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	
	起点となったネットワークの中にいる攻撃者が、境界におけるフィルタリングルールに合わない偽ったソースアドレスを使用して、この種の攻撃を仕掛けることを防ぎます。				
	攻撃者が、正規に通知されているプリフィックス（ IP アドレス）の範囲内にない、偽った 発信元アドレスを使用することをはばむために、すべてのインターネット接続プロバイダーには、この文書に記述されたフィルタリングを実装することが強く薦められます。				
	いいかえれば、ISP が、複数のダウンストリームネットワークの経路情報を持っている場合、これらの経路情報以外から来たトラフィックを防ぐために、厳格なトラフィック フィルタリングが使用される必要があります。				
	この種のフィルタリングを実装することの利点には、他に、「発信者の本当の発信元を容易に追跡することができるようになること」があります。それは、攻撃者は、正規の、実在する到達可能な発信元アドレスを使用する必要があるからです。				
	この脅威に対応して、大部分のオペレーティングシステムベンダーは、標的とされたサーバーが、非常に高い頻度でコネクションを試みてくる攻撃を保留できるように自社のソフトウェアを改良しました。これは歓迎すべきことであり、この問題に対する対策として必要なことです。				
	攻撃者のネットワークとの接続を提供する、"router 2"の境界（ input ）リンク上のインプット トラフィック フィルタは、204.69.207.0/24 プリ フィックスの範囲内の発信元アドレスからのものだけを許すように トラフィックを制限し、攻撃者が、このプリフィックスの範囲外の「不正な」発信元アドレスを使用することを防ぎます。				
	将来のプラットフォーム実装について、追加的な機能も考慮される必要があります。下記のものが注目に値します。: －リモートアクセスサーバーへの自動的なフィルタリングの実装があげられます。大部分の場合、アクセスサーバーにダイアルするユーザは、1 台の PC を使った個人ユーザーです。その PC から来るパケットについて、唯一の正しい発信元ソース IP アドレスは、（静的であれ動的であれ）その ISP によって割り当てられたものです。リモートアクセスサーバーは、ユーザが、パケット上の発信元アドレスを偽っていないことを確かめるように、すべてのパケットを境界でチェックすることができます。明らかなことですが、顧客が正規にそのネット、もしくはサブネットに接続している場合には、その用意も必要です。しかし、これは、オプションの選択肢として実装することができます。我々は、既に、この機能を実装し始めているベンダーや ISP があるという報告を受けています。				
	フィルタリングには、その性質上、ある種の「特別な」サービスを行えなくする可能性があります。しかし、この種の特別なサービスを提供している ISP にとっては、これらのサービスを実装することの代替手法を検討することが、境界でのトラフィック フィルタリングの影響を受けることを避けるためには最も有益です。				

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	
	この進行中の作業によって、モバイルノードから転送されたデータがインターネットに転送される前に、ホームエージェントをトンネルさせられる手法が提供さ れることになっています。リバーストンネリングのスキームには、マルチキャストトラフィックのより良い扱い方など、他の利益もあります。Mobile IP システムを実装している 方は、このリバース トンネリングの手法を実装することが強く推奨 されています。				
	インターネットに接続されたネットワーク外辺における境界におけるトラフィックフィルタリングは、発信元アドレススプーフィングを行うサービス妨害攻撃の有効性を減らします。				
	企業のネットワーク管理者は、彼らの企業ネットワークがそのような問題の起点とならないようにフィルタリングを実装する必要があります。				