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、3 つの新規のコマンドライン インターフェイス（CLI）が導入され、これらのインターフェイスにより、ユーザは、ピア IP アドレス、暗号エンジンの接続 ID、および Security Parameter Index（SPI; セキュリティ パラメータ インデックス）などの事前に定義し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 サポートの機能履歴

機能の履歴	
リリース	**変更点**
12.3(2)T	この機能が追加されました。

プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明の場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

暗号条件付きデバッグ サポートの前提条件

新しい暗号 CLI を使用するには、k8 または k9 サブシステムなどの暗号イメージを使用する必要があります。

暗号条件付きデバッグ サポートの制約事項

- この機能は、ハードウェア暗号エンジン用のデバッグ メッセージ フィルタ機能をサポートしません。
- 条件付きデバッグは、特定のピアまたは機能に関連する Internet Key Exchange（IKE; インターネット キー エクスチェンジ）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

conditional crypto debug コマンドをイネーブルにするには、次の概念を理解しておく必要があります。

- 「サポートされる条件タイプ」（P.2）

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**、**show crypto debug-condition**）では、条件（フィルタ値）を指定し、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および表示できます。表 1 に、サポートされる条件タイプを示します。

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。
flowid[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フロー 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	Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing and Forwarding（VRF; VPN ルーティングおよび転送）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。

表 1　暗号デバッグ CLI でサポートされる条件タイプ （続き）

条件タイプ（キーワード）	説明
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。
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。
peer hostname	Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）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 ipaddress	単一の IP アドレス。現在の IPSec 処理がこのピアの IP アドレスに関連する場合は、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）。
SPI[1]	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。

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 フローのデバッグ メッセージが生成されます。1 つの IPSec フローには、connid、flowid および SPI が 2 つずつあり、1 つは着信側、もう 1 つは発信側にあります。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

ここでは、次の各手順について説明します。

暗号条件付きデバッグ メッセージのイネーブル化

暗号条件付きデバッグ 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。

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 つのグローバル暗号 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、条件付き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**]（任意）

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 モードをイネーブルにします。 • 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	**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**] **例：** `Router# debug crypto condition connid 2000 engine-id 1`	条件付きデバッグ フィルタを定義します。
ステップ 3	**show crypto debug-condition** {[**peer**] [**connid**] [**spi**] [**fvrf**] [**ivrf**] [**unmatched**]} **例：** `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** **例：** `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** **例：** `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** **例：** `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**] **例：** `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。 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 コマンドをイネーブルにすると、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** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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	**debug crypto {isakmp | ipsec | engine} error** **例：** `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

ここでは、次の設定例について説明します。

- 「暗号条件付きデバッグのイネーブル化：例」（P.6）
- 「暗号条件付きデバッグのディセーブル化：例」（P.7）

暗号条件付きデバッグのイネーブル化：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：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

内容	参照先
IPSec および IKE 設定作業	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Internet Key Exchange for IPsec VPNs」
IPSec および IKE コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **debug crypto condition**
- **debug crypto condition unmatched**
- **debug crypto error**
- **show crypto debug-condition**

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『Master Command List』を参照してください。
