IP アドレッシング：フラグメンテーションおよびリアセンブル コンフィギュレーション ガイド

初版：2012 年 12 月 05 日

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。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。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。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号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、ネットワーク トポロジ図、およびその他の図は、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および電話番号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。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/go/trademarksでご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください。 1

仮想フラグメンテーション リアセンブル 3

機能情報の確認 3

仮想フラグメンテーション リアセンブルの制約事項 4

パフォーマンス上の影響 4

VFR の設定 4

仮想フラグメンテーション リアセンブルに関する情報 4

VFR によるフラグメント攻撃の検出 4

VFR の有効化 5

VFR の無効化 6

アウトバウンド インターフェイスの VFR 7

仮想フラグメンテーション リアセンブルの設定方法 7

VFR の設定 7

アウトバウンド インターフェイス トラフィックに対する VFR の手動有効化 9

トラブルシューティングのヒント 10

仮想フラグメンテーション リアセンブルの設定例 11

例：アウトバウンド インターフェイス トラフィックに対する VFR の設定 11

仮想フラグメンテーション リアセンブルのその他の参考資料 11

仮想フラグメンテーション リアセンブルの機能情報 12

IPv6 仮想フラグメンテーション リアセンブル 15

機能情報の確認 15

IPv6 仮想フラグメンテーション リアセンブルに関する情報 16

IPv6 仮想フラグメンテーション リアセンブル 16

IPv6 仮想フラグメンテーション リアセンブルの導入方法 16

IPv6 仮想フラグメンテーション リアセンブルの設定 16

IPv6 仮想フラグメンテーション リアセンブルの設定例 18

例：IPv6 仮想フラグメンテーション リアセンブルの設定 18

その他の参考資料 18
IPv6 仮想フラグメンテーション リアセンブルの機能情報 19
GRE フラグメントおよびリアセンブル パフォーマンス チューニング 21
機能情報の確認 21
GRE フラグメントおよびリアセンブルの制約事項 22
GRE フラグメントおよびリアセンブルの情報 22
フラグメンテーションとリアセンブル 22
Out-of-Order パケットの処理 22
GRE フラグメントおよびリアセンブルの使用方法 23
GRE フラグメントおよびリアセンブル（GFR）の設定 23
GRE フラグメントおよびリアセンブルの設定例 25
例：GFR の設定 25
GRE フラグメントおよびリアセンブルのその他の参考資料 25
GRE フラグメントおよびリアセンブルの機能情報 26

第 1 章

最初にお読みください。

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと発展しています。これにより、スイッチングおよびルーティング ポートフォリオの幅広い範囲のアクセスおよびエッジ製品に 1 つのリリースで対応できます。

（注） 技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディング ページに表示されている場合は、その機能がプラットフォームでサポートされていることを示します。

第 2 章

仮想フラグメンテーション リアセンブル

仮想フラグメンテーション リアセンブル（VFR）は、一部の機能（NAT、Cisco IOS XE Firewall、IPSec など）によってレイヤ4またはレイヤ7の情報を取得するために自動的に有効化されます。VFR を使用すると、Cisco IOS XE Firewall で適切なダイナミック アクセス コントロール リスト（ACL）を作成してさまざまなフラグメンテーション攻撃からネットワークを防御できます。

レイヤ4ヘッダーは通常、最初のフラグメントとともに移動するため、最初以外のフラグメントのほとんどにはレイヤ4ヘッダーがありません（マイクロフラグメンテーションおよびタイニーフラグメントの場合を除く）。このため、一部の機能（NAT、Cisco IOS XE Firewall、IPSec など）はパケットからポート情報を収集できません。これらの機能では、レイヤ 7 ペイロードをチェックする必要があります。このペイロードのためにフラグメントをリアセンブルし、後から再フラグメント化する必要があります。

- 機能情報の確認，3 ページ
- 仮想フラグメンテーション リアセンブルの制約事項，4 ページ
- 仮想フラグメンテーション リアセンブルに関する情報，4 ページ
- 仮想フラグメンテーション リアセンブルの設定方法，7 ページ
- 仮想フラグメンテーション リアセンブルの設定例，11 ページ
- 仮想フラグメンテーション リアセンブルのその他の参考資料，11 ページ
- 仮想フラグメンテーション リアセンブルの機能情報，12 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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、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。

仮想フラグメンテーション リアセンブルの制約事項

パフォーマンス上の影響

VFR はパケットのコピー、フラグメントの検証、フラグメントの再順序付けなどの機能に基づいてパフォーマンスに影響を及ぼします。このパフォーマンスへの影響は、リアセンブルされる同時 IP データグラムの数によって異なります。

VFR の設定

リアセンブル プロセスでは IP データグラム内のすべてのフラグメントが必要です。ロード バランシングによって、IPデータグラム内のフラグメントが異なるデバイスに送信された場合（パケットごとのロード バランシングまたは Cisco Catalyst 6500 シリーズ スイッチまたは Cisco Nexus デバイスのポートを含む）、VFR が失敗し、フラグメントは廃棄される可能性があります。

仮想フラグメンテーション リアセンブルに関する情報

VFR によるフラグメント攻撃の検出

VFR は、次のタイプのフラグメント攻撃を検出および防止します。

- タイニーフラグメント攻撃：このタイプの攻撃では、攻撃者はフラグメントのサイズを非常に小さくすることで、レイヤ 4（TCP および UDP）ヘッダーフィールドを次のフラグメントに強制的に挿入します。したがって、これらのフィールドに設定した ACL ルールは一致しません。

- VFR はすべての小さいフラグメントを破棄し、「VFR-3-TINY_FRAGMENTS」などの警告メッセージが syslog サーバにログ記録されます。

- オーバーラッピング フラグメント攻撃：このタイプの攻撃では、攻撃者は非先頭 IP フラグメント パケットのフラグメントのオフセットを上書きできます。ファイアウォールが IP フラグメントをリアセンブルすると、不正な IP パケットが生じる場合があり、メモリのオーバーフローやシステムのリロードが発生します。

- VFR は、重複するフラグメントが検出されると、フラグメント チェーン内のすべてのフラグメントを廃棄します。

- バッファ オーバーフロー攻撃：このタイプのサービス妨害（DoS）攻撃では、攻撃者は継続的に不完全な IP フラグメントを大量に送信します。その結果、ファイアウォールは偽のパケットをリアセンブルしようとして、時間とメモリを消費します。

バッファ オーバーフローを回避し、メモリの使用を制御するには、リアセンブルされるIPデータグラムおよびデータグラムごとのフラグメント数について最大しきい値を設定します。**ipvirtual-reassembly** コマンドまたは **ipvirtual-reassembly-out** コマンドを使用してこれらのパラメータを指定できます。

特定の時間でリアセンブルできるデータグラムの最大数に到達すると、後続のすべてのフラグメントが破棄され、グローバルな統計項目の「ReassDrop」が 1 つ大きい数になります。

データグラムあたりのフラグメントの最大数に到達すると、後続のフラグメントが破棄され、グローバルな統計項目の「ReassTooManyFrags」が 1 つ大きい数になります。

設定された最大しきい値に加えて、各 IP データグラムは管理型タイマーに関連付けられています。IP データグラムが指定された時間内にすべてのフラグメントを受信しないと、タイマーが期限切れとなり、IP データグラムおよびそのすべてのフラグメントが廃棄されます。

VFR の有効化

VFRは、フラグメントリアセンブリを必要とするあらゆる機能と連携するように設計されています（Cisco IOS XE Firewall、NAT、および IPSec など）。デフォルトで、NAT、Cisco IOS XE Firewall、暗号ベース IPSec、NAT64、および onePK は、VFR を内的に有効化および無効化します。つまり、これらの機能がインターフェイスで有効になっていると、そのインターフェイスで VFR が自動的に有効になります。

複数の機能が自動的にインターフェイスのVFRを有効にしようとすると、VFRを有効にした機能の数を追跡するために、VFR は参照回数を維持します。参照回数が減少してゼロになると、VFR は自動的に無効になります。

NAT がインターフェイス（GigabitEthernet 0/0/0 など）で有効になっている場合、VFR（入力/出力）はこのインターフェイスで有効化されます。

```
Device(config-if)# do show ip virtual-reassembly features
GigabitEthernet0/0/0:
  Virtual Fragment Reassembly (VFR) Current Status is ENABLED [in]
  Features to use if VFR is Enabled:NAT
GigabitEthernet0/0/0:
  Virtual Fragment Reassembly (VFR) Current Status is ENABLED [out]
  Features to use if VFR is Enabled:NAT
```

Cisco IOS XE Firewall がインターフェイス（GigabitEthernet 0/0/0 など）で有効になっている場合、VFR（出力）はこのインターフェイスで有効化されます。

```
Device(config-if)# do show ip virtual-reassembly features
GigabitEthernet0/0/0:
  Virtual Fragment Reassembly (VFR) Current Status is ENABLED [out]
  Features to use if VFR is Enabled:FW
```

IPSec がインターフェイス（GigabitEthernet 0/0/0 など）で有効になっている場合、VFR（出力）はこのインターフェイスで有効化されます。

```
Device(config-if)# do show ip virtual-reassembly features
GigabitEthernet0/0/0:
```

```
Virtual Fragment Reassembly (VFR) Current Status is ENABLED [out]
Features to use if VFR is Enabled:IPSec
```

（注） VFR が NAT や Cisco IOS XE Firewall などの機能によって有効化されている場合、**ip virtual-reassembly [-out]** コマンドは **show running-config** コマンドの出力に表示されません。

VFR は、[**no**] **ip virtual-reassembly [-out]** コマンドを使用して、手動で有効化または無効化できます。

NAT や Cisco IOS XE Firewall などの機能によって有効化されているかどうかにかかわらず、VFR が有効化されている場合、**ip virtual-reassembly [-out]** コマンドは **show running-config** コマンドの出力に表示されます。

VFR の無効化

次の方法を使用して、仮想フラグメンテーション リアセンブル（VFR）を無効化できます。

- VFR を手動で有効化した場合は、**noip virtual-reassembly [-out]** コマンドを使用して手動で無効化できます。このコマンドは、**show running-config** コマンドの出力に表示されません。
- VFR が機能（NAT または Cisco IOS Firewall など）によって有効になっている場合、手動で無効にするか、またはその機能を無効にすることで無効化できます。手動で無効になっている場合は、**noip virtual-reassembly [-out]** コマンドが **show running-config** コマンドの出力に表示されます。
- VFR を手動で有効化した場合および機能によって有効化した場合は、どちらも **noip virtual-reassembly [-out]** コマンドを使用して手動で無効化できます。このコマンドは、**show running-config** コマンドの出力に表示されます。

（注） VFR が有効になっていない場合は、**noip virtual-reassembly [-out]** コマンドは、**show running-config** コマンドの出力に表示されません。

VFR を無効化した後に有効化する場合、つまり、**noip virtual-reassembly [-out]** コマンドが **show running-config** コマンドの出力に表示されるときは、**ip virtual-reassembly [-out]** コマンドを使用するか、または関連する機能を無効化してからその機能を有効化しなおすことで、手動で VFR を有効化します。

暗号マップ ベースの IPSec 導入シナリオ（GETVPN など）では、VFR は IPSec を使用して設定されているデバイスでデフォルトで有効になっています。同じパケットのフラグメントは、パケットのロード バランス アルゴリズム（パケットごとのロード バランスまたは何らかの Nexus デバイスの宛先ごと）のために上位のデバイスによって異なるデバイス（IPSec が有効になっているもの）に送信されることがあります。VFR は、同じ IP パケットのフラグメントをすべて受信しなかった場合、フラグメントを破棄する場合があります。この問題の推奨される回避策は、同じパケットのすべてのフラグメントが必ず同じパスを通過するようにロード バランス アルゴリズムを変更することです。レイヤ 4 情報（ポート）が IPSec ポリシーのフィルタ条件でない場合、別の回避策は、IPSec が設定されているインターフェイスで **no ip virtual-reassembly [-out]** を使用して VFR を無効化することです。

アウトバウンド インターフェイスの VFR

Cisco IOS XE Release 3.2S 以降のリリースでは、**ipvirtual-reassembly-out** コマンドを使用して、アウトバウンドのインターフェイスのトラフィックに対して手動で VFR を有効化または無効化できます。

仮想フラグメンテーション リアセンブルの設定方法

VFR の設定

この作業を行ってインターフェイスで VFR を有効化し、最大しきい値を指定してバッファ オーバーフローに対処し、メモリ使用率を制御し、VFR 設定を確認できるようにします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***interface-typeinterface-number*
4. **ip virtual-reassembly** [**max-reassemblies***number*] [**max-fragments***number*] [**timeout***seconds*] [**drop-fragments**]
5. **end**
6. **show ip virtual-reassembly** [*interface type*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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	**configureterminal** 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	**interface***interface-typeinterface-number* 例： `Device(config)# interface GigabitEthernet0/0/1`	インターフェイス タイプを設定し、インターフェイス 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	**ip virtual-reassembly** [**max-reassemblies***number*] [**max-fragments***number*] [**timeout***seconds*] [**drop-fragments**] 例： `Device(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5`	インタフェースで VFR を有効化し、最大しきい値を指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show ip virtual-reassembly** [*interface type*] 例： `Device# show ip virtual-reassembly GigabitEthernet0/0/1`	VFR の設定および統計情報を表示します。 • インターフェイスが指定されていない場合、すべての設定済みインターフェイスで VFR 情報が表示されます。

アウトバウンド インターフェイス トラフィックに対する VFR の手動有効化

アウトバウンド インターフェイス トラフィックに対して VFR を手動で有効化するには、次の作業を行います。アウトバウンド インターフェイス トラフィックに対して VFR が無効になっている場合などは、次の手順を使用して VFR を再有効化することができます。これには、**noipvirtual-reassembly** コマンドを使用します。

（注） VFR がインバウンドとアウトバウンド両方のインターフェイス トラフィックで有効化されている場合は、**noipvirtual-reassembly [-out]** コマンドを使用してアウトバウンドインターフェイス トラフィックのみで無効化することができます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ip virtual-reassembly** [**max-reassemblies***number*] [**max-fragments***number*] [**timeout***seconds*] [**drop-fragments**]
5. **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	イネーブル化 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet0/0/1`	インターフェイス タイプを設定し、インターフェイス 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	**ip virtual-reassembly** [**max-reassemblies***number*] [**max-fragments***number*] [**timeout***seconds*] [**drop-fragments**] 例： `Device(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5`	インタフェースで VFR を有効化し、最大しきい値を指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。

トラブルシューティングのヒント

VFR サブシステムに関連するデバッグ メッセージを表示するには、**debug ip virtual-reassembly** を使用します。

仮想フラグメンテーション リアセンブルの設定例

例：アウトバウンド インターフェイス トラフィックに対する VFR の設定

次の例は GigabitEthernet0/0/1、GigabitEthernet0/0/0.773、および Serial 3/0 インターフェイスの発信トラフィックで VFR を手動で有効化する方法を示しています。

```
interface Loopback 0
 ip address 10.0.1.1 255.255.255.255
 !
interface GigabitEthernet0/0/1
 description LAN1
 ip address 10.4.0.2 255.255.255.0
 ip virtual-reassembly-out
 !
interface GigabitEthernet0/0/0.773
 encapsulation dot1Q 773
 description LAN2
 ip address 10.15.0.2 255.255.255.0
 ip virtual-reassembly-out
 !
interface Serial 3/0
 description Internet
 ip unnumbered Loopback0
 encapsulation ppp
 ip virtual-reassembly-out
 serial restart-delay 0
```

仮想フラグメンテーションリアセンブルのその他の参考資料

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』
ダイナミック IDS	『Cisco IOS Intrusion Prevention System』
CBAC	「Configuring Context-Based Access Control」の章

RFC

RFC	Title
RFC 791	*Internet Protocol*（インターネット プロトコル）
RFC 1858	『*Security Considerations for IP Fragment Filtering*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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

仮想フラグメンテーション リアセンブルの機能情報

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*：仮想フラグメンテーション リアセンブルの機能情報

機能名	リリース	機能情報
仮想フラグメンテーション リアセンブル	Cisco IOS XE Release 3.2S	VFR を使用すると、Cisco IOS Firewall で適切なダイナミック ACL を作成してさまざまなフラグメンテーション攻撃からネットワークを防御できます。 Cisco IOS Release XE 3.2S では、アウトバウンドまたはインバウンド インターフェイス トラフィック用に手動で VFR を設定する機能が追加されました。 次のコマンドが導入または変更されました。**ipvirtual-reassembly-out**、**showipvirtual-reassembly**。

第 3 章

IPv6 仮想フラグメンテーション リアセンブル

- 機能情報の確認，15 ページ
- IPv6 仮想フラグメンテーション リアセンブルに関する情報，16 ページ
- IPv6 仮想フラグメンテーション リアセンブルの導入方法，16 ページ
- IPv6 仮想フラグメンテーション リアセンブルの設定例，18 ページ
- その他の参考資料，18 ページ
- IPv6 仮想フラグメンテーション リアセンブルの機能情報，19 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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、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。

IPv6 仮想フラグメンテーション リアセンブルに関する情報

IPv6 仮想フラグメンテーション リアセンブル

フラグメンテーションは、異なるタイプのネットワーク メディアを介して送信するために、IP データグラムをより小さいパケットに分割するプロセスです。フラグメント化された IPv6 パケットの最初以外のフラグメントを使用して IPsec および NAT64 を検査なし（L4 ヘッダーがないため）でパス スルーしますが、これは通常、最初のフラグメントでのみ利用できます。IPv6 仮想フラグメンテーション リアセンブル（VFR）機能は、フラグメントを収集する機能を提供し、L4 の情報を IPsec および NAT64 の機能に向けたすべてのフラグメントに提供します。

IPv6 仮想フラグメンテーション リアセンブルの導入方法

IPv6 仮想フラグメンテーション リアセンブルの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. ipv6 virtual-reassembly [**in** | **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments**
5. **exit**
6. show ipv6 virtual-reassembly interface *interface-type*
7. show ipv6 virtual-reassembly features interface *interface-type*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# 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	**interface***typenumber* 例： `Router(config)# interface gigabitethernet 3/1/1`	インターフェイスのタイプと番号を指定し、ルータをインターフェイスコンフィギュレーションモードにします。
ステップ 4	ipv6 virtual-reassembly [**in** | **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments** 例： `Router(config-if)# ipv6 virtual-reassembly max-reassemblies 32 max-fragments 4 timeout 7`	インターフェイスに対してVFRをイネーブルにします。
ステップ 5	**exit** 例： `Router(config-if)# exit`	インターフェイスコンフィギュレーションモードを終了し、ルータをグローバル コンフィギュレーション モードに設定します。 • このコマンドを 2 回入力して、特権 EXEC モードにします。
ステップ 6	show ipv6 virtual-reassembly interface *interface-type* 例： `Router# show ipv6 virtual-reassembly interface e1/1/1`	特定のインターフェイスについてVRF設定および統計情報を表示します。
ステップ 7	show ipv6 virtual-reassembly features interface *interface-type* 例： `Router# show ipv6 virtual-reassembly features`	すべてのインターフェイスまたは指定したインターフェイスの VFR 情報を表示します。

IPv6 仮想フラグメンテーション リアセンブルの設定例

例：IPv6 仮想フラグメンテーション リアセンブルの設定

```
Router# show ipv6 virtual-reassembly interface gigabitethernet1/1/1
GigabitEthernet1/1/1:
IPv6 Virtual Fragment Reassembly (VFR) is ENABLED(in)
Concurrent reassemblies (max-reassemblies): 64
Fragments per reassembly (max-fragments): 16
Reassembly timeout (timeout): 3 seconds
Drop fragments: OFF
Current reassembly count: 0
Current fragment count: 0
Total reassembly count: 6950
Total reassembly timeout count: 9
GigabitEthernet1/1/1:
IPv6 Virtual Fragment Reassembly (VFR) is ENABLED(out)
Concurrent reassemblies (max-reassemblies): 64
Fragments per reassembly (max-fragments): 16
Reassembly timeout (timeout): 3 seconds
Drop fragments: OFF
Current reassembly count: 0
Current fragment count: 0
Total reassembly count: 0
Total reassembly timeout count: 0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Master Commands List, All Releases』
IPv6 コマンド	IPv6 コマンド リファレンス
Cisco IOS IPv6 機能	『IPv6 Feature Mapping』

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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

IPv6 仮想フラグメンテーション リアセンブルの機能情報

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*：*IPv6* 仮想フラグメンテーション リアセンブルの機能情報

機能名	リリース	機能情報
IPv6 仮想フラグメンテーション リアセンブル	Cisco IOS XE Release 3.4S	IPv6 VFR 機能は、フラグメントを収集する機能を提供し、L4 の情報を IPsec および NAT64 の機能に向けたすべてのフラグメントに提供します。

第 4 章

GRE フラグメントおよびリアセンブル パフォーマンス チューニング

GRE フラグメントおよびリアセンブル パフォーマンス チューニング機能を使用すると、リアセンブル リソースをカスタマイズできます。リアセンブル リソースは、フラグメント関連の攻撃を防ぐために各インターフェイスに均等に割り当てられます。ただし、一部の Generic Routing Encapsulation（GRE）トンネルの導入では、フラグメントは特定のインターフェイスにリアセンブルされます。また、この機能を使用すると、リアセンブル タイマーを調整して不完全なフラグメント セッションを迅速に解放し、優先順位の高いパケットのためにリアセンブル リソースを予約することができます。

- 機能情報の確認，21 ページ
- GRE フラグメントおよびリアセンブルの制約事項，22 ページ
- GRE フラグメントおよびリアセンブルの情報，22 ページ
- GRE フラグメントおよびリアセンブルの使用方法，23 ページ
- GRE フラグメントおよびリアセンブルの設定例，25 ページ
- GRE フラグメントおよびリアセンブルのその他の参考資料，25 ページ
- GRE フラグメントおよびリアセンブルの機能情報，26 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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、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。

GRE フラグメントおよびリアセンブルの制約事項

- インターフェイスで IPv4 または IPv6 プロトコルが有効になっている必要があります。
- この機能は、手動で作成されたトンネルインターフェイスまたは物理インターフェイス（仮想テンプレートは正式にはサポートされていません）をサポートしています。

GRE フラグメントおよびリアセンブルの情報

フラグメンテーションとリアセンブル

シスコのソフトウェアでは、インターフェイスに同時にフラグメントが到達したとき、他のインターフェイスにはフラグメントをリアセンブルするためのリソースがあっても、インターフェイスのリアセンブル リソースが利用可能でないことが原因でパケットが破棄されることがあります。場合によっては、Generic Routing Encapsulation（GRE）トンネルの導入など、一部のインターフェイスに追加のリソースが必要になります。また、リソースは、フラグメントがリアセンブルされたときにのみ解放されます。したがって、すべてのフラグメントを受信していない場合、リアセンブル リソースは解放されません。

GRE フラグメントおよびリアセンブル パフォーマンス チューニング機能は、優先度の高いフラグメントをリアセンブルすることで、優先度が低いフラグメントがリアセンブル リソースを占有してもフラグメントが破棄されないようにしてリアセンブルのパフォーマンスを向上します。

Out-of-Order パケットの処理

場合によって、大きいパケットを受信してから小さいパケットを受信しても、小さいパケットが転送された後で転送される場合があります。大きいパケットに小さいパケット（出力インターフェイス MTU よりも小さいパケット サイズ）が続くシナリオを考えてみましょう。大きいパケットは、フラグメント化およびリアセンブルされる場合があります。大きいパケットのフラグメント化とリアセンブルには追加のプロセッサ サイクルが必要です。Cisco IOS XE ソフトウェアで動作するデバイスは、マルチスレッド プロセスに従います。つまり、小さいパケットにはより短い時間の処理しか必要ではないため、フラグメント化された大きなパケットよりも先に転送される可能性があります。このプロセスは受信者側のパケット シーケンスの変更につながります（大きいパケットは小さいパケットよりも先に受信されますが、小さいパケットの後で転送される可能性があります。

GRE フラグメントおよびリアセンブルの使用方法

GRE フラグメントおよびリアセンブル（GFR）の設定

この作業を行って、次の処理を実行します。

- インターフェイスで、Generic Routing Encapsulation（GRE）のフラグメントおよびリアセンブル（GFR）を有効化します。
- バッファ オーバーフローに対処し、メモリ使用率を制御するための最大しきい値を指定します。
- GFR 設定を確認します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber*
4. 次のいずれか 1 つを入力します。
   - **ip reassembly** [**max-reassemblies***number*] [**timeout***milliseconds*] [**percentage***percent* {**dscp***dscp-value* | **precedence***precedence-value*}]
   - **ipv6 reassembly** [**max-reassemblies***number*] [**timeout***milliseconds*] [**percentage***percent* {**dscp***dscp-value* | **precedence***precedence-value*}]
5. **end**
6. 次のいずれか 1 つを入力します。
   - **show ip reassemblyinterface***typenumber*
   - **show ipv6 reassemblyinterface***typenumber*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 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）。

	コマンドまたはアクション	目的
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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスタイプを設定し、インターフェイス 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	次のいずれか 1 つを入力します。
	• **ip reassembly** [**max-reassemblies***number*] [**timeout***milliseconds*] [**percentage***percent* {**dscp***dscp-value* | **precedence***precedence-value*}]
	• **ipv6 reassembly** [**max-reassemblies***number*] [**timeout***milliseconds*] [**percentage***percent* {**dscp***dscp-value* | **precedence***precedence-value*}]
	
	例：
	`Device(config-if)# ip reassembly max-reassemblies 1024 timeout 1000 percentage 50 precedence critical routine`
	
	例：
	`Device(config-if)# ipv6 reassembly max-reassemblies 1024 timeout 1000 percentage 50 precedence critical routine`
		必要に応じて IPv4 または IPv6 インターフェイスで GFR を有効化します。

ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 6	次のいずれか 1 つを入力します。
	• **show ip reassemblyinterface***typenumber*
	• **show ipv6 reassemblyinterface***typenumber*
	
	例：
	`Device# show ip reassembly GigabitEthernet 0/0/0`
	
	例：
	`Device# show ipv6 reassembly GigabitEthernet 0/0/0`
		インターフェイスについて設定されている GFR の統計情報を表示します。

GRE フラグメントおよびリアセンブルの設定例

例：GFR の設定

次の例は、ギガビット イーサネット インターフェイスで GFR を設定し、最大のリアセンブリおよびタイムアウト設定を指定する方法を示しています。

```
interface GigabitEthernet 0/0/0
 ip address 10.10.10.1 255.255.255.0
 ipv6 address 2001:DB8:1::1
 ip reassembly max-reassemblies 1024 timeout 1 percentage 50 dscp ef
 ipv6 reassembly max-reassemblies 1024 timeout 1 percentage 50 dscp ef
 ip virtual-reassembly max-reassemblies 1024 timeout 1 percentage 10 dscp af41
 ipv6 reassembly out max-reassemblies 1024 timeout 1 percentage 50 precedence cs1
```

GRE フラグメントおよびリアセンブルのその他の参考資料

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』
セキュリティ 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』
仮想フラグメンテーションおよびリアセンブル	『*Virtual Fragmentation and Reassembly*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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

GRE フラグメントおよびリアセンブルの機能情報

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 *3*：*GRE* フラグメントおよびリアセンブルの機能情報

機能名	リリース	機能情報
GRE フラグメントおよびリアセンブル パフォーマンス チューニング	Cisco IOS XE Release 3.8S	GRE フラグメントおよびリアセンブル パフォーマンス チューニング機能を使用すると、リアセンブル リソースをカスタマイズできます。リアセンブル リソースは、フラグメント関連の攻撃を防ぐために各インターフェイスに均等に割り当てられます。ただし、一部の Generic Routing Encapsulation（GRE）トンネルの導入では、フラグメントは特定のインターフェイスにリアセンブルされます。また、この機能を使用すると、リアセンブル タイマーを調整して不完全なフラグメントセッションを迅速に解放し、優先順位の高いパケットのためにリアセンブル リソースを予約することができます。 次のコマンドが導入または変更されました。**ip reassembly**、**show ip reassembly**。