電子証明書自動更新 API 利用ガイドライン

概要説明版

V1.0.0

インターネット EDI 普及推進協議会

Japan internet EDI Association (JiEDIA)

目　次

1. 要旨

1.1. はじめに

東日本電信電話株式会社ならびに西日本電信電話株式会社より、2024 年から 2025 年にかけて公衆電話回線網（PSTN）を IP 網に移行する方針が発表された。これに合わせて EDI 用途でも広く利用されている「INS ネットディジタル通信モード（ISDN)」もサービス提供終了が発表されており、各業界団体においてはインターネットを介した通信プロトコルの導入が検討されている。

インターネット EDI 普及推進協議会（JiEDIA）では、各業界の取り組みを尊重しながら連携を図り、継続的なインターネット EDI 普及推進に寄与することを基本方針として活動を行っている。このたび、「インターネット EDI 導入に伴う証明書運用の負荷軽減」という視点から検討を行った。

1.2. ガイドライン作成の背景と目的

インターネットを利用して EDI を行うためにはセキュリティ対策が重要であり、現在は電子証明書を利用することが一般的である。しかしながら、ユーザー企業にとって証明書の運用は難易度が高いため、現実問題として証明書発行から通信製品設定まで、手厚いサポートが必要となってくる。証明書には必ず有効期限が存在することから、実運用においては発行時だけでなく、定期的な更新時にも更新忘れや適用作業ミスといったトラブルの発生も懸念される。また、インターネット EDI 通信製品は市場に多数存在するが、証明書を含むセキュリティ関連の運用が多様で、ユーザー企業や VAN 事業者が機能差を吸収するケースも確認されている。

今後、各業界団体で対応方針の検討が行われるものと考えるが、インターネット EDI への安定かつ円滑な移行の一助となるよう、JiEDIA は証明書発行（更新）機能を API 化することにより、ユーザー企業および SI 事業者双方の作業負担低減を図るとともに証明書を含むセキュリティ運用機能を標準化することで、相互接続性の向上と運用上のトラブルを回避する目的で本ガイドラインを作成した。

本書の内容は逐次改定を加える予定である。本書を引用する場合は、

「出典：電子証明書自動更新 API 利用ガイドライン 概要説明版　VX.X.X（インターネット EDI 普及推進協議会)」と出典を明記していただきたい。

1.3. 適用範囲

本ガイドラインは証明書発行（更新）機能の API 化に対して補完するものであり、その他の証明書のライフサイクル管理については基本的に言及しない。特に、証明書の失効については本ガイドラインの対象外とする。

また、本ガイドラインは証明書発行（更新）機能の実装・利用にあたっての概要を説明し、

具体的な API の実装方法については、詳細版のガイドラインで説明する。

1.4. 本ガイドラインが対象とする範囲と想定する読者

本ガイドラインはインターネット EDI への移行促進に関わる証明書認証局機能を有する企業ならびに、インターネット EDI 手順を利用してシステムを構築・運用する企業向けに記載する。

1.5. 用語

本ガイドラインで記載する HTTP リクエスト／レスポンスのデータ構造は以下の通りとする。

リクエスト	メソッド	リクエスト対象	HTTP バージョン
	リクエストヘッダ		
	リクエストデータ		

図表 1　HTTP リクエスト構造

レスポンス	HTTP バージョン	ステータスコード
	レスポンスヘッダ	
	レスポンスデータ	

図表 2　HTTP レスポンス構造

2. 概要

2.1. 証明書自動発行・更新の仕組み

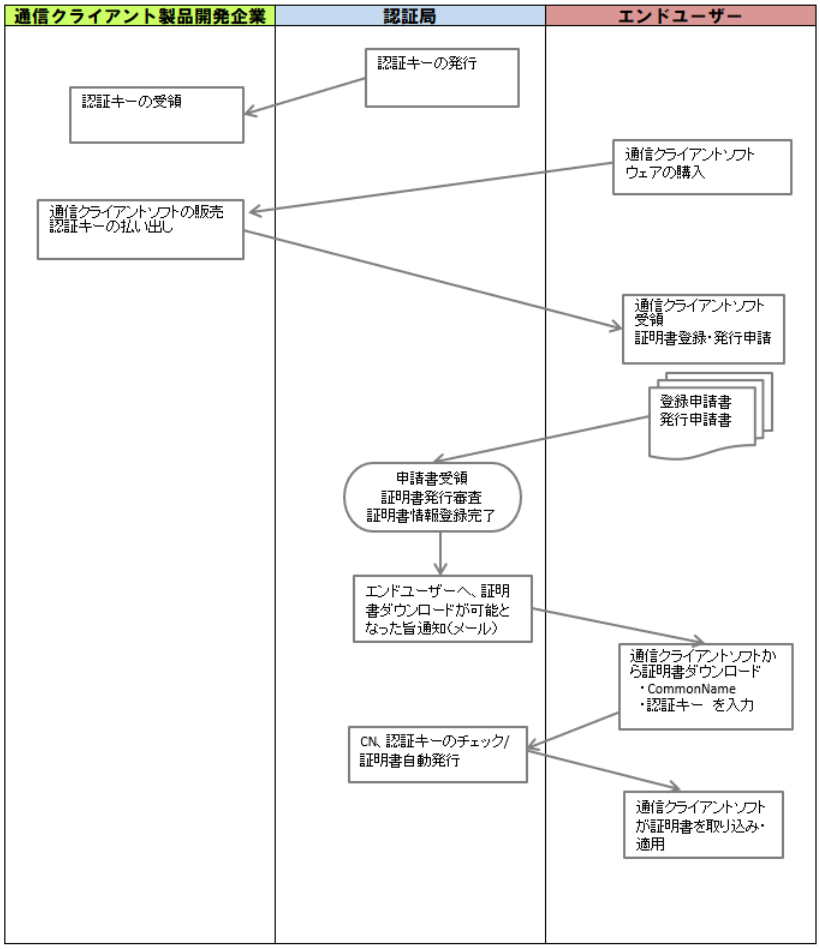
証明書自動発行・更新は、認証局で自動発行・更新用の API（Web ベース）を公開して実現する。

通信クライアントは、認証局の定めた API インタフェースに従って証明書発行・更新要求を送信し、認証局側で発行された証明書を製品に取り込む。

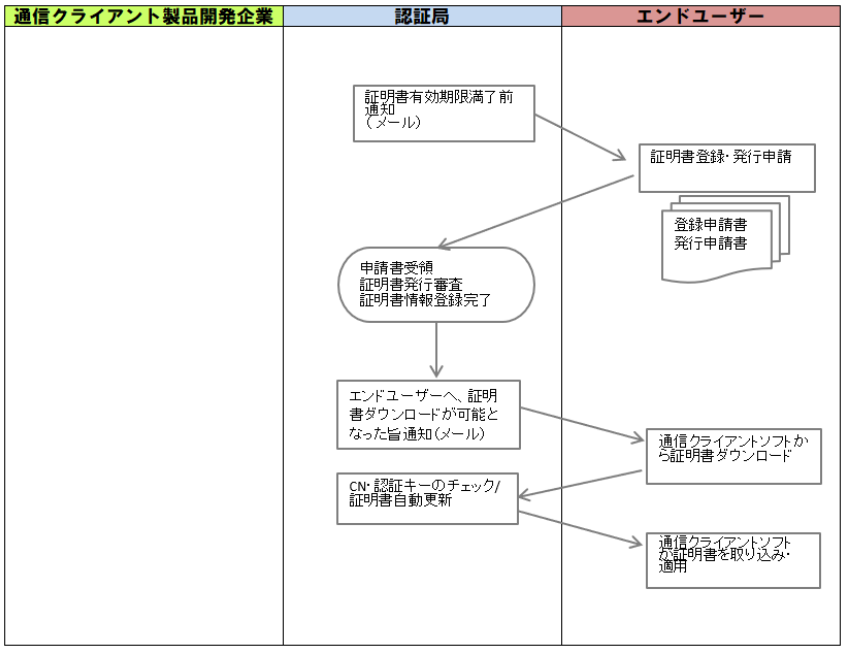
証明書自動発行・更新にあたり、認証局ベンダは従来のデータ交換認証局運用規定（CPS）に則って、証明書発行審査を実施する。

2.2. 運用フローモデル

証明書自動発行・更新の運用フローモデルは以下の通りとなる。



図表 3　証明書発行運用フロー



図表 4　証明書更新運用フロー

3. 認証局実装ガイドライン

3.1. 認証局側の仕様概要

認証局側では、証明書の新規発行と更新発行の API を用意する。

新規発行時、更新発行時に通信クライアントから送信されるリクエストデータは以下のとおりとする。

項目	項目説明	例
CommonName	発行される証明書の CommonName	user1
認証キー	認証局から事前に払い出したランダムな文字列で、証明書発行時の認証で利用 ※通信クライアント製品開発企業側では、新規証明書発行処理以降においては、本認証キーを保持・管理し続けなくとも良い	XXXX12345678
証明書更新時パスワード	証明書更新時に使用するパスワード	Passw0rd1
PKCS#12 パスワード	発行される PKCS#12 形式証明書の保護パスワード	p12Pass

図表 5　証明書新規発行リクエストデータ

項目	項目説明	例
証明書更新時パスワード	証明書更新時に使用するパスワード	Passw0rd1
PKCS#12 パスワード	発行される PKCS#12 形式証明書の保護パスワード	p12Pass

図表 6　証明書更新リクエストデータ

認証局側で証明書発行後、通信クライアントに送信されるレスポンスデータは以下のとおりとする。

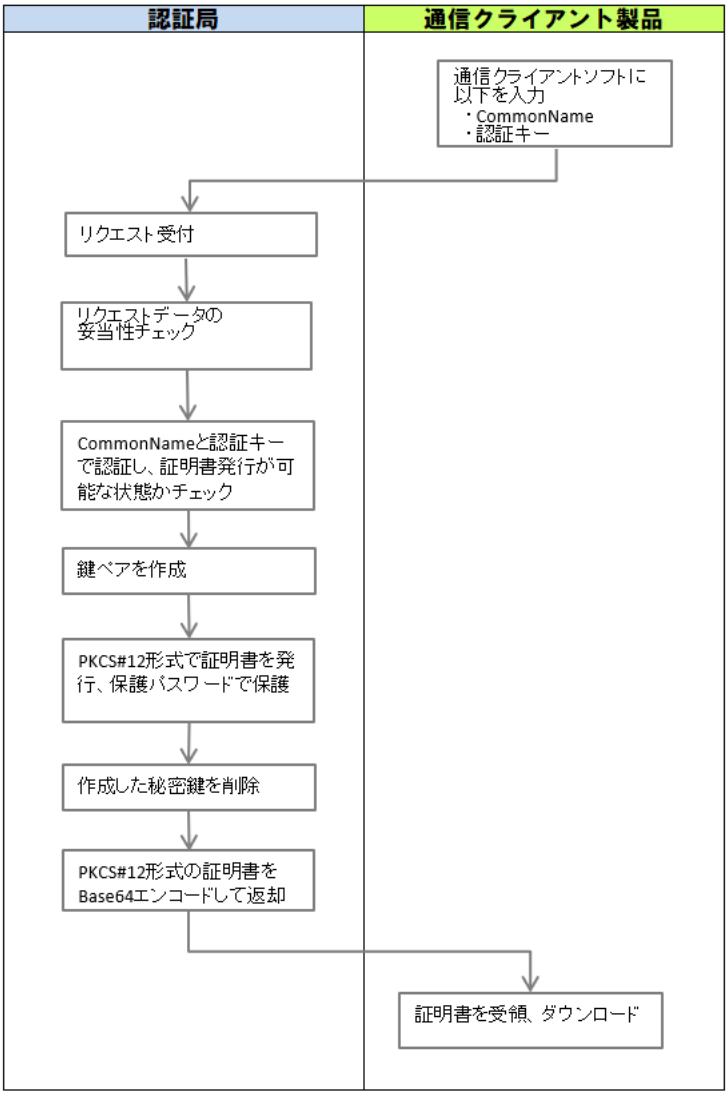
項目	項目説明	例
処理ステータスコード	証明書発行・更新処理結果 -正常終了：0 -エラー終了：0 以外の値	0 1111
証明書	発行された PKCS#12 形式証明書（認証局証明書とクライアント証明書を含む）を Base64 エンコードした値	MIIK・・・IAA==

図表 7　証明書発行・更新レスポンスデータ

なお、リクエストデータのデータフォーマットやレスポンスデータの処理ステータスコードについては、詳細版のガイドラインで説明する。

3.2. 詳細処理フロー

認証局側では以下のフローで証明書を発行する。



図表 8　証明書発行詳細処理フロー

3.3. エラー処理

証明書発行処理でエラーが発生した場合、通信クライアント側に処理ステータスコードとして 0 以外のエラーコードを返却する。

エラーコードは認証局側の API 仕様に準じ、代表的なエラー内容は以下のとおりとする。

・　証明書発行リクエストデータに設定した値の文字列長、使用可能文字などのフォーマットエラー
・　証明書発行リクエストデータに設定した CommonName、認証キーで証明書発行審査が完了していない
・　証明書更新可能期間外で証明書更新処理を実施した
・　使用済みの認証キーで証明書発行・更新処理を実施した

3.4. 運用管理

認証局側では以下の運用管理機能を備えることが望ましい。

・　同一利用者に対して複数の証明書を発行できる。
・　証明書発行（更新）API の実行日時・結果が記録できる。
・　新規取得証明書・更新取得証明書をオーバーラップして発行することができる。
・　認証局で定める通常の発行手順(Web 画面からダウンロード等)とは別に証明書発行(更新）API で証明書を取得することができ、何らかの方法で、どれが証明書発行（更新）API で取得した証明書であるかを特定できる。
・　証明書更新 API 実行時に、発行済み証明書で SSL/TLS クライアント認証を実施し、証明書の有効期限切れ等のクライアント認証エラー時にはレスポンスコード「403」を返却できる。
・　証明書有効期限満了前に利用者に対して証明書有効期限満了前である旨通知できる。

3.5. サーバ環境維持に置いて留意すべきこと

認証局側のサーバ環境の維持にあたり、以下のセキュリティ機能を備えることが望ましい。

・　通信経路を SSL/TLS で暗号化し、盗聴を防止する
・　証明書発行要求時に認証局から払い出されたランダムな文字列で認証を行い、なりすましを防止する
・　認証局側には IPS/IDS を導入して侵入検知などの対策を講じておくことが望ましい

4. 通信クライアント実装ガイドライン

4.1. クライアント側仕様概要

通信クライアント側では、証明書の新規発行と更新発行の API を用意する。通信クライアント側は常にリクエスト発行側となり、リクエスト受信側（サーバ）にはならない。

新規発行・更新発行では、発行に必要な情報を認証局側の仕様で定められたリクエストデータとして送信し、発行された証明書を認証局側の仕様で定められたレスポンスデータの形式で受信する。レスポンスデータとして受信した証明書を、通信クライアントに組み込んでインターネット EDI 通信で使用する。

認証局との通信方式は、認証局側の仕様に則る。また、新規発行・更新発行の通信に使用する認証局の証明書発行システムのサーバ証明書は、通信クライアントにあらかじめ登録しておく必要がある。

API の実行トリガーは、通信クライアント側で任意に決定してよい。利用者による手動実行・EDI 通信と同時に自動実行などの方法が考えられる。ただし、更新発行については、通信クライアント起動時に証明書の有効期限を確認し、有効期限満了間近の場合に、EDI 通信を行う前に証明書を自動で更新する機能を備えることが望ましい。

証明書の新規発行・更新発行の可否については、基本的に認証局側で検証が行われる。しかし、更新発行については、以下の内容については通信クライアント側でも検証可能であるため、リクエスト発行前に検証を行うことが望ましい。

検証事項	補足
更新発行を行う認証局から､API で新規発行を行っているか	API で新規発行を行っていない場合、認証局側で更新リクエストがエラーになる。
更新対象の証明書が、更新可能期間に達しているか	更新可能期間は、認証局によって異なる。期間に達していない場合、認証局側で更新リクエストがエラーになる。
更新対象の証明書の有効期限が切れていないか	更新のリクエストは、更新対象の証明書で SSL/TLS クライアント認証を実施するため、有効期限が切れている場合は認証局への接続でエラーになる。

図表 9　証明書更新発行での通信クライアント側検証事項

通信クライアント側で取得した証明書は、通信ソフトが複数種類存在する場合、それらで共通利用してもよい。証明書発行（更新）機能の API を有さない通信ソフトでの利用も可能とする。ただし、複数の通信クライアントからの更新発行の要求は認めない。更新発行はい

ずれか１つの通信クライアントから実行する必要がある。

4.2. 処理フロー

通信クライアント側では以下のフローで API を実行する。

4.2.1　　新規発行処理フロー

① 新規発行に必要な項目について、利用者からの入力を受け付ける。方法は任意。（画面、設定ファイルなど）

② 認証局の新規発行用 API に対して、証明書新規発行リクエストを送信する。

③ 認証局からの証明書新規発行レスポンスを受け取る。

④ レスポンスから証明書データを取り出し、通信クライアントに設定する。
受け取った証明書データは、通信クライアント以外にも保管しても良い。（ファイルに保存するなど）
また、レスポンスの証明書データに含まれる CA 証明書も通信クライアントに設定することが望ましい。

4.2.2　　更新発行処理フロー

① 更新発行に必要な項目について、利用者からの入力を受け付ける。方法は任意。（画面、設定ファイル保持など）

② 新規取得した証明書が更新可能かどうかを検証することが望ましい。ただし、クライアント側で検証しない場合も、条件を満たしていなければ認証局側でエラーとなるため、必須ではない。

③ 認証局の更新発行用 Web サービス受付 URL に対して、証明書更新発行リクエストを送信する。この際、新規発行した証明書をクライアント認証証明書として提示する。

④ 認証局からの証明書更新発行レスポンスを受け取る。

⑤ レスポンスから証明書データを取り出し、通信クライアントに設定する。
通信クライアントの設定で、接続相手先ごとに使用する証明書を指定している場合、設定を編集する必要なくこの更新処理だけで使用証明書を自動的に変更することが望ましい。
インターネット EDI 通信に使用する証明書は、証明書の更新成功後に直ちに変更しても、変更日時を指定して後日変更してもよい。ただし直ちに変更しない場合、旧証明書の有効期限が切れるまでには必ず変更すること。
受け取った証明書データは、通信クライアント以外にも保管しても良い。（ファイルに保存するなど）

4.3. エラー処理

通信クライアント側で発生するエラーを、以下の三種に分けて記載する。

4.3.1　　認証局への接続前に発生するエラー

認証局への接続前にエラーが発生した場合、通信クライアント側の設定やネットワーク環境に問題がある可能性が高いため、エラー内容に応じてそれらを確認する。

また、認証局への接続前のエラーに対しては、リトライが可能であること・タイムアウト時間が設定可能であることが望ましい。

代表的なエラー例を以下に記載する。

エラー種類	原因	対処法
接続エラー	社外のインターネット環境に接続できない。	ネットワーク設定を確認する。プロキシを使用している場合、プロキシの設定を確認する。
SSL 認証エラー	認証局に接続するためのサーバ証明書が正しく設定されていない可能性がある。	認証局に接続するためのAPIのサーバ証明書の設定を見直す。
HTTP レスポンスコード 404	接続 URL が間違っている。	接続 URL を確認する。
HTTP レスポンスコード 5XX	認証局のシステムに何らかの問題が発生している可能性がある。	認証局に確認する

図表 10　認証局への接続前に発生するエラー例

4.3.2　　認証局から返却されるエラー

認証局への接続後、レスポンスでエラーが返却された場合、認証局のエラーコード仕様を確認して、各対処法を実行する。

なお、リトライしても解消する見込みのないエラーの場合は、通信クライアントは無駄にリトライを行わないことが望ましい。

例)「更新要求で、更新対象の証明書の有効期限が切れている」というエラーの場合など

4.3.3　　認証局から証明書を取得後に発生するエラー

認証局から証明書を取得後にエラーが発生した場合、通信クライアント側の内部処理で問題が起こった可能性が高いため、エラー内容に応じてそれらを確認する。

また、これらエラーについては、認証局側の発行処理は正常終了しているため、エラーリカバリ処理には注意が必要である。基本的には通信クライアント側だけでリカバリを行い認証局へのリクエスト送信は再実行しないことが望ましい。どうしても通信クライアント

側だけでのリカバリが不可能な場合は、認証局に連絡の上、リクエスト送信再実行のための調整を行う必要がある。

代表的なエラー例を以下に記載する。

エラー種類	原因	対処法
取得証明書保存エラー	何らかの理由により、取得した証明書データを保存する処理が失敗した。	認証局側の証明書の発行は完了しているため、クライアント側だけでリカバリできる方法を設けて、利用者がそれを実行することが望ましい。 どうしても証明書の再発行が必要な場合は、認証局に連絡して対処する。
取得証明書のパスワード解除エラー	パスワード解除に使用したパスワードと、認証局が証明書発行時に暗号化で使用したパスワードが不一致。	パスワード解除に使用したパスワードが間違っている可能性があるため、確認して、再度解除を試みる。
取得証明書登録エラー	何らかの理由により、取得した証明書を通信ソフトに新規登録・更新する処理が失敗した。	認証局側の証明書の発行は完了しているため、クライアント側だけでリカバリできる方法を設けて、利用者がそれを実行する。

図表 11　認証局から証明書を取得後に発生するエラー例

4.4. 運用管理機能

通信クライアントでは以下の運用管理機能を備えることが望ましい。

- 証明書発行（更新）API の実行日時・結果が記録できる。
- 証明書発行（更新）API で取得した証明書以外の証明書も、登録することができ、混在して使用できる。何らかの方法で、どれが証明書発行（更新）API で取得した証明書であるかを特定できる。
- 取得した証明書を、紛失に備えて、何らかの方法でバックアップすることができる。
- 新規取得証明書・更新取得証明書をオーバーラップして登録することができる。
- 通信クライアントの設定で、接続相手先ごとに使用する証明書を指定している場合、その証明書の更新を行うと、接続相手先の設定で使用する証明書を指定しなおす必要なく、使用証明書を自動的に変更することができる。
- 更新発行について、証明書の有効期限・認証局の更新可能期間と連動して、自動で実行

することができる。

4.5. クライアント環境の維持に必要なもの

通信クライアントでは、以下の環境を維持する必要がある。

- インターネットに接続でき、認証局の URL に接続可能なネットワーク環境
- 認証局の証明書発行システムのサーバ証明書

5. 接続試験

5.1. 試験の目的

新規に参入する通信クライアント製品開発企業ならびに認証局構築企業において、事前に相互接続性確認を目的とした相互接続試験を行うことが望ましい。

5.2. 試験の実施方法

相互接続試験の実施にあたり、すでに参入済みの通信クライアント製品開発企業ならびに認証局構築企業は、以下の通り相互接続試験に協力することが望ましい。

○ すでに参入済みの認証局構築企業から新規参入する通信クライアント製品開発企業に対する協力
- 詳細通信仕様の提供
- 相互接続試験環境の提供

○ すでに参入済みの通信クライアント製品開発企業から新規参入する認証局構築企業に対する協力
- 新規参入認証局構築が提供する相互接続試験環境に対する通信可否

改訂の要約

・V1.0.0（2021 年 4 月公開）作成

- 新規作成

電子証明書自動更新 API 利用ガイドライン

概要説明版

2021 年 4 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