



MACsec の設定

この章では、Cisco NX-OS デバイスに MACsec を設定する手順について説明します。

- [MACsec について \(1 ページ\)](#)
- [MACsec の注意事項と制約事項 \(2 ページ\)](#)
- [MACsec の有効化 \(7 ページ\)](#)
- [MACsec の無効化 \(7 ページ\)](#)
- [MACsec キーチェーンとキーの設定 \(8 ページ\)](#)
- [MACsec パケット番号の消耗 \(10 ページ\)](#)
- [MACsec フォールバック キーの設定 \(11 ページ\)](#)
- [MACsec ポリシーの設定 \(12 ページ\)](#)
- [PSK のローテーション \(14 ページ\)](#)
- [設定可能な EAPOL の宛先とイーサネットタイプについて \(15 ページ\)](#)
- [MACsec 設定の確認 \(17 ページ\)](#)
- [MACsec 統計の表示 \(19 ページ\)](#)
- [MACsec の設定例 \(22 ページ\)](#)
- [XML の例 \(24 ページ\)](#)
- [MIB \(32 ページ\)](#)
- [関連資料 \(32 ページ\)](#)

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、転送できません（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（8 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（11 ページ）](#) を参照してください。

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。

- Cisco Nexus リリース 10.2(1) 以降、MACsec は Cisco Nexus N9K-X9716D-GX でサポートされます。

- Cisco Nexus リリース 10.1(1) 以降、MACsec は Cisco Nexus N9K-C9336C-FX2-E でサポートされます。
- 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） access and trunk
 - 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、FX3、および GX2 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 および Cisco Nexus 3264C-E 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 N9K-C9364C、N9K-C9332C、および N9K-C9348GC-FXP プラットフォーム 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。
 - N9K-C9364C : MACsec は N9K-C9364C の次の 16 ポートでサポートされ、緑色でマークされます (ポート 49 ~ 64)。
 - N9K-C9332C : MACsec は N9K-C9332C の次の 8 ポートでサポートされ、緑色でマークされます (ポート 25 ~ 32)。
 - N9K-C9348GC-FXP : MACsec は、N9K-C9348GC-FXP の次の 6 ポート (ポート 49 ~ 54) でサポートされます。



注 Cisco N9K-C9364C および N9K-9332C プラットフォーム スイッチでは、MACsec がポートで設定または未設定の場合、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 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。
- Cisco NX-OS リリース 9.3(1) では、Cisco Nexus 9332C および 9364C シリーズ スイッチでは EAPOL 設定はサポートされていません。
- 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) 以降では、MACsec は次でサポートされます。
 - Cisco Nexus N9K-C93180YC-FX3S スイッチ。MACsec は、すべてのポートでサポートされています。
 - Cisco N9K-X9732C-FX および Cisco N9K-X9788TC-FX ラインカード
- Cisco Nexus 9300-FX2 ファミリ スイッチは、ベアヴァレーポートが 1G 速度で動作する場合を除き、すべてのポートで MACsec をサポートします。
- MACsec は、Cisco Nexus N9K-C93240YC-FX2、N9K-C93336C-FX2、N9K-C93108TC-FX、N9K-C93180YC-FX プラットフォーム スイッチ、および N9K-X9736C-FX および N9K-X9732C-EXM ラインカードでサポートされています。

- 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 N9K-C9336C-FX2、N9K-C9336C-FX2-E、および N9K-C9364C プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 9.3(7) 以降では、QSA が使用されている場合、MACsec は Cisco Nexus N9K-C9364C および N9K-C9336C-FX2 プラットフォーム スイッチでサポートされます。

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せん。

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 `secyRxSASStatsOKPkts`、`secyTxSASStatsProtectedPkts`、および `secyTxSASStatsEncryptedPkts` 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。

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 ボックスでは、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 タイプの一意的な組み合わせを 1 つだけ設定できます。
- 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 - 0x599 の範囲のイーサネット タイプの範囲が無効です。
- 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 : 0xff0、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
- N9K-X9736C-FX、N9K-C9348GC-FXP、N9K-C93180YC-FX、N9K-C93108TC-FX、N9K-X9732C-FX、および N9K-X9788TC-FX プラットフォーム スイッチは、1G ポートで MACsec をサポートしていません。MACsec は 1G ポートを有する mac ブロックのポートではサポートされません。

- MACSEC対応モジュールで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。
- ポートチャネルメンバーごとの MACsec 設定サポートなしで Cisco NX-OS リリース 9.3(1) から Cisco NX-OS リリースにダウングレードしようとした場合、同じポートチャネルインターフェイスのメンバーに異なる MACsec 設定がある場合その他の場合は、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	実行設定を、スタートアップ設定にコピーします。

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 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 2	<p>(任意) [no] key-chain macsec-psk no-show</p> <p>例 :</p> <pre>switch(config)# key-chain macsec-psk no-show</pre>	<p>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。</p> <p>(注) オクテット文字列は、設定をファイルに保存するときにも非表示になります。</p>
ステップ 3	<p>key chain name macsec</p> <p>例 :</p> <pre>switch(config)# key chain 1 macsec switch(config-macseckeychain)#</pre>	<p>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。</p>
ステップ 4	<p>key key-id</p> <p>例 :</p> <pre>switch(config-macseckeychain)# key 1000 switch(config-macseckeychain-macseckey)#</pre>	<p>MAC secキーを作成し、MACsec キー設定モードを開始します。範囲は1-32 オクテットで、最大サイズは 64 です。</p> <p>(注) キーの文字数は偶数でなければなりません。</p>
ステップ 5	<p>key-octet-string octet-string cryptographic-algorithm {AES_128_CMAC AES_256_CMAC}</p> <p>例 :</p> <pre>switch(config-macseckeychain-macseckey)# key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC</pre>	<p>そのキーの octet ストリングを設定します。<i>octet-string</i> 引数には、最大 64 文字の 16 進数文字を含めることができます。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。</p> <p>キーオクテット文字列には、次のものが含まれます。</p> <ul style="list-style-type: none"> • 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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> 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 <p>(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。</p>
ステップ 6	send-lifetime 開始時間 duration 長さ 例 : <pre>switch(config-macseckeychain-macseckey) # send-lifetime 00:00:00 Oct 04 2016 duration 100000</pre>	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。 <i>start-time</i> 引数は、キーがアクティブになる日時です。 <i>duration</i> 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 : <pre>switch(config-macseckeychain-macseckey) # show key chain 1</pre>	キーチェーンの設定を表示します。
ステップ 8	(任意) copy running-config startup-config 例 : <pre>switch(config-macseckeychain-macseckey) # copy running-config startup-config</pre>	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-XPB-128 または GCM-AES-XPB-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費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 XPB 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： <pre>switch# configure terminal switch(config)#</pre>	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 name 例： <pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>	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： <pre>switch(config-if)# macsec keychain kc2 policy abc fallback-keychain fb_kc2</pre>	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

	コマンドまたはアクション	目的
		<p>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。</p> <p>(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。</p> <p>「MACsec キーチェーンとキーの設定」を参照してください。</p>
ステップ 4	<p>(任意) copy running-config startup-config</p> <p>例 :</p> <pre>switch(config-if)# copy running-config startup-config</pre>	実行設定を、スタートアップ設定にコピーします。

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	<p>configure terminal</p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>	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	<p>macsec policy name</p> <p>例 :</p> <pre>switch(config)# macsec policy abc switch(config-macsec-policy)#</pre>	MACsec ポリシーを作成します。

	コマンドまたはアクション	目的
ステップ 3	cipher-suite name 例 : <pre>switch(config-macsec-policy)# cipher-suite GCM-AES-256</pre>	GCM-AES-128、GCM-AES-256、GCM-AES-XPN-128、または GCM-AES-XPN-256 のいずれかを設定します。
ステップ 4	key-server-priority number 例 : <pre>switch(config-macsec-policy)# key-server-priority 0</pre>	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）～255（最低）で、デフォルト値は16です。
ステップ 5	security-policy name 例 : <pre>switch(config-macsec-policy)# security-policy should-secure</pre>	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。 <ul style="list-style-type: none"> • 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 6	window-size number 例 : <pre>switch(config-macsec-policy)# window-size 512</pre>	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設定します。範囲は0～596000000です。
ステップ 7	sak-expiry-time time 例 : <pre>switch(config-macsec-policy)# sak-expiry-time 100</pre>	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。
ステップ 8	conf-offset name 例 : <pre>switch(config-macsec-policy)# conf-offset CONF-OFFSET-0</pre>	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。

	コマンドまたはアクション	目的
ステップ 9	(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 10	(任意) copy running-config startup-config 例： switch(config-macsec-policy)# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

PSK のローテーション

SAK の有効期限が MACsec ポリシーで 60 秒に設定されている場合は、次の手順に従って PSK を切り替えます。

手順

ステップ 1 MACsec ポリシーから SAK 期限切れタイマーを削除するには、**no sak-expiry-time** コマンドを使用します。

(注) 設定内のポリシーの数だけ、SAK の有効期限タイマーを削除する必要があります。インターフェイスごとに削除する必要はありません。ポリシーを1つだけ定義してすべてのインターフェイスに適用した場合は、このポリシーからのみ SAK の有効期限タイマーを削除する必要があります。

ステップ 2 2 分間待機します。

ステップ 3 **key key-id** コマンドを使用して、キーチェーンの下に新しいキーをプログラムします。

ステップ 4 新しいキーとのセッションが保護されたら、**no key key-id** コマンドを使用して古いキーを削除します。

ステップ 5 2 分間待機します。

ステップ 6 SAK キー再生成タイマーを MACsec ポリシーに追加するには、**sak-expiry-timer 60** コマンドを使用します。

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 : <pre>switch# configure terminal switch(config)#</pre>	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 name 例 : <pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>	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	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。

	コマンドまたはアクション	目的
		(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 [<i>ethertype eth_type</i>]	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： <pre>switch(config-macseckeychain-macseckey)# copy running-config startup-config</pre>	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： <pre>switch# configure terminal switch(config)#</pre>	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 name 例： <pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>	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 [<i>ethertype eth_type</i>]	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： <pre>switch(config-macseckeychain-macseckey)# copy running-config startup-config</pre>	実行設定を、スタートアップ設定にコピーします。

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
<code>show key chain name</code>	キーチェーンの設定を表示します。
<code>show macsec mka session [interface type slot/port] [detail]</code>	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。
<code>show macsec mka session details</code>	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。
<code>show macsec mka summary</code>	MACsec MKA 設定を表示します。
<code>show macsec policy [policy-name]</code>	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。
<code>show running-config macsec</code>	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
poll              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-XPB-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
a05000101005e0e50510f005c4b5f5d0b5b070e234e4d01d0112175b5e 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 [<i>interface type slot/port</i>]	MACsec MKA 統計情報を表示します。
show macsec secy statistics [<i>interface type slot/port</i>]	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	1/100000000000000000
Ethernet2/14	1	1/100000000000000000

```

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-  Yes        tests2      keych2
  no keychain      XPN-256
Ethernet2/3      Secured   GCM-AES-  Yes        tests3      keyc3
  no keychain      256

```

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://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://ww.cisco.com/nxos:1.0">
  <nf:data>
    <show>

```



```

<__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

```


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://www.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>
                    </ROW_statistics>
                  </TABLE_statistics>
                </_readonly__>
              </_XML_OPT_Cmd_some_macsec_secy_statistics__readonly__>
            </interface>
          </statistics>
        </secy>
      </macsec>
    </show>
  </nf:data>
</nf:rpc-reply>
```

```

    <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.cisco.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-policy" 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>
</interface>

```

```

        </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 を検索してダウンロードするには、
<ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html> にアクセスします。

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