RFC3704　マルチホームされたネットワークのためのイングレスフィルタリング

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	
	「イングレスフィルタリングは、ISP とエンドユーザの間の『最後の（last-mile）』インターフェイスにのみ適用されるわけではないこと」				
	「同一の合意は、ISP のアップストリームと、ピアとなるリンクにも適用されること」				
	イングレスフィルタリングを配備することによって、人は、単にインターネット全体を助けるのみならず、あなた自身のインフラストラクチャに対するいくつかの脅威のクラスからも防護します。				
	「混合されたアップストリーム／ダウンストリームや、ピアとなるリンクをもつ異なるリンクは、異なる属性をもつ可能性があること（例： 契約、信用、イングレスフィルタリングメカニズムの実行可能性等に関連する。）」に注意することが重要です。				
	Failing that,唯一の現実の選択肢は、イングレスフィルタリングを行わずに,use a マニュアルのアクセスリスト（possibly in addition to 何らかの他のメカニズムs）か、あるいは、何らかの形態の「Loose RPF」チェックを使うことです。				
	「その ISP が実際に、そのアドレスを、ルーティングの際に運んでいること」				
	「その prefix が主要な transit ISP 宛にアップストリームに運ばれていること」				
	「そのエッジネットワークは、to qualify for a 分離されたアドレス割り当てと AS（Autonomous System）番号 from its RIR 大きさになり、技術的に準拠するものとなること」				
	「ISP のイングレスフィルタが完全であること」				
	プロバイダーに基づくアドレス割り当てを使っていおり、その ISP が（実装すべき）イングレスフィルタを実装している、より小さなエッジネットワーク用の 3 番目のオプションは、一定のプロバイダーのアドレス空間から発信されたトラフィックを、そのプロバイダー宛てに経路制御することです。				
	「あるネットワークインターフェイスに到着するトラフィックが、正規に、そのインターフェイスを通じて到達可能なネットワーク上にあるコンピュータから来ること」を確保する				
	。「最初のホップのルーターは、『近隣のエンドシステムから経路制御されているトラフィックは、正しく宛てられていたこと』を確認すること」				
	「そのようなシステムが示された prefix 内にある可能性があること」				
	結果として、すべての運用管理的ドメインは、その境界において、十分なレベルのイングレスフィルタリングを確保することを試す必要があります。				
	イングレスアクセスリストは、典型的には、手作業による保守管理を要求しますが、正しく行われたとき、最も防弾性を発揮します。典型的には、イングレスアクセスリストは、are best fit between the エッジ and the ISP when the 設定 is not too dynamic,「Strict RPF」がオプションでない場合、between ISPs if the number of used prefixes is low, or as an additional layer of 防護。				

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	
	「Strict RPF」チェックは、イングレスフィルタリングを実装するのに、非常に容易で確実な方法です。これは、典型的には、エッジネットワークと、その ISP の間に適します。多くの場合において、シンプルな「Strict RPF」は、can be augmented by operational procedures in 非対称のトラフィックパターンの場合,or 「Feasible Path RPF」テクニック to also account for 他の代替パス。				
	「Feasible Path RPF」チェックは、「Strict RPF」の拡張です。これは、「Strict RPF」があるすべてのシナリオに適しますが、特に、マルチホームされた、あるいは、非対称なシナリオに適します。しかし、「Feasible RPF は、整合性ある発信元と、ルーティング情報の公告が機能することを想定すること」を覚えておかなければなりません。この示唆は、特に、prefix の公告が第三者を通過する場合、理解されなければなりません 。				
	「Loose RPF」は、主に、Martian アドレスのような経路制御されない prefixes をフィルタします。これは、経路制御されない発信元アドレスをもつ DoS 攻撃の規模を低減するために、アップストリームインターフェイスに適用できます。ダウンストリームインターフェイスにおいて、これは、「他方のネットワー クは、少なくとも何らかのイングレスフィルタリングを行った」という契約の検証としてのみに使えます。				
	イングレスフィルタリングは、常に、ISP とシングルホームされたエッジネットワークの間において行われる必要があります。				
	「Feasible RPF」をもつイングレスフィルタリング、もしくは、同様な「Strict RPF」テクニックは、ほとんど常に、ISP とマルチホームされたエッジネットワークの間にも適用できます。				
	ISP とエッジの両方のネットワークは、「彼ら自身のアドレスが、彼らのネットワークの外部から来るパケットの発信元アドレス中に使われていないこと」を検証する必要があります。				
	イングレスフィルタリングの形態によっては、ISP 間において、特に、prefix の数が少ない場合、合理的なものもあります。				
	そのメカニズムを、より詳細に規定する。: 実装間には、相違があります。(例: あるアドレス宛のトラフィックは、常に「Strict RPF フィルタ」を通過するか否かについて。)そのメカニズムを正式に規定することによって、その実装は、調和されることができます。				
	RIB(Routing Information Base)に基づく RPF メカニズムについて調査し、規定する。(例: 「Feasible Path RPF」について、より詳細に。)特に、「どのような想定のもとで、これらのメカニズムは、意図したように機能するか？」および「どのような想定のもとで、機能しないか？」を考慮する。				
	分類論とその詳細もしくはメカニズム(上記)の基礎が築かれた後、イングレスフィルタリングのメカニズムについて、このメモよりも一般的な注意事項を書くこと。				

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	
	より複雑な場合を考えるとすると、ネットワークが異なる属性（例：ピアやアップストリーム）の接続性をもつ場合、「ピアのアドレスで経路制御されたトラフィックは、そのアップストリームから受容されてはいけないこと」を確認することを望みます。				