MPLS-TE への RSVP の実装

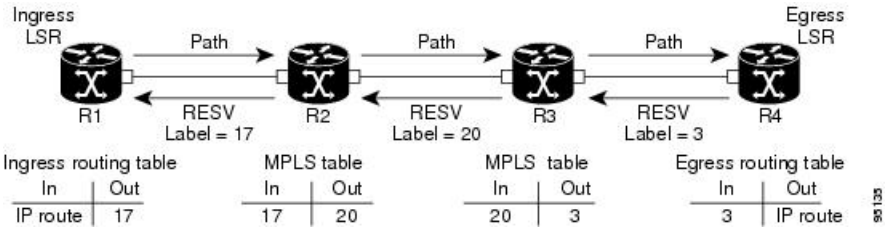
リソース予約プロトコル（RSVP）は、システムによるネットワークからのリソース予約要求を可能にするシグナリング プロトコルです。RSVP は、他のシステムからのプロトコル メッセージを処理し、ローカル クライアントからのリソース要求を処理して、プロトコル メッセージを生成します。結果として、リソースは、ローカルおよびリモート クライアントの代わりにデータ フローに予約されます。RSVP は、これらのリソース予約を作成、保守および削除します。

MPLS トラフィック エンジニアリング（MPLS-TE）はトポロジとネットワーク内で使用可能なリソースを学習し、帯域幅などのリソース要件とネットワーク リソースに基づいてトラフィック フローを特定のパスにマッピングします。MPLS TE では、ラベル スイッチド パス（LSP）の形でソースから宛先への単方向トンネルが構築され、その後トラフィックの転送で使用されます。MPLS-TE では、RSVP を使用して LSP をシグナリングします。

RSVP を使用した MPLS LSP の設定

次の図は、MPLS 環境で TE に使用できるルータ R4 を介してルータ R1 から LSP が RSVP によってどのように設定されるかを示しています。

図 *1 : RSVP* を使用した *MPLS LSP*



LSP の設定は LSP のヘッドノードが、テールノードにパスメッセージを送信すると開始されます。パスメッセージにより、各ノードへのパスに沿ってリソースが予約され、各ノードでセッ

ションに関連付けられたパスステートが作成されます。テール ノードがパス メッセージを受信すると、ラベル付きの予約（RESV）メッセージを直前のノードに戻します。各ルータの予約状態はソフト状態と見なされます。つまり、状態を維持するためには、各ホップで定期的なPATH メッセージと RESV メッセージを送信する必要があります。

予約メッセージが直前のノードに到着すると、予約されたリソースがロックされ、転送エントリが、テールエンドノードから送信されるMPLSラベルでプログラムされます。新しいMPLSラベルが割り当てられ、次のノードのアップストリームに送信されます。予約メッセージがヘッドノードに到着すると、ラベルがプログラムされ、MPLSデータがパスに送信されます。

MPLS-TE 用 RSVP の機能の概要

このセクションでは、MPLS-TE 用 RSVP のさまざまな機能の概要を示します。

RSVPは、MPLS-TEが設定されるインターフェイスで自動的にイネーブルにされます。帯域幅を持つ MPLS-TE LSP では、RSVP 帯域幅をインターフェイスで設定する必要があります。すべての MPLS-TE LSP がゼロ帯域幅の場合、RSVP を設定する必要はありません。

RSVP グレースフルリスタートは、高可用性を確保し、RSVP TE 対応ルータでネットワーク障害後にネイバーから RSVP 状態情報を回復できるようにします。

RSVP では、リフレッシュメッセージを定期的に送信することによって、LSP シグナリング時に設定されるパスと予約状態を更新する必要があります。リフレッシュメッセージは、RSVPネイバー間で状態を同期するため、および失われたRSVPメッセージから情報を回復するために使用されます。RSVP リフレッシュ削減機能では、メッセージが失われた場合に迅速に送信される信頼性の高いメッセージをサポートしています。サマリー リフレッシュ メッセージには、多数の状態を更新し、状態の更新に必要なメッセージの数を減らすための情報が含まれています。

RSVP メッセージを認証して、信頼できるネイバーのみが予約を設定できるようにすることができます。

MPLS-TE用RSVPの機能の詳細については、「*MPLS-TE*機能に対する*RSVP*（詳細）」を参照してください。

MPLS-TE 用 RSVP の設定

RSVP は、いくつかのルータでの調整が必要で、LSP を設定するため RSVP メッセージの交換を確立します。RSVPを設定するには、次の2つのRPMをインストールする必要があります。

- ncs540-mpls-2.0.0.0-r601.x86_64.rpm-6.0.1
- ncs540-mpls-te-rsvp-2.0.0.0-r601.x86_64.rpm-6.0.1

要件に応じて、RSVP では、次のトピックで説明するいくつかの基本設定が必要です。

RSVP メッセージ認証のグローバル設定

RSVP 認証機能により、RSVP ネットワークのネイバーは、安全なハッシュアルゴリズムを使用して、すべての RSVP シグナリングメッセージをデジタルで認証できます。この認証は、RSVP メッセージの RSVP インテグリティオブジェクトを使用して RSVP ホップごとに実行されます。インテグリティ オブジェクトには、キー ID、メッセージのシーケンス番号、およびキー付きメッセージ ダイジェストが含まれています。

キーチェーン、信頼できる他の RSVP ネイバーとのセキュリティアソシエーションを RSVP が保持する期間（ライフタイム）、順序が正しくなくても受信できる RSVP 認証済みメッセージの最大数（ウィンドウサイズ）など、認証パラメータの値をグローバルに設定できます。これらのデフォルトは、各ネイバーまたはインターフェイスで継承されます。

設定例

この例では、ルータで認証パラメータをグローバルに設定しています。認証キーチェーン、ライフタイム、ウィンドウサイズを含む認証パラメータを設定しています。このタスクを実行する前に、有効なキーチェーンを設定する必要があります。

```
RP/0/RP0/cpu 0: router# configure
RP/0/RP0/cpu 0: router(config)# key chain mpls-keys
RP/0/RP0/cpu 0: router(config-mpls-keys)# exit
RP/0/RP0/cpu 0: router(config)# rsvp authentication
RP/0/RP0/cpu 0: router(config-rsvp-auth)# key-source key-chain mpls-keys
RP/0/RP0/cpu 0: router(config-rsvp-auth)# life-time 2000
RP/0/RP0/cpu 0: router(config-rsvp-auth)# window-size 33
```

確認

次のコマンドを使用して、認証パラメータの設定を確認します。

```
RP/0/RP0/cpu 0: router# show rsvp authentication detail

  RSVP Authentication Information:
    Source Address:          3.0.0.1
    Destination Address:     3.0.0.2
    Neighbour Address:       3.0.0.2
    Interface:               HundredGigabitEthernet 0/0/0/3
    Direction:               Send
    LifeTime:                2000 (sec)
    LifeTime left:           1305 (sec)
    KeyType:                 Static Global KeyChain
    Key Source:              mpls-keys
    Key Status:              No error
    KeyID:                   1
    Digest:                  HMAC MD5 (16)
    window-size:             33
Challenge:               Not supported
    TX Sequence:             5023969459702858020 (0x45b8b99b00000124)
    Messages successfully authenticated:    245
    Messages failed authentication:         0
```

関連項目

- インターフェイスでの RSVP 認証の設定 （4 ページ）
- ネイバーでの RSVP 認証の設定 （5 ページ）

- #unique_60

インターフェイスでの RSVP 認証の設定

インターフェイスで、キーチェーン、ライフタイム、ウィンドウサイズを含むRSVP認証パラメータの値を個別に設定できます。インターフェイス固有の認証パラメータは、2 つの RSVP ネイバー間で特定のインターフェイスのセキュリティを確保するために使用します。

設定例

この例では、インターフェイスで、認証キーチェーン、セキュリティアソシエーションのライフタイム、およびウィンドウサイズを設定しています。有効なキーチェーンが、このタスクの一部として使用できるようにすでに設定されている必要があります。

```
RP/0/RP0/cpu 0: router# configure
RP/0/RP0/cpu 0: router(config)# rsvp interface HundredGigabitEthernet0/0/0/3
RP/0/RP0/cpu 0: router(config-rsvp-if)# authentication
RP/0/RP0/cpu 0: router(config-rsvp-if-auth)# key-source key-chain mpls-keys
RP/0/RP0/cpu 0: router(config-rsvp-if-auth)# life-time 2000
RP/0/RP0/cpu 0: router(config-rsvp-if-auth)# window-size 33
RP/0/RP0/cpu 0: router(config)# commit
```

確認

次のコマンドを使用して、認証パラメータの設定を確認します。

```
RP/0/RP0/cpu 0: router# show rsvp authentication detail

  RSVP Authentication Information:
    Source Address:         3.0.0.1
    Destination Address:    3.0.0.2
    Neighbour Address:      3.0.0.2
    Interface:              HundredGigabitEthernet 0/0/0/3
    Direction:              Send
    LifeTime:               2000 (sec)
    LifeTime left:          1305 (sec)
    KeyType:                Static Global KeyChain
    Key Source:             mpls-keys
    Key Status:             No error
    KeyID:                  1
    Digest:                 HMAC MD5 (16)
    window-size:            33
    Challenge:              Not supported
    TX Sequence:            5023969459702858020 (0x45b8b99b00000124)
    Messages successfully authenticated:    245
    Messages failed authentication:         0
```

関連項目

- RSVP メッセージ認証のグローバル設定 （3 ページ）
- ネイバーでの RSVP 認証の設定 （5 ページ）
- #unique_60

ネイバーでの RSVP 認証の設定

ネイバーで、キーチェーン、ライフタイム、ウィンドウサイズを含むRSVP認証パラメータの値を個別に設定できます。

設定例

この例では、RSVPネイバーで、認証キーチェーン、セキュリティアソシエーションのライフタイム、およびウィンドウサイズを設定しています。有効なキーチェーンが、このタスクの一部として使用できるようにすでに設定されている必要があります。

```
RP/0/RP0/cpu 0: router# configure
RP/0/RP0/cpu 0: router(config)# rsvp neighbor 1.1.1.1 authentication
RP/0/RP0/cpu 0: router(config-rsvp-if-auth)# key-source key-chain mpls-keys
RP/0/RP0/cpu 0: router(config-rsvp-if-auth)# life-time 2000
RP/0/RP0/cpu 0: router(config-rsvp-if-auth)# window-size 33
RP/0/RP0/cpu 0: router(config)# commit
```

確認

次のコマンドを使用して、認証パラメータの設定を確認します。

```
RP/0/RP0/cpu 0: router# show rsvp authentication detail

  RSVP Authentication Information:
    Neighbour Address:      1.1.1.1
    Interface:              HundredGigabitEthernet 0/0/0/3
    Direction:              Send
    LifeTime:               2000 (sec)
    LifeTime left:          1205 (sec)
    KeyType:                Static Global KeyChain
    Key Source:             mpls-keys
    Key Status:             No error
    KeyID:                  1
    Digest:                 HMAC MD5 (16)
    window-size:            33
    Challenge:              Not supported
```

関連項目

- RSVP メッセージ認証のグローバル設定 （3 ページ）
- インターフェイスでの RSVP 認証の設定 （4 ページ）
- #unique_60

グレースフル リスタートの設定

RSVPグレースフルリスタートは、高可用性（HA）を確保するためのメカニズムを提供して、Cisco IOS XR ソフトウェアを実行するシステムで障害状態を検出および回復できるようにし、ノンストップ フォワーディング サービスを実現します。RSVP グレースフルリスタートは、RSVPhelloメッセージに基づいており、RSVPTE対応ルータでネットワーク障害後にネイバーから RSVP 状態情報を回復できるようにします。RSVP では、hello メッセージ内の Restart Cap オブジェクト（RSVPRESTART）を使用して、ノードの再起動機能をアドバタイズするために

再起動時間と回復時間を指定します。ネイバーノードは、再起動ノードのフォワーディングステートを回復するための Recover Label オブジェクトを送信することで、再起動ノードを支援します。

ノード ID アドレスベースの hello メッセージに基づく標準グレースフルリスタートを設定することも、インターフェイスアドレス ベースの hello メッセージに基づくインターフェイスベースのグレースフルリスタートを設定することもできます。

設定例

この例では、ネットワーク上のルータノードで RSVP-TE がすでに有効になっており、障害から回復できるようにルータノードでグレースフルリスタートが有効になっている必要があります。グレースフルリスタートを、有効なノード ID アドレスベースの hello メッセージに対してグローバルに設定し、インターフェイスアドレス ベースの hello メッセージをサポートするためにルータインターフェイスで設定します。

```
RP/0/RP0/cpu 0: router# configure
RP/0/RP0/cpu 0: router(config)# rsvp
RP/0/RP0/cpu 0: router(config-rsvp)# signalling graceful-restart
RP/0/RP0/cpu 0: router(config-rsvp)# interface HundredGigabitEthernet 0/0/0/3
RP/0/RP0/cpu 0: router(config-rsvp-if)# signalling graceful-restart
interface-based
RP/0/RP0/cpu 0: router(config)# commit
```

確認

次のコマンドを使用して、グレースフルリスタートが有効になっていることを確認します。

```
RP/0/RP0/cpu 0: router# show rsvp graceful-restart
 Graceful restart: enabled Number of global neighbors: 1
 Local MPLS router id: 192.168.55.55
 Restart time: 60 seconds  Recovery time: 120 seconds
 Recovery timer: Not running
 Hello interval: 5000 milliseconds Maximum Hello miss-count: 4

RP/0/RP0/cpu 0: router# show rsvp graceful-restart neighbors detail

 Neighbor: 192.168.77.77 Source: 192.168.55.55 (MPLS)
   Hello instance for application MPLS
     Hello State: UP        (for 00:20:52)
     Number of times communications with neighbor lost: 0
     Reason: N/A
Recovery State: DONE
   Number of Interface neighbors: 1
     address: 192.168.55.0
   Restart time: 120 seconds  Recovery time: 120 seconds
   Restart timer: Not running
   Recovery timer: Not running
   Hello interval: 5000 milliseconds  Maximum allowed missed Hello messages: 4
```

関連項目

- #unique_60

リフレッシュ削減の設定

RSVP リフレッシュ削減は、デフォルトで有効になっており、Resource Reservation Protocol（RSVP）シグナリングの信頼性を高めてネットワークのパフォーマンスとメッセージ配信の信頼性を向上します。リフレッシュ削減は、ネイバーでサポートされている場合に限り、ネイバーで使用されます。必要に応じて、インターフェイスでリフレッシュ削減を無効にすることもできます。

設定例

この例では、リフレッシュ削減機能で使用できるさまざまなパラメータを設定する方法を示します。

次のパラメータを設定して、そのデフォルト値を変更します。

- 更新間隔
- ノードで許容される、失われたリフレッシュメッセージの数
- 再送信時間
- 確認応答保持時間
- 確認応答メッセージのサイズ
- サマリー リフレッシュ メッセージのサイズ

```
RP/0/RP0/cpu 0: router# configure
RP/0/RP0/cpu 0: router(config)# rsvp
RP/0/RP0/cpu 0: router(config-rsvp)# interface HundredGigabitEthernet 0/0/0/3
RP/0/RP0/cpu 0: router(config-rsvp-if)# signalling refresh interval 40
RP/0/RP0/cpu 0: router(config-rsvp-if)# signalling refresh missed 6
RP/0/RP0/cpu 0: router(config-rsvp-if)# signalling refresh reduction reliable
retransmit-time 2000
RP/0/RP0/cpu 0: router(config-rsvp-if)# signalling refresh reduction reliable ack-hold-time
 1000
RP/0/RP0/cpu 0: router(config-rsvp-if)# signalling refresh reduction reliable ack-max-size
 1000
RP/0/RP0/cpu 0: router(config-rsvp-if)# signalling refresh reduction summary  max-size
1500
RP/0/RP0/cpu 0: router(config)# commit
```

ACL ベース プレフィックス フィルタリングの設定

拡張アクセス制御リスト（ACL）を設定して、RSVP ルータ アラート（RA）パケットで通常の処理を転送、ドロップ、または実行できます。各着信 RSVP RA パケットについて、RSVP では、IP ヘッダーを検査し、送信元 IP アドレスまたは宛先 IP アドレスと拡張 ACL で設定されたプレフィックスとの照合を行います。明示的な許可も明示的な拒否もない場合、デフォルトでは、ACL インフラストラクチャは暗黙的な拒否を返します。デフォルトでは、ACL 一致により暗黙的な（デフォルト）拒否が返された場合、RSVP によりパケットが処理されます。

設定例

この例では、RSVP RA パケットに対する ACL ベースのプレフィックス フィルタリングを設定します。RSVP で送信元アドレス 1.1.1.1 から RA パケットを受信した場合はそのパケットは転送され、IP アドレス 2.2.2.2 宛てのパケットはドロップされます。

```
RP/0/RP0/cpu 0: router# configure
RP/0/RP0/cpu 0: router(config)# ipv4 access-list rsvpac1
RP/0/RP0/cpu 0: router(config-ipv4-acl)# 10 permit ip host 1.1.1.1 any
RP/0/RP0/cpu 0: router(config-ipv4-acl)# 20 deny ip any host 2.2.2.2
RP/0/RP0/cpu 0: router(config)# rsvp
RP/0/RP0/cpu 0: router(config-rsvp)# signalling prefix-filtering access-list rsvp-acl
RP/0/RP0/cpu 0: router(config)# commit
```

確認

ACL ベース プレフィックス フィルタリングの設定の確認

```
RP/0/RP0/cpu 0: router# show rsvp counters prefix-filtering access-list rsvp-ac1

  ACL:rsvp-ac1            Forward          Local          Drop           Total
  Path                      0              0              0              0
  PathTear                  0              0              0              0
  ResvConfirm               0              0              0              0
  Total                     0              0              0
```

関連項目

- RSVP パケット ドロップの設定 （8 ページ）

RSVP パケット ドロップの設定

拡張アクセス制御リスト（ACL）を設定して、RSVP ルータ アラート（RA）パケットで通常の処理を転送、ドロップ、または実行できます。デフォルトでは、ACL との照合で暗黙的な拒否が返された場合でも、RSVP はその RA パケットを処理します。ACL との照合で暗黙的な拒否になった場合には RA パケットをドロップするように、RSVP を設定することもできます。

設定例

この例では、RSVP RA パケットに対する ACL ベースのプレフィックス フィルタリングを設定します。RSVP で送信元アドレス 1.1.1.1 から RA パケットを受信した場合はそのパケットは転送され、IP アドレス 2.2.2.2 宛てのパケットはドロップされます。ACL との照合で暗黙的な拒否になった場合には、RA パケットはドロップされます。

```
RP/0/RP0/cpu 0: router# configure
RP/0/RP0/cpu 0: router(config)# ipv4 access-list rsvpac1
RP/0/RP0/cpu 0: router(config-ipv4-acl)# 10 permit ip host 1.1.1.1 any
RP/0/RP0/cpu 0: router(config-ipv4-acl)# 20 deny ip any host 2.2.2.2
RP/0/RP0/cpu 0: router(config)# rsvp
RP/0/RP0/cpu 0: router(config-rsvp)# signalling prefix-filtering default-deny-action
RP/0/RP0/cpu 0: router(config)# commit
```

確認

次のコマンドを使用して、RSVP パケットドロップの設定を確認します。

```
RP/0/RP0/cpu 0: router# show rsvp counters prefix-filtering access-list rsvpac1

  ACL: rsvpac1            Forward          Local          Drop           Total
  Path                      4              1              0              5
  PathTear                  0              0              0              0
  ResvConfirm               0              0              0              0
  Total                     4              1              0              5
```

関連資料

- ACL ベース プレフィックス フィルタリングの設定 （7 ページ）

RSVP トラップの有効化

RSVP MIB を実装することで、SNMP を使用して、RSVP に属するオブジェクトにアクセスできます。また、新しいフローの作成または削除時にトリガーされる 2 つのトラップ（NewFlow と LostFlow）を指定できます。RSVP MIB は RSVP をオンにすると自動的に有効になりますが、RSVP トラップは別に有効にする必要があります。

設定例

この例は、フローが削除または作成された場合の RSVP MIB トラップを有効にする方法に加えて、両方のトラップを有効にする方法も示しています。

```
RP/0/RP0/cpu 0: router# configure
RP/0/RP0/cpu 0: router(config)# snmp-server traps rsvp lost-flow
RP/0/RP0/cpu 0: router(config)# snmp-server traps rsvp new-flow
RP/0/RP0/cpu 0: router(config)# snmp-server traps rsvp all
RP/0/RP0/cpu 0: router(config)# commit
```

MPLS-TE 用 RSVP の機能の詳細

RSVP グレースフルリスタートの動作

RSVP グレースフルリスタートは、RSVP hello メッセージに基づきます。hello メッセージは、ルータとそのネイバーノードの間で交換されます。各ネイバーノードは、hello 要求オブジェクトを含む hello メッセージを自律して発行できます。hello 拡張をサポートするレシーバは、hello 確認（ACK）オブジェクトを含む hello メッセージで応答します。送信側ノードが状態の回復をサポートしている場合、ノードの再起動機能を示す Restart Cap オブジェクトも hello メッセージで伝送されます。Restart Cap オブジェクトでは、再起動時間と回復時間が指定されています。再起動時間は、hello メッセージが失われてから RSVP hello セッションを再確立するまでの時間です。回復時間は、hello メッセージの再確立後に受信者が状態を再同期するまで送信側が待機する時間です。

グレースフル リスタートでは、hello メッセージは、64 の IP Time to Live（TTL）で送信されます。これは、hello メッセージの宛先が数ホップ離れることがあるためです。グレースフル リ

スタートがイネーブルで、RSVP ステートがネイバーと共有される場合、hello メッセージ（Restart Cap オブジェクトを含む）は RSVP ネイバーに送信されます。Restart Cap オブジェクトが RSVP ネイバーに送信される場合に、ネイバーが Restart Cap オブジェクトを含む hello メッセージで応答すると、そのネイバーはグレースフルリスタート可能と見なされます。ネイバーが hello メッセージに応答しない場合、または Restart Cap オブジェクトを含まない hello メッセージに応答した場合、RSVP は、そのネイバーへの hello の送信をバックオフします。hello Request メッセージが不明ネイバーから受信された場合、hello ACK は返されません。

RSVP 認証

ネットワーク管理者は、RSVP 要求を開始するシステムのセットを制御するセキュリティ ドメインを確立できる機能が必要です。RSVP 認証機能を使用すると、RSVP ネットワークのネイバーは、安全なハッシュを使用して、すべての RSVP シグナリング メッセージにデジタル署名できます。これにより、RSVP メッセージの受信側は、送信側の IP アドレスだけに頼ることなく、メッセージの送信側を確認できます。

署名は、RFC 2747 で定義されている RSVP メッセージの RSVP インテグリティ オブジェクトで RSVP ホップごとに実行されます。インテグリティ オブジェクトには、キー ID、メッセージのシーケンス番号、およびキー付きメッセージ ダイジェストが含まれています。この方式では、偽造やメッセージ改ざんに対する保護が提供されます。ただし、受信側で、受信した RSVP メッセージ内のデジタル署名を確認するためには、送信側で使用されたセキュリティ キーを取得する必要があります。ネットワーク管理者は、共有ネットワークの各 RSVP ネイバーで共有のキーを手動で設定します。送信側システムと受信側システムでは、共有する各認証キーのセキュリティ アソシエーションが維持されます。さまざまなセキュリティ アソシエーション パラメータの詳細については、**セキュリティ アソシエーション パラメータ**の表を参照してください。

キー、ウィンドウ サイズおよびライフタイムを含むすべての認証パラメータに対してグローバル デフォルトを設定できます。これらのデフォルトは、各ネイバーまたはインターフェイスで認証を設定するときに継承されます。ただし、これらのパラメータはネイバーまたはインターフェイスで個別で設定できますが、この場合はグローバル値（設定値またはデフォルト値）は継承されません。

インターフェイス モードおよびネイバー インターフェイス モードは、明示的に設定されていない限り、次のように、グローバル コンフィギュレーション モードからパラメータを継承します。

- ウィンドウ サイズは、1 に設定されます。
- 制限は 1800 に設定されます。
- key-source key-chain コマンドは、none またはディセーブルに設定されます。

次に、グローバル、インターフェイス、またはネイバー コンフィギュレーション モードの選択方法を示します。

- グローバル コンフィギュレーション モードは、ルータが単一のセキュリティ ドメインに属する場合に最適です（たとえば、プロバイダー コア ルータのセットの一部などです）。単一の共有キー セットは、すべての RSVP メッセージの認証に使用されます。

- インターフェイスまたはネイバー コンフィギュレーション モードは、ルータが複数のセキュリティ ドメインに属する場合に最適です。たとえば、プロバイダー ルータが、プロバイダーエッジ（PE）に隣接する場合や、PE がエッジデバイスに隣接する場合です。異なるキーを使用できますが、共有はできません。

セキュリティ アソシエーション（SA）は、ピアとの安全な通信を維持するために必要な情報のコレクションです。次の表に、セキュリティアソシエーションを定義する主要パラメータを示します。

表 *1*：セキュリティ アソシエーションのパラメータ

セキュリティ アソシエーションのパラメータ	説明
src	送信元の IP アドレス。
dst	最終的な宛先の IP アドレス。
interface	セキュリティアソシエーションのインターフェイス。
direction	セキュリティ アソシエーションの送信または受信タイプ。
Lifetime	未使用のセキュリティアソシエーションデータの収集に使用される有効期限タイマーの値。
Sequence Number	送信または受信（direction のタイプ）された最後のシーケンス番号。
key-source	設定可能パラメータのキーのソース。
keyID	最後に使用されたキー番号（key-source から返されます）。
Window Size	順序どおりでなくても受信できる認証済みメッセージの最大数を指定します。
Window	受信または受け入れられた最後の *window size* 値のシーケンス番号を指定します。