MACsec を構成します

この章では、Cisco NX-OS デバイスで MACsec を構成する方法について説明します。

MACsec について

Media Access Control Security（MACsec）である IEEE 802.1AE と MACsec Key Agreement（MKA）プロトコルは、イーサネットリンク上でセキュアな通信を提供します。次の機能があります。

- ライン レート暗号化機能を提供します。
- レイヤ 2 で強力な暗号化を提供することで、データの機密性を確保します。
- 整合性チェックを行い、転送中にデータを変更できないことを保証します。

- 中央集中型ポリシーを使用して選択的に有効にでき、MACsec 非対応コンポーネントがネットワークにアクセスできるようにしながら、必要に応じて適用することができます。
- レイヤ 2 ではホップバイホップ ベースでパケットを暗号化します。これにより、ネットワークは、既存のポリシーに従って、トラフィックを検査、モニタ、マーク、転送できます（エンドツーエンド レイヤ 3 暗号化技術とは異なり、パケットの内容をネットワークデバイスから非表示にします）

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では、キーがいつ有効になり、いつ期限切れになるかが指定されます。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て、ライフタイムの期限が切れると、MKA はキー チェーン内で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。デフォルトの時間帯は UTC です。

MACsec キーチェーンを設定するには、MACsec キーチェーンとキーの設定 （11 ページ）を参照してください。

（キーチェーン内で）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、そのキーチェーン内の 2 番目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た場合、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。

フォールバック キー

MACsec セッションは、キー/キー名（CKN）のミスマッチで、またはスイッチとピア間のキーの期限が切れて、失敗する可能性があります。MACsec セッションが失敗した場合、フォールバック キーが設定されていれば、フォールバック セッションが引き継ぐことができます。フォールバック セッションは、プライマリ セッションの障害によるダウンタイムを防止し、ユーザが障害の原因となっている主要な問題を修正できるようにします。フォールバック キーは、プライマリ セッションの開始に失敗した場合のバックアップ セッションも提供します。この機能はオプションです。

MACsec フォールバックキーを設定するには、MACsec フォールバック キーの設定 （14 ページ）を参照してください。

MACsec のライセンス要件

製品	ライセンス要件
Cisco NX-OS	MACsec にはセキュリティ ライセンスが必要です。Cisco NX-OS ライセンス方式の詳 スの取得および適用の方法については、Cisco NX-OS ライセンス ガイドを参照してく

MACSec の注意事項と制約事項

MACsec に関する注意事項と制約事項は次のとおりです。

- MACsec は、次のインターフェイス タイプでサポートされます。
  - レイヤ 2 スイッチポート（アクセスとトランク）
  - レイヤ 3 ルーテッド インターフェイス（サブインターフェイスなし）

（注） レイヤ 3 ルーテッド インターフェイスで MACsec を有効にすると、そのインターフェイスで定義されているすべてのサブインターフェイスでも暗号化が有効になります。ただし、同じレイヤ 3 ルーテッド インターフェイスのサブインターフェイスのサブセットで MACsec を選択的に有効にすることはサポートされていません。

  - レイヤ 2 およびレイヤ 3 ポート チャネル（サブインターフェイスなし）

- Cisco Nexusリリース10.2（1）F以降では、Cisco Nexus 9000 ToRスイッチのMACSecセキュリティタグ（SecTAG）からセキュアチャネル識別子（SCI）を無効にできます。
  - FX2 および FX3 プラットフォームでサポートされています。
  - XPN暗号スイートを使用するFXプラットフォームでのみサポートされます。
- Cisco Nexus ToR スイッチを Cisco NX-OS リリース 9.3.7 から Cisco NX-OS リリース 9.3.6 以前のリリースにダウングレードする場合、MACsec はサポートされません。
- MKA は、MACsec でサポートされている唯一のキー交換プロトコルです。Security Association Protocol（SAP）はサポートされていません。
- リンクレベルフロー制御（LLFC）およびプライオリティ フロー制御（PFC）は、MACsec ではサポートされません。
- 同じインターフェイスに対する複数の MACsec ピア（異なる SCI 値）はサポートされません。

- **macsec shutdown** コマンドを使用して MACsec を無効にすると、MACsec 設定を保持できます。
- MACsec セッションは、最新の Rx および最新の Tx フラグが Tx SA のインストール後に最初に廃止されたキーサーバからのパケットを受け入れるのに寛容です。MACsec セッションは、セキュアな状態に収束します。
- Cisco NX-OS リリース 9.2(1) 以降では、次の設定が可能です。
  - ポリシーがインターフェイスによって参照されている間に、MACSec ポリシーを変更できるようにします。
  - ブレークアウト ポートの異なるレーン間で異なる MACsec ポリシーを許可します。
- Cisco Nexus リリース 9.2(1) 以降、MACsec は Cisco Nexus 93180YC-FX スイッチでサポートされます。
- Cisco Nexus リリース 9.3(1) 以降、MACsec は Cisco Nexus 9348GC-FXP スイッチでサポートされます。これらのスイッチで MACsec を使用する場合は、次の制限が適用されます。
  - Cisco Nexus 9348GC-FXP：MACsec は 6 ポート（ポート 49 ～ 54）でサポートされます。
- Cisco Nexus リリース 9.3(1) 以降では、ポートチャネル インターフェイスに MACsec 設定を直接適用することはできません。ただし、MACsec 設定をポートチャネル メンバー ポートに直接適用できます。これは、NX-OS と vPC ポートチャネルの両方に適用されます。
- Cisco Nexus リリース 9.3(3) 以降、MACsec は Cisco Nexus 93216TC-FX2、Cisco Nexus 93360YC-FX2 でサポートされています。
- Cisco NX-OS リリース 9.3(5) 以降、MACsec は次のスイッチおよびライン カードでサポートされます。
  - Cisco Nexus 93180YC-FX3S スイッチ：MACsec はすべてのポートでサポートされます。
  - Cisco Nexus X9732C-FX および X9788TC-FX ライン カード
- Cisco Nexus 9300-FX スイッチおよび 9700-FX ライン カード
  - MACsec は 1G ポートではサポートされていません。
  - さらに、 MAC ブロックに 1G ポートが含まれている場合、 MACsec はその MAC ブロック内のポートではサポートされません。
  - MACsec 対応の 9700-FX ライン カードで 1G 光ファイバを使用する場合は、診断モードを「最小」に変更することを推奨します。診断の詳細については、『**Cisco Nexus 9000 シリーズ NX-OS システム管理コンフィギュレーション ガイド**』の「起動時の診断」のセクションを参照してください。
- Cisco Nexus 9300-FX2 スイッチの場合：

- MACsecは、1Gポートでサポートされます（ポートが非BVまたは非リタイマー ポートである場合）。

  リタイマー ポートの詳細については、『**Cisco Nexus 9000 シリーズ NX-OS インターフェイス構成ガイド**』の 「サポートされているリタイマー ポート」 セクションを参照してください。

- Cisco NX-OS リリース 10.1(1) 以降、Cisco Nexus 93180YC-FX3 および 93108TC-FX3P スイッチは、1Gおよび10Gポート速度を含むすべてのポート速度でMACsecをサポートします。
- MACsec は、Cisco Nexus 93240YC-FX2、9336C-FX2、93108TC-FX、93180YC-FX スイッチ、および X9736C-FX および X9732C-EXM ライン カードでサポートされています。
- 1G は BV ポートまたはリタイマー ポートではサポートされません。リタイマー ポートの詳細については、『**Cisco Nexus 9000 シリーズ NX-OS インターフェイス構成ガイド**』の「サポートされているリタイマー ポート」セクションを参照してください。
- Cisco NX-OS リリース 9.3(7) 以降、QSA が使用されている場合、MACsec は Cisco Nexus 9336C-FX2 スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(1) 以降、QSA が使用されている場合、MACsec は Cisco Nexus 9336C-FX2、9336C-FX2-E スイッチでサポートされます。
- Cisco NX-OS リリース 10.1(2) 以降では、QSA が使用されている場合、MACsec は Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。
- Cisco Nexus リリース 10.1(1) 以降、MACsec は Cisco Nexus 9336C-FX2-E でサポートされます。
- Cisco Nexus リリース 10.2(1)F 以降、MACsec は Cisco Nexus X9716D-GX でサポートされます。
- Cisco NX-OS リリース 10.2(1q)F 以降、MACsec は Cisco Nexus 9332D-GX2B スイッチのポート 25 ～ 32 でサポートされます。
- Cisco NX-OS リリース 10.2(2)F 以降、MACsec は Cisco Nexus N9K-C9348D-GX2A スイッチの 1 ～ 48 ポートでサポートされます。
- Cisco NX-OS リリース 10.2(2)F 以降、MACsec は 10G QSA リンクを備えた Cisco Nexus X9736C-FX、および X9736Q-FX ラインカードをサポートします。
- Cisco NX-OS リリース 10.2(2)F 以降、MACsec は Cisco Nexus 9364D-GX2A スイッチのポート 1 ～ 16 でサポートされます。
- Cisco Nexus 9332D-GX2B、9364D-GX2A および 9348D-GX2A スイッチ と Cisco Nexus X9836DM-A ライン カードでは、ポートで MACsec が設定されていても設定されていなくても、MACsec セキュリティ ポリシー タイプに関係なくポートフラップが発生します。
- Cisco NX-OS リリース 10.3(1)F 以降、MACsec は Cisco Nexus 9800 プラットフォーム スイッチの Cisco Nexus X9836DM-A ライン カードでサポートされます。

- Cisco NX-OS リリース 10.3(2)F 以降、MACsec は、LEM モジュール X9400-16W および X9400-8D を搭載した Cisco Nexus 9408 スイッチのサポートされているすべてのリンクでサポートされます。
- Cisco Nexus リリース 10.3(3)F 以降、暗号キーの適用機能には、Cisco Nexus 9332D-GX2B、9336C-FX2、93180YC-FX、および 93180YC-FX3 スイッチで、最も優先される暗号スイートから最も優先されない暗号スイートまでを定義するオプションを提供します。ただし、以下の制限があります。
  - 暗号キーの適用機能は、キーサーバとして優先順位が付けられている場合にのみ効果的に機能します。それ以外の場合は、**init** または **pending** 状態のセッションになります。
  - 暗号キーの適用機能は、2つのピア間の直接接続でのみサポートされます。MKA セッションが複数のピアとの間で行われている場合、この機能は正常に動作しません。
  - ピア暗号スイート許可の変更中、最も優先されるサポートされている暗号スイートでセッションが保護されない場合があります。
  - 任意のセキュリティで保護された MACsec セッションで使用されるポリシーで暗号を any から強制ピア暗号に変更する場合は、期待される動作が実現されるよう、暗号を変更した後にポートをフラップすることをお勧めします。フラッピングが行われない場合、セッションはスイッチ上保護されていると表示されますが、ピアセッションではサポートされていない暗号で保留中と表示されます。また、サポートされている暗号が強制ピア暗号スイートに存在する場合でも、セッションがすぐに保護されない可能性があります。
  - 許可されたピア暗号スイート（APSC）を空にすることはできません。また、重複させることはできません。
  - cipher-suite コマンドと cipher-suite enforce-peer コマンドは、同じポリシーの下で共存できません。
  - SAK 暗号適用タイマーがタイムアウトして次の暗号スイートを試行するのを待機している間、データおよび制御トラフィックでは、セキュアモードであっても、一方向のトラフィックの中断が発生する可能性があります。中断は、セッションが保護された場合にのみ回復します。
- Cisco Nexus リリース 10.4(1)F 以降、MACsec はCisco Nexus 9348GC-FX3 および 9348GC-FX3PH スイッチのポート 49 ～ 54 でサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、MACsec は Cisco Nexus 9332D-H2R プラットフォームスイッチのすべての前面パネルポート（ポート1～32）でサポートされます。ただし、MACsec は Ethernet1/33 および Ethernet1/34 ではサポートされません。
- Cisco Nexus リリース 10.4(2)F 以降、MACsec は以下のスイッチでサポートされます。
  - Cisco Nexus 93400LD-H1 のすべてのポート。
  - Cisco Nexus 93108TC-FX3 のポート 49 ～ 54

- Cisco Nexus リリース 10.4(3)F 以降、MACsec は Cisco Nexus 9364C-H1 スイッチのポート 49 ～ 64 でサポートされます。
- MACsec は、Nexus 9600-R/R2 ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチではサポートされません。
- MACsec 機能が設定されている場合、無停止 ISSU はサポートされません。

キーチェーンの制限：

- MACsec キーのオクテット文字列は上書きできません。代わりに、新しいキーまたは新しいキーチェーンを作成する必要があります。
- **end** または **exit** を入力すると、キーチェーンの新しいキーが設定されます。エディタ モードのデフォルトのタイムアウト値は 6 秒です。キーがキー オクテット文字列または 6 秒間の送信ライフタイムで設定されていない場合、MACsec セッションを起動するために不完全な情報が使用され、セッションが承認保留状態のままになる可能性があります。設定の完了後に MACsec セッションがコンバージされない場合は、ポートをシャットダウン/非シャットダウンすることをお勧めします。
- 指定したキーチェーンでは、キーの有効期間を重複させて、有効なキーの不在期間を避ける必要があります。キーがアクティブ化されない期間が発生すると、セッション ネゴシエーションが失敗し、トラフィックがドロップされる可能性があります。MACsec キー ロールオーバーでは、現在アクティブなキーの中で最も遅い開始時刻のキーが優先されます。
- セキュリティ アドオン ライセンスを使用するためには、MACsec 機能を有効にすることに加えて、少なくとも 1 つのインターフェイスで MACsec キーチェーンを設定する必要があります。

フォールバックの制限：

- MACsecセッションが古いプライマリキーで保護されている場合、最新のアクティブなプライマリ キーが一致しない場合、フォールバック セッションには進みません。そのため、セッションは古いプライマリ キーで保護されたままになり、ステータスが古い CA のキー再生成として表示されます。プライマリ PSK の新しいキーの MACsec セッションは init 状態になります。
- フォールバック キーチェーンでは、無期限のキーを 1 つだけ使用します。複数のキーはサポートされていません。
- フォールバック キー チェーンで使用されるキー ID（CKN）は、プライマリ キー チェーンで使用されるキー ID（CKN）のいずれとも一致しないようにしてください。
- 一度設定すると、インターフェイスのすべての MACsec 設定が削除されない限り、インターフェイスのフォールバック設定は削除できません。

MACsec ポリシーの制限：

- MACsec セッションがセキュアになる前に、BPDU パケットを送信できます。

レイヤ 2 トンネリング プロトコル（L2TP）の制約事項：

- MACsec は、dot1q トンネリング（スイッチポート モード dot1q-tunnel）または L2TP 用に設定されたポートではサポートされません。
- 非ネイティブ VLAN のトランク ポートで STP が有効になっている場合、L2TP は機能しません。

統計情報の制限：

- MACsec モードと非 MACsec モード（通常のポート シャットダウン/非シャットダウン）の間の移行中に発生する CRC エラーはほとんどありません。
- Secy 統計情報は累積され、30 秒ごとにポーリングされます。
- IEEE8021-SECY-MIB OID secyRxSAStatsOKPkts、secyTxSAStatsProtectedPkts、および secyTxSAStatsEncryptedPkts は最大 32 ビットのカウンタ値しか伝送できませんが、トラフィックは 32 ビットを超える可能性があります。
- Cisco Nexus 9300-FX3 プラットフォーム スイッチでは、**show macsec secy statistics** コマンドは、レート統計情報と、Cisco NX-OS リリース 10.4(2)F 以降のレート関連の「CISCO-SECY-EXT-MIB」OID をサポートします。
  - cseSecyIfRxUncontrolledPktRate、
  - cseSecyIfRxControlledPktRate、
  - cseSecyIfTxUncontrolledPktRate、
  - cseSecyIfTxControlledPktRate
  - cseSecyIfRxControlledOctetRate
  - cseSecyIfTxControlledOctetRate
  - cseSecyIfRxUnControlledOctetRate
  - cseSecyIfTxUnControlledOctetRate

相互運用性の制限：

- N9K-X9732C-EXM と他のピア スイッチ（他のシスコおよびシスコ以外のスイッチ）の相互運用性は、XPN 暗号スイートでのみサポートされます。
- MACsec ピアは、AES_128_CMAC 暗号化アルゴリズムを使用するために同じ Cisco NX-OS リリースを実行する必要があります。以前のリリースと Cisco NX-OS リリース 9.2(1) の間の相互運用性のために、AES_256_CMAC 暗号化アルゴリズムでキーを使用する必要があります。
- 以前のリリースと Cisco NX-OS リリース 9.2(1) の間の相互運用性を確保するために、MACsec キーが 32 オクテット未満の場合は、MACsec キーにゼロを付加します。
- Cisco NX-OS スイッチでは、すべてのインターフェイスで代替 MAC アドレスとイーサネット タイプの一意の組み合わせを 1 つだけ設定できます。

- Cisco NX-OS リリース 9.3(1) から、ポートチャネル メンバーごとの MACsec 設定サポートのない Cisco NX-OS リリースにダウングレードしようとした場合、スイッチの同じポートチャネル インターフェイスのメンバーに、相互に異なる MACsec 設定があった場合、次のエラー メッセージが表示されることがあります。

```
ポートチャネル メンバーに非対称 macsec 設定が存在します。メンバー間で対称 macsec 設定を使用して、中断のない ISSU を実行してください。
```

- MACsec のソフトウェア サポートは、Cisco Nexus X9400-22L LEM カードでは使用できません。

EAPOL には、次の注意事項と制約事項があります。

- 転送エンジンの同じスライス内では、EAPOL ethertype と dot1q ethertype に同じ値を指定することはできません。
- EAPOL 設定を有効にするには、0 ー 0x599 の範囲のイーサネット タイプの範囲が無効です。
- EAPOL 設定を有効にする場合、N9K-X9836DM-A ラインカードでサポートされる EAPOL mac アドレスは、0x0180c2000000 ～ 0x0180c20000ff の範囲のみです。
- EAPOL パケットの設定中は、次の組み合わせを使用しないでください。
  - MAC アドレス 0100.0ccd.cdd0 と ethertype
  - MAC アドレスと ethertype：0xfff0、0x800、0x86dd
  - デフォルトの宛先 MAC アドレス0180.c200.0003 とデフォルトのイーサネット タイプ 0x888e
  - 両方の MACsec ピアで異なる EAPOL DMAC アドレス。MACsec セッションは、MACsec ピアがローカルに設定された DMAC を使用して MKAPDU を送信している場合にのみ機能します。
- Cisco NX-OS リリース 10.2(1)F 以降、EAPOL は Cisco Nexus 9300-FX3 シリーズ スイッチでサポートされます。

Cisco Nexus 9336C-SE1 スイッチ上の MACsec のガイドラインと制限事項

Cisco Nexus 9336C-SE1 スイッチでMACsec機能を使用する場合は、次のガイドラインと制限事項を確認してください。

Supported Features

- Cisco Nexus リリース 10.6（1）F 以降、Cisco Nexus 9336C-SE1 スイッチは、40G/100G ポートで MACsec 機能をサポートします。
- スイッチの 36 個のポートはすべてインターフェイスブレークアウトをサポートしており、MACsec 用に個別に構成できます。

制限事項

- Macsec SecY 統計情報は、出力セキュア アソシエーション（SA）カウンタに関連する統計情報をサポートしていません。出力統計データは常にゼロとして表示されます。

EAPOL 構成要件

- EAPOL 構成では、次の要件が満たされていることを確認します。
  - EAPOL MAC アドレスの範囲は 0180.C200.0000 ～ 0180.C200.00FF（最後のバイトは 0x00 ～ 0xFF）、EtherType は 0x600 ～ 0xFFFF の任意の値にできます。
  - EtherType がデフォルト値の 0x888E に設定されている場合、任意のMAC アドレスが許可されます。
  - ブロードキャスト MAC アドレスは、 0x600 ～ 0xFFFF の範囲内の任意の EtherType 値で使用できます。

MACsec の有効化

MACsec および MKA コマンドにアクセスする前に、MACsec 機能を有効にする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**feature macsec** 例： `switch(config)# feature macsec`	デバイスで MACsec および MKA を有効にします。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec の無効化

Cisco NX-OS リリース 9.2(1) 以降では、MACsec 機能を無効にしても、この機能が非アクティブ化されるだけで、関連する MACsec 設定は削除されません。

MACsec の無効化には、次の条件があります。

- MACsec shutdown はグローバルコマンドであり、インターフェイス レベルでは使用できません。
- macsec shutdown、show macsec mka session/summary、show macsec mka session detail、およびshow macsec mka/secy statistics コマンドは、「Macsec is shutdown」メッセージを表示します。ただし、show macsec policy および show key chain コマンドは出力を表示します。
- 連続する MACsec ステータスが macsec shutdown から no macsec shutdown に変更された場合、またはその逆の場合は、ステータス変更の間に 30 秒の間隔が必要です。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**macsec shutdown** 例： `switch(config)# macsec shutdown`	デバイスの MACsec 設定を無効にします。**no** オプションは、MACsec 機能を復元します。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。この手順は、スイッチのリロード後に MACsec をシャットダウン状態に維持する場合にのみ必要です。

MACsec キーチェーンとキーの設定

デバイスに MACsec キーチェーンとキーを作成できます。

（注） MACsec キーチェーンのみが MKA セッションをコンバージします。

始める前に

MACsec が有効であることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	（任意）[**no**] **key-chain macsec-psk no-show** 例： `switch(config)# key-chain macsec-psk no-show`	**show running-config** および **show startup-config** コマンドの出力で、暗号化されたキーオクテット文字列をワイルドカード文字に置き換えて非表示にします。デフォルトでは、PSK キーは暗号化形式で表示され、簡単に復号化できます。このコマンドは、MACsec キーチェーンにのみ適用されます。 （注） キーオクテット文字列は、設定をファイルに保存するときに非表示になります（アステリスクに変更）。その結果、このコマンドを設定して ASCII リロードまたは設定置換を実行すると、「key-octet-string」設定は保持されません。

ステップ 3	**key chain** *name* **macsec**
	例：
	`switch(config)# key chain 1 macsec`
	`switch(config-macseckeychain)#`
		MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。

ステップ 4	**key** *key-id*
	例：
	`switch(config-macseckeychain)# key 1000`
	`switch(config-macseckeychain-macseckey)#`
		MACsec キーを作成し、MACsec キー設定モードを開始します。範囲は 1ー32 オクテットで、最大サイズは 64 です。
		（注）
		キーの文字数は偶数でなければなりません。

ステップ 5	**key-octet-string** *octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**}	そのキーのオクテット ストリングを設定します。*octet-string* 引数には、最大 64 文字の 16 進数文字を含めることがで

	コマンドまたはアクション	目的
	例： `switch(config-macseckeychain-macseckey)# key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC`	きます。オクテット キーは内部でエンコードされるため、**show running-config macsec** コマンドの出力にクリア テキストのキーが現れることはありません。 キーオクテット文字列には、次のものが含まれます。 • 0 暗号化タイプ - 暗号化なし（デフォルト） • 6 暗号化タイプ - 独自仕様（タイプ 6 暗号化）。詳細については、MACsec キーでのタイプ 6 暗号化の有効化を参照してください。 • 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キー オクテット文列 （注） AES_128_CMAC 暗号化アルゴリズムを使用するためには、MACsec ピアは同じ Cisco NX-OS リリースを実行する必要があります。以前のリリースと、Cisco NX-OS リリース 7.0(3)I7(2) 以降のリリース間で相互運用できるようにするには、キーを AES_256_CMAC 暗号化アルゴリズムで使用する必要があります。
ステップ 6	**send-lifetime** 開始時間 **duration** 長さ 例： `switch(config-macseckeychain-macseckey)# send-lifetime 00:00:00 Oct 04 2016 duration 100000`	キーの送信ライフタイムを設定します。デフォルトでは、デバイスは開始時間を UTC として扱います。 *start-time* 引数は、キーがアクティブになる日時です。*duration* 引数はライフタイムの長さ（秒）です。最大値は 2147483646 秒（約 68 年）です。
ステップ 7	（任意） **show key chain** *name* 例： `switch(config-macseckeychain-macseckey)# show key chain 1`	キーチェーンの設定を表示します。

	コマンドまたはアクション	目的
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config-macseckeychain-macseckey)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec パケット番号の消耗

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 消耗後（2^{32}- 1 の 75% に達した後）、SAK リキーは自動的に行われ、データ プレーン キーを更新し、PN を周囲に配置します。

たとえば、64 バイトの 10G フル ライン レートでは、PN の枯渇により 216 秒ごとに SAK キー再生成が発生します。

これは、GCM-AES-PN-128 または GCM-AES-PN-256 暗号スイートを使用する場合に適用されます。

GCM-AES-XPN-128 または GCM-AES-XPN-256 暗号スイートが使用されている場合、SAK キー再生成は 2^{64}- 1 の 75% に達すると自動的に行われます（パケットの番号付けを消耗するのに数年かかります）。暗号スイートは macsec ポリシーで設定可能で、動作する暗号スイートはキー サーバ デバイスによって決定されます。

N9K-X9732C-EXM ライン カードで XPN 暗号スイートを使用することを推奨します。

MACsec フォールバック キーの設定

Cisco NX-OS リリース 9.2(1) 以降では、プライマリ セッションがスイッチとピア間のキー/キー名（CKN）のミスマッチまたはキーの有効期限の結果として失敗した場合にバックアップ セッションを開始するようにデバイスのフォールバック キーを設定できます。

始める前に

MACsec が有効になっており、プライマリおよびフォールバック キーチェーンとキー ID が設定されていることを確認します。「MACsec キーチェーンとキーの設定」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**interface** *name*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。

ステップ 3	**macsec keychain** *keychain-name* **policy** *policy-name* **fallback-keychain** *keychain-name* 例： `switch(config-if)# macsec keychain kc2 policy abc fallback-keychain fb_kc2`	キー/キー ID のミスマッチまたはキーの期限切れによる MACsec セッションの失敗後に使用するフォールバック キーチェーンを指定します。フォールバック キー ID は、プライマリ キーチェーンのキー ID と一致してはなりません。 フォールバック キーチェーン名を変更して同じコマンドを再発行することで、MACsec 設定を削除せずに、各インターフェイスのフォールバック キーチェーン設定を対応するインターフェイスで変更できます。 （注） コマンドは、フォールバック キーチェーン名を除き、インターフェイスの既存のコンフィギュレーション コマンドとまったく同じように入力する必要があります。 「MACsec キーチェーンとキーの設定」を参照してください。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec ポリシーの設定

異なるパラメータを使用して複数の MACSec ポリシーを作成できます。しかし、1 つのインターフェイスでアクティブにできるポリシーは 1 つのみです。

始める前に

MACsec が有効であることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**macsec policy** *name*
	例：
	`switch(config)# macsec policy abc`
	`switch(config-macsec-policy)#`
		MACsec ポリシーを作成します。

ステップ 3	（任意） **[no] cipher-suite** { { **enforce-peer** <*allowed-peer-cipher-suite1*> [*allowed-peer-cipher-suite2*> [*allowed-peer-cipher-suite3*> [*allowed-peer-cipher-suite4*>]]] } | **<suite>**} 例： `switch(config-macsec-policy)# cipher-suite enforce-peer GCM-AES-XPN-256 GCM-AES-XPN-128`	次の暗号スイートの順序を、最も優先度の高いものから最も低いものへと構成します。セッションは、ピアでサポートされている最も優先される暗号スイート（GCM-AES-128、GCM-AES-256、GCM-AES-XPN-128、または GCM-AES-XPN-256）で保護されます。 構成を解除するには、**no** フォームを使用するか、必要な順序設定で既存の順序を上書きします。 （注） • この機能を動作させるには、Cisco NX-OS スイッチがキー サーバーとして設定されていることを確認します。 • **cipher-suite enforce-peer** コマンドで定義された暗号スイートのセットに含まれていない暗号スイートをピアがサポートしている場合、MKA セッション状態は保護されず、保留状態になります。

	コマンドまたはアクション	目的
ステップ 4	（任意） **[no] include-sci** 例： `switch(config-macsec-policy)# no include-sci`	SecTAG の SCI を無効にします。デフォルトでは、SCI は常に有効になっています。 （注） パケットのドロップを防ぐには、SCI タギング設定が入力ポイントと出力ポイントの両方で一貫していることを確認します。
ステップ 5	（任意） **no protocol lldp encrypted** 例： `switch(config-macsec-policy)# no protocol lldp encrypted`	must-secure ポリシーが設定されたポートの MACsec 構成がセキュアでない場合でも、LLDP パケットを許可します。Cisco NX-OS リリース 10.5(3)F より前では、must-secure ポリシーを備えたポートの MACsec 構成がセキュアな状態でない場合、LLDP パケットはドロップされていました。 （注） このコマンドは、Cisco Nexus 9300-GX2、H2R、H1 シリーズ スイッチのみでサポートされます。
ステップ 6	（任意） **key-server-priority** *number* 例： `switch(config-macsec-policy)# key-server-priority 0`	キー交換中はピア間の接続が解除されるように、キー サーバのプライオリティを設定します。範囲は0（最高）ー255（最低）で、デフォルト値は 16 です。
ステップ 7	（任意） **security-policy** *name* 例： `switch(config-macsec-policy)# security-policy should-secure`	次のいずれかのセキュリティ ポリシーを設定して、データおよび制御パケットの処理を定義します。 • **must-secure**：MACsec をヘッダー持たないパケットはドロップされます。 • **should-secure**：MACsec ヘッダーを持たないパケットも許可されます。これはデフォルト値です。
ステップ 8	（任意） **window-size** *number* 例：	インターフェイスが、設定されたウィンドウサイズ未満のパケットを受け入れないように、再生保護ウィンドウを

	コマンドまたはアクション	目的
	`switch(config-macsec-policy)# window-size 512`	設定します。範囲は 0 ～ 596000000 です。
ステップ 9	（任意） **sak-expiry-time** *time* 例： `switch(config-macsec-policy)# sak-expiry-time 100`	SAK キー再生成を強制する時間を秒単位で設定します。このコマンドを使用して、セッションキーを予測可能な時間間隔に変更できます。デフォルトは 0 です。 （注） 10.5(3)F リリースより前は、SAK の有効期限の最小時間は 60 秒でした。10.5(3)F リリース以降、最小時間 30 秒がサポートされています。
ステップ 10	（任意） **conf-offset** *name* 例： `switch(config-macsec-policy)# conf-offset CONF-OFFSET-0`	暗号化を開始するレイヤ 2 フレームの機密性オフセットの 1 つとして、CONF-OFFSET-0、CONF-OFFSET-30、またはCONF-OFFSET-50 のいずれかを設定します。このコマンドは、中間スイッチがパケット ヘッダー {dmac、smac、etype} を MPLS タグのように使用するために必要です。
ステップ 11	（任意） **show macsec policy** 例： `switch(config-macsec-policy)# show macsec policy`	MACSec ポリシー設定を表示します。
ステップ 12	（任意） **copy running-config startup-config** 例： `switch(config-macsec-policy)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MACsec EAP の構成

Cisco NX-OS リリース 10.4(1)F 以降では、802.1X 認証に MACsec EAP プロファイルを使用できます。

始める前に

- Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

- MACsec コマンドを設定し、should-secure（デフォルト）または must-secure macsec ポリシーを指定します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 1/30`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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。

ステップ 3	**[no] macsec eap policy** *policy name*
	例：
	`switch(config-if)# macsec eap policy P1`
	`switch(config-eap-profile)#`
		MACsec eap プロファイルを作成します。
		コマンドの **no** フォームは、MACsec eap プロファイルを無効にするために使用されます。

ステップ 4	**[no] dot1x supplicant eap profile** *eap profile name* } 例： `switch(config-if)# dot1x supplicant eap profile`	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。 サプリカントが使用する eap プロファイルを設定します。

QKD と MACsec での SKIP の統合

量子安全暗号化について

量子コンピューティングの最近の進歩により、さまざまな暗号化アルゴリズムの脆弱性が明らかになっており、将来のアプリケーションでの安全性は保証されていません。計算の複雑さに依存する RSA（素因数分解）および DHE（離散対数）公開鍵アルゴリズムには、現在、Shor または Grover のアルゴリズムを使用する量子コンピュータによって解決されるリスクがあります。

その結果、通信する当事者間で共有秘密キーを確立することが、重要な課題になっています。この問題を回避するには、量子安全アルゴリズムを構成するか、量子キー配布（QKD）を実装します。

QKD と Secure Key Integration Protocol の統合について

Secure Key Integration Protocol（SKIP）プロトコルをスイッチに統合すると、外部量子デバイスとの通信を確立できます。この機能強化により、スイッチ間でMACsec暗号キーを交換する際に Quantum Key Distribution（QKD）デバイスを使用できるようになります。

QKD は量子物理学の原理に基づいて動作し、光子の量子状態を利用して光リンク経由で情報をエンコードおよび共有します。さらに、認証された従来のチャネルが、測定値の共有に使用されます。量子状態の変化は、通信チャネルの2つのエンドパーティがキーの傍受を検出するのに役立ちます。

QKDは、暗号解読や量子コンピューティングが将来的に進歩しても、量子攻撃に対抗できる、セキュアなキー交換メカニズムです。QKD は、検出された脆弱性に基づく継続的な更新を必要としません。

ポスト量子事前共有キー（PPK）

事前共有キーに十分なエントロピーがあり、疑似乱数関数（PRF）、暗号化、および認証変換が量子セキュアである場合、事前共有キーに基づくセッションキーは、量子攻撃に対して脆弱ではありません。このようにして得られるシステムは、今日の古典的な攻撃者や量子コンピュータを使用する将来の攻撃者に対してセキュアであると考えられます。

注意事項と制約事項

QKD と MACsec 通信用の SKIP の統合には、次の注意事項と制限事項があります。

- Cisco NX-OS リリース 10.4（3）F 以降では、次の Cisco Nexus スイッチで Secure Key Integration Protocol がサポートされています。
  - N9K-C9348GC-FXP
  - N9K-C93216TC-FX2
  - N9K-C93360YC-FX2
  - N9K-C9336C-FX2
  - N9K-C9348GC-FX3
  - N9K-C9348D-GX2A
  - N9K-C9332D-H2R
- SKIP プロトコルは、ポイントツーポイント MACsec リンク暗号化のシナリオでのみ使用できます。
- SKIP プロトコルは、MACsec 暗号化をサポートするインターフェイスでのみ使用できます。
- スイッチに HTTPS 接続が確立されている場合は、管理インターフェイスを介して QKD サーバーにアクセスできることを確認します。

- MACsec ピアが 2 つの異なる QKD サーバに接続されている場合、QKD サーバはキーを同期して MKA セッションを確立します。この同期により、MACsec キー（CKN）とキー ストリング（CAK）が両端で同じになります。
- セキュアな Transport Layer Security（TLS）接続を確立し、相互認証を有効にするには、スイッチにトラストポイント証明書をインストールする必要があります。これらの証明書により、スイッチはサーバからキーを取得できます。詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ構成ガイド』のPKI の構成を参照してください。
- MACsec PPK セッションと EAP-TLS セッションは、同じのインターフェイスではサポートされません。
- スイッチは、スイッチごとに 1 つの QKD サーバーと 1 つの QKD プロファイルにのみ接続できます。
- SKIP プロトコルの場合、1 つの remoteSystemID のみがサポートされます。
- QKD 接続の場合、IPv6 はサポートされていません。
- QKD キーを交換する MACsec ピアは、 Cisco NX-OS スイッチである必要があります。
- MACsec セッションが確立されると、QKD プロファイルを変更すると、 **MUST SECURE MACSEC** モードでトラフィックが失われます。
- KME サーバーから取得された QKD キーを使用してMACsec セッションが確立されると、QKD プロファイルの一部であるトラストポイントの変更は、現在のセッションに影響しません。
- 機能応答では、remoteSystemID 属性は必須です。
- Cisco NX-OS リリース 10.5（2）F 以降では、以下の注意事項と制限事項を持つプライマリ PPK に障害が発生した場合にセキュアな MKA セッションを確立するために、PSK サポートへの QKD MACsec フォールバックが提供されます。
  - PPK が構成されている場合は、PSK が最初に構成されていることを確認します。
  - PPK モードは、PSK のキーチェーン フォールバック メソッドをサポートしていません。
  - MACsec セッションが PPK モードで保護されている場合、QKD サーバがダウンしたり切断されたりした場合、または cryptopqc 機能が削除された場合、SAK の有効期限のタイムアウトまたは PN の枯渇などキー再生成イベントがトリガされるまで、現在の PPK セッションとキーが引き続き維持され、使用されます。その後、PPK セッションはセキュアな PSK モードにフォールバックします。ただし、PPK 暗号化 QKD プロファイルが MACsec ポリシーから削除されると、PPK セッションはすぐに PSK モードにフォールバックします。

SKIP を使用したポイントツーポイント MACsec リンク暗号化の設定

ポイントツーポイント MACsec リンク暗号化では、スイッチで SKIP を使用してセキュアな暗号化を確立します。この暗号化は、ピアスイッチの2つのインターフェイス間で設定されるもので、QKDデバイスネットワークの支援を必要とします。スイッチネットワークの代わりに、QKD ネットワークが MACsec 暗号キーを共有します。したがって、スイッチがピア スイッチインターフェイス間に MACsec リンクを作成する必要がある場合、スイッチは外部 QKD デバイスに接続し、キーを要求します。外部 QKD デバイスは、キー ID とキーで構成されるキーペアを生成します。

キー ID は、キーの一意の ID 文字列として機能します（共有秘密）。QKD デバイスはキー ID とキーの両方をスイッチと共有しますが、スイッチはキー ID のみをピアと共有します。ピアスイッチは、このキー ID を使用して、QKD デバイスから暗号キーを取得します。したがって、量子ネットワークは常に暗号キーをセキュアに通信します。

ポスト量子暗号化の有効化

始める前に

- MACsec 事前共有キー（PSK）を設定します。
- PPK モードで MACsec を設定します。
- 外部 QKD デバイス ネットワーク。
- QKD サーバー CA をスイッチのトラストポイントに追加し、QKD サーバー ルート CA 証明書をスイッチにインポートします。

手順

	コマンドまたはアクション	目的

ステップ 1	switch# **configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	switch(config)# **feature cryptopqc** 例： `switch(config)# feature cryptopqc`	スイッチでポスト量子暗号化（cryptopqc）を有効にします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

MACsec および MKA 機能の有効化

手順

	コマンドまたはアクション	目的

ステップ 1	switch# **configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	switch(config)# **feature macsec** 例： `switch(config)# feature macsec`	スイッチで MACsec および MKA を有効にします。
ステップ 3	（任意） switch(config)# copy running-config startup-config 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

量子キー配布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	switch (config)# **crypto qkd profile***name* 例： `switch(config)# crypto qkd profile ppk1`	ppk1 という名前の QKD プロファイルを作成します。
ステップ 2	switch (config)# **kme server**<*hostname*/*IP*> **port** *portnumber* 例： `switch(config-crypto-qkd-profile)# kme server 172.0.0.2 port 6000`	キー管理エンジン（KME）/QKD サーバーの IP と TCP ポート番号を設定します。 （注） ポート番号はオプションです。デフォルトでは、ポート番号は 443 です。
ステップ 3	switch(config)#**transport tls authentication-type trustpoint**<*trustpoint name*> 例：	CA（認証局）トラストポイントを設定します。トラストポイントを作成するには、「PKI の設定」の項を参照してください。

	コマンドまたはアクション	目的
	`switch(config-crypto-qkd-profile)# transport tls authentication-type trustpoint tp1`	
ステップ 4	（任意） switch(config)# **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

MACsec および MKA 機能の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **macsec policy**<*name*> 例： `switch(config)# [no] macsec policy test-policy`	MACsec ポリシーを作成します。
ステップ 2	switch(config)# **ppk crypto-qkd-profile**<*name*> 例： `switch(config-macsec-policy)# [no] ppk crypto-qkd-profile ppk1`	PPK プロファイル名を構成します。
ステップ 3	（任意） switch(config)# copy running-config startup-config 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

設定例

次に、QKD プロファイルの設定と、設定された詳細の表示の例を示します。

- QKD プロファイルの設定

```
switch(config)# feature cryptopqc
switch(config)#
switch(config)# crypto qkd profile ppk1
switch(config-crypto-qkd-profile)# kme server 168.20.1.2 port 5000
switch(config-crypto-qkd-profile)# transport tls authentication-type trustpoint tp1
switch(config-crypto-qkd-profile)# end
switch#
```

- QKD 設定の表示

```
switch# show running-config cryptopqc
!Command: show running-config cryptopqc
!Running configuration last done at: Mon Jan 29 22:19:16 2024
!Time: Mon Jan 29 22:19:35 2024
version 10.4(3) Bios:version 05.51
feature cryptopqc
crypto qkd profile ppk1
kme server 168.20.1.2 port 5000
transport tls authentication-type trustpoint tp1
switch#
```

次に、MACsec ポリシーの PPK プロファイルの設定と、設定された詳細の表示の例を示します。

- MACsec ポリシー上の PPK プロファイルの設定

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# macsec policy test
switch(config-macsec-policy) # ppk crypto-qkd-profile ppk1
switch(config-macsec-policy)# sak-expiry-time 1800
switch(config-macsec-policy)# exit
switch(config)# end
```

- 設定された MACsec ポリシーの表示

```
switch# show macsec policy test
MACSec Cipher     Pri Window Offset Security     SAKRekey   timeICV     Policy
Indicator     Include-SCI
--------------------------------- ---------------- ---- ------------ --------
-------------- -------------- ------------- ------------
test   GCM-AES-XPN-256 16     148809600 0         should-secure 1800         FALSE
               TRUE
MACSec Policy     PPK Crypto-QKD-Profile Name
-------------------------------- --------------------------------
test                ppk1
switch#
```

次に、キー チェーンの設定、インターフェイスでの MACsec ポリシー、および設定された詳細の表示の例を示します。

- キー チェーンの設定

```
switch(config)# key chain KC1 macsec
switch(config-macseckeychain)#key 10100000
switch(config-macseckeychain-macseckey)#key-octet-string
F123456789ABCDEF0123456789ABCDEFF123456789ABCDEF0123456789ABCDEF
cryptographic-algorithm AES_256_CMAC
switch(config-macseckeychain-macseckey)#exit
```

- インターフェイスへの MACsec ポリシーの設定

```
switch(config)# interface Ethernet 1/21
switch(config-if)# macsec keychain KC1 policy test
```

- MACsec セッションの表示

```
switch(config)# show macsec mka session
Interface     Local-TxSCI #     Peers     Status     Key-Server Auth Mode
----------------- -------------------------------- ------------------
```

```
------------------ ------------------ ------------------
Ethernet1/21  6cb2.ae9f.e766/0001 1     Secured         No     PRIMARY-PPK
```

次に、ポイントツーポイント MACsec QKD プロファイルを設定し、QKD プロファイルを MACsec ポリシーにバインドし、MACsec ポリシーをインターフェイスにバインドする例を示します。

（注） 管理ポートを介した接続に対して、KME1およびKME2サーバーがアクティブである必要があることを確認します。

スイッチ 1 の設定

```
switch1# configure terminal
switch1(config)# crypto ca trustpoint tp1
switch1config-trustpoint)# end
switch1#

switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# feature cryptopqc
switch1(config)#
switch1(config)# crypto qkd profile PPK1
switch1(config-crypto-qkd-profile)# kme server KME1 port 7010
switch1(config-crypto-qkd-profile)# transport tls authentication-type trustpoint tp1
switch1(config-crypto-qkd-profile)# end
switch1#

switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# feature macsec
switch1(config)#

switch1(config)# macsec policy MP1
switch1(config-macsec-policy)# ppk crypto-qkd-profile PPK1
switch1(config-macsec-policy)#exit
switch1(config-if)# interface Ethernet1/21
switch1(config-if)# macsec keychain KC1 policy MP1
switch1(config-if)#

switch1(config-if)# interface Ethernet1/22
switch1(config-if)# macsec keychain KC1 policy MP1
switch1(config-if)#
switch1(config-if)# end
switch1#
```

スイッチ 2 の設定

```
switch2# configure terminal
switch2(config)# crypto ca trustpoint tp1
switch2config-trustpoint)# end
switch2#

switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch2(config)# feature cryptopqc
switch2(config)#
switch2(config)# crypto qkd profile PPK1
switch2(config-crypto-qkd-profile)# kme server KME2 port 7010
```

```
switch2(config-crypto-qkd-profile)# transport tls authentication-type trustpoint tp1
switch2(config-crypto-qkd-profile)#
switch2(config-crypto-qkd-profile)# end
switch2#

switch2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch2(config)# feature macsec
switch2(config)#

switch2(config)# macsec policy MP1
switch2(config-macsec-policy)# ppk crypto-qkd-profile PPK1
switch2(config-macsec-policy)# exit

switch2(config-if)# interface Ethernet1/53
switch2(config-if)# macsec keychain KC1 policy MP1
switch2(config-if)#
switch2(config-if)# interface Ethernet1/54
switch2(config-if)# macsec keychain KC1 policy MP1
switch2(config-if)# end
switch2#
```

次に、スイッチ 1 とスイッチ 2 の設定の出力を示します。

Switch 1

```
switch1#
switch1# show macsec mka session
Interface     Local-TxSCI #     Peers     Status     Key-Server     Auth Mode
----------------- ------------------------------- ----------------- ------------------
 ------------------ ------------------
Ethernet1/22   3c8b.7ffe.0244/0001 1     Secured         Yes        PRIMARY-PPK
Ethernet1/21   3c8b.7ffe.0240/0001 1     Secured         Yes        PRIMARY-PPK
N9K3K STANDARD TEMPLATE FOR FEATURE REVIEWS
----------------- ------------------------------- ----------------- ------------------
 ------------------ ------------------
Total Number of Sessions : 2
Secured Sessions : 2
Pending Sessions : 0
switch1#
```

スイッチ 2

```
switch2#
switch2# show macsec mka session
Interface     Local-TxSCI #     Peers     Status     Key-Server     Auth Mode
----------------- ------------------------------- ----------------- ------------------
 ------------------ ------------------
Ethernet1/53  5451.deb8.62b4/0001 1         Secured     No         PRIMARY-PPK
Ethernet1/54  5451.deb8.62b8/0001 1         Secured     No         PRIMARY-PPK
----------------- ------------------------------- ----------------- ------------------
 ------------------ ------------------
Total Number of Sessions : 2
Secured Sessions : 2
Pending Sessions : 0
switch2#
```

設定可能なEAPOLの宛先とイーサネットタイプについて

Cisco NX-OS リリース 9.2(2) 以降では、WAN MACsec を使用するネットワークで、Extensible Authentication Protocol（EAP）over LAN（EAPOL）プロトコルの宛先アドレスとイーサネットタイプの値を非標準値に変更できます。

設定可能なEAPOL MACおよびイーサネットタイプでは、標準MKAパケットを消費するイーサネットネットワーク上でCEデバイスがMKAセッションを形成できるように、MKAパケットの MAC アドレスとイーサネット タイプを変更できます。

EAPOL 宛先イーサネット タイプは、デフォルトのイーサネット タイプ 0x888E から代替値に変更できます。または、EAPOL宛先MACアドレスは、デフォルトDMACの01:80:C2:00:00:03から代替値に変更できます。プロバイダー ブリッジによって消費されないようにします。

この機能はインターフェイス レベルで使用でき、代替EAPOL設定は、次のように任意のインターフェイスでいつでも変更できます。

- MACsecがインターフェイスですでに設定されている場合、セッションは新しい代替EAPOL設定で起動します。
- MACsecがインターフェイスで設定されていない場合、EAPOL設定はインターフェイスに適用され、MACsec がそのインターフェイスで設定されている場合に有効になります。

EAPOL 設定の有効化

EAPOL 設定は、使用可能な任意のインターフェイスで有効にできます。

始める前に

MACsec が有効であることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**interface** *name*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。

	コマンドまたはアクション	目的
ステップ 3	**eapol mac-address** *mac_address* [**ethertype** *eth_type*]	指定されたインターフェイス タイプおよびIDでEAPOL設定を有効にします。 （注） イーサネット タイプが指定されていない場合、MKA パケットのデフォルト イーサネット タイプ（0x888e）であると見なします。
ステップ 4	**eapol mac-address broadcast-address** [**ethertype** *eth_type*]	ブロードキャストアドレスを代替MACアドレスとして有効にします。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-macseckeychain-macseckey)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 6	**show macsec mka session detail**	EAPOL 設定を表示します。

EAPOL 設定の無効化

使用可能なインターフェイスで EAPOL 設定を無効にできます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**interface** *name*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。

ステップ 3	[**no**] **eapol mac-address** *mac_address* [**ethertype** *eth_type*]	指定されたインターフェイス タイプおよびIDでEAPOL設定を無効にします。
ステップ 4	（任意） **copy running-config startup-config** 例：	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	`switch(config-macseckeychain-macseckey)# copy running-config startup-config`	

MACsec 設定の確認

MACsec 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show key chain *name*	キーチェーンの設定を表示します。
show macsec mka session [**interface** *type slot*/*port*] [**detail**]	特定のインターフェイスまたはすべてのインターフェイスの MACsec MKA セッションに関する情報を表示します。
show macsec mka session details	すべての EAPOL パケットのインターフェイスで現在使用されている MAC アドレスおよびイーサネット タイプに関する情報を表示します。
show macsec mka summary	MACsec MKA 設定を表示します。
show macsec policy [*policy-name*]	特定の MACsec ポリシーまたはすべての MACsec ポリシーの設定を表示します。
show running-config macsec	MACsec の実行コンフィギュレーション情報を表示します。

次に、すべてのインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。。

```
switch# show macsec mka session
Interface          Local-TxSCI                     #Peers            Status
  Key-Server         Auth Mode
------------------ ------------------------------- ------------------ ----------------
 ------------------ ------------------
Ethernet2/2        2c33.11b8.7d14/0001             1                  Secured
   Yes               PRIMARY-PSK
Ethernet2/3        2c33.11b8.7d18/0001             1                  Secured
   Yes               PRIMARY-PSK
------------------ ------------------------------- ------------------ ----------------
 ------------------ ------------------
Total Number of Sessions : 2
        Secured Sessions : 2
        Pending Sessions : 0
```

次に、特定のインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。前の例で説明したテーブルの一般的な要素に加えて、現在の MACsec セッション タイプを定義する認証モードも示します。

```
switch# show macsec mka session interface ethernet 1/1

Interface      Local-TxSCI          # Peers   Status        Key-Server     Auth Mode
```

```
-------------- -------------------- --------- ------------- -------------- -------------
Ethernet1/1    70df.2fdc.baf4/0001      0     Pending       Yes            PRIMARY-PSK
Ethernet1/1    70df.2fdc.baf4/0001      1     Secured       No             FALLBACK-PSK
```

次に、特定のイーサネット インターフェイスの MACsec MKA セッションに関する詳細情報を表示する例を示します。

```
Interface Name          : Ethernet2/2
    Session Status                    : SECURED - Secured MKA Session with MACsec
    Local Tx-SCI                      : 2c33.11b8.7d14/0001
    Local Tx-SSCI                     : 2
    MKA Port Identifier               : 2
    CAK Name (CKN)                    : 12
    CA Authentication Mode            : PRIMARY-PSK
    Member Identifier (MI)            : B54263EF7949A561E25CE617
    Message Number (MN)               : 523
    MKA Policy Name                   : tests2
    Key Server Priority               : 16
    Key Server                        : Yes
    Include ICV                       : No
    SAK Cipher Suite                  : GCM-AES-XPN-256
    SAK Cipher Suite (Operational)    : GCM-AES-XPN-256
    Replay Window Size                : 148809600
    Confidentiality Offset            : CONF-OFFSET-0
    Confidentiality Offset (Operational): CONF-OFFSET-0
    Latest SAK Status                 : Rx & TX
    Latest SAK AN                     : 0
    Latest SAK KI                     : B54263EF7949A561E25CE61700000001
    Latest SAK KN                     : 1
    Last SAK key time                 : 12:59:38 PST Tue Mar 19 2019
    CA Peer Count                     : 1
    Eapol dest mac                    : 0180.c200.0003
    Ether-type                        : 0x888e
Peer Status:
    Peer MI                           : 2C2C090E62A96F4D6E018210
    RxSCI                             : 2c33.11b8.8b88/0001
    Peer CAK                          : Match
    Latest Rx MKPDU                   : 13:16:54 PST Tue Mar 19 2019
```

次に、MACsec MKA 設定を表示する例を示します。

```
switch# show macsec mka summary
Interface          MACSEC-policy                    Keychain
------------------ -------------------------------- ------------------------
Ethernet2/13       1                                1/10000000000000000
Ethernet2/14       1                                1/10000000000000000
```

次に、すべての MACsec ポリシーの設定を表示する例を示します。

```
switch# show macsec policy
MACSec Policy        Cipher          Pri  Window     Offset   Security   SAK Rekey time
 ICV Indicator  Include-SCI
----------------- -------------     --- --------   --------  --------  --------------
 ------------- -------------
KC256-Po117b        GCM-AES-256      16   148809600    0    should-secure  pn-rollover
   FALSE        True
pol1                GCM-AES-XPN-256  100  148809600    30   must-secure    60
   FALSE        True
pol256-FanO         GCM-AES-XPN-256  16   148809600    0    must-secure    60
   FALSE        True
pol256-MCT          GCM-AES-XPN-256  16   148809600    0    should-secure  60
   FALSE        FALSE
```

```
system-default-
macsec-policy       GCM-AES-XPN-256  16   148809600    0    should-secure  pn-rollover
   FALSE        FALSE
test1               GCM-AES-XPN-256  16   148809600    0    should-secure  pn-rollover
   FALSE        True
```

次の例では、**show running-config** および **show startup-config** コマンドの出力にキー オクテット文字列が表示されることを示しています。ただし、**key-chain macsec-psk no-show** コマンドが設定されている場合を除きます。

```
key chain KC256-1 macsec
  key 2000
    key-octet-string 7
075e701e1c5a4a5143475e5a527d7c7c706a6c724306170103555a5c57510b051e47080
a05000101005e0e50510f005c4b5f5d0b5b070e234e4d0a1d0112175b5e cryptographic-algorithm
AES_256_CMAC
```

次の例では、**show running-config** および **show startup-config** コマンドの出力にキー オクテット文字列が表示されることを示しています。こちらは、**key-chain macsec-psk no-show** コマンドが設定されている場合です。

```
key chain KC256-1 macsec
  key 2000
    key-octet-string 7 ****** cryptographic-algorithm AES_256_CMAC
```

MACsec 統計の表示

次のコマンドを使用して、MACsec 統計情報を表示できます。

コマンド	説明
show macsec mka statistics [**interface** *type slot*/*port*]	MACsec MKA 統計情報を表示します。
show macsec secy statistics [**interface** *type slot*/*port*]	MACsec セキュリティ統計情報を表示します。

次に、特定のイーサネット インターフェイスの MACsec MKA 統計情報の例を示します。

```
switch# show macsec mka statistics interface ethernet 2/2

Per-CA MKA Statistics for Session on interface (Ethernet2/2) with CKN 0x10
================================================================================
CA Statistics
   Pairwise CAK Rekeys..... 0

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

MKPDU Statistics
   MKPDUs Transmitted...... 1096
      "Distributed SAK".. 0

   MKPDUs Validated & Rx... 0
      "Distributed SAK".. 0
```

```
MKA Statistics for Session on interface (Ethernet2/2)
=====================================================
CA Statistics
   Pairwise CAK Rekeys..... 0

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

MKPDU Statistics
   MKPDUs Transmitted...... 1096
      "Distributed SAK".. 0
   MKPDUs Validated & Rx... 0
      "Distributed SAK".. 0
   MKPDUs Tx Success.......... 1096
   MKPDUs Tx Fail.............. 0
   MKPDUS Tx Pkt build fail... 0
   MKPDUS No Tx on intf down.. 0
   MKPDUS No Rx on intf down.. 0
   MKPDUs Rx CA Not found..... 0
   MKPDUs Rx Error............. 0
   MKPDUs Rx Success.......... 0

MKPDU Failures
   MKPDU Rx Validation ..................... 0
   MKPDU Rx Bad Peer MN..................... 0
   MKPDU Rx Non-recent Peerlist MN.......... 0
   MKPDU Rx Drop SAKUSE, KN mismatch........ 0
   MKPDU Rx Drop SAKUSE, Rx Not Set......... 0
   MKPDU Rx Drop SAKUSE, Key MI mismatch.... 0
   MKPDU Rx Drop SAKUSE, AN Not in Use...... 0
   MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set... 0
   MKPDU Rx Drop Packet, Ethertype Mismatch. 0

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

CA Failures
   ICK Derivation.................. 0
   KEK Derivation.................. 0
   Invalid Peer MACsec Capability... 0

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

次に、特定のイーサネット インターフェイスの MACsec セキュリティ統計情報を表示する例を示します。

（注） Rx および Tx 統計情報の非制御パケットと制御パケットには、次の違いがあります。

- Rx 統計
  - 非制御=暗号化および非暗号化
  - 制御 = 非暗号化
- TX 統計情報：
  - 非制御 = 非暗号化
  - 制御 = 暗号化
  - 共通 = 暗号化および非暗号化

```
switch(config)# show macsec secy statistics interface e2/28/1

Interface Ethernet2/28/1 MACSEC SecY Statistics:
-----------------------------------------
Interface Rx Statistics:
   Unicast Uncontrolled Pkts: 14987
   Multicast Uncontrolled Pkts: 1190444
   Broadcast Uncontrolled Pkts: 4
   Uncontrolled Pkts - Rx Drop: 0
   Uncontrolled Pkts - Rx Error: 0
   Unicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Multicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Broadcast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Controlled Pkts: 247583
   Controlled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
   Controlled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
   In-Octets Uncontrolled: 169853963 bytes
   In-Octets Controlled: 55027017 bytes
   Input rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
   Input rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
   Input rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Input rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)

Interface Tx Statistics:
   Unicast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
   Multicast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
   Broadcast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
   Uncontrolled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
   Uncontrolled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
   Unicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Multicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Broadcast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Controlled Pkts: 205429
   Controlled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
   Controlled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
   Out-Octets Uncontrolled: N/A (N9K-X9736C-FX not supported)
   Out-Octets Controlled: 20612648 bytes
   Out-Octets Common: 151787484 bytes
   Output rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
   Output rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
   Output rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Output rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)
```

```
SECY Rx Statistics:
  Transform Error Pkts: N/A (N9K-X9736C-FX not supported)
   Control Pkts: 952284
   Untagged Pkts: N/A (N9K-X9736C-FX not supported)
   No Tag Pkts: 0
   Bad Tag Pkts: 0
   No SCI Pkts: 0
   Unknown SCI Pkts: 0
   Tagged Control Pkts: N/A (N9K-X9736C-FX not supported)

SECY Tx Statistics:
   Transform Error Pkts: N/A (N9K-X9736C-FX not supported)
   Control Pkts: 967904
   Untagged Pkts: N/A (N9K-X9736C-FX not supported)

SAK Rx Statistics for AN [3]:
   Unchecked Pkts: 0
   Delayed Pkts: 0
   Late Pkts: 0
   OK Pkts: 1
   Invalid Pkts: 0
   Not Valid Pkts: 0
   Not-Using-SA Pkts: 0
   Unused-SA Pkts: 0
   Decrypted In-Octets: 235 bytes
   Validated In-Octets: 0 bytes

SAK Tx Statistics for AN [3]:
   Encrypted Protected Pkts: 2
   Too Long Pkts: N/A (N9K-X9736C-FX not supported)
   SA-not-in-use Pkts: N/A (N9K-X9736C-FX not supported)
   Encrypted Protected Out-Octets: 334 bytes
switch(config)#
```

MACsec の設定例

次に、ユーザ定義のMACsecポリシーを設定し、そのポリシーをインターフェイスに適用する例を示します。

```
switch(config)# macsec policy 1
switch(config-macsec-policy)# cipher-suite GCM-AES-256
switch(config-macsec-policy)# window-size 512
switch(config-macsec-policy)# key-server-priority 0
switch(config-macsec-policy)# conf-offset CONF-OFFSET-0
switch(config-macsec-policy)# security-policy should-secure
switch(config-macsec-policy)# exit

switch(config)# int e2/13-14
switch(config-if-range)# macsec keychain 1 policy 1
switch(config-if-range)# exit
switch(config)# show macsec mka summary
Interface          MACSEC-policy                    Keychain
------------------ -------------------------------- ------------------------
Ethernet2/13       1                                1/10000000000000000
Ethernet2/14       1                                1/10000000000000000

switch(config)# show macsec mka session
Interface      Local-TxSCI          # Peers    Status     Key-Server
-------------- -------------------- ---------- ---------- -------------
Ethernet2/13   006b.f1be.d31c/0001  1          Secured    Yes
```

```
Ethernet2/14   006b.f1be.d320/0001  1          Secured    No

switch(config)# show running-config macsec
!Command: show running-config macsec
!Time: Mon Dec  5 04:53:40 2016

version 9.2(1)feature macsec
macsec policy 1
  cipher-suite GCM-AES-256
  key-server-priority 0
  window-size 512
  conf-offset CONF-OFFSET-0
  security-policy should-secure

interface Ethernet2/13
  macsec keychain 1 policy 1

interface Ethernet2/14
  macsec keychain 1 policy 1
```

次に、MACsec キーチェーンを設定し、インターフェイスにシステムデフォルトの MACsecポリシーを追加する例を示します。

```
switch(config)# key chain 1 macsec
switch(config-macseckeychain)# key 1000
switch(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm
 aes_256_CMAC
switch(config-macseckeychain-macseckey)# exit

switch(config)# int e2/13-14
switch(config-if-range)# macsec keychain 1
switch(config-if-range)# exit
switch(config)#

switch(config)# show running-config macsec
!Command: show running-config macsec
!Time: Mon Dec  5 04:50:16 2016
version 7.0(3)I4(5)
feature macsec
interface Ethernet2/13
  macsec keychain 1 policy system-default-macsec-policy
interface Ethernet2/14
  macsec keychain 1 policy system-default-macsec-policy

switch(config)# show macsec mka session
Interface          Local-TxSCI                     # Peers            Status
   Key-Server         Auth Mode
------------------ ------------------------------- ------------------ ------------------
 ------------------ ------------------
Ethernet2/2        2c33.11b8.7d14/0001             1                  Secured
   Yes                PRIMARY-PSK
Ethernet2/3        2c33.11b8.7d18/0001             1                  Secured
   Yes                PRIMARY-PSK
------------------ ------------------------------- ------------------ ------------------
 ------------------ ------------------
Total Number of Sessions : 2
        Secured Sessions : 2
        Pending Sessions : 0

switch(config)# show macsec mka summary
Interface         Status   Cipher (Operational)   Key-Server   MACSEC-policy   Keychain
  Fallback-keychain
```

```
------------------ -------- ---------------------- ------------ -------------- ----------
 ---------------
Ethernet2/1        down       -                      -          tests1           keych1
    no keychain
Ethernet2/2        Secured  GCM-AES-XPN-256        Yes          tests2           keych2
    no keychain
Ethernet2/3        Secured  GCM-AES-256            Yes          tests3           keyc3
    no keychain
```

次に、Peer Enforce Cipher 設定機能 MACsec の設定と出力の例を示します。

```
switch# show key chain
Key-Chain KC1 Macsec
Key 10000000 -- text 7
"0729701e1d5d4c53404a522d26090f010e6364704053435560e007971772a263e30080a040707030353022725 7b7321355655095852 5a771b1650382734362e2a"
cryptographic-algorithm AES_256_CMAC
send lifetime (always valid) [active]

Key-Chain KC2 Macsec
Key 10100000 -- text 7
"0729701e1d5d4c53404a522d26090f010e6364704053435560e007971772a263e30080a040707030353022725 7b7321355655095852 5a771b1650382734362e2a"
cryptographic-algorithm AES_256_CMAC
send lifetime (always valid) [active]

switch#
switch# show run macsec

!Command: show running-config macsec
!Running configuration last done at: Mon Apr 17 16:49:57 2023
!Time: Mon Apr 17 16:50:09 2023

version 10.3(3) Bios:version 05.47
feature macsec

macsec policy MP1
no protocol lldp encrypted
cipher-suite enforce-peer GCM-AES-XPN-256 GCM-AES-XPN-128
macsec policy MP2
no protocol lldp encrypted
cipher-suite enforce-peer GCM-AES-256
interface Ethernet1/97/1
macsec keychain KC1 policy MP1

interface Ethernet1/97/2
macsec keychain KC2 policy MP2

switch#

switch# show macsec policy
MACSec Policy Cipher Pri Window Offset Security SAK Rekey time ICV Indicator Include-SCI
------------------------------- ---------------- ---- ------------ -------- --------------
 -------------- ------------- -------------
MP1 Enforce-Peer 16 148809600 0 should-secure pn-rollover FALSE TRUE
MP2 Enforce-Peer 16 148809600 0 should-secure pn-rollover FALSE TRUE
system-default-macsec-policy GCM-AES-XPN-256 16 148809600 0 should-secure pn-rollover
FALSE TRUE

MACSec Policy                  Lldp-bypass
------------------------------- -------------
MP1                                True
MP2                                True
system-default-macsec-policy       FALSE
```

```
MACSec Policy PPK Crypto-QKD-Profile Name
-------------------------------- --------------------------------

MACSec Policy Cipher-Suite Enforce-Peer
-------------------------------- --------------------------------------------------
MP1 GCM-AES-XPN-256 GCM-AES-XPN-128
MP2 GCM-AES-256
switch#
```

次の例は、**show macsec mka session detail** コマンドのサンプル出力を示しています。

```
switch# show macsec mka session details
Detailed Status for MKA Session
---------------------------------
Interface Name : Ethernet1/97/1
Session Status : SECURED - Secured MKA Session with MACsec
Local Tx-SCI : c4f7.d530.1484/0001
Local Tx-SSCI : 1
MKA Port Identifier : 1
CAK Name (CKN) : 10000000
CA Authentication Mode : PRIMARY-PSK
Member Identifier (MI) : D94B90E3FDB111CE583E7158
Message Number (MN) : 111
MKA Policy Name : MP1
Key Server Priority : 16
Key Server : Yes
Include ICV : No
SAK Cipher Suite : GCM-AES-XPN-128
SAK Cipher Suite (Operational) : GCM-AES-XPN-128
Replay Window Size : 148809600
Confidentiality Offset : CONF-OFFSET-0
Confidentiality Offset (Operational): CONF-OFFSET-0
Latest SAK Status : Rx & TX
Latest SAK AN : 1
Latest SAK KI : D94B90E3FDB111CE583E715800000001
Latest SAK KN : 1
Last SAK key time : 16:48:41 PST Mon Apr 17 2023
CA Peer Count : 1
Eapol dest mac : 0180.c200.0003
Ether-type : 0x888e
Peer Status:
Peer MI : 00110000000100010000001
RxSCI : 0011.0000.0001/0001
Peer CAK : Match
Latest Rx MKPDU : 16:52:07 PST Mon Apr 17 2023

Interface Name : Ethernet1/97/2
Session Status : SECURED - Secured MKA Session with MACsec
Local Tx-SCI : c4f7.d530.1485/0001
Local Tx-SSCI : 1
MKA Port Identifier : 1
CAK Name (CKN) : 10100000
CA Authentication Mode : PRIMARY-PSK
Member Identifier (MI) : 43AE54C19982238C298E0241
Message Number (MN) : 107
MKA Policy Name : MP2
Key Server Priority : 16
Key Server : Yes
Include ICV : No
SAK Cipher Suite : GCM-AES-256
SAK Cipher Suite (Operational) : GCM-AES-256
Replay Window Size : 148809600
Confidentiality Offset : CONF-OFFSET-0
Confidentiality Offset (Operational): CONF-OFFSET-0
```

```
Latest SAK Status : Rx & TX
Latest SAK AN : 0
Latest SAK KI : 43AE54C19982238C298E024100000001
Latest SAK KN : 1
Last SAK key time : 16:48:42 PST Mon Apr 17 2023
CA Peer Count : 1
Eapol dest mac : 0180.c200.0003
Ether-type : 0x888e
Peer Status:
Peer MI : 00270000000010001000000001
RxSCI : 0027.0000.0001/0001
Peer CAK : Match
Latest Rx MKPDU : 16:52:06 PST Mon Apr 17 2023
switch#
```

XML の例

MACsec は、**| xml** を使用したスクリプト用に次の **show** コマンドの XML 出力をサポートします。

- **show key chain** *name* **| xml**
- **show macsec mka session interface** *interface slot/port* **details | xml**
- **show macsec mka statistics interface** *interface slot/port* **| xml**
- **show macsec mka summary | xml**
- **show macsec policy** *name* **| xml**
- **show macsec secy statistics interface** *interface slot/port* **| xml**
- **show running-config macsec | xml**

次に、上記の各 **show** コマンドの出力例を示します。

例 1：キーチェーンの設定を表示します

```
switch# show key chain "Kc2" | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0:rpm">
 <nf:data>
  <show>
   <key>
    <chain>
     <__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
      <keychain>Kc2</keychain>
     </__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
    </chain>
   </key>
  </show>
 </nf:data>
</nf:rpc-reply>
]]>]]>
```

例 2：特定のインターフェイスの MACsec MKA セッションに関する情報を表示します。

```
switch# show macsec mka session interface ethernet 4/31 details | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0">
 <nf:data>
  <show>
   <macsec>
    <mka>
     <session>
      <__XML__OPT_Cmd_show_macsec_mka_session_interface>
       <interface>
        <__XML__INTF_ifname>
         <__XML__PARAM_value>
          <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
         </__XML__PARAM_value>
        </__XML__INTF_ifname>
       </interface>
       <__XML__OPT_Cmd_show_macsec_mka_session_details>
        <details/>
        <__XML__OPT_Cmd_show_macsec_mka_session___readonly__>
         <__readonly__>
          <TABLE_mka_session_details>
           <ROW_mka_session_details>
            <ifname>Ethernet4/31</ifname>
            <status>Secured</status>
            <sci>0c75.bd03.5360/0001</sci>
            <ssci>1</ssci>
            <port_id>1</port_id>
            <mi>02000000000000000000000000000000000000000000000000000000000000000000
</mi>
            <mi>F511280A765CE41C79458753</mi>
            <mn>2770</mn>
            <policy>am2</policy>
            <ks_prio>0</ks_prio>
            <keyserver>No</keyserver>
            <cipher>GCM-AES-XPN-256</cipher>
            <window>512</window>
            <conf_offset>CONF-OFFSET-0</conf_offset>
            <sak_status>Rx & TX</sak_status>
            <sak_an>1</sak_an>
            <sak_ki>516486241</sak_ki>
            <sak_kn>90</sak_kn>
            <last_sak_rekey_time>07:12:02 UTC Fri Jan 20 2017</last_sak_rekey_ti
me>
           </ROW_mka_session_details>
          </TABLE_mka_session_details>
         </__readonly__>
        </__XML__OPT_Cmd_show_macsec_mka_session___readonly__>
       </__XML__OPT_Cmd_show_macsec_mka_session_details>
      </__XML__OPT_Cmd_show_macsec_mka_session_interface>
     </session>
    </mka>
   </macsec>
  </show>
 </nf:data>
</nf:rpc-reply>
]]>]]>
```

例 3：MACsec MKA 統計情報を表示します。

```
switch# show macsec mka statistics interface ethernet 4/31 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0">
```

```
 <nf:data>
  <show>
<macsec>
    <mka>
     <statistics>
      <__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
       <interface>
        <__XML__INTF_ifname>
         <__XML__PARAM_value>
          <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
          <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
         </__XML__PARAM_value>
        </__XML__INTF_ifname>
       </interface>
       <__XML__OPT_Cmd_some_macsec_mka_statistics___readonly__>
        <__readonly__>
         <TABLE_mka_intf_stats>
          <ROW_mka_intf_stats>
           <TABLE_ca_stats>
            <ROW_ca_stats>
             <ca_stat_ckn>0x2</ca_stat_ckn>
             <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
             <sa_stat_sak_generated>0</sa_stat_sak_generated>
             <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
             <sa_stat_sak_received>91</sa_stat_sak_received>
             <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
             <mkpdu_stat_mkpdu_tx>2808</mkpdu_stat_mkpdu_tx>
             <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
             <mkpdu_stat_mkpdu_rx>2714</mkpdu_stat_mkpdu_rx>
             <mkpdu_stat_mkpdu_rx_distsak>91</mkpdu_stat_mkpdu_rx_distsak>
            </ROW_ca_stats>
           </TABLE_ca_stats>
          </ROW_mka_intf_stats>
         </TABLE_mka_intf_stats>
        </__readonly__>
       </__XML__OPT_Cmd_some_macsec_mka_statistics___readonly__>
       <interface>
        <__XML__INTF_ifname>
         <__XML__PARAM_value>
          <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
         </__XML__PARAM_value>
        </__XML__INTF_ifname>
       </interface>
       <__XML__OPT_Cmd_some_macsec_mka_statistics___readonly__>
        <__readonly__>
         <TABLE_mka_intf_stats>
          <ROW_mka_intf_stats>
           <TABLE_idb_stats>
            <ROW_idb_stats>
             <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
             <sa_stat_sak_generated>0</sa_stat_sak_generated>
             <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
             <sa_stat_sak_received>91</sa_stat_sak_received>
             <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
             <mkpdu_stat_mkpdu_tx>2808</mkpdu_stat_mkpdu_tx>
             <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
             <mkpdu_stat_mkpdu_rx>2714</mkpdu_stat_mkpdu_rx>
             <mkpdu_stat_mkpdu_rx_distsak>91</mkpdu_stat_mkpdu_rx_distsak>
             <idb_stat_mkpdu_tx_success>2808</idb_stat_mkpdu_tx_success>
             <idb_stat_mkpdu_tx_fail>0</idb_stat_mkpdu_tx_fail>
             <idb_stat_mkpdu_tx_pkt_build_fail>0</idb_stat_mkpdu_tx_pkt_build_fail>
             <idb_stat_mkpdu_no_tx_on_intf_down>0</idb_stat_mkpdu_no_tx_on_intf_down>
             <idb_stat_mkpdu_no_rx_on_intf_down>0</idb_stat_mkpdu_no_rx_on_intf_down>
             <idb_stat_mkpdu_rx_ca_notfound>0</idb_stat_mkpdu_rx_ca_notfound>
```

```
            <idb_stat_mkpdu_rx_error>0</idb_stat_mkpdu_rx_error>
            <idb_stat_mkpdu_rx_success>2714</idb_stat_mkpdu_rx_success>
            <idb_stat_mkpdu_failure_rx_integrity_check_error>0</idb_stat_mkpdu_
failure_rx_integrity_check_error>
            <idb_stat_mkpdu_failure_invalid_peer_mn_error>0</idb_stat_mkpdu_fai
lure_invalid_peer_mn_error>
            <idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>1</idb_stat_mkp
du_failure_nonrecent_peerlist_mn_error>
            <idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>0</idb_stat_mkpdu_
failure_sakuse_kn_mismatch_error>
<idb_stat_mkpdu_failure_sakuse_rx_not_set_error>0</idb_stat_mkpdu_f
ailure_sakuse_rx_not_set_error>
            <idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>0</idb_stat_mk
pdu_failure_sakuse_key_mi_mismatch_error>
            <idb_stat_mkpdu_failure_sakuse_an_not_in_use_error>0</idb_stat_mkpd
u_failure_sakuse_an_not_in_use_error>
            <idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>0</idb_stat_m
kpdu_failure_sakuse_ks_rx_tx_not_set_error>
            <idb_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>0</id
b_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>
            <idb_stat_sak_failure_sak_generate_error>0</idb_stat_sak_failure_sa
k_generate_error>
            <idb_stat_sak_failure_hash_generate_error>0</idb_stat_sak_failure_h
ash_generate_error>
            <idb_stat_sak_failure_sak_encryption_error>0</idb_stat_sak_failure_
sak_encryption_error>
            <idb_stat_sak_failure_sak_decryption_error>0</idb_stat_sak_failure_
sak_decryption_error>
            <idb_stat_sak_failure_ick_derivation_error>0</idb_stat_sak_failure_
ick_derivation_error>
            <idb_stat_sak_failure_kek_derivation_error>0</idb_stat_sak_failure_
kek_derivation_error>
            <idb_stat_sak_failure_invalid_macsec_capability_error>0</idb_stat_s
ak_failure_invalid_macsec_capability_error>
            <idb_stat_macsec_failure_rx_sa_create_error>0</idb_stat_macsec_fail
ure_rx_sa_create_error>
            <idb_stat_macsec_failure_tx_sa_create_error>0</idb_stat_macsec_fail
ure_tx_sa_create_error>
           </ROW_idb_stats>
          </TABLE_idb_stats>
         </ROW_mka_intf_stats>
        </TABLE_mka_intf_stats>
       </__readonly__>
      </__XML__OPT_Cmd_some_macsec_mka_statistics___readonly__>
     </__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
    </statistics>
   </mka>
  </macsec>
 </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
```

例 4：MACsec MKA 設定を表示します。

```
switch# show macsec mka summary | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0">
 <nf:data>
  <show>
   <macsec>
    <mka>
     <__XML__OPT_Cmd_some_macsec_summary>
```

```
      <__XML__OPT_Cmd_some_macsec___readonly__>
       <__readonly__>
        <TABLE_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet2/1</ifname>
          <policy>am2</policy>
<keychain>kc2/020000000000000000000000000000000000000000000000000000000000
00000000</keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet3/1</ifname>
          <policy>am2</policy>
          <keychain>kc2/020000000000000000000000000000000000000000000000000000000000
00000000</keychain>
         </ROW_mka_summary>

[TRUNCATED FOR READABILITY]

<ROW_mka_summary>
          <ifname>Ethernet3/32</ifname>
          <policy>am2</policy>
          <keychain>kc2/020000000000000000000000000000000000000000000000000000000000
00000000</keychain>
         </ROW_mka_summary>
        </TABLE_mka_summary>
       </__readonly__>
      </__XML__OPT_Cmd_some_macsec___readonly__>
     </__XML__OPT_Cmd_some_macsec_summary>
    </mka>
   </macsec>
  </show>
 </nf:data>
</nf:rpc-reply>
]]>]]>
```

例 5：特定の MACsec ポリシーの設定を表示します。

```
switch# show macsec policy am2 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0">
 <nf:data>
  <show>
   <macsec>
    <policy>
     <__XML__OPT_Cmd_some_macsec_policy_name>
      <policy_name>am2</policy_name>
      <__XML__OPT_Cmd_some_macsec___readonly__>
       <__readonly__>
        <TABLE_macsec_policy>
         <ROW_macsec_policy>
          <name>am2</name>
          <cipher_suite>GCM-AES-XPN-256</cipher_suite>
          <keyserver_priority>0</keyserver_priority>
          <window_size>512</window_size>
          <conf_offset>0</conf_offset>
          <security_policy>must-secure</security_policy>
          <sak-expiry-time>60</sak-expiry-time>
         </ROW_macsec_policy>
        </TABLE_macsec_policy>
       </__readonly__>
      </__XML__OPT_Cmd_some_macsec___readonly__>
     </__XML__OPT_Cmd_some_macsec_policy_name>
    </policy>
```

```
   </macsec>
  </show>
 </nf:data>
</nf:rpc-reply>
]]>]]>
```

例 6：MACsec セキュリティ統計情報を表示します。

```
switch# show macsec secy statistics interface ethernet 4/31 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://w
ww.cisco.com/nxos:1.0">
 <nf:data>
  <show>
   <macsec>
    <secy>
     <statistics>
      <interface>
       <__XML__INTF_ifname>
        <__XML__PARAM_value>
         <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
        </__XML__PARAM_value>
        <__XML__OPT_Cmd_some_macsec_secy_statistics___readonly__>
         <__readonly__>
          <TABLE_statistics>
           <ROW_statistics>
            <in_pkts_unicast_uncontrolled>0</in_pkts_unicast_uncontrolled>
            <in_pkts_multicast_uncontrolled>42</in_pkts_multicast_uncontrolled>
            <in_pkts_broadcast_uncontrolled>0</in_pkts_broadcast_uncontrolled>
            <in_rx_drop_pkts_uncontrolled>0</in_rx_drop_pkts_uncontrolled>
            <in_rx_err_pkts_uncontrolled>0</in_rx_err_pkts_uncontrolled>
            <in_pkts_unicast_controlled>0</in_pkts_unicast_controlled>
            <in_pkts_multicast_controlled>2</in_pkts_multicast_controlled>
            <in_pkts_broadcast_controlled>0</in_pkts_broadcast_controlled>
            <in_rx_drop_pkts_controlled>0</in_rx_drop_pkts_controlled>
            <in_rx_err_pkts_controlled>0</in_rx_err_pkts_controlled>
            <in_octets_uncontrolled>7230</in_octets_uncontrolled>
            <in_octets_controlled>470</in_octets_controlled>
            <input_rate_uncontrolled_pps>0</input_rate_uncontrolled_pps>
            <input_rate_uncontrolled_bps>9</input_rate_uncontrolled_bps>
            <input_rate_controlled_pps>0</input_rate_controlled_pps>
            <input_rate_controlled_bps>23</input_rate_controlled_bps>
            <out_pkts_unicast_uncontrolled>0</out_pkts_unicast_uncontrolled>
            <out_pkts_multicast_uncontrolled>41</out_pkts_multicast_uncontrolled>
            <out_pkts_broadcast_uncontrolled>0</out_pkts_broadcast_uncontrolled>
            <out_rx_drop_pkts_uncontrolled>0</out_rx_drop_pkts_uncontrolled>
            <out_rx_err_pkts_uncontrolled>0</out_rx_err_pkts_uncontrolled>
            <out_pkts_unicast_controlled>0</out_pkts_unicast_controlled>
            <out_pkts_multicast_controlled>2</out_pkts_multicast_controlled>
            <out_pkts_broadcast_controlled>0</out_pkts_broadcast_controlled>
            <out_rx_drop_pkts_controlled>0</out_rx_drop_pkts_controlled>
            <out_rx_err_pkts_controlled>0</out_rx_err_pkts_controlled>
            <out_octets_uncontrolled>6806</out_octets_uncontrolled>
            <out_octets_controlled>470</out_octets_controlled>
            <out_octets_common>7340</out_octets_common>
            <output_rate_uncontrolled_pps>2598190092</output_rate_uncontrolled_pps>
            <output_rate_uncontrolled_bps>2598190076</output_rate_uncontrolled_bps>
            <output_rate_controlled_pps>0</output_rate_controlled_pps>
            <output_rate_controlled_bps>23</output_rate_controlled_bps>
            <in_pkts_transform_error>0</in_pkts_transform_error>
            <in_pkts_control>40</in_pkts_control>
            <in_pkts_untagged>0</in_pkts_untagged>
            <in_pkts_no_tag>0</in_pkts_no_tag>
            <in_pkts_badtag>0</in_pkts_badtag>
```

```
            <in_pkts_no_sci>0</in_pkts_no_sci>
            <in_pkts_unknown_sci>0</in_pkts_unknown_sci>
            <in_pkts_tagged_ctrl>0</in_pkts_tagged_ctrl>
            <out_pkts_transform_error>0</out_pkts_transform_error>
            <out_pkts_control>41</out_pkts_control>
            <out_pkts_untagged>0</out_pkts_untagged>
            <rx_sa_an>1</rx_sa_an>
            <in_pkts_unchecked>0</in_pkts_unchecked>
            <in_pkts_delayed>0</in_pkts_delayed>
            <in_pkts_late>0</in_pkts_late>
            <in_pkts_ok>1</in_pkts_ok>
            <in_pkts_invalid>0</in_pkts_invalid>
            <in_pkts_not_valid>0</in_pkts_not_valid>
            <in_pkts_not_using_sa>0</in_pkts_not_using_sa>
            <in_pkts_unused_sa>0</in_pkts_unused_sa>
            <in_octets_decrypted>223</in_octets_decrypted>
            <in_octets_validated>0</in_octets_validated>
            <tx_sa_an>1</tx_sa_an>
            <out_pkts_encrypted_protected>1</out_pkts_encrypted_protected>
            <out_pkts_too_long>0</out_pkts_too_long>
            <out_pkts_sa_not_inuse>0</out_pkts_sa_not_inuse>
            <out_octets_encrypted_protected>223</out_octets_encrypted_protected>
           </ROW_statistics>
          </TABLE_statistics>
         </__readonly__>
        </__XML__OPT_Cmd_some_macsec_secy_statistics___readonly__>
       </__XML__INTF_ifname>
      </interface>
     </statistics>
    </secy>
   </macsec>
  </show>
 </nf:data>
</nf:rpc-reply>
]]>]]>
```

例 7：MACsec の実行コンフィギュレーション情報を表示します。

```
switch# show running-config macsec | xml

!Command: show running-config macsec
!Time: Fri Jan 20 07:12:34 2017

version 7.0(3)I4(6)
****************************************
This may take time. Please be patient.
****************************************
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cis
co.com/nxos:7.0.3.I4.6.:configure_" xmlns:m="http://www.cisco.com/nxos:7.0.3.I4.
6.:_exec" xmlns:m1="http://www.cisco.com/nxos:7.0.3.I4.6.:configure__macsec-poli
cy" xmlns:m2="http://www.cisco.com/nxos:7.0.3.I4.6.:configure__if-eth-non-member
" message-id="1">
  <nf:get-config>
    <nf:source>
      <nf:running/>
    </nf:source>
    <nf:filter>
      <m:configure>
        <m:terminal>
          <feature>
            <macsec/>
          </feature>
          <macsec>
```

```
                <policy>
                  <__XML__PARAM__policy_name>
                    <__XML__value>am2</__XML__value>
                    <m1:cipher-suite>
                      <m1:__XML__PARAM__suite>
                        <m1:__XML__value>GCM-AES-XPN-256</m1:__XML__value>
                      </m1:__XML__PARAM__suite>
                    </m1:cipher-suite>
                    <m1:key-server-priority>
                      <m1:__XML__PARAM__pri>
                        <m1:__XML__value>0</m1:__XML__value>
                      </m1:__XML__PARAM__pri>
                    </m1:key-server-priority>
<m1:window-size>
<m1:__XML__PARAM__size>
                        <m1:__XML__value>512</m1:__XML__value>
                      </m1:__XML__PARAM__size>
                    </m1:window-size>
                    <m1:conf-offset>
                      <m1:__XML__PARAM__offset>
                        <m1:__XML__value>CONF-OFFSET-0</m1:__XML__value>
                      </m1:__XML__PARAM__offset>
                    </m1:conf-offset>
                    <m1:security-policy>
                      <m1:__XML__PARAM__policy>
                        <m1:__XML__value>must-secure</m1:__XML__value>
                      </m1:__XML__PARAM__policy>
                    </m1:security-policy>
                    <m1:sak-expiry-time>
                      <m1:__XML__PARAM__ts>
                        <m1:__XML__value>60</m1:__XML__value>
                      </m1:__XML__PARAM__ts>
                    </m1:sak-expiry-time>
                  </__XML__PARAM__policy_name>
                </policy>
              </macsec>
              <interface>
                <__XML__PARAM__interface>
                  <__XML__value>Ethernet2/1</__XML__value>
                  <m2:macsec>
                    <m2:keychain>
                      <m2:__XML__PARAM__keychain_name>
                        <m2:__XML__value>kc2</m2:__XML__value>
                        <m2:policy>
                          <m2:__XML__PARAM__policy_name>
                            <m2:__XML__value>am2</m2:__XML__value>
                          </m2:__XML__PARAM__policy_name>
                        </m2:policy>
                      </m2:__XML__PARAM__keychain_name>
                    </m2:keychain>
                  </m2:macsec>
                </__XML__PARAM__interface>
              </interface>

[TRUNCATED FOR READABILITY]

<interface>
                <__XML__PARAM__interface>
                  <__XML__value>Ethernet4/31</__XML__value>
                  <m2:macsec>
                    <m2:keychain>
                      <m2:__XML__PARAM__keychain_name>
                        <m2:__XML__value>kc2</m2:__XML__value>
                        <m2:policy>
```

```
                        <m2:__XML__PARAM__policy_name>
                          <m2:__XML__value>am2</m2:__XML__value>
                        </m2:__XML__PARAM__policy_name>
                      </m2:policy>
                    </m2:__XML__PARAM__keychain_name>
                  </m2:keychain>
                </m2:macsec>
              </__XML__PARAM__interface>
            </interface>
          </m:terminal>
        </m:configure>
      </nf:filter>
    </nf:get-config>
</nf:rpc>
]]>]]>
```

MIB

MACsec は次の MIB をサポートします。

- IEEE8021-SECY-MIB
- CISCO-SECY-EXT-MIB

サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください：https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html。

関連資料

関連項目	マニュアル タイトル
キーチェーン管理	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
システム メッセージ	Cisco Nexus 9000 シリーズ NX-OS システム メッセージ リファレンス

関連資料

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。