資料６－５

認証プラットフォーム（仮称）について
＜未定稿＞

平成27年２月18日
総務省行政管理局

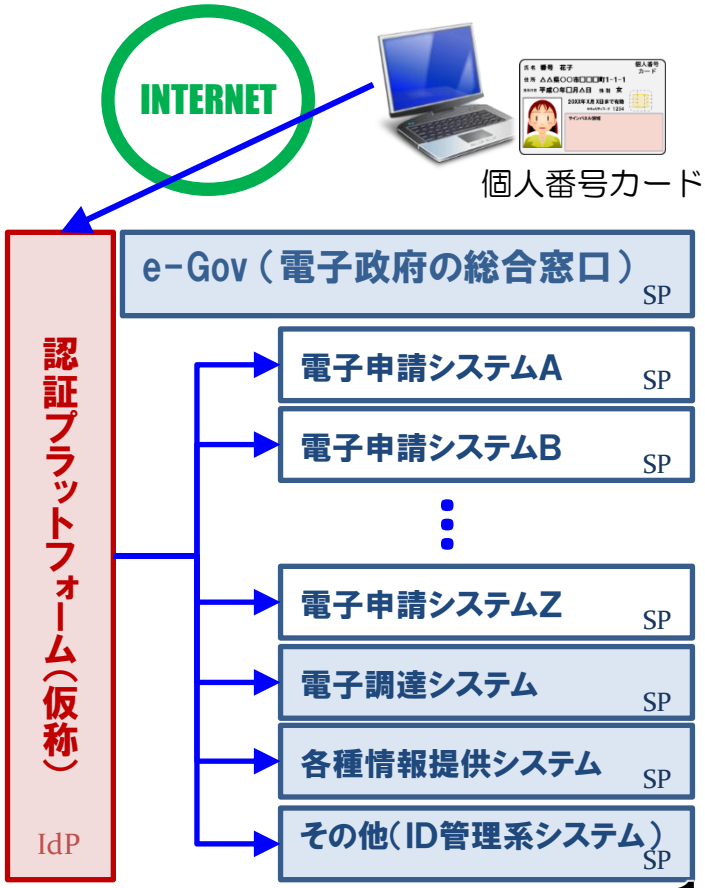
認証プラットフォーム（仮称）概要

○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



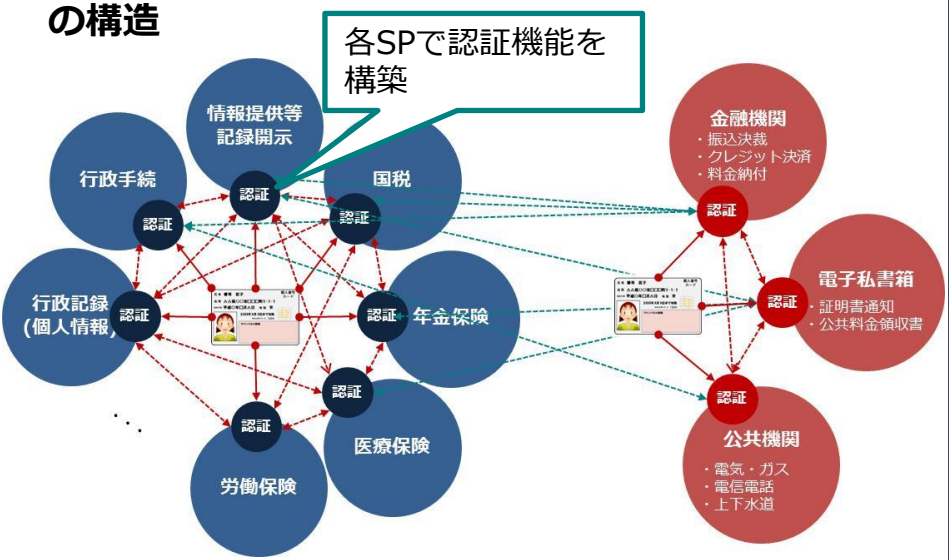
※IdP：Identity Provider、SP：Service Provider

政府情報システムにおけるＩｄＰの有用性①

個人番号カードにより、従来のＩＤ／ＰＷとは異なる強固なアクセスセキュリティを確保可能。
これにより、従前に比べ、プライバシー情報を伴う情報提供（行政記録開示）、行政手続、決済処理などのオンラインサービスを拡大させ、行政サービスの利便性を向上させる取組が可能。
その実現のために政府内にＩｄＰを構築することで、重複投資を回避することができ、官官・官民で相互連携する際に、メッシュ型の複雑な構造を回避し、効率的なシステム体系とすることが可能。

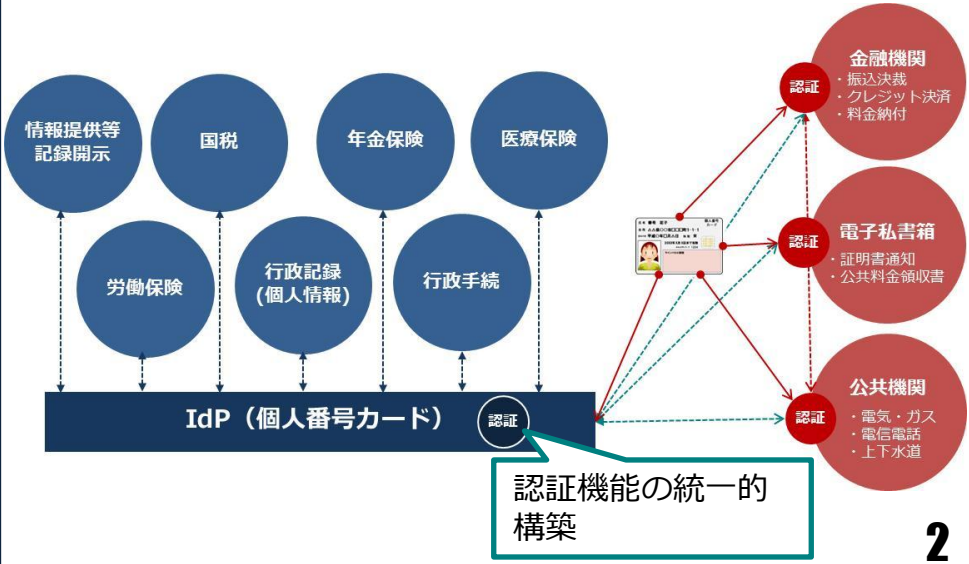
【ＩｄＰがない場合】

- **各省システム（ＳＰ）のそれぞれで認証機能を構築する必要。**
- **官民連携を行う場合、各省のシステムと民間システムがそれぞれ個別に連携関係を構築するメッシュ型の構造**



【ＩｄＰがある場合】

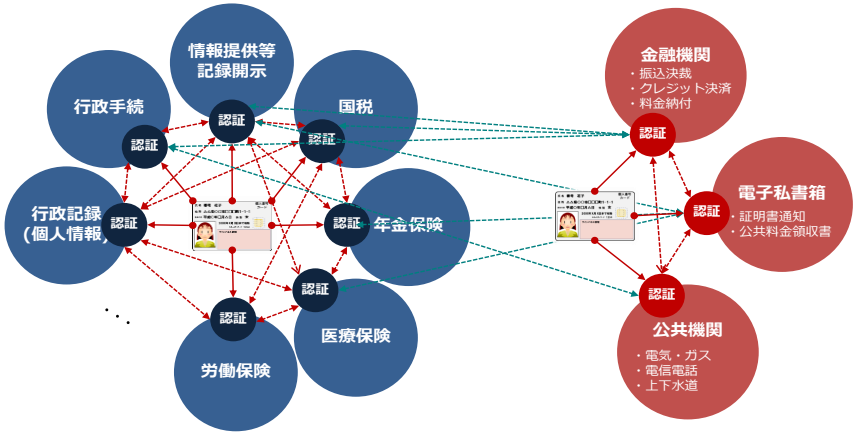
- **各省システム（ＳＰ）側での重複した投資を抑制し、政府内でスター型の認証連携を構築可能**
- **民間との連携を代表して行うことで、官民相互の連携をブリッジし、効率的なシステム体系を構築可能**



政府情報システムにおけるＩｄＰの有用性②

本人認証の仕組みは、技術進展によって、将来、個人番号カードからさらに進んだ新しい認証デバイス・方法が実装可能になる可能性大。ＩｄＰによって、効率的かつ柔軟に、政府情報システム全体に新しい認証技術の導入・転換が可能。

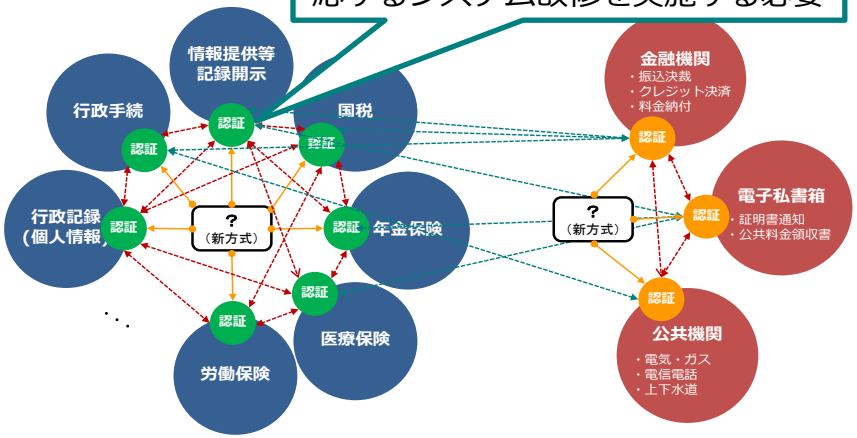
【ＩｄＰがない場合】



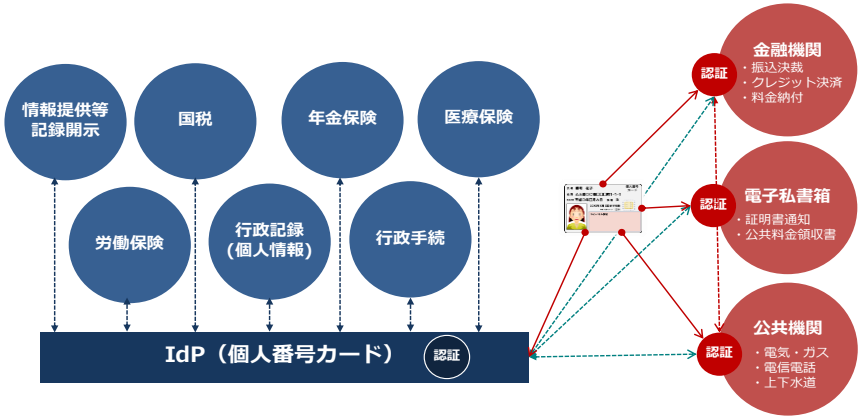
技術進歩

(将来)

すべての情報システムで新技術に適応するシステム改修を実施する必要



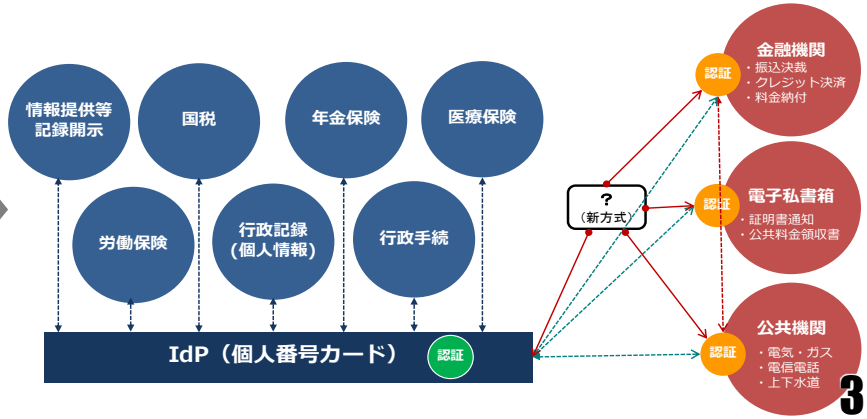
【ＩｄＰがある場合】



技術進歩

(将来)

※ＩｄＰのみ新技術に適応する改修を行い、ＳＰとの仕組みはそのまま継続

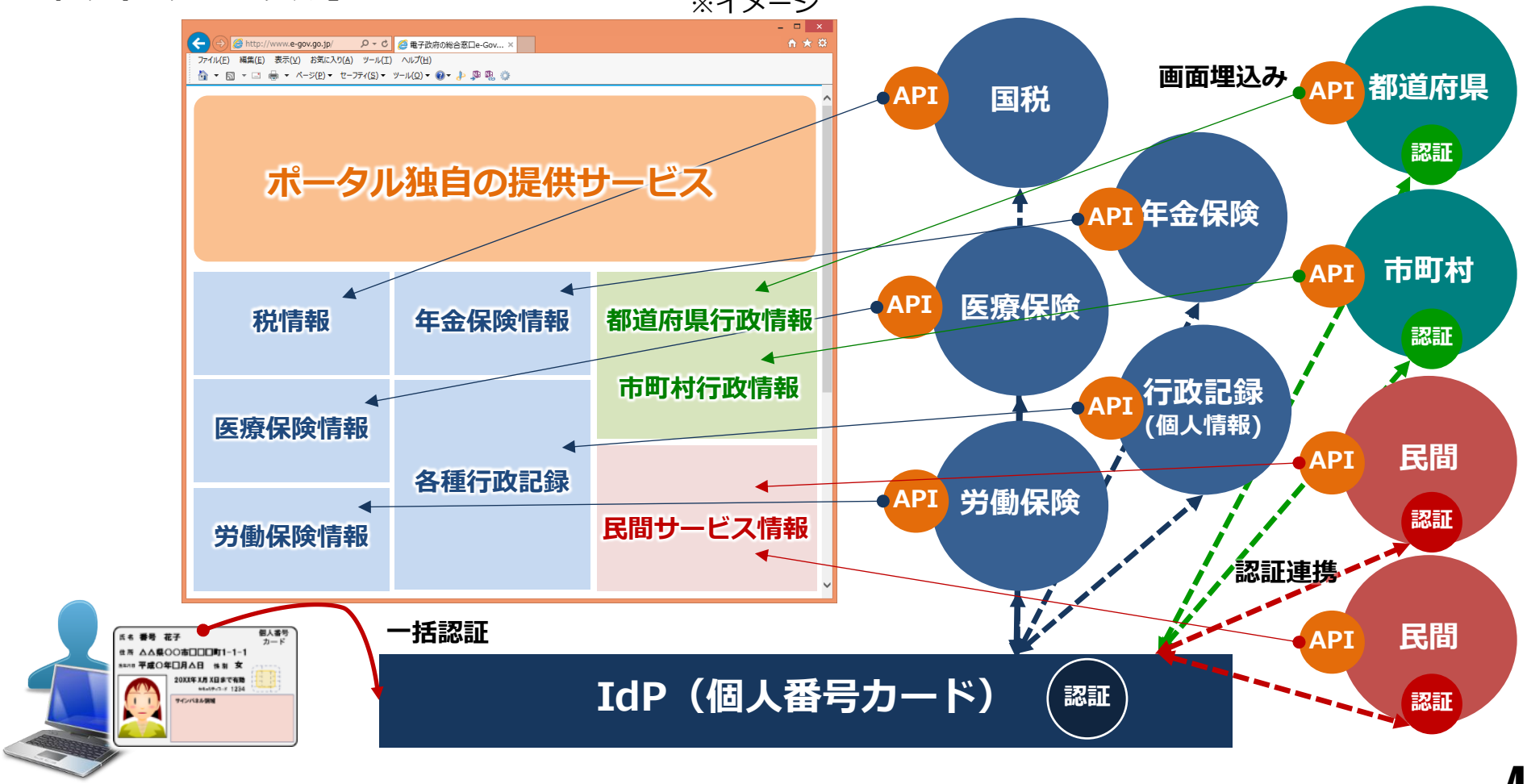


政府情報システムにおけるＩｄＰの有用性③

IdPと、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・民間サービス情報を一括表示（シングルウィンドウ化）する個人向けポータルサービスの提供可能性にもつながる。

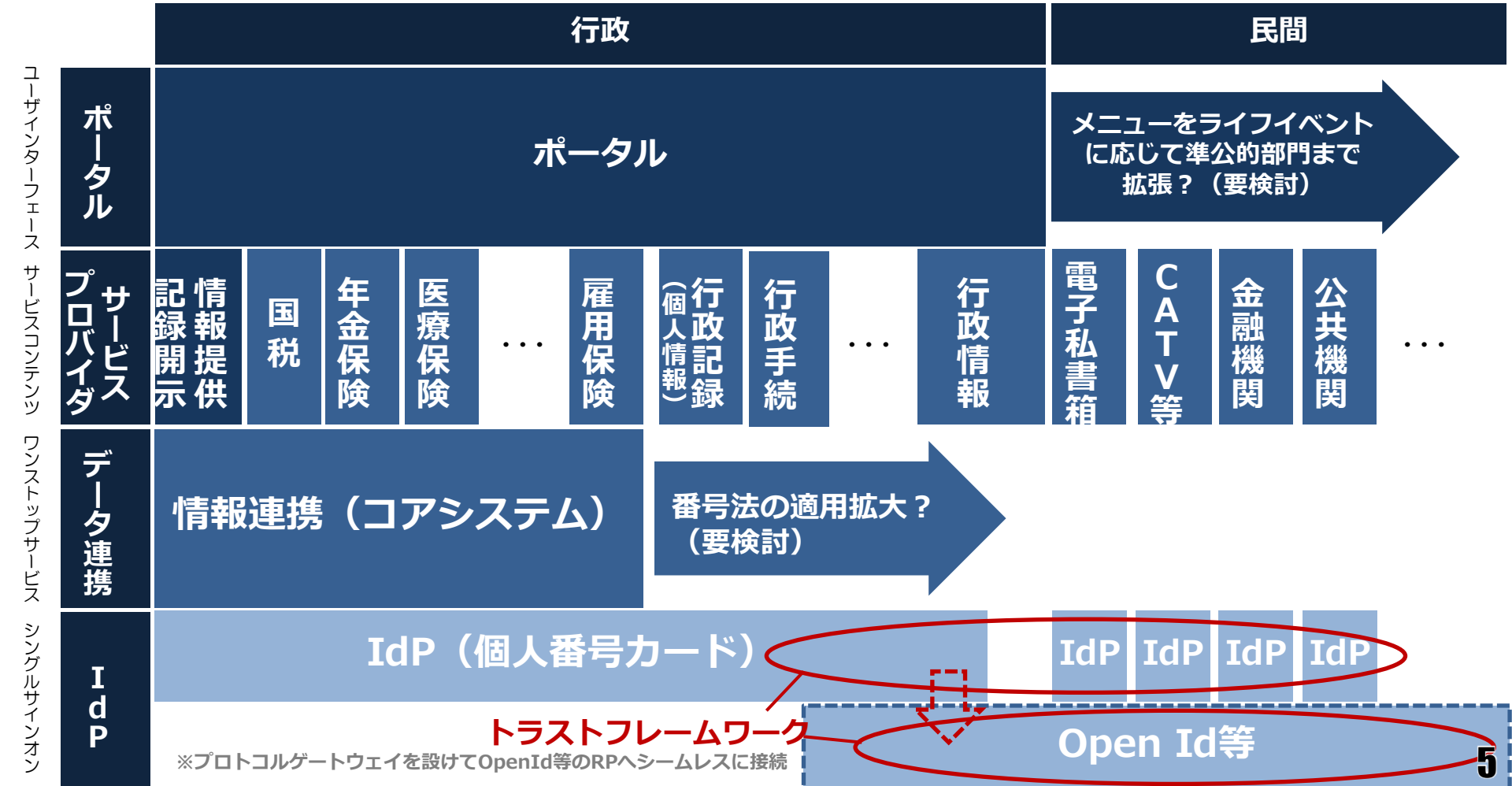
【個人向けポータル】

※イメージ



電子政府のサービスとＩｄＰ<イメージ>

電子政府のサービス全体のシステム設計を、①ポータル、②サービスプロバイダ、③データ連携、④ＩｄＰ（認証プロバイダ）を要素として、グランドデザインを描くことが肝要ではないか。その際、各提供サービスをシームレスに連結させるため、官官・官民のシステム間をつなぐＩｄＰとトラストフレームワークの構築が重要。



政府情報システムのＩｄＰ整備の留意要件

○政府内のIdPとSP間のID連携は、セクトラルモデルで構築

○属性・権限認証はIdPから分離（IdPは本人認証（存否確認）に特化。分散管理モデル）し、IdPと連携するこれらの認証モデル・シーケンスを確立

○公的個人認証サービスの証明書更新時に、ユーザ登録の再設定を各SPで行う必要のないユーザビリティ

○民間IdP・民間SPとの認証連携には、SAML等の標準的なプロトコルを採用

※取組上の留意点として考えられる事項

○IdPだけを構築しても意義はなく、各府省のSPの改修とセットで統一的に取り組むことが必要

○行政手続には属性・権限認証（士業資格等）も必要となるものがあり、業界とも連携の上、SP側アプリの構築を進めることが肝要

○個人番号カードによる認証を、従来のＩＤ・パスワードによる認証方式の代替方法として取り組むのではなく、これまでの方式では提供されていなかった新しい情報提供サービスを創出する取組の展開が肝要（※ポータルとも密接に関連）

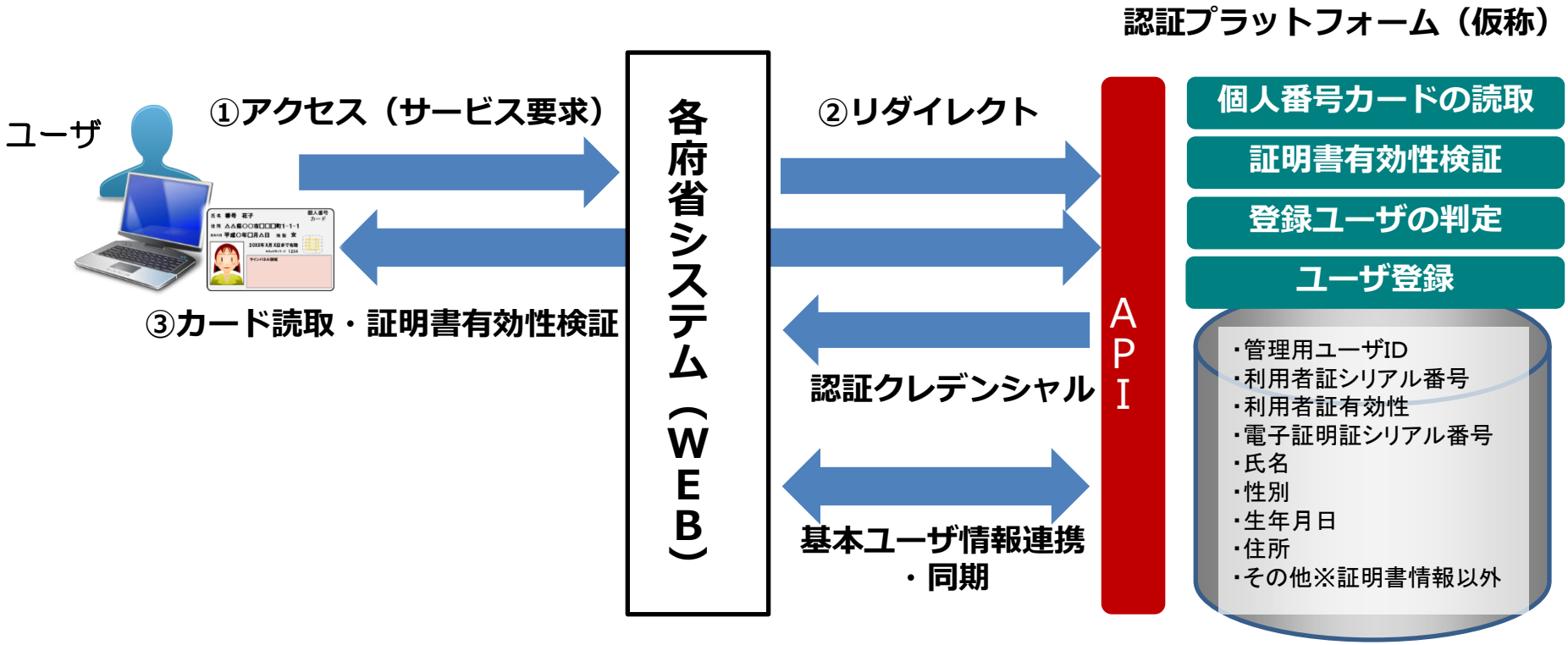
認証プラットフォーム（仮称）基本ユーザ情報

認証フラットフォーム（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）

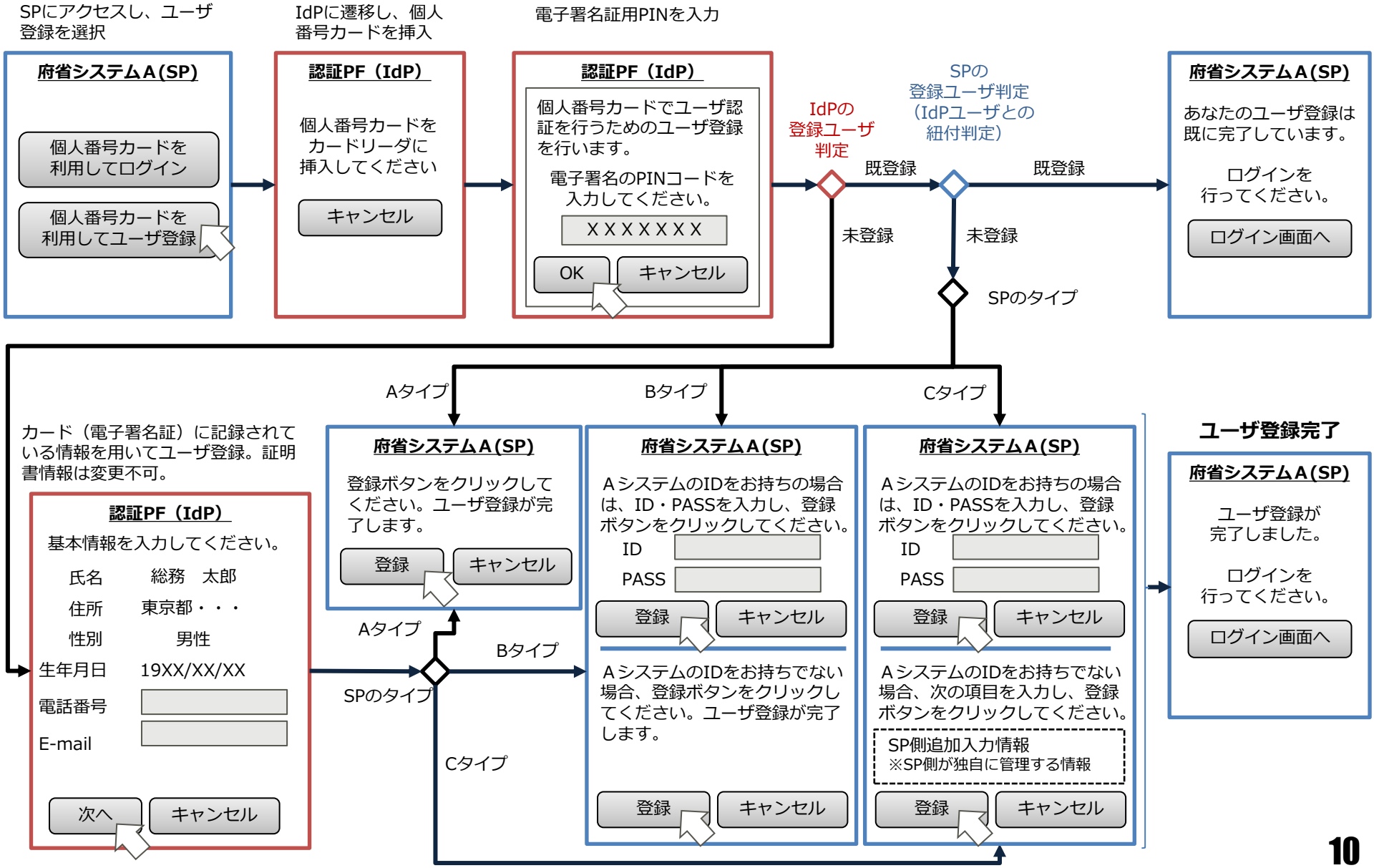
認証プラットフォーム（仮称）の機能については、ＡＰＩを装備し、各府省等に連携・開発ツールとして提供。効率的な設計・開発を促し、政府全体の開発コストを抑制するとともに、利用者に対し、統一された利用し易いインターフェイスを提供。



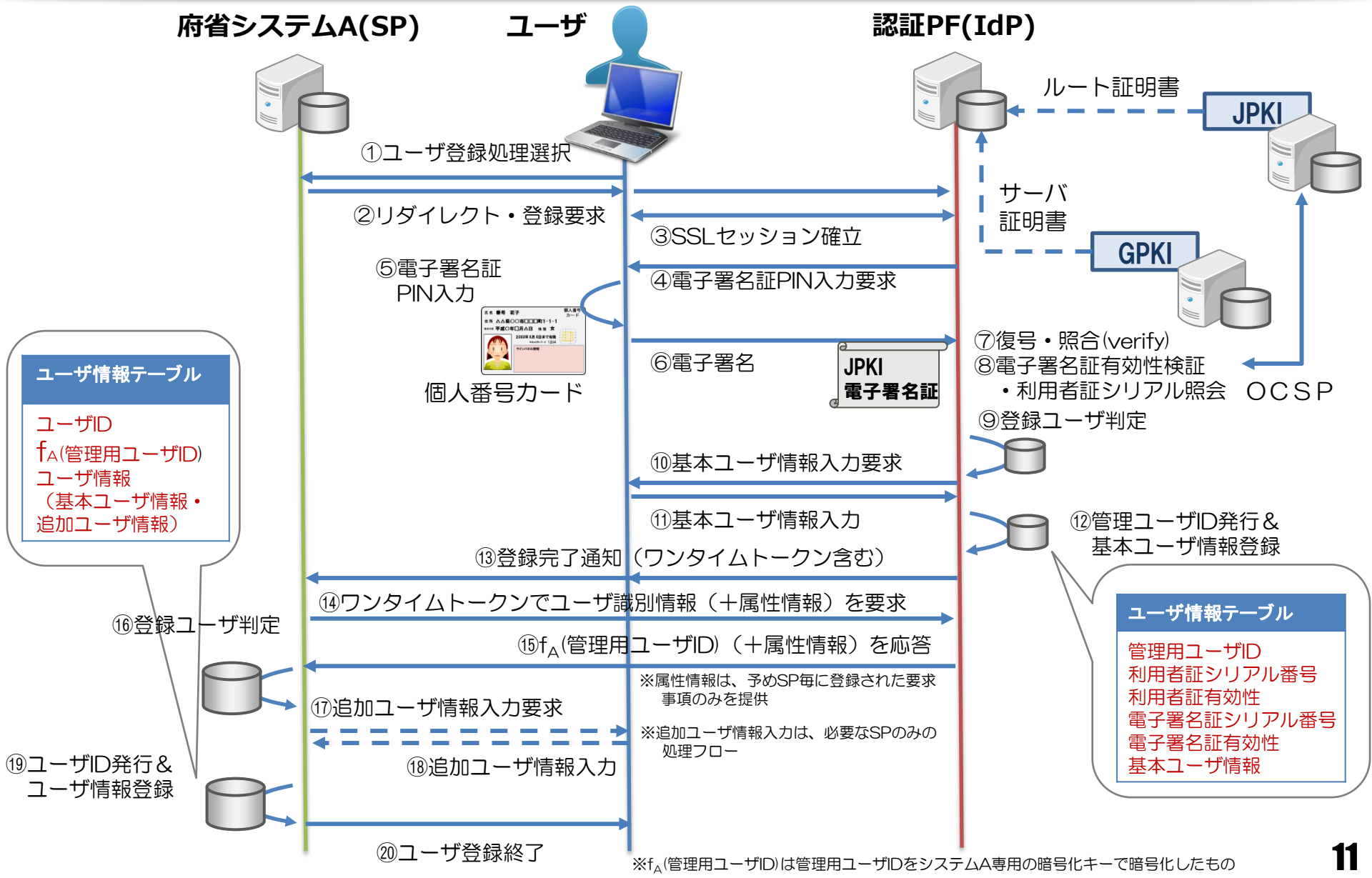
SP側ID管理パターン

	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

ユーザ登録の画面遷移

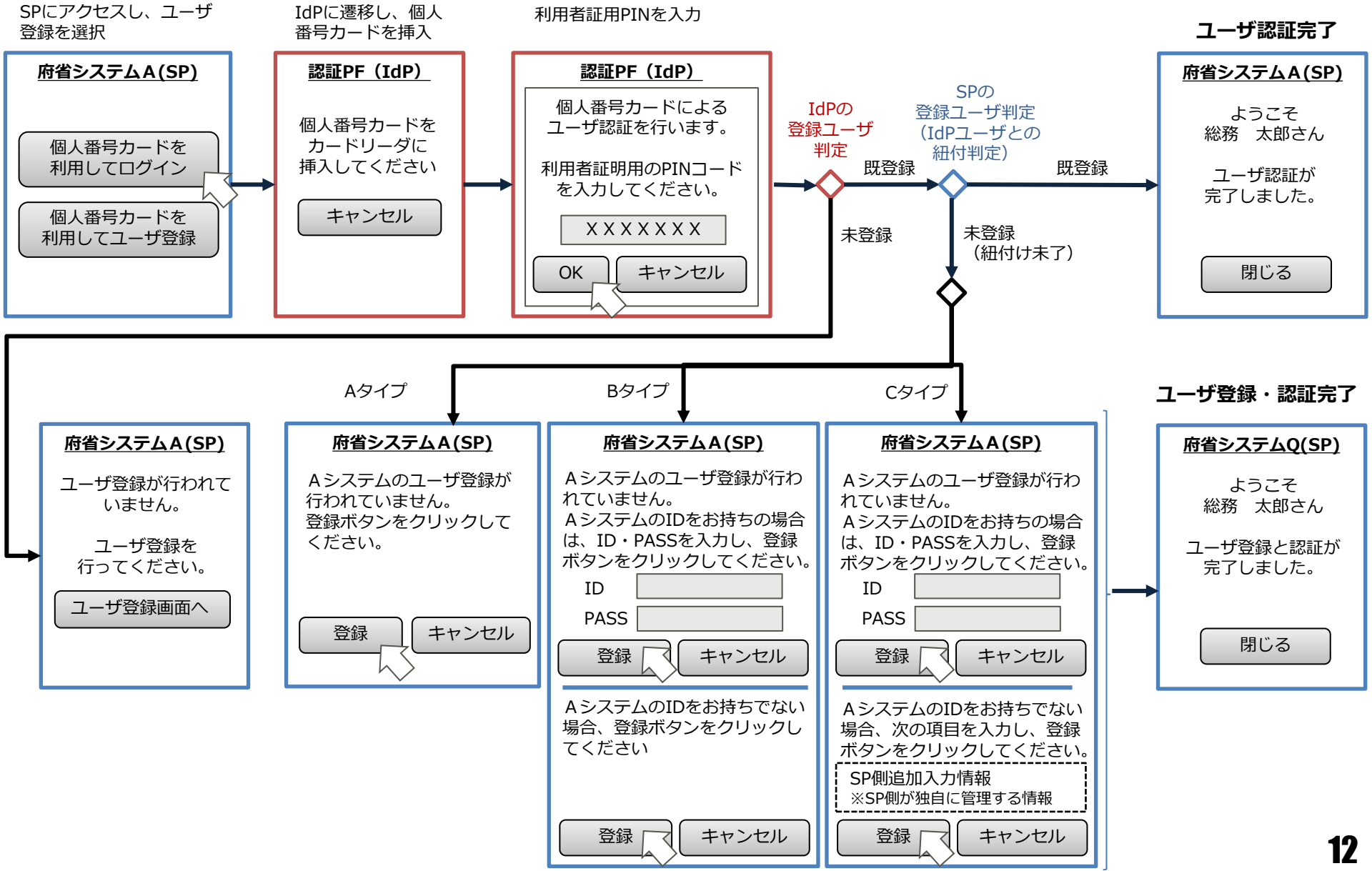

SPにアクセスし、ユーザ登録を選択
IdPに遷移し、個人番号カードを挿入
電子署名証用PINを入力
府省システムA(SP)
個人番号カードを利用してログイン
個人番号カードを利用してユーザ登録
認証PF（IdP）
個人番号カードをカードリーダに挿入してください
キャンセル
認証PF（IdP）
個人番号カードでユーザ認証を行うためのユーザ登録を行います。
電子署名のPINコードを入力してください。
ＸＸＸＸＸＸ
OK
キャンセル
IdPの登録ユーザ判定
既登録
未登録
SPの登録ユーザ判定（IdPユーザとの紐付判定）
既登録
未登録
府省システムA(SP)
あなたのユーザ登録は既に完了しています。
ログインを行ってください。
ログイン画面へ
SPのタイプ
Aタイプ
Bタイプ
Cタイプ
カード（電子署名証）に記録されている情報を用いてユーザ登録。証明書情報は変更不可。
認証PF（IdP）
基本情報を入力してください。
氏名 総務 太郎
住所 東京都・・・
性別 男性
生年月日 19XX/XX/XX
電話番号
E-mail
次へ
キャンセル
SPのタイプ
Aタイプ
Bタイプ
Cタイプ
府省システムA(SP)
登録ボタンをクリックしてください。ユーザ登録が完了します。
登録
キャンセル
府省システムA(SP)
AシステムのIDをお持ちの場合は、ID・PASSを入力し、登録ボタンをクリックしてください。
ID
PASS
登録
キャンセル
AシステムのIDをお持ちでない場合、登録ボタンをクリックしてください。ユーザ登録が完了します。
登録
キャンセル
府省システムA(SP)
AシステムのIDをお持ちの場合は、ID・PASSを入力し、登録ボタンをクリックしてください。
ID
PASS
登録
キャンセル
AシステムのIDをお持ちでない場合、次の項目を入力し、登録ボタンをクリックしてください。
SP側追加入力情報
※SP側が独自に管理する情報
登録
キャンセル
ユーザ登録完了
府省システムA(SP)
ユーザ登録が完了しました。
ログインを行ってください。
ログイン画面へ

ユーザ登録のシーケンス



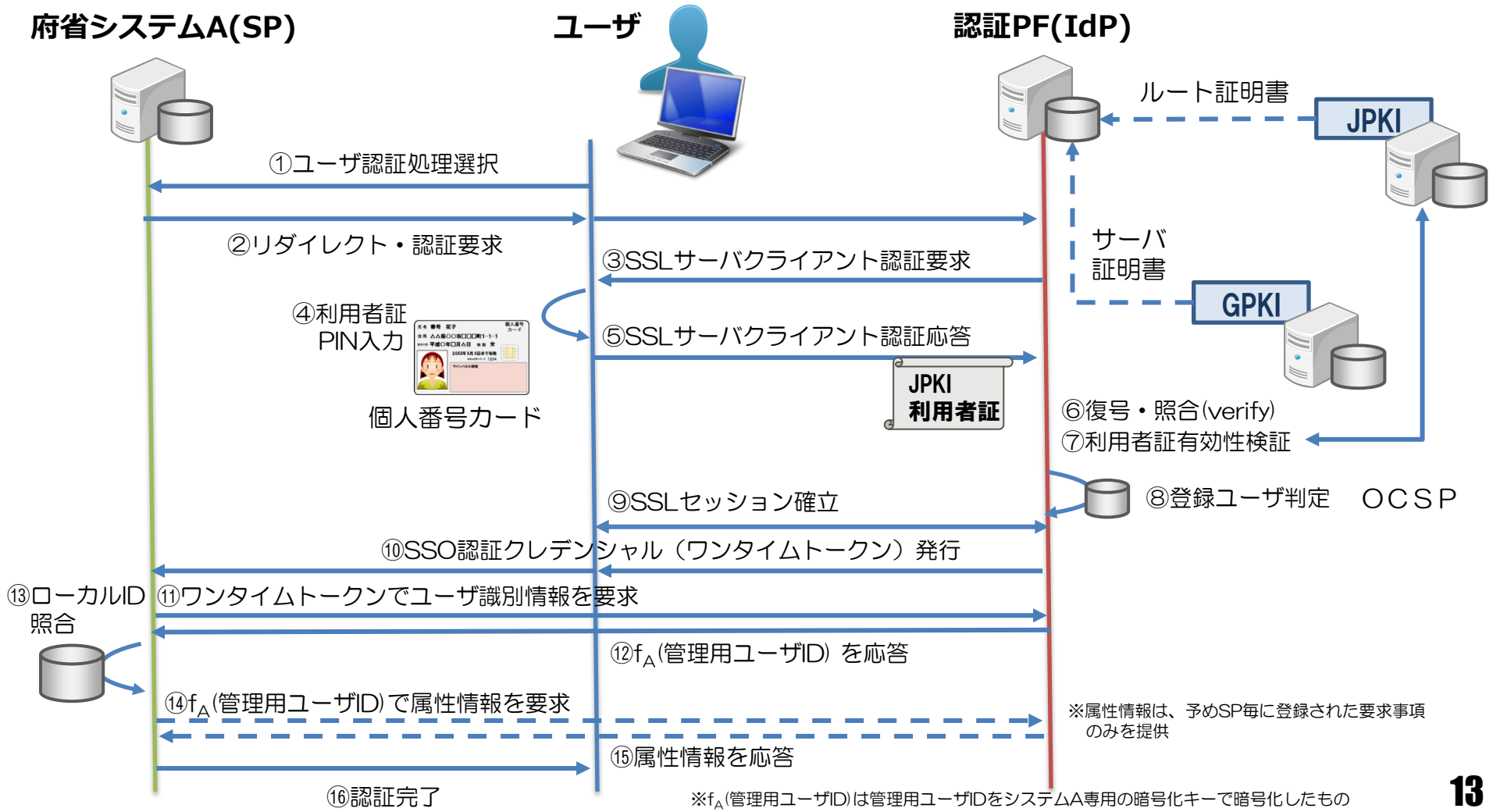
※f_A(管理用ユーザID)は管理用ユーザIDをシステムA専用の暗号化キーで暗号化したもの

ユーザ認証の画面遷移


SPにアクセスし、ユーザ登録を選択
IdPに遷移し、個人番号カードを挿入
利用者証用PINを入力
ユーザ認証完了
府省システムA(SP)
個人番号カードを利用してログイン
個人番号カードを利用してユーザ登録
認証PF（IdP）
個人番号カードをカードリーダに挿入してください
キャンセル
認証PF（IdP）
個人番号カードによるユーザ認証を行います。
利用者証明用のPINコードを入力してください。
ＸＸＸＸＸＸ
OK
キャンセル
IdPの登録ユーザ判定
既登録
SPの登録ユーザ判定（IdPユーザとの紐付判定）
既登録
府省システムA(SP)
ようこそ
総務　太郎さん
ユーザ認証が完了しました。
閉じる
未登録
未登録（紐付け未了）
Aタイプ
Bタイプ
Cタイプ
ユーザ登録・認証完了
府省システムA(SP)
ユーザ登録が行われていません。
ユーザ登録を行ってください。
ユーザ登録画面へ
府省システムA(SP)
Aシステムのユーザ登録が行われていません。
登録ボタンをクリックしてください。
登録
キャンセル
府省システムA(SP)
Aシステムのユーザ登録が行われていません。
Aシステムの IDをお持ちの場合は、ID・PASSを入力し、登録ボタンをクリックしてください。
ID
PASS
登録
キャンセル
Aシステムの IDをお持ちでない場合、登録ボタンをクリックしてください
登録
キャンセル
府省システムA(SP)
Aシステムのユーザ登録が行われていません。
Aシステムの IDをお持ちの場合は、ID・PASSを入力し、登録ボタンをクリックしてください。
ID
PASS
登録
キャンセル
Aシステムの IDをお持ちでない場合、次の項目を入力し、登録ボタンをクリックしてください。
SP側追加入力情報
※SP側が独自に管理する情報
登録
キャンセル
府省システムQ(SP)
ようこそ
総務　太郎さん
ユーザ登録と認証が完了しました。
閉じる

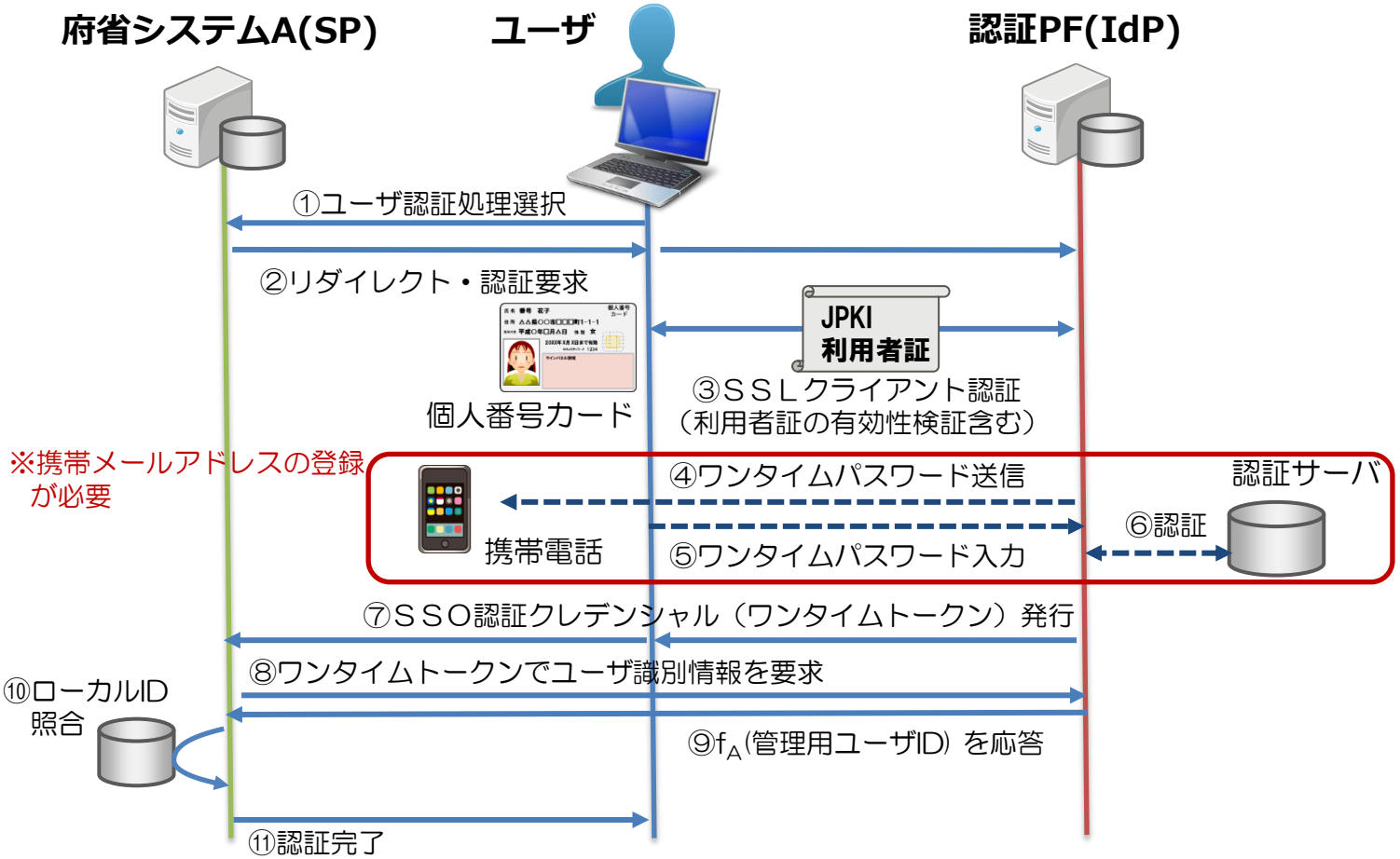
ユーザ認証のシーケンス

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

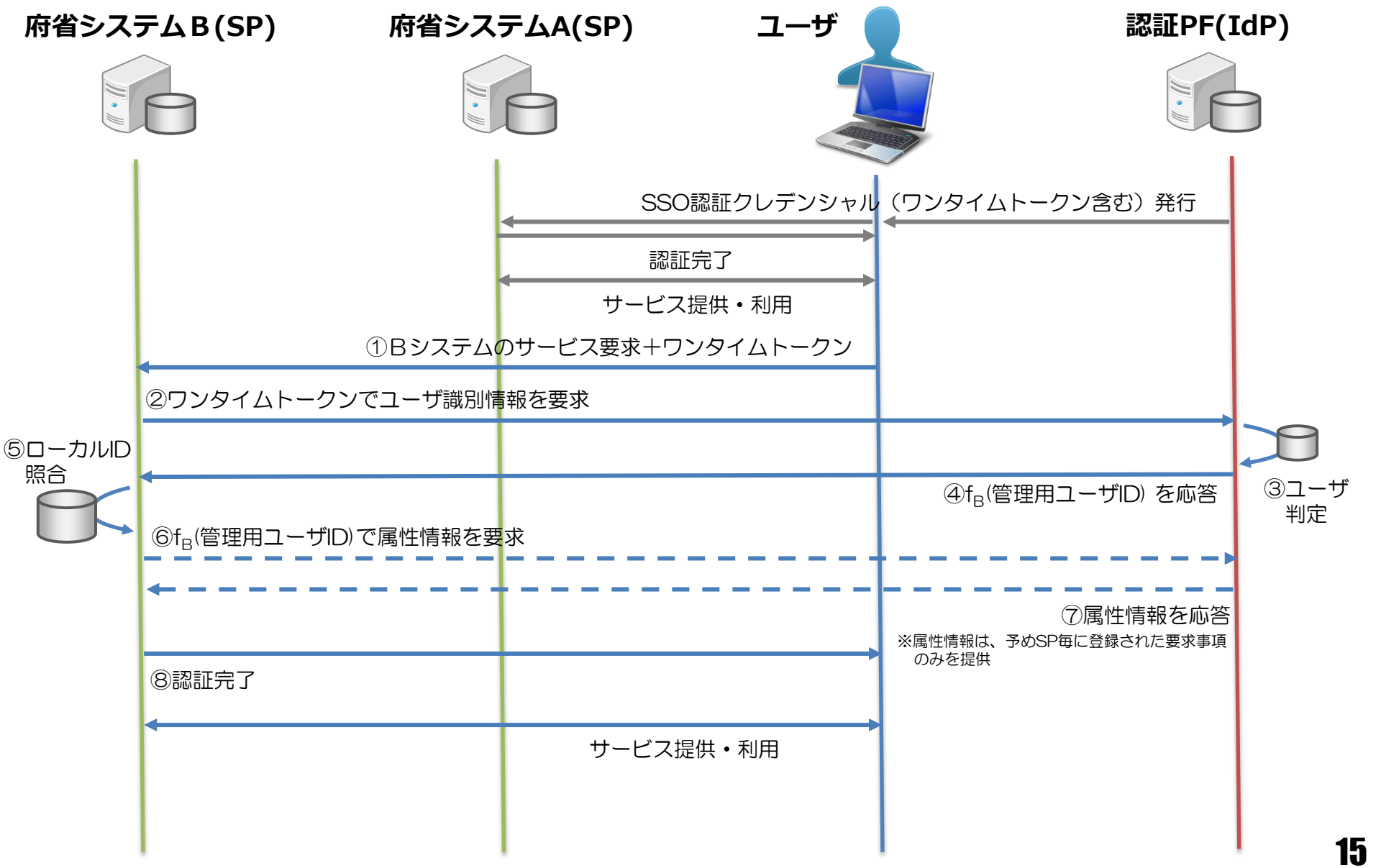


ユーザ認証の選択的セキュリティ強化

ユーザ認証のオプション的方式として、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。

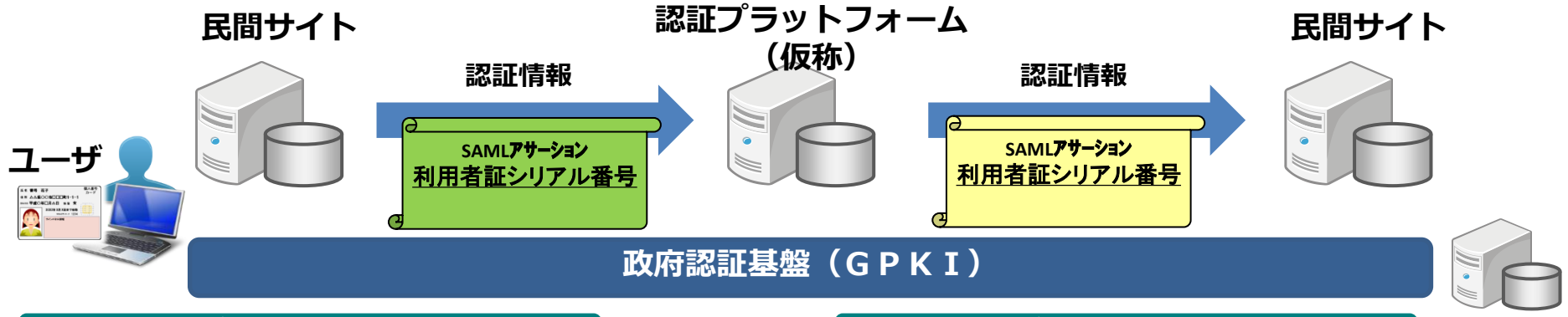


ユーザ認証のシーケンス（ＳＳＯ）



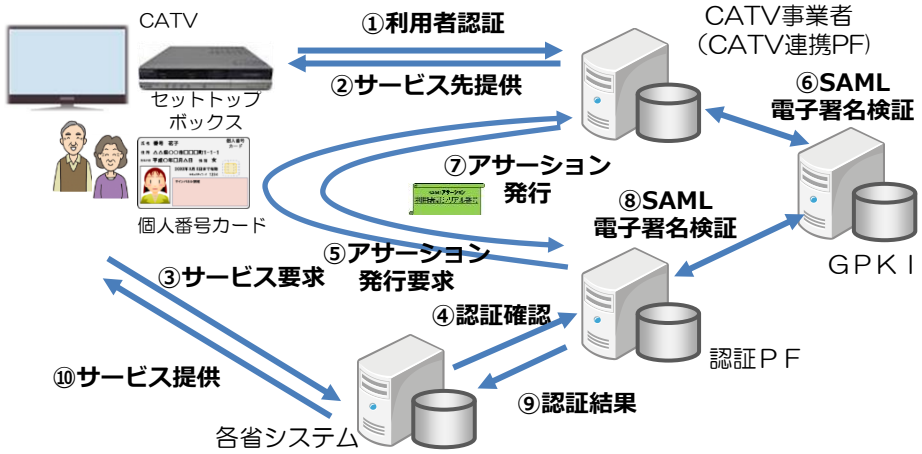
提携する民間サイトとの連携

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



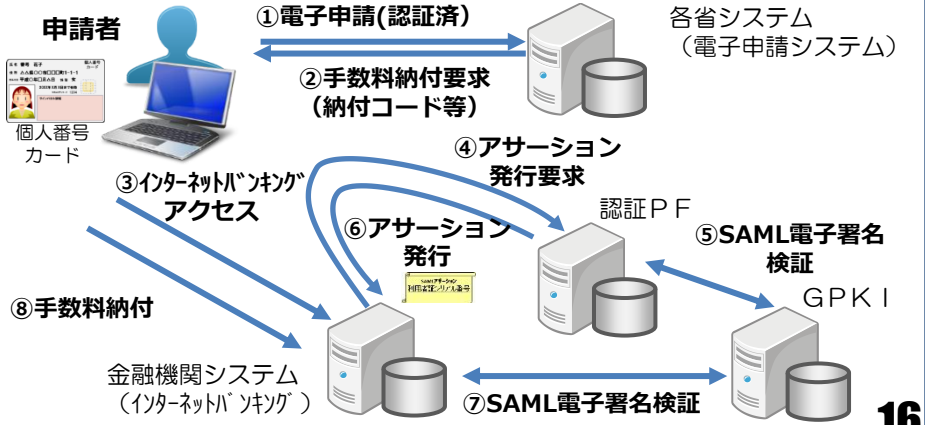
ケーススタディ（マルチチャネル化）

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

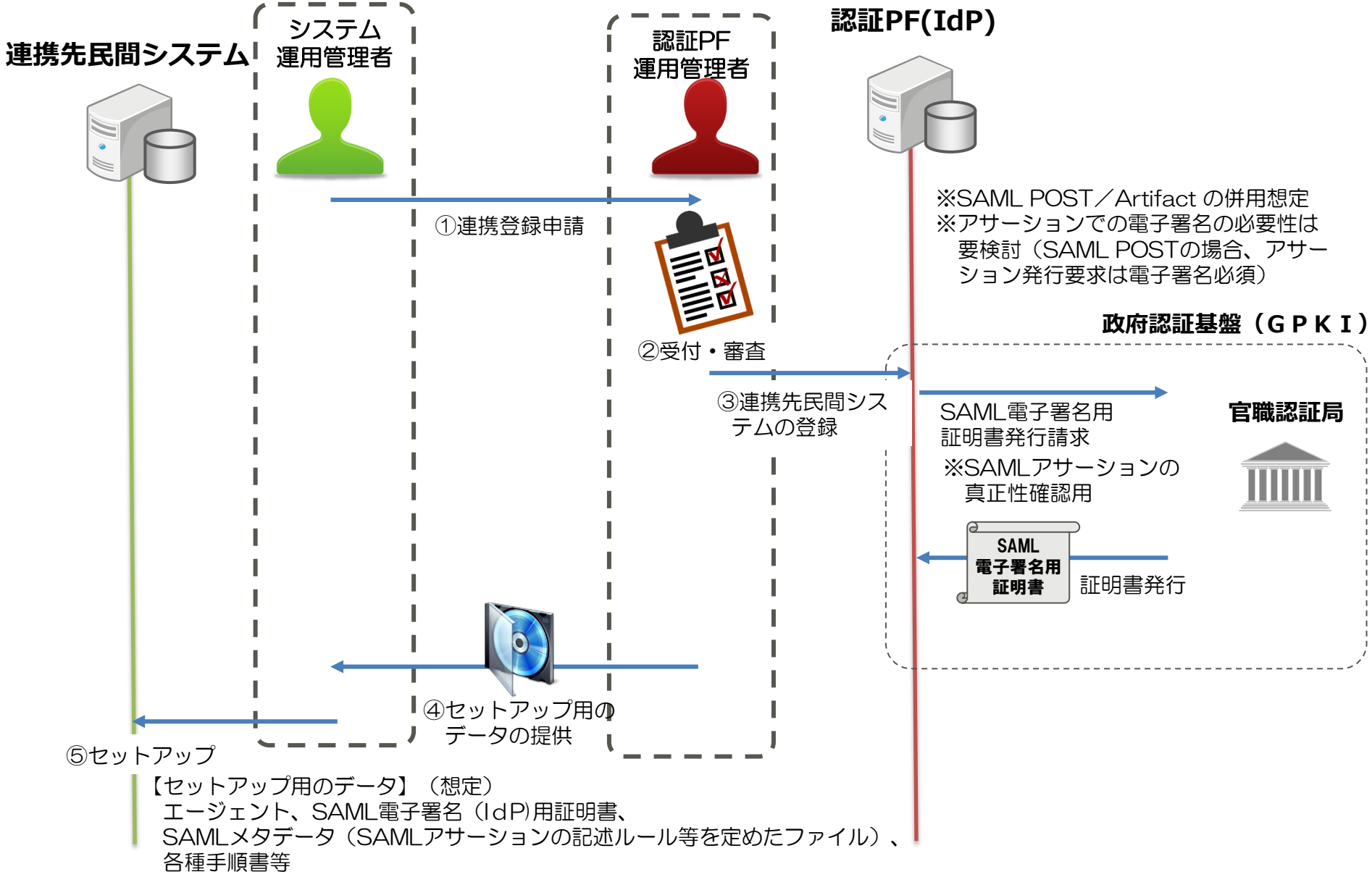


ケーススタディ（手数料納付）

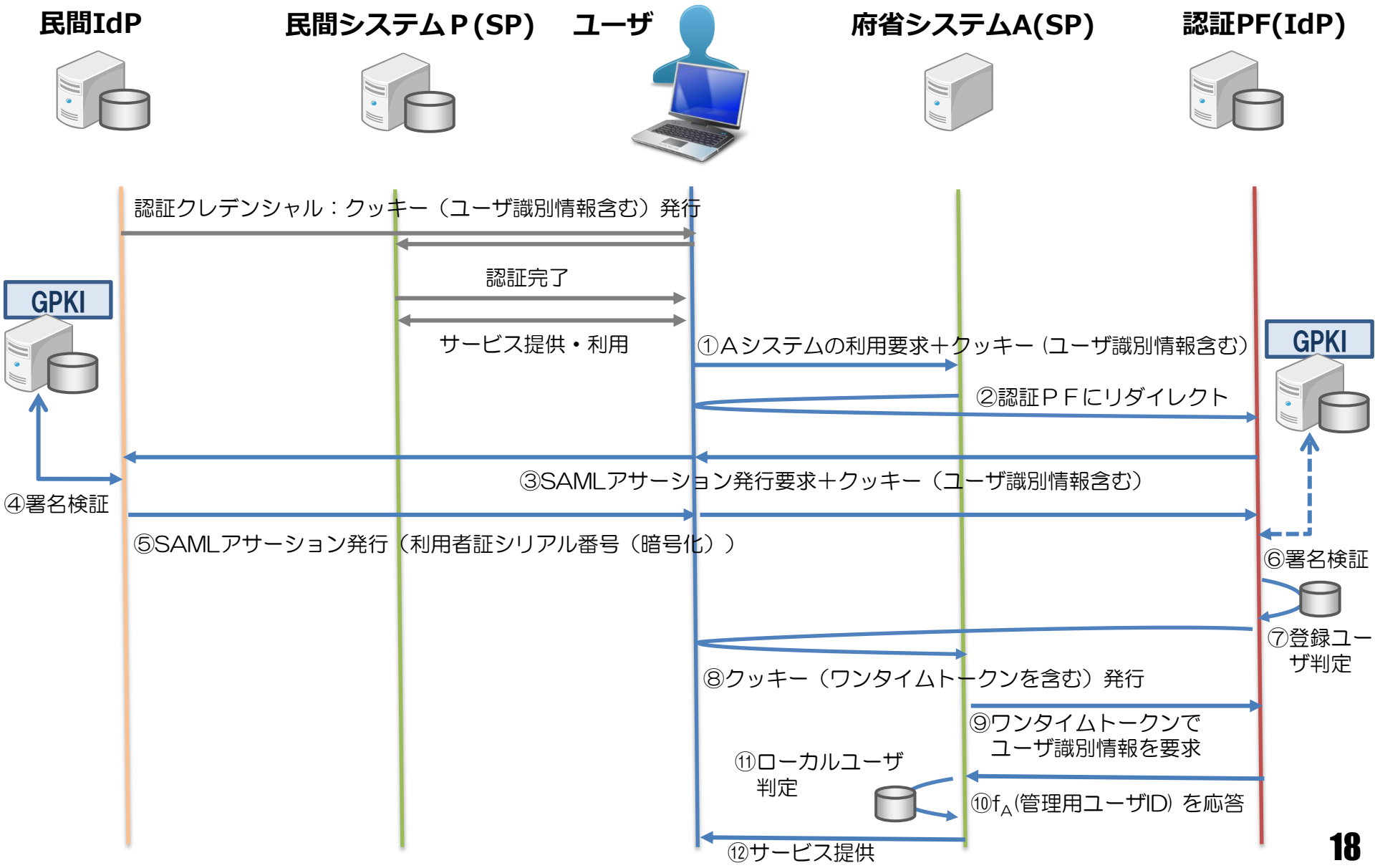
公的個人認証サービスの署名検証者である金融機関と連携し、電子申請の後、手数料納付するためのインターネットバンキングにシームレスに接続



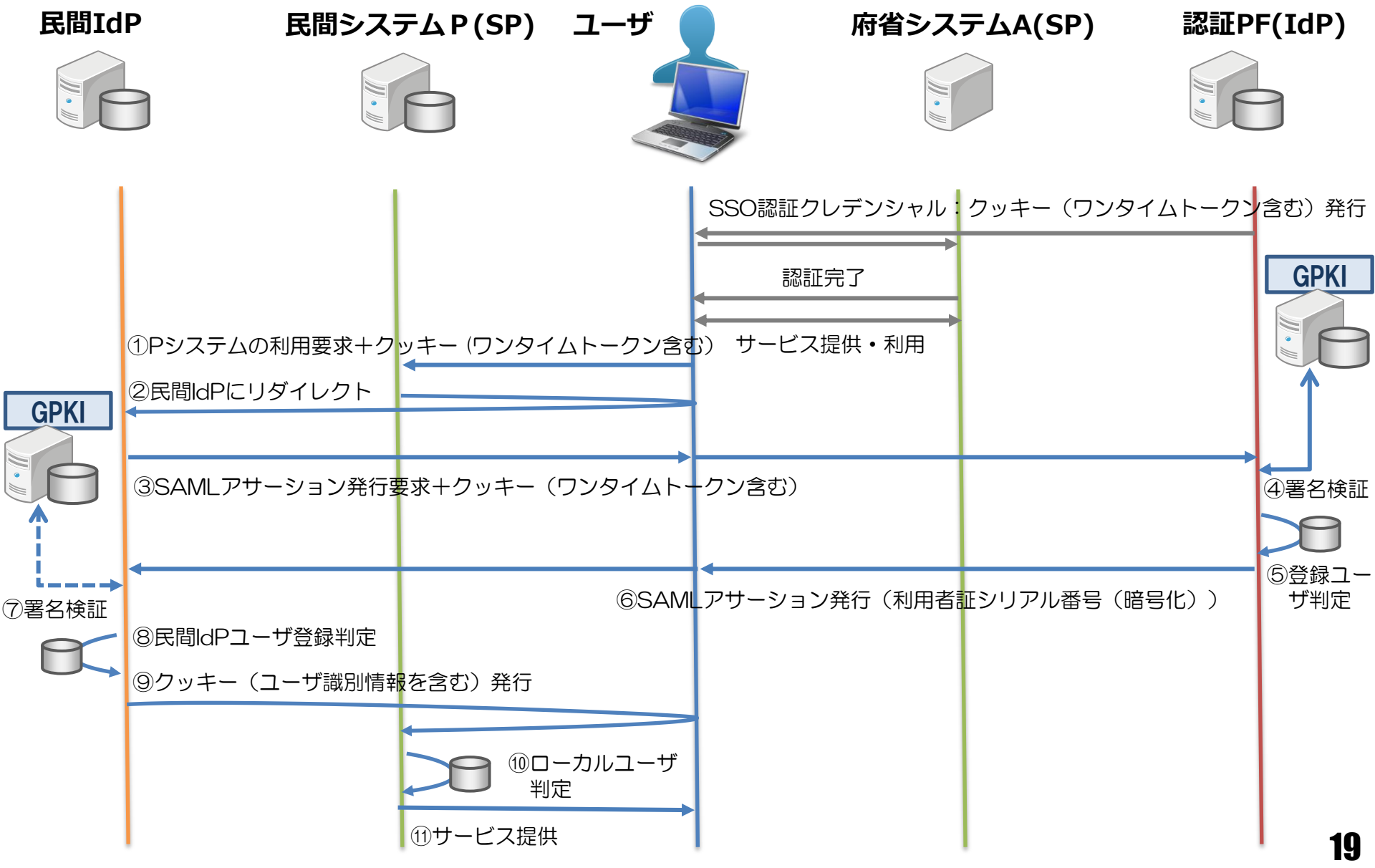
連携先民間システムの登録



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



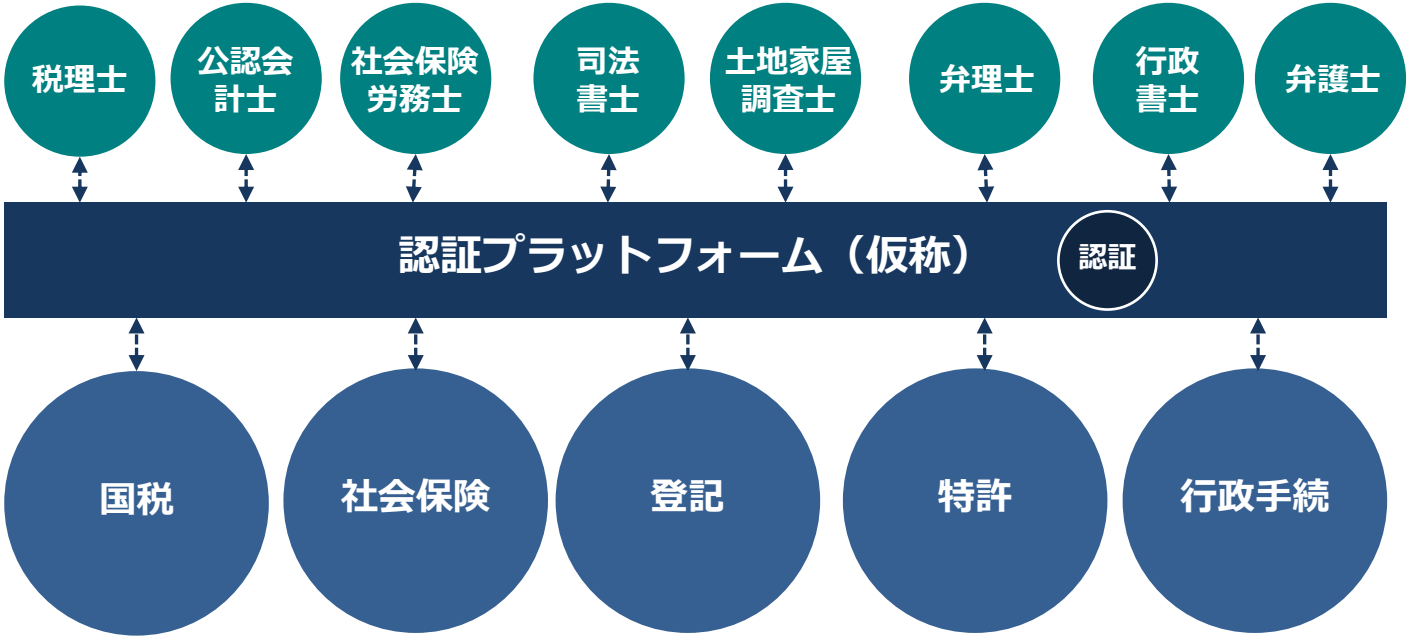
電子署名の代替可能性

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

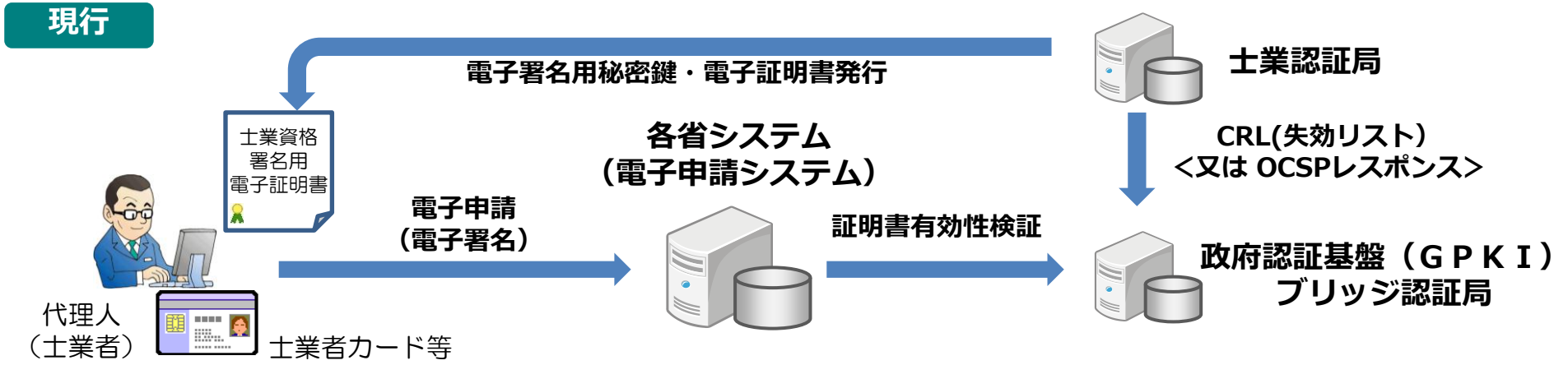
政府情報システムのＩｄＰでは、各行政手続が士業者による代理・復代理申請が行われるため、ワンカード化を実現するためには、カード所有者の本人認証だけでなく、士業資格等の資格・属性認証を行えるモデル構築と機能実装が必要



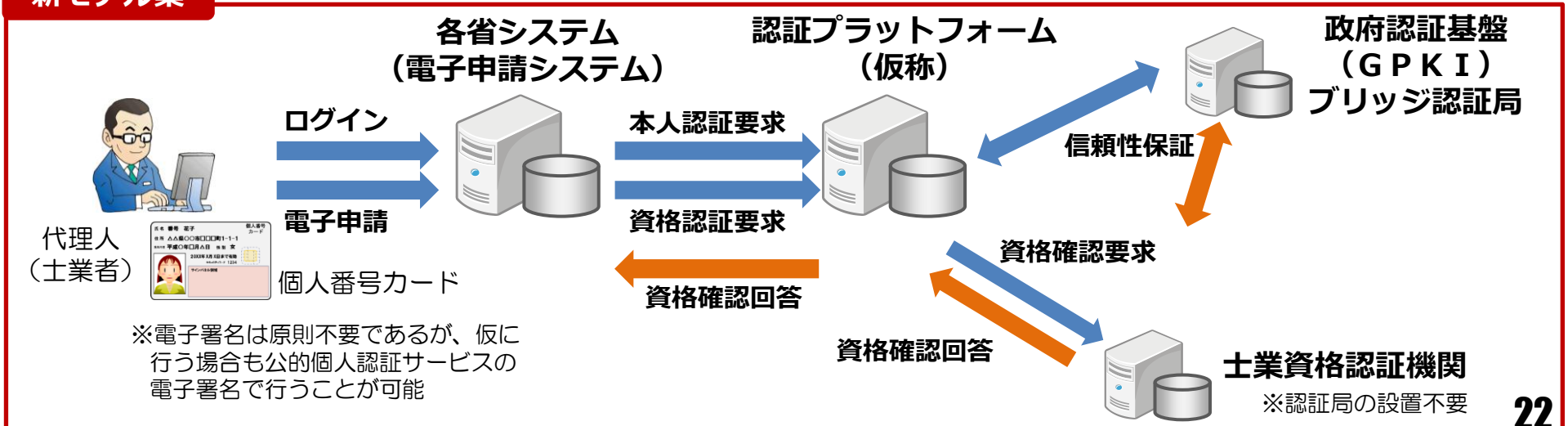
資格情報確認（応用：代理申請）

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

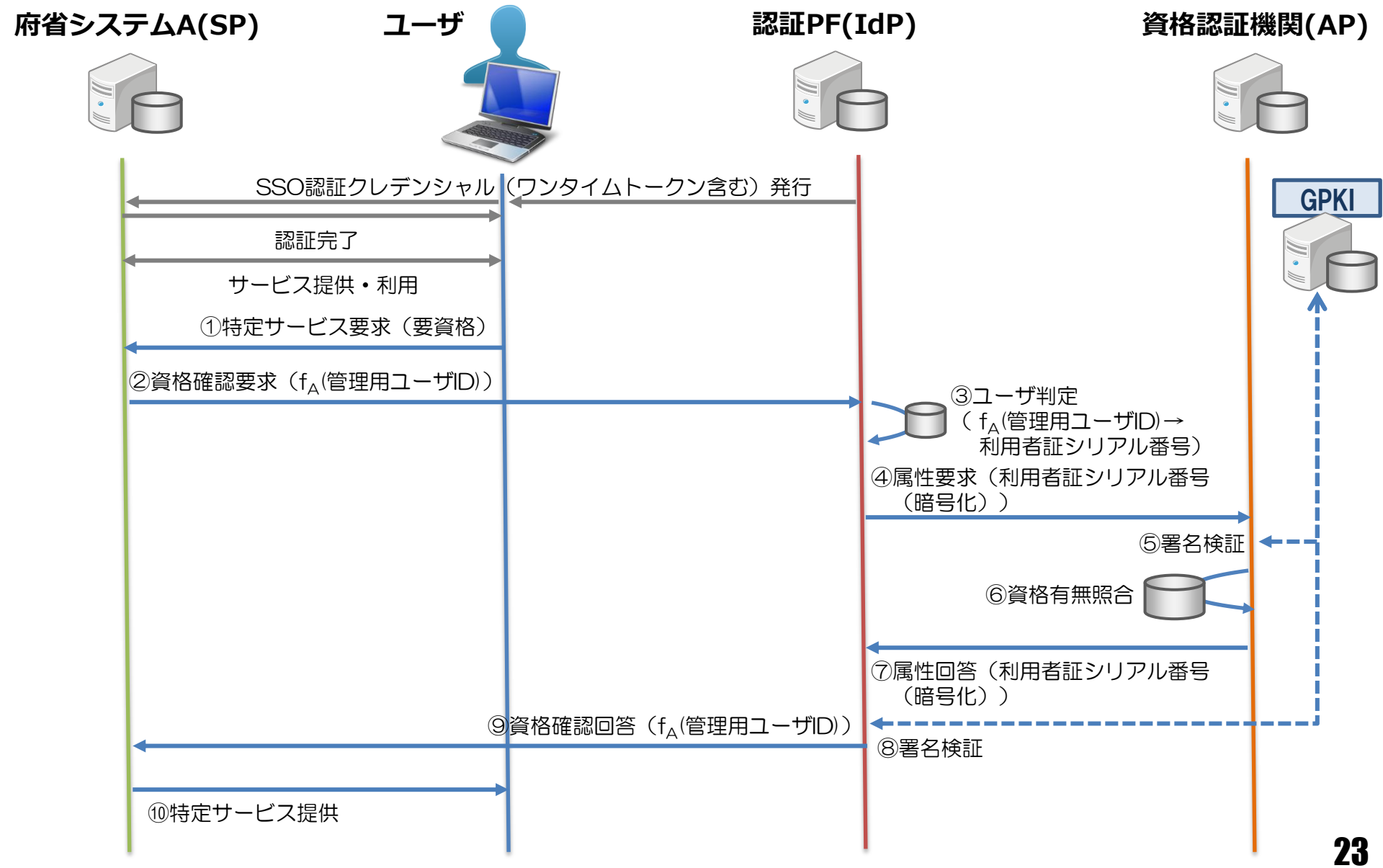


新モデル案



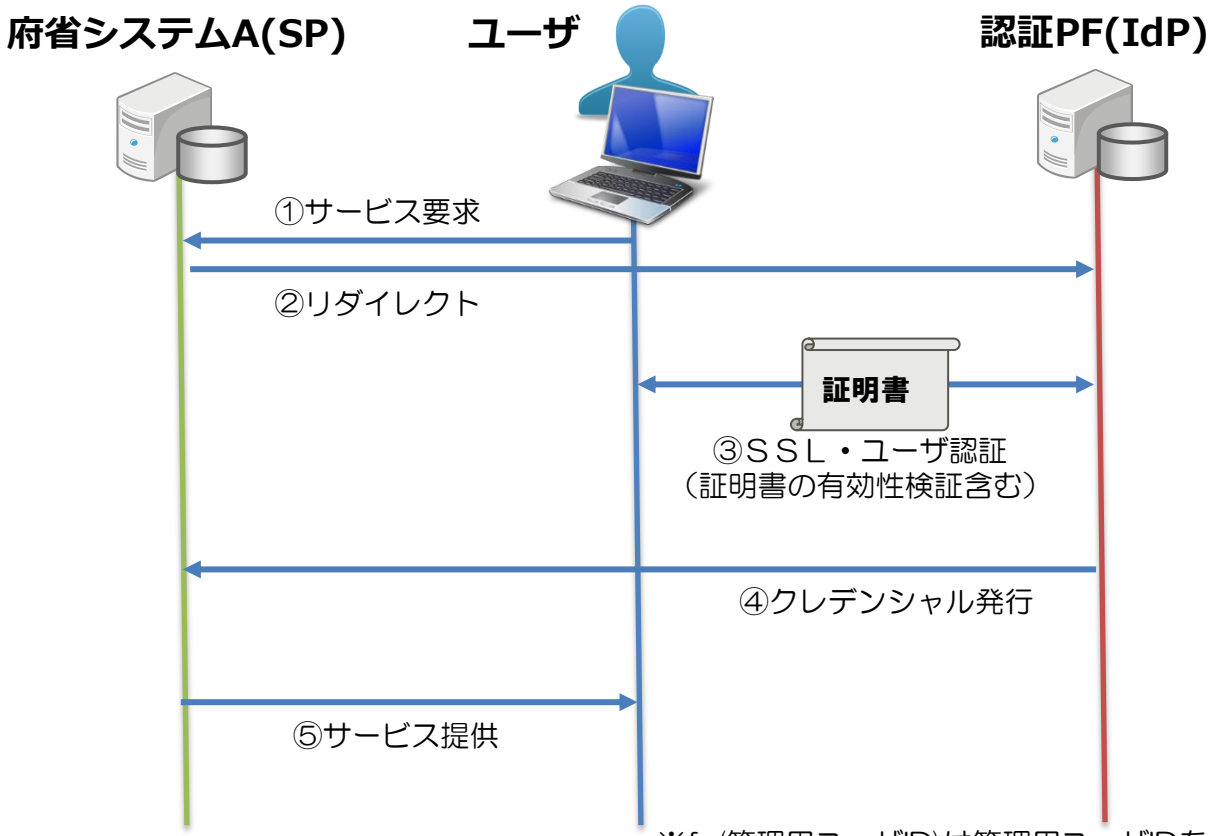
※電子署名は原則不要であるが、仮に行う場合も公的個人認証サービスの電子署名で行うことが可能

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)
GPKI
SSO認証クレデンシャル（ワンタイムトークン含む）発行
認証完了
サービス提供・利用
①特定サービス要求（要資格）
②資格確認要求（f_A(管理用ユーザID)）
③ユーザ判定
（ f_A(管理用ユーザID)→
利用者証シリアル番号）
④属性要求（利用者証シリアル番号
（暗号化））
⑤署名検証
⑥資格有無照合
⑦属性回答（利用者証シリアル番号
（暗号化））
⑧署名検証
⑨資格確認回答（f_A(管理用ユーザID)）
⑩特定サービス提供

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。



※f_A(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