PKI Day 2016

デジタルWatashiアプリ

平成28年4月22日

経済産業省

CIO補佐官　満塩　尚史

デジタルwatashiアプリの取り組みの観点

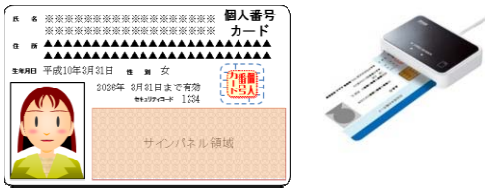
- **ID連携に基づくデータ活用**
  - 官民連携を想定し、行政機関が保有するデータと、民間が推進するサービスの連携を、個人の管理の下で実施できる仕組みを検討する必要があるのではないか。
- **オンライン完結社会の実現**
  - 対面書類の撤廃等、オンラインで完結した社会を目指すには、『デジタルであることを前提にする（デジタル・デフォルト）』ことに配慮する必要があるのではないか。
- **マイナンバー制度の活用**
  - マイナンバー制度（券面表示、マイナポータル、個人番号カード内に格納された　公的個人認証を含む）を民間サービスで利用する場合には、利用者が受けたい　サービスにおいて『ペルソナを使い分けること（自己情報のコントロール）が可能な環境』が必要ではないか。
  - 例：基本４情報（氏名、住所、生年月日、性別）を提供事業者に一律に渡すのではなく、サービスによって渡す情報を調整できる等
- **普及促進**
  - 全ての関係者にID連携を分かり易く理解できるルール、仕組みの整備として、ID連携トラストフレームワークとしてID連携の見せ方をルール化し、トラストフレームワーク内で共通化を図っていくべきではないか。
  - 全ての関係者にID連携によるメリットを理解できる事例を検討すべきではないか。

マイナンバー制度の民間活用の可能性のある分野

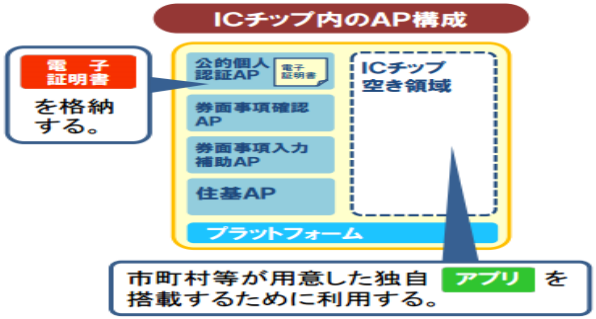
（1）マイナンバー自体

123456789101

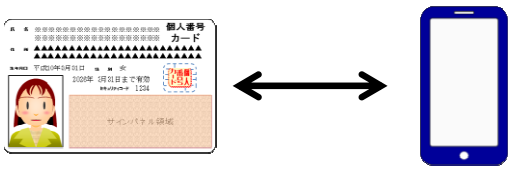
（2）個人番号カードの公的個人認証の民間利用



（3）個人番号カードの空き容量



（4）個人番号カードのサブカード（スマホSIMの利用など）

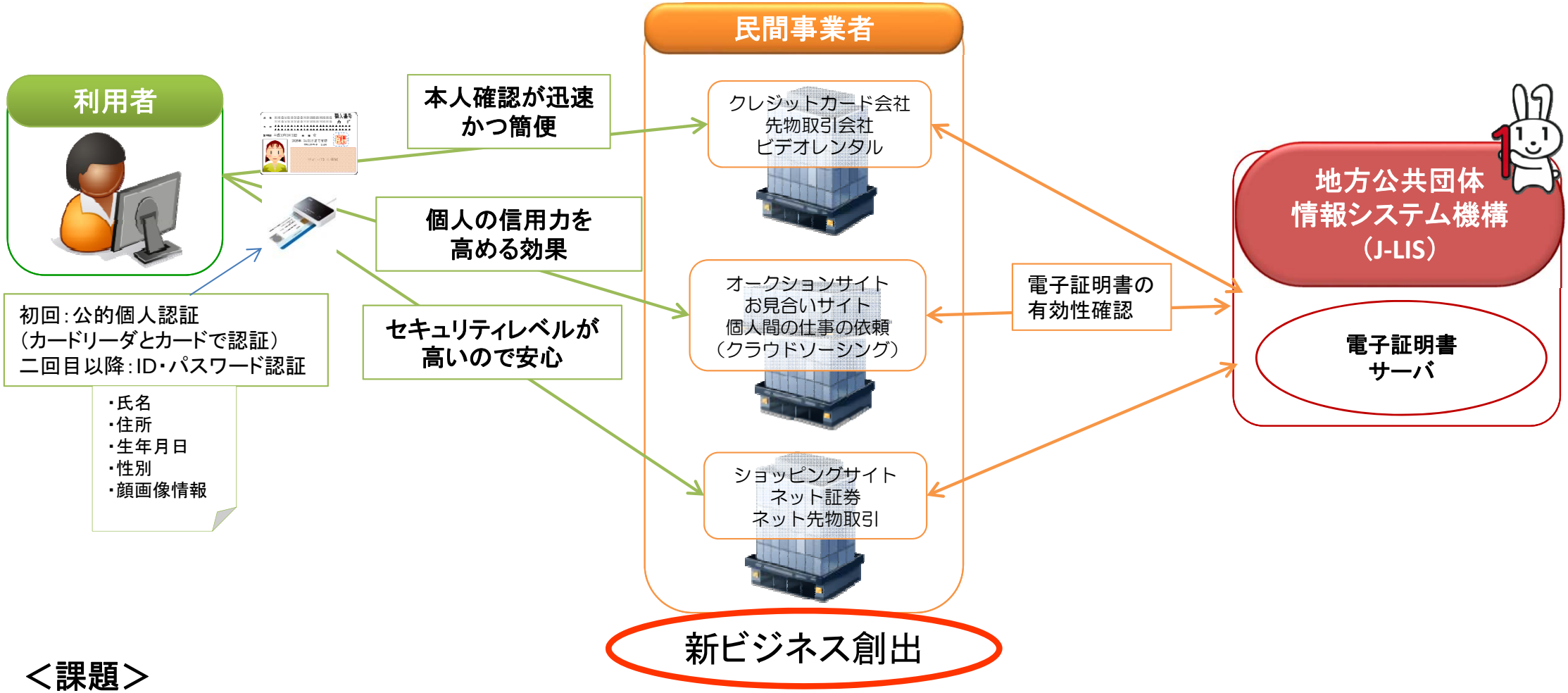


（5）マイナポータルにおける民間サービスの提供

注）民間活用の可能性に関しては、民間活用するにあたっては、法律改正等を必要する場合もあります。

公的個人認証の民間活用について

1.個人番号カードの認証による民間サイトでのビジネスの創出

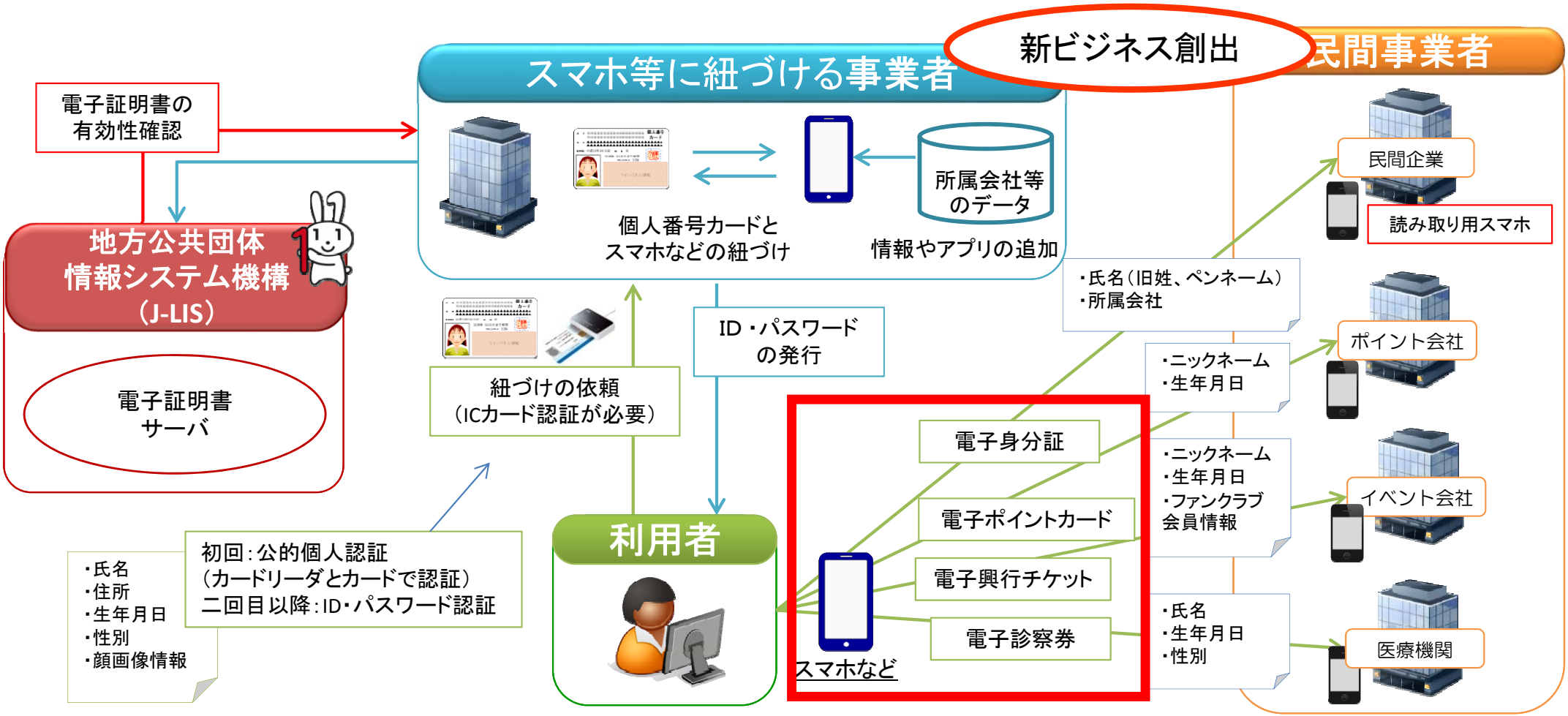


＜課題＞

○ 民間サイトがJ-LISから失効情報を取得するには、総務大臣の認定を受けて、J-LISへの届け出が必要。この認定基準に対応できるのか、民間企業では検討が必要。 民間企業において、ビジネスが成り立つかどうかに、J-LISによる有効性確認の手数料が影響するが、例えば、入会時に公的個人認証を行うとともに、IDパスワードを発行すれば、その後のログインでは、手数料は発生しなくなる。

○ 個人番号カードの空き容量の民間活用は、政令制定が必要であり、機動性に欠けるため、公的個人認証の方が民間活用に適当との意見がある。

2.個人番号カードに紐づけたスマホ等を活用したビジネスの創出



これまでの施策

- 企業が個人データを利用する際に、データを共有する企業間で、遵守するルールのひな形等を作成（ID連携トラストフレームワーク）
- データの情報交換に関する実証事業（訪日外国人向けおもてなしサービス）

今後の施策

- 民間企業の参入を促進させるために、民間企業とともに民間サイトがJ-LISに認証してもらう上での課題を抽出する。
- 民間サイトがJ-LISに認証してもらうことに関連して、実証事業を行う。

公的個人認証サービスの「プラットフォーム事業者」の活用（総務省資料より）

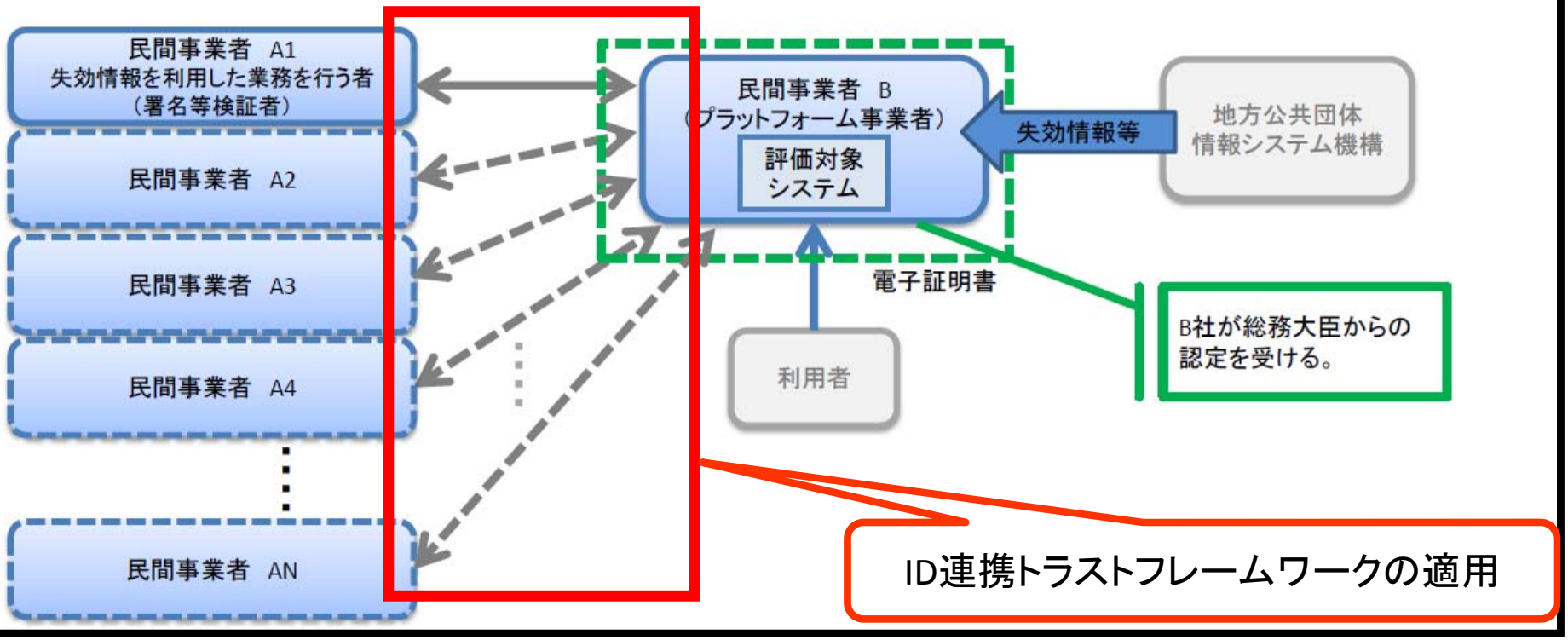
「プラットフォーム事業者」を活用した公的個人認証サービスの利用の推進について

● 公的個人認証サービスの利用のために必要となる「電子証明書の受付・有効性確認等のためのシステム」を、各民間事業者（署名等検証者）が個別に整備・運用するのではなく、特定事業者（いわゆる「プラットフォーム事業者」）が整備し、これを、各民間事業者が利用することとすれば、いわゆる「割り勘効果」により、各民間事業者の導入・利用コストを大きく削減することが期待できる。

● こうした、プラットフォーム事業者を活用した公的個人認証サービスの利用の拡大を推進するため、制度面において、以下の趣旨の措置を講じることを予定している。

① 「総務大臣の認定」（法17条1項6号）について
「電子証明書の受付・有効性確認のためのシステム」の全部を、プラットフォーム事業者に委託する場合には、各民間事業者に代わり、プラットフォーム事業者が認定を受けることができることとし、各民間事業者の負担を軽減する。

② 「機構への届出」（法第17条第1項）について
「電子証明書の受付・有効性確認のためのシステム」の全部を、プラットフォーム事業者に委託する場合には、各民間事業者に代わり、プラットフォーム事業者が届出を行うことができることとし、各民間事業者の負担を軽減する。



人の写像（ペルソナ）

場面に応じて自然に使い分ける

本人確認なしでは、なりすましの可能性を高くする

行政における個人

真の人物像

ビジネス上の私

プライベートな私

マイナンバー法の正式名称：
<u>行政手続における特定の個人</u>を識別するための番号の利用等に関する法律

ペルソナによるシーンや個人の属性情報の違い

ペルソナ	シーン	主な個人の属性情報
行政における個人	• 市役所、区役所等で行政手続きを行う。 • 納税者として納税をする。社会保障の保険料等を支払う。 • 行政機関の長や議員等の投票をする。 • 社会保障の手当等を受け取る	• マイナンバー • 氏名 • 住民票上の住所 • 生年月日 • 性別 • 納税情報、保険料の支払い情報
ビジネス上の私	• 会社の社内で、仕事をする。 • 他社の社員と打ち合わせをする。 • ビジネスについて講演を行う。 • 会社の備品を購入する。	• 会社名、部署名 • 勤務先住所 • 肩書き • 業務上の資格 • 氏名、ニックネーム（旧姓、ペンネーム）
プライベートな私	• 週末の買い物をする。 • 夜中にネットショッピングする。 • 治療のため、病院に行く。 • 趣味のイベントに参加する。	• ニックネーム（ハンドルネーム） • 居住地住所、物の送付先住所 • 金銭の支払能力 • ファンクラブ会員番号

デジタルwatashiアプリイメージ

行政における個人

本人確認し
デジタルwatashiアプリをつくる

シーンによって使い分ける

ビジネス上の私

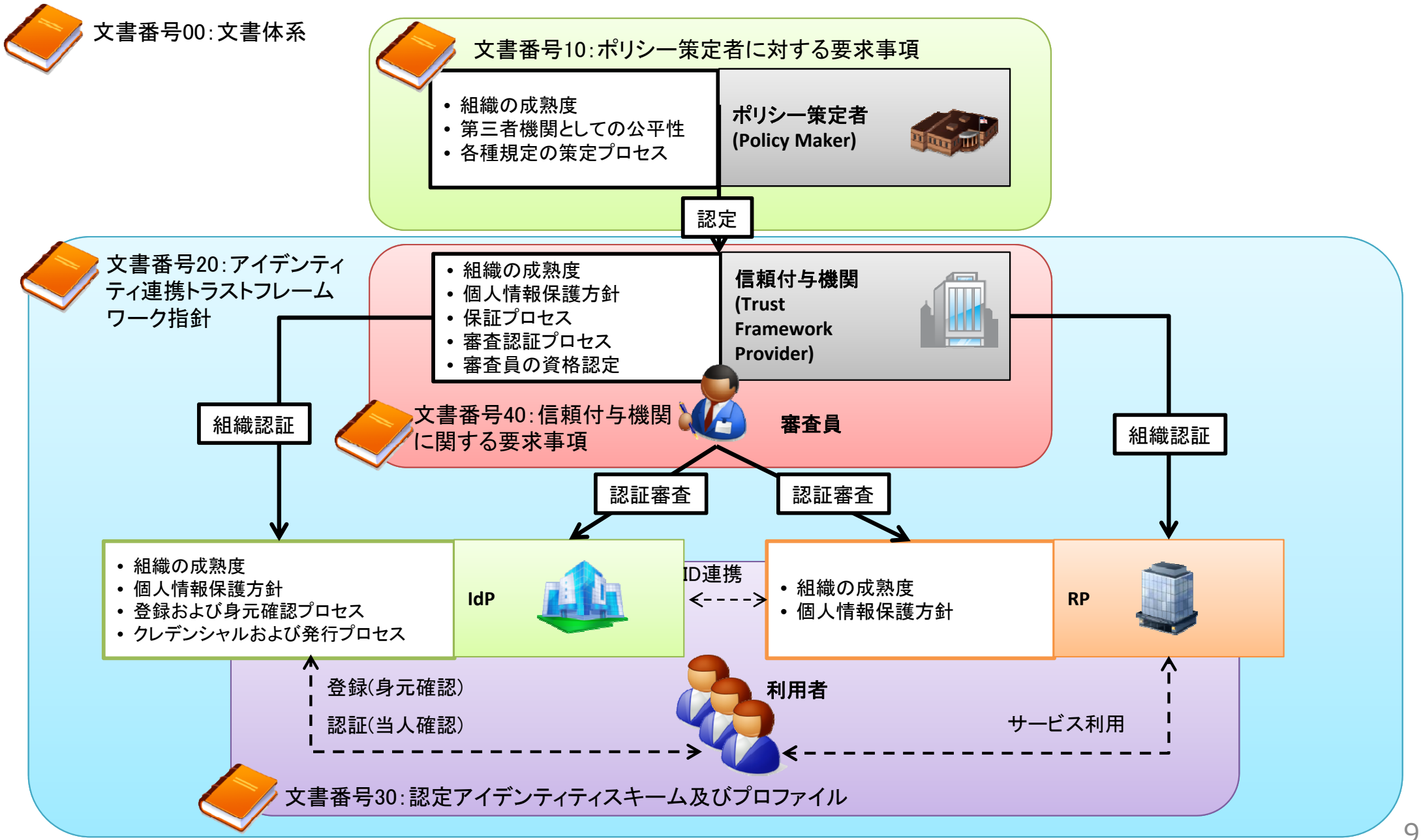
プライベートな私

シーンによって使い分ける

真の人物像

ID連携トラストフレームワーク基準の構成

策定した基準の構成と各文書が対象としている範囲を、以下に示す。



保証レベルと信頼レベル

日本版の基準案では、サービスの種類によって、身元確認と当人確認のレベルを分けているサービスが存在するため、保証レベル（アイデンティティに関する信用の程度）を身元確認保証レベルと当人確認保証レベルを分けて規定（米国ICAM基準では全体を通した保証レベルしか規定していない）。また、米国ICAM基準では、RPが政府機関であるため基準がなく。日本では民間事業者同士の連携が想定されることから、プライバシー及び個人情報保護信頼レベル（プライバシー及び個人情報保護の信用の程度）を新たに規定。

区分	保証レベル					信頼レベル
	身元確認保証レベル（登録時のレベルを規定）	当人確認保証レベル（トークン, トークン及びクレデンシャル管理, 認証プロセス, アサーション等のレベルを規定）				プライバシー及び個人情報保護信頼レベル
	全体保証レベル（米ICAMで規定されているもの）					
評価軸	登録	トークン	トークン及びクレデンシャル管理	認証プロセス	アサーション	プライバシー及び個人情報保護
レベル1（低）	（対面 / 非対面） 自己申告 / 身元確認は不要。 レベル1+ （対面 / 非対面）身分証明書の提示	単要素認証 （例）パスワード(6桁以上)、秘密の質問（最低5問から選択） 等	等 デ ト	認証プロセス実行時における脅威に対する基準	アサーション利用時に想定される脅威に対する基準	状 プ プライバシー及び個人情報保護の程度の基準
レベル2（中）	（対面）写真付き公的身分証明書の提示 （非対面）公的身分証及び金融／携帯電話の個別番号を提示。申請情報を記録と照合。	単要素認証 （例）パスワー （最低7問から選択） が記載されたカード 送られるワンタイムパスワード機器 ワンタイムパスワード機器 カード 等	発行、保管 失効等の運用ルール			
レベル3（高）	（対面）LV2に加え、申請情報を記録と照合。録音等による否認防止。 （非対面）LV2に加え、申請情報を公的機関および金融／携帯事業者の記録と照合。録音等による否認防止	多要素認証 （例）認証時にパスワード入力を求めるSSLクライアント認証、ICカード＋パスワード 等				
レベル4（特高）	（対面のみ）写真付き公的身分証明書2種又は公的身分証及び金融／携帯電話の個別番号を提示。全ての申請情報を記録と照合。生体情報の記録。	多要素認証トークン機器 （例）暗証番号認証付きワンタイムパスワード機器、指紋認証付きICカード 等				

ビジネス上の私
プライベートな私

デジタルwatashi認証アプリ

行政機関における個人

ICカードの電子署名による認証

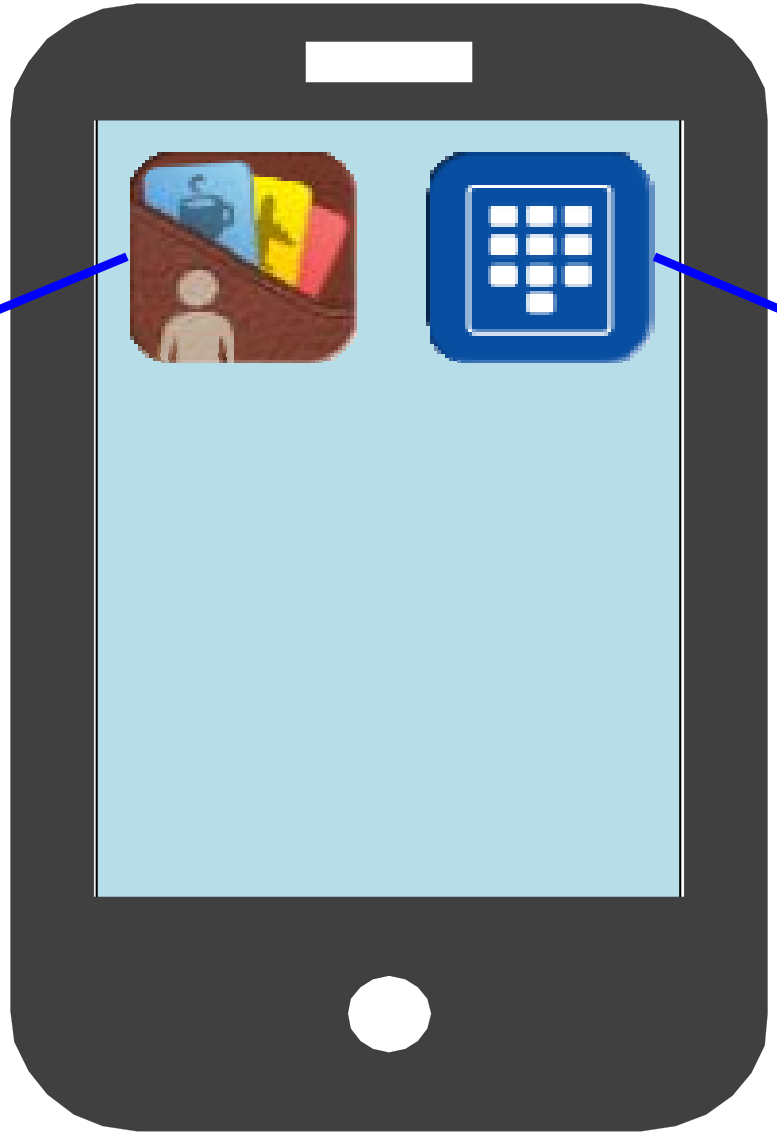
デジタルWatashiアプリの具体化

デジタルwatashiアプリのご紹介

JIPDEC

属性情報表示機能

主に対面利用を想定した基本情報や属性情報等を表示する機能



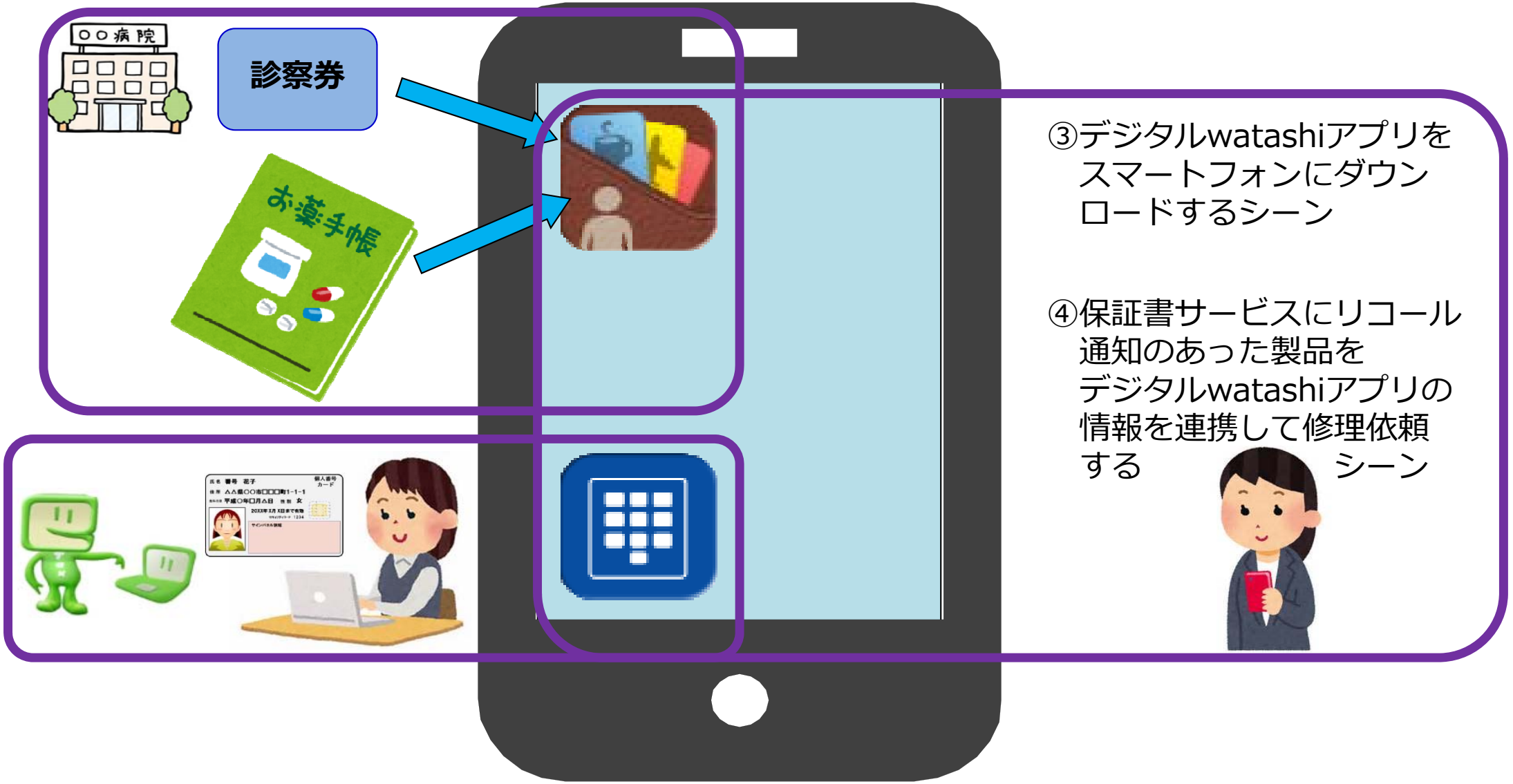
多要素・帯域外認証機能

主にオンラインサービスの認証に、スマートフォンを認証装置として利用する機能

２つの機能を持ったアプリの総称

デジタルwatashiアプリの利用例

①デジタルwatashiアプリに格納した診察券やお薬手帳の情報を活用するシーン



③デジタルwatashiアプリをスマートフォンにダウンロードするシーン

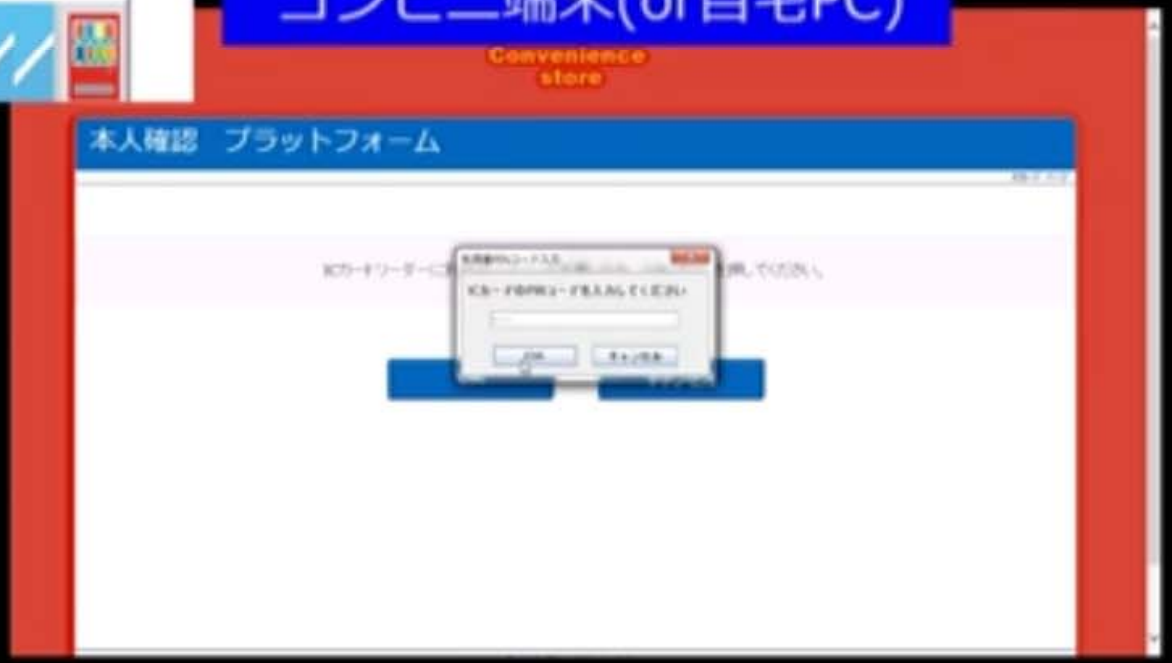
④保証書サービスにリコール通知のあった製品をデジタルwatashiアプリの情報を連携して修理依頼するシーン

②支払った医療費や薬代をオンライン家計簿に連携し、確定申告するシーン

2) アカウント本登録

公的個人認証サービスを利用するためのパスワードを入力します。

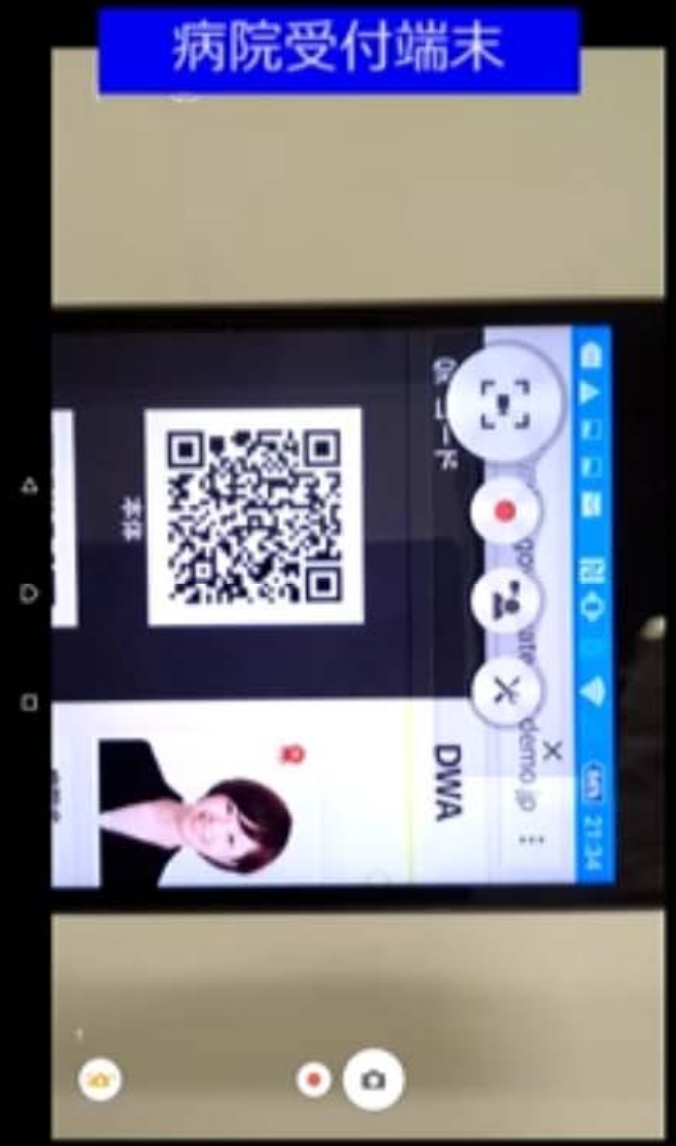
コンビニ端末(or自宅PC)



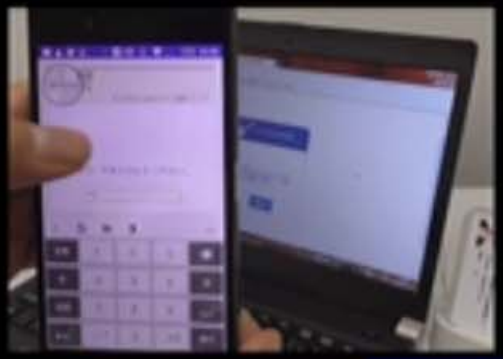
スマートフォン

2) 病院受診

watashiアプリに登録している診察券情報からQRコードを表示し、病院の受付端末に読み取らせることで受付を行います。



1) オンライン家計簿の確認

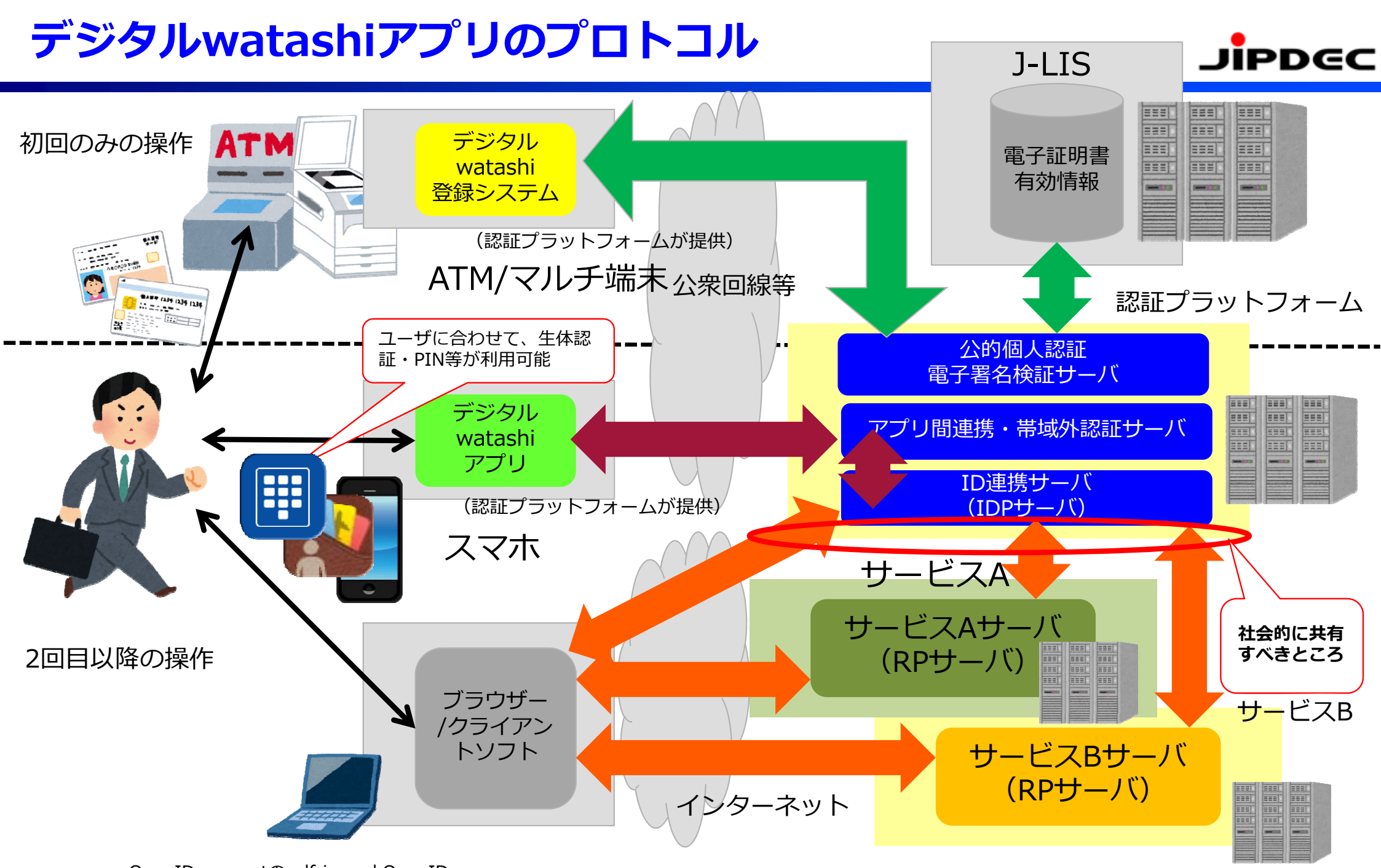


watashi認証アプリに通知が届き、PINコードを入力することで認証を進めます。

自宅PC

スマートフォン

デジタルwatashiアプリのプロトコル



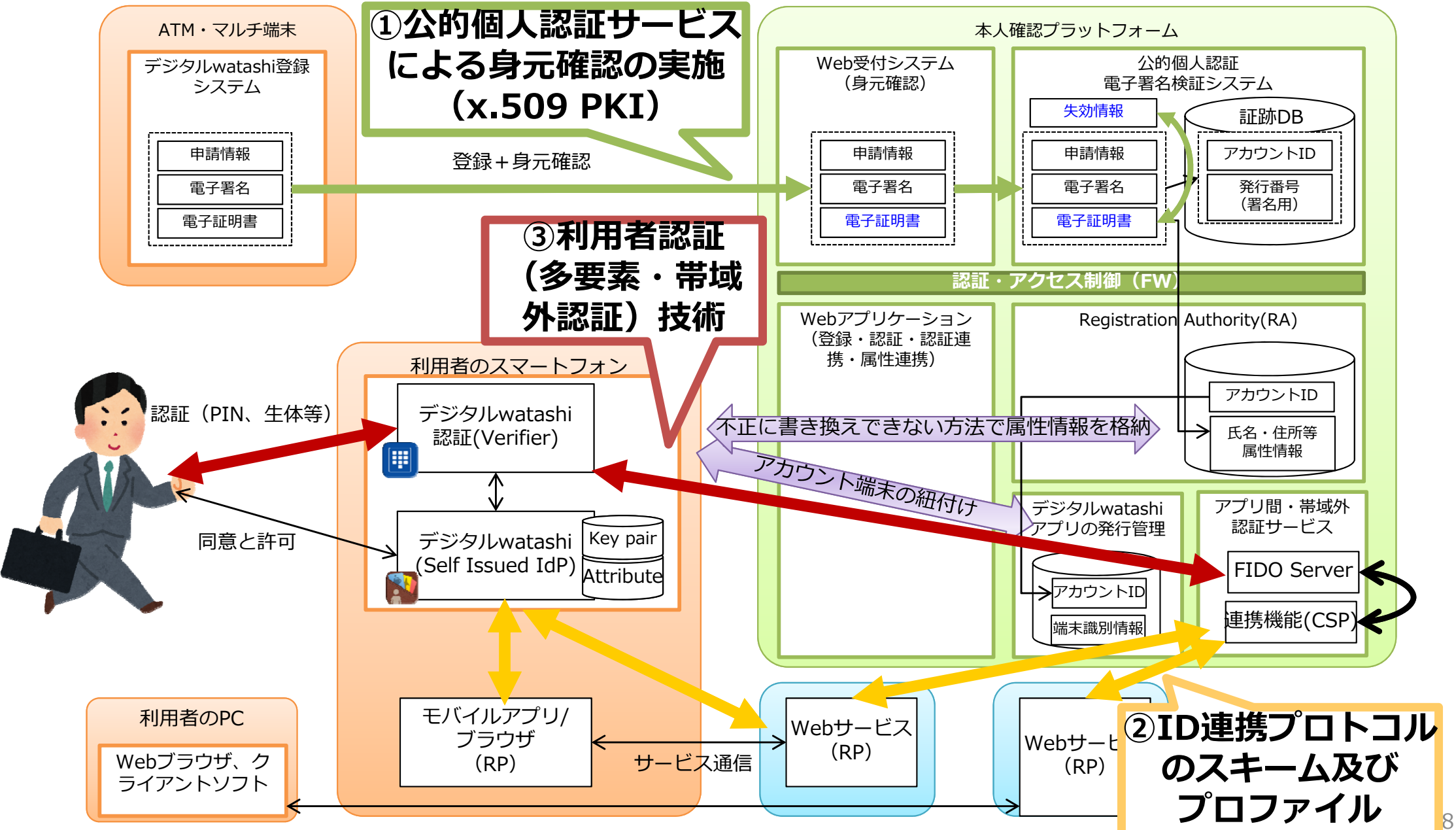
OpenID connectのself-issued OpenID Provider、FIDO　UAFや類似プロトコルに準拠（認証プラットフォーム事業者内のシステム）

電子署名の検証プロトコルに準拠（認証プラットフォーム事業者内のシステム）

ID連携プロトコル（OAuth対応）に準拠（認証プラットフォーム事業者、サービスA事業者、サービスB事業者で共有するシステム）

技術要件の検討・整理箇所

■ **①公的個人認証サービスによる身元確認の実施、②ID連携プロトコルのスキーム及びプロファイル、③利用者認証**という役割を分業することで、効率的に環境を実現できる。



技術要件のまとめ

デジタルwatashiアプリ技術要件の構成（案）

1. **登録と発行プロセス**
   - 公的個人認証サービスを用いた本人確認
   - 利用者の保有するスマホとアイデンティティの紐付け
2. **クレデンシャル管理**
   - クレデンシャルの生成、発行、有効化、更新等の要件
   - セキュアかつ安全なクレデンシャル発行方法（≒アプリの配布）
   - セキュアかつ安全なクレデンシャル再発行（個人番号カードを用いる）
3. **認証要素・認証プロセス**
   - デジタルwatashi認証アプリの要件
   - 認証には、当人確認保証レベル３以上の認証要素（又はその組合せ）を用いる
   - マルチデバイス連携の場合、帯域外認証を用いる
     - 帯域外認証（OTPなど）
   - アプリ間連携の場合、多要素認証を用いる
     - 多要素認証
       - 所有物（スマホ）＋生体（指紋など）
       - 所有物（スマホ）＋記憶（PIN、パターンなど）
4. **ID連携プロトコル（アサーション）**
   - デジタルwatashiアプリ（ID連携機能）の仕様
   - デジタルwatashiアプリにおけるID連携プロトコルの技術的要求事項
     - OpenID connect（OAuth）、SAML等。

①公的個人認証サービスによる身元確認の実施（x.509 PKI）

③利用者認証（多要素、帯域外認証）技術

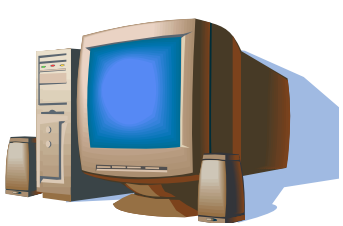
②ID連携プロトコルのスキーム及びプロファイル

PKIの抱える課題

ICカードを使ったPKIの場合、ICカードが必要

- PKIのICカードを使う場合、ICカードリーダが必要。
- 今後、デバイスの種類増加。
  - パソコン、タブレット、スマートフォン、スマートウォッチ、その他ウェアラブルデバイス

ハードウェアの標準構成
部品になるのか？



- CPU
- IDE
- DIMM
- PCI
- SCSI
- USB

電子署名をおこなうためのサーバとICカードのやり取りの複雑性

- サーバ－クライアントソフトウェア（ブラウザー等）間
  - 専用電子署名用クライアントソフトウェア（Windows Crypto API等）
  - java applet（Java Cryptography Extension）
  - W3C Web Crypto APIサポートブラウザー（W3C Web Crypto API）
  - その他（Digital Signing for ActiveX Components等）
- クライアントソフトウェア（ブラウザー等）－ICカードリーダー間
  - ICカードドライバーの対応状況依存

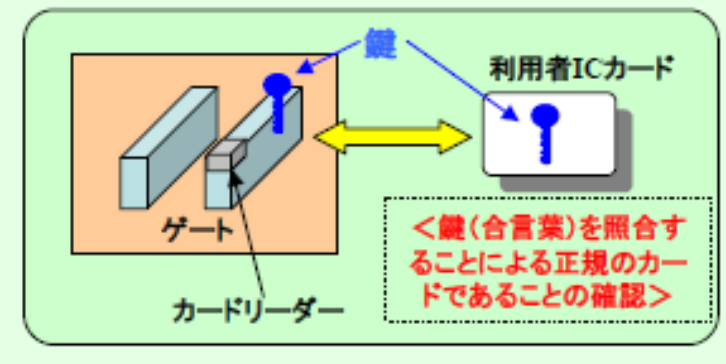
  Windows Crypto API等、Java Cryptography Extension、W3C Web Crypto API、Digital Signing for ActiveX Components等

単純なWebアプリケーションとは、全く異なり、サーバからICカードまでデータまでやり取りできなければいけない。

※サーバとICカードで電子署名でなく、データ交換（例えば、ID交換）をするだけであれば、「サーバ－クライアントソフトウェア（ブラウザー等）間」「クライアントソフトウェア（ブラウザー等）－ICカードリーダー間」のやり取りは、比較的複雑ではない。

※国家公務員のICカード

- 国家公務員のICカード身分証に関する基本仕様等

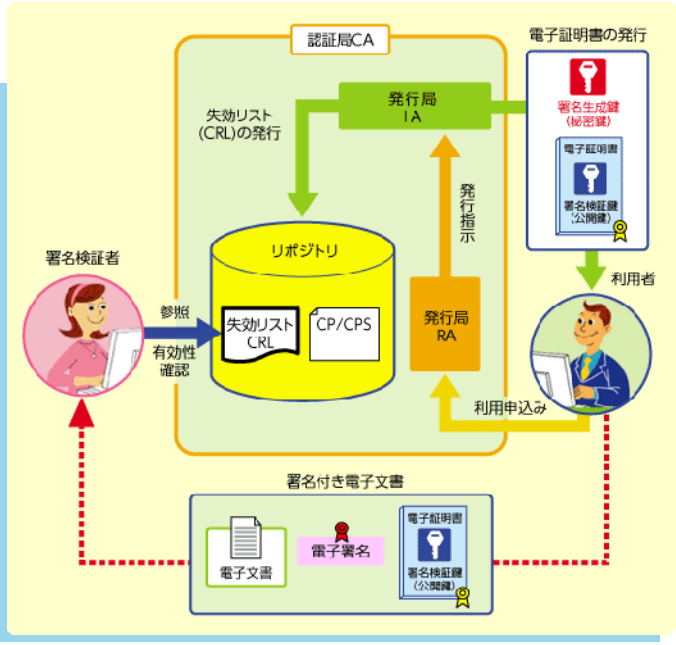


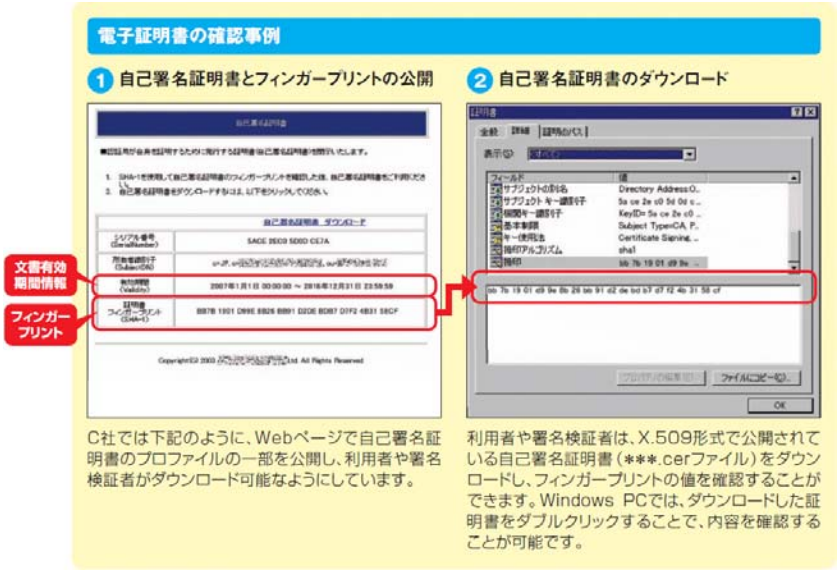
平成21年7月1日第37回CIO連絡会議
「国家公務員ICカード身分証の仕様及び運用ガイドラインの改定についての」資料より

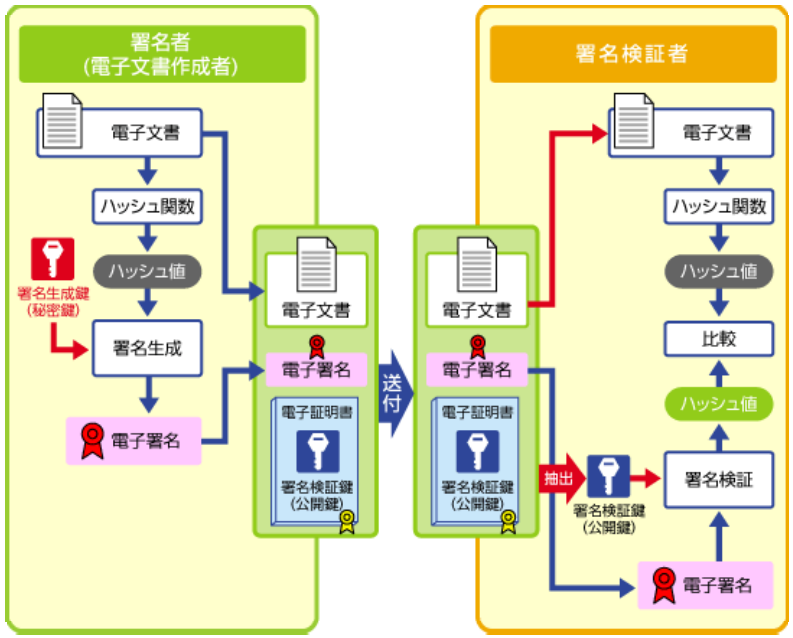
PKIの検証の複雑さ

- X.509フォーマットの電子証明書や電子署名の検証方法：
  - 電子証明書の記載事項
  - 電子署名の検証方法
  - 電子証明書のトラストパスの検証方法
  - 失効情報の検証方法

署名検証者／電子証明書の提示を受ける人の注意事項
- 電子証明書を発行した認証局の確認
- 電子証明書の失効情報等の確認







JIPDEC　電子署名・認証センターのホームページから引用

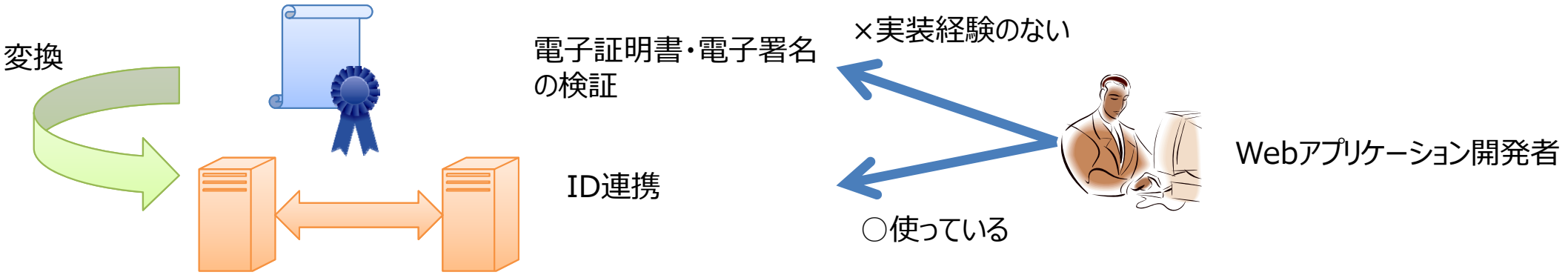
デジタルWatashiアプリで
PKIをサポートする

PKIからID連携への変換サービスの提供

- ほとんどの技術が実装したことのないX.509フォーマットの電子証明書や電子署名の検証をWebアプリケーション開発者が使ったことのあるID連携へ変換する。
  - PKIにおいては、電子証明書の記載事項は修正できない。電子証明書の記載事項を変更する場合、電子証明書の再発行をすることになる。権限を持って記載事項を修正するのであれば、ID連携等が親和性が高い。
- Webアプリケーション開発者のID連携を使う機会が増加
  - Facebookアカウント認証、twitterアカウント認証、YahooID認証等
- ID連携（OAuth等）での確認方法

SAML、OpenID connect等のID連携プロトコル、役割分担（IDP、RP）の関係性、IDPのURLの確認

- 「信頼ある」プロトコル、「信頼ある」IDP・RPは、重要である。そのため、トラストフレーム（ポリシーのリポジトリーや「信頼ある」IDPのURLリスト等）は、必要である。



身元確認と当人確認の使い分け

- 身元確認は、PKIの電子証明書・電子署名の確認を利用して、オンラインで確度の高い身元確認を実施。
- 当人確認は、PKIによる電子認証（電子署名技術の利用）ではなく、多要素認証を用いることにより、利便性の向上

	ビジネスプロセス	従来のオンラインサービスの場合での実現方法	デジタルwatashiでの実現方法
身元確認 Identity Proofing	サービスアカウントの開設、アカウント登録時の属性情報の確認。原則、サービス利用開始時のみにおこなう。	オンラインサービスでも、必要な場合、対面又は郵送等により確認。対面の場合、利用者が実在し、提示された属性情報であることを直接確認。又は、郵送等で証明書、実印により押印された申請書と印鑑証明書等により確認。	オンラインにより、マイナンバーカードの公的個人認証サービスの電子署名用電子証明書と電子署名による確認。
当人確認 Authentication	サービス利用時に毎回おこなう確認。そのため、属性情報を確認するのではなく、アカウントの所有のみを確認。	レベルの応じて、単要素認証（ID・パスワード等）、多要素認証（所有物＋パスワード等）、ICカードによる電子署名を利用した認証により確認。	スマホ上の「デジタルwatashi認証アプリ」を使って、多要素認証（スマホという所有物＋パスワードや生体認証等）により確認。

Authenticatorデバイスを位置づける

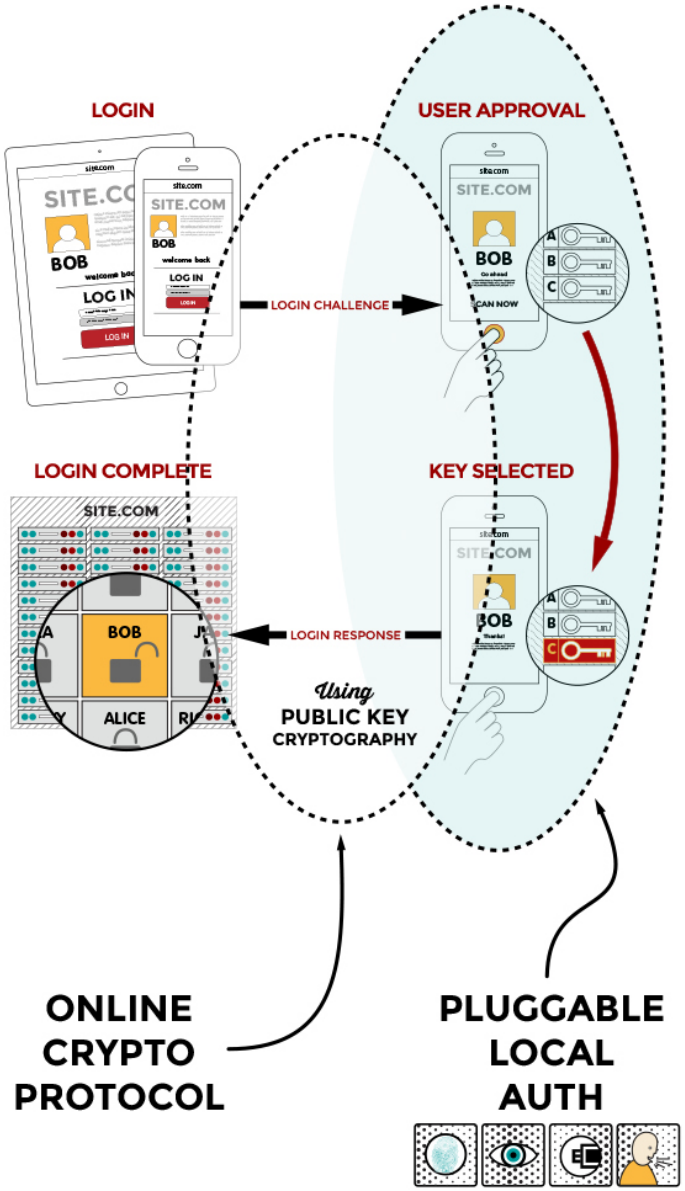
- ICカードを使ったPKIでの連携

人⇔ICカード⇔ ICカードリーダー⇔サービス利用端末⇔サーバ

- Authenticatorデバイスを使った連携

人－Authenticatorデバイス－サーバ

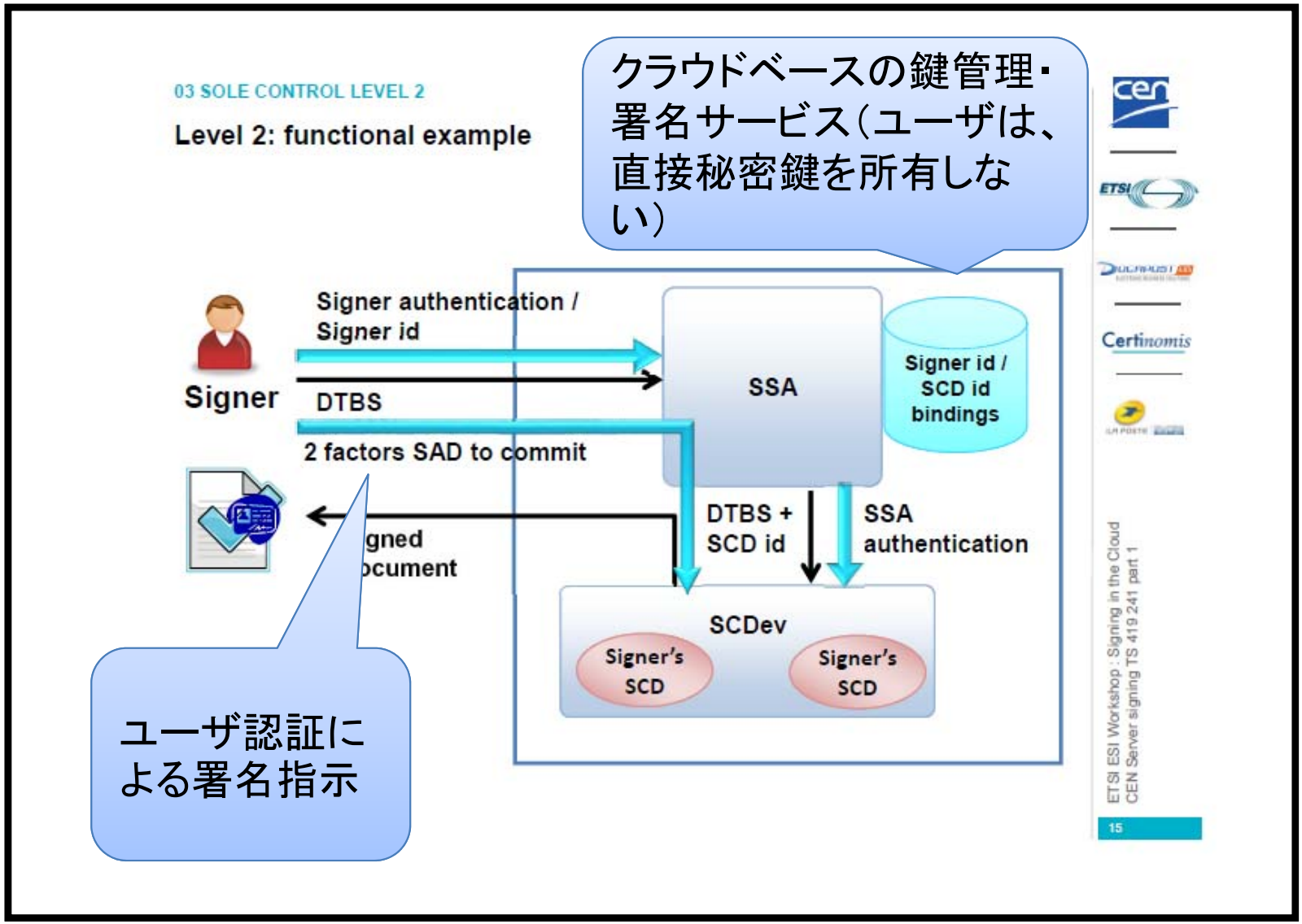
- Authenticatorデバイスのバリエーション
  - スマートフォン
  - ウェアラブルデバイス
  - PKI機能を使わないICカード
  - その他
- 従来のソリューションにおいては、サービス利用端末とAuthenticationは、同じデバイスを利用。一方、生体認証等に取り組んでいるFIDO　Allianceにおいては、明示的にFIDO Authenticatorや2nd Factorデバイスが定義されている。
- 結果として、Authenticatorデバイス以外のサービス利用端末でのサービスに関しては、単純化することができる。



FIDO (Fast IDentity Online) Allianceの資料より

今後の可能性

- リモート署名サービスとの組合せによるICカードなしでの電子署名の実現



ETSI ESI Workshop Barcelona, 14th March 2013 Signing in the Cloud CEN Server signing TS 419 241 part 1
https://docbox.etsi.org/workshop/2013/201303_SIGNATURES_IN_CLOUD/3b-CEN-Server-Signing.pdf

最後に

- 電子署名・電子認証は、利便性と安全性のバランスを取ることが重要。

利便性

- 一番理解しているのは、利用者である。
- ビジネスモデルにも大きな影響を与える。
- 技術者は、見失うことが多い。
  - PKIだから利便性が高いということは全くない。

安全性

- 利用者は、一般的には判断できない。
- 安全性は、①技術的安全性②運用面的安全性がある。まずは、①技術的安全性を考える必要がある。①技術的安全性を②運用面的安全性でカバーする場合もある。
- 専門知識を理解した人で議論すべきである。論点としては、安全性が高い低いが論点ではない。安全性が、妥当かどうかが論点である。