



TCP リセット セグメント制御

TCP リセット セグメント制御機能は、ハーフクローズ セッション、ハーフオープン セッション、またはアイドル セッションのセッション削除が発生した場合に TCP リセット (RST) セグメントが送信されるかどうかを設定するメカニズムを提供します。

- [機能情報の確認, 1 ページ](#)
- [TCP リセット セグメント制御について, 2 ページ](#)
- [TCP リセット セグメント制御の設定方法, 3 ページ](#)
- [TCP リセット セグメント制御の設定例, 7 ページ](#)
- [TCP リセット セグメント制御の追加情報, 8 ページ](#)
- [TCP リセット セグメント制御の機能情報, 9 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。最新の注意事項と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。

TCP リセット セグメント制御について

TCP リセット セグメント制御

TCP ヘッダーには、リセット (RST) フラグと呼ばれるフラグが含まれます。参照される接続の基準を満たさないセグメントが到着するたびに、RST フラグが設定された TCP セグメントが送信されます。たとえば、接続要求が宛先ポートで受信されたが、そのポートでリッスンしているプロセスがない場合、RST フラグが設定された TCP セグメントが送信されます。

この動作は、ホスト間通信用に RFC 793、『Transmission Control Protocol』で定義され、さまざまなベンダーによって実装されています。ただし、ホスト間のネットワークに存在するネットワークデバイスの場合、セッション（ハーフオープン、アイドル、ハーフクローズ）がクリアされたときに、デバイスが TCP RST セグメントを接続の開始側、受信側、またはその両方に送信するかどうかを決定する特定のルールは定義されていません。一部のデバイスは、セッションがクリアされると、送信元ポートおよび受信側ポートの両方に TCP RST セグメントを送信する一方で、一部のデバイスは、TCP RST セグメントを送信せずにセッションテーブル内のセッションを暗黙的に削除します。

TCP リセットセグメント制御機能は、ハーフクローズセッション、ハーフオープンセッション、またはアイドルセッションのセッションがクリアされた場合に TCP RST セグメントを送信するかどうかを設定するメカニズムを提供します。

ハーフオープンセッションは、TCP 同期 (SYN) セグメントによって開始されたが、TCP スリーウェイ ハンドシェイクが発生しただけの不完全な未確立セッションであり、タイマーが起動されます。

TCP は、接続の一方の端が、接続の反対の端からのデータを引き続き受信する一方で、その出力を終了する機能を提供します。この TCP 状態は、ハーフクローズと呼ばれます。セッションは、最初の TCP FIN セグメントを受信するとハーフクローズ状態になり、タイマーを起動します。セッションがタイムアウトする前に別のセグメントを受信した場合、タイマーが再起動されます。

tcp synwait-time コマンドを使用して、ハーフオープンセッションとハーフクローズセッションのタイムアウト値を設定できます。デフォルトのタイムアウト値は 30 秒です。

アイドルセッションは、2 つのデバイス間でアクティブで、長期にわたっていずれのデバイスからもデータが送信されない TCP セッションです。 **tcp idle-time** コマンドを使用して、アイドルセッションのタイムアウト値を設定できます。アイドルセッションのデフォルトのタイムアウト値は 3600 秒です。

タイムアウトが TCP セッションで発生し、セッションがクリアされると、TCP RST セグメントが送信され、TCP リセットセグメント制御がセッションに設定されている場合のみ、セッションがリセットされます。

TCP リセット セグメント制御の設定方法

ハーフオープン セッションの TCP リセットの設定

ハーフオープンセッションは、TCP 同期 (SYN) セグメントによって開始されたが、スリーウェイ ハンドシェイクが不完全な未確立セッションです。不完全なスリーウェイ ハンドシェイクが発生するとただちに、タイマーが起動されます。 **tcp synwait-time** コマンドを使用して、ハーフオープンセッション タイムアウトのタイマー値を設定できます。これらのセッションのデフォルトのタイムアウト値は 30 秒です。

タイムアウトが発生すると、ハーフオープン TCP セッションのセッションはクリアされ、TCP リセット (RST) セグメントが送信され、TCP リセット セグメント制御がセッションで設定されている場合のみ、セッションがリセットされます。

tcp half-open reset on コマンドを設定している場合は、セッションがクリアされると、ハーフオープンセッションの両端に TCP RST セグメントが送信されます。**tcp half-open reset off** コマンドを設定している場合は、セッションがクリアされても TCP RST セグメントは送信されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect *parameter-map-name***
4. **tcp synwait-time *seconds***
5. **tcp half-open reset {off | on}**
6. **end**

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 : Device> 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	configure terminal 例 : Device# configure terminal	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。

	コマンドまたはアクション	目的
ステップ 3	parameter-map type inspect <i>parameter-map-name</i> 例 : Device(config)# parameter-map type inspect pmap-name	(任意) 接続しきい値、タイムアウト、および inspect キーワードに関連するその他のパラメータの検査パラメータマップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	tcp synwait-time seconds 例 : Device(config-profile)# tcp synwait-time 10	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。
ステップ 5	tcp half-open reset {off on} 例 : Device(config-profile)# tcp half-open reset on	タイムアウトが発生し、ハーフオープンセッションのセッションがクリアされた場合に、TCP RST セグメントが送信されるかどうかを指定します。
ステップ 6	end 例 : Device(config-profile)# end	パラメータマップタイプ検査コンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

ハーフクローズ セッションの TCP リセットの設定

TCP は、接続の一方の端が、接続の反対の端からのデータを引き続き受信する一方で、その出力を終了する機能を提供します。この TCP 状態は、ハーフクローズと呼ばれます。セッションは、最初の TCP finish (FIN) セグメントを受信するとハーフクローズ状態になり、タイマーを起動します。セッションがタイムアウトする前に別のセグメントを受信した場合、タイマーが再起動されます。 **tcp synwait-time** コマンドを使用して、ハーフクローズセッションのタイムアウト値を設定できます。ハーフクローズセッションのデフォルトのタイムアウト値は 30 秒です。

タイムアウトがハーフクローズ TCP セッションで発生すると、TCP RST セグメントが送信され、TCP リセットセグメント制御がセッションに設定されている場合のみ、セッションがリセットされます。

tcp half-close reset on コマンドを設定している場合は、タイムアウトが発生し、セッションがクリアされると、ハーフオープンセッションの両端に TCP RST セグメントが送信されます。 **tcp half-close reset off** コマンドを設定している場合は、セッションタイムアウトが発生し、セッションがクリアされても、TCP RST セグメントは送信されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp synwait-time** *seconds*
5. **tcp half-close reset** {**off** | **on**}
6. **end**

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： Device> 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	configure terminal 例： Device# configure terminal	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	parameter-map type inspect <i>parameter-map-name</i> 例： Device(config)# parameter-map type inspect pmap-name	接続しきい値、タイムアウト、および inspect キーワードに関連するその他のパラメータの検査パラメータマップを設定し、パラメータ マップ タイプ 検査 コンフィギュレーション モードを開始します。
ステップ 4	tcp synwait-time <i>seconds</i> 例： Device(config-profile)# tcp synwait-time 10	（任意）セッションをドロップする前に、TCP セッションが設定された状態に達するまで待機する時間を指定します。
ステップ 5	tcp half-close reset { off on } 例： Device(config-profile)# tcp half-close reset on	セッションの削除がハーフオープンセッションで発生した場合に TCP RST セグメントが送信されるかどうかを指定します。
ステップ 6	end 例： Device(config-profile)# end	パラメータマップタイプ検査コンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

アイドルセッションの TCP リセットの設定

アイドルセッションは、2つのデバイス間でアクティブで、長期にわたっていずれのデバイスからもデータが送信されていない TCP セッションです。 **tcp idle-time** コマンドを使用して、アイドルセッションのタイムアウト値を設定できます。アイドルセッションのデフォルトのタイムアウト値は 3600 秒です。

タイムアウトがアイドル TCP セッションで発生すると、TCP RST セグメントが送信され、TCP リセット セグメント制御がセッションに設定されている場合はセッションがリセットされます。

tcp idle reset on コマンドを設定している場合は、タイムアウトが発生し、セッションがクリアされると、アイドルセッションの両端に TCP RST セグメントが送信されます。**tcp idle reset off** コマンドをしている場合は、セッションタイムアウトが発生し、セッションがクリアされても、TCP RST セグメントは送信されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect *parameter-map-name***
4. **tcp idle-time *seconds***
5. **tcp idle reset {off | on}**
6. **end**

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： Device> 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	configure terminal 例： Device# configure terminal	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	parameter-map type inspect <i>parameter-map-name</i> 例： Device(config)# parameter-map type inspect pmap-name	接続しきい値、タイムアウト、および inspect キーワードに関連するその他のパラメータの検査パラメータ マップを設定し、パラメータ マップ タイプ 検査 コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	tcp idle-time seconds 例 : Device(config-profile)# tcp idle-time 90	(任意) TCP セッションのタイムアウトを設定します。
ステップ 5	tcp idle reset {off on} 例 : Device(config-profile)# tcp idle reset on	セッションの削除がアイドルセッションで発生した場合に TCP RST セグメントが送信されるかどうかを指定します。
ステップ 6	end 例 : Device(config-profile)# end	パラメータ マップ タイプ検査コンフィギュレーションモードを終了し、特権 EXEC モードを開始します。

TCP リセット セグメント制御の設定例

例：ハーフオープンセッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp synwait-time 10
Device(config-profile)# tcp half-open reset on
Device(config-profile)# end
```

例：ハーフクローズセッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp synwait-time 10
Device(config-profile)# tcp half-close reset on
Device(config-profile)# end
```

例：アイドルセッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp idle-time 90
Device(config-profile)# tcp idle reset on
```

```
Device(config-profile)# end
```

TCP リセット セグメント制御の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	『Cisco IOS Security Command Reference: Commands A to C』 『Cisco IOS Security Command Reference: Commands D to L』 『Cisco IOS Security Command Reference: Commands M to R』 『Cisco IOS Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 793	『Transmission Control Protocol』

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

TCP リセット セグメント制御の機能情報

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: TCP リセット セグメント制御の機能情報

機能名	リリース	機能情報
TCP リセット セグメント制御	Cisco IOS XE Release 3.8S	TCP リセット セグメント制御機能は、ハーフオープン セッション、ハーフクローズ セッション、およびアイドル セッションのセッションがクリアされた場合に、TCP RST ビットが送信されるかどうかを設定するための一貫したメカニズムを提供します。 次のコマンドが導入または変更されました。tcp idle reset、tcp half-close reset、および tcp half-open reset。

