Cisco TrustSec（CTS）

Cisco TrustSec は、ネットワーク内のユーザ、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコ ネットワーク デバイスのセキュリティの改善に関する包括的な用語です。TrustSec は、特定のロールについてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセス コントロールを実現します。TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。

Cisco TrustSec の主要コンポーネントは、Cisco Identity Services Engine です。これは、Cisco ISE で TrustSec アイデンティティおよびセキュリティ グループ ACL（SGACL）を使用してスイッチをプロビジョニングする場合に一般的です。ただし、これらは Catalyst 6500 で手動で設定する場合があります。

Cisco Catalyst 6500 シリーズ スイッチで Cisco Trustsec を設定するには、次の URL の『*Cisco TrustSec Switch Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Cisco TrustSec General Availability リリースのリリース ノートについては、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html

Cisco TrustSec Solution の詳細（概要、データシート、およびケース スタディなど）については、次の URL を参照してください。

http://www.cisco.com/en/US/netsol/ns1051/index.html

表 1 に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

Catalyst 6500 ラインカードでサポートされる TrustSec 機能の詳細については、「サポートされるハードウェア」を参照してください。

表 1　Cisco TrustSec の主要機能：TrustSec 1.0 General Availability 2010 Release

Cisco TrustSec の機能	説明
802.1AE タギング（MACSec）	IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。 MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。 この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。
エンドポイント アドミッション コントロール（EAC）	EAC は、TrustSec ドメインに接続しているエンドポイント ユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。
ネットワーク デバイス アドミッション コントロール（NDAC）	NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。
セキュリティ グループ アクセス コントロール リスト（SGACL）	セキュリティ グループ アクセス コントロール リスト（SGACL）は、セキュリティ グループ タグをポリシーと関連付けます。ポリシーは、TrustSec ドメインから出力される SGT タグ付きトラフィックに対して適用されます。
セキュリティ アソシエーション プロトコル（SAP）	NDAC 認証のあと、セキュリティ アソシエーション プロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。
セキュリティ グループ タグ（SGT）	SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。
SGT 交換プロトコル（SXP）	Security Group Tag Exchange Protocol（SXP）。TrustSec ハードウェア対応ではないデバイスは、SXP により、Cisco ACS から認証されたユーザまたはデバイスの SGT 属性を受信し、sourceIP-to-SGT バインディングを TrustSec ハードウェア対応デバイスに転送し、タギングおよび SGACL を適用できます。

サポートされるハードウェア

表 63-2 に、Catalyst 6500 ラインカードでサポートされている Cisco TrustSec レベルの一覧を示します。この表の内容は、次の URL にあるホワイト ペーパー『*Cisco Catalyst 6500 Series with Supervisor Engine 2T: Enabling Cisco TrustSec with Investment Protection*』から入手されたものです。

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

表 63-2　Cisco TrustSec の Cisco Catalyst 6500 ラインカードのサポート レベル

Cisco TrustSec のサポート レベル	説明	ラインカード
Cisco TrustSec 対応	セキュリティ グループ タグ インポジションおよび IEEE 802.1AE MACsec のハードウェア アクセラレーションを使用する完全な Cisco TrustSec 機能をサポートします。	Supervisor Engine 2T
Cisco TrustSec 認識	セキュリティ グループ タグ インポジションまたは IEEE 802.1AE MACsec をサポートしていません。これらのラインカードは、セキュリティ グループ タグ情報を含む転送の決定を理解できます。これにより、出力の Cisco TrustSec 対応ラインカードにトラフィックを転送できます。	• WS-X6716-10T • WS-X6716-10GE
Cisco TrustSec の使用に非対応	セキュリティ グループ タグ インポジションまたは IEEE 802.1AE MACsec をサポートせず、セキュリティ グループ タグ情報を含む転送の決定を解釈できません。	• WS-X6724-SFP • WS-X6748-SFP • WS-X6748-GE-TX • WS-X6704-10G • WS-X6148 シリーズ（すべて）

すべての Cisco TrustSec ハードウェア プラットフォームおよび機能のサポートの詳細については、次の URL にある TrustSec Product Bulletin を参照してください。

http://www.cisco.com/en/US/netsol/ns1051/index.html