社会基盤としての
モバイルPKIの動向

2010年6月29日

東京工科大学
手塚　悟
tezuka@cs.teu.ac.jp

目次

目次

1. モバイルPKIの背景

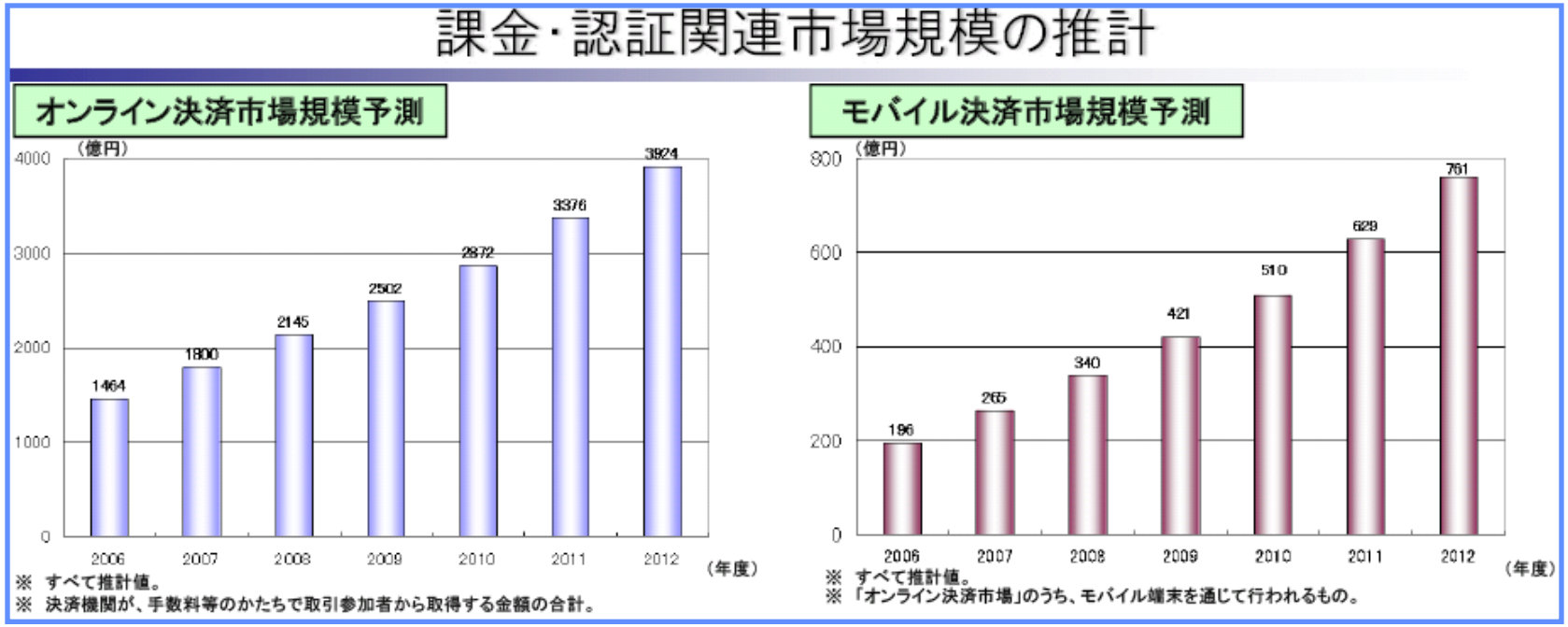
●各種端末の普及率

端末の種類	普及率
パソコン	71.0%
携帯電話	88.0%
テレビ放送受信機	99.5%

※1:主要耐久財費財等の普及率(一般世帯)「内閣府　消費動向調査　平成19年3月」を参考

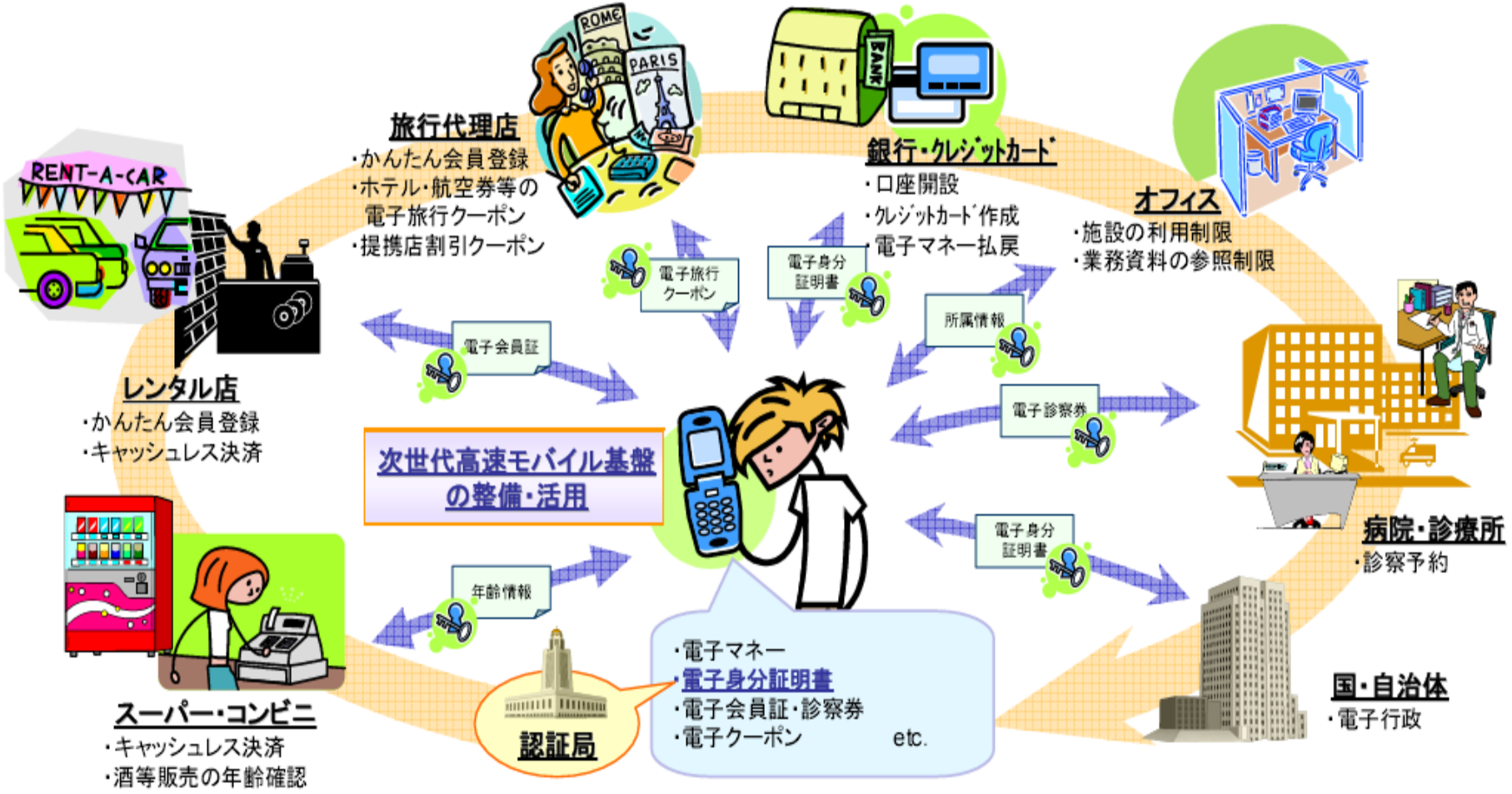
1. モバイルPKIの背景

- 今まで以上に、携帯電話の安全性が必要
  - 携帯電話は単なるコミュニケーション手段としてではなく、各種サービスを享受するためのアクセス手段として利用するケースが増えてきている。



「通信プラットフォーム研究会」参考資料A（補足資料）（2009/1/30, 総務省）より

1. モバイルPKIの背景



「IT新改革戦略政策パッケージの概要について」(H19/4/5) http://www.kantei.go.jp/jp/singi/it2/kettei/070405gaiyou.pdf

1. モバイルPKIの背景

- 今まで以上に、携帯電話の安全性が必要
  - 携帯電話の契約台数は1億台を突破(*)しており、携帯電話の利用率は、PCの利用率よりも高い。
  - 誰もが一台保有している携帯電話を用いてサービスを享受することで、さまざまなサービスのオンライン利用率の向上が期待される。
  - 常に持ち歩く携帯電話ならではの使い方が、従来のPCなどとは異なり、常時持ち歩く特徴を生かした新たなサービス用途が拡大する。

(*) 社団法人電気通信事業者協会(TCA)によると、09年6月末時点で携帯電話の契約数は108,488,700 台、携帯電話・PHSの契約数合計は113,024,800 台にのぼる。

1. モバイルPKIの背景

国民が実感できる実現目標:

高度なセキュリティを実現した本人認証技術を活用して、電子行政サービス等の本人認証が必要な場合も含め、携帯端末により、ペーパーレス、キャッシュレスはもとより、多様なネットワークサービスを飛躍的に安全かつ簡易に利用可能となる世界最先端の次世代モバイル生活基盤を2010年を目途に構築する。

「IT新改革戦略政策パッケージの概要について」
(H19/4/5)より

次世代モバイルライフワーク基盤の要件:

(1)電子行政サービスや銀行口座の開設等における本人確認を実現するために、
信頼できる認証基盤であること
(2)ペーパーレス、キャッシュレス等の多様なサービスに対応できる認証基盤であること

次世代モバイルライフワーク基盤実現に向けての課題:

(1)サービス要求の分析と、最適なモバイル認証に関する方式、運用、制度の検討
(2)高信頼な本人確認を実現する電子証明書(本人確認基盤)を、携帯電話等に搭載するための検討 (例:JPKIのモバイル適応)
(3)多様なサービスへの対応を実現するキャリア証明書との連携方法の検討(例:属性証明書の利用)

目次

2. モバイルPKIの現状

■現状のモバイルサービスでは以下のような様々な認証方式が用いられている

- ID/Password
- 電番(MSISDN)
- 機体番号(UTN)
- オペレータ付与ID(subscriber-ID)
- CP付与ID(マイボックス)
- 生体認証(顔、指紋)
- 加入者証明書(Security Pass, FirstPass)
- 他社証明書(VeriSign Managed-PKI, オリジナル証明書)

2. モバイルPKIの現状

■さらに現状のモバイルサービスの認証方式を整理する

オペレータ管理ID

- ●オペレータ付与ID(iﾓｰﾄﾞID、ｻﾌﾞｽｸﾗｲﾊﾞID、ﾕｰｻﾞID)
- ●加入者証明書(FirstPass、 Security Pass)

メーカー管理ID

- ●機体番号(FOMA端末製造番号、FOMAｶｰﾄﾞ製造番号、端末ｼﾘｱﾙ番号)

その他

- ●他社証明書(VeriSign マネージドPKI for Mobile, オリジナル証明書)

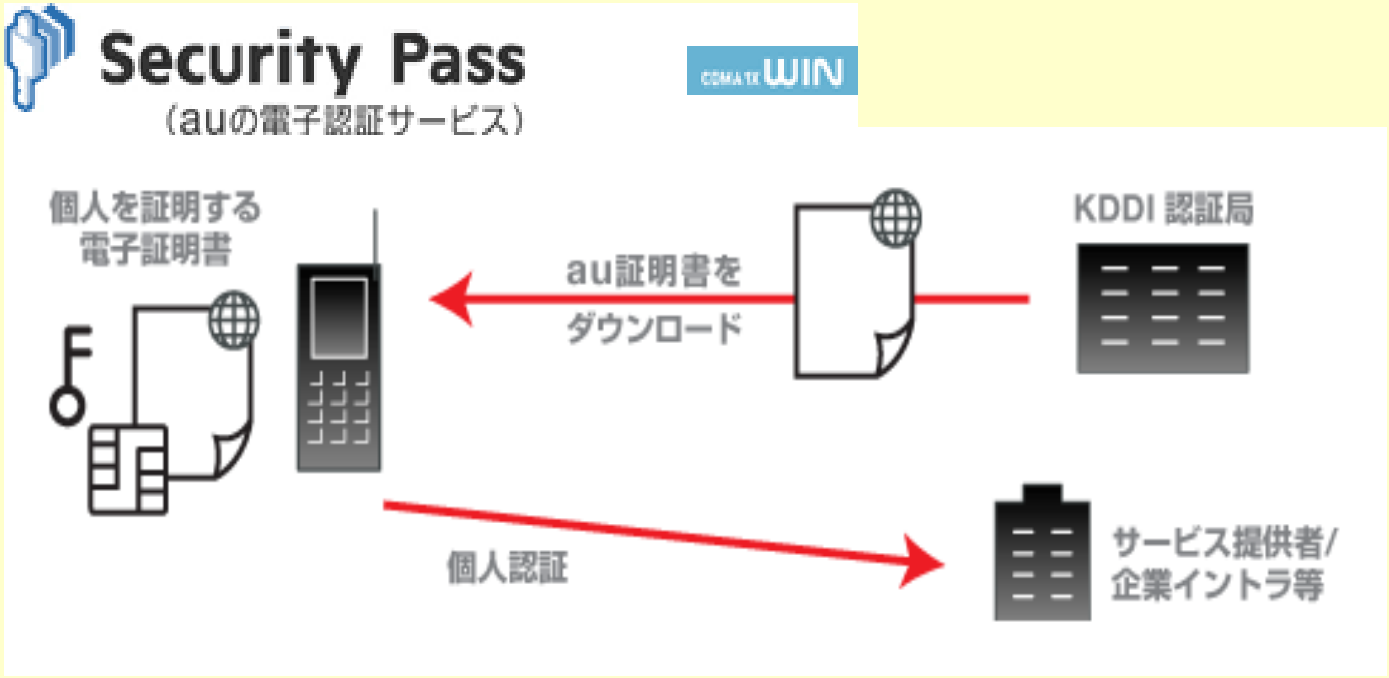
2. モバイルPKIの現状

SSLクライアント認証(NTTドコモ)

http://www.docomo.biz/html/product/firstpass/index.html

2. モバイルPKIの現状

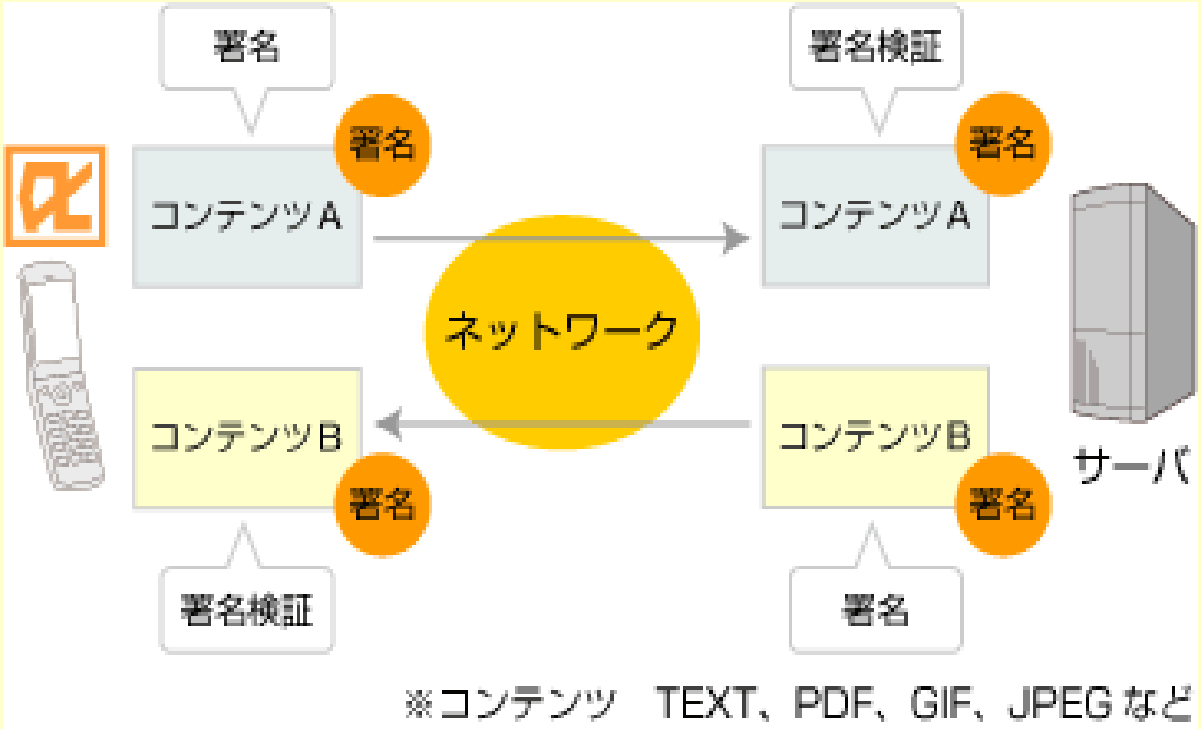
SSLクライアント認証(au by KDDI)



http://www.au.kddi.com/notice/securitypass/

2. モバイルPKIの現状

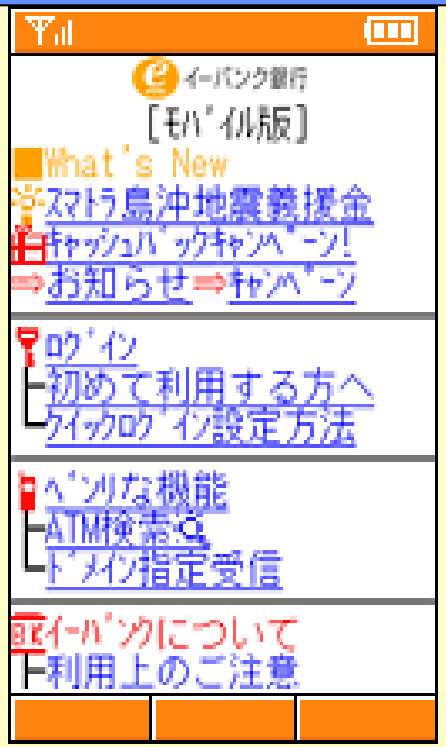
電子署名



http://www.docomo.biz/html/product/firstpass/index.html

2. モバイルPKIの現状

サービス例(イーバンク銀行)



- 利用可能な電子証明書
  - FirstPass
  - Security Pass

http://www.au.kddi.com/notice/securitypass/

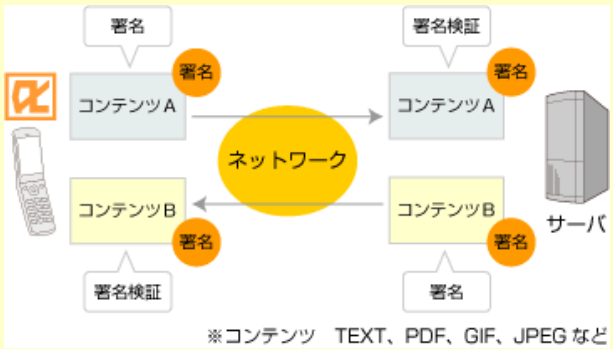
2. モバイルPKIの現状

- FirstPass、Security Passは従来のID／パスワード認証に代わる「PKI技術」を使った電子認証サービス
- 面倒な入力が必要なく、キャリアが発行したキャリア証明書を対応サイトへ送信するだけで簡単に認証が行える

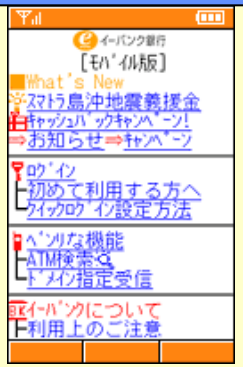
SSLクライアント認証（NTTドコモ）

SSLクライアント認証（au）

電子署名



サービス例（イーバンク銀行）



- 利用可能な電子証明書
  - FirstPass
  - Security Pass

http://www.docomo.biz/html/product/firstpass/index.html

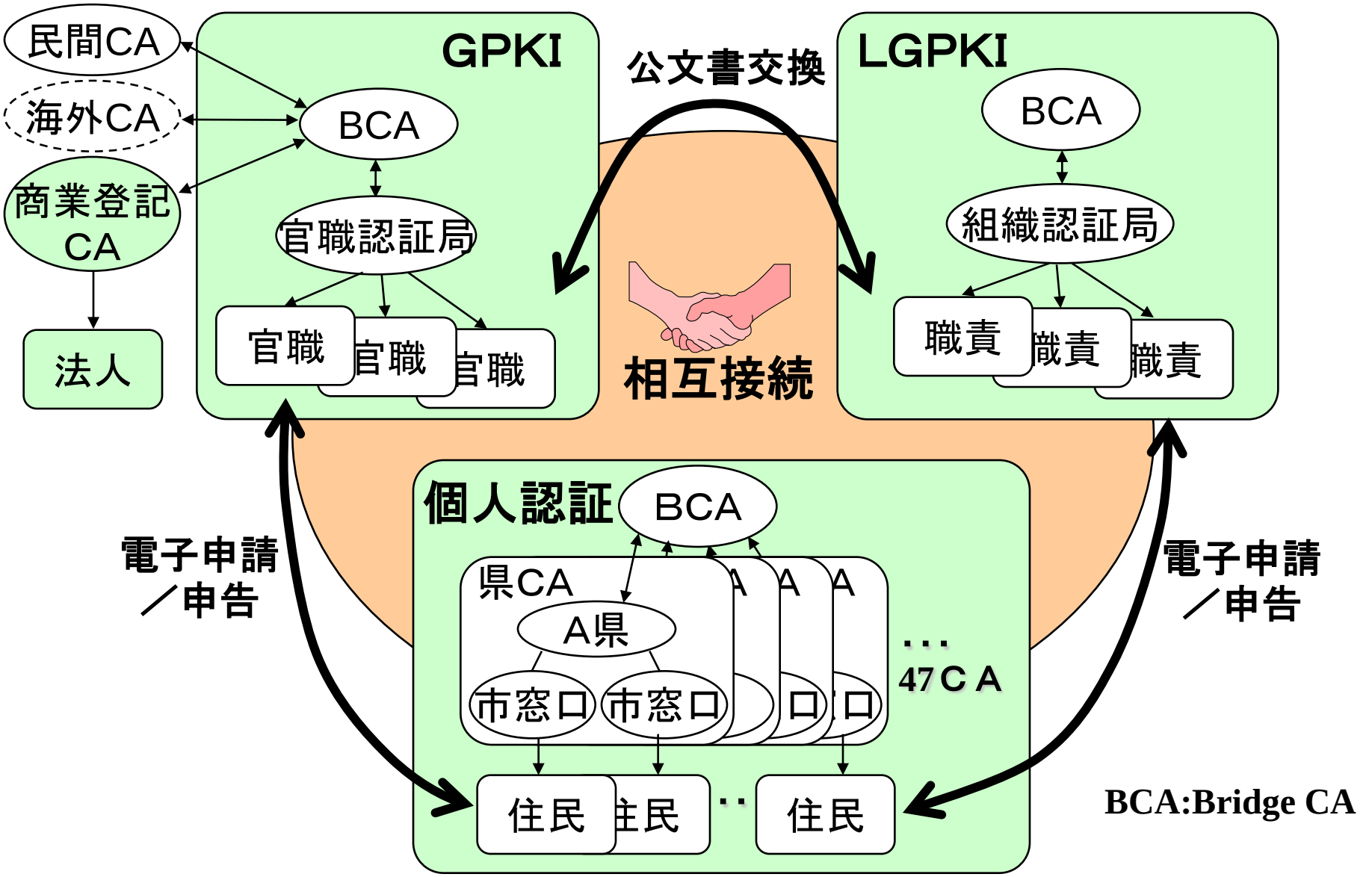
http://www.au.kddi.com/notice/securitypass/

目次

3. モバイルPKIと電子政府・電子自治体の関係

認証基盤名	発行者		ユーザ		法律	用途
GPKI	官	官職CA	官	政府官職		G to G,B,C
LGPKI		組織CA		地方官職		G to G,B,C
法務省商業登記		法務省	民	法人代表者	○	B to G,B,C
公的個人認証サービス		県知事		住民	○	C to G
認定認証業務	民	民間事業者		自然人	○	C to G,B,C
その他の認証局		民間事業者等		人、物、アドレス、他		B,C to B,C

3. モバイルPKIと電子政府・電子自治体の関係



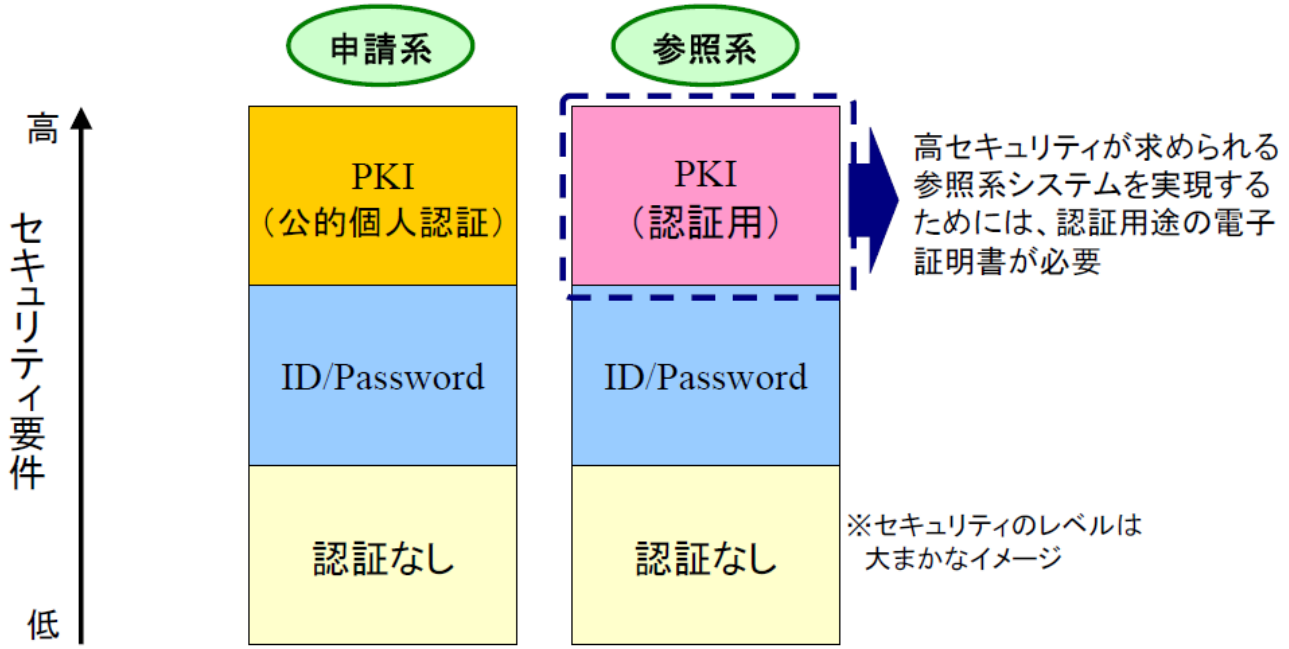
3. モバイルPKIと電子政府・電子自治体の関係

申請システムと参照システムにおける認証

電子行政システムは、大きく以下の2パターンに分類。

◆申請系システム：署名が要求される電子文書のやりとりを伴う手続き
◆参照系システム：行政が保管する自身の個人情報等を、必要なときにすぐに確認できるようなオンライン手続き

それぞれのシステムにおいて必要な認証技術は下図のようなイメージ。



※参照系であっても、申請系の手続き（情報参照の申請）として構成することは可能。

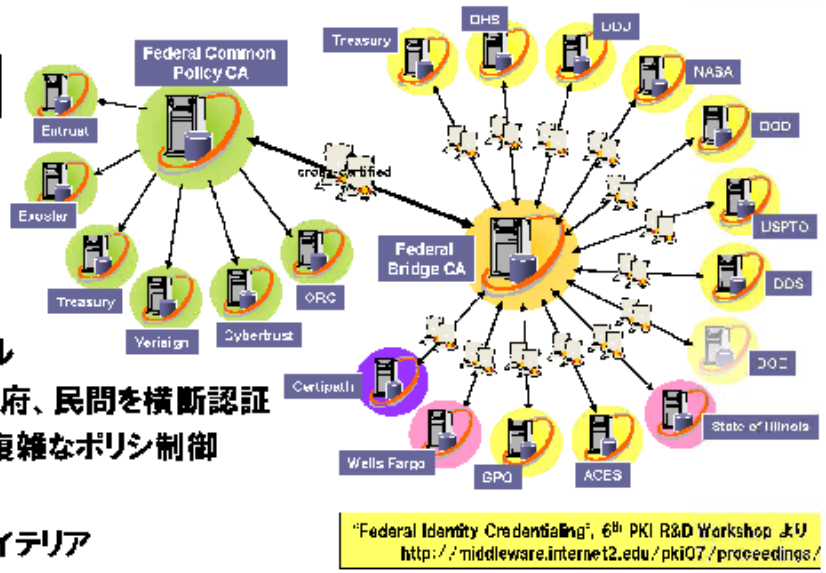
1

出典：公的個人認証サービスの利活用のあり方に関する検討会（資料2）
http://www.soumu.go.jp/menu_03/shingi_kenkyu/kenkyu/kojin_ninsho/071211_2.html

3. モバイルPKIと電子政府・電子自治体の関係

Challenge PKI Project
The Multidomain PKI Interoperability Framework

Federal PKI



"Federal Identity Credentialing", 6th PKI R&D Workshop より
http://middleware.internet2.edu/pki07/proceedings/

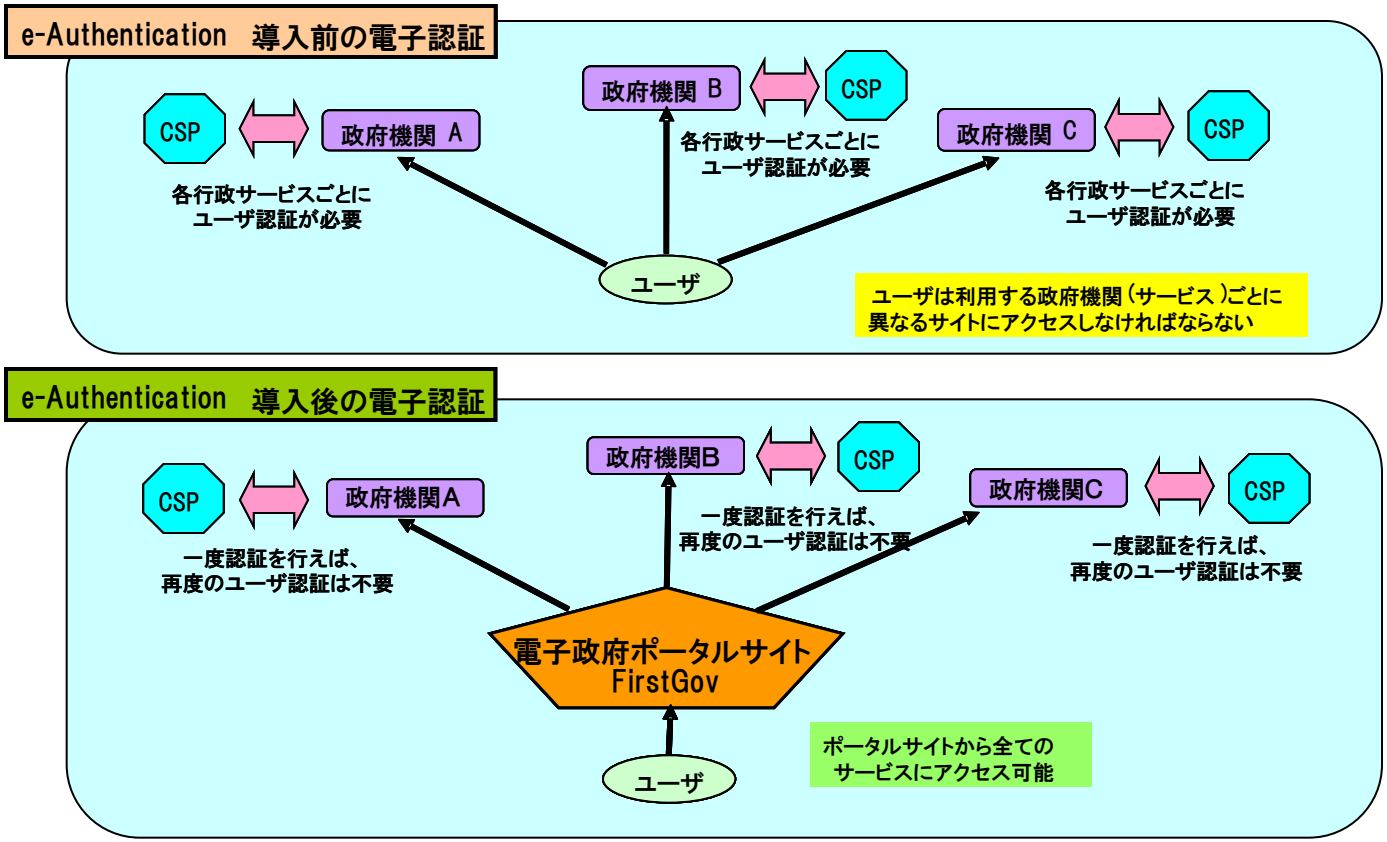
- 米連邦政府のPKI
- 大規模なブリッジモデル
  - 連邦政府省庁、州政府、民間を横断認証
  - 複雑な認証パスと、複雑なポリシ制御
- コモンポリシの整備
  - 4レベルのポリシクライテリア
    - High, Medium, Basic, Rudimentary
  - 各CAのポリシをいずれかにマッピング
- コモンポリシにもとづく共用CAサービスの提供
  - Shared Service Provider
  - C4CA (Citizen and Commerce Class Common CA)

2007/06/25 PKI day 2007 5

出典:PKI day 2007「PKIドメインを確立するには」
http://www.jnsa.org/seminar/2007/070625/data/03_shimaoka.pdf

3. モバイルPKIと電子政府・電子自治体の関係

- 政府機関が実施する電子政府プログラムにおける認証技術のニーズを満たすと共に、各政府機関において横断的に利用可能な共通の認証インフラを構築すること(政府機関を横断したシングルサインオン(SSO)の実現)を目的としている。



出典:mITF MC部会平成18年度活動報告書
http://www.mitf.org/public_j/archives/index.html

3. モバイルPKIと電子政府・電子自治体の関係

- NISTガイドラインに規定されている「保証レベル」と「使用すべき認証トークン」との対応を表す。
- 保証レベルが1あるいは2ではPINかパスワードによる認証が利用できるが、保証レベルが3以上の場合にはPINやパスワードの利用は許可されず、ワンタイムパスワードや暗号化されたトークン(具体的には電子証明書など)を用いることが要求される。
- このように、複数の保証レベルを提供し、サービスによって最適な認証を選択できる。

表　NISTガイドラインが規定する保証レベルに対応した認証トークン

	保証レベル （詳細は付録3）			
利用可能なトークン	1	2	3	4
特別なハードウェアデバイス(FIPS140－2 全体Level2、物理セキュリティLevel3相当以上)に格納された暗号鍵	✓	✓	✓	✓
一般的なPCあるいはハードウェアトークン(FIPS140－2Level1相当以上)に格納された暗号鍵	✓	✓	✓	
ワンタイムパスワード生成装置	✓	✓	✓	
パスワードを開示せずにパスワードを知っていることを証明する	✓	✓	✓	
強度の高いパスワード	✓	✓		
個人識別番号	✓	✓		

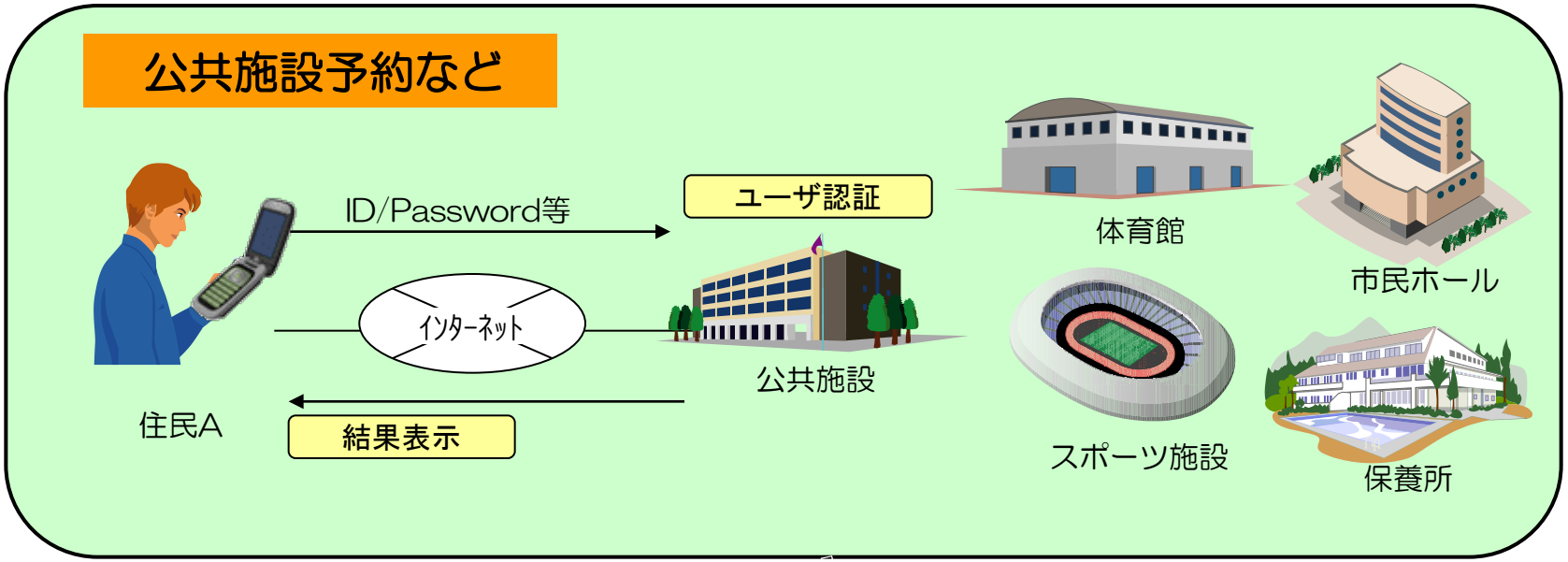
出典：mITF MC部会平成18年度活動報告書　http://www.mitf.org/public_j/archives/index.html　より作成

- モバイルでの利用シーンではレベル3くらいまでが主流（普通実印は持ち歩かない）
- モバイルでレベル4を利用するには課題が多い。
  - 実装上の課題：耐タンパハードウェアを前提とするため、既存の移動機での対応は難しく、実装コストの増大が必至である。（競争の激しい移動機価格へも反映される）
  - 利用上の課題：保証レベル4の認証は、実印相当の効力が想定される。この場合、盗難や誤使用、詐欺のリスクが高い。たとえ移動機のセキュリティを向上させたとしても、そもそもモバイルで持ち歩くこと自体に抵抗が想定される。

3. モバイルPKIと電子政府・電子自治体の関係

(1)公共施設予約サービス
～主な特徴～

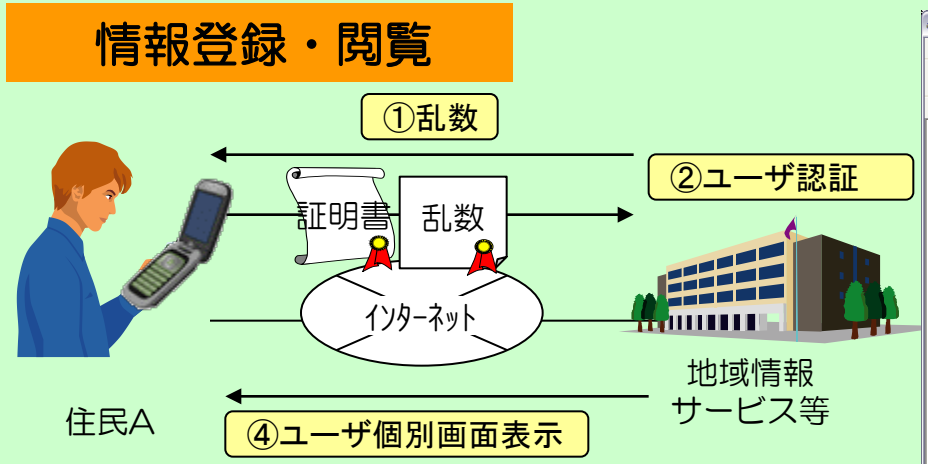
- 電子証明書を利用しない
- 簡易、気軽に使えることの方が重要な公共施設予約など
- 必ずしも4情報全てを出す必要もない



3. モバイルPKIと電子政府・電子自治体の関係

(2)地域情報登録・閲覧サービス
～主な特徴～

- 電子証明書を参照系として利用する
- 市民参加型地域生活情報サイト「深ナビ」
- 《公的個人認証サービス》を活用した投稿者(情報提供者:お店)の本人確認によって情報の安全性や信頼性を保っている。



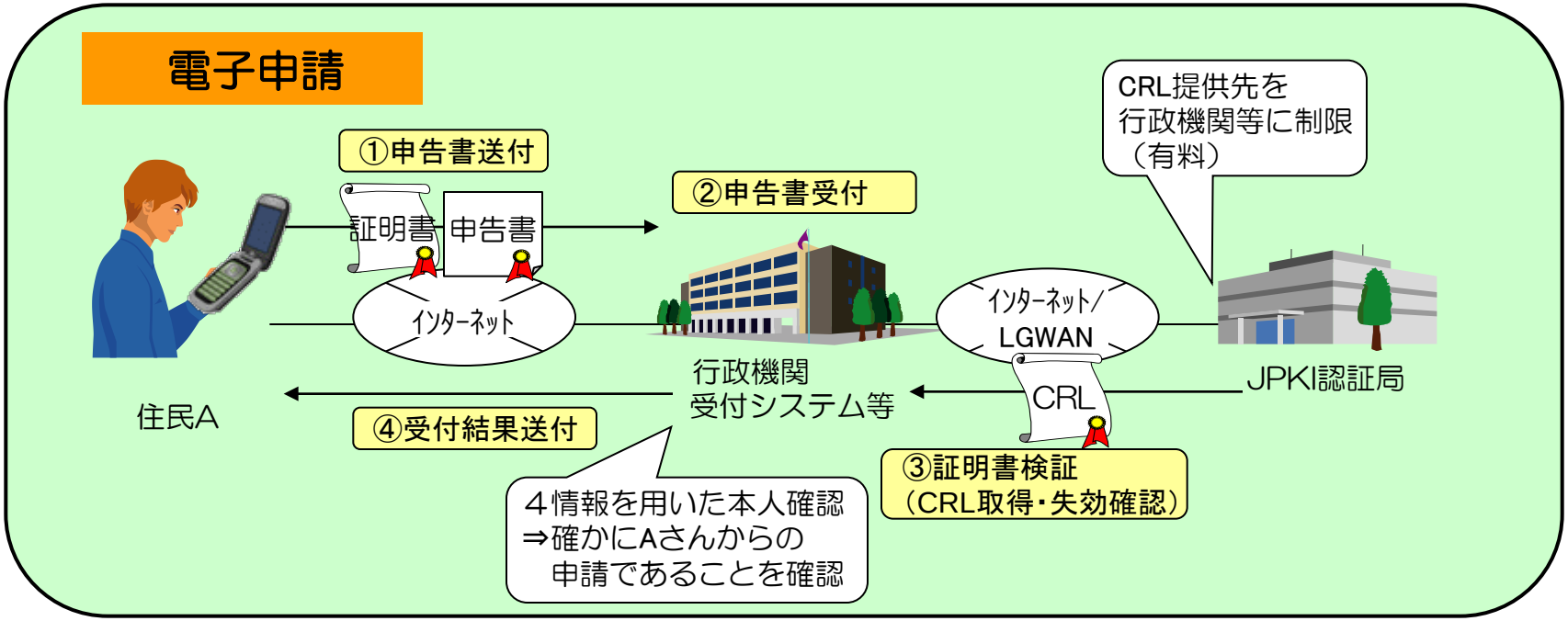
http://www.fukanavi.com/

3. モバイルPKIと電子政府・電子自治体の関係

(3)電子申請サービス

～主な特徴～

- 電子証明書を申請系として利用する
- 申告書の電子データに電子署名と電子証明書を付与して行政機関へ送付
- 行政機関は電子証明書の有効性を確認(認証局から失効リスト(CRL)を取得)
- 電子証明書に記載された4情報での本人確認が可能
- ただし、CRL提供先は行政機関や認定認証事業者等に制限



3. モバイルPKIと電子政府・電子自治体の関係

●社会基盤としてのモバイルPKI実現の課題

本人認証の手段

- 公的カード
  免許証、保険証、パスポート
- 公的個人認証
  住民基本台帳カードと公的個人認証システム
- キャリア証明書(モバイルID証明書)
- 金融事業者証明書
- 医療向け認証基盤(HPKI)

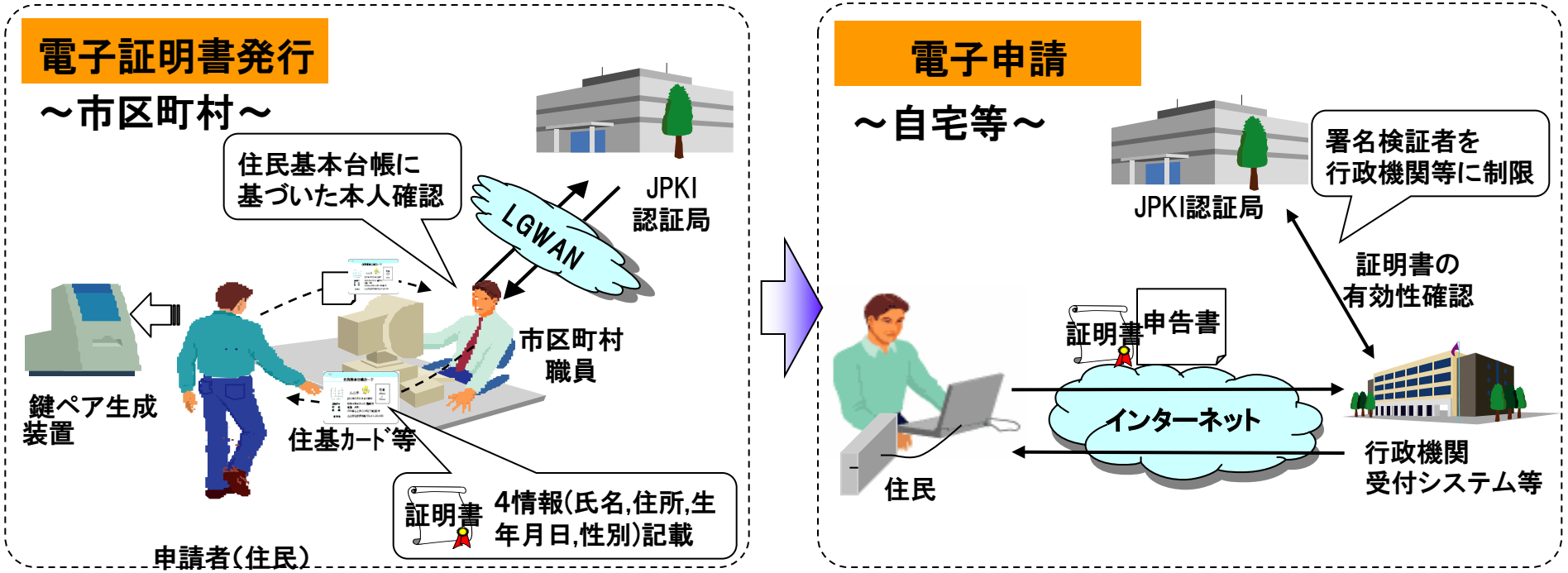
整理すべき主な課題

- どうやって携帯電話に格納するのか
- 魅力ある利用シーンの創出
- 本人認証の方式は？
- 外部I／Fの方式
  Type A／Type B／FeliCa/NFC？
- かざすインフラ整備
  コスト負担、誰が整備？

3. モバイルPKIと電子政府・電子自治体の関係

【現状のJPKIの特徴】

- 市町村窓口で住民基本台帳に基づいた本人確認を実施
- 利用者の証明書に4情報が記載
- 格納媒体は住基カード等のICカード
- 証明書の種類は「電子署名用」(否認防止等に利用)
- 署名検証者を行政機関等に制限(電子申請に利用されることを想定)



3. モバイルPKIと電子政府・電子自治体の関係

携帯電話の利用シーンを整理し、ユーザやサービスにとって有効な利用形態を検討する必要があります。

■証明書の利用パターン

（1）携帯電話でJPKI証明書をそのまま利用する
- ・JPKI証明書を用いて本人確認を行い、サービスを利用する
- ・特定認証事業者が発行する証明書を用いて本人確認を行い、サービスを利用する　等

（2）JPKI証明書を用いて本人確認を行い、多様な証明書を発行する場合
- ・JPKI証明書／民間証明書を用いて本人確認を行い、属性証明書を発行する
- ・JPKI証明書／民間証明書を用いて本人確認を行い、認証用証明書を発行する　等

（3）多様な証明書を用いてサービスを利用する場合
- ・属性証明書（モバイルID証明書※等と紐付けて発行）を利用した電子クーポン、電子会員証
- ・認証用証明書を利用したアクセス制御
- ・JPKI証明書による本人登録と、それ以降のモバイルID証明書でのアクセス制御　等

■利用形態のパターン

①リモートでの利用
携帯電話のブラウザ等から、直接サービスを利用する形態

②パーソナルでの利用
PCからR/Wを通して携帯電話の情報（証明書）を読み取り、サービスを利用する形態

③ローカルでの利用
携帯電話をサービス側のR/Wに直接かざしてサービスを利用する形態

※モバイルID証明書：FirstPass, Security Pass等

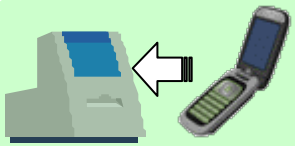
3. モバイルPKIと電子政府・電子自治体の関係

発行時　特徴：既存のJPKI証明書の発行と同レベルの本人確認が必要

●市役所での対面発行

～市区町村～

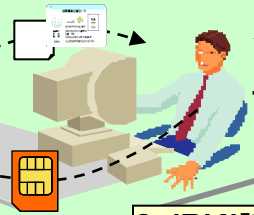
1.住民基本台帳に基づいた本人確認



鍵ペア生成装置

【課題①】：SIMへの証明書の搭載

申請者（住民）



市区町村職員

LGWAN

JPKI認証局

【課題②】：役所へ出向く手間

2.JPKI証明書発行

JPKI証明書

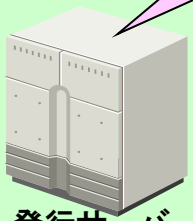
4情報（氏名、住所、生年月日、性別）記載

●既に発行済みのJPKI証明書を用いてのリモート発行

1.発行申請

JPKI証明書

【課題④】：有効性確認の方法



2.JPKI証明書による本人確認

発行サーバ

3.（モバイル用）JPKI証明書発行

【課題⑤】：モバイル網を使った（OTA）発行方式

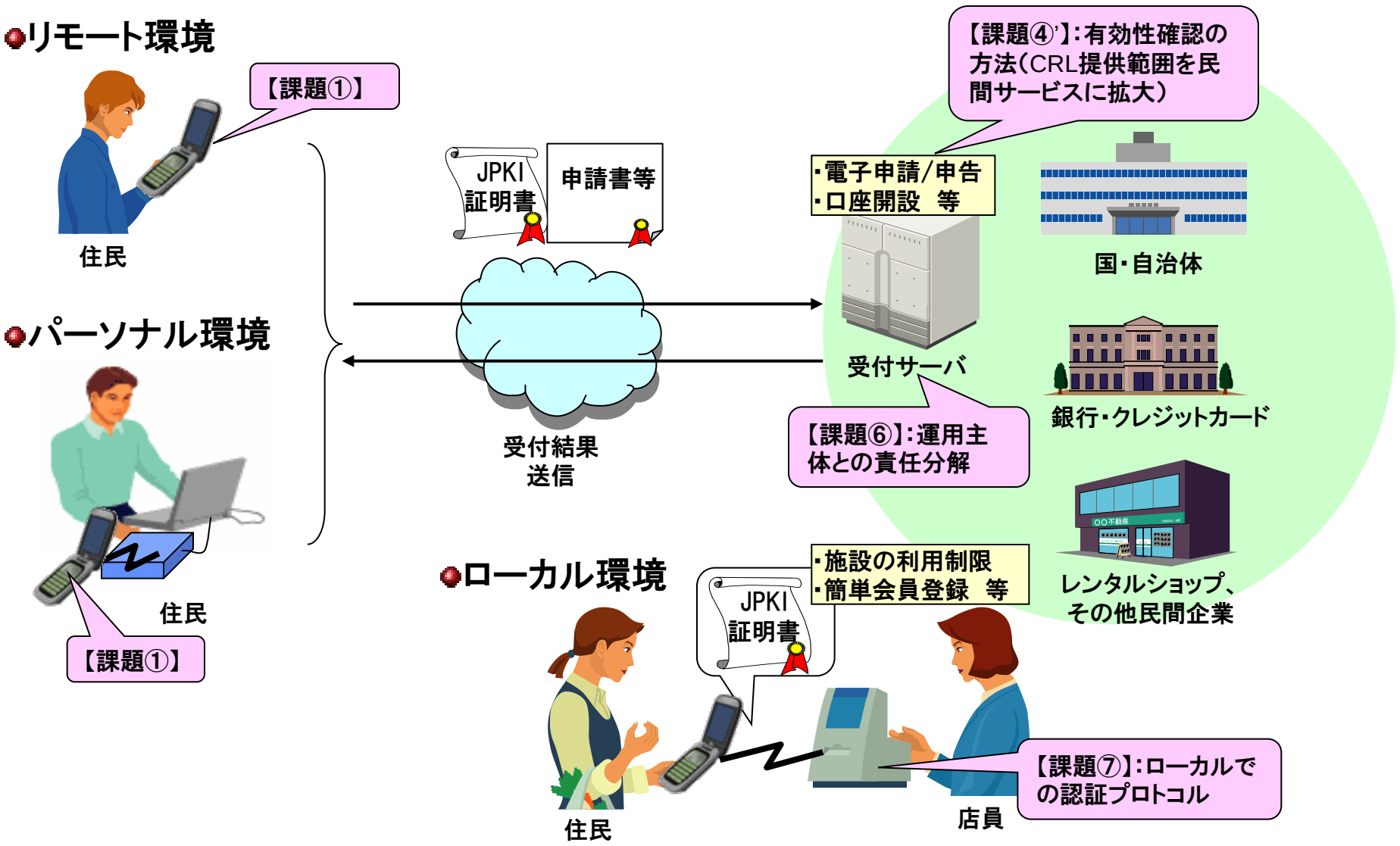
4.（モバイル用）JPKI証明書配布

JPKI証明書

【課題③】：JPKIカードとリーダの普及

3. モバイルPKIと電子政府・電子自治体の関係

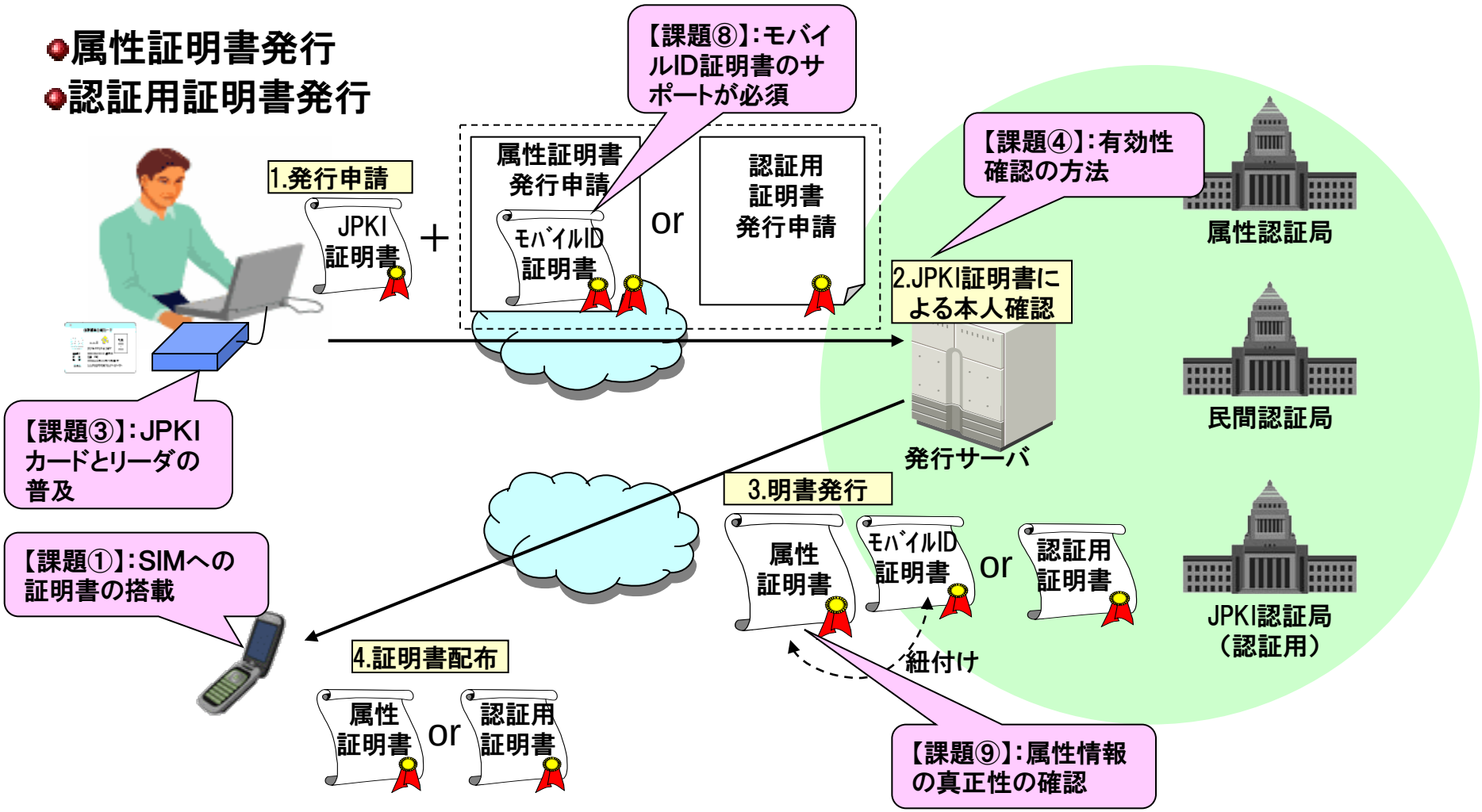
利用時　特徴：既存のJPKI証明書と同等のサービスが受けられる



3. モバイルPKIと電子政府・電子自治体の関係

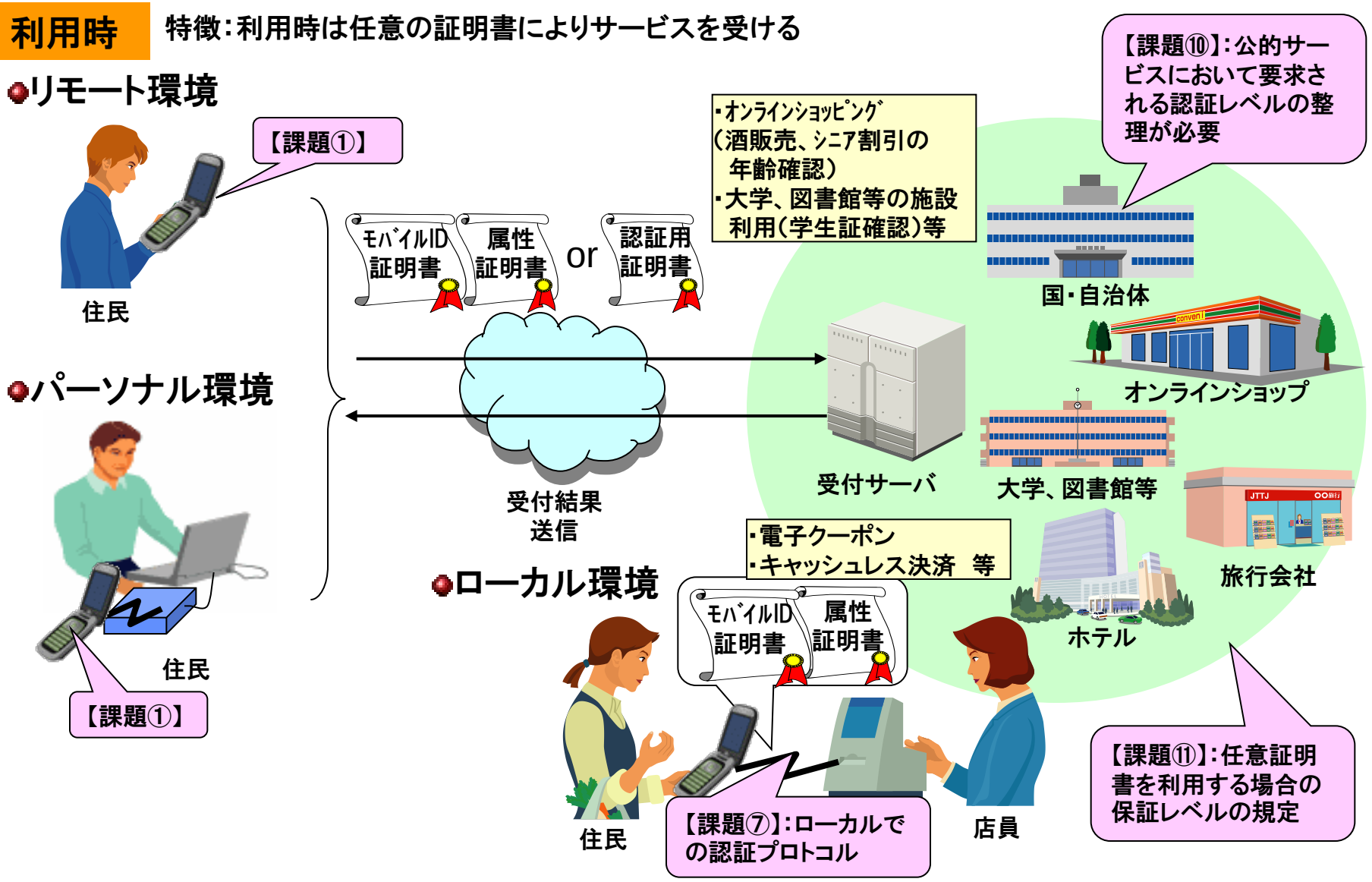
発行時　特徴：JPKI証明書により厳密な本人確認が行える

- 属性証明書発行
- 認証用証明書発行



3. モバイルPKIと電子政府・電子自治体の関係

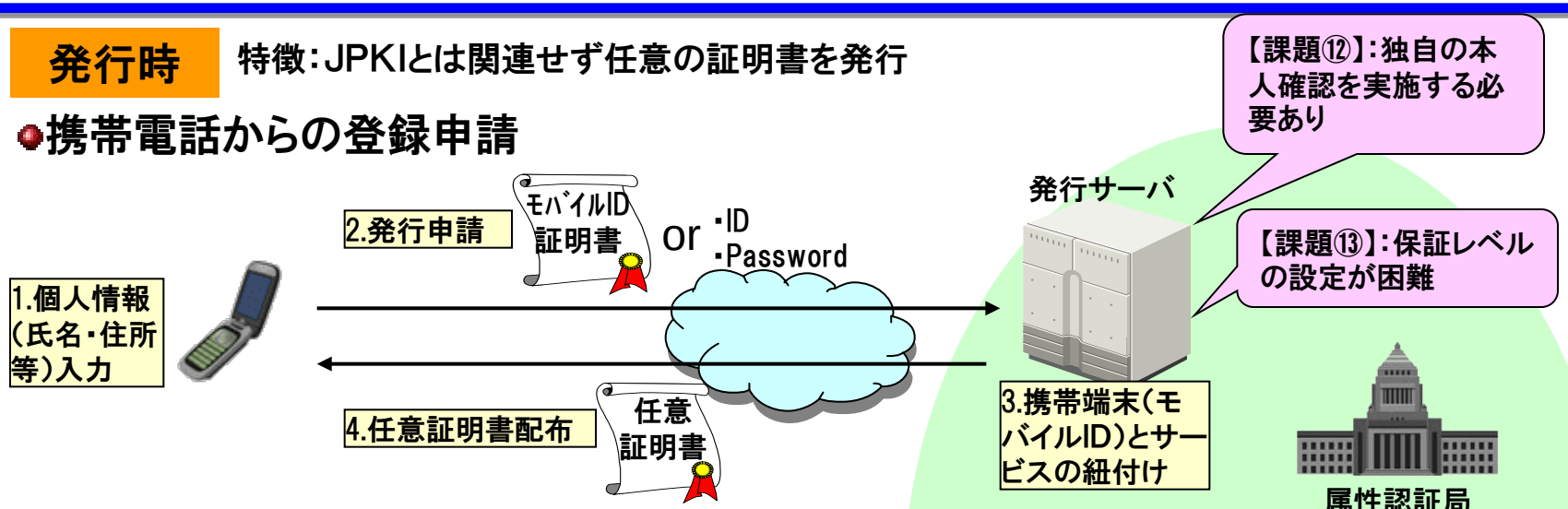
利用時　特徴：利用時は任意の証明書によりサービスを受ける



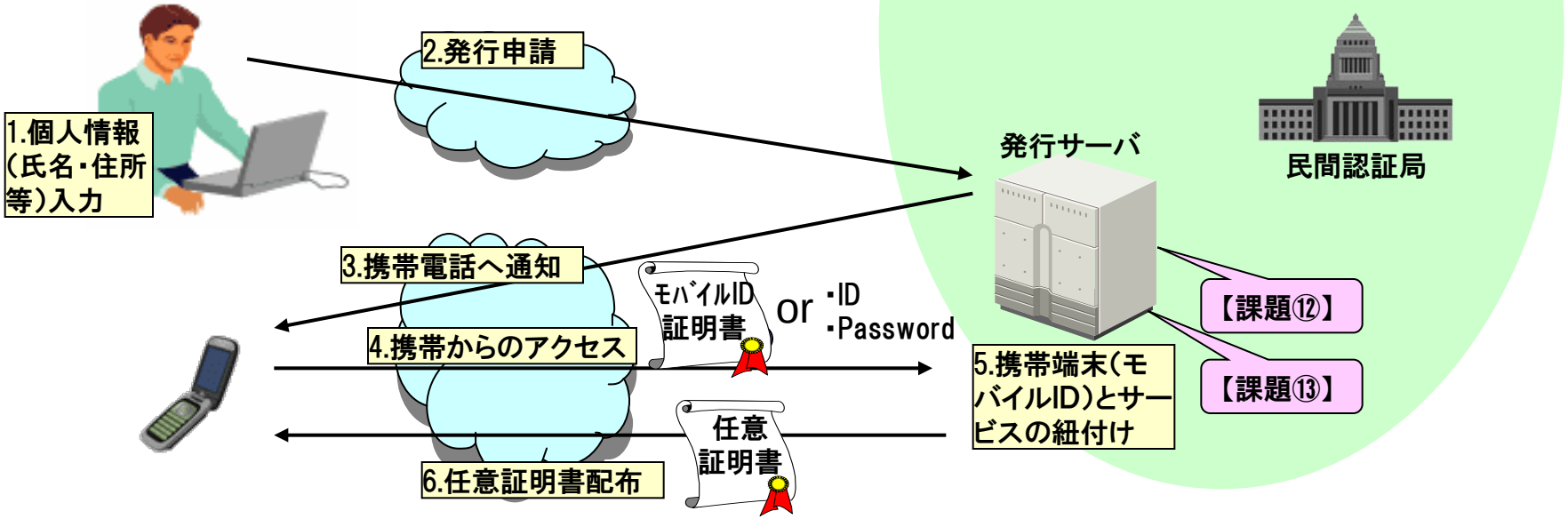
3. モバイルPKIと電子政府・電子自治体の関係

発行時　特徴：JPKIとは関連せず任意の証明書を発行

●携帯電話からの登録申請



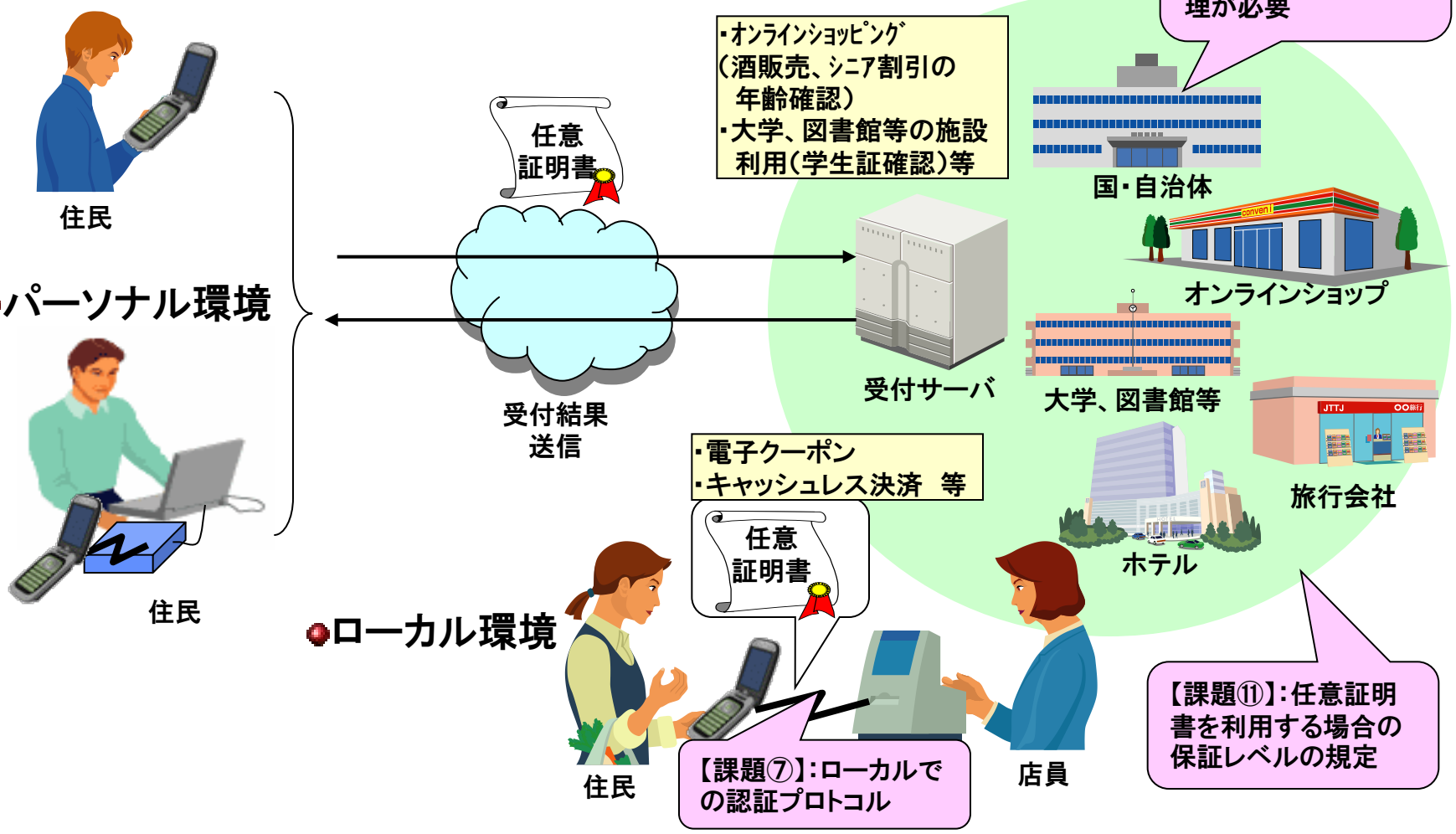
●PCからの登録申請



3. モバイルPKIと電子政府・電子自治体の関係

利用時　特徴：利用時は任意の証明書によりサービスを受ける

- リモート環境
- パーソナル環境
- ローカル環境



目次

4. モバイルPKIの今後

●携帯電話からの次世代電子行政・電子私書箱等へのアクセス手段の分類

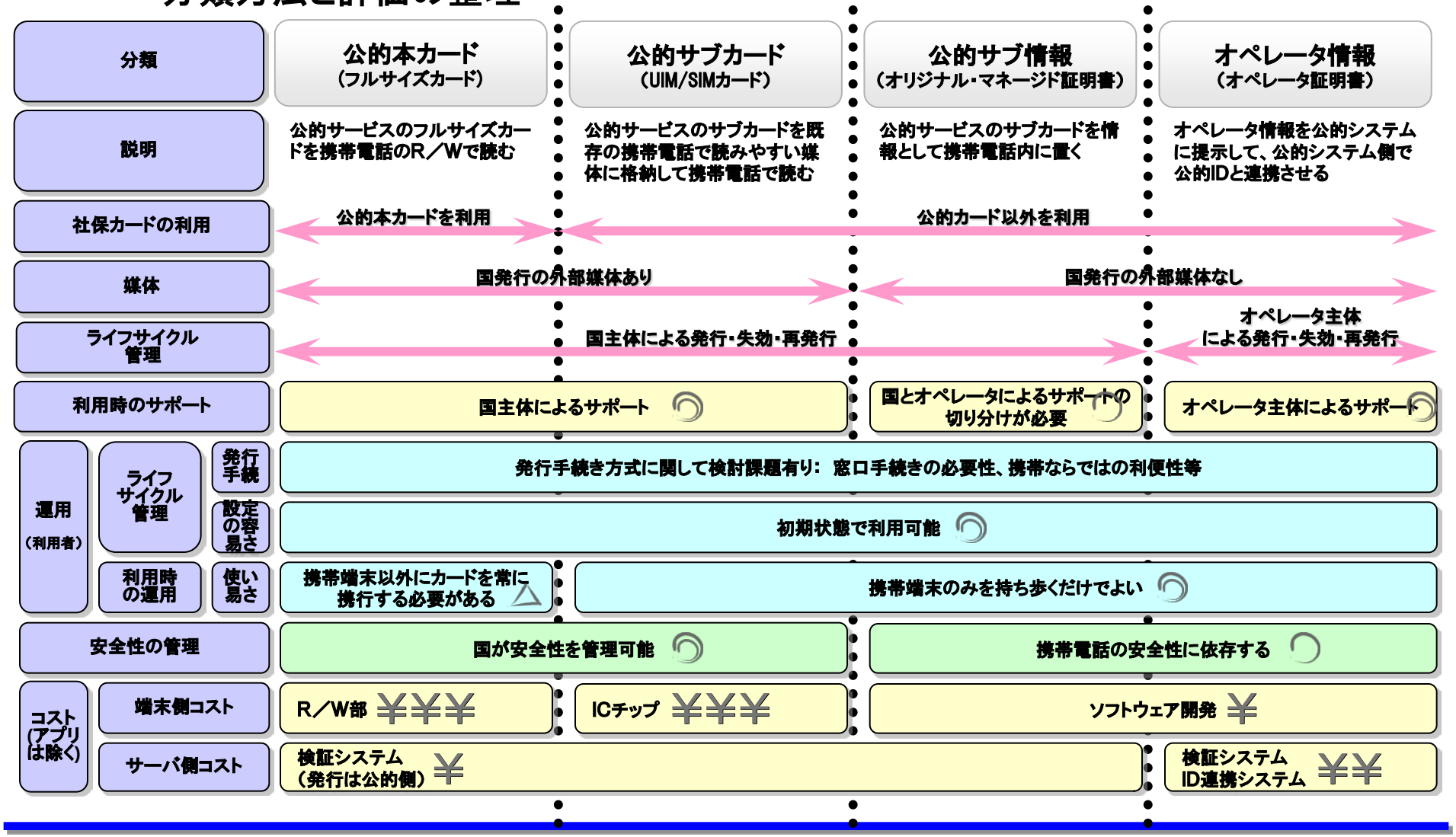
•発行・登録と利用のイメージ

分類	公的本カード（フルサイズカード）	公的サブカード（UIM/SIMカード）	公的サブ情報（オリジナル・マネージド証明書）	オペレータ情報（オペレータ証明書）
発行・登録イメージ	 ①窓口で申請  ②国発行のICカードを受取る	 ①窓口で申請  ②国発行のサブカードを受取る	 ①窓口で申請  ②持参した携帯・SD等に証明書を書込む	 ①窓口で申請  ②持参した携帯のIDを登録
利用イメージ	 ①ICカードを近づける  ②PINを入力	 ①サブカードを挿入  ②PINを入力	 ①PINを入力	 ①PIN入力または操作確認

4. モバイルPKIの今後

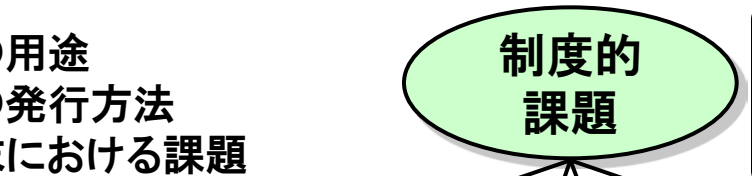
●携帯電話からの次世代電子行政・電子私書箱等へのアクセス手段の分類

•分類方法と評価の整理



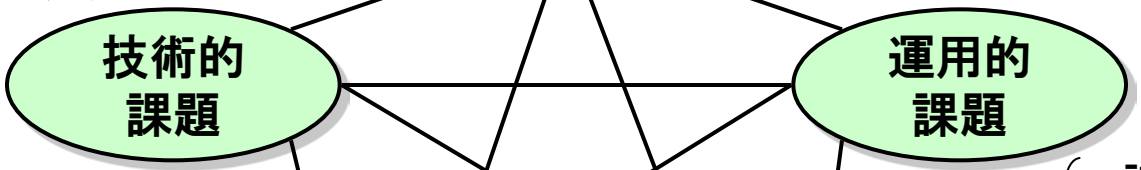
4. モバイルPKIの今後

- さまざまな観点で質、量ともに多くの課題が存在する
- 個々の課題に対しても多くの深堀検討が必要

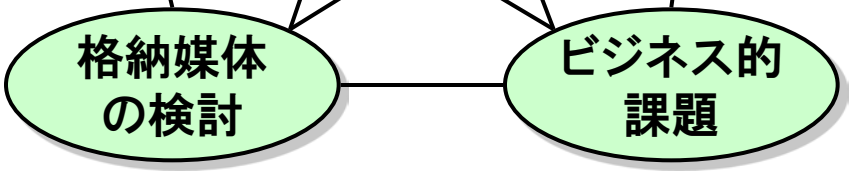


- 公的個人認証法
- 他の法制度
- その他

- 証明書の用途
- 証明書の発行方法
- 携帯端末における課題
- 証明書の利用方法
- その他



- 証明書発行・失効・更新時の運用
- 証明書利用時の運用
- 他認証基盤との連携
- 格納媒体に対する認定
- その他



- セキュリティレベル携帯内蔵型／着脱型
- セキュリティレベルの検討
- その他

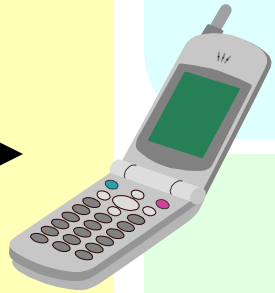
- ユーザの利便性向上
- R／W整備
- SP支援環境の整備
- 携帯キャリアとの連携
- JPKI運営組織との連携
- AP側組織との連携
- その他

4. モバイルPKIの今後

ローカル環境系

対面サービス

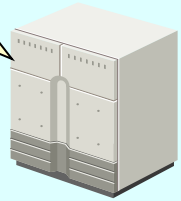
●ポータルから持ち出したデータをセキュアに携帯電話に格納し、リアルな環境で使う。
●非接触ICインタフェース等を用いて利便性を高める。



認証系

●携帯電話からポータルにアクセスする。
●キャリアが異なっても同様の認証方式が利用できるような共通基盤を構築する。
●認証後は個人データを携帯電話に持ち出して利用する

ポータル



オンライン行政

●携帯電話で申請データを作成する。
●申請データ作成後、署名を付与して電子申請を行う。
●リーダやICカードは不要とする。

申請系

4. モバイルPKIの今後