CHAPTER 11

MACsec の暗号化設定

この章では、Catalyst 3560-C スイッチで Media Access Control Security（MACsec）暗号化を設定する方法について説明します。

- 「MACsec と Cisco TrustSec の概要」（P.11-1）
- 「Media Access Control Security と MACsec キーの承諾の概要」（P.11-2）
- 「MKA および MACsec の設定」（P.11-6）
- 「Cisco TrustSec MACsec について」（P.11-8）
- 「Cisco TrustSec MACsec の設定」（P.11-10）

MACsec と Cisco TrustSec の概要

MACsec は 2 台の MACsec 対応デバイス間のパケットの認証と暗号化の IEEE 802.1AE 規格です。Catalyst 3560-C スイッチは、スイッチとホスト デバイス間の暗号化のために、ダウンリンク ポートとアップリンク ポートで MACsec Key Agreement（MKA）を使用した 802.1AE 暗号化をサポートします。また、スイッチは、Cisco 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）および Security Association Protocol（SAP）キー交換を使用して MACsec リンク層スイッチ間セキュリティをサポートします。リンク層セキュリティはスイッチ間のパケット認証とスイッチ間の MACsec 暗号化の両方を含みます（暗号化は任意です）。

（注） MACsec は、no payload encryption（NPE）または LAN Base イメージによってユニバーサル IP イメージが実行されているスイッチではサポートされません。

スイッチのすべてのダウンリンク ポートおよびアップリンク ポートで、Cisco TrustSec MACsec のリンク層スイッチ間セキュリティを実行できます。

表 1 にスイッチのポートでの MACsec のサポートを一覧します。

表 1　スイッチ ポートの MACsec サポート

インターフェイス	接続	MACsec のサポート
ユーザに送信されるダウンリンク ポート	スイッチからホストへ	MKA MACsec 暗号化
他のスイッチに接続されているスイッチ ポート	スイッチからスイッチへ	Cisco TrustSec NDAC MACsec

Cisco TrustSec と Cisco SAP はスイッチ間のリンクにのみ使用され、PC や IP 電話などのエンド ホストに接続されたスイッチ ポートではサポートされません。MKA はスイッチからホストへのリンク用であり、スイッチ間のリンクではサポートされません。ホスト側のリンクは、IEEE 802.1x の有無にかかわらず異種デバイスを扱うために、一般に柔軟な認証順序を使用し、オプションで MKA 暗号を使用できます。Cisco NDAC および SAP は、コンパクトなスイッチがワイヤリング クローゼットの外側にセキュリティを拡張するために使用する、ネットワーク エッジ アクセス トポロジ（NEAT）と相互排他的です。

Media Access Control Security と MACsec キーの承諾の概要

802.1AE で定義された MACsec では、暗号化キー入力のためにアウトオブバンド方式を使用することによって、有線ネットワーク上で MAC レイヤの暗号化を実現します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。MKA と MACsec は、802.1x 拡張認証プロトコル（EAP）フレームワークを使用した認証に成功した後に実装されます。ホスト側のリンク（ネットワーク アクセス デバイスと、PC や IP 電話などのエンドポイント デバイス間のリンク）だけが MACsec を使用して保護できます。Catalyst 3560-C スイッチでは、ホスト側のリンク（ネットワーク アクセス デバイスと、PC や IP 電話などのエンドポイント デバイス間のリンク）だけが MACsec を使用して保護できます。MACsec は、ダウンリンク インターフェイス ギガビット イーサネット 0/1 から 0/8 でサポートされています。

MACsec を使用するスイッチでは、クライアントに関連付けられたポリシーに応じて、MACsec フレームまたは非 MACsec フレームを許可します。MACsec フレームは暗号化され、Integrity Check Value（ICV; 整合性チェック値）で保護されます。スイッチはクライアントからフレームを受信すると、MKA によって提供されたセッション キーを使用してこれらのフレームを暗号化し、正しい ICV を計算します。スイッチはこの ICV をフレーム内の ICV と比較します。一致しない場合は、フレームが破棄されます。また、スイッチは現在のセッション キーを使用して、ICV を暗号化し、セキュアなポート（セキュアな MAC サービスをクライアントに提供するために使用されるアクセス ポイント）を介して送信されたフレームに追加します。

MKA プロトコルは、基礎となる MACsec プロトコルで使用される暗号キーを管理します。MKA の基本要件は 802.1x-REV で定義されます。MKA プロトコルでは 802.1x を拡張し、相互認証の確認によってピアを検出し、MACsec 秘密キーを共有してピアで交換されるデータを保護できます。

EAP フレームワークでは、新しく定義された EAP-over-LAN（EAPOL）パケットとして MKA を実装します。EAP 認証では、データ交換で両方のパートナーで共有される Master Session Key（MSK; マスター セッション キー）を生成します。EAP セッション ID を入力すると、セキュアな Connectivity Association Key Name（CKN; 接続アソシエーション キー名）が生成されます。スイッチはオーセンティケータであるため、キー サーバでもあり、ランダムな 128 ビットのセキュア アソシエーション キー（SAK）を生成し、クライアント パートナーに送信します。クライアントはキー サーバではなく、単一の MKA エンティティであるキー サーバとだけ対話できます。キーの派生と生成の後で、スイッチは定期的にトランスポートをパートナーに送信します。デフォルトの間隔は 2 秒間です。

EAPOL プロトコル データ ユニット（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。MKA セッションと参加者は、MKA ライフタイム（6 秒間）が経過しても参加者から MKPDU を受信していない場合に削除されます。たとえば、クライアントが接続を解除した場合、スイッチ上の参加者はクライアントから最後の MKPDU を受信した後、6 秒間が経過するまで MKA の動作を継続します。

詳細については、次の項を参照してください。

- 「MKA ポリシー」（P.11-3）
- 「仮想ポート」（P.11-3）

- 「MACsec、MKA、および 802.1x ホスト モード」（P.11-3）
- 「MACsec、MKA、および 802.1x ホスト モード」（P.11-3）
- 「MKA 統計情報」（P.11-5）

MKA ポリシー

定義済みの MKA ポリシーをインターフェイスに適用すると、インターフェイス上で MKA がイネーブルになります。MKA ポリシーを削除すると、そのインターフェイス上で MKA がディセーブルになります。次のオプションを設定可能です。

- 16 文字以下の ASCII 文字によるポリシー名。
- 物理インターフェイスごとの 0 バイト、30 バイト、または 50 バイトの機密保持（暗号化）オフセット。
- 再送保護。

  許可される順序外のフレームの数によって定義される MACsec ウィンドウ サイズを設定できます。この値は MACsec でセキュリティ アソシエーションをインストールする際に使用されます。値 0 は、フレームが正しい順序で許可されることを意味します。

仮想ポート

仮想ポートは、1 つの物理ポート上の複数のセキュアな接続アソシエーションに使用します。各接続アソシエーション（ペア）は仮想ポートを表します。1 つの物理ポートにつき、仮想ポートは最大 2 つです。2 つの仮想ポートのうち、1 つだけをデータ VLAN の一部とすることができます。もう 1 つは、音声 VLAN に対してパケットを外部的にタグ付けする必要があります。同じポートで同じ VLAN 内のセキュアなセッションとセキュアでないセッションを同時にホストすることはできません。この制限のため、802.1x マルチ認証モードはサポートされません。

この制限の例外は、マルチホスト モードで最初の MACsec サプリカントが正常に認証され、スイッチに接続されたハブに接続される場合です。ハブに接続された非 MACsec ホストでは、マルチホスト モードであるため、認証なしでトラフィックを送信できます。最初にクライアントが成功した後、他のクライアントでは認証が必要ないため、マルチホスト モードを使用することは推奨しません。

仮想ポートは、接続アソシエーションの任意の ID を表し、MKA プロトコル外では意味を持ちません。仮想ポートは個々の論理ポート ID に対応します。仮想ポートの有効なポート ID は 0x0002 ～ 0xFFFF です。各仮想ポートは、16 ビットのポート ID に連結された物理インターフェイスの MAC アドレスに基づいて、一意の Secure Channel Identifier（SCI; セキュア チャネル ID）を受け取ります。

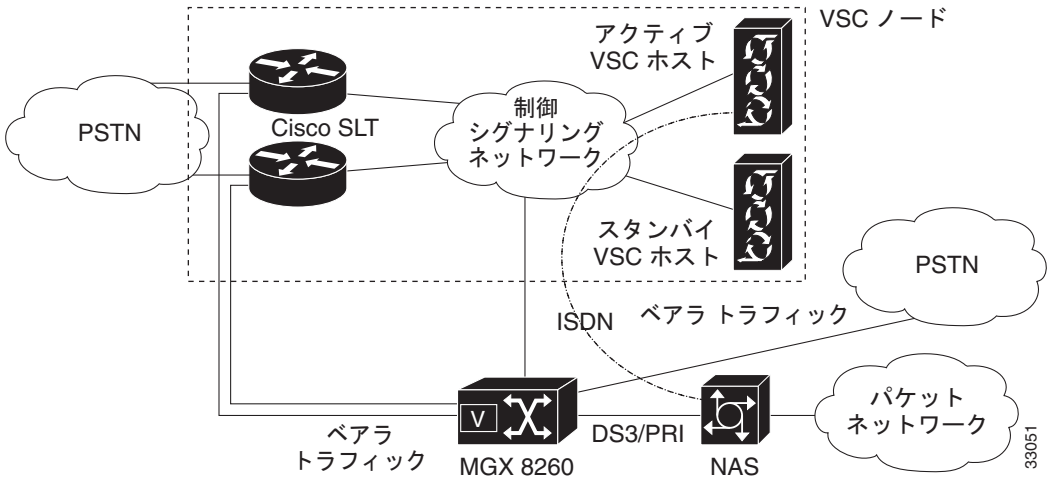
MACsec、MKA、および 802.1x ホスト モード

MACsec と MKA プロトコルは、802.1x シングルホスト モード、マルチホスト モード、またはマルチドメイン認証（MDA）モードで使用できます。マルチ認証モードはサポートされません。

シングルホスト モード

図 11-1 に、MKA を使用して、MACsec で 1 つの EAP 認証済みセッションをセキュアにする方法を示します。

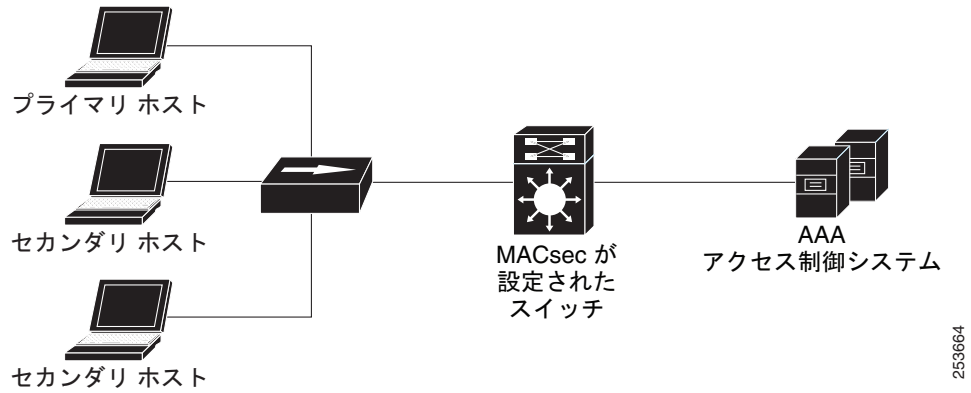
図 11-1　セキュアなデータ セッションでのシングルホスト モードの MACsec



マルチホスト モード

標準（802.1x REV ではない）802 の マルチホスト モードでは、1 つの認証に基づいてポートが開いているか、閉じられています。プライマリ セキュア クライアント サービスのクライアント ホストなど、あるユーザが認証されると、同じポートに接続されているホストに同じレベルのネットワーク アクセスが提供されます。セカンダリ ホストが MACsec サプリカントの場合、認証できず、トラフィック フローは発生しません。非 MACsec ホストであるセカンダリ ホストは、マルチホスト モードであるため、認証なしでネットワークにトラフィックを送信できます。図 11-2 を参照してください。

図 11-2　標準マルチホスト モードの MACsec：非セキュア



マルチホスト モードを使用することは推奨しません。これは最初にクライアントが成功した後、他のクライアントでは認証が必要ないことから、安全性が低いためです。

MKA 統計情報

一部の MKA カウンタはグローバルに集約され、その他のカウンタはグローバルとセッション単位の両方で更新されます。また、MKA セッションのステータスに関する情報も取得できます。

次の例では、**show mka statistics** コマンドの出力を示します。

```
SWitch# show mka statistics
MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 32
   Reauthentication Attempts.. 31

   Deleted (Secured).......... 1
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 32
   Pairwise CAK Rekeys........ 31
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated............. 32
   SAKs Rekeyed............... 31
   SAKs Received.............. 0
   SAK Responses Received..... 32

MKPDU Statistics
   MKPDUs Validated & Rx...... 580
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 597
      "Distributed SAK"..... 32
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Bring-up Failures.................. 0
Reauthentication Failures.......... 0

SAK Failures
   SAK Generation.................. 0
   Hash Key Generation............. 0
   SAK Encryption/Wrap............. 0
   SAK Decryption/Unwrap........... 0

CA Failures
   Group CAK Generation............ 0
   Group CAK Encryption/Wrap....... 0
   Group CAK Decryption/Unwrap..... 0
   Pairwise CAK Derivation......... 0
   CKN Derivation.................. 0
   ICK Derivation.................. 0
   KEK Derivation.................. 0
   Invalid Peer MACsec Capability.. 2

MACsec Failures
   Rx SC Creation.................. 0
   Tx SC Creation.................. 0
   Rx SA Installation.............. 0
   Tx SA Installation.............. 0
```

```
MKPDU Failures
   MKPDU Tx..................... 0
   MKPDU Rx Validation.......... 0
   MKPDU Rx Bad Peer MN......... 0
   MKPDU Rx Non-recent Peerlist MN.. 0
```

出力フィールドの説明については、このリリースに対応するコマンド リファレンスを参照してください。

MKA および MACsec の設定

- 「MACsec MKA のデフォルト設定」（P.11-6）
- 「MKA ポリシーの設定」（P.11-6）
- 「インターフェイスでの MACsec の設定」（P.11-7）

MACsec MKA のデフォルト設定

MACsec はディセーブルです。MKA ポリシーは設定されていません。

MKA ポリシーの設定

MKA プロトコル ポリシーを作成するには、特権 EXEC モードで次の手順を実行します。MKA では 802.1x をイネーブルにすることも必要であることに注意してください。

	コマンド	目的
ステップ 1	**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	**mka policy** *policy name*	MKA ポリシーを指定し、MKA ポリシー コンフィギュレーション モードを開始します。ポリシー名の長さは最大で 16 文字です。
ステップ 3	**replay-protection window-size** *frames*	再送保護をイネーブルにして、ウィンドウ サイズをフレームの数で設定します。指定できる範囲は 0 ～ 4294967295 です。デフォルトのウィンドウ サイズは 0 です。 ウィンドウ サイズに 0 を入力することと、**no replay-protection** コマンドを入力することとは異なります。ウィンドウ サイズを 0 に設定すると、厳密なフレーム順序でリプレイ保護が使用されます。**no replay-protection** を入力すると、MACsec 再送保護が無効になります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mka policy**	入力を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、MKA ポリシー relay-policy を設定する例を示します。

```
Switch(config)# mka policy replay-policy
Switch(config-mka-policy)# replay-protection window-size 300
Switch(config-mka-policy)# end
```

インターフェイスでの MACsec の設定

音声用に 1 つの MACsec セッションとデータ用に 1 つの MACsec セッションが存在するインターフェイスで MACsec を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**interface** *interface-id*	MACsec 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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 3	**switchport access vlan** *vlan-id*	このポートのアクセス VLAN を設定します。
ステップ 4	**switchport mode access**	インターフェイスをアクセス ポートとして設定します。
ステップ 5	**macsec**	インターフェイスで 802.1AE MACsec をイネーブルにします。
ステップ 6	**authentication event linksec fail action authorize vlan** *vlan-id*	（任意）認証の試行に失敗した後で、ポート上の制限付き VLAN を許可することによって、ユーザ証明書が認識されない認証リンク セキュリティの問題をスイッチが処理することを指定します。
ステップ 7	**authentication host-mode multi-domain**	ホストと音声デバイスの両方が、802.1x で許可されたポート上で認証されるように、ポート上の認証マネージャ モードを設定します。設定されていない場合、デフォルトのホスト モードはシングルです。
ステップ 8	**authentication linksec policy must-secure**	LinkSec セキュリティ ポリシーを設定して、ピアを利用できる場合に、MACsec でセッションをセキュアにします。設定されていない場合、デフォルト値は *should secure* です。
ステップ 9	**authentication port-control auto**	ポートでの 802.1x 認証をイネーブルにします。スイッチとクライアント間の認証交換に基づいてポートが許可ステートまたは無許可ステートに変わります。
ステップ 10	**authentication violation protect**	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続された後に新しいデバイスがそのポートに接続された場合に、予期しない着信 MAC アドレスを破棄するようポートを設定します。設定されていない場合、デフォルトではポートをシャット ダウンします。
ステップ 11	**mka policy** *policy name*	既存の MKA プロトコル ポリシーをインターフェイスに適用し、インターフェイス上で MKA をイネーブルにします。（**mka policy** グローバル コンフィギュレーション コマンドを入力して）MKA ポリシーが設定されていない場合、**mka default-policy** インターフェイス コンフィギュレーション コマンドを入力して、MKA のデフォルトのポリシーをインターフェイスに適用する必要があります。
ステップ 12	**dot1x pae authenticator**	ポートを 802.1x Port Access Entity（PAE; ポート アクセス エンティティ）オーセンティケータとして設定します。
ステップ 13	**spanning-tree portfast**	関連するすべての VLAN 内の特定のインターフェイスで、スパニングツリー PortFast をイネーブルにします。PortFast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。
ステップ 14	**end**	特権 EXEC モードに戻ります。
ステップ 15	**show authentication session interface** *interface-id*	許可されたセッションのセキュリティ ステータスを確認します。
ステップ 16	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

これは、インターフェイス上での MACsec の設定と確認の例です。

```
Switch(config)# interface GigabitEthernet0/2
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# macsec
Switch(config-if)# authentication event linksec fail action authorize vlan 2
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication linksec policy must-secure
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication violation protect
Switch(config-if)# mka policy replay-policy
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast
Switch(config-if)# end
Switch# show authentication sessions interface gigabitethernet1/0/2
Interface: GigabitEthernet0/2
MAC Address: 001b.2140.ec3c
IP Address: 1.1.1.103
User-Name: ms1
Status: Authz Success
Domain: DATA
Security Policy: Must Secure ß--- New
Security Status: Secured ß--- New
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 10
Session timeout: 3600s (server), Remaining: 3567s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: 0A05783B0000001700448BA8
Acct Session ID: 0x00000019
Handle: 0x06000017
Runnable methods list:
Method State
dot1x Authc Success
```

Cisco TrustSec MACsec について

（注） スイッチ間セキュリティのための Cisco TrustSec MACsec は、IP ベースまたは IP サービス フィーチャ セットが稼働しているスイッチでだけサポートされます。NPE または LAN Base イメージを実行しているスイッチではサポートされません。

Cisco TrustSec MACsec はスイッチ間の暗号化機能を提供します。Cisco TrustSec NDAC スイッチ間認証に対応しているあるスイッチのポートと別のスイッチのポートとの間に、Cisco TrustSec MACsec を設定できます。

表 11-2 で、スイッチでサポートされる Cisco TrustSec 機能について説明します。詳細については、『*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/arch_over.html#wp1054561

表 11-2　Cisco TrustSec の機能

Cisco TrustSec の機能	説明
802.1AE 暗号化（MACsec）	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。デバイス内では暗号化は行われません。 この機能は、802.1AE 対応デバイス間だけで使用できます。
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使用し、EAP 方式として Extensible Authentication Protocol Flexible Authentication with Secure Tunnel（EAP-FAST）を使用します。NDAC で認証および許可されると、802.1AE 暗号化のためのセキュリティ 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。
セキュリティ アソシエーション プロトコル（SAP）	SAP はスイッチ間のシスコ独自のキー交換プロトコルです。NDAC スイッチ間認証の後、SAP は、その後の TrustSec ピア間のスイッチ間 MACSec 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。プロトコルの記述は機密保持契約の下で利用できます。
セキュリティ グループ タグ（SGT） **（注）** SGT はこのリリースでサポートされていません。	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。
SXPv2 を含む SGT Exchange Protocol（SXP）	SXP を使用すると、TrustSec にハードウェアで対応していないデバイスが、Cisco アクセス コントロール システム（ACS）からの認証済みユーザまたはデバイスの SGT 属性を受信できます。デバイスは、タグ付けおよびセキュリティ グループ ACL（SGACL）の適用のために、TrustSec にハードウェアで対応しているデバイスに、送信元 IP から SGT へのバインディングを転送します。

リンクの両端で 802.1AE MACsec をサポートしている場合、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。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンと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）：認証と暗号化
- GCM 認証（GMAC）：GCM 認証、暗号化なし
- カプセル化なし：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

Cisco TrustSec は、AES-128 GCM および GMAC を使用し、802.1AE 規格に準拠しています。GCM は、NPE または LAN Base イメージを実行しているスイッチではサポートされません。

Cisco TrustSec SAP NDAC は、ネットワーク デバイスからネットワーク デバイスへのリンク、つまりスイッチ間リンクのみで使用することを意図しているため、トランク ポートでサポートされます。次のものではサポートされません。

- ホスト側のアクセス ポート（これらのポートは、MKA MACsec をサポートします）
- スイッチ仮想インターフェイス（SVI）

- SPAN 宛先ポート

スイッチは、セキュリティ グループ ACL もサポートしません。

Cisco TrustSec ネットワークを作成するために Cisco TrustSec クレデンシャルを設定する必要があります。

802.1x モードまたは手動モードで Cisco TrustSec リンク層セキュリティを設定できます。

Cisco TrustSec MACsec の設定

- 「スイッチの Cisco TrustSec クレデンシャルの設定」（P.11-10）
- 「802.1X モードでの Cisco TrustSec スイッチ間のリンク セキュリティの設定」（P.11-11）
- 「手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定」（P.11-14）
- 「Cisco TrustSec スイッチ間リンク セキュリティの設定例」（P.11-17）

（注）　最後の項のサンプル設定は、AAA および RADIUS の設定を示します。スイッチ間のセキュリティを設定する前に、RADIUS および AAA の設定にこの例を使用します。

スイッチの Cisco TrustSec クレデンシャルの設定

Cisco TrustSec 機能をイネーブルにするには、他の TrustSec 設定で使用するスイッチで Cisco TrustSec クレデンシャルを作成する必要があります。Cisco TrustSec クレデンシャルを設定するには、特権 EXEC モードで次の手順を行います。

	コマンド	目的
ステップ 1	**cts credentials id** *device-id* **password** *cts-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 クレデンシャルを指定します。 • **id** *device-id* : スイッチの Cisco TrustSec デバイス ID 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。 • **password** *cts-password* : デバイスの Cisco TrustSec パスワードを指定します。
ステップ 2	**show cts credentials**	（任意）スイッチで設定された Cisco TrustSec クレデンシャルを表示します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Cisco TrustSec クレデンシャルを削除するには、**clear cts credentials** 特権 EXEC コマンドを入力します。

次に、Cisco TrustSec クレデンシャルを作成する例を示します。

```
Switch# cts credentials id trustsec password mypassword
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.

Switch# show cts credentials
```

```
CTS password is defined in keystore, device-id = trustsecchange-password  Initiate
password change with AAA server
```

（注）　Cisco TrustSec MACsec 認証を設定する前に、Cisco TrustSec シードおよび非シード デバイスを設定する必要があります。802.1x モードでは、アクセス コントロール システム（ACS）に最も近い少なくとも 1 台のシード デバイスを設定する必要があります。『*Cisco TrustSec Configuration Guide*』のこの項を参照してください。
http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html

802.1X モードでの Cisco TrustSec スイッチ間のリンク セキュリティの設定

別の Cisco TrustSec デバイスに接続されているインターフェイス上で Cisco TrustSec リンク層スイッチ間セキュリティをイネーブルにします。インターフェイス上で 802.1X モードの Cisco TrustSec を設定する場合は、次の注意事項に従ってください。

- 802.1x モードを使用するには、各デバイスでグローバルに 802.1x をイネーブルにする必要があります。
- SAP 動作モードとして GCM を選択すると、シスコの MACsec 暗号化ソフトウェア ライセンスが必要です。MACsec は Catalyst 356o-C ユニバーサル IP ベースおよび IP サービスのライセンスでサポートされます。これは NPE ライセンスまたは LAN ベース サービス イメージではサポートされません。

  必要なライセンスなしで GCM を選択した場合、インターフェイスはリンク ダウン状態になります。

特権 EXEC モードから 802.1x で Cisco TrustSec のスイッチ間のリンク層セキュリティを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	**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	**interface** *interface-id*	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。 （注）　インターフェイスは、ネットワーク サービス モジュールのアップリンク インターフェイスである必要があります。
ステップ 3	**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。

	コマンド	目的
ステップ 4	**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。優先する順序で許容されるモードを入力します。 *mode* の選択肢は次のとおりです。 • **gcm-encrypt**：認証と暗号化 **（注）** ソフトウェア ライセンスが MACsec 暗号化をサポートする場合、MACsec の認証と暗号化にこのモードを選択します。 • **gmac**：認証、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化、認証または暗号化なし **（注）** インターフェイスでデータ 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。SGT はサポートされません。

（注） CLI ヘルプには表示されますが、**timer reauthentication** および **propagate sgt** キーワードはサポートされません。

ステップ 5	**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 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show cts interface** [*interface-id* | **brief** | **summary**]	（任意）TrustSec 関連のインターフェイス特性を表示して、設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、優先 SAP モードとして GCM を使用して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例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet/2
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# end
```

次の例では、**show cts interface summary** コマンドの出力を示します。

```
Switch# show cts interface summary
Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache
------------------------------------------------------------
Gi 0/1    DOT1X   INIT      unknown    unknown    invalid
Gi 0/2    DOT1X   OPEN      Authent    b6-3560x-c invalid

CTS Layer3 Interfaces
---------------------
Interface   IPv4 encap       IPv6 encap       IPv4 policy      IPv6 policy
-------------------------------------------------------------------------
```

次に、指定したインターフェイスの **show cts interface** コマンドの出力例を示します。

```
Switch# show cts interface gigabitethernet 0/2
Global Dot1x feature is Enabled
Interface GigabitEthernet0/2:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "b6-3560x-cts-nsd"
        Peer's advertised capabilities: "sap"
        802.1X role:         Authenticator
        Reauth period configured:       86400 (default)
        Reauth period per policy:       600 (server configured)
        Reauth period applied to link:  600 (server configured)
        Reauth starts in approx. 0:00:09:44 (dd:hr:mm:sec)
    Authorization Status:    SUCCEEDED
        Peer SGT:            3
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt
            gmac

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

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

    Statistics:
        authc success:              2
        authc reject:               5
        authc failure:              0
        authc no response:          0
        authc logoff:               1
        sap success:                2
        sap fail:                   0
        authz success:              2
        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
```

手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定

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、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を手動で設定する必要があります。

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。
- SAP 動作モードとして GCM を選択すると、シスコの MACsec 暗号化ソフトウェア ライセンスが必要です。必要なライセンスなしで GCM を選択した場合、インターフェイスはリンク ダウン状態になります。
- これらの保護レベルは、SAP の Pairwise Master Key（**sap pmk**）を設定する場合にサポートされます。
  - SAP が設定されていない：保護は行われません。
  - **sap mode-list gcm-encrypt gmac no-encap**：保護が望ましいものの必須ではありません。
  - **sap mode-list gcm-encrypt gmac**：機密保持が望ましく整合性が必要です。保護はサプリカントの設定に応じてサプリカントによって選択されます。
  - **sap mode-list gmac**：整合性のみ。
  - **sap mode-list gcm-encrypt**：機密保持が必要です。
  - **sap mode-list gmac gcm-encrypt**：整合性が必要かつ推奨され、機密保持は任意です。

特権 EXEC モードから、別の Cisco TrustSec デバイスへのアップリンク インターフェイスで Cisco TrustSec を手動で設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**interface** *interface-id*	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。 **（注）** インターフェイスは、ネットワーク サービス モジュールのアップリンク インターフェイスである必要があります。
ステップ 3	**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。

	コマンド	目的
ステップ 4	**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 動作モードのオプションは次のとおりです。 • **gcm-encrypt**：認証と暗号化 （注）　ソフトウェア ライセンスが MACsec 暗号化をサポートする場合、MACsec の認証と暗号化にこのモードを選択します。 • **gmac**：認証、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化、認証または暗号化なし （注）　インターフェイスでデータ 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。SGT はサポートされません。
ステップ 5	**no propagate sgt**	ピアが SGT を処理できない場合、このコマンドの **no** 形式を使用します。**no propagate sgt** コマンドは、インターフェイスが SGT をピアに送信することを防ぎ、手動モードでは必要です。
ステップ 6	**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 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show cts interface** [*interface-id* | **brief** | **summary**]	（任意）TrustSec 関連のインターフェイス特性を表示して、設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

次の例では、**show cts interface summary** コマンドの出力を示します。

```
Switch# show cts interface summary

Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache
-------------------------------------------------------------
Gi0/1    DOT1X   INIT      unknown    unknown    invalid
Gi-/2    MANUAL  OPEN      unknown    unknown    invalid

CTS Layer3 Interfaces
---------------------
Interface   IPv4 encap       IPv6 encap       IPv4 policy      IPv6 policy
```

```
-----------------------------------------------------------------------
```

次に、指定したインターフェイスの **show cts interface** コマンドの出力例を示します。

```
Switch# show cts interface gigabitethernet 0/2
Global Dot1x feature is Enabled
Interface GigabitEthernet1/1/2:
    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:             2
        Configured pairwise ciphers:
            gcm-encrypt
            gmac

        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:              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
```

Cisco TrustSec スイッチ間リンク セキュリティの設定例

次に、Cisco TrustSec スイッチ間のセキュリティのためにシードおよび非シード デバイスに必要な設定を示します。リンク セキュリティ用に AAA および RADIUS を設定する必要があります。この例では、*ACS-1* から *ACS-3* は任意のサーバ名、*cts-radius* は Cisco TrustSec サーバです。

シード デバイスの設定

```
Switch(config)# aaa new-model
Switch(config)# radius server ACS-1 address ipv4 10.5.120.12 auth-port 1812 acct-port 1813
pac key cisco123
Switch(config)# radius server ACS-2 address ipv4 10.5.120.14 auth-port 1812 acct-port 1813
pac key cisco123
Switch(config)# radius server ACS-3 address ipv4 10.5.120.15 auth-port 1812 acct-port 1813
pac key cisco123
Switch(config)# aaa group server radius cts-radius
Switch(config-sg-radius)# server name ACS-1
Switch(config-sg-radius)# server name ACS-2
Switch(config-sg-radius)# server name ACS-3
Switch(config-sg-radius)# exit
Switch(config)# aaa authentication login default none
Switch(config)# aaa authentication dot1x default group cts-radius
Switch(config)# aaa authentication network cts-radius group radius
Switch(config)# aaa session-id common
Switch(config)# cts authorization list cts-radius
Switch(config)# dot1x system-auth-control

Switch(config)# interface gim 0/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)#exit
Switch(config-if)# exit

Switch(config)# interface gi0/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts manual
Switch(config-if-cts-dot1x)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)# no propagate sgt
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# end
Switch# cts credentials id cts-36 password trustsec123
```

非シード デバイス

```
Switch(config)# aaa new-model
Switch(config)# aaa session-id common
Switch(config)# dot1x system-auth-control

Switch(config)# interface gi0/2
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit
```

```
Switch(config)# interface gi0/4
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)#  switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts manual
Switch(config-if-cts-dot1x)#  sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)# no propagate sgt
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# end
Switch# cts credentials id cts-72 password trustsec123
```