# 暗号条件付きデバッグ サポート

暗号条件付きデバッグサポート機能では、新しいdebugコマンドが導入され、これらのコマンドにより、ユーザは、ピアIPアドレス、暗号エンジンの接続ID、セキュリティパラメータインデックス（SPI）などの事前に定義された暗号条件に基づいてIPセキュリティ（IPSec）トンネルをデバッグできます。特定のIPsec処理に限定してデバッグメッセージを表示し、デバッグ出力の量を減らすことにより、多数のトンネルを使用するルータを効率的にトラブルシューティングできます。



# 暗号条件付きデバッグ サポートの前提条件

# 暗号条件付きデバッグ サポートの制約事項

- 
- 条件付きデバッグは、特定のピアまたは機能に関連するインターネットキー交換（IKE）およびIPSecの問題をトラブルシューティングする際に役立ちますが、デバッグ条件が多すぎると、そのデバッグ条件を定義およびチェックできない場合があります。デバッグ条件値を保管するために空き領域が余分に必要となるため、CPUの処理オーバーヘッドが増加し、メモリ使用量も増加します。したがって、大量のトラフィックを処理するルータで暗号条件付きデバッグをイネーブルにする場合は、注意が必要です。

# 暗号条件付きデバッグ サポートに関する情報

## サポートされる条件タイプ

新しい暗号条件付きデバッグ CLI（**debug crypto condition**、 **debug crypto condition unmatched**、**and show crypto debug-condition**）を使用すれば、条件（フィルタ値）を指定して、指定した条件に関連するデバッグメッセージだけを生成して表示することができます。次の表に、サポートされる条件タイプを示します。

（注） **ipv4** または **ipv6** キーワードを指定した **debug crypto condition peer** コマンドは、ハードウェアプラットフォーム固有のデバッグ出力を提供できます。残りの条件フィルタは、プラットフォーム固有のデバッグ出力を提供しません。

表 *1:* 暗号デバッグ *CLI* でサポートされる条件タイプ

| 条件タイプ（キーワード） | 説明 |
|---|---|
| connid [1] | 1 ～ 32766 の整数。現在の IPSec 処理で、この値が暗号エンジンのあるインターフェイスへの接続 ID として使用されている場合、関連するデバッグ メッセージが表示されます。 |
| FVRF | バーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスの名前を表す文字列。この VRF インスタンスが、現在の IPSec 処理で、前面扉 VRF（FVRF）として使用されている場合、関連するデバッグ メッセージが表示されます。 |
| ikev2 | IKEv2 プロファイルの名前文字列。IKEv2 プロファイル名が指定された場合は、関連するデバッグ メッセージが表示されます。 |
| isakmp | ISAKMP プロファイルの名前文字列。ISAKMP プロファイル名が指定された場合は、関連するデバッグ メッセージが表示されます。 |
| IVRF | VRF インスタンスの名前を表す文字列。この VRF インスタンスが、現在の IPSec 処理で、内部 VRF（IVRF）として使用されている場合、関連するデバッグ メッセージが表示されます。 |
| local | IPv4 または IPv6 ローカル アドレスの名前文字列。 |
| peer group | Unity グループ名を表す文字列。このグループ名をピアがアイデンティティとして使用している場合、関連するデバッグ メッセージが表示されます。 |

| 条件タイプ（キーワード） | 説明 |
|---|---|
| peer hostname | 完全修飾ドメイン名（FQDN）を表す文字列。この文字列をピアがアイデンティティとして使用している場合、関連するデバッグ メッセージが示されます（たとえば、ピアがこの FQDN 文字列を使用して IKE Xauth をイネーブルにする場合）。 |
| peer ipv4 または peer ipv6 | 単一の IP アドレス。現在の IPSec 処理が、このピアの IP アドレスに関係している場合、関連するデバッグ メッセージが表示されます。 |
| peer subnet | ピアの IP アドレスの範囲を指定するサブネットおよびサブネットマスク。現在の IPSec ピアの IP アドレスが、指定したサブネット範囲に属する場合、関連するデバッグ メッセージが表示されます。 |
| peer username | ユーザ名を表す文字列。このユーザ名をピアがアイデンティティとして使用している場合、関連するデバッグ メッセージが示されます（たとえば、ピアがこのユーザ名を使用して IKE 拡張認証（Xauth）をイネーブルにする場合）。 |
| session | 暗号セッションに関する情報を提供します。 |
| SPI | 32 ビットの符号なし整数。現在の IPSec 処理がこの値を SPI として使用する場合、関連するデバッグ メッセージが表示されます。 |
| unmatched | コンテキスト情報が使用できない場合にデバッグ メッセージを提供します。 |

[1] IPSec connid、flowid、または SPI をデバッグ条件として使用する場合、関連する IPSec フローに関するデバッグメッセージが生成されます。IPSec フローには、connid、flowid、および SPI が 2 つ（インバウンドとアウトバウンド）ずつ含まれています。各 2 つの connid、flowid、および SPI は、IPSec フローのデバッグ メッセージをトリガーするデバッグ条件として使用できます。

# 暗号条件付きデバッグ サポートのイネーブル化方法

## 暗号条件付きデバッグ メッセージのイネーブル化

### パフォーマンス上の考慮事項

- 暗号条件付きデバッギングをイネーブルにする前に、使用するデバッグ条件タイプ（デバッグ フィルタとしても知られる）および値を決める必要があります。デバッグ メッセージの量は、定義する条件数によって異なります。

（注） 多数のデバッグ条件を指定すると、CPUサイクルが消費され、ルータのパフォーマンスに悪影響を及ぼすことがあります。

- ルータによって条件付きデバッグが実行されるのは、最低 1 つのグローバル crypto debug コマンド（**debug crypto isakmp**、**debug crypto ipsec**、および **debug crypto engine**）がイネーブルに設定されている場合に限られます。この要件により、条件付きデバッグを使用していないときは、ルータのパフォーマンスに影響が出ないようになっています。

## 暗号条件付きデバッグのディセーブル化

暗号条件付きデバッグをディセーブルにするには、発行済みのグローバルな暗号デバッグ CLI を事前にディセーブルにする必要があります。その後で、条件付デバッグをディセーブルにできます。

（注） **reset** キーワードを使用すると、設定されたすべての条件を同時にディセーブルにできます。

### 手順の概要

1. **enable**
2. **debug crypto condition** [**connid** *integer* **engine-id** *integer*] [**flowid** *integer***engine-id** *integer*] [**fvrf** *string*] [**ivrf** *string*] [**peer** [**group** *string*] [**hostname** *string*] [**ipv4** *ipaddress*] [**subnet** *subnet mask*] [**username** *string*]] [**spi** *integer*] [**reset**]
3. **show crypto debug-condition** {[**peer**] [**connid**] [**spi**] [**fvrf**] [**ivrf**] [**unmatched**]}
4. **debug crypto isakmp**
5. **debug crypto ipsec**
6. **debug crypto engine**
7. **debug crypto condition unmatched** [**isakmp** | **ipsec** | **engine**]

### 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**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **debug crypto condition** [**connid** *integer* **engine-id** *integer*] [**flowid** *integer***engine-id** *integer*] [**fvrf** *string*] [**ivrf** *string*] [**peer** [**group** *string*] [**hostname** *string*] [**ipv4** *ipaddress*] [**subnet** *subnet mask*] [**username** *string*]] [**spi** *integer*] [**reset**]<br>例： | 条件付きデバッグ フィルタを定義します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Router# debug crypto condition connid 2000 engine-id 1` | |
| ステップ 3 | **show crypto debug-condition** {[**peer**] [**connid**] [**spi**] [**fvrf**] [**ivrf**] [**unmatched**]}<br>例：<br>`Router# show crypto debug-condition spi` | ルータ上ですでにイネーブルに設定されている暗号デバッグ条件を表示します。 |
| ステップ 4 | **debug crypto isakmp**<br>例：<br>`Router# debug crypto isakmp` | グローバル IKE デバッグをイネーブルにします。 |
| ステップ 5 | **debug crypto ipsec**<br>例：<br>`Router# debug crypto ipsec` | グローバル IPSec デバッグをイネーブルにします。 |
| ステップ 6 | **debug crypto engine**<br>例：<br>`Router# debug crypto engine` | グローバル暗号エンジン デバッグをイネーブルにします。 |
| ステップ 7 | **debug crypto condition unmatched** [**isakmp** \| **ipsec** \| **engine**]<br>例：<br>`Router# debug crypto condition unmatched ipsec` | （任意）デバッグ条件をチェックするためのコンテキスト情報がない場合、デバッグ条件付き暗号メッセージを表示します。<br>オプションのキーワードを指定しない場合は、暗号関連のすべての情報が表示されます。 |

# 暗号エラー デバッグ メッセージのイネーブル化

暗号エラー デバッグ フィルタリングをイネーブルにするには、次の作業を実行する必要があります。

## デバッグ暗号エラー CLI

**debug crypto error** コマンドを有効にすると、エラーに関連するデバッグメッセージだけが表示されます。これにより、IKEネゴシエーションなどの暗号処理がシステム内で失敗した理由を簡単に判別できます。

（注） このコマンドをイネーブルにする場合は、グローバル暗号 debug コマンドがイネーブルに設定されていないことを確認してください。設定されていると、グローバル コマンドによってエラー関連のデバッグ メッセージが上書きされます。

### 手順の概要

1. **enable**
2. **debug crypto isakmp** | **ipsec** | **engine**} **error**

### 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**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **debug crypto isakmp** | **ipsec** | **engine**} **error**<br>例：<br>`Router# debug crypto ipsec error` | 暗号エリアに関するエラー デバッグ メッセージだけをイネーブルにします。 |

# 暗号条件付きデバッグ CLI の設定例

## 暗号条件付きデバッグのイネーブル化の例

次の例では、ピアの IP アドレスが 10.1.1.1、10.1.1.2、または 10.1.1.3 で、暗号エンジン 0 の接続 ID に 2000 が使用されている場合のデバッグ メッセージの表示例を示します。また、この例では、グローバルデバッグ暗号 CLI をイネーブルする方法と、**show crypto debug-condition** コマンドをイネーブルにして条件付きの設定を確認する方法も示します。

```
Router#
debug crypto condition connid 2000 engine-id 1
Router#
debug crypto condition peer ipv4 10.1.1.1
Router#
debug crypto condition peer ipv4 10.1.1.2
Router#
debug crypto condition peer ipv4 10.1.1.3
Router#
debug crypto condition unmatched
! Verify crypto conditional settings.
Router#
show crypto debug-condition
Crypto conditional debug currently is turned ON
```

```
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON
IKE peer IP address filters:
10.1.1.1  10.1.1.2   10.1.1.3
Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
Router#
debug crypto isakmp
Router#
debug crypto ipsec
Router#
debug crypto engine
```

# 暗号条件付きデバッグのディセーブル化の例

次の例では、すべての暗号条件付き設定をディセーブルにし、またこれらの設定がディセーブルになったことを確認する方法を示します。

```
Router#
debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router#
show crypto debug-condition
Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

# その他の参考資料

ここでは、暗号条件付きデバッグ サポート機能に関する関連資料について説明します。

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| IPSec および IKE 設定作業 | 『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Internet Key Exchange for IPsec VPNs」の章 |
| IPSec および IKE コマンド | 『*Cisco IOS Security Command Reference*』 |

### 標準

| 標準 | タイトル |
|---|---|
| なし | -- |

### MIB

| MIB | MIB のリンク |
|---|---|
| なし | 選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索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。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | タイトル |
|---|---|
| なし | -- |

### 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 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。<br>お使いの製品のセキュリティ情報や技術情報を入手するために、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。<br>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。 | http://www.cisco.com/en/US/support/index.html |

# 暗号条件付きデバッグ サポートに関する機能情報

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。

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。