



OSPFv3 認証トレーラの設定

- [OSPFv3 認証トレーラに関する情報 \(1 ページ\)](#)
- [OSPFv3 認証トレーラの設定方法 \(2 ページ\)](#)
- [OSPFv3 認証トレーラの設定例 \(4 ページ\)](#)
- [OSPFv3 認証トレーラに関する追加情報 \(6 ページ\)](#)
- [OSPFv3 認証トレーラの機能情報 \(6 ページ\)](#)

OSPFv3 認証トレーラに関する情報

OSPFv3 認証トレーラ機能 (RFC 7166 で定義されている) は、Open Shortest Path First バージョン 3 (OSPFv3) プロトコルパケットを認証する代替メカニズムを提供します。OSPFv3 認証トレーラの前は、OSPFv3 IPsec (RFC 4552 で定義されている) がプロトコルパケットの認証を行う唯一のメカニズムでした。OSPFv3 認証トレーラ機能は、シーケンス番号を介したパケットリプレイ保護も提供し、プラットフォームに依存しません。

非 IPsec 暗号化認証を実行するため、デバイスは OSPFv3 パケットの末尾に特別なデータブロック (認証トレーラ) を追加します。認証トレーラの長さは OSPFv3 パケットの長さに含まれず、IPv6 ペイロード長に含まれます。リンクローカルシグナリング (LLS) ブロックは OSPFv3 hello パケットおよびデータベース記述パケットの **OSPFv3 Options** フィールドの L-bit 設定で確立されます。存在する場合、LLS データブロックは OSPFv3 パケットとともに暗号化認証計算に含まれます。

新しい認証トレーラビットは **OSPFv3 Options** フィールドに導入されています。OSPFv3 デバイスは、このリンク上のすべてのパケットに認証トレーラが含まれていることを示すため、OSPFv3 hello パケットおよびデータベース記述パケットで認証トレーラビットを設定する必要があります。OSPFv3 hello パケットおよびデータベース記述パケットの場合、認証トレーラビットは認証トレーラが存在することを示します。他の OSPFv3 パケットタイプでは、OSPFv3 hello およびデータベース記述設定の OSPFv3 認証トレーラビット設定は OSPFv3 ネイバーデータ構造に保持されます。**OSPFv3 Options** フィールドを含まない OSPFv3 パケットタイプでは、ネイバーデータ構造の設定を使用して認証トレーラが必要かどうかを決定します。認証トレーラビットは、認証トレーラを含むすべての OSPFv3 hello パケットおよびデータベース記述パケットで設定する必要があります。

認証トレーラを設定するには、OSPFv3 では既存の Cisco IOS **key chain** コマンドを使用します。発信 OSPFv3 パケットでは、次のルールを使用してキーチェーンからキーを選択します。

- 最後に期限切れになるキーを選択します。
- 2つのキーの終了時間が同じ場合、最も大きいキー ID のキーを選択します。

セキュリティアソシエーション ID は認証アルゴリズムと秘密鍵にマッピングされ、メッセージダイジェストの生成および検証に使用されます。認証が設定されていても、最後の有効なキーが期限切れになると、パケットはそのキーを使用して送信されます。syslog メッセージも生成されます。有効なキーが使用できない場合は、トレーラ認証なしでパケットが送信されず。パケットが受信されると、そのキーのデータを検索するためにキー ID が使用されます。キーチェーンにキー ID が見つからない、またはセキュリティアソシエーションが有効でない場合、パケットはドロップされます。そうでない場合、パケットはキー ID で設定されたアルゴリズムとキーを使用して検証されます。キーチェーンはキーのライフタイムを使用するロールオーバーをサポートします。新しいキーは、将来設定する開始時間の送信でキーチェーンに追加できます。この設定により、キーが実際に使用される前に新しいキーをすべてのデバイスで設定できます。

hello パケットの優先順位はその他の OSPFv3 パケットより高いため、発信インターフェイスで順序変更することができます。この再順序付けにより、隣接デバイスでシーケンス番号の検証に関する問題が発生することがあります。シーケンスの不一致を防ぐには、OSPFv3 でパケットタイプごとに個別にシーケンス番号を検証します。認証手順の詳細については、RFC 7166 を参照してください。

ネットワークでの認証トレーラ機能の初期ロールオーバー時に、認証ルートで設定されているデバイスと展開モードを使用してまだ設定されていないデバイスの隣接関係を維持できます。**authentication mode deployment** コマンドを使用して展開モードが設定されている場合、パケットの処理が異なります。発信パケットの場合は、認証トレーラが設定されていても、OSPF チェックサムが計算されます。着信パケットの場合は、認証トレーラのないパケットまたは認証ハッシュが正しくないパケットはドロップされます。展開モードでは、**show ospfv3 neighbor detail** コマンドによって最後のパケット認証ステータスが表示されます。**authentication mode normal** コマンドを使用して通常モードに設定する前に、この情報を使用して、認証トレーラ機能が動作しているかどうかを確認できます。

OSPFv3 認証トレーラの設定方法

OSPFv3 認証トレーラを設定するには、次の手順を実行します。

始める前に

OSPFv3 認証トレーラを設定するには、認証キーが必要です。認証キーの設定の詳細については、「プロトコル独立機能」の「認証キーの設定方法」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	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>type number</i> 例： Device(config)# interface GigabitEthernet 2/0/1	インターフェイスタイプおよび番号を指定します。
ステップ 4	ospfv3 [<i>pid</i>] [<i>ipv4</i> <i>ipv6</i>] authentication { key-chain <i>chain-name</i> null } 例： Device(config-if)# ospfv3 1 <i>ipv6</i> authentication key-chain <i>ospf-1</i>	OSPFv3 インターフェイスの認証タイプを指定します。
ステップ 5	router ospfv3 [<i>process-id</i>] 例： Device(config-if)# router ospfv3 1	OSPFv3 ルータ コンフィギュレーション モードを開始します。
ステップ 6	address-family ipv6 unicast 例： Device(config-router)# address-family <i>ipv6</i> unicast	OSPFv3 プロセスに IPv6 アドレス ファミリを設定し、IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 7	area <i>area-id</i> authentication { key-chain <i>chain-name</i> null } 例： Device(config-router-af)# area 1 authentication key-chain <i>ospf-chain-1</i>	OSPFv3 エリア内のすべてのインターフェイスの認証トレーラを設定します。
ステップ 8	area <i>area-id</i> virtual-link <i>router-id</i> authentication key-chain <i>chain-name</i> 例： Device(config-router-af)# area 1 virtual-link 1.1.1.1 authentication key-chain <i>ospf-chain-1</i>	仮想リンクの認証を設定します。
ステップ 9	area <i>area-id</i> sham-link <i>source-address</i> <i>destination-address</i> authentication key-chain <i>chain-name</i> 例：	模造リンクの認証を設定します。

	コマンドまたはアクション	目的
	Device(config-router-af)# area 1 sham-link 1.1.1.1 1.1.1.0 authentication key-chain ospf-chain-1	
ステップ 10	authentication mode {deployment normal} 例： Device(config-router-af)# authentication mode deployment	(任意) OSPFv3 インスタンスに使用する認証のタイプを指定します。 deployment キーワードは、認証を設定済みのデバイスと未設定のデバイス間の隣接関係を表示します。
ステップ 11	end 例： Device(config-router-af)# end	IPv6 アドレス ファミリ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 12	show ospfv3 interface 例： Device# show ospfv3	(任意) OSPFv3 関連のインターフェイス情報を表示します。
ステップ 13	show ospfv3 neighbor [detail] 例： Device# show ospfv3 neighbor detail	(任意) OSPFv3 ネイバー情報をインターフェイスごとに表示します。
ステップ 14	debug ospfv3 例： Device# debug ospfv3	(任意) OSPFv3 のデバッグ情報を表示します。

OSPFv3 認証トレーラの設定例

ここでは、OSPFv3 認証トレーラを設定する方法と OSPFv3 認証トレーラの設定を確認する方法の例を示します。

例：OSPFv3 認証トレーラの設定

次に、ギガビットイーサネットインターフェイス 1/0/1 で認証トレーラを定義する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ospfv3 1 ipv6 authentication key-chain ospf-1
Device(config-if)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)# area 1 authentication key-chain ospf-1
Device(config-router-af)# area 1 virtual-link 1.1.1.1 authentication key-chain ospf-1
```

```
Device(config-router-af)# area 1 sham-link 1.1.1.1 authentication key-chain ospf-1
Device(config-router-af)# authentication mode deployment
Device(config-router-af)# end
Device(config)# key chain ospf-1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ospf
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-256
!
```

例：OSPFv3 認証トレーラの確認

次に、**show ospfv3** コマンドの出力例を示します

```
Device# show ospfv3
  OSPFv3 1 address-family ipv6
  Router ID 1.1.1.1
  ...
  RFC1583 compatibility enabled
  Authentication configured with deployment key lifetime
  Active Key-chains:
    Key chain ospf-1: Send key 1, Algorithm HMAC-SHA-256, Number of interfaces 1
    Area BACKBONE(0)
```

次に、**show ospfv3 neighbor detail** コマンドの出力例を示します

```
Device# show ospfv3 neighbor detail
OSPFv3 1 address-family ipv6 (router-id 2.2.2.2)
Neighbor 1.1.1.1
  In the area 0 via interface GigabitEthernet0/0
  Neighbor: interface-id 2, link-local address FE80::A8BB:CCFF:FE01:2D00
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 2.2.2.2 BDR is 1.1.1.1
  Options is 0x000413 in Hello (V6-Bit, E-Bit, R-Bit, AT-Bit)
  Options is 0x000413 in DBD (V6-Bit, E-Bit, R-Bit, AT-Bit)
  Dead timer due in 00:00:33
  Neighbor is up for 00:05:07
  Last packet authentication succeed
  Index 1/1/1, retransmission queue length 0, number of retransmission 0
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 0, maximum is 0
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

次に、**show ospfv3 interface** コマンドの出力例を示します

```
Device# show ospfv3 interface
GigabitEthernet1/0/1 is up, line protocol is up
  Cryptographic authentication enabled
  Sending SA: Key 25, Algorithm HMAC-SHA-256 - key chain ospf-1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

OSPFv3 認証トレーラに関する追加情報

関連資料

関連項目	マニュアルタイトル
OSPF 機能の設定	IP ルーティング : OSPF 設定ガイド

標準および RFC

標準/RFC	マニュアルタイトル
RFC 7166	OSPFv3 認証トレーラのサポートに関する RFC
RFC 6506	OSPFv3 認証トレーラのサポートに関する RFC
RFC 4552	OSPFv3 の認証/機密性に関する RFC

OSPFv3 認証トレーラの機能情報

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

表 1: OSPFv3 認証トレーラの機能情報

機能名	リリース	機能情報
OSPFv3 認証トレーラ	Cisco IOS XE Fuji 16.8.1a	OSPFv3 認証トレーラ機能は、既存の OSPFv3 IPsec 認証の代替として OSPFv3 プロトコル パケットを認証するメカニズムを提供します。

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。