RFC3365 IETF標準プロトコルについての強いセキュリティ要件

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	本書の目的は、プロトコルについてのセキュリティ要件における IETF の総意（コンセンサス）を文書化するとともに、その背景と動機について提供することにあります。						
	セキュリティは、「エンド to エンド」もしくは「ホスト to ホスト」に提供される必要があります。	○	○	○		○	○
	IETF のセキュリティについての役割は、アプリケーションがインターネット越しに利用される際に、IETF 標準プロトコルが適切なセキュリティを適用するのに必要不可欠な機能を持つようにすることです。			○		○	
	メカニズムを実装することが強制的であることは、慎重を要するビジネスアプリケーションを防護するために、適切なセキュリティを提供するはずです。			○		○	
	認証（authentication）サービス: 要求された／要求する主体（プロセス／コンピュータシステム／人）のアイデンティティを検証するセキュリティサービス。インターネットワーク層において、これは、データグラムが表現している起点から来たことを検証することを含みます。アプリケーション層において、これは、操作を行っている主体が主張されて いる本人であることを検証することを含みます。			○		○	
	データ守秘性（data confidentiality）サービス: データを、認可されていない個人／プロセスへの認可されていない開示から防護するセキュリティサービス。（インターネット標準文書は、データ守秘性（data confidentiality）を「プライバシー」の同義語として使う**べきではありません（SHOULD NOT）**。「プライバシー」は、異なる概念です。「プライバシー」は、主体（通常は人）が自らの役割で、その環境と相互作用する程度を決定する権限を意味し、主体が自らの情報について他者と共有することを望む程度を含みます。）			○		○	
	データインテグリティ（data integrity）サービス: 認可されていないデータの変更に対して防護するセキュリティサービス。意図的な変更（破壊を含む）とアクシデントによる変更（喪失を含む）の両方を含む。データへの変更が検知可能であることを確認することによる。			○		○	
	IETF は、いくつかのセキュリティプロトコルと標準をもっています。						
	プロトコル設計者がしなければならない決定的な選択のひとつは、「既存のプロトコルのひとつを利用するか、標準ツールのひとつを利用するように自らのプロトコルを工夫するか、あるいは何か全く違うことをするか」についての選択です。						
	すべてのプロトコルについて、唯一の正解は無く、設計者は、自らのプロトコルに対する脅威に本当に注目し、適切な対策を設計する必要があります。				○		○
	インターネットスタンダードトラックの RFC 中に記述されることが要求される「セキュリティについての考慮事項（Security Considerations）」という章の目的は、プロトコル設計者に、脅威を文書化し彼らのセキュリティ設計のためのロジックを説明する場所を提供することにあります。						
	圧倒的多数によるコンセンサスは、「IETF は、国家の政策に関わらず、利用可能な最善のセキュリティの利用について標準化する必要がある」ということでした。						
	「我々がセキュアなプロトコルを提供することに失敗すれば、インターネットは、国際的な通信インフラストラクチャを提供することにおいて、その有用性を低下させるであろう」						

	解決策は、我々は、プロトコルがグローバルなインターネットにおいて広く利用されるようになることが頻発する日に備えて提供するために、強いセキュリティをすべてのプロトコルに実装**しなければならない（MUST）**ということです。			○		○	
	セキュリティは、エンドユーザが状況に応じてそれを可能にすることができるように必須実装（MUST IMPLEMENT）でなければなりません。			○		○	
	「セキュリティがプロトコルの実装において考慮されなければならない」				○		○