

ソフトウェア強制クラッシュについて

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[考えられる原因](#)

[トラブルシューティング](#)

[設定手順](#)

[TFTP サーバ ホストの設定手順](#)

[TAC のサービスリクエストをオープンする場合に収集すべき情報](#)

[関連情報](#)

概要

このドキュメントでは、ソフトウェア強制クラッシュの原因として最も頻度の高いものについて説明し、さらに、トラブルシューティングのために収集する必要がある情報について説明します。ソフトウェア強制クラッシュの TAC サービス リクエストをオープンする場合は、収集するように要求される情報は、問題のトラブルシューティングに必要です。

前提条件

要件

このドキュメントの読者は次のトピックについて理解している必要があります。

- [ルータのクラッシュのトラブルシューティング](#)方法。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

ルータによって深刻で修復不可能なエラーが検出されると、ソフトウェアによる強制クラッシュ

が発生し、破損したデータの送信を防止するためにリロードが実行されます。ソフトウェア強制クラッシュの圧倒的多数は Cisco IOS[®] ソフトウェアバグによっていくつかのプラットフォームがソフトウェア強制クラッシュとして (古い Cisco 4000 のような) ハードウェア上の問題を報告できるが、引き起こされます。

ルータの電源のオフ/オンや手動でのリロードを行っていないければ、show version コマンドからの出力が次のように表示されます。

```
Router uptime is 2 days, 21 hours, 30 minutes
System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt
System image file is "flash:c2500-is-l.112-15a.bin", booted via flash
```

Cisco デバイスからの show version コマンドの出力がある場合、潜在的な問題および修正を表示するのに [Cisco CLI アナライザ](#) ([登録ユーザのみ](#)) を使用できます。

考えられる原因

次の表に、ソフトウェア強制クラッシュの考えられる原因を示します。

原因	説明
ウォッチドッグ タイムアウト	プロセッサは無限ループを避けるためにタイマーを使用していますが、これが原因でルータのタイマーは CPU によって定期的な間隔でリセットされます。これに失敗した場合、ソフトウェア強制クラッシュとしてレポートされるウォッチドッグ タイムアウトは、ソフトウェア強制クラッシュとしてレポートされるウォッチドッグ タイムアウトのトラブルシューティングについては、 ウォッチドッグ タイムアウトのトラブルシューティング ドキュメントがループ状態に陥っています。そのため、スタックトレースは必ずしも関係があるソフトウェア強制クラッシュは、コンソール ログの次の行から識別できます。 Router uptime is 2 days, 21 hours, 30 minutes System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt System image file is "flash:c2500-is-l.112-15a.bin", booted via flash
メモリ不足	ルータはメモリが極端に少なくなると、自らリロードしてソフトウェア強制クラッシュは、コンソール ログに次のようなメモリ割り当てエラー メッセージが表示されます。 Router uptime is 2 days, 21 hours, 30 minutes System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt System image file is "flash:c2500-is-l.112-15a.bin", booted via flash ブートアップの際に、ルータによって Cisco IOS ソフトウェア イメージが破損しているため「checksum is incorrect」というメッセージが返され、リロードが行われます。この場合、ソフトウェア強制クラッシュとして報告されます。 Router uptime is 2 days, 21 hours, 30 minutes System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt System image file is "flash:c2500-is-l.112-15a.bin", booted via flash
ソフトウェア イメージの破損	これは、ルータへの転送の際に実際に破損した Cisco IOS ソフトウェア イメージによりルータに新しいイメージをロードすることによって問題を解決することができます。 [プラットフォーム固有の ROMmon 復旧手順を参照してください。] また、この現象は、メモリのハードウェア故障が発生する場合があります。
その他の障害	クラッシュの原因になったエラーは、多くの場合、プロセッサ ハードウェアによって検出された特別なエラー処理コードが呼び出されます。 ROM モニタはエラーを識別し、メッセージを使用してシステムを再起動します。しかし、これらのいずれも行われなかったクラッシュも存在し (ソフトウェアが問題を検出して、クラッシュダンプ機能と呼ばれたクラッシュも存在し、ソフトウェア強制クラッシュとも言えます。少なくともごく最近まで、Power PC プラットフォームでは、「SIGTRAP」例外と呼ばれていました。その件はリリース 12.2(12.7) より前) では、これらは「SIGTRAP」例外と呼ばれていました。その件は、

トラブルシューティング

ソフトウェア強制クラッシュは、通常は Cisco IOS ソフトウェアのバグによって発生します。メモリ割り当てエラー メッセージがログに表示される場合は、[メモリ問題のトラブルシューティング](#)を参照してください。

メモリアロケーション障害 エラーメッセージが表示されないし、ソフトウェア強制クラッシュの後で手動でルータをリロードしなかったし、またはパワーサイクルを行わなかったら場合、である既知 マッチするバグID を探す [Cisco CLI アナライザ \(登録ユーザのみ\)](#) 使用できる最もよいツール。このツールには、従来のスタック デコーダ ツールの機能が組み込まれています。

例：

1. ルータから **show stack** の出力を収集します。
2. [Cisco CLI アナライザ \(登録ユーザのみ\)](#) ツールに行ってください。
3. プルダウン メニューから [show stack] を選択します。
4. 収集した出力を貼り付けます。
5. [Submit] をクリックします。 **show stack** コマンドからのデコード出力が既知のソフトウェアバグと一致する場合は、ソフトウェア強制クラッシュの原因である可能性が最も高いソフトウェアバグのバグ ID が送信されます。
6. バグ ID のハイパーリンクをクリックすると、[Cisco Bug Toolkit \(登録ユーザ専用\)](#) からのバグ詳細情報が表示されます。この情報は、バグ ID が一致しているかどうかの判別に役立ちます。

エラーと一致するバグ ID が特定されたら、「fixed in」フィールドを参照して、そのバグの修正が入っている最初の Cisco IOS ソフトウェア バージョンを確認します。

バグ ID が不明な場合、または問題の修正が入っている Cisco IOS ソフトウェア バージョンが不明な場合は、Cisco IOS ソフトウェアをリリース群の最新バージョンにアップグレードします。最新バージョンには多数のバグに対する修正プログラムが含まれているため、この方法は有効です。問題が解決しなくても、ソフトウェアが最新バージョンになっていることによって、バグの報告や解決プロセスが簡単かつ迅速になります。

Cisco CLI アナライザを使用した後、未解決に残る不具合を疑うか、または肯定的に識別したら、不具合が最終的に解決される時その他の情報を提供するように不具合の解決を助けるように TAC サービス リクエストを開くおよび推奨しますことをより速い通知のために。

設定手順

問題が新規のソフトウェアバグであることが確認された場合は、シスコ TAC エンジニアからお客様に、ルータでコア ダンプが収集されるように設定することをお願いする場合があります。コア ダンプは、ソフトウェアバグの修正方法を突きとめるために必要になることがあります。

コア ダンプでできるだけ有用な情報を収集するため、隠しコマンド **debug sanity** を使用することをお勧めします。これにより、システム内で使用されるすべてのバッファについて、それらの割り当て時および解放時に正常性がチェックされます。 **debug sanity** コマンドは特権 EXEC モード (イネーブルモード) で発行する必要があるため、多少 CPU を必要としますが、ルータの機能に大きな影響を与えることはありません。サニティチェックを無効にするには、**undebug sanity** 特権 EXEC コマンドを使用します。

ルータのメイン メモリが 16 MB 以下の場合、Trivial File Transfer Protocol (TFTP; トリビアル

ファイル転送プロトコル)を使用してコア ダンプを収集できます。ルータのメイン メモリが 16 MB を超える場合は、File Transfer Protocol (FTP; ファイル転送プロトコル) を使用することをお勧めします。このセクションの設定手順を使用します。または、[コア ダンプの作成](#)を参照してください。

ルータを設定するには、次の手順を実行します。

1. `configure terminal` コマンドを使用してルータを設定します。
2. 「`exception dump n.n.n.n`」と入力します。ここで、n.n.n.n はリモート Trivial File Transfer Protocol (TFTP) サーバ ホストの IP アドレスです。
3. 設定モードを終了します。

TFTP サーバ ホストの設定手順

次の手順を実行して、TFTP サーバ ホストを設定します。

1. 任意のエディタを使用して、リモート ホストの /tftpboot ディレクトリの下にファイルを作成します。ファイル名は Cisco ルータのホスト名-core です。
2. UNIX システムでは、「ホスト名-core」の権限モードを 666 に変更し、グローバルに互換性のあるものとします。TFTP セットアップを検査するには、そのファイルに `copy running-config tftp` コマンドを使用します。
3. /tftpboot の下に 16 MB を超える空きディスク領域があることを確認します。システムがクラッシュすると、`exception dump` コマンドによって上記のファイルへの出力が作成されます。ルータのメイン メモリが 16 MB を超える場合は、File Transfer Protocol (FTP) または Remote Copy Protocol (RCP) を使用してコア ダンプを取得する必要があります。ルータで、次のように設定します。

```
exception protocol ftp
exception dump n.n.n.n
ip ftp username <string> ip ftp password <string> ip ftp source-interface
<slot/port/interface> exception core-file <core-filename>
```

[コア ダンプを収集したら、ftp://ftp-sj.cisco.com/incoming にアップロードし \(UNIX の場合は pftp ftp-sj.cisco.com と入力してから cd incoming と入力し \)、所有者にこの事例とファイル名を通知します。](#)

TAC のサービスリクエストをオープンする場合に収集すべき情報

上記のトラブルシューティング方法を実行した後も、依然としてサポートが必要で、Cisco TAC でサポート

- `show technical-support` の出力 : `show technical-support` コマンドの出力には、ルータの現在の状態の
- コンソール ログ : 通常は syslog サーバに保存されるコンソール ログは、クラッシュ前にルータ上で合、収集可能な最も重要な情報になります。
- [crashinfo ファイル](#) (存在する場合) : トラブルシューティングを成功させるためには、crashinfo 機そのためには、バージョンがネットワークの他のニーズを満たしている必要があります。crashinfo [ファイルからの情報の取得](#)」を参照するか、[Software Advisor \(登録ユーザ専用 \)](#) ツールを使用してサポートする新しい IOS ソフトウェア リリースに切り替えることによってバグが修正されること情報をサービス リクエストに添付するには、[TAC Service Request Tool \(登録ユーザ専用 \)](#) を使用して電子メールの添付ファイルとし、メッセージの件名にサービス リクエスト番号を付けて [attach@cisco.c](#)

注意：問題の根本原因を特定するのに必要な重要情報が失われる可能性があるため、可能な限り、上記
ください。

関連情報

- [Crashinfo ファイルからの情報の取得](#)
- [コア ダンプの作成](#)
- [メモリの問題に関するトラブルシューティング](#)
- [テクニカルサポート - Cisco Systems](#)