

電子証明書の動向

2026年9月版

インターネットEDI普及推進協議会

Japan internet EDI Association (JiEDIA)

<https://www.jisa.or.jp/jiedia/tabid/2822/Default.aspx>

Agenda

- 1.インターネットEDI普及推進協議会のご紹介
- 2.電子証明書の動向
- 3.EDIへの影響
- 4.対応の方向性

1. インターネットEDI普及推進協議会のご紹介

(出典：固定電話網のIP網移行によるEDIへの影響と対策【概説】 V5.1.1)

●協議会設立の目的・概要（2019.07設立）

名称：インターネットEDI普及推進協議会

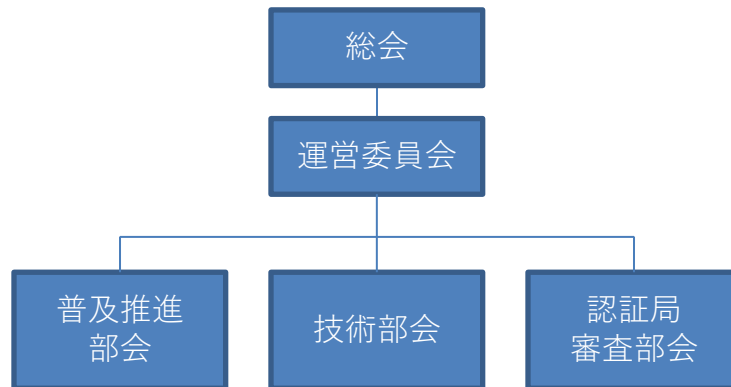
英語名称：Japan internet EDI Association（略称：JiEDIA/ジェディア）

設立目的：我が国における各産業界でのサプライチェーンの情報流通をインターネットEDIによって最適化、高度化ならびに効率化する活動を行う。

活動内容：国内インターネットEDI通信プロトコル（JX手順、全銀TCP/IP・広域IP網）の維持管理に加え、データ交換共通認証局認定制度の推進・運営活動を行う。

想定会員：（１）正会員 本会の設立趣旨に賛同した業界団体
及び 別に定める団体または企業
（２）特別会員 大学、団体、研究機関 及び それに準ずる
組織に属する有識者であって、本会の要請
により入会した者

●協議会の体制



会 長 : 藤野 裕司
幹事(会長代理) : 仲矢 靖之
幹事(会長代理) : 石金 克也
事務局 : JISAの事務局が担当

総会：意思決定機関。年1回程度（または重要審議事項が発生した際）に開催。

運営委員会：本協議会の実質的な推進組織。隔月程度（または必要に応じて）開催。

普及推進部会：

- 関連省庁（総務省、経産省）、NTT東西、各業界団体との連携
- 広報資料の作成、セミナーの開催 等

技術部会

- ネットワークや関係ハード、プロトコルの仕様調査確認
- 実証実験の計画と実施、移行方法の検討 等

認証局審査部会

- データ交換共通認証局認定制度の推進・運営
- 認証局証明書ポリシーの作成、認証局の認定 等

2.電子証明書の動向

① パブリックTLS証明書有効期限の大幅な短縮

- ・ 最大398日 → 200日（2026年3月15日～／適用済み） → 100日（2027年3月15日～） → 47日（2029年3月15日～）
- ・ ドメイン検証（DCV）データの再利用期間も同じ日程で短縮され、最終的に10日となる。
- ・ 更新回数は8～9倍規模に増加。運用負荷が高くなることが予想されるため、ACME/CLM等による自動化が望ましい。
- ・ 根拠：CA/Browser Forum Ballot SC-081v3（2025年4月11日可決）

② パブリック証明書の用途分離（デュアルEKUの廃止）

- ・ 1枚の証明書でサーバ認証（serverAuth）とクライアント認証（clientAuth）を兼務することが不可に。
- ・ 根拠は Google Chrome ルートプログラムポリシー（v1.6～v1.8）。 ※SC-081v3とは別の施策。
- ・ 下位CAの分離は2026年6月15日から適用済み。加入者証明書は2027年3月15日から。
- ・ mTLS・機器認証などのclientAuth用途はプライベートCAへ移る。

③ 耐量子暗号（PQC）への移行

- ・ 2024年8月13日、NISTがPQC標準（FIPS 203／204／205）を公表。
- ・ 証明書の署名はML-DSA（FIPS 204）が本命。鍵交換はML-KEM。（FIPS 203）
- ・ RSA／ECCは2030年に非推奨、2035年に使用禁止。（NIST IR 8547）

①パブリックTLS証明書有効期限の大幅な短縮

最大有効期間とDCV再利用期間のスケジュール (Ballot SC-081v3)

適用時期	最大有効期間	DCV (ドメイン検証) 再利用期間	状況
～2026年3月14日	398日	398日	終了
2026年3月15日～	200日	200日	適用済み (現在地)
2027年3月15日～	100日	100日	今後
2029年3月15日～	47日	10日	今後

- ・OV等の組織情報の再利用期間は 825日 → 398日 (2026年3月15日～) に短縮
- ・DCV再利用の10日化により、再検証は「年1回の作業」から「更新のたびに走る常時処理」へ変わる
- ・各認証局は業界上限より1日短く運用する場合がある (例：一部認証局では199日／2026年2月25日～)

運用へのインパクト

- 8～9倍** 更新回数の増加規模
- 30万枚超** 大企業が平均で保有する証明書数
- 87%** 証明書の予期せぬ失効による障害を経験

対応の方向性

ACME (RFC 8555) による発行・更新の自動化と、CLM (証明書ライフサイクル管理) 基盤の整備が望ましい。

検証 (DCV) 自体の自動化と監視も同時に必要となる。6割程度の組織が今なお表計算や手作業で台帳管理しており、この体制では追従できない。

②パブリック証明書の用途分離

これまで

パブリックTLS証明書（1枚）

serverAuth + clientAuth

1枚で兼務 — これが禁止に

これから（2026年6月～／2027年3月～）

パブリックCA発行：serverAuth のみ
WebサーバのHTTPS用途

プライベートCA発行：clientAuth
mTLS・機器／ワークロード認証

主なマイルストーン（Chrome Root Program Policy v1.8／2026年2月5日更新）

適用時期	内容	状況
2025年10月1日～	主要CAがclientAuth EKUのデフォルト付与を停止	適用済み
2026年6月15日	CCADBに開示される新規の下位CAはEKU分離（serverAuthのみ）が必須	適用済み
2027年3月1日	CAによってはこの日で発行を終了	今後
2027年3月15日	新規発行のパブリックTLS証明書はserverAuthのみ	今後

- ・影響を受けるのはmTLS、機器・ワークロード認証、サーバ間連携。通常のHTTPS閲覧には影響なし。
- ・発行済みの証明書は有効期限まで利用可能。ただし更新時には分離が前提となる。
- ・リーフ証明書だけでなく、中間CAの階層自体をサーバ用／クライアント用に分離することが求められる。

③耐量子暗号（PQC）への移行

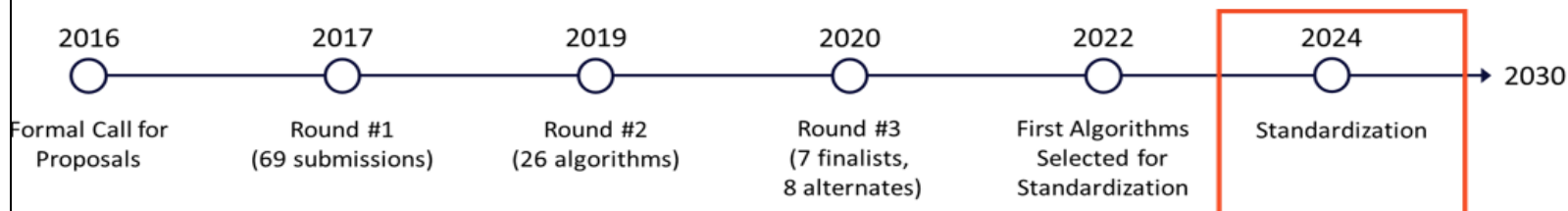
耐量子計算機暗号と標準化動向

■ 耐量子計算機暗号とは

	アルゴリズム	脅威となる量子アルゴリズム	対策
公開鍵暗号	RSA, ECC, DH	ショアのアルゴリズム (素因数分解・離散対数問題を多項式時間で解ける)	耐量子計算機暗号へ移行 (NISTによる標準化)
共通鍵暗号	AES	グローバーのアルゴリズム (総当たりで古典よりも高速に検索)	鍵長を拡張する(2倍)

数学的に解きにくくすることで対応

■ NISTによる標準化動向



- ・ 2016年にNIST（アメリカ国立標準技術研究所）がPQC標準化計画を発表
- ・ 2024年8月13日にNISTよりPQC標準方式のアナウンス

	公開鍵暗号/鍵交換方式	デジタル署名
標準化アルゴリズム	CRYSTALS-KYBER	CRYSTALS-DILITHIUM SPHINCS+

③耐量子暗号（PQC）への移行（つづき）

2024年8月13日	～2030年	～2035年
NISTがPQC標準を公表 ・ FIPS 203 = ML-KEM（鍵交換） ・ FIPS 204 = ML-DSA（署名） ・ FIPS 205 = SLH-DSA（署名）	非推奨（deprecated） ・ RSA-2048／ECC-224相当（112ビット強度）が非推奨に（NIST IR 8547） ・ 米国連邦民生機関は2030年12月31日までに移行完了を目標 大統領令14412：2026年6月22日署名 OMB M-26-15：2026年6月24日発出	使用禁止（disallowed） ・ 量子計算機に脆弱な公開鍵暗号の利用を原則禁止 ・ 英国・カナダ・豪州・EU・日本も同様の時間軸で移行計画を提示

押さえておく前提

- ・ 証明書の署名はML-DSAが主軸。SLH-DSAはハッシュベースで、長期保証やファームウェア署名向け
- ・ Harvest Now, Decrypt Later — 今日暗号化した長期保存データは、すでに将来の解読リスクに晒されている
- ・ 鍵交換ではML-KEM-768がデファクトスタンダードとして推奨されている
- ・ 現行アルゴリズムとPQCアルゴリズムを併用する並行稼働期間の証明書フォーマット（ハイブリッド）についても、IETFやNISTで標準化が進められている
- ・ 日本においても、政府機関等は原則2035年までにPQCへ移行することを目指し、工程表（ロードマップ）を2026年度に策定する方針
（内閣官房 国家サイバー統括室「PQCへの移行について（中間とりまとめ）」2025年11月20日公表）

【補足】最新動向アップデート（2026年8月時点）

47日への道はすでに始まっている

- ・ 2026年3月15日に第1段階（200日）が発効。
同日、CAによるDNSSEC検証を義務づけるBallot SC-085v2も同時に適用開始。
- ・ 一部認証局では上限より1日短い199日運用。
既存のドメイン検証も適用日をもって短縮されるため、更新設計の見直しが必要。

短命証明書が実用段階へ

- ・ Let's Encryptが6日間（160時間）証明書とIPアドレス証明書を2026年1月に一般提供開始。
（ACMEのshortlivedプロファイル）
- ・ 既定の有効期間も90日から45日へ段階的に短縮する方針。
- ・ 47日を待たずに「常時自動更新」が現実解になりつつある。

clientAuth分離はスケジュールが緩和

- ・ Chromeがルートプログラムの期限を見直し、パブリックTLS証明書へのclientAuth EKU付与は2027年3月1日まで継続可能に。
- ・ 一方、下位CAの分離（2026年6月15日）はすでに適用済みで、clientAuthを発行できる公開CAの母数は縮小し続けている。

PQCは「鍵交換」が先行、「証明書」はこれから

- ・ 主要ブラウザはハイブリッド鍵交換（X25519+ML-KEM-768）に既定対応。
上位サイトの約4割が対応済みだが全体では1割未満。
- ・ 公開トラストのPQC証明書はまだ存在せず、登場は2026年後半以降。
Let's EncryptはMerkle Tree Certificatesを移行手段として推進。
- ・ MicrosoftはAD CSのML-DSA対応を2026年5月に一般提供。
- ・ FIPS 140-2認証は2026年9月21日にHistoricalへ移行。

出典：CA/Browser Forum Ballot SC-081v3／SC-085v2、Chrome Root Program Policy v1.8、Let's Encrypt、DigiCert、NIST（FIPS 203-205／IR 8547）、米国大統領令14412・OMB M-26-15、内閣官房 国家サイバー統括室

3.EDIへの影響

①EDI通信におけるサーバ証明書の運用

- ・サーバ証明書の運用は、以下のいずれかのパターンが多いと想定されます。
 - EDIエンジンにて管理
 - apacheやnginx等のwebサーバにて管理
 - SSLアクセラレータ(ロードバランサーを含む)での管理
 - クラウドWAFでの管理

サーバ証明書の有効期限が短くなることから、更新作業の自動化を検討することが望ましいと考えます。

②EDI通信におけるクライアント証明書の運用

- ・クライアント証明書の運用は、以下のいずれかのパターンが多いと想定されます。
 - EDIエンジンで管理
 - Javaのkeystoreファイルで管理

パブリック証明書を利用する場合、サーバ証明書との兼用ができなくなることから、対応を検討する必要があります。

→ パブリック証明書を維持する場合

サーバ証明書との兼用ができなくなるため、クライアント証明書の準備が必要になります。

(クライアント証明書分のコストが発生)

また、証明書の自動更新手段を検討することが望ましいと考えます。

→ プライベート証明書を利用する場合

ご利用の認証局の情報を入手し、影響範囲を確認する必要があります。

②EDI通信におけるクライアント証明書の運用（つづき）

・SSL/TLS通信時の課題（プロトコル共通）

EDIサービス事業者の場合、クライアント証明書の取得をユーザーが行うケースがあります。

- クライアント証明書の申請・取得：ユーザー
- ユーザークライアント証明書の登録：サービス事業者

この場合、サービス事業者によるクライアント証明書の自動更新は行えないと想定されます。パブリック証明書を継続利用する場合、サーバ証明書との兼用ができなくなるため、ユーザーとサービス事業者間で新たに証明書の受け渡しフローが必要となり、更新の都度この作業が発生することで運用負担が増加することが予想されます。

・AS2署名機能の課題

AS2において署名機能を利用しているケースでの影響です。

- クライアント証明書の秘密鍵を自社に登録
- 検証用の公開鍵をデータ受信側に登録

ユーザーはクライアント証明書の発行・受け渡し、公開鍵の作成、および通信相手への公開鍵送付を証明書の更新の都度行う必要があります。これは人手を介する作業が必要となることが予想されます。

③Web-EDIへの影響

- ・ 証明書更新頻度の増加によるリスク

Web-EDIも通常のWebサイトと同様に、SSL/TLS証明書の有効期限短縮や更新ルール改訂の影響を受けます。
証明書更新が遅れた場合、取引先との接続が停止する可能性があります。

- ・ クライアント証明書の運用負担増

クライアント証明書を利用している場合、取引先との証明書の受け渡しや登録作業など、
更新に伴う運用負担が増加します。

- ・ プライベート証明書利用へのリスク

プライベート証明書をWeb-EDIで利用する場合は、利用端末・ブラウザへの信頼設定や、
今後のブラウザ／OSポリシーとの適合性を継続的に確認する必要があります。

【参考】 JiEDIAにおけるクライアント証明書自動更新の取り組み

JiEDIAでは、インターネットEDIにおける電子証明書の運用負荷軽減と相互接続性の向上を目的として、認証局とEDI通信クライアント間の証明書発行・更新API仕様を策定しています。

「電子証明書自動更新API利用ガイドライン」 V1.0.0（2021年4月）

- ・ 証明書の新規発行・更新をAPI化
- ・ EDI通信クライアントへの証明書取得・登録を自動化
- ・ 証明書の有効期限に応じた自動更新を想定

※今回の証明書短命化・用途分離への対応を目的として策定したものではありません。

詳細は以下「JiEDIAホームページ」の「電子証明書自動更新API利用ガイドラインについて」をご参照ください。
<https://www.jisa.or.jp/jiedia/tabid/2822/Default.aspx>

4.対応の方向性

プライベート認証局の動き

役割の拡大：クライアント認証の受け皿へ

- ・パブリック側でclientAuthが使えなくなるため、mTLS・機器認証・サービス間認証はプライベート／エンタープライズPKIへ移管するのが既定路線。
- ・主要CAベンダも、clientAuth証明書はプライベートCAソリューションとして提供する方針を打ち出している。

内部PKI更改のトレンド

- ・ACME対応の内部CAへ。HTTP-01／DNS-01に加え、device-attest-01で機器そのものを検証する方式も利用可能。
- ・Kubernetes、サービスメッシュ、CI/CDへ組み込み、短命証明書を前提とした「制御プレーン」として運用する構成。
- ・AD CS等の従来型内部CAから、マネージド／SaaS型プライベートCAへの移行検討が進む。

有効期限もパブリックに追随する動き

- ・内部証明書も短期化＋自動更新を前提とした設計へ。自動化なしに期限短縮への追従はできない。
- ・一方で内部CAは有効期間を自社ポリシーで決められるため、移行の緩衝材としても機能する。

ガバナンス面の要件

- ・発行ポリシーの明文化、ACMEアカウントと実IDの紐付け、監査ログ、失効運用と可視化（インベントリ）の整備。

想定されるアクション

短期（～2026年度）

- ・ 証明書インベントリの整備。パブリック／プライベート別に用途・EKU・有効期限・設置先を可視化する。
- ・ デュアルEKUを使っている箇所を洗い出し、プライベートCAへの移行計画を策定。
（パブリックTLS証明書の用途分離は2027年3月が次の節目）
- ・ 200日への短縮（2026年3月～）を踏まえ、更なる短期化に向けた更新運用の見直し。

中期（～2027年）

- ・ ACME／CLMによる更新自動化を本番適用し、100日、さらに47日サイクルに耐える運用へ。
- ・ 内部CAのACME対応・短期証明書対応を含むプライベートPKIの更改。

長期（～2030／2035年）

- ・ 暗号資産インベントリを起点にPQC移行計画を策定し、ハイブリッド構成で段階的に移行。
- ・ 調達・設計要件にクリプトアジリティを組み込む。

出典：NIST IR 8547／NIST PQC標準（FIPS 203-205）、CA/Browser Forum Ballot SC-081v3、Chrome Root Program Policy v1.8、米国OMB M-26-15、MITRE PQC Migration Roadmap、各認証局の公表情報

ご清聴ありがとうございました。

インターネットEDI普及推進協議会
Japan internet EDI Association (JiEDIA)

本資料に関する問い合わせは、下記までお願いします。

JiEDIA 事務局：一般社団法人 情報サービス産業協会
<https://www.jisa.or.jp/tabid/2821/Default.aspx>

〒101-0047
東京都千代田区内神田2-3-4
S-GATE大手町北6F
TEL：03-5289-7651（代表）
FAX：03-5289-7653

本資料は、作成時点における公開情報等に基づき作成したものであり、記載内容の正確性・完全性を保証するものではありません。各種仕様・ポリシー・スケジュール等は変更される可能性がありますので、最新情報をご確認ください。