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	
	フレッシュな短期セッション鍵が生成されていること				
	いくつかの共通鍵暗号アルゴリズムについて、実装は、各鍵の超過利用を防がなければなりません				
	鍵管理スキームをアマチュアが設計しては、いけません。				
	一般に、自動化された鍵管理は、セッション鍵を確立するために使われる必要があります(SHOULD)。				
	下記のいずれかの状態が保たれる場合、自動化された鍵管理が行われなければなりません(MUST) 。: - n の数が増える場合、主体は、n^2 の鍵を管理する必要がある。(RC4 [TK]、AES-CTR [NIST]、AES-CCM [WHF] のような、あらゆるストリーム暗号が使われます。) - IV(Initialization Vector)(特に、黙示的な IV)は、 再利用される可能性がある。(「明示的な乱数、もしくは擬似乱数の IV は、確率が高くない限り、問題とならないこと」に注意してください。) - 大量のデータが、短期間に暗号化される必要がある可能性があり、頻繁な短期セッション鍵の変更をもたらす。 - 長期セッション鍵は、2 者以上によって使われる。(マルチキャストは、避けられない例外ですが、マルチキャスト鍵管理標準は、将来、これを避けるために台頭しつつあります。長期セッション鍵を共有することは、一般に、止める必要があります。)				
	マニュアル鍵管理を採用しているシステムは、鍵交換についての規定を必要とします。「どの鍵が移行における問題を避けるために使われているか?」を示すための何らかの方法がなければなりません(MUST)。				
	設計は、新しい鍵を配備し、侵されている可能性がある古い鍵を置換することについて、追加可能なメカニズムを描く必要があります(SHOULD)。				
	マニュアル鍵管理が使われるとき、長期に「共有される秘密(shared secret)」の値は、少なくとも 128 bit である必要があります(SHOULD)。				