# 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、ハーフオープン、またはアイドルセッションに対して、セッション削除が発生したときにTCP リセット（RST）セグメントを送信する必要があるかどうかを設定するメカニズムを提供します。


- TCP リセット セグメント制御について （1 ページ）
- TCP リセット セグメント制御の設定方法 （2 ページ）
- TCP リセット セグメント制御の設定例 （6 ページ）
- TCP リセット セグメント制御に関する追加情報 （7 ページ）
- TCP リセット セグメント制御に関する機能情報 （8 ページ）


# 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）フラグというフラグが含まれます。TCPセグメントは、参照される接続の条件を満たしていないセグメントが到着するたびに、RSTフラグとともに送信されます。たとえば、接続要求が宛先ポートで受信されたにもかかわらず、そのポートでリッスンしているプロセスがない場合、TCPセグメントはRSTフラグとともに送信されます。

この動作は、ホスト間通信用に RFC 793 の伝送制御プロトコルで定義され、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あるネットワークデバイスに関しては、セッション（ハーフオープン、アイドル、ハーフクローズ）のクリア時に、デバイスが接続の発信側、受信側、またはその両方に TCP RST セグメントを送信する必要があるかどうかを判別するための特定の規則が定義されていません。一部のデバイスはセッションのクリア時に送信側と受信側の両方のポートにTCPRSTセグメントを送信しますが、TCPRSTセグメントを送信せずにセッションテーブルのセッションを暗黙的に削除するデバイスもあります。

TCP リセットセグメント制御機能は、ハーフクローズ、ハーフオープン、またはアイドルセッションに対して、セッションがクリアされるときに TCP RST セグメントを送信する必要があ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未確立のセッションで、TCP スリーウェイ ハンドシェイクのみが発生し、タイマーが開始されるため、不完全です。

TCPは、接続の一端で出力を終了すると同時に、接続のもう他端からデータを受信し続け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セグメントを受信し、タイマーが起動すると、ハーフクローズ状態になります。セッションがタイム アウトになる前に別のセグメントを受信した場合、タイマーが再開されます。

ハーフオープンおよびハーフクローズのセッションのタイムアウト値は、それぞれ **tcp synwait-time** コマンドと **tcp finwait-time** コマンドを使用して設定できます。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、長時間どちら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。アイドルセッションのタイムアウト値は、**tcp idle-time** コマンドを使用して設定できます。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。

TCPセッションでタイムアウトが発生し、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、セッションに TCP リセット セグメント制御が設定されている場合に限り、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とは、TCP 同期（SYN）セグメントによって開始されたが、3 ウェイ ハンドシェイクがまだ完了していない未確立セッションです。未完了 3 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開始します。**tcp synwait-time** コマンドを使用すると、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。このようなセッションのデフォルト タイムアウト値は 30 秒です。

ハーフオープンTCPセッションでタイムアウトが発生してセッションがクリアされると、セッションで TCP リセット セグメント制御が設定されている場合にのみ、TCP リセット（RST）セグメントが送信されてセッションがリセットされます。

**tcp half-open reset on** コマンドを設定すると、セッションがクリアされたときに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** コマンドを設定すると、セッションがクリアされても TCP RST セグメントは伝送されません。

### 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**<br>例：<br>`Device> 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 | **configure terminal**<br>例：<br>`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** *parameter-map-name*<br>例：<br>`Device(config)# parameter-map type inspect pmap-name` | （任意）接続しきい値、タイムアウト、その他の **inspect** キーワードに関連するパラメータに対する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*<br>例：<br>`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なるのを待機する時間を指定します。 |
| ステップ 5 | **tcp half-open reset** {**off** \| **on**}<br>例：<br>`Device(config-profile)# tcp half-open reset on` | ハーフオープン セッションのタイムアウトが発生して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**<br>例：<br>`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 では、接続の一方の終端が出力を終了しても、接続のもう一方の終端から引き続きデータを受信することができます。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 終了（FIN）セグメントを受信するとハーフクローズ状態になり、タイマーを開始します。セッションがタイムアウトになる前に別のセグメントを受信した場合、タイマーが再開されます。**tcp finwait-time** コマンドを使用すると、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。ハーフクローズ セッションのデフォルト タイムアウト値は 30 秒です。

ハーフクローズ TCP セッションでタイムアウトが発生すると、セッションで TCP リセット セグメント制御が設定されている場合にのみ、TCP RST セグメントが送信されてセッションがリセットされます。

**tcp half-close reset on** コマンドを設定すると、タイムアウトが発生してセッションがクリアされたときに、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** コマンドを設定すると、セッションタイムアウトが発生してセッションがクリアされたときに TCP RST セグメントが伝送されません。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp finwait-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**<br>例：<br>`Device> 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 | **configure terminal**<br>例：<br>`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** *parameter-map-name*<br>例：<br>`Device(config)# parameter-map type inspect pmap-name` | 接続しきい値、タイムアウト、その他の **inspect** キーワードに関連するパラメータに対する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 finwait-time** *seconds*<br>例：<br>`Device(config-profile)# tcp finwait-time 10` | （任意）ファイアウォールが FIN-exchange を検出してから TCP セッションが管理される時間を指定します。 |
| ステップ 5 | **tcp half-close reset** {**off** \| **on**}<br>例：<br>`Device(config-profile)# tcp half-close reset on` | ハーフオープンセッションでセッション削除が発生した場合に 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**<br>例：<br>`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とは、2つのデバイス間でアクティブな、長時間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。アイドルセッションのタイムアウト値は、**tcp idle-time** コマンドを使用して設定できます。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。

アイドル TCP セッションでタイムアウトが発生すると、セッションで TCP リセット セグメント制御が設定されている場合には TCP RST セグメントが送信され、セッションがリセットされます。

**tcp idle reset on** コマンドを設定すると、タイムアウトが発生してセッションがクリアされたときに、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** コマンドを設定すると、セッションタイムアウトが発生してセッションがクリアされたときに TCP RST セグメントが伝送されません。

## 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**<br>例：<br>`Device> 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 | **configure terminal**<br>例：<br>`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** *parameter-map-name*<br>例：<br>`Device(config)# parameter-map type inspect pmap-name` | 接続しきい値、タイムアウト、その他の **inspect** キーワードに関連するパラメータに対する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 idle-time** *seconds*<br>例：<br>`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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **tcp idle reset** {**off** \| **on**}<br>例：<br>`Device(config-profile)# tcp idle reset on` | アイドルセッションでセッション削除が発生した場合に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**<br>例：<br>`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 finwait-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 セグメント制御に関する追加情報

## 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』<br>• 『Cisco IOS Security Command Reference: Commands D to L』<br>• 『Cisco IOS Security Command Reference: Commands M to R』<br>• 『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 |
|---|---|
| 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。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。

**表 *1: TCP* リセット セグメント制御に関する機能情報**

| 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 リリース 3.8S | TCP リセット セグメント制御機能は、ハーフオープン、ハーフクローズ、およびアイドル セッションに関するセッションがクリアされたときに TCP RST ビットが送出されるように設定するための一貫したメカニズムを提供します。<br><br>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**、**tcp half-open reset** |

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。