SSL/TLS証明書有効期限短縮に伴うEDIへの影響
2026年1月版

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

はじめに

JiEDIA

本資料は、EDIを利用しているユーザー企業ならびにEDIサービス/EDI関連事業を提供しているVAN/ASP/SI事業者の方を対象としています。

※本資料の取扱いについて

本資料は原則公開可能としますので、貴社顧客説明やセミナ等においてご利用ください。ただし、内容の改変は厳禁とさせていただきます。
また、本資料の一部を引用する場合は、
「SSL/TLS証明書有効期限短縮に伴うEDIへの影響　20XX年X月版（インターネットEDI普及推進協議会）」
を明記ください。

なにが起こるのか？

JiEDIA

認証局やWebブラウザを提供している主要企業で構成される「CA/Browser Forum」において、以下が決定されました。

1.パブリック証明書の有効期限短縮

パブリック証明書（SSL/TLS証明書）の有効期間が段階的に短縮され、
2029年3月15日以降に発行される証明書は「最大47日」になります。

また、Google社の「Chrome Root Program Policy」において、セキュリティ強化の一環として証明書の用途を分離する方針が発表されました。

2.サーバ証明書とクライアント証明書の兼用禁止

パブリック認証局（CA）が発行するサーバー証明書（TLS/SSL証明書）にクライアント認証の機能を含めることが段階的に禁止されます。
これは「兼用の禁止」を意味する措置であり、
2026年6月15日以降に完全適用される予定です。

※本資料の内容は、2025年12月1日時点で入手可能な証明書関連の動向に基づいています。
今回のルール改訂はパブリック証明書を対象としており、プライベート証明書は現時点では対象外です。ただし、将来的にプライベート証明書にも影響が及ぶ可能性がありますので、注意が必要です（詳細は後述）。

移行スケジュール

JiEDIA

1.パブリック証明書の有効期限短縮

移行スケジュールは以下となります。

運用開始日	最大有効期間
～ 2026年3月14日	398日（約13ヶ月）
2026年3月15日～	200日
2027年3月15日～	100日
2029年3月15日～	47日

2.サーバ証明書とクライアント証明書の兼用禁止

このルールはすでに段階的に適用が始まっています。

・2025年後半以降

多くの認証局において、新規に発行されるサーバ証明書に「clientAuth」がデフォルトで含まれなくなります。

・2026年6月15日以降

Google Chromeが信頼するパブリック認証局においては、「clientAuth」を含むサーバ証明書を新規に発行することができなくなります。

ルール改訂の背景

JiEDIA

今回のルール改定は「セキュリティ強化」を目的としたものです。
具体的には以下の点が挙げられます。

1.パブリック証明書の有効期限短縮

・侵害リスクの低減
　秘密鍵が万一漏洩した場合でも、有効期間が短いため攻撃者が不正利用できる時間が大幅に制限されます。これにより、フィッシングサイトや中間者攻撃などのリスクが軽減されます。
・最新技術への迅速な対応
　新しい暗号化アルゴリズムやより安全な技術が登場した際、証明書の有効期間が短いことでエコシステム全体が速やかに移行しやすくなります。
・ドメイン正当性の担保
　証明書の更新頻度が高まることで、ドメイン所有者の正当性を確認する機会が増え、不正な証明書発行を防止しやすくなります。

2.サーバ証明書とクライアント証明書兼用禁止

・セキュリティリスクの低減
　サーバー用とクライアント用の証明書を兼用すると、秘密鍵漏洩時の被害が広範囲に及ぶ懸念がありました。用途を分けることで、インシデント発生時の影響を限定できます。
・エコシステムの健全化
　証明書の発行ルール（ポリシー）は、サーバー認証・クライアント認証・S/MIMEなどそれぞれ異なり、一枚の証明書に複数の用途を持たせると、最も緩いルールが悪用される懸念がありました。用途を分離することで、それぞれに適切なセキュリティポリシーを適用でき、全体の健全性が向上します。

今後の影響

今回のルール改定による最も大きな影響は、証明書運用管理の負荷増加にあります。
具体的には以下の点が挙げられます。

・更新頻度の増加
　証明書管理の運用サイクルが短縮されるため、証明書更新作業の頻度が大幅に増加する可能性があります。これまで1年に1回だった更新作業が、将来的には年に約8回（47日ごと）必要になります。手動での更新作業は、管理する証明書の数が少なくても現実的ではありません。

・サービス停止リスクの増大
　証明書の更新を忘れると、Webサイトに「保護されていない通信」といった警告が表示され、ユーザーがアクセスできなくなります。これはビジネスの機会損失や信用の低下につながります。

・用途ごとの証明書分離
　サーバ認証用とクライアント認証用を兼用している場合、証明書を明確に分けて運用する必要があります。

・システム設定／運用設計の見直し
　認証局やブラウザベンダーの対応スケジュールに従い、既存システムの証明書設定や運用設計を見直すことが求められます。

想定される影響範囲

JiEDIA

今回のルール改訂により影響を受けるサービスやシステムは多岐に渡ることが想定されます。
一例を以下に記載します。

・自社ホームページ
　SSL/TLS証明書の更新が必要で、更新が遅れるとブラウザ上で「安全ではないサイト」と表示される可能性があります。

・顧客向けサイト
　会員ログインやお問い合わせフォームなど、SSL/TLS通信を利用する機能に影響が出る可能性があります。

・ECサイト
　HTTPS接続や決済サービスとの通信に影響し、証明書切れにより顧客が購入できなくなるリスクがあります。

・EDI
　EDIサービスや外部取引先との通信で利用されるSSL/TLS通信に影響し、接続障害が発生する可能性があります。

EDIへの影響①

JiEDIA

1.EDI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。

2.EDI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。

EDIへの影響②

JiEDIA

2.EDI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、ユーザーとサービス事業者間で証明書の受け渡しが47日ごとに発生することになり、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47日ごとに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。

EDIへの影響③

JiEDIA

3.Web-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でSSL/TLS通信を行っている場合、将来的にブラウザ側で接続拒否されることが予想されます。

（段階的に「警告表示 → 接続遮断」へ移行する可能性があります。）

対応方針

JiEDIA

■全企業共通

1.自社で利用している証明書の洗い出し

まず、自社で利用している証明書の一覧を洗い出し、「パブリック証明書」か「プライベート証明書」かを確認してください。

1-1.パブリック証明書の場合

自社システム部門、開発/運用委託先、認証局事業者を含めて、対応方針を検討してください。

1-2.プライベート証明書の場合

今回のルール改訂はパブリック証明書が対象であり、プライベート証明書は基本的に対応不要です。ただし、将来的にパブリック証明書に準じた運用に移行する可能性があること、また取引先から「プライベート証明書でセキュリティは十分か？」といった問い合わせが入る可能性があるため、理論的な説明準備を検討してください。

1-3.不明の場合

自社システム部門、開発/運用委託先、認証局事業者などに確認してください。

■EDIサービス事業者・通信製品ベンダなど

2.自社サービス/通信製品で利用している証明書の洗い出し

自社サービス/通信製品で利用している証明書について「パブリック証明書」か「プライベート証明書」かを確認してください。

顧客からの依頼で取り込んでいる証明書も併せて確認してください。

3.調査結果を元に、対応方針を検討してください。

併せて、自動更新プロトコル「ACME」への対応も検討してください。

補足

JiEDIA

・ACMEとは
「Automated Certificate Management Environment」の略称で、Webサーバやサービスで利用するSSL/TLSサーバ証明書を自動的に発行・更新・管理するためのプロトコルです。「Let's Encrypt」などで利用されています。
クライアント証明書には対応していません。

・JiEDIAでは、クライアント証明書の「電子証明書自動更新API利用ガイドライン」を公表しております。詳細は以下URLからご参照ください。
https://www.jisa.or.jp/jiedia/tabid/2822/Default.aspx

・JiEDIA認証局認定制度で電子証明書発行サービスとして認定している株式会社INTECが発行しているプライベート証明書（EINS/PKI for EDI）について、現状（3年間）のままで特に有効期限短縮やACME対応の予定はありません。
※ただし、世の中の動向や利用業界の要望を受けて今後検討予定。
※JiEDIA認証局認定制度の詳細は以下URLからご参照ください。
https://www.jisa.or.jp/jiedia/tabid/2822/Default.aspx

SSL/TLS証明書有効期限短縮に伴うEDIへの影響

2026年1月　発行

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