RFC3552　RFCの「セキュリティについての考慮事項」についての文章を書くためのガイドライン

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	
	アプリケーションプロトコル設計者は、「すべての攻撃者はパス外にいる」と想定してはなりません。可能であれば、プロトコルは、ネットワークを完全にコントロールできる攻撃者からの攻撃に耐えるように設計される必要があります				
	一定のフレームワークが使われる状況において、設計者は、フレームワークのオプションを注意深く検討し、特定の脅威モデルに対して適切なメカニズムのみを指定する必要があります。フレームワークが必要不可欠な場合、設計者は自ら設計せずに、確立したものの中のひとつを選択する必要があります				
	設計者は、「IPsec が利用可能である」と想定してはなりません。一般的なアプリケーション層プロトコルのためのセキュリティポリシーは、「IPsec が意図された配備環境で利用可能である」と信じる何らかの根拠がない限り、「IPsec が使われなければならない」と述べるだけではいけません				
	自動的鍵管理 (IKE) は、実装することが要求されていないので、プロトコル設計者は、「これが在るであろう」と想定してはいけません				
	そのプロトコルが影響を受けるサービス妨害攻撃について記述しなければなりません。この記述は、このようなサービス妨害攻撃を避ける試みが、非合理的である旨か、範囲外であるかのいずれかの理由を含まなければなりません				
	次のことを記述しなければなりません 1. どの攻撃が範囲外であるのか（その理由） 2. どの攻撃が範囲内であるのか 2.1 かつそのプロトコルが何の影響をうけるのか 2.2 かつそのプロトコルが何を護るのか				
	下記の形態の攻撃が考慮されなければなりません 盗聴、リプレイ、メッセージ挿入・削除・変更および中間者によるもの				
	潜在的なサービス妨害攻撃も識別されなければなりません				
	技術が認証（特にユーザ／ホスト認証）を含む場合、認証手段のセキュリティは、明確に仕様としなければなりません。この認証手法のセキュリティが前提としている仮定を文書化しなければなりません				
	システムがセキュリティについて下位層のセキュリティサービスに依存している場合、それらのサービスが提供することを期待されている防護は、仕様とされなければなりません				
	「セキュリティについての考慮事項」の章によって対応される脅威環境は、たとえ「なぜ、そのような考慮事項がそのプロトコルについて範囲外であるか」についての理由のみを提供する場合でも、最低限、ファイアウォールがあることを想定せずに、複数の運用管理上の境界をまたぐグローバルなインターネットにおける配備を想定しなければなりません				

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	
	複数の RCPT コマンドがあるとき、かつ、これらのメカニズムの目的の阻害を避けるために、SMTP のクライアントとサーバーは、トレースヘッダーの一部としても、情報提供もしくはプライベート拡張ヘッダーとしても、RCPT コマンドアーギュメントの全体をヘッダーにコピーしてはいけません				
	受信システムは、このような推論（(MAIL, SAML 等のコマンド中の）"reverse" か SMTP トランザクション（"envelope"）中の "forward" (RCPT) アドレス のいずれかと、ヘッダー中のアドレスの間に関係がある）すること を試みて、配信メッセージのヘッダーを置き換えるために、これらを使ってはいけません。 正規の"Apparently-to"ヘッダーは、 意図しない情報開示の源泉としてありがちなものであるとともに、この原則の侵害であり、使ってはいけません				
	個々のサイトは、セキュリティについての理由で VRFY と EXPN のいずれか、または両方を不能にすることを望む可能性があります。上記のこととは対称的に、これを許す実装は、実際には検証されていないのに検証されたアドレスをもつように見えてはなりません。サイトがセキュリティの理由によってこれらのコマンドを利用不能にする場合、SMTP サーバーは、検証が成功／失敗したか紛らわしい可能性がある コードではなく、252 レスポンスを返さなければなりません				
	EXPN の"harvest" アドレスへの利用は、メーリングリストのシステム管理者がメーリングリスト自体の不適切な利用に対する防護を導入しため、増加しました。実装者は、EXPN についてサポートし続ける必要がありますが、サイトは、注意深く二律背反を評価する必要があります				
	サイトによっては、既知もしくは識別可能な源泉についてのリレー機能の利用を 制限することを決定しており、各実装は、この種のフィルタリングを行う能力を提供する必要があります。メールが、これらの理由あるいは他のポリシーによる理由によって拒否されるとき、適切である限り、EHLO, MAIL, RCPT に応答して 550 コードが 使われる必要があります				
	SMTP サーバーの実装者もしくは SMTP のシステム管理者は、IPsec が利用可能であると信じる根拠がない限り、「IPsec が（2 マシン間における既存の協定の存在のように）利用可能である」と想定してはなりません				
	「認証なし」この認証タイプの利用は、「VRRP プロトコル交換は認証されていないこと」を意味します。この種の認証が使われるは、セキュリティリスク がほとんど無く、設定エラーの可能性が低い環境においてのみである必要があります				
	AH は、同一の LAN 上の他のノードからの攻撃から VRRP を防護する唯一のメカニズムであり、同一のネットワーク上に信用されていないノードがある場合においては必須である必要があります。いずれにせよ、AH は、実装されなければなりません				