我が国における
電子署名認証基盤のあり方

2009年11月25日

東京工科大学
手塚　悟
tezuka@cs.teu.ac.jp

目次

目次

1. 電子署名認証基盤の現状

- 公的基盤
  - GPKI : Government Public Key Infrastructure
  - LGPKI : Local Government Public Key Infrastructure
  - 公的個人認証サービス(JPKI)
  - 法務省商業登記の電子署名基盤

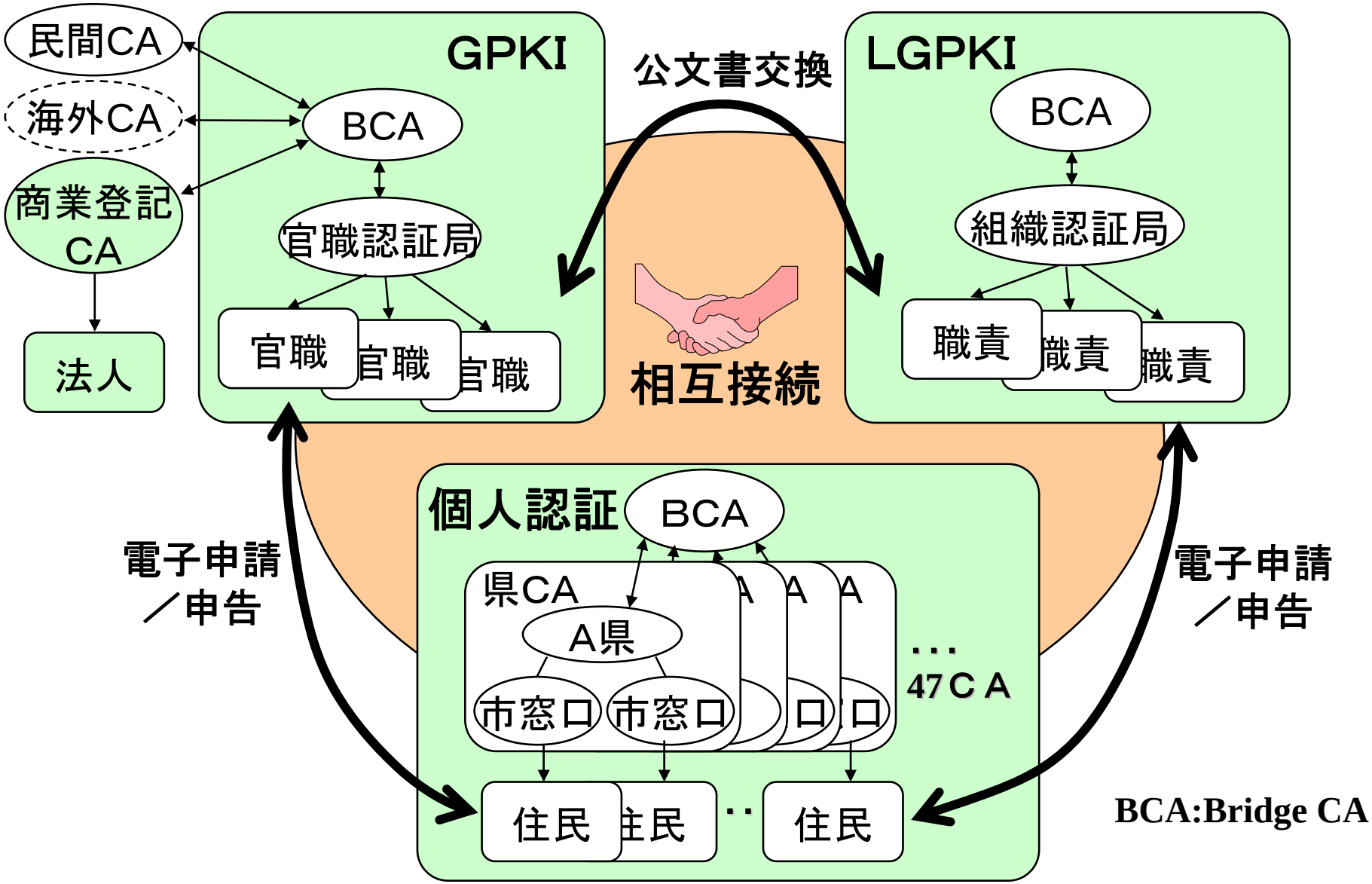
- 民間基盤
  - 電子署名法対応民間電子署名認証基盤　：　認定認証業務
  - その他の電子署名認証基盤
    - 携帯電話等

1. 電子署名認証基盤の現状

- 公的基盤の連携
  - BCA間で相互認証
    - GPKIのBCA(Bridge Certificate Authority)
    - LGPKIのBCA
    - JPKIのBCA
  - 法務省商業登記の電子認証局はGPKIのBCAで相互認証

- 公的基盤と民間基盤の連携
  - 認定認証業務の電子認証局はGPKIのBCAで相互認証
    - 認定認証業務の認定を受ける
    - GPKIの相互運用性仕様書に定める技術基準等を満たす

1. 電子署名認証基盤の現状



1. 電子署名認証基盤の現状

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

目次

2. 電子署名認証基盤の課題

- 公的基盤
  - 利用拡大
    - 公的個人認証サービス(JPKI) ： EE(End Entity)が住民
    - 法務省商業登記の電子署名基盤 ： EEが法人

- 民間基盤
  - 利用拡大
    - 電子署名法対応民間電子署名認証基盤 ： EEが自然人
    - その他の電子署名認証基盤 ： EEが自然人、機器等
      - 携帯電話等

2. 電子署名認証基盤の課題

- 公的基盤と民間基盤の連携
  - 公的個人認証サービス(JPKI)のサービスを拡大していくと、民間基盤のサービスとの重複可能性
    - 住み分けをどうするか
    - 責任分解点をどうするか

- 電子署名認証基盤の利便性向上
  - 現在最も個人に普及している携帯電話の活用
    - モバイルPKI

2. 電子署名認証基盤の課題

- 国際間の電子署名認証基盤の連携
  - 各国の公的基盤間の連携
  - 各国の民間基盤間の連携

- 電子署名と電子認証の違い
  - 明確に違いを理解する必要あり

2. 電子署名認証基盤の課題

- 電子署名法
  - 電子署名及び認証業務に関する法律
  - 民事訴訟法228条1項

    文章は、その成立が真正であることを証明しなければならない。

- 公的個人認証サービスに関する法律
  - 電子署名に係る地方公共団体の認証業務に関する法律

    （公的個人認証法）
  - インタネットを通じて安全・確実な行政手続き等を行うために、

    他人によるなりすまし申請や電子データが通信途中で改ざんされていないことを確認するための機能

2. 電子署名認証基盤の課題

●日本語の「認証」という言葉は、主に以下のような4つの意味で用いられる

– 本人確認（Identification）

検証者が被検証者の本人性を確認する（本人の識別をする）

– 身元証明（Authentication）

被検証者が検証者に対して自分の身元を証明する
（電子証明書を用いた本人確認に相当）

– 身元保証（Certification）

第三者（権威者）が被検証者の本人性を保証する
（電子証明書の発行に相当）

– 権限確認（Authorization）

被検証者が何らかの処理を行おうとした際に，検証者が被検証者の権限の有無を確認する

2. 電子署名認証基盤の課題

- 電子署名法
  - 電子署名及び認証業務に関する法律
  - ここで言う 「認証」は、「Certification」のこと

- 公的個人認証サービスに関連する法律
  - 電子署名に係る地方公共団体の認証業務に関する法律
    （公的個人認証法）
  - ここで言う 「認証」は、「Certification」のこと

- 電子署名：Electronic Signature

- 電子認証：Electronic Authentication

2. 電子署名認証基盤の課題

- 電子認証局： Certificate Authority
  - RA : Registration Authority 登録局
  - IA ： Issuing Authority 発行局
  - VA ： Validation Authority 検証局

- RA : 登録局
  - 本人確認
  - 本人確認の厳格さによって、電子署名認証基盤の信頼性が決まるといっても過言ではない

3. 電子署名認証基盤のあるべき姿

●本人確認を行っているサービスにて発生したトラブル事例を示す

記事掲載日	分類	見出し	トラブル概要	被害額
2008/4/16	通信／モバイル	架空の健康保険証を使用して携帯電話を不正入手	武南署は詐欺未遂などの疑いで会社役員を逮捕した。調べで、容疑者は同市内の携帯電話販売店で、無職少年に架空の健康保険証などを渡して不正契約させ、携帯電話をだまし取ろうとした疑い。同署は不正契約した携帯電話が犯罪に使われたとみて、調べている。	不明 ※不正入手された携帯電話は犯罪での使用の可能性有
2008/1/5		「携帯1000台だまし取った」偽造住基カード使用　男2人逮捕	福井、愛知両県警の合同捜査本部は、偽造した住民基本台帳カードを使って携帯電話を販売店からだまし取ったとして容疑者を逮捕した。容疑者は住基カードを約200枚偽造し、携帯電話約1000台をだまし取った疑い、被害総額は5000万円以上とみて余罪を追及している。容疑者は携帯電話販売店で身分証明書として、虚偽の住所を記載した偽造住基カードを店員に示し、携帯電話2台をだまし取った疑い。	5000万円以上
2007/2/21		NTT東西、なりすましによる虚偽 申し込み被害が「ボイスワープ」 で相次ぐ	NTT東西両社によると、2007年1～2月以降、「116」に対して、第三者による「ボイスワープ」への申し込みが複数件発覚したという。 確認されている被害は、NTT東日本が25件、同西日本が3件。うち3件は、「ボイスワープ」の開通後、虚偽申し込みの被害者がNTTを名乗った“なりすまし者”の電話を受け、故障修理の名目で、“なりすまし者”が指定したボイスワープの転送先電話番号に登録させられていたという。	不明
2007/11/9	小売／サービス	モバイルSuica不正利用相次ぐ被害1000万円超	JR東日本の「モバイルSuica」で、昨年12月ごろから、不正に入手したカード情報で他人になりすまし、電子マネーが使用される被害が発生。被害額は確認できているものだけで約1000万円に上る。	約1000万円
2007/2/18	金融機関／保険	ペーパー会社で健康保険証詐取 兵庫県警、詐欺容疑立件へ	公判中の男2人が、ペーパーカンパニーを設立し、架空の従業員名義で社会保険事務所から健康保険証をだまし取っていた疑いが強まった。2人は架空の従業員11人分の健康保険証を同事務所に交付させた疑いが持たれている。実際に病院で受診もしていたという。2人はこの保険証で消費者金融の無人契約機で詐取したキャッシングカードで、現金自動預け払い機（ATM）から50万円を引き出した。	50万円以上

サービス提供者による本人確認にも関わらず、トラブルの発生が後を絶たない

2. 電子署名認証基盤の課題

●本人確認方法の事例

	分類	提供時の本人確認方法	利用時の本人確認（目視を除く）
パスポート	行政	戸籍謄本または抄本、住民票の写し、運転免許証（住基カード等の国が発行した資格証1種類、年金手帳、健康保険証、印鑑登録証等のうち2種類）	パスポート所持
運転免許証		住民票の写しに加え、パスポート等（住基カード、健康保険証等）	運転免許証所持
taspo		運転免許証、各種健康保険証、住基カード（写真付）、年金手帳、福祉手帳、外国人登録証明書、住民票の写し。	Taspo所持
口座開設	銀行／保険	運転免許証、住民票の写し、各種年金手帳、各種健康保険証、印鑑証明書、外国人登録証明書	通帳所持
銀行キャッシュカード		運転免許証、パスポート、住基カード、年金手帳、健康保険証等。 または、本人の住所宛に送った書類に加え、住民票の写し等（印鑑登録証、戸籍謄本、抄本等）	カード所持及び暗証番号
クレジットカード		運転免許証、パスポート、住民票の写し、住基カード、健康保険証等	カード所持及び、 サインまたは暗証番号
TSUTAYA レンタル機能有会員証	小売／サービス	運転免許証、障害者手帳、福祉・生活に関する証明書、外国人登録証明書、住民基本台帳等。もしくは、顔写真を含まない本人確認書類＋住民確認書類	カード所持
電子マネー		特になし	カード所持
ビックカメラ ビックポイントカード		特になし （但し、カード再発行時には、運転免許証等の本人確認が必要）	カード所持
携帯電話	通信／モバイル	運転免許証、パスポート、住基カード。または、健康所検証に加え、住民票の写し等（公共料金領収書等）。または、クレジットカードに加え、住民票の写し等（健康保険証等）	ー

サービス提供時に必要となる本人認証書類はサービス毎にさまざま

2. 電子署名認証基盤の課題

● 本人確認方法の違い

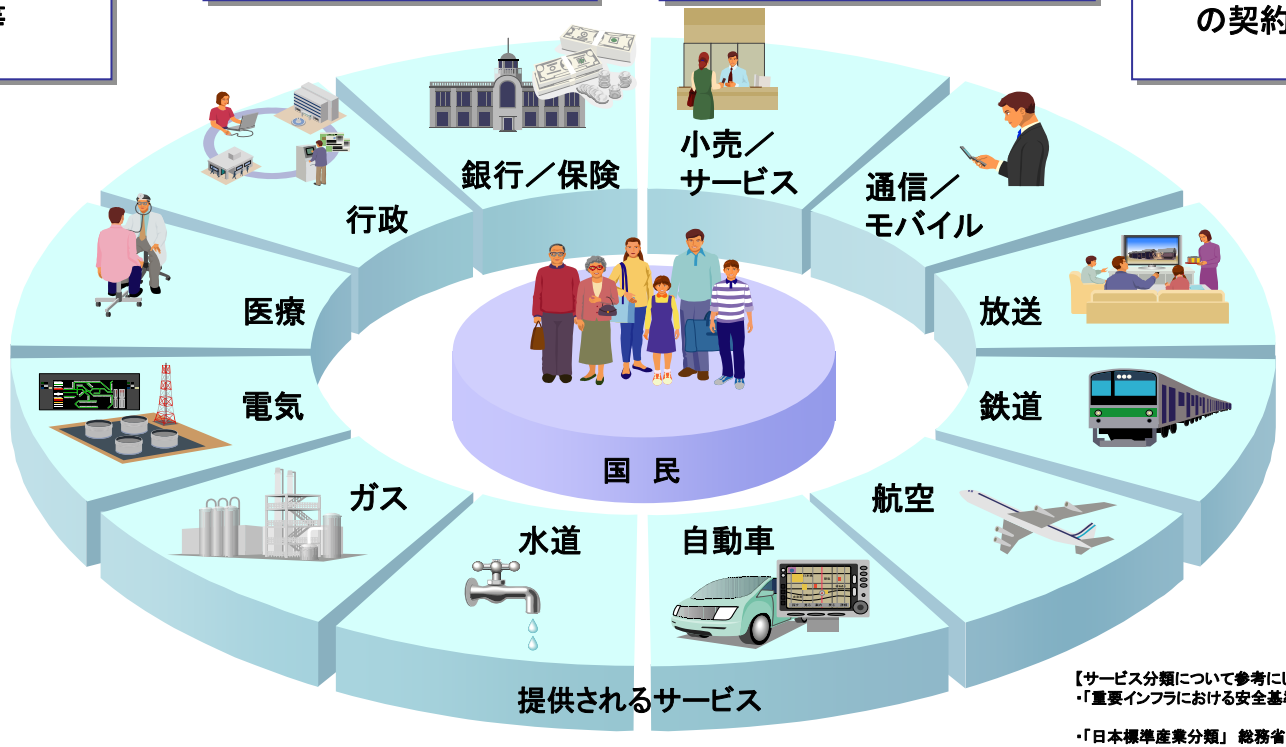
●サービス利用者はサービス提供を受ける際に、本人確認を求められることが多い

【本人確認事例】
・パスポート申請時
・運転免許証申請時
・taspo申請時　等

【本人確認事例】
・口座開設申込時
・キャッシュカード申込時
・クレジットカード申込時

【本人確認事例】
・会員カード申込・利用時
・電子マネー申込・利用時
・ポイントカード申込・利用時
等

【本人確認事例】
・携帯電話契約時
・インターネットサービスの契約・利用時　等



【サービス分類について参考にした資料】
・「重要インフラにおける安全基準等の策定・見直しについて」
内閣官房情報セキュリティセンター
・「日本標準産業分類」 総務省統計局

2. 電子署名認証基盤の課題

- 本人確認の体系化
  - ID管理
    - ✓国家レベル
    - ✓企業レベル

- 国家レベル
  - 国民ID

- 企業レベル
  - 企業ID

- 本人確認の体系化は、すなわちIDの体系化である

目次

3. 電子署名認証基盤のあるべき姿

- 公的電子署名認証基盤と民間電子署名認証基盤を総合的に活用
  - 官民連携

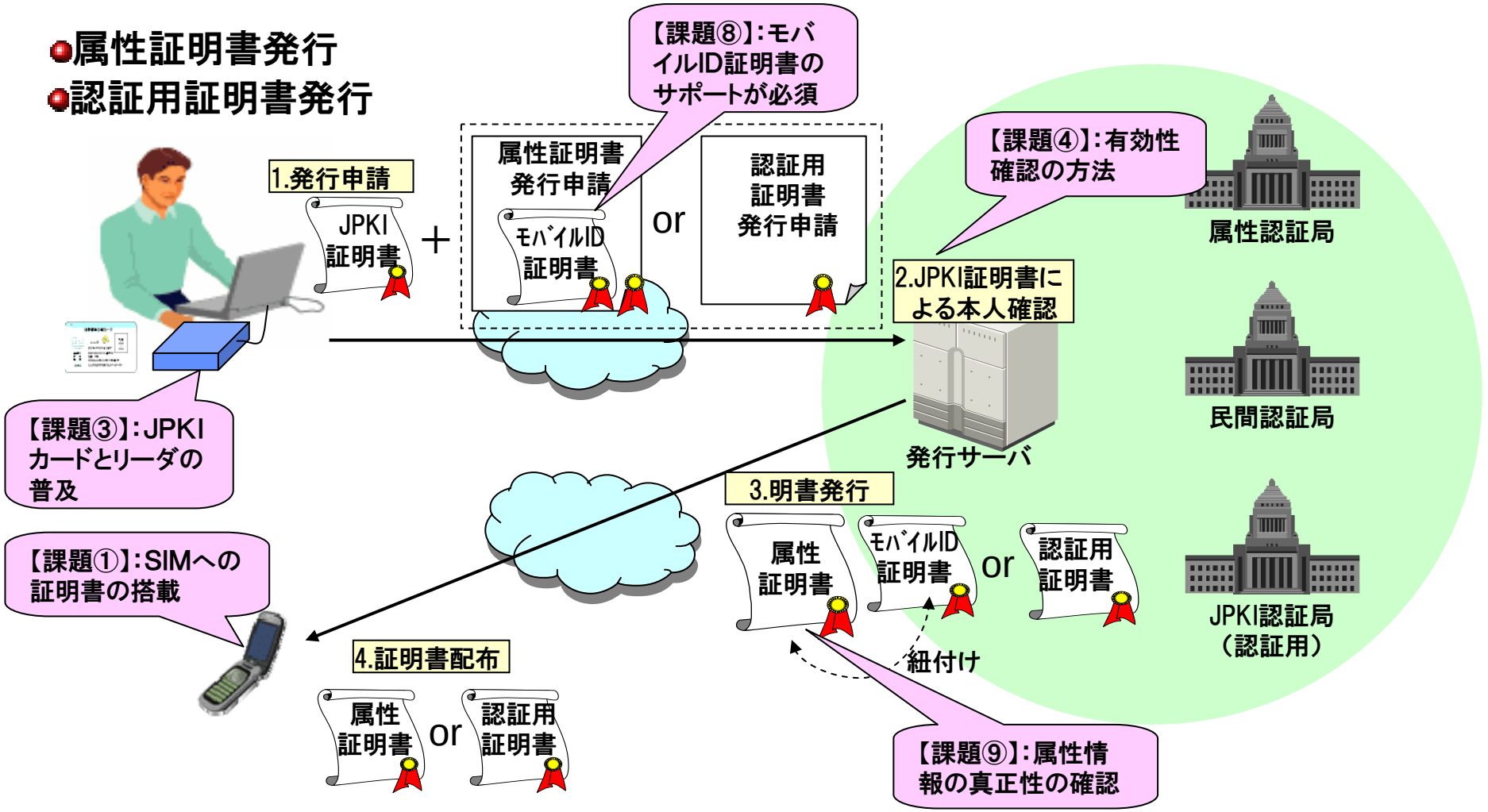
- 本人確認を公的電子署名認証基盤が担う
  - 民間の様々なサービスのオンライン登録に活用

- 我が国の電子署名認証基盤を検討する第3者機関を組織
  - GPKI
  - LGPKI
  - 公的個人認証サービス(JPKI)
  - 法務省商業登記の電子署名基盤
  - 電子署名法
  - その他の民間電子署名認証基盤　例：モバイルPKI

3. 電子署名認証基盤のあるべき姿

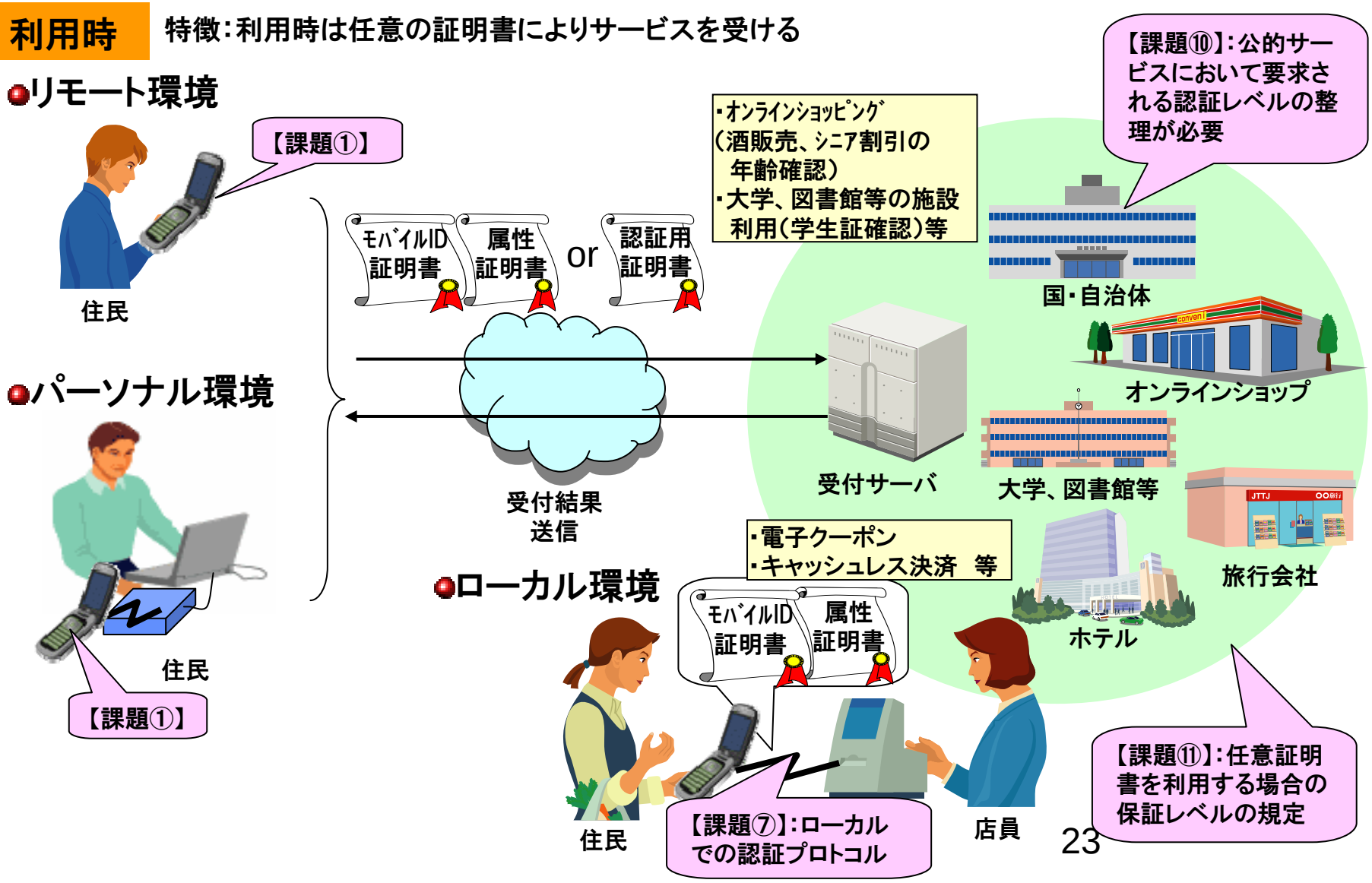
発行時　特徴：JPKI証明書により厳密な本人確認が行える

- 属性証明書発行
- 認証用証明書発行



3. 電子署名認証基盤のあるべき姿

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

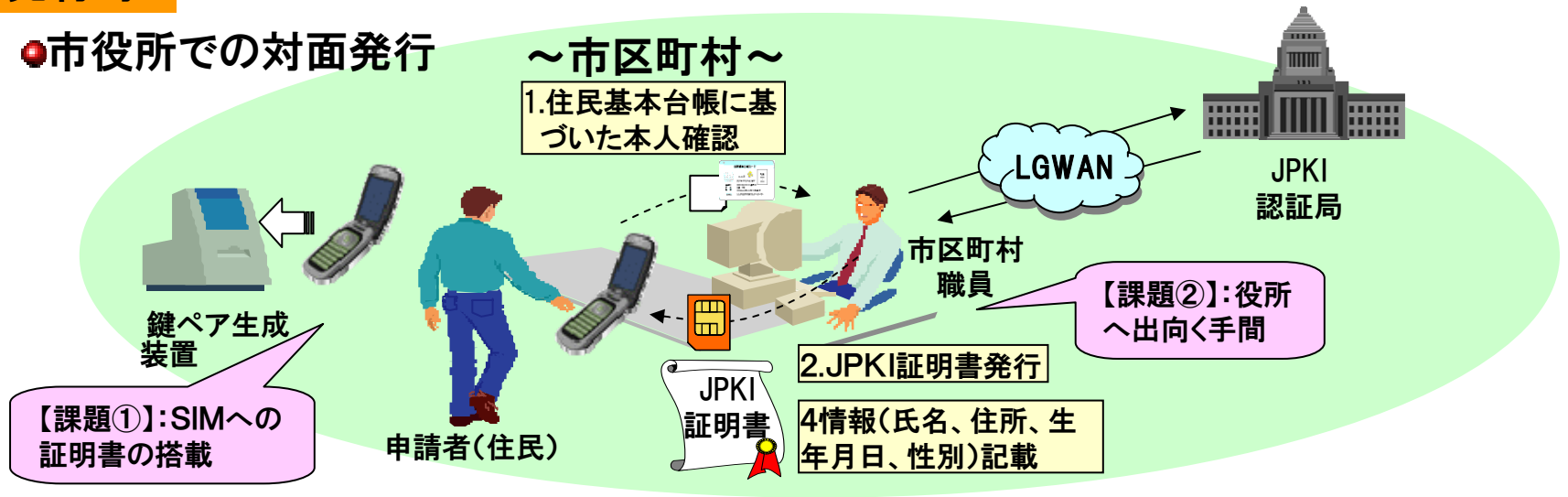


3. 電子署名認証基盤のあるべき姿

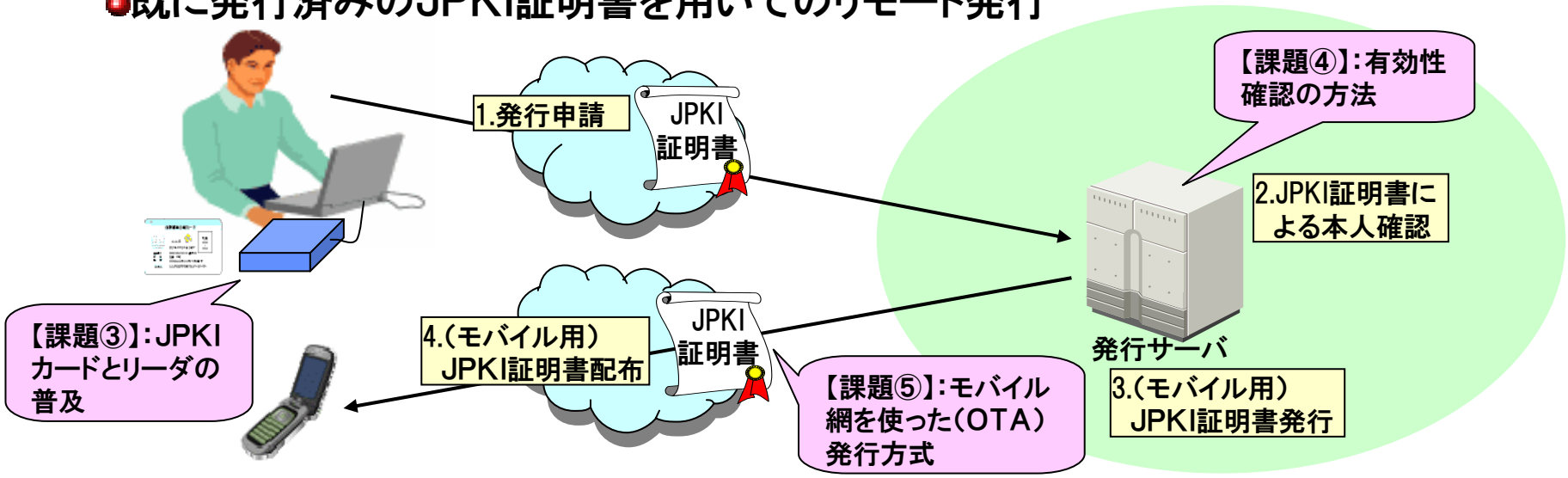
発行時　特徴：既存のJPKI証明書の発行と同レベルの本人確認が必要

●市役所での対面発行

～市区町村～

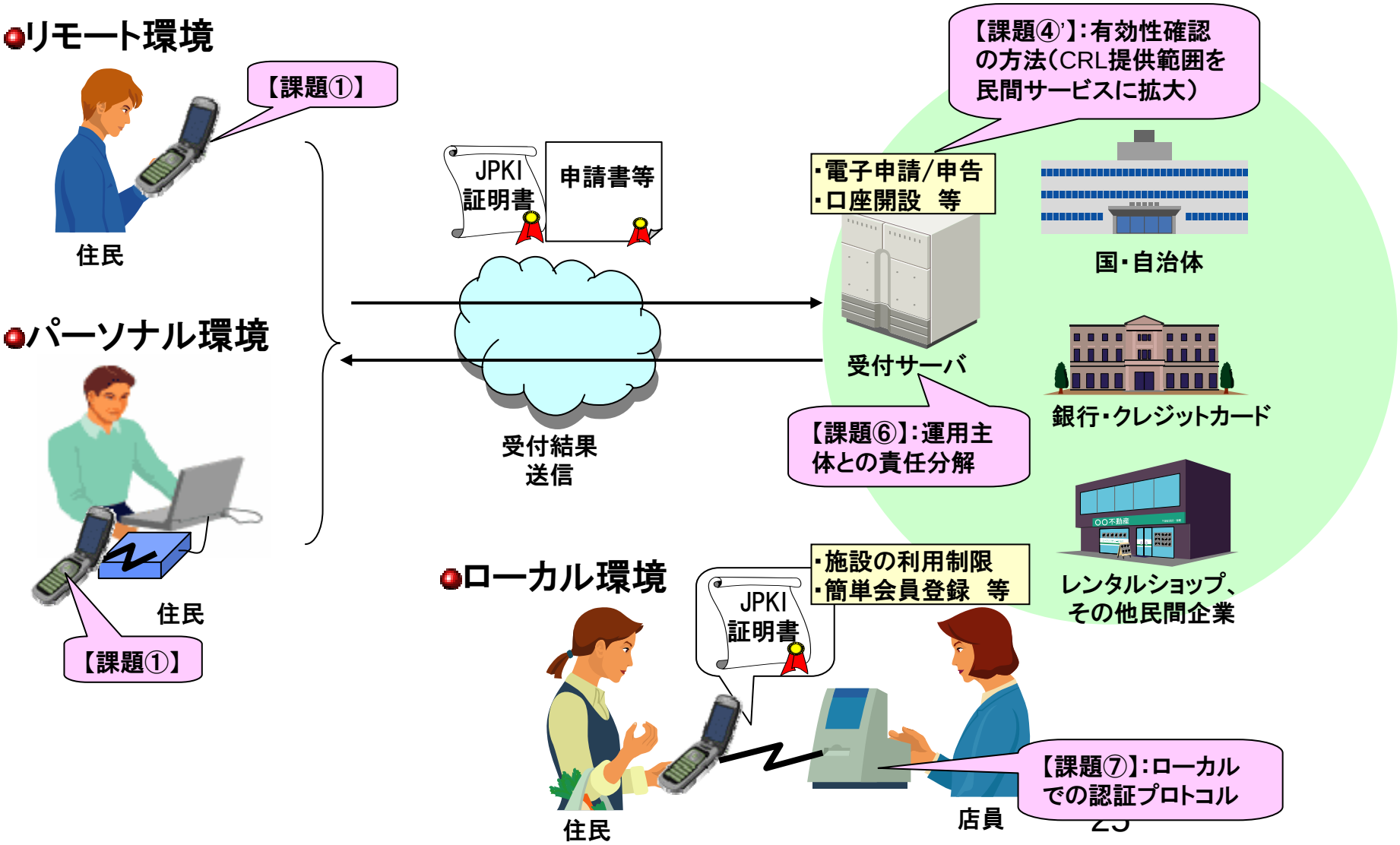


●既に発行済みのJPKI証明書を用いてのリモート発行



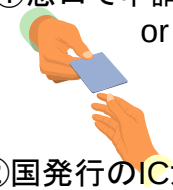
3. 電子署名認証基盤のあるべき姿

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



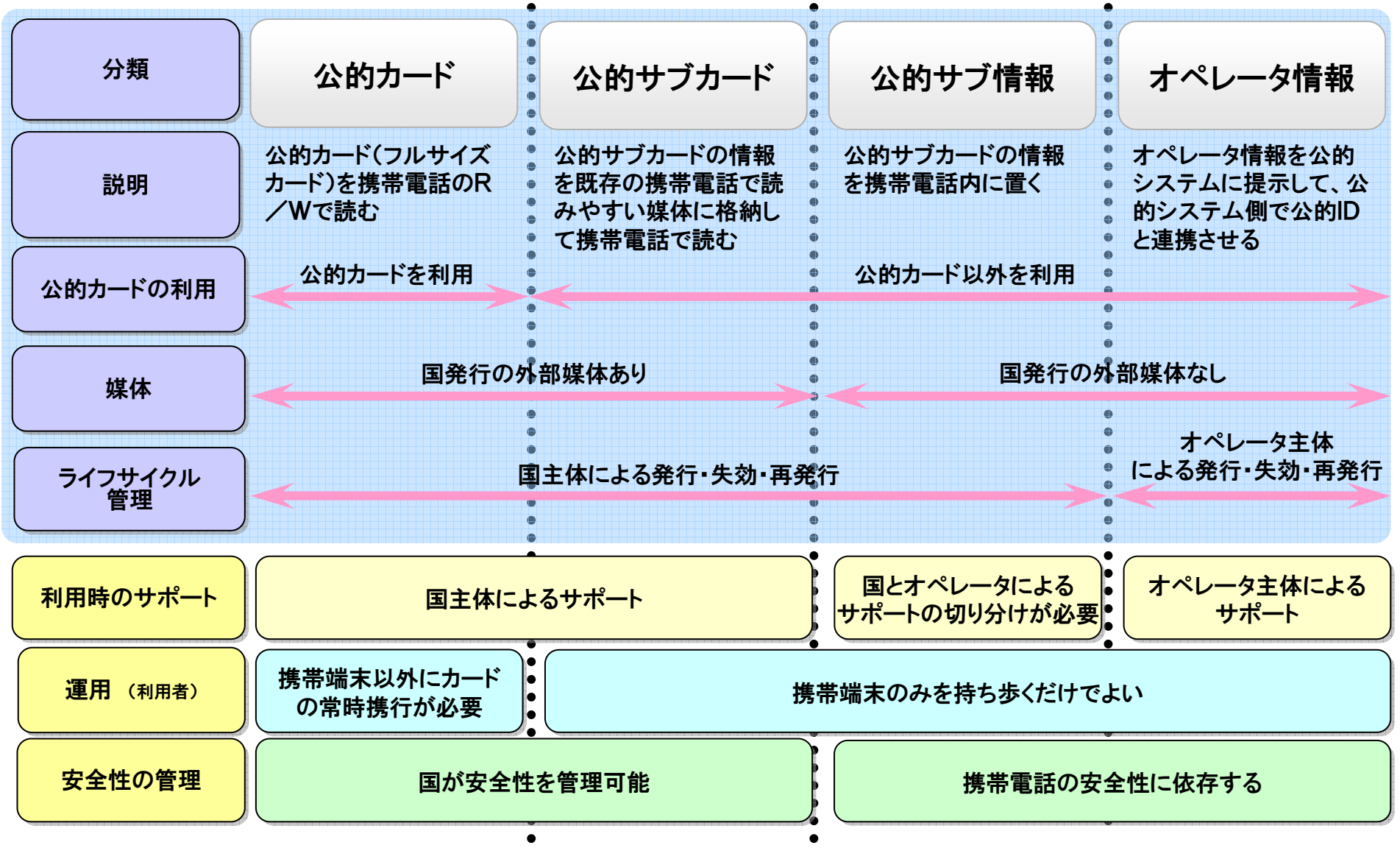
3. 電子署名認証基盤のあるべき姿

■ 発行・登録／利用イメージによる分類

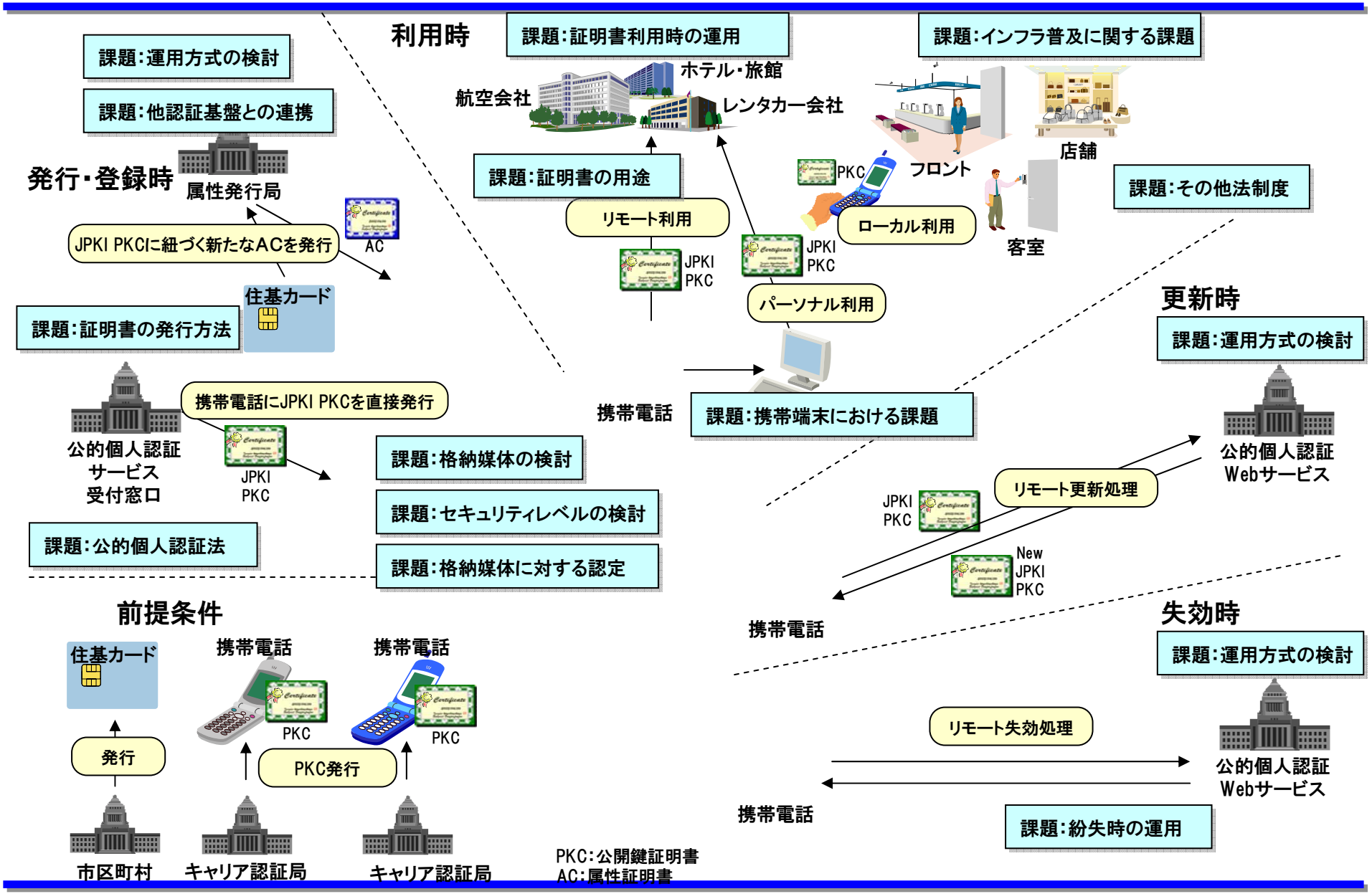
分類	公的カード	公的サブカード	公的サブ情報	オペレータ情報
発行・登録イメージ	 ①窓口で申請 or 郵送  ②国発行のICカードを受取る	 ①窓口で申請 or 郵送  ②国発行のサブカードを受取る	 ①窓口で申請 or オンライン  ②持参した携帯・SD等に証明書を書込む	 ①窓口で申請 or オンライン  ②持参した携帯のIDを登録
利用イメージ	 ①ICカードを近づける  ②PINを入力	 ①サブカードを挿入  ②PINを入力	 ①PINを入力	 ①PIN入力または操作確認

3. 電子署名認証基盤のあるべき姿

■ 発行・登録／利用イメージによる分類と評価（机上）

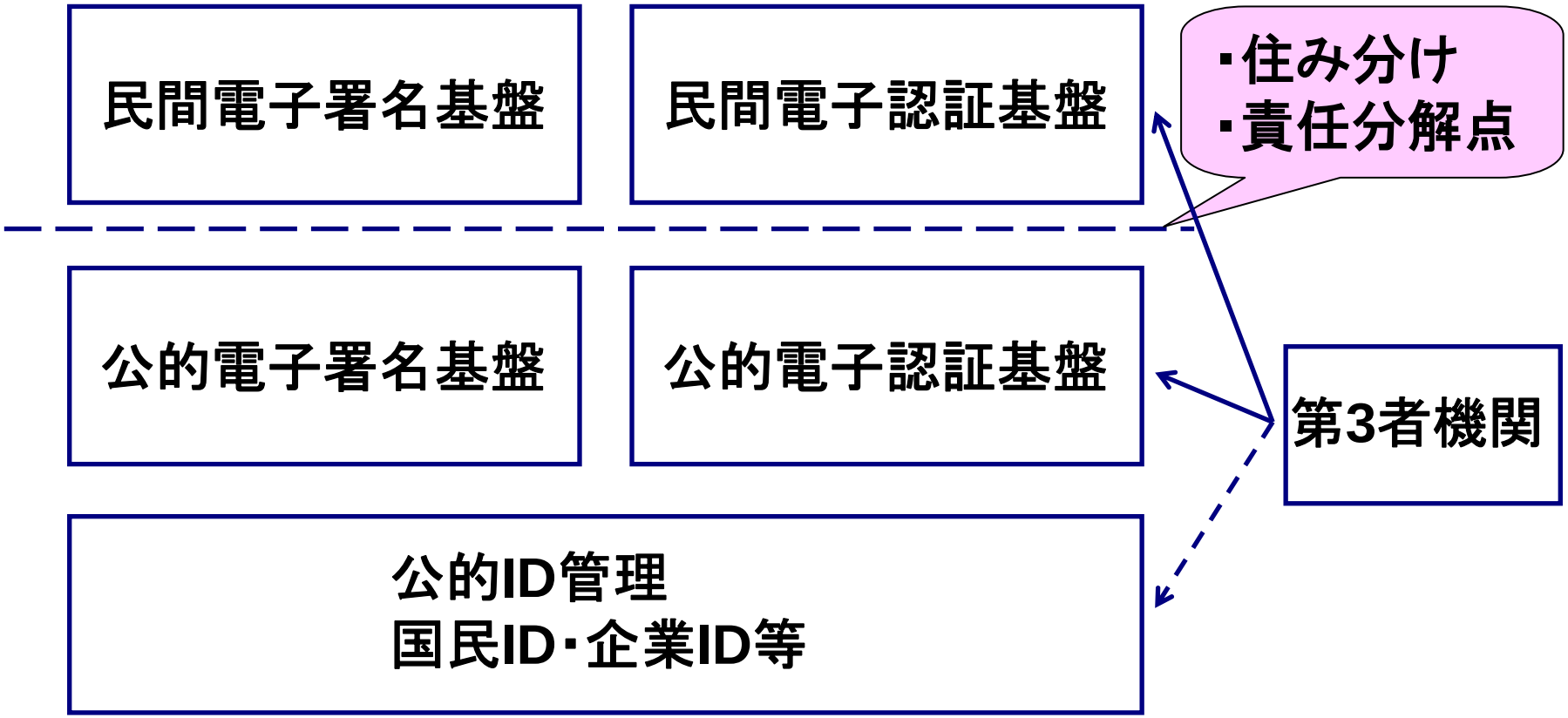


3. 電子署名認証基盤のあるべき姿



3. 電子署名認証基盤のあるべき姿

●我が国における官民連携による電子署名認証基盤のあるべき姿



ただし、上記以外の電子署名認証基盤を規制するものではない