

JavaScript による End-to-End セキュリティ

補足資料: 標準規格とセキュリティエンジニアリング

栗原 淳 ^{1),2)}

¹⁾ 株式会社ゼタント

²⁾ 兵庫県立大学

January 26, 2020

はじめに

はじめに

この資料は、「JavaScript による End-to-End セキュリティ」の補足資料である。

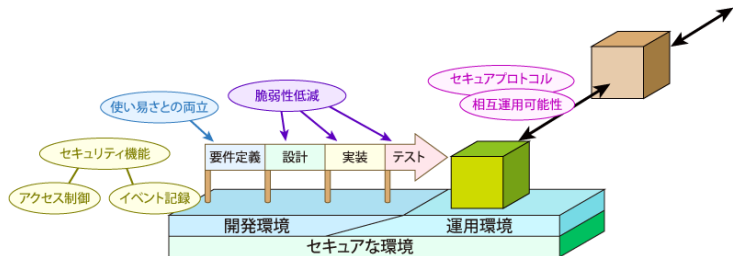
「標準規格」そのもの、および一連の勉強会にて話題に上げた鍵フォーマットや標準アルゴリズムについてを解説を与える。

セキュリティ関連の標準規格

はじめに：セキュリティエンジニアリングと標準規格

セキュリティエンジニアリング¹

ソフトウェア・アプリケーション開発において、セキュリティを考慮したエンジニアリング、あるいはセキュリティエンジニアリングを行うためには、要件定義・設計・実装・テストの段階ごとに種々のセキュリティ関連事項を検討する必要がある。



¹<https://www.ipa.go.jp/security/awareness/vendor/software.html>

一方で、標準規格は:

標準規格となるアルゴリズム・プロトコル

国家や団体の標準文書に載せるために、**安全性・相互接続性・効率性**を分析し、**安全性や将来性などがある程度確保**されたもの、
と言える。



すなわち、標準規格を要件に応じて適切に選択し、設計・実装を行うことで脆弱性低減、使いやすさとの両立や相互運用可能性の担保が容易になると言える。

つまり、最新の標準規格とその推奨される利用方法²を把握しておくことで、**効率的なセキュリティエンジニアリングが行える**。

²なぜそのように利用するのか・載っているのか、も正しく知っておく必要がある。悪い例は、脆弱性はあるが互換性のために残っている RFC8017 の RSAES-PKCS1-v1.5。

次ページからは、実際のセキュリティ関連標準について紹介する。

PKCS (Public Key Cryptography Standards)

PKCS とは？

RSA Security 社³の研究部門 RSA Labs が策定・公開している、公開鍵暗号を中心とする一連のセキュリティ技術標準のこと。比較的古い、枯れた標準になる。

- #1,...#15 の 15 本が存在⁴。
- 暗号化・署名生成の手続き・アルゴリズム、データフォーマットの規定など、いわゆる「ローレベル」の技術標準が中心。
- RSA 暗号標準を定める#1 を代表に、重要なものはメンテされ続けている。が、他の新標準規格で代替されるものなどは破棄・管理移譲されている。

³RSA 暗号を作った Rivest-Shamir-Adleman の会社。

⁴破棄・廃盤も含む。

PKCS は、その名目上「私企業」が策定した技術標準。
しかし、採用された技術は、十分にセキュリティ評価されていると見做されるものが多く、また他の技術標準に採用・移植・継承されている。特に多くは IETF RFC の管理下へ継承されているようだ。

PKCS 文書一覧 (1/2)

	Ver.	名称	内容
PKCS #1	v2.2	RSA Cryptography Specifications ⁵	RSA 鍵ペアの構造、暗号化手法、署名手法を策定。
PKCS #3	v1.4	Diffie-Hellman Key Agreement Standard	Diffie-Hellman 鍵交換の仕様を策定。RFC では Internet Key Exchange (IKE) へ継承 (?)。
PKCS #5	v2.1	Password-Based Cryptography Specification ⁶	パスワードからの鍵導出手法、暗号化手法 (PBKDF1/2, PBES1/2) の策定。
PKCS #6	廃止	Extended-Certificate Syntax Standard	X.509v1 証明書の拡張。X.509v3 へ統合されて廃止。
PKCS #7	廃止 (?)	Cryptographic Message Syntax Standard ⁷	暗号メッセージ構文を策定。S/MIME に利用。より新しい仕様 (RFC5652) により廃止 (?)。
PKCS #8	廃止 (?)	Private-Key Information Syntax Specification ⁸	秘密鍵フォーマットを策定。より新しい仕様 (RFC5968) により v1.2 で廃止 (?)。
PKCS #9	v2.0	Selected Object Classes and Attribute Types ⁹	各種フォーマットにおける「属性」タイプを策定。

⁵<https://tools.ietf.org/html/rfc8017>

⁶<https://tools.ietf.org/html/rfc8018>

⁷<https://tools.ietf.org/html/rfc2315>

⁸<https://tools.ietf.org/html/rfc5208>

⁹<https://tools.ietf.org/html/rfc2985>

PKCS 文書一覧 (2/2)

	Ver.	名称	内容
PKCS #10	v1.7	Certification Request Syntax Specification ¹⁰	証明書リクエスト構文を策定。元は PKCS のみで策定されていたが、利用されるメディアタイプを RFC5967 で拡張。
PKCS #11	v2.40	Cryptographic Token Interface	Cryptoki としても知られる、暗号トークン (H/W セキュリティモジュール) インターフェースの仕様を策定。OASIS PKCS 11 Technical Committee へ継承。
PKCS #12	v1.1	Personal Information Exchange Syntax Standard ¹¹	パスワード暗号化された秘密鍵、公開鍵証明書の構文を策定。IETF IESG 管理下へ継承。
PKCS #15	v1.1	Cryptographic Token Information Format Standard	暗号トークン向け、ユーザ特定標準仕様の策定。IC カード部分は ISO/IEC 7816-15 へ移譲。

策定中のまま立ち消えたものなどは削除。

IETF RFC などへ Republication、あるいは継承されて新しい標準になっている。

¹⁰<https://tools.ietf.org/html/rfc2986> + <https://tools.ietf.org/html/rfc5967>

¹¹<https://tools.ietf.org/html/rfc7292>

NIST FIPS/SP800 とは？

米国国立標準技術研究所 (NIST; National Institute of Standards and Technology) の発行する文書のこと。

- **FIPS; Federal Information Processing Standards**: 米国商務長官の承認の下、NIST が公布した情報セキュリティ関連の米国の標準規格文書。詳細な基準や要求事項、ガイドラインが記載されている。
- **SP800; Special Publication**: 米国政府がセキュリティ対策を実施する際に参考とすることを前提とした、コンピュータセキュリティ関係のレポート。

¹²参考: <https://www.ipa.go.jp/security/publications/nist/>

すなわち NIST FIPS は、米国ローカルの標準規格と言える。

- 多くは、他の国別標準規格同様に ANSI/ISO/IEEE 等で広く使われていた既存規格を引き継ぐ。
- 一部は NIST FIPS 独自に公募・評価・策定した独自規格。代表的なものは、公募されてきた 'Rijndael' という新暗号アルゴリズムを採用した FIPS 197; Advanced Encryption Standard (AES)。

RFC (Request for Comments) とは？

「インターネット技術」全般の国際標準を議論策定するグループ IETF (Internet Engineering Task Force) で議論策定された、「インターネット技術標準」および「その他」¹³ の広範な内容を扱う文書 (群) のこと。

詳細仕様を策定する ITU-T や ISO と異なり、「まずは動作させる」ことを目的として実験的な「Rough」な仕様をまず策定することが特徴。

¹³<https://www.nic.ad.jp/ja/rfc-jp/RFC-Category.html>

RFC は 5 つのカテゴリに分類される:

- **Standards Track**: Proposed Standard → Internet Standard という策定過程を経る「インターネット標準技術仕様」の文書。
- **Informational**: すでにデファクト標準であったり、インターネット標準の議論・策定において有益として公開されたもの。例えば、RSA セキュリティ社の PKCS#1 v2.1 = RFC8017。
- **Experimental**: デファクト標準を狙うような、研究等の目的で公開される技術仕様文書。
- **Historical**: 過去の記録として残す情報としての文書。
- **Best Current Practice**: 現状のベストプラクティスをまとめた仕様文書。

特に Standard Track, Informational, Experimental に関して、PKCS 等の他標準を引き継いだり、新たな技術標準を定めた文書が策定される。

セキュリティ関係の RFC 化の事例：

- 事例 1: OpenID Connect によって利用される鍵や署名、暗号化の仕様: JWS¹⁴, JWE¹⁵, JWK¹⁶, JWT¹⁷ について、OpenID Foundation のメンバにより、RFC Standards Track として国際標準化。
- 事例 2: PKCS#1, #5, #9 等の RSA セキュリティ社の独自標準は、Informational として RFC 化。
- 事例 3: HTTPS を支える TLS v1.3¹⁸ は、Standards Track として RFC 化。

¹⁴ JSON Web Signature <https://tools.ietf.org/html/rfc7515>

¹⁵ JSON Web Encryption <https://tools.ietf.org/html/rfc7516>

¹⁶ JSON Web Key <https://tools.ietf.org/html/rfc7517>

¹⁷ JSON Web Token <https://tools.ietf.org/html/rfc7519>

¹⁸ <https://tools.ietf.org/html/rfc8446>

ISO¹⁹/IEC²⁰ JTC (Joint Technical Committee) 1 とは

情報技術の分野で国際標準化を行うための、ISO と IEC の第一合同技術委員会のこと。セキュリティ技術は、第 27 subcommittee (SC27)。

ISO/IEC JTC 1 は各国が提案を持ち寄り議論が進められる国際標準化団体。他の標準規格からの引継ぎだけではなく、国際会議等で発表された新しいメカニズムやアルゴリズムも標準規格として提案される。

¹⁹ 国際標準化機構; International Organization for Standardization

²⁰ 国際電気標準会議; International Electrotechnical Commission

ISO/IEC JTC1 SC27 は 5 つの Working Group で構成される²¹。特に WG2 で扱われるものが、セキュリティ「技術」や「メカニズム」の標準規格となる。

- WG 1 情報セキュリティマネジメントシステム (いわゆる ISMS)
- **WG 2 暗号とセキュリティメカニズム**: 暗号アルゴリズム・プロトコルの標準規格。他の標準規格からの引継ぎだけでなく、各国から新たに提案されたものを議論し、標準規格を決定している。
- WG3 セキュリティの評価・試験・仕様
- WG4 セキュリティコントロールとサービス
- WG5 アイデンティティ管理とプライバシー技術

²¹https://www.itscj.ipsj.or.jp/hyojunka/h_sn_member/h_sn_katsudo/h_sn_katsudo2013/sc27_2013.html

W3C (World Wide Web Consortium)

W3C とは？

WWW で用いられる Web 技術の標準化、相互運用性の確保を目的とする団体。ブラウザの API や HTML, XML, DOM 等の標準規格を「勧告 (Recommendation)」として策定する。

W3C のセキュリティ関連 WG (Working Group) で有名な活動として、以下のような国際標準化策定が上げられる。

- **WebCrypto WG**²²: WebCrypto API を策定、勧告として国際標準化。
- **WebAuthn WG**²³: FIDO アライアンスの技術仕様を勧告として国際標準化²⁴

²²<https://www.w3.org/2012/webcrypto/> 現状は Close。

²³<https://www.w3.org/blog/webauthn/>

²⁴対象はブラウザ・端末・認証サーバの連携プロトコルである FIDO2 WebAuthn <https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.ja>。デバイス連携プロトコルである FIDO2 CTAP は ITU-T で国際標準化。

ITU-T (International Telecommunication Union Telecommunication Standardization Sector) SG17 (Study Group 17) とは？²⁵

- ITU-T: ITU (International Telecom. Union; 国際電気通信連合) における通信分野の標準技術を策定する「電気通信標準化部門」。策定された標準は「勧告」として発行される。
- Study Group 17: ITU-T においてセキュリティ関連勧告作成の中心となるグループ。

²⁵https://www.ituaj.jp/wp-content/uploads/2016/07/2016_08-06-spotITU-T.pdf

ITU-T SG17 で取り扱う技術は、SDN・IoT・ITS・クラウドのセキュリティ技術、SPAM 対策、ID 管理技術、認証技術、テレバイオメトリクスなど、ソフトウェア実装のためのアルゴリズムというより「通信事業者」や「通信端末」を対象とした分野の技術。

昨今だと、「FIDO アライアンスの技術仕様を勧告として国際標準化²⁶」している。

²⁶対象はデバイス連携プロトコルである FIDO UAF 1.1 および CTAP <https://fidoalliance.org/fido-alliance-specifications-now-adopted-as-itu-international-standards/>。Web 関連プロトコルである FIDO2 WebAuthn は W3C で国際標準化。

その他; 各国の推奨技術リストとしての標準規格

■ CRYPTOREC²⁷

電子政府推奨暗号リストを作り、その実装や運用方法も含めて安全性を調査・評価・監視・検討するプロジェクト (2000 年～)

■ NESSIE²⁸

EU の制定した暗号標準リストを策定するプロジェクト (2000 年～)

基本的には、「評価検討した結果、既存のアルゴリズム・プロトコルのどれそれを標準として採用する」という「推奨技術リスト」の策定プロジェクトだと思って差し支えない。

²⁷ Cryptography Research and Evaluation Committee

²⁸ New European Schemes for Signature, Integrity, and Encryption

「各国独自」という意味

推奨技術リストへ採用されたアルゴリズム・プロトコルは、「その国において正しく評価された比較的安全なもの」というお墨付きを得る。
セキュリティ技術は国防上重要な意味を持つため、このお墨付きは、その技術を自国で利用して良いものかどうかを判定するもの、と言える。

仕様の詳細は IETF (RFC), ISO, NIST 公募など国際的に比較的オープンな場でまず評価・採用・策定される²⁹。

その後、各国が独自に調査検討して推奨技術リストとして採用する、というケースが多い。

²⁹例外は存在する。元々 PKCS は RSA Labs. の独自標準を公開したものだったが、IETF の公開の場で Internet Draft の形で標準化されてきている。

その他; 諸々

- FIDO Alliance: フォーラム標準を定める業界団体。国際標準ではない。
- OpenID Foundation: 上記同様。
- Ecma International: JavaScript のメイン機能の標準規格 (ECMAScript) を策定する業界団体。JS 以外にも多種の規格策定、および Ecma 規格の国際標準化を行っている。³⁰

³⁰例えば: Ecma 規格 ECMA-334 “C#” は、国際規格 ISO/IEC 23270 として標準化。

公開鍵・秘密鍵等の表現形式

公開鍵・秘密鍵・証明書等の形式

公開鍵・秘密鍵・証明書などを表すための代表的な表現形式:

- DER (Distinguished Encoding Rules) 形式: ANS.1 で記述されるエンコード方法。RSA 暗号の公開鍵・秘密鍵、楕円曲線暗号の公開鍵・秘密鍵など、それぞれエンコード方法を規定。
- PEM (Privacy Enhanced Mail³¹): DER の Base64 テキスト。
- SECG SEC1 形式: (楕円曲線暗号の鍵のみ) 業界団体 SECG で定められた公開鍵・秘密鍵のバイナリ表現方法。³²
- JWK/JWE/JWS (JSON Web Key/Encryption/Signature) 形式: JSON 形式での表現方法。³³

基本、JavaScript では鍵を JWK として使うことが多いだろうが、OpenSSL 等で最も良く利用されるのは DER・PEM 形式の鍵。

³¹元々メールを暗号化したデータのエンコード方法だったので。

³²<http://www.secg.org/sec1-v2.pdf>

³³<https://tools.ietf.org/html/rfc7517>, <https://tools.ietf.org/html/rfc7516>, <https://tools.ietf.org/html/rfc7515>

Table: 各データの表現形式の規定文書一覧³⁴

	DER/PEM	SECG SEC1	JWK/E/S
RSA 公開鍵	1) PKCS#1 2) RFC5280 ³⁵	N/A	RFC7517
RSA 秘密鍵	RFC5958 ³⁶ , PKCS#1 ³⁷	N/A	RFC7517
ECC 公開鍵	RFC5480 ³⁸	SECG SEC1 v2	RFC7517
ECC 秘密鍵	RFC5958 ³⁹ , RFC5915 ⁴⁰	SECG SEC1 v2	RFC7517
(AES) 共通鍵	N/A	N/A	RFC7517
公開鍵証明書	RFC5280 (他)	N/A	N/A ⁴¹
RSA 暗号文	N/A	N/A	RFC7516
ECDH+AES 暗号文	N/A	N/A	RFC7516
AES 暗号文	N/A	N/A	RFC7516
HMAC	N/A	N/A	RFC7515
RSA 署名	N/A	N/A	RFC7515
ECDSA 署名	RFC5759	N/A	RFC7515

³⁴ 調べ間違い等あったらご指摘を！

³⁵ 証明書の中にある SubjectPublicKeyInfo フィールド

³⁶ 秘密鍵の暗号化サポート。RFC5958 は PKCS#8 の拡張。

³⁷ RSA 秘密鍵自体の構造を定義

³⁸ 証明書の中にある SubjectPublicKeyInfo フィールド

³⁹ 秘密鍵の暗号化をサポートするフォーマット

⁴⁰ ECC 秘密鍵自体の構造を定義

⁴¹ X.509 証明書への URI 等は記述可能 <https://tools.ietf.org/html/rfc7517>

WebCrypto API/Node.js でサポートする公開鍵・秘密鍵フォーマット

- WebCrypto API:
RFC5280 形式 (公開鍵のみ)、RFC5958 形式 (秘密鍵のみ)、JWK
- Node.js Crypto:
RFC5280 形式 (公開鍵のみ)、RFC5958 形式 (秘密鍵のみ)、PKCS#1 形式

統一が取れていないため、環境に応じて適切な表現形式の変換が必要⁴²

⁴²jscu はこれらの鍵変換をサポート。

<https://github.com/junkurihara/jscu/tree/develop/packages/js-crypto-key-utils>

楕円曲線暗号のパラメタについて

ECDH, ECDSA の鍵選択 (曲線の選択)

RSA 暗号と楕円曲線暗号 (ECDH/ECDSA) のパラメタ

- RSA: パラメタは「公開鍵ビット長」
- 楕円曲線: パラメタは「曲線の種類」

曲線の種類は、公開鍵ビット長を定めれば一意に決まるわけではない⁴³。

※ただし、RSA 暗号・楕円曲線暗号共々、“一般的には” **公開鍵ビット長が大きいほど、より安全になり、より処理が重くなる**というトレードオフがある。

⁴³e.g., 公開鍵長 256bit では、P-256 や P-256K など複数の利用可能な曲線の種類が存在。

では、こういった曲線を選べば良いのか？

代表的な楕円曲線パラメタの標準

- SEC2: 業界団体 SECG の標準 ⁴⁴
- ANSI X9.62: 米国標準 ⁴⁵
- NIST FIPS186-4: 米国標準 ⁴⁶

それぞれで標準化されたパラメタは、大きくオーバーラップしている ⁴⁷ が、最も頻繁に更新されている標準パラメタリストは **NIST FIPS 186** のものである。

⁴⁴<http://www.secg.org/sec2-v2.pdf>

⁴⁵American National Standards Institute, “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),” ANSI X9.62, November 2005.

⁴⁶<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

⁴⁷<https://tools.ietf.org/html/rfc8422#appendix-A>

WebCrypto API/Node.js 両方で選択できる NIST 曲線パラメタ

- P-256: 公開鍵長 = 256bits, 安全性 \approx 128bit 鍵 AES
- P-384: 公開鍵長 = 384bits, 安全性 \approx 192bit 鍵 AES
- P-521: 公開鍵長 = 521bits, 安全性 \approx 256bit 鍵 AES

Bitcoin Blockchain で使用されている曲線⁴⁸ は、WebCrypto API でネイティブには未実装。

⁴⁸SECG パラメタ secp256k1 あるいは P-256K と呼ばれる。

曲線パラメタに対して、より学術的な脆弱性の有無の一覧：
Safe Curves: <https://safecurves.cr.yp.to/>



現実的な攻撃かどうかはさておき、NIST 曲線パラメタには有効な攻撃が知られている⁴⁹。

実装に不備がある場合に発生する脆弱性が多く、“正しく設計・実装されている既存ライブラリ”のAPI経由で利用する分には問題ないと言ってもよいだろう。

⁴⁹ safecurves のサイトで Safe?=False の場合、攻撃が存在。