RFC3360 不適切なTCP Resetは有害である

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	「一般的ルールとして、Reset（RST）は、その外観が現在のコネクションのために意図されたものではないセグメントが到着するときには常に送られなければならない。Reset は、これが該当するか不明な場合、送られてはならない。」				
	「あなたが受信するものついては寛容であれ。送信するものについては、保守的であれ。」				
	「この『堅牢性原則』は、『ひとつの変なふるまいをするホストが多くの他のホストに対するインターネットサービスを不能にする可能性があるインターネット層において特に重要であること』」				
	RFC 1122 における「堅牢性原則」の検討は、「変更の採用可能性については、インターネットホストのすべてのレベルのソフトウェアにおいて設計されなければならない」				
	「TCP ヘッダー中の Reserved フィールドは、将来の利用のために確保されており、ゼロでなければならない」				
	「アプリケーションは、ファイアウォールが在る場合でも正しく動作し続けなければならない。これは、下記の透過性ルールに翻訳されます。: ファイアウォールや、あらゆる関連するトンネリング設備（あるいはアクセス交渉設備）の導入は、そのファイアウォールが無かった場合、動作する正規かつ標準準拠の用法の意図しない失敗をもたらしては**ならない（MUST NOT）**。」				
	「この要求に対する必要不可欠な類推は、『このような失敗が実際に起きたとき、その問題に対応することは、ファイアウォールや関連するソフトウェアの責任となる』ということである。: 既存の標準プロトコルの実装の変更も、そのプロトコル自体の変更も、必須であっては**ならない（MUST NOT）**。」				
	「TCP Reset が混雑制御メカニズムとしては使われないこと」				
	「単に、SYN パケットを棄却することが、混雑に対する最も効果的な応答であること」				
	「入り方向のセグメントがセキュリティのレベル、もしくはコンパートメントをもつ場合、もしくは、必ずしもレベルやコンパートメントに合致しない「優先権（precedence）」をもち、優先権がそのコネクションを要求した場合、Reset が送られ、コネクションは、CLOSED 状態になる。」				
	「Reset は、外観上、現在のコネクションとして意図されていないセグメントが到達するときにのみ送られる必要がある」				
	「TCP は、すべての受信したセグメントの優先権を無視しなければならず、その優先権（precedence）フィールドにおける変更に応じて Reset を送ってはならない」				
	「この論点について、非ゼロの TCP Reserved フィールドをもつセグメントに応じた Reset の送信は、決して許されないこと」				
	TCP は、あらゆるセグメント中の TCP オプションを受信することができなければ**ならない（MUST）**。				
	TCP は、オプションとして、長さ（length）フィールドをもつことと想定して、実装していない、いかなる TCP オプションもエラーとすることなく、無視しなければ**ならない（MUST）**。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	(将来規定されるすべての TCP オプションは、長さ(length)フィールドをもつ。)TCP は、クラッシュすることなく、不正なオプション長(例: ゼロ)を扱うことに備えなければ**ならない(MUST)**。				
	示唆される手順は、そのコネクションをリセットし、その理由を記録することである				
	「この論点は、非ゼロの TCP Reserved フィールドをもつセグメントに応じて Reset の送信を決して許容しないこと」				
	「トランスポートプロトコルは、ネットワーク中のファイアウォール、ノーマライザー(Normalizer)および他の中間ボックスの未知かつ任意に見える活動から自らを防護する必要があること」				
	「トランスポートプロトコルは、そのコネクションの存続期間において、パス上の中間ボックスからの干渉についてチェックするために、さらなるチェックも追加しなければならないこと」				
	『IPsec が使われているとき、そのトランスポートヘッダーは、トンネルモードとトランスポートモード [ESP, AH] の両方において防護されること』				
	トランスポートプロトコルは、また、中間ボックスが、この形態の ICMP の「宛先到達不能(Destination Unreachable)」メッセージを「そのパケットは、許可されていない機能 [RFC1812] を使っていること」を示すために使い始めた場合、ICMP コード:「通信は運用管理的に禁止されている(Communication Administratively Prohibited)」に対して何らかのかたちで応答しなければなりません。				
	「ファイアウォールは、『通信は運用管理的に禁止されている(Communication Administratively Prohibited)[B01] 』コードと共に ICMP『宛先到達不能(Destination Unreachable)』メッセージを送ること」				
	「本書は、完全なトランスポートプロトコルをブロックする中間ボックスを考慮しないこと」				
	「本書は、firewalled-off TCP ポート宛の TCP SYN パケットに応じて Reset を送信するファイアウォールに対応していないこと」				
	「ひとたび特定の機能をブロックするために、あるメカニズムがファイアウォールにインストールされると、ネットワーク運用管理者が そのブロックを『アンインストール』するために相当な労力を要する可能性があること」				
	「ファイアウォールにおける拡張可能な設定は、全体的に、より少ない痛みで将来のインシデントから復旧させる可能性があること」				
	「ファイアウォールが TCP パケットを棄却しなければならないのにもかかわらず、TCP Reset を送ることは、不適切である」				
	「ファイアウォールには、混雑制御メカニズムとしての TCP SYN パケットに応じて Rreset を送るものがあること」				
	「Reset を送信することなく、単にパケットを棄却することは、 for the TCP コネクション in resending the SYN パケット without the 禁止された機能 遅延をもたらすこと」				

RFC3360　不適切なTCP Resetは有害である

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	「あるプロトコルに追加された新しい機能の利用をブロックできることがファイアウォールについて要求される場合、これは、ファイアウォールコミュニティとプロトコル設計者の協働によって、初期設計段階において、もっともうまく対応される」				
	「単にそのパケットが TCP Reserved フィールド中のフラグを使っているからといって、TCP SYN パケットに Reset で応答することは、ファイアウォール、ロードバランサーもしくは Web サーバーについての現在の標準に準拠していない」				
	「エンドノードに、これらの活動についての理由を通知するための明確な手法を伴わない、この種のふるまいは、TCP の開発に対して、顕著な障害をもたらす可能性があること」				