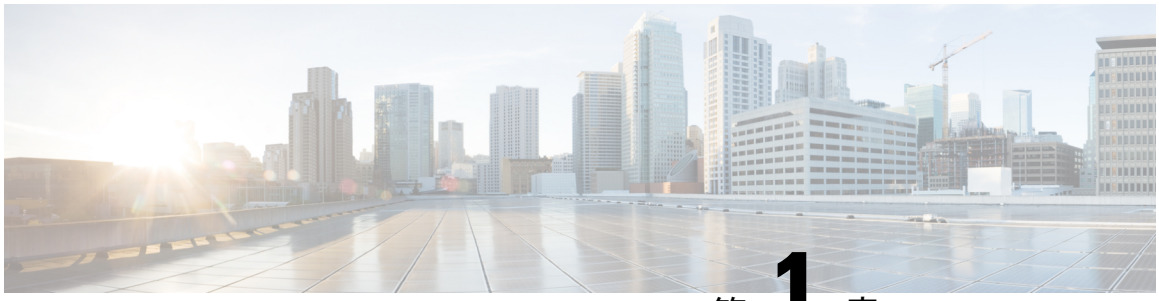
MACsec/MKA コンフィギュレーション ガイド（Cisco IOS XE Gibraltar 16.10.x 向け）

初版：2014 年 12 月 17 日

最終更新：2018 年 7 月 19 日

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/

目 次



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Catalyst スイッチング用 Cisco IOS XE Release 3.7.0E、および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の現行の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

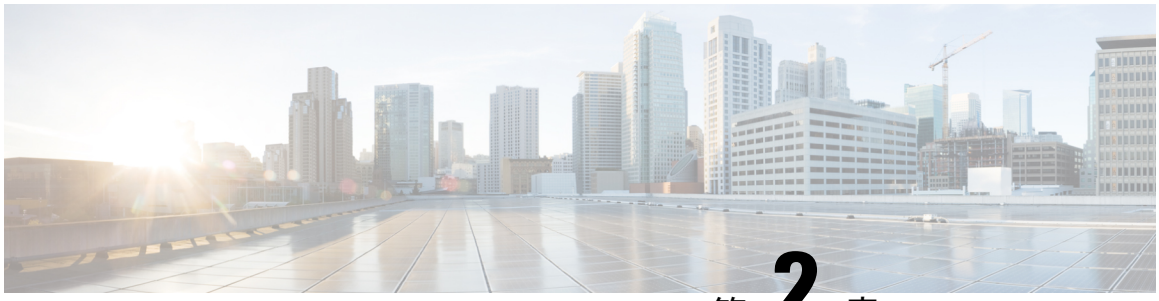
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- 『Cisco IOS コマンド リファレンス』、すべてのリリース

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

WAN MACSEC および MKA のサポートの機能強化

WAN MACsec および MKA 機能により、WAN 上での MACsec のサポート、および MACsec Key Agreement（MKA）プロトコルのアップリンクのサポートと事前共有キーのサポートが導入されます。

WAN MACsec および MKA

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : WAN MACsec* および *MKA*

機能名	リリース	機能情報
WAN MACsec と MKA	Cisco IOS XE リリース 3.14S	WAN MACsec および MKA 機能により、WAN 上での MACsec のサポート、および MACsec Key Agreement（MKA）プロトコルのアップリンクのサポートと事前共有キーのサポートが導入されます。 次のコマンドが導入または変更されました。confidentiality-offset、eapol destination-mac、key-server、linksec policy、replay-protection window-size
WAN インターフェイス カード上の MACsec	Cisco IOS XE Release 3.16S	WAN インターフェイス カード上の MACsec 機能により、Cisco 4000 シリーズ サービス統合型ルータ（ISR）上の WAN インターフェイス カードに MACsec サポートが導入されます。
EAPoL フレームイーサネット タイプを変更する MACsec CLI オプション	Cisco IOS XE リリース 3.17S	EAPOL フレーム イーサネット タイプを変更する MACsec CLI オプションの機能により、Extensible Authentication Protocol over LAN（EAPoL）フレーム イーサネット タイプをユーザが変更できるようにするための設定オプションが提供されます。 次のコマンドが導入または変更されました。eapol eth-type
MACsec Extended Packet Numbering（XPN）	Cisco IOS XE Fuji リリース 16.8.1	MKA/MACsec の XPN 機能を使用すると、大容量リンク（40 Gb/s、100 Gb/s およびそれ以上）で発生する可能性のある頻繁な SAK キー再生成が不要になり、定義された MKA ポリシーの下で GCM-AES-XPN-128 または GCM-AES-XPN-256 暗号スイートを使用するためのオプションが提供されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

WAN MACsec および MKA のサポート機能強化の前提条件

- WAN MACsec には MACsec ライセンスが必要です。*Cisco ASR 1000* シリーズ イーサネット ラインカード データシート ドキュメントの表 8 を参照してください。
  https://www.cisco.com/c/en/us/products/collateral/application-networking-services/wide-area-application-services-waas-software/data-sheet-c78-729778.html
- Cisco ISR 4000 プラットフォームでは、MACsec を設定するために HSECK9 ライセンスが必要です。
- レイヤ 2 の透過型イーサネット サービスが存在している必要があります。
- サービス プロバイダ ネットワークが、Extensible Authentication Protocol over LAN（EAPoL）などの 透過的な MACsec レイヤ 2 制御プロトコルを提供する必要があります。

WAN MACsec および MKA のサポート機能強化の制約事項

- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、MACsecで AAA アカウンティングがサポートされません。
- MACsec でサポートされる最大速度は、各インターフェイスのライン レートです。ただし、転送機能はシステムの最大転送容量によって制限される場合があります。
- 1 つの ギガビットイーサネット インターフェイスに対して、インターフェイスあたり最大 8 個のピアを設定できます。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ（ASR 1000）では、10 個のギガビットイーサネット インターフェイスで、インターフェイスごとに最大 32 ピアを設定できます。
- Cisco ASR1001-X ルータでは、MACsec は内蔵ポートでのみサポートされます。ルータに取り付けられている共有ポート アダプタ（SPA）では有効にすることはできません。
- イーサ チャネル（リンク バンドル）での MACsec の設定はサポートされていません。
- MACsec を使用して設定されたインターフェイスは、イーサ チャネルの一部にはできません。
- メイン インターフェイス上でコマンド **macsec dot1q-in-clear 1** を使用してネイティブ サブインターフェイス上に設定された MACsec はサポートされません。
- Cisco IOS XE Denali 16.3.3 リリース以降では、RP のスイッチオーバー時に、物理/サブインターフェイス コンフィギュレーション モードでの macsec コマンドの再入力は必要ありません。
- キーのラップ解除の失敗が原因で MKA セッションが切断された場合は、それぞれのインターフェイスで MACsec 設定コマンドを使用して事前共有キー ベースの MKA セッションを再設定し、MKA セッションを接続状態にします。

- イーサネット仮想回線（EVC）を使用した物理インターフェイスで設定されたMACsecはサポートされません。このような場合、EAPoL フレームはドロップされます。

WAN MACsec および MKA のサポートの機能強化に関する情報

MACsec および MKA の概要

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。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。 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 フォン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 Key Agreement（MKA）による 802.1AE 暗号化は、ルータまたはスイッチとホスト デバイス間の暗号化用に、ダウンリンク ポートでサポートされます。

MACsec は、イーサネット パケットの送信元および宛先 MAC アドレスを除くすべてのデータを暗号化します。

WAN またはメトロ イーサネット上に MACsec サービスを提供するために、サービス プロバイダーは、Ethernet over Multiprotocol Label Switching（EoMPLS）および L2TPv3 などのさまざまなトランスポート レイヤ プロトコルを使用して、E-Line や E-LAN などのレイヤ 2 透過サービスを提供しています。

EAP-over-LAN（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。3 ハートビート（1 ハートビートは 2 秒）後に MKPDU が受信されない場合、ライブ ピアのリストからピアが削除されます。たとえば、クライアントが切断さると、最後の MKPDU が クライアントにより受信されてから 3 ハートビートが経過するまで、スイッチ上の参加者は MKA を操作し続けます。

MKA 機能のサポートにより、暗号化されていない VLAN タグ（802.1Q タグ）などのトンネリング情報を提供します。そのため、サービス プロバイダーは、複数のポイントツーポイント サービスやマルチポイント サービスが単一の物理インターフェイス上で共存でき、表示されるようになった VLAN ID に基づいて差別化できるように、サービス多重化を提供できます。

サービス多重化の他に、暗号化されていない VLAN タグもサービス プロバイダーが 802.1Q タグの一部として表示されている 802.1P（CoS）に基づいて SP ネットワーク全体にわたり Quality of Service（QoS）を提供できるようにします。

WAN MACsec および MKA のサポート機能強化の利点

- ポイントツーポイント（P2P）導入モデルのサポート。
- ポイントツーマルチポイント（P2MP）導入モデルのサポート。
- 同一の物理インターフェイス上の複数の P2P および P2MP 導入のサポート。
- 128 ビットおよび 256 ビット Advanced Encryption Standard のサポート：データ パケットの Galois Counter Mode（AES-GCM）暗号化。
- 128 ビットおよび 256 ビット Advanced Encryption Standard のサポート：制御パケットの暗号ベースのメッセージ認証コード（AEC-CMAC）暗号化。
- キャリア イーサネット サービス多重化を有効にするための、clear オプションでの VLAN タグのサポート。
- MACsec サブインターフェイスと非 MACsec サブインターフェイスの共存のサポート。
- 設定可能な Extensible Authentication Protocol over LAN 宛先アドレスのサポート。
- EAPoL イーサネット タイプを変更する設定可能オプションのサポート。
- サービス プロバイダ ネットワークでのパケット再順序付けに対応するための、設定可能なリプレイ保護ウィンドウ サイズのサポート。
- MACsec ステートレス スイッチオーバーのサポート。デュアル RP セットアップでのルート プロセッサ（RP）スイッチオーバーの実行時に、既存の MACsec セッションが切断され、セッションが自動的に再ネゴシエート/再初期化されます（ステートレス スイッチオーバー）。このプロセス中に、数秒間のトラフィック ドロップが複数回発生することがあります。MACsec ステートレス スイッチオーバーは、Cisco IOS XE Everest 16.6 リリース以降でサポートされています。

WAN MACsec および MKA のサポート機能強化の実装のベスト プラクティス

- MACsec を有効にする前に、基本的なレイヤ 2 イーサネット接続が確立され、検証されていることを確認します。カスタマー エッジ デバイス間の基本的な ping が機能している必要があります。
- WAN MACsec を初めて設定する場合は、MACsec を有効にした後にセッションの確立に失敗した場合にロック アウトされないように、リモート サイトへのアウトオブバンド接続が確立されていることを確認します。
- MACsec を初めて確立するときには **access-control should-secure** コマンドを設定し、その後、移行で必要になる場合以外は、セッションの確立が成功した後にこのコマンドをデフォルトの **access-control must-secure** に変更することを推奨します。

- インターフェイス MTU を設定し、これを MACsec オーバーヘッドに合わせて調整することを推奨します（例：32 バイト）。MACsec の暗号化と復号化は物理レベルで行われ、MTU のサイズは送信元または宛先のルータには影響しませんが、中間サービス プロバイダ ルータに影響を与える可能性があります。インターフェイスで MTU 値を設定すると、MACsec オーバーヘッドを含む MTU ネゴシエーションが可能になります。

MKA ポリシーの継承

WAN ルータでは MKA ポリシーは継承され、デフォルト値も含まれます。新しいセッションが開始されると、次のルールが適用されます。

- MKA ポリシーがサブインターフェイスに設定されている場合、このポリシーは MKA セッションが開始されると適用されます。
- MKA ポリシーがサブインターフェイスに設定されていない場合、物理インターフェイスに設定されているポリシーがセッションの開始時に適用されます。
- MKA ポリシーがサブインターフェイスまたは物理インターフェイスに設定されていない場合、デフォルトのポリシーがセッションの開始時に適用されます。

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。

MACsec キー チェーンを設定するには、**key chain** *name* **macsec** を使用します。

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。

プロトコル パケットの暗号化アルゴリズム

MKA 制御プロトコル パケット暗号化の暗号化アルゴリズムの選択は次のように行われます。

- MKA 制御プロトコル パケットを暗号化するための暗号化アルゴリズムは、キーチェーンの一部として設定されます。1 つのキー チェーンに設定できる暗号化アルゴリズムは 1 つだけです。
- キー サーバは、使用されるキー チェーン内に設定された MKA 暗号化アルゴリズムを使用します。
- すべての非キー サーバは、キー サーバと同じ暗号化アルゴリズムを使用する必要があります。

MKA 暗号化アルゴリズムが設定されていない場合、デフォルトの暗号化アルゴリズムである AES-CMAC-128（128 ビット Advanced Encryption Standard を使用した暗号ベースのメッセージ認証コード）が使用されます。

データ パケットの暗号化アルゴリズム：

```
mka policy p1
macsec-cipher-suite [gcm-aes-128 | gcm-aes-256
```

MKA 制御パケットの暗号化アルゴリズム：

```
key chain <name> macsec
key 01
key-string <Hex string>
cryptographic-algorithm [aes-256-cmac  | aes-128-cmac]
```

非キー サーバでリストにキー サーバと同じ暗号スイートが設定されているか、デフォルト設定になっている場合、暗号スイートのロールオーバーをシームレスにするために、キー サーバ内のデータ パケット暗号スイートを変更することが推奨されます。

スムーズな移行のためのアクセス制御オプション

MACsec がインターフェイスで有効になっている場合、デフォルトでインターフェイス トラフィック全体がセキュリティ保護されます。MACsec は、暗号化されていないパケットを同じ物理インターフェイスから送受信することを許可しません。ただし、限定されたサブインターフェイスで MACsec を有効にするために、暗号化されていないパケットを同じ物理インターフェイスから送受信できるようにする追加のシスコ独自の拡張機能が実装されています。

暗号化されていないパケットの動作を制御するには、**macsec access-control** {**must-secure** | **should-secure**} コマンドを使用します。

- キーワード **should-secure** は、物理インターフェイスまたはサブインターフェイスからの暗号化されていないパケットの送受信を許可します。
- キーワード **must-secure** は、物理インターフェイスまたはサブインターフェイスからの暗号化されていないパケットの送受信を許可しません。このようなパケットは、MKA 制御プロトコル パケットを除きすべてドロップされます。
- 限定されたサブインターフェイスでのみMACsecが有効になっている場合は、対応するインターフェイスで **should-secure** キーワード オプションを設定します。

サブインターフェイスでの MACsec のデフォルト設定は、**macsec access-control must-secure** です。このオプションは、**macsec** コマンドがインターフェイスで設定されている場合、デフォルトで有効になっています。

（注） **macsec access-control should-secure** コマンドはインターフェイス レベルでのみ設定でき、サブインターフェイス レベルでは設定できません。このコマンドを設定すると、セキュリティ保護された MACsec セッションで暗号化されていないトラフィックが許可されます。

（注） 非 MACsec サブインターフェイスの場合は、トラフィックが通過できるように **should-secure** オプションを設定する必要があります。

Extensible Authentication Protocol over LAN 宛先アドレス

MACsec セキュア セッションを確立する前に、MKA（MACsec Key Agreement）が制御プロトコルとして使用されます。MKA は、暗号化に使用する暗号スイートを選択し、必要なキーとパラメータをピア間で交換します。

MKA は、MKA メッセージを送信するためのトランスポート プロトコルとして Authentication Protocol over LAN（EAPoL）を使用します。デフォルトでは、EAPoL は宛先マルチキャスト MAC アドレスとして 01:80: c2:00:00:03 を使用して、複数の宛先へパケットをマルチキャストします。EAPoL は標準ベースのプロトコルであり、IEEE 802.1 x などの他の認証メカニズムでも同じプロトコルが使用されます。サービス プロバイダ クラウド内のデバイスは、（宛先マルチキャスト MAC アドレスに基づいて）このパケットを消費し、EAPoL パケットの処理を試み、最終的にはパケットをドロップします。これにより、MKA セッションが失敗します。

インターフェイス上でサービス プロバイダに送信される EAPoL パケットの宛先 MAC アドレスを変更するには、**eapol destination-address** コマンドを使用します。これにより、サービス プロバイダは、パケットを消費せずに、他のデータ パケットと同様にトンネリングできます。

（注） EAPoL宛先アドレスは、物理レベルまたはサブインターフェイスレベルで、独立して設定できます。物理インターフェイスで設定する場合、設定はサブインターフェイスによって自動的に継承されます。サブインターフェイスでの明示的な設定は、そのサブインターフェイスで継承された値またはポリシーよりも優先されます。

リプレイ保護ウィンドウ サイズ

リプレイ保護は、リプレイ攻撃に対抗するためにMACsecにより提供される機能です。暗号化された各パケットには一意のシーケンス番号が割り当てられ、シーケンスはリモートエンドで確認されます。メトロ イーサネット サービス プロバイダ ネットワークを介して送信されるフ

レームは、順序が変更されることが多くあります。これは、ネットワーク内で使用されている優先順位付けとロードバランシング のメカニズムによるものです。

フレームの順序が変更されるプロバイダ ネットワーク上で MACsec の使用をサポートするには、リプレイ ウィンドウが必要です。ウィンドウ内のフレームは順不同で受信できますが、リプレイ保護されません。デフォルトのウィンドウ サイズは 64 に設定されています。リプレイ ウィンドウ サイズを変更するには、**macsec replay-protection window-size** コマンドを使用します。ウィンドウ サイズの範囲は 0 ～ 4294967295 です。

リプレイ保護ウィンドウは、ゼロに設定することで、厳格な受信順序とリプレイ保護を強制できます。

（注） リプレイ保護ウィンドウは、物理インターフェイスまたはサブインターフェイスで独立して設定できます。物理インターフェイスで設定する場合、設定はサブインターフェイスによって自動的に継承されます。サブインターフェイスでの明示的な設定は、そのサブインターフェイスで継承された値またはポリシーよりも優先されます。

Extended Packet Numbering（XPN）

各 MACsec フレームには 32 ビット パケット番号（PN）が含まれており、特定のセキュリティ アソシエーション キー（SAK）に対して一意です。PN が枯渇すると（75% のしきい値に達した後）、SAK キーが再生成されてデータ プレーン キーが更新されます。40 Gb/s などの高容量リンクの場合は数秒以内に PN が枯渇し、コントロール プレーンに対する SAK キーの頻繁な再生成が必要になります。XPN が使用されている場合、MACsec フレームの PN は64 ビット値であるため、PN が枯渇するまで数年を要します。これにより、高速リンクで頻繁な SAK キー再生成が発生しなくなります。MKA/MACsec の XPN 機能により、大容量リンクで発生する可能性のある頻繁な SAK キー再生成が不要になります。XPN は、40 Gb/s、100 Gb/s などの高速リンクでの FIPS/CC 準拠の必須要件です。XPN では、次の 2 種類のキー再生成が可能です。

- **ボリュームベースのキー再生成**：頻繁な SAK キー再生成が発生しないようにするために、定義された MKA ポリシーの下で GCM-AES-XPN-128 または GCM-AES-XPN-256 暗号スイートを使用して XPN を設定できます。これらの暗号スイートを使用すると、1 つの SAK で 2^{32} 以上のフレームを保護できます。XPN では、64 ビット値の PN がサポートされています。MACsec フレームには最下位 32 ビットのみが含まれ 、最上位 32 ビットはピア自身、つまり送信側と受信側のピアの両方により維持されます。それぞれのピアの LAPN（許容される最小パケット番号）の MSB（最上位ビット）が設定され、MACsec フレームで受信した PN 値の MSB が 0 の場合、PN の最上位 32 ビットが受信側で増分されます。したがって、送信側と受信側の両方のピアが、MACsec フレーム構造を変更せずに同じ PN 値を維持します。

- **時間ベースのキー再生成**：SAK キー再生成を手動で設定するために、タイマーベースのキー再生成がサポートされており、指定された間隔で SAK キー再生成を開始することができます。インターフェイスに適用される定義済み MKA ポリシーの SAK キー再生成間隔を設定するには、MKA ポリシーコンフィギュレーションモードで **sak rekey interval** *interval* コマンドを使用します。

WAN インターフェイス カード上の MACsec

Cisco IOS XE リリース 3.16Sでは、MACsec は Cisco 4000 シリーズ サービス統合型ルータ（ISR）上の WAN インターフェイス カード（NIM-2GE-CU-SFP および NIM-2GE-CU-SFP）に導入されています。

この WAN インターフェイス カードは、2 つの 1 ギガビット イーサネット ポートを持つ次世代 WAN インターフェイス カードです。

次世代 WAN インターフェイス カードは、次のプラットフォームでサポートされます。

- Cisco ISR 4451
- Cisco ISR4431
- Cisco ISR4351
- Cisco ISR 4331
- Cisco ISR 4321

OIR サポート

WANインターフェイスカードが動作中に挿入または取り外し（OIR）されると、そのインターフェイスに関連付けられている設定が保持されます。そのため、インターフェイスがシステムに再挿入された場合、同じ設定で動作します。ただし、Cisco ISR ルータ上の Cisco IOS XE リリース 3.16s では、MACsec および MKA セッションに次の制限が適用されます。

- 一部のスケーリング シナリオでは、OIR 後に MKA/MACsec セッションが失われる可能性があります。
- MKA/MACsec セッションは、OIR 後に再確立する必要があります。

Cisco 4000 シリーズ サービス統合型ルータでの MACsec のパフォーマンス

表 *2 : Cisco ISR 4451* ルータのパフォーマンス数値

フレーム サイズ	ポートごとの**NDR**（**pps**）	ライン レート（**%**）	モジュール **CPU**（**%**）	ホスト **CPU**（**%**）
64	1,077,532	72.41	44	65
128	692,568	82	29	42
256	405,797	89.6	17	25
iMIX	296,500	90.57	13	24
512	221,615	94.32	9	14

フレーム サイズ	ポートごとの**NDR**（**pps**）	ライン レート（**%**）	モジュール **CPU**（**%**）	ホスト **CPU**（**%**）
1024	116,163	97.02	5	7
1518	79,609	97.95	3.5』	5
9000	13,808	99.64%	1	2

Cisco ASR 1000 プラットフォーム上の MACsec のパフォーマンス

次の表に、Cisco IOS XE 16.6 リリース以降の Cisco ASR 1000 ルータのパフォーマンス数値を示します。

表 *3 : Cisco ASR1001-X* ルータのパフォーマンス数値

フレーム サイズ	集約レート ビット（**bps**）	ライン レート（**%**）	**ESP CPU**（**%**）
64	10064767891.17	65.59	93.33
iMIX	17763891467.40	93.14	26
1418	19311044388.60	97.89	9

表 *4 : Cisco ASR1001-HX* ルータのパフォーマンス数値

フレーム サイズ	集約レート ビット（**bps**）	ライン レート（**%**）	**ESP CPU**（**%**）
64	28681245486.53	65.59	99
iMIX	65019905182.40	93.14	42
1418	64975057119.60	97.89	11

表 *5 : Cisco ASR1002-HX* ルータのパフォーマンス数値

フレーム サイズ	集約レート ビット（**bps**）	ライン レート（**%**）	**ESP CPU**（**%**）
64	51467063849.50	52.84	96
iMIX	105267526427	87.60	36
1418	100007152449	84.48	10

ASR 1000 および ISR 4400 プラットフォームの MACsec 互換性マトリックス

プラットフォーム	内蔵ポート	EPA-18x1GE	EPA-10x10GE	EPA-1x40GE / EPA-2x40GE	NIM-2GE-CU-SFP
ASR1001-X	Cisco IOS XE Release 3.13.1S	該当なし	該当なし	該当なし	該当なし
ASR1001-HX	Cisco IOS XE Everest リリース 16.4.1	該当なし	該当なし	該当なし	該当なし
ASR1002-HX	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Denali リリース 16.3.2 / 16.4.1	Cisco IOS XE Fuji リリース 16.8.1	該当なし
ASR1006-X	該当なし	Cisco IOS XE Everest リリース 16.4.1	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Fuji リリース 16.8.1	該当なし
ASR1009-X	該当なし	Cisco IOS XE Everest リリース 16.4.1	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Fuji リリース 16.8.1	該当なし
ASR1013	該当なし	Cisco IOS XE Everest リリース 16.4.1	Cisco IOS XE Denali リリース 16.3.1	Cisco IOS XE Fuji リリース 16.8.1	該当なし
ISR44XX	該当なし	該当なし	該当なし	該当なし	Cisco IOS XE Release 3.16.0S

（注）

- GLC-100FX はサポートされていません。
- MIP-100 は、ASR1006X、ASR1009X、ASR1013 プラットフォームで EPA18x1GE、EPA-10x10GE、EPA-1x40GE、および EPA-2x40GE に対応するために必要です。
- ASR1001-X 上の MACsec には IPsec ライセンスが必要です。
- ASR1001-HX、ASR1002-HX、および EPA 上の MACsec には、ポートごとに MACsec ライセンスが必要です。
- Cisco ISR 4000 プラットフォームでは、MACsec を設定するために HSECK9 ライセンスが必要です。

WAN MACsec および MKA のサポート機能強化の設定方法

MKA の設定

MACsec Key Agreement（MKA）は、キー管理パラメータの設定と制御を可能にします。MKA を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mka policy** *policy-name*
4. **include-icv-indicator**
5. **key-server priority** *key-server-priority*
6. **macsec-cipher-suite** {**gcm-aes-128** | **gcm-aes-256** | **gcm-aes-xpn-128** | **gcm-aes-xpn-256**}
7. **sak-rekey interval** *interval*
8. **confidentiality-offset 30**
9. **end**

手順の詳細

	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。 • 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 MKAPolicy`	MKA ポリシーを設定します。
ステップ 4	**include-icv-indicator** 例： `Device(config-mka-policy)# include-icv-indicator`	（任意）MKPDU に ICV インジケータを含めます。
ステップ 5	**key-server priority** *key-server-priority* 例：	（任意）MKA キー サーバの優先度を設定します。

	コマンドまたはアクション	目的
	`Device(config-mka-policy)# key-server priority 200`	
ステップ 6	**macsec-cipher-suite** {**gcm-aes-128** | **gcm-aes-256** | **gcm-aes-xpn-128** | **gcm-aes-xpn-256**} 例： `Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128 gcm-aes-256`	（任意）セキュア アソシエーション キー（SAK）導出のための暗号スイートを設定します。各暗号スイートの各オプションは 1 回だけ繰り返すことができますが、任意の順序で使用できます。
ステップ 7	**sak-rekey interval** *interval* 例： `Device(config-mka-policy)# sak-rekey interval 30`	（任意）SAK キー再生成間隔を秒単位で設定します。範囲は 30 ～ 65535 で、デフォルト値は 0 です。SAK キー再生成タイマーは、デフォルトでは設定されるまで開始されません。 • SAK キー再生成タイマーを停止するには、定義された MKA ポリシーの下で **no sak-rekey interval** コマンドを使用します。
ステップ 8	**confidentiality-offset 30** 例： `Device(config-mka-policy)# confidentiality-offset 30`	（任意）MACsec 操作の機密性オフセットを設定します。
ステップ 9	**end** 例： `Device(config-mka-policy)# end`	特権 EXEC モードに戻ります。

例

show mka policy コマンドを使用して設定を確認できます。次に、**show** コマンドの出力例を示します。MKPDU に icv-indicator を含めないようにするには、MKA ポリシーで **no include-icv-indicator**でコマンドを使用します。

```
MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
================================================================================
*DEFAULT POLICY*  0    FALSE 0  FALSE TRUE   GCM-AES-128     N/A
                                              GCM-AES-256

confid50          0    FALSE 50 FALSE TRUE   GCM-AES-128
                                              GCM-AES-256

icv               0    FALSE 0  FALSE TRUE   GCM-AES-128     Te3/0/9
```

```
                                                GCM-AES-256

k10               0     FALSE 0   FALSE TRUE    GCM-AES-128
                                                GCM-AES-256

xpn128            0     FALSE 0   FALSE TRUE    GCM-AES-XPN-128 Fo2/1/1
```

インターフェイスでの MACsec および MKA の設定

インターフェイスで MACsec と MKA を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **mka policy** *policy-name*
5. **mka pre-shared-keykey-chain***key-chain-name*
6. **macsec** *ethertype*
7. **macsec replay-protection window-size**
8. **end**

手順の詳細

	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。 • 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** *type number* 例： `Device(config)# 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	**mka policy** *policy-name* 例： `Device(config-if)# mka policy MKAPolicy`	MKA ポリシーを設定します。
ステップ 5	**mka pre-shared-keykey-chain***key-chain-name* 例：	MKA pre-shared-key key-chain に keychain1 を設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# mka pre-shared-key key-chain key-chain-name`	（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のいずれかで設定できますが、物理インターフェイスとサブインターフェイスの両方で設定することはできません。
ステップ 6	**macsec** *ethertype* 例： `Device(config-if)# macsec ethertype`	EAPOL フレーム イーサネット タイプの MACsec を設定します。
ステップ 7	**macsec replay-protection window-size** 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`	特権 EXEC モードに戻ります。

MKA 事前共有キーの設定

MACsec Key Agreement（MKA）事前共有キーを設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *key-chain-name* [**macsec**]
4. **key** *hex-string*
5. **cryptographic-algorithm** {**gcm-aes-128** | **gcm-aes-256**}
6. **key-string** {[**0** | **6**] *pwd-string* | **7** | *pwd-string*}
7. **lifetime local** {{*day month year* **duration** *seconds*}
8. **end**

手順の詳細

	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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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** *key-chain-name* [**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** *hex-string* 例： `Device(config-keychain)# key 9ABCD`	キーを設定して、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。 （注） Cisco IOS XE Everest リリース 16.6.1 以降では、接続アソシエーション キー名（CKN）は、このキーの 16 進文字列として設定されている文字列とまったく同じ文字列を使用します。この動作の変更の詳細については、このタスクの後の「MKA-PSK：CKN動作の変更」セクションを参照してください。
ステップ 5	**cryptographic-algorithm** {**gcm-aes-128** | **gcm-aes-256**} 例： `Device(config-keychain-key)# cryptographic-algorithm gcm-aes-128`	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**] *pwd-string* | **7** | *pwd-string*} 例： `Device(config-keychain-key)# key-string 0 pwd`	キー文字列のパスワードを設定します。
ステップ 7	**lifetime local** {{*day month year* **duration** *seconds*} 例： `Device(config-keychain-key)# lifetime local 16:00:00 Nov 9 2014 duration 6000`	キー文字列のパスワードを設定します。
ステップ 8	**end** 例： `Device(config-keychain-key)# end`	特権 EXEC モードに戻ります。

接続アソシエーション キー（CAK）再生成の例

CAK のキー再生成は、次の場合に発生します。

- キー チェーン K1 内でキー 01 からキー 02 に移動する場合。
- あるキー チェーン K1 から別のキー チェーン K2 に移動する場合。

注：CAS キー再生成が正常に行われ、キー/CA 間のシームレスな移行（トラフィック損失やセッションの再起動を伴わない）が実現するように、各キーのライフタイム間にオーバーラップがあるようにキーを設定することを推奨します。

```
Device# show key chain k1
Key-chain k1:
    MacSEC key chain
    key 01 — text "c890433a1e05ef42d723a6b58af8fdbf7a25f42b3cda6a5eeb5ae4bf3a0a679f"
        lifetime (00:00:00 UTC Oct 29 2014) - (12:10:00 UTC Oct 29 2014)
    key 02 — text "14d9167d538819405c0ff78c655141ed4b3c7242562c0fb0f7a56f780bf29e52"
        lifetime (12:00:00 UTC Oct 29 2014) - (18:05:00 UTC Oct 29 2014)
    key 03 — text "88d971cb19d9f2598ad76edc562ade2e7e91e3ed70524f5c3c4d8d9599d0670e"
        lifetime (18:00:00 UTC Oct 29 2014) - (18:10:00 UTC Oct 29 2014)
    key 04 — text "75474bce819b49ad7e5bd06236bc0c944c69892f71e942e2f9812b7d3a7b2a5f"
        lifetime (18:10:00 UTC Oct 29 2014) - (infinite)

!In this case, Key 01, 02, 03 have overlapping time, but not key 04. Here is the sequence,
 how this works:
  @00:00:00 - A new MKA session is Secured with key 01
  @12:00:00 - CAK Rekey triggers with key 02 and upon success goes to Secured state
  @18:00:00 - CAK Rekey triggers with key 03 and upon success goes to Secured state
  @18:10:00 - Key 03 dies, hence MKA sesion using this key is brought down
  @18:10:00 - Key 04 becomes active and a new MKA session is triggered with this key.
Upon success, session will be Secured and UP for infinite time.
```

MKA-PSK：CKN 動作の変更

Cisco IOS XE Everest リリース 16.6.1 以降では、MKA-PSK セッションで、固定 32 バイトの代わりに、接続アソシエーション キー名（CKN）は、このキーの 16 進文字列として設定されている文字列とまったく同じ文字列を CKN として使用します。

設定例：

```
configure terminal
key chain abc macsec
  key 11
    cryptographic-algorithm aes-128-cmac
    key-string 12345678901234567890123456789013
    lifetime local 12:21:00 Sep 9 2015 infinite

 end
```

上記の例では、 **show mka session** コマンドの **show** コマンド出力は次のようになります。

```
Device# show mka session

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

==============================================================================================
```

```
          Interface      Local-TxSCI         Policy-Name      Inherited        Key-Server
           Port-ID        Peer-RxSCI           MACsec-Peers     Status             CKN

=============================================================================================

           Et0/0          aabb.cc00.6600/0002     icv            NO                NO

           2              aabb.cc00.6500/0002 1                  Secured           11
*Note that the CKN key-string is exactly the same that has been configured for the key
as hex-string.*
```

一方でCKN動作が変更され、もう一方でCKN動作が変更されていない2つのイメージ間の相互運用性の場合、キーの16進数文字列は64文字の16進数文字列である必要があります。この文字列は、CKN動作が変更されたイメージを持つデバイスで動作するようにゼロ パディングされている必要があります。次の例を参照してください。

Configuration without CKN key-string behavior change:

```
config t
  key chain abc macsec
   key 11
   cryptographic-algorithm aes-128-cmac
   key-string 123456789012345678901234567890123
   lifetime local 12:21:00 Sep 9 2015 infinite
```

Configuration with CKN key-string behavior change:

```
config t
  key chain abc macsec
   key 1100000000000000000000000000000000000000000000000000000000000000000000
   cryptographic-algorithm aes-128-cmac
   key-string 123456789012345678901234567890123
   lifetime local 12:21:00 Sep 9 2015 infinite
```

EAPoL イーサネット タイプを変更するオプションの設定

-

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **eapol** *eth-type*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**enable** 例：	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
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** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	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	**eapol** *eth-type* 例： `Device(config-if)# eapol eth-type 0xB860`	インターフェイス上の EAPoL フレームのイーサネット タイプ（16 進数）を設定します。 （注） Cisco IOS リリース XE 3.17 以降では、**macsec eth-type** コマンドは **eapol eth-type** コマンドに置き換えられました。
ステップ 5	**exit** 例： `Device(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、グローバル コンフィギュレーション モードに戻ります。

インターフェイスおよびサブインターフェイスでの宛先 MAC アドレスの設定

インターフェイスまたはサブインターフェイスで宛先 MAC アドレスを設定するには、次のタスクを実行します。宛先 MAC は、ピアの MAC またはマルチキャスト MAC アドレスにすることができます。**eapol destination-address** コマンドがメイン インターフェイスで設定されている場合は、そのインターフェイス上のすべてのサブインターフェイスに適用されます。ただし、 **eapol destination-address** コマンドがサブインターフェイスで設定されている場合は、メイン インターフェイスのコマンドよりも優先されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **eapol destination-address** [*MAC-Address* | [**bridge-group-address** | **broadcast-address** | **lldp-multicast-address**]
5. **eapol destination-address bridge-group-address**
6. **eapol destination-address broadcast-address**
7. **eapol destination-address lldp-multicast-address**
8. **end**

手順の詳細

	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。 • 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** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/1`	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	**eapol destination-address** [*MAC-Address* | [**bridge-group-address** | **broadcast-address** | **lldp-multicast-address**] 例： `Device(config-if)# eapol destination-address 0018.b967.3cd0`	インターフェイス上の Extensible Authentication Protocol over LAN（EAPoL）宛先 MAC アドレスを設定します。
ステップ 5	**eapol destination-address bridge-group-address** 例： `Device(config-if)# eapol destination-address bridge-group-address`	宛先アドレスをブリッジ グループとして設定します。
ステップ 6	**eapol destination-address broadcast-address** 例： `Device(config-if)# eapol destination-address broadcast-address`	宛先 MAC アドレスをブロードキャスト アドレスとして設定します。
ステップ 7	**eapol destination-address lldp-multicast-address** 例： `Device(config-if)# eapol destination-address lldp-multicast-address`	宛先アドレスを LLDP マルチキャスト アドレスとして設定します。
ステップ 8	**end** 例： `DeviceDevice(config-if)# end`	特権 EXEC モードに戻ります。

WAN MACsec および MKA の設定例

例：EPL サービスを使用した CE から CE へのポイントツーポイント接続

次に、ポートベースのサービスを使用して、イーサネット プライベート回線（EPL）を使用したポイントツーポイントのカスタマーエッジからカスタマーエッジへの接続の設定例を示します。

```
!Customer Edge 1
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!Customer Edge 2
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  ip address 10.3.1.2 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
```

例：EVPLサービスを使用したハブとスポークのポイントツーポイント接続

次に、VLANモードのイーサネット仮想プライベート回線（EVPL）サービスを使用した、ポイントツーポイントのハブ アンド スポーク接続の設定例を示します。

```
!CE 1
key chain k1 macsec*
 key 01
 key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
interface GigabitEthernet0/0/4.2
  encapsulation dot1Q 20
  ip address 10.3.2.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
```

```
!CE 2
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
   ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!CE 3
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
```

（注） アスタリスク（*）付きのコマンドは、すべて必須コマンドです。

例：MACsec および非 MACsec スポークを使用したポイントツーポイントのハブ アンド スポーク接続

次に、MACsec および非 MACsec スポークを使用したポイントツーポイントのハブアンドスポーク接続の出力例を示します。

```
!CE1
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec access-control should-secure*
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
interface GigabitEthernet0/0/4.2
  encapsulation dot1Q 20
  ip address 10.3.2.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
interface GigabitEthernet0/0/4.3
  encapsulation dot1Q 30
  ip address 10.3.3.1 255.255.255.0

!CE2
```

```
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec access-control should-secure*
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
   ip address 10.3.1.2 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!CE3
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 20
  ip address 10.3.2.2 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*


!CE4
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 30
  ip address 10.3.3.2 255.255.255.0
```

例：EP-LANサービスを使用したハブとスポークのマルチポイントツーマルチポイント接続

次に、ポート モードのイーサネット プライベート回線（EP-LAN）サービスを使用した、マルチポイントツーマルチポイントのハブアンドスポーク接続の設定例を示します。

```
!CE 1
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
  cryptographic-algorithm aes-128-cmac
mka policy p1
  macsec-cipher-suite gcm-aes-256
interface GigabitEthernet0/0/4
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  mka policy p1
  macsec*

!CE 2
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
  cryptographic-algorithm aes-128-cmac
mka policy p1
  macsec-cipher-suite gcm-aes-256
interface GigabitEthernet0/0/4
  ip address 10.3.1.2 255.255.255.0
```

```
  mka pre-shared-key key-chain k1*
  mka policy p1
  macsec*

!CE 3
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
  cryptographic-algorithm aes-128-cmac
mka policy p1
  macsec-cipher-suite gcm-aes-256
interface GigabitEthernet0/0/4
  ip address 10.3.1.3 255.255.255.0
  mka pre-shared-key key-chain k1*
  mka policy p1
  macsec*
```

例：EVP-LANサービスを使用したハブとスポークのマルチポイントツーマルチポイント接続

次に、VLANモードのイーサネット仮想プライベート回線（EVP-LAN）サービスを使用した、マルチポイントツーマルチポイントのハブアンドスポーク接続の設定例を示します。

```
!CE 1
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
  eapol destination-address broadcast
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.1 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!CE 2
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
  eapol destination-address broadcast
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.2 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*

!CE 3
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
```

```
  eapol destination-address broadcast
interface GigabitEthernet0/0/4.1
  encapsulation dot1Q 10
  ip address 10.3.1.3 255.255.255.0
  mka pre-shared-key key-chain k1*
  macsec*
```

例：トラフィックに影響を与えずにメンテナンス タスクを実行する

次に、トラフィックに影響を与えないパフォーマンス メンテナンス タスクの設定例を示します。

事前共有キーの変更（CAK ロールオーバー）

次に、事前共有キーを変更するための設定例を示します。

（注） キーは、両方のルータでライフタイムを設定することで、次のキーに自動的にロールバックされるように設定できます。

```
!From
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012

!To
key chain k1 macsec*
  key 01
   key-string 12345678901234567890123456789012
   lifetime local 10:30:00 Oct 30 2014 11:30:00 Oct 30 2014
  key 02
   key-string 11145678901234567890123456789012
```

キー チェーンの変更（キー チェーン ロールオーバー）

キーチェーンを変更するための設定例を次に示します：キーチェーン ロールオーバー

```
! From
key chain k1 macsec*
  key 01
  key-string 12345678901234567890123456789012
interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k1

! To
key chain k1 macsec
  key 01
   key-string 12345678901234567890123456789012
key chain k2 macsec
  key 02
   key-string abcdef0987654321abcdef0987654321
interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k2
```

（注） 任意のキーチェーンの下に定義されたキーIDは、デバイス上の一意の値にする必要があります。

ルータは、同じセッションに参加する他のピア ルータよりも低いプライオリティを設定することによって、キーサーバになることができます。確定的にキーサーバに選択されるように、キーサーバのプライオリティを設定します。たとえば、ハブアンドスポーク シナリオでは、キーサーバの最も理想的な場所はハブ サイトのルータです。

```
!Hub Site (Key Server):
mka policy p1
key-server priority 0
!0 is the default.

interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k1
mka policy p1

!Spoke Sites (non-Key Servers):
mka policy p1
key-server priority 1

interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k1
mka policy p1
```

次に、データ トラフィックを暗号化する暗号スイートを変更するための設定例を示します。

```
mka policy p1
 macsec-cipher-suite gcm-aes-128
interface GigabitEthernet0/0/1.10
 mka policy p1

!Alternate configuration

mka policy p1
 macsec-cipher-suite gcm-aes-256
interface GigabitEthernet0/0/1.10
 mka policy p1

key chain k3 macsec
 key 01
   key-string abcdef0987654321abcdef0987654321
   cryptographic-algorithm aes-128-cmac
interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k3

!Alternate configuration:

key chain k3 macsec
 key 01
   key-string abcdef0987654321abcdef0987654321
   cryptographic-algorithm aes-256-cmac
interface TenGigabitEthernet0/0/0.10
 mka pre-shared-key key-chain k3
```

EAPOL 宛先 MAC アドレスは、物理インターフェイス コンフィギュレーション モードまたはサブインターフェイス コンフィギュレーション モードから変更できます。物

理インターフェイス レベルで設定されている場合は、サブインターフェイスによって自動的に継承されます。継承された値をオーバーライドするには、サブインターフェイス モードで MAC アドレスを設定します。デフォルトの EAPOL 宛先 MAC アドレスは 01:80: c2:00:00:03 です。

```
interface TenGigabitEthernet0/0/0
eapol destination-address <H.H.H>

!Alternate configuration

interface TenGigabitEthernet0/0/0
 bridge-group-address

!Alternate configuration

interface TenGigabitEthernet0/0/0
 lldp-multicast-address>

mka policy p1
 confidentiality-offset 30
interface GigabitEthernet0/0/1.10
 mka policy p1
```

例：メンテナンス タスクの実行（トラフィックに影響する）

リプレイ保護ウィンドウ サイズの変更

リプレイ保護ウィンドウは、物理インターフェイス コンフィギュレーション モードまたはサブインターフェイス コンフィギュレーション モードから変更できます。物理インターフェイス レベルで設定されている場合は、サブインターフェイスによって自動的に継承されます。継承された値をオーバーライドするには、サブインターフェイス モードで値を設定します。デフォルトのリプレイ保護ウィンドウ サイズは 64 です。

```
interface TenGigabitEthernet0/0/0
macsec replay-protection window-size 10

interface TenGigabitEthernet0/0/0.10
macsec replay-protection window-size 5
```

clear オプションでの VLAN（dot1q）タグの有効化または無効化

macsec dot1q-in-clear コマンドは物理インターフェイス上でのみ設定できます。この設定はサブインターフェイスによって自動的に継承されます。

```
interface GigabitEthernet0/0/1
macsec dot1q-in-clear 1
```

macsec access-control [must-secure | should-secure コマンドは物理インターフェイス上でのみ設定できます。この設定はサブインターフェイスによって自動的に継承されます。

```
interface GigabitEthernet0/0/1
macsec access-control must-secure/should-secure
```

その他の参考資料

関連資料

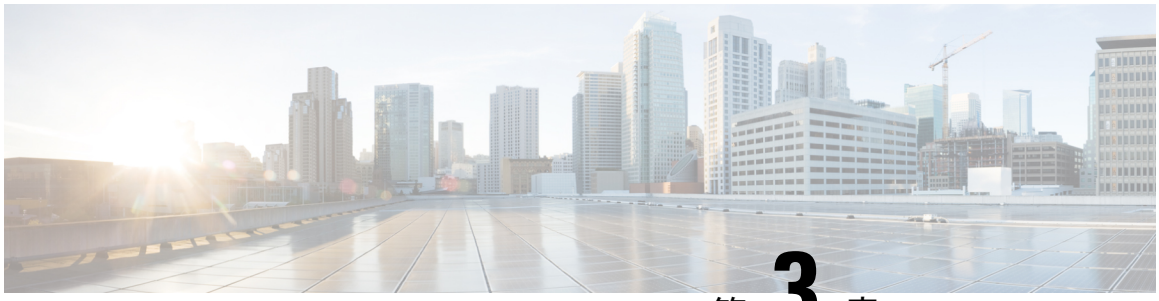
関連項目	マニュアル タイトル
Cisco IOS コマンド	Cisco IOS Master Command List, All Releases
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
IEEE 802.1AE-2006	*Media Access Control*（*MAC*）セキュリティ
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	*Media Access Control*（*MAC*）セキュリティ（IEEE 802.1AE-2006 の修正）：Extended Packet Numbering（XPN）
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（IEEE 802.1 x-2010 の修正）
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
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html



第 3 章

証明書ベースの MACsec 暗号化

証明書ベースの MACsec 暗号化機能は、Extensible Authentication Protocol – Transport Layer Security（EAP-TLS）による802.1X ポートベース認証を使用して、MACsec 暗号化が必要なルータ ポートの証明書を伝送します。EAP-TLS メカニズムを使用して相互認証を実行し、マスター セッション キー（MSK）を取得します。この MSK から、MACsec Key Agreement（MKA）プロトコル用の接続アソシエーション キー（CAK）が導出されます。

証明書ベースのMACsec暗号化は、リモート認証またはローカル認証のいずれかを使用して実行されます。

証明書ベース MACsec 暗号化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6 :* 証明書ベース *MACsec* 暗号化の機能情報

機能名	リリース	機能情報
証明書ベースの MACsec 暗号化	Cisco IOS XE Everest リリース 16.6.1	証明書ベースの MACsec 暗号化機能は、MACsec 暗号化が必要なルータポートの証明書を伝送するために、拡張認証プロトコルを使用した 802.1 x ポートベースの認証を使用します。 Transport Layer Security (eap-tls) を使用します。EAP-TLS メカニズムを使用して相互認証を実行し、マスター セッション キー（MSK）を取得します。この MSK から、MACsec Key Agreement（MKA）プロトコル用の接続アソシエーション キー（CAK）が導出されます。

証明書ベース MACsec 暗号化の前提条件

- 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。『*Cisco Identity Services Engine* リリース *2.3* 管理者ガイド』を参照してください。
- 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。

証明書ベース MACsec 暗号化の制約事項

- MKA は、ポート チャネルではサポートされていません。
- MKA のハイ アベイラビリティはサポートされません。
- サブインターフェイスでの証明書ベースの MACsec 暗号化はサポートされていません。

証明書ベース MACsec 暗号化に関する情報

MKA MACsec は、ルータ間のリンクでサポートされています。Extensible Authentication Protocol（EAP-TLS）による IEE 802.1X ポートベース認証を使用して、デバイスのポート間の MKA MACsec を設定できます。EAP-TLS 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 プロトコル用の接続アソシエーション キー（CAK）が取

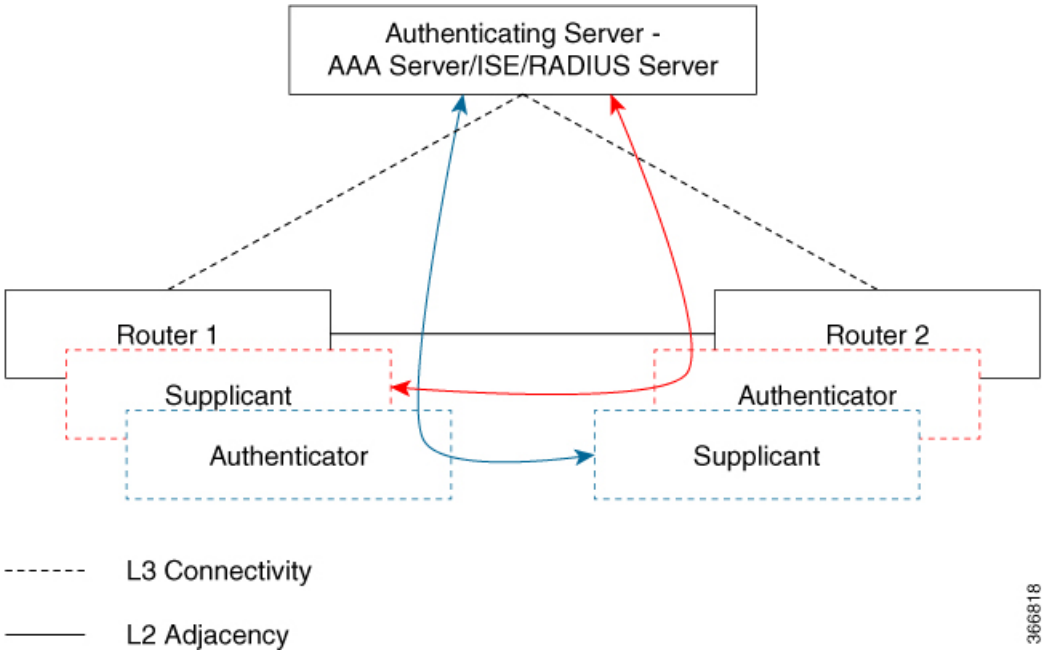
得されます。デバイスの証明書は、AAA サーバへの認証用に、EAP-TLS を使用して伝送されます。

リモート認証を使用した証明書ベース MACsec 暗号化のコール フロー

サプリカントは、ネットワークへアクセスしようとする未承認デバイスです。オーセンティケータは、サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御するデバイスです。

次の図に示すように、デバイスは直接接続されています。ルータは、ポート上で EAP サプリカントとオーセンティケータの両方として機能します。

次の図は、ルータ上の 2 つの EAP コール フロー（個別の EAP セッション ID を持つ）を示しています。赤色のフローは、ルータ 1 をサプリカントとして、ルータ 2 をオーセンティケータとして示しています。青のフローはその逆を示しています。



インターフェイスが 802.1 x の両方のロールとして設定されている場合、ルータの認証マネージャは、サプリカントとオーセンティケータのロールを使用して 2 つの EAP セッション（個別の EAP セッション ID を持つ青色と赤色のセッション）フローを持つセッションを作成し、両方のロールがリモート認証サーバ（AAA サーバ/ISE/RADIUS）を使用した EAP-TLS 相互認証をトリガします。

相互認証後、認証サーバとしてより大きい MAC アドレスを持ち、オーセンティケータ ロールを持つルータに対応するフローの MSK が選択されて CAK を導出します。

上の図では、ルータ 1 の MAC アドレスがルータ 2 の MAC アドレスより小さい場合、EAP セッション（青色のフロー）から取得されたマスターセッション キー（MSK）が MKA の EAP-MSK として使用されます（ルータ 1 はオーセンティケータとして、ルータ 2 はサプリカントとして

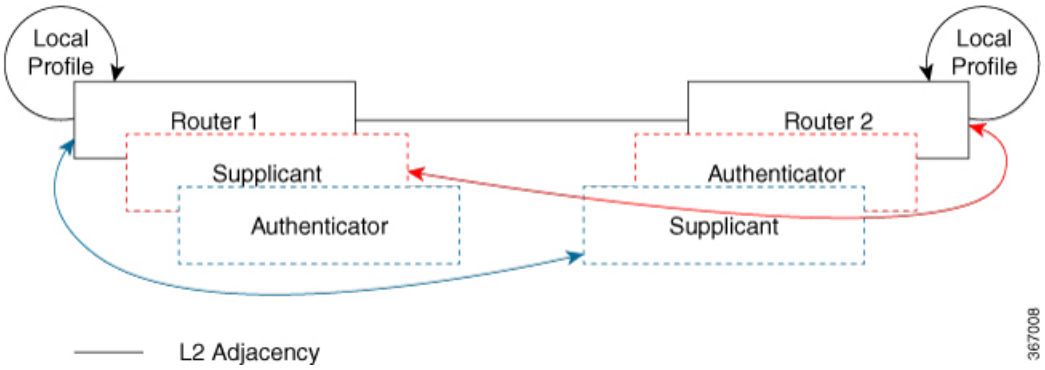
機能）。これにより、ルータ 1 が MKA キー サーバとして機能し、ルータ 2 が非キー サーバとなります。

ルータ 2 の MAC アドレスがルータ 1 のMAC アドレスよりも小さい場合は、EAP セッションから取得された MSK（赤色のフロー）が（両方のルータにより） MKA の EAP-MSK として使用され、CAK が導出されます。

ローカル認証を使用した証明書ベース MACsec 暗号化のコール フロー

次の図に示すように、デバイスは直接接続されています。ルータは、ポート上で EAP サプリカントとオーセンティケータの両方として機能します。

次の図は、ルータ上の 2 つの EAP コール フロー（個別の EAP セッション ID を持つ）を示しています。赤色のフローは、ルータ 1 をサプリカントとして、ルータ 2 をオーセンティケータとして示しています。青のフローはその逆を示しています。



インターフェイスが 802.1 x の両方のロールとして設定されている場合、ルータの認証マネージャは、サプリカントとオーセンティケータのロールを使用して 2 つの EAP セッション（個別の EAP セッション ID を持つ青色と赤色のセッション）フローを持つセッションを作成し、両方のロールがローカル認証サーバを使用した EAP-TLS 相互認証をトリガします。

相互認証後、認証サーバとしてより大きいMAC アドレスを持ち、オーセンティケーター ロールを持つルータに対応するフローの MSK が選択されて CAK を導出します。

上の図では、ルータ1の MAC アドレスがルータ2より小さい場合、eap セッション (青色のフロー) から取得したマスターセッションキー (MSK) が MKA の MSK として使用されます (ルータ1はオーセンティケータとして、ルータ2はサプリカントとして機能します)。これにより、ルータ1が MKA キーサーバとして機能し、ルータ2が非キーサーバとして機能することが保証されます。

ルータ2の MAC アドレスがルータ1よりも小さい場合は、eap セッションから取得した MSK (red フロー) が MKA の MSK として、cak を導出するために使用されます (両方のルータによって)。

リモート認証を使用した証明書ベース MACsec 暗号化の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • 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**	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*	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**	特権 EXEC モードに戻ります。
ステップ 5	**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 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。

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用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**	特権 EXEC モードをイネーブルにします。 • 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**	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*	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*	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*	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**	**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 7	**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**	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**	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。

	コマンドまたはアクション	目的
		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。 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。 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。 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。 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が示されます。「! RSA key pair associated with trustpoint is exportable.」 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。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**exit**	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 crypto pki certificate** *trustpoint name*	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**	特権 EXEC モードをイネーブルにします。 • 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**	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	**crypto pki trustpoint** *server name*	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*	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*	証明書に関連付けるキー ペアを指定します。
ステップ 6	**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 7	**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**	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	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**crypto pki enroll** *name*	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。 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。 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。 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。
ステップ 12	**crypto pki import** *name* **certificate**	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。 デバイスは、拡張子が「.req」から「.crt」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

	コマンドまたはアクション	目的
		合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 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。 （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。
ステップ 13	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 14	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。
ステップ 15	**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。

802.1x 認証の有効化と AAA 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**	特権 EXEC モードをイネーブルにします。 • 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**	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	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**dot1x system-auth-control**	デバイス上で 802.1X を有効にします。
ステップ 5	**radius server** *name*	RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 6	**address** *ip-address* **auth-port** *port-number* **acct-port** *port-number*	RADIUSサーバのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 7	**automate-tester username** *username*	RADIUS サーバの自動テスト機能を有効にします。 このようにすると、デバイスは RADIUS サーバにテスト認証メッセージを定期的に送信し、サーバからの RADIUS 応答を待機します。成功メッセージは必須ではありません。認証失敗であっても、サーバが稼働していることを示しているため問題ありません。
ステップ 8	**key** *string*	デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。
ステップ 9	**radius-server deadtime** *minutes*	いくつかのサーバが使用不能になったときの RADIUS サーバの応答時間を短くし、使用不能になったサーバがすぐにスキップされるようにします。
ステップ 10	**exit**	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 11	**aaa group server radius** *group-name*	異なる RADIUS サーバ ホストを別々のリストと方式にグループ化し、サーバ グループ コンフィギュレーション モードを開始します。
ステップ 12	**server** *name*	RADIUS サーバ名を割り当てます。
ステップ 13	**exit**	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 14	**aaa authentication dot1x default group** *group-name*	IEEE 802.1x 用にデフォルトの認証サーバ グループを設定します。
ステップ 15	**aaa authorization network default group** *group-name*	ネットワーク認証のデフォルト グループを設定します。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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	**eap profile** *profile-name*	EAP プロファイルを設定し、EAP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**method tls**	デバイスで EAP-TLS 方式を有効にします。
ステップ 5	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 6	**exit**	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 7	**dot1x credentials** *profile-name*	802.1x クレデンシャルプロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 8	**username** *username*	認証ユーザ ID を設定します。
ステップ 9	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MKA MACsec 設定の適用

EAP-TLS 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**	特権 EXEC モードをイネーブルにします。 • 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**	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*	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**	インターフェイス上で MACsec をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**authentication periodic**	このポートの再認証をイネーブルにします。
ステップ 6	**authentication timer reauthenticate interval**	再認証間隔を設定します。
ステップ 7	**access-session host-mode multi-domain**	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**	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**	ポートの認可状態を設定します。
ステップ 10	**dot1x pae both**	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプ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**	802.1x クレデンシャ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	**dot1x supplicant eap profile** *name*	EAP-TLS 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 13	**service-policy type control subscriber** *control-policy name*	インターフェイスに加入者制御ポリシーを適用します。
ステップ 14	**exit**	特権 EXEC モードに戻ります。
ステップ 15	**show macsec interface**	インターフェイスの MACsec の詳細を表示します。
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。

ローカル認証を使用した証明書ベース MACsec 暗号化の設定

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。

ローカル認証を使用した EAP クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • 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**	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	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa local authentication default authorization default**	デフォルトのローカル認証およびデフォルトのローカル認証方法を設定します。
ステップ 5	**aaa authentication dot1x default local**	IEEE 802.1x 用にデフォルトのローカル ユーザ名認証リストを設定します。
ステップ 6	**aaa authorization network default local**	ローカル ユーザの認可方式リストを設定します。
ステップ 7	**aaa authorization credential-download default local**	ローカル クレデンシャルの使用に関する認可方式リストを設定します。
ステップ 8	**exit**	特権 EXEC モードに戻ります。

ローカル EAP-TLS 認証と認証プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • 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**	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	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**dot1x credentials** *profile-name*	dot1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル 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	**username** *name* **password** *password*	認証のユーザ ID およびパスワードを設定します。

	コマンドまたはアクション	目的
ステップ 6	**exit**	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 7	**aaa attribute list** *list-name*	（任意）AAA 属性リスト定義を設定し、属性リスト コンフィギュレーション モードを開始します。
ステップ 8	**aaa attribute type linksec-policy must-secure**	（任意）AAA 属性タイプを指定します。
ステップ 9	**exit**	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 10	**username** *name* **aaa attribute list** *name*	（任意）ユーザ ID に AAA 属性リストを指定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。

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用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**	特権 EXEC モードをイネーブルにします。 • 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**	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*	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*	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*	証明書に関連付けるキー ペアを指定します。

	コマンドまたはアクション	目的
		（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**	**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 7	**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**	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**	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。 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。 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。 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。 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。 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が示されます。「! RSA key pair associated with trustpoint is exportable.」 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。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**exit**	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 crypto pki certificate** *trustpoint name*	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**	特権 EXEC モードをイネーブルにします。 • 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**	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*	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*	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*	証明書に関連付けるキー ペアを指定します。
ステップ 6	**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 7	**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**	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	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**crypto pki enroll** *name*	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。 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。

	コマンドまたはアクション	目的
		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。 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。
ステップ 12	**crypto pki import** *name* **certificate**	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。 デバイスは、拡張子が「.req」から「.crt」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.crt」および「-encr.crt」が使用されます。 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。 （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。
ステップ 13	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 14	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。
ステップ 15	**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。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**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	**eap profile** *profile-name*	EAP プロファイルを設定し、EAP プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**method tls**	デバイスで EAP-TLS 方式を有効にします。
ステップ 5	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 6	**exit**	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 7	**dot1x credentials** *profile-name*	802.1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 8	**username** *username*	認証ユーザ ID を設定します。
ステップ 9	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MKA MACsec 設定の適用

EAP-TLS 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**	特権 EXEC モードをイネーブルにします。 • 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**	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*	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**	インターフェイス上で MACsec をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**authentication periodic**	このポートの再認証をイネーブルにします。
ステップ 6	**authentication timer reauthenticate interval**	再認証間隔を設定します。
ステップ 7	**access-session host-mode multi-domain**	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**	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**	ポートの認可状態を設定します。
ステップ 10	**dot1x pae both**	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプ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**	802.1x クレデンシャ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	**dot1x authenticator eap profile** *name*	EAP-TLS オーセンティケータ 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 13	**dot1x supplicant eap profile** *name*	EAP-TLS サプリカント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 14	**service-policy type control subscriber** *control-policy name*	インターフェイスに加入者制御ポリシーを適用します。
ステップ 15	**exit**	特権 EXEC モードに戻ります。
ステップ 16	**show macsec interface**	インターフェイスの MACsec の詳細を表示します。
ステップ 17	**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。

証明書ベース MACsec 暗号化の確認

証明書ベースの MACsec 暗号化の設定を確認するには、次の **show** コマンドを使用します。次に、 **show** コマンドの出力例を示します。

show mka sessions コマンドは、アクティブな MACsec Key Agreement（MKA）プロトコルのセッションの概要を表示します。

```
Device# show mka sessions

  Total MKA Sessions....... 1
```

```
      Secured Sessions... 1
      Pending Sessions... 0

==========================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server

Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN

==========================================================================================
Te0/1/3        74a2.e625.4413/0013 *DEFAULT POLICY* NO                YES

19             74a2.e625.4c22/0012 1                Secured
10000000000000000000000000000000000000000000000000000000000000000000
```

show macsec status interface *interface-id* は、指定されたインターフェイスの MACsec ステータス情報を表示します。

```
Device# show macsec status interface te0/1/2

  Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256
  Cipher:                   GCM-AES-128
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure

Transmit SC:
  SCI:                      74A2E6254C220012
  Transmitting:             TRUE
Transmit SA:
  Next PN:                  412
  Delay Protect AN/nextPN:  99/0

Receive SC:
  SCI:                      74A2E62544130013
  Receiving:                TRUE
Receive SA:
  Next PN:                  64
  AN:                       0
  Delay Protect AN/LPN:     0/0
```

show access-session interface *interface-id* **details** は、指定されたインターフェイスのアクセス セッションに関する詳細情報を表示します。

```
Device# show access-session interface te1/0/1 details

   Interface:  TenGigabitEthernet1/0/1
             IIF-ID:  0x17298FCD
         MAC Address:  f8a5.c592.13e4
        IPv6 Address:  Unknown
        IPv4 Address:  Unknown
           User-Name:  DOT1XCRED
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-host
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  000000000000000BB72E8AFA
     Acct Session ID:  Unknown
```

```
               Handle:  0xc3000001
       Current Policy:  MUSTS_1


Local Policies:
 Security Policy:  Must Secure
      Security Status:  Link Secured

Server Policies:


Method status list:
       Method           State
     dot1xSup           Authc Success
        dot1x           Authc Success
```

証明書ベース MACsec 暗号化の設定例

例:：証明書の登録

```
Configure Crypto PKI Trustpoint:
  crypto pki trustpoint POLESTAR-IOS-CA
   enrollment terminal
   subject-name CN=ASR1000x1@polestar.com, C=IN, ST=KA, OU=ENG,O=Polestar
   revocation-check none
   rsakeypair mkaioscarsa
   storage nvram:
  !
Manual Installation of Root CA certificate:
 crypto pki authenticate POLESTAR-IOS-CA
```

例：802.1x 認証の有効化と AAA の設定

```
aaa new-model
dot1x system-auth-control
radius server ISE
 address ipv4 <ISE ipv4 address> auth-port 1645 acct-port 1646
 automate-tester username dummy
 key dummy123
 radius-server deadtime 2
!
aaa group server radius ISEGRP
 server name ISE
!
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

例：EAP-TLS プロファイルと 802.1x クレデンシャルの設定

```
eap profile EAPTLS-PROF-IOSCA
 method tls
 pki-trustpoint POLESTAR-IOS-CA
!

dot1x credentials EAPTLSCRED-IOSCA
 username asr1000@polestar.company.com
 pki-trustpoint POLESTAR-IOS-CA
!
```

例：インターフェイスでの 802.1X、PKI、および MACsec の設定の適用

```
interface TenGigabitEthernet0/1
 macsec network-link
 authentication periodic
 authentication timer reauthenticate <reauthentication interval>
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae both
 dot1x credentials EAPTLSCRED-IOSCA
 dot1x supplicant eap profile EAPTLS-PROF-IOSCA
 service-policy type control subscriber DOT1X_POLICY_RADIUS
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	Cisco IOS Master Command List, All Releases

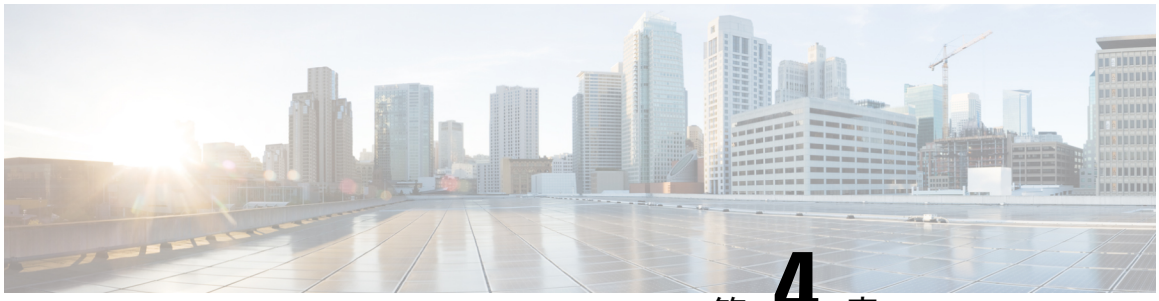
関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
IEEE 802.1AE-2006	*Media Access Control*（*MAC*）セキュリティ
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	*Media Access Control*（*MAC*）セキュリティ（IEEE 802.1AE-2006 の修正）：Extended Packet Numbering（XPN）
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（IEEE 802.1 x-2010 の修正）
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
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html



第 4 章

MACsec スマート ライセンス

MACsec スマートライセンスの概要

この章では、MACsec スマート ライセンスの概要を説明します。スマート ライセンス機能は、Cisco ソフトウェアを簡素化し、Cisco ソフトウェアがネットワーク全体でどのように使用されるかを理解するのに役立つ標準化されたライセンス プラットフォームです。Smart Licensing は、すべての Cisco ソフトウェア ライセンスの次世代プラットフォームです。MACsec ライセンスにより、Cisco ASR 1000 プラットフォームで CSL 永久ライセンスとスマート ライセンスを有効にすることが可能になります。

MACsec スマート ライセンスの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7: MACsec* スマート ライセンスの機能情報

機能名	リリース	機能情報
MACsec および DLC のサポート	Cisco IOS XE Fuji 16.9.1	Smart Licensing クライアントの機能は、Cisco ソフトウェアを簡素化し、Cisco ソフトウェアがネットワーク全体でどのように使用されるかを理解するのに役立つ標準化されたライセンス プラットフォームです。Smart Licensing は、すべての Cisco ソフトウェア ライセンスの次世代プラットフォームです。この機能によって導入または変更されたコマンドはありません。

MACsec スマート ライセンスに関する情報

Cisco IOS XE Fuji リリース 16.9.1 では、MACsec スマート ライセンス（SL）は次のプラットフォームでサポートされています。

ポート	ライセンス機能	ライセンス PID	サポートされるプラットフォーム		
			MIP-100（RP2/RP3）	ASR1001-HX	ASR1002-HX
内蔵 1 GE ポート	MACSEC1G	FLSA1-MACSEC1G	該当なし	対応	対応
内蔵 10 GE ポート	MACSEC10G	FLSA1-MACSEC10G	該当なし	対応	対応
EPA-18X1GE	MACSEC1G	FLSA1-MACSEC1G	対応	該当なし	対応
EPA-10X10GE	MACSEC10G	FLSA1-MACSEC10G	対応	該当なし	対応
EPA-1X40GE	MACSEC40G	FLSA1-MACSEC40G	対応	該当なし	対応
EPA-2X40GE	MACSEC40G	FLSA1-MACSEC40G	対応	該当なし	対応
EPA-QSFP-1X100GE	MACSEC100G	FLSA1-MACSEC100G	対応	該当なし	対応

MACsec ライセンスはポートごとに提供され、物理ポートにのみ適用されます（サブインターフェイスには追加のライセンスは必要ありません）。MACsec ポート ライセンスでは、デバイス リード変換（DLC）のサポートが提供され、ペーパー ライセンスがスマート アカウントに確実に追加されます。

デバイス リード変換により、デバイス上のライセンスについてクラシック ライセンスからスマート ライセンスへのライセンス移行が自動的に実行されます。スマート ライセンスへの変換が自動的に行われるようにするには、デバイスを Cisco Smart Software Manager（SSM）に登録する必要があります。

（注）
- 以前のリリースに従って、ASR1001 内蔵は MACsec ライセンスとして機能する IPsec ライセンスで引き続き使用できます。
- MACsec ライセンスは EPA-1X100GE および EPA-CPAK-2X40GE ではサポートされていません。
- CSL：EvalRTU ライセンスは MACsec ライセンスでは使用できません。

MACsec の設定を含むポートが閉じられていない場合、または閉じられていないポートに設定が適用されている場合は、MACsec ライセンスの 1 つのユニットが使用されます。

MACsec の設定を含むポートが閉じられた場合、または閉じられていないポートから設定が削除された場合は、MACsec ライセンスの 1 つのユニットがリリースされます。

導入と移行の例

Cisco IOS XE Fuji 16.9.1 以降では、MACsec のサポートは Cisco ソフトウェア ライセンス（CSL）モードおよびスマート ライセンス（SL）モードで提供されます。ただし、16.9.1 より後のリリースでは、MACsec はスマート ライセンスのみをサポートします。

次のシナリオでは、既存のルータを Cisco IOS XE Fuji 16.9.1 に展開、および移行する方法について説明します。

永久ライセンスがインストールされている場合の CSL モードでのアップグレード

アップグレードする前（Cisco IOS XE Fuji 16.9.1 リリースより前のリリース）に MACsec 永久ライセンスがデバイスにインストールされている場合は、アップグレード後にこれらのライセンスが使用されます。

- アップグレードの前は、次の状態であることを前提としています。
  - ルータは、Cisco IOS XE Fuji 16.9.1 より前のリリースで動作している
  - MACsec が、閉じられていない 4 つの 1G インターフェイスで設定されている
  - 4 つの MACSEC1G 永久ライセンスがインストールされている
- アップグレード後、4 つの MACSEC1G ライセンスが使用されます。

永久ライセンスがインストールされていない場合の CSL モードでのアップグレード

閉じられていないポートで MACsec が設定されている場合、アップグレード後に EvalRTU ライセンスを使用するのが理想的です。EvalRTU サポートが提供されないため、ライセンス要求はスキップされ、警告メッセージが表示されます。次に例を示します。

%IOSXE_LICENSE_POLICY_MANAGER-4-INSUF_PERM_LIC: 0/0/0: Insufficient MACSEC40G permanent license, skipping license request assuming customer has honour license

- アップグレードの前は、次の状態であることを前提としています。
  - ルータは、Cisco IOS XE Fuji 16.9.1 より前のリリースで動作している
  - MACsec は、4つの非シャットダウン1g インターフェイスで設定されます。
- アップグレード後
  - 使用できる MACsec ライセンスはありません
  - 警告メッセージが表示されます
  - その後、4 つの永久ライセンスを後でインストールすると、これらのライセンスは直ちに使用されます

SL モードへの移行

コンプライアンス違反シナリオを回避するには、すべての製品アクティベーションキー（PAK）および非 PAK ライセンスをお客様の仮想 CSSM アカウントに追加する必要があります。

デバイス リード変換（DLC）機能は、ライセンスをスマート アカウントに移行します。DLC が正常に動作するには、SL モードに移行する前に、すべてのライセンスを CSL モードで有効にする必要があります。

SL モードに移行するには、次の手順を実行します。

- Cisco IOS XE 16.9.1 より前のリリースから Cisco IOS XE 16.9.1 へのアップグレード
  1. CSL モードで Cisco IOS XE Fuji 16.9.1 へアップグレードします
  2. SL モードへ移行して DLC をトリガします
- Cisco IOS XE Fuji 16.9.1 以前のリリースから以降のリリースへのアップグレード
  1. CSL モードで Cisco IOS XE Fuji 16.9.1 へアップグレードします
  2. SL モードへ移行して DLC をトリガーします
  3. Cisco IOS XE Fuji 16.9.1 より後のリリースへアップグレードします