



MACsec の暗号化

- [MACsec 暗号化の前提条件](#) (1 ページ)
- [MACsec 暗号化の制約事項](#) (2 ページ)
- [MACsec 暗号化について](#) (3 ページ)
- [MACsec 暗号化の設定方法](#) (10 ページ)
- [MACsec 暗号化の設定例](#) (33 ページ)
- [MACsec 暗号化に関する追加情報](#) (51 ページ)
- [MACsec 暗号化の機能履歴](#) (52 ページ)

MACsec 暗号化の前提条件

MACsec 暗号化の前提条件

- シスコ以外および IOS XE 以外のデバイスとの相互運用性を可能にするために、デバイスで MACsec 暗号化を設定するときに **ssci-based-on-sci** コマンドを有効にします。
- 802.1x 認証と AAA がデバイスに設定されていることを確認します。

証明書ベース MACsec の前提条件

- 認証局 (CA) サーバがネットワークに設定されていることを確認します。
- CA 証明書を生成します。
- Cisco Identity Services Engine (ISE) リリース 2.0 が設定されていることを確認します。
- 両方の参加デバイス (CA サーバと Cisco Identity Services Engine (ISE)) が Network Time Protocol (NTP) を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。

MACsec 暗号化の制約事項

- MACsec Key Agreement (MKA) はハイアベイラビリティではサポートされません。
- MKA を使用した MACsec は、ポイントツーポイントリンクでのみサポートされます。
- MACsec 設定は、EtherChannel ポートではサポートされません。代わりに、EtherChannel の個々のメンバポートに MACsec 設定を適用できます。MACsec 設定を削除するには、最初に EtherChannel からメンバポートをバンドル解除してから、個々のメンバポートから削除する必要があります。
- スイッチで Cisco StackWise Virtual を有効にした場合、ラインカードポートではスイッチ間 MACsec のみがサポートされます。MACsec はスーパーバイザポートでは設定できません。
- MACsec は、C9400-SUP-1XL-Y スーパーバイザモジュールではサポートされません。C9400-SUP-1 および C9400-SUP-1XL スーパーバイザモジュールでのみサポートされます。
- 遅延保護および機密性のオフセットが 50 の場合、スーパーバイザポートではサポートされません。
- MACsec 暗号アナウンスメントは、MACsec XPN 暗号およびスイッチ間 MACsec 接続ではサポートされません。
- 証明書ベースの MACsec は、アクセスセッションがクローズドとして、またはマルチホストモードで設定されている場合にのみサポートされます。他のコンフィギュレーションモードはサポートされません。
- パケット番号枯渇キ再生成はサポートされません。
- MACsec XPN 暗号スイートは、スーパーバイザポートおよびスイッチとホスト間の MACsec 接続ではサポートされません。
- GCM-AES-256 暗号スイートは、Network Advantage ライセンスでのみサポートされます。
- MACsec のスイッチとホスト間の接続は、スーパーバイザポートではサポートされません。
- MACsec は、スーパーバイザモジュールの 1 ギガビットイーサネットポートではサポートされません。
- **dot1q tag vlan native** コマンドがグローバルレベルで設定されている場合、トランクポートでの dot1x 再認証は失敗します。
- MACsec XPN 暗号スイートは、機密性オフセットを含む機密性保護を提供しません。
- Precision Time Protocol (PTP) を備えた MACsec はサポートされません。
- MACsec は、Locator ID Separation Protocol (LISP) インターフェイスおよび Cisco Software-Defined Access (SD-Access) ソリューションではサポートされません。

- Cisco Secure StackWise Virtual はサポートされません。

MACsec 暗号化について

MACsec 暗号化の推奨事項

ここでは、MACsec 暗号化の設定に関する推奨事項を示します。

- スイッチとホスト間の接続では、機密性（暗号化）オフセットを 0 として使用します。
- 双方向フォワーディングおよび検出（BFD）タイマー値は、10 Gbps ポートでは 750 ミリ秒、10 Gbps を超える速度のポートでは 1.25 秒として使用します。
- アクティブセッションの MKA ポリシーまたは MACsec 設定を変更した後、ポートで **shutdown** コマンドを実行し、**no shutdown** コマンドを実行して、変更がアクティブセッションに適用されるようにします。
- 40Gbps 以上のポート速度には、Extended Packet Numbering（XPN）暗号スイートを使用します。
- 10Gbps を超えるポート速度には、Cisco TrustSec Security Association Protocol（SAP）MACsec 暗号化を使用しないでください。
- 接続アソシエーションキー（CAK）キー再生成オーバーラップタイマーを 30 秒以上に設定します。

MACsec 暗号化の概要

MACsec は、MACsec 対応可能な 2 台のデバイス間でのパケットの認証と暗号化の IEEE 802.1AE 標準規格です。Cisco Catalyst 9400 シリーズスイッチは、スイッチとホストデバイス間の暗号化について、ラインカードポートでの MACsec Key Agreement（MKA）を使用した 802.1AE 暗号化をサポートしています。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）、Security Association Protocol（SAP）および MKA ベースのキー交換プロトコルを使用して、スイッチ間（ネットワーク間デバイス）セキュリティの MACsec 暗号化をサポートします。



- (注) スイッチ間 MACsec が有効な場合、EAP-over-LAN（EAPOL）パケットを除くすべてのトラフィックが暗号化されます。

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）。リンク層セキュリティは、SAP ベースの MACsec でサポートされます。

表 1: スイッチ ポートの MACsec サポート

接続	MACsec のサポート
スイッチからホストへ	MACsec MKA の暗号化
スイッチからスイッチへ	MACsec MKA の暗号化 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 フォン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、ラインカードポートから発信されるスイッチ対ホスト側リンクおよびスイッチ対スイッチ側リンクでサポートされます。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 ベースの MACsec 暗号化を使用できます。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 Key Agreement

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、証明書ベース MACsec 暗号化または事前共有キー (PSK) 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。

MACsec を使用するスイッチでは、MKA ピア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、整合性チェック値 (ICV) で保護されます。スイッチは MKA ピア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 MKA ピア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 の基本的な要件は 802.1x-REV で定義されています。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マスターセッションキー (MSK) を生成します。EAP セッション ID を入力すると、セキュアな接続アソシエーション キー名 (CKN) が生成されます。

これによってランダムなセキュアアソシエーション キー (SAK) が生成され、クライアントパートナーに送信されます。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、MKA ピアが接続を解除した場合、スイッチ上の参加者は MKA ピアから最後の MKPDU を受信した後、6 秒間経過するまで MKA の動作を継続します。



(注) MKPDU の整合性チェック値 (ICV) インジケータはオプションです。トラフィックが暗号化されている場合、ICV はオプションではありません。

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 ASCII 文字未満のポリシー名。
- 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。

ポリシーマップアクションの定義

ここでは、ポリシーマップアクションとその定義について説明します。

- **Activate** : サービステンプレートをセッションに適用します。
- **Authenticate** : セッションの認証を開始します。
- **Authorize** : セッションを明示的に許可します。
- **Set-domain** : クライアントのドメインを明示的に設定します。
- **Terminate** : 実行中のメソッドを終了し、セッションに関連付けられているすべてのメソッドの詳細を削除します。
- **Deactivate** : セッションに適用されたサービステンプレートを削除します。適用されない場合、アクションは実行されません。
- **Set-timer** : タイマーを開始し、セッションに関連付けます。タイマーが期限切れになると、開始する必要があるアクションを処理できます。
- **Authentication-restart** : 認証を再開します。
- **Clear-session** : セッションを削除します。
- **Pause** : 認証を一時停止します。

残りのアクションについては説明の必要はなく、認証に関連したものです。

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。スイッチ間では、物理ポートごとに1つの仮想ポートのみを指定できます。スイッチとホスト間では、物理ポートごとに最大2つの仮想ポートを指定でき、一方の仮想ポートはデータ VLANの一部にできます。もう一方は音声 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 サブ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の使用は推奨しません。

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、一意のセキュア チャネル ID (SCI) を受け取ります。

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。詳細については、[例：MKA 情報の表示（45 ページ）](#) を参照してください。

キー ライフタイムおよびヒットレス キー ロールオーバー

MACsec キー チェーンには、キー ID とオプションのライフタイムが設定された複数の事前共有キー (PSK) を含めることができます。キーのライフタイムには、キーが期限切れになる時刻が指定されます。ライフタイム設定が存在しない場合は、無期限のデフォルトライフタイムが使用されます。ライフタイムが設定されている場合、ライフタイムの期限が切れた後に、MKA はキー チェーン内の次に設定された事前共有キーにロールオーバーします。キーのタイムゾーンは、ローカルまたは UTC を指定できます。デフォルトのタイムゾーンは UTC です。

キー チェーン内に2番目のキーを設定し、最初のキーのライフタイムを設定することで、同じキーチェーン内の次のキーにロールオーバーできます。最初のキーのライフタイムが期限切れになると、リスト内の次のキーに自動的にロールオーバーします。同一のキーがリンクの両側で同時に設定されている場合、キーのロールオーバーはヒットレスになります。つまり、キーはトラフィックを中断せずにロールオーバーされます。



(注) キーのライフタイムは、ヒットレス キー ロールオーバーを実現するためにオーバーラップする必要があります。

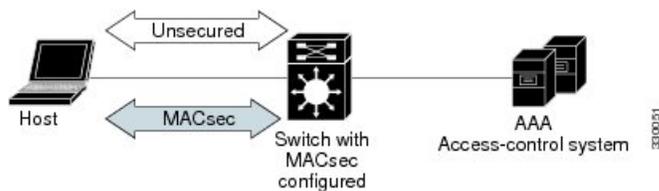
MACsec、MKA、および 802.1x ホストモード

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

次の図に、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。

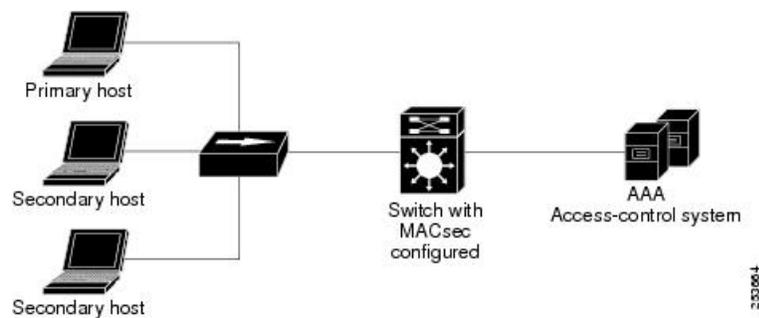
図 1: セキュアなデータセッションでのシングルホストモードの MACsec



マルチホストモード

標準の (802.1x REV ではない) 802.1x 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。1 人のユーザ (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) が認証される場合は、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 サブリカントの場合、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。次の図に、標準のマルチホスト非セキュアモードにおける MACsec を示します。

図 2: マルチホストモードの MACsec : 非セキュア



(注) マルチホストモードは推奨されていません。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、安全性が低いからです。

標準の (802.1x REV ではない) 802.1x マルチドメインモードでは、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。プライマリユーザ (データドメインの PC) が認証さ

れると、同じレベルのネットワークアクセスが同じポートに接続されているドメインに提供されます。セカンダリユーザが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ユーザ（音声ドメインのIPフォン）は、マルチドメインモードであるため、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。

マルチドメインモード

標準の（802.1x REV ではない）802.1x マルチドメインモードでは、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。プライマリユーザ（データドメインのPC）が認証されると、同じレベルのネットワークアクセスが同じポートに接続されているドメインに提供されます。セカンダリユーザが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ユーザ（音声ドメインのIPフォン）は、マルチドメインモードであるため、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。

証明書ベースの MACsec を使用した MACsec MKA

証明書ベースの MACsec 暗号化を使用すると、ラインカードポートからスイッチ間リンクに MACsec MKA を設定できます。証明書ベースの MACsec 暗号化は相互認証を許可し、MSK（マスターセッションキー）を取得します。そのキーから、MKA 操作用の接続アソシエーションキー（CAK）が取得されます。デバイスの証明書は、AAA サーバへの認証用に、証明書ベースの MACsec 暗号化を使用して伝送されます。

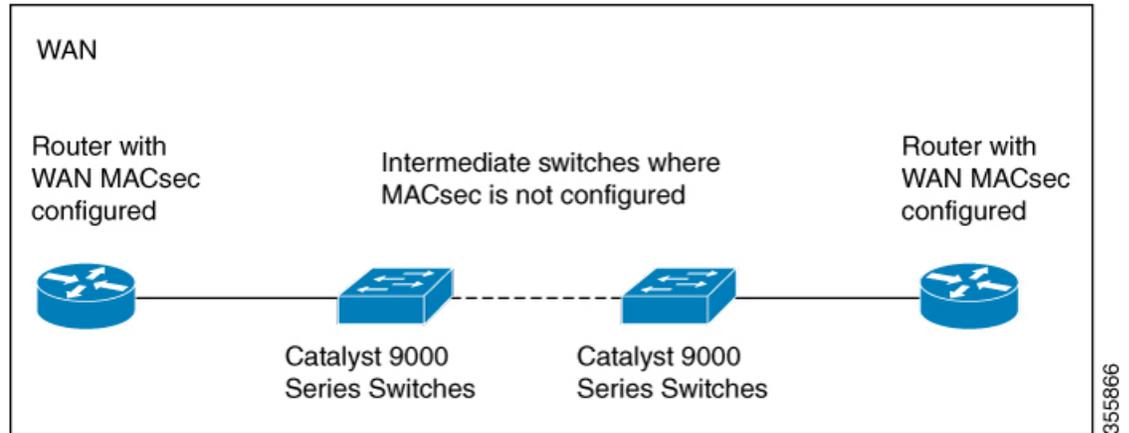
証明書ベースの MACsec を使用した MACsec MKA の前提条件

- 認証局（CA）サーバがネットワークに設定されていることを確認します。
- CA 証明書を生成します。
- Cisco Identity Services Engine（ISE）リリース 2.0 が設定されていることを確認します。
- 両方の参加デバイス（CA サーバと Cisco Identity Services Engine（ISE））が Network Time Protocol（NTP）を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。
- 802.1x 認証と AAA がデバイスに設定されていることを確認します。

中間スイッチの MACsec 接続

Cisco IOS XE Gibraltar 16.10.1 より前は、中間スイッチが Cisco Catalyst 9000 シリーズスイッチの WAN MACsec 導入環境でのエンドデバイス間 MACsec 接続はサポートされませんでした。MACsec が中間スイッチに設定されていない状態でエンドデバイスに WAN MACsec を設定すると、暗号化されたパケットはドロップされました。ASIC に ClearTag 機能が実装されている場合、スイッチは MACsec ヘッダーを解析せずに暗号化されたパケットを転送します。以下のトポロジは、暗号化されたパケットが L2 スイッチングの中間スイッチを介してどのように転送されるかを示しています。

図 3: ClearTag MACsec のトポロジ: MACsec が中間スイッチで設定されていない



中間スイッチの MACsec 接続に関する制約事項

- Catalyst 9000 シリーズスイッチを WAN MACsec がルータに設定されている中間スイッチとして使用するホップバイホップ MACsec 暗号化はサポートされていません。
- 中間スイッチが Catalyst 9000 シリーズスイッチのルータに設定された WAN MACsec は、レイヤ 3 VPN ではサポートされません。
- 中間スイッチが Catalyst 9000 シリーズスイッチのルータに設定された WAN MACsec では、should-secure モードのみで Cisco Discovery Protocol ネイバーが表示されます。

ポートチャネルの MKA/MACsec

MKA/MACsec は、ポートチャネルのポートメンバで設定できます。ポートチャネルのポートメンバ間で MKA セッションが確立されるため、MKA/MACsec はポートチャネルに依存しません。



- (注) ポートチャネルの一部として形成される EtherChannel リンクは、合同または異種のいずれかです。つまり、リンクは MACsec セキュアまたは非 MACsec セキュアのいずれかになります。ポートチャネルの一方のポートメンバが MACsec に設定されていない場合でも、ポートメンバ間の MKA セッションが確立されます。

ポートチャネルのセキュリティを強化するために、すべてのメンバポートで MKA/MACsec を有効にすることをお勧めします。

MACsec 暗号アナウンスメント

暗号アナウンスメントを使用すると、サブリカント (AnyConnect) とオーセンティケータ (スイッチ) は、それぞれの MACsec 暗号スイート機能を相互にアナウンスできます。サポートさ

れる暗号スイートは、GCM-AES-128およびGCM-AES-256です。サブリカントとオーセンティケータの両方が、サポートされる最大の共通 MACsec 暗号スイートを計算し、MKA セッションのキー情報と同じものを使用します。Cisco AnyConnect セキュア モビリティ クライアントのリリース 4.6.02074 以降では、暗号アナウンスメントがサポートされています。



(注) MKA ポリシーで設定されている MACsec 暗号スイート機能だけが、オーセンティケータ（スイッチ）からサブリカント（AnyConnect）にアナウンスされます。

サブリカント側では、AnyConnect ネットワーク アクセス マネージャの [Profile Editor] セクションで、暗号スイート（GCM-AES-128、GCM-AES-256、または両方）を選択できます。[Key Management] タブのドロップダウンリストから [MKA] を選択した場合にのみ、暗号スイートを選択できます。

EAPoL アナウンスメントには 2 つのタイプがあります。

- 非セキュアアナウンスメント（EAPoL PDU）：非セキュアアナウンスメントは、MACsec 暗号スイート機能を非セキュアな方法で伝送する EAPoL アナウンスメントです。これらのアナウンスメントは、認証の前に MKA セッションに使用するキーの幅を決定するために使用されます。
- セキュアアナウンスメント（MKPDU）：セキュアアナウンスメントは、以前は非セキュアアナウンスメントで共有されていた MACsec 暗号スイート機能を再検証します。

セッションが認証されると、EAPoL アナウンスメントを介して受信されたピア機能がセキュアアナウンスメントで再検証されます。機能に不一致がある場合、MKA セッションは切断されます。

MACsec 暗号アナウンスメントに関する制約事項

- MACsec 暗号アナウンスメントは、スイッチからホストへのリンクでのみサポートされません。
- サブリカントとオーセンティケータ間の MKA セッションは、両方に設定された MACsec 暗号スイート機能が共通の暗号スイートにならない場合でも切断されません。

MACsec 暗号化の設定方法

MKA および MACsec の設定

デフォルトでは、MACsec は無効です。MKA ポリシーは設定されていません。

MKA ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	mka policy policy-name 例： Device(config)# mka policy mka_policy	MKA ポリシーを指定して、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。 (注) MKA ポリシー内のデフォルトの MACsec 暗号スイートは常に「GCM-AES-128」です。デバイスが「GCM-AES-128」および「GCM-AES-256」の両方の暗号方式をサポートしている場合は、ユーザ定義の MKA ポリシーを定義して使用し、必要に応じて、128 および 256 ビット両方の暗号を含めるか、または 256 ビットのみを含めることを強くお勧めします。
ステップ 4	key-server priority 例： Device(config-mka-policy)# key-server priority 200	MKA キーサーバオプションを設定し、優先順位を設定します（0 ～ 255 の値）。 (注) キーサーバプライオリティの値を 255 に設定した場合、ピアはキーサーバになることはできません。キーサーバの優先順位の値は MKA PSK に対してのみ有効です。MKA EAPTLS に対しては有効ではありません。

	コマンドまたはアクション	目的
ステップ 5	include-icv-indicator 例： Device(config-mka-policy)# include-icv-indicator	MKPDU の ICV インジケータを有効にします。ICV インジケータを無効にするには、このコマンドの no 形式を使用します。
ステップ 6	macsec-cipher-suite { <i>gcm-aes-128</i> <i>gcm-aes-256</i> } 例： Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128	128 ビットまたは 256 ビット暗号化により SAK を取得するための暗号スイートを設定します。
ステップ 7	confidentiality-offset <i>offset-value</i> 例： Device(config-mka-policy)# confidentiality-offset 0	各物理インターフェイスに機密性（暗号化）オフセットを設定します。 (注) オフセット値は、0、30、または 50 を指定できます。クライアントで Anyconnect を使用している場合は、オフセット 0 を使用することをお勧めします。
ステップ 8	ssci-based-on-sci 例： Device(config-mka-policy)# ssci-based-on-sci	(任意) Secure Channel Identifier (SCI) 値に基づいて Short Secure Channel Identifier (SSCI) 値を計算します。SCI 値が高いほど、SSCI 値は低くなります。
ステップ 9	end 例： Device(config-mka-policy)# end	MKA ポリシー コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 10	show mka policy 例： Device# show mka policy	MKA ポリシー設定情報を表示します。

スイッチからホストへの MACsec の暗号化設定

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、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface GigabitEthernet 1/0/1	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 4	switchport access vlan vlan-id 例： Device(config-if)# switchport access vlan 1	このポートのアクセス VLAN を設定します。
ステップ 5	switchport mode access 例： Device(config-if)# 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 6	macsec 例： Device(config-if)# macsec	インターフェイス上で 802.1ae MACsec をイネーブルにします。 macsec コマンドを使用すると、スイッチからホストへのリンクでのみ MKA MACsec が有効になります。
ステップ 7	access-session host-mode multi-host 例： Device(config-if)# access-session host-mode multi-host	ホストにインターフェイスへのアクセスを許可します。
ステップ 8	access-session closed 例： Device(config-if)# access-session closed	インターフェイスへの事前認証アクセスを防止します。
ステップ 9	access-session port-control auto 例：	ポートの認可状態を設定します。

	コマンドまたはアクション	目的
	Device(config-if) # access-session port-control auto	
ステップ 10	authentication periodic 例： Device(config-if) # authentication periodic	(任意) このポートの再認証を有効または無効にします。
ステップ 11	authentication timer reauthenticate 例： Device(config-if) # authentication timer reauthenticate	(任意) 1 から 65535 までの値 (秒) を入力します。サーバから再認証タイムアウト値を取得します。デフォルトの再認証時間は 3600 秒です。
ステップ 12	authentication violation protect 例： Device(config-if) # 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 13	mka policy policy name 例： Device(config-if) # mka policy mka_policy	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 を有効にします。MKA ポリシーを設定しなかった場合 (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)。
ステップ 14	dot1x pae authenticator 例： Device(config-if) # dot1x pae authenticator	ポートを 802.1x ポートアクセスエンティティ (PAE) オーセンティケータとして設定します。
ステップ 15	spanning-tree portfast 例： Device(config-if) # spanning-tree portfast	関連するすべての VLAN 内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。Port Fast 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状態からフォワーディング状態に直接移行します。その際に、中間のスパニングツリー状態は変わりません。
ステップ 16	end 例： Device(config) # end	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、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 17	show authentication session interface <i>interface-id</i> 例： Device# show authentication session interface GigabitEthernet 1/0/1	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 18	show macsec interface <i>interface-id</i> 例： Device# show macsec interface GigabitEthernet 1/0/1	インターフェイスの MACsec ステータスを確認します。
ステップ 19	show mka sessions 例： Device# show mka sessions	確立された mka セッションを確認します。

PSK を使用した MKA MACsec の設定

PSK を使用した MACsec MKA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	key chain <i>key-chain-name</i> macsec 例： Device(config)# key chain keychain1 macsec	キーチェーンを設定して、キーチェーン 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	key <i>hex-string</i> 例： Device(config-key-chain)# key 1000	キーチェーン内の各キーの固有識別子を設定し、キーチェーンのキー コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
		(注) 128 ビット暗号化の場合は、1～32 文字の 16 進数キー文字列を使用します。256 ビット暗号化の場合は、64 文字の 16 進数キー文字列を使用します。
ステップ 5	cryptographic-algorithm { <i>gcm-aes-128</i> / <i>gcm-aes-256</i> } 例： Device(config-key-chain)# cryptographic-algorithm gcm-aes-128	128 ビットまたは 256 ビット暗号による暗号化認証アルゴリズムを設定します。
ステップ 6	key-string { [0/6/7] <i>pwd-string</i> / <i>pwd-string</i> } 例： Device(config-key-chain)# key-string 12345678901234567890123456789012	キー文字列のパスワードを設定します。16 進数の文字のみを入力する必要があります。
ステップ 7	lifetime local [<i>start timestamp</i> { <i>hh::mm::ss</i> / <i>day</i> / <i>month</i> / <i>year</i> }] [duration seconds <i>end timestamp</i> { <i>hh::mm::ss</i> / <i>day</i> / <i>month</i> / <i>year</i> }] 例： Device(config-key-chain)# lifetime local 12:12:00 July 28 2016 12:19:00 July 28 2016	事前共有キーの有効期間を設定します。
ステップ 8	end 例： Device(config-key-chain)# end	キーチェーン コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

PSK を使用した、インターフェイスでの MACsec MKA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface <i>interface-id</i> 例： Device(config-if) # interface GigabitEthernet 0/0/0	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 4	macsec network-link 例： Device(config-if) # macsec network-link	インターフェイス上で MACsec をイネーブルにします。
ステップ 5	mka policy <i>policy-name</i> 例： Device(config-if) # mka policy mka_policy	MKA ポリシーを設定します。
ステップ 6	mka pre-shared-key key-chain <i>key-chain name</i> 例： Device(config-if) # mka pre-shared-key key-chain key-chain-name	MKA 事前共有キーのキーチェーン名を設定します。
ステップ 7	macsec replay-protection window-size <i>frame number</i> 例： Device(config-if) # macsec replay-protection window-size 10	リプレイ保護の MACsec ウィンドウサイズを設定します。
ステップ 8	end 例： Device(config-if) # end	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、特権 EXEC モードに戻ります。

証明書ベース MACsec 暗号化を使用した MACsec MKA の設定

ポイントツーポイントリンクで MKA による MACsec を設定するには、次のタスクを実行します。

- 証明書登録の設定
 - キーペアの生成
 - SCEP 登録の設定
 - 証明書の手動設定
- 認証ポリシーの設定
- 証明書ベース MACsec 暗号化プロファイルと IEEE 802.1x ログイン情報の設定

- インターフェイスで証明書ベース MACsec 暗号化を使用する MACsec MKA の設定

キー ペアの生成

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto key generate rsa label label-name general-keys modulus size 例： Device(config)# crypto key generate rsa label general-keys modulus 2048	署名および暗号化用に RSA キー ペアを作成します。 label キーワードを使用すると、各キー ペアにラベルを割り当てることもできます。このラベルは、キー ペアを使用するトラストポイントによって参照されます。ラベルを割り当てなかった場合、キー ペアには <Default-RSA-Key> というラベルが自動的に付けられます。 追加のキーワードを使用しない場合、このコマンドは汎用 RSA キー ペアを 1 つ生成します。係数が指定されていない場合は、デフォルトのキー係数である 1024 が使用されます。その他の係数サイズを指定するには、modulus キーワードを使用します。
ステップ 4	end 例： Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	show authentication session interface interface-id 例： Device# show authentication session interface gigabitethernet 0/1/1	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。

SCEP による登録の設定

Simple Certificate Enrollment Protocol (SCEP) は、HTTP を使用して認証局 (CA) または登録局 (RA) と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信に最も一般的に使用される方式です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	crypto pki trustpoint server name 例： Device(config)# crypto pki trustpoint ka	トラストポイントおよび設定された名前を宣言して、CA トラストポイント 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	enrollment url url name pem 例： Device(ca-trustpoint)# enrollment url http://url:80	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、 http://[2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail (PEM) の境界を追加します。
ステップ 5	rsakeypair label 例： Device(ca-trustpoint)# rsakeypair exampleCAkeys	証明書に関連付けるキーペアを指定します。 (注) rsakeypair 名は、信頼ポイント名と一致している必要があります。
ステップ 6	serial-number none 例： Device(ca-trustpoint)# serial-number none	none キーワードは、証明書要求にシリアル番号が含まれないことを指定します。

	コマンドまたはアクション	目的
ステップ 7	ip-address none 例： Device(ca-trustpoint)# ip-address none	none キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	revocation-check crl 例： Device(ca-trustpoint)# revocation-check crl	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	auto-enroll percent regenerate 例： Device(ca-trustpoint)# auto-enroll 90 regenerate	<p>自動登録をイネーブルにします。これにより、クライアントは CA から自動的にロールオーバー証明書を要求できます。</p> <p>自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。</p> <p>デフォルトでは、デバイスのドメインネームシステム (DNS) 名だけが証明書に含められます。</p> <p>現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。</p> <p>名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。</p> <p>ロールオーバー中のキーペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キーペアがエクスポート可能かどうかを示されます。「! RSA key pair associated with trustpoint is exportable.」</p> <p>新しいキーペアは、セキュリティ上の問題に対処するために生成することを推奨します。</p>
ステップ 10	exit 例：	CA トラストポイントコンフィギュレーションモードを終了し、グローバルコ

	コマンドまたはアクション	目的
	Device (ca-trustpoint) # exit	コンフィギュレーションモードに戻ります。
ステップ 11	crypto pki authenticate name 例： Device (config) # crypto pki authenticate myca	CA 証明書を取得して、認証します。
ステップ 12	end 例： Device (config) # end	グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 13	show crypto pki certificate trustpoint name 例： Device # show crypto pki certificate ka	信頼ポイントの証明書に関する情報を表示します。

登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device > enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	enable 例： Device > enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。
ステップ 4	configure terminal 例： Device # configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 5	crypto pki trustpoint <i>server name</i> 例： Device# crypto pki trustpoint ka	トラストポイントおよび設定された名前を宣言して、CA トラストポイント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	enrollment url <i>url name pem</i> 例： Device(ca-trustpoint)# enrollment url http://url:80	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail (PEM) の境界を追加します。
ステップ 7	rsa keypair <i>label</i> 例： Device(ca-trustpoint)# rsa keypair exampleCAkeys	証明書に関連付けるキーペアを指定します。
ステップ 8	serial-number <i>none</i> 例： Device(ca-trustpoint)# serial-number none	none キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 9	ip-address <i>none</i> 例： Device(ca-trustpoint)# ip-address none	none キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 10	revocation-check <i>crl</i> 例： Device(ca-trustpoint)# revocation-check crl	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 11	exit 例： Device(ca-trustpoint)# exit	CA トラストポイントコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 12	crypto pki authenticate <i>name</i> 例： Device(config)# crypto pki authenticate myca	CA 証明書を取得して、認証します。

	コマンドまたはアクション	目的
ステップ 13	crypto pki enroll name 例 : Device(config)# crypto pki enroll myca	<p>証明書要求を生成し、証明書サーバにコピーおよびペーストするために要求を表示します。</p> <p>プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。</p> <p>コンソール端末に対して証明書要求を表示するかについても選択できます。</p> <p>必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。</p>
ステップ 14	crypto pki import name certificate 例 : Device(config)# crypto pki import myca certificate	<p>許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。</p> <p>デバイスは、拡張子が「.req」から「.cert」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.cert」および「-encr.cert」が使用されます。</p> <p>デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。</p> <p>(注) 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキーペアのいずれも使用しません。</p>

	コマンドまたはアクション	目的
ステップ 15	end 例： Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 16	show crypto pki certificate trustpoint name 例： Device# show crypto pki certificate ka	信頼ポイントの証明書に関する情報を表示します。

インターフェイスでの 802.1x MACsec MKA 設定の適用

証明書ベース MACsec 暗号化を使用して MKA MACsec をインターフェイスに適用するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 0/2/1	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 4	macsec network-link 例： Device(config-if)# macsec network-link	インターフェイス上で MACsec をイネーブルにします。
ステップ 5	authentication periodic 例： Device(config-if)# authentication periodic	(任意) このポートの再認証を有効にします。
ステップ 6	authentication timer reauthenticate interval 例：	(任意) 再認証間隔を設定します。

	コマンドまたはアクション	目的
	<code>Device (config-if) # authentication timer reauthenticate interval</code>	
ステップ 7	access-session host-mode multi-host 例： <code>Device (config-if) # access-session host-mode multi-domain</code>	ホストにインターフェイスへのアクセスを許可します。
ステップ 8	access-session closed 例： <code>Device (config-if) # access-session closed</code>	インターフェイスへの事前認証アクセスを防止します。
ステップ 9	access-session port-control auto 例： <code>Device (config-if) # access-session port-control auto</code>	ポートの認可状態を設定します。
ステップ 10	dot1x pae both 例： <code>Device (config-if) # dot1x pae both</code>	ポートを 802.1X ポート アクセス エンティティ (PAE) のサブリカントおよびオーセンティケータとして設定します。
ステップ 11	dot1x credentials profile 例： <code>Device (config-if) # dot1x credentials profile</code>	802.1x クレデンシアルプロファイルをインターフェイスに割り当てます。
ステップ 12	end 例： <code>Device (config-if) # end</code>	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、特権 EXEC モードに戻ります。
ステップ 13	show macsec interface 例： <code>Device # show macsec interface</code>	インターフェイスの MACsec の詳細を表示します。

PSK を使用したポートチャネルの MKA/MACsec の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config-if)# interface gigabitethernet 1/0/3	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 4	macsec network-link 例： Device(config-if)# macsec network-link	インターフェイス上で MACsec をイネーブルにします。レイヤ 2 およびレイヤ 3 ポートチャネルをサポートします。
ステップ 5	mka policy policy-name 例： Device(config-if)# mka policy mka_policy	MKA ポリシーを設定します。
ステップ 6	mka pre-shared-key key-chain key-chain-name 例： Device(config-if)# mka pre-shared-key key-chain key-chain-name	MKA 事前共有キーのキーチェーン名を設定します。 (注) MKA 事前共有キーは、物理インターフェイスまたはサブインターフェイスで設定できませんが、両方で設定することはできません。
ステップ 7	macsec replay-protection window-size frame number 例： Device(config-if)# macsec replay-protection window-size 0	リプレイ保護の MACsec ウィンドウ サイズを設定します。
ステップ 8	channel-group channel-group-number mode {auto desirable} {active passive} {on} 例：	チャンネルグループ内にポートを設定し、モードを設定します。

	コマンドまたはアクション	目的
	<pre>Device(config-if)# channel-group 3 mode auto active on</pre>	<p>(注) インターフェイスで MACsec を設定しないと、チャンネルグループのポートを設定できません。このステップの前に、ステップ3、4、5、および6のコマンドを設定する必要があります。</p> <p>channel-number の指定できる範囲は 1 ~ 4096 です。ポートチャネルがない場合は、このチャンネルグループに関連付けられたポートチャネルが自動的に作成されます。モードは、以下のキーワードのいずれかを選択します。</p> <ul style="list-style-type: none"> • auto : PAgP デバイスが検出された場合に限り、PAgP を有効にします。ポートをパッシブ ネゴシエーションステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケットネゴシエーションを開始することはありません。 <p>(注) EtherChannel メンバが、スイッチスタックにある異なるスイッチのメンバである場合、auto キーワードはサポートされません。</p> <ul style="list-style-type: none"> • desirable : 無条件に PAgP を有効にします。ポートをアクティブ ネゴシエーションステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 <p>(注) EtherChannel メンバが、スイッチスタックにある異なるスイッチのメンバである場合、desirable キーワードはサポートされません。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • on : PAgP または LACP を使用せずにポートが強制的にチャンネル化されます。on モードでは、EtherChannel が存在するのは、on モードのポートグループが、on モードの別のポートグループに接続する場合だけです。 • active : LACP デバイスが検出された場合に限り、LACP を有効にします。ポートをアクティブネゴシエーションステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • passive : ポート上で LACP を有効にして、ポートをパッシブネゴシエーションステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケットネゴシエーションを開始することはありません。
ステップ 9	end 例 : Device(config-if)# cend	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、特権 EXEC モードに戻ります。

レイヤ 2 EtherChannel のポートチャネル論理インターフェイスの設定

レイヤ 2 EtherChannel 用のポートチャネルインターフェイスを作成するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	[no] interface port-channel <i>channel-group-number</i> 例： Device(config)# interface port-channel 1	ポートチャネルインターフェイスを作成します。 (注) ポートチャネルインターフェイスを削除するには、このコマンドの no 形式を使用します。
ステップ 4	switchport 例： Device(config-if)# switchport	レイヤ 3 モードになっているインターフェイスを、レイヤ 2 設定のレイヤ 2 モードに切り替えます。
ステップ 5	switchport mode {access trunk} 例： Device(config-if)# switchport mode access	すべてのポートをスタティックアクセスポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。
ステップ 6	end 例： Device(config-if)# end	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、特権 EXEC モードに戻ります。

レイヤ 3 EtherChannel のポートチャネル論理インターフェイスの設定

レイヤ 3 EtherChannel 用のポートチャネルインターフェイスを作成するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/2	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。

	コマンドまたはアクション	目的
ステップ 4	no switchport 例： Device(config-if)# no switchport	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 5	ip address ip-address subnet-mask 例： Device(config-if)# ip address 10.2.2.3 255.255.255.254	EtherChannel に IP アドレスおよびサブネット マスクを割り当てます。
ステップ 6	end 例： Device(config-if)# end	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、特権 EXEC モードに戻ります。

MACsec 暗号アナウンスメントの設定

セキュアアナウンスメントの MKA ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	mka policy policy-name 例： Device(config)# mka policy mka_policy	MKA ポリシーを指定して、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。

	コマンドまたはアクション	目的
		<p>(注) MKA ポリシー内のデフォルトの MACsec 暗号スイートは常に「GCM-AES-128」です。デバイスが「GCM-AES-128」および「GCM-AES-256」の両方の暗号方式をサポートしている場合は、ユーザ定義の MKA ポリシーを定義して使用し、必要に応じて、128 および 256 ビット両方の暗号を含めるか、または 256 ビットのみ暗号を含めることを強くお勧めします。</p>
ステップ 4	key-server priority 例： Device(config-mka-policy)# key-server priority 200	<p>MKA キーサーバオプションを設定し、優先順位を設定します (0 ~ 255 の値)。</p> <p>(注) キーサーバプライオリティの値を 255 に設定した場合、ピアはキーサーバになることはできません。キーサーバの優先順位の値は MKA PSK に対してのみ有効です。MKA EAPTLS に対しては有効ではありません。</p>
ステップ 5	[no] send-secure-announcements 例： Device(config-mka-policy)# send-secure-announcements	<p>セキュアアナウンスメントの送信を有効にします。セキュアアナウンスメントの送信を無効にするには、このコマンドの no 形式を使用します。デフォルトでは、セキュアアナウンスメントは無効になっています。</p>
ステップ 6	macsec-cipher-suite {gcm-aes-128 gcm-aes-256} 例： Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128	<p>128 ビットまたは 256 ビット暗号化により SAK を取得するための暗号スイートを設定します。</p>
ステップ 7	end 例： Device(config-mka-policy)# end	<p>MKA ポリシーコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
ステップ 8	show mka policy 例： Device# show mka policy	MKA ポリシーを表示します。

セキュアアナウンスメントのグローバル設定（すべての MKA ポリシー）

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	mka defaults policy send-secure-announcements 例： Device(config)# mka defaults policy send-secure-announcements	MKA ポリシーを介した MKPDU でのセキュアアナウンスメントの送信を有効にします。デフォルトでは、セキュアアナウンスメントは無効になっています。
ステップ 4	end 例： Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インターフェイスでの EAPoL アナウンスメントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	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 4	eapol announcement 例： Device(config-if)# eapol announcement	EAPoL アナウンスメントを有効にします。EAPoL アナウンスメントを無効にするには、コマンドの no 形式を使用します。デフォルトでは、EAPoL アナウンスメントは無効になっています。
ステップ 5	end 例： Device(config-if)# configure terminal	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、特権 EXEC モードに戻ります。

MACsec 暗号化の設定例

例：MKA および MACsec の設定

次に、MKA ポリシーを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy mka_policy
Device(config-mka-policy)# key-server priority 200
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Device(config-mka-policy)# confidentiality-offset 30
Device(config-mka-policy)# ssci-based-on-sci
Device(config-mka-policy)#end
```

次は、インターフェイスに MACsec を設定する例です。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# switchport access vlan 1
Device(config-if)# switchport mode access
Device(config-if)# macsec
Device(config-if)#access-session event linksec fail action authorize vlan 1
Device(config-if)# access-session host-mode multi-domain
Device(config-if)# access-session linksec policy must-secure
Device(config-if)# access-session port-control auto
Device(config-if)#authentication periodic
Device(config-if)# authentication timer reauthenticate
Device(config-if)# authentication violation protect
Device(config-if)#mka policy mka_policy
Device(config-if)# dot1x pae authenticator
```

```
Device(config-if)# spanning-tree portfast
Device(config-if)#end
```

例：PSK を使用した MACsec MKA の設定

次に、PSK を使用して、MKA MACsec を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# Key chain keychain1 macsec
Device(config-key-chain)# key 1000
Device(config-keychain-key)# cryptographic-algorithm gcm-aes-128
Device(config-keychain-key)# key-string 12345678901234567890123456789012
Device(config-keychain-key)# lifetime local 12:12:00 July 28 2016 12:19:00 July 28 2016
Device(config-keychain-key)# end
```

次に、PSK を使用して、インターフェイスに MACsec MKA を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# mka policy mka_policy
Device(config-if)# mka pre-shared-key key-chain key-chain-name
Device(config-if)# macsec replay-protection window-size 10
Device(config-if)# end
```

例：証明書ベース MACsec を使用した MACsec MKA の設定

この例では、証明書ベース MACsec を使用した MACsec MKA の設定方法について説明します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# macsec network-link
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate interval
Device(config-if)#access-session host-mode multi-domain
Device(config-if)# access-session closed
Device(config-if)# access-session port-control auto
Device(config-if)# dot1x pae both
Device(config-if)#dot1x credentials profile
Device(config-if)# dot1x supplicant eap profile profile_eap_tls
Device(config-if)#service-policy type control subscriber sub1
Device(config-if)# end
```

例：PSK を使用したポートチャネルの MACsec MKA の設定

Etherchannel モード - Static/On

次に、EtherChannel モードがオンのデバイス 1 およびデバイス 2 の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# key chain KC macsec
```

```

Device(config-key-chain)# key 1000
Device(config-key-chain)# cryptographic-algorithm aes-128-cmac
Device(config-key-chain)# key-string FC8F5B10557C192F03F60198413D7D45
Device(config-key-chain)# exit
Device(config)# mka policy POLICY
Device(config-mka-policy)# key-server priority 0
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Device(config-mka-policy)# confidentiality-offset 0
Device(config-mka-policy)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# channel-group 2 mode on
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# channel-group 2 mode on
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# end

```

レイヤ 2 EtherChannel 設定

デバイス 1

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end

```

デバイス 2

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end

```

次に、**show etherchannel summary** コマンドの出力例を示します。

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

```

```

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
2      Po2 (RU)        -         Te1/0/1 (P)  Te1/0/2 (P)

```

レイヤ 3 EtherChannel 設定

デバイス 1

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# ip address 10.25.25.3 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# end

```

デバイス 2

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# ip address 10.25.25.4 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# end

```

次に、**show etherchannel summary** コマンドの出力例を示します。

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

```

```

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----

```

```
2          Po2 (RU)          -          Te1/0/1 (P)  Te1/0/2 (P)
```

EtherChannel モード - LACP

次に、EtherChannel モードが LACP のデバイス 1 およびデバイス 2 の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# key chain KC macsec
Device(config-key-chain)# key 1000
Device(config-key-chain)# cryptographic-algorithm aes-128-cmac
Device(config-key-chain)# key-string FC8F5B10557C192F03F60198413D7D45
Device(config-key-chain)# exit
Device(config)# mka policy POLICY
Device(config-mka-policy)# key-server priority 0
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Device(config-mka-policy)# confidentiality-offset 0
Device(config-mka-policy)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# channel-group 2 mode active
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# channel-group 2 mode active
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# end
```

レイヤ 2 EtherChannel 設定

デバイス 1

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end
```

デバイス 2

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end
```

次に、**show etherchannel summary** コマンドの出力例を示します。

```
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby  (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
```



```

Group   Port-channel   Protocol   Ports
-----+-----+-----+-----
2       Po2 (RU)        LACP      Te1/1/1 (P) Te1/1/2 (P)

```

EtherChannel モード - PAgP

次に、EtherChannel モードが PAgP のデバイス 1 およびデバイス 2 の設定例を示します。

```

Device> enable
Device# configure terminal
Device(config)# key chain KC macsec
Device(config-key-chain)# key 1000
Device(config-key-chain)# cryptographic-algorithm aes-128-cmac
Device(config-key-chain)# key-string FC8F5B10557C192F03F60198413D7D45
Device(config-key-chain)# exit
Device(config)# mka policy POLICY
Device(config-mka-policy)# key-server priority 0
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Device(config-mka-policy)# confidentiality-offset 0
Device(config-mka-policy)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# channel-group 2 mode desirable
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# channel-group 2 mode desirable
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# end

```

レイヤ 2 EtherChannel 設定

デバイス 1

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end

```

デバイス 2

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end

```

次に、**show etherchannel summary** コマンドの出力例を示します。


```

Key Server..... YES
MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)

MKA Policy Name..... p2
Key Server Priority..... 2
Delay Protection..... NO
Replay Protection..... YES
Replay Window Size..... 0
Confidentiality Offset... 0
Algorithm Agility..... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite..... 0080C20001000001 (GCM-AES-128)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                MN                Rx-SCI (Peer)          KS Priority
-----
  38046BA37D7DA77E06D006A9  89560                c800.8459.e764/002a   10

Potential Peers List:
  MI                MN                Rx-SCI (Peer)          KS Priority
-----

Dormant Peers List:
  MI                MN                Rx-SCI (Peer)          KS Priority
-----

```

次に、セキュアアナウンスメントが無効になっている **show mka policy policy-name detail** コマンドの出力例を示します。

```

Device# show mka policy p2 detail

MKA Policy Configuration ("p2")

```



```

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                               MN           Rx-SCI (Peer)       KS Priority
-----
  38046BA37D7DA77E06D006A9  89560       c800.8459.e764/002a  10

Potential Peers List:
  MI                               MN           Rx-SCI (Peer)       KS Priority
-----

Dormant Peers List:
  MI                               MN           Rx-SCI (Peer)       KS Priority
-----

```

次に、**show mka policy** コマンドの出力例を示します。

```
Device# show mka policy
```

```
MKA Policy Summary...
```

Policy	KS	Delay	Replay	Window	Conf	Cipher
Interfaces						
Name	Priority	Protect	Protect	Size	Offset	Suite(s)
Applied						
DEFAULT POLICY	0	FALSE	TRUE	0	0	GCM-AES-128
p1	1	FALSE	TRUE	0	0	GCM-AES-128
p2	2	FALSE	TRUE	0	0	GCM-AES-128
Gi1/0/1						

次に、**show mka policy policy-name** コマンドの出力例を示します。

```
Device# show mka policy p2
```

```
MKA Policy Summary...
```

Policy	KS	Delay	Replay	Window	Conf	Cipher
Interfaces						
Name	Priority	Protect	Protect	Size	Offset	Suite(s)
Applied						

```
p2                2          FALSE  TRUE    0      0      GCM-AES-128
  GigabitEthernet1/0/1
```

次に、**show mka policy *policy-name* detail** コマンドの出力例を示します。

```
Device# show mka policy p2 detail

MKA Policy Configuration ("p2")
=====
MKA Policy Name..... p2
Key Server Priority.... 2
Confidentiality Offset. 0
Send Secure Announcement..DISABLED
Cipher Suite(s)..... GCM-AES-128

Applied Interfaces...
  GigabitEthernet1/0/1
```

次に、**show mka statistics interface *interface-name*** コマンドの出力例を示します。

```
Device# show mka statistics interface GigabitEthernet 1/0/1

MKA Statistics for Session
=====
Reauthentication Attempts.. 0

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

SA Statistics
  SAKs Generated..... 1
  SAKs Rekeyed..... 0
  SAKs Received..... 0
  SAK Responses Received.. 1

MKPDU Statistics
  MKPDUs Validated & Rx... 89585
    "Distributed SAK".. 0
    "Distributed CAK".. 0
  MKPDUs Transmitted..... 89596
    "Distributed SAK".. 1
    "Distributed CAK".. 0
```

次に、**show mka summary** コマンドの出力例を示します。

```
Device# show mka summary

Total MKA Sessions..... 1
  Secured Sessions... 1
  Pending Sessions... 0
```



```

SAK Generation..... 0
Hash Key Generation..... 0
SAK Encryption/Wrap..... 0
SAK Decryption/Unwrap..... 0
SAK Cipher Mismatch..... 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... 0
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

```

MACsec 暗号化に関する追加情報

標準および RFC

標準/RFC	タイトル
IEEE 802.1AE-2006	<i>Media Access Control (MAC) セキュリティ</i>
IEEE 802.1X-2010	ポートベースのネットワーク アクセス コントロール
IEEE 802.1AEbw-2013	<i>Media Access Control (MAC) セキュリティ (IEEE 802.1AE-2006 の修正) : Extended Packet Numbering (XPN)</i>
IEEE 802.1Xbx-2014	ポートベースのネットワーク アクセス コントロール (<i>IEEE 802.1X-2010</i> の修正)

標準/RFC	タイトル
RFC 4493	AES-CMAC アルゴリズム

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	http://www.cisco.com/support

MACsec 暗号化の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.1	MACsec の暗号化	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。
Cisco IOS XE Amsterdam 17.3.x	Cisco StackWise Virtual での MACsec のサポート	Cisco StackWise Virtual がデバイスに設定されている場合に、ラインカードで MKA MACSec および SAP MACSec スイッチ間接続がサポートされるようになりました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。