



## ユニキャスト リバース パス転送の設定

- [ユニキャスト リバース パス転送の設定 \(1 ページ\)](#)
- [IPv6 ユニキャスト リバース パス転送の設定 \(1 ページ\)](#)

## ユニキャスト リバース パス転送の設定

ユニキャスト リバース パス転送 (ユニキャスト RPF) 機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違っまたは偽造 (スプーフィングされた) 送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network (TFN) など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃者が阻止できるようにします。パブリックアクセスを提供するインターネットサービスプロバイダ (ISP) の場合、uRPF が IP ルーティングテーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、そのような攻撃をそらします。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。



- (注)
- ユニキャスト RPF は、Network Essentials でサポートされています。
  - スイッチが複数のスイッチタイプが混在する混合ハードウェアスタック内にある場合は、ユニキャスト RPF を設定しないでください。

IP uRPF 設定の詳細については、『Cisco IOS Security Configuration Guide』の「Other Security Features」の章を参照してください。

## IPv6 ユニキャスト リバース パス転送の設定

ユニキャスト リバース パス転送 (ユニキャスト RPF) 機能は、検証できない送信元 IP アドレスの IP パケットを廃棄することで、間違っまたは偽造 (スプーフィングされた) 送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network (TFN) など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃

者が阻止できるようにします。パブリックアクセスを提供するインターネットサービスプロバイダ（ISP）の場合、uRPFがIPルーティングテーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、そのような攻撃をそらします。この処理により、ISPのネットワーク、その顧客、および残りのインターネットが保護されます。



- 
- (注)
- スイッチが複数のスイッチタイプが混在する混合ハードウェアスタック内にある場合は、ユニキャストRPFを設定しないでください。
- 

IP ユニキャスト RPF 設定の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「*Other Security Features*」の章を参照してください。

## 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。