CHAPTER 44

Cisco TrustSec の設定

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制御を実現します。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 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

『Release Notes for Cisco TrustSec 1.0 General Availability 2010 Release』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_xplat.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 44-1 に、TrustSec がイネーブルになったネットワーク デバイスで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるネットワーク デバイスの数および各デバイスでサポートされる TrustSec 機能の数は増加しています。実装される 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 44-1　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 アクセス制御リスト（SGACL）	セキュリティ グループ アクセス制御リスト（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 リンク暗号化の鍵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 Exchange Protocol（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 44-2 に、Cisco IOS 12.2(33) SXI4 のリリース時点で各プラットフォームでサポートされている TrustSec 機能を示します。

表 44-2　機能およびプラットフォームのサポート：TrustSec 1.0 General Availability 2010 Release

ハードウェア	ソフトウェア リリース	導入された TrustSec 機能
Catalyst 3560 シリーズ	Cisco IOS 12.2 (53) SE	EAC; SXP
Catalyst 3750 シリーズ	Cisco IOS 12.2 (53) SE	EAC; SXP
Catalyst 4500 シリーズ	Cisco IOS 12.2 (50) SG5	EAC; SXP
Catalyst 6500 シリーズ	Cisco IOS 12.2(33) SXI3[1]	EAC; SXP; NDAC（SAP なし）
Nexus 7000 シリーズ	Cisco NX-OS 4.2.1	EAC; SXP; NDAC; SGACL; MACSec

1. Cisco TrustSec は、SXI3 において Catalyst 6500 シリーズ上で実装されましたが、SXI4 において通常使用可能とアナウンスされました。