資料１

公的個人認証サービス普及拡大検討会

中間取りまとめ（たたき台）

１．認証用途の付加

⑴ 課題

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

課題２：認証用途の電子証明書（以下「認証用証明書」という。）を発行する場合の記載事項

課題３：認証用証明書を発行する場合に必要となるコスト

課題４：利用者が現行の署名用の電子証明書（以下「現行証明書」という。）と認証用証明書を適切に使い分けることは可能か

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

課題６：認証用途に関する具体的ニーズ

⑵ 考えられる方策案

案１　：現行証明書を認証用として併用する。

案２　：現行証明書とは別に、基本４情報の一部のみを記載する認証用証明書を発行する。

⑶ 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：利便性

⑷ 視点ごとの評価

〔安全性〕

現行証明書を認証用途に利用する案１については、第１に、推定効により送信否認を防ぐ一定の効果が生じる中で、不正データに誤って電子署名を行ってしまうリスク、第２に、記載されている基本４情報が詐取、不正利用されるリスクがあるとの指摘がある。他方、第１のリスクについては、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、法実務の観点からは問題は生じないとの指摘もある。また、署名検証者を一定の信頼性を有する者に限定する、安全かつ確実に認証するための仕組みを設ける（例；認証用途のための専用のモジュール（以下「認証モジュール」という。）の開発）等により、これらのリスクを

相当程度軽減することが可能と考えられる。

〔コスト〕

案１については、署名検証者及び利用者に配布する認証モジュールを開発し、維持管理するためのコストが生じる。

案２については、現行証明書とは別に、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、また、認証用証明書を利用する各署名検証者においても個別にシステム改修等を行うことが必要となる。総じて言えば、案２は案１と比較してコストが顕著に高い。

〔利便性〕

案１については、利用者が２つの電子証明書を使い分ける必要がなく、開発する認証モジュールの機能によっては、署名用途と認証用途を意識せずに電子証明書を利用できるという利点がある。

⑸ 方向性

コストや利便性の観点から案１を軸に検討を行う。

なお、認証用証明書の場合は、証明書の記載事項を基本４情報の一部のみとした上でメールアドレス等の情報を付加することが可能であるとの指摘もあり、将来的により広範な場面で利用する可能性を視野に、現時点において認証用証明書の発行のために必要となる開発実証に取り組むことも考えられる。その場合、発行事務の効率的な実施の観点から、登録業務（ＲＡ）は現行証明書に委ね、利用者は現行証明書によりオンラインで認証用証明書を取得できる方法とすることが考えられる。

２．記録媒体の拡大

(1) 課題

課題１：セキュリティ水準を含む現行の技術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

(2) 記録媒体候補

記録媒体候補
住民基本台帳カード
ＩＣカード　TypeＢ （住民基本台帳カードを除く。）
ＩＣカード　TypeＣ ※フェリカ（PKI　Option）
携帯電話端末（ＳＩＭカード）
ＵＳＢスマートトークン

(3) 検討を進めるに当たっての視点

視点１：セキュリティを含む技術基準

視点２：製品価格

視点３：普及状況

視点４：市町村窓口等での運用負担

視点５：オンライン更新の実現等

(4) 視点ごとの評価

〔セキュリティを含む技術基準〕

住民基本台帳カード以外の記録媒体で、住民基本台帳カードと同等の安全性を確保することが可能と考えられる製品は存在する（上記(2)参照）。実際に当該製品に現行証明書を格納するためには、現行又は現行と同等の技術基準（ＩＣチップに専用の領域を有する、当該領域に電子証明書の記録が可能である、当該領域に耐タンパ性を有する等）を満たすことが求められる。

〔利用者負担〕

携帯電話端末やフェリカ対応の交通カード等については、多くの利用者が既に保有しており、このような媒体を記録媒体にすれば追加的な利用者のコスト負担を最小限に抑えることが可能とも考えられる。

住民基本台帳カード以外のＩＣカード、ＵＳＢスマートトークンについて、利用者が技術基準に適合した製品（ＵＳＢスマートトークンについては 6,000 円程度）を自らの責任で購入することとした場合、利用者負担が増加する。

〔普及状況〕

携帯電話端末やフェリカ対応の交通カード等の普及が著しい。

〔市町村窓口等での運用負担〕

住民基本台帳カード以外のＩＣカード、ＵＳＢスマートトークンについては、利用者が技術基準に適合した製品を自らの責任で購入することとした場合は、各市町村の窓口で正しい媒体であることを確認するための事務が生じる。なお、携帯電話端末のＳＩＭカードについては、携帯電話事業者が媒体の確認に一定の役割を果たすことが考えられる。

また、住民基本台帳カード以外のＩＣカード、ＵＳＢスマートトークンに格納するためには、鍵ペア生成装置、受付窓口端末等の市町村端末の改修等の対応が必要となる。

〔オンライン更新の実現等〕

携帯電話端末のＳＩＭカードに格納する場合、携帯電話事業者の既存システムと連携することにより、センター設備や市町村端末の改修を最小限に抑えられるとともに、独自の方式によりオンライン更新を実現できる可能性がある。なお、携帯電話事業者の既存システムとの連携を検討する場合は、携帯電話事業者による協力も不可欠となる。

⑸ 方向性

現行証明書の記録媒体としては、セキュリティ確保と普及状況等を考慮し、携帯電話端末（ＳＩＭカード）等に拡大することを検討する。

また、現行法上、利用者１人に発行できる電子証明書は１枚とされているが、記録媒体の拡大による利便性の高まりを享受するため、複数枚発行を認めることが考えられる。不正利用防止の観点からは、無制限に複数枚発行を認めることは適当でないため、利用者１人に記録媒体の種類毎に１枚の電子証明書を発行できるようにする（例えば、住民基本台帳カード用に１枚、携帯電話端末（ＳＩＭカード）用に１枚）ことが考えられる。なお、複数枚発行を行うためには、住民基本台帳システムも含めたシステム改修等を検討する必要がある。

３．オンライン更新

⑴ 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

課題２：どのように安全に鍵を生成するか

⑵ 考えられる方策案

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

⑶ 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：鍵ペア生成に要する時間

⑷ 視点ごとの評価

〔安全性〕

鍵の生成から格納までの一連の過程において秘密鍵がＩＣカードの外に出ない案２は、秘密鍵がインターネットや利用者のパソコンを経由する案１と比較して、安全性が高いと評価できる。

〔コスト〕

案１、案２ともに、センター側に更新サーバ等を設置するためのコスト、利用者に配布する更新用ソフトウェアを開発し、維持管理するためのコスト等が生じるが、案２は案１と比較してコストが低いと考えられる。

また、案１、案２ともに、市町村窓口での不具合等に対するリカバリ対応コストについて十分に検討することが必要と考えられる。（ＩＣカード内で鍵ペアの生成や格納をしている途中で処理を中断した場合等に不具合が発生し、市町村窓口等でリカバリ対応を行うことが想定される。）

〔鍵ペア生成に要する時間〕

案２は、案１と比較して、品質チェックに要する処理負荷が大きくなり、鍵ペア生成に要する時間が長い（数分程度）と考えられる。

⑸ 方向性

案２は案１と比較して安全性が高く、まず、案２によるオンライン更新の実現を検討する。

なお、現行の住民基本台帳カードの仕様では案２は実現できないため、新

たな暗号アルゴリズムに対応する住民基本台帳カードの発行（2011 年度末目途）にあわせ、その仕様に必要な機能を盛り込むことにより実現を図ることが考えられる。

また、携帯電話端末（ＳＩＭカード）に記録媒体を拡大する場合は、携帯電話事業者の既存システムと連携することにより、オンライン更新の実現を検討することが考えられる。

４．有効期間の延長

(1) 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

課題２：有効期間を延長する場合何年とすべきか

(2) 考えられる方策案

案１　：現行の暗号方式（RSA1024、SHA-1）で有効期間を５年とする。

案２　：新暗号方式（RSA2048、SHA-256）で有効期間を５年とする。

案３　：有効期間は延長しない。

(3) 検討を進めるに当たっての視点

視点１:「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」でとりまとめられた「公的個人認証サービスにおける暗号アルゴリズムの移行スケジュール」（以下「暗号移行スケジュール」という。）（※）との整合性

視点２：有効期間延長による暗号アルゴリズムの安全性

視点３：有効期間延長によるシステムへの影響

※　暗号移行スケジュール（「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（平成 21 年 1 月 26 日））

〇2014 年度早期

; SHA-256 及び RSA2048 による電子証明書の発行を開始するとともに、SHA-1 及び RSA1024 による電子証明書の発行を停止する。

〇2017 年度早期（電子証明書の有効期間が 5 年に延長された場合には 2019 年度早期）

; 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。

(4) 視点ごとの評価

〔暗号移行スケジュールとの整合性〕

いずれの案も、暗号移行スケジュールに即した対応が可能である。

〔有効期間延長による暗号アルゴリズムの安全性〕

案１の場合は、暗号移行スケジュールで想定されている現行暗号方式の利用終了時期を 2019 年とすると、現行暗号の危殆化リスクがあるとの指摘もある。この点、暗号危殆化リスクは、直ちに法実務や訴訟のリスクに結びつくものではない点についても十分考慮すべきとの指摘もある。

〔有効期間延長によるシステムへの影響〕

いずれの案も、2014 年の新暗号アルゴリズムの電子証明書の発行から 2017 年（暗号移行スケジュールでは、案１の場合は 2019 年）の現行暗号アルゴリズムの電子証明書利用の停止までの期間、新旧の両暗号アルゴリズムで発行された電子証明書を並行して取り扱えるようにするためのシステム負担が生じる。

また、案１、案２の場合は、保存する失効情報件数が５／３倍程度に増加することが想定されるため、それに対応するためのシステム負担が生じる。

(5) 方向性

現暗号アルゴリズムの電子証明書については、有効期間を５年に延長するとともに、セキュリティや信頼性の確保の観点や両暗号アルゴリズムで発行される期間のシステム負担の軽減の観点から、暗号移行スケジュールで認められている 2019 年までの使用終了時期を 2017 年早期までとすることを検討する。

また、2014 年より発行される予定の新暗号アルゴリズムの電子証明書については、有効期間を５年にすることを検討する。

５．署名検証者の拡大（民間事業者への拡大）

⑴ 課題

課題１：署名検証者の範囲をどこまで拡大するか

課題２：署名検証者に求められる義務の適用について

課題３：民間事業者の利用促進

⑵ 考えられる方策案

まず、署名検証者を民間事業者に拡大する範囲を決める。

次に、署名検証を行う方策について、次の案１及び案２の検討を行う。

案１　：署名検証に必要な設備は民間事業者において整備する。

案２　：民間事業者に署名検証を適切に行わせるための共同利用可能な基盤設備（以下「事業者基盤設備」という。）を整備し、民間事業者に必要なサービスを提供する。

（想定されるサービス）

・署名検証者向け標準インターフェース（証明書検証標準サービス）の提供

・署名検証者認証証明書の発行

⑶ 検討を進めるに当たっての視点

視点１：利用ニーズ

視点２：民間認証局との棲み分け

視点３：署名検証者の信頼性

視点４：コスト

視点５：適切な署名検証の実施

⑷ 視点ごとの評価

〔利用ニーズ〕

ヒアリングの結果等から、金融機関や電子商取引事業者に利用ニーズがあると考えられる。

〔民間認証局との棲み分け〕

署名検証者の範囲は、民間認証局との棲み分けの観点から、地方公共団体という公的部門が提供する公的サービスとして、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業種を中心に拡大することが適当と考えられる。

〔署名検証者の信頼性〕

署名検証者の範囲は、制度としての信頼性を確保するため、署名検証者としての法律上の義務を適切に遂行することができる事業者に限定して拡大することが適当と考えられる。

〔コスト〕

案１では､各民間事業者において個別に署名検証に必要な設備を開発し、維持管理を行う必要がある。

案２では、事業者基盤設備の維持管理コストやサービス提供のためのコストが発生する。当該コストはサービスを利用する民間事業者が負担することが適当と考えられるが、利用事業者数が増大することにより、１事業者当たりのコスト負担を低減させることが可能である。

〔適切な署名検証の実施〕

案１では、各民間事業者において適切な手順で署名検証が実施されないおそれがあるとの指摘がある。

案２では、事業者基盤設備において標準化された署名検証インターフェースを利用するため､適切な手順での署名検証の実施が担保される｡また、署名検証者用の証明書を新たに発行するとすれば、署名検証者の認証を適切に行うことが可能である。

(5) 方向性

署名検証者の範囲は、民間事業者に利用ニーズがあり、かつ、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事業者として、金融機関や電子商取引事業者等に拡大することを検討する。その際、署名検証者の信頼性を確保する方策を十分に検討することが重要である。

また、署名検証者の範囲を民間事業者に拡大するに当たり、合理的に民間事業者のコスト負担の軽減を図るための方策として､案２の検討を行う。その場合、事業者基盤設備の運営やサービスの提供を行う主体やコスト負担の方法、事業者基盤設備を利用して適切な署名検証の実施を担保する仕組み等について検討することが必要となる。

６．利用用途の拡大（署名メール及び暗号メール）

⑴ 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

⑵ 考えられる方策案

案　：個人の署名メール及び暗号メールの利用ニーズに応え、その利用を支援するための共同利用設備を設置し、個人が署名メール及び暗号メールを利用するために必要なサービスを提供する。

⑶ 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

⑷ 視点ごとの評価

〔安全性〕

共同利用設備を利用することにより、個人が署名検証を行う場合のリスク（失効情報等や基本４情報の漏えい等）を回避することが可能と考えられる。他方、共同利用設備について通信の秘密や検閲の禁止との関係をどのように考えるか慎重な検討が必要との指摘がある（特に運営主体が公的部門の場合）。

〔コスト〕

共同利用設備の維持管理コストやサービス提供のためのコストが発生する。共同利用設備の運営主体をどうするか、あるいは、個人に対価を徴求する仕組み（課金システム）を設けるかについて検討が必要となる。

〔その他〕

共同利用設備を利用する場合は、一般に利用されている署名メール及び暗号メールとは別の方式のメーラーソフトウェア等の開発・実装が必要となる。

⑸ 方向性

共同利用設備を利用した署名メール及び暗号メールの実現のための検討を進める。運営主体は、安全性やコスト面から検討する必要がある。

併せて、例えば、ＩＳＰや民間認証局と連携し、登録業務（ＲＡ）は公的個人認証サービスの電子証明書が担い、ＩＳＰ等が当該電子証明書を利用してオンラインで署名メール及び暗号メール用の電子証明書を発行する方式等を検討することも考えられる。