RFC4086　セキュリティのための乱雑性についての要件

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	
	秘匿性を確保して、かつ／あるいは、認証と共に通信することを望む主体は、同一の秘密鍵を知らなければなりません。				
	他の場合として、共通鍵もしくは「公開鍵」暗号技術的テクニックが使われるとき、鍵は、ペアとなります。そのペアのひとつの鍵は、プライベートなものであり、ひとりによって、秘密に保たなければなりません。				
	必要なのは、予測不可能な数の物理的源泉です。				
	発信源から採取されたビット列は、ディスク回転のタイミングが平滑化されなければならないのと同様に、強く平滑化されなければなりません。				
	特に、攻撃者によるこのようなネットワークトラフィック測定の操作の可能性と、システム起動時における履歴の欠如が、注意深く考慮されなければなりません。				
	この入力が捜査の対象となる場合、これを、エントロピーの源泉として信頼してはなりません。				
	追加されたソフトウェアの複雑性に起因する失敗全体の機会における可能性ある増加に照らして重みづけられる必要があります。				
	メッセージダイジェスト関数は、可変量の入力用に設計されていますが、AES や他の暗号化関数は、任意の数の入力を組み合わせるためにも使えます。128 bit の出力が適切である場合、その入力は、必要に応じて、0 をパディングして、128 bit データ量と連続した AES「鍵」にまとめることができます。				
	このようなアルゴリズムは、プラットフォーム独立的であり、あらゆるコンピュータ上で、同じように動作できます。セキュアにされるべきアルゴリズムについて、それらの入力と内部の動作は、敵対的な観察から防護されなければなりません。				
	一連の乱数が生成されなければならない場合、攻撃者は、そのシーケンス中の何らかの値を学習する可能性があります。一般に、攻撃者が、知っている値から他の値を予測できるようではいけません。一般に、攻撃者が、知っている値から他の値を予測できるようではいけません。				
	一例は、下図に示されます。ここで、シフト演算とマスキングが、出力フィードバックの部分を古い入力の部分と結合するために使われます。この種の並行フィードバックは、下記の理由によって、避ける必要があります。				
	「特定の出力が要するものを使うこと」をサポートするために、十分なエントロピーが、そのプールに加えられるように、注意が払われなければなりません。				
	下記の節において、HMAC ハッシュの組み立ては、HMAC として言及されますが、当然ながら、特定の標準 SHA 関数が、特定の用途について選択されなければなりません。				
	一般に、生成されるべき擬似乱数値の強度が N bit でなければならないとされる場合、選択された SHA 関数は、N bit 以上の出力を生成しなければならず、少なくとも N bit の入力エントロピーの源泉が要求されます。				

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	
	上記のように、擬似乱数出力ビット列取り出し、保存したあと、返す前に、あなたは、下記のように、あと 2 回 HMAC も行う必要があります。: - K = HMAC (K, V | 0x00) - V = HMAC (K, V)				
	ANSI は、鍵のシーケンスを生成することについて、下記の手法を規定しました。 s は、64 bit の初期種です。 0 g は、生成された 64 bit の鍵のシーケンスです。 n k は、この鍵シーケンスを生成するために確保された乱雑な鍵です。 t は、鍵ができる限り長く(最高 64 bit)生成された時刻です。 DES (K, Q) は、数 Q を鍵 Kで DES 暗号化します。 次に、: g = DES (k, DES (k, t) XOR s) n s = DES (k, DES (k, t) XOR g) n+1 g sub n が DES 鍵として使われる場合、毎 8 bit は、パリティについて、その用途に応じて調整される必要がありますが、64 bit の変更されていない g の全体は、次の s を計算する際に使われる必要があります。				