



公的個人認証サービスの 利便性向上に向けた取組

平成21年2月6日

総務省地域情報政策室

公的個人認証制度の概要

<根拠法>

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)

- 平成16年1月 施行 ※関係省庁と協議の上施行時期を決定
- 平成18年11月 一部改正(士業団体等を署名検証者に追加)

<実施体制>

■ 運営主体

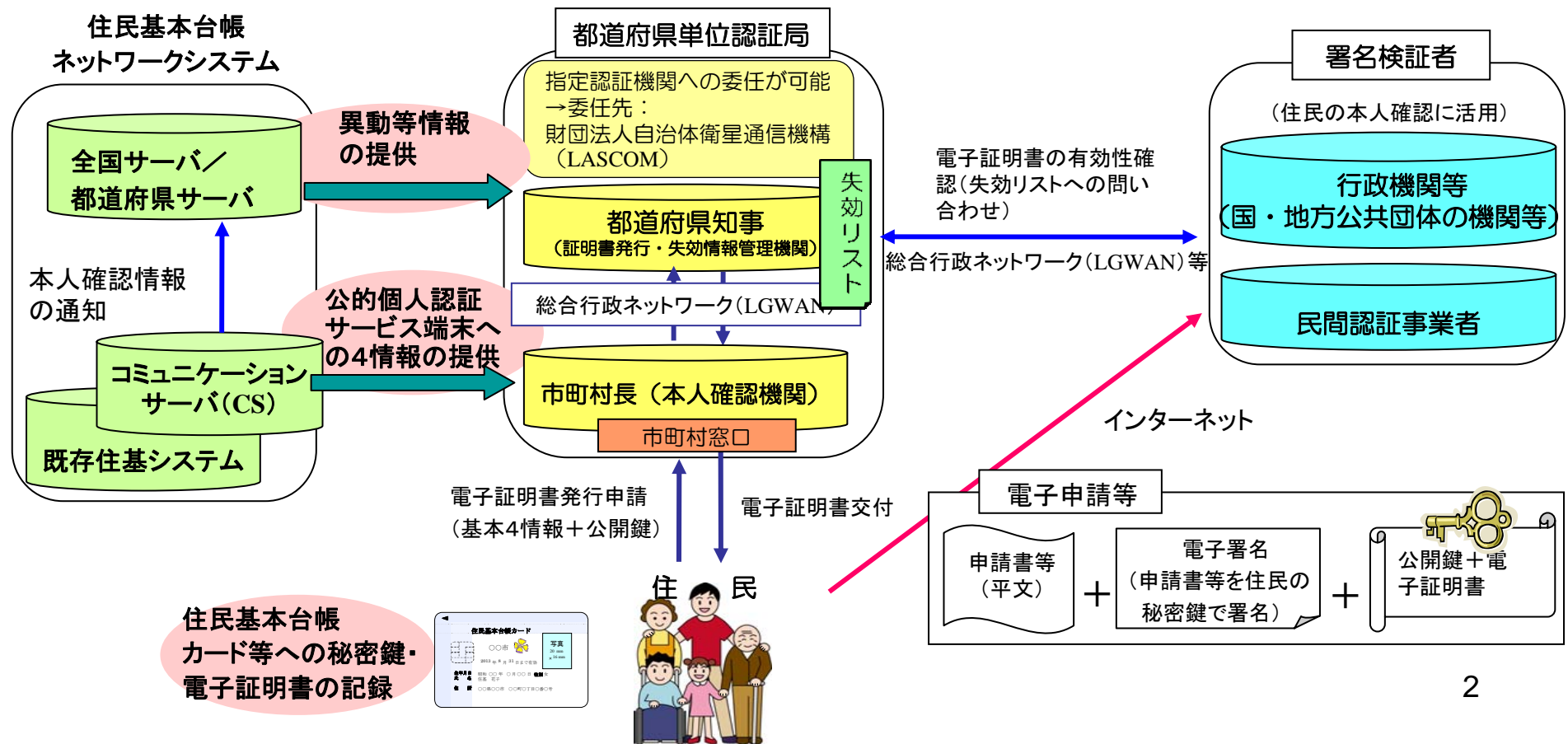
- 都道府県・・・電子証明書の発行事務・失効情報等提供事務
- 市町村・・・電子証明書を発行する際の本人確認事務
- (財)自治体衛星通信機構・・・都道府県知事が業務を委任

■ サービス利用主体

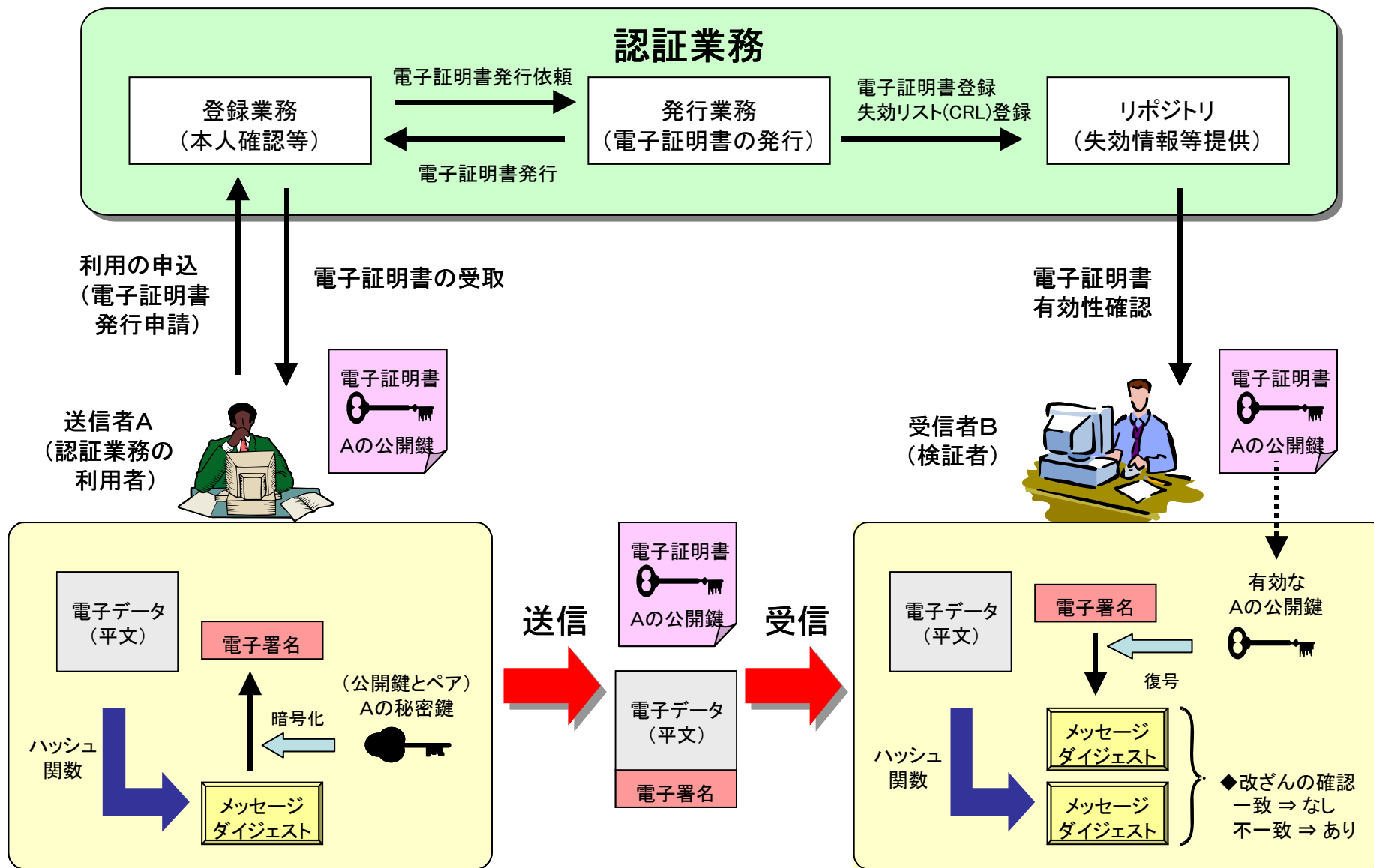
- 署名検証者(行政機関等。民間分野については特定認証業務を行う者であることが要件) <参考1>参照
- 住民

公的個人認証サービス

- オンラインでの行政手続等における本人確認のためのしくみ。
- 成りすまし、改ざん、送信否認などを防ぐため、高いセキュリティを確保。
- 電子証明書の発行件数：約85万件（2009年1月）



電子署名・認証業務の詳細



ハッシュ関数: 任意のデータ量の情報を一定のデータ量の情報に圧縮変換する一方向性の関数
 メッセージダイジェスト: 電子データをハッシュ関数で変換して得た値

発行手続の流れ

1. 市区町村役所(役場)へ行く



2. 受付手続 (申請書提出)

公的個人認証サービス
電子証明書発行申請書
平成 年 月 日

申請者氏名	総務 太郎
ふりがな	そうむ たろう
生年月日	昭和37年 6月17日
男女の別	男
住所	霞が関2丁目1番地2号

※1 氏名、住所の記載表記は、住民票に記載されている漢字を用いてください。
※2 パソコン等で、住民票に記載されている漢字が表記できない場合、申請者が日常パソコン等で使用している代替文字を記載してください。

代替文字	有 ・ 無
指定代替文字	

3. 本人確認



4. 本人確認後、 自分で鍵生成

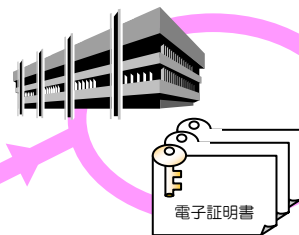


5. 公開鍵提出



6. 証明書発行手続

都道府県知事が発行



7. 証明書の交付

CD-ROM(利用者クライアントソフト)
利用のご案内ほかを併せて配付



公的個人認証を利用したオンライン手続の準備<PCの設定等>

1. パソコンの環境確認


OS

- ・Microsoft Windows Vista / XP / 2000
- ・Mac OS X v10.4

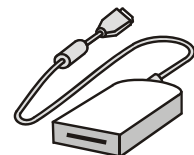
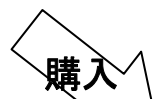
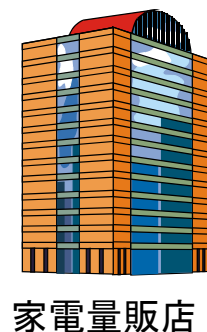
JRE
※推奨

- ・JRE 6.0 Update 7
- ・JRE 5.0 Update 15
- ・JRE 1.4.2_17

お使いのパソコン

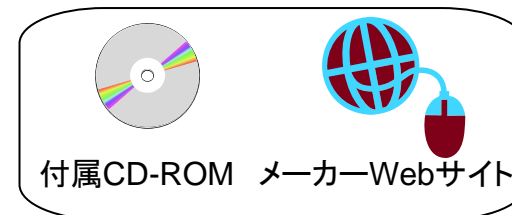


2. ICカードR/Wの取得

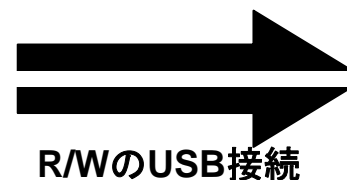


ICカードR/W

3. ICカードR/Wの設定



ドライバのインストール



4. JREをインストール

申請先受付システムに対応したJREをインストール



※JREとは、Javaプログラムを実行するソフトウェアのこと

Sun microsystems Webサイト



インストール



5. 利用者クライアントソフトのダウンロード/インストール



公的個人認証サービスポータルサイト



インストール



6. 電子申請先の受付システムにアクセス



e-Tax



eLTAX

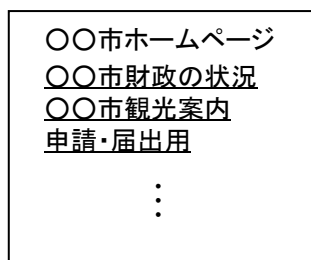
5



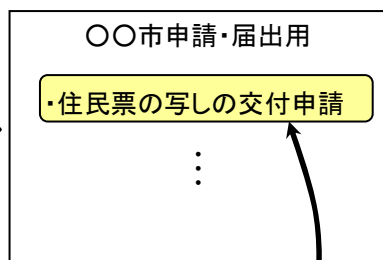
アクセス

公的個人認証を利用したオンライン手続の流れ

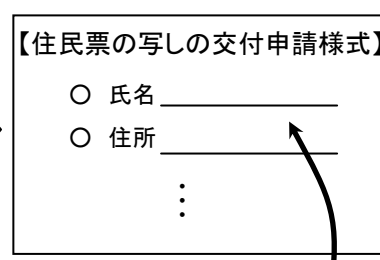
1, 自宅等のパソコンで行政機関等のホームページを開く



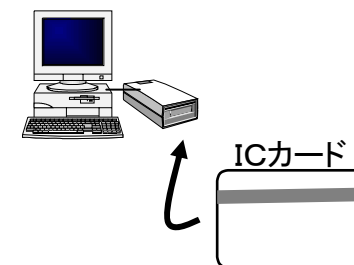
2, 利用しようとする申請・届出等のページを選択し、該当箇所をクリック



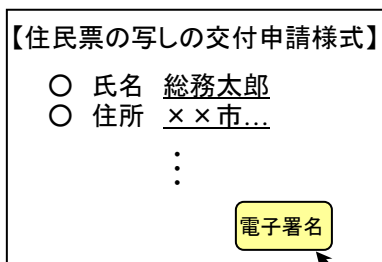
3, 様式に記入



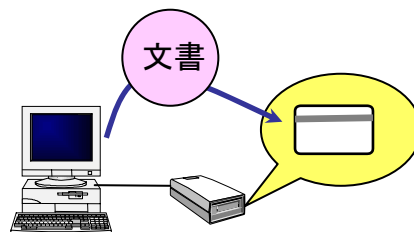
4, 利用者の秘密鍵が格納されたICカードをパソコンに接続されたリーダーライターにセットし、秘密鍵を使用するためのパスワードを入力する



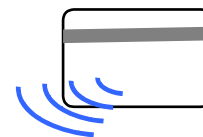
5, 電子署名の該当箇所をクリック



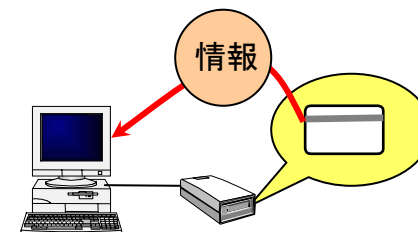
【電子署名の方法】



①電子署名を施すべき文書(デジタル情報)がICカード内に取り込まれる



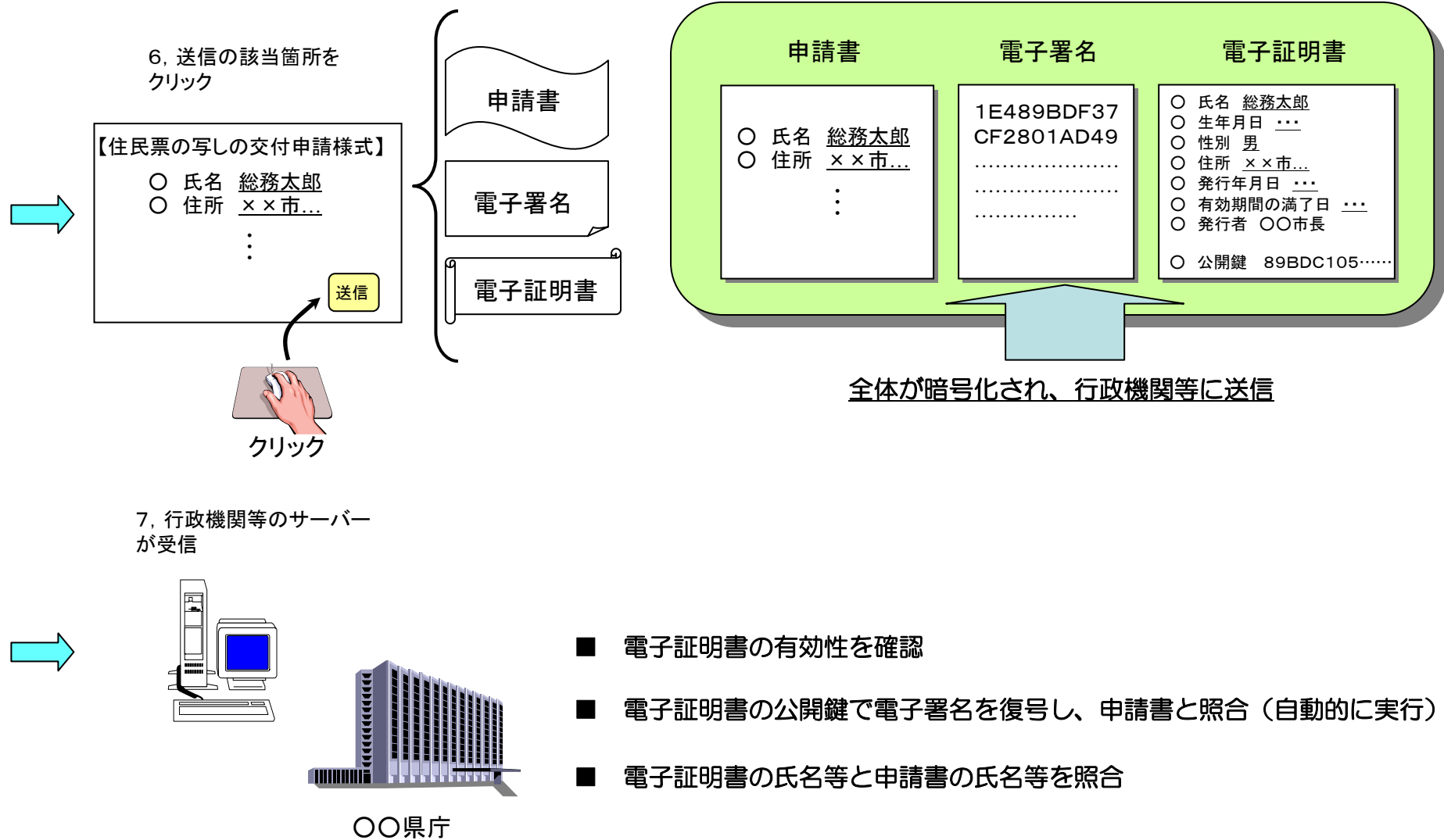
②ICカード内で電子署名の処理(暗号化)が行われる



③電子署名が付された情報がパソコン内に取り込まれる

電子署名はICカード内で行われ、パソコン内に秘密鍵のデータが移ることはない。

公的個人認証を利用したオンライン手続の流れ



公的個人認証の主な対象手続(2008年4月1日現在)

国(15府省庁等)

- ・自動車検査登録(自動車保有関係手続ワンストップサービス)
- ・国税関係手続
- ・社会保険関係手続
- ・国民年金及び厚生年金の年金加入状況・年金見込額の提供
- ・商業・法人登記申請
- ・不動産登記申請

等

都道府県(47団体)

- ・自動車税・自動車取得税申告(自動車保有関係手続ワンストップサービス)
- ・都道府県税の電子申告
- ・道路占用許可申請

等

市町村(35都道府県内の市町村)

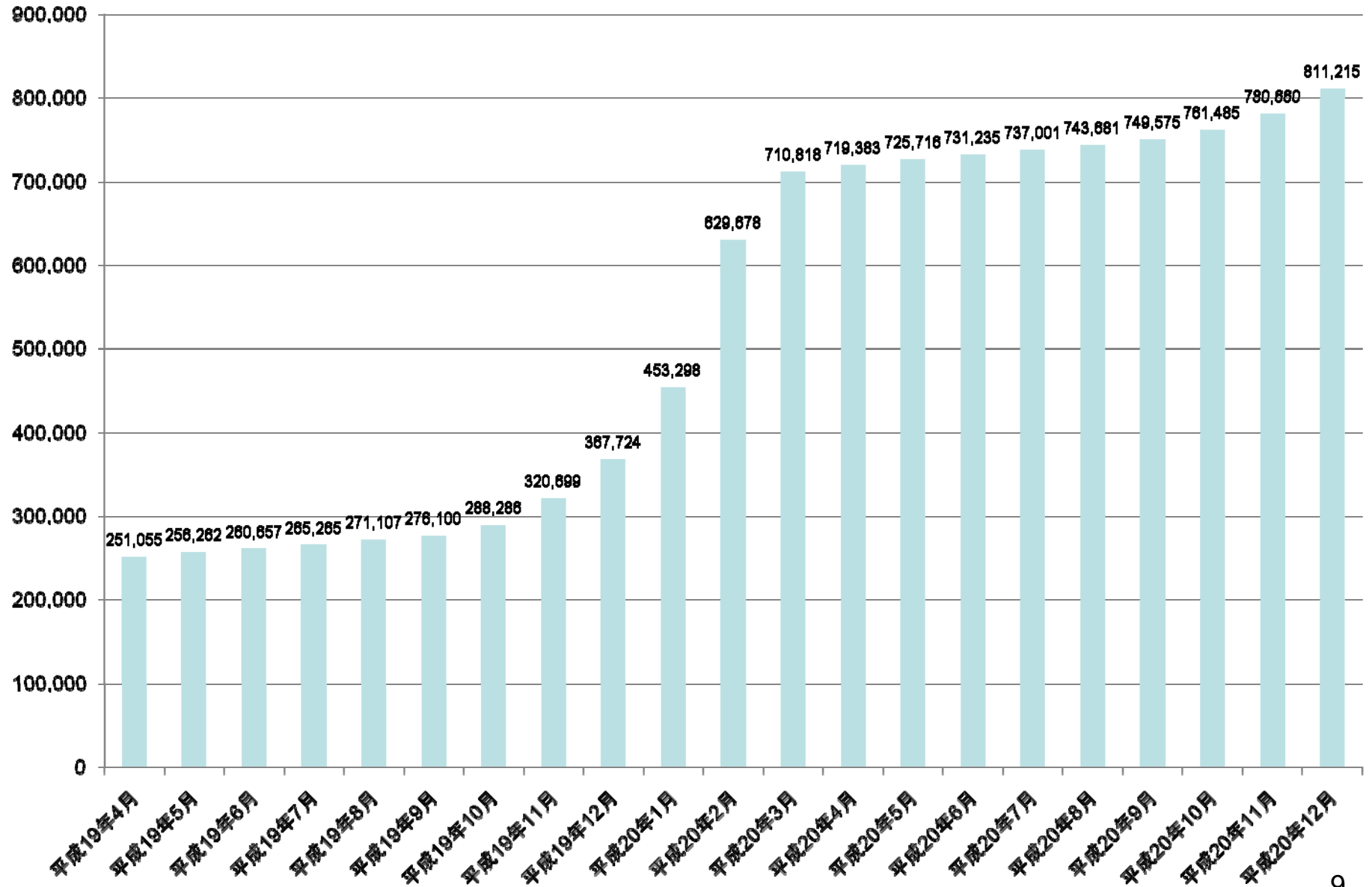
- ・市町村税の電子申告
- ・介護保険関係手続
- ・児童手当関係手続
- ・国民健康保険関係手続

等

(注1) 都道府県数及び市町村数は、共同運用システムに参加している自治体を含む。

(注2) 都道府県及び市町村の対象手続は、自治体毎に異なる。

電子証明書の発行件数(累計)



公的個人認証サービスの利便性向上に向けた取組(1)

技術・セキュリティ面や費用負担面等を十分に踏まえながら、徹底した利用者の利便性向上策に取り組む

○ 改善事項

【操作性の改善】

- ・ 非JAVA化(11月)
- ・ ICカードリーダーライタの自動設定化(11月)

総クリック回数
41回(昨年)→8回(今年)

※若干の調整可能性有り

【利用者サポートの充実】

- ・ 所得税の確定申告期に向けた公的個人認証ヘルプデスクの設置(12月)
- ・ ICカードリーダーライタの取得の容易化(市町村売店での販売を働きかけ)
- ・ 公的個人認証ポータルサイト・FAQの改善(11月中)
- ・ 公的個人認証からe-Taxに至る一連の操作に対応した利用者マニュアルの作成(1月中)

公的個人認証サービスの利便性向上に向けた取組(2)

【周知・広報の充実】

- ・ 各種団体(経済団体、士業団体、利用者団体等)等への周知・推奨、働きかけ
- ・ 利用者マニュアルの作成・PDF配布(1月)
- ・ 政府広報(インターネットでのフラッシュ動画)(2月～)
- ・ 各方面へのリーフレットの配布(1月～ 数十万部)
- ・ 地方におけるシニア向けパソコン教室の開催(2月～3月、3000人目途)
- ・ 公的個人認証サービスリーフレットの市町村への配布(1月～ 約70万部)
- ・ 国税庁ダイレクトメールに公的個人認証リーフレットを同封し配布
- ・ リーフレットの窓口(市町村・税務署・家電量販店等)配布
- ・ 自治体広報誌での周知・広報
- ・ ICカードリーダーライタ普及促進協議会と協力し、全国のICカードリーダーライタ取扱店に関する都道府県別の資料を作成・配布

○ 制度的検討事項

- ・ 電子証明書の有効期限の延長(例:3年→5年)
- ・ 電子証明書のオンラインでの更新
- ・ 格納媒体の多様化
- ・ 公的個人認証サービスの用途の拡大

例: 認証用途の付加

〈メリット〉 簡易な手続についても同一手段により利用
〈課題〉 セキュリティ水準、具体的ニーズ

署名検証者の範囲(公的個人認証法第17条)

- ① 行政機関等〔国、地方公共団体、独立行政法人、認可法人等〕
- ② 裁判所
- ③ 行政機関等に対する申請、届出その他の手続に随伴して必要となる事項につき、電磁的方式により提供を受け、行政機関等に対し自らこれを提供し、又はその照会に応じて回答する業務を行う者として行政庁が法律の規定に基づき指定し、登録し、認定し、又は承認した者
〔自動車ワンストップサービスの登録情報処理機関〕
- ④ 電子署名及び認証業務に関する法律第8条に規定する認定認証事業者
- ⑤ 電子署名及び認証業務に関する法律第2条第3項に規定する特定認証業務を行う者であって政令で定める基準に適合するものとして総務大臣が認定する者
- ⑥ 行政機関等及び裁判所に対する申請、届出その他の手続に必要な電磁的記録を提供する団体で政令で定めるもの〔学校法人等〕
- ⑦ 法律の規定に基づき他人の依頼を受けて行政機関等及び裁判所に対する申請、届出その他の手続を行う者が所属する団体で政令で定めるもの〔士業団体〕
- ⑧ 行政機関等及び裁判所に対する申請、届出その他の手続に必要な電磁的記録を提供する者が所属する団体又は機関で政令で定めるもの〔法務省(公証人に失効情報等を提供)〕

団体署名検証者

公開鍵認証基盤(PKI)の仕組み

PKI (Public Key Infrastructure : 公開鍵認証基盤)
 = 公開鍵暗号方式に基づく電子認証の技術基盤
 秘密鍵による暗号化 (電子署名)、公開鍵による復号化、第三者機関 (認証局 (CA))
 が発行する公開鍵の電子証明書を組み合わせることで本人性の確認や文書の改ざんの有無の検知を行う。

公開鍵暗号方式

公開鍵暗号方式とは、公開鍵・秘密鍵を用いた暗号技術。
 公開鍵・秘密鍵とは、暗号化・復号化のアルゴリズム(処理手順)のこと。
 二つの鍵はペアとなっており、片方の鍵で暗号化されたものは、もう一方の鍵でしか復号化できない。
 片方の鍵からもう一方の鍵を割り出すことは事実上不可能 (公開鍵を公開しても秘密鍵を複製されるおそれがない。)

