source IP        : 2.2.2.2
Set up           : Peer
Conn status      : Delete_Hold_Down
Connection mode  : SXP Listener
Connection inst# : 1
```

```
TCP conn fd      : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)

---------------------------------------------
Peer IP          : 3.3.3.1
Source IP        : 3.3.3.2
Set up           : Peer
Conn status      : On
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)


Total num of SXP Connections = 2
```

次の例は、SXP を介して学習された現在の SourceIP-to-SGT マッピング データベースを表示します。

```
router# show cts sxp sgt-map
IP-SGT Mappings as follows:
IPv4,SGT: <2.2.2.1 , 7>
source  : SXP;
Peer IP : 2.2.2.1;
Ins Num : 1;
IPv4,SGT: <2.2.2.1 , 7>
source  : SXP;
Peer IP : 3.3.3.1;
Ins Num : 1;
Status  : Active;
IPv4,SGT: <3.3.3.1 , 7>
source  : SXP;
Peer IP : 2.2.2.1;
Ins Num : 1;
```

次の例は、**brief** キーワードを使用して現在の SourceIP-to-SGT マッピング データベースを表示します。

```
Router# show cts sxp sgt-map brief
IP-SGT Mappings as follows:
IPv4,SGT: <2.2.2.1 , 7>
IPv4,SGT: <3.3.3.1 , 7>
IPv4,SGT: <4.4.4.1 , 7>
IPv4,SGT: <43.13.21.41 , 7>
```

関連コマンド

コマンド	説明
cts sxp	ネットワーク デバイスに SXP を設定します。

show cts keystore

ソフトウェアまたはハードウェア暗号化キーストアの内容を表示するには、EXEC モードまたは特権 EXEC モードで **show cts keystore** コマンドを使用します。

show cts keystore

構文の説明　このコマンドには、コマンドまたはキーワードはありません。

デフォルト　なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが **show cts keystore** として Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン　このコマンドは、キーストアに保存されているすべてのレコードを示します。保存された秘密は表示されません。

例　次の例は、Catalyst 6500 ソフトウェア エミュレート キーストアの内容を表示します。

```
Router# show cts keystore
No hardware keystore present, using software emulation.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):

Index  Type  Name
-----  ----  ----
    0     P  05181D8147015544BC20F0119BE8717E
    1     S  CTS-password
```

次の例は、Catalyst 6500 ハードウェア キーストアの内容を表示します。

```
Router# show cts keystore
CTS keystore firmware version 2.0.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):

Index  Type  Name
-----  ----  ----
    0     S  CTS-passwordFOX094901KW
    1     P  74656D706F72617279

Hardware Keystore error counters:
       FW Panics = 0
       FW Resets = 0
       RX FIFO underruns = 12
       RX timeouts = 0
```

```
RX bad checksums = 0
RX bad fragment lengths = 0
Corruption Detected in keystore = 0
```

関連コマンド

コマンド	説明
cts credentials	TrustSec ID およびパスワードを指定します。
cts sxp	ネットワーク デバイスに SXP を設定します。

show platform cts reflector

特定のインターフェイスの Cisco TrustSec リフレクタ モード（Ingress、Egress、Pure、No CTS）のステータスを表示するには、**show platform cts reflector** コマンドを使用します。

show platformcts reflector interface type *slot*/*port*

構文の説明

interface type *slot*/*port*	ステータスを表示するインターフェイス タイプ、スロット、およびポートを指定します。

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

関連コマンド

コマンド	説明
platform cts	TrustSec 出力または入力のリフレクタをイネーブルにします。

timer（cts do1x インターフェイス サブモード）

dot1x 認証タイマーを設定するには、タイマーの認証の CTS dot1x インターフェイス コンフィギュレーション コマンドを使用します。dot1x 再認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] timer reauthentication *seconds*

構文の説明

reauthentication *seconds*	（0 ～ 2147483）秒単位のタイマー。dot1x 再認証をディセーブルにするには、0 を入力します。

デフォルト

デフォルトの期間は 86,400 秒（24 時間）です。

コマンド モード

CTS dot1x インターフェイス コンフィギュレーション サブモード（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

認証サーバが期間を指定していない場合は、**timer reauthentication** コマンドを使用して dot1x 再認証期間を設定します。再認証期間が指定されていない場合、デフォルトの期間は 86,400 秒です。dot1x 再認証をディセーブルにするには、このコマンドの **no** 形式を使用するか、または 0 秒の期間を指定します。デフォルト値に戻すには、**default timer reauthentication** コマンドを使用します。

例

次の例では、802.1X 再認証期間を 48 時間（172,800 秒）に設定します。

```
router# config t
router(config)# interface gigabitEthernet 6/1
router(config-if)# cts dot1x
router(config-if-cts-dot1x)# timer reauthentication 172800
```

関連コマンド

コマンド	説明
show cts interface	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。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
propagate（cts dot1x サブモード）	dot1x モードの SGT 伝搬をイネーブルまたはディセーブルにします。

APPENDIX A

Catalyst 3750、3560、および 2960 シリーズ スイッチのリリース ノート

Cisco TrustSec 機能の最小 Cisco IOS Release

機能	必要な最小 Cisco IOS Release	Catalyst スイッチ サポート
Cisco TrustSec SGA、SGT と SGACL	15.0(2)SE	3750-X および 3650-X
Cisco TrustSec SXP バージョン 2、Syslog メッセージおよび SNMP サポート	15.0(2)SE 15.0(1)SE 12.2(53)SE2	3560-C、2960-S、2960-C 3750 および 3560 3750-X および 3560-X

TrustSec SGT と SGACL の設定時の注意事項および制約事項

次の注意事項と制約事項は、Catalyst 3750-X および Catalyst 3560-X スイッチの Cisco TrustSec SGT と SGACL の設定に適用されます。

- SGT に静的に IP サブネットをマッピングできません。IP アドレスを SGT にマッピングできるだけです。IP-address-to-SGT マッピングを設定する場合、IP アドレス プレフィックスは 32 である必要があります。
- ポートがマルチ認証モードに設定されると、そのポートに接続されたすべてのホストは同じ SGT を割り当てる必要があります。ホストが認証を試みると、割り当てられた SGT は以前に認証されたホストに割り当てられた SGT と同じでなければなりません。ホストが認証を試みたとき、その SGT が以前に認証されたホストの SGT と異なる場合、これらのホストが属する VLAN ポート（VP）は errdisable になります。

- Cisco TrustSec 強制は VLAN トランク リンクの最大 8 つの VLAN でだけサポートされます。VLAN トランク リンクに設定された VLAN が 8 つを超えていて、Cisco TrustSec 強制がこれらの VLAN でイネーブルになっている場合、それらの VLAN トランク リンクのスイッチ ポートが errdisable になります。
- スイッチは、エンドホストがスイッチに隣接するレイヤ 2 である場合にだけ SGT を割り当て、SXP リスニングに基づいて、対応する SGACL をエンドホストに適用できます。
- ポートから SGT へのマッピングは、Cisco TrustSec リンク（つまり、スイッチ間リンク）でだけ設定できます。ポートから SGT へのマッピングはホストとスイッチの間リンクには設定できません。
- ポートから SGT へのマッピングがポートで設定されている場合、SGT はそのポートのすべての入力トラフィックに割り当てられます。ポート出力トラフィックに対する SGACL 強制はありません。

APPENDIX B

Catalyst 4500 シリーズ スイッチのノート

このセクションは、意図的に空白にしています。

このセクションは、意図的に空白にしています。

APPENDIX C

Catalyst 6500 シリーズ スイッチのノート

この付録の内容は、次のとおりです。

TrustSec のサポート対象ハードウェア

TrustSec 対応スーパーバイザおよびラインカードは、次の URL の『*Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection*』の表 3 および 4 にリストされています。

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-658388.html

TrustSec ハードウェア対応ではない Catalyst 6500 シリーズ スイッチは、SAP または 802.1AE リンク暗号化を使用しないで TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）を実装しています。

Flexible NetFlow のサポート

リリース	機能の履歴
IOS 12.2(50) SY IP ベース LAN イメージ	次の Flexible NetFlow コマンドおよびフロー オブジェクトは Catalyst 6500 シリーズ スイッチで導入されました。 • **cts role-based** {**ip** | **ipv6**} **flow monitor** *monitor_name* **dropped** • cts source group-tag • cts destination group-tag

標準の 5 タプル フロー オブジェクトを使用してフロー レコードに SGT および DGT フロー オブジェクトが設定されている場合、Flexible NetFlow は、SGACL 強制によってドロップされたパケットに対応できます

flow record および **flow exporter** 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フロー レコードおよびフロー エクスポータを設定してから、それらを **flow monitor** コマンドを使用してフロー モニタに追加します。**show flow** show コマンドを使用して設定を確認します。

SGACL のドロップされたパケットだけを収集するには、**[no] cts role-based {ip | ipv6} flow monitor dropped** 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。

Flexible NetFlow の概要および設定の詳細については、次のマニュアルを参照してください。

『Cisco IOS Flexible Netflow Configuration Guide, Release 15.0SY』

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-0sy/fnf-15-0sy-book.html

『Catalyst 6500 Release 15.0SY Software Configuration Guide』

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/15_0_sy_swcg.html

設定例

IPV4 フロー レコードの設定の抜粋（5 タプル、方向、SGT、DGT）

```
router(config)# flow record cts-record-ipv4
router(config-flow-record)# match ipv4 protocol
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match transport source-port
router(config-flow-record)# match transport destination-port
router(config-flow-record)# match flow direction
router(config-flow-record)# match flow cts source group-tag
router(config-flow-record)# match flow cts destination group-tag
router(config-flow-record)# collect counter packets
```

IPV6 フロー レコードの設定の抜粋（5 タプル、方向、SGT、DGT）

```
router(config)# flow record cts-record-ipv6
router(config-flow-record)# match ipv6 protocol
router(config-flow-record)# match ipv6 source address
router(config-flow-record)# match ipv6 destination address
router(config-flow-record)# match transport source-port
router(config-flow-record)# match transport destination-port
router(config-flow-record)# match flow direction
router(config-flow-record)# match flow cts source group-tag
router(config-flow-record)# match flow cts destination group-tag
router(config-flow-record)# collect counter packets
```

IPv4 フロー モニタの設定の抜粋

```
router(config)# flow monitor cts-monitor-ipv4
router(config-flow-monitor)# record cts-record-ipv4
```

IPv6 フロー モニタの設定の抜粋

```
router(config)# flow monitor cts-monitor-ipv6
router(config-flow-monitor)# record cts-record-ipv6
```

グローバル フロー モニタの設定の抜粋（IPv4 および IPv6）

次の設定は、ルータまたはスイッチのすべての TrustSec インターフェイスのロールベース アクセス コントロール リスト（RBACL）によってドロップされたパケットにフロー モニタを適用します。

```
router(config)# cts role-based ip flow monitor cts-monitor-ipv4 dropped
router(config)# cts role-based ipv6 flow monitor cts-monitor-ipv6 dropped
```

インターフェイスのモニタ設定の抜粋

フロー モニタはインターフェイスごとに接続でき、入力（受信）、出力（発信）、マルチキャスト、ユニキャスト、またはレイヤ 2 でスイッチングされるトラフィックの組み合わせでフィルタリングするように設定できます。

IPv6 の場合、フロー モニタは Cisco IOS Release 12.2(50) SY でルーティングされたトラフィックに対してだけサポートされます。

```
router(config)# interface TenGigabitEthernet 8/1
router(config-if)# ip address 192.1.1.1 255.255.255.0

;; Ingress IPv4 unicast only and egress unicast only
router(config-if)# ip flow monitor cts-monitor-ipv4 unicast input
router(config-if)# ip flow monitor cts-monitor-ipv4 unicast output

;; Ingress IPV4 L2-switched traffic only
router(config-if)# ip flow monitor cts-monitor-ipv4 layer2-switched input

;; Ingress Ipv4 multicast and egress IPv4 multicast traffic only
router(config-if)# ip flow monitor cts-monitor-ipv4 multicast input
router(config-if)# ip flow monitor cts-monitor-ipv4 multicast output

;; For both Unicast/multicast egress traffic
router(config-if)# ip flow monitor cts-monitor-ipv4 output

;; For both Unicast/multicast ingress traffic
router(config-if)# ip flow monitor cts-monitor-ipv4 input

;; For Ipv6 only the following are supported in Cisco IOS Release 12.2(50)SY
router(config-if)# ipv6 address 2022::22:1:1:11/64
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 input
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 unicast input
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 output
router(config-if)# ipv6 flow monitor cts-monitor-ipv6 unicast output
```

Flexible NetFlow の show コマンド

show flow record

show flow monitor

show flow exporter

show flow interface

show cts role-based counters

show flow monitor <monitor_name> cache

show flow monitor <monitor_name> statistics

show platform flow ip

show platform software flow internal fnf

show platform hardware flow table flowmask

show platform hardware flow table profile

show platform hardware acl entry rbacl all

show platform hardware acl entry tcam

show platform software flow internal export

show platform software flow internal export statistics

show platform internal export information

show platform internal export statistics

TrustSec システム エラー メッセージ

Cisco TrustSec システム エラー メッセージは、次の URL の『Cisco Catalyst 6500 Series Switches Error and System Messages』ガイドにリストされています。
http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guides_list.html

エラー メッセージ デコーダ ツールは次の URL にあります。
http://www.cisco.com/en/US/support/tsd_most_requested_tools.html

FIPS のサポート

Catalyst 6500 シリーズ スイッチ ソフトウェアおよびハードウェアの組み合わせに対する、連邦情報処理標準（FIPS）認証ドキュメントは、次の Web サイトで公開されています。

http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_fips140.html

Catalyst 6500 シリーズの FIPS 認証ドキュメントでは、ソフトウェアとハードウェアの組み合わせごとに FIPS の概念および実装を説明します。

FIPS の設定時の TrustSec に関する考慮事項

ご使用のハードウェアおよびソフトウェア設定に適した FIPS 認証ガイドに従って、Catalyst スイッチの初期設定、初期化、設定手順を実行してください。

FIPS のライセンス要件

FIPS は Catalyst 6500 シリーズ スイッチのライセンスは必要としません。

FIPS 設定の前提条件

- Telnet をディセーブルにします。ユーザのログインはセキュア シェル（SSH）だけで行ってください。

- SNMP v1 および v2 をディセーブルにしてください。SNMP v3 に対して設定された、デバイス上の既存ユーザ アカウントのいずれについても、認証およびプライバシー用 AES/3DES は SHA で設定されていなければなりません。
- SSH サーバの RSA1 キー ペアすべてを削除してください。

FIPS の注意事項と制約事項

- RADIUS keywrap 機能は Cisco Identity Services Engine 1.1 または Cisco ACS Release 5.2 以降のリリースだけで動作します。
- モジュールへの HTTPS/TLS アクセスは SSLv3.1/TLSv1.0 および FIPS で承認されているアルゴリズムを使用して FIPS で承認されている動作モードで許可されます。
- モジュールへの SSH アクセスは SSHv2 と FIPS で承認されているアルゴリズムを使用して FIPS で承認されている動作モードで許可されます。多くの SSH クライアントは、すべての暗号操作を FIPS 140-2 レベル 2 準拠にして、FIPS モードに設定できる暗号ライブラリを提供します。
- パスワードは、最低 1 文字は数字を含む 8 文字以上の英数字であることが必要です。

FIPS のデフォルト設定

デフォルトは FIPS モードはディセーブル、RADIUS keywrap はディセーブルです。

GLOSSARY

数値

802.1AE IEEE 802.1AE は Cisco TrustSec ハードウェア対応デバイス間で使用されるレイヤ 2 のホップバイホップ暗号化プロセスを定義します。TrustSec では、キー管理および暗号ネゴシエーション メカニズムに、SAP を使用します。

C

CTS Cisco Trusted Security、または Cisco TrustSec、または TrustSec。

E

EAC エンドポイント アドミッション コントロール。エンドポイントの特定の IP アドレスへの SGT 値の割り当てプロセス。ハードウェアおよびソフトウェアのサポートに応じて、802.1X 認証、MAC 認証バイパス、Web 認証バイパス、手動割り当て、または IPM で、SGT を送信元 IP アドレスに割り当てることができます。

EAP Extensible Authentication Protocol。EAP-FAST は、NDAC 認証用に TrustSec ネットワークで使用する EAP バリアントです。

I

IPM アイデンティティとポートのマッピング。エンドポイントが接続されているポートのアイデンティティを定義し、このアイデンティティを使用して Cisco Secure ACS サーバで特定の SGT 値を検索する、スイッチの方式。

M

MACSec ホップ単位のリンク暗号化を提供するための、IEEE 802.1AE に基づく Media Access Control Security。TrustSec ハードウェア対応デバイスは、TrustSec ハードウェア対応ピアとの MACSec リンクを確立できます。

N

NDAC ネットワーク デバイス アドミッション コントロール。802.1X プロセスを使用してピアを認証および認可する CTS デバイス間の相互認証のメカニズム。EAP-FAST は、EAP タイプとして使用されます。

R

RBAC ロールベース アクセス コントロール。エンドポイントのロールに基づくアクセス コントロール メカニズム。RBAC は複数のロール ファクタで特定のエンティティの最終ポリシーを取得することができるという点で、RBAC はグループ ベースのアクセス コントロールとは異なります。

RBACL ロールベース アクセス コントロール リスト。TrustSec は Cisco Secure ACS の RBAC 機能を使用するため、SGACL を特徴付けるためによく使用されます。

S

SAP セキュリティ アソシエーション プロトコル。NDAC の認証および認可の成功後に、リンク暗号化のキーおよび暗号スイートをネゴシエートします。SAP は 802.11i 標準をベースとしています。SAP ネゴシエーションは NDAC プロセス後自動的に開始できます。それ以外の場合は PMK をインターフェイスでスタティックに設定できます。

Seed Device シード デバイスは、TrustSec ポリシー認可のために Cisco Secure ACS で認証する最初の TrustSec ハードウェア対応デバイスです。シード デバイスは次の TrustSec サプリカント デバイスのオーセンティケータになり、そのサプリカント デバイスはさらにそのサプリカント デバイスのオーセンティケータになります。

SGACL セキュリティ グループ アクセス コントロール リスト。SGT の値に従ってフィルタリングを行う、レイヤ 3 からレイヤ 4 へのアクセス コントロール リスト。通常、フィルタリングは CTS ドメインの出力ポートで発生します。

SGT セキュリティ グループ タグ。ロールに基づいてトラフィックを分類するために、イーサネット フレームに追加されたレイヤ 2 タグ。タグの処理は、CTS のドメインの入力で実行されます。SGT は Cisco Secure ACS 設定で定義されています。

SXP SGT 交換プロトコル。SXP をサポートするデバイスが送信元 IP と SGT のバインディング テーブルを作成し、MD5 ベースの認証を使用して範囲外の TCP 接続を通じて TrustSec ハードウェア対応デバイスにそのテーブルを転送できるようにします。

T

TrustSec Trusted Security。Cisco Trusted Security（CTS）と同じです。

TrustSec ソフトウェア対応 TrustSec ピアとの NDAC および SXP 接続を確立できるネットワーク デバイス。

TrustSec ハードウェア対応 トラフィックに SGT をタグ付けし、SGACL を適用し、TrustSec ピアとの MACSec の接続を確立できるネットワーク デバイス。

お

オーセンティケータ TrustSec ネットワークのメンバであるネットワーク デバイスは、サプリカント デバイスに対するオーセンティケータのロールで、TrustSec ネットワークに参加しようとするネットワーク デバイスを認証できます。NDAC はサプリカント デバイスが TrustSec ネットワークに入ることを許可されるプロセスです。

さ

サプリカント TrustSec において、認証された TrustSec ネットワーク デバイス（オーセンティケータ）からの TrustSec 認証を要求している、Cisco Secure ACS に直接接続していないネットワーク デバイス。NDAC は、サプリカント デバイスが TrustSec ネットワークに入ることを許可されるプロセスです。

ひ

非シード デバイス 非シード デバイスには Cisco Secure ACS への直接 IP 接続がないため、シード デバイスまたはすでに TrustSec ネットワークに登録されたデバイスなどのその他のデバイスが、非シード デバイスの TrustSec ネットワークへの参加を認証および許可する必要があります、

INDEX

数字

C

D

E

F

G

I

L

M

N

P

S

T

V

W

あ

い

え

か

さ

し

せ

に

ね

ふ

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/