IKEv2 フラグメンテーションの設定

RFC 機能に準拠した IKE フラグメンテーションでは、IETF の **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネット キー エクスチェンジ バージョン 2 （IKEv2）パケットのフラグメンテーションを実装しました。

- 機能情報の確認 （1 ページ）
- IKEv2 フラグメンテーションの設定に関する情報 （1 ページ）
- IKEv2 フラグメンテーションの設定方法 （5 ページ）
- IKEv2 フラグメンテーションの設定例 （6 ページ）
- IKEv2 フラグメンテーションの設定に関する追加情報 （11 ページ）
- IKEv2 フラグメンテーションの機能情報 （12 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

IKEv2 フラグメンテーションの設定に関する情報

IKEv2 フラグメンテーション

インターネット キー エクスチェンジ バージョン 2（IKEv2）フラグメンテーション プロトコルは、大きな IKEv2 メッセージを IKE フラグメント メッセージと呼ばれる一連の小さなメッセージに分割します。IKEv2 リモート アクセスのヘッドエンド機能によって Cisco IOS ソフト

ウェアに実装されたIKEv2フラグメンテーション方式は、シスコ独自の方法であり、シスコ以外のピアとの相互運用性は制限されます。フラグメンテーションは、暗号化されたIKEv2パケットでのみ実行されます。そのため、ピアがすべてのフラグメントを受信するまで、ピアはメッセージを復号したり認証することはできません。RFCに準拠したIKEフラグメンテーション機能は、フラグメンテーション後にパケットを暗号化することによってIETF **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントを実装し、シスコ独自のフラグメンテーション方式を引き続きサポートしながらシスコ以外のピアとの相互運用性を実現します。

ピア間のネゴシエーション

RFC 機能に準拠した IKE フラグメンテーションから有効。IETF 標準フラグメンテーション方式のサポートが通知ペイロードとして IKE_SA_INIT メッセージに追加されました。一方、シスコ独自のフラグメンテーション方式は、同じIKE_SA_INIT メッセージ内で引き続きベンダーID ペイロードを使用します。フラグメンテーションが有効な場合、両方の方式が **show crypto ikev2 sa detail** コマンドで適切と表示されます。最大伝送ユニット（MTU）はローカルで設定され、メッセージ間のネゴシエーションも交換も行いません。INIT交換の後、いずれかの方式で設定されたネットワーク内のピアは、使用する必要がある認証方式と、AUTHメッセージをフラグメント化できるかどうかをを認識します。

次に、デバッグが有効で、INIT要求メッセージでのネゴシエーション機能を表している場合のデバイスからの出力例を示します。

```
*Oct 14 08:45:24.732: IKEv2:(SESSION ID = 0,SA ID = 1):Next payload: SA, version: 2.0
Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 524
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 144
…
Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP
NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) Next payload: VID, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: IKEV2_FRAGMENTATION_SUPPORTED
VID Next payload: NONE, reserved: 0x0, length: 20
```

上記の出力では、メッセージ内の IKEV2_FRAGMENTATION_SUPPORTED および VID 値によって、IETF 標準フラグメンテーション方式とシスコ独自のフラグメンテーション方式の両方をサポートすることを示す、発信側から応答側へのメッセージが INIT 要求に含まれます。

次に、デバッグが有効で、INIT応答メッセージでのネゴシエーション機能を表している場合のデバイスからの出力例を示します。

```
*Oct 14 08:45:24.732: IKEv2:(SESSION ID = 0,SA ID = 1):Next payload: SA, version: 2.0
Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 524
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 144
last proposal: 0x0, reserved: 0x0, length: 140
…
NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) Next payload: VID, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: IKEV2_FRAGMENTATION_SUPPORTED
<-------- Response, supporting both
VID Next payload: NONE, reserved: 0x0, length: 20 <-------- Response, supporting both
```

上記の出力では、メッセージ内の IKEV2_FRAGMENTATION_SUPPORTED および VID 値によって、IETF 標準フラグメンテーション方式とシスコ独自のフラグメンテーション方式の両方をサポートすることを示す、応答側から発信側へのメッセージが応答要求に含まれます。

以前のリリースのフラグメンテーション サポート

シスコ独自のフラグメンテーション方式を使用する以前のリリースのフラグメンテーションサポートを保証するために、IKEv2 はIETF 標準フラグメンテーション方式の IKEv2 通知ペイロード タイプと共にベンダー ID を引き続き使用します。両方のフラグメンテーション方式がサポートされている場合、IKEv2 は IETF 標準フラグメンテーション方式を優先します。

次の表に、ピアの機能に基づいてフラグメンテーションのタイプを特定する方法を示します。CISCO はシスコ独自のフラグメンテーション方式を示し、STD は IETF 標準フラグメンテーション方式を示します。

ピア 1 の機能	ピア 2 の機能	セキュリティ アソシエーションでアクティブなフラグメンテーション タイプ
STD + CISCO	STD + CISCO	STD
STD	STD	STD
CISCO	CISCO	CISCO
CISCO	STD + CISCO	CISCO
STD	STD + CISCO	STD
STD	CISCO	なし
なし	なし、STD + CISCO、または STD または CISCO	なし

フラグメントの暗号化、複合化、および再送信

フラグメンテーションおよび暗号化

パケットは、**crypto ikev2 fragmentation** コマンドで指定された最大伝送ユニット（MTU）値またはデフォルトMTU値のいずれかに基づいてフラグメント化されます。暗号化されたペイロードのみを含む IKE メッセージがフラグメント化されます。アナウンス メッセージ内の新しいペイロードタイプ（暗号化および認証されたフラグメント）は、フラグメントの合計数以上のフラグメント番号を示します。このペイロードは SKF として注釈がつけられ、値は 53 です。

発信パケットを暗号化する前に、パケット長を確認します。確立済みのセキュリティ アソシエーションは、IETF 標準フラグメント方式でSAが有効になっているかどうかも確認します。次に、フラグメント化されたパケットの伝送が表示されるデバイスからの出力例を示します。

```
*Oct 16 10:31:22.221: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 1 OF Total Fragments: 3
*Oct 16 10:31:22.222: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
```

```
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 2 OF Total Fragments: 3
*Oct 16 10:31:22.222: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 3 OF Total Fragments: 3
```

「SKF Next payload: COOP, reserved: 0x90, length: 216」および「SKF Fragment number: 1 OF Total Fragments: 3」は、メッセージが 3 つのフラグメントにフラグメント化された協調キー サーバのアナウンスメント（ANN）パケットであることを示します。

復号と最適化

応答側で受信フラグメントが受信されると、各フラグメントは復号されて一時的に保存されます。復号（元のパックへのフラグメントのアセンブリ）時に、重複するフラグメント、フラグメントの合計数以上のフラグメント番号、およびまったく別のフラグメント番号を持つフラグメントはドロップされます。フラグメントは、受信した順ではなくフラグメント番号の昇順で追加されます。そのため、パケットアセンブリが高速化します。ただし、順序どおりではないフラグメントも許可され、処理されます。各フラグメントは、メッセージに関係するすべてのフラグメントが受信されていることを確認するために検証されます。すべてのフラグメントが受信されると、パケットはフラグメントからアセンブリされ、新しく受信したメッセージとして処理されます。確認応答（ACK）メッセージは、元のパケットがアセンブリされると送信されます。各フラグメントには送信されません。

再送信

IKEv2 再送信は、IKEv2 再送信タイマーから求められた場合に発生します。一度構成され最初に送信されたフラグメントは、リスト化され、再送信タイマーがトリガーされた場合に再送信できるよう準備されます。再送信要求を受信すると、IKEv2 は応答を再送信します。この応答は、最初のフラグメント（#1）再送信が受信されると、再送信されます。残りのフラグメント番号は無視されるため、応答のより短時間での処理が可能になります。

フラグメンテーションの有効化

セキュリティ アソシエーション（SA）ごとにフラグメンテーションをグローバルに有効にするには、**crypto ikev2 fragmentation** コマンドを使用します。両方のピアが各ピアでの INIT 交換の後に IKE_AUTH 交換に使用されるフラグメンテーションのサポートを示している場合、フラグメンテーションは SA で有効になっています。

（注） このコマンドは、IKEv2 リモート アクセス ヘッドエンド機能によって導入され、変更されていません。

mtu *mtu-size* キーワード/引数のペアを使用して、最大伝送ユニット（MTU）をバイト単位で指定できます。MTU サイズは、IP または UDP カプセル化済みの IKEv2 パケットを示します。

MTU の範囲は 68 ～ 1500 バイトです。デフォルトの MTU サイズは、IPv4 パケットでは 576 バイト、IPv6 パケットでは 1280 バイトです。

RFC 機能に準拠した IKE フラグメンテーションで有効な **crypto ikev2 fragmentation** コマンドは、次のように動作します。

- 将来の SA にのみ影響し、既存の古い SA には影響しません。
- シスコ独自のフラグメンテーション方式と IETF 標準のフラグメンテーション方式をサポートします。

show crypto ikev2 sa detail コマンドにより、以下の情報が表示されます。

- ピアで有効なフラグメンテーション方式。有効なフラグメンテーション方式が IETF 標準のフラグメンテーションの場合、出力には使用中の MTU が表示されます。
- フラグメンテーションが両方のピアで有効になっているか、ローカル ピアでのみ有効になっているか。

IPv6 のサポート

RFC 機能に準拠した IKE フラグメンテーションでは、IETF 標準フラグメンテーション方式を使用している場合の、IPv6 IKE エンドポイントでの IPv6 パケットの断片化のサポートを追加しました。デフォルトの MTU 値は 1280 バイトであり、**crypto ikev2 fragmentation** コマンドで MTU が指定されていない場合に使用されます。フラグメンテーションで使用される MTU は、**show crypto ikev2 sa detail** コマンドの出力に表示されます。

IKEv2 フラグメンテーションの設定方法

IKEv2 フラグメンテーションの設定

このタスクを実行して、大規模な IKEv2 パケットのラグメンテーションを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 fragmentation** [**mtu** *mtu-size*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： 	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Device> enable`	
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	**crypto ikev2 fragmentation** [**mtu** *mtu-size*] 例： `Device(config)# crypto ikev2 fragmentation mtu 100`	IKEv2 フラグメンテーションを設定します。 • MTU の範囲は 68 ～ 1500 バイトです。デフォルトの MTU サイズは、IPv4 パケットでは 576 バイト、IPv6 パケットでは 1280 バイトです。 （注） MTU のサイズは、IP または UDP でカプセル化された IKEv2 パケットを示します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル 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。

IKEv2 フラグメンテーションの設定例

例：設定された MTU の表示が有効な IETF フラグメンテーション

次は、IETF 標準フラグメンテーション方式が有効であることを示すサンプル出力です。このステートメントは、応答側が IETF 標準フラグメンテーション方式もサポートしている場合に表示されます。また、出力には、使用中の MTU も表示されます。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none IN-NEG
Encr: Unknown - 0, PRF: Unknown - 0, Hash: None, DH Grp:0, Auth sign: Unknown - 0, Auth
 verify: Unknown - 0
Life/Active Time: 86400/0 sec
CE id: 0, Session-id: 0
Status Description: Initiator waiting for INIT response
Local spi: 2CD1BEADB7C20854 Remote spi: 0000000000000000
Local id: 10.0.8.3
Remote id:
Local req msg id: 0 Remote req msg id: 0
Local next msg id: 1 Remote next msg id: 0
Local req queued: 0 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 272 bytes.
```

```
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA
```

例：発信側で設定される IETF 標準フラグメンテーション方式

次は、発信側で設定されたIETF標準フラグメンテーション方式を表示するサンプル出力です。応答側はシスコ独自のフラグメンテーション方式をサポートしています。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/59 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 84350219051DB9E3 Remote spi: 52A8BB3898E8B5CF
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 4 Remote req msg id: 0
Local next msg id: 4 Remote next msg id: 0
Local req queued: 4 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA
```

次は、応答側の設定を表示するサンプル出力です。この出力では、シスコ独自のフラグメンテーション方式が構成されていますが、有効ではない点に注意してください。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.9.4/848 10.0.8.3/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/52 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 52A8BB3898E8B5CF Remote spi: 84350219051DB9E3
Local id: 10.0.9.4
Remote id: 10.0.8.3
Local req msg id: 0 Remote req msg id: 4
Local next msg id: 0 Remote next msg id: 4
Local req queued: 0 Remote req queued: 4
Local window: 5 Remote window: 5
```

```
DPD configured for 0 seconds, retry 0
Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

IPv6 Crypto IKEv2 SA
```

次は、発信側がIETF標準フラグメンテーション方式をサポートし、応答側はフラグメンテーションをサポートしていない例を示します。この出力は、IETF標準フラグメンテーション方式が構成されていますが、有効ではないことを示す点に注意してください。

```
Device# show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/44 sec
CE id: 1004, Session-id: 2
Status Description: Negotiation done
Local spi: 03534703287D9CA1 Remote spi: 146E1CFA68008A92
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 4 Remote req msg id: 0
Local next msg id: 4 Remote next msg id: 0
Local req queued: 4 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

次は、応答側の設定を表示するサンプル出力です。ステートメント「Fragmentation not configured.」に注意してください。

```
Device# show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.9.4/848 10.0.8.3/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/23 sec
CE id: 1004, Session-id: 4
Status Description: Negotiation done
Local spi: 146E1CFA68008A92 Remote spi: 03534703287D9CA1
Local id: 10.0.9.4
Remote id: 10.0.8.3
Local req msg id: 0 Remote req msg id: 3
Local next msg id: 0 Remote next msg id: 3
Local req queued: 0 Remote req queued: 3
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is not detected
```

```
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

例：発信側で設定されない IETF 標準フラグメンテーション方式

次は、発信側で設定されるフラグメンテーション方式が表示されないサンプル出力です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 10.0.8.3/848 10.0.9.4/848 none/none DELETE
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/28 sec
CE id: 1001, Session-id: 1
Status Description: Deleting IKE SA
Local spi: 1A375C00C1D157CF Remote spi: DB50F1BC58814FFA
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 2 Remote req msg id: 4
Local next msg id: 4 Remote next msg id: 5
Local req queued: 2 Remote req queued: 4
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

IPv6 Crypto IKEv2 SA
```

例：フラグメンテーションの IPv6 サポート

次の例は、FlexVPN エンドポイント（ハブとスポーク）のフラグメンテーションを示します。次は、パケットのフラグメント化に 1300 の最大伝送ユニット（MTU）を設定したハブに関連する設定です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA

Tunnel-id fvrf/ivrf Status
1 none/none READY
Local 4001::2000:3/500
Remote 4001::2000:1/500
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/64 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 45BA0D30D0EB5FFF Remote spi: 8D7B5A8389CEB8B3
```

```
Local id: R2.cisco.com
Remote id: R1.cisco.com
Local req msg id: 3 Remote req msg id: 0
Local next msg id: 3 Remote next msg id: 0
Local req queued: 3 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 1272 bytes.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
Remote subnets:
10.0.0.251 255.255.255.255
IPv6 Remote subnets:
3001::/112
5001::/64
```

次は、デフォルトの MTU を設定したスポークに関連する設定です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA

Tunnel-id fvrf/ivrf Status
1 none/none READY
Local 4001::2000:1/500
Remote 4001::2000:3/500
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/58 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 8D7B5A8389CEB8B3 Remote spi: 45BA0D30D0EB5FFF
Local id: R1.cisco.com
Remote id: R2.cisco.com
Local req msg id: 0 Remote req msg id: 3
Local next msg id: 0 Remote next msg id: 3
Local req queued: 0 Remote req queued: 3
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 1232 bytes.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
Remote subnets:
10.0.0.3 255.255.255.255
```

IKEv2 フラグメンテーションの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List』、すべてのリリース
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
IKEv2 フラグメンテーション	*draft-ietf-ipsecme-ikev2-fragmentation-10*

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IKEv2 フラグメンテーションの機能情報

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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IKEv2* フラグメンテーションの機能情報

機能名	リリース	機能情報
RFC に準拠した IKEv2 フラグメンテーション		RFC 機能に準拠した IKE フラグメンテーションでは、IETF の **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネット キー エクスチェンジ バージョン 2 （IKEv2）パケットのフラグメンテーションを実装しました。 **show crypto ikev2 sa** コマンドが変更されました。