商業登記電子証明書及び認証局の移行について

法務省民事局商事課
デジタル庁

２０２５年1月１０日

商業登記電子証明書

法務省：商業登記に基づく電子認証制度

http://www.moj.go.jp/ONLINE/CERTIFICATION/GUIDE/guide03.html

概要（抜粋）：

従来、企業取引等においては、取引相手方の「本人性」、「法人の存在」、「代表権限の存在」を確認するための信頼性の高い手段として、登記所が発行する印鑑証明書・登記事項証明書が広く利用されてきたところですが、「商業登記に基づく電子認証制度」（以下「電子認証制度」といいます。）は、これらの証明書に代わって、電子的な取引社会において用いられる証明として、法人の登記情報に基づいて「電子証明書」を発行する制度です。

例えば、ある会社の代表者が電子署名を行った電子文書を送信する際に、この電子証明書を併せて送信すれば、これを受信した相手方は、その送信者の電子証明書に表示（記録）された会社の商号、本店、代表者の資格・氏名に関して、その時点での登記情報に変更が生じていないか（これらを変更する登記がされていると、その電子証明書は無効とされます。）等について、インターネットを通じて確認することができます。

これにより、電子申請のほか、電子取引等の場面においても、従来の文書による取引と同様に、相手方の「本人性」、「法人の存在」、「代表権限の存在」等を確認することができることとなります。

商業登記電子証明書の利用場面

1. 行政手続の電子申請に利用
2. 電子契約や会社が発行する文書への署名に利用

商業登記電子証明書が利用可能な行政手続の例	
登記・供託オンライン 申請システム	商業・法人登記 / 不動産登記 / 動産・債権譲渡登記 / 成年後見登記 / 供託 / 電子公証　のオンライン申請
	印鑑証明書のオンライン請求
e-Tax（国税電子申告・納税システム）	
eLTAX（地方税電子申告）	
社会保険・労働保険関係手続	
特許のインターネット出願	
自動車保有関係手続のワンストップサービス	
総務省 電波利用 電子申請・届出システム	
防衛装備庁 電子入札・開札システム	
オンラインによる支払督促手続（督促手続オンラインシステム）	
府省共通の電子調達システム(GEPS)	
電子自治体における各種の申請・届出システム	

商業登記電子証明書の利用システムに該当するケース

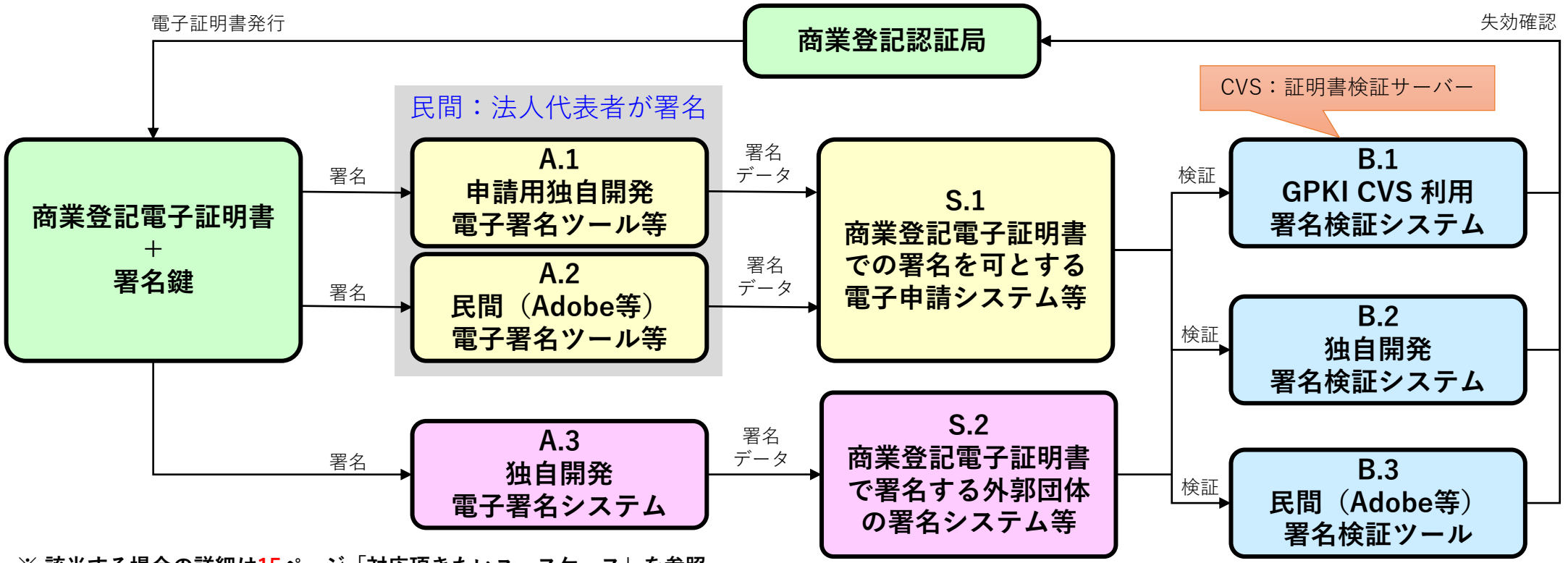
S.1 商業登記電子証明書での署名を認めている電子申請システム等（申請者が署名している場合）

電子申請データに対して、商業登記電子証明書による電子署名を行うことを認めているシステム

S.2 商業登記電子証明書での署名を認めている外郭団体の署名システム等（サーバーで署名している場合）

一般財団法人等の外郭団体にて、商業登記電子証明書による電子署名を行うことができるシステム

※ GPKIの電子証明書を利用中の場合は対象外です（GPKIは検証時利用なので署名時は該当しません）。



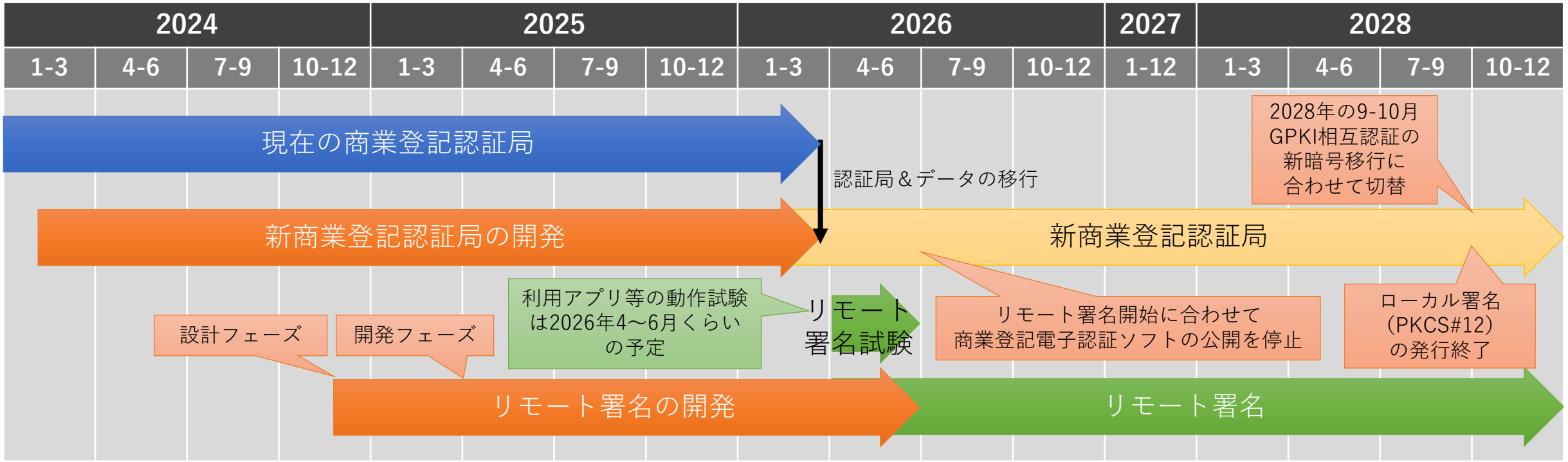
※ 該当する場合の詳細は15ページ「対応頂きたいユースケース」を参照。

商業登記電子証明書と認証局の移行

1. スケジュール
    1. 2026年3月末に認証局は新システムへ移行し、新商業登記電子証明書の発行と利用が開始される予定です。
    2. 2026年7月からリモート署名が新たに利用可能となる予定です。
2. 新システムの概要
    1. 移行前に発行された現商業登記電子証明書（PKCS#12ファイル形式）は、有効期間内（最大2年3ヶ月）であれば移行後も有効です。
    2. 新システムへの移行後も、2028年の新暗号方式への対応までの間は、現商業登記電子認証ソフトで生成されたローカル署名（PKCS#12ファイル形式の提供）と、リモート署名（オンラインでの提供）の両方が利用可能です。ただし、~~2028年の新暗号方式への対応までにリモート署名への移行を促進するため、~~リモート署名開始と同時に、商業登記電子認証ソフトの法務省のホームページでの提供及び同ソフトのサポート（問合せ対応）は停止する予定です。
    3. 新商業登記電子証明書においても従来通りGPKI相互認証を行います。
    4. 新商業登記電子証明書では以下の2点が変更となります。
        1. 電子証明書の検証について、既存のOCSP方式に加え、CRL方式が利用可能となります。
        2. 鍵の利用用途（keyUsage）が追加されます。
3. リモート署名の概要
    1. リモート署名用の商業登記電子証明書の発行には専用ポータルサイトを用意します。
    2. 利用にはGビズIDプライムまたはエントリー（即時発行可能）以上が必要となります。
    3. 登記ねっとによる電子証明書の発行申請手順に変更はありません。
4. 民間で提供しているICカード格納サービスは移行後も利用可能となる予定です。
5. 新システムへの移行に伴い、現在商業登記電子証明書を利用中のシステムでは、署名付与と署名検証のプロセスにおいて新たに対応が必要となる場合があるため、ご確認願います。

※ 本資料は開発ベンダー等へ共有いただいて問題ありません。
※ 必要に応じて個別の打合せに対応いたします。

新商業登記電子証明書の移行スケジュール



1. 現在の商業登記認証局からの電子証明書発行は**2026年3月末を目途に新商業登記認証局に切り替え**ます。
2. 新商業登記認証局への切替後もローカル署名（PKCS#12ファイル形式）の発行が可能※ですが、
   リモート署名開始と同時に、商業登記電子認証ソフトの公開及び同ソフトのサポートを停止する予定です。
   ※　2028年の新暗号移行まで
3. 新商業登記電子証明書を使った電子署名アプリの動作試験は2026年4～6月頃から可能となる予定です。
   - リモート署名開発の調達後に開発ベンダーより正確な日時が決まりますので決まり次第お知らせします。
4. 2028年末に新暗号移行を予定していますが新暗号移行によるリモート署名の仕様に変更はありません。
   - 独自検証をしている場合には新暗号への対応は2028年末までに対応が必要となります。

新商業登記電子証明書では何が変わるのか？

変更１（署名）：署名方式をローカル署名（ファイル発行）からリモート署名に順次移行

- リモート署名では署名鍵はローカル保持からサーバー（リモート）保持に変更されスマホ認証（GビズID）により利用します。
- 署名鍵はサーバーの安全な場所（ハードウェア/HSM）に保管されており紐づいた利用者以外は管理者でも利用できません。

利用方法１：仮想ICカード署名ドライバ（仮想ローカル署名）をWindows PC用に提供します（ツールの変更が必要）。
利用方法２：外部署名サービスとの連携も可能です（外部署名サービス側の対応が必要です）。
注１：署名認可が必須となるのでサーバー自動署名（eシール的利用）には対応できなくなります。
注２：現在のローカル署名方式の証明書は2028年の新暗号移行まで発行可能ですが商業登記電子認証ソフトの公開が停止となる予定です。

変更２（検証）：認証局のモダナイズ化で検証時の利便性を向上

- 有効性確認の為にOCSP（有効性確認）に加えてCRL（失効リスト）による検証も可能となります。

注３：2028年末までにGPKIと共に暗号方式を新暗号（RSA 3072bitsかECDSA P-256以上）へ移行予定です。

変更３（発行）：商業登記電子認証ソフトから商業登記電子認証ポータルへ移行

- リモート署名では商業登記電子認証ポータル（以下、認証ポータル）上で発行手続きを行います。
- 認証ポータルへのログインにGビズIDエントリー以上のID取得が必要です。GビズIDエントリーはメールアドレス登録で即日発行可能です。

継続１：GPKIとの相互認証は従来通り維持

- GPKIのCVS（証明書検証サーバー）にて有効期間内の現電子証明書も新電子証明書もどちらも検証が可能です。

継続２：民間ベンダーのICカード発行サービスは従来通り利用が可能

- 既存の民間ベンダーのICカード発行サービスにおける申請手順に変更はありません。

継続３：従来通り法務局窓口か登記・供託オンライン申請システムから申請（小変更あり）

小変更：リモート署名に関する事前準備の鍵ペア生成は、オンラインの認証ポータルからとなります。

- 既存のSHINSEIファイルを用いた商業登記電子証明書の発行手順に変更はありません。

なぜリモート署名化するのか？

1．署名鍵の安全性の向上が目的

- 現在提供しているPKCS#12ファイル形式では署名鍵がソフト的に格納されているので安全性が低いと言う問題がありました。解決策はICカード化かリモート署名化でした。

※ ICカード化しない理由

- ICカード化は物理媒体の配布となりオペレーションが複雑になりコストの問題もあります。
- 民間サービスとしてICカード格納は提供済みであり新規に採用する意味が低いと言えます。

※ リモート署名化する理由

- サーバー側のHSMと言う専用ハードウェアに署名鍵を格納するので安全性を高くできます。
- 要件さえ遵守すればICカードと同等の安全性を実現できます（海外でも実績あり）。
- 物理媒体を必要とせずスマホ認証アプリのみが必要なので利用コストも低減できます。

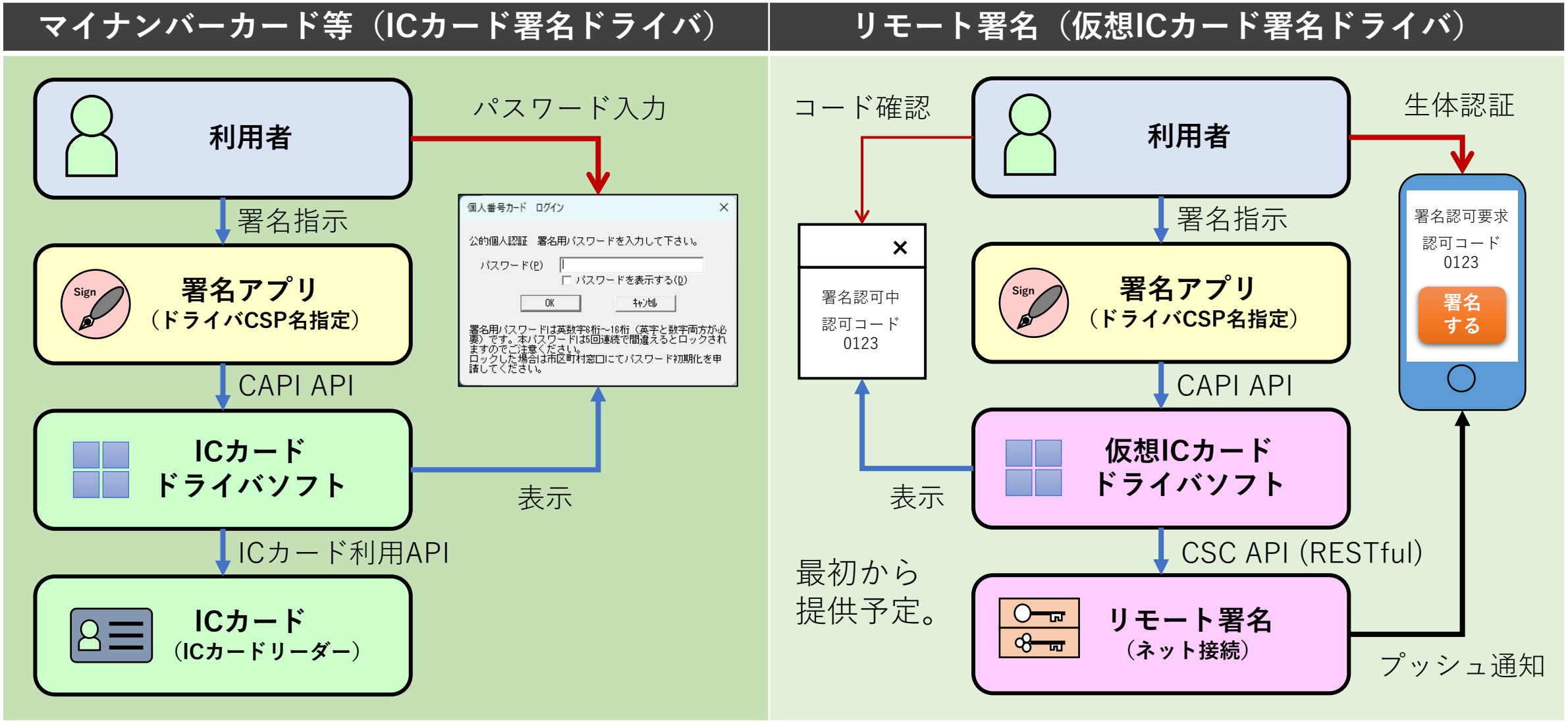
2．仮想ICカード署名ドライバの利用でローカル署名として利用も可能

- ネット接続環境ではICカード利用のローカル署名と同じ利用方法での署名処理が行えます。

3．各種クラウドサービスとの連携での利用も可能（将来）

- リモート署名の仕様はCSCにて業界標準化されており今後の普及が見込まれています。
- 電子申請サービスや電子契約サービスがCSC標準に対応することで、直接連携できるようになるとブラウザから直接署名処理（署名値の計算）を行うことが可能となります。
- Windows環境だけでは無くMacOS/Linux/スマホから利用も可能となります。

利用方法１：仮想ICカード署名ドライバ



仮想ICカード署名ドライバの利用

CAPI：CryptSignHash署名APIの利用

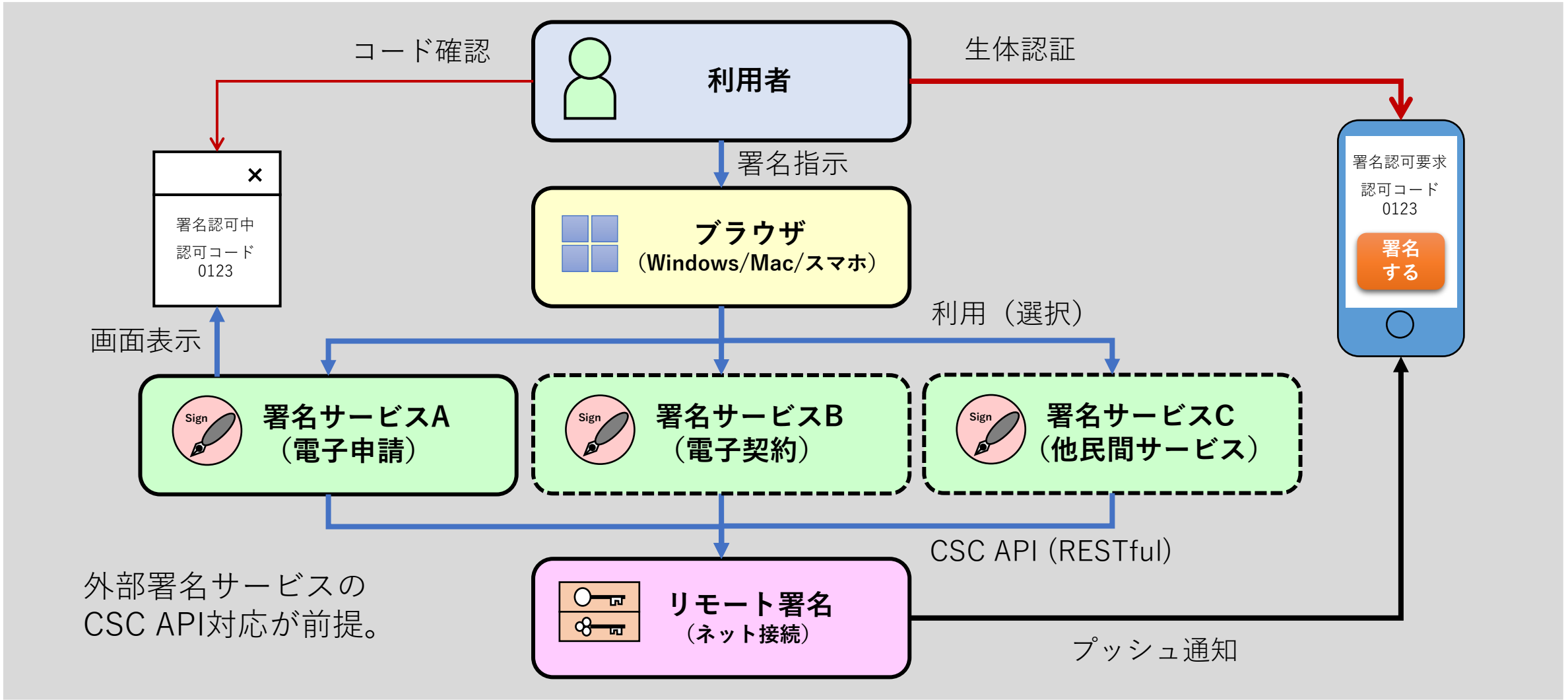
注：ドライバと管理ツールの事前インストールが必要。

1. Windows証明書ストア「個人」から証明書を選択して利用
   - 管理ツールにより証明書に署名ドライバの独自CSP名をセットして証明書ストアに証明書をインストールして利用。
   - CryptAcquireCertificatePrivateKey APIで証明書から秘密鍵を取得する。
2. CSP名を指定して利用（MNCのCSP名の直接利用と同じ）
   - 署名ドライバの独自CSP名を指定することで利用。
   - 複数の署名鍵がある場合は管理ツールで利用署名鍵を指定しておく。

※ マイナンバーカード/MNCがPC利用可能なら対応は比較的簡単。
上記の、方法1なら変更不要、方法2ならCSP名の追加が必要。

利用方法２：外部署名サービスとの連携

リモート署名（CSC API対応の署名サービス利用）



CSC API（業界標準の署名連携API）

CSC : Cloud Signature Consortium の略

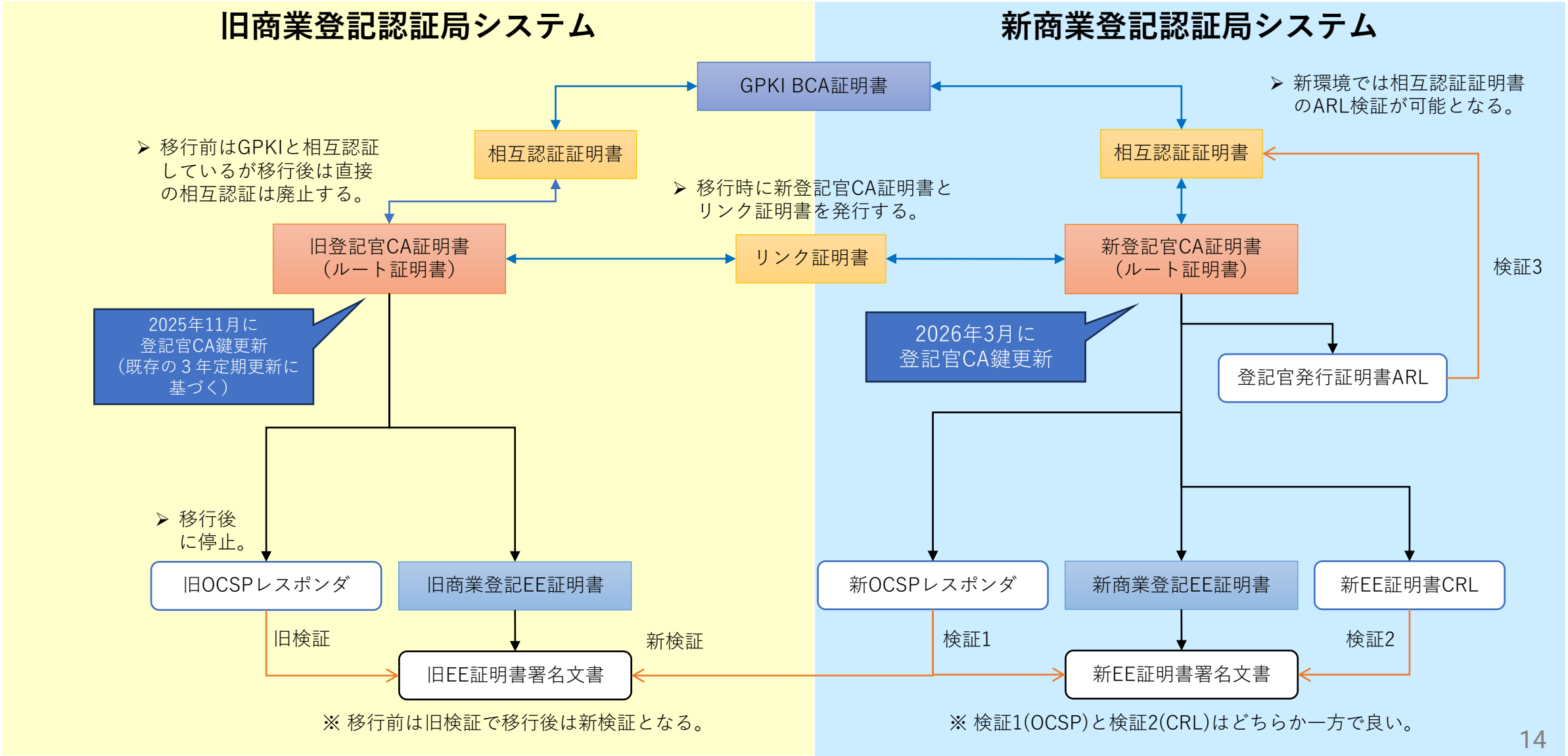
https://cloudsignatureconsortium.org/

- CSCは欧州eIDASの署名連携APIをベースに国際的標準化を目指す民間の標準化団体。日本の民間署名事業者も参加。
- リモート署名の事実上の業界標準となっており今後普及が見込まれている。既に Adobe Sign 等が実装済み。
- 日本国内においても採用するシステムやサービスが増加する予定となっている。SIPの欧州相互実証実験にも使われている。
- 電子署名以外に電子シール（eシール）での利用も可能。

APIの仕様書を公開中：

https://cloudsignatureconsortium.org/resources/download-api-specifications/

新旧認証局の証明書関連図



対応頂きたいユースケース

署名時		対応
1	Windows環境にてCAPI利用の署名アプリを利用している場合	仮想ICカード署名ドライバ利用へ移行が必要です。 → 16ページを参照
2	Windows環境にてPKCS#12ファイルを直接利用している場合	Windows証明書ストアにインストールして仮想ICカード署名ドライバ利用へ移行が必要です。→ 16ページを参照
3	Windows環境以外でPKCS#12ファイルを利用している場合	外部署名サービスとしての利用へ移行が必要です。 → 17ページを参照
4	サーバー環境にてPKCS#12ファイルをeシール的に直接利用している場合	リモート署名では実現不可となりますので、2028年までに他証明書等へ移行が必要です。→ 18ページを参照
5	ICカード格納サービス発行のICカードを利用している場合	不要：発行申請の手順は変わりませんので署名は従来通り行うことが可能です。
6	ネット接続できない環境で署名付与している場合	リモート署名方式は使えませんのでICカードか他証明書等への移行が必要です。→ 19ページを参照
検証時		対応
A	GPKI/LGPKIの証明書検証サーバーを利用している場合	不要：従来通り証明書検証サーバーで検証が可能です。
B	Adobe Reader等の一般的な検証アプリを利用している場合	不要：OCSPやCRLを使って検証可能ですが、登記CAルート証明書が必要です。
C	独自に実装した検証器でOCSP等を利用して直接検証している場合	CRL/ARLが利用可能等のPKI構造が変更になりますので対応が必要になる場合があります。 → 14ページの関連図を参照して検討が必要。

仮想ICカード署名ドライバ利用への移行

概要：

- Windows環境に仮想ICカード署名ドライバをインストールしてCAPIから利用する方法です。
- CSP名を指定して直接利用する場合には、マイナンバーカードをWindows環境で使う場合とCSP名が異なりますが利用方法はほぼ同じです。
- 仮想ICカード署名ドライバのCSP名を設定した証明書をWindows証明書ストアにインストール可能とするので証明書選択する利用方法に対応済みであれば従来通りの利用も可能です。
- PKCS#12ファイルを直接読み込んで利用している場合には、Windows証明書ストアにインストールしてから仮想ICカード署名ドライバを使うことになります。

利用が可能な時期：2026年7月以降のリモート署名稼働時から対応が可能となる予定です。

試験が可能な時期：2026年4月以降に動作確認の試験が可能となる予定です。

移行が必要なソフトウェア：

- Windows環境で署名付与するアプリケーションやプラグインは移行が必要です。
- 証明書ストアから証明書を選択して署名が可能なソフトウェアの場合には、そのまま動作する可能性がありますのでご確認ください。

Windows環境以外で署名利用の場合

概要：

- 仮想ICカード署名ドライバは、サービス開始時点ではWindows環境用のみ提供予定です。
- ご要望があればPKCS#11形式の署名ドライバは他環境でも提供可能である可能性があります。
- リモート署名に対応した外部署名サービスと連携可能であればブラウザから署名が可能です。
- 今後リモート署名は民間も含め増えると考えられており、申請サービス等でも直接リモート署名利用することもご検討ください。
- 市販されている多くの署名ライブラリ等はリモート署名にも対応が可能です。

移行が必要なソフトウェア：

- Windows環境以外（MacOS/iOS/Android/Linux等）で署名付与するアプリケーションやプラグインは移行が必要です。
- PKCS#11対応で良ければMacOS等への提供の可能性はありますので必要な場合には最終ページの問合わせ先までご連絡ください。

サーバー自動署名（eシール的）利用の場合

概要：

- サーバー上にPKCS#12ファイルを置きプログラムからPINを与えることで自動的に署名認可している場合となります。新システムでは署名の都度スマホでの署名認可が必要ですので自動署名はできなくなります。
- ICカードに格納するサービスを利用すればICカードを接続しての利用は可能ですが性能的に問題が出ると予想されます。
- 商業登記電子証明書は登記する代表印相当となるので新システムではeシール的な利用方法へは対応しません。eシールは総務省にて認定を検討しており移行を検討ください。

対応が必要な時期：　2028年の新暗号移行までには対応が必要です。

移行電子証明書の選択肢案：

1. 新たにeシール認定されたeシールの電子証明書に移行する。
2. 電子署名法の認定認証局のうちPKCS#12ファイル発行可能な電子証明書に移行する。
3. 行政等の利用目的であればGPKIのサーバーHSM格納型のGPKI電子証明書に移行する。

ネット接続できない環境の場合

概要：

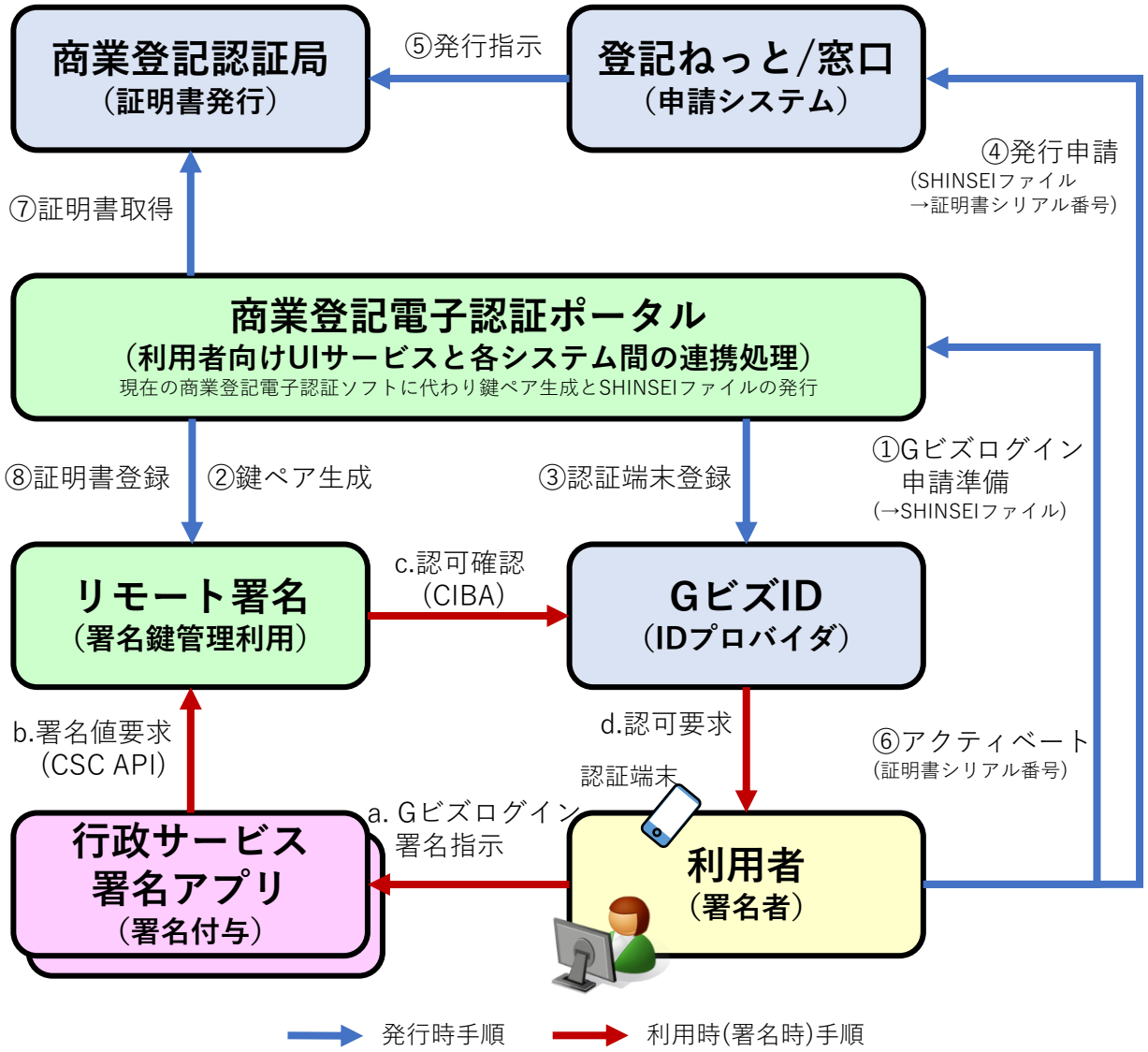
- PKCS#12ファイルをネット接続できない環境に置き署名している場合となります。新システムではリモート署名サーバーへのネット接続が必要となる為にネット接続できない環境では署名ができなくなります。
- ICカードに格納するサービスを利用すればICカードを接続しての利用は可能です。ICカード利用の場合にはネット接続は不要となります。

対応が必要な時期：　2028年の新暗号移行までには対応が必要です。

移行の選択肢案：

1. 商業登記電子証明書のICカード格納サービスを利用してICカード化して利用する。
2. 電子署名法の認定認証局のうちPKCS#12ファイルまたはICカード発行可能な電子証明書に移行する。
3. 行政等の利用目的であればGPKIのサーバーHSM格納型のGPKI電子証明書に移行する。

参考：システム連携図



システム	開発	補足
商業登記認証局 [CA]	既存システム（更新予定）	更新開発中
登記ねっと/窓口	既存システム	従来と同じ申請手順
電子認証ポータル [PORTAL]	新規開発	現在の電子認証ソフトと同等機能をWebサービスとして提供。利用の為にGビズIDアカウントが必要。
リモート署名 [RSSP]	新規開発	業界標準仕様で開発。※ CSC API
GビズID [IdP]	既存システム（更新予定）	GビズIDアプリによる署名認可を行う。
行政サービス or 署名アプリ [SCA]	新規開発 or 更新開発	CSC APIを利用して署名値を要求して署名文書を作成する。署名ドライバを提供することで既存アプリ(Acrobat等)から利用可能とする。

参考：新暗号方式への移行

概要：

- 2028年のGPKI相互認証（BCA）の新暗号移行に伴い商業登記認証局でも2028年新暗号に移行予定です。
- 詳しくは「政府認証基盤（GPKI）における暗号アルゴリズムの移行に係る周知及び依頼について」を参照。

■ 新暗号に対応した情報システムの相互運用性の**検証環境を2023年に検討、2024年に構築予定（2025年1月～暗号移行検証環境が段階的に利用可）**

■ **ブリッジ認証局は、**2026年のシステム更改にあわせ新暗号に対応して、**2028年9～10月に鍵更新により新暗号の利用を開始**。官職認証局で発行する**官職証明書は、新暗号(ECDSA P-256,384及びRSA3072)により発行**する。

※現行の官職認証局で2026年以降に発行する旧暗号（RSA2048）の官職証明書については、有効期限を2030年末にする予定

旧暗号：RSA2048

新暗号：RSA3072
ECDSA P-256

新暗号：ECDSA P-384

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビットセキュリティ	新規生成	移行完遂期間	利用不可	利用不可	利用不可	利用不可
	処理		許容			
128 ビットセキュリティ	新規生成	利用可	利用可	移行完遂期間	利用不可	利用不可
	処理				許容	
192 ビットセキュリティ	新規生成	利用可	利用可	利用可	利用可	利用可
	処理					
256 ビットセキュリティ	新規生成	利用可	利用可	利用可	利用可	利用可
	処理					

問合せ先

デジタル庁　商業登記電子証明書担当
Mail: crpki@digital.go.jp