RFC2316 IAB セキュリティアーキテクチャワークショップの報告（1998）

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	
	「セキュリティはオプションではなく、最初から設計の中に入っている必要があること」				
	我々は、「一般に エンド to エンドのセキュリティが望ましい」と結論づけました。				
	それゆえ、E メールには IPsec 層でリレーするよりも、PGP もしくは S/MIME のようなものを使用すべきです。				
	一般に、インフラストラクチャのセキュリティに依存するのは、よい考え方とはいえません。				
	理想的には、インフラストラクチャは、可用性（ availability ）を提供すべきです。				
	攻撃の最中に、インフラストラクチャ上で不合理な要求をしないようにすることは、個々のプロトコルの責任です。				
	プロトコルを攻撃から守るために、当然ながら、起こりうる攻撃の種類を知る必要があります。				
	さらに、プロトコルには、不必要にファイアウォールと相性の悪い性格をもったものがあります。そのような実践は避ける必要があります。				
	このワーキング グループによって開発されたプロトコルは、潜在的なセキュリティ侵害の起点とならないか解析され、認識された脅威は、可能であればプロトコルから除去され、そうでない場合には、文書化され保護されるものとする。				
	「脅威」とは、その定義により、動機を持った潜在的な敵が攻撃できる弱点のことをいいます。				
	CERT アドバイザリは、脅威の対象の知識について、極めて有用です。				
	要点は、どのような攻撃がありうるか（潜在的な攻撃者の「可能性（capabilities）」）を断定することと、攻撃に対する防御を定式化すること、 ないし、ある環境ではその攻撃は非現実的であることや、その環境でそのプロトコルの使用制限をすべきことについての説得力のある説明を行うことにありま す。				
	そのプロトコル、もしくは、それが仕様を決める手続きにおいて、十分にセキュリティに対応しなければ**なりません（MUST）**。				
	RFC は、「敵」にそのデータをを与えており、その友達に配布して、その意図どおりのやり方で使用することをお願いしていることを考慮しなければ**なりません （MUST）**。				
	その状況に依拠する危険の改善について、考慮されねば**なりません（MUST）**。				
	そのプロトコルが弱点を持つ脅威をリストする「忠実義務（due diligence）」を果たさなければ**なりません（MUST）。**				
	法的な用語の使用は、法的な義務を意味するものではなく、その分析に適用されることが期待される責任のレベルを意味するものです。				
	この検討は、その文書全体にわたって、もしくは「セキュリティ関連の考慮事項」の項の中で行なわれます。その文書全体にわたる場合には、「セキュリティ関連の考慮事項」の項の中で要約され、参照されなければ**なりません（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	
	下記のいずれの脅威であるかを検討しなければ**なりません（MUST）**。 －プロトコルメカニズムによって改善させるもの （例：SYN 攻撃は、SYN 攻撃の最中、ランダムにセッションをドロップ させる上手なコードによって改善させます。） －外部メカニズムを利用することによって改善させるもの （例：IPSEC ESP によって提供される TCP データの秘匿性） －見当違いのもの （「多くの場合、MIB は、それ自体はセキュリティリスクではありません。SNMP セキュリティが意図的に運用されている場合、システムの設定を変更するための MIB の使用は、ツールであって、脅威ではありません。SNMP セキュリティの脅威分析については、RFC ZZZZ をご覧ください。」） －プロトコルによって対応されるものではないもの これについては、適用可能性についての表明をすることになります。（「このプロトコルは、この攻撃の対象となる環境においては使用されるべきではありません。」）				
	IPsec [RFC 1825] 基本的なホスト間のセキュリティメカニズムです。アドレスに基づいた保護が使用されている場合には、いつでも使用するのが適切であるといえます。これには rsh や rlogin のようなプログラムも含まれます。プラットフォームがユーザに基づいた鍵をサポートしている場合、この方法が適用されることでしょう。 IPsec で使用されている技術として、HMAC [RFC 2104] は、より一般的に有用です。暗号技術的な認証が必要で、暗号化は不要な場合で、かつ、IPsec が適用でない場合、HMAC が使用されるべきです。				
	ISAKMP/Oakley [ISAKMP drafts] IPsec 用の基本的な鍵交渉（ negotiation ）プロトコルです。このように、これは IPsec が使用されている場合には採用されるべきです。これは、適切な「 domain of interpretation 」文書とともに、他のプロトコル用に、一組の鍵を交渉（ negotiate ）するのに使用されるべきです。				
	DNSsec [RFC 2065] DNS を防御することにおいてのみ重要であるのではありません。（能動的な攻撃をしかけるのに、キャッシュの改ざんが、最も容易なやり方です。）IPsec が使われている多くの場合においても要求されるものです。				
	Security/Multipart [RFC 1847] MIME でカプセル化された E メールに、セキュアにしたセクションを追加するための好ましいやり方です。				

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	
	DNS においてキーに署名する 　既に述べたように、「DNS のレコード自体が保護されなければならない」という合意が広くなされています。キーレコードは、それ自体、署名される必要があり、有効な認証（ certificates ）がなされるようにしなければならないという合意は、それほどではありませんでした。とはいえ、これはインターネット認証（ certificate ）について、将来が約束された方向性のひとつです。				
	X.509v3 　明らかに認証（certificate）インフラストラクチャのためのもうひとつの選択肢です。しかし、繰り返しになりますが、この点については、強い合意はありませんでした。				
	LS [TLS draft] 　トランスポート層でのセキュリティのための好ましい選択肢であるとする人もいました。しかし、この点については共通認識はありませんでした。TLS は、IPsec よりも OS（オペレーティングシステム）に干渉しません。さらに、このやり方の方が、詳細な保護を提供するのが容易です。				
	「有用でない」と考えられたプロトコルは、ほとんどありませんでした。				
	ひとつのセキュリティメカニズムだけが、許容できないものと考えられました。それは平文のパスワードです。つまり、暗号化されていないチャネル上で送られるパスワードに依存するプロトコルは許容できないということです。				
	「オブジェクトセキュリティ」とは、トランスポートとは独立に、個々のデータオブジェクトを保護することをいいます。セキュア DNS のようなものが既にありますが、我々が必要としているのは、より一般的なスキームです。MIME は、部分的に候補となるオブジェトフレームワークです。それは、web と E メールという 2つの最も広く採用・使用されているアプリケーションの核心部分であるからです。しかし、E メールをセキュアにすることは問題をかかえていますし、web はまだ始まったばかりです。				
	「セキュア Eメール」については、現在も、そして以前から極めて強い要求があります。セキュア E メールプロトコルを標準化しようとした 2つの試み（PEM と MOSS）は、コミュニティに受け入れられませんでした。一方、第 3 のプロトコル（ PGP ）が世界中でデファクトスタンダードになりました。第 4 のプロトコル、業界標準（S/MIME）が、人気を集めています。これら、後の 2 つとも、インターネット標準化過程に入りました。				
	「経路セキュリティ」は、最近になって極めて強く要求されるようになりました。攻撃者が巧妙になっており、様々な攻撃用ツールキットが巧妙な攻撃の件数を増加させました。この作業は、特に複雑です。それは、最高のパフォーマンスの要求と、セキュリティ向上の目標は、相容れないからです。セキュリティの向上は、ルーターの性能向上に活用できるであろう資源を奪ってしまうのです。				

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	
	セキュリティは、お菓子のクッキーの型抜きのようなものではありませんし、そうであるはずがありません。プロトコルの上に撒くとセキュアにしてくれるような妖精の魔法の粉はありません。それぞれのプロトコルは、どのような弱点があるか、どのようなリスクを導くか、どのような緩和手段をとることができるか、および残るリスクは何かを判定するために、個々に解析されなければなりません。				