Chapter 4 TLSを支える標準

IETF（Internet Engineering Task Force）は、インターネットプロトコルの標準化を目的とした標準化団体であり、TCP/IPをはじめとして多くのインターネットの基本となるプロトコル標準を策定してきました。それらの標準はRFC（Request For Comments）という形で発行されています。例えばTLS1.3の骨子はRFC8446にまとめられています。

しかし、その詳細はそれぞれ個別のRFCで定義されています。また、それらの定義は別の標準化団体の標準をベースとしていたりもします。そのため、TLSプロトコルの標準を正しく理解するためには、そうした規定同士の関係やベースとなる標準まで遡って理解する必要も出てくる場合があります。

本章では、そうしたTLSにまつわる標準規定の関係を俯瞰的に見ていきます。

4.1 IETFによる標準化

IETF（Internet Engineering Task Force）は、インターネットプロトコルの標準化を目的とした標準化団体であり、TCP/IPをはじめとして多くのインターネットの基本となるプロトコル標準を策定してきました。それらの標準はRFC（Request For Comments）という形で発行されています。TLSもRFC 2246としてバージョン1.0が策定され、その後の改版を経て今日のRFC 8446によるTLS 1.3となっています。

表4.1に、TLSとDTLS（☆脚注：UDPなど、データグラムプロトコルのセキュリティを実現するためのプロトコル。）に関連するRFCを示します。

[表4.1 TLS／DTLS関連のRFC]

技術分野	RFC番号	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	RFC 4346により廃止
	4346	TLS プロトコル v1.1	RFC 5246により廃止
	5246	TLS プロトコル v1.2	RFC 8446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			

技術分野	RFC番号	説明	備考
	4347	データグラムトランスポートレイヤーセキュリティ	RFC 6347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	

また、これらプロトコル規定の詳細は個別のRFCとして規定され、参照されています。表4.2に、TLS 1.3の詳細を規定するRFCをまとめます。

[表4.2 TLSのRFCが参照する個別のRFC]

技術分野	RFC番号	説明	備考
TLS拡張			
	6066	TLS拡張：拡張定義	
	4366	TLS拡張	RFC 6066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 Client Hello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	
	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	
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	RFC 8446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定	

技術分野	RFC番号	説明	備考
	8954	OCSPナンス拡張	
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）	RFC 6234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、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	
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ー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	

技術分野	RFC番号	説明	備考
楕円曲線			
	7748	セキュリティのための楕円曲線	
	8422	TLS 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	

4.2 公開鍵標準（PKCS：Public-Key Cryptography Standards）

PKCSは、RSAセキュリティ社により、PKI（公開鍵基盤）を具体的な標準として定めることを目的として、公開鍵暗号技術の初期段階から策定された一連の標準です。今日では、その多くがIETFのRFCに引き継がれ、インターネットプロトコル標準のベースとして参照されています（表4.4）。

[表4.4 PKCSとRFC]

PKCS番号	RFC番号	内容
#1	8017	RSA暗号スキーム
#2	-	PKCS #1へ統合され廃止
#3	-	Diffie-Hellman鍵共有
#4	-	PKCS #1へ統合され廃止
#5	8018	パスワードベース鍵導出（PBKDF2）
#6	-	X.509証明書v1の拡張構文。X.509 v3により破棄
#7	5652	暗号メッセージ構文（CMS：Cryptographic Message Syntax）
#8	5958	秘密鍵情報の構文

PKCS番号	RFC番号	内容
#9	2985	選択されたオブジェクトクラス、属性タイプ
#10	2986／5967	証明書署名要求（CSR：Certificate Signing Request）
#11		暗号トークンインターフェイス。HMS（Hardware Security Module）のためのAPI
#12	7292	パスワードベース暗号によるファイル保護。個人情報交換のための構文
#13	-	楕円曲線暗号
#14	-	擬似乱数
#15	-	暗号トークンフォーマット

4.3 X.509

X.509はITU-T（☆脚注：ITU（国際通信連合：International Telecommunications Union）の電気通信標準化部門（Telecommunication sector）。）の定めるPKI（公開鍵基盤）のための幅広い標準規格であり、TLSの中では公開鍵証明書の標準として利用されています。X.509は最初のバージョンが1988年に公開され、その後v2、v3と改訂されています。IETFではv3が参照され、RFC 5280として規定されています。なお、TLSではX.509 v2またはv3を使用することが義務付けられています。

ASN.1（抽象構文記法1：Abstract Syntax Notation One）は、X.509を始めネットワーク、コンピューターで使われるデータを汎用的な可変長レコードの集合として表現し、データ形式を厳密に定義するための標準です。当初CCITT（国際電信電話諮問委員会：Comité Consultatif International Télégraphique et Téléphonique）によるX.409勧告の一部として策定されました。その後X.208、X.680シリーズへと改訂され、現在に引き継がれていますが、今日でもASN.1の呼称が広く使われています。

ASN.1はデータの論理的な表記のみを規定します。そのため、それを物理的なデータ構造にマッピングするためにはエンコーディング規則が必要であり、BER（Basic Encoding Rules）、DER（Distinguished Encoding Rules）などが定められています。なお、DERとともに広く利用されているPEM（Privacy Enhanced Mail）のエンコード規定は、IETFでメールメッセージの秘匿性向上のためのエンコード規則として制定されました。

4.4 NISTによる標準規定

アメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）は、コンピューターセキュリティのためにSP-800（Special Publication 800）シリーズ、FIPS Pub（Federal Information Processing Standards Publication）シリーズの一連のガイドライン、および推奨ドキュメントを発表しています。これらのドキュメントは米国連邦政府による規定で、国際標準ではないものの、多くのドキュメントがインターネットにおける標準のベースとして参照し、国際的な標準にも取り入れられています。

[表4.5 ☆☆☆]

ドキュメント	内容	タイトル

ドキュメント	内容	タイトル
SP800-38D	GCM/GMAC	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM)and GMA
SP800-38C	CCM	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
SP800-38B	CMAC	Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication
SP800-38A	CBC	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
SP800-52 Rev. 2	TLS利用ガイドライン	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (2nd Draft)
SP800-56C	鍵導出	Recommendation for Key-Derivation Methods in Key-Establishment Schemes
SP 800-90A	擬似乱数	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
SP 800-90B	真性乱数	Recommendation for the Entropy Sources Used for Random Bit Generation
SP 800-131A REV. 2	鍵長	Transitioning the Use of Cryptographic Algorithms and Key Lengths
FIPS PUB 197	AES	Advanced Encryption Standard (AES)
FIPS PUB 198-1	HMAC	The Keyed-Hash Message Authentication Code(HMAC)
FIPS 186-4	DSS	Digital Signature Standard (DSS)
FIPS 180-4	SHA-1, SHA-2	Secure Hash Standard (SHS)
FIPS 202	SHA-3	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
FIPS 140-2/3	暗号アルゴリズムのセキュリティ要件	Security Requirements for Cryptographic Modules