RFC3631　インターネットについてのセキュリティメカニズム

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
	セキュリティメカニズムの選択における最も重要な要素は、「脅威のモデル」です。						
	「誰が、どの資源を、どの種のメカニズムを使って攻撃することが予期されるか？」です。						
	侵害された場合にインターネットインフラストラクチャの要所を露呈する可能性があるような資源（例えば、主要なバックボーンルーター、あるいは、高レベルの DNS サーバー）は、非常に強いメカニズムによって防護される必要があります。			○		○	
	すべてのインターネットに接続されたシステムは、最低限の防護を要求します。	○		○		○	
	「どの種類の攻撃が予期される可能性があるか？」も考慮しなければなりません。		○		○		○
	最低限、盗聴は、深刻な脅威として見なされなければなりません。			○		○	
	暗号技術は、ネットワーク自体の、いかなる特定のセキュリティ属性に依存する必要無しに、データがネットワークを転送される際に、様々な種類の防護を適用できるようにします。			○		○	
	最後に、当然ながら、防護する者には暗号技術を使う費用が発生します。		○				○
	一般に、今日、断りのない場合、あらゆるプロトコルにおいて、利用可能な最強の暗号技術を使う必要があります。			○		○	
	しかし、多くのプロトコルにおいて、我々は、「いかなる 2 つの実装でも、最終的には、両者間で共通の暗号技術的システムを交渉できること」を確保するために、「実装することの必須」を規定する必要があります。		○		○		○
	「特定のプロトコルについての実装の対象ドメインは、十分によく定義されており、セキュアであるので、そのプロトコル自体は、いかなるセキュリティメカニズムをも提供する必要がないこと」			○		○	
	「たとえ利用されるドメインが、当初、非常に限られていると想定されると確信されるときでも、『すべての』プロトコルが適切なセキュリティメカニズムを提供すること」を要求します。			○		○	
	「強制的メカニズムは、『実装』することが必須であること」			○		○	
	理想的な防護の粒度を事前評価するとき、プロトコル設計者は、典型的な利用パターン、実装する層（下記 参照）および配備可能性を考慮する必要があります。			○		○	
	「新しいパスワードがネットワーク越しにクリアテキストで送られること」を要求すること無く 、その認証データベースを最初期化する方法を提供する必要があること			○		○	
	適切である限り、HMAC は、より古いテクニック（特に、鍵付きハッシュ関数）より選好されて使われる必要があります。			○		○	
	（BGP セッションセキュリティメカニズム [RFC2385] において使われているのような）MD5 [RFC1321] に基づくシンプルな鍵付きハッシュは、特に、MD5 における弱点のヒントが与えられたら、新しいプロトコルにおいては、避けるべきものです。			○		○	
	「HMAC に基づくメカニズムは、すべてのプロトコルデータユニット（aka packet）について採用される必要があること」			○		○	
	IPsec は、IP 層に導入されるので、ネットワーキングのコードにまで入り込む可能性があります。これを実装することは、一般に、新しいハードウェアか、あるいは、新しい プロトコルスタックのいずれかを要求します。他方、これは、アプリケーションにとっては、相当に透過的です。			○		○	

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
	設計者は、TLS によって防護されたコネクション越しでも、プレインテキストパスワードを求めることを心配する必要があります。(この要件は、実装が そのサーバーの証明書の真正性と認可を検証できる可能性が高い場合、緩和できます。)			○			
	SASL は、(パスワード(ワンタイム、または otherwise)のような)より伝統的なクライアント認証技術の利用を許容します。強力な組み合わせは、基盤の防護とサーバーの認証のために TLS を使い、クライアントを認証するために SASL に基づくシステムを使うものです。異なる認証テクニックが異なる方向で使われているとき、中間者による脆弱性を避けるために、注意が払われねばなりません。			○			
	「DNS キャッシュを汚染する攻撃」から防護する			○		○	
	「DNS 中に一般目的アプリケーションの強い鍵を置くという概念は、否決されました [RFC3445] が、特定のアプリケーション(特に、IPsec)についての強い鍵の標準化が、進行中であること」						
	「チャレンジ／レスポンス認証」の最強の形態のひとつは、デジタル署名に基づきます。						
	デジタル署名を正しく使うことは、意外に困難です。クライアントは、送られてきたチャレンジそのものに署名してはいけません。なぜなら、このような状況において放つことができる数論的攻撃が、いくつかあるからです。	○					
	DSA で署名することは、「良い乱数の利用」を要求します。						
	既知の信頼可能な源泉(X.509(証明書)のルート(CA)か、あるいは、しばしば自分自身であるところの検証者によって高度に信頼されている者のいずれか)から出発しなければなりません。		○		○		○
	署名の連鎖は、信頼できなければなりません。		○		○		○
	「ある S/MIME クライアント(メーラー)が『この署名は、妥当です。』という場合、そのユーザは、その基礎となっている意味合いを理解することを必要とせずに、その言明を額面通りに『信用』できる必要がある」						
	これを達成するために、S/MIME は、典型的には、現定数の「ルート」CA(Certifying Authorities)に基づきます。その目標は、「地球規模の信用された証明書インフラストラクチャを構築すること」です。				○		○
	このアプローチの短所は、「これが機能する前に、公開鍵インフラストラクチャが配備されていることを要求すること」です。						
	一方もしくは両方が、相互に信用された CA から証明書を入手する必要がある可能性があります。		○				○
	その CA は、事前に、彼らのメールを扱うソフトウェアによって信用されていなければなりません。						
	セキュリティに関心ある人は、必要不可欠な地球規模のインフラストラクチャが存在しない環境においてもセキュアな電子メールを必要としています。						
	ファイアウォールは、トポロジー的な防護メカニズムです。						
	ファイアウォールは、ドメインの良い「内部」と悪い「外部」の間のきちんと定義された境界に依拠し、ファイアウォールは、情報の通過を仲介します。						

RFC3631　インターネットについてのセキュリティメカニズム

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
	ファイアウォールは、セキュリティの構造全体の 1要素として使われるとき、最善に動作します。例えば、厳密なファイアウォールは、露出している Web サーバーとバックエンドデータベースの間の通信チャネルのみを開けることによって、両者を分離するために使うことができます。同様に、暗号化されたトンネルトラフィックのみを許容するファイアウォールは、VPN の一部をセキュアにするために使えます。また、VPN の他方のエンドである場合は、同等にセキュアにする必要があります。	○	○	○		○	○
	Kerberos [RFC1510] は、2 つの主体に、相互に認証し、鍵とする素材を交換するメカニズムを提供します。クライアント側において、アプリケーションは、Kerberos「チケット」と「認証子（authenticator）」を入手します。オペイク（opaque： 不透明）データと見なされる必要がある、	○				○	
	プレーンテキストのパスワードは、今日、使われている最も卑近なセキュリティメカニズムです。			○		○	
	その他の卑近なセキュリティメカニズムには、アドレスに基づく認証があります。			○		○	
	最低限、DNS からホスト名を取得するプロセスは、対応するアドレスレコードを取得し、クロスチェックする必要があります。			○		○	
	完全なセキュリティメカニズムは、ありません。						
	所与のメカニズムを採用することについてのあらゆる意思決定は、可能性のある失敗モードのすべてを測る必要があります。これら（の意思決定）は、次に、その終点におけるセキュリティの失敗についてのリスクを測る必要があります。						