



Embedded Packet Capture コンフィギュレーションガイド Cisco IOS Release 15.1SG

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2013 Cisco Systems, Inc. All rights reserved.



目次

Embedded Packet Capture 1

機能情報の確認 1

Embedded Packet Capture の前提条件 2

Embedded Packet Capture の制約事項 2

Embedded Packet Capture について 2

Embedded Packet Capture の概要 2

EPC の利点 3

キャプチャ バッファ 3

キャプチャ ポイント 4

Embedded Packet Capture の実装方法 4

パケット データ キャプチャの開始 4

パケット データ キャプチャの停止 6

分析のためのパケット データのエクスポート 7

キャプチャされたデータのモニタリングとメンテナンス 7

Embedded Packet Capture の設定例 8

パケット データ キャプチャの開始の例 8

パケット データ キャプチャの停止の例 9

パケット データのエクスポートの例 9

キャプチャされたデータのモニタリングとメンテナンスの例 9

その他の関連資料 10

Embedded Packet Capture の機能情報 11



第 1 章

Embedded Packet Capture

Embedded Packet Capture (EPC) は、ネットワーク管理者がデバイスを出入りするかデバイスを通るパケットをキャプチャし、パケットをローカルで分析するか、または Wireshark のようなツールを使用してオフライン分析を行うために、パケットを保存してエクスポートできるようにするオンボードパケットキャプチャファシリティです。この機能は、デバイスがネットワークの管理と操作にアクティブに参加できるようにすることによって、ネットワーク操作を簡略化します。この機能は、パケットの形式に関する情報を収集することによって、トラブルシューティングを容易にします。また、アプリケーションの分析とセキュリティも容易にします。

- [機能情報の確認, 1 ページ](#)
- [Embedded Packet Capture の前提条件, 2 ページ](#)
- [Embedded Packet Capture の制約事項, 2 ページ](#)
- [Embedded Packet Capture について, 2 ページ](#)
- [Embedded Packet Capture の実装方法, 4 ページ](#)
- [Embedded Packet Capture の設定例, 8 ページ](#)
- [その他の関連資料, 10 ページ](#)
- [Embedded Packet Capture の機能情報, 11 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。最新の警告および機能情報については、『[Bug Search Tool](#)』およびご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

Embedded Packet Capture の前提条件

Embedded Packet Capture (EPC) ソフトウェア サブシステムは、その動作で CPU とメモリ リソースを消費します。さまざまなタイプの操作を行うために十分なシステムリソースを準備する必要があります。システムリソースの使用のためのガイドラインを次の表に示します。

表 1: EPC サブシステムのシステム要件

システム リソース	要件
ハードウェア	CPU 利用率の要件は、プラットフォームによって異なります。
メモリ	パケット バッファは DRAM に保存されます。パケット バッファのサイズは、ユーザが指定します。
ディスクスペース	パケットは外部のデバイスにエクスポートできます。フラッシュ ディスクでの中間保管は必要ありません。

Embedded Packet Capture の制約事項

- Cisco IOS Release 12.2(33)SRE では、EPC は 7200 プラットフォームでのみサポートされます。
- EPC は入力マルチキャスト パケットだけをキャプチャし、出力の複製パケットをキャプチャしません。
- 現在、キャプチャ ファイルはデバイスの外部 (TFTP または FTP サーバおよびローカル ディスクなど) にだけエクスポートできます。

Embedded Packet Capture について

Embedded Packet Capture の概要

Embedded Packet Capture (EPC) は、パケットのトレースとトラブルシューティングに役立つ組み込みシステム管理機能を提供します。この機能を使用すると、ネットワーク管理者は、シスコ デバイスを出入りするか通過するデータ パケットをキャプチャできます。ネットワーク管理者は、キャプチャ バッファ サイズとタイプ (循環またはリニア) およびキャプチャする各パケットの最大バイト数を定義する場合があります。パケット キャプチャ レートは、詳細な管理制御を使用してスロットリングできます。たとえば、アクセス コントロール リストを使用してキャプチャ対象パケットをフィルタリングするオプションや、最大パケット キャプチャ レートまたはサンプリング間隔の指定などの詳細な定義を行うオプションが利用できます。

EPC の利点

この機能の利点は次のとおりです。

- シスコ エクスプレス フォワーディング (CEF) パスにある IPv4 および IPv6 パケットをキャプチャする機能
- キャプチャ バッファ パラメータを指定するフレキシブルな方法
- フィルタにキャプチャされたパケット
- さまざまな程度の詳細さでキャプチャされたデータ パケットをデコードする方法
- 外部ツールを使用して、パケットキャプチャを分析に適した PCAP 形式でエクスポートするファシリティ
- パケット キャプチャ ポイントをイネーブルにする拡張可能なインフラストラクチャ

キャプチャ バッファ

キャプチャ バッファは、パケット データを収容するメモリ内の領域です。バッファの一意の名前、サイズ、およびタイプを指定し、バッファが必要に応じて着信データを処理するように設定できます。

キャプチャ バッファには次のタイプのデータが保存されます。

- パケット データ
- メタデータ

パケット データは `datagramstart` から開始され、最小の 1 パケットあたりのキャプチャ サイズ (`datagramsize`) をキャプチャ バッファにコピーします。

メタデータには、パケットデータのセットについての説明情報が含まれています。内容は、次のとおりです。

- バッファに追加される時期のタイムスタンプ
- パケット データが送信される方向 (出力または入力)
- キャプチャされたスイッチ パス
- L2 デコーダのデコードを可能にする入力または出力インターフェイスに対応するカプセル化のタイプ

キャプチャ バッファでは、次の作業を実行できます。

- キャプチャ バッファを定義し、キャプチャ ポイントと関連付けます。
- キャプチャ バッファをクリアします。

- オフライン分析用にキャプチャバッファをエクスポートします。サポートされたファイル転送オプション（FTP、HTTP、HTTPS、PRAM、RCP、SCP、およびTFTP）のいずれかを使用して、ファイルの書き込みをエクスポートします。
- キャプチャバッファの内容を表示します。

キャプチャポイント

キャプチャポイントは、パケットがキャプチャされ、バッファと関連付けられるトラフィックトランジットポイントです。一意の名前と異なるパラメータを提供することによって、キャプチャポイントを定義できます。

次のキャプチャポイントが使用できます。

- インターフェイス入力および出力がある IPv4 CEF/割り込みスイッチング パス
- インターフェイス入力および出力がある IPv6 CEF/割り込みスイッチング パス

キャプチャポイントでは、次の作業を実行できます。

- キャプチャポイントをキャプチャバッファと関連付けるか、関連付けを解除します。各キャプチャポイントは、1つのキャプチャバッファとだけ関連付けることができます。
- キャプチャポイントを破棄します。
- 特定のインターフェイスのパケットキャプチャポイントをアクティブにします。複数のパケットキャプチャポイントを特定のインターフェイスでアクティブにできます。たとえば、ボーダーゲートウェイプロトコル（BGP）パケットを1つのキャプチャバッファにキャプチャし、Open Shortest Path First（OSPF）パケットを別のキャプチャバッファにキャプチャできます。
- アクセスコントロールリスト（ACL）をキャプチャポイントに適用できます。

Embedded Packet Capture の実装方法

パケット データ キャプチャの開始

この作業を実行し、分析とトラブルシューティングのためのパケットデータのキャプチャを開始します。パケットデータをキャプチャするには、キャプチャバッファとキャプチャポイントを定義する必要があります。次に、キャプチャポイントをキャプチャバッファと関連付ける必要があります。キャプチャポイントをイネーブルにすると、パケットデータをキャプチャするプロセスが開始されます。

手順の概要

1. **enable**
2. **monitor capture buffer** *buffer-name* [**clear** | **export** *export-location* | **filter access-list** {*ip-access-list* | *ip-expanded-list* | *access-list-name*} | **limit** {**allow-nth-pak** *nth-packet* | **duration** *seconds* | **packet-count** *total-packets* | **packets-per-sec** *packets*} | [**max-size** *element-size*] [**size** *buffer-size*] [**circular** | **linear**]]
3. **monitor capture point** {**ip** | **ipv6**} {**cef** *capture-point-name interface-name interface-type* {**both** | **in** | **out**} | **process-switched** *capture-point-name* {**both** | **from-us** | **in** | **out**}}
4. **monitor capture point associate** *capture-point-name capture-buffer-name*
5. **monitor capture point start** {*capture-point-name* | **all**}

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。 • パスワードを入力します（要求された場合）。
ステップ 2	monitor capture buffer <i>buffer-name</i> [clear export <i>export-location</i> filter access-list { <i>ip-access-list</i> <i>ip-expanded-list</i> <i>access-list-name</i> } limit { allow-nth-pak <i>nth-packet</i> duration <i>seconds</i> packet-count <i>total-packets</i> packets-per-sec <i>packets</i> } [max-size <i>element-size</i>] [size <i>buffer-size</i>] [circular linear]] 例： Router# monitor capture buffer pktracel size 256 max-size 100 circular	キャプチャバッファを指定された名前とパラメータで定義します。 • この例では、pktracel という名前と、サイズが 256 バイト、バッファ要素の最大サイズが 100 バイトの循環式キャプチャ バッファが定義されています。
ステップ 3	monitor capture point { ip ipv6 } { cef <i>capture-point-name interface-name interface-type</i> { both in out } process-switched <i>capture-point-name</i> { both from-us in out }} 例： Router# monitor capture point ip cef ipceffa0/1 fastEthernet 0/1 both	キャプチャポイントを指定されたパラメータで定義します。 • この例では、ipceffa0/1 という名前と、ファストイーサネット 0/1 インターフェイスが両方向にあるキャプチャ ポイントが定義されています。
ステップ 4	monitor capture point associate <i>capture-point-name capture-buffer-name</i> 例： Router# monitor capture point associate ipceffa0/1 pktracel	キャプチャポイントを指定されたキャプチャ バッファと関連付けます。 • キャプチャポイントをキャプチャ バッファと関連付けると、指定されたキャプチャポイントからキャ

	コマンドまたはアクション	目的
		<p>プチャされたすべてのパケットが関連付けられたキャプチャバッファにダンプされます。</p> <ul style="list-style-type: none"> この例では、キャプチャポイント ipceffa0/1 がキャプチャバッファ pktrace1 と関連付けられています。
ステップ 5	monitor capture point start { <i>capture-point-name</i> all } 例 : <pre>Router# monitor capture point start ipceffa0/1</pre>	<p>キャプチャポイントでのパケットデータのキャプチャの開始をイネーブルにします。</p> <ul style="list-style-type: none"> この例では、キャプチャポイント ipceffa0/1 がイネーブルになっています。

パケット データ キャプチャの停止

パケットデータのキャプチャを停止するには、次の作業を実行します。

手順の概要

1. **enable**
2. **monitor capture point stop** {*capture-point-name* | **all**}

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>	<p>特権 EXEC モードをイネーブルにします。</p> <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	monitor capture point stop { <i>capture-point-name</i> all } 例 : <pre>Router# monitor capture point stop ipceffa0/1</pre>	<p>キャプチャポイントをディセーブルにし、パケットデータキャプチャプロセスを停止します。</p> <ul style="list-style-type: none"> この例では、キャプチャポイント ipceffa0/1 がディセーブルになっています。

分析のためのパケットデータのエクスポート

外部ツールを使用して、分析のためにパケットデータをエクスポートするには、次の作業を実行します。

手順の概要

1. **enable**
2. **monitor capture buffer** *buffer-name* **export** *export-location*

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 モードをイネーブルにします。 <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	monitor capture buffer <i>buffer-name</i> export <i>export-location</i> 例： <pre>Router# monitor capture buffer pktracel export tftp://10.1.88.9/pktracel</pre>	分析のためにデータをエクスポートします。 <ul style="list-style-type: none"> • この例では、キャプチャバッファ <code>pktracel</code> からのデータは、TFTP プロトコルを使用してエクスポートされます。

キャプチャされたデータのモニタリングとメンテナンス

キャプチャされたパケットデータのモニタリングとメンテナンスを行うには、次の作業を実行します。キャプチャバッファの詳細とキャプチャポイントの詳細を表示できます。

手順の概要

1. **enable**
2. **show monitor capture** **{buffer {capture-buffer-name [parameters] | all parameters | merged capture-buffer-name1 capture-buffer-name2}[dump] [filter filter-parameters]}** **| point {all | capture-point-name}}**
3. **debug packet-capture**

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。 <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	show monitor capture {buffer {capture-buffer-name [parameters] all parameters merged capture-buffer-name1 capture-buffer-name2}[dump] [filter filter-parameters]} point {all capture-point-name}} 例 : Router# show monitor capture buffer pktracel dump	キャプチャされたデータを表示します。 <ul style="list-style-type: none"> この例では、キャプチャバッファ pktracel からのデータが表示されています。
ステップ 3	debug packet-capture 例 : Router# debug packet-capture	パケットキャプチャインフラデバッグをイネーブルにします。

Embedded Packet Capture の設定例

パケット データ キャプチャの開始の例

次に、ファストイーサネット 0/1 インターフェイスから、またはファストイーサネット 0/1 インターフェイスにパケットをキャプチャする例を示します。

```
Router> enable
Router# monitor capture buffer pktracel ip cef ipceffa0/1 fastEthernet 0/1 both
Router# monitor capture point associate ipceffa0/1 pktracel
Router# monitor capture point start ipceffa0/1
Mar 21 11:13:34.023: %BUFCAP-6-ENABLE: Capture Point ipceffa0/1 enabled.
Router# show monitor capture point all
Status Information for Capture Point ipceffa0/1
IPv4 CEF
Switch Path: IPv4 CEF          , Capture Buffer: pktracel
Status : Inactive
Configuration:
monitor capture point ip cef ipceffa0/1 FastEthernet0/1 both
Router# show monitor capture buffer all
Capture buffer pktracel (circular buffer)
Buffer Size : 262144 bytes, Max Element Size : 256 bytes, Packets : 31
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
```

```

Associated Capture Points:
Name : ipceffa0/1, Status : Active
Configuration:
monitor capture buffer pktracel size 256 max-size 256 circular
monitor capture point associate ipceffa0/1 pktracel

```

パケット データ キャプチャの停止の例

次に、パケット データのキャプチャを停止する例を示します。

```

Router> enable
Router# monitor capture point stop ipceffa0/1
Mar 21 11:14:20.152: %BUFCAP-6-DISABLE: Capture Point ipceffa0/1 disabled.

```

パケット データのエクスポートの例

次に、外部ツールを使用して分析のためにデータをエクスポートする例を示します。

```

Router> enable
Router# monitor capture buffer pktracel export tftp://10.1.88.9/pktracel

```

キャプチャされたデータのモニタリングとメンテナンスの例

EPC 機能を使用すると、パケットを ASCII でダンプできます。次の例は、1つのホストから別のホストへの IPv4 ICMP エコー応答パケットを示します。

```

<timestamp>: IPv4 packet received on Ethernet0/0 in the IPv4 CEF LES switch path
029E28E0: AABECC01 2D00AABB CC013000 08004500 *;L.-.*;L.0...E.
029E28F0: 00640001 0000FE01 A8950A00 00020A00 .d....~.(.....
029E2900: 00010000 D5C80001 00000000 00000000 ....UH.....
029E2910: B080ABCD ABCDABCD ABCDABCD ABCDABCD 0.+M+M+M+M+M+M+M
029E2920: ABCDABCD ABCDABCD ABCDABCD ABCDABCD +M+M+M+M+M+M+M+M
029E2930: ABCDABCD ABCDABCD ABCDABCD ABCDABCD +M+M+M+M+M+M+M+M
029E2940: ABCDABCD ABCDABCD ABCDABCD ABCDABCD +M+M+M+M+M+M+M+M
029E2950: ABCD

```

次に、キャプチャバッファ `pktracel` の内容を表示する例を示します。この出力は、`show monitor capture buffer capture-buffer-name dump` コマンドを使用して表示されます。このコマンドは、デフォルトモードとダンプモードの2つのモードをサポートしています。ダンプモードでは、キャプチャされたパケットの16進数でのダンプも表示されます。

```

Router> enable
Router# show monitor capture buffer pktracel dump

11:13:00.593 EDT Mar 21 2007 : IPv4 Turbo          : Fa2/1 Fa0/1
65B6F500: 080020A2 44D90009 E94F8406 08004500 .. "DY..iO...E.
65B6F510: 00400F00 0000FE01 92AF5801 13025801 .@....~..-/X...X.
65B6F520: 58090800 4D1A1169 00000000 0005326C X...M..i.....21
65B6F530: 01CCABCD ABCDABCD ABCDABCD ABCDABCD .L+M+M+M+M+M+M+M
65B6F540: ABCDABCD ABCDABCD ABCDABCD ABCD00 +M+M+M+M+M+M+M.
11:13:20.593 EDT Mar 21 2007 : IPv4 Turbo          : Fa2/1 Fa0/1

65B6F500: 080020A2 44D90009 E94F8406 08004500 .. "DY..iO...E.
65B6F510: 00400F02 0000FE01 92AD5801 13025801 .@....~..-X...X.
65B6F520: 58090800 FEF91169 00000000 0005326C X...~y.i.....21
65B6F530: 4FECABCD ABCDABCD ABCDABCD ABCDABCD 0l+M+M+M+M+M+M+M
65B6F540: ABCDABCD ABCDABCD ABCDABCD ABCDFE +M+M+M+M+M+M+M

```

次に、パケット キャプチャ インフラ デバッグをイネーブルにする例を示します。

```
Router> enable
Router# debug packet-capture
Buffer Capture Infrastructure debugging is on
```

その他の関連資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『 Cisco IOS Master Commands List, All Releases 』
ネットワーク管理コマンド（EEM コマンドを含む）：コマンド構文の詳細、デフォルト設定、コマンドモード、コマンド履歴、使用上のガイドライン、および例	『 <i>Cisco IOS Network Management Command Reference</i> 』

標準

標準	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

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。	選択したプラットフォーム、Cisco IOS リリース、およびフィー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。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンラインリソースを提供しています。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

Embedded Packet Capture 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 2 : *Embedded Packet Capture* の機能情報

機能名	リリース	機能情報
Embedded Packet Capture	12.2(33)SRE 12.4(20)T	

機能名	リリース	機能情報
		<p>Cisco IOS Embedded Packet Capture (EPC) は、ネットワーク管理者がデバイスを出入りするかデバイスを通るパケットをキャプチャし、パケットをローカルで分析するか、または Wireshark のようなツールを使用してオフライン分析を行うために、パケットを保存してエクスポートできるようにするオンボードパケットキャプチャファシリティです。この機能は、デバイスがネットワークの管理と操作にアクティブに参加できるようにすることによって、操作を簡略化します。この機能は、パケットの形式に関する情報を収集することによって、よりよいトラブルシューティングを容易にします。また、アプリケーションの分析とセキュリティも容易にします。</p> <p>この機能は Cisco IOS Release 12.4(20)T で導入され、Cisco IOS Release 12.2(33)SRE に統合されました。</p> <p>(注) Cisco IOS Release 12.2(33)SRE では、EPC は 7200 プラットフォームでのみサポートされます。</p> <p>次のコマンドが導入または変更されました。</p> <p>debug packet-capture、monitor capture buffer、monitor capture point、monitor capture point associate、monitor capture point disassociate、monitor capture point start、monitor capture point stop、show monitor capture。</p>



索引

き

キャプチャ バッファの内容の表示 [9](#)
キャプチャ ポイントの定義 [4](#)

て

デバイス上でのキャプチャ バッファの定義 [3](#)

と

トレース ポイントにおけるパケット データのバッファへのキャプチャ [4, 8](#)

