

認証プラットフォーム（仮称）について ＜未定稿＞

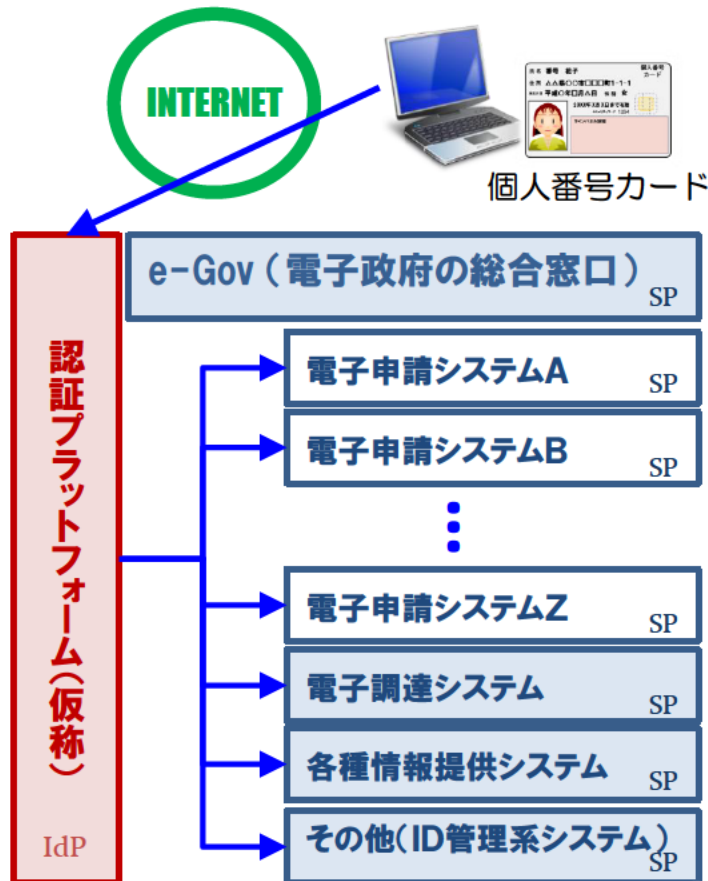
平成27年1月26日
総務省行政管理局

認証プラットフォーム（仮称）概要

- 世界最先端IT国家創造宣言（H25.6.14閣議決定。H26.6.24改定）において、「**政府の情報システムについては、個人番号カード等による本人認証を一括して行える認証プラットフォーム（仮称）の構築に向けて検討する**」こととしている。
- 以下及び次頁以降は、ICT街づくり推進会議の共通ID利活用WGの議論等を踏まえ、同WGの検討向けに行政管理局で検討・整理した認証プラットフォーム（仮称）のイメージ（未定稿）

【認証プラットフォーム（仮称）の主な特長】

主な特長	説明等
住民基本台帳等と連動する一元的本人確認	公的個人認証サービスと連携し、住民基本台帳に連動する本人確認等をインターネットで行う政府内システムを代表して一元的に実施
シングルサインオン（SSO）	政府情報システムと連携し、1回のログインで全ての政府の公開システムにアクセス可能
民間サイトとのシームレスなアクセス	連携する民間サイトで改めてログイン・パスワードの入力不要
オンライン手続の電子署名の代替・省略	暗号化通信と電子証明書を用いて、オンライン手続の都度必要な電子署名を代替・省略
より安心・安全なオンラインアクセス	ID・パスワード方式から個人番号カード方式へセキュリティを向上
開発コストの圧縮・重複排除	APIを用いて各システムの認証機能の開発を一元化
住所変更、資格情報等の一括提供	政府内のシステムに対し、住所変更情報や資格情報をプッシュ型・プル型で提供



※個人だけでなく、法人認証についても同様な方向で検討

※IdP : Identity Provider、SP : Service Provider

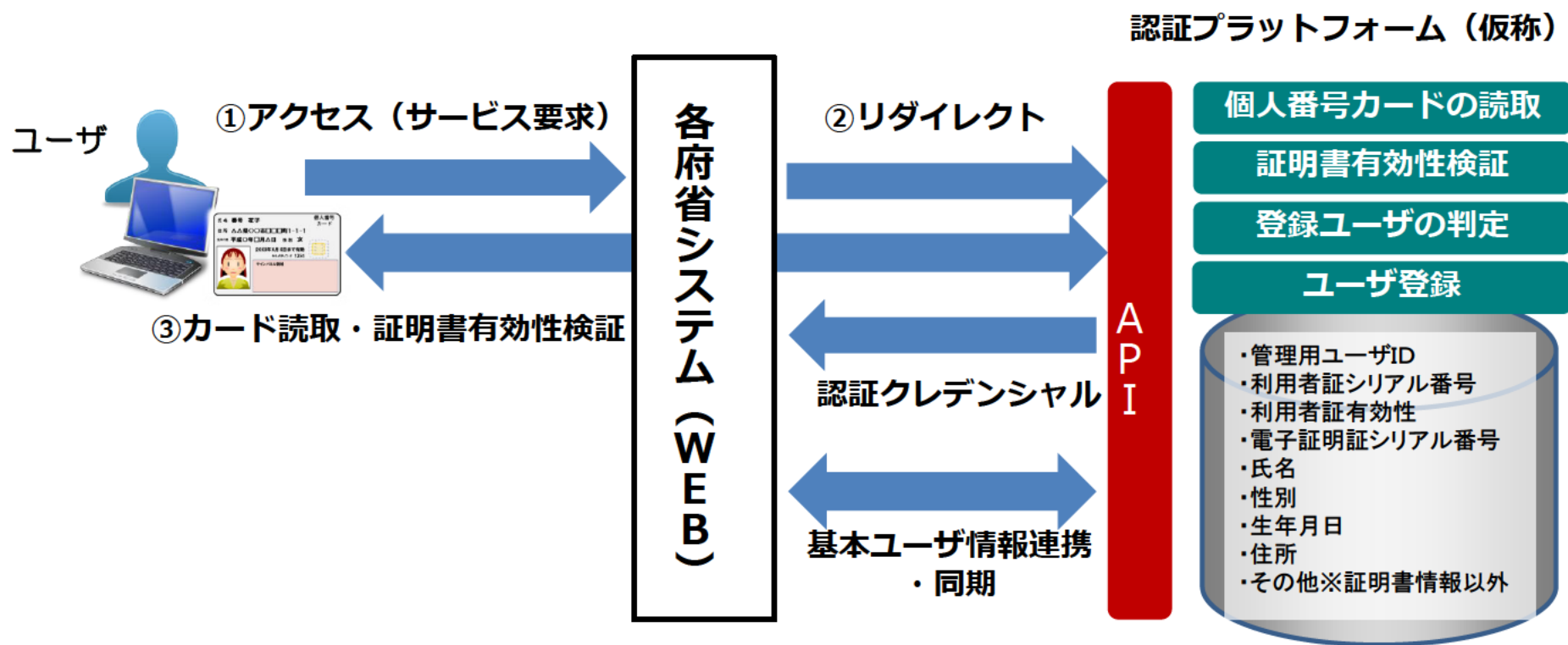
認証プラットフォーム（仮称）基本ユーザ情報

認証プラットフォーム（仮称）では、政府情報システムのIdPとして個人番号カードによるユーザ認証及び本人情報のSPへの通知を行うために、本人確認に係る基礎的情報を保有する。

登録事項	概要	入力源
管理用ユーザID	登録ユーザを識別するコード。IdPのみで使用し、非提供。	自動付与
利用者証シリアル番号	公的個人認証サービスの利用者証明用電子証明書のシリアル番号	個人番号カード（利用者証）
利用者証有効性	利用者証の有効・無効の別	公的個人認証サービス認証局（JPKI）
電子署名証シリアル番号	公的個人認証サービスの電子署名用電子証明書のシリアル番号	個人番号カード（電子署名証）
電子署名証有効性	電子署名省の有効・無効の別	公的個人認証サービス認証局（JPKI）
氏名	公的個人認証サービスの電子署名証に記録されている氏名（漢字）	個人番号カード（電子署名証）
住所	公的個人認証サービスの電子署名証に記録されている住所（漢字）	個人番号カード（電子署名証）
生年月日	公的個人認証サービスの電子署名証に記録されている生年月日	個人番号カード（電子署名証）
性別	公的個人認証サービスの電子署名証に記録されている性別	個人番号カード（電子署名証）
氏名かな	氏名の読み仮名	画面入力
連絡先電話番号	連絡用の電話番号	画面入力
連絡先メールアドレス	連絡用のメールアドレス	画面入力
携帯アドレス	ワンタイムパスワード送信用携帯アドレス	画面入力
…その他…		画面入力

各府省システムとの連携（API）

認証プラットフォーム（仮称）の機能については、APIを装備し、各府省等に連携・開発ツールとして提供。効率的な設計・開発を促し、政府全体の開発コストを抑制するとともに、利用者に対し、統一された利用し易いインターフェイスを提供。



SP側ID管理パターン

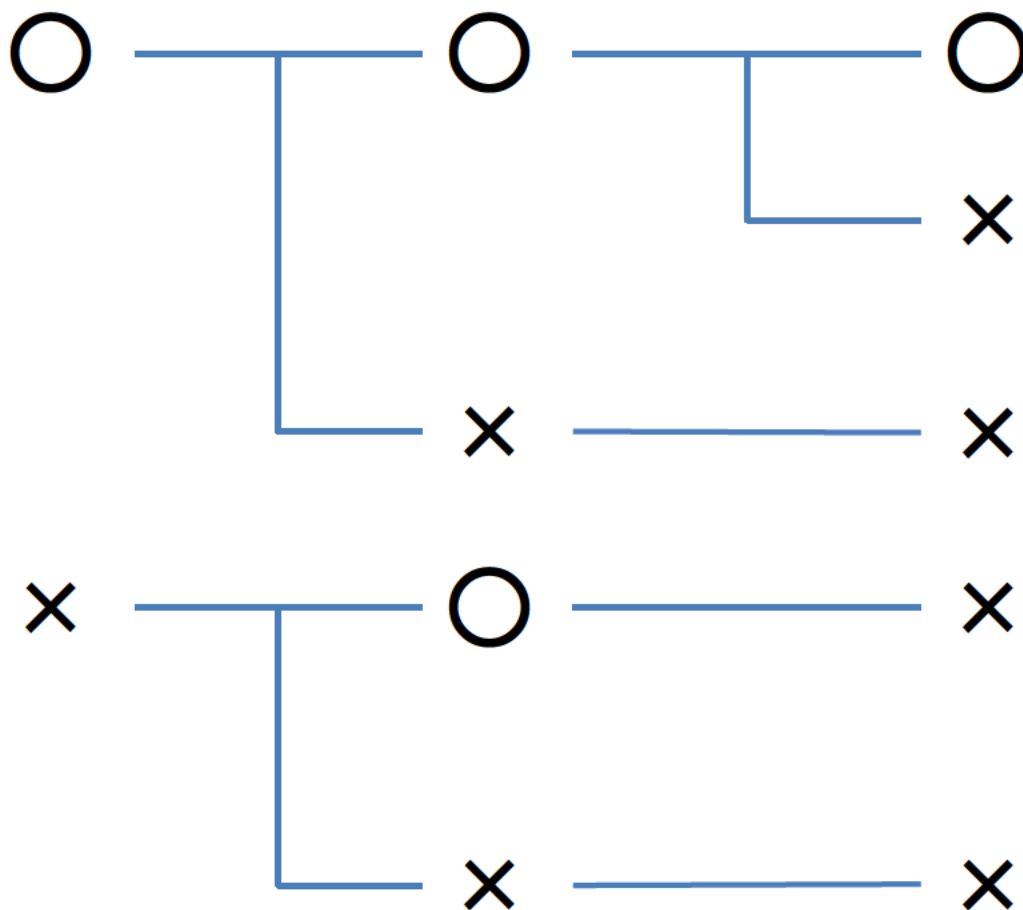
	Oタイプ	Aタイプ		Bタイプ		Cタイプ	
		A-1	A-2	B-1	B-2	C-1	C-2
タイプ説明	現在ユーザを識別したサービス（ID管理）は行っておらず、IdP運用後も行う予定のないもの ※ユーザ管理概念がないシステム	現在ユーザを識別したサービスは行っていないものの、IdP運用後、そのId管理の下に（個人番号カードにより）ユーザを識別したサービス提供を開始するもの	現在ユーザを識別したサービス提供を行っており、IdP運用後、個人番号カードによる認証と現行IDによる認証を並行して実施するもの。	現在ユーザを識別したサービス提供を行っており、IdP運用後、個人番号カードによる認証と現行IDによる認証を並行して実施するもの。ユーザ情報に独自事項が存在。			
独自のID登録	なし	なし	あり	あり			
ユーザ情報	なし	IdPの基本ユーザ情報の範囲内	IdPの基本ユーザ情報の範囲内	IdPの基本ユーザ情報の全部又は一部に加え、独自の登録事項			
IdPの基本ユーザ情報の独自保有・管理	不要	不要	必要	不要	必要	不要	必要

ユーザ登録の状態パターン

IdPのユーザ登録

SPのユーザ登録

IdPとSPのユーザ紐付け



※基本形（完成形）

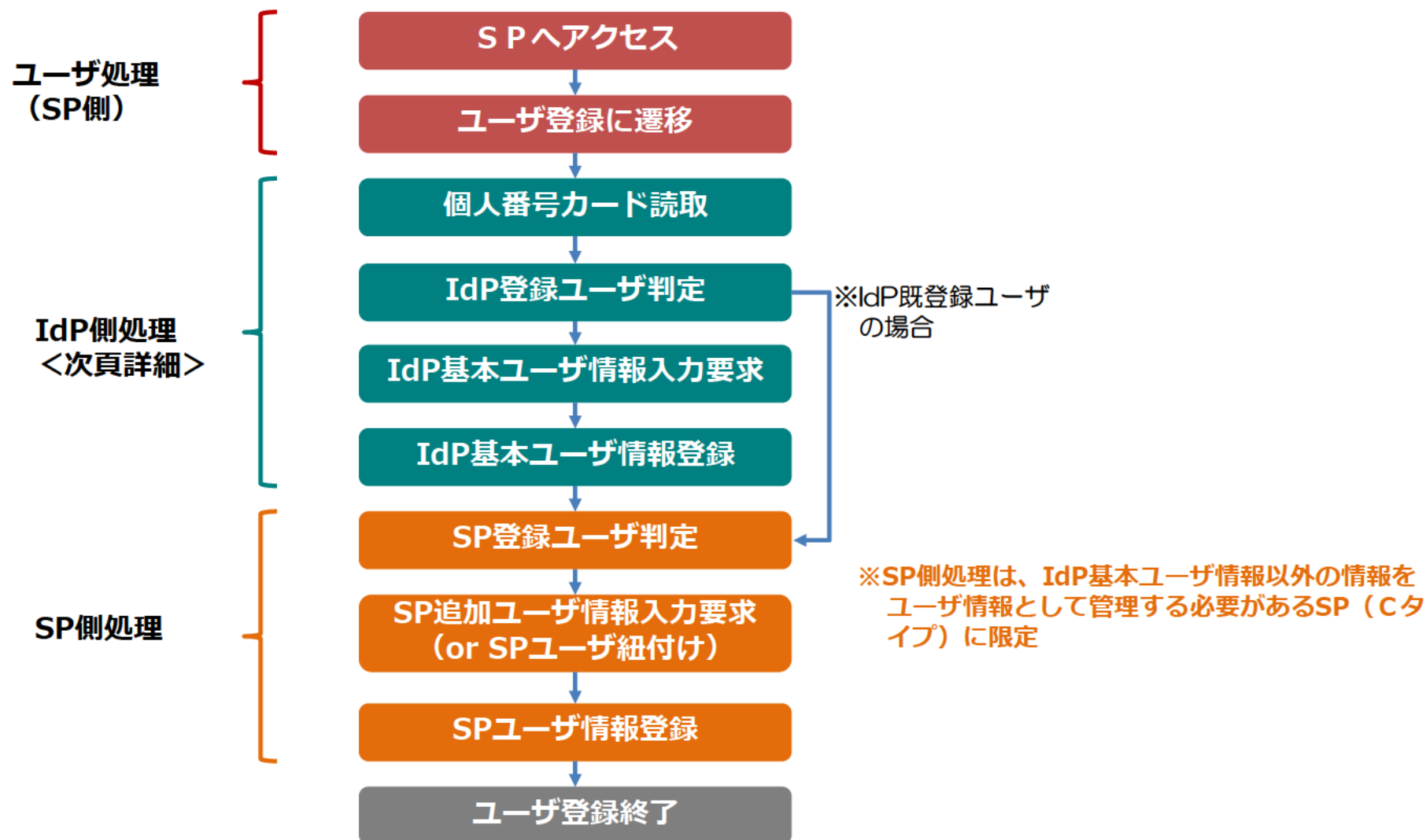
- ・ユーザが従前からID登録しているSPで、ユーザがIdPにユーザ登録した後、初めてSPにアクセスした際発生
- ・独自のID登録を行っているSP（B・Cタイプ）で、SPにユーザ登録した後、IdPにユーザ登録し、その後、初めてSPにアクセスした際発生

- ・ユーザがIdPにユーザ登録した後、初めてSPにアクセスした際発生

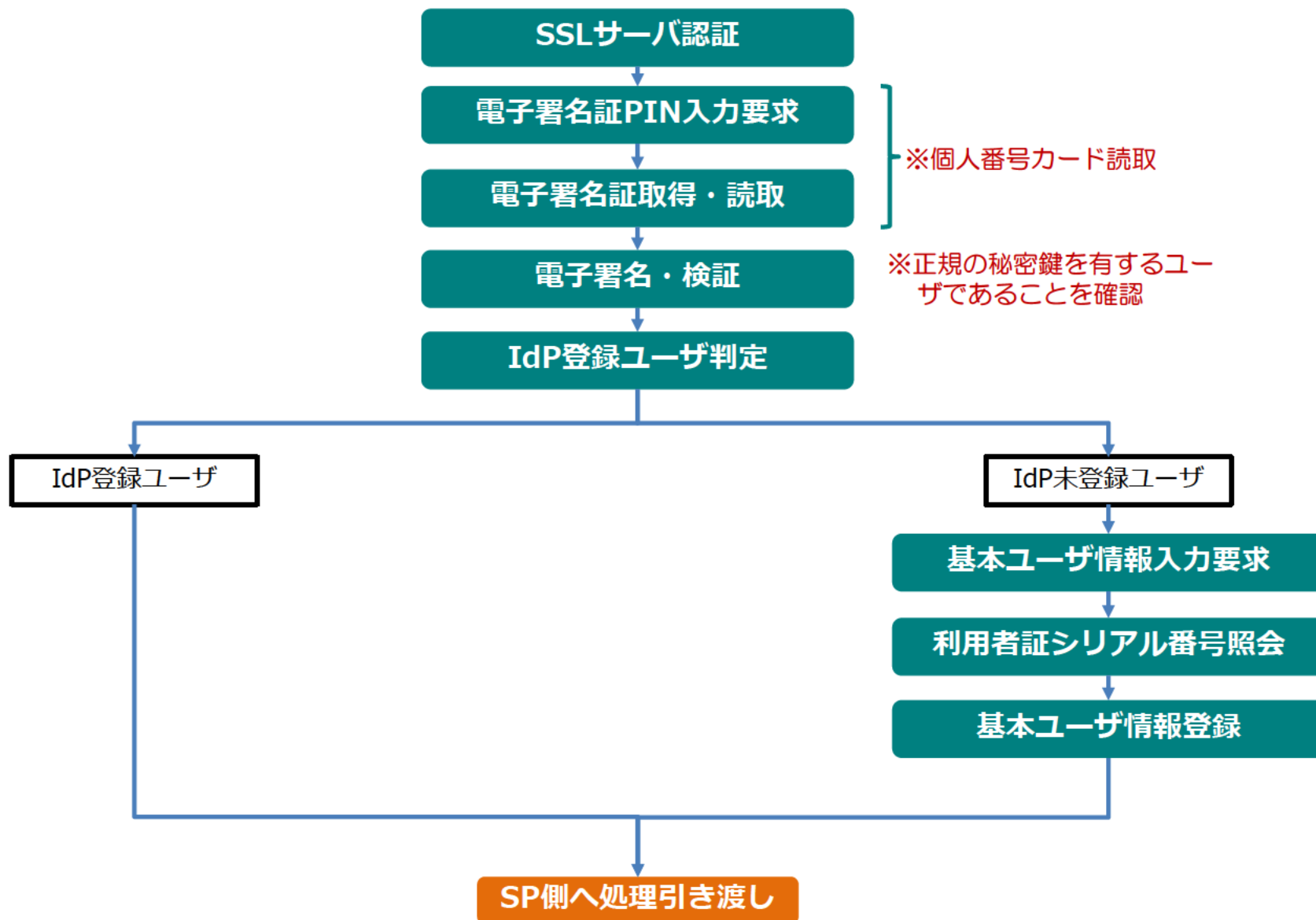
- ・ユーザが従前からID登録しているSPで、IdPへのユーザ登録が未だされていない状態でSPにアクセスされた際発生
- ・独自のID登録を行っているSP（B・Cタイプ）で、SPにユーザ登録した後、IdPへのユーザ登録が未だされていない状態でSPにアクセスされた際発生

ユーザ登録の主な流れ

以下は、SP側からユーザ登録を行う場合の主な処理の流れ。なお、SPを介さず、直接IdPにアクセスし、IdPのユーザ登録を行う場合は「IdP基本ユーザ情報登録」の完了によってユーザ登録終了



ユーザ登録（IdP側処理）



ユーザ登録時の I d P 登録ユーザの判定フロー

ユーザ登録時は、電子署名証のシリアル番号を用いて登録ユーザの判定処理を実施（認証時は、利用者証のシリアル番号を用いて登録ユーザの判定処理を行う）。既に登録ユーザである場合は、ユーザ登録処理を終了する。

※ここでいう登録ユーザは、IdPの登録ユーザであり、SPの登録ユーザ（正確には個人番号カードとの紐付けがされているSPの登録ユーザ）であるか否かは、IdPがSPに対して提供する連携管理IDを用いてSP側で判別

個人番号カードの電子署名証のシリアル番号をJPKIのOCSPレスポンスに問い合わせし、当該電子署名証の有効性を取得（※従前どおりCLR方式によるバッチ処理もあり得る）

利用者証が有効な場合

個人番号カードの電子署名証のシリアル番号
が基本ユーザ情報の既登録番号か確認

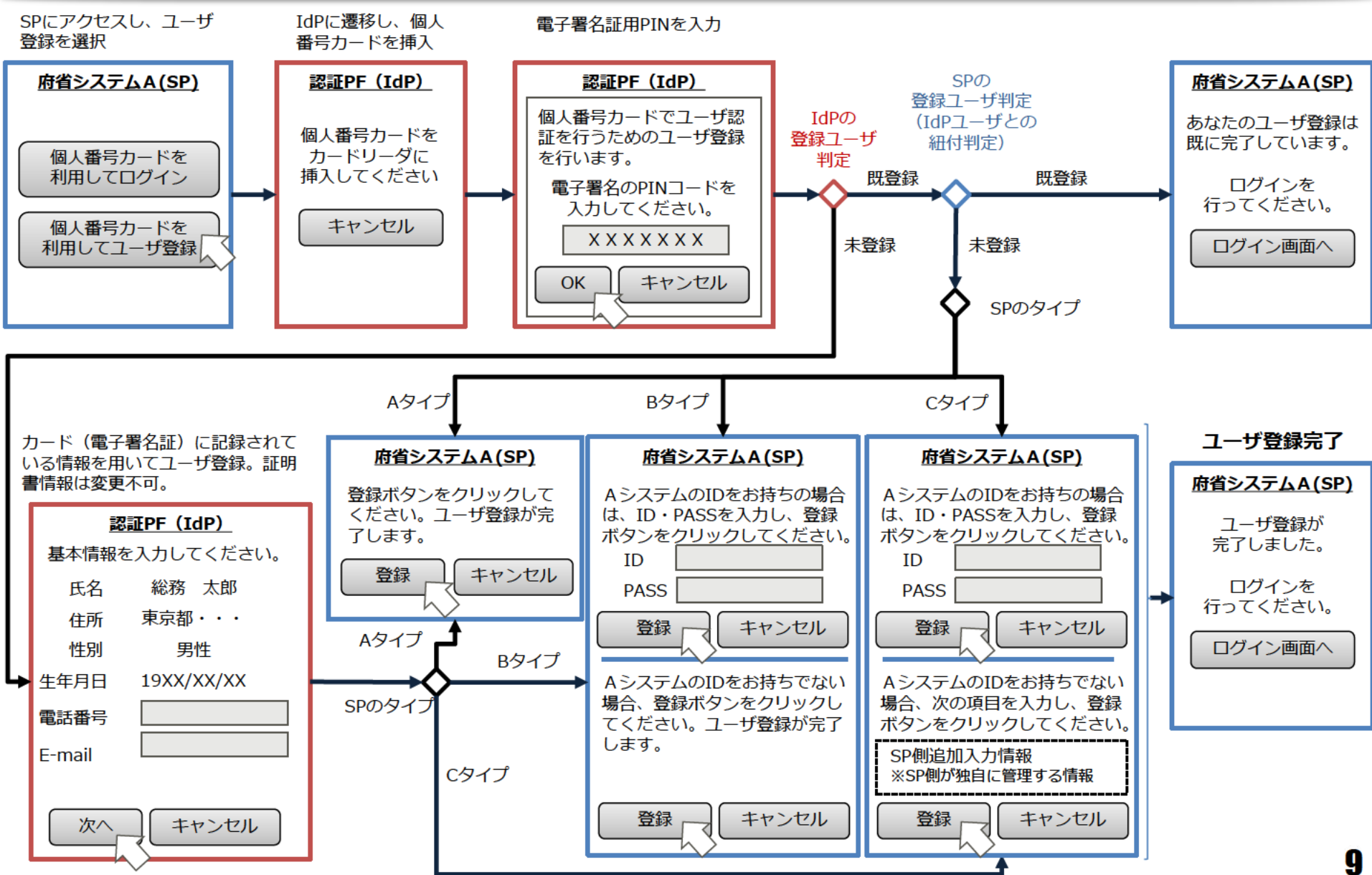
既登録番号

登録ユーザ

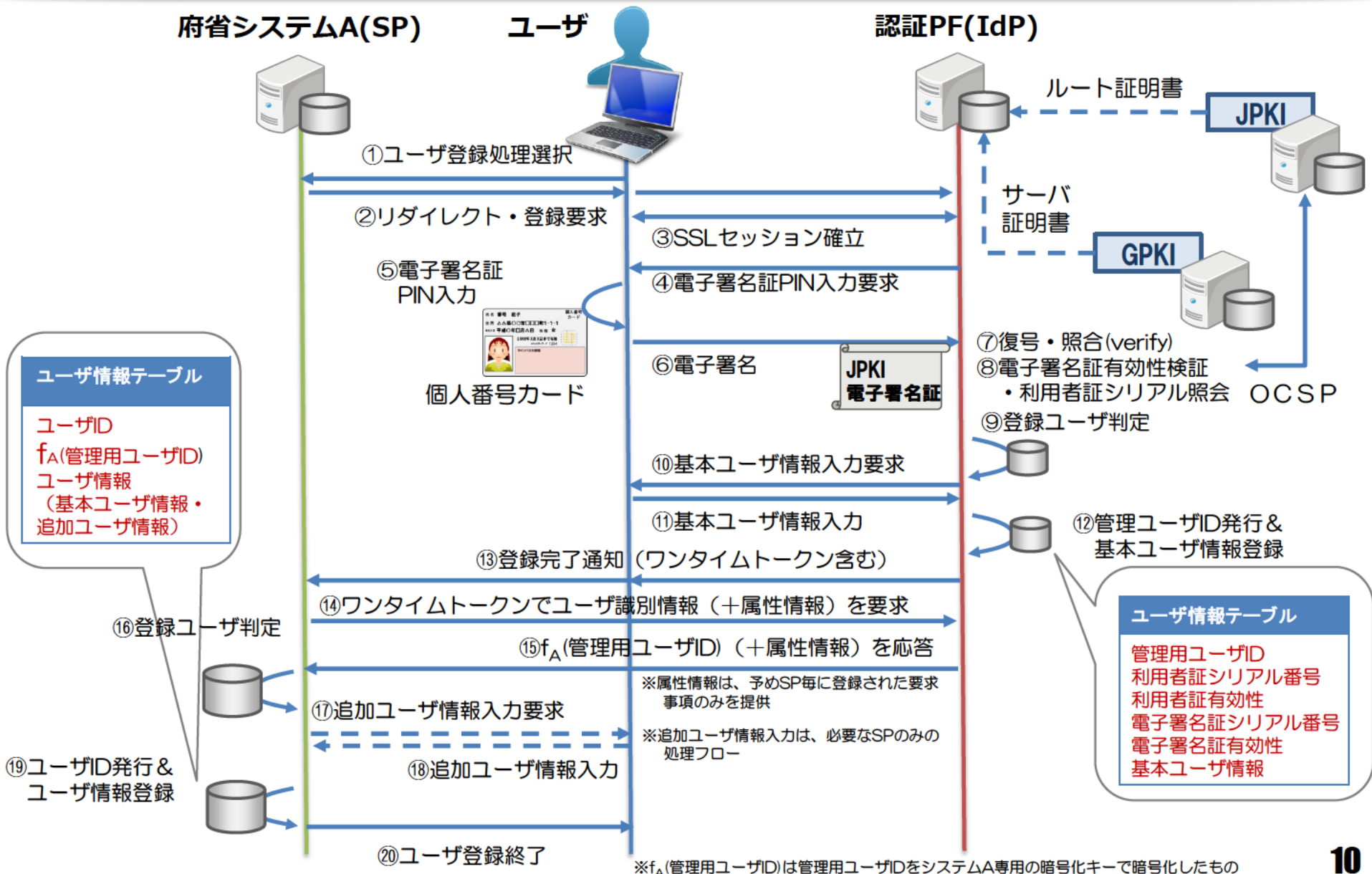
未登録番号

未登録ユーザ

ユーザ登録の画面遷移

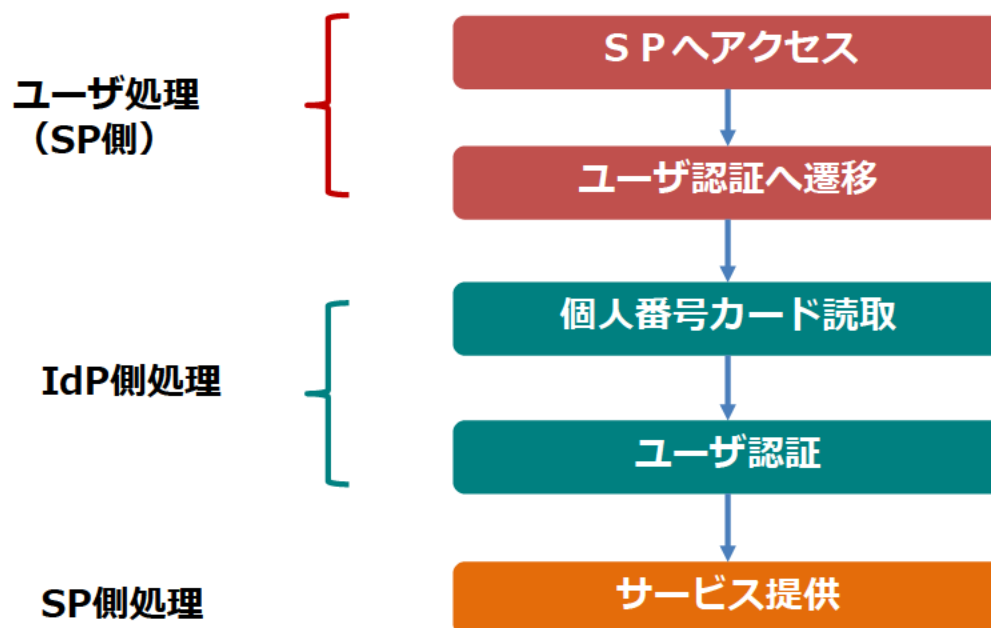


ユーザ登録のシーケンス



ユーザ認証の主な流れ

以下は、SP側から個人番号カードによるユーザ認証を行う場合の主な処理の流れ。
ユーザ認証は、SSLによるサーバ認証／暗号化に加え、利用者証を用いたクライアント認証を実施
この場合、ユーザ認証の実装方法については要検討。



ユーザ認証時の I d P 登録ユーザの判定フロー

SSLサーバ/クライアント認証時、利用者の有効性検証シーケンスの中に、登録ユーザの判定を組み込み、登録ユーザでない場合は認証処理を終了する。

※ここでいう登録ユーザは、IdPの登録ユーザであり、SPの登録ユーザ（正確には個人番号カードとの紐付けがされているSPの登録ユーザ）であるか否かは、IdPがSPに対して提供する連携管理IDを用いてSP側で判別

個人番号カードの利用者証のシリアル番号をJPKIのOCSPレスポンスに問い合わせし、

①当該利用者証の有効性、②前利用者証のシリアル番号を取得

①利用者証が有効な場合

個人番号カードの利用者証のシリアル番号が基本ユーザ情報の既登録番号か確認

既登録番号

未登録番号

基本ユーザ情報から当該シリアル番号が該当する管理用ID、電子署名証の有効性を取得

②前利用者証のシリアル番号が基本ユーザ情報の既登録番号か確認

既登録番号

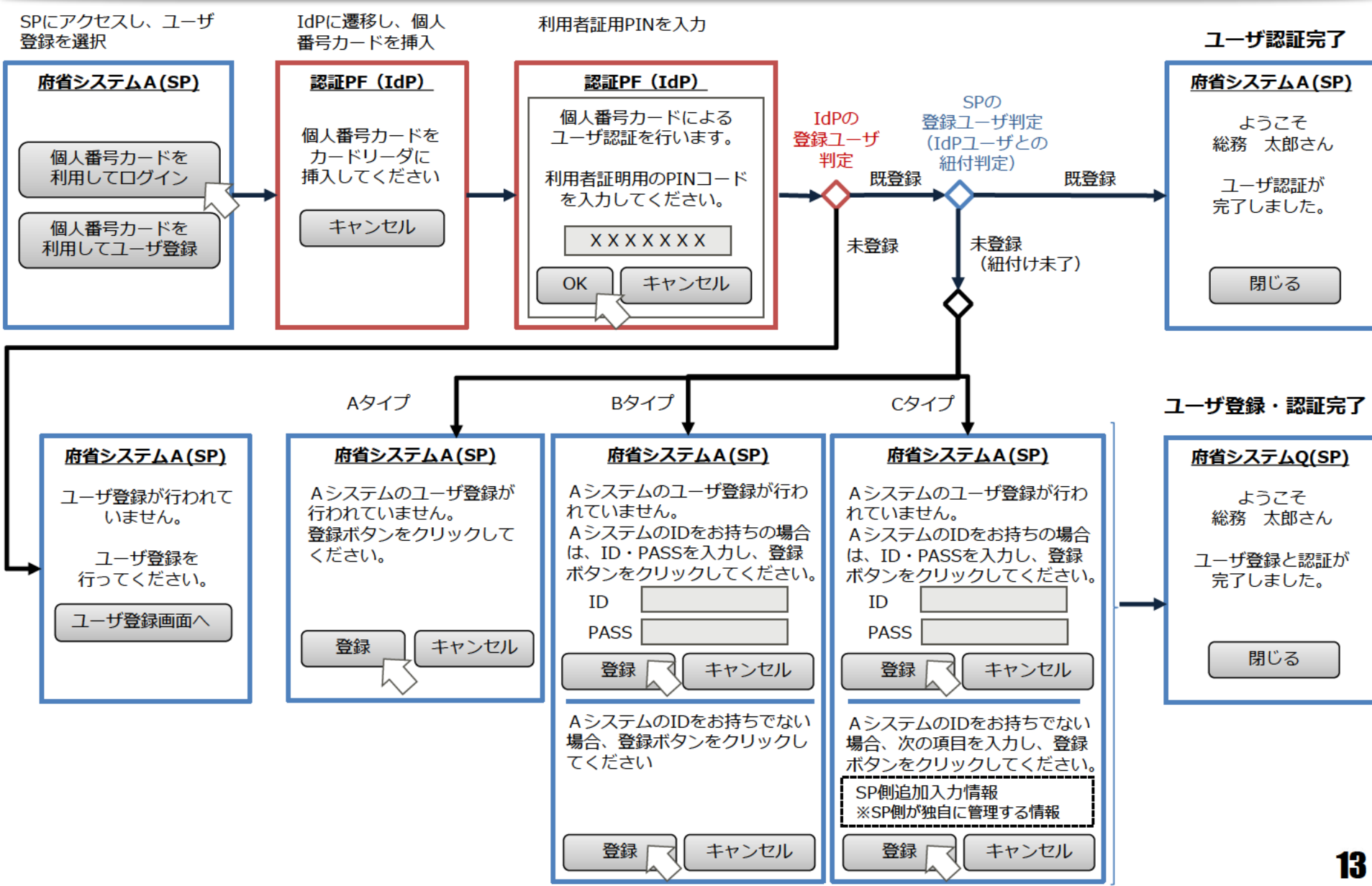
未登録番号

基本ユーザ情報に記録する利用者証のシリアル番号を個人番号カードから読み取ったシリアル番号に置換し、管理用ID、電子署名証の有効性を取得

登録ユーザ

未登録ユーザ

ユーザ認証の画面遷移



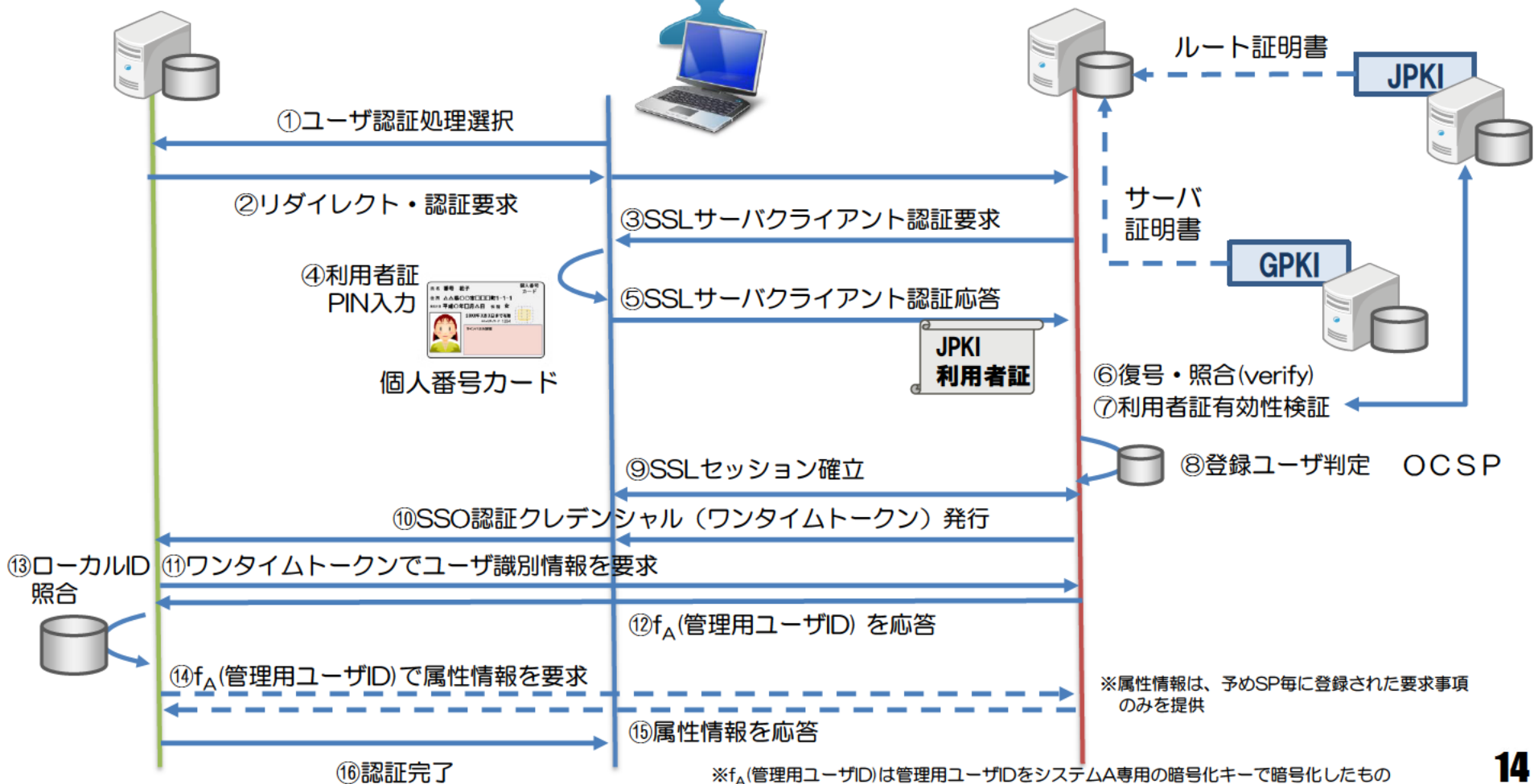
ユーザ認証のシーケンス

サービス利用を行うための初期段階の処理であるユーザ認証は、個人番号カードの利用者証明用秘密鍵及びその電子証明書（利用者証）を用いたSSLサーバ/クライアント認証によって実施

府省システムA(SP)

ユーザ

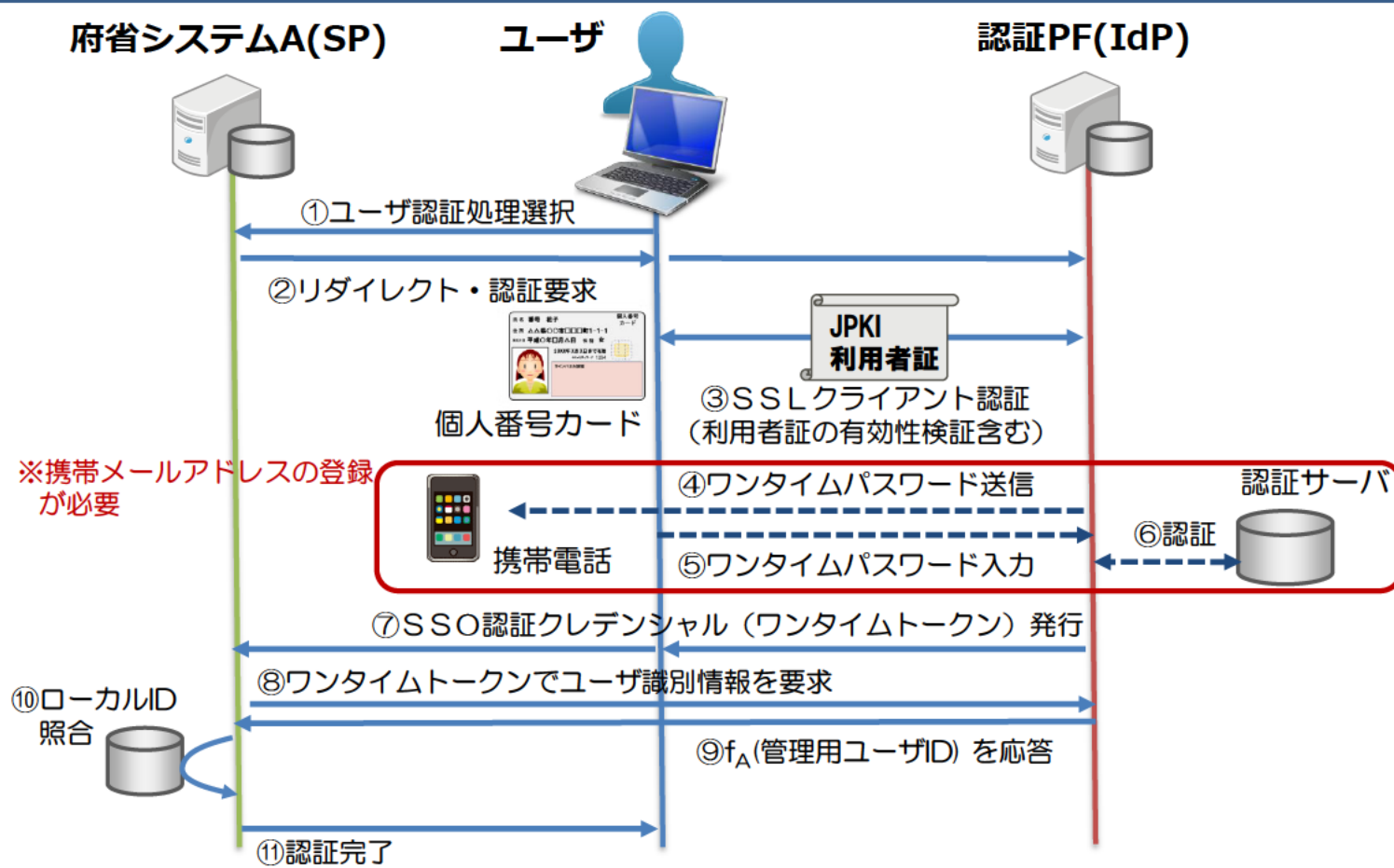
認証PF(IdP)



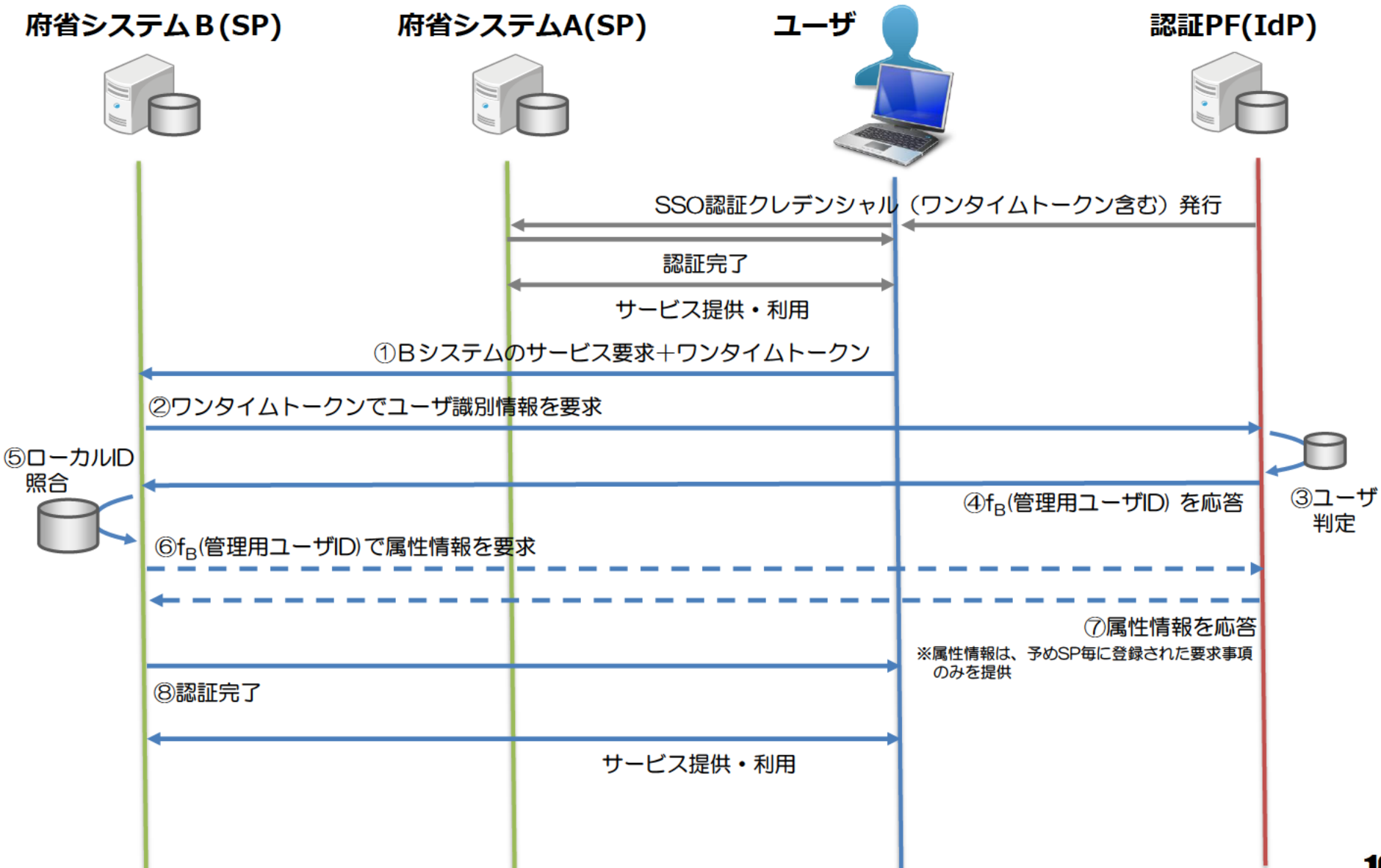
ユーザ認証の選択的セキュリティ強化

ユーザ認証のプシヨンの方式として、ユーザの選択により個人番号カードの認証に加えて、ワンタイムパスワード方式（将来的には生体認証など）を付加することができるようにし、ユーザ自身がセキュリティをより強固にすることを可能とする。

※将来的には、生体認証（サーバ方式）等も導入し、大規模災害等が発生した際には、行政での本人確認に活用できるようにすることが考えられる。

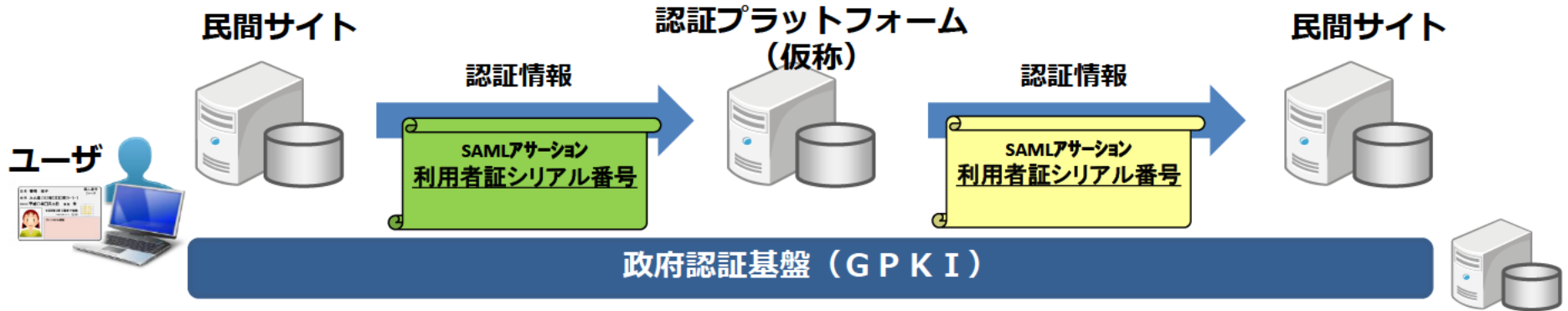


ユーザ認証のシーケンス (SSO)



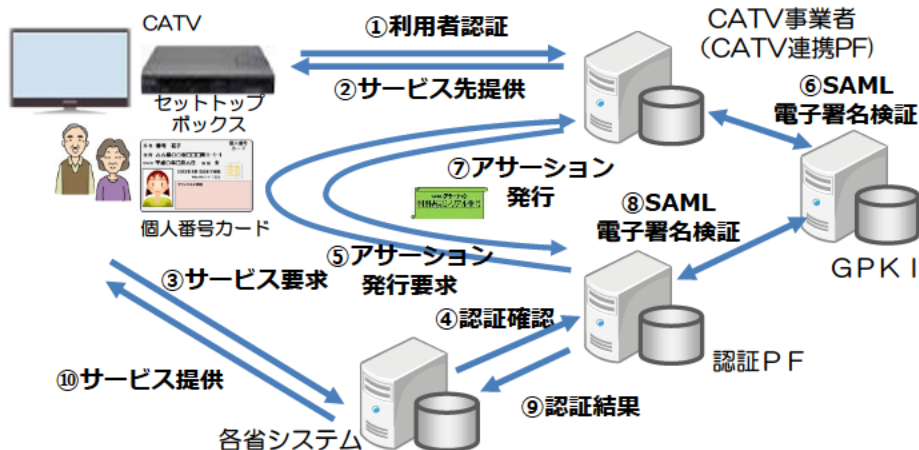
提携する民間サイトとの連携

政府認証基盤（GPKI）をトラストフレームワークプロバイダとし、個人番号カードによる利用者認証（Authentication）を認証プラットフォーム（仮称）と同等の方法で行う、信頼できる民間サイト・業界認証プラットフォームと連携し、SAMLをプロトコルに、個人番号カードによるシームレスなアクセス可能範囲を拡充



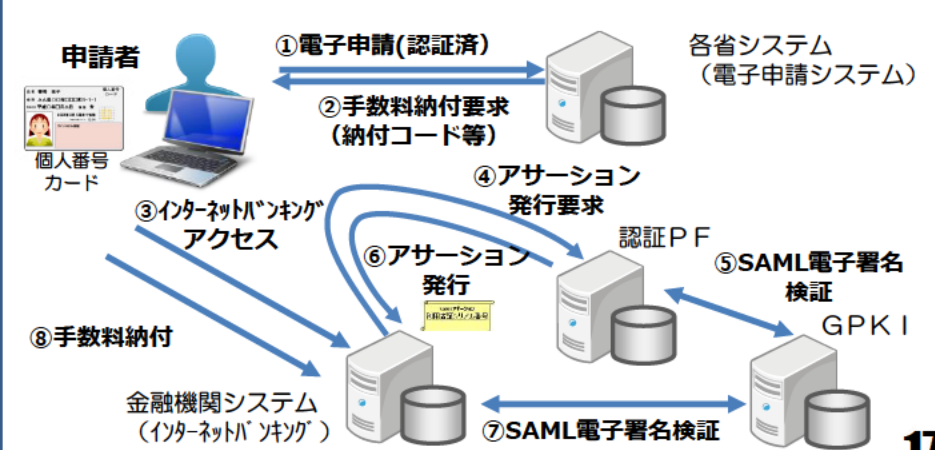
ケーススタディ（マルチチャネル化）

公的個人認証サービスの署名検証者であるCATV事業者と連携し、CATV画面から政府情報システムへのアクセスを実現

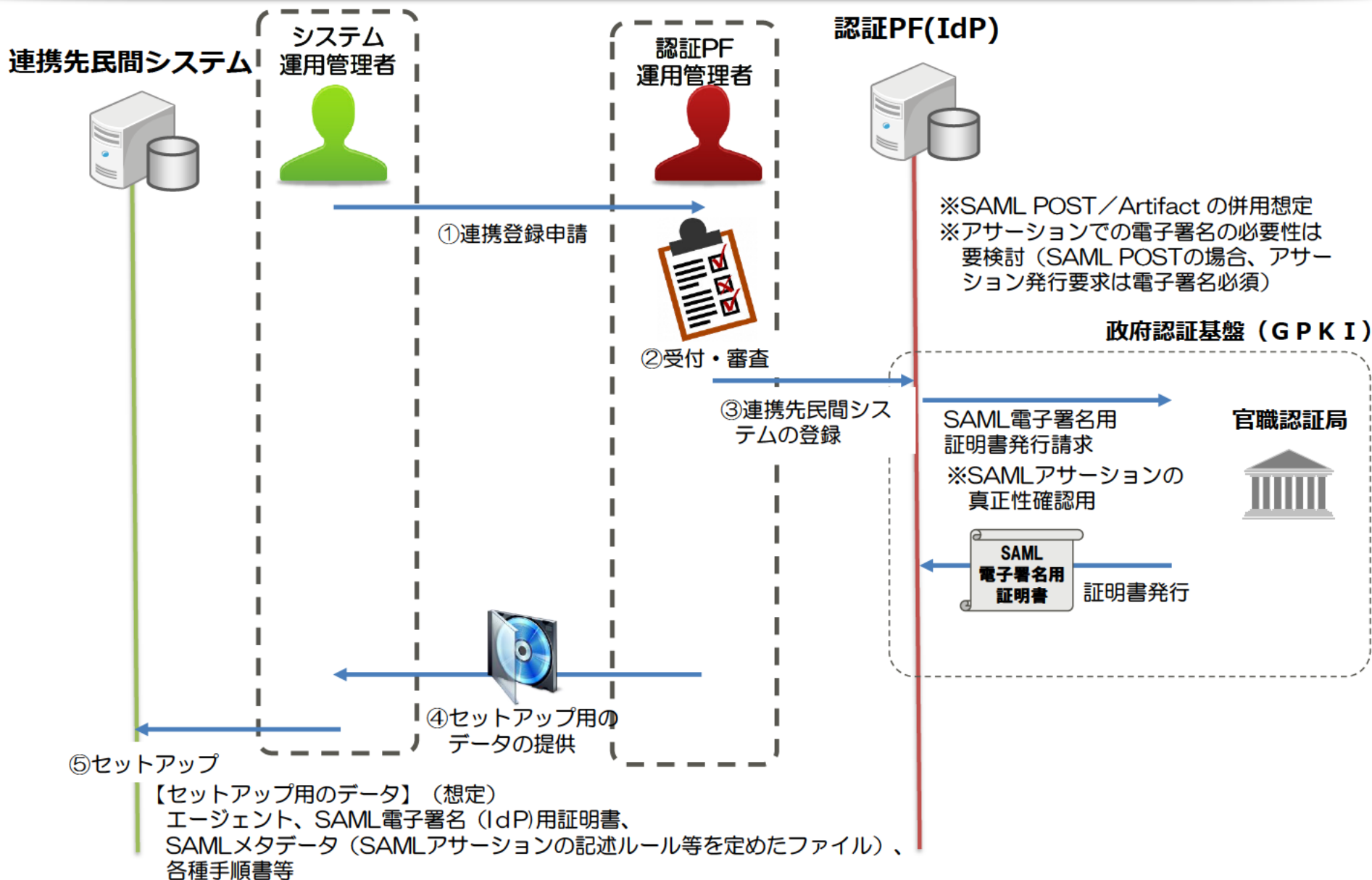


ケーススタディ（手数料納付）

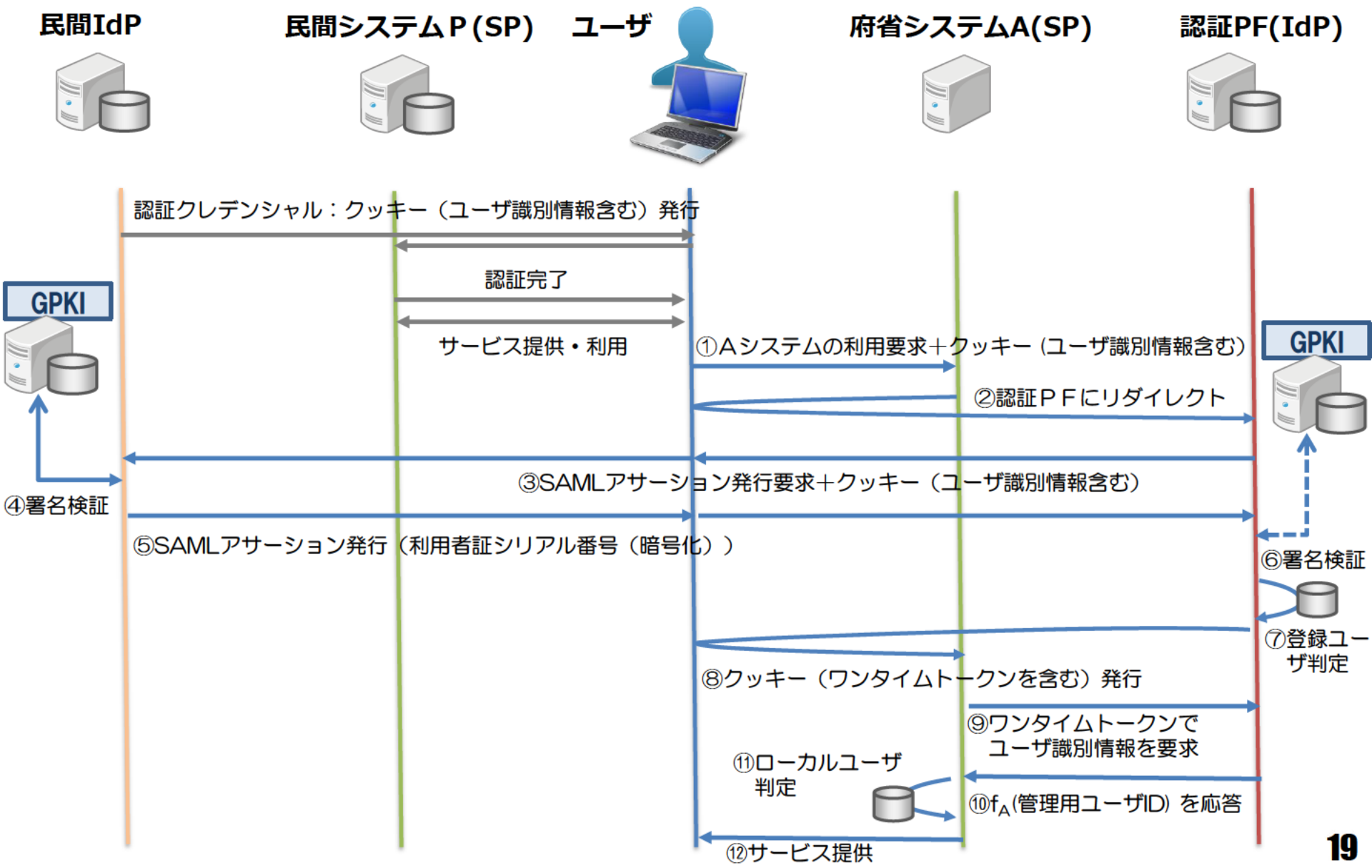
公的個人認証サービスの署名検証者である金融機関と連携し、電子申請の後、手数料納付するためのインターネットバンキングにシームレスに接続



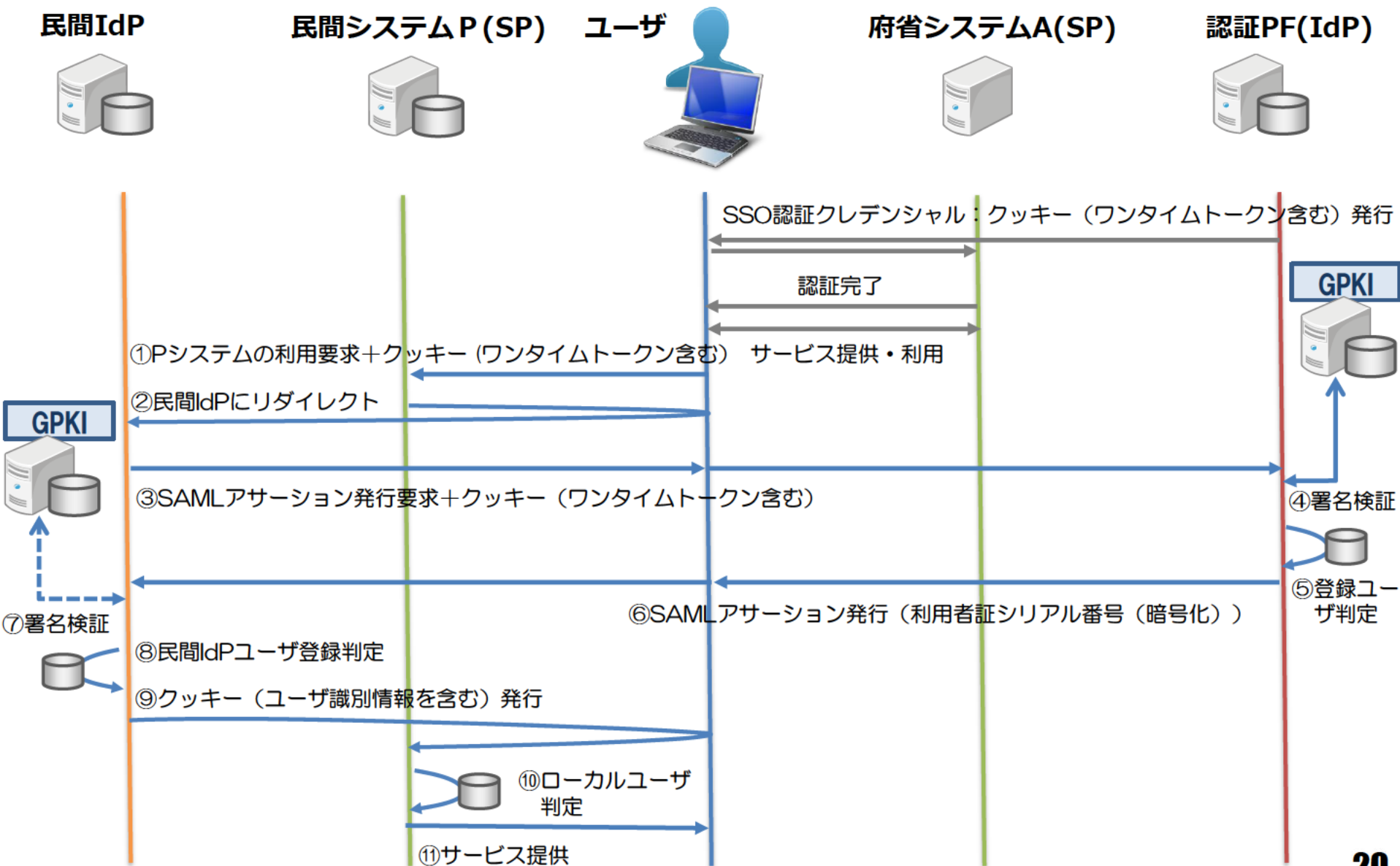
連携先民間システムの登録



ユーザ認証のシーケンス (官民連携) 民→官



ユーザ認証のシーケンス (官民連携) 官→民



電子署名の代替可能性

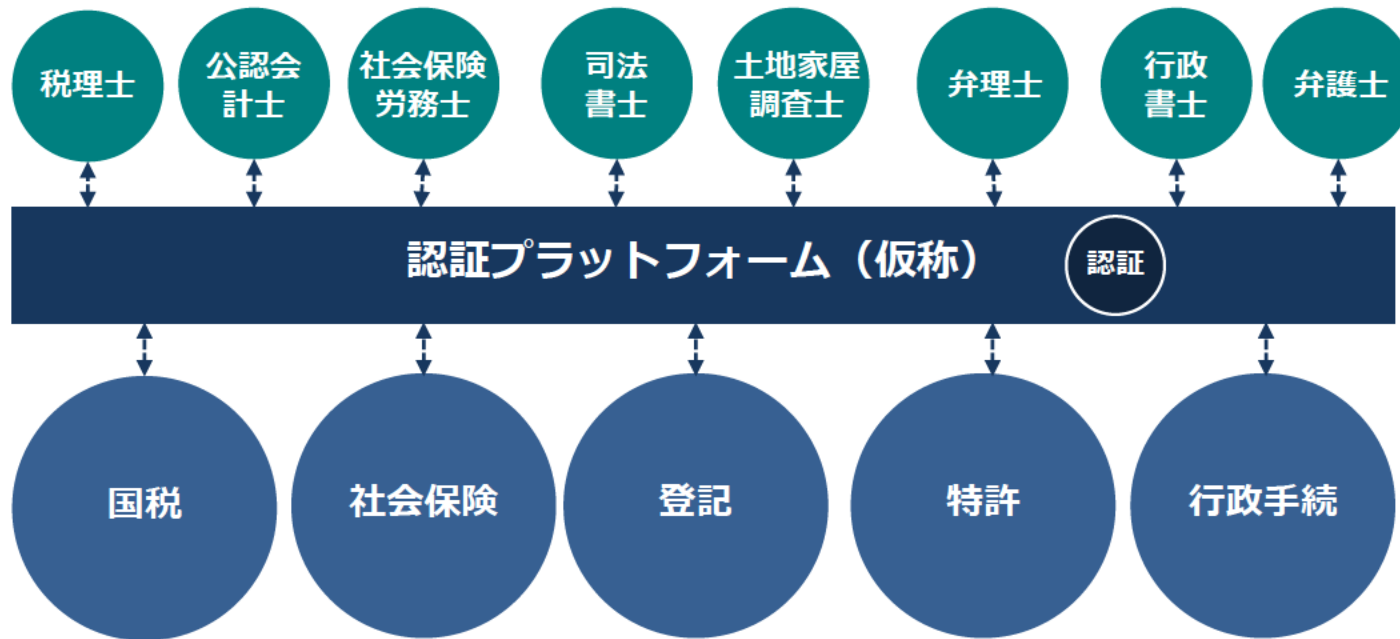
政府のオンライン申請では、電子署名を基本とし、一部の手続ではID方式を採用（電子署名の代替方法とされている）。認証プラットフォーム（仮称）による本人認証方式（「本方式」）では、電子署名に用いる電子証明書又はそれと個人番号カードの同領域に格納される電子証明書、さらにそれらに対応する秘密鍵を用いており、電子署名を代替可能と考えられる。

※各手続で要求されるLoA（保証レベル）によって方式の採否を判断する必要

要件	電子署名	本方式	ID方式
受信する情報が送信者本人によって作成・提出されたものであることを確保すること（成りすましの防止）	送信対象の情報に対し、PKIによる秘密鍵による暗号化を行うことによって確保	対象情報の送信を含む通信において、PKIによる秘密鍵による暗号化を用いた送信者の本人認証（PKIによるSSLクライアント認証通信）によって確保	対象情報の送信を含む通信において、ID（本人識別情報）及びパスワード等の認証によって確保
送信者が住民基本台帳に記載され、実存する本人であることを確保すること	電子署名とともに送信される公開鍵の電子証明書が、住民基本台帳を基に地方公共団体が発行した電子証明書であることで確保	認証の際に送信される公開鍵の電子証明書が、住民基本台帳を基に地方公共団体が発行した電子証明書であることで確保	ID登録手続において住民票の写しの提出によって確保 ※電子申請の多くは行っておらず、原則確保できていない
受信する情報が通信仮定において第三者による改ざんが行われていないことを確保すること	送信対象の情報に対し、PKIによる秘密鍵による暗号化を行うことによって確保 ※電子申請の多くは情報漏洩防止の観点から、SSL通信を行っており、それによって改ざんも防止	送信者との通信を、PKIによるSSL通信とすることによって確保	送信者との通信を、PKIによるSSL通信とすることによって確保

資格情報確認

政府情報システムの I d P では、各行政手続が士業者による代理・復代理申請が行われるため、ワンカード化を実現するためには、カード所有者の本人認証だけでなく、士業資格等の資格・属性認証を行えるモデル構築と機能実装が必要



各省システム
(資格確認を行うSP)



① 資格認証要求



④ 資格認証結果返答

認証プラットフォーム
(仮称)



② 資格確認要求



③ 資格確認結果返答

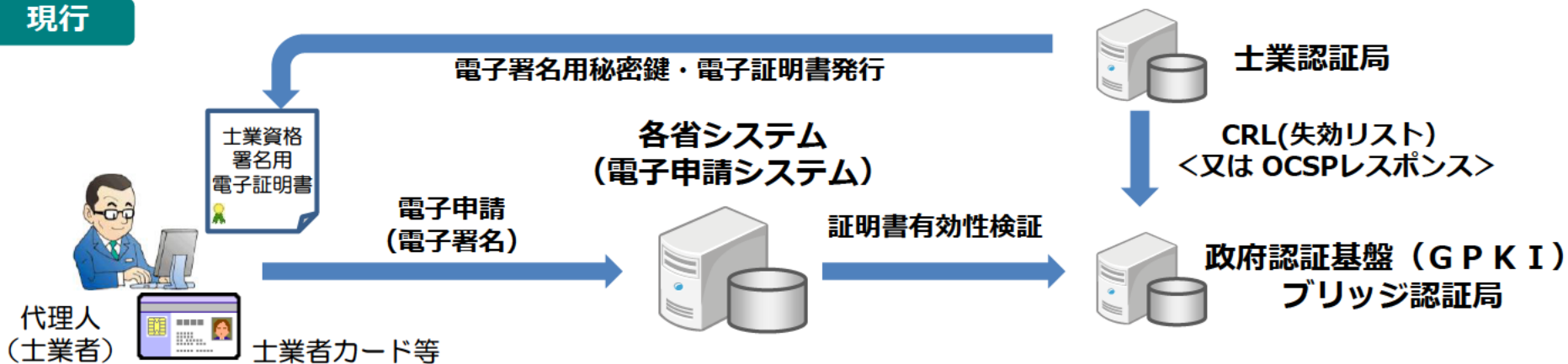
資格認証機関



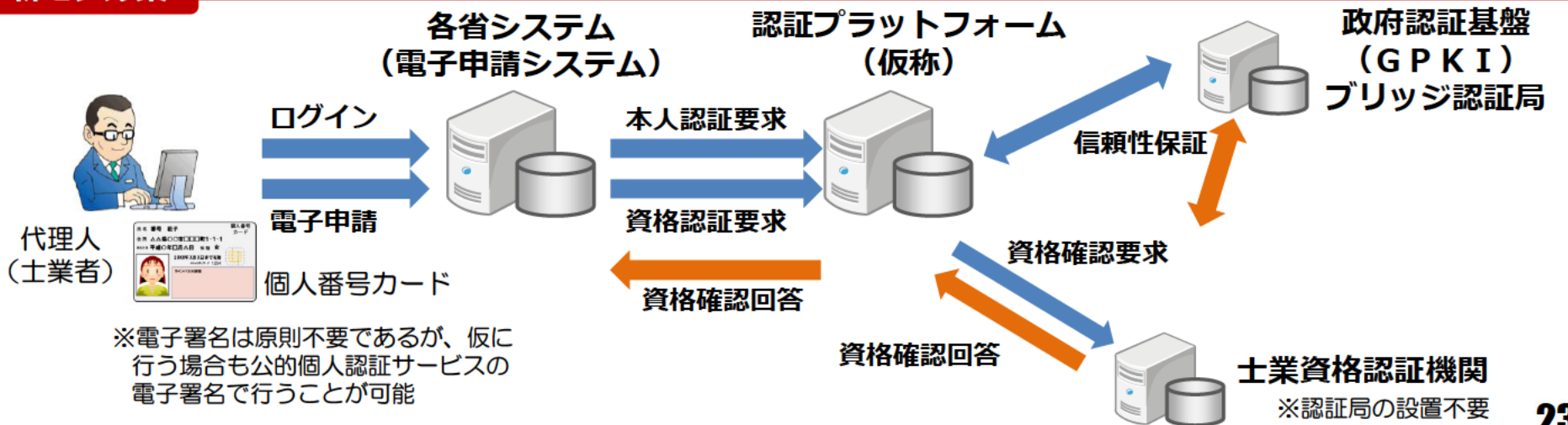
資格情報確認（応用：代理申請）

これまで士業者が代理申請を行う場合、士業資格で電子署名をするために特別のPKIを必要としていたが、認証プラットフォームで資格情報確認を代表して行うことで、特別のPKIを用いずとも簡便な方法で資格確認を行うことも可能となり、ワンカード化も実現。〈要検討・調整〉

現行



新モデル案



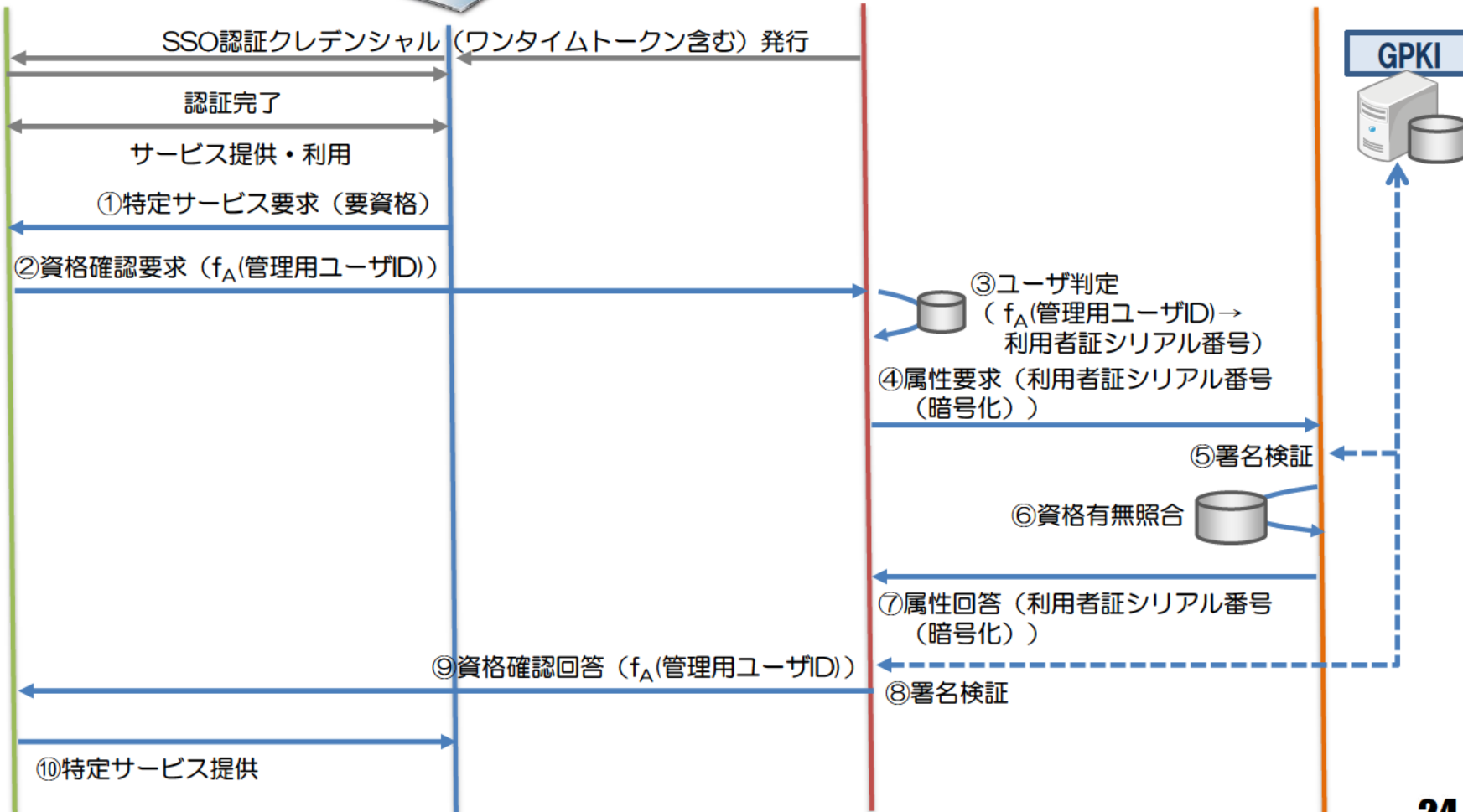
資格認証のシーケンス

府省システムA(SP)

ユーザ

認証PF(IdP)

資格認証機関(AP)

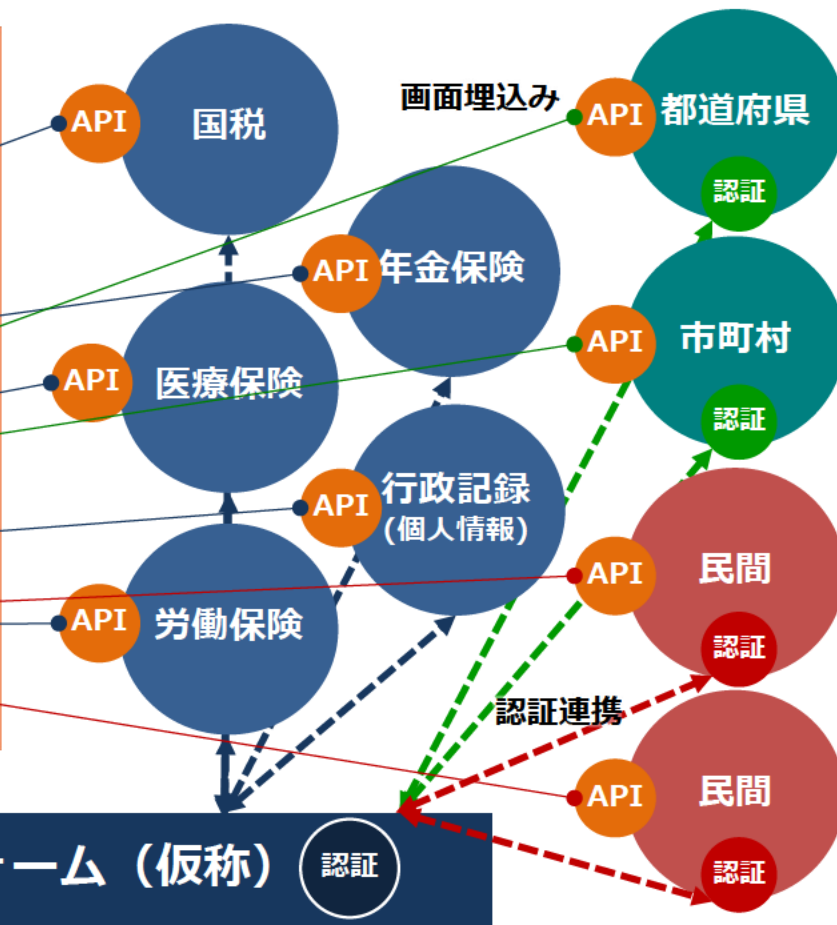
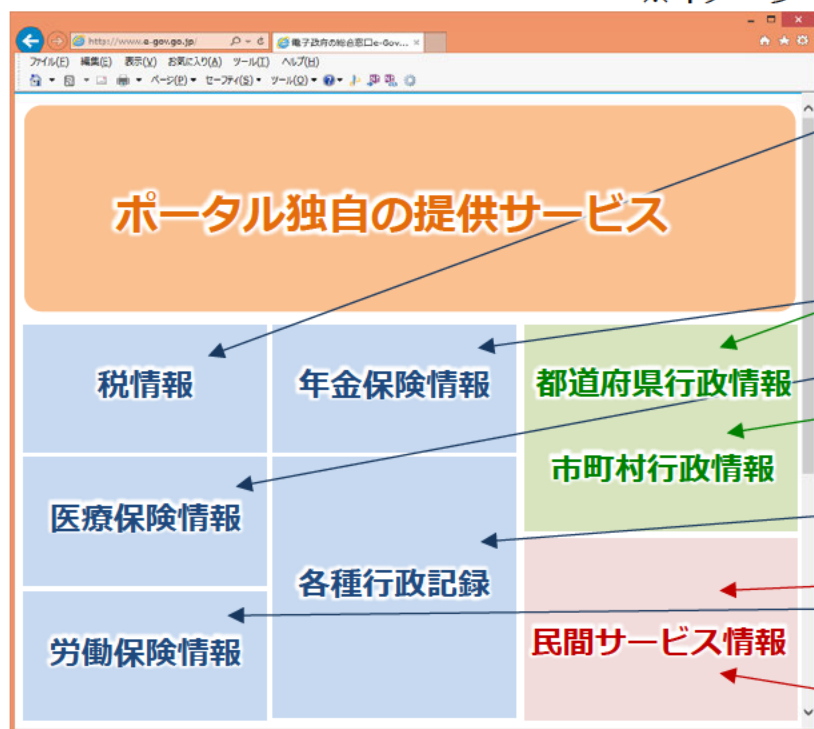


ポータル機能との連携

SPに埋め込み型ページのAPIを用意することで、ユーザが選択・設定する関係SPに一斉ログインし、当該ユーザに関する行政情報・公共サービス情報の一括表示（シングルウィンドウ化）する個人向けポータルのサービス提供が考えられる。

【個人向けポータルサービス】

※イメージ



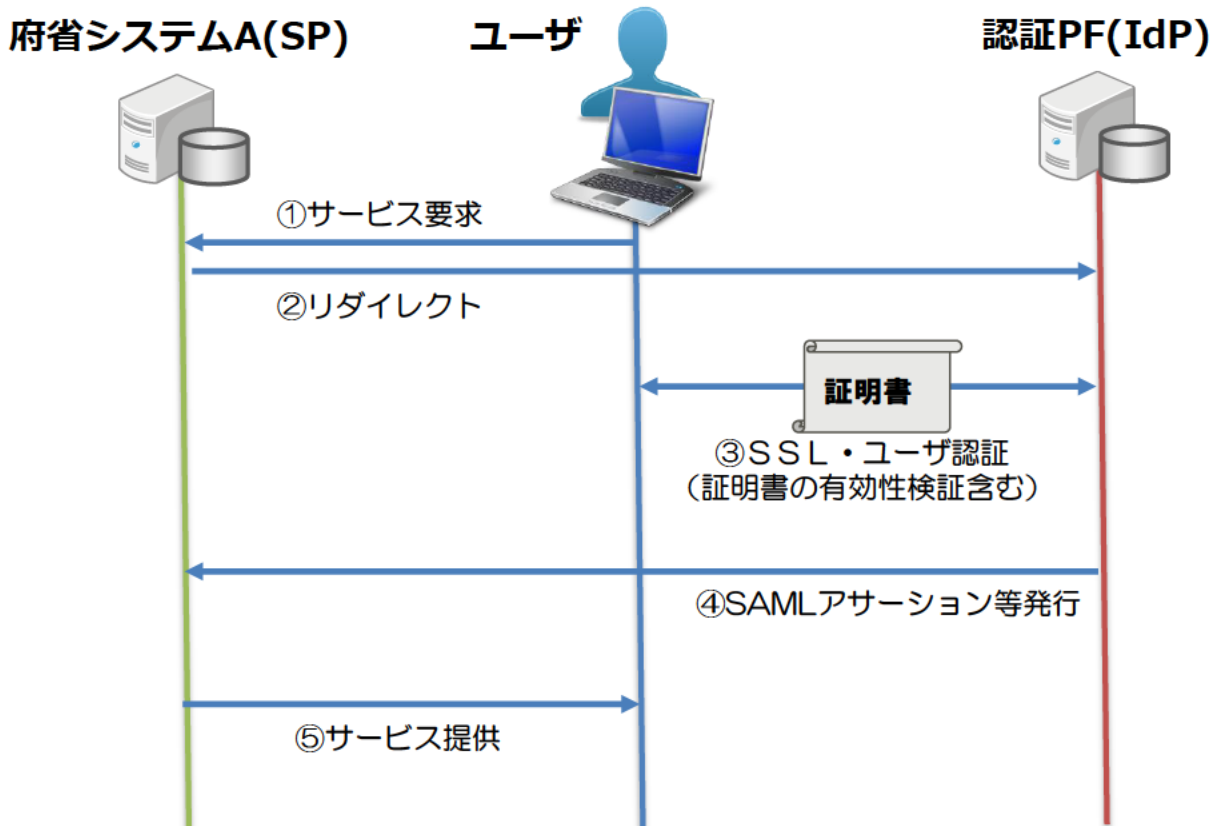
一括認証

認証プラットフォーム (仮称)

認証

法人認証について

オンライン申請では申請者が法人（代表者）である場合があり、個人番号カードによる個人認証のほか、法人認証についても要検討。具体的な方法は個人番号カードによる個人認証と同じであるが、基本とする認証サービスは、電子認証登記所(商業登記認証局)その他法人職員を対象として電子証明書を発行する、政府認証基盤（GPKI）と相互認証を行っている認証サービスが候補。



※fA(管理用ユーザID)は管理用ユーザIDをシステムA専用の暗号化キーで暗号化したもの