参照RFC：

技術分野	RFC#	説明	備考
SSL/TLS			
	6101	セキュア・ソケット・レイヤー（SSL）プロトコルバージョン 3.0	
	2246	TLS プロトコル v1.0	RFC4346により廃止
	4346	TLS プロトコル v1.1	RFC5246により廃止
	5246	TLS プロトコル v1.2	RFC8446により廃止
	8446	TLS プロトコル v1.3	
	6176	セキュアソケットレイヤー（SSL)バージョン2.0の禁止	
	7568	セキュアソケットレイヤー（SSL)バージョン3.0の廃止	
	8996	TLS 1.0 と TLS 1.1の廃止	
DTLS			
	4347	データグラムトランスポートレイヤーセキュリティ	RFC6347により廃止
	6347	データグラムトランスポートレイヤーセキュリティバージョン 1.2"	
	Draft	データグラムトランスポートレイヤーセキュリティバージョン 1.3"	
TLS拡張			
	6066	TLS 拡張： 拡張定義	
	4366	TLS 拡張	RFC6066により廃止
	6520	TLSおよびDTLSハートビート拡張	
	8449	TLSのレコードサイズ制限拡張	
	7627	TLSセッションハッシュおよび拡張マスターシークレット拡張	
	7685	TLS ClientHelloパディング拡張	
	7924	TLS キャッシュ情報拡張	
	7301	TLS アプリケーション層プロトコルネゴシエーション拡張	

技術分野	RFC#	説明	備考
	8422,7919	サポートする楕円曲線暗号グループ拡張	
	5746	TLS再ネゴシエーション表明拡張	
	7250	クライアントがサポートする証明書タイプ拡張が規定	
OCSP			
	6960	オンライン証明書ステータスプロトコル（OCSP)	
	6961	複数証明書のステータス要求拡張	RFC8446により廃止
	6962	証明書の透明性、署名付き証明書タイムスタンプ拡張を規、、	
	8954	OCSPノンス拡張	
乱数			
	4086	セキュリティのためのランダム性要件	
ハッシュ			
	3174	US セキュアハッシュアルゴリズム 1 (SHA1)	
	4634	US セキュアハッシュアルゴリズム(SHAとHMAC-SHA)	RFC6234により廃止
	6234	US セキュアハッシュアルゴリズム(SHA, SHA-based HMAC と HKDF)	
共通鍵暗号			
	1851	ESP 3DES Tansform	
	3602	AES-CBC アルゴリズムとIPsec での使用	
	3686	AES-CTR モードをIPsecのESPとしての使用	
	5288	TLS向けAES-GCM暗号スイート	
	6655	TLS向けAES-CCM暗号スイート	
	Draft	RC4	
	7465	RC4暗号スイートの禁止	
	5932	TLSのためのCamellia暗号スイート	
	8439	IETFプロトコル向けChaCha20 と Poly1305	
	5116	認証された暗号化のためのインタフェースとアルゴリズム	

技術分野	RFC#	説明	備考
鍵導出			
	5705	TLSのための鍵要素エクスポート	
	5869	HMACベースのエクストラクト-エキスパンド鍵導出関数 (HKDF)	
	8018	パスワードベース鍵導出 (PBKDF2)	
RSA			
	8017	PKCS #1: RSA暗号化仕様バージョン2.2	
	5756	RSA-OAEPとRSA RSASSA-PSS アルゴリズムパラメータのア ップデート	
楕円曲線			
	7748	セキュリティのための楕円曲線	
	8422	TLSバージョン1.2以前の楕円曲線暗号スイート	
鍵合意			
	7250	TLSおよびDTLSでの未加工公開鍵の使用	
	7919	TLSのネゴシエーション済み有限体DH一時パラメータ	
署名			
	6979	デジタル署名アルゴリズム(DSA)と 楕円曲線デジタル署名アルゴリズム(ECDSA)の使用法	
	8032	エドワーズ曲線デジタル署名アルゴリズム（EdDSA）	
証明書			
	3647	インターネット X.509 PKIによる証明書ポリシーと認証実施フ レームワーク	
	5280	X.509公開鍵インフラストラクチャー証明書および 証明書失効リスト（CRL)プロファイル	