

---

# 認定認証業務における リモート署名実現について

2026年2月19日(木)

NTTビジネスソリューションズ バリューデザイン部  
ソーシャルイノベーション部門 トラストビジネス担当

新井 聡

1. リモート署名とは
2. 認定認証とは
3. 認定認証でリモート署名を実現する課題
4. 課題の解決
5. リモート署名実演
6. 今後の課題
7. まとめ

あらい さとし  
新井 聡

N T Tビジネスソリューションズ株式会社 バリューデザイン部  
ソーシャルイノベーション部門 トラストビジネス担当

情報処理安全確保支援士(013032)



## 主な経歴

- 1999年 N T T(西日本)入社(富山支店で遠隔映像コミュニケーション実証、ISDNやフレッツの販促に従事)
- 2002年 N T T情報流通プラットフォーム研究所にて、認証局プログラム開発に従事
- 2008年 N T Tアプリエ(現N T Tビジネスソリューションズ)にて認定認証業務e-Probatio認証局の運用に従事  
この間、マイナンバーカードの利活用検討、Gビズ I Dの有識者会などに参加
- 2024年 10月に電子認証局会議 会長を就任(<https://www.c-a-c.jp/>)

現在に至る

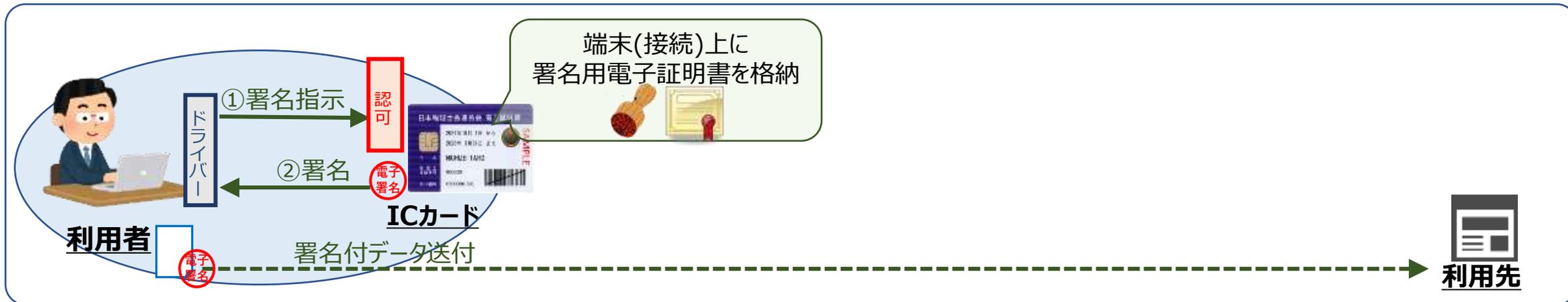
## リモート署名との関わり

- 2020年 4月 JNSA/JT2Aにて、小川氏、宮地氏らとリモート署名ガイドラインを作成
- 2023年 デジタル庁電子署名法認定基準のモダナイズ検討会にてリモート電子署名基準等に関する調査に参画
- 2025年 8月 認定認証業務e-Probatio PSA サービスにてリモート署名対応の電子証明書発行開始
- 2026年 JNSA/JT2Aにて、小川氏、宮地氏らとリモートeシールガイドラインが完成予定

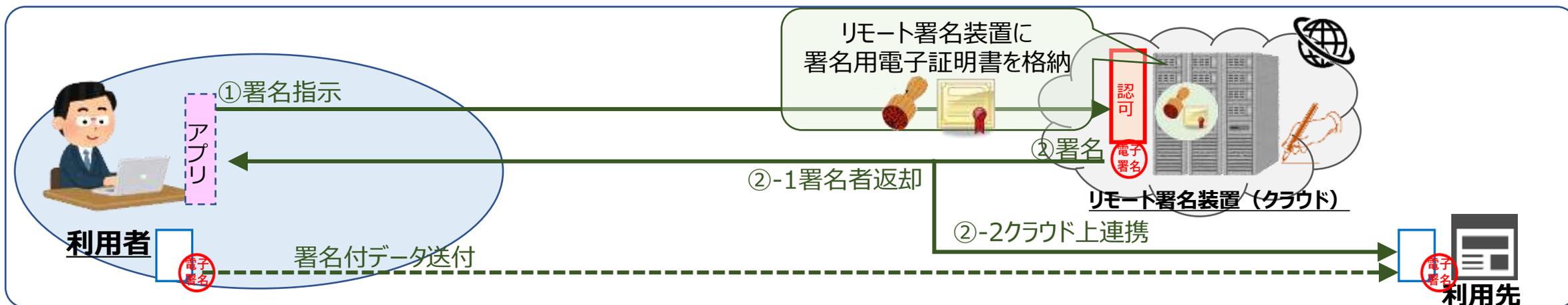
# 1. リモート署名とは

- 署名鍵が署名者自身が直接操作する端末に接続する媒体に格納され、署名を実施するローカル署名に対して、署名鍵がネットワークを介した遠隔に設置された媒体に格納され、署名者の指示により署名を実施することをリモート署名という。
- リモート署名では、クラウド上で利用先と連携するも視野に入れることが可能である。

## ローカルとリモート署名の概要



## ローカル署名



## リモート署名

## 2. 認定認証業務とは

- ① 概要
- ② 主な利用先
- ③ 一覧

## 2. 認定認証業務 ① 概要

- **電子署名**のための**電子証明書発行業務**であり、**電子署名法に基づく業務基準**を満たし**大臣認定**を受けた高信頼の認証業務。
- **本人確認**と**鍵管理**を厳格に行い、**日本の法律の中で信頼性の高い電子証明書**を発行する。
- 認証基準を維持するため、毎年、大臣が認定する**指定調査機関から調査**を受け、適合性を確認し認定更新している。

### 利用者



入札/申請

### 入札機関



有効性  
確認

申込

提供

### 認定認証業務

本人確認

身元確認 当人確認

意思確認

認定認証事業  
業務オペレーション

公開鍵基盤運用



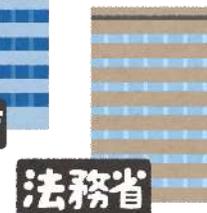
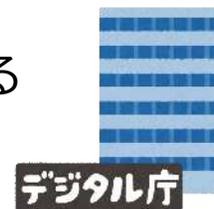
認証局  
設備



認定認証事業  
設備オペレーション

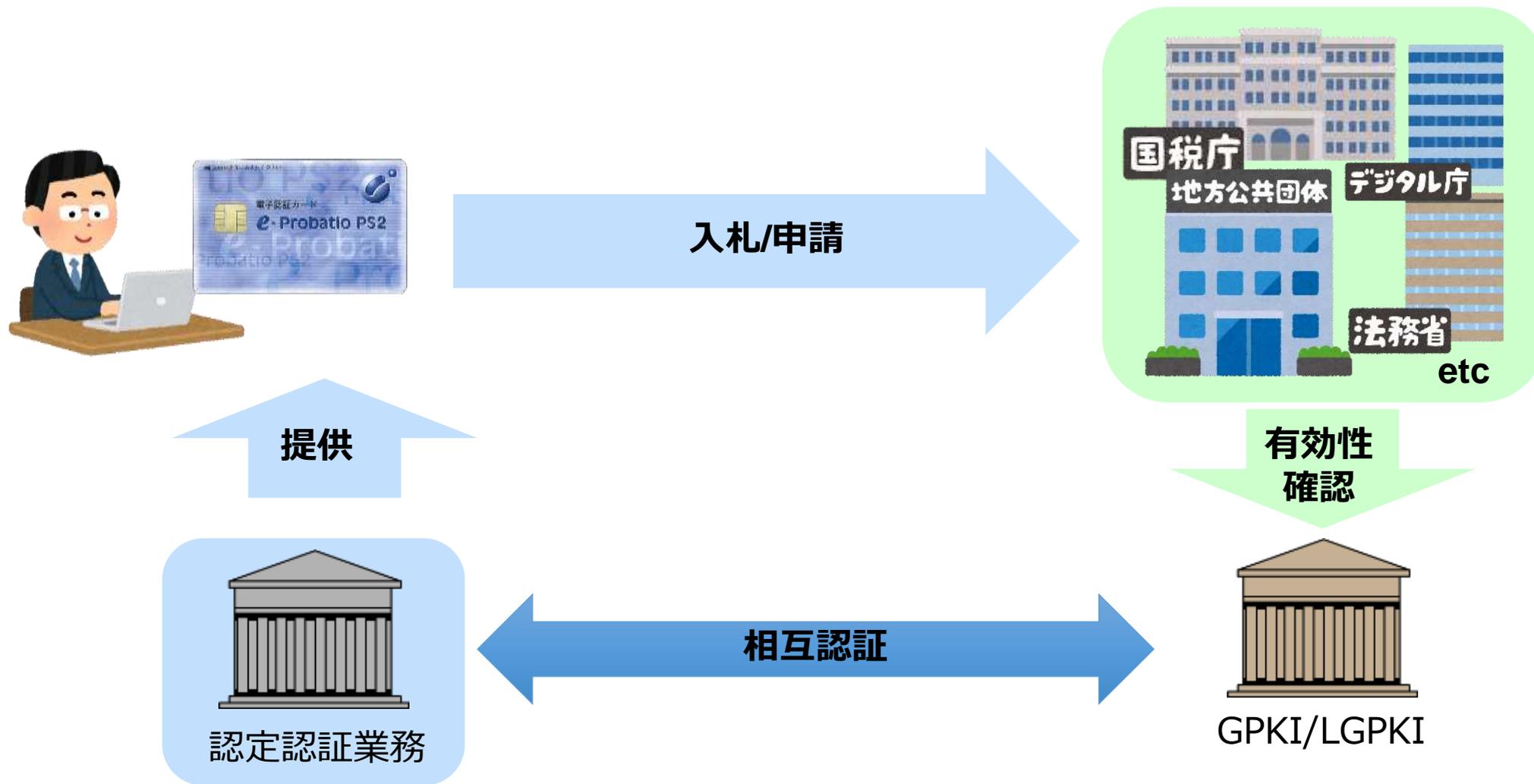
電子署名法による  
調査/認定

JIPDEC



## 2. 認定認証業務 ② 利用先

- 認定認証業務の多くは**GPKIやLGPKIと相互認証**し、**公的機関と安全に連携できる認証基盤**を提供する。
- 公的入札や行政申請で利用されるため、**政府機関や自治体**に対する利用が特に多い。
- 相互認証で広く信頼を得る一方、**既存行政基盤に合わせた運用**となっている。



## 2.認定認証業務 ③認定認証業務一覧

認定認証業務名	業務名事業者名	認定日	業務の特徴（概要）
セコムパスポート for G-ID	セコムトラストシステムズ株式会社	平成14年7月4日	行政手続の電子申請向け。公共分野で広く利用。
TOiNX電子入札対応認証サービス	株式会社トインクス	平成14年12月10日	公共・民間の電子入札や調達で利用。
TDB電子認証サービス TypeA	株式会社帝国データバンク	平成15年2月5日	行政電子申請・入札など幅広い用途に対応。
<b>e-Probatio PS2 サービス</b>	<b>N T Tビジネスソリューションズ株式会社</b>	<b>平成17年11月9日</b>	<b>電子契約・電子申請など特定サービス向け。</b>
DIACERTサービス	三菱電機デジタルイノベーション株式会社	平成26年2月6日	e-Tax など政府向け申請に強み。
AOSign サービス G2	日本電子認証株式会社	平成26年7月31日	電子調達・電子商取引・文書保存など多用途対応。
DIACERT-PLUSサービス	三菱電機デジタルイノベーション株式会社	平成27年1月21日	電子入札コアシステムなど自治体向けで使用。
<b>e-Probatio PSA サービス</b>	<b>N T Tビジネスソリューションズ株式会社</b>	<b>平成28年11月1日</b>	<b>税理士法に関連する特定の業務に利用。</b>
my電子証明書	my FinTech株式会社	令和3年11月10日	本人性・非改ざん性担保の電子署名用途。

参照

[https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/04e470aa-73e3-435a-b841-939582c7a549/fcd8c2ae/20250527\\_policies\\_digitalsign\\_outline\\_01.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/04e470aa-73e3-435a-b841-939582c7a549/fcd8c2ae/20250527_policies_digitalsign_outline_01.pdf)

<https://www.moj.go.jp/MINJI/minji32.html>

<https://www.jipdec.or.jp/project/designated-investigative-organization/accredited-ca-list.html>

# 3. 認定認証でリモート署名を実現する課題

- ① 電子署名法の媒体規定がない
- ② 利用先がリモート署名に対応していない
- ③ 認証認可手段の選択

# 3. 認定認証でリモート署名を実現する課題

- ① 電子署名法の媒体規定がない
- ② 利用先がリモート署名に対応していない
- ③ 認証認可手段の選択

## 媒体規定はない！

あるとして

第三条 電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために**必要な符号及び物件を適正に管理**することにより、**本人だけが行うことができる**こととなるものに限る。）が行われているときは、真正に成立したものと推定する。

新井訳

**署名鍵は、**  
署名者自身のみが署名できるように、  
**署名者自身が適切に管理する！**

### 3.①電子署名法の媒体規定 その2 施行規則

#### 電子署名法施行規則 第六条

三 利用者が電子署名を行うために用いる符号（以下「利用者署名符号」という。）を**認証事業者が作成する場合**においては、当該利用者署名符号を安全かつ確実に利用者に渡すことができる方法により交付し、又は送付し、かつ、当該**利用者署名符号**及びその複製を**直ちに消去すること**。

#### 要約

**認証局が**  
利用者**署名鍵**を作成  
→利用者署名鍵は  
認証局に残さない

三の二 **利用者署名符号を利用者が作成する場合**において、当該利用者署名符号に対応する利用者署名検証符号を認証事業者が電気通信回線を通じて受信する方法によるときは、次に掲げる場合の区分に応じそれぞれ次に定めるものであること。

**利用者が**  
利用者**署名鍵**を作成

イ 当該利用者から**現に有している電子証明書**又は**公的個人認証法第三条第一項に規定する署名用電子証明書**に係る**電子署名が行われた情報**が送信される場合であって、当該利用者となるための申込みの際に当該**利用者署名検証符号**を認証事業者に電気通信回線を通じて**送信**するとき当該電子署名により当該利用者の真偽の確認を行うこと。

利用者が  
利用者**検証鍵**を  
所定の電子証明書による  
**電子申込時に送付**  
(昨年6月に制定)

ロ イに該当しない場合 あらかじめ、**利用者識別符号**（認証事業者において、一回に限り利用者の識別に用いる符号であって、容易に推測されないように作成されたものをいう。）を**安全かつ確実に当該利用者に渡す**ことができる方法により交付し、又は送付し、かつ、**当該利用者の識別に用いる**までの間、当該利用者以外の者が知り得ないようにすること。

認証局が**真偽確認後**、  
利用者が  
認証局が発行した  
**利用者識別符号**とともに  
**利用者検証鍵**を送付

**鍵の生成/管理は認証局か利用者に対しての規程のみ**

# 3.①電子署名法の媒体規定 その3 施行規則図説

## 施行規則第六条三



認定認証事業者

②真偽確認完了

③鍵ペア作成



④証明書作成



⑤格納



利用者署名鍵  
完全消去

⑥受領



①申込



利用者

## 施行規則第六条三の二 イ



認定認証事業者

③真偽確認完了

④証明書作成



②申込



①鍵ペア作成



⑤受領



⑥格納



利用者

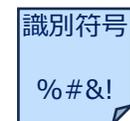
## 施行規則第六条三の二 ロ



認定認証事業者

②真偽確認完了

③利用者識別  
符号発行



①申込

④鍵ペア作成



⑤証明書  
発行依頼



⑥証明書作成



⑦受領



⑧格納



利用者

### 3. 認定認証でリモート署名を実現する課題

- ① 電子署名法の媒体規定がない
- ② 利用先がリモート署名に対応していない
- ③ 認証認可手段の選択

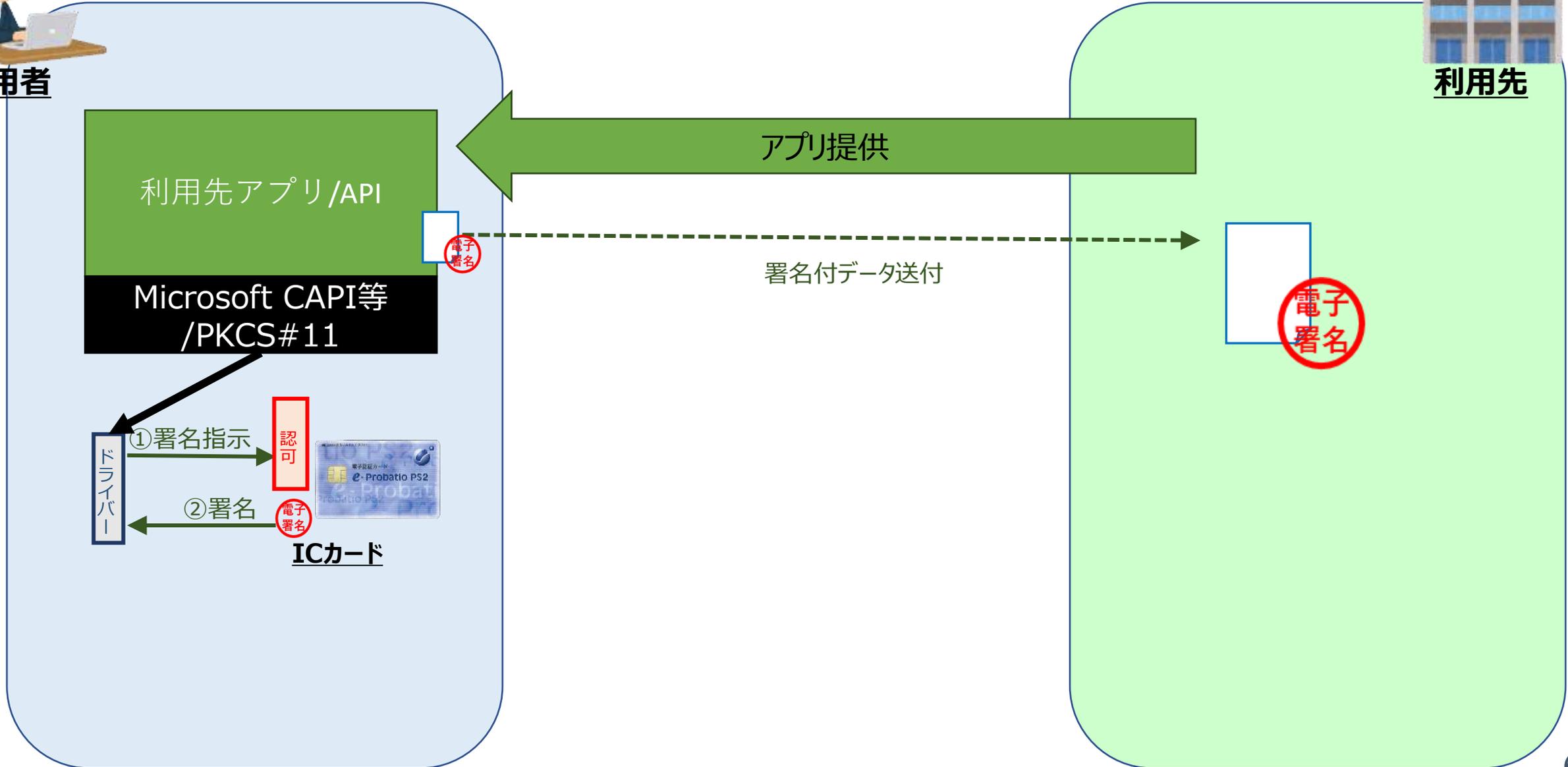
### 3.②利用先が基本的にローカル署名対応



利用者



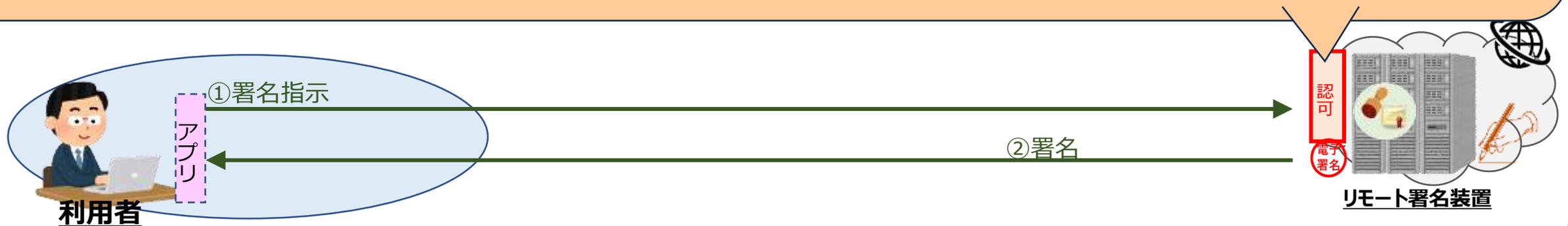
利用先



### 3. 認定認証でリモート署名を実現する課題

- ① 電子署名法の媒体規定がない
- ② 利用先がリモート署名に対応していない
- ③ 認証認可手段の選択

どんな**認証認可手段**を使って  
署名者自身のみが署名できるようにするの？



## 4. 課題の解決

- ① 利用者が署名鍵を作成と解釈
- ② 現行のカードAPIのラッパを作成
- ③ 認証認可を選ぶ
- ④ <実現したリモート署名>

## 4. 課題の解決

- ① 利用者が署名鍵を作成と解釈
- ② 現行のカードAPIのラッパを作成
- ③ 認証認可を選ぶ
- ④ <実現したリモート署名>

# 4.①利用者が署名鍵を作成と解釈 その1

## 施行規則第六条三



認定認証事業者

②真偽確認完了

③鍵ペア作成



④証明書作成



⑤格納



利用者署名鍵  
完全消去

⑥受領



①申込



利用者

## 施行規則第六条三の二 イ



認定認証事業者

③真偽確認完了

④証明書作成



②申込



①鍵ペア作成



⑤受領



⑥格納



利用者

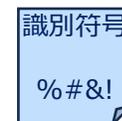
## 施行規則第六条三の二 ロ



認定認証事業者

②真偽確認完了

③利用者識別  
符号発行



①申込

④鍵ペア作成



⑤証明書  
発行依頼



⑥証明書作成



⑦受領



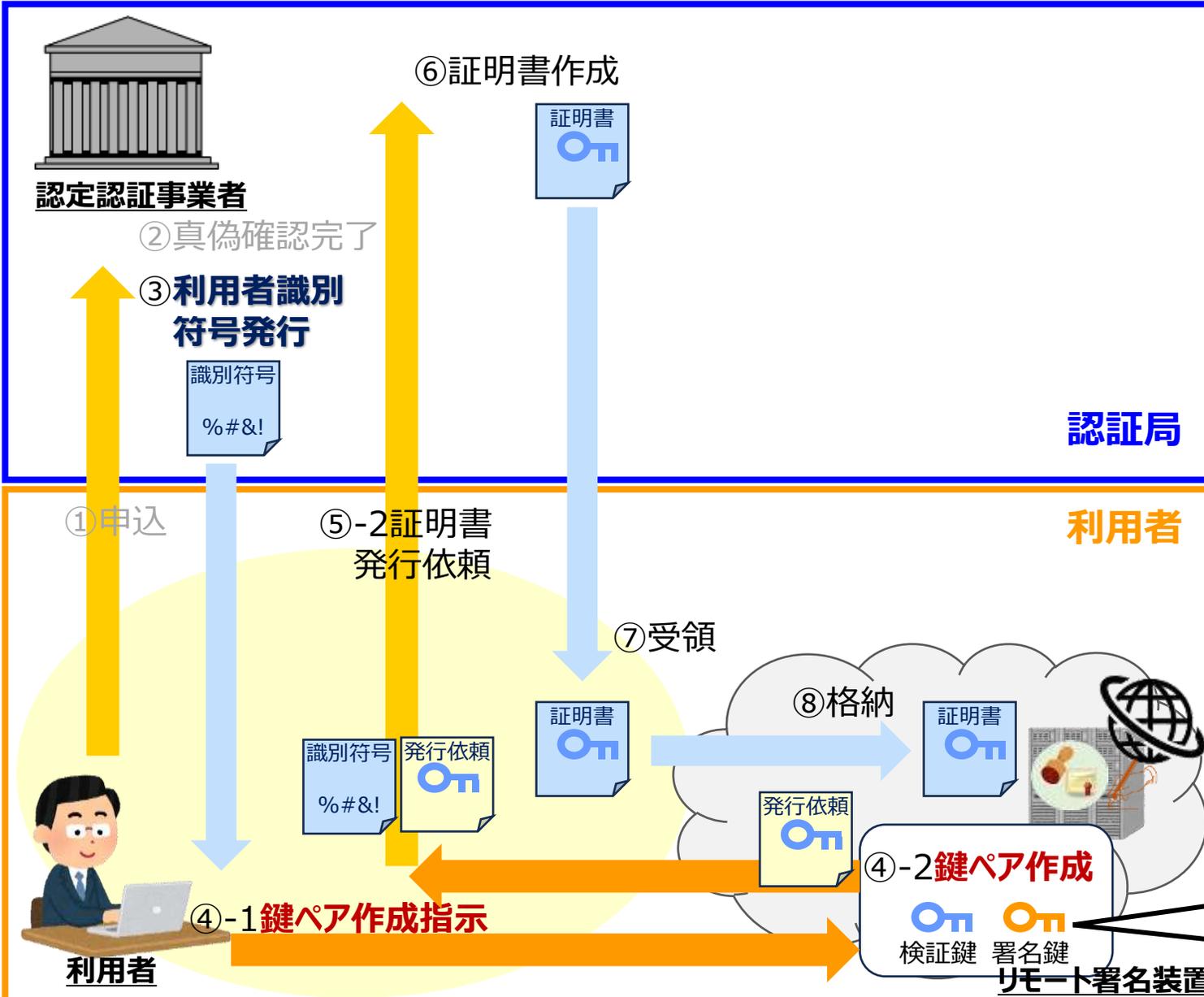
⑧格納



利用者

# 4.①利用者が署名鍵を作成と解釈 その2

施行規則第六条三の二 □



## リモート署名鍵は利用者の管理として扱う

	フロー	主体者	施行規則
①	電子証明書の利用申込みをする	利用者	第五条
②	利用申込書の受付・真偽確認の審査を行う	認証局	第六条三の二□
③	利用申込みの真偽確認の審査完了。 <b>利用者識別符号</b> を発行し、 <b>安全かつ確実に当該利用者に渡すことができる方法</b> にて送付する		
④	1.リモート署名装置に <b>鍵ペア作成</b> を指示 2.リモート署名装置は <b>鍵ペアを作成</b>	利用者	—
⑤	1.検証鍵を格納した発行依頼(CSR)を生成する 2.発行依頼(CSR)と <b>利用者識別符号</b> を認証局へ送付する		第六条三の二□
⑥	CSRと <b>利用者識別符号</b> を受領し検証を行い、電子証明書を発行する ※ <b>利用者識別符号</b> は、識別のみ1回	認証局	
⑦	リモート署名装置へ電子証明書を登録する	利用者	
⑧	受領書（登録完了通知）を作成する		

署名鍵は生成から署名まで一切装置の外に出ない

## 4. 課題の解決

- ① 利用者が署名鍵を作成と解釈
- ② 現行のカードAPIのラッパを作成
- ③ 認証認可を選ぶ
- ④ <実現したリモート署名>

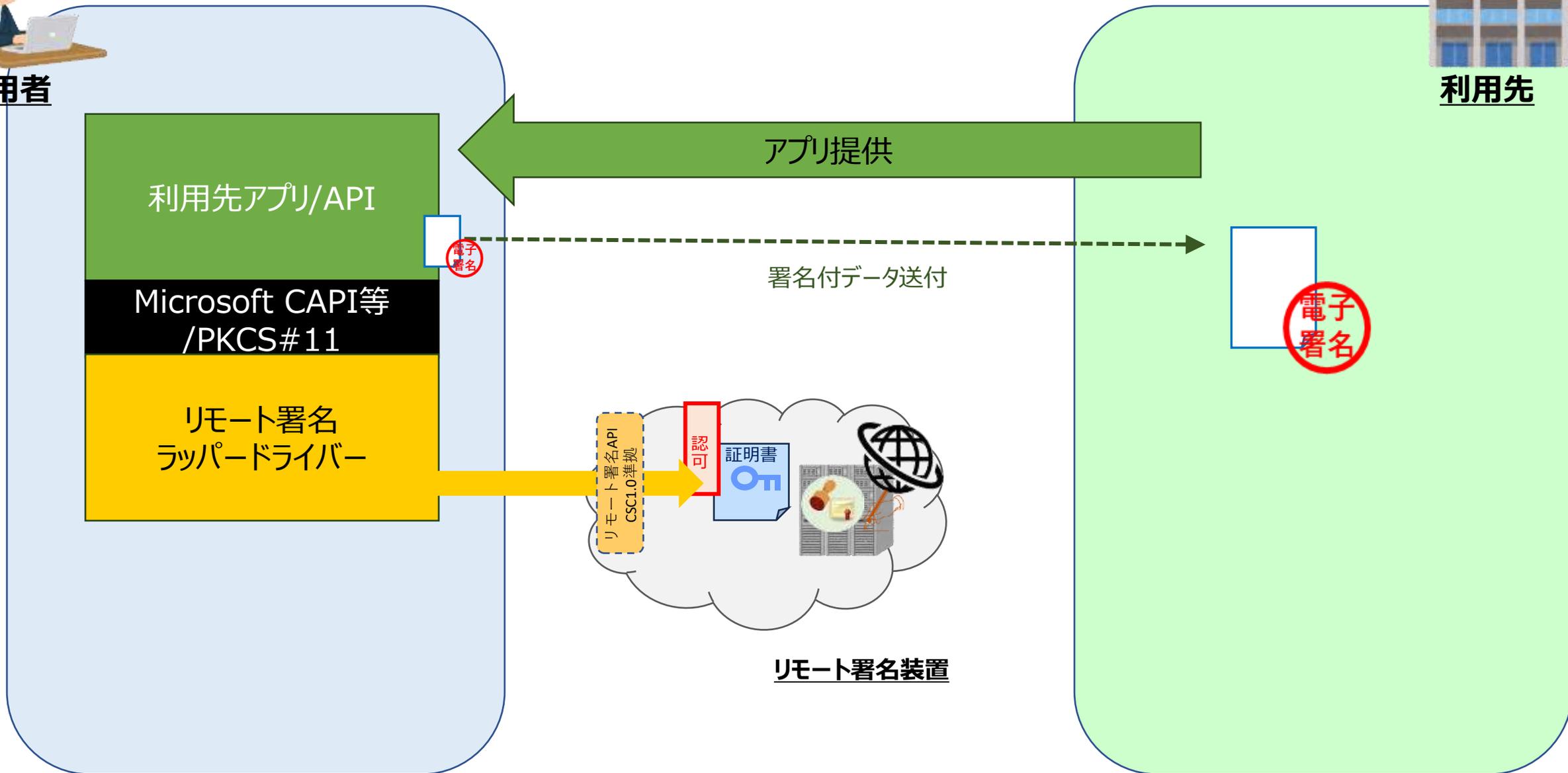
## 4.② 現行のカードAPIのラッパを作成 その2



利用者



利用先



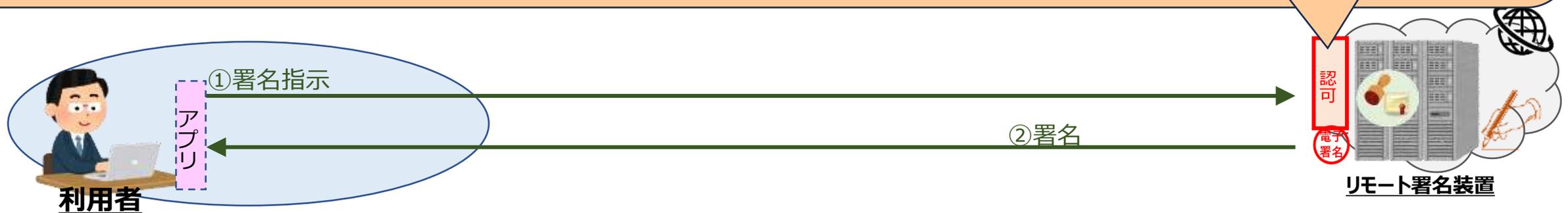
## 4. 課題の解決

- ① 利用者が署名鍵を作成と解釈
- ② 現行のカードAPIのラッパを作成
- ③ 認証認可を選ぶ
- ④ <実現したリモート署名>

## 4.③認証認可手段

### 考えられる主な認証認可手段

	認証認可手段	特徴	メリット	デメリット	選択
1	ICカード 	<ul style="list-style-type: none"> <li>証明時にICカードで本人確認を実施します</li> <li>二要素認証</li> </ul>	<ul style="list-style-type: none"> <li>管理・持ち運びが容易です</li> <li>ICチップに証明書が格納されており、<b>安全性が高い</b>です</li> <li>社員証や会員証などの流用が可能です。</li> </ul>	<ul style="list-style-type: none"> <li>ICカードリーダが必須となります</li> <li>紛失・破損する可能性があります</li> </ul>	○
2	ワンタイムパスワード トークン 	<ul style="list-style-type: none"> <li>証明時に一度だけ使えるパスワードを表示する機器を利用し本人確認を実施します</li> <li>二要素認証</li> </ul>	<ul style="list-style-type: none"> <li>管理・持ち運びが容易です</li> <li>システムの認証にも利用可能です</li> </ul>	<ul style="list-style-type: none"> <li>紛失・破損の可能性があります</li> <li>文字を読み入力する必要があります</li> <li>電池等の寿命があります</li> </ul>	△
3	スマートフォン 	<ul style="list-style-type: none"> <li>証明時にスマートフォンを利用し本人確認を実施します</li> <li>二要素認証</li> </ul>	<ul style="list-style-type: none"> <li>スマートフォンのみで証明が可能です</li> <li>署名時にポップアップ可能で操作が容易です</li> </ul>	<ul style="list-style-type: none"> <li>スマートフォンが必須となります</li> <li>スマートフォンの故障や充電が切れると、利用できません</li> </ul>	○
4	ID/PW 	<ul style="list-style-type: none"> <li>証明時にID/PWで本人確認を実施します</li> <li>単要素認証</li> </ul>	<ul style="list-style-type: none"> <li>ID/PWの配付が容易です</li> <li>システムの対応も容易です</li> </ul>	<ul style="list-style-type: none"> <li>なりすましでログインできるため、セキュリティレベルが低いです</li> </ul>	×



## 4. 課題の解決

- ① 利用者が署名鍵を作成と解釈
- ② 現行のカードAPIのラッパを作成
- ③ 認証認可を選ぶ
- ④ <実現したリモート署名>

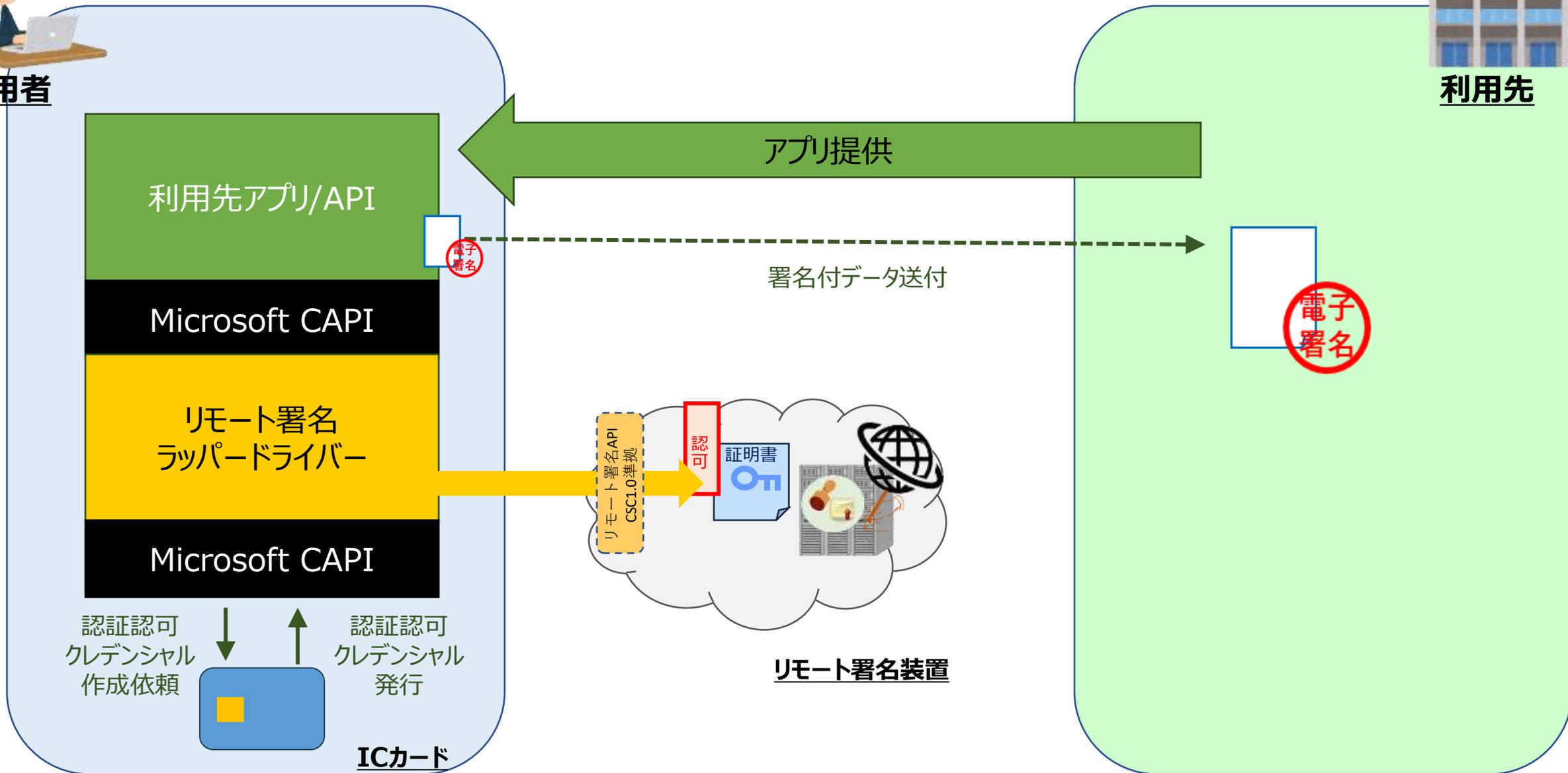
# 4.④ <実現したリモート署名>



利用者



利用先

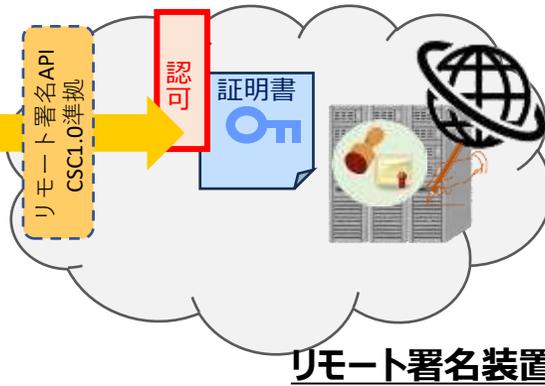


マイナンバーカード(利用者証明用証明書)で  
認証しリモート署名を実施

# 5.実演



利用者



利用者証明用電子証明書有効性確認



(流れ)

- ① マイナンバーカード(テスト)の確認
- ② アクロバットリーダーの起動
- ③ 電子署名実施  
　　<リモート署名開始>  
　　マイナンバーカードPIN入力  
　　<リモート署名開始>
- ④ 署名完了
- ⑤ 署名確認  
　　# 専用認証用カードでも可

- ① ラッパードライバーはいつまで必要か
- ② リモート署名標準APIは変容している
- ③ リモート署名の認証認可は議論が必要

- APIも進化し続け、まだまだ過渡期  
⇒CSC APIも1.0から2.0は大きく変容
- 認証認可手段に選択肢がある  
⇒電子署名保証ガイドラインに期待
- PQC時代にICカードやスマホが脆弱なら  
リモート署名が使われるかもしれない

ご清聴、ありがとうございました。

以下のQRからアンケートをお願いします！！

