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ー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 暗号化を使用したポートチャネルの設定のサポート	Cisco IOS XE Gibraltar 17.2	この機能拡張により、MACsec 対応インターフェイスでポートチャネルを設定して、ポートチャネルトラフィックのシームレスなフローを実現できます。それにより、トラフィックが保護されます。

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 プロバイダー 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。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、高可用性クラスタでの MKA の設定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。
- 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。
- ポートチャネルを設定するには、リンクバンドルの各インターフェイスでMACsecを設定してください。
- 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。
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータについて、次の表に、GigabitEthernet インターフェイスと、インターフェイスごとにサポートされるピアの最大数を示します。

GigabitEthernet インターフェイス	インターフェイスごとのピア数	
1G	8	
10G	32	
40G	60	
100 G	120	

- `macsec dot1q-in-clear` が有効になっている場合、ネイティブ VLAN はサポートされません。

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 プロバイダー 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。

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 プロバイダー 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 サーバーは、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 サーバーは、キー サーバー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 サーバーでリストにキー サーバー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 サーバー内のデータ 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 プロバイダー 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 プロバイダーに送信される 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 プロバイダーは、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 プロバイダー 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ー 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。

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
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**）	ポートあたりのライン 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**）	ポートあたりのライン 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）	ポートあたりのライン レート（%）	ESP CPU（%）
64	51467063849.50	65.59	96
iMIX	105267526427	93.14	36
1418	100007152449	97.89	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
ISR43XX	該当なし	該当なし	該当なし	該当なし	Cisco IOS XE Release 3.16.0S
ISR4462	Cisco IOS XE Fuji リリース 16.9.1	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。

（注） IOS XE 17.2 Gibraltar 以降、ポートチャネル設定は MACsec でサポートされています。この機能を設定するには、リンクバンドルの各インターフェイスでMACsecを設定してください。詳細については、「設定例」を参照してください。

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 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： `Device(config-mka-policy)# key-server priority 200`	（任意）MKA キー サーバの優先度を設定します。
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。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-mka-policy)# end`	特権 EXEC モードに戻ります。 （注） MKA ポリシーは、XPN 暗号の機密性オフセットを処理しません。したがって、XPN および非 XPN 暗号の両方が機密性オフセットとともに MKA ポリシーで設定されている場合、機密性オフセットは XPN 暗号では無視されます。そのため、XPN または非XPN 暗号を使用して MKA ポリシーを設定する際は、慎重に判断してください。

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**
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** *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： `Device(config-if)# mka pre-shared-key key-chain key-chain-name`	MKA pre-shared-key key-chain に keychain1 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** 例： `Device(config-if)# macsec`	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。

	コマンドまたはアクション	目的
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** *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：	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。

	コマンドまたはアクション	目的
	`Device(config-keychain)# key 9ABCD`	（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`	キー文字列のライフタイムを設定します。 期間に指定できる範囲は、1 ～ 864000 秒です。
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 12345678901234567890123456789013
   lifetime local 12:21:00 Sep 9 2015 infinite
```

Configuration with CKN key-string behavior change:

```
config t
  key chain abc macsec
   key 11000000000000000000000000000000000000000000000000000000000000000000
   cryptographic-algorithm aes-128-cmac
   key-string 12345678901234567890123456789013
   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： `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** *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。

	コマンドまたはアクション	目的
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 モードを有効にします。 • 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	**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 123456789012345678901234567890123456
  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 123456789012345678901234567890123456
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 123456789012345678901234567890123456
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 123456789012345678901234567890123456
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、キーサーバーになることができます。確定的にキーサーバーに選択されるように、キーサーバー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、キーサーバー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
```

例：MACsec を使用したポートチャネルの設定

次に、リンクバンドルの2つの個別インターフェイスでMACsecを使用してポートチャネルを設定する設定例を示します。

（注） ポートチャネルの MACsec 設定を有効にしたり削除する前に、すべてのインターフェイスがシャットダウンされていることを確認してください。

```
key chain kc1 macsec
  key 01
  key-string 12345678901234567890123456789012
  cryptographic-algorithm aes-128-cmac

key chain kc2 macsec
  key 02
  key-string 12345678901234567890123456789013
  cryptographic-algorithm aes-128-cmac

mka policy policy1
  macsec-cipher-suite gcm-aes-256

!Port-Channel Configuration

 interface Port-channel2
  mtu 9216
  ip mtu 9184
  ip address 10.3.1.3 255.255.255.0
  load-interval 30
  bfd interval 750 min_rx 750 multiplier 5
  lacp min-bundle 2
  no shut
  exit

!Member link configuration 1

 interface TenGigabitEthernet0/1/1
  no shut
  mtu 9216
  no ip address
  ip mtu 9184
  load-interval 30
  cdp enable
  no cdp tlv app
  mka policy policy1
  mka pre-shared-key key-chain kc1
  macsec
  lacp rate fast
  channel-group 2 mode active

!Member link configuration 2

  interface TenGigabitEthernet0/1/2
  no shut
  mtu 9216
  no ip address
  ip mtu 9184
  load-interval 30
```

```
cdp enable
no cdp tlv app
mka policy policy1
mka pre-shared-key key-chain kc2
macsec
lacp rate fast
channel-group 2 mode active
```

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
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
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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。