資料2

課題検討資料

目次

①【利便性の向上】オンライン更新‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥ 2
②【利便性の向上】有効期間の延長‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥ 4
③【利便性の向上】記録媒体の拡大‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥ 6
④【利用サービスの拡大】署名検証者の拡大（民間事業者への拡大）‥‥‥‥‥ 9
⑤【利用サービスの拡大】利用用途の拡大
（行政情報の閲覧等(認証用途)）‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥‥ 11
⑥【利用サービスの拡大】利用用途の拡大（署名メール・暗号メール）‥‥‥‥‥‥ 15

①【利便性の向上】オンライン更新

１．方向性

利用者の利便性向上の観点から、市町村窓口での対面形式のみとしている電子証明書の更新を自宅等からオンライン更新により行うことを検討する。

★ H18年度　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　論点整理より
サービスのセキュリティや信頼性が損なわれることがないよう十分配慮しながら、電子証明書の有効期間を５年程度へ期間延長を行うことや、電子証明書の更新手続をオンラインで提供することなどについて検討する必要がある。

２．課題

課題１：不正に鍵情報が取得されることをいかに防ぐか

オンライン更新を行う場合、電子証明書及び鍵情報のICカードへの書き込みは、書込み指示を行うサーバ（以下「更新サーバ」という。）からインターネットと自宅等のPC（以下「利用者PC」という。）を介して行われることから、インターネット、利用者PCから不正に鍵情報が取得されることを防ぐ方法を検討する必要がある。

課題２：どのように安全に鍵を生成するか

オンライン更新を安全に行うためには、どこで、どのように鍵を生成するかを検討する必要がある。また、利用者が鍵生成中に処理を中断した場合等についても考慮する必要がある。

①【利便性の向上】オンライン更新

３．考えられる方策例

案１：双方向認証後、更新サーバ側で鍵ペアを生成し、暗号化してICカードまで送信する方式

案２：双方向認証後、ICカード内で鍵ペアを生成する方式

※案2の場合は、住民基本台帳カード（以下「住基カード」という。）の仕様変更が必要であり、暗号アルゴリズム移行に伴い仕様を変更する平成24年まで実施困難。

４．検討を進めるに当たっての視点

視点１：安全性

視点２：コスト

視点３：その他

鍵ペア生成に要する時間

②【利便性の向上】有効期間の延長

１．方向性

利用者の利便性向上の観点から、電子証明書の有効期間を現行の３年から延長し、電子証明書を更新する頻度（電子証明書の更新に伴い市町村窓口に訪れる頻度）を下げることを検討する。

★ H18年度　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　論点整理より
サービスのセキュリティや信頼性が損なわれることがないよう十分配慮しながら、電子証明書の有効期間を５年程度へ期間延長を行うことや、電子証明書の更新手続をオンラインで提供することなどについて検討する必要がある。

２．課題

課題１：セキュリティや信頼性をどのように担保するか

同一の電子証明書を長期間利用することにより、サービスのセキュリティや信頼性が損なわれることを防ぐため、電子証明書で利用している暗号アルゴリズムが十分な強度を確保できる期間内で延長する必要がある。

課題２：有効期間を延長する場合何年とすべきか

電子署名法では「電子証明書の有効期間は、５年を超えないものである」としている。なお、住基カードの有効期間は１０年であり、その約数であれば利便性が高いとの指摘もある。

②【利便性の向上】有効期間の延長

３．考えられる方策例

案１：現行の暗号方式（RSA1024、SHA-1）で有効期間を５年に延長する。

案２：新暗号方式（RSA2048、SHA-256）で有効期間を５年に延長する。

案３：有効期間は延長しない。

４．検討を進めるに当たっての視点

視点１：有効期間延長による暗号アルゴリズムの安全性

視点２：暗号移行スケジュールの変更

※　2008年度に取りまとめられた「公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書」では、SHA-1及びRSA1024 による電子証明書の発行停止時期を2014年度早期としている。また、SHA-1及びRSA1024による電子証明書の有効期間後に、SHA-1及びRSA1024による電子署名に係る認証業務を停止するとし、その時期を2017年度早期としている。ただし、電子証明書の有効期間が5年に延長された場合は、その時期を2019年度早期としている。

視点３：その他

有効期間延長によるセンター設備への影響

③【利便性の向上】記録媒体の拡大

１．方向性

利用者の利便性向上の観点から、住民基本台帳カード以外に電子証明書を格納できる媒体について検討する。

★ H18年度　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　論点整理より

現行法制度においては、電子証明書の格納媒体の要件として、「住民基本台帳カードその他の半導体集積回路を一体として組み込んだカードであって、総務大臣が定める技術的基準を満たすもの」としており、技術要件を満たすカード（ICカード）であれば、種類を問わず電子証明書を格納することが可能となっている。ただし、現時点においては、住基カード以外で、技術要件を満たすことができる適切な格納媒体が見当たらないことから、住基カードをベースにサービスの運用がなされている。

・・・

今後、電子証明書の格納媒体について選択肢を増やしていくことも、利用者の利便性の観点からは有用と考えられる。

２．課題

課題１：セキュリティ水準を含む現行の技術的基準を満たすことができるか

課題２：電子証明書の複数発行についてどのように整理するか

記録媒体を拡大した場合、現行法上禁止されている電子証明書の複数発行を認めるかを検討することが考えられる。

③【利便性の向上】記録媒体の拡大

3. 媒体候補

	セキュリティ規格の準拠状況	製品価格
住基カード （現行の格納媒体）	◆ISO/15408　EAL4+ ◆FIPS140-2　レベル2相当	媒体：500円 RW　：3,000円～
ICカード　TypeB （住基カードを除く）	◆ISO/15408　EAL4+ ◆FIPS140-2　レベル2相当	媒体：500円～ RW　：3,000円～
ICカード　TypeC ※フェリカ	◆ISO/15408　EAL4+ ◆FIPS140-2　レベル2相当	媒体：1,500円～ RW　：3,000円～
携帯電話端末（SIMカード）	◆ISO/15408　EAL4+ ◆FIPS140-2　レベル2相当	媒体：2,000円～
USBスマートトークン	◆ISO/15408　EAL4+ ◆FIPS140-3　レベル3認定	媒体：3,000円～

③【利便性の向上】記録媒体の拡大

４．検討を進めるに当たっての視点

視点１　：　セキュリティ

視点２　：　製品価格

視点３　：　普及状況

視点４　：　市町村窓口での運用負担

視点５　：　その他

オンライン更新の実現性　等

※　本年度実施予定の新暗号方式に対応した鍵ペア生成装置の開発との連携が必要

④【利用サービスの拡大】署名検証者の拡大（民間事業者への拡大）

１．方向性

公的個人認証サービスの利用サービスの拡大を図るため、署名検証者を認定認証事業者等以外の民間事業者に拡大することを検討する。

★H18年度　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　論点整理より

公的個人認証サービスは、行政手続のオンライン化を進めるための基盤を整備することを主たる目的としており、現行法では、電子証明書の有効性を確認できる者（署名検証者等）の範囲については、行政機関、裁判所、行政手続の代理者、民間の認定認証事業者等に限定されている。このような限定を緩和し、より多くの者が公的個人認証サービスを使えるようにすれば、サービスの利便性の向上と利用促進に繋がることが期待される。

２．課題（1/2）

課題１：署名検証者の範囲をどこまで拡大するか

公的個人認証サービスは、地方公共団体という公的部門が提供するサービスであり、また、高い信頼性を確保することが求められていることから、国民が広く利用するなど基盤としての役割が求められる利用を中心に検討することが考えられる。

④【利用サービスの拡大】署名検証者の拡大（民間事業者への拡大）

２．課題（2/2）

課題２：署名検証者に求められる義務の適用について

署名検証者に求められる現行法上の義務（失効情報等の安全確保、電子証明書の目的外利用の禁止等）について、民間事業者に適用する必要があると考えられる。

課題３：民間事業者の利用促進

制度上、署名検証者の範囲を認定認証事業者等以外の民間事業者に拡大しても、民間事業者はビジネスベースに乗らなければ署名検証者とはならない。したがって、セキュリティ上の要請を満たすことを前提に、民間事業者のコスト負担の軽減を図るための方策等を検討することが考えられる。

また、民間事業者の業態別等による固有のニーズ（例：金融機関における証拠保全の必要性）に応える可能性等を検討することが考えられる。

⑤【利用サービスの拡大】利用用途の拡大(行政情報の閲覧等(認証用途))

1．方向性

利用サービスの拡大の観点から、各種情報を効率的に閲覧するための本人確認手段・認証手段としての役割を担うことが重要と考えられ、そのために必要な認証用途の付加について検討する。

＜検討対象パターン＞

パターン①　：　現行の署名用の電子証明書を認証用として併用する。

パターン②　：　現行の署名用の電子証明書とは別に、新たに認証用途の電子証明書（以下「認証用証明書」という。）を発行する

★ H18年度　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　論点整理より
公的個人認証サービスが認証用途の電子証明書を発行する形態としては、以下のようなパターンが考えられる。
①現行の公的個人認証サービスの署名用途の電子証明書を認証用として併用する
②現行法を改正し、公的個人認証サービスの都道府県単位認証局から、署名用途の電子証明書とは別に認証用途の電子証明書を発行する

⑤【利用サービスの拡大】利用用途の拡大(行政情報の閲覧等(認証用途))

２．課題（1/3）

課題１：送信否認を防ぐ効果を有するまま認証用途で利用することにより生じるリスクの排除

現行の署名用途の電子証明書は、推定効により送信否認を防ぐ一定の効果が働くが、当該電子証明書を認証用途に用いた場合、利用者が意図せず、不正な電子データに電子署名を行うリスクが生じるとの指摘がある。

そのため、パターン①では、署名検証者を一定の信頼性を有する者に限定するとともに、安全かつ確実に認証するための仕組みを設けることを検討することが考えられる。

※　技術的観点から当該リスクは事実上存在しない、あるいは、当該リスクが存在したとしても、法制度の実運用の観点からは問題は生じないとの指摘もある。

課題２：電子証明書を認証用途に利用する場合の記載事項について

電子証明書を認証用途で利用し、それが民間分野を含む広範な場面で利用され、利用頻度が飛躍的に増加した場合、証明書に基本4情報が記載されていると、悪意をもった相手に搾取され不正利用されるリスクが高まるとの指摘がある。

そのため、パターン①では署名検証者を一定の信頼性を有する者に限定するか、いわゆる「墨塗り」の技術等により基本4情報の一部又は全てを公開しないようにする、パターン②では基本４情報の一部のみを記載すること等を検討することが考えられる。

※ 「墨塗り」の技術を用いる場合は、各署名検証者のシステムを含むシステム全体に影響が及ぶため、移行に係るコストや各署名検証者が当該コストを負担する可能性等について慎重に検討する必要がある。

⑤【利用サービスの拡大】利用用途の拡大(行政情報の閲覧等(認証用途))

２．課題（2/3）

課題３：認証用証明書を発行するために必要となるコスト

パターン②では、認証用証明書を発行するシステムを開発し、維持管理するためのコストが生じる。また、認証用証明書を利用する各署名検証者においてシステム開発・改修等が必要。

課題４：利用者が２種類の証明書を適切に使い分けることが可能か

パターン②の場合、個々の利用者が署名用の電子証明書と認証用証明書を適切に使い分けることは困難との指摘がある。また、その場合は、パターン②でも上記課題１を解決することはできない。

課題５：認証用証明書の効率的な発行と記録媒体の拡大等の可能性

パターン②により認証用証明書を発行する場合は、発行事務全体の効率的な実施の観点から、登録業務（RA）は現行の電子証明書に委ねることとし、利用者は現行の電子証明書によりオンラインで認証用証明書を取得できるようにすることが考えられる。

また、認証用証明書の場合は、記録媒体に求められるセキュリティ水準が署名用の電子証明書ほどは高くはないとの指摘もあり、オンラインで取得した認証用証明書をパソコンのHDDに記録し利用する等、より利便性の高い方策を検討する余地が広がるとも考えられる。

⑤【利用サービスの拡大】利用用途の拡大(行政情報の閲覧等(認証用途))

２．課題（3/3）

課題６：具体的ニーズとの関係

認証用途の利用に関する具体的なニーズとして、社会保障カード（仮称）構想（H23年度開始予定）、国民電子私書箱構想での利用が想定されている。したがって、これらの実現スケジュールや検討内容との整合性を考慮する必要がある。

⑥【利用サービスの拡大】利用用途の拡大（署名メール、暗号メール）

１．方向性

公的個人認証サービスの利用サービスの拡大を図るため、署名メール及び暗号メールの実現について検討する。

２．課題

課題：署名検証者の範囲を個人へ拡大することが適当か

個人に対して、署名検証者に求められる現行法上の義務（失効情報等の安全確保、電子証明書の目的外利用の禁止等）の確実な遂行を求めることは現実的には困難との指摘がある。

そのため、個人を署名検証者としない仕組み（例：第三者機関による署名検証）による署名メール及び暗号メールの実現を検討することが考えられる。