



「IPsec Dead Peer Detection Periodic Message Option」

IPSecデッドピア検出定期メッセージオプション機能を使用すれば、ルータに対し、そのインターネットキーエクスチェンジ (IKE) ピアの活性を定期的に照会するよう設定できます。このオプションを使用すると、デフォルトのオンデマンドデッドピア検出機能を使用した場合に比べ、停止しているピアをより早期に検出できます。

- [IPSec デッドピア検出定期メッセージオプションの前提条件 \(1 ページ\)](#)
- [IPSec デッドピア検出定期メッセージオプションの制約事項 \(2 ページ\)](#)
- [IPSec デッドピア検出定期メッセージオプションに関する情報 \(2 ページ\)](#)
- [IPSec デッドピア検出定期メッセージオプションの設定方法 \(3 ページ\)](#)
- [IPSec デッドピア検出定期メッセージオプションの設定例 \(7 ページ\)](#)
- [その他の参考資料 \(10 ページ\)](#)
- [デッドピア検出定期メッセージオプションの機能情報 \(12 ページ\)](#)

IPSec デッドピア検出定期メッセージオプションの前提条件

IPSecデッドピア検出定期メッセージオプション機能を設定するには、次のことが必要です。

- IPセキュリティ (IPsec) の設定についての知識。
- DPD (Dead Peer Detection) がサポートされている IKE ピア。DPD をサポートしているのは、Cisco VPN 3000 コンセントレータ、Cisco PIX ファイアウォール、Cisco VPN Client、およびすべての動作モードの Cisco IOS XE ソフトウェア (サイト間および Easy VPN サーバー) などです。

IPSec デッドピア検出定期メッセージオプションの制約事項

定期的な DPD を使用すると、ルータによって、オンデマンドの DPD と比較してより速い応答時間で無応答の IKE ピアを検知できる可能性があります。ただし、定期的な DPD では、余分なオーバーヘッドが発生します。大量の IKE ピアと通信する場合は、オンデマンドの DPD の方を検討してください。

IPSec デッドピア検出定期メッセージオプションに関する情報

DPD および Cisco IOS XE キープアライブ機能の動作

DPD および Cisco IOS XE キープアライブは、タイマーに基づいて機能します。タイマーが 10 秒に設定されている場合、ルータは 10 秒毎に「hello」メッセージが送信されます（もちろん、ルータによってピアからの「hello」メッセージが受信された場合は除きます）。IOS キープアライブおよび定期的な DPD の利点は、デッドピアの検知が早くなることです。しかし、IOS キープアライブおよび定期的な DPD では、かなりの頻度でメッセージを定期的に送信する必要があります。頻繁にメッセージを送信する結果、通信を行うピアによって暗号化および復号化しなければならないパケット数が増加します。

DPD にはオンデマンド方式もあります。対称的なこのオンデマンド方式がデフォルトです。オンデマンド DPD では、トラフィックパターンに基づいてメッセージが送信されます。たとえば、ルータによって発信トラフィックが送信される必要があります。ピアの活性に疑問がある場合、ルータによって DPD メッセージが送信され、ピアのステータスが照会されます。ルータに送信するトラフィックがない場合、DPD メッセージは送信されません。ピアが停止しており、ピアに送信するトラフィックがルータにない場合、IKE または IPsec セキュリティアソシエーション (SA) のキー再生成が必要でないかぎり、ルータによる検知は行われません（ルータによるピアとの通信が行われない場合、ピアの活性は重要ではありません）。一方、ピアに送信するトラフィックがルータにあり、ピアの応答がない場合は、ピアのステータスを判断するために、ルータによって DPD メッセージが開始されます。

IPSec デッドピア検出定期メッセージオプションの使用

IPSec デッドピア検出 (DPD) 定期メッセージオプション機能では、DPD メッセージが定期的に「強制される」ようルータを設定できます。この強制方式の結果、デッドピアが早期に検知されます。たとえば、送信するトラフィックがルータにない場合でも、DPD メッセージが定期的に送信され、ピアが停止していた場合、IKE SA による検知がタイムアウトになるまでルータが待機する必要はありません。

DPD 定期メッセージオプションを設定する場合、**crypto isakmp keepalive** コマンドは **periodic** キーワードを指定して使用する必要があります。**periodic** キーワードを指定しない場合、ルータはデフォルトのオンデマンド方式になります。



(注) **crypto isakmp keepalive** コマンドを設定すると、Cisco IOS ソフトウェアは、ピアがサポートしているプロトコルに応じて、Cisco IOS キープアライブまたは DPD の使用についてネゴシエーションを行います。

暗号マップ内の複数のピアとの DPD および Cisco IOS XE キープアライブ機能の使用

暗号マップ内で DPD および Cisco IOS XE キープアライブ機能を複数のピアと組み合わせることにより、ステートレス フェールオーバーを実現できます。DPD により、ルータによる停止 IKE ピアの検知が可能となり、ルータによって停止状態が検知されると、ルータによってピアに対する IPsec と IKE SA が削除されます。複数のピアを設定している場合、ルータによって、次にリストされているピアへの切り替えが行われ、ステートレスフェールオーバーが実現します。

IPSec デッド ピア検出定期メッセージオプションの設定方法

定期的な DPD メッセージの設定

定期的な DPD メッセージを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive seconds [retries] [periodic | on-demand]**

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： Router> enable	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
ステップ 2	configure terminal 例 : <pre>Router# configure terminal</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 3	crypto isakmp keepalive seconds [retries] [periodic on-demand] 例 : <pre>Router (config)# crypto isakmp keepalive 10 periodic</pre>	<p>ゲートウェイによるピアへの DPD メッセージの送信を許可します。</p> <ul style="list-style-type: none"> • seconds : periodic キーワードを使用する場合、この引数には DPD メッセージの間隔を秒数で指定します。範囲は 10 ～ 3600 秒です。 <p>on-demand キーワードを使用する場合、この引数には、送信するデータ (IPsec) トラフィックがあるときに、DPD リトライメッセージを送信するまでピアからトラフィックを受信しない間に待機する秒数を指定します。範囲は 10 ～ 3600 秒です。</p> <p>(注) 間隔を指定しない場合、エラーメッセージが表示されます。</p> <ul style="list-style-type: none"> • retry-seconds : (任意) ピアによって DPD リトライメッセージが失われた場合の DPD リトライメッセージの送信間隔を秒数で指定します。範囲は 2 ～ 60 秒です。 <p>1つの DPD メッセージがピアで失われると、ルータはよりアグレッシブな状態に移行し、より短いリトライ間隔で DPD リトライメッセージを送信します。ピアによって DPD リトライメッセージが失われた場合のこの間隔は、DPD リトライ間の秒数です。デフォルトで、DPD リトライメッセージは 2 秒ごとに送信されます。アグレッシブな 5 回の DPD リトライメッセージが失われると、トンネルがダウンした状態としてマークされます。</p> <p>(注) IPsec ハイアベイラビリティ (HA) を使用して DPD を設定するには、デフォルト (2 秒) 以外の値を使用することを推奨します。HA には、キープアライブ時間を 10 秒、試行を 5 回に設定するのが適しています。その時間が、ルータがアクティブモードになるためにかかる時間であるからです。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • periodic : (任意) DPD メッセージが定期的に送信されます。 • on-demand : (任意) デフォルトの動作です。DPD リトライがオンデマンドで送信されます。 <p>(注) このオプションはデフォルトであるため、on-demand キーワードは設定の出力に表示されません。</p>

暗号マップ内の複数のピアとの DPD および Cisco IOS XE キープアライブの設定

DPD および IOS キープアライブを、クリプト マップと組み合わせて使用するよう設定し、ステートレスフェールオーバーを実現するには、次の手順を実行します。この設定により、最初のピアが停止していることが検知されると、ルータによってピア リストが循環されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map map-name seq-num ipsec-isakmp**
4. **set peer {host-name [dynamic] | ip-address}**
5. **set transform-set transform-set-name**
6. **match address [access-list-id | name]**

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 : <pre>Router> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : <pre>Router# configure terminal</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 3	crypto map map-name seq-num ipsec-isakmp 例 : <pre>Router (config)# crypto map green 1 ipsec-isakmp</pre>	クリプト マップ コンフィギュレーション モードを開始して、クリプト マップ エントリを作成または変更します。

DPD が有効化されていることの確認

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • ipsec-isakmp キーワードは、このクリプトマップエントリによって指定されたトラフィックを保護するための IPsec SA を確立するために、IKE が使用されることを示します。
ステップ 4	set peer { <i>host-name</i> [dynamic] <i>ip-address</i> } 例： <pre>Router (config-crypto-map)# set peer 10.12.12.12</pre>	クリプトマップ内の IPsec ピアを指定します。 <ul style="list-style-type: none"> • このコマンドを繰り返すことによって、複数のピアを指定できます。
ステップ 5	set transform-set <i>transform-set-name</i> 例： <pre>Router (config-crypto-map)# set transform-set txfm</pre>	クリプトマップエントリで使用可能なトランスフォームセットを指定します。 <ul style="list-style-type: none"> • このコマンドを繰り返すことによって、複数のトランスフォームセットを指定できます。
ステップ 6	match address [<i>access-list-id</i> <i>name</i>] 例： <pre>Router (config-crypto-map)# match address 101</pre>	クリプトマップエントリの拡張アクセスリストを指定します。

DPD が有効化されていることの確認

DPD を使用すれば、ピアが到達不能になった時に、ルータによる IKE ステートのクリアが可能になります。DPD が有効化されており、ピアがしばらくの間到達不能になった場合、**clear crypto session** コマンドを使用して、手動で IKE と IPsec SA をクリアできます。

debug crypto isakmp コマンドを使用すると、DPD が有効化されていることを確認できます。

手順の概要

1. **enable**
2. **clear crypto session** [**local** *ip-address* [**port** *local-port*]] [**remote** *ip-address* [**port** *remote-port*]] | [**fvrif** *vrf-name*] [**ivrf** *vrf-name*]
3. **debug crypto isakmp**

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： <pre>Router> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • 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
ステップ 2	clear crypto session [local ip-address [port local-port]] [remote ip-address [port remote-port]] [fvrf vrf-name] [ivrf vrf-name] 例： Router# clear crypto session	暗号セッション（IPsec および IKE SA）を削除します。
ステップ 3	debug crypto isakmp 例： Router# debug crypto isakmp	IKE イベントに関するメッセージを表示します。

IPsec デッドピア検出定期メッセージオプションの設定例

定期的な DPD を有効化したサイト間設定の例

次の設定は、定期的な DPD が有効になっているサイト間設定用です。設定は、IKE フェーズ 1 ポリシー用と IKE 事前共有キー用です。

IKE フェーズ 1 ポリシー

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 14
!
```

IKE 事前共有キー

```
crypto isakmp key kd94j1ksldz address 10.2.80.209 255.255.255.0
crypto isakmp keepalive 10 periodic
crypto ipsec transform-set Trans1 esp-aes esp-sha-hmac

!
!
interface
  ip address 10.1.32.14 255.255.255.0
  speed auto

!
```

debug crypto isakmp コマンドを使用した DPD 設定の確認の例

次の `debug crypto isakmp` コマンドの出力例では、IKE DPD が有効化されていることを確認しています。

```
*Mar 25 15:17:14.131: ISAKMP:(0:1:HW:2):IKE_DPD is enabled, initializing timers
```

IKE DPD がイネーブルになっていること（および、ピアによって DPD がサポートされていること）を確認するには、定期的な DPD をイネーブルにする時に、コマンドによって指定された間隔で次のデバッグメッセージが出力されることを確認する必要があります。

```
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:18:52.107: ISAKMP:(0:1:HW:2):purging node 899852982 *Mar 25 15:18:52.111:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:18:52.111: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

上記のメッセージは、DPD R_U_THERE メッセージの送信に対応しています。

```
*Mar 25 15:18:52.123: ISAKMP (0:268435457): received packet from 10.2.80.209
dport 500 sport 500 Global (I) QM_IDLE
*Mar 25 15:18:52.123: ISAKMP: set new node -443923643 to QM_IDLE *Mar 25 15:18:52.131:
ISAKMP:(0:1:HW:2): processing HASH payload. message ID =
-443923643
*Mar 25 15:18:52.131: ISAKMP:(0:1:HW:2): processing NOTIFY R_U_THERE_ACK protocol 1
spi 0, message ID = -443923643, sa = 81BA4DD4
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2): DPD/R_U_THERE_ACK received from peer
10.2.80.209, sequence 0x9
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):deleting node -443923643 error FALSE
reason "informational (in) state 1"
*Mar 25 15:18:52.135: ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_PEER, IKE_INFO_NOTIFY *Mar
25 15:18:52.135: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

上記のメッセージは、ピアからの確認応答（ACK）メッセージに対応しています。

```
Router#
*Mar 25 15:47:35.335: ISAKMP: set new node -90798077 to QM_IDLE *Mar 25 15:47:35.343:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:35.343: ISAKMP:(0:1:HW:2):purging node -90798077 *Mar 25 15:47:35.347:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_IM_ALIVE
*Mar 25 15:47:35.347: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
*Mar 25 15:47:36.611: ISAKMP:(0:1:HW:2):purging node 1515050537 *Mar 25 15:47:37.343:
ISAKMP:(0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:37.343: ISAKMP: set new node -1592471565 to QM_IDLE *Mar 25 15:47:37.351:
ISAKMP:(0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:37.351: ISAKMP:(0:1:HW:2):purging node -1592471565 *Mar 25 15:47:37.355:
ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER_PEERS_ALIVE
*Mar 25 15:47:37.355: ISAKMP:(0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
*Mar 25 15:47:39.355: ISAKMP:(0:1:HW:2):incrementing error counter on sa:
```



```

PEERS_ALIVE_TIMER
*Mar 25 15:47:39.355: ISAKMP: set new node 1758739401 to QM_IDLE *Mar 25 15:47:39.363:
ISAKMP: (0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:39.363: ISAKMP: (0:1:HW:2):purging node 1758739401 *Mar 25 15:47:39.367:
ISAKMP: (0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER PEERS_ALIVE
*Mar 25 15:47:39.367: ISAKMP: (0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
*Mar 25 15:47:41.367: ISAKMP: (0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:41.367: ISAKMP: set new node 320258858 to QM_IDLE *Mar 25 15:47:41.375:
ISAKMP: (0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:41.379: ISAKMP: (0:1:HW:2):purging node 320258858 *Mar 25 15:47:41.379:
ISAKMP: (0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER PEERS_ALIVE
*Mar 25 15:47:41.379: ISAKMP: (0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
*Mar 25 15:47:43.379: ISAKMP: (0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:43.379: ISAKMP: set new node -744493014 to QM_IDLE *Mar 25 15:47:43.387:
ISAKMP: (0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:43.387: ISAKMP: (0:1:HW:2):purging node -744493014 *Mar 25 15:47:43.391:
ISAKMP: (0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER PEERS_ALIVE
*Mar 25 15:47:43.391: ISAKMP: (0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
*Mar 25 15:47:45.391: ISAKMP: (0:1:HW:2):incrementing error counter on sa:
PEERS_ALIVE_TIMER
*Mar 25 15:47:45.391: ISAKMP: (0:1:HW:2):peer 10.2.80.209 not responding! *Mar 25
15:47:45.391: ISAKMP: (0:1:HW:2):peer does not do paranoid keepalives.
*Mar 25 15:47:45.391: ISAKMP: (0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.395: ISAKMP: Unlocking IPSEC struct 0x81E5C4E8 from
delete_siblings, count 0
*Mar 25 15:47:45.395: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer
10.2.80.209:500 Id: 10.2.80.209
*Mar 25 15:47:45.399: ISAKMP: set new node -2061951065 to QM_IDLE *Mar 25 15:47:45.411:
ISAKMP: (0:1:HW:2): sending packet to 10.2.80.209 my_port
500 peer_port 500 (I) QM_IDLE
*Mar 25 15:47:45.411: ISAKMP: (0:1:HW:2):purging node -2061951065 *Mar 25 15:47:45.411:
ISAKMP: (0:1:HW:2):Input = IKE_MSG_FROM_TIMER,
IKE_TIMER PEERS_ALIVE
*Mar 25 15:47:45.411: ISAKMP: (0:1:HW:2):Old State = IKE_P1_COMPLETE New State =
IKE_DEST_SA
*Mar 25 15:47:45.415: ISAKMP: (0:1:HW:2):deleting SA reason "peers alive" state
(I) QM_IDLE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.415: ISAKMP: Unlocking IKE struct 0x81E5C4E8 for
isadb_mark_sa_deleted(), count 0
*Mar 25 15:47:45.415: ISAKMP: Deleting peer node by peer_reap for 10.2.80.209:
81E5C4E8
*Mar 25 15:47:45.415: ISAKMP: (0:1:HW:2):deleting node -1067612752 error TRUE
reason "peers alive"
*Mar 25 15:47:45.415: ISAKMP: (0:1:HW:2):deleting node -114443536 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP: (0:1:HW:2):deleting node 2116015069 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP: (0:1:HW:2):deleting node -1981865558 error TRUE
reason "peers alive"
*Mar 25 15:47:45.419: ISAKMP: (0:1:HW:2):Input = IKE_MSG_INTERNAL, IKE_PHASE1_DEL *Mar
25 15:47:45.419: ISAKMP: (0:1:HW:2):Old State = IKE_DEST_SA New State =
IKE_DEST_SA

```

```

*Mar 25 15:47:45.419: ISAKMP: received ke message (4/1)
*Mar 25 15:47:45.419: ISAKMP: received ke message (3/1)
*Mar 25 15:47:45.423: ISAKMP: ignoring request to send delete notify (no ISAKMP
sa) src 10.1.32.14 dst 10.2.80.209 for SPI 0x3A7B69BF
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting SA reason "" state (I)
MM_NO_STATE (peer 10.2.80.209) input queue 0
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -1067612752 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node -114443536 error FALSE
reason ""
*Mar 25 15:47:45.423: ISAKMP:(0:1:HW:2):deleting node 2116015069 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):deleting node -1981865558 error FALSE
reason ""
*Mar 25 15:47:45.427: ISAKMP:(0:1:HW:2):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH *Mar 25
15:47:45.427: ISAKMP:(0:1:HW:2):Old State = IKE_DEST_SA New State =
IKE_DEST_SA

```

上記のメッセージは、リモートピアが到達不能になっている時に何が発生しているのかを示しています。ルータによって、最終的に IPsec および SA が削除される前に、1つの DPDR_U_THERE メッセージおよび 4 つの転送が送信されます。

暗号マップ内の複数のピアとの組み合わせで使用される DPD および Cisco IOS XE キープアライブ：例

次に、セキュリティアソシエーション (SA) を確立するために IKE が使用される場合に、DPD および Cisco IOS XE キープアライブが暗号マップ設定内の複数のピアとの組み合わせで使用される例を示します。この例では、SA が、10.0.0.1、10.0.0.2、または 10.0.0.3 の IPsec ピアに設定される可能性があります。

```

crypto isakmp keepalive 10 periodic
crypto map green 1 ipsec-isakmp
  set peer 10.0.0.1
  set peer 10.0.0.2
  set peer 10.0.0.3
  set transform-set txfm
  match address 101

```

その他の参考資料

次の項では、IPSec デッド ピア検出定期メッセージ オプションの関連資料を示します。

関連資料

関連項目	マニュアルタイトル
IPsec の設定	IPsec を使用した VPN のセキュリティの設定
IPsec コマンド	『Cisco IOS Security Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
DPD は、インターネット ドラフト「draft-ietf-ipsec-dpd-04.txt」に準拠しています。このドラフトは、Informational RFC（番号はまだ割り当てられていません）として公表の検討中です。	--

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	http://www.cisco.com/en/US/support/index.html

デッドピア検出定期メッセージオプションの機能情報

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: デッドピア検出の機能情報

機能名	リリース	機能情報
デッドピア検出定期メッセージオプション	Cisco IOS XE Release 2.1	<p>この機能により、ルータに対し、その IKE ピアの有効性について定期的に照会が行われるよう設定できます。このオプションを使用すると、デフォルトのオンデマンドデッドピア検出機能を使用した場合に比べ、停止しているピアをより早期に検出できます。</p> <p>次のコマンドが導入または変更されました。 crypto isakmp keepalive。</p>

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。